



Managing System Settings

This section describes how to manage system settings.



Note To manage system settings, you must be logged in either as root or as a user with Administrative Operations permissions.

System settings are managed from the **ADMIN > System Management** menu.

ADMIN ▾	
Access Management	System Management
Users	Active Sessions
Roles	Audit Trail
Domains	Certificates
Password Policy	Data Retention
Authentication	License Center
	Logging
	Syslog Settings
	Provisioning Settings
	Server Settings
	Jobs

- [Managing Active Sessions, on page 2](#)
- [Displaying the Audit Trail, on page 3](#)
- [Managing Certificates, on page 5](#)
- [Configuring Data Retention, on page 8](#)
- [Managing Licenses, on page 9](#)
- [Cisco IoT FND Logs, on page 9](#)
- [Configuring Provisioning Settings, on page 11](#)
- [Configuring Server Settings, on page 16](#)
- [Configure the Issue Status Bar, on page 22](#)

- [Manage the Syslog, on page 22](#)
- [View Jobs, on page 23](#)

Managing Active Sessions

IoT FND tracks active user sessions and lets you log out users.

Viewing Active Sessions

To view active user sessions:

Procedure

Choose **ADMIN > System Management > Active Sessions**.

IoT FND displays the Active Sessions page.

ADMIN > SYSTEM MANAGEMENT > ACTIVE SESSIONS				
<input type="button" value="Refresh"/> <input type="button" value="Logout Users"/> <input type="button" value="Clear Filter"/>				
<input type="checkbox"/>	User Name	IP	Login Time	Last Access Time
<input type="checkbox"/>	root	10.65.50.154	2021-11-11 12:57	2021-11-11 14:23
<input type="checkbox"/>	root	10.65.40.200	2021-11-10 16:45	2021-11-11 14:23
<input type="checkbox"/>	root	10.65.79.9	2021-11-11 10:47	2021-11-11 14:23
<input type="checkbox"/>	root	10.65.231.232	2021-11-11 11:01	2021-11-11 12:20
<input type="checkbox"/>	root	10.65.35.187	2021-11-10 13:24	2021-11-11 08:55
<input type="checkbox"/>	root	10.227.243.226	2021-11-10 10:19	2021-11-10 18:45

The table describes the Active Session fields:

Field	Description
User Name	The user name in the session record. To view user settings, click the user name.
IP	The IP address of the system the user employs to access IoT FND.
Login Time	The log in date and time for the user.
Last Access Time	The last time the user accessed the system.

Tip

Click the **Reload** button (upper-left hand corner) to update the users list.

Logging Out Users

To log out an IoT FND user:

Procedure

- Step 1** Choose **ADMIN > System Management > Active Sessions**.
- Step 2** Select the check boxes for those users you want to log out.
- Step 3** Click **Logout Users**.
- Step 4** Click **Yes** to confirm logout of the users.

Filtering the Active Sessions List

To filter the Active Sessions list using column filtering:

Procedure

- Step 1** Choose **ADMIN > System Management > Active Sessions**.
- Step 2** Hover the mouse over the User Name column heading to expose the filter icon (triangle). Enter the user name or the first characters of the user name to filter the list.

The screenshot shows the Cisco IoT Field Network Director interface. The top navigation bar includes the Cisco logo, the title 'IoT FIELD NETWORK DIRECTOR', and tabs for DASHBOARD, DEVICES, OPERATIONS, CONFIG, and ADMIN. Below the navigation bar, the breadcrumb trail is 'ADMIN > SYSTEM MANAGEMENT > ACTIVE SESSIONS'. There are three buttons: Refresh, Logout Users, and Clear Filter. The main table has four columns: User Name, IP, Login Time, and Last Access Time. The User Name column has a dropdown menu open, showing options for Sort Ascending, Sort Descending, and Filters. The table contains several rows of active sessions, all with the User Name 'root'.

User Name	IP	Login Time	Last Access Time
<input type="checkbox"/> root		21-11-10 10:19	2021-11-10 18:45
<input type="checkbox"/> root		21-11-10 13:24	2021-11-11 08:55
<input type="checkbox"/> root	10.65.231.232	2021-11-11 11:01	2021-11-11 12:20
<input type="checkbox"/> root	10.65.79.9	2021-11-11 10:47	2021-11-11 14:27
<input type="checkbox"/> root	10.65.40.200	2021-11-10 16:45	2021-11-11 14:27
<input type="checkbox"/> root	10.65.50.154	2021-11-11 12:57	2021-11-11 14:27

For example, to list the active sessions for the root user, enter **root**.

Tip

To remove the filter, from the User Name drop-down menu, clear the **Filters** check box or click **Clear Filter**.

Displaying the Audit Trail

Use the audit trail to track IoT Field Network Director user activity.

To display the Audit Trail:

Procedure

Choose **ADMIN > System Management > Audit Trail**.

