Cisco Spaces: Connector 3 Configuration Guide

First Published: 2022-06-24

Last Modified: 2025-08-05

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.

CONTENTS

PREFACE

CHAPTER 1

PART I

CHAPTER 2

PART II

CHAPTER 3

Preface

Audience

This document is meant for Cisco Spaces network and IT administrators who deploy Cisco Spaces to monitor, manage, and optimize usage of assets in an organization.

Conventions

This document uses the following conventions.

Table 1: Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	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. Otherwise, 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.

Convention	Indication
!, #	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.

Tip Means the following information will help you solve a problem.

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

Related Documentation

Cisco Spaces

Cisco Spaces Configuration Guide

Connector

- *Cisco Spaces: Connector Configuration Guide*
- *Cisco Spaces: Connector Command Reference Guide*
- *Release Notes for Cisco Spaces: Connector*

IoT Service

- *Cisco Spaces: IoT Service Configuration Guide (Wireless)*
- *Cisco Spaces: IoT Service Configuration Guide (Wired)*

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.

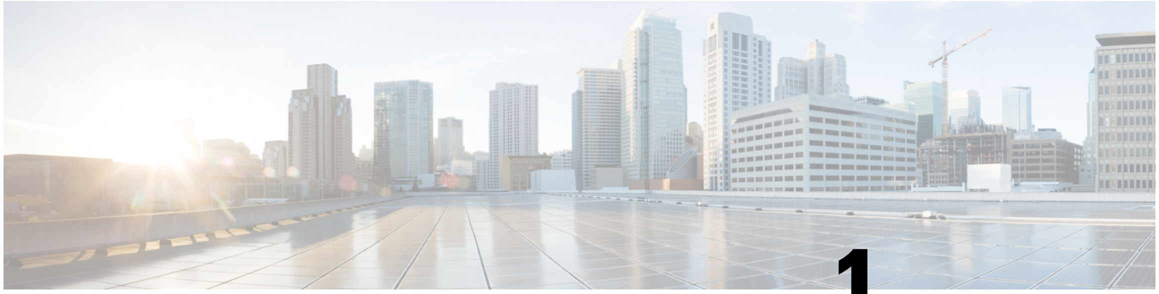
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



CHAPTER 1

Overview

Note Starting from December 2023, Cisco Spaces: Connector 2.x has entered maintenance mode, and only security updates will be available up to June 2024. Extended support is limited to critical bug fixes, offered until October 2024. We strongly recommend that you upgrade to connector 3. To migrate from Connector 2.x to Connector 3, see Migrate from Connector 2.x to Connector 3.

Introduction to Connector 3

Cisco Spaces: Connector Release 3 (subsequently referred to as Connector 3) is a fully redesigned version of the Cisco Spaces: Connector Release 2.x, with the capability to efficiently manage multiple services that connect to different network devices such as wireless controllers, access points (APs), and switches. connector gathers and aggregates data from these devices and sends the data to Cisco Spaces.

With connector 3, you can do the following:

- Add or remove new services from Cisco Spaces.
- Perform advanced troubleshooting with the debugging, log upload, and restart functionalities in Cisco Spaces.
- Obtain detailed metrics for each service, such as, CPU, memory, connectivity, and up or down status.
- Configure Virtual IP address (VIP) pairs or active-active pairs that allow for high availability. You can view details of each instance that is a part of a high-availability pair.
- Monitor connector 3 and device status that are aggregated from each instance of connector.
- View how services are running on each instance, their upgrade status, and so on.
- Perform actions on an instance, such as restarting of services.
- Configure instances for connector. Device status is aggregated from each connector instance for monitoring.

Connector 3 sends data to Cisco Spaces over HTTPS; a proxy can also be used to route data.

See Initial Setup, Upgrading the Connector, and Migrating from Connector 2.x to Connector 3.

Note The term wireless controller is used in this document to collectively refer to the following:

- Cisco AireOS Wireless Controller or AireOS controller
- Cisco Catalyst 9800 Series Wireless Controller or Catalyst 9800 controller
- Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)

PART I

Getting Started

CHAPTER 2

Prerequisites

Prerequisites for Configuring Connector 3

- Make sure you allow access to necessary endpoints based on the region of your Cisco Spaces account. Refer to the following table for the endpoints that must be enabled:

  Table 2: Enable Endpoints

Cisco Spaces Account	Endpoint to be Enabled
https://dnaspaces.io	https://connector.dnaspaces.io
https://dnaspaces.eu	https://connector.dnaspaces.eu
https://ciscospaces.sg	https://connector.ciscospaces.sg

- The Cisco Spaces: Connector works as expected when two tokens are generated and configured on two separate instances. However, if an additional token is generated and configured on a third connector instance, a certificate will not be issued, causing the hotspot to fail.

  Ensure that no more than two tokens are generated for each Connector and configured on the Cisco Spaces: Connector instances to prevent hotspot failures.

- Connector needs to be able to reach a Domain Name System (DNS) server. If you set up an explicit proxy, ensure that Connector 3 maintains the ability to communicate through this proxy.

- VMware ESXi 7.0 or 8.0.

- VMware vCenter 7.0 or 8.0

- Virtual machine size: Advanced 2 (Recommended)

- Minimum bandwidth required: 4 Mbps

Note Make sure that the x86-64-v2 CPU is available for Enterprise Linux 9. Also, ensure that the x86-64-v2 CPU supports the following flags: SSE3, SSE4_1, SSE4_2, and SSSE3.

Recommended Deployment Architecture

The following is the recommended deployment architecture for connector:

- Virtual machine size (vCPU): 2
- RAM: 4 GB
- Hard Disk: 120 GB

PART II

Configuration

CHAPTER 3

Initial Setup

Initial Setup of Cisco Spaces: Connector

To get the Cisco Spaces: Connector up and running, perform these steps:

1. Install connector 3 in your local deployment network. See Deploying the Connector 3 OVA (Single Interface), on page 65

2. On the Cisco Spaces dashboard, create a Cisco Spaces: Connector and generate a token for connector. See Activating Connector 3 on Cisco Spaces, on page 10

3. Configure this token on the deployed Cisco Spaces: Connector. This establishes a connection between Cisco Spaces and the deployed Cisco Spaces: Connector. The equivalent connector 3 (based on the token) on the Cisco Spaces now turns active. See Activating Connector 3 on Cisco Spaces, on page 10

4. Add the services based on your required workflow on Cisco Spaces.

Table 3: Enabling Services

Service	Link
Service manager service	Enabled by default.
IoT service (wireless)	For information, see Configure IoT Service (Wireless), on page 166.
IoT service (wired)	For information, see Configure IoT Service (Wireless), on page 166.
Hotspot service	For information, see Configure Hotspot Service, on page 193.
Local firehose service	For information, see Configure Hotspot Service, on page 193.

Activating Connector 3 on Cisco Spaces

This section provides information about how to activate a deployed connector on your Cisco Spaces account.

Using the following procedure, you generate a token for a deployed connector that you want to add to your Cisco Spaces account. Note that you need a separate token for each deployed connector. Each token is specific to a connector and hence enables Cisco Spaces to identify and connect to connector.

Cisco Spaces supports multiple connectors, and you can associate each connector with one or multiple wireless controllers.

Note A Cisco Spaces: Connector instance can communicate with only one Cisco Spaces account at a time.

Before you begin

Download and deploy the Cisco Spaces: Connector OVA. See Deploying the Connector 3 OVA (Single Interface), on page 65

Procedure

Step 1 Log in to **Cisco Spaces**.

Note
The Cisco Spaces URL is region-dependent.

Step 2 From the left navigation pane, choose **Setup** > **Wireless Networks**.

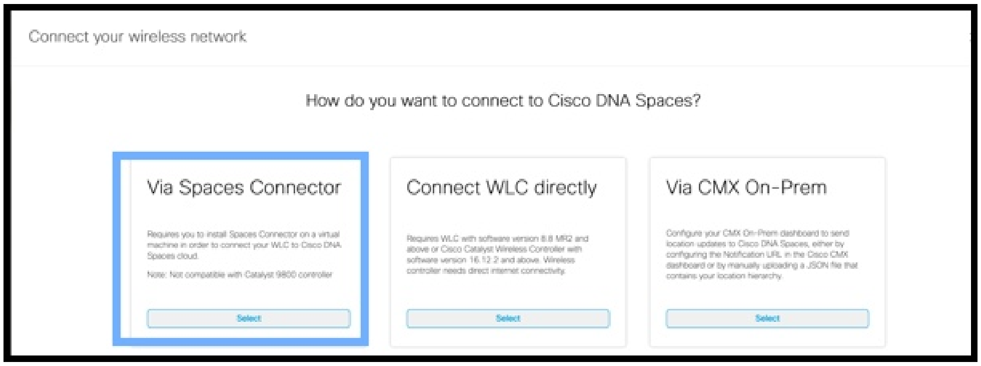
Step 3 In the **Get your wireless network connected with Cisco DNA Spaces** area, click **Add New**.

Step 4 In the **Cisco AireOS Controller/Catalyst 9800 Wireless Controller** area, click **Select.**

Figure 1: Choose Cisco AireOS Controller/Catalyst 9800 Wireless Controller

Step 5 In the **Via Spaces Connector** area, click **Select**.

Figure 2: Via Spaces Connector



Connect your wireless network

How do you want to connect to Cisco DNA Spaces?

Via Spaces Connector

Requires you to install Spaces Connector on a virtual machine in order to connect your WLC to Cisco DNA Spaces cloud.

Note: Not compatible with Catalyst 9800 controller

Select

Connect WLC directly

Requires WLC with software version 8.8 MR2 and above or Cisco Catalyst Wireless Controller with software version 16.12.2 and above. Wireless controller needs direct internet connectivity.

Select

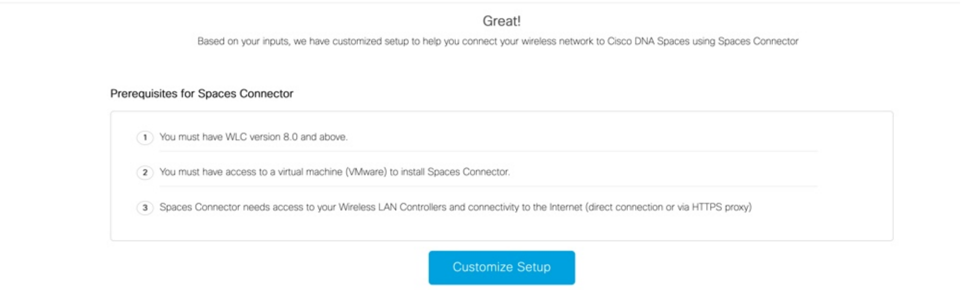
Via CMX On-Prem

Configure your CMX On-Prem dashboard to send location updates to Cisco DNA Spaces, either by configuring the Notification URL in the Cisco CMX dashboard or by manually uploading a JSON file that contains your location hierarchy.

Select

Step 6 In the **Prerequisites for Spaces Connector** dialog box, click **Continue Setup**.

Figure 3: Read Prerequisites for Spaces Connector



Great!

Based on your inputs, we have customized setup to help you connect your wireless network to Cisco DNA Spaces using Spaces Connector

Prerequisites for Spaces Connector

1 You must have WLC version 8.0 and above.

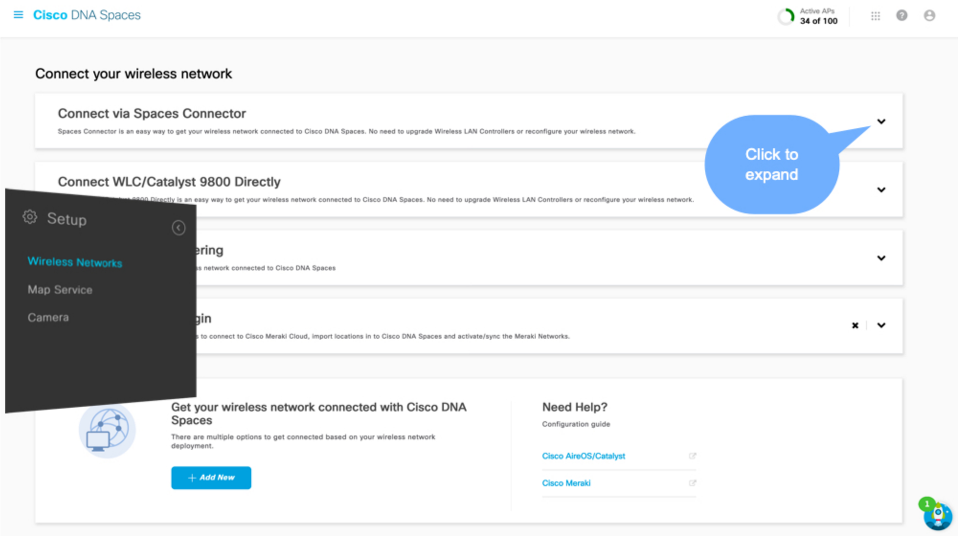
2 You must have access to a virtual machine (VMware) to install Spaces Connector.

