



# Release Notes for Cisco Unified Service Monitor 2.0

---

**Revised: April 22, 2009**

Cisco Unified Service Monitor is a product from the Cisco Unified Communications Management Suite. These release notes provide:

- [New Features, page 1](#)
- [Product Documentation, page 2](#)
- [Related Documentation, page 3](#)
- [Supported Versions of Cisco Unified CallManager, page 5](#)
- [Supported Cisco 1040 Binary Image Files, page 7](#)
- [Known Problems, page 7](#)
- [Documentation Errata, page 14](#)
- [Obtaining Documentation and Submitting a Service Request, page 15](#)

## New Features

The following changes and enhancements are included in Service Monitor 2.0:

- Cisco Unified CallManager support—Service Monitor can monitor calls from Cisco Unified CallManager clusters only, or in conjunction with sensors. For more information, see [Supported Versions of Cisco Unified CallManager, page 5](#).
- Cluster and sensor management—You can suspend and resume monitoring of clusters and sensors.
- Reports—Service Monitor reports display Mean Opinion Score (MOS), endpoints involved in voice activity, and other details obtained from sensors and clusters during the last 30 days.
- Threshold for each codec—Service Monitor supplies a set of global thresholds that enable you to set a MOS threshold value for each supported codec. You can selectively override global thresholds by creating sensor threshold groups and Cisco Voice Transmission Quality (CVTQ) threshold groups.



---

**Corporate Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006-2008 Cisco Systems, Inc. All rights reserved.

If you upgraded to Service Monitor 2.0 from an earlier version, you will notice changes in the following:

- Licensing—Specifies the number of phones that Service Monitor can monitor instead of the number of sensors that can register with Service Monitor.
- MOS violation SNMP trap definition—Specifies whether the trap was generated for sensor-based data or cluster-based data in the TT field. The trap definition also includes additional fields for each type of data.
- Cisco 1040 Sensor management:
  - TFTP servers—Instead of just one TFTP server, multiple TFTP servers can be added to Service Monitor. Service Monitor now automatically copies any updated sensor configuration files to the TFTP servers if permitted by the security settings on them. After successfully copying the sensor configuration files, Service Monitor resets affected sensors to load the new configuration.




---

**Note** You can still manually copy configuration files to the TFTP servers and then reset the sensors from the Service Monitor user interface.

---

- Sensor IDs—MAC addresses replace the *Annn* naming scheme formerly used for sensor IDs; in addition, you can add a descriptive name for a sensor.
- Sensor-calculated MOS—Sensors send data to Service Monitor every 60 seconds without determining whether a threshold has been violated. That determination is made by Service Monitor which stores the sensor data in the database, where it is available for reporting.
- Trap suppression—Service Monitor 2.0 introduces a setting to reduce the number of traps that Service Monitor sends for each endpoint, sending a trap every *n* minutes with a minimum value of 5. Additional traps for that endpoint during that time are suppressed (not sent).
- Failover from Primary Service Monitor—Sensor failover to a secondary Service Monitor is still supported; the ability to define and fail over to a tertiary Service Monitor is no longer supported.

## Product Documentation



**Note**

---

The originally published printed and electronic documentation is included with your product. Any changes after original publication are reflected on Cisco.com, where you will find the most up-to-date documentation.

---

[Table 1](#) describes the product documentation that is available.

**Table 1**      **Product Documentation**

Document Title	Available Formats
<i>Release Notes for Cisco Unified Service Monitor 2.0</i>	<ul style="list-style-type: none"> <li>PDF on the product CD-ROM.</li> <li>On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6536/prod_release_notes_list.html">http://cisco.com/en/US/products/ps6536/prod_release_notes_list.html</a></li> </ul>
<i>Quick Start Guide for Cisco Unified Service Monitor 2.0</i> <b>Note</b> This quick start guide explains how to install and upgrade Service Monitor.	<ul style="list-style-type: none"> <li>Printed document that was included with the product.</li> <li>PDF on the product CD-ROM.</li> <li>On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6536/prod_installation_guides_list.html">http://cisco.com/en/US/products/ps6536/prod_installation_guides_list.html</a></li> </ul>
<i>User Guide for Cisco Unified Service Monitor</i>	<ul style="list-style-type: none"> <li>PDF on the product CD-ROM.</li> <li>PDF accessible from online help.</li> <li>On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6536/products_user_guide_list.html">http://cisco.com/en/US/products/ps6536/products_user_guide_list.html</a></li> </ul>
Context-sensitive online help	Available by clicking one of the following: <ul style="list-style-type: none"> <li><b>Help</b> link in the upper right-hand corner of the window.</li> <li>Help button in the dialog box.</li> </ul>

## Related Documentation

**Note**

The originally published printed and electronic documentation is included with your product. Any changes after original publication are reflected on Cisco.com, where you will find the most up-to-date documentation.

