CA NetQoS® Unified Communications Monitor 3.1 Administrator Guide

www.ca.com

CA NetQoS Unified Communications Monitor Administrator Guide

DU31AG-0

The contents of this document are for informational purposes only and subject to change without notice. No liability is assumed for technical or editorial omissions contained herein.

Required Notices of Third Party Copyright and License Information

Contents

PREFACE

About This Document

This document provides background information, procedures, and best-practices advice to help you effectively use CA NetQoS Unified Communications Monitor version 3.1.

Unified Communications Monitor has been updated to provide a broader range of monitoring and reporting features, including additional support for unified communications deployments by different product vendors. Some of the capabilities of previous product releases have been enhanced.

The *Administrator Guide* includes the following chapters:

Chapter	Description
Chapter 1, “Best Practices, Hints, and Tips”	Introduces you to Unified Communications Monitor by providing recommendations for effective configuration and usage.
Chapter 2, “Installing and Setting Up UC Monitor Components”	Outlines steps to take to prepare to deploy the UC Monitor product and describes how to install it.
Chapter 3, “Preparing to Monitor a Microsoft Environment”	Summarizes UC Monitor support for monitoring Microsoft Office Communications Server 2007, describes requirements, and provides troubleshooting tips.
Chapter 4, “Preparing to Monitor Avaya”	Provides the necessary steps to set up the Avaya Communication Manager for monitoring with Unified Communications Monitor.
Chapter 5, “Setting Up the Management Console”	Details procedures for configuring the Management Console and collection components, including Collector thresholds.
Chapter 6, “Setting Reporting Parameters”	Provides background information, best practices, and procedures for adding Locations and voice gateways to your UC Monitor system.
Chapter 7, “Managing Data”	Provides best practices and procedures for changing the default performance and call server thresholds and setting up automated actions in response to threshold violations.
Chapter 8, “Using Troubleshooting Features”	Describes the Call Watch feature and provides instructions for using it.
Chapter 9, “Managing the Database”	Advises an Administrator how best to maintain the UC Monitor MySQL database.
Chapter 10, “Setting Up Security”	Explains UC Monitor security features and describes procedures for adding users and assigning permissions.
Appendix A, “Working with Groups in the CA NetQoS Performance Center”	Describes the grouping feature that works with the CA NetQoS Performance Center and provides tips and procedures for creating and using groups of devices and Locations.

Product References

This document references the following CA NetQoS products:

- CA NetQoS NetVoyant
- CA NetQoS ReporterAnalyzer
- CA NetQoS Performance Center

For more information about these products, consult their technical documentation and their context-sensitive online Help systems.

In addition to this book, you can find useful information in the following publications:

Document	Description
CA NetQoS Unified Communications Monitor Release Notes	Summarizes product features, supported VoIP and video hardware, and open issues.
CA NetQoS Unified Communications Monitor User Guide	Provides information for users to help them understand how the Unified Communications Monitor product tracks and rates VoIP system performance and call quality, and helps network engineers and operators interpret UC Monitor reports.
UC Monitor online Help	Provides context-sensitive and more detailed Help that can be accessed from the **Help** link in the UC Monitor user interface.

The product documentation is available in PDF format on the server where the UC Monitor Management Console is installed. Find the PDF files in the following location:

```
D:\NETQOS\VoIPMonitor\WebSite\Docs
```

In addition, the current versions of the PDF files for the product documentation, including the Release Notes, are always available on the CA Support Web site (http://support.ca.com/).

Conventions

The following conventions are used in this book:

- In instructions, **boldface** type highlights information that you enter or elements on the user interface that you click or select.
- `All syntax and literal examples are presented in this typeface.`
- In syntax, path names, or system messages, text enclosed in angle brackets (<>) represents a variable, as shown in the following example:

  `net time /setsntp: <ntpserver>`

Contact Technical Support

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 http://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

Provide Feedback

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

To provide feedback about CA product documentation, you can complete our short customer survey, which is also available on the CA Support Web site at http://ca.com/docs.

CHAPTER I

Best Practices, Hints, and Tips

This *Administrator Guide* provides in-depth information about how to install, configure, and run the CA NetQoS Unified Communications Monitor hardware and software. You should be able to start collecting data from your system within about an hour. However, an Administrator must complete a few steps to ensure that the data collected will be useful for systemwide monitoring and troubleshooting. In addition, administration tasks related to system performance and database maintenance must be performed periodically to ensure continued excellent performance.

This chapter provides a few pointers to assist you in installing and connecting the UC Monitor server, maintaining it and preserving a healthy state, and changing some of the default settings used in reporting and Incident creation.

This chapter covers the following topics:

- "Best Practices for UC Monitor Installation" on page 2
- "Best Practices for System Configuration" on page 4
- "Best Practices for System Maintenance" on page 8
- "About UC Monitor Performance Thresholds" on page 10
- "About Incidents and Incident Responses" on page 11

Best Practices for UC Monitor Installation

Depending on your environment, you should be able to start viewing UC Monitor report data soon after unpacking the hardware device. However, you will need to take a few steps to verify some settings and make sure the required packets are properly routed to the collection device. And to support monitoring in a multi-vendor or Microsoft Office Communications Server environment, more preparation is necessary.

- Chapter 2, “Installing and Setting Up UC Monitor Components,” walks you step-by-step through the installation process for a Cisco, Avaya, or Microsoft environment.
- Take the steps outlined in Chapter 3, “Preparing to Monitor a Microsoft Environment” on page 37 for a multi-vendor or Microsoft-only environment.
- Chapter 4, “Preparing to Monitor Avaya” on page 63 discusses items to configure for a multi-vendor or Avaya-only environment.

To monitor Cisco Unified Communications Manager, the Collector must be able to inspect every VoIP-related packet that passes between the call servers and endpoints in your system. It must therefore be connected at an appropriate network location, using a properly configured SPAN switch port. The following topics provide clarification of the SPAN port and switch requirements and discuss possible workarounds for environments where a SPAN port on a core switch is not available, or must be shared with another monitoring product.

Note: SPAN port configuration is not required to monitor Microsoft or Avaya.

Another installation best practice is to read “Planning for Deployment” on page 14 and “Gathering Required Information” on page 19 before you try to install the collection device to monitor Cisco devices. These sections provide advice about system scalability and firewalls, which you should consider as you set up your monitoring system.

The Collector Incidents Report, which supplies information about NetQoS Collector threshold violations, is a valuable resource to help ensure that the system is performing as expected. During the early phase of Unified Communications Monitor deployment, you should plan to check the Collector Incidents page regularly to ensure that SPAN ports are configured correctly and that the Collectors in your system are performing as expected. In the navigation links, click **Monitoring > Incidents > Collector** to see the Collector Incidents Report.

Spanning Tips

To monitor in a Cisco VoIP environment, you must connect a Collector to a SPAN (Switched Port ANalyzer) or mirror port on all switches carrying VoIP traffic on your network. A SPAN session on a switch allows network traffic from designated ports (or all ports) to be copied and sent to a single port on that switch (called the *destination* port or *monitor* port). The ideal location would be a core switch in a network operations or data center, but any switch with maximum visibility into call server traffic is acceptable.

Be careful not to oversubscribe the SPAN port output capacity. If possible, you should SPAN or mirror only VoIP traffic. For example, add any VLANs dedicated to voice traffic to the list of SPANned ports. VACLs are a useful tool. If you set up access lists, make sure the following traffic is being sent to the SPAN port:

- TCP traffic on Port 2000 (SCCP flows)
- TCP and UDP traffic on Port 5060 (SIP flows)
- UDP traffic on Port 2427 (MGCP flows)
- TCP traffic on Port 2428 (PRI backhaul)

Avoid situations in which a large-capacity switch is sending data from all ports to a single mirror port; data will be lost. Make sure call server traffic is being mirrored.

When determining where Collectors should be installed, select switches that are as close to the monitored call server(s) or voice gateways as possible. Server response times are calculated based on the assumption 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 should share a router to ensure that the paths returned from traceroute testing reflect the path taken by packets sent to and from the call server.

Before you start configuring your UC Monitor system (by defining Locations), check the dropped packets statistics on the switch SPAN port where you have connected the Collector to make sure it isn't congested or misconfigured.

A Distributed Collector and a Standalone server use one NIC for the Collector service, and one for management. If a tap is used, one NIC is used for management and two NICs are used for the Collector service. You should disable any unused ports.

Call Server Cluster Considerations

Cisco Unified Communications Manager (CUCM, or CallManager) servers can act in multiple roles to provide failover and load balancing capabilities. As a result, you should plan to configure the SPAN port so that VoIP-related traffic to and from all call servers is captured. That is, span network traffic associated with both CallManager Publishers and Subscribers.

Similar advice applies to voice gateway devices and their interactions with call servers. Voice gateways may register with either the Cisco Unified Communications Manager Publisher or Subscriber. Like the call servers, gateways are often configured to perform failover duties. The key point to remember is that any signaling between a voice gateway and a call server—in both directions—needs to reach the Collector to ensure monitoring of all call traffic on the network.

In a very large CUCM installation (of, for example just over 10,000 phones), each cluster would typically include as many as four servers, such as one Publisher, two Subscribers handling call processing, and one TFTP server, with the Publisher and TFTP server acting as backups for failover situations. In such a configuration, you would need to span the traffic going to two of the servers in the cluster, sending it to one Collector, and sending 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 would see data from only half the phones, a manageable load.

Some other advice pertinent to monitoring behavior in a clustered environment is specific to the use of grouping to organize report data. See "More about Cisco Call Servers" on page 249.

Best Practices for System Configuration

You need to perform a few simple customizations to ensure that UC Monitor data helps you understand VoIP and video performance on your network. Before you try to use the data collected and formatted in your first UC Monitor reports:

- Assign all phones or endpoints to Locations. Or for Avaya, create a Location for each IP Network Region.

  See "Purpose of Location Definitions" on page 5.
- Check voice gateway and interface configuration, and manually update it if necessary.

  See "Voice Gateway Definitions" on page 7.
- Supply SNMP information for all voice gateways and all Avaya call servers.

  See "Working with SNMP Profiles" on page 234.
- Customize performance thresholds.

  See "About UC Monitor Performance Thresholds" on page 10.
- Assign the custom thresholds to the Locations where the defaults don't seem to be appropriate.

  See "Threshold Guidelines" on page 10.
- Make sure Incidents trigger response notifications so that network operators can react quickly. By default, notifications are not enabled.

  See "About Incidents and Incident Responses" on page 11.

After you've gathered data for three or four days, you'll have a good sense for whether network operators are receiving too many Incident reports, or whether Incidents are being generated at a rate that's useful for managing call performance. A few days of monitoring will indicate whether degraded performance is being detected quickly enough by network operators. You can then adjust your Location definitions, threshold settings, and Incident responses if necessary and perhaps create custom groups to organize the Locations and devices being monitored.

Note: Groups are optional and require CA NetQoS Performance Center version 4.0 or later; see Appendix A, "Working with Groups in the CA NetQoS Performance Center" on page 241 for more information.

Purpose of Location Definitions

Defining Locations for your network only takes a few minutes. Location definitions determine:

- how data is displayed in reports
- the number of Incidents that are generated
- who is notified in response to each Incident

UC Monitor reports group call performance data based on Location. And threshold settings for each Location determine when Incidents are raised.

For example, one default threshold specifies that anytime latency values rise above 150 milliseconds for at least 15 call minutes at any Location, an Incident is opened to report degraded call performance. But on any given network, performance can vary substantially per subnet. Your network might include several branch offices, connected to each other by WAN links. Network performance is usually different over WAN links than on a LAN, so any calls that travel over these links might report worse latency and jitter metrics, at the least. Locations are used to monitor and report on such network segments separately.

It's important for you and your network operators to differentiate between expected performance and unusual, or truly degraded, performance. Otherwise, Incidents that correspond to an actual network anomaly that requires investigation might be lost amid a long series of Incidents that are being raised continually in response to a normal performance condition.

Incident response actions, such as automatically sending an email message to a network operator or launching a traceroute investigation, are also dependent on Location definitions and the threshold settings you have applied to them. Automatic email notifications are most effective if they are sent to the people closest to the source of the problem being reported.

Advice for Setting up Locations

The main rule to apply when adding Locations to your Unified Communications Monitor system is this:

- ▶ All UC components within a given Location, under normal operating conditions, ought to achieve similar performance based on the network links and equipment they access.

Anytime a network or network segment has distinctive characteristics, such as an Ethernet LAN segment connected to a Frame Relay network, you should create a separate Location for that network. Similarly, any phones that use a different codec from most other phones in the system should probably receive a separate Location definition.

Locations should help you identify subnets and hosts at a fairly granular level. In an Avaya system, you'll most likely create Location definitions to match your IP Network Regions. However, in most cases, you should avoid segmenting your enterprise into too many distinct Locations. An excessively long list of Locations won't be easy to view in reports. In addition, with too many Locations, you might see multiple Incidents that stem from the same root issue. If you (for example) divide a large LAN into multiple Locations, any problems that equally affect all IP phones on that LAN will still create multiple Incident reports, one for each Location.

The UC Monitor Management Console lets you set VoIP and video performance thresholds on a per-Location basis—or even between pairs of Locations, or pairs of Locations and voice gateways. As you define Locations, be aware of which call servers and gateways the phones in each subnet or IP network region are using. Doing so will make it easier to configure thresholds and gateways and interpret report data.

Once you reach about 100 Locations and voice gateways in your system, database performance may be affected. The Unified Communications Monitor Release Notes contain more information about database scalability.

One best practice we highly recommend for monitoring larger networks with many Locations is setting up a hierarchical structure to organize Locations, call servers, and voice gateways into groups of related items. Use the CA NetQoS Performance Center to create custom groups. UC Monitor reports then provide a drilldown path from group names and data rollups at the group level into data from individual managed items.

If you decide to organize Locations and devices into groups, the hierarchical structure you require may affect the naming of Locations. For example, you may choose an organizational rather than a geographical structure. We recommend planning out this structure before you begin so that Location definitions remain valid and useful. See Appendix A, "Working with Groups in the CA NetQoS Performance Center" on page 241 for a full discussion of the grouping feature.

That appendix also contains helpful information about monitoring networks in separate domains. If you plan to create custom domain groups so that overlapping IP addresses are monitored as discrete items, try to use the following workflow, where feasible:

- Create custom domains (specialized groups) in the CA NetQoS Performance Center.
- In the UC Monitor Management Console, create Location definitions and add subnets to them.
- Add Collectors, or if Collectors are already up and running, change the NPC Domain parameter to select the appropriate custom domain for the traffic they will monitor.

Key Phones

When adding Location definitions, you should designate a "key phone" at every Location. This step requires you to supply the IP address of a phone in one of the Location subnets. The key phone provides a target address for routine, automatic traceroute testing to create a baseline of route information.

Note: Use only Cisco IP phones as key phones. Routine traceroute testing is a Cisco-only feature.

By providing a known target, key phones also support the *investigations* feature. If a key phone is defined for a Location, each time a traceroute investigation is launched for a phone at that Location, the Investigation Report includes the baseline traceroute data just below the most recent traceroute data from the investigation. You can quickly see whether anything about the route, such as hops or latency, has changed.

Traceroute investigations are available for Cisco devices, and also for Avaya with some limitations. Such investigations may be launched on demand (with manual configuration) or automatically, in response to an Incident. We particularly recommend configuring the traceroute investigation action for call server group Incidents. The *UC Monitor User Guide* contains more information about the investigations feature and associated reports.

More tips about Location definitions and key phone selection are provided to help you gain value from the Phone Status Changes call server Incident. See "Call Server Group Threshold Settings" on page 151 and "More about the Phone Status Changes Incident" on page 152.

Voice Gateway Definitions

Unified Communications Monitor discovers most voice gateways and other media devices automatically and adds them to a list view. You need to review the list of discovered voice gateways and make sure that an SNMP profile with the correct SNMP community or other security parameters has been created to allow the Collector to poll Cisco gateways for management information.

In certain instances, you should also manually add voice gateway definitions to your system. You might want to do this if:

- some analog phones in the system are connected to a Cisco VG-224 gateway device. These gateway devices can be identified incorrectly in reports unless you add them as gateways.
- your voice gateways are running different versions of SNMP or are in different SNMP communities. Each voice gateway definition you add can be associated with a different SNMP profile.

  Note: The procedure for adding a new voice gateway includes an option to verify the SNMP security parameters and make sure the Collector can poll the device.
- you want to set up custom groups of devices and Locations in the NetQoS Performance Center. Groups allow you to grant view access to UC Monitor data when you configure user accounts. Voice gateways should be included in each user's permission groups.

You cannot add gateway voice interfaces to the system, but interface parameters can be edited. As a best practice, you should make sure that all known gateway voice interfaces have the number of channels correctly configured (check the **Discovered Capacity** parameter, and change it if necessary). In many cases, the Collector can get this capacity information from polling the gateway; if it changes, however, this information is not updated. The Voice Interface reports in the Capacity Planning section use the information shown in the **Channel Capacity** column of the Voice Interfaces list to calculate interface utilization as a percentage of capacity. These reports are less accurate if the device MIB is incorrectly reporting the gateway voice channel capacity.

See "Editing a Gateway Voice Interface" on page 123 for more information.

Best Practices for System Maintenance

Periodic maintenance ensures that product functionality and performance are unaffected by database size. CA NetQoS Unified Communications Monitor performs automatic system maintenance, including a weekly check for database corruption, and where necessary, performs repair operations.

By default, system maintenance runs every Sunday morning at 12:00 am on the Management Console. It involves a purging of data from the database as soon as it is out of compliance with the current database retention settings, which can be customized.

In situations of extremely high call volumes, however, a regular check should be manually performed each quarter and just before a product upgrade to ensure that database retention settings are appropriate for your environment. In extreme cases, SPAN configuration or the number of Management Consoles that are required to monitor in a given environment might also need to be considered. A thorough "tuneup" should include a brief consultation with a CA Support representative, who can advise you about any hardware updates that might be required to keep your system up to date. The following topic provides some guidance for you as you perform this periodic "tuneup" of your UC Monitor system.

Periodic Tuneups in High-Volume Environments

The key metric for understanding UC Monitor system performance is **call volume**. The Management Console can handle call data for up to **10 million calls per month**. That load can be spread out among multiple Collectors. But another factor must also be considered: the number of unique Locations and media devices being monitored. When the database contains **100** configured Locations and media devices, Console performance may start to decline.

The MySQL database on the Management Console has an upper limit of **40 million rows** before performance deteriorates. At this level of usage, the size of the database might produce display errors in the user interface and impede the performance of UC Monitor reports. Your tuneup of the UC Monitor system must include an analysis of database size, the types of data being retained, and the retention periods.

If your database is nearing this limit, you do not have to purge all data to maintain good performance. Several options are available for the duration of data storage and the type of data retained. They are discussed in detail in "Database Retention Options" on page 211.

Warning: If call volumes in your environment are very heavy, be careful not to run a database purge or any system maintenance during peak hours. System maintenance (including database pruning) runs automatically on a weekly basis; by default, it runs each Sunday at 12:00 am.

One simple way to improve database performance without sacrificing historical data is to remove any Location and voice gateway definitions that are no longer in use on your network. As part of your "tuneup," export a list of currently configured Locations from the Location List page and check for IP addresses that are no longer in use. See "Exporting Location Definitions" on page 114 for instructions.

Periodic Tuneups and User Accounts

A final check that should be performed during any “tuneup” concerns auditing product user accounts. Multiple, unique user accounts can be logged in and accessing the UC Monitor Management Console simultaneously. Your configuration might require multiple user accounts, often with different levels of access to data, or access only to certain groups.

Although there is no hardcoded limit to the number of users who can simultaneously access the Console, keep in mind that user interface performance may be affected if many users query the database at the same time. Each user account also adds a level of complexity to the database and can overburden it in extreme cases.

Another aspect of user accounts to consider during an audit is whether users’ assigned permission groups are still appropriate for their current job purview. Consider whether groups should be redesigned to make use of the group rules feature. Starting with CA NetQoS Performance Center version 6.0, system groups work slightly differently and are not very useful as a basic component of UC Monitor group construction. Grouping should now largely be accomplished automatically, by setting up group rules that add or exclude items as soon as they are discovered.

In the past, we encouraged UC Monitor Administrators to use system groups when building a grouping structure as a means of granting operators access to call data on a per-Location basis. This strategy is far less effective than leveraging the group rules feature. Because individual VoIP Locations cannot be added to a group by dragging and dropping them from the VoIP Locations system group, as could be done in past versions, the NetQoS Performance Center interface now encourages you to build groups another way, by either:

- selecting Locations and devices for each group from the lists provided on the **Items** tab.

  A separate list of devices makes it easier to remember to add call servers to each group, which is required to create valid permissions that allow the operator to see call data.
- creating rules to add items to groups automatically.

  For example, each time a new media device is detected from call traffic, it can be added to the appropriate group, based on its IP address.

Finally, when you perform an audit of existing user accounts, you should plan to delete any unused accounts to tighten product security.

About UC Monitor Performance Thresholds

Location definitions, discussed above, and the UC Monitor default performance threshold settings both play a role in call performance Incident reporting.

Performance thresholds define the boundaries of acceptable VoIP call or component behavior. They enable the UC Monitor software to rate collected data, and they contribute to Incident creation.

Unified Communications Monitor provides a set of default thresholds that were selected according to well-defined industry standards for acceptable VoIP performance. But even if these thresholds represent optimal call performance, they don't reflect the realities of performance on your particular network. The main reason to change the default thresholds is to *fine-tune Incident reporting*. Your ultimate goal is to ensure that the right personnel are receiving the right number of Incident reports.

You can create and apply unique performance threshold settings that are suitable for each of the Locations you've defined. Or you can apply a single set of threshold settings to all Locations in a particular region, to selected pairs of Locations, or even to pairs of endpoints that consist of Locations and voice gateways. See "Customizing Performance Thresholds" on page 162 for a full discussion.

If a particular part of the network is known to have relatively high latency, you can customize and apply a different latency threshold for the affected Locations and gateways. Threshold customization lets you ensure that Incidents are created at a modest rate and that they correspond to real performance anomalies that warrant investigation.

Installing the CA NetQoS Event Manager, which correlates and displays event information from multiple data sources in the CA NetQoS Performance Center, provides the additional benefits of event aggregation and correlation, as well as automatic notifications. The main data view, the Event List, displays aggregate event information from related call performance Incidents, alongside events reported by other CA NetQoS monitoring tools around the same time frame, to help IT staff quickly narrow down the sources of performance issues. See the Event Manager appendix to the UC Monitor *User Guide* for more information about Unified Communications Monitor support for the CA NetQoS Event Manager.

Threshold Guidelines

VoIP call performance occurs between pairs of phones and related endpoints. For example, call setup performance involves an interaction between the phone placing the call and a call server or voice gateway. Call quality performance occurs between pairs of phones.

By design, UC Monitor thresholds are also applied to pairs of endpoints.

- To use custom threshold values for call setup metrics, you change and then apply threshold values to a Location or to a voice gateway.
- To use custom threshold values for call quality metrics, you must apply the new threshold values to a pair consisting of two Locations, two voice gateways, or a Location paired with a gateway.

Note: Thresholds are not applied to the groups of devices or Locations that you can create in the CA NetQoS Performance Center.

Multiple Incidents are not created in response to the same call performance condition. All phones in the same defined Location produce only one Incident in response to similar data. For example, if the Collector detected low MOS values for three calls made at 2:07 p.m. at the St. Louis Location, it would open a single Incident—but only if the calls lasted at least 15 total minutes. The default threshold settings (the **Minimum Observations** parameter) specify that 15 call minutes must show low MOS values before the MOS Call Quality threshold is considered to have been breached.

Note: The default settings for the minimum observations were designed for the original reporting interval in versions 1.0 to 3.0 of CA NetQoS Unified Communications Monitor. Now that the reporting interval has been reduced to five minutes, this value might need to be reduced.

On the other hand, you might want to know immediately whenever an excessive threshold is violated. You can associate a notification action—either an email message or an SNMP trap—with the excessive threshold for that particular metric and decrease the required number of observations (a minimum number of calls originated for call setup, or call minutes for call quality).

In a relatively small-scale UC deployment, we recommend reducing the minimum required number of observations. Try running with all thresholds set to 1 call minute or 1 call originated for a week or so to see how many Incidents are raised.

About Incidents and Incident Responses

The term **Incident response** refers to one or more actions to be taken automatically in response to a threshold violation. CA NetQoS Unified Communications Monitor creates Incidents when thresholds are crossed.

The UC Monitor Administrator associates an Incident response with the Incident type (either Call Setup or Call Quality) while setting up thresholds. The Administrator then associates an action with selected Incident responses.

Like performance thresholds, Incident responses are available on a per-Location or per-voice gateway basis. Performance Incident thresholds and responses are configured based on the type of metric being monitored that will trigger that Incident:

- Call Setup Incident responses apply to Locations and to voice gateways.
- Call Quality Incident responses apply to pairs of Locations, pairs of voice gateways, or pairs of Locations and voice gateways.

  Call Quality monitoring occurs between IP phones, or between IP phones and gateways.

Neither performance thresholds, Incidents, nor Incident responses are applied to groups.

Incident Response Actions

By default, no actions are associated with Incident responses. You should plan to create at least one Incident response for call-setup or call-quality threshold violations and associate at least one action with it. The available actions are **sending an email notification**, **sending an SNMP trap**, and **launching a traceroute investigation** (call setup Incidents only).

See “Setting up Incident Responses” on page 191 for a full set of instructions.

The Launch Traceroute Investigation Incident response action is designed for call setup and call server group Incidents only. Traceroute investigations can be launched in response to call quality Incidents, but the results are usually not very helpful. The Collector, which is co-located with the call servers, launches the traceroute and can gather accurate data about the routing of call setup traffic between phones and call servers. But as stated above, call quality Incidents are reported between Locations. The routing data found will not be as accurate if the Collector is located in North Carolina (along with the call servers) and it launches a traceroute in response to a call quality issue that was reported in Texas, for example.

Incident Acknowledgement and Notifications

An Incident can be acknowledged to indicate that a UC Monitor operator is working on the problem. However, the action of acknowledging an Incident does not close it. A UC Monitor operator can 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 (indicated with gray shading in Incident reports).

To avoid such a situation, it's a good idea to configure an automatic email or SNMP trap notification as an Incident response action. Email messages are then automatically sent anytime an open Incident undergoes a change of severity status. Or if an SNMP trap action is configured, you can enable Severity Updates to receive similar notifications. See "Creating a New Incident Response" on page 192 for more information.

Also be aware that the CA NetQoS Event Manager, which displays aggregated event information from multiple CA NetQoS monitoring products, allows CA NetQoS Performance Center operators to close events from some data sources, such as CA NetQoS NetVoyant. But operators who try to close a UC Monitor event from the Event Manager can only succeed in acknowledging the Incident itself. The Incident that reported the event to the Event Manager will display as Acknowledged in UC Monitor reports while appearing to be in Closed state in the Event Manager.

An appendix to the UC Monitor *User Guide* explains UC Monitor support for the CA NetQoS Event Manager and describes how Incident status translates to event status. Versions 6.0 and later of the CA NetQoS Performance Center support Event Manager automated notifications to help you create a systemwide alerting procedure. We recommend upgrading as soon as version 6.0 is available.

For More Information

For more information about UC Monitor best practices, such as keeping monitoring configuration up to date when changes occur in the network or even setting up the SPAN port, log into the CA Support Online Web site. Documents maintained by the Support team are posted there, as well as product updates. A Knowledge Base contains articles that respond to specific customer questions or that provide supplemental information, such as how duplicate packets are counted by the Collector.

CHAPTER 2

Installing and Setting Up UC Monitor Components

CA NetQoS Unified Communications Monitor ensures the availability and performance of your Voice over IP (VoIP) or unified communications (UC) system. By passively monitoring all the VoIP call setup traffic associated with your Cisco Unified Communications Manager (CallManager®) clusters and voice gateways, by monitoring all calls processed by the Avaya Communication Manager, and by receiving call audio and video quality data from the Microsoft Quality of Experience Monitoring Server or OCS Front-End server, the UC Monitor software keeps a continuous record of call setup performance and call quality.

Before you try to set up your UC Monitor system, you'll need to gather some information about your network and equipment and check some configuration parameters at the call servers.

This chapter discusses pre-installation tasks and describes setup procedures. It covers the following topics:

- "Planning for Deployment" on page 14
- "Planning for System Scalability" on page 17
- "Pre-Installation Configuration Checklist" on page 20
- "Hardware Installation" on page 23
- "UC Monitor Licensing" on page 31
- "Launching the UC Monitor Management Console" on page 35

Planning for Deployment

Before you start setting up the UC Monitor components, take some time to plan your deployment. A misconfigured collection device won't gather the data you need to monitor your unified communications system. And UC Monitor reports won't help you monitor or troubleshoot your servers, phones, and gateways if the necessary data isn't being collected, or if it's being prevented from reaching the Management Console by a firewall.

Installing and setting up a UC Monitor system is a simple process. Most of the necessary tasks are performed by CA technicians before the equipment is shipped. However, at each step, you need to take care to create an organized system. Use methods and naming conventions that are helpful and meaningful to you and to your network operators.

The following sections provide an overview of the necessary steps for planning the installation, installing Unified Communications Monitor, and configuring the servers, gateways, and VoIP phones to be monitored. The UC Monitor Release Notes contain up-to-date information about call server, voice gateway, and IP phone device support. They are available in PDF format on the CA Support Online Web site.

For a discussion of post-installation configuration steps, see Chapter 5, "Setting Up the Management Console" on page 77 and Chapter 6, "Setting Reporting Parameters" on page 103. In addition to step-by-step instructions, best-practices information and practical advice are included in those chapters to help you get the most out of the UC Monitor product.

Planning for Hardware Requirements

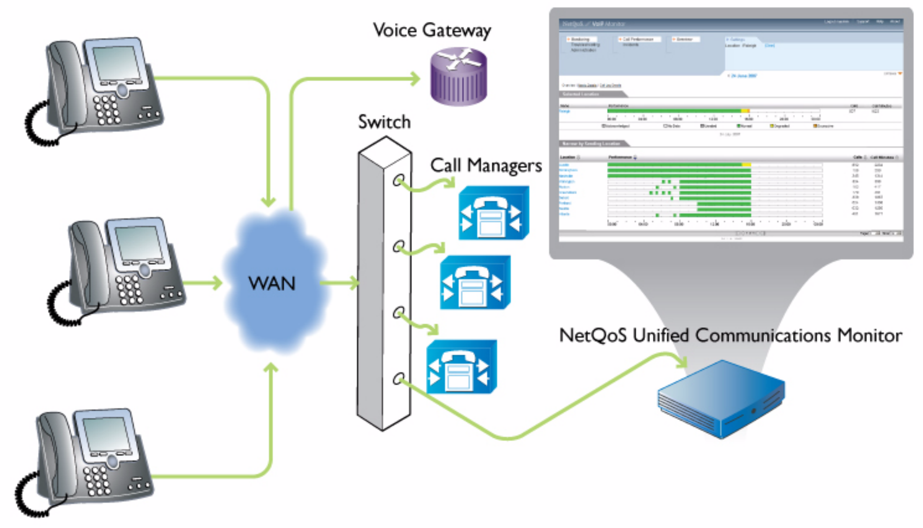
CA NetQoS Unified Communications Monitor consists of two major software and hardware components: the collection device and the UC Monitor Management Console. You can install multiple collection devices and have them all communicate with the same Management Console. For monitoring Cisco or Avaya VoIP deployments, the collection device is the NetQoS Collector (called simply the Collector). For monitoring Microsoft Office Communications Server voice and video calls, the collection device is the *OCS Collector*. The OCS Collector is actually the Microsoft Quality of Experience Monitoring Server (also called the "QoE Monitoring Server") or the Front-End server, configured to send quality metrics to the UC Monitor Management Console.

Two UC Monitor configurations are possible:

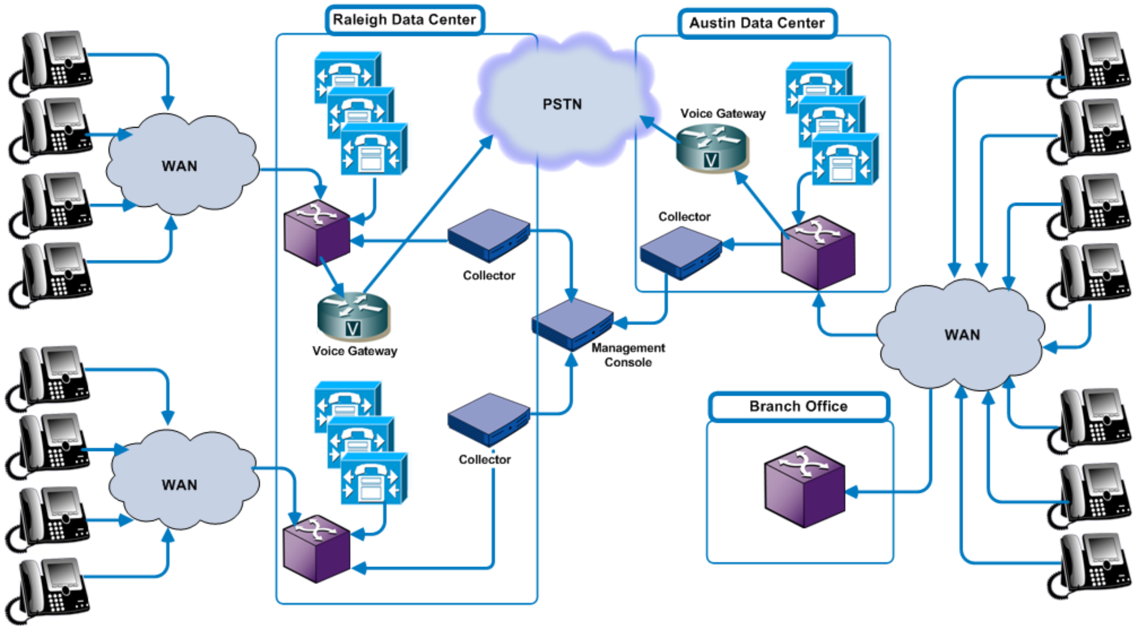
Standalone system — All UC Monitor components are installed on a single computer. To monitor Cisco, that computer must then be connected to a SPAN port (or mirror port) on a switch to which your call servers are connected. If you are evaluating the software, you are running a Standalone system.

Although additional Collectors cannot be added to a Distributed system without an upgrade, you can add an OCS Collector to a Standalone system.

Here's an illustration of a Standalone deployment:



Distributed system — At least two computers are used: one for the Collector, and one for the Management Console. To monitor in a large Cisco or Avaya environment, or in a large multi-vendor environment, a Distributed system architecture is required. The following image illustrates a Distributed UC Monitor system for monitoring a Cisco VoIP deployment:



Refer to "UC Monitor Architecture for Microsoft Deployments" on page 41 for an illustration of the Microsoft monitoring environment. Or refer to "UC Monitor Architecture for Avaya Deployments" on page 65 for an illustration of the Avaya monitoring environment.

When you purchase Unified Communications Monitor, you specify the desired configuration; CA technicians prepare the hardware component or components, install the necessary software, and mail the hardware to you for installation.

As shown in the above illustration, in order to monitor Cisco, a Collector is needed for every switch to which call servers are connected. However, multiple call servers might be connected to each monitored switch. See “Planning for System Scalability” on page 17 for more information.

Switch SPAN connections are not needed to monitor Avaya. And the Collector component itself is not required for monitoring Microsoft Office Communications Server 2007. Instead, a Microsoft server role is configured to send data to the UC Monitor Management Console for reporting. See Chapter 3, “Preparing to Monitor a Microsoft Environment” on page 37 for more information.

The maximum number of collection devices that can connect to a single Management Console is ten.

SPAN Port Configuration

To monitor in a Cisco VoIP environment, the UC Monitor Collector component must be connected—by means of a SPAN or mirror port—to any switches carrying VoIP traffic on your network. The topic titled “Spanning Tips” on page 2 provides helpful information about SPAN port requirements.

Note: A SPAN port connection is not needed to monitor Avaya or Microsoft deployments.

When determining where Collectors should be installed, select switches that are as close to the monitored call server(s) or voice gateways as possible. The UC Monitor software calculates server response times based on the assumption 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 and shares a router with it.

Configure the port to which the Collector is attached as a SPAN output port, such that the traffic of interest is forwarded to the Collector for monitoring. Be careful not to oversubscribe the SPAN port output capacity.

SPAN/Mirror Ports and Taps

As a general rule, SPAN or mirror ports work better with the Collector than network taps. Plan to plug the Monitor NIC on the Collector into the SPAN port unless it is already being used for another purpose, in which case, you should configure a network tap. (An exception would be an asynchronous routing environment.) You also have the option to configure remote spanning of switch traffic to another switch and connect the Collector to the SPAN port on the remote switch. But having a dedicated Collector for each switch is the recommended configuration.

If you are also running CA NetQoS SuperAgent on the network, you will probably want to connect SuperAgent to a SPAN port on a different switch. However, if you need to install both systems so that they monitor the same switch, you can use a network tap to segment the traffic intended for SuperAgent from the traffic intended for UC Monitor. The Collector may be connected to a standard tap (copper or fiber) or an aggregating tap in place of a SPAN or mirror port. Although SuperAgent supports a dual-NIC Collector, which a standard tap would require, the UC Monitor system does not support this type of Collector. You need to purchase a tap that sends the request and the response traffic over the same connection on the tap.

In some high-traffic situations, it's good practice to set Access Control Lists (ACLs) on the SPAN port so that only VoIP traffic is forwarded to the Collector. With ACLs, only useful traffic is forwarded to the Collector, and traffic not monitored by the Collector is discarded before it is sent out the SPAN or mirror port. If you decide to do this, make sure the following VoIP protocols are being forwarded to the Collector:

Protocol	Description
SIP	Session Initiation Protocol. An IETF standard protocol for multimedia applications that 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.
H.323	Designed to support real-time transfer of audio and video data over packet networks by allowing for communications between H.323-enabled devices (such as VoIP gateways). A family of related protocols. You'll need to 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	Skinny Call Control Protocol. Cisco proprietary protocol used for messaging between skinny clients and a Cisco CallManager. Forward TCP traffic on Port 2000 to the Collector to get Skinny flows.
MGCP	Media Gateway Control Protocol. Enables call-control devices, such as media gateway controllers (MGCs), to control VoIP calls. Performs similar functions to H.323 (see above). Forward UDP traffic on Port 2427 to the Collector to get MGCP flows.
Q.931	In a Cisco IP Telephony environment, call setup traffic is backhauled over a TCP connection to the CallManager so that it can directly control the Voice Gateway's ISDN PRI. The Collector needs to see the Q.931 Setup/Alerting messages that are sent between the CallManager and the gateway. Forward TCP traffic on Port 2428 to the Collector to get the PRI backhaul flows.

Also see "Call Server Cluster Considerations" on page 3 for more advice on setting up monitoring in clustered or large systems.

Planning for System Scalability

No matter how large your unified communications deployment is at present, you've probably built the system with future growth in mind. The number of users on the system may not grow substantially in the near term, but the number of calls made by your existing users might increase. Or you may decide to add some extra features to your system, such as video conferencing, which could alter usage patterns and increase the demand for network bandwidth.

When VoIP equipment vendors discuss scalability, it's usually in terms of the number of IP phone users or the expected number of calls. Cisco uses the terms **BHCC** and **BHCA**, or busy hour call completions and attempts: the number of calls or call attempts that can be processed during the busiest hours of the day. Cisco estimates that about five calls per user, per hour is a good starting point for calculating the BHCA of your system. They also recommend that each Communications

Manager call server manage no more than 7,500 IP users, or 30,000 users per cluster of call servers, with a maximum of 100,000 busy-hour call completions (BHCCs) per call server and 250,000 per server cluster.

The Cisco figures are dependent on other factors, such as system architecture and configuration. The presence and location of WAN links are extremely important scalability factors, for example. However, as a general rule, the BHCA is the most important metric for planning your UC Monitor system, no matter which vendor's equipment you are monitoring.

The UC Monitor components, particularly the Collector, have been designed to handle a BHCA of 25,000. In laboratory testing, the Collector could actually handle a higher BHCA; however, under normal or recommended operating conditions, multiple switches would handle that amount of call traffic, and an additional Collector is required for every switch that is handling Cisco VoIP calls.

Monitoring Microsoft Office Communications Server is not subject to the same limitations that apply to the Collector. With a single OCS Collector configured, you can monitor up to 40,000 endpoints. See "OCS Collector Bandwidth Consumption" on page 56 for more information.

Or see "Bandwidth Requirements" on page 66 for specific information about Avaya scalability.

Cisco further recommends the following to ensure failover capability and processing redundancy:

- The members of a single call server cluster should not share a single VLAN or switch.
- Different access switches should be used; you can connect them to the same distribution or core switch, or to different distribution or core switches.
- Call servers should be placed in different buildings within the same LAN or MAN.[1]

The Collector is also designed to handle "call storms," situations where the volume of VoIP traffic is far greater than normal. Keep the above information in mind when making decisions about the number of Collectors to purchase and where they should be installed.

Database Limitations

The main factor to consider when scaling up your UC Monitor system is database performance. Once the system includes more than 100 Locations and/or voice gateway definitions, reports become slower to generate because the database takes longer to process requests and search its tables.

The UC Monitor Release Notes contain information about the latest scalability figures, derived from laboratory and beta testing. You should also refer to "Recommended Database Limits" on page 215 for information about database retention rates and performance.

[1] See http://cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a00806e8c0a.html

Gathering Required Information

Before you install any UC Monitor components, review the documentation that describes the topology of your IP network and VoIP system. You need information about the geographical and logical distribution of network and VoIP components. The locations and IP addresses of all call servers and voice gateways are very useful, but not required, information. Similarly, you need a basic understanding of the logical groupings of the IP phones in your system, including their designated call servers and the switches to which they are connected.

In addition, you need to know the SNMP community strings for all voice gateway routers.

Depending on the security policies being applied on your network, you may also need to know how firewalls are configured so that communications between the Collector and Management Console are allowed to pass. The following topic contains more information.

Collector-to-Management Console Communications and Firewalls

In a **Distributed** system (that is, a system in which you have separate computers for the Collector and Management Console), the locations and configurations of any firewalls that are active in your network are required. You need to be aware of firewalls to prevent communication problems between the Collector and Management Console. Find answers to the following questions:

- Which firewall ports are open?
- What types of traffic are allowed on those ports?

The Collector includes a service that provides support for communications from the Management Console, which needs to send instructions, data-collection parameters, and other configuration information to the Collector periodically. Communications from the Collector to the Management Console use TCP over Port 1001.

The Management Console includes a corresponding service to provide communication support. Communications from the Management Console to the Collector use TCP over Port 1000. The following table summarizes the information you need to ensure that communications between the Management Console and collection devices are allowed to pass any active firewalls in the network. Note that no extra configuration is necessary if you are running the UC Monitor components in Standalone mode.

Parameter	Description
Collector Communication Service	
Service Name	`NetQoSVoIPCommunicator`
Display Name	NetQoS UC Collector Communicator
Service Description	Sends data from the Collector to the UC Monitor Management Console.
Path	`D:\NETQOS\VoIPMonitor\bin\commcollector.exe`
Listening Port	1000
Management Console Communication Service	
Service Name	`NetQoSVoIPConsoleCommunicator`

Parameter	Description
Display Name	NetQoS UC Console Communicator
Service Description	Handles communications between the UC Monitor Management Console and the Collector.
Path	`D:\NETQOS\VoIPMonitor\bin\commconsole.exe`
Listening Port	1001

The two services use different ports because in a standalone configuration, they must coexist.

Two more firewall settings are optional:

- For the Collector to be able to send SNMP traps (as Incident notifications) to a trap receiver, UDP needs to be allowed on Port 162.
- To allow on-demand traceroutes from the Collector to a selected endpoint, ICMP needs to be allowed.

For Avaya monitoring, the Collector listens for:

- RTCP flows on Port 5005 (UDP must also be allowed for transport)
- CDR data (TCP) on Port 9000

The default port settings are stored in the UC Monitor database and in the Windows Registry on the Collector; you can change these ports if necessary. Contact CA Technical Support for more information.

Pre-Installation Configuration Checklist

Before you begin a UC Monitor installation to monitor in a **Cisco** environment, make sure the following steps have been taken to configure the IP phones and call servers in your network:

Note: To monitor Avaya or Microsoft, other preparatory steps are required. See Chapter 3, "Preparing to Monitor a Microsoft Environment" on page 37 or Chapter 4, "Preparing to Monitor Avaya" on page 63 for more information.

Setting	Description
□ IP phones: Enable Web server	An IP phone's internal Web server enables other programs to access the phone's Web page, which displays configuration and status information used by the Collector. The `Web Access Enabled` configuration parameter indicates whether a phone's internal Web server is enabled. You can check this setting from the Network Configuration menu at the phone itself, but you can only change it at the phone's CUCM call server.

Setting	Description
□ Cisco call servers (Unified Communications Manager or CallManager): Enable CDRs and CMRs	If call data record (CDR) and call management record (CMR) collection is enabled, the Cisco Unified Communications Manager requests these records from the IP phones. They contain information about when calls were made, where they were directed, which phones made them, and whether they were successfully completed. You can enable CDR and CMR collection using Cisco Unified CallManager Administration. If the security requirements in your enterprise prohibit the storage of these records, see "Notes about Security Settings," below. Before you install the UC Monitor components, make sure that CDR and CMR collection is enabled on each call server in each monitored cluster. To enable CDR and CMR collection, set the `CDR Enabled` and `Call Diagnostics Enabled` flags on each call server to `True`. By default, both settings are disabled. You do not need to restart the call server for the change to take effect.
□ SIP Environments: Enable Call Stats	The SIP Profile in Cisco Unified CallManager Administration needs to be edited to enable call quality statistics. See "Requirements for SIP Support" on page 22 for the steps.

Notes about Security Settings

The `Web Access Enabled` setting on the IP phones may be disabled for security reasons. The Web servers are required for the Call Watch feature. Core monitoring functionality does not require you to enable this setting.

In some secure environments, CDR data cannot be stored on the call server. In such a case, you can enable the setting that instructs the phones to send the data to the call server, but disable the storage of CDR data on that server. Depending on your requirements, you may also want to enable CallManager purge settings to ensure that unwanted data is regularly purged.

In Cisco Unified CallManager versions 4.2.3 and later, you have the additional option of leaving CDRs disabled (the default). Call Watch will still work on these versions without CDRs. Or you can configure settings to enable the call server to request quality statistics at the end of calls without storing a CDR. The steps are similar for other versions of Communications Manager.

To prevent the Cisco call server from storing CDRs:

1. In Cisco CallManager Administration, navigate to **Service > Service Parameters**.
2. Select the **Cisco CallManager Service**.
3. Click the **Advanced** button.
4. Set the **CDR Enabled** flag to False.
5. Set the **Call Diagnostics Enabled** flag to True.

With those settings, the call server will still store a CMR in its database but discard the CDR. If you also need to discard the CMR, you can configure a setting to purge them:

1. Click **Service > Service Parameters**.
2. Select the **Cisco Database Layer Monitor**.

   This page includes settings for Max CDR Records and a Maintenance Time, the time of day when the system deletes CDRs and CMRs from the database.
3. Set the **Max CDR Records** to 1 (0 is not allowed).
4. Set the maintenance time to an appropriate time. CMRs will be purged automatically at that time.

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 your environment.

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.

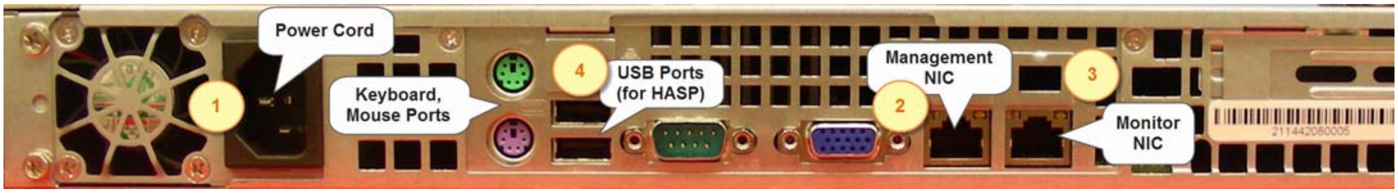
Requirements for Grouping Support

If you plan to take advantage of UC Monitor support for custom grouping of devices and Locations to help you organize reporting and user permissions, you must have an instance of the CA NetQoS Performance Center running in your environment. Groups can only be created, modified, and assigned to user accounts in the NetQoS Performance Center. Version 4.0 or later is required for integration with CA NetQoS Unified Communications Monitor.

See Appendix A, "Working with Groups in the CA NetQoS Performance Center" on page 241 for a full discussion of the grouping feature.

Hardware Installation

To set up CA NetQoS Unified Communications Monitor, you must install the following hardware components, which you have purchased and received from CA:



The diagram above shows the back of the UC Monitor appliance, where you must plug in the following components:

Component	Description
1. Power cord	Connects the UC Monitor device to a power supply, preferably a UPS.
2. Management NIC cable, either: **a.** A copper NIC cable (pictured above), or **b.** A Gb fiber NIC cable	When plugged into the switch, the Management network interface card (NIC) provides network access to the UC Monitor server and allows for remote viewing of the UC Monitor Management Console.
3. Monitor NIC cable	The Monitor NIC collects network traffic from a spanned port on the switch.
4. HASP (where applicable)	A Hardware Against Software Piracy (HASP) device; a hardware-based licensing and protection system, plugged into one of the USB ports shown above. Some systems use a software-based license instead of a HASP. If your appliance does have a HASP: • Install this device in the USB port for both the UC Monitor Management Console and any Collector appliances. • When you power on the systems, the HASP glows, indicating it is functional.

Note: If you are evaluating the UC Monitor product and the HASP or license expires before you purchase a license, data collection stops until you update the HASP or license.

The following table describes the steps you must perform to set up the hardware for a standalone or a Distributed system:

Standalone System	Distributed System
Management Console and Collector:	**Management Console:**
1. Plug the power cable into the power cable outlet (pictured above). **2.** Connect the Monitor cable to the NIC. It is Slot 2 for a copper connection (pictured above). **3.** Connect the Management cable to the NIC in Slot 1. **4.** Connect the Management and Monitor cables to the appropriate switches. ***Note:*** While the Monitor cable must be attached to the switch where call servers are connected, the Management cable enables network access to the Management Console and may need to be connected to another switch. **5.** If available, insert the HASP in the USB port (labeled in the picture above). **6.** Power it on.	**1.** Plug the power cable into the power cable outlet (pictured above). **2.** Connect the Management cable to the NIC in Slot 1. **3.** Connect the Management cable to an appropriate switch. ***Note:*** The Management cable enables network access to the Management Console. **4.** If available, insert the HASP in the USB port in the back or front of the unit. **5.** Power it on.
	Each Collector (maximum of 10):
	1. Plug the power cable into the power cable outlet (pictured above). **2.** Connect the Monitor cable to the NIC. It is Slot 2 for a copper connection (pictured above). **3.** Connect the Management cable to the NIC in Slot 1. **4.** Connect the Monitor cable to the switch SPAN port. **5.** Connect the Management cable to the Management Console computer. **6.** If available, insert the HASP in the USB port (labeled in the picture above). **7.** Power it on.

Distributed System Requirements

Follow the instructions in this chapter, with the following exceptions:

1. Configure the Management NIC on the UC Monitor Management Console only.
2. Configure the Monitor and Management NICs on the Collectors.
3. Disable all unused NICs on each system.

Configuring the NICs

One of the first steps to take to set up the Collector is to set up network connections for each Collector NIC. One NIC should be designated the Management NIC and the other as the Monitor NIC. The UC Monitor Management Console also needs to have the Management NIC prioritized as first in the list of adapters to be able to recognize it correctly.

You will first need to log into the UC Monitor computers (both the Management Console and Collectors in a Distributed system). Do the following:

1. Access the Standalone or Distributed UC Monitor Management Console.

   Use Terminal Services (Microsoft Remote Desktop), or access the Management Console computer directly.

2. Log in with these credentials:
   - Username: `netqos`
   - Password: `Changepassword1`

   This account has Administrator privileges on the UC Monitor device.

Collector Configuration

When you are setting up the Collector in a Distributed system, you might want to change the hostname assigned to it by CA. The following table suggests a naming convention for Collectors to help you identify them:

Suggested Naming Convention	Example
<*CollectorName*>-<*ManagementConsoleName*>-<*Location*>	CallManager-1-MainOffice-NYC

You will probably need to configure the network connections for the Collector NICs. In some cases, the settings are already correct, having been configured by a CA representative. Verify these settings or update them to suit your environment.

To configure the Collector NICs:

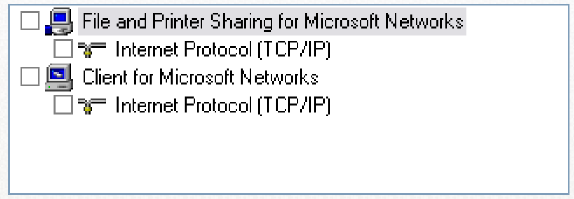
1. In the Windows Start menu, right-click **My Network Places** and select **Properties**.
2. In the Network Connections dialog box, check the names of the LAN or High-Speed Internet Connections. If necessary, edit the default names to correspond to the appropriate interfaces shown in the following table:

Device Name	Default Name	New Name to Assign
Copper Ethernet adapter	Local Area Connection 2	Management
Copper Ethernet adapter	Local Area Connection 3	Monitor
Gigabit Fiber port	Local Area Connection	Fiber Monitor

   You can identify ports by disconnecting the cable from the back of the unit and noting which interface status changes to **Disconnected** in the Network Connections window.

3. Disable any unused Monitor NICs by right-clicking the NIC and selecting **Disable**.
4. On the Advanced menu, click **Advanced Settings**.

5. On the **Adapters and Bindings** tab, use the up arrow on the right side to move the Management NIC to the top. This action sets the priority and is necessary for UC Monitor to operate correctly.
6. In the **Bindings** box, for the Monitor NIC, clear the check box for **Internet Protocol (TCP/IP)** on the following bindings:
   - File and Printer Sharing for Microsoft Networks
   - Client for Microsoft Networks



□ File and Printer Sharing for Microsoft Networks
  □ Internet Protocol (TCP/IP)
□ Client for Microsoft Networks
  □ Internet Protocol (TCP/IP)

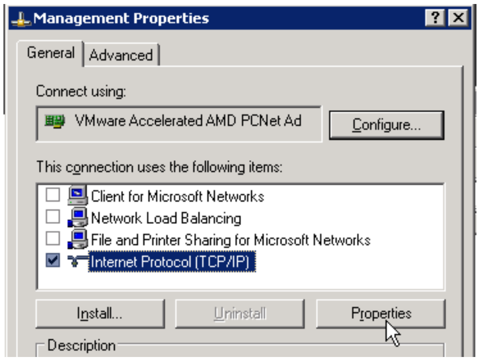
7. Click **OK**.

Assigning IP Addresses

Add the Collector to the network as if it were a new network user. Assign a static IP address, subnet mask, and default gateway to the Management NIC.

To configure the Management NIC as a network user:

1. On the **Start** menu, click **Settings** > **Control Panel**.
2. In the Control Panel, select **Network Connections**.
3. Right-click the **Management** entry under **Local Area Connections** and select **Properties**.



Connect using:
VMware Accelerated AMD PCNet Ad

This connection uses the following items:
□ Client for Microsoft Networks
□ Network Load Balancing
□ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

4. On the **General** tab, select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select **Use the following IP address**, and enter an IP address, subnet mask, and default gateway. Click **OK**.
6. Configure the DNS server by supplying its IP address.

   Problems are likely to occur if you try to use a DHCP address for the Management NIC.

The other NICs on the Collector—including the Monitor NIC—do not transmit data to the network, so the IP addresses assigned to them do not need to be valid for the network to which they are connected, nor do they require a default gateway assignment. Repeat the preceding steps to assign the following suggested values to the Monitor NIC(s):

NIC	IP Address	Subnet Mask
Monitor NIC	1.1.0.0	255.0.0.0
Fiber Monitor NIC	1.1.0.1	255.0.0.0

Additional Setup

After installing the HASP and configuring the NICs, take the following steps to update the UC Monitor computer(s) and make sure they are secure:

1. Access the Standalone or Distributed UC Monitor Management Console by:
   - Using Terminal Services (Microsoft Remote Desktop). Use the username `netqos` and the password `changeme`
   - Logging into the computer directly. Use the username `netqos` and the password `changeme`

   Note: If the password is not accepted, try `Changepassword1`
2. Check the Internet for any applicable Windows updates.
3. Check the **Support By Product** section of CA Support Online for software updates.

   The NetQoS products are all listed in the **Select a Product Page** menu under "CA NetQoS".
4. Install anti-virus software.
5. In your anti-virus program, exclude the `D:\NetQoS` directory *and all subdirectories* from any directory scans.
6. Verify the system time and time zone; we recommend making sure it is time synchronizing to the same source that your call servers are using.
7. (*Optional*) Configure the Network Time Protocol (NTP) and the server to which the computer should time-synchronize:
   a. At a command prompt, enter the following command:

   ```
   net time /querysntp
   ```
   b. Replace *NTPServer* in the following command with the name of the SNTP server that is returned for the query:

   ```
   net time /setsntp:NTPServer
   ```
   c. Configure the Windows Time service to start automatically.

   d. Restart the computer.

Upgrading a UC Monitor System

Support from CA and flexible licensing make it easy to upgrade your present Unified Communications Monitor system. If you have purchased the required maintenance, you can upgrade your system to a newer version. See "Upgrading from a Previous Version of Unified Communications Monitor" below.

In addition, you can convert a Standalone UC Monitor system to a Distributed system. This type of upgrade allows you to add more Collectors and monitor additional call servers and subnets. See "Upgrading from a Standalone System to a Distributed System" on page 30 for more information.

The best way to proceed with an upgrade in an environment where multiple CA NetQoS products are running on separate servers is to upgrade the CA NetQoS Performance Center software first, and then upgrade Unified Communications Monitor or another data source product, such as CA NetQoS NetVoyant. However, if you want to install the NetQoS Performance Center software on the same server as Unified Communications Monitor, be careful to always install the Unified Communications Monitor software first.

You should always have the latest version of the CA NetQoS Performance Center to take full advantage of integration features.

Upgrading from a Previous Version of Unified Communications Monitor

If you are running an earlier version of the product and have purchased a maintenance plan, you can upgrade your Management Console and Collector(s) from the CA Support Online Web site. Instructions are provided along with the software.

Before you perform the upgrade, back up the Console database. See "Backing Up and Restoring the UC Monitor Database" on page 217 for instructions.

- To upgrade a **Distributed** system, take a staged approach, running the upgrade executable on the Collectors first, and then run it on the Management Console server. Once you have upgraded one component, you should upgrade the others within a day to ensure database continuity.
- To upgrade a **Standalone** system, run the upgrade executable on the standalone device. Both components are upgraded simultaneously.

CA Support provides an Upgrade Guide, which you can find on the page with the other product documentation on the CA Support Online Web site.

Upgrade Tips

Before upgrading, you should make sure that any data collected has been processed by the Management Console. To see whether all data has been processed, check to make sure that the `D:\netqos\VoIPMonitor\Datafiles` folder is empty.

To prevent new data from being sent to the Console until the upgrade has completed, stop one of the services listed below:

- Upgrading a standalone system: Stop the NetQoS UC Collector (formerly the “NetQoS VoIP Agent”) service
- Upgrading a Management Console: Stop the NetQoS UC Console Communicator (formerly the “NetQoS VoIP Console Communicator”) service

Once the service is stopped, the files in `D:\NetQoS\VoIPMonitor\Datafiles` should be processed within 15 minutes. You can then proceed with the upgrade as described in the previous section. All services are restarted as part of the upgrade procedure.

Failure to stop the services will not cause the upgrade to fail, but some collected data may not be processed.

Any features added with the newer version of the UC Monitor software will be supported as soon as the new data becomes available. For reports newly added to a release, the data begins to be collected immediately, but some data rollups, such as hourly call volumes, for example, begin to become available one hour after the upgrade completes.

Browser and Display Issues

After an upgrade, you should clear the Internet Explorer browser cache before you log into the newer version of the UC Monitor Management Console for the first time. Otherwise, when you try to access reports, you may see some issues associated with cached content.

To clear the Internet Explorer browser cache:

1. On the Management Console device, launch Internet Explorer.
2. Click **Tools > Internet Options**.
3. In the Browsing History section, click **Delete**.
4. In the Delete Browsing History dialog box, click to delete **Temporary Internet Files**.

Another upgrade symptom is associated with the change to a more granular reporting interval for call setup and call quality data. As you are viewing reports, if you use the Time Period selector to view data collected in the past, you might inadvertently select a timeframe that spans older data collected at 15-minute intervals and newer data collected at five-minute intervals. In that case, you’ll see an informational message stating that the data views have been modified because “the time period you selected comprises data from five-minute and 15-minute reporting intervals.” The message further informs you that the older data is being filtered out of the view: “Only the 5-minute interval data is being displayed.”

To avoid this upgrade behavior, use the Time Period selector to change the timeframe so that the time when the upgrade was performed is not included, and only data collected before or after the upgrade is displayed.

Upgrading from a Standalone System to a Distributed System

If you are monitoring in a Cisco or Avaya environment, a standalone installation of the UC Monitor hardware and software is inherently limited with respect to the number of phones and calls you can monitor. In larger environments, a Distributed architecture (where the Management Console and Collectors are all installed on separate hardware components) is required.

Important: A Standalone system is all you need to monitor up to a maximum of 100,000 Microsoft endpoints, once you've purchased the necessary license upgrades. If you are monitoring in a Microsoft Office Communications Server environment, you would only need to upgrade a Standalone system to a Distributed system if you planned to start monitoring Cisco or Avaya call servers and IP phones in addition to the Microsoft endpoints.

You can convert a Standalone system to a Distributed system and avoid losing your data, preserving the Locations you have defined and the data you have collected. When you perform this type of upgrade, the existing UC Monitor hardware device becomes the Management Console, preserving your database. If the Standalone appliance has a hardware against software piracy (HASP) device, you must upgrade the HASP to support the new system configuration (that is, Distributed). You receive a new hardware appliance for the Collector. Its software license allows you to monitor up to 5000 phones.

Note: The term "Master Console" is used to describe the computer where the Management Console and database are installed in a Distributed UC Monitor system.

Future upgrades can be accomplished in a similar manner, with additional licenses available up to the maximum limit of 10000 phones and endpoints per Collector. (Additional Collectors may also be purchased, up to the maximum limit of 10 per Management Console.)

To convert a Standalone UC Monitor system to a Distributed system:

1. Access the UC Monitor Management Console.

   Use Terminal Services (Microsoft Remote Desktop), or access the computer directly.
2. Log in with Administrator credentials.
3. Open a command prompt.
4. Change directories to the `D:\NETQOS\VoIPMonitor\bin` directory.
5. If applicable, make sure the Standalone HASP has been reconfigured to enable the new Master Console. The necessary steps are described in "Applying Additional Licenses" on page 32.
6. Enter `UpgradeToMaster` to launch the upgrade.
7. Edit Collector Properties to update the name of the Collector and the IP addresses of the Management and Monitor NICs. See "Managing or Editing Collection Devices" on page 87 for more information.

UC Monitor Licensing

When you installed the UC Monitor software, you agreed to accept the accompanying license agreement. UC Monitor licenses are purchased based on a number of phones or endpoints to be monitored. A base license for monitoring either Cisco or Avaya allows you to monitor a maximum of either 2500 phones or endpoints (standalone configuration) or up to 5000 phones or endpoints (Distributed). In a Microsoft environment, the base license allows you to monitor up to 2500 endpoints. For installations of 1,000 phones or fewer where additional phones will not be added, a special Small-Site Collector is available, with its own licensing.

Depending on the monitoring environment, UC Monitor licenses usually correspond to the types of system that are available. The limits on the number of monitored phones or endpoints therefore ensure optimal performance. For example, a Standalone license does not allow you to exceed the recommended number of monitored IP phones so that UC Monitor database performance can be ensured. Within these performance limits, license upgrades are available to allow more phones to be monitored.

A license report is provided to let you know the status of your license and check whether you are nearing the maximum number of phones allowed by your license. You can view this report by clicking **Administration** > **Licensing** in the Management Console navigation links.

Product Licenses

UC Monitor product licenses correspond to the types of system that are available:

- **Standalone** — You receive a single hardware device that holds the Collector and Management Console. A base license supports monitoring up to 2500 phones or endpoints. This is the configuration to use for monitoring in a Microsoft-only environment.
- **Distributed** — You receive separate computers for the required number of Collectors and at least one Management Console. Each Collector base license supports up to 5000 phones.

  Note: Collectors are needed to monitor in either a Cisco or Avaya environment.
- **Small-Site**—You receive separate computers for the required number of Collectors and at least one Management Console. Each Collector license supports up to 1000 phones, with no upgrade option.

Each time a phone call is made on the monitored system, the phones involved in the call are logged in the UC Monitor database. A count of the total number of monitored phones is derived from these statistics. Even if you purge all data from your database, phone data is retained for at least 30 days.

Each time a new IP phone is seen, it is added to the database unless this addition would exceed the Collector's maximum license limit. If an additional phone would exceed the maximum limit, the Collector does not process the new phone; calls from that phone are not monitored.

Analog phones that are using a voice gateway for communications with the IP phones being monitored are not counted separately toward the license limit. Calls made with these phones are still monitored if the voice gateway itself is monitored. In all vendor environments that are monitored, the voice gateways/media devices themselves are counted as one phone for licensing purposes.

Depending on the type of licensing you purchased for CA NetQoS Unified Communications Monitor, each product component usually has an attached hardware against software piracy (HASP) device, which contains the license information necessary to enable product functionality. For new or evaluation licenses, the HASP is programmed before the components are shipped and sent to you for installation.

Software-based licensing may apply to your system instead of a HASP. However, with software licensing and HASP-based licensing alike, license upgrades can be purchased to increase the number of phones or endpoints that can be monitored. See "Applying Additional Licenses" on page 32 for more information.

Whichever type of licensing is used, any components that are licensed for evaluation only enforce an expiration date, typically 30 to 40 days after first use.

Applying Additional Licenses

UC Monitor license upgrades are available in increments of 2500 phones. In a Distributed system, you can upgrade any given Collector twice, from 5000 phones to 7500 phones, and then again to 10000 phones (the maximum recommended number of phones for a single Collector). For a Standalone system, license upgrades appropriate for monitoring additional endpoints or phones can also be purchased.

Note: The Small-Site Collector does not support license upgrades.

CA Support provides license upgrades. The Support technician requests some information and provides a software tool that reads the serial number of the Collector HASP or the key that is set in the software license and reports it to you. When you send this information to Support, a technician generates a new license key with the upgraded license information and sends it back to you.

You supply the new license key to the licensing tool, which reprograms your license and enables the UC Monitor components to monitor the additional phones.

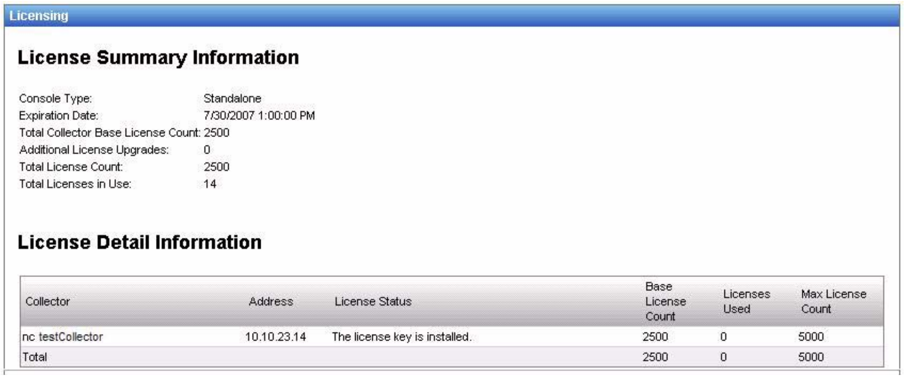
Upgrading a license differs based on the type of configuration you purchased:

Type of System	Upgrade Steps
Standalone	This configuration does not allow an additional Collector to be added (but OCS Collectors can be added). If you decide to upgrade this system, several options are available, depending on whether you are monitoring a single-vendor or hybrid environment. • See "Upgrading from a Standalone System to a Distributed System" on page 30 for more information about Cisco and Avaya monitoring. • If you are only monitoring Microsoft Office Communications Server 2007, license upgrades are available to allow you to monitor more Microsoft endpoints.

Type of System	Upgrade Steps
Distributed	In this configuration, you have purchased a Management Console and at least 1 Collector for monitoring Cisco or Avaya. Each Collector enforces a base count of 5000 phones based on its license. The Management Console tracks a total number of phones or endpoints and enforces a maximum limit of 10000 total phones and endpoints that can be monitored without an upgrade. **Initial rollout**: You do not enter any license information. As soon as you add the Collectors to the Management Console, the Collectors report their license limits and any phones they detect. The Management Console then tracks the total number of phones in the system and enforces the license limit. **Future upgrade options**: • You purchase another Collector. When you add it to the system, the Management Console tracks the number of additional phones supported by means of the license maintained on the new Collector. • You purchase a license upgrade for an existing Collector. You will need to contact Support and take the steps described above.
Evaluation	Same as for Standalone, described above.

The License Report

A License Summary report is available to keep you informed about the status of your UC Monitor licenses. The report consists of two sections: a license summary, and a section containing detailed information about your licenses:



License Summary Information

Console Type:	Standalone
Expiration Date:	7/30/2007 1:00:00 PM
Total Collector Base License Count:	2500
Additional License Upgrades:	0
Total License Count:	2500
Total Licenses in Use:	14

License Detail Information

Collector	Address	License Status	Base License Count	Licenses Used	Max License Count
nc testCollector	10.10.23.14	The license key is installed.	2500	0	5000
Total			2500	0	5000

License Summary

The following information is provided in the License Summary section of the License Report:

- **Console Type** — The type of UC Monitor system you purchased, either Distributed (“Master”) or Standalone. An evaluation license is only available in the Standalone configuration.
- **Expiration Date** —The date and time that your UC Monitor license will expire.
- **Total Collector Base License Count** — The total number of phones (IP phones or any supported endpoints) that your collection devices are licensed to monitor. This is a base amount and does not include any license upgrades you may have purchased. The Collectors maintain separate totals of IP phones and endpoints that each is licensed to monitor.

See "Product Licenses" on page 31 for more information about these values and how they are enforced.

- **Additional License Upgrades** — The number of phones or endpoints authorized for monitoring as a result of any license upgrades you have purchased. This count is maintained at the Management Console and distributed among all Collectors as additional phones are added.

  License upgrades are available in bundles of 2500 phones.
- **Total License Count** — The total number of IP phones or endpoints that your system is licensed to monitor. Collectors maintain limits and counts of phones they are licensed to monitor simultaneously. The Management Console maintains this total count, which, in a Distributed system, includes the Console total and all Collector totals.
- **Total Licenses in Use** — The total count of phones and endpoints currently being monitored. The difference between this value and the Total License Count is the number of new phones you can monitor without purchasing an additional license.

License Details

The following information is provided in the **License Detail Information** section of the License Report:

Column Title	Description
Collector	The names of all active Collectors—those you have installed and added to your Management Console. Does not include OCS Collectors.
Address	The IP addresses of all active Collectors. If you are running a standalone configuration, the address is the same as that of the Management Console.
License Status	The status of the license. Typically reads, "The license key is installed."
Base License Count	The total number of phones that each Collector is authorized to monitor simultaneously.
Max License Count	The total number of phones that you can monitor with your system, including all Collector totals and any license upgrades you have purchased.

Column totals are provided to help you track the number of licenses available and in use.

Launching the UC Monitor Management Console

To launch the UC Monitor Management Console for the first time, use the login information provided in the previous topic to access the computer. A UC Monitor icon is available on the Desktop. When you launch the Management Console, you will see the UC Monitor Login page.

Enter the default username and password as follows:

- **Username**: `nqadmin`
- **Password**: `nq`

Or you can browse to the Management Console over the network. The following steps provide instructions:

To launch the UC Monitor Management Console remotely:

1. Open a Web browser window. Microsoft Internet Explorer versions 7.0 and 8.0 are supported.
2. In the **Address** field of the browser, enter the IP address of the UC Monitor Management Console, such as:

   ```
   http://<IPaddress>
   ```
3. On the UC Monitor Login page, enter the default username and password as follows:
   - **Username**: `nqadmin`
   - **Password**: `nq`

For better security, we recommend changing the password. See "Initial Security Procedures" on page 78.

We also recommend adding the server hostname to the list of trusted Internet sites in the Internet Explorer browser instance to improve user interface performance. By default, Internet Explorer uses high security settings that restrict navigation to trusted sites or repeatedly display a warning message when you navigate to sites that are not on the list of trusted sites.

To add the UC Monitor server to the list of trusted sites:

1. First, launch the UC Monitor Management Console by double-clicking the UC Monitor icon on the Desktop.
2. In Internet Explorer, click **Tools > Internet Options**.
3. Click the **Security** tab.
4. Click the **Trusted Sites** icon in the list of security zones.
5. Click **Sites**.
6. The field labeled **Add this Web site to the zone** should show the following URL:

   ```
   http://localhost
   ```

   Click **Add** to add it to the list of trusted sites.
7. Click **Close** to return to the Internet Options dialog box. Then click **OK** to save your changes.

The first page you see when you launch the Management Console for the first time after installation is the Console Settings Administration page. See "Management Console Settings" on page 78 for more information about these settings.

Post-Installation Tips

The chapter titled “Setting Up the Management Console” on page 77 contains instructions for configuring the UC Monitor Management Console and Collector for monitoring Cisco or Avaya. You’ll need to take a few steps to establish communication between these components. If you are monitoring in a Microsoft-only or multi-vendor environment, you should carefully read Chapter 3, “Preparing to Monitor a Microsoft Environment” on page 37 before you add a Microsoft collection device. Chapter 4, “Preparing to Monitor Avaya” on page 63 provides important information about preparing the Avaya environment for monitoring with Unified Communications Monitor.

