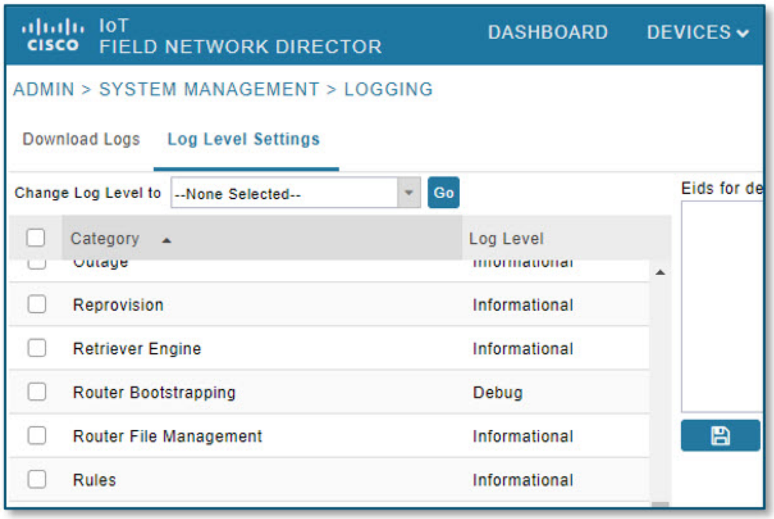
Troubleshooting for Specific IoT FND Components

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

Troubleshoot PNP

Figure 1: ADMIN > SYSTEM MANAGEMENT > LOGGING > Log Level Settings



Change Log Level to: --None Selected--

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

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

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

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

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

d. Click **Go**.

You can find the generated logs in the following location:

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

Step 2 Debug on FAR by entering the following commands:

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

Step 3 Check certificates and the ‘fnd’ trustpoint.

Step 4 Check provisioning link in settings.

Step 5 Check archive configuration and directory.

Troubleshooting Steps to Upload ODM File

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

- Download device-specific ODM file from FND server, on page 3
- Upload the ODM File from FND UI, on page 4

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

Download device-specific ODM file from FND server

To download device-specific ODM file from FND server:

Step 1 Log in to the FND server through SSH.

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

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

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

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

Step 4 Unzip the `cgms.ear` file.

```
 unzip cgms.ear
```

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

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

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

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

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

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

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

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

To list the ODM files, run the following command:

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

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

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

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

What to do next

Upload the ODM File from FND UI, on page 4

Upload the ODM File from FND UI

To upload the ODM file from FND UI:

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

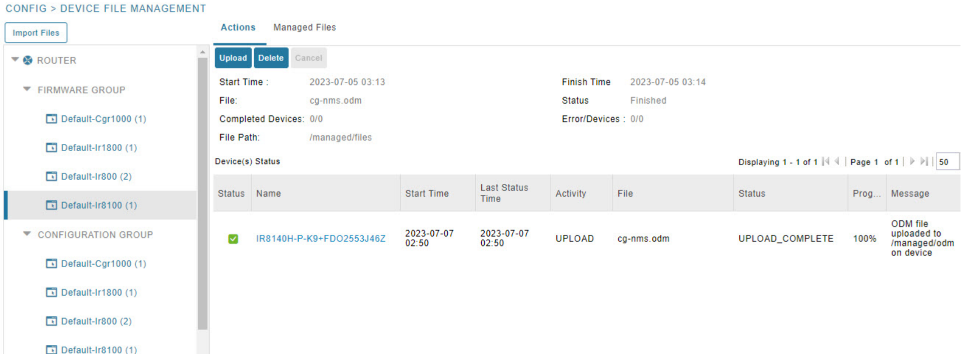
Before you begin

Download device-specific ODM file from FND server, on page 3.