[Table 2](#) describes the additional documentation that is available.

**Table 2**      **Related Documentation**

Document Title	Description and Available Formats
<i>Release Notes for Cisco Unified Operations Manager 2.0</i>	On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6535/prod_release_notes_list.html">http://cisco.com/en/US/products/ps6535/prod_release_notes_list.html</a>
<i>Quick Start Guide for Cisco 1040 Sensor</i>	Describes how to install a Cisco 1040 and provides regulatory compliance and safety information. This document is available on Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6536/prod_installation_guides_list.html">http://cisco.com/en/US/products/ps6536/prod_installation_guides_list.html</a>
<i>Quick Start Guide for Cisco Unified Operations Manager 2.0</i>	On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html">http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html</a>

**Table 2**      **Related Documentation (continued)**

<b>Document Title</b>	<b>Description and Available Formats</b>
<i>Installation Guide for Cisco Unified Operations Manager (Includes Service Monitor)</i>	On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html">http://cisco.com/en/US/products/ps6535/prod_installation_guides_list.html</a>
<i>User Guide for Cisco Unified Operations Manager</i>	On Cisco.com at the following URL: <a href="http://cisco.com/en/US/products/ps6535/products_user_guide_list.html">http://cisco.com/en/US/products/ps6535/products_user_guide_list.html</a>
<i>Release Notes for CiscoWorks Common Services 3.0.3 (Includes CiscoView 6.1.2) on Windows</i>	On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_note09186a00805af53a.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_note09186a00805af53a.html</a>
<i>Readme for Common Services 3.0.4 on Windows</i>	On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/prod_installation_guide09186a00805f7d64.html">http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/prod_installation_guide09186a00805f7d64.html</a>
<i>Installation and Setup Guide for Common Services 3.0.3 (Includes CiscoView) on Windows</i>	<ul style="list-style-type: none"> <li>• On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/products_installation_guide_book09186a00805305cb.html">http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3996/products_installation_guide_book09186a00805305cb.html</a></li> <li>• Printed document available by order (part number DOC-7817184=)<sup>1</sup></li> </ul>
<i>User Guide for CiscoWorks Common Services 3.0.3</i>	<ul style="list-style-type: none"> <li>• On Cisco.com at the following URL: <a href="http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_book09186a008053eabf.html">http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_book09186a008053eabf.html</a></li> <li>• Printed document available by order (part number DOC-7817182=)<sup>1</sup></li> </ul>

1. See the “Obtaining Documentation and Submitting a Service Request” section on page 15.

# Supported Versions of Cisco Unified CallManager

When properly configured, Service Monitor can report on voice activity from these versions of Cisco Unified CallManager.

Cisco Unified CallManager Version	Information Available from this Version
3.3	The following information is available for Service Monitor to include in reports:
4.0	
4.1	
4.2	In addition to the information provided by earlier versions, MOS is available for Service Monitor to use in determining whether a threshold has been violated and, if so, send a trap. Other data, such as concealment ratio and severely concealed seconds, is also available for inclusion on reports and in traps.
5.0	
5.1	
<p>MOS is calculated using the CVTQ algorithm on specific phones. To make CVTQ data available, you need to:</p> <ul style="list-style-type: none"> <li>• Ensure that you have applied any required patches to Cisco Unified CallManager.</li> <li>• Use the specified models of Cisco IP phones with the specified protocol and firmware; these phones must be registered with Cisco Unified CallManager 4.2, 5.0, or 5.1.</li> </ul> <p>See the information in the following sections.</p>	

## Required Cisco Unified CallManager Patches and Workarounds

Problems with CVTQ data can occur due to known problems with certain versions of Cisco Unified CallManager. [Table 3](#) documents these problems.

