Cisco Spaces: IoT Service Configuration Guide (Wired)

First Published: 2020-08-31

Last Modified: 2023-04-04

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 NONINFRINGEMENT 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)

© 2020–2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

PART I **Prerequisites** 5

CHAPTER 1 **Overview** 1

Overview of IoT Service (Wired) 1

Prerequisites for Cisco Spaces: IoT Service (Wired) 3

Design Prerequisites 4

Compatibility Matrix for IoT Service (Wired) 6

Open Ports for IoT service (wired) 7

CHAPTER 2 **Getting Started** 9

Activate IoT Service (Wired) 9

PART II **Configuration** 17

CHAPTER 3 **Switch as a Gateway** 19

Switch as a Gateway 19

Configuring a Switch as a Wired Gateway 19

Uninstall, or Upgrade a Wired Application on a Switch 22

CHAPTER 4 **Sensors and Wired Devices** 25

Viewing Wired Sensors or Devices on IoT Service 25

Configure a Smart PDU 26

Configure a Hella Camera 31

PART III **Device Management** 35

CHAPTER 5 **Device Management** 37

Dashboard View of Devices 37

Categorizing Devices into Groups 37

PART IV **Troubleshooting** 41

CHAPTER 6 **Switch** 43

Switch 43

What TDL subscriptions are created 43

How do I verify the TDL subscriptions are created and valid? 44

What is the TDL status? 44

What commands are run on the switch? 45

CHAPTER 7 **Troubleshooting IoT service (wired)** 47

Connector 47

What are the metrics available in connector for IoT service (wired)? 47

CHAPTER 8 **IoX Application** 49

IoX Application 49

How do I verify the IoX Application is running on the switch? 49

How do I start an interactive shell session for the IoX Application? 49

How can I see the logs for the IOx application? 49

How do I monitor metrics in the IoX Application? 50

What files exist in the IoX Application? 52

How do I verify that the IoX Application is receiving span session data? 52

Why am I not seeing span session data in the IoX Application? 53

CHAPTER 9 **802.1x** 55

802.1x 55

How to enable 802.1x port-based authentication on the switch? 55

How to enable 802.1x port-based authentication on the switch interface? 56

How to configure the switch for RADIUS-server communication? 56

How to view the current 802.1x status for a switch interface? 56

PART I

Prerequisites

- Overview, on page 1
- Getting Started, on page 9

CHAPTER 1

Overview

Note **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

- Overview of IoT Service (Wired) , on page 1
- Prerequisites for Cisco Spaces: IoT Service (Wired) , on page 3
- Compatibility Matrix for IoT Service (Wired) , on page 6
- Open Ports for IoT service (wired), on page 7

Overview of IoT Service (Wired)

Cisco Spaces enables end-to-end wired and wireless IoT device management, monitoring, and business outcome delivery at an enterprise scale using the following:

- Cisco Spaces: IoT Service
- Cisco Spaces: IoT Device Marketplace
- Cisco Spaces App Center

In addition to serving as the management hub for wireless IoT devices, IoT Service can now integrate with Cisco Catalyst 9300 and 9400 Series Switches from Release 17.3.3 or later to receive IoT service (wired) data from sensors, such as:

- Passive infrared (PIR) sensors for presence detection
- Temperature and humidity sensors
- Smart lighting devices
- Smart shades
- Ethernet port status
- Smart power distribution unit (PDU)

- Hella Camera

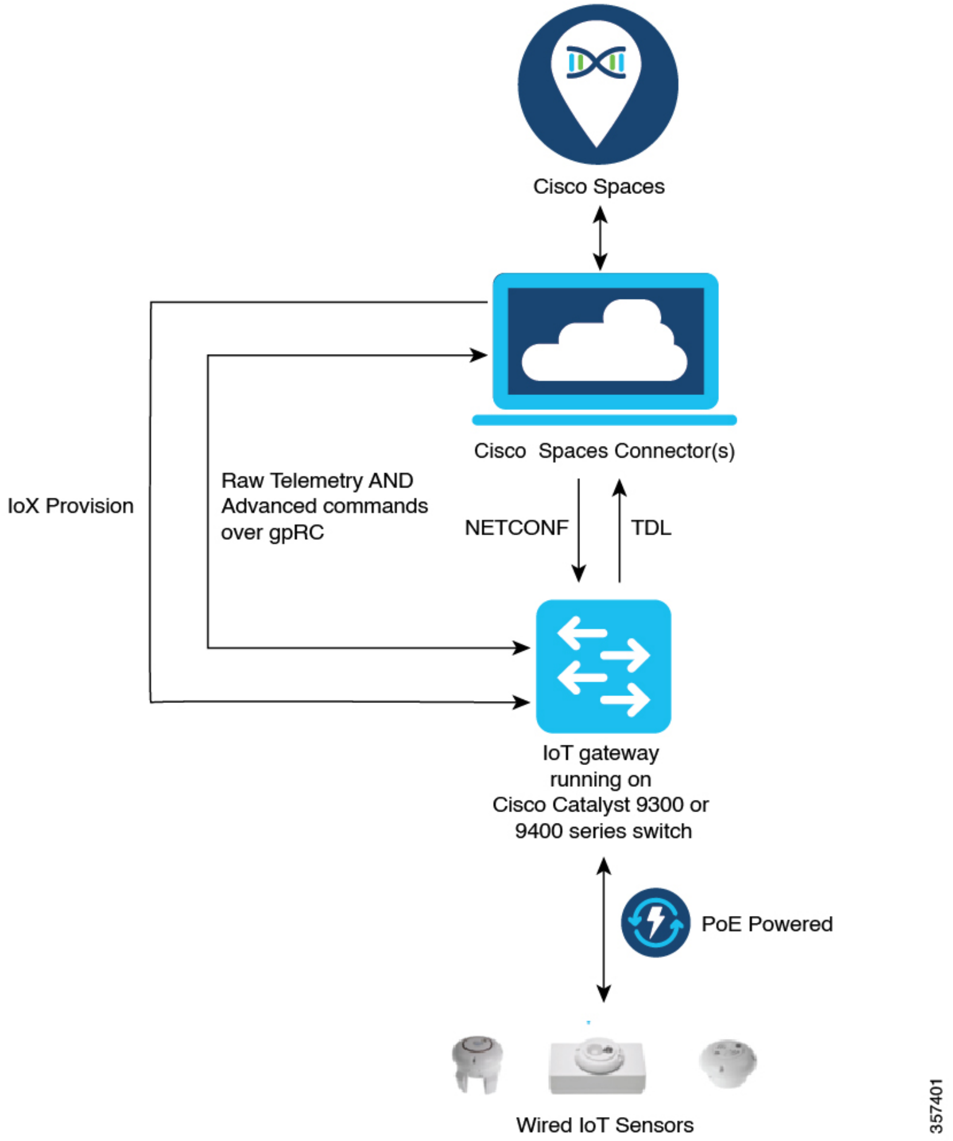
Integrating IoT service (wired) with the Cisco Catalyst 9300 and 9400 Series Switches series platform requires the following:

- Cisco Spaces: Connector
- A IoT service (wired) gateway deployed and managed by Cisco Spaces

Cisco Catalyst 9300 and 9400 Series Switches can send critical IoT data to IoT service (wired). IoT service (wired) can then transmit the information to:

- Business outcome applications on Cisco Spaces
- Cisco Spaces App Center using the Firehose API

Figure 1: Data flow in IoT Service (Wired)



Prerequisites for Cisco Spaces: IoT Service (Wired)

The following are the necessary prerequisites to get you started with Cisco Spaces: IoT Service (Wired):

- Install Cisco Spaces: Connector in your network.
- Configure a network with one or more Cisco Catalyst 9300 and 9400 Series Switches, Release 17.3.3 or later.
- Switches must have **Cisco DNA Advantage** subscription.
- Deploy wired sensors in your network. See Compatibility Matrix for IoT Service (Wired) , on page 6.

- Ensure that Cisco Spaces is configured with maps either from Cisco Prime Infrastructure or Cisco DNA Center.
- Configure AAA on aCisco Catalyst 9300 Series Switches or a Cisco Catalyst 9400 Series Switches before adding it to Cisco Spaces by running these commands in:
    - **aaa new-model**
    - **aaa authentication login default local**
    - **aaa authorization exec default local**

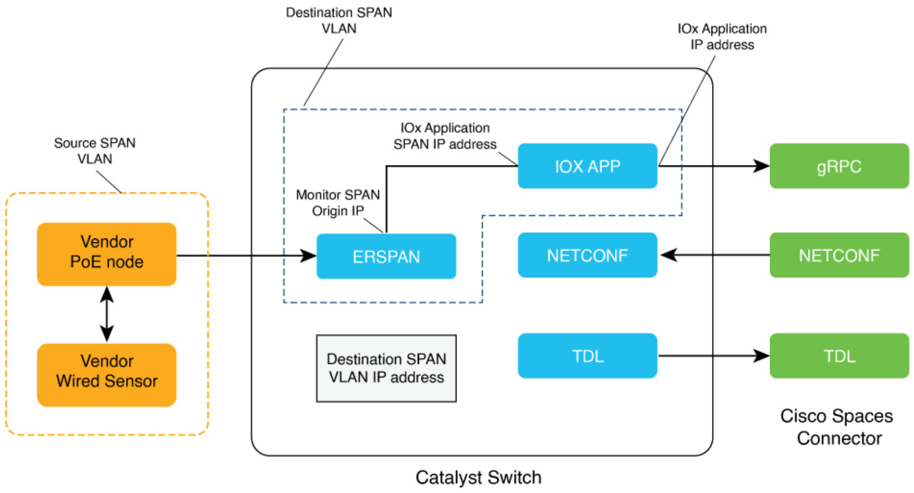
  For more information, see **Command Reference, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9300 Switches)**
- Perform NTP synchronization across wireless controllers, Cisco Spaces: Connectors, and switches in the network.
- Enable NETCONF on Cisco Catalyst 9300 or 9400 Series Switches on port 830, along with permission to use NETCONF.

Note Cisco Catalyst 9300 and 9400 Series Switches require a local privilege level 15 user to use NETCONF. Additionally, the user must be a password-protected local user, because public-key authentication is not supported.

Design Prerequisites

Ensure you have the following information handy before proceeding:

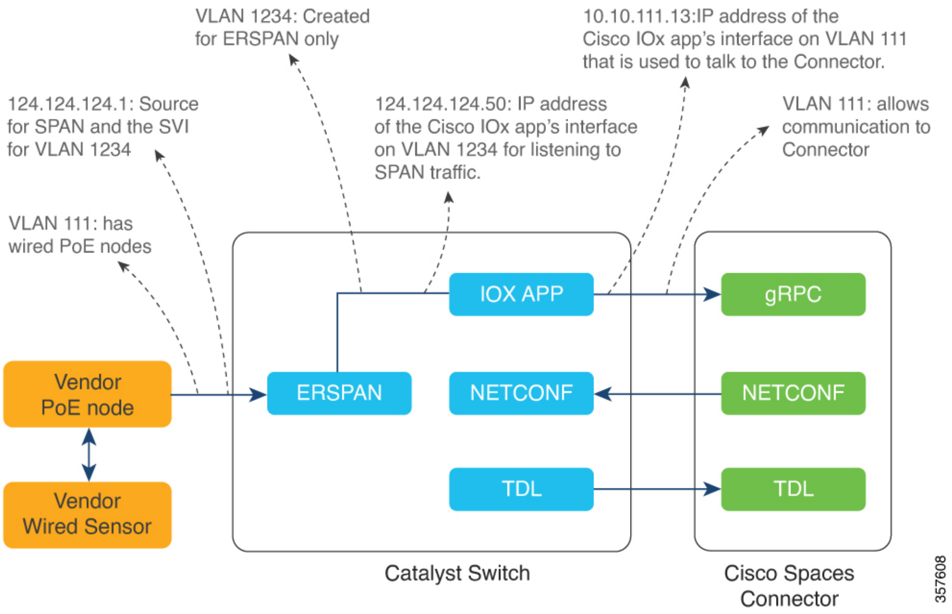
Figure 2: Design Prerequisites



- **Destination SPAN VLAN**: The VLAN used to send Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic from Power over Ethernet (PoE) nodes to Cisco IOx App. You can use an existing VLAN or create a new one. This VLAN can also be local to the switch.

- **Destination SPAN VLAN IP address**: This is the Switched Virtual Interface (SVI) or the IP address of the destination VLAN that can be used to route traffic. If you are using an existing VLAN, you can provide the same IP address. We recommend that you create a new VLAN so that you can keep the ERSPAN traffic local without impacting the existing configuration. Note that this VLAN is used only within the switch for the SPAN traffic.
- **Source SPAN VLAN list:** List of VLANs to which the wired devices are connected. The traffic on these VLANs are monitored. If the wired devices are connected to multiple VLANs, enter the VLANs separated by a comma.
- **Monitor SPAN origin IP address**: This is the source IP address of the monitor session. This can be from the SPAN VLAN. This can also be the same as the destination VLAN IP address.
- **IoX application Span IP Address**
- **Application Cisco Spaces Connector VLAN**: This is the VLAN on which the connector is reachable (for management or data). You can configure the Cisco IOx App's second interface to use this VLAN to send traffic to the connector. This VLAN can be the same as the wired PoE node VLAN. The connector must be permitted to accept communications from the Cisco IOx application.
- **DHCP**: When enabled, DHCP allocates an IP address from the **Application DNA Spaces Connector VLAN** to the Cisco IOx App's second interface.
- **IoX application IP address**: This is the IP address that you must manually configure for the Cisco IOx App's second interface, and is used to communicate with the Connector. This is not required if you select DHCP.
- **IoX application netmask**: This is the IP subnet mask that you must manually configure for the Cisco IOx App's second interface, and is used to communicate with the connector. This is not required if you select DHCP.
- **IoX application gateway address**: This is the IP address that you must manually configure for the Cisco IOx App's second interface, and is used to communicate with the connector. This is not required if you select DHCP.

Figure 3: Sample Configuration


VLAN 1234: Created for ERSPAN only
10.10.111.13:IP address of the Cisco IOx app's interface on VLAN 111 that is used to talk to the Connector.
124.124.124.1: Source for SPAN and the SVI for VLAN 1234
124.124.124.50: IP address of the Cisco IOx app's interface on VLAN 1234 for listening to SPAN traffic.
VLAN 111: allows communication to Connector
VLAN 111: has wired PoE nodes
IOX APP
gRPC
Vendor PoE node
ERSPAN
NETCONF
NETCONF
Vendor Wired Sensor
TDL
TDL
Catalyst Switch
Cisco Spaces Connector
357608

Compatibility Matrix for IoT Service (Wired)

Application Name	Support for Cisco Spaces: IoT Service
Cisco Spaces: Connector Docker	2.0.455 and later
Cisco Spaces: Connector OVA	2.3 and later
Cisco Prime Infrastructure	Cisco Prime Infrastructure Release 3.8 MR1
Cisco DNA Center (for map import)	Cisco DNA Center Release 2.1.1 and later
Switch as a gateway	• Cisco Catalyst 9300 Series Switches • Cisco Catalyst 9400 Series Switches Cisco IOS XE Amsterdam 17.3.x and later releases.
Wired Application Version	1.0.46 and later

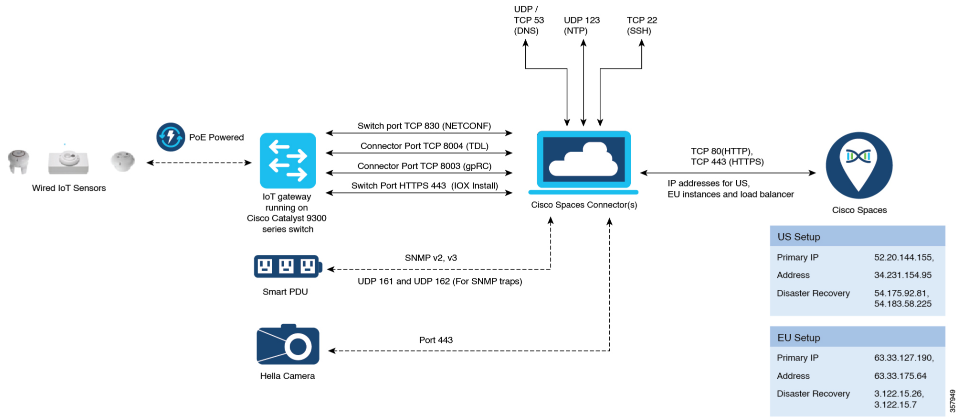
IoT service (wired) is not supported with Cisco Spaces tenants or deployments leveraging the following configurations:

- Connecting directly with controller
- CMX Tethering

Open Ports for IoT service (wired)

This section lists the connector ports that must be open for the proper functioning of each service or protocol.

