



Cisco Wireless Gateway for LoRaWAN Software Configuration Guide

First Published: 2017-06-22

Last Modified: 2022-11-30

Americas Headquarters

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

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

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017-2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

Preface ix

Conventions ix

Related Publications x

Obtaining Documentation and Submitting a Service Request x

CHAPTER 1

Overview 1

Overview 1

Switching to Virtual Mode 2

GPS Channel Plans 2

Displaying System Information 5

Displaying Version Information 5

Displaying Platform Status 5

Displaying AES Key 6

Displaying GPS Information 6

Displaying FPGA Information 7

Displaying Inventory Information 7

Displaying Radio Information 8

Displaying Certificate Information 9

CHAPTER 2

Assigning IP Address and Domain Name Server 11

Assigning IP Address 11

Configuring DHCP 11

Understanding DHCP 11

Enabling DHCP on Interfaces 12

Manually Assigning IP Information	12
Configuring DNS	13
DNS Client	13
Name Servers	13
DNS Operation	14
Configuring DNS Server	14
Mapping Hostnames to IP Addresses	14

CHAPTER 3**Administering the Cisco LoRaWAN Gateway** 17

Managing the System Time and Date	17
Network Time Protocol (NTP)	17
NTP Version 4	17
Configuring NTP Server	18
Configuring a System Name and Prompt	18
Configuring GPS as the Clock Source	19
Configuring UBX Support for GPS	19
Checking and Saving the Running Configuration	20
Reloading IXM	20
Using Reset Button	20

CHAPTER 4**Configuring VLAN** 21

Configuring IP Address for VLAN	21
Configuring VLAN Trunks	22
Configuring a Trunk Port	22
Defining the Allowed VLANs on a Trunk	22
Enabling Sending and Receiving Tagged Packet on Ethernet Port	23
Examples of Show Commands	24

CHAPTER 5**Configuring CDP** 25

Understanding CDP	25
Configuring CDP	25
Enabling and Disabling CDP	25
Configuring the CDP Characteristics	26

CHAPTER 6**Configuring Authentication 27**

- Preventing Unauthorized Access 27
- Protecting Access to Privileged EXEC Commands 27
 - Configuring Enable Secret Passwords with Encryption 27
 - Configuring Username and Password for Local Authentication 28
- Configuring Secure Shell 29
 - Configuring IP SSH Limit Local 30
 - Displaying the SSH Configuration and Status 31
 - Using SCP to Upload Files 31
- SSH Access Over IPsec Tunnel 32
- Configuring Reverse SSH and Connecting to Container 32
 - Configuring Reverse SSH 32
 - Copying Files From the Container 33
- Changing Private Network Between Host and Container 33
- User Accounts 34
- Configuring Logging in Container 35

CHAPTER 7**Configuring IPsec 37**

- Understanding IPsec 37
- Configuring IPsec 37
- Configuring Crypto IPsec Profile Common 39
- Configuring Crypto IPsec Profile Individual 41
- Basic Configuration for RSA to Connect to Primary and Secondary 42
- Locking Traffic to IPsec Tunnels 43
- Erasing IPsec Certificates and Key 43
- Uploading Certificates from USB or Local Flash 43
- Disabling LXC Restart During IPsec Reauthentication 43
- Resetting Secure-Storage for Certificate Download 43

CHAPTER 8**Configuring PPPoE 45**

- PPPoE Client Overview 45
- Configuring the Dialer Interface 45
- Configuring the Ethernet Interface 47

Enabling the PPPoE Service 47

Monitoring and Debugging the PPPoE Configuration 48

PPPoE Configuration Examples on IXM and IR829 49

CHAPTER 9

Managing Packet Forwarder 55

Uploading or Downloading Packet Forwarder 55

Managing Packet Forwarder 56

Managing Common Packet Forwarder (CPF) 57

Understanding Common Packet Forwarder 57

Configuring Common Packet Forwarder 57

Guidelines and Limitations of Configuring RX Channel Frequency and Bandwidth 61

Debugging Common Packet Forwarder 62

CHAPTER 10

Managing Plug-n-Play (PnP) 65

Understanding Plug-n-Play 65

Configuring Plug-n-Play 65

Debugging Plug-n-Play 67

CHAPTER 11

Smart Licensing Using Policy 69

Overview of Smart Licensing Using Policy 69

Smart Account 70

Virtual Account 70

Architecture 70

Product Instance 70

Cisco Smart Software Manager (CSSM) 71

Cisco Smart Licensing Utility (CSLU) 71

Concepts 71

License Enforcement Types 72

License Duration 72

Authorization Code 72

Policy 72

Understanding Policy Selection 73

RUM Report and Report Acknowledgement 74

Trust Code 74

Supported Topologies	74
Workflow for Topology: Full Offline Access	76
Workflow for Topology: CSLU Has Access to CSSM	77
Workflow for Topology: CSLU Has No Access to CSSM	80
Removing the Product Instance from CSSM	85

CHAPTER 12**Working with Configuration Files and Software Images 87**

Managing Files	87
Copying Files	87
File Management Commands	88
Working with Configuration Files	88
Configuration File Types and Location	89
Displaying Configuration Files	89
Removing Configuration Files	89
Reloading the System	89
Working with Software Images	89
Downloading an Image File	89
USB Support	91
Configuring U-boot	91

CHAPTER 13**FND Configuration for IXM 93**

Preparing FND for IXM ZTD	93
IXM modem Firmware Update	103
Configuring IGMA	105
Troubleshooting	106

Preface

This document describes how to configure the Cisco LoRaWAN Gateway in your network.

This guide does not describe how to install the Cisco LoRaWAN Gateway. For information about how to install the Cisco LoRaWAN Gateway, see the hardware installation guide pertaining to your device.



Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{x y z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.



Danger **IMPORTANT SAFETY INSTRUCTIONS** Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. **SAVE THESE INSTRUCTIONS**

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Related Publications

- [Cisco LoRaWAN Interface Module Hardware Installation Guide](#)
- [Release Notes for the Cisco LoRaWAN Gateway](#)
- [Getting Started and Product Document of Compliance for the Cisco LoRaWAN Interface Module](#)
- [Cisco IR800 Integrated Services Router Software Configuration Guide](#)

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#) .

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#) . The RSS feeds are a free service.



CHAPTER 1

Overview

The Cisco LoRaWAN Gateway is a module from Cisco Internet of Things (IoT) extension module series. It can be connected to the Cisco 809 and 829 Industrial Integrated Services Routers (IR800 series) or be deployed as standalone for low-power wide-area (LPWA) access and is positioned as a carrier-grade gateway for indoor and outdoor deployment, including harsh environments. It adds a ruggedized remote LoRaWAN radio modem interface to create a gateway between the Cisco Field Network Director and a partner's LoRa network server.

- [Overview, on page 1](#)
- [Switching to Virtual Mode, on page 2](#)
- [GPS Channel Plans, on page 2](#)
- [Displaying System Information, on page 5](#)

Overview

The following models are covered by this document:

- IXM-LPWA-800-16-K9
- IXM-LPWA-900-16-K9

There are two LoRaWAN gateway modes as below:

- Virtual interface mode – IR800 series including the LoRaWAN module as a virtual interface
- Standalone mode – The LoRaWAN module working alone as an Ethernet backhaul gateway or attached to a cellular router through Ethernet

You can configure the LoRaWAN IXM running on virtual interface mode or standalone mode through CLI or Cisco IoT Field Network Director (IoT FND).

This guide will provide the configuration steps for standalone mode and guide you to swap between these two modes.

For detailed information of configuring virtual interface mode, see the “Configuring Virtual-LPWA” chapter of the Cisco IR800 Integrated Services Router Software Configuration Guide at:

<http://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/configuration/guide/IR800config/VLPWA.html>

For the information of software installation procedure, see the release notes of Cisco LoRaWAN Gateway at:

<http://www.cisco.com/c/en/us/support/routers/interface-module-lorawan/products-release-notes-list.html>

For more information of IoT-FND, see <https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/tsd-products-support-series-home.html>.

Switching to Virtual Mode

You can use the **switchover** EXEC command to switch to the virtual mode.



Note Once the IXM is switched over to virtual mode, you need to have an IR829/IR809 to bring it back to standalone mode.

Use this command, if you are fully aware of your environment and confident of switching over and managing it via IR8x9.

```
Gateway#switchover
```

GPS Channel Plans

GPS check for verification of channel plans is included.



Note This table is derived from the LoRaWAN Regional Parameters document, version RP2-1.0.2.



Note The CPF feature is intended to operate only when a GPS fix is actively available or has been stored from an earlier fix. The location derived from the GPS fix must be in one of the countries listed in the table below. If not, the radio will not turn on. This does not apply to Actility LRR since the channel plan is configured on the network server.

Countries supported by this GPS check include:

Code	Name	Channel plan
AL	Albania	EU868
AD	Andorra	EU868
AM	Armenia	EU868
AR	Argentina	AU915-928
AT	Austria	EU868
AU	Australia	AU915 (default) AS923
AZ	Azerbaijan	EU868
BY	Belarus	EU868

Code	Name	Channel plan
BE	Belgium	EU868
BA	Bosnia	EU868
BN	Brunei	EU868
BG	Bulgaria	EU868
KH	Cambodia	EU868
CA	Canada	US915 (default) AU915
CN	China	AS923
HR	Croatia	EU868
CY	Cyprus	EU868
CZ	Czech Republic	EU868
DK	Denmark	EU868
EE	Estonia	EU868
FI	Finland	EU868
FR	France	EU868
DE	Germany	EU868
GR	Greece	EU868
HK	Hongkong	EU868
HU	Hungary	EU868
IS	Iceland	EU868
IE	Ireland	EU868
IN	India	IN865
IT	Italy	EU868
JP	Japan	AS923
LA	Laos	EU868
LV	Latvia	EU868
LI	Liechtenstein	EU868
LT	Lithuania	EU868
LU	Luxembourg	EU868

Code	Name	Channel plan
MK	Macedonia	EU868
MY	Malaysia	EU868
MX	Mexico	US915
MD	Moldova	EU868
ME	Montenegro	EU868
NL	Netherlands	EU868
NZ	New Zealand	AS923 AU915
NO	Norway	EU868
PL	Poland	EU868
PT	Portugal	EU868
PR	Puerto Rico	US915
RO	Romania	EU868
RS	Serbia	EU868
SG	Singapore	EU868
SK	Slovakia	EU868
SI	Slovenia	EU868
ZA	South Africa	EU868
ES	Spain	EU868
SE	Sweden	EU868
CH	Switzerland	EU868
TH	Thailand	EU868
TR	Turkey	EU868
GB	United Kingdom	EU868
UA	Ukraine	EU868
US	United States	US915 (default) AU915
VA	Vatican City	EU868
VN	Vietnam	EU868



Note Refer to the [LoRa Alliance Technical Specifications](#) for more information.

Displaying System Information

Use the show commands to display system information.

Displaying Version Information

Use the **show version** command to display system version information.

```
Gateway#show version
Corsica Software, Version 2.0.10.K5, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012-2014, 2017 by Cisco Systems, Inc.
Compiled 12-Jun-2017.19:06:44UTC-04:00 by Corsica Team

ROM: Bootstrap program is Corsica boot loader
Firmware Version : 2.0.10.K5, RELEASE SOFTWARE
Bootloader Version: 20160830_cisco

Hostname:ipsecrsa uptime is 15 hours, 44 minutes
Using secondary system image

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco model: IXM-LPWA-800-16-K9
Processor : ARMv7 Processor rev 1 (v7l) with 1026764K bytes of memory.
Last reset from power-on

Base ethernet MAC Address : 00:50:43:14:32:45
Model revision number: : B0
System serial number: : FOC20394ANP
```

Displaying Platform Status

Use the **show platform status** command to display the platform status:

```
Gateway#show platform status
Load Average : 1min:0.23 5min:0.22 15min:0.23
Memory Usage : 0.38
```

```
Flash Usage : sys:0.06 app:0.06
CPU Temperature : 39.0 C
Board Temperature: 39.5 C
Door Status : DoorClose
```

Displaying AES Key

The LoRaWAN Chip ID is used to obtain the AES key. On the Thingpark Network Server, the AES key is stored in the **custom.ini** file. The AES key can be displayed from CLI.



Note On other 3rd party network servers, the AES key may be stored in a different location.

Obtaining the AES key requires LoRaWAN geolocation. The AES key is used to decrypt the fine - timestamps required for LoRa Geo-location calculation. The AES keys are licensed via a partner.



Note The false AES key will report incorrect geo-localization information.

Use the **show aes key** command to display AES key.

- The following example shows an existing AES key:

```
Gateway#show aes key
AES KEY: 595EB592055421C06895E4D4CE0FE63D
```

- The following example shows an unknown key:

```
Gateway#show aes key
AES KEY: Unknown
```

Displaying GPS Information

The GPS antenna must be properly installed on the LoRaWAN interface for both LoRaWAN Class B endpoints and geolocation support.

GPS information can be displayed from Cisco IOS or from the LoRaWAN interface Linux shell.

- When there is no GPS antenna attached, the **show gps log** command will have an output like the following example:

```
Gateway#show gps log
Unknown
```

- When there is a GPS antenna attached, the **show gps log** command and the **show gps status** command will have an output like the following example:

```
Gateway#show gps log
$GNRMC,231503.00,A,3725.12517,N,12155.20795,W,0.353,241.48,040517,,A*65
$GNVTG,241.48,T,M,0.353,N,0.653,K,A*2D
```



```
$GNGGA,231503.00,3725.12517,N,12155.20795,W,1,04,5.85,72.2,M,-29.8,M,,*4B
$GNGSA,A,3,24,15,12,13,,,,,,,,,9.40,5.85,7.35*1B
$GNGSA,A,3,,,,,,,,,9.40,5.85,7.35*18
$GPGSV,3,1,10,02,22,184,,06,49,142,,12,24,297,27,13,16,212,26*75
$GPGSV,3,2,10,15,17,248,31,17,51,041,,19,74,024,16,24,44,305,35*7C
$GPGSV,3,3,10,28,25,087,,30,05,146,*7F
$GGLSV,1,1,00*65
$GNGLL,3725.12517,N,12155.20795,W,231503.00,A,A*6B
$GNZDA,231503.00,04,05,2017,00,00*7B
```

```
Gateway#show gps status
INFO: SPI speed set to 2000000 Hz
reading GPS data...
total data length: 0
reading GPS data...
total data length: 246
$GNRMC,,V,,,,,,,,,N*4D
$GNVTG,
##PASS: GPS I2C interface check OK
```

- To display the GPS history information, use the following command:

```
Gateway#show gps history
Info: 23:31:50 3725.13869N 12155.17038W
GPS Satellites in View: 12
GPS Satellites in Use: 10
```

Displaying FPGA Information

Use the **show fpga** command to display the FPGA information, and the **show fpga version** command to display the FPGA version.



Note FPGA version may require specific LoRaWAN forwarder version from the LoRaWAN Network Server partner.

```
#show fpga
INFO: SPI speed set to 2000000 Hz
checking FPGA version...
FPGA version: 48
HAL version: 3.5.0
SX1301 #0 version: 103
SX1301 #0 chip ID: 1
SX1301 #1 version: 103
SX1301 #1 chip ID: 1
##PASS: FPGA version check OK

#show fpga version
FGPA version: 58
```

Displaying Inventory Information

The show inventory command displays the general Cisco LoRaWAN Gateway information.



Note After a firmware upgrade, the FPGAStatus may show it is under upgrade. Wait for "Ready" status before performing any other operation.

```
Gateway#show inventory
Name       : Gateway
ImageVer   : 20170427144502_DEV
BootloaderVer : 20160830_cisco_DEV
SerialNumber : FOC20133FNF
PID        : IXM-LORA-900-H-V2
UTCTime    : 02:40:53.464 UTC Sat Aug 12 2023
IPv4Address : 192.168.3.5
IPv6Address : None
FPGAVersion : 58
FPGAStatus  : Ready
ChipID     : LSB = 0x2866ff0b MSB = 0x00f14184
TimeZone   : UTC
LocalTime  : Sat Aug 12 02:40:53 UTC 2023
ACT2 Authentication: PASS
```

Displaying Radio Information

The **show radio** command displays the radio information.

```
Gateway#show radio
LORA_SN: FOC20195V3C
LORA_PN: 95.1602T00
LORA_SKU: 868
LORA_CALC:
<115,106,100,95,89,86,83,80,72,63,55,46,38,33,29,25-126,114,106,97,89,85,81,77,69,60,52,43,35,30,26,22>
CAL_TEMP_CELSIUS: 29
CAL_TEMP_CODE_AD9361: 91
RSSI_OFFSET: -203.46,-203.75
LORA_REVISION_NUM:
RSSI_OFFSET_AUS:

radio status:
off
```



Note The radio status is off by default. Please turn on radio before working with the packet forwarder. Use the following commands to turn on radio:

```
Gateway#configure terminal
Gateway(config)#no radio off
```



Note The LORA_CALC value is the Calibration table from manufacturing, which cannot be changed, but can be used for hardware troubleshooting.

Displaying Certificate Information

The `show sudi certificate` command displays the certificate information.

```
Gateway#show sudi certificate
Calculating... please wait for seconds...
Certificate:
  X509v3 Key Usage: critical
  Issuer: O=Cisco, CN=ACT2 SUDI CA
  Subject: serialNumber=PID:IXM-LPWA-900-16-K9 SN:FOC21182U6D, O=Cisco, OU=ACT-2 Lite SUDI,
  CN=IXM-LPWA-900-16-K9
  Signature Algorithm: sha256WithRSAEncryption, Digital Signature, Non Repudiation, Key
  Encipherment
  Validity
    Not Before: May 16 19:21:43 2017 GMT
    Not After : May 16 19:21:43 2027 GMT
```




CHAPTER 2

Assigning IP Address and Domain Name Server

This chapter describes how to create the initial configuration (for example, assigning the IP address and default gateway information) for the Cisco LoRaWAN Gateway by using a variety of automatic and manual methods.



Note Information in this chapter about configuring IP addresses and DHCP is specific to IP Version 4 (IPv4).

- [Assigning IP Address, on page 11](#)
- [Configuring DNS, on page 13](#)
- [Mapping Hostnames to IP Addresses, on page 14](#)

Assigning IP Address

You can assign IP address through a DHCP server or manually.

Use a DHCP server for centralized control and automatic assignment of IP information after the server is configured.

Configuring DHCP

Understanding DHCP

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and a mechanism for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices.

DHCP client support is enabled on the Fast Ethernet 0/1 or VLAN interface on the LoRaWAN Gateway for automatic IPv4 address assignment.

The DHCP server, which supplies the IP addresses to the LoRaWAN Gateway interfaces, does not need to be on the same subnet as the LoRaWAN Gateway. However, when the DHCP server and the LoRaWAN Gateway are on different subnets, DHCP relay must be active in the network. Generally, DHCP relay is configured on a LoRaWAN Gateway in the path between the LoRaWAN Gateway and the DHCP server. The DNS address and default gateway can also be assigned via DHCP.

Enabling DHCP on Interfaces

To assign IP address by negotiation via DHCP, use the **ip address dhcp** privileged EXEC command.