**Table 3**      **Circumstances that Can Affect Data**

Description	Circumstances
Service Monitor CVTQ reports show many calls for a Cisco Unified CallManager 5.x cluster during a period of 10 to 12 hours, followed by no calls	<p>After pushing huge numbers of Call Detail Records (CDRs) and Call Management Records (CMRs) to external servers, Cisco Unified CallManager 5.x stops pushing CMRs and CDRs.</p> <p>Bug ID: CSCsg50434</p> <p>This problem has been fixed in Cisco Unified CallManager 5.1.</p> <p>To work around this problem if you are monitoring a Cisco Unified CallManager 5.0 cluster, restart the CDR Repository Service as follows:</p> <ol style="list-style-type: none"> <li>1. From Cisco Unified CallManager Serviceability, select <b>Tools &gt; Control Center - Network Services</b>.</li> <li>2. Select <b>Publisher &gt; Stop / Start or Restart Cisco CDR Repository Manager</b>.</li> </ol>
Service Monitor CVTQ reports do not show any calls in a Cisco Unified CallManager 5.0 cluster	<p>If a space is included in the cluster ID, an error occurs in a component of Cisco Unified CallManager, and CDRs and CMRs are not pushed.</p> <p>Bug ID: CSCsd81400</p> <p>This problem has been fixed and verified in Cisco Unified CallManager 5.0(3.9911.35).</p> <p>Workaround: If you do not have the Cisco Unified CallManager 5.0(3.9911.35) image or later, do the following.</p> <ol style="list-style-type: none"> <li>1. Change the cluster ID to a name that doesn't include a space; from Cisco Unified CallManager Administration: <ol style="list-style-type: none"> <li>a. Select <b>System &gt; Enterprise Parameters</b>. The Enterprise Parameters Configuration page appears.</li> <li>b. Change the cluster ID.</li> <li>c. Click <b>Update</b>.</li> </ol> </li> <li>2. Repeat this step for each Cisco Unified CallManager: <ol style="list-style-type: none"> <li>a. From Cisco Unified CallManager Serviceability select <b>Tools &gt; Control Center - Feature Services</b>.</li> <li>b. Select the Cisco Unified CallManager server.</li> <li>c. Click the <b>Restart</b> button.</li> </ol> </li> <li>3. Remove old files from the Cisco Unified CallManager 5.0 server: <ol style="list-style-type: none"> <li>a. Log in to the server.</li> <li>b. Go to the <code>/var/log/active/cm/cdr</code> directory.</li> <li>c. Remove all files that start with <code>cdr_old cluster name_</code> and <code>cmr_old cluster name_</code>.</li> </ol> </li> </ol>

## Supported Cisco IP Phone Models and Phone Protocols

The following Cisco IP phone models support the Cisco Voice Transmission Quality (CVTQ) algorithm in SCCP mode if they have the 8.0(3) firmware which can be downloaded from Cisco Unified CallManager versions 4.2 and 5.x:

- 7940
- 7941
- 7960
- 7961
- 7970
- 7971

All other Cisco IP phone models, including 7985, do not support CVTQ. All SIP-based phones do not support CVTQ.

**Note**

---

The 8.0(3) phone firmware should also be accessible from this URL:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser>.

---

## Supported Cisco 1040 Binary Image Files

Only the following binary image files are supported for use on Cisco 1040 Sensors while using Service Monitor 2.0:

- SvcMonAA2\_34.img—Installed in the *NMSROOT*\ImageDir folder when you install Service Monitor 2.0.
- SvcMonAA2\_37.img—Available from Cisco TAC by request; for more information, see [Fixing the DHCP Option 150 Issue for Cisco 1040 Sensors](#), page 13.

**Caution**

---

Installing binary image files other than SvcMonAA2\_34.img and SvcMonAA2\_37.img can cause severe problems.

---

**Note**

---

For the Cisco 1040 binary images that are supported while using Service Monitor 2.0.1, see *Release Notes for Cisco Unified Service Monitor 2.0.1* at this URL:  
[http://www.cisco.com/en/US/partner/docs/net\\_mgmt/cisco\\_unified\\_service\\_monitor/2.0.1/release/notes/SrvMonRN.html](http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0.1/release/notes/SrvMonRN.html).

