Managing System Settings

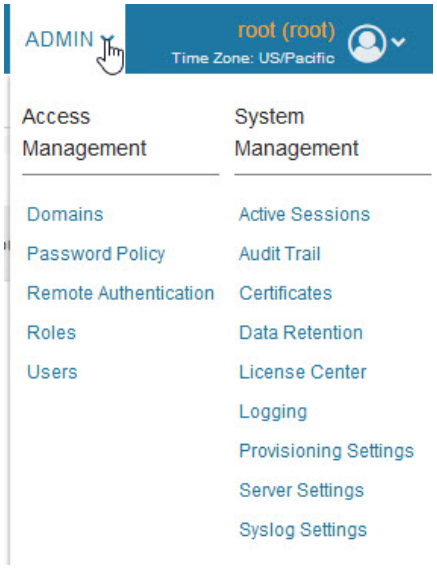
This section describes how to manage system settings, and includes the following sections:

- Managing Active Sessions
- Displaying the Audit Trail
- Managing Certificates
- Configuring Data Retention
- Managing Licenses
- Managing Logs
- Configuring Provisioning Settings
- Configuring Server Settings
- Managing the Syslog

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 (Figure 1)**

Figure 1 Admin Menu



Managing Active Sessions

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

- Viewing Active Sessions
- Logging Users Out
- Filtering the Active Sessions List

Viewing Active Sessions

To view active user sessions, choose **ADMIN > System Management > Active Sessions**. IoT FND displays the Active Sessions page (Figure 2).

Figure 2 Active Sessions Page

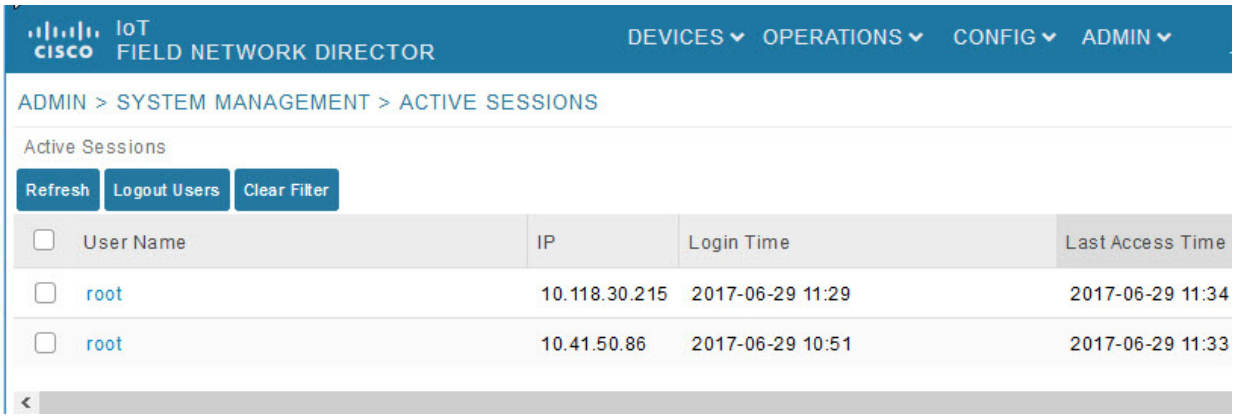


Table 1 describes the Active Session fields.

Table 1 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 Users Out

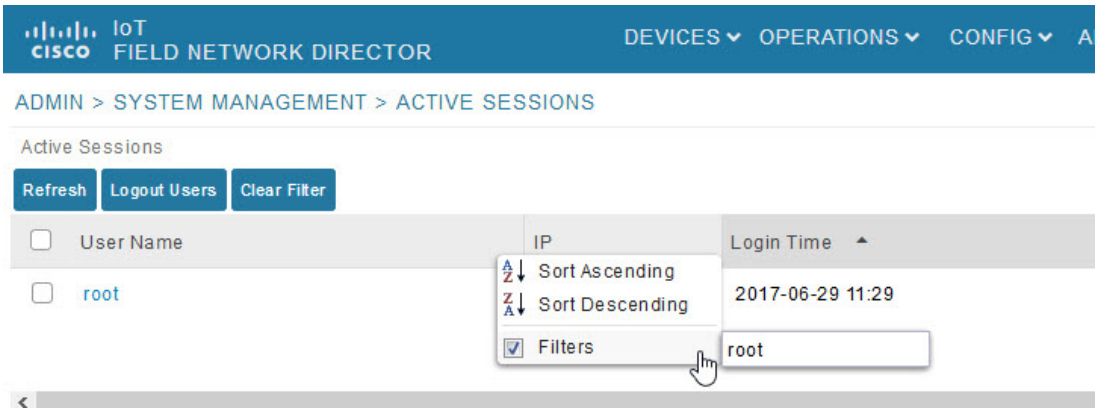
To log out an IoT FND user:

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

Filtering the Active Sessions List

To filter the Active Sessions list using column filtering:

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

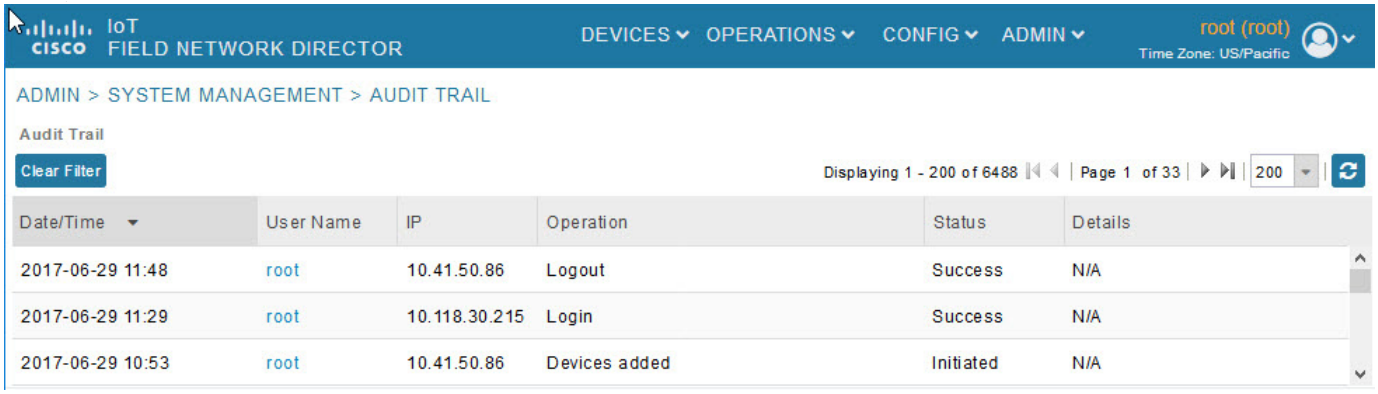


Table 2 describes the Audit Trail fields.

Table 2 Audit Trail Fields

Field	Description
Date/Time	Date and time of the operation.
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:

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

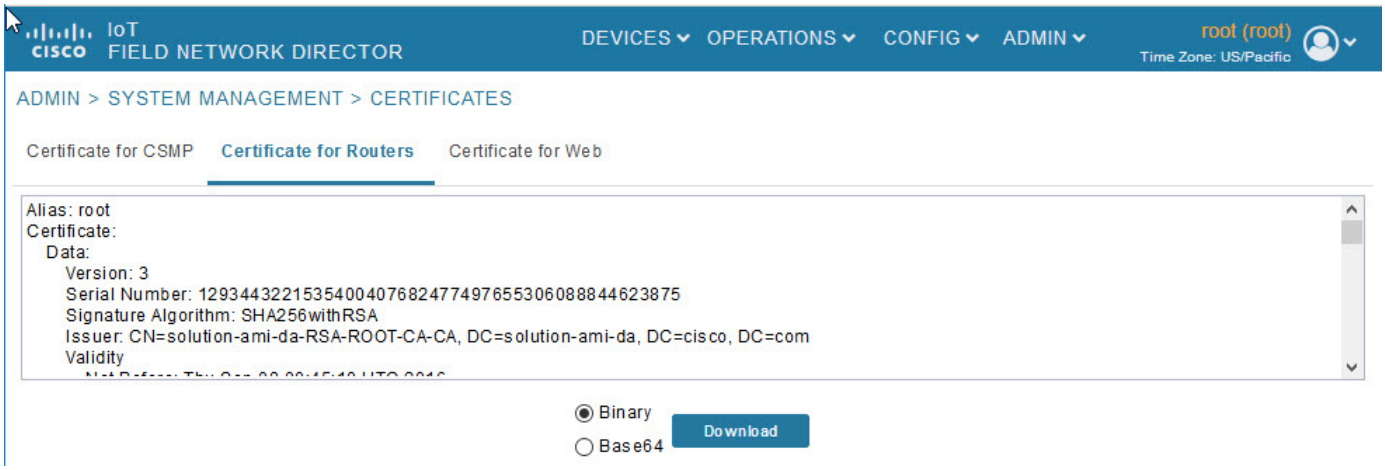
   Tip: To remove the filter, from the User Name drop-down menu, uncheck the **Filters** check box or click **Clear Filter** (left of the screen).