Beginning in privileged EXEC mode, follow these steps to enable DHCP on interfaces:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface_type interface_number</i>	Enter interface configuration mode.
Step 3	ip address dhcp	Enable DHCP client on the interface to allow automatic assignment of IP addresses to the specified interface.
Step 4	description [<i>interface_description</i>]	Enter description for the interface.
Step 5	exit	Return to global configuration mode.
Step 6	ip default-gateway <i>ip-address</i>	Configure default gateway. Note The default gateway may be learned from DHCP.
Step 7	Use the following commands to verify the configuration: <ul style="list-style-type: none"> • show interfaces <i>interface_type interface_number</i> • show ip interfaces <i>interface_type interface_number</i> • show ip route 	Verify the configuration.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Manually Assigning IP Information

Beginning in privileged EXEC mode, follow these steps to manually assign IP information to multiple interfaces:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface_type interface_number</i>	Enter interface configuration mode.
Step 3	ip address <i>ip-address subnet-mask</i>	Enter the IP address and subnet mask.

	Command or Action	Purpose
Step 4	description [<i>interface_description</i>]	Enter description for the interface.
Step 5	exit	Return to global configuration mode.
Step 6	ip default-gateway <i>ip-address</i>	Configure default gateway.
Step 7	Use the following commands to verify the configuration: <ul style="list-style-type: none"> • show interfaces <i>interface_type</i> <i>interface_number</i> • show ip interfaces <i>interface_type</i> <i>interface_number</i> • show ip route 	Verify the configuration.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

What to do next

To remove the IP address, use the **no ip address** interface configuration command. If you are removing the address through SSH, your connection to the LoRaWAN Gateway will be lost.

Configuring DNS

DNS Client

When your network devices require connectivity with devices in networks for which you do not control the name assignment, you can assign device names that uniquely identify your devices within the entire internetwork using the domain name server (DNS). DNS uses a hierarchical scheme for establishing host names for network nodes, which allows local control of the segments of the network through a client-server scheme. The DNS system can locate a network device by translating the hostname of the device into its associated IP address.

On the Internet, a domain is a portion of the naming hierarchy tree that refers to general groupings of networks based on the organization type or geography. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco is a commercial organization that the Internet identifies by a .com domain, so its domain name is cisco.com. A specific hostname in this domain, the File Transfer Protocol (FTP) system, for example, is identified as ftp.cisco.com.

Name Servers

Name servers keep track of domain names and know the parts of the domain tree for which they have complete information. A name server might also store information about other parts of the domain tree. To map domain names to IP addresses on the LoRaWAN Gateway, you must identify the hostnames, specify a name server, and enable the DNS service.

You can configure the LoRaWAN Gateway to use one or more domain name servers to find an IP address for a host name.

DNS Operation

A name server handles client-issued queries to the DNS server for locally defined hosts within a particular zone as follows:

An authoritative name server responds to DNS user queries for a domain name that is under its zone of authority by using the permanent and cached entries in its own host table. When the query is for a domain name that is under its zone of authority but for which it does not have any configuration information, the authoritative name server replies that no such information exists.

A name server that is not configured as the authoritative name server responds to DNS user queries by using information that it has cached from previously received query responses.

Configuring DNS Server

To configure the DNS server, use the **ip name-server** privileged EXEC command

Beginning in privileged EXEC mode, follow these steps to configure DNS:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip name-server <i>ip-address</i>	Configure DNS server.
Step 3	exit	Return to global configuration mode.
Step 4	show hosts	Verify the configuration.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Mapping Hostnames to IP Addresses

This section provides configuration of hostname to IP address mapping, so that host can be reached by name without DNS.

Beginning in privileged EXEC mode, follow these steps to map hostnames to IP addresses:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip host <i>hostname ip-address</i>	Define a static hostname-to-address mapping. You can define up to 5 mapping entries. Use the no form of the command to delete the mapping entry.

	Command or Action	Purpose
		Note You can also use this command to set the LXC /etc/hosts entries from the CLI.
Step 3	exit	Return to global configuration mode.
Step 4	show ip host	Verify the configuration.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Example

```
Gateway#config terminal
Gateway(config)#ip host thinkpark.com 122.23.12.1
```

```
Gateway#show ip host
IP                               Hostname
--                               -
11.11.11.1                       apple.com
11.11.11.2                       apple2.com
11.11.11.3                       apple3.com
11.11.11.4                       apple4.com
```




CHAPTER 3

Administering the Cisco LoRaWAN Gateway

This chapter describes how to perform one-time operations to administer the Cisco LoRaWAN Gateway.

- [Managing the System Time and Date, on page 17](#)
- [Configuring a System Name and Prompt, on page 18](#)
- [Configuring GPS as the Clock Source, on page 19](#)
- [Configuring UBX Support for GPS, on page 19](#)
- [Checking and Saving the Running Configuration, on page 20](#)
- [Reloading IXM, on page 20](#)
- [Using Reset Button, on page 20](#)

Managing the System Time and Date

You can manage the system time and date on your LoRaWAN Gateway, either by using automatic configuration, such as the Network Time Protocol (NTP), or by using the GPS as a source for the clock.

Network Time Protocol (NTP)

Network Time Protocol (NTP) is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305 and RFC 5905.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

NTP Version 4

NTP version 4 is implemented on the modem. NTPv4 is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides these capabilities:

- Support for IPv6. (Note that IXM supports only IPv4.)
- Improved security compared to NTPv3. The NTPv4 protocol provides a security framework based on public key cryptography and standard X509 certificates.
- Automatic calculation of the time-distribution hierarchy for a network. Using specific multicast groups, NTPv4 automatically configures the hierarchy of the servers to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

Configuring NTP Server

Beginning in privileged EXEC mode, follow these steps to configure the NTP server:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ntp server {ip name address address }	Defines the NTP server that provides the clocking source for the modem.
Step 3	exit	Return to privileged EXEC mode.
Step 4	show ntp status	(Optional) Show NTP status to verify the configuration.
Step 5	show ntp associations	(Optional) Show the NTP associations with upstream servers.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

What to do next

To disable the NTP service, use the **no ntp server hostname** global configuration command.

Configuring a System Name and Prompt

You configure the system name on the LoRaWAN Gateway to identify it. By default, the system name and prompt are *Router* .

Beginning in privileged EXEC mode, follow these steps to manually configure a system name:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.

	Command or Action	Purpose
Step 2	<code>hostname name</code>	Manually configure a system name. The default setting is <i>Router</i> . The name must follow the rules for ARPANET hostnames. They must start with a letter, exit with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.
Step 3	<code>exit</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	Verify your entries.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

What to do next

When you set the system name, it is also used as the system prompt.

To return to the default hostname, use the **no hostname** global configuration command.

Configuring GPS as the Clock Source

Beginning in privileged EXEC mode, follow these steps to configure GPS as the gateway clock source:

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>clock gpstime enable</code>	Use the GPS as the modem clock source.
Step 3	<code>exit</code>	Return to privileged EXEC mode.

Configuring UBX Support for GPS

The UBX protocol is the communication convention used by certain GPS receiver chips. The UBX format is binary as opposed to text-based. UBX Protocol messages operate over an asynchronous serial connection following the RS-232 standard. Messages are classified into different categories such as Configuration, Timing, Informative, Monitor, and Navigation. Messages sent to the chip are either commands or enquiries.

Beginning in privileged EXEC mode, follow these steps to configure the UBX support for GPS.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>gps ubx enable</code>	Enable the UBX protocol to UART output. To disable the UBX support, use the no form of the command.
Step 3	<code>exit</code>	Return to privileged EXEC mode.
Step 4	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Checking and Saving the Running Configuration

You can check the configuration settings that you entered or changes that you made by entering this privileged EXEC command:

```
Router# show running-config
```

To store the configuration or changes you have made to your startup configuration in flash memory, enter this privileged EXEC command:

```
Router# copy running-config startup-config
```

This command saves the configuration settings that you made. If you fail to do this, your configuration will be lost the next time you reload the system. To display information stored in the NVRAM section of flash memory, use the **show startup-config** privileged EXEC command.

Reloading IXM

The **reload** command halts the system. If the system is not set to manually boot up, it reboots itself. Use the **reload** command after you save the LoRaWAN Gateway configuration information to the startup configuration (**copy running-config startup-config**).

Using Reset Button

A Cisco Wireless Gateway for LoRaWAN that has already been configured can be reset to the manufacturing configuration by pressing the **Reset** button located at the side of the Console port on the device.

If you press the **Reset** button and release it in less than 5 seconds, the system will reboot immediately with the last saved configuration.

If you press the **Reset** button and release it after more than 5 seconds, the system will reboot immediately and restore to the factory default.



CHAPTER 4

Configuring VLAN

This chapter describes how to configure VLAN on the Cisco LoRaWAN Gateway. The LoRaWAN Gateway supports IEEE 802.1Q encapsulation. You can configure the fastethernet port as a trunk port that enables tagging of outgoing traffic from the Cisco LoRaWAN Gateway.

- [Configuring IP Address for VLAN, on page 21](#)
- [Configuring VLAN Trunks, on page 22](#)
- [Enabling Sending and Receiving Tagged Packet on Ethernet Port, on page 23](#)
- [Examples of Show Commands, on page 24](#)

Configuring IP Address for VLAN

Beginning in privileged EXEC mode, follow these steps to configure IP address for the VLAN:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface vlan <i>vlan-id</i>	Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. The VLAN range is 1 to 4094.
Step 3	ip address {<i>ip-address subnet-mask</i> dhcp}	Configure the IP address.
Step 4	exit	Return to global configuration mode.
Step 5	show interfaces vlan <i>vlan-id</i>	Verify the configured IP address.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring VLAN Trunks

A trunk is a point-to-point link between one or more Ethernet interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

You can configure the FastEthernet port as a trunk port that enables tagging of outgoing traffic from the Cisco LoRaWAN Gateway.

Configuring a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure a trunk port:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the port to be configured for trunking, and enter interface configuration mode.
Step 3	switchport mode trunk	Set the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.
Step 4	exit	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

What to do next

To reset all trunking characteristics of a trunking interface to the defaults, use the **no switchport trunk** interface configuration command.

Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk.

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of a trunk:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.

	Command or Action	Purpose
Step 2	<code>interface interface-id</code>	Specify the port to be configured, and enter interface configuration mode.
Step 3	<code>switchport mode trunk</code>	Configure the interface as a VLAN trunk port.
Step 4	<code>switchport trunk allowed vlan vlan-id</code>	(Optional) Configure the VLAN allowed on the trunk.
Step 5	<code>exit</code>	Return to privileged EXEC mode.
Step 6	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

What to do next

To return to the default allowed VLAN list of all VLANs, use the **no switchport trunk allowed vlan** interface configuration command.

Enabling Sending and Receiving Tagged Packet on Ethernet Port

To enable sending and receiving of tagged packets on the Ethernet port, the following needs to be configured on the Cisco LoRaWAN Gateway:

```
interface FastEthernet 0/1
switchport mode trunk
switchport trunk allowed vlan <vlan id 1-4094>
exit
!
interface Vlan <vlan-id>
ip address <dhcp | ip mask>
```



Note Only a single vlan tag is allowed on the trunk port. All traffic destined for network specified by interface vlan IP address will go out of the Ethernet port with that vlan tag.

The port will also expect incoming packets (with its own ip address or broadcast address) to be tagged with the same vlan tag. In order for the peer switch or router to send tagged packets to the Cisco LoRaWAN Gateway, they need to be configured as trunk ports as well.

Here is a configuration example on a Cisco ME3400 switch:

```
interface FastEthernet0/23
switchport trunk allowed vlan 220
switchport mode trunk
```



Note The uplink to the rest of the network from this switch also needs to include this vlan.

On a Catalyst 3750 it would be:

```
interface GigabitEthernet 1/0/1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan <vlan_id>
  switchport mode trunk
```

If you need to use Vlan 1, remember that Cisco switches treat Vlan 1 as the native vlan on trunk ports by default. That is, incoming “untagged” packets will be treated as they belong to Vlan 1. And similarly when Vlan 1 packets untagged are sent. These packets will not be picked up on the Cisco LoRaWAN Gateway Vlan interface. To avoid this, a different native vlan must be chosen on the peer switch. See the following example:

```
interface GigabitEthernet 1/0/1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan <vlan id other than 1>
  switchport trunk allowed vlan 1
  switchport mode trunk
```

Examples of Show Commands

```
Router# show vlan
VLAN Name                Status      Ports
-----
220 VLAN0220              Active     Fa0/1
```

```
Router# show interfaces
Vlan220 is up
  address is 00:50:43:24:1F:4A
  MTU is 1500 bytes
FastEthernet0/1 is up
  Hardware is Fast Ethernet, address is 00:5F:86:5C:27:78
  MTU is 1500 bytes
```

```
Router# show interfaces Vlan 220
Vlan220 is up
  address is 00:50:43:24:1F:4A
  MTU is 1500 bytes
```

```
Router# show ip interface
FastEthernet FastEthernet IEEE 802.3
Vlan          Vlan IEEE 802.1q
```

```
Router# show ip interface Vlan 220
Vlan220 is up
  Internet address is 172.27.165.208
  Netmask is 255.255.255.128
  Broadcast address is 172.27.165.255
  MTU is 1500 bytes
```



CHAPTER 5

Configuring CDP

This chapter describes how to configure Cisco Discovery Protocol (CDP) on the Cisco LoRaWAN Gateway.

- [Understanding CDP, on page 25](#)
- [Configuring CDP, on page 25](#)

Understanding CDP

CDP is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP). Because CDP runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each CDP-configured device sends periodic messages to a multicast address, advertising at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime information, which is the length of time a receiving device holds CDP information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

Configuring CDP

These sections include CDP configuration information and procedures.

Enabling and Disabling CDP

Beginning in privileged EXEC mode, follow these steps to enable or disable the CDP device discovery capability:

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.

	Command or Action	Purpose
Step 2	(no) cdp run	Enable or disable CDP.
Step 3	exit	Return to privileged EXEC mode.

Configuring the CDP Characteristics

Beginning in privileged EXEC mode, follow these steps to configure the CDP timer and holdtime.

You can configure the frequency of CDP updates, and the amount of time to hold the information before discarding it.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	cdp timer <i>seconds</i>	(Optional) Set the transmission frequency of CDP updates in seconds. The range is 5 to 254; the default is 60 seconds.
Step 3	cdp holdtime <i>seconds</i>	(Optional) Specify the amount of time a receiving device should hold the information sent by your device before discarding it. The range is 10 to 255 seconds; the default is 180 seconds.
Step 4	exit	Return to privileged EXEC mode.
Step 5	show cdp	Verify configuration by displaying global information about CDP on the device.
Step 6	show cdp neighbors	Display information about neighbors.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

What to do next

Use the **no** form of the CDP commands to return to the default settings.



CHAPTER 6

Configuring Authentication

This chapter describes how to configure authentication on the Cisco LoRaWAN Gateway.

- [Preventing Unauthorized Access, on page 27](#)
- [Protecting Access to Privileged EXEC Commands, on page 27](#)
- [Configuring Secure Shell, on page 29](#)
- [SSH Access Over IPsec Tunnel , on page 32](#)
- [Configuring Reverse SSH and Connecting to Container, on page 32](#)
- [Changing Private Network Between Host and Container, on page 33](#)
- [User Accounts, on page 34](#)
- [Configuring Logging in Container, on page 35](#)

Preventing Unauthorized Access

You can prevent unauthorized users from reconfiguring your LoRaWAN Gateway and viewing configuration information. Typically, you want network administrators to have access to your device while you restrict access to users who dial from outside the network through an asynchronous port, connect from outside the network through a serial port, or connect through a terminal or workstation from within the local network.

To prevent unauthorized access into your LoRaWAN Gateway, you should configure username and password pairs, which are locally stored on the device. These pairs are assigned to lines or ports and authenticate each user before that user can access the LoRaWAN Gateway. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Protecting Access to Privileged EXEC Commands

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device.

Configuring Enable Secret Passwords with Encryption

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use the **enable secret** global configuration commands.

The command allows you to establish an encrypted password that users must enter to access privileged EXEC mode (the default).

Beginning in privileged EXEC mode, follow these steps to configure encryption for enable secret passwords:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	enable secret <i>{password 5 encrypted_passwd 8 encrypted_passwd}</i>	Define a secret password for access to privileged EXEC mode. Specify 5 to indicate md5 encryption. Specify 8 to indicate SHA512 password. Note Special characters cannot be used for the plain password. Note While upgrading to Release 2.0.20, admin has to reconfigure the passwords for SHA512 to be effective and downgrade is not supported.
Step 3	exit	Return to privileged EXEC mode.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

What to do next

To remove a password, use the **no enable secret** global configuration command.

Configuring Username and Password for Local Authentication

You can configure username and password pairs, which are locally stored on the LoRaWAN Gateway. These pairs are assigned to lines or ports and authenticate each user before that user can access the LoRaWAN Gateway.

Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	username <i>name {password 5 encrypted_passwd 8 encrypted_passwd}</i>	Enter the username and password for each user. Specify 5 to indicate md5 encryption. Specify 8 to indicate SHA512 password.

	Command or Action	Purpose
		<p>Note Special characters cannot be used for the plain password.</p> <p>Note While upgrading to Release 2.0.20, admin has to reconfigure the passwords for SHA512 to be effective and downgrade is not supported.</p>
Step 3	exit	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

What to do next

To disable username authentication for a specific user, use the **no username name** global configuration command.



Note For enable secret, username, and system admin, use the following characters for the password:

- Lowercase alphabet: [a-z]
- Uppercase alphabet: [A-Z]
- Numbers: [0-9]
- Special Character: [\$%{}+_:]

Configuring Secure Shell

This section describes how to configure the Secure Shell (SSH) feature.

SSH is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 2 (SSHv2).

Beginning in privileged EXEC mode, follow these steps to configure SSH on the LoRaWAN Gateway.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.

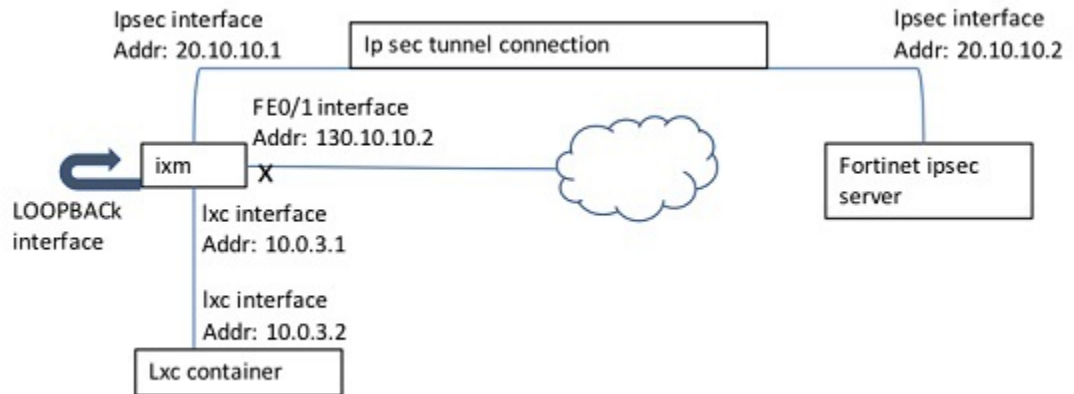
	Command or Action	Purpose
Step 2	hostname <i>hostname</i>	Configure a hostname for your LoRaWAN Gateway.
Step 3	ip domain name <i>domain_name</i>	Configure a host domain for your LoRaWAN Gateway.
Step 4	ip ssh { port session authentication-retries time-out admin-access local limit-local }	Configure the SSH control parameters: <ul style="list-style-type: none"> • port – Configure SSH port. • session – Configure number of SSH session. • authentication-retries – Configure number of authentication retries. • time-out – Configure timeout interval. • admin-access – Allow admin access via SSH. • local – Restrict user to container and reverse-tunnel SSH access only. • limit-local – Permit SSH on local only. Limit the listening address to local address only (for example, 127.0.0.1 or 10.0.3.1). Not listen on LAN interface.
Step 5	crypto key generate rsa	Enable the SSH server for local and remote authentication on the LoRaWAN Gateway and generate an RSA key pair. Generating an RSA key pair automatically enables SSH.
Step 6	exit	Return to privileged EXEC mode.
Step 7	Do one of the following: <ul style="list-style-type: none"> • show ip ssh • show ssh 	Show and configuration information for your SSH server. Show the status of the SSH server on the LoRaWAN Gateway.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

What to do next

To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration command. After the RSA key pair is deleted, the SSH server is automatically disabled.