---

## Known Problems

**Note**

---

To obtain more information about known problems, access the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. (You will be prompted to log into Cisco.com.)

---

Table 4 describes problems known to exist in this release. For circumstances under which a Cisco 1040 Sensor becomes unable to find the TFTP server, see [Fixing the DHCP Option 150 Issue for Cisco 1040 Sensors, page 13](#). For additions to Service Monitor documentation, see [Documentation Addenda, page 13](#).

**Table 4** Known Problems in Service Monitor 2.0

Bug ID	Summary	Explanation
CSCsj91958	SM does not report endpoint properly for intercluster call	<p>In CVTQ reports, you will see the following as endpoints:</p> <ul style="list-style-type: none"> <li>• Cisco Unified Communications Manager</li> <li>• Cisco Unified Customer Voice Portal</li> <li>• Cisco Unified Presence Server</li> </ul> <p>even though the RTP media stream does not flow to the them as they are used only for signaling.</p> <p>This occurs in Cisco Unified Service Monitor 2.1 and earlier versions.</p> <p>There is no workaround.</p>
CSCso65632	Installation sometimes corrupts because DEP is not suppressed	<p>Installation sometimes fails. This happens when Windows Data Execution Prevention (DEP) is enabled.</p> <p>To work around this problem:</p> <ol style="list-style-type: none"> <li>1. Disable DEP: <ol style="list-style-type: none"> <li>a. Log in to the machine on which you will install Service Monitor as an administrator or a member of the Administrators group.</li> </ol> </li> </ol> <p><b>Note</b> If your computer is connected to a network, network policy settings might prevent you from completing this procedure.</p> <ol style="list-style-type: none"> <li>b. Open System Properties by right-clicking the My Computer icon on your desktop and selecting Properties.</li> <li>c. Click the Advanced tab; then, under Performance, click Settings.</li> <li>d. Click the Data Execution Prevention tab. If Turn on DEP for all programs and services except those I select is selected, DEP is enabled.</li> <li>e. Select Turn on DEP for essential Windows programs and services only.</li> <li>f. Click OK.</li> </ol> <ol style="list-style-type: none"> <li>2. Install Service Monitor.</li> <li>3. Install the DST patch by following the instructions for <a href="#">CSCsh81265, page 9</a>.</li> </ol> <p><b>Note</b> Install the DST patch whether or not you have previously installed it.</p> <ol style="list-style-type: none"> <li>4. If desired, re-enable DEP: <ol style="list-style-type: none"> <li>a. Perform steps 1a-1d.</li> <li>b. Select Turn on DEP for all programs and services except those I select.</li> </ol> </li> </ol>

Table 4 Known Problems in Service Monitor 2.0 (continued)




Bug ID	Summary	Explanation
CSCsh81265	Daylight Savings Time (DST) change in US	<p>In the United States beginning in March 2007, DST starts earlier—on the second Sunday in March—and ends later—on the first Sunday in November—than in previous years. During DST, Service Monitor user interface and reports will be an hour off.</p> <p>To work around this problem:</p> <p>Apply the US Daylight Saving Time (DST) Patch for Cisco Unified Service Monitor 1.1 and 2.0:</p> <ol style="list-style-type: none"> <li>1. Enter this URL into your browser: <a href="http://www.cisco.com/cgi-bin/tablebuild.pl/servmon">http://www.cisco.com/cgi-bin/tablebuild.pl/servmon</a> and follow instructions to log in.</li> <li>2. Download and read "Readme for US Daylight Saving Time (DST) Patch for Cisco Unified Service Monitor 1.1 and 2.0" (<a href="#">cusmdst_win.readme.pdf</a>). This document includes the amount of time required to install, installation instructions, and steps to complete after installing the patch.</li> <li>3. Download and install "Daylight Saving Patch for Cisco Unified Service Monitor 1.1 and 2.0" (<a href="#">cusmdst_win_k9.zip</a>).</li> <li>4. Sun Alert 102836 describes a bug in the latest JDK releases when using EST, MST, and HST abbreviations. To work around this problem for Service Monitor, complete either one of these workarounds: <ul style="list-style-type: none"> <li>– <b>Workaround Alternative 1</b> <ol style="list-style-type: none"> <li>a. From the command line on the Service Monitor system, stop the daemon manager using this command: <pre>net stop crmdmgt</pre></li> <li>b. Delete three time zone data files: EST, MST, and HST from the NMSROOT\lib\jre\lib\zi directory (or &lt;JRE_HOME&gt;/lib/zi).</li> </ol> <hr/> <p> <b>Note</b> NMSROOT is the directory where you installed Service Monitor; it is C:\Program Files\CSCOpX if you used the default location.</p> <hr/> <ol style="list-style-type: none"> <li>c. Start the daemon manager using this command: <pre>net start crmdmgt</pre></li> </ol> </li> <li>– <b>Workaround Alternative 2</b> <ol style="list-style-type: none"> <li>a. From the command line on the Service Monitor system, stop the daemon manager using this command: <pre>net stop crmdmgt</pre></li> <li>b. Download and extract the tzupdater tool from this URL: <a href="http://java.sun.com/javase/downloads/index.jsp">http://java.sun.com/javase/downloads/index.jsp</a></li> </ol> <hr/> <p> <b>Note</b> This website is Copyright © 1994-2008, Sun Microsystems, Inc.</p> </li> </ul> </li> </ol>