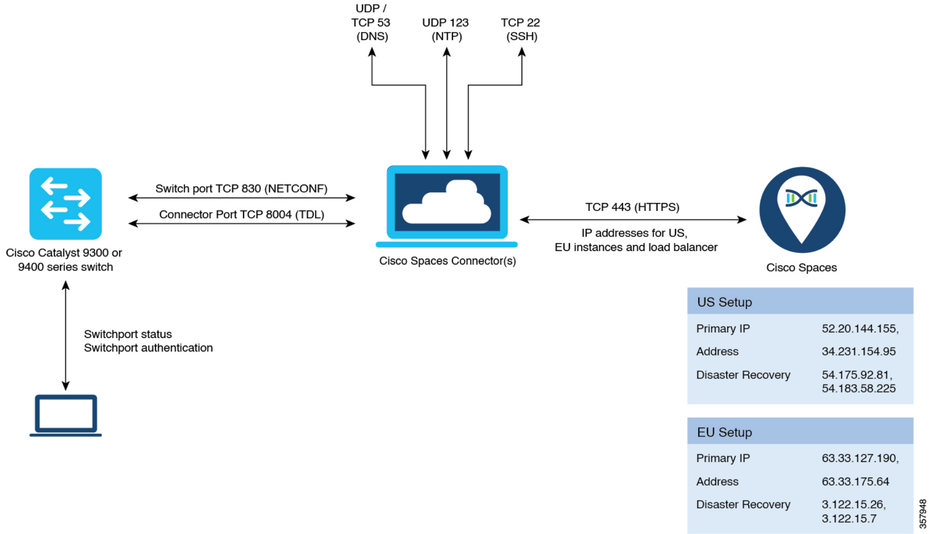
Figure 4: Open Ports for IoT Service (Wired) with the IoT Gateway


UDP / TCP 53 (DNS)
UDP 123 (NTP)
TCP 22 (SSH)
PoE Powered
Wired IoT Sensors
IoT gateway running on Cisco Catalyst 9300 series switch
Switch port TCP 830 (NETCONF)
Connector Port TCP 8004 (TDL)
Connector Port TCP 8003 (gpRC)
Switch Port HTTPS 443 (IOX Install)
Cisco Spaces Connector(s)
TCP 80(HTTP), TCP 443 (HTTPS)
IP addresses for US, EU instances and load balancer
Cisco Spaces
SNMP v2, v3
UDP 161 and UDP 162 (For SNMP traps)
Smart PDU
Port 443
Hella Camera
357949

US Setup	
Primary IP Address	52.20.144.155, 34.231.154.95
Disaster Recovery	54.175.92.81, 54.183.58.225

EU Setup	
Primary IP Address	63.33.127.190, 63.33.175.64
Disaster Recovery	3.122.15.26, 3.122.15.7

Open Ports for IoT Service (Wired) without the IoT Gateway


UDP / TCP 53 (DNS)
UDP 123 (NTP)
TCP 22 (SSH)
Cisco Catalyst 9300 or 9400 series switch
Switch port TCP 830 (NETCONF)
Connector Port TCP 8004 (TDL)
Cisco Spaces Connector(s)
TCP 443 (HTTPS)
IP addresses for US, EU instances and load balancer
Cisco Spaces
Switchport status
Switchport authentication
357948

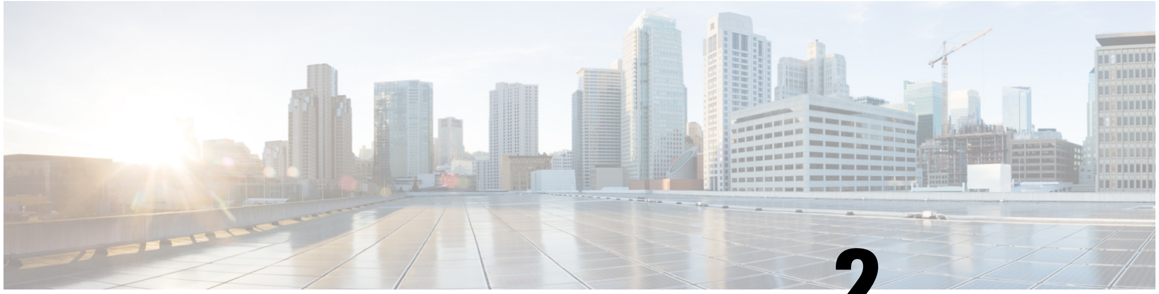
US Setup	
Primary IP Address	52.20.144.155, 34.231.154.95
Disaster Recovery	54.175.92.81, 54.183.58.225

EU Setup	
Primary IP Address	63.33.127.190, 63.33.175.64
Disaster Recovery	3.122.15.26, 3.122.15.7

Table 1: Setup Types

	Primary IP Address	Disaster Recovery
US Setup Type	52.20.144.155 34.231.154.95	54.176.92.81 54.183.58.225
EU Setup Type	63.33.127.190 63.33.175.64	3.122.15.26 3.122.15.7

	Primary IP Address	Disaster Recovery
Singapore Setup (SG) Type	13.228.159.49 54.179.105.241	13.214.251.223 54.255.57.46



CHAPTER 2

Getting Started

- Activate IoT Service (Wired), on page 9

Activate IoT Service (Wired)

The following procedure shows you how to activate IoT service (wired) on your devices from the Cisco Spaces dashboard.

Before you begin

To activate IoT service (wired), here are some prerequisites.

- Cisco Spaces: Connector
- Cisco Catalyst 9300 or 9400 Series Switches with Cisco IOS XE Amsterdam 17.3.x and later

Note The workflow initiated by this procedure automatically checks for these prerequisites.

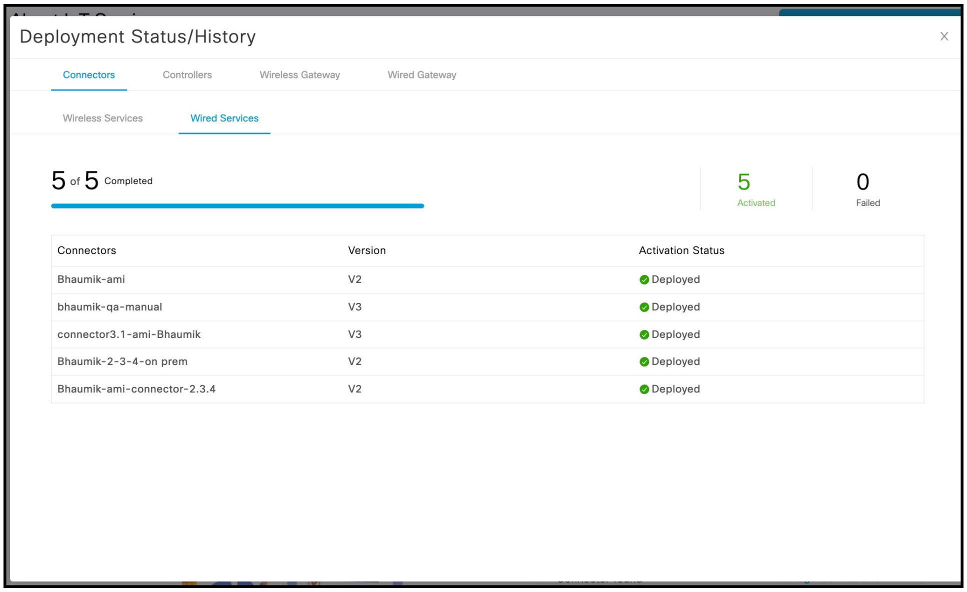
Step 1 Log in to Cisco Spaces.

Step 2 From the left navigation pane, click **IoT Services** > **About IoT Services**.

You can see the number of connectors activated with the IoT service (wired) service. You can also see the number of switches deployed as an IoT service (wired) gateway.

Click **View Detailed Status** to see the breakdown of the activation status by individual devices.

Figure 5: Detailed Status of Connectors Activated With IoT Service (Wired)



Deployment Status/History

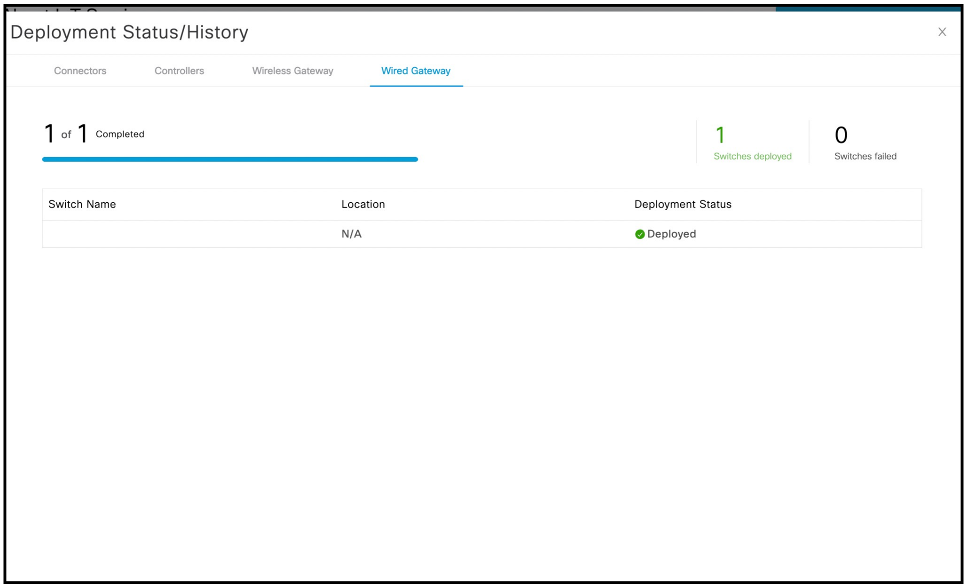
5 of 5 Completed

5 Activated

0 Failed

Connectors	Version	Activation Status
Bhaumik-ami	V2	✓ Deployed
bhaumik-qa-manual	V3	✓ Deployed
connector3.1-ami-Bhaumik	V3	✓ Deployed
Bhaumik-2-3-4-on prem	V2	✓ Deployed
Bhaumik-ami-connector-2.3.4	V2	✓ Deployed

Figure 6: Detailed Status of Switches Activated as IoT Service (Wired) Gateways



Deployment Status/History

1 of 1 Completed

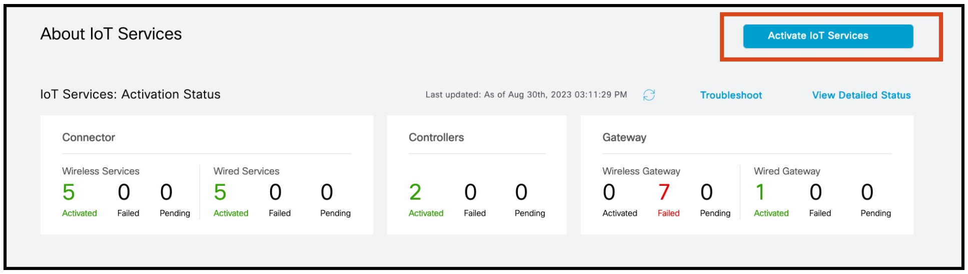
1 Switches deployed

0 Switches failed

Switch Name	Location	Deployment Status
	N/A	✓ Deployed

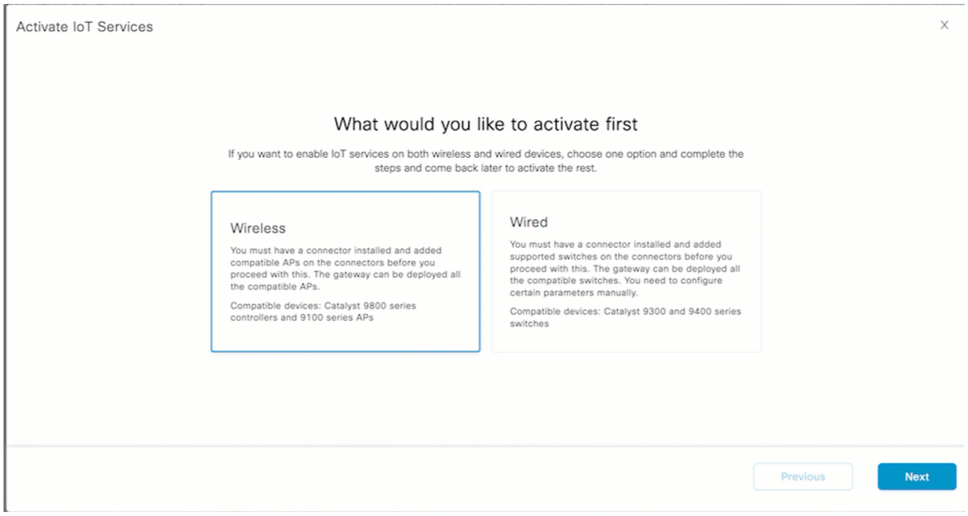
Step 3 In the **About IoT Services** window top-right corner, click **Activate IoT Services**.

Figure 7: Activate IoT Services



Step 4 In the **Activate IoT Services** window that is displayed, choose **Wired**.

Figure 8: Activate IoT Service (Wired)



What would you like to activate first

If you want to enable IoT services on both wireless and wired devices, choose one option and complete the steps and come back later to activate the rest.

Wireless

You must have a connector installed and added compatible APs on the connectors before you proceed with this. The gateway can be deployed all the compatible APs.

Compatible devices: Catalyst 9800 series controllers and 9100 series APs

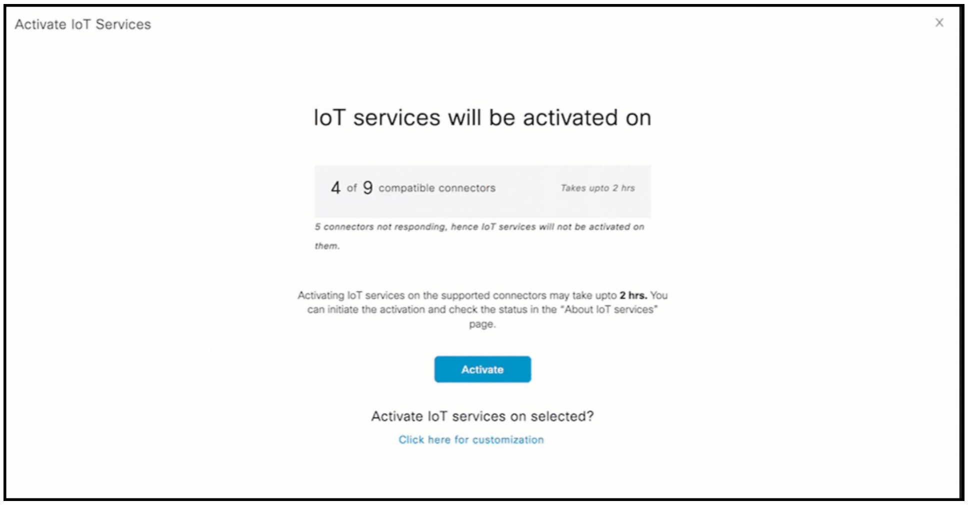
Wired

You must have a connector installed and added supported switches on the connectors before you proceed with this. The gateway can be deployed all the compatible switches. You need to configure certain parameters manually.

Compatible devices: Catalyst 9300 and 9400 series switches

You can see the list of all devices that can be activated with IoT service (wired), along with the time taken for activation.

Figure 9: List of Devices that Support IoT Service (Wired)



IoT services will be activated on

4 of 9 compatible connectors *Takes upto 2 hrs*

5 connectors not responding, hence IoT services will not be activated on them.

Activating IoT services on the supported connectors may take upto **2 hrs.** You can initiate the activation and check the status in the "About IoT services" page.

Activate IoT services on selected?

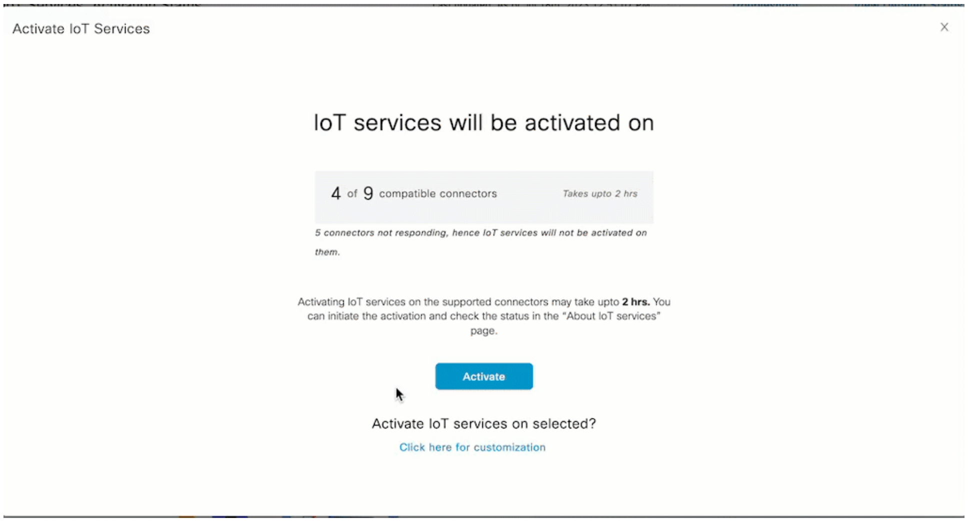
Step 5 To activate IoT service (wired) on all devices on your network, do the following:

a) In the **IoT services will be activated on** window, click **Activate**.

