Troubleshooting Guide for Cisco IoT Field Network Director

First Published: 2020-08-20

Last Modified: 2023-07-21

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

Troubleshooting Guide for Cisco Field Network Director

This guide provides steps to troubleshoot both common IoT FND issues and specific IoT FND components.

Introduction

This guide applies to the following deployments in IoT FND:

- IoT FND Installation using Docker, PostgreSQL and InfluxDB
- IoT FND Installation using Oracle

Note Not all troubleshooting options noted in this document apply to both deployment types noted above.

- Troubleshooting Common IoT FND Issues
- Troubleshooting for Specific IoT FND Components
- Operational Issues You May Encounter
- FAR Management Issues
- Mesh Endpoint Management Issues
- Licensing Issues, on page 53

CHAPTER 2

Troubleshooting Common IoT FND Issues

This chapter explains some common IoT FND issues and the workaround for them.

Log Files

Note All log files are case-sensitive.

```
[root@iot-fnd ~]# ls -1 /var/lib/pgsql/9.6/data/pg_log/postgresql-*
/var/lib/pgsql/9.6/data/pg_log/postgresql-Fri.log
/var/lib/pgsql/9.6/data/pg_log/postgresql-Mon.log
/var/lib/pgsql/9.6/data/pg_log/postgresql-Sat.log
/var/lib/pgsql/9.6/data/pg_log/postgresql-Sun.log
/var/lib/pgsql/9.6/data/pg_log/postgresql-Thu.log
/var/lib/pgsql/9.6/data/pg_log/postgresql-Tue.log
/var/lib/pgsql/9.6/data/pg_log/postgresql-Wed.log
```

You can find the main FND log file at the following path:

```
/opt/cgms/server/cgms/logs/server.log
```

- For an OVA install, you can find the log file at:
  - `/opt/fnd/logs/server.log`

points to `/opt/cgms/server/cgms/logs` in the Docker container.

- `tail -f + grep`

  on serial is often handy as the logs are very verbose.

- For a PostgreSQL install, you can find the log file at:

  `/var/lib/pgsql/9.6/data/pg_log/postgresql-XXX.log`

  where XXX=day, for example XXX = Wed.log.

Note The PostgreSQL version may differ given the FND release and/or OVA release.

- For an Oracle install, you can find the log file at:

  `/home/oracle/app/oracle/diag/rdbms/cgms/cgms/trace/alert_cgms.log`

FND Debugging — How to Enable

To enable FND debugging, follow these steps:

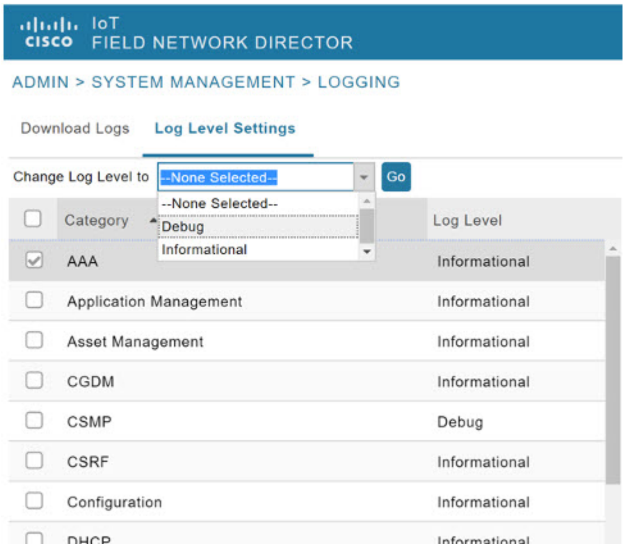
Option 1:

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

Step 2 In the screen that appears, select the **Log Level Settings** tab and then choose the **Debug** option from the drop-down menu (such as AAA as shown in Figure 1).

Step 3 Click the **Disk** icon to save (not shown).

Figure 1: Enabling Debug on FND (left-side of the screen)



Change Log Level to --None Selected--

--None Selected--
Debug
Informational

	Category	Log Level
☑	AAA	Informational
□	Application Management	Informational
□	Asset Management	Informational
□	CGDM	Informational
□	CSMP	Debug
□	CSRF	Informational
□	Configuration	Informational
□	DHCP	Informational

Step 4 **Option 2:**Choose **ADMIN** > **System Management** > **Logging**.

Step 5 Select the **Log Level Settings** tab.

Step 6 Enter the EIDs for each system such in the debugging panel on the right of the screen (Figure 2) such as:

IR829GW- LTE-GA-EK9+FGL204220HB

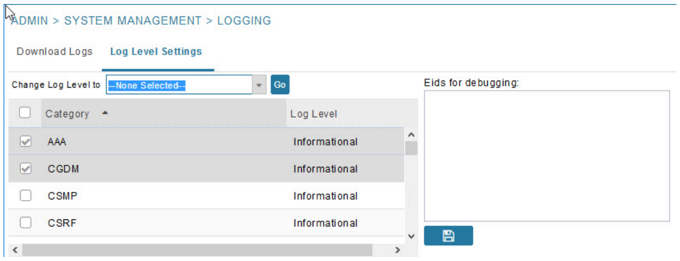
See Figure 3.

Step 7 Click the **Disk** icon to save. A separate file is created for each EID in the log location. To locate that file enter the commands below with the relevant EID.

```
[root@iot-fnd ~]# ls /opt/fnd/logs/I*
```

```
/opt/fnd/logs/IR829GW-LTE-GA-EK9+FGL204220HB.log
```

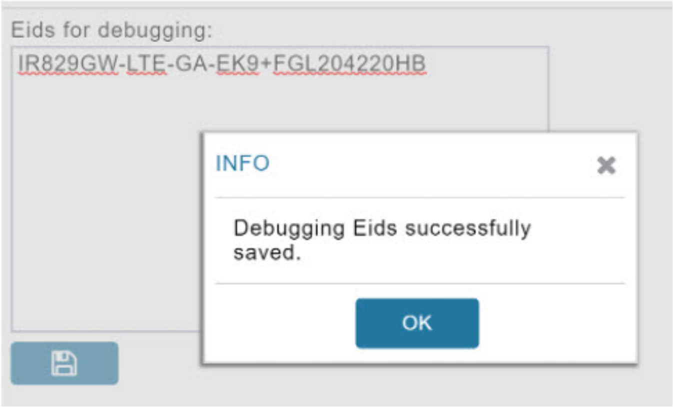
Figure 2: Entering EIDs



Change Log Level to --None Selected--

☐ Category	Log Level
☑ AAA	Informational
☑ CGDM	Informational
☐ CSMP	Informational
☐ CSRF	Informational

Figure 3: Populated EID panel



Eids for debugging:

IR829GW-LTE-GA-EK9+FGL204220HB

Debugging Eids successfully saved.

Access Docker Containers

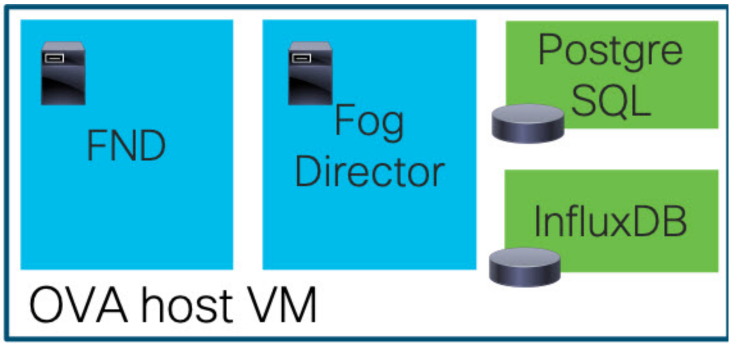
Step 1 To access FND or FD container shell (see Figure 5):

```
[root@iot-fnd ~]# docker exec -it fnd-container bash
[root@fnd-server /]#
```

Step 2 To copy files to and from containers (containers are not persistent):

```
[root@iot-fnd ~] # docker cp fnd-container:/opt/cgms/version.txt
[root@iot-fnd ~]# cat version.txt
JBoss Enterprise Application Platform - Version 6.2.0 GA
```

Figure 4: Access Docker Container



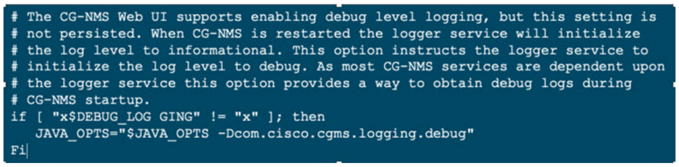
FND Debugging — Enable from FND Boot

Before you begin

You can enable debug logging from the start by setting an environment variable or by changing the cgms start script temporarily.

Step 1 To start the script, enter: `opt/cgms/bin/cgms`.