Date/Time	Domain	User Name	IP	Operation	Status	Details
2023-10-12 06:31:30	root	root	10.142.92.90	Tunnel provisioning template updated	Success	Device type: Lgt 1000
2023-10-12 08:26:15	root	root	10.142.92.80	Login	Success	N/A
2023-10-12 08:44:29	root	root	10.232.4.123	Login	Success	N/A
2023-10-11 08:59:16	root	root	10.196.134.90	Devices removed	Success	N/A
2023-10-11 08:52:08	root	root	10.196.134.90	Login	Success	N/A
2023-10-11 06:57:09	root	root	10.196.134.90	IPAM IPv6 address generation	Success	Excluded Ipv6 [13], Usable Ipv6 generated [243]
2023-10-11 06:57:09	root	root	10.196.134.90	Tunnel provisioning settings changed	Success	N/A
2023-10-11 06:52:50	root	root	10.196.134.90	Login	Success	N/A

The table below describes the Audit Trail Fields:

Field	Description
Date/Time	Date and time of the operation.
Domain	Specifies domains with root or non-root access. <ul style="list-style-type: none"> Root - The Admin user who defines root access for other users while creating a domain. Non-root - Admin creates the domain without root access.
User Name	The user who performed the operation. To view user settings, click the user name.
IP	IP address of the system that the user employs to access IoT FND.
Operation	Type of operation performed.
Status	Status of the operation.
Details	Operation details.

Tip

Click the **Refresh** icon (far right) to update the list.

Filtering the Audit Trail List

To filter the Audit Trail list using column filtering:

Procedure

Step 1 Choose **ADMIN > System Management > Audit Trail**.

Step 2 From the User Name drop-down menu, pass over Filters option and in the field that appears enter the user name or the first characters of the user name to filter the list.

For example, to list the Audit Trail entries for the user jane, enter **jane**.

Tip

To remove the filter, from the User Name drop-down menu, uncheck the **Filters** check box or click **Clear Filter** (left of the screen).

Managing Certificates

The Certificates page displays the certificates for CSMP (CoAP Simple Management Protocol), and Web certificates used by IoT FND and lets you download these certificates.

To display the CSMP, and Web certificates:

Procedure

Step 1 Choose **ADMIN > System Management > Certificates**.

Step 2 To view a certificate, click its corresponding heading (such as Certificate for Routers).

ADMIN > SYSTEM MANAGEMENT > CERTIFICATES

Certificate for CSMP Certificate for Routers Certificate for Web Certificate Settings

Certificate:
Data:
Version: 3
Serial Number: 191174027
Signature Algorithm: SHA256withECDSA
Issuer: CN=SSM_CSMP, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US
Validity
Not Before: Tue Jul 22 23:32:52 UTC 2014
Not After: Thu Jul 21 23:32:52 UTC 2044
Subject: CN=SSM_CSMP, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US
Fingerprints:
MD5: 2E:AC:06:1F:3E:AB:A6:BE:33:1F:1E:EF:33:D9:80:29
SHA1: 48:A2:EC:63:2F:6F:54:25:23:5D:E7:6F:4E:E9:8E:2D:93:50:A0:FF
SHA256: C4:10:BB:56:16:52:CC:A8:40:8C:E8:46:50:71:01:EE:D1:BB:15:7F:0E:1B:32:9E:93:20:36:72:62:47:1C:49
Subject Public Key Info:
Public Key Algorithm: EC
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:
2A:86:48:CE:3D:03:01:07:03:42:00:04:23:D2:83:
45:E8:D5:DF:86:9D:6E:E7:58:0D:C1:8F:35:9D:57:
B1:3D:50:4A:16:01:15:C4:81:19:B0:E6:60:B8:64:
14:01:5D:56:83:BE:E1:85:98:CB:90:E1:F7:9B:F4:
33:5A:4B:29:AD:35:69:9B:4F:DC:42:7F:EB:C2:99:
A5
X509v3 extensions:

☒ Binary ☐ Base64 [Download](#)

Step 3 To download a certificate, select encoding type (**Binary** or **Base64**) radio button, and then click **Download**.

For more information about certificates, see [Generating and Installing Certificates](#) in the Cisco IoT Field Network Director Installation Guide.

Configuring CA Certification to verify the App Signature

Allows you to import and add a trust anchor to the default profile for a Cisco IOx device that is being managed by IoT FND such as IC3000 or IR800. (The default profile is not visible to the user). You can enable this capability on the Application Security tab of the Certificate page.

The Application Security tab only appears when both of the following conditions are met:

- The user should have application management permission.
- At least one IOx device is being managed such as IC3000 or IR800.

To import and add a trust anchor to a default profile for a Cisco IOx device:

Procedure

Step 1 Choose **ADMIN > System Management > Certificates**.

Step 2 Select the Application Security tab. The page that appears displays any existing trust anchors.

Note

By default, no information will display for new installations or updates and the fields for Checksum and Trust Anchor will display a value of 'None'.)

Step 3 To import a new a new trust anchor, check the boxes next to App Signature and Import New Trust Anchor and then enter a path to the file. Click the disk icon to Save your entries. File will also be pushed to Fog Director.

Note

After you save and reload the Certificates page, the Checksum and Trust Anchor File name appear on the page replacing the previous values of None.

