· I | I · I | I · CISCO .

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)

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

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
----------	--------	----------	------

cisco IoT Field Network Director	Device	s , Operations , Config ,	Admin ,	root * Time Zone: America/Los_Angeles
Active Sessions Audit Trail Certificates	Data Retention	License Center Logging Provis	oning Settings Server Settings Syslog Settings	
Active Sessions				
Refresh Logout Users Clear Filter				
User Name	3P	Login Time	Last Access Time ~	
Toot 🔄	10.24.52.107	2015-07-24 12:47	2015-07-24 17:07	
toon 🔄	127.0.0.1	2015-07-24 12:14	2015-07-24 17:07	

Table 1 describes the Active Session fields.

Fable 1Active 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 Refresh to update the users list.

Logging Users Out

To log IoT FND users out:

- 1. Choose Admin > System Management > Active Sessions.
- 2. Check the check boxes of the users to log out.
- 3. Click Logout Users.
- 4. Click Yes.

Filtering the Active Sessions List

To filter the Active Sessions list using column filtering:

1. Choose Admin > System Management > Active Sessions.

2. From the User Name drop-down menu, choose Filters and enter the user name or the first characters in the user name to filter the list.

cisco IoT Field	Network Dire	ctor		Devices	-	Operations	- Confi	9 -	Admin 🖕			
Active Sessions	Audit Trail	Certificates	D	ata Retention	Lice	ense Center	Logging	Provisionin	ig Settings	Serve	er Settings	Syslog Settings
Active Sessions												
Refresh Logout Users Clear Filter												
User Name			- 1	IP	Logi	n Time			Last Access Ti	me 👻		
root			₽↓	Sort Ascending		-07-24 12:47			2015-07-24 17	7:07		
root		Z Sort Descending		a	-07-24 12:14		2015-07-24 17:07					
				C :14								
				Filters	-{h}							

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.

Active Sessions	Audit Trail Certi	ficates Data Ref	tention License Center Logging P	rovisioning Settings	Server Settings Syslog Settings
Audit Trail					
Clear Filter					Displaying 1 - 50 of 223 🕅 🗐 Page 1 of 5 🕨 🕅 😒 🧟
Date/Time +	User Name	IP	Operation	Status	Details
2015-07-21 14:41	root	127.0.0.1	Scheduled reboot and load firmware image	Initiated	Group: IOSCGR, Device Category: router, For image:null
2015-07-21 14:24	root	127.0.0.1	Logging levels changed.	Success	N/A
2015-07-21 14:23	root	127.0.0.1	Firmware download started	Initiated	Group: IOSCGR, Device Category: router, Firmware image: cgr1000-universalk9-bundle.SPA.155- 2.25.M0.7
2015-07-21 14:22	root	127.0.0.1	Firmware image is added to NMS	Success	Firmware image: cgr1000-universalk9-bundle.SPA.155-2.25.M0.7, Device type: router
2015-07-10 14:50	root	10.154.201.111	Changed device properties	Initiated	N/A
2015-07-09 18:49	root	10.154.201.111	User added.	Success	User 'smoc' added.
2015-07-09 18:49	root	10.154.201.111	Role added.	Success	Role 'SMOC Operator' added.
2015-07-07 19:17	root	10.154.201.54	Scheduled reboot and load firmware image	Initiated	Group: default-ir800, Device Category: router, For image:null
2015-07-07 19:10	root	10.154.201.54	Firmware download started	Initiated	Group: default-ir800, Device Category: router, Firmware image: ir800-universalk9-bundle.SPA.155- 2.25.M0.5
2015-07-07 19:05	root	10.154.201.54	Firmware download started	Initiated	Group: default-ir800, Device Category: router, Firmware image: ir800-universalk9-bundle.SPA.155- 2.25.M0.5
2015-07-07 19:01	root	127.0.0.1	Logging levels changed.	Success	N/A
2015-07-07 18:51	root	127.0.0.1	Firmware image is added to NMS	Success	Firmware image: ir800-universalk9-bundle.SPA.155-2.25.M0.5, Device type: router
2015-07-07 17:42	root	127.0.0.1	Logging levels changed.	Success	N/A
2015-07-07 17:41	root	127.0.0.1	Logging levels changed.	Success	N/A
2015-07-07 17:28	root	127.0.0.1	Configuration template updated	Success	Group: default-ir800, Device Category: router
2015-07-07 17:25	root	127.0.0.1	Devices added	Initiated	N/A
2015-07-07 13:22	root	127.0.0.1	Devices removed	Initiated	N/A
2015-07-06 14:07	root	127.0.0.1	User added.	Success	User 'tester' added.
2015-07-02 12:51	root	127.0.0.1	Scheduled reboot and load firmware image	Initiated	Group: default-ir800, Device Category: router, For image:null

Table 2 describes the Audit Trail fields.

