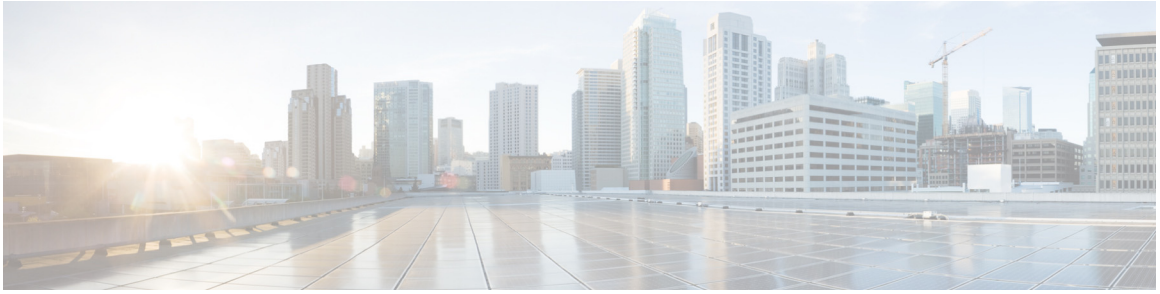
Cisco Fog Director Reference Guide

Release 1.6

March 30, 2018

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



Preface

Overview

This manual explains how to use Cisco Fog Director to manage, administer, monitor, and troubleshoot Cisco IOx apps and devices.

Organization

This manual is organized as follows:

Chapter 1, "Overview"	Provides an overview of Cisco IOx, Cisco Fog Director, and the life-cycle of a Cisco IOx app
Chapter 2, "Installing Cisco Fog Director"	Provides instructions for installing Cisco Fog Director
Chapter 3, "Cisco Fog Director General Operations"	Describes general operations that you perform with Cisco Fog Director
Chapter 4, "Managing Apps"	Describes the Cisco Fog Director Apps page, from which you manage app
Chapter 5, "Managing Devices"	Describes the Cisco Fog Director Devices page, from which you manage devices
Chapter 6, "Managing Cisco Fog Director Settings"	Describes the Cisco Fog Director Settings page, from which you view information about Cisco Fog Director and manage its debug logs
Chapter 7, "Managing Cartridges"	Describes the Cisco Fog Director Cartridges page, from which you manage cartridges

Obtaining Documentation and Support

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*. This document also lists new and revised Cisco technical documentation. It is available at:

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

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

Overview

This chapter provides an overview of Cisco IOx, Cisco Fog Director, and the lifecycle of a Cisco IOx app. It includes these sections:

About Cisco IOx

Cisco IOx is an application enablement platform that provides uniform and consistent hosting capabilities for various types of applications, or *apps*, across various Cisco platforms. This platform brings together Cisco IOS, the industry-leading networking operating system, and Linux, the leading open source platform. Linux-based applications can run on Cisco devices in the Cisco IOx framework, so using this platform, you can bring custom applications and interfaces to the network.

With Cisco IOx, developers can create a wide variety of IoT apps, such as data aggregation system and control systems.

About Cisco Fog Director

Cisco Fog Director allows administrators to manage, administer, monitor, and troubleshoot Cisco IOx apps and devices. It provides a web-based user interface from which you can perform activities that include the following:

- Install and uninstall apps
- Start and stop apps
- Upgrade apps
- View the status of apps
- Backup and restore apps
- Monitor apps and devices and collect statistics
- Create and obtain debug logs for troubleshooting

App Configuration Caveat

Cisco Fog Director provides options for configuring apps as described in the "Reconfiguring App Parameters" section on page 4-32. You can use these options or another tool, such as Cisco IOx Local Manager or a custom device manager, to configure an app. However, if you use another tool, the configuration updates that you make are not synced to Cisco Fog Director. As a best practice, we recommend that you use only the Cisco Fog Director configuration options or another tool to configure an app that you manage with Cisco Fog Director, and that you do not switch between tools to configure that app.

Hardware Platform Caveat

Cisco C800 series devices do not provide dedicated storage for apps. These devices have a single, soldered-on flash storage that is shared between Cisco IOS and apps. The flash storage is not field replaceable.

Flash has a finite number of P/E cycles. It is expected to last for the duration of the device lifecycle if the flash is used only for Cisco IOS configuration. If apps write to the flash frequently, flash wear out becomes a serious concern.

We recommend that developers and users monitor and throttle the frequency of writes to flash. If an app demands frequent writes or a large amount of data storage, we recommend that data be exported for off-device storage.

App Health Script

An app developer can write a health script for an app and include that script as part of the app package. If an app includes a health script, the Cisco application-hosting framework monitors the health of the app. If app monitoring determines that an app is unhealthy, the App Health field in Apps area on the Device Details page displays **UNHEALTHY**. In this situation, you can use the **Show report** link in the Apps Area to view error information and health information output from the monitor script. This information can help you resolve the health issue.

For information about developing a health script, see the "Application Health Monitoring" section in *IOx Application Developer Guide*, which is available at the following URL:

https://developer.cisco.com/site/iox/docs/#application-development-concepts

For information about the UNHEALTHY app state in Cisco Fog Director, see the "Apps Area" section on page 5-12.

App Lifecycle

The following table provides the general operations that are involved in the lifecycle of a Cisco IOx app. Use this information as a guide as you deploy apps. There are many additional operations that you can perform as needed. Although those operations are not listed in this table, they are described in detail in this manual.

	Operation	Reference
Step 1	Add to Cisco Fog Director each device on which the app is to be installed.	See the "Adding Devices" section on page 5-17 or the "Importing Devices" section on page 5-19.
Step 2	Add to Cisco Fog Director cartridges that PAAS apps require.	See the "Adding a Cartridge Manually" section on page 7-2
Step 3	Upload the app to Cisco Fog Director. The app is now an *unpublished app* and displays in the Unpublished Apps section on the Cisco Fog Director Apps View page. It is now in Cisco Fog Director but not yet ready to be installed on a device.	See the "Adding an App" section on page 4-10.
Step 4	Publish the unpublished app in Cisco Fog Director. The app is now an *available app* and displays in the Available Apps section on the Cisco Fog Director Apps View page. The app can now be installed on a device.	See the "Publishing an App" section on page 4-13.
Step 5	Use Cisco Fog director to update or add information for the app as needed. This information includes an icon, description, release notes, and external links.	See the "Editing an App Icon, Description, and Release Notes" section on page 4-31 and the "Configuring App Links" section on page 4-41.
Step 6	Use Cisco Fog Director to install the available app on one or more devices. The app is now an *installed app* and displays in the Installed Apps section on the Cisco Fog Director Apps View page.	See the "Installing an App" section on page 4-13.
Step 7	Use Cisco Fog Director to reconfigure the app if needed.	See the "Reconfiguring App Parameters" section on page 4-32.
Step 8	To keep the app current, use Cisco Fog Director to upgrade the app when needed.	See the "Upgrading an App" section on page 4-26.

Installing Cisco Fog Director

This chapter describes how to install or upgrade Cisco Fog Director and provides related deployment information. It includes these sections:

Installation

The following sections describes how to install the Cisco Fog Director OVA file on a virtual machine (VM).

System Requirements

The VM host on which you install must meet the following minimum requirements:

- 4 core CPU
- 6 GB RAM
- 100 GB hard disk

Installation in VMware vSphere

To install Cisco Fog Director in VMware vSphere Hypervisor, perform the following steps.

Before You Begin

- Review the information in the "System Requirements" section on page 2-1.

- Make sure that you have a valid Cisco.com user ID and password, which are required to obtain the VM OVA image for installation.

Procedure

Step 1 From a client PC, take these actions to obtain the VM OVA image:

a. Go to the following URL and click the **IOx Fog Director Software** link in the Select a Software Type box:

https://software.cisco.com/download/type.html?mdfid=286290097&catid=null

b. Click the **Download** button that corresponds to the .ova file that you want.

c. Follow the on-screen instructions to download the file to your local drive.

Step 2 From a client PC, use the VMware vSphere Hypervisor client application to log in to your VMWare host.

Step 3 Choose **File > Deploy OVF Template**.

The Deploy OVF Template Wizard starts.

Step 4 In the Deploy OVF Template Wizard, take these actions:

a. In the Deploy OVF Template window, locate to and select the Fog Director OVF template that you downloaded in Step 1, and then click **Next**.

b. In the OVF Template Details window, click **Next**.

c. In the Name and Location window Inventory Location area, choose the VM host on which to install the OVA file, and then click **Next**.

d. In the Datastore window, click the datastore in which to store the VM files, and then click **Next**.

e. In the Host / Cluster window, click **Next**.

f. In the Specify a Specific Host window, click **Next**.

g. In the Disk Format window, click **Next**.

h. In the Network Mapping window, click **Next**.

i. (Optional) In the Ready to Complete window, if DCHP is configured in your environment and you want Cisco Fog Director to start automatically when the installation completes, check the **Power on after deployment** check box.

j. In the Ready to Complete window, click **Finish**.

Step 5 When the Deployment Completed Successfully window displays, click **Close** in that window.

The installation is completes. If needed, configure a static IP address as described in the "DHCP Configuration" section on page 2-5 before you start Cisco Fog Director.

Installation in VMware Player

To install Cisco Fog Director in VMware Player, perform the following steps.

Before You Begin

- Review the information in the "System Requirements" section on page 2-1.

- Make sure that you have a valid Cisco.com user ID and password, which are required to obtain the VM OVA image for installation.

Procedure

Step 1 From a client PC, take these actions to obtain the VM OVA image.:

a. Go to the following URL and click the **IOx Fog Director Software** link in the Select a Software Type box:

https://software.cisco.com/download/type.html?mdfid=286290097&catid=null

b. Click the **Download** button that corresponds to the .ova file that you want.

c. Follow the on-screen instructions to download the file to your local drive.

Step 2 From a client PC, use the VMware Player client application to log in to your VMWare host.

Step 3 In the right side of the Welcome window, click **Open a Virtual Machine**.

Step 4 Follow the on-screen prompts to locate and select the he Fog Director OVF template that you downloaded in Step 1.

Step 5 In the Import Virtual Machine dialog box, click the **Import** button.

The installation completes. If needed, configure a static IP address as described in the "DHCP Configuration" section on page 2-5 before you start Cisco Fog Director.

Installation in VMWare Fusion

To install Cisco Fog Director in VMware Fusion, perform the following steps.

Before You Begin

- Review the information in the "System Requirements" section on page 2-1.
- Make sure that you have a valid Cisco.com user ID and password, which are required to obtain the VM OVA image for installation.

Procedure

Step 1 From a client PC, take these actions to obtain the VM OVA image.:

a. Go to the following URL and click the **IOx Fog Director Software** link in the Select a Software Type box:

https://software.cisco.com/download/type.html?mdfid=286290097&catid=null

b. Click the **Download** button that corresponds to the .ova file that you want.

c. Follow the on-screen instructions to download the file to your local drive.

Step 2 From the File menu, choose **Import**.

Step 3 In the Choose an Existing Virtual Machine dialog box, click **Choose File** and follow the on-screen prompts to locate and select the he Fog Director OVF template that you downloaded in Step 1.

Step 4 In the Choose an Existing Virtual Machine dialog box, click **Choose File** button.

The installation completes. If needed, configure a static IP address as described in the "DHCP Configuration" section on page 2-5 before you start Cisco Fog Director.

Upgrade

You can upgrade Cisco Fog Director release 1.5 to Cisco Fog Director release 1.6. When you do so, your current Cisco Fog Director data is migrated to the new release.

To upgrade Cisco Fog Director release 1.5 to release 1.6, follow these steps:

Procedure

Step 1 Create a create a backup file of your Cisco Fog Director 1.5 data as described in the "Creating a Backup File" section on page 6-5.

Step 2 From a client PC, take these actions to obtain the VM OVA image for Cisco Fog Director 1.6:

a. Go to the following URL and click the **IOx Fog Director Software** link in the Select a Software Type box:

https://software.cisco.com/download/type.html?mdfid=286290097&catid=null

b. Click the **Download** button that corresponds to the .ova file that you want.

c. Follow the on-screen instructions to download the file to your local drive.

Step 3 Use the VM OVA image that you downloaded to deploy a VM for Cisco Fog Director 1.6.

Step 4 Take these actions to update Cisco Fog Director 1.6 with the information in the backup file that you created in Step 1:

a. Start and log in to Cisco Fog Director release 1.6.

b. Click the **Settings** tab and then click the **Settings** sub-tab.

The Settings page displays.

c. In the Backup & Restore area on the Settings page, click the **RESTORE** button.

The Restore dialog box displays.

d. In the Decryption password field in the Restore dialog box, enter the passphrase that you created for the backup file.

e. Click **SELECT BACKUP ARCHIVE** in the Restore dialog box, and then navigate to and select the backup file that you copied to the client PC.

The system updates Cisco Fog Director 1.6 with the information in the backup file. This process can take some time, depending on how much data is in the backup file.

When the upgrade completes, the Cisco Fog Director 1.6 Log In page displays.

DHCP Configuration

By default, Cisco Fog Director fetches an IP address from your DHCP server when it starts. If your environment does not support DHCP, you can configure a static IP address for Cisco Fog Director.

To configure a static IP address, follow these steps:

Procedure

Step 1 From a VMware console, to log in to the VM on which you installed Cisco Fog Director.

Use the following log in credentials:

- Username—**fogdir**
- Password—**fogdir**

Step 2 Use the **sudo vi** command to open the /etc/network/interfaces file.

Step 3 In the interfaces file, update the following fields as needed:

- address
- netmask
- gateway
- dns-nameservers

The following shows an example of the interfaces file:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address <ip address>
netmask <subnet mask>
gateway <gateway ip address>
dns-nameservers <name server add 1> <name server add 2> <name server add 3> //optional
```

Step 4 Save the interfaces file and reboot the VM

RADIUS Authentication

By default, Cisco Fog Director permits logging in only by users whose user names and passwords successfully authenticate against its internal database. You can configure Cisco Fog Director to instead permit logging in only by users whose user names and passwords successfully authenticate against a RADIUS database on a designated RADIUS server.

To configure Cisco Fog Director to authenticate users only against a RADIUS database on a designated RADIUS server, perform the following steps.

Before You Begin

Make sure that a configured RADIUS server is available for use by Cisco Fog Director and that you know the IP address and the shared secret of that server.

Procedure

Step 1 Access the Cisco Fog Director server via an SSH client.

The default user name and password for logging in to the server both are **fogdir**.

Step 2 Enter the following commands to stop Cisco Fog Director and edit the appmgr.properties file on the server:

- prompt% **sudo service fogd stop**
- prompt% **cd /opt/cisco/fogdirector/dist/appmgr/WEB-INF/classes/META-INF/spring**
- prompt% **sudo vi appmgr.properties**

Step 3 In the appmgr.properties file, update the **authentication.radius.serverIPAddress** parameter to include the IP address of the RADIUS server and update the **authentication.radius.serverSharedSecret** parameter to include the shared secret for the RADIUS server.

Here is an example of an appmgr.properties file that includes the IP address 10.255.255.254 and the shared secret 12345:

```
#radius server properties
authentication.radius.enabled=true
authentication.radius.serverIPAddress=10.255.255.254
authentication.radius.serverSharedSecret=12345
#optional radius server auth port, defaults to 1812
#authentication.radius.serverAuthPort=1812
#optional radius server accounting port, defaults to 1813
#authentication.radius.serverAcctPort=1813
#optional radius server connection timeout, defaults to 2000 ms
#authentication.radius.serverTimeOut=2000
```

Step 4 Save and close the appmgr.properties file.

Step 5 Enter the following command to restart Cisco Fog Director:

prompt% **sudo service fogd start**

Cisco Fog Director now permits logging in only by users whose user names and passwords successfully authenticate against the RADIUS database on the RADIUS server.

Step 6 Exit the SSH session.

Docker Daemon Proxy Settings

If you are adding or upgrading an app and want to have Cisco Fog Director create and upload an app package from a Docker image that is in a third party registry, and if Cisco Fog Director can access that registry only via an HTTP proxy server, you must configure the Docker daemon proxy settings in the Cisco Fog Director virtual machine before you perform the add or upgrade procedure. To do so, follow these steps:

Procedure

Step 1 Access the Cisco Fog Director server via an SSH client.

Step 2 Use a text editor to open the docker file in the /etc/default directory.

Step 3 Locate the line that appears as **#export http_proxy=http://*server*:*port*/** and take these actions:

- **a.** Delete the pound sign (#) at the beginning of the line to uncomment this command.
- **b.** Replace *server* with the IP address or the host name of the HTTP proxy server through which Cisco Fog Director accesses the registry.
- **c.** Replace *port* with and port on which the HTTP proxy server listens for requests.

Step 4 Save and close the docker file.

Step 5 Enter the following commands to stop Cisco Fog Director, restart the Docker service, and then restart start Cisco Fog Director:

prompt% **sudo service fogd stop**

prompt% **sudo service docker restart**

prompt% **sudo service fogd start**

Step 6 Exit the SSH session.

Cisco Fog Director General Operations

This chapter describes general operations that you perform with Cisco Fog Director.

This chapter includes these sections:

Browser Guidelines

The following browser guidelines apply to Cisco Fog Director:

- You can access the Cisco Fog Director user interface by using Mozilla Firefox release 44 and above or Google Chrome release 48 and above
- For increased system security, a Cisco Fog Director browser session times out after a 30 minute period of no use
- To ensure that a Cisco Fog Director page shows the most current information, use your browser Refresh feature to periodically update the page that you are viewing

Accessing Cisco Fog Director

After you install Cisco Fog Director, you can access it from any supported computer that has IP connectivity to the Cisco Fog Director server.

To access Cisco Fog Director, follow these steps:

Procedure

Step 1 Start a supported browser, and in the Address field, enter the fully-qualified hostname or the IP address of the server on which Cisco Fog Director is running.

If you are logging in for the first time, the End User License Agreement (EULA) dialog box displays. Otherwise, the Log In page displays.

Step 2 If the End User License Agreement dialog box displays, review the EULA and click the **Accept** button to continue.

Step 3 Enter your Cisco Fog Director ID in the **LOGIN ID** field, and enter your Cisco Fog Director Password in the **PASSWORD** field.

IDs and passwords are case-sensitive, so make sure to enter them exactly as they are configured.

The default Fog Director ID is **admin** and the default password is **admin**.

Step 4 Click **Login**.

If you entered the default password (admin), the system prompts you to change your password. Otherwise, the Cisco Fog Director Apps page displays.

Step 5 If the system prompts you to change your password, take these actions:

a. Enter your new password in the **NEW PASSWORD** and **CONFIRM PASSWORD** fields.

The password is case-sensitive and can include any number of alphanumeric and special characters, but no spaces.

b. Click **CHANGE PASSWORD**.

c. Enter your new password in the **PASSWORD** field.

d. Click **Login**.

Viewing Notifications

A notification is a system message that Cisco Fog Director provides. For example, the system provides a notification when a new version of Cisco Fog Director is available.

When notifications have been provided and not addressed, the Notification icon in the Cisco Fog Director menu bar displays the number of notifications. For example, this icon indicates that you have one notification: .

To see a summary of notifications, hover your mouse pointer over the Notification icon. If you hover your mouse pointer over the icon when there are no notifications, the system displays the message "You're all caught up!"

To see detailed information about notifications, click the Notification icon and then click the desired notification summary box.

Exiting Cisco Fog Director

To exit Cisco Fog Director, click the **Logout** button from any Cisco Fog Director page.

The Log In page displays.

Changing Your Cisco Fog Director Password

To change your Cisco Fog Director password, follow these steps:

Procedure

Step 1 Take either of these actions:

- If you are logged in to Cisco Fog Director, click the **Logout** button .
- If you are not logged in to Cisco Fog Director, start a supported browser, and in the Address field, enter the fully-qualified hostname or the IP address of the server on which Cisco Fog Director is running.

The Log In page displays.

Step 2 Enter your Cisco Fog Director ID in the **LOGIN ID** field, and enter your Cisco Fog Director Password in the **PASSWORD** field.

IDs and passwords are case-sensitive, so make sure to enter them exactly as they are configured.

Step 3 Enter your new password in the **NEW PASSWORD** and in the **CONFIRM NEW PASSWORD** fields.

The password is case-sensitive and can include any number of alphanumeric and special characters, but no spaces.

Step 4 Click **CHANGE PASSWORD**.

To cancel a password change operation, click **Login** instead of **CHANGE PASSWORD**.

Understanding Managed and Unmanaged States for Apps

Cisco Fog Director considers a Cisco IOx app to be in *managed state* when you can manage the app on a device by using Cisco Fog Director. Cisco Fog Director considers an app to be in *unmanaged state* when the app has been added to device by a method other than using Cisco Fog Director.

In general, a Cisco IOx app is in managed state when it has been installed on a device through Cisco Fog Director. However, in some scenarios in which an app already is installed on a device using a method other than Cisco Fog Director, the app does not go to managed state when device is then added to Cisco Fog Director.

This section provides an overview of the general steps to take in these scenarios to ensure that an app is in managed state.

Scenario 1

If an app is in unmanaged state on a device, follow these steps to change it to managed state:

	Procedure	Reference
Step 1	Take either of these actions: • Uninstall the app from the device by using Cisco Fog Director, Cisco IOx Client, or Cisco IOx Local Manager • Delete the device from Cisco Fog Director	To uninstall the app, see the "Uninstalling an App" section on page 4-22, your Cisco IOx Client documentation, or your Cisco IOx Local Manager documentation To delete the device, see the "Deleting Devices" section on page 5-36.
Step 2	If you uninstalled the app from the device, remove the app from the Installed App area on the Cisco Fog Director App View page by clicking the Remove button in this area for the app.	See the "Managing Installed Apps" section on page 4-2
Step 3	Add or import the device to Cisco Fog Director.	See the "Adding Devices" section on page 5-17 or the "Importing Devices" section on page 5-19.
Step 4	Add the app to Cisco Fog Director.	See the "Adding an App" section on page 4-10.
Step 5	Install the app on the device using Cisco Fog Director.	See the "Installing an App" section on page 4-13.

Scenario 2

If you have a device on which an app is installed using a method other than Cisco Fog Director, follow these steps to ensure that the app does not go to unmanaged state with you add the device to Cisco Fog Director:

	Procedure	Reference
Step 1	Take either of these actions: • Uninstall the app from the device by using Cisco Fog Director, Cisco IOx Client, or Cisco IOx Local Manager • Delete the device from Cisco Fog Director	To uninstall the app, see the "Uninstalling an App" section on page 4-22, your Cisco IOx Client documentation, or your Cisco IOx Local Manager documentation To delete the device, see the "Deleting Devices" section on page 5-36.
Step 2	Add the app to Cisco Fog Director.	See the "Adding an App" section on page 4-10.
Step 3	Add or import the device to Cisco Fog Director.	See the "Adding Devices" section on page 5-17 or the "Importing Devices" section on page 5-19.
Step 4	Install the app on the device using Cisco Fog Director.	See the "Installing an App" section on page 4-13.

Scenario 3

An app goes to unmanaged state if the following occurs:

1. You add a device to Cisco Fog Director.
2. You install the app on the device by using Cisco Fog Director.
3. You delete the device from Cisco Fog Director (with the app still installed on the device).
4. You delete the app from Cisco Fog Director.

5. You add the device again to Cisco Fog Director.

To prevent the app from going to unmanaged state, follow these steps before you add the device again to Cisco Fog Director:

	Procedure	Reference
Step 1	Add the app to Cisco Fog Director.	See the "Adding an App" section on page 4-10.
Step 2	Add or import the device to Cisco Fog Director.	See the "Adding Devices" section on page 5-17 or the "Importing Devices" section on page 5-19.

Troubleshooting

The following sections provide information that can be useful for troubleshooting Cisco Fog Director. In addition, the Cisco Fog Director apps pages and device pages provide information and features that you can use to monitor and troubleshoot apps.

- Cisco Fog Director Logs, page 3-5
- Cisco Fog Director Processes, page 3-6

Cisco Fog Director Logs

Cisco Fog Director provides several options for viewing or obtaining logs for apps, devices, and the system. You can use these logs to monitor operations or troubleshoot issues that occur.

Logs are stored in the /opt/cisco/fogdirector/logs folder on the server on which Cisco Fog Director is running.

Table 3-1 describes the logs and provides references to sections that provide more detailed information.

Table 3-1 Logs for Troubleshooting

Log	Description	Reference
App log	Log information that is generated by an app on a device.	See the description of the **View App Log** button in the "Viewing Detailed Monitoring Information" section on page 4-62. Also see the description of the App Log tab and View all App Logs in the "Apps Area" section on page 5-12

Table 3-1 Logs for Troubleshooting (continued)

Log	Description	Reference
Device log	Log information that is generated by the device.	See the description of Collect Debug Logs, the **VIEW DEVICE LOGS** button, and the **DOWNLOAD TECH SUPPORT LOGS** button in the "Device Details Area" section on page 5-7. Also see the "Obtaining Device Logs" section on page 5-47
Cisco Fog Director debug log	Information about actions performed by users, and errors or exceptions generated by a device or persistent store.	See the "Managing Cisco Fog Director Debug Logs" section on page 6-2.

Cisco Fog Director Processes

To operate properly, Cisco Fog Director requires that its processes be running on the server on which it is installed. If you experience problems with Cisco Fog Director, such as its web-based user interface becoming unresponsive, you can check the status of the processes and stop and restart them if needed.

To manage Cisco Fog Director processes, use an SSH client to access the server on which Cisco Fog Director is installed, log in using your Cisco Fog Director user name and password, and then use the commands that Table 3-2 describes.

Table 3-2 Managing Cisco Fog Director Processes

Activity	Command	Remarks
Display the status of Cisco Fog Director processes.	**# sudo service fogd status**	If Cisco Fog Director is not operating properly, use this command to ensure that all processes are running.
Stop Cisco Fog Director processes.	**# sudo service fogd stop**	If the Cisco Fog Director web-based user interface becomes unresponsive, use these commands to stop and then start the Cisco Fog Director processes. Restarting processes in this way may resolve the issue.
Start Cisco Fog Director processes.	**# sudo service fogd start**	

Managing Apps

The Cisco Fog Director Apps pages provide information about Cisco IOx apps, and provide access to features for managing these apps and performing related operations.

When you log in to Cisco Fog Director, the Apps View page displays, If no apps have yet been added to Cisco Fog Director, this page displays "Welcome to Cisco Fog Director" and displays the **ADD NEW APP** button and the **IMPORT APPS** button.

If at least one app has been added, this page includes these areas:

- Installed Apps area—Lists apps that have been installed, are scheduled to be installed, or are in the process of being installed, through Cisco Fog Director on at least one device. Also provide information about these apps and devices, and access to other features and information for managing these apps. (An app that has been installed and then removed from a device appear in this area until you manually remove it from this area.)
- Available Apps area—Lists apps that have been published are so are available to be installed on one or more devices. Also provide information about these apps and devices, and access to other features and information for managing these apps.
- Unpublished Apps area—Lists apps that have been uploaded to Cisco Fog Director but that have not been published.

If an app requires or IOxCore and IOxGPS service package, you can install the service package from the Apps View page. For more information, see, *IOx Services Architecture*, which is available here: https://developer.cisco.com/docs/iox/#iox-services-architecture/iox-services-architecture.

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

This chapter includes these sections:

Managing Installed Apps

The Installed Apps area on the Apps View page lists each app that is installed through Cisco Fog Director on at least one device or that is scheduled to be installed, provides information about these apps, and provides access to related features.

For an app that is scheduled to be installed, this area displays the message "*App_name* is scheduled to install on # devices." In this message, *App_name* is the name of the app and # is the number of devices on which the app is scheduled to be installed. You can click the number to display the Actions page, which provides detailed information about the scheduled installation and lets you perform related activities (see the "Managing Outstanding and Expired Actions for Apps" section on page 4-53). For information about scheduling app actions, see the "Using Action Plans" section on page 4-49.

For each installed app, this area includes the items that Table 4-1 describes.

Table 4-1 Installed Apps Area Items

Item	Description
Search Installed apps field	To display in Installed Apps area only apps that have names that contain a specific character string, enter the string in this field. The display of apps updates as you type. To display all installed apps, delete all characters in the search field.
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 Installed or Available App" section on page 4-6.
Device counter	Number of devices on which the app is installed.
Alert counter	Number of Alerts that the app has generated. Click to manage alerts. See the "Managing App Alerts" section on page 4-63.

Table 4-1 Installed Apps Area Items (continued)

Item	Description
Status button	Click to display text and a chart that provide information about the states of an app that is installed on at least one device. App states can include the following: • Running—App is running on a device • In Progress—App is in the process of installing on a device • Stopped—An app that was running has been stopped on a device • Failed—A start, stop, install, uninstall, upgrade, or configuration action that was performed on an app did not execute properly The text that describes each state shows the number of devices on which the app in that state and the total number of devices on which the app is installed For example, "8/12 Running" means that the app is installed on 12 devices and is running on 8 of them. The donut chart provides a visual representation of each state of an app as a percentage of the number of devices on which the app is installed. Hover your mouse pointer over any section of a chart to see what state that section represents and the percentage of devices on which the app is in that state. Click a chart to display monitoring information for the app, as described in the "Monitoring an App" section on page 4-59.
Memory button	Click to display the hostnames of up to 5 devices on which the app has consumed the most CPU resources during the past 24 hours.The percentage value next to a hostname indicates the average amount of CPU resources the app consumed on the device during the past 24 hours. Click a hostname to display device detailed information about the device. See the "Viewing Detailed Information about a Device" section on page 5-6 for more information.
CPU button	Click to display the hostnames of up to five devices on which the app has consumed the most RAM resources during the past 24 hours, and the amount of memory, in MG, consumed on each device.The percentage value next to a hostname indicates the average amount of RAM resources the app consumed on the device during the past 24 hours. Click a hostname to display device details information about the device. See the See the "Viewing Detailed Information about a Device" section on page 5-6 for more information.
Remove button	Appears if an app is not currently installed on any device. Click to remove the app from the Installed Apps area.

Managing Available Apps

The Available Apps area on the Apps View page lists each app that has been published, provides information about these apps, and provides access to related features. An available app is ready to be installed on one or more devices.

The Available Apps area includes the items that Table 4-2 describes.

Table 4-2 Available Apps Area

Item	Description
Export Apps button	See the "Backing Up and Restoring Apps" section on page 4-58.
App icon, name, and version	Displays the name, version, and icon of each available 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 Installed or Available App" section on page 4-6.
App signed status icon	If Cisco Fog Director knows whether an app is signed, a shield icon appears next to the app version number. A green shield icon indicates that the app is signed. A red shield icon indicates that the app is not signed. If Cisco Fog Director does know whether an app is signed, no shield icon appears.
Update button for each app	Lets you upload a newer version of an app to Cisco Fog Director. See the "Upgrading an App" section on page 4-26.
Unpublish button for each app	See the "Unpublishing an App" section on page 4-13.

Managing Unpublished Apps

The Unpublished Apps area on the Apps View page on the Apps View page lists each app that has been uploaded to Cisco Fog Director and is not yet published. An unpublished app must be published before it can be installed on one or more devices.

The Unpublished Apps area includes the items that Table 4-3 describes.

Table 4-3 Unpublished Apps Area Items

Item	Description
Add New App button	Lets you upload an app to Cisco Fog Director. See the "Adding an App" section on page 4-10.
App icon, name, and version	Displays the name, version, and icon of each unpublished app.Click an icon to display additional information for the app, as described in Table 4-4 on page 4-5.

Table 4-3 Unpublished Apps Area Items (continued)

Item	Description
App signed status icon	If Cisco Fog Director knows whether an app is signed, a shield icon appears next to the app version number. A green shield icon indicates that the app is signed. A red shield icon indicates that the app is not signed. If Cisco Fog Director does know whether an app is signed, no shield icon appears.
Publish button for each app	Lets you publish an app, which makes it available for installation on a device. See the "Publishing an App" section on page 4-13.
Remove button for each app	See the "Removing an App" section on page 4-31.

When you click an app icon in the Unpublished Apps area, a configuration page displays. The items that this page displays vary depending on the type of the app, and can include the items that Table 4-4 describes.

Table 4-4 Unpublished Apps Area > Configuration Page Items

Item	Description
App icon	The icon that displays in Cisco Fog Director for the app. This icon comes from an image file that you specify. You can click **Edit Icon** to select an image file as described in the "Editing an App Icon, Description, and Release Notes" section on page 4-31.
Author	Entity that authored the app, as specified in the app metadata.
Resource Profile	Resource profile of the app, which specifies the amount of host system CPU and memory (RAM) resources that the app requires on a device. For information about assigning resource profiles to an app, see *Cisco IOx Local Manager Reference Guide*.
CPU	Number of CPU units that the app requires on a device.
Memory	Amount of RAM, in KB, that the app requires on a device.
Disk	Amount of disk space, in MB, that the app requires on a device.
App Type	Type of the app (**PaaS**, **VM**, or **Docker**)
Runtime	Runtime environment that the app requires on a device.
CPU Architecture	Type of device on which the app is supported.
App Links	Appears if you configured links for an app. Click a link to go to the configured resource. See the "Configuring App Links" section on page 4-41.
UPGRADE PKG button	Lets you upload a newer version of an app to Cisco Fog Director. See the "Upgrading an App" section on page 4-26.
PUBLISH button	Click to publish the app, which makes the app available for installation on devices. See the "Publishing an App" section on page 4-13.

Table 4-4 Unpublished Apps Area > Configuration Page Items (continued)

Item	Description
SAVE button	Click to save updates that you make to the description or release notes for the app. See the "Editing an App Icon, Description, and Release Notes" section on page 4-31.
Description	Brief description of the app that displays when you view detailed information for the app. You can click **Edit** next to "Description" to enter description text as described in the "Editing an App Icon, Description, and Release Notes" section on page 4-31.
Release Notes	Notes for the app that appear when you view detailed information for the app. For example, notes might include a list and descriptions of features added in an updated app. You can click **Edit** next to "Release Notes" to enter release note text as described in the "Editing an App Icon, Description, and Release Notes" section on page 4-31.
Packaged Services	Appears only for an app that provides services and lists the service APIs that the includes. This type of app includes services that are defined in the service-bundle section in the package.yaml file for a the app. These services can be consumed by other apps.
App Links button	Let you configure external links for an app. See the "Configuring App Links" section on page 4-41.

Viewing Detailed Information about an Installed or Available App

To view detailed information about an installed app or available, click its icon in the Installed Apps area or in the Available Apps area on the Apps View page. The App Configuration page displays.

This page includes information and features that apply to the app. The items that this page displays vary depending on the state of the app, and can include the items that Table 4-5 describes.

Table 4-5 Detailed Information about an Installed or Available App Items

Item	Description
General information	The name of the app, its version, and the date and time it was last updated. If Cisco Fog Director knows whether an app is signed, a shield icon appears next to the app version number. A green shield icon indicates that the app is signed. A red shield icon indicates that the app is not signed.If Cisco Fog Director does know whether an app is signed, no shield icon appears.
Author	Entity that authored the app, as specified in the app metadata.
CPU	Number of CPU units that the app requires on a device.
Memory	Amount of RAM, in KB, that the app requires on a device.

Table 4-5 Detailed Information about an Installed or Available App Items (continued)

Item	Description
Disk	Amount of disk space, in MB, that the app requires on a device.
App Type	Type of the app (**PaaS**, **VM**, or **Docker**)
Runtime	Runtime environment that the app requires on a device.
CPU Architecture	Type of device on which the app is supported.
App Links	Appears if you configured links for an app. Click a link to go to the configured resource. See the "Configuring App Links" section on page 4-41.
INSTALL button	Lets you install an app on one or more devices. See the "Installing an App" section on page 4-13.
MONITOR APP button	Displays information about the operation of the app and its resource consumption on devices See the "Monitoring an App" section on page 4-59.
UNINSTALL button	Lets you uninstall an app from one or more devices. See the "Uninstalling an App" section on page 4-22.
Installation Successful on display	Shows the number of devices on which the app has been successfully installed. The **EDIT CONFIGURATION** button under this display lets you update configuration parameters that apply to an app, These items may include configuration information, resource profile, networking, and port information. See the "Reconfiguring App Parameters" section on page 4-32 for more information.
Actions Failed on display	Shows the number of devices on which an installation, update, uninstall, or reconfiguration action failed for the app. Hover your mouse pointer over this area to see more detailed information about specific action failure types. You can click the **RETRY NOW** button retry an action. See the "Retrying a Failed Action for an App" section on page 4-45 for more information.
Upgrade Required on display	After you add and publish a newer version of an already-published app, this field displays the app version number (in the left column) and the number of devices on which the corresponding app version should be upgraded to the newer version (in the right column). You can click the **UPGRADE** button to perform the upgrade. See the "Upgrading an App" section on page 4-26 for more information.
