CHAPTER 5

Managing Devices

A *device* is a Cisco IOS device that supports Cisco IOx. You can install Cisco IOx apps on these devices only.

The Cisco Fog Director Device pages provide information about devices, and provide access to features for monitoring and troubleshooting devices, and for administering apps on devices.

To access the Devices pages, log in to Cisco Fog Director as described in the "Accessing Cisco Fog Director" section on page 3-1, and then click the **DEVICES** tab. The Devices View page displays.

This chapter includes these sections:77

- Viewing General Information about Devices, page 5-2
- Viewing Detailed Information about a Device, page 5-5
- Adding Devices, page 5-16
- Importing Devices, page 5-18
- Editing Attributes for a Device, page 5-20
- Managing Device Profiles, page 5-21
- Rediscovering Devices, page 5-32
- Editing Devices, page 5-33
- Deleting Devices, page 5-37
- Managing Tags for Devices, page 5-38
- Starting or Stopping an App on a Device, page 5-40
- Removing an App from a Device, page 5-41
- Deleting Unused Cartridges, page 5-42
- Managing Layers, page 5-42
- Recovering an App on a Device, page 5-43
- Viewing Diagnostic Information, page 5-44
- Obtaining Device Logs, page 5-48
- Accessing an App via a Console, page 5-48

Cisco Fog Director Reference Guide, Release 1.11

5-1

Viewing General Information about Devices

The Devices View page, which displays when you choose the **DEVICES** tab in Cisco Fog Manager, provides general information about devices that have been added or uploaded to Cisco Fog Manager.

This page includes the items that Table 5-1 describes.

Table 5-1   Devices View Page Items

Item	Description
Reachability chart	Number of devices with which Cisco Fog Director can communicate (shown as *In Contact*), and number of devices with which Cisco Fog Director cannot communicate (shown as *Lost Contact*).
	Click any section of the graph or a device number to filter the devices that display in the Device table by the corresponding reachability status.
Last Heard chart	Number of devices with which Cisco Fog Director successfully interacted with during the past 0 to 1 days, 2 to 7 days, 8 to 28 days, and 29 more days.
	(Cisco Fog director considers a device that it has not successfully communicated with for more than 28 consecutive day as having never been communicated with.)
	Click any section of the graph or a number in the Devices column to filter the devices that display in the Device table display in the Device by the corresponding period.
Platform version chart	Platform versions of devices in your deployment.
	Click any section of the graph or a platform number to filter the devices that display in the Device table by the corresponding value.
Add New Device button	Displays the Adds New Device window, which you use to add a device to Cisco Fog Director. See the "Adding Devices" section on page 5-16.
Import Devices button	Lets you add devices to Cisco Fog Director by importing a CSV file in which information for the devices is defined. See the "Importing Devices" section on page 5-18.

***Table 5-1   Devices View Page Items (continued)***

| Item	Description
Additional Actions button ⸽⸽⸽	Displays the following options:
	• **Re-Discover**—Choose this option to cause Cisco Fog Director discover device information, capabilities, and app states for a selected set of devices. See the "Rediscovering Devices" section on page 5-32.
	• **Edit**—Choose this option to update user name, password, port, and contact information for a selected set of devices. See the "Editing Devices" section on page 5-33.
	• **Tag**—Choose this options to add a tag to or remove a tag from multiple devices. See the "Managing Tags for Devices" section on page 5-38.
	• **Delete**—Choose this option to delete multiple devices from Cisco Fog Director inventory. See the "Deleting Devices" section on page 5-37.
	• **Profiles**—Choose this option to manage device profiles for devices. See the "Managing Device Profiles" section on page 5-21.
Top 5 Consumers	Displays only if Cisco Fog Director can obtain this information, and includes the following charts, which provide information about resources that IOx apps consumed on devices during the past 24 hours. Hover your mouse pointer over any circle in a chart to see the hostname of the device for which that circle provides information. Double-click any circle in a chart to display detailed information about the device for which that circle provides information, as described in the "Viewing Detailed Information about a Device" section on page 5-5.
	• CPU—Shows the percentage of CPU resources consumed by apps for the five devices on which the apps consumed the most resources
	• Memory—Shows the memory, in KB, consumed by apps for the five devices on which the apps consumed the most memory
	• Disk—Shows the disk space, in MB, consumed by apps for the five devices on which the apps consumed the most disk space
	• Network—Shows the network bandwidth, in KB, consumed by the five devices that consumed the most bandwidth when running apps
Device Filters field	Click this field and then choose from the available options to display in the Device table only devices that meet designated criteria. When you choose an option, it displays in the Device Filters field and the Device table updates automatically. You can add as many device filter options as needed. To remove a device filter option from this field, click the X icon ✕ next to the option.

Table 5-1   ***Devices View Page Items (continued)***

Item	Description
Device table	Provides information about each device that has been added to Cisco Fog Director. This table includes the following: • Search Hostname, IP Address field—Type all or part of a hostname or IP address of a device to display information for devices with matching information. The table display updates as you type. • All Tags field —Enter the name of a tag and then press the **Enter** key to display information for devices with a matching tag. You can display a drop-down of tags that you can choose typing the first few letters of the tag. • Host Name—Hostname of the device. Click a hostname to display detailed information about the device. See the "Viewing Detailed Information about a Device" section on page 5-5. • IP Address—IP address of the device. Click a hostname to display device detailed information about the device. See the "Viewing Detailed Information about a Device" section on page 5-5. • Tags—Tags for the device. See the "Managing Tags for Devices" section on page 5-38. • Capacity—Icons that represent information about CPU use or memory use on the device. Hover your mouse pointer over an icon to see more detailed information. • Last Heard—How long ago Cisco Fog Director last communicated with the device, or a brief explanation of why the last attempt to communicate with the device was unsuccessful. • Pagination controls—Click a control to go to the first, next, last, previous, or specific page in the table. • Items per page drop-down list—Choose the maximum number of devices that appear in each page of the table. To see additional information about a device or access various functions for a device, click the Expand icon ⌃ to the left of the device hostname in the Device table. The following row in this table describes the items that appear.

Table 5-1   Devices View Page Items (continued)

Item	Description
Expanded device information and functions	The following items appear when you click the Expand icon ⌄ to the left of the device hostname in the Device table:
	• **Delete Device**—Click to remove the device from Cisco Fog Director. See the "Deleting Devices" section on page 5-37.
	• **Edit Device**—Click to edit various attributes for the device. See the "Editing Attributes for a Device" section on page 5-20.
	• **Refresh Device**—Click to cause Cisco Fog Director to rediscover the device and update information that displays.
	• Installed Apps information and controls—Provides the following for each app that is installed on the device
	– App—Name of the app.
	– Downtime - today—Amount of time during the past 24 hours that the app was in Stopped state.
	– CPU - mean % today—Average (mean) percentage of CPU resources that the app used on the device during the past 24 hours.
	– Memory - mean Kb today—Average (mean) memory (RAM) in KB, that the app consumed on the device during the past 24 hours.
	– Status—State of the app.
	– Action—**Stop** button ▪ , **Start** button ▶ , **Remove** button ✖ , depending on the state of the app. See the "Starting or Stopping an App on a Device" section on page 5-40 or the "Removing an App from a Device" section on page 5-41.

Viewing Detailed Information about a Device

To view detailed information about a device, take either of these actions:

- On the Devices View page, double-click a circle in a Top 5 Consumers chart. Detailed information displays for the device for which that circle provides information. (This chart displays only if Cisco Fog Director can obtain this information.)

- On the Apps View page or the Devices View page, click the hostname or the IP address of a device anywhere that either of these items displays as a link.

The Device Details page displays. This page includes information and features that apply to the app, as the following sections describe:

- Device Details Area, page 5-6

- Apps Area, page 5-11

Device Details Area

The Device Details area on the Device Details page provides detailed information about a device, and includes the items that Table 5-1 describes.

If service packages have been installed for an app on a device, this area also provides information about each service package. For more information, see, *IOx Services Architecture*, which is available here: https://developer.cisco.com/docs/iox/#iox-services-architecture/iox-services-architecture.

Table 5-2   Device Details Area Items

Item	Description
Host Information Items	
Version	Version of the app that is installed on the device.
Contact Person	Name of the person who is responsible for the device or the app.
IP Address	IP address of the device
Port	Port on which Cisco IOx runs on the device

Table 5-2   Device Details Area Items (continued)

Item	Description
Profile	Shows the name of the device profile that is associated with the device.
	Hover your mouse pointer over the name to see the following summary information about the device profile:
	• Name—Name of the device profile.
	• Events collection frequency—How often Cisco Fog Director collects events information from a device. This information is shown in various summary and detail displays throughout Cisco Fog Director.
	• Metrics collection frequency—How often Cisco Fog Director collects metrics information such as CPU, memory, and network resource use from a device. This information is shown in various summary and detail displays throughout Cisco Fog Director.
	• Heartbeat miss count—Number of consecutive failed attempts by Cisco Fog Director to poll a device after which Cisco Fog Director indicates that it has lost contact with the device.
	• Default timeout—Amount of time, in seconds, after which Cisco Fog Director generates an error if it does not receive a response to a request that it sends to a device.
	• File transfer timeout—Amount of time, in seconds, after which Cisco Fog Director generates an error if an attempt to transfer an app, service, or cartridge file from Cisco Fog Director to a device does not execute.
	• Auto recovery—Shows **true** if the auto recover feature is enabled or **false** if it is not enabled.
	• Verify application signature—Shows **true** if the verify app signature feature is enabled or **false** if it is not enabled.
	• Trust anchor name—If the verify app signature feature is enabled and you have uploaded a trust anchor, shows the name of the trust anchor.
	• Trust anchor checksum—If the verify app signature feature is enabled and you have uploaded a trust anchor, shows the checksum value of the trust anchor.
	• Default profile—Shows **true** if this device profile is the default or **false** if it is not the default.
	For related information, see the "Managing Device Profiles" section on page 5-21.
Resource Usage	
Resources charts	Shows the amount of CPU (in units), memory (in MB), and disk (in MB) resources that are in use and available for apps on the device. Hover your mouse pointer over a chart to see more detailed information.

