CA Unified Communications Monitor

Use Cases for Managing Thresholds

Version 3.5

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

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Creating and Assigning Call Setup Thresholds

UC Monitor thresholds define the boundaries of acceptable performance. Call setup thresholds trigger incident actions (email, SNMP traps, or traceroutes) in response to poor call setup metrics, such as excessive delay to dial tone.

By creating call setup thresholds and assigning them to Locations and media devices, you can determine the manner and frequency with which UC Monitor responds to performance conditions in your unified communications system.

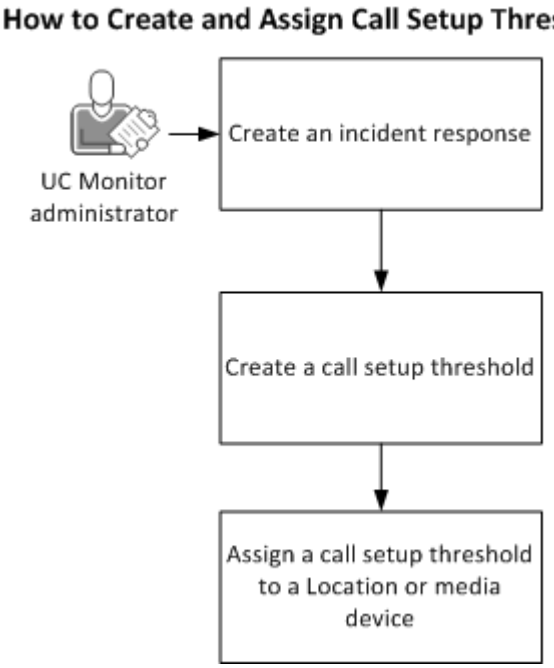
This use case shows UC Monitor administrators how to perform the following tasks:

- Create a custom incident response.
- Create a call setup threshold, which includes the incident response.
- Assign a threshold to Locations or media devices.

This section contains the following topics:

Overview

The following diagram illustrates the process for creating incident responses, and for creating and assigning call setup thresholds:



The following topics describe how to create incident responses, and how to create and assign call setup thresholds:

- Create an incident response (see page 9).
- Create a call setup threshold (see page 11).
- Assign a call setup threshold to a Location or media device (see page 13).

Prerequisites

This use case assumes the following:

- You created Location definitions, or UC Monitor discovered at least one voice gateway or other media device. For information about defining Locations, see the online help or the use case titled *Creating Location Definitions* in the CA Unified Communications Monitor bookshelf on CA Support Online.
- You identified the SMTP server on the Console Settings page in the management console. For more information, click Administration, Console, Settings in the navigation bar, and then click Help.

Create an Incident Response

You can configure different responses for each Location, for each media device, for each call server or call server group, or for pairs of Locations or media devices. You then associate the responses with the different thresholds for call quality, call setup, or call server incidents.

You can associate an incident response with more than one action.

Note: UC Monitor provides one default incident response, Default, which is not associated with an action.

Follow these steps:

1. Click Administration, Policies, Incident Responses in the navigation bar.

   The Incident Response List opens.

2. Click New to create an incident response.

   The Incident Response Properties page opens.

3. Type a name for the incident response in the Name field. The name helps you identify the response in the list of responses on the Threshold Properties page.

4. Click New to add an action.

   The Add Action to Incident Response page opens.

5. Select the Action Type, which determines the other selections on this page:

   - **Send Email**. Supply the email address of the person to notify when the associated threshold is violated. You can specify multiple email addresses, separated by commas or semicolons.
   - **Send SNMP Trap**. Supply parameters to send an SNMP trap to a third-party network monitoring operating environment.
   - **Launch Traceroute Investigation**. Lets you run an automatic traceroute to collect extra data about routing from the affected Location or voice gateway. The Launch Traceroute Investigation action is designed for call setup and call server group incidents only.

6. Set the Minimum Conditions for Taking Action:

   - **Severity**. Select the threshold severity level that can trigger this action when crossed: degraded or excessive. 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. Incidents of these types always have a severity of “excessive.”
   - **Duration**. Select the interval during which a monitored metric must violate the threshold before the action is launched. Use this option to launch actions either more or less quickly in response to threshold violations.

     For example, select 30 minutes to launch an action when latency exceeds the threshold during a 30-minute interval. It does not matter how many times during the interval that the threshold is crossed. It matters only that the condition still exists at the end of the selected duration.

7. Set the parameters that control the recipient and format of the notification. The available parameters vary depending on the selected Action Type:

   - **Recipients**. Provide the full email address of the person to receive an automatic email notification about this type of incident. Select someone who is most likely to respond quickly and accurately to remedy the problem that caused the incident. You can specify multiple email addresses, separated by commas or semicolons.
   - **Send SNMP Trap to**. The IP address or host name of the computer to receive the SNMP trap.

     Note: UC Monitor includes a MIB file that contains unique OIDs. You can import them into your trap receiver. The file is located in the following directory on the management console:

     `<install path>\CA\VoIPMonitor\MIB\NETQOS-VMTRAP-MIB.txt`

     Tip: To send a trap to more than one computer, create additional actions within the same response, one for each additional trap destination.
   - **Send Test Trap**: Click to send a trap to the IP address you entered in the "Send SNMP Trap to" field. Results of the test appear at the top of the Add Action to Incident Response page.
   - **Severity Updates**. Select when to send SNMP traps:
     - **Send update traps when Incident severity changes**. Send an SNMP trap if the incident severity changes, but the incident remains open. Also send an SNMP trap when a new incident is opened.
     - **Send only Incident open and close traps**. Send an SNMP trap only if a new incident is opened or if an incident is closed.

       Note: Some incident types do not have a severity parameter, such as the Poor Call Quality incident, or their severity is always excessive. The option to send only open and close traps is always used for these incidents.
   - **SNMP Profile**. Select the SNMP profile to use for the trap.

- **Time Zone**. Select the time zone of the recipient. The default time zone corresponds to the locale where the management console is installed.

8. Click OK.

   The action appears on the Incident Response Properties page.

9. Save the response:

   - Click Save to save the response and return to the Incident Response List.
   - Click Save & Add Another to save the response and create another response.

   You can now associate the incident response with a threshold.

Create a Call Setup Threshold

Call setup thresholds trigger incidents in response to poor call setup, such as excessive delay to dial tone.

A call setup threshold includes degraded and excessive severity settings for each metric that is monitored.

Follow these steps:

1. Click Administration, Policies, Call Performance, Call Setup Thresholds in the navigation bar.

   The Call Setup Threshold List opens.

2. Click New.

   The Call Setup Threshold Properties page opens.

3. Provide a name for the custom threshold in the Name field.

4. Select an incident response from the Incident Response field. The response is launched when the threshold is violated. The incident response you created appears in this field.

5. (*Optional*) Describe the threshold in the Description field. For example, the description can indicate which Locations or media devices are assigned these custom settings, or why a particular metric has a higher threshold.

6. Set threshold values for the following metrics:
   - **Delay to Dial Tone**. The default values are 2000 milliseconds for the degraded threshold, 4000 milliseconds for the excessive threshold, and a minimum of five calls.
   - **Post Dial Delay**. The default values are 2000 milliseconds for the degraded threshold, 4000 milliseconds for the excessive threshold, and a minimum of five calls.
   - **Call Setup Failures**. The default values are 2 percent for the degraded threshold, 10 percent for the excessive threshold, and a minimum of five calls.