3 Spaces Connector needs access to your Wireless LAN Controllers and connectivity to the Internet (direct connection or via HTTPS proxy)

Customize Setup

Step 7 Expand the **Connect via Spaces Connector** area using the respective drop-down arrow.

Figure 4: Expand Connect via Spaces Connector



Cisco DNA Spaces

Active APs 34 of 100

Connect your wireless network

Connect via Spaces Connector

Spaces Connector is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.

Connect WLC/Catalyst 9800 Directly

9800 Directly is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.

ering

s network connected to Cisco DNA Spaces

gin

to connect to Cisco Meraki Cloud, import locations in to Cisco DNA Spaces and activate/sync the Meraki Networks.

Get your wireless network connected with Cisco DNA Spaces

There are multiple options to get connected based on your wireless network deployment.

Need Help?

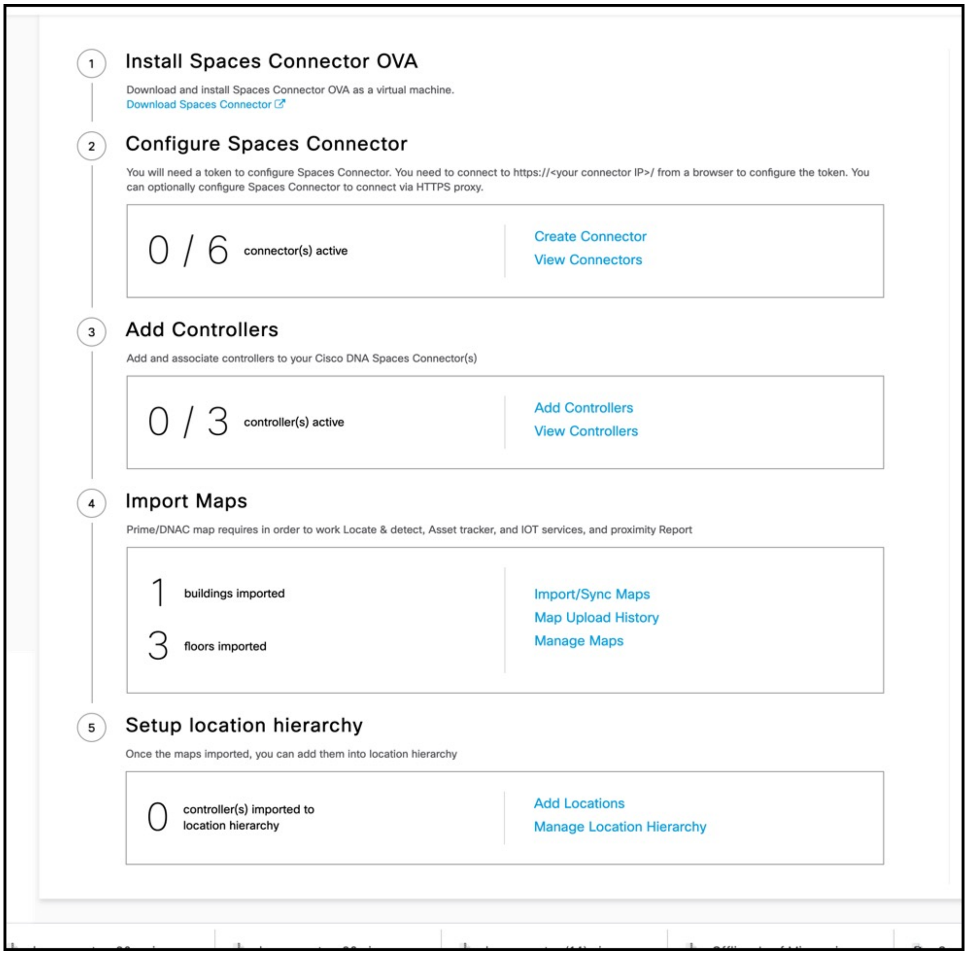
Configuration guide

Cisco AireOS/Catalyst

Cisco Meraki

Step 8 In the displayed list of steps, in the **Configure Spaces Connector** area, click **Create Connector**.

Figure 5: Connect via Spaces Connector > Create Connector



1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.
Download Spaces Connector

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

0 / 6 connector(s) active

3 Add Controllers

Add and associate controllers to your Cisco DNA Spaces Connector(s)

0 / 3 controller(s) active

4 Import Maps

Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

1 buildings imported

3 floors imported

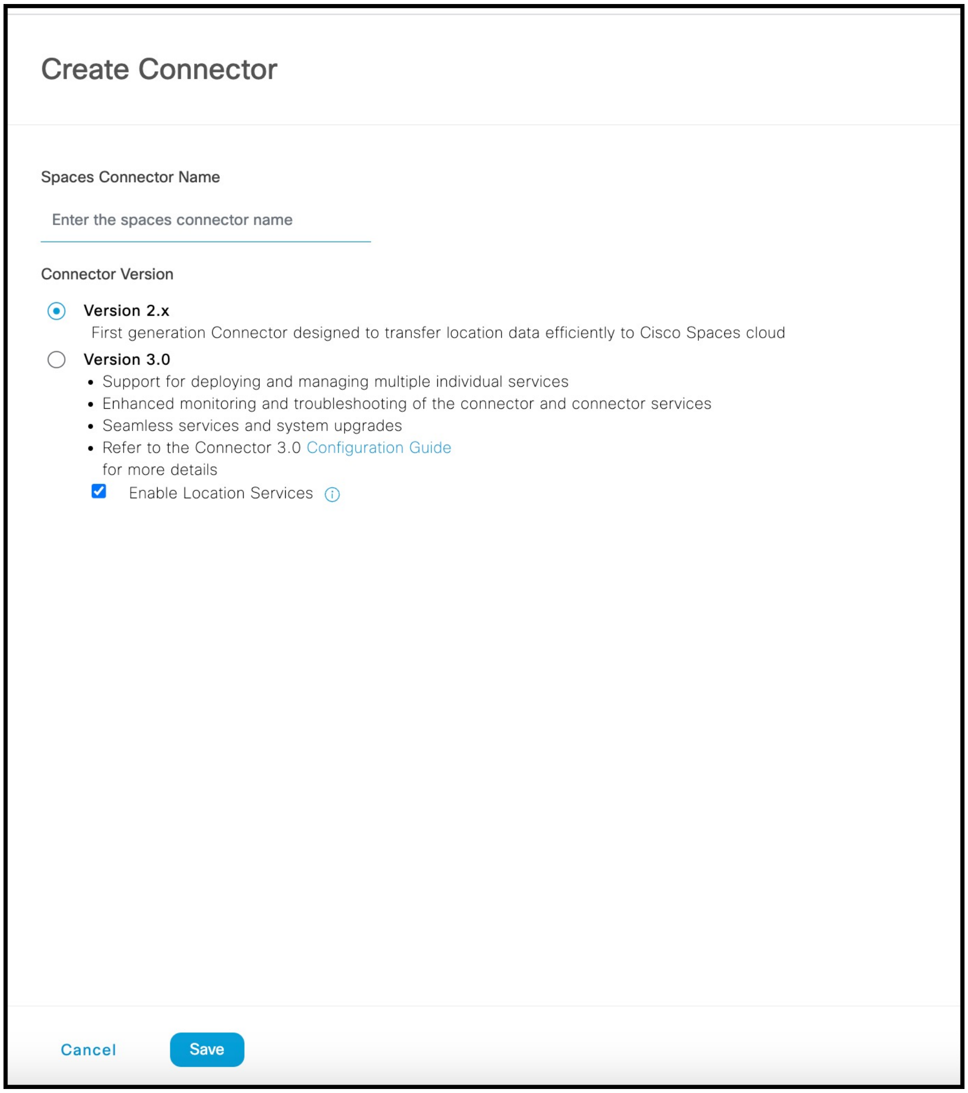
5 Setup location hierarchy

Once the maps imported, you can add them into location hierarchy

0 controller(s) imported to location hierarchy

Step 9 In the **Create connector** window that is displayed, enter a name for connector, and click **Version 3.0 (beta).** as the **Connector Version**, and click **Save**.

Figure 6: Name and Version of Connector



Create Connector

Spaces Connector Name

Enter the spaces connector name

Connector Version

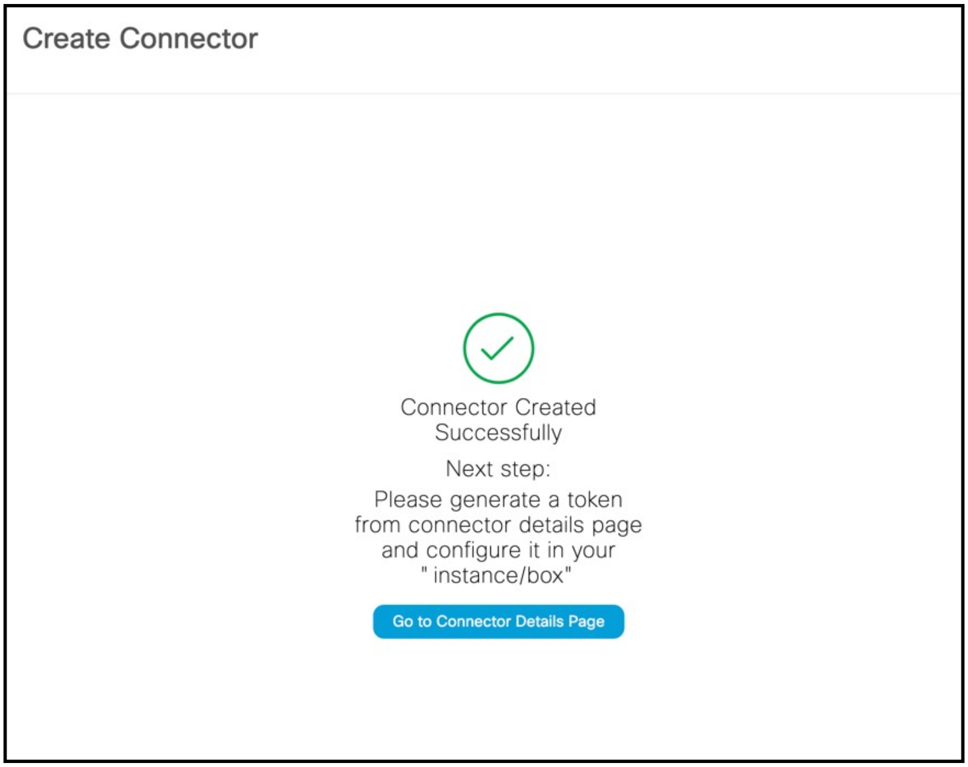
● Version 2.x
First generation Connector designed to transfer location data efficiently to Cisco Spaces cloud

○ Version 3.0
- Support for deploying and managing multiple individual services
- Enhanced monitoring and troubleshooting of the connector and connector services
- Seamless services and system upgrades
- Refer to the Connector 3.0 Configuration Guide for more details

☑ Enable Location Services ⓘ

Connector is successfully created. Click **Go to Connector Details** Page.

