CHAPTER 4

# Managing Cisco 1040s

The following topics are included:


- Performing Initial Configuration in Service Monitor for Cisco 1040s, page 4-1
- Configuring Cisco 1040s in Service Monitor, page 4-5
- Viewing the Configuration for a Cisco 1040, page 4-12
- Moving a Cisco 1040 from One Location to Another, page 4-16
- Understanding How Cisco 1040s Register with Service Monitors, page 4-16
- Understanding Cisco 1040 Call Metrics Archive Files, page 4-17


# Performing Initial Configuration in Service Monitor for Cisco 1040s

To configure Cisco 1040s, do the following:

1. Add one or more TFTP servers for Service Monitor and Cisco 1040s to use. See Configuring TFTP Servers for Cisco 1040 Configuration and Image Files, page 4-1.
2. Copy the binary image file from the Service Monitor server to the root location on each TFTP server that you added in step 1.
3. Create a default configuration file. See Setting Up the Cisco 1040 Sensor Default Configuration, page 4-3.

   Service Monitor copies Cisco 1040 configuration files to each TFTP server that you configure. When a Cisco 1040 connects to the network, it downloads a configuration file from a TFTP server before registering to a Service Monitor. For more information, see Understanding Cisco 1040 Registration with a Primary Service Monitor, page 4-16.

## Configuring TFTP Servers for Cisco 1040 Configuration and Image Files

Service Monitor 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 Service Monitor to use. You can configure additional TFTP servers if you either want a backup server or have more than one DHCP scope.

After you add or edit a Cisco 1040, 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 Cisco 1040s 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 Cisco 1040, page 4-13.)

You must copy the binary image file for Cisco 1040s to the root location on each TFTP server that you add to Service Monitor; see Copying the Binary Image File to the TFTP Server, page 4-3.

To manage TFTP servers, select **Configuration > Cisco 1040 > 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. See Adding a TFTP Server, page 4-2. |
| Delete button | Select a check box and click to delete the selected TFTP server. |

## Adding a TFTP Server

To enable Cisco 1040s to register with Service Monitor, you must define at least one TFTP server where Service Monitor can provide Cisco 1040 configuration files (and the binary image file). You can configure additional TFTP servers; for example, if you want a backup server or if you have more than one DHCP scope.

**Note**

- Using Service Monitor as a TFTP server is not supported. Additionally, we recommend disabling the CWCS TFTP service on the Service Monitor server. For more information, see Disabling the CWCS TFTP Service, page 6-9.
- If you plan to use a Unified Communications Manager version 4.2 or later as a TFTP server, consider that:
  - You must manually copy configuration and image files from Service Monitor to the root location on the Unified Communications Manager 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 Communications Manager) for Cisco 1040s to be able to download the files. For more information, see Restarting the TFTP Service on Cisco Unified Communications Manager, page B-13.

**Step 1** Select **Administration > Configuration > Cisco 1040 > 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

Copy the binary image file, SvcMonAB*n_nnn*.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.) For the name of the most recently supported binary image file, see *Cisco Unified Service Monitor 8.5 Compliance Matrix.*

## Deleting a TFTP Server

**Note** TFTP servers supply configuration and image files to Cisco 1040 sensors.

**Step 1** Select **Administration > Configuration > Cisco 1040 > 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 Cisco 1040 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 Cisco 1040 can register.

**Step 1** Select **Administration > Configuration > Cisco 1040s > 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:<br>• Enable—After analysis, Service Monitor saves data from sensors to disk files.<br>• Disable—After analysis, Service Monitor discards data.<br>Default: Disable. |
| Data File Directory | Directory where files are stored if call metrics archiving is enabled. You cannot edit this field.<br>**Note** Call metrics are archived to *NMSROOT*\DataDir. (*NMSROOT* is the directory where Service Monitor is installed. Its default location is C:\Program Files\CSCOpx.) |
| Image File Directory | Directory where Cisco 1040 binary image file and configuration files are stored locally: *NMSROOT*/ImageDir—*NMSROOT* is the directory where Service Monitor is installed; its default location is C:\Program Files\CSCOpx.<br>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 Service Monitor every 60 seconds. Service Monitor 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 Service Monitor 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).<br>For more information, see MIBs Used and SNMP Traps Generated, page D-1. |
| **Default Configuration to TFTP Server** | |
| Image Filename | Enter the image filename if you are using a new image (for example, after a product upgrade). |
| 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 Editing the Configuration for a Cisco 1040, page 4-9.) |