     Note: Threshold values are not inclusive. Metrics must exceed a threshold to create an incident. For example, based on the default values, a delay to dial tone of 2000 milliseconds does not launch an incident. A delay to dial tone of 2001 milliseconds does launch an incident.
7. Select Milliseconds or Percentage as the unit of measure, or select None to disable the degraded threshold or excessive threshold. Disabling thresholds is not recommended.
8. Set values for the units of measure. The value for the excessive threshold must be larger than the value for the degraded threshold. The larger value indicates more severe delay or more setup failures.
9. (*Optional*) Provide a value in the Minimum Calls Originated field. This value sets a minimum number of calls that must be initiated during a monitoring interval before an incident is created.
   Note: Set a lower value in the Minimum Calls Originated field to see incidents more quickly in response to poor call setup performance. Set a higher value to see incidents more slowly, after more data is collected.
10. Save the threshold:
    - Click Save to save the threshold and return to the Call Setup Threshold List. The threshold appears in the list.
    - Click Save & Add Another to save the threshold and create another threshold.

    You can now assign the threshold to a Location or a media device.

Assign a Call Setup Threshold

During call monitoring, call setup thresholds are applied to the Locations or devices from which calls are made. You can assign the same call setup threshold to multiple Locations or media devices. You cannot assign call setup thresholds to groups.

Follow these steps:

1. Click Administration, Policies, Call Performance, Call Setup Threshold Assignments in the navigation bar.

   The Call Setup Threshold Assignment List opens.

2. Click New.

   The Call Setup Threshold Assignment Properties page opens. The Available Locations/Media Devices list displays all Locations and media devices that have not been assigned to a threshold.

   Note: Two call setup threshold metrics do not apply to Microsoft media devices: Delay to Dial Tone and Post Dial Delay.

3. Select a threshold to assign from the Threshold list.

4. Double-click an item in the Available Locations/Media Devices list to move it to the Selected list.

   Tip: The Filter field accepts wildcard (*) search strings to limit the data shown in the list. For a string with no asterisks, the Filter field assumes wildcards (for example, “*abc*”) when it searches. Filtering can be useful when you have a long list of Locations and media devices. For example, to see only items for the Raleigh office, enter **ral** for the filter and click Apply. Only items whose name begins with Ral are shown in the list.

5. Save the assignment:

   - Click Save to save the assignment and return to the Call Setup Threshold Assignment List. The new assignment appears in the list.
   - Click Save & Add Another to save the assignment and assign another threshold.

   The threshold is now applied to the Location or media device you selected.

Chapter 2: Creating and Assigning Call Quality Thresholds

UC Monitor thresholds define the boundaries of acceptable performance. Call quality thresholds trigger incidents in response to poor call quality, such as low MOS, and poor video quality, such as video packet loss.

By creating call quality thresholds and assigning them to pairs of Locations and media devices, you can determine the manner and frequency with which UC Monitor responds to performance conditions in your unified communications system.

This use case shows UC Monitor administrators how to perform the following tasks:

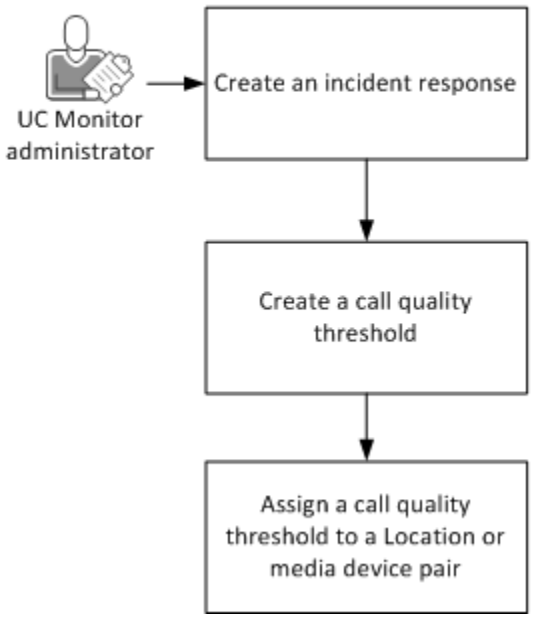
- Create a custom incident response.
- Create a call quality threshold, which includes the incident response.
- Assign the threshold to pairs of Locations or media devices.

This section contains the following topics:

Overview

The following diagram illustrates the process for creating incident responses, and for creating and assigning call quality thresholds:

How to Create and Assign Call Quality Thresholds



The following topics describe how to create incident responses, and how to create and assign call quality thresholds:

- Create an incident response (see page 9).
- Create a call quality threshold (see page 19).
- Assign a call quality threshold to a Location or media device pair (see page 21).

Prerequisites

This use case assumes the following:

- You created Location definitions, or UC Monitor discovered at least one voice gateway or other media device. For information about defining Locations, see the online help or the use case titled *Creating Location Definitions* in the CA Unified Communications Monitor bookshelf on CA Support Online.
- You identified the SMTP server on the Console Settings page in the management console. For more information, click Administration, Console, Settings in the navigation bar, and then click Help.

Create an Incident Response

You can configure different responses for each Location, for each media device, for each call server or call server group, or for pairs of Locations or media devices. You then associate the responses with the different thresholds for call quality, call setup, or call server incidents.

You can associate an incident response with more than one action.

Note: UC Monitor provides one default incident response, Default, which is not associated with an action.

Follow these steps:

1. Click Administration, Policies, Incident Responses in the navigation bar.

   The Incident Response List opens.

2. Click New to create an incident response.

   The Incident Response Properties page opens.

3. Type a name for the incident response in the Name field. The name helps you identify the response in the list of responses on the Threshold Properties page.

4. Click New to add an action.

   The Add Action to Incident Response page opens.

5. Select the Action Type, which determines the other selections on this page:

   - **Send Email**. Supply the email address of the person to notify when the associated threshold is violated. You can specify multiple email addresses, separated by commas or semicolons.
   - **Send SNMP Trap**. Supply parameters to send an SNMP trap to a third-party network monitoring operating environment.
   - **Launch Traceroute Investigation**. Lets you run an automatic traceroute to collect extra data about routing from the affected Location or voice gateway. The Launch Traceroute Investigation action is designed for call setup and call server group incidents only.

6. Set the Minimum Conditions for Taking Action:

   - **Severity**. Select the threshold severity level that can trigger this action when crossed: degraded or excessive. 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. Incidents of these types always have a severity of “excessive.”
   - **Duration**. Select the interval during which a monitored metric must violate the threshold before the action is launched. Use this option to launch actions either more or less quickly in response to threshold violations.

     For example, select 30 minutes to launch an action when latency exceeds the threshold during a 30-minute interval. It does not matter how many times during the interval that the threshold is crossed. It matters only that the condition still exists at the end of the selected duration.

7. Set the parameters that control the recipient and format of the notification. The available parameters vary depending on the selected Action Type:

   - **Recipients**. Provide the full email address of the person to receive an automatic email notification about this type of incident. Select someone who is most likely to respond quickly and accurately to remedy the problem that caused the incident. You can specify multiple email addresses, separated by commas or semicolons.
   - **Send SNMP Trap to**. The IP address or host name of the computer to receive the SNMP trap.

