CGR1240 to IR8140 Migration Guide

Revised: October 9, 2023

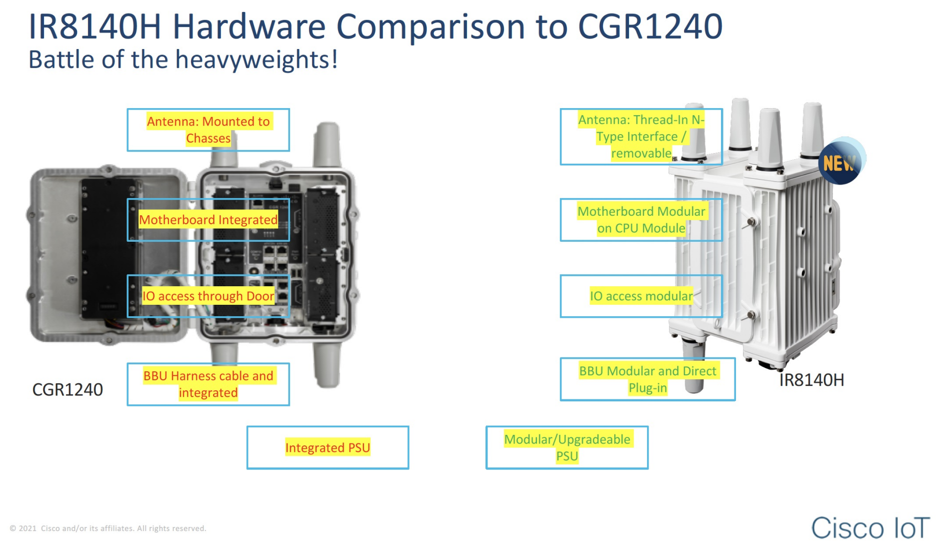
CGR1240 to IR8140 Migration Guide

This document contains high level END USER requirements for migration from CGR to IR8100.

Introduction

This document describes end customer requirements and differences that should be understood when migrating from CGR1240 to IR8140 deployments. The configuration of SNI (Secure Network Infrastructure) that supports ZTD (Zero Touch Deployment) and operations of the router in the field are remarkably similar. However, there are differences that need to be addressed for a successful deployment of IR8140 as a replacement or in addition to the CGR1240 deployments.

Hardware Differences: IR8140 vs CGR1000



IR8140H Hardware Comparison to CGR1240

Battle of the heavyweights!

Antenna: Mounted to Chasses

Motherboard Integrated

IO access through Door

BBU Harness cable and integrated

Integrated PSU

CGR1240

Antenna: Thread-In N-Type Interface / removable

Motherboard Modular on CPU Module

IO access modular

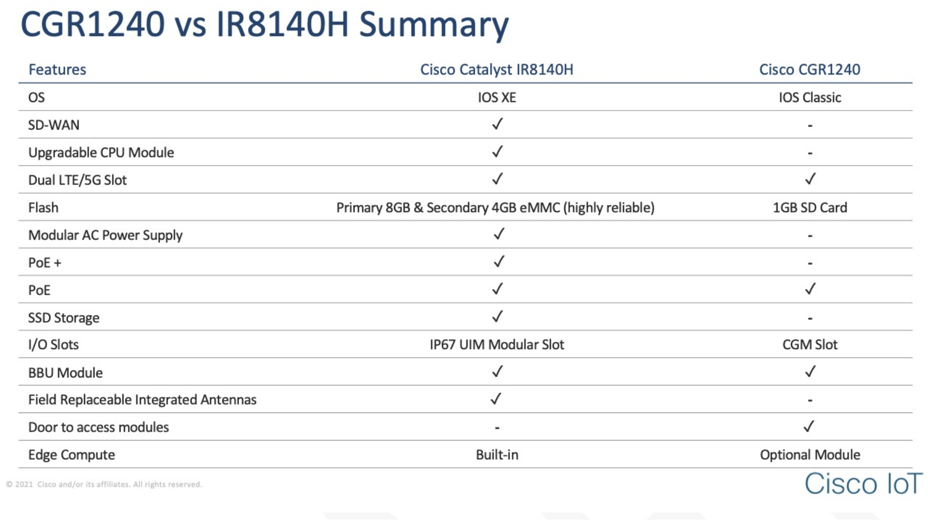
BBU Modular and Direct Plug-in

Modular/Upgradeable PSU

IR8140H

Cisco IoT

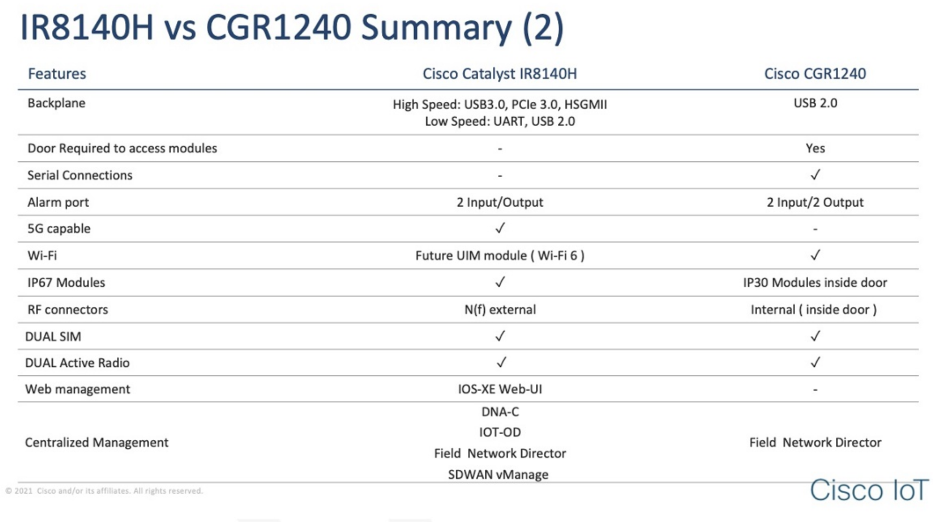
IMPORTANT: The IR8140 chassis can be deployed onto existing CGR1240 pole mount brackets.