Note For Smart power distribution unit (PDU) and Hella cameras, IoT service (wired) is now activated. Click **Finish** to exit this procedure. Continue the procedure only for sensors and other devices.

b) To use wired sensors, you can activate wired gateway on your switches. Click **Activate Wired.**

Figure 10: Activate IoT service (wired)


Activate IoT Services
×
IoT services will be activated on
4 of 9 compatible connectors
Takes upto 2 hrs
Activate
Activate IoT services on selected?
Click here for customization

5 connectors not responding, hence IoT services will not be activated on them.

Activating IoT services on the supported connectors may take upto **2 hrs.** You can initiate the activation and check the status in the "About IoT services" page.

c) Continue to Step 7 to deploy the IoT service (wired) gateway.

Step 6 To activate IoT service (wired) only on specific devices of your network, do the following:

a) In the **IoT services will be activated on** window, click **Click here for customization**.

b) Check if your preferred connector is activated. If it is not activated, choose one or more connectors you want to activate with IoT service (wired), and click **Activate**.

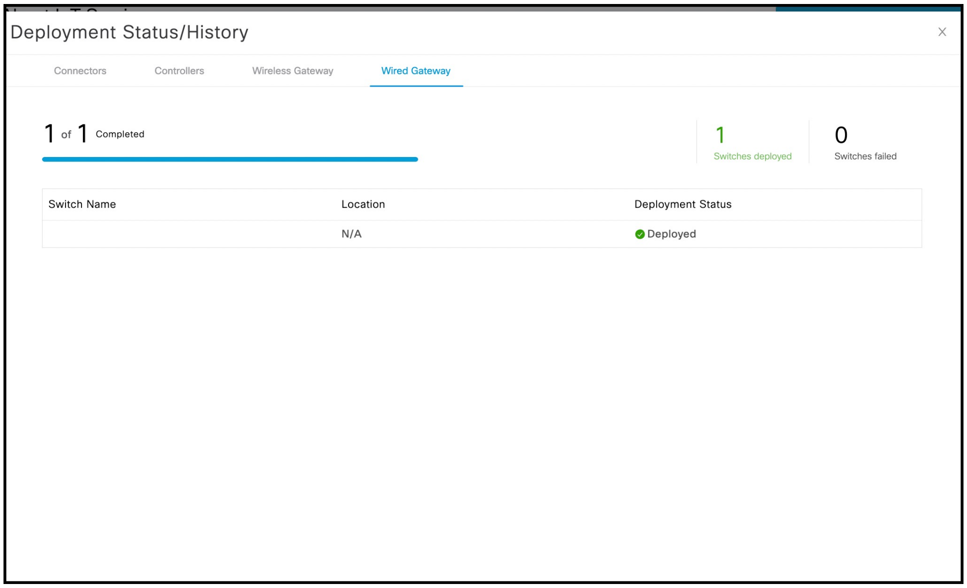
Note For Smart PDU and Hella cameras, IoT service (wired) is now activated. There is no further need to proceed with the following steps in this task. Click **Finish** to exit this procedure. Continue the steps only for sensors and other devices, and click **Activate Wired**.

c) If your connector is already activated, you can click **Skip to Gateway Deployment**.

Step 7 To deploy a switch as a IoT service (wired) gateway, do the following:

a) In the **Deploy Wired Gateway: 1. Choose Switches** window that is displayed, check the respective switches check box on which you want to deploy IoT service (wired) gateway.

Figure 11: Common Parameters: Wired Gateway



Deployment Status/History

1 of 1 Completed

1 Switches deployed

0 Switches failed

Switch Name	Location	Deployment Status
	N/A	✓ Deployed

b) In the **Deploy Wired Gateway: 2. Choose Type** window that is displayed, choose **Static** to configure static IP addresses and other details for the gateway.

c) In the **Deploy Wired Gateway: 3. Common Parameters** window that is displayed, you can configure the following common parameters of the gateway:

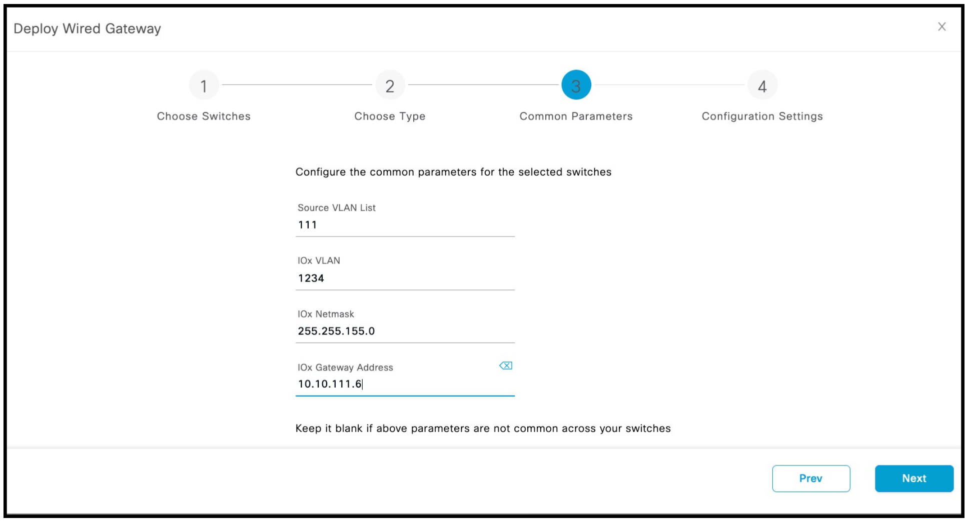
- **Source VLAN list:** List of VLANs to which the wired devices are connected. The traffic on these VLANs is monitored. If the wired devices are connected to multiple VLANs, enter the VLANs separated by a comma.

- **IOx VLAN**: This is the VLAN on which the connector is reachable (for management or data). You must configure the Cisco IOx App's second interface to use this VLAN to send traffic to the connector. This VLAN can be the same as the wired PoE node VLAN. The connector must have the required permissions to accept communications from the Cisco IOx App.

- **IOx Netmask**: This is the IP subnet mask that you must manually configure for the Cisco IOx App's second interface, and is used to communicate with the connector. This is not required if you select DHCP.

- **IoX Gateway Address**: This is the IP address that you must manually configure for the Cisco IOx App's second interface, and is used to communicate with the connector. This is not required if you select DHCP.

Figure 12: Common Parameters: Wired Gateway



Deploy Wired Gateway

Configure the common parameters for the selected switches

Source VLAN List
111

IOx VLAN
1234

IOx Netmask
255.255.155.0

IOx Gateway Address
10.10.111.6

Keep it blank if above parameters are not common across your switches

Figure 13: ERSPAN Session Interfaces

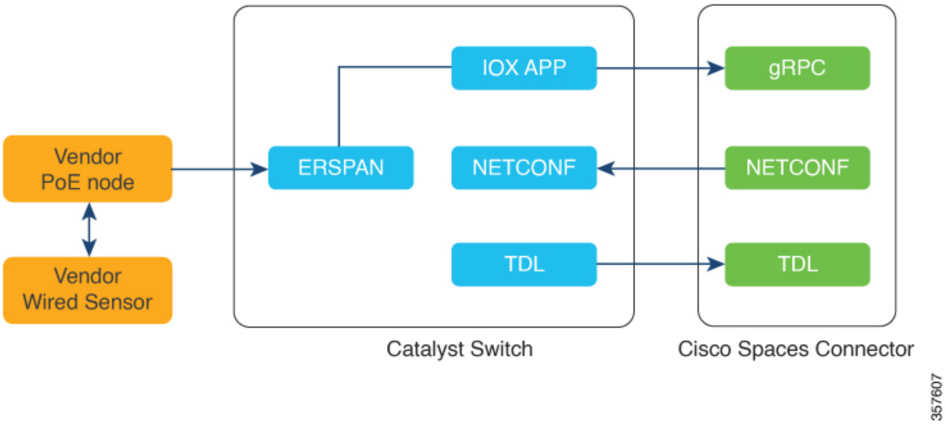
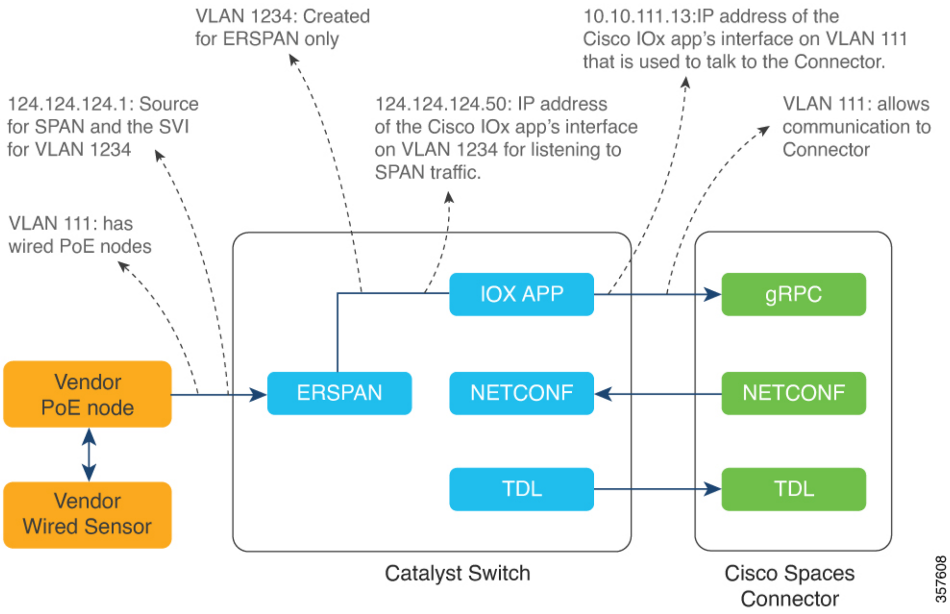


Figure 14: Sample Configuration


VLAN 1234: Created for ERSPAN only
10.10.111.13:IP address of the Cisco IOx app's interface on VLAN 111 that is used to talk to the Connector.
124.124.124.1: Source for SPAN and the SVI for VLAN 1234
124.124.124.50: IP address of the Cisco IOx app's interface on VLAN 1234 for listening to SPAN traffic.
VLAN 111: allows communication to Connector
VLAN 111: has wired PoE nodes
IOX APP
gRPC
Vendor PoE node
ERSPAN
NETCONF
NETCONF
Vendor Wired Sensor
TDL
TDL
Catalyst Switch
Cisco Spaces Connector
357608

d) In the **Deploy Wired Gateway: 4. Configuration Settings** window that is displayed, you can add the IOx IP Address by clicking the pen icon. This is the IP address that you must manually configure for the Cisco IOx App's second interface, and is used to communicate with the Connector. This is not required if you select DHCP.

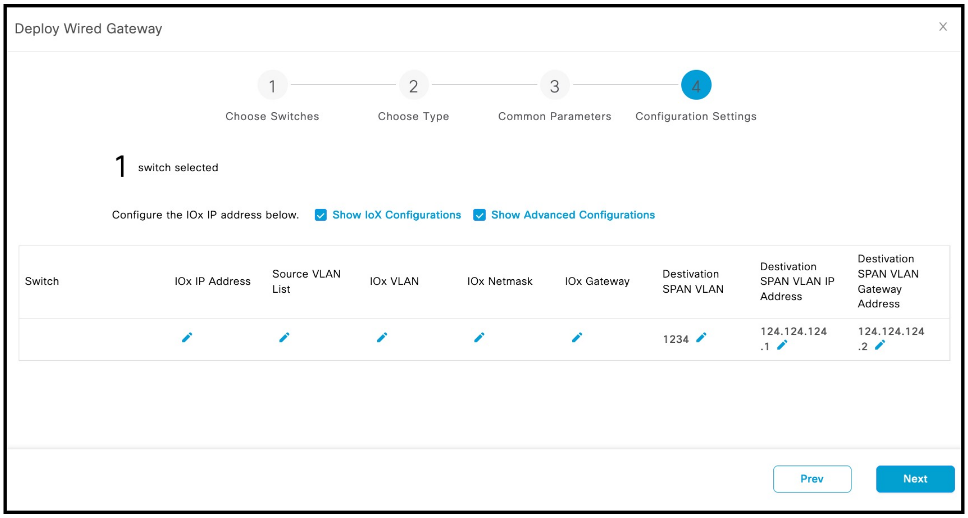
You can also see and edit the wired gateway configurations you made previously by checking **Show IoX Configurations** check box. You can edit the IoX configurations:

- Source VLAN list:
- IOx VLAN
- IOx Netmask
- IoX Gateway Address
- IOx IP Address

You can also edit the default advanced configurations:

- **Destination SPAN VLAN**: The VLAN used to send ERSPAN traffic from Power over Ethernet (PoE) nodes to Cisco IOx App. You can use an existing VLAN or create a new one. This VLAN can also be local to the switch.
- **Destination SPAN VLAN IP address**: This is the Switched Virtual Interface (SVI) or the IP address of the destination VLAN that can be used to route traffic. If you are using an existing VLAN, you can provide the same IP address. We recommend that you create a new VLAN so that you can keep the ERSPAN traffic local without impacting the existing configuration. This VLAN is used only within the switch for the SPAN traffic.
- **Destination SPAN VLAN Gateway Address**:

Figure 15: Deploy Wired Gateway: 4. Configuration Settings



1 switch selected

Configure the IOx IP address below. ☑ Show IoX Configurations ☑ Show Advanced Configurations

Switch	IOx IP Address	Source VLAN List	IOx VLAN	IOx Netmask	IOx Gateway	Destivation SPAN VLAN	Destivation SPAN VLAN IP Address	Destivation SPAN VLAN Gateway Address
	✎	✎	✎	✎	✎	1234 ✎	124.124.124.1 ✎	124.124.124.2 ✎

e) Click **Finish** to deploy the IoT service (wired) gateway on the selected switch.

PART II

Configuration

- Switch as a Gateway, on page 19
- Sensors and Wired Devices, on page 25

CHAPTER 3

Switch as a Gateway

- Switch as a Gateway, on page 19
- Configuring a Switch as a Wired Gateway, on page 19
- Uninstall, or Upgrade a Wired Application on a Switch, on page 22

Switch as a Gateway

You can configure the following switches as a wired gateway:

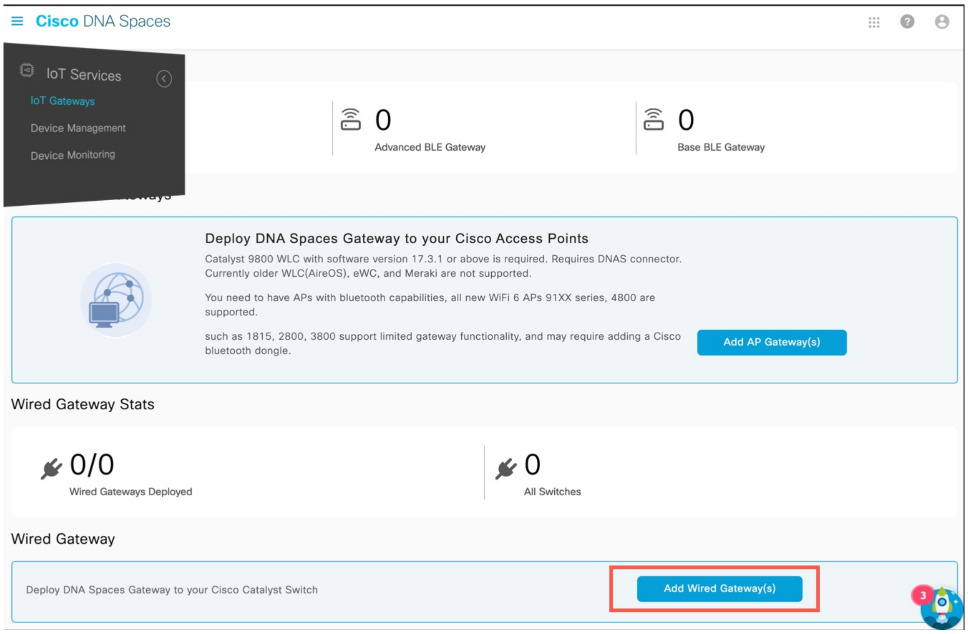
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches

Configuring a Switch as a Wired Gateway

Step 1 In the IoT Service dashboard, choose **IoT Gateways > Wired Gateways**.