Once the various UC Monitor components are up and running, be sure to follow the guidelines provided in Chapter 9, “Managing the Database” on page 209 to ensure database integrity and performance. Specifically, you need to:

- Schedule and run regular defragmentation operations on the hard disk drive where the UC Monitor database is installed. See “Hard Drive Maintenance” on page 221 for more information.
- Schedule and run regular database backup operations. See “Backing Up and Restoring the UC Monitor Database” on page 217 for more information.

Next Steps

After you’ve configured your Management Console, as instructed in the previous topics in this chapter, you’ll need to inform the Management Console about any collection device(s) on the network to establish communication between them. You’ll need to create Location definitions to identify IP phones in reports and supply security information to allow the Collector to access MIB data from voice gateways. And you’ll want to change the default parameters that allow data to be evaluated and control how Incidents are reported.

Finally, you’ll create or edit the roles and user accounts that identify UC Monitor users and allow them access to the data that’s collected and stored.

The following chapters discuss the necessary steps in detail.

CHAPTER 3

Preparing to Monitor a Microsoft Environment

In addition to VoIP systems running on equipment made by Cisco Systems and Avaya, CA NetQoS Unified Communications Monitor offers support for monitoring VoIP and video deployments using Microsoft Office Communications Server 2007 and 2007 R2. The flexible product architecture allows you to monitor both Cisco and Avaya call servers and the Microsoft software-based system, or a single-vendor system.

Note: The version of Microsoft OCS that became available in late 2010, Microsoft® Lync™ Server 2010, or Lync Server, has not been fully tested with CA NetQoS Unified Communications Monitor version 3.1. Therefore, the configuration guidelines in this document do not apply in a Microsoft Lync Server environment. If you would like to use Unified Communications Monitor in a Microsoft Lync Server environment, contact CA Support.

A Collector is not required to monitor Microsoft deployments. Instead, Unified Communications Monitor uses information collected by the Microsoft OCS components themselves to calculate and report call quality. When Microsoft servers are configured to report data to CA NetQoS Unified Communications Monitor, they are referred to as *OCS Collectors*.

To monitor in a Microsoft environment, a monitoring server that is considered optional in the standard Office Communications Server deployment may be required. You'll need to configure parameters on that server or on your Front-End server to allow them to send data to the UC Monitor Management Console. This chapter discusses the required installation tasks and describes setup procedures. It covers the following topics:

- "Overview: Microsoft UC System Architecture" on page 38
- "UC Monitor Architecture for Microsoft Deployments" on page 41
- "Preparing the Microsoft Environment" on page 44
- "Preparing the Quality of Experience Monitoring Server" on page 45
- "Security in the Office Communications Server 2007 Environment" on page 53
- "Troubleshooting Tips" on page 57

Overview: Microsoft UC System Architecture

The Microsoft software-based VoIP and video solution is radically different from the Cisco Unified Communications system, which is based on dedicated call servers and supporting phone and gateway hardware. Where in a Cisco VoIP deployment the call servers act as PBXs to set up and route call traffic, in a Microsoft Office Communications Server 2007 deployment, no dedicated telephony hardware is required (although the system does support optional integration with a PBX). Instead, the standard Office Communications Server 2007 is now capable of processing VoIP and video calls. Audio and video calls are therefore integrated with other Office applications, such as Outlook and SharePoint, and with user contact information, such as IP address, SIP URI, and presence status. Users can, for example, access voice mail messages from their email Inbox and check another person's current status before placing a call to him or her.

The hardware-based IP phones of a Cisco deployment are another optional component in the Microsoft system. Users can make calls from supported phones, such as the Office Communicator hardphone, or from the lightweight Office Communicator application if their PC has a connected microphone and speakers.

Office Communications Server 2007 Configuration Options

The Microsoft documentation describes two basic configurations of the Office Communications Server 2007 system:

- **Standard Edition Server**—The Office Communications Server 2007 Front End acts as the *home server* for all users in the system and has the "Standard Edition" server role. It acts as a both a SIP registrar and SIP proxy and includes a SQL Server database containing all user contact information. Periodically, the Office Communications Server synchronizes user information from the nearest Active Directory global catalog.
- **Enterprise Edition Pool**—The functions performed by the Standard Edition Server are divided up and performed by multiple physical servers, which are organized in "pools." Users are assigned to different home servers in the Front-End cluster, which must be load-balanced. In this configuration, "Back-End" SQL Server databases are always hosted on servers that are separate from the Front-End servers, which provide IM, Web or telephony conferencing, and other optional services related to Web access.

  If further expansion of the system is needed, the Enterprise Edition Pool can be configured in an "expanded" architecture, in which each Front-End server hosts a single server role. In the expanded configuration, a dedicated physical server also runs each optional server role. Microsoft recommends designating one Front-End server as a "Director" to ensure that when users log in, Office Communicator clients can find their appropriate home server without querying multiple servers.

Voice and video calls from Microsoft use the SIP protocol for signaling and RTP for voice data. The SIP flows that pass among the software endpoints in the Office Communications Server system are encrypted by default, using TLS, and the RTP flows are encrypted using SRTP. A Mediation Server can perform transcoding and route PSTN calls to a media gateway, and voice mail storage is performed by Exchange Server 2007 Unified Messaging. If a PBX is used, it handles those tasks. An A/V Conferencing Server is required to enable conference calls.

The UC Monitor Release Notes contain up-to-date information about voice gateway and endpoint device support. They are available in PDF format on the CA Support Online Web site.

Office Communications Server Endpoints

In any Office Communications Server 2007 and later deployment, various servers perform the roles that in other telephone networks are performed by dedicated hardware, such as a PBX. In the Microsoft UC system, the VoIP or video *endpoints* are not always phones; they are typically instances of either the Office Communicator application or Office Communicator Phone Edition. These applications run on end-users' computers and mobile devices to enable calls from multiple access points. However, supported endpoints also include standard phones in the PSTN, IP phones from a supported vendor, and certain Microsoft servers.

Because of the security scheme used for communications in the Microsoft UC system, the endpoints are the only source of quality metrics from VoIP and video calls that travel over the network. The Office Communicator instances send out quality reports for every call they make. But quality reporting of some types of calls must be handled differently. For example, metrics from calls made by phones in the PSTN must be reported by the Microsoft Mediation Server.

At the end of each call handled by the system, a Microsoft server, either the QoE Monitoring Server or the Front-End server(s) in Office Communications Server 2007 R2, collects and stores call quality reports from the following sources:

- Microsoft endpoints, the devices that are configured to send and receive VoIP calls using the Office Communications Server as their home server.

  These include supported IP phones, Office Communicator 2007 clients, and Office Live Meeting 2007 clients.
- The Mediation Server, which handles calls from the PSTN.
- The A/V Conferencing Server, which enables conference calls that involve phones in the PSTN.

Once you have configured the UC Monitor collection device, the stored reports are batched and sent at regular intervals to the UC Monitor Management Console.

The Microsoft Office Communications Server Front End

An Office Communications Server 2007 pool consists of one or more Front-End servers that provide call processing, IM, presence, and conferencing services. They are connected to a SQL Server database for storing user data and conference information. In smaller systems, the database is installed in the Front-End server (the Standard Edition server).

The Office Communications Server 2007 Front-End server performs the following tasks:

- Call processing and other signaling among servers and between servers and clients
- Call routing within the system and to the PSTN
- Authenticating users
- Maintaining and providing user data, including all user endpoints and user presence status
- Initiating and managing conferences
- Routing IM and conferencing traffic, and managing conferencing media

Note: If you are running OCS Standard Edition, the standalone server takes the place of the Front-End server.

In Office Communications Server 2007 R2, the Front-End server has an additional role: it receives and forwards call quality (QoE) reports from the endpoints. If your system is running the R2 version of Office Communications Server 2007, any Front-End servers you have installed need to be configured to send these reports to the UC Monitor report recipient Web service.

As the main call-processing server, the Front-End server acts in a role somewhat analogous to the Cisco Unified Communications Manager in a Cisco UC system. In UC Monitor reports, the Front-End server that sends the QoE report for a particular call is featured in reports as a call server.

The Microsoft QoE Monitoring Server

The Quality of Experience Monitoring Server (QoE Monitoring Server) is an optional server role to enable audio and video quality monitoring in a Microsoft Office Communications Server 2007 system (pre-R2 only). To monitor in this environment, Unified Communications Monitor leverages data collected by the QoE Monitoring Server, which collects and stores end-of-call QoE reports from the endpoints.

The QoE Monitoring Server offers basic quality reports if you configure them in SQL Server Reporting Services (an optional component that must be installed on the server). In addition, if you install the optional MOM Management Pack, you can set up some basic alerts to respond to selected performance counters. However, when the QoE Monitoring Server is configured as an OCS Collector, the reporting and alerting features are greatly enhanced, leveraging the reporting and Incident creation capabilities of Unified Communications Monitor.

In Office Communications Server 2007 R2, the QoE Monitoring Server has a reduced role. It is still available as an option, but its name is changed to the Monitoring Server, and it is not necessary to facilitate the sending of QoE reports. It instead functions as a repository for CDRs in the R2 version and is not required for UC Monitor reporting.

The Microsoft Mediation Server

The Mediation Server is a required server role in most Microsoft voice and video deployments to provide PSTN access. In certain configurations, the Microsoft Office Communications Server 2007 system can also integrate with a third-party voice gateway to eliminate the Mediation Server role. Where it is deployed, the Mediation Server performs the SIP protocol translation necessary to allow voice (or media) gateways to communicate with the secure environment of the Office Communications Server 2007. It also uses a two-way connection to the voice gateway to:

- translate signals from older VoIP codecs to the new Microsoft Real-time Audio codec.
- enable calls from the PSTN to pass in and out of the OCS system.

A Mediation Server is required for each voice (or media) gateway, and it must be configured with a connection to an Office Communications Server. It also has to have a server certificate from a Certificate Authority (CA) that is trusted in the Office Communications Server environment.

Mediation Servers are monitored by Unified Communications Monitor, providing QoE reports for all calls involving phones in the PSTN. The Media Device views in UC Monitor Call Performance reports include performance ratings from the call legs they handle, and their volume statistics are also included in the Capacity Planning reports. But no baseline traceroute data is available from these devices.

To see a list of the Mediation Servers known to Unified Communications Monitor, click **Administration > Data Collection > Media Devices > Other Devices**.

UC Monitor Architecture for Microsoft Deployments

As explained in "Planning for Hardware Requirements" on page 14, CA NetQoS Unified Communications Monitor consists of two major software and hardware components: the Collector and the Management Console. Only the Management Console component is required in a Microsoft Office Communications Server environment, but an additional source of data is needed.

To monitor in a Microsoft Office Communications Server environment, Unified Communications Monitor leverages data that is actually collected by a Microsoft component:

- In Office Communications Server **2007**, the Quality of Experience Monitoring Server (called the QoE Monitoring Server, an optional server role).
- In Office Communications Server **2007 R2**, the Front-End server(s) (or a standalone Standard Edition server).

An architecture change for the R2 version of Office Communications Server 2007 affected the location of APIs to collect and forward the quality data that CA NetQoS Unified Communications Monitor uses to calculate and report VoIP and video call quality in a Microsoft UC deployment. To sum up the change, once you upgrade to R2, the optional QoE Monitoring Server becomes obsolete.

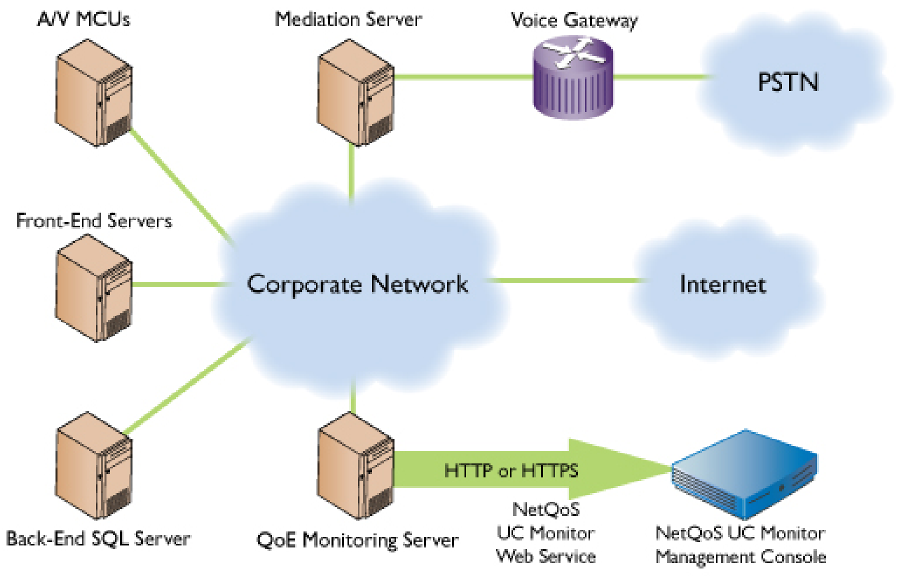
Note: The version of Microsoft OCS that became available in late 2010, Microsoft® Lync™ Server 2010, or Lync Server, has not been thoroughly tested with CA NetQoS Unified Communications Monitor version 3.1. Contact CA Support if you want to use Unified Communications Monitor in a Microsoft Lync Server deployment.

Supported UC Monitor Configurations

In a Microsoft single-vendor environment, only the standalone UC Monitor configuration is supported. The Collector component is *only* needed for monitoring Cisco deployments and is not supported in the Microsoft system. This component is still included on the UC Monitor standalone device, but it is disabled. If you later decide to monitor Cisco IP phones and call servers in addition to the Microsoft components, you can enable it by adding the Collector as a collection device.

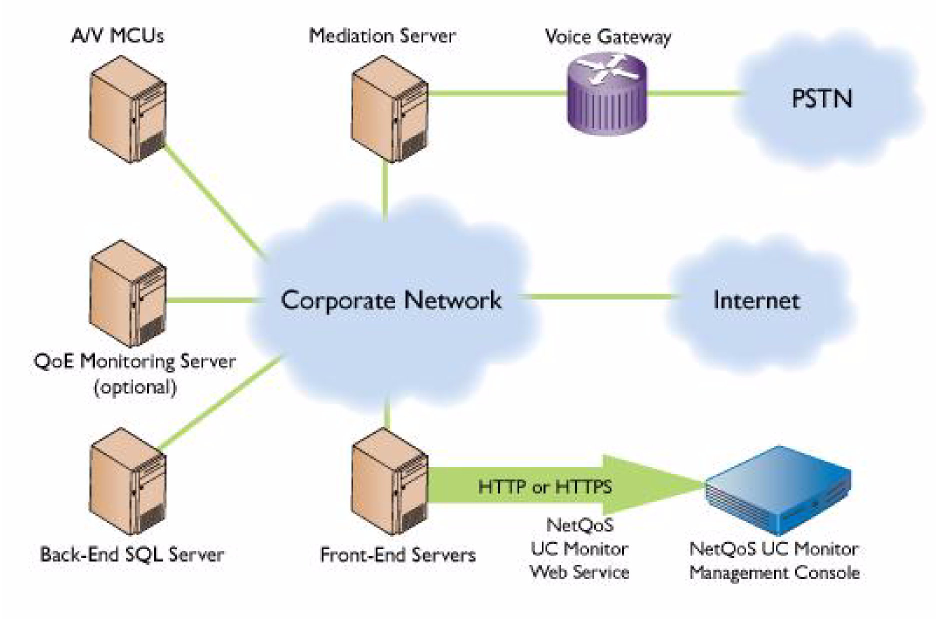
To monitor Microsoft Office Communications Server 2007, the UC Monitor standalone device is installed with network connectivity to the Microsoft QoE Monitoring Server. This server communicates via the UC Monitor Web service at the Management Console.

Here's an illustration of a UC Monitor standalone deployment in a Microsoft-only, **pre-R2** environment:



Note that in the Office Communications Server 2007 (pre-R2) system, the separate servers shown above are actually server roles that can be installed and running on a single computer. Usually, the QoE Monitoring Server runs on a separate computer.

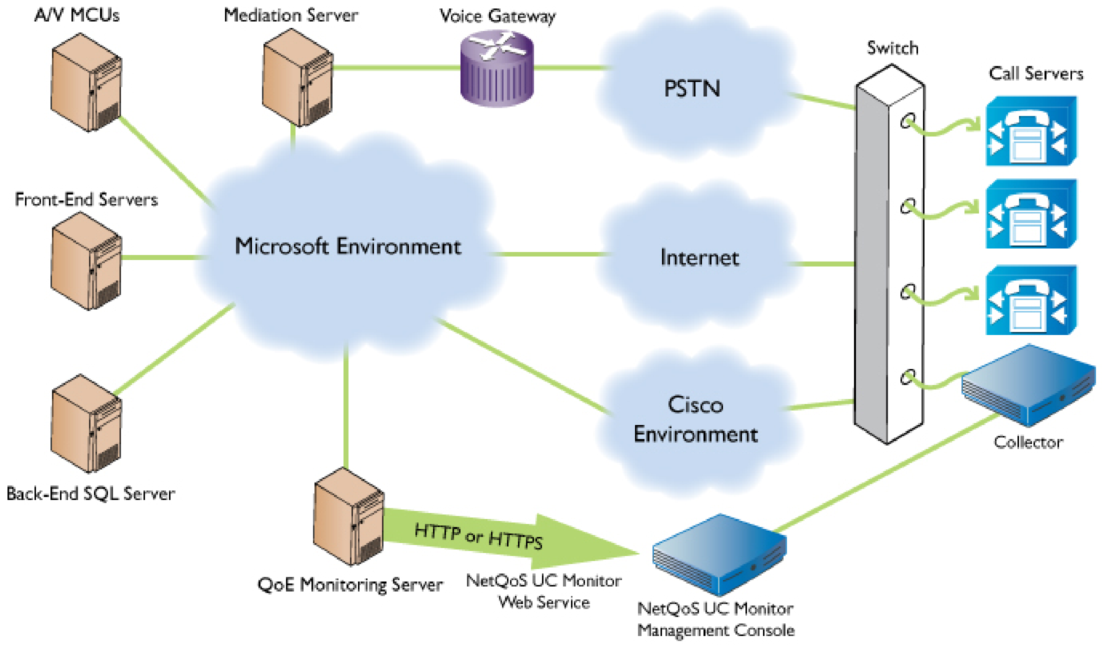
Once you upgrade the Office Communications Server 2007 to the R2 version, you can eliminate the QoE Monitoring Server. The Microsoft Front-End Server creates a connection to a Web service running on the UC Monitor Management Console so that it can send call quality reports to it via HTTP. Here's an illustration of the **R2 architecture** for Unified Communications Monitor:



System Architecture for Monitoring Another Vendor and Microsoft

A Standalone system is capable of monitoring a Cisco-Microsoft or Avaya-Microsoft mixed unified communications environment. As stated above, the Collector component on the Standalone device is disabled if only Microsoft components are monitored, and it can be enabled at a later point to allow for Cisco monitoring. (Avaya is handled differently.) No additional license is needed unless monitoring the additional phones would exceed the license limits.

But in a multi-vendor UC deployment, a Distributed UC Monitor architecture is also supported. In the **Distributed architecture** for monitoring Cisco or Avaya equipment and Microsoft Office Communications Server, at least two computers are used: one for the Collector to monitor Cisco or Avaya, and one for the Management Console. For Cisco monitoring, the Collector must be attached to a SPAN port on a switch where Cisco call servers are connected. In addition, either the Microsoft QoE Monitoring Server or the Front-End servers (for Office Communications Server version R2 and later), running within the Microsoft secure environment, provide call audio and video quality metrics. The following image illustrates such a system:



The Distributed architecture shown in the above image is needed for hybrid deployments that include Cisco. The Distributed architecture also allows for flexibility because Collector licenses can be upgraded to support more IP phones. But Collectors are not needed for monitoring Microsoft; therefore, a Standalone UC Monitor server is deployed in a Microsoft-only system.

To monitor Avaya along with Microsoft, the architecture is much simpler; no switch SPAN port is needed. A Standalone UC Monitor server is usually sufficient to monitor both.

Important: In an Office Communications Server 2007 R2 deployment, the Front-End servers send quality reports to the Unified Communications Monitor Web service, and the QoE Monitoring Server is not needed.

Preparing the Microsoft Environment

A few steps are required to enable Microsoft servers to act as UC Monitor collection devices (or *OCS Collectors*). The main tasks are related to report routing and security. By default, these collection devices—which have different server roles in the Office Communications Server 2007 and 2007 R2 environments—receive quality reports from Microsoft endpoints but do not send this information to an external source.

The external source, the UC Monitor *report recipient*, is configured automatically when you add a Microsoft server as a new OCS Collector:

Microsoft Environment	Server to Configure as OCS Collector
Office Communications Server 2007	Quality of Experience Monitoring Server
Office Communications Server 2007 R2	• Front-End server pool (Enterprise Edition), or • Standard Edition server

The UC Monitor Administrator must supply the relevant Microsoft server with the information required to direct the call quality reports to the UC Monitor report recipient. Unified Communications Monitor performs this step for you when you add the OCS Collector. As part of collection device configuration, the UC Monitor Administrator can also supply certificate information so that HTTPS can be used for encrypted communications between the Microsoft and CA components.

The following topics describe each component involved in UC Monitor support for monitoring Microsoft voice and video. And the section titled "Preparing the Quality of Experience Monitoring Server" walks you through the necessary steps to configure the UC Monitor collection device for your Microsoft environment.

More about the Quality of Experience Monitoring Server

In an Office Communications Server 2007 (pre-R2) deployment, the optional QoE Monitoring Server role collects and stores end-of-call quality reports from the endpoints.

The QoE Monitoring Server can be configured to transmit an audio/video quality (QoE) report for every call placed on the network to a QoE monitoring application, such as Unified Communications Monitor. Such an application is referred to as the *report recipient* (the "report consumer" in some Microsoft documentation). It uses `HTTP POST` to send these reports.

Warning: Each QoE Monitoring Server in your system can have only one report recipient configured. For purposes of Unified Communications Monitor, the recipient is the UC Monitor Web service.

When you configure Unified Communications Monitor to monitor in a Microsoft (pre-R2) environment, the Quality of Experience Monitoring Server becomes the UC Monitor "OCS Collector." This collection device can report to the same Management Console as the Collector that performs Cisco monitoring. The Microsoft quality reports, formatted in XML, are posted to a Web service on the UC Monitor Management Console, where they are processed, stored in the database, and used for UC Monitor reports.

For more information about the QoE Monitoring Server, see “The Microsoft QoE Monitoring Server” on page 40.

Preparing the Quality of Experience Monitoring Server

Note: These preparatory steps are not required if you are running Office Communications Server 2007 R2 or later. They apply to the Office Communications Server 2007 environment only.

The *Microsoft Office Communications Server 2007 Quality of Experience Monitoring Server Guide*, available from the Microsoft Web site, provides a full set of instructions for setting up a QoE Monitoring Server. The server must be up and running in the Office Communications Server 2007 secure environment before you can configure it as an OCS Collector in Unified Communications Monitor. The basic Microsoft guidelines apply: each server pool or Mediation Server can only communicate with a single QoE Monitoring Server, but a given QoE Monitoring Server can support multiple pools or Mediation Servers.

The steps involved in preparing the QoE Monitoring Server are as follows:

- Install the server
- Activate the server
- Configure a certificate for MTLS secure communications
- Start server services
- Associate the QoE Monitoring Server with pools and Mediation Servers

Once you’ve completed the required server setup, you use the Collection Device Administration pages of the UC Monitor Management Console to add the QoE Monitoring Server as a collection device. The Management Console report consumer then sends information to the QoE Monitoring Server to instruct it where to send call quality information.

If a firewall prevents the Management Console from configuring the QoE Monitoring Server, you’ll need to run the CA OCS Collector Configuration Utility. This utility is discussed below in “Creating a Connection to the Report Recipient” on page 49.

Installing and Setting Up the Quality of Experience Monitoring Server

Note: The information provided in this installation chapter assumes that you already have a functioning Office Communications Server 2007 voice and video deployment (pre-R2). The following topic provides an overview of the required installation and configuration steps. For in-depth information, consult the *Microsoft Office Communications Server 2007 Quality of Experience Monitoring Server Guide*.

To enable Unified Communications Monitor to monitor the Microsoft Office Communications Server 2007 environment, you must first install the Microsoft Quality of Experience Monitoring Server. Do not attempt to install it on the CA server. The first step is to download the Office Communications Server 2007 QoE Monitoring Server installer package, `OCSQms.msi`. You can then run the `setup.exe` program from the default location on the server hard drive:

```
<drive>:\Office Communications Server\QMS\setup\i386\.
```

A Deployment wizard walks you through the necessary steps to install the software. You must then activate the server. The required steps are dependent on the version of SQL Server you are running on the selected system. You can select whether to configure a new database or reuse an existing one.

As another required step, the Deployment wizard instructs you to configure a certificate to allow the QoE Monitoring Server to communicate with other servers in the Office Communications Server 2007 system using MTLS. The Deployment wizard allows you to create a new certificate using a Certificate wizard or to use an existing certificate.

The final pages in the Deployment wizard enable you to start the services. The Start Office Communications Server 2007 Services page contains a list of services that were found on the server. Click **Next** to start all services. When this step has been completed, click to enable the check box labeled **View the log when you click 'Finish'**, and then click **Finish**. In the log file, check to make sure each service has been started successfully, as indicated by the word `<Success>` in the **Execution Result** column.

After you complete these tasks, you must select the servers or server pools that the QoE Monitoring Server will monitor. This configuration step is called "association." The Deployment wizard launches a Configure Associations Wizard to help you select pools and Mediation Servers to monitor.

Important: If you are configuring multiple QoE Monitoring Servers, or if you have multiple pools or Mediation Servers in your environment, be careful to set up an association for every server that acts as the home server for a group of users. All the Mediation Servers in your system must also be associated because they are the source of quality reports from calls that involve parties in the PSTN.

When you have selected all the server pools and Mediation Servers that you want to associate with this QoE Monitoring Server, click **Next** on the Confirmation page. Then click to enable the check box labeled **View the log when you click 'Finish'**, and click **Finish**. In the log file, check to make sure each association has been configured successfully, as indicated by the word `<Success>` in the **Execution Result** column. Also check each listed task for the `<Success>` indicator.

Other configuration tasks outlined in the Microsoft documentation for the QoE Monitoring Server are not required. For example, configuring the Reporting Services is not necessary. You are now ready to instruct the UC Monitor Management Console how to contact the QoE Monitoring Server.

Preparing the Front-End Server (R2 Only)

The Front-End server is an integral part of the Microsoft Office Communications Server 2007 deployment and is already running when you install Unified Communications Monitor and prepare to monitor Microsoft OCS R2. However, in the R2 environment, the Front End server usually needs some extra configuration to prepare it to receive and forward call quality reports from the endpoints to the UC Monitor Management Console. Specifically, you need to take a few steps to enable the HTTP Report Provider service on the Microsoft server.

Note: The role of the Front-End server is provided by the standalone server in a Standard Edition deployment of Microsoft Office Communications Server 2007. The steps provided below apply equally to the standalone server. They are not required in a pre-R2 environment because the HTTP Report Provider service is installed along with the QoE Monitoring Server.

First of all, the Microsoft Message Queuing service (sometimes called “MSMQ”) is required. The report provider service will not start unless Message Queuing is installed on the Front-End or Standard Edition server. This service is not installed on the server by default. But it is included with the operating system and can be installed from the Control Panel. You might have installed it if you have already installed a Monitoring Server for call detail recording (CDR) or for QoE monitoring.

Note: The server must be a member of a Windows Authorization Access group so that it can authenticate users in a Microsoft Windows Server 2003 (or Active Directory, for Windows Server 2008) domain. The privacy level must be set to either **Body** or **Optional** (the default).

The following procedures explain how to install MSMQ on Windows Server 2003 and on Windows Server 2008:

To install Message Queuing on Windows Server 2003:

1. Log in to the server that will be running the Monitoring Server with a user account that is a member of the Administrators group.
2. Click **Start > Control Panel > Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. On the Windows Components page, click to select the **Application Server** check box, and then click **Details**.
5. In the Application Server dialog box, select the **Message Queuing** check box.
6. Click **OK** to start the installation.
7. On the Windows Components page, click **Next**.
8. Accept the default settings in the wizard to complete the installation.

Once Message Queuing is installed, you might need to take a few more steps to enable the HTTP Report Provider service. Otherwise, the service will start, but a message states that it will not run because there is no associated back-end server.

If the Front-End server is a member of a pool, the UC Monitor Management Console might not be able to enable QoE monitoring on all members of the pool, and your UC Monitor reports will therefore lack some data. You’ll need to perform some additional setup.

To install Message Queuing on Windows Server 2008:

1. Log in to the server that will be running the Monitoring Server with a user account that is a member of the Administrators group.
2. Click **Start > Programs > Administrative Tools**, and then click Server Manager.
3. Click the **Features** icon in the Server Manager tree.
4. Click **Add Features**.
5. Expand **Message Queuing**, expand **Message Queuing Services.**
6. Select the check boxes for the Message Queuing features that you want to install:
   - MSMQ-Server - Message Queuing Server
   - MSMQ-Directory - Directory Service Integration
7. Click **Next**, and then click **Install**.

If you are prompted to restart the computer, click **OK** to complete the installation.

To prepare the Front-End server pool:

1. First, add the Microsoft Office Communications Server 2007 R2 Front-End server (or standalone server in a Standard Edition deployment) as a collection device. See "Creating a Connection to the Report Recipient" on page 49 for the steps.

   If the server is a member of a pool, the Collection Device Properties page displays a message advising you to check the status of the **Enable QoE Monitoring** setting.

2. On a server where the Office Communications Server 2007 R2 MMC is installed, click **Start > Control Panel > Administrative Tools**.
3. Launch the Office Communications Server management console snap-in.
4. For each pool, take the following steps:
   - Right-click, and select **Front End Properties**.
   - In the Front End Properties dialog box, click the **Monitoring** tab.
   - Verify that the check box labeled **Enable QoE Monitoring** is checked.

   If the check box is checked, click **OK** to exit the dialog box.

5. If it is not checked, take **one of the following** steps:
   - Associate a Monitoring Back-End server with the pool:
     a. Click the **Associations** tab. Select a Back-End server from the list, and click **OK** to associate the Back-End server with the pool.
     b. Click the **Monitoring** tab again, and verify that the **Enable QoE Monitoring** check box is selected.
     c. Click **OK** to save the changes.
   - Use the CA configuration utility to configure the Front-End server to bypass the Monitoring Back-End server:
     a. Copy the `QMSConfig.exe` utility to one of the Front-End servers in the pool.
        This utility is provided in the `D:\netqos\VoIPMonitor\bin` directory on the UC Monitor Management Console.
     b. Run the utility on the Front-End server. You will probably want to keep the default settings.

        Note: When prompted, do not supply the optional username and password. WMI does not allow you to specify a different username/password combination when using a local WMI connection.

     c. Save the settings again.

     This procedure enables Unified Communications Monitor to collect data from this pool without a Monitoring Back-End Server.

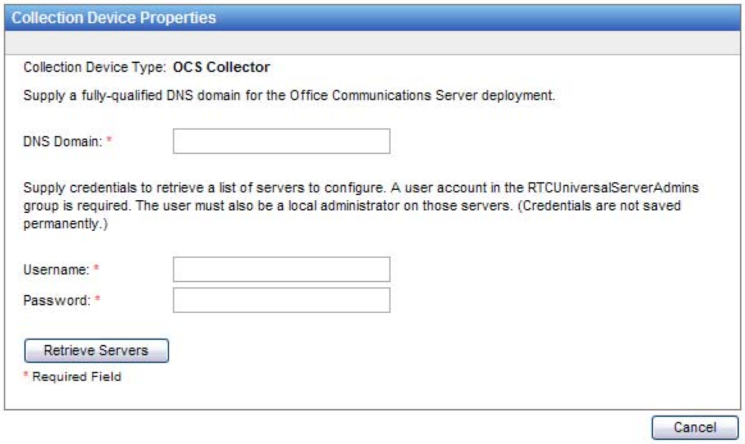
After you've completed the necessary steps to prepare the Front-End server(s), you should start receiving QoE reports from the endpoints within a few minutes. If you are not seeing any data in the main Call Performance Overview report after 20 minutes, you might need to perform some troubleshooting to determine whether the system is configured correctly. See, for example, "Failure to Configure OCS Collector (R2 Only)" on page 59 in the "Troubleshooting Tips" for more information.

Creating a Connection to the Report Recipient

The final required step in OCS Collector configuration is configuring the report recipient on the QoE Monitoring Server or Front-End servers. In Microsoft documentation, the recipient is often referred to as the *report consumer*.

The Microsoft server requires information to identify the UC Monitor report recipient Web service. It also needs to know how to contact the report recipient and how often to post the call quality reports it receives from the endpoints to the UC Monitor Management Console. Because external report recipient information cannot be configured in the user interface of the QoE Monitoring Server, the parameters are set by Unified Communications Monitor, using WMI and the export parameters on the Microsoft server.

In the UC Monitor Management Console, the Administrator can use the Collection Device configuration pages to add the OCS Collector as a new collection device. Where a **Monitor Address** is used for Collectors, for the Microsoft server, a secure username and password are required to allow remote configuration of the report recipient identity and server behavior, as shown below:



Collection Device Properties

Collection Device Type: **OCS Collector**

Supply a fully-qualified DNS domain for the Office Communications Server deployment.

DNS Domain: *

Supply credentials to retrieve a list of servers to configure. A user account in the RTCUniversalServerAdmins group is required. The user must also be a local administrator on those servers. (Credentials are not saved permanently.)

Username: *

Password: *

Note: Be sure you are logged into the domain with the appropriate administrative privileges. To successfully configure the OCS Collector and retrieve the settings, your login account needs *both* Domain User and Local Administrator privileges on the computer where you are performing the Add Collection Device task (the Management Console).

For a full discussion of OCS Collector configuration, see:

- "Adding a Collection Device" on page 83
- "Collection Device Properties" on page 88
- "Editing OCS Collector Advanced Settings" on page 90

Updating the System after Changes to Pool Configuration

Anytime you make certain changes that affect the identity of the Microsoft report recipient, whether the changes relate to additional Enterprise Edition servers in the pool, or whether they stem from a UC Monitor Management Console upgrade that affects the management address, you will need to edit the OCS Collector to make sure call quality reports are routed correctly. For example, the IP address of the Management Console might change. OCS Collectors that send reports to that report recipient will need to be notified of the change.

To update the OCS Collector after a change:

1. Access the Collection Device List by clicking **Administration > Data Collection > Collectors**.
2. In the list of collection devices, click to select the OCS Collector, and click **Edit**.
3. On the Collection Device Properties page, supply the username and password for a secure Windows account with Administrator access to the Microsoft server that is acting as an OCS Collector.

   Note: Supply credentials for an account in the RTCUniversalServerAdmins group to allow for read-write access to the target Microsoft server.
4. Click **Retrieve Settings**. If your credentials allow you to query the target server for current report recipient settings, additional information about the Collector is displayed on the Collection Device Properties page.
5. Check the report recipient information in the collection device properties. The IP address shown in the field labeled **Send reports to:** should be the IP address of the UC Monitor Management Console server. If it has changed, update it.
6. Click **Save** to save the settings. This sends the information to all members of the pool, including any new members.
7. If necessary, repeat the above steps for all OCS Collectors.

When the Management Console receives quality reports from any new servers, they are added to the existing call server group that represents the pool that was affected by the change.

OCS Collector Remote Configuration

Configuring the report recipient on the Microsoft QoE Monitoring Server or Front-End server is normally a simple task, part of the process of adding collection devices to the UC Monitor Management Console. The necessary steps are described in "Adding a Collection Device" on page 83.

If a firewall or policy restrictions prevent the Management Console from contacting the Microsoft server, your attempt to add the OCS Collector will fail. For such cases, CA has provided a utility to configure the report recipient information and set the required parameters. You can find this utility, `QMSConfig.exe`, in the following directory on the Management Console computer:

```
D:\netqos\VoIPMonitor\bin
```

You can run the configuration utility on the QoE Monitoring Server or Front-End server itself, or from another computer with secure, unrestricted access to that server. Depending on your security settings, you may need to copy the executable to the Microsoft server before running it. Its user interface displays the same parameters you can set in the Management Console. See "Collection Device Properties" on page 88 for a description of the parameters you can configure and suggestions for changing them.

In general, we recommend using the UC Monitor default settings, which closely resemble the Microsoft defaults.

Important: When running the `QMSConfig` utility on the computer you are configuring, do not supply the optional username and password. WMI does not allow you to specify a different username/ password combination when using a local WMI connection.

The easiest way to set up a connection to the report recipient is by adding an OCS Collector from the Collection Device Administration page. However, one final option is to set the required WMI parameters from a remote computer. See the following Microsoft article for details on how to connect remotely to use WMI:

http://msdn2.microsoft.com/en-us/library/aa389290(VS.85).aspx

The quality metric export configuration parameters can be configured via the WMI singleton class `MSFT_SIPQMSExternalConsumer`. The following table describes the required and recommended settings for this class:

Name	Description	Type	Default	Notes
InstanceID	GUID identifying the class	GUID	`53094317-4455-44ed-B8D5-A716972B3344`	
ConsumerURL	The URL where call quality reports will be posted. The URL must start with `http://` or `https://`	String	Null	Must be set to the CA `QMSReportConsumer` Web service method that will receive the report posts.
ConsumerName	The friendly name of the third-party monitor.	String	Null	Set to NetQoS.
ClientCertIssuer	The certificate authority that issued the certificate as a byte array. If MTLS is specified, this property must contain the fully qualified domain name of the certificate server. This value must be NULL for TCP connections, and can be not NULL for MTLS connections	unit8 []	Null	Needed for HTTPS support.

Name	Description	Type	Default	Notes
ClientCertSN	The serial number of the certificate as a byte array. Must be NULL for TCP connections. Cannot be NULL for MTLS connections.	unit8 []	Null	Needed for HTTPS support.
Enabled	Whether the MetricsReceiver is able to receive call quality reports from the endpoints.	Boolean	False	Set to `true` to enable OCS Collector functionality.
ErrorRetryEnabled	Whether the Microsoft server should retry when transient errors occur that prevent the sending of quality reports.	Boolean	True	We recommend the default.
MaxPostBatchSize	Maximum number of reports to send in one transaction (as a batch).	unit32	50	We recommend the default. Acceptable range is 5-100.
MaxQueueSize	The amount of memory that may be used to cache call quality reports that cannot immediately be sent to the consumer. Once the queue limit has been reached, the Microsoft server may discard reports.	unit32	50000 KB	We recommend the default.

An additional class is configured in the Office Communications Server 2007 R2 environment: the `MSFT_SIPLogSetting`.

Name	Description	Type	Default	Notes
EnableQMS	Whether the delivery of reports to an external consumer is allowed without a Monitoring Server.	Boolean	False	Set to `true` to enable the OCS Collector. This setting is exposed in the Office Communications Server R2 MMC in the Front End Properties via an **Enable QoE monitoring** check box on the **Monitoring** tab. The check box cannot be enabled in the MMC without associating a Monitoring Server. This WMI setting allows for an external consumer without the Monitoring Back-End Server association.

Removing the OCS Collector

The OCS Collector can easily be deleted if it is no longer required, or if you are changing something in the environment that requires a new setup.

First, follow the typical procedure for removing a Collector in a Distributed configuration:

1. In the navigation links, click **Administration > Data Collection > Collectors**.

   The Collection Device List page is displayed.
2. Click to select the OCS Collector in the list, and click **Delete**.
3. Click OK to confirm the deletion.

The Collector status might still appear as “Configured” at this point. But the act of deleting the Collector instructs the Microsoft server to discontinue posting call quality reports to the report consumer and to retain them in the local server database instead. If calls are active, you can run a command on the Management Console server to confirm that the Microsoft server is no longer sending report files:

```
dir d:\netqos\voipmonitor\datafiles\q*.xml /s /b
```

If no files are returned from this directory command, the Collector has been successfully deleted.

If you have used the `QMSConfig.exe` utility to configure the Collector on a remote server, clear the **Enabled** check box and also clear the address shown in the **Send reports to:** field. These additional steps ensure that WMI discards the settings.

Security in the Office Communications Server 2007 Environment

The endpoints and servers in the Microsoft Office Communications Server 2007 environment use encryption for signaling and media flows by default. The SIP flows used for call setup are encrypted using MTLS (specifically, Transport Layer Security with mutual authentication), and the RTP flows carrying audio and video data are encrypted using Secure RTP (SRTP).

The standard collection architecture for monitoring Cisco Unified Communications Manager environments does not support encrypted call setup flows. Call quality information can be posted in unencrypted format to the UC Monitor Web service and sent out to the Management Console, but because the Microsoft server acting as an OCS Collector and the Web service reside within the secured Active Directory domain of the associated Office Communications Server, they cannot receive any incoming communications from a client or server that lacks a certificate.

Depending on the security policies in use in your own environment, you may need to use HTTPS for communications between the Microsoft servers and Unified Communications Monitor. Or you might want to use an authentication scheme using certificates. The fully qualified domain name of a certificate server (certificate authority, or CA) and the serial number of the client certificate are required to enable mutual authentication using client-side certificates.

Note: The configuration of certificates and the use of HTTPS are **optional**.

Configuring Secure Communications

Certificate information is required if you plan to use HTTPS for encrypted communications between the Microsoft server acting as an OCS Collector and the UC Monitor Management Console. If you supply a certificate on the UC Monitor server or on both the UC Monitor server and the Microsoft server, communications between the two computers are encrypted.

Note: Authentication and encryption are **not** normally required for monitoring Microsoft Office Communications Server 2007 and later with Unified Communications Monitor.

Two modes of authentication and encryption are supported for these communications:

- **Single certificate authentication**. A single certificate is installed on the report recipient (the UC Monitor server). The HTTPS specification allows only the Microsoft server to authenticate the report recipient. Communications between them are encrypted.
- **Mutual certificate authentication**. Certificates are installed on both the Microsoft server and the UC Monitor server. With this setup, the Microsoft server must authenticate the report recipient, and the report recipient must also authenticate the Microsoft server. Communications between them are encrypted.

  This type of authentication provides the strongest possible security. However, mutual certificates require additional configuration. On the Microsoft server, not only must the certificate be installed, but also two additional WMI parameters must be set. The `MSFT_SIPQMSExternalConsumer.ClientCertIssuer` and `MSFT_SIPQMSExternalConsumer.ClientCertSN` parameters must be configured to match the values in the client-side certificate.

To configure single certificate authentication:

Take the following steps to use single certificate authentication on the UC Monitor report recipient:

1. Install a certificate on the UC Monitor Web site in Microsoft IIS.

   Microsoft provides several Knowledge Base articles that describe the procedure to install and configure the certificate in IIS. Refer to the following:

   http://support.microsoft.com/kb/299875

   http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/559bb9d5-0515-4397-83e0-c403c5ed86fe.mspx?mfr=true

   If your enterprise has its own certificate authority (CA) established that is trusted by the QoE Monitoring Server, use that CA to create the certificate. Otherwise, take the next step.
2. Verify that the Microsoft server trusts the root CA that issued the certificate you installed. In the MMC Certificates plugin, go to **Trusted Root Certification Authorities**. Verify that the CA that issued the report recipient certificate is listed.
3. If the Microsoft server does not trust the CA, use the MMC Certificates plugin to import the certificate into the list. Look for the **Trusted Root Certification Authorities** option.
4. Verify that the subject name of the UC Monitor report recipient certificate matches the FQDN of the report recipient URL configured on the Microsoft server.

   The domain name of the report recipient is set in the `ConsumerURL` WMI property. Make sure the hostname specified in the URL matches the subject name in the certificate.

The WMI parameters required to enable metric export from the Microsoft server are discussed above in "OCS Collector Remote Configuration" on page 50.

To configure mutual certificate authentication:

1. First, take the steps listed above to set up single certificate authentication.
2. Import the client certificate on the Microsoft server, and make sure the certificate is stored in the local computer store so that the server can locate the certificate.
3. Store the client certificate in the **Trusted Root Certification Authorities** folder. It must have the enhanced key usage (EKU) extension for client authentication.
4. The report consumer must be configured to trust the root CA that issued the client certificate. Store the root CA in the **Trusted Root Certification Authorities** folder under the local computer store.
5. Appropriate permissions must be granted to the `RTCComponentUniversalServices` domain group for the certificate to be read. This requires programmatic intervention. In our testing, we used a Microsoft tool, `winhttpcertcfg.exe`, to grant permissions.
6. Configure the certificate in Microsoft WMI on the Microsoft server. See "OCS Collector Remote Configuration" on page 50 for more information.

   Some special requirements apply to the WMI parameters:

   - The **Certificate Issuer Name** must be specified in ASN.1 byte array format. We created a C# utility that queried the certificate information and then set the value via WMI.
   - The **Certificate Serial Number** must be specified in reverse order from what is shown in the MMC Certificates plug-in.

In most environments, the report recipient (the UC Monitor Management Console) does not have to be part of the same domain as the Microsoft server.

Server-to-Management Console Communications and Firewalls

If any firewalls are active in your network, you might need to configure them to allow communications between the Microsoft server acting as an OCS Collector and the UC Monitor Management Console.

The QoE Monitoring Server or R2 Front-End server uses Port 80 to communicate with the UC Monitor report recipient Web service on the Management Console via HTTP. If you have configured HTTPS for communications between the Microsoft server and the UC Monitor server, it uses Port 443.

The only communications that take place from the Management Console to the Microsoft server occur when the OCS Collector is configured as a collection device. Usually, this is a one-time event, described in "Adding a Collection Device" on page 83. These communications begin by using Port 135, but because the processes use DCOM, the port selection may be dynamic. You may need to restrict the ports used by DCOM on the Management Console by editing some Registry keys. The following article from the Microsoft Developer Network provides more information:

http://msdn.microsoft.com/en-us/library/ms809327.aspx

If you think firewalls are causing issues with OCS Collector setup, see "Firewall Issues" on page 59.

OCS Collector Bandwidth Consumption

In our testing of Unified Communications Monitor with Office Communications Server 2007 and R2 servers, we took some measurements of quality report size and volume to derive some guidelines about bandwidth consumption for the OCS Collector. When the Microsoft QoE Monitoring Server or the Front-End servers (in the R2 system) send quality reports in batches to the report recipient Web service on the UC Monitor Management Console, the bandwidth consumption is roughly as follows:

- **Audio calls**: 3500 bytes per report, or 7000 bytes per call
- **Audio + Video calls**: 5300 bytes per report, or 10,600 bytes per call

The Microsoft capacity planning guidelines identify 125 reports/second as the limit for a single QoE Monitoring Server. This represents call traffic from over 125,000 users. With this benchmark, the bandwidth consumption would be:

Audio calls:

```
125 reports/sec * 3500 bytes/report = 437500 bytes/sec = 3500 kbps = 3.5 Mbps.
```

Audio + video calls:

```
125 reports/sec * 5300 bytes/report = 662500 bytes/sec = 5300 kbps = 5.3 Mbps
```

The baseline of 125 reports/sec equates to a call volume of over 220,000 calls per hour. A more likely enterprise benchmark that we have observed in our testing is probably more like 22,000 calls per hour:

Audio calls:

```
12.5 reports/sec * 3500 bytes/report = 43750 bytes/sec = 350 kbps
```

Audio + video calls:

```
12.5 reports/sec * 5300 bytes/report = 66250 bytes/sec = 530 kbps
```

Troubleshooting Tips

When you add the OCS Collector in an Office Communications Server environment where calls are running, the OCS Collector should start receiving data from the Microsoft server within minutes. You can confirm that the OCS Collector is operational in the Administration pages of the UC Monitor Management Console by clicking **Administration > Data Collection > Collectors**. The Collection Device List should have an entry for the OCS Collector. Check the **Last Collection** time, which shows whether reports have been sent.

Note: The **Collector Status** column does not apply to this collection device type.

If, after 15 minutes, the Last Collection still shows a blank, you'll need to check your configuration and confirm that the Microsoft server is sending data to the correct recipient. The following topics list possible issues to address. And if you suspect that a reboot is needed, try some of the suggested tasks in "No OCS Collector Status" on page 61 before you disrupt your system unnecessarily.

Inadequate Windows Administrative Privileges

A lack of the required login privileges is by far the most common reason for problems in setting up monitoring in a Microsoft OCS environment. When you add the OCS Collector, the Windows user account that you use to log in must have adequate permissions in the domain to both **edit** the required WMI variables and **retrieve** those settings for display in the UC Monitor Management Console (where they can be verified or edited).

In order to successfully configure the OCS Collector and retrieve the settings, your login account needs *both* Domain User and Local Administrator privileges on the computer where you are performing the Add Collection Device task (where you are accessing the Management Console).

Note: Members of the RTCUniversalServerAdmins group, an Office Communications Server security group whose members can manage all aspects of Office Communications Server within the Active Directory forest, including all server roles and users, can retrieve settings on the Microsoft server but cannot save them to the UC Monitor database.

Microsoft Server Not Enabled for Quality Reporting

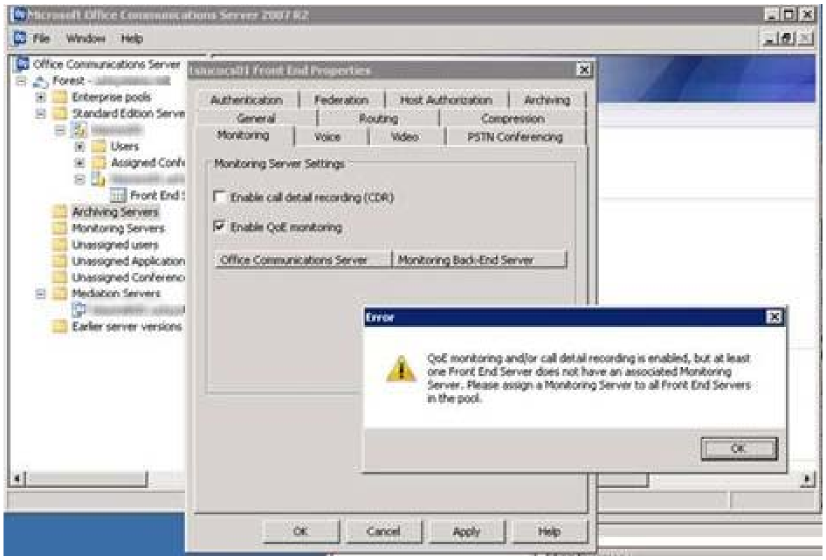
Check to make sure the Microsoft server that will act as an OCS Collector is actually configured to receive reports from the endpoints in the Office Communications Server system. The section titled "Preparing the Front-End Server (R2 Only)" on page 46 describes some of the requirements that are not included on the Microsoft server by default.

On the Microsoft QoE Monitoring Server or Front-End server, launch the MMC Admin plug-in from the Administrative Tools. Check the **Associations** section. Make sure the **OCS Pool** and **Mediation Server** are associated with the QoE Monitoring Server or Front-End server. If not, neither endpoints in the pool nor the Mediation Server will send reports to the OCS Collector, which in turn will not send them to the Management Console.

To make sure the Microsoft server is receiving the required quality reports from the endpoints, check to see whether it has stored any reports. The QoE Monitoring Server or Front-End server stores any reports it receives in the local SQL database. Launch SQL Tools, and browse the `QoEMetrics` database. You should see rows in the `AudioStream` table if the server is receiving reports.

Microsoft Error Message about Monitoring Server (R2 Only)

This problem is actually a confusing symptom of the previous problem we have described. A Microsoft “Monitoring” (or “Back-End”) Server associated with the Front-End server(s) you are setting up as OCS Collectors is not required to enable Unified Communications Monitor collection: the UC Monitor system can work with or without the Back-End Monitoring Server. The Microsoft Office Communications Server Admin interface displays an error message whenever a third-party consumer is configured to receive quality reports without a Microsoft Back-End Monitoring Server. This message instructs you to “assign a Monitoring Server to all Front-End Servers in the pool,” but when you try to do so, no server is available in the **Monitoring Back-End Server** list. Here is an image of the error message:



☐ Enable call detail recording (CDR)

☑ Enable QoE monitoring

QoE monitoring and/or call detail recording is enabled, but at least one Front End Server does not have an associated Monitoring Server. Please assign a Monitoring Server to all Front End Servers in the pool.

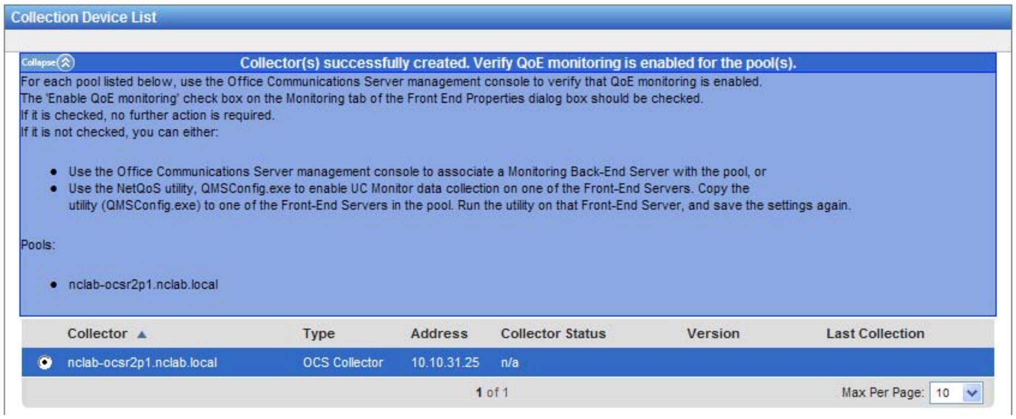
If you see this error, click **OK** in the error dialog box, and then click either **Apply** or **Cancel** in the Properties dialog box to ignore it.

Failure to Configure OCS Collector (R2 Only)

In an Office Communications Server 2007 R2 environment, the Front-End server acts as an OCS Collector. And if you are running Enterprise Edition, separate servers house the Front-End components (which send the quality reports) and their Back-End database servers. In some cases, this usage of separate servers—a supported Microsoft configuration—causes authentication issues when you create OCS Collectors.

Usually, most of the servers you selected can be successfully configured, but if an extra hop is required to reach the Back-End servers, the UC Monitor Management Console cannot be authenticated using the credentials you supplied. Some of the required settings changes are prevented on these servers.

In a typical case, you might see both the Front-End and Back-End servers in the list of servers eligible to act as OCS Collectors. You might then select all of them and click **Save** to create OCS Collectors. A success message would appear to indicate that the OCS Collectors were configured; however, a message on the Collector List page states that you need to verify that QoE Monitoring is enabled by checking the status of the **Enable QoE Monitoring** check box in the Front End Properties dialog box.



Collector(s) successfully created. Verify QoE monitoring is enabled for the pool(s).

For each pool listed below, use the Office Communications Server management console to verify that QoE monitoring is enabled.
The 'Enable QoE monitoring' check box on the Monitoring tab of the Front End Properties dialog box should be checked.
If it is checked, no further action is required.
If it is not checked, you can either:

- Use the Office Communications Server management console to associate a Monitoring Back-End Server with the pool, or
- Use the NetQoS utility, QMSConfig.exe to enable UC Monitor data collection on one of the Front-End Servers. Copy the utility (QMSConfig.exe) to one of the Front-End Servers in the pool. Run the utility on that Front-End Server, and save the settings again.

Pools:

- nclab-ocsr2p1.nclab.local

	Collector ▲	Type	Address	Collector Status	Version	Last Collection
◉	nclab-ocsr2p1.nclab.local	OCS Collector	10.10.31.25	n/a		

1 of 1 Max Per Page: 10

Pay careful attention to this message. Even if collection begins and you start to see report data from some Microsoft servers, other data is not being collected. Take the steps provided in "To prepare the Front-End server pool:" on page 48 to check the status of QoE Monitoring on each server in the pool.

Firewall Issues

If any firewalls are active in your network, you might need to configure them to allow communications between the Microsoft server acting as an OCS Collector and the UC Monitor Management Console.

The Microsoft server uses **Port 80** to communicate with the report recipient Web service on the UC Monitor Management Console via HTTP. Or, if you have configured HTTPS for communications between the Microsoft server and the Management Console, it uses **Port 443**.

The only communications that take place from the Management Console to the Microsoft server occur when the OCS Collector is configured as a collection device. Usually, this is a one-time event that occurs automatically when you add the new OCS Collector. These communications begin by using **Port 135**; however, the port selection may be dynamic. See "Server-to-Management Console Communications and Firewalls" on page 55 for more information.

If you think that a firewall might be causing an issue, test the connectivity between the Unified Communications Monitor server and the Microsoft server acting as an OCS Collector. After you add the OCS Collector using the Management Console or by running the QMSConfig executable, you should see the URL for the report Web service displayed. On the Microsoft server, launch a Web browser. Enter the URL in the address field and try to connect to it where it is running on the UC Monitor Management Console. This connection simulates what happens when the Microsoft server forwards a quality report to the UC Monitor Management Console. If you see a Web page that says OK, you have confirmed no firewall is blocking HTTP from the OCS server to the Management Console.

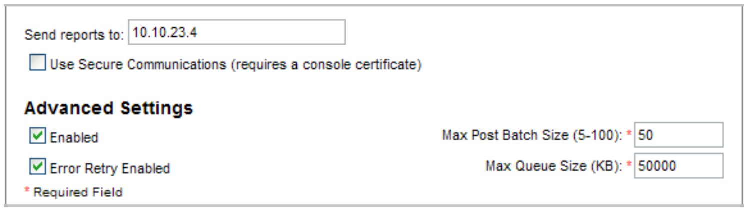
In a few cases, issues related to firewalls or similar security measures may affect the metrics that are collected and reported. For example, Unified Communications Monitor may not be able to find the address of the endpoint that sent the call quality report if an intervening HTTP proxy is active; all traffic forwarded by the proxy may be associated with a single “call server” with the IP address of the proxy. As a best practice, make sure that all HTTP traffic from the Microsoft servers acting as OCS Collectors is sent directly to the UC Monitor Management Console, or is sent through a firewall that is not using an HTTP proxy server.

Server or OCS Collector Not Enabled

It is possible to add and save a new OCS Collector and then specify that it should not send reports. The **Enabled** setting instructs the Microsoft server acting as an OCS Collector to begin sending reports to the UC Monitor Web service.

To check whether the OCS Collector is enabled:

1. In the UC Monitor Management Console, click **Administration > Data Collection > Collectors**.
2. In the Collection Device List, click to select the OCS Collector, and click **Edit**.
3. Supply the required username and password to retrieve settings from the Microsoft server.
4. Click **Retrieve Settings**.
5. In the Collector Properties Advanced Settings, check to make sure the **Enabled** check box is selected:



Send reports to: 10.10.23.4

□ Use Secure Communications (requires a console certificate)

Advanced Settings

☑ Enabled — Max Post Batch Size (5-100): * 50

☑ Error Retry Enabled — Max Queue Size (KB): * 50000

* Required Field

6. If you are not certain that you have the required server certificate installed, make sure the option to **Use Secure Communications** is cleared.

You can also use the OCS Collector Configuration Utility to check these settings. See “OCS Collector Remote Configuration” on page 50 for more information about this utility.

No OCS Collector Status

After you add the OCS Collector, the Collection Device Properties page should say that settings have been loaded successfully, and that the server status is "Configured." However, when you check the Collection Device List page for Collector status, it might show "n/a" for the status and a blank space for the Last Collection time. The "n/a" designation is no cause for concern, reflecting the lack of a connection from the Management Console to the OCS Collector.

However, the lack of a Last Collection time indicates that no reports have yet been received from the Collector. If calls are active, you need to run a command on the Management Console server to check for Microsoft Office Communications Server report files:

```
dir d:\netqos\voipmonitor\datafiles\q*.xml /s /b
```

If no files are returned from this directory command, you need to restart some services. Try each of the following strategies, listed in order from least disruptive to most disruptive to your OCS unified communications system:

- Restart the QoE Monitoring Agent Service on the Front-End server (or on all Front-End servers in an Enterprise Edition pool).
- Restart the OCS services on the Front-End server(s).
- Restart the Microsoft servers themselves (any servers that you have configured as OCS Collectors).

After you try each of the above tasks, wait 15 minutes and run the directory command again to check for `q*.xml` files, which are sent if calls are active.

Post-Installation Tips

The chapter titled "Setting Up the Management Console" contains instructions for configuring the UC Monitor Management Console and OCS Collector. You'll need to take a few steps to establish communication between these components.

You'll also need to take the same steps to set up Location definitions as you would for a Cisco monitoring deployment. The Quality of Experience Monitoring Server supports Location definitions to help you identify endpoints based on their subnets. If you have these definitions on your server, you should plan to import a list of these definitions in `.csv` format into the UC Monitor Management Console so that the Locations used in UC Monitor reports are identical. See "About UC Monitor Locations" on page 104 for more information.

Once the UC Monitor system is up and running, be sure to follow the guidelines provided in Chapter 9, "Managing the Database" on page 209 to ensure database integrity and performance. Specifically, you need to:

- Schedule and run regular defragmentation operations on the hard disk drive where the UC Monitor database is installed. See "Hard Drive Maintenance" on page 221 for more information.
- Schedule and run regular database backup operations. See "Backing Up and Restoring the UC Monitor Database" on page 217 for more information.

Requirements for Grouping Support

If you plan to take advantage of UC Monitor support for custom grouping of devices and Locations to help you organize reporting and user permissions, you must have an instance of the NetQoS Performance Center running in your environment. Groups can only be created, modified, and assigned to user accounts in the NetQoS Performance Center. Version 4.0 or later is required for integration with Unified Communications Monitor.

See Appendix A, "Working with Groups in the CA NetQoS Performance Center" on page 241 for a full discussion of the grouping feature.

CHAPTER 4

Preparing to Monitor Avaya

In addition to Cisco and Microsoft, CA NetQoS Unified Communications Monitor monitors UC deployments that rely on the Avaya Communication Manager for call processing. The UC Monitor Collector that monitors Cisco UC systems also monitors voice calls made using Avaya components, including desk phones and softphones, the Communication Manager (including Aura Communication Manager), and Avaya voice gateways. Both multi-vendor and single-vendor systems are supported.

To monitor in an Avaya environment, you will need to change some configuration parameters on the Avaya Communication Manager. This chapter discusses the required setup tasks. It covers the following topics:

- “Avaya UC System Architecture” on page 64
- “UC Monitor Architecture for Avaya Deployments” on page 65
- “Preparing the Avaya Environment” on page 68

Avaya UC System Architecture

For Avaya, unified communications is a means, not an end. They see UC as an enabling set of technologies, or a kind of "portal to the Intelligent Communications space." Their Web site defines unified communications as "the convergence of real-time and non-real-time business communication applications," adding that when it has been configured correctly, "UC provides a superior, seamless user experience across all enterprise communication solutions regardless of location, network, or device."

Avaya UC solutions are designed to operate in a vendor-neutral, cross-platform environment. They rely on the SIP protocol to allow users to run communications applications on devices manufactured by Avaya as well as by competitors (including Cisco and Microsoft). The Avaya Aura architecture treats UC as an application that can be managed from a few central locations, rather than as a network of many individual hardware devices requiring management and configuration (as in the old PBX-centric architecture). SIP creates a common communication layer to link all the disparate communications systems together, allowing each user to access the system from anywhere by means of a single profile.

The following topic describes each component involved in UC Monitor support for monitoring Avaya unified communications.

Avaya Hardware and Software

The Avaya UC environment comprises several component devices:

- **Communication Manager**: A Linux-based server that fills the role of the call server for purposes of UC Monitor reports. It provides call processing and routing functionality. Later versions are called Avaya Aura™ Communication Manager (CM).
- **SIP Enablement Services Server (SES)**: A Linux-based server that provides SIP proxy functions to SIP-enabled endpoints. SES is required for all SIP endpoints.
- **Media Gateways**: Media devices that provide connectivity to the PSTN, and that terminate RTP streams from IP-enabled endpoints making PSTN calls.
- **IP phones**: Devices (both "hard" and "soft") that both make calls and report on the call quality. The "one-X" (or "one experience") brand name is often used to refer to both Avaya softphones and desk phones. More traditional analog phones, IP desk phones, and softphones are treated as "complementary" technologies in the Avaya system and can be monitored with Unified Communications Monitor as long as they are capable of sending RTCP call-quality data. The one-X Communicator application provides features such as user presence, voice mail, conferencing, and video and can interoperate with the Microsoft Office Communicator application for instant messaging.

The Communication Manager does not resemble a classic call server in the sense that Cisco UCM is called such. Unified Communications Monitor discovers call servers from monitored call data and uses that information to report on call server performance. In the case of the Avaya CM, call server identification also allows the Collector to find information to identify endpoints and trunk groups. Call server discovery is complicated in an Avaya deployment; you are likely to find that only the

C-LAN board and the MedPro have been identified in the Call Server List, and not the call server itself. We strongly recommend checking the Call Server List to make sure all CM servers are correctly identified, and adding any CM server IP addresses that are not included in the list.

The UC Monitor Release Notes contain up-to-date information about call server, media server, and endpoint device support. They are available in PDF format on the CA Support Online Web site.

UC Monitor Architecture for Avaya Deployments

As explained in "Planning for Hardware Requirements" on page 14, CA NetQoS Unified Communications Monitor consists of two major software and hardware components: the Collector and the Management Console. As with a Cisco monitoring deployment, both the Management Console and Collector components are required for monitoring in an Avaya UC environment.

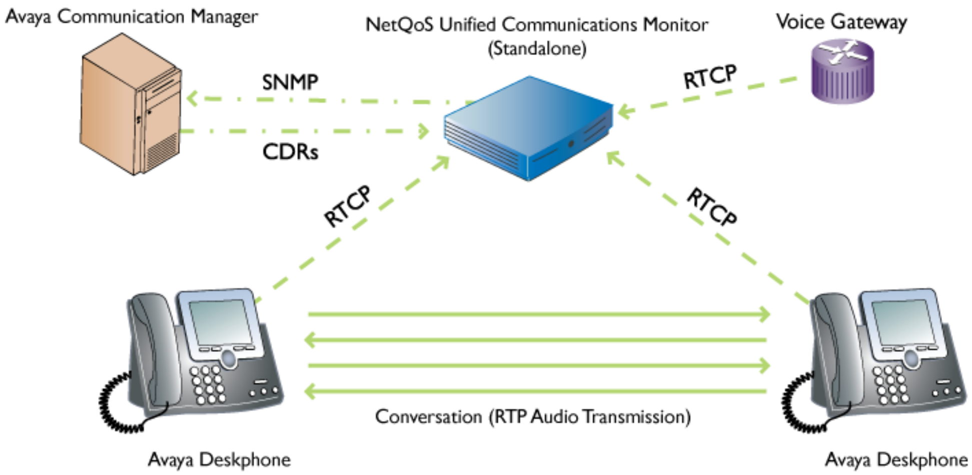
Where in a Cisco deployment Unified Communications Monitor receives VoIP-related data from a switch SPAN port, for Avaya, the Collector leverages data that is reported by the Avaya endpoints. Many Avaya IP phones and voice gateways use the RTCP protocol to send frequent call-quality packets.

The streaming-media protocol RTCP, which stands for the Real-Time Transport Control Protocol, is a standards-based method of communicating quality information for an RTP media stream containing voice or video data. In the Avaya system, RTCP data is sent between the phones and gateways during an active call. When the requisite Communication Manager settings are enabled, the endpoints will also send RTCP packets to a designated monitoring server, called the *RTCP Monitor*. In the past, Avaya provided a server for this purpose, but they now rely on third parties, such as CA, to collect the RTCP call-quality data and format it in reports.

Supported UC Monitor Configurations

To monitor a system using the Avaya (Aura) Communication Manager, the UC Monitor Collector component must have network connectivity to the network(s) where Avaya endpoints and phones are making calls. The endpoints will be sending data directly to a Web service on the Collector.

Here's an illustration of a UC Monitor server in the **Standalone** configuration, monitoring in an Avaya-only environment:


Avaya Communication Manager
NetQoS Unified Communications Monitor (Standalone)
Voice Gateway
SNMP
CDRs
RTCP
RTCP
RTCP
Conversation (RTP Audio Transmission)
Avaya Deskphone
Avaya Deskphone

Avaya endpoints, including voice gateways, send frequent call-quality reports directly to the UC Monitor Collector while calls are in progress. The quality data is sent as RTCP packets. Using SNMP, the Collector periodically polls the Communication Manager for device information. And the Communication Manager sends CDR data to the Collector after each call completes.

A Standalone system is capable of monitoring an Avaya-Cisco hybrid unified communications environment. A switch SPAN session is still required to enable Cisco monitoring in such an environment.

To monitor an Avaya-Microsoft hybrid deployment, a **Distributed** UC Monitor configuration is recommended. Typically, the Collector component on the standalone device is disabled when Microsoft components are monitored. With the Distributed UC Monitor architecture, at least two computers are used: one for the Collector (in this case, to monitor Avaya), and one for the Management Console. The Distributed architecture is also recommended for larger Avaya-only deployments. The Distributed Collector is then configured as the quality report recipient for the phones and endpoints registered to the Avaya Communication Manager.

In large or growing UC systems, the Distributed architecture allows for flexibility because Collector licenses can be upgraded to support more IP phones or endpoints.

Bandwidth Requirements

Call volume is the key metric to consider when determining the scale of any UC Monitor deployment, regardless of the equipment being monitored. In the case of Avaya, call volume affects not only UC Monitor database size and growth and Collector load, but also bandwidth usage, as two different types of endpoint send quality data to the Collector. However, our testing indicates that the amount of additional bandwidth used is negligible.

The following breakdown is based on our testing and should provide a range that includes the approximate usage in your environment.

In an Avaya UC system, the average RTCP packet size is 250 bytes, which includes Ethernet and UDP headers. By default, the Avaya endpoints (the phones and voice gateways) send RTCP call-quality reports at 5-second intervals, which amounts to 12 packets sent per call minute, per endpoint. With two different devices sending reports, you could see 2 x 12 = 24 packets sent per call minute. With 24 packets per minute at 250 bytes each, network traffic from Avaya endpoints to the Collector reaches approximately 6000 bytes per minute, or .0977 Kbps (or equally, 100 bytes per second, per call minute, which is .0000954 MBps per call minute).

The endpoints throttle the number report packets sent if they encounter congestion by increasing the 5-second interval. We recommend increasing the interval to 10 seconds and using the class-default queue for the RTCP traffic to prevent congestion on WAN links.

The following table provides a further illustration of bandwidth usage (in Kilobytes per second) based on the number of simultaneous calls and the average duration of each call, in number of minutes:

	Average Call Duration (in minutes)			
Busy-Hour Calls	**2**	**3**	**4**	**5**
1000	0.19 MBps	0.29 MBps	0.38 MBps	0.48 MBps
5000	0.95 MBps	1.43 MBps	1.91 MBps	2.38 MBps
10000	1.91 MBps	2.86 MBps	3.81 MBps	4.77 MBps
20000	3.81 MBps	5.72 MBps	7.63 MBps	9.54 MBps
50000	9.54 MBps	14.3 MBps	19.1 MBps	23.8 MBps
100000	19.1 MBps	28.6 MBps	38.1 MBps	47.7 MBps

If the network where the Avaya endpoints are running is too busy, the devices themselves begin to throttle the number of RTCP packets sent by increasing the interval between packets. As a result, even at 100,000 simultaneous calls of an average length of 5 minutes, the network traffic generated by these call quality reporting flows will only be around 815 Kilobytes/second. This level of bandwidth usage is significantly less than the amount of traffic generated by a simple Web browser request to access a popular page on the World Wide Web.

The call data records (CDRs) sent from the Avaya Communication Manager to the Collector are 155 bytes per call, and only one CDR is sent for each call, containing information for both directions of call data flow. CDR-related traffic is further reduced by the recommendation to install the Collector (usually a UC Monitor Standalone server) near the Communication Manager.

Preparing the Avaya Environment

A few steps are required to enable Avaya phones and endpoints to send quality data to the UC Monitor Collector. The main tasks are related to SNMP polling access, RTCP routing, security, and call data record (CDR) collection and transmission.

The Communication Manager provides information about relevant devices, such as phones, call servers, and voice gateways, and also determines phone behavior related to the sending of RTCP packets containing the call-performance metrics that are used in UC Monitor reports. By default, the Avaya endpoints do not send this data and must be instructed to do so in order to enable monitoring with Unified Communications Monitor. The required parameters can be set globally or for each IP network region.

The topics in this section explain how to enable data collection from the Avaya system. The first step is to enable SNMP access to MIB data on the Communication Manager. See "Enabling SNMP Access" on page 69 for instructions. Next, the section titled "RTCP Monitor Configuration" on page 70 walks you through the necessary steps to define the UC Monitor collection device for your Avaya endpoints. You should check and, if necessary, change settings for the Communication Manager firewall to allow SNMP data to pass. See "Avaya Firewall Settings" on page 71.

You must add the UC Monitor Collector as an "IP node" so that it can receive CDRs from the Communication Manager. CDRs enable the collection of additional metrics from Avaya endpoints. See "Enabling CDR Collection" on page 72. And as a final step, you need to enable trunk group monitoring; see "Enabling Trunk Group Monitoring" on page 74.

Communication Manager Configuration: Overview

The Collector needs to be able to poll the call servers for endpoint data and also receive RTCP call-quality information from the Avaya endpoints. To enable monitoring, the SNMP agent on the server needs to allow read-only access, and the Avaya endpoints need to send RTCP packets to the Collector.

To enable monitoring with CA NetQoS Unified Communications Monitor, you must:

- Enable SNMP access for the Communication Server SNMP agents
- Set RTCP parameters at the Communication Manager
- Enable each IP network region for RTCP reporting
- If necessary, change settings in the Communication Manager firewall to allow SNMP traffic
- Set the necessary parameters on the Communication Manager to allow it to send CDRs to the Collector.
- Enable trunk group monitoring by adding trunk groups to a list.