Table 4 Known Problems in Service Monitor 2.0 (continued)

Bug ID	Summary	Explanation
CSCsh81265 (continued)	Daylight Savings Time (DST) change in US	<p><b>c.</b> From the command line, execute this command:</p> <pre data-bbox="657 352 1409 380">&lt;NMSROOT&gt;\CSCOPx\lib\jre\java.exe -jar tzupdater.jar -f -bc</pre> <hr/> <p> <b>Note</b> NMSROOT is the directory where you installed Service Monitor; it is C:\Program Files\CSCOPx if you used the default location.</p> <hr/> <p><b>d.</b> Start the daemon manager using this command:</p> <pre data-bbox="657 604 889 632">net start crmdmgtd</pre>
CSCsh01863	New Cisco CallManager with same cluster ID corrupts info for previously added cluster	<p>Adding two Cisco Unified CallManager clusters with the same cluster ID to Service Monitor causes data corruption in Service Monitor.</p> <p><b>Note</b> Cisco Unified CallManager 3.3 and later use the default cluster name <i>StandAloneCluster</i>. If you are managing multiple Cisco Unified CallManager clusters, you must change the default cluster name.</p> <p>To prevent this problem, before adding credentials for a Cisco Unified CallManager to Service Monitor, confirm that the cluster ID is unique.</p> <p>To work around this problem:</p> <ol style="list-style-type: none"> <li><b>1.</b> Delete credentials from Service Monitor for each Cisco Unified CallManager with the same cluster ID.</li> </ol> <p><b>Note</b> For detailed instructions on configuring Cisco Unified CallManager, see the Cisco Unified CallManager documentation.</p> <ol style="list-style-type: none"> <li><b>2.</b> Update the cluster IDs to make them unique: <ol style="list-style-type: none"> <li><b>a.</b> Log in to Cisco Unified CallManager Administration.</li> <li><b>b.</b> Select <b>System &gt; Enterprise Parameters</b>. The Enterprise Parameters Configuration page appears.</li> <li><b>c.</b> In the Cluster ID field, enter a new cluster name.</li> <li><b>d.</b> Click <b>Update</b>.</li> </ol> </li> <li><b>3.</b> Add the Cisco Unified CallManager credentials to Service Monitor again.</li> </ol>

