

Manage 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.

- Managing Active Sessions, on page 1
- Google Snap to Roads, on page 3
- Configure the Google Maps API key, on page 4
- Displaying the Audit Trail, on page 4
- Managing Certificates, on page 6
- Data retention, on page 9
- Managing Licenses, on page 11
- Cisco IoT FND Logs, on page 11
- Configuring Provisioning Settings, on page 16
- Configuring Server Settings, on page 19
- Configure the Issue Status Bar, on page 25
- Manage the Syslog, on page 25
- View Jobs, on page 26

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**.

Cisco 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:

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.

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**.

Google Snap to Roads

Google Snap to Roads is a map visualization feature in Cisco IoT FND that uses the Google Roads API to associate a sequence of reported GPS positions with the most likely roads traveled.

GPS positions reported by a moving device might not align exactly with a road on the map. GPS signal conditions, sampling intervals, and measurement noise can cause the displayed route to appear beside the road or contain gaps and abrupt changes.

When Google Snap to Roads is enabled, Cisco IoT FND uses the reported latitude and longitude coordinates to obtain corresponding points aligned with the road geometry. Cisco IoT FND uses the returned points to display a road-aligned route on the map.

- The service evaluates a sequence of GPS positions rather than treating each position as an independent point.
- The displayed route follows the geometry of the road that the service determines was most likely traveled.
- The snapped route is an estimated representation and does not verify the route that the device actually traveled.

Factors that affect route accuracy

The accuracy of the snapped route depends on the quality and frequency of the GPS positions reported by the device. The service works best when consecutive positions are part of a continuous route and are located close to one another.

The displayed route might be less accurate under the following conditions:

- Consecutive GPS positions are far apart.
- GPS reporting is interrupted or contains large changes in location.
- Two or more roads run close together, such as parallel roads, service roads, or stacked highways.
- The device travels on a private, newly constructed, or unmapped road.
- The reported positions do not represent a continuous route.

Note Google recommends that consecutive GPS positions be no more than 300 metres apart for the best snapping results. Sparse or noisy position data can cause the service to select a road different from the one actually traveled.

Google Snap to Roads requires a valid Google Maps API key. To request a key, contact the designated Cisco support team or representative and provide the fully qualified domain name used to access the Cisco IoT FND application.

Configure the Google Maps API key

Configure the API key required to display Google Maps in Cisco IoT FND.

The API key is associated with the fully qualified domain name (FQDN) used to access the Cisco IoT FND application.

Before you begin

- Contact the designated Cisco support team or representative to request a Google Maps API key. Provide the FQDN used to access the Cisco IoT FND application.
- Use a Cisco IoT FND account that has permission to modify server settings.

Procedure

Step 1 Sign in to Cisco IoT FND.
Step 2 Choose **ADMIN** > **Server Settings** > **Map Settings**.
Step 3 Enter the API key in the **Google Map Key** field.
Step 4 Click the save icon.
Step 5 Choose **DEVICES** > **Field Devices**.
Step 6 Open the **Map** tab and verify that the map displays without an authorization error.

Maps functionality and Google Snap to Roads are available in Cisco IoT FND.

What to do next

If the map displays an authorization error, confirm that the FQDN used to access Cisco IoT FND was provided when the API key was requested. Contact the designated Cisco support team or representative if the error continues.

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**.

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.

Filter the Audit Trail list

Use the Audit Trail to locate and review specific system-management records.

Use search or column filtering to locate entries in the Audit Trail list.

Procedure

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

Step 2 Enter all or part of a value in the **Search** field to locate specific audit trail entries.

Cisco IoT FND filters the list and displays the matching entries. Clear the **Search** field to display all audit trail entries.

Step 3 From the **User Name** drop-down list, point to **Filters**, and enter all or part of a user name in the field that appears.

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



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

Managing Certificates

The **Certificates** page displays the certificates for CSMP (CoAP Simple Management Protocol), and web certificates used by Cisco 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**).

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-Oracle Deployment.

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.

View and export trusted certificates

Beginning with Cisco IoT FND Release 26.2.1, the **Trusted Certificates** tab displays certificate details in a table. The status icons help you identify valid, soon-to-expire, and expired certificates.

Before you begin

Enable the **New UI** toggle if it is off.

Procedure

Step 1 Choose **Admin** > **Certificates**.

Step 2 Click the **Trusted Certificates** tab.

The tab displays the number of certificates and the certificate table.

Step 3 Review the certificate details and status in the table.

The following table describes the displayed columns.