Figure 5: Example script for FND Debugging



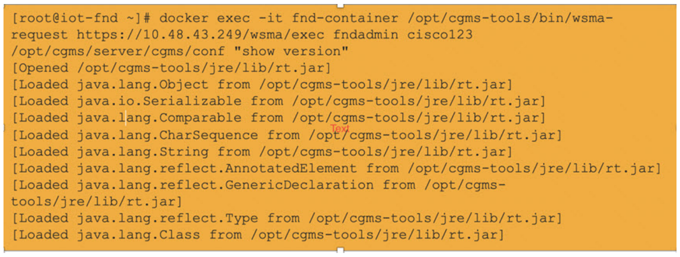
```
# The CG-NMS Web UI supports enabling debug level logging, but this setting is
# not persisted. When CG-NMS is restarted the logger service will initialize
# the log level to informational. This option instructs the logger service to
# initialize the log level to debug. As most CG-NMS services are dependent upon
# the logger service this option provides a way to obtain debug logs during
# CG-NMS startup.
if [ "x$DEBUG_LOG GING" != "x" ]; then
   JAVA_OPTS="$JAVA_OPTS -Dcom.cisco.cgms.logging.debug"
Fi
```

Step 2 Set DEBUG_LOGGING as non-empty. For example script, see Figure 4.

Java Debugging

To determine which JAR file (.jar) is causing issues, add Java option: -verbose:class as shown in the WSMA testscript example below:

```
java -verbose:class -Dlog4j.configuration=file:
$HOME/conf/log4j.properties =Dconf-dire=$HOME/conf
-classpath “$CLASSPATH” com.cisco.cgms.tools.WsmaSimClient “$@”
```



```
[root@iot-fnd ~]# docker exec -it fnd-container /opt/cgms-tools/bin/wsma-
request https://10.48.43.249/wsma/exec fndadmin cisco123
/opt/cgms/server/cgms/conf "show version"
[Opened /opt/cgms-tools/jre/lib/rt.jar]
[Loaded java.lang.Object from /opt/cgms-tools/jre/lib/rt.jar]
[Loaded java.io.Serializable from /opt/cgms-tools/jre/lib/rt.jar]
[Loaded java.lang.Comparable from /opt/cgms-tools/jre/lib/rt.jar]
[Loaded java.lang.CharSequence from /opt/cgms-tools/jre/lib/rt.jar]
[Loaded java.lang.String from /opt/cgms-tools/jre/lib/rt.jar]
[Loaded java.lang.reflect.AnnotatedElement from /opt/cgms-tools/jre/lib/rt.jar]
[Loaded java.lang.reflect.GenericDeclaration from /opt/cgms-
tools/jre/lib/rt.jar]
[Loaded java.lang.reflect.Type from /opt/cgms-tools/jre/lib/rt.jar]
[Loaded java.lang.Class from /opt/cgms-tools/jre/lib/rt.jar]
```

SSL Debugging

Set DEBUG_SSL to ‘true’ in `/opt/bin/cgms/bin/cgms.conf` as shown in the steps below:

```
[root@fnd bin]# cat opt/cgms/bin/cgms.conf
MAX_JAVA_HEAP_SIZE=8g
DEBUG_SSL=true
[root@fnd bin] service cgms restart
```

Common Errors

Listed below are some common errors that you may see during various stages of using IoT FND with suggested ways to resolve the problems.

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

Table 1: For CGMS

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

Similarly, use the systemctl command for TPS Proxy and SSM as well.

Table 2: For TPSPROXY

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

Table 3: For SSM

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

Table 4: For FND RA

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

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

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

Table 5: Common Errors

Common Errors	Items to Check and/or Resolve Errors
Checkpoint Failed.	Check the archive.
CiscoIosFileUploadException: Full error: Error occurred while verifying file upload operation for net element CGR1120/K9+FOC21255MYX	Check provisioning URL (HTTP, HTTPS) Check WSMA with test script: user and port
org.apache.cxf.interceptor.Fault: Connection refused (Connection refused)	Check port used for HTTPS communication (varies by platform). For example: • FAR: ip http secure-port 8443 • IR1101: ip http secure-port 443

Common Errors	Items to Check and/or Resolve Errors
PnP Service Error 3341 Full error: Error while creating FND trustpoint on the device. errorCode: PnP Service Error 3341, errorMessage: SSL Server ID check failed after cert-install	Check SAN field in the FND certificate: • Certificate which FND offers for PNP: https://10.48.43.229:9120/pnp/HELLO • Trustpoint which FND offers for PNP: Click to view the truspoint. For additional information, click to view the document: Enter the keystore command to list SAN fields on the certificate in the keystore used for PNP. This verifies the accuracy of the SAN field(s). keytool -list -v -keystore cgms_keystore | grep SubjectAlt -A3 Enter keystore password: keystore SubjectAlternativeName [IPAddress: 10.48.43.229]

Common Errors	Items to Check and/or Resolve Errors
PnP Service Error 1702 Full error: Error while deploying odm/config file on the device. errorCode: PnP Service Error 1702, errorMessage: I/O error	If error is seen, enable debug in FND for bootstrapping, Ensure that FAR is able to reach TPS or FND using its hostname. For example, in the below debug logs for FND bootstrapping, FAR should be able to resolve and reach iot-tps.example.cisco.com on 9120 and viceversa. [sev=DEBUG][tid=tunnelProvJetty-534][part=33728.4/16]: <fileTransfer> [sev=DEBUG][tid=tunnelProvJetty-534][part=33728.5/16]: <copy> [sev=DEBUG][tid=tunnelProvJetty-534][part=33728.6/16]: <source> [sev=DEBUG][tid=tunnelProvJetty-534][part=33728.7/16]: <location>https://iot-tps.example.cisco.com:9120/pnp/odm/IR829GW </location> [sev=DEBUG][tid=tunnelProvJetty-534][part=33728.8/16]: </source> [sev=DEBUG][tid=tunnelProvJetty-534][part=33728.9/16]: <destination> [sev=DEBUG][tid=tunnelProvJetty-534][part=33728.10/16]: <location>flash:/managed/odm/cg-nms.odm</location> [sev=DEBUG][tid=tunnelProvJetty-534][part=33728.11/16]: </destination>
java.lang.reflect. InnvocationTargetException. Full error description: PnP request for element ID [IR1101-K9+FCW223700AV] failed [java.lang.reflect.InvocationTargetException].	Check bootstrap configuration. If error is seen immediately after updating ODM: • Check provisioning settings in the user interface. • Check debug log for empty value for proxy-bootstrap-ip property field. • Must provide a valid IP address or hostname.
Could not generate DH keypair. Full error description: java.security.Invalid.AlgorithmParameterException: DH key size must be multiple of 64 and must be in the range of 512 to 2048 (inclusive). The specific key size 4096 is not supported.	Check: ip http secure-ciphersuite

Common Errors	Items to Check and/or Resolve Errors
Error: PKIX path building failed: sun.security.provider.certpath. SunCertPathBuilderException: unable to find valid certification path to requested target. Cause: Wrong certificate is offered through HTTPS-server on FAR.	Check the certificate for Web communication with IoT FND on the router (FAR): **1.** Check the configuration of the secure-transport: • Router# sh run | i secure-trustpoint • ip http secure-trustpoint LDevID • ip http client secure-trustpoint LDevID **2.** If the secure-transport configuration is correct, then restart https server on FAR: • router(config)# no ip http secure-server • router(config)# ip http secure-server

Common Errors	Items to Check and/or Resolve Errors
Error: PKIX path validation failed: java.security.cert.CertPathValidatorException: validity check failed. Cause: Wrong certificate is offered through HTTPS-server on FAR.	If this error is seen, then there is an issue with the certificate used for https communication between IoT FND and FAR. In certain situations, for example, if reload-during-bootstrap=true property is used in the cgms.properties file, then this error might be seen once, after which the tunnel formation is successful. This is because of the delay in obtaining the LDevID certificate after the router boots up. But the first tunnel formation request has already been sent before LDevID is obtained. So the first time failure of tunnel formation, this error message is seen. However, when the second tunnel formation request in sent, the LDevID has already been obtained by this time for the https communication and hence the tunnel formation is successful. Workaround: From IoT FND 4.6.x onwards, remove reload-during-bootstrap=true from the cgms.properties file, as this property was introduced as a workaround for CSCvk66991. **Note** CSCvk66991 is fixed now, hence this property is not mandatory from IoT FND 4.6.x onwards.