CGR1240 vs IR8140H Summary

Features	Cisco Catalyst IR8140H	Cisco CGR1240
OS	IOS XE	IOS Classic
SD-WAN	✓	-
Upgradable CPU Module	✓	-
Dual LTE/5G Slot	✓	✓
Flash	Primary 8GB & Secondary 4GB eMMC (highly reliable)	1GB SD Card
Modular AC Power Supply	✓	-
PoE +	✓	-
PoE	✓	✓
SSD Storage	✓	-
I/O Slots	IP67 UIM Modular Slot	CGM Slot
BBU Module	✓	✓
Field Replaceable Integrated Antennas	✓	-
Door to access modules	-	✓
Edge Compute	Built-in	Optional Module

Cisco IoT



IR8140H vs CGR1240 Summary (2)

Features	Cisco Catalyst IR8140H	Cisco CGR1240
Backplane	High Speed: USB3.0, PCIe 3.0, HSGMII Low Speed: UART, USB 2.0	USB 2.0
Door Required to access modules	-	Yes
Serial Connections	-	✓
Alarm port	2 Input/Output	2 Input/2 Output
5G capable	✓	-
Wi-Fi	Future UIM module (Wi-Fi 6)	✓
IP67 Modules	✓	IP30 Modules inside door
RF connectors	N(f) external	Internal (inside door)
DUAL SIM	✓	✓
DUAL Active Radio	✓	✓
Web management	IOS-XE Web-UI	-
Centralized Management	DNA-C IOT-OD Field Network Director SDWAN vManage	Field Network Director

Cisco IoT

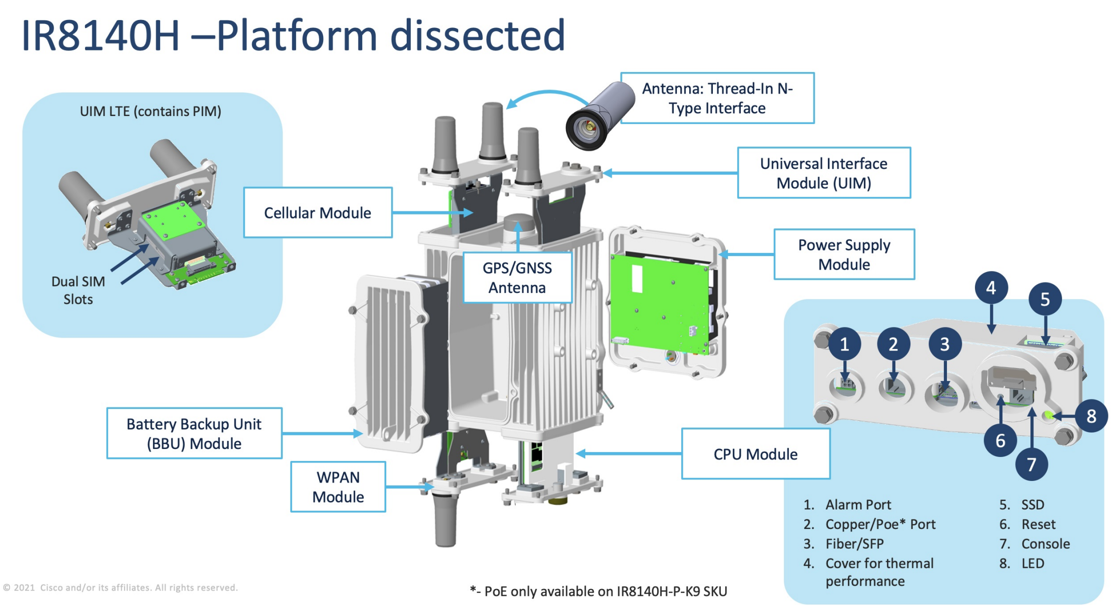
Table 1: Interfaces Naming

	CGR1240	**IR8140H**
Fixed Interfaces	GigabitEthernet0/1, FastEthernet2/3 – 6, GigabitEthernet2/1 – 2 Dot11Radio2/1	GigabitEthernet0/0/0 GigabitEthernet0/0/1
Modular interfaces	Cellular 2-4/1 WPAN 2-4/1	Cellular 0/1-3/0 WPAN 0/1-3/0

IR8140 Hardware Overview

A disassembled IR8140 is shown in Figure 1. These figures show the front and back views of a IR8140 ready for final module insertion such as the Cellular module shown in Figure 4. This unit is assembled to fit the customer’s specifications and has been tested for basic hardware functionality. The system is ready for configuration. For more details about IR8140H hardware, see the Cisco Catalyst IR8140 Heavy Duty Router Installation Guide.

Figure 1: Dissasembled View



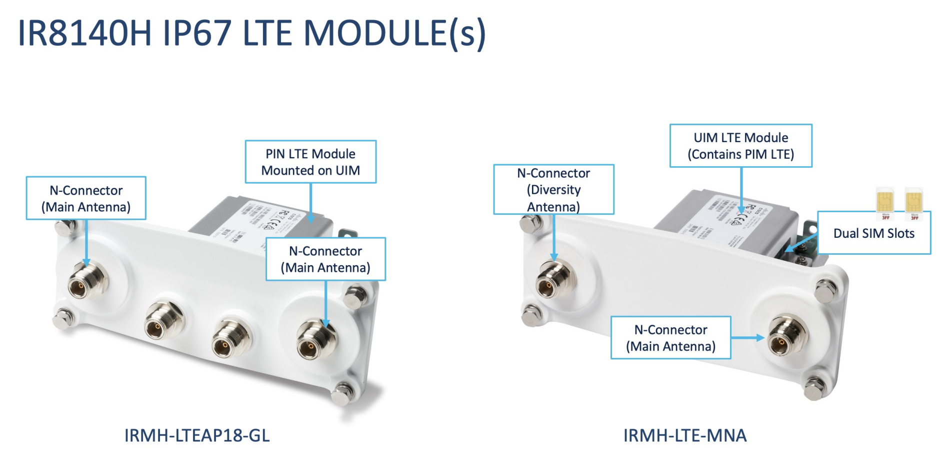
IR8140H –Platform dissected

1. Alarm Port
2. Copper/Poe* Port
3. Fiber/SFP
4. Cover for thermal performance
5. SSD
6. Reset
7. Console
8. LED

© 2021 Cisco and/or its affiliates. All rights reserved.

