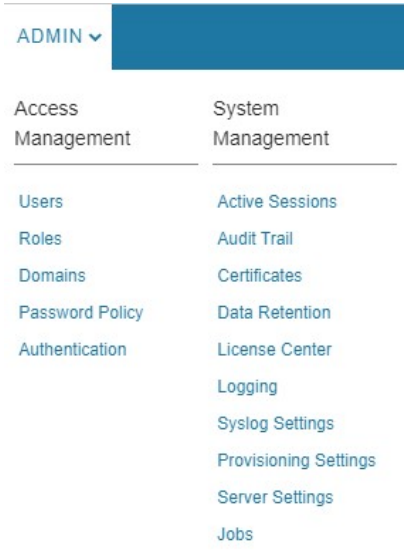
Managing System Settings

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.



• Viewing Jobs, on page 25

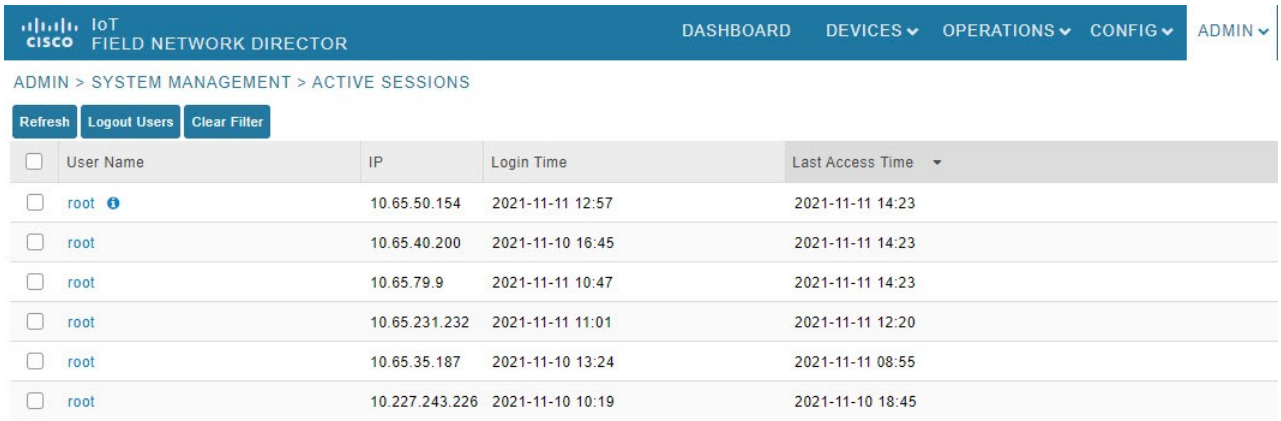
Managing Active Sessions

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

Viewing Active Sessions

To view active user sessions:

Choose **ADMIN** > **System Management** > **Active Sessions**.
IoT FND displays the Active Sessions page.



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:

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.

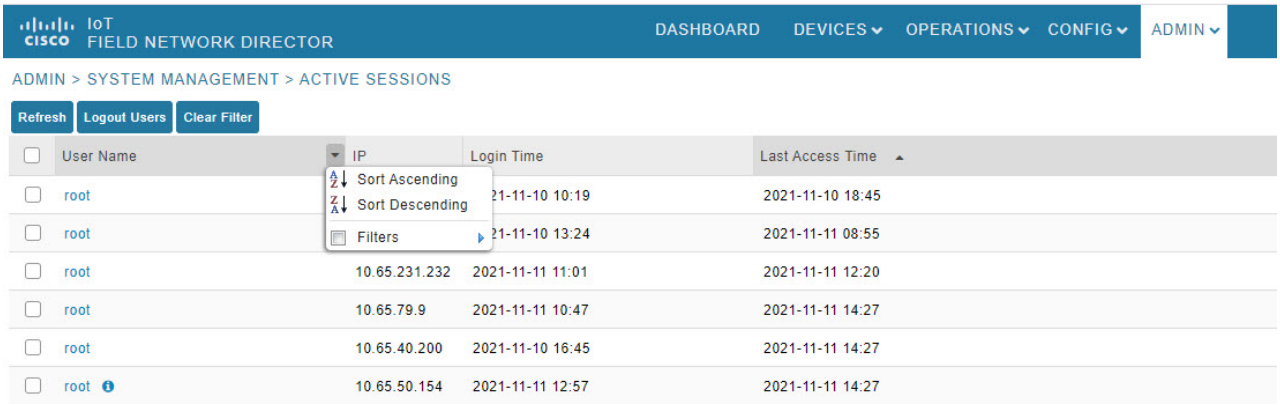
Step 4 Click **Yes** to confirm logout of the users.

Filtering the Active Sessions List

To filter the Active Sessions list using column filtering:

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.