**Table 4**      **Known Problems in Service Monitor 2.0 (continued)**


Bug ID	Summary	Explanation
CSCsg86540	During reinstall, database backup continues indefinitely	<p>When reinstalling Service Monitor on a system with a large database, the backup operation can go on indefinitely.</p> <p>To work around this problem, skip the database backup during reinstallation (see step 2 in the following procedure). To also save the existing database, perform all of these steps:</p> <ol style="list-style-type: none"> <li>1. Save the existing database to a temporary location outside of NMSROOT before reinstalling Service Monitor:           <ol style="list-style-type: none"> <li>a. Stop the daemon manager using the following command:               <pre>net stop crmdmgt</pre> </li> <li>b. Change the qovr database password to something that you will remember. In this example, the new password is admin:               <pre>NMSROOT\C\bin\perl dbpasswd.pl dsn=qovr npwd=admin</pre> </li> </ol> </li> </ol> <p> <b>Note</b> NMSROOT is the location where Service Monitor is installed. If you used the default location, it is C:\Program Files\CSCOPx.</p> <ol style="list-style-type: none"> <li>c. From NMSROOT\databases\qovr, copy these files—qovr.db and qovrx.log—to a location outside of NMSROOT.</li> </ol> <ol style="list-style-type: none"> <li>2. Skip database backup while reinstalling Service Monitor:           <ol style="list-style-type: none"> <li>a. From the command line, change directory to the drive with the product CD.</li> <li>b. Issue this command:               <pre>Setup.exe nobackup</pre> </li> </ol> <p>To complete the reinstallation, follow the instructions online or consult <i>Quick Start Guide for Cisco Unified Service Monitor</i>.</p> </li> <li>3. After completing the reinstallation and rebooting your system, replace the newly created database with the database that you saved:           <ol style="list-style-type: none"> <li>a. Stop the daemon manager using the following command:               <pre>net stop crmdmgt</pre> </li> <li>b. Set the password on the newly created database to match the password that you set on the database that you saved:               <pre>NMSROOT\C\bin\perl dbpasswd.pl dsn=qovr npwd=admin</pre> </li> <li>c. Copy the database files—qovr.db and qovrx.log—from the location outside of NMSROOT (see step 1.c.) to NMSROOT\databases\qovr.</li> <li>d. Restart the daemon manager using the following command:               <pre>net start crmdmgt</pre> </li> </ol> </li> </ol>

Table 4 Known Problems in Service Monitor 2.0 (continued)

Bug ID	Summary	Explanation
CSCsg67050	G711 Ulaw not in sensor report; G711 Ulaw threshold not applied to sensor data	<p>Cisco 1040 sensors report a codec of G711 Alaw for calls that are actually G711 Ulaw. Therefore, no sensor records include G711 Ulaw. As a result, data from a sensor:</p> <ul style="list-style-type: none"> <li>• Cannot trigger global thresholds and sensor group thresholds for G711 Ulaw.</li> <li>• Does not appear in sensor diagnostic reports if you select G711 Ulaw (and not G711 Alaw) to generate the report.</li> </ul> <p>To work around this problem:</p> <ul style="list-style-type: none"> <li>• Select G711 Alaw on the Sensor Filter Reports page to generate a report that includes G711 Ulaw in addition to G711 Alaw.</li> <li>• Keep in mind that G711 Ulaw thresholds are not applied to data from Cisco 1040 sensors. Instead, G711 Alaw thresholds—global or from a sensor threshold group—are applied.</li> </ul>
CSCsb46108	Cisco 1040 sets syslog D field incorrectly for G711 Ulaw	<p>When G711Ulaw codec is used, the Cisco 1040 sets the syslog D field value to 2, which indicates that the codec is G711 Alaw. The correct syslog D field value for G711 Ulaw is 4.</p> <p>There is no workaround for this problem.</p>
CSCsc31319	Service Monitor shows Cisco 1040 waiting to register while receiving syslog	<p>The web interface on a Cisco 1040 displays status as operational and lists the Service Monitor to which the Cisco 1040 is registered. However, this Service Monitor shows the Cisco 1040 registered to Waiting while still receiving and processing syslog messages from this Cisco 1040.</p> <p>This problem occurs after a user does either of the following:</p> <ul style="list-style-type: none"> <li>• Uses <b>pdterm</b> to stop the QOVR process, and, in quick succession, uses <b>pdexec</b> to start it again.</li> <li>• Changes the time on the system where Service Monitor is installed without subsequently stopping and restarting the daemon manager process.</li> </ul> <p>To work around this problem, use one of these procedures:</p> <ul style="list-style-type: none"> <li>• Wait at least 5 minutes between stopping and starting the QOVR process. If you stopped and started the QOVR process in quick succession: <ol style="list-style-type: none"> <li>1. From the command line, stop the QOVR process again, by entering the <b>pdterm QOVR</b> command: <pre>pdterm QOVR</pre> </li> <li>2. Wait at least 5 minutes.</li> <li>3. Enter the <b>pdexec</b> command: <pre>pdexec QOVR</pre> </li> </ol> </li> <li>• Stop and start the daemon manager after you change the time on the server where Service Monitor is installed, by issuing the following commands: <pre>net stop crmdmgt net start crmdmgt</pre> </li> </ul>

**Table 4** Known Problems in Service Monitor 2.0 (continued)

Bug ID	Summary	Explanation
CSCsc19066	Cisco 1040 does not generate syslog messages for Audio Codec G722	There is no workaround for this problem.