*- PoE only available on IR8140H-P-K9 SKU

Figure 2: IR8140 Cellular/5G Module



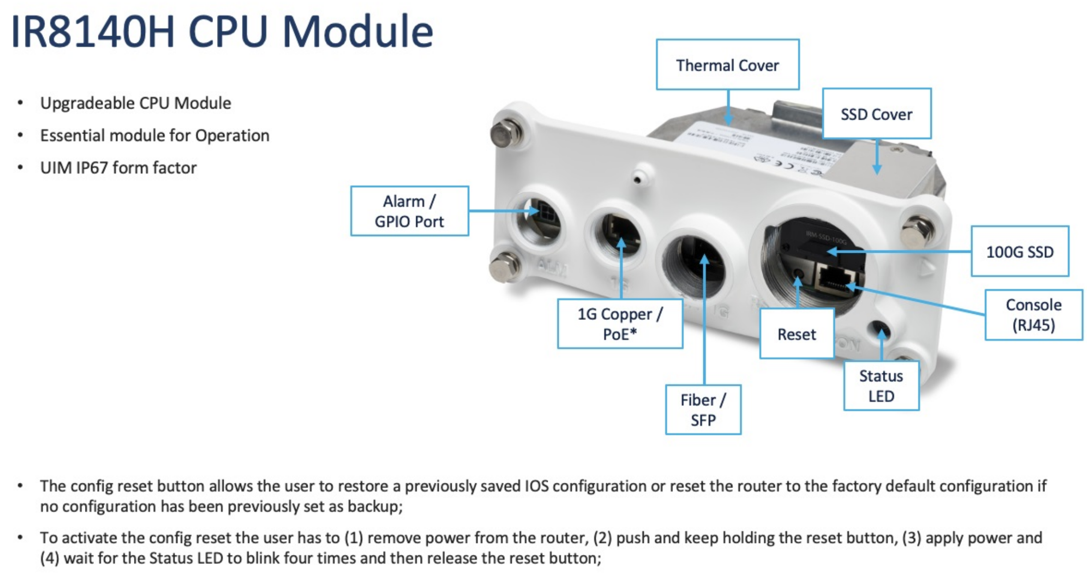
IR8140H IP67 LTE MODULE(s)

N-Connector (Main Antenna)
PIN LTE Module Mounted on UIM
N-Connector (Main Antenna)
N-Connector (Diversity Antenna)
UIM LTE Module (Contains PIM LTE)
Dual SIM Slots
N-Connector (Main Antenna)

IRMH-LTEAP18-GL

IRMH-LTE-MNA

Figure 3: IR8140 CPU Module

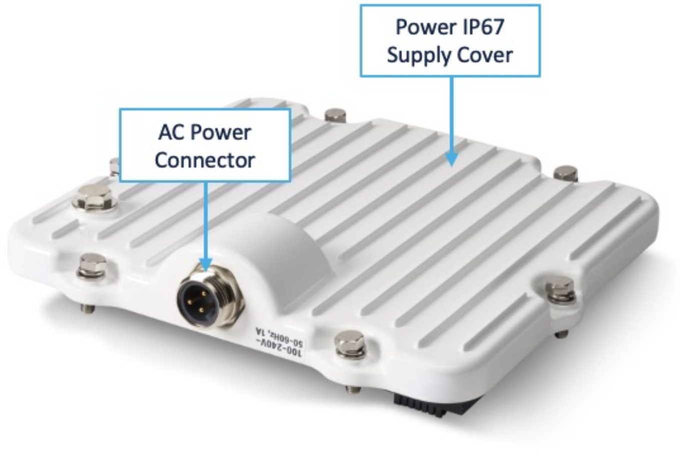


IR8140H CPU Module

- Upgradeable CPU Module
- Essential module for Operation
- UIM IP67 form factor

- The config reset button allows the user to restore a previously saved IOS configuration or reset the router to the factory default configuration if no configuration has been previously set as backup;
- To activate the config reset the user has to (1) remove power from the router, (2) push and keep holding the reset button, (3) apply power and (4) wait for the Status LED to blink four times and then release the reset button;

Figure 4: IR8140 Power Module



This table describes the different hardware components included in an IR8140:

Name	**Fixed or Modular**	**Description**
Module Slot 0	Modular	CPU module (contains Fiber + Copper ports
Module Slot 1	Modular	Typically houses the WPAN card
Module Slot 2	Modular	Typically houses the Cellular module
Module Slot 3	Modular	(Optional) 2nd Cellular or WPAN module

All configuration operations are performed through either (1) the console port or (2) GigabitEthernet port GigabitEthernet 0/0/0 or Fiber GigabitEthernet0/0/1 (see Figure 3) . The console port uses a standard RJ45 console cable connected to the IR8140 console port on the CPU module located at the bottom of the IR8140 as shown in Figure 1. This console is configured to use the settings 9600/8/N/1.

Power is connected to a standard power outlet using the supplied power cord. IR8140's software image is stored in the bootflash (eMMC).

In addition, a secondary eMMC storage for automatic file corruption recovery is added to this platform. This redundancy is critical because these systems are installed on utility poles, and to access and recover them otherwise will require a truck roll.

Software Differences: IR8140 vs CGR1000

The following sections describe the main differences between the configuration required on IOS XE software supported on IR8140H vs. IOS software supported on CGR1000. In addition, if more details are required about the configuration, visit Cisco Catalyst IR8140 Heavy Duty Series Router Software Configuration Guide.

Installation

CGR1240H follows this order of boot sequence:

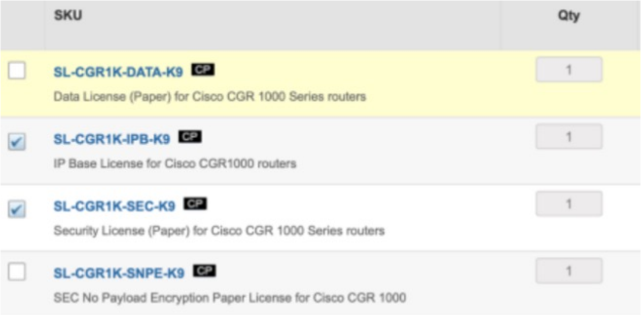
1. Power on
2. Hypervisor Image (Rommon-1>)
3. System image (Rommon-2>)
4. Normal Operation for IOS

In contrast, IR8140H follows this order of boot sequence:

1. Power on
2. System image (Rommon>)
3. Normal Operation for IOS XE

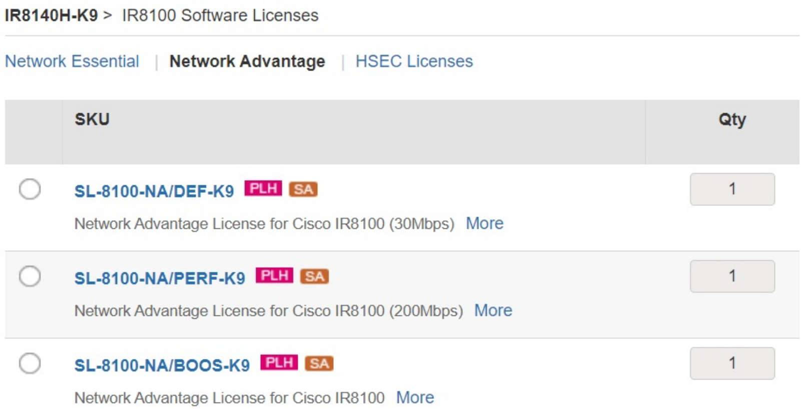
Licensing

The CGR1240 is ordered usually with the SL-CGR1k-SEC-K9 license, and there is no need to do any configuration on the router. Currently, ordering of CGR1240 security license is from CCW (Cisco Commerce Workspace):