     Note: UC Monitor includes a MIB file that contains unique OIDs. You can import them into your trap receiver. The file is located in the following directory on the management console:

     `<install path>\CA\VoIPMonitor\MIB\NETQOS-VMTRAP-MIB.txt`

     Tip: To send a trap to more than one computer, create additional actions within the same response, one for each additional trap destination.
   - **Send Test Trap**: Click to send a trap to the IP address you entered in the "Send SNMP Trap to" field. Results of the test appear at the top of the Add Action to Incident Response page.
   - **Severity Updates**. Select when to send SNMP traps:
     - **Send update traps when Incident severity changes**. Send an SNMP trap if the incident severity changes, but the incident remains open. Also send an SNMP trap when a new incident is opened.
     - **Send only Incident open and close traps**. Send an SNMP trap only if a new incident is opened or if an incident is closed.

       Note: Some incident types do not have a severity parameter, such as the Poor Call Quality incident, or their severity is always excessive. The option to send only open and close traps is always used for these incidents.
   - **SNMP Profile**. Select the SNMP profile to use for the trap.

- **Time Zone**. Select the time zone of the recipient. The default time zone corresponds to the locale where the management console is installed.

8. Click OK.

   The action appears on the Incident Response Properties page.

9. Save the response:

   - Click Save to save the response and return to the Incident Response List.
   - Click Save & Add Another to save the response and create another response.

   You can now associate the incident response with a threshold.

Create a Call Quality Threshold

A call quality threshold includes degraded and excessive severity settings for each metric that is monitored. Threshold properties include a unique name for the custom settings, an incident response, and an optional description of the settings.

Threshold values are not inclusive. Metrics must exceed a threshold to create an incident. For example, based on the default values, latency of 150 milliseconds does not launch an incident. Latency of 151 milliseconds does launch an incident.

Follow these steps:

1. Click Administration, Policies, Call Performance, Call Quality Thresholds in the navigation bar.

   The Call Quality Threshold List opens.

2. Click New.

   The Call Quality Threshold Properties page opens.

3. Provide a name for the custom threshold in the Name field.

4. Select an incident response from the Incident Response field. This response is launched when the threshold is violated. The response you created appears in this list.

5. (*Optional*) Briefly describe the threshold in the Description field. The description can indicate which pairs of Locations and media devices are assigned the threshold, for example.

6. Select a unit of measure for the MOS and Network MOS metrics, or select None to disable the threshold:

   - **MOS**: Select this option to monitor call quality that is based on a fixed MOS value for the degraded and excessive thresholds.
   - **Codec**: Select this option to monitor call quality that is based on the codec that is detected during call monitoring. UC Monitor uses the degraded and excessive thresholds for the detected codec. Codec is the default unit of measure.

     Note: For information about setting codec thresholds, see the use case titled Understanding and Managing Codec Thresholds in the CA Unified Communications Monitor bookshelf on CA Support Online.

7. Select Milliseconds, Percentage, or Decibel (dB) as the unit of measure for the remaining audio and video metrics, or select None to disable the threshold. Disabling thresholds is not recommended.
8. Provide a value for the units of measure. The value for the excessive threshold must be larger than the degraded threshold value.
9. Provide a new value in the Minimum Calls Minutes field. This value sets the minimum amount of time that a metric can cross the threshold during a monitoring interval before an incident is created. The following list describes the default values for each field.

   - **MOS and Network MOS**: The default values are 4.03 for the degraded MOS threshold, 3.6 for the excessive MOS threshold, and a minimum of 15 call minutes.
   - **Packet Loss** and **Jitter Buffer Loss**: The default values are 1 percent for the degraded threshold, 5 percent for the excessive threshold, and a minimum of 15 call minutes.
   - **Latency** and **Video Latency**: The default values are 150 milliseconds for the degraded threshold, 400 milliseconds for the excessive threshold, and a minimum of 15 call minutes.
   - **ACOM**: The default values are 15 dB for the degraded threshold, 6 dB for the excessive threshold, and a minimum of 15 call minutes.

- **Frozen Video**, **Video Frame Loss**, and **Video Packet Loss**: The default values are 1 percent for the degraded threshold, 5 percent for the excessive threshold, and a minimum of 15 call minutes.

  Tip: Set a lower value for the Minimum Call Minutes field to see incidents more quickly in response to poor call quality performance. Set a higher value to see incidents more slowly, after more data is collected.

10. Save the threshold:

    - Click Save to save the threshold and return to the Call Quality Threshold List. The new threshold appears in the list.
    - Click Save & Add Another to save the threshold add another custom threshold.

    You can now assign the threshold to a Location or a media device.

Assign a Call Quality Threshold

VoIP and video call performance occurs between pairs of related endpoints. Therefore, you want to understand the call quality data that is reported for paired network locations. By default, the Default call quality threshold is assigned to all pairs of Locations and media devices. In addition, you can assign custom call quality thresholds to selected pairs of Locations and media devices:

- Pairs of Locations to include all computers in the relevant Location subnets
- Pairs of media devices
- Pairs that consist of a Location and a media device

You can assign the same call quality thresholds to multiple pairs, such as all Locations in one geographical region of your enterprise. You cannot assign call quality thresholds to CA Performance Center groups.

Follow these steps:

1. Click Administration, Policies, Call Performance, Call Quality Threshold Assignments in the navigation bar.

   The Call Quality Threshold Assignment List opens.

2. Click New.

   The Call Quality Threshold Assignment Properties page opens. The Available Locations/Media Device Pairs list displays all Locations and media devices that have not been assigned to a threshold.

3. Select the threshold that you want to assign from the Threshold field.

4. (*Optional*) Select IP Domain if you are monitoring an environment with multiple custom IP domains.

   The Available Locations/Media Device Pairs list is filtered to show only pairs of Locations and media devices from the selected domain.

5. Select an item in the Available Locations/Media Device Pairs list.

   The Filter field accepts wildcard (*) search strings to limit the data in the list. For a string with no asterisks, the Filter field assumes wildcards (for example, “*abc*”) when it searches. Filtering can be useful when you have a long list of Locations and media devices.

   For example, to see only items for the Raleigh office, enter **ral** for the filter and click Apply. Only items whose name begins with Ral are shown in the list.

6. Double-click the item in the Available list to move it to the Selected Location/Media Device Pairs list.

   Tip: You can use the Shift or Control key or click and drag with the left mouse button to select multiple items. Then click the Right arrow to move the items to the Selected list.

7. Save the assignment.

   - Click Save to save the assignment and return to the Call Quality Threshold Assignment List. The new assignment appears in the list.
   - Click Save & Add Another to save the assignment and assign another threshold.

   The threshold is now applied to the Locations and media devices you selected.

Chapter 3: Creating and Assigning Call Server Thresholds

UC Monitor thresholds define the boundaries of acceptable performance. Call server thresholds trigger incidents in response to registration failures and poor call quality (the Cisco QRT feature), based on information in the Phone Details reports. For example, when a Registration Failures incident is reported, multiple endpoints in the Phones report have a status of Registration Failed.

By creating call server thresholds and assigning them to individual call servers, you can determine the manner and frequency with which UC Monitor responds to registration failures and poor call quality conditions in your Cisco Unified Communications Manager system.