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

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

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



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

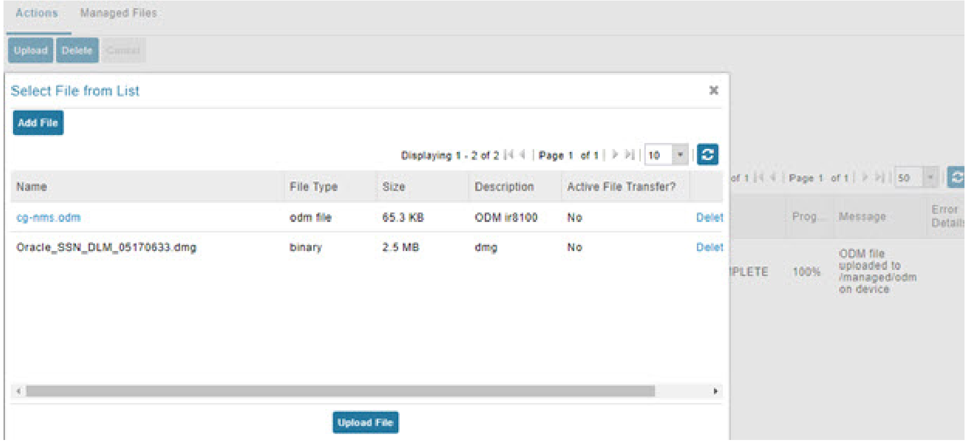
Finish Time 2023-07-05 03:14
Status Finished
Error/Devices : 0/0