Managing Certificates

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

To display the CSMP, IoT-DM and Web certificates:

1. Choose **ADMIN > System Management > Certificates**.
2. To view a certificate, click its corresponding heading (such as Certificate for Routers).



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 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:

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

2. For each of the retention categories, specify the number of days to retain data.

   Table 3 lists the allowable maximum values for each field.

Table 3 Data Retention Fields Allowable Maximum Values

Field	Value in Days		
	Minimum	Maximum	Default
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

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

- Viewing License Summary
- Viewing License Files
- Adding License Files
- Deleting License Files

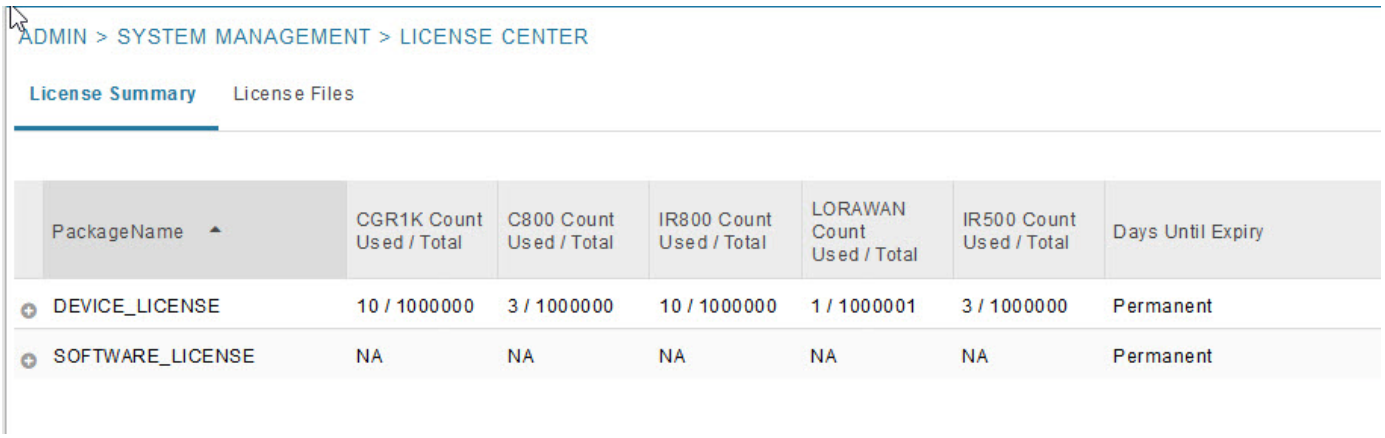
Note: IoT FND performs license enforcement when importing devices. If you add licenses, IoT FND only allows the permitted number of devices to be imported, as defined in the licenses.

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

Viewing License Summary

To view IoT FND license summary:

1. Choose **ADMIN > System Management > License Center**.
2. Click **License Summary**.



For every license, IoT FND displays the information described in Table 4.