View Outstanding Actions link	Appears if an install, edit, upgrade, or uninstall action for the app is in Outstanding state or in Expired state as a result of an action plan, Click to display the Actions page, which provides options for managing actions that are in these states. See the "Managing Outstanding and Expired Actions for Apps" section on page 4-53 for more information.

Table 4-5 Detailed Information about an Installed or Available App Items (continued)

Item	Description
Installing Display	Displays information about the devices on which the app is installing. This information includes: • One or more *device squares*. Each one represents a device on which you are installing the app and shows the status of the install operation on that device. You can hover your mouse pointer over a device square to display the Edit Resource Profile dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and the resource profile that has been assigned for the app on the device You can click the hostname and IP address in the dialog box to exit the installation and display the Device Details page for the device. • The hostname of the device on which the app is installing and the status and progress of the installation operation on that device. Click the hostname to display detailed information about the device, as described in the "Viewing Detailed Information about a Device" section on page 5-6. • A search device field, which you can display by clicking the expand icon next to Search Device. Enter the IP address or hostname of a device to see the status of the app installation process on that device.

Table 4-5 Detailed Information about an Installed or Available App Items (continued)

Item	Description
App State on installed devices display	Includes a chart that provides a visual representation of the number of devices on which the app in a particular state. Hover your mouse pointer over any section of a chart to see what state that section represents and the number of devices on which the app is in that state. Click any section of the chart to display a table with detailed information about each device on which the app is in the state. This table includes the following: • App state and percentage—Name of the state, and the percentage of devices on which the app is installed that the app is in that state. • 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 the app is in the state. Click a hostname to display detailed information about the device. See the See the "Viewing Detailed Information about a Device" section on page 5-6 for more information. • IP address—IP address of the device on which the app is in the state. Click an IP address to display detailed information for the device. See the "Viewing Detailed Information about a Device" section on page 5-6 for more information. • 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. • Error Summary—For an app that is in the Failed state, provides information about the cause of the action that failed. • 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.
Description	Brief description of the app. See the "Editing an App Icon, Description, and Release Notes" section on page 4-31 for related information.
Release Notes	Release notes for the app. See the "Editing an App Icon, Description, and Release Notes" section on page 4-31 for related information.

Adding an App

Adding a Cisco IOx app uploads the app package for the app to Cisco Fog Director. When you add an app, it displays in the Unpublished area on the Apps View page and becomes available to be published.

When you add an app, you can choose to upload an app package that was created with the Cisco IOx SDK, or choose to have Cisco Fog Director create and upload an app package from a Docker image that is in the Cisco Docker registry or in a third party registry such as Docker Hub.

To add an app, perform the following steps.

Before You Begin

- If you are uploading an app package that was created with the Cisco IOx SDK, the app package must be on your local drive.
- If you are creating and uploading an app package from a Docker image, the app descriptor file (package.yaml), if used, and the configuration parameters file (package_config.ini) for the Docker image must be on your local drive. In addition, you must make the configuration update as described in the "Docker Daemon Proxy Settings" section on page 2-7. (If you do not use a package.yaml file for a Docker app, Cisco Fog Director generates metadata from the Docker image automatically.)

Procedure

Step 1 On the Apps View page, click the **Add New App** button.

If other apps have already been added, this button displays In the Unpublished Apps area,

Step 2 In the dialog box that displays, take either of these actions:

- To upload an app package that was created with the Cisco IOx SDK, click the **Upload from my computer radio** button, click the **Select App Package** button, and then follow the on-screen prompts to locate and select on your local drive the app that you want to add.

  The app is added to Cisco Fog Director and a page with the items that Table 4-6 on page 4-11 displays. The items in this page depend on the type of app that you added.
- To create and upload an app package from a Docker image that is present in a Docker registry, click the **Create from Docker image** button, and then continue to Step 3.

Step 3 If you chose to have Cisco Fog Director create an app package from a Docker image, take these actions:

1. In the **Image name or ID** field, enter the name or ID of the Docker image.
2. (Optional) In the **Image tag** field, enter a tag for the Docker image.

   If you do not enter a tag name, Cisco Fog Director uses the tag named "latest."
3. If the Docker image is in a Docker registry other than Docker Hub, enter either of the following in the **Docker Registry** field:

   - Hostname and optional port of the Docker registry, in the format *hostname*[**:***port*]

   - IP address and optional port of the Docker registry, in the format *ip_address*[**:***port*]

   If the Docker image is in Docker Hub, leave the **Docker Registry** field blank.
4. (Optional) If the Docker registry requires authentication before you can pull an image from it, and if you did not instruct Cisco Fog Director to remember your credentials for this registry when you previously added or upgraded a Docker app, take these actions:

   – In the **Registry Username** field, enter the user name that authenticates you to the Docker Registry.

- In the **Registry Password** field, enter the password that authenticates you to the Docker Registry.
- Check the **Remember these credentials** check box if you want Cisco Fog Director to store the user name and password that you enter and automatically populate the **Username** and **Password** fields with this information the next time you add or upgrade a Docker app.

If you instructed Cisco Fog Director to remember your credentials for this registry when you previously added or upgraded a Docker app, the message "You have saved credentials (*username*). Use them?" displays below the **Image requires authentication to pull** check box. Click either of the following options that also appear:

- **Yes, use them**—Causes Cisco Fog Director to use the user name and password that have been stored.
- **No, forget them**—Causes Cisco Fog Director to no longer store the user name and password for this Docker registry. In you choose this option, enter the user name and password that authenticate you to the Docker registry in the **User Name** and **Password** fields that appear. If you want Cisco Fog Director to remember these credentials, check the **Remember these credentials** check box.

5. Click the **Browse** button next to **Choose package.yaml and package_config.ini files** and then follow the on-screen prompts to locate and select on your local drive the following files that relate to the Docker image:
   - package.yaml (optional)—App descriptor file
   - package_config.ini—Configuration parameters file

   The files that you select are listed under the **Browse** button. To remove a file from this list, click the Remove icon ✕ next to the file.
6. Click the **SUBMIT** button.

   Cisco Fog Director creates an app by packaging the Docker image and related files and adds the app.

   A dialog box appear while the add process executes. This process can take some time.

   When the app is added to Cisco Fog Director, a page with the items that Table 4-6 on page 4-11 displays. The items in this page depend app that you added.

Table 4-6 Added App Page Items

Item	Description
Edit Icon	Click to add an icon for the app. See the "Editing an App Icon, Description, and Release Notes" section on page 4-31.

Table 4-6 Added App Page Items (continued)

Item	Description
App Information	Includes the following information • Name of the app • Latest version—Version of the app that you added • Last updated—Date and time that the app was last updated • Docker image name—Name or ID of the docker image, depending on the information that you entered, if Cisco Fog Director created the app from a Docker image • Docker Repository—Docker repository that you entered, if Cisco Fog Director created the app from a Docker image • Tag—Tag of the Docker image, if Cisco Fog Director created the app from a Docker image and you designated a tag
Author	Entity that authored the app, as specified in the app metadata.
Resource Profile	Resource profile of the app, which specifies the amount of host system CPU and memory (RAM) resources that the app requires on a device. For information about assigning resource profiles to an app, see *Cisco IOx Local Manager Reference Guide*.
CPU	Number of CPU units that the app requires on a device.
Memory	Amount of RAM, in KB, that the app requires on a device.
Disk	Amount of disk space, in MB, that the app requires on a device.
Services	Name of another app that provides services that the app requires.
App Type	Type of the app (**PaaS**, **VM, LXC**, or **Docker**)
Runtime	Runtime environment that the app requires on a device.
App Links button	Let you configure external links for an app. See the "Configuring App Links" section on page 4-41.
UPGRADE PKG button	Lets you upload a newer version of an app to Cisco Fog Director. See the "Upgrading an App" section on page 4-26.
PUBLISH button	Click to publish the app, which makes the app available for installation on devices. See the "Publishing an App" section on page 4-13.
SAVE button	Click to save updates that you make to the description or release notes for the app. See the "Editing an App Icon, Description, and Release Notes" section on page 4-31.
Description	Brief description of the app that displays when you view detailed information for the app. You can click **Edit** next to "Description" to enter description text as described in the "Editing an App Icon, Description, and Release Notes" section on page 4-31.

Table 4-6 Added App Page Items (continued)

Item	Description
Release Notes	Notes for the app that appear when you view detailed information for the app. For example, notes might include a list and descriptions of features added in an updated app. You can click **Edit** next to "Release Notes" to enter release note text as described in the "Editing an App Icon, Description, and Release Notes" section on page 4-31.

Publishing an App

You can publish an app after it has been added to Cisco Fog Director. A published app becomes available to install on devices.

To publish an app, take any of these actions:

- In the Unpublished Apps area on the Apps View page, click the **Publish** button that displays under the app that you want to publish
- In the page that displays when you add an app, click the **PUBLISH** button.

After you perform the Publish action, the app moves from the Unpublished Apps area to the Available Apps area on the Apps View page.

Unpublishing an App

Unpublishing an app moves the app to the unpublished area and makes it unavailable for installation on any device. Unpublishing an app does not remove it from devices on which it is installed already.

To unpublish an app, click the **Unpublish** button under the icon for the app.

Installing an App

You can install a published app on a device that has been added or imported to Cisco Fog Director.

The following sections provide additional information:

- Install App Options, page 4-13
- Install App Procedure, page 4-15

Install App Options

To view options for installing an app, click the **INSTALL** button on the App Configuration page for the app.

The Filter Devices page displays. This page includes the items that Table 4-7 describes.

Table 4-7 Filter 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. • 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 4-7 Filter Devices Page Items (continued)

Item	Description
Selected Devices table	Provides information about each device on which you want to install the app. Devices appear in this table after you check their check boxes in the Installed Devices table and then click **ADD SELECTED DEVICES**. This table includes the following items: • Selected Devices—Number of devices on which you want to install the app. • 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.
Next button	Available if there is at least one device in the Selected Devices table. Click to continue an app install procedure.

Install App Procedure

To install an app on one or more devices, perform the following steps.

If you are installing an app on multiple devices and want to stop the installation procedure at any time, unpublish the app as described in the "Unpublishing an App" section on page 4-13.

Cisco Fog Director associates an action plan with each app installation procedure that you perform. An action plan instructs Cisco Fog Director to retry an installation if the installation fails due to certain conditions, or to perform the installation within a designated maintenance window. By default, the action plan causes Cisco Fog Director to perform the installation immediately and to retry a failed installation up to 10 times at 2 minute intervals. You can change these parameters as needed when you perform the

app installation procedure. For more information, see the "Using Action Plans" section on page 4-49.

Before You Begin

- Add or import each device on which you are installing the app to Cisco. Fog Director. See the "Adding Devices" section on page 5-17 or the "Importing Devices" section on page 5-19.
- Add the app to Cisco Fog Director. See the "Adding an App" section on page 4-10.
- Publish the app. See the "Publishing an App" section on page 4-13.
- If the app that you are installing requires services from an app that provides services, the app that provides the services must first be installed on the devices on which you are installing this app. Otherwise, this app install operation fails.

Procedure

Step 1 In the Available Apps area on the Apps View page, click the icon for the app that you want to install, and then click the **INSTALL** button.

Step 2 In the Installed Devices table, check the check box for each device on which you want to install the app.

For detailed information about this table and locating devices, see the "Install App Options" section on page 4-13.

Step 3 Click the **ADD SELECTED DEVICES** button.

The devices that you selected and on which the app can be installed are added to the Selected Devices table. The app will be installed on the devices that this table lists. For detailed information about this table and about removing devices from this table, see the "Install App Options" section on page 4-13.

Step 4 Click the **Next** button near the bottom of the page.

The Installation Summary page displays. This page lets you review and configure operations that are performed by Cisco Fog Director on the devices on which you are installing the app.

Step 5 (Optional) In the Installation Summary page, expand **Selected Devices** (if it is not expanded already) to review the following information for each device that you selected:

- Host Name—Hostname of the device.
- IP Address—IP address of the device.
- Tags—Tags that are assigned to the device.
- 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.

You can click a pagination control to go to the first, next, last, previous, or specific page in the table. From the **Items per page** drop-down list you can choose the maximum number of devices that appear in each page of the table.

Step 6 In the Installation Summary page, take the following actions as needed:

- (Optional) To change the list of devices that you selected, click the **Back** button, update information in the Selected Devices table as described earlier in this procedure, and then click the **Next** button again.
- (Optional) To change the default tag that will be added to each device, type another tag name in the **Tag Selected Devices as** field.

By default, the system adds a tag with the app name to each device. You can change this name, or, if you do not want a tag to be added, delete all text in this field. See the "Managing Tags for Devices" section on page 5-37 for related information.

- (Optional) To cause the app to start automatically after it installs, check the **Start app after installation** check box. 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.
- (Optional) Click the **VIEW INCOMPATIBLE DEVICES** button (if this button is not dimmed) to see a table that provides information about devices that you selected but on which the app cannot be installed. This table includes the following items:
  - Host Name—Hostname of the device.
  - IP Address—IP address of the device.
  - Tags—Tags that are assigned to the device.
  - 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.
  - Incompatibility Cause—A brief description of why the app cannot be installed on the device.

  You can click a pagination control to go to the first, next, last, previous, or specific page in the table. From the **Items per page** drop-down list you can choose the maximum number of devices that appear in each page of the table.

Step 7 (Optional) In the Installation Summary page, expand **Customize Configuration** to view and update configuration information for this app.

The configuration items that display are defined in the package_config.ini file for the app. The value that each field displays is the default value for that item as defined by the app. You can make updates in these fields as needed.

Step 8 (Optional) In the Installation Summary page, expand **Configure Resource Profiles** to view and update the resource profiles that have been assigned for the app on each device.

You can update the resource profile for a specific device, some devices, or all devices.

The *device squares* in the box in the middle of the Configure Resource Profile area represent devices on which you are installing the app. You can hover your mouse pointer over a device square to display the Edit Resource Profile dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and the resource profile that has been assigned for the app on the device. You can click the hostname and IP address in the dialog box to exit the installation and display the Device Details page for the device.

To update a resource profile on one or more devices, take these actions:

a. If you want to limit the device squares displays to one or more specific devices, take either of these actions:
  - 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.

b. Take the desired action:
  - To change the resource profile for a specific device, hover your mouse pointer over the device square for that device, and in the Edit Resource Profile dialog box, choose a resource profile from the **Select Profile** drop-down list.
  - To change the resource profile for all devices for which a device square displayed, click the desired profile radio button and then click the **REASSIGN PROFILE** button:

- **Exact matching profile**—Assigns the resource profile that is defined for the app in its metadata, if the resources are available on a device.

- **Largest available profile**—Assigns the largest resource profile that is currently available on each device on which you are installing.

- **Allocate all available resources**—Assigns all CPU and memory resources that are available on each device on which you are installing.

- **Custom profile**—On each device on which you are installing, assigns the CPU and memory resources that you specify. After you click this radio button, the **CPU** and the **Memory** fields appear. Enter the CPU resources, in units, and memory resources, in MB, to assign on each device. The Max value under each field shows the maximum value that you can enter without exceeding the available corresponding resource on at least one device. If you enter a value that exceeds this maximum value, the **REASSIGN PROFILE** button is dimmed and cannot be used.

Step 9 (Optional) In the Installation Summary page, expand **Configure Networking** to view and update network information that relates to how the app obtains its IP address or addresses on each device.

The Configure Networking area is available only if its options apply to this installation.

You can update network information for a specific device, some of devices, or all devices. If network information is not configured for a device by default, you must configure it as described in this step.

The *device squares* in the box at the left of the Configure Networking area represent devices on which you are installing the app. You can hover your mouse pointer over a device square to display the Edit Network Details dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and network interface information for each network interface that is defined in the package_config.ini file for the app.

The Preferred Networks sub areas at the right of the Configure Networking area provide information for each network interface that is defined in the package_config.ini file for the app. You can expand a sub area to display and update options in it.

If you want to limit the device squares to one or more specific devices, take either of these actions:

- 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 reassign network information for an app on one or more devices, take either of these actions:

- To change network information for a specific device, take these actions:
  a. Hover your mouse pointer over the device square for that device, and in the Edit Network Details dialog box, choose a network for the corresponding network interface from the **Select Network** drop-down list. Network options are:

  - **iox-bridge#**—App obtains its IP address from a DCHP pool that is configured in Cisco IOS

  - **iox-nat#**—App obtains its IP address from an internal network address translator

  b. If you choose **iox-bridge#** and if you want to assign a static IP address from the DHCP pool for this network interface, check the **Static Mode** check box that displays. If you check this check box, the network interface uses IP addresses that are dynamically assigned from the DCHP pool.

  c. If you check the **Static Mode** check box, configure the following fields that appear as needed:

- **IPv# Address** and **Mask** fields—Enter the static address and subnet mask to use. If the IPv6required field is set to "true" in the app descriptor file (package.yaml) for an app, you must enter an IPv6 address. Otherwise, you can enter an IPv4 or an IPv6 address. If you enter an IPv6 address but a device on which you are installing the app does not support IPv6, the app installation will fail on that device.

- **DNS** field—(Optional) Enter the IP address of the DNS server that the app uses for external communication.

- **Default Gateway** field—(Optional) Enter the IP address of the default gateway that the app uses for external communication.

- To update network information for all devices for which a device square is displayed, take these actions for each network interface that you want to configure:

  a. Expand the Preferred networks sub area.

  b. Choose a network from the **Select Network** drop-down list. Network options are:

  - **iox-bridge#**—App obtains its IP address from a DCHP pool that is configured in Cisco IOS

  - **iox-nat#**—App obtains its IP address from an internal network address translator

  c. If you choose **iox-bridge#**, click one of the following radio buttons that appear:

  - **Static**— Click to assign a static IP address from the DHCP pool for this network interface

  - **Dynamic**—Click to use a dynamically assigned IP address from the DCHP pool for this network interface

  d. If you click the **Static** radio button, configure the following fields that appear as needed:

  - **IPv# Address** and **Mask** fields—Enter the static address and subnet mask to use. If the IPv6required field is set to "true" in the app descriptor file (package.yaml) for an app, you must enter an IPv6 address. Otherwise, you can enter an IPv4 or an IPv6 address. If you enter an IPv6 address but a device on which you are installing the app does not support IPv6, the app installation will fail on that device.

  - **Default Gateway** field—(Optional) Enter the IP address of the default gateway that the app uses for external communication.

  - **DNS** field—(Optional) Enter the IP address of the DNS server that the app uses for external communication.

  e. After you configure each network interface that you want, click the **REASSIGN NETWORKS** button.

Step 10 (Optional) In the Installation Summary page, expand **Configure VNC Password** to set the VNC password that is required to access an app on devices via a VNC session.

The Configure VNC Password area is available only if the app requests a serial port.

The *device squares* in the box in the middle of the Configure VNC Password area represent devices on which you are installing the app. You can hover your mouse pointer over a device square to display the Edit VNC password dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and provides a field for entering the VNC password for the device.

To set the VNC password for an app on one or more devices, take these actions:

a. If you want to limit the device squares to one or more specific devices, take either of these actions:

– 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.

b. Take either of these actions:

- To set the VNC password for a specific device, hover your mouse pointer over the device square for that device, and in the Edit VNC Password dialog box, enter the password in the **VNC Password** field
- To set the VNC password for all devices for which a device square is displayed, enter the password in the **VNC Password** field that displays to the right of the device squares, and then click the thee **Assign** button.

Step 11 (Optional) In the Installation Summary page, expand **Configure VCPUs** to configure the number of virtual CPUs that the app requires on a device.

The Configure VCPUs area is available only if the app requests virtual CPUs.