Device(s) Status

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

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

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



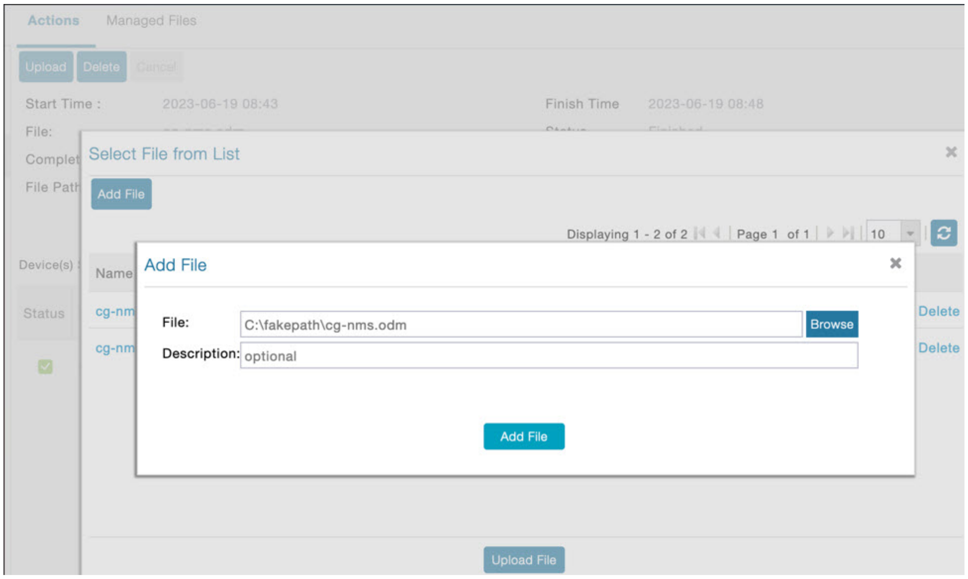
Select File from List

Displaying 1 - 2 of 2 | Page 1 of 1 | 10

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

Prog...	Message	Error Details
100%	ODM file uploaded to /managed/odm on device	

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



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

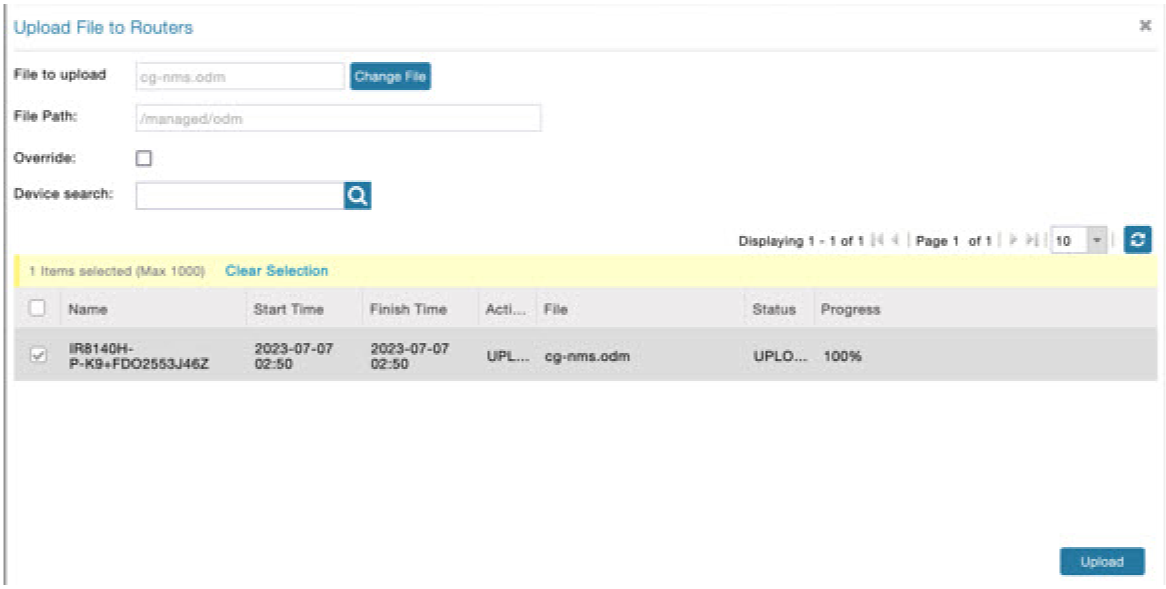
Displaying 1 - 2 of 2 | Page 1 of 1 | 10

Add File

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

Description: optional

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



Upload File to Routers

File to upload: cg-nms.odm

File Path: /managed/odm

Override: □

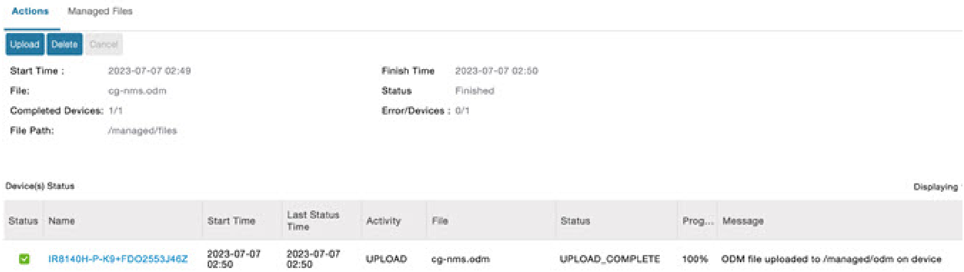
Device search:

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

1 Items selected (Max 1000) Clear Selection

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

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



Start Time : 2023-07-07 02:49

File: cg-nms.odm

Completed Devices: 1/1

File Path: /managed/files

Finish Time 2023-07-07 02:50

Status Finished

Error/Devices : 0/1

Device(s) Status

Displaying

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

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

Troubleshoot TCL Scripts

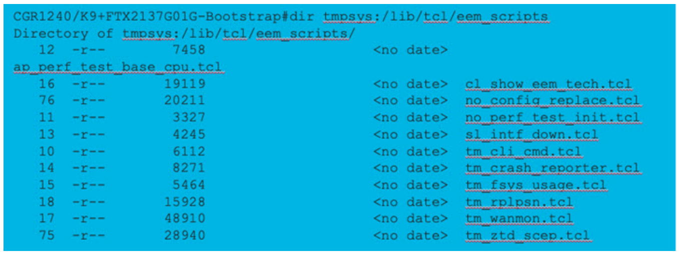
You can find the TCL scripts on a FAR at: `tmpsys:/lib/tcl/eem_scripts`.