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

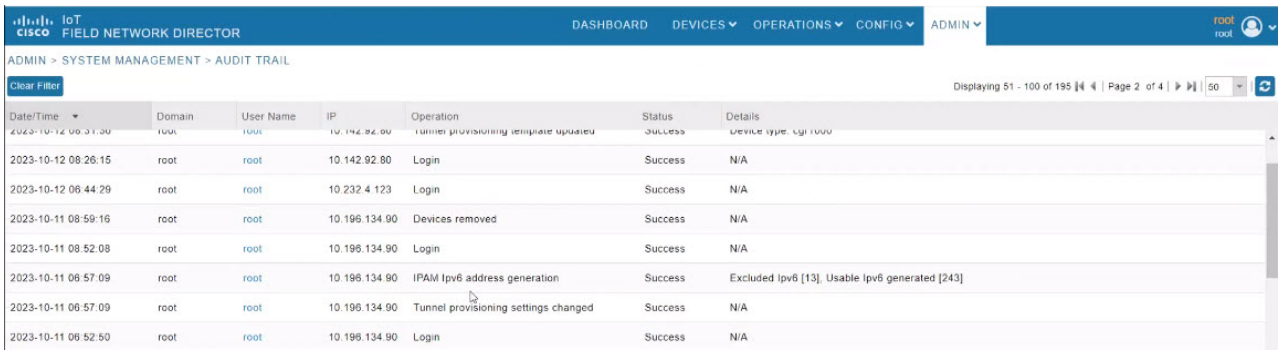
Tip To remove the filter, from the User Name drop-down menu, clear the **Filters** check box or click **Clear Filter**.

Displaying the Audit Trail

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

To display the Audit Trail:

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



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. • 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:

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)**.

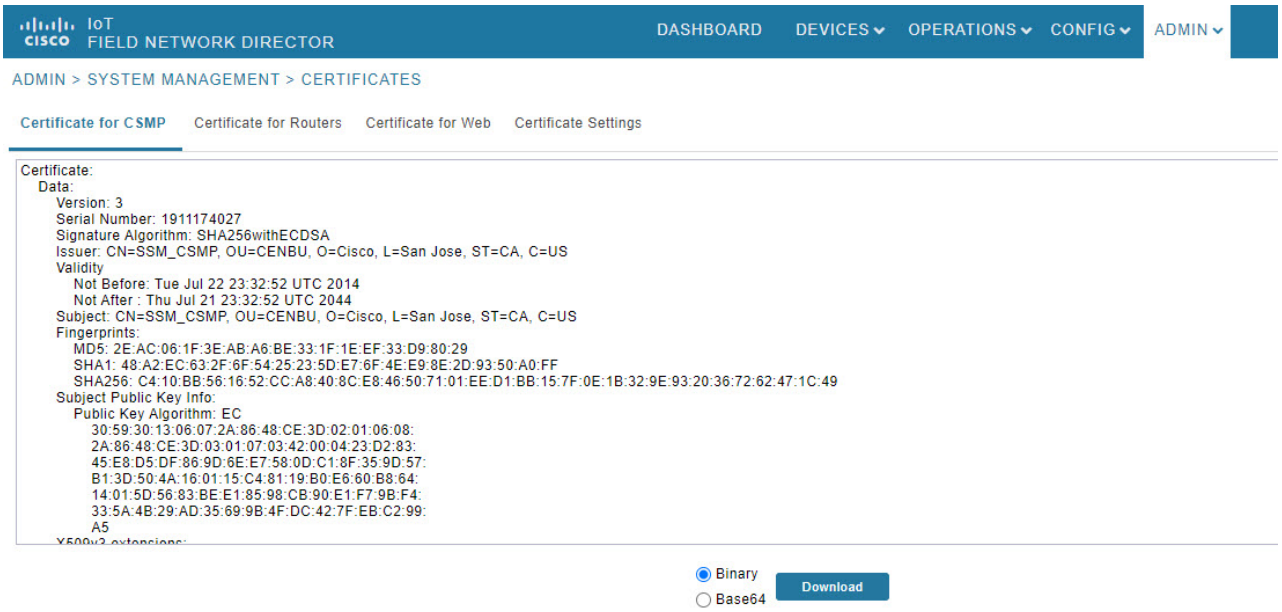
Managing Certificates

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:

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

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



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:

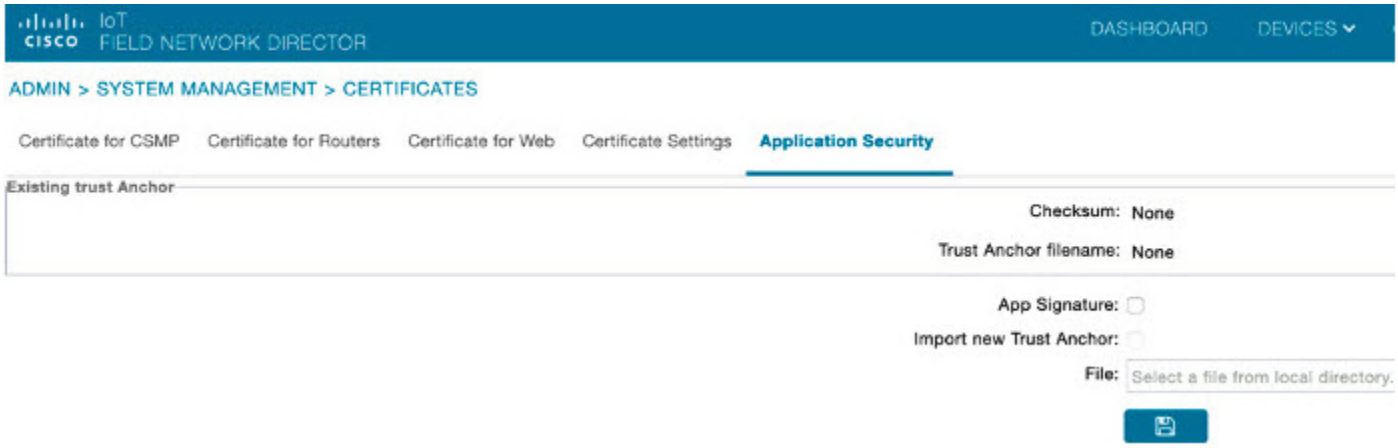
Step 1 Choose **ADMIN** > **System Management** > **Certificates**.

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.



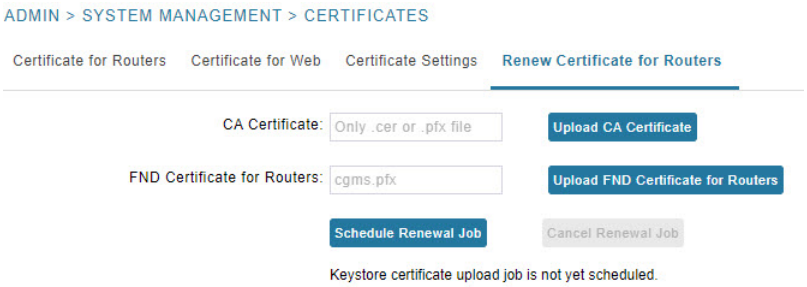
CGMS Certificate Renewal for Routers

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:

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

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

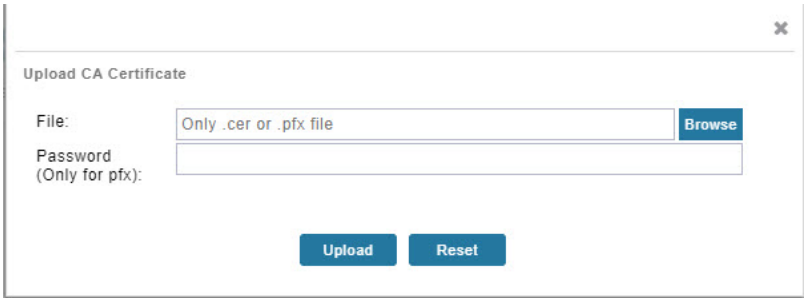


Step 3 Click either **Upload CA Certificate** or **Upload FND Certificate for Routers** to upload a CA or CGMS certificate.

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

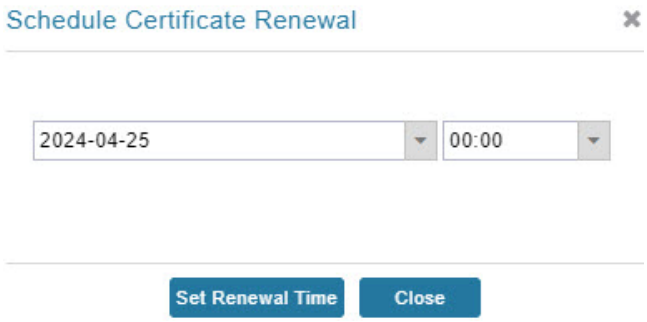
Step 4 Browse and select a valid CGMS or CA certificate in either (`.cer`) or (`.pfx`) format.

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



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.



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:

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
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

The License Center page, **ADMIN** > **System Management** > **License Center**, lets you view and manage license files.

Note IoT FND performs license enforcement when importing devices. If you add licenses, IoT FND only allows the permitted number of devices to be imported, as defined in the licenses.

Without licenses, IoT FND allows only 3 routers and 100 mesh endpoints.

Adding License Files

To add a license file:

Step 1 Choose **ADMIN** > **System Management** > **License Center**.

Step 2 Click **Classic Licenses**.

Step 3 Click **Add**. An **Upload License File** window appears.

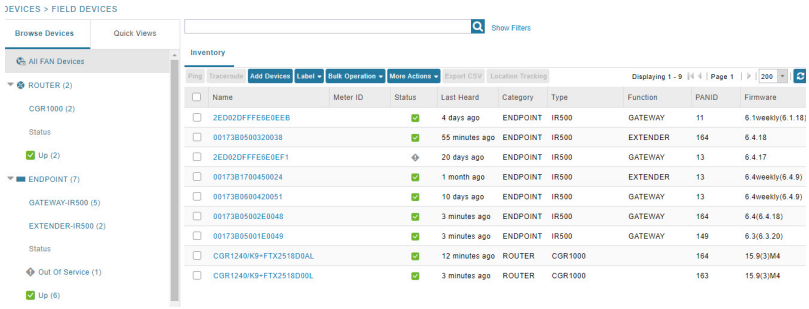
Step 4 Click **Browse** to locate the license file and then click **Open**.