Table 2Audit 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 Refresh 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, choose Filters and 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, clear the Filters check box or click Clear Filter.

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 tab.

cisco IoT Fie	ld Network Dir	rector	Device	is . Operatio	ons , Co	nfig . Admin .				root v T	ime Zone: Amer	rica/Los_Angeles
Active Sessions	Audit Trail	Certificates	Data Retention	License Center	Logging	Provisioning Settings	Server Settings	Syslog Settings				
Certificate for CSMP	Certificate for F	touters Cert	ficate for Web									
Alias: root Certificate: Data: Version: 3 Serial Number: Signature Algor Issuer: Chincen Validity Not Before: S Not After: Fri Subject: Public Fingerprints: MD5: 75:00// SHA1: 1F:CC Subject Public Public Key Al 30:82:02:2 01:01:05 00:01:00:0 02:01:00:0 00:00:0 01:00:0 00:0	19876512211508 thm: SHA1withRS bursaca-CENBU-4 at Nov 17 03 08:5 Nov 17 03 18:50 nbursaca-CENBU 41:99:C9 D5:C2:E :04:C3:26.88:38:16 (ay Info: :03:82:02.0F:00: 00:382:02.0F:00: 00:382:02.0F:00: 00:382:02.0F:00: 00:382:02.0F:00: 00:382:02.0F:00: 01:26:00:38:9F 17:46:D2:EB:37:FB:00: 11:46:52:EA:7F:94 C2:P:06:74:B8:9-3 11:73:E2:B0:1A:48	0256952401070 3A ROOT-CA, DC= 4 UTC 2012 UTC 2017 IROOT-CA, DC B:11:49:06:3E 04:40:36:0A:A7 30:82:02:0A:02 50:16:8E:6E:C 0:7A:6D:C9:C0:1 54:05:6D:28:5C 0:5A:28:7A:97:0 C:5E:EE:81:C7 1:54:36:98:78:2 7:F4:76:58:07:E 4:E8:4E:24:E8:F 1:89:90:CC:FE: 38A:FE:CC:FE:	97776994407 cenbursaca, DC=ciso =cenbursaca, DC=ciso 54.72-CA-18 81:11:E5-79:42:51:33 101: 62: 57:88: 13:F7: 9:D4: 1.7E: 0:59: 9:54: 0:59: 17:C8: 6:94: 57:BF: 57:BF: 57:BF:	o, DC≈com co, DC≃com :50								
					 Base 	e64 Download						
© 2012-2015 Cisco	o Systems, Inc. Al	Rights Reserve	d						issues	00	V 1	<u>4</u> 0

3. To download a certificate, click the encoding (Binary or Base64) radio button, and then click Download.

For more information about certificates, see Generating and Installing Certificates.

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.

cisco ToT Field Network Director	Devices . Of	erations , Config , Admin ,		root v Time Zone: America/Los_Angeles
Active Sessions Audit Trail Certificates	Data Retention License Ce	nter Logging Provisioning Settings	Server Settings Syslog Settings	
Keep Event data for	31 day(s)			^
Keep Endpoint Firmware Operation data for	90 day(s)			
Keep Historical Dashboard data for	30 day(s)			
Keep Dashboard data for	7 day(s)			
Keep Closed Issues data for	31 day(s)			
Keep JobEngine data for	7 day(s)			
Keep Historical Router Statistics for	62 day(s)			
Keep Device Network Statistics for	7 day(s)			
Keep Service Provider down routers data for	31 day(s)			
Save Reset				

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 Value

Field	Value in Days			
	Minimum	Maximum	Default	
Event data	1	90	31	
Firmware data	7	180	7	
Historical NMS data	1	90	62	
NMS data	1	7	7	
Closed issues data	1	90	30	
Job engine data	1	30	30	
Historical router data	1	90	30	
Device data	1	7	7	
Service provider down routers data	1	31	31	

- 3. Click Save.
- 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
- Viewing License File Details
- Adding License Files
- Deleting License Files

Note: IoT FND performs license enforcement when importing devices. Without licenses, IoT FND allows only 3 FARs and 100 mesh endpoints. If you add licenses, IoT FND only allows the permitted number of devices to be imported, as defined in the licenses.

