



## Managing Sensors

---

The following topics are included:

- [Overview: Examining Data From Sensors, page 4-1](#)
- [Performing Initial Configuration in Service Monitor for Sensors, page 4-2](#)
- [Configuring Sensors in Service Monitor, page 4-6](#)
- [Viewing the Configuration for a Sensor, page 4-12](#)
- [Understanding How Sensors Register with Service Monitors, page 4-14](#)
- [Updating Image Files on Sensors, page 4-15](#)
- [Moving a Sensor from One Location to Another, page 4-16](#)
- [Understanding Sensor Call Metrics Archive Files, page 4-16](#)
- [Understanding Cisco 1040 Unreachable Trap, page 4-17](#)

### Overview: Examining Data From Sensors

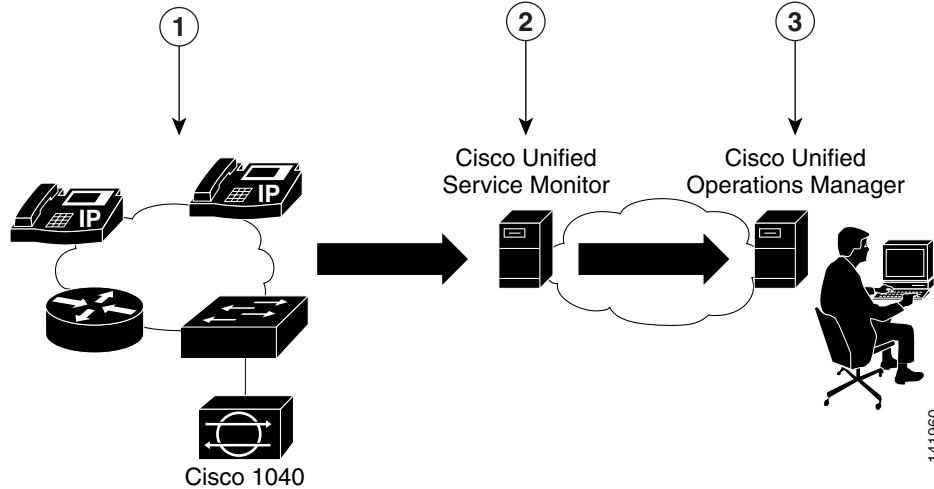
Service Monitor analyzes data that it receives from Cisco 1040 Sensors (Cisco 1040s) installed in your voice network. Each licensed instance of Service Monitor acts as a primary Service Monitor for multiple Cisco 1040s. A Service Monitor can also be configured to act as a secondary Service Monitor for Cisco 1040s that are managed by other licensed instances of Service Monitor. When a Service Monitor becomes unavailable, Cisco 1040s temporarily fail over to secondary Service Monitors until the primary Service Monitor becomes available again.

Service Monitor examines the data it receives from Cisco 1040s, comparing Mean Opinion Scores (MOS)—computed by Cisco 1040s for each RTP stream—against a user-specified threshold value. When MOS drops below the threshold, Service Monitor generates SNMP traps and sends them to up to four trap receivers. Optionally, Service Monitor stores the call metrics it receives from Cisco 1040s to disk files.

To further analyze, display, and act on Service Monitor data, you can use Cisco Unified Operation Manager (Operations Manager), by configuring it as a trap receiver for Service Monitor. Operations Manager can generate events for Service Monitor traps, display the events on the Service Quality Alerts dashboard, and store event history for up to 30 days. For more information, see *User Guide for Cisco Unified Operations Manager*.

[Figure 4-1](#) shows Service Monitor and Cisco 1040s installed with Operations Manager.

Figure 4-1 Service Monitor Deployment



<b>1</b>	Cisco 1040 monitors actual voice calls.	<b>3</b>	Operations Manager presents alert information.
<b>2</b>	Service Monitor evaluates MOS values and sends SNMP traps when a threshold is violated. Service Monitor also sends an SNMP trap when a Cisco 1040 is unreachable.	—	—

For more information, see the following topics:

- [Understanding Cisco 1040 Unreachable Trap](#), page 4-17
- [MIBs Used and SNMP Traps Generated](#), page C-1

## Performing Initial Configuration in Service Monitor for Sensors

To configure sensors, do the following:

1. Add one or more TFTP servers for Service Monitor and sensors to use. See [Configuring TFTP Servers for Sensor Configuration and Image Files](#), page 4-3.
2. Copy the binary image file from the Service Monitor server to the TFTP server.
3. Create a default configuration file. See [Setting Up the Sensor Default Configuration](#), page 4-4.