Common Errors	Items to Check and/or Resolve Errors
Error: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath. SunCertPathBuilderException: unable to find valid certification path to requested target Cause: Issuing CA certificate is missing in keystore.	Install Issuing CA cert.
Error in running file check command Full error: Error in running file check command: dir flash:/managed/odm/cg-nms.odm., Reason: javax.xml.ws.soap.SOAPFaultException: Serve D-H key verification failed	Add the following command to the file check: • ip http secure-client-auth • Check username and password or http conf.
Error during registration process: javax.xml.ws.WebServiceException: Could not send Message	Check WSMA. On the router (FAR), run debug: Router# debug ip http all
HTTP response '502: Bad Gateway' Full error: org.apache.cxf.transport.http.HTTPException: HTTP response '502:Bad Gateway' when communicating with https://10.48.43.249.443/wsma/config Error is typically seen with NGINX on IR1101. **Note** NGINX is a software-based web server. **Note** In most cases, the '502: Bad Gateway' error is related to http max-connections set in the command below. tunnel(config)# ip http max-connections 20 **Note** Should the value that you enter in the command (noted above) return an error, you can increase the value until the error goes away.	On the IR1101, check NGINX log by entering one of the commands: IR1101# show platform software trace message nginx RP active -or- You can find the latest nginx file in the directory: IR1101# dir bootflash/tracelogs/nginx* To copy the latest nginx file, use one of the following: Cisco IOS file operations such as SCP or TFTP.

Common Errors	Items to Check and/or Resolve Errors
Failed to load function 'CA InitRolePIN'Issue with (outdated) HSM Java libraries Full error: Failed to load function 'CA_InitSlotRolePIN' Failed to load function 'CA_...Failed to load function 'CA_DescribeUtilizationCounterId' Failed to load function 'CA TestTrace'	Backup/copy new libs to cgms or cgms-tools libs folder: [root@FNDPRDAPP01 bin]# cp -r /opt/cgms-tools/jre/lib/ext/opt/cgms-tools/jre/lib/ext-bc/ root@FNDPRDAPP01 bin]# cp /usr/safenet/lunaclient/jsp/lib/*/opt/cgms-tools/jre/lib/ext/
Reverse DNS (1 of 2) Nothing in FND log when running CGNA on FAR tcpdump does not show incoming traffic to FND Debugging CGNA/HTTP on FAR shows: cgna_httpc_post: http_send_request rc= 0 tid=55 cgna_prf timer_start:cg-nms-register:timer started Thu Jul 18 14:10:55 2019 httpc_request:Do not have the credentials cgna_http_resp_data: Received for sid=5 tid=55 status= 7	Debugging CGNA/HTTP on FAR should be (rather than the display to the left): cgna_httpc_post: http_send_request rc= 0 tid=114 cgna_prf timer_start:cg-nms-periodic: timer started Thu Jul 18 16:37:38 2019 httpc_request: Dont have the credentials Jul 18 16:37:40.844 UTC: Thu, 18 Jul 2019 14:37:40 GMT 10.48.43.251 http:10.48.43.299/cgna/ios/metrics ok Protocol = HTTP/1.1 Jul 18 16:37:40.844 UTC: Date =Thu, 18 Jul 2019 14:40:27 GMT cgna_http_resp_data: Received for sid= 4 tid=114 status=8
Reverse DNS (2 of 2) Every time FAR tries (http client) to create a TLS connection with FND, Java does a reverse DNS lookup of the source IP of the device. This is by design in Java. Apparently, for preventing DDoS attacks.	Remove DNS server or set the following in the cgms.properties: enable-reverse-dns-lookup=false (Addressed in CSCvk59944)

Common Errors	Items to Check and/or Resolve Errors
FND will not start (1 of 2) Symptom: FND stops suddenly or is unable to start on an Oracle installation where the database is installed locally.	Check the hard disk space using the command 'df-h' on the linux shell. If the disk is showing as 'full', most likely the Oracle DB archive logs have filled up the disk space and needs cleaning. Another reason could be that the database password has expired. Run the command to confirm: /opt/cgms/server/cgms/log/cgms_db_connection_test.log To change the password, become the oracle user and use the script provided in the Oracle RPM: su - oracle $ORACLE_BASE/cgms/scripts/change_password.sh
FND will not start (2 of 2) Symptom: FND service is up but GUI will not load.	Issue is mostly likely due to Linux firewall getting enabled. Disable firewall using the Linux CLI command: systemctl firewalld stop

Common Errors	Items to Check and/or Resolve Errors
After FND is upgraded to FND 4.8, the HSM Client to FND Server communication does not work and displays the following error message: ‘Could not get CsmpSignatureKeyStore instance. Please verify HSM connection. Exception: Object not found.’ The error above is seen in FND Deployments with HSM that are running with or without High Availability (HA).	This is an HSM library issue. HSM client is not sending right slot ID to the FND server. Hence, the customer will have to follow up with HSM support. ‘Could not get CsmpSignatureKeyStore instance. Please verify HSM connection. Exception: Object not found.’ (CSCvz59702) Although, the HSM client resides on the same Linux server, where the FND Application Server is also installed. The HSM client is not provided by HSM and not by Cisco. Only HSM has the expertise and visibility to the HSM code and the HSM support team can help fix this issue. FND uses SSM or HSM to store encrypted information and keys. If there is an issue with SSM or HSM, then FND will not initialize. The IoT FND component remains in Down state even if the FND application server is in UP state. In this case, when the SSM is used, then you can contact Cisco Support. They have the expertise and visibility to the code to help you resolve this issue. However, if the HSM client to server connection has issues, then the Thales/HSM vendor has the visibility and expertise to help resolve the issue.

Common Errors	Items to Check and/or Resolve Errors
CSMP certificate not displayed in IoT FND GUI during fresh install.	

Common Errors	Items to Check and/or Resolve Errors
	For a fresh install of IoT FND and HSM integration, the CSMP certificate appears in the FND UI only when an endpoint/meter is added to FND, irrespective of whether th emeter/endpoint is registered to FND or not. You can also add a dummy entry for meter/endpoint. If there is no real endpoint or meter to add at the point of testing CSMP certificate display. Apart from the CSMP certificate displayed in the GUI, you can also use the following methods to verify if IoT FND can access and retrieve the CSMP certificate from HSM: • **Method 1** Run the following command: cat /opt/cgms/server/cgms/log/server.log | grep -i HSM If you get the below message, then IoT FND and HSM communication is successful, and FND can retrieve the public key. %IOTFND-6-UNSPECIFIED: %[ch=HSMKeyStore][sev=INFO] [tid=MSC service thread 1-3]: Retrieved public key: 3059301306072a8648ce3d020106082a864 8ce3d03010703 420004d914167514ec0a110 f3170eef742a000572cea6f0285a3074db 87e43da398 ab016e40ca4be5b888c26c4 fe91106cbf685a04b0f61d599826bdbcff 25cf065d24 • **Method 2** Run the following command. The cmu list command checks if FND can see

Common Errors	Items to Check and/or Resolve Errors
	two objects stored in HSM partition, namely private keys and CSMP certificate. [root@iot-fnd ~]# cd /usr/safenet/lunaclient/bin [root@iot-fnd bin]# ./cmu list Certificate Management Utility (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved. Please enter password for token in slot 0 : ******* handle=2000001 label=NMS_SOUTHBOUND_KEY handle=2000002 label=NMS_SOUTHBOUND_KEY--cert0 You have new mail in /var/spool/mail/root
Error: Caused by FATAL: terminating connection due to idle-in-transaction timeout	**Note** This is applicable only to FND-Postgres ova deployments. Edit the idle_in_transaction_session_timeout property in postgresql.conf file. By default it is set to 3h. If any operation requires the transaction to be opened for more than 3h then on getting the above error, set the value for the idle_in_transaction_session_timeout property to more than 3h and restart Postgresql service for the property to take effect. **Note** • The postgresql.conf file is located in the path: /var/lib/pgsql/12/data. • The postgres version is 12. (replace this with the current version that you are using).

Common Errors	Items to Check and/or Resolve Errors
With IoT FND and HSM integration, the CSMP certificate will not load in IoT FND UI after the upgrade.	The inability of the certificate to load is mostly likely due to the upgrade process overwriting the old HSM client libraries (example: version 5.x) with the new client libraries (example: version 7.x or 10.x or higher) that are bundled with FND 4.4 and later releases. **Note** For more information on the HSM client version that is bundled with IoT FND, refer to the corresponding FND release notes. To restore the old libraries, perform the following on the Linux shell: cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar /opt/cgms/jre/lib/ext/ cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so /opt/cgms/jre/lib/ext/ cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar /opt/cgms/safenet/ cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so /opt/cgms/safenet/ To restore the tools package: cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar /opt/cgms-tools/jre/lib/ext cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so /opt/cgms-tools/jre/lib/ext cp /usr/safenet/lunaclient/jsp/lib/LunaProvider.jar /opt/cgms-tools/safenet/ cp /usr/safenet/lunaclient/jsp/lib/libLunaAPI.so /opt/cgms-tools/safenet/
ODM file will not update on the router Symptom: During Plug and Play (PnP) or ZTD, the ODM file on the router does not get updated, which results in failure to register the device.	Issue is most likely due to the following entry in the cgms.properties file: update-files-oncgr=false Either remove the entry above or change it to 'true' as shown below: update-files-oncgr=true

Common Errors	Items to Check and/or Resolve Errors
Any CGR running Cisco IOS 15.6.x will not register with FND 4.3 or newer release.	Problem occurs because the WPAN high-availability (HA) feature was introduced in FND 4.3. This feature requires a minimum Cisco IOS release of 15.7(M)4.