The *device squares* in the box in the middle of the Configure VCPUs area represent devices on which you are installing the app. You can hover your mouse pointer over a device square to display the Edit VCPU Details dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and the number of virtual CPUs that have been assigned for the app on the device.

To configure the number of virtual CPUs that an app requires on one or more devices, take these actions:

a. If you want to limit the device squares to one or more specific devices, take either of these actions:

- 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.

b. Take either of these actions:

- To configure the number of virtual CPUs for a specific device, hover your mouse pointer over the device square for that device, and in the Edit VCPU dialog box, type or use the up or down arrow buttons to enter the desired value.
- To configure the number of virtual CPUs for all devices for which a device square is displayed, in the **Select VCPU Value** field that displays to the right of the device square, type or use the up or down arrow buttons to enter the desired value, and then click the **REASSIGN VCPU** button. The text above the **Select VCPU Value** field indicates the number of virtual CPUs that the descriptor file for the app specifies and the maximum number of virtual CPUs that you can designate for the app on the devices that you selected.

Step 12 (Optional) In the Installation Summary page, expand **Configure Device Resource Ports** to view and update the serial port that an app uses on a device.

The Configure Device Resource Ports area is available only if the app requests a serial port.

The *device squares* in the box in the middle of the Configure Device Resource Ports area represent devices on which you are installing the app. You can hover your mouse pointer over a device square to display the Edit Serial Details dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and the serial port that has been assigned for the app on the device.

To update a serial port for an app on one or more devices, take these actions:

a. If you want to limit the device squares to one or more specific devices, take either of these actions:

- 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.

b. Hover your mouse pointer over the device square for the device that you want to update, and in the Edit Serial Details dialog box, choose a port from the **Select Serial Port** drop-down list.

Step 13 (Optional) In the Installation Summary page, expand **Configure Action Plan** to choose, view, modify or add an action plan.

The action plan designates how many times and at what interval Cisco Fog Director retries an action if the action fails on a device due to certain device reachability or network connectivity issues. If Cisco Fog Director cannot complete the app installation action after the number of retries that the action plan designates, the app installation does not complete.

When you expand **Configure Action Plan**, the **Selected Action Plan** field shows the name of the action plan that is in effect. The **Details** field describes the number of retries and time between retries that the selected action plan defines.

You can choose the action plan that you want from the Selected Action Plan drop-down list.

For information about modifying or adding action plans, see the "Using Action Plans" section on page 4-49.

Step 14 (Optional) In the Installation Summary page, expand **Network Status** to view network, resource, and related information for apps and devices.

The Network Status area displays the following information:

- How many of the devices that you selected for installation of the app are reachable. ("Reachable" means that Cisco Fog Director can communicate with the device.) Hover your mouse pointer over a graph to see more detailed information.
- The *device squares* in the box in the middle of the area. Each box represents a device on which you are installing the app. You can hover your mouse pointer over a device square to display the following information:
  - **Cartridges**—Cisco cartridges that a PAAS app requires to run. These cartridges must already be uploaded to Cisco Fog Director (see Chapter 7, "Managing Cartridges") and are installed automatically on the device as part of the app installation process.
  - **CPU Availability**—Number of free CPU units on the device.
  - **Memory Availability**—Amount of free RAM, in MB, on the device.
- How often the Cisco Fog Director updates the information in this area. You can choose a value from the **Collect resource usage at least every** drop-down list. Options are **Every 15 mins**, **Every 1 hour**, **Every 4 hour**, **Every 8 hour**, **Every 16 hour**, and **Never ever**.

Step 15 (Optional) In the Installation Summary page, expand **Upload App Data** to upload an app data file for the app to each device

An app data file is a file that an app requires, such as a configuration file.

To update an app data file to one or more devices, take these actions:

a. (Optional) In the **File path on app container** field, 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.

b. (Optional) In the **New file name** field, 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.

c. Click the **SELECT FILES** button 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.

Step 16 When you are satisfied with the information on the Installation Summary page, click the **DONE, LET'S GO** button.

The App Configuration page displays, as described in the "Viewing Detailed Information about an Installed or Available App" section on page 4-6.

While the app is installing on a device, the status of the installation displays for that device. Click the device to see the progress of the installation. You can click the **ABORT** button under the status display to abort the installation action, as described in the "Aborting an Action" section on page 4-42.

If the Actions Failed display on this page indicates that the installation failed on any device, you can take any of these actions:

- Click the **RETRY NOW** button to try the installation on these devices again. See the "Retrying a Failed Action for an App" section on page 4-45.
- Click the **View Outstanding Actions** link to display the Actions page, which provides options for managing failed actions for which an action plan is in effect. See the "Managing Outstanding and Expired Actions for Apps" section on page 4-53 for more information.
- Wait for Cisco Fog Director to retry the failed action according to an action plan that is in effect. See the "Using Action Plans" section on page 4-49.

Uninstalling an App

You can uninstall an app from any device on which it is running. Uninstalling an app removes it from the device and releases device CPU and memory (RAM) resources that were reserved for it.

You can uninstall an app that is in any state.

The following sections provide additional information:

Uninstall App Options

To view options for uninstalling an app, click the **UNINSTALL APP** button on the App Configuration page for the app.

A page displays that includes the items that Table 4-8 describes.

Table 4-8 Uninstall App Items

Item	Description
Installed Devices table	Provides information about each device on which the app is installed, 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. • 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 from which you want to uninstall 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 installed. • IP Address—IP address of the device on which the app is installed. • Tags—Tags that are assigned to the 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 4-8 Uninstall App Items (continued)

Item	Description
Selected Devices table	Provides information about each device from which you want to uninstall the app. Devices appear in this table after you check their check boxes in the Installed Devices table and then click **ADD SELECTED DEVICES**. This table includes the following items: • Selected Devices—Number of devices from which you want to remove the app. • 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 from which you want to uninstall the app. • IP Address—IP address of the device from which you want to uninstall the app. • Tags—Tags that are assigned to the device from which you want to uninstall 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 and does not remove the app from 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.
DONE, LET'S GO button	Executes an uninstall operation.

Uninstall App Procedure

Uninstalling an app removes the installed app from one or more devices.

When you uninstall a Docker app, layers that are used by that app are not deleted automatically. If you want to delete these layers, see the "Managing Layers" section on page 5-41. If you do not delete a layer, it is reused if you later install an app that requires it.

Cisco Fog Director associates an action plan with each app uninstallation procedure that you perform. An action plan instructs Cisco Fog Director to retry an uninstallation if the uninstallation fails due to certain conditions, or to perform the uninstallation within a designated maintenance window. By default, the action plan causes Cisco Fog Director to perform the uninstallation immediately and to retry a failed uninstallation up to 10 times at 2 minute intervals. You can change these parameters as needed when you

perform the app uninstallation procedure. For more information, see the "Using Action Plans" section on page 4-49.

To uninstall an app, follow these steps:

Procedure

Step 1 Take either of these actions:

- In the Installed Apps area on the Apps View page, click the icon for the app that you want to uninstall, and then click the **UNINSTALL** button.
- In the Available Apps area on the Apps View page, click the icon for the app that you want to uninstall, and then click the **UNINSTALL** button.

Step 2 In the Installed Devices table, check the check box for each device from which you want to uninstall the app.

For detailed information about this table and locating devices, see the "Uninstall App Options" section on page 4-22.

Step 3 Click the **ADD SELECTED DEVICES** button.

The devices with checked check boxes are added to the Selected Devices table. The app will be uninstalled from devices that this table lists. For detailed information about this table and about removing devices from this table, see the "Uninstall App Options" section on page 4-22.

Step 4 (Optional) In the Installation Summary page, expand **Configure Action Plan** to choose, view, modify or add an action plan.

The action plan designates how many times and at what interval Cisco Fog Director retries an action if the action fails on a device due to certain device reachability or network connectivity issues. If Cisco Fog Director cannot complete the app uninstallation action after the number of retries that the action plan designates, the app uninstallation does not complete.

When you expand **Configure Action Plan**, the **Selected Action Plan** field shows the name of the action plan that is in effect. The **Details** field describes the number of retries and time between retries that the selected action plan defines.

You can choose the action plan that you want from the Selected Action Plan drop-down list.

For information about modifying or adding action plans, see the "Using Action Plans" section on page 4-49.

Step 5 Click the **DONE, LET'S GO** button.

The App Configuration page displays, as described in the "Viewing Detailed Information about an Installed or Available App" section on page 4-6.

While the app is uninstalling on a device, the status of the uninstallation displays for that device. Click the device to see the progress of the uninstallation. You can click the **ABORT** button under the status display to abort the uninstallation action, as described in the "Aborting an Action" section on page 4-42.

If the Actions Failed display on this page indicates that the uninstallation failed on any device, you can take any of these actions:

- Click the **RETRY NOW** button to try the uninstallation on these devices again. See the "Retrying a Failed Action for an App" section on page 4-45.
- Click the **View Outstanding Actions** link to display the Actions page, which provides options for managing failed actions for which an action plan is in effect. See the "Managing Outstanding and Expired Actions for Apps" section on page 4-53 for more information.

- Wait for Cisco Fog Director to retry the failed action according to an action plan that is in effect. See the "Using Action Plans" section on page 4-49.While the uninstallation is in progress, you can click the **ABORT** button on the App Configuration page that displays, as described in the "Aborting an Action" section on page 4-42.

Upgrading an App

When an new version of an installed app becomes available, you can upgrade the app. This process includes uploading the app package for the app to Cisco Fog Director and then upgrading devices with the new app version.

When you upgrade an app, you can choose to upload an app package that was created with the Cisco IOx SDK, or choose to have Cisco Fog Director create and upload an app package from a Docker image that is in the Cisco Docker registry or in a third party registry such as Docker Hub.

When you upgrade a Docker app, layers that are used by the previous version and the upgraded version of the app are reused automatically. Layers that are not used by the upgraded version are not deleted automatically. If you want to delete these layers, see the "Managing Layers" section on page 5-41.

Cisco Fog Director associates an action plan with each app upgrade procedure that you perform. An action plan instructs Cisco Fog Director to retry an upgrade if the upgrade fails due to certain conditions, or to perform the upgrade within a designated maintenance window. By default, the action plan causes Cisco Fog Director to perform the upgrade immediately and to retry a failed upgrade up to 10 times at 2 minute intervals. You can change these parameters as needed when you perform the app upgrade procedure. For more information, see the "Using Action Plans" section on page 4-49.

To upgrade an app, perform the following steps.

Before You Begin

If you are uploading an app package that was created with the Cisco IOx SDK, the app package must be on your local drive.

If you are creating and uploading an app package from a Docker image, the app descriptor file (package.yaml), if used, and the configuration parameters file (package_config.ini) for the Docker image must be on your local drive. In addition, you must make the configuration update as described in the "Docker Daemon Proxy Settings" section on page 2-7. (If you do not use a package.yaml file for a Docker app, Cisco Fog Director generates metadata from the Docker image automatically.)

If you are upgrading an app that provides services, you must first uninstall other apps that uses the services that this app provides.

Procedure

Step 1 If you are not viewing the page that displays when you add an app, in the Available Apps area on the Apps View page, click the icon for the app for the app to upgrade.

Step 2 Click the **UPGRADE PKG** button.

Step 3 In the dialog box that displays, take either of these actions:

- To upload an app package that was created with the Cisco IOx SDK, click the **Upload from my computer radio** button, click the **Select App Package** button, and then follow the on-screen prompts to locate and select on your local drive the app that you want to add.

  The app package that you select uploads to Cisco Fog Director. Skip to Step 5.

- To create and upload an app package from a Docker image that is present in a Docker registry, click the **Create from Docker image** button, and then continue to Step 4.

Step 4 If you chose to have Cisco Fog Director create an app package from a Docker image, take these actions:

a. In the **Image name or ID** field, enter the name or ID of the Docker image.

b. (Optional) In the **Image tag** field, enter a tag for the Docker image.

If you do not enter a tag name, Cisco Fog Director uses the tag named "latest."

c. If the Docker image is in a Docker registry other than Docker Hub, enter either of the following in the **Docker Registry** field:

– Hostname and optional port of the Docker registry, in the format *hostname*[**:***port*]

– IP address and optional port of the Docker registry, in the format *ip_address*[**:***port*]

If the Docker image is in Docker Hub, leave the **Docker Registry** field blank.

d. (Optional) If the Docker registry requires authentication before you can pull an image from it, and if you did not instruct Cisco Fog Director to remember your credentials for this registry when you previously added or upgraded a Docker app, take these actions:

– In the **Registry Username** field, enter the user name that authenticates you to the Docker Registry.

– In the **Registry Password** field, enter the password that authenticates you to the Docker Registry.

– Check the **Remember these credentials** check box if you want Cisco Fog Director to store the user name and password that you enter and automatically populate the **Username** and **Password** fields with this information the next time you add or upgrade a Docker app.

If you instructed Cisco Fog Director to remember your credentials for this registry when you previously added or upgraded a Docker app, the message "You have saved credentials (*username*). Use them?" displays below the **Image requires authentication to pull** check box. Click either of the following options that also appear:

– **Yes, use them**—Causes Cisco Fog Director to use the user name and password that have been stored.

– **No, forget them**—Causes Cisco Fog Director to no longer store the user name and password for this Docker registry. In you choose this option, enter the user name and password that authenticate you to the Docker registry in the **User Name** and **Password** fields that appear. If you want Cisco Fog Director to remember these credentials, check the **Remember these credentials** check box.

e. Click the **Browse** button next to **Choose package.yaml and package_config.ini files** and then follow the on-screen prompts to locate and select on your local drive the following files that relate to the Docker image:

– package.yaml (optional)—App descriptor file

– package_config.ini—Configuration parameters file

The files that you select are listed under the **Browse** button. To remove a file from this list, click the Remove icon ✕ next to the file.

f. Click the **SUBMIT** button.

Cisco Fog Director creates an app by packaging the Docker image and related files and adds the app.

A dialog box appear while the add process executes. This process can take some time.

Step 5 Click the **Publish** button on the Configuration page.

The app is published, which makes it available for upgrading, and the Apps View page displays.

Step 6 Take these actions to upgrade devices with the app that you uploaded:

a. In the Installed Apps area on the Apps View page, click the icon for the app to upgrade.

b. Click the **UPGRADE** button, which displays under the "Upgrade Required on" display.

   The Filter Devices page displays. This page includes the items that Table 4-7 on page 4-14 describes.

c. In the table, check the check box for each device on which you want to upgrade the app, and then click the **ADD SELECTED DEVICES** button.

d. Click the **Next** button.

   The Upgrade Summary page displays.

e. (Optional) To change the list of devices that you selected, click the **Back** button, update information in the Selected Devices table as described earlier in this procedure, and then click the **Next** button again.

f. (Optional) In the Upgrade Summary page, check the **Retain App Data** check box cause the app upgrade process to retain existing information that the app has written to the device.

   This information includes files and data that the app has written to the device, such as app log files and app property files, and that is stored in the /data directory for the app on the device.

   If this check box is not checked, the app upgrade process deletes existing information that the app has written to the device.

   This check box is checked by default.

g. (Optional) In the Upgrade Summary page, expand **Selected Devices** (if it is not expanded already) to see a table that displays the following information for each device that you selected for the app upgrade:

   – Host Name—Hostname of the device.

   – IP Address—IP address of the device.

   – Tags—Tags that are assigned to the device.

   – 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.

   You can take the following actions in the Selected Devices area:

   – Use the pagination controls 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 devices that appear in each page of the table.

   – Displays the tag that has been assigned to each device See the "Managing Tags for Devices" section on page 5-37 for related information.

   – Click the **VIEW INCOMPATIBLE DEVICES** button (if this button is not dimmed) to see a table that provides information about devices that you selected but on which the app cannot be upgraded. This table includes the following items:

     - Host Name—Hostname of the device.

     - IP Address—IP address of the device.

     - Tags—Tags that are assigned to the device.

- 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.

- Incompatibility Cause—A brief description of why the app cannot be upgraded on the device.

You can click a pagination control to go to the first, next, last, previous, or specific page in the table. From the **Items per page** drop-down list you can choose the maximum number of devices that appear in each page of the table.

h. (Optional) In the Upgrade Summary page, expand **Customize Configuration** to instruct Cisco Fog Director whether to retain or update existing configuration information for the app.

This area includes sub areas for each version of the app that currently is installed on a device. You can expand a sub area to display and update designated app configuration information for the corresponding app version. The information that displays is defined in the package_config.ini file for the app.

The fields that a sub area displays and the action that Cisco Fog Director takes when you upgrade the app depend on the status of the **Retain app configuration changes done on selected devices and merge configuration from this version** check box as follows:

– Checked—The fields that display are new configuration fields that are available in this version of the app. The value in each field is the default value for that item as defined by the app. You can make updates as needed in these fields. The upgrade process applies the configuration information in these fields but makes no changes to configuration information that exists for the current version of the app on a device.

– Unchecked—The fields that display are all configuration fields (both new in this version and existing) that are available in this version of the app. The value in each field is the default value for that item as defined by the app. You can make updates as needed in these fields. The upgrade process applies the configuration information in these fields and overwrites configuration information that exists for the current version of the app on a device.

This check box is checked by default.

i. (Optional) In the Upgrade Summary page, expand **Configure Action Plan** to choose, view, modify or add an action plan.

The action plan designates how many times and at what interval Cisco Fog Director retries an action if the action fails on a device due to certain device reachability or network connectivity issues. If Cisco Fog Director cannot complete the app upgrade action on a device after the number of retries that the action plan designates, the app upgrade does not complete on the device.

When you expand **Configure Action Plan**, the **Selected Action Plan** field shows the name of the action plan that is in effect. The **Details** field describes the number of retries and time between retries that the selected action plan defines.

You can choose the action plan that you want from the Selected Action Plan drop-down list.

For information about modifying or adding action plans, see the "Using Action Plans" section on page 4-49.

j. (Optional) In the Upgrade Summary page, expand **Network Status** to view network, resource, and related information for apps and devices.

The Network Status area displays the following information:

– How many of the devices that you selected for installation of the app are reachable. ("Reachable" means that Cisco Fog Director can communicate with the device.) Hover your mouse pointer over a graph to see more detailed information.

– The *device squares* in the box in the middle of the area. Each box represents a device on which you are installing the app. You can hover your mouse pointer over a device square to display the following information:

  - **Cartridges**—Cisco cartridges that a PAAS app requires to run. These cartridges must already be uploaded to Cisco Fog Director (see Chapter 7, "Managing Cartridges") and are installed automatically on the device as part of the app installation process.

  - **CPU Availability**—Number of free CPU units on the device.

  - **Memory Availability**—Amount of free RAM, in MB, on the device.

– How often the Cisco Fog Director updates the information in this area. You can choose a value from the **Collect resource usage at least every** drop-down list. Options are **Every 15 mins**, **Every 1 hour**, **Every 4 hour**, **Every 8 hour**, **Every 16 hour**, and **Never ever**.

k. Click the **DONE, LET'S GO** button.

The App Configuration page displays, as described in the "Viewing Detailed Information about an Installed or Available App" section on page 4-6.

While the app is upgrading on a device, the status of the upgrade displays for that device. Click the device to see the progress of the upgrade. You can click the **ABORT** button under the status display to abort the upgrade action, as described in the "Aborting an Action" section on page 4-42.

If the Actions Failed display on this page indicates that the upgrade failed on any device, you can take any of these actions:

- Click the **RETRY NOW** button to try the upgrade on these devices again. See the "Retrying a Failed Action for an App" section on page 4-45.
- Click the **View Outstanding Actions** link to display the Actions page, which provides options for managing failed actions for which an action plan is in effect. See the "Managing Outstanding and Expired Actions for Apps" section on page 4-53 for more information.
- Wait for Cisco Fog Director to retry the failed action according to an action plan that is in effect. See the "Using Action Plans" section on page 4-49

Reverting to the Previous Version of an App