**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 Cisco 1040 Configuration and Image Files, page 4-1.

**Note** If you are using Unified Communications Manager 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 Service Monitor server to the root location on the Unified Communications Manager TFTP server. If your Cisco 1040s do not register or fail to load the latest files, see Restarting the TFTP Service on Cisco Unified Communications Manager, page B-13.

# Configuring Cisco 1040s 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*.

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.

The following information is available for managing Cisco 1040s:


- Understanding the Cisco 1040 Sensor Details Page, page 4-5
- Adding a Cisco 1040 to Service Monitor, page 4-7
- Editing the Configuration for a Cisco 1040, page 4-9
- Resetting Cisco 1040s, page 4-10
- Deleting a Cisco 1040 Sensor from Service Monitor, page 4-11


## Understanding the Cisco 1040 Sensor Details Page

To see Cisco 1040 Sensor details, select **Administration > Configuration > Cisco 1040s > 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.<br>**Note** If your client system seems unresponsive when you try to export files, see Troubleshooting File Download Issues, page 4-7. |
|  | 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 Viewing Details in Service Monitor for a Specific Cisco 1040, page 4-12. |
| 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. (See Viewing the Configuration Using the Cisco 1040 Web Interface, page 4-14.) |

| GUI Element | Description/Action |
|---|---|
| Service Monitor columns | Displays the following:<br>• Primary—IP address or hostname of the primary Service Monitor defined for the Cisco 1040.<br>• Secondary—IP address or hostname of the secondary Service Monitor defined for the Cisco 1040.<br>• Registered with—Displays one of the following:<br>– IP address or hostname of the Service Monitor to which the Cisco 1040 is currently sending data.<br>– Waiting—The Cisco 1040 is not yet registered.<br>– Older Image—The binary image on the Cisco 1040 is not supported. For more information, see *Cisco Unified Service Monitor 8.5 Compatibility Matrix*. |
| Reset Time column | The last date and time that Service Monitor sent a reset command to the Cisco 1040. |
| **Buttons** | |
| Add | See Adding a Cisco 1040 to Service Monitor, page 4-7. |
| Edit | See Editing the Configuration for a Cisco 1040, page 4-9. |
| Delete | See Deleting a Cisco 1040 Sensor from Service Monitor, page 4-11. |
| Reset | See Resetting Cisco 1040s, page 4-10. |
| Show Deleted | Displayed only if sensors that were previously registered to this Service Monitor have been deleted from it. See Viewing Cisco 1040s that Have Been Manually Deleted, page 4-9. |
| Refresh | Refresh the Cisco 1040 Sensor Details page. |