Common Errors	Items to Check and/or Resolve Errors
SSM certificate will not load.	After upgrading to FND 4.4 or newer versions, the SSM cert is no longer seen in the CSMP certificates page. This occurs because the web certificate is getting changed after every upgrade. The web cert is used for establishing secure communication with the SSM. This change was done as part of the security compliance in FND 4.4. and all subsequent releases of FND, which generates a unique web (browser) certificate upon install or upgrade. To fix, export the self-signed web certificate from FND GUI: **1.** Go to Admin > Certificates > web certificate tab. Use the base64 format. **2.** Transfer the file to the opt/cgms-ssm directory. **3.** Stop SSM service: service ssm stop. **4.** Enter cd /opt/cgms-ssm/bin. **5.** Execute: /ssm setup.sh. **6.** Select option 8 : Import a trusted certificate to SSM-Web keystore. **7.** Enter current ssm_web_keystore password: *ssmweb*. **8.** Enter the alias for import: *fnd*. **9.** Enter Certificate filename: /opt/cgms-ssm/certForWeb.pem. **10.** Start the SSM service: service ssm start.
Could not get CsmpSignatureKeyStore instance. Please verify HSM connection.	This is an HSM client library issue. The HSM client is not sending the correct slot ID to the FND server. Please follow up with HSM support.

Common Errors	Items to Check and/or Resolve Errors
fndserver1.test.com: %IOTFND-3-UNSPECIFIED: %[ch=CgmsAuthenticator][sev=ERROR] [tid=http-/0.0.0.0:443-4] [part=150156.1/55]: Exception when adding remote user to the db. fndserver1.test.com: %IOTFND-3-UNSPECIFIED: %[ch=CgmsAuthenticator][sev=ERROR] [tid=http-/0.0.0.0:443-4] [part=150156.2/55]: com.cisco.cgms.exceptions.AAAException: failed to decrypt stored shared secret	The IoT FND server certificate contents for HA setup is: • The Subject — Must have the FQDN of the VIP. Example: FNDSERVERVIP.TEST.COM • The Subject Alternative Name (SAN) — Added must include the FQDN of the VIP. Example: FNDSERVERVIP.TEST.COM (same as the subject) • The Subject Alternative Name — Must NOT have the individual server names. Example: It must not contain FNDSERVER1.TEST.COM, FNDSERVER2.TEST.COM

Zero Touch Deployment — Tunnel Provisioning

```
Received tunnel provisioning request from [IR1101-K9+FCW22520078]
Adding tunnel provisioning request to queue for FAR ID=
Provisioning tunnels on element [IR1101-K9+FCW22520078]
Retrieved current configuration of element [IR1101-K9+FCW22520078] before tunnel provisioning
Retrieved status of file [flash:/before-registration-config] on [IR1101-K9+FCW22520078].
File does not
exist
Retrieved status of file [flash:/before-tunnel-config] on [IR1101-K9+FCW22520078]. File
does not exist.
Copied running-config of [IR1101-K9+FCW22520078] to [flash:/before-tunnel-config]
Opened a NETCONF session with element [HTABT-TGOT-DC-RT1] at [163.88.181.2]
Sending [show interfaces | include Description: | Encapsulation | address is | line protocol
 | packets
input, | packets output, | Tunnel protection | Tunnel protocol| Tunnel source] to element
[HTABT-TGOT-DC-RT1]
Received response to [show interfaces | include Description: | Encapsulation | address is
| line
protocol | packets input, | packets output, | Tunnel protection | Tunnel protocol| Tunnel
source] from
element [HTABT-TGOT-DC-RT1]
Sending [show ip nhrp | include ^[0-9A-F]| Tunnel| NBMA] to element [HTABT-TGOT-DC-RT1]
Received response to [show ip nhrp | include ^[0-9A-F]| Tunnel| NBMA] from element
[HTABT-TGOT-DC-RT1]
Sending [show ipv6 nhrp | include ^[0-9A-F]| Tunnel| NBMA] to element [HTABT-TGOT-DC-RT1]
Received response to [show ipv6 nhrp | include ^[0-9A-F]| Tunnel| NBMA] from element
[HTABT-TGOT-DC-RT1]
Sending [show ipv6 interface | include address | protocol | subnet] to element
[HTABT-TGOT-DC-RT1]
Received response to [show ipv6 interface | include address | protocol | subnet] from element
[HTABT-TGOT-DC-RT1]
Closed NETCONF session with element [HTABT-TGOT-DC-RT1]
```

```
Obtained current configuration of element [HTABT-TGOT-DC-RT1] before tunnel provisioning
Configured tunnels on [IR1101-K9+FCW22520078]
Retrieved current configuration of element [IR1101-K9+FCW22520078] after tunnel provisioning.
Processed tunnel template for element [ASR1001+93UA2TVWZAR]. Time to process [5 ms].
Configured element [IR1101-K9+FCW223700AG] to register with IoT-FND at
[https://10.48.43.229:9121/cgna/ios/registration]
-OR -
Tunnel provisioning request for element [IR1101-K9+FCW22520078] failed
```

ZTD Easy Mode for PNP

```
[UPDATING_ODM]
[COLLECTING_INVENTORY]
[VALDIATING_CONFIGURATION]
[PUSHING_BOOTSTRAP_CONFID_FILE]
[CONFIGURING+STARTUP_CONFIG]
[APPLYING_CONFIG]
[TERMINATING_BS_PROFILE]
[BOOTSTRAP_DONE]
```

Zero Touch Deployment Steps — Log Entries for Plug and Play

```
Received pnp request from [IR1101-K9+FCW22520078]
state: NONE
state: CONFIGURING_HTTP_FOR_SUDI
state: CONFIGURED_HTTP_FOR_SUDI
state: CREATING_FND_TRUSTPOINT msgType: PNP_GET_CA
state: CREATING_FND_TRUSTPOINT msgType: PNP_WORK_REQUEST
state: AUTHENTICATING_WITH_CA
state: AUTHENTICATED_WITH_CA
state: UPDATING_TRUSTPOINT
state: UPDATED_TRUSTPOINT
state: UPDATING_ODM msgType: PNP_GET_ODM
state: UPDATING_ODM msgType: PNP_WORK_RESPONSE
state: UPDATING_ODM_VERIFY_HASH msgType: PNP_WORK_REQUEST
state: UPDATING_ODM_VERIFY_HASH msgType: PNP_WORK_RESPONSE
state: UPDATED_ODM msgType
state: COLLECTING_INVENTORY
state: COLLECTED_INVENTORY
state: VALIDATING_CONFIGURATION
state: VALIDATED_CONFIGURATION
state: PUSHING_BOOTSTRAP_CONFIG_FILE msgType: PNP_GET_BSCONFIG
state: PUSHING_BOOTSTRAP_CONFIG_FILE msgType: PNP_WORK_RESPONSE
state: PUSHING_BOOTSTRAP_CONFIG_VERIFY_HASH msgType: PNP_WORK_REQUEST
state: PUSHING_BOOTSTRAP_CONFIG_VERIFY_HASH msgType: PNP_WORK_RESPONSE
state: PUSHED_BOOTSTRAP_CONFIG_FILE
state: CONFIGURING_STARTUP_CONFIG
state: CONFIGURED_STARTUP_CONFIG
state: RELOADING
Updating PnP state to: [BOOTSTRAP_DONE]
[eid=IR1101-K9+FCW22520078][ip=91.91.91.10][sev=INFO][tid=tunnelProvJetty-263]: Status
updated
to:[bootstrapped]
```

ZTD Step by Step — Entries for IXM Registration

```
Got IGMA POST with authtype: CLIENT_CERT
Received registration request for LoRaWAN Gateway with eid: [IXM-LORA-800-H-V2+FOC20133FJQ]
Executing registration request for LoRaWAN Gateway with EID: [100082].Processing LoRa Gateway
Registration Request
Processing LoRaWAN Gateway Command...
Tunnel1 Ip and/or prefix not received from LoRa Gateway. Tunnel Ip may not be updated
properly.
Tunnel2 Ip and/or prefix not received from LoRa Gateway. Tunnel Ip may not be updated
properly.
Processed LoRaWAN Gateway Command...
Processing LoRa Gateway Configuration
Processing Post Configuration
Processing Packet Forwarder Installation
Processed Packet Forwarder Installation
LoRaWAN Gateway Registration Process Complete
```

ZTD Step by Step — Log Entries for IXM Tunnel

```
Received Tunnel Prov Request for LoRaWAN Gateway with eid: [IXM-LORA-800-H-V2+FOC20133FJQ]
Checking if file:[before-registration-config] exist. Delete if Present. Tunnel Reprovisioning
 Request
File [before-tunnel-config] not found on the element. Creating the file.
Processed LoRaWAN Gateway Tunnel Provisioning
```