Step 2 Click **Add New Gateways**.

Figure 16: Adding a New Gateway



Deploy DNA Spaces Gateway to your Cisco Access Points

Catalyst 9800 WLC with software version 17.3.1 or above is required. Requires DNAS connector. Currently older WLC(AireOS), eWC, and Meraki are not supported.

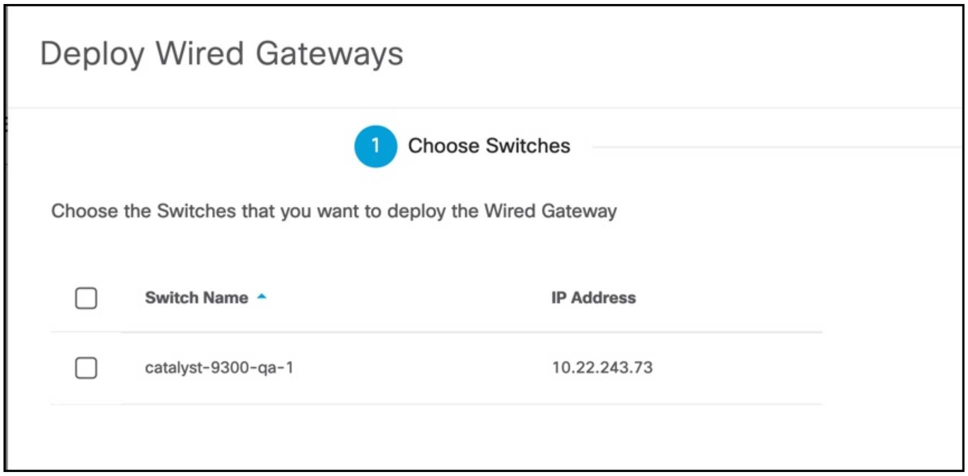
You need to have APs with bluetooth capabilities, all new WiFi 6 APs 91XX series, 4800 are supported.

such as 1815, 2800, 3800 support limited gateway functionality, and may require adding a Cisco bluetooth dongle.

Deploy DNA Spaces Gateway to your Cisco Catalyst Switch

Step 3 In the **Deploy Wired Gateways** window that is displayed, select the switch you want to deploy as a wired gateway. (IoT Service configures a compatible switch as a wired gateway.)

Figure 17: Deploy Wired Gateways



Deploy Wired Gateways

1 Choose Switches

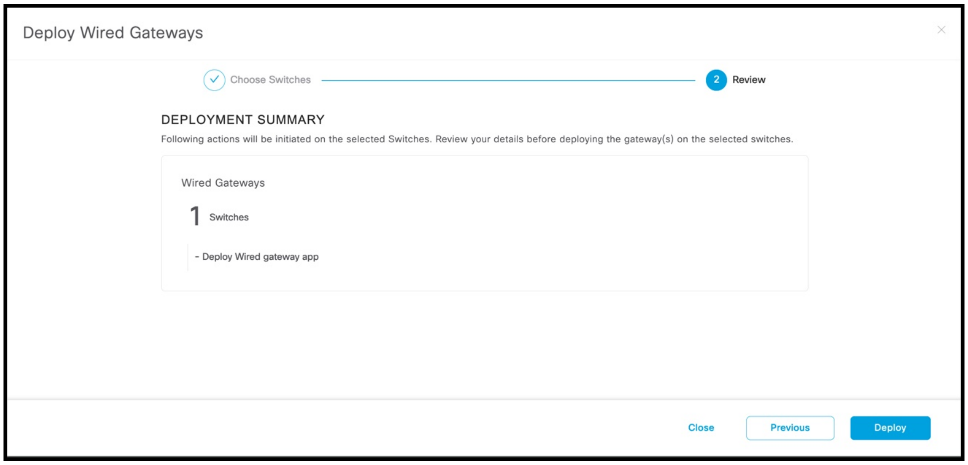
Choose the Switches that you want to deploy the Wired Gateway

	Switch Name ▲	IP Address
□	catalyst-9300-qa-1	10.22.243.73

A switch that is enabled as a wired gateway, can scan for wired sensors using an installedIoX Application .

Step 4 You can review the requested changes and click **Deploy**.

Figure 18: Review Changes



Deploy Wired Gateways

DEPLOYMENT SUMMARY

Following actions will be initiated on the selected Switches. Review your details before deploying the gateway(s) on the selected switches.

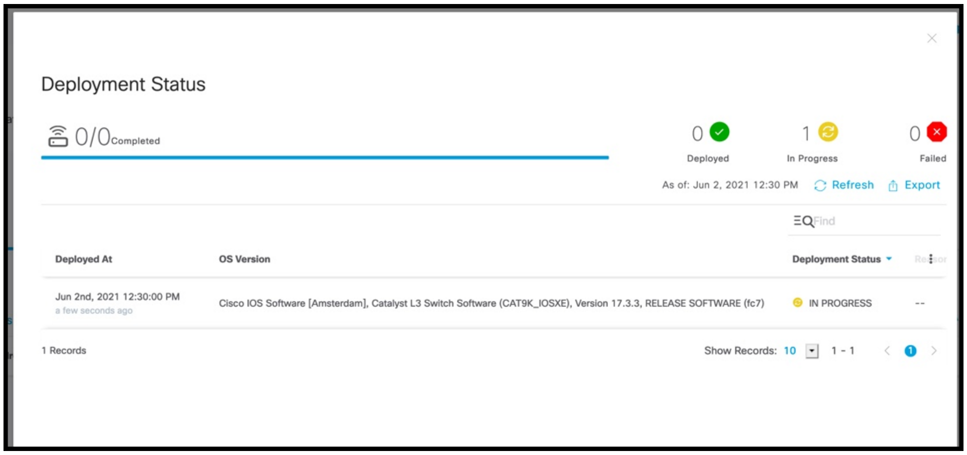
Wired Gateways

1 Switches

- Deploy Wired gateway app

After the switch receives the change requests, the switch is queued to be deployed as a wired gateway. You can observe the progress on the displayed deployment status window.

Figure 19: Deployment Status



Deployment Status

0/0 Completed

0 ✓ Deployed

1 In Progress

0 ✕ Failed

As of: Jun 2, 2021 12:30 PM

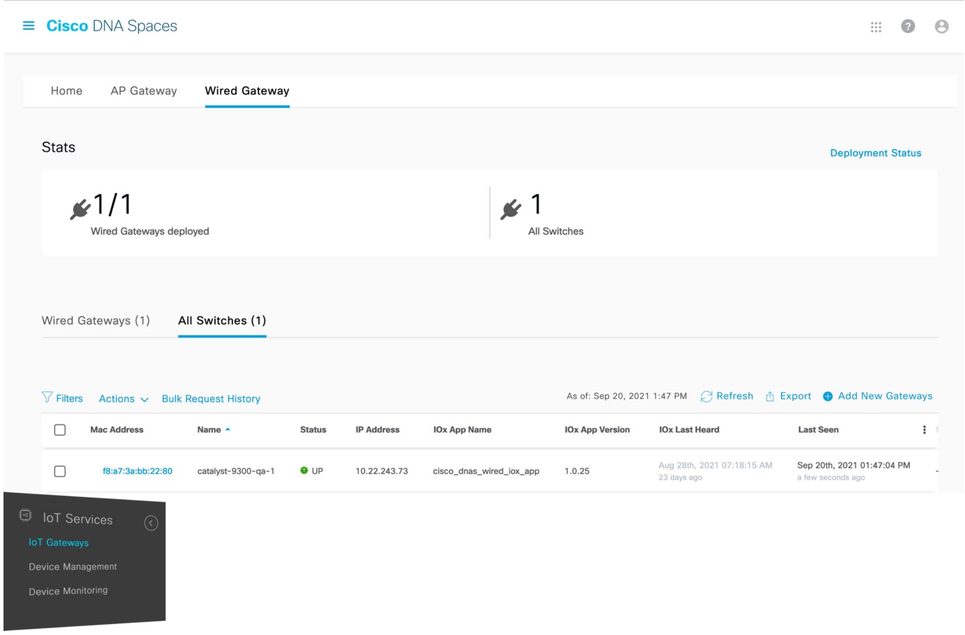
Deployed At	OS Version	Deployment Status	Reason
Jun 2nd, 2021 12:30:00 PM a few seconds ago	Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.3, RELEASE SOFTWARE (fc7)	IN PROGRESS	--

1 Records

Show Records: 10 1 - 1

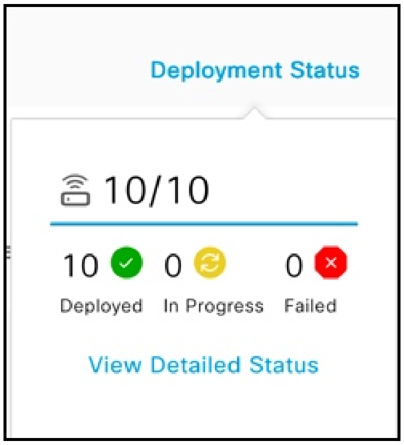
You can also check the status of the deployment by clicking the **Wired Gateways** tab and then clicking **Deployment Status** button at the top-right corner.

Figure 20: Deployment Status



□	Mac Address	Name	Status	IP Address	IOx App Name	IOx App Version	IOx Last Heard	Last Seen
□	f8:a7:3a:bb:22:80	catalyst-9300-qa-1	● UP	10.22.243.73	cisco_dnas_wired_iox_app	1.0.25	Aug 28th, 2021 07:18:15 AM 23 days ago	Sep 20th, 2021 01:47:04 PM a few seconds ago

Figure 21: Deployment Status: Summarized view



Uninstall, or Upgrade a Wired Application on a Switch

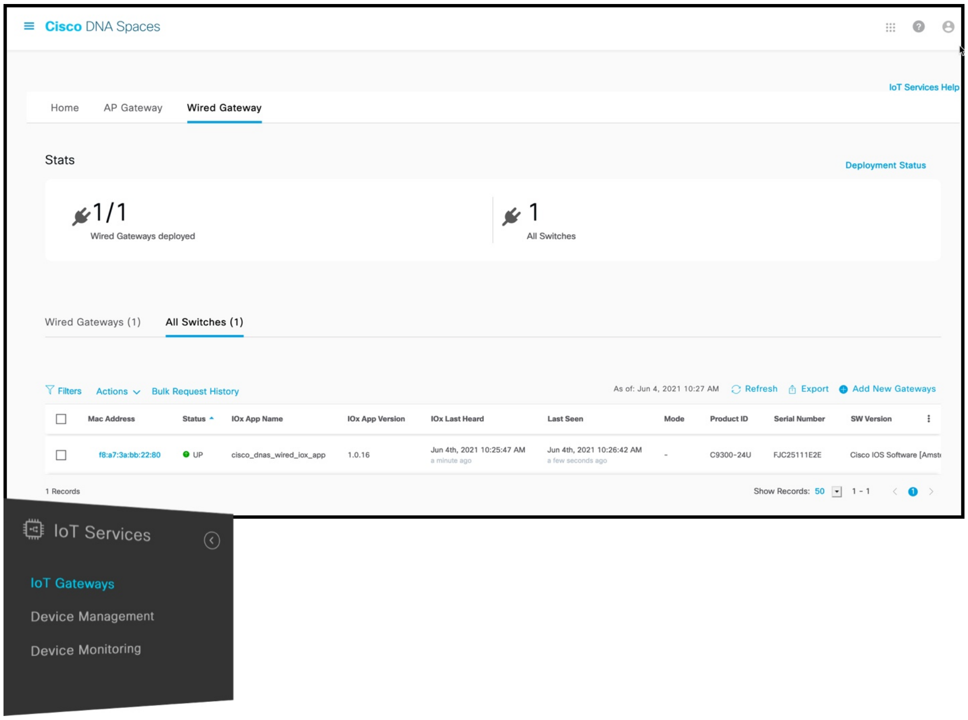
You can uninstall, or upgrade wired applications on wired gateways. The Cisco Spaces Wired app is one such application.

Before you begin

Ensure that you have configured a switch as an wired gateway.

Step 1 In the Cisco Spaces dashboard, choose **IoT Gateways** > **Wired Gateways** and click **All Switches.**

Figure 22: Unistalling or Upgrading an IoX Application



Cisco DNA Spaces

IoT Services Help

Home | AP Gateway | Wired Gateway

Stats

Deployment Status

1/1 Wired Gateways deployed

1 All Switches

Wired Gateways (1) | All Switches (1)

Filters | Actions | Bulk Request History

As of: Jun 4, 2021 10:27 AM | Refresh | Export | Add New Gateways

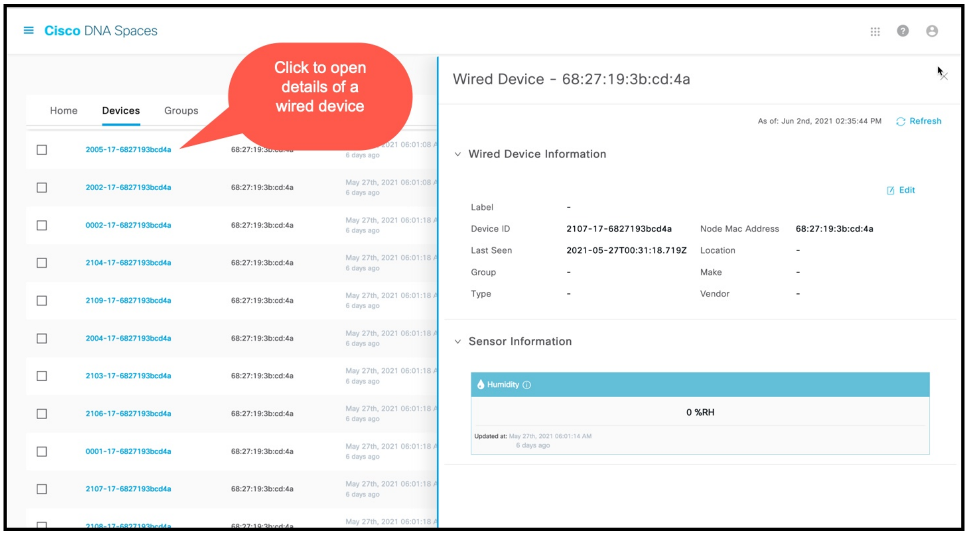
□	Mac Address	Status	IOx App Name	IOx App Version	IOx Last Heard	Last Seen	Mode	Product ID	Serial Number	SW Version
□	f8:a7:3a:bb:22:80	● UP	cisco_dnas_wired_iox_app	1.0.16	Jun 4th, 2021 10:25:47 AM a minute ago	Jun 4th, 2021 10:26:42 AM a few seconds ago	-	C9300-24U	FJC25111E2E	Cisco IOS Software [Amst

1 Records

Show Records: 50 | 1 - 1

Step 2 Click the MAC address of the switch to open the **Wired Switch** window containing the details.

