Operational Issues You May Encounter

This chapter explains some of the operational issues and possible resolutions.

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.

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 OS version is RHEL 8.x, then use **systemctl** command instead of the **service** command as given in the table.

RHEL Version	Command
8.x	`systemctl <status/start/restart/stop> cgms`
7.x	`service cgms <status/start/restart/stop>`

Note To check the OS version, run the following command:

```
cat /etc/os-release
```

If the IoT FND service does not start:

Step 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.

Note 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. is correct (see the System Requirements chapter).

Step 2 Verify that the JRE version installed on the server is correct. (See FND release notes).

Step 3 Verify that database migration was performed successfully.

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

If 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:

Step 1 Use the script: `/opt/cgms/bin/ encryption_util.sh`

Step 2 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 script:

```
/opt/cgms/bin/password_admin.sh
```

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 an IoT FND server and it does not join the cluster:

Step 1 Verify that your servers are on the same subnet, can ping each other, and share the same cluster name.

Step 2 Check the status of all members by running the script:

```
/opt/cgms/bin/print_cluster_view.sh
```

Step 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.

Step 4 Verify that all the cluster nodes are configured to use NTP (see Configuring NTP Service).

Step 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 following script on the IoT server as root.

```
/opt/cgms/bin/deinstall_cgms_watchdog.sh
```

Fallback URL When SSO Fails

Use the FND console URL as a fallback URL to configure the authentication settings when SSO login fails. The root users and the users with administrative privileges only can access the FND console URL.

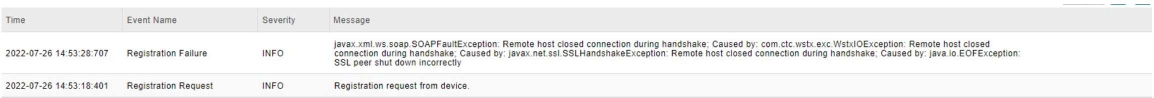
Table 1: Console URL

IoT FND Releases	Console URL
IoT FND Release 4.10.0	https://<FND-IP>/consolelogin.seam
IoT FND Releases 4.9.x and 4.8.x	https://<FND-IP>/console/home.seam

Note The FND console URL is not used for the IDP authentication.

Router Registration with IoT FND Fails over Cellular Network after Successful Tunnel Provisioning

Router registration with IoT FND fails with “SSL peer shutdown incorrectly” error over the cellular network after successful tunnel provisioning.



Time	Event Name	Severity	Message
2022-07-26 14:53:28:707	Registration Failure	INFO	javax.xml.ws.soap.SOAPFaultException: Remote host closed connection during handshake; Caused by: com.ctc.wstx.exc.WstxIOException: Remote host closed connection during handshake; Caused by: javax.net.ssl.SSLHandshakeException: Remote host closed connection during handshake; Caused by: java.io.EOFException: SSL peer shut down incorrectly
2022-07-26 14:53:18:401	Registration Request	INFO	Registration request from device.

The provisioned tunnels did not have the MTU set correctly for the cellular network. The MTU settings are on both sides of the tunnel; the HeadEnd Router (HER) and the Field Area Router (FAR).

On HER, the sample configuration below shows the settings required for MTU and MSS:

```
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
ip mtu 1300
ip tcp adjust-mss 1260
ipv6 unnumbered Loopback0
ipv6 enable
ipv6 mtu 1280
ipv6 tcp adjust-mss 1220
nat64 enable
tunnel source GigabitEthernet0/0/1
tunnel path-mtu-discovery
tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
ip tcp mss 1460
ip tcp path-mtu-discovery
!
```

On the FAR side, the sample configuration below shows the settings required for MTU and MSS:

```
interface Tunnel10
 description to HER
 no ip address
 ipv6 unnumbered Loopback0
 ipv6 mtu 1280
 ipv6 tcp adjust-mss 1240
 tunnel source Cellular0/3/0
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
```

```
interface Cellular0/3/0
 ip address negotiated
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip tcp adjust-mss 1390
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 dialer-group 1
 ipv6 enable
 pulse-time 1
!
ip tcp mss 1460
ip tcp path-mtu-discovery
```

The MTU settings above 1300 on cellular backhauls can cause the registration error message.