Figure 7: Connector Created Successfully



Create Connector

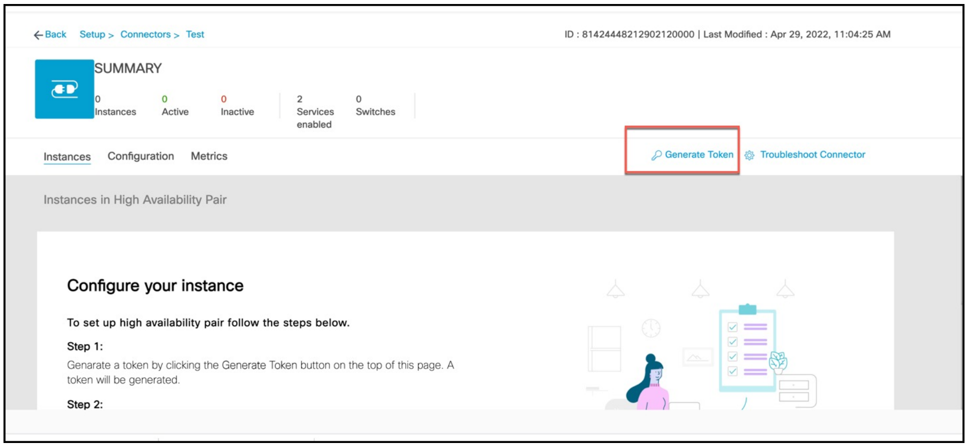
Connector Created Successfully

Next step:

Please generate a token from connector details page and configure it in your " instance/box"

Step 10 In the connector details window, you can see a summary of the configurations for this connector. Click **Generate Token.**

Figure 8: Generate Token



ID : 81424448212902120000 | Last Modified : Apr 29, 2022, 11:04:25 AM

SUMMARY

0 Instances

0 Active

0 Inactive

2 Services enabled

0 Switches

Instances in High Availability Pair

Configure your instance

To set up high availability pair follow the steps below.

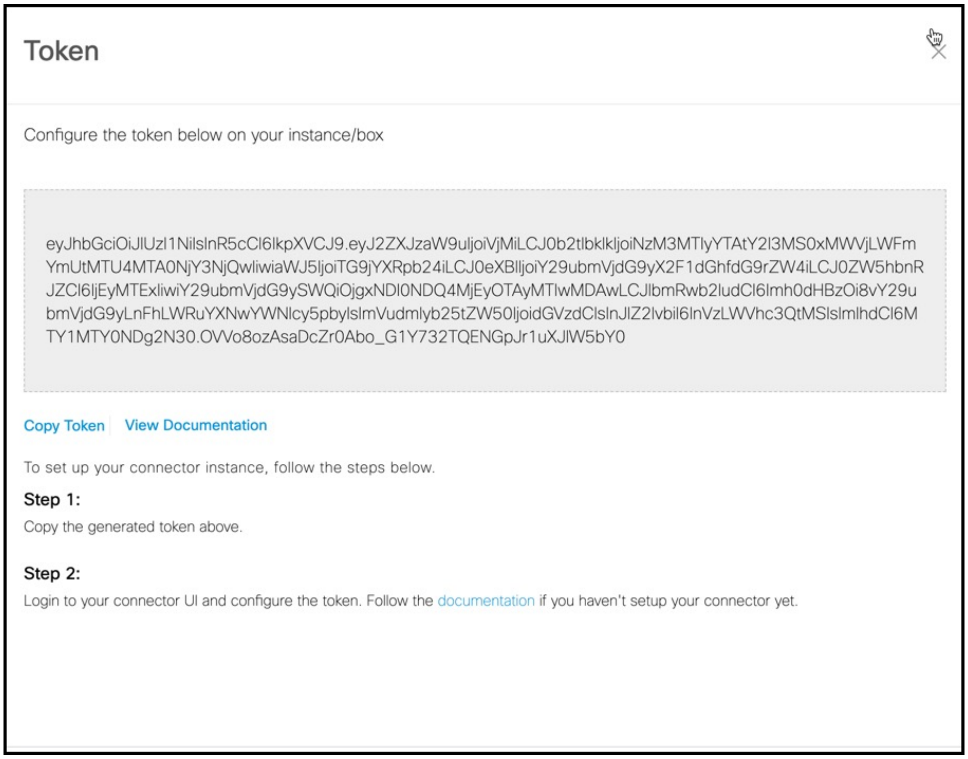
Step 1:

Genarate a token by clicking the Generate Token button on the top of this page. A token will be generated.

Step 2:

Step 11 In the **Token** window that is displayed, click **Copy Token**.