Table 5-2   Device Details Area Items (continued)

Item	Description
Show Advanced/Hide Advanced toggle button	Click **Show Advanced** to display the DEVICE DETAILS, LAYERS, CARTRIDGES, and OUTSTSANDING ACTIONS tabs, and Troubleshooting items. Click **Hide Advanced** to collapse this expanded display.
SSD wear level message	This message appears when the Cisco IOx framework detects that the SSD in the host system is nearing the end of its expected lifetime, if the host system supports obtaining and sending this information. When the expected remaining lifetime of an SSD is between 6% and 15% of its total expected lifetime, a warning-level message appears. When the expected remaining lifetime of an SSD is 5% or less than its total expected lifetime, a critical-level message appears.
Tabs	
DEVICE DETAILS tab	Displays the following information: • Last Heard—How long ago Cisco Fog Director last communicated with the device, or a brief explanation of why the last attempt to communicate with the device was unsuccessful • Serial number—Serial number of the device • Managed by—Shows Fog Director if the device is managed by Cisco Fog Director, or shows the name of a third-party manager if the device is managed by that manager • Tags—Tags that are assigned to a device • Description—Description of the device that was entered when the device was added to Cisco Fog Director • IOx Release—Cisco IOx version that is running on the device, if the device provides this information

Table 5-2   Device Details Area Items (continued)

Item	Description
LAYERS tab	Displays the following fields and buttons, which allow you to manage layers that are on a device.
	For related information, see the "Managing Layers" section on page 5-42.
	• Check boxes—Check the check box for each layer that you want the DELETE SELECTED LAYERS action to affect. You can click the check box at the top of the list of layers to quickly check boxes for all layers.
	• LAYER ID—Content-addressable identifier of the layer.
	• SIZE—Amount of disk space that the layer consumes on the device, in KB.
	• USAGE—Status of the layer:
	– **IN USE**—At least one app in Running state is using the layer
	– **NOT IN USE**—No installed app is using the layer
	• Pagination controls—Click a control to go to the first, next, last, previous, or specific page in the list.
	• Items per page drop-down list—Choose the maximum number of devices that appear in each page of the list.
	• **DELETE SELECTED LAYERS**—Click to delete each layer with a status of NOT IN USE for which the corresponding check box is checked.
	• **DELETE ALL UNUSED LAYERS**—Click to delete all layers that are not used by any app that is installed on the device.
CARTRIDGES tab	Displays for devices that provide native Docker support and includes the following (see Chapter 7, "Managing Cartridges," for more information about cartridges):
	• Cartridges—Number of cartridges that are installed on the.
	• NAME—Name of each cartridge. Hover your mouse pointer over a cartridge name to see detailed information about the cartridge.
	• VERSION—Version number of each cartridge.
	• SIZE—Size, in MB, of each cartridge.
	• USAGE—Indicates whether the cartridge is in use by any app on the device.
	• **DELETE UNUSED CARTRIDGES** button—Removes all unused cartridges from the device. See the "Deleting Unused Cartridges" section on page 5-42.

Table 5-2   Device Details Area Items (continued)

Item	Description
OUTSTANDING ACTIONS tab	Displays the following information. For related information, see the "Managing Outstanding and Expired Actions for Apps" section on page 4-54. • Outstanding Actions—Number of actions that are in Outstanding state on this device. • Outstanding Actions table—Includes these items: – Check box—Check the check box for each app for which you want to cancel additional retries of the corresponding action on the device. You can click the check box in the title row of the table to quickly check all boxes in the table. – App—Name of the app to which the outstanding action relates. – Action—Type of the outstanding action (**Install**, **Edit**, **Upgrade**, or **Uninstall**). – Next Attempt at—Date and time that Cisco Fog Director will next attempt to perform the action on the device, according to the action plan that is in effect for this action. – Pending Attempts—Maximum number of additional times that Cisco Fog Director will attempt to perform the action on the device, according to the action plan that is in effect for this action. • **CANCEL OUTSTANDING** button—Click to stop Cisco Fog Director from retrying the action on the devices that are listed in the Selected Devices table. Choosing this option cancels the action plan that is in effect for the action on this device and moves the action on this device to Expired state.
Troubleshooting Items	
Launch Local Manager link	Opens the Cisco IOx Local Manager application in a new browser tab or window. This application is installed on a device as part of the installation of the Cisco IOx framework on that device. It provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot apps on the host system, and to perform a variety of related activities. For detailed information about this application, see *Cisco IOx Local Manager Reference Guide*.
Collect Debug Logs	Turns Cisco IOx debug log collection on or off for the device. See the "Obtaining Device Logs" section on page 5-48.
Download Tech Support Logs button	Click to obtain a log file that contains log information that was generated by the device. If the Collect Debug Logs option is set to **Yes** on this Device Details page, the log file also includes debug information. See the "Obtaining Device Logs" section on page 5-48.

Table 5-2   Device Details Area Items (continued)

Item	Description
View Device Logs button	Click to display a window that lets you view log information that is generated by the device. If the Collect Debug Logs option is set to **Yes** on this Device Details page, the device log also includes debug information. See the "Obtaining Device Logs" section on page 5-48.
Device Diagnostics button	Click to display the Diagnostics window, which lets you view diagnostic information about errors, events, memory, disk operation, processes, networking, apps, app manager jobs, and app lifecycle tasks on the device. See the "Viewing Diagnostic Information" section on page 5-44.
Refresh Device button	Click to cause Cisco Fog Director to rediscover the device and update information that displays on the Device Details page.

Apps Area

The Apps area on the Device Details page includes the items that Table 5-3 describes for each Cisco IOx app that is installed on the device. Some items might not appear depending on your deployment.

To display the items for an app, click the **Expand** button ⌄ next to the app name. To hide the items for an app, click the **Collapse** button ⌃ next to the app name.

Table 5-3   Apps Area Items

Item	Description
App/Service Details Items	
App icon, name, and version	Displays the name and version of the app and an icon for the app. Click an app icon to display more detailed information about the app and to access features for managing the app, as described in the "Viewing Detailed Information about an App" section on page 4-5.
Start button	Start the app, which initiates its operation on the device and puts the app in Running state.
Stop button	Stops the app, which shuts down its operation on he device and puts the app in Stopped state. You cannot stop an app that provides services if the services that it provides are being used by one or more other apps that are in Running state. To stop an app that provides services, first stop each app that uses the services that it provides.
Uninstall button	Appear only for an app that is not in Running state. Removes the app from the device. See the "Removing an App from a Device" section on page 5-41.
Status	Status of the app (for example, RUNNING).

Table 5-3   Apps Area Items (continued)

Item	Description
Health	Health state of the app on the device. Health states are: • **HEALTHY**—App is operating normally on the device. • **UNHEALTHY**—Appear only if the app includes an app monitoring script and the script has determined that there is a problem with the health of the app. See the "App Health Script" section on page 1-2 for related information. • **CORRUPTED**—Cisco Fog Director has detected that the app is corrupted but has not taken a recover action • **CORRUPTED_RECOVERY_NOT_ATTEMPTED**—Cisco Fog Director detected that the app is corrupted but cannot take a recovery action because the app is in the unmanaged state. (An app is in unmanaged state when it has been imported to a device by a method other than by using Cisco Fog Director.) • **CORRUPTED_RECOVERY_FAILED**—Cisco Fog Director detected that the app is corrupted and performed an auto recovery, but the auto recovery was not able to recover the app. The following links can appear to the right of certain health states: • **Recover**—Appears if Cisco Fog Director determines that the app is corrupted and if auto recovery is not enabled or an auto recovery action did not recover the app. Click to execute a manual recovery action. See the "Recovering an App on a Device" section on page 5-43. • **Show report**—Appears if an app includes an optional monitor script and the script has determined that the app is unhealthy. (Therefore, this link appears only for apps in the UNHEALTHY state.) Click to display the App Health window, which provides information about the health of the app. In this window: – The top line displays a app monitor script status code of 1 if a health script is included in the app package or a code of 0 if a monitor script is not included. This line also displays how long ago the information in this window was captured. – Click **STANDARD ERROR** to display the standard error that is generated by app monitor script. – Click **STANDARD OUTPUT** to display the standard output generated by app monitor script. • In the App Health window, you can click the **STANDARD ERROR** tab to display the error information output of the monitor script. You click the **STANDARD OUTPUT** tab to display the health information output of the monitor script.
Type	Type of the app.
Installed on	Date and time that the app was installed on the device.
Last Upgrade	Date and time that the app was upgraded on the device.
Version	Version number of the app.
Cartridges Used	Cisco cartridges that the app requires to run, if any.
Links	App links configured for the app, if such links were configured in a previous version of Cisco Fog Director that supported app link configuration.

Table 5-3   Apps Area Items (continued)

Item	Description
Services Bundle Used	Appears if the app requires services that are provided by another app. Hover your mouse pointer over this text to see the name and version number of the app that provides the services.
Used By	Appears for a app that provides services. Hover your mouse pointer over this text to see the name and version number of each app that requires the services that this app provides.
Resource Profile	Resource profile that is configured for the app. Hover your mouse pointer over the resource profile name to see system CPU and memory (RAM) resources that the app requires on the device.
Network Interface	Includes these items: • Network Interface drop-down list—Choose an app internal interface for which you want to view information. This options that appear in this list come from the package.yaml file for the app. • App IP—IP address that is assigned to the app on the device for the network interface that you choose. • Ports—Hover your mouse pointer over **Ports** to see port asked and port mapping information for TCP ports and UDP ports for the network interface that you choose. **Port Asked** is the port that the app requests in its package.yaml file. **Mapped Port** is the port is the port to which you mapped the port, if you mapped ports when you performed an install app or reconfigure app procedure. These ports are used for external communication with the app. • mac—MAC address that is assigned to the app on the device for the network interface that you choose. • Network Mode—Network mode that is assigned to the app for the network interface that you choose. • Network name—Name of the VLAN, if configured. Otherwise, the name of the network bridge. • Mirroring—Displays **true** if you enabled port mirroring when you performed an install app or reconfigure app procedure. Displays **false** if you did not enable port mirroring.
Serial Port	Dedicated serial port that is assigned to the app.
USB Port	Dedicated USB port that is assigned to the app.
USB Device	External USB device that is assigned to the app.
Refresh App button	Click to cause Cisco Fog Director to rediscover the device and update information that displays in the Apps area.