SNMP access is required to allow the Collector to poll the Communication Manager for device information and discover the Communication Manager servers. The necessary steps are described in the following topic.

The endpoints send call-quality data to their "RTCP Monitor," essentially an IP address and port reserved for this purpose. Therefore, Collector addressing information needs to be supplied for the RTCP Monitor settings.

In a large-scale Avaya UC deployment, different IP network regions may report quality reports to different UC Monitor Collectors. For this configuration, the Distributed collection architecture is required, with at least two servers hosting Collectors. The Avaya Communication Manager configuration allows for RTCP monitoring server configuration at the IP network region level. The necessary steps to take are provided in "RTCP Monitor Configuration" on page 70.

Your Communication Managers might already be set up to send CDRs to a billing application. In such a case, the Collector needs to be configured as the recipient of "Secondary" CDR output. The steps are provided in "Enabling CDR Collection" on page 72.

Enabling SNMP Access

The UC Monitor Collector needs to be able to poll the Avaya Communication Manager for certain records that it maintains in a MIB to track active UC devices and servers. The Communication Manager provides some administrative settings in the Server Maintenance area that affect SNMP access to the server MIB. You will need to log into the Communication Manager Administration interface to make sure the SNMP agents are enabled for SNMP access. If necessary, you will need to place the Master Agent in a Down state and then change several settings to enable read-only polling access. The steps to take are provided below.

If you have already enabled read-only access to the SNMP Master Agent on the Communication Manager, you can skip to the next topic. You will still need to make sure that an SNMP profile is configured on the UC Monitor Management Console with the community string and SNMP version of the Communication Manager. Those steps are detailed in "Working with SNMP Profiles" on page 234.

To enable SNMP agents for read-only polling access:

1. In a Web browser, access the Avaya Communication Manager Web interface. Enter `https://<IP Address of Avaya Communication Manager>` to access the login page.
2. Log into the server using an account with Administrator credentials.
3. On the System Management Interface page, click **Administration > Server Maintenance**.
4. In the **Alarms** section, click **SNMP Agents**.

   The SNMP Agents page is displayed.
5. If SNMP access is not currently enabled, click **Agent Status** in the **Alarms** section and place the Master Agent in a Down state. This step is necessary before you make any changes to agent configuration.

   When you've changed the agent state so that it is no longer running, return to the SNMP Agents page.
6. Under **IP Addresses for SNMP Access**, click to enable **Any IP address**.
7. Scroll down to the **SNMP Users/Communities** section.
8. Click the check box to enable either **SNMP Version 2c** or **SNMP Version 3** (or both).
   - For SNMP version 2c, supply the appropriate **Community Name** for read-only access.
   - For SNMP version 3, in the **User (read-only)** section, supply a valid username for the **User Name**, and supply either an **Authentication Password** or a **Privacy Password**.

9. Click **Submit**.
10. Return to the Agent Status Administration page, and restore the Master Agent to the Up state.

The Collector will start polling the call server using the security information in the Default SNMP Profile, which is configured in the **Administration > Security > SNMP Profiles** section of the UC Monitor Management Console. If the default profile does not contain the correct SNMP community or SNMP v3 secure username and password for the Communication Manager, the Collector proceeds down its list of profiles and tries each in turn. You therefore need to verify that an SNMP profile with the correct information for your Communication Manager is present on the Management Console. See "Viewing the SNMP Profile List" on page 235 to get started.

RTCP Monitor Configuration

Setting up the Unified Communications Monitor system to monitor Avaya requires a few steps to instruct the Avaya endpoints to send RTCP call-quality data to the Collector, which takes the role of the RTCP Monitor in the Avaya system.

The RTCP Monitor server for Avaya endpoints is configured at the Communication Manager, either globally or per IP network region. The global system setting for the routing of RTCP packets is configured via the `system-parameters ip-options` command in the Avaya (Aura) Communication Manager. To see the current settings, use the following command:

```
display system-parameters ip-options
```

The Avaya documentation describes the steps required to enable RTCP reporting. We have also provided them here. Once reporting is enabled, you must then supply the Communication Manager with the IP address of the Collector, which takes the role of the RTCP Monitor server. The steps are repeated for each Avaya Communication Manager server.

The following method of configuring the Avaya system to send RTCP quality reports to the Collector is suitable for an environment in which multiple IP network regions are defined. The first several steps explain how to configure global RTCP report settings that apply to all IP network regions.

To enable RTCP reporting for each IP network region:

1. In a Web browser, access the login page of the Communication Manager.
2. Log into the server using an account with Administrator credentials.
3. On the main page, click the link to **Launch Native Configuration Manager**.

   The Native Configuration Manager page is displayed.
4. In the **Command** field, enter the following command:

   ```
   change system-parameters ip-options
   ```
5. Tab to the **RTCP MONITOR SERVER** section.
6. Set the **Default Server IP Address** to the IP address of the Collector Management NIC.

   To check the Management address, in the UC Monitor Management Console, click **Administration > Data Collection > Collectors**. Select the Collector in the list, and click **Edit**. The **Address** is shown on the Collection Device Properties page.
7. Set the **Default Server Port** to `5005`.

8. Set the **Default RTCP Report Period (secs)** to `5`.
9. Save your settings.
10. In the **Command** field, enter:

    ```
    change ip-network-region N
    ```

    where *N* is the number of the IP network region to be monitored.
11. Tab to the **RTCP Reporting Enabled?** field, and set it to `y`.
12. Tab to the **Use Default Server Parameters?** field, and set it to `y`.

    This value means that the phones in this IP network region will use the same parameters you set in Steps 6 - 8. If you want to use different Collectors for selected IP network regions, set this field to **`n`** for any region where you need to configure a different Collector IP address.

    Note: Only one RTCP Monitor Server can be configured per IP network region.
13. Save your settings.
14. Repeat Steps 10 - 13 for each IP network region that you want to monitor with Unified Communications Monitor.

Avaya Firewall Settings

The Avaya Communication Manager runs its own firewall, which you can manage in the Administration Web interface. If it is not already allowing SNMP flows to pass between points on the network and the Communication Manager, you need to update the settings on the Firewall page to allow the Collector to poll it for device information.

To configure the Avaya Communication Manager firewall:

1. In a Web browser, access the login page of the Communication Manager.
2. Log into the server using an account with Administrator privileges.
3. On the System Management Interface page, click **Administration > Server Maintenance**.
4. In the left pane, scroll down to the **Security** section, and click **Firewalls**.

   The Firewalls page is displayed.
5. In the **Service** column, find **snmp**.
6. Click to select the check boxes in both the **Input to Server** and **Output from Server** columns.
7. Click **Submit**.

In addition, if other firewalls are active in your network, you might need to configure them to allow communications—specifically, the RTCP packets—to pass between the Avaya endpoints and the UC Monitor Collector.

To allow RTCP data to pass, you must also allow UDP data on the same ports because RTCP uses UDP for transport. By default, the Collector listens on the following ports:

- **Port 5005**: RTCP data from the endpoints
- **Port 9000**: CDR data (TCP) from the Communication Manager

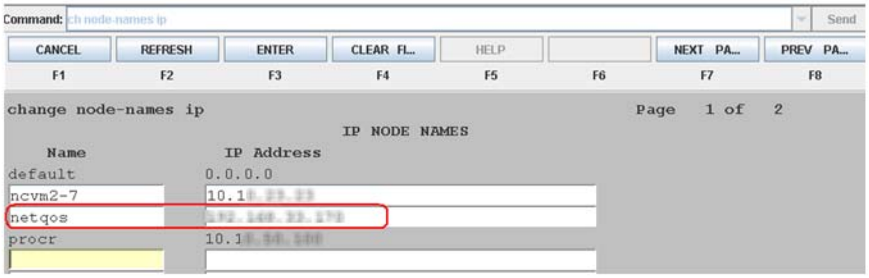
A final, optional firewall setting allows the Collector to send SNMP traps (as Incident notifications) to a trap receiver: UDP on Port 162.

Enabling CDR Collection

By default, the Avaya Communication Manager does not provide information about call direction or voice gateway dialed numbers, nor is this information included in the RTCP call-quality reporting performed by the phones and endpoints. To include this information in your reports, you must enable CDR monitoring by supplying information at the Communication Manager instructing it to send CDR reports at the end of each call to the UC Monitor Collector. If you do not enable CDR collection, information that identifies the direction of each call leg and any PSTN numbers involved in calls is not available in reports.

To configure the Collector as a CDR recipient:

1. In a Web browser, log into the Communication Manager System Access Terminal (SAT) using an account with Administrator credentials.
2. Use the `change node-names ip` command to associate the IP address of the UC Monitor Collector to a node name.



```
change node-names ip                                    Page   1 of   2
                                 IP NODE NAMES
    Name              IP Address
default               0.0.0.0
ncvm2-7               10.1[redacted]
netqos                [redacted]
procr                 10.1[redacted]
```

For this example, the node name **netqos** was assigned to IP address **192.168.33.170**.

Also make a note of the node name that represents the IP address of the source of the CDR data.

For S8300 servers (shown in the above example), the default node name is `procr`; for S8700 or S8500 servers, the node name can be `clan1` or `clan2`.

3. Use the `change ip-services` command to define the CDR link between the Avaya Communication Manager and the Collector.
4. In the **Service Type** field, enter `CDR1` for the primary CDR link.
5. In the **Local Node** field, enter the node name that will terminate the CDR link on the Avaya Communication Manager. (This will either be `procr` or `clan1,` as discussed above.)
6. Set the **Remote Node** field to the node name defined in the previous step for the Collector. The **Remote Port** may be set to a value between 5000 and 64500 (inclusive), but it must match the port being used by the Collector, which is `9000` by default.
7. Disable the use of the Avaya Reliable Session Protocol (RSP) for CDR transmission; make sure the **Reliable Protocol?** field is set to n.
8. Use the `change system-parameters cdr` command to set the parameters and the format of the CDR data.

9. Set the **Primary Output Format** field to `unformatted` and the **Primary Output Endpoint** field to `CDR1`.

   Or, if the Collector will act as the second of two CDR recipients, set the **Secondary Output Format** field to `unformatted`, and enter `CDR2` for the **Secondary Output Endpoint** field.

10. Verify that the following fields are set to the values shown (these should be the defaults):

Field	Setting	Description
Use Legacy CDR Formats?	y	Allows support for 3.x systems.
Intra-switch CDR?	y	Allows call records for internal calls involving specific stations.
Record Outgoing Calls Only?	n	Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.
Outg Trk Call Splitting?	y	Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.
Suppress CDR for Ineffective Call Attempts?	n	Prevents calls that are blocked from appearing in the CDR record.
Inc Trk Call Splitting?	y	Allows a separate call record for any portion of an incoming call that is transferred or conferenced.

   Default values may be used for all other fields.

11. If the **Intra-switch CDR** field is set to `y` on the CDR System Parameters page, use the `change intra-switch-cdr` command to define the extensions for call detail record collection.

12. In the **Assigned Members** field, enter specific extensions whose usage will be tracked with a CDR record. Add an entry for each extension of interest.

    Note: Avaya provides a utility to help you perform large-scale configuration changes for multiple extensions; contact your Avaya account representative and request a license for the Intra-Switch CDR by COS feature.

13. For each trunk group whose CDR records you want to monitor, verify that CDR reporting is enabled by using the following command:

    ```
    change trunk-group n
    ```

    where `n` is the trunk group number.

14. Verify that the **CDR Reports** field is set to `y`. This applies to all trunk group types.

By default, the Collector listens for CDR data as incoming TCP flows on **Port 9000**. In the Collection Device Properties, this field is labeled **CDR Monitor Port**. If you need to change this setting, click **Administration > Data Collection > Collectors**, select the Collector from the list, and click **Edit**. See "Collection Device Properties" on page 88 for more information.

Enabling Trunk Group Monitoring

Avaya trunk group monitoring requires some extra configuration at the Communication Manager. The Communication Manager needs to be instructed to collect the necessary data from specific trunk groups. Therefore, all trunk groups that you want to monitor must be listed in the Trunk Group Measurement Selection form in the Communication Manager.

Each time you add a new trunk group, you will also need to update this form to include it.

To specify trunks to monitor for Trunk Group reporting:

1. In a Web browser, access the login page of the Communication Manager.
2. Log into the server using an account with Administrator credentials.
3. On the main page, click the link to **Launch Native Configuration Manager**.

   The Native Configuration Manager page is displayed.
4. In the **Command** field, enter the following command:

   ```
   change meas-selection trunk-group
   ```

   The Trunk Group Measurement Selection page appears. This page lets you specify trunk groups to be monitored.
5. Check the Summary Report, which lists all administered trunks, to verify the trunk groups that you want to monitor.
6. Check to see whether particular trunk group numbers are listed.
7. If they are not listed, add the trunk group numbers of trunk groups to be monitored by Unified Communications Monitor by typing them in the empty fields.

   Note: Trunk group numbers do not have to be in numerical order.

   (*Optional*) You can also replace an existing trunk group number that you no longer need to monitor.

   - Press **Enter** until the cursor is positioned on the unwanted trunk group number.
   - Click **CLEAR FIELD**, and enter a new trunk group number.

Next Steps

Once you've prepared the Avaya environment for monitoring with Unified Communications Monitor, make sure the UC Monitor appliance is set up properly, as instructed in "Hardware Installation" on page 23. Once the appliance is plugged in and running, you need to configure the UC Monitor Management Console. See Chapter 5, "Setting Up the Management Console" on page 77 for instructions.

You'll need to create Location definitions to identify Avaya endpoints in reports and supply security information, by means of SNMP profiles, to allow the Collector to poll the Communication Manager for data.

Important: When monitoring has proceeded for a few hours, we strongly recommend checking the Call Server List to see whether you need to manually edit call server information or add a call server.

The C-LAN board and MedPro might have been discovered without the Communication Manager itself. See "Adding a New Call Server" on page 136 for more information.

Finally, you'll create or edit the roles and user accounts that identify other UC Monitor users and allow them access to the data that's collected and stored.

The following chapters discuss the necessary steps in detail.

CHAPTER 5

Setting Up the Management Console

As soon as you've completed the steps outlined in the previous chapter to install CA NetQoS Unified Communications Monitor, you are ready to set up the Management Console.

Management Console configuration includes a few simple security procedures, such as changing the default Administrator username and password, as well as some basic administrative settings to identify the Management Console on the network and point it toward the collection device(s) with which it will communicate. You might also want to complete some optional steps, such as setting up masks that conceal directory numbers in UC Monitor reports, and creating schedules for UC Monitor reports to be sent by email to designated recipients.

This chapter covers the following topics:

- "Initial Security Procedures" on page 78
- "Management Console Settings" on page 78
- "Configuring Collection Devices" on page 83
- "Working with Collector Thresholds" on page 93
- "Scheduled Email Report Delivery" on page 99

Initial Security Procedures

CA NetQoS Unified Communications Monitor has built-in security features to prevent unauthorized users from viewing data about your network, gaining access to SNMP community information, or reading sensitive telephone records. But your system is only as secure as your own practices. To ensure the security of your system, one of the first steps you should take during initial setup is to change the default username and password associated with the Administrator role.

To change the default password:

1. In the navigation links, click **Administration > Security > Users**.
2. On the User List page, click to select the check box for the default Administrator, **nqadmin**.
3. Click **Edit**.
4. The User Properties page includes a **Password** field. Enter a new password in the field.
5. Confirm the new password by retyping it, and then click **Save**.

You can use a similar procedure to change the passwords assigned to the user accounts you define for your UC Monitor system. See "Adding or Editing a User" on page 228 for more information.

If you are using the CA NetQoS Performance Center, version 4.0 or later, you can create custom groups of media devices, call servers, and Locations and grant users view access to UC Monitor data on a per-group basis. See Appendix A, "Working with Groups in the CA NetQoS Performance Center" on page 241 for more information.

Management Console Settings

By default, the UC Monitor Management Console is identified on the network by its IP address and hostname. You can update the Management Console settings to make it easier for remote users to access the Management Console and view reports.

The first time you use Unified Communications Monitor, you will probably need to change a few of the default Management Console settings. For example, you should provide the name of your SMTP server so that the Management Console can send email messages automatically in response to Incidents. The steps to take depend on whether the UC Monitor product is installed as a **Standalone** system (all components installed on a single computer) or as a **Distributed** system (the Collector(s) and Management Console installed on separate computers), and on the collection device type, either:

- a **NetQoS Collector**—for monitoring Cisco Unified Communications Manager or Avaya Communication Manager
- an **OCS Collector**—for monitoring Microsoft deployments

The following topic walks you through the necessary steps for each type of system and collection device.

Editing Management Console Settings

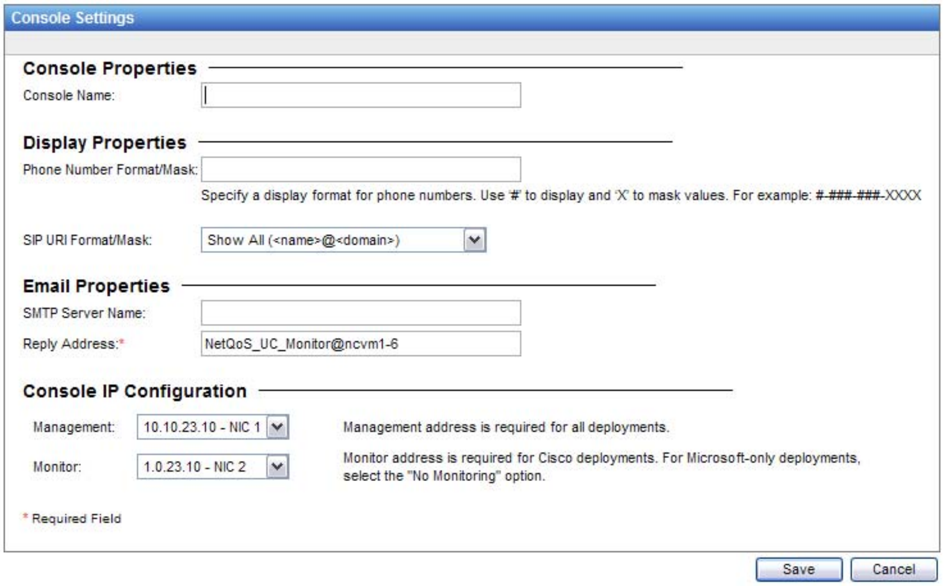
In the Installation chapter of this guide, you were instructed to configure NIC cards and LAN connection settings for the Management Console. After you have set up those network connections, the Management Console detects them and displays their properties on the Console Settings Administration page. Verify the settings and make sure the Management Console is using the correct connections for management and monitoring. The steps to take are slightly different for each type of UC Monitor system (Standalone or Distributed).

In a **Standalone** environment, you won't have to change Collector settings because they are automatically detected by the Management Console that is running on the same computer. But you will need to take a few other steps to configure your Management Console.

To edit Management Console settings in a Standalone environment:

Note: The Console Settings page is the first page you see after logging in for the first time.

1. To return to the Console Settings page after navigating away from it, in the navigation links, click **Administration > Console**, and then click **Settings**.



Console Settings

Console Properties

Console Name:

Display Properties

Phone Number Format/Mask:

Specify a display format for phone numbers. Use '#' to display and 'X' to mask values. For example: #-###-###-XXXX

SIP URI Format/Mask: Show All (<name>@<domain>)

Email Properties

SMTP Server Name:

Reply Address:* NetQoS_UC_Monitor@ncvm1-6

Console IP Configuration

Management: 10.10.23.10 - NIC 1 — Management address is required for all deployments.

Monitor: 1.0.23.10 - NIC 2 — Monitor address is required for Cisco deployments. For Microsoft-only deployments, select the "No Monitoring" option.

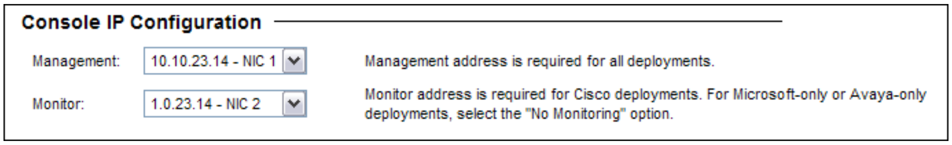
* Required Field

2. Change or supply the following properties to match your network:

Console Setting	Description
Console Properties	
Console Name	The name of your Management Console; not the hostname of the server.
Display Properties	
Phone Number Format/Mask	The format to use when displaying phone numbers on report pages. Use a # character for the portions of the phone number you want to display in the Management Console. Use an X character for the portions that you want to mask, or hide. You can also specify other characters as separators. For example, specify `(###) ###-#XXX` to see a phone number that looks like this in reports: (888) 543-2XXX
SIP URI Format/ Mask	The format to use when displaying SIP universal resource identifiers (URIs) on report pages. Select a format for the portions of the identifier—usually an email address—that you want to display in the Management Console. The default is to show the entire URI. You can also select: • **Show Name/Hide Domain**. For example, `jdoe@X` or `john.doe@X` • **Hide Name/Show Domain**. For example, `X@netqos.com` • **Hide All**. For example, `X@X`
Email Properties	
SMTP Server Name	The address of the SMTP server responsible for sending email messages on your network. Unified Communications Monitor can use this information to send email messages automatically in response to Incidents. Or, if an SMTP server is not configured locally, UC Monitor does not send email messages.
Reply Address	The email address to which the recipient of the emailed report should send responses. Also displays as the **From** address in the emailed report. The default setting is `NetQoS_UC_Monitor@[server hostname]`. You might want to set up an email alias with this username so that reply email can be sent. ***Important:*** Some mail servers, including Microsoft Exchange, automatically disable all links in email from unknown addresses. We therefore recommend changing this address to a real email address that is known to your email server. Otherwise, recipients receive a warning message that identifies messages from the Management Console as possible "phishing" messages. The default Reply address cannot be added to the Safe Senders list, which requires a ".com" suffix. If a user who is setting up an email report schedule has an email address defined in the User Properties for his or her user account, that email address overrides this Reply Address. See "Adding or Editing a User" on page 228 for more information.

Console Setting	Description
Console IP Configuration	
NIC	Either 1 or 2; the priority of this adapter in the Adapters and Bindings Network Connections list. ***Important:*** To monitor Avaya, leave the default settings as they are. Check this identifier to make sure that Windows has not switched the assigned priorities of the adapters. The Management NIC needs to be the first one listed. If it isn't, follow the instructions in "Configuring the NICs" on page 25.
Management Monitor	The IP addresses of the Management and Monitor NICs, which you assigned during the installation. See "Configuring the NICs" on page 25. To prompt you to select the correct NIC, a note stating "This is most likely your management address" may appear next to the Management and Monitor fields. In a standalone system, the Management Console is able to detect their identities from the NICs themselves. The following step provides instructions for selecting the Management and Monitor addresses.
IP Address	The IP address assigned to each adapter.

3. Any NIC cards installed on the computer are shown in the Console IP Configuration section. Select the Management and Monitor NICs from the lists of known IP addresses:



Console IP Configuration

Management: 10.10.23.14 - NIC 1 — Management address is required for all deployments.

Monitor: 1.0.23.14 - NIC 2 — Monitor address is required for Cisco deployments. For Microsoft-only or Avaya-only deployments, select the "No Monitoring" option.

- The **Management** address is for the NIC card that the Management Console uses to connect to the network. It needs to have priority 1 in the Adapters and Bindings Network Connections list.
- The **Monitor** address applies to a NIC on the Collector that is only used to monitor **Cisco** call traffic.

  If you are **not** monitoring any Cisco call servers, select **No Monitoring** from the **Monitor** list.

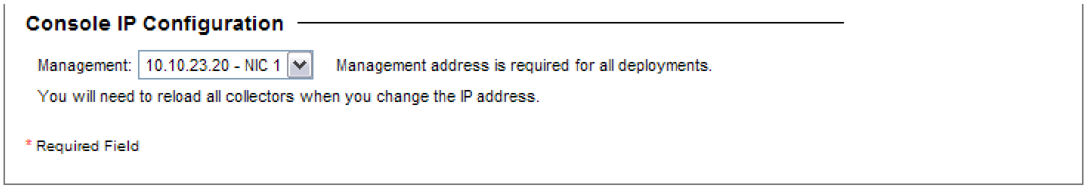
4. Click **Save** to save your settings.

▶ **Microsoft** monitoring uses an OCS Collector. You will add it to the Management Console as a separate step.

▶ **Avaya** monitoring uses two additional Collector ports. If you need to change the default ports for receiving RTCP and CDR data, edit the Collector. For more information, see "Collection Device Properties" on page 88.

To verify or change settings in a Distributed environment:

1. In the navigation links, click **Administration > Console**, and then click **Settings**.
2. The Console Settings page is displayed. Change or supply any of the Console Properties or Email settings as described above for a standalone system.
3. The Console IP Configuration settings are different for a Distributed system:



Console IP Configuration

Management: 10.10.23.20 - NIC 1 Management address is required for all deployments.

You will need to reload all collectors when you change the IP address.

* Required Field

4. Verify or select the **Management Address** from the list. Select the NIC IP address that the Management Console should use for management information (incoming data from the collection devices and outgoing configuration information to the collection devices).

   Note: The "NIC 1" or "2" designation indicates the priority of this NIC in the Adapters and Bindings Network Connections list on the Management Console server. Make sure that the Management NIC has the "NIC 1" designation. If it doesn't, follow the instructions in "Configuring the NICs" on page 25.

5. Click **Save** to save your settings.

The Management Console immediately attempts to verify the Management NIC you selected. If it succeeds, a message states, "`Console successfully updated.`"

Next Steps

In a **Standalone system**, the Collector should now be active, unless you selected the **No Monitoring** option (which disables it in preparation for monitoring in a Microsoft-only or Avaya-only environment).

- If you're monitoring Cisco-only, you can begin setting reporting parameters. For more information, see "About UC Monitor Locations" on page 104.
- If you're monitoring Microsoft, you need to add an OCS Collector. For more information, see "Adding a Collection Device" on page 83.
- If you're monitoring Avaya, you need to create SNMP profiles so that the Collector can poll the Communication Manager for additional endpoint and trunk group data. For more information, see "Working with SNMP Profiles" on page 234.

In a **Distributed system**, you must now **add a collection device**. The following sections provide instructions for managing Collector settings and adding collection devices to the system.

Configuring Collection Devices

In a Distributed system, the collection devices that gather call performance information and send it to the Management Console for analysis and reporting are running on different servers than the UC Monitor Management Console. For this type of system, you must initially add at least one collection device to initiate monitoring—either a Collector to monitor Cisco or Avaya UC deployments, or an OCS Collector to monitor Microsoft voice and video calls. The Management Console needs information about where collection devices are running.

In a **Distributed system**, data collection does not begin until you add collection devices to the Management Console. You must add at least one Collector to allow monitoring to begin. You can add additional collection devices later with this type of system. For more information, see "Adding a Collection Device" on page 83.

In a **Standalone system**, the Collector is installed and running on the same computer as the Management Console. But you still need to add the OCS Collector if you want to monitor Microsoft. The following topic, "Adding a Collection Device" on page 83, describes the necessary steps.

A few management tasks are required for each collection device. To enable optional monitoring of multiple, separate domains, the **NPC Domain** parameter must be edited in the Collection Device Properties. This parameter instructs the Collector to associate all the traffic that it sees with a custom group created in the CA NetQoS Performance Center (NPC). For more information, see "Monitoring by Domain" on page 255.

In addition, if you are monitoring Cisco or Avaya, you might need to reload your Collector periodically to send it all the current configuration data stored in the Management Console. For more information, see "Managing or Editing Collection Devices" on page 87.

Adding a Collection Device

In a Distributed system, you must configure collection devices by providing information to the Management Console about the Collectors you have installed and, if applicable, the Microsoft servers you want to use as collection devices.

You must add at least one collection device; data collection does not begin until you add a device through the Management Console. You can then add additional collection devices at any time.

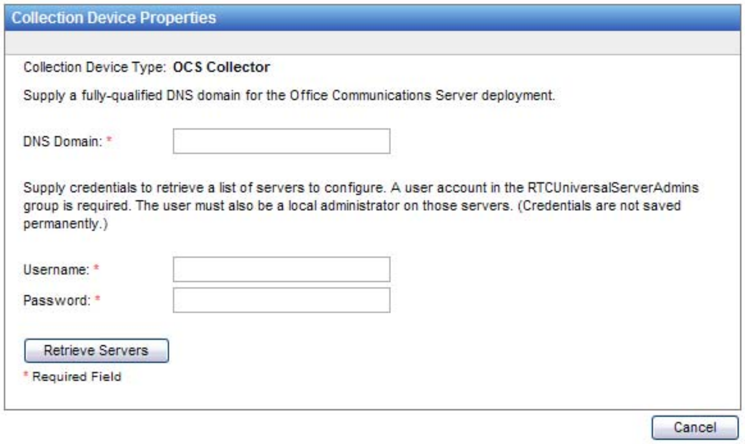
Note: This step is not necessary in a Standalone system if only Cisco or Avaya equipment is monitored; a Standalone system has the Collector and Management Console installed on a single computer.

To monitor in a Cisco or Avaya environment, add a **Collector**. To monitor in a Microsoft environment, add an **OCS Collector**. The necessary steps to add either one (or both) are provided below.

To add a collection device to the Management Console:

1. In the navigation links, click **Administration > Data Collection**, and then click **Collectors**.
2. The Collection Device List page appears.
3. Click **New**.

4. The Collection Device Properties page appears. If you are running a standalone UC Monitor system, a message indicates that **OCS Collector** is the only type of collection device that can be added:



Collection Device Type: **OCS Collector**

Supply a fully-qualified DNS domain for the Office Communications Server deployment.

DNS Domain: *

Supply credentials to retrieve a list of servers to configure. A user account in the RTCUniversalServerAdmins group is required. The user must also be a local administrator on those servers. (Credentials are not saved permanently.)

Username: *

Password: *

5. For a Distributed system, select the type of collection device, one of the following:
   - **Collector**—The NetQoS Collector. Monitors Cisco and Avaya deployments only.
   - **OCS Collector**—The Microsoft Office Communications Server 2007 server that receives call quality reports from the endpoints. Monitors Microsoft deployments only.

   The next steps to take depend on the type of device you are setting up.

6. Supply the following information for a **Collector** (to monitor Cisco or Avaya deployments):

Collection Device Property	Description
Server Name	The DNS hostname of the server hosting this collection device. If you do not know the server name, enter the IP address in the **Management Address** field and click the **DNS** button.
IP	Click to find the IP address that corresponds to the DNS name you typed.
NPC Domain	The domain with which all traffic seen by this Collector should be associated. A custom group created in the CA NetQoS Performance Center (NPC). Select it from the list. ***Note:*** This parameter is not visible unless UC Monitor is registered to a CA NetQoS Performance Center instance where at least one custom domain has been created. See “Monitoring by Domain” on page 255 for more information.
Management Address	The IP address you assigned to the Management NIC when you configured it on the collection device. See “Configuring the NICs” on page 25 for more information. Use dotted notation, such as 10.10.2.34. If you do not know the IP address, enter the server DNS hostname in the **Server Name** field and click **IP**.
DNS	Click to find the DNS hostname that corresponds to the IP address you typed.

Collection Device Property	Description
Monitor Address	The IP address you assigned to the Monitor NIC when you configured it on the Collector. See "Configuring the NICs" on page 25 for more information. It is not needed for Avaya monitoring. Use dotted notation, such as 1.1.0.0. If you do not know the IP address, click the **Check** button (see below).
Check	Click to verify the IP address you entered for the Collector **Monitor Address** above. The Management Console then attempts to contact the Collector at the Management Address you supplied and tries to get its status and its version.

7. Click **Save** to save the information about this collection device and leave this Administration page.

   Or click **Save and Add Another** to save the information about this collection device and refresh the page to add an additional collection device.

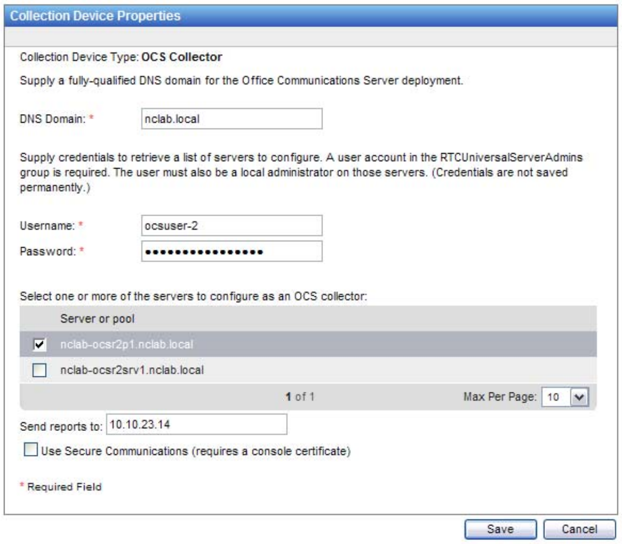
8. Supply information for an **OCS Collector** (to monitor Microsoft deployments).

   Note: In order to successfully configure the OCS Collector and retrieve the settings, the target login account that you are accessing from the UC Monitor Management Console needs *both* Domain User and Local Administrator privileges.

Collection Device Property	Description
NPC Domain	The domain with which all traffic seen by this OCS Collector should be associated. A custom group created in the CA NetQoS Performance Center (NPC). Select the domain from the list. ***Note:*** This parameter is not visible unless UC Monitor is registered to a NetQoS Performance Center instance where at least one custom domain has been created. See "Monitoring by Domain" on page 255 for more information.
DNS Domain	The fully-qualified DNS name of a domain in the Active Directory forest where the Microsoft server that will act as an OCS Collector is running. Include the top-level domain for the target forest. For example, use the format "netqos.com" rather than just "netqos". This information is required to help the Management Console locate the target Microsoft server(s) in cases where the Management Console is not in the Microsoft domain. If you do not know the domain of the server itself, any domain in the same forest will suffice due to Active Directory replication.
Username	A username for a secure Windows account with Administrator access to the Microsoft server. Supply credentials for an account in the RTCUniversalServerAdmins group to allow for read-write access to the target Microsoft server.
Password	A password for the secure Windows account.
Retrieve Servers	Click to search the domain for servers that are eligible for configuration as OCS Collectors. See "Collection Device Properties" on page 88 for more information about these settings.

9. Click the **Retrieve Servers** button.

The Management Console Web service searches the domain you supplied for a QoE Monitoring Server or Front-End server(s). If it succeeds in locating eligible servers, it displays a list of servers to configure as OCS Collectors:



Collection Device Type: **OCS Collector**

Supply a fully-qualified DNS domain for the Office Communications Server deployment.

DNS Domain: * nclab.local

Supply credentials to retrieve a list of servers to configure. A user account in the RTCUniversalServerAdmins group is required. The user must also be a local administrator on those servers. (Credentials are not saved permanently.)

Username: * ocsuser-2

Password: * ••••••••••••••••

Select one or more of the servers to configure as an OCS collector:

	Server or pool
☑	nclab-ocsr2p1.nclab.local
□	nclab-ocsr2srv1.nclab.local

1 of 1 Max Per Page: 10

Send reports to: 10.10.23.14

□ Use Secure Communications (requires a console certificate)

* Required Field

10. Click to select the server(s) to configure.
11. The **Send reports to** field shows the IP address of the Management Console by default. The Microsoft server will send all the call quality reports it receives to a Web service at this address. If you need to specify another location for the Management Console report recipient Web service, supply the IP address here.
12. Click to enable the **Use Secure Communications** check box if you want to use HTTPS for communications between the Management Console and Microsoft server.

    Note: Client certificates are not supported. The certificate server (or CA) and serial number must already be set on the Microsoft server. See Chapter 3, "Preparing to Monitor a Microsoft Environment" on page 37 for more information.
13. Click **Save**.

    The Management Console attempts to send report recipient information to the QoE Monitoring Server or Front-End server(s) using the credentials you supplied above. If it succeeds, a message states, "`Loaded settings successfully from server <server hostname>.`"

When you add an OCS Collector, the Management Console automatically configures it with the default settings. You can edit these settings if desired. See "Collection Device Properties" on page 88 for more information about them. In certain environments, not all servers in the enterprise pool can be configured. An informational message instructs you to perform some extra steps, which are discussed in "Preparing the Front-End Server (R2 Only)" on page 46.

If the attempt to add the OCS Collector fails, the most common reason is insufficient user account privileges. However, if the issue is an intervening firewall, you may have to configure the report recipient information manually, using the OCS Collector Configuration Utility provided by CA. See "Creating a Connection to the Report Recipient" on page 49 for more information about this utility.

For more information about the options for editing OCS Collector settings or about the actions available on the Collection Device List page, see the following topic, "Managing or Editing Collection Devices."

Managing or Editing Collection Devices

In addition to providing a means of adding new collection devices to the Management Console settings, the Collection Device List page provides several options for managing the collection devices that are already active in your system.

Access the Collection Device List by clicking **Administration > Data Collection > Collectors**.

For more information about the type and status information shown in the table, see "Viewing the List of Collection Devices" on page 92.

The following actions are available on the Collection Device List page:

Action	Description
Update Status	Get a recent status for all Collectors. You are prompted whether to continue or cancel. If you continue, the Management Console contacts any Collectors in the list to get their status.
Reload All	Instructs the Management Console to contact Collectors all and send them the latest configuration data. Each time you change certain configuration parameters, this action is essential to pass updates to the Collectors and ensure that they perform the required functions. For example, if you set up a new Call Watch or make any changes to a Call Watch definition, you must pass the associated information to all Collectors. Other times to reload are after editing the default SNMP community string or making any changes to a media device defined in the system. ***Note:*** The Update Status and Reload options do not apply to OCS Collectors.
New	Lets you add a new collection device to your UC Monitor system. See "Adding a Collection Device" on page 83.
Edit	Lets you change collection device properties or run a trace of packets coming into the Collector. See "Collection Device Properties" on page 88 for more information.
Delete	Lets you delete a collection device. On the Delete Confirmation page, click **Continue with Delete** to delete the device. Otherwise, click **Cancel**. The collection device is removed from the UC Monitor Management Console settings. The following then occurs, depending on the type of collection device: • On the Collector, the agent service stops running. However, the agent communicator service continues to run. If a Management Console contacts it (if you decide to add the Collector definition to another Management Console, for example), the agent service restarts. • On the Microsoft server (OCS Collector), the Web service sends instructions to discontinue posting call quality reports to the report consumer and to retain them in the local server database instead.

In a Distributed system, you must configure collection devices by providing information to the Management Console about devices you have installed. This step is not necessary in a Standalone system (where the necessary UC Monitor components are installed on a single computer).

You must add at least one collection device to the Management Console to allow data collection to begin. You can then add additional collection devices at any time.

When you add or edit a collection device in a Distributed system, you supply or change information on the Collection Device Properties page. You may need to reload the device to update its information.

Collection Device Properties

The following table describes the properties you can view or edit on the Collection Device Properties page. The different collection device types have different properties.

Access the Collection Device List by clicking **Administration > Data Collection > Collectors**. Then click the **Add** or **Edit** button to see the Collection Device Properties page.

The following table describes **Collector** properties (for monitoring Cisco and Avaya deployments):

Property	Description
Status	The current status of the collection device. Not available for an OCS Collector. Should be `Running`.
Collection Device Type	The type of collection device. For Cisco or Avaya monitoring, the type is **Collector**.
NPC Domain	The domain with which all traffic seen by this Collector should be associated. This type of domain is actually a custom group created in the CA NetQoS Performance Center (NPC). Select the domain from the list. Otherwise, all traffic seen by this Collector is associated with the default domain. ***Note:*** This parameter is not visible unless UC Monitor is registered to a NetQoS Performance Center where at least one custom domain has been created in the Manage Groups section of the **Admin** tab. See "Monitoring by Domain" on page 255 for more information.
Server Name	The DNS hostname of the server hosting this collection device. If you do not know the DNS hostname, enter the IP address in the **Management Address** field and click the **DNS** button.
Management Address	The IP address of the NIC that sends data to the Management Console. Click the **IP** button to resolve a hostname in the **Server Name** field to its IP address.
Monitor Address	The IP address of the NIC that is attached to the SPAN port on the switch. Not available for Avaya-only monitoring.
RTCP Monitor Port	(*Avaya monitoring only*.) The port on which the Collector listens for incoming RTCP data from Avaya phones and endpoints. Corresponds to the port you configured on the Communication Manager. See "RTCP Monitor Configuration" on page 70. Default is 5005.

Property	Description
CDR Monitor Port	(*Avaya monitoring only.*) The port on which the Collector listens for incoming TCP data (Avaya CDRs) from the Avaya Communication Manager. Corresponds to the port you configured on the Communication Manager. See "Enabling CDR Collection" on page 72. Default is 9000.

Note: In a standalone system, most Collector settings cannot be edited.

If the collection device type is **Collector**, the following actions may be performed from the Collection Device Properties page:

- **Reload**—Sends the most recent configuration data, such as newly created Call Watch or media device definitions, to the collection device. See "Managing or Editing Collection Devices" on page 87 for more information.
- **Packet Trace** – (*Cisco Only.*) Launches the trace file utility. All packets being seen by the Collector are traced and saved in a trace file on the Collector. A CA Support technician may ask you to use this feature and will tell you how to access the file.

If the collection device is an **OCS Collector** (for monitoring Microsoft deployments), a secure login is required to retrieve and view the configured settings. The following table describes **the OCS Collector** properties you can see without logging in:

Property	Description
Status	Due to security restrictions in the Microsoft environment, this parameter is not available from the OCS Collector. Says "**n/a**".
Collection Device Type	The type of collection device. For Microsoft monitoring, the type is **OCS Collector**.
Server Name	The DNS hostname of the Microsoft OCS Collector you selected for editing. Note that the DNS domain you supplied when you configured the OCS Collector is stored in the UC Monitor database. For security reasons, the login credentials are not stored.
Username	A username for a secure Windows account with Administrator access to the Microsoft server. Supply credentials for an account in the RTCUniversalServerAdmins group to allow for read-write access to the target Microsoft server.
Password	A password for the secure Windows account. Always shown in encrypted format.
Retrieve Settings	Click to search the domain for servers that are eligible for configuration as OCS Collectors. See "Collection Device Properties" on page 88 for more information about these settings.

When you create an OCS Collector, a utility running on the UC Monitor Management Console uses WMI on the target Microsoft server to set the necessary parameters. If you supply a username and password with the required permissions described above, you can retrieve, view, and edit these settings. See the following topic, "Editing OCS Collector Advanced Settings," for more information.

Editing OCS Collector Advanced Settings

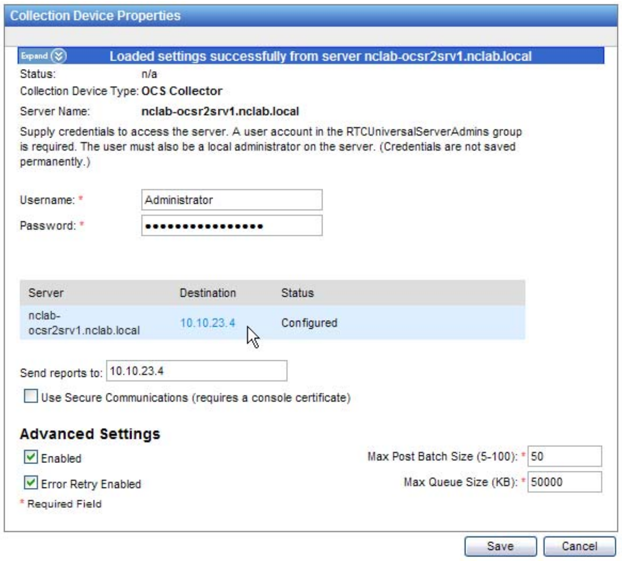
When the OCS Collector is created, a configuration utility on the UC Monitor Management Console uses WMI to change some settings on the Microsoft server. The affected parameters determine a new target location for the quality reports that the server continually receives from the endpoints and, if desired, enable the Web service running on the Management Console to use HTTPS for communications between the OCS Collector and the Management Console. Other parameters maintain the Microsoft default settings for QoE Monitoring Server or Front-End server behavior. These settings are included in the Advanced OCS Collector Settings and can be viewed and edited.

You might need to view the Advanced OCS Collector Settings for troubleshooting purposes. For example, if reports are not being received from the OCS Collector, you should check to make sure the Collector has been enabled. Like the target location for quality reports, the **Enabled** setting is normally configured via WMI on the Microsoft server and is later available in the Advanced Collector Settings.

To view or edit the advanced OCS Collector Settings:

1. Access the Collection Device List by clicking **Administration > Data Collection > Collectors**.
2. In the list of collection devices, click to select the OCS Collector, and click **Edit**.
3. On the Collection Device Properties page, supply the username and password for a secure Windows account with Administrator access to the Microsoft server that is acting as an OCS Collector.

   Note: Supply credentials for an account in the RTCUniversalServerAdmins group to allow for read-write access to the target Microsoft server.
4. Click **Retrieve Settings**. If your credentials allow you to query the target server for current report recipient settings, the following additional information about the Collector is displayed on the Collection Device Properties page:



Collection Device Properties

Loaded settings successfully from server nclab-ocsr2srv1.nclab.local

Status: n/a

Collection Device Type: OCS Collector

Server Name: nclab-ocsr2srv1.nclab.local

Supply credentials to access the server. A user account in the RTCUniversalServerAdmins group is required. The user must also be a local administrator on the server. (Credentials are not saved permanently.)

Username: * Administrator

Password: * ••••••••••••••••

Server	Destination	Status
nclab-ocsr2srv1.nclab.local	10.10.23.4	Configured

Send reports to: 10.10.23.4

□ Use Secure Communications (requires a console certificate)

Advanced Settings

☑ Enabled

☑ Error Retry Enabled

Max Post Batch Size (5-100): * 50

Max Queue Size (KB): * 50000

* Required Field

Property	Description
Server	The DNS hostname of the Microsoft server that has been configured as an OCS Collector.
Destination	The report recipient: the new target for call quality reports from the Microsoft endpoints. By default, the recipient is the Web service running at the UC Monitor Management Console IP address. The indicated server will send all quality reports to this address, unless you change it.
Send reports to	Supply a new IP address if you want to instruct the Microsoft server to send reports to a computer or Web service other than the one shown (that is, the UC Monitor Management Console).
Use Secure Communications	Click to enable this check box if you want to use HTTPS for communications between the Management Console and report recipient. Client certificates are not supported. A certificate must be configured on the UC Monitor Management Console. See "Configuring Secure Communications" on page 54 for more information. ***Note:*** The certificate server (or CA) and serial number must already be set on the Microsoft server. See "Installing and Setting Up the Quality of Experience Monitoring Server" on page 45 for more information.
Advanced Settings	
Enabled	Whether the OCS Collector is enabled for reports. If the check box is cleared, the Collector definition can be saved, but reporting does not begin. By default, the server is enabled.
Max Post Batch Size	The maximum size, in number of reports, of the batch file containing call quality reports that the OCS Collector can post. Normally, the Microsoft server sends call quality reports continually, as they arrive from the endpoints. However, during busy hours, multiple call quality reports may arrive simultaneously. In such a case, the server compiles them into batches before posting them. Select a size, from 5 to 100 call quality reports. The default size is 50.
Error Retry Enabled	Whether the Microsoft server should try to send reports to the report consumer Web service a second time if the first attempt fails with an error. By default, error retries are enabled.
Max Queue Size	The maximum size of the report buffer, in KB. When connectivity issues occur that prevent it from posting data to the report consumer, the server buffers call quality reports, up to the limit set here, before discarding data. The default is 50000 KB.

5. If you've made any changes to the settings, click **Save**.

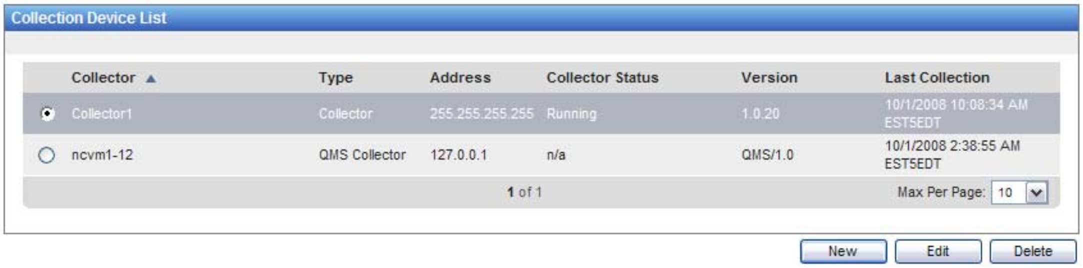
The UC Monitor Management Console sends the changes to the Microsoft server.

Viewing the List of Collection Devices

After you've added a least one collection device to your UC Monitor Management Console, data collection begins. You can then view information about any Collectors or OCS Collectors you've configured on the Collection Device List page.

To view the list of collection devices in your UC Monitor system:

1. In the navigation links, click **Administration > Data Collection**, and then click **Collectors**.
2. The Collection Device List page is displayed:



Collection Device List

	Collector ▲	Type	Address	Collector Status	Version	Last Collection
●	Collector1	Collector	255.255.255.255	Running	1.0.20	10/1/2008 10:08:34 AM EST5EDT
○	ncvm1-12	QMS Collector	127.0.0.1	n/a	QMS/1.0	10/1/2008 2:38:55 AM EST5EDT

1 of 1 Max Per Page: 10

The following information about the collection devices you have installed or configured is provided in the Collection Device List:

Property	Description
Collector	The DNS hostname of the server hosting this Collector. Or the hostname of the Microsoft server acting as an OCS Collector.
Type	The type of collection device, either: • **Collector**: A NetQoS Collector to monitor Cisco or Avaya deployments, or • **OCS Collector**: A Microsoft Office Communications Server 2007 server role, configured as a collection device
Address	The IP address of the computer that sends data to the Management Console. The Management address.
NPC Domain	The domain with which all traffic seen by this Collector is being associated. Actually a custom group created in the CA NetQoS Performance Center (NPC). ***Note:*** This parameter is not visible unless UC Monitor is registered to a NetQoS Performance Center instance where at least one custom domain has been created. For more information, see "Monitoring by Domain" on page 255.
Collector Status	(*Collector only*.) The status of the collection device with respect to the Management Console. If this is a device you have just added, shows "Never Contacted." If any issues have been detected on this Collector, they are indicated here. For more information, see "Working with Collector Thresholds" on page 93.

Property	Description
Version	The Collector version. For a Collector, corresponds to the associated release of Unified Communications Monitor; the build number is included. For an OCS Collector, the version of Microsoft Office Communications Server.
Last Collection	The last date and time that data was received from this collection device. **Note:** Use this property to determine OCS Collector status.

Only a UC Monitor Administrator can edit these settings. See "Adding a Collection Device" on page 83 for more information.

Working with Collector Thresholds

Collector thresholds are used to enable notifications of poor Collector performance, which may indicate a problem with the SPAN port or with the Collector itself. When crossed, these thresholds trigger any Incident responses that you have configured and selected. See "Setting up Incident Responses" on page 191 for more information.

Collector Incidents are reported in the Collector Incidents Report.

Initially, we recommend that you use the default thresholds for Collectors. However, as you gain a sense of Collector performance, tune SPAN port configuration, and determine whether the number of Collectors you have purchased is appropriate for the call volume of your system, you can change the thresholds to define poor Collector performance and ensure you are notified of any associated issues.

Note: Collector thresholds are designed to monitor the UC Monitor Collector and its features for monitoring Cisco IP telephony. They do not apply to other collection device types. However, the Abnormal Termination Incident is generated for any Collector failures in a Cisco or Avaya deployment.

Collector Threshold Settings

The following table summarizes the available thresholds for Collector performance and availability:

Collector Threshold	Description
Duplicate Packets	The maximum percentage of traffic observed by the Collector that can be composed of duplicate packets. Packet duplication is generally caused by a network or spanning (mirror port) problem. Duplicate packets are usually packets that are retransmitted when a response to a previous transmission is not received in time. This may indicate network problems. Duplication can also occur due to a SPAN misconfiguration that causes packets to be seen by the Collector twice.

Collector Threshold	Description
Discarded Packets	The maximum percentage of packets passing through the SPAN port that can be intentionally discarded by the Collector. Packets are usually discarded due to traffic bursts that exceed UC Monitor capacity for analysis given the current configuration. Packets are dropped if they arrive for processing when the Collector is too busy to receive them. The UC Monitor Release Notes provide information about scalability and hardware requirements.
Lost Bytes	The maximum percentage of traffic that can be lost by the Collector. Bytes of data are usually lost due to traffic bursts that exceed UC Monitor capacity for analysis given the current configuration. Some messages are too large to fit in one packet and must be split into separate packets. Packets can also arrive out of order. To handle these situations, the Collector contains a re-assembly engine that re-orders and re-assembles packets using their sequence numbers. During this processing, if the sequence numbers indicate that expected data has not been received, the bytes not received are counted as lost. A high number of lost bytes usually indicates a "one-way" spanning problem. Because the Collector is only seeing the packets from one side of a conversation, it will count the data traveling in the other direction as being lost because it cannot see it. The UC Monitor Release Notes provide information about scalability and hardware requirements.
Abnormal Termination	If enabled, creates an Incident whenever a service on the Collector logs a fatal exception. If the Incident does occur, the path to the "crash dump" file and, when possible, the path to a packet capture file are provided in the Incident report as additional information to send to CA Support.

Note: Collector thresholds only apply to UC Monitor Collectors for monitoring Cisco or Avaya environments.

Customizing Collector Thresholds

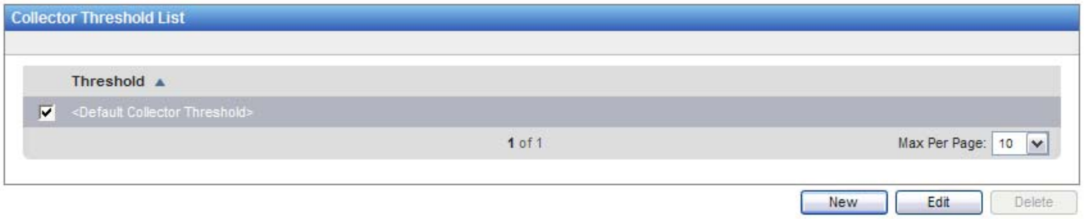
When you customize Collector thresholds, you change the threshold values that you want to change and supply a name for the custom settings. The UC Monitor interface lets you view the list of existing Collector threshold settings by name, edit the default thresholds, and add new, custom Collector thresholds. Thresholds include any responses you want to associate with Incidents raised in response to a potential threshold violation.

Note: Collector thresholds do not apply to the OCS Collector used for monitoring Microsoft Office Communications Server 2007. Only the Abnormal Termination threshold applies to Avaya.

To change a Collector threshold:

1. In the navigation links, click **Administration > Policies > Collectors**, and then click **Collector Thresholds**.

   The Collector Threshold List page is displayed:

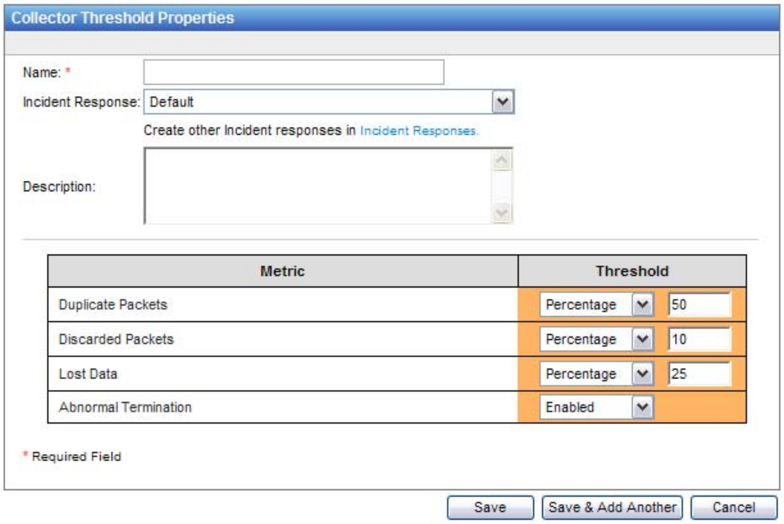


Before you create any new Collector threshold settings, only the name of the pre-defined settings, `<Default Collector Threshold>`, appears in the list. The pre-defined settings are used by default for all Collectors. You can edit these settings or create a new set of threshold settings and assign them to Collectors, as appropriate.

See "Collector Threshold Settings" on page 93 for an explanation of the threshold settings.

2. Click **New** to create a new set of custom Collector thresholds.

   The Collector Threshold Properties page is displayed:


Collector Threshold Properties
Name: *
Incident Response: Default
Create other Incident responses in Incident Responses.
Description:
* Required Field
Save
Save & Add Another
Cancel

Metric	Threshold	
Duplicate Packets	Percentage	50
Discarded Packets	Percentage	10
Lost Data	Percentage	25
Abnormal Termination	Enabled	

Collector threshold properties include a unique name for the custom settings, any Incident response you want to associate with violations of these thresholds, and an optional description of the settings.

3. Type a name for the settings you're customizing in the **Name** field.
4. To launch an Incident response action automatically when a threshold is violated, select an Incident response from the **Incident Response** list.

   All Incident responses, including the default and any you have already defined, are available in the **Incident Response** list. See "Setting up Incident Responses" on page 191 for more information.
5. (*Optional*) In the **Description** field, type a description of the settings. The description might indicate which Collectors should be assigned these custom settings, for example.
6. In the threshold properties table, find the metric whose threshold you want to change.
   - In the **Threshold** column for the Duplicate Packets, Discarded Packets, or Lost Data metrics, leave the default units (`Percentage`), or select `None` to disable that threshold.

If desired, type a new value for the maximum percentage of duplicate, discarded, or lost packets failures before an Incident is created.

- In the **Threshold** column for the Abnormal Termination metric, leave the default setting (`Enabled`), or select **None** to disable that threshold.

7. Click **Save** to save the new performance thresholds and return to the Collector Threshold List page. The new set of thresholds now appears in the list.

   Or click **Save and Add Another** to save the new threshold settings and return to the Collector Threshold Properties page, where you can add another set of custom thresholds.

Now that you have customized a set of thresholds, you need to apply the settings to a Collector. See the following topic, "Assigning Collector Thresholds," for instructions on applying the threshold settings to a Collector.

Assigning Collector Thresholds

The pre-defined UC Monitor Collector thresholds are applied to all Collectors as soon as you add them to the Management Console unless you change the threshold settings. You can change them by editing the default settings or customizing Collector thresholds and assigning the custom thresholds to selected Collectors.

Note: Collector thresholds do not apply to the OCS Collector used for monitoring Microsoft Office Communications Server 2007.

All the Collectors that have been added to the UC Monitor system are listed on the Collection Device List page. Click **Administration > Data Collection > Collectors** to see the list.

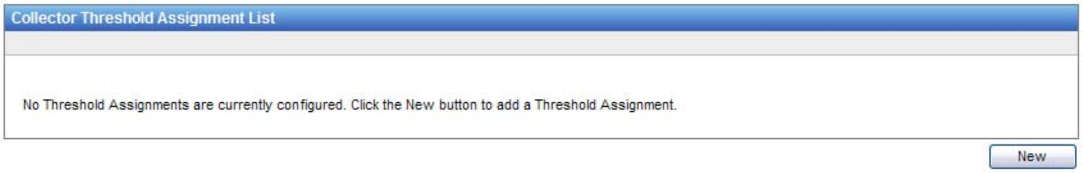
To assign a custom set of Collector thresholds:

In a Distributed system, you must have added at least one Collector to the Management Console before you can assign thresholds to it. See "Managing or Editing Collection Devices" on page 87 for more information.

You also must have customized at least one set of Collector thresholds before you attempt to apply them to a Collector. Follow the steps outlined above in "Customizing Collector Thresholds" on page 94.

1. In the **navigation link**s, click **Administration > Policies > Collectors**, and then click **Collector Threshold Assignments**.

   The Collector Threshold Assignment List page is displayed:



Collector Threshold Assignment List

No Threshold Assignments are currently configured. Click the New button to add a Threshold Assignment.

   All the Collector threshold assignments are shown in the list. Before you have assigned any thresholds to Collectors, a message states, `No Threshold Assignments are currently configured`.

2. Click **New** to create a new Collector threshold assignment.

The Collector Threshold Assignment Properties page is displayed.

Unless they have already been assigned to a set of custom Collector threshold settings, all known Collectors are shown in the **Available Collectors** list on the left.

Note: Other types of collection device are not listed; Collector thresholds apply to NetQoS Collectors only.

3. From the **Threshold** list, select a set of threshold settings to assign.
4. Click to select a Collector from the list. Then click the right directional arrow to move the selected item to the list of **Selected Collectors**.

   Select as many Collectors as you like. The named set of threshold settings shown in the **Threshold** field is assigned to all of them.
5. Click **Save** to save the new assignments. You return to the Collector Threshold Assignment List page. The new assignments now appear in the list.

   Or click **Save & Add Another**. Select another set of thresholds from the **Threshold** list at the top of the page and repeat Steps 4 and 5.

The **Filter** field accepts wildcard (*) search strings to limit the data shown in the Available Collectors list. If you supply a string but no asterisks, the **Filter** field assumes wildcards (for example, "*abc*") when it searches. Filtering can be useful if you have a long list of Collectors.

Example: To see only Collectors whose names associate them with the Raleigh, NC office, you would enter `ral*` for the filter and click **Apply**. Only Collectors whose name begins with Ral would be shown in the list.

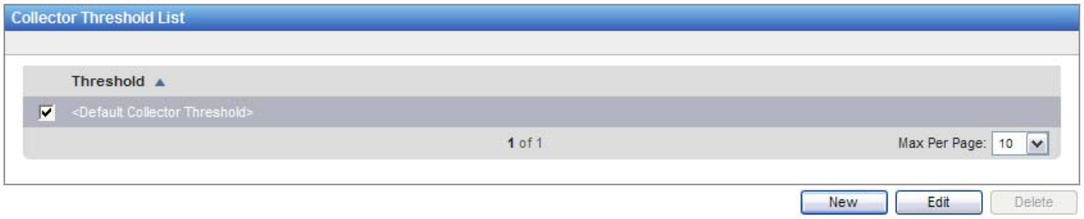
Editing Collector Threshold Settings

Collector thresholds, including ones you have customized, can be edited. You may, for example, find after a few days of data collection that you want to increase the value you selected for a Discarded Packets threshold so that you'll receive fewer Collector Incidents. Or you may want to edit the assignment of a named set of thresholds so that the settings are applied to additional Collectors. Instructions for editing threshold settings and editing threshold assignments are provided below.

To edit Collector threshold settings:

1. In the **navigation link**s, click **Administration > Policies > Collectors**, and then click **Collector Thresholds**.

   The Collector Threshold List page is displayed:



Collector Threshold List

Threshold ▲
☑ <Default Collector Threshold>

1 of 1   Max Per Page: 10

2. Select the threshold settings you want to edit.
3. Click **Edit**.

The Collector Threshold Properties page is displayed. The settings you selected when you customized these thresholds are shown.

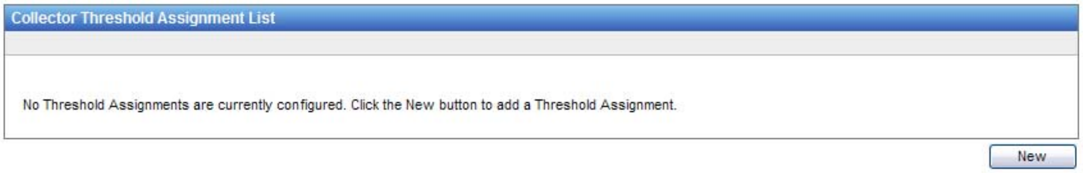
4. Make the desired changes to any of the settings. For more information about any of these settings, see "Collector Threshold Settings" on page 93.
5. Click **Save** to save your changes to the settings.

Your changes are applied as soon as you reload your Collectors. Click the link provided on the Collector Threshold List page to reload Collectors.

To change the assignment of a set of Collector thresholds:

1. In the **navigation link**s, click **Administration > Policies**, and then click **Collector Threshold Assignments**.

   The Collector Threshold Assignment List page is displayed:



Collector Threshold Assignment List

No Threshold Assignments are currently configured. Click the New button to add a Threshold Assignment.

2. Select the settings you want to edit.
3. Click **Edit**.

   The Collector Threshold Assignment Properties page is displayed.
4. Select a different set of threshold settings from the **Threshold** list.
5. Click **Save** to save the new assignment. You return to the Collector Threshold Assignment List page.

   The new assignment now appears in the list.

Your changes are applied as soon as you reload your Collectors. Click the link provided on the Collector Threshold List page to reload Collectors.

Scheduled Email Report Delivery

The UC Monitor Management Console can send report pages as email attachments, either immediately or according to a preselected schedule. As part of Console configuration, the UC Monitor Administrator must enable this feature by designating an SMTP server that is then used to send reports by email. See “Management Console Settings” on page 78 for more information.

Any UC Monitor operator with the permission to view a report also has the ability to schedule that report to be sent by email. Administrators can view and edit all email schedules, which instruct the Management Console to automatically send reports of certain types to designated recipients.

By contrast, UC Monitor operators with user account permissions can configure their own schedules and can unsubscribe themselves from scheduled email messages, but they cannot edit email report schedules that were set up by an Administrator.

On-demand email delivery is available for all report types. Scheduled email delivery is available for the following types of UC Monitor reports:

- Call Performance Overview and Call Details
- Troubleshooting reports
- Capacity Planning reports, all types
- Incidents. Scheduled email delivery is not supported for Incident Details, Incident Metric Details, or Incident Call Leg Details Reports.
- Investigations. Scheduled email delivery is not supported for Investigation Details.

Managing Email Report Schedules

Report delivery by email is an option available for UC Monitor reports by clicking **Email Page** on the Page menu of the selected report. For many report types, UC Monitor operators with the appropriate permission to view a report also have the ability to schedule that report to be sent by email. They can edit or delete any schedules they have created, and they can unsubscribe themselves from any scheduled email messages they receive.

However, Administrator account permissions are required to manage email report schedules created by other UC Monitor operators. In addition to being able to create new email schedules from report Page menus, Administrators can also view and edit all email schedules that have been created.

For example, if a UC Monitor operator with user account permissions sets up three separate schedules to send a single report to three other users, and if the operator then decides that one of those schedules is not necessary, either the operator or the UC Monitor Administrator can delete that schedule. But only the Administrator can delete schedules created by the Administrator.

To manage email schedules:

1. In the navigation links, click **Administration** > **Console > Scheduled Email**.

   The Scheduled Email List page is displayed. If no schedules have been created, a message appears stating that “`No emails are currently scheduled.`”

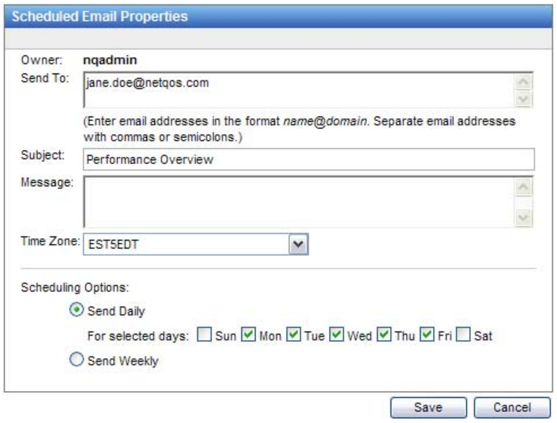
   Any email schedules that have been created by the Unified Communications Monitor user who is currently logged in are visible in the list. The Administrator can see all schedules.

The following information about each schedule is included in the list:

Column	Description
Owner	The operator who created the email schedule.
Subject	The subject of the email message; usually, the report title.
Recipients	The email addresses of the recipient(s) of the email containing the report.
Schedule	The frequency of report delivery by email.
Next Delivery	The next date and time that the report will be sent by email. Depends on the schedule.

2. To edit any schedule shown in this list, click to select the schedule, and then click **Edit**.

   The Scheduled Email Properties page is displayed:



Scheduled Email Properties

Owner: nqadmin

Send To: jane.doe@netqos.com

(Enter email addresses in the format *name@domain*. Separate email addresses with commas or semicolons.)

Subject: Performance Overview

Message:

Time Zone: EST5EDT

Scheduling Options:

● Send Daily

For selected days: □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

○ Send Weekly

3. The following table describes the available options for scheduled email report delivery:

Field	Description
Owner	The user account of the operator who created the email schedule. Other than the UC Monitor Administrator, only the owner can edit a schedule.
Send To:	Enter email addresses of report recipients in the following format: `<name>@<domain>` Separate multiple addresses with commas or semicolons. You can enter an email alias that includes multiple recipients.
Subject	The subject of the email message.
Message	The text sent in the body of the email message containing the report.
Time Zone	The time zone of the data shown in the emailed report. Select the time zone of the intended recipient. The time zone of the message recipient is set during user account configuration. See "Adding or Editing a User" on page 228 for more information.
Scheduling Options	
Send Now	Send the email message immediately.

Field	Description
Send on a Schedule	Schedule the email message containing a current version of the report to be sent on a regular basis. If enabled, reveals scheduling options (see below).
Send Daily	Schedule the email message to be sent once per day. If enabled, reveals check boxes where you can select the day of the week when the report should be sent. By default, the daily schedule sends the emailed report every weekday (Monday - Friday) at 00:30 hours in the time zone of the Management Console. The time frame of the daily report is the previous day.
Send Weekly	Schedule the email message to be sent once per week. If enabled, reveals a menu where you can select the day of the week when the report should be sent. By default, the weekly schedule sends the emailed report every Sunday at 01:00 in the time zone of the Management Console. The time frame of the weekly report is the previous week (Sunday - Saturday).
Send Monthly	An option to schedule the email message to be sent once per month. If enabled, reveals menus where you can select the day of the month when the report should be sent. ***Note:*** This option is only available for the Capacity Planning reports. By default, the monthly schedule sends the emailed report on the first day of each month at 01:30 in the time zone of the Management Console. The time frame of the monthly report is the previous month.

4. Click **Save** to save your changes to the email schedule.

The necessary steps to take to create a new email schedule from the Page menu of a selected report are documented in the *CA NetQoS Unified Communications Monitor User Guide*.

CHAPTER 6

Setting Reporting Parameters

By now, you should have completed the initial steps necessary to set up your Management Console. You should already have performed some preliminary security steps, such as changing the default password to access the Management Console, and you should be confident that the Management Console and Collector are communicating with each other over the network. You also should have gathered security information that enables the Collector to access MIB data from media devices, such as voice gateways.

Now you need to assign identifying names and other features to the logical and geographical segments of your network for reporting purposes and provide information required for monitoring PSTN calls. If your environment includes Cisco Unified Communications Manager call servers configured in clusters, you might also need to create call server groups. These groups help you organize call server reporting and assign call server group thresholds.

This chapter covers the following topics:

- "About UC Monitor Locations" on page 104
- "Configuring Media Devices" on page 117
- "Working with Call Servers and Groups" on page 132

About UC Monitor Locations

Before you begin defining Locations, be sure to read "Best Practices for System Configuration" on page 4 in the "Best Practices" chapter. That chapter provides essential tips and background information to help you understand how Locations are used.

Your Location definitions are the key to getting the most out of UC Monitor reports. Locations that correspond to easily understood network entities, such as branch offices, departments, or buildings, will help you quickly locate the sources of performance issues when they arise.

Your aim in creating Location definitions is to set up a reporting system in which:

- A single problem, such as slow call server response time, that may affect several end-users is not reported multiple times.
- More specifically, a single problem only creates one Incident in the system.
- The network operator or engineer who receives an automatic notification about a VoIP performance Incident is the person most capable of troubleshooting the problem.
- That same operator or engineer only receives a minimal number of email notifications about any specific performance Incident.
- UC Monitor operators see reports that contain only the call data that they have permission to view. Confidential call data is restricted to reports that most operators cannot access.

The Administrator should create Location definitions that cover all IP phones in the system being monitored. The basic definition consists of a name and a subnet or a list of subnets to help you identify sets of IP phones when their statistics appear in reports.

Until you assign a Location to a phone by adding its subnet to a Location definition, UC Monitor reports identify the Location of the phone as `<Unassigned>`. Phones with the "Unassigned" designation are ones the Collector has detected from the monitored network traffic whose IP addresses do not fall into any of the Locations that have been defined.

Location designations are never applied retroactively. Any phone subnets already in the database when they are added to a Location definition will only appear in new reports with that Location applied; they will remain categorized in their previous Location, which is `<Unassigned>` by default, in any historical reports. The same rule applies to monitoring by domain. When you create a custom domain in the NetQoS Performance Center, all Locations previously defined will continue to be placed in the Default Domain until you manually edit Locations to select the custom domain. See "Location Options and Best Practices" on page 104 for more information.

Location Options and Best Practices

When properly deployed, Locations provide the flexibility needed to organize and secure the entire system. In this section, we discuss some optional features related to Location definitions.

Some deployments provide more accurate reports if you selectively exclude less reliable data. For example, the phones in laboratory testbeds or pilot deployments should not contribute performance metrics to reports that pertain to a production network. When adding a Location definition, you can select a Monitoring Status option to exclude it from monitoring. Statistics from the phones and devices in the Location subnets will no longer be collected. This feature should be used with some caution; see "Disabling Monitoring of Selected Locations" on page 110 for more information.

Location definitions can also include *key phone* designations. By serving as the target for regular traceroute testing, the key phone allows the NetQoS Collector to gather additional data for baseline traceroute reporting. Key phones are optional, but recommended in a Cisco environment. Use only Cisco IP phones as key phones.

If you are monitoring a Microsoft Office Communications Server 2007 deployment, you should take steps to ensure that UC Monitor Locations and any locations known to the Quality of Experience Monitoring Server match each other as closely as possible. The Microsoft concept of locations corresponds to that used in Unified Communications Monitor: subnets where endpoints (phones and analogous devices) are connected.