Figure 23: Unistalling or Upgrading an IoX Application



Cisco DNA Spaces

Home | Devices | Groups

□	2005-17-6827193bcd4a	68:27:19:3b:cd:4a	2021 06:01:08 A 6 days ago
□	2002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:08 A 6 days ago
□	0002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2104-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2109-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2004-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2103-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2106-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	0001-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2107-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2108-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A

Click to open details of a wired device

Wired Device - 68:27:19:3b:cd:4a

As of: Jun 2nd, 2021 02:35:44 PM | Refresh

Wired Device Information

Edit

Label	-		
Device ID	2107-17-6827193bcd4a	Node Mac Address	68:27:19:3b:cd:4a
Last Seen	2021-05-27T00:31:18.719Z	Location	-
Group	-	Make	-
Type	-	Vendor	-

Sensor Information

Humidity

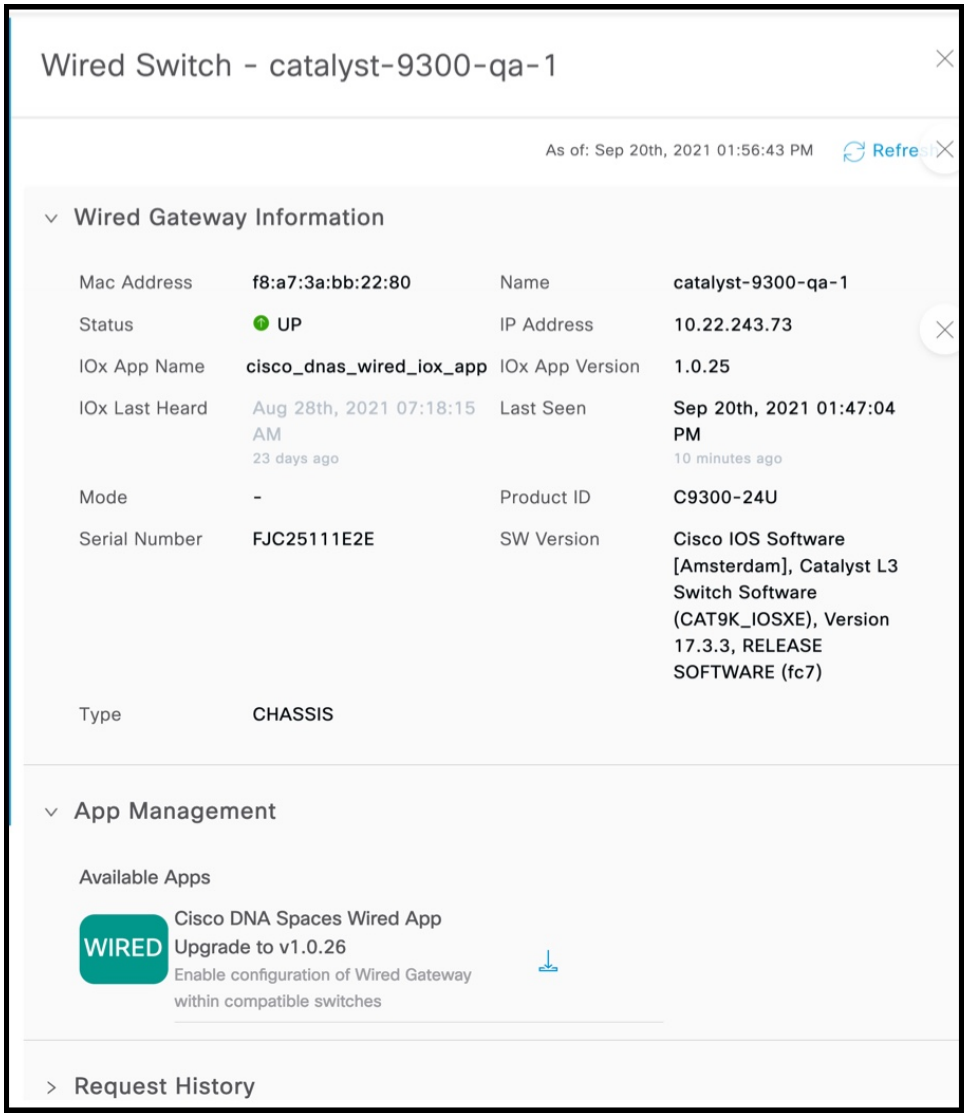
0 %RH

Updated at: May 27th, 2021 06:01:14 AM
6 days ago

Step 3 In the **App Management** section, you can see the applications available for installation, uninsallation, or upgrade. Do one of the following:

- To uninstall, click the uninstall icon near the Cisco Spaces Wired app.
- To upgrade, check if a version is available for upgrade near the Cisco Spaces Wired app and click it.
- To upload tech support files to the connector, click the gear icon.

Figure 24: Unistalling or Upgrading an Cisco Spaces Wired app



Wired Switch - catalyst-9300-qa-1

As of: Sep 20th, 2021 01:56:43 PM

Wired Gateway Information

Mac Address	f8:a7:3a:bb:22:80	Name	catalyst-9300-qa-1
Status	● UP	IP Address	10.22.243.73
IOx App Name	cisco_dnas_wired_iox_app	IOx App Version	1.0.25
IOx Last Heard	Aug 28th, 2021 07:18:15 AM 23 days ago	Last Seen	Sep 20th, 2021 01:47:04 PM 10 minutes ago
Mode	-	Product ID	C9300-24U
Serial Number	FJC25111E2E	SW Version	Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.3, RELEASE SOFTWARE (fc7)
Type	CHASSIS		

App Management

Available Apps

WIRED Cisco DNA Spaces Wired App
Upgrade to v1.0.26
Enable configuration of Wired Gateway within compatible switches

The switch, which is the wired gateway, receives these change requests for installation. You can observe the progress on the displayed window. You can also check the status of the wired gateway deployment by clicking the **Deployment status** icon at the top-right corner of the dashboard (in the **AP Gateways** window). Here, you can see the deployment status of the wired gateway at a more detailed level. You can see whether the gateway is enabled and whether an app is being installed. Unlike bulk history, you can view the details of an individual wired gateway. If the gateway deployment fails, the reasons are listed here.

CHAPTER 4

Sensors and Wired Devices

- Viewing Wired Sensors or Devices on IoT Service, on page 25
- Configure a Smart PDU, on page 26
- Configure a Hella Camera, on page 31

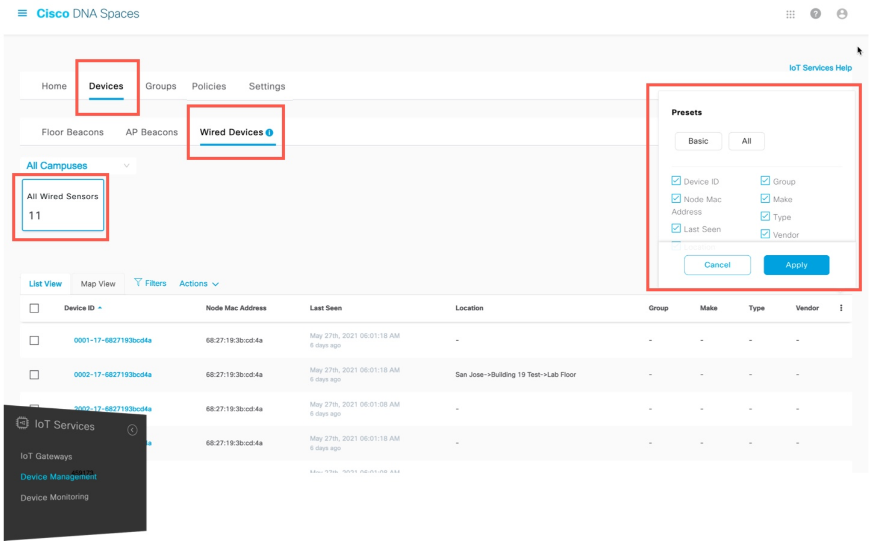
Viewing Wired Sensors or Devices on IoT Service

Step 1 In the IoT Service dashboard, click **Device Management**.

Step 2 Click **Devices** > **Wired Devices** to view the sensors and wired devices.

Step 3 To add or delete columns, click the corresponding vertical three-dot icon.

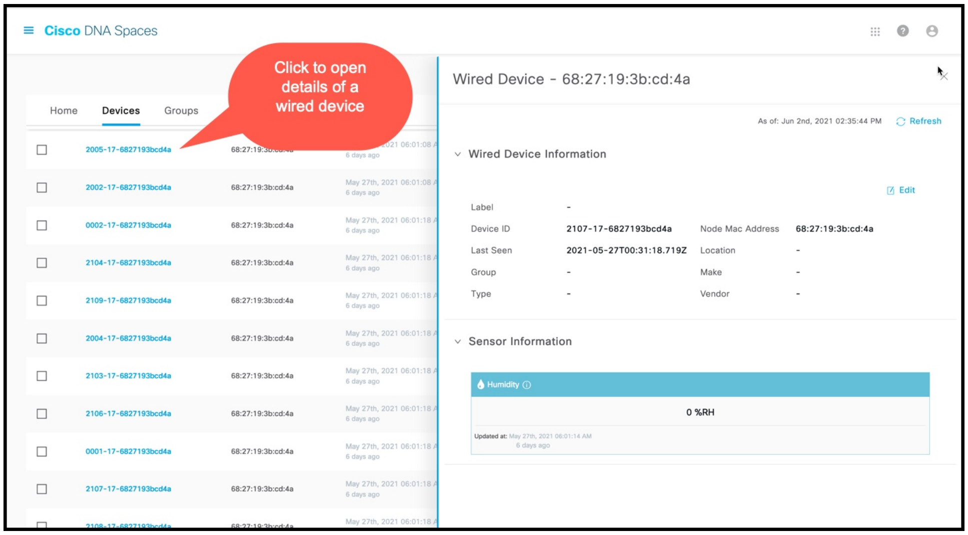
Figure 25: Adding or Removing a Column



□	Device ID	Node Mac Address	Last Seen	Location	Group	Make	Type	Vendor
□	0001-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 AM 6 days ago	-	-	-	-	-
□	0002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 AM 6 days ago	San Jose->Building 19 Test->Lab Floor	-	-	-	-
	2002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:08 AM 6 days ago	-	-	-	-	-
	a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 AM 6 days ago	-	-	-	-	-

Step 4 Click a MAC address to view further details.

Figure 26: Viewing Details of a Switch



□	2005-17-6827193bcd4a	68:27:19:3b...	...2021 06:01:08 A 6 days ago
□	2002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:08 A 6 days ago
□	0002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2104-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2109-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2004-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2103-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2106-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	0001-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2107-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2108-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A

Wired Device - 68:27:19:3b:cd:4a

As of: Jun 2nd, 2021 02:35:44 PM Refresh

Wired Device Information

Edit

Label	-		
Device ID	2107-17-6827193bcd4a	Node Mac Address	68:27:19:3b:cd:4a
Last Seen	2021-05-27T00:31:18.719Z	Location	-
Group	-	Make	-
Type	-	Vendor	-

Sensor Information

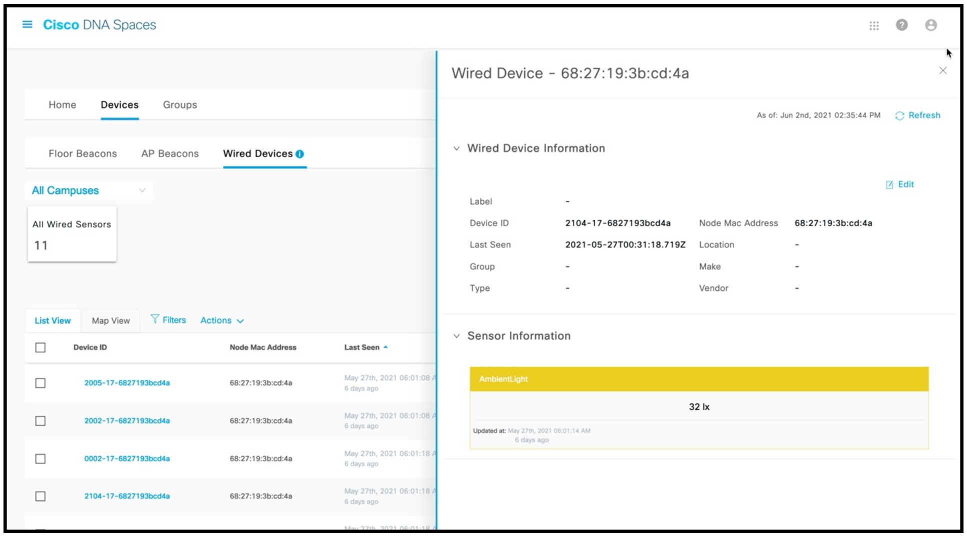
Humidity

0 %RH

Updated at: May 27th, 2021 06:01:14 AM
6 days ago

Step 5 Expand the **Sensor Information** section, to view the telemetry details collected by the wired sensor.

Figure 27: Telemetry Information



All Wired Sensors
11

□	Device ID	Node Mac Address	Last Seen
□	2005-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:08 A 6 days ago
□	2002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:08 A 6 days ago
□	0002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago
□	2104-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 A 6 days ago

Wired Device - 68:27:19:3b:cd:4a

As of: Jun 2nd, 2021 02:35:44 PM Refresh

Wired Device Information

Edit

Label	-		
Device ID	2104-17-6827193bcd4a	Node Mac Address	68:27:19:3b:cd:4a
Last Seen	2021-05-27T00:31:18.719Z	Location	-
Group	-	Make	-
Type	-	Vendor	-

Sensor Information

AmbientLight

32 lx

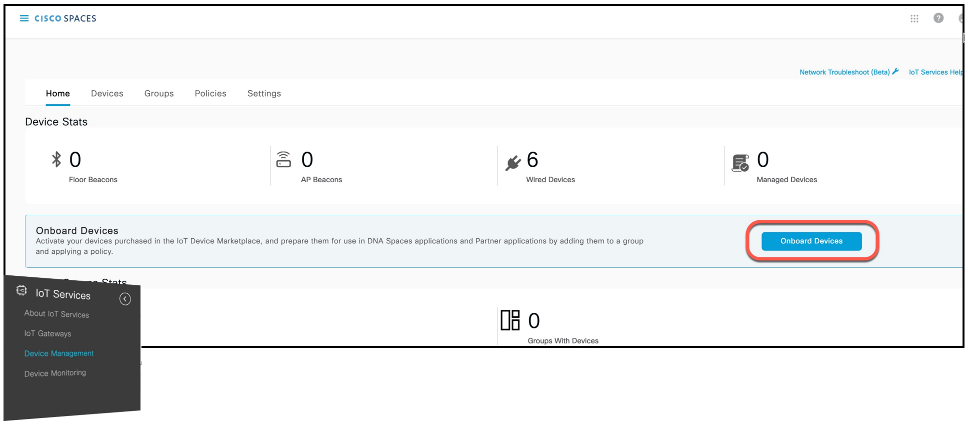
Updated at: May 27th, 2021 06:01:14 AM
6 days ago

Configure a Smart PDU

You can configure your Smart PDU with the following steps.

Step 1 In the Cisco Spaces dashboard, navigate to **IoT Service** > **Device Management** > **Home** and then click **Onboard Devices**.

Figure 28: Onboard Devices



Device Stats

0 Floor Beacons

0 AP Beacons

6 Wired Devices

0 Managed Devices

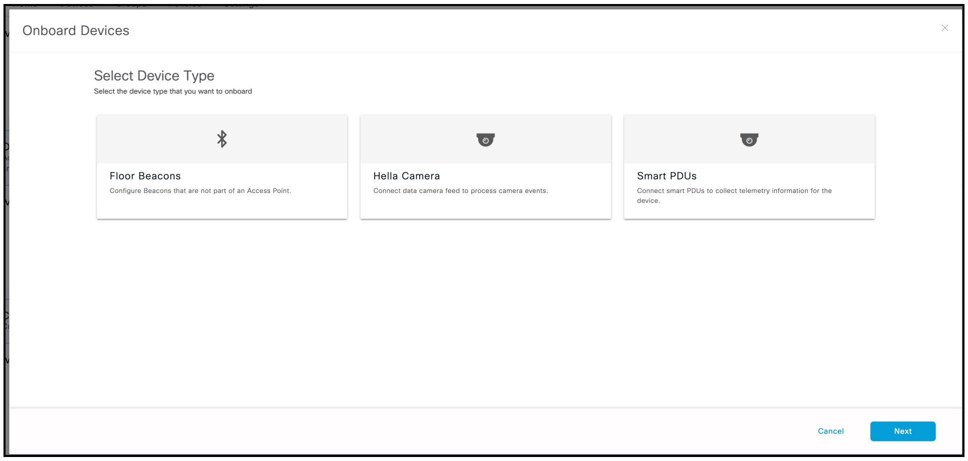
Onboard Devices

Activate your devices purchased in the IoT Device Marketplace, and prepare them for use in DNA Spaces applications and Partner applications by adding them to a group and applying a policy.

0 Groups With Devices

Step 2 In the **Onboard Devices** window, click **Smart PDUs**.

Figure 29: Smart PDUs



Onboard Devices

Select Device Type

Select the device type that you want to onboard

Floor Beacons

Configure Beacons that are not part of an Access Point.

Hella Camera

Connect data camera feed to process camera events.

Smart PDUs

Connect smart PDUs to collect telemetry information for the device.