Table 5-3   Apps Area Items (continued)

Item	Description
App Configuration Items	
Edit Settings tab	Lets you reconfigure specific items that are defined for an app. This area does not appear for apps that were installed out of band from Cisco Fog Director.
	Items that you can reconfigure include:
	• Resource Profiles—Resource profile for the app.
	• Network Configuration—Network information that relates to how the app obtains its IP address or addresses on each device, and TCP and UDP port mapping, and mirroring.
	The TCP port and UDP port fields appear if a NAT network is selected. These fields let you map the corresponding ports that the app descriptor file (package.yaml) for the app defines to other valid ports. These ports are used by the network interface for external communication. The values that these fields display come from the app descriptor file for the app or are the values to which you mapped the values from the package.yaml file for the app. If is file defines a range of ports, for example, 9000-9200, you must enter a range that includes the same number of ports, for example, 9400-9600. Valid TCP and UDP port numbers are 1 through 65535.
	The Mirror Mode Enabled check box appears if a bridge network is selected. This check box lets you enable port mirroring for the app.
	If a bridge network is selected and the device on which you are installing the app supports a VLAN on this network, in the **Vlan ID** field that appears, enter the unique identifier of the VLAN on which this internal network operates. Valid values are integers 1 through 4094.
	If the device on supports a VLAN on this network interface, the Vlan ID lets you enter the unique identifier of the VLAN on which this internal network operates. Valid values are integers 1 through 4094
	• Serial Configuration—Device serial port that the app uses.
	• VNC Password—VNC password that is required to access an app on the device via a VNC session.
	• VCPU Configuration—Number of virtual CPUs that the app requires on a device.
	• Docker Runtime Options—One or more Docker run options to be used when the app starts. If you enter more than one option, separate each option with a space.
	This field includes the --rm option by default.
	a. Remove writable layer on container stop—If checked, the writable container layer is removed from the app container when the app is stopped.
	Checking this check box to adds the --rm run option to the Docker Run Options field.
	If you make changes in this tab, click the **Reconfigure Settings** button to send the updated information to the device.
	For detailed information about these settings, see the "Install App Procedure" section on page 4-13.
Edit Configuration tab	Lets you update configuration for the app. The items that display are defined in the package.yaml file for the app.

Table 5-3   *Apps Area Items (continued)*

Item	Description

App Log tab
 	
(This tab name displays the name of a log files that was generated by the app.)
	By default, displays the last 10 lines of a log file that was generated by the app on the device.
	
	This area includes these items:
	
	• Drop down list—Choose an option to update the log file display (**Last 10 lines**, **Last 25 lines**, **Last 100 lines**, or **Full log**).
	
	• **Refresh** button—Click to update the log file display with current information.
	
	• **View all App Logs**—Click to display the App Logs window, which that contains the following items:
	
	  – Log file list—Name of each log file that was generated by the app on the device. Click a file name to display content from that file.
	
	  – Log displays area—By default, displays the first 10 lines of the log file that is selected in the list. This area displays information for the first file in the Log File list when you first access the View all App Logs window.
	
	  – Drop down list—Choose an option to update the log file display for the selected file (**Last 10 lines**, **Last 25 lines**, **Last 100 lines**, or **Full log**).
	
	  – **REFRESH** button—Click to update the log file display with current information for the selected file.

MANAGE APP DATA tab	Lets you upload one or more app data files for the app. An app data file is a file that an app requires, such as a configuration file. This area includes these items: • **Delete all files in /appdata** check box—Check this check box if you want Cisco Fog Director to delete all files and subdirectories that are in the /data/appdata directory on a device before uploading an app data file. • **File path on app container** field—Optionally enter the name of a directory under the /data/appdata directory on the device in which to upload the app data file. If you enter the name of a directory that does not exist, Cisco Fog Director creates that directory under the /data/appdata directory. If you do not enter the name of a directory, Cisco Fog Director uploads the file to the /data/appdata directory • **New file name** field—Optionally enter a name to which Cisco Fog Director changes the name of the file that you upload when that file is placed on the device. If you do not enter a file name, Cisco Fog Director does not change the original name of the uploaded file. For example, if you upload a file that is named abc.txt but you want the file to be stored as abc_ver2.txt, enter **abc_ver2.txt** in this field • **SELECT FILE** button—Click and then follow the on-screen prompts to locate and select the app data file that you want to upload. Each file that you select appears in a list of files to upload under the SELECT FILES button. To remove a file from this list, click the Remove icon ✕ next to the file. • **Upload** button—Click to upload the app data file. You can use these fields to upload as many app data files as needed.
View all App Logs	Displays all logs that the app generates on the device Click **Refresh** to update the display with current information.

Table 5-3   Apps Area Items (continued)

Item	Description
App Downtime Items	
Displays if Cisco Fog Director can obtain this information.	
App Downtime chart	Shows the states that the app was in on the device over the past month. Hover your mouse pointer over any section of a chart to see the name of the state, the date and time that the app entered the state, and the amount of time the app was in the state.
View Audit Details button	Click to display detailed information about operations that affected the app, including who performed the operation (Who column), what the operation was (What column), when the operation occurred (When column), and a brief system message relating to the operation (Message column).
	When detailed information displays, you can choose an option from the **Show** drop-down list to display only operations whose "What" information corresponds to that option. Choose **All** to display information for all operations.
	Click a control to go to the first, next, last, previous, or specific page in the list of detailed operations. From the **Items per page** drop-down list, choose the maximum number of device profile that appear in each page of the list.
Collapse button	When detailed information about operations that affected the app displays, click to hide the detailed information.
App Consumption Items	
App Consumption charts	The following charts provide information about device resources that the app consumes:
	• CPU Consumption—Percentage of CPU resources that the app used on the device during the designated time period.
	• Memory Consumption—RAM resources, in KB, that the app used on the device during the designated time period.
	• Disk Consumption—Hard disk space, in MB, that the app used on the device during the designated time period.
	• Network Consumption—Network bandwidth, in bytes, that the device used for the app during the designated time period.
	You can click **Day**, **Week**, or **Month** above these charts to designate the time period for the information that the charts display.
	Hover your mouse pointer over any part of a chart to see detailed information about a data point.
App Console Support Items	
Enable Debug Option	Turns app debug log collection on or off.
Command and links	Displays the command that you can use to access the app via a console. See the "Accessing an App via a Console" section on page 5-48.

Adding Devices

Adding a device makes it manageable by Cisco Fog Director and available for the installation and running of IOx apps.

All devices that you add to Cisco Fog Director should be configured to synchronize their time from same NTP server. In this way, Cisco Fog Director can accurately aggregate data from the servers.

To add a device, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Add New Device** button.

The Add New Device window displays.

Step 3   In the Add New Device window, enter information for the device to add, as described in the following table:

Field	Description
IP Address	Required. IP address of the device to be added.
Port	Required. HPPTS port on which Cisco IOx runs on the device.
	Valid values are 0 through 65535. The default port is 844.
Username	Required. Cisco IOS user name that is configured on the device.
Password	Required. Cisco IOS password that is configured on the device.
Tags	Optional. One or more tags for the device. (See the "Managing Tags for Devices" section on page 5-38 for an explanation of tags.)
	To enter more than one tag, separate each tag by pressing the **Tab** key.
Serial Number	Serial number of the device.
	Required if Verify Serial Number is enabled in the device profile for the device. For related information, see the "Managing Device Profiles" section on page 5-21.
Network Element ID	Identifier of the network element for the device.
	This ID typically uses a hierarchical naming convention, for example, us-west.cal.ne1. Space, hyphen (-), and underscore (_) characters are not allowed. The maximum length is 135 characters.
Contact Details	Optional. Contact information of the person who is responsible for the device.
Description	Optional. Brief description of the device.
Profile	Device profile to associate to the device. If you do not specify a device profile, the default device profile is used.
	To enter a device profile, start typing the name of the profile to display profiles that begin with the characters you type, then click the one that you want.
	For related information, see the "Managing Device Profiles" section on page 5-21.

Step 4   In the Add New Device window, take one of these actions:

- To save the information you entered, add the device, and exit the window, click the **Save & Close** button.

- To save the information you entered, add the device, and clear the fields in the window, click the **Save & Add More** button. Now you can enter information for another device to add.

- To clear the fields in the window and exit the window without adding the device, click the **Cancel** button.

Importing Devices

Importing devices provides you with a convenient way to add several devices to Cisco Fog Director at once. The import process involves creating a comma-separated value (CSV) file that includes information about each device to be added, and then importing that file to Cisco Fog Director.

The following sections provide detailed information:

- Creating an Import File, page 5-18

- Importing an Import File, page 5-19

Creating an Import File

To import devices to Cisco Fog Director, you begin by creating a CSV import file. This file includes one record for each device that is to be added Cisco Fog Director.

Cisco Fog Director provides a sample CSV file that you can use to create your own file.

We recommend that you use Microsoft Excel to edit the sample CSV file, then use the Save As command in Excel to save the file as a **CSV (Comma delimited)** type.

An import file must adhere to these guidelines:

- The file must be comma delimited.

- Lines preceded with a pound sign (#) are comment lines and are ignored by the import process.

- Each record must include each field that the following procedure describes. The fields must be in the order shown. A field that is indicated as "Optional" can be blank.

To use the sample CSV file to create an import file, perform the following steps.

> **Note** For security reasons, you may not want to include valid user name, password, port, or contact information when you create an import file. In this case, use dummy values in these fields and do not check the **Discover devices after import** check box when you import the import file. Then, after you import the import file, you can use the Device Edit feature to update these values for the devices. For more information, see the "Editing Devices" section on page 5-33.

Procedure

Step 1 In Cisco Fog Director, click the **DEVICES** tab.

Step 2 On the Devices View page, click the **Import Devices** button.

The Import window displays.

Step 3 Click **Download Sample CSV** at the bottom right of the Import window and follow the on-screen prompts to open a sample CSV file or save it in to the location of your choice.

Step 4 If you saved the sample CSV file, open it with Microsoft Excel or another editor that can open a CSV file.