ZTD Step by Step — Log Entries for Registration

```
Received registration request from element: [IR1101-K9+FCW22520078]
Element IR1101-K9+FCW22520078 is running supported firmware version 16.10.01.
Continuing with element configuration
Retrieved status of file [flash:/before-registration-config] on [IR1101-K9+FCW22520078].
File does not
exist.
Copied running-config of [IR1101-K9+FCW22520078] to [flash:/before-registration-config]
Successfully deactivated the cgna registration profile and copied the running-config to
start-up config
for the element IR1101-K9+FCW22520078
Completed configuration of element [IR1101-K9+FCW22520078]
Registration phase completed for element [IR1101-K9+FCW22520078]
```

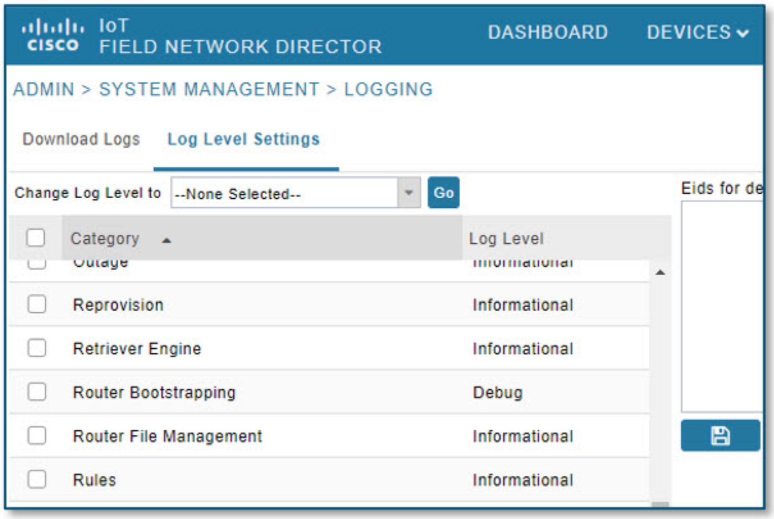
CHAPTER 3

Troubleshooting for Specific IoT FND Components

This chapter explains some of the component-specific IoT FND issues and possible resolutions.

Troubleshoot PNP

Figure 6: ADMIN > SYSTEM MANAGEMENT > LOGGING > Log Level Settings



Change Log Level to: --None Selected--

□	Category ▲	Log Level
□	Outage	Informational
□	Reprovision	Informational
□	Retriever Engine	Informational
□	Router Bootstrapping	Debug
□	Router File Management	Informational
□	Rules	Informational

Step 1 Check the FND-server logs by doing the following:

a. Increase the log level: Choose **ADMIN** > **SYSTEM MANAGEMENT** > **LOGGING**.

b. Select the **Log Level Settings** tab.

c. Select the box next to the **Router Bootstrapping** option; and, select the **Debug** option from the **Change Log Level to** drop-down menu.

d. Click **Go**.

You can find the generated logs in the following location:

`opt/cgms/server/cgms/logs/server.log (RPM) and opt/fnd/logs/server.log (OVA)`

Step 2 Debug on FAR by entering the following commands:

```
debug pnp
debug ip http client
```

Step 3 Check certificates and the ‘fnd’ trustpoint.

Step 4 Check provisioning link in settings.

Step 5 Check archive configuration and directory.

Troubleshooting Steps to Upload ODM File

At times, during the periodic metrics refresh, the IoT FND UI fails to provide the device metrics updates due to the absence of the ODM file (`cg-nms.odm`). To resolve this issue, you can download the `cg-nms.odm` file from the FND server and upload the file to the `/managed/odm` folder of the device from the Device File Management page of the FND UI.

- Download device-specific ODM file from FND server, on page 29
- Upload the ODM File from FND UI, on page 30

Note This workaround is applicable to all Cisco IOS and IOS-XE device types that FND supports.

Download device-specific ODM file from FND server

To download device-specific ODM file from FND server:

Step 1 Log in to the FND server through SSH.

Step 2 Go to the folder location `/opt/cgms/standalone/deployments` and copy the `cgms.ear` file into a separate folder (example: `/opt/cgms-ear`).

```
cp cgms.ear /opt/cgms-ear
```

Step 3 Change directory to `/opt/cgms-ear`.

```
cd /opt/cgms-ear
```

Step 4 Unzip the `cgms.ear` file.

```
 unzip cgms.ear
```

Step 5 Copy the `cgms-odms.jar` file from this folder into a separate folder, (example: `/opt/cgms-odms`).

```
cp cgms-odms.jar /opt/cgms-odms
```

Step 6 Change directory to `/opt/cgms-odms`.

```
cd /opt/cgms-odms
```

Step 7 Unzip the `cgms-odms.jar` file.

```
unzip cgms-odms.jar
```

Step 8 The ODM files are present in the following location.

```
/opt/cgms-odms/META-INF/odm
```

To list the ODM files, run the following command:

```
[root@iot-fnd-oracle odm]# ls -lrt
total 468
-rw-r--r-- 1 root root 19867 Jul  4 20:31 cg-nms-sbr.odm
-rw-r--r-- 1 root root 67648 Jul  4 20:31 cg-nms.odm
-rw-r--r-- 1 root root 66339 Jul  4 20:31 cg-nms-ir8100.odm
```

```
-rw-r--r-- 1 root root 71472 Jul  4 20:31 cg-nms-ir800.odm
-rw-r--r-- 1 root root 57578 Jul  4 20:31 cg-nms-ir1800.odm
-rw-r--r-- 1 root root 57537 Jul  4 20:31 cg-nms-ir1100.odm
-rw-r--r-- 1 root root 16884 Jul  4 20:31 cg-nms-ie4010.odm
-rw-r--r-- 1 root root 16884 Jul  4 20:31 cg-nms-ie4000.odm
-rw-r--r-- 1 root root 26950 Jul  4 20:31 cg-nms-esr5900.odm
-rw-r--r-- 1 root root 26776 Jul  4 20:31 cg-nms-c800.odm
-rw-r--r-- 1 root root  8916 Jul  4 20:31 cg-nms-ap800r.odm
-rw-r--r-- 1 root root  8658 Jul  4 20:31 cg-nms-ap800.odm
[root@iot-fnd-oracle odm]#
```

Note The default `cg-nms.odm` file in the above list is for CGR1000 device type.

Step 9 Rename the device-specific odm file (example: `cg-nms-ir1100.odm`) to `cg-nms.odm` in a specific directory (example: `/opt/cgms-odms/odm-ir1100`) before uploading the file into the IoT FND UI.

What to do next

Upload the ODM File from FND UI, on page 30

Upload the ODM File from FND UI

To upload the ODM file from FND UI:

Note Ensure that the ODM file renamed as `cg-nms.odm` is available in your PC.

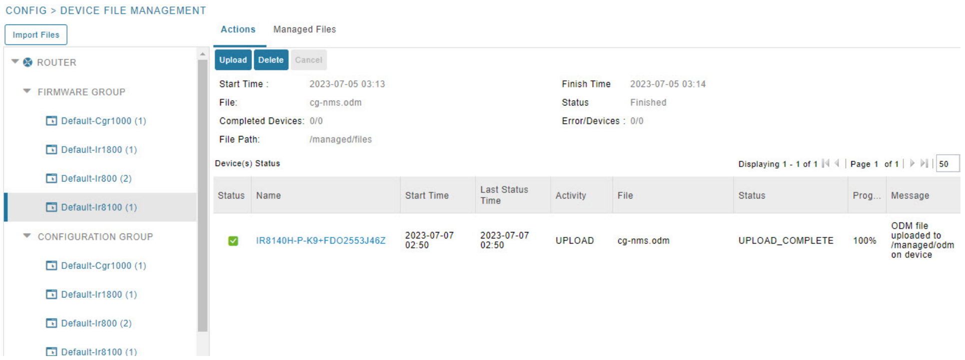
Before you begin

Download device-specific ODM file from FND server, on page 29.

Step 1 Log in to IoT FND UI using a browser.

Step 2 Navigate to **CONFIG** > **Device File Management** page.

Step 3 In the Device File Management page, select the **Actions** tab and click **Upload**.