	SKU	Qty
☐	SL-CGR1K-DATA-K9 CP Data License (Paper) for Cisco CGR 1000 Series routers	1
☑	SL-CGR1K-IPB-K9 CP IP Base License for Cisco CGR1000 routers	1
☑	SL-CGR1K-SEC-K9 CP Security License (Paper) for Cisco CGR 1000 Series routers	1
☐	SL-CGR1K-SNPE-K9 CP SEC No Payload Encryption Paper License for Cisco CGR 1000	1

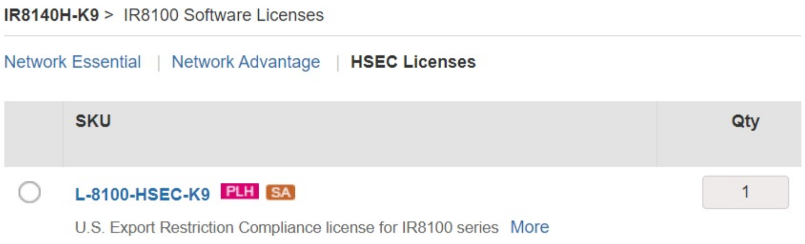
In IR8140H, WPAN and Mesh Management requires a Network-Advantage license to recognize the WPAN and enable the mesh security feature. For the use cases that require higher throughput (>200 MB), it necessitates HSEC license in additional to the boost license to get more than 200 MB encrypted traffic. Order the Network-Advandage and HSEC license from CCW:



IR8140H-K9 > IR8100 Software Licenses

Network Essential | **Network Advantage** | HSEC Licenses

	SKU	Qty
○	SL-8100-NA/DEF-K9 PLH SA Network Advantage License for Cisco IR8100 (30Mbps) More	1
○	SL-8100-NA/PERF-K9 PLH SA Network Advantage License for Cisco IR8100 (200Mbps) More	1
○	SL-8100-NA/BOOS-K9 PLH SA Network Advantage License for Cisco IR8100 More	1



IR8140H-K9 > IR8100 Software Licenses

Network Essential | Network Advantage | **HSEC Licenses**

	SKU	Qty
○	L-8100-HSEC-K9 PLH SA U.S. Export Restriction Compliance license for IR8100 series More	1

User must enable Advandage license on IOS XE and install HSEC, if it is not installed on the router.

```
IR8140H(config)#license boot level ?
  network-advantage   License Level Network-Advantage
  network-essentials  License Level Network-Essentials
IR8140H(config)#license boot level NEtwork-Advantage
% use 'write' command to make license boot config take effect on next boot

IR8140H#wr
```

After reload:

```
IR8140H#show license summary
License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage_2G   (IR8100_P_2G_E)                    1 IN USE
  IR8100 HSEC             (IR8100_HSEC)                     0 NOT IN USE
```

FND Licensing

IR8100 requires an “IOTFND-IR8100” license type on FND to start managing devices.

IR8140 FND License:

```
Subscription PID:
Top line PID: IOTFND-SOFTWARE-K9
1/3/5 Year options: IOTFND-IR8100
```

```
Top line PID: IOTFND-SUB-K9-10
10-Year Option: IOTFND-IR8100-10
```

CGR1240 FND License:

```
Perpetual PID:
Top line PID: IOT-FND
Perpetual PID: L-IOTFND-CGR1000

Subscription PID:
Top line PID: IOTFND-SOFTWARE-K9
1/3/5 Year options: IOTFND-CGR1000

Top line PID: IOTFND-SUB-K9-10
10-Year Option: IOTFND-CGR1000-10
```

FND/TPS Certificates for IR8140 Management

All communications between the managed routers and the Cisco IoT Field Network Director (IoT FND) must be authenticated in both directions through mutual authentication. Before mutual authentication occurs, the Cisco IoT FND and the device must each have a certificate signed by the same Certificate Authority (CA). The certificates for TPS and FND must be added to their respective keystores. See FND Installation Guide for step-by-step instructions.

If the FND server managed CGOS-based CGR1000 routers, the FND and TPS servers' certificates likely contained OIDs for Command Authorization Support.

Due to stricter TLS implementation of the IR8140, these OIDs will cause failure during HTTP/SSL handshake during FND provisioning.

For a fresh installation of FND, ensure that certificates for the FND and TPS servers are generated without the OIDs for command authorization support.

If upgrading from a previous version of FND that supported CGOS routers, new certificates for the TPS and FND will have to be issued without the OIDs and updated in the respective cgms_keystore files to support IR8140 management.

Support for Dual WPAN

IR8140 supports up to two WPAN modules. While in CGR1240, we support just one module.

SNI Migration

This section providing information about SNI migration.

NPS and AAA requirements

NPS server policy needs to be modified wherever the string CGR1240 is used to match policies to authenticate the device – the PID (Product Identifier) needs to be updated to IR8140. **Keep in mind that the PID of the PoE version is IR8140H-P-K9, and the Non-PoE is IR8140H-K9.**

Refer to CGR1000 guide for enrollment if needed :

https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/certificates/CertsGuide_cgr1000.html

In particular, pay attention to step 13 in section "Defining a Connection Policy"– In Attribute manipulation rule, enter the appropriate PID+SN for the IR8140.