Step 3 In the **Onboard Smart PDU** window displayed, do the following:

a) From the **Select Connector** drop-down list, choose a connector

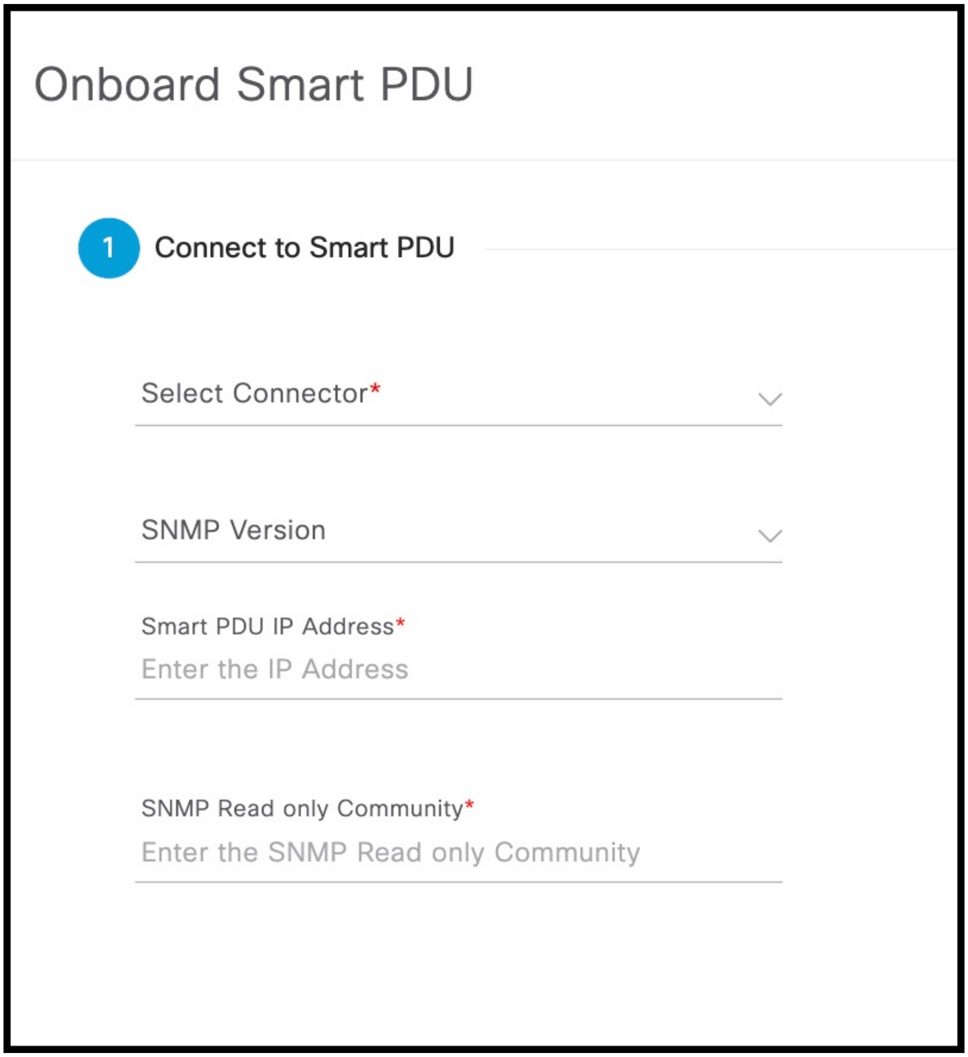
b) From the **SNMP Version** drop-down list, choose a **v2c** or **v3**.

c) Enter the IPv4 or IPv6 address of the device in the **Smart PDU IP address** field.

Step 4 If you chose v2c in the previous step (Step 3), do the following:

a) Enter a text in the **SNMP Read only Community** field.

Figure 30: SNMP Read only Community



Onboard Smart PDU

1 Connect to Smart PDU

Select Connector*

SNMP Version

Smart PDU IP Address*

Enter the IP Address

SNMP Read only Community*

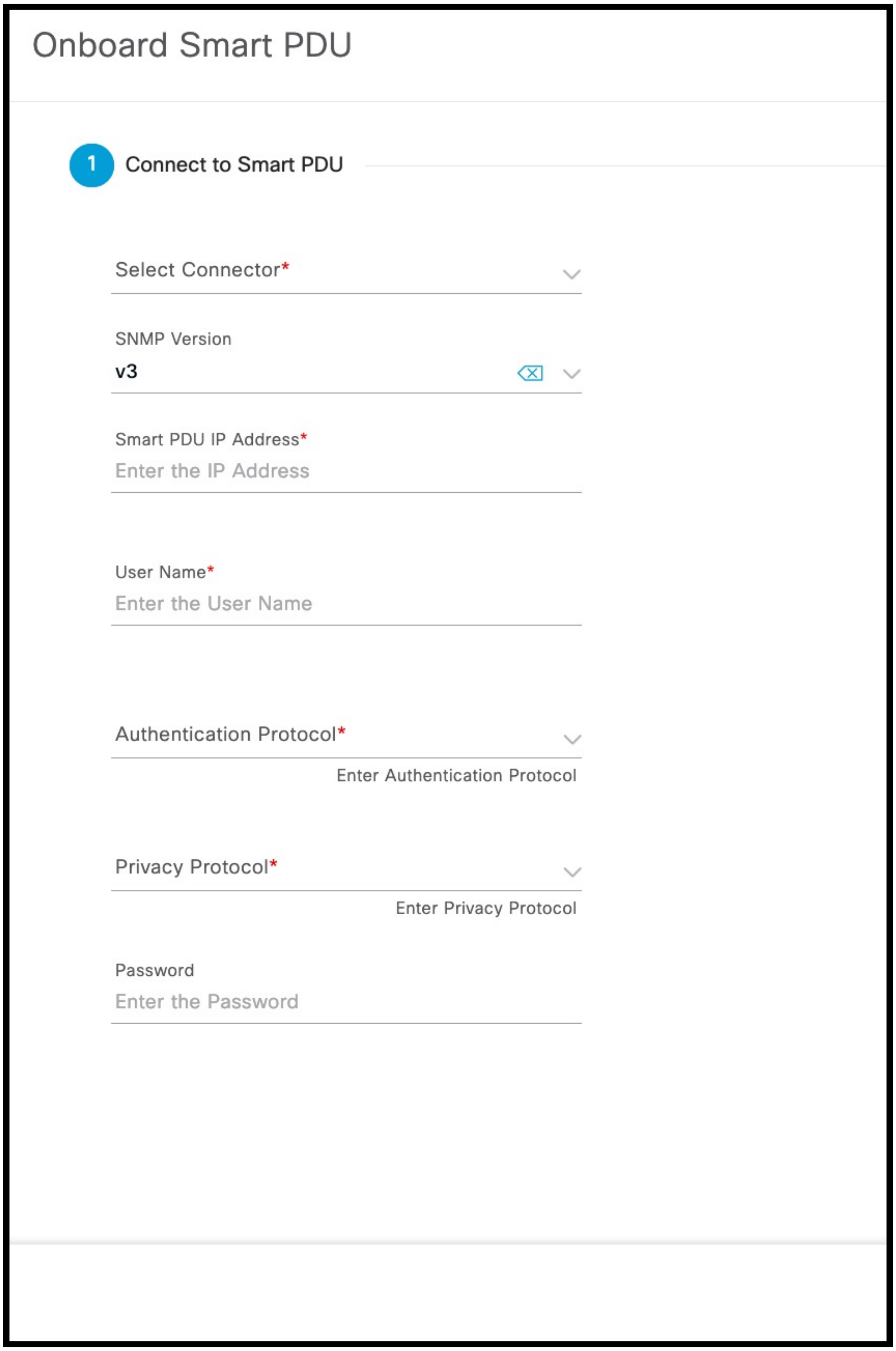
Enter the SNMP Read only Community

b) Click **Next**.

Step 5 If you chose v3 in Step 3, do the following:

a) Enter a user name.

Figure 31: User Name



Onboard Smart PDU

1 Connect to Smart PDU

Select Connector*

SNMP Version

v3

Smart PDU IP Address*

Enter the IP Address

User Name*

Enter the User Name

Authentication Protocol*

Enter Authentication Protocol

Privacy Protocol*

Enter Privacy Protocol

Password

Enter the Password

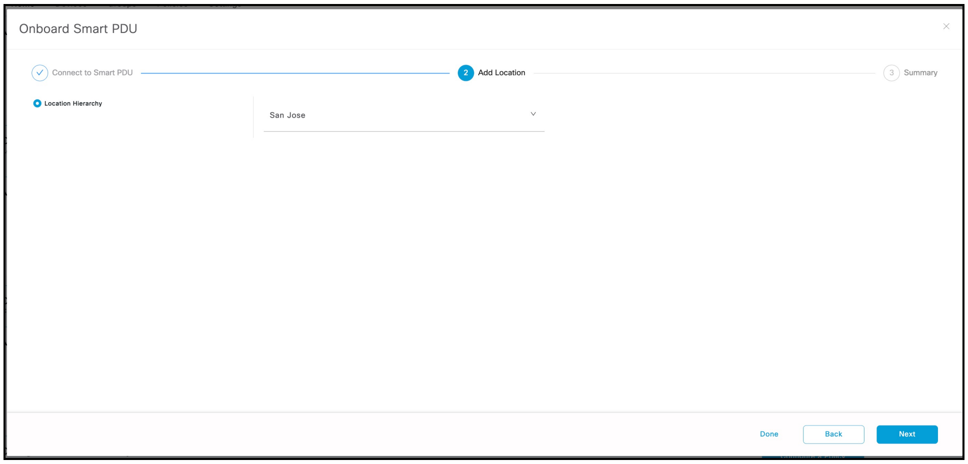
b) Choose an Authentication Protocol. You can choose from **HMAC-MD5** or **HMAC-SHA**

c) Enter a Privacy Protocol. You can choose from **CBC-DES** or **CFB-AES-128**.

d) Click **Next**.

Step 6 From the **Location Hierarchy** drop-down list, choose the current location of the device, and then click **Next**.

Figure 32: Location Hierarchy

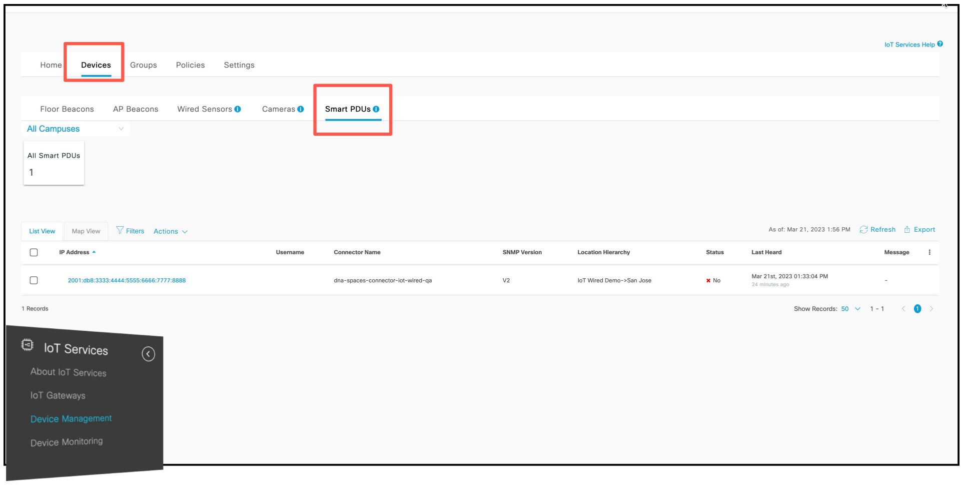


Onboard Smart PDU

● Location Hierarchy: San Jose

Step 7 Observe that the smart PDU is configured successfully, and then click **Done**

Figure 33: Smart PDU Configured



All Smart PDUs 1

As of: Mar 21, 2023 1:56 PM

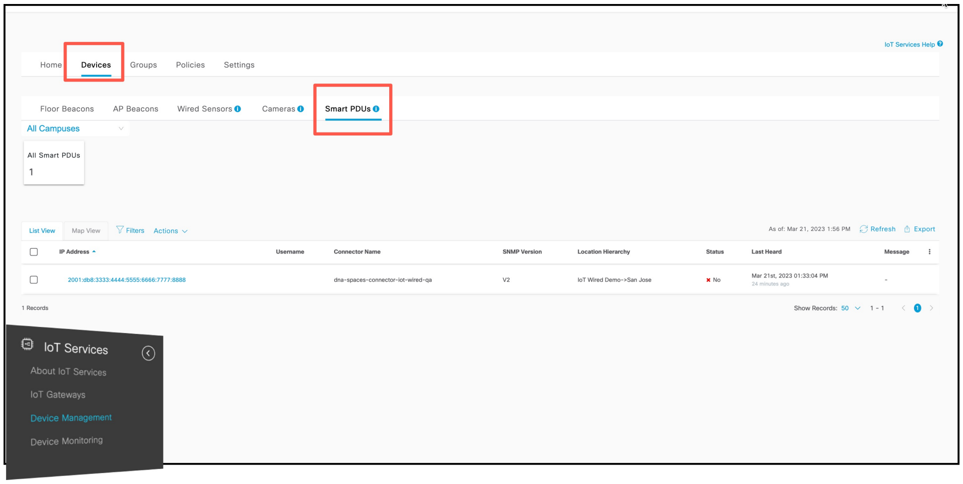
IP Address	Username	Connector Name	SNMP Version	Location Hierarchy	Status	Last Heard	Message
2001:db8:3333:4444:5555:6666:7777:8888		dna-spaces-connector-iot-wired-qa	V2	IoT Wired Demo->San Jose	✖ No	Mar 21st, 2023 01:33:04 PM 24 minutes ago	-

1 Records

Show Records: 50 1 - 1

The window listing all configured Smart PDUs is displayed, at **IoT Service > Device Management > Devices**, at the **Smart PDU** tab. You can observe all the configured details, as well as information about when the device was last heard from. Click on the respective smart PDU to see more details or to edit it.

Figure 34: Smart PDU



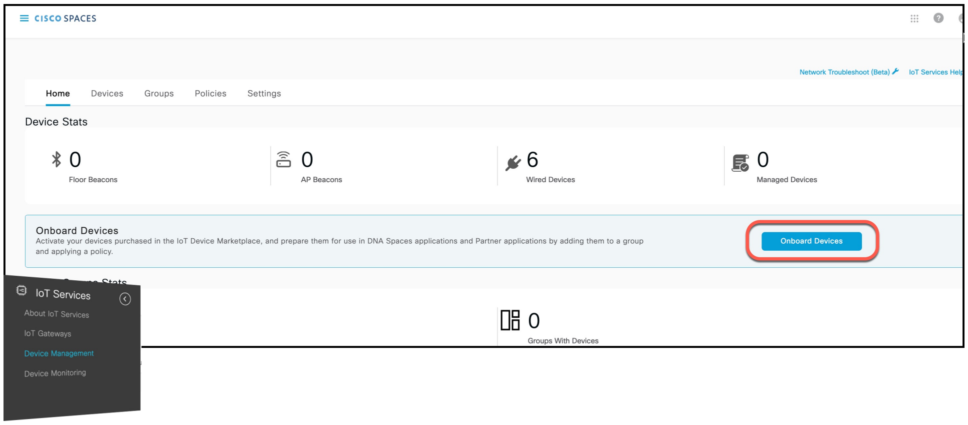
IP Address	Username	Connector Name	SNMP Version	Location Hierarchy	Status	Last Heard	Message
2001:db8:3333:4444:5555:6666:7777:8888		dna-spaces-connector-iot-wired-qa	V2	IoT Wired Demo->San Jose	✖ No	Mar 21st, 2023 01:33:04 PM 24 minutes ago	-

Configure a Hella Camera

You can configure your Hella Camera with the following steps.

Step 1 In the Cisco Spaces dashboard, navigate to **IoT Service** > **Device Management** > **Home** and then click **Onboard Devices**.

Figure 35: Onboard Devices

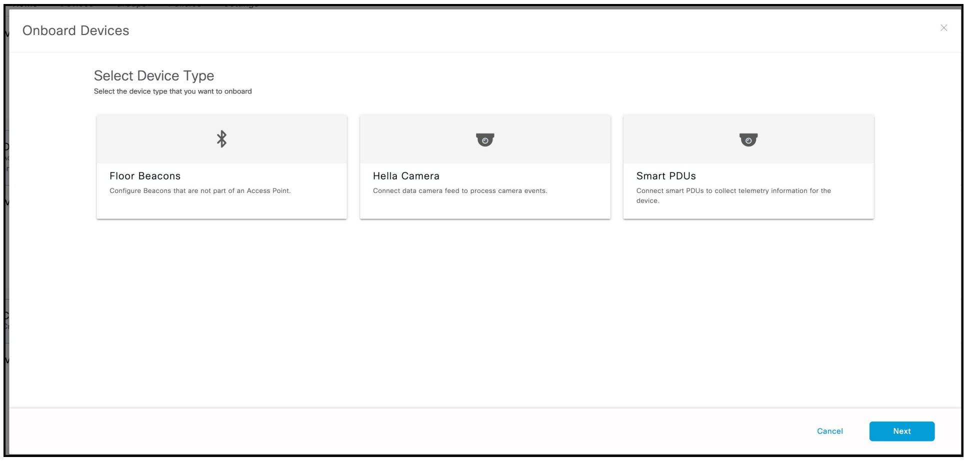


Onboard Devices

Activate your devices purchased in the IoT Device Marketplace, and prepare them for use in DNA Spaces applications and Partner applications by adding them to a group and applying a policy.