Configuring IP SSH Limit Local

The following figure shows an example of the **IP SSH limit local** command behavior.



When **IP SSH limit local disabled** is configured, the SSH connections to all innterfaces are allowed. When **IP SSH limit local enabled** is configured, the SSH connection to FE0/1 (130.10.10.2) is not allowed.



Note When **IP SSH limit local** is enabled on the IXM, the SSH access from outside is disabled for the unit. The **uboot console disable** option only checks whether SSH is enabled or not, and does not factor the **IP SSH limit local** option. If both commands are configured, it is possible that both the console conntecvity and SSH connectivity are lost. In that case, the only way to access the unit is through container via Thing park.

Displaying the SSH Configuration and Status

To display the SSH server configuration and status, use one or more of the privileged EXEC commands in [Table 1: Commands for Displaying the SSH Server Configuration and Status](#), on page 31:

Table 1: Commands for Displaying the SSH Server Configuration and Status

Command	Purpose
show ip ssh	Shows the version and configuration information for the SSH server.
show ssh	Shows the status of the SSH server.

Using SCP to Upload Files

To copy a local file to a remote location, use the following **scp** EXEC command:

scp local *src_filename username host dst_filename*

To copy a remote file to local flash, use the following **scp** EXEC command:

scp remote *username host src_filename dst_filename*

SSH Access Over IPSec Tunnel

From the primary server and secondary server, you can SSH to IXM over the tunnel.

Example from IR800:

```
IR800# ssh -v 2 -l via 172.27.170.71
```

Configuring Reverse SSH and Connecting to Container

To open a shell to the container for user, use the **request shell container-console** EXEC command. Password is needed when you request shell container. If you have changed the system admin password, you need to use the new password.



Note Admin can change the password by using the **sysadmin security password** command.

Configuring Reverse SSH

Beginning in privileged EXEC mode, follow these steps to create a reverse SSH tunnel.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	secure-tunnel create <i><port-no></i> <i><user-id></i> <i><remote-host></i>	Create a reverse SSH tunnel.
Step 3	exit	Return to privileged EXEC mode.
Step 4	show secure-tunnel	Show the secure tunnel status.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Example

```
configure terminal
  secure tunnel create 30000 vnallamo 10.28.29.226
```

From the 10.28.29.226 server, execute the following command to reverse SSH:

```
ssh -l vik localhost -p 30000
```



Note When IPsec is enabled, secure tunnel may not be working due to gateway reachability. This is a known issue.

Copying Files From the Container

Beginning in privileged EXEC mode, follow these steps to copy files from the container to the host.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>container copy <filename> <path></code>	Copy files from the container to the host.
Step 3	<code>exit</code>	Return to privileged EXEC mode.
Step 4	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Changing Private Network Between Host and Container

Beginning in privileged EXEC mode, follow these steps to change the private network between the host and the container.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>container private-network <chosen-private-network-option-from-the-list></code>	Change the private network between the host and the container. You can choose one of the following options: 10.0.0.0/28, 172.16.0.0/28, or 192.168.0.0/28. By default, the private network is 10.0.3.0/24, which is configured on startup. To restore the default, use the no form of the command.
Step 3	<code>exit</code>	Return to privileged EXEC mode.
Step 4	<code>show container private-network</code>	Verify the configuration.

	Command or Action	Purpose
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Example

```
Gateway#show container private-network
Container private network: 172.16.0.0/2
```

User Accounts

This section describes the user accounts and their usages.

Use the **request shell host** command to enter the Linux shell and use the **request shell exit** command to exit.

Table 2: User Accounts

userID	SSH connection	Shell	Linux shell access through request shell host	Notes
system	no (default)	/bin/sh	yes	<ul style="list-style-type: none"> Use the ip ssh admin-access CONF command to allow SSH access. Use the sysadmin security password EXEC command to change system password.
user1	yes	clish	no	-
user2	yes	clish	no	-

Table 3: Linux Shell Access

Request Shell	Exit	Host
SSH	Exit from host	Go into console
console	Go into console	Go into console



Note It is recommended to change the Linux shell password using this command "sysadmin security password".

Table 4: Password Change on Switchover

Switchover Type	Description
From virtual mode to standalone mode	The virtual mode root password is assigned to the standalone mode system password.
From standalone mode to virtual mode	The standalone mode system password is lost during the switchover, and the virtual mode root password remains.

Configuring Logging in Container

Beginning in privileged EXEC mode, follow these steps to configure logging in the container.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>container log all</code>	Enable logging through syslog-ng in the container. To restore the default, use the no form of the command.
Step 3	<code>exit</code>	Return to privileged EXEC mode.

After the `is` command is enabled, you can view the logs by logging into the container. The logs are located in `/var/run`.

Example

```
Gateway(config)#container log all
Container syslog has started.
```




CHAPTER 7

Configuring IPsec

This chapter provides information about IPsec configuration on the Cisco LoRaWAN Gateway.

- [Understanding IPsec, on page 37](#)
- [Configuring IPsec, on page 37](#)
- [Configuring Crypto IPsec Profile Common, on page 39](#)
- [Configuring Crypto IPsec Profile Individual , on page 41](#)
- [Basic Configuration for RSA to Connect to Primary and Secondary, on page 42](#)
- [Locking Traffic to IPsec Tunnels, on page 43](#)
- [Erasing IPsec Certificates and Key, on page 43](#)
- [Uploading Certificates from USB or Local Flash, on page 43](#)
- [Disabling LXC Restart During IPsec Reauthentication, on page 43](#)
- [Resetting Secure-Storage for Certificate Download, on page 43](#)

Understanding IPsec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (site-to-site), or between a security gateway and a host (remote-access).

IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at Application layer. Hence, only IPsec protects any application traffics over an IP network. Applications can be automatically secured by its IPsec at the IP layer. Without IPsec, the protocols of TLS/SSL must be inserted under each of applications for protection.

Configuring IPsec

Beginning in privileged EXEC mode, follow these steps to configure IPsec on the Cisco LoRaWAN Gateway:

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>crypto ipsec profile</code> { <code>common</code> <code>primary</code> <code>secondary</code> }	Configure parameters used by tunnel. Note The primary profile MUST be configured. Common and secondary are optional. For more information, see Configuring Crypto IPsec Profile Common , on page 39 and Configuring Crypto IPsec Profile Individual , on page 41.
Step 3	Do one of the following: <ul style="list-style-type: none"> • <code>ipsec isakmp username password group group_id psk</code> • <code>ipsec cert install {usb local} enable</code> • <code>ipsec cert scep <url> <country_code> <state> <locality> <organization> <unit> <name> <device-id> {ndes xpki} <persistence> <key-length></code> 	These commands are exclusive. <ul style="list-style-type: none"> • Configure PSK. • Enable downloading certificates from USB or local flash. Note If SCEP is enabled, the <code>ipsec cert install local enable</code> command will fail. Disable SCEP and then execute this command. • Configure SCEP. From Release 2.0.20, xpki is supported as well as ndes. <ul style="list-style-type: none"> • xpki - Use a Cisco Router as the CA server • ndes - Use a Window server as the CA server Example <pre>Gateway(config)#ipsec cert scep http://172.27.163.69/cgi-bin/pkiclient.exe US CA Milpitas Cisco iot CSR1K true</pre>
Step 4	<code>ipsec retry retry-count delay delay-time</code>	Configure number of IPsec retries and delay time (minutes) before IPsec restarts when IPsec is down: <ul style="list-style-type: none"> • <i>retry-count</i>—Number of IPsec retries when IPsec is down. • <i>delay-time</i>—Minutes of delay before restarting IPsec.

	Command or Action	Purpose
Step 5	<code>ipsec enable</code>	Enable IPsec.
Step 6	<code>ipsec subnet lock</code>	Lock the device traffic with IPsec subnet. Traffic outside of the subnet will not be accepted.
Step 7	<code>exit</code>	Return to global configuration mode.
Step 8	<code>show ipsec certs</code>	(Optional) Display details about certificates (RSA only).
Step 9	<code>show ipsec status {info detail}</code>	(Optional) Display details about IPsec status.
Step 10	<code>debug ipsec</code>	(Optional) Enable logging for IPsec. This command should be executed after the ipsec enable command is configured. To disable the logging for IPsec, use the no debug ipsec command. Note This command should be used ONLY for debugging purpose as it can impact performance.
Step 11	<code>show ipsec log</code>	(Optional) Display the IPsec logs on the screen.
Step 12	<code>clear ipsec log</code>	(Optional) Clear the existing IPsec logs.
Step 13	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

What to do next

Before PSK or PKI can be configured, you must configure the primary crypto ipsec profile at the minimum. For more information, see [Configuring Crypto IPsec Profile Common, on page 39](#) and [Configuring Crypto IPsec Profile Individual , on page 41](#).



Note No spaces are allowed in any DNS (or IDs) or ca parameters.



Note Only PSK (IKEv1) and RSA (IKEv2) are supported.

Configuring Crypto IPsec Profile Common

This section contains configurations of attributes shared by all the tunnels.



Note The crypto ipsec profile common command can only configure attributes shared by tunnels for RSA only, but not for PSK.

Beginning in privileged EXEC mode, follow these steps to configure crypto IPsec profile common on the Cisco LoRaWAN Gateway:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	crypto ipsec profile common	Configure parameters used by all tunnels.
Step 3	leftid <left_id>	(Optional) Configures the ID of the LoRaWAN module. <ul style="list-style-type: none"> • <i>left_id</i> - Full subject distinguished name (DN) of the certificate, including IP address, domain name, or e-mail address
Step 4	leftca <left_ca_issuer>	(Optional) Configures the DN of the CA the LoRaWAN module received its certificates from. <ul style="list-style-type: none"> • <i>left_ca_issuer</i> - CA DN of the Cisco LoRaWAN Gateway
Step 5	rightca <right-ca-issuer>	(Optional) Configures the DN of the CA the corresponding IPsec server received its certificates from. <ul style="list-style-type: none"> • <i>right-ca-issuer</i> - CA DN of the IPsec server
Step 6	exit	Exit the crypto ipsec profile common block and updates the IPsec configuration.
Step 7	exit	Return to global configuration mode.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Example

Example of Common Profile Block

```
crypto ipsec profile common
leftid C=CN,ST=Nanning, L=Nanning, O=Cisco,OU=iot,CN=cisco-iot
```

```
leftca cn=LASSI-ROOT-CA,dc=LASSI,dc=example,dc=com
```

Configuring Crypto IPSec Profile Individual

This section contains configuration of the parameters of the individual tunnels between the IPSec server and the Cisco LoRaWAN Gateway. The primary block **MUST** be configured before any other IPSec configurations are implemented.



Note Adding the subnet parameter enforces a subnet-only tunnel. Any packets within that subnet will travel through the tunnel and any packets outside of that subnet will not travel within the tunnel. If all packets need to go through the tunnel, do not configure any subnet. This will establish a host-only tunnel.



Note Primary configurations will override secondary configurations, so if no subnet is configured in primary (default, host-only tunnel) and subnet is configured in the secondary tunnel, then packets will not be able to go through the secondary tunnel.

Beginning in privileged EXEC mode, follow these steps to configure crypto IPSec profile individual on the Cisco LoRaWAN Gateway:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	crypto ipsec profile {primary secondary}	Configure parameters used by individual tunnel.
Step 3	ipaddr <ip-address> ike-time <ike-lifetime> key-time <key-life> aes <ike-encryption>	Configures the required parameters of the tunnel. <ul style="list-style-type: none"> <i>ip-address</i> - IP address or hostname of the IPSec server. <i>ike-lifetime</i> - Lifetime of ISAKMP or IKE SA in seconds. <i>key-life</i> - Lifetime of one tunnel connection instance in seconds. <i>ike-encryption</i> – Encryption method of ike directive in strongSwan; 128 or 256 for aes128-sha256-ecp256 or aes256-sha256-ecp256 by default.
Step 4	rightid <right_id>	(Optional) Configure the ID of the IPSec server.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • <i>right-id</i> - IPsec server's certificate's full subject DN, IP address, domain name, or e-mail address.
Step 5	subnet <subnet/mask>	(Optional) Configures the subnet and mask of IP addresses the IPsec server will accept in the tunnel. <ul style="list-style-type: none"> • <i>subnet/mask</i> - Subnet and mask, for example, 10.0.0.0/8.
Step 6	exit	Exit the crypto ipsec profile individual block and update the IPsec configuration.
Step 7	exit	Return to global configuration mode.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Example

Examples of Primary and Secondary Profile blocks:

```
crypto ipsec profile primary
ipaddr 192.168.3.4 ike-time 86400 key-time 86400 aes 128
subnet 10.10.0.0/8
rightid SN=FTX2103Z05B, unstructuredName=CRS829.cisco.com
exit
!
crypto ipsec profile secondary
ipaddr 192.168.3.1 ike-time 86400 key-time 86400 aes 128
subnet 10.10.0.0/8
rightid
unstructuredName=IR829_CH.cisco.com,C=CN,ST=Nanning,L=Nanning,O=Cisco,OU=IR829,CN=ndes.com
exit
```

Basic Configuration for RSA to Connect to Primary and Secondary

```
172.27.170.71 LoRaWAN Module <-----> Primary 172.27.170.77
                           <-----> Secondary 172.27.170.72
```

```
crypto ipsec profile primary
ipaddress 172.27.170.77 ike-time 86400 key-time 86400 yes 256
exit
crypto ipsec profile secondary
ipaddress 172.27.170.77 ike-time 86400 key-time 86400 yes 256
exit
ipsec cert scep http://172.27.126.60/CertSrv/mscep/mscep.dll US CA Milpitas Cisco iot
```

```
LORA ndes true 2048
ipsec enable
```

Locking Traffic to IPSec Tunnels

When subnets are configured, only the packets destined for that subnet pass through the IPSec tunnel. To make sure that all traffic passes through IPSec tunnels when subnets are configured, use the **ipsec subnet lock** command to allow only the traffic between the IXM and its designated subnets.

Erasing IPSec Certificates and Key

To erase IPSec certificates and key, use the **ipsec cert erase EXEC** command.

Uploading Certificates from USB or Local Flash

To upload certificates from USB, use the following EXEC command:

```
ipsec install usb <pfx-file> <cr> | <password>
```

To upload certificates from local flash, use the following EXEC command:

```
ipsec install local path: file password
```

Example

```
ipsec install local flash:ndes2.pfx cisco
```

Disabling LXC Restart During IPSec Reauthentication

To disable LXC to restart during the IPSec reauthentication, use the **ipsec lxc-restart-disable** command.

Resetting Secure-Storage for Certificate Download

For gateways with a minimum Release 2.1.0.1, if the box is downgraded to an older image, certificates are inaccessible while the older image is loaded. If you want to download new certificates in the older image, run the **pki secure-storage reset EXEC** command before downgrading. This command deletes all currently installed certificates and restructure secure storage. If you do not want to install new certificates in the older image, it is recommended not to run this command.



CHAPTER 8

Configuring PPPoE

This section describes how to configure the Point-to-Point over Ethernet (PPPoE) client on the Cisco LoRaWAN Gateway.

- [PPPoE Client Overview, on page 45](#)
- [Configuring the Dialer Interface, on page 45](#)
- [Configuring the Ethernet Interface, on page 47](#)
- [Enabling the PPPoE Service, on page 47](#)
- [Monitoring and Debugging the PPPoE Configuration, on page 48](#)
- [PPPoE Configuration Examples on IXM and IR829, on page 49](#)

PPPoE Client Overview

The Point-to-Point over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frame. PPPoE combines Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems.

The Cisco Wireless Gateway for LoRaWAN can be configured as a PPPoE client, so that a tunnel can be established for the router to access the WAN.

At system initialization, the PPPoE client establishes a session with the access concentrator by exchanging a series of packets. Once the session is established, a PPP link is set up, which includes authentication using Password Authentication protocol (PAP). Once the PPP session is established, each packet is encapsulated in the PPPoE and PPP headers.

Configuring the Dialer Interface

Beginning in privileged EXEC mode, follow these steps to configure the dialer interface:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dialer <i>number</i>	Enter interface configuration mode for the dialer interface.

