Cisco 1040 Sensor Management

This section explains the following:

Cisco 1040 Sensor Management

Cisco Prime Collaboration Assurance uses the data that it receives from Cisco 1040 Sensors to determine the voice transmission quality in your network.

For the Cisco 1040 Sensor to operate as desired, the switch connected to Cisco 1040 must be managed and configured in Cisco Prime Collaboration Assurance. For more details, see the Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide:

Note The Cisco 1040 Sensor management is not applicable if you have installed Cisco Prime Collaboration Assurance in MSP mode.

This section contains the following:

Overview of Cisco Prime NAM/vNAM

Cisco 1040 Sensor is now end of sale. For more information, see End-of-Sale and End-of-Life Announcement for the Cisco 1040 Sensor page.

The Cisco Prime NAM/vNAM replaces the Cisco 1040 Sensor and fills the missing capabilities gap. You can use Cisco Prime Network Analysis Module (NAM) and Cisco Prime Collaboration Assurance together to monitor and troubleshoot voice and other network-related issues. For more information, see the Using Cisco Prime Virtual Network Analysis Module and Cisco Prime Collaboration to Monitor and Troubleshoot Voice and Video white paper.

To know about what information you can get from the NAM reports, see NAM & Sensor Report.

Perform Initial Configuration in Cisco Prime Collaboration Assurance

For initial configuration of Cisco 1040 Sensors, do the following:

Step 1 Add one or more TFTP servers for Cisco Prime Collaboration Assurance and Cisco 1040 Sensors to use. See Configuration for TFTP Servers for Cisco 1040 Configuration and Image Files.

Step 2 Create a default configuration file. See Set Up the Cisco 1040 Sensor Default Configuration.

When a Cisco 1040 connects to the network, it downloads a configuration file from a TFTP server before registering to Cisco Prime Collaboration Assurance.

Configuration for TFTP Servers for Cisco 1040 Configuration and Image Files

Cisco Prime Collaboration Assurance uses one or more TFTP servers to provide configuration files and binary image files for Cisco 1040s. You must define at least one TFTP server for Cisco Prime Collaboration Assurance to use. You can configure additional TFTP servers if you either want a backup server or have more than one DHCP scope.

You can use the configuration files that Cisco Prime Collaboration Assurance 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 Cisco Prime Collaboration Assurance to each TFTP server that is configured for Cisco Prime Collaboration Assurance.

Add and Delete a TFTP Server

To enable Cisco 1040s to register with Cisco Prime Collaboration Assurance, you must define at least one TFTP server where Cisco Prime Collaboration Assurance can provide Cisco 1040 configuration files (and the binary image file).

Note

- Using Cisco Prime Collaboration Assurance as a TFTP server is not supported. Additionally, we recommend disabling the CWCS TFTP service on the Cisco Prime Collaboration Assurance server.
- If you plan to use Unified CM as a TFTP server, consider that:
  - You must manually copy configuration and image files from Cisco Prime Collaboration Assurance to the root location on the Unified CM TFTP server.
  - After you update files and copy them to the TFTP server, you might also need to restart the Cisco TFTP service (on Unified CM) for Cisco 1040s to be able to download the files.

Step 1 Choose **Alarm & Report Administration** > **1040 Sensor Setup** > **TFTP Servers**.
The TFTP Server Setup page is displayed.

Step 2 Click **Add**.
The TFTP Server Settings dialog box is displayed.

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 To delete, select the TFTP server and click Delete.

Set Up the Cisco 1040 Sensor Default Configuration

Use this procedure to:

- Enable or disable call metrics archiving — Cisco Prime Collaboration Assurance 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 Cisco Prime Collaboration Assurance to which a Cisco 1040 can register.

Note If you are using Unified CM software version 4.2 or later as a TFTP server, you must manually copy the default configuration file from the image file directory on the Cisco Prime Collaboration Assurance server to the root location on the Unified CM TFTP server. For more information, see step 3, in the following procedure.