The screenshot shows the Cisco IoT Field Network Director web interface. The top navigation bar includes the Cisco logo, 'IoT FIELD NETWORK DIRECTOR', and links for 'DASHBOARD' and 'DEVICES'. Below this, the breadcrumb trail is 'ADMIN > SYSTEM MANAGEMENT > CERTIFICATES'. A sub-navigation bar contains tabs for 'Certificate for CSMP', 'Certificate for Routers', 'Certificate for Web', 'Certificate Settings', and 'Application Security' (which is selected and highlighted). The main content area is titled 'Existing trust Anchor' and contains a large empty text box. To the right of this box, the following fields are displayed: 'Checksum: None', 'Trust Anchor filename: None', 'App Signature: ☐', and 'Import new Trust Anchor: ☐'. Below these is a 'File:' label followed by a text input field containing 'Select a file from local directory.' and a blue button with a disk icon.

CGMS Certificate Renewal for Routers

The **Renew Certificate for Routers** option in the UI automates the CGMS and/or CA certificate renewal process by updating the certificates in the keystore and encrypting the router password with new certificate. The supported certificate file extension is either (.cer) or (.pfx). We recommend you to schedule the automation job during the maintenance window to avoid conflict with other active operations (such as configuration push, firmware upgrade) running in FND.

To automate cgms or CA certificate renewal for routers:

Procedure

Step 1 Choose **ADMIN > System Management > Certificates**.

Step 2 Select the **Renew Certificate for Routers** tab.

ADMIN > SYSTEM MANAGEMENT > CERTIFICATES

Certificate for Routers Certificate for Web Certificate Settings **Renew Certificate for Routers**

CA Certificate: Only .cer or .pfx file **Upload CA Certificate**

FND Certificate for Routers: cgms.pfx **Upload FND Certificate for Routers**

Schedule Renewal Job **Cancel Renewal Job**

Keystore certificate upload job is not yet scheduled.

Step 3 Click either **Upload CA Certificate** or **Upload FND Certificate for Routers** to upload a CA or CGMS certificate.

Note

You can also upload both CA certificate and CGMS certificate simultaneously.

Step 4 Browse and select a valid CGMS or CA certificate in either (.cer) or (.pfx) format.

Step 5 Enter the password (applicable only for (.pfx file) and then click **Upload**.

Upload CA Certificate

File: Only .cer or .pfx file **Browse**

Password (Only for pfx):

Upload **Reset**

Step 6 After uploading the certificate, click **Schedule Renewal Job**.

Step 7 Specify the date and time and then click **Set Renewal Time** to schedule the renewal job. The scheduled job appears in the page.

Schedule Certificate Renewal



2024-04-25

00:00

Set Renewal Time

Close

Use **Cancel Renewal Job** to cancel the scheduled job.

Configuring Data Retention

The Data Retention page lets you determine the number of days to keep event, issue, and metric data in the IoT FND database.



Note Data retention prunes events even if they have associated open issues.

To set IoT FND data retention:

Procedure

Step 1 Choose **ADMIN > System Management > Data Retention**.

Step 2 For each of the retention categories, specify the number of days to retain the data as specified in the table.

Table 1: Data Retention Field Allowable Maximum Values

Field	Minimum Values in Days	Maximum Values in Days	Default Values in Days
Keep Event data for	1	90	31
Keep Endpoint Firmware Operation data for	7	180	7
Keep Historical Dashboard data for	1	90	62
Keep Dashboard data for	1	7	7
Keep Historical Endpoint Metrics for	1	7	7
Keep Closed Issues data for	1	90	30

Field	Minimum Values in Days	Maximum Values in Days	Default Values in Days
Keep JobEngine data for	1	30	30
Keep Historical Router Statistics data for	1	90	30
Keep Device Network Statistics data for	1	7	7
Keep Service Provider down routers data for	1	31	31

Step 3 To save the maximum values, click the disk icon.

Step 4 To revert to default settings, click **Reset**.

Managing Licenses

This section is moved to a new location with improved user experience. For more information on managing licenses on Cisco IoT FND see, [Classic Licensing In Cisco IoT FND](#).

Cisco IoT FND Logs

Cisco IoT FND logs

Cisco IoT FND logs are systematic records of events, operations, and system activities generated by Cisco IoT FND and the managed devices. These logs capture information such as system status, configuration changes, user actions, communications, errors, and warnings. Cisco IoT FND logs are essential for:

- tracking the health and performance of the Cisco IoT network and devices
- diagnosing and resolving issues by reviewing historical events and error messages
- maintaining a secure environment by recording user activities and configuration changes for compliance purposes.

Cisco IoT FND provides various types of logs:

- system logs
- audit logs
- event logs

Benefits

- Cisco IoT FND logs provide better visibility into system activity, supporting proactive monitoring and ongoing operational health.

Prerequisites

- Logs require disk space. For example, with 5 million meters (8-hour reporting) and 5,000 routers (60-minute notifications), disk usage is about 7 MB/sec. Ensure your server has sufficient space for logs.

Restrictions

- Cisco IoT FND logs does not include separate logs from Cisco Fog Director. Cisco Fog Director has its own built-in logging mechanism that records information related to edge operations, such as application lifecycle events, local errors, device interactions, and communication with the central Cisco IoT FND server.
- During server startup, relevant ports are temporarily blocked at the firewall level to prevent processing until the server is fully initialized and ready to handle requests.