Service Monitor copies sensor configuration files to each TFTP server that you configure. When a sensor connects to the network, it downloads a configuration file from a TFTP server before registering to a service monitor. For more information, see [Understanding How a Sensor Registers with Service Monitor](#), page 4-15.

## Configuring TFTP Servers for Sensor Configuration and Image Files

Service Monitor uses one or more TFTP servers to provide configuration files and binary image files for sensors. You must define at least one TFTP server for Service Monitor to use. You can configure additional TFTP servers either as backup or if you have more than one DHCP scope.

After you add or edit a sensor, Service Monitor updates the configuration file locally, on its server, before copying the configuration file to all known TFTP servers. Keeping copies of the configuration files on each TFTP server enables sensors to fail over efficiently to a secondary Service Monitor.

You can use the configuration files that Service Monitor keeps on the server to recover if there is a write failure on the TFTP server. In this case, you can manually copy configuration files from Service Monitor to each TFTP server that is configured for Service Monitor. (To verify the contents of a configuration file on the TFTP server, see [Viewing the Configuration File on the TFTP Server from a Sensor, page 4-13.](#))

You must copy the binary image file for sensors to each TFTP server that you add to Service Monitor; see [Copying the Binary Image File to the TFTP Server, page 4-4.](#)

- Step 1** Select **Configuration > Sensor > TFTP Servers**. The TFTP Server Setup page appears, displaying the information in the following table.

GUI Element	Description/Action
Check box	Select when you want to delete a TFTP server.
TFTP Server	IP address or DNS name.
Port	The customary port number is 69.
Add button	Click to add a TFTP server.
Delete button	Select a check box and click to delete the selected TFTP server.

### Adding a TFTP Server

To enable sensors to register with Service Monitor, you must define at least one TFTP server where Service Monitor can provide sensor configuration files. You can configure additional TFTP servers; for example, to serve as backup or if you have more than one DHCP scope.



**Note**

You can use a Cisco Unified CallManager 5.x or 4.2 as a TFTP server. Security settings on Cisco Unified CallManager can prevent Service Monitor from uploading configuration files. You must manually copy configuration and image files from Service Monitor to Cisco Unified CallManager TFTP server.

- Step 1** Select **Configuration > Sensor > TFTP Servers**. The TFTP Server Setup page appears.
- Step 2** Click **Add**. The TFTP Server Settings dialog box appears.

- Step 3** Enter data in the following fields:
- TFTP Server—IP address or DNS name.
  - Port Number—The customary port number is 69.
- Step 4** Click **OK**.



**Note** Copy the binary image file to each TFTP server that you add to Service Monitor.

## Copying the Binary Image File to the TFTP Server



**Note** For the binary image files that are supported with Service Monitor 2.0, see *Release Notes for Cisco Unified Service Monitor 2.0* at this URL: [http://www.cisco.com/en/US/partner/docs/net\\_mgmt/cisco\\_unified\\_service\\_monitor/2.0/release/notes/SrvMonRN.html](http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html).

- Step 1** Copy the binary image file, SvcMonAA2\_34.img, from *NMSROOT*\ImageDir on the Service Monitor server to the root location on the TFTP server. (*NMSROOT* is the directory where Service Monitor is installed; its default location is C:\Program Files\CSCOPx.)

## Deleting a TFTP Server

- Step 1** Select **Configuration > Sensor > TFTP Servers**. The TFTP Server Setup page appears.
- Step 2** Select a check box.
- Step 3** Click **Delete**. A confirmation dialog box appears.
- Step 4** Click **Yes**.

## Setting Up the Sensor Default Configuration

Use this procedure to:

- Enable or disable call metrics archiving—Service Monitor saves MOS data in the database. Optionally, you can also save the data to files.
- View the directory path for the archive data file and the Cisco 1040 image file.
- Create the default configuration file—QOVDefault.CNF specifies the primary and secondary Service Monitor to which a sensor can register.

- Step 1** Select **Configuration > Sensor > Setup**. The Setup page appears.
- Step 2** Update data described in the following table.