After you upgrade an app, you can revert to the most recent previously installed version of that app, if needed.

The following sections provide additional information:

Reverting to the Previous Version of a Published App

If you have upgraded an app and then published the upgraded version, you can revert to the previous version of the app.

To revert to the previous version of a published app, follow these steps:

Procedure

Step 1 Uninstall the app from each device on which it is installed, as described in the "Uninstalling an App" section on page 4-22.

Step 2 Unpublish the app, as described in the "Unpublishing an App" section on page 4-13.

The previous version of the app displays in the Published area on the Apps View page.

Reverting to the Previous Version of an Unpublished App

If you have upgraded an app but not published the upgraded version, you can revert to the previous version of the app.

To revert to the previous version of an unpublished app, remove the app as described in the "Removing an App" section on page 4-31. The previous version of the app displays in the Unpublished area on the Apps View page.

Removing an App

Removing an app removes it from Cisco Fog Director.

To remove an app, follow these steps:

Procedure

Step 1 Uninstall the app as described in the "Uninstalling an App" section on page 4-22.

The app moves to the Available Apps area on the Apps View page.

Step 2 In the Available Apps area, click the **Unpublish** button under the icon for the app.

The app moves to the Unpublished Apps area on the Apps View page.

Step 3 In the Unpublished Apps area, click the **Remove** button under the icon for the app.

Editing an App Icon, Description, and Release Notes

You can add or update the following items for an app:

- Icon—The icon that displays in Cisco Fog Director for the app.

  This icon comes from an image file that you specify. The image size should be 250 x 250 pixels. The system accepts images that are other sizes, but those images are scaled and may not appear as desired. The image file can in any of these formats: ai, bmp, drw, gif, ico, jpe, jpeg, jpg, pct, png, psd, psp, raw, scf, svg, svgz, tif, or tiff.
- Description—Brief description of the app that displays when you view detailed information for the app.

- Release Notes (optional)—Notes for the app that appear when you view detailed information for the app. For example, notes might include a list and descriptions of features added in an updated app.

To add or update an icon, description, or release notes for an app, follow these steps:

Procedure

Step 1 If you are not viewing the page that displays when you add an app, in the Available Apps area on the Apps View page, click the icon for the app for which you want to add or update the icon, description, or release notes.

Step 2 To add or update an icon, take these actions:

a. Click **Edit Icon**.

b. Follow the on-screen prompts to locate and select the image file for the icon that you want.

Step 3 To add or update a description, take these actions:

a. Click **Edit** next to "Description."

b. In the edit area that displays, type the description. You can use the formatting tools at the top of the Edit area to format the text and perform related operations.

c. Click **Apply**.

d. Click the **SAVE** button.

Step 4 To add or update release notes, take these actions:

a. Click **Edit next to** "Release Notes."

b. In the edit area that displays, type the notes. You can use the formatting tools at the top of the Edit area to format the text and perform related operations.

c. Click **Apply**.

d. Click the **SAVE** button.

Reconfiguring App Parameters

You can reconfigure a variety of items that apply to an app. Depending on the app, items that you can reconfigure include:

- Configuration information—Configuration items that are defined in the package_config.ini file for the app
- Resource profile—Amount of host system CPU and memory (RAM) resources that the app requires on a device.
- Networking—Network from which the app obtains its IP address or addresses.
- Resource port—Serial port that the app uses on a device.
- Action plan—The number of times and at what intervals Cisco Fog director retries an install, reconfigure, upgrade, or uninstall action that fails due to certain device reachability or network connectivity issues.

The following sections provide additional information:

- Reconfigure App Options, page 4-33

- Reconfigure App Procedure, page 4-34

Reconfigure App Options

To view options for reconfiguring an app, take either of these actions:

- Click the **EDIT CONFIGURATION** button on the App Configuration page for the app
- From the Devices tab, choose a device, and then click **EDIT CONFIGURATION** near the bottom of the page that displays for the device

If you clicked **Edit Configuration** from the App Configuration page, the Reconfigure App page displays, which displays that includes the items that Table 4-9 describes.

Table 4-9 Reconfigure App Page Items

Item	Description
Installed Devices table	Provides information about each device on which the app is installed, 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. • 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 reconfigure 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 installed. • IP Address—IP address of the device on which the app is installed. • Tags—Tags that are assigned to the device on which the app is installed. • 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 4-9 Reconfigure App Page Items (continued)

Item	Description
Selected Devices table	Provides information about each device on which you want to reconfigure the app. Devices appear in this table after you check their check boxes in the Installed Devices table and then click **ADD SELECTED DEVICES**. This table includes the following items: • Selected Devices—Number of devices on which you want to reconfigure the app. • 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 reconfigure the app. • IP Address—IP address of the device on which you want to reconfigure the app. • Tags—Tags that are assigned to the device on which you want to reconfigure 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 and does not remove the app from 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.

Reconfigure App Procedure

You can reconfigure an app from the Apps View page or the Devices View page, as described in the following sections:

- Reconfiguring an App from the Apps View Page, page 4-35
- Reconfiguring an App from the Devices View Page, page 4-39

If you are reconfiguring an app that provides services, you must first uninstall other apps that uses the services that this app provides.

Reconfiguring an App from the Apps View Page

Reconfiguring an app from the Apps View page is useful if you want to apply the reconfiguration to multiple devices.

Cisco Fog Director associates an action plan with each app reconfiguration procedure that you perform. An action plan instructs Cisco Fog Director to retry a reconfiguration if the reconfiguration fails due to certain conditions, or to perform the reconfiguration within a designated maintenance window. By default, the action plan causes Cisco Fog Director to perform the reconfiguration immediately and to retry a failed reconfiguration up to 10 times at 2 minute intervals. You can change these parameters as needed when you perform the app reconfiguration procedure. For more information, see the "Using Action Plans" section on page 4-49.

To reconfigure an app from the Apps View page, perform the following steps. The items that you can reconfigure depend on the app, so some configuration options that the following procedure includes may not be available for some apps.

Note To add app data files, see the "Adding App Data Files" section on page 4-40.

Before You Begin

Make sure that the app is installed as described in the "Installing an App" section on page 4-13.

Procedure

Step 1 Take one of these actions:

- In the Installed Apps area on the Apps View page, click the icon for the app that you want to reconfigure, and then click the **EDIT CONFIGURATION** button on the App Configuration page.
- In the Available Apps area on the Apps View page, click the icon for the app that you want to reconfigure, and then click the **EDIT CONFIGURATION** button on the App Configuration page.

Step 2 In the Installed Devices table, check the check box for each device on which you want to reconfigure the app.

For detailed information about this table and locating devices, see the "Reconfigure App Options" section on page 4-33.

Step 3 Click the **ADD SELECTED DEVICES** button.

The devices with checked check boxes are added to the Selected Devices table. The app can be reconfigured on devices that this table list. For detailed information about this table and about removing devices from this table, see the "Reconfigure App Options" section on page 4-33.

Step 4 To change configuration information for this app, take these actions:

a. Click the Expand icon next to **Customize Configuration**.

The configuration items that display are defined in the package_config.ini file for the app.

b. Make updates as needed in the fields that appear.

The value that each field displays is the default value for that item as defined by the app. To see the current value of an item on a particular device, from the Devices tab, choose a device, and then click **EDIT CONFIGURATION** near the bottom of the page that displays for the device.

c. (Optional) **Check the Restart app** after configuration check box if you want the app to restart after you save the configuration updates. Some apps require a restart after a configuration change.

d. Click the **DONE, LET'S GO** button to complete the changes to configuration information.

Step 5 To reconfigure resource profiles that have been assigned for the app, take these actions:

a. Click the Expand icon next to **Customize Resources**, if this area is not expanded already.

b. Click the Expand icon next to **Configure Resource Profiles**.

You can update the resource profile for a specific device, some devices, or all devices.

The *device squares* in the box in the middle of the Configure Resource Profile area represent devices on which the app is installed. You can hover your mouse pointer over a device square to display the Edit Resource Profile dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and the resource profile that has been assigned for the app on the device. You can click the hostname and IP address in the dialog box to exit the reconfigure procedure and display the Device Details page for the device.

c. If you want to limit the device squares displays to one or more specific devices, take either of these actions:

– 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.

d. Take the desired action:

– To change the resource profile for a specific device, hover your mouse pointer over the device square for that device, and in the Edit Resource Profile dialog box. choose a resource profile from the **Select Profile** drop-down list.

– To change the resource profile for all devices for which a device square displayed, click the desired profile radio button and then click the **Reassign Profile** button:

- **Exact matching profile**—Assigns the resource profile that is defined for the app in its metadata, if the resources are available on a device.

- **Largest available profile**—Assigns the largest resource profile that is currently available on a device.

- **Allocate all available resources**—Assigns all CPU and memory resources that are available on each device on which you are installing.

- **Custom profile**—On each device on which you are installing, assigns the CPU and memory resources that you specify. After you click this radio button, the **CPU** and the **Memory** fields appear. Enter the CPU resources, in units, and memory resources, in MB, to assign on each device. The Max value under each field shows the maximum value that you can enter without exceeding the available corresponding resource on at least one device. If you enter a value that exceeds this maximum value, the **REASSIGN PROFILE** button is dimmed and cannot be used.

e. If you are finished reconfiguring the app, click the **EDIT RESOURCES** button. Otherwise, continue to the following step.

Step 6 To reconfigure network information that relates to how the app obtains its IP address or addresses on each device, take these actions:

a. Click the Expand icon next to **Customize Resources**, if this area is not expanded already.

b. Click the Expand icon next to **Configure Networking**.

You can update the network for a specific device, some devices, or all devices.

The *device squares* in the box at the left of the Configure Networking area represent devices on which the app is installed. You can hover your mouse pointer over a device square to display the Edit Network Details dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and network interface information for each network interface that is defined in the package_config.ini file for the app.

The Preferred Networks sub areas at the right of the Configure Networking area provide information for each network interface that is defined in the package_config.ini file for the app. You can expand a sub area to display and update options in it.

If you want to limit the device squares to one or more specific devices, take either of these actions:

- 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 update network information for an app on one or more devices, take either of these actions:

- To change network information for a specific device, take these actions:
  a. Hover your mouse pointer over the device square for that device, and in the Edit Network Details dialog box, choose a network for the corresponding network interface from the **Select Network** drop-down list. Network options are:

     - **iox-bridge#**—App obtains its IP address from a DCHP pool that is configured in Cisco IOS

     - **iox-nat#**—App obtains its IP address from an internal network address translator

  b. If you choose **iox-bridge#** and if you want to assign a static IP address from the DHCP pool for this network interface, check the **Static Mode** check box that displays. If you check this check box, the network interface uses IP addresses that are dynamically assigned from the DCHP pool.

  c. If you check the **Static Mode** check box, configure the following fields that appear as needed:

     - **IPv# Address** and **Mask** fields—Enter the static address and subnet mask to use. If the IPv6required field is set to “true” in the app descriptor file (package.yaml) for an app, you must enter an IPv6 address. Otherwise, you can enter an IPv4 or an IPv6 address. If you enter an IPv6 address but a device on which you are installing the app does not support IPv6, the edit configuration operation will fail on that device.

     - **DNS** field—(Optional) Enter the IP address of the DNS server that the app uses for external communication.

     - **Default Gateway** field—(Optional) Enter the IP address of the default gateway that the app uses for external communication.

- To update network information for all devices for which a device square is displayed, take these actions for each network interface that you want to configure:
  a. Expand the Preferred networks sub area.

  b. Choose a network from the **Select Network** drop-down list. Network options are:

     - **iox-bridge#**—App obtains its IP address from a DCHP pool that is configured in Cisco IOS

     - **iox-nat#**—App obtains its IP address from an internal network address translator

  c. If you choose **iox-bridge#**, click one of the following radio buttons that appear:

     - **Static**— Click to assign a static IP address from the DHCP pool for this network interface

     - **Dynamic**—Click to use a dynamically assigned IP address from the DCHP pool for this network interface

d. If you click the **Static** radio button, configure the following fields that appear as needed:

- **IPv# Address** and **Mask** fields—Enter the static address and subnet mask to use. If the IPv6required field is set to "true" in the app descriptor file (package.yaml) for an app, you must enter an IPv6 address. Otherwise, you can enter an IPv4 or an IPv6 address. If you enter an IPv6 address but a device on which you are installing the app does not support IPv6, the edit configuration operation will fail on that device.

- **Default Gateway** field—(Optional) Enter the IP address of the default gateway that the app uses for external communication.

- **DNS** field—(Optional) Enter the IP address of the DNS server that the app uses for external communication.

e. After you configure each network interface that you want, click the **REASSIGN NETWORKS** button.

Step 7 To reconfigure a VNC password that is required to access an app on devices via a VNC session, take these actions:

a. Click the Expand icon next to **Customize Resources**, if this area is not expanded already.

b. Click the Expand icon next to **Configure VNC Password**.

The *device squares* in the box in the middle of the Configure VNC Password area represent devices on which you are installing the app. You can hover your mouse pointer over a device square to display the Edit VNC password dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and provides a field for entering the VNC password for the device.

c. If you want to limit the device squares to one or more specific devices, take either of these actions:

– 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.

d. Take either of these actions:

– To set the VNC password for a specific device, hover your mouse pointer over the device square for that device, and in the Edit VNC Password dialog box, enter the password in the **VNC Password** field

– To set the VNC password for all devices for which a device square is displayed, enter the password in the **VNC Password** field that displays to the right of the device squares, and then click the thee **Assign** button.

Step 8 To reconfigure the number of virtual CPUs that the app requires on a device:

a. Click the Expand icon next to **Customize Resources**, if this area is not expanded already.

b. Click the Expand icon next to **Configure VCPUs**.

The *device squares* in the box in the middle of the Configure VCPUs area represent devices on which you are installing the app. You can hover your mouse pointer over a device square to display the Edit VCPU Details dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and the number of virtual CPUs that have been assigned for the app on the device.

a. If you want to limit the device squares to one or more specific devices, take either of these actions:

– 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.

b. Take either of these actions:

- To configure the number of virtual CPUs for a specific device, hover your mouse pointer over the device square for that device, and in the Edit VCPU dialog box, type or use the up or down arrow buttons to enter the desired value.
- To configure the number of virtual CPUs for all devices for which a device square is displayed, in the **Select VCPU Value** field that displays to the right of the device square, type or use the up or down arrow buttons to enter the desired value, and then click the **REASSIGN VCPU** button. The text above the **Select VCPU Value** field indicates the number of virtual CPUs that the descriptor file for the app specifies and the maximum number of virtual CPUs that you can designate for the app on the devices that you selected.

Step 9 To reconfigure the serial port that the app uses on a device, take these actions:

a. Click the Expand icon next to **Customize Resources**, if this area is not expanded already.

b. Click the Expand icon next to **Configure Device Resource Ports**.

The *device squares* in the box in the middle of the Configure Device Resource Ports area represent devices on which the app is installed. You can hover your mouse pointer over a device square to display the Edit Serial Details dialog box. This dialog box shows the hostname and IP address of the device, tags assigned to the device, and the serial port that has been assigned for the app on the device.

a. If you want to limit the device squares to one or more specific devices, take either of these actions:

- 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.

b. Hover your mouse pointer over the device square for the device that you want to update, and in the Edit Serial Details dialog box, choose a port from the **Select Serial Port** drop-down list.

c. When you are finished reconfiguring resources, click the **EDIT RESOURCES** button.

Step 10 (Optional) To choose, view, modify or add an action plan, click the Expand icon next to **Configure Action Plan**.

The action plan designates how many times and at what interval Cisco Fog Director retries an action if the action fails on a device due to certain device reachability or network connectivity issues. If Cisco Fog Director cannot complete the app reconfiguration action after the number of retries that the action plan designates, the app reconfiguration does not complete.

When you expand **Configure Action Plan**, the **Selected Action Plan** field shows the name of the action plan that is in effect. The **Details** field describes the number of retries and time between retries that the selected action plan defines.

You can choose the action plan that you want from the Selected Action Plan drop-down list.

For information about modifying or adding action plans, see the "Using Action Plans" section on page 4-49.

Reconfiguring an App from the Devices View Page

Reconfiguring an app from the Devices View page applies the reconfiguration to a specified device.

To reconfigure an app from the Devices View page, follow these steps:

Before You Begin

Make sure that the app is installed as described in the "Installing an App" section on page 4-13.

Procedure

Step 1 On the Devices page, choose the device on which you want to reconfigure the app.

Step 2 Click **Edit Configuration** under the app that you want to reconfigure.

The configuration items that display are defined in the package_config.ini file for the app.

Step 3 Make updates as needed in the fields that appear.

The value that each field displays is the value for that item on the device that you chose.

Step 4 (Optional) **Check the Restart app** after configuration check box if you want the app to restart after you save the configuration updates. Some apps require a restart after a configuration change.

Step 5 Click the **RECONFIGURE APP** button.

Adding App Data Files

An app data file is a file that an app requires, such as a configuration file. You can add app data files to devices as needed.

To add app data files, follow these steps

Before You Begin

Make sure that the app is installed as described in the "Installing an App" section on page 4-13.

Procedure

Step 1 Take one of these actions:

- In the Installed Apps area on the Apps View page, click the icon for the app that you want, and then click the **EDIT CONFIGURATION** button on the App Configuration page.
- In the Available Apps area on the Apps View page, click the icon for the app that you want, and then click the **EDIT CONFIGURATION** button on the App Configuration page.

Step 2 In the Installed Devices table, check the check box for each device on which you want to install the app data files.

For detailed information about this table and locating devices, see the "Reconfigure App Options" section on page 4-33.

Step 3 Click the **ADD SELECTED DEVICES** button.

The devices with checked check boxes are added to the Selected Devices table. The app data files can be installed on devices that this table list. For detailed information about this table and about removing devices from this table, see the "Reconfigure App Options" section on page 4-33.

Step 4 To upload one or more app data files for the app, take the following actions.

a. Click the Expand icon next to **Manage App Data**.

b. (Optional) Check the **Delete all files in /appdata** 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.

c. (Optional) In the **File path on app container** field, 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.

d. (Optional) In the **New file name** field, 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.

e. Click the **SELECT FILES** button and then follow the on-screen prompts to locate and select the app data file that you want to upload.

f. Repeat Step 10b through Step 10e to select additional app files 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.

g. Click the **UPLOAD** button to upload the app data file.

Repeat these steps as needed to upload additional app data files.

Configuring App Links

You can use app links to associate links to external resources with an app. For example, you could include a link to a web site or document that provides information about an app, or you could include a link to a reference guide or configuration guide for an app. You can associate as many links as needed with an app.

After you configure a link for an app, the link displays under App Links on the App Configuration page, and in the Apps area on the Device Details page. Click a link to go to the configured resource.

The following sections describe how add, update, or delete app links.

- Adding an App Link, page 4-41
- Updating or Deleting an App Link, page 4-42

Adding an App Link

To configure an app link, follow these steps:

Procedure

Step 1 If you are not viewing the page that displays when you add an app, in the Available Apps area on the Apps View page, click the icon for the app for which you want to add links.

Step 2 Click the **App Links** button ✚.

Three fields appear.

Step 3 In the first field, enter a name for the link.

For example, enter the name of the web page or a document that the link references.

Step 4 In the second field, enter the URL of the link.

Step 5 In the third field, enter a brief description of the linked resource.

Step 6 Take either of these actions:

- To save your changes, click the Check icon .
- To close the fields without saving your changes, click the X icon .

Updating or Deleting an App Link

To update or delete an app link, follow these steps:

Procedure

Step 1 If you are not viewing the page that displays when you add an app, in the Available Apps area on the Apps View page, click the icon for the app for which you want to add links.

Step 2 Take either of these actions

- To delete the link, click the Delete icon .
- To update the link, click the Delete icon and continue to Step 3.

Step 3 In the fields that display, update the name a name of the link, the URL of the link, or the description of the link as needed.

Step 4 Take either of these actions:

- To save your changes, click the Check icon .
- To close the fields without saving your changes, click the X icon .

Aborting an Action