This use case shows UC Monitor administrators how to perform the following tasks:

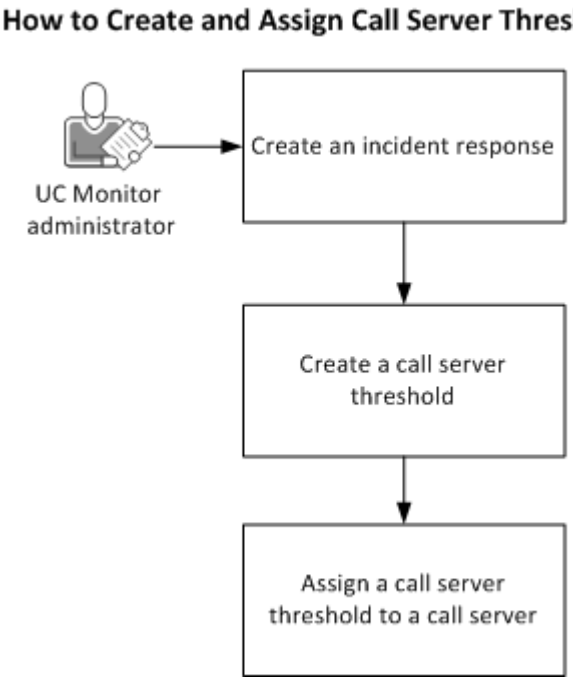
- Create a custom incident response.
- Create a call server threshold, which includes the incident response.
- Assign a threshold to one or more call servers.

Note: Call server thresholds apply only to Cisco Unified Communications Manager environments.

This section contains the following topics:

Overview

The following diagram illustrates the process for creating and assigning call server thresholds:



The following topics describe the process for creating and assigning call server thresholds:

- Create an incident response (see page 9).
- Create a call server threshold (see page 28).
- Assign a call server threshold to a call server (see page 29).

Understanding Call Server Thresholds

The call server threshold consists of the following metrics, each of which has its own threshold values.

Registration Failures threshold

The Registration Failures threshold creates an incident when devices repeatedly, but unsuccessfully, try to register with a call server. Excessive registration failures can indicate a configuration problem, a call server issue, or a security problem that can impede server performance. When an endpoint tries to register from an unauthorized address, the call server ultimately denies the request. The call server responds to every registration request. Therefore, excessive registrations consume bandwidth and tie up the call server while it tries to resolve device addresses and process requests.

Poor Call Quality threshold

The Poor Call Quality threshold is based on the Quality Report Tool (QRT), a feature of some Cisco IP telephone models. The QRT allows users to press a key during or after a call to report poor call quality. When the key is pressed, the QRT collects information useful for troubleshooting the poor performance from various sources. The QRT then formats the information and sends it to its call server. The call server places the information in a call detail record.

The Poor Call Quality threshold creates an incident when a user presses the QRT key. When a Poor Call Quality incident is reported, a Phone Details table is available from the Incidents Overview report. The Phone Details table shows call legs for the 15 minutes before the QRT key was pressed and identifies the associated telephone.

Create an Incident Response

You can configure different responses for each Location, for each media device, for each call server or call server group, or for pairs of Locations or media devices. You then associate the responses with the different thresholds for call quality, call setup, or call server incidents.

You can associate an incident response with more than one action.

Note: UC Monitor provides one default incident response, Default, which is not associated with an action.

Follow these steps:

1. Click Administration, Policies, Incident Responses in the navigation bar.

   The Incident Response List opens.

2. Click New to create an incident response.

   The Incident Response Properties page opens.

3. Type a name for the incident response in the Name field. The name helps you identify the response in the list of responses on the Threshold Properties page.

4. Click New to add an action.

   The Add Action to Incident Response page opens.

5. Select the Action Type, which determines the other selections on this page:

   - **Send Email**. Supply the email address of the person to notify when the associated threshold is violated. You can specify multiple email addresses, separated by commas or semicolons.
   - **Send SNMP Trap**. Supply parameters to send an SNMP trap to a third-party network monitoring operating environment.
   - **Launch Traceroute Investigation**. Lets you run an automatic traceroute to collect extra data about routing from the affected Location or voice gateway. The Launch Traceroute Investigation action is designed for call setup and call server group incidents only.

6. Set the Minimum Conditions for Taking Action:

   - **Severity**. Select the threshold severity level that can trigger this action when crossed: degraded or excessive. 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. Incidents of these types always have a severity of “excessive.”
   - **Duration**. Select the interval during which a monitored metric must violate the threshold before the action is launched. Use this option to launch actions either more or less quickly in response to threshold violations.

     For example, select 30 minutes to launch an action when latency exceeds the threshold during a 30-minute interval. It does not matter how many times during the interval that the threshold is crossed. It matters only that the condition still exists at the end of the selected duration.

7. Set the parameters that control the recipient and format of the notification. The available parameters vary depending on the selected Action Type:

   - **Recipients**. Provide the full email address of the person to receive an automatic email notification about this type of incident. Select someone who is most likely to respond quickly and accurately to remedy the problem that caused the incident. You can specify multiple email addresses, separated by commas or semicolons.
   - **Send SNMP Trap to**. The IP address or host name of the computer to receive the SNMP trap.

     Note: UC Monitor includes a MIB file that contains unique OIDs. You can import them into your trap receiver. The file is located in the following directory on the management console:

     `<install path>\CA\VoIPMonitor\MIB\NETQOS-VMTRAP-MIB.txt`

     Tip: To send a trap to more than one computer, create additional actions within the same response, one for each additional trap destination.
   - **Send Test Trap**: Click to send a trap to the IP address you entered in the "Send SNMP Trap to" field. Results of the test appear at the top of the Add Action to Incident Response page.
   - **Severity Updates**. Select when to send SNMP traps:
     - **Send update traps when Incident severity changes**. Send an SNMP trap if the incident severity changes, but the incident remains open. Also send an SNMP trap when a new incident is opened.
     - **Send only Incident open and close traps**. Send an SNMP trap only if a new incident is opened or if an incident is closed.

       Note: Some incident types do not have a severity parameter, such as the Poor Call Quality incident, or their severity is always excessive. The option to send only open and close traps is always used for these incidents.
   - **SNMP Profile**. Select the SNMP profile to use for the trap.
   - **Time Zone**. Select the time zone of the recipient. The default time zone corresponds to the locale where the management console is installed.

8. Click OK.

   The action appears on the Incident Response Properties page.

9. Save the response:

   - Click Save to save the response and return to the Incident Response List.
   - Click Save & Add Another to save the response and create another response.

   You can now associate the incident response with a threshold.

Create a Call Server Threshold

Call server thresholds trigger incidents in response to registration failures and poor call quality (the Cisco QRT feature), based on information in the Phone Details reports.

When you create a call server threshold, you select the incident response to launch when the threshold is violated.

Follow these steps:

1. Click Administration, Policies, Call Servers, Call Server Thresholds in the navigation bar.

   The Call Server Threshold List opens.

2. Click New.

   The Call Server Threshold Properties page opens.

3. Provide a name for the threshold in the Name field.

4. Select an incident response from the Incident Response field. This incident is launched when the threshold is violated. The incident response you created appears in this list.