GUI Element	Description/Action
Call Metrics Archiving radio buttons	Select one of the following: <ul style="list-style-type: none"> <li>• Enable—After analysis, Service Monitor saves data from Cisco 1040s to disk files.</li> <li>• Disable—After analysis, Service Monitor discards data.</li> </ul> Default: Disable.
Data File Directory	Directory where files are stored if call metrics archiving is enabled. You cannot edit this field. <p><b>Note</b> Call metrics are archived to <i>NMSROOT/DataDir</i>. (<i>NMSROOT</i> is the directory where Service Monitor is installed. Its default location is <i>C:\Program Files\CSCOpX</i>.)</p>
Image File Directory	Directory where sensor binary image file and configuration files are stored locally: <i>NMSROOT/ImageDir</i> — <i>NMSROOT</i> is the directory where Service Monitor is installed; its default location is <i>C:\Program Files\CSCOpX</i> . You cannot edit this field. <p><b>Note</b> For more information, see <a href="#">Updating Image Files on Sensors, page 4-15</a>.</p>
Send traps every <i>n</i> minutes per endpoint	Enter a number greater than or equal to 5. Sensors send data to Service Monitor every 60 seconds. Service Monitor determines whether a violation has occurred and can potentially send a trap-a-minute for that endpoint. Use this setting to reduce the number of traps that Service Monitor sends for each endpoint. For a given endpoint, a trap is sent every <i>n</i> minutes and additional traps during that time are suppressed (not sent).
<b>Default Configuration to TFTP Server</b>	
Image Filename	Enter the image filename if you have downloaded a new image. See <a href="#">Updating Image Files on Sensors, page 4-15</a> . <p><b>Note</b> For the binary image filenames that are supported with Service Monitor 2.0, see <i>Release Notes for Cisco Unified Service Monitor 2.0</i> at this URL: <a href="http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html">http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html</a>.</p>
Primary Service Monitor	IP address or DNS name for the primary Service Monitor.
Secondary Service Monitor	IP address or DNS name for the secondary Service Monitor; blank if not set. (See <a href="#">Editing the Configuration for a Specific Sensor, page 4-10</a> .)

**Step 3** Click **OK**. Service Monitor stores the configuration file locally and copies it to the TFTP servers that are added to Service Monitor. For more information, see [Configuring TFTP Servers for Sensor Configuration and Image Files, page 4-3](#).

**Note**

If you are using Cisco Unified CallManager 5.x or 4.2 as a TFTP server, you must manually upload the default configuration from the image file directory on the Service Monitor server to Cisco Unified CallManager TFTP server.

## Configuring Sensors in Service Monitor

**Note**



You must configure DHCP and DNS correctly for Cisco 1040s to work properly. For more information, see *Quick Start Guide for Cisco 1040 Sensor*.

The following information is available for managing Cisco 1040s:

- [Understanding the Cisco 1040 Sensor Details Page, page 4-7](#)
- [Adding a Sensor to Service Monitor, page 4-8](#)
- [Editing the Configuration for a Specific Sensor, page 4-10](#)
- [Resetting a Sensor, page 4-11](#)
- [Deleting a Sensor, page 4-11](#)

## Understanding the Cisco 1040 Sensor Details Page

**Step 1** Select **Configuration > Sensor > Management**. The Cisco 1040 Sensor Details page displays information listed in the following table.

GUI Element	Description/Action
	Exports data from the Cisco 1040 Sensor Details page to a CSV or PDF file. See <a href="#">Exporting Data to a CSV or PDF File, page 4-8</a> .
	Opens a printer-friendly version of the data in another window; for printing from a browser window.
Check box column	Select Cisco 1040s that you want to edit, reset, or delete.
Name column	Click the name link to view details of the Cisco 1040 configuration. See <a href="#">Viewing Details in Service Monitor for a Specific Sensor, page 4-12</a> .
Sensor Address columns	Displays MAC and IP addresses for Cisco 1040. Click the MAC address link to launch an HTML page on the Cisco 1040. (See <a href="#">Viewing the Configuration Using the Sensor Web Interface, page 4-13</a> .)
Service Monitor columns	Displays the following: <ul style="list-style-type: none"> <li>• Primary—IP address or hostname of the primary Service Monitor defined for the Cisco 1040.</li> <li>• Secondary—IP address or hostname of the secondary Service Monitor defined for the Cisco 1040.</li> <li>• Registered with—IP address or hostname of the Service Monitor to which the Cisco 1040 is currently sending data. If the sensor is not yet registered, Waiting is displayed.</li> </ul> <p><b>Note</b> If you have recently changed the time on your system or, in rapid succession, stopped and started the QOVR process, Service Monitor might display a Cisco 1040 as registered with Waiting, while still receiving and processing syslog messages from the Cisco 1040. To fix this problem, see <a href="#">Restarting Processes to Update Sensor Registration Information in Service Monitor, page 4-8</a>.</p>
Reset Time column	The last date and time the Cisco 1040 was rebooted.
Edit button	Click to edit the Cisco 1040 configuration. See <a href="#">Editing the Configuration for a Specific Sensor, page 4-10</a> .