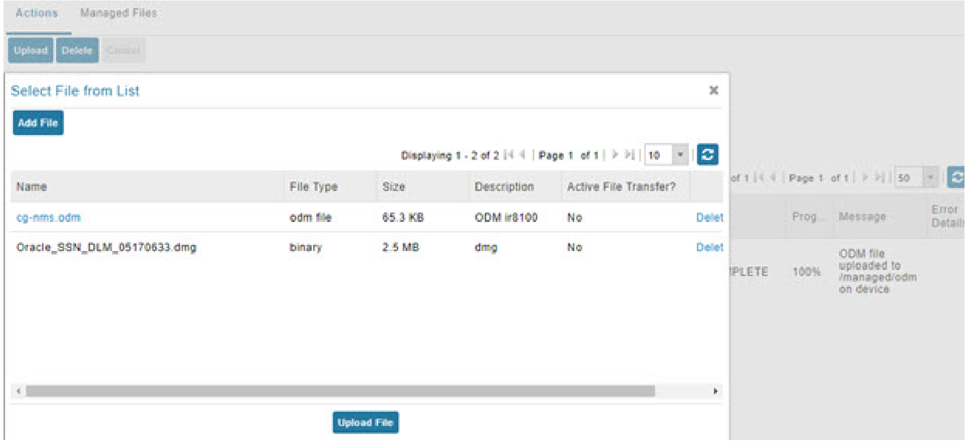
Start Time : 2023-07-05 03:13
File: cg-nms.odm
Completed Devices: 0/0
File Path: /managed/files
Finish Time 2023-07-05 03:14
Status Finished
Error/Devices : 0/0

Device(s) Status

Displaying 1 - 1 of 1 | Page 1 of 1 | 50

Status	Name	Start Time	Last Status Time	Activity	File	Status	Prog...	Message
✓	IR8140H-P-K9+FDO2553J46Z	2023-07-07 02:50	2023-07-07 02:50	UPLOAD	cg-nms.odm	UPLOAD_COMPLETE	100%	ODM file uploaded to /managed/odm on device

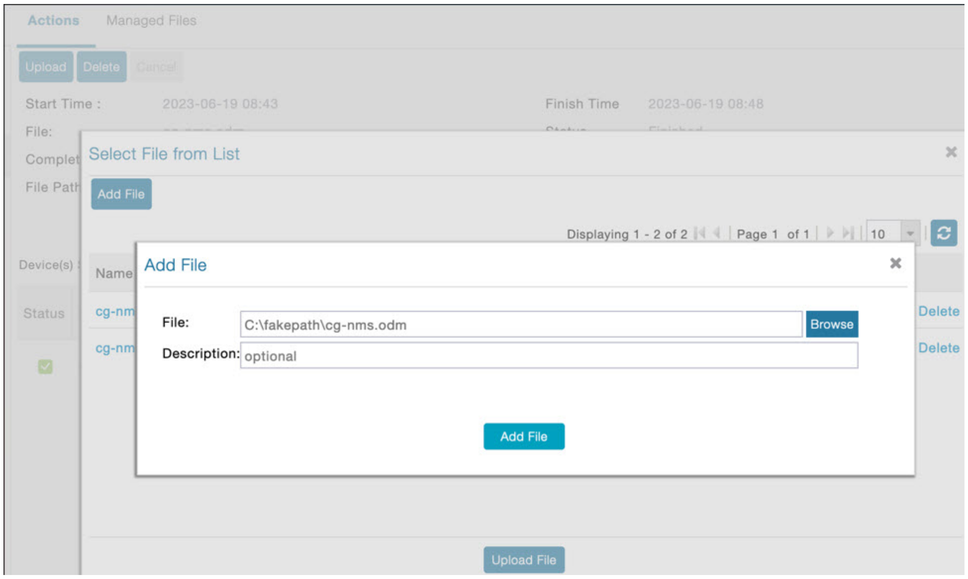
Step 4 In the **Select File from List** window, click **Add File**.



Name	File Type	Size	Description	Active File Transfer?	
cg-nms.odm	odm file	65.3 KB	ODM ir8100	No	Delet
Oracle_SSN_DLM_05170633.dmg	binary	2.5 MB	dmg	No	Delet

IPLETE 100% ODM file uploaded to /managed/odm on device

Step 5 Browse to the ODM file path (`cg-nms.odm`) and click **Add File** and then **Upload File**.



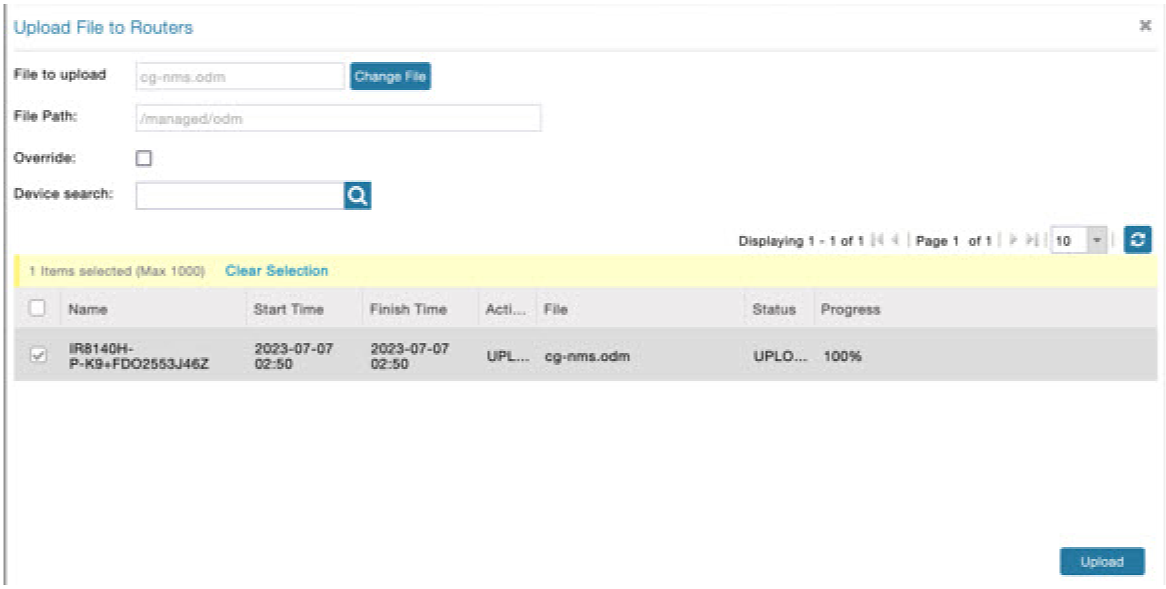
Start Time : 2023-06-19 08:43
Finish Time 2023-06-19 08:48
File:

Add File

File: C:\fakepath\cg-nms.odm

Description: optional

Step 6 Select the check box of the device(s) in the **Upload File to Routers** window and click **Upload**.



File to upload: cg-nms.odm

File Path: /managed/odm

Override: □

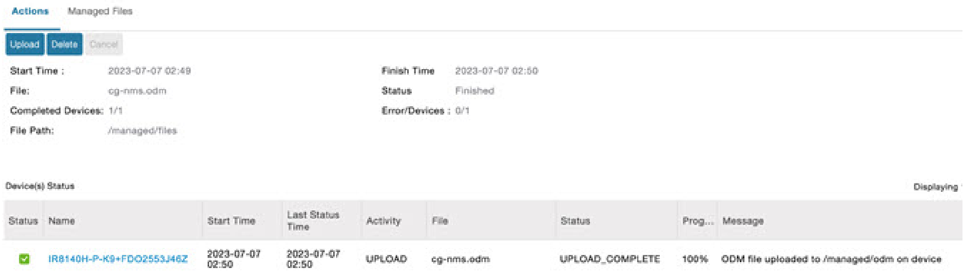
Device search:

Displaying 1 - 1 of 1 | Page 1 of 1 | 10

1 Items selected (Max 1000)

☐	Name	Start Time	Finish Time	Acti...	File	Status	Progress
☑	IR8140H-P-K9+FDO2553J46Z	2023-07-07 02:50	2023-07-07 02:50	UPL...	cg-nms.odm	UPLO...	100%

On successful completion of the upload, the Device Status table displays the upload completion message as shown below.



Start Time : 2023-07-07 02:49

File: cg-nms.odm

Completed Devices: 1/1

File Path: /managed/files

Finish Time 2023-07-07 02:50

Status Finished

Error/Devices : 0/1

Device(s) Status

Displaying

Status	Name	Start Time	Last Status Time	Activity	File	Status	Prog...	Message
✓	IR8140H-P-K9+FDO2553J46Z	2023-07-07 02:50	2023-07-07 02:50	UPLOAD	cg-nms.odm	UPLOAD_COMPLETE	100%	ODM file uploaded to /managed/odm on device

Note Only the `cg-nms.odm` file gets uploaded to the `/managed/odm` folder, while the other files get uploaded to the `/managed/files` folder.

Troubleshoot TCL Scripts

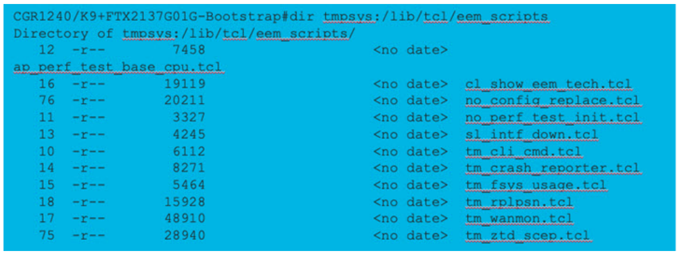
You can find the TCL scripts on a FAR at: `tmpsys:/lib/tcl/eem_scripts`.