5. (*Optional*) Briefly describe the threshold in the Description field. The description can indicate which server is assigned these custom settings, or why a particular metric has a higher threshold, for example.

6. Set the values for the Registration Failures threshold:

   - Accept Number as the unit of measure, or select None to disable the threshold. Disabling thresholds is not recommended.
   - Provide a value for the unit of measure. This value sets the minimum number of registration failures that can occur during a monitoring interval before an incident is created.

   Note: The default value for a Registration Failures threshold is 15 failures per reporting interval. The severity is always excessive.

7. Enable the Poor Call Quality (QRT) threshold, or select None to disable the threshold. Disabling thresholds is not recommended.

   Note: The Poor Call Quality threshold is enabled by default, and its severity is always excessive.

8. Save the threshold:

   - Click Save to save the threshold and return to the Call Server Threshold List.
   - Click Save & Add Another to save the threshold and create another threshold.

   The threshold is saved and can be assigned to one or more call servers. Your changes are applied to the next data-collection interval. Data that is already collected is not reevaluated with the new settings.

Assign a Call Server Threshold to a Call Server

The Default call server threshold is applied to all call servers when the call servers are discovered during monitoring. However, you can assign custom call server thresholds to selected call servers. You can assign a threshold to multiple call servers.

Follow these steps:

1. Click Administration, Policies, Call Servers, Call Server Threshold Assignments in the navigation bar.

   The Call Server Threshold Assignment List opens.

2. Click New.

   The Call Server Threshold Assignment Properties page opens. The Available Call Servers list displays all call servers that have not been assigned to a customized threshold.

3. Select the threshold that you want to assign from the Threshold field.

4. Select a call server in the Available Call Servers list.

   The Filter field accepts wildcard (*) search strings to limit the data shown in the list. For strings with no asterisks, the Filter field assumes wildcards (for example, “*abc*”) when it searches. Filtering can be useful when you have a long list of call servers.

   For example, to see only items for the Raleigh office, enter **ral** for the filter and click Apply. Only items whose name begins with Ral are shown in the list.

5. Double-click the call server in the Available list to move it to the Selected Call Servers list.

   Tip: You can use the Shift or Control key or click and drag with the left mouse button to select multiple items. Then click the Right arrow to move the items to the Selected list.

6. Save the assignment:

   - Click Save to save the assignment and return to the Call Server Threshold Assignment List.
   - Click Save & Add Another to save the assignment and assign another threshold.

   The threshold is now applied to the call servers you selected.

Chapter 4: Creating and Assigning Call Server Group Thresholds

UC Monitor thresholds define the boundaries of acceptable performance. Call server group thresholds trigger incidents in response to changes in phone status, such as missing, moved, or new phones.

Call server group thresholds are designed to be applied to your Cisco call server clusters, or to other logical groupings of call servers. Each call server in a cluster can play several different roles to provide failover safeguards and load balancing. The call server group thresholds apply to all call servers in a cluster.

By creating call server group thresholds and assigning them to your Cisco call server clusters, you can determine the manner and frequency with which UC Monitor responds to status changes in your unified communications system.

This use case shows UC Monitor administrators how to perform the following tasks:

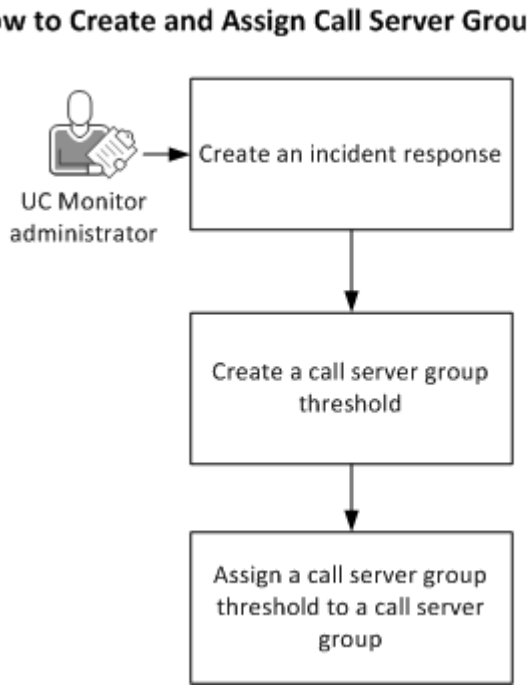
- Create a custom incident response.
- Create a call server group threshold, which includes the incident response.
- Assign a threshold to call server clusters or other logical groupings of call servers.

Note: Call server group thresholds apply only to Cisco Unified Communications Manager environments.

This section contains the following topics:

Overview

The following diagram illustrates the process for creating and assigning call server group thresholds.



The following topics describe the process for creating and assigning call server group thresholds.

- Create an incident response (see page 9).
- Create a call server group threshold (see page 36).
- Assign a call server group threshold to a call server group (see page 37).

Prerequisites

This use case assumes you created at least one call server group that contains at least one Cisco call server. For information about creating call server groups, see the online help or the use case titled *Creating Call Server Groups* in the CA Unified Communications Monitor bookshelf on CA Support Online.

Understanding Call Server Group Thresholds

Call server group thresholds are designed for your Cisco call server clusters and other logical groupings of call servers. Each call server in a cluster can play several different roles to provide failover safeguards and load balancing. The call server group thresholds apply to all call servers in a cluster.

Note: Call server group thresholds apply only to Cisco Unified Communications Manager environments.

Call server group thresholds trigger incidents when status changes exceed the Phone Status Changes metric. The Phone Status Changes incident helps you detect failover events and branch office outages. The incident also helps identify call server performance issues and costly branch office connectivity failures. Typically, the incident itself provides enough information to help you identify the affected devices and call server group. The Phone Status Changes incident helps you distinguish between endpoints that access call servers over a WAN link and endpoints that use a local cluster.

The Default call server group threshold triggers incidents when 50 percent of all devices had status changes during the reporting interval.

The following types of status changes contribute to a Phone Status Changes incident.

Currently Missing Phones status

The percentage of endpoints that were once registered to a server in the group, but are not now registered to any server in the group, and were not observed to have been formally unregistered. The total does not include endpoints that had normal deregistration, which can occur during a restart.

Recently Moved Phones status

The percentage of endpoints that were registered to a call server in this group, but are now registered to a different call server in the same group.

New/Found Phones status

The percentage of endpoints that are registered to a call server in this group, but were not registered during the previous reporting interval.

- A *new* endpoint has never registered to this call server group since monitoring with UC Monitor began.
- A *found* endpoint lost contact with this call server group in the past, but registered again during the last reporting interval.

When the threshold is exceeded, a Phone Status Changes incident appears in the Call Server Incident Details. Separate data views provide more information when you drill down into the detailed incident report.

The incident is not dependent on the similar information reported in the Phones Report. For example, when a Currently Missing Phones status change occurs, multiple devices in the Phones List can show a status of Unavailable or Lost Contact. The status of an endpoint is actually the device status at the end of the reporting interval. When a change in status occurs, the incident is created before another status change occurs. The later status is reflected in the Phones Report and is slightly out of sync with the incident. Review the Phone Details Report, which includes the Previous Status for each endpoint.

Create an Incident Response

You can configure different responses for each Location, for each media device, for each call server or call server group, or for pairs of Locations or media devices. You then associate the responses with the different thresholds for call quality, call setup, or call server incidents.