### Restarting Processes to Update Sensor Registration Information in Service Monitor

Service Monitor might show a Cisco 1040 waiting to register while receiving and processing syslogs from it; this problem can occur after a user does one of the following:

- Uses **pdterm** to stop the QOVR process, and, in quick succession, uses **pdexec** to start it again. To prevent this problem, wait at least 5 minutes between stopping and starting the QOVR process. To correct this problem:
  1. From the command line, stop the QOVR process again, by entering this command:

```
pdterm QOVR
```
  2. Wait at least 5 minutes.
  3. Enter this command:

```
pdexec QOVR
```
- Changes the time on the system where Service Monitor is installed without subsequently stopping and restarting the daemon manager. To correct this problem, stop and start the daemon manager from the command line by issuing the following commands:

```
Net stop crmdmgt  
Net start crmdmgt
```

### Exporting Data to a CSV or PDF File

After you click the export icon, a dialog box appears.

- 
- Step 1** Select one radio button: CSV or PDF.
- Step 2** Browse to the location where you want to store the file and click **OK**.
- 

## Adding a Sensor to Service Monitor

If a sensor is already registered with Service Monitor, you must select it and click the Edit button to update it. For more information, see [Editing the Configuration for a Specific Sensor, page 4-10](#).

- 
- Step 1** Select **Configuration > Sensor > Management**. The Cisco 1040 Sensor Detail page appears.
- Step 2** Click **Add**. The Add a Cisco 1040 Sensor dialog box appears.
- Step 3** Enter data listed in the following table.

GUI Element	Description/Action
Sensor Name	Enter up to 20 characters. This name is used on Service Monitor windows, such as reports.  <b>Note</b> Sensor names do not need to be unique. Sensors that register to Service Monitor using the default configuration file each use the name Cisco 1040.
Image File Name	Enter the binary image filename. The filename format is SvcMon<vendor code><Cisco 1040 type><major version>_<minor version><bugfix version>.img. For example:  SvcMonAA2_34.img  For the binary image filenames that are supported with Service Monitor 2.0, see <i>Release Notes for Cisco Unified Service Monitor 2.0</i> at this URL: <a href="http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html">http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html</a> .  For more information, see <a href="#">Viewing the Configuration Using the Sensor Web Interface, page 4-13</a> and <a href="#">Updating Image Files on Sensors, page 4-15</a> .
MAC Address	Enter the MAC address for the Cisco 1040 that you are adding.
Primary Service Monitor	Enter an IP address or DNS name of a host where Service Monitor is installed. The Cisco 1040 sends data to this Service Monitor unless it becomes unreachable.
Secondary Service Monitor	(Optional) Enter an IP address or DNS name of a host where another instance of Service Monitor is installed. The Cisco 1040 sends data to this Service Monitor only if the primary Service Monitor becomes unreachable. For more information, see <a href="#">Viewing the Configuration Using the Sensor Web Interface, page 4-13</a>
Description	Enter up to 80 characters.

**Step 4** Click **OK**. The configuration file is saved on the server where Service Monitor is installed and is copied to all TFTP servers. (See [Configuring TFTP Servers for Sensor Configuration and Image Files, page 4-3](#).) The configuration file is named QOV<MAC address>.CNF, where <MAC address> is the MAC address for the Cisco 1040. (To view the MAC address, see [Viewing the Configuration Using the Sensor Web Interface, page 4-13](#).)



**Note** If you are using Cisco Unified CallManager 5.x or 4.2 as a TFTP server, you must manually upload the MAC-specific configuration file from the image file directory on the Service Monitor server to Cisco Unified CallManager TFTP server. The image file directory is *NMSROOT/ImageDir*; *NMSROOT* is the directory where Service Monitor is installed; its default location is C:\Program Files\CSCOpX.