Step 1 Debug using the `debug event manager tcl` commands.

Step 2 List planned scripts: `sh event manager statistics` policy.

Step 3 Manual execution: `event manager run tm_ztd_scep.tcl`.

Figure 7: Supported Troubleshooting TCL Scripts



```
CGR1240/K9+FTX2137G01G-Bootstrap#dir tmpsys:/lib/tcl/eem_scripts
Directory of tmpsys:/lib/tcl/eem_scripts/
   12  -r--        7458                         <no date>
ap_perf_test_base_cpu.tcl
   16  -r--       19119                         <no date>  cl_show_eem_tech.tcl
   76  -r--       20211                         <no date>  no_config_replace.tcl
   11  -r--        3327                         <no date>  no_perf_test_init.tcl
   13  -r--        4245                         <no date>  sl_intf_down.tcl
   10  -r--        6112                         <no date>  tm_cli_cmd.tcl
   14  -r--        8271                         <no date>  tm_crash_reporter.tcl
   15  -r--        5464                         <no date>  tm_fsys_usage.tcl
   18  -r--       15928                         <no date>  tm_rplpsn.tcl
   17  -r--       48910                         <no date>  tm_wanmon.tcl
   75  -r--       28940                         <no date>  tm_ztd_scep.tcl
```

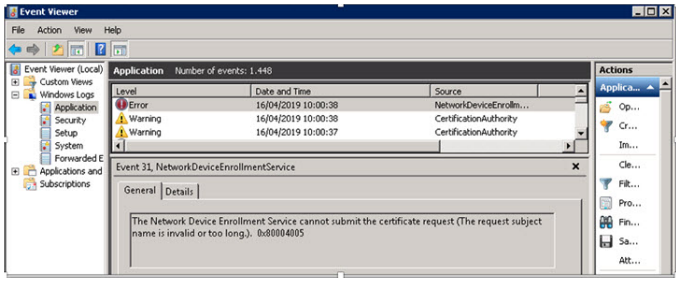
Troubleshoot Certificate Enrollment

Debug EEM and TCL on a FAR by entering the following command:

```
event manager environment ZTD_SCEP_Debug TRUE
```

- Manually perform trustpoint authentication and enrollment.
- Check Time and NTP
- Check NDES logs

Figure 8: Event Viewer



Application Number of events: 1.448

Level	Date and Time	Source
Error	16/04/2019 10:00:38	NetworkDeviceEnrollm...
Warning	16/04/2019 10:00:38	CertificationAuthority
Warning	16/04/2019 10:00:37	CertificationAuthority

Event 31, NetworkDeviceEnrollmentService

The Network Device Enrollment Service cannot submit the certificate request (The request subject name is invalid or too long.). 0x80004005

Certificate Enrollment — Test Manual

Step 1 Save the current crypto config:

```
FGL204220HB# sh run | s crypto pki profile enrollment LDevID
```

```
FGL204220HB# sh run | s crypto pki trustpoint LDevID
```

Step 2 Remove crypto trustpoint in order to reset state and remove certificates:

```
no crypto pki trustpoint LDevID
```

Step 3 Re-add the saved configuration:

```
configure terminal
FGL204220HB# sh run | s crypto pki profile enrollment LDevID
FGL204220HB# sh run | s crypto pki trustpoint LDevID
```

Step 4 Authenticate with SCEP:

```
crypto pki authenticate LDevID
```

Step 5 Request Certificate:

```
crypto pki enroll LDevID
```

Certificate Enrollment — Example Output

```
CGR1120/K9+FOC21255M(config)#crypto pki authenticate LDevID
Certificate has the following attributes:
Fingerprint MD5: 438C8EB4 145564EF 4BACAFDB E5A338BB
Fingerprint SHA1: 0CF137AC F108235C F7125434 A0383728 852508D5
Trustpoint Fingerprint: 0CF137AC F108235C F7125434 A0383728 852508D5
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
CGR1120/K9+FOC21255M(config)#crypto pki enroll LDevID
%
% Start certificate enrollment...
% The subject name in the certificate will include: serialNumber=PID:CGR1120
SN:xxxxxxxxxx,CN=yyyyyyyyy
% The fully-qualified domain name will not be included in the certificate
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose LDevID' command will show the fingerprint.
CGR1120/K9+FOC21255M(config)#
Mar 21 08:13:38.475 UTC: CRYPTO_PKI: Certificate Request Fingerprint MD5: 34AE797C E6A9DB7E
 8EAA43E8
DC50CC45
Mar 21 08:13:38.475 UTC: CRYPTO_PKI: Certificate Request Fingerprint SHA1: F79DD9C7 015B8B7D
 E37130B7
543F2721 330E235C
Mar 21 08:13:43.201 UTC:%PKI-6-CERTRET: Certificate received from Certificate Authority
```

Troubleshoot WSMA

Before you begin

You must have cgms-tools installed before you can troubleshoot WSMA.

Step 1 To execute:

```
/opt/cgms-tools/bin/wsma-request https://10.48.43.249:443/wsma/exec fndadmin cisco123
/opt/cgms/server/cgms/conf "show version | format flash:/managed/odm/cg-nms.odm"
```

Step 2 For an OVA install:

```
docker exec -it fnd-container /opt/cgms-tools/bin/wsma-request https://<FAR IP>:443/wsma/exec
<username> <password> /opt/cgms/server/cgms/conf "show version | format flash:/managed/odm/cg-nms.odm"
```

```
Example Output:
[root@iot-fnd ~]# docker exec -it fnd-container /opt/cgms-tools/bin/wsma-request
https://10.48.43.249/wsma/exec fndadmin cisco123 /opt/cgms/server/cgms/conf "show version | format
flash:/managed/odm/cg-nms.odm"
sending command: show version | format flash:/managed/odm/cg-nms.odm
<?xml version="1.0" encoding="UTF-8"?>
<ShowVersion xmlns="ODM://bootflash:/managed/odm/cg-nms.odm//show_version">
<Version>17.01.01</Version>
<VersionNonXe>17.1.1</VersionNonXe>
<HostName>IR1101</HostName>
<Uptime>1 week, 6 days, 3 hours, 3 minutes</Uptime>
<SystemImageFile>&quot;bootflash:ir1101-universalk9.17.01.01.SPA.bin&quot;</SystemImageFile>
<ReloadReason>Reload Command</ReloadReason>
<HardwareRevision>1.2 GHz</HardwareRevision>
<ProcessorBoardId>FCW223700AV</ProcessorBoardId>
<FastEthernetIntfCnt>4</FastEthernetIntfCnt>
<GigabitEthernetIntfCnt>2</GigabitEthernetIntfCnt>
<LicenseUdiTable>
</LicenseUdiTable></ShowVersion>
```

Troubleshoot Tunnel Provisioning

Step 1 Substitute variables in the Router Tunnel Addition template (Figure 9) and check if the configuration is valid.

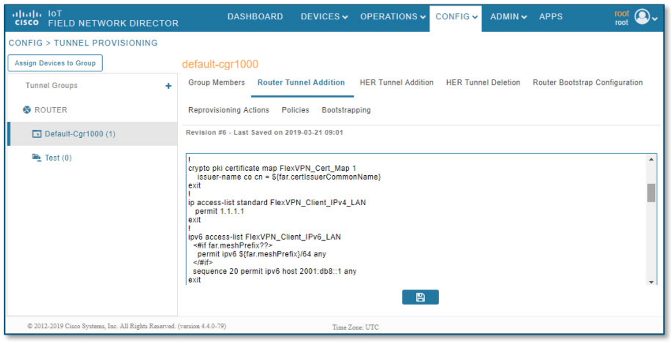
Step 2 Check server.log and optionally increase the log level.

Step 3 Check the head-end router (HER) Flex VPN.

