

Troubleshooting Common IoT FND Issues

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

- Access Docker Containers, on page 1
- Common Errors, on page 2
- Troubleshoot Influx event migration to Postgres, on page 18
- FND Debugging — How to Enable, on page 20
- FND Debugging — Enable from FND Boot, on page 22
- Java Debugging, on page 23
- Log Files, on page 23
- Troubleshoot L+G device metrics refresh, on page 24
- Troubleshoot Metric Interval Errors, on page 25
- SSL Debugging, on page 32
- Troubleshoot High CPU Issues, on page 33
- Zero Touch Deployment — Tunnel Provisioning, on page 36
- ZTD Easy Mode for PNP, on page 36
- Zero Touch Deployment Steps — Log Entries for Plug and Play, on page 37
- ZTD Step by Step — Entries for IXM Registration, on page 37
- ZTD Step by Step — Log Entries for IXM Tunnel, on page 38
- ZTD Step by Step — Log Entries for Registration, on page 38
- Upgrading the Virtual Machine, on page 38

Access Docker Containers

Procedure

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 1: Access Docker Container



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/

Common Errors	Items to Check and/or Resolve Errors
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
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

Troubleshoot Influx event migration to Postgres

This task helps you migrate influx events to postgres without issues.

- When devices remain registered in Cisco IoT FND, migrating Influx events to Postgres completes without issues.
- If a device is removed from Cisco IoT FND, the **Events** page shows in the Name column: **eid doesn't exist in the system anymore**. In this state, the events migration throws errors and the affected records do not migrate to Postgres.

Before you begin

Here is how you troubleshoot the influx event migration to postgres:

Procedure

Re-upload the device CSV to restore the device in Cisco IoT FND, then rerun the events migration.

Example:

```
[root@iot-fnd log]# tail -f influx2postgres.log
2025-08-17 12:59:32 INFO  Influx2PostgresMigrator:102 - ##### Migration of records from Influx to
Postgres process: Started 2025-08-17T16:59:32.589Z #####

2025-08-17 12:59:42 INFO  Influx2PostgresMigrator:119 - parallelize : true
2025-08-17 12:59:42 INFO  Influx2PostgresMigrator:131 - Total number of measurements to migrate: 1
2025-08-17 12:59:42 INFO  Influx2PostgresMigrator:132 - Measurements : [events]
```

```
2025-08-17 12:59:42 INFO  Influx2PostgresMigrator:157 - Measurement: events has a retention period
of 31 days.
2025-08-17 12:59:43 INFO  Influx2PostgresMigrator:162 - Successfully updated retention period for
postgres table: events
2025-08-17 12:59:43 INFO  Influx2PostgresMigrator:178 - Parallel migration enabled at measurements
level. Using maximum of 20 read threads and 32 write threads.
2025-08-17 12:59:43 INFO  Influx2PostgresMigrator:246 - Starting migration for measurement: events
2025-08-17 12:59:43 INFO  Influx2PostgresMigrator:249 - Migration for measurement: events started at
 2025-08-17T16:59:43.227Z
2025-08-17 12:59:43 INFO  Influx2PostgresMigrator:263 - Max ID value in Postgres table events before
 migration: 0
2025-08-17 12:59:43 INFO  Influx2PostgresMigrator:334 - Processing measurement: events with fields:
 eventmessage,eventtypename,eventsev,eventsource,geohash,lat,lng,eid,issueid,domainname,netobjtypekind
 for target table: events
2025-08-17 12:59:43 INFO  Influx2PostgresMigrator:397 - Processed last chunk for measurement: events,
 fields:
eventmessage,eventtypename,eventsev,eventsource,geohash,lat,lng,eid,issueid,domainname,netobjtypekind,
 offset: 0
2025-08-17 12:59:43 ERROR PostgresWriteTask:106 - [BATCH] FAILED in INSERT SQL: INSERT INTO events
(eventtime,eventmessage,eventtypename,eventsev,eventsource,geohash,lat,lng,eid,issue_id,domain_id,id,eventseverity,event_type_id,net_element_id)
 VALUES (?,?,?,?,?,?,?,?,?,?,?,?,?,?,?) Retrying rows individually
2025-08-17 12:59:43 ERROR PostgresWriteTask:176 - [ERROR] Exception during individual row insert in
 postgres DB: ERROR: null value in column "net_element_id" of relation "events" violates not-null
constraint
  Detail: Failing row contains (5, null, 1755449042531, 0, asr1000, 891, interfaceUp, GRE tunnel on
 interface Virtual-Access2 connected to 3.3.3.221 c..., 1000, 1000, null, CSR1000V+9PB415ITOSI, 0,
INFO, 1).
org.postgresql.util.PSQLException: ERROR: null value in column "net_element_id" of relation "events"
 violates not-null constraint
  Detail: Failing row contains (5, null, 1755449042531, 0, asr1000, 891, interfaceUp, GRE tunnel on
 interface Virtual-Access2 connected to 3.3.3.221 c..., 1000, 1000, null, CSR1000V+9PB415ITOSI, 0,
INFO, 1).
    at org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2725)
    at org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:2412)
    at org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:371)
    at org.postgresql.jdbc.PgStatement.executeInternal(PgStatement.java:502)
    at org.postgresql.jdbc.PgStatement.execute(PgStatement.java:419)
    at org.postgresql.jdbc.PgPreparedStatement.executeWithFlags(PgPreparedStatement.java:194)
    at org.postgresql.jdbc.PgPreparedStatement.executeUpdate(PgPreparedStatement.java:155)
    at
com.cisco.cgms.influx2postgres.threads.PostgresWriteTask.insertSingleRow(PostgresWriteTask.java:172)

    at
com.cisco.cgms.influx2postgres.threads.PostgresWriteTask.lambda$null$2(PostgresWriteTask.java:156)
    at java.util.stream.ReferencePipeline$2$1.accept(ReferencePipeline.java:174)
    at java.util.ArrayList$ArrayListSpliterator.forEachRemaining(ArrayList.java:1384)
    at java.util.stream.AbstractPipeline.copyInto(AbstractPipeline.java:482)
    at java.util.stream.AbstractPipeline.wrapAndCopyInto(AbstractPipeline.java:472)
    at java.util.stream.ReduceOps$ReduceTask.doLeaf(ReduceOps.java:747)
    at java.util.stream.ReduceOps$ReduceTask.doLeaf(ReduceOps.java:721)
    at java.util.stream.AbstractTask.compute(AbstractTask.java:327)
    at java.util.concurrent.CountedCompleter.exec(CountedCompleter.java:731)
    at java.util.concurrent.ForkJoinTask.doExec(ForkJoinTask.java:289)
    at java.util.concurrent.ForkJoinTask.doInvoke(ForkJoinTask.java:401)
    at java.util.concurrent.ForkJoinTask.invoke(ForkJoinTask.java:734)
    at java.util.stream.ReduceOps$ReduceOp.evaluateParallel(ReduceOps.java:714)
    at java.util.stream.AbstractPipeline.evaluate(AbstractPipeline.java:233)
    at java.util.stream.LongPipeline.reduce(LongPipeline.java:461)
    at java.util.stream.LongPipeline.sum(LongPipeline.java:419)
    at java.util.stream.ReferencePipeline.count(ReferencePipeline.java:593)
    at
com.cisco.cgms.influx2postgres.threads.PostgresWriteTask.lambda$handlePerRowParallel$3(PostgresWriteTask.java:156)

    at java.util.concurrent.ForkJoinTask$AdaptedCallable.exec(ForkJoinTask.java:1424)
```

```
    at java.util.concurrent.ForkJoinTask.doExec(ForkJoinTask.java:289)
    at java.util.concurrent.ForkJoinPool$WorkQueue.runTask(ForkJoinPool.java:1056)
    at java.util.concurrent.ForkJoinPool.runWorker(ForkJoinPool.java:1692)
    at java.util.concurrent.ForkJoinWorkerThread.run(ForkJoinWorkerThread.java:175)
2025-08-17 12:59:43 ERROR PostgresWriteTask:176 - [ERROR] Exception during individual row insert in
 postgres DB: ERROR: null value in column "net_element_id" of relation "events" violates not-null
constraint
  Detail: Failing row contains (2, null, 1755449042531, 0, asr1000, 891, interfaceUp, GRE tunnel on
 interface Virtual-Access3 connected to 3.3.3.231 c..., 1000, 1000, null, CSR1000V+9PB415ITOSI, 0,
INFO, 1).
org.postgresql.util.PSQLException: ERROR: null value in column "net_element_id" of relation "events"
 violates not-null constraint
  Detail: Failing row contains (2, null, 1755449042531, 0, asr1000, 891, interfaceUp, GRE tunnel on
 interface Virtual-Access3 connected to 3.3.3.231 c..., 1000, 1000, null, CSR1000V+9PB415ITOSI, 0,
INFO, 1).
    ...
2025-08-17 12:59:53 INFO  Influx2PostgresStatsLogger:124 - ##########################################
 INFLUX TO POSTGRES ##########################################
2025-08-17 12:59:53 INFO  Influx2PostgresStatsLogger:129 - [MIGRATION] events: 1/6 records copied
(16.67%)
2025-08-17 12:59:53 INFO  Influx2PostgresStatsLogger:132 - ##########################################
 INFLUX TO POSTGRES ##########################################

2025-08-17 12:59:53 INFO  Influx2PostgresMigrator:209 - ##### Migration of records from Influx to
Postgres process: Completed 2025-08-17T16:59:53.422Z Total time taken: 00:00:20 #####
```