Cisco Fog Director provides the ability to abort a variety of actions after you start them. This feature is useful if you start an action that is to take place on several devices and you want to stop the action before it completes on all devices.

To use this feature, you select the devices on which to abort the action. Cisco Fog Director then does not perform the action on any selected device on which the action has not yet started. The action might continue on devices on which it has started already, but Cisco Fog Director stops monitoring and displaying status information about the action on those devices.

You can abort the following actions:

- Installing an app

- Uninstalling an app
- Upgrading an app
- Reconfiguring app parameters from the Apps View page
- Retrying failed actions for an app

The following sections provide additional information:

- Table 4-9Abort Ongoing Actions Options, page 4-43
- Aborting an Action on Selected Devices, page 4-44

Abort Ongoing Actions Options

Options for aborting actions appear in the Abort Ongoing Actions page. This page displays when you click the ABORT button on a page that displays after you start an action.

The Abort Ongoing Actions page displays. This page includes the items that Table 4-10 describes.

Table 4-10 Abort Ongoing Actions Page Items

Item	Description
Devices table	Provides information about each device on which you specified that the action be performed: • 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. • 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 abort the action. 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 you specified that the action be performed. • IP Address—IP address of the device on which you specified that the action be performed. • 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 4-10 Abort Ongoing Actions Page Items (continued)

Item	Description
Selected Devices table	Provides information about each device for which you want to abort the action. Devices appear in this table after you check their check boxes in the Devices table and then click **ADD SELECTED DEVICES**. This table includes the following items: • Selected Devices—Number of devices on which you want to abort the action. • 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 abort the action. • IP Address—IP address of the device on which you want to abort the action. • Tags—Tags that are assigned to the device on which you want to abort the action. • 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.
SUBMIT button	Appears when one or more devices appear in the Selected Devices table. Click to abort the action on the devices in the Selected Devices table.

Aborting an Action on Selected Devices

To abort an action, follow these steps:

Procedure

Step 1 In the page that displays after you start the action, click the **ABORT** button.

The Abort Ongoing Actions page displays.

Step 2 In the Installed Devices table, check the check box for each device for which you want to abort the action.

For detailed information about this table and locating devices, see the "Abort Ongoing Actions Options" section on page 4-43.

Step 3 Click the **ADD SELECTED DEVICES** button.

The devices that you selected are added to the Selected Devices table. The action will be aborted on the devices that this table lists. For detailed information about this table and about removing devices from this table, see the "Abort Ongoing Actions Options" section on page 4-43.

Step 4 Click the **SUBMIT** button.

The action aborts on the devices that you selected. If the action has started on a device, the action might continue on that device, but Cisco Fog Director stops monitoring and displaying status information about the action on that device.

Retrying a Failed Action for an App

If any of the following actions fails on one or more devices, you can use the **RETRY NOW** button on the App Configuration page to retry the action:

- Installing an app
- Reconfiguring app parameters
- Upgrading an app
- Uninstalling an app
- Editing app resources

Note If a failed action has an associated action plan that instructs Cisco Fog Director to retry an app, you also can manually retry the action by using the **RETRY NOW** button on the Actions page as described in the "Outstanding and Expired Actions Management Procedure" procedure on page 4-56.

For detailed information about action plans, see the "Using Action Plans" procedure on page 4-49.

The following sections provide additional information:

- Retry Failed Action Options, page 4-45
- Retry Failed Action Procedure, page 4-48

Retry Failed Action Options

To view options for retrying a failed action, click the **RETRY NOW** button on the App Configuration page for the app.

The Select Retry Actions page displays. This page includes the items that Table 4-11 describes.

Table 4-11 Select Retry Actions Page Items

Item	Description
Redeploy app on devices where it failed installation area	
Redeploy button	Click to retry the failed installation operation on the devices that you select in the Devices table in this area.
REMOVE FOREVER button	Click to delete information about the action that failed on the devices that you select in the Devices table in this area and to clear the error from the system.
VIEW DEPLOY ACTION HISTORY button	Click to display the Actions History window for the devices that you select in the Devices table in this area. For a description of this window, see Table 4-12 on page 4-47.
Devices table	Provides information about each device on which an installation action failed, 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. • 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 perform an action. 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 action is to be performed. • IP Address—IP address of the device on which action is to be performed. • 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.
Edit configuration on devices where configuration failed area	
EDIT CONFIGURATION button	Click to retry the failed configuration operation on the devices that you select in the Devices table in this area.
VIEW EDIT CONFIGURATION ACTION HISTORY button	Click to display the Actions History window for the devices that you select in the Devices table in this area. For a description of this window, see Table 4-12 on page 4-47.
Devices table	Provides information about each device on which an edit configuration action failed. This table contains the information that the Devices table row in this table describes.

Table 4-11 Select Retry Actions Page Items (continued)

Item	Description
Restart app after configuration check box	Check this check box if you want the app to restart after the configuration operation completes. Some apps require a restart after a configuration change.
Customize configuration fields	Displays configuration items that are defined in the package_config.ini file for the app. You can make updates in these fields as needed.
Upgrade app on devices where upgrade failed area	
Upgrade button	Click to retry the failed upgrade operation on the devices that you select in the Devices table in this area.
VIEW UPGRADE ACTION HISTORY button	Click to display the Actions History window for the devices that you select in the Devices table in this area. For a description of this window, see Table 4-12 on page 4-47.
Devices table	Provides information about each device on which an upgrade action failed. This table contains the information that the Devices table row in this table describes.
Uninstall app from devices where uninstall failed area	
Uninstall button	Click to retry the failed uninstall operation on the devices that you select in the Devices table in this area.
VIEW UINSTALL ACTION HISTORY button	Click to display the Actions History window for the devices that you select in the Devices table in this area. For a description of this window, see Table 4-12 on page 4-47.
Devices table	Provides information about each device on which an uninstall action failed. This table contains the information that the Devices table row in this table describes.
Allocate resource for app on devices where resource allocation failed area	
EDIT RESOURCES button	Click to retry the failed resource allocation operation on the devices that you select in the Devices table in this area.
VIEW EDIT RESOURCES ACTION HISTORY button	Click to display the Actions History window for the devices that you select in the Devices table in this area. For a description of this window, see Table 4-12 on page 4-47.
Devices table	Provides information about each device on which a resource allocation action failed. This table contains the information that the Devices table row in this table describes.

The Action History window displays when you click a **VIEW *TYPE* ACTION HISTORY** button for a failed action in the Select Retry Actions page. This window includes the items that Table 4-12 describes.

Table 4-12 Action History Window Items

Item	Description
Outstanding tab	Click to display devices on which the action is in Outstanding state.
Expired tab	Click to display devices on which the action is in Expired state.

Table 4-12 Action History Window Items (continued)

Item	Description
Host Name field	Hostname of a device on which the action is in Outstanding state or Expired state. You can click a hostname to display the Device Details page for the corresponding device.
IP Address field	IP address of a device on which the action is in Outstanding state or Expired state. You can click an IP address to display the Device Details page for the corresponding device.
Last Attempted field	Date and time that Cisco Fog Director last attempted to perform the action on a device.
Message	Brief description of why the action last failed on the device.
Next attempt	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.
Action Type	Type of the outstanding action (**Install**, **Uninstall**, **Upgrade**, **Edit Configuration**, or **Edit Resources**).
Pending attempts	For a device with actions in Outstanding state, displays the 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. For a device that you moved to Expired state by manually canceling future retries, displays the maximum number of retries that were pending when you canceled the retries.

Retry Failed Action Procedure

To retry a failed action, follow these steps:

Procedure

Step 1 From the App Configuration page for the app, click the **RETRY NOW** button.

This button is available only if an action failed.

The Select Retry Actions page displays, as described in Table 4-11 on page 4-46. This page includes areas that relate to the following failed actions types:

- App install action
- App reconfigure action
- App upgrade action
- App uninstall action
- App resource allocation action

Step 2 (Optional) To view a history of failed actions on one or more devices, take these actions:

a. In the Devices table in the area for the type of failed action for which you want to view history, check the check box for each device for which you want to see information.

b. **VIEW *TYPE* ACTION HISTORY** button in the same area.

Step 3 Take the desired actions:

- To retry an install action, take these actions in the **Redeploy app on devices where it failed installation** area:
  - **a.** In the devices table, check the check box for each device on which you want to retry the action.
  - **b.** Click the **REDEPLOY** button to retry the installation operation on the devices that you selected, or click the **REMOVE FOREVER** button delete information about the action that failed on the devices that you select and to clear the error from the system.
- To retry an edit configuration action, take these actions in the **Edit Configuration on devices where configuration failed** area:
  - **a.** In the devices table, check the check box for each device on which you want to retry the action.
  - **b.** If needed, edit information that displays tine the Customize Configuration fields. These fields display configuration items that are defined in the package_config.ini file for the app.
  - **c.** Check the **Restart app after configuration** check if you want the app to restart after the edit configuration operation completes. Some apps require a restart after a configuration change.
  - **d.** Click the **EDIT CONFIGUATION** button to retry the edit configuration operation on the devices that you selected.
- To retry an upgrade action, take these actions in the **Upgrade app on devices where upgrade failed** area:
  - **a.** In the devices table, check the check box for each device on which you want to retry the action.
  - **b.** Click the **UPGRADE** button to retry the upgrade operation on the devices that you selected
- To retry an uninstall action, take these actions in the **Uninstall app on devices where uninstall failed** area:
  - **a.** In the devices table, check the check box for each device on which you want to retry the action.
  - **b.** Click the **UINSTALL** button to retry the uninstall operation on the devices that you selected.
- To retry a resource allocation action, take these actions in the **Allocate resource for app on devices where resource allocation failed** area:
  - **a.** In the devices table, check the check box for each device on which you want to retry the action.
  - **b.** Click the **EDIT RESOURCES** button to retry the resource allocation operation on the devices that you selected.

The App Configuration page displays, as described in the "Viewing Detailed Information about an Installed or Available App" section on page 4-6.

While the system is retrying an action on a device, the status of the retry operation displays for that device. Click the device to see the progress of the operation. You can click the **ABORT** button under the status display to abort the abort the operation, as described in the "Aborting an Action" section on page 4-42.

Using Action Plans

An *action plan* is a Cisco Fog Director policy that instructs Cisco Fog Director to retry an app installation, configuration, upgrade, or uninstallation action if the action fails due to certain conditions, or to perform the action within a designated maintenance window.

Cisco Fog Director automatically associates an action plan with each app installation, configuration, upgrade, or uninstallation that you perform. By default, the action plan causes Cisco Fog Director to perform the action immediately and to retry a failed action up to 10 times at 2 minute intervals. You can change these parameters as needed when you perform an app installation, configuration, upgrade, or uninstallation procedure.

If you perform an action that has an action plan that instructs Cisco Fog Director to retry the action and the action does not complete successfully when you execute it, or if the action plan instructs Cisco Fog to perform the action in a designated maintenance window, the action will be in one of these states:

- Outstanding—The action will be retried or executed in a maintenance window according to the action plan that is associated with the action
- Expired—The action did not complete successfully but will no longer be retried because the maximum number of retries that the associated action plan specifies, the maintenance window or windows that were scheduled for the action no longer exist, you manually canceled future retries of the action, or the failure is not related to certain device reachability or network connectivity issues

For more information about these states and how to manage actions that are in these states, including information about manually retrying or canceling future retries of an action, see the "Managing Outstanding and Expired Actions for Apps" procedure on page 4-53.

- The following sections provide more detailed information about action plans:
- Action Plan Guidelines, page 4-50
- Managing Action Plans, page 4-51

Action Plan Guidelines

The following guidelines apply to action plans:

- Cisco Fog Director associates an action plan with every app installation, configuration, upgrade, and uninstallation procedure that you perform.
- Cisco Fog Director includes the action plan named FogDirectorDefaultPolicy. By default, this action plan designates that an action that fails be retried up to 10 times at 2 minute intervals. The system uses this action plan unless you specify that it use another one.
- You can modify or create an action plan when you perform an app installation, configuration, upgrade, or uninstallation procedure. If you do so, Cisco Fog Director saves the modifications or creation when you complete the procedure. If you exit the procedure without completing it, your action plan changes are not saved.
- For each action plan, you can designate that it take effect immediately or within a maintenance window, the number of times and at what interval it causes an action to be retried, and whether it is the default action plan.
- After action plan modifications or creations are saved, the updates that you made are available and used for all future app installation, configuration, upgrade, or uninstallation actions.
- If you delete an action plan, it is removed from Cisco Fog Director immediately. You do not need to complete the app installation, configuration, upgrade, or uninstallation procedure to save the deletion.
- The action plan that is currently designated as the default cannot be deleted from Cisco Fog Director.
- When you make an action plan the default, any actions that are pending under an action plan that was the previous default are not affected.

- If you do not want Cisco Fog Director to automatically retry a failed action, you can set the existing default action plan to 0 retries, or create a new default action plan that designates 0 retries.
- If Cisco Fog Director cannot complete an action after the number of retries that the action plan designates, the action does not complete.

Managing Action Plans

This section describes how to manage action plans. Action plan management tasks include:

- Modifying the number of times and at what interval an action plan causes Cisco Fog Director to retry a failed action
- Configuring (scheduling) an action plan to execute or retry actions only during one or more designated time periods, called *maintenance windows*
- Setting an action plan as the default action plan
- Creating a new action plan, called a *custom action plan*
- Deleting an action plan that is not the current default action plan or in use

To manage an action plan, follow these steps:

Procedure

Step 1 When performing an app installation, configuration, upgrade, or uninstallation procedure, expand **Configure Action Plan** when this option becomes available during the procedure.

Step 2 Take one of these actions:

- To create a new custom action plan, from the **Selected Action Plan** drop-down list, choose **[Define a new plan...]**. Continue to Step 3.
- To modify an custom action plan, from the **Selected Action Plan** drop-down list, choose the name of the plan, and the click the Edit Action Plan icon next to the action plan name. Skip to Step 4.

  You cannot modify an action plan when an action is in Outstanding state according to the plan. In this situation, the Edit Action Plan icon is dimmed.
- To delete an action plan, from the **Selected Action Plan** drop-down list, choose the name of the plan, and click the Delete icon next to the name.

  The action plan is removed from Cisco Fog Director immediately and no further steps are needed, although you can complete the app installation, configuration, upgrade, or uninstallation procedure.

  You cannot delete an action plan that is the current default or when an action is in Outstanding state according to the plan. In these situations, the delete icon is dimmed.

Step 3 In the **Plan Name** field, enter a descriptive name for the new action plan.

Step 4 (Optional) Check the **Make this plan the default** check box to make this action plan the default action plan.

Cisco Fog Director uses the default action plan if you do not choose another one when performing an action.

This check box does not appear if this action plan is the current default.

Step 5 Choose one of the following ***Action* Type** radio buttons (*Action* identifies the type of procedure that you are performing when you access this option):

- **Now**—Causes the action plan to take effect as soon as you complete the app installation, configuration, upgrade, or uninstallation procedure. In this situation, if an action that is associated with this action plan fails, Cisco Fog Director immediately begins to retry the action according to this action plan. Skip to Step 7.
- **In a maintenance window**—Causes the action plan to be in effect according to the schedule (called a *maintenance window*) that you specify. In this situation, an action that is associated with this action plan does not execute until the beginning of the maintenance window, and if the action fails, Cisco Fog Director retries the action according to this action plan only within the maintenance window. Continue to Step 6.

Step 6 From the **Maintenance window type** drop-down list, choose one of the following options to define the schedule for this action plan:

- **Once**—Causes the action plan to be in effect for the designated time period on the designated date. If you choose this option, enter information in the **Maintenance window date and time** fields that appear as follows:
  - **Date** field—Click the calendar icon and then choose the date on which the action plan should be in effect.
  - **From** field—Click the clock icon and then choose the time on the selected date at which the action plan should begin to take effect.
  - **To** field—Click the clock icon and then the time on the selected date after which the action plan should no longer be in effect.
  - **Time zone** field—Specifies the time zone for the times in the **From** and **To** fields. By default, this field displays the time zone of your PC. We recommend that you use the time zone of the server on which Cisco Fog Director is running. To change the time zone that displays in this field, click this field, click its delete icon , and then start typing the time zone that you want. You can choose a time zone from the list that displays.
- **Every day**—Causes the action plan to be in effect for the designated time period every day or until the action goes to Expired state. If you choose this option, enter information in the **Maintenance window** fields that appear as follows:
  - **From** field—Click the clock icon and then choose the time on the selected date at which the action plan should begin to take effect.
  - **To** field—Click the clock icon and then the time on the selected date after which the action plan should no longer be in effect.
  - **Time zone** field—Specifies the time zone for the times in the **From** and **To** fields. By default, this field displays the time zone of your PC. We recommend that you use the time zone of the server on which Cisco Fog Director is running. To change the time zone that displays in this field, click this field, click its delete icon , and then start typing the time zone that you want. You can choose a time zone from the list that displays.
- **On selected days of the week**—Causes the action plan to be in effect for the designated time period on each day that you choose or until the action goes to Expired state. If you choose this option, enter information in **Maintenance days** and **Maintenance window** fields that appear:
  - **Maintenance days** field—Check the check box for each day on which the action plan should be in effect.
  - **From** field—Click the clock icon and then choose the time on each day at which the action plan should begin to take effect.
  - **To** field—Click the clock icon and then the time on the selected date after which the action plan should no longer be in effect.

  - **Time zone** field—Specifies the time zone for the times in the **From** and **To** fields. By default, this field displays the time zone of your PC. We recommend that you use the time zone of the server on which Cisco Fog Director is running. To change the time zone that displays in this field, click this field, click its delete icon ✕, and then start typing the time zone that you want. You can choose a time zone from the list that displays.

- **On a cron schedule**—Causes the action plan to be in effect for a time period that begins according to a cron schedule that you designate and lasts for the amount of time that you specify. If you choose this option, enter information in the **Cron Expression** and **Maintenance window duration** fields that appear:
  - **Cron expression** field—Enter a cron expression that defines date and time that the action plan should start. The expression should be in the format *MinuteHourDateMonthDayYear*, where:

    - *Minute*—Minutes after the hour. Valid values are 1 through 59.

    - *Hour*—Hour of the day, in 24-hour format. Valid values are 0 through 23.

    - *Date*—Date of the month. Valid values are 1 through 31.

    - *Month*—Month of the year. Valid values are 1 (January) through 12 (December).

    - *Day*—Day of the week. Valid values are 1 (Sunday) through 7 (Saturday).

    - *Year*—Four-digit year.
  - **Maintenance window duration** field—Enter the number of minutes that the action plan should be in effect from the time that it starts.

Step 7 In the **Number of times to retry failed installs** field, enter the number of times that Cisco Fog Director retries a failed action.

If you do not want Cisco Fog Director to retry a failed action, enter **0** in this field.

Step 8 In the **Minimum duration between retries** field, enter the minimum number of minutes that Cisco Fog Director waits from the time that an action last failed before retrying the action.

In some situations, internal system factors can cause the system to wait for a time that is longer than the minimum.

Step 9 Complete the app installation, configuration, upgrade, or uninstallation procedure to save modifications that you made to this custom action plan.

You do not need to complete the procedure if you deleted this action plan.

Managing Outstanding and Expired Actions for Apps

If an action does not complete successfully when you execute it and it has an action plan that instructs Cisco Fog Director to retry a failed action, or if an action has an action plan that instructs Cisco Fog to perform the action in a designated maintenance window, the action will be in one of these states:

- Outstanding—The action will be retried or executed in a maintenance window according to the action plan that is associated with the action
- Expired—The action did not complete successfully but will no longer be retried due to any of the following situations:
  - The maximum number of retries that an action plan specifies for the action has been reached
  - The maintenance window or windows that were scheduled for the action no longer exist

  - You manually cancel future retries of the action
  - The failure is not related to certain device reachability or network connectivity issues

You can manage actions that are in these states by using information and options on the Actions page.