To set up the Cisco 1040 sensor:

Step 1 Select **Alarm & Report Administration** > **1040 Sensor Setup**
The Setup page is displayed.

Step 2 Update data described in the following table.

Step 3 Click **OK**. Cisco Prime Collaboration Assurance stores the configuration file locally and copies it to the TFTP servers that are added to Cisco Prime Collaboration Assurance.

Cisco 1040 Sensor/NAM Setup Page—Graphical User Interface Elements

Table 1: Cisco 1040 Sensor/NAM Setup Page—Graphical User Interface Elements

Graphical User Interface Element	Description
Call Metrics Archiving	Select one of the following: • Enable — After analysis, Cisco Prime Collaboration Assurance saves data from sensors to disk files. • Disable — After analysis, Cisco Prime Collaboration Assurance discards data. Default: Disable.

Graphical User Interface Element	Description
Data File Directory	Directory where files are stored if call metrics archiving is enabled. You cannot edit this field.
Image File Directory	Directory where Cisco 1040 binary image file and configuration files are stored locally. You cannot edit this field.
Send traps every *n* minutes per endpoint	Enter a number greater than or equal to 5. Cisco 1040s send data to Cisco Prime Collaboration Assurance every 60 seconds. Cisco Prime Collaboration Assurance determines whether a violation has occurred and can potentially send a trap-a-minute for each endpoint. Use this setting to reduce the number of traps that Cisco Prime Collaboration Assurance sends for each endpoint. For a given endpoint, a trap is sent every *n* minutes and additional traps during that time are suppressed (not sent).
Default Configuration to TFTP Server	
Image Filename	Enter the image file name if you are using a new image (for example, after a product upgrade).
Primary Prime Collaboration	IP address or DNS name for the primary Cisco Prime Collaboration Assurance.

Configure Cisco 1040 Sensors in Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance analyzes data that it receives from Cisco 1040 Sensors installed in your voice network. Cisco Prime Collaboration Assurance manages multiple Cisco 1040 Sensors.

This section contains the following:

Cisco 1040 Sensor Details

To see Cisco 1040 Sensor details, choose **Alarm & Report Administration** > **1040 Sensor Setup** > **Management**. The Cisco 1040 Sensor Details page displays information listed in the following table:

Graphical User Interface Element	Description
	Exports data from the Cisco 1040 Sensor/NAM Details page to a CSV or PDF file.
	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.

Graphical User Interface Element	Description
Cisco 1040 Address columns	Displays MAC and IP addresses for Cisco 1040. Click the MAC address link to launch an HTML page on the Cisco 1040.

Prime Collaboration columns	Displays the following:
	• Primary — IP address or hostname of the primary Cisco Prime Collaboration Assurance defined for the Cisco 1040.
	• Registered with — Displays one of the following:
	  • IP address or hostname of the Cisco Prime Collaboration Assurance to which the Cisco 1040 is currently sending data.
	  • Waiting — The Cisco 1040 is not yet registered.
	  • Older Image—The binary image on the Cisco 1040 is not supported.

Reset Time column	The last date and time that Cisco Prime Collaboration Assurance sent a reset command to the Cisco 1040.
Buttons	
Add	See Add a Cisco 1040 Sensor.
Edit	See Edit Configurations for Multiple Cisco 1040s.
Delete	See Delete a Cisco 1040 Sensor.
Reset	See Reset Cisco 1040s.
Refresh	Refresh the Cisco 1040 Sensor Details page.

Restart Processes to Update Cisco 1040 Registration Information in Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance might show a Cisco 1040 Sensors 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:

  From the command line, stop the QOVR process again, by entering this command:

  ```
  pdterm QOVR
  ```

  Wait at least 5 minutes.

  Enter this command:

```
pdexec QOVR
```

- Changes the time on the system where Cisco Prime Collaboration Assurance is installed without subsequently stopping and restarting the daemon manager. To correct this problem, login as admin and execute the following commands:

```
<hostname>/admin#application stop cpcm
<hostname>/admin#application start cpcm
```

Add a Cisco 1040 Sensor

To add a Cisco 1040 Sensor to Cisco Prime Collaboration Assurance, perform the following procedure.