## Editing the Configuration for a Specific Sensor



**Note** Do not edit a Cisco 1040 configuration file using a text editor. Edit a Cisco 1040 configuration file using this procedure only.

**Step 1** Select **Configuration > Sensor > Management**. (For more information, see [Understanding the Cisco 1040 Sensor Details Page, page 4-7.](#))

**Step 2** Select the check box for a sensor and click **Edit**.

**Step 3** Update any of the following fields.

Fields	Description/Action
Sensor Name	If you want to change the name, enter up to 20 characters. This name is used on Service Monitor windows, such as reports.
MAC Address	Cisco 1040 MAC address. <b>Note</b> You cannot edit this field.
IP Address	Cisco 1040 IP address. <b>Note</b> You cannot edit this field. To update the IP address for a sensor, delete the sensor from Service Monitor and add it again.
Image File Name	Enter the binary image filename. The filename format is SvcMon<vendor code><Cisco 1040 type><major version>_<minor version><bugfix version>.img. For example: <code>SvcMonAA2_34 .img</code>  Where: <ul style="list-style-type: none"> <li>• A is the vendor code for this Cisco 1040 (for internal use)</li> <li>• A is the Cisco 1040 type (for internal use)</li> <li>• 2 is the major release number</li> <li>• 3 is the minor release number</li> <li>• 4 is the bugfix number</li> </ul> For the binary image filenames that are supported with Service Monitor 2.0, see <i>Release Notes for Cisco Unified Service Monitor 2.0</i> at this URL: <a href="http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html">http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html</a> .  For more information, see <a href="#">Viewing the Configuration Using the Sensor Web Interface, page 4-13</a> and <a href="#">Updating Image Files on Sensors, page 4-15</a> .
Primary Service Monitor	Enter an IP address or DNS name of a host where Service Monitor is installed. The Cisco 1040 sends data to this Service Monitor unless it becomes unreachable.

Fields	Description/Action
Secondary Service Monitor	(Optional) Enter an IP address or DNS name of a host where Service Monitor is installed. The Cisco 1040 sends data to this Service Monitor only if the primary Service Monitor becomes unreachable.
Description	Enter up to 80 characters.

- Step 4** Click **OK**. Service Monitor saves the configuration file on the local server copies it to all TFTP servers. Then Service Monitor resets the sensor, so that it loads the updated configuration.



**Note** If you are using Cisco Unified CallManager 5.x or 4.2 as a TFTP server, you must manually upload the updated configuration file from the image file directory on the Service Monitor server to Cisco Unified CallManager TFTP server. Afterward, you must reset the sensor. (The image file directory is *NMSROOT/ImageDir*; *NMSROOT* is the directory where Service Monitor is installed; its default location is *C:\Program Files\CSCOpX*.)

## Resetting a Sensor

Use this procedure to boot a Cisco 1040. After a Cisco 1040 boots, it first uses DHCP to obtain the IP address of the TFTP server. From the TFTP server, Cisco 1040 obtains a configuration file. If the configuration file specifies a binary image file that is different from the currently installed image, Cisco 1040 also obtains the binary image file from the TFTP server.

- Step 1** Select **Configuration > Sensor > Management**. (For more information, see [Understanding the Cisco 1040 Sensor Details Page, page 4-7](#).)
- Step 2** Select check boxes for the Cisco 1040s that you want to reset.
- Step 3** Click **Reset**.

## Deleting a Sensor

Before you complete this procedure, delete the sensor from any sensor threshold groups. See [Editing a Sensor Group, page 5-10](#).

- Step 1** Delete the configuration file for the Cisco 1040 (*QOVmacaddress.CNF*) from the TFTP servers.
- Step 2** Select **Configuration > Sensors**. The Cisco 1040 Sensor Details page opens. (For more information, see [Understanding the Cisco 1040 Sensor Details Page, page 4-7](#).)
- Step 3** Select check boxes for the Cisco 1040s that you want to delete.
- Step 4** Click **Delete**. One of the following occurs:
- A confirmation dialog box appears.
  - An error message appears, displaying a list of sensor threshold groups to which the sensor belongs. You will need to remove the sensor from these sensor threshold groups and repeat this procedure.