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

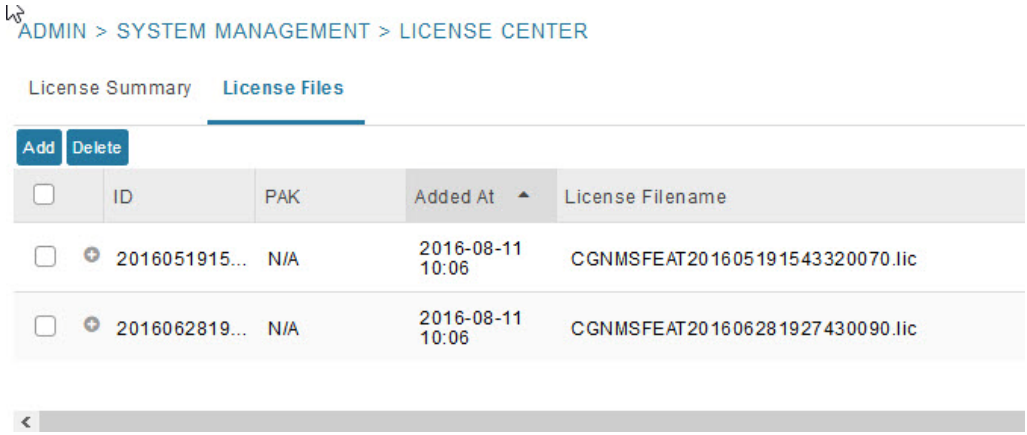
Table 4 Device License Summary Information

Field	Description
Package Name	Name of license package.
CGR1K Count Used/Total	Lists the number of CGR1000 devices currently active in the network and the maximum number of CGR1000s supported by the license.
C800 Count Used/Total	Lists the number of C800 devices currently active in the network and the maximum number of C800 devices supported by the license.
IR800 Count Used/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 Count Used/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 Count Used/Total	Lists the number of IR509 devices currently active in the network and the maximum number of IR509 devices supported by the license.
Days Until Expiry	Number of days remaining until the license expires.

Viewing License Files

To view IoT FND license files:

1. Choose **ADMIN > System Management > License Center**.
2. Click **License Files** to display details on all active licenses.



For every file, IoT FND displays the fields described in Table 5.

Table 5 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.

Adding License Files

To add a license file:

1. Choose **ADMIN > System Management > License Center**.
2. Click **License Files**.
3. Click **Add** to open a search window.
4. Click **Browse** to locate the desired license file and then click **Open**.
5. Click **Upload**. To cancel the upload, click **Reset**.
6. Click **Reset** to cancel the selected file and search for another file.

Deleting License Files

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

To delete a single license or multiple license files:

1. Choose **ADMIN > System Management > License Center**.
2. Click **License Files**.
3. Select the box next to each license file that you want to delete.
4. Click **Delete**. To confirm deletion, click **Yes**. To cancel the action, click **No**.

Managing Logs

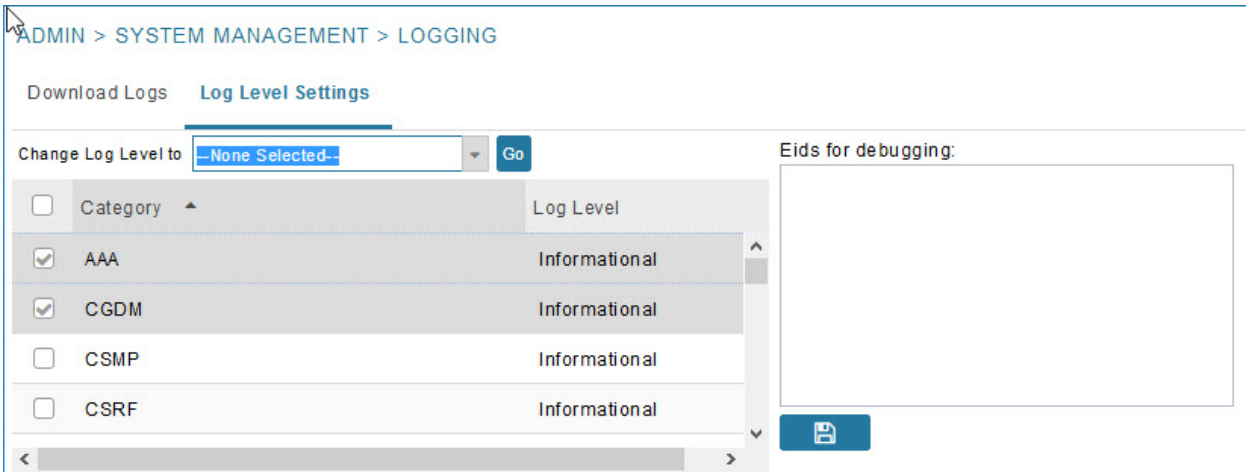
- Configuring Log Settings
- Downloading Logs