Step 1 Select **Alarm & Report Administration** > **1040 Sensor Setup** > **Management**.
The Cisco 1040 Sensor/NAM Details page is displayed.

Step 2 Click **Add**.
The Add a Cisco 1040 Sensor dialog box is displayed.

Step 3 Enter data listed in the following table:

Step 4 Click **OK**. The configuration file is saved on the server where Cisco Prime Collaboration Assurance is installed and is copied to all TFTP servers. (See Configuration for TFTP Servers for Cisco 1040 Configuration and Image Files.) The configuration file is named QOV<*MAC address*>.CNF, where <*MAC address*> is the MAC address for the Cisco 1040. Similarly, for updating the configuration, select one or more check boxes and click **Edit**.

Note

- Select a Cisco 1040 Sensor to edit the name or description.
- Do not edit a Cisco 1040 configuration file using a text editor.

Cisco 1040 Sensor/NAM Dialog Box—Graphical User Interface Elements Description

Graphical User Interface Element	Description
Sensor Name	Enter up to 20 characters. This name is used to identify the sensor on Cisco Prime Collaboration Assurance windows, such as reports. **Note** Cisco 1040 names must be unique. Cisco 1040s that register to Cisco Prime Collaboration Assurance using the default configuration file use the name Cisco 1040 + <*last 6 digits from MAC address*>.
Image File Name	Enter the binary image file name. The filename format is SvcMonAB2_*nnn*.img where *nnn* is a revision number.

Graphical User Interface Element	Description
MAC Address	Enter the MAC address for the Cisco 1040 that you are adding.
Primary Prime Collaboration	Enter an IP address or DNS name of a host where Cisco Prime Collaboration Assurance is installed.
Description	(Optional) Enter up to 80 characters.

Edit Configurations for Multiple Cisco 1040s

- If you use Unified CM as a TFTP server, you must manually upload the updated configuration file from the image file directory on the Cisco Prime Collaboration Assurance server to the root location on Unified CM TFTP server. Afterward, you must reset the Cisco 1040. (The image file directory is *NMSROOT*/ImageDir. *NMSROOT* is the directory where Cisco Prime Collaboration Assurance is installed; its default location is C:\Program Files\CSCOpx.) If the Cisco 1040 does not register or does not load the latest files, restart the TFTP Server.
- Do not edit a Cisco 1040 configuration file using a text editor. Edit a Cisco 1040 configuration file using this procedure only.

To edit configurations for multiple Cisco 1040s:

Step 1 Select **Alarm & Report Administration** > **1040 Sensor Setup** > **Management**.

Step 2 Select check boxes for more than one Cisco 1040 and click **Edit**.

Step 3 Update any of the fields.

Step 4 Click **OK**.
Cisco Prime Collaboration Assurance saves the configuration files on the local server copies it to all TFTP servers. Then Cisco Prime Collaboration Assurance resets the Cisco 1040s, so that they load the updated configuration.

Cisco 1040 Management - Field Descriptions

Table 2: Cisco 1040 Management - Field Descriptions

Fields	
Image File Name	Enter the binary image filename. The filename format is SvcMonAB2_*nnn*.img where *nnn* is a revision number. For the name of the most recently supported binary image file, see Cisco Prime Unified Service Monitor 2.3 Compatibility Matrix.
Primary Prime Collaboration	Enter an IP address or DNS name of a host where Cisco Prime Collaboration Assurance is installed. The Cisco 1040 sends data to this Cisco Prime Collaboration Assurance unless it becomes unreachable.

Fields	
Secondary Prime Collaboration	(Optional) Enter an IP address or DNS name of a host where Cisco Prime Collaboration Assurance is installed. The Cisco 1040 sends data to this Cisco Prime Collaboration Assurance only if the primary Cisco Prime Collaboration Assurance becomes unreachable.