**Step 5** Click **OK**.




## Viewing the Configuration for a Sensor

Configuration data for a Cisco 1040 Sensor is stored in Service Monitor, is copied to a configuration file for the sensor on each TFTP server, and is copied down to the sensor (the sensor downloads the configuration from the TFTP server). You can look at the configuration details that are stored for a Cisco 1040 Sensor on each point: Service Monitor, TFTP server, and the sensor itself:

- [Viewing Details in Service Monitor for a Specific Sensor, page 4-12](#)
- [Viewing the Configuration File on the TFTP Server from a Sensor, page 4-13](#)
- [Viewing the Configuration Using the Sensor Web Interface, page 4-13](#)

## Viewing Details in Service Monitor for a Specific Sensor

To open the Cisco 1040 Sensor Detail dialog box, click the name link on the Cisco 1040 Sensor Details page. The Cisco 1040 Sensor Detail dialog box displays the Cisco 1040 Sensor Information table described here.

Field	Description/Action
	Exports data from the Cisco 1040 Sensor Information table to a CSV or PDF file. See <a href="#">Exporting Data to a CSV or PDF File, page 4-8</a> .
	Opens a printer-friendly version of the data in another window; for printing from a browser window.
	Opens context-sensitive online help.
Name link	Cisco 1040 user-entered name—Click to open a web interface on the Cisco 1040. See <a href="#">Viewing the Configuration Using the Sensor Web Interface, page 4-13</a> .
MAC Address	Cisco 1040 MAC address.
IP Address	Cisco 1040 IP address.
Primary Service Monitor	IP address or DNS name for the primary Service Monitor.
Secondary Service Monitor	IP address or DNS name for the secondary Service Monitor; blank if not set. (See <a href="#">Editing the Configuration for a Specific Sensor, page 4-10</a> .)
Registered with	IP address or DNS name for the Service Monitor that this Cisco 1040 is registered with.

Field	Description/Action
Image File Name	<p>Name of the image file installed on the Cisco 1040.</p> <p>For the binary image filenames that are supported with Service Monitor 2.0, see <i>Release Notes for Cisco Unified Service Monitor 2.0</i> at this URL:  <a href="http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html">http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html</a>.</p> <p><b>Note</b> If there is a more recent image file available on the TFTP server, you must edit the configuration file for the Cisco 1040, specifying the filename for the more recent image, and you must reset the Cisco 1040. (See <a href="#">Editing the Configuration for a Specific Sensor</a>, page 4-10.)</p>
Last Reset Time	Date and time that the Cisco 1040 was last reset. (See <a href="#">Resetting a Sensor</a> , page 4-11.)
Description	User-entered description for the Cisco 1040. (See <a href="#">Editing the Configuration for a Specific Sensor</a> , page 4-10.)

## Viewing the Configuration File on the TFTP Server from a Sensor

- Step 1** From your browser, enter `http://<IP address or DNS name>/Communication` where IP address is the address of your Cisco 1040 and DNS name is the DNS name for the Cisco 1040. For example:
- ```
http://Cisco-1040-sj/Communication
```
- Step 2** The Communication Log File window displays the following information from the configuration file on the TFTP server for this Cisco 1040:
- Receiver—IP address or DNS name of each Service Monitor—primary and secondary—defined in the configuration file, separated by semicolons.
  - ID—User-defined name of the Cisco 1040 that uses this configuration file.
  - Image—Name of the binary image file that the Cisco 1040 should download and run from the TFTP server.
  - Last Updated—The last time that this configuration file was updated on the Service Monitor system.
  - CDPGlobalRunState—States whether CDP is enabled (true) or disabled (false).
  - SyslogPort—States the port protocol (UDP) and port number used for sending syslogs to Service Monitor.
  - SkinnyPort—States the port protocol (TCP) and port number used to communicate with Service Monitor.

## Viewing the Configuration Using the Sensor Web Interface

To use the web interface to view the contents of the configuration file for this Cisco 1040 on the TFTP server, see [Viewing the Configuration File on the TFTP Server from a Sensor](#), page 4-13.

You can open a web interface to view the information stored on a Cisco 1040 in one of the following ways:

- Click the **(View)** link on the Cisco 1040 Sensor Details page. See [Understanding the Cisco 1040 Sensor Details Page, page 4-7](#).
- Enter `http://<IP address>` in your browser where IP address is the address of your Cisco 1040.