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:

1. Choose **ADMIN > System Management > Logging**.
2. Select **Log Level Settings**.
3. Check the check boxes of all logging categories to configure.



4. From the **Change Log Level to** 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.
5. To apply the configuration, click **Go**.

   Note: The server.log file is rotated based on size.
6. Click the **disk** icon to save the configuration.

Downloading Logs

To download logs:

1. Choose **ADMIN > System Management > Logging**.
2. Click the **Download Logs** tab.
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.
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 (Figure 3). See Figure 1 for an example of tunnels as used in the IoT FND architecture. See “Tunnel Provisioning Configuration Process for information on provisioning tunnels in the “Managing Tunnel Provisioning” chapter in the IoT FND 4.2 Installation Guide.

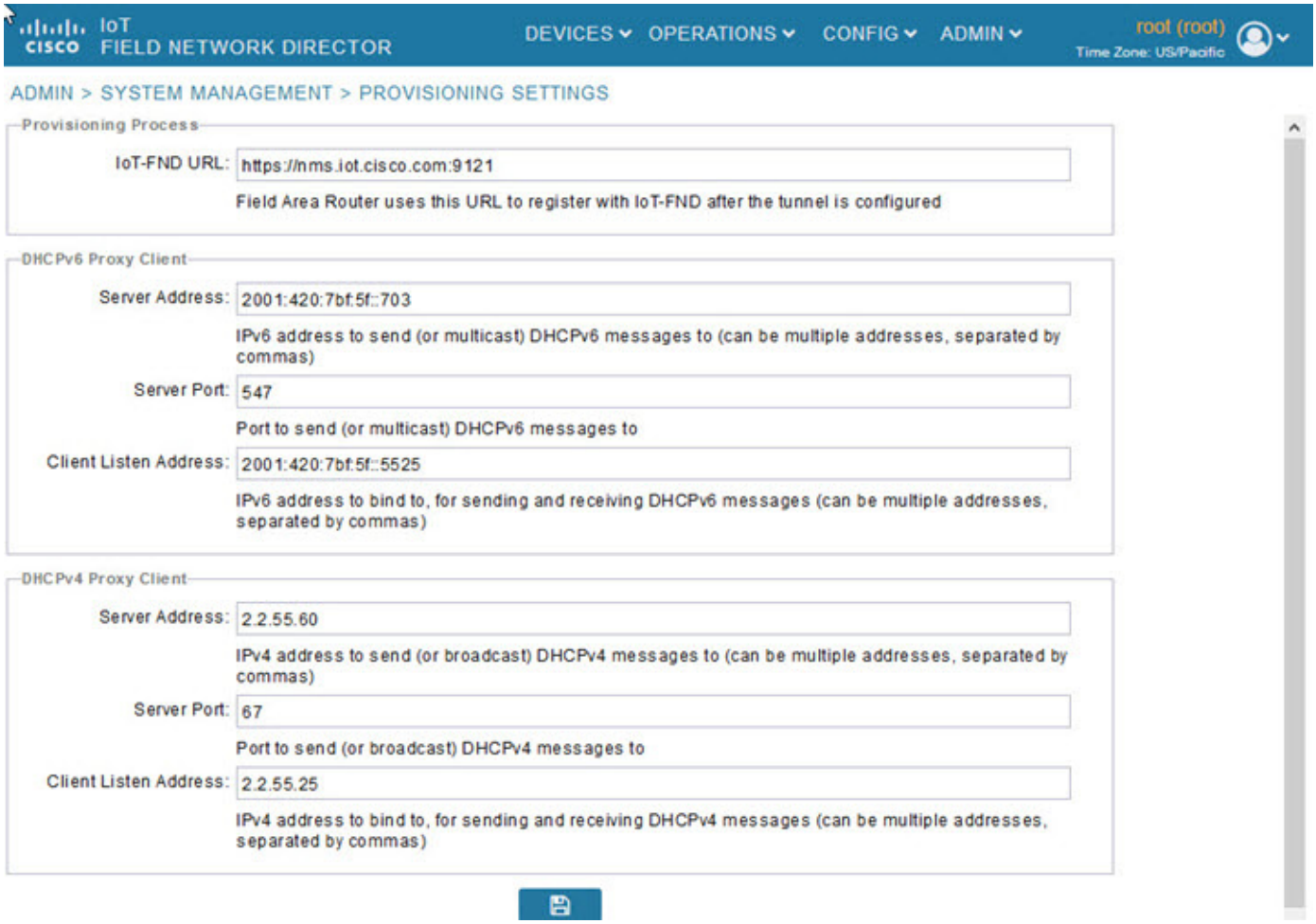
During Zero Touch Deployment (ZTD), you can add DHCP calls to the device configuration template for leased IP addresses.