Step 2 In the **Onboard Devices** window, click **Hella Camera**.

Figure 36: Onboard Hella Camera



Onboard Devices

Select Device Type

Select the device type that you want to onboard

Floor Beacons

Configure Beacons that are not part of an Access Point.

Hella Camera

Connect data camera feed to process camera events.

Smart PDUs

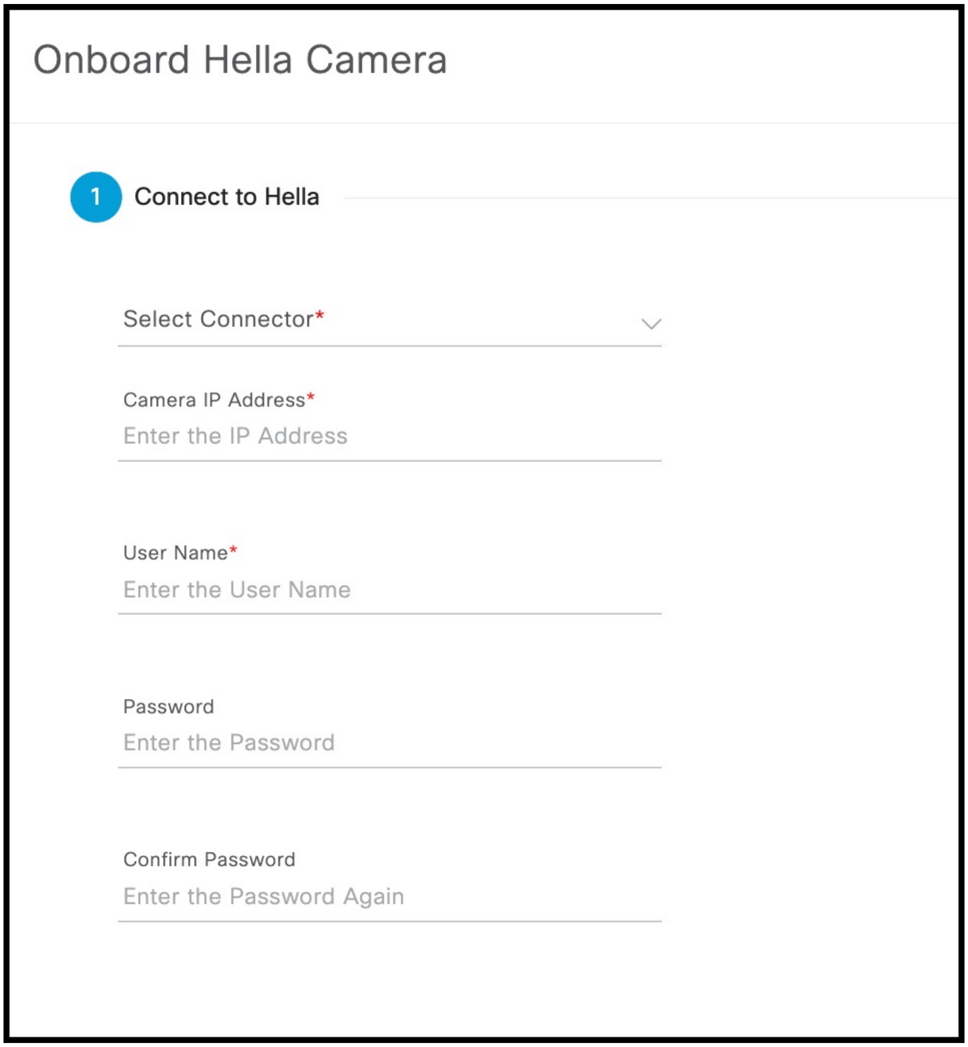
Connect smart PDUs to collect telemetry information for the device.

Step 3 In the **Onboard Hella Camera** window displayed, do the following:

a) From the **Select Connector** drop-down list, choose a connector

b) Enter the IPv4 or IPv6 address of the device in the **Camera IP address** field.

Figure 37: Onboard Hella Camera



Onboard Hella Camera

1 Connect to Hella

Select Connector*

Camera IP Address*
Enter the IP Address

User Name*
Enter the User Name

Password
Enter the Password

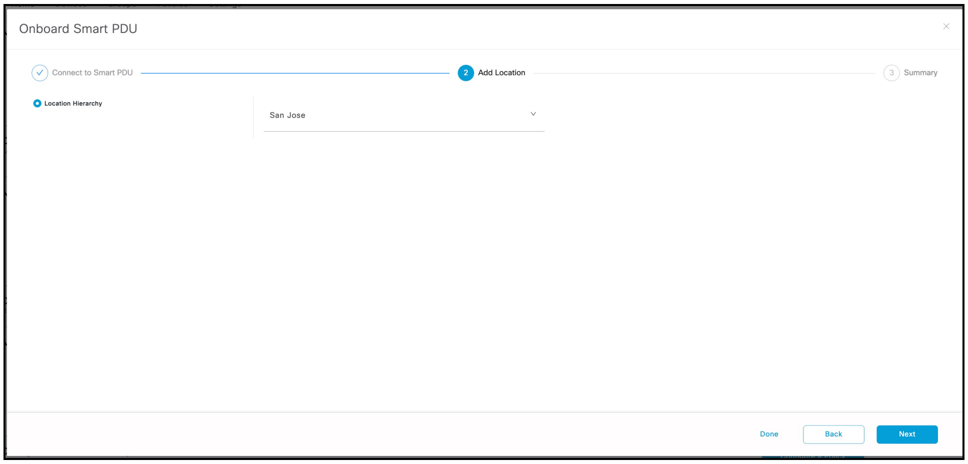
Confirm Password
Enter the Password Again

c) Enter a user name to access this device.

d) Create a password to access this device, and confirm the password.

Step 4 From the **Location Hierarchy** drop-down list, choose the current location of the device, and then click **Next**.

Figure 38: Location Hierarchy



Location Hierarchy

San Jose

Step 5 Observe that the Hella Camera is configured successfully, and then click **Done**

You are taken to the list of configured Hella Camera in **IoT Service** > **Device Management** > **Devices**, at the **Cameras** tab. You can observe all the configured details, as well as information about when the device was last heard from. Click on the respective Hella Camera to see more details or to edit it.

PART III

Device Management

- Device Management, on page 37

CHAPTER 5

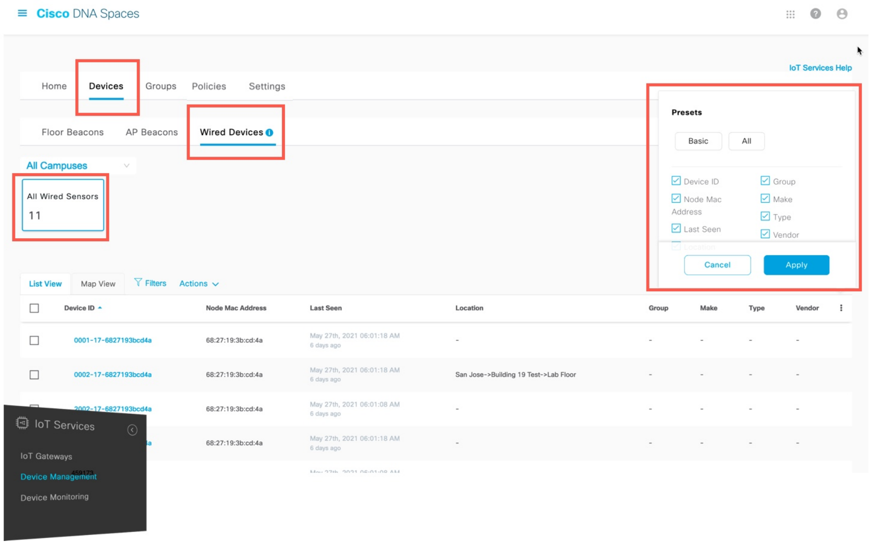
Device Management

- Dashboard View of Devices, on page 37
- Categorizing Devices into Groups, on page 37

Dashboard View of Devices

Choose **IoT Service > Device Management > Devices** and select a device type (**Floor Beacons**, **AP Beacons**, **Wired Devices**) to view an overview of that device.

Figure 39: Dashboard View of Devices



□	Device ID	Node Mac Address	Last Seen	Location	Group	Make	Type	Vendor
□	0001-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 AM 6 days ago	-	-	-	-	-
□	0002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 AM 6 days ago	San Jose->Building 19 Test->Lab Floor	-	-	-	-
□	2002-17-6827193bcd4a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:08 AM 6 days ago	-	-	-	-	-
	a	68:27:19:3b:cd:4a	May 27th, 2021 06:01:18 AM 6 days ago	-	-	-	-	-

Categorizing Devices into Groups

You can create groups and assign devices to them. This allows you to focus your attention on certain devices, and view only these devices by filtering them by the group.

Step 1 In the Cisco Spaces: IoT Service dashboard, choose **Device Management > Groups**.

Step 2 Click **Create a new group**, enter a **Group Name** and **Description**, and click **Next**.

Step 3 In the **Add a group** window that is displayed, select the devices you want to add to this group and click **Create Group**.

Step 4 Click **Close** or **Create another group**.

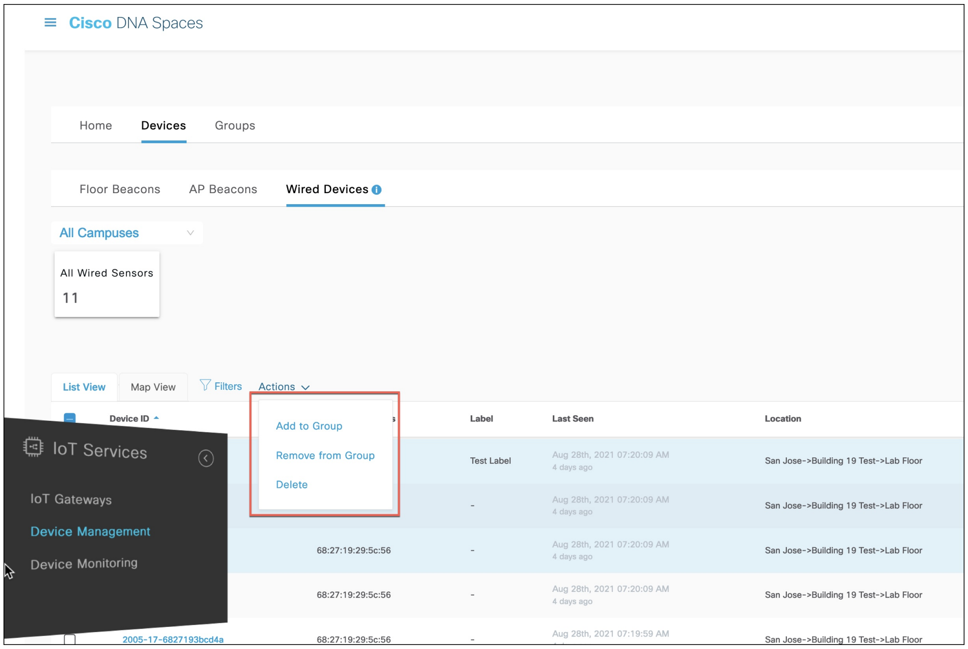
Step 5 To add one or more devices to the created group, click the **Devices** tab and then click one of the following:

- **Floor Beacons**
- **AP Beacons**
- **Wired Devices**

Step 6 In the **List View**, check the check boxes of the devices to add.

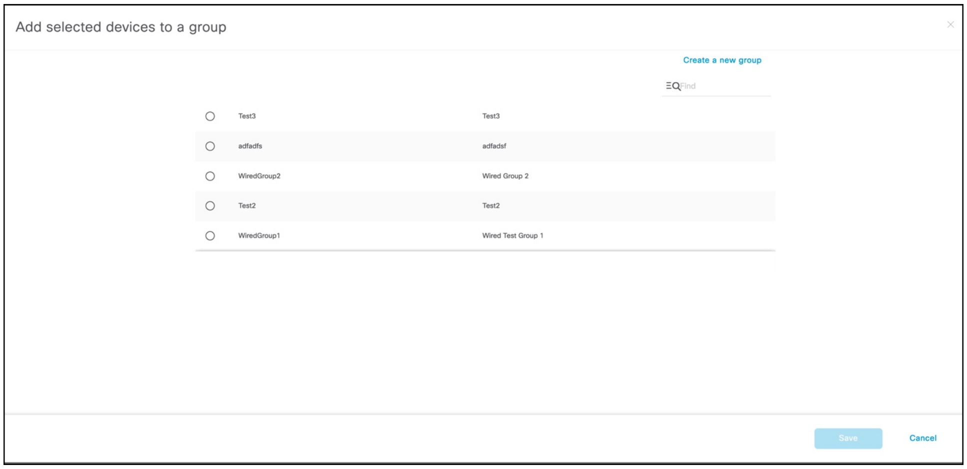
Step 7 Choose **Actions** > **Add to Group**.

Figure 40: Add to Group



	Device ID	s	Label	Last Seen	Location
			Test Label	Aug 28th, 2021 07:20:09 AM 4 days ago	San Jose->Building 19 Test->Lab Floor
			-	Aug 28th, 2021 07:20:09 AM 4 days ago	San Jose->Building 19 Test->Lab Floor
		68:27:19:29:5c:56	-	Aug 28th, 2021 07:20:09 AM 4 days ago	San Jose->Building 19 Test->Lab Floor
		68:27:19:29:5c:56	-	Aug 28th, 2021 07:20:09 AM 4 days ago	San Jose->Building 19 Test->Lab Floor
□	2005-17-6827193bcd4a	68:27:19:29:5c:56	-	Aug 28th, 2021 07:19:59 AM	San Jose->Building 19 Test->Lab Floor

Figure 41: Add to Group



Add selected devices to a group

○	Test3	Test3
○	adfadfs	adfadsf
○	WiredGroup2	Wired Group 2
○	Test2	Test2
○	WiredGroup1	Wired Test Group 1

Step 8 Click the group to which devices should be added.

Step 9 (Optional) Click the **Groups** tab to see the group you created. Click the group name to see the devices in the group. You can also edit the group details from this window.

Note You can delete a group by checking the check box adjacent to a group and choosing **Actions > Delete Group**.

PART IV

Troubleshooting

- Switch, on page 43
- Troubleshooting IoT service (wired), on page 47
- IoX Application, on page 49
- 802.1x, on page 55

CHAPTER 6

Switch

- Switch , on page 43

Switch

What TDL subscriptions are created

The following table shows you the list of TDL subscriptions created for a switch.

Switch Subscriptions

Subscription Number	TDL	Update Policy	Description
222	/services;serviceName=ios_oper/platform_component	1 hour	Used for device discovery
223	/services;serviceName =ios_emul_oper/device_hardware;singleton_id =0/device_system_data;singleton_id=0	3 seconds	Device system information

The following table shows you the list of TDL subscriptions created for the switch port status.

Subscription Number	TDL	Update Policy	Description
224	/services;serviceName=ios_emul_oper/interface	On charge	Switch port interface status

The following table shows you the list of TDL subscriptions created for the switch PoE subscription.

Subscription Number	TDL	Update Policy	Description
225	/services;serviceName =ios_oper/platform_component;cname =Switch1/platform_properties	5 seconds	Switch platform properties
226	/services;serviceName=ios_oper/poe_module	4 seconds.	Switch POE Module
227	/services;serviceName=ios_oper/poe_port_detail	3 seconds	Switch POE Port

How do I verify the TDL subscriptions are created and valid?

Run the command **show telemetry ietf subscription all** command on the switch.

The command displays the subscriptions, the subscription type, and if a subscription is valid. switch creates five different subscriptions 222-227.

```
Device# show telemetry ietf subscription all

  Telemetry subscription brief

  ID                Type        State       Filter type
  --------------------------------------------------------
  222               Configured  Valid       tdl-uri
  223               Configured  Valid       tdl-uri
  224               Configured  Valid       tdl-uri
  225               Configured  Valid       nested-uri
  226               Configured  Valid       tdl-uri
  227               Configured  Valid       tdl-uri
```

What is the TDL status?

Run the **show telemetry ietf subscription ID receiver** command on the switch.

The command displays the TDL subscriptions status.

```
Device# show telemetry ietf subscription 222 receiver
Telemetry subscription receivers detail:

  Subscription ID: 222
  Address: 192.168.46.20
  Port: 8004
  Protocol: cloud-native
  Profile:
  Connection: 32037
  State: Connected
  Explanation:
```

The switch has five different subscriptions ranging from 222-227 which can be used as the **Subscription ID**. Check if the **Address** is the IP address of the Cisco Spaces: Connector. Also check if the **State** is **Connected**.

What commands are run on the switch?