SCEP and RA configuration

With IOS CGRs – the RA was using CISCO SUDI (Secure Unique Device Identifier) with 2029 expiry. **For IR8140, the SUDI has been updated to use 2099 expiry**. This means that the RA will need to support both SUDI authentications temporarily until the migration to IR8140 is complete. The following configuration is an example to support both SUDI types on ISR4431 version 17.4.1:

Create a trustpoint “CA IR8140_SUDI_CA” containing the SUDI 2099 certificate:

```
crypto  pki trustpoint IR8140_SUDI_CA
enrollment terminal
exit
crypto pki authenticate IR8140_SUDI_CA
-----BEGIN CERTIFICATE-----
MIIEZzCCA0+gAwIBAgIJCmR1UkzYYXxiMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODEx
MjAyODA4WhgPMjA5OTA4MDkyMDU4MjdaMDExHzAdBgNVBAMTFkhpZ2ggQXNzdXJh
bmNlIFNVREkgQ0ExDjAMBgNVBAoTBUNpc2NvMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAvdzeSWdDI6lRZDYRvA6JqaRvQyy6Dx1WaqI82UeKR4ZRn0ef
xMGvp4c88/VMS8WSjQO1qolMfMxqHkcSiFBOULx6Trquw4TrEf9sIuzvgJvDaEa8
IllXPwtPtNqZEIWi8jlinz2uGam93KuGPcioHfruzbDKWHL/HWFGYMgz+OKwhD3J
4NRySknQvUovfV8eWLeVOqW8rbnG3TZxv5VexOiK4jL3ObvsQPuAWUwUoo7nuFlE
GTG/VCeyCe/H8+afIScbZOkI9xejtckflnBYFVCyFxzm2H3YZatb6ohbyRXLtOPj
T3SJ+OOoYMlSLd28z727LpRbFFLGYhyWxEXDuQIDAQABo4IBgjCCAX4wDgYDVR0P
AQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwfwYIKwYBBQUHAQEEczBxMEEG
CCsGAQUFBzAChjVodHRwczovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2Nl
cnRzL2NyY2EyMDk5LmNlcjAsBggrBgEFBQcwAYYgaHR0cDovL3BraWN2cy5jaXNj
by5jb20vcGtpL29jc3AwHwYDVR0jBBgwFoAUOJVXDzQjTvOhJiC6FJHHQYgdo1sw
UgYDVR0gBEswSTBHBgorBgEEAQkVAR4AMDkwNwYIKwYBBQUHAgEWK2h0dHA6Ly93
d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9wb2xpY2llcy8wQwYDVR0fBDwwOjA4
oDagNIYyaHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2NybC9jcmNh
MjA5OS5jcmwwHQYDVR0OBBYEFOpro7nBE5d+G/s6jWhgBzlfh0j6MA0GCSqGSIb3
DQEBCwUAA4IBAQBcqYEOgAHhGWKndwM901XX2Enh4hjXR5avDg7G/f6Tb9H509dt
QW+AeZGEghhwUrw1EeG79tHkncAe+m+64xMC1ttyI1RSyn8rBqQYkXnnCRbtF/Nw
pQe5fjvdeIFWJhUI16TOt/ZlkNnWnLsUU1alZmN+J/FhSr8VTJWGRM9gY8hefH8f
5U7LMiDXxsFVHB7R6KGNjvtawrl6W6RKp2dceGxEIIvMahgMWWHHiWOQAOtVrHuE
NEjYR/7klLLwdgQF/NNCA2z47pSfMFnBcr8779GqVIbBTpOP2E6+1pBrE2jBNNoc
uBG1fgvh1qtJUdBbTziAKNoCo4sted6PW2/U
-----END CERTIFICATE-----
quit
Trustpoint 'IR8140_SUDI_CA' is a subordinate CA and holds a non self signed cert
Certificate has the following attributes:
       Fingerprint MD5: E6897BC6 27D7C558 A2330EC7 C2D7A10B
      Fingerprint SHA1: F81D5550 D67DCD1D D11192B5 7F8FDE09 A4A569B7

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

You can check it via the following:

```
show crypto pki certificate verbose IR8140_SUDI_CA
```

Change the grating trustpoint to a tp-list:

```
configure terminal
crypto pki server UTILITY_RA
no grant auto trustpoint ACT2_SUDI_CA
grant auto tp-list ACT2_SUDI_CA IR8140_SUDI_CA
```

IMPORTANT: It is required to **no** the “auto trusthpoint” and then add the “auto tp-list” as they are mutually exclusive. Also, the trustpoint names are “space” delimited.

Refer to Configuring Certificate Renewal by Enabling Multiple Trustpoints for more information.

IDevID Certificate and Subject Alternative Names

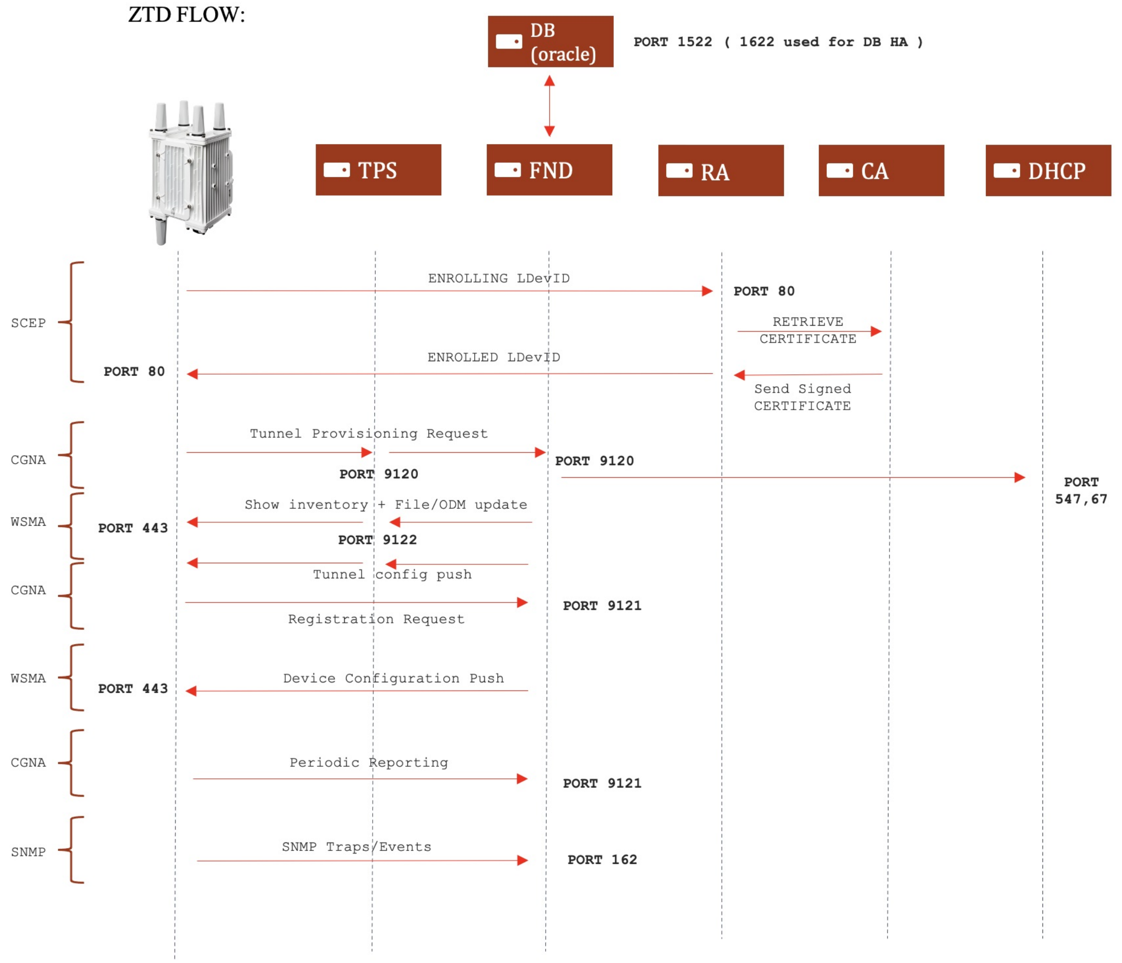
Note If using a CN.<domain name> in the CSR signing , please make sure the signing CA is equipped to handle alternate names. The IR8140H will auto-create a subject-alt-name line for the router under the LDevID trustpoint if a domain name is added to the CN .

Example:

```
subject-name serialNumber=PID:IR8140H-K9 SN:FDO2515JD0B,CN=IR8140.cisco.com
subject-alt-name IR8140.cisco.com
```

FND State machine, Firewall ports, and ZTD

The TLS (Transport Layer Security) default ports is being changed to **443** from **8443** for FND mutual HTTPS auth on IOS XE. FND communicates with IOS XE using port 443.

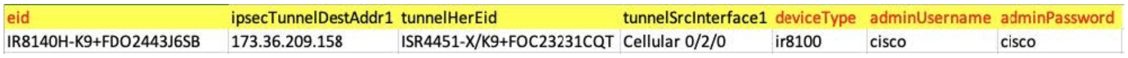


Notice of Shipment File (Requirements) (Min FND version 4.8)

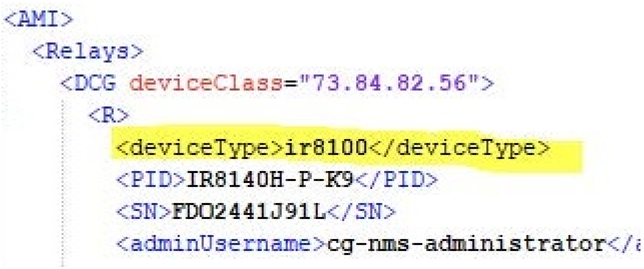
FND defines and classifies the IR8140 as an IR8100 ‘deviceType’, as a results all properties and groups in FND carry forward the principles of defining separate groups for the device.

To create notice of shipment file to add to FND (CSV or XML) :

Mandatory Fields (red required for Provisioning Tunnels from FND):

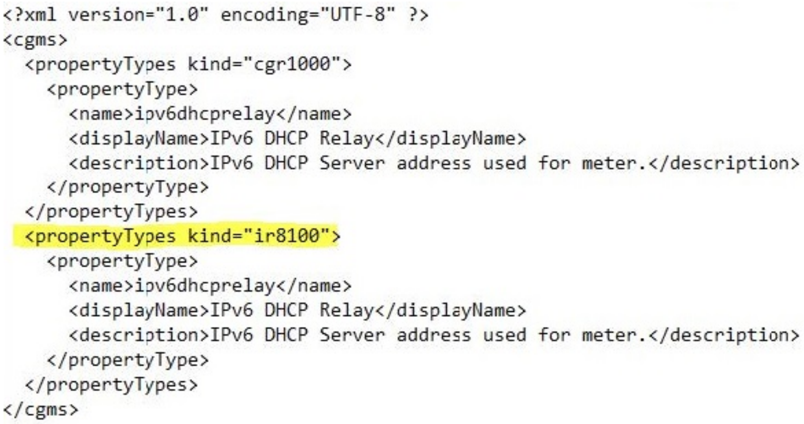


eid	ipsecTunnelDestAddr1	tunnelHerEid	tunnelSrcInterface1	deviceType	adminUsername	adminPassword
IR8140H-K9+FDO2443J6SB	173.36.209.158	ISR4451-X/K9+FOC23231CQT	Cellular 0/2/0	ir8100	cisco	cisco



```
<AMI>
  <Relays>
    <DCG deviceClass="73.84.82.56">
      <R>
        <deviceType>ir8100</deviceType>
        <PID>IR8140H-P-K9</PID>
        <SN>FDO2441J91L</SN>
        <adminUsername>cg-nms-administrator</
```

If you use the **userPropertyType.xml** in /opt/cgms/server/conf/userPropertyTypes.xml, you'll need to update it by adding the ir8100 as a device type.



```
<?xml version="1.0" encoding="UTF-8" ?>
<cgms>
  <propertyTypes kind="cgr1000">
    <propertyType>
      <name>ipv6dhcprelay</name>
      <displayName>IPv6 DHCP Relay</displayName>
      <description>IPv6 DHCP Server address used for meter.</description>
    </propertyType>
  </propertyTypes>
  <propertyTypes kind="ir8100">
    <propertyType>
      <name>ipv6dhcprelay</name>
      <displayName>IPv6 DHCP Relay</displayName>
      <description>IPv6 DHCP Server address used for meter.</description>
    </propertyType>
  </propertyTypes>
</cgms>
```

Examples of FND Template for IR8140 AMI Use Cases

These are examples of the templates used by our solution and services teams to deploy the router. For reference only.

1. Tunnel Template (This template will handle both CGRs and IR8100s.)