Step 5 For each device to be added, create a record for it that includes the following information:

Field	Description
ipv4_address	Required. IP address of the device.
https_port	Required. HTTPS port on which Cisco IOx runs on the device.
	Valid values are 0 through 65535. The default port is 844.
https_username	Optional. Cisco IOS user name that is configured on the device.
	If you do not include user names in the CSV file, you can enter a user name for a device in the Edit Device dialog box for the device. See the "Editing Attributes for a Device" section on page 5-20.
https_password	Optional. Cisco IOS password that is configured on the device.
	If you do not include passwords in the CSV file, you can enter a password for a device in the Edit Device dialog box for the device. See the "Editing Attributes for a Device" section on page 5-20
tags	Optional. One or more tags for the device. (See the "Managing Tags for Devices" section on page 5-38 for an explanation of tags.)
	If you include more than one tag, separate each tag with a comma.
	Enclose the tag or tag string of tags with double quotation marks (").
contact_details	Optional. Contact information of the person who is responsible for the device.
description	Optional. Brief description of the device.
device_serial_number	Serial number of the device.
	Required if Verify Serial Number is enabled in the device profile for the device. For related information, see the "Managing Device Profiles" section on page 5-21.

Step 6 Save the import file as a **CSV (Comma delimited)** type in the location of your choice.

You can give this file any valid Windows file name.

Importing an Import File

After you create an import file as described in the "Creating an Import File" section on page 5-18, you can import the file to Cisco Fog Director. Doing so adds the devices that the file defines to Cisco Fog Director.

If the import file includes a record for a device that already exists in Cisco Fog Director, the information for that device is updated with the information in the record.

To import an import file, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Import Devices** button.

The Import window displays.

Step 3   Check the **Discover devices after import** check box if you want Cisco Fog Director to discover the devices after they are imported.

If you do not choose to discover the devices now, you can discover them later as described in the "Rediscovering Devices" section on page 5-32. By choosing not to discover devices now, you can avoid storing user names and passwords in the import CSV file.

Step 4   Click the **Select devices csv** button and follow the on-screen prompts to locate and select the CSV file that you want to import.

Editing Attributes for a Device

Editing attributes for a device lets you update various information for the device.

To edit device information, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   In the Device table, click the **Expand** icon ⌃ to the left of the hostname of the device for which you want to edit attributes.

Step 3   Click **Edit Device**.

The Edit Device dialog box displays. This dialog box shows information that relates to the device and provides fields in which you can enter or update information.

Step 4   In the Edit Device dialog box, enter information in the following fields as needed:

- **IP Address**—IP address of the device.

- **Port**—HTTPS port on which Cisco IOx runs on the device.

  Valid values are 0 through 65535. The default port is 844.

- **Username**—Cisco IOS user name that is configured on the device.

- **Password**—Cisco IOS password that is configured on the device.

- **Serial Number**—Serial number of the device.

- **Network Element ID**—Identifier of the network element for the device. This ID typically uses a hierarchical naming convention, for example, us-west.cal.ne1. Space, hyphen (-), and underscore (_) characters are not allowed. The maximum length is 135 characters.

- **Contact Details**—Contact information of the person who is responsible for the device.

- **Description**—Brief description of the device.

Step 5   In the Edit Device dialog box, take either of these actions:

- Click the **Save & Close** button to save your changes and exit the dialog box

- Click the **Close** button to exit the dialog box without saving your changes

Managing Device Profiles

A device profile is a set of events monitoring, metrics monitoring, communication, and security configuration settings that can be associated with one or more devices.

There is always a device profile called "System Default Profile" that associated with a device if the device does not have another device profile associated with it.

- Device Profile Configuration Options, page 5-21

- Adding a Device Profile, page 5-22

- Viewing a Device Profile, page 5-25

- Editing a Device Profile, page 5-27

- Deleting a Device Profile, page 5-32

Device Profile Configuration Options

To view options for managing device profiles, on the Devices View page, click the **Additional Actions** button [...] and then click **Profiles**.

The Profiles page displays. This page includes the items that Table 5-4 describes.

Table 5-4   Profiles Page Items

Item	Description
Available Profiles	Displays the number of device profiles that are available.
ADD button	Displays the Adds New Profile window, which you use to add a device profile to Cisco Fog Director. See the "Adding a Device Profile" section on page 5-22.
VIEW button	Displays detailed information about a device profile for which the corresponding check box is checked. See the "Viewing a Device Profile" section on page 5-25. This button is dimmed if you do not check a check box for a device profile.

Table 5-4   Profiles Page Items (continued)

Item	Description
Additional Actions button [···]	Displays the following options. This button is dimmed if you do not check a check box for a device profile. • **EDIT**—Displays the Edit Profile window, from which you can view or edit information for a device profile. See the "Viewing a Device Profile" section on page 5-25. • **MARK AS DEFAULT**—Sets as the default the device profile for which the corresponding check box is checked. See the "Setting a Device Profile as the Default" section on page 5-31. • **DELETE**—Deletes from Cisco Fog Director the device profile for which the corresponding check box is checked. See the "Deleting a Device Profile" section on page 5-32.
Search Profile Name field	Type all or part of a device profile name to display information for devices profiles with matching names. The Device Profile list display updates as you type.
Device Profile list	Displays the device profiles that have been created in Cisco Fog Director and that can be associated with devices. This list includes the following items for each device profile • Check box—Check to choose a device profile to view details about, set as the default, or delete • NAME—Name of the device profile • DEFAULT—Displays "DEFAULT" for the device profile that is set to the default and "NON DEFATULT" for other device profiles • ASSOCIATED DEVICES COUNT—Number of devices with which the device profile is associated
Pagination controls	Click a control to go to the first, next, last, previous, or specific page in the table. From the **Items per page** drop-down list, choose the maximum number of device profile that appear in each page of the table.

Adding a Device Profile

Adding a device profile specifies the configuration settings that the profile includes and makes the profile available to associate with devices.

To add a device profile, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Additional Actions** button [···] and then click **Profiles**.

The Profiles page displays.

Step 3   On the Profiles page, click the **ADD** button.

The Add New Profile window displays.

Step 4 In the Add New Profile window, take these actions:

    a. In the Profile Name field, enter a name for the device profile.

    b. If you want to set this device profile the default device profile, check the **Mark this Profile as Default** check box.

    c. In the MONITORING tab, take these actions:

        – From the **Events Collection Frequency** drop-down list, choose and option to specify how often Cisco Fog Director collects events information from the device. This information is shown in various summary and detail displays throughout Cisco Fog Director. The default value is **Every 2 hrs**.

        – From the **Metrics Collection Frequency** drop-down list, choose and option to specify how often Cisco Fog Director collects metrics information such as CPU, memory, and network resource use from the device. This information is shown in various summary and detail displays throughout Cisco Fog Director. The default value is **Every 2 hrs**.

        – In the **Heartbeat Miss Count** field, enter the number of consecutive failed attempts by Cisco Fog Director to poll a device after which Cisco Fog Director indicates that it has lost contact with the device. The default value is 3.

        – Check the **Enable Auto Recovery** check box if you want to enable the auto recovery feature on devices that are associated with this device profile. This check box is checked by default. See the "Recovering an App on a Device" section on page 5-43 for related information.

    d. In the COMMUNICATION tab, take these actions:

        – In the **Default timeout for control actions** field, enter the amount of time, in seconds, after which Cisco Fog Director generates an error if it does not receive a response to a control request that it sends to a device. The default value is 600 seconds (10 minutes).

        – In the **Timeout for file transfers** field, enter the mount of time, in seconds, after which Cisco Fog Director generates an error if an attempt to transfer an app, service, or cartridge file from Cisco Fog Director to a device does not execute. The default value is 3600 seconds (1 hour).

        – In the **Proxy address** field, enter the IP address of an HTTP proxy server that Cisco Fog Director uses to communicate with a device, if such proxy communication is configured in your deployment.

        – In the **Proxy port** field, enter the HTTP proxy server port that Cisco Fog Director uses to communicate with a device, if such proxy communication is configured in your deployment. You can type a number or use the arrow buttons to enter a value.

    e. In the SECURITY tab, take these actions:

        – Check the Verify SSL Certificates check box if you want Cisco Fog Director to validate certificates as part of the SSL handshake when it contacts the devices with which this device profile is associated. If you enable this feature and validation fails, Cisco Fog Director cannot communicate with the device. (This feature is enabled by default.)

        This validation process requires that a public key certificate and corresponding private key be imported to the device by using Cisco IOx Local Manager. If the device public key certificate is self-signed, import this public key certificate into Cisco Fog Director. If the device public key certificate is signed by a trusted Certificate Authority (CA), import the trust anchors (public key certificate of CA) into Cisco Fog Director.

        To import certificates to Cisco Fog Director now, hover your mouse pointer over the information icon next to "Verify SSL Certificate," click the **Click here** link in the message that displays, and then use the Trust Anchors page that displays to import the certificates.

–   (Optional) If you checked the Verify SSL Certificates check box, check the Verify Serial Number check box if you want Cisco Fog Director to validate the serial number of the device against the serial number that your provide when adding, importing, or editing a device. If you check the Verify Serial Number check box, you must provide a device serial number when you perform these actions. If you enable this feature and validation fails, Cisco Fog Director does not communicate with the device.

If you enable this feature, you must provide the serial number when you add, edit, or import a device.

> **Note**   Check the **Verify App Signature** check box if you want to enable App Package Signature Verification on the device. When this option is enabled, the system verifies the app when the app is installed or upgraded on a device with which this device profile is associated. If the app signature is not verified, the installation fails. The system performs this verification in two steps. First, it uses local trust anchors on the device to ensure that the embedded package certificate in the application is trusted. Next, it ensures that the embedded package signature is valid.
>
> For related information, see Configure IOx Package Signature Validation, which is available here: https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/iox/212472-configure-iox-package-signature-validati.html.

–   (Optional) If you checked the **Verify App Signature**, check click **Browse** and navigate to and select the trust anchor (a .tar.gz or .tgz certificate file) that is required for the app signature to be verified. The trust anchor is uploaded to Cisco Fog Director when you click the **SAVE** button. When you install an app, Cisco Fog Director pushes this trust anchor file to the device. If the trust anchor file exists on the device, Cisco Fog Director overwrites the existing file.