When a switch port status changes to UP, Cisco Spaces: Connector polls the switch for any potential switch port identity information. The connector executes the NETCONF GET command, which is similar to the **show dot1x interface GigabitEthernet 1/0/1 details** command.

Below is the output of the NETCONF command.

```
<filter xmlns=\"urn:ietf:params:xml:ns:netconf:base:1.0\">
    <identity-oper-data xmlns=\"http://cisco.com/ns/yang/Cisco-IOS-XE-identity-oper\">
        <session-context-data>
            <intf-iifid>___interface_index___</intf-iifid>
        </session-context-data>
    </identity-oper-data>
</filter>
```

Below is the output of the NETCONF command.

CHAPTER 7

Troubleshooting IoT service (wired)

- Connector, on page 47

Connector

What are the metrics available in connector for IoT service (wired)?

Table 2: General Information

Metrics Name	Metrics Description
Mac Address	MAC address of the IoT service (wired)on the connector
IP Address	IP address of the IoT service (wired) on the connector
Log Level	Logging level used for the IoT service (wired)
Incoming gRPC rate	Incoming gRPC events per second
Incoming TDL rate	Incoming TDL events per second
Incoming TDL failed rate	Incoming TDL failed events per second
Last 5 minutes Incoming gRPC rate	Last 5 minutes for the incoming gRPC rate
Last 5 minutes TDL rate	Last 5 minutes for the incoming TDL rate
Last 5 minutes TDL failed rate	Last 5 minutes for the incoming failed TDL rate
Active gRPC connection count	Active gRPC connection count

Table 3: Switches

Metrics Name	Metrics Description
Host	IP address of the switch

Metrics Name	Metrics Description
Version	Parsed version of the switch
POE Port Meter Count	POE Port Meter current counter value
POE Port Meter Rate	POE Port Meter rate per second
POE Module Meter Count	—
PoE Module Meter Rate	—
Switch Power Meter Count	—
Switch Power Meter Rate	—
Switch Port Identity Meter Count	—
Switch Port Identity Meter Rate	—

Table 4: Smart PDUs

Metrics Name	Metrics Description
Host	IP address of the PDU
Smart PDU Global Meter Count	—
Smart PDU Global Meter Rate	—
Smart PDU Port Meter Count	—
Smart PDU Port Meter Rate	—

Table 5: Hella Cameras

Metrics Name	Metrics Description
Host	IP address of the PDU
Hella Incoming Counting Meter Count	—
Hella Incoming Counting Meter Rate	—
Hella Incoming Zones Meter Count	—
Hella Incoming Zones Meter Rate	—

CHAPTER 8

IoX Application

- IoX Application, on page 49

IoX Application

How do I verify the IoX Application is running on the switch?

Run the **show app-hosting list** command.

App State should be RUNNING to indicate that it is running.

```
Switch# show app-hosting list
App id                                   State
---------------------------------------------------------
cisco_dnas_wired_iox_app                 RUNNING
```

How do I start an interactive shell session for the IoX Application?

Run the **app-hosting connect appid cisco_dnas_wired_iox_app session /bin/bash** command.

This command starts a shell that runs inside the IoX Application container.

```
Switch# app-hosting connect appid cisco_dnas_wired_iox_app session /bin/bash
root@5c423778c2d6:/var/dnas_wired#
```

How can I see the logs for the IOx application?

Run the **tail -F /tmp/dnas_ble.log** command.

You can see the logs for the IoX Application.

```
root# tail -F /data/logs/dnas_wired.log
Tue Jun 15 04:26:36 2021 [INFO]: Starting DNA Spaces Wired IOx Application
Tue Jun 15 04:26:36 2021 [INFO]: gRPC Server IP Address: 10.22.243.59
Tue Jun 15 04:26:36 2021 [INFO]: gRPC Server Port: 8003
Tue Jun 15 04:26:36 2021 [INFO]: gRPC Server Token: eyJhbGciOiJIUzI1NiIsInR5cCI66
IkpXVCJ9.eyJ0aWQiOjE2Mzc0LCJjaWQiOjMyMjQ5NzMxMDYzOTkwNzEwMDAsImVwIjoiMTAuMjIuMjQQ
zLjU5OjgwMDAiLCJpYXQiOjE2MjIwOTQ5OTV9.KOK6EYM6_8r7nTs2U-13CotT8S-qOUphKf7s57L-Kxx
U
Tue Jun 15 04:26:36 2021 [INFO]: Application Host ID: 44:b6:be:37:a0:00
Tue Jun 15 04:26:36 2021 [INFO]: Application Host IP: 10.22.243.63
Tue Jun 15 04:26:36 2021 [INFO]: Product ID: C9300-24U
Tue Jun 15 04:26:36 2021 [INFO]: Attempting to connect using MAC address: 52:54::
dd:59:c2:51
Tue Jun 15 04:26:36 2021 [INFO]: HTTP Post: https://10.22.243.59:8000/streaming//
token/validate Post String: {"apMacaddress":"52:54:dd:59:c2:51","streamAuthKey"::
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aWQiOjE2Mzc0LCJjaWQiOjMyMjQ5NzMxMDYzOTT
kwNzEwMDAsImVwIjoiMTAuMjIuMjQzLjU5OjgwMDAiLCJpYXQiOjE2MjIwOTQ5OTV9.KOK6EYM6_8r7nn
Ts2U-13CotT8S-qOUphKf7s57L-KxU"}
Tue Jun 15 04:26:36 2021 [INFO]: HTTP Post Resonse from perform
Tue Jun 15 04:26:36 2021 [INFO]: HTTP Post Resonse code: 200
Tue Jun 15 04:26:36 2021 [INFO]: HTTP Post Response: {"endpoint":"10.22.243.59:88
000","streamAccessKey":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aWQiOjE2Mzc0LCJJ
jaWQiOjMyMjQ5NzMxMDYzOTkwNzEwMDAsImlhdCI6MTYyMzczMTIyNCwiZXhwIjoxNjIzODE3NjI0fQ..
```

How do I monitor metrics in the IoX Application?

Run the **tail -F /data/logs/dnas_wired_metrics.log** command.

This command reads the log file for IoX Application metrics. The log file updates metrics every 5 minutes. The log file updates any detected MAC addresses every 5 minutes.

Metrics Name	Metrics Description
Application Version	IoX Application version currently running
Start Time	Local time on the AP that the application was started and indicates how long the application has been running
Total Physical Memory	Total physical memory used for the container
Physical Memory Used	Physical memory used for the container
Total AP Percent CPU Used	Percent CPU used in the container
Process Virtual Memory	Process virtual memory used
Process Physical Memory	Process physical memory used
Process CPU Used	Process CPU Used
gRPC Reconnect Count	Number of times gRPC was reconnected while the application has been running
Log Rotation Count	Number of times the *dnas_ble.log* file has been rotated while the application has been running
Event Data Message Count	Number of scan data messages sent since the application started
Event Data Message Rate Per Second	Number of scan data messages sent per second

Metrics Name	Metrics Description
Source MAC Dest MAC UUID Name Count Interval Last-heard	Periodically the scanned are dumped in the log with the attributes Source MAC: Source MAC address of the device scanned Dest MAC: Destination MAC address of the device scanned UUID: Universal Unique Identifier NAME: Device name Count: Number of times the device was heard since last scan values dumped Interval: Number of seconds between each device scan Last-heard: Last heard since the last scan values dumped

```
root# tail -F /data/logs/dnas_wired_metrics.log
Tue Jun 15 07:08:12 2021 [INFO]: Application Version: 1.0.16
Tue Jun 15 07:08:12 2021 [INFO]: Start Time: Tue Jun 15 06:03:12 2021 Up Time:
0000D:01H:05M:00S
Tue Jun 15 07:08:12 2021 [INFO]: Total Physical Memory: 6443 MB
Tue Jun 15 07:08:12 2021 [INFO]: Physical Memory Free: 868 MB
Tue Jun 15 07:08:12 2021 [INFO]: Physical Memory Used: 5574 MB
Tue Jun 15 07:08:12 2021 [INFO]: Total Physical Shared Memory: 277 MB
Tue Jun 15 07:08:12 2021 [INFO]: Total Physical Buffer Memory: 390 MB
Tue Jun 15 07:08:12 2021 [INFO]: Total AP Percent CPU Used: 1.723203
Tue Jun 15 07:08:12 2021 [INFO]: Process Virtual Memory: 655436 kB
Tue Jun 15 07:08:12 2021 [INFO]: Process Physical Memory: 25820 kB
Tue Jun 15 07:08:12 2021 [INFO]: Process CPU Used: 0.100417
Tue Jun 15 07:08:12 2021 [INFO]: gRPC Reconnect Count: 0
Tue Jun 15 07:08:12 2021 [INFO]: Log Rotation Count: 20
Tue Jun 15 07:08:12 2021 [INFO]: Event Data Message Count: 8284
Tue Jun 15 07:08:12 2021 [INFO]: Event Data Message Rate Per Second: 20
Tue Jun 15 07:08:12 2021 [INFO]: Source MAC        Dest MAC          UUID
          Name            Count  Interval    Last-heard
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 0001-17-6827193bcd4a
          i0.1_POWER      44     3.87        0000D:00H:00M:01S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 0002-17-6827193bcd4a
          i0.2_ENERGY     44     3.87        0000D:00H:00M:01S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 2002-17-6827193bcd4a
          d0.2_RGB        44     3.87        0000D:00H:00M:01S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 2004-17-6827193bcd4a
          d0.4_ALS        43     7.74        0000D:00H:00M:01S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 2005-17-6827193bcd4a
          d0.5_PIR        44     3.87        0000D:00H:00M:01S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 2103-17-6827193bcd4a
          d1.3_R          232    0.02        0000D:00H:00M:00S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 2104-17-6827193bcd4a
          d1.4_ALS        231    0.04        0000D:00H:00M:00S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 2106-17-6827193bcd4a
          d1.6_TEMP       226    0.04        0000D:00H:00M:01S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 2107-17-6827193bcd4a
          d1.7_HUM        225    0.02        0000D:00H:00M:01S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 2108-17-6827193bcd4a
          d1.8_AQ         130    0.03        0000D:00H:00M:01S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed 2109-17-6827193bcd4a
          d1.9_CO2        41     0.03        0000D:00H:00M:01S
Tue Jun 15 07:08:12 2021 [INFO]: 68:27:19:3b:cd:4a 00:50:56:87:db:ed e4c5-17-6827193bcd4a
                          68     1.47        0000D:00H:00M:01S
```

What files exist in the IoX Application?

The following log files are created while the IoX Application is running. These files are located in the */data/logs* directory.

Log File Name	**Description**
dnas_wired.log	Active log file for debug message for the application.
dnas_wired_1.log	Rotated log file for the debug messages for the application
dnas_wired_metrics.log	Active log file for metric messages
dnas_wired_metrics_1.log	Rotated log file for metric messages
dnas_wired_stdout.log	Standard output and standard error messages are written to the file
dnas_wired_last_restart.log	If the IoX Application is restarted, then the *dnas_wired_last_restart.log* file is copied to this file. You can use this file to troubleshoot the reason for the restart
dnas_wired_metrics_last_restart.log	If the IoX Application is restarted, then the *dnas_wired_metrics_last_restart.log* file is copied to this file. You can use it to troubleshoot the reason for the restart.

The following are binary files installed specifically for the IoX Application. All the files are located in the */var/dnas_wired* directory.

File Name	**Description**
dnas_wired_iox_app	IoX Application binary which scan for wired devices
dnas_wired_iox_app_start.sh	Script to start and in the case of a failure restart the application again

How do I verify that the IoX Application is receiving span session data?

pen the interactive shell of the IoX Application. Refer to How do I start an interactive shell session for the IoX Application?

Run the **tcpdump -i** *eth1* command.

eth1 is the interface that receives the span traffic. This command begins a TCP dump on the *eth1* interface.

The dump should show that the interface is receiving GRE. If the GRE traffic is not seen, then you can conclude that the span session is not working as expected.

```
root# tcpdump -i eth1

07:38:03.153932 IP 124.124.124.5 > 124.124.124.10: GREv0, seq 0, length 130: gre-proto-0x88be
07:38:03.154147 IP 124.124.124.5 > 124.124.124.10: GREv0, seq 0, length 186: gre-proto-0x88be
07:38:03.154214 IP 124.124.124.5 > 124.124.124.10: GREv0, seq 0, length 314: gre-proto-0x88be
07:38:03.166872 IP 124.124.124.5 > 124.124.124.10: GREv0, seq 0, length 74: gre-proto-0x88be
07:38:03.173112 IP 124.124.124.5 > 124.124.124.10: GREv0, seq 0, length 74: gre-proto-0x88be
07:38:03.173119 IP 124.124.124.5 > 124.124.124.10: GREv0, seq 0, length 74: gre-proto-0x88be
07:38:03.173128 IP 124.124.124.5 > 124.124.124.10: GREv0, seq 0, length 138: gre-proto-0x88be
07:38:03.173764 IP 124.124.124.5 > 124.124.124.10: GREv0, seq 0, length 610: gre-proto-0x88be
07:38:03.173772 IP 124.124.124.5 > 124.124.124.10: GREv0, seq 0, length 130: gre-proto-0x88be
```

Why am I not seeing span session data in the IoX Application?

First, ensure that you have enabled ip routing on the switch using the **show running-config | inc ip routing** command.

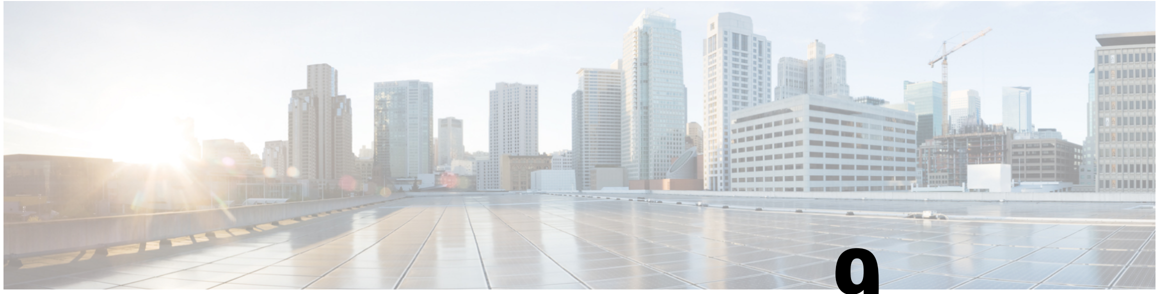
This command displays the running configuration and show if you have enabled ip routing.

```
switch# show running-config | inc ip routings

ip routing
```

If you have not enabled ip routing on the switch, then run the **ip routing** command in the configuration mode.

```
switch# configure terminal
switch(config)# ip routing
switch(config)# exit
```



CHAPTER 9

802.1x

The following section is used to capture wired user authentication information. This information is used by Cisco Spaces apps such as Right Now, where dot1x has been configured.

- 802.1x, on page 55

802.1x

The following section is used to capture wired user authentication information. This information is used by Cisco Spaces apps such as Right Now, where dot1x has been configured.

How to enable 802.1x port-based authentication on the switch?

There are several ways to configure 802.1x port-based authentication on a switch. This task shows you one of the way to enable 802.1x.

Step 1 aaa new-model

This command enables AAA.

Step 2 aaa authentication dot1x default group radius

This command creates a series of authentication methods to determine user privilege. If the user has the necessary previlige, the device can communicate with the AAA server.

Step 3 dot1x system-auth-control

This command globally enables 802.1X port-based authentication.

Example:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# end
```

How to enable 802.1x port-based authentication on the switch interface?

This task shows you how to enable 802.1x port-based authentication on the switch interface.

Step 1 authentication port-control auto

This command enables port authentication.

Step 2 dot1x pae authenticator

This command enables 802.1x port authentication.

Example:

```
Switch# configure terminal
Switch(config)# interface <interface-id>
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# end
```

How to configure the switch for RADIUS-server communication?

This task shows you how to configure a switch for RADIUS-server communication.

Step 1 radius server RADIUS

This command configures the RADIUS server.

Step 2 address ipv4 *radius-ip* auth-port 1645 acct-port 1646

This command configures the server IP address and port.

Step 3 key*var*

This command configures the RADIUS key.

Example:

```
Switch# configure terminal
Switch(config)# radius server RADIUS
Switch(config)# address ipv4 <radius-ip> auth-port 1645 acct-port 1646
Switch(config)# key <key>
Switch(config)# end
```

How to view the current 802.1x status for a switch interface?

The following command displays the details of a switch interface.

show dot1x interface *interface-id*

```
Switch# show dot1x interface GigabitEthernet 1/0/1 details
```

```
Dot1x Info for GigabitEthernet1/0/1
--------------------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------

EAP Method                = PEAP
Supplicant                = f076.1cc7.8386
Session ID                = 000000000000000BA3185562
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
```