Figure 9: Copy Token



Token

Configure the token below on your instance/box

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2ZXJzaW9uIjoiVjMiLCJ0b2tlbklkIjoiNzM3MTIyYTAtY2I3MS0xMWVjLWFm
YmUtMTU4MTA0NjY3NjQwIiwiaWJ5IjoiTG9jYXRpb24iLCJ0eXBlIjoiY29ubmVjdG9yX2F1dGhfdG9rZW4iLCJ0ZW5hbnR
JZCI6IjEyMTExIiwiY29ubmVjdG9ySWQiOjgxNDI0NDQ4MjEyOTAyMTIwMDAwLCJlbmRwb2ludCI6Imh0dHBzOi8vY29u
bmVjdG9yLnFhLWRuYXNwYWNlcy5pbyIsImVudmlyb25tZW50IjoidGVzdCIsInJlZ2lvbiI6InVzLWVhc3QtMSIsImlhdCI6M
TY1MTY0NDg2N30.OVVo8ozAsaDcZr0Abo_G1Y732TQENGpJr1uXJlW5bY0
```

Copy Token | View Documentation

To set up your connector instance, follow the steps below.

Step 1:

Copy the generated token above.

Step 2:

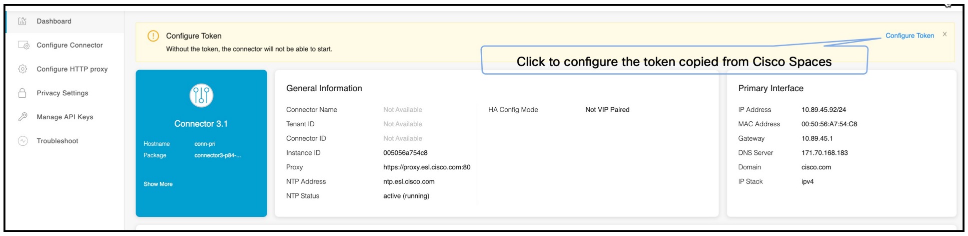
Login to your connector UI and configure the token. Follow the documentation if you haven't setup your connector yet.

Step 12 Open the connector GUI.

Step 13 (Optional) If your network is behind a proxy, configure the GUI with the proxy. See Configure a Proxy , on page 109

Step 14 In the **Configure Token** area that is displayed, click **Configure Token**.

Figure 10: Configure Token



Configure Token

Without the token, the connector will not be able to start.

Configure Token ×

Click to configure the token copied from Cisco Spaces

Connector 3.1

Hostname conn-pri

Package connector3-p84-...

Show More

General Information

Connector Name Not Available

Tenant ID Not Available

Connector ID Not Available

Instance ID 005056a754c8

Proxy https://proxy.esl.cisco.com:80

NTP Address ntp.esl.cisco.com

NTP Status active (running)

HA Config Mode Not VIP Paired

Primary Interface

IP Address 10.89.45.92/24

MAC Address 00:50:56:A7:54:C8

Gateway 10.89.45.1

DNS Server 171.70.168.183

Domain cisco.com

IP Stack ipv4

Step 15 In the window that is displayed, in the **Token** text, field enter the token copied from Cisco Spaces and click **Configure**.

Warning

During this step, if you face a connectivity issue between Cisco Spaces: Connector and Cisco Spaces dashboard, the Connector could hang without an error. You can still access the Connector through SSH. You may also be unable to log in the Connector GUI after this issue.

Step 16 Add the following services as required:

- Configuring IoT Services

- Configuring Hotspot Services

Upgrading the Connector from Cisco Spaces Dashboard

Use the connector's GUI to upgrade connector.

Note

- This is referred to as **system inline upgrade** or **system upgrade** using the connector GUI.
- Upgrade is not supported on AMI connector instances.

Log in to the connector GUI, check for new upgrades and the summary of changes, and initiate the upgrade. Note that you must ensure that the connector's Service manager service is updated before you start the connector upgrade. You can upgrade the Service manager service from the connector GUI. The following procedure describes how to first upgrade the Service manager service and then upgrade connector itself from the connector GUI.

Procedure

Step 1 Log in to **Cisco Spaces**.

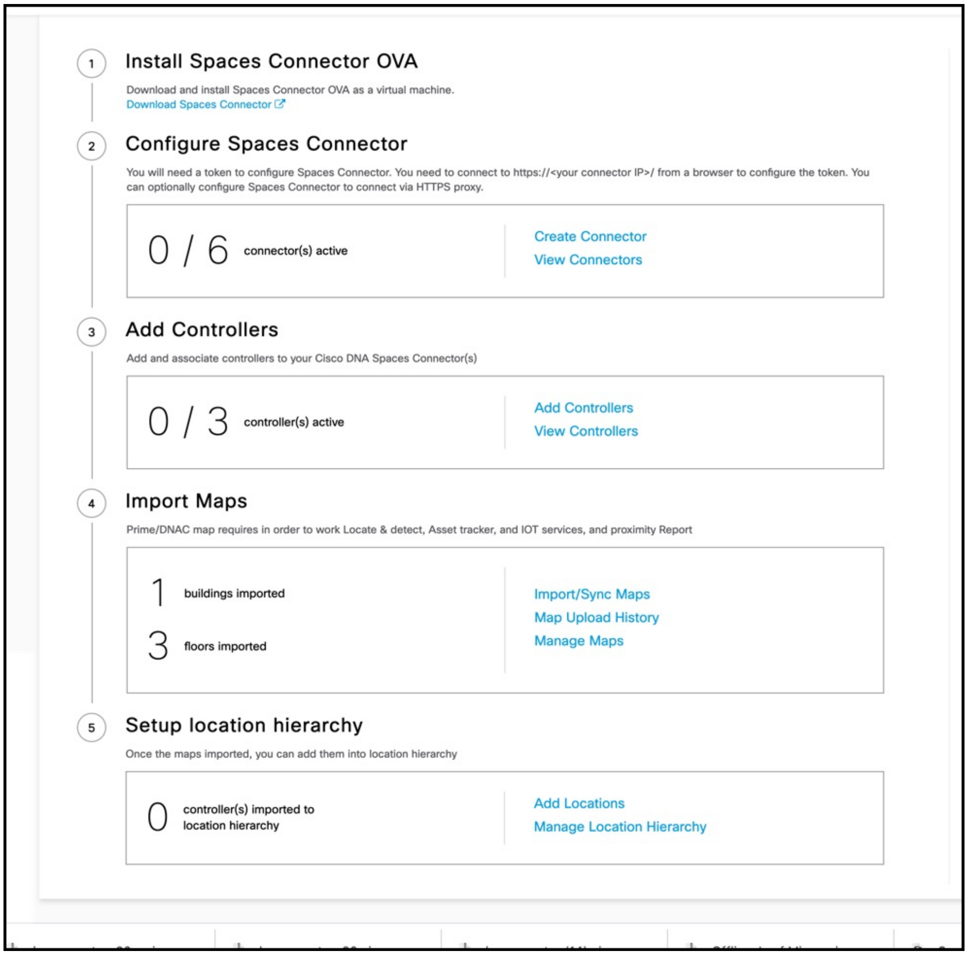
Note

The Cisco Spaces URL is region-dependent.

Step 2 In the Cisco Spaces dashboard, choose **Setup** > **Wireless Networks**.

Step 3 From the **2. Configure Spaces Connector** area, click **View Connectors**

Figure 11: View Connectors



1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.

Download Spaces Connector

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

0 / 6 connector(s) active

Create Connector
View Connectors

3 Add Controllers

Add and associate controllers to your Cisco DNA Spaces Connector(s)

0 / 3 controller(s) active

Add Controllers
View Controllers

4 Import Maps

Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

1 buildings imported
3 floors imported

Import/Sync Maps
Map Upload History
Manage Maps

5 Setup location hierarchy

Once the maps imported, you can add them into location hierarchy

0 controller(s) imported to location hierarchy

Add Locations
Manage Location Hierarchy

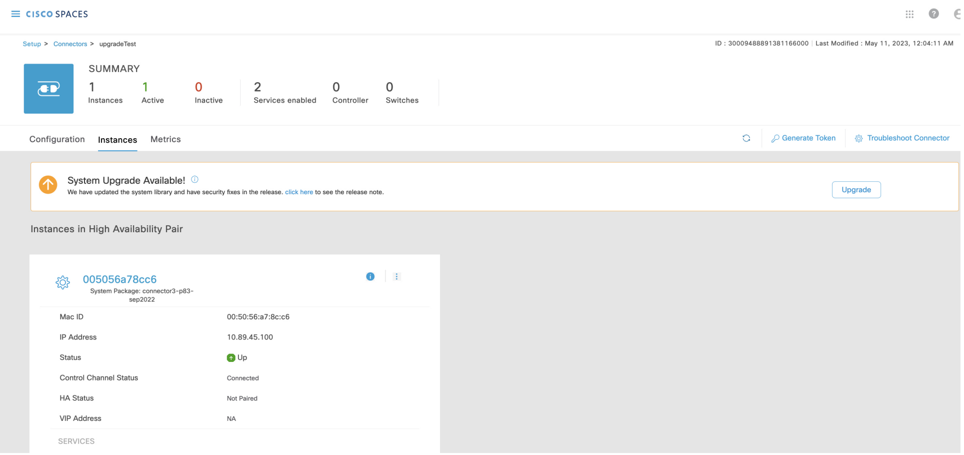
Step 4 From the list of connectors that are displayed, click the connector of your choice.

Step 5 From the **Configuration** tab of the specific connector, ensure that the Service manager service is upgraded. If not upgraded, under the **Actions** column, check for any available **Upgrade** option.

Step 6 Click the **Instances** tab, and choose the instances you want to upgrade.

Step 7 In the **System Upgrade Available** area, and click **Upgrade**.

Figure 12: Upgrade



ID : 30009488891381166000 | Last Modified : May 11, 2023, 12:04:11 AM

1	1	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

System Upgrade Available!

We have updated the system library and have security fixes in the release. click here to see the release note.

Instances in High Availability Pair

005056a78cc6

System Package: connector3-p83-sep2022

Mac ID	00:50:56:a7:8c:c6
IP Address	10.89.45.100
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

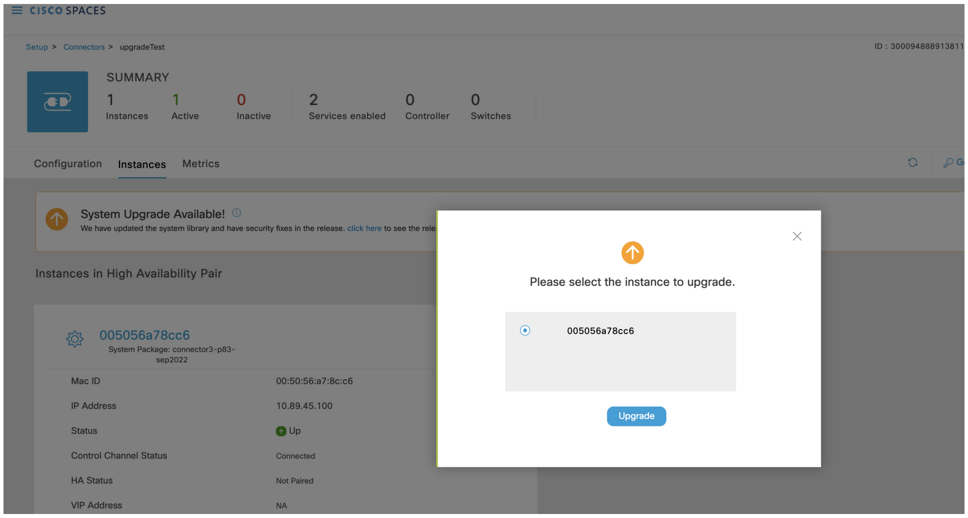
Note

For connector Release 3, the system inline upgrade may not succeed in a low latency network. You can upgrade the connector manually. Downloading the connector OVA from cisco.com and using the **connectoros upgrade <package-name>** command from the connector CLI.

For connector Release 3.1, the upgrade option is available from the Cisco Spaces dashboard as the timeout period has been increased to accommodate low latency networks.

Step 8 From the popup displayed, select the instance you want to upgrade.

Figure 13: Select instance



ID : 300094888913811

1	1	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

System Upgrade Available!

We have updated the system library and have security fixes in the release. click here to see the rele

Instances in High Availability Pair

005056a78cc6

System Package: connector3-p83-sep2022

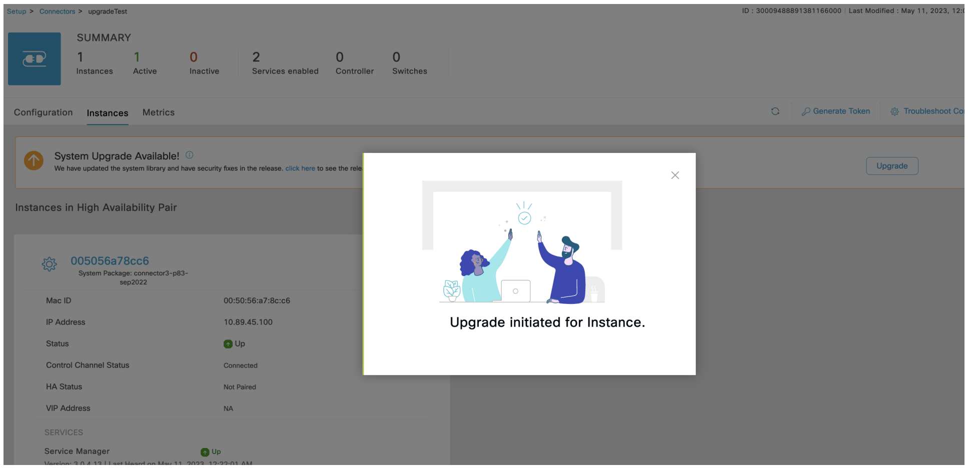
Mac ID	00:50:56:a7:8c:c6
IP Address	10.89.45.100
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

Please select the instance to upgrade.

● 005056a78cc6

An **Upgrade Initiated for instance** message is displayed.

Figure 14: Upgrade Initiated for Instance



Setup > Connectors > upgradeTest

ID : 30009488891381166000 | Last Modified : May 11, 2023, 12:

SUMMARY

1	1	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

System Upgrade Available!

We have updated the system library and have security fixes in the release. click here to see the rele

Upgrade initiated for Instance.

Instances in High Availability Pair

005056a78cc6

System Package: connector3-p83-sep2022

Mac ID	00:50:56:a7:8c:c6
IP Address	10.89.45.100
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

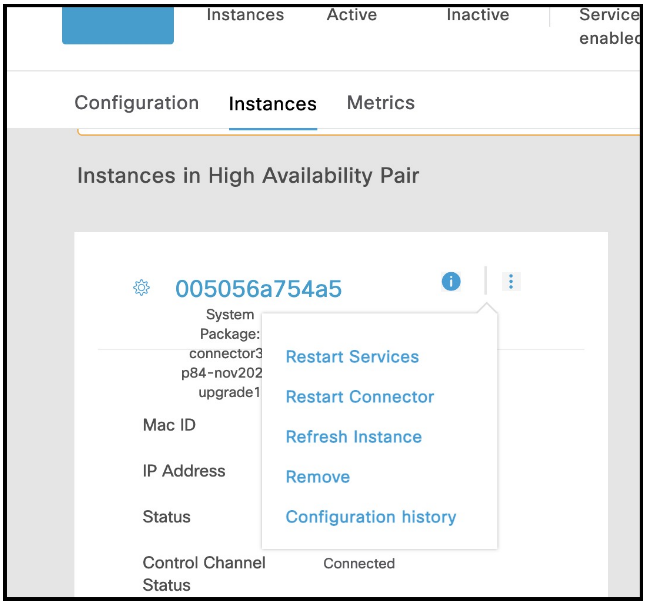
SERVICES

Service Manager Up

Version: 3.0.4.13 | Last Heard on May 11, 2023, 12:22:01 AM

Step 9 Observe the status of the installation by clicking the three-dot icon of an instance. From the menu displayed, choose **Configuration History**.

Figure 15: Configuration History



Instances in High Availability Pair

005056a754a5

System Package: connector3 p84-nov202 upgrade1

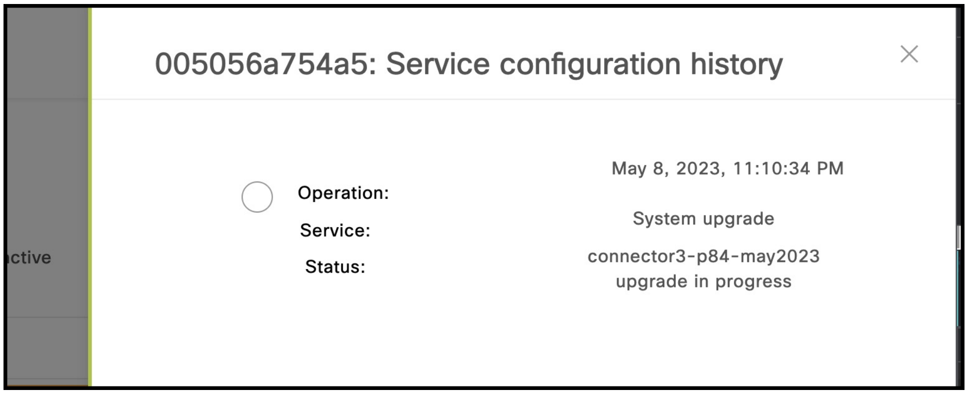
Mac ID

IP Address

Status

Control Channel Status Connected

Figure 16: Configuration History



005056a754a5: Service configuration history

○ Operation: May 8, 2023, 11:10:34 PM

Service: System upgrade

Status: connector3-p84-may2023 upgrade in progress

Upgrading the Connector Using CLI

Use the connector's CLI to upgrade connector.

Note

- This is referred to as **system inline upgrade** or **system upgrade** using the connector CLI.
- System upgrade is not supported for AMI connector instances.

Log in to the connector CLI, check for new upgrades and the summary of changes, and initiate the upgrade. Note that you must ensure that the connector's Service manager service service is updated before you start the connector command line upgrade. You can upgrade the Service manager service from the connector GUI. then upgrade connector itself from the connector CLI.

Before you begin

Ensure that the Service manager service is upgraded from the connector GUI.

Procedure

Step 1 Log in to the connector CLI.

Step 2 Check the availability of upgrades, and view a summary of the changes that are part of this upgrade package. Run the **connectorctl systemupgrade list** command.

Step 3 Initiate the upgrade of connector packages. Run the **connectorctl systemupgrade install** command:

```
[spacesadmin@connector03 ~]$ connectorctl systemupgrade install

Executing command:systemupgrade
Command execution status :Success

System upgrade operation is queued. Use tail -f
```

```
/opt/spaces-connector/runtime/logs/service-manager/system-upgrade/system-upgrade. log to see upgrade
 progress
```

Step 4 Observe the status of the upgrade. Do one of the following:

- To populate the CLI with regular updates of the upgrade, run the **tail -f /opt/spaces-connector/runtime/logs/service-manager/system-upgrade/system-upgrade.log** command.
- To view the status of the upgrade at any point in time, run the **connectorctl systemupgrade status** command:

```
 [spacesadmin@connector ~]$ connectorctl systemupgrade status
Executing conmand:systemupgrade
Command execution status: Success

System upgrade is in progress for package:connector3-p84-jan2023-upgrade2 at:Jan-10-2023 05:31:33.
 Details:Downloading image.
```

```
[spacesadmin@connector ~]$ connectorctl systemupgrade status
Executing command: systemupgrade
Command execution status: Success

Successfully upgraded system to package: connector3-p84-jan2023-upgrade2 at :Jan-1
 0-2023 04:34:04
```

Occasionally, you may see the following error while running the **connectorctl systemupgrade status** command. Ignore this output and wait for a few minutes before running the **connectorctl systemupgrade status** command again:

```
[spacesadmin@connector ~]$ connectorct1 systemupgrade status
Traceback (most recent call last>:
    File "/opt/spaces-connector/static/service-agent/core/src/cli/cli.py'.line10,in<module>
       from core.src.log.log_task import Loglask

File"/opt/spaces-connector/static/service-agent/core/src/cli/../../../core/src/log/log_task-py".line16,in<module>

        from -utils import pathconstant, constant, utilities
   File
"/opt/spaces-connector/static/service-agent/core/src/cli/../../../core/src/utils/utilities-py',line31,in<module>

        import psutil
ModuleNotFoundError: No module named ›psutil'
```

Upgrading the Connector Using Downloaded Connector Package

You can upgrade the connector manually. Downloading the connector OVA from cisco.com and using the **connectoros upgrade <package-name>** command from the connector CLI.

Procedure

Step 1 Log in to the connector CLI.

Step 2 Run the **connectoros upgrade** command to upgrade the installed connector.

The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectoros upgrade
cisco-spaces-connector3-p84-jul2024.connectorpkg
```

For more information on this command, see **connectoros upgrade**.