#### Restarting Processes to Update Cisco 1040 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 crmdmgtd
  Net start crmdmgtd
  ```

### Exporting Data to a CSV or PDF File

After you click the export icon, a dialog box appears. (If the dialog box does not appear, see Troubleshooting File Download Issues, page 4-7.)

**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**.

### Troubleshooting File Download Issues

If you try to export a report or other data to a file from Service Monitor and either the export dialog box or the window that prompts you to save the export file does not appear, use these procedures to try to fix the problem.

1. If you set the custom levels of security in Internet Explorer to medium or greater, the option, Automatic prompt to file download, is disabled. If you try to download a PDF or CSV file to a client system where Adobe Acrobat Reader or Microsoft Excel not installed, nothing happens. The PDF file or the spreadsheet is not displayed nor is a window that prompts you to save the file.

   To enable file download windows to display, do this on your desktop:

   a. In Internet Explorer, select **Tools > Options**.

   b. Select the **Security** tab and click **Custom Level**.

   c. Scroll to **Downloads** and for Automatic prompt to file download, select Enable.

2. If you are using Internet Explorer, Automatic prompt to file download is enabled, and the window that prompts you to save the file still does not appear, do this:

   a. Press the Ctrl key and click the OK button on the export dialog box.

   b. Continue to hold the Ctrl key down until the window that prompts you to save the file appears.

## Adding a Cisco 1040 to Service Monitor

If a Cisco 1040 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 Cisco 1040, page 4-9.

**Step 1** Select **Administration > Configuration > Cisco 1040s > Management**. The Cisco 1040 Sensor Details 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 to identify the sensor on Service Monitor windows, such as reports.<br>**Note** Cisco 1040 names must be unique. Cisco 1040s that register to Service Monitor using the default configuration file use the name Cisco 1040 + <*last 6 digits from MAC address*>. |
| Image File Name | Enter the binary image filename. The filename format is SvcMonAB2_*nnn*.img where *nnn i*s a revision number. For the name of the most recently supported binary image file, see *Cisco Unified Service Monitor 8.5 Compatibility Matrix*. For more information, see Viewing the Configuration Using the Cisco 1040 Web Interface, page 4-14. |
| 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 Viewing the Configuration Using the Cisco 1040 Web Interface, page 4-14 |
| 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 Cisco 1040 Configuration and Image Files, page 4-1.) 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 Cisco 1040 Web Interface, page 4-14.)

**Note** If you use Unified Communications Manager as a TFTP server, you must manually upload the MAC-specific configuration file from the image file directory on the Service Monitor server to the root location on the Unified Communications Manager 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.) For Cisco 1040s to load the files, you might first need to restart the TFTP server; see Restarting the TFTP Service on Cisco Unified Communications Manager, page B-13.

# Viewing Cisco 1040s that Have Been Manually Deleted

If a Show Deleted button appears on the Cisco 1040 Sensor Details page, you can use it to view any Cisco 1040 that was registered to this Service Monitor previously, but was manually deleted.

To add a previously deleted Cisco 1040 to Service Monitor again, use this procedure.

**Step 1** Click the **Show Deleted** button.

**Step 2** Select the Cisco 1040s that you want to add.

**Step 3** Click **Re-Add**.

# Editing the Configuration for a Cisco 1040

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

Use this procedure to update the configuration for one or more Cisco 1040s.

**Step 1** Select **Administration > Configuration > Cisco 1040s > Management**. (For more information, see Understanding the Cisco 1040 Sensor Details Page, page 4-5.)

**Step 2** Select one or more check boxes and click **Edit**.

**Note** To edit the name or description for a Cisco 1040, select only one Cisco 1040.

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

| Fields | Description/Action |
|---|---|
| Sensor Name | If you want to change the name, enter up to 20 characters. This name must be unique; it is used on Service Monitor windows, such as reports.<br>**Note** This field is displayed only when one sensor is selected for editing. |
| MAC Address | Cisco 1040 MAC address.<br>**Note** You cannot edit this field. (This field is displayed only when one Cisco 1040 is selected for editing.) |