Configure log level settings

This task guides you to configure log level settings using Cisco IoT FND for various log level categories.

Procedure

- Step 1** Choose **ADMIN > System Management > Logging**.
- Step 2** Click **Log Level Settings** tab.
- Step 3** Check the check boxes of the logging categories that you would like to configure.
- Step 4** Choose either the **Debug** or **Informational** log level from the **Change Log Level to** drop-down menu.

Note

- To generate all possible logging messages, use the **Debug** level.
- To generate a subset of these messages, use the **Informational** level.
- When you first open Cisco IoT FND, the logging level for all categories is automatically set to **Informational** by default. If you change the logging level, for example, to **Debug** during your session, your custom settings are saved and used the next time you log in, as long as the IoT FND server has not been restarted.

- Step 5** If you'd like to debug particular devices, enter their Eids in the **Eids for debugging** text box.
- Step 6** Click **Go**.

Note

Once server.log gets too big, it is saved as an archive (often with a new name or number), and a fresh server.log file is created to continue logging new information.

- Step 7** Click the disk icon to save the configuration.
-

Example

What to do next

Download Cisco IoT FND Logs

To download logs:

Procedure

Step 1 Choose **ADMIN > System Management > Logging**.

Step 2 Click the **Download Logs** tab.

Step 3 Click the **Download Logs** button.

- When you click this button in a single-server deployment, IoT FND compresses the log files into a single zip file and adds an entry to the Download Logs pane with a link to the zip file.
- In IoT FND cluster deployments, when you click this button, the IoT FND server to which you are connected:
 - Compresses the log files on the server into a single zip file and adds an entry to the Download Logs pane with a link to the zip file.
 - Initiates the transfer of the log files in .zip format from the other servers to this server. As files become available, the server adds entries for these files to the Download Logs pane.

Step 4 To download a zip file locally, click its file name.

Tip

In a cluster environment, if you need to send log files to Cisco Support, ensure that you send the log files of all cluster servers.

Configuring Provisioning Settings

The Provisioning Settings page (**ADMIN > System Management > Provisioning Settings**) lets you configure the IoT FND URL, DHCPv4 Proxy Client, and DHCPv6 Proxy Client settings required for IoT FND to create tunnels between routers and ASRs/C8000 ([Provisioning Settings page](#)). For an example of tunnels as used in the IoT FND, see [Tunnel Provisioning Configuration Process](#) topic in the Managing Tunnel Provisioning chapter.

During Zero Touch Deployment (ZTD), you can add DHCP calls to the device configuration template for leased IP addresses.



Note For Red Hat Linux 7.x server installations, you must configure specific IPv4 and IPv6 addresses from the IoT FND Linux host server to which to bind DHCP IPv4 and IPv6 clients by setting the following values in IoT FND:

ADMIN > Provisioning Settings > DHCPv6 Proxy Client > Client Listen Address	Set the value to the IPv6 address of the interface to use to obtain IPv6 DHCP leases from the DHCP server. The default value is ":::". Change the default setting to an actual IPv6 address on the Linux host machine.
ADMIN > Provisioning Settings > DHCPv4 Proxy Client > Client Listen Address	Set the value to the IPv4 address of the interface to use to obtain IPv4 DHCP leases from the DHCP server. The default value is "0.0.0.0". Change the default setting to an actual IPv4 address on the Linux host machine.



Note To configure tunnel and proxy settings, you must be logged in either as root or as a user with Administrative Operations permissions.

Under **ADMIN > System Management > Provisioning Setting** page, the CSMP optimization settings help to configure the timeout to acquire lock when processing the csmg messages. By default, the timeout value is 5 seconds which can be configured between 1 to 30 seconds.



Note This csmg setting is applicable only for Oracle deployments.

If the timeout happens, then during registration, the following message is displayed in the server.log file.

```
"Failed to acquire lock for <Endpoint Eid> during registration.
Another Operation seems to be in progress."
```

During csmg notification, the following log message is displayed in the server.log file when handing csmg messages.

```
"Failed to acquire lock to update Endpoint Status. Another Operation seems to be in progress."
```

Provisioning Settings Page

Provisioning Process

IoT-FND URL:

Field Area Router uses this URL to register with IoT-FND after the tunnel is configured

Periodic Metrics URL:

Field Area Router uses this URL for reporting periodic metrics with IoT-FND

DHCPv6 Proxy Client

Server Address:

IPv6 address to send (or multicast) DHCPv6 messages to (can be multiple addresses, separated by commas)

Server Port:

Port to send (or multicast) DHCPv6 messages to

Client Listen Address:

IPv6 address to bind to, for sending and receiving DHCPv6 messages (for cluster deployment use cgms.properties file)

DHCPv4 Proxy Client

Server Address:

IPv4 address to send (or broadcast) DHCPv4 messages to (can be multiple addresses, separated by commas)

Server Port:

Port to send (or broadcast) DHCPv4 messages to

Client Listen Address:

IPv4 address to bind to, for sending and receiving DHCPv4 messages (for cluster deployment use cgms.properties file)