Table 1: Trusted Certificates table columns

Column	Description
Certificate Type	The certificate category, such as Web/Server or Router.
Alias	The name used to identify the certificate in its keystore.
Subject CN	The common name (CN) of the certificate subject.
Issuer CN	The common name (CN) of the authority or entity that issued the certificate.
SAN	The subject alternative names, such as DNS names, included in the certificate. The table displays N/A when no value is available.

Column	Description
Valid From	The date and time when the certificate becomes valid.
Expiration Date	The date and time when the certificate expires.
Status	An icon showing whether the certificate is valid, about to expire, or expired.
Usage Type	The service or function that uses the certificate, such as JBoss service or IoT FND service.
Serial Number	The serial number assigned to the certificate by its issuer.
Version	The X.509 version of the certificate.
Subject DN	The full distinguished name (DN) of the certificate subject.
Issuer DN	The full distinguished name (DN) of the certificate issuer.

The **Status** icons use these colors:

- Green: The certificate is valid.
- Amber: The certificate is about to expire.
- Red: The certificate has expired.

Use **Rows per page** and the page controls to navigate a longer list.

Step 4 To update the displayed information, click **Refresh**.

The **As of** timestamp shows when the list was last refreshed.

Step 5 To export certificate information, click **Export**.

Cisco IoT FND downloads a comma-separated values (CSV) file with the certificate table columns. The CSV contains text values in the Status column rather than the colored icons displayed in the user interface.

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.

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.

Data retention

The **Data Retention** page helps you control how long the historical data is kept in the application database and when old records are purged. It's primarily used to manage database growth, keep the system responsive, and align with your organization's compliance policies. Here are the major data categories that can be retained or pruned.

- Events data: Historical event records and their state transitions.
- Fimware operation data
- Historical dashboard data
- Historical endpoint metrics
- Closed issues
- JobEngine data
- Historical metrics statistics
- Service provider down routers data

Feature name	Release info	Description
Manage data retention of open issues	Cisco IoT FND Release 5.1	Cisco IoT FND retrieves open issues and prunes them based on a configurable retention period. By default, open issues are retained for 31 days, and older items are automatically removed. You can control this period using the **Keep Open Issues data for** field.

Configure data retention

This task guides you to configure data retention metrics on your Cisco IoT FND.

The **Data Retention** page lets you determine the number of days to retain the events, issues, and metrics related data in the Cisco IoT FND database.



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

Here are the instructions to set Cisco IoT FND data retention:

Procedure

Step 1 From the Cisco IoT FND menubar, 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 2: Data Retention field permitted 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	31
Keep Job Engine data for	1	30	7
Keep Historical Router Statistics data for	1	90	30
Keep Device Network Statistics data for	1	7	7
Keep Open Issues data for	1	90	31
Keep Service Provider down routers data for	1	31	31

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

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

You've successfully configured data retention on Cisco IoT FND.

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

Table 3: Feature history

Feature name	Release information	Description
Feature-Specific and Heartbeat Logs	Cisco IoT FND Release 5.1	In Cisco IoT FND, errors, startup events, and heartbeat logs are recorded in dedicated logs instead of a single consolidated server log. A predefined list of feature-specific logs provides quick access, allowing you to efficiently monitor system activity.

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
- hearbeat logs
- feature-specific logs

Benefits

- Cisco IoT FND logs provide better visibility into system activity, supporting proactive monitoring and ongoing operational health.
- Feature-specific logs make it easier to identify and resolve issues by separating errors, startup events, and heartbeat messages into dedicated log files.
- The predefined list of log categories improves accessibility and organization, helps you quickly locate and review relevant logs.
- The segregation of heartbeat messages prevents excessive log volume in main server logs, making analysis more efficient in large-scale deployments.

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.
- To view feature-specific logs and heartbeat logs, your Cisco IoT FND should be running Cisco IoT FND Release 5.1 and later releases.

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.

Configue 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.

You've configured log level settings.

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.

Configure feature specific logs

This task guides you to configure feature-specific logs using Cisco IoT FND.

Procedure

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

Step 2 Click **Log Level Settings** tab.