CHAPTER 4

Cisco Spaces: Connector AMI

Launch Connector 3 as an EC2 Instance from AMI

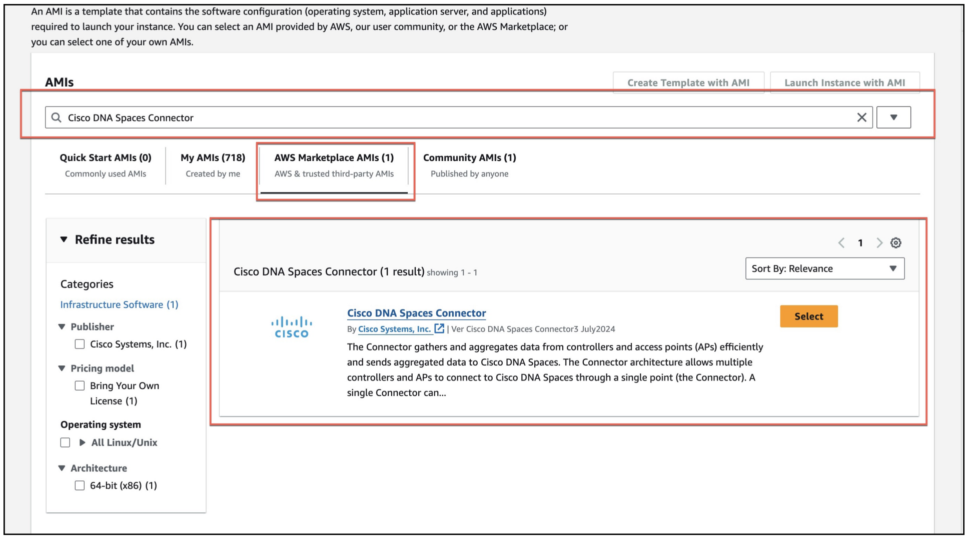
This chapter provides information about how to launch a connector 3 as an EC2 instance from Amazon Machine Images (AMI), configure the connector 3 instance, and finally obtain a URL to log in to the connector connector and CLI.

Procedure

Step 1 Log in to your Amazon Web Services account and navigate to the **EC2 Dashboard**. In the left-navigation pane, choose **Images** > **AMI Catalog**.

Step 2 In the **AMIs** search area, click **AWS MarketPlace AMIs** and enter `DNA Spaces Connector`. Press **Enter**.

Figure 17: Configuration



An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Cisco DNA Spaces Connector

Cisco DNA Spaces Connector (1 result) showing 1 - 1

Cisco DNA Spaces Connector

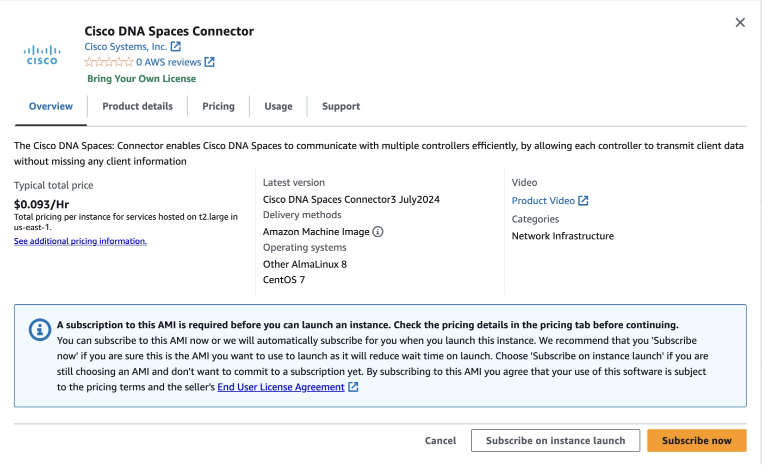
By Cisco Systems, Inc. | Ver Cisco DNA Spaces Connector3 July2024

The Connector gathers and aggregates data from controllers and access points (APs) efficiently and sends aggregated data to Cisco DNA Spaces. The Connector architecture allows multiple controllers and APs to connect to Cisco DNA Spaces through a single point (the Connector). A single Connector can...

Step 3 Click the displayed image and click **Select**.

Step 4 In the **Cisco DNA Spaces Connector** window displayed, click **Continue**.

Figure 18: AWS MarketPlace AMIs



Cisco DNA Spaces Connector
Cisco Systems, Inc.
0 AWS reviews
Bring Your Own License

The Cisco DNA Spaces: Connector enables Cisco DNA Spaces to communicate with multiple controllers efficiently, by allowing each controller to transmit client data without missing any client information

Typical total price
$0.093/Hr
Total pricing per instance for services hosted on t2.large in us-east-1.
See additional pricing information.

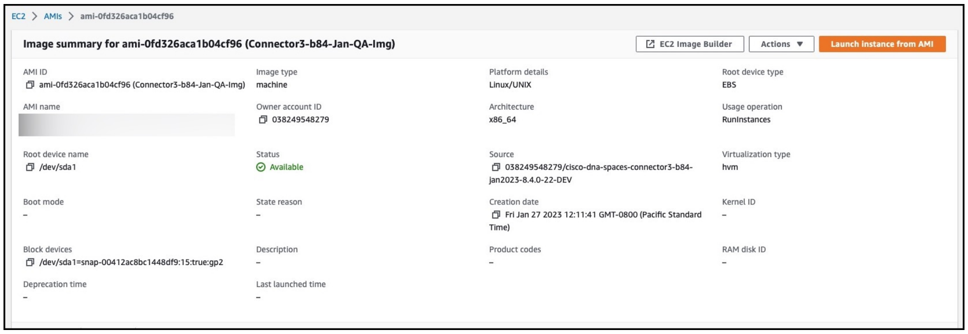
Latest version
Cisco DNA Spaces Connector3 July2024
Delivery methods
Amazon Machine Image
Operating systems
Other AlmaLinux 8
CentOS 7

Video
Product Video
Categories
Network Infrastructure

A subscription to this AMI is required before you can launch an instance. Check the pricing details in the pricing tab before continuing.
You can subscribe to this AMI now or we will automatically subscribe for you when you launch this instance. We recommend that you 'Subscribe now' if you are sure this is the AMI you want to use to launch as it will reduce wait time on launch. Choose 'Subscribe on instance launch' if you are still choosing an AMI and don't want to commit to a subscription yet. By subscribing to this AMI you agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement

Step 5 In the **Image Summary** window displayed, click **Launch Instance from AMI**

Figure 19: Launch Instance from AMI



EC2 > AMIs > ami-0fd326aca1b04cf96

Image summary for ami-0fd326aca1b04cf96 (Connector3-b84-Jan-QA-Img)

AMI ID
ami-0fd326aca1b04cf96 (Connector3-b84-Jan-QA-Img)

Image type
machine

Platform details
Linux/UNIX

Root device type
EBS

AMI name
[redacted]

Owner account ID
038249548279

Architecture
x86_64

Usage operation
RunInstances

Root device name
/dev/sda1

Status
Available

Source
038249548279/cisco-dna-spaces-connector3-b84-jan2023-8.4.0-22-DEV

Virtualization type
hvm

Boot mode
–

State reason
–

Creation date
Fri Jan 27 2023 12:11:41 GMT-0800 (Pacific Standard Time)

Kernel ID
–

Block devices
/dev/sda1=snap-00412ac8bc1448df9:15:true:gp2

Description
–

Product codes
–

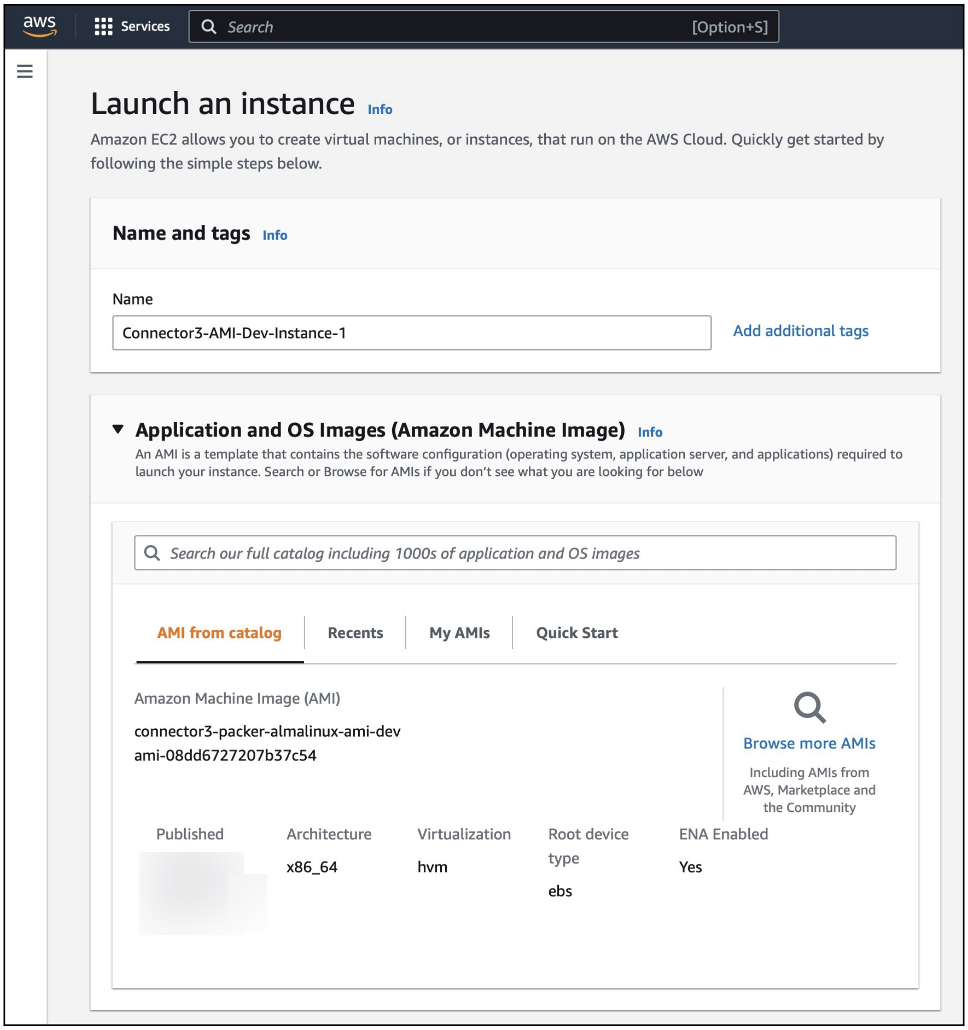
RAM disk ID
–

Deprecation time
–

Last launched time
–

Step 6 In the **Launch an Instance** window displayed, enter an instance name, and add any additional labels for your instance by clicking the **Add Additional tags** button.

Figure 20: Launch Instance from AMI



Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: Connector3-AMI-Dev-Instance-1

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)

connector3-packer-almalinux-ami-dev
ami-08dd6727207b37c54

Browse more AMIs

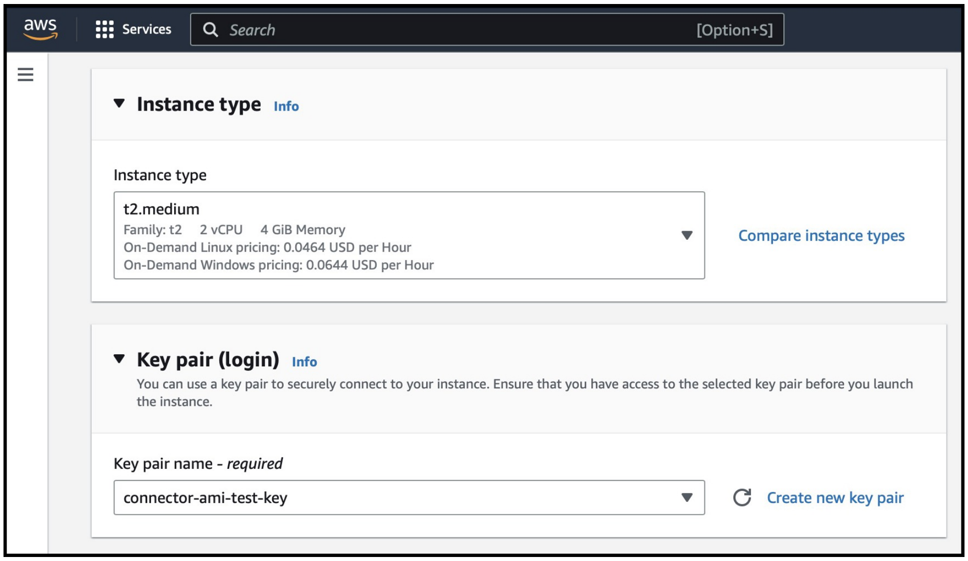
Including AMIs from AWS, Marketplace and the Community

Published	Architecture	Virtualization	Root device type	ENA Enabled
[redacted]	x86_64	hvm	ebs	Yes

Step 7 Choose any EC2 instance that has a minimum of 2 vCPU and 4GB Memory. Click **Next: Configure Instance Details**.

t2.medium corresponds to a standard window with 2vCPUs and 4-GB memory and is the recommended setting.