ZTD Properties

Select CA Type: ☐ PnP Install TrustPool ☐ Cisco Cloud Redirection ☒ Custom CA

SCEP URL:

URL of the CA server. The URL could point to a RA instead

CA Fingerprint:

Fingerprint of the issuing CA Server

Proxy Bootstrap Address:

TPS IPv4 address or Hostname

PNP Continue on Error: ☒ True ☐ False

PNP State Max Retries On Error:

PNP State Max Retries On Error - Enter a value between 1 and 5

*ZTD Settings in UI will take precedence over the same in cgms properties

CSMP Optimization Settings

CSMP Optimization Settings Enabled: ☒ True ☐ False

Time to wait for acquiring lock:

Min value is 1 sec and Max value is 30 secs

Configuring the IoT FND Server URL

The IoT FND URL is the URL that routers use to access with IoT FND after the tunnel is established. This URL is also accessed during periodic inventories. During ZTD, routers transition from accessing IoT FND through the TPS proxy to using this URL, which must be appropriate for use through the tunnel.

To configure the IoT FND URL:

Procedure

Step 1 Choose **ADMIN > System Management > Provisioning Settings**.

Step 2 In the **IoT FND URL** field, enter the URL of the IoT FND server.

The URL must use the HTTPS protocol and include the port number designated to receive registration requests. By default, the port number is 9121. For example:

```
https://nms.sgbu.example.com:9121
```

Step 3 Click **Save**.

Configuring DHCP Option 43 on Cisco IOS DHCP Server

To configure for IPv4, enter:

```
ip dhcp pool fnd-pool
network 192.0.2.0 255.255.255.0
default-router 192.0.2.1
option 43 ascii "5A;K4;B2;I192.0.2.215;J9125"

5 - DHCP type code 5
A - Active feature operation code
K4 - HTTP transport protocol
B2 - PnP/FND server IP address type is IPv4
I - 192.0.2.215 - PnP/FND server IP address
J9125 - Port number 9125
```

Configuring DHCPv4 Proxy Client

To configure DHCPv4 Proxy client settings:

Procedure

Step 1 Choose **ADMIN > System Management > Provisioning Settings**.

Step 2 Configure the DHCPv4 Proxy Client settings:

- a) In the **Server Address** field, enter the address of the DHCPv4 server that provides tunnel IP addresses.

Note

You can enter multiple addresses separated by commas. However, in most cases, you only need one server. IoT FND tries to get the tunnel IP addresses from the first server in the list. If it cannot, it moves to the next server in the list, and so on.

- b) In the **Server Port** field, enter the port address on the DHCP server to send DHCPv4 requests to.

Note

Do not change the default port number (67) unless you have configured your DHCP server to operate on a non-standard port.

- c) In the **Client Listen Address** field, enter the address to bind to for send and receive DHCPv4 messages.

Note

This is the address of the interface that the DHCP server uses to communicate with IoT FND. You can enter multiple backup addresses separated by commas.

Step 3 Click **Save**.

Configuring DHCPv6 Proxy Client

To configure DHCPv6 Proxy client settings:

Procedure

Step 1 Choose **ADMIN > System Management > Provisioning Settings**.

Step 2 Configure the DHCPv6 Proxy client settings:

- a) In the **Server Address** field, enter the address of the DHCPv6 server that provides tunnel IP addresses.

You can enter multiple addresses separated by commas. However, in most cases, you only need one server. IoT FND tries to get the tunnel IP addresses using DHCP protocols. If it cannot, it goes to the next server in the list and so on.

- b) In the **Server Port** field, enter the port address on the DHCP server to send DHCPv6 requests.

Note

Do not change the default port number (547) unless you have configured your DHCP server to operate on a non-standard port.

- c) In the **Client Listen Address** field, enter the address to bind to for DHCPv6 send and receive messages.

This is the address of the interface that the DHCP server uses to communicate with IoT FND. You can enter multiple backup addresses separated by commas.

Tip

For IoT FND installations where the host has multiple interfaces, the client sends requests using each listed source address. The default values, "0.0.0.0" (IPv4) and ":::" (IPv6), cause the client to send requests out each interface. Usually, one interface faces the DHCP server(s). In these installations, setting the **Client Listen Address** field to the IP address of the facing interface sends all client requests out that interface.

Step 3 Click **Save**.

Configuring Server Settings

The Server Settings page (**ADMIN > System Management > Server Settings**) lets you view and manage server settings.

Configuring Download Log Settings



Note Configuring download log settings is only required for IoT FND cluster setup.

The Download Logs page lets you configure the Keystore settings.

To configure download log settings:

Procedure

Step 1 Choose **ADMIN > System Management > Server Settings**.

Step 2 Click the **Download Logs** tab.

Step 3 Configure these settings:

Table 2: Keystore Settings

Field	Description
Keystore Filename	Click Upload Keystore File to upload a Keystore file with the public key of the X.509 certificate that IoT FND uses. You can reuse the same Keystore file.
Keystore Password	Enter the password that IoT FND uses to access the Keystore file on start up.
Confirm Keystore Password	
FTP Password	Enter the FTP password.
Confirm FTP Password	

Step 4 To save the configuration, click the disk icon.