	Command or Action	Purpose
Step 3	ip address negotiated	Specify that the IP address for a particular interface is obtained via PPP/IPCP address negotiation.
Step 4	ip mtu <i>number</i>	Configure the maximum transmission unit (MTU) of the PPPoE interface. Default is 1492. <i>number</i> - PPPoE MTU
Step 5	ip tcp adjust-mss <i>number</i>	Configure the Maximum Segment Size (MSS) of the PPPoE interface. Default is 1412. <i>number</i> - PPPoE MSS
Step 6	ppp authentication chap	Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP).
Step 7	ppp chap hostname <hostname>	Define an interface-specific CHAP hostname.
Step 8	ppp chap password <password>	Define an interface-specific CHAP password.
Step 9	dialer-group <i>name</i>	Assign the dialer interface to a dialer group. This command applies the interesting traffic definition to the interface.
Step 10	dialer-pool <i>name</i>	Specify the dialer pool to use to connect to a specific destination subnetwork.
Step 11	exit	Return to global configuration mode.
Step 12	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Example

```

config terminal
interface Dialer 1
 ip address negotiated
 dialer-group 1
 ppp authentication chap
 ppp chap hostname alice
 ppp chap password 1234
 dialer-pool 1
 exit

```


Configuring the Ethernet Interface

Beginning in privileged EXEC mode, follow these steps to configure the Ethernet interface:

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface FastEthernet <i>number</i></code>	Enter interface configuration mode for the Ethernet interface.
Step 3	<code>pppoe-client dial-pool-number <i>number</i></code>	Configure the PPPoE client and specifies the dialer pool.
Step 4	<code>exit</code>	Return to global configuration mode.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Example

```
config terminal)
interface FastEthernet 0/1
 pppoe-client dial-pool-number 1
exit
```

Enabling the PPPoE Service

Beginning in privileged EXEC mode, follow these steps to enable the PPPoE service:

Procedure

	Command or Action	Purpose
Step 1	<code>pppoe <i>profile_number</i></code>	Connect to the PPPoE service. For <i>profile_number</i> , specify the target tunnel profile.
Step 2	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Example

```
# pppoe 1
```

Monitoring and Debugging the PPPoE Configuration

Use the following global configuration commands to display the PPPoE session statistics:

```
#show pppoe session [status|packets|log]
```

```
#show ip interface pppoe
```

Use the following global configuration command to debug the PPPoE configuration:

```
# [no] debug pppoe detail
```

Examples

```
Gateway#show pppoe session status
pppoe-status: Link is up and running on interface ppp1
ppp1      Link encap:Point-to-Point Protocol
          inet addr:13.13.1.10 P-t-P:13.13.13.1 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1
          RX packets:310 errors:0 dropped:0 overruns:0 frame:0
          TX packets:439 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:76623 (74.8 KiB) TX bytes:128214 (125.2 KiB)

Gateway#show pppoe session packets
      IN  PACK VJCOMP  VJUNC  VJERR  |      OUT  PACK VJCOMP  VJUNC  NON-VJ
      76623   310     0     0     0  |  128214   439     0     0     439

Gateway#show ip interface PPPoE
PPP1 is up
  Internet address is 13.13.1.10
  Netmask is 255.255.255.255
  Server address is 13.13.13.1
  MTU is 1492 bytes

Gateway#show ip route
Kernel IP routing table
Destination        Gateway           Genmask           Flags Metric Ref    Use Iface
0.0.0.0            0.0.0.0          0.0.0.0           U     0     0     0 ppp1
10.0.3.0          0.0.0.0          255.255.255.0    U     0     0     0 lxcbr0
13.13.13.1        0.0.0.0          255.255.255.255 UH    0     0     0 ppp1
```

PPPoE Configuration Examples on IXM and IR829

The following is an example of PPPoE client configuration on IXM:

```
!
interface FastEthernet 0/1
 pppoe-client dial-pool-number 1
 exit
!
interface Dialer 1
 ip address negotiated
 dialer-group 1
 ppp authentication chap
 ppp chap hostname alice
 ppp chap password 1234
 dialer-pool 1
 exit
!
pppoe 1

ipsec enable
```

The following is an example of PPPoE server configuration on IR829:

```
IR800#show running-config
*Jul 31 23:55:30.118: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...

Current configuration : 3713 bytes
!
! Last configuration change at 23:55:30 UTC Mon Jul 31 2017
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IR800
!
boot-start-marker
boot system flash:ir800-universalk9-mz.SPA.156-3.M2
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authentication login default local enable
aaa authentication login IKE1_IKE2_AUTHEN_LOCAL local
aaa authorization network IKE1_IKE2_AUTHOR_LOCAL local
!
!
!
!
!
aaa session-id common
service-module wlan-ap 0 bootimage autonomous
!
```



```
    ip address 13.13.13.1 255.255.255.0
    !
interface GigabitEthernet0
    no ip address
    shutdown
    !
interface GigabitEthernet1
    no ip address
    !
interface GigabitEthernet2
    no ip address
    !
interface GigabitEthernet3
    no ip address
    pppoe enable group ALTAMEER
    !
interface GigabitEthernet4
    switchport access vlan 10
    no ip address
    !
interface Wlan-GigabitEthernet0
    no ip address
    !
interface Wpan2
    no ip address
    ieee154 txpower 25
    no ieee154 fec-off
    !
interface GigabitEthernet5
    no ip address
    shutdown
    duplex auto
    speed auto
    !
interface Cellular0
    no ip address
    encapsulation slip
    dialer in-band
    dialer string lte
    !
interface Cellular1
    no ip address
    encapsulation slip
    !
interface Virtual-Template33
    mtu 1492
    ip unnumbered Loopback3
    ip nat inside
    ip virtual-reassembly in
    peer default ip address pool ALTAMEER
    ppp authentication chap
    !
interface wlan-ap0
    no ip address
    shutdown
    !
interface Vlan1
    no ip address
    ip nat outside
    ip virtual-reassembly in
    pppoe enable group ALTAMEER
    !
interface Vlan10
    ip address 172.27.170.119 255.255.255.128
```

```

ip nat outside
ip virtual-reassembly in
!
interface Async0
no ip address
encapsulation scada
!
interface Async1
no ip address
encapsulation scada
!
!
ip local pool ALTAMEER 13.13.1.10 13.13.1.20
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface Vlan10 overload
ip route 0.0.0.0 0.0.0.0 Vlan10 172.27.170.1
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
ipv6 ioam timestamp
!
!
access-list 10 permit any
!
!
!
control-plane
!
!
!
!
line con 0
exec-timeout 0 0
stopbits 1
line 1 2
stopbits 1
line 3
script dialer lte
modem InOut
no exec
transport preferred lat pad telnet rlogin lapb-ta mop udptn v120 ssh
transport input all
transport output all
rxspeed 2400000
txspeed 153000
line 4
no activation-character
no exec
transport preferred none
transport input all
transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line 8
no exec
transport preferred lat pad telnet rlogin lapb-ta mop udptn v120 ssh
transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line 1/3 1/6
transport preferred none
transport output none
stopbits 1
line vty 0 4

```

```
exec-timeout 0 0
privilege level 15
password cisco
transport input all
transport output all
!
no scheduler max-task-time
iox client enable interface GigabitEthernet5
!
!
!
!
!
!
end
```




CHAPTER 9

Managing Packet Forwarder

This chapter describes how to configure and manage the LoRaWAN packet forwarder (LRR) based on Thingpark implementation. Note that other 3rd party LoRaWAN packet forwarder may have different file structure. All examples in this section are based on Thingpark.

You can use the packet forwarder upload command to upload any *.ini files to the LXC container /etc/ folder.

LRR package can be copied to flash or usb and installed using packet forwarder command.



Note LRR ID is the key information required to register a LoRaWAN Gateway on Thingpark Network Manager.

- [Uploading or Downloading Packet Forwarder, on page 55](#)
- [Managing Packet Forwarder, on page 56](#)
- [Managing Common Packet Forwarder \(CPF\), on page 57](#)

Uploading or Downloading Packet Forwarder

Beginning in privileged EXEC mode, follow these steps to upload or download configuration files to host or USB from LRR.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>packet-forwarder {upload normal <path> download normal <filename>}</code>	Upload or download configuration files to host or USB from LRR.
Step 3	<code>exit</code>	Return to privileged EXEC mode.
Step 4	<code>show packet-forwarder uploads [detail]</code>	Display details about uploaded files.

Managing Packet Forwarder

Beginning in privileged EXEC mode, follow these steps to manage the packet forwarder.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>packet-forwarder [install uninstall] [firmware pubkey]</code>	Install or uninstall the packet forwarder. The packet forwarder can be installed from a file in USB drive or in flash.
Step 3	<code>packet-forwarder [start restart stop]</code>	Start, restart, or stop the packet forwarder.
Step 4	<code>exit</code>	Return to privileged EXEC mode.
Step 5	<code>show packet-forwarder [info status log [list name]]</code>	Show packet forwarder details.

Example

- The following commands install the LRR package:

```
(config)#packet-forwarder install pubkey flash:lrr-opk.pubkey
(config)#packet-forwarder install firmware flash:lrr-1.8.23-ciscoms_noconfig.cpkg
```

- The following commands show the packet forwarder information and status:

```
#show packet-forwarder info
PublicKeyStatus : Installed
FirmwareStatus : Installed
PacketFwdVersion : 1.8.23
LRRID : 6596c32a
PartnerID : 0001
#
#show packet-forwarder status
Status : Running
```

- When the packet-forwarder is shown as “running”, the LRR log files can be displayed IXM through the by using the `show packet-forwarder log list` command:

```
#show packet-forwarder log list
Log file      Description
=====
lrr.ini       lrr.ini information
config        Get the detail config
radio         Radio status
trace         LRR Trace log
```

- The following command specifies the numbers of log to be displayed.

```
#show packet-forwarder log name config 10
11:37:41.696 (3168) sortchan frhz=913900000 index=58
11:37:41.696 (3168) sortchan frhz=914100000 index=59
11:37:41.696 (3168) sortchan frhz=914200000 index=71
11:37:41.696 (3168) sortchan frhz=914300000 index=60
```

```

11:37:41.696 (3168) sortchan frhz=914500000 index=61
11:37:41.696 (3168) sortchan frhz=914700000 index=62
11:37:41.696 (3168) sortchan frhz=914900000 index=63
$ROOTACT /tmp/mdm/pktfwd/firmware
ConfigDefault '/tmp/mdm/pktfwd/firmware/lrr/config'
ConfigCustom '/tmp/mdm/pktfwd/firmware/usr/etc/lrr'

```

- The following command displays the lrr.ini file.

```

#show packet-forwarder log name lrr.ini
port_crypted_k=0
ftppaddr=[58ba93ec55edaf7b8d43c8fb34bc96652abf5db92b0b675a405ad3abf93289d2]
ftppaddr_crypted_k=0
ftppuser=[df09087afa773c3dde7994ee50ab0ad9]
ftppuser_crypted_k=0
ftpppass=[ed37881434753d194bbe66a8bc2de5ba]
ftpppass_crypted_k=0
ftppport=[2ab6268fa568f91eaa80c4e531aabe80]
ftppport_crypted_k=0
use_sftp=0

```

Managing Common Packet Forwarder (CPF)

This section describes how to configure and manage the common packet forwarder (CPF) on the Cisco LoRaWAN Gateway.

Understanding Common Packet Forwarder

CPF is an agent running on the host of a LoRa gateway, forwarding RF packets received by the concentrator (uplinks) to a LoRaWAN Network Server (LNS) through secured IP links and transmitting RF packets sent by the LNS (downlinks) through the same secured IP links to some device.

Configuring Common Packet Forwarder

If the LRR packages are installed, CPF cannot be enabled. Uninstall any LRR packages before configuring CPF.

When CPF is enabled, it will perform a GPS check on bootup. This GPS check will use the currently recorded coordinates to verify that the given channel plans are valid in that location. Once a location fix is achieved, the location is stored in non-volatile memory. The location fix status can be viewed using the **show gps history** command. After this point, GPS is no longer required and the antenna does not need to be connected.



Note Factory defaulting the IXM deletes this stored location information, in which case, a location fix will need to be achieved again.

Refer to the respective [Release Notes](#) for countries supported by the IXM.

Beginning in privileged EXEC mode, follow these steps to configure common packet forwarder on the Cisco LoRaWAN Gateway:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	common-pack-forwarder cert install gw <i>path-to-cert path-to-key</i>	Install IXM gateway's certification and key (mandatory if <i>auth-mode</i> is client-server): <i>path-to-cert</i> – file path to the gateway's cert <i>path-to-key</i> – file path to the gateway's key
Step 3	common-pack-forwarder cert install srv <i>path-to-cert</i>	Install IXM LNS' CA certificate (mandatory if <i>auth-mode</i> is other than none): <i>path-to-cert</i> – file path to the LNS' CA cert
Step 4	common-pack-forwarder cert erase gw	Erase IXM LoRa gateway's certification and key.
Step 5	common-pack-forwarder cert erase srv	Erase LNS server's certification.
Step 6	common-packet-forwarder profile	Configure parameters for the CPF.
Step 7	ipaddr <i>ip-address</i> port <i>port</i>	Configure network server IP address and port. <i>ip-address</i> – Network server IP address <i>port</i> – Network server port number
Step 8	auth-mode <i>mode</i>	Authentication mode. <ul style="list-style-type: none"> • none: use websocket (ws), default • client-server: authenticate both client and server with secure websocket (wss) • server: server authentication, only
Step 9	gps enable	Enable CPF to utilize GPS signal.
Step 10	aeskey <i>key</i>	Configure AES key used for CPF. <i>key</i> – AES key used for CPF
Step 11	gatewayid <i>gateway-id</i>	Configure gateway id used for CPF. <i>gateway-id</i> – Gateway ID used for CPF
Step 12	antenna <i>antenna-number</i> type <i>antenna-type</i> gain <i>antenna-gain</i> loss <i>cable-loss</i>	Configure individual antenna properties. <i>antenna-number</i> – Antenna ID <1,2> <i>antenna-type</i> – Antenna type <omni, sector> <i>antenna-gain</i> – Antenna gain <i>cable-loss</i> – Cable loss

	Command or Action	Purpose
Step 13	region-cp <i>lora-region-name</i>	Configure LoRa region channel plan code per naming convention defined in LoRa Alliance RP2-1.0.2 (for example: EU868, AU915, AS923-1, AS923-2, AS923-3, IN65, RU864). <i>lora-region-name</i> – LoRa region code name (optional if default one is used)
Step 14	board-bw <i>bandwidth</i>	<i>bandwidth</i> – Manually setup the board rx bandwidth if you need to change the default. Note Default board RX channel frequency and bandwidth are 866.5 MHz, 7 MHz for 800 SKU, and 908.6 MHz, 13 MHz for 900 SKU. You need to manually configure the frequency and bandwidth for regions that use frequencies falling outside of the defaults. AU915, KR920, and AS923-x are the specific channel plans that do not work with the default settings.
Step 15	board-freq <i>freq</i>	<i>freq</i> – Manually setup the board rx frequency if you need to change the default. Note Default board RX channel frequency and bandwidth are 866.5 MHz, 7 MHz for 800 SKU, and 908.6 MHz, 13 MHz for 900 SKU. You need to manually configure the frequency and bandwidth for regions that use frequencies falling outside of the defaults. AU915, KR920, and AS923-x are the specific channel plans that do not work with the default settings.
Step 16	tcp-user-timeout <i>timeout</i>	Configure TCP user timeout option: • <i>timeout</i> – TCP timeout in seconds.
Step 17	tls-sni <i>enable</i>	<i>enable</i> – Connect to LNS to compare the configured LNS server name with the one embedded in the LNS server's certificate.

	Command or Action	Purpose
Step 18	<code>cpf enable</code>	Start the CPF. If prompted about a Smart License, answer "yes".
Step 19	<code>exit</code>	Exit the CPF profile block and update the CPF configuration.
Step 20	<code>exit</code>	Return to privileged EXEC mode.
Step 21	<code>show common-packet-forwarder info</code>	(Optional) Show CPF configuration and information.
Step 22	<code>show common-packet-forwarder status</code>	(Optional) Show current state of CPF and if registration with NS was successful.
Step 23	<code>show common-packet-forwarder log list</code>	(Optional) List available log options such as CPF configuration or trace.
Step 24	<code>show common-packet-forwarder log name trace number-of-lines</code>	(Optional) Display the CPF trace log. <i>number-of-lines</i> – Number of lines in log to display from end of file.
Step 25	<code>show common-packet-forwarder log name config number-of-lines</code>	(Optional) Display the current CPF configuration. <i>number-of-lines</i> – Number of lines in config to display from end of file.
Step 26	<code>debug cpf</code>	(Optional) Change CPF trace log level to "DEBUG". Note The default log level is "WARNING". This command is to change CPF log level to "DEBUG".



- Note**
1. Usually the country configuration is not needed and is not used by the gateway. The resident country is determined by the gps location information automatically. It is used only when the LoRa gateway is managed by Cisco IDA agent in privileged mode.
 2. Region-cp is only needed when the resident country supports multiple LoRa region channel plans and a non-default one is used (for example, in US, default channel plan is US915. If AU915 is wanted, set region-cp to AU915).
 3. Class B is supported. Refer to <https://doc.sm.tc/station/tcp proto.html#> for more information about Class B requirements on LoRa Server side (time sync and beacon configurations).

Example

- Example of Common Packet Forwarder Profile Block:

```
common-packet-forwarder profile
  ipaddr A.B.C.D port XXXX
  gps enable
  aeskey 00AEAEFFFE000000
  antenna 1 omni gain 1.5 loss 0.2
  antenna 2 sector gain 1.5 loss 0.2
  gatewayid ::1
  cpf enable
  exit
```

- Example of showing Common Packet Forwarder information and status:

```
#show common-packet-forwarder info
FirmwareStatus : Installed
FirmwareVersion : 2.1.0.1
Gateway ID : ::1
Region : US915
IPAddress:Port : A.B.C.D:XX
TXLut :
<NA,NA,NA,50,32,105,96,88,79,71,63,53,44,35,26,17-NA,NA,NA,48,30,102,93,85,77,69,61,52,43,34,25,16>
GPS : Enabled
AESKey : 00AEAEFFFE000000
Antenna 1 : enabled, type omni, gain 1.5, loss 0.2
Antenna 2 : enabled, type sector, gain 1.5, loss 0.2

#show common-packet-forwarder status
Enabled : Yes
Running : Yes
NS Registration : Successful
```



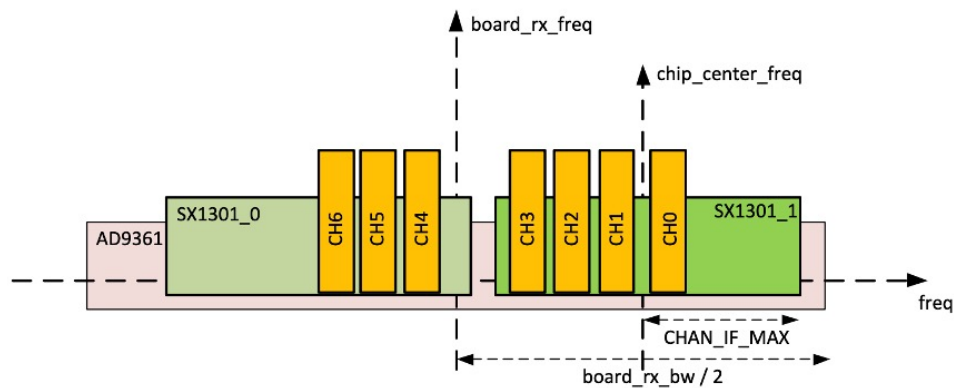
Note The **Enabled** status simply means that CPF has been configured successfully. **Running** status depicts whether CPF has started successfully or not. Note that GPS signal should be available for the CPF to run correctly.

Guidelines and Limitations of Configuring RX Channel Frequency and Bandwidth

There are some constraints when you configure RX channel frequency and bandwidth on the IXM gateway. The CPF checks if the channel definition is optimal, and returns an error if it is not. It will also check if all the channels defined fit in the sx1301 (the LoRa concentrator chip) band (3 MHz) and in the AD9361 (the main radio board) radio band (4 MHz, 7 MHz, or 13 MHz depending on the region).

The following figure illustrates what is being checked when configuring a channel.

The board RX channel frequency and bandwidth can be configured through the CPF commands **board-freq** and **board-bw** *bandwidth*, if the default values do not fit your use case. Default values are 866.5 MHz, 7 MHz for 800 SKU, and 908.6 MHz, 13 MHz for 900 SKU. The sx1301 related configurations come from the LNS.

**Note**

- It is not recommended to set a channel frequency to the same as the AD9361 radio center frequency (“*board_freq*”). It will degrade the sensitivity on this channel.
- In the figure above, *CHAN_IF_MAX* is set to 1.5 MHz.
- It is not recommended to set a channel above or below 1.3 MHz around the *chip_center_freq* (due to the RX digital filter).
- There is a flexibility to allow having the sx1301 band partly outside of the radio band, if there is no channel in this “outer” band.