Step 3 Select **Feature Specific Log** from the **Select Log Type** drop-down list. Here's a list of feature-specific logs:

Feature Category Name	Description
Pnp Bootstrapping	Includes WSMA and CGNA, Router bootstrapping, firmware, template.log name (pnp_bootstrapping.log)
Tunnel Provisioning	Includes WSMA and CGNA, DHCP, reprovisioning, tunnel provisioning, templates.log name (tunnel_provisioning.log)
Registration	Includes WSMA and CGNA, CSMP, Configuration, Snmp, generic endpoint, LWM2M, NETCONF, reprovision, websocket, templates.log name (registration.log)
Periodic Metrics Collection	WSMA and CGNA, CSMP, Generic endpoint, LWM2M, metrics, NETCONF, websocket, log name (periodic_metrics_collection.log)
Config Push	WSMA and CGNA,CSMP, configuration, job engine, LWM2M, websocket, template. log name (config_push.log)
Firmware Upgrade	WSMA and CGNA, CSMP, Firmware, job engine, LWM2M, software patch service, websocket.log name (firmware_upgrade.log)

Step 4 Check the **Include System Log Category** check box adjacent to each feature category if you want to include all the system logs.

Step 5 Click **Enable** in the **Actions** column.

Note

- If the **Enable** button is visible, logging is stopped and can be resumed by clicking it; if the **disable** button is visible, logging is active and can be halted by clicking it.
- For all the logs that you want Cisco IoT FND to display at a feature-specific level, you need to enable the debug logs for the corresponding category.

  The respective category is displayed in the info button for each feature.

Step 6 Click **Download** in the **Actions** column to download the feature specific logs.

Note The downloadable logs appear in the **File** column.

Step 7 Select **Feature Specific Log** from the **Select Log Type** drop-down list.

Step 8 In the desired **Feature Category Name**, click **Enable**.

Step 9 Click **Download** once the logs are available after processing.

You've downloaded feature specific logs.

Configure heartbeat logs

This task guides you to configure heartbeat logs using Cisco IoT FND.

Procedure

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

Step 2 Click **Log Level Settings** tab.

Step 3 Select **Heartbeat log** from the **Select Log Type** drop-down list.

Step 4 Check the **Log router heartbeat in server.log** if you want to include the heartbeat logs in the server.log.

Step 5 If you don't enable **Log router heartbeat in server.log**, the logs are saved in heartbeat.log.

Step 6 Click the **Save** icon.

Step 7 Click **Download Logs** tab and wait for the logs to process and appear.

Step 8 Once the log file appears, click the file to download the logs to your local storage.

You've configured heartbeat logs

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). 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."
```

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 4: 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 managed by IoT FND, such as routers (CGR1000, IR800, IR8100,), endpoints, and gateways. When the specified device down timeout interval is reached, devices move to the Down state in the IoT FND GUI based on the last-heard value from the device and the tunnel interface state.

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

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

Device status changes to Uo 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, or 1800 seconds, 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

Routing Protocol for Low Power and Lossy Networks (RPL) is the IPv6 Routing Protocol for LLN (Low-Power and Lossy Networks) as defined in RFC6550. The Routing Protocol for Low Power and Lossy Networks feature implements RPL on Cisco IOS software.

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.

There are two types of RPL tree settings available in Cisco IoT FND:

- RPL Tree Update from Mesh Nodes

- RPL Tree Update from Routers

Table 5: Feature History

Release	Feature Name	Description
Cisco IoT FND Release 5.1	RPL Tree Update from both Mesh and Routers Nodes	You can collect endpoint metrics from both mesh nodes as well as routers independent of RPL tree settings.

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.

Table 6: 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.

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 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 update from both mesh and router nodes

Starting from Cisco IoT FND release 5.1.0, you can fetch the endpoint metrics from both mesh nodes as well as router nodes using the **Both Mesh & Router Nodes** option in RPL tree settings in Cisco IoT FND.

When you select **Both Mesh & Router Nodes** option, Cisco IoT FND updates the metrics based on whichever update is received first. See Global RPL tree settings for Cisco IoT FND for mesh and see Device configuration group properties for router nodes.

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** or **Both Mesh & Router Nodes** 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.
- If you select **Both Mesh & Router Nodes**, the **Number of Periodic Notifications between RPL Tree Polls** and **Maximum Time between RPL Tree (minutes)** fields get enabled automatically.

a) Enable the `processLinkPathCostRssifRssirRouter` property in the `cgms.properties` file optionally, if you select the **Both Mesh & Router Nodes** option, to process Link Cost, Path Cost, RSSI, and Reverse RSSI as given in the example.

Example:

```
processLinkPathCostRssifRssirRouter=true
```

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** > checkbox.

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 Navigate to the **Certificate Settings** tab and enter the threshold value in the **Certificate Expiry Threshold (days)** field for your supported routers or the Cisco IoT FND application server.

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, 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**. Cisco 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.