Figure 21: Configure Instance Details



▼ **Instance type** Info

Instance type

t2.medium
Family: t2 2 vCPU 4 GiB Memory
On-Demand Linux pricing: 0.0464 USD per Hour
On-Demand Windows pricing: 0.0644 USD per Hour

Compare instance types

▼ **Key pair (login)** Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

connector-ami-test-key

Create new key pair

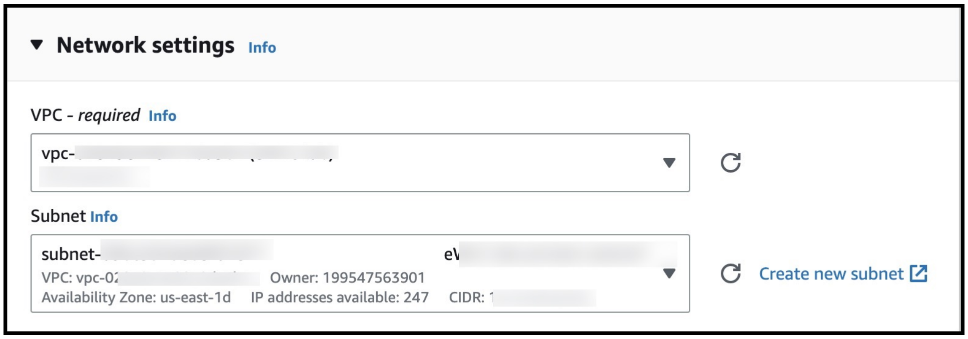
Note

You can have a more advanced configuration by choosing an option with higher vCPU and memory, by choosing an instance type with one of the following configurations. If an exact match is unavailable, you can choose a configuration with the next-available vCPU or memory:

- 4 vCPUs and 8-GB memory (referred to in this document as **Advanced1**)
- 8 vCPUs and 16-GB memory (referred to in this document as **Advanced2**)

Step 8 Choose a **Network** and a **Subnet**. Click **Next: Add Storage**.

Figure 22: Add Storage



▼ **Network settings** Info

VPC - *required* Info

vpc-[redacted]

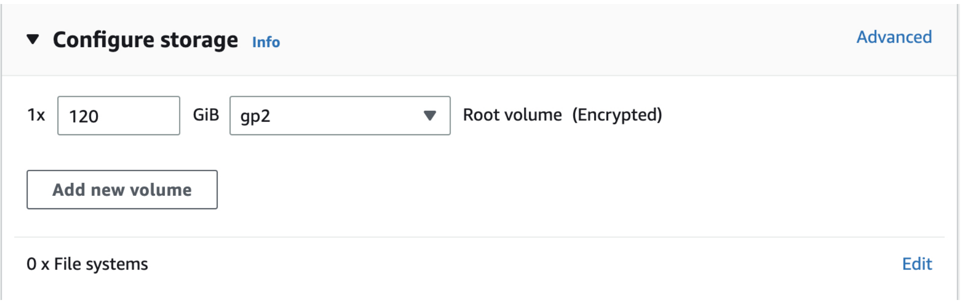
Subnet Info

subnet-[redacted] e[redacted]
VPC: vpc-0[redacted] Owner: 199547563901
Availability Zone: us-east-1d IP addresses available: 247 CIDR: 1[redacted]

Create new subnet

Step 9 Enter the value of **Size(GB)** as 120. Click **Next: Configure Security Group**.

Figure 23: Configure Storage



Configure storage Info — Advanced

1x 120 GiB gp2 Root volume (Encrypted)

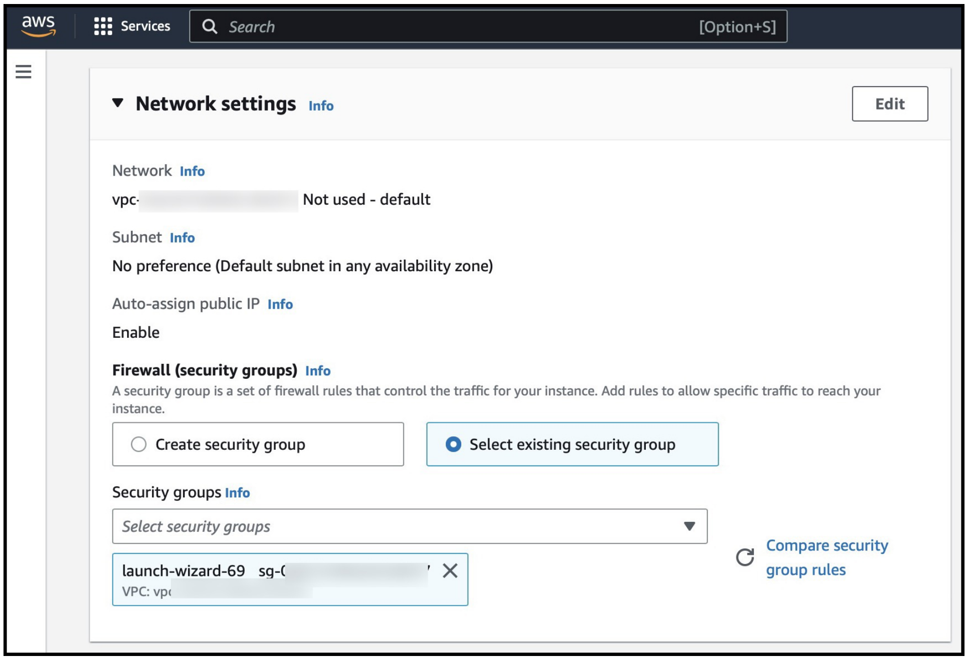
Add new volume

0 x File systems — Edit

Step 10 Configure a security group by following these steps:

a) Create a new security group or modify an existing one by clicking the respective radio button.

Figure 24: Configure Security Group



Network settings Info

Network Info
vpc-[redacted] Not used - default

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

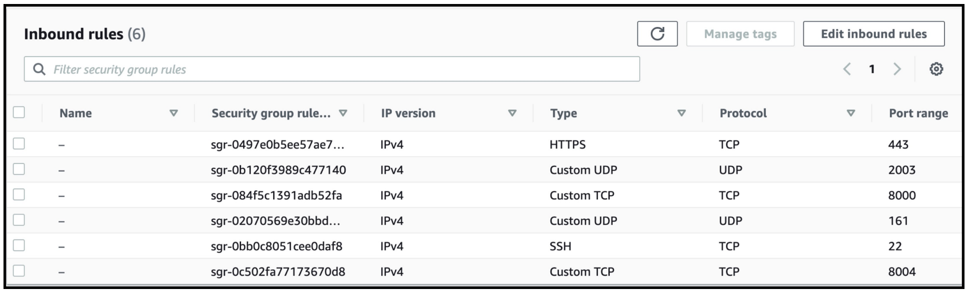
Security groups Info
Select security groups

launch-wizard-69 sg-[redacted]
VPC: vp[redacted]

Compare security group rules

b) Configure rules permitting inbound traffic to specific ports, as shown in the following image. You can allow inbound traffic to these ports for all IP addresses or choose to restrict them for specific IP addresses.

Figure 25: Configure These Inbound Rules Permitting Traffic to Specific Ports



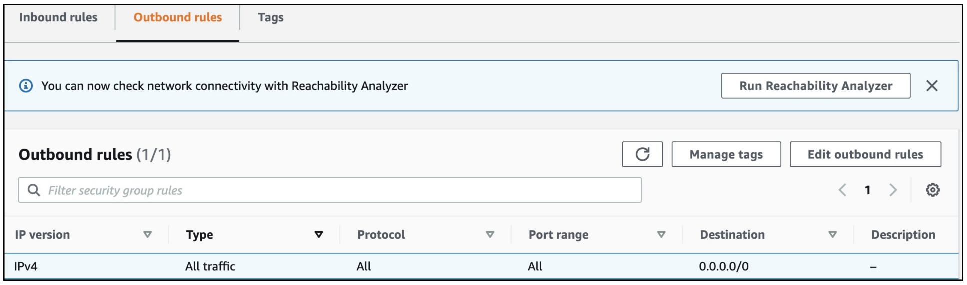
Inbound rules (6)

□	Name	Security group rule...	IP version	Type	Protocol	Port range
□	–	sgr-0497e0b5ee57ae7...	IPv4	HTTPS	TCP	443
□	–	sgr-0b120f3989c477140	IPv4	Custom UDP	UDP	2003
□	–	sgr-084f5c1391adb52fa	IPv4	Custom TCP	TCP	8000
□	–	sgr-02070569e30bbd...	IPv4	Custom UDP	UDP	161
□	–	sgr-0bb0c8051cee0daf8	IPv4	SSH	TCP	22
□	–	sgr-0c502fa77173670d8	IPv4	Custom TCP	TCP	8004

Note
Using an inbound rule, you can also specify the network subnet range that can access this instance (For example, through SSH).

c) Configure the outbound rule shown in the following image.

Figure 26: Configure This Outbound Rule



You can now check network connectivity with Reachability Analyzer

Outbound rules (1/1)

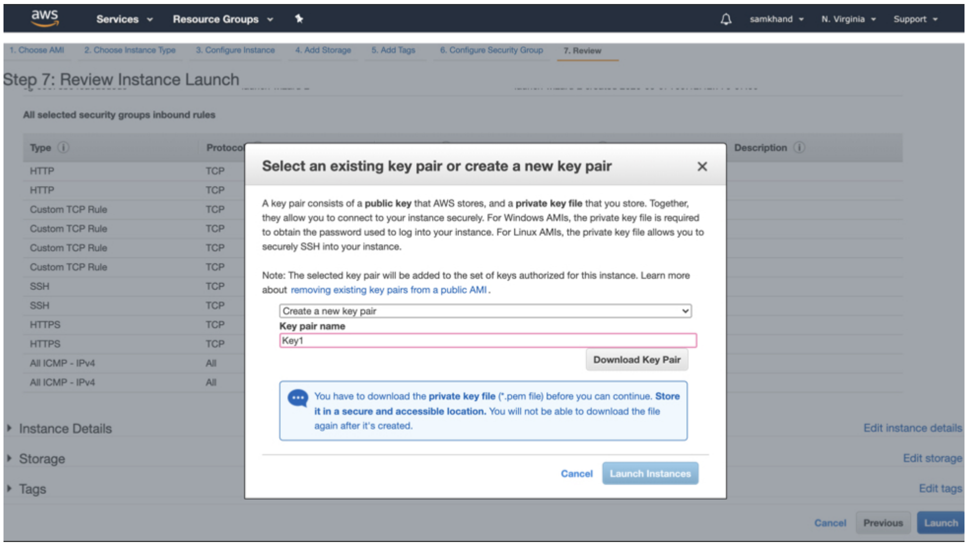
IP version	Type	Protocol	Port range	Destination	Description
IPv4	All traffic	All	All	0.0.0.0/0	–

Note
For various connector services to work, you must open specific ports. See the respective **Information About Open Ports** section of the connector service for more information.

Step 11 In the displayed **Select an existing key pair or create a new key pair** dialog box, do either of the following:

- Choose **Create a new key pair** from the drop-down list. Provide a **Key pair name** and click **Download Key Pair** to download it. Then click **Launch Instance** to launch the instance.
- Choose **Choose an existing key pair** from the drop-down list. Select the previously downloaded key pair from the **Select a key Pair** drop-down list. Then click **Launch Instance** to launch the instance.