In an Avaya UC deployment, IP network regions typically provide a way to apply configuration information to IP endpoints in the same segments of the network. For example, you can set QoS parameters, VoIP or video codecs, RTCP monitoring defaults, and call routing settings. IP network regions can also help you identify the physical or logical locations of phones and endpoints. We recommend using your existing IP network region parameters when setting up Location definitions.

As you create Location definitions and select key phones, follow best practices for placing Locations into NetQoS Performance Center groups so that UC Monitor operators gain access only to the call data that they need to do their job. An organizational strategy that leverages groups and Locations to protect sensitive call data is essential. Consult the relevant topics in Appendix A, "Working with Groups in the CA NetQoS Performance Center" before you create Locations and groups.

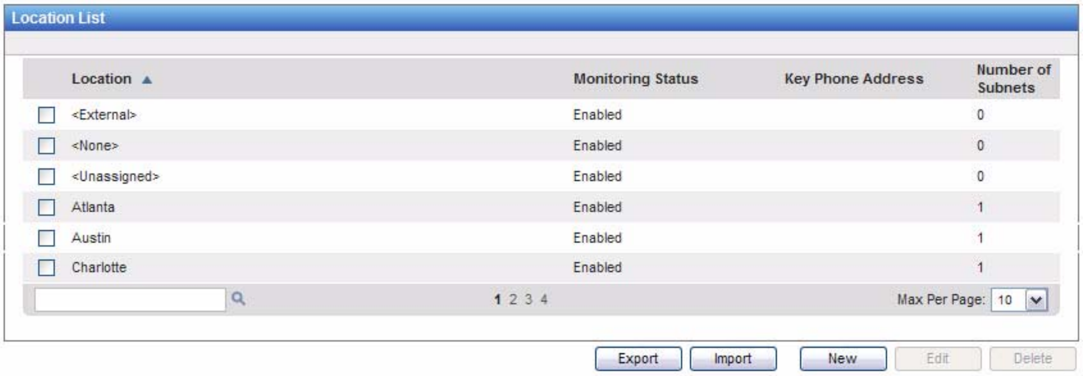
Any Location definition that already contains at least one subnet cannot be "moved" to another domain, once you've begun monitoring with custom domains. Use the workflow outlined in "Making Changes to Domain Assignments" on page 260 if you need to make changes after data has been collected.

Also consider some configuration-related strategies for gaining more value from the Phone Status Changes call server Incident. See "More about the Phone Status Changes Incident" on page 152 for some useful advice.

Viewing the Location List

Location definitions should be created to cover all IP phones and endpoints in the system being monitored. These definitions consist of an identifying name and an IP subnet or subnet range, plus an optional key phone that serves as a target for troubleshooting investigations.

Locations help you identify sets of IP phones when their statistics appear in reports. You can see any Locations that have already been defined on the Location List page.



Location List

	Location ▲	Monitoring Status	Key Phone Address	Number of Subnets
☐	<External>	Enabled		0
☐	<None>	Enabled		0
☐	<Unassigned>	Enabled		0
☐	Atlanta	Enabled		1
☐	Austin	Enabled		1
☐	Charlotte	Enabled		1

1 2 3 4 Max Per Page: 10

The following table describes the information included in the Location List:

Item	Description
Location	The Location definitions that are currently in use by Unified Communications Monitor. Either custom Locations that the Administrator has created, or the following pre-defined Locations: • **<External>**—Microsoft only. A default Location used for any endpoint that is being reported to the Microsoft quality monitoring server (either the QoE Monitoring Server or Front-End server) as being "remote." • **<None>**—A designation that indicates that the IP address of a phone that was detected during monitoring could not be determined. • **<Unassigned>**—A default Location for any phone or endpoint that the Collector detects from call traffic but that lacks an assigned Location. These usually indicate IP phones or media devices to which you need to assign Locations. See "Adding Locations" for more detailed information about Locations.
NPC Domain	The domain, actually a custom group created in the CA NetQoS Performance Center, with which traffic from this Location is being associated by Unified Communications Monitor. ***Note:*** If Unified Communications Monitor has not been registered to a NetQoS Performance Center instance where at least one custom domain has been defined, this parameter is not visible. See "Monitoring by Domain" on page 255 for more information.
Monitoring Status	Whether monitoring is enabled for this Location. You can select whether to exclude an entire Location from monitoring. The Collector discards any data collected from the subnets included in the Location definition. See "Adding Locations" on page 108 for more information about this option.

Item	Description
Key Phone Address	The IP address of the Location "key phone," an IP phone in one of the subnets included in this Location definition. The key phone allows the Collector to collect additional baseline data in Cisco environments by serving as the target for regular traceroute testing. If you supply a key phone address for a Location, the Collector runs a traceroute test to that phone every four hours. Baseline traceroute data is then reported in the "Traceroute Investigation Details" Report.
Number of Subnets	The total number of IP subnets included in this Location definition.

Just below the Location List, the following options are available:

- **Export**—The Location export feature assists you in keeping UC Monitor configuration up to date when changes to the UC system occur. Click the button to create and save a list of Locations and subnets to a file in comma-separated values (`.csv`) file format. Spreadsheet programs, such as Microsoft Excel, can read files in this format. See "Exporting Location Definitions" on page 114 for more information.
- **Import**—The Location import feature is provided for cases where the network contains a large number of IP phones or subnets. The import feature speeds up the process of defining Locations. To import Locations, the Management Console reads data from a file in `.csv` format.

  The required syntax for the data to be imported is provided in "Importing Location Definitions" on page 112.
- **New**—When you create a Location definition, you assign a useful name to an IP subnet or to multiple subnets and have the option to designate a key phone for use in baseline traceroute data collection. See "Adding Locations" on page 108 for more information.
- **Edit**—You can edit a Location definition that you have created to change its name, add or remove a subnet, add an identifying description, or change its monitoring status. Some parameters of the pre-defined Locations can also be edited. See "Editing Locations" on page 112 for more information.

Click **New** to start adding Location definitions, or click **Import** to add a list of definitions.

Tips about Location Subnets

The key information to supply when creating a new Location is the subnet, or list of subnets, that the Location definition includes. The UC Monitor interface lets you enter a 25-bit network address, such as 10.2.3.0, and select a value for the mask length, a valid number of bits to use for the subnet mask, such as 24.

For the final octet of the network address, you do not need to enter a more precise subnet specification than a bit value for the bits that are used for the mask. If you enter, for example, 10.2.3.**4** for the subnet with a mask of 27, the subnet is stored in the UC Monitor database and shown subsequently in Administration pages with the conventional syntax, 10.2.3.**0**/27.

You also have the option to limit a Location to a single IP address. The appropriate syntax would specify the IP address with a mask of 32 (all bits).

Multiple subnets can be added to each Location definition. To extend the previous example, other valid subnets that use the mask of 27 would be:

- 10.2.3.32
- 10.2.3.64
- 10.2.3.96
- 10.2.3.128
- 10.2.3.160
- 10.2.3.198
- 10.2.3.224

Each of these subnets can contain as many as 32 hosts. The Location definition you've created is then applied to any valid subnets you add. See "Adding Locations" on page 108 for instructions.

When you're adding subnets to a Location definition, be careful not to add any subnets that overlap. Overlapping subnets are not supported. A warning displays on the Add Location page if you try to add a subnet whose address range overlaps with one you've already added.

You should also avoid defining subnets with a mask of 32 bits, which defines the subnet as a single host address. This configuration also restricts the rest of the subnets in that range because of the restriction on overlapping. For example, if you first added a subnet of 10.10.44.55/32, you could not then add the subnet 10.10.44.0/24. To add the rest of the host addresses in the .44 subnet, you would have to manually add all the subnets from 10.10.44.**0**/24 through 10.10.44.**54**/24, and then add another set of subnets to include 10.10.44.**56**/24 through 10.10.44.**255**/24.

Adding Locations

Adding Locations is an essential first step to take when setting up your UC Monitor system. Location definitions cannot be applied retroactively to data already collected, so you need to add or import them as soon as you have installed and configured your Collector(s) and Management Console.

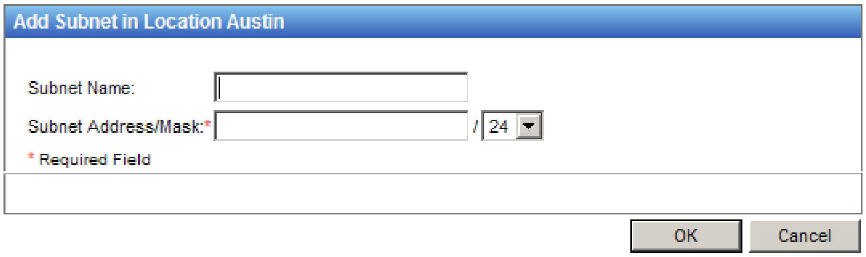
If you plan to define a large number of Locations, you might save some time by entering them into a spreadsheet document and importing them. See "Importing Location Definitions" on page 112 for more information.

To add a Location:

1. In the navigation links across the top of the Management Console user interface, click **Administration > Data Collection**, and then click **Locations**.
2. On the Location List page, click **New**.
3. On the Location Properties page, supply the following information:

Property	Description
Name	A name you assign to the Location. It's helpful to assign names based on: • Geography, such as "New York," or "Eastern Region," for example • Domain name, such as "Operations-US" • Exact location, such as "Building A" • Data center or NOC associated with the subnets in this Location • A combination of geographical location and department, such as "New York-Accounting"
NPC Domain	The domain with which traffic from this Location is being associated by Unified Communications Monitor. ***Note:*** If Unified Communications Monitor has not been registered to a NetQoS Performance Center instance where at least one custom domain has been defined, this parameter is not visible. For more information, see "Monitoring by Domain" on page 255.
Key Phone Address	The IP address of an IP phone in a subnet you plan to add to this Location definition. Select a Cisco IP phone. Other endpoints do not support this feature. The key phone allows the Collector to collect additional baseline data from regular traceroute testing. If you supply a key phone address here, the Collector runs a traceroute test to it every four hours. Baseline traceroute data is included in the Investigations Report. See "Baseline Traceroutes" on page 116 for more information.
Description	Any descriptive terms you want to associate with this Location, to help other network operators identify it.
Monitoring Status	Whether to include data from this Location in reports. The following options are available: • **Enabled**: Monitoring is enabled for any subnets you add to this Location, either now or at a later time. • **Disabled**: The subnets in this Location are not monitored; data collected from them is discarded. • **Enabled (Sending Only)**: Monitoring of these subnets is disabled, except for calls placed by phones in these subnets and received by phones in monitored Locations. See "Disabling Monitoring of Selected Locations" on page 110 for some advice before deploying the exclusion feature.

4. Click **New** to add a subnet to the Location definition. The Add Subnet page is displayed:



Add Subnet in Location Austin

Subnet Name:

Subnet Address/Mask:* / 24

* Required Field

5. Enter the following information about the first subnet that you want to add to this Location definition:

Field	Description
Name	A name to identify each subnet when it appears in the Administration pages.
Subnet	The IP network address, in dotted notation, for a subnet to be included in this Location definition. For example, `1.23.45.64` Corresponds to the IP addresses for the components in this Location. For a given Location, a single subnet or multiple subnets may be applicable. Select the subnet mask (designated by the number of bits in use) from the list provided in the next column.
/ [Mask]	Select the number of bits used in the subnet mask to create this subnet. For example, select 29 to indicate that the first three bits of the final octet are used to create subnets.

6. Click **OK**.

   The Unified Communications Monitor system validates the uniqueness of the new subnet. Subnets must not share addresses (that is, overlap) with other subnets you've defined previously. You can then click **New** again to add another subnet to this Location.

7. Click **Save** to save the Location definition.

   You return to the Location List page. The new Location appears in the list, showing the number of subnets you configured.

   Or click **Save and Add Another** to save the Location definition and return to the Location Properties page. You can then click **New** to add another subnet to the Location.

Disabling Monitoring of Selected Locations

Circumstances may suggest that data from selected Locations should be routinely excluded from reports, or that Incidents should not be created for those Locations. For example, your system might include a bank of phones that are regularly used in testing, and you would like to avoid seeing these calls reflected in the volume statistics in the Capacity Planning reports, or you do not want to see Incidents for these phones. Unified Communications Monitor offers a few options for excluding Locations from monitoring or disabling Incidents for subsets of devices.

First, to avoid collecting data from or generating Incidents for specific endpoints or phones, you should make sure the phones and gateways in question are assigned to a dedicated Location definition. And keep in mind that Location subnets cannot overlap.

The options available for disabling monitoring or Incidents partially depend on your environment:

Option	Applicable Vendors	Notes
Change SPAN configuration to exclude data from selected subnets or hosts	Cisco	Hosts in question are not monitored. Adds an extra layer of complexity to SPAN or ACL configuration. Requires careful testing to avoid excluding other, relevant data

Option	Applicable Vendors	Notes
Disable monitoring for selected Locations or media devices	Cisco Avaya Microsoft	Data from the subnets or devices in question is discarded by the collection device. Select the **Enabled (Sending Only)** option if you still want to see data from calls placed to monitored Locations by the phones in the excluded subnets.
Disable thresholds for selected Locations	Cisco Avaya Microsoft	Data from the hosts in question is still monitored, but it is shown in reports as "Unrated," and performance Incidents are not created.

Some tips:

Generally, it is a better practice to disable monitoring per-Location or per-media device rather than to disable thresholds. However, either approach should be taken with caution. If monitoring is disabled, some volume statistics (particularly in the Capacity Planning reports) might become less reliable. In addition, disabling monitoring also disables the automatic discovery of media devices in the affected subnets. And if thresholds are disabled, data rating is also disabled; this means that in some detailed data views, data collected with the disabled thresholds applied is rated as "Normal," even if it isn't.

The option to enable monitoring in a single direction (the **Enabled [Sending Only]** option) might be more appropriate for your situation. The term *Sending* refers to the direction in which the call data is traveling. UC Monitor reports take the perspective of the listener to gauge call quality; the "Sending" direction thus refers to outbound call legs that users of the phones in the selected Location are not hearing. If you select this option instead of completely disabling monitoring for the default ("`Unassigned`") Location, you'll still see data for incoming calls placed by phones in the PSTN.

See "Adding Locations" on page 108 for information about disabling monitoring for a Location. The steps are similar for a voice gateway or other media device.

The topic titled "Disabling Incidents for a Threshold Metric" on page 174 provides instructions for disabling monitoring for a single performance threshold metric. To disable the thresholds for an entire Location, follow the same steps to edit the threshold settings. On the Threshold Properties page, click to select **None** from the units menu for all audio and/or video metrics, in both the **Degraded** and **Excessive** columns of the Thresholds table. Save the threshold settings with an easily identifiable name. Then assign the threshold settings to the Locations that you want to exclude from Incident reporting.

If you plan to routinely exclude selected Locations from threshold monitoring, you should create two custom sets of call performance thresholds, one for call setup and one for call quality. Edit these performance thresholds to disable all metrics (that is, select **None** for all units). That way, when you want to exclude a Location, you can quickly assign a "disabled" set of thresholds to it.

Disabling thresholds is a less-precise method of filtering report data than disabling monitoring. In a Cisco environment, you can change SPAN port configuration (by setting up an ACL that excludes the selected hosts or subnets from the SPAN session) so that the phones and gateways at the selected Location are not monitored at all. For other types of deployment, you must edit Location or media device definitions to disable monitoring. Otherwise, data is still collected from those devices and appears as "Unrated" in reports, with a gray color in charts.

Editing Locations

You can edit a Location definition that you have created to change its name, add or remove a subnet, or add a description to help identify the Location. Some parameters of the pre-defined Locations can also be edited.

If you plan to edit a large number of Locations, you might save time by exporting the current Location definitions into a spreadsheet, deleting the current definitions, modifying any desired parameters in the spreadsheet or selecting a custom domain, and re-importing them. See the following topics for more information:

- "Making Changes to Domain Assignments" on page 260
- "Importing Location Definitions" on page 112

The Location Properties page lets you modify the Location name or description, view the subnets that are currently configured for the selected Location, and add, edit, or delete subnets.

To edit the properties of a Location:

1. In the navigation links, click **Administration > Data Collection > Locations**.

   The Location List page is displayed.
2. In the Location List, find and select the Location you want to modify.
3. Click **Edit**.

   The Location Properties page is displayed.
4. The **Name**, **NPC Domain**, **Key Phone Address**, and **Description** parameters can be edited. You can add, modify, or delete the information in these fields.

   You can also disable monitoring of this Location by selecting **Disabled** from the **Monitoring Status** list.

   See "Adding Locations" on page 108 for information about the options on the Location Properties page.
5. The table of subnets shows the subnets that are already configured for this Location. Select a subnet and click **Edit** to modify an existing subnet definition.

   Or click **New** to add an additional subnet. See "Tips about Location Subnets" on page 107 for information about Location subnet definitions.

   Delete a subnet by selecting it, clicking **Delete**, and then confirming the Delete operation by clicking **Delete** on the confirmation page.
6. Click **OK**.

You return to the Location List page. The changes are reflected in the list.

Importing Location Definitions

For cases where many distinct Locations are needed to organize your VoIP and video monitoring system, or where the network contains a large number of subnets, Unified Communications Monitor provides a Location and subnet import feature.

The import feature may be used for both initial UC Monitor configuration and subsequent additions of Locations and subnets. The import wizard does not allow you to edit or delete Locations; however, once you have imported the definitions, you can easily edit and delete them from the Location List page.

The Location and subnet import procedure imports data from a file in comma-separated values (`.csv`) file format. Spreadsheet programs, such as Microsoft Excel, can read and save files in this format. The required syntax for the data to be imported is provided in the online Help and discussed below.

We recommend that you read "Advice for Setting up Locations" on page 5 before you start creating a `.csv` file. Then use the documentation about your network architecture to plan the Location definitions you need and create the `.csv` file. The basic syntax is to separate items with commas (,) and no spaces.

Domain definitions are not included in the supported syntax and are selected as a separate step during the import operation. To expose the **NPC Domain** parameter that allows you to import Locations into a domain container, you must first create the domain group definition in the NetQoS Performance Center. See "Monitoring by Domain" on page 255 for more information.

Note: The monitoring status of imported Locations is always set to **Enabled**. To disable monitoring of an imported Location, select it in the Location List and click **Edit**.

The following table provides details:

Data Type and Syntax	Notes and Examples

Location definition (complete):
`LOCATION,LocationName,"Location Description",Key Phone IP Address`
	The quotation marks are only needed to enclose strings that contain commas, double quotation marks, or other punctuation.
	Examples:
	`LOCATION,Austin,"All phones, Third Floor at HQ",14.5.67.89`
	`LOCATION,"Sales - Milwaukee",Branch office,12.34.5.67`

Subnet definition (complete):
`SUBNET,LocationName,SubnetName,Subnet IP Address,Mask`
	`LocationName` must correspond to a defined Location.
	Mask must be a value of 1 to 32, inclusive.
	See "Tips about Location Subnets" on page 107 for advice.
	Examples:
	`SUBNET,Austin,Marketing - Austin Office, 192.168.104.0,24`
	`SUBNET,Sales - Milwaukee,Remote Sales,10.12.34.0,30`

Location definition (no description):
`LOCATION,LocationName,,Key Phone IP Address`
	Location description and key phone IP address are optional.
	Examples:
	`LOCATION,Marketing - Raleigh Office`
	`LOCATION,Finance,,14.15.167.89`

Data Type and Syntax	Notes and Examples

Subnet definition (no subnet name):
`SUBNET,LocationName,SubnetName,Subnet IP Address,Mask`
	Subnet name is optional.
	Note that `LocationName` is *required* for subnets.
	Examples:
	`SUBNET,Marketing - Raleigh Office,,192.168.104.0,24`
	`SUBNET,Finance,,10.12.34.0,30`

When you have created an appropriate `.csv` file, you are ready to import Locations and subnets.

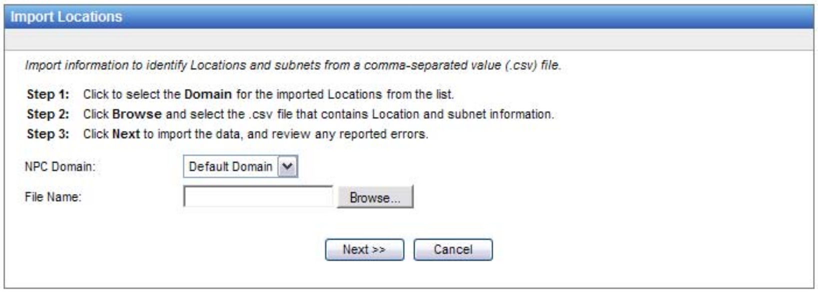
To import Location and subnet definitions:

1. In the navigation links, click **Administration > Data Collection > Locations**.

   The Location List is displayed.

2. Click **Import**.

   The first page of the Import Locations wizard is displayed:



Import information to identify Locations and subnets from a comma-separated value (.csv) file.

Step 1: Click to select the **Domain** for the imported Locations from the list.
Step 2: Click **Browse** and select the .csv file that contains Location and subnet information.
Step 3: Click **Next** to import the data, and review any reported errors.

NPC Domain: Default Domain
File Name:

3. (*Optional.*) Select a custom domain for the **NPC Domain** parameter.
4. Click **Browse**, and browse to the `.csv` file that contains your Location and subnet definitions.
5. Click **Next**.

   The UC Monitor software analyzes the file and reports any syntax errors.

6. Correct any errors in the file and save it. Then repeat Steps 3 and 4.
7. If no errors are found, the import operation is completed, and a confirmation page is displayed. The appropriate database objects are created.
8. Click **OK**. You return to the Location List page.

The new Locations are shown in the list.

Exporting Location Definitions

If new subnets have been created in your network, call traffic from those phones is labeled as “`<Unassigned>`” until you create a Location definition for those subnets. Adding new Location definitions to accommodate new subnets is required to keep the monitoring configuration current. The Location List page in UC Monitor Administration provides a list of all Locations in the system, but because a single Location can contain multiple subnets, this page does not list the subnets associated with each Location.

To see a list of all currently defined Locations and their associated subnets, use the Location and subnet export feature. This feature creates a file in comma-separated values (`.csv`) file format that lists Location names, subnet IP addresses, and masks. Spreadsheet programs, such as Microsoft Excel, can read and save files in this format. The resulting file can be used to keep an up-to-date record of UC Monitor configuration.

Note: Only the **Location Name** and any associated subnets are exported. The **Key Phone**, **Domain**, **Monitoring Status**, and **Description** parameters are not exported.

To export the current Location List:

1. In the navigation links, click **Administration > Data Collection > Locations**.

   The Location List is displayed.
2. Click **Export**.
3. The File Download dialog box is displayed. You are asked whether you want to open or save the file. For fastest download times, click **Save**.
4. Enter or browse to the file save location and click **OK**.
5. The current list of Location names and their associated subnets is exported to a file in `.csv` format. The filename begins with `UCMLocationsExport` and includes the date and time you exported the information.
6. When the file has been created, the Download Complete dialog box provides an option to open it.

The new file can be imported via the Location import feature discussed above in "Importing Location Definitions," but this method is only useful for sharing configuration data among separate UC Monitor Management Consoles. You cannot re-import any Locations or subnets because the existing definitions are then treated as "overlapping" subnets, which are not supported. Instead, you should use the export feature to check configuration currency and find areas where updates are needed. Or you can export Locations to a `.csv` file, modify parameters, delete the current definitions, and reimport them with the new parameters.

Location Pairs

UC Monitor call quality performance thresholds are applied to pairs of Locations, to pairs of Locations and media devices, or to pairs of media devices. You can customize the default call quality threshold settings and then apply the new settings to pairs of Locations and/or media devices.

Note: Call *setup* performance thresholds are assigned to individual managed items, not to pairs of items. Thresholds cannot be assigned to *groups* of Locations and devices.

After you've added some Locations to your system by taking the steps outlined in "Adding Locations" on page 108, change the default thresholds for selected pairs of Locations and voice gateways by accessing the Call Quality Thresholds page. (In the navigation links, click **Administration > Policies to see the links to Call Setup and Call Quality Threshold customizations**).

The Call Quality Threshold Assignments page lets you apply new call quality threshold settings to specific pairs of Locations and/or voice gateways. For more information about changing the default thresholds, see "Customizing Performance Thresholds" on page 162.

Baseline Traceroutes

Unified Communications Monitor calculates baseline routes by running regular traceroutes to selected Cisco IP phones and all media devices that support this feature. The route information appears in the Traceroute Investigation Details Report. The key phone serves as the target device for the traceroutes at each Location. These “routine” traceroutes are a Cisco-only feature. By default, all Cisco voice gateways are targets for traceroute monitoring unless you explicitly disable routine traceroutes. See “Adding a New Voice Gateway” on page 124 for more information.

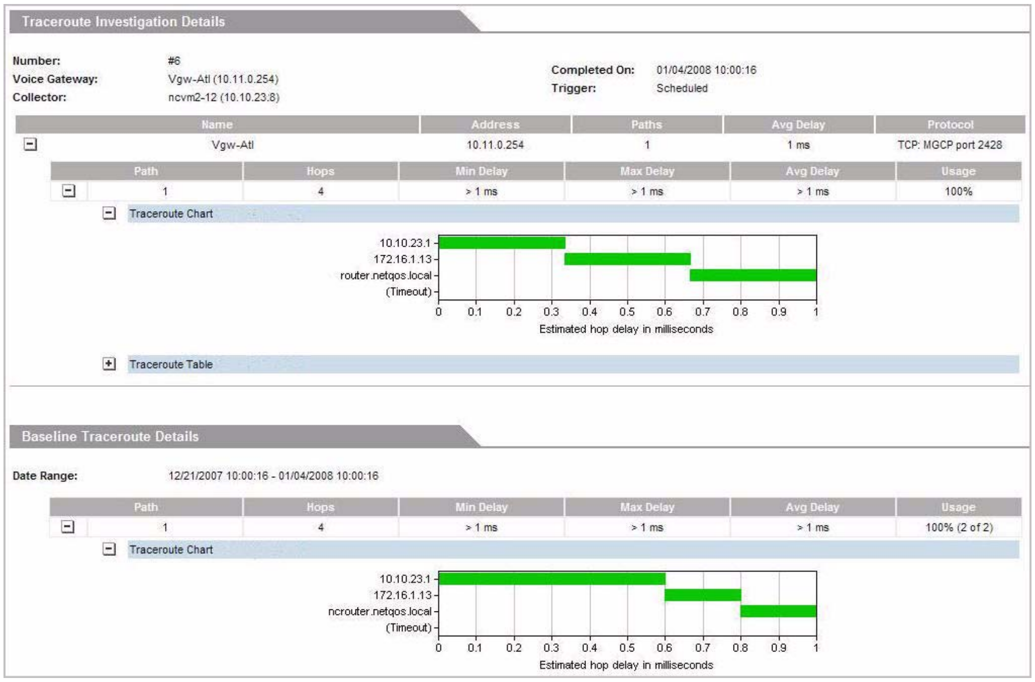
Note: Routine traceroutes to derive a baseline route are not supported by media devices or voice gateways in Microsoft or Avaya deployments. To find out more about a particular Avaya call path, try performing a Traceroute Investigation with the phone, gateway, or Communication Manager as the target. See “Launching a Traceroute Investigation” on page 205 for more information.

Routine traceroutes are launched every four hours, starting at 2:00 AM. The schedule is determined by the time zone of the Collector, but the times that appear in reports reflect the Management Console time zone.

In general, only one Collector will run a routine traceroute to a target, but under certain circumstances, multiple Collectors might run traceroute tests to the same target. In such a case, baseline path results are less accurate: different Collectors are likely to get different results, and baselines are calculated based on the frequency of path results. The main Investigations Report page therefore identifies the Collector that performed the traceroute.

Each test uses a data payload size of 0 bytes, with DiffServ ToS bit settings appropriate for VoIP call setup traffic (CS3), and it includes a timeout setting. For more information about baseline traceroute testing, see the “Baseline Traceroutes” topic in the online Help.

Baseline traceroute data can be viewed in the Investigation Details report. Tables of data from baseline testing can then be compared with any data taken from traceroutes that were launched automatically, in response to an Incident, or that were launched on demand. Here’s an example:



Traceroute Investigation Details

Number: #6
Voice Gateway: Vgw-Atl (10.11.0.254)
Collector: ncvm2-12 (10.10.23.8)
Completed On: 01/04/2008 10:00:16
Trigger: Scheduled

Name	Address	Paths	Avg Delay	Protocol
Vgw-Atl	10.11.0.254	1	1 ms	TCP: MGCP port 2428

Path	Hops	Min Delay	Max Delay	Avg Delay	Usage
1	4	> 1 ms	> 1 ms	> 1 ms	100%

Traceroute Chart

Traceroute Table

Baseline Traceroute Details

Date Range: 12/21/2007 10:00:16 - 01/04/2008 10:00:16

Path	Hops	Min Delay	Max Delay	Avg Delay	Usage
1	4	> 1 ms	> 1 ms	> 1 ms	100% (2 of 2)

Traceroute Chart

If you have not defined any key phones at your Locations, no baseline traceroute data is collected from phones. See “Adding Locations” on page 108 for more information.

Configuring Media Devices

Unified communications systems require specialized devices to handle call routing from the PSTN, or perform other functions, such as handling conference calls or transcoding media streams. The Media Devices area of UC Monitor Administration includes information about voice gateways, Mediation Servers, Conferencing Servers, and Unified Messaging servers.

The media devices that are active in a Cisco environment are different from those required to support Avaya unified communications or Microsoft voice and video. And Unified Communications Monitor provides different types of monitoring support for these devices.

Unlike UC Monitor Locations, which you define yourself, media devices are automatically added to the database as soon as calls passing through them are detected. The Collector identifies active voice gateways and attempts to contact them using the default SNMP profile. It also identifies Microsoft media devices and does not attempt to contact them, but reports information about them on the Other Device List page and includes them in performance reports.

The following topics provide detailed information about the media devices you can monitor with Unified Communications Monitor and the options you have for viewing media device data in reports.

Important: If you are monitoring a Cisco environment, you need to supply SNMP community and/or security information about your voice gateway devices. See “Working with SNMP Profiles” on page 234 for more information. If you are monitoring a Microsoft-only or Avaya-only environment, no configuration of media device information is required. However, because some devices straddle several functional categories and are difficult to identify, you can improve reporting by adding media devices to the database. See "Adding a Device to the Other Device List" on page 131.

About the Media Devices Category

Media devices in a **Cisco** VoIP deployment are generally known as **voice gateways** or **VoIP gateways**. They primarily function to route VoIP phone calls to and from the Public Switched Telephone Network, or PSTN. Thus, they act as "gateways" from your private network out into the larger world of analog telephony. They are essential VoIP components and must not only be available, but also performing well at all times.

Voice gateway devices provide important information about call performance and quality. The Collector polls Cisco voice gateways for performance data about the calls that enter your VoIP network from the public telephone network. By default, the Collector also runs a traceroute to each Cisco voice gateway every four hours to establish a baseline of data about paths through the network. This "baseline traceroute" option can be disabled when you add or edit a voice gateway definition.

By contrast, in a **Microsoft** or **Avaya** environment, media devices, while still playing an essential role in call routing and processing, do not provide useful metrics via SNMP. In these types of UC deployment, several types of device may be in use, including Mediation Servers, Conferencing Servers, and Unified Messaging Servers. Unified Communications Monitor still monitors the performance of the call legs they handle and includes their performance metrics in the media device views in UC Monitor performance reports. But SNMP polling is not enabled for these devices. Similarly, no baseline traceroute data is available from the media devices in a Microsoft Office Communications Server or Avaya system.

More about Voice Gateway Monitoring

After your collection devices have been active for several hours, the UC Monitor Administrator needs to review the list of discovered voice gateways, add gateways if necessary, and supply the correct SNMP community or other security parameters to allow the Collector to poll Cisco gateways for management information. The SNMP community or SNMPv3 security parameters for a gateway device allow the Collector to poll it for status and call performance information from its MIB.

You can also add a voice gateway definition to your system. You might want to do this if:

- some analog phones in the system are connected to a Cisco **VG-224** gateway device. These gateway devices allow up to 24 analog phones to connect to the call server; however, they can appear incorrectly in reports unless you add them as gateways.
- your unified communications network includes gateways that are in different SNMP communities, or that support different versions of SNMP. Any new gateway definition can be associated with an appropriate *SNMP profile*, which contains gateway-specific security parameters.
- you suspect that SNMP community information is incorrect or needs to be updated. The procedure for adding a new voice gateway includes an option to verify the SNMP security parameters and make sure the Collector can poll the device.
- you want to set up custom groups of devices and Locations in the NetQoS Performance Center. Groups allow you to grant view access to UC Monitor data when you configure user accounts.

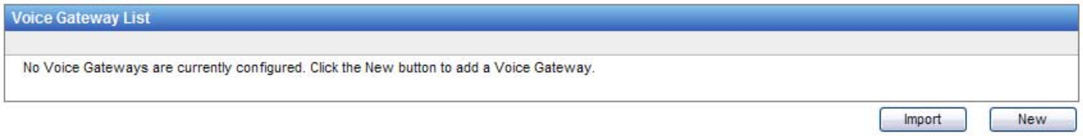
Voice gateways should be included in each user’s permission groups. See “Grouping and Permissions” on page 245 for more information.

Gateway interfaces cannot be added; however, interface parameters can be edited. See “Editing a Gateway Voice Interface” on page 123 for more information.

In a Microsoft-only or Avaya-only environment, SNMP polling and baseline traceroute monitoring of media devices are not performed. No configuration of media devices is therefore required. See “Viewing the List of Other Media Devices” on page 128 for information about the types of devices that are discovered from monitoring Microsoft Office Communications Server 2007.

Viewing the List of Voice Gateways

After data has been collected from your system for a few hours, the Voice Gateways Administration page lists all the voice gateway devices that have been discovered on your network. In the navigation links, click **Administration** > **Data Collection** > **Media Devices > Voice Gateways** to view the list of gateways that have been detected. If no gateways have been detected, a message appears:



No Voice Gateways are currently configured. Click the New button to add a Voice Gateway.

Note: Until a user has made or received a phone call involving the PSTN, no voice gateways will have been discovered. A message states, “`No voice gateways are currently configured.`” Wait for a few more hours, and then check the list again to see whether the gateways in your system have been discovered.

As soon as any gateways have been added to the system, you can view information about them in the Voice Gateway List. The hostnames and IP addresses of all gateways detected by the Collector or manually added to the system are included. The following table explains the information you see on the Voice Gateway List page:

Field or Column	Description
Voice Gateway	The name of the gateway device.
NPC Domain	The domain, actually a custom group defined in the CA NetQoS Performance Center, with which call data from this device is being associated. ***Note:*** This parameter is not visible unless Unified Communications Monitor is registered to a NetQoS Performance Center instance where at least one custom domain has been created. For more information, see “Monitoring by Domain” on page 255.
Monitoring Status	Indicates whether this device is enabled for monitoring. For more information, see “Editing a Voice Gateway” on page 120.
SNMP Profile	The name of the SNMP profile associated with this device. The SNMP profile contains SNMP security information, such as the community string, which is required to poll voice gateway devices. Unless you have changed it, the Collector uses a default profile for SNMPv1 or SNMPv2C. See below for more information.

Field or Column	Description
Voice Interfaces	The number of voice interfaces detected on the gateway device.
Address	The IP address of the gateway device.
Perform routine traceroute	Indicates whether baseline traceroute monitoring of this gateway device is enabled. By default, routine traceroute testing is enabled for each new Cisco gateway device. The gateway devices in Avaya and Microsoft deployments do not perform call setup and therefore do not need to provide baseline data for investigations. If this option is enabled, routine traceroutes are run to this device every four hours to establish a baseline of data about common paths through the network. For more information, see “Baseline Traceroutes” on page 116.

To access information about the gateway voice interfaces that have been discovered on a gateway, click to select the gateway in the list, and click **Edit**. See the following topic for more information.

By default, the Collector attempts to poll all the Cisco voice gateways it finds in the network using the default SNMP profile. The default profile instructs the Collector to use SNMPv1/SNMPv2C and the community string “`public`” unless you change it. You should update the UC Monitor default SNMP profile to match the one most commonly used in your network. The topic titled “Editing an SNMP Profile” on page 238 provides more information.

And if multiple SNMP communities are in use in your UC system, you must:

- Create new SNMP profiles with the correct community string or SNMPv3 security parameters
- Edit the appropriate gateway definitions to use the new SNMP profiles.

In cases where all Cisco voice gateways in your system use the same SNMPv1/2C community, you can edit the default SNMP profile to supply the correct information. For any single SNMP profile you create, you can check the **Use as Default** option so that the Collector always uses the information in that profile to contact new gateways as they are discovered.

See “Working with SNMP Profiles” on page 234 for a full discussion of SNMP profiles.

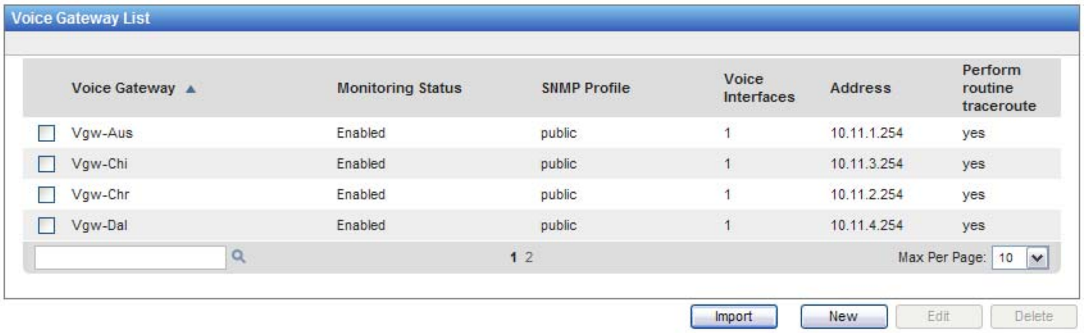
Editing a Voice Gateway

The Collector detects voice gateways on your network as soon as those gateways route calls to your call servers. It adds the gateways it detects to the database and immediately begins polling them if they respond to the default SNMP community.

The Voice Gateway List provides information about voice gateways that have been detected on your network and lets you manually edit information about the voice gateways in the database, including the community string to use to contact each one.

To edit the properties of a voice gateway:

1. In the navigation links, click **Administration > Data Collection > Media Devices**.
2. Click **Voice Gateways**.
3. The Voice Gateway List page is displayed.



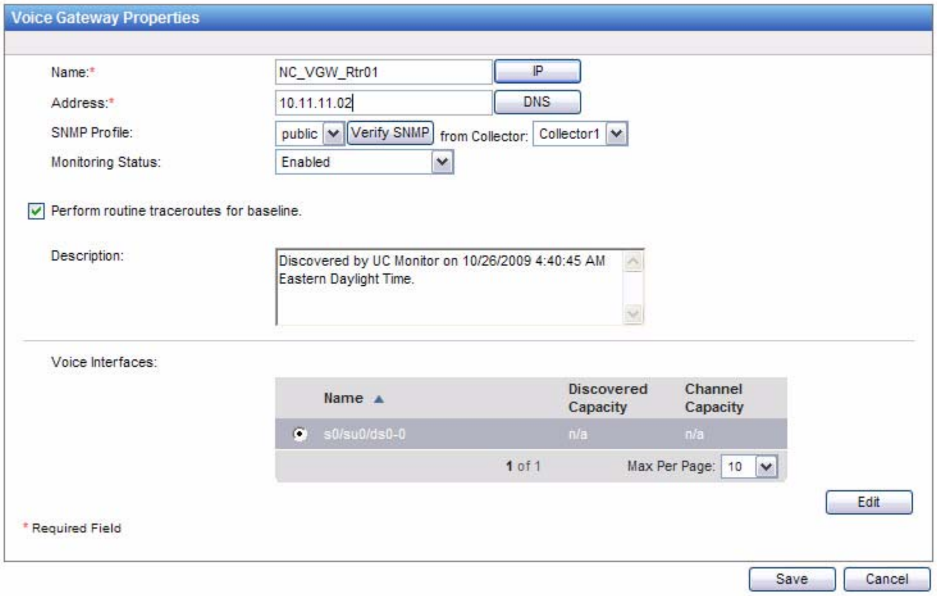
Voice Gateway List

	Voice Gateway ▲	Monitoring Status	SNMP Profile	Voice Interfaces	Address	Perform routine traceroute
□	Vgw-Aus	Enabled	public	1	10.11.1.254	yes
□	Vgw-Chi	Enabled	public	1	10.11.3.254	yes
□	Vgw-Chr	Enabled	public	1	10.11.2.254	yes
□	Vgw-Dal	Enabled	public	1	10.11.4.254	yes

4. Click to select the voice gateway whose properties you want to edit.

5. Click the **Edit** button.

   The Voice Gateway Properties page is displayed:



Voice Gateway Properties

Name:* NC_VGW_Rtr01

Address:* 10.11.11.02

SNMP Profile: public Verify SNMP from Collector: Collector1

Monitoring Status: Enabled

☑ Perform routine traceroutes for baseline.

Description: Discovered by UC Monitor on 10/26/2009 4:40:45 AM Eastern Daylight Time.

Voice Interfaces:

	Name ▲	Discovered Capacity	Channel Capacity
●	s0/su0/ds0-0	n/a	n/a

6. Edit the following information for a voice gateway:

Property	Description
Name	A name for the voice gateway device. Typically, the DNS hostname, although you can enter any name you choose. If you do not know the DNS hostname, enter the IP address in the **Address** field and click the **DNS** button.
IP	Click to find the IP address that corresponds to the DNS name you typed.
Address	Enter the IP address of the voice gateway device. Use dotted notation, such as `10.10.2.34`. If you do not know the IP address, enter the server DNS hostname in the **Name** field and click **IP**.
DNS	Click to find the DNS hostname that corresponds to the IP address you typed.

Property	Description
NPC Domain	The domain, actually a custom group defined in the CA NetQoS Performance Center, with which call data from this device is being associated. ***Note:*** This parameter is not visible unless Unified Communications Monitor is registered to a NetQoS Performance Center instance where at least one custom domain has been created. For more information, see "Monitoring by Domain" on page 255.
Monitoring Status	Whether to include data from this device in reports. The following options are available: • **Enabled**: Monitoring is enabled for any calls routed by this gateway device. • **Disabled**: Calls routed by this device are not monitored; data collected from them is discarded. • **Enabled (Sending Only)**: Monitoring of calls routed by this device is disabled, except for calls placed by phones in the PSTN and sent through this gateway to phones in monitored Locations. See "Disabling Monitoring of Selected Locations" on page 110 for some advice before deploying the exclusion feature.
SNMP Profile	Select the SNMP profile to associate with this gateway. The SNMP profile contains security information, such as the SNMP community string, to allow the Collector to query the MIB of this gateway device. The default SNMP profile is used unless you have created at least one custom profile and select it from the list. See "Creating a New SNMP Profile" on page 236 for more information. Unless you have changed it, the default SNMP profile uses the string `public`.
Verify SNMP	Click to instruct the Collector to try to contact the gateway using the specified SNMP profile.
from Collector	By default, the Collector that first detected the voice gateway is used for the verification. We recommend using the default Collector. If the verification fails, you can select another Collector from the list and try again. ***Note:*** If you are monitoring by domain, the domain with which the Collector is associating call data is indicated, appended to the Collector hostname.
Perform routine traceroutes for baseline	When selected, enables routine traceroute testing of this device every four hours. Results are included in the Investigation Details Report. See "Baseline Traceroutes" on page 116 for more information. Selected by default. Always disabled automatically if Monitoring Status is Disabled.
Description	Optional description to help operators identify this gateway, including its location, its capabilities, or its past performance.

The **Voice Interfaces** section reports information about the gateway voice interfaces that have been discovered on the selected voice gateway device. This information can be modified.

7. Click to select the interface whose capacity information you want to change. Click **Edit**.
8. Edit the following information for a gateway voice interface:

Property	Description
Name	The name for the gateway voice interface. By default, the interface name is based on information from the gateway and the naming convention employed by the trunking equipment. For example, a PRI-type interface is typically named something like “`Slot#/Subunit#/Trunk type-Port#/channel#`”, or `S0/SU1/ds1-0/1` (for example). You may want to edit the name to supply a more human-readable name. Enter any name you choose for this parameter.
Discovered Capacity	The maximum number of simultaneous calls that this interface can support, according to information discovered by the Collector. The Collector finds information on interface capacity using different methods for each type of gateway device or protocol. The discovered capacity is collected from the gateway MIB.
Override Channel Capacity	By default, this value is the same as the Discovered Capacity. If it is different, someone has edited it to override the discovered capacity value. See “Editing a Gateway Voice Interface” on page 123 for more information.

9. Click **Save** to save the new voice gateway properties.

Editing a Gateway Voice Interface

The Voice Interfaces section of the Voice Gateway Properties page displays information about the gateway voice interfaces that have been discovered on the selected gateway device. This information can be modified to suit your environment. Instructions are provided above, in “Editing a Voice Gateway” on page 120.

Two parameters of a gateway voice interface can be edited:

- the interface name
- its channel capacity

The Collector finds information on interface names and capacity by polling the gateway MIB.

By default, the interface names displayed on the Voice Gateway Properties page are based on information from the gateway and, therefore, on the naming convention employed by the trunking equipment. For example, a PRI-type interface is typically named something like

“`Slot#/Subunit#/Trunk type-Port#/channel#`”, or `S0/SU1/ds1-0/1` (for example).

You may want to edit the interface name to supply a more human-readable name. Multiple interfaces on the same gateway cannot have the same name, however.

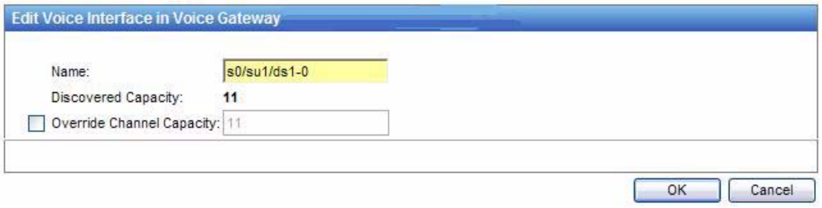
Similarly, the Voice Gateway Properties page provides the **channel capacity** of the interface as it was discovered on the system.

You may want to change the discovered capacity of the interface for various reasons that depend on your environment. For example, the device MIB may be misreporting the interface capacity. Or for capacity-planning purposes, you may want to see utilization statistics in UC Monitor reports that reflect a different call capacity for a given interface.

To change the discovered channel capacity for an interface:

1. On the Voice Gateway List page, click to select the voice gateway that contains the interface whose properties you want to edit.
2. Click the **Edit** button.
3. On the Voice Gateway Properties page, scroll down to the **Voice Interfaces** section.
4. Select the interface you want to edit in the list. Click **Edit**.

   The Edit Voice Interface page is displayed:



Edit Voice Interface in Voice Gateway

Name: s0/su1/ds1-0

Discovered Capacity: 11

□ Override Channel Capacity: 11

5. Click to select the **Override Channel Capacity** check box. Then supply a new value for the channel capacity.
6. Click **OK**.

   The new value appears in the **Channel Capacity** column of the Voice Interfaces list.
7. Click **Save** to save your changes to the Voice Gateway Properties.

Adding a New Voice Gateway

In most cases, the Collector discovers the voice gateways and other media devices on your network as soon as those devices route calls to your call servers. However, you can also add voice gateways to the database. The voice gateways you add to UC Monitor Administration can then be added to custom permission groups in the NetQoS Performance Center. If you are monitoring Cisco voice gateways, you can also associate them with an SNMP profile, enabling the Collector to poll them for call quality information.

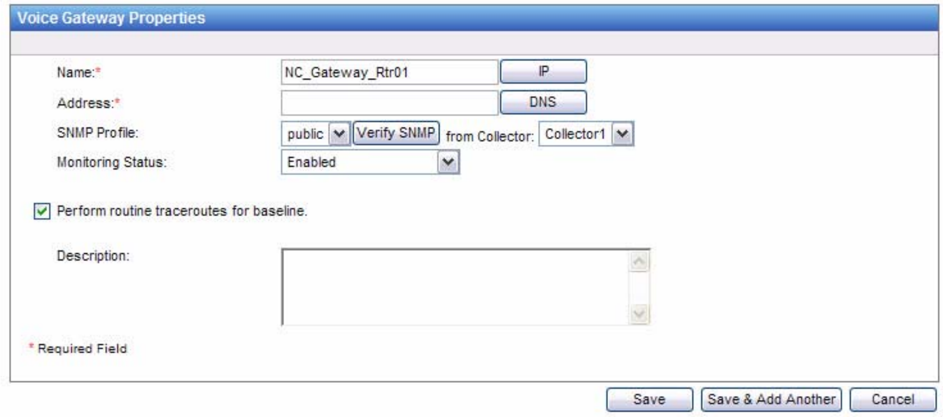
The Voice Gateway List page provides a list of voice gateways that have been detected on your network and lets you manually add voice gateways to the database.

To add a voice gateway:

1. In the navigation links, click **Administration > Data Collection > Media Devices**.
2. Click **Voice Gateways**.

   The Voice Gateway List is displayed.
3. Click **New** to add a new voice gateway to the list.

   The Voice Gateway Properties page is displayed:



Name:* NC_Gateway_Rtr01

Address:*

SNMP Profile: public from Collector: Collector1

Monitoring Status: Enabled

☑ Perform routine traceroutes for baseline.

Description:

* Required Field

See the topic titled "Editing a Voice Gateway" on page 120 for a full description of each parameter on this page.

Gateway voice interfaces cannot be added. Once you've added a voice gateway, the UC Monitor system polls the gateway and discovers information on available voice interfaces.

4. Supply the necessary information in the fields provided. Be sure to select the SNMP profile that allows the Collector to poll this device for call quality information.
5. Click **Save** to save the new voice gateway. Or click **Save & Add Another** to save these properties and then add another voice gateway to the list.

Importing Voice Gateway Definitions

For cases where the network contains a large number of voice gateway devices, you'll want to use the Unified Communications Monitor voice gateway import feature. This feature may be used for both initial UC Monitor configuration and subsequent additions of gateways.

Note: Only voice gateways that support SNMPv1 or SNMPv2C can be imported. Gateways that support SNMPv3 must be manually added to the system. See "Adding a New Voice Gateway" on page 124.

The import interface does not allow you to edit or delete gateways that are already in the system; however, once you have imported the definitions, you can easily edit and delete them from the Voice Gateway List page.

The import procedure takes data from a file in comma-separated values (`.csv`) file format. Spreadsheet programs, such as Microsoft Excel, can save files into this format. The required syntax for the data to be imported is provided in the online Help and also discussed below.

As a first step, you need to create a `.csv` file containing voice gateway definitions. Use the documentation about your UC system (that is, the hostnames, IP addresses, and SNMP communities of voice gateways) to create the `.csv` file.

For each SNMP community you supply, Unified Communications Monitor checks for the corresponding SNMP profile. If no profile is found that uses the community string you supplied in the `.csv` file, Unified Communications Monitor creates a profile for it.

For any gateway whose SNMP community you do not specify in the `.csv` file, the Collector uses the default SNMP profile when attempting to contact it. If you have created new SNMP profiles, you can set one of them as the default prior to importing the `.csv` file. Otherwise, the pre-defined default profile (for SNMP v1/2c, which uses the “`public`” community string) is used.

See “Viewing the SNMP Profile List” on page 235 for more information.

Note: The monitoring status of imported voice gateways is always set to **Enabled**. To disable monitoring of an imported gateway, select it in the Voice Gateway List and click **Edit**.

Domain definitions are not included in the supported syntax. Domains are determined on a per-Collector basis and are assigned to gateways as they are detected during monitoring. To expose the **NPC Domain** parameter that allows you to instruct the Collector to associate voice gateways with a domain container, you must first create the domain group definition in the CA NetQoS Performance Center. See “Monitoring by Domain” on page 255 for more information.

The basic syntax is to separate items with commas (,) and no spaces. The following table provides details of the import syntax:

Data Type and Syntax	Notes and Examples

Voice gateway definition (complete):
`Voice gateway name,IP address,SNMP community,Description,Traceroute`
	Quotation marks are only needed to enclose strings that contain commas, double quotation marks, or other punctuation.
	The voice gateway name can be different from its hostname.
	Only include the word “`Traceroute`” if you want to enable the option to “Perform routine traceroutes for baseline.” To disable this option, leave the `Traceroute` field blank.
	Examples:
	`Houston Data Center,10.12.34.56,private,"Data center, gateway router",Traceroute`
	`HoustonDataCtr01,10.12.34.56,private,Data center gateway router`
	`Austin_HQ_FXO,10.123.45.67,ultra5ecur3PW,VGW at HQ,Traceroute`

Voice gateway definition (no SNMP community, no description):
`Voice gateway name,IP address,,,Traceroute`
	SNMP community, description, and traceroute are optional. (The default SNMP profile is used.)
	Examples:
	`Houston Data Center,10.12.34.56,,,Traceroute`
	`HoustonDataCtr01,10.12.34.56`
	`Austin_HQ_FXO,10.123.45.67,,,Traceroute`

Voice gateway definition (no description):
`Voice gateway name,IP address,SNMP community,,Traceroute`
	Voice gateway description and traceroute are optional.
	Examples:
	`Houston Data Center,10.12.34.56,private`
	`HoustonDataCtr01,10.12.34.56,private,,Traceroute`
	`Austin_HQ_FXO,10.123.45.67,ultra5ecur3PW,,Traceroute`

Data Type and Syntax	Notes and Examples

Voice gateway definition (no SNMP community):
`Voice gateway name,IP address,,Description,Traceroute`
	SNMP community string is optional. If none is supplied, the Collector uses the default SNMP profile.
	Examples:
	`Houston Data Center,10.12.34.56,,"Data center, gateway router",Traceroute`
	`HoustonDataCtr01,10.12.34.56,,Data center gateway router`
	`Austin_HQ_FXO,10.123.45.67,,VGW at HQ,Traceroute`

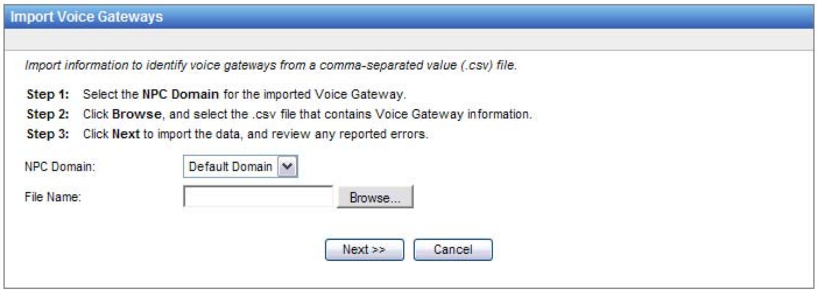
When you have created an appropriate `.csv` file, you are ready to import voice gateways.

To import voice gateway definitions:

1. In the navigation links, click **Administration > Data Collection > Media Devices**.
2. Click **Voice Gateways**.

   The Voice Gateway List is displayed.
3. Click **Import**.

   The first page of the Import Voice Gateways wizard is displayed:



Import Voice Gateways

Import information to identify voice gateways from a comma-separated value (.csv) file.

Step 1: Select the **NPC Domain** for the imported Voice Gateway.
Step 2: Click **Browse**, and select the .csv file that contains Voice Gateway information.
Step 3: Click **Next** to import the data, and review any reported errors.

NPC Domain: Default Domain

File Name:

4. (*Optional*) Select a custom domain for the **NPC Domain** parameter.
5. Click **Browse**, and browse to the `.csv` file that contains your gateway definitions.
6. Click **Next**.

   The UC Monitor software analyzes the file and reports any syntax errors.
7. Correct any errors in the file and save it. Then repeat Steps 3 and 4.
8. If no errors are found, the import operation is completed, and a confirmation page is displayed. The appropriate database objects are created.
9. Click **OK**.

   You return to the Voice Gateway List page.

The new voice gateways are shown in the list.

Viewing the List of Other Media Devices

In a Microsoft environment, several types of server fall into the UC Monitor “Media Devices” category. Like Cisco voice gateways, these servers play an essential role in call routing and processing, but because they are not contacted via SNMP, they are not monitored in the same way as Cisco voice gateway devices.

A Microsoft UC deployment may include several different types of device to support voice and video calls, conferencing, and voice mail. These devices are discovered by Unified Communications Monitor, and information about their IP address and when they were discovered during call performance monitoring is provided on the Other Device List page. The Other Devices category includes Microsoft Mediation Servers, Edge Servers (or “media relays”), Conferencing Servers, and Unified Messaging Servers. It also includes devices that do not contribute to call performance reporting by Unified Communications Monitor, but which you might want to include in a device inventory, such as unsupported types of voice gateway.

Note: Avaya devices are not included in this category. Check the Voice Gateway List for these devices.

Unified Communications Monitor still monitors the performance of the call legs that these devices handle. Both VoIP and video call performance metrics from these call legs are included in the media device views in UC Monitor performance reports. But no baseline traceroute data is available from the media devices in a Microsoft Office Communications Server system, and they cannot be included in performance threshold configuration.

To view the list of media devices in a Microsoft UC deployment:

1. In the navigation links, click **Administration > Data Collection > Media Devices**.
2. Click **Other Devices**.

   The Other Device List page is displayed.

   The following table describes the information provided in the Other Device List:

Column	Description
Device	The DNS hostname of the media device.
NPC Domain	The domain, actually a custom group defined in the CA NetQoS Performance Center, with which call data from this device is being associated. ***Note:*** This parameter is not visible unless Unified Communications Monitor is registered to a NetQoS Performance Center instance where at least one custom domain has been created. For more information, see “Monitoring by Domain” on page 255.
Monitoring Status	Indicates whether this device is enabled for monitoring. See “Editing a Media Device” on page 129 for more information.
Address	The IP address of the media device.

Column	Description
Type	The type of media device, such as Mediation Server, Conferencing Server, or Unified Messaging Server. If this value appears inaccurate, you can edit the device to select another type. See the following topic for more information about this parameter.
Description	The date and time when this device was discovered by Unified Communications Monitor.

You can edit the information that is displayed for a given device. You can also add media devices to the system. See "Adding a Device to the Other Device List" on page 131 for more information.

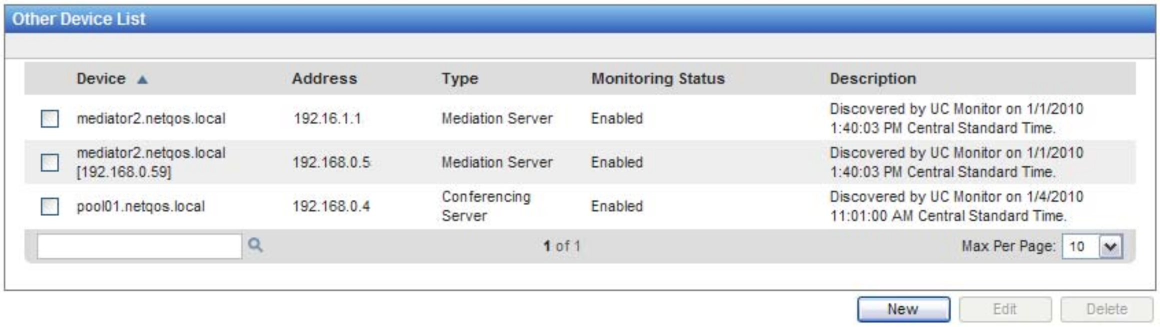
Editing a Media Device

The OCS Collector detects most media devices on your network as soon as they are involved in handling call traffic. It adds the devices it detects to the database, displays information about them in the Other Device List, and includes them in reports.

The Other Device List provides information about media devices that have been detected on your network and lets you manually edit information about any devices already in the database, such as their type and description.

To edit the properties of a media device:

1. In the navigation links, click **Administration > Data Collection > Media Devices**.
2. Click **Other Devices**.
3. The Other Device List page is displayed.



Other Device List

	Device ▲	Address	Type	Monitoring Status	Description
□	mediator2.netqos.local	192.16.1.1	Mediation Server	Enabled	Discovered by UC Monitor on 1/1/2010 1:40:03 PM Central Standard Time.
□	mediator2.netqos.local [192.168.0.59]	192.168.0.5	Mediation Server	Enabled	Discovered by UC Monitor on 1/1/2010 1:40:03 PM Central Standard Time.
□	pool01.netqos.local	192.168.0.4	Conferencing Server	Enabled	Discovered by UC Monitor on 1/4/2010 11:01:00 AM Central Standard Time.

1 of 1

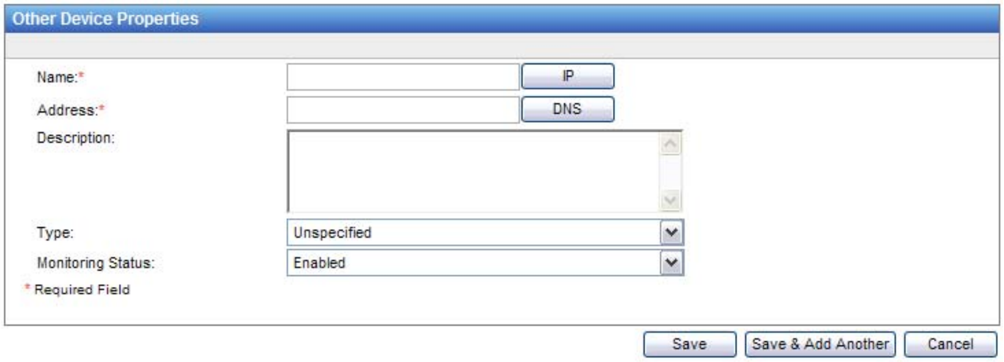
Max Per Page: 10

4. Click to select the media device whose properties you want to edit.

   You can edit devices that you added manually, or those that were automatically discovered during monitoring.

5. Click the **Edit** button.

   The Other Device Properties page is displayed:



Other Device Properties

Name:*	IP
Address:*	DNS
Description:	
Type:	Unspecified
Monitoring Status:	Enabled

* Required Field

6. Edit the media device definition. Modify or supply text for the following properties:

Property	Description
Name	A name for the media device. Typically, the DNS hostname, although you can enter any name you choose. If you do not know the hostname, enter the IP address in the **Address** field and click the **DNS** button.
IP	Click to find the IP address that corresponds to the DNS name you typed.
Address	Enter the IP address of the media device. Use dotted notation, such as `10.10.2.34`. If you do not know the IP address, enter the server DNS hostname in the **Name** field and click **IP**.
DNS	Click to find the DNS hostname that corresponds to the IP address you typed.
NPC Domain	The domain, actually a custom group defined in the CA NetQoS Performance Center, with which call data from this device is being associated. ***Note:*** This parameter is not visible unless Unified Communications Monitor is registered to a NetQoS Performance Center instance where at least one custom domain has been created. For more information, see "Monitoring by Domain" on page 255.
Description	*Optional*. Supply a description to help operators identify this device, including its location, its capabilities, or its past performance. The description appears in the Other Device List.

Property	Description
Type	The type of media device, such as Instant Messaging Client, IP phone, IP PBX, Unified Messaging Server, or Mediation Server. The **Type** parameter is used for identification purposes. It allows you to create an inventory of servers, including servers that do not contribute to call performance reporting by Unified Communications Monitor, such as a Unified Messaging Server or a voice gateway that it cannot monitor (servers with the **Voice Gateway (Unsupported)** type). Some devices play multiple roles. Once this data source is registered to the CA NetQoS Performance Center, devices are assigned generic types, such as “server” or “router.” If this value appears inaccurate for a discovered device, you can edit the device to select another type. Or you can select “**Unspecified**,” an option that causes the Collector to re-discover the device from monitored call traffic and re-assign it a type.
Monitoring Status	Whether to include data from this media device in reports. The following options are available: • **Enabled**: Monitoring is enabled for any calls routed by this media device. • **Disabled**: Calls routed by this device are not monitored; data collected from them is discarded. • **Enabled (Sending Only)**: Monitoring of calls routed by this device is disabled, except for calls placed by phones in the PSTN and sent through this device to phones in monitored Locations. See “Disabling Monitoring of Selected Locations” on page 110 for some advice before deploying the exclusion feature.

7. Click **Save** to save the media device definition and return to the Other Device List page. Or click **Save & Add Another** to create another media device definition.

The changes are displayed in the Other Device List.

Adding a Device to the Other Device List

In most cases, the OCS Collector discovers the media devices on your network as soon as those devices handle calls within the system. However, you can also add media devices to the database so that you can easily identify them in reports and place them in custom permission groups in the NetQoS Performance Center.

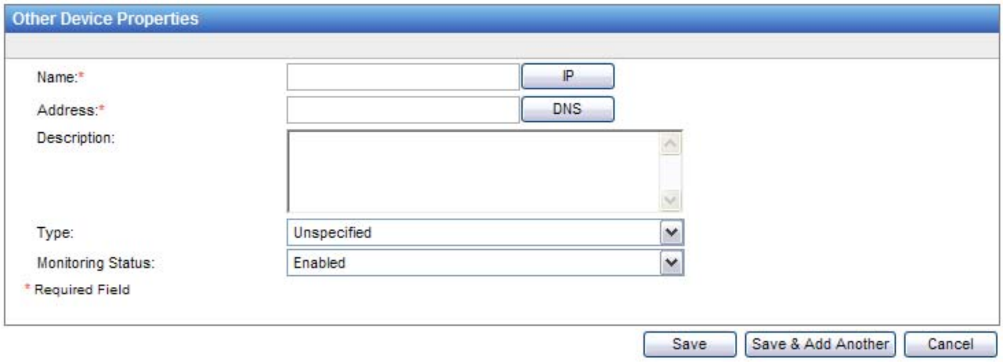
The Other Device List page provides a list of media devices that have been detected on your network and lets you manually add devices to the database. The key piece of information you need to supply about each device is its hostname or IP address. The hostname and address identify the device in the database.

To add a media device:

1. In the navigation links, click **Administration > Data Collection > Media Devices**.
2. Click **Other Devices**.

   The Other Device List is displayed.
3. Click **New** to add a new device to the list.

The Other Device Properties page is displayed:



4. Supply information in the fields provided.

   The topic titled "Editing a Media Device" on page 129 describes the available properties.

5. Click **Save** to save your changes to the media device definition and return to the Other Device List page. Or click **Save & Add Another** to create another media device definition.

The new device appears in the Other Device List. If the UC Monitor data source is registered to the NetQoS Performance Center, the device is also sent up at the next synchronization, where it can be added to groups.

Working with Call Servers and Groups

Although every UC deployment is unique, each relies on specialized server hardware and/or software to route calls, log quality data, and keep track of registered phones and endpoints. No matter which physical server takes on the main call processing tasks in a given system, Unified Communications Monitor labels it a call server and displays it as such in reports.

For the most part, call servers are discovered automatically from monitored call traffic and entered in the UC Monitor database. However, because so many different types of server might take on the call server role in a multi-vendor environment, you can also manually supply information to identify the call servers in your network.

Note: If you are monitoring Avaya, make sure SNMP information is configured for each Communication Manager so that the Collector can poll them for data. This step is taken on the SNMP Profiles page and is not a part of call server configuration. See "Viewing the SNMP Profile List" on page 235 for more information.

The ability to perform call processing in conjunction with several other servers in a cluster configuration is built into the Cisco Unified Communications Manager software. The sharing of resources, such as the Publisher database, and the failover safeguards that server clustering provides are among the many benefits of clustering. Unified Communications Monitor allows you to organize call server reporting based on *call server groups*, which correspond to these clusters of interoperating servers. Or in a Microsoft system, the servers that perform call processing can be placed in call server groups to represent their server pools.

Call server groups work in conjunction with a set of thresholds specific to call server groups. Call server group Incidents are triggered when a certain percentage of registered IP phones stop sending keepalive messages to their call server, or whenever enough new phones appear in the system to exceed a threshold value.

Note: Even though call servers from Avaya, Microsoft, and Cisco can be organized into call server groups, the call server group threshold and Incident only apply to Cisco call servers. The automatic group assignment for Microsoft call servers that belong to pools cannot be edited.

For Cisco, you can control how call server Incidents are created by first creating call server groups and then assigning call server group thresholds to these groups. For a full discussion of call server group thresholds, see "Customizing Call Server Group Thresholds" on page 181.

If you have created at least one custom domain group in the NetQoS Performance Center, an "NPC Domain" identifier is included in each call server definition. A call server's domain is also indicated in Call Performance reports. UC Monitor operators can then be prevented from viewing data from selected Locations by denying them access to selected domains via their user account role.

Domain groups are distinct from call server groups. Domain identifiers do not apply to call server groups. As a result, a situation can occur in which, based on the permissions assigned to his or her user account, a UC Monitor operator might see only call server groups in reports, but no call servers—or their associated calls.

The topics in this section explain how call server groups are used and discuss the necessary steps to take to create call server groups and assign call servers to groups.

Why Do I Need Call Server Groups?

Call server groups help you organize call servers in a way that mimics the clusters or server pools in your VoIP system. These groups are primarily useful for the following purposes:

- Identifying call server clusters or pools in reports
- Helping you to understand call volumes as reported in the Capacity Planning reports
- Creating valid permission groups so that UC Monitor operators can see the report data they need in the CA NetQoS Performance Center
- Allowing call server group thresholds to be assigned, enabling Incident creation (Cisco only)

Note: Because call server group thresholds can only be assigned to call servers that have been identified as a group, the administrative tasks required to place call servers in groups are performed in the UC Monitor Management Console. Most other tasks related to placing managed items in groups must be performed in the NetQoS Performance Center.

Call server identity is critical for the permission groups you can create and assign to UC Monitor operators in the NetQoS Performance Center. Without permission to access a call server, an operator cannot view any of the data associated with that call server. For a full discussion of call servers and their contribution to permission groups, see:

- "Call Servers and System Groups" on page 247
- "Creating Permission Groups" on page 252

As soon as a new call server is discovered, it is added to the UC Monitor database and identified as a member of the default call server group, <Unassigned>. Where Microsoft call servers are monitored and servers are running in pools, call server groups are automatically created to mimic pool identity and membership. The default group is the same in all UC Monitor data sources, which can be confusing if multiple UC Monitor data sources are all registered to the same instance of the CA NetQoS Performance Center. Your call server groups help to identify call servers in the NetQoS Performance Center.

Cisco call server groups enable Incident creation based on the call server group thresholds. The default call server group enables these Incidents automatically, but it does not identify individual clusters in UC Monitor reports.

Tips for Setting Up Call Server Groups

Most call servers are automatically discovered from monitored call traffic. By default, all call servers are placed in the default ("<Unassigned>") call server group as soon as they are discovered. After a day or two of monitoring, most of your call servers will probably have been entered into the UC Monitor database. You can verify whether all call servers have been discovered by accessing the Call Server List page, which displays information about all known call servers.

Once enough call servers are displayed in the list to represent all the clusters that are running in your system, you are ready to create call server groups. First, use the Call Server Groups Administration page to create empty groups. It's a good idea to assign these groups names that correspond to their cluster names.

Then use the Call Server List to edit each call server and select a group for it. You can do this on the Call Server Properties page. See "Adding a Call Server to a Call Server Group" on page 140 for more information.

If your environment does not contain multiple call server clusters, you should edit the "<Unassigned>" call server group and assign it the name of the cluster so that call server Incidents are reported correctly. Any new call servers that come online are automatically added to this group because it is the default group. But be aware that only one call server group can serve as the default group. This designation is indicated in the Call Server Group List, where the **Default** column states `True` for the default group.

In the navigation links, click **Administration > Data Collection > Call Server Groups** to get started.

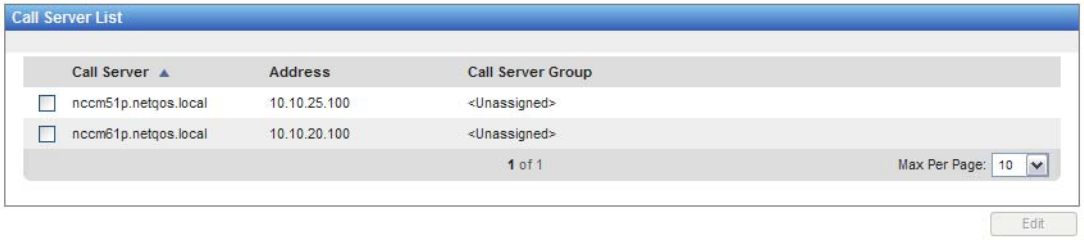
Viewing the List of Call Servers

Most call servers are discovered from call performance monitoring and automatically added to the UC Monitor database. However, you can manually add call server definitions, if desired, and organize call servers into groups. Call server groups are required if you plan to configure and use the call server group thresholds that are available for Incident reporting.

To view the list of available call servers:

1. In the navigation links, click **Administration > Data Collection > Call Servers**.

   The Call Server List page is displayed:



Call Server List

	Call Server ▲	Address	Call Server Group
□	nccm51p.netqos.local	10.10.25.100	<Unassigned>
□	nccm61p.netqos.local	10.10.20.100	<Unassigned>

The following information is provided to identify each call server:

Property	Description
Call Server	The hostname of the call server. ***Note:*** Some gateway components may be discovered and identified as call servers in an Avaya environment. See “Adding a New Call Server” on page 136 for some tips.
NPC Domain	The domain—actually a custom group created in the CA NetQoS Performance Center—with which this call server is associated. This parameter is useful for the NetQoS Performance Center Administrator in creating permission groups that place call data into separate domains, allowing the Administrator to grant operator access to call data on a per-domain basis. ***Note:*** Unless Unified Communications Monitor has been registered to a NetQoS Performance Center instance where at least one custom domain has been defined, this parameter is not visible. See “Monitoring by Domain” on page 255 for more information.
Address	The IP address of the call server.
Call Server Group	The name of the call server group of which this server is a member. By default, all newly discovered call servers are members of the `<Unassigned>` call server group. If the Management Console is registered to the NetQoS Performance Center, this group assignment is sent up to it at the next synchronization. Microsoft call servers that are running in Enterprise Edition pools are placed in call server groups automatically, based on pool identity and membership.