Configuring Web Sessions

The Web Sessions page lets you specify the number of timeout seconds after which IoT FND terminates web sessions and logs users out.

To configure web session timeout:

Procedure

Step 1 Choose **ADMIN > System Management > Server Settings**.

Step 2 Click the **Web Session** tab.

Step 3 Enter the number of timeout seconds.
The valid values are 0–86400 (24 hours).

Note

If a web session is idle for the specified amount of time, IoT FND terminates the session and logs the user out.

Step 4 To save the configuration, click the disk icon.

Configuring Device Down Timeouts

The **Server Settings** page allows you to configure the device down timeout globally for head-end routers (ASR, C8000) and other devices that are managed by IoT FND such as routers (CGR1000, IR800, IR8100,), endpoints, and gateways. On reaching the specified device down timeout interval, the devices move to *Down* state in the IoT FND GUI based on the last heard value from the device (must be greater than the down timeout value) and the tunnel interface state. If the tunnel interface that is associated with the device is *Down* as well, then devices are marked *Down* in IoT FND GUI. Otherwise, IoT FND must wait until the tunnel interface goes *Down* to mark the device as *Down* in IoT FND GUI.

From the Device Configuration page (**CONFIG > DEVICE CONFIGURATION**), you can configure the device downtime for a specific router or endpoint configuration group. For more information, refer to [Configuring Mark-Down Timer](#)



Note For HER, you can set the device down timeout only in the Server Settings page.

Device status changes to *Up* when IoT FND detects any of the following:

- Periodic inventory notifications
- Events
- Manual metric refreshes
- Device registrations

To configure device down timeout settings:

Procedure

Step 1 Choose **ADMIN > System Management > Server Settings**.

Step 2 Click the **Device Down Timeouts** tab.

Note

The device down timeout value must be greater than the corresponding polling intervals. For example, if the polling interval for routers is 30 minutes (1800 seconds), then the value in the Mark Routers Down After (secs) field must be 1801 or greater.

Step 3 Click the disk icon to save the configuration.

Configuring Billing Period Settings

IoT FND lets you configure the start day of the monthly billing periods for cellular and Ethernet (satellite) services.

To configure the billing period settings:

Procedure

- Step 1** Choose **ADMIN > System Management > Server Settings**.
- Step 2** Click the **Billing Period Settings** tab.
- Step 3** Enter the starting days for the cellular and Ethernet billing periods.
- Step 4** From the drop-down menu, choose the time zone for the billing period.
- Step 5** To save the configuration, click the disk icon.

RPL tree settings

The RPL tree routing table is generated using the CSMP messages from the Mesh nodes. The data that is obtained from the mesh nodes is often outdated. The solution for this issue is to use the RPL tree routing data from FAR which is more up to date.

- [RPL Tree Update from Mesh Nodes](#)
- [RPL Tree Update from Routers](#)

RPL tree updates from mesh nodes

The default RPL tree update is always set to `Mesh Nodes`. This is a global setting for the entire Cisco IoT FND system.

RPL data is reported to the Cisco IoT FND by the mesh nodes as part of `IPRoute` and `IPRouteRPLMetrics` during the periodic inventory reporting.

Global RPL tree settings for entire Cisco IoT FND

The screenshot shows the Cisco IoT Field Network Director (FND) configuration interface. The top navigation bar includes 'DASHBOARD', 'DEVICES', 'OPERATIONS', 'CONFIG', and 'ADMIN'. The breadcrumb trail is 'ADMIN > SYSTEM MANAGEMENT > SERVER SETTINGS'. The 'RPL Tree Settings' tab is active. The configuration area contains three settings: 'Enable RPL tree update from' with radio buttons for 'Mesh Nodes' (selected) and 'Routers'; 'Number of Periodic Notifications between RPL Tree Polls' with a value of 8; and 'Maximum Time between RPL Tree Polls (minutes)' with a value of 480. A 'Save' button is located at the bottom right of the settings area.

Table 3: Global RPL tree settings for Cisco IoT FND

Field	Description
Enable RPL tree update from	Select Routers. Note By default, Mesh Nodes is selected.
Number of Periodic Notifications between RPL Tree Polls	Number of periodic notification from CGR between each RPL pull.
Maximum time between RPL Tree Polls in minutes	Maximum time Cisco IoT FND waits to pull RPL from a CGR for the associated PAN.

RPL tree update from routers

When mesh node data is outdated, the RPL tree from FAR provides the most current information. As the RPL tree is not pushed via periodic notifications, Cisco IoT FND gets this data at intervals configured through the **Device Configuration Group** properties.

Cisco IoT FND determines its RPL tree polling frequency based on periodic notifications, configured to poll FAR for updates after every 'N' such notifications. In case any periodic notifications are missed, the RPL tree is fetched from FAR after a maximum time threshold is reached.

Because FAR polls data at a much higher frequency than individual mesh nodes, its RPL data offers a more accurate and real-time snapshot of the entire Personal Area Network (PAN). Cisco IoT FND obtains the RPL tree for the associated PAN by executing the **show rpl dag 1 itable** command on the CGR.

