Troubleshooting IoT FND

This section describes how to troubleshoot common IoT FND issues.

Note: Always reference the release notes for your IoT FND version.

Tunnel Provisioning DHCP Configuration Issues

If there is a problem allocating an address, IoT FND logs a Tunnel Provisioning Failure event. The log entry includes details of the error.

To monitor the address allocation process:

- Check the IoT FND server.log file to determine if IoT FND is sending a DHCP request during tunnel provisioning.
- Check your DHCP server log file to determine if the DHCP request from IoT FND reached the DHCP server.

If requests are not reaching the server:

- Ensure that the DHCP server address is correct on the **Provisioning Settings** page in IoT FND (**Admin > System Management > Provisioning Settings**).
- Check for network problems between IoT FND and the DHCP server.

If the DHCP server is receiving the request but not responding:

- View the DHCP server log file, and ensure that the DHCP server is configured to support requests from the link address included in the DHCP requests. The link address is defined in the tunnel provisioning template.
- Ensure that the DHCP server has not exhausted its address pool.

If the DHCP server is responding, but IoT FND is not processing the response:

- Ensure that the lease time is infinite. Otherwise, IoT FND will not process the response.
- View the DHCP server logs and IoT FND server logs for other errors.

Mesh Endpoint Registration Issues

To determine why MEs register with IoT FND, IoT FND collects the registration reason code from the MEs and logs events and the code with other relevant information as printed key value pairs to help diagnose registration issues.

Here is an example of a logged event:

```
?Event logged: Event(id=0, eventTime=1335304407477, eventSeverity=0, eventSource=cgmesh,
eventMessage=Mesh node registered due to cold  boot: [lastReg: 0, lastRegReason: 1],
NetElement.id=10043, EventType.name=null, lat=1000.0, lng=1000.0, geoHash=null
```

Table 1 lists reason codes for ME registration and corresponding event:

Table 1 Mesh Endpoint Registration Reason Codes

Registration Reason Code	Code	Event Type Name	Severity	Message	Description
REASON_UNKNOWN	0	unknownRegReason	INFO	Mesh node registered for unknown reason.	
REASON_COLDSTART	1	coldBoot	INFO	Mesh node registered due to cold boot.	The message includes the new IP address of the ME.
REASON_ADMIN	2	manualReRegistration	INFO	Mesh node registered due to manual registration.	The endpoint received an NMSRedirectRequest without a URL field.
REASON_IP_CHANGE	3	rejoinedWithNewIP	INFO	Mesh node registered with new IP address.	The message includes the new IP address of the ME.
REASON_NMS_CHANGE	4	nmsAddrChange	INFO	Mesh node registered due to NMS address change.	The IoT FND IP address changed OUTSIDE of an NMSRedirect (a new DHCPv6 option value was received).
REASON_NMS_REDIRECT	5	manualNMSAddrChange	INFO	Mesh node registered due to manual NMS address change.	Endpoint received an NMSRedirect request.
REASON_NMS_ERROR	6	nmsError	INFO	Mesh node registered due to NMS error.	Endpoint received an error from IoT FND.

In addition to generating events when MEs register with IoT FND, IoT FND also generates events after receiving a WPAN change TLV `WPANStatus`.

```
Event logged: Event(id=0, eventTime=1335304407974, eventSeverity=0, eventSource=cgmesh,
eventMessage=WPAN change due to migration to better PAN: [lastChanged: 0, astChangedReason: 4],
NetElement.id=10044, EventType.name=null, lat=1000.0, lng=1000.0, geoHash=null)
```

Table 2 lists reasons for ME WPAN changes and the corresponding event.

Table 2 Reasons for Mesh Endpoint WPAN Changes

Registration Reason Code	Code	Event Name	Severity Type	Description
IEEE154_PAN_LEAVE_UNKNOWN	-1	unknownWPANChange	MAJOR	WPAN change for unknown reason.
IEEE154_PAN_LEAVE_INIT	0	meshInit	N/A	No event is generated for this code.
IEEE154_PAN_LEAVE_SYNC_TIMEOUT	1	meshConnectivityLost	MAJOR	WPAN change due to mesh connectivity loss.
IEEE154_PAN_LEAVE_GTK_TIMEOUT	2	meshLinkKeyTimeout	MAJOR	WPAN change due to mesh link key timeout.
IEEE154_PAN_LEAVE_NO_DEF_ROUTE	3	defaultRouteLost	MAJOR	WPAN change for no default route.
IEEE154_PAN_LEAVE_OPTIMIZE	4	migratedToBetterPAN	MAJOR	WPAN change due to migration to better PAN.

For these events, the message includes the time elapsed since the ME left the network to when it rejoined. IoT FND displays the amount of time the ME was offline since the event was logged (for example, 4 hours 23 minutes ago).

Recovering an Expired Database Password

To recover from an expired password, run these commands:

```
su - oracle

sqlplus sys/cgmsDbaAccount@cgms as sysdba
  alter user cgms_dev identified by test;
  alter user cgms_dev identified by password;
  exit;
```

Unlocking the IoT FND Database Password

If you enter an incorrect IoT FND Database password multiple times, Oracle locks your user account. Unlock your password using the Oracle software, as shown in this example:

```
# su - oracle
# sqlplus sys/<database_password>@cgms as sysdba
  alter user cgms_dev account unlock;
  exit;
```

IoT FND Service Will Not Start

If the IoT FND service does not start:

1. Validate connectivity to the database:
   a. Log in as root on the IoT FND server.
   b. Enter the following at the command prompt:

```
service cgms status
```

c. Verify the database server IP address and that IoT FND can connect to the database.