After you import a trust anchor file, the file name displays on this tab. Click the remove icon ✕ next to the file name to remove from the list, it if needed.

You do not need to upload a trust anchor file if a trust anchor for app signature verification already exists on the device.

Step 5   (Optional) Click the **Show Advanced** button on any tab to the Advanced area, which contains the following tabs:

•   OVERVIEW tab—Displays JSON code for the device profile.

•   DEVICES tab—Includes the following items:

–   Total associated devices—Number of devices with which this device profile is associated.

–   Search Hostname, IP Address field—Type all or part of a hostname or IP address of a device to display information for devices with matching information. The Devices table display updates as you type.

–   Devices table—Provides information about each device with which this device profile is associated. The table includes the following items:

- Host Name—Hostname of the device

- IP Address—IP address of the device

- Tags—Tags that are assigned to a device

- Pagination controls—Click a control to go to the first, next, last, previous, or specific page in the table

- Items per page drop-down list—Choose the maximum number of devices that appear in each page of the table

You can click a name in the Host Name column or an IP address in the IP Address column to display the Device Details page for the corresponding device.

The button changes to **Hide Advanced**. Click the **Hide Advanced** button to collapse expanded display.

Step 6   Click the **SAVE** button to save the device profile.

To exit the Add New Profile window without saving the device profile, click the **Cancel** button.

Viewing a Device Profile

You can view detailed information about any device profile.

To view a device profile, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Additional Actions** button [⋯].

Step 3   Take either of these actions:

- To view information for a device profile from by the **Profiles** option:

    1. Click **PROFILES**.

    The Profiles page displays.

    2. On the Profiles page, check the check box for the profile that you want to view, and then click the **VIEW** button.

- To view information for a device profile from by using the **Edit** option:

    1. Click **Edit**.

    The Edit Devices page displays.

    2. In the Device table on the Edit View page, check the check box for the device for which you want to view the device profile and then click **Add Selected Devices**.

    3. In the Edit Devices Information area, click the **Show Profile Details** link.

The View Profile window displays if you clicked the **VIEW** button, or the Profile Details window displays if you clicked the **Show Profile Details** link. These windows include the items that Table 5-5 describes.

Table 5-5   View Profile Window and Profile Details Window Items

Item	Description
MONITORING Tab	
Event Collection Frequency	How often Cisco Fog Director collects events information from a device. This information is shown in various summary and detail displays throughout Cisco Fog Director.

Table 5-5   View Profile Window and Profile Details Window Items (continued)

Item	Description
Metrics Collection Frequency	How often Cisco Fog Director collects metrics information such as CPU, memory, and network resource use from a device. This information is shown in various summary and detail displays throughout Cisco Fog Director.
Heartbeat Miss Count	Number of consecutive failed attempts by Cisco Fog Director to poll a device after which Cisco Fog Director indicates that it has lost contact with the device.
Enable Auto Recovery	If checked, the auto recovery feature is enabled on device that are associated with this device profile. See the "Recovering an App on a Device" section on page 5-43 for related information.
COMMUNICATION Tab	
Default timeout for control actions	Amount of time, in seconds, after which Cisco Fog Director generates an error if it does not receive a response to a control request that it sends to a device.
Timeout for file transfers	Amount of time, in seconds, after which Cisco Fog Director generates an error if an attempt to transfer an app, service, or cartridge file from Cisco Fog Director to a device does not execute.
Proxy address	IP address of an HTTP proxy server that Cisco Fog Director uses to communicate with a device, if such proxy communication is configured in your deployment.
Proxy port	HTTP proxy server port that Cisco Fog Director uses to communicate with a device, if such proxy communication is configured in your deployment. You can type a number or use the arrow buttons to enter a value.
SECURITY Tab	
Verify SSL Certificates	If checked, Cisco Fog Director validates certificates as part of the SSL handshake when it contacts the devices with which this device profile is associated. This check box is checked by default.
Verify Serial Number	Check this check box to cause Cisco Fog Director to verify a device serial number provided by the SSL certificate of the device against a serial number that you provide when adding, importing, or editing the device. If the serial numbers do not match, the verification fails and the add, import, or edit option does not complete successfully. This check box can only be checked if you check the Verify SSL Certificates check box first.
Verify App Signature	If checked, App Package Signature Verification is enabled on the device. When this option is enabled, the system verifies the signature of an app when the app is installed or upgraded on a device with which this device profile is associated. If the app signature is not verified, the installation fails.

Table 5-5   View Profile Window and Profile Details Window Items (continued)

Item	Description
Trust Anchor for App Signature Verification	Appears when you check the Verify App Signature check box. Name of the trust anchor (certificate file) on the device that is compared with a certificate in the app during the app signature verification process.

Advanced Options

These options do not display on the Profile Details window.

Advanced Options button	Click to display the Overview tab and the Devices tab. The button changes to **Hide Advanced**. Click the **Hide Advanced** button to collapse the advanced display.
Overview tab	Displays JSON code for the device profile.
Devices tab	Includes the following items • Total associated devices—Number of devices with which this device profile is associated. • Search Hostname, IP Address field—Type all or part of a hostname or IP address of a device to display information for devices with matching information. The Devices table display updates as you type. • Devices table—Provides information about each device with which this device profile is associated. The table includes the following items: – Host Name—Hostname of the device – IP Address—IP address of the device – Tags—Tags that are assigned to a device. – Pagination controls—Click a control to go to the first, next, last, previous, or specific page in the table – Items per page drop-down list—Choose the maximum number of devices that appear in each page of the table Click a name in the Host Name column or an IP address in the IP Address column to display the Device Details page for the corresponding device.

Editing a Device Profile

You can edit device profile security options.

To a device profile, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Additional Actions** button [⋯] and then click **Profiles**.

The Profiles page displays.

Step 3   On the Profiles page, check the check box for the profile that you want to edit, click the **Additional Actions** button [⋯], and then choose **EDIT**.

The Edit Profile window displays. It includes the items that Table 5-6 describes.

Step 4   If you make configuration updates in the Edit Profile window, click the **UPDATE** button to save your changes.

Table 5-6   Edit Profile Window Items

Item	Description
MONITORING Tab	
Event Collection Frequency	How often Cisco Fog Director collects events information from a device. This information is shown in various summary and detail displays throughout Cisco Fog Director. The default value is **Every 1 hr**.
Metrics Collection Frequency	How often Cisco Fog Director collects metrics information such as CPU, memory, and network resource use from a device. This information is shown in various summary and detail displays throughout Cisco Fog Director. The default value is **Every 2 hrs**.
Heartbeat Miss Count	Number of consecutive failed attempts by Cisco Fog Director to poll a device after which Cisco Fog Director indicates that it has lost contact with the device. The default value is **3.**
Enable Auto Recovery	If checked, the auto recovery feature is enabled on device that are associated with this device profile. See the "Recovering an App on a Device" section on page 5-43 for related information. This check box is checked by default.
COMMUNICATION Tab	
Default timeout for control actions	Amount of time, in seconds, after which Cisco Fog Director generates an error if it does not receive a response to a control request that it sends to a device. The default value is **600**.
Timeout for file transfers	Amount of time, in seconds, after which Cisco Fog Director generates an error if an attempt to transfer an app, service, or cartridge file from Cisco Fog Director to a device does not execute. The default value is **3600**.
Proxy address	IP address of an HTTP proxy server that Cisco Fog Director uses to communicate with a device, if such proxy communication is configured in your deployment.

Table 5-6   Edit Profile Window Items (continued)

Item	Description
Proxy port	HTTP proxy server port that Cisco Fog Director uses to communicate with a device, if such proxy communication is configured in your deployment. You can type a number or use the arrow buttons to enter a value.
SECURITY Tab	
Verify SSL Certificates	Check this check box if you want Cisco Fog Director to validate certificates as part of the SSL handshake when it contacts the devices with which this device profile is associated.
	This validation process requires that the certificates (or *trust anchors*) that are present on a device also be imported to Cisco Fog Director. To import certificates to Cisco Fog Director now, hover your mouse pointer over the information icon 🛈 next to "Verify SSL Certificate," click the **Click here** link in the message that displays, and use the Trust Anchors page that displays to import the certificates. For related information, see the "Importing a Trust Anchor" section on page 6-4.
	This check box is checked by default.
Verify Serial Number	Check this check box to cause Cisco Fog Director to verify a device serial number provided by the SSL certificate of the device against a serial number that you provide when adding, importing, or editing the device. If the serial numbers do not match, the verification fails and the add, import, or edit option does not complete successfully.
	This check box can only be checked if you check the Verify SSL Certificates check box first.
Verify App Signature	Check this check box if you want to enable App Package Signature Verification on the device. When this option is enabled, the system verifies the app when the app is installed or upgraded on a device with which this device profile is associated. If the app signature is not verified, the installation fails. The system performs this verification by comparing a certificate on the device with a certificate in the app.

Table 5-6   *Edit Profile Window Items (continued)*

Item	Description
Trust anchor radio buttons	The following radio buttons appear if the Verify App Signature check box is checked:
	• **Existing Trust Anchor**—Appears if there is an existing trust anchor on the device. Click to use the trust anchor that is shown.
	You can hover your mouse pointer over the trust anchor name to see the checksum value certificate.
	• **New Trust Anchor**—Click to import a new trust anchor for the device. After you click this radio button, click **Browse** and navigate to and select the trust anchor (a .tar.gz or .tgz certificate file) that is required for the app signature to be verified. The trust anchor is uploaded to Cisco Fog Director when you click the **UPDATE** button.
	After you import a trust anchor file, the file name displays under the BROWSE button. Click the X next to the file name to remove from the list, it if needed.
	• **No Trust Anchor**—Click to if you want to delete the existing trust anchor from the device profile. The trust anchor is deleted when you click the **UPDATE** button.
Advanced Options	
Show Advanced	Click to display the Overview tab and the Devices tab. The button changes to **Hide Advanced**. Click the **Hide Advanced** button to collapse the advanced display.
Overview tab	Displays JSON code for the device profile.