The Cisco 1040 web interface displays a Cisco 1040 Information window with the following information:

- **ID**—Cisco 1040 MAC address.
- **MAC Address**—Cisco 1040 MAC address.
- **Time stamp**—Current time on the Cisco 1040.
- **Status**—Status of the Cisco 1040; one of the following:
  - operational—Cisco 1040 is receiving RTP streams, analyzing data, and sending data to Service Monitor.
  - not communicating with receiver—The Service Monitor is unreachable.
- **Current Service Monitor**—Name of the Service Monitor to which the Cisco 1040 is sending data; this could be the primary or secondary Service Monitor.
- **TFTP IP Address**—TFTP server from which the Cisco 1040 downloads its binary image file and configuration file.
- **Switch IP Address**—Switch that this Cisco 1040 is connected to.
- **Switch Port**—Switch port that this Cisco 1040 is connected to.
- **Software Version**—Name of the binary image file installed on the Cisco 1040. See [Updating Image Files on Sensors, page 4-15](#).
- **Last Updated**—Last time that the configuration for the Cisco 1040 was updated on Service Monitor. See [Editing the Configuration for a Specific Sensor, page 4-10](#).

## Understanding How Sensors Register with Service Monitors

After you have configured a default sensor configuration file, `QOVDefault.CNF`, sensors can register with Service Monitor automatically. When a sensor registers automatically, Service Monitor uses the information in the default configuration file and creates a MAC-specific configuration file, `QOVmacaddress.CNF`, for the newly registered sensor. After a default sensor configuration file is created, if you want to add a sensor to Service Monitor manually, do so before plugging the sensor in.

After it is connected to a switch, a Cisco 1040 uses DHCP to obtain the IP address of the TFTP server. The Cisco 1040 checks the TFTP server for a configuration file, using the first of the following files that it finds:

- `QOVmacaddress.CNF`—Where MAC address is the MAC address of the Cisco 1040.
- `QOVDefault.CNF`—Default configuration file; used when a specific configuration file for the Cisco 1040 is not found (see [Setting Up the Sensor Default Configuration, page 4-4](#).)

## Understanding How a Sensor Registers with Service Monitor

A newly connected sensor registers to a Service Monitor using a specific configuration file for that sensor, `QOV<MAC address>.CNF` or using the default configuration file, `QOVDefault.CNF`. If using the default configuration file, from it, Service Monitor creates a MAC-specific configuration file, `QOV<MAC address>.CNF`, for the sensor.

There can be only one default configuration file on the TFTP server. The default configuration file specifies the primary Service Monitor. Therefore, sensors that use same TFTP server also use the same default configuration file and register with the same primary Service Monitor.

## Understanding Sensor Failover to a Secondary Service Monitor

A Cisco 1040 sends keepalive messages to the Service Monitor to which it is registered and receives acknowledgements from the Service Monitor. After sending three keepalives without receiving any acknowledgement, a Cisco 1040 starts a failover process to a secondary Service Monitor:

1. The Cisco 1040 sends a keepalive to the secondary Service Monitor that is listed in its configuration file and, upon acknowledgement, registers with that Service Monitor.
2. The secondary Service Monitor obtains the latest configuration file for this Cisco 1040 from the TFTP server, registering the Cisco 1040 as a failover Cisco 1040.
3. The Cisco 1040 starts sending syslog messages to the secondary Service Monitor while continuing to send keepalives to the primary Service Monitor to determine whether it is back up. The secondary Service Monitor processes the syslog messages from the failed-over Cisco 1040.
4. When the primary Service Monitor is back up, the Cisco 1040 unregisters from the secondary Service Monitor and registers to the primary Service Monitor again.

## Updating Image Files on Sensors

For the binary image files that are supported with Service Monitor 2.0, see *Release Notes for Cisco Unified Service Monitor 2.0* at this URL: [http://www.cisco.com/en/US/partner/docs/net\\_mgmt/cisco\\_unified\\_service\\_monitor/2.0/release/notes/SrvMonRN.html](http://www.cisco.com/en/US/partner/docs/net_mgmt/cisco_unified_service_monitor/2.0/release/notes/SrvMonRN.html).

---

**Step 1** When a new image file becomes available, download it from the Cisco software download site:

- a. Point your browser to <http://www.cisco.com>.
- b. Select **Support > Software Downloads**.
- c. Click the link for Cisco Unified Service Monitor to see and download available images.