Viewing License Summary

To view IoT FND license summary:

- 1. Choose Admin > System Management > License Center.
- 2. Click License Summary.

CISCO IOT Field	d Network Directo	or	Devices ,	, Operations	Config	Admin 🖕
Active Sessions	Audit Trail Ce	ertificates Dat	a Retention	icense Center	Logging Provision	ning Settings Server
License Summary	License Files					
License Summary	1					
Package Name 🔺	Max CGR1000 Count	Max C800 Count	Max IR800 Count	Max IR509 Count	Max Endpoint Count	Max LoRaWAN Modem Count
DEVICE_LICENSE	1000	1000	1000	N/A	N/A	N/A
SOFTWARE_LICENSE	N/A	N/A	N/A	N/A	N/A	N/A

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

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

Table 4License File Information

Field	Description
Package Name	Name of license package.
Max CGR1000 Count	Maximum number of CGR 1000s supported.
Max C800 Count	Maximum number of C800 devices supported.
Max IR800 Count	Maximum number of IR809 and IR829 devices supported.
Max IR509 Count	Maximum number of IR500 devices supported.
Max Endpoint Count	Maximum number of mesh endpoints supported.
Max LoRaWAN Modem Count	Maximum number of LoRaWAN modems (modules) supported.
Max User	Maximum number of users supported.
Max NBAPI User	Maximum number of IoT FND North Bound API users supported.
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.

CISCO IoT Field Network Director	Devices	. Operations . Cor	nfig . Admin .	-	oot • Time Zone: America/Los_Angeles
Active Sessions Audit Trail Certificate	s Data Retention L	License Center Logging	Provisioning Settings Server Setting	ps Syslog Settings	
License Summary License Files					
Add Delete All Show Details					
License Files					
ID	PAK		Added At ~	License Filename	
20150204160300015	N/A		2015-02-04 17:04	CGNMSFEAT201502041603000150.llc	
20150204195950018	N/A		2015-02-04 17:04	CGNMSFEAT201502041959500180.lic	
C License File Details					>
Package Name - Type	Max Count	Days Until Expiry			
ADVANCED_SECURITY C800	10000	Permanent			
ADVANCED_SECURITY IRS00	200000	Permanent			
BASE C800	10000	Permanent			
BASE IRSOC	200000	Permanent			
PROACTIVE_MONITORING C800	10000	Permanent			
PROACTIVE_MONITORING IRSOU	200000	Permanent			
STANDARD_PRODUCT_NT N/A	1	Permanent			
<					>
© 2012-2015 Cisco Systems, Inc. All Rights Reser	ved. (version 2.2.0-74)			Issues	O ♥1 ▲0

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

Table 5License File Fields

Field	Description
ID	License ID.
РАК	Number for issuing license fulfillment.
Added At	Date and time the license was added to IoT FND.
License Filename	Filename of the license.

Viewing License File Details

To view license file details:

- 1. Choose Admin > System Management > License Center.
- 2. Click License Files.
- 3. Choose the licenses to view.
- 4. Click Show Details.

For every selected file, the License File Details section displays the following information:

Table 6License File Details

Field	Description
Package Name	License package name.

Field	Description
Туре	License target (ROUTER, ENDPOINT, USER, NB_USER). The type is an empty string if a value is not applicable.
Max Count	Maximum number of target devices entitled by this license.
Days Until Expiry	The number of days remaining until the license expires.

Table 6 License File Details (continued)

Adding License Files

To add a license file:

- 1. Choose Admin > System Management > License Center.
- 2. Click License Files.
- 3. Click Add.

				×
Upload	License File			
File:	A valid license file		Browse	
		Upload Reset		1

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

5. Click Upload.

Deleting License Files

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

To delete license files:

- 1. Choose Admin > System Management > License Center.
- 2. Click License Files.
- 3. Click Delete All, and then click Yes.

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.