Debugging Common Packet Forwarder

When the CPF is running, the CPR trace log file can be displayed through the IXM by using the **show common-packet-forwarder log name trace** command:

```
#show common-packet-forwarder log list
Log file      Description
=====
config        CPF Configuration
trace         CPF Trace log

#show common-packet-forwarder log name trace 15
2019-04-16 09:38:40.625 [SYS:INFO] proto EUI   : ::1      (station.conf)
2019-04-16 09:38:40.625 [SYS:INFO] prefix EUI  : ::0      (station.conf)
2019-04-16 09:38:40.625 [SYS:INFO] Station EUI : ::1
2019-04-16 09:38:40.625 [SYS:INFO] Station home: /etc/cpf/      (--home)
2019-04-16 09:38:40.625 [SYS:INFO] Station temp: /var/tmp/     (builtin)
2019-04-16 09:38:40.625 [SYS:WARN] Station in NO-CUPS mode
2019-04-16 09:38:40.825 [TCE:INFO] Starting TC engine
2019-04-16 09:38:40.828 [AIO:ERRO] [4] WS connect failed: NET - The connection to the given
server / port failed
2019-04-16 09:38:40.828 [AIO:DEBU] [4] WS connection shutdown...
2019-04-16 09:38:40.828 [TCE:ERRO] TC connect failed - URI: ws://10.156.154.54:6090
2019-04-16 09:38:40.828 [TCE:INFO] INFOS reconnect backoff 0s (retry 0)
2019-04-16 09:38:41.821 [AIO:ERRO] [4] WS connect failed: NET - The connection to the given
server / port failed
2019-04-16 09:38:41.821 [AIO:DEBU] [4] WS connection shutdown...
```



```
2019-04-16 09:38:41.821 [TCE:ERRO] TC connect failed - URI: ws://10.156.154.54:6090
2019-04-16 09:38:41.821 [TCE:INFO] INFOS reconnect backoff 10s (retry 1)
```

```
# show common-packet-forwarder log name config 15
  "log_size": 10000000,
  "log_rotate": 3,
  "gps": "/dev/ttyS1",
  "TX_AIM_GAP": "90ms",
  "pps": "fuzzy"
},
"gps_conf": {
  "gw_latitude": 0,
  "gw_longitude": 0,
  "gw_altitude": 0,
  "fixed_altitude": false
}
}
=====
station channel plan
```

The command **debug cpf** can also be executed to increase the log level of cpf logging.



CHAPTER 10

Managing Plug-n-Play (PnP)

This chapter describes how to configure and manage the Plug-n-Play (PnP) on the Cisco LoRaWAN Gateway.

- [Understanding Plug-n-Play, on page 65](#)
- [Configuring Plug-n-Play, on page 65](#)
- [Debugging Plug-n-Play, on page 67](#)

Understanding Plug-n-Play

The PnP agent is an embedded software application running on Cisco routers, switches, wireless access points, and sensors. It enables zero-touch provisioning by automatically starting on boot up for new or factory reset devices and by automatically discovering the PnP server. Once a secure channel communication is established with the PnP server through one of the secure PnP discovery mechanisms, the PnP agent is capable of performing different operations on a Cisco device, such as image upgrading, configuration upgrading, and CLI executing.

Configuring Plug-n-Play



Note The PnP agent will be triggered only by doing a factory reset on an existing device or on a completely new device.

PnP agent on the IXM supports the following DHCP, DNS, and CCO discovery mechanisms:

- DHCP/DNS discovery: The precondition of using DHCP and DNS discovery is to setup DHCP server first. Refer to <http://pnp.cisco.com/index.php/solutions/training/agent-discovery> for information on configuring the DHCP server.

- CCO discovery:

This configuration is only for PnP CCO discovery use. If IXM needs NTP server, it still needs to go through CLIs.

1. Log in to <https://software.cisco.com/#>
2. Choose [Plug and Play Connect](#) under Network Plug and Play.

3. Add the device information.
4. You will see status "Pending Redirection."
5. When device connects to CCO status will be "Contacted" and after some time "Redirected."
6. After successful PNP, a Redirection Successful message appears.

For more information, see the following document: <http://pnp.cisco.com/index.php/solutions/pnp-connect>.

Follow these steps to configure pnp on the LoRaWAN gateway:

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	pnp enable	Start the PnP agent.
Step 3	pnp disable	Stop the PnP agent.
Step 4	exit	Exit the global configuration mode.
Step 5	show pnp profiles	(Optional) Show PnP version.
Step 6	show pnp status	(Optional) Show PnP status.
Step 7	show pnp log name trace <i>number-of-lines</i>	(Optional) Display the PnP trace log. <i>number-of-lines</i> – Number of lines in the log to display from end of file. <i>number-of-lines</i> – Number of lines in config to display from end of file.

Example

Example of showing PnP profiles and status

```
#show pnp profiles
Created by                UDI
DHCP Discovery  PID:POSIX-Reference,VID:V01,SN:23336985067

Primary transport: http
Address: 10.154.201.104
Port: 9455
CA file:

Work-Request Tracking:
  Pending-WR: Correlator=
Cisco-PnP-POSIX-reference-1.8.1.dev19-2-7013f6f5-ac52-4a96-b589-ac35d91c499b-1
  Last-WR:    Correlator=
Cisco-PnP-POSIX-reference-1.8.1.dev19-1-c9aad77-760b-42b6-b6c7-859093ab5e09-1
  PnP Response Tracking:
  Last-PR:   Correlator=
Cisco-PnP-POSIX-reference-1.8.1.dev19-1-c9aad77-760b-42b6-b6c7-859093ab5e09-1
```

```
#show pnp status
PnP Agent is running

#show pnp status
PnP Agent is not running
file-transfer
    status: Failure
    time: 17:44:01 Aug 06
server-connection
    status: Success
    time: 17:44:01 Aug 06
```

Debugging Plug-n-Play

When the PnP is running , the PnP trace log file can be displayed through the IXM using the **show pnp log name trace** command:

```
#show pnp log name trace 15
2016-08-06 17:43:56,023 - pnp.infra.network.HTTPConnClient - DEBUG - PNP requests with url:
    http://10.154.201.104:9455/pnp/HELLO
2016-08-06 17:43:56,040 - pnp.discovery.infra.discovery_manager - DEBUG - Existing profile
    config found valid.
2016-08-06 17:43:56,041 - pnp.discovery.infra.discovery_manager - DEBUG - Discovery skipped
    upon existing profile configs presence
2016-08-06 17:43:56,043 - pnp.infra.utils.pnp_utils - DEBUG - PnP config read: Connection
Info:
Transport: http
Address: 10.154.201.104
Port: 9455
Remote CA File:
Core Trust Enabled? False
2016-08-06 17:43:56,056 - pnp.agent - INFO - platform_dict: {'hardwareInfo': {'platformName':
    'reference', 'hostname': 'Gateway', 'vendor': 'Network-PnP', 'processorT
2016-08-06 17:43:56,058 - pnp.agent - DEBUG - Unsuccessful attempt to get reason code from
    msg: INVALID_REASON_CODE
2016-08-06 17:43:56,058 - pnp.agent - DEBUG - Agent not using reload reason.
2016-08-06 17:43:56,058 - pnp.agent - INFO - UDI: PID:POSIX-Reference,VID:V01,SN:81961640269
2016-08-06 17:43:56,061 - pnp.infra.utils.pnp_utils - DEBUG - PnP config read: Connection
Info:
Transport: http
Address: 10.154.201.104
```




CHAPTER 11

Smart Licensing Using Policy

- [Overview of Smart Licensing Using Policy, on page 69](#)
- [Architecture, on page 70](#)
- [Concepts, on page 71](#)
- [Supported Topologies, on page 74](#)
- [Workflow for Topology: Full Offline Access, on page 76](#)
- [Workflow for Topology: CSLU Has Access to CSSM, on page 77](#)
- [Workflow for Topology: CSLU Has No Access to CSSM, on page 80](#)
- [Removing the Product Instance from CSSM, on page 85](#)

Overview of Smart Licensing Using Policy

Smart Licensing Using Policy is supported on Cisco Wireless Gateway for LoRaWAN Release 2.2 and later, for the subscription of Common Packet Forwarder (CPF).

Smart Licensing Using Policy is an enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use. Smart Licensing Using Policy provides a seamless experience with the various aspects of licensing.

- **Purchase licenses:** Purchase licenses through the existing channels and use the Cisco Smart Software Manager (CSSM) portal to view product instances and licenses.



Note To simplify your implementation of Smart Licensing Using Policy, provide your Smart Account and Virtual Account information when placing an order for new hardware or software. This allows Cisco to install applicable policies and authorization codes (terms explained in the [Concepts, on page 71](#) section below), at the time of manufacturing.

- **Use:** All licenses on your devices are unenforced. This means that you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date.
- **Report license usage to CSSM:** Multiple options are available for license usage reporting. You can use the Cisco Smart Licensing Utility (CSLU), or report usage information directly to CSSM. For air-gapped

networks, a provision for offline reporting where you download usage information and upload it to CSSM, is also available. The usage report is in plain text XML format.

- Reconcile: For situations where delta billing applies (purchased versus consumed).

The primary benefits of this enhanced licensing model are:

- Seamless day-0 operations

After a license is ordered, no preliminary steps, such as registration or generation of keys etc., are required unless you use an export-controlled or enforced license.

- Visibility and manageability

Tools, telemetry and product tagging, to know what is in-use.

- Flexible, time series reporting to remain compliant

Easy reporting options are available, whether you are directly or indirectly connected to Cisco Smart Software Manager (CSSM), or in an air-gapped network.

Smart Account

To use Smart Licensing, you must first set up a Cisco Smart Account at [Cisco Software Central](#).

A Smart Account provides a single location for all Smart-enabled products and entitlements. It helps speed procurement, deployment, and maintenance of Cisco Software. When creating a Smart Account, you must have the authority to represent the requesting organization. After submitting, the request goes through a brief approval process.

Virtual Account

A Virtual Account exists as a sub-account within the Smart Account. Virtual Accounts are a customer-defined structure based on organizational layout, business function, geography or any defined hierarchy. They are created and maintained by the Smart Account administrator.

Architecture

This section explains the various components that can be part of your implementation of Smart Licensing Using Policy.

Product Instance

A product instance is a single instance of a Cisco product, identified by a Unique Device Identifier (UDI).

A product instance records and reports license usage (RUM reports), and provides alerts and system messages about overdue reports, communication failures, etc. The RUM reports and usage data are also stored securely in the product instance.

Cisco Smart Software Manager (CSSM)

CSSM is a portal that enables you to manage all your Cisco software licenses from a centralized location. CSSM helps you manage current requirements and review usage trends to plan for future license requirements.

You can access CSSM at <https://software.cisco.com>. Under the License tab, click the Smart Software Licensing link.

In CSSM you can:

- Create, manage, or view virtual accounts.
- Create and manage Product Instance Registration Tokens.
- Transfer licenses between virtual accounts or view licenses.
- Transfer, remove, or view product instances.
- Run reports against your virtual accounts.
- Modify your email notification settings.
- View overall account information.

Prior to using CSSM, please view a short video about how to use the portal found here:

<https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html>

Click on the **View Video** button.

Cisco Smart Licensing Utility (CSLU)

CSLU is a Windows-based reporting utility that provides aggregate licensing work-flows. This utility performs the following key functions:

- Provides the options relating to how work-flows are triggered. The work-flows can be triggered by CSLU or by the product instance.
- Collects usage reports from the product instance and upload these usage reports to the corresponding smart account or virtual account – online, or offline, using files. Similarly, the RUM report ACK is collected online, or offline, and provided back to the product instance.
- Sends authorization code requests to CSSM and receives authorization codes from CSSM.

CSLU can be part of your implementation in the following ways:

- Install the windows application, to use CSLU as a standalone tool and connect it to CSSM.
- Install the windows application, to use CSLU as a standalone tool and not connect it to CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited to air-gapped networks.

Concepts

This section explains the key concepts of Smart Licensing Using Policy.

License Enforcement Types

A given license belongs to one of three enforcement types. The enforcement type indicates if the license requires authorization before use, or not.

- Unenforced or Not Enforced

Unenforced licenses *do not* require authorization before use in air-gapped networks, or registration, in connected networks. The terms of use for such licenses are as per the end user license agreement ([EULA](#)).

- Enforced

Licenses that belong to this enforcement type require authorization before use. The required authorization is in the form of an authorization code, which must be installed in the corresponding product instance.

An example of an enforced license is the Media Redundancy Protocol (MRP) Client license, which is available on Industrial Ethernet Switches.

- Export-Controlled

Licences that belong to this enforcement type are export-restricted by U.S. trade-control laws and these licenses require authorization before use. The required authorization code must be installed in the corresponding product instance for these licenses as well. Cisco may pre-install export-controlled licenses when ordered with hardware purchase.

An example of an export-controlled license is the High Speed Encryption (HSECK9), which is available on certain Cisco Routers.

License Duration

This refers to the duration or term for which a purchased license is valid. A given license may belong to any one of the enforcement types mentioned above and be valid for the following durations:

- Perpetual: There is no expiration date for such a license.
- Subscription: The license is valid only until a certain date.

Authorization Code

The Smart Licensing Authorization Code (SLAC) allows activation and continued use of a license that is export-controlled or enforced.

If you are upgrading from an earlier licensing model to Smart Licensing Using Policy, you may have a Specific License Reservation (SLR) with its own authorization code. The SLR authorization code is supported after upgrade to Smart Licensing Using Policy.

Policy

A policy provides the product instance with these reporting instructions:

- License usage report acknowledgement requirement (Reporting ACK required): The license usage report is known as a RUM Report and the acknowledgement is referred to as an ACK (See [RUM Report and Report Acknowledgement, on page 74](#)). This is a yes or no value which specifies if the report for this product instance requires CSSM acknowledgement or not. The default policy is always set to “yes”.

- First report requirement (days): The first report must be sent within the duration specified here.
- Reporting frequency (days): The subsequent report must be sent within the duration specified here.
- Report on change (days): In case of a change in license usage, a report must be sent within the duration specified here.

Understanding Policy Selection

CSSM determines the policy that is applied to a product instance. Only one policy is in use at a given point in time. The policy and its values are based on a number of factors, including the licenses being used.

`Cisco default` is the default policy that is always available in the product instance. If no other policy is applied, the product instance applies this default policy. The table below shows the `Cisco default` policy values.

While you cannot configure a policy, you can request for a customized one, by contacting the Cisco Global Licensing Operations team. Go to [Support Case Manager](#). Click **OPEN NEW CASE** > Select **Software Licensing**. The licensing team will contact you to start the process or for any additional information. Customized policies are also made available through your Smart account in CSSM.



Note To know which policy is applied (the policy in-use) and its reporting requirements, enter the **show license all** command in privileged EXEC mode.

Table 5: Policy: Cisco default

Policy: <code>Cisco default</code>	Default Policy Values
Export (Perpetual/Subscription) Note Applied only to licenses with enforcement type "Export-Controlled".	Reporting ACK required: Yes First report requirement (days): 90 Reporting frequency (days): 90 Report on change (days): 90
Enforced (Perpetual/Subscription) Note Applied only to licenses with enforcement type "Enforced".	Reporting ACK required: Yes First report requirement (days): 90 Reporting frequency (days): 90 Report on change (days): 90
Unenforced/Non-Export Perpetual ¹	Reporting ACK required: Yes First report requirement (days): 365 Reporting frequency (days): 0 Report on change (days): 90

Policy: <code>Cisco default</code>	Default Policy Values
Unenforced/Non-Export Subscription	Reporting ACK required: Yes First report requirement (days): 90 Reporting frequency (days): 90 Report on change (days): 90

¹ For Unenforced/Non-Export Perpetual: the default policy's first report requirement (within 365 days) applies only if you have purchased hardware or software from a distributor or partner.

RUM Report and Report Acknowledgement

A Resource Utilization Measurement report (RUM report) is a license usage report, which the product instance generates, to fulfil reporting requirements as specified by the policy.

An acknowledgement (ACK) is a response from CSSM and provides information about the status of a RUM report.

The policy that is applied to a product instance determines the following reporting requirements:

- Whether a RUM report is sent to CSSM and the maximum number of days provided to meet this requirement.
- Whether the RUM report requires an acknowledgement (ACK) from CSSM.
- The maximum number of days provided to report a change in license consumption.

A RUM report may be accompanied by other requests, such as a trust code request, or a SLAC request. So in addition to the RUM report IDs that have been received, an ACK from CSSM may include authorization codes, trust codes, and policy files as well.

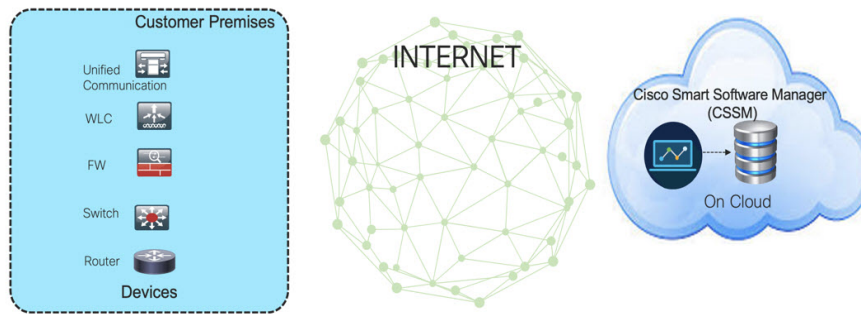
Trust Code

A UDI-tied public key with which the product instance signs a RUM report. This prevents tampering and ensures data authenticity.

Supported Topologies

This section describes the various ways in which you can implement Smart Licensing Using Policy. Cisco Wireless Gateway for LoRaWAN supports the following topologies:

- Full Offline Access



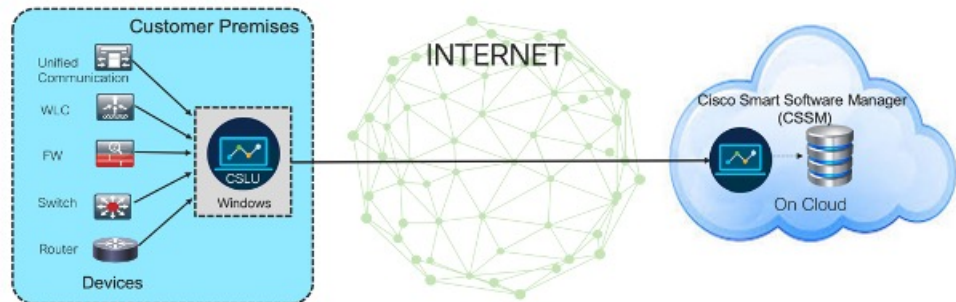
In this topology, devices do not have connectivity to CSSM (software.cisco.com). You must copy and paste information between Cisco products and CSSM to manually check in and out licenses.

To implement this topology, see [Workflow for Topology: Full Offline Access, on page 76](#).

- CSLU (Cisco Smart Licensing Utility) mode

CSLU mode has two different kind of CSLU modes depending on the topology between the CSLU and CSSM.