If you have created any call server groups, you can assign call servers from the list to these groups. Click the **Edit** button to add a call server to a group. See “Adding a Call Server to a Call Server Group” for more information.

Adding a New Call Server

In most cases, the Collector discovers the call servers on your network as soon as they route calls to registered phones or endpoints. However, you can also add call servers to the database so that you can more easily identify them in reports. Once call servers are defined, you can add them to call server groups, or to custom permission groups in the CA NetQoS Performance Center.

Adding call server definitions is especially recommended in an Avaya environment, where the identity of the Communication Manager is not easily determined from call data, or in a hybrid deployment where several different types of servers handle call processing. For example, in the case of the Avaya G650 voice gateway device, the UC Monitor Collector identifies any Controller-LAN boards (C-LANs) running on the device as separate call servers. Each of these boards has a dedicated IP address, which then appears in UC Monitor reports as a call server. However, the actual call server (Communication Manager) is usually installed on a separate media server. Once calls have been monitored for a few hours, check the Call Server List. Make sure the media server where the Communication Manager is running, the gateway device itself, and any C-LANs you want to monitor as separate devices are appropriately identified on the Call Server and Voice Gateway list pages.

The Call Server List page provides a list of call servers that have been detected on your network and lets you manually add call servers to the database. If you have created any call server groups, you can add the new server to a group as part of the call server definition.

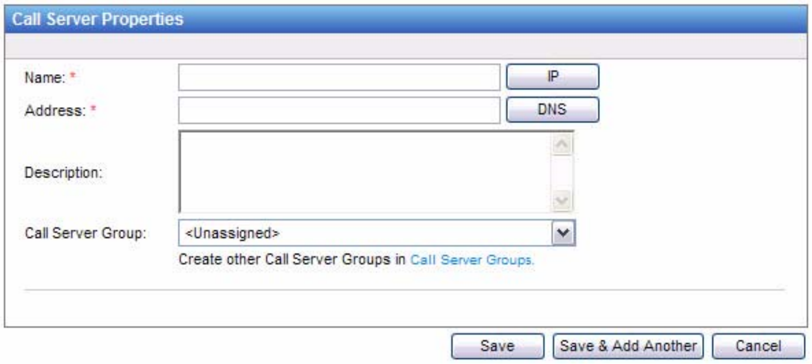
To add a call server:

1. In the navigation links, click **Administration > Data Collection > Call Servers**.

   The Call Server List is displayed. Any call servers that have already been discovered from monitored call data are displayed in the list.

2. Click **New** to add a new call server definition to the list.

   The Call Server Properties page is displayed:



Call Server Properties

Name: *

Address: *

Description:

Call Server Group: <Unassigned>

Create other Call Server Groups in Call Server Groups.

3. Supply the following information to identify this call server:

Call Server Property	Description
Name	The DNS hostname of the call server. If you do not know the hostname, enter the IP address in the **Address** field and click the **DNS** button.
IP	Click to find the IP address that corresponds to the DNS name you typed.
Address	The IP address of the call server. Use dotted notation, such as 10.10.2.34. If you do not know the IP address, enter the server DNS hostname in the **Name** field and click **IP**.
DNS	Click to find the DNS hostname that corresponds to the IP address you typed.
NPC Domain	The domain—actually a custom group created in the CA NetQoS Performance Center—with which this call server is associated. ***Note:*** If Unified Communications Monitor has not been registered to a NetQoS Performance Center instance where at least one custom domain has been defined, this parameter is not visible. See "Monitoring by Domain" on page 255 for more information.
Description	Optional description to help UC Monitor operators identify this call server, including its location, its capabilities, or its past performance.

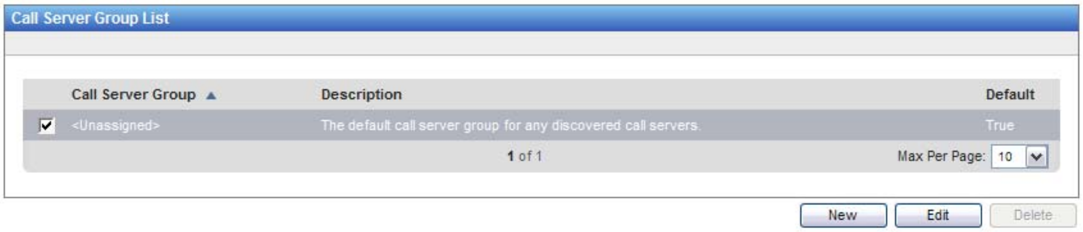
4. (*Optional*) The **Call Server Group** list contains all call server groups you have created. Click to select the group to which you want to add this call server.
5. Click **Save**. Or click **Save & Add Another** to save the information about this call server and refresh the page to add an additional call server definition.

The call server definition is added to the database, and the call server is added to the group you specified.

Note: You do not need to associate SNMP profiles with Avaya call servers, but you do need to make sure a profile is available that reflects the necessary security information to allow the Collector to poll each server using SNMP. The Collector will try each profile in turn, beginning with the default profile, until it succeeds in contacting the Communication Manager.

Viewing the List of Call Server Groups

The Call Server Group List page lists all the available call server groups. In the navigation links, click **Administration** > **Data Collection** > **Call Server Groups** to view the list of call server groups. If you have not yet created any new call server groups, only the default group, `<Unassigned>`, appears in the list.



Call Server Group List

	Call Server Group ▲	Description	Default
☑	<Unassigned>	The default call server group for any discovered call servers.	True

All Cisco and Avaya call servers are automatically added to the `<Unassigned>` call server group as soon as they are discovered. If you register the UC Monitor data source with the NetQoS Performance Center, the `<Unassigned>` call server group appears in the Groups tree under the **All Servers** system group.

Microsoft call servers are handled differently. They are placed in call server groups automatically, based on pool identity (to reflect Enterprise Edition pool structure). Pool and call server group identities are assigned slightly differently, depending on whether you are monitoring Office Communications Server 2007 or R2.

As soon as any call servers are discovered and added to the system, you can view information about them in the Call Server List. The hostnames, IP addresses, and call server group assignment is shown for each call server. See "Viewing the List of Call Servers" on page 135 for more information.

The following information about each call server group is included in the Call Server Group List:

Property	Description
Call Server Group	The name of the call server group. When you create a new call server group, you supply a name for that group. For Microsoft, the name of the Enterprise Edition pool.
Description	*(Optional)* A description of the call server group. When you create a new call server group, you have the option to provide a description to help identify it.
Default	Whether this call server group is the default group. The default call server group is automatically populated with call servers as soon as the UC Monitor system discovers them. Either true (the default group) or false (a custom group). Only one call server group can have the "default" attribute. The `<Unassigned>` call server group has this attribute by default. You can rename this group, but you cannot change the default attribute.

Click **Edit** to change a call server group name or to add or edit its description. Or click **New** to create a new call server group definition. You must add call servers to groups as a separate step. See "Creating a Call Server Group" on page 139 and "Adding a Call Server to a Call Server Group" on page 140 for more information.

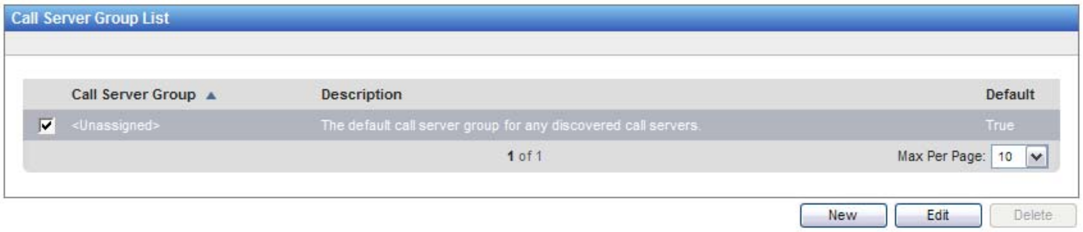
Creating a Call Server Group

Call server groups help you organize call servers for reporting purposes and assign call server group thresholds to your call server clusters. You might want to create call server groups to mimic the call server cluster configurations that are running in your VoIP system.

To add a new call server group:

1. In the navigation links, click **Administration > Data Collection > Call Server Groups**.

   The Call Server Group List page is displayed:

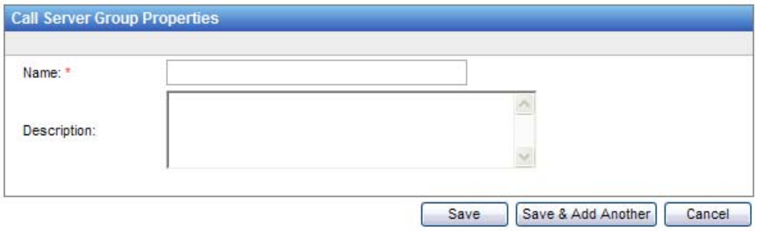
   

	Call Server Group ▲	Description	Default
☑	<Unassigned>	The default call server group for any discovered call servers.	True

   Until you create new call server groups, only the default group, `<Unassigned>`, appears in the list.

2. Click **New** to create a new call server group.

   The Call Server Group Properties page is displayed:

3. Supply a name for the call server group in the **Name** field. You will probably want to use the name of the call server cluster or server pool to help identify this group.

   Note: This name will be sent up to the NetQoS Performance Center at the next synchronization, where it will be available for group creation in the Groups tree.

4. If desired, provide a brief description of the group in the **Description** field.

   This is an optional step. The description helps to identify the group when it appears in the View Group Members pane of the NetQoS Performance Center Manage Groups page.

5. Click **Save** to save the call server group definition and return to the Call Server Groups List page. Or click **Save & Add Another** to create another call server group.

Your new group appears in the Call Server Groups List, but it does not yet contain any members. Members are added to call server groups by editing call server properties to include a group designation. See "Adding a Call Server to a Call Server Group" on page 140 for the steps.

Editing a Call Server Group

Once you've created a call server group, you can edit it to change its name or description.

To add members to a call server group, you edit **call server** properties to add a call server group designation. Click **Administration > Data Collection > Call Servers** to see a list of call servers that you can add to groups in this way. See "Adding a Call Server to a Call Server Group" on page 140 for instructions.

To edit a call server group:

1. In the navigation links, click **Administration > Data Collection > Call Server Groups**.

   The Call Server Group List page is displayed.

2. Select the call server group that you want to edit, and click **Edit**.

   The Call Server Group Properties page is displayed.

3. If desired, assign a new name to the call server group. You will probably want to use the name of the call server cluster or server pool to help identify this group.

   Note: This name will be sent up to the NetQoS Performance Center at the next synchronization, where it will be available to be added to groups of Locations in the Groups tree.

4. If desired, provide a brief description of the group in the **Description** field.

   The description helps to identify the group when it appears in the View Group Members pane of the NetQoS Performance Center Manage Groups page.

5. Click **Save** to save your changes to the call server group.

Adding a Call Server to a Call Server Group

When you create a call server group, you must add call servers to it as a separate series of steps. The call server group assignment is a call server property. Add call servers to groups by editing call servers.

Each new call server that is discovered during monitoring is automatically assigned membership in the pre-defined call server group (`<Unassigned>`). You can view call servers and call server groups in the NetQoS Performance Center if you have registered the UC Monitor data source, but unlike other groups, call server groups are managed only in the UC Monitor Management Console.

Depending on how you want to view call volume data in the Capacity Planning reports, call server groups can contain Cisco Unified Communications Managers only, Avaya Communication Managers only, Microsoft Office Communications Server 2007 servers only, or a mixture. The recommended organization of call server groups is by cluster or server pool. However, you can only assign the call server group threshold (for the Phone Status Changes Incident) to a call server group that contains at least one Cisco call server.

To add members to a call server group:

1. In the navigation links, click **Administration > Data Collection > Call Servers**.

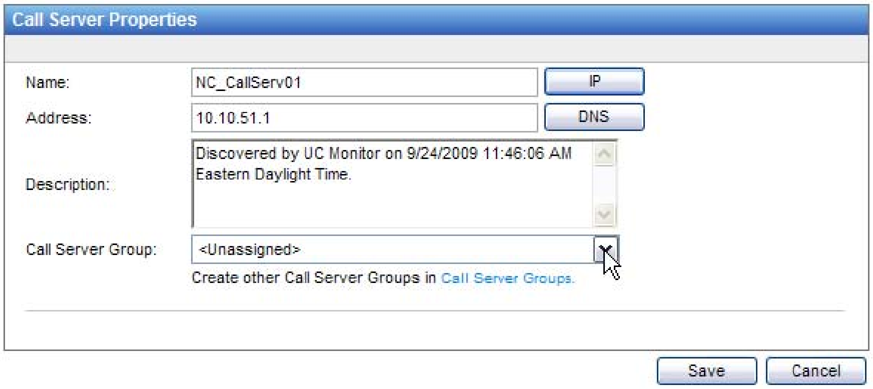
   The Call Server List page is displayed.

2. Click to select the first call server you want to add to the call server group.

Or use **Shift + Click** or **Ctrl + Click** to select multiple call servers and add them all to the group at once.

3. Click **Edit**.

   The Call Server Properties page is displayed:



Call Server Properties

Name: NC_CallServ01

Address: 10.10.51.1

Description: Discovered by UC Monitor on 9/24/2009 11:46:06 AM Eastern Daylight Time.

Call Server Group: <Unassigned>

Create other Call Server Groups in Call Server Groups.

Note: If you are monitoring by domain, the **NPC Domain** parameter is also visible. Custom domains do not apply to call server groups; only to call servers.

The **Call Server Group** list contains all call server groups you have created.

4. Click to select the group to which you want to add this call server.
5. Click **Save**.

The call server is added to the call server group. Repeat Steps 2-4 to add other call servers to this group.

CHAPTER 7

Managing Data

The UC Monitor software offers several features to transform raw data into useful information, to flag problematic performance or call server issues as soon as they're detected, and to launch automatic actions in response to poor performance. But before these features can begin to work for you, it's important to familiarize yourself with them.

Even if you plan to use the default settings for the UC Monitor performance and call server thresholds, you need to understand these settings. The performance thresholds affect almost every aspect of how collected data is handled. You need to be familiar with the default performance and codec threshold settings, to understand their intended use in monitoring voice over IP call quality and call setup, and to understand how to change those settings where appropriate. And you need to make some decisions about call server threshold settings, which can flag excessive phone registration failures and other changes in phone status.

This chapter covers the following topics:

Understanding Performance Thresholds

Performance thresholds define the boundaries of acceptable call performance or component behavior. They enable the UC Monitor software to rate collected data, and they contribute to Incident creation.

CA NetQoS Unified Communications Monitor offers two different types of performance thresholds:

- Call setup thresholds — Trigger Incidents in response to poor call setup performance metrics, such as an excessive delay to dial tone.
- Call quality thresholds — Trigger Incidents in response to poor call quality performance metrics, such as low MOS values.

Some segments of your network may habitually exhibit some minor performance issues. You have a couple of options for ensuring that Unified Communications Monitor does not launch multiple Incidents for expected behavior. You can edit the default thresholds. Or you can create custom performance thresholds and assign them to the problematic areas of the network.

The call quality thresholds provide an option to set performance expectations by codec type. You can set up codec-specific thresholds that apply only to the MOS and Network MOS metrics, or you can use the predefined thresholds that are available for most common codecs. Equally, you can choose to set fixed threshold values for the MOS metrics.

For each threshold, you can also select a sample size for Incident reporting. The two types of thresholds have different sampling units, or observations. Select a minimum number of originated calls (for call setup) or a minimum number of call minutes (for call quality) that must be observed before an Incident is created.

You can customize performance thresholds and apply them to selected Locations, media devices, or both. You can change and assign sets of performance thresholds and Incident responses for call setup and call quality. See “Customizing Performance Thresholds” on page 162 for more information.

In addition to controlling the frequency of Incident creation, performance thresholds allow the UC Monitor software to rate the collected data. For example, a call quality latency threshold of 150 milliseconds indicates a degraded condition. If that threshold is crossed, Unified Communications Monitor rates the latency data as Degraded, shown in yellow in report bar charts. In the same manner, a measurement of 400-millisecond latency would indicate an Excessive condition, shown in orange in the bar charts.

Tips for Customizing Performance Thresholds

Unified Communications Monitor allows you to customize the default performance thresholds in order to tune your system and make sure you are seeing the desired Incident frequency and severity.

The first decision to make is whether the default call quality threshold settings are the right choice for your system. The codec being used by the IP phones in your system plays a critical role in call quality. If some phones are using the G.729 codec or another low-bandwidth codec, you might need to create a new set of thresholds for them based on lower performance expectations, or based on the codec instead of on a fixed threshold value. If necessary, create a separate Location definition for those phones so that you can then apply a different set of thresholds to them.

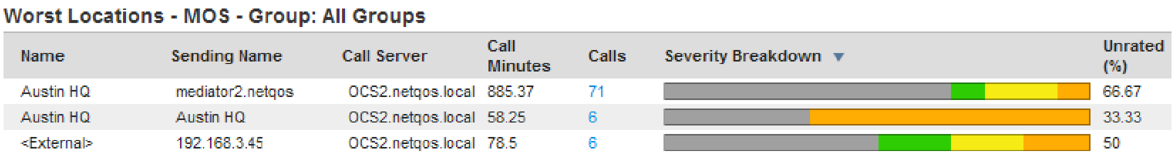
You may want to apply custom thresholds to ensure that the settings are suitable for:

- all Locations in a particular region
- all Locations in a logical network segment
- pairs of Locations that communicate with each other over a WAN link
- pairs of Locations and media devices

If a particular part of the network is known to have slightly higher network latency than the rest of your system, you can apply different thresholds for the affected Locations and media devices to make sure your network operators aren't overwhelmed with Incident notifications.

Note: Thresholds are only applied to individual managed items and not to entire groups, if custom grouping is used for devices and Locations. See Appendix A, "Working with Groups in the CA NetQoS Performance Center" on page 241 for more information about the grouping feature.

Gray-shaded areas in reports indicate that collected data is "unrated". Most commonly, data is unrated because the number of **observations** collected for a particular metric during a five-minute reporting interval did not meet the minimum threshold—either a minimum number of calls originated, for call setup thresholds, or a minimum number of call minutes, for call quality thresholds. As you are tuning performance thresholds, use the Worst Locations report as a gauge. You'll see lots of unrated data in this report if call traffic on your network is too light for the default minimum observation thresholds. Here's an example:



Worst Locations - MOS - Group: All Groups

Name	Sending Name	Call Server	Call Minutes	Calls	Severity Breakdown ▼	Unrated (%)
Austin HQ	mediator2.netqos	OCS2.netqos.local	885.37	71		66.67
Austin HQ	Austin HQ	OCS2.netqos.local	58.25	6		33.33
<External>	192.168.3.45	OCS2.netqos.local	78.5	6		50

If you see areas of unrated data like these, you could reduce the Minimum Observations setting so that more data is rated. See "Customizing Call Setup Thresholds" on page 162 or "Customizing Call Quality Thresholds" on page 169 for more information.

Call Setup Performance Threshold Settings

Customizing threshold settings is not required. The default UC Monitor performance threshold settings were selected according to a set of well-established industry guidelines to help you determine the quality of VoIP performance on your network. Different performance thresholds are used for call setup and call quality metrics. You can edit them as two distinct tasks.

For any call performance metric that is monitored by Unified Communications Monitor, two performance thresholds are available:

- Degraded Threshold— Indicates a decline in performance
- Excessive Threshold— Indicates a severe decline in performance

The following table describes the UC Monitor **Call Setup** performance thresholds and their default settings:

Metric	Description	Threshold Defaults	Minimum Observations
Delay to Dial Tone	Time elapsed from when a user enters the last digit of a telephone number to when the user hears a ring or busy signal.	2000 ms (Degraded) 4000 ms (Excessive)	5 calls originated
Post-Dial Delay	Time elapsed between a user's punching in the last digit of a telephone number and receiving a ring or busy signal.	2000 ms (Degraded) 4000 ms (Excessive)	5 calls originated
Call Setup Failures	The rate at which calls are failing during the call setup phase.	2% (Degraded) 10% (Excessive)	5 calls originated

For either the Degraded or Excessive threshold units, you can select `None` to disable the threshold. The "minimum observations" parameter lets you set a minimum number of times per reporting interval that the monitored metrics can cross the performance threshold before an Incident is created.

Threshold values are not treated as inclusive, which means that they must be actually exceeded, and not met, for an Incident to be created. For example, the highest Delay to Dial Tone metric that can be rated as normal performance is 2000 ms.

You can customize call setup thresholds and apply them to selected Locations, media devices, or both. See "Customizing Call Setup Thresholds" on page 162 for more information.

Call Quality Performance Threshold Settings

VoIP call quality is heavily dependent on the codec being used by the IP phones. A high-performing codec encodes the voice signal, breaks it into packets, and places the packets on the wire more rapidly and with less data loss than a lower-performing codec. By default, a codec-specific threshold is used for two of the call quality performance threshold metrics: MOS and Network MOS. For more information about codec threshold settings, see "Codec Threshold Settings" on page 155.

For any call performance metric that is monitored by Unified Communications Monitor, two performance thresholds are available:

- Degraded Threshold— Indicates a decline in performance
- Excessive Threshold— Indicates a severe decline in performance

The following table describes the UC Monitor **Call Quality** performance thresholds and their default settings:

Metric	Description	Default Thresholds	Minimum Observations
Audio Metrics			
MOS	Mean Opinion Score: an industry standard for gauging call quality by estimating the impact of various impairments on the listener's likely perception of the call quality. Theoretically, highest score is 5.0. In practice, highest score is probably 4.5.	Codec. See the Notes below.	15 call minutes
Network MOS	Predictive MOS listening quality metrics based on network factors alone.	Codec. See the Notes below.	15 call minutes
Packet Loss	The rate at which VoIP packets are being lost—sent, but never received.	1% (Degraded) 5% (Excessive)	15 call minutes
Jitter Buffer Loss	The rate at which packets are being lost due to jitter buffer overruns.	1% (Degraded) 5% (Excessive)	15 call minutes
Latency	Delay, or the time taken for a VoIP packet to travel between the calling parties. Measured from end to end in a single direction.	150 ms 400 ms	15 call minutes
ACOM (ERL/ ERLE)	Sum of Echo Return Loss (ERL—echo reduction from the network without echo canceling devices), echo reduction due to echo canceling devices (ERLE, or Echo Return Loss Enhancement), and nonlinear processing loss for the call. The total reduction in echo seen by the network. This metric only applies to voice gateway media devices. It does not apply to Microsoft media devices.	15 decibels (dB) 6 decibels (dB)	15 call minutes
Video Metrics			
Video Latency	Delay, or the maximum time taken for a video packet to travel between the calling parties, measured from end to end in a single direction. Calculated by taking the average round-trip time for a call leg in a given video call and dividing it in half.	150 ms 400 ms	15 call minutes
Video Packet Loss	Average network packet loss for the entire stream.	1% (Degraded) 5% (Excessive)	15 call minutes

Metric	Description	Default Thresholds	Minimum Observations
Video Frame Loss	Average number of unique consecutive images, or video frames, lost due to corruption and error concealment for the entire stream. Video frames can span multiple packets, so this threshold is useful in conjunction with the video packet loss threshold.	1% (Degraded) 5% (Excessive)	15 call minutes
Frozen Video	The frequency of long and noticeable frozen video for the whole session.	1% (Degraded) 5% (Excessive)	15 call minutes

Notes

For the **MOS** and **Network MOS** audio metrics, you have two options for setting the Degraded and Excessive thresholds:

- Select **MOS** and supply a fixed MOS value.

  Defaults are: Degraded — 4.03; Excessive — 3.6.
- Select **Codec** to instruct Unified Communications Monitor to use the codec threshold that applies to the codec being used for monitored calls. For more information about codec thresholds, see "Understanding Codec Thresholds" on page 154.

The **Minimum Call Minutes** parameter lets you set a minimum number of observations—the length of time that the monitored metrics can cross the performance threshold within a reporting interval before an Incident is created. If you are seeing a lot of "unrated" calls in the Worst Locations report, you probably need to reduce this value from the default. See "Tips for Customizing Performance Thresholds" on page 144 for more information.

Threshold values are not treated as inclusive, which means that they must be actually crossed, not met, for an Incident to be created. For example, for phones using the default threshold settings, 4.03 is the lowest possible MOS value that can be rated as normal performance.

You can customize call quality thresholds and apply them to pairs of selected Locations, media devices, or both. See "Customizing Call Quality Thresholds" on page 169 for more information.

Understanding Call Server Thresholds

In a VoIP system, call server performance and status have a powerful impact on the user's quality of experience when making or receiving calls. IP phones and voice gateway devices must register with a call server and send it periodic keepalive messages to inform the rest of the system of their status. The call server handles all aspects of call setup, including sending dial tones and ringing or busy signals, routing calls, and cleaning up resources after a call has been completed.

To help you track call server and phone status, two types of call server thresholds are available in Unified Communications Monitor:

- Call server thresholds
- Call server group thresholds

Important: The call server thresholds are designed for monitoring in Cisco environments. They cannot be applied to Microsoft or Avaya components.

While the call server thresholds must be applied to *individual* servers, the call server group thresholds must be applied to call server *groups* that you create to represent your server clusters. The two different threshold types provide more accurate Incident reporting when applied this way.

Each call server in a cluster is capable of playing several different roles to provide failover safeguards and load balancing. For example, in a Cisco Unified Communications Manager cluster, any server in the cluster can take on the call-processing role if the primary call server for a particular set of phones is taken offline for maintenance or becomes unavailable for another reason. The call server group thresholds could potentially apply to any call server in a cluster because they relate to this type of shared or redundant functionality.

Before you can apply the call server group thresholds, you must add call servers to groups, as described in "Creating a Call Server Group" on page 139.

Call Server Threshold Settings

Unlike the call server group thresholds, which are applied to call server clusters, the call server thresholds can only be applied to individual call servers.

The following table describes the available call server thresholds:

Metric	Description	Default Values
Registration Failures	Creates an Incident if the number of times a device fails to register with the call server exceeds the threshold. This Incident can indicate a configuration or security problem.	**15** failures per call server, per reporting interval Select **None** to disable this threshold. Severity is always Excessive.

Metric	Description	Default Values
Poor Call Quality QRT	Creates an Incident every time an IP phone user clicks the **QRT** soft key to report poor call quality. The QRT soft key activates the Cisco Quality Report Tool, an optional feature that the VoIP administrator can enable. See "More about the Poor Call Quality (QRT) Threshold" on page 150. Incident may be reported at two different times: • On Hook—While the phone is hung up • In Progress—During an active call	**Enabled** Severity is always Excessive.

Both of these thresholds are designed to be applied to individual call servers.

More about the Registration Failures Threshold

The registration failures call server threshold was designed to notify an administrator if one or more devices are repeatedly, but unsuccessfully, trying to register with a call server. Excessive phone registration failures can indicate a configuration problem, a call server issue, or a network issue, such as a connectivity outage.

In some cases, excessive registration failures can also indicate a security problem that can impede server performance; if a phone is trying to register from an unauthorized address, the call server will try to resolve the address but will ultimately deny the registration request. Because the call server has to respond to every device registration request, excessive device registrations use up bandwidth and can tie up the call server as it attempts to resolve device addresses and process requests.

If you see a Registration Failures Incident report, check call setup performance statistics in the Performance Overview Report to see whether problems associated with an overburdened call server have caused other issues. Then check the Phone Details related report, linked to the Incident Details report page, to see whether the registration requests are coming from an unauthorized IP address.

More about the Poor Call Quality (QRT) Threshold

The poor call quality (QRT) call server threshold is based on a feature of some Cisco IP phone models. The Quality Report Tool, or QRT, feature allows phone users to press a **QRT** softkey to report poor call quality. When the key is pressed, the Quality Report Tool collects information useful for troubleshooting the poor performance, such as jitter and packet counts, from various sources, formats the information in an IP Phone Problem report, and send it to its call server. The call server places the information in a CDR and also retains the report.

To enable this reporting feature, a Cisco Unified Communications administrator must define a softkey that an end-user can press to report a poor-quality call. The **QRT** softkey can be enabled for use while a call is in progress, after a call has completed, or at other times.

The UC Monitor Collector can detect whether the QRT softkey message has been sent, and whether a call was in progress when it was sent. If this threshold is enabled, the Collector automatically generates an Incident when it detects a QRT event.

This feature is supported by Cisco phones using the SCCP and SIP protocols. If enabled, the threshold applies to the devices that are associated with individual call servers, not to call server groups or Locations.

When a poor call quality call server Incident is reported, a Phone Details report is available as a **Related Reports** link from the UC Monitor Call Server Incident Details report page. The Phone Details related report shows call legs for the 15 minutes just before the time the QRT key was pressed and provides information needed to identify the phone where it was pressed.

If the user presses the softkey while the call is in progress, Unified Communications Monitor initiates an automatic Call Watch for the phone where the key was pressed. Data views from the Call Watch Details Report are then included in the Incident Details Report.

The poor call quality call server Incident does not have a threshold value or a severity. The threshold is enabled by default. You can disable it on the Call Server Threshold Properties page.

This Incident type is distinct from a call quality performance Incident in the sense that the call quality performance Incident is created in response to VoIP network performance metrics that cross a threshold. By contrast, the poor call quality call server Incident is triggered when a phone user presses a softkey. It’s therefore possible that a user error is involved, and no actual performance issue exists.

The usual rules of Incident closure also do not apply to this type of Incident. Because no metrics are being monitored whose improvement could trigger Incident closure, this Incident is either never in an Open state (if triggered while the phone is on-hook) or is closed automatically closed as soon as the Call Watch action is launched (if triggered while the call is still in progress).

Call Server Group Threshold Settings

Unlike the call server thresholds described in “Call Server Threshold Settings” on page 149, the call server group thresholds are designed to be applied to your call server clusters, or to other logical groupings of call servers. Each call server in a cluster is capable of playing several different roles to provide failover safeguards and load balancing. For example, in a Cisco Unified Communications Manager cluster, any server in the cluster can take on the call-processing role if the primary call server for a particular set of phones is taken offline for maintenance. The call server group thresholds could potentially apply to any call server in a cluster because they relate to this type of shared or redundant functionality.

Before you can apply the call server group thresholds, you must add call servers to groups, as described in “Creating a Call Server Group” on page 139.

The following table describes the events that could trigger a Phone Status Changes call server group Incident. The total number of all phone status changes for the group is used to trigger the Incident:

Status Changes	Description
Currently Missing Phones	The percentage of devices previously registered to this call server group that are no longer registered to (sending keepalive messages to) any of the call servers in the cluster. The missing phones total does not include any phones that had normal shutdowns (and accompanying deregistrations).

Status Changes	Description
Recently Moved Phones	The percentage of devices previously registered to a call server in this call server group, but that are currently registered to a different call server in the same group.
New/Found Phones	The percentage of devices that are registered to this call server group, but that were not registered during the previous reporting interval (five minutes ago). • A "new" phone has never registered to this call server group since monitoring with Unified Communications Monitor began. • A "found" phone has lost contact with this call server group at some point in the past, but in the last reporting interval, it registered again with the same group.

As shown in the table, different types of status change can trigger the Phone Status Changes Incident as long as the threshold value is exceeded. The default value is **50%**, which refers to a percentage of all devices that are members of this call server group and that had status changes during the 15-minute reporting interval. A "member" of a call server group (commonly a cluster) is identified in a list that is maintained by a call server and shared among the servers in a cluster.

The total percentage of phones with applicable changes must exceed, and not meet, the threshold to trigger the Incident. A single Phone Status Changes Incident is then included in the summary list of Call Server Incidents; separate data views provide information about each type of status change when you drill down into the detailed Incident report.

The Incident is not dependent on the similar information being reported in the Phone Details Reports. For example, if a Currently Missing Phones status change is reported, multiple phones in the Phones List might show a status of **Unavailable** or **Lost Contact**, but keep in mind that the status of a device being reported at a given moment is actually the device status *at the end* of the reporting interval. If a change in status occurred earlier, the Incident might be created before another status change occurs; the later status would then be reflected in the Phone Details and would be slightly out of synch with the Incident.

More about the Phone Status Changes Incident

The Phone Status Changes Incident was designed to detect failover events and branch office outages. It can also assist in improving the ability to identify call server performance issues and branch office connectivity failures that can be costly. Typically, the Incident itself provides enough information to help you identify the affected phones and call server group. However, planning Location definitions carefully makes it easier to identify the phones involved in the Incident.

In the most common scenarios, the Phone Status Changes Incident is used to report a bank of phones that have failed over to another call server, or that have gone missing from the network due to an outage. Often, call servers are shared among several remote sites, with banks of phones that may be in widely different geographical regions or that are using topologically distinct networks. Therefore, you need to be able to easily distinguish phones in branch offices that access call servers over a WAN link from other phones using a local cluster when a call server group Incident is reported.

As a best practice, you should place remote phones in a separate Location from phones local to the call server cluster. Then if the branch office phones undergo an outage or failover, the Incident notification will provide the Location name of the branch office, and the tables of information in the Incident report itself will also direct UC Monitor operators more quickly toward the phones and other equipment that need to be investigated.

If you set up representative Locations that aid in quick identification of any issues that crop up, the Incident report becomes even more valuable. For example, in your UC system, you might want to see information related to the following:

- Branch office costs (PSTN usage, or SRST hot backup to PSTN)
- Branch office status, connectivity by location
- Cluster failovers; cluster load-balancing events

Data useful for analyzing these and related issues is provided in UC Monitor reports. To ensure that you collect this type of data, you might also consider the potential value of selecting a single phone to represent a device pool, and assigning that phone its own identifying Location definition. This configuration carries a potential drawback, possibly masking problems with other phones in the same subnet because of the restriction on overlapping subnets in Location definitions. But the benefits would include the ability to identify cluster changes that cost significantly more per minute of downtime; the ability to assign multiple thresholds to each call server cluster; and a general reduction in MTTR.

The data views in the Phone Status Changes Incident Details reports can be sorted by Location to further reduce troubleshooting time. Click the column header to sort by Location.

Typical enterprise networks have offices of widely varying sizes. The ability to set multiple thresholds that report on the same cluster is beneficial if you want to know about any changes in the smallest office or segment of phones. If you follow the advice outlined above and create separate Locations for representative phones, you can then set a significantly lower phone status changes threshold for each call server group so that Incidents are reported more frequently.

We also recommend setting up an action to automatically run a traceroute investigation in response to the Phone Status Changes Incident. However, the traceroute cannot be sent unless key phones are available to serve as targets for the investigation and are also affected by the conditions that triggered the Incident. If you have set up a Launch Traceroute Investigation Incident response for the Phone Status Changes Incident, anytime enough phone status changes occur at a particular call server group to trip the threshold, the Collector does some checking to see which Locations were assigned to the affected phones. The traceroute is only launched if key phones have been defined at any of the Locations whose phones had applicable status changes. Also note that the traceroute is only launched once, even if the Incident remains open for multiple reporting intervals.

When setting up key phones, where possible, try using Skinny (SCCP) IP phones instead of SIP phones. Skinny phones send keepalive `ACK` messages every 30 seconds; they are therefore more likely to be detected as missing and to contribute to the Incident that launches the automatic traceroute investigation.

See “Setting up Incident Responses” on page 191 for more information about Incident responses.

Understanding Codec Thresholds

Codec-based thresholds supplement call quality performance thresholds to help you better understand and manage call quality. A basic component of any VoIP or video over IP component that includes a microphone, the codec encodes and decodes the audio from both ends of a telephone conversation, producing packets that can be sent and received across the network. Codec performance has a noticeable effect on VoIP and video performance.

A wide range of codecs are available to optimize VoIP or video performance, each with an accompanying set of drawbacks and benefits. In addition to the different bandwidth requirements associated with different codec types, codecs have other characteristics that can affect network performance. For example, some of the high-performance codecs do not compress the data they send and as a result, they use more bandwidth than codecs that use a compression scheme. Compression often degrades the audio signal and adds delay.

For the most part, codecs are commonly understood to provide a certain level of audio quality, which is expressed as a theoretical maximum Mean Opinion Score (MOS). The newer software-only codecs from Microsoft are unique, however, in receiving ratings for two types of theoretical maximum MOS, as well as in advertising different performance expectations in wideband and narrowband environments.

The UC Monitor codec thresholds feature provides more flexibility and accuracy when you are working with two of the call quality thresholds, **MOS** and **Network MOS**. The ability to use a codec threshold allows you to set these thresholds either relative to codec performance or relative to absolute MOS value. When you select **Codec** for one or both of these thresholds and assign the call quality performance threshold settings to a pair of Locations and/or media devices, Unified Communications Monitor automatically applies the appropriate codec threshold based on the codecs that are detected in use during monitoring.

The following topics contain more information about the codec thresholds in Unified Communications Monitor.

Codec Threshold Settings

You can modify codec threshold settings on the Codec Threshold Properties page. The Codec Threshold List page indicates the UC Monitor default threshold values for each supported audio codec. See "Editing Codec Threshold Settings" on page 189 for more information about editing these settings.

Audio codec standards typically specify a theoretical maximum MOS value, derived through testing, which represents the highest possible mean opinion score value that this codec is able to achieve in the absence of any other impairments (such as delay due to network congestion).

All codec thresholds accept MOS values from **1.00** to **5.00**, inclusive. For each codec whose threshold you customize, the value you select for the Excessive threshold must be *more severe* than the Degraded threshold value. For example, if the value for the Degraded threshold is 4.03, the value for the Excessive threshold must be *less than* 4.02, indicating a lower Mean Opinion Score and thus, a more severe decline in performance.

The following table summarizes the default codec threshold settings:

Codec	Description	Default Threshold Values
G.711a	High-performance, high-bit rate codec (64 Kbps). Uses the "A-law" sampling method; popular in Europe and Asia.	Degraded MOS: 4.03 Excessive MOS: 3.60 Network MOS: 3.30 (Degraded); 2.95 (Excessive)
G.711u	High-performance, high-bit rate codec (64 Kbps). Uses the "U-law" sampling method; popular in North America and Japan.	Degraded MOS: 4.03 Excessive MOS: 3.60 Network MOS: 3.30 (Degraded); 2.95 (Excessive)
G.722 64k	ITU-T standard wideband speech codec. With a faster sampling rate, offers high-quality audio. ***Note:*** Cisco IP phones report quality scores based on the scale for the **G.711** wideband codecs (with the same theoretical maximum MOS). The same threshold settings should be used for these two codecs.	Degraded MOS: 4.03 Excessive MOS: 3.60
G.722.1 24k	Variation of the G.722 codec with lower bit-rate compression.	Degraded MOS: 3.75 Excessive MOS: 3.35 Network MOS: 3.58 (Degraded); 3.20 (Excessive)
G.723.1	Low-bandwidth codec used by Microsoft Exchange Unified Messaging.	Degraded MOS: 3.38 Excessive MOS: 3.02 Network MOS: 2.41 (Degraded); 2.15 (Excessive)

Codec	Description	Default Threshold Values
G.726 32k	ITU-T standard adaptive differential pulse-code modulation (ADPCM) codec. A low-bandwidth codec.	Degraded MOS: 3.86 Excessive MOS: 3.45 Network MOS: 3.17 (Degraded); 2.83 (Excessive)
G.729	High-performance, low-bit rate codec (8 Kbps). Compression and coding of speech using the conjugate-structure algebraic-code-excited linear prediction (CS-ACELP) algorithm.	Degraded MOS: 3.59 Excessive MOS: 3.21
G.729A	"Annex A" to the G.729 specification. Reduced-complexity CS-ACELP codec (8 Kbps).	Degraded MOS: 3.48 Excessive MOS: 3.11
G.7.29AB	A G.729 codec that is fully compliant with ITU annexes A and B to the G.729 standard specification. Uses CS-ACELP with silence suppression.	Degraded MOS: 3.48 Excessive MOS: 3.11
G.729B	"Annex B" to the G.729 specification. Adds a silence compression scheme.	Degraded MOS: 3.59 Excessive MOS: 3.21
GSM FR	Early speech coding standard used in digital mobile phone systems. Uses a 13 kbit/s sampling rate and delivers relatively poor quality.	Network MOS: 2.49 (Degraded); 2.22 (Excessive)
iLBC	The Internet Low Bit Rate Codec. Uses an 8 kHz/16 bit sampling rate. Designed to handle lost data.	Degraded MOS: 3.57 Excessive MOS: 3.19
RTAudio NB	Microsoft-proprietary codec, Realtime Audio in narrowband mode. Uses an 8 kHz sampling rate.	MOS: 3.48 (Degraded); 3.11 (Excessive) Network MOS: 2.70 (Degraded); 2.41 (Excessive)
RTAudio WB	Microsoft-proprietary codec, Realtime Audio in wideband mode. Uses a 16 kHz sampling rate.	Degraded MOS: 3.84 Excessive MOS: 3.44 Network MOS: 3.75 (Degraded); 3.35 (Excessive)
Siren	Polycom-proprietary codec; used by Microsoft Office Communications Server 2007 for A/V conferencing. Provides high-quality audio at low bit rates. Operates at 24 kbps and 32 kbps for wideband (50 Hz - 7 kHz).	Degraded MOS: 3.66 Excessive MOS: 3.27 Network MOS: 3.40 (Degraded); 3.04 (Excessive)

Note: The proprietary Microsoft codecs, RTAudio and Siren, and a few other codecs used by Microsoft Exchange Unified Messaging, offer an option to set a threshold for Network MOS. The Network MOS metric is only available in the Microsoft Office Communications Server 2007 environment. Also be aware that the MOS scale used in the Microsoft codec implementations is different from that used by other supported codecs. For example, the MOS value used for the default Degraded threshold for the RTAudio NB codec, 3.48, does not represent exactly equivalent performance to the same value if reported for the G.729 codec.

More about Codec Thresholds

To help you set accurate performance thresholds, a substantial number of codec threshold settings have been pre-defined by CA for the most common codecs. These values are used by default for all call quality performance monitoring; however, they can also be modified to suit your specific monitoring needs.

Codec thresholds can be added, edited, deleted, or disabled by the UC Monitor Administrator. The new codec threshold settings that you add are based on the pre-defined codecs that are supported. All codec settings, including new ones you've added, appear in the Codec Threshold List. Click **Administration > Policies > Call Performance > Codec Thresholds** to see the list.

Any customizations you make to the codec threshold settings are treated as part of the custom call quality thresholds. Therefore, they are automatically assigned to any Location/media device pairs to which the associated call quality performance thresholds are assigned.

Codec threshold settings consist of Degraded and Excessive values for one of the two MOS metrics. To set custom values for both MOS and Network MOS and associate them with the same codec, create two codec thresholds with the same codec selected for the **Codec** parameter.

No "default" codec threshold is defined. Instead, if you select **Codec** for a MOS threshold and assign the accompanying set of call quality threshold values to a pair of Locations, Unified Communications Monitor applies the codec threshold settings—either pre-defined or custom—associated with any codecs it detects while monitoring calls to and from those Locations.

If a codec that is not in the list of pre-defined or custom codec threshold settings is detected, the Collector attempts to identify it based on the packet payload. If it cannot be identified, it may appear as "Nonstandard" or as "Dynamic Payload" in reports. Data from the unknown codec appears as "Unrated" because Unified Communications Monitor does not have the commonly accepted MOS thresholds for that codec. These values continue to be unrated (and assigned a gray color in the Call Details) until you assign a fixed-value MOS threshold to the affected Locations. After you assign a custom threshold, data previously collected still appears as "Unrated".

Understanding Incidents and Incident Responses

Unified Communications Monitor uses Incidents to report degraded conditions in VoIP call performance.

UC Monitor performance thresholds represent boundaries of acceptable VoIP performance. They exist by default for each monitored VoIP performance metric. As discussed above, Administrators can change thresholds to make them more or less sensitive to performance changes.

The performance thresholds trigger **Incidents**, which are records of information created when a performance threshold is crossed. Incidents are assigned sequential case numbers and reported on the Incident Report page. Each discrete type of Incident uses its own sequence.

Incident responses are associated with specific performance thresholds. You can set up one or more automatic **actions** for each Incident response. The following Incident types have thresholds that can trigger actions:

- Call Quality Incidents
- Call Setup Incidents
- Call Server Incidents
- Collector Incidents

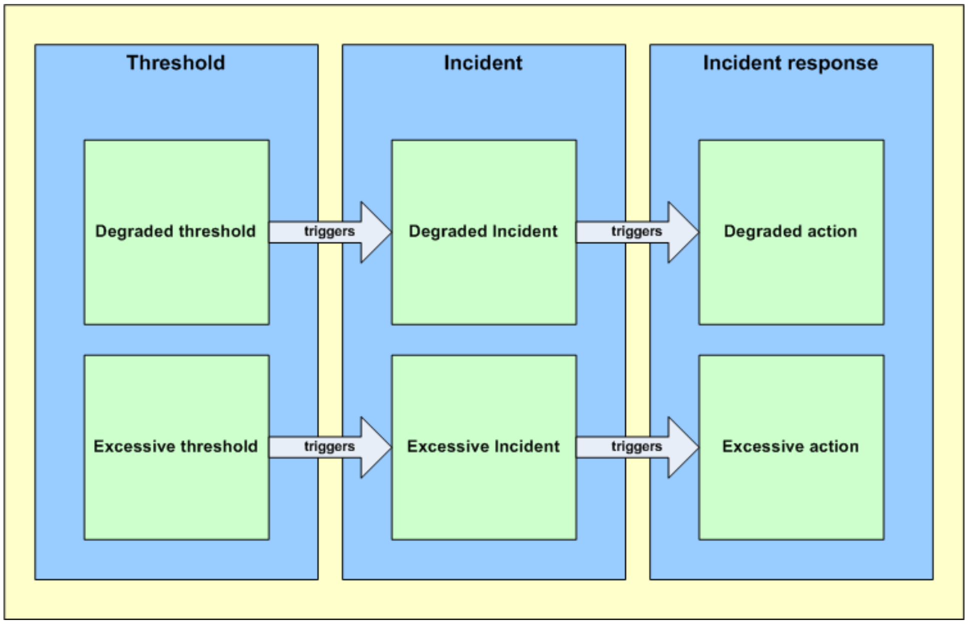
By default, no actions are triggered by UC Monitor performance thresholds. When you customize thresholds, you can select Incident responses that have associated actions. The response actions include network-specific parameters, such as email addresses that should receive automatic notifications. For a given Incident, an Administrator can specify one of the following responses:

- An action or notification to occur when performance exceeds the Degraded threshold
- An action or notification to occur when performance exceeds the Excessive threshold

The default performance thresholds generally suffice to trigger Incidents that indicate performance problems. However, you have several options for editing thresholds. For more information, see "Understanding Performance Thresholds" on page 144.

How Incidents Trigger Responses

CA NetQoS Unified Communications Monitor creates an Incident whenever it detects a performance condition on the network that exceeds a threshold. If an Incident response is enabled for that threshold condition, any associated actions are launched automatically, as shown in the following diagram:



Keep in mind the following details about Incidents, Incident responses, and actions:

- The UC Monitor system creates an Incident the first time a threshold is crossed. The Incident remains open until incoming metrics meet the criteria for automatic Incident closure. See "How Incidents Are Closed" on page 160 for more information.
- To trigger an Incident response, a violation must exceed minimum severity and duration criteria—either a minimum number of calls, or a minimum number of call minutes.
- The UC Monitor Administrator associates an Incident response with the Incident type (such as call setup, call server, or Collector) while setting up thresholds. The threshold configuration page includes an option to select an Incident response.
- By default, each Incident response has no action associated with it.

  To enable Incident response actions, you must create Incident responses, add actions to these responses, and select the responses while customizing thresholds. See "Creating a New Incident Response" on page 192 for the steps.
- For a few types of Incident, such as the Collector Abnormal Termination Incident, no applicable metrics can be monitored for improvement so that the Incident can be closed. Therefore, the Incident is briefly opened to trigger any automatic actions (such as sending an email notification), but it is immediately closed by the UC Monitor system. Any accompanying email or SNMP trap notification might indicate that the Incident is open, but in fact closure is pending.
- The traceroute investigation action should be configured as an Incident response action for call setup or call server group Incidents only.

The user interface generally allows you to select the Launch Traceroute Investigation action for other types of Incidents, such as call quality Incidents; however, the results of such investigations are usually not very helpful because traceroutes are launched from the Collector, which is located on the same switch as the call servers reporting the metrics that triggered the Incident.

For the same reason, this type of action will not be taken for Collector Incidents even if it is configured.

- If you assign the Launch Traceroute Investigation action to a call server group Incident, the Collector checks for a key phone in the Location whose phones triggered the Incident. If a key phone has been defined, it serves as the target for the traceroute.
- It is a best practice to assign the Launch Traceroute Investigation action to the call server group Phone Status Changes Incident. The information returned by the traceroute will be very helpful for troubleshooting the underlying call server or network issue.

  A traceroute investigation can also be launched independently of an Incident. For more information, see "Launching a Traceroute Investigation" on page 205.

How Incidents Are Closed

An Incident stays open until it is automatically closed. If the severity of the performance condition changes, but the metrics still violate either the Degraded or Excessive threshold, the Incident is updated to reflect the change in severity, but it is not closed.

Incidents are closed when:

- One full hour of clock time (measured from the top of one hour to the top of the next hour) has elapsed since the threshold violation occurred, and the violation has not been repeated.
- The performance condition that triggered the Incident has persisted for 24 hours. A new Incident is then opened.

The call setup Incident type can change. A call quality threshold violation overrides a call setup violation if they affect the same pair. An Incident remains open for that pair, but the type of Incident changes to call quality if a call quality threshold violation has been detected.

Other Incident types do not have an applicable state. These are considered "closed" by default. For example, the abnormal termination Collector Incident type is never in an "open" state.

It's possible for a UC Monitor operator 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 (indicated with gray shading in Incident reports).

The best way to avoid such a situation is to configure an SNMP trap notification as an Incident response action. If an applicable SNMP notification action is configured, traps are automatically sent anytime an open Incident undergoes a change of severity status. Enable the Severity Updates parameter when you set up the SNMP trap action. For more information, see "Creating a New Incident Response" on page 192.

When the CA NetQoS Event Manager is also running in your environment, CA NetQoS Performance Center operators might try to close UC Monitor events because events from other CA NetQoS data sources can be closed manually. However, a NetQoS Performance Center operator's act of closing a UC Monitor event does not close the actual *Incident* that sent the event to the Event Manager. Such an Incident will have an Acknowledged status in the UC Monitor interface while appearing to have a Closed status in the Event Manager.

Example: Thresholds and Incidents

Here's an example of how performance thresholds, Incidents, and Incident responses work together:

1. A call server cluster at the Austin, TX network location becomes unavailable due to a LAN connectivity issue.
2. The delay to dial tone call setup Excessive **performance threshold**, 2000 ms, is exceeded when several users try to make calls with their IP phones and are routed to a backup call server cluster in Phoenix.
3. Unified Communications Monitor creates a single call setup **Incident** for all affected IP phones at the Austin Location.
4. The call setup Incident launches two associated **Incident response actions**, notifying a network engineer at the Austin location via **email** that a call setup threshold has been exceeded, and automatically launching a traceroute investigation to the key phone at the Austin Location.
5. The network engineer at the Austin site clicks a link in the email message he received. The link takes him to a page of **Incident reports**, where he can quickly drill down to find the affected call server cluster.
6. From the Related Reports list above the Incident report, he can easily access the Investigation Details page, where he can compare the baseline route to the current route to find the connectivity issue that is occurring.

In this example, if the Incident or Investigations reports had not included sufficient information to help the network engineer resolve the problem, he could have launched a Call Watch to gather more information about the problem. See Chapter 8, "Using Troubleshooting Features" on page 197 for more information.

Customizing Performance Thresholds

The UC Monitor Administration pages let you customize performance threshold settings and associate Incident responses with thresholds. This design helps you determine exactly how—and how frequently—the UC Monitor system will respond to degraded or excessive UC system performance conditions.

Unified Communications Monitor provides default performance thresholds for all monitored call setup and call quality metrics. You may want to apply different settings if you know in advance that certain performance characteristics, such as increased delay on a high-latency WAN link, apply to phones in selected Locations.

When you customize thresholds, you edit and selectively apply them in sets that include:

- your selected settings for the Degraded and Excessive thresholds that are available for each monitored metric
- any Incident responses you want to associate with these thresholds

  Incidents are raised in response to a threshold violation. You can associate automated response actions with Incidents as a separate step. See "Setting up Incident Responses" on page 191 for more information.

You can change default performance threshold values or disable a particular threshold. Threshold settings can be customized for either call setup or call quality metrics (or both). You can assign **Call Setup** performance threshold settings to either:

- a single Location, or
- a single media device

You can assign **Call Quality** performance threshold settings to any of the following:

- a pair of Locations
- a pair of media devices
- a pair that consists of a Location and a media device

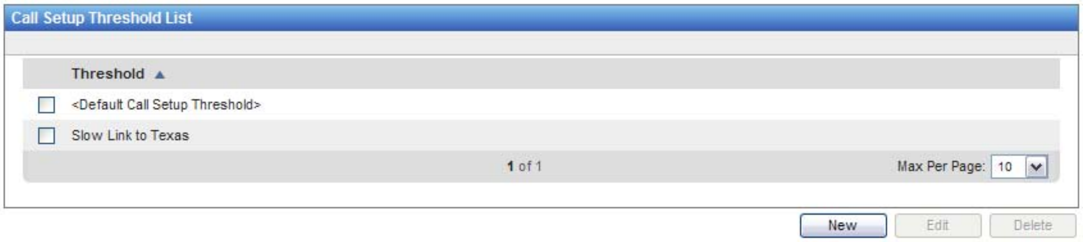
Customizing threshold settings is *not required*. If you do not customize any thresholds, the UC Monitor default threshold settings are used. The default settings are based on industry standards for quality VoIP performance.

Customizing Call Setup Thresholds

When you customize performance thresholds, you first change the performance threshold values that you want to change and then supply a name for the custom settings. The UC Monitor interface lets you view the list of existing threshold settings by name, edit the default thresholds, and add new, custom call setup thresholds. Thresholds include severity settings, Degraded and Excessive, as well as any responses you want to associate with Incidents raised in response to a potential threshold violation.

To customize call setup thresholds:

1. In the **navigation links**, click **Administration > Policies > Call Performance**, and then click **Call Setup Thresholds**.
2. The Call Setup Threshold List page is displayed:

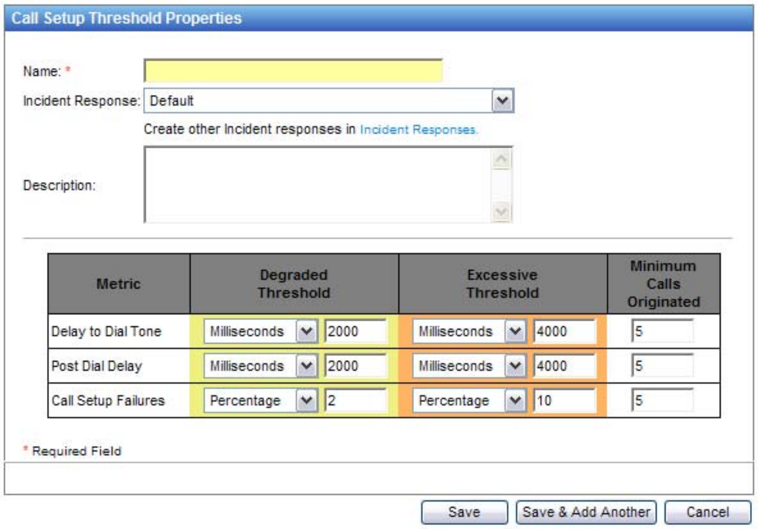


	Threshold ▲
□	<Default Call Setup Threshold>
□	Slow Link to Texas

1 of 1 Max Per Page: 10

Before you create any new performance threshold settings, only the name for the default settings, `<Default Call Setup Threshold>`, appears in the list.

3. Click **New** to create a new set of custom call setup thresholds.
4. The Call Setup Threshold Properties page is displayed:



Name: *
Incident Response: Default
Create other Incident responses in Incident Responses.
Description:

Metric	Degraded Threshold		Excessive Threshold		Minimum Calls Originated
Delay to Dial Tone	Milliseconds	2000	Milliseconds	4000	5
Post Dial Delay	Milliseconds	2000	Milliseconds	4000	5
Call Setup Failures	Percentage	2	Percentage	10	5

* Required Field

A set of call setup performance thresholds includes two severity settings—Degraded and Excessive—for each call setup metric that is monitored. Threshold properties include a unique name for the custom settings, any Incident response you want to associate with violations of these thresholds, and an optional description of the settings.

5. Type a name for the settings you're customizing in the **Name** field.
6. To launch an Incident response action automatically when a threshold is violated, select an Incident response from the **Incident Response** list.

   All Incident responses, including the default and any you have already defined, are available in the **Incident Response** list. See "Setting up Incident Responses" on page 191 for more information.

7. In the **Description** field, type a description of the settings. The description might indicate which Locations or media devices should be assigned these custom settings, or why a particular metric has a higher threshold, for example. This field is optional.

8. In the threshold properties table, find the metric whose threshold you want to change.
9. In the **Degraded Threshold** column for the selected metric, leave the default units (either **Milliseconds** or **Percentage**), or select `None` to disable that threshold. (Disabling thresholds is not recommended.)
10. Type a new value for the threshold.

    See "Call Setup Performance Threshold Settings" on page 145 for an explanation of each default call setup threshold setting.
11. In the **Excessive Threshold** column for the selected metric, type a new value for the threshold.

    Note: The value you enter for the Excessive threshold must be *more severe* than the Degraded threshold value. For example, if the selected metric is Post Dial Delay, the value for the Excessive threshold must be greater than the value for the Degraded threshold, indicating more severe delay.
12. In the **Minimum Calls Originated** column, type a new value, if desired. This value sets a minimum number of calls that must be initiated during a monitoring interval for an Incident to be created.

    Note: Set a lower value for Minimum Calls Originated if you want to see Incidents more quickly in response to poor call setup performance. Set a higher value to see Incidents more slowly, after more data has been collected. Unless the minimum value is met during a monitoring interval, data is not rated for that interval.
13. Perform one of the following actions:
    - Click **Save** to save the new performance thresholds and return to the Call Setup Threshold List page. The new set now appears in the list.
    - Click **Save and Add Another** to save the new performance thresholds and return to the Call Setup Threshold Properties page, where you can add another set of custom thresholds.

To enable the new thresholds, apply the settings to a Location or media device. See the following topic, "Assigning Call Setup Thresholds to Locations or Media Devices."

Assigning Call Setup Thresholds to Locations or Media Devices

The pre-defined UC Monitor call setup performance thresholds are applied to all Locations and media devices unless you change the threshold settings. You can change them by customizing call setup thresholds and assigning the custom thresholds to selected Locations or media devices.

Unlike call quality performance threshold settings, which are applied to *pairs* of network locations, call setup thresholds are only applied to a single selected Location or media device at a time. During call monitoring, the settings are applied only to the Locations or devices from which calls are made.

You can assign the same call setup thresholds to multiple Locations or media devices. Performance threshold settings cannot be assigned to groups.

To assign a custom set of call setup thresholds to a Location or device:

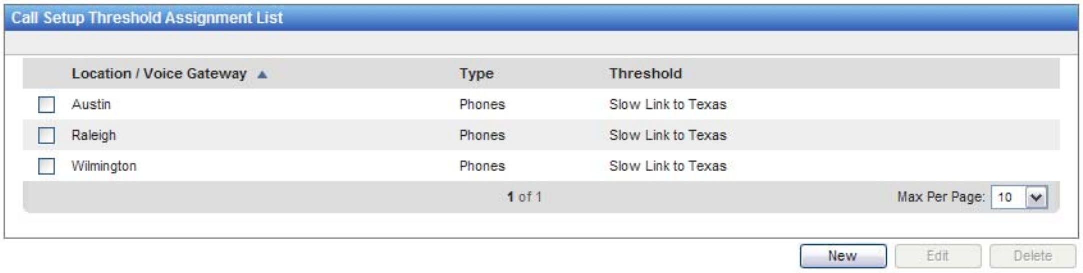
First, be sure you have defined some Locations, or that the system has discovered at least one voice gateway or other media device. See one of the following topics for more information:

- “Adding Locations” on page 108
- “Viewing the List of Voice Gateways” on page 119
- “Viewing the List of Other Media Devices” on page 128

You also must have customized at least one set of call setup performance thresholds before you attempt to apply them to a Location or media device. Otherwise, the default settings are used. Follow the steps outlined above in “Customizing Call Setup Thresholds” on page 162.

1. In the **navigation links**, click **Administration > Policies > Call Performance**, and then click **Call Setup Threshold Assignments**.

   The Call Setup Threshold Assignment List page is displayed:



Call Setup Threshold Assignment List

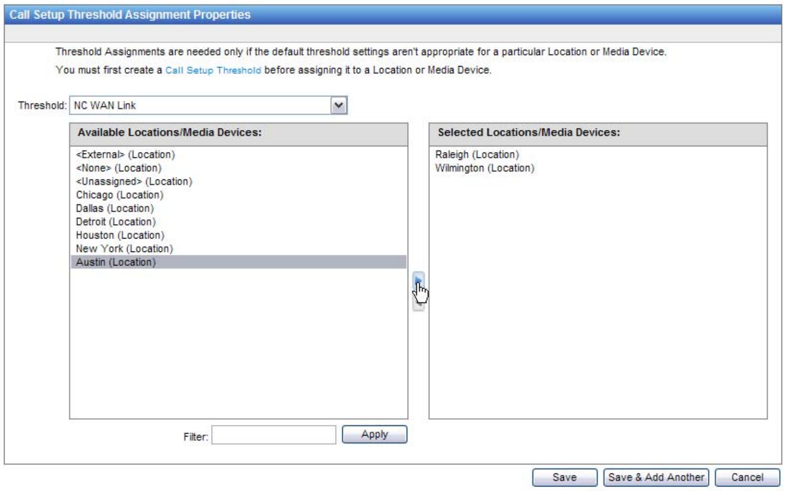
	Location / Voice Gateway ▲	Type	Threshold
□	Austin	Phones	Slow Link to Texas
□	Raleigh	Phones	Slow Link to Texas
□	Wilmington	Phones	Slow Link to Texas

1 of 1 Max Per Page: 10

   All the call setup threshold assignments are shown in the list. Before you have assigned any thresholds to Locations or media devices, a message states, `No Threshold Assignments are currently configured`.

2. Click **New** to create a new call setup threshold assignment.

   The Call Setup Threshold Assignment Properties page is displayed:



Call Setup Threshold Assignment Properties

Threshold Assignments are needed only if the default threshold settings aren't appropriate for a particular Location or Media Device.

You must first create a Call Setup Threshold before assigning it to a Location or Media Device.

Threshold: NC WAN Link

Available Locations/Media Devices:

<External> (Location)
<None> (Location)
<Unassigned> (Location)
Chicago (Location)
Dallas (Location)
Detroit (Location)
Houston (Location)
New York (Location)
Austin (Location)

Selected Locations/Media Devices:

Raleigh (Location)
Wilmington (Location)

Filter:

   Unless they have already been assigned to a set of custom performance threshold settings, all the Locations you have defined, and all media devices that have been detected on your network, are shown in the **Available Locations/Media Devices** on the left.

   Note: Two call setup threshold metrics do not apply to Microsoft media devices: Delay to Dial Tone and Post Dial Delay.

3. From the **Threshold** list, select a set of threshold settings to assign.

4. Click to select a Location or media device from the list. Then click the right directional arrow (as shown in the image above) to move the selected item to the list of **Selected Locations/Media Devices**.

   Select as many Locations or media devices as you like. Use **Ctrl + Click** or **Shift + Click** to select a range of items. The named set of threshold settings shown in the **Threshold** field is assigned to all of them.

5. Click **Save** to save the new assignments. You return to the Call Setup Threshold Assignment List page. The new assignments now appear in the list.

   Or select another set of thresholds from the **Threshold** list at the top of the page, click **New** to create other assignments, and repeat Steps 6 and 7.

The **Filter** field accepts wildcard (*) search strings to limit the data shown in the Available Locations/ Media Devices list. If you supply a string but no asterisks, the **Filter** field assumes wildcards (for example, "*`abc`*") when it searches. Filtering can be very useful if you have a long list of Locations and media devices.

Example: To see only Locations associated with the Raleigh, NC office, you would enter `ral*` for the filter and click **Apply**. Only Locations whose name begins with Ral would be shown in the list.

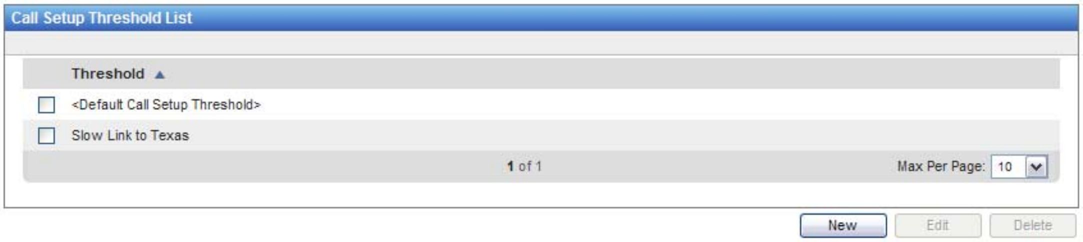
Editing Call Setup Threshold Settings

Call setup performance thresholds, including ones you have customized, can be edited. For example, after a few days of data collection, you may find that you want to increase the value you selected for an Excessive threshold so that you'll receive fewer Incidents. Or you may want to edit the assignment of a named set of thresholds so that the settings are applied to additional Locations or media devices. Instructions for editing threshold settings and editing threshold assignments are provided below.

To edit call setup threshold settings:

1. In the **navigation link**s, click **Administration > Policies > Call Performance**, and then click **Call Setup Thresholds**.

   The Call Setup Threshold List page is displayed:



Call Setup Threshold List

	Threshold ▲
□	<Default Call Setup Threshold>
□	Slow Link to Texas

1 of 1 Max Per Page: 10

2. Select the settings you want to edit.

3. Click **Edit**.

   The Call Setup Threshold Properties page is displayed. The settings you selected when you customized these thresholds are shown.

4. Make the desired changes to any of the settings. For more information about any of these settings, see "Customizing Call Setup Thresholds" on page 162.

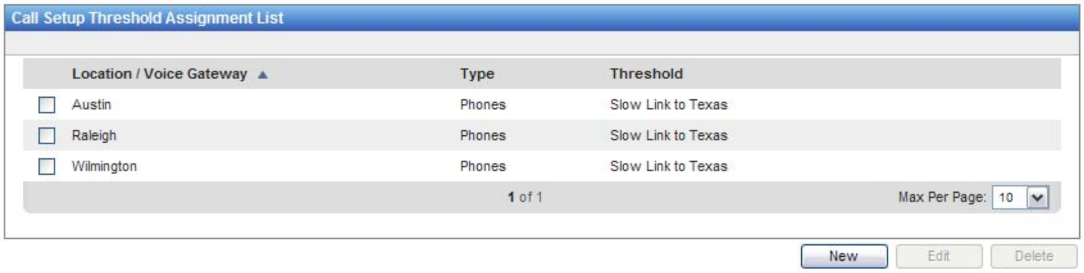
5. Click **Save** to save your changes to the settings.

Your changes are applied to the next data-collection interval. Data already collected is not re-evaluated using the new settings.

To change the assignment of a set of call setup thresholds:

1. In the **navigation links**, click **Administration > Policies**, and then click **Call Setup Threshold Assignments**.

   The Call Setup Threshold Assignment List page is displayed:



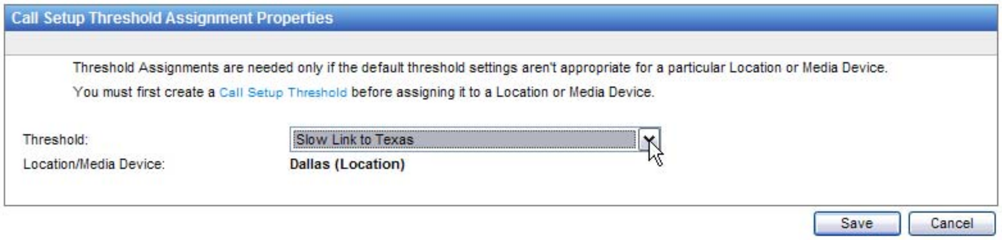
Call Setup Threshold Assignment List

	Location / Voice Gateway ▲	Type	Threshold
□	Austin	Phones	Slow Link to Texas
□	Raleigh	Phones	Slow Link to Texas
□	Wilmington	Phones	Slow Link to Texas

1 of 1 Max Per Page: 10

2. Select the settings you want to edit.
3. Click **Edit**.

   The Call Setup Threshold Assignment Properties page is displayed:



Call Setup Threshold Assignment Properties

Threshold Assignments are needed only if the default threshold settings aren't appropriate for a particular Location or Media Device.

You must first create a Call Setup Threshold before assigning it to a Location or Media Device.

Threshold: Slow Link to Texas

Location/Media Device: **Dallas (Location)**

4. Select the name of the threshold settings you want to assign to this pair from the **Threshold** list.
5. Click **Save** to save the new assignment. You return to the Call Setup Threshold Assignment List page. The new assignment now appears in the list.

Your changes are applied to the next data-collection interval. Data already collected is not re-evaluated using the new settings.

Deleting a Set of Custom Call Setup Thresholds

You can delete any set of call setup performance thresholds that are not currently assigned to a Location or media device. If you attempt to delete a set of assigned thresholds, a warning is displayed, and the deletion fails.

To delete a set of assigned thresholds, edit the set to remove the assignment before you can delete it. The set of thresholds only appears in the Call Setup Threshold Assignment List if it has been assigned.

To delete a set of unassigned call setup thresholds:

1. In the **navigation link**s, click **Administration > Policies > Call Performance**, and then click **Call Setup Thresholds**.

   The Call Setup Threshold List page is displayed.
2. Select all the Locations or media devices whose threshold assignments you want to delete.
3. Click **Delete**.
4. Click **OK** to confirm the deletion.

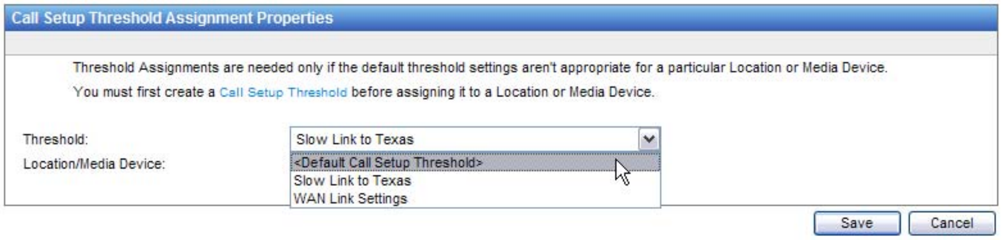
The set is deleted and no longer appears in the Call Setup Threshold List.

To delete a set of assigned Call Setup thresholds:

1. In the **navigation link**s, click **Administration > Policies > Call Performance**, and then click **Call Setup Threshold Assignments**.

   The Call Setup Threshold Assignment List page is displayed.
2. Select the set of thresholds you want to edit.
3. Click **Edit**.

   The Call Setup Threshold Assignment Properties page is displayed. The **Threshold** list shows the set of thresholds. Below it, the Locations or media devices to which the thresholds are currently assigned are shown.



Call Setup Threshold Assignment Properties

Threshold Assignments are needed only if the default threshold settings aren't appropriate for a particular Location or Media Device.

You must first create a Call Setup Threshold before assigning it to a Location or Media Device.

Threshold: Slow Link to Texas

Location/Media Device:

4. In the **Threshold** list, click to select `<Default Call Setup Threshold>`. This removes the current threshold assignment.
5. Click **Save** to save the change. You return to the Call Setup Threshold Assignment List page. The set of thresholds now appears with the `<Default Call Setup Threshold>` assignment in the list.
6. In the navigation links, click **Call Setup Thresholds**.
7. In the Call Setup Threshold List, select the set of thresholds you want to delete.
8. Click **Delete**.
9. Click **OK** to confirm the deletion.

The set is deleted and no longer appears in the Call Setup Threshold list.

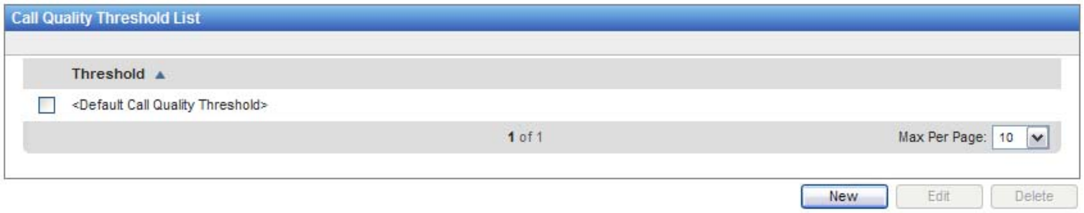
Customizing Call Quality Thresholds

When you customize performance thresholds, you first change the performance threshold values that you want to change and then supply a name for the custom settings. The UC Monitor interface lets you view the list of existing threshold settings by name and add new custom call quality thresholds. Thresholds include severity settings, Degraded and Excessive, as well as any responses you want to associate with Incidents raised in response to a potential threshold violation.

To customize call quality thresholds:

1. In the **navigation links**, click **Administration > Policies > Call Performance**, and then click **Call Quality Thresholds**.