Figure 27: Create a New Key Pair



Step 7: Review Instance Launch

All selected security groups inbound rules

Type	Protocol	Description
HTTP	TCP	
HTTP	TCP	
Custom TCP Rule	TCP	
Custom TCP Rule	TCP	
Custom TCP Rule	TCP	
Custom TCP Rule	TCP	
SSH	TCP	
SSH	TCP	
HTTPS	TCP	
HTTPS	TCP	
All ICMP - IPv4	All	
All ICMP - IPv4	All	

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

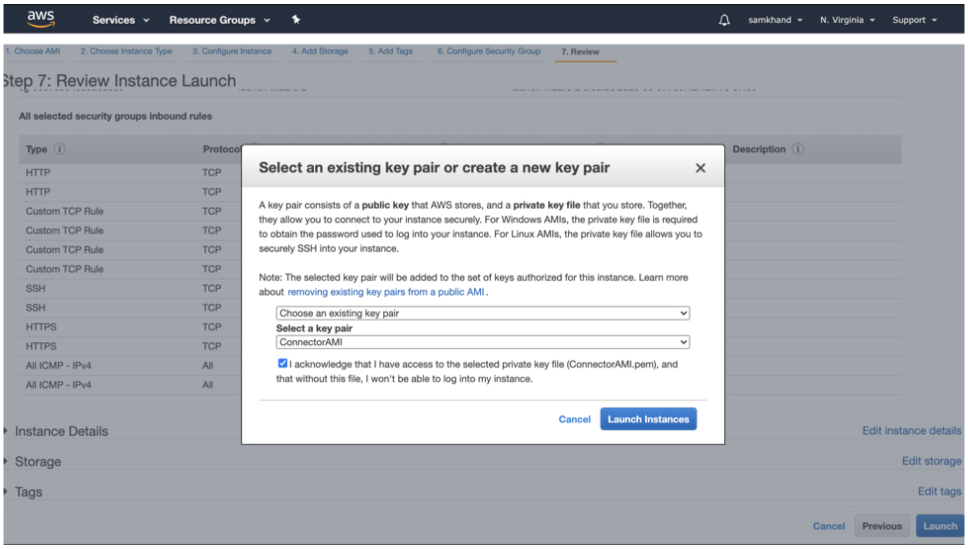
Key pair name
Key1

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel Launch Instances

Figure 28: Choose an Existing Key Pair



Step 7: Review Instance Launch

All selected security groups inbound rules

Type	Protocol	Description
HTTP	TCP	
HTTP	TCP	
Custom TCP Rule	TCP	
Custom TCP Rule	TCP	
Custom TCP Rule	TCP	
Custom TCP Rule	TCP	
SSH	TCP	
SSH	TCP	
HTTPS	TCP	
HTTPS	TCP	
All ICMP - IPv4	All	
All ICMP - IPv4	All	

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair

Select a key pair

ConnectorAMI

☑ I acknowledge that I have access to the selected private key file (ConnectorAMI.pem), and that without this file, I won't be able to log into my instance.

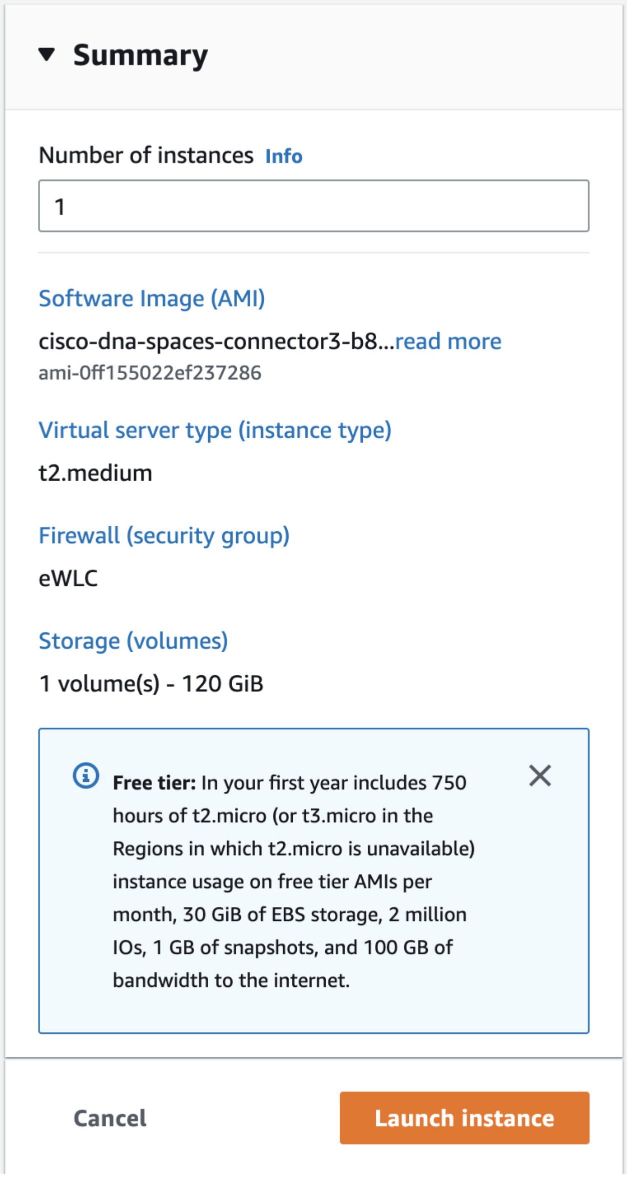
Cancel Launch Instances

Step 12 After you have downloaded the key pair (.pem) file to your system, navigate to the file location. Configure appropriate permissions for the .PEM file using the **chmod** command.

```
chmod 400 /path/to/MyAccessKey1.pem
```

Step 13 Review the instance and click **Launch**.

Figure 29: Review Instance and Launch



▼ Summary

Number of instances Info

1

Software Image (AMI)

cisco-dna-spaces-connector3-b8...read more

ami-0ff155022ef237286

Virtual server type (instance type)

t2.medium

Firewall (security group)

eWLC

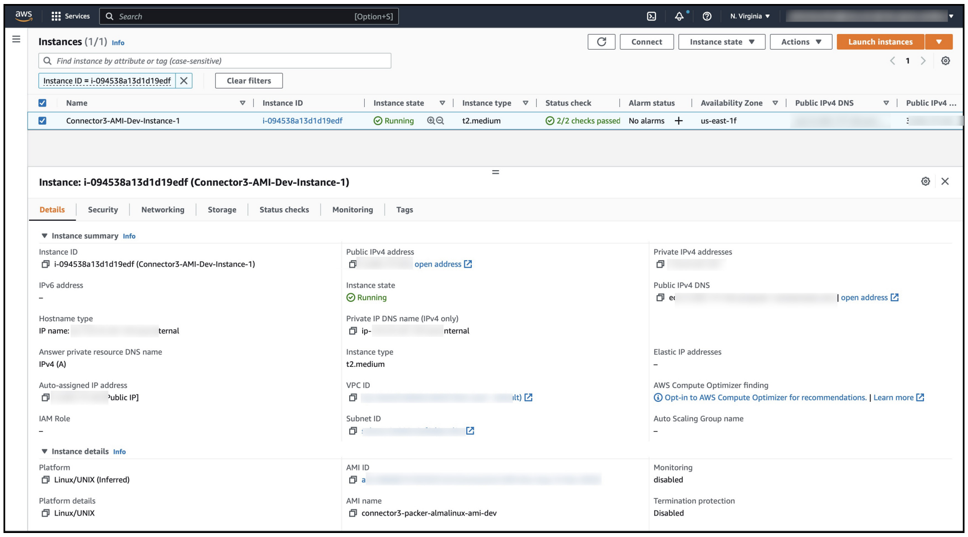
Storage (volumes)

1 volume(s) - 120 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Step 14 On the EC2 dashboard, wait for the instance to finish launching and the status to change to **Running**. Alternatively, you can see the running instances on the **Instances** page. Click the instance to obtain the IPv4 address of the instance.

Figure 30: Obtain IPv4 Address of Instance



Instances (1/1) Info

Find instance by attribute or tag (case-sensitive)

Instance ID = i-094538a13d1d19edf ✕ | Clear filters

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
☑	Connector3-AMI-Dev-Instance-1	i-094538a13d1d19edf	✓ Running	t2.medium	✓ 2/2 checks passed	No alarms +	us-east-1f	[redacted]	3[redacted]

Instance: i-094538a13d1d19edf (Connector3-AMI-Dev-Instance-1)

▼ Instance summary Info

Instance ID
i-094538a13d1d19edf (Connector3-AMI-Dev-Instance-1)

Public IPv4 address
[redacted] open address

Private IPv4 addresses
[redacted]

IPv6 address
–

Instance state
✓ Running

Public IPv4 DNS
ec[redacted] | open address

Hostname type
IP name: [redacted]ternal

Private IP DNS name (IPv4 only)
ip-[redacted]nternal

Answer private resource DNS name
IPv4 (A)

Instance type
t2.medium

Elastic IP addresses
–

Auto-assigned IP address
[redacted]Public IP]

VPC ID
[redacted]lt)

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role
–

Subnet ID
s[redacted]

Auto Scaling Group name
–

▼ Instance details Info

Platform
Linux/UNIX (Inferred)

AMI ID
a[redacted]

Monitoring
disabled

Platform details
Linux/UNIX

AMI name
connector3-packer-almalinux-ami-dev

Termination protection
Disabled

Step 15 Perform initial setup to configure a hostname, and change passwords for **spacesadmin** and **root** users.

a) Log in to the connector using the **ssh -i** command and the following parameters:

- The .PEM key pair downloaded in step 11
- ec2-user
- The IPv4 address obtained in step 14

```
ssh -i /path/to/key/MyAccessKey1.pem ec2-user@IPv4-address
```

b) Change passwords for **spacesadmin** and **root** users. Avoid a BAD PASSWORD prompt by complying with the following password requirements:

- Length is more than 14 characters.
- Includes at least one uppercase letter.
- Includes at least one lowercase letter.
- Includes at least one special character.

The following is a sample output of the command:

```
Welcome to Cisco Spaces Connector Setup
Changing password for user spacesadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Password changed successfully
Setting rbash...
Restarting docker...
Changing shell for root.
Shell changed.
Changing shell for spaces.


Remove default users...
Relabeled /etc/sudoers from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:etc_t:s0
```

```
Cisco Spaces Connector UI:
https://XX.XXX.XX.XXX
Username log in: spacesadmin
The install is complete, a reboot will occur in 10 seconds...
```

Once the installation is complete, a reboot occurs within 10 seconds. Note down the public IP address before reboot.

Step 16 Log in to the connector and configure the connector further. Do one of the following using the public IPv4 address from the previous step (step 15):

- Log in to the connector GUI using the browser window and the address https://*public-ipv4-address*
- Log in to the connector CLI using the SSH command and the username **spacesadmin**. Use the command **ssh spacesadmin@***public-ipv4-address*. When prompted, use the password configured for the **spacesadmin** user.

CHAPTER 5

Cisco Spaces: Connector Hyper-V

The chapter shows you how to install a connector as a Hyper-V instance. To do this, you must perform two tasks. The first task is to create a virtual switch and the second is to download and deploy Hyper-V image as a connector:

- Creating a Virtual Switch, on page 35
- Downloading and Deploying HYPER-V, on page 42

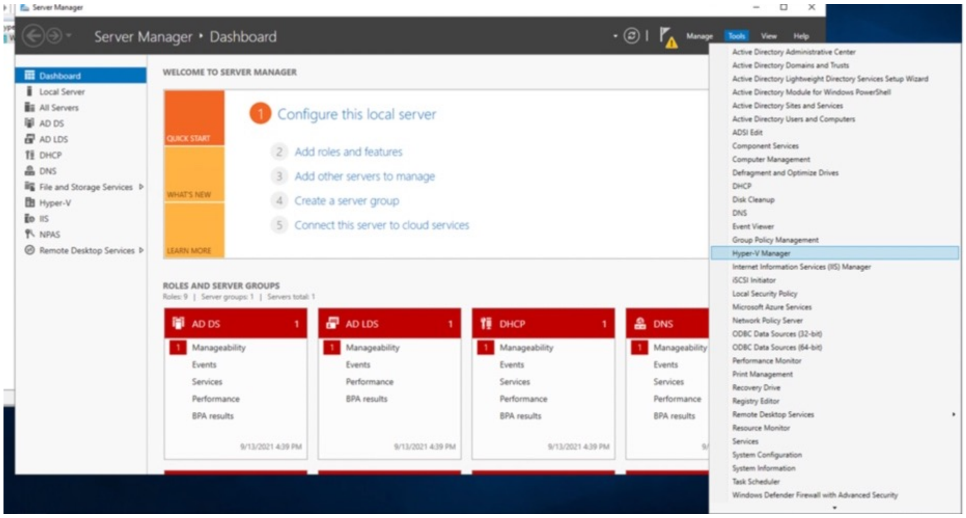
Creating a Virtual Switch

This task shows you how to install a Hyper-V manager. The task also shows you how to use the Hyper-V manager to installs a virtual switch.