*Table 5-6   Edit Profile Window Items (continued)*

Item	Description
Devices tab	Includes the following items:
	• Total associated devices—Number of devices with which this device profile is associated.
	• Search Hostname, IP Address field—Type all or part of a hostname or IP address of a device to display information for devices with matching information. The Devices table display updates as you type.
	• Devices table—Provides information about each device with which this device profile is associated. The table includes the following items:
	– Host Name—Hostname of the device
	– IP Address—IP address of the device
	– Tags—Tags that are assigned to a device
	– Pagination controls—Click a control to go to the first, next, last, previous, or specific page in the table
	– Items per page drop-down list—Choose the maximum number of devices that appear in each page of the table
	Click a name in the Host Name column or an IP address in the IP Address column to display the Device Details page for the corresponding device.
UPDATE button	Click to update the device profile with changes that you made and exit the Edit Profile window.
CANCEL button	Click to exit the Edit Profile window without saving any changes.

Setting a Device Profile as the Default

You can set any device profile as the default. The system automatically associates the default device profile with devices that do not have another device profile associated with them.

To set a device profile as the default, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Additional Actions** button ⌈ ⋯ ⌉ and then click **Profiles**.

The Profiles page displays.

Step 3   On the Profiles page, take these actions:

a.   Check the check box for the profile that you want to set as the default.

b.   Click the **Additional Actions** button ⌈ ⋯ ⌉ and then choose **MARK AS DEFAULT**.

The DEFAULT field in the Device Profile list in the Profiles page updates to show "DEFAULT" for this device profile and to show "NON DEFAULT" for other device profiles.

Deleting a Device Profile

Deleting a device profile removes it from Cisco Fog Director. You cannot delete a device profile that is set as the default or a device profile that is associated with one or more devices.

To delete device profile as the default, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Additional Actions** button [⋯] and then click **Profiles**.

The Profiles page displays.

Step 3   On the Profiles page, take these actions:

a.   Check the check box for the profile that you want to delete.

b.   Click the **Additional Actions** button [⋯] and then choose **DELETE**.

Rediscovering Devices

Rediscovering devices causes Cisco Fog Director to discover device information (including host name and serial ID), capabilities (including CPU, memory, disk and network resources), and states of apps for the devices that you select.

To rediscover devices, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Additional Actions** button [⋯] and then click **Re-Discover**.

The Re-Discover Devices page displays. The top part of this page displays the Devices table, which lists the devices that can be rediscovered.

Step 3   If you want to limit the devices that display in the Devices table to one or more specific devices, take the appropriate action:

- To limit the device display to a specific device based on its hostname or IP address, enter all or part of the hostname or IP address in the **Search Hostname, IP Address** field.

- To limit the device display to specific devices based on a tag, choose a tag from the **Show** drop-down list

- To limit the device display to specific devices based on reachability, last heard, or discovery status, click the Device Filters and then choose the desired filter option. When you choose an option, it displays in the Device Filters field and the Device table updates automatically. You can add as many

device filter options as needed. To remove a device filter option from this field, click the X icon ✕ next to the option. For descriptions of the device filter options, see the Device Filters field row in Table 5-1 on page 5-2.

Step 4   In the Installed Devices table, check the check box for each device that you want to be rediscovered.

Step 5   Click the **Add Selected Devices** button.

The devices with checked check boxes are added to the Selected Devices table. The devices that this table lists will be rediscovered.

To remove a device from this table, click the x icon ✖ in the Action column that corresponds to the device to remove.

Step 6   Click the **Done, Let's Go** button.

Cisco Fog Director rediscovers the devices that you selected.

Editing Devices

For security reasons, you may not want to include valid user name, password, port, or contact information when you create an import file. In this case, you can use dummy values for this information and uncheck the **Discover devices after import** check box when you import the import file. Then, after you import the import file, you can use the Device Edit feature to update these values for the devices. (For related information, see the "Importing Devices" section on page 5-18.)

The Edit Devices feature lets you update user name, password, port, and contact information for multiple devices simultaneously.

The following sections provide additional information:

- Edit Device Options, page 5-33
- Editing Information for Multiple Devices, page 5-36

Edit Device Options

To view options for editing devices on the Devices View page, click the **Additional Actions** button ⬚ and then click **Edit**.

The Edit Devices page displays. This page includes the items that Table 5-7 describes.

Table 5-7   Edit Devices Page Items

Item	Description
Installed Devices table	Provides information about each device that has been added to Cisco Fog Director, and includes the following items: • Search Hostname, IP address field—Type all or part of a hostname or IP address of a device to display information for devices with matching information. The table display updates as you type. • Device filters field—To limit the device display to specific devices based on reachability, last heard, or discovery status, click the Device Filters and then choose the desired filter option. When you choose an option, it displays in the Device Filters field and the Device table updates automatically. You can add as many device filter options as needed. To remove a device filter option from this field, click the X icon ⨉ next to the option. For descriptions of the device filter options, see the Device Filters field row in Table 5-1 on page 5-2. • Show field—Enter the name of a tag and then press the **Enter** key to display information for devices with a matching tag. You can choose a tag from a drop-down list of available tags by typing the first few letters of the tag and then clicking the tag that you want. • Check box—Check the check box for each device on which you want to install the app. You can click the check box in the title row of the table to quickly check all boxes in the table. • Host Name—Hostname of the device on which the app is to be installed. • IP Address—IP address of the device on which the app is to be installed. • Tags—Tags that are assigned to a device. • Installed Apps—Apps that are installed on the device. • Pagination controls—Click a control to go to the first, next, last, previous, or specific page in the table. • Items per page drop-down list—Choose the maximum number of devices that appear in each page of the table.
Add Selected Devices button	Click to add devices with checked check boxes to the Selected Devices table.

*Table 5-7   Edit Devices Page Items (continued)*

Item	Description
Selected Devices table	Provides information about each device for which you want to edit information. Devices appear in this table after you check their check boxes in the Installed Devices table and then click **Add Selected Device**. This table includes the following items:

• Selected Devices—Number of devices on which you want to install the app.

• Exclude readonly devices—Check this check box to remove read-only devices from the Selected Devices table

• Search Hostname, IP Address field—Type all or part of a hostname or IP address of a device to display information for devices with matching information. The table display updates as you type.

• Host Name—Hostname of the device on which you want to install the app.

• IP Address—IP address of the device on which you want to install the app.

• Tags—Tags that are assigned to the device on which you want to install the app.

• Health—Icons that represent information about CPU use or memory use on the device. Hover your mouse pointer over an icon to see more detailed information.

• Last Heard—How long ago Cisco Fog Director last communicated with the device, or a brief explanation of why the last attempt to communicate with the device was unsuccessful.

• Action—Click the x icon ✖ to remove a device from the Selected Devices table. Clicking this icon does not affect the device.

• Pagination controls—Click a control to go to the first, next, last, previous, or specific page in the table.

• Items per page drop-down list—Choose the maximum number of devices that appear in each page of the table.

Table 5-7   Edit Devices Page Items (continued)

Item	Description
Edit Devices Information	Appears when one or more devices appear in the Selected Devices table, and includes the following items. The Username, Port, Password, and Contact Details page can be edited only if you checked the **Exclude readonly devices** check box in the Selected Devices table. Check the check box next to a field name to cause Cisco Fog Director to update devices with information in the corresponding field when you click the **Done, Let's Go** button. • Username—Cisco IOS user name for the devices. This field can be edited only if you checked the **Exclude readonly devices** check box in the Selected Devices table. • Port—HTTPS port on which Cisco IOx runs on the devices. This field can be edited only if you checked the **Exclude readonly devices** check box in the Selected Devices table. • Password—Cisco IOS password for the devices. This field can be edited only if you checked the **Exclude readonly devices** check box in the Selected Devices table. • Contact Details—Contact information of the person who is responsible for the devices. This field can be edited only if you checked the **Exclude readonly devices** check box in the Selected Devices table. • Device Profile—Name of the device profile to be associated with the selected devices. • **Show Profile Details** link—Click to displays the Profile Details window for the device profile that is associated with the device. See the "Viewing a Device Profile" section on page 5-25.
Done, Let's Go button	Appears when one or more devices appear in the Selected Devices table. Click to update the devices in the Selected Devices table with the information in the Edit Devices Information fields.

Editing Information for Multiple Devices

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Additional Actions** button [⋯] and then click **Edit**.

The Edit Devices page displays. The top part of this page displays the Devices table, which lists the devices that have been added to Cisco Fog Director.

Step 3   In the Installed Devices table, check the check box for each device for which you want to edit information.

For detailed information about this table and locating devices, see the "Edit Device Options" section on page 5-33.

Step 4   Click the **Add Selected Devices** button.

The devices that you selected are added to the Selected Devices table. The information that you provide will be updated on the devices that this table lists. For detailed information about this table and about removing devices from this table, see the "Edit Device Options" section on page 5-33.

Step 5   In the Edit Devices information area, take the following actions.

You might need to scroll down to see this area.

- In the Username field, enter Cisco IOS user name that is configured on the devices.
- In the Port field, enter HTTPS port on which Cisco IOx runs on the devices. You can type a number or use the Up or Down arrow buttons to enter a value.
- In the Password field, enter Cisco IOS password that is configured on the devices.
- In the Contact Details field, enter the contact information of the person who is responsible for the device.

Step 6   Click the **Done, Let's Go** button.

The devices that you selected are updated with the information that you entered.

Deleting Devices

Deleting a device removes it from Cisco Fog Director.

You delete as described in the following sections:

- Deleting One Device, page 5-37
- Deleting Multiple Devices, page 5-38

Deleting One Device

To delete single device from Cisco Fog Director, perform the following steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   In the Device table, click the **Expand** icon ⌃ to the left of the device hostname of the device that you want to delete.

Step 3   Click **Delete Device**.

The Delete dialog box displays.

Step 4   Click **OK** in the delete dialog box.

Deleting Multiple Devices

To delete several devices from Cisco Fog Director at the same time, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Additional Actions** button [⋯] and then click **Delete**.

The Delete Devices page displays. The top part of this page displays the Devices table, which lists the devices that you can delete.

Step 3   If you want to limit the devices that display in the Devices table to one or more specific devices, take the appropriate action:

- To limit the device display to a specific device based on its hostname or IP address, enter all or part of the hostname or IP address in the **Search Hostname, IP Address** field.

