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 host name 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 appears.

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**.

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 host name 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 my 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 using Cisco IOx Client or Cisco IOx Local Manager • Delete the device from Cisco Fog Director	See your Cisco IOx Client or Cisco IOx Local Manager documentation, or see the "Deleting a Device" section on page 5-13.
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 5-9 or the "Importing Devices" section on page 5-10.
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	Uninstall the app from the device using Cisco IOx Client or Cisco IOx Local Manager.	See your Cisco IOx documentation.
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 5-9 or the "Importing Devices" section on page 5-10.
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 5-9 or the "Importing Devices" section on page 5-10.

Troubleshooting

The following sections provide information that can be useful for troubleshooting Cisco Fog Director.

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 4-54. Also see the description of the App Log tab and View all App Logs in the "Apps Area" section on page 5-7
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 5-5. Also see the "Obtaining Device Logs" section on page 5-16
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**	