You can associate an incident response with more than one action.

Note: UC Monitor provides one default incident response, Default, which is not associated with an action.

Follow these steps:

1. Click Administration, Policies, Incident Responses in the navigation bar.

   The Incident Response List opens.

2. Click New to create an incident response.

   The Incident Response Properties page opens.

3. Type a name for the incident response in the Name field. The name helps you identify the response in the list of responses on the Threshold Properties page.

4. Click New to add an action.

   The Add Action to Incident Response page opens.

5. Select the Action Type, which determines the other selections on this page:

   - **Send Email**. Supply the email address of the person to notify when the associated threshold is violated. You can specify multiple email addresses, separated by commas or semicolons.
   - **Send SNMP Trap**. Supply parameters to send an SNMP trap to a third-party network monitoring operating environment.
   - **Launch Traceroute Investigation**. Lets you run an automatic traceroute to collect extra data about routing from the affected Location or voice gateway. The Launch Traceroute Investigation action is designed for call setup and call server group incidents only.

6. Set the Minimum Conditions for Taking Action:

   - **Severity**. Select the threshold severity level that can trigger this action when crossed: degraded or excessive. 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. Incidents of these types always have a severity of “excessive.”
   - **Duration**. Select the interval during which a monitored metric must violate the threshold before the action is launched. Use this option to launch actions either more or less quickly in response to threshold violations.

     For example, select 30 minutes to launch an action when latency exceeds the threshold during a 30-minute interval. It does not matter how many times during the interval that the threshold is crossed. It matters only that the condition still exists at the end of the selected duration.

7. Set the parameters that control the recipient and format of the notification. The available parameters vary depending on the selected Action Type:

   - **Recipients**. Provide the full email address of the person to receive an automatic email notification about this type of incident. Select someone who is most likely to respond quickly and accurately to remedy the problem that caused the incident. You can specify multiple email addresses, separated by commas or semicolons.
   - **Send SNMP Trap to**. The IP address or host name of the computer to receive the SNMP trap.

     Note: UC Monitor includes a MIB file that contains unique OIDs. You can import them into your trap receiver. The file is located in the following directory on the management console:

     `<install path>\CA\VoIPMonitor\MIB\NETQOS-VMTRAP-MIB.txt`

     Tip: To send a trap to more than one computer, create additional actions within the same response, one for each additional trap destination.
   - **Send Test Trap**: Click to send a trap to the IP address you entered in the "Send SNMP Trap to" field. Results of the test appear at the top of the Add Action to Incident Response page.
   - **Severity Updates**. Select when to send SNMP traps:
     - **Send update traps when Incident severity changes**. Send an SNMP trap if the incident severity changes, but the incident remains open. Also send an SNMP trap when a new incident is opened.
     - **Send only Incident open and close traps**. Send an SNMP trap only if a new incident is opened or if an incident is closed.

       Note: Some incident types do not have a severity parameter, such as the Poor Call Quality incident, or their severity is always excessive. The option to send only open and close traps is always used for these incidents.
   - **SNMP Profile**. Select the SNMP profile to use for the trap.

- **Time Zone**. Select the time zone of the recipient. The default time zone corresponds to the locale where the management console is installed.

8. Click OK.

   The action appears on the Incident Response Properties page.

9. Save the response:

   - Click Save to save the response and return to the Incident Response List.
   - Click Save & Add Another to save the response and create another response.

   You can now associate the incident response with a threshold.

Create a Call Server Group Threshold

When you create a call server group threshold, you select the incident response to launch when the threshold is violated.

Follow these steps:

1. Click Administration, Policies, Call Servers, Call Server Group Thresholds in the navigation bar.

   The Call Server Group Threshold List opens.

2. Click New.

   The Call Server Group Threshold Properties page opens.

3. Provide a name for the custom threshold in the Name field.

4. Select an incident response in the Incident Response field. This incident is launched when the threshold is violated. The incident response you created appears in this list.

5. (*Optional*) Briefly describe the threshold in the Description field. The description can indicate which server group is assigned these custom settings, for example.

6. Set the values for the Phone Status Changes threshold in the Threshold field.

   - Select Percentage as the unit of measure, or select None to disable the threshold. Disabling thresholds is not recommended.
   - Provide a value for the unit of measure. An incident is created when the percentage of devices that undergo a status change during the reporting interval exceeds the value you specify. Set a lower value to see incidents more quickly in response to status changes. Set a higher value to see incidents only after more status changes are observed. An incident is created only if the minimum value is met during a monitoring interval.

7. Save the threshold:
   - Click Save to save the threshold and return to the Call Server Group Threshold List.
   - Click Save & Add Another to save the threshold and create another threshold.

   The threshold is saved, and can be assigned to one or more call server groups.

Assign a Call Server Group Threshold to a Call Server

The call server group thresholds are appropriate for Cisco call server clusters. These thresholds apply to functionality that is shared among the call servers in a cluster. The Default call server group threshold is assigned to all call server groups unless you assign a custom threshold. You can assign a custom threshold to multiple call server groups.

Follow these steps:

1. Click Administration, Policies, Call Servers, Call Server Group Threshold Assignments in the navigation bar.

   The Call Server Group Threshold Assignment List opens.

2. Click New.

   The Call Server Group Threshold Assignment Properties page opens. The Available Call Server Groups list displays all call servers that have not been assigned to a customized threshold.

3. Select the threshold that you want to assign from the Threshold field.

4. Select a group in the Available Call Server Groups list.

   The Filter field accepts wildcard (*) search strings to limit the data shown in the list. For strings with no asterisks, the Filter field assumes wildcards (for example, “*abc*”) when it searches. Filtering can be useful when you have a long list of call server groups.

   For example, to see only items for the Raleigh office, enter **ral** for the filter and click Apply. Only items whose name begins with Ral are shown in the list.

5. Double-click an item in the Available list to move it to the Selected Call Server Groups list.

   Tip: You can use the Shift or Control key or click and drag with the left mouse button to select multiple items. Then click the Right arrow to move the items to the Selected list.

6. Save the assignment:
   - Click Save to save the assignment and return to the Call Server Groups Threshold Assignment List. The new assignment appears in the list.
   - Click Save & Add Another to save the assignment and assign another threshold.

   The threshold is now applied to the call server groups you selected.

Chapter 5: Understanding and Managing Codec Thresholds

The UC Monitor default codec thresholds let you monitor MOS relative to codec performance or relative to absolute MOS value. The codecs that your endpoints use play a critical role in call quality. Endpoints that use a low-bandwidth codec, such as G.729, can require new thresholds. You can base the new thresholds on lower performance expectations, or on the codec rather than a fixed threshold value.