The migration completes successfully.

FND Debugging — How to Enable

To enable FND debugging, follow these steps:

Option 1:

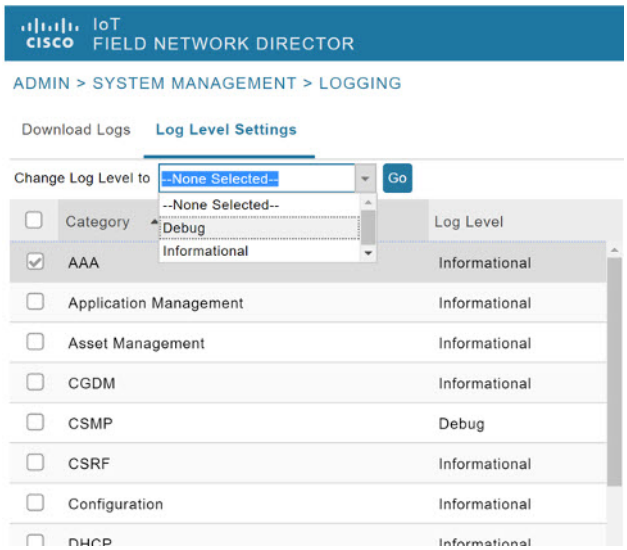
Procedure

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 2: 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 3: Entering EIDs

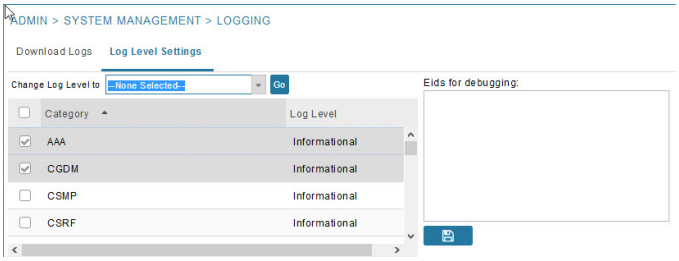
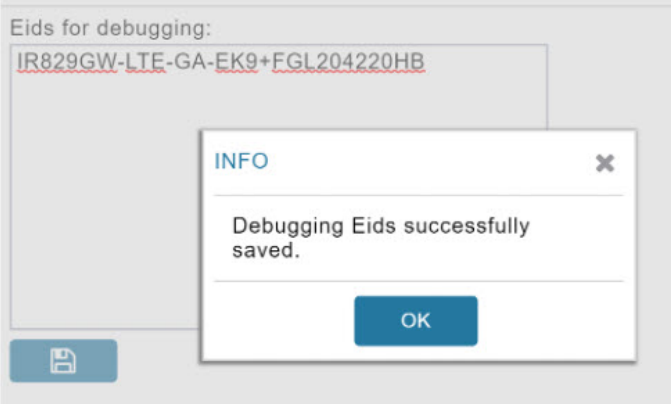


Figure 4: Populated EID panel



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.