Step 5 Click **Upload**.

Note The license is consumed only by devices in the Managed device category. The devices in OOS device category do not consume license.

Step 6 Click **Reset** to cancel the selected file and search for another file.

Note If you import more devices that your Classic License allows, the import process will not fail. Any devices imported beyond the license limit will be marked as 'Unmanaged' and listed under Status in the Browse Devices panel. No other license types other than Classic Licenses support this capability.



Viewing License Summary

To view IoT FND license summary:

Step 1 Choose **ADMIN** > **System Management** > **License Center**.

Step 2 Click **License Summary**. A list of devices with their license information is displayed.

Note The License Summary page displays the license information for devices in the Managed status only. The OOS devices are not displayed on this page, as they do not consume the license.

For every license, IoT FND displays the information as described in the table.

Note IR500s use mesh endpoint licenses and require no special license.

Table 2: Device License Summary Information

Field	Description
Package Name	Name of license package.
CGR1K Licenses Consumed / Total	Lists the number of CGR1K devices currently active in the network and the maximum number of CGR1000s supported by the license.
IR800 Licenses Consumed / Total	Lists the number of IR800 (IR809 and IR829) devices currently active in the network and the maximum number of IR800 devices supported by the license.
LORAWAN Licenses Consumed / Total	Lists the number of Cisco interface modules for LoRaWAN devices currently active in the network and the maximum number of Cisco interface modules for LoRaWAN devices that are supported by the license.
IR500 Licenses Consumed / Total	Lists the number of IR509 devices currently active in the network and the maximum number of IR509 devices supported by the license.
ENDPOINT Licenses Consumed / Total	Lists the number of endpoint devices currently active in the network and the maximum number of endpoint devices supported by the license.
CELL_ENDPOINT Licenses Consumed / Total	Lists the number of cell_endpoint devices currently active in the network and the maximum number of cell_endpoint devices supported by the license.
IR8100 Licenses Consumed / Total	Lists the number of IR8100 devices currently active in the network and the maximum number of IR8100 devices supported by the license.
Days Until Expiry	Number of days remaining until the license expires.

Table 3: Feature History

Feature Name	Release Information	Description

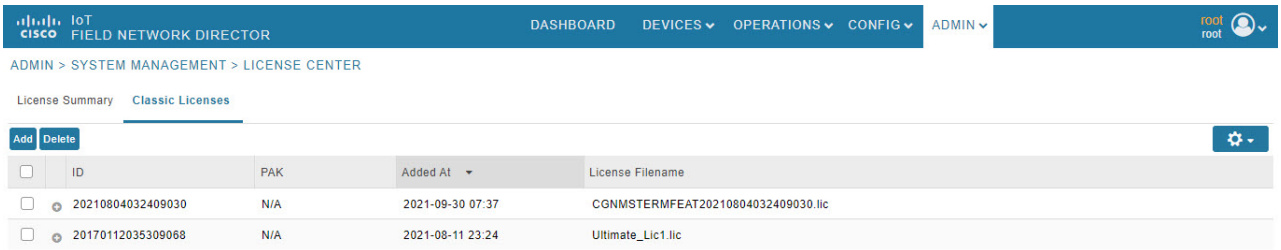
Enable 8140 Licensing	IoT FND 4.8	The licensing for device type IR8100 is now supported in FND. The license PID for IR8100 devices is IOTFND-IR8140. After adding the license, go to **ADMIN** > **System Management** > **License Center** > **License Summary** page to view the licenses consumed and total license count for IR8100 devices. It is also possible to allocate licenses for each domain. Go to **ADMIN** > **Access Management** > **Domains**. In the Edit Domain page, you can allocate licenses for the IR8100 devices.

Viewing License Files

To view IoT FND license files:

Step 1 Choose **ADMIN** > **System Management** > **License Center**.

Step 2 Click **Classic Licenses** to display details on all active licenses.



For every file, IoT FND displays the fields as described in the table:

Table 4: License File Fields

Field	Description
ID	License ID.
PAK	Number for issuing license fulfillment. Displays as N/A.
Added At	Date and time the license was added to IoT FND.
License Filename	Filename of the license.

Deleting the License Files

Note Ensure that you have access to license files before deleting existing license files. Without licenses, IoT FND only allows registration of 3 routers and 100 mesh endpoints.

To delete a single license or multiple license files:

Step 1 Choose **ADMIN** > **System Management** > **License Center**.

Step 2 Click **Classic Licenses**.

Step 3 Check the license file ID check box that you want to delete.