CISCO IoT Field Network Director	Devices , Operations , Config , Admin ,		root v	Time Zone: Am	rica/Los_An
Active Sessions Audit Trail Certificates	Data Retention License Center Logging Provisioning Settings Server Settings Syslog Settings				
Download Logs Log Level Settings					
Sanne Los Level In None Selected.					
(0					
Category A	Log Level				
AAA	Informational				
GDM	Informational				
CSMP	Informational				
CSRF	Informational				
Configuration	Informational				
DHCP	Informational				
Dashboard	Informational				
Data Aggregation	Informational				
Data Retention	Informational				
Device Actions	Informational				
Fibers	Informational				
Firmware	Informational				
GOS App Management	Informational				
Group Management	Informational				
Inventory	Informational				
Issues and Events	Informational				
Job Engine	Informational				
Labels	Informational				
Licensing	Informational				
Mark Down	Informational				
Metrics	Informational				
NBAPI	Informational				
NETCONF	Informational				
Outage	Informational				
Reprovision	Informational				
Retriever Engine	Informational				
Router File Management	Informational				
Rules	Informational				
Scheduler	Informational				
Security	Informational				
Snmp	Informational				
System	Informational				
Templates	Informational				
Tools	Informational				
Tunnel Provisioning	Informational				
ut ut	Informational				
WSMA and CGNA	Informational				
Work Order	Informational				
© 2012-2015 Cisco Systems, Inc. All Rights Reserver		Issues	00	71	<u>^</u> 0

2. Click 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.

Downloading Logs

To download logs:

- 1. Choose Admin > System Management > Logging.
- 2. Click the Download Logs tab.

cisco IoT Field Network Director	Devices Operations Config Admin Time Zone: America/Los_Angeles
Active Sessions Audit Trail Certificates	Data Retention License Center Logging Provisioning Settings Server Settings Syslog Settings
Download Logs Log Level Settings	
Download Logs	
Server	File (click on the filename to download the file to your computer)
m-linux	Processing

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 FARs 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. Also, during 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.

Active Sessions Au	St Trail Certificates Data Retention License Center Logging Provisioning Settings Server Settings Syslog Set	tings	
Provisioning Process			
IoT-FND URL:	https://mms.iot.cisco.com/9121		
	Field Area Router uses this URL to register with IoT-FND after the tunnel is configured		
HCPv6 Proxy Client			
Server Address:	105:13		
	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 (can be multiple addresses, separated by commas)		
HCPv4 Proxy Client			
Server Address:	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:	0000		
	IPv4 address to bind to, for sending and receiving DHCPv4 messages (can be multiple addresses, separated by commas)		
	3/02		

Figure 3 Provisioning Settings Page

This section provides the following topics for configuring tunnel settings:

- Configuring the IoT FND Server URL
- Configuring DHCPv6 Proxy Client
- Configuring DHCPv4 Proxy Client

Configuring the IoT FND Server URL

The IoT FND URL is the URL that FARs use to access with IoT FND after the tunnel is established. This URL is also accessed during periodic inventories. During ZTD, FARs 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 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." (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.

CISCO IoT Field Network Director	Devices . Operations .	Config . Admin .	root ¥ Time Zone: America/Los_Angeles
Active Sessions Audit Trail Cert	Icates Data Retention License Center Log	ging Provisioning Settings Server Settings	Syslog Settings
Download Logs Web Session Device Do	wn Timeouts Billing Period Settings RPL Tree Settings	Issue Settings	
Keystore Filename	/opt/cgms/server/cgms/cont/cgms_keystore		Upload Keystore File
Keystore Password	•••••		
Confirm Keystore Password	•••••		
FTP Password	•••••		
Confirm FTP Password	•••••		
		Save	

3. Configure these settings:

Table 7Keystore 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. Click Save.

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.

CISCO IoT Field Network Director	Devices Operations Config Admin	root Time Zone: America/Los_Angeles
Active Sessions Audit Trail Certificates	Data Retention License Center Logging Provisioning Settings Server Settings Syslog Settings	
Download Logs Web Session Device Down Timeouts	Billing Period Settings RPL Tree Settings Issue Settings	
Web Session Timeout (secs): 1800		
	Save	

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. Click Save.

Configuring Device Down Timeouts

The Device Down Timeouts page lets you specify the number of timeout seconds after which the status of Routers (ASRs, FARs) 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 FAR device down timeout value is set to two hours (7200 seconds), all FARs with a last heard time older than 2 hours are marked as status Down.

You can also configure the device timeout setting for FAR 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.