- To limit the device display to specific devices based on a tag, choose a tag from the **Show** drop-down list

- To limit the device display to specific devices based on reachability, last heard, or discovery status, click the Device Filters and then choose the desired filter option. When you choose an option, it displays in the Device Filters field and the Device table updates automatically. You can add as many device filter options as needed. To remove a device filter option from this field, click the X icon ✕ next to the option. For descriptions of the device filter options, see the Device Filters field row in Table 5-1 on page 5-2.

Step 4   In the Installed Devices table, check the check box for each device that you want to delete.

Step 5   Click the **Add Selected Devices** button.

The devices with checked check boxes are added to the Selected Devices table. The devices that this table lists will be deleted.

To remove a device from this table, click the x icon ✖ in the Action column that corresponds to the device to remove.

Step 6   Click the **Done, Let's Go** button.

The devices that you selected are removed from Cisco Fog Director.

Managing Tags for Devices

A tag is a brief descriptive label that you assign to a device. For example, a tag could be the name of an administrator, the name of an app, or the purpose of an app. Tags are useful for categorizing devices. In some areas on the Apps pages, you can display devices with matching tags.

The following guidelines apply to tags:

- There is no limit to the number of tags that can be assigned to a device

- A tag can include alphanumeric characters, special characters, and spaces

- Tags are case sensitive

You manage tags for devices in the Device table on the Devices View page as described in the following sections:

Managing Tags for One Device

To assign a tag to a single device, click the **Enter new tag** field in the Tags column that corresponds to the device, enter the tag that you want, and then press the **Enter** key or the **Tab** key. If the tag does not already exist, the system creates a new one with the name that you enter.

To remove a tag from a device, click the **X** next to the tag.

Managing Tags for Multiple Devices

You can assign tags to or remove tags from several devices at the same time. Tags that you assign must already have been created in Cisco Fog Director as described in as described in the "Managing Tags for One Device" section on page 5-39,

To assign tags to or remove tags from multiple devices, follow these steps

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   On the Devices View page, click the **Additional Actions** button ⋯ and then click **Tag**.

The Tag page displays. The top part of this page displays the Devices table, which lists the devices on which you can assign or remove a tag.

Step 3   If you want to limit the devices that display in the Devices table to one or more specific devices, take the appropriate action:

- To limit the device display to a specific device based on its hostname or IP address, enter all or part of the hostname or IP address in the **Search Hostname, IP Address** field.
- To limit the device display to specific devices based on a tag, choose a tag from the **Show** drop-down list
- To limit the device display to specific devices based on reachability, last heard, or discovery status, click the Device Filters and then choose the desired filter option. When you choose an option, it displays in the Device Filters field and the Device table updates automatically. You can add as many device filter options as needed. To remove a device filter option from this field, click the X icon ✕ next to the option. For descriptions of the device filter options, see the Device Filters field row in Table 5-1 on page 5-2.

Step 4   In the Installed Devices table, check the check box for each device on which you want assign or remove a tag.

Step 5   Click the **Add Selected Devices** button.

The devices with checked check boxes are added to the Selected Devices table. Tags will be assigned to or removed from the devices that this table lists.

To remove a device from this table, click the x icon ✖ in the Action column that corresponds to the device to remove.

Step 6   In the Tag Configuration area, take either of these actions:

- To assign a tag to all selected devices:

     a. Click **Tag** next to Action.

     b. In the Tag field, enter the tag that you want to assign. The system displays a list of tags with initial characters that match the characters you type. To display a list of all tags, press the Spacebar in this field.

  • To remove a tag from all selected devices:

     a. Click **Tag** next to Action.

     b. In the Tag field, enter the tag that you want to remove. The system displays a list of tags with initial characters that match the characters you type. To display a list of all tags, press the Spacebar in this field.

       After you choose a tag, a the system displays the number of devices on which the tag is assigned.

Step 7   Click the **Done, Let's Go** button.

    The designated tag is assigned to or removed from all devices that you selected.

Starting or Stopping an App on a Device

Starting an app initiates its operation on a host device and puts the app in Running state. CPU and memory (RAM) resources that were reserved for the app become in use.

Stopping an app shuts down its operation on a host device and puts the app in Stopped state. CPU and memory (RAM) resources that were used by the app remain reserved for it but stop being used.

The following sections describe how to start and stop an app from the DEVICES tab. You also can start and stop an app from the App Configuration Page as described in the "Starting or Stopping an App on Selected Devices" section on page 4-28 and from the App Monitoring page by using the **START** and **STOP** buttons under the Status Charts as described in the "Viewing General Monitoring Information" section on page 4-60.

  • Starting an App on a Device, page 5-40

  • Stopping an App on a Device, page 5-41

Starting an App on a Device

Starting an app initiates its operation on a host device and puts the app in Running state.

To start an app on a device, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   Take either of these actions:

  • In the Device table on the Devices View page, click the IP address or the hostname of the device on which you want to start the app.

  • In the Device table, click the **Expand** icon ⌃ to the left of the device hostname of the device of the device on which you want to start the app.

Step 3   If the app is running, take either of these actions:

- If you clicked the IP address or the hostname of the device in Step 2, click the **Start** button that displays under the icon of the app that you want to start.
- If you clicked the **Expand** icon in Step 2, click the **Start** button ▶ that corresponds to the app that you want to start.

Stopping an App on a Device

Stopping an app shuts down its operation on a host device and puts the app in Stopped state.

You cannot stop an app that provides services if the services that it provides are being used by one or more other apps that are in Running state. Before you stop an app that provides services, stop each app that uses the services that it provides.

To stop an app on a device, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   Take either of these actions:

- In the Device table on the Devices View page, click the IP address or the hostname of the device on which you want to stop the app.
- In the Device table, click the **Expand** icon ⌃ to the left of the device hostname of the device of the device on which you want to stop the app.

Step 3   If the app is running, take either of these actions:

- If you clicked the IP address or the hostname of the device in Step 2, click the **Stop** button that displays under the icon of the app that you want to stop.
- If you clicked the **Expand** icon in Step 2, click the **Stop** button ■ that corresponds to the app that you want to stop

Removing an App from a Device

Removing an app from a device removes it from the host device and releases CPU and memory (RAM) resources that were reserved for the app.

To remove an app from a device, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   Take either of these actions:

- In the Device table on the Devices View page, click the IP address or the hostname of the device from which you want to remove the app.

- In the Device table, click the **Expand** icon ⌃ to the left of the device hostname of the device from which you want to remove the app.

Step 3   If the app is running, take either of these actions:

- If you clicked the IP address or the hostname of the device in Step 2, click the **Stop** button that displays under the icon of the app that you want to remove from the device.

- If you clicked the **Expand** icon in Step 2, click the **Stop** button ▢ that corresponds to the app that you want to remove from the device,

**Step 4**   Take either of these actions:

- If you clicked the IP address or the hostname of the device in Step 2, click the **Uninstall** button that displays under the icon of the app that you want to remove from the device, then click the **YES** button in the confirmation dialog box that displays.

- If you clicked the **Expand** icon in Step 2, click the **Remove** button ✖ that corresponds to the app that you want to remove from the device,

Deleting Unused Cartridges

For system maintenance and to free disk space on a device, you can delete cartridges that have been installed on the device but that are not used by any apps. Deleting cartridges removes them and their metadata from a device.

To delete unused cartridges from a device, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   In the Device table on the Devices View page, click the IP address or the hostname of the device for which you want to delete unused cartridges.

Step 3   Click the **CARTRIDGES** tab under the Host Information area.

Step 4   In the Unused Cartridges area on the page that displays, click the **DELETE UNUSED CARTRIDGES** button.

Managing Layers

The Layers tab on the Device Details page provides options for viewing information about and managing layers on a device. A layer is a component of a Docker image from which an app package has been created.

When you upload or upgrade an app package from a Docker image, Cisco Fog Director automatically identifies the layers that the image requires and transfers only the component layers that do not exist on the device.

When you uninstall an app, the system does not automatically remove from the device the layers that relate to that app. Similarly, when you upgrade an app and the new version no longer needs some layers that were used by the older version, the system does not automatically remove from the device the layers that are no longer used. In both cases, if you want to remove unused layers from the device, you must remove them manually.

You can delete any layer that is not in use by an installed app.

To delete layers that are not used by installed apps from a device, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   In the Device table on the Devices View page, click the IP address or the hostname of the device for which you want to delete layers.

Step 3   Click the **LAYERS** tab under the Host Information area.

Step 4   In the Layers tab, take either of these actions:

- To delete specific layers, check the check box for each layer that you want to delete, and then click the **DELETE SELECTED LAYERS** button.

  You can click the check box at the top of the list of layers to quickly check boxes for all layers. You cannot delete a layer that is in use by an installed app.

- To delete all layers that are not used by any installed app, click the **DELETE ALL UNUSED LAYERS** button.

Recovering an App on a Device

Cisco Fog Director can detect if an app has become corrupted. An app can become corrupted as a result of a variety of issues, such as issues with its configuration or missing or damaged files.

Cisco Fog Director provides features for recovering an app that is corrupted. The recovery features apply only to apps that are in *managed state*. (An app is in this state when you can manage it on a device by using Cisco Fog Director. See the "Understanding Managed and Unmanaged States for Apps" section on page 3-3.)

App recovery features include the following:

- Auto recovery—By default, Cisco Fog Director enables the auto recovery feature. When this feature is enabled, Cisco Fog Director checks each app for corruption once per minute, by default. (You configure this check interval in the properties file of the app.) If Cisco Fog Director detects that an is app corrupted, it attempts to recover the app automatically.

- Manual recovery—If auto recovery is not enabled, or if an auto recovery action is unable to recover an app, you can attempt to recover an app manually as described in this section.

The recovery process can involve reinstalling an app, reactivating an app, installing cartridges, and so on. A successful recovery process fixes problems that Cisco Fog Director identifies and returns the app returns to normal operation.

To manually recover an app on a device, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   In the Device table on the Devices View page, click the IP address or the hostname of the device from which you want to remove the app.

Step 3   Click the **Expand** button ⌄ next to the name of the app that you want to recover.

The App Info area for the app displays

Step 4   In the App Info area, click **Recover** link, which appears next to the App Health state for an app for which you can attempt a recovery action.

Cisco Fog Director attempts to recover the app. If the recovery is successful, the App Health state updates to display **HEALTHY**.