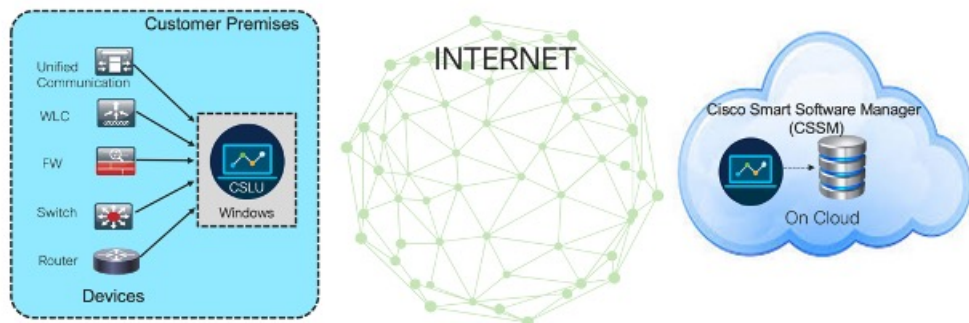
- CSLU has access to CSSM



In this topology the devices are connected to CSLU controller. There is connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com). Cisco products send usage information to a locally installed CSLU. There is online transmission between CSLU and CSSM to check-in and check-out licenses and data.

To implement this topology, see [Workflow for Topology: CSLU Has Access to CSSM, on page 77](#).

- CSLU has No Access to CSSM.



In this topology the devices are connected to CSLU. There is no connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com). Cisco products send usage information to a locally installed CSLU. You need to copy and paste information between CSLU and CSSM to manually check-in and check-out licenses.

To implement this topology, see [Workflow for Topology: CSLU Has No Access to CSSM, on page 80](#).

Workflow for Topology: Full Offline Access

This procedure requires a manual exchange of required information between the router and CSSM.

Procedure

-
- Step 1** Set license transport method to “off”.
- In configuration mode, perform the following:
- Example:**
- ```
Gateway#configure terminal
Gateway(config)#license smart transport off
```
- Step 2** Start license service through enabling common-packet-forwarder.
- In configuration mode, perform the following:
- Example:**
- ```
Gateway(config)#common-packet-forwarder profile
Gateway(config-cpf-profile)#ipaddr A.B.C.D port X
Gateway(config-cpf-profile)#cpf enable
```
- Step 3** Generate a license usage (RUM reports) file from the device and export the license usage file to your host laptop/PC.
- Enter the **license smart save usage** command in privileged EXEC mode.
- Example:**
- ```
Gateway#license smart save usage all file flash:report
```
- Step 4** Copy the usage report from IXM using the SCP command in privileged EXEC mode.
- Example:**
- ```
Gateway#scp local flash:report user1 171.69.181.77 /ws/user1/report
```
- Step 5** Import the license usage file to CSSM on Cloud.
- Log in to the CSSM Web UI at <https://software.cisco.com>, using the username and password provided by Cisco.
 - Select the **Smart Account** (upper left-hand corner of the screen) that will receive the report.
 - Select **Smart Software Licensing** → **Reports** → **Usage Data Files**.
 - The **Upload Usage Data** window appears. Click **Browse**, and navigate to where the file is. Click on **Upload Data**.

- e) From the **Select Virtual Accounts** pop-up, select the Virtual Account that will receive the uploaded file. The file is uploaded to Cisco and is listed in the Usage Data Files table in the Reports screen showing the File Name, time it was Reported, which Virtual Account it was uploaded to, the Reporting Status, Number of Product Instances reported, and the Acknowledgement status.
- f) In the Acknowledgement column, click **Download** to save the **.txt** ACK file for the report you uploaded. Wait for the ACK to appear in the Acknowledgement column.
- g) Check under the **Product Instances** tab to verify your device is listed.

Step 6 Download the ACK file, using the SCP command in privileged EXEC mode.

Example:

```
Gateway#scp remote user 171.69.181.77 /ws/ACK_report flash:ACK_report
```

Step 7 Import the ACK file from CSSM to your device, using the **license smart import file** command in privileged EXEC mode.

Example:

```
Gateway#license smart import file flash: ACK_report
```

Step 8 Verify the Product Instance has imported the data. Use the following command to display license authorization, policy and reporting information for the product instance.

Example:

```
Gateway#show license usage
```

Step 9 Verify the license is in use.

Example:

```
Gateway#show license summary
```

Workflow for Topology: CSLU Has Access to CSSM

Tasks for Product Instance-Initiated Communication:

- Ensure network reachability (SSH).
- Check NTP status is in sync.
- Ensure the transport type is set to **cslu** (default).

```
Device (config) #license smart transport cslu
```

- Specify the CSLU information to be used.

Configure a specific URL for CSLU by using the following CLI:

```
Device (config) #license smart url cslu http://<HOST or IP>:<port-num>/cslu/v1/pi
```

- *HOST or IP* – Hostname / IP address of the windows (where CSLU is installed)
 - *port-num* – use 8180 or 8182.
- Verify the license policy is successfully installed by running the CLI command and verifying the time/date stamp.

```

Gateway#show common-packet-forwarder status
Enabled : Yes
Running : Yes
NS Registration : Successful
License Status: Reported - Yes, Acknowledged - Yes

Gateway#show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: http://172.27.164.116:8182/cslu/v1/pi
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Feb 23 2021 02:14:41 UTC
  Policy name: Test Policy
  Reporting ACK required: no (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 94 (Customer Policy)
    Reporting frequency (days): 100 (Customer Policy)
    Report on change (days): 100 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 100 (Customer Policy)
    Report on change (days): 100 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 204 (Customer Policy)
    Report on change (days): 100 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 100 (Customer Policy)
    Report on change (days): 100 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Feb 23 2021 02:14:41 UTC
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: Feb 23 2021 02:10:41 UTC
  Last report file write: <none>

Trust Code Installed: <none>
Gateway#

```

Sample configuration


```

Gateway#configure terminal
Gateway(config)#interface FastEthernet 0/1
Gateway(config-if)#ip address 172.27.170.104 255.255.255.128
Gateway(config-if)#exit
Gateway(config)#ip default-gateway 172.27.170.1
Gateway(config)#
Gateway(config)#exit
*Feb 20 02:37:17: Configured from console by console
Gateway#
Gateway#configure terminal
Gateway(config)#crypto key generate rsa
Gateway(config)#ip ssh admin-access
Gateway(config)#exit
*Feb 20 02:37:31: Configured from console by console

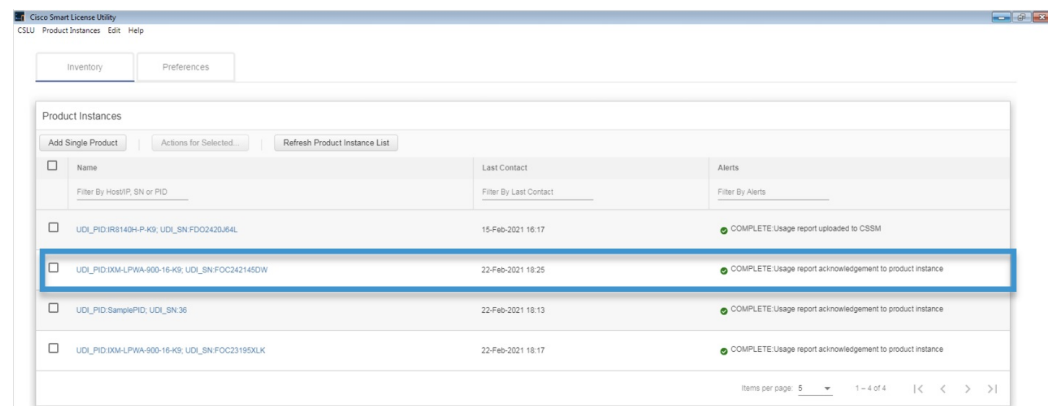
Gateway#
Gateway(config)#configure terminal
Gateway(config)#common-packet-forwarder profile
Gateway(config-cpf-profile)#ipaddr 172.27.166.121 port 6070
Gateway(config-cpf-profile)#cpf enable
By typing 'y' below, I agree that to abide to SMART LICENSING subscription royalty agreement
with Cisco on this unit
Do you agree the above statement? [y/n]y
common-packet-forwarder started successfully

Gateway(config-cpf-profile)#exit
Gateway(config)#exit
Gateway#
Gateway#configure terminal
Gateway(config)#license smart transport cslu
Gateway(config)#license smart url cslu http://172.27.164.116:8182/cslu/v1/pi
Gateway(config)#exit
%SMART_LIC-6-POLICY_INSTALL_SUCCESS:A new licensing policy was successfully installed

```

Check the status of the device on CSLU as shown below:

Figure 1: Verify the status of the device on CSLU



Check updated information on CSSM as shown below:

Figure 2: Verify updated information on CSSM

Cisco Software Central > Smart Software Licensing SA-IOT-Polaris

Smart Software Licensing Feedback Support Help

Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: DEFAULT 1 Minor 2 Informational Hide Alerts

General Licenses **Product Instances** Event Log

Authorize License-Enforced Features... FOC242145DW

Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:XXM-LPWA-900-16-K9; UDI_SN:FOC242145DW	AIRWAN	2021-Feb-23 02:10:47		Actions

Showing 1 Record

Workflow for Topology: CSLU Has No Access to CSSM

In this topology, the devices are connected to CSLU. There is no connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com). Cisco products send usage information to a locally installed CSLU. You need to copy and paste information between CSLU and CSSM to manually check-in and check-out licenses.

Procedure

- Step 1** In the CSLU Preferences tab, click the **Cisco Connectivity** toggle switch to **off**. The field switches to “Cisco Is Not Available”.

CSLU Product Instances Edit Help

Inventory Preferences

Preferences

Cisco Connectivity
 Cisco Is Not Available

CSLU Connectivity

Product Instance Service Port *
8182

REST API Port *
8180

Smart Account
BU Production Test

Virtual Account
Starfleet

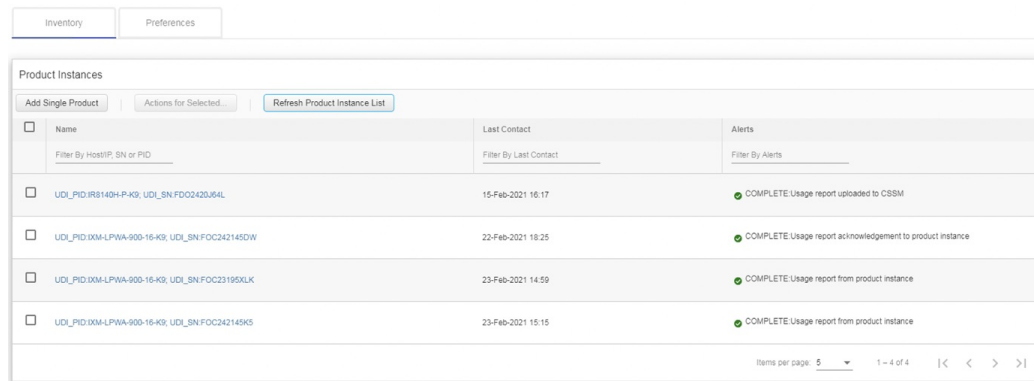
Validate Device

CSLU Working Directory
C:\Users\inagramac\AppData\Roaming\CSLU

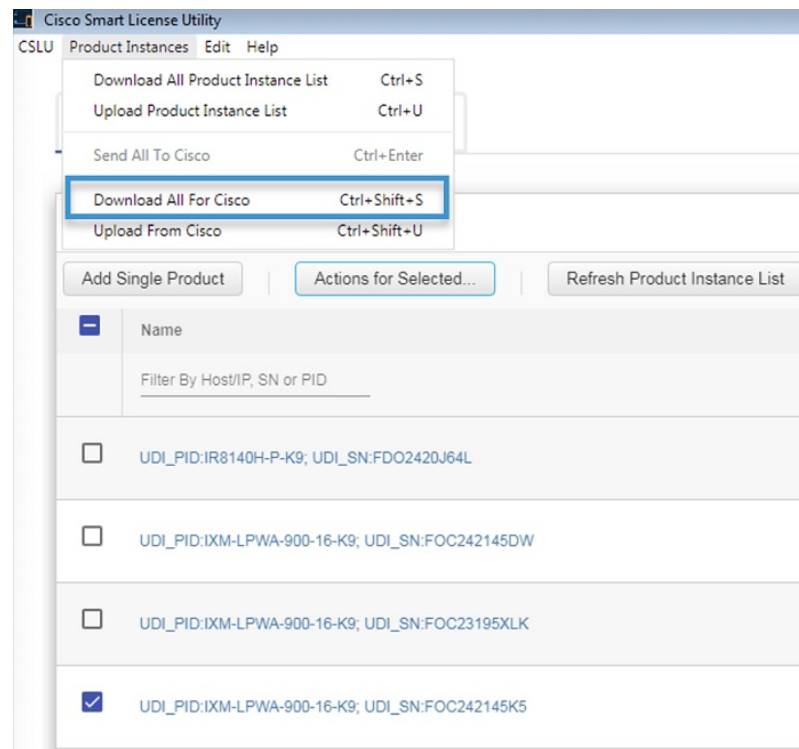
Default Connect Method
Product Instance Initiated only

Save Reset

- Step 2** Download tar file from CSLU.

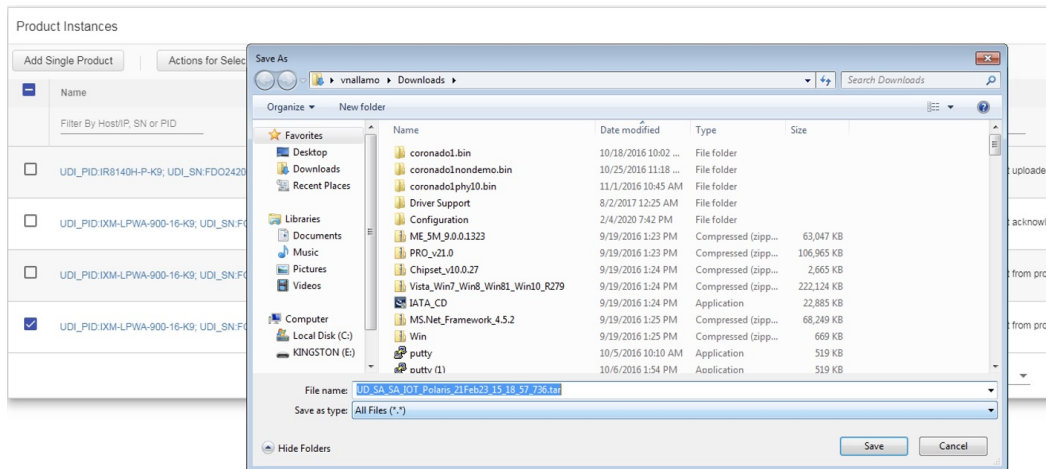


Step 3 Select the PID and choose **Download All for Cisco** from CSLU

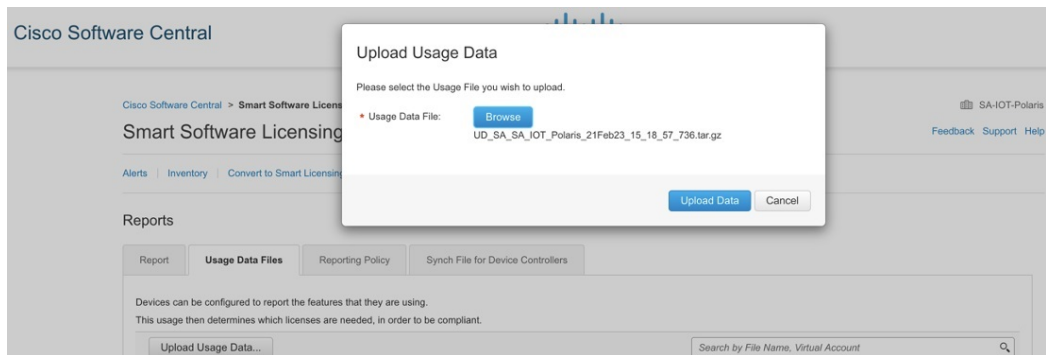


Step 4 Save the file from CSLU.

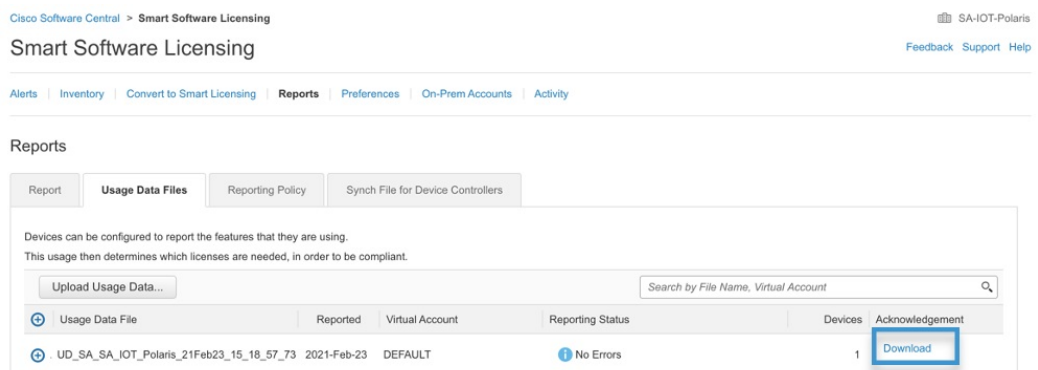
Workflow for Topology: CSLU Has No Access to CSSM



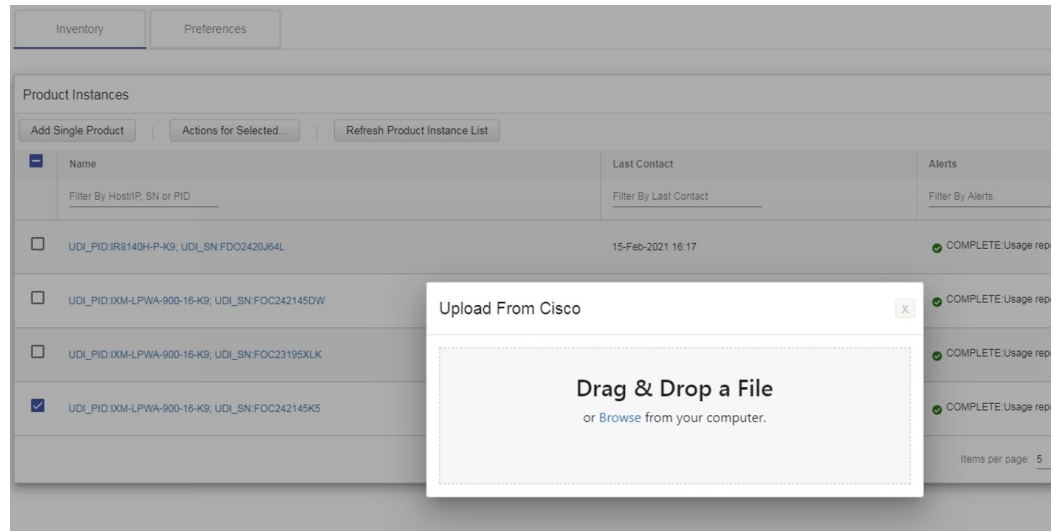
Step 5 Upload the tar file downloaded from CSLU to CSSM.