The following sections provide additional information:

- Outstanding and Expired Actions Management Options, page 4-54
- Outstanding and Expired Actions Management Procedure, page 4-56

Outstanding and Expired Actions Management Options

To view options for outstanding actions, click the **View outstanding actions** link on the App Configuration page. This link displays if one or more app actions are in Outstanding state. The following information displays:

- Install—Number of devices on which an app install action is in Outstanding state
- Edit—Number of devices on which an app configuration action is in Outstanding state
- Upgrade—Number of devices on which an app upgrade action is in Outstanding state
- Uninstall—Number of devices on which an app uninstall action is in Outstanding state

To see detailed information about the install, edit, upgrade, or uninstall action that are in Outstanding state or Expired state, click the display for the action type that you want. The Actions page displays. This page includes the items that Table 4-13 describes.

Table 4-13 Actions Page Items

Item	Description
Search box	Type all or part of a hostname or IP address to display information for devices with matching information. The table display updates as you type.
Show drop-down list	Choose an option to designate the devices that display in the Devices table: • **All**—Displays devices on which one or more app install, configuration, upgrade, or uninstall action is in Outstanding state or Expired state • **Install**—Displays devices on which one or more app install action is in Outstanding state or Expired state • **Edit**—Displays devices on which one or more app configuration action is in Outstanding state or Expired state • **Upgrade**—Displays devices on which one or more app upgrade action is in Outstanding state or Expired state • **Uninstall**—Displays devices on which one or more app uninstall action is in Outstanding state or Expired state
Outstanding button	Click to displays devices for which actions are in Outstanding state.
Expired button	Click to displays devices for which actions are in Expired state.

Table 4-13 Actions Page Items (continued)

Item	Description
Devices table	Provides information about each device on which actions are in Outstanding state or Expired state: • Check box—Check the check box for each device on which you want to manually retry the action or cancel additional retries of an action. You can click the check box in the title row of the table to quickly check all boxes in the table. • Host Name field—Hostname of a device on which the action is in Outstanding state or Expired state. • IP Address field—IP address of a device on which the action is in Outstanding state or Expired state. • Last Attempted field—Date and time that Cisco Fog Director last attempted to perform the action on the device. • Message—Brief description of why the action last failed on the device. • Next attempt—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. • Action Type—Type of the outstanding action (**Install**, **Uninstall**, **Upgrade**, **Edit Configuration**, or **Edit Resources**). • Pending attempts—For a device with actions in Outstanding state, displays the 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. For a device that you moved to Expired state by manually canceling future retries, displays the maximum number of retries that were pending when you canceled the retries. • 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 4-13 Actions Page Items (continued)

Item	Description
Selected Devices table	Provides information about each device on which you want to manually retry an action or cancel additional retries of an action Devices appear in this table after you check their check boxes in the Installed Devices table and then click **ADD SELECTED DEVICES**. This table includes the following items: • Host Name field—Hostname of a device on which to manually retry or cancel future retries of an action • IP Address field—IP address of a device on which to manually retry or cancel future retries of an action • Message—Can display the following information: – Brief description of why the action last failed on the device – "Scheduled"—Indicates that the action is scheduled to run in an a future maintenance window – "Expired because no future maintenance window exists"—Indicates that the action is in Expired state • Action Type—Type of the outstanding action (**Install**, **Uninstall**, **Upgrade**, **Edit Configuration**, or **Edit Resources**) • Action—Click the x icon ✖ to remove a device from the Selected Devices table • 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
RETRY NOW button	Click to immediately execute on the devices that are listed in the Selected Devices table an action that is in Outstanding device.
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.

Outstanding and Expired Actions Management Procedure

This section describes how to manage actions that are in Outstanding state or Expired state. Management tasks include:

- Viewing information about actions.
- Manually retrying actions. You can manually retry actions that are in Outstanding state or in Expired state.
- Canceling future retries of actions.

You also can manually retry an action as described in the "Retrying a Failed Action for an App" section on page 4-45, and cancel future retries for outstanding actions on a device as described in the "Device Details Area" section on page 5-7.

To view information about, manually retry, or cancel future retries of actions in Outstanding state or Expired state, follow these steps:

Procedure

Step 1 On the App Configuration page, click the **View outstanding actions** link, and then click the Action display (**Install**, **Edit**, **Upgrade**, or **Uninstall**) for the action type that you want.

The Actions page displays. By default, this page shows devices on which the action that you chose is in Outstanding state. For descriptions of the items on this page, see Table 4-13 on page 4-54.

Step 2 (Optional) To display information in the Devices table for devices that have actions of a specific type or in a specific state, take these actions:

- To display information for devices that have outstanding actions of a particular type, choose one of the following options from the **Show** drop-down list:
  - **All**—Displays devices on which one or more app install, configuration, upgrade, or uninstall actions are in Outstanding state or Expired state
  - **Install**—Displays devices on which one or more app install actions are in Outstanding state or Expired state
  - **Edit**—Displays devices on which one or more app configuration action is in Outstanding state or Expired state
  - **Upgrade**—Displays devices on which one or more app upgrade actions are in Outstanding state or Expired state
  - **Uninstall**—Displays devices on which one or more app uninstall actions are in Outstanding state or Expired state
- To display devices on which an action type is in Expired state, click the **Expired** button.
- To display devices on which an action type is in Outstanding state, click the **Outstanding** button.

Step 3 To manually retry an action or cancel future retries of an action, take these actions:

a. In the Installed Devices table, check the check box for each device on which you want to manually retry an action or cancel future retries of an action.

For detailed information about this table and locating devices, see the "Outstanding and Expired Actions Management Options" section on page 4-54.

b. Click the **ADD SELECTED DEVICES** button.

The devices with checked check boxes are added to the Selected Devices table. Actions will be retried or canceled on the devices that this table lists. For detailed information about this table and about removing devices from this table, see the "Outstanding and Expired Actions Management Options" section on page 4-54.

c. Click the desired button:

- **RETRY NOW**—Click to immediately retry the actions on the devices that are listed in the Selected Devices table.
- **CANCEL OUTSTANDING**—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. In his situation, Cisco Fog Director no longer retries the action or runs it a future maintenance window.

Backing Up and Restoring Apps

The Cisco Fog Director export and import features let you back up and restore apps. These features can be useful for creating an archive of apps or for importing apps to another Cisco Fog Director.

The export feature saves all apps that appear in the Available and the Unpublished areas on the Apps View page to a zip file outside of Cisco Fog Director. The import feature restores apps that have been exported to a zip file.

The following sections describe these features in detail:

- Exporting Apps, page 4-58
- Importing Apps, page 4-58

Exporting Apps

Exporting apps lets you save apps in an export file, which is a zip file named exportedApps.zip that is stored outside of Cisco Fog Director. This action affects all apps that appear in the Available and the Unpublished areas on the Apps View.

`To export an app, follow these steps:

Procedure

Step 1 In the Available Apps area on the Apps View page, click the **Export Apps** button.

Step 2 Follow the on-screen prompts to save the app in the location of your choice.

The file is named exportedApps.zip.

Importing Apps

When you import apps that you exported as described in the "Exporting Apps" section on page 4-58, the apps are added to Cisco Fog Director. You can import apps only to a Cisco Fog Director to which no apps have yet been added.

To import an app, follow these steps:

Procedure

Step 1 In the Apps View page, click the **Import Apps** button.

This button appears only if no apps have yet been added to Cisco Fog Director.

Step 2 In the Import Apps dialog box that displays, click the **Select Apps Archive** button.

Step 3 Follow the on-screen prompts to locate and select the exportedApps.zip export file that you want to import.

When the import process completes, the Import Apps Dialog box confirms the completion. It also provides information about any apps that could not be imported (you might need to scroll down in the dialog box to see this information).

Monitoring an App

Monitoring an app provides information about the operation of an app across all devices on which it is installed. This information can be useful for evaluating the operation of the app or for troubleshooting. The following sections describe the app monitoring features:

- Viewing General Monitoring Information, page 4-59
- Viewing Detailed Monitoring Information, page 4-62

Viewing General Monitoring Information

To view general monitoring information about an installed app, take any of these actions:

- In the Installed Apps area on the Apps View page, click the App Status donut chart for the app
- In the Available Apps area on the Apps View page, click the icon for the app that you want to monitor, and then click the **MONITOR APP** button
- Click the **MONITOR APP** button when you are viewing detailed information about the app

The App Monitoring page displays. This page includes information and features that apply to the app, and includes some or all of the items that Table 4-14 describes.

Table 4-14 App Monitoring Page Items

Item	Description
Installed-on information	Shows the number of devices on which the app has been successfully installed.
Configuration View link	Click to display detailed information about the app, as described in the "Viewing Detailed Information about an Installed or Available App" section on page 4-6.
APP DOWNTIME	Shows the number of devices on which the app has been in Running state or in Stopped state during the designated time period. Hover your mouse pointer over any part of the chart to see detailed information about a data point. You can click **Day**, **Week**, or **Month** above this graph to designate the time period for the information.

Table 4-14 App Monitoring Page Items (continued)

Item	Description
Status charts	Show information about devices on which an app is running and on which an app is stopped. For each state, a chart shows the name of the state, and the number of devices on which the app is in that state, and the percentage of devices on which the app is installed that the app is in that state. You can click the following buttons under a status chart: • **STOP**—Appears under the Running chart. Click to stop the app, which shuts down its operation on the host devices on which it is running and puts it in Stopped state on these devices. • **START**—Appears under the Stopped chart. Click to start the app, which initiates its operation on the host devices on which it is stopped and puts it in Running state on these devices. • **VIEW DETAIL**—Appears under each chart and provides access to information that can be useful for troubleshooting. See the "Viewing Detailed Monitoring Information" section on page 4-62. **Note** You also can start and stop an app from the Devices View page as described in the "Starting or Stopping an App on a Device" section on page 5-39. 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.
Alert Information	Appears if Cisco Fog Director has detected one or more alerts for the app and you have not yet responded to the alerts. This area includes these items: • Alerts bar—Displays the number of alerts for this app that you have not ignored. • **Critical Issues**—Displays the number of alerts whose severity is critical. Click to display the App Alerts table on this page with information about these alerts. • **Warnings**—Displays the number of alerts whose severity is warning. Click to display the App Alerts table on this page with information about these alerts. • **Info Events**—Displays the number of alerts whose severity is info. Click to display the App Alerts table on this page with information about these alerts. See the "Managing App Alerts" section on page 4-63.

Table 4-14 App Monitoring Page Items (continued)

Item	Description
App Alerts table	Appears if you click **Critical Issue**s, **Warnings**, or **Info Events** in the Alert Information area and provides information about each active alert for the app. Includes the following items: • Show drop-down list—Choose the type of alert to display in the App Alerts table. Options are **All** (to display all alerts), **Status**, **Health**, **Configuration**, **Resources**, **Memory Consumption**, **Disk Consumption**, **CPU Consumption**, **Device Clock Sync**, and **Device Reachability**. • **VIEW ALL** button—Click to display the Alerts page, on which you can view alerts for the app and respond to alerts. See the "Managing App Alerts" section on page 4-63. • Search Hostname, IP address field—Type all or part of a hostname or IP address of a device to display alert information for devices with matching information. The table display updates as you type. • Show field—Enter the name of a tag and then press the **Enter** key to display alert 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. • Type—Type of alert (status, health, config, resource, reachability, memoryconsumption, diskconsumption, cpuconsumption, clocksync). • IP Address—IP address of the device on which the alert is active. • Time—Date and time that the alert was generated. • Message—Brief description of the alert. • Suggestion—Recommended action for you to take to clear the alert. • 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 4-14 App Monitoring Page Items (continued)

Item	Description
App Consumption	Displays the following charts, which provide information about device resources that the app consumes: • Mean CPU Consumption—Average (mean) CPU resources that the app used on devices on which it ran during the designated time period. • Mean Disk Consumption—Average (mean) hard disk space that the app used on devices on which it ran during the designated time period. • Mean Memory Consumption—Average (mean) RAM resources that the app used on devices on which it ran during the designated time period. • Mean Network Consumption—Average (mean) network bandwidth that the devices on which the app ran 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. Click a chart to display a table with detailed information about the corresponding resource consumption for individual devices. The tables include the following items: • Host Name—The hostname of the device on which the resource is consumed. Click a hostname to display device details information for the device. See the "Viewing Detailed Information about a Device" section on page 5-6. • IP Address—The IP Address of the device on which the resource is consumed. Click an IP address to display device details information for the device. See the "Viewing Detailed Information about a Device" section on page 5-6. • Tags—Tags that have been assigned to the device. See the "Managing Tags for Devices" section on page 5-37. • CPU Consumption, Disk Consumption, Memory Consumption, or Network Consumption (depending on the chart that you clicked)—Shows the average (mean) resource consumption of the app on the device during the designated time period.

Viewing Detailed Monitoring Information

To view general monitoring information about an installed app, click either of these buttons on the App Monitoring page:

- **VIEW DETAIL** under the Running Devices chart—Displays a table for the devices on which the app is in Running state. This table includes the **Running Devices** tab and the **Error** tab.

  This button is dimmed if the app is not in the Running state on at least one device.

- **VIEW DETAIL** under the Stopped Devices chart—Displays a table for the devices on which the app is in Stopped state. This table includes the **Stopped Devices** tab and the **Error** tab.

  This button is dimmed if the app is not in the Stopped state on at least one device.

The **Running Devices** or **Stopped devices** tab in the table provide information for devices on which the app is in the corresponding state. The **Error** tab provides information about devices on which the app is in an error state of some kind.

This table includes the items that Table 4-3 describes.

Table 4-15 Detailed Monitoring Information for an App

Item	Description
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 the app is in the state. Click a hostname to display device details information for the device. See the "Viewing Detailed Information about a Device" section on page 5-6.
IP Address	IP Address of the device on which the app is in the state. Click an IP address to display device details information for the device. See the "Viewing Detailed Information about a Device" section on page 5-6.
Tags (on **Running Devices** or **Stopped Devices** tab only)	Tags that have been assigned to the device. See the "Managing Tags for Devices" section on page 5-37.
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.
View App Log button (on **Running Devices** or **Stopped Devices** tab only)	Click to display log information that is generated by the app on a device.
Error Summary (on **Error** tab only)	Brief description of the error that occurred.
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 devices that appear in each page of the table.

Managing App Alerts

Cisco Fog Director generates alerts in various situations. An alert is information that the system collects and provides when it detects certain issues with an app or device.

Each alert has one of the following types, depending on the situation that caused Cisco Fog Director to generate the alert:

- Status—App has a state mismatch on a device or failed to install or uninstall on a device. An app state mismatch situation occurs when the state of the app (Running, In Progress, Stopped, or Failed) is not the state that Cisco Fog Director expects.
- App Health—App is corrupted on a the device or has some other issue with its health.
- App Configuration—Configuration of the app does not match the app configuration settings on the device. This situation can occur if the app configuration is modified outside of Cisco Fog Director.
- App Resource—Resources of the app do not match the app resource settings on the device. This situation can occur if the app resources are modified outside of Cisco Fog Director.
- Device Reachability—Cisco Fog Director cannot contact the device after making the number of consecutive polling attempts as configured for **Heartbeat Miss Count** for the device profile of the device. In this situation, there is one Device Reachability alert for each app that is installed on the device.
- Memory Consumption—During the last hour, an app has consumed more than 95% of the memory that is configured for it on the device.
- Disk Consumption—During the last hour, an app has consumed more than 95% of the disk space that is configured for it on the device.
- CPU Consumption—During the last hour, an app has consumed more than 95% of the CPU resources that are configured for it on the device.
- Device Clock Sync—The time of the device clock is ahead of the time of the Cisco Fog Director clock.
- Read Rate—App has read data from the from the disk on a device at a rate faster than the maximum read rate threshold that is configured for the device. This threshold is configured by using the max_read_rate parameter in the device system-config.ini file.
- Write Rate—App has written data to the from the disk on a device at a rate faster than the maximum write rate threshold that is configured for the device. This threshold is configured by using the max_write_rate parameter in the device system-config.ini file.

In addition, each app has one of the following severity levels, which helps you determine the importance of the alert:

- Critical—App has crashed or has a state mismatch.
- Warning—App has a configuration mismatch or resource mismatch.
- Info—App was detected on the device but Cisco Fog Director does now know the intended state of the app. This situation occurs in a app is installed on a device through Cisco Fog Director and then the device is deleted from and then added again to Cisco Fog Director.

Cisco Fog Director provides detailed alert information on the Alerts page and on the App Monitoring page. An alert that Cisco Fog Director displays on these pages is an *active alert*. You can choose to ignore any alert, which permanently removes if from the display on these pages and from Cisco Fog Director.

The following sections provide additional information:

- App Alert Options, page 4-65
- Ignoring App Alerts, page 4-67

App Alert Options

To display options for viewing and ignoring alerts for an app take either of these actions:

- On the Apps View page, click **Alerts** under the app name and icon for the app whose alerts you want to view or ignore
- In the Alerts area on the App Monitoring page, click **Critical Issues**, **Warnings**, or **Info Events** to display the Alerts table for alerts of the corresponding severity, and then click the **VIEW ALL** button that appears above the table

The Alerts page displays. This page includes the items that Table 4-16 describes.

If you accessed this page from the Apps View page, the App Alerts table shows by default all active alerts. If you accessed this page from the App Monitoring page, the App Alerts table shows by default only alerts that match the severity that you chose (critical, warning, or info).

Table 4-16 Alerts Page Items

Item	Description
App Alerts table	Provides information about active alerts for the app, and includes the following items: • Show drop-down list—Choose the type of alert to display in the App Alerts table. Options are Options are **All** (to display all alerts), **Status**, **Health**, **Configuration**, **Resources**, **Memory Consumption**, **Disk Consumption**, **CPU Consumption**, **Device Clock Sync**, and **Device Reachability**. • Critical button—Click to display in the App Alerts table only alerts with a severity of Critical. • Warning button—Click to display in the App Alerts table only alerts with a severity of Warning. • Info button—Click to display in the App Alerts table only alerts with a severity of Info. • Search Hostname, IP address field—Type all or part of a hostname or IP address of a device to display alert information for devices with matching information. The table display updates as you type. • Show field—Enter the name of a tag and then press the **Enter** key to display alert 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 ignore the alert. You can click the check box in the title row of the table to quickly check all boxes in the table. • Type—Type of alert (status, health, config, resource, reachability, memoryconsumption, diskconsumption, cpuconsumption, clocksync). • IP Address—IP address of the device on which the alert is active. • Time—Date and time that the alert was generated. • Message—Brief description of the alert. • Suggestion—Recommended action for you to take to resolve the issues that generated the alert • 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 ALERTS button	Click to add devices with checked check boxes to the Selected Alerts table.

Table 4-16 Alerts Page Items (continued)

Item	Description
Selected Alerts table	Provides information about each alert that you want to ignore. Alerts appear in this table after you check their check boxes in the App Alerts table and then click **ADD SELECTED ALERTS**. This table includes the following items: • Selected Alerts—Number alerts that you want to ignore. • Search Hostname, IP Address field—Type all or part of a hostname or IP address of a device to display alerts for devices with matching information. The table display updates as you type. • Type—Type of alert (status, health, config, resource, reachability). • IP Address—IP address of the device on which the alert is active. • Time—Date and time that the alert was generated. • Action—Click the x icon ✖ to remove an alert from the Selected Alerts table. Clicking this icon does not affect the alert. • 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.
Ignore button	Available if there is at least one device in the Selected Alerts table. Click to remove the alert from Cisco Fog Director.

Ignoring App Alerts

You remove an app alert from Cisco Fog Director by choosing to ignore it. When you ignore an app, it is removed from the Alerts page, from the alert counters on the Apps View page, and from the Alert Information area and the Alerts table on the App Monitoring page.

To ignore an app alert, follow these steps:

Procedure

Step 1 Take either of these actions:

- On the Apps View page, click **Alerts** under the app name and icon for the app whose alerts you want to ignore
- In the Alerts area on the App Monitoring page, click **Critical Issues**, **Warnings**, or **Info Events** to display the Alerts table for alerts of the corresponding severity, and then click the **VIEW ALL** button that appears above the table

The Alerts page displays. If you accessed this page from the Apps View page, the App Alerts table shows by default all active alerts. If you accessed this page from the App Monitoring page, the App Alerts table shows by default only alerts that match the severity that you chose (Critical Issues, Warning, or Info Events).