Procedure

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

Procedure

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]
```

Log Files

Note All log files are case-sensitive.

Postgres Log Files:

```
[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
```

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.

FND log files:

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

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

Troubleshoot L+G device metrics refresh

An L+G router or endpoint is present in Cisco IoT FND, but device metrics or telemetry do not refresh. The device may appear reachable, while the `Last Metric Heard` field, charts, or metric values remain stale after a periodic refresh or after selecting `Refresh Metrics`.

Here are the possible causes:

- The L+G device was imported with an inconsistent EID or the EID case does not match the certificate or device profile.
- The device is not in the expected group, such as `Default-lgrouter` for routers or the correct L+G endpoint group for endpoints.
- The periodic metrics URL configured in IoT FND does not match the URL configured on the router or telemetry source.
- A firewall, proxy, NAT device, or load balancer blocks the configured metrics port or terminates long-lived WebSocket traffic.
- The device can register, but periodic metric or telemetry messages are not being sent, are rejected by IoT FND, or are failing during processing.

Before you begin

Use the following procedure to isolate whether the problem is device identity, group assignment, network reachability, IGMA/WebSocket communication, or metric processing.

Procedure

Step 1 From Cisco IoT FND menubar, choose **DEVICES** > **FIELD DEVICES** > **Browse Devices**.

Step 2 Select `ROUTER` for L+G routers or `ENDPOINT` for L+G endpoints.

Step 3 Open the L+G device details and record the EID, IP address, status, configuration group, `Last Heard`, and `Last Metric Heard`.

Step 4 Verify that the device is a member of the expected group. L+G routers should be in `Default-lgrouter` or the intended custom router group; L+G endpoints should be in the expected L+G endpoint group. Verify that the EID uses the same

letter case in the import file, certificate identity, device profile, Cisco IoT FND UI, and logs. If the same device appears with different EID case, correct the import or device identity before troubleshooting metrics.

Step 5 Trigger a manual metric refresh from the device details page and record the timestamp and enable Cisco IoT FND log levels for L+G device debugging:

a) Choose `ADMIN > Logging`. In releases where logging is grouped under system management, choose `ADMIN > System Management > Logging`.
b) Click the `Log Level Settings` tab.
c) Set `Lwm2m` to the required debug log level.
d) Set `Websocket` to the required debug log level.
e) Save the log level settings.
f) Enable EID-specific debug logging for the L+G device if the deployment uses per-EID debug logging.

he L+G device debug details are written to `server.log`.

Step 6 Check the Cisco IoT FND logs on the node that handled the request:

```
RPM deployments: /opt/cgms/server/cgms/logs/server.log
Primary L+G debug log: server.log
```

Step 7 Search server.log for device EID and for IGMA, LWM2M or WebSocket terms around the timestamp of the refresh.

Example:

```
grep -i "<L+G-device-EID>" /opt/cgms/server/cgms/logs/server.log
grep -Ei
"igma|lwm2m|websocket|metric|telemetry|register|timeout|reset|certificate|unauthorized|forbidden"
/opt/cgms/server/cgms/logs/server.log
```

Step 8 Verify the metrics endpoint in `ADMIN > SYSTEM MANAGEMENT > Provisioning Settings`.

- If no metric request reaches Cisco IoT FND, verify DNS, routing, firewall rules, NAT rules, proxy settings, load balancer settings, and device profile URLs from the L+G device network toward Cisco IoT FND.
- If the metric request reaches Cisco IoT FND but the UI remains stale, check `server.log` for parsing, authorization, certificate, database, or transaction errors.

Troubleshoot Metric Interval Errors

Runtime Exception Error

Problem

The error message `java.lang.NullPointerException` is a common runtime exception in Java. It occurs when a program attempts to use an object reference that has not been initialized. Here's an example error message with the logs:

```
java.lang.NullPointerException
fcw2536xabcd][ip=IPv6-Address][sev=ERROR][tid=IOS CGR Request-1][part=64856087.1/9]: Failed
 to processinventory for device. Reason:
64856088: fnd-server: Aug 30 2024 14:17:23.357 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=CiscoCgrMetricsProcess][eid=IR1101-K9+fcw2536abcd][ip=IPv6-Address][sev=ERROR][tid=IOS
 CGR Request-1][part=64856087.2/9]:java.lang.NullPointerException
```

