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 5-22.

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 5-22.) 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 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 5-22.

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.