- If the IP address is incorrect or if IoT FND cannot access the database, run **setupCgms.sh** and enter the correct values.

d. Run the **service cgms status** command and verify connectivity.

e. Start IoT FND.

2. Verify that the JRE version installed on the server is correct (see the System Requirements chapter).
3. Verify that database migration was performed successfully.

Exception in the server.log File on the IoT FND Server

If the there is an exception in the server.log file indicating that IoT FND could not open the cgms_keystore file, then the cgms_keystore password stored in the cgms.properties file on the IoT FND server is incorrect.

The password for the cgms_keystore file is encrypted and stored in the /opt/cgms/server/cgms/conf/cgms.properties file.

To encrypt or decrypt the password, use the /opt/cgms/bin/**encryption_util.sh** script.

Verify or update the password in the cgms.properties file, and if an update is required, restart IoT FND after modifying the password.

Resetting the root Password

If you forget the password of the IoT FND root user account, reset the password by running the /opt/cgms/bin/**password_admin.sh** script.

Second IoT FND Server Not Forming a Cluster

Typically, discovery of nodes in a IoT FND cluster is automatic. As long as the IoT FND servers are on the same subnet, they form a cluster.

If you install a IoT FND server and it does not join the cluster:

1. Verify that your servers are on the same subnet, can ping each other, and share the same cluster name.
2. Check the status of all members by running the /opt/cgms/bin/print_cluster_view.sh script.
3. Modify the cluster name, as follows:
   a. Change the value of the HA_PARTITION_NAME parameter on all IoT FND cluster nodes, and then restart them.
   b. Change the value of the UDP_MULTICAST_ADDR parameter (unique multicast address) to match on all nodes in the cluster.
   c. Change the value of the CLUSTER_BIND_ADDR parameter to the interface to which you want the NMS to bind.
4. Verify that all the cluster nodes are configured to use NTP (see Configuring NTP Service)
5. Check the /etc/hosts file and verify that the IP address is correctly mapped to the hostname of the local server.

IoT FND Service Restarts Automatically

When the IoT FND services are started, the watchdog script is invoked. The watchdog script checks the health of the IoT FND services. If the watchdog script detects an anomaly, it logs the conditions in the /opt/cgms/server/cgms/log/cgms_watchdog.log file

The watchdog script tries three times to determine if the anomaly condition improved. If not, it restarts the IoT FND services automatically, unless the database has become unreachable. If the database is not reachable, the watchdog stops the IoT FND services. Check the log files, including server.log, to determine what is causing the restarts.

Manually disable the watchdog process by running the /opt/cgms/bin/deinstall_cgms_watchdog.sh script on the IoT FND server as root.

FAR Management Issues

This section presents common issues with FAR management and possible resolutions.

Certificate Exception

If this exception appears in the server.log file stored on the IoT FND server when a FAR attempts to register with IoT FND, the cgms_keystore file does not contain the CA server certificates or the CA certificates that were imported into the cgms_keystore file are incorrect:

```
SSLException: Received fatal alert: unknown_ca
```

For information about how to import certificates into the cgms_keystore file, see “Generating and Installing Certificates in the Cisco IoT FND Installation Guide, 4.0.x and greater.

FAR Keeps Reloading and Does Not Switch to the Up State

When a FAR is continuously reloading every time it contacts IoT FND, it could be because the configuration pushed to the FAR by IoT FND is not being applied successfully.

Check the server.log file on the IoT FND server for clues on the cause of the configuration push failure. Sometimes, typos in the in the Field Area Router Tunnel Addition template cause this failure (IoT FND does not provide template validation).

Note: When a FAR registers with IoT FND, IoT FND queries the FAR with show commands. IoT FND then configures the FAR based on the configuration commands in the Field Area Router Tunnel Addition template.

Other reasons for continuous reloads may be:

- A bad WAN link that drops packets and does not allow the registration to complete.
- Firewall issues. Ensure that the firewall allows traffic in both directions and that traffic to and from the correct ports is allowed to pass.

Incorrect FAR State in IoT FND

In IoT FND, a FAR might appear in a Down state even though you can ping and trace the route to it without a problem.

IoT FND manages the FAR via the IoT-DM service running on the FAR. So even though the FAR is pingable and reachable, it is important to verify that the jetty server and call home features are enabled on the FAR:

```
'show run callhome' should have 'enable' in the config and 'sh jvm status'
```

Mesh Endpoint Management Issues

This section presents common issues with ME management and possible resolutions.

Mesh Endpoints Not Registering with IoT FND

Verify that the MEs have joined the FAR and are pingable from IoT FND over IPv6. If they are pingable, verify the following:

- The clock is in sync.
- The DHCP server used by the MEs is programmed with the correct IoT FND IP address.
- The MEs are running an image compatible with the current version of IoT FND.
- If HSM is used, HSM must be online and responding correctly.

Licensing Issues

This section presents common issues with license management and possible resolutions.

Device Import Failure

The importing of devices into IoT FND is dependent on the number of allotted IoT FND server licenses.

Verify that your IoT FND server has the adequate license count available for the number and type of devices being imported into the IoT FND database.

Only unique device EIDs are allowed in IoT FND. Check that no one else imported this device EID in to IoT FND or is currently trying to import the same device EID. Verify that no other user is simultaneously importing the same device into IoT FND.

License File Upload Failure

An expired license file will cause an error. Check the license file validity and expiration date.