Step 4 Click **Delete**.

Note On deleting the license file, devices in Out of Service (OOS) status move to Unmanaged status. If license is added again, the devices move back to OOS status.

Step 5 Click **Yes** to confirm deletion or click **No** to cancel the action.

Managing Logs

This section explains about configuring and downloading logs.

Configuring Log Settings

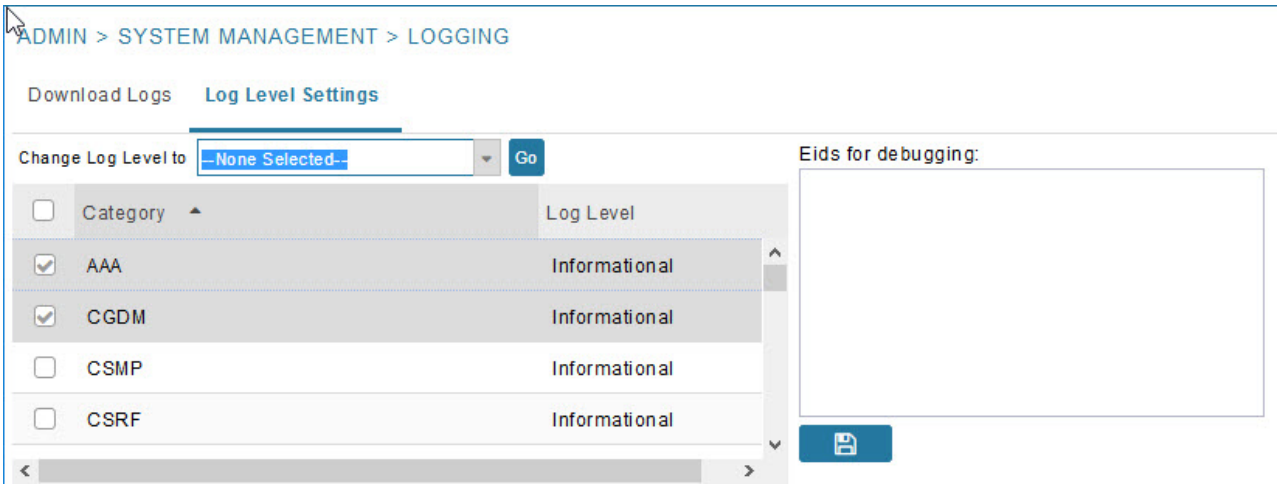
IoT FND lets you change the logging level for the various log categories and download the logs. Logs incur a certain amount of disk space. For example, for 5 million meters at an 8-hour reporting interval and 5000 routers at a 60-minute periodic inventory notification, disk consumption is approximately 7MB/sec. Ensure that your server has enough disk space to contain your logs.

To configure the logging level:

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

Step 2 Select **Log Level Settings**.

Step 3 Check the check boxes of all logging categories to configure.



Step 4 From the **Change Log Level** drop-down menu, choose the logging level setting (**Debug or Informational**).

- To generate all possible logging messages, use the **Debug** level.

Note Running the **Debug** logging category can impact performance.

- To generate a subset of these messages, use the **Informational** logging level.

Note The **Informational** logging level is the default for all categories when IoT FND opens. Custom logging level settings are retained between log-in sessions, but not after IoT FND restarts.

Step 5 To apply the configuration, click **Go**.

Note The server.log file is rotated based on size.

Step 6 Click the disk icon to save the configuration.

Downloading Logs

To download logs:

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 csmp messages. By default, the timeout value is 5 seconds which can be configured between 1 to 30 seconds.

Note This csmp setting is applicable only for Oracle deployments.