Step 2 In the App Alerts table, check the check box for each alert that you want to ignore.

For detailed information about this table and locating alerts, see the "App Alert Options" section on page 4-65.

Step 3 Click the **ADD SELECTED ALERTS** button.

The alerts that you selected are added to the Selected Alerts table. You can ignore the alerts that this table lists. For detailed information about this table and about removing alerts from this table, see the "App Alert Options" section on page 4-65.

Step 4 Click the **IGNORE** button, which appears under the Selected Alerts table

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

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
Last Heard chart	Number of devices with which Cisco Fog Director successfully interacted over the past month. The chart can include sections for day, week, month, and never. Hover your mouse pointer over a section of the cart to see the percentage of devices that correspond to that section.
Reachability chart	Number of devices with which Cisco Fog Director can communicate. Hover your mouse pointer over a section of the cart to see the percentage of devices that correspond to that section.
Top 5 Consumers	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 5-6. • 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
ADD 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 5-17.
IMPORT 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 5-19.

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 5-31. • **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 5-32. • **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 5-37. • **DELETE**—Choose this option to delete multiple devices from Cisco Fog Director inventory. See the "Deleting Devices" section on page 5-36. • **PROFILES**—Choose this option to manage device profiles for devices. See the "Managing Device Profiles" section on page 5-21.

Table 5-1 Devices View Page Items (continued)

Item	Description
Device Filters field	Click this field and then choose from the following 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. • REACHABLE option: – **Online**—Choose this option to display only devices that are on line – **Offline**—Choose this option to display only devices that are not on line • LAST HEARD options: – **Day**—Choose this option to display only devices with which Cisco Fog Director successfully interacted over the past 24 hours – **Week**—Choose this option to display only devices with which Cisco Fog Director successfully interacted beginning from the current time 7 days ago – **Month**—Choose this option to display only devices with which Cisco Fog Director successfully interacted beginning with the current time 28 days ago – **Never**—Choose this option to display only devices with which Cisco Fog Director has not successfully interacted • DISCOVERY STATUS option: – **Not Discovered**—Choose this option to display only devices that Cisco Fog Director has not yet discovered – **Discovering**—Choose this option to display only devices that Cisco Fog Director is in the process of discovering – **Discovered**—Choose this option to display only devices that Cisco Fog Director has discovered – **Discovery Failed**—Choose this option to display only devices that Cisco Fog Director tried to discover was unable to discover (for example, because the device is unreachable)

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. • 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 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 5-6. • 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 5-6. • Tags—Tags for the device. See the "Managing Tags for Devices" section on page 5-37. • 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. • 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: • **Edit Device**—Click to edit various attributes for the device. See the "Editing Attributes for a Device" section on page 5-21. • **Delete Device**—Click to remove the device from Cisco Fog Director. See the "Deleting Devices" section on page 5-36. • **Refresh Device**—Click to cause Cisco Fog Director to rediscover the device and update information that displays. • App 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 %age 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 5-39 or the "Removing an App from a Device" section on page 5-40.

Viewing Detailed Information about a Device

To view detailed information about a device, take any 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.
- On the Apps View page or the Devices View page, click the hostname of 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 5-7
- Apps Area, page 5-12

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 of 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.

Table 5-2 Device Details Area Items (continued)

Item	Description
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 5-47.
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 5-47.
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 5-43.
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 5-47.
REFRESH DEVICE button	Click to cause Cisco Fog Director to rediscover the device and update information that displays on the Device Details page.
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
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
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 5-41. • 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.

Table 5-2 Device Details Area Items (continued)

Item	Description
CARTRIDGES tab	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 5-41.
OUTSTANDING ACTIONS tab	Displays the following information. For related information, see the "Managing Outstanding and Expired Actions for Apps" section on page 4-53. • 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.

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 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 Installed or Available App" section on page 4-6.
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 5-40.
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 added 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 5-42. • **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.

Table 5-3 Apps Area Items (continued)

Item	Description
Cartridges Used	Cisco cartridges that the app requires to run, if any.
Links	Available if you configured links for an app. Click a link to go to the configured resource. See the "Configuring App Links" section on page 4-41.
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 internal interfaces of the app for which you want to view information • 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_config.ini file. **Mapped Port** is the port that is used for external communication with the app. Port mapping is handled by Cisco IOx. • App mac—MAC address that is assigned to the app on the device for the network interface that you choose. • Network Mode—Network mode in that is assigned to the app for the network interface that you choose.
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 change the following settings for an app: • 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 • 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 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 4-15.
Edit Configuration tab	Lets you update configuration for the app. The items that display are defined in the package_config.ini file for the app.
App Log tab (This tab name displays the name of a log files that was generated by the app.)	By default, displays first 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.

Table 5-3 Apps Area Items (continued)

Item	Description
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 FILES** 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.
App Downtime Items	
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.

Table 5-3 Apps Area Items (continued)

Item	Description
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 5-47.

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** 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 5-37 for an explanation of tags.) To enter more than one tag, separate each tag by pressing the **Tab** key.
Contact Details	Optional. Contact information of the person who is responsible for 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.
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 & AND 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 5-19
- Importing an Import File, page 5-20

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.

Cisco recommends 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 5-32.

Procedure

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

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

The Import window displays.

Step 3 Click **Download Sample CSV** 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	Required. Cisco IOS user name that is configured on the device.
https_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 5-37 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.

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 5-19, 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** 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 5-31.

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 device 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.
- **Contact Details**—Contact information of the person who is responsible for 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.
- **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 5-22
- Adding a Device Profile, page 5-23
- Viewing a Device Profile, page 5-25
- Editing a Device Profile, page 5-27
- Deleting a Device Profile, page 5-31

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 5-23.
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.
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 5-30. • **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 5-31.
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

Table 5-4 Profiles Page Items (continued)

Item	Description
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 of 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 5-42 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 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 use the Trust Anchors page that displays to import the certificates.

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 Cisco application-hosting framework 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 the JSON code 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 using 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.
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 of 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 5-42 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.

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

Item	Description
Verify App Signature	If checked, App Package Signature Verification is enabled on the device. When this option is enabled, the Cisco application-hosting framework 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.
Trust Anchor for App Signature Verification	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, take one of these actions, 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. You can view options in the MONITORING and CONMMUNICATION tab and update options in the SECURITY tab.

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 (read only)	
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.
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.
COMMUNICATION Tab (read only)	
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.

Table 5-6 Edit Profile Window Items (continued)

Item	Description
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.
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 Cisco application-hosting framework 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.
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	
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.

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 DEFATUL**.

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 5-19.)

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 5-32
- Editing Information for Multiple Devices, page 5-35

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 DEVICES**. 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 5-32.

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 5-32.

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 5-36
- Deleting Multiple Devices, page 5-37

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 5-38,

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 Monitoring Page by using the as described in the **START** and **STOP** buttons under the Status Charts as described in the "Viewing General Monitoring Information" section on page 4-59).

- Starting an App, page 5-39
- Stopping an App, page 5-40

You also can start or stop an app from the App Monitoring page by clicking the **START** or **STOP** button under a status chart. See the "Viewing General Monitoring Information" section on page 4-59 for more information.

Starting an App

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

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 images that 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 any 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 of 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:

prompt% **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.

Managing Cisco Fog Director Settings

The Cisco Fog Director Settings page includes these sub-tabs:

- Settings—Provides information about Cisco Fog Director, and provides options for downloading the end user license agreement and managing Cisco Fog Director debug logs
- Extensions—Reserved for Future Use

To access the Settings page, log in to Cisco Fog Director as described in the "Accessing Cisco Fog Director" section on page 3-1, and then click the **SETTINGS** tab.

This chapter includes these sections:

Note The Trust Anchors page is reserved for future use.

Viewing Information about Cisco Fog Director

The About Fog Director area on the Settings page > Settings sub-tab provides the information that Table 6-1describes.

Table 6-1 About Fog Director Items

Item	Description
API Version	Version of the Cisco Fog Director API
Release Version	Cisco Fog Director version that you are using
Built On	Date and time that the Cisco Fog Director version that you are using was built

Viewing the License Agreement

Cisco Fog Director End User License Agreement (EULA) contains license, warranty, terms of use, and related information that apply to Cisco Fog Director.

To view the Cisco Fog Director End User License Agreement, follow these steps:

Procedure

Step 1 Click the Cisco Fog Director **Settings** tab.

Step 2 On the Settings page, click the **Settings** sub-tab.

Step 3 In the End User License Agreement area, click the **VIEW END USER LICENSE AGREEMENT** button.

The End User License Agreement window opens and displays the Cisco Fog Director End User License Agreement.

Step 4 After reviewing the license agreement, click the **OK** button to close the End User License Agreement window.

Managing Cisco Fog Director Debug Logs

Cisco Fog Director can create and collect information about your Cisco Fog Director session. This information includes actions performed by users, and errors or exceptions generated by the device or persistent store. You can configure Cisco Fog Director to store this information in a debug log file, which you can provide to your Cisco representative for assistance with troubleshooting, if needed.

To create a debug log file for Cisco Fog Director, follow these steps:

Procedure

Step 1 Click the Cisco Fog Director **Settings** tab.

Step 2 On the Settings page, click the **Settings** sub-tab.

Step 3 In the Logging Configuration area, click the **Yes** button next to “Collect Debug Logs.”

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

Step 5 Click the **DOWNLOAD 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.”

Managing a Syslog Server

You can configure Cisco Fog Director to send information about unexpected app stopping events that it detects to a Syslog service. To do so, follow these steps:

Procedure

Step 1 Click the Cisco Fog Director **Settings** tab.

Step 2 On the Settings page, click the **Settings** sub-tab.

Step 3 In the Logging Configuration area, click the **Yes** button next to "Syslog Server."

The Syslog Configuration fields and the **Apply** button displays.

Step 4 In the first field next to "Syslog Configuration," enter the host name or the IP address of the Syslog server that to which Cisco Fog Director should send information about events.

Step 5 In the second field next to "Syslog Configuration," enter the port number on which a Cisco Fog Director communicates with the Syslog server.

Step 6 Click **APPLY** button.

Step 7 (Optional) To stop Cisco Fog Director from sending events to a Syslog server, click the **No** button next to "Syslog Configuration."

Managing Trust Anchors

A trust anchor is a PEM encoded or DER encoded X509 certificate that Cisco Fog Director uses for SSL validation when it contacts devices with which a device profile that enables **Verify SSL Certificates** is associated. Certificate validation is performed as part of the SSL handshake. If the validation fails, Cisco Fog Director cannot communicate with the device.

For information about enabling this verification feature, see the "Managing Device Profiles" section on page 5-21.

Trust Anchors Page

The Trust Anchors page displays when you click the **MANAGE TRUST ANCHORS** button in the Security area of the Settings tab on the Settings page. (You also can access this page when you add or edit a device profile as described in the "Managing Device Profiles" section on page 5-21.) The Trust Anchors page provides information about trust anchors and lets you import or delete trust anchors.

The Trust Anchors page includes the items that Table 6-2 describes.

Table 6-2 Trust Anchors Page Items

Item	Description
Trust Anchors field	Displays the number of trust anchors that have been imported.
IMPORT button	Click to import a trust anchor to Cisco Fog Director.
DELETE button	Click to remove the selected trust anchor from Cisco Fog Director.

Table 6-2 Trust Anchors Page Items (continued)

Item	Description
Trust Anchor table	Provides information about each trust alias can be imported to Cisco Fog Director. This table includes the following: • Check box—Click to select the corresponding trust anchor. You can then delete that trust anchor. • ALIAS—Alias of the trust anchor. You designate the alias when you import the trust anchor. • SUBJECT—Subject of the trust anchor. The subject is assigned automatically. • Expiration date—Date and time that the trust anchor expires. You can click the **ALIAS**, **SUBJECT**, or **Expiration date** column heading repeatedly to change the order that the trust anchors display in the table. As you click, the display between ascending alphanumeric order, descending alphanumeric order, and default order based on the corresponding column.

Importing a Trust Anchor

Importing a trust anchor is the process of importing a PEM encoded or DER encoded X509 certificate to Cisco Fog Director.

To import a trust anchor, follow these steps:

Procedure

Step 1 Take either of these actions:

- Click the Cisco Fog Director **Settings** tab, click the **Settings** sub-tab, and then click the **MANAGE TRUST ANCHORS** button in the Security area.
- When adding or editing a device profile, click the Security tab, hover your mouse pointer over the information icon ℹ next to "Verify SSL Certificate," and then click the **Click here** link in the message that displays. See the "Managing Device Profiles" section on page 5-21.

The Trust Anchors page displays.

Step 2 In the Trust Anchors page, click the **IMPORT** button.

The Import dialog box displays.

Step 3 In the Import dialog box, take these actions:

a. In the **Alias to be used for this certificate** field, enter an alias to be used to identify the trust anchor. if you use an existing alias name, the certificate with that name is overwritten with the certificate that you are importing. An alias can contain any character and is not case sensitive.

b. Click the **SELECT CERTIFICATE** button and then navigate to and select the certificate to import.

The certificate is imported and the Trust Anchors page redisplays with the trust anchor shown in the Trust Anchors table.

Deleting a Trust Anchor

To delete a trust anchor from Cisco Fog Director, follow these steps:

Procedure

Step 1 Click the Cisco Fog Director **Settings** tab.

Step 2 On the Settings page, click the **Settings** sub-tab.

Step 3 In the Security area, click the **MANAGE TRUST ANCHORS** button.

The Trust Anchors page displays.

Step 4 In the Trust Anchors page, check the check box for the certificate that you want to delete, and then click the **DELETE** button.

The certificate is deleted from Cisco Fog Director.

Managing Cisco Fog Director Data Backup and Restore

The Backup & Restore area on the Settings page > Settings sub-tab provides options for creating and restoring a backup file. A backup file is an encrypted archive file that contains Cisco Fog Director data.

This page includes these buttons:

- **Backup**—Click to create a backup file. See the "Creating a Backup File" section on page 6-5.
- **Restore**—Click to restore the data in a backup file to Cisco Fog Director. See the "Restoring a Backup" section on page 6-6.

Creating a Backup File

Creating a backup file creates an encrypted archive file that contains the following Cisco Fog Director data:

- Information about devices that Cisco Fog Director manages
- Information about apps
- Device monitoring information
- Configuration settings

The backup file creation process stops and starts Cisco Fog Director automatically.

To create a backup file, follow these steps:

Procedure

Step 1 Click the Cisco Fog Director **Settings** tab.

Step 2 On the Settings page, click the **Settings** sub-tab.

Step 3 In the Backup & Restore area, click the **BACKUP** button.

The Backup dialog box displays.

Step 4 In the Backup dialog box, take these actions:

a. In the Encryption password field, enter a string of characters to be used for encryption and decryption of the backup file.

b. Click the **START BACKUP** button.

Step 5 Follow the on-screen prompts to save the backup file with a name and in the location of your choice.

The system creates the backup file. This process can take some time, depending on how much data is to be backed up. Cisco Fog Director stops and then restarts when the process completes.

Restoring a Backup

Restoring a backup restores the backed up data to Cisco Fog Director.

The restore process stops and starts Cisco Fog Director automatically.

To restore a backup file, follow these steps:

Procedure

Step 1 Click the Cisco Fog Director **Settings** tab.

Step 2 On the Settings page, click the **Settings** sub-tab.

Step 3 In the Backup & Restore area, click the **RESTORE** button.

The Restore dialog box displays.

Step 4 In the Restore dialog box, take these actions:

a. In the Decryption password field, enter the encryption password that you specified when you created the backup file.

b. Click **SELECT BACKUP ARCHIVE**, and then navigate to and select the backup file that you want to restore.

The system updates Cisco Fog Director with the information in the backup file. This process can take some time, depending on how much data is in the backup file. Cisco Fog Director stops and then restarts when the process completes.

Managing Cartridges

Packages for PAAS apps include only the app logic (such as Python or Java files), but not the Linux operating files or the root file system that the app requires. Cartridges provide the root file system and Python or Java files that an app requires to run.

Before you can install a PAAS through Cisco Fog Director, you must add the cartridges that the app requires. Cisco Fog Director prevents installing a PAAS app that requires cartridges if the cartridges have not been added.

Cartridges are not used by KVM apps.

The Cisco Fog Director Cartridges page provides information about cartridges and lets you manually add a cartridge to Cisco Fog Director.

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

This chapter includes these sections:

Viewing General Information about Cartridges

The Cartridges page, which displays when you choose the **CARTRIDGES** tab in Cisco Fog Manager, provides general information about cartridges that have uploaded to Cisco Fog Manager, and lets you upload additional cartridges.

This page includes the items that Table 7-1 describes.

Table 7-1 Cartridges Page Items

Item	Description
Cartridges table	Provides information about each cartridge that has been uploaded to Cisco Fog Director. This table includes the following items: • NAME—Cisco-assigned name of the cartridge. • VERSION—Version of the cartridge. • CPU ARCH—CPU architecture that is required for the cartridge to operate. • DESCRIPTION—Cisco-assigned description of the cartridge. • SOURCE—Indicates the source location of the cartridge as follows: – **Fog Director**—Source location is Fog Director. – **Local**—Source location is your local drive. • ACTION—Click the **Delete** icon to delete the corresponding cartridge and its metadata from Cisco Fog Director. See the "Deleting a Cartridge" section on page 7-3. • 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 cartridges that appear in each page of the table.
Search box	Type all or part of a cartridge name, CPU architecture, or description to display information for cartridges with matching information. The table display updates as you type.
ADD NEW CARTRIDGE button	Click to manually add a cartridge to Cisco Fog Director. See the "Adding a Cartridge Manually" section on page 7-2.

Adding a Cartridge Manually

Manually adding a cartridge uploads from your local drive to Cisco Fog Director. The app is then available for installation when you install an app that requires it.

To manually add a cartridge to Cisco Fog Director, follow these steps:

Procedure

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

Step 2 On the Cartridges page, click the **ADD NEW CARTRIDGE** button.

The Add New Cartridge window displays.

Step 3 In the Add New Cartridge window, click the **Select Cartridge Package** button.

Step 4 Locate and select the cartridge that you want to upload.

Deleting a Cartridge

Deleting a cartridge removes the cartridge and its metadata from Cisco Fog Director.

For information about deleting unused cartridges from a device, see the "Deleting Unused Cartridges" section on page 5-41.

To delete a cartridge, follow these steps:

Procedure

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

Step 2 On the Cartridges page, click the **Delete** icon in the ACTION column for the cartridge that you want to delete.

A

B

C

D

E

F

H

I

L

M

N

O

P

R

S

T

U

V