## Fixing the DHCP Option 150 Issue for Cisco 1040 Sensors

A Cisco1040 Sensor does not correctly interpret DHCP Option 150 if the IP address includes an octet with the value of 32, such as 10.10.32.1, or an octet with the value of 92, such as 10.10.1.92.

This problem is fixed in binary image file, SvcMonAA2\_37.img, which you can obtain from Cisco Technical Assistance Center (TAC). (For contact information, see [Obtaining Documentation and Submitting a Service Request, page 15.](#)) Until you load SvcMonAA2\_37.img onto your sensors, use one of the workarounds.

### Workarounds

- Use the ASCII type when providing the Option 150 IP address.
- Ensure that the IP address for the TFTP server does not include an octet with the value 32 or 92.

### Loading SvcMonAA2\_37.img onto Cisco 1040 Sensors

You will need to employ one of the workarounds to enable the sensors to find a TFTP server and download the SvcMonAA2\_37.img from it. After SvcMonAA2\_37.img is loaded onto the sensors, workarounds are no longer necessary.

1. Put one of the workarounds in place in your DHCP configuration.
2. Add any new TFTP server to Service Monitor.
3. On your TFTP servers:
  - a. Delete the default sensor configuration file, QOVDefault.CNF, the sensor-specific configuration files QOV<MACAddress>.CNF, and the earlier binary image file, SvcMonAA2\_nn.img.
  - b. Copy SvcMonAA2\_37.img into the root directory.
4. From Service Monitor, edit the default sensor configuration file, entering SvcMonAA2\_37.img as the image filename.
5. Verify that the new default sensor configuration file, QOVDefault.CNF, has been copied to the TFTP servers. If not, copy it from the image file directory on the Service Monitor server (*NMSROOT*\ImageDir) to the root on the TFTP servers.
6. Reset the sensors. To reset a sensor, you can restart the SPAN or RSPAN port on the switch to which the sensor is connected.
7. If desired, remove the workaround from your DHCP configuration.

## Documentation Addenda

The following information is missing from the hardcopy, online help, or PDF versions of the Service Monitor documentation. The documentation on Cisco.com has been updated with this information.

## Configuring the Service Monitor Client to Allow Popup Windows


**Note**

This topic has been added to *Quick Start Guide for Cisco Unified Service Monitor 2.0*.

When using Service Monitor, disable any software on your desktop that you use to prevent popup windows from displaying. Service Monitor must be able to open multiple windows to display information.

## Disabling Virus Scanning on the Databases Directory


**Note**

This topic has been added to *Quick Start Guide for Cisco Unified Service Monitor 2.0*.

You should exclude the *NMSROOT*\databases directory from virus scanning. Problems can arise if database files are locked because of virus scanning.


**Note**

*NMSROOT* is the directory where Service Monitor is installed on your system. If you selected the default directory during installation, it is C:\Program Files\CSCOpX.

## Ensuring Successful Reinstallation


**Note**

This step has been added to *Quick Start Guide for Cisco Unified Service Monitor 2.0*.

If you uninstall Service Monitor from a system, you should delete any files left in the *NMSROOT* directory prior to installing Service Monitor again on the same system.

## Documentation Errata

The following information is missing from the online help and from the PDF user guide included in the online help and on the product CD and has been added to the user guide on Cisco.com.

## Activating the AXL Web Service on Unified Communications Manager (Appendix B)

Perform this procedure for Unified Communications Manager versions 5.x and later.

- 
- Step 1** Launch Unified Communications Manager Serviceability.
  - Step 2** Select **Tools > Service Activation**.
  - Step 3** Select a server.


**Note**

Activate the AXL Web Service on the Publisher node only.

- Step 4** Scroll down to Database and Admin Services and select [Cisco AXL Web Service](#).
- Step 5** Click **Save**.
- 

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

---

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006-2009 Cisco Systems, Inc. All rights reserved.