Procedure

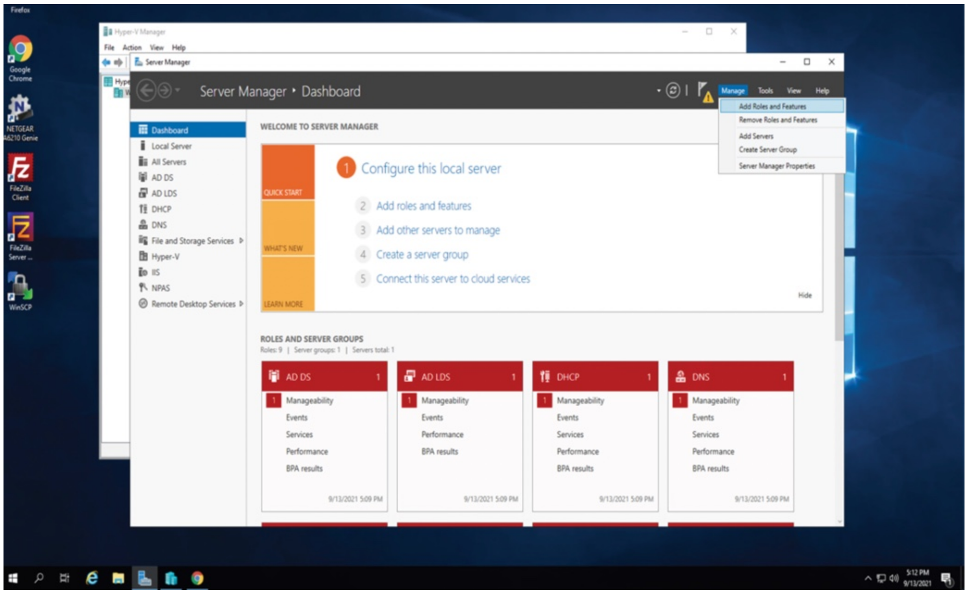
Step 1 Navigate to **Windows** > **Server Manager**.

Figure 31: Windows > Server Manager



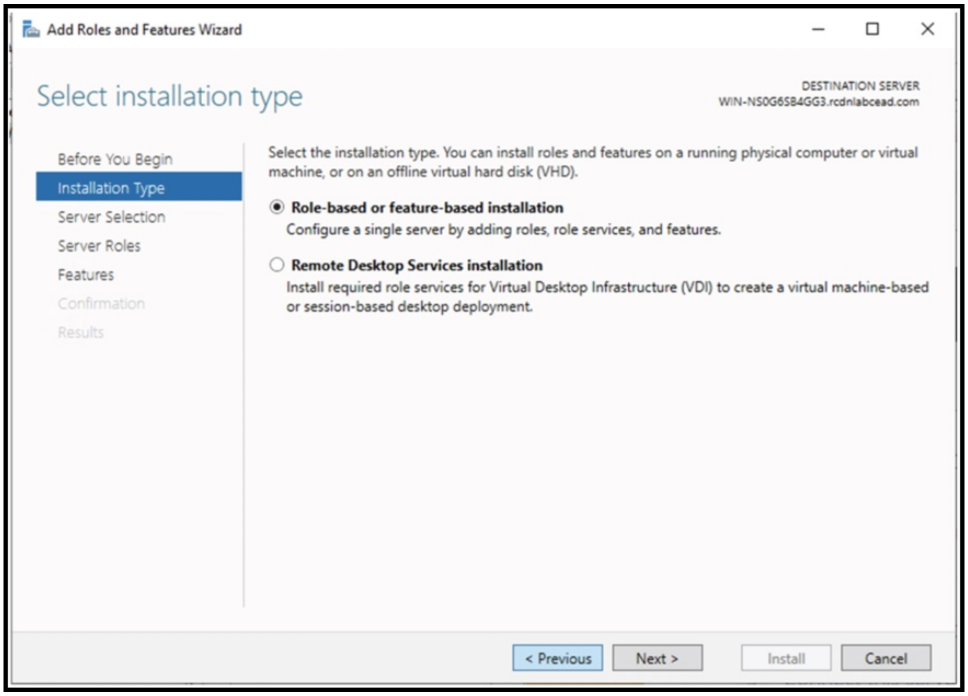
Step 2 Choose **Manage** > **Add Roles and Features**.

Figure 32: Manage > Add Roles and Features



Step 3 Click the **Role-based or feature-based installation** radio button.

Figure 33: Role-based or Feature-Based Installation


Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
WIN-NS0G6S84GG3.rcdnlabcead.com

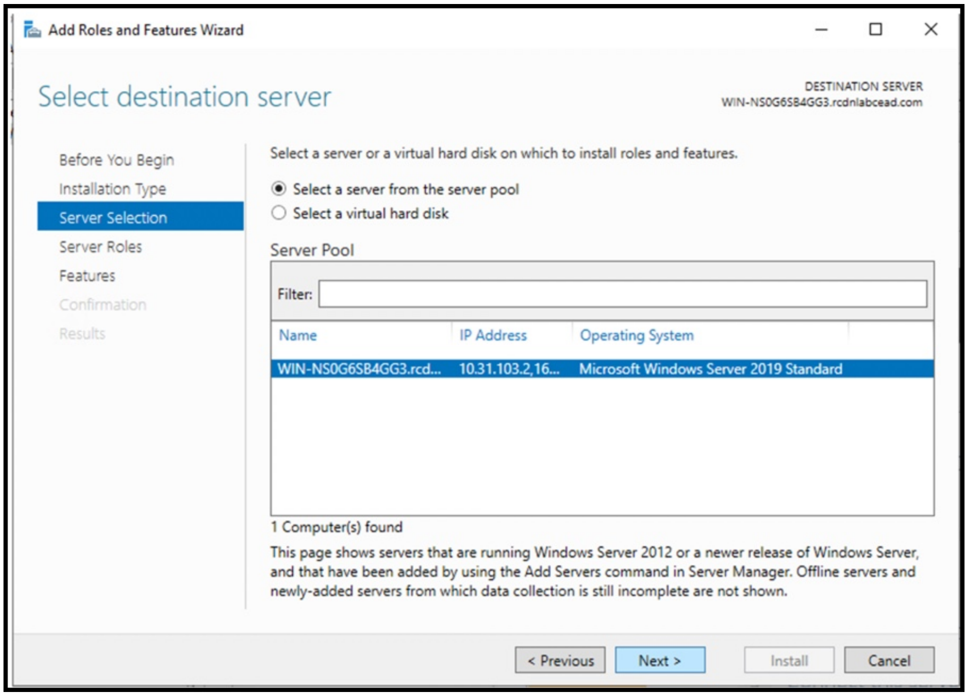
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Step 4 Click the **Select a server from the server pool** radio button.

Figure 34: Select a Server From the Server Pool



Select destination server

DESTINATION SERVER
WIN-NS0G6SB4GG3.rcdnlabcead.com

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

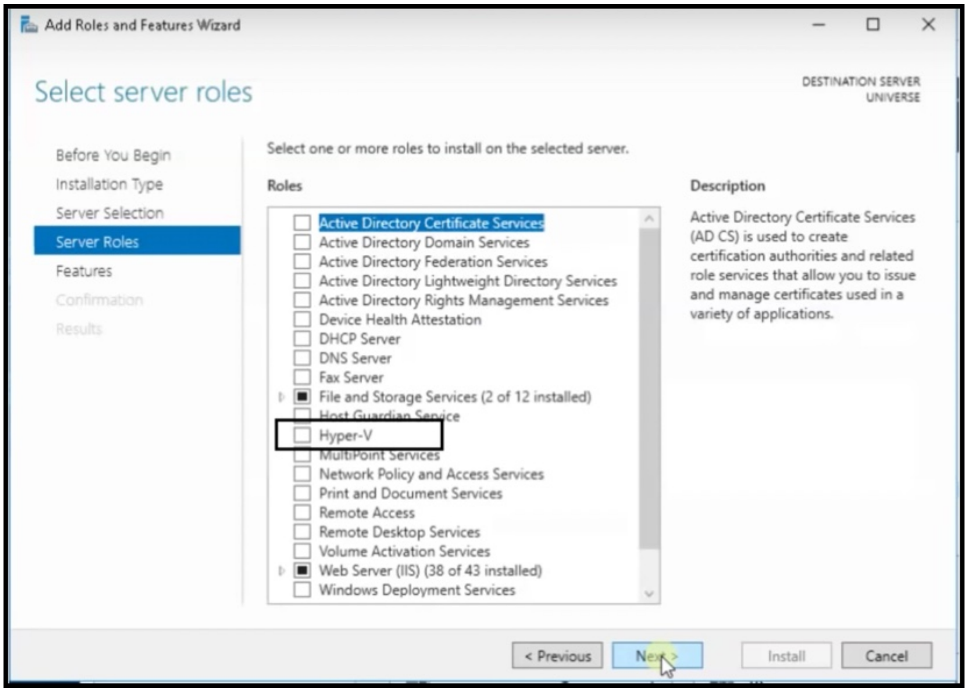
Name	IP Address	Operating System
WIN-NS0G6SB4GG3.rcd...	10.31.103.2,16...	Microsoft Windows Server 2019 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Step 5 In the **Select server roles** window, check the Hyper-V checkbox, and click **Next**.

Figure 35: Select Server Roles



Select server roles

DESTINATION SERVER
UNIVERSE

Select one or more roles to install on the selected server.

Roles

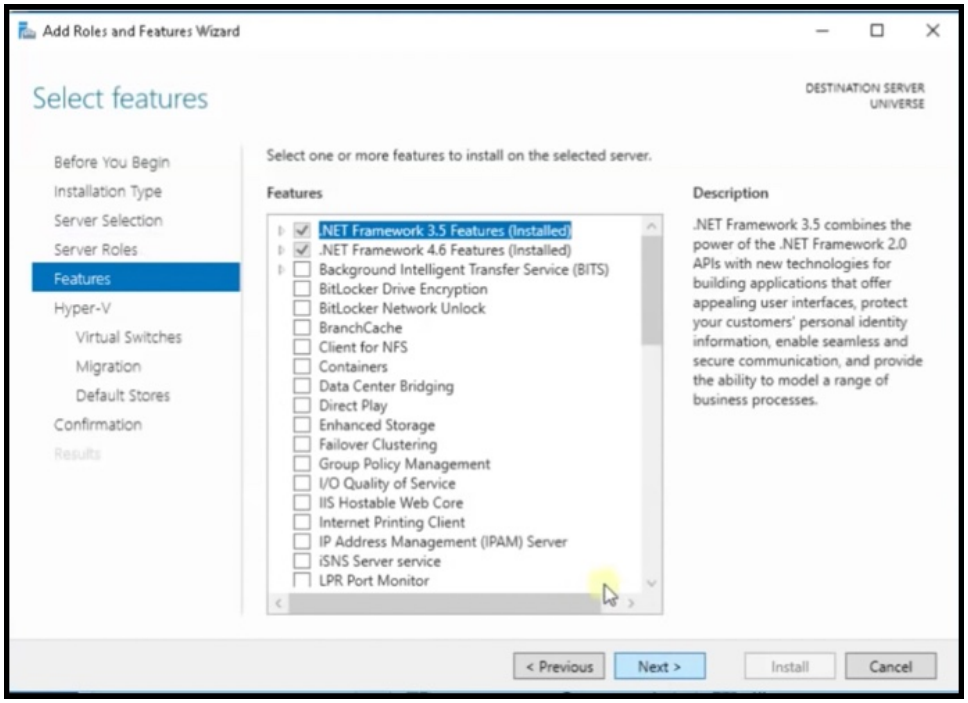
- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (38 of 43 installed)
- □ Windows Deployment Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Step 6 In the **Select features** window, check the **.NET Framework** checkbox, and click **Next**.

Figure 36: Select Features



Select features

DESTINATION SERVER
UNIVERSE

Select one or more features to install on the selected server.

Features

- ☑ .NET Framework 3.5 Features (Installed)
- ☑ .NET Framework 4.6 Features (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- □ Group Policy Management
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service
- □ LPR Port Monitor