```
64856089: fnd-server: Aug 30 2024 14:17:23.357 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=CiscoCgrMetricsProcess][eid=IR1101-K9+fcw2536abcd][ip=IPv6-Address][sev=ERROR][tid=IOS
 CGR Request-1][part=64856087.3/9]:
atcom.cisco.cgms.elements.ciscocgr.ios.operations.CiscoIosMetricsOperation.getCommandsFromData(CiscoIosMetricsOperation.java:529)
64856090: fnd-server: Aug 30 2024 14:17:23.357 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=CiscoCgrMetricsProcess][eid=IR1101-K9+fcw2536abcd][ip=IPv6-Address][sev=ERROR][tid=IOS
 CGR Request-1][part=64856087.4/9]:
atcom.cisco.cgms.elements.ciscocgr.ios.operations.CiscoIosMetricsOperation.processMetricsData(CiscoIosMetricsOperation.java:606)
64856091: fnd-server: Aug 30 2024 14:17:23.357 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=CiscoCgrMetricsProcess][eid=IR1101-K9+fcw2536abcd][ip=IPv6-Address][sev=ERROR][tid=IOS
 CGR Request-1][part=64856087.5/9]:
atcom.cisco.cgms.elements.ciscocgr.ios.operations.CiscoIosMetricsOperation.processInventoryUpload(CiscoIosMetricsOperation.java:416)
64856092: fnd-server: Aug 30 2024 14:17:23.357 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=CiscoCgrMetricsProcess][eid=IR1101-K9+fcw2536abcd][ip=IPv6-Address][sev=ERROR][tid=IOS
 CGR Request-1][part=64856087.6/9]:
atcom.cisco.cgms.elements.ciscocgr.ios.operations.CiscoCgrMetricsProcess.run(CiscoCgrMetricsProcess.java:128)
64856093: fnd-server: Aug 30 2024 14:17:23.357 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=CiscoCgrMetricsProcess][eid=IR1101-K9+fcw2536abcd][ip=IPv6-Address][sev=ERROR][tid=IOS
 CGR Request-1][part=64856087.7/9]:
atjava.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
64856094: fnd-server: Aug 30 2024 14:17:23.357 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=CiscoCgrMetricsProcess][eid=IR1101-K9+fcw2536abcd][ip=IPv6-Address][sev=ERROR][tid=IOS
 CGR Request-1][part=64856087.8/9]:
atjava.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
64856095: fnd-server: Aug 30 2024 14:17:23.357 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=CiscoCgrMetricsProcess][eid=IR1101-K9+fcw2536abcd][ip=IPv6-Address][sev=ERROR][tid=IOS
 CGR Request-1][part=64856087.9/9]:
atjava.lang.Thread.run(Thread.java:748)
64856096: fnd-server: Aug 30 2024 14:17:23.358 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=TxConnectionListener][eid=IR1101-K9+fcw2536abcd][ip=IPv6-Address][sev=DEBUG][tid=IOS
CGR Request-1]: Unfinished local transaction wasrolled
back.org.jboss.jca.core.connectionmanager.listener.TxConnectionListener@39f31201[state=NORMAL
 managedconnection=org.jboss.jca.adapters.jdbc.local.LocalManagedConnection@568ee3c connection
 handles=0lastReturned=1725027443340 lastValidated=1725027054869 lastCheckedOut=1725027443341
 trackByTx=falsepool=org.jboss.jca.core.connectionmanager.pool.strategy.PoolBySubject@4c313ad0
mcp=SemaphoreConcurrentLinkedQueueManagedConnectionPool@216c3b91[pool=postgresDS]
xaResource=LocalXAResourceImpl@50f733b7[connectionListener=39f31201 connectionManager=9380d48
 warned=false
currentXid=null productName=PostgreSQL productVersion=12.12 jndiName=java:/DefaultDS]
txSync=null]
```

Solution

The router is onboarded using a lowercase EID (eid=IR1101-K9+fcw2536abcd), while the router certificate is generated with an uppercase EID (eid=IR1101-K9+FCW2536ABCD). This discrepancy causes a HASH mismatch, resulting in a `java.lang.NullPointerException`. For more information see,CSCwm39996. The following steps can help avoid the common runtime exception:

- Check the refresh metrics from Cisco IoT FND periodically.
- Trigger periodic metric profiles from the router with debugging enabled on both Cisco IoT FND and the router.
- Perform system, metric, and router bootstrapping debugs. Use the `debug cgna logging all` command to enable comprehensive logging.
- Ensure that the EID is entered consistently in all configurations and interfaces using the same case format.

File Upload Error

Problem

The `com.cisco.cgms.exceptions.CiscoIosFileUploadException` is an exception that occurs in Cisco IoT FND, when there is an issue related to file uploads, particularly involving Cisco IOS files. Here's an example error message:

```
com.cisco.cgms.exceptions.CiscoIosFileUploadException: Error occurred while verifying file
 upload operation for net element
IR1101-K9+FCW2425ABCD; Caused by: com.cisco.cgms.exceptions.CiscoIosFileUploadException:
Exception occured while
performing file upload operation for net element IR1101-K9+FCW2425ABCD; Caused by:
com.cisco.cgms.exceptions.CiscoIosFileUploadException: Error occured while performing file
 upload operation; Caused by:
com.cisco.cgms.wsma.client.CgmsWsmaException: Error in running file check
```

Solution

While onboarding routers, when the CA server validation or authentication fails, the error message `CiscoIosFileUploadException` appears. Here's how you can troubleshoot and resolve the issue:

- **Check the Router's Certificate Details**: Use the command `show crypto pki certificate verbose LDevID` on the router to display detailed information about the Local Device Identifier (LDevID) certificate. This information can help identify discrepancies or issues in the certificate.
- **Verify the SAN Field**: Ensure that the SAN field in the certificate is correctly populated. The SAN field should match the expected values required for successful validation.
- **Use Debug Commands on the Router**: The following debug commands can provide detailed insights into the certificate-related processes and help diagnose the cause of the failure:
  - **`debug crypto pki messages`**: Captures general messages related to Public Key Infrastructure (PKI) operations.
  - **`debug crypto pki scep`**: Provides information specific to the Simple Certificate Enrollment Protocol (SCEP), which is often used for certificate issuance and renewal.
  - **`debug crypto pki transactions`**: Logs all PKI transaction details to identify any issues during certificate processing.
  - **`debug crypto pki validation`**: Offers insights into the validation process of certificates, helping identify why a certificate might be considered invalid.
  - **`debug crypto pki server`**: If applicable, provides details on the PKI server interactions, which can be useful if the router acts as a CA.
- **Additional Considerations:**
  - Ensure network connectivity between the router and the CA server.
  - Verify that all configurations related to certificate enrollment and PKI are correct on both the router and the FND.
  - Consult Cisco support or documentation for specific guidance related to the version of the software in use if the issue persists.

Missing Configuration Error

Problem

The `com.cisco.cgms.properties.PropertyNotFoundException` is an exception indicating that a specific property or configuration setting expected by Cisco IoT FND could not be found. This exception typically arises when a required configuration parameter is missing or incorrectly specified within the system properties files or settings. Here is an example error message:

```
com.cisco.cgms.properties.PropertyNotFoundException: Required property [Administrator
Password(adminPassword)] has
not been configured on [IR1101-K9+FCW2425ABCD]
```

Solution

The `com.cisco.cgms.properties.PropertyNotFoundException` appears when the admin password of Cisco IoT FND doesn't match with the admin password of the router. Update the password for Cisco IoT FND in the CSV file that matches with the password of the router.

Retrieve Inventory Error

Problem

The error message `java.io.IOException: Failed to retrieve inventory from device. Reason: \[invalid cli command\]` indicates that there was an attempt to execute a command on a network device, but the command was not recognized or valid, leading to a failure in retrieving inventory information. Here's an example error message:

```
java.io.IOException: Failed to retrieve inventory from device. Reason: [invalid cli command]
 Sent [[show version | format
flash:/managed/odm/cg-nms.odm
show iox-service | format flash:/managed/odm/cg-nms.odm
show platform resources | format flash:/managed/odm/cg-nms.odm]]
```

Solution

When comparing the inventory from a router with the `cg-nms.odm` file, discrepancies during the bootstrapping process can lead to errors. Look at the specifics provided in the error message to identify which parts of the configuration are inconsistent. Adjust the router configuration to match the expectations defined in the `cg-nms.odm` file, if appropriate.

SOAP Error

Problem

The `javax.xml.ws.soap.SOAPFaultException` is an exception that occurs during Simple Object Access Protocol (SOAP) web service communication. This exception indicates that there was a problem processing a SOAP message, and a fault was returned by the web service.

Solution

To address connectivity issues between the Cisco IoT FND and a router, you can perform the following steps to isolate and diagnose the problem:

1. Use the ping command to test basic network connectivity between the Cisco IoT FND and the router. This helps determine if there is a reachable network path.
2. Use the following command to execute a Web Services Management Agent (WSMA) request to the router, checking if the WSMA communication is functioning correctly:

```
/opt/cgms-tools/bin/wsma-request https://<ROUTER IPv4 or IPv6 address>:443/wsma/exec
admin
          /opt/cgms/server/cgms/conf "show version | format
        flash:/managed/odm/cg-nms.odm"
```

3. Use `tcpdump --list-interfaces` to list available network interfaces on the Cisco IoT FND, helping you identify the correct interface for capturing traffic.
4. Use `tcpdump -i ens192 -w cisco.pcap` to capture network packets on the specified interface and write them to a file named `cisco.pcap`. Analyzing this file can help identify anomalies in network traffic.
5. The following debug commands on the router can help identify failures related to WSMA or HTTP communication:
   - **`debug cgna logging all`**: Enable comprehensive logging for Cisco Generic Network Architecture (CGNA) to capture detailed logs.
   - **`debug wsma agent`**: Monitor the WSMA agent for any issues in handling requests.
   - **`debug wsma profile`**: Check the WSMA profile configurations and operations.
   - **`debug ip http all`**: Capture all HTTP-related activities, which can be useful if WSMA over HTTP is involved.
6. Enter configuration mode with `conf t` and set the environment variable for logging configuration replacements with:

```
event manager environment LOG_CONFIG_REPLACE TRUE
exit
```

Timeout Error

Problem

The error message you're encountering involves a `javax.xml.ws.WebServiceException` and a `java.net.SocketTimeoutException`, indicating a timeout issue during a web service communication attempt. High latency in the network can cause timeouts if the response from the server takes too long.

Solution

To troubleshoot and isolate connectivity issues between the Cisco IoT FND and a router, particularly when dealing with WSMA or HTTP-related problems, you can perform the following steps:

1. Use the `ping` command to test basic connectivity from the Cisco IoT FND to the router.
2. Execute the following command to test WSMA communication:

```
/opt/cgms-tools/bin/wsma-request https://<ROUTER IPv4 or IPv6 address>:443/wsma/exec
admin /opt/cgms/server/cgms/conf "show version | format flash:/managed/odm/cg-nms.odm"
```

The output will help you understand if WSMA is functioning properly.

3. Run `tcpdump --list-interfaces` to see all available network interfaces on the FND. This is useful for identifying the correct interface to monitor.
4. Use the following command to capture network packets on a specific interface (e.g., `ens192`) and save them to a file (`cisco.pcap`):

```
tcpdump -i ens192 -w cisco.pcap
```

5. The following debug commands can provide insights into WSMA and HTTP operations on the router:
   - **`debug cgna logging all`**: Enables comprehensive logging for Cisco Generic Network Architecture (CGNA) to capture detailed logs.
   - **`debug wsma agent`**: Monitors the WSMA agent for any issues or errors during request handling.
   - **`debug wsma profile`**: Examines WSMA profile configurations and operations to identify misconfigurations.
   - **`debug ip http all`**: Captures all HTTP-related activities, useful if WSMA operates over HTTP.
6. Enter configuration mode and set an environment variable to log configuration changes:

```
conf t
event manager environment LOG_CONFIG_REPLACE TRUE
exit
```

Network Connectivity Errors

Problem

The following error messages indicate various network connectivity issues encountered during SOAP web service communication.

1. **Read Timed Out**: This error occurs when a connection is established, but the server does not send a response within the expected time frame. Here's an example:

```
javax.xml.ws.soap.SOAPFaultException: Read timed out; Caused by:
com.ctc.wstx.exc.WstxIOException: Read timed out
```

2. **Connect Timed Out**: This error indicates that the client was unable to establish a connection to the server within the allotted time. Here's an example:

```
javax.xml.ws.soap.SOAPFaultException: connect timed out; Caused by:
com.ctc.wstx.exc.WstxIOException: connect timed
out
```

3. **Connection Reset**: This occurs when an established connection is unexpectedly closed by the server. Here's an example:

```
javax.xml.ws.soap.SOAPFaultException: Connection reset; Caused by:
com.ctc.wstx.exc.WstxIOException: Connection reset
```

4. **Connection Refused**: This error means the server actively refused the connection attempt, often because the service is not running on the specified port. Here's an example:

```
javax.xml.ws.soap.SOAPFaultException: Connection refused (Connection refused); Caused
by:
com.ctc.wstx.exc.WstxIOException: Connection refused (Connection refused)
```

Solution

To effectively troubleshoot connectivity and communication issues between the Field Network Director (FND) and a router, you can perform the following diagnostic steps:

1. Perform a ping test from both Cisco IoT FND and the router.
2. Execute the following WSMA request command to test the ability to execute management commands on the router:

   ```
   /opt/cgms-tools/bin/wsma-request https://<ROUTER IPv4 or IPv6 address>:443/wsma/exec
   admin /opt/cgms/server/cgms/conf "show version | format flash:/managed/odm/cg-nms.odm"
   ```

3. Use `tcpdump --list-interfaces` to list all available network interfaces on the FND. This helps you identify which interface to monitor for packet capture.
4. Run `tcpdump` on the identified network interface to capture packets and write them to a file for analysis:

   ```
   tcpdump -i ens192 -w cisco.pcap
   ```

5. The following debug commands help identify failures related to WSMA or HTTP communication:
   - **`debug cgna logging all`**: Enables detailed logging for Cisco Generic Network Architecture, capturing extensive logs.
   - **`debug wsma agent`**: Monitors the WSMA agent for potential issues or errors in handling requests.
   - **`debug wsma profile`**: Examines WSMA profile configurations and operations to find misconfigurations.
   - **`debug ip http all`**: Captures all HTTP-related activities, useful for diagnosing HTTP-based WSMA issues.
6. Enter configuration mode and set an environment variable to log configuration changes, which can help track and diagnose issues:

   ```
   conf t
   event manager environment LOG_CONFIG_REPLACE TRUE
   exit
   ```

Webservice Error

Problem

The `javax.xml.ws.WebServiceException: Could not send Message` indicates a problem with sending a SOAP message to a web service endpoint, which resulted in an HTTP 504 Gateway Timeout error. This typically means that a server, acting as a gateway or proxy, did not receive a timely response from an upstream server it needed to access to complete the request. Here's an example error message:

```
javax.xml.ws.WebServiceException: Could not send Message.; Caused by:
org.apache.cxf.transport.http.HTTPException:
HTTP response '504: Gateway Time-out' when communicating with https://[IPV6 address / IPV4
 Address]:443/wsma/exec
```

Solution

The issue may be related to an invalid or improperly configured self-signed certificate, which can cause communication problems, especially in secure network environments. Self-signed certificates are often used for testing or internal purposes, but they need to be correctly configured and trusted by the systems that interact with them. Here are the steps to address the issue:

1. Ensure the current self-signed certificate is valid. If it's expired or improperly configured, re-generate it following the appropriate process for your device or system.
2. The following commands are used on network devices to manage HTTP and SSH services. They first disable and then re-enable these services, potentially refreshing or resetting their configurations:
   - **`no ip http server`**: Disables the HTTP server on the device.
   - **`no ip http authentication local`**: Removes local authentication for HTTP, if previously set.
   - **`no ip http secure-server`**: Disables the HTTPS server, which might be necessary before making changes to certificates.
   - **`no ip ssh version 2`**: Disables SSH version 2; however, this step might be intended to reset SSH configurations.
   - **`ip http server`**: Enables the HTTP server on the device.
   - **`ip http authentication local`**: Sets local authentication for HTTP access.
   - **`ip http secure-server`**: Enables the HTTPS server, allowing secure web-based management.
   - **`ip ssh version 2`**: Re-enables SSH version 2, which is the more secure version of the SSH protocol.
3. After re-generating the self-signed certificate, ensure that any clients or systems interacting with this device trust the certificate. This might involve importing the certificate into their trust store.

SSL Debugging

Procedure

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
```

Troubleshoot High CPU Issues

Problem

Often facing a spike in the CPU usage.

Solution

Here are the instructions to analyze and troubleshoot some of the high CPU issues:

1. Analyze if the CPU spike is intermittent or constant. If intermittent, make a note of the duration.
2. From the Cisco IoT FND Menubar, choose **Devices** > **Servers**.
3. Choose the problematic Cisco IoT FND server which has CPU issues and analyze the charts to spot any CPU spike issues.
4. Run the following commands as root using the SSH command:

Command	Description
lscpu	Gathers CPU architecture information from sysfs and /proc/cpuinfo, information includes number of CPUs, threads, cores, sockets etc.
ps-aux	View statistics about system's running processes, like the percent of CPU and memory that the process is using etc
ps aux k-pcpu | head -6	This command sorts the list of running processes by CPU usage in descending order (using `k-pcpu`) and then displays the top 6 processes (`head -6`). It's useful for identifying which processes are consuming the most CPU.
ps aux | sort -nrk 3,3 | head -n 5	This command sorts the running processes by the third column (which is typically %CPU) in numerical reverse order (`-nrk 3,3`) and displays the top 5 entries (`head -n 5`). Similar to the previous command, it helps identify CPU-intensive processes.
top	View a real-time view of running processes in Linux and displays kernel-managed tasks, enables user to monitor CPU-intensive tasks
top -b -n 1 | head -n 12 | tail -n 5	This command runs `top` in batch mode (`-b`) for one iteration (`-n 1`). It then takes the first 12 lines of the output and displays the last 5 lines (`head -n 12 | tail -n 5`). This typically shows the header information and the most CPU-intensive processes at a given moment.