```
<#if far.eid?contains("IR81") || far.eid?contains("IR11")>
   <#assign isRunningIosXe=true>
<#else>
    <#assign isRunningIosXe=false>
</#if>

<#if !(far.ipsecTunnelDestAddr1??)>
 ${provisioningFailed("FAR property ipsecTunnelDestAddr1 is undefined.")}
</#if>

aaa authorization network FlexVPN_Author local
```

```
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = FANRSACA.cisco.com

<#if !(far.dhcpV6LoopbackLink??)>
 ${provisioningFailed("FAR property dhcpV6LoopbackLink is undefined.")}
<#else>
 ipv6 unicast-routing
 <#if !isRunningIosXe>
    ipv6 cef
 </#if>
 interface Loopback0
   ipv6 address ${far.ipv6Address(far.enDuid,0,far.dhcpV6LoopbackLink).address}/128
 interface Tunnel10
   ipv6 unnumbered Loopback0
   ipv6 mtu 1280
   ipv6 tcp adjust-mss 1240
</#if>

<#if (far.meshPanidConfig??)>
 <#if !far.eid?contains("IR81")>
    ipv6 access-list bmr-prefix
      permit ipv6 2001:abcd:1::/56 any

    route-map conn2Ikev2 permit 10
      match ipv6 address bmr-prefix
    route-map conn2Ikev2 permit 20
      match interface loopback0 wpan4/1

    crypto ikev2 authorization policy FlexVPN_Author_Policy
      route redistribute connected route-map conn2Ikev2
 <#else>
    ipv6  access-list local-prefixes
      permit ipv6 ${far.meshPrefixConfig}/${far.meshPrefixLengthConfig} any
      permit ipv6 2001:abcd:1::/56 any

    crypto ikev2 authorization policy FlexVPN_Author_Policy
      route set interface
      route set access-list ipv6 local-prefixes
 </#if>
<#else>
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
</#if>


crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal

crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 no lifetime certificate
 dpd 30 3 on-demand
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy

crypto ikev2 fragmentation mtu 1000
crypto ikev2 redirect client
crypto ikev2 nat keepalive 10

crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile FlexVPN_IPsec_Profile
 set security-association lifetime days 1
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group19
 set ikev2-profile FlexVPN_IKEv2_Profile


interface Tunnel10
 description to ${her.eid}
 tunnel source ${far.tunnelSrcInterface1}
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile


crypto ikev2 client flexvpn VPN_LB
  peer 1 ${far.ipsecTunnelDestAddr1}
  client connect Tunnel10
```

2. Configuration Template

```
<#--
    If a Loopback0 interface is present on the device (normally configured
    during tunnel provisioning) then use that as the source interface for
    the HTTP client, SNMP traps and RADIUS protocol. The source for the HTTP client is not
    changed during tunnel provisioning because usually the addresses assigned
    to the loopback interface are only accessible through the tunnels.
    Waiting insures the tunnel is configured correctly and comes up.
  -->
  <#if far.interfaces("Loopback0")?size != 0>
    ip http client source-interface Loopback0
    snmp-server trap-source Loopback0
    ipv6 radius source-interface loopback0
  </#if>

  <#-- Enable periodic inventory notification to report metrics. -->
    cgna profile cg-nms-periodic
      interval 60
    exit

  <#-- Enable periodic configuration (heartbeat) notification. -->
  cgna heart-beat interval 20

  <#-- Interfaces configuration -->
  interface ${far.tunnelSrcInterface1}
   no ip redirects
   no ip unreachables
   no ip proxy-arp

  line console 0
   exec-timeout 5

  line vty 0 4
   exec-timeout 5
   transport input ssh
   transport output none

  service nagle
  no service pad
  service tcp-keepalives-in
  service tcp-keepalives-out
  service timestamps debug datetime msec localtime
  service timestamps log datetime msec localtime
  service password-encryption
  service sequence-numbers
  no ip source-route
  no ipv6 source-route
  no ip gratuitous-arps
  no ip bootp server
  no cdp run
  no ip finger
  no boot network
  ip tcp synwait-time 5
  ip tcp path-mtu-discovery
  ip tcp mss 1460

<#if (far.meshPrefixConfig??)>

 radius server fanheradius
  address ipv6 fd10::1:10 auth-port 1812 acct-port 1813
  key rhHHBiMZ

 aaa group server radius radius-group
   server name fanheradius

 aaa authentication dot1x default group radius-group

 dot1x system-auth-control

 ipv6 multicast-routing
 ipv6 multicast pim-passive-enable

 ipv6 pim rp-address fd10::2:20a


 <#if far.meshPrefixConfig?matches(".*::.*")>
   <#assign mcastAddress="ff38:40:${far.meshPrefixConfig}"+"1">
 <#else>
   <#assign sublist=far.meshPrefixConfig?split(":")[0..5]>
   <#assign mcastAddress="ff38:40:"+sublist[0]+":"+sublist[1]+":"+sublist[2]+":"+sublist[3]+"::1">
 </#if>

 int loopback 0
  ipv6 mld join-group ${mcastAddress}
  ipv6 pim passive

 interface Wpan0/1/0
  no ip address
  ip broadcast-address 0.0.0.0
  ieee154 beacon-async min-interval 10 max-interval 60 suppression-coefficient 1
  ieee154 panid ${far.meshPanidConfig}
  ieee154 phy-mode 2
  ieee154 ssid Mesh
  ieee154 phy-mode 66 166 <<< needed only for WISUN mode deployment
  ieee154 beacon-ver-incr-time 0 <<< needed only for WISUN mode deployment
  wisun-mode <<< needed only for WISUN mode deployment
  dtls-relay fd10::1:13 port 61629 max-sessions 20 lifetime 120
  rpl dag-lifetime 60
  rpl dio-min 15
  rpl dio-dbl 2
  rpl version-incr-time 10
  outage-server fd10::1:d
  authentication host-mode multi-auth
  authentication port-control auto
  ipv6 address ${far.meshAddressConfig}/64
  ipv6 enabled
  ipv6 dhcp relay destination  fd10::1:b
  no ipv6 pim
  dot1x pae authenticator
  mesh-security max-active-key-exchange 10
  mesh-security max-active-authentication 15
  mesh-security authentication-timeout 45
  no shut

</#if>

<#-- Enable BBU (Battery Backup Unit) discharge if one is present -->
<#if far.hasActiveBattery()>
   do request platform hardware battery enable
</#if>

Add section for CRM
                                             END OF CONFIGURATION
```

Frequently Asked Questions

Certificates Used in Cisco Industrial Solution

Certificate Name	Source	Signed By	Installed By	Manufacturing Process	Required By
IDevID	Generated by Cisco	Cisco CA	Cisco Manufacturing	Pre-configured	Cisco Identification of Device, SCEP
Customer Issuer CA Certificate	Generated by customer CA. Needs to be delivered to manufacturing.	Customer root CA	Partner	Manually imported or dynamically during SCEP	CGNA, FND, IKEv2
LDevID	Option 1: Generated by FAR	Customer Issuer CA	FAR via SCEP Process in the field	Partner enters SCEP Provisioning Commands	CGNA, FND, IKEv2
	Option 2: Generated off-box by Utility CA on behalf of the FAR using FAR’s unique information (product id + serial no)		Partner	Generated and imported via script.	

Common Commands that are different on IR8140

Some commands are different because of the new OS – IOS-XE.

Reload modules:

```
IR8140#show platform
Chassis type: IR8140H-P-K9

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         IR8140H-P-K9        ok                    2w5d
 0/0      IR8140H-2x1GE       ok                    2w5d
 0/1      IRMH-WPAN-NA        ok                    2w5d
 0/2      IRMH-LTEA-LA        ok                    2w5d
R0        IR8140H-P-K9        ok, active            2w5d
F0        IR8140H-P-K9        ok, active            2w5d
P0        IRMH-PWR60W-AC      ok                    2w5d
```

Eg: reloading a cellular module:

```
IR8140(config)#hw-module subslot 0/2 ?
  3rdparty-mode  Assign this slot for 3rd-party module
  battery-mode   Power-off the target subslot when powered by backup-battery
  shutdown       Shutdown the target subslot
IR8140(config)#hw-module subslot 0/2 shutdown unpowered
IR8140(config)#no hw-module subslot 0/2 shutdown unpowered

OR

IR8140#hw-module subslot 0/2 reload
```

GPS:

```
IR8140H#show platform hardware gnss details
GNSS details:

Status: GNSS fix acquired
Time: 2023-01-10 17:08:55 UTC
Latitude: 37 Deg 25 Min 6.075 Sec North (37.418354)
Longitude: 121 Deg 55 Min 9.58 Sec West (-121.919327)
Height: 26.4m
Fix type: 3D PDOP: 1.58 HDOP: 1.04 VDOP: 1.18

Total RMS standard deviation: NA
Latitude error: 6.1m Longitude error: 6.0m Altitude error: 13.0m

GPS:

6 satellites used for fix: 3, 4, 7, 9, 26, 31
13 satellites in view
ID = 01 elevation = 05 azimuth = 199 CN0 = 10
ID = 03 elevation = 65 azimuth = 174 CN0 = 27
ID = 04 elevation = 66 azimuth = 344 CN0 = 21
ID = 06 elevation = 17 azimuth = 300 CN0 = 21
ID = 07 elevation = 25 azimuth = 239 CN0 = 26
ID = 09 elevation = 36 azimuth = 302 CN0 = 25
ID = 11 elevation = 00 azimuth = 331 CN0 = NA
ID = 16 elevation = 46 azimuth = 113 CN0 = 17
ID = 22 elevation = 04 azimuth = 093 CN0 = 11
ID = 26 elevation = 36 azimuth = 063 CN0 = 23
ID = 31 elevation = 05 azimuth = 052 CN0 = 18
ID = 46 elevation = 46 azimuth = 192 CN0 = NA
ID = 48 elevation = 46 azimuth = 185 CN0 = NA

GLONASS:

1 satellites used for fix: 76
10 satellites in view
ID = 65 elevation = 00 azimuth = 124 CN0 = NA
ID = 67 elevation = 58 azimuth = 350 CN0 = 20
ID = 68 elevation = 14 azimuth = 317 CN0 = NA
ID = 76 elevation = 40 azimuth = 036 CN0 = 23
ID = 77 elevation = 79 azimuth = 144 CN0 = NA
ID = 78 elevation = 24 azimuth = 201 CN0 = NA
ID = 82 elevation = 02 azimuth = 254 CN0 = NA
ID = 83 elevation = 09 azimuth = 294 CN0 = NA
ID = 84 elevation = 01 azimuth = 349 CN0 = NA
ID = 92 elevation = 14 azimuth = 316 CN0 = NA

GALILEO:

3 satellites used for fix: 5, 9, 36
11 satellites in view
ID = 01 elevation = 06 azimuth = 034 CN0 = NA
ID = 03 elevation = 05 azimuth = 291 CN0 = NA
ID = 04 elevation = 13 azimuth = 099 CN0 = NA
ID = 05 elevation = 52 azimuth = 314 CN0 = 26
ID = 09 elevation = 59 azimuth = 068 CN0 = 17
ID = 15 elevation = 09 azimuth = 320 CN0 = NA
ID = 24 elevation = 47 azimuth = 154 CN0 = 17
ID = 25 elevation = 06 azimuth = 193 CN0 = NA
ID = 31 elevation = 47 azimuth = 074 CN0 = 21
ID = 34 elevation = 21 azimuth = 271 CN0 = 18
ID = 36 elevation = 12 azimuth = 220 CN0 = 14
```

NTP:

Hardware clock is automatically updated from NTP server configured without "ntp update-calendar" command in global configuration.

BBU:

You can use the following command to enable or disable BBU:

request platform hardware battery {**enable** | **disable**}

Use the following command to show BBU status:

show platform hardware battery {**brief** | **details** | **event-log** | **pins** | **short** | **sprom** | **unit**}

Setup WPAN (IRMH-WPAN-NA) to Function Like CGR WPAN (CGM-WPAN-FSK-NA)

The IRMH-WPAN-NA supports various physical protocols. Select FSK for compatibility with CGR WPAN modules. Please see template examples for further information.

Adding WPAN configuration is the same as CGR:

```
interface Wpan0/1/0
 ieee154 phy-mode 2
```

Minimal setup:

```
!
interface WPAN0/1/0
no ip address
no shutdown
ieee154 phy-mode 2
ieee154 panid 9016
ieee154 ssid sqaFT06
outage-server 2620:CB:0:1006:1480:100:0:131
ipv6 address 2620:CB:0:9016::/64
ipv6 enable
ipv6 dhcp relay destination 2620:CB:0:1006:1480:100:0:221
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
```

```
no mop enabled
no mop sysid
!
```

Troubleshooting

ISSUE: PKIX path validation failed

Log:

```
5801: localhost.localdomain: Oct 25 2022 14:38:21.642 +0000: %IOTFND-3-UNSPECIFIED:
%[ch=CiscoIosTunnelProvServlet$CiscoIosTunnelProvProcess][eid=IR8140H-K9+FDO2515JDBU]
[ip=10.236.2.2][sev=ERROR][tid=IOS CGR Tunnel-1]:
Tunnel provisioning request for element [IR8140H-K9+FDO2515JDBU] failed [javax.xml.ws.soap.SOAPFaultException:

sun.security.validator.ValidatorException: PKIX path validation failed:
 java.security.cert.CertPathValidatorException: validity check failed].
75802: localhost.
```

Solution:

Subbordinate or signing CA must have an alias in the keystore of “subca”:

```
keytool -import -trustcacerts -alias subca -keystore cgms_keystore -file subca.pem
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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