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:

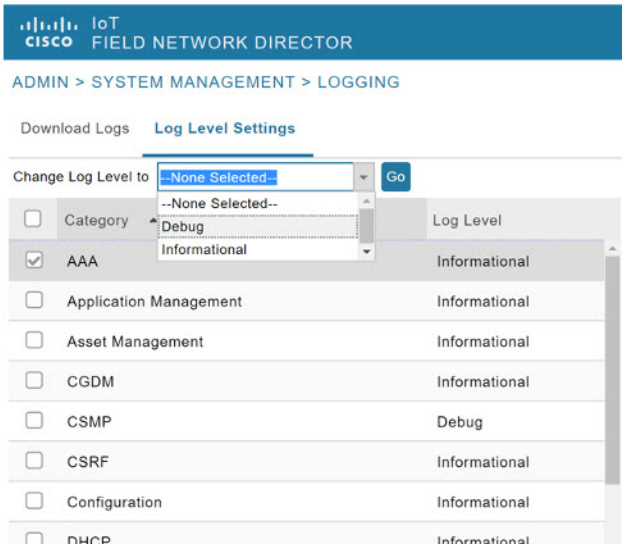
Option 1:

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)



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

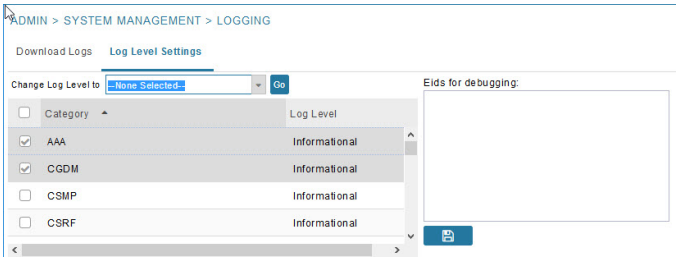
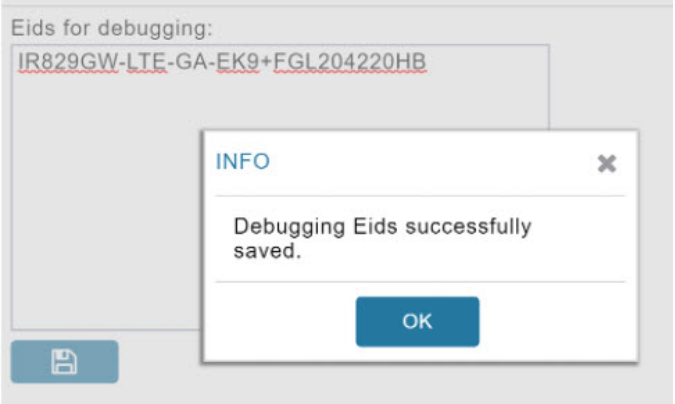


Figure 3: Populated EID panel



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]
```