Command	Description
sar -t -r -f	The `sar` command is used for collecting, reporting, or saving system activity information. The `-r` flag is for memory usage, and `-t` specifies time format. The `-f` flag is used to read data from a file, typically a `sar` data file. This would provide historical data on memory usage over time.
sar -t -q -f	Similar to the previous `sar` command, but with the `-q` flag, which is used to report queue length and load average. This helps in understanding how the system load has been distributed over time.
iostat	Monitor CPU utilization, system input/output statistics for all the disks and partitions
free -m	Get detailed report on the system's memory usage
mpstat	View information about CPU utilization and performance
vmstat	View information about processes, memory, disk, and CPU activity

Here's a sample output:

```
ps -aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.0 191428 4332 ? Ss Jul09 20:48 /usr/lib/systemd/systemd --switched-roo
root 2 0.0 0.0 0 0 ? S Jul09 0:00 [kthreadd]
root 4 0.0 0.0 0 0 ? S< Jul09 0:00 [kworker/0:0H]
root 6 0.0 0.0 0 0 ? S Jul09 3:22 [ksoftirqd/0]
root 7 0.0 0.0 0 0 ? S Jul09 0:06 [migration/0]
root 8 0.0 0.0 0 0 ? S Jul09 0:00 [rcu_bh]
root 9 0.0 0.0 0 0 ? R Jul09 59:17 [rcu_sched]
root 10 0.0 0.0 0 0 ? S< Jul09 0:00 [lru-add-drain]
root 11 0.0 0.0 0 0 ? S Jul09 0:49 [watchdog/0]
root 12 0.0 0.0 0 0 ? S Jul09 0:17 [watchdog/1]
root 52 0.0 0.0 0 0 ? S Jul09 0:20 [watchdog/9]
root 53 0.0 0.0 0 0 ? S Jul09 0:19 [migration/9]
root 54 0.0 0.0 0 0 ? S Jul09 0:28 [ksoftirqd/9]
root 56 0.0 0.0 0 0 ? S< Jul09 0:00 [kworker/9:0H]
```

Gather the Heap and Thread Dumps

When you notice slowness in your Cisco IoT FND, collect the JAVA heap and thread dumps. Use the following instructions to collect the heap and thread dumps:

1. Download the JDK package which is an OpenJDK distribution for Linux (64-bit) from https://corretto.aws/downloads/latest/amazon-corretto-8-x64-linux-jdk.tar.gz.
2. Extract the JDK tar.gz file.

   For example:

   ```
   tar -xzf amazon-corretto-8-x64-linux-jdk.tar.gz
   ```

3. Transfer the extracted JDK file to the Cisco IoT FND server using the scp command.

   For example:

   ```
   scp -r amazon-corretto-8-x64-linux-jdk user@fnd-server:/path/to/destination
   ```

4. Navigate to the `bin` directory of the JDK installation to access the `jmap` utility. Example:

   ```
   cd /path/to/destination/amazon-corretto-8-x64-linux-jdk/bin
   ```

5. Find the docker ID using the `docker ps` command. Here's an example:

   ```
   [root@iot-fnd ~]# docker ps
   CONTAINER ID        IMAGE               COMMAND                  CREATED
   STATUS              PORTS

                                                                          NAMES
   54e349b30f46        fogd-image:active   "/bin/sh -c /usr/loc…"   12 days ago
   Up 12 days          443/tcp

                                                                          fogd-container
   f67d89e4188b        fnd-image:active    "/bin/sh -c /opt/fnd…"   12 days ago
   Up 2 days           0.0.0.0:80->80/tcp, 0.0.0.0:162->162/udp, 0.0.0.0:443->443/tcp,
   0.0.0.0:9120-9121->9120-9121/tcp, 0.0.0.0:5683->5683/udp,
   0.0.0.0:61624-61626->61624-61626/udp, 0.0.0.0:9124-9125->9124-9125/tcp,
   0.0.0.0:61628->61628/udp   fnd-container
   ```

6. Copy the tar.gz file to the docker using the following command and paste the docker ID:

   ```
   docker cp /amazon-corretto-8.422.05.1-linux-x64.tar.gz f67d89e4188b
   ```

7. Log in to the docker using the following command:

   ```
   [root@iot-fnd ~]# docker exec -i -t fnd-container /bin/bash
   ```

8. Unzip the tar.gz file using the `tar-xvf<complete path>` command. Here's an example:

   ```
   [root@iot-fnd ~]# tar -xvf /CISCO/amazon-corretto-8.422.05.1-linux-x64.tar.gz]
   ```

9. Find the CGMS process ID using the `ps -eaf | grep cgms` command. Here's an example:

   ```
   [root@iot-fnd ~]# ps -eaf | grep cgms
   root      308261       1  0 Jul29 pts/0    00:00:00 runuser -c bin/cgms -s /bin/bash
   root
   root      308262  308261  0 Jul29 pts/0    00:00:00 /bin/sh bin/cgms
   root      308265  308262  0 Jul29 pts/0    00:00:00 /bin/sh bin/standalone.sh
   -Djboss.server.log.dir=bin/../server/cgms/log --server-config=standalone.xml -b 0.0.0.0
   root      308382  308265  2 Jul29 pts/0    05:55:42 java -D[Standalone] -verbose:gc
   -Xloggc:/opt/cgms/server/cgms/log/gc.log -XX:+PrintGCDetails -XX:+PrintGCDateStamps
   -XX:+UseGCLogFileRotation -XX:NumberOfGCLogFiles=5 -XX:GCLogFileSize=3M
   -XX:-TraceClassUnloading -Xms1g -Xmx6g -XX:MaxPermSize=512m
   -Dcom.cisco.cgms.ciscolog.host=fnd-server -server -XX:+HeapDumpOnOutOfMemoryError
   -XX:HeapDumpPath=bin/../server/cgms/log -Djava.security.egd=file:/./dev/urandom
   -XX:+UnlockDiagnosticVMOptions -XX:+LogVMOutput
   -XX:LogFile=bin/../server/cgm/log/cgms_stacktrace.log -XX:-OmitStackTraceInFastThrow
   -Dorg.terracotta.quartz.skipUpdateCheck=true -Dbase.dir=bin
   -Dorg.jboss.boot.log.file=/opt/cgms/server/cgms/log/server.log
   -Dlogging.configuration=file:/opt/cgms/standalone/configuration/logging.properties
   -jar /opt/cgms/jboss-modules.jar -mp /opt/cgms/modules org.jboss.as.standalone
   -Djboss.home.dir=/opt/cgms -Djboss.server.base.dir=/opt/cgms/standalone
   -Djboss.server.log.dir=bin/../server/cgms/log --server-config=standalone.xml -b 0.0.0.0
   root      430277  430190  0 17:34 pts/1    00:00:00 grep --color=auto cgms
   ```