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.

Figure 3 Provisioning Settings Page



This section provides the following topics for configuring tunnel settings:

- Configuring the IoT FND Server URL
- Configuring DHCP Option 43 on Cisco IOS DHCP Server
- Configuring DHCPv6 Proxy Client
- Configuring DHCPv4 Proxy Client

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:

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

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 DHCPv6 Proxy Client

To configure DHCPv6 Proxy Client settings:

1. Choose **ADMIN > System Management > Provisioning Settings**.
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.
3. Click **Save**.

Configuring DHCPv4 Proxy Client

To configure DHCPv4 Proxy Client settings:

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

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.

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.

3. Click **Save**.

Configuring Server Settings

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

- Configuring Download Logs Settings
- Configuring Web Sessions
- Configuring Device Down Timeouts
- Configuring Billing Period Settings
- Configuring RPL Tree Polling
- Configuring the Issue Status Bar

Configuring Download Logs 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 Logs settings:

1. Choose **ADMIN > System Management > Server Settings**.
2. Click the **Download Logs** tab.
3. Configure these settings:

Table 6 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	

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:

1. Choose **ADMIN > System Management > Server Settings**.
2. Click the **Web Session** tab.
3. Enter the number of timeout seconds. Valid values are 0–86400 (24 hours).

   If a web session is idle for the specified amount of time, IoT FND terminates the session and logs the user out.
4. To save the configuration, click the **disk** icon.

Configuring Device Down Timeouts

The Device Down Timeouts page lets you specify the number of timeout seconds after which the status of Head-end routers (ASR) and Routers (CGR1000, IR800, C800, ESR) and Endpoints changes to *Down* in IoT FND. The device down poll interval is five minutes. The system uses the device down timeouts values and the last heard time to decide whether to change the device status to Down. For example, if the router device down timeout value is set to two hours (7200 seconds), all routers with a last heard time older than 2 hours are marked as status Down.