Active Sessions Audit Trail Certificates			cates D	ata Retention	Licer	nse Center	Logg	ing P	rovision	ing Settings	Server Setting	iettings	Syslog Settings
Download Logs	Web Session	Device Down	Timeouts	Billing Period	Settings	RPL Tree S	ettings	Issue Set	tings				
Mark Head-I	End Routers Do	wn After (secs):	1800										
N	lark Routers Do	wn After (secs):	1800										
Mark AC	T Endpoints Do	wn After (secs):	57600										
Mark CA	M Endpoints Do	wn After (secs):	57600										
Mark Cellula	ar Endpoints Do	wn After (secs):	57600										
Mark IR50	0 Endpoints Do	wn After (secs):	57600										
March Market	er Endpoints Do	wn After (secs):	57600										

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

This 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 Mesh Endpoints Down After (secs) field must be greater than 28800.

4. Click Save.

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

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

- 1. Choose Config > Device Configuration.
- 2. Select the Device you want to configure <ROUTERS or ENDPOINTS> in the left pane.
- 3. Click the Group Properties tab.

CISCO IoT Field Network Director	Devices Operations Config Admin . root v Time Zone: America/Los Angeles
App Management Device Configuration	Firmware Update Router File Management Rules Tunnel Provisioning
Assign Devices to Group Change Device Properties	new_CGR_Group
CONFIGURATION GROUPS	Group Members Edit Configuration Template Push Configuration Group Properties
- S ROUTER	Mark Routers Down After (secs): 3600
21MR2 (2)	Number of Periodic Notifications between RPL Tree Polls:
default-c800 (0)	Maximum Time between RPL Tree Polls (minutes): 400
default-cgr1000 (2)	
C default-ir800 (1)	Save Changes
new_CGR_Group (1)	
ENDPOINT	
default-cgmesh (1)	
default-ir500 (0)	

4. In the Mark Routers Down After (secs) or Mark Endpoints 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 FARs is 30 minutes (1800 seconds), so the value in the Mark Routers Down After (secs) field must be greater than 1800.

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. Click Save Changes.

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.

CISCO IoT Field Network Director Dr	vices . Operations .	. Config . Adm	in .	-	root V Time Zone: America/Los_Angeles
Active Sessions Audit Trail Certificates Data Retention	n License Center Lo	ogging Provisioning Sel	tings Server Settings	Syslog Settings	
Download Logs Web Session Device Down Timeouts Billing Period	Settings RPL Tree Setting	gs Issue Settings			
Monthly Cellular Billing Period Start (ay: 1]			
Monthly Ethernet Billing Period Start 0	ay: 1	1			
Time Zr	ne: UTC	v			
		Save			

- 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. Click Save.

Configuring RPL Tree Polling

RPL tree polls are derived from FAR periodic notification events. Since the RPL tree is not pushed from the FAR 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.

cisco IoT	Field Netwo	rk Director	Devices .	Operations .	Config		Admin 🖕	root 🔻	Time Zone: US/Pacific
Active Sess	Active Sessions Audit Trail Certificates		Data Retention License Center Logging F				oning Settings	Server Setting	Syslog Settings
Download Logs	Web Session	Device Down Timeouts	Billing Period Settings	RPL Tree Settings	Issue Se	ttings			
			Number of Periodic Notifi	Enable RPL tree upd	late from:	Mes Rou	sh Nodes Iters		
			Maximum Time be	tween RPL Tree Polls (minutes):	480			
				Save					

- 3. Choose the Enable RPL tree update from radio button for Mesh Nodes or CGR devices to receive the RPL tree update from those devices at the specified intervals.
- 4. For Router polling, enter the number of events that pass between RPL tree polling intervals in the Number of Periodic Notification RPL Tree Polls field.
 - The default value is 8.

Note: If thresholds are exceeded during periodic notification events, IoT FND performs a RPL tree poll.

- 5. In the Maximum Time between RPL Tree Polling (minutes) field, enter the maximum amount of time between tree polls in minutes.
 - The default value is 480 minutes (8 hours).
- 6. Click Save.

Configuring the Issue Status Bar

The Issue Status bar displays issues by device type (as set in user preferences; see Setting 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.

cisco IoT Field Network Director	Devices , Operations , Config , Admin ,	* toor
Active Sessions Audit Trail Certificates	Data Retention License Center Logging Provisioning Settings Server Settings Syslog Settings	
Download Logs Web Session Device Down Timeouts	Billing Period Settings RPL Tree Settings Issue Settings	
	Enable/Disable Issue Status Bar: 🗸	
	Issue Status Bar Refresh Interval(seconds): 30	
	Certificate Expiry Threshold(days): 180	

- 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 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.

Data Retention	License Center	Logging Prov	isioning Settings Se	erver Settings Syn	slog 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.