Step 4 Debug on FAR using the following commands:

```
debug crypto sess
debug crypto ikev2
debug crypto ipsec
```

Figure 9: CONFIG > Tunnel Provisioning



Revision #6 - Last Saved on 2019-03-21 09:01

```
!
crypto pki certificate map FlexVPN_Cert_Map 1
   issuer-name co cn = ${far.certIssuerCommonName}
exit
!
ip access-list standard FlexVPN_Client_IPv4_LAN
  permit 1.1.1.1
exit
!
ipv6 access-list FlexVPN_Client_IPv6_LAN
  <#if far.meshPrefix??>
   permit ipv6 ${far.meshPrefix}/64 any
  </#if>
  sequence 20 permit ipv6 host 2001:db8::1 any
exit
```

© 2012-2019 Cisco Systems, Inc. All Rights Reserved. (version 4.4.0-79)
Time Zone: UTC

Troubleshoot Netconf: FND—HER Communications

Step 1 Start netconf session:

```
[root@iot-fnd ~]# ssh -l admin 10.48.43.228 -s netconf
Password:
```

Step 2 Device sends hello:

```
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
<capability>urn:ietf:params:netconf:capability:writeable-running:1.0</capability>
<capability>urn:ietf:params:netconf:capability:startup:1.0</capability>
<capability>urn:ietf:params:netconf:capability:url:1.0</capability>
<capability>urn:cisco:params:netconf:capability:pi-data-model:1.0</capability>
<capability>urn:cisco:params:netconf:capability:notification:1.0</capability></capabilities><session-id>2036979584</session-id></hello>]]>]]>
```

Step 3 Send a hello yourself:

```
<?xml version=”1.0″ encoding=”UTF-8″?>

<hello>

<capabilities>

<capability>urn:ietf:params:netconf:base:1.0</capability>

</capabilities>

</hello>]]>]]>
```

Step 4 Request running config (for example):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<ns2:rpc xmlns:ns2="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1">

<ns2:get-config>

<source>

<ns2:running/>

</source>

</ns2:get-config>

</ns2:rpc>]]>]]>
```

Step 5 Device Response:

```
<?xml version=”1.0" encoding="UTF-8"?><rpc-reply message-id="1"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><data><cli-config-data-block>!

! Last configuration change at 16:10:25 UTC Thu Apr 4 2019 by admin

! NVRAM config last updated at 16:20:47 UTC Thu Apr 4 2019 by admin

!
```

```
version 16.3

service timestamps debug datetime msec

service timestamps log datetime msec

no platform punt-keepalive disable-kernel-core

platform console auto

!

hostname fnd4her
```

Troubleshoot Configuration Deployment

Step 1 Substitute configuration and try manually line by line:

Step 2 Check device events: **Devices** > **Inventory** > **Select Device**.

Step 3 Debug CGNA/WSMA:

```
show cgna profile-state all
debug cgna logging ?
debug wsma agent
```

Troubleshoot HSM Connectivity

To troubleshoot HSM connectivity:

```
[root@FNDPRDAPP01 bin]# /opt/cgms-tools/bin/signature-tool print

Certificate:

Data:

Version: 1

Serial Number: xxxxxxxxxx

Signature Algorithm: SHA256withECDSA

Issuer: CN=CGNMS, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US

Validity

Not Before: Tue Feb 19 19:10:29 ICT 2019

Not After: Fri Feb 19 19:10:29 ICT 2049

Subject: CN=CGNMS, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US
```

```
Fingerprints:

MD5: 4D:BB:C7:7A:02:2D:74:E5:99:62:AC:92:4A:8D:01:66

SHA1: 9B:C5:8F:BF:0B:7D:BF:4E:5F:E1:DB:8D:86:FC:8C:D0:C9:A1:F3:BA

Subject Public Key Info:

Public Key Algorithm: EC

…

Signature Algorithm: SHA256withECDSA
```

Issues Faced During HSM Client Upgrade

IoT FND accesses the HSM Server using the HSM Client.

In order for IoT FND to access the HSM Server, the HSM Client corresponding to the HSM Server version must be installed on the Linux server where the IoT FND application server is installed.

IoT FND is integrated with the HSM Client by using the HSM client API. The HSM client assigns a slot number to the HSM Server and also to the HA Group. On HSM Client 5.4 or earlier, the slot numbering started from one (1). However, in HSM Client 6.x and later, the slot numbering starts from zero (0).

Note IoT FND gets the slot value dynamically from the HSM Client API. Sometimes during an upgrade from 5.4 to 7.3, the slot ID change is not dynamically populated. (CSCvz38606).

Note HSM Client 5.4 uses slot ID 1 (one). However, HSM Client 6.x and onward, slot ID 0 (zero) is used by the HSM client. The IoT FND application gets the value of the slot ID dynamically from the HSM client. The slot ID change will be communicated to the FND server by the HSM Client API upon restart of the IoT FND application. However, in some cases, the HSM client fails to send the correct value of the slot to the FND application server.

In such cases, where the FND Application Server has a value of 1 for the slot ID, but the HSM Client is using slot 0, and the HSM Client API is not giving the correct value dynamically, we can set the slot ID manually to one (1) in the HSM Client configuration file -/etc/Chrystoki.conf with the below:

```
Presentation = {OneBaseSlotID=1;}
```

CHAPTER 4

FAR Management Issues

This chapter explains some of the FAR management issues and workaround for them.

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 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`

CHAPTER 5

Mesh Endpoint Management Issues

This chapter explains some of the mesh endpoint issues and possible resolutions.

Mesh Endpoints Not Registering with IoT FND

Verify that the mesh endpoints 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 mesh endpoints is programmed with the correct IoT FND IP address.
- The mesh endpoints are running an image compatible with the current version of IoT FND.
- If HSM is used, HSM must be online and responding correctly.

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	N/A
REASON_COLDSTART	1	coldBoot	INFO	Mesh node registered due to cold boot.	This message includes the new IP address of the mesh endpoint.

Registration Reason Code	Code	Event Type Name	Severity	Message	Description
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	This message includes the new IP address of the mesh endpoint.
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	nmsNMSAddrChange	INFO	Mesh node registered due to manual NMS address change.	Endpoint received an error from IoT FND.
REASON_NMS_ERROR	6	nmsError	INFO	Mesh node registered due to NMS error.	Endpoint received an error from IoT FND.

Reasons for Mesh Endpoint WPAN Changes

In addition to generating events when mesh endpoints 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,
evenMessage=WPAN change due to migration to better
PAN: [lastChanged: 0, lastChangedReason: 4],
NetElement, id=10044,
EventType, name=null, lat=1000.0,
lng=1000.0, geoHash=null)
```

Table 6: 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.

Registration Reason Code	Code	Event Name	Severity Type	Description
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 mesh endpoint left the network to when it rejoined. IoT FND displays the amount of time the mesh endpoint was offline since the event was logged (for example, 4 hours 23 minutes ago).

CHAPTER 6

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.

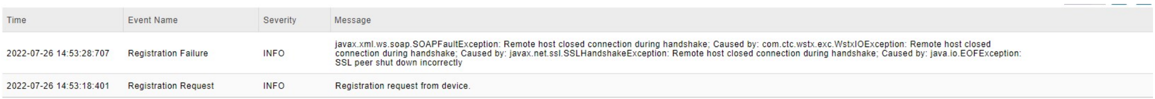
Table 7: Console URL

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;
/
```

Missing Endpoint Marker Line to CGR

If the FND is directly upgraded from version 4.6.1 to 4.8.1 by skipping the version 4.7.1, the location details are missing in the ROOT CAMs.

To manually add the location details:

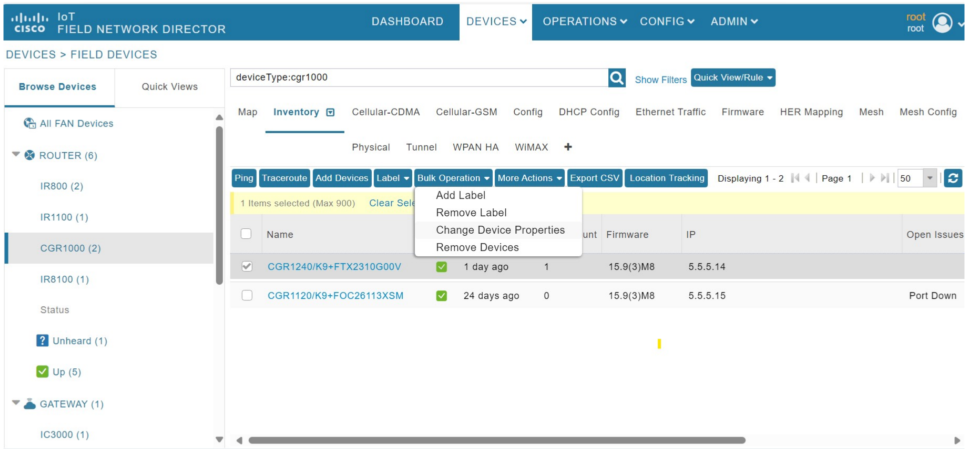
Step 1 Choose **DEVICES** > **Field Devices**.

Step 2 Select the **Browse Devices** tab from the left pane.

Step 3 Select **CGR1000** from the Router list and select the **Inventory** tab.

Step 4 Select the appropriate CGR check box.

Step 5 Click the **Bulk Operation** drop-down menu and select **Change Device Properties** option.



deviceType:cgr1000

	Name			unt	Firmware	IP	Open Issues
☑	CGR1240/K9+FTX2310G00V	✓	1 day ago	1	15.9(3)M8	5.5.5.14	
□	CGR1120/K9+FOC26113XSM	✓	24 days ago	0	15.9(3)M8	5.5.5.15	Port Down

Step 6 Add the cam device latitude and logitude manually in the csv file.

Step 7 Click **Change** to upload the csv file.

CHAPTER 7

Licensing Issues

This chapter explains some of the license issues and the 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 into 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.