   The Call Quality Threshold List page is displayed:



Call Quality Threshold List

Threshold ▲
□ <Default Call Quality Threshold>

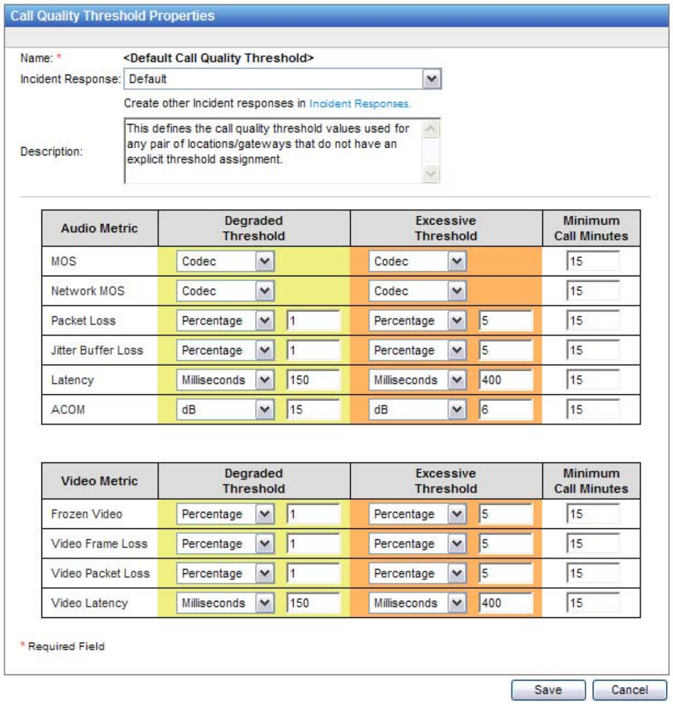
1 of 1 Max Per Page: 10

   Before you create any new performance threshold settings, only the pre-defined settings, enclosed in brackets, appear in the list.

   See "Call Quality Performance Threshold Settings" on page 146 for an explanation of the default call quality thresholds.

2. Click **New** to create a new set of custom call quality performance thresholds.

   The Call Quality Threshold Properties page is displayed:



Call Quality Threshold Properties

Name: * <Default Call Quality Threshold>

Incident Response: Default

Create other Incident responses in Incident Responses.

Description: This defines the call quality threshold values used for any pair of locations/gateways that do not have an explicit threshold assignment.

Audio Metric	Degraded Threshold		Excessive Threshold		Minimum Call Minutes
MOS	Codec		Codec		15
Network MOS	Codec		Codec		15
Packet Loss	Percentage	1	Percentage	5	15
Jitter Buffer Loss	Percentage	1	Percentage	5	15
Latency	Milliseconds	150	Milliseconds	400	15
ACOM	dB	15	dB	6	15

Video Metric	Degraded Threshold		Excessive Threshold		Minimum Call Minutes
Frozen Video	Percentage	1	Percentage	5	15
Video Frame Loss	Percentage	1	Percentage	5	15
Video Packet Loss	Percentage	1	Percentage	5	15
Video Latency	Milliseconds	150	Milliseconds	400	15

* Required Field

A set of call quality performance thresholds includes two severity settings—Degraded and Excessive—for each call quality metric that is monitored. Threshold properties include a unique name for the custom settings, any Incident response you want to associate with violations of these thresholds, and an optional description of the settings.

3. In the **Name** field, type a name for the settings you're customizing.
4. To launch an Incident response action automatically when a threshold is violated, select an Incident response from the **Call Quality Incident Response** list.

   All Incident responses, including the default and any you have already defined, are available in the **Incident Response** list. See "Setting up Incident Responses" on page 191 for more information about defining them.
5. In the **Description** field, type a description of the settings. The description might indicate which Location or media device pairs should be assigned these custom settings, for example. This field is optional.
6. In the **Audio Metrics** table of threshold properties (shown above), find the metric whose threshold you want to change.
7. In the **Degraded Threshold** column for the selected metric, leave the default units (either `Milliseconds` or `Percentage`), or select `None` to disable that threshold.
8. Type a new value for the threshold.

   See "Call Quality Performance Threshold Settings" on page 146 for an explanation of each default call quality performance threshold setting.

   Codec thresholds are used by default for MOS metrics. See "Understanding Codec Thresholds" on page 154 for more information.
9. In the **Excessive Threshold** column for the selected metric, disable the threshold by selecting `None` in the units list, if desired. Or type a new value for the threshold.

   Note: The value you enter for the Excessive threshold must be *more severe* than the Degraded threshold value. For example, if the selected metric is Latency, the value for the Excessive threshold must be greater than the value for the Degraded threshold, indicating more severe latency. However, the Excessive threshold for MOS must be *smaller* than the Degraded threshold value, indicating a lower VoIP call quality score.
10. In the **Minimum Call Minutes** column, type a new value if desired. This value sets a minimum number of minutes during which active calls must be observed for an Incident to be created. The value you enter must be > 0.

    Note: Set a lower value for Minimum Call Minutes if you want to see Incidents more quickly in response to poor call quality. Set a higher value to see Incidents only after more calls have been observed. If the minimum value is not met during a monitoring interval, data is not rated as degraded.
11. Repeat Steps 6-10 above to select values for the metrics in the **Video Metrics** table.
12. Click **Save** to save the new performance thresholds and return to the Call Quality Threshold List page. The new set of thresholds now appears in the list.

    Or click **Save and Add Another** to save the new performance threshold settings and return to the Call Quality Threshold Properties page, where you can add another set of custom thresholds.

Now that you have customized a set of thresholds, you need to apply the settings to a pair of network locations, such as two Locations or a Location paired with a media device. Only then will the new settings you have just selected for the threshold metrics be applied to any component. See the following topic, "Assigning Call Quality Thresholds to Pairs of Locations or Devices."

Assigning Call Quality Thresholds to Pairs of Locations or Devices

The pre-defined UC Monitor call quality performance thresholds are applied to all Locations and media devices unless you change the threshold settings. You can change them by customizing call quality performance thresholds and assigning the custom thresholds to selected pairs of Locations and media devices.

VoIP call performance occurs between pairs of phones and related endpoints. Therefore, when you're monitoring voice over IP, you should try to understand the call quality data that's reported on the basis of paired network locations.

UC Monitor call quality performance thresholds are distinct from call setup thresholds in that they are applied based on pairs. They can be assigned to pairs of Locations to include all computers in the relevant Location subnets. They can also be assigned to pairs of media devices, or to pairs that consist of a Location and a media device. The same set of call quality performance thresholds can be assigned to multiple pairs, such as all the Locations in a single geographical region of your enterprise. However, you must *assign* the threshold settings to each selected pair.

Note: Performance threshold settings cannot be assigned to groups.

To assign a custom set of call quality thresholds:

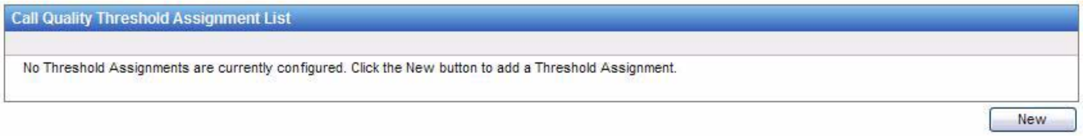
First, be sure you have created some Location definitions, or that the system has discovered at least one voice gateway or other media device. See one of the following for more information:

- "Adding Locations" on page 108
- "Viewing the List of Voice Gateways" on page 119

You also must have customized at least one set of call quality performance thresholds before you attempt to apply them to a Location or media device. Follow the steps outlined above in "Customizing Call Quality Thresholds" on page 169.

1. In the **navigation link**s, click **Administration > Policies > Call Performance**, and then click **Call Quality Threshold Assignments**.

   The Call Quality Threshold Assignment List page is displayed:

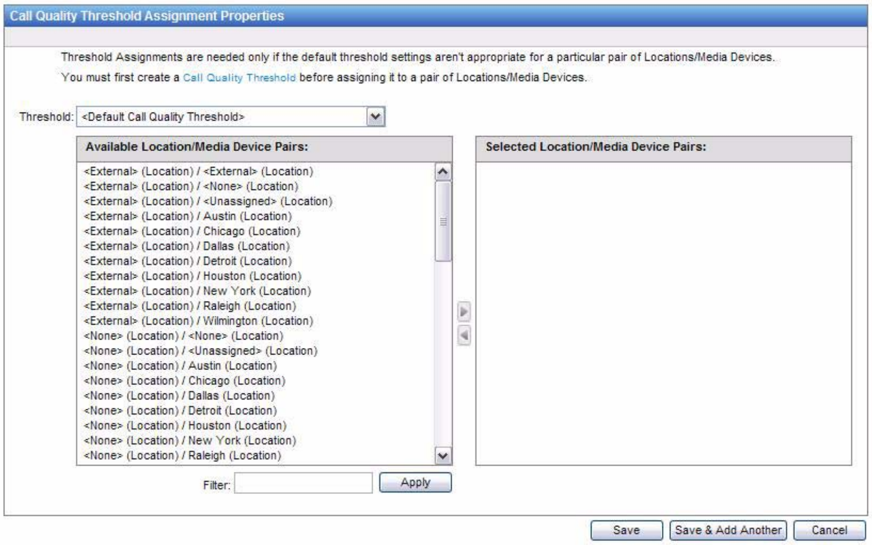
   Call Quality Threshold Assignment List

   No Threshold Assignments are currently configured. Click the New button to add a Threshold Assignment.

   All the call quality threshold assignments in the system are shown in the list. Before you have assigned any thresholds to pairs of Locations or devices, a message states, `No Threshold Assignments are currently configured`.

2. Click **New** to create a new call quality performance threshold assignment.

The Call Quality Threshold Assignment Properties page is displayed:



Call Quality Threshold Assignment Properties

Threshold Assignments are needed only if the default threshold settings aren't appropriate for a particular pair of Locations/Media Devices.

You must first create a Call Quality Threshold before assigning it to a pair of Locations/Media Devices.

Threshold: <Default Call Quality Threshold>

Available Location/Media Device Pairs:

<External> (Location) / <External> (Location)
<External> (Location) / <None> (Location)
<External> (Location) / <Unassigned> (Location)
<External> (Location) / Austin (Location)
<External> (Location) / Chicago (Location)
<External> (Location) / Dallas (Location)
<External> (Location) / Detroit (Location)
<External> (Location) / Houston (Location)
<External> (Location) / New York (Location)
<External> (Location) / Raleigh (Location)
<External> (Location) / Wilmington (Location)
<None> (Location) / <None> (Location)
<None> (Location) / <Unassigned> (Location)
<None> (Location) / Austin (Location)
<None> (Location) / Chicago (Location)
<None> (Location) / Dallas (Location)
<None> (Location) / Detroit (Location)
<None> (Location) / Houston (Location)
<None> (Location) / New York (Location)
<None> (Location) / Raleigh (Location)

Selected Location/Media Device Pairs:

Unless they have already been assigned to a set of custom threshold settings, all possible pairs of Locations and media devices are shown in the **Available Location/Media Device Pairs** list.

3. (*Optional*) If you are monitoring in a multiple-domain environment, an additional parameter allows you to select the **NPC Domain**.

   The list is then filtered to show only pairs of Locations and media devices from the selected domain.

4. From the **Threshold** list, select the name of the threshold settings to assign to this pair.

5. Select any pairs to which you want to apply a set of custom thresholds and Incident responses. Use **Ctrl + Click** or **Shift + Click** to select a range of items. Double-click to move the items to the **Selected Location/Media Device Pairs** list.

   Note: A Location may be paired with another Location or with a media device. Pairs of media devices are also possible.

6. Click **Save** to save the new performance threshold assignment. You return to the Call Quality Threshold Assignment List page. The new assignment now appears in the list.

   Or click **Save and Add Another** to save this assignment and return to the Call Quality Threshold Assignment page.

The **Filter** field accepts search strings to limit the data shown in the **Available Location/Media Device Pairs** list. Wildcard characters are added for you before and after the string when you click **Apply**, so do not include * or % characters.

Filtering can be very useful if you have a long list of Locations and media devices defined.

Example: To see only Locations or media devices associated with the Raleigh, NC office, you would enter `ral` for the filter and click **Apply**. Any Locations or media devices whose name includes Ral would be shown in the list.

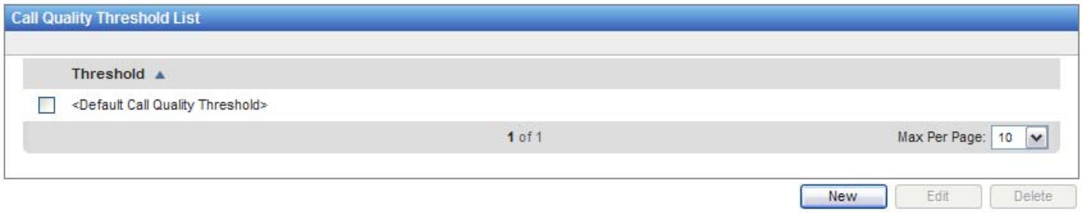
Editing Call Quality Threshold Settings

The call quality performance thresholds you have customized can be edited. For example, after a few days of data collection, you may find that you want to increase the value you selected for an Excessive threshold so that you'll receive fewer Incidents. Or you may want to edit the assignment of a named set of thresholds so that the settings are applied to additional Locations or media devices. Instructions for editing threshold settings and editing threshold assignments are provided below.

To edit call quality threshold settings:

1. In the **navigation links**, click **Administration > Policies > Call Performance**, and then click **Call Quality Thresholds**.

   The Call Quality Threshold List page is displayed:


Call Quality Threshold List
Threshold ▲
□ <Default Call Quality Threshold>
1 of 1
Max Per Page: 10
New
Edit
Delete

2. Select the settings you want to edit.
3. Click **Edit**.

   The Call Quality Threshold Properties page is displayed. See "Customizing Call Quality Thresholds" on page 169 for information about the options on this page.
4. Click **Save** to save your changes to the settings.

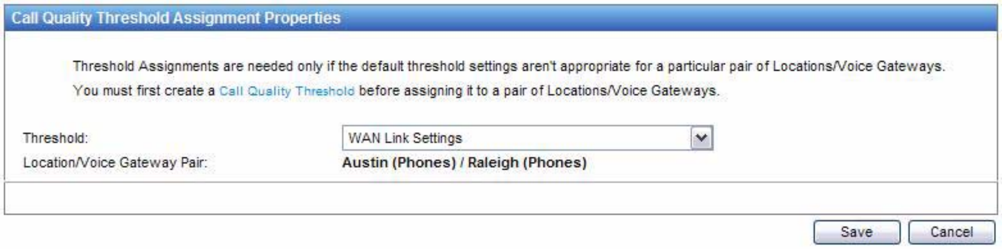
Your changes are applied to the next data-collection interval. Data already collected is not re-evaluated using the new settings.

To change the assignment of a set of call quality thresholds:

1. In the **navigation links**, click **Administration > Policies > Call Performance**, and then click **Call Quality Threshold Assignments**.

   The Call Quality Threshold Assignment List page is displayed.
2. Select the settings you want to edit.
3. Click **Edit**.

   The Call Quality Threshold Assignment Properties page is displayed:



Threshold Assignments are needed only if the default threshold settings aren't appropriate for a particular pair of Locations/Voice Gateways. You must first create a Call Quality Threshold before assigning it to a pair of Locations/Voice Gateways.

Threshold: WAN Link Settings
Location/Voice Gateway Pair: Austin (Phones) / Raleigh (Phones)

4. Select a different set of threshold settings from the **Threshold** list.
5. Click **Save** to save the new assignment. You return to the Call Quality Threshold Assignment List page. The new assignments now appear in the list.

Your changes are applied to the next data-collection interval. Data already collected is not re-evaluated using the new settings.

Deleting a Set of Custom Call Quality Thresholds

You can delete any call quality performance thresholds that are not currently assigned to a pair of Locations and/or media devices. If you attempt to delete a set of assigned thresholds, a warning is displayed, and the deletion fails.

After a set of performance thresholds has been assigned to a pair, you must first edit the set to remove the assignment before you can delete it. Click the **Threshold** column in the Call Quality Threshold Assignment List to sort by threshold name and see whether the set has been assigned.

See the online Help for instructions on deleting unassigned and assigned thresholds.

Disabling Incidents for a Threshold Metric

The UC Monitor software provides a set of default thresholds for all the performance metrics that it monitors. By default, both Degraded and Excessive thresholds raise an Incident each time they're crossed. However, Incidents are never double-reported: if an Excessive threshold is crossed, a single Incident is reported in the Incidents report even though the Degraded threshold, which is always less severe than the Excessive threshold, was also crossed.

You may still decide that you don't want to see any Incidents or data in reports about a particular performance metric that the UC Monitor product supports. Thresholds, and thus, Incidents, can be disabled for any or all metrics, on a per-Location or per-media device basis. For example, you may have a voice gateway that does not perform echo cancellation. You may therefore want to disable Incident reporting from that gateway for the ACOM metric.

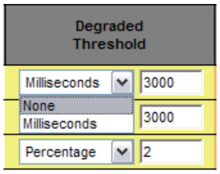
Important: Disabling thresholds (Incidents) is not recommended. When you disable thresholds, you also disable data rating, which means that in some detailed data views, data collected with the disabled thresholds applied is rated as "Normal," even if it isn't. A better option might be to disable monitoring of an entire Location, or of an individual media device. See "Disabling Monitoring of Selected Locations" on page 110 for more information.

To disable Incident reporting:

1. In the **navigation link**s, click **Administration > Policies > Call Performance**, and then click to select either **Call Setup Thresholds** or **Call Quality Thresholds**.

   The corresponding Threshold List page is displayed.
2. Select the set of performance thresholds you want to edit.
3. Click **Edit**.
4. In the selected Threshold Properties page, find the metric for which you want to disable Incident reporting in the Thresholds table.

5. Next to the Degraded or Excessive threshold (or both), click to select **None** from the units menu, as shown below:



6. Click **OK**.

The threshold for that metric is disabled. Any changes you made are automatically applied to any Location, media device, or pair to which these custom thresholds are assigned.

Disabling a threshold disables Incidents for the applicable metric, but it does not remove that metric from reports. You must set both the Degraded and Excessive thresholds to `None` if you do not want that metric to be rated in reports. A metric with both performance thresholds disabled appears in dark gray, identifying it as "Unrated" in reports.

You can disable either the Degraded or Excessive performance thresholds for a selected metric, or both. Any Location or media device that does not have that threshold assignment still shows ratings for that metric in reports and still creates Incidents when the threshold is violated.

Depending on your existing settings, disabling a threshold for a particular metric may require some extra configuration of your Incident responses. They will still function normally, but if, for example, you disable a Degraded threshold, be sure that any Incident responses you want to assign to that metric are set to be launched by the Excessive threshold.

Working with Call Server Thresholds

Call server thresholds were designed to provide more information about phone registration activity and phone status, as well as Incidents and notifications of user-reported call quality issues. Two types of call server thresholds are available:

- **Call server thresholds**—Thresholds that are assigned to individual call servers. See "Customizing Call Server Thresholds" on page 176 for more information.
- **Call server group thresholds**—Thresholds that are assigned to call server groups, which represent the clusters in your system. See "Customizing Call Server Group Thresholds" on page 181 for more information.

To provide call server Incidents and associated Incident responses, Unified Communications Monitor tracks phone registration status to determine when phones switch to another call server, and it tracks phone keepalive messages to maintain a current record of phone status. Incident responses can be configured based on the percentage of all phones that have a status of "missing" or "new," or based on a maximum number of registration failures that can occur during a reporting interval.

If you see some call server or call server group Incidents, you can immediately launch a traceroute investigation to find out whether a failover has occurred and begin troubleshooting a possible call server or network outage. See "Launching a Traceroute Investigation" on page 205 for more information.

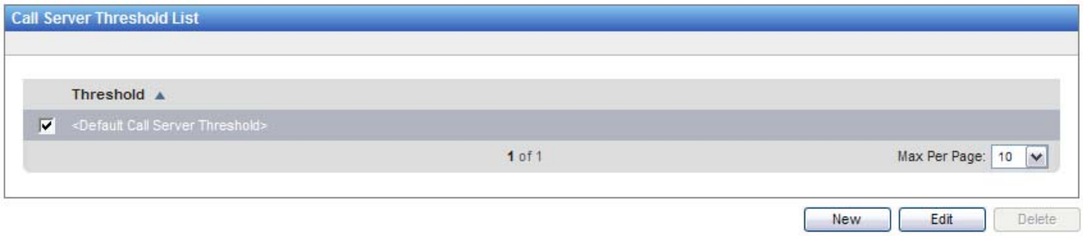
Customizing Call Server Thresholds

When you customize any thresholds, including performance thresholds and call server thresholds, you change the threshold values, supply a name for the custom settings, and save the new settings as a set. You must then apply the set of custom values to a call server. The UC Monitor interface lets you view the list of existing threshold settings by name and add new custom call server thresholds. Threshold properties include threshold maximum values and any responses you want to associate with Incidents raised in response to a potential threshold violation.

To customize call server thresholds:

1. In the navigation links, click **Administration > Policies > Call Servers**, and then click **Call Server Thresholds**.

   The Call Server Threshold List page is displayed:



Call Server Threshold List

	Threshold ▲
☑	<Default Call Server Threshold>

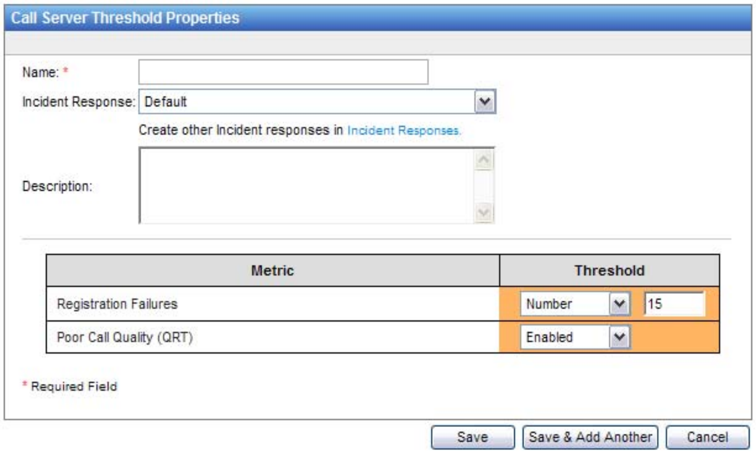
1 of 1 Max Per Page: 10

   Before you create any new call server threshold settings, only the name of the pre-defined settings, enclosed in brackets, appears in the list. The pre-defined settings are used by default for all call servers discovered during monitoring. You can edit these settings or create a new set of threshold settings and assign them to call servers, as appropriate.

   See “Call Server Threshold Settings” on page 149 for an explanation of the threshold settings.

2. Click **New** to create a new set of custom call server thresholds.

   The Call Server Threshold Properties page is displayed:



Call Server Threshold Properties

Name: *

Incident Response: Default

Create other Incident responses in Incident Responses.

Description:

Metric	Threshold
Registration Failures	Number 15
Poor Call Quality (QRT)	Enabled

* Required Field

   Call server threshold properties include a unique name for the custom settings, any Incident response you want to associate with violations of these thresholds, and an optional description of the settings.

3. In the **Name** field, type a name for the settings you're customizing.
4. To launch an Incident response action automatically when a threshold is violated, select an Incident response from the Incident Response list.

   All Incident responses, including the default and any you have already defined, are available in the **Incident Response** list. See "Setting up Incident Responses" on page 191 for more information about defining them.
5. (*Optional*) In the **Description** field, type a description of the settings. The description might indicate which call servers should be assigned these custom settings, for example.
6. In the threshold properties table (shown above), find the threshold you want to change.
   - In the **Threshold** column for the Registration Failures metric, leave the default units (`Number`), or select `None` to disable that threshold.

     If desired, type a new value for the maximum number of registration failures before an Incident is created.
   - In the **Threshold** column for the Poor Call Quality (QRT) metric, leave the default setting (`Enabled`), or select `None` to disable that threshold.

   See "Call Server Threshold Settings" on page 149 for an explanation of the default call server threshold settings.
7. Click **Save** to save the new call server thresholds and return to the Call Server Threshold List page. The new set of thresholds now appears in the list.

   Or click **Save and Add Another** to save the new threshold settings and return to the Call Server Threshold Properties page, where you can add another set of custom thresholds.

Now that you have customized a set of thresholds, you need to apply the settings to a call server. See the following topic, "Assigning Call Server Thresholds," for instructions on applying the threshold settings to a call server.

Assigning Call Server Thresholds

The pre-defined UC Monitor call server thresholds are applied to all call servers as soon as they are discovered during monitoring unless you change the threshold settings. You can change them by editing the default settings or by customizing call server thresholds and assigning the custom thresholds to selected call servers.

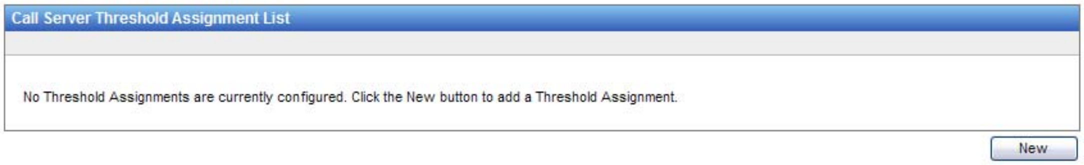
Unlike the call server group thresholds, which are appropriate for call server clusters, the call server thresholds must be assigned to individual call servers. See "Understanding Call Server Thresholds" on page 149 for more information.

To assign a custom set of call server thresholds:

You also must have customized at least one set of call server thresholds before you attempt to apply them to a call server. Follow the steps outlined above in "Customizing Call Server Thresholds" on page 176.

1. In the navigation links, click **Administration > Policies > Call Servers**, and then click **Call Server Threshold Assignments**.

   The Call Server Threshold Assignment List page is displayed:



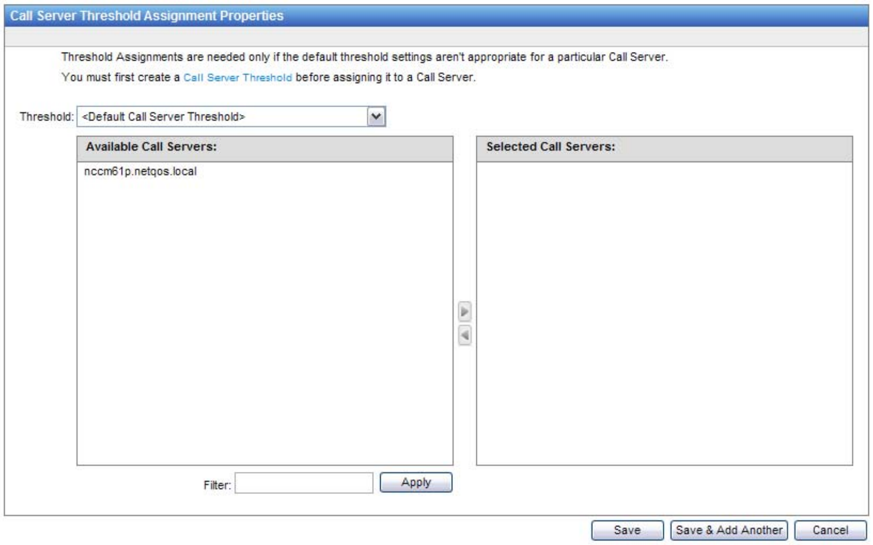
Call Server Threshold Assignment List

No Threshold Assignments are currently configured. Click the New button to add a Threshold Assignment.

   All the call server threshold assignments in the system are shown in the list. Before you have assigned any custom thresholds to call servers, a message states, `No Threshold Assignments are currently configured`.

2. Click **New** to create a new call server threshold assignment.

   The Call Server Threshold Assignment Properties page is displayed:



Call Server Threshold Assignment Properties

Threshold Assignments are needed only if the default threshold settings aren't appropriate for a particular Call Server.

You must first create a Call Server Threshold before assigning it to a Call Server.

Threshold: <Default Call Server Threshold>

Available Call Servers:

nccm61p.netqos.local

Selected Call Servers:

Filter:

   Unless they have already been assigned a set of custom threshold settings, all call servers are shown in the **Available Call Servers** list.

3. From the **Threshold** list, select the name of the threshold settings to assign to this server.

4. Select any call servers to which you want to apply a set of custom thresholds and Incident responses. Use **Ctrl + Click** or **Shift + Click** to select a range of items. Double-click to move the items to the **Selected Call Servers** list.

5. Click **Save** to save the new call server threshold assignment. You return to the Call Server Threshold Assignment List page. The new assignment now appears in the list.

   Or click **Save and Add Another** to save this assignment and return to the Call Server Threshold Assignment page.

The **Filter** field accepts search strings to limit the data shown in the Available Call Servers list. Wildcard characters are added for you before and after the string when you click **Apply**, so do not include * or % characters. Filtering can be very useful if you have a long list of call servers.

Example: To see only call servers associated with the Raleigh, NC office, you would enter `ral` for the filter and click **Apply**. Any call servers whose name includes `Ral` would be shown in the list.

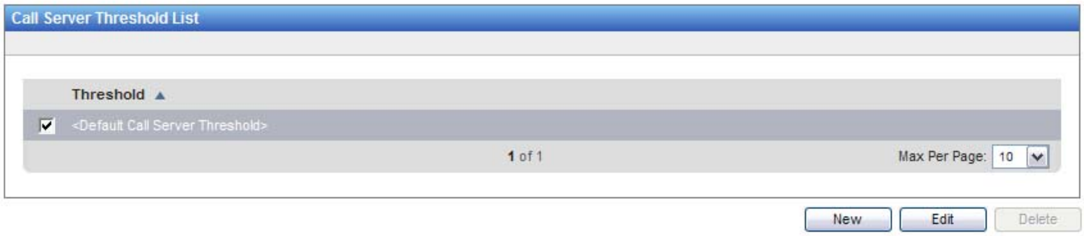
Editing Call Server Threshold Settings

The call server thresholds you have customized can be edited. For example, after a few days of data collection, you may decide to increase the value you selected for the Registration Failures threshold so that you'll receive fewer Incidents. Or you may want to edit the assignment of a named set of thresholds so that the settings are applied to additional call servers. Instructions for editing threshold settings and editing threshold assignments are provided below.

To edit call server threshold settings:

1. In the navigation links, click A**dministration** > **Policies** > **Call Servers**, and then click **Call Server Thresholds**.

   The Call Server Threshold List page is displayed:



Call Server Threshold List

	Threshold ▲
☑	<Default Call Server Threshold>

1 of 1   Max Per Page: 10

2. Select the threshold settings you want to edit.
3. Click **Edit**.

   The Call Server Threshold Properties page is displayed. See "Customizing Call Server Thresholds" on page 176 for information about the options on this page.
4. Click **Save** to save your changes to the settings.

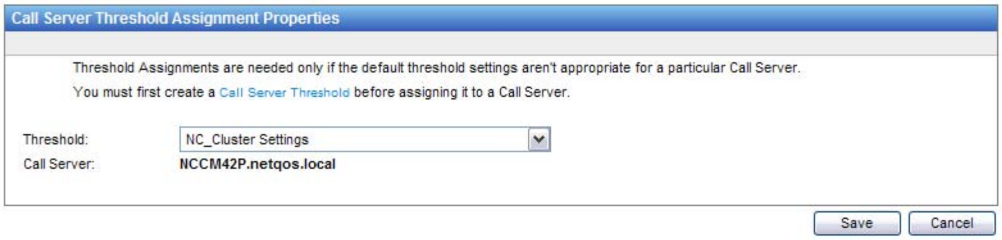
Your changes are applied to the next data-collection interval. Data already collected is not re-evaluated using the new settings.

To change the assignment of a set of call server thresholds:

1. In the navigation links, click **Administration** > **Policies** > **Call Servers**, and then click **Call Server Threshold Assignments**.

   The Call Server Threshold Assignment List page is displayed.
2. Select the call server whose assignment you want to remove or edit.
3. Click **Edit**.

   The Call Server Threshold Assignment Properties page is displayed:



Call Server Threshold Assignment Properties

Threshold Assignments are needed only if the default threshold settings aren't appropriate for a particular Call Server.
You must first create a Call Server Threshold before assigning it to a Call Server.

Threshold: NC_Cluster Settings
Call Server: NCCM42P.netqos.local

4. Select a different set of threshold settings from the **Threshold** list.
5. Click **Save** to save the new assignment. You return to the Call Server Threshold Assignment List page. The new assignment now appears in the list.

Your changes are applied to the next data-collection interval. Data already collected is not re-evaluated using the new settings.

Deleting a Set of Custom Call Server Thresholds

You can delete any call server thresholds that are not currently assigned to a call server. If you attempt to delete a set of assigned thresholds, a warning is displayed, and the deletion fails.

After a set of call server thresholds has been assigned to a server, you must first edit the set to remove the assignment before you can delete it. Click the **Threshold** column in the Call Server Threshold Assignment List to sort by threshold name and see whether the set has been assigned.

Below, instructions for deleting unassigned and assigned thresholds are provided.

To delete a set of unassigned call server thresholds:

1. In the navigation links, click **Administration > Policies > Call Servers**, and then click **Call Server Threshold Assignments**.

   The Call Server Threshold Assignment List page is displayed.
2. Select the set of thresholds you want to delete.
3. Click **Delete**.
4. Click **OK** to confirm the deletion.

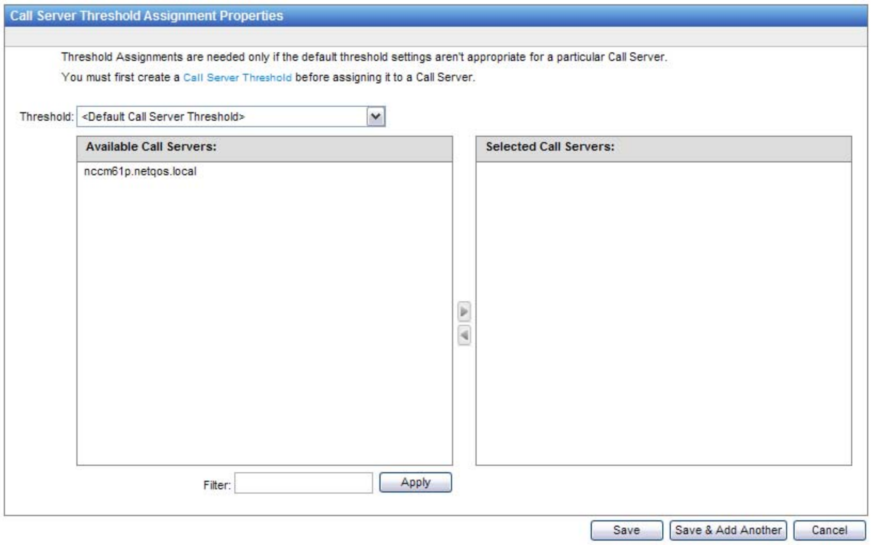
The set is deleted and no longer appears in the Call Server Threshold Assignment list.

To delete a set of assigned call server thresholds:

1. In the navigation links, click **Administration > Policies > Call Servers**, and then click **Call Server Threshold Assignments**.

   The Call Server Threshold Assignment List page is displayed.
2. Select all the call servers to which the set of thresholds you want to delete is assigned. Use **Ctrl + Click** to select multiple call servers.
3. Click the **Edit** button.

   The Call Server Threshold Assignment Properties page is displayed:



Call Server Threshold Assignment Properties

Threshold Assignments are needed only if the default threshold settings aren't appropriate for a particular Call Server.
You must first create a Call Server Threshold before assigning it to a Call Server.

Threshold: <Default Call Server Threshold>

Available Call Servers:
nccm61p.netqos.local

Selected Call Servers:

Filter:

4. In the **Threshold** list, click to select the default call server threshold. Or click to select any other set of thresholds you defined.
5. Click **Save** to save the change. This removes the current threshold assignment.

   You return to the Call Server Threshold Assignment List page. The new threshold assignment you selected now appears in the list for the selected call servers.
6. In the navigation links, click **Call Server Thresholds**.
7. In the Call Server Threshold list, select the set of thresholds you want to delete.
8. Click **Delete**.
9. Click **OK** to confirm the deletion.

The set is deleted and no longer appears in the Call Server Threshold list.

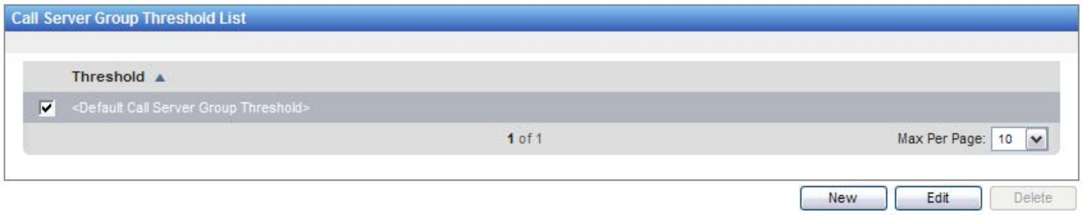
Customizing Call Server Group Thresholds

When you customize call server group thresholds, you first change the threshold values that you want to change and then supply a name for the custom settings. The UC Monitor interface lets you view the list of existing threshold settings by name and add new custom call server group thresholds. Thresholds include maximum values that, if exceeded, trigger an Incident, as well as any responses you want to associate with any Incidents that are created.

To customize call server group thresholds:

1. In the navigation links, click **Administration > Policies > Call Servers**, and then click **Call Server Group Thresholds**.

   The Call Server Group Threshold List page is displayed:



Call Server Group Threshold List

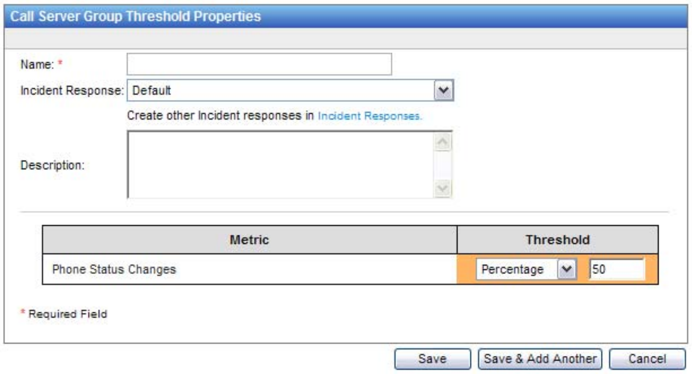
	Threshold ▲
☑	<Default Call Server Group Threshold>

1 of 1 Max Per Page: 10

Before you create any new call server group threshold settings, only the name of the pre-defined settings, enclosed in brackets, appears in the list.

2. Click **New** to create a new set of custom call server group thresholds.

   The Call Server Group Threshold Properties page is displayed:



Call Server Group Threshold Properties

Name: *

Incident Response: Default

Create other Incident responses in Incident Responses.

Description:

Metric	Threshold
Phone Status Changes	Percentage 50

* Required Field

A single threshold metric, **Phone Status Changes**, can be configured. Threshold properties include a unique name for the custom settings, any Incident response you want to associate with violations of these thresholds, and an optional description of the settings.

3. In the **Name** field, type a name for the settings you're customizing.
4. To launch an Incident response action automatically when a threshold is violated, select an Incident response from the **Incident Response** list. All Incident responses, including the default and any you have already defined, are available in the list. See "Setting up Incident Responses" on page 191 for more information about defining them.
5. (*Optional*) In the **Description** field, type a description of the settings. The description might indicate which clusters should be assigned these custom settings, for example.
6. In the threshold properties table (shown above), find the metric whose threshold you want to change.
7. In the **Threshold** column, leave the default units (`Percentage`), or select **None** to disable threshold monitoring.
8. Type a new value for the threshold, if desired. By default, an Incident is created if more than **50%** of the devices that were active on servers in this call server group at the beginning of the reporting interval underwent a status change during that interval.

   See "Call Server Group Threshold Settings" on page 151 for an explanation of each default call server group threshold setting.

   Note: Set a lower value for the threshold if you want to see Incidents more quickly in response to call server or phone issues. Set a higher value to see Incidents only after more device deregistration or registration activities are observed. If the minimum value is not met during a monitoring interval, no Incident is created.

9. Click **Save** to save the new call sever group thresholds and return to the Call Server Group Threshold List page. The new set of thresholds now appears in the list.

   Or click **Save and Add Another** to save the new call server group threshold settings and return to the Call Server Group Threshold Properties page, where you can add another set of custom thresholds.

Now that you have customized a set of thresholds, you need to apply the settings to a call server group, representing a call server cluster. Only then will the new settings you have just selected for the threshold metrics be applied to any cluster. See the following topic, "Assigning Call Server Group Thresholds."

Assigning Call Server Group Thresholds

The call server group thresholds are appropriate for call server clusters because they apply to functionality that is often shared among the call servers in a cluster. A set of pre-defined threshold values is applied to all the call server groups you create unless you assign custom threshold values to selected call server groups.

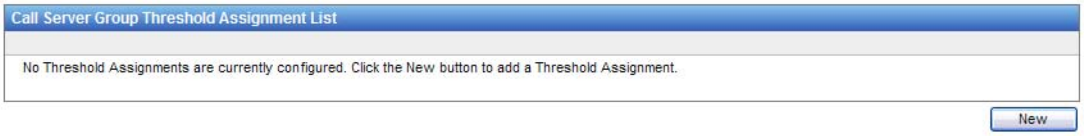
Before you can assign call server group thresholds, you should create at least one call server group that contains at least one Cisco call server. Or you can rename the default ("Unassigned") group to identify it in reports. See "Creating a Call Server Group" on page 139 for more information.

To assign a custom set of call server group thresholds:

You must have customized at least one set of call server group thresholds before you attempt to apply them to a call server group. Follow the steps outlined above in "Customizing Call Server Group Thresholds" on page 181.

1. In the navigation links, click **Administration > Policies > Call Servers**, and then click **Call Server Group Threshold Assignments**.

   The Call Server Group Threshold Assignment List page is displayed:



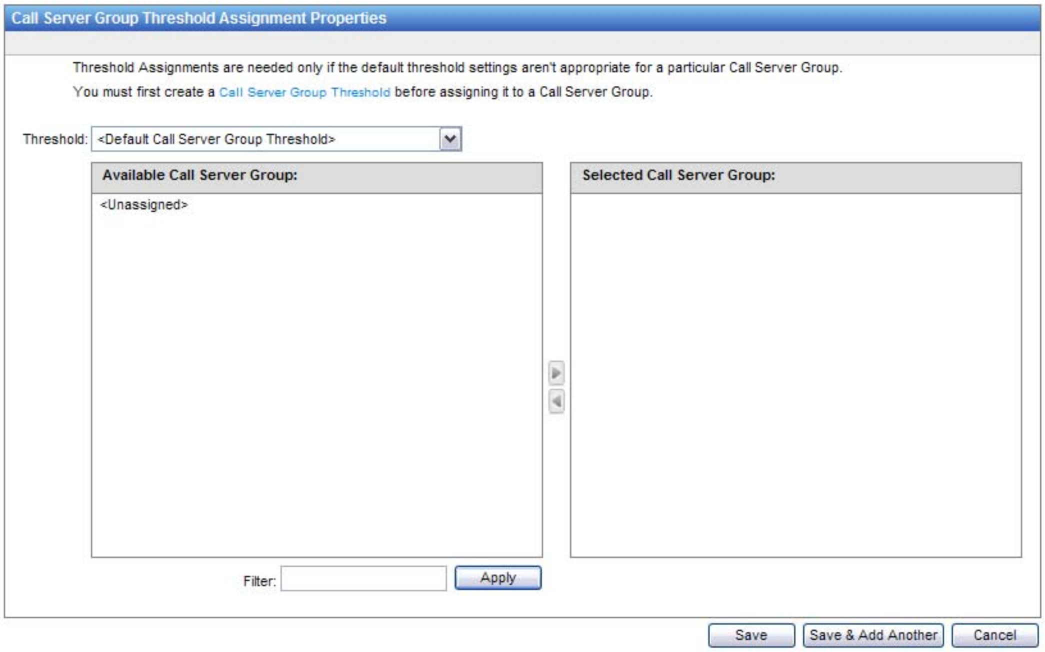
Call Server Group Threshold Assignment List

No Threshold Assignments are currently configured. Click the New button to add a Threshold Assignment.

   All the call server group threshold assignments in the system are shown in the list. Before you have assigned any thresholds to call server groups, a message states, `No Threshold Assignments are currently configured`.

2. Click **New** to create a new call server group threshold assignment.

   The Call Server Group Threshold Assignment Properties page is displayed:



Call Server Group Threshold Assignment Properties

Threshold Assignments are needed only if the default threshold settings aren't appropriate for a particular Call Server Group.

You must first create a Call Server Group Threshold before assigning it to a Call Server Group.

Threshold: <Default Call Server Group Threshold>

Available Call Server Group: <Unassigned>

Selected Call Server Group:

Unless they have already been assigned to a set of custom threshold settings, all call server groups that contain at least one Cisco call server are shown in the **Available Call Server Groups** list.

3. From the **Threshold** list, select the name of the threshold settings to assign to this group.
4. Select any groups to which you want to apply a set of custom thresholds and Incident responses. Use **Ctrl + Click** or **Shift + Click** to select a range of items. Double-click to move the items to the **Selected Call Server Groups** list.
5. Click **Save** to save the new call server group threshold assignment. You return to the Call Server Group Threshold Assignment List page. The new assignment now appears in the list.

   Or click **Save and Add Another** to save this assignment and return to the Call Server Group Threshold Assignment page.

The **Filter** field accepts search strings to limit the data shown in the Call Server Groups list. Wildcard characters are added for you before and after the string when you click **Apply**, so do not include * or % characters.

Filtering can be very useful if you have a long list of call server groups defined.

Example: To see only call server groups whose names begin with NC Office, you would enter `nc` for the filter and click **Apply**. Any groups whose name includes `NC` would be shown in the list.

Editing Call Server Group Threshold Settings

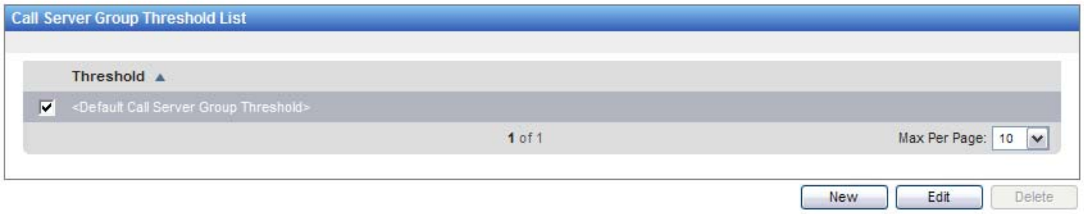
The call server group thresholds you have customized can be edited. For example, after a few days of data collection, you may decide to increase the value you selected for the percentage of phones that have status changes for a particular group so that you'll receive fewer Incidents. Or you may want to edit the assignment of a named set of thresholds so that the settings are applied to additional groups you've created.

Instructions for editing threshold settings and editing threshold assignments are provided below.

To edit call server group threshold settings:

1. In the navigation links, click **Administration > Policies > Call Servers**, and then click **Call Server Group Thresholds**.

   The Call Server Group Threshold List page is displayed:



Call Server Group Threshold List

	Threshold ▲
☑	<Default Call Server Group Threshold>

2. Select the settings you want to edit.
3. Click **Edit**.

   The Call Server Group Threshold Properties page is displayed. See "Customizing Call Server Group Thresholds" on page 181 for information about the options on this page.
4. Click **Save** to save your changes to the settings.

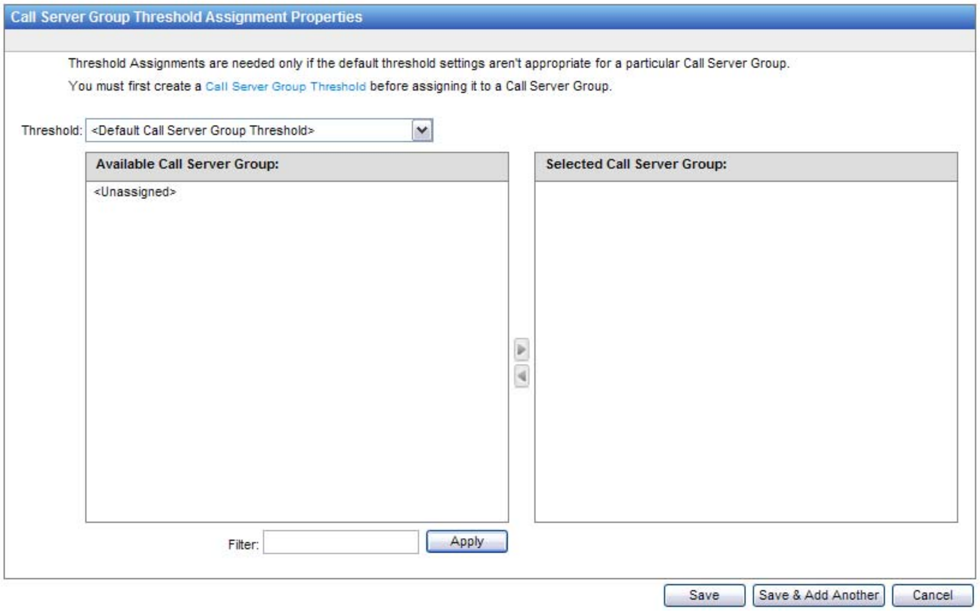
Your changes are applied to the next data-collection interval. Data already collected is not re-evaluated using the new settings.

To change the assignment of a set of call server group thresholds:

1. In the navigation links, click **Administration > Policies > Call Servers**, and then click **Call Server Group Threshold Assignments**.

   The Call Server Group Threshold Assignment List page is displayed.
2. Select the settings you want to edit.
3. Click **Edit**.

   The Call Server Group Threshold Assignment Properties page is displayed:



Call Server Group Threshold Assignment Properties

Threshold Assignments are needed only if the default threshold settings aren't appropriate for a particular Call Server Group.

You must first create a Call Server Group Threshold before assigning it to a Call Server Group.

Threshold: <Default Call Server Group Threshold>

Available Call Server Group:	Selected Call Server Group:
<Unassigned>	

Filter:

4. Select a different set of threshold settings from the **Threshold** list.
5. Click **Save** to save the new assignment. You return to the Call Server Group Threshold Assignment List page. The new assignments now appear in the list.

Your changes are applied to the next data-collection interval. Data already collected is not re-evaluated using the new settings.

Deleting a Set of Custom Call Server Group Thresholds

You can delete any call server group thresholds that are not currently assigned to a call server group. If you attempt to delete a set of assigned thresholds, a warning is displayed, and the deletion fails.

After a set of call server group thresholds has been assigned to a group, you must first edit the set to remove the assignment before you can delete it. Click the **Threshold** column in the Call Server Group Threshold Assignment List to sort by threshold name and see whether the set has been assigned.

The online Help contains a full set of instructions for deleting assigned and unassigned call server group thresholds.

Customizing Codec Thresholds

Codec-based thresholds supplement call quality performance thresholds to help you better understand and manage call quality. Unified Communications Monitor provides a wide range of pre-defined codecs, with default thresholds for their expected MOS values and, where applicable, Network MOS values. The basic feature allows you to set MOS thresholds either relative to codec performance or as fixed MOS values.

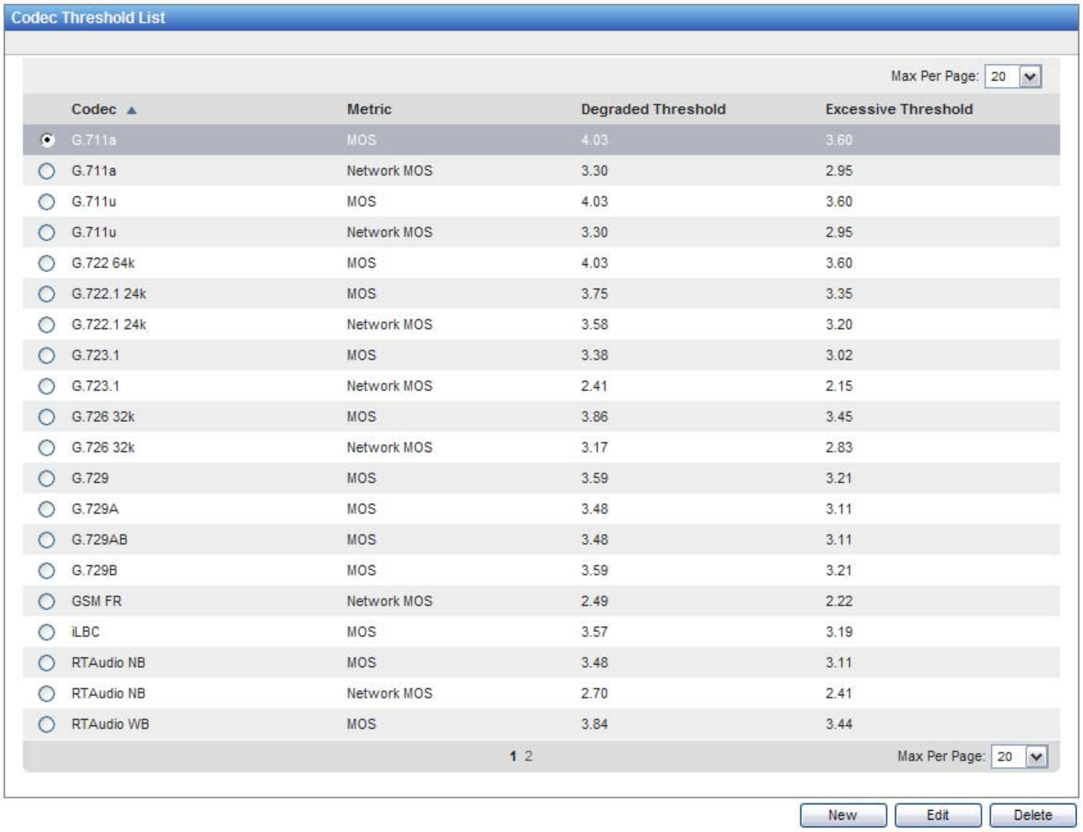
By default, codec thresholds are enabled. Unified Communications Monitor therefore uses a set of pre-defined threshold values, automatically applying appropriate thresholds based on the codecs that are detected in use during monitoring. The default threshold values are based on unique codec attributes, such as theoretical maximum MOS. But you can also customize these values.

All the available codec thresholds are shown in the **Codec Threshold List**, including any custom thresholds you have created. By default, any values currently defined for a particular codec are used each time that codec is detected in call traffic. For a table of default codec threshold values, see "Codec Threshold Settings" on page 155.

To customize codec threshold values:

1. In the navigation links, click **Administration > Policies > Call Performance**, and then click **Codec Thresholds**.

   The first page of the Codec Threshold List is displayed:



Codec Threshold List

Max Per Page: 20

	Codec ▲	Metric	Degraded Threshold	Excessive Threshold
●	G.711a	MOS	4.03	3.60
○	G.711a	Network MOS	3.30	2.95
○	G.711u	MOS	4.03	3.60
○	G.711u	Network MOS	3.30	2.95
○	G.722 64k	MOS	4.03	3.60
○	G.722.1 24k	MOS	3.75	3.35
○	G.722.1 24k	Network MOS	3.58	3.20
○	G.723.1	MOS	3.38	3.02
○	G.723.1	Network MOS	2.41	2.15
○	G.726 32k	MOS	3.86	3.45
○	G.726 32k	Network MOS	3.17	2.83
○	G.729	MOS	3.59	3.21
○	G.729A	MOS	3.48	3.11
○	G.729AB	MOS	3.48	3.11
○	G.729B	MOS	3.59	3.21
○	GSM FR	Network MOS	2.49	2.22
○	iLBC	MOS	3.57	3.19
○	RTAudio NB	MOS	3.48	3.11
○	RTAudio NB	Network MOS	2.70	2.41
○	RTAudio WB	MOS	3.84	3.44

1 2

Max Per Page: 20

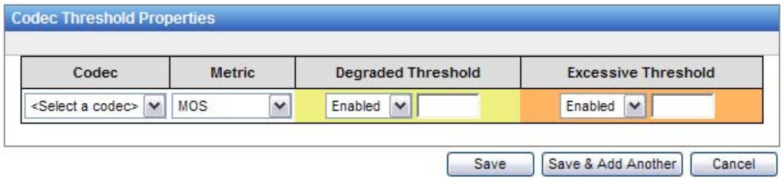
   The list shows all the default codec threshold settings.

Note: These values are based on published industry performance data, specifically on the theoretical maximum MOS scores associated with each codec.

2. Click **New** to customize the threshold settings for a codec.

   Note: New codecs cannot be added. For more information, see "More about Codec Thresholds" on page 157.

   The Codec Threshold Properties page is displayed:



Codec Threshold Properties

Codec	Metric	Degraded Threshold	Excessive Threshold
<Select a codec>	MOS	Enabled	Enabled

   A set of codec threshold values includes two value parameters for each metric. For most codecs, only the **MOS** metric is available. The Microsoft proprietary codecs offer an additional metric, the **Network MOS**.

3. In the **Codec** list, select the codec whose settings you're customizing.
4. In the **Metric** list, select the metric to customize, either **MOS** or **Network MOS**.
5. For the **Degraded Threshold**, select **Disabled** if you want to disable alerting for that threshold.

   Or leave the default (`Enabled`) and type a new value for the threshold metric. All codec thresholds accept MOS values from **1.00** to **5.00**, inclusive.

   - See "Codec Threshold Settings" on page 155 for an explanation of the default settings.
   - See the Appendix about MOS calculations in the *User Guide* for more information about the MOS metric.

6. Repeat the same steps to set a value for the Excessive threshold (or to disable alerting).

   Note: The value you select for the Excessive threshold must be more severe than the Degraded threshold value. For example, if the value for the Degraded threshold is 4.02, the value for the Excessive threshold must be *less than* 4.02, indicating a *lower* Mean Opinion Score and thus, a more severe decline in performance.

7. Click **Save** to save the new codec thresholds and return to the Codec Threshold List page. The new threshold settings now appear in the list.

   Or click **Save and Add Another** to save the new codec threshold settings and return to the Codec Threshold Properties page, where you can add another set of custom thresholds.

Now that you have customized codec thresholds, you need to enable the **Codec** option within a set of Call Quality performance threshold settings and make sure those settings have been assigned to a pair of Locations or media devices. Only then will the new values you have just selected for the MOS metrics be applied to any Locations or devices. See "Customizing Call Quality Thresholds" on page 169 for more information.

Editing Codec Threshold Settings

Both pre-defined and custom codec thresholds can be edited. For example, after a few days of data collection, you may decide to increase the value you selected for the G.711u 56k codec Degraded threshold so that you'll receive fewer Incidents.

No custom codec threshold settings are applied unless you enable the **Codec** option for the **MOS** metric on the Call Quality Threshold Properties page and then assign the custom set of Call Quality performance threshold settings to a pair of Locations and/or media devices. See the following topics for more information:

- "Customizing Call Quality Thresholds" on page 169
- "Assigning Call Quality Thresholds to Pairs of Locations or Devices" on page 171

Instructions for editing threshold settings are provided below.

To edit codec threshold settings:

1. In the navigation links, click A**dministration > Policies > Call Performance**, and then click **Codec Thresholds**.

   The Codec Threshold List page is displayed.

   Note: All codec types that are supported for the codec threshold feature are included in the list. The list includes pre-defined codecs and those discovered during call quality monitoring on your system. You cannot add new codecs to the list.
2. Select the codec whose threshold settings you want to edit. If necessary, click the page number link at the bottom of the list to see a second page of pre-defined codecs.
3. Click **Edit**.

   The Codec Threshold Properties page is displayed. The codec you selected is indicated in the first column of the properties table.

   See "Customizing Codec Thresholds" on page 187 for information about the options on this page.
4. Click **Save** to save your changes to the settings.

Your changes are applied to the next data-collection interval. Data already collected is not re-evaluated using the new settings.

Deleting Custom Codec Thresholds

You can delete any codec thresholds that you have customized. However, it is usually easier simply to disable them. Disabling codec thresholds is accomplished by disabling Call Quality performance monitoring by codec. You can do this by editing the set of custom Call Quality performance thresholds where performance monitoring by codec is enabled.

Below, instructions for disabling codec thresholds in performance monitoring and for deleting unwanted, custom codec thresholds are provided.

To disable Call Quality monitoring by codec:

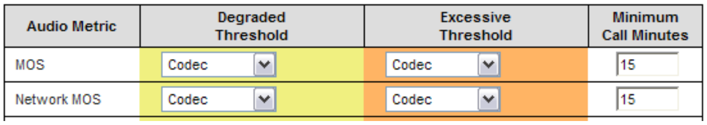
1. In the navigation links, click **Administration > Policies > Call Performance**, and then click **Call Quality Thresholds**.

   The Call Quality Threshold List page is displayed.

2. Click to select the set of Call Quality performance thresholds that you want to edit.
3. Click **Edit**.

   The Call Quality Threshold Properties page is displayed.

   Call Quality monitoring by codec is associated with either the MOS or Network MOS Audio metric. It is enabled by default. Its enabled status is indicated by the **Codec** value in the Degraded and Excessive Threshold columns:



Audio Metric	Degraded Threshold	Excessive Threshold	Minimum Call Minutes
MOS	Codec	Codec	15
Network MOS	Codec	Codec	15

4. Click to select **MOS** for either the Degraded or Excessive threshold. Because the codec threshold option must be applied to both threshold levels, this action disables the codec threshold for both the Degraded and Excessive MOS values.

   Note: You can also select **None** for the threshold value. This option not only disables the codec threshold, but also disables alerting for the associated MOS metric. We do not recommend disabling monitoring of any threshold metric.

5. Default MOS values associated with the most common VoIP audio codecs are shown. If desired, click to supply new values.
6. Click **Save** to save your changes to the set of Call Quality performance thresholds.

If they were already assigned to a pair of Locations and/or media devices, the Call Quality performance threshold settings remain assigned. However, the associated codec threshold is not used; instead, the MOS value included in the threshold settings is applied.

To delete a set of custom codec thresholds:

1. In the navigation links, click **Administration > Policies > Call Performance**, and then click **Codec Thresholds**.

   The Codec Threshold List page is displayed.

2. Select the set of thresholds you want to delete.
3. Click **Delete**.
4. Click **OK** to confirm the deletion.

The set is deleted and no longer appears in the Codec Threshold list.

However, as soon as that codec is detected during call quality monitoring, it is restored in the list, with the UC Monitor pre-defined threshold settings. These settings are not used in call quality performance monitoring unless you re-enable the codec threshold setting in a set of Call Quality performance thresholds and assign them to a pair of Locations and/or devices.

Setting up Incident Responses

Incident responses are actions to be taken automatically in response to a threshold violation. The actions available for Incident responses include notifications, via email or SNMP trap, or an Investigation, depending on the type of Incident.

You can set up different responses for each Location, for each media device, for each call server or call server group, or for selected pairs of components. Although you can create a common set of Incident responses that apply equally to call performance or call server Incidents, they are applied along with threshold customizations, and are therefore assigned either to single components or pairs of components just as thresholds are. See the following for more information:

- “Customizing Call Setup Thresholds” on page 162
- “Customizing Call Quality Thresholds” on page 169
- “Customizing Call Server Thresholds” on page 176
- “Customizing Call Server Group Thresholds” on page 181

By default, no actions are associated with Incident responses. However, you can configure the following Incident response actions:

Type of Incident	Applicable Actions	Description
Call Performance: Call Setup	Send Email	Notification: Send an email message to selected user(s).
	Send SNMP Trap	Notification: Send an SNMP trap to selected computer(s).
	Launch Traceroute Investigation	Action: Run a traceroute to the affected Location or voice gateway and report the results
Call Performance: Call Quality	Send Email	Notification: Send an email message to selected user(s).
	Send SNMP Trap	Notification: Send an SNMP trap to selected computer(s).
Call Server or Call Server Group	Send Email	Notification: Send an email message to selected user(s).
	Send SNMP Trap	Notification: Send an SNMP trap to selected computer(s).
Call Server Group	Launch Traceroute Investigation	Action: Run a traceroute to any key phones that have been defined at affected Locations. See the **Note**, below, for more information.
Collector	Send Email	Notification: Send an email message to selected user(s).
	Send SNMP Trap	Notification: Send an SNMP trap to selected computer(s).

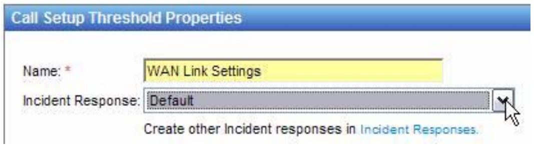
Note: If you have set up a Launch Traceroute Investigation Incident response action for the Phone Status Changes Incident, the traceroute is only sent to key phones. Thus, if the percentage of phone status changes at a particular call server group crosses the threshold, the traceroute is only launched if key phones have been defined at any of the Locations whose phones had applicable status changes.

One other Incident response action is static. The Launch Call Watch Investigation action occurs automatically in response to a poor call quality (QRT) call server Incident. This action cannot be disabled.

Incident responses should be edited in the context of an overall strategy for notifying network personnel of any issues in your UC deployment. Be sure to read "Understanding Performance Thresholds" on page 144 and "Understanding Incidents and Incident Responses" on page 158 before you try to edit the default Incident responses to add actions.

Creating a New Incident Response

Incident responses are applied during threshold customization. The Call Setup and Call Quality Properties pages include an Incident Response list, which contains all available Incident Responses. UC Monitor provides a single default Incident response, `<Default>`, which does not have any actions associated with it.



Call Setup Threshold Properties

Name: * WAN Link Settings

Incident Response: Default

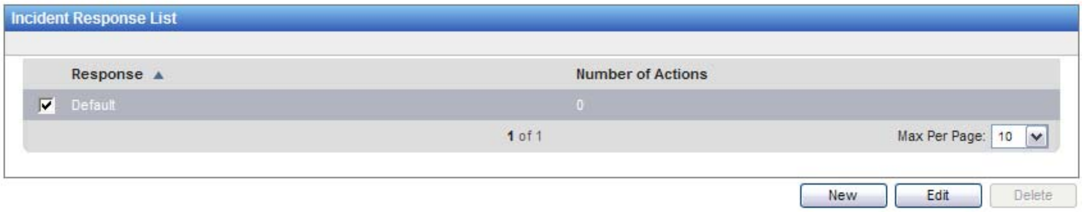
Create other Incident responses in Incident Responses.

To associate Incident response actions with performance thresholds, you will need first to create at least one Incident response, select at least one action to go with that response, and then select that Incident response during threshold customization.

To create an Incident response:

1. In the **navigation links**, click **Administration > Policies**, and then click **Incident Responses**.

   The Incident Response List page is displayed:



Incident Response List

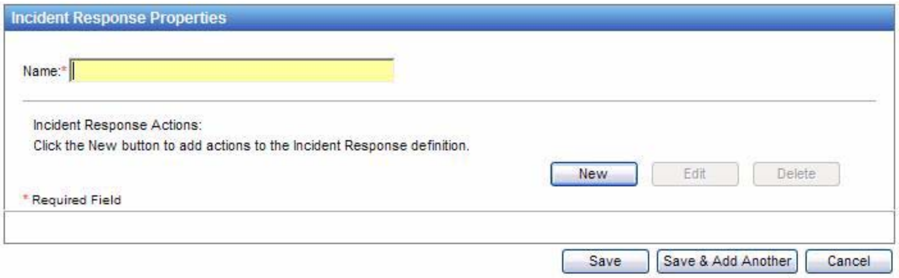
	Response ▲	Number of Actions
☑	Default	0

1 of 1

Max Per Page: 10

2. Click **New**.

   The Incident Response Properties page is displayed:



Incident Response Properties

Name:*

Incident Response Actions:
Click the New button to add actions to the Incident Response definition.

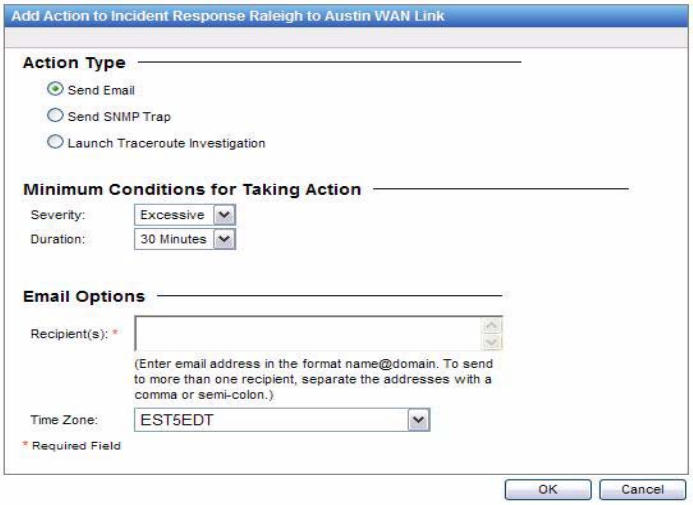
* Required Field

3. Type a name for this Incident response.

   The name helps you identify this response so that you can assign it to a threshold. It appears in a list of responses on the Threshold Properties page.

4. By default, no actions are associated with the new Incident response. Click **New** to add an action.

   The Add Action in Incident Response page is displayed:



Add Action to Incident Response Raleigh to Austin WAN Link

Action Type

● Send Email
○ Send SNMP Trap
○ Launch Traceroute Investigation

Minimum Conditions for Taking Action

Severity: Excessive
Duration: 30 Minutes

Email Options

Recipient(s): *

(Enter email address in the format name@domain. To send to more than one recipient, separate the addresses with a comma or semi-colon.)

Time Zone: EST5EDT

* Required Field

5. First, click to select the **Action Type**, which determines the other selections on this page. Select either:

   - **Send Email** — Lets you supply an email address for the person(s) to notify when the associated threshold is violated.
   - **Send SNMP Trap** — Lets you supply parameters for an SNMP trap to be sent to a third-party network monitoring platform.
   - **Launch Traceroute Investigation** — Runs a traceroute automatically to collect extra data about routing from the affected Location or voice gateway.

   Note: The **Launch Traceroute Investigation** action type is designed for call setup and call server group Incidents only. If you assign this action to other Incident types, the traceroute may not be run, or the results may be unhelpful. See "How Incidents Trigger Responses" on page 159 for more information.

6. Set the conditions under which the action should be taken, parameters that control who receives the notification, and the format of the notification.

   The following options are available:

Action Property	Description
Minimum Conditions for Taking Action	
Severity	The minimum conditions setting lets you select the threshold conditions that must be detected before the action is launched. Severity refers to the threshold severity level that, when crossed, can trigger this action. Select either: • Degraded, or • Excessive ***Note:*** Severity does not apply to the automatic actions initiated in response to Collector Incidents, call server Incidents, or call server group Incidents. These actions are always performed. Also note that Incidents of these types always have a severity of Excessive.
Duration	The duration of the condition; the length of time that the collected data values must violate the threshold before the action is launched. The threshold itself already enforces a minimum number of data samples that must report poor performance before the threshold is considered to be violated and an Incident is launched. This parameter adds flexibility to Incident reporting. Use this parameter to launch actions either more or less quickly in response to threshold violations. For example, you may be concerned about latency. The default Latency threshold specifies a minimum observation count of 15 call minutes, which corresponds to three reporting intervals. If you select 30 minutes for the **Duration**, the UC Monitor system sends an email message only if delay totals exceed the 150 ms threshold for 30 minutes, or six consecutive reporting intervals.
Email Options	
Recipients	The full email address of the person (such as a network operator) who should receive an automatic email notification about this particular type of Incident. Select someone who is most likely to respond quickly and accurately to remedy the problem that caused the Incident. Use the following format: `username@domain.com` If desired, enter multiple email addresses separated by commas or semicolons and no spaces.
Time Zone	The time zone of the email recipient's locale. The default time zone is the same as the locale where the UC Monitor Management Console is installed.
SNMP Trap Options	
Send SNMP trap to	The IP address of the computer to which you want to send the SNMP trap. ***Note:*** CA has included a MIB file containing the OIDs unique to the UC Monitor product so that you can import them into your trap receiver. The file is located in the following directory on the Management Console: `netqos\VoIPMonitor\MIB\NETQOS-VMTRAP-MIB.txt` To send a trap to more than one computer, you should create additional actions within the same response, one for each additional trap destination.

Action Property	Description
Time Zone	The time zone of the trap recipient's locale. The default time zone is the same as the locale where the UC Monitor Management Console is installed.
Severity updates	Parameters for SNMP traps. Traps can be sent each time an Incident is updated. The topic titled "How Incidents Trigger Responses" on page 159 explains the logic that determines when Incidents are updated or closed. Click to select either: • **Send update traps when Incident severity changes**: Send an SNMP trap if the Incident severity changes, but the Incident remains open. If you select this option, traps are also sent when a new Incident is opened. • **Send only Incident open and close traps**: Only send an SNMP trap if a new Incident is opened or if an Incident is closed. Some Incident types do not have a Severity parameter (the poor call quality [QRT] Incident, for example), or their severity is always Excessive. If you select the option to **Send update traps when Incident severity changes**, the option to send only open and close traps is used instead for these Incidents.

7. Click **OK**. The action is updated to reflect the selected parameters.
8. On the Incident Response Properties page, click **Save** to save the new Incident response with its associated action.

To associate Incident responses with thresholds, edit the thresholds themselves. Refer to "Customizing Call Setup Thresholds" on page 162 or "Customizing Call Quality Thresholds" on page 169.

Editing an Incident Response

The UC Monitor software provides one default Incident response, which is not associated with an action. You can edit the default Incident response to add an action. Or you can create new Incident responses with actions, and edit them later to add or change the associated actions.

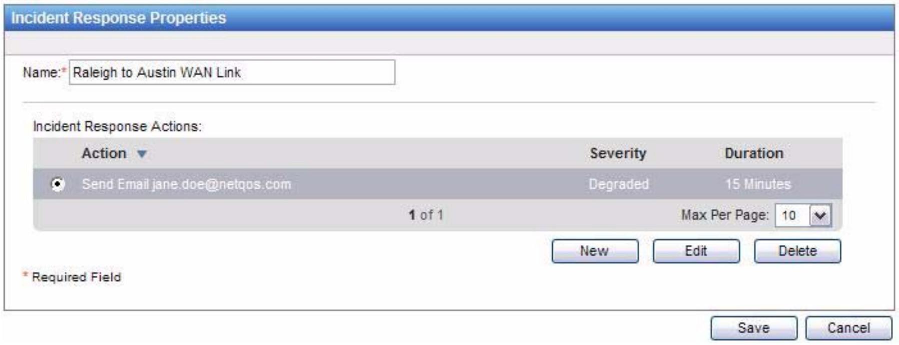
You can do any of the following when you edit an Incident response:

- Add an action (multiple actions are allowed).
- Change or delete an action you've added.
- Change the threshold parameters that control when the response is launched.