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

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

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

Figure 2: Supported Troubleshooting TCL Scripts



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

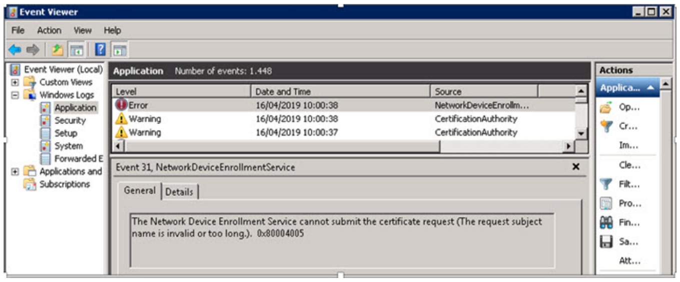
Troubleshoot Certificate Enrollment

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

```
event manager environment ZTD_SCEP_Debug TRUE
```

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

Figure 3: Event Viewer



Application   Number of events: 1.448

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

Event 31, NetworkDeviceEnrollmentService

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

Certificate Enrollment — Test Manual

Step 1 Save the current crypto config:

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

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

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

```
no crypto pki trustpoint LDevID
```

Step 3 Re-add the saved configuration:

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

Step 4 Authenticate with SCEP:

```
crypto pki authenticate LDevID
```

Step 5 Request Certificate:

```
crypto pki enroll LDevID
```

Certificate Enrollment — Example Output

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

Troubleshoot WSMA

Before you begin

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

Step 1 To execute:

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

Step 2 For an OVA install:

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

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

Troubleshoot Tunnel Provisioning

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

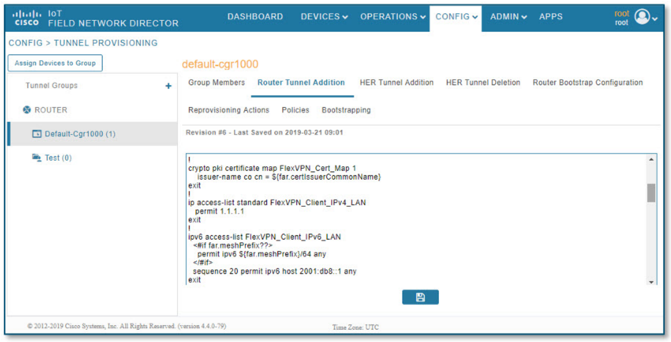
Step 2 Check server.log and optionally increase the log level.

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

Step 4 Debug on FAR using the following commands:

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

Figure 4: CONFIG > Tunnel Provisioning



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

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

Troubleshoot Netconf: FND—HER Communications

Step 1 Start netconf session:

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

Step 2 Device sends hello:

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

Step 3 Send a hello yourself:

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

<hello>

<capabilities>

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

</capabilities>

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

Step 4 Request running config (for example):

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

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

<ns2:get-config>

<source>

<ns2:running/>

</source>

</ns2:get-config>

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

Step 5 Device Response:

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

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

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

!
```

```
version 16.3

service timestamps debug datetime msec

service timestamps log datetime msec

no platform punt-keepalive disable-kernel-core

platform console auto

!

hostname fnd4her
```

Troubleshoot Configuration Deployment

Step 1 Substitute configuration and try manually line by line:

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

Step 3 Debug CGNA/WSMA:

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

Troubleshoot HSM Connectivity

To troubleshoot HSM connectivity:

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

Certificate:

Data:

Version: 1

Serial Number: xxxxxxxxxx

Signature Algorithm: SHA256withECDSA

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

Validity

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

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

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

```
Fingerprints:

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

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

Subject Public Key Info:

Public Key Algorithm: EC

…

Signature Algorithm: SHA256withECDSA
```

Issues Faced During HSM Client Upgrade

IoT FND accesses the HSM Server using the HSM Client.

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

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

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

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

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

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