| IP Address | Cisco 1040 IP address.<br>**Note** You cannot edit this field. To update the IP address for a Cisco 1040, delete the Cisco 1040 from Service Monitor and add it again. (This field is displayed only when one Cisco 1040 is selected for editing.) |

| Fields | Description/Action |
|---|---|
| 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 Unified Service Monitor 8.5 Compatibility Matrix*. For more information, see Viewing the Configuration Using the Cisco 1040 Web Interface, page 4-14. |
| 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 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.<br>**Note** This field is displayed only when one Cisco 1040 is selected for editing. |

**Step 4** Click **OK**. Service Monitor saves the configuration file on the local server and copies it to all TFTP servers. Then Service Monitor resets the Cisco 1040, so that it loads the updated configuration.

**Note** If you use Unified Communications Manager as a TFTP server, you must manually upload the updated configuration file from the image file directory on the Service Monitor server to the root location on the Unified Communications Manager TFTP server. Afterward, you must reset the Cisco 1040. (The image file directory is *NMSROOT*/ImageDir; *NMSROOT* is the directory where Service Monitor is installed; its default location is C:\Program Files\CSCOpx.) If the Cisco 1040 does not register or does not load the latest files, see Restarting the TFTP Service on Cisco Unified Communications Manager, page B-13.

# Resetting 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. 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, the Cisco 1040 also obtains the binary image file from the TFTP server.

**Step 1** Select **Administration > Configuration > Cisco 1040s > Management**. (For more information, see Understanding the Cisco 1040 Sensor Details Page, page 4-5.)

**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 Service Monitor.

**Note** If you use Unified Communications Manager as a TFTP server and, after reset, the Cisco 1040 does not register or does not load the most recent image file, see Restarting the TFTP Service on Cisco Unified Communications Manager, page B-13.

When you reset a Cisco 1040, Service Monitor sends the most recent time to the sensor. The Cisco 1040 resets its clock as needed. For more information, see Understanding When Service Monitor Provides the Time to a Cisco 1040, page 4-12.

# Deleting a Cisco 1040 Sensor from Service Monitor

Before you delete a Cisco 1040, use the information in Table 4-1 to determine whether you must first perform additional actions.

*Table 4-1 Considerations and Actions Before Deleting a Cisco 1040*

| If You Plan to Configure the Cisco 1040 to Register with… | | |
|---|---|---|
| **a Primary Receiver that Is…** | **And the Secondary Receiver Will Be…** | **Recommended Action** |
| Not this Service Monitor | One of these:<br>• Not this Service Monitor<br>• None | Ensure that the Cisco 1040 is communicating with the other instance of Service Monitor—the primary receiver—before you delete the Cisco 1040.<br>**Note** If, at a later point, you reconfigure the Cisco 1040 to use this Service Monitor as a primary or secondary receiver, you must manually add the Cisco 1040 to this Service Monitor. See Viewing Cisco 1040s that Have Been Manually Deleted, page 4-9. |
| Not this Service Monitor | This Service Monitor | Do not delete the Cisco 1040 from this Service Monitor. Otherwise, failover is delayed until a user manually adds the Cisco 1040 to this Service Monitor. |
| None | None | Before you delete the Cisco 1040, you must shut the switch port that physically connects to the 10/100-1 Fast Ethernet port on the Cisco 1040:<br>1. To identify the port, get the switch IP address and the switch port from the Cisco 1040 web interface. See Viewing the Configuration Using the Cisco 1040 Web Interface, page 4-14.<br>2. To shut the port, use the CLI on the switch.<br>**Note** Do not delete the Cisco 1040 from Service Monitor until you shut the switch port.<br>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 Service Monitor from which it has been deleted. To enable such a Cisco 1040 to register with this Service Monitor again, you must add the Cisco 1040 manually. For more information, see Viewing Cisco 1040s that Have Been Manually Deleted, page 4-9 or Adding a Cisco 1040 to Service Monitor, page 4-7.

Before you complete this procedure, delete the Cisco 1040 from any sensor threshold groups. See Editing a Sensor Group, page 5-10.

**Step 1** Select **Administration > Configuration > Cisco 1040s**. The Cisco 1040 Sensor Details page opens. (For more information, see Understanding the Cisco 1040 Sensor Details Page, page 4-5.)

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