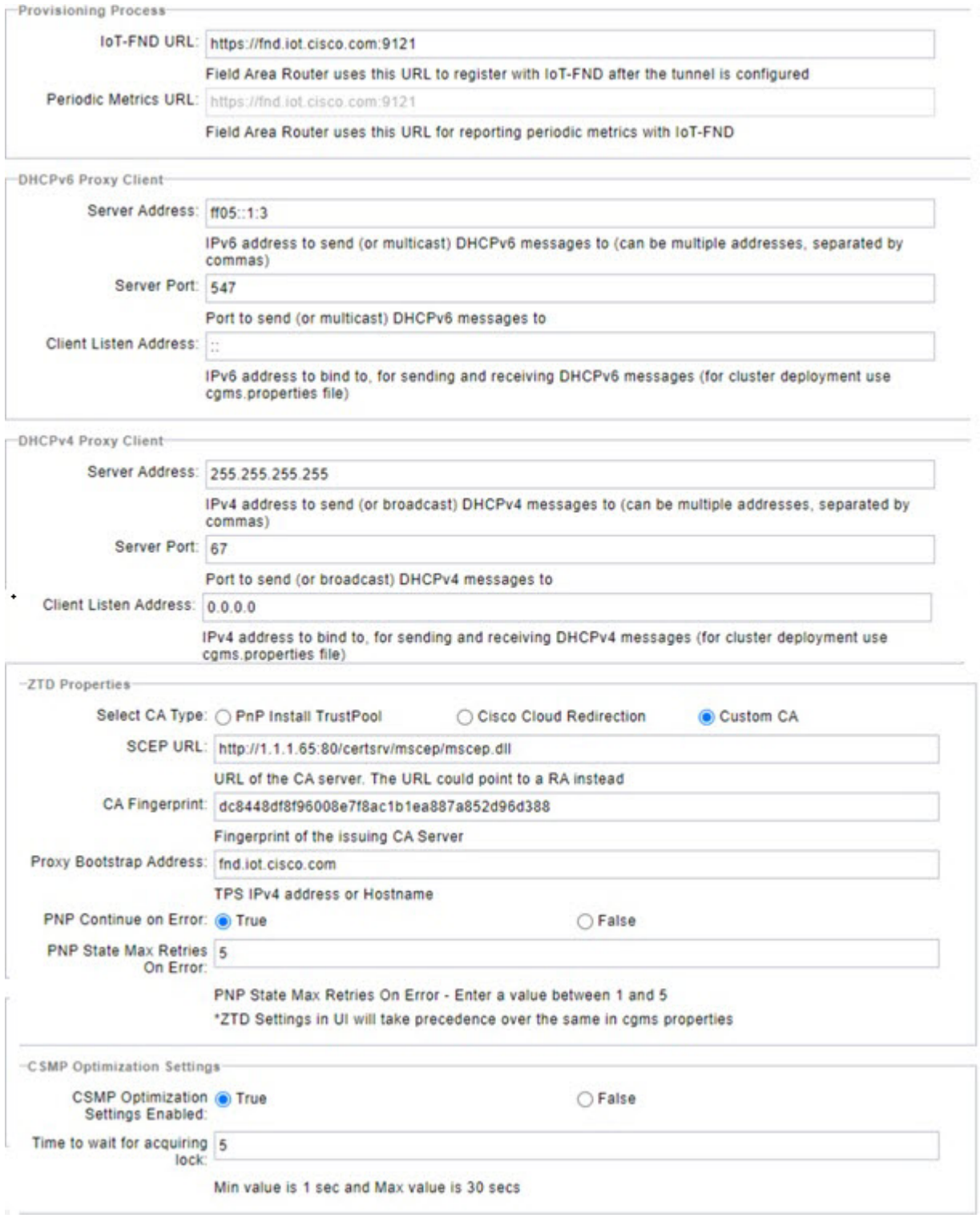
If the timeout happens, then during registration, the following message is displayed in the server.log file.

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

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

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

Provisioning Settings Page


Provisioning Process
IoT-FND URL: https://fnd.iot.cisco.com:9121
Field Area Router uses this URL to register with IoT-FND after the tunnel is configured
Periodic Metrics URL: https://fnd.iot.cisco.com:9121
Field Area Router uses this URL for reporting periodic metrics with IoT-FND
DHCPv6 Proxy Client
Server Address: ff05::1:3
IPv6 address to send (or multicast) DHCPv6 messages to (can be multiple addresses, separated by commas)
Server Port: 547
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: 255.255.255.255
IPv4 address to send (or broadcast) DHCPv4 messages to (can be multiple addresses, separated by commas)
Server Port: 67
Port to send (or broadcast) DHCPv4 messages to
Client Listen Address: 0.0.0.0
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: http://1.1.1.65:80/certsrv/mscep/mscep.dll
URL of the CA server. The URL could point to a RA instead
CA Fingerprint: dc8448df8f96008e7f8ac1b1ea887a852d96d388
Fingerprint of the issuing CA Server
Proxy Bootstrap Address: fnd.iot.cisco.com
TPS IPv4 address or Hostname
PNP Continue on Error: True False
PNP State Max Retries On Error: 5
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: 5
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:

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:

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:

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:

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

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

Step 3 Configure these settings:

Table 5: 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:

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.

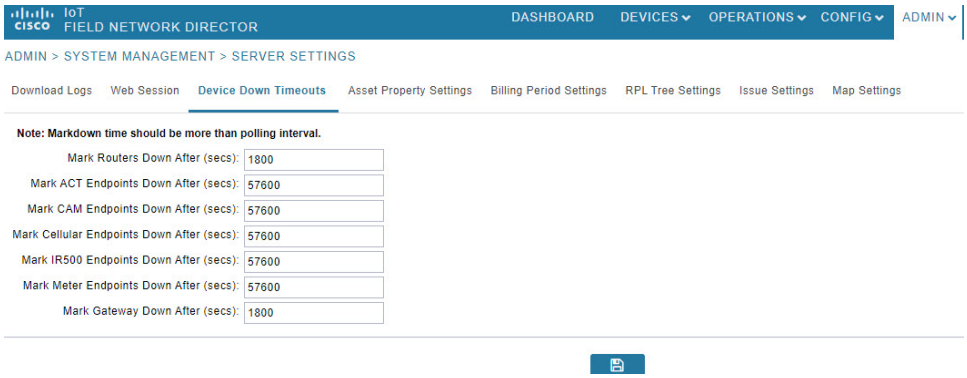
Device status changes to *Up* when IoT FND detects any of the following:

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

To configure device down timeout settings:

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:

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 proposed solution is to use the RPL tree routing data from FAR which is more up to date.