To edit an Incident response:

1. In the **navigation link**s, click **Administration** > **Policies** > **Incident Responses**.
2. In the Incident Response list, click to select the Incident response that you want to edit.
3. Click **Edit**.

   The Incident Response Properties page is displayed:



Incident Response Properties

Name:* Raleigh to Austin WAN Link

Incident Response Actions:

	Action	Severity	Duration
●	Send Email jane.doe@netqos.com	Degraded	15 Minutes

1 of 1 Max Per Page: 10

* Required Field

4. In the Incident Response Actions list, click to select the Incident response action that you want to change.
5. Click **Edit**.

   The Edit Action in Incident Response page displays. The fields on this page are described above in "Creating a New Incident Response" on page 192.

   Note: Multiple email recipients are allowed; separate multiple addresses with commas and no spaces.
6. Make your changes to the action and click **OK**.

   The changes do not appear in the Incident Response Actions list until you click **Save** on the Incident Response Properties page.

   A given Incident response can have multiple actions associated with it. To add a second action to an Incident response, click **New**.
7. Follow the steps provided in "Creating a New Incident Response" on page 192 to configure the additional action, and click **OK** when you have finished.
8. On the Incident Response Properties page, click **Save** to save your changes.

The Incident response is updated to reflect your changes.

Now you need to associate the response with a set of thresholds. See "Customizing Call Setup Thresholds" on page 162 or "Customizing Call Quality Thresholds" on page 169 for more information.

CHAPTER 8

Using Troubleshooting Features

CA NetQoS Unified Communications Monitor offers additional features to gather information useful for troubleshooting specific problems that have been detected from routine monitoring.

The **Call Watch** feature collects data from real-time monitoring of selected phone directory numbers (DNs) for troubleshooting and presents it in a Call Watch report. This feature is distinct from the core monitoring functionality that the Collector provides, which is largely passive monitoring based on the collection of all VoIP-related data from a selected switch. It is supported in Cisco and Avaya environments.

The **traceroute investigations** feature allows you to configure a traceroute test to run automatically as an Incident response or to launch a traceroute test on demand, to a selected target. For more information about Incident responses, see "Creating a New Incident Response" on page 192. On-demand traceroute investigations are discussed in this chapter.

As the UC Monitor Administrator, you are also responsible for determining which users have permission to launch a Call Watch and a traceroute investigation. See "UC Monitor Roles" on page 231 for more information.

This chapter covers the following topics:

- "About the Call Watch Feature" on page 198
- "Setting Up a Call Watch Definition" on page 202
- "Launching a Traceroute Investigation" on page 205

The "UC Monitor Reports" chapter of the *UC Monitor User Guide* contains a full discussion of the reports associated with the Call Watch and investigations features and explains the metrics and path information that are gathered.

About the Call Watch Feature

The UC Monitor Call Watch feature provides an extra layer of call quality monitoring and can gather additional data from a potential problem area to use in troubleshooting. With the Call Watch feature, you can instruct the Collector to actively collect detailed, real-time call data for all calls made to and from a single, selected phone number.

All calls made in an Avaya (Aura) Communication Manager environment are automatically watched. Data from these calls is displayed in the Call Watch Overview Report, with a **Type** of **Automatic**. You still have the option to set up a manual Call Watch for a selected Avaya phone; this option stores the Call Watch data in the UC Monitor database for a longer period of time.

For Cisco monitoring, you must set up a Call Watch definition by supplying a DN and the duration of the watch period. If a user complained of poor call quality, for example, you could initiate a Call Watch for her phone number to collect additional performance data. In the resulting report, you would notice patterns in the measurements that would help you sort out the underlying problem.

An active Call Watch provides real-time reporting and drilldown for detailed metrics. In the Call Watch Overview Report, you can watch and analyze the data as it comes in from an in-progress call. For more information, see the Reports chapter of the *UC Monitor User Guide*.

Note: Call Watch is not supported for endpoints in a Microsoft Office Communications Server environment. In addition, a few older Cisco IP phone models do not support the collection of all Call Watch statistics. The Call Watch Reports will show no data for the statistics that are not supported.

How the Collector Gathers Call Watch Data

Call Watch is supported by equipment from Cisco and Avaya, but the methods used in each environment are slightly different. Unlike the passive monitoring performed by the Collector at the core switch in a Cisco environment, a Call Watch is performed by means of active data collection: the Collector conducts active polling of the IP phones. When you create a Call Watch definition for a Cisco phone and reload the Collector, the Collector is notified of the DN for the selected phone. As soon as it detects any call activity involving that phone number, the Collector begins polling the phone, or, if the number corresponds to an analog phone in the PSTN, it polls the relevant voice gateway for call performance data.

As it “watches” a Cisco IP phone, the Collector communicates with the phone via HTTP to collect in-progress call performance data from the phone’s Web page. The HTTP query occurs every 15 seconds during each active call until the watch period expires. If an analog phone in the PSTN is watched, the Collector uses SNMP to query the MIB of the voice gateway every 15 seconds. Performance data is immediately reported.

By contrast, a Call Watch occurs automatically when a supported Avaya endpoint makes a call using the Communication Manager. Avaya endpoints send in-progress call quality information via RTCP to the Collector every 15 seconds or so (the reporting interval can be changed). In turn, the Collector reports this information to the Management Console in near real-time. Reporting continues until the call is terminated.

Through these methods, the UC Monitor system can gather the following information from either the IP phone or voice gateway device. Note that some metrics are vendor-specific: :

Type of Data	Description
Delay to Dial Tone	The time it took, in milliseconds, for the calling phone to receive a dial tone from the call server or voice gateway.
Post-Dial Delay	The time between entering the last digit of a telephone number and receiving a ring or call connect.
MOS	The Mean Opinion Score (MOS) Listening Quality (LQK) is a call quality score based on impairments to the audio signal. This score is updated every second during a single voice stream and based on data traveling toward the listener. The *UC Monitor User Guide* includes an appendix that contains a full discussion of MOS values and how they are derived.
Packet Loss	Number of data packets lost in transit, expressed as a percentage of all packets in the stream.
Latency	One-way delay, calculated from the calling party to the called party. Latency of 200 ms and higher has a noticeable effect on call quality.
Jitter Buffer Loss	Percentage of packets lost due to jitter buffer overruns or underruns. Different metrics are collected based on the type of phone watched (analog or digital).
Jitter Buffer Delay	The delay introduced by the receiver while it holds one or more packets to reduce variations in packet arrival times.
Jitter Buffer Over Runs	The number of times that the actual jitter (variation among packet delay values) exceeded the maximum size setting of the jitter buffer. Usually packet loss is a result.
Jitter Buffer Under Runs	The number of times that the jitter buffer became empty. Usually indicates that delays are too lengthy for the buffer setting.
Jitter Max Jitter	The average or maximum jitter (variation in delay times among packets in the same stream, in milliseconds), measured for each call leg.
Sequence Jumps	The number of times that at least one consecutive packet was lost.
Max Sequence Jump	The maximum number of consecutive packets that were lost during any reporting interval.
Sequence Falls	The number of times that at least one packet arrived out of order.
Max Sequence Fall	The maximum number of packets that arrived out of order for any reporting interval.
ACOM	Sum of the following values recorded for a VoIP phone call: • Echo Return Loss (ERL) • Cancellation loss • Nonlinear processing loss **PSTN calls only.**
ERL	Echo Return Loss (ERL) — Reduction in the echo level produced in the circuit without an echo canceler. **PSTN calls only**.
Signal In	Signal level of the data flow traveling into the echo canceler. **PSTN calls only**.

Type of Data	Description
Signal Out	Signal level of the data flow traveling out of the echo canceler toward the IP network. **PSTN calls only**.
Concealed Seconds	Number of call seconds that had concealment events (due to lost packets) from the start of the voice stream. **IP phone calls only**.
Severely Concealed Seconds	Number of call seconds that had more than 5% concealment events from the start of the voice stream. **IP phone calls only**.

More information about the metrics in the Call Watch reports is available in the online Help and in the Reports chapter of the *UC Monitor User Guide*.

Example of How to Use the Call Watch Feature

The Call Watch feature is specially designed for troubleshooting a reported problem with call setup or call quality. An example of when you would want to set up a Call Watch for a Cisco phone would be something like the following:

1. A coworker submits a Help Desk ticket claiming that the audio quality of the last call he made from his IP phone was very poor.
2. You set up a Call Watch, using the coworker's phone number and lasting two hours.
3. When you call the coworker at his desk, you ask him to make the call again to help you test the system.
4. When he makes the call again, the Call Watch feature performs extra polling to gather information about call performance.
5. You access the Call Watch Real-Time Report and watch the incoming data. Jitter and latency measurements are high, and the MOS value for the call is only 3.3.
6. You click the MOS bar chart to see which direction of the call was affected and note that the poor performance is occurring between the called party's phone (which is located in the PSTN) and the coworker's phone in the incoming direction only.

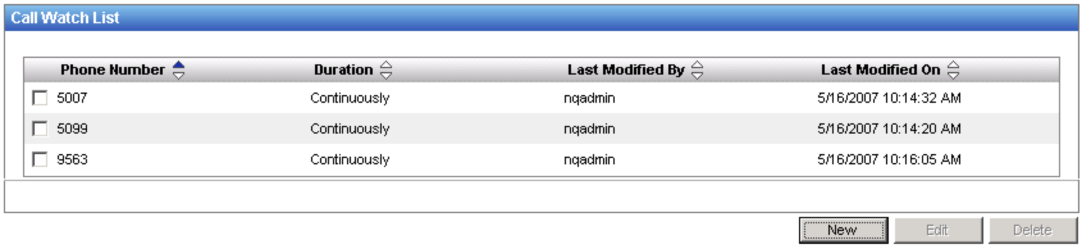
   This information indicates that the problem is most likely occurring at the voice gateway.
7. You scroll toward the bottom of the Call Watch Report. Gateway-only metrics are shown below the charts of call quality metrics. You can see from the ACOM detailed chart that PSTN calls involving this gateway have very low ACOM values, which could indicate a problem with excessive echo.

As a next step, you will need to determine whether the echo canceller is functioning properly.

Viewing the Call Watch List

Each time you set up a Call Watch, a new Call Watch definition appears in the Call Watch List.

The Call Watch List is accessible from the navigation links. Click **Troubleshooting > Call Watch**, and then click **Definitions**:


Call Watch List

	Phone Number	Duration	Last Modified By	Last Modified On
□	5007	Continuously	nqadmin	5/16/2007 10:14:32 AM
□	5099	Continuously	nqadmin	5/16/2007 10:14:20 AM
□	9563	Continuously	nqadmin	5/16/2007 10:16:05 AM

The following information about each Call Watch definition is provided on the Call Watch List page:

Column Title	Definition
Phone Number	The phone number (or DN) used to call this telephone or IP phone, in the format 8887675443.
Duration	The length of time that the Call Watch will be performed. The date and time when UC Monitor will stop watching this phone are shown.
Last Modified by	The username of the user who set up this Call Watch.
Last Modified on	The date and time the Call Watch was set up; also the date and time when calls from and to this phone began to be actively monitored.

Click **New** to begin setting up a new Call Watch. For more information about setting up a Call Watch, see the topic "Setting Up a Call Watch" on page 203.

Call Watch List Limits

Both the Call Watch Overview Report and the Call Watch list have limits that affect the number of items displayed. Avaya Call Watch data accumulates rapidly because all calls made by Avaya phones are automatically watched. As a result, Call Watch data from such "automatic" Call Watch entries is purged after seven days. To gather Call Watch data for an Avaya phone and retain it for a longer period of time, set up a manual Call Watch for that phone.

Unified Communications Monitor supports up to 50 simultaneous Call Watch definitions. However, this limit requires some clarification. Up to 50 IP or analog phones—specifically, voice gateways, which are actively polled during watched calls involving the PSTN—may be watched simultaneously. But because every call involves two conversing parties, the limit of 50 may mean that as few as 25 calls are displayed in the Call Watch List if all the phones (both calling party and called party) are actively being watched. The number of Call Watch definitions shown in the list depends on:

- How you set up each definition.
- The specific calls being made at a given moment.

In addition, be aware that the limit of 50 simultaneous Call Watch definitions is a per-Collector limit. This means that in a standalone implementation of the UC Monitor system:

- A limit of 50 watched entries in the Call Watch list is enforced if only 1 phone involved in each call is actively being watched (that is, is defined as the watched phone).
- A limit of 25 watched entries in the Call Watch list is enforced if both phones in each call are actively being watched.
- A limit of anywhere from 25 to 50 watched entries in the Call Watch list is enforced, depending on how many phones are both in use and actively being watched.

If you have multiple Collectors (a Distributed UC Monitor system), multiply the number of Collectors by the per-Collector limits discussed above to see how many calls defined in the Call Watch list may be concurrently active.

Setting Up a Call Watch Definition

When you set up a Call Watch, you instruct the Collector to actively collect detailed, real-time call data for all calls made to and from a single, selected phone DN for a specific period of time.

Calls made by supported Avaya phones and endpoints in the Communication Manager environment are watched automatically; no setup is necessary to watch these calls.

During the Call Watch timeframe you specify, the Collector actively polls the selected device for information about call performance while calls are active.

Tips for Setting Up a Call Watch

As you select the DN to watch, keep the following guidelines in mind:

- All calls made by supported Avaya phones are automatically watched. It’s not necessary to create Call Watch definitions in the Avaya (Aura) Communication Manager environment.
- Avaya Call Watch data accumulates rapidly and is therefore purged after seven days. To retain Call Watch data for a longer period of time, set up manual Call Watch definitions.
- The Call Watch feature is not supported in a Microsoft Office Communications Server 2007 environment. In addition, a few older Cisco IP phone models do not support the collection of all Call Watch statistics. Select newer Cisco IP phones to watch.
- Call Watch works in both directions of the call.

  Unless there’s a configuration issue in the Call Watch definition or in your network, Call Watch is bi-directional. Therefore, when you enter a DN to watch, all calls made by and to that phone number will be monitored for quality statistics.
- Do not include hyphens (-) or periods (.) to indicate the area code or exchange in the DN.
- Use an IP phone for the Call Watch.

  It’s almost always best to select an IP phone as the number to be watched. The UC Monitor Administration page allows you to enter the directory numbers of analog phones located in the PSTN, but the complicating factors of number transformations (see the next tip, below), area codes, and prefix digits make it difficult to do this accurately. Plus, IP phones provide extra information about call performance. To troubleshoot a voice gateway, select an IP phone associated with that gateway for the Call Watch.

- Supply enough digits to correctly identify the phone DN on your network.

  Depending on the "transformations" being applied on your network, the phone's extension may not be enough to identify it in CUCM and gateway records. The *User Guide* contains more information about transformations.

  A phone's actual identity at the gateway matters because if you only enter a phone's extension as the Call Watch DN while the gateway is using more digits to identify phones, calls made to and from that phone *won't be watched* because the Collector won't be able to identify them.

- Reload the Collectors each time you set up a new Call Watch or make changes to an existing one.
- Call the watched number.

  One good way to start gathering data from the Call Watch right away is to simply place a call to the selected phone number after you schedule the watch to start and reload the Collectors. Using this method, you can then check the Call Watch Overview Report to make sure the number is being watched and update the Call Watch definition if necessary.

- Watch a gateway.

  If you're interested in watching a particular voice gateway, set up a Call Watch to an IP phone that uses that gateway for incoming PSTN calls. Then use a mobile phone to place a call to the watched phone number, or make a call with the watched phone. When the call is routed from the PSTN through the gateway, you'll see useful call performance statistics.

Setting Up a Call Watch

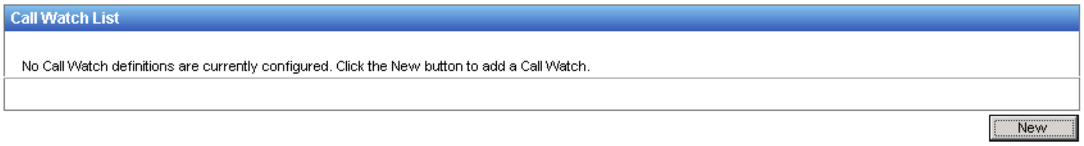
You set up a Call Watch definition by selecting a phone directory number (DN) and the duration of the watch period.

Note: Calls made by phones in the Avaya environment are watched automatically; no setup is necessary.

To add a Call Watch definition:

1. In the **navigation links**, click **Troubleshooting** > **Call Watch**, and then click **Definitions**.

   The Call Watch List page is displayed:

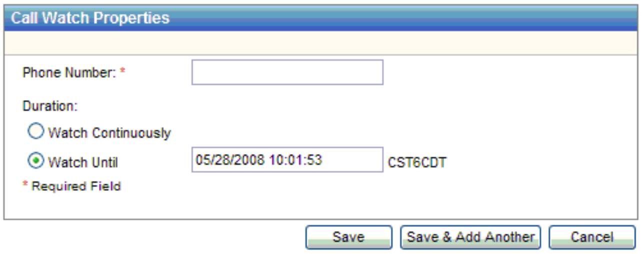
   Call Watch List

   No Call Watch definitions are currently configured. Click the New button to add a Call Watch.

   A message bar indicates that no Call Watch definitions have been set up yet.

2. Click **New** to add a new Call Watch definition.

   The Call Watch Properties page is displayed:



Call Watch Properties

Phone Number: *

Duration:

○ Watch Continuously

● Watch Until 05/28/2008 10:01:53 CST6CDT

* Required Field

3. Supply information for the following properties:

Property	Description
Phone number	The phone number or DN used to call this IP phone. Use the format 8887675443. Do not use hyphens (-) or periods (.) to separate the area code and number. Enter a direct-dial number.
Duration	
Watch Continuously	Continue to perform Call Watch functions until the Call Watch is manually canceled.
Watch Until	Perform Call Watch functions until a specified date and time. Enter the date when the Call Watch should end, using the format `MM/DD/YYYY`. The time is automatically set relative to the time zone of the currently logged-in user. You can edit it as a separate step. The default setting is to Watch Until 24 hours from the time the Call Watch definition is saved.

4. Click **Save** to save this Call Watch definition.

   Or click **Save and Add Another** to save this definition and return to the Call Watch Properties dialog box to set up another Call Watch.

5. Reload the Collectors. In the navigation links, click **Administration** > **Data Collection** > **Collectors**, and then click the **Reload All** button to reload Collectors.

Note: Each time you set up a new Call Watch, or edit or delete an existing Call Watch, you must reload the Collectors. The Reload operation sends configuration information from the Management Console to all Collectors and ensures that the Call Watch is initiated immediately.

Refer to the section on Call Watch Reports in the “UC Monitor Reports” chapter of the *UC Monitor User Guide* for a full discussion of Call Watch overview and detailed reports.

Launching a Traceroute Investigation

To help you collect extra information about the sources of poor call performance, Unified Communications Monitor offers traceroute investigations. Investigations may be launched automatically, in response to an Incident report of a call setup threshold violation. However, traceroute investigations can also be launched:

- According to a schedule to establish a baseline of data, such as the route most frequently taken by calls between certain Locations.
- On demand by users with the appropriate permissions to launch investigations manually.

Scheduled, or “routine” traceroutes run automatically to all key phones and, by default, to all Cisco voice gateways. See “Baseline Traceroutes” on page 116 more information about routine traceroutes.

Note: Routine traceroute testing is not available for Microsoft or Avaya media or voice gateway devices.

Traceroute investigations are available for Cisco devices, and also for Avaya with some limitations. Avaya IP phones do not support traceroute investigations using protocols other than ICMP. However, Avaya voice gateways and Communication Managers support traceroute investigations that use either TCP or ICMP. Be aware that the baseline route shown for an Avaya phone’s call path is calculated differently from the baseline that is available from Cisco baseline traceroute testing.

To instruct Unified Communications Monitor to launch a traceroute automatically, the Administrator enables a traceroute investigation as a call setup Incident response action. See “Creating a New Incident Response” on page 192 for more information.

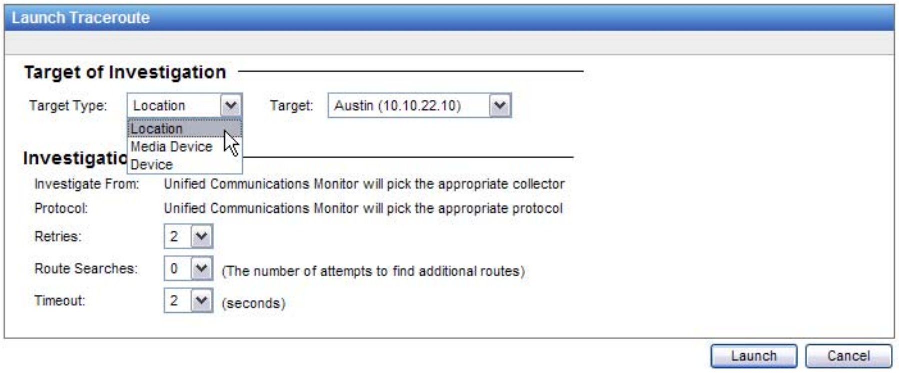
Any UC Monitor operator with the necessary user account permissions can launch an investigation on demand.

Note: If broader access to this feature is desired, you must grant each user account permission (by means of its role) to launch an investigation; this ability is not enabled by default for new user accounts unless they have the Network Manager role. It must be added to any user accounts that have been in use from a previous version of the UC Monitor product. See “Adding or Editing Roles” on page 232 for more information.

To launch a traceroute investigation manually:

1. In the navigation links, click **Troubleshooting > Launch Investigation**.

   The Launch Traceroute page provides options to determine the target for the traceroute and other parameters, such as the timeout and number of retries to attempt:



Launch Traceroute

Target of Investigation

Target Type: Location

Target: Austin (10.10.22.10)

Investigatio

Investigate From: Unified Communications Monitor will pick the appropriate collector

Protocol: Unified Communications Monitor will pick the appropriate protocol

Retries: 2

Route Searches: 0 (The number of attempts to find additional routes)

Timeout: 2 (seconds)

2. Supply the following information in the fields provided:

Property	Description
Target of Investigation	
Target Type	The type of target for the investigation. Select either **Location**, **Media Device**, or **Device**. Your selection determines the options that are available in the **Target** menu. The **Device** option lets you enter an IP address as the target. Select the **Media Device** option for a voice gateway.
Target	The target device for the investigation; the destination of the traceroute. The available targets depend on the Target Type you selected. If you selected **Location** as the Target Type, the target must be a key phone. Typically, a key phone is a Cisco IP phone that is designated at each Location you have defined. If you have not designated any key phones, edit the Locations under investigation to designate a key phone and then return to this page to launch a traceroute. Or select **Device** as the Target Type and enter its IP address.
Investigation Options	
Investigate From	The Collector that will launch the traceroute. The Management Console selects the appropriate Collector based on the Target unless you selected **Device** as the Target Type.
Protocol	The protocol to use for the traceroute. If you selected either **Location** or **Media Device** as the Target Type, the Collector uses TCP over Port 80. If you selected **Device** as the Target Type, select the appropriate protocol and port, based on the call setup protocol used by the call server or gateway device: • ICMP • TCP over port 80 • TCP for SIP (port 5060) • TCP for MGCP (port 2428) • TCP for H.323 (port 1720) ICMP is the only supported protocol for Avaya IP phone targets. For all traceroutes, including baseline traceroutes, the DiffServ ToS bits in the header are set for CS3 handling, the standard for call setup traffic.

Property	Description
Retries	The number of probes, from 0 to 10, to send to each router hop in the route in the event that a target endpoint does not respond. Default is 2 retries.
Route Searches	The number of times, from 0 to 20, to attempt to find additional routes for the selected target. Multiple traceroutes are attempted to see whether any alternate routes are likely to be used between the Collector and the target device. Default is 0 additional times. ***Note:*** All unique routes attempted are included in the Investigation Report.
Timeout	The number of seconds, from 1 to 10, that must elapse for a traceroute to be considered timed out (target unreachable). Default is 2 seconds.

3. Click **Launch** to launch the traceroute immediately.

Whether the traceroute test was launched as an Incident response or on demand, the results of a traceroute investigation are displayed in a report. See the Reports chapter of the *UC Monitor User Guide* for more information about the Traceroute Investigations reports.

CHAPTER 9

Managing the Database

CA NetQoS Unified Communications Monitor uses a MySQL database for data storage. In a Distributed UC Monitor system, the database resides on the same computer as the Management Console.

Periodic maintenance ensures that product functionality and performance are unaffected by database size. Unified Communications Monitor runs two regular checks for database corruption:

- During scheduled database maintenance (once a week).
- Every time the “Inspector” database management service on the Management Console starts.

If the results from the check indicate database corruption, Unified Communications Monitor runs a repair operation on the affected table.

On new installations (that is, non-upgrade installations), database backup operations are not performed automatically. You need to install the NetQoS Database Tools Suite, available from the CA Support Online Web site. See “The NetQoS Database Tools Suite” on page 217 for more information.

Several options are available for the duration of data storage and the type of data that is retained. This chapter covers the following topics:

- “UC Monitor Database Options” on page 210
- “Viewing Database Status” on page 212
- “Changing Database Settings” on page 213
- “Purging Data from the Database” on page 216
- “Backing Up and Restoring the UC Monitor Database” on page 217
- “Hard Drive Maintenance” on page 221

UC Monitor Database Options

To configure or change any options available for the UC Monitor database, you can access several database options from the navigation links.

Database options are associated with the UC Monitor Management Console. Click **Administration** > **Console** > **Database** to see the following categories of database options:

- Status
- Maintenance
- Purge Data

The Administration page for each set of database options is described in the topics below.

Types of Data that Are Stored

The UC Monitor database stores several different types of data, each with its own tables and row counts. The following table describes the different types of data that are stored:

Type of Data	Description
Interval data	Data collected during regular monitoring at five- or 15-minute intervals by the Collector. Incident data is included in this category. Includes the following database tables: • classify_interval_* (14 tables) • callperformance_episodes • collector_episodes; collector_metrics • device_status_history • inv_devices • inv_report_definitions; inv_report_results; inv_report_targets • inv_trace_args; inv_trace_result_args; inv_trace_result_details; inv_trace_results; inv_trace_unique_routes • server_episodes; server_group_history • performance_incident • poor_quality_history • registration_failure_history
Summary data	Data generated on a periodic basis by the Management Console. Used for certain long-range reports, such as the Capacity Planning Reports. Includes the following database tables: • rollup_hourly_call_setup • rollup_hourly_call_volume • rollup_hourly_mos • rollup_hourly_network_mos (Microsoft only) • rollup_hourly_phone_volume • hourly_trunk_group_metrics (Avaya only)

Type of Data	Description
Call data	Data about individual calls. Includes the following database tables: • calls • call_legs • call_legs_video • endpoints • monitored_call_legs; monitored_locations; monitored_servers • phones • sessions
Call Watch data	Data taken from watched phones. Includes the following database tables: • call_watch_legs • call_watch_metrics • path_trace_results • path_trace_result_details • path_trace_unique_routes

Database Retention Options

Unified Communications Monitor stores the following types of data for the following amounts of time:

Type of Data	Default Storage Period	Available Storage Period
Interval data	3 months	1 to 24 months
Summary data	6 months	1 to 24 months
Call data	3 months	1 to 24 months
Call Watch data	3 months	1 to 24 months

You can change the default storage period for any of these data types by clicking **Administration** > **Console** > **Database > Maintenance** in the navigation links. See "Changing Database Settings" on page 213 for more information.

By default, system maintenance runs every Sunday morning at 12:00 am on the Management Console computer. System maintenance involves a purging of data from the database as soon as it is out of compliance with database retention settings. You can change the day and time that it runs.

Some restrictions apply to database storage options:

- Call data must be stored for at least as long as, or longer than, Call Watch data due to dependencies.
- Call Watch data, by the same token, must be stored for a shorter length of time, or for the same length of time, as call data.

Viewing Database Status

Access the Database Status page to see:

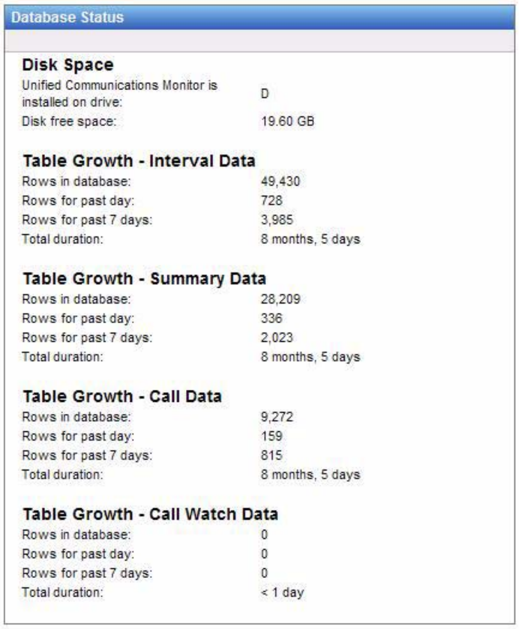
- The amount of disk space used by Unified Communications Monitor
- How that space is used
- How fast the database is growing

A full, or nearly full, hard drive affects the reporting performance of the existing data and the collection of new data.

To view database status:

1. In the **navigation links, click Administration > Console** > **Database**, and then click **Status**.

   The Database Status page is displayed:



Database Status

Disk Space

Unified Communications Monitor is installed on drive:	D
Disk free space:	19.60 GB

Table Growth - Interval Data

Rows in database:	49,430
Rows for past day:	728
Rows for past 7 days:	3,985
Total duration:	8 months, 5 days

Table Growth - Summary Data

Rows in database:	28,209
Rows for past day:	336
Rows for past 7 days:	2,023
Total duration:	8 months, 5 days

Table Growth - Call Data

Rows in database:	9,272
Rows for past day:	159
Rows for past 7 days:	815
Total duration:	8 months, 5 days

Table Growth - Call Watch Data

Rows in database:	0
Rows for past day:	0
Rows for past 7 days:	0
Total duration:	< 1 day

The Database Status page provides information about the current total number of rows containing data. Row totals are broken out by data category. The rate of growth, as measured by the number of new rows over the past 24 hours and over the past week, is also shown.

The following table explains what is shown on the Database Status page:

Section or Metric	Description
Disk Space	Indicates the hard drive where UC Monitor is installed and how much disk space is free on that computer. We recommend having at least 6 GB of free hard disk space on the D: drive where the UC Monitor Management Console is installed. By default, a warning is sent when free hard disk space falls below 5 GB.

Section or Metric	Description
Table Growth - Interval Data	The rate at which the database (MySQL) is growing.
Table Growth - Summary Data Table Growth - Call Data Table Growth - Call Watch Data	The rate of database growth is shown per data type. The categories of data in the database are described in "Types of Data that Are Stored" on page 210.
Rows in database	The total row count. For Call Watch data, includes all watched calls that the Collector has seen, whether they are still in progress or not.
Rows for past day	The row count for data collected over the past 24 hours. For Call Watch data, calls still in progress are not included; an end time is required. To have a known end time: • the call must have been completed • the Collector must have detected the call completion and reported it to the Management Console • the Management Console must have processed the results ***Note:*** Because of delays that occur during Collector reporting, the row counts for past day and past 7 days may show an undercount.
Rows for past 7 days	The row count for data collected in the past 7 days. For Call Watch data, calls still in progress are not included; an end time is required. Same rules apply as to **Rows for past day**, above.
Total duration	The "duration" of a data type is determined by calculating the difference between the oldest and newest row in the relevant database table.

The topic "Recommended Database Limits" provides information to help you gauge the impact of the growth rates shown in the Database Status table.

Changing Database Settings

The UC Monitor Management Console offers options for changing database retention periods for certain types of data and setting up notifications to let you know when a database metric has reached a certain limit so you can take steps to keep it performing at peak levels.

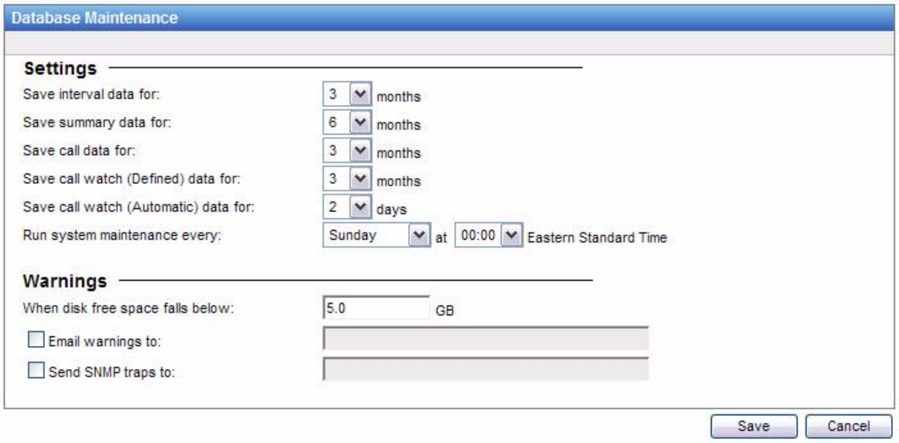
A UC Monitor Administrator can change some of the default database maintenance and notification settings. On the Database Maintenance page, you can perform the following database maintenance tasks:

- Change the database retention settings.
- Select a time when system maintenance is performed.
- Configure SNMP traps or email warnings to be sent when available disk space falls below a threshold.

To perform database maintenance:

1. In the **navigation links, click Administration > Console** > **Database**, and then click **Maintenance**.

   The Database Maintenance page is displayed:



Database Maintenance

Settings

Save interval data for: 3 months

Save summary data for: 6 months

Save call data for: 3 months

Save call watch (Defined) data for: 3 months

Save call watch (Automatic) data for: 2 days

Run system maintenance every: Sunday at 00:00 Eastern Standard Time

Warnings

When disk free space falls below: 5.0 GB

□ Email warnings to:

□ Send SNMP traps to:

2. Enter or select the following information:

Database Maintenance Setting	Description
Settings	
Save interval data for	The length of time that five- or 15-minute data should be stored. Select from 1 to 24 months. The default is 3 months.
Save summary data for	The length of time that summary data—generated by the Management Console periodically, for long-range reporting—should be stored. Select from 1 to 24 months. The default is 6 months.
Save call data for	The length of time that call data should be stored. Select from 1 to 24 months. The default is 3 months. Call data must be stored for at least as long as, or longer than, Call Watch data due to dependencies.
Save Call Watch (Defined) data for	The length of time that rolled up Call Watch data from the Call Watch definitions you create should be stored. Call Watch definitions only apply to Cisco IP phones. For automatic Call Watch data, see the following table entry. Select from 1 to 24 months. The default is 3 months. Call Watch data must be stored for a smaller length of time, or for the same length of time, as call data due to dependencies.
Save Call Watch (Automatic) data for	The length of time that rolled up Call Watch data from automatically watched calls (that is, all calls made by Avaya phones and endpoints) should be stored. Select from 1 to 28 days. The default is 7 days. Call Watch data must be stored for a smaller length of time, or for the same length of time, as call data due to dependencies.

Database Maintenance Setting	Description
Run system maintenance every	Lets you select a day of the week and a time to run system maintenance. The default setting is Sunday at 12:00 am.
Warnings	
When disk free space falls below	Enter a threshold, in Gigabytes, to determine when UC Monitor should send a low disk space notification to the specified recipient. Default threshold is 5 GB.
Email warnings to	Select this check box to automatically send an email message when the available disk space falls below the specified threshold. Enter an email address to which to send the warning.
Send SNMP traps to	Select this check box to automatically send an SNMP trap when the available disk space falls below the specified threshold. Enter the name of the server or the IP address to which to send the SNMP trap.

3. Click **OK**.

The following topic, "Recommended Database Limits," provides some guidelines to help you select data-retention settings.

Recommended Database Limits

The amount of data in the UC Monitor MySQL database depends on the volume of call activity on the network. We recommend the following time limits on data storage to avoid performance degradation:

Call Volume	10 M calls/ month	3.3 M calls/ month	1.6 M calls/ month	800 K calls/ month
Data Type				
Interval Data	1 month	3 months	6 months	12 months
Summary Data	1 month	3 months	6 months	12 months
Call Data	1 month	3 months	6 months	12 months
Call Watch Data (Defined)	1 month	3 months	6 months	12 months
Call Watch Data (Automatic)	2 days	7 days	14 days	28 days

You can change the default settings for the amount of time data is stored in the database by clicking **Administration > Console** > **Database** > **Maintenance**. See the previous topic, "Changing Database Settings," for more information.

Purging Data from the Database

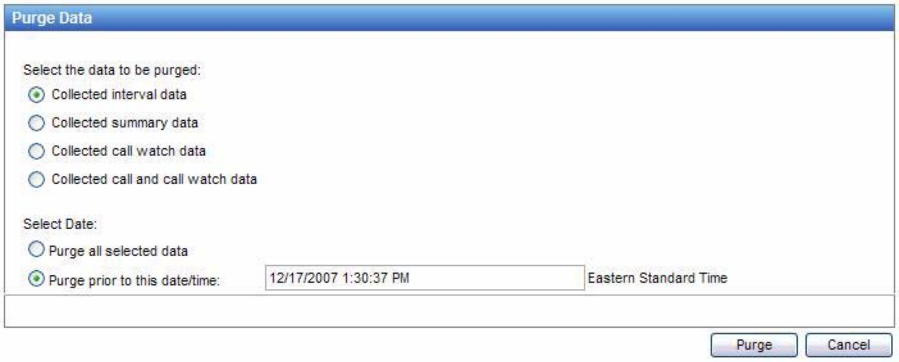
A UC Monitor Administrator can choose to purge selected data, or all data, from the UC Monitor database.

Purging data permanently removes it from the database. You *cannot* recover purged data.

To purge data from the UC Monitor database:

1. In the **navigation links**, click **Administration > Console** > **Database**, and then click **Purge Data**.

   The Purge Data page is displayed:



Select the data to be purged:

● Collected interval data
○ Collected summary data
○ Collected call watch data
○ Collected call and call watch data

Select Date:

○ Purge all selected data
● Purge prior to this date/time: 12/17/2007 1:30:37 PM Eastern Standard Time

2. Select from the following choices:

Purge Data Property	Description
Select the data to be purged	
Collected interval data	Purges all five- or 15-minute data from regular monitoring, including all Incident data, collected by all collection devices.
Collected summary data	Purges all summary data generated by the Management Console for long-range reporting.
Collected call watch data	Purges all data collected by the Collector(s) from watched phones.
Collected call and call watch data	Purges all data collected by all collection devices from detailed call records and from watched phones. ***Note:*** When you enable this purge setting, if you then select the option to **Purge prior to this date/time** (see below), the last 30 days of phone data is retained, while all other call and Call Watch data is purged. To purge all phone data, select the option to **Purge all selected data**.
Select Date	
Purge all selected data	Purges selected data across all dates.
Purge prior to this date/time	Lets you select a specific timeframe for the data that should be purged. Enter a date and time before which all data should be purged. Use the following format: `MM/DD/YYYY HH:MM:SS`

3. Click **OK**.

4. On the Purge Data Confirmation page, click **Continue** to delete the selected data from the database.

   Or if you change your mind, click **Cancel** to cancel the purge operation.

Backing Up and Restoring the UC Monitor Database

Because various situations can lead to an unrecoverable database, we recommend that you perform regular database backups.

Unified Communications Monitor stores all data in the following directories:

```
D:\NETQOS\MySQL51\data\voip
D:\NETQOS\MySQL51\data\netqosvoipconsole
```

When you install UC Monitor 3.1 or later for the first time, it does not automatically perform a database backup operation as part of its weekly database maintenance. If you have upgraded the product from an earlier version, weekly backups will continue to run automatically, as scheduled. However, we recommend using the CA NetQoS Database Tools Suite to schedule and perform weekly database backups using the Windows Scheduled Tasks feature. The tools suite includes scripts to help you integrate the UC Monitor database into an existing backup routine that you are currently using.

The topic titled "CA-Supported Database Backup Method" on page 218 provides more information about the officially supported database tools that you should use to back up your data. However, you can also manually back up the metric and configuration databases. See "Manual Backups" on page 219.

The NetQoS Database Tools Suite

The CA NetQoS Database Tools Suite contains a bundle of small, efficient tools that interact with the MySQL databases on most CA NetQoS products, including CA NetQoS Unified Communications Monitor. These tools have been developed to ease the administrative overhead associated with database backups, optimization, repairs, and restoration of an existing backup. In addition, a user administration tool is included to create MySQL user accounts with `SELECT` only rights for accessing and exporting data.

The CA NetQoS Database Tools Suite is not provided with Unified Communications Monitor. The latest version of the tools suite is located on the CA NetQoS Support Tools page. You must download it from the CA Support Online Website at this location:

support.ca.com

After you log into the Support site, use the **search** field at the top of the Web page to search for the following string:

```
netqos database tools
```

You can save the executable or run it from the Web page. A valid `D:\` drive must be defined to enable the installation. Post-installation, the executable can be launched from the Program Files > NetQoS Database Tools Suite > **NetQoS Database Tools Suite** folder.

Important: You must also download and install an ODBC MySQL driver to enable this set of database tools to run on the UC Monitor server. Download the driver from
http://dev.mysql.com/downloads/connector/odbc/5.1.html
And contact CA Support if you have difficulty locating the download package.

The NetQoS Database Tools Suite folder provides a link where you can check for updates to the database tools. The installation also saves a *Database Tools User Guide* in PDF format, with filename `nqdbtoolssuiteGuide.pdf`, in the same folder.

CA-Supported Database Backup Method

The officially supported CA database backup script, which is provided with the CA NetQoS Database Tools Suite, is named NetQoS Backup & Restore MT. It is available free of charge to CA customers and is provided "as is." Data collection services continue running during the backup or restore processes, but CA cannot guarantee data continuity, and beginning and ending timestamps might be affected.

NetQoS Backup & Restore MT creates a backup archive for any CA | NetQoS product that uses a MySQL 4.1 or 5.1 database. Each database table is stored in a separate archive.

Note: CA NetQoS Unified Communications Monitor version 3.1 uses MySQL 5.1.

The backup script, `DBBackupMT.exe`, runs at a command prompt and requires two parameters:

- the database name. See "Types of Data that Are Stored" on page 210 for a list of UC Monitor database names.
- the filepath where the backup archive should be saved.

`DBBackupMT.exe` creates a folder in the filepath that you specify and gives it the name of the database that was backed up. Each time it runs, the database tool performs a multi-threaded operation of `mysqldump` on multiple database tables. Error checking and logging are performed.

Optional parameters can also be supplied to specify that a Windows Shadow Copy of the database be created before running the backup operation, to compress the database archives, and to specify a number of threads to run simultaneously to speed up the operation.

The same executable (`DBBackupMT.exe`) is used to restore the database from a backup when you include the `restore` command in the argument. When you enter the command, you are prompted to specify whether to restore the entire database or a single table, and then you are prompted to specify the database or table.

If you suspect that an error has caused the backup or restore operation to hang, the **Ctrl + C** (break) command is the safest way to terminate the program. It ensures that all open processes exit cleanly.

For more information about the standard usage, optional parameters, and examples, read the *Database Tools User Guide*, provided in PDF format in the Database Tools Suite folder as part of the installation process. The guide also contains information about error messages.

Manual Backups

The CA NetQoS Database Tools Suite provides the preferred method for backing up the UC Monitor database. However, you can also run a backup operation manually. Use the data directory backup method to back up and restore the UC Monitor database.

To back up the database manually:

1. On the **Start** menu, click **Settings > Control Panel**.
2. In the Control Panel, double-click **Administrative Tools**.
3. In Administrative Tools, double-click **Services**.
4. In Services, stop the following UC Monitor services:
   - the NetQoS UC Console Communicator
   - the NetQoS UC Monitor Inspector
5. Stop the MySQL Service. *Do not* stop the NetQoS UC Collector Service.

   To stop a service, right-click it, and click **Stop**.
6. Copy the `D:\NetQoS\MySQL51` data directories to a backup location.
7. Restart all services. To start a service, in Services, right-click the service, and click **Start**.

If you have created a backup file using the data directory method outlined above, you can then restore the database by means of a manual copy operation if you first stop the affected services. Upgrade installations of Unified Communications Monitor can use the following procedure after the voiprestore routine runs. It is no longer applicable in versions of Unified Communications Monitor later than 3.0.

To restore the database from a manual backup:

1. On the **Start** menu, click **Settings > Control Panel**.
2. In the Control Panel, double-click **Administrative Tools**.
3. In Administrative Tools, double-click **Services**.
4. In Services, stop all services listed for backup.
5. Replace the `D:\NetQoS\MySQL51` data directories with the most recent database backup versions.
6. In Services, restart all services.

Backup Operations in Back-Level Versions of UC Monitor

If your version of the UC Monitor software was new as of version 3.1, you need to follow the advice provided in "The NetQoS Database Tools Suite" on page 217, and install the CA NetQoS Database Tools Suite to enable you to perform database backups.

Previous versions of Unified Communications Monitor backed up the database automatically every week, on Sunday at 12:00 am. These backup files were stored in the `D:\NetQoS\VoIPMonitor\archive` directory. If you have upgraded the software from a previous version (that is, pre-3.1), these backup files are still being created. Each time a new backup file is created, the previous one is copied to a file named `fullbackup-old.zip`.

Only one extra backup file is preserved from the automatic backup during weekly database maintenance. If you want to save a database backup more permanently, rename the zip file to something other than "`fullbackup.zip`" or "`fullbackup-old.zip`". Once renamed, database backup files in the `\archive` directory are never pruned.

Restoring the Database from an Automatic Backup (Pre-Version 3.1 Only)

The following steps provide instructions for restoring the UC Monitor database from its most recent, automatic backup operation in cases where you have upgraded the software from a previous version. You can also restore the database from a manual backup that was created using the directory method described in "Manual Backups" on page 219.

To restore the database from an automatic backup:

1. On the **Start** menu, click **Run**.
2. Open a command prompt by entering the following command:

   ```
   cmd
   ```
3. Change directories to `D:\NetQoS\VoIPMonitor\archive`
4. Enter the following:

   ```
   voiprestore fullbackup.zip
   ```

   This routine stops the necessary services (including IIS), restores the `voip` and `netqosvoipconsole` databases, and then restarts the services that were stopped.

Database Repair Operations

The CA NetQoS Database Tools Suite (discussed in "The NetQoS Database Tools Suite" on page 217) includes a tool to perform database repair operations. The NetQoS DB Repair tool was designed to make database repairs easier. This tool is not needed for Unified Communications Monitor, which runs automatic database checks and, when necessary, repair operations each week during regular maintenance.

If you have installed the Database Tools Suite, you can launch a repair operation on demand, outside of the regular, automatic check and repair procedures. Double-click the `DBrepair.exe` file, installed in the `D:\DBTools3` folder.

Hard Drive Maintenance

Unified Communications Monitor contains several tables that it consistently accesses for read/write operations. These tables occupy the majority of the disk space on the drive where the UC Monitor Management Console is installed. As a result of these I/O operations, disk fragmentation is likely to occur over time.

We recommend that you perform the following tasks to maintain the hard disk drive (HDD):

- **Regular defragmentation**. For databases larger than 10 GB in total size, defragment the D: drive (or the drive where the UC Monitor Management Console is installed) on a monthly basis. Make sure that at least 20% of this drive contains free disk space before starting the defragmentation process. Also, stop all NetQoS services, including the MySQL service, prior to defragmentation; restart these processes after the defragmentation is complete.

  Note: The topic titled "Manual Backups" on page 219 contains an image of the Services Panel showing all the UC Monitor services.

- **Regular backups**. NetQoS products are constantly writing to the HDD, and during data seek operations in support of report compilation, the drive heads move about simultaneously writing and reading. As with any HDD, this stress over time could lead to failure. To recover quickly with minimal data loss, we recommend that you schedule a regular database backup. For information about backing up the UC Monitor database, see "Backing Up and Restoring the UC Monitor Database" on page 217.

CHAPTER 10 Setting Up Security

The security features in CA NetQoS Unified Communications Monitor are similar to those of other CA NetQoS products and were designed for compatibility with the CA NetQoS Performance Center. Permissions to access report pages and perform certain tasks are tied to the roles associated with user accounts. The Administrator creates a user account for each UC Monitor operator and determines his or her level of product privilege, or access. This design provides a flexible and secure way to determine the product features and reports that each different operator can use or view.

The product privilege and role associated with each user account can be shared among CA NetQoS products. After you register Unified Communications Monitor with the CA NetQoS Performance Center, you must manage users, roles, and permissions across all CA NetQoS products from the NetQoS Performance Center. The Administrator product privilege is required to add, edit, or delete a user.

SNMP profiles can also be shared among CA NetQoS products. These profiles allow you to define parameters to use when contacting devices, such as voice gateways and Avaya Communication Managers, using SNMP to request information about call quality and volume. If your devices are using SNMPv3, SNMP profiles include options to require authentication and encryption for these queries.

Unified Communications Monitor and the other CA NetQoS data sources leverage the Single Sign-On product when users log in to the NetQoS Performance Center. CA Single Sign-On provides user authentication for CA NetQoS products and eliminates the need to re-authenticate when navigating among them. An instance of the Single Sign-On software is automatically installed on each computer where a data source product is installed. See “CA NetQoS Single Sign-On” on page 225 for more information.

The grouping feature in the CA NetQoS Performance Center provides an extra layer of granularity to the built-in UC Monitor security options. By placing Locations into custom groups, you can restrict the call data that a given operator can access with his or her permissions. See Appendix A, “Working with Groups in the CA NetQoS Performance Center” on page 241 for a full discussion of the grouping feature.

This chapter covers the following topics:

- “Introduction to UC Monitor Security” on page 224
- “Working with Users and Roles” on page 226
- “Working with SNMP Profiles” on page 234

Introduction to UC Monitor Security

The UC Monitor approach to security could be termed “role-based user management.” Like other CA NetQoS products, CA NetQoS Unified Communications Monitor provides role-based security by allowing an Administrator to manage the level of access to product functionality that is granted to individual operators.

UC Monitor security is based on the *role* and on the *product privilege* granted to each user account by the UC Monitor Administrator. Roles are associated with permissions to access certain product features and to view reports; the product privilege determines whether the user has Administrator access to UC Monitor configuration views:

- **Roles** — Limit the general product functional areas that may be accessed by an associated user.

  The UC Monitor system offers two default roles. An Administrator can create additional roles. Roles determine the pages that a selected user can access. For example, when creating a new role, an Administrator chooses the reports to which that role has access. The default roles are described in “Adding or Editing Roles” on page 232.
- **Product Privilege** — Defines the category of user and the level of access to the UC Monitor system. The product offers two sets of pre-configured privileges:
  - Administrator: Performs all functions, including all administrative tasks (creating and editing Locations, media devices, thresholds, Call Watch definitions, Incident responses, roles, and user accounts).
  - User: Views the pages and performs some basic functions selected by an Administrator; has no access to administrative functions.

  Product privilege is discussed in more detail in “More about Product Privileges” on page 254.
- **Users** — Associate a username and password with a role and product privileges. Each user account provides a UC Monitor operator with the access associated with their assigned role and privilege level.

With the most recent versions of the CA NetQoS Performance Center, users, roles, privileges, and groups are coordinated among CA NetQoS monitoring products and are managed in the NetQoS Performance Center. The following topic explains this coordinated security.

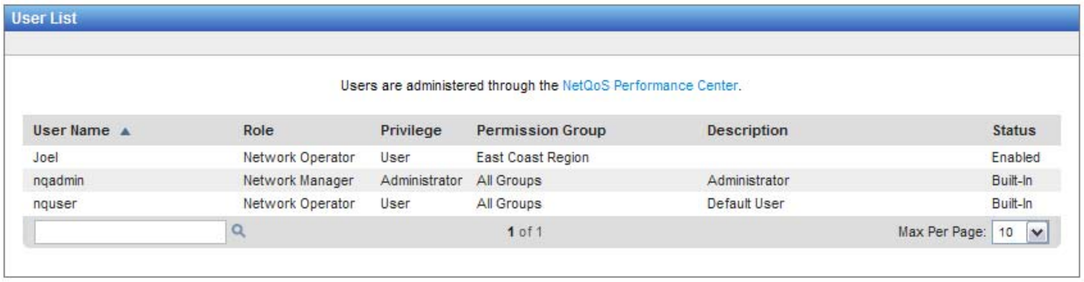
Registration with the CA NetQoS Performance Center

Once you have registered Unified Communications Monitor as a NetQoS Performance Center data source, you are redirected to the Administration pages in the CA NetQoS Performance Center for all administrative tasks associated with privileges, roles, and users. More information about this integration with the NetQoS Performance Center is provided in an appendix to the *CA NetQoS Unified Communications Monitor User Guide*.

Note: Registration is required to enable the grouping feature, which is described in Appendix A, “Working with Groups in the CA NetQoS Performance Center” on page 241.

Registration is accomplished when you add the UC Monitor data source to the NetQoS Performance Center. The View Data Sources page in the Administration section of the NetQoS Performance Center displays the current status of all configured data sources. During registration, the status is "`Registering`". When registration has successfully completed, the data source status is shown as "`Available`".

The User List and Role List pages in Unified Communications Monitor display all available users and roles, but these pages no longer provide Add, Edit, or Delete capabilities once registration to the NetQoS Performance Center has completed. A message indicates that these administrative tasks are now performed in the NetQoS Performance Center, and a link is provided to the appropriate administration page in the NetQoS Performance Center interface.



Users are administered through the NetQoS Performance Center.

User Name ▲	Role	Privilege	Permission Group	Description	Status
Joel	Network Operator	User	East Coast Region		Enabled
nqadmin	Network Manager	Administrator	All Groups	Administrator	Built-In
nquser	Network Operator	User	All Groups	Default User	Built-In

As long as the current user account has the appropriate product privilege for both Unified Communications Monitor and the CA NetQoS Performance Center, additional authentication is no longer needed to move between these product interfaces and perform the desired functions. Product privilege can vary per data source; see "More about Product Privileges" on page 254.

See the following topic for information about how user authentication is handled between CA NetQoS products.

CA NetQoS Single Sign-On

"Single Sign-On" is the term used to describe the authentication scheme used by all CA NetQoS products. Aside from providing a login page, the Single Sign-On feature provides LDAP support for every CA NetQoS product and the ability for a user to change between product interfaces without having to re-authenticate—that is, without having to sign in a second time.

If you are already familiar with the CA NetQoS Performance Center, you know that it provides a drilldown path from report pages to the data sources that reported the data shown on those pages. In the case of Unified Communications Monitor, links on the Unified Communications Dashboard page take you back to the UC Monitor user interface with the same report context selected. In past versions of the NetQoS Performance Center, however, returning to the UC Monitor product required re-authentication. This second sign-in is no longer required if you have an instance of the Single Sign-On software installed on the UC Monitor appliance.

The Single Sign-On feature uses a distributed architecture, which enables users to sign into individual CA NetQoS products as long as they can log into the servers where these products are running. An instance of Single Sign-On is installed automatically with Unified Communications Monitor. Once it has been installed, its use is transparent; logging in proceeds as before, and the Login page appears similar to the UC Monitor Login page. A link to the NetQoS Performance Center (labeled **NPC**) appears in the upper right corner of the UC Monitor Management Console.

For information on how to set up and configure Single Sign-On, refer to the *CA NetQoS Single Sign-On Guide*, which is installed with the CA NetQoS Performance Center software.

Working with Users and Roles

The UC Monitor Administrator must set up accounts for the operators who will access various UC Monitor reports and functions, add those user accounts to the system, and assign them roles and product privileges.

To get your VoIP and video monitoring system up and running, you'll need to create users and assign them specific, pre-defined *privilege* levels and either pre-defined or custom *roles*. The main access levels that you might want to change from their default settings involve role-based permissions to view reports and initiate a Call Watch or traceroute investigation.

You also need to be sure that no user accounts are shared. When more than one user is logged into the UC Monitor system with the same user account, the results are unpredictable. Page and view settings could interfere with each other if accessed simultaneously on different computers.

The following table provides a brief explanation of the parameters used in UC Monitor security and the available defaults:

Category	Description
Privilege	The user's level of access to product features. Determines whether a user can perform UC Monitor administrative functions, such as product configuration. The name of the product privilege level is either: • Administrator, or • User
User	The credentials of a person who is authorized to operate Unified Communications Monitor and to perform certain tasks. Identified by a username and an associated email address, role, and product privilege level. Each user you add to the system is associated with one role and one product privilege level. ***Note:*** Only a single user should be logged in with the same credentials at any point.
Role	Defines which UC Monitor report pages are accessible. The following report types are used to grant access: • Monitoring • Troubleshooting • Capacity Planning Two default roles are provided: • Network Manager • Network Operator You will probably want to create custom roles to suit your enterprise.

Note: Once you have registered Unified Communications Monitor with the CA NetQoS Performance Center, you are redirected to the Administration pages in the NetQoS Performance Center for all administrative tasks associated with users, product privileges, and roles. See "Grouping and Security" on page 251 for more information.

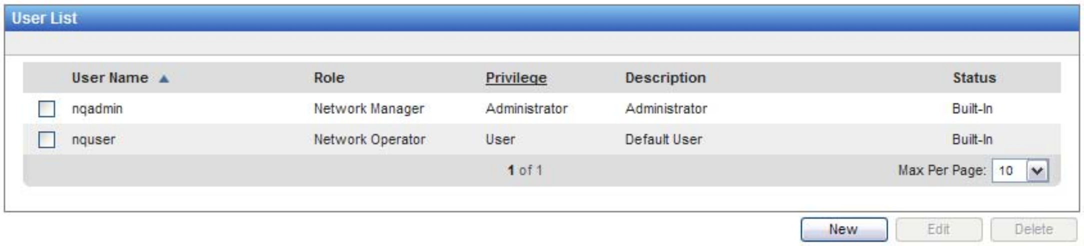
Viewing Users

Unified Communications Monitor provides two pre-defined users with different roles and product privileges. Before you register Unified Communications Monitor with the CA NetQoS Performance Center, the User List page allows you to view these UC Monitor user accounts, edit or delete these users, or add new, custom users. All users defined in the system, including those created in other CA NetQoS products that are registered with the NetQoS Performance Center, are displayed on the UC Monitor User List page after registration.

To view the list of pre-defined users:

1. In the navigation links, click **Administration > Security**, and then click **Users**.

   The list of users is displayed in the User List page:



User List

	User Name ▲	Role	Privilege	Description	Status
□	nqadmin	Network Manager	Administrator	Administrator	Built-In
□	nquser	Network Operator	User	Default User	Built-In

1 of 1

Max Per Page: 10

From the User List page, you can add, edit, or delete users. The following table explains the information provided in the User List:

Column Name	Description
User Name	A meaningful name to identify this user account. May be the name of a network account with appropriate permissions, or a new username. Two users are predefined: • the UC Monitor Administrator, `nqadmin` • the default product user, `nquser` ***Note:*** If you decide to assign users to these default user accounts, be sure to change the default passwords. Only a single user should be logged in with the same credentials at any point.
Role	The role assigned to this user.

Column Name	Description
Privilege	The level of product access. The name of the privilege set indicates the level of access. Select either Administrator or User. Accounts with the User product privilege set cannot perform any administrative functions, such as Management Console configuration. You select the product privilege for each user when you add new users. See "Adding or Editing a User" on page 228 for more information. User product privileges for Unified Communications Monitor are compatible with those of other CA NetQoS products. See "More about Product Privileges" on page 254 for more information.
Description	A description of this user account.
Status	The status of this user, either Enabled or Disabled. Or, for the pre-defined user accounts, shows "Built-In". You can disable a user account when you add or edit a user account. See "Adding or Editing a User" on page 228 for more information.

Adding or Editing a User

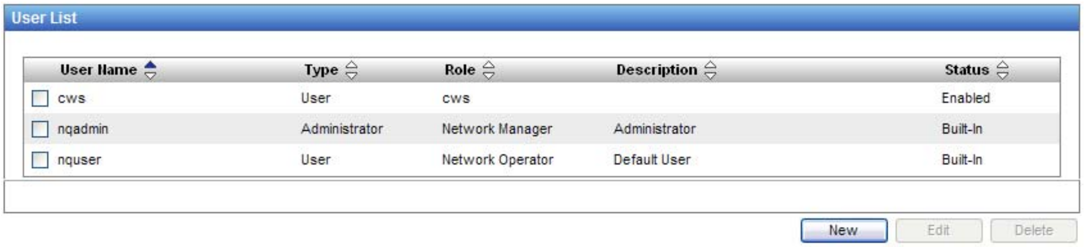
For each authorized user of Unified Communications Monitor, you'll need to create a user account by adding a new user on the User List page. Before you register Unified Communications Monitor with the CA NetQoS Performance Center, the User List page allows you to view all the UC Monitor user accounts, edit or delete these accounts, or add new, custom users.

Once you have registered Unified Communications Monitor with the NetQoS Performance Center, you are redirected to the NetQoS Performance Center for all administrative tasks associated with users, privileges, and roles. All users defined in the system, including those created in other CA NetQoS products that are registered with the NetQoS Performance Center, are displayed on the UC Monitor User List page after registration.

To add a new user:

1. In the navigation links, click **Administration > Security**, and then click **Users**.

   The User List page is displayed:

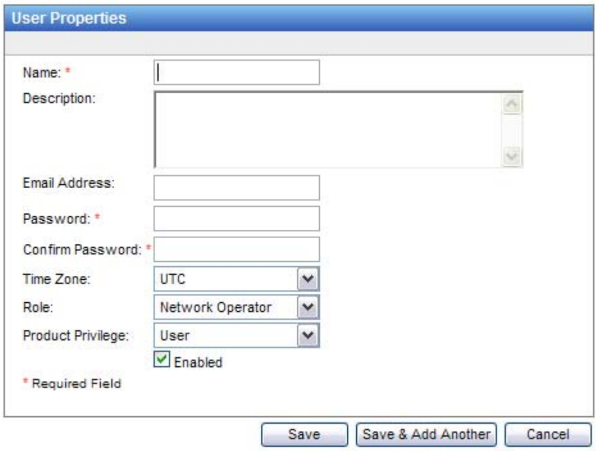


User List

User Name	Type	Role	Description	Status
□ cws	User	cws		Enabled
□ nqadmin	Administrator	Network Manager	Administrator	Built-In
□ nquser	User	Network Operator	Default User	Built-In

2. Perform one of the following tasks:
   - To add a new user, click **New**.
   - To edit a user, click to select the check box next to the username in the **User Name** column. Then click **Edit**.

The User Properties page is displayed:



User Properties

Name: *	
Description:	
Email Address:	
Password: *	
Confirm Password: *	
Time Zone:	UTC
Role:	Network Operator
Product Privilege:	User
	☑ Enabled

* Required Field

3. Enter or change the following information for a user:

User Property	Description
Name	A username for this user account.
Description	Optional field. A description of this user account. For example, you could enter the user's full name and the location of his or her office to identify the person using this account.
Email Address	The email address of the user. Used as the "**Reply to**" address in any scheduled email that is set up by this user.
Password	A password for this user account. A password is not required, but is recommended for security purposes. Blank passwords are accepted.
Confirm Password	The password for this user account, entered again to confirm it.
Time Zone	Select the time zone where the UC Monitor operator will be working and viewing reports. If UC Monitor users are in different time zones, you can assign each of them a local time zone so that UC Monitor reports are displayed in their time zone. The default time zone is UTC (coordinated universal time), which is the same as Greenwich Mean Time (GMT). See the online Help for a description of other time zones.
Role	The role for this user. Select either **Network Manager**, **Network Operator**, or a custom role you have created. To create a new, custom role, see "Adding or Editing Roles" on page 232.

User Property	Description
Product Privilege	The user's level of access to product functionality and configuration. Select either Administrator or User: • **Administrator**: By default, has access to all product configuration views, functionality, and reports. • **User**: By default, has view access to all reports. Only a user with the Administrator product privilege can change product configuration. The Administrator controls the reports that this user is able to view by editing the role assigned to him or her. See "Adding or Editing Roles" on page 232 for more information.
Enabled	If selected, indicates that this user account is enabled, or active, and ready to be used to access the UC Monitor features specified by the role and privilege level.

4. Click **OK**.

The user is added to the list in the Users table.

Deleting a User

If a user leaves the organization or transfers to a different position, you may want to delete a UC Monitor user you've created. Before you register Unified Communications Monitor with the CA NetQoS Performance Center, the User List page allows you to view, edit, or delete all UC Monitor user accounts, or add new, custom user accounts.

Once you have registered the UC Monitor data source, you are redirected to the NetQoS Performance Center Administration pages for all administrative tasks associated with users, privileges, and roles.

Note: You cannot delete the pre-defined users: **nqadmin** and **nquser**.

To delete a user:

1. In the navigation links, click **Administration > Security**, and then click **Users**.
2. On the User List page, click the **Delete** icon next to a user that you want to delete.
3. On the Confirm Delete page, click **Delete** to complete the deletion.

   Otherwise, click **Cancel**.

The deleted account no longer appears in the User List when the deletion has completed.

UC Monitor Roles

Roles, which define the permissions allocated to each user, are a means of protecting sensitive information. For example, the Calls report reveals which phones made calls, which phone numbers they called, and when they called them. Roles can be used to limit the number of UC Monitor operators who can view such information. They can also be used to restrict the number of operators who are able to launch a Call Watch and an on-demand traceroute investigation.

Unified Communications Monitor provides two pre-defined roles that you can use or modify. You can assign these roles to the people who will be using Unified Communications Monitor during user account creation. See “Adding or Editing a User” on page 228 for more information.

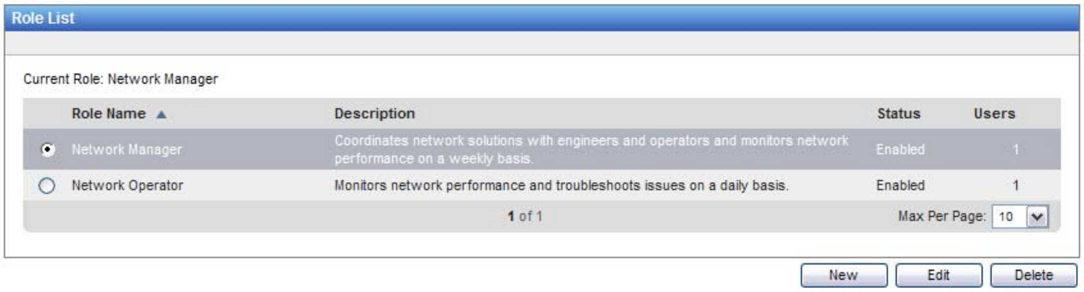
Before you register Unified Communications Monitor with the CA NetQoS Performance Center, the Role List page allows you to view the currently configured UC Monitor roles. You can see how many users have these roles assigned to their account, edit or delete these roles, or add new, custom roles.

Once you have registered the UC Monitor data source, a link to the appropriate Administration page in the NetQoS Performance Center is provided on the UC Monitor Role List page. In addition, all roles defined in the system, including custom roles created in other CA NetQoS products that are registered with the NetQoS Performance Center, are displayed in the Role List.

To view the pre-defined UC Monitor roles:

1. In the navigation links, click **Administration > Security**, and then click **Roles**.

   The Role List page is displayed, with the two pre-defined roles listed:



Role List

Current Role: Network Manager

	Role Name ▲	Description	Status	Users
●	Network Manager	Coordinates network solutions with engineers and operators and monitors network performance on a weekly basis.	Enabled	1
○	Network Operator	Monitors network performance and troubleshoots issues on a daily basis.	Enabled	1

1 of 1 Max Per Page: 10

   The following table describes the pre-defined roles:

Role Name	Description
Network Manager	Role assigned to the user with permission to install and configure the UC Monitor system. Has permission to view all reports and set up and launch a Call Watch and a traceroute investigation. Usually assigned to a single user, such as a VoIP System Administrator, with perhaps a backup user assigned for emergency situations to avoid configuration errors and duplication of effort.
Network Operator	Role assigned to a user with permission to view Performance Reports, Incidents, and Call Watch Reports. Cannot set up or launch a Call Watch or change other UC Monitor configuration.

You may want to add new, custom roles for users in your UC Monitor system. You also have the option to edit the pre-defined roles. The following topic explains how to add or edit a role.

Adding or Editing Roles

Roles control which UC Monitor features, such as the data associated with particular groups or selected reports, users are able to view. You may want to create new roles or edit the pre-defined roles to customize the product areas that each UC Monitor operator can view.

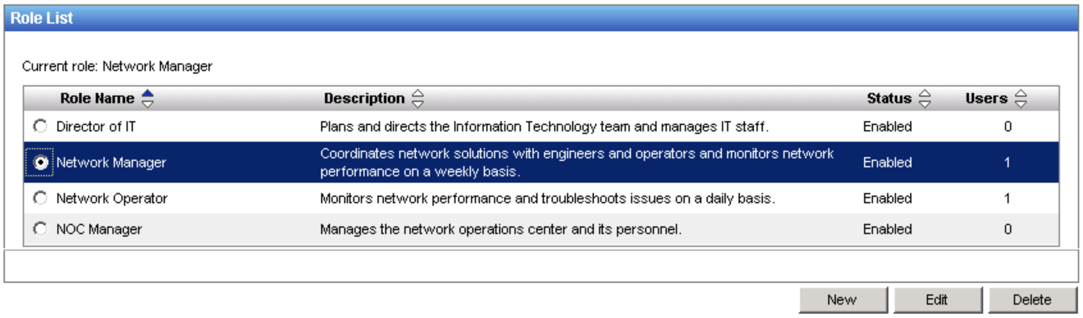
Roles are created and assigned as separate steps. For each user account you create, you assign a role on the User Properties page. You can then edit that role to change the product access privileges. Or you can create new, custom roles and return to the User Properties page to assign them.

Before you register Unified Communications Monitor with the CA NetQoS Performance Center, the Role List page allows you to view the currently configured UC Monitor roles, see how many users have these roles assigned to their account, edit or delete roles, or add new, custom roles. Once UC Monitor is registered with the NetQoS Performance Center, you are redirected to the NetQoS Performance Center for all administrative tasks associated with roles, privileges, and users. A link to the appropriate Administration page in the NetQoS Performance Center is provided.

To create a new role or edit an existing role:

1. In the navigation links, click **Administration > Security**, and then click **Roles**.

   The Role List page is displayed. The following image shows pre-defined and custom roles:



Role List

Current role: Network Manager

Role Name	Description	Status	Users
○ Director of IT	Plans and directs the Information Technology team and manages IT staff.	Enabled	0
● Network Manager	Coordinates network solutions with engineers and operators and monitors network performance on a weekly basis.	Enabled	1
○ Network Operator	Monitors network performance and troubleshoots issues on a daily basis.	Enabled	1
○ NOC Manager	Manages the network operations center and its personnel.	Enabled	0

   The Role List contains the following information:

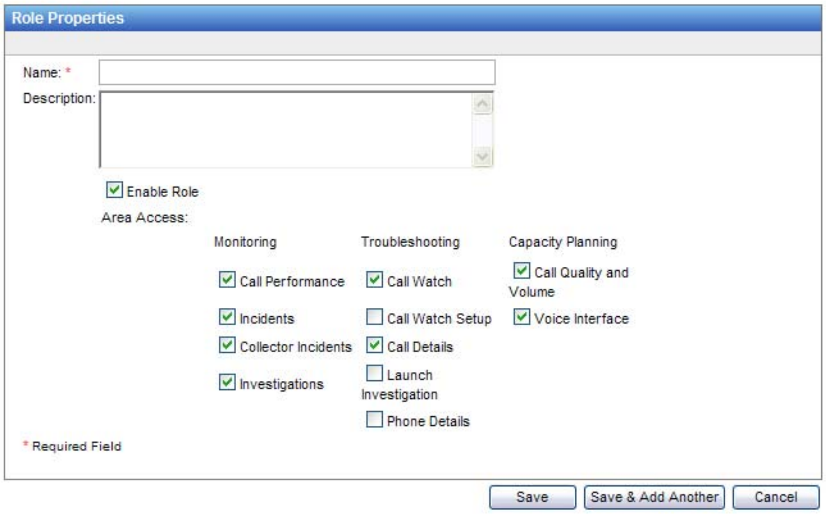
Field	Description
Role Name	Name of the role. Either Network Manager or Network Operator, or a custom role you've created and named. ***Note:*** Once registered with the CA NetQoS Performance Center, all roles in all registered CA | NetQoS products are included in the list.
Description	(*optional*) Description to identify this role.

Field	Description
Status	The status of this role, either Enabled or Disabled. You can disable a role by clearing the **Enable Role** check box while you are editing it on the Role Properties page. See below for more information.
Users	The number of users to whom this role is assigned. ***Note:*** A role cannot be deleted if it is currently assigned to a user.

2. To create a new, custom role, click **New**.

   To edit a role, click to select the role that you want to edit. Click **Edit**.

   The Role Properties page is displayed:



Role Properties

Name: *

Description:

☑ Enable Role

Area Access:

Monitoring	Troubleshooting	Capacity Planning
☑ Call Performance	☑ Call Watch	☑ Call Quality and Volume
☑ Incidents	☐ Call Watch Setup	☑ Voice Interface
☑ Collector Incidents	☑ Call Details	
☑ Investigations	☐ Launch Investigation	
	☐ Phone Details	

* Required Field

3. Enter or change the following information for a role:

Property	Description
Name	A name for the role. ***Note:*** If you are editing a role, you can change the name of a custom or predefined role.
Description	(Optional.) A description to identify this role.
Enable Role	If selected, indicates that the role is currently active. The role must be enabled to give users with this role the access that you designate here.
Area Access	Product features to which users with this role have access. Select one or more areas. The areas listed refer to reports that can be viewed and product functionality that can be accessed. For example, the Call Watch option allows the user to view the Call Watch Real-Time Report, while the Call Watch Setup option enables that user to configure and launch a Call Watch. When you upgrade from a previous version of Unified Communications Monitor, new options and areas often become available. These options are not enabled for any custom roles you created with a previous version of the product. You can, however, manually enable them for these custom roles.