**Step 3** 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 Cisco 1040 belongs. You will need to remove the Cisco 1040 from these sensor threshold groups and repeat this procedure.

**Step 4** Click **OK**.

## Understanding When Service Monitor Provides the Time to a Cisco 1040

Service Monitor sends a time synchronization message to each Cisco 1040 hourly. Service Monitor 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. (For more information, see Resetting Cisco 1040s, page 4-10). The Cisco 1040 receives the time from Service Monitor and resets its clock as needed.

# Viewing the Configuration for a Cisco 1040

Configuration data for a Cisco 1040 Sensor is stored in Service Monitor, is copied to a configuration file for the Cisco 1040 on each TFTP server, and is copied down to the Cisco 1040 (the Cisco 1040 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:

- Viewing Details in Service Monitor for a Specific Cisco 1040, page 4-12
- Viewing the Configuration File on the TFTP Server from a Cisco 1040, page 4-13
- Viewing the Configuration Using the Cisco 1040 Web Interface, page 4-14

In addition, you can view diagnostic information on the Cisco 1040. For more information, see Viewing Diagnostic Information on a Cisco 1040, page 4-15.

## Viewing Details in Service Monitor for a Specific Cisco 1040

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 Exporting Data to a CSV or PDF File, page 4-7. |
|  | 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 Viewing the Configuration Using the Cisco 1040 Web Interface, page 4-14. |
| 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 Editing the Configuration for a Cisco 1040, page 4-9.) |
| Registered with | IP address or DNS name for the Service Monitor that this Cisco 1040 is registered with. |
| Image File Name | Name of the image file installed on the Cisco 1040.<br>**Note** 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 Editing the Configuration for a Cisco 1040, page 4-9.) |
| Reset Time | Date and time that the Cisco 1040 was last reset. (See Resetting Cisco 1040s, page 4-10.) |
| Description | User-entered description for the Cisco 1040. (See Editing the Configuration for a Cisco 1040, page 4-9.) |

# Viewing the Configuration File on the TFTP Server from a Cisco 1040

**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 information from the configuration file on the TFTP server as listed in the table below.

| Field | Description |
|---|---|
| Retrieve | Configuration filename and the IP address from which it was downloaded. |
| Configuration file | Configuration filename. |
| 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 | 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 Cisco 1040 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 Cisco 1040, 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 4-5.
- 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.

| Field | Description |
|---|---|
| ID | Cisco 1040 MAC address. |
| MAC Address | Cisco 1040 MAC address. |
| Time stamp | Current time on the Cisco 1040.<br>**Note** The Cisco 1040 receives the hourly time synchronization message from Service Monitor and resets the time as needed. |
| Status | Status of the Cisco 1040; one of the following:<br>• operational—Cisco 1040 is receiving RTP streams, analyzing data, and sending data to Service Monitor.<br>• not communicating with receiver—The Service Monitor is unreachable. |

| Field | Description |
|---|---|
| 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. |
| Last Updated | Last time that the configuration for the Cisco 1040 was updated on Service Monitor. See Editing the Configuration for a Cisco 1040, page 4-9. |

# Viewing 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”.<br>**Note** Service Monitor sends hourly time synchronization messages to Cisco 1040s. |
| 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 Service Monitor. |
| Last Successful Report Time | Time and date that the Cisco 1040 last sent data to Service Monitor. |
| 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. |
| 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). |

# Moving a Cisco 1040 from One Location to Another

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

**Step 1** (Optional) To configure the Cisco 1040 to point to a new primary Service Monitor, edit the configuration for the Cisco 1040. For more information, see Editing the Configuration for a Cisco 1040, page 4-9.

**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 How Cisco 1040s Register with Service Monitors

After you have configured the default Cisco 1040 configuration file, QOVDefault.CNF, Cisco 1040s can register with Service Monitor automatically. When a Cisco 1040 registers automatically, Service Monitor uses the information in the default configuration file and creates a MAC-specific configuration file, QOV<*MAC address*>.CNF, for the newly registered Cisco 1040. After a default Cisco 1040 configuration file is created, if you want to add a Cisco 1040 to Service Monitor manually, do so before plugging the Cisco 1040 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:

- QOV<*MAC address*>.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 Cisco 1040 Sensor Default Configuration, page 4-3.)

## Understanding Cisco 1040 Registration with a Primary Service Monitor

A newly connected Cisco 1040 registers with a Service Monitor using a specific configuration file for that Cisco 1040 (QOV<*MAC address*>.CNF), or using the default configuration file (QOVDefault.CNF). If using the default configuration file, Service Monitor uses it to create a MAC-specific configuration file (QOV<*MAC address*>.CNF) for the Cisco 1040.

There can be only one default configuration file on the TFTP server. The default configuration file specifies the primary Service Monitor. Therefore, Cisco 1040s that use the same TFTP server also use the same default configuration file and register with the same primary Service Monitor.

# Understanding Cisco 1040 Failover Registration with 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.

# Understanding Cisco 1040 Call Metrics Archive Files

Service Monitor stores the data it receives from Cisco 1040s in the database, where it remains available for reports for a number of days; for more information, see Configuring and Viewing Other Settings, page 3-34. Service Monitor can also save the data to files in a directory on the server if you enable call metrics archiving. To enable or disable call metrics archiving, see Setting Up the Cisco 1040 Sensor Default Configuration, page 4-3.

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_20091101.csv is a data file for November 1, 2009. 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 6-5.

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 4-2 lists the format for call metrics data files.

***Table 4-2 Cisco 1040 Archived Call Metric File Format***

| Description | Value |
|---|---|
| Cisco 1040 MAC address | MAC address of the Cisco 1040 sensor |
| Time stamp | Date and time when the sensor calculated the MOS value. |
| Source device IP address | The source IP of the RTP stream being reported.<br>IPv4 address; for example:<br>`172.020.119.043` |
| Destination device IP address | The destination IP of the RTP stream being reported.<br>IPv4 address, for example:<br>`172.020.119.025` |

*Table 4-2 Cisco 1040 Archived Call Metric File Format (continued)*

| Description | Value |
|---|---|
| Codec of call data record | One of the following numbers is displayed:<br>1—NonStandard<br>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>9—G723.1<br>10—G728<br>11—G729<br>12—G729AnnexA<br>15—G729AnnexB<br>16—G729AnnexAwAnnexB<br>18—GSM Full Rate<br>19—GSM Half Rate<br>20—GSM Enhanced Full Rate<br>40—G722.1 32k<br>41—G722.1 24k<br>42—AAC<br>80—GSM<br>82—G726 32K<br>83—G726 24K<br>84—G726 16K |
| 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.<br>None: Reported when jitter and packet loss values are both 0 (zero). |
| Actual packet loss | Number of packets lost due to network transmission during the sample duration. Computed based on observed RTP sequence number analysis. |
| Actual jitter, in milliseconds | <numeric value> |

*Table 4-2 Cisco 1040 Archived Call Metric File Format (continued)*

| Description | Value |
|---|---|
| Packet Loss (%) | Percentage of packets dropped by the network on the way to the destination address. (Packets lost divided by total packets expected expressed as a percent.) |
| Adjusted Packet Loss (%) | Percentage packet loss due to high jitter; computed based on a reference jitter buffer with a fixed-length delay. This value is not affected by network loss. |
| Sample Duration(s) | Number of seconds, between the first and last packets that are analyzed. The value is usually 60, but can be less for an initial or final stream. |
| Concealed Seconds | Cisco 1040 does not report concealed seconds. |
| Severely Concealed Seconds | Cisco 1040 does not report severely concealed seconds. |
| TOS/DSCP | The IP header TOS/DSCP (QOS) byte value of the RTP stream from the first packet in the reporting interval. |
| Minimum MOS | Minimum MOS score within the sample duration; 2-digit number with an implied decimal point between the first and second digit.<br>The value might be N/A or not available if the sample duration is very short. |
| SSRC | Synchronization source ID. |
| Source UDP Port | Transport layer source port of the media stream. |
| Destination UDP Port | Transport layer destination port of the media stream. |
| Peak to peak packet jitter | Highest single instance of packet jitter in the media stream. Given a uniform network delay of 100 ms for packets in a media stream, if a single packet experiences a total delay of 110 ms, the reported peak to peak packet jitter value would be 10 ms. |

**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 6-5.