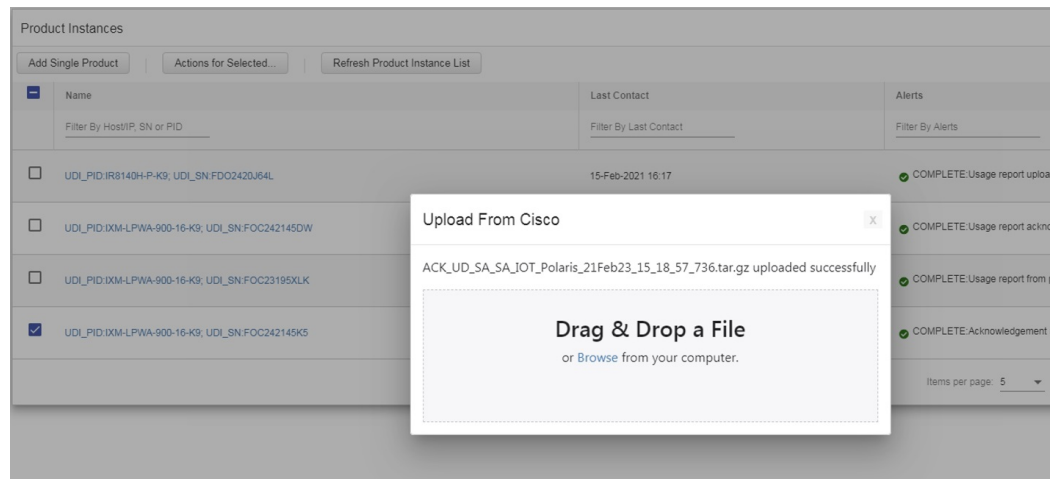
Step 6 Check the status on CSSM and download the file from CSSM.



Step 7 Upload the file downloaded file from CSSM on the CSLU.



Step 8 Upload the specified tar file.



Step 9 Verify the status on CSLU.

Name	Last Contact	Alerts
UDI_PID:IR8140H-P-K9; UDI_SN:FDO2420J64L	15-Feb-2021 16:17	COMPLETE: Usage report uploaded to CSSM
UDI_PID:IXM-LPWA-900-16-K9; UDI_SN:FOC242145DW	22-Feb-2021 18:25	COMPLETE: Usage report acknowledgement to product instance
UDI_PID:IXM-LPWA-900-16-K9; UDI_SN:FOC23195XLK	23-Feb-2021 14:59	COMPLETE: Usage report from product instance
UDI_PID:IXM-LPWA-900-16-K9; UDI_SN:FOC242145K5	23-Feb-2021 15:26	COMPLETE: Acknowledgement received from CSSM

Gateway#**show license usage**

```
License Authorization:
  Status: Not Applicable
```

```
LORAWAN_CPF (LORAWAN_CPF):
  Description: LORAWAN_CPF
  Count: 1
  Version: v01
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: LORAWAN_CPF
  Feature Description: LORAWAN_CPF
  Enforcement type: NOT ENFORCED
  License type: Invalid
Gateway#show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: http://172.27.164.116:8182/cslu/v1/pi
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Feb 24 2021 00:04:10 UTC
  Policy name: Test Policy
  Reporting ACK required: no (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 94 (Customer Policy)
    Reporting frequency (days): 100 (Customer Policy)
    Report on change (days): 100 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 100 (Customer Policy)
    Report on change (days): 100 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 204 (Customer Policy)
    Report on change (days): 100 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 100 (Customer Policy)
    Report on change (days): 100 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Feb 24 2021 00:04:10 UTC
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: Feb 23 2021 23:04:11 UTC
  Last report file write: <none>
```

```
Trust Code Installed: <none>  
Gateway#
```

Removing the Product Instance from CSSM

Procedure

- Step 1** Log in to the CSSM Web UI at <https://software.cisco.com> and click **Smart Software Licensing**. Log in using the username and password provided by Cisco.
 - Step 2** Click the **Inventory** tab.
 - Step 3** From the **Virtual Account** drop-down list, choose your virtual account.
 - Step 4** Click the **Product Instances** tab. The list of product instances that are available is displayed.
 - Step 5** Locate the required product instance from the product instances list. Optionally, you can enter a name or product type string in the search tab to locate the product instance.
 - Step 6** Click the required product instance to expand the same. The **Overview** window is displayed.
 - Step 7** From the **Actions** drop-down list, choose **Remove**. The **Remove Product Instance** window is displayed.
 - Step 8** In the **Reservation Return Code** field, enter the return code.
 - Step 9** Click **Remove Product Instance**. The license is returned to the license pool.
-



CHAPTER 12

Working with Configuration Files and Software Images

This chapter describes how to copy configuration files and how to download software images to a Cisco LoRaWAN Gateway.

- [Managing Files, on page 87](#)
- [Working with Configuration Files, on page 88](#)
- [Working with Software Images, on page 89](#)
- [USB Support, on page 91](#)
- [Configuring U-boot, on page 91](#)

Managing Files

You can manage the files system in USB or flash.

Copying Files

To copy a file from a source to a destination, use the **copy** *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

Network file system URLs include **ftp:** and **tftp:** and have these syntaxes:

- FTP—**ftp:**[[//username [:password]@location]/directory]/filename
- TFTP—**tftp:**[[//location]/directory]/filename

Local writable file systems include flash:

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

You can copy from remote to local, local to remote, and local to local. However, copying from remote to remote is not supported. During the copying process, one symbol ! printed on the screen indicates 100 blocks (512 bytes per block) transferred.

For specific examples of using the **copy** command with configuration files, see [Working with Configuration Files, on page 88](#).

To copy software images either by downloading a new version or by uploading the existing one, use the **archive download-sw** or the **archive upload-sw** privileged EXEC command. For more information, see [Working with Software Images, on page 89](#).

File Management Commands

You can use the commands in the following table to manage the file system.

Table 6: File Management Commands

Command	Description
cd	Change current directory.
copy	Copy from one file to another.
delete	Delete a file.
dir	List files on a filesystem.
format	Format a filesystem. Note Only flash can be formatted.
mkdir	Create a new directory.
more	Display the contents of a file.
pwd	Display the current working directory.
rename	Rename a file.

Working with Configuration Files

This section describes how to download or maintain configuration files.

You can copy (*download*) configuration files from a TFTP or FTP server to the running configuration or startup configuration of the Cisco LoRaWAN Gateway. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

The protocol you use depends on which type of server you are using. The FTP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP is built on and uses the TCP/IP stack, which is connection-oriented.

Configuration File Types and Location

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. For example, you might want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration but not save the configuration by using the **copy running-config startup-config** privileged EXEC command.

Displaying Configuration Files

To display the configuration of the device, use the **show [running-config | startup-config]** EXEC command.

Removing Configuration Files

To remove the configuration of the device, use the **no configuration** command in global configuration mode.

Reloading the System

To reboot the system, use the **reload** EXEC command.

The reload command will first check if the running configuration has been saved and prompt user if not. You can enter **yes** to save the configuration or **no** to skip this step. Then, you will be prompted to reload the system.

Working with Software Images

This section describes how to download software image files, which is stored as a *.tar.gz* file and contains the kernel and root file system.

You can download a Cisco LoRaWAN Gateway image file from a TFTP or FTP server, or from a USB device, to upgrade the Cisco LoRaWAN Gateway software.

Downloading an Image File



Note When upgrading from any version prior to Release 1.0.20 to Release 2.0, you must perform a factory upgrade for proper behavior.



Note To download the firmware from an USB device, you should first enable the USB support by executing the **usb enable** command.

Beginning in privileged EXEC mode, follow these steps to download a new image file.

Procedure

	Command or Action	Purpose
Step 1	—	<p>Log into the Cisco LoRaWAN Gateway through SSH or Console.</p> <p>Note The console port is 115.2kbs.</p>
Step 2	<pre>archive download-sw firmware {/factory /normal /uboot-only /uboot-normal /uboot-factory [/save-reload /force-reload]} path</pre>	<p>Download the image file to the Cisco LoRaWAN Gateway.</p> <ul style="list-style-type: none"> • /factory – Upgrade the firmware and delete user data. <p>Note Avoid using the /factory option with this command, because it erases everything and brings back to factory default.</p> <ul style="list-style-type: none"> • /factory - Upgrade the firmware and delete the user data • /normal - Upgrade the firmware and keep the user data • /uboot-only - Upgrade the uboot and keep the user data • /uboot-normal - Upgrade the uboot and firmware, and keep the user data • /uboot-factory - Upgrade the uboot and firmware, and delete the user data • /save-reload – Save the current configuration if required and reload the system after successful upgrade. • /force-reload – Do not save the current configuration and reload the system after successful upgrade. • path - The location of the file, which can be usb:, tftp, ftp, or flash:

What to do next**Example**

```
#archive download-sw firmware /normal /save-reload
tftp://172.27.74.9/corsica_i_k9-2.0.0015.tar.gz
```

USB Support

After the USB is plugged in:

- To enable USB, use the following command:

```
Router# usb enable
```

- To display the USB content, use the following command:

```
Router# dir usb:
```

- To disable USB, use the following command:

```
Router# usb disable
```

The USB partition should be formatted to FAT//ms-dos. Other file system types are not supported.

- For the formatting on Windows 7 and Windows 10, choose **Fat** (default) for the format option, and **4096 bytes** for the allocation size; or choose **Fat32** for the format option, and **2048 bytes** for the allocation size.
- For the formatting on MAC OS, choose **MS-Dos (FAT)**.



Note

To make sure that the USB is detected and usable on the IXM:

1. If any error is shown during the formatting, try to format it again or use another USB.
2. Do not unplug the USB directly after formatting. Use the **Eject** command provided by the host OS.

Configuring U-boot

U-boot is a universal bootloader for embedded boards based on PowerPC, ARM, MIPS and several other processors, which can be installed in a boot ROM and used to initialize and test the hardware or to download and run OS and application code.

Bootloader version requirement for the u-boot feature is “Bootloader Version: 20170515_cisco”.

Beginning in privileged EXEC mode, follow these steps to configure U-boot option.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.

	Command or Action	Purpose
Step 2	<code>uboot console {disable restore}</code>	<p>Configure U-boot console.</p> <ul style="list-style-type: none"> • disable - Disable U-boot console (and System console if SSH is enabled). <p>Note When IP SSH limit local is enabled on the IXM, the SSH access from outside is disabled for the unit. The uboot console disable option only checks whether SSH is enabled or not, and does not factor the IP SSH limit local option. If both commands are configured, it is possible that both the console connectivity and SSH connectivity are lost. In that case, the only way to access the unit is through container via Thing park.</p> <ul style="list-style-type: none"> • restore - Restore U-boot console (and System console if it was disabled).
Step 3	<code>uboot protection word</code>	<p>Enable U-boot password protection.</p> <ul style="list-style-type: none"> • <i>word</i> - 8 to 30 alphanumeric or special characters. <p>To disable U-boot password protection, use the no uboot protection command.</p>
Step 4	<code>exit</code>	Return to privileged EXEC mode.
Step 5	<p><code>show uboot console</code></p> <p>Example:</p> <p><code>show uboot protection</code></p>	<p>Show U-boot console status.</p> <p>Show U-boot password protection status.</p>



CHAPTER 13

FND Configuration for IXM

The Cisco IoT Field Network Director (IoT FND) is a software platform that manages a multi-service network and security infrastructure for IoT applications, such as smart grid applications, including Advanced Metering Infrastructure (AMI), Distribution Automation (DA), distributed intelligence, and substation automation. IoT FND is a scalable, highly-secure, modular, and open platform with an extensible architecture. IoT FND is a multi-vendor, multi-service, communications network management platform that enables network connectivity to an open ecosystem of power grid devices.

For more information about FND, see the FND documentation at the following URL:

<https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/tsd-products-support-series-home.html>.

IoT FND supports the following configurations for the Cisco Wireless Gateway for LoRaWAN:

- Firmware upgrade
- Hardware monitoring and events report
- IP networking configuration and operations (for example, IP address and IPsec)
- Zero Touch provisioning, including initial installation of the Thingpark LRR software

This chapter contains the following topics.

- [Preparing FND for IXM ZTD, on page 93](#)
- [IXM modem Firmware Update, on page 103](#)
- [Configuring IGMA, on page 105](#)
- [Troubleshooting, on page 106](#)

Preparing FND for IXM ZTD

Follow these steps to prepare FND for IXM ZTD:

Procedure

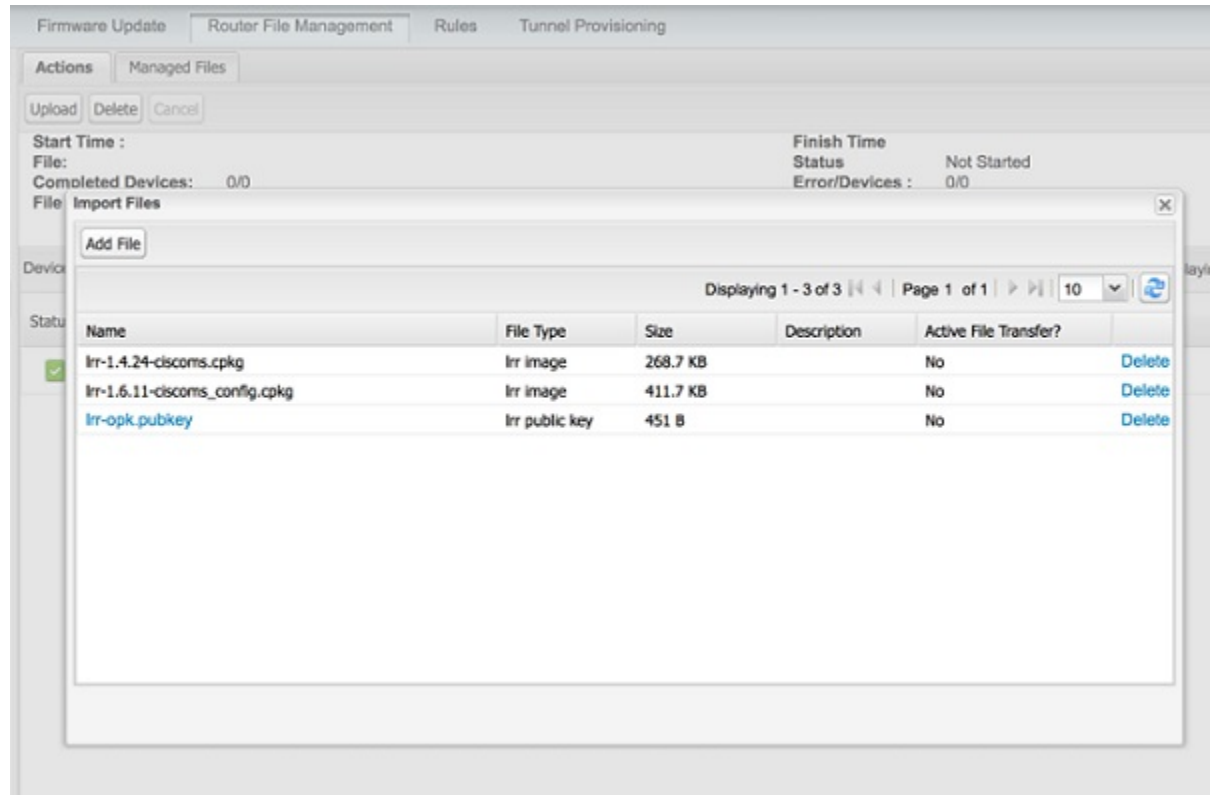
- Step 1** If you are using PSK authentication for tunneling, add the **userPropertyTypes.xml** file to the FND server under **/opt/cgms/server/cgms/conf**. Restart the FND service after adding the following. If you are using RSA, ignore this step.

```

<?xml version="1.0" encoding="UTF-8"?>
<cgms xmlns="http://www.w3schools.com"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.w3schools.com propertyTypes.xsd">
  <propertyTypes kind="lorawan">
    <!--Psk Properties -->
    <propertyType>
      <name>pskUsername</name>
      <displayName>XAUTH Username</displayName>
      <description>Username for PSK IPsec XAUTH</description>
    </propertyType>
    <propertyType>
      <name>pskPassword</name>
      <issecure>1</issecure>
      <displayName>XAUTH Password</displayName>
      <description>Password for PSK IPsec XAUTH</description>
    </propertyType>
    <propertyType>
      <name>pskClientConfGrp</name>
      <displayName>PSK Client Configuration Group</displayName>
      <description>PSK Client Configuration Group</description>
    </propertyType>
    <propertyType>
      <name>psk</name>
      <issecure>1</issecure>
      <displayName>Pre Shared Key</displayName>
      <description>Pre Shared Key</description>
    </propertyType>
  </propertyTypes>
</cgms>

```

Step 2 Add the Activity LRR and public key to FND by clicking the **import** button on the File Management page.



Step 3 Update the Tunnel Configuration group with the following parameters and save the changes. The following figure shows an example for PSK.

© 2012-2017 Cisco Systems, Inc. All Rights Reserved. (version 4.0.0-299)

Step 4 Update the Device Configuration group with the following parameters and save the changes. The following figure shows a sample configuration.

The screenshot shows the Cisco IoT Field Network Director (FND) configuration interface. The top navigation bar includes the Cisco logo and the text "IoT FIELD NETWORK DIRECTOR". Below this, the breadcrumb "CONFIG > DEVICE CONFIGURATION" is visible. Two buttons, "Assign Devices to Group" and "Change Device Properties", are located at the top of the main content area. The left sidebar displays a tree view of device configuration groups, including "Default-esr (0)", "Default-ir800 (10,000)", "Sdfasdf (1)", "Ss (1)", "Test (1)", "ENDPOINT" (expanded), "Default-act (0)", "Default-bact (0)", "Default-cam (0)", "Default-cgmesh (76,592)", "Default-ir500 (0)", "GATEWAY" (expanded), "Asd (0)", "Default-lorawan (0)", and "Ssaa (0)". The "Default-lorawan (0)" group is selected and highlighted. The main content area shows the configuration for the "default-lorawan" group, with tabs for "Group Members", "Edit Configuration Template", and "Push Configuration". The "Edit Configuration Template" tab is active, displaying the current configuration revision #20, last saved on 2017-07-28 14:49. The configuration text in the editor is as follows:

```
igma profile iot-fnd-metric
interval 2
exit
```

At the bottom of the interface, a copyright notice reads: "© 2012-2017 Cisco Systems, Inc. All Rights Reserved. (version 4.0.0-299)".

Update the Device Configuration Group properties with the following parameters and save the changes.

CONFIG > DEVICE CONFIGURATION

Assign Devices to Group Change Device Properties **default-lorawan**

Configuration Groups + Group Members Edit Configuration Template Push Configuration **Group Properties**

ROUTER

- Default-c800 (0)
- Default-cgr1000 (0)
- Default-esr (0)
- Default-ir800 (1)

ENDPOINT

- Default-act (0)
- Default-bact (0)
- Default-cam (0)
- Default-cgmesh (0)
- Default-ir500 (0)


GATEWAY

- Default-lorawan (0)

Mark Gateway Down After (secs): 5400

LRR Image: lrr-1.6.11-ciscoms_co

LRR Public Key: lrr-opk.pubkey



The Tunnel Provisioning settings page will have the FND common name populated as the following figure shows.