Reset Cisco 1040s

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

Step 1 Select **Alarm & Report Administration** > **1040 Sensor Setup** > **Management**.

Step 2 Select check boxes for the Cisco 1040s that you want to reset.

Step 3 Click **Reset**. The Cisco 1040 will take a few minutes to complete the startup sequence, reconfigure (if necessary), and register with Cisco Prime Collaboration Assurance.

Note If you use Unified CM as a TFTP server, the Cisco 1040 Sensor does not register or does not load the most recent image file after reset. You must restart the TFTP Service on Cisco Prime Unified Communications Manager.

When you reset a Cisco 1040, Cisco Prime Collaboration Assurance sends the most recent time to the sensor. The Cisco 1040 resets its clock as needed.

Delete a Cisco 1040 Sensor

Before you delete a Cisco 1040 Sensor from Cisco Prime Collaboration Assurance, you must shut the switch port that physically connects to the 10/100-1 Fast Ethernet port on the Cisco 1040:

Step 1 To identify the port, get the switch IP address and the switch port from the Cisco 1040 web interface.

Step 2 To shut the port, use the CLI on the switch.

Note Do not delete the Cisco 1040 from Cisco Prime Collaboration Assurance until you shut the switch port.

You should also either shut or reconfigure the SPAN or RSPAN destination port on the switch. For information about configuring SPAN and RSPAN on Cisco Catalyst switches and modules, see http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml.

After you delete a Cisco 1040, it cannot automatically register again to the Cisco Prime Collaboration Assurance from which it has been deleted. To enable such a Cisco 1040 to register with this Cisco Prime Collaboration Assurance again, you must add the Cisco 1040 Sensor manually. See Add a Cisco 1040 Sensor.

To delete, select **Alarm & Report Administration** > **1040 Sensor Setup** > **Management**. Select check boxes for the Cisco 1040s that you want to delete from the Cisco 1040 Sensor Details page and click Delete.

Note Delete a Cisco 1040 Sensor from any sensor threshold groups, before you delete the Cisco 1040 Sensor.

Cisco Prime Collaboration Assurance sends a time synchronization message to each Cisco 1040 Sensor hourly. Cisco Prime Collaboration Assurance also sends a time synchronization message when a Cisco 1040 registers. A Cisco 1040 registers when it is added to the network and when it has been reset. The Cisco 1040 receives the time from Cisco Prime Collaboration Assurance and resets its clock as needed.

View Diagnostic Information on a Cisco 1040

To view the diagnostics stored on a Cisco 1040, enter http://<*IP address*>/Diagnostics in your browser, where IP address is the address of your Cisco 1040.

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

Field	Description
Current Time	Current time and date (HH:MM:SS MM/DD/YYYY).
Clock Drift	Seconds of drift and the last time and date that the clock was reset; for example, "1 second(s) updated at 9:23:37 03/16/2009".
Last Analysis Time	Time and date when the Cisco 1040 last ran an analysis.
Streams Analyzed	Number of RTP streams that were analyzed during the last interval.
Last Communication	Time and date when the sensor last received an ACK or timeSet message, or any supported message from the Cisco Prime Collaboration Assurance.
Last Successful Report Time	Time and date that the Cisco 1040 last sent data to Cisco Prime Collaboration Assurance.
Report Destination	Destination hostname or IP address and port number to which the report was sent.
Report Length (bytes)	Number of bytes in the last report record.
Received Packets	Number of packets that the Cisco 1040 received during the last interval.
Receive Errors	Number of errors received on the monitoring interface as reported by pcap.
Packets Dropped	Number of packets dropped on the monitoring interface as reported by pcap.
Buffer overruns	Number of buffer overruns on the monitoring interface as reported by pcap.

Field	Description
Framing Errors	Number of framing errors on the monitoring interface as reported by pcap.
Interface Promiscuous	Monitoring interface is in promiscuous mode (yes) or not (no).