Device Configuration Group Properties

Table 4: Device configuration group properties

Field	Description
RplTreePullingCycle	The number of periodic notification intervals. Note The default maximum number of RplTreePullingCycle is 8.
RplTreePullingMaxTime	The maximum time interval between the pulls in minutes. Note The default maximum time between pulls is 480 minutes (8 * 60).

When processing a periodic notification event, if either of these [thresholds](#) have passed, then Cisco IoT FND starts RPL tree retrieval from FAR.

The RPL pull times can be configured to each CGR configuration group as shown in the [Device Configuration Group Properties](#). For the settings to take effect, the Global Settings must be set to `Routers`, See [Global RPLTree Settings for Entire FND](#).

RPL tree retrieval

Cisco IoT FND currently collects the following information from CGR as part of RPL tree data:

- Node IP address
- Next hop IP address
- Number of parents
- Number of hops from root node
- ETX for path
- ETX for link
- Forward RSSI
- Reverse RSSI



Note No changes are required on FAR configuration when RPL updates setting is changed to routers or vice versa. If changed, Cisco FND automatically schedules for gathering the RPL updates from FARs.

Configure RPL tree polling

Use this task to configure RPL tree polling.

Before you begin



Note

- RPL tree polls are triggered by router periodic notification events, but the RPL tree itself is not pushed automatically.

Therefore, Cisco IoT FND must explicitly poll for the RPL tree at the configured intervals. You can configure both the RPL tree polling cycle with the number of periodic notifications between polls and the maximum time allowed between these polls.

Procedure

Step 1 Choose **ADMIN > System Management > Server Settings**.

Step 2 Choose **RPL Tree Settings** tab.

Step 3 Click **Mesh Nodes** or **Routers** radio button in **Enable RPL tree update from** option to receive the RPL tree update from the specific devices at specified intervals.

Note

- The **Mesh Nodes** radio button is ON, by default. The **Mesh Nodes** option in the **RPL Tree Settings** tab ensures proper functionality of the L+G endpoints graph.

Step 4 Enter the number of events that pass between RPL tree polling intervals in the **Number of Periodic Notifications between RPL Tree Polls** field for Router polling.

Note

The default value is eight. If thresholds are exceeded during periodic notification events, Cisco IoT FND performs an RPL tree poll.

Step 5 Enter the maximum amount of time between tree polls in the **Maximum Time between RPL Tree (minutes)** field in minutes,

Note

The default value is 480 minutes (8 hours).

Step 6 Click the disk icon to save configuration.

Configure the Issue Status Bar

The Issue Status bar displays issues by device type (as set in user preferences) and severity level in the lower-left browser frame.

To enable the Issue Status bar and configure the refresh interval:

Procedure

-
- Step 1** Choose **ADMIN > System Management > Server Settings > Issue Settings**.
- Step 2** To display the Issue status bar in the browser frame, check the **Enable/Disable Status Bar** > check box.
- Step 3** In the Issue **Status Bar Refresh Interval (seconds)** field, enter a refresh value in seconds.
The valid values are 30 secs (default) to 300 secs (5 minutes).
- Step 4** In the Certificate Expiry Threshold (days) field for all supported routers or a Cisco IoT FND application server, enter a value in days.
The valid value is 180 days (default) to 365 days.

Note

When the configured Certificate Expiry Threshold default date is met, a Major event, certificateExpiration, is created. When the Certificate has expired (>180 days), a Critical event, certificateExpired, is created.

Manage the Syslog

When Cisco IoT FND receives device events, it stores them in its database and sends syslog messages to a syslog server that allows third-party application integration.



Note The syslog server receives only the Cisco IoT FND device events (listed on Operations > Events page) and not the other Cisco IoT FND application logs in the server.log.

To configure Syslog forwarding:

Procedure

-
- Step 1** Choose **ADMIN > System Management > Syslog Settings**.
- Step 2** In the **Syslog Server IP Address** field, enter the IP address of the Syslog server.
- Step 3** In the **Syslog Server Port Number** field, enter the port number (default is 514) over which to receive device events.
- Click **Enable Syslog Sending Events** to enable message forwarding to the Syslog server.
 - Click **Disable Syslog Sending Events** to disable message forwarding to the Syslog server.

For Cisco IoT FND cluster solutions, each server in the cluster sends events to the same Syslog server.