10. Use the following command to generate the heap dump:

    ```
    [root@iot-fnd ~]# /CISCO/amazon-corretto-8.422.05.1-linux-x64/bin/jmap
    -dump:file=heap_dump_11082024.hprof 308382
    ```

```
Dumping heap to /ENEDIS/heap_dump_11082024.hprof ...
Heap dump file created
[root@fnd-server CISCO]#
[root@fnd-server CISCO]#
[root@fnd-server CISCO]# ls -l | grep -i hprof
-rw------- 1 root root 1148131128 Aug 11 11:34 heap_dump_11082024.hprof
```

11. Use the following command to generate the thread dump:

```
[root@iot-fnd ~]# kill -3<CGNMSpid>
```

12. Upload both the cgms_stacktrace.log to TAC SR for further analysis.

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]
```

Upgrading the Virtual Machine

Before you begin

- Create a backup or snapshot of the virtual machines.
- Make sure the .vmdk files are available to the ESXi host on VMFS3, VMFS5, and NFS datastore.
- Make sure the virtual machine is stored on VMFS3, VMFS5, or NFS datastores.
- Make sure the compatibility settings for the virtual machines are not set to the latest supported version.
- Determine the ESXi versions that you want the virtual machines to be compatible with.

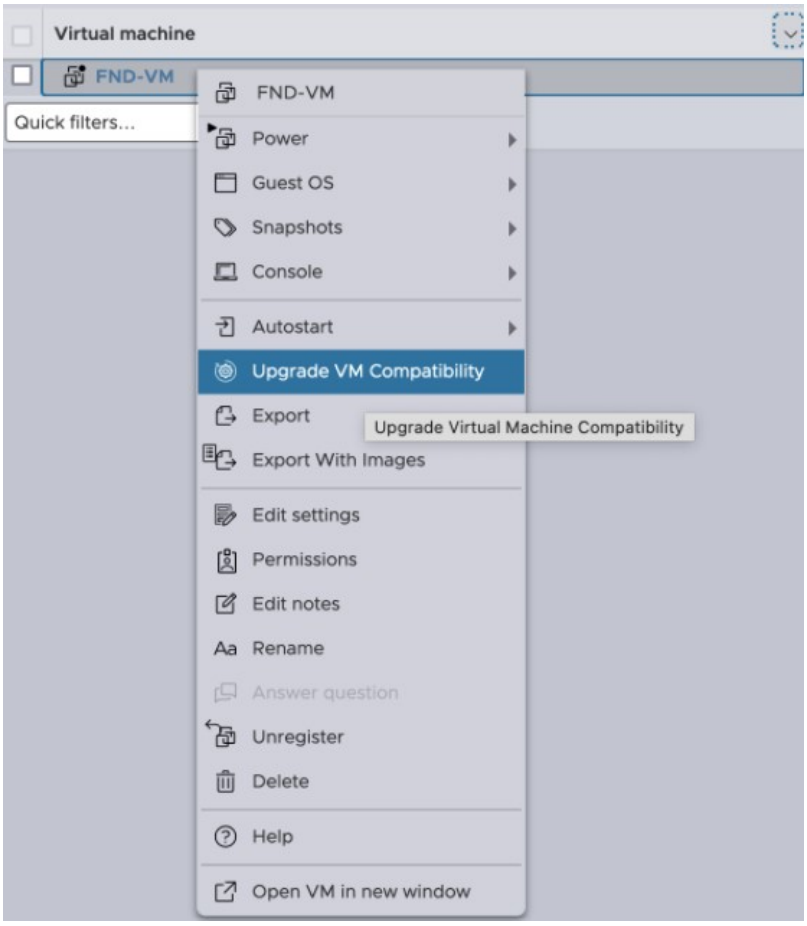
Note In Cisco IoT FND running Cisco IoT FND Release 4.12 and earlier releases, the maximum vCPU count is limited to 32 due to virtual machine compatibility being set to ESXi 5.0. Starting from Cisco IoT FND 5.0 version onwards, you can increase the CPU count beyond 32.

In case you upgrade your Cisco IoT FND from an older release to a newer release, follow the steps below to upgrade virtual machine compatibility.

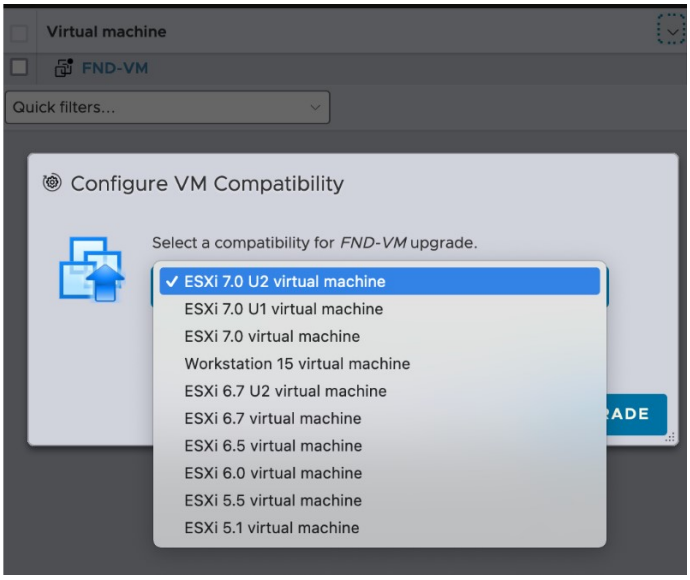
Procedure

Step 1 Power off the virtual machine.

Step 2 Right-click the virtual machine from the **Virtual machine** drop down list and select **Upgrade VM Compatibility** from the popup menu.



Step 3 Choose the latest supported version from the drop-down box.



Step 4 Cick **Upgrade**.