IoT FND uses the command below to fetch the RPL tree data:

```
show rpl dag 1 itable | xml
```

- RPL Tree Update from Mesh Nodes
- RPL Tree Update from Routers

RPL Tree Update from Mesh Nodes

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

Traditionally, the RPL data has been reported to the FND by the mesh nodes as part of `IPRoute` and `IPRouteRPLMetrics` during the periodic inventory reporting.

Global RPL Tree Settings for Entire FND

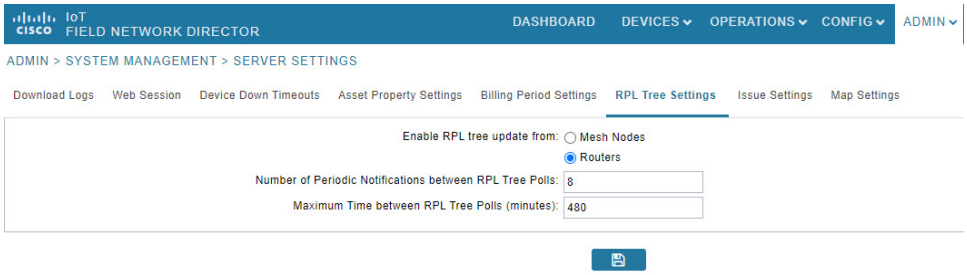


Table 6: Global RPL Tree Settings for Entire FND

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.

Field	Description
Maximum Time between RPL Tree Polls (minutes)	Maximum time FND waits to pull RPL from a CGR for the associated PAN.

RPL Tree Update from Routers

As the Mesh nodes data is often outdated, the proposed solution is to use the RPL tree routing from FAR, which is more up to date. The RPL tree is not pushed from the FAR with the periodic notification. Therefore, the FND explicitly needs to pull the RPL tree at regularly configured intervals based on the Device Configuration Group properties. The FND depends on the periodic notification to determine when to poll next for the RPL tree. The FND is configured to poll the FAR for RPL tree update after every "N" periodic notifications. At times, some periodic notifications are missed. If that happens, after an absolute maximum time value, the RPL tree is fetched from the FAR.

The FAR pulls at a much higher frequency than the mesh nodes. Therefore, the RPL data is more accurate and provides a snapshot of entire PAN at any given point in time. The FND invokes **show rpl dag 1 itable** command on the CGR to obtain the RPL tree for the associated PAN.

Device Configuration Group Properties

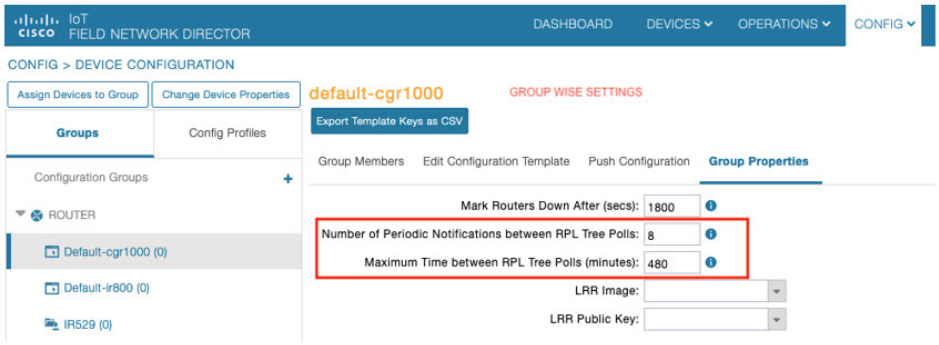


Table 7: Device Configuration Group Properties

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 Table 7: Device Configuration Group Properties have passed, then the 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'`, refer to Global RPLTree Settings for Entire FND.

RPL Tree Retrieval

The FND currently collects the following information from CGR as part of the 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. When changed, the FND automatically schedules for gathering the RPL updates from FARs.

Configuring RPL Tree Polling

RPL tree polls are derived from router periodic notification events. Since the RPL tree is not pushed from the router with the periodic notification event, IoT FND must explicitly poll for the RPL tree at the configured intervals. IoT FND lets you configure the RPL tree polling cycle (that is, how many periodic notification events occur between RPL tree polls), and set the maximum amount of time between tree polls.