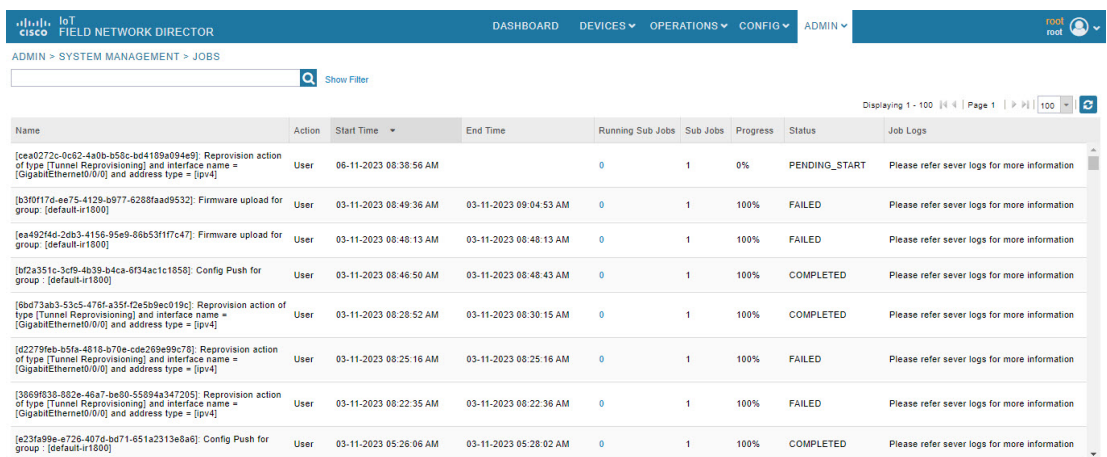
View Jobs

The user triggered jobs in Cisco IoT FND are displayed in the Jobs page. The information about the jobs and their sub jobs are stored in the database in order to ensure that jobs are not lost in case of system restart or failure. Cisco IoT FND allows you to monitor and respond to job scheduling events, such as job completion or failure. The status of the jobs of Cisco IoT FND such as config push, firmware upload and install, and reprovisioning can be seen in the Jobs page. This Jobs page provides a detailed summary of the jobs along with their respective sub jobs.

The supported job types are add/remove/export device, update statuses, change properties, add/remove labels (bulk operation), add/update/remove assets, upload firmware image to devices, install firmware image on devices, tunnel/factory re-provisioning, config push, and export events/dashboard dashlet data.

To view the jobs:

- Choose **ADMIN > SYSTEM MANAGEMENT > JOBS**. Cisco IoT FND displays the Jobs page.



Name	Action	Start Time	End Time	Running Sub Jobs	Sub Jobs	Progress	Status	Job Logs
[ceae0272c-0c62-4a0b-b50c-bd4189a094e9]: Reprovision action of type [Tunnel Reprovisioning] and interface name = [GigabitEthernet0/0/0] and address type = [ipv4]	User	06-11-2023 08:38:56 AM		0	1	0%	PENDING_START	Please refer sever logs for more information
[b3f0f17d-ee75-4129-b977-6288faad9532]: Firmware upload for group : [default-ir1800]	User	03-11-2023 08:49:36 AM	03-11-2023 09:04:53 AM	0	1	100%	FAILED	Please refer sever logs for more information
[ea492f4d-2db3-4156-95e0-86b53f1f7c47]: Firmware upload for group : [default-ir1800]	User	03-11-2023 08:48:13 AM	03-11-2023 08:48:13 AM	0	1	100%	FAILED	Please refer sever logs for more information
[b2a351c-3c09-4b39-b4ca-6f34ac1c1850]: Config Push for group : [default-ir1800]	User	03-11-2023 08:46:50 AM	03-11-2023 08:48:43 AM	0	1	100%	COMPLETED	Please refer sever logs for more information
[8bd73ab3-53c5-478f-a35f-72a5b9ec019c]: Reprovision action of type [Tunnel Reprovisioning] and interface name = [GigabitEthernet0/0/0] and address type = [ipv4]	User	03-11-2023 08:28:52 AM	03-11-2023 08:30:15 AM	0	1	100%	COMPLETED	Please refer sever logs for more information
[d2279fb-b5fa-4918-b70e-cde269e99c78]: Reprovision action of type [Tunnel Reprovisioning] and interface name = [GigabitEthernet0/0/0] and address type = [ipv4]	User	03-11-2023 08:25:16 AM	03-11-2023 08:25:16 AM	0	1	100%	FAILED	Please refer sever logs for more information
[3669f38-882e-46a7-be80-55894a347205]: Reprovision action of type [Tunnel Reprovisioning] and interface name = [GigabitEthernet0/0/0] and address type = [ipv4]	User	03-11-2023 08:22:35 AM	03-11-2023 08:22:36 AM	0	1	100%	FAILED	Please refer sever logs for more information
[e23fa99e-a726-407d-bd71-651a2313e8a8]: Config Push for group : [default-ir1800]	User	03-11-2023 05:26:06 AM	03-11-2023 05:28:02 AM	0	1	100%	COMPLETED	Please refer sever logs for more information



Note

- The logs are not displayed for tunnel provisioning, config push, and firware upgrade. You can view the server logs for more information.
- The completed or failed jobs show 0 under running sub jobs.
- The jobs are displayed in the Jobs page as per their retention time.
- Clicking on Running Sub Jobs opens up the pop-up window to show the status of the running jobs.

×

☒ Auto Refresh

Name	Status	Start Time	End Time
324	SUCCESS	12-10-2023 04:11:17 AM	12-10-2023 04:11:17 AM

⏪ ⏩ Page 1 of 1 50 🔄

Displaying 1 - 1 of 1

×

- The filter allows you to filter jobs based on name, action, sub jobs, and status. To filter the job list using column filtering, click show filter to insert the search string. For example, click Name from the drop down and provide the search string. Click + icon to add the job selected and click search icon to display the search results.