Viewing Diagnostic Information

Cisco Fog Director lets you view the following information that relates to a device. This information can help you monitor and diagnose issues on a device.

- Errors—Information about errors that occurred on the device. An error is an issue or problem. The system captures information about errors that have been written to the Cisco application-hosting framework log files since the Cisco application-hosting framework last started on the device.

- Events—Information about events that occurred on the device. An event is an activity that typically relates to a Cisco application-hosting framework operation. The system captures information about events that have been written to the Cisco application-hosting framework log files since the Cisco application-hosting framework last started on the device.

- System information—Provides summary or detailed information that relates to memory use, disk operation, processes, networking, or apps on the device. The system captures this information from a script that the Cisco application-hosting framework runs on a device.

- App manager jobs—Provides high-level information about Cisco Fog Director activities that relate to a device.

- App lifecycle tasks—Provides detailed information about Cisco Fog Director activities that are related to apps on a device.

To view diagnostic information for a device, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   In the Device table on the Devices View page, click the IP address or the hostname of the device for which you want to create a log file.

Step 3   Click the **Device Diagnostics** button next near the top right of the screen.

The Diagnostics window displays. This window includes these tabs:

- ERRORS—Provides information about errors that occurred on the device

- EVENTS—Provides information about events that occurred on the device
- SYSTEM—Provides options for viewing summary or detailed information that relates to memory use, disk operation, processes, networking, or apps on the device.
- APP MANAGER JOBS—Provides information about app manager jobs that occurred on the device
- APP LIFE CYCLE TASKS—Provides information about app lifecycle tasks that occurred on the device

Table 5-8 describes the items in Diagnostics window in detail.

Step 4 (Optional) To view information about errors, events, app manager jobs, or app lifecycle tasks, click the corresponding tab.

See Table 5-8 for more detailed information.

Step 5 (Optional) To obtain summary or detailed information that relates to memory use, disk operation, processes, networking, or apps click the **SYSTEM** tab, and then take either of these actions:

- To see summary information for an item in the Diagnostics column, click **Run (Normal Mode)** in the corresponding action column.
- To see detailed information for an item in the Diagnostics column, click **Run (Detail Mode)** in the corresponding action column.

Summary or detail information appears in the SYSTEM tab. To exit this information display, click the **BACK** button. To update this display with current information, click the **REFRESH** button.

See Table 5-8 for more detailed information.

Table 5-8 describes the items in the Diagnostics window.

The top part of this window includes tabs, the search field (for the ERRORS and EVENTS tab), and the REFRESH button. The bottom part of this window contains the Information area, which displays information for the tab that you choose.

You can click any field title in the Information area, except on the RUN DIAGNOSTICS tab, to toggle the information in that table in default, ascending, or descending alphanumeric order by that field. An up arrow ↑ in a field indicates that the information is in ascending alphanumeric order by that field. A down arrow ↓ in a field indicates descending order.

Table 5-8   Diagnostics Window Items

Item	Description
ERRORS Tab	
Search field	To display only information for errors that have text in the Type or Message fields that contains a specific character string, enter the string in the Search field and then click the **Search** button.
	To clear a search, delete characters in the field and press **Enter** or click the **REFRESH** button.
REFRESH button	Click to update Information area with current information.
Timestamp	Date and time that the error occurred.
SN	Unique system-assigned sequence number of the event.
Type	Type of error: INFO, ERROR, CRITICAL, or WARNING.
Message	Text that briefly describes the error.

Table 5-8   Diagnostics Window Items (continued)

Item	Description
Pagination controls	Click a control to go to the first, next, last, or previous page in the Information area.
Items per page drop-down list	Choose the maximum number of errors that appear in the Information area. Options are **5**, **10**, **20**, **50**, and **100**.
EVENTS Tab	
Search field	To display only information for events that have text in the App ID, Event Type, and Message fields that contains a specific character string, enter the string in the Search field and then click the **Search** button. To clear a search, delete characters in the field and press **Enter**.
REFRESH button	Click to update Information area with current information.
Timestamp	Date and time that the event occurred.
SN	Unique system-assigned sequence number of the event.
Source	Cisco IOx component that generated the event.
Severity	Severity level of the event.
App ID	Identifier of the app to which the event relates.
Event Type	Descriptive term that indicates the type of event.
Message	Text that briefly describes the event.
Pagination controls	Click a control to go to the first, next, last, previous, or specific page in the Information area.
Items per page drop-down list	Choose the maximum number of events that appear in the Information area. Options are **5**, **10**, **20**, **50**, and **100**.
SYSTEM Tab	
REFRESH button	Click to update Information area with current information.
BACK button	Appears when you are viewing system information. Click to exit the information display.
Diagnostics	Items for which you can view diagnostic information: • summary—High-level system-wide information • memory—Memory use on the device • disk—Disk use on the host device • process—Information about Cisco IOx processes that are running on the device • networking—Information about networking configuration and status on the device • application—Information about Cisco IOx apps that are installed on the device
Action	Click **Run (Normal Mode)** to display summary information for the corresponding Diagnostics field item.

Table 5-8   Diagnostics Window Items (continued)

Item	Description
Extended Action	Click **Run (Detail Mode)** to display detail information for the corresponding Diagnostics field item.
APP MANAGER JOBS Tab	
REFRESH button	Click to update Information area with current information.
Job ID	Unique system-assigned identifier of the job.
Type	Type of the job.
Start Time	Date and time that the job started.
End Time	Date and time that the job ended.
Status	Status of the job (CREATED, SUBMITTED, STARTED, WAITING, FAILED, COMPLETED, SCHEDULED, PAUSE).
Message	Information that relates to the job.
Pagination controls	Click a control to go to the first, next, last, previous, or specific page in the Information area.
Items per page drop-down list	Choose the maximum number of app manager jobs that appear in the Information area. Options are **5**, **10**, **20**, **50**, and **100**.
APP LIFE CYCLE Tab	
REFRESH button	Click to update Information area with current information.
Task ID	Unique system-assigned identifier of the app lifecycle task.
Job ID	Unique system-assigned identifier of the job of which this app lifecycle task is part.
App Deploy ID	Unique system-assigned identifier that was assigned to the app when it was deployed in Cisco Fog Director.
Type	Type of the app lifecycle task (DEPLOY, START. STOP, UNDEPLOY, UPDATE).
Start Time	Date and time that the app lifecycle task started.
End Time	Date and time that the app lifecycle task ended.
Status	Status of the app lifecycle task (CREATED, FILE_TRANSFER_SUBMITTED, STARTED, IN_PROGRESS, FILE_TRANSFERRING, SUCCEEDED, FAILED, CANCELLED, FILE_TRANSFR_FAILED, RETRIED).
Message	Information that relates to the app lifecycle task.
Pagination controls	Click a control to go to the first, next, last, previous, or specific page in the Information area.
Items per page drop-down list	Choose the maximum number of app lifecycle items that appear in the Information area. Options are **5**, **10**, **20**, **50**, and **100**.

Obtaining Device Logs

To troubleshoot a device, you can view and download a device log file that you can review or provide to Cisco for assistance. The file contains log information that was generated by the device. If the Collect Debug Logs option on the Device Details page is set to **Yes**, the log file also includes debug information.

To create a log file for a device, follow these steps:

Procedure

Step 1   In Cisco Fog Director, click the **DEVICES** tab.

Step 2   In the Device table on the Devices View page, click the IP address or the hostname of the device for which you want to create a log file.

Step 3   Click the **Yes** button next to Collect Debug Logs near the top right of the screen.

Step 4   Try to reproduce the issue that you are troubleshooting.

Step 5   Take either of these actions:

- To review log information, click the **View Device Logs** button.

  The Device Logs window displays. This window lets you view information in any of the device files that the device generates. You can take the following actions in this window:

  – Click a log file name near the top of the window to display the first 10 lines from that file, if the device supports tailing of device log files. Otherwise, the entire log file displays.

  – Choose an option from the drop-down list to update the display of lines for the file that you chose. Options are **Last 10 Lines**, **Last 25 Lines**, **Last 100 Lines**, or **Full log**, if the device supports tailing of log files. If the device does not support tailing, **Full log** is the only option.

  – Click the **Refresh** button to update the log file display with current information.

- To save a log file, click the **Download Tech Support Logs** button and then follow the on-screen prompts to save the log file in the location of your choice.

Step 6   (Optional) To stop collecting log information, click the **No** button next to Collect Debug Logs.

Accessing an App via a Console

You can access an installed on a device via a console. After you access an app, you can use Linux console commands to obtain information about it.

Cisco Fog Director provides the command and related information that you can use to access an app via a console.

To access an app via a console, perform the following steps.

Before You Begin

Use Cisco IOS configuration options to forward an SSH port on the router that you want to use for console access to port 22.

Procedure

Step 1   Take either of these actions to display the Device Details page for the device on which you want to access the app via a console:

- On the Devices View page, double-click a circle in a Top 5 Consumers chart.

- On the Apps View page or the Devices View page, click the hostname or the IP address of a device anywhere that either of these items displays as a link.

Step 2   On the Device Details page, take these actions to obtain the private key that you need for console access:

a.   In the App Console Support area at the bottom of the page, click the ***app_id*.pem** link that displays in the sample command, where *app_id* is the identifier of the app.

b.   In the dialog box that displays, follow the prompts to download the *app_id*.pem file.

c.   Use a text editor to open the *app_id*.pem file, highlight and copy all text that displays.

Make sure to include the "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----" text.

Step 3   On the system from which you logged in to Cisco Fog Director, take these actions:

a.   Use a text editor to create a text file called *app_id*.pem, where *app_id* is the identifier of the app whose container or VM you want to access.

b.   Paste the private key that you copied into this file, and save it locally.

c.   Make sure that this file has the Linux permission 600.

Step 4   Take these actions to connect to the host system from a console:

a.   From the console system, start an SSH client.

b.   Enter the following command to obtain the SSH port required for console access:

> show running-config | i 22

c.   Enter the command that displays in the App Console Support area on the Device Details page.

When you enter the command:

- Replace **SSH_PORT** with the port number for console access.

- Replace ***app_id*.pem** with the path to the file that you created in Step 3, if the file is not in the current directory.

d.   Use the commands in your SSH client to complete the connection process.