To configure RPL tree polling settings:

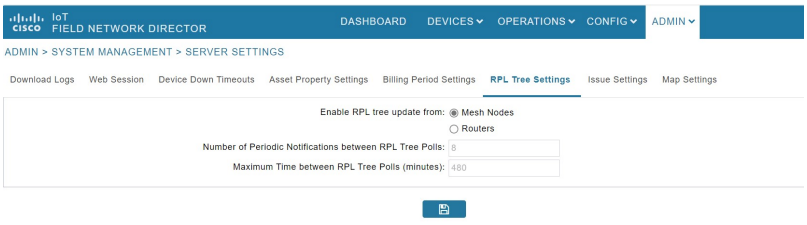
Step 1 Choose **ADMIN** > **System Management** > **Server Settings**.

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

Step 3 Choose the **Enable RPL tree update from** radio button for **Mesh Nodes** or **Routers** to receive the RPL tree update from those devices at the specified intervals.

Note By default, **Mesh Nodes** radio button is selected.

Note To make the L+G endpoints graph functionality work, ensure to select the **Mesh Nodes** option in the **RPL Tree Settings**.



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

Note The default value is 8. If thresholds are exceeded during periodic notification events, IoT FND performs a RPL tree poll.

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

Note The default value is 480 minutes (8 hours).

Step 6 To save the configuration, click the disk icon.

Configuring 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:

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 an 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.

Managing the Syslog

When 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 IoT FND device events (listed on Operations > Events page) and not the other IoT FND application logs in the server.log.

To configure Syslog forwarding:

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

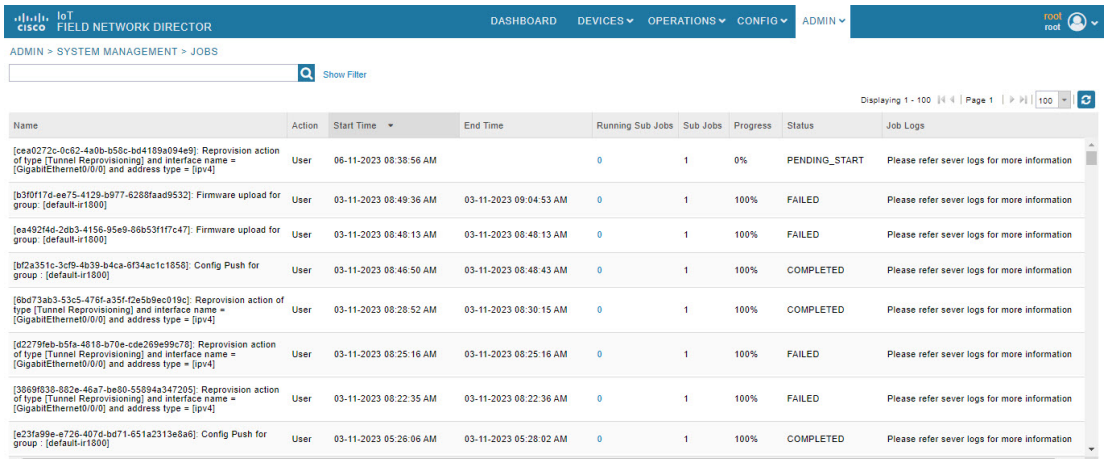
Viewing Jobs

The user triggered jobs in 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. IoT FND allows you to monitor and respond to job scheduling events, such as job completion or failure. The status of the jobs of IoT FND such as config push, firware 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:

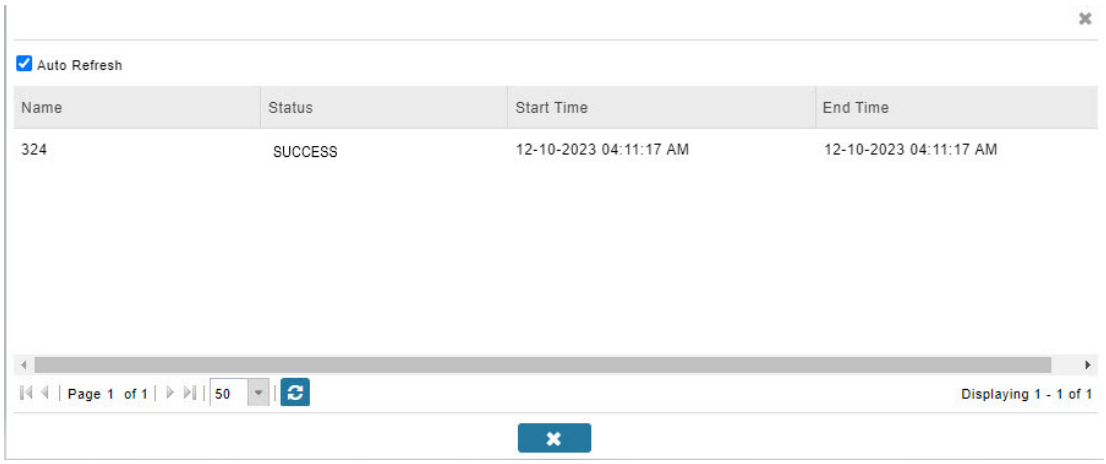
- Choose **ADMIN** > **SYSTEM MANAGEMENT** > **JOBS**. IoT FND displays the Jobs page.



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.



- 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.