DB Migration fails due to Incorrect Incremental Size

During IoT FND upgrade to 4:10, DB migration fails due to incorrect incremental size. The database schema and IoT FND should match in order to avoid the failure during DB migrate, and hence the hibernate jars were upgraded in Cisco IoT FND 4.10.0. The following error message appears when the sequence name (for example, audit_trail_id_seq) in the db is not properly updated:

```
Current schema version: A.4.9.0.20220809.01
Migrating to version A.4.10.0.20230316.01
Migration completed. Successfully applied 1 migration.
07-18-2023 14:48:43 EDT: INFO: Migration completed.
07-18-2023 14:48:43 EDT: INFO: Performing post migration. This may take a while. Please
wait ...
2023-07-18 18:48:47,709:ERROR:main:CgmsDbMigrationDriver: Migration failed. Exception:
Reason :
javax.persistence.PersistenceException: [PersistenceUnit: common] Unable to build Hibernate

SessionFactory
at org.hibernate.jpa.boot.internal.EntityManagerFactoryBuilderImpl.persistenceException
(EntityManagerFactoryBuilderImpl.java:1336)
at org.hibernate.jpa.boot.internal.EntityManagerFactoryBuilderImpl.build
(EntityManagerFactoryBuilderImpl.java:1262)
at org.hibernate.jpa.HibernatePersistenceProvider.createEntityManagerFactory
(HibernatePersistenceProvider.java:56)
at javax.persistence.Persistence.createEntityManagerFactory(Persistence.java:55)
at com.cisco.cgms.tools.CommandLineInit.initDataSource(CommandLineInit.java:57)
at com.cisco.cgms.tools.CommandLineInit.<init>(CommandLineInit.java:26)
at com.cisco.cgms.tools.CgmsDbMigrationDriver.<init>(CgmsDbMigrationDriver.java:41)
at com.cisco.cgms.tools.CgmsDbMigrationDriver.main(CgmsDbMigrationDriver.java:93)
Caused by: org.hibernate.tool.schema.spi.SchemaManagementException: Schema-validation:
sequence [cgms_dev.audit_trail_id_seq] defined inconsistent increment-size; found [1000]
but exp ecting [1]
at org.hibernate.tool.schema.internal.AbstractSchemaValidator.validateSequence
(AbstractSchemaValidator.java:191)
at org.hibernate.tool.schema.internal.AbstractSchemaValidator.performValidation
(AbstractSchemaValidator.java:100)
at org.hibernate.tool.schema.internal.AbstractSchemaValidator.doValidation
(AbstractSchemaValidator.java:68)
at org.hibernate.tool.schema.spi.SchemaManagementToolCoordinator.performDatabaseAction
(SchemaManagementToolCoordinator.java:192)
at org.hibernate.tool.schema.spi.SchemaManagementToolCoordinator.process
(SchemaManagementToolCoordinator.java:73)
```

```
at org.hibernate.internal.SessionFactoryImpl.<init>(SessionFactoryImpl.java:316)
at
org.hibernate.boot.internal.SessionFactoryBuilderImpl.build(SessionFactoryBuilderImpl.java:469)
at org.hibernate.jpa.boot.internal.EntityManagerFactoryBuilderImpl.build
(EntityManagerFactoryBuilderImpl.java:1259)
... 6 more
2023-07-18 18:48:47,713:ERROR:main:CgmsDbMigrationDriver: Migration failed. Exception:
07-18-2023 14:48:47 EDT: ERROR: Post migration failed. See log file for more information.
```

Execute the following query in the DB:

```
DECLARE
seq_name VARCHAR2(100);
current_increment PLS_INTEGER;
BEGIN
FOR seq IN (SELECT sequence_name FROM all_sequences WHERE sequence_owner = 'CGMS_DEV') LOOP
seq_name := seq.sequence_name;
IF seq_name NOT IN ('CONFIG_GROUPS_ID_SEQ', 'FIRMWARE_GROUPS_ID_SEQ',
'NET_C8000_METRICS_ID_SEQ',
'NET_C8000_PROPERTIES_ID_SEQ', 'NET_LGLFN_METRICS_ID_SEQ','NET_LGLFN_PROPERTIES_ID_SEQ')
THEN
-- Get the current increment for the sequence
EXECUTE IMMEDIATE 'SELECT INCREMENT_BY FROM ALL_SEQUENCES WHERE SEQUENCE_NAME = :seq and
sequence_owner = ''CGMS_DEV'''
INTO current_increment
USING seq_name;

IF current_increment <> 1 THEN
-- If the current increment is not 1, update it to 1
EXECUTE IMMEDIATE 'ALTER SEQUENCE ' || seq_name || ' INCREMENT BY 1';
END IF;
END IF;
END LOOP;
END;
/
```