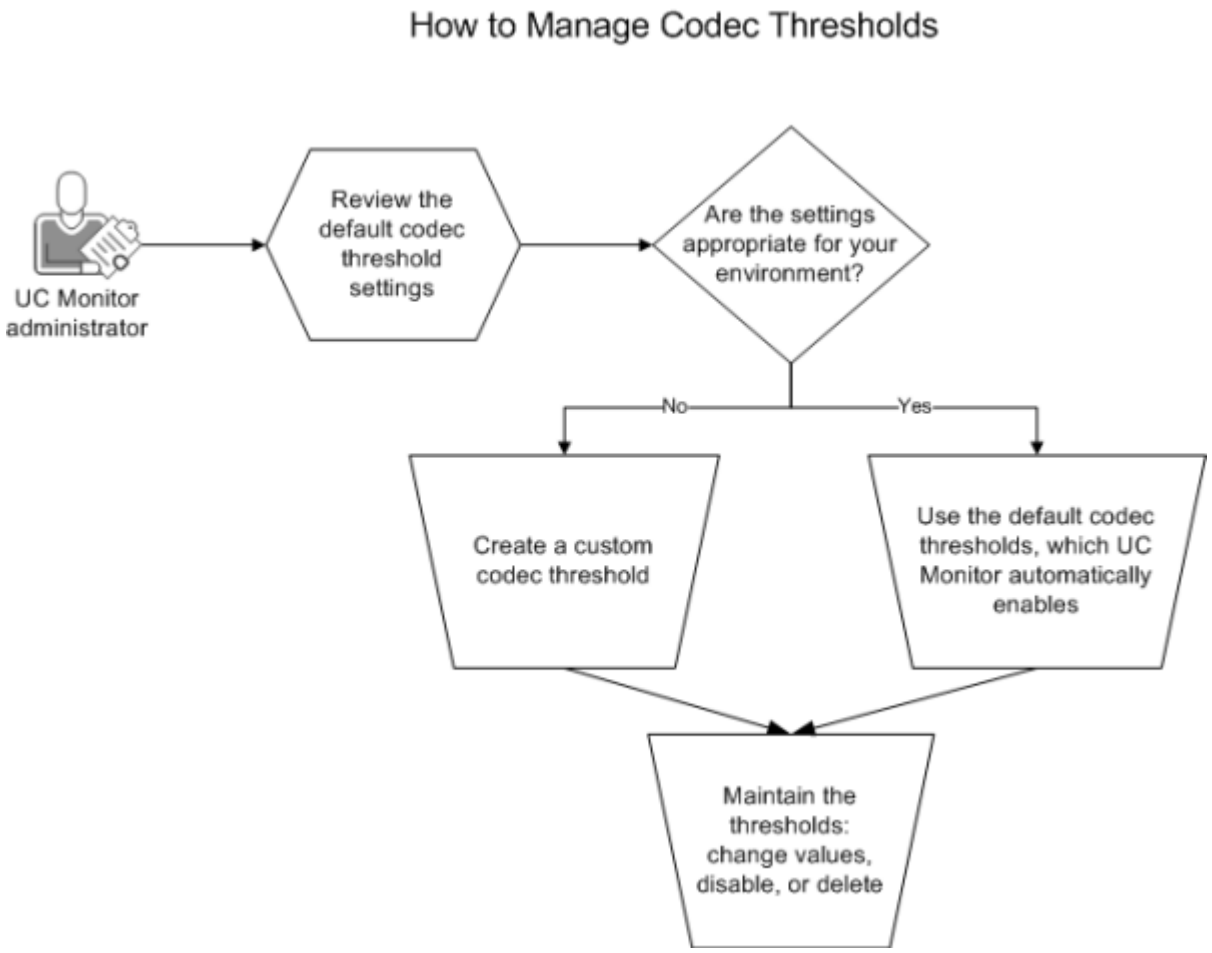
If the settings of the default codec thresholds are inappropriate for your environment, you can create your own thresholds for the codecs that UC Monitor supports. You cannot create thresholds for unsupported codecs.

This use case describes the default codec thresholds, and shows a UC Monitor administrator how to create, change, disable, and delete a codec threshold.

This section contains the following topics:

Overview

The following diagram illustrates the process for managing codec thresholds:



The following topics describe the process of managing codec thresholds:

- Review the settings for the default codec thresholds (see page 41).
- Create a custom codec threshold (see page 45).
- Change a threshold value (see page 46).
- Disable a threshold (see page 46).
- Delete a threshold (see page 47).

Codecs and Codec Thresholds

The codec is a component of VoIP or video over IP devices. Codec performance has a noticeable effect on VoIP and video performance. A high-performing codec encodes the voice signal, breaks it into packets, and queues the packets faster and with less data loss than a low-performing codec.

Many codecs are available to optimize VoIP or video performance. Some codec characteristics can affect network performance:

- Different codec types have different bandwidth requirements.
- Some codecs do not compress the data that they send. These codecs use more bandwidth than codecs that use a compression scheme. However, compression often degrades the audio signal and adds delay.

Codecs provide a certain level of audio quality, which is expressed as a theoretical maximum MOS. The software-only codecs from Microsoft receive ratings for theoretical maximum MOS, and advertise different performance expectations in wideband and narrowband environments. The theoretical maximum MOS is derived through testing. The theoretical maximum represents the highest possible MOS that a codec can achieve (without other impairments), such as delay due to network congestion.

Note: The Mean Opinion Score (MOS) is an industry standard method for gauging call quality. MOS is an estimation of how impairments to a voice signal affect listener perception of call quality.

Default Codec Thresholds

A codec threshold includes values for the following types of MOS.

- MOS: Available for most codecs.
- Network MOS: Offered by the Microsoft proprietary codecs.
- Wideband Listening MOS: Offered by the G.711a, G.711u, G.722 64K, RTAudio NB, RTAudio WB, and Siren codecs in a Microsoft Lync environment.

UC Monitor automatically applies the appropriate default threshold to the codec that is detected during monitoring. The default threshold values are based on unique codec attributes, such as theoretical maximum MOS.

Notes:

- There are no industry standards for rating the Wideband Listening MOS for a codec. The default threshold values for Wideband Listening MOS are based on CA internal testing. Your environment may require different values. Adjust them as necessary. For more information, see Manage Codec Thresholds.

- The collector attempts to identify unsupported codecs by the packet payload. An unidentified codec can appear as *Nonstandard* or *Dynamic Payload* in reports. Data from an unknown codec appears as *Unrated* because UC Monitor does not have the commonly accepted MOS thresholds for that codec. These values continue to be unrated until you assign a fixed-value MOS threshold to the affected Locations.

The following list summarizes the default codec threshold settings:

G.711a

This variation of the G.711 codec uses the A-law sampling method, popular in Europe and Asia. The default threshold values are as follows:

- MOS: 4.03 (Degraded), 3.60 (Excessive)
- Network MOS: 3.30 (Degraded), 2.95 (Excessive)
- Wideband Listening MOS: 2.50 (Degraded), 1.75 (Excessive)

G.711u

This variation of the G.711 codec uses the U-law sampling method, popular in North America and Japan. The default threshold values are as follows:

- MOS: 4.03 (Degraded), 3.60 (Excessive)
- Network MOS: 3.30 (Degraded), 2.95 (Excessive)
- Wideband Listening MOS: 2.50 (Degraded), 2.00 (Excessive)

G.722 64k

This wideband speech codec offers high-quality audio with a faster sampling rate. Cisco IP telephones report quality scores according to the G.711 wideband codecs, with the same theoretical maximum MOS. The same threshold settings are used for these two codecs. The default threshold values are as follows:

- Degraded MOS: 4.03
- Excessive MOS: 3.60
- Wideband Listening MOS: 3.00 (Degraded), 2.50 (Excessive)