**Step 2** Copy the image file to both of the following:

- The image file directory, `NMSROOT\CSCOpX\ImageDir`—Copy the image file here to retain a local copy as a backup. `NMSROOT` is the directory where Service Monitor is installed; its default location is `C:\Program Files\CSCOpX`.
- The TFTP server—Copy the file here to provide access to it for Cisco 1040s that are configured to use the image. For TFTP server addresses, see [Configuring TFTP Servers for Sensor Configuration and Image Files, page 4-3](#)



**Note** The image filename format is SvcMon<vendor code><Cisco 1040 type><major version>\_<minor version><bugfix version>.img; for example, SvcMonAA2\_34.img.

**Step 3** Modify the configuration for each Cisco 1040, entering the new image filename; see [Editing the Configuration for a Specific Sensor, page 4-10](#).

## Moving a Sensor from One Location to Another



### Warning

**Before moving a sensor, read the regulatory compliance and safety information in *Quick Start Guide for Cisco 1040 Sensor*.**

**Step 1** (Optional) Perform this step if you want to configure the Cisco 1040 to point to a new primary Service Monitor. Edit the configuration file for the Cisco 1040; for more information, see [Editing the Configuration for a Specific Sensor, page 4-10](#).

**Step 2** Unplug the Cisco 1040.

**Step 3** Plug in the Cisco 1040 at a new location. The Cisco 1040 downloads its configuration file from the TFTP server.



### Note

The Cisco 1040 retains its name after the move.

## Understanding Sensor Call Metrics Archive Files

Service Monitor stores the data it receives from Cisco 1040s in the database, where it remains available for reports for 30 days. Service Monitor can also save the data to files in a directory on the server if you have enabled call metrics archiving. To enable or disable call metrics archiving, see [Setting Up the Sensor Default Configuration, page 4-4](#).

Service Monitor creates a new data file daily at midnight. The data filename is QoV\_YYYYMMDD.csv where YYYY is the 4-digit year, MM is the two-digit month and DD is the two-digit day. For example, QOV\_20061101.csv is a data file for November 1, 2006. Service Monitor also backs up data files that exceed a size limit and deletes older data files; for more information, see [Understanding Sensor Archive File Purging, page 6-3](#).

You can use the data for further analysis or you can disable archiving. (Service Monitor does not send the archived data to other applications.) [Table 4-1](#) lists the format for call metrics data files.

**Table 4-1 Service Monitor Archived Call Metrics File Format**

| Description                                            | Value                                                                                                                                                                                                       |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco 1040 MAC address                                 | MAC address of the Cisco 1040 Sensor                                                                                                                                                                        |
| Time stamp                                             | Date and time                                                                                                                                                                                               |
| Source device IP address                               | IPv4 address; for example:<br>172.020.119.043                                                                                                                                                               |
| Destination device IP address                          | IPv4 address, for example:<br>172.020.119.025                                                                                                                                                               |
| Codec of call data record                              | 2: G711Alaw 64k<br>3: G711Alaw 56k<br>4: G711Ulaw 64k<br>5: G711Ulaw 56k<br>6: G722 64k<br>7: G722 56k<br>8: G722 48k<br>10: G728<br>11: G729<br>12: G729AnnexA<br>15: G.729AnnexB<br>16: G729AnnexAwAnnexB |
| Calculated MOS score                                   | 2-digit number with an implied decimal point between the first and second digit                                                                                                                             |
| Primary cause of call degradation                      | J: Jitter<br>P: Packet loss                                                                                                                                                                                 |
| Actual packet loss in the previous minute              | <numeric value>                                                                                                                                                                                             |
| Actual jitter, in milliseconds, in the previous minute | <numeric value>                                                                                                                                                                                             |

**Note**

Call metrics data files remain on disk for 30 days. Service Monitor deletes them thereafter. If you would like to save these files, you must back them up using whatever method you normally use to back up your disk. For more information, see [Understanding Sensor Archive File Purging, page 6-3](#).

## Understanding Cisco 1040 Unreachable Trap

When a Service Monitor stops receiving keepalives from a Cisco 1040 that is registered to it, the Service Monitor generates a Cisco 1040 Unreachable SNMP trap. The Service Monitor sends this trap to up to four recipients. For more information, see [Setting Up the Sensor Default Configuration, page 4-4](#) and [MIBs Used and SNMP Traps Generated, page C-1](#).

**Note**

---

If you configure Operations Manager to receive traps from Service Monitor, the Cisco 1040 Unreachable trap is displayed on the Alerts and Events monitoring dashboard under the unidentified trap device type.

---

For information on Cisco Unified CallManager reachability, see [Understanding Last Contact Status and When to Verify Credentials](#), page 3-7.