ADMIN > SYSTEM MANAGEMENT > PROVISIONING SETTINGS

Provisioning Process

IoT-FND URL:
Field Area Router uses this URL to register with IoT-FND after the tunnel is configured

DHCPv6 Proxy Client

Server Address:
IPv6 address to send (or multicast) DHCPv6 messages to (can be multiple addresses, separated by commas)

Server Port:
Port to send (or multicast) DHCPv6 messages to


Client Listen Address:
IPv6 address to bind to, for sending and receiving DHCPv6 messages (can be multiple addresses, separated by commas)

DHCPv4 Proxy Client

Server Address:
IPv4 address to send (or broadcast) DHCPv4 messages to (can be multiple addresses, separated by commas)

Server Port:
Port to send (or broadcast) DHCPv4 messages to

Client Listen Address:
IPv4 address to bind to, for sending and receiving DHCPv4 messages (can be multiple addresses, separated by commas)



- Step 5** Make sure you have obtained certificates from the CA (the same ones used to issue certs for FND). Execute the **show ipsec certs** command to verify. Make sure the firewall allows ports 9120, 9121, 9122, and all the SSH, telnet, and DHCP ports. Make sure the TPS name is pingable. Then execute the **copy running express-setup-config** command.

```

Hostname IXM
!
ip domain lookup
ip domain name cisco.com
!
ip name-server 55.55.0.15
!
interface FastEthernet 0/1
description interface
ip address 4.4.4.2 255.255.255.0
exit
!
ip default-gateway 4.4.4.1
!
ntp server ip 55.55.0.1
!
clock timezone America/Los_Angeles
!
igma profile iot-fnd-tunnel

```

```

active
add-command show fpga
interval 5
url https://ps.sgbu.cisco.com:9120/igma/tunnel
exit

ipsec cert scep https://55.55.0.15/csertsrv/msecp.dll us ca mil cisco iot test true ndes
true 2048

```

You need to add the HER configuration manually, for example, the tunnel crypto profiles and transform sets. The following easyVPN example uses PSK as authentication.

```

username cisco password 0 cisco

crypto isakmp policy 1
  encr aes 256
  hash sha256
  authentication pre-share
  group 19
crypto isakmp keepalive 10
!
crypto isakmp client configuration group 19
  key cisco
  domain cisco.com
  pool POOL
  acl split
  save-password
  netmask 255.255.255.128
crypto isakmp profile test
  match identity group 19
  client authentication list AUTH
  isakmp authorization list NET
  client configuration address respond
  client configuration group 19
  virtual-template 1
!
!
crypto ipsec transform-set test esp-aes 256 esp-sha256-hmac
mode tunnel
!
!
crypto ipsec profile ipsecprof
  set security-association lifetime kilobytes disable
  set transform-set test
  set isakmp-profile test

interface Virtual-Templatel type tunnel
  tunnel protection ipsec profile ipsecprof
  ip unnumbered GigabitEthernet0/1
  tunnel source GigabitEthernet0/1
  tunnel mode ipsec ipv4

ip local pool POOL 20.20.0.0 20.20.255.255

```

- Step 6** Encrypt the PSK passwords using the signature-tool under **/opt/cgms-tools/bin**. Add the encrypted passwords in the CSV file and prepare it for upload. Add the modem to FND as the following sample CSV shows. Add ISR4K using the following CSV.

```

eid,netconfUsername,netconfPassword,ip,deviceType,lat,domaIn,lng,ipsecTunnelDestAddr,tunnelHerEid,
pskUsername,pskPassword,pskClientConfGrp,psk
IXM-LPWA-900-16-K9+FOC21028RAK,,,,,lorawan,10,root,10,4.4.4.1,C3900-SPE250/K9+FOC172417YT,cisco,
ki80jE05Pr+krJTtUooUMD0Goqm0Aznc2JObiUUr4ismXyP0uXs8JRuSPOfojMDavGIHi08unUUJm3zdxv0LP8b6fe5G+
oshy76A6IqX1jk7ymSFOaVPQBT8fUS6onjsuStHiLERS0B6Brn2gRx/KpQMk9IdYQMOSsHh4khvtxbqBZy6j++pIjeG4+
dPz/v52DmJR+DOrE7ZQpfvS9PSHkJoaqC2o6PrKN5YZ50G9+Tm+diPmbyv/PdHKtXn1ny3qBAdbfDwOj1A+NtJP1d3/
06vq6WhHsgujYwMJWs7Cuu3rR0/FVHF/5wFarakJsfo/zd69EpzrI8Hsic/QmMzA==,19,
ki80jE05Pr+krJTtUooUMD0Goqm0Aznc2JObiUUr4ismXyP0uXs8JRuSPOfojMDavGIHi08unUUJm3zdxv0LP8b6fe5G+
oshy76A6IqX1jk7ymSFOaVPQBT8fUS6onjsuStHiLERS0B6Brn2gRx/KpQMk9IdYQMOSsHh4khvtxbqBZy6j++pIjeG4+
dPz/v52DmJR+DOrE7ZQpfvS9PSHkJoaqC2o6PrKN5YZ50G9+Tm+diPmbyv/PdHKtXn1ny3qBAdbfDwOj1A+NtJP1d3/
06vq6WhHsgujYwMJWs7Cuu3rR0/FVHF/5wFarakJsfo/zd69EpzrI8Hsic/QmMzA==
C3900-SPE250/K9+FOC172417YT,nms,sgbu123!,55.55.0.18,isr3900,,,,,,,,,

```

Step 7 Once the Modem is registered, the IXM will show as up in the FND. Please check the following events if there are issues during ZTD.

2017-08-21 15:29:45:886	Registration Success	INFO	Registration of LoRaWAN Gateway successful.LoRaWAN Gateway Registration Success for EID [00M-LPWA-900-16-K9-FOC21028RAK].
2017-08-21 15:29:45:846	Up	INFO	LoRaWAN Gateway is up
2017-08-21 15:29:03:220	Registration Request	INFO	Registration request from LoRaWAN Gateway.LoRaWAN Gateway Registration Request from EID [IXM-LPWA-900-16-K9-FOC21028RAK].
2017-08-21 15:24:40:008	Down	MAJOR	LoRaWAN Gateway is down
2017-08-21 15:24:14:692	Tunnel Provisioning Success	INFO	Tunnel provisioning successful.
2017-08-21 15:23:27:798	Tunnel Provisioning Request	INFO	Tunnel provisioning request from LoRaWAN Gateway.

Step 8 Detailed IXM modem information can be viewed by clicking on the modem link.

<< Back **IXM-LPWA-900-16-K9+FOC21028RAK**

Show on Map Ping Traceroute Refresh Metrics

Device Info Events Config Properties Running Config

Inventory

Name	IXM-LPWA-900-16-K9+FOC21028RAK
EID	IXM-LPWA-900-16-K9+FOC21028RAK
Domain	test-lora
Device Category	IOTGATEWAY
Device Type	LORAWAN
Status	up
IP Address	20.20.0.37
Operating Mode	Standalone
IPv6 Address	unknown
First Heard	2017-07-28 15:03
Last Heard	2017-08-07 12:13
Last Property Heard	2017-08-07 12:13
Last Metric Heard	2017-08-07 12:13
Last Reboot Time	unknown
Model Number	IXM-LPWA-900-16-K9
Serial Number	FOC21028RAK
Firmware Version	2.0.01.rc30
Agent Version	N-A
Boot Loader Version	20160830_cisco

Gateway Health

Uptime	5d 23hr 42min
Door Status	unknown
Modem Temperature	35.5 Celsius
Load Average	1min 0.19 5min 0.20 15min 0.22

Packet Forwarder Information

Packet Forwarder Status	Stopped
Packet Forwarder Firmware	Installed
Packet Forwarder Version	1.4.24
Packet Forwarder Public Key	Installed
Packet Forwarder Id	/tmp/rtr_id.sh line 2 /etc/profile No such file or directory

Gateway Properties

Location	10.0, 10.0
GPS Info Time	unknown
RF Chip ID	LSB = 0x26790912 MSB = 0x00f1400e
Tx Power Calibration	<NA,NA,NA,53,34,108,99,91,82,74,66,56,47,38,29,20>NA,NA,NA,52,33,107,98,90,81,73,65,55,46,37,28,19>
Antenna 1 RSSI Offset(dBm)	-205.00
Antenna 2 RSSI Offset(dBm)	-204.00
AES Key	unknown

Network Interfaces

Interface	Admin Status	Oper. Status	IP Address	Physical Address	Tx Speed (bps)	Tx Drops (bps)	Rx Speed (bps)
FastEthernet 0/1	up						

Load Average

● Load Average

Modem Temperature

● Modem Temperature

Step 9

If configuration update is required or a new modem is added to the router, follow the same procedure from Step 1. But in this case you invoke a configuration push.

default-ir800

Group Members Edit Configuration Template Edit AP Configuration Template **Push Configuration**

Push Router Configuration ▼ Start

Pushing Config Version: 77 **Status:** Finished
Pushed Data: Config Push with template revision 48
Start Time: never **Finish Time:** never
Completed Devices: 0/2 **Error Devices:** 0/2

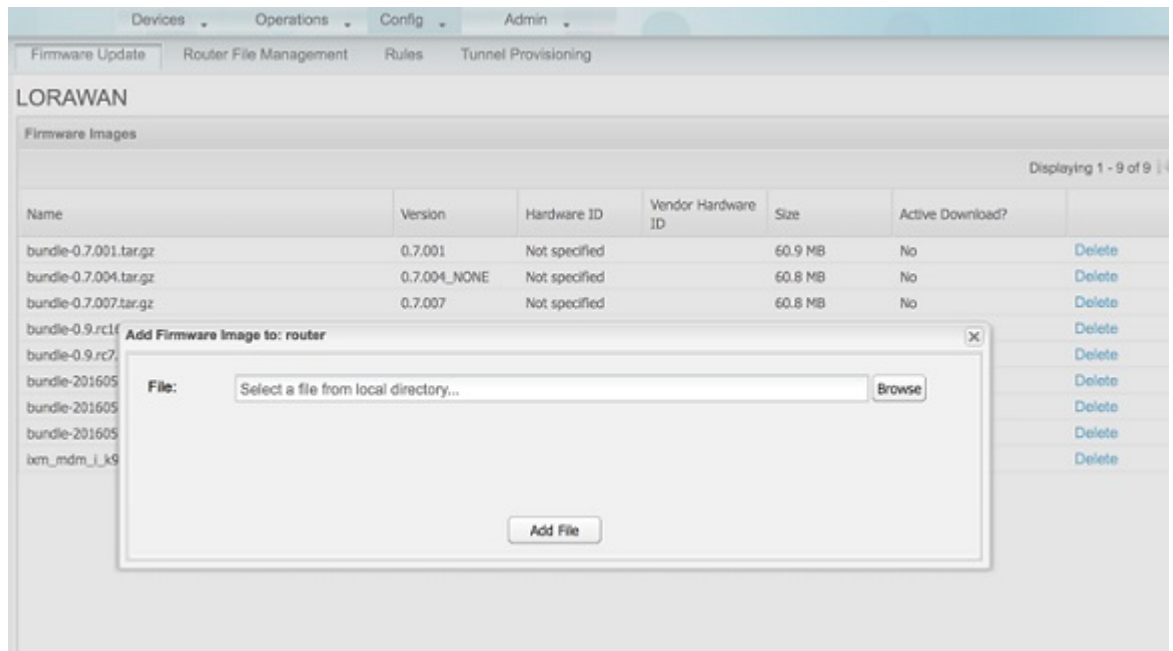
Device Status

Name	Push Status	IP Address	Error Message
IR809G-LTE-GA-K9+JMX1915X01Q	NOT_STARTED		
IR809G-LTE-VZ-K9+JMX2023X031	NOT_STARTED	55.55.0.81	

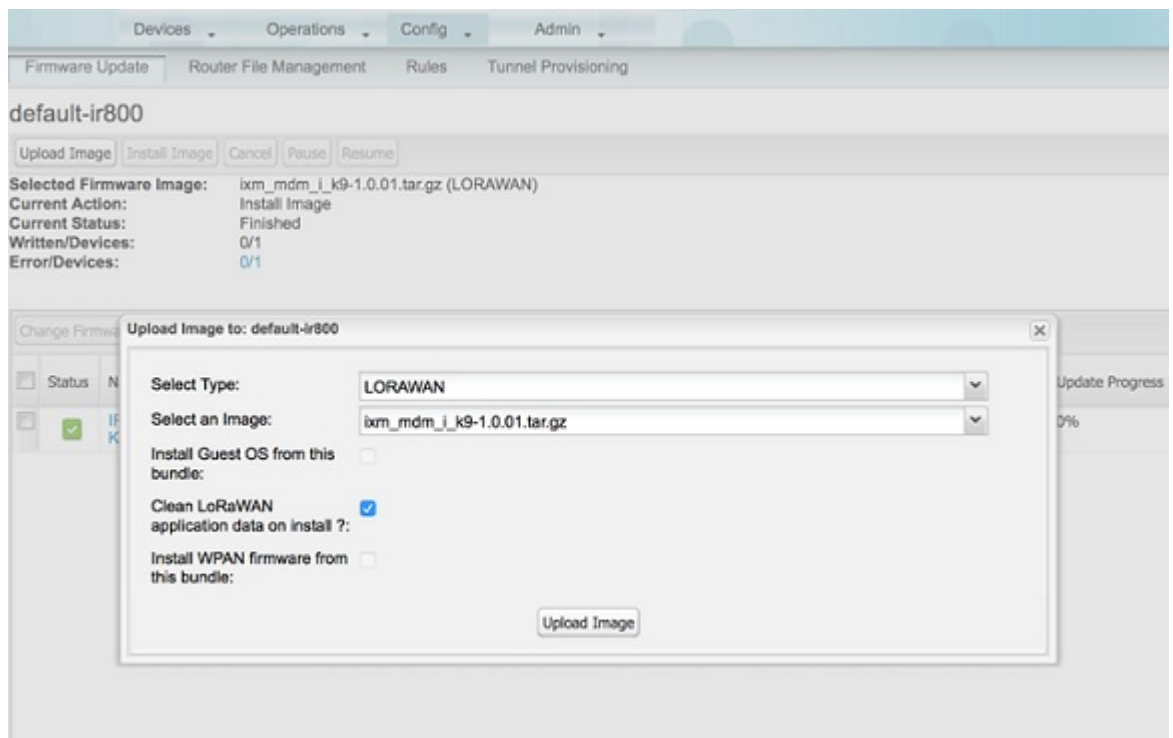
IXM modem Firmware Update

Procedure

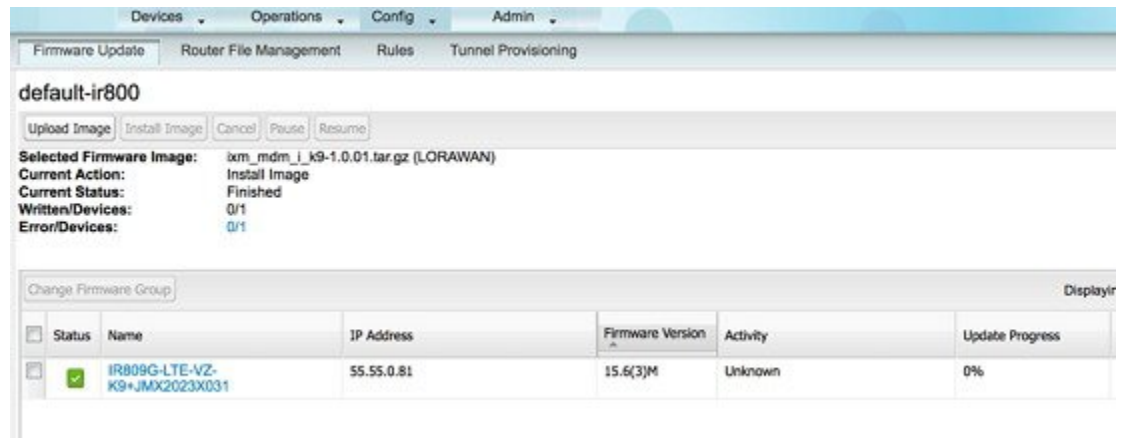
- Step 1** Load the firmware file to FND.



Step 2 Push the firmware to the IXM modem. If you want to erase the LRR or pubkey, select the clean install option as shown below.



Step 3 When upload is complete, install the image by clicking the **install** button.



Configuring IGMA

IoT Gateway Management Agent (IGMA) is for management in conjunction with FND.

The IGMA configuration commands are as following:

- To start IGMA, use the following command:

```
IXM#igma start
IGMA Starting...
```

- To configure IGMA, use the following command:

```
IXM#configure terminal
IXM(config)#igma
    event          IGMA Event Configuration
    local-trustpoint Set IGMA local-trustpoint configuration
    profile        IGMA Profile Configuration
    secure         Set igma secure mode
```

- To check the status of IGMA:

```
IXM#request shell container-console
Enter System Password:

Connected to tty 0
Type <Ctrl+a q> to exit the console, <Ctrl+a Ctrl+a> to enter Ctrl+a
itself

bash-3.2#
bash-3.2#
bash-3.2#
bash-3.2# ps -ef | grep igma
7151 root      0:00 grep igma
bash-3.2#
```

- Regarding ports, trustpoints and security, Apache web server should be running with the port 443.

Also the following CLI will activate igma using SUDI:

```
igma local-trustpoint sudi
```

- Configuration in combination with CPF

```
Sample Configuration along with CPF
!
igma secure enable
!
igma event destination https://us-int.ciscoiot.com 5683
!
igma profile iot-fnd-metric
active
add-command show common-packet-forwarder info
add-command show common-packet-forwarder status
add-command show fpga
add-command show inventory
add-command show ip interface FastEthernet 0/1
add-command show ipsec status info
add-command show led status
add-command show platform status
add-command show radio
add-command show version
interval 15
url https://us-int.ciscoiot.com/cgna/igma/metric
exit

igma profile iot-fnd-register
add-command show fpga
add-command show inventory
add-command show ip interface FastEthernet 0/1
add-command show ipsec status info
add-command show platform status
add-command show radio
add-command show version
interval 5
url https://us-int.ciscoiot.com:443/cgna/igma/register
exit
!
common-packet-forwarder profile
ipaddr us-int.ciscoiot.com port 3001
antenna 1 omni gain 1.5 loss 0.0
gatewayid 1000000000000031
auth-mode none
country UnitedStates
cpf enable
exit
!
igma local-trustpoint sudi
```

Troubleshooting

Enable the following debug categories on FND before troubleshooting:

ADMIN > SYSTEM MANAGEMENT > LOGGING

Download Logs **Log Level Settings**

Change Log Level to

<input type="checkbox"/>	Category ▲	Log Level
<input type="checkbox"/>	Dashboard	Informational
<input type="checkbox"/>	Data Aggregation	Informational
<input type="checkbox"/>	Data Retention	Informational
<input type="checkbox"/>	Device Actions	Informational
<input type="checkbox"/>	Filters	Informational
<input type="checkbox"/>	Firmware	Informational
<input type="checkbox"/>	GOS App Management	Informational
<input type="checkbox"/>	Group Management	Informational
<input checked="" type="checkbox"/>	IGMA	Informational

- TPS does not have any messages from IXM.
 - Check if the certs are installed correctly on IXM and from the same CA as the FND certs.
 - Make sure the IGMA profile is pointing to the correct tunnel profile and the proxy name resolution is correct.
 - Make sure the proxy can be pinged.
 - Make sure the IGMA profile has the correct commands.
- FND does not have any messages from the IXM.
 - Check if the tunnel network is reachable from the FND cluster.
 - Make sure the IGMA profile is pointing to the correct FND profile and the name resolution is correct.
 - Make sure the FND can be pinged.
- Tunnel provisioning request failed.
 - Check the FND tunnel template for command accuracy.
- FND Registration failed.
 - Check the FND configuration template for command accuracy.

- Tunnel issues (for example, flapping or disconnect).