G.722.1 24k

This variation of the G.722 codec offers lower bit-rate compression. The default threshold values are as follows:

- MOS: 3.75 (Degraded), 3.35 (Excessive)
- Network MOS: 3.58 (Degraded), 3.20 (Excessive)

G.723.1

Microsoft Exchange Unified Messaging uses this low-bandwidth codec. The default threshold values are as follows:

- MOS: 3.38 (Degraded), 3.02 (Excessive)
- Network MOS: 2.41 (Degraded), 2.15 (Excessive)

G.726 32k

This codec offers adaptive differential pulse-code modulation (ADPCM) with low bandwidth. The default threshold values are as follows:

- MOS: 3.86 (Degraded), 3.45 (Excessive)
- Network MOS: 3.17 (Degraded), 2.83 (Excessive)

G.729

This high-performance, low-bit-rate codec (8 Kbps) offers compression and coding of speech using the conjugate-structure algebraic-code-excited linear prediction (CS-ACELP) algorithm. The default threshold values are as follows:

- Degraded MOS: 3.59
- Excessive MOS: 3.21

G.729A

This reduced-complexity CS-ACELP codec is “Annex A” to the G.729 specification. The default threshold values are as follows:

- Degraded MOS: 3.48
- Excessive MOS: 3.11

G.7.29AB

This G.729 codec is fully compliant with ITU annexes A and B to the G.729 standard specification. The codec uses CS-ACELP with silence suppression. The default threshold values are as follows:

- Degraded MOS: 3.48
- Excessive MOS: 3.11

G.729B

This codec is “Annex B” to the G.729 specification and adds a silence compression scheme. The default threshold values are as follows:

- Degraded MOS: 3.59
- Excessive MOS: 3.21

GSM FR

This codec is an early speech coding standard for digital mobile telephone systems. The codec uses a 13-kbit-per-second sampling rate and delivers relatively poor quality. The default threshold values are as follows:

- Degraded Network MOS: 2.49
- Excessive Network MOS: 2.22

iLBC

The Internet Low Bit Rate Codec uses an 8-kHz/16-bit sampling rate and is designed to handle lost data. The default threshold values are as follows:

- Degraded MOS: 3.57
- Excessive MOS: 3.19

RTAudio NB

This proprietary Microsoft codec offers Realtime Audio in narrowband mode and uses an 8-kHz sampling rate. The default threshold values are as follows:

- MOS: 3.48 (Degraded), 3.11 (Excessive)
- Network MOS: 2.70 (Degraded), 2.41 (Excessive)
- Wideband Listening MOS: 3.00 (Degraded), 2.25 (Excessive)

RTAudio WB

This proprietary Microsoft codec offers Realtime Audio in wideband mode and uses a 16-kHz sampling rate. The default threshold values are as follows:

- MOS: 3.84 (Degraded), 3.44 (Excessive)
- Network MOS: 3.75 (Degraded), 3.35 (Excessive)
- Wideband Listening MOS: 2.50 (Degraded), 1.75 (Excessive)

Siren

Microsoft Lync uses this proprietary Polycom codec for audio-visual conferencing. The codec provides high-quality audio at low bit rates, and operates at 24 kbps and 32 kbps for wideband (50 Hz - 7 kHz). The default threshold values are as follows:

- MOS: 3.66 (Degraded), 3.27 (Excessive)
- Network MOS: 3.40 (Degraded), 3.04 (Excessive)
- Wideband Listening MOS: 2.75 (Degraded), 2.00 (Excessive)

Create a Custom Codec Threshold

If the settings of the default codec thresholds are inappropriate for your environment, you can create custom thresholds based on the codecs that UC Monitor supports. You cannot create thresholds for unsupported codecs.

Follow these steps:

1. Click Administration, Policies, Call Performance, Codec Thresholds in the navigation bar.

   The Codec Threshold List opens.

2. Click New.

   The Codec Threshold Properties page opens.

3. Select the codec for which you want to create a threshold in the Codec field.

   Tip: Codec thresholds consist of degraded and excessive values for one type of MOS. To set custom values for multiple MOS types, such as MOS and Network MOS, and associate them with the same codec, create two codec thresholds. Select the same codec in the Codec field.

4. Select the metric you want to customize in the Metric field: MOS, Network MOS, or Wideband Listening MOS.

5. Complete the Degraded Threshold and Excessive Threshold fields:

   - Select Enabled to enable alerting for the metric, or select Disabled to disable alerting for the metric. For example, you may want to receive alerts only for MOS that exceeds the excessive threshold.
   - Provide a value for the metric. All codec thresholds accept MOS values from 1.00 to 5.00, inclusive.

   Note: The value of the excessive threshold must be more severe than the value of the degraded threshold. For example, when the value for the degraded threshold is 4.02, the value for the excessive threshold must be less than 4.02. The difference indicates a lower MOS and, thus, a more severe decline in performance.

6. Save the threshold:

   - Click Save to save the threshold and return to the Call Threshold List. The new threshold appears in the list.
   - Click Save & Add Another to save the threshold and create another threshold.

   The threshold is enabled, and can be changed, disabled, or deleted.

Change a Threshold Value

You can change the value of the degraded and excessive thresholds.

Follow these steps:

1. Click Administration, Policies, Call Performance, Codec Thresholds in the navigation bar.

   The Codec Threshold List opens.

2. Select the codec whose threshold values you want to change and click Edit.

   The Codec Threshold Properties page opens.

3. Provide new values for the metrics in the Degraded Threshold and Excessive Threshold fields. All codec thresholds accept MOS values from 1.00 to 5.00, inclusive.

   Note: The value of the excessive threshold must be more severe than the value of the degraded threshold. For example, when the value for the degraded threshold is 4.02, the value for the excessive threshold must be less than 4.02. The difference indicates a lower MOS and, thus, a more severe decline in performance.

4. Click Save.

   The Call Threshold List displays the revised threshold values.

Disable a Threshold

When you do not want to monitor call quality for a particular codec, you can disable the internal Degraded and Excessive Thresholds for that codec threshold. Disabling these thresholds disables the entire codec threshold.

Follow these steps:

1. Click Administration, Policies, Call Performance, Codec Thresholds in the navigation bar.

   The Codec Threshold List opens.

2. Select the codec whose threshold you want to disable and click Edit.

   The Codec Threshold Properties page opens.

3. Select Disabled in the Degraded Threshold and Excessive Threshold fields to disable the entire codec threshold.

4. Select Disabled in either the Degraded Threshold or Excessive Threshold field to disable only one of the thresholds. For example, you may want to receive alerts only for MOS that exceeds the excessive threshold.
5. Click Save.

   The Call Threshold List indicates that the thresholds are disabled.

Delete a Threshold

You can delete custom codec thresholds. However, it is simpler to disable (see page 46) them. You can easily enable a disabled codec threshold. In contrast, you must recreate a deleted codec threshold.

Follow these steps:

1. Click Administration, Policies, Call Performance, Codec Thresholds in the navigation bar.

   The Codec Threshold List opens.
2. Select the codec whose threshold you want to delete.
3. Click Delete.

   The Confirm Delete page opens.
4. Click Delete.

   The threshold is deleted and no longer appears in the Codec Threshold List. However, when that codec is detected during call quality monitoring, the threshold is restored in the list with the default settings.