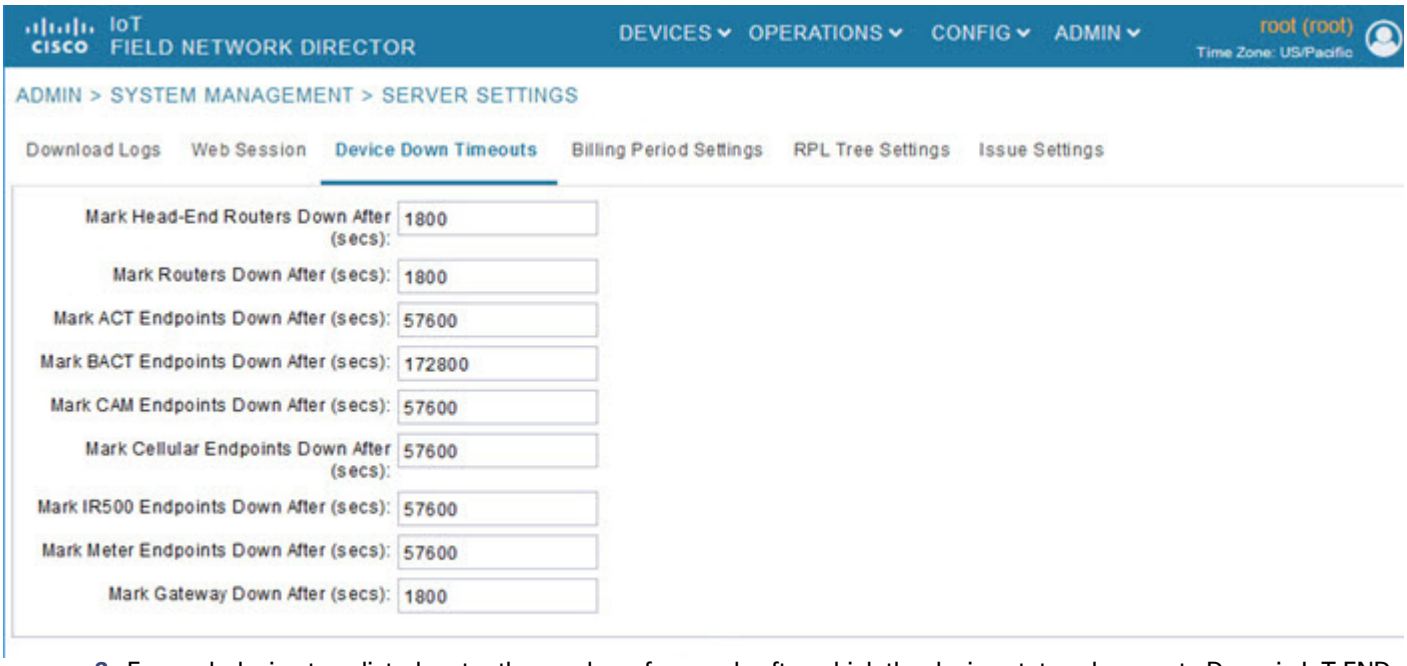
You can also configure the device timeout setting for router Config groups and Endpoint Config Groups.

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:

1. Choose **ADMIN > System Management > Server Settings**.
2. Click the **Device Down Timeouts** tab.



3. For each device type listed, enter the number of seconds after which the device status changes to Down in IoT FND.

   The parameter value must be greater than the corresponding polling intervals. For example, the default polling interval for endpoints is 8 hours (28800 seconds), so the value in the **Mark {ACT | BACT | CAM | Cellular | IR500> Meter} Endpoints Down After (secs)** field must be greater than 28800.

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

Device Down Timeout Settings for Router Config Groups and Endpoint Config Groups

To configure device down timeout settings for Router Config groups or Endpoint Config Groups:

1. Choose **CONFIG > Device Configuration**.
2. Select the Device you want to configure **{ROUTER** | **ENDPOINT}** in the left pane.
3. Click the **Group Properties** tab.
4. In the **Mark Routers Down After (secs)** field, enter the number of seconds after which the status of the devices (router or endpoints) in the group changes to Down in IoT FND.

   This value must be greater than the corresponding polling interval.

   For example, the default polling interval for routers is 30 minutes (1800 seconds), so the value in the Mark Routers Down After (secs) field must be 1801 or greater.

   The default polling interval for ENDPOINTS is 960 minutes (57600 seconds), so the value in the Mark Routers Down After (secs) field must be greater than 57600 seconds.

5. To save the configuration, click the **disk** icon.

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:

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

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.

Caution: CG-NMS 1.1(5) release does not support router RPL tree updates. Do not enable RPL tree updates from Routers.

To configure RPL tree polling settings:

1. Choose **ADMIN > System Management > Server Settings**.
2. Choose the **RPL Tree Settings** tab.
3. Choose the **Enable RPL tree update from** radio button for Mesh Nodes to receive the RPL tree update from those devices.
4. 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:

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

To configure Syslog forwarding:

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

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