4. Click **OK**.

The new role appears in the Role List, where it can be edited or even deleted, if desired. The following topic explains how to delete a role.

Deleting a Role

Before you register Unified Communications Monitor with the NetQoS Performance Center, the Role List page allows you to view the currently configured UC Monitor roles, see how many users have these roles assigned to their account, and delete roles as desired. Any role to which no users are currently assigned may be deleted, including the default roles (Network Manager and Network Operator). Once UC Monitor has been registered with the NetQoS Performance Center, however, you are redirected to the NetQoS Performance Center for all administrative tasks associated with roles, privileges, and users. A link to the appropriate Administration page in the NetQoS Performance Center is provided.

You cannot delete a role to which a user is assigned. If you want to delete a role, first determine whether a role has any assigned users by checking the **Users** column on the Role List page. The number of assigned users is indicated.

To delete a role:

1. In the navigation links, click **Administration > Security**, and then click **Roles**.
2. On the Role List page, scan the **Users** column to make sure no users are assigned to the role you plan to delete.

   If any users are assigned to this role, refer to "Adding or Editing a User" on page 228 for the steps to take. You'll need to access the User List to find out which users are assigned to the role and then edit the user accounts to change their assignments.
3. Click the radio button next to the role that you want to delete.
4. Click the **Delete** button.
5. On the Confirm Delete page, click **Delete** to complete the deletion. Otherwise, click **Cancel**.

The role is removed from the Role List.

Working with SNMP Profiles

SNMP polling of voice gateway devices and Avaya Communication Managers is required to gather important call performance data. To enhance system security, SNMP community (or context, for SNMPv3) information is handled by means of *SNMP profiles*, definitions that the Collector uses to query media devices for quality information. Profiles are used for all versions of SNMP, but any profiles that use SNMPv3 include several additional security parameters that are not available with other versions of SNMP.

The Administration section of the UC Monitor Management Console contains several pages where you can create, modify, and delete SNMP profiles, as well as associate them with the appropriate voice gateways. If the data source is registered to the CA NetQoS Performance Center, profiles are then sent up at the next synchronization. The NetQoS Performance Center allows other CA NetQoS data sources to share SNMP profile definitions so that you only have to create them once.

Any synchronization data flows between UC Monitor and the NetQoS Performance Center are encrypted, and SNMP security information is stored in encrypted format.

Viewing the SNMP Profile List

For every Cisco voice gateway device and every Avaya Communication Manager, the Collector needs access to SNMP security information to allow it to poll for end-of-call quality metrics or device records. You supply community information and, where applicable, SNMPv3 security parameters, by creating SNMP profile definitions. You can view any profiles that have already been created in the system on the SNMP Profile List page. Click **Administration > Security > SNMP Profiles** to see the list.

The following table describes the information provided in the SNMP Profile List:

Column	Description
SNMP Profile	The name you assigned to this profile.
SNMP Version	The version of SNMP with which this profile should be used. Either: • SNMPv1/SNMPv2C, or • SNMPv3
Authentication	The type of authentication protocol to use to contact devices associated with this profile. One of the following: • None (do not attempt authentication) • MD5 • SHA
Privacy	The encryption protocol to use for data flows sent to any devices associated with this profile. One of the following: • None (do not encrypt communications) • AES (128-bit encryption) • DES • Triple DES Always “None” if no authentication is enabled for this profile.
Use as Default	Whether the Collector should use this profile first to attempt SNMP polling whenever it discovers a new Avaya Communication Manager or voice gateway device, or for any device that supports SNMP polling by the Collector but does not have an associated SNMP profile.

Creating a New SNMP Profile

SNMP profiles supply information to the Collector to use when contacting voice gateway devices or Avaya call servers using SNMP queries to get end-of-call quality metrics or device information. You need to create a new SNMP profile for each SNMP community or each SNMPv3 secure device MIB. If the Collector cannot contact your voice gateways via SNMP, it cannot report metrics for call legs that travel through a gateway to or from points in the PSTN. If it cannot contact Communication Manager call servers, it cannot report identifying information for devices.

Each SNMP profile consists of the following components:

- A name for the profile
- The SNMP version
- The port
- Whether this profile should be used as the default, for all new media devices or Avaya call servers that are discovered
- The SNMP community or context, and other security information, where applicable

Because the first two versions of SNMP were very similar from a security standpoint, only two options are available for the **SNMP Version** parameter: SNMPv1/SNMPv2C and SNMPv3. If you create an SNMP profile for SNMPv1 and v2C and provide a **Profile Name**, only one additional parameter is actually required—the SNMP Community Name. The remaining parameters (**Port** and **Use as Default**) are optional.

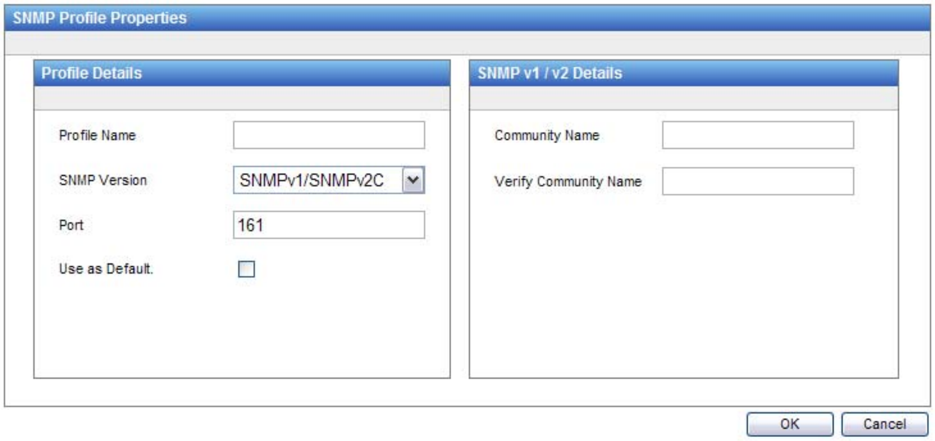
To create a new SNMP profile:

1. Click **Administration > Security > SNMP Profiles**.

   The SNMP Profile List page is displayed. If no profiles have been created, only the default profile, Public, is shown in the list.

2. Click **New** to add a new profile.

   The SNMP Profile Properties page is displayed:



SNMP Profile Properties

Profile Details

Profile Name

SNMP Version: SNMPv1/SNMPv2C

Port: 161

Use as Default. □

SNMP v1 / v2 Details

Community Name

Verify Community Name

3. Supply the required information in the fields provided.

The following table describes the available parameters. Different parameters are available for each version of SNMP that is supported:

Parameter	Description
SNMPv1/SNMPv2C	
Profile Name	A name to use to identify this SNMP profile.
SNMP Version	The version of SNMP to use, either: • SNMPv1 or SNMPv2C (profile parameters are identical for both versions), or • SNMPv3 Additional parameters are required for SNMPv3. See below.
Port	The port to use to make SNMP connections to the media device associated with this profile. The default should typically be used: Port 161.
Use as Default	Whether the Collector should use the information in this profile as a default—to contact any new media devices that are discovered from monitored traffic. A default profile is required. You can only remove the **Use as Default** designation from an SNMP profile if you have edited another profile to add this designation. Only one profile may have the default designation at a time.
Community Name	The SNMP community, a secure string that allows the Collector to query the MIB of this gateway device. The community you supply needs to provide read-only access to the device MIB. In the default SNMP profile, the community is public.
Verify Community Name	The SNMP community, retyped to confirm it.
SNMPv3 Details	
User Name	The user name used for secure access to the media device(s) or server(s) associated with this profile.
Context Name	(*Optional*) Determines the context of the SNMP session. The SNMP agent on the associated device uses the context to control which MIBs or MIB content (rows) are exposed for the SNMP session.
Authentication Protocol	The type of authentication protocol to use to contact devices associated with this profile. One of the following: • None (do not attempt authentication) • MD5 • SHA
Authentication Password	The password to use for authentication using SNMPv3 and the selected authentication protocol.
Verify Authentication Password	The password to use for authentication, retyped to confirm it.

Parameter	Description
Privacy Protocol	The encryption protocol to use for data flows sent to any devices or servers associated with this profile. One of the following: • None (do not encrypt communications) • AES (128-bit encryption) • DES • Triple DES Always “None” if no authentication is enabled for this profile.
Privacy Password	The password to use when exchanging encryption keys.
Verify Privacy Password	The password to use when exchanging encryption keys, retyped to confirm it.

4. When you have finished supplying information for the required parameters, click **OK** to save the new profile.

The new SNMP profile appears in the SNMP Profile List. You now need to associate it with the voice gateways whose security parameters it contains. To do that, edit each gateway to select the appropriate SNMP profile. Click **Administration > Data Collection > Media Devices** to get started. And see “Editing a Voice Gateway” on page 120 for more information.

Note: You do not need to edit Avaya call servers to select their SNMP profile. The Collector will try each profile in turn, beginning with the default profile, until it succeeds in contacting the Communication Manager.

Editing an SNMP Profile

You can edit an SNMP profile that you have already created to change its name, change the port or the default designation, or change security parameters (most are available for SNMPv3 only).

The SNMP Profile Properties page lets you modify the profile name, view the security information that has been configured in this profile, select or clear the **Use as Default** check box to select a default SNMP profile, and change any security information already configured, such as the authentication protocol or password (SNMPv3 only).

SNMP profiles must be associated with the appropriate voice gateway devices as a separate step. Any modifications you make to a profile by means of the following procedure do not affect any existing associations of profiles with devices. See “Editing a Voice Gateway” on page 120 for information about associating an SNMP profile with a voice gateway device.

To edit the properties of an SNMP profile:

1. In the navigation links, click **Administration > Security > SNMP Profiles**.

   The SNMP Profile List page is displayed.

2. In the table, find and select the profile you want to modify.

3. Click **Edit**.

   The SNMP Profile Properties page is displayed.

Any of the fields shown in the **Details** panes can be edited. You can add, modify, or delete the information in these fields. See "Creating a New SNMP Profile" on page 236 for information about these fields.

4. When you have finished making modifications to the profile, click **OK** to save your changes.

   You return to the SNMP Profile List page. Changes to any parameters that are normally displayed in the list are reflected.

   Note: The SNMP Profile List does not display any secure information, such as passwords.

   You must now reload the Collector(s). The Reload operation sends the updated SNMP information to all NetQoS Collectors (this operation does not apply to OCS Collectors).

5. In the navigation links, click **Administration > Data Collection > Collectors**, and then click the **Reload All** button to reload Collectors.

APPENDIX A

Working with Groups in the CA NetQoS Performance Center

After you complete the initial configuration tasks required to run CA NetQoS Unified Communications Monitor in your environment, you should consider the usefulness of creating custom groups to help you manage and organize your Locations and devices. Custom groups serve several purposes:

- to group managed items in a way that facilitates reporting.
- to control the managed items and associated data that each UC Monitor operator can view.
- to allow for monitoring of multiple enterprises with overlapping IP addresses as separate entities (domain groups).

The CA NetQoS Performance Center is required to enable the grouping feature. Domain groups are supported starting with CA NetQoS Performance Center version 6.1. Only a user with the Administrator product privilege in the NetQoS Performance Center can create or edit groups.

This appendix covers the following topics:

ABOUT THE GROUPING FEATURE

UC Monitor groups enable you to logically organize your call servers, media devices, voice interfaces, and Locations. Groups function similar to a tree file structure, with each group containing subgroups, Locations, or devices. You can view this hierarchical structure in the CA NetQoS Performance Center, where all group management tasks are performed. The structure is propagated to UC Monitor reports, where it allows for drilldown from top-level groups into subgroups and into individual Locations.

Properly organizing your devices and Locations in groups enables you to:

- Manage and organize UC Monitor reports.
- Assign UC Monitor user permissions appropriately.

You should plan to set up groups that resemble the reporting structure of your IT organization, the geography of your organization, or the logical structure of your system. To ensure group validity, always place call servers and media devices at the nodes in the Groups tree where access permissions will be applied.

Grouping is configured by means of a tri-pane interface that allows you to see items nested in a hierarchical structure, create new groups and view information about their membership. Groups can contain multiple levels of subgroups. A user with permission to view a group can also view all of its subgroups.

Groups cannot be created or edited in the UC Monitor Management Console. To create or edit groups for Locations and devices being monitored with Unified Communications Monitor, you must first register the Unified Communications Monitor data source with the CA NetQoS Performance Center. Once registration is complete, access to the group management interface requires you to be logged into the NetQoS Performance Center with Administrator privileges.

Grouping Terms and Types

CA NetQoS Performance Center groups perform two major functions:

- they are assigned to each user account to control the associated operator’s product access.
- they are used to determine the data context for views and report pages.

  Groups provide a logical structure to help IT staff identify managed items and understand system performance in context.

We recommend that UC Monitor Administrators create groups based on location or site so that report data is organized to be useful for IT staff.

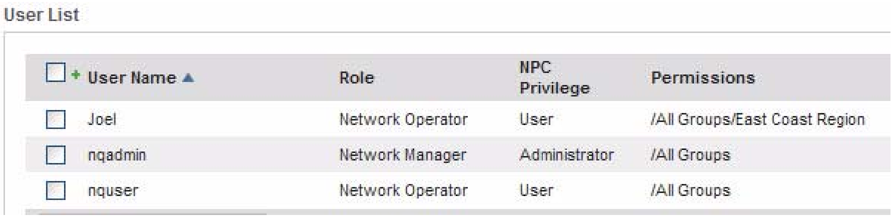
All groups discussed in this Appendix are containers of managed items whose data the assigned user can view. They are configured in the **Admin** area of the NetQoS Performance Center and can be viewed in the *Groups tree*. See “System Groups” on page 244 for an image.

The CA NetQoS Performance Center supports multiple group types, which enable other features, such as troubleshooting by site and monitoring by domain. When you add a new group, you can select whether to create a new **Custom** group or a new **Site** group. Site groups resemble custom groups, but they include additional parameters to identify a physical location, such as a street address, a city, or a state. We recommend adding Location groups to Site groups so that managed items representing a distinct physical location within an enterprise can be monitored per site.

Permission Groups

Limiting access to data based on groups is supported by all CA NetQoS products that offer integration with the CA NetQoS Performance Center. A NetQoS Performance Center Administrator can assign groups to each user account to filter the data that the associated product user can view.

For example, if I wanted to grant a UC Monitor operator named Joel permission to see the call servers, media devices, and Locations on the East Coast within our enterprise, I could create a Site group called `East Coast Region` and add all the call servers, media devices, and Locations in the East Coast region of my network to that group. I could then edit Joel's user account in the NetQoS Performance Center and add `East Coast Region` to his list of **Assigned Groups**. When he accessed reports in the UC Monitor Management Console, Joel would only be able to view UC Monitor data from calls involving servers, devices, and Locations on the East Coast.



User List

□ + User Name ▲	Role	NPC Privilege	Permissions
□ Joel	Network Operator	User	/All Groups/East Coast Region
□ nqadmin	Network Manager	Administrator	/All Groups
□ nquser	Network Operator	User	/All Groups

We discuss permission groups in more depth in the topic titled "Creating Permission Groups" on page 252.

Groups and Subgroups

To continue the previous example, Joel might find it easier to locate the sources of poor call performance if we created subgroups within his East Coast permission group, such as a Massachusetts subgroup, and a North Carolina subgroup. The grouping feature allows you to create multiple levels of groups nested within other groups. Subgroups can provide more precision when an operator is attempting to identify a problem area. If Joel sees that a poorly performing Location isn't merely on the East Coast, but is in North Carolina, he has a smaller set of data to consider when troubleshooting.

We refer to nested groups as *subgroups,* but aside from the fact that data access permissions filter from groups into their subgroups, there is no practical difference between groups and subgroups. Any given subgroup may also serve as a top-level group within the Groups tree, and this structure will be valid until the subgroup is assigned to a user account.

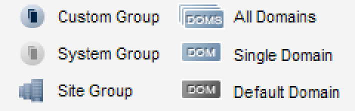
The crucial distinction between a group and a subgroup lies in the way access permissions are applied downward, from top-level groups into their subgroups. It's relatively easy to create groups and assign them to user accounts in such a way as to produce reports that contain no data because the user's permissions do not allow him or her access to that data. Be sure to read and understand "Grouping and Permissions" on page 245 before you start to organize devices and Locations into groups.

System Groups

As CA NetQoS data sources are registered with the CA NetQoS Performance Center, automatic groups of similar managed items are created, based on the contents of each additional database. These automatic groups are called *system groups* and are displayed in the Groups tree with a *system icon* to indicate that they are read-only.

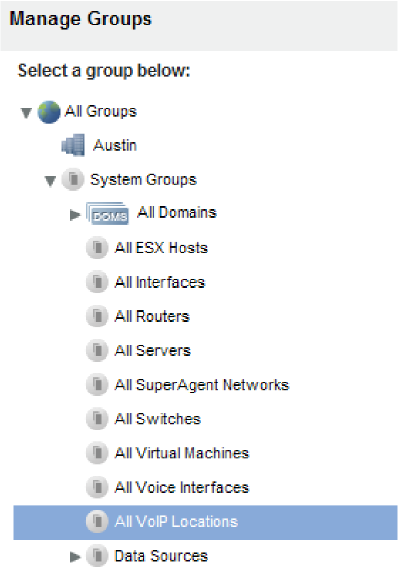
System groups, system group references, and system managed items cannot be deleted from the Groups tree, nor can you edit them. However, they can be added to custom groups as subgroups, and assigned as permission sets to user accounts.

The Manage Groups page provides a legend to indicate how groups and system items are displayed in the Groups tree. The read-only status of system groups is indicated by gray system icons:



Custom Group	DOMS All Domains
System Group	DOM Single Domain
Site Group	DOM Default Domain

When you register the UC Monitor data source with the NetQoS Performance Center, the two products perform a synchronization. Two new groups, the **All Voice Interfaces** and **All VoIP Locations** system groups, appear in the Groups tree:



Manage Groups

Select a group below:

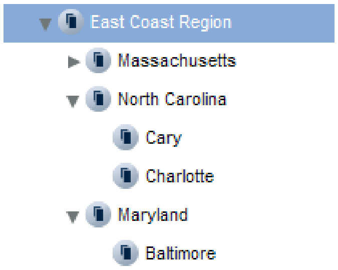
- ▼ All Groups
  - Austin
  - ▼ System Groups
    - ▶ DOMS All Domains
    - All ESX Hosts
    - All Interfaces
    - All Routers
    - All Servers
    - All SuperAgent Networks
    - All Switches
    - All Virtual Machines
    - All Voice Interfaces
    - All VoIP Locations
    - ▶ Data Sources

Any Locations you add to the UC Monitor data source are sent up to the NetQoS Performance Center during product synchronization, where they are automatically added to the All VoIP Locations system group, highlighted in the above image. The UC Monitor data source itself also appears as a group under the Data Sources branch. It contains several subgroups that, in turn, contain managed items (Locations, call servers, and media devices).

Group membership (managed items, such as media devices, call servers, call server groups, and Locations) is visible in the Show Items pane on the right. Select a node that contains these items to see them.

Grouping and Permissions

NetQoS Performance Center grouping is hierarchical. The Groups tree helps you visualize and organize your grouping structure, and it also enforces some basic rules about permissions. Top-level groups act as containers for individual items, such as call servers, or for subgroups of items, creating a tree structure similar to a typical Windows directory structure. If a UC Monitor operator has permission to view data from a top-level group under the main UC Monitor data source group, that operator can also view data from all items within that group and within all its subgroups. Here's an example:



Access to call server data is required to enable an operator to view useful data in Unified Communications Monitor. Call servers are not members of the All VoIP Locations group, so adding this group to a user's permissions is not sufficient to grant access to call performance data. If you want selected users to have access to call performance data from Unified Communications Monitor, you need to create some custom groups that contain Locations and call servers, and then edit selected user accounts to add the custom groups to their list of Permission Groups.

Any user whose list of assigned permission groups includes "North Carolina" can view call data from the six Locations in the East Coast Region/North Carolina/Cary subgroup, as well as the data associated with the two Locations in the East Coast Region/North Carolina/Charlotte subgroup, but *only if* the required devices—the call servers carrying the call data to and from North Carolina—are members of the North Carolina group.

The placement of the devices is important. Without permission to access the call server data, a user would not be able to view data from that Location. Permissions are applied downward, from groups into their subgroups.

By default, every UC Monitor user has view access to the system group known as **All Groups/Data Sources/VoIP@<DataSourceName>**. (The Data Sources system group is two levels above the "East Coast Region" custom group in the Groups tree shown above.) All managed items known to the UC Monitor data source are contained in this group. As a result, the Administrator seeking to restrict access to UC Monitor data on a per-user basis must create and assign custom groups. But also by default, users with permission to view data from other CA NetQoS data sources have no access to UC Monitor data. The NetQoS Performance Center **Admin > User Settings** pages allow you to control user access to group data.

About Managed Items

No managed items are available for grouping unless they are known to the CA NetQoS Performance Center. First, the UC Monitor data source must be registered to the NetQoS Performance Center. And managed items must have been either detected by the Collector or defined manually by an Administrator before they can be viewed in the NetQoS Performance Center and added to groups.

Managed items in the UC Monitor database are reported to the NetQoS Performance Center every 5 minutes, at each synchronization. Specifically, the Locations and voice gateways you have defined or imported into the UC Monitor Management Console, as well as all call servers and media devices that have been detected during call performance monitoring, are reported up during synchronization. On the NetQoS Performance Center Groups pages, they appear under the **All Groups** heading as system groups, shown in gray to indicate that they are view-only. See the image in "Grouping and Permissions" on page 245 for an illustration of system groups and custom groups.

Two types of groups are handled slightly differently than the groups that are flexible containers of managed items: call server groups, and Avaya trunk groups. (Cisco trunk groups must be manually created as typical custom groups.) These types of groups cannot be created in the NetQoS Performance Center and are therefore sent up from the UC Monitor data source as system groups instead of as items that can be added to custom groups.

As soon as they have been reported up to the CA NetQoS Performance Center, managed items can be added to groups. An individual item monitored by Unified Communications Monitor, such as a Location, a trunk group, or a call server, may be assigned to multiple groups and subgroups. The multiple assignments may be accomplished by creating group rules, or by adding an item separately to each group and subgroup.

Group Membership

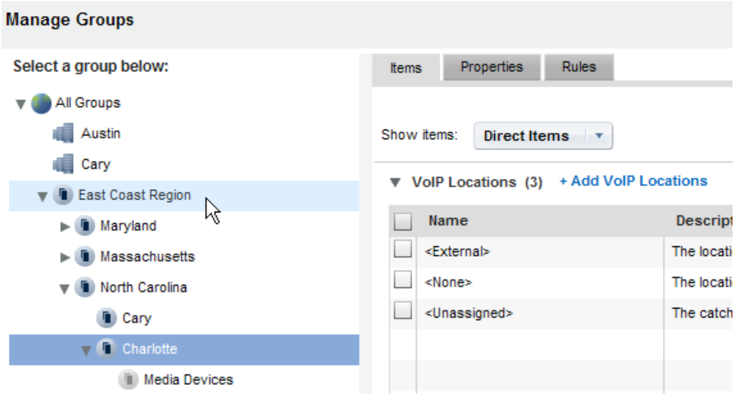
Groups appear in the Groups tree, but individual items do not. (In previous versions of the CA NetQoS Performance Center, you could expand a group until its member nodes appeared in the tree.) You can now view basic information about group membership in the Show Items pane.

To view the membership of a group:

1. In the CA NetQoS Performance Center, click **Admin > Groups**.
2. Locate a group that contains managed items by clicking to expand the groups that contain it in the Groups tree.

   You might have to continue clicking past groups that are merely containers of the subgroups that contain managed items.
3. Click to select the node that contains items.

   A list of its members appears in the Show Items pane.



□	Name	Descript
□	<External>	The locati
□	<None>	The locati
□	<Unassigned>	The catch

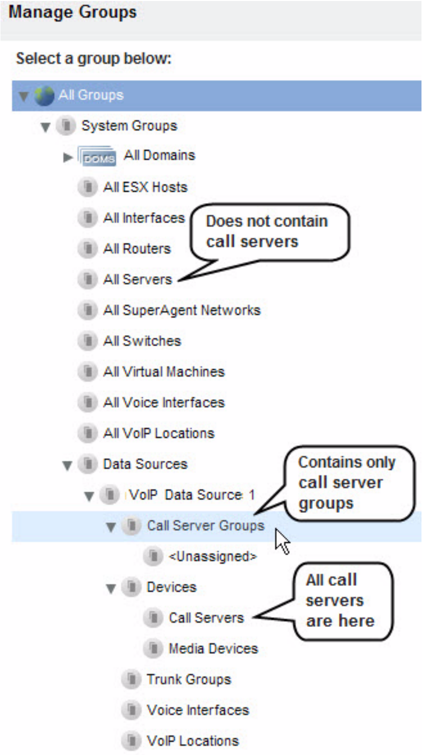
Items designated as "direct items" were added to the group, either manually or by the application of a group rule. Otherwise, managed items may be "inherited items," indicating that they are child items of a managed item that was added to the group directly. An example of a child item would be an interface that was inherited by the group when its router was added directly. The inheritance feature does not apply to Unified Communications Monitor.

Call Servers and System Groups

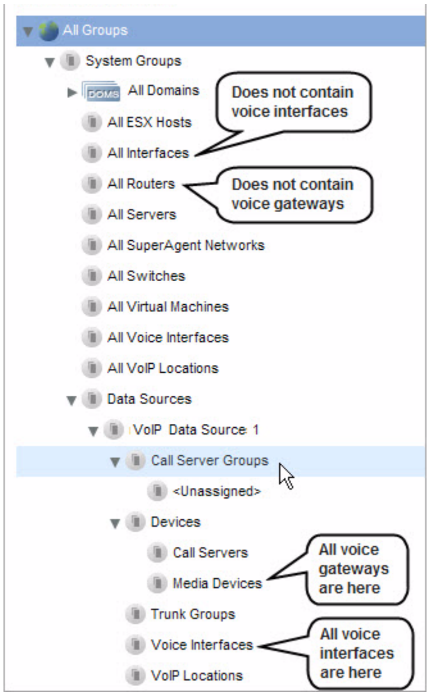
Unified Communications Monitor discovers most call servers from monitored call traffic, although they can also be added to the system manually. The identities and configuration of call servers and call server groups are sent up to the CA NetQoS Performance Center at each synchronization. As soon as new call servers are discovered, they are automatically added to a default UC Monitor call server group (named "`<Unassigned>`"). When this information is sent from Unified Communications Monitor to the NetQoS Performance Center, they are also added to a system group named Call Server Groups. Individual call servers are added to the Data Sources\[UC Monitor DataSourceName]**Devices****Call Servers** system group; they do not appear in the All Servers system group.

Note: Media devices are handled slightly differently. If a NetVoyant data source is also registered to the NetQoS Performance Center, they are also monitored as routers, which they closely resemble. The Media Devices group (under Data Sources\[UC Monitor DataSourceName]\Devices**Media Devices**) contains both routers and voice gateways; you can therefore see many of the same devices in the All Routers system group.

Here's an illustration of the Groups tree, showing where call servers and call server groups are placed:



And to fully understand the above note about media device placement in the Groups tree, refer to the following image:



Be aware that no system groups can be edited. Any custom call server groups you create in Unified Communications Monitor are treated as view-only system groups in the CA NetQoS Performance Center because they can only be created or edited in the UC Monitor interface. They are displayed in the tree at the same level as the `<Unassigned>` call server group node. Although you cannot change its membership in the NetQoS Performance Center, you can add a call server group to another custom group by copying and pasting. (You *can* change call server group membership in Unified Communications Monitor. See "Adding a Call Server to a Call Server Group" on page 140.)

Finally, where pools of Microsoft servers are being monitored, a system call server group is created for each pool. Such groups cannot be edited, but they can be viewed in Unified Communications Monitor. To change the way these groups appear in UC Monitor reports, create custom groups and add call server groups to them in the NetQoS Performance Center. At the next synchronization, information about the new group organization is sent to Unified Communications Monitor.

The grouping of call servers works slightly differently when monitoring Cisco or Avaya than when monitoring Microsoft Office Communications Server 2007, but any automatically created groups are displayed in gray in the Groups tree to show that they cannot be edited. See "More about Cisco Call Servers" on page 249 and "More about Microsoft Call Servers" on page 250 for details.

Using Groups to Ensure Data Privacy

One of the main reasons to set up a grouping structure is related to data privacy concerns. Some call data is sensitive in nature, and access to it should be controlled. The section titled "Grouping and Security" on page 251 treats this topic in depth.

A typical example of using groups to ensure VoIP data security is limiting the call data that UC Monitor operators can view on a per-Location basis. To do that, you first create groups that contain only the Locations that selected users need to access, and then customize each user account, adding these new groups to their permissions. But when you create the custom groups, you also need to explicitly grant access to data from the call servers that handled the calls. Otherwise, these users will see reports that contain no data.

By granting users access to *all* call servers, you can be sure they can see all call data for the Locations to which they have been granted access. While call servers are likely to be displayed slightly differently in the Groups tree for the different monitoring environments, it's a best practice in each case to set up grouping based on group rules so that newly discovered call servers or pools of call servers are automatically added to users' permissions.

More about Cisco Call Servers

One issue you might encounter when setting up groups to allocate access permissions to call data concerns call server cluster behavior. In a Cisco environment where call servers are running in clusters, multiple call servers in your system might serve as backups for load-balancing and failover situations. Until a failover occurs, these call servers might not be discovered by the Collector.

It is therefore possible for a UC Monitor operator to be prevented from seeing the call data associated with a particular report if a failover occurs. The permission group assigned to that operator's user account might not include the failover call server, which was previously unknown to the NetQoS Performance Center.

To avoid this situation, you would need to manually add every call server, using the Call Server List page in UC Monitor Administration. These actions would avoid the need for Unified Communications Monitor to discover every call server. Or you could create a custom permission group for selected users under the **All Groups** branch. The top-level items in this custom permission group tree would have to include the Call Servers system group. The rest of the group structure would contain the VoIP Locations that each user needed to monitor. With that structure, each time a new call server is discovered, it is automatically added to the user's permission group, and data from VoIP Locations is accessible to the UC Monitor operator.

Creating a custom group structure based on group rules allows you to automate the process of adding items to groups. These rules allow for extensive customization. Newly discovered call servers can be added to custom groups much more quickly when group rules are in effect; the only delaying factor is the five minutes between product synchronizations.

More about Microsoft Call Servers

Microsoft OCS does not deploy standard "call servers" in the sense that Cisco uses that term. However, in an OCS Enterprise Edition environment, Unified Communications Monitor designates the servers that send call quality reports to the UC Monitor Management Console as call servers. Depending on your version of Office Communications Server 2007, they are either QoE Monitoring Servers or Front-End servers (in R2).

If Microsoft call servers are members of pools, call server groups are created automatically and sent up to the CA NetQoS Performance Center based on pool identity and membership. In the Show Items pane on the Manage Groups page, you might notice that member identity depends on pool configuration, on the server that sends call quality reports to the UC Monitor Management Console, and on the version of Office Communications Server 2007 you are running.

These automatically created call server groups contain no Locations until the Administrator manually creates a new, custom grouping structure to include both call server (system) groups and their associated VoIP Locations.

It's therefore a best practice to create group rules in the CA NetQoS Performance Center that automatically add all members of the Call Server Groups system group to an upper-level custom grouping structure, and automatically populate lower-level groups with VoIP Locations. This practice ensures that group membership is always up-to-date as new Locations, media devices, and call servers are discovered from call traffic. See "Creating Permission Groups" on page 252 for more information about group rules.

The same permissions issue described above for Cisco monitoring also faces the operator whose permission group includes the Microsoft call server group with no Locations: no data is available in reports viewed by that operator. The solution is also similar: to manually create a permission group that includes items from the Call Server Groups and VoIP Locations system groups so that data from associated Locations can be viewed.

See "Rearranging Group Structure" on page 267 for more information about access permissions and valid grouping structure.

Grouping and Security

Grouping provides additional granularity to the UC Monitor role-based security. Chapter 10, “Setting Up Security” on page 223 provides detailed information about the UC Monitor security features and explains the differences among users, roles, and product privileges. The ability to create permission groups that restrict view access to certain data, such as all call data from a selected Location, works something like a filter to further control the data each UC Monitor user sees in reports.

The following table shows how these security features work together:

Feature	Description	Examples
User account	The credentials of a person who is authorized to operate Unified Communications Monitor and perform certain tasks. Each pre-defined user is associated with one role and one product privilege level. Custom users can have different product privileges for different data sources and permission groups (see below).	Two UC Monitor users are pre-defined: • the UC Monitor Administrator, `nqadmin` • the default product user, `nquser` The main difference between them is their assigned product privilege. See below.
Product privilege	The user’s broad level of access to product functionality and configuration.	Determines whether the user can perform administrative actions. In Unified Communications Monitor, either: • Administrator—Can perform all administrative tasks, or • User—Cannot perform any administrative tasks.
Role	The role for the associated user. Defines the area access allocated to each user. Provides a means of protecting sensitive information.	The pre-defined UC Monitor roles are: • Network Manager —An administrative role; by default, can access all product areas and features. • Network Operator—A restricted role; by default, can access all reports but cannot launch an investigation or set up a Call Watch. Role has no effect on user access to features in the Administration area. This access is determined by the product privilege.
Permission group	The group of managed items (call servers, media devices, and Locations) whose data can be viewed in reports. Within reports, restricts the data that is shown.	A user with the Network Operator role can access all reports by default. With the “North Carolina” permission group applied to his user account in the NetQoS Performance Center, he can now only view data from groups of call servers, media devices, and Locations that are included in the “North Carolina” group or in its “Raleigh” subgroup in those reports.

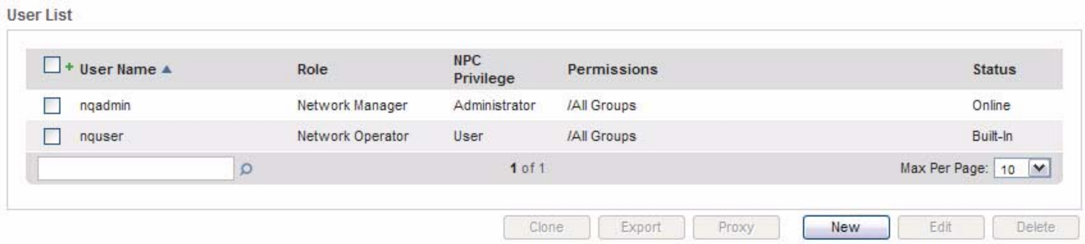
Without custom permission groups, you could create a user account with a User product privilege and a custom role that only allows view access to reports in the Monitoring section, preventing that person from seeing any Troubleshooting or Capacity Planning reports. You could not, however, prevent that person from drilling down into Performance Call Details and Call Leg Details reports. These reports contain potentially sensitive data about who is calling whom, and at what time of day.

Instead, you would have to create permission groups that contained the sensitive call data. For example, the Location containing the CEO's phone could be placed in a group with the phones belonging to the CFO and VP of Finance. Or you could create a separate Location definition for each confidential phone in your system and place them in custom groups. Either strategy would allow you to prevent selected UC Monitor operators from accessing the confidential data.

Warning: The second strategy, creating a dedicated Location for each confidential phone, is limited by the restriction on overlapping subnets in Location definitions. Specifically, it could prevent you from adding a subnet that contains a larger group of phones to a Location definition. If the more inclusive subnet contained the single phone's IP address, these overlapping subnets would not be allowed, and, lacking a Location definition, a large number of phones would end up in the "Unassigned" Location.

Creating Permission Groups

Once you've created some groups for your Locations and devices, you can assign permissions to UC Monitor users and restrict their product access to the data they need to see. User accounts for the CA NetQoS Performance Center include a **Permissions** property, which determines the domains or the groups of call servers, media devices, and Locations that each user can access. The following illustration shows the two default user accounts and their default permissions:

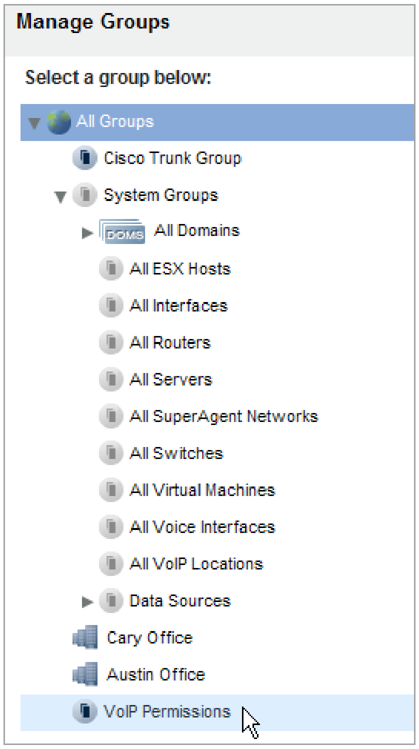


User List

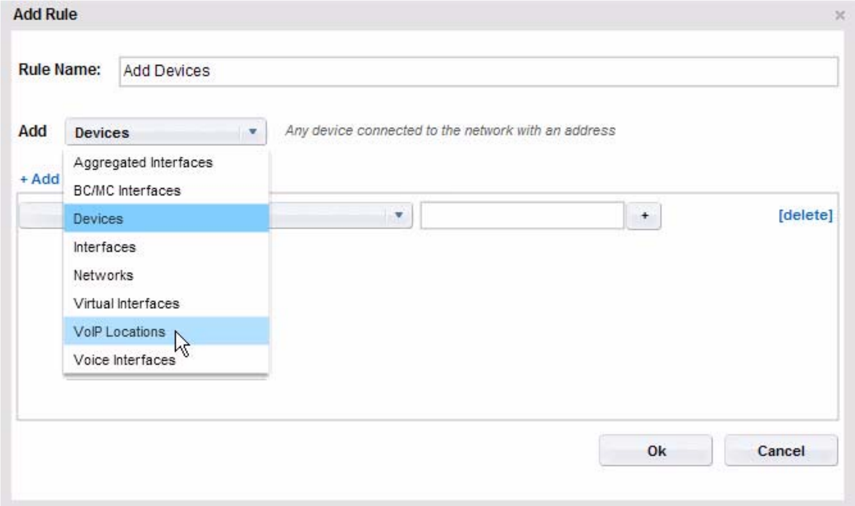
□ User Name ▲	Role	NPC Privilege	Permissions	Status
□ nqadmin	Network Manager	Administrator	/All Groups	Online
□ nquser	Network Operator	User	/All Groups	Built-In

The default permission group, **All Groups**, allows users to access all groups defined in the NetQoS Performance Center, both system groups and custom groups. System groups, permission groups that are automatically created during registration with NetQoS Performance Center, are discussed above in "System Groups" on page 244. To create a more secure system, you should create custom groups that limit operator access to call data that is either confidential or irrelevant to their responsibilities.

Here's an example of a NetQoS Performance Center Groups tree containing several types of groups, including system groups, site groups, and a custom group specifically created to allocate access permissions:



In the above image, the NetQoS Performance Center Administrator has created the **VoIP Permissions** group and added a group rule that places all managed items discovered by Unified Communications Monitor in it. The group rules interface allows you to select call servers and VoIP Locations for a new group.

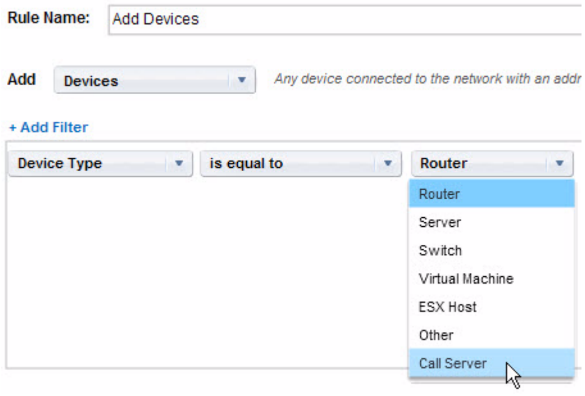

Add Rule

Rule Name: Add Devices

Add: Devices

Any device connected to the network with an address

To write a group rule that adds all call servers to a group, click **Add Filter**, and then select **Device Type is equal to Call Server**, as shown below:



Rule Name: Add Devices

Add: Devices — Any device connected to the network with an addr

Any users with the **VoIP Permissions** group assigned to their user account will be able to see all data collected by Unified Communications Monitor. Restrictions on user accounts can be placed by creating subgroups within the VoIP Permissions group and granting users access only to those subgroups. To ensure a valid permission group, each subgroup should contain a subset of VoIP Locations and call servers.

More about Product Privileges

Basic permissions to access the CA NetQoS Performance Center and Unified Communications Monitor are required for users who want to view data in both consoles. They do not allow users to change group configuration or create new groups.

The **Product Privilege** user account property in the NetQoS Performance Center is used to grant or restrict user access to specific data sources. The Administrator product privilege is required to enable the creation of custom groups: the UC Monitor Administrator must also have the Administrator product privilege assigned to her NetQoS Performance Center user account to enable her to use the grouping feature.

Product privilege can be applied very specifically. For example, a person can be a user of the CA NetQoS Performance Center, giving her the ability to view items in the NetQoS Performance Center console but not perform any administrative tasks, and that same person can be an Administrator in a specific instance of Unified Communications Monitor, allowing her full administrative privileges to that data source when she drills into data from the Unified Communications Dashboard page. Note, however, that the role assigned to her UC Monitor user account must also allow her to view specific product areas (that is, Monitoring, Troubleshooting, Capacity Planning, or Administration) before she can access them.

The NetQoS Performance Center online Help contains a full set of instructions for modifying user accounts to change the product privileges associated with each account.

Monitoring by Domain

The CA NetQoS Performance Center supports monitoring by domain, which means that overlapping IP addresses that correspond to separate enterprise networks, or that have different domain name assignments, can be monitored separately, with either no or carefully controlled sharing of secure data. Domain support is implemented as part of the grouping feature in CA NetQoS Performance Center version 6.0 and later. Registration with the NetQoS Performance Center is required to enable it in Unified Communications Monitor.

Domains are special system groups that are used to organize monitored items into separate containers, where they can be monitored and reported on separately. The Domain group type was designed for use by service providers, who might be monitoring the networks of multiple discrete enterprises. When you deploy domain definitions in Unified Communications Monitor, the phone traffic from entities that use the same IP address can be monitored separately. After some extra configuration, your current Location names can be used to report performance data per domain. UC Monitor operators can be granted access to report data per domain, similar to the way that reporting per group is handled.

Each time a new managed item is discovered, the Collector can assign it to a domain, based on the **NPC Domain** parameter in the Collector Properties. Domains are a shared configuration resource; custom definitions created in other CA NetQoS data sources can be used in Unified Communications Monitor. You can see a list of custom domain definitions from all data sources in the Groups tree in the NetQoS Performance Center.

The following topics provide more detailed information about domain support in Unified Communications Monitor and the steps to take to configure and populate domain definitions:

- "When to Use Custom Domains" on page 255
- "About NPC Domains" on page 256
- "Custom Domain Assignments in Unified Communications Monitor" on page 257
- "Setting up Domains" on page 257
- "Creating Domain Definitions" on page 258
- "Enabling Domain Monitoring at the Collector" on page 259
- "Using Domains as Permission Groups" on page 260
- "Making Changes to Domain Assignments" on page 260
- "Deleting Domain Groups" on page 261

When to Use Custom Domains

The ability to monitor using separate, custom domain groups is a feature designed for a managed services environment. The ideal situation where this feature adds significant value is a large Internet Service Provider (ISP), with multiple customers whose networks might contain redundant IP addresses. In such a situation, custom domain groups ensure data privacy and allow you to segregate data from separate customer networks. ISP staff can be assigned access permissions to items in a single domain and prevented from sharing data among domains.

A less ideal situation where domain groups might still be deployed is a hosted service provider solution, where the provider has full control of call servers and voice gateways. Domain separation and the association of managed items, such as Locations, with domains are actions that cannot be performed by the call server and are instead performed by the Collector, with each Collector placing items into a single domain. If the Collector itself is hosted, items can be associated with domains, but then the service provider must be responsible for multiple Collectors to accommodate all domains. Issues with firewalls and private networks also come into play, depending on how the ISP has segregated each hosted solution. If the Collector is placed on the customer network, it still must be able to communicate with a central Management Console at the ISP data center.

The call server groups you can create within Unified Communications Monitor do not enforce a domain association and as a result, call servers within call server groups can span multiple domains unless you proceed very carefully with domain and call server group setup. Other warnings and best practices are included in the sections that follow. We advise reading these sections before you set up your custom domains.

About NPC Domains

NetQoS Performance Center domains provide a way to indicate that two managed items that otherwise appear as duplicate IP addresses are actually two different IP addresses. Monitoring by domain allows for CA NetQoS data sources to be deployed in a service-provider environment, in which multiple networks can be monitored as completely separate entities.

Domain monitoring is enabled for each data source as soon as it is registered with the CA NetQoS Performance Center. However, domain identifiers and configuration parameters are not visible in the data sources until at least one custom domain group has been created in the NetQoS Performance Center. The following managed types are associated with the Default Domain once domain monitoring is enabled:

- Devices
- Interfaces and interface addresses
- Networks
- Locations

The data sources that monitor these item types can then report up a domain identifier along with the items' other properties during synchronization with the NetQoS Performance Center. A data source can associate any item type with a domain by including a `DomainID` item type property. For any item whose domain ID is not reported, that item is automatically placed in the Default Domain.

Domains are shared among data sources registered to the same NetQoS Performance Center instance. Although domain containers appear in the NetQoS Performance Center Groups tree as specialized groups, the Group Properties view does not provide a list of items assigned to each one.

The NetQoS Performance Center domain administration feature allows you to specify a primary and secondary name server for each domain you define. For cases in which multiple domains that are monitored by CA NetQoS software products are sharing DNS name servers, you can also supply a proxy server address and a port number on each name server, but these parameters are not used by Unified Communications Monitor.

Custom Domain Assignments in Unified Communications Monitor

The task of creating domain definitions is performed in the CA NetQoS Performance Center. But the UC Monitor Administrator determines the domain assignments of monitored items by selecting the appropriate domain for each Collector.

Domains are defined in the **Manage Groups** section of the NetQoS Performance Center **Admin** tab. Once domain definitions have been sent down to the data sources during synchronization, they are available for use during data collection configuration. In the case of Unified Communications Monitor, at least one custom domain must be created in the NetQoS Performance Center before the necessary parameters are exposed.

The domain definitions that are synchronized to Unified Communications Monitor must be assigned to Collectors. A Collector associates all items it discovers with the Default Domain until the Administrator assigns it a custom domain in the Collector Properties. These items are then automatically associated with the custom domain, but only as they are re-discovered. Domain assignments are not applied retroactively.

The phrase “all items it discovers” is important: where phones, call servers, and voice gateways are discovered during monitoring, Locations and call server groups are not. Location definitions must be manually edited to select a custom domain for the NPC Domain parameter. Otherwise, they are placed in the Default Domain.

After you create a custom NPC domain, you will notice that the Location List reflects the new domain after the first synchronization. New default Locations for the `<External>`, `<None>`, and `<Unassigned>` categories are included in the list so that one of each appears in each domain. Each domain, including the Default Domain, must retain these Locations so that all phones detected in call traffic can be properly classified. Domain designations also appear in report views, where domain identity is indicated by the addition of an “**NPC Domain**” column to the data tables.

Setting up Domains

The domain definitions you create in the Manage Groups section of the CA NetQoS Performance Center are simple containers for managed items discovered by the Collector during monitoring. Custom domains contain no members until you instruct your Collectors to associate all the items they discover with these domains.

As soon as data associated with any managed item, such as a media device or Location containing subnets, has been collected, the domain identifier is bound to that item. Domain associations are not applied retroactively, to data already collected. And a domain association cannot be removed or changed unless you follow the workflow outlined in “Making Changes to Domain Assignments” on page 260.

Because domain monitoring is Collector-based, you should have a clear understanding of which Locations are monitored by each Collector—based on the traffic it collects—before you proceed.

The workflow for implementing domain monitoring is as follows:

1. Create custom domain groups in the CA NetQoS Performance Center.
2. Give the UC Monitor Administrator permission to see all domain groups.

Note: Permissions can be added from the NetQoS Performance Center Edit User Account page.

3. In the UC Monitor Management Console, create new Location definitions. Or edit existing Location definitions to remove all subnets.

   This step prepares Location definitions for further modification.

4. Select appropriate custom domains in the Location Properties, and then add subnets to Locations.
5. Edit each Collector to select the appropriate custom domain for the traffic it monitors.

The topics titled "Creating Domain Definitions" on page 258, "Enabling Domain Monitoring at the Collector" on page 259, and "Making Changes to Domain Assignments" on page 260 cover these steps in detail.

Creating Domain Definitions

To monitor by domain, you must first create the required domain definitions in the CA NetQoS Performance Center. The Administrator product privilege for the NetQoS Performance Center is required.

To create domain definitions:

1. Click the **Groups** menu item on the NetQoS Performance Center **Admin** tab.
2. In the Groups tree, click to expand **System Groups**, and then select the **All Domains** item.

   The **Add Domain** button is enabled.

3. Click **Add Domain**.
4. In the Add Domain dialog box, supply the following parameters:
   - **Domain Name**: The fully-qualified domain name.
   - **Description**: (*Optional*) Descriptive information about this domain namespace, such as the enterprise that owns it.

   The following parameters are not used by Unified Communications Monitor:

   - **Primary DNS**
   - **Primary DNS Port**
   - **Secondary DNS**
   - **Secondary DNS Port**
5. The check box labeled **Enable DNS Proxy Address** refers to networks located behind DNS proxy servers. This parameter is ignored by Unified Communications Monitor.
6. Click **Save** to complete the domain definition, and continue creating all the domain definitions that you will require for your monitoring tasks.
7. As soon as you've created the required domain definitions, navigate to the NetQoS Performance Center Data Sources page (on the **Admin** tab).
8. Select the UC Monitor data source and click **Resync**.

   This action sends the domain definitions to the UC Monitor Management Console immediately instead of waiting until the next automatic synchronization.

You are now ready to instruct the Collectors how to place VoIP and video traffic into separate domains. The following topic provides the steps.

Enabling Domain Monitoring at the Collector

Once you have created at least one custom domain definition in the CA NetQoS Performance Center and data source synchronization has occurred, the **NPC Domain** parameter becomes available in the Collector Properties. And any new Collectors you add to a Distributed system also have this parameter, which instructs the Collector to associate all performance data taken from calls running between the phones and devices it monitors with a selected domain.

The following instructions apply to either a NetQoS Collector or an OCS Collector.

To enable domain categorization by a collection device:

1. In the UC Monitor Management Console, click **Administration > Data Collection > Collectors**.
2. In the Collection Device List, select a Collector, and click **Edit**.

   The Collection Device Properties page is displayed.
3. For the **NPC Domain** parameter, select the appropriate domain from the list.
4. Click **Save** to save the change.
5. Repeat for each Collector. For all the phones and devices it discovers, each Collector will create an association with the same domain.
6. Reload the Collectors to send them the domain information.

Domains are populated with managed items as soon as items are discovered from call traffic. You will need to manually edit Location definitions to select the domain because Locations are not discovered. See “Making Changes to Domain Assignments” on page 260 for more information.

Once you have correctly configured the system, the domain designation is included for each phone, Location, or media device where it appears in reports. You can also verify domain identity in the Location List or Voice Gateway List.

Using Domains as Permission Groups

As soon as you have finished creating custom domain groups in the NetQoS Performance Center, you should add them to user accounts so that Unified Communications Monitor and NetQoS Performance Center operators can see the items that they contain. This is a recommended best practice. However, permission to see any managed item that is associated with a custom domain also automatically grants that user access to data from all other items in that domain group. It is not necessary to grant users explicit permission to see the items in a domain group. By the same token, you should not add the All VoIP Locations group to any user's permissions in a multiple-domain environment because doing so implicitly grants that user access to data from all domains.

Another best practice is to explicitly grant the Administrator permission to see all domain groups. This action makes domain administration much easier. For example, the Administrator will be able to see domain identifiers for all Collectors, Locations, call servers, and voice gateways. By contrast, individual users usually only need access to a single domain.

Avaya trunk groups do not have domain identifiers. As a result, they are not included when you add domains to user account permissions and must be added as individual permission groups. While Locations, media devices, and call servers are managed items, with domain identifiers based on your Collector configuration, Avaya trunk groups are treated as groups in the NetQoS Performance Center, and groups do not have domain identifiers.

Making Changes to Domain Assignments

Because of the way collected data is classified in the UC Monitor database, Location and domain designations cannot be applied retroactively. Phone subnets that were already in the database when they were added to a Location definition will remain categorized as `<Unassigned>` in any historical data views, while being correctly placed in the Location in new views. Similar logic applies to the use of custom domains: those same subnets may be associated with custom domains when new calls are made, with no effect on data already collected.

When you create a custom domain in the CA NetQoS Performance Center, all Locations previously defined will continue to be associated with the Default Domain until you manually edit Locations to remove subnets, select the custom domain, and then add the subnets back to them. This manual procedure is often time-consuming. We recommend using the following workflow instead:

To change the domain assignment of multiple Location subnets:

1. Export the current list of Location definitions (**Administration > Data Collection > Locations**, click **Export**).
2. Check the exported `.csv` file to verify that its contents are as expected.
3. Delete all Location definitions: click **Administration > Data Collection > Locations**. Use **Click, Shift+Click** to select all Locations on a page. Then click **Delete**.
4. Import the `.csv` file, after selecting the new domain in Step 1 of the Import procedure (the **NPC Domain** parameter).

You will also need to select the new domain in the Collector Properties, as discussed in "Enabling Domain Monitoring at the Collector" on page 259.

Deleting Domain Groups

Like the associations between performance statistics and managed items, domain associations are stored along with items in the UC Monitor database. As a result, domains cannot simply be deleted from Unified Communications Monitor. If you delete domain groups, they are marked as inactive in Unified Communications Monitor and not exposed in reports that display new data. But if you then unregister the UC Monitor data source and register it again, it sends the domain group back up to the NetQoS Performance Center at the first synchronization because managed items in the UC Monitor database retain the association.

In most cases, the following workflow is recommended.

To delete a custom domain group definition:

1. Delete the domain group from the NetQoS Performance Center Groups tree.
2. Edit the Collector in UC Monitor Administration to change the NPC Domain assignment for the deleted domain group.

   Note: We recommend selecting another custom domain for the Collector. Otherwise, it will associate items with the Default Domain.

   Any data previously collected and associated with the deleted domain remains associated with it and is displayed as such in historical reports.

Trunk Groups and Voice Interfaces

Data from Cisco and Avaya trunk groups is reported in the Trunk Groups reports in the Capacity Planning section. Trunk groups are not identical to the other types of groups discussed in this appendix. And because of differences in the way they are monitored by the Collector, Avaya trunk groups are handled differently from Cisco trunk groups.

Note: The concept of trunk groups does not apply in a Microsoft-only environment.

The Collector discovers Avaya trunk groups for monitoring purposes by querying the Avaya Communication Manager using SNMP. The Communication Manager must be correctly configured to enable this polling. The steps are outlined in "Enabling SNMP Access" on page 69. You should also make sure that the Avaya trunk groups you want to monitor are listed in the "Trunk Group Measurement Selection" form that is maintained by the Communication Manager. The steps are provided in "Enabling Trunk Group Monitoring" on page 74.

By contrast, Cisco trunk groups can only be monitored as grouped items if you create them in the CA NetQoS Performance Center. Typically, users who want to monitor Cisco trunk groups create this type of structure by adding voice interfaces to groups, and using a naming convention to designate such groups as "trunk groups."

If you have upgraded the UC Monitor software from a previous version, you will need to specifically grant permission to view the Trunk Groups reports to each user who needs to be able to access these reports. Access to reports is granted by editing the user account role. Roles are not automatically allocated rights to view new reports after an upgrade.

Trunk Groups

Reporting per-trunk group is available for both Cisco and Avaya environments. However, performance and capacity data must be collected differently in each environment. As a result, a few configuration requirements apply to either case.

In an Avaya unified communications environment, trunk groups determine Avaya hardware requirements, including the type and number of required circuit packs and open ports, as well as voice gateway capacity and utilization, and are a required component of system setup. Their configuration is reported by the Communication Manager during SNMP polling by the Collector. The Communication Manager must therefore be configured to allow the Collector SNMP read-only polling access. And each trunk group must be enabled for monitoring at the Communication Manager. The necessary steps are provided in "Enabling SNMP Access" on page 69.

In a Cisco environment, trunk groups can provide a valuable means of reporting on capacity and utilization that reflects your actual usage and routing patterns.

Once the system is properly configured, the Collector receives data to identify trunk groups in the system and report their utilization and capacity. The two Trunk Group reports are automatically populated with data if at least one trunk group is detected.

Best Practices for Avaya Trunk Group Reporting

Avaya trunk group names are reported by the Avaya Communication Manager during SNMP polling by the Collector. Administrators typically use the defaults provided by the Communication Manager when using the Avaya Site Administration (ASA) interface to configure the system. This practice can easily lead to redundant trunk group names, which then appear identical in reports.

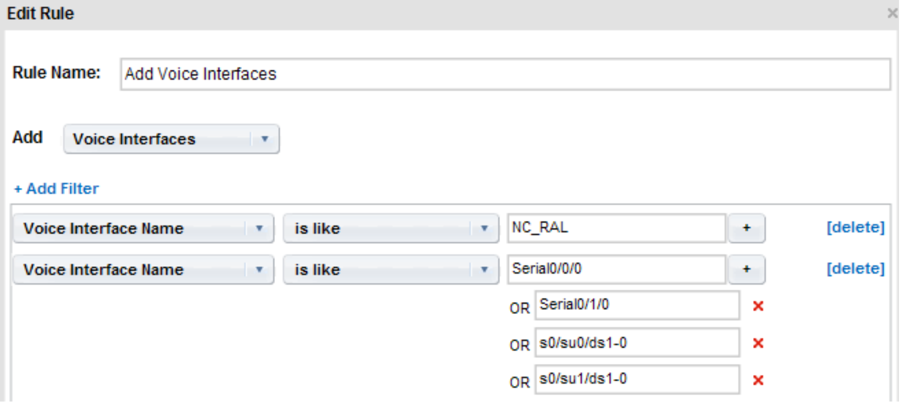
We recommend using the ASA interface to change the names and make each trunk group readily distinguishable in NetQoS Performance Center reports. If you decide to do this after monitoring has already begun, no report data is lost because internal identifiers are used to correlate the default names with the new ones.

Important: If you are monitoring items in custom domain groups, be aware that when you add a domain to a user account as a permission group, any Avaya trunk groups that were discovered by Collectors with that domain assignment are not included and must be added as individual permission groups. These trunk groups are treated as groups in the NetQoS Performance Center, as opposed to managed items, and groups do not have explicit domain identifiers.

Best Practices for Cisco Trunk Group Reporting

In a Cisco environment, trunk groups are not discovered from the call servers or from network traffic, but must instead be created as groups of voice interfaces in the CA NetQoS Performance Center. As you create these groups, be aware that the items known to the NetQoS Performance Center as "voice interfaces" are not placed in the same item type category as "interfaces," which are monitored by CA NetQoS ReporterAnalyzer and CA NetQoS NetVoyant. You can see them on the NetQoS Performance Center **Inventory** tab.

We recommend creating group rules that automatically place gateway voice interfaces into custom groups, which you designate—by means of a clear naming convention—as trunk groups. These special trunk groups can only contain items of the voice interface type. Here is an example of a rule that automatically adds voice interfaces on a Cisco voice gateway named NC_RAL to a custom group of voice interfaces named "NC_RAL Trunk Group":



Edit Rule

Rule Name: Add Voice Interfaces

Add: Voice Interfaces

+ Add Filter

Voice Interface Name — is like — NC_RAL — + — [delete]

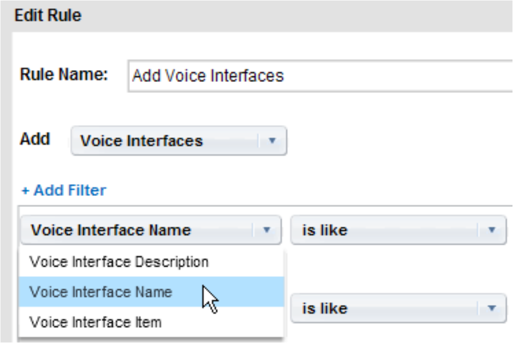
Voice Interface Name — is like — Serial0/0/0 — + — [delete]

OR Serial0/1/0

OR s0/su0/ds1-0

OR s0/su1/ds1-0

The interface for creating group rules provides a **Voice Interface** type that you can select from a list of items to add to the group automatically. Filtering provides further options to include items according to their name or description. And a **Voice Interface Item** option lets you filter by prior group membership. The following image illustrates the options that are typically useful for creating trunk group rules:



Edit Rule

Rule Name: Add Voice Interfaces

Add: Voice Interfaces

+ Add Filter

Voice Interface Name — is like

Cisco Administrators also need to periodically verify the voice interface capacity values being reported by voice gateway device MIBs. This information can be viewed on the UC Monitor Voice Gateway Properties page. The Voice Interface reports in the Capacity Planning section use the information shown in the **Channel Capacity** column of the Voice Interfaces list on that page to calculate interface utilization as a percentage of capacity. These reports are less accurate if the device MIB is incorrectly reporting the gateway voice channel capacity.

As a best practice, you should make sure that all known gateway voice interfaces have the number of channels correctly configured. The Collector typically can get this capacity information from polling the gateway. If it changes, however, this information is not updated in the device MIB. For the necessary steps to check Cisco voice interface capacity data, see "Editing a Gateway Voice Interface" on page 123.

You and other UC Monitor operators might see some unexpected items in reports if you do not proceed carefully with group creation and user account permission assignments. Specifically, try to avoid placing gateway voice interfaces in groups that you then copy into other group containers (that is, avoid making them subgroups). When you copy a group of interfaces and make it a subgroup, any operator with permission to view the *container* group can also see all its *subgroups*. As a result, that operator might see the same interface group listed twice in the Top Trunk Groups report: once where it appears in its own group, and once where it appears in its container group.

This behavior is unavoidable because the Trunk Group reports do not handle container groups the same way as trunk groups. Specifically, only the custom groups that (directly) contain at least one voice interface are identified as trunk groups. To the UC Monitor reporting interface, a voice interface that belongs to a trunk group and to a subgroup is included twice in the Top Trunk Groups report but does not appear to be a duplicate because only one instance is a member of a trunk group.

To avoid duplication of trunk groups in the Trunk Group reports, make sure trunk groups do not contain any items that are not voice interfaces. As soon as a non-voice interface item is detected, the group is no longer handled as a trunk group. And then either:

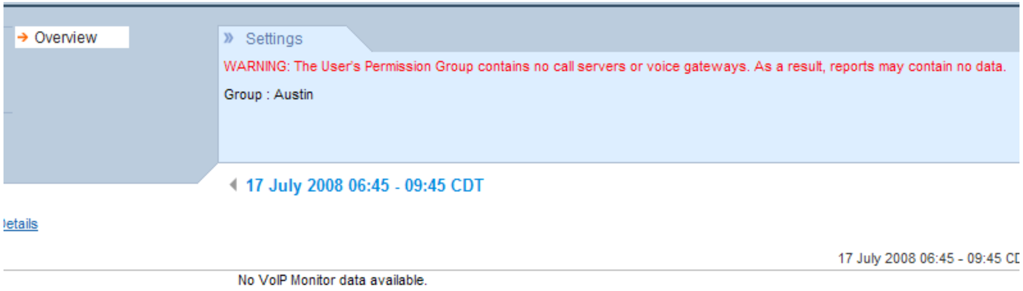
- Do not place trunk groups into container groups that you then copy into other positions in the Groups tree, or
- Be careful to assign permissions at the level of each specific trunk group, not above it, at the container level.

Working with the Grouping Feature

To organize your Locations, call servers, and media devices into groups, the main configuration tasks you will perform are creating new groups, editing these groups to add or remove members, and organizing groups into a logical structure. The following topics explain how to perform these tasks.

CA NetQoS Performance Center support for organizing managed items into hierarchical groups is a powerful feature that requires thoughtful planning and configuration. Grouping of items is an optional feature to help Administrators organize their reporting and maintain confidentiality of sensitive monitoring data. Be sure to read through this entire appendix before you begin creating groups and assigning permissions.

As you create groups and assign permissions to user accounts based on these group definitions, you need to be careful not to restrict UC Monitor operators from seeing the data they need to do their jobs. No checking is done to ensure that a given group definition is valid. For example, you might create a group that includes all Locations on the East Coast but neglect to add call servers carrying traffic to the phones in those Locations. In such a case, the group name would appear in UC Monitor reports but would never display any data. Users with this permission would instead see a warning similar to the following:



WARNING: The User's Permission Group contains no call servers or voice gateways. As a result, reports may contain no data.

Group : Austin

17 July 2008 06:45 - 09:45 CD

No VoIP Monitor data available.

The topic titled "Rearranging Group Structure" on page 267 contains some tips to help you plan your permission groups and assign valid permissions to user accounts.

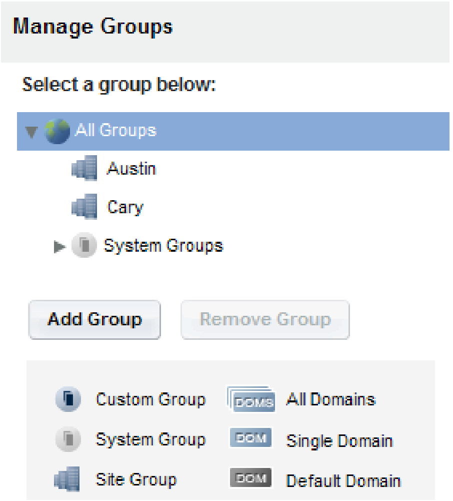
Creating Groups

New views providing a drilldown path from group names into data for individual group members are included in UC Monitor reports as soon as you define some groups and collect data from the associated managed items. Filtering of report data is also available at the group level by means of the Settings dialog boxes on report pages. The "UC Monitor Reports" chapter of the *UC Monitor User Guide* provides more information about these new views and drilldown paths.

To create groups of managed items for Unified Communications Monitor, these items must already be known to the CA NetQoS Performance Center. You must first use Unified Communications Monitor to create Location definitions, detect, create, or import voice gateway definitions, and detect any media devices and call servers you plan to include in groups. Any UC Monitor data source that is registered will automatically report these managed items to the NetQoS Performance Center, whose list of managed items is updated at each synchronization (every 5 minutes).

To create a new group of items:

1. In the CA NetQoS Performance Center, click **Admin > Groups**.
2. Create a new, empty group by selecting the **All Groups** icon at the top of the Groups tree and clicking the **Add Group** button below the tree.



3. The Add Group dialog box opens. You are prompted to supply a name for the new group.
4. (*Optional*) Type a description of the group in the **Description** field.
5. Leave the option to **Include the children of managed items** disabled (cleared). It does not apply to the present release of Unified Communications Monitor.
6. In the **Group Type** list, leave the default selection (**Custom**), or click to select **Site** if you are creating a Site group.
7. Click **Save** to save the new group.

   In the right pane (the Show Items pane), a message informs you that `No items were added to this group`.
8. At the bottom of the pane, click the **Add Item Type** button.

   Note: We recommend adding rules to your groups so that membership is updated automatically. Click the **Add Rule** button to add a rule. See "Creating Permission Groups" on page 252 or the NetQoS Performance Center online Help for more information about group rules.
9. The Add Items dialog box displays lists of managed items. The menu lets you select the type of item to add to the group. For a group of VoIP Locations and associated devices:
   - Click **Devices** to add call servers and media devices to the group.
   - Click **VoIP Locations** to add Locations to the group.

   By default, all managed items of the selected item type, from all data sources, are listed, along with their properties. All VoIP managed items are either Devices or VoIP Locations. Columns can be sorted by clicking column titles.
10. Click to select item check boxes, and then click **Add Items**.
11. When you have finished selecting all the members that you want to add to the group, click **Close** to save the changes to the group.

Important: For Unified Communications Monitor, groups that contain at least one call server, in addition to associated VoIP Locations, are the only valid permission groups. Without call servers, a group will not display data in reports.

The new group appears in the Groups tree in the left pane. If you change your mind, remove a member from a group by selecting its check box and clicking the **Remove Devices** link.

The NetQoS Performance Center Manage Groups page lets you edit the groups you've created. When you edit a group, you can change the group's name or description, change the option to include child items, remove group members, or add new members. You'll need to edit groups when you add a new UC Monitor data source to the CA NetQoS Performance Center, add new Locations to a data source, or when new call servers come online, for example. The changes are sent down to the data source at the next synchronization.

You can modify groups by adding subgroups, or by copying and pasting existing subgroups into multiple groups. See the following topic, "Rearranging Group Structure" on page 267, for more information.

Rearranging Group Structure

The topic titled "Creating Groups" on page 265 describes how to create a new group under the **All Groups** heading in the Groups tree. The steps outlined in that topic result in the creation of a new first-level group. To reflect the structure of your enterprise geography or IT organization, you might want to create subgroups within your first-level groups. For example, your IT organization might consist of East Coast and West Coast divisions. You could begin by creating two first-level groups: East Coast and West Coast. As a next step, you could create subgroups within the East Coast group:

- Maryland
- Massachusetts
- North Carolina

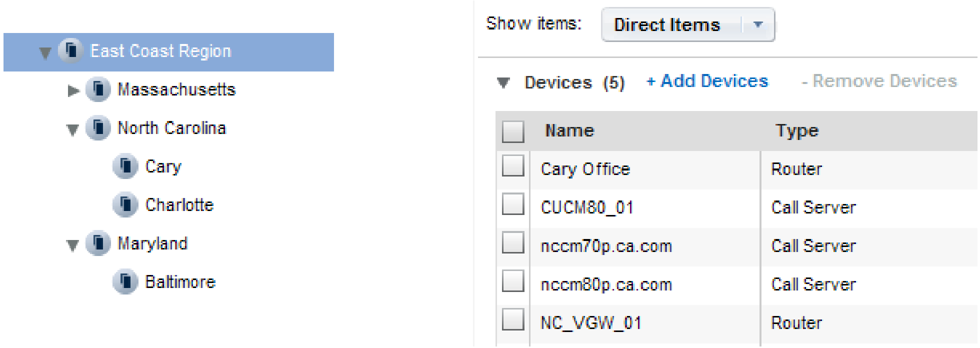
Within each subgroup, you could create more subgroups. Or you could add devices and Locations to these subgroups. Both groups and subgroups can contain items, subgroups, or both.

As you create your grouping structure, keep the following tips in mind:

- Plan carefully when placing devices in groups. To give a UC Monitor operator permission to view data about the Raleigh, NC Location, for example, you must also give that operator permission to view data from the call server being used by the phones in that Location. When you assign the permission group, the user needs permission to access both the Raleigh Location and its call servers.

  Important: Permission to view the Location itself does not suffice.

- We recommend adding call servers and media devices to top-level groups, with associated Locations in custom subgroups underneath them. Here's an example of valid grouping structure:



□ Name	Type
□ Cary Office	Router
□ CUCM80_01	Call Server
□ nccm70p.ca.com	Call Server
□ nccm80p.ca.com	Call Server
□ NC_VGW_01	Router

In this example, the East Coast Region group is at the top level of the tree. As shown in the above image, it contains all the call server devices—along with some voice gateways, which are not required group members—necessary to provide access to call data in all the subgroups of the East Coast group. The subgroups contain the Locations and are all placed at lower levels in the hierarchy. The permission group should be assigned at the "East Coast Region" level in the tree, not on a lower node.

- For Monitoring and Capacity Planning reports, permissions are based on receiving Locations. It is therefore possible to grant a user view permissions that result in the exclusion of half the call data from certain calls in these report views.

  For example, a UC Monitor user's permissions may allow her to see data for the managed items in the North Carolina, Massachusetts, and Maryland groups. However, when she drills down into data for the Raleigh, NC Location, she will not be able to see some of the data for calls made from Raleigh to Dallas and vice versa because Dallas is in a subgroup of the group named "Southwest Region". Call quality and call setup data will still be available for those calls, but in the associated Call Leg Details report, she will only see table entries for call data sent toward the Raleigh Location.

  Permissions for Troubleshooting reports work differently. An operator with permission to view data from any watched call will be allowed to view all data for that call.

- If you are not completely familiar with the logical organization of some subnets in your enterprise, you might want to wait a week or so after installing the UC Monitor system and creating the Location definitions before you place Locations and devices in groups. Give the system time to collect some data so that you can fully understand which call servers and gateway media devices are being used at each Location or Site. You will then be able to create groups and assign the appropriate permissions to allow UC Monitor operators to view all the data they need to do their jobs.

- Decide early in the process whether you want to create a grouping structure based on geography or based on an organizational chart. Once you've created first-level nodes, CA NetQoS Performance Center does not support separate geographical and organizational trees.

- We recommend creating group containers first and making sure you are satisfied with grouping structure before you begin adding items to groups.

- Once you have created a group and added members to it, you cannot copy or move the group *members* to another group to create a subgroup. You can, however, remove the members, create a new subgroup, and add the members to it. Or you can copy an entire first-level *group* into another first-level group to create a subgroup. The necessary procedure follows.

To move a first-level group into another group:

1. In the CA NetQoS Performance Center, click **Admin > Groups**.
2. In the Groups tree, find the group you want to move.
3. Right-click the group name, and select **Copy Group**.
4. Click the group where you want to place the first-level group as a subgroup.
5. Right-click, and select **Paste Group**.

The group reference is displayed as a new subgroup that looks identical to the original group that you copied. The same group can exist in multiple places within the hierarchy in the Groups tree.

Index

CA NetQoS Main Office
5001 Plaza on the Lake
Austin, TX 78746
tel: 512.776.0042
800.225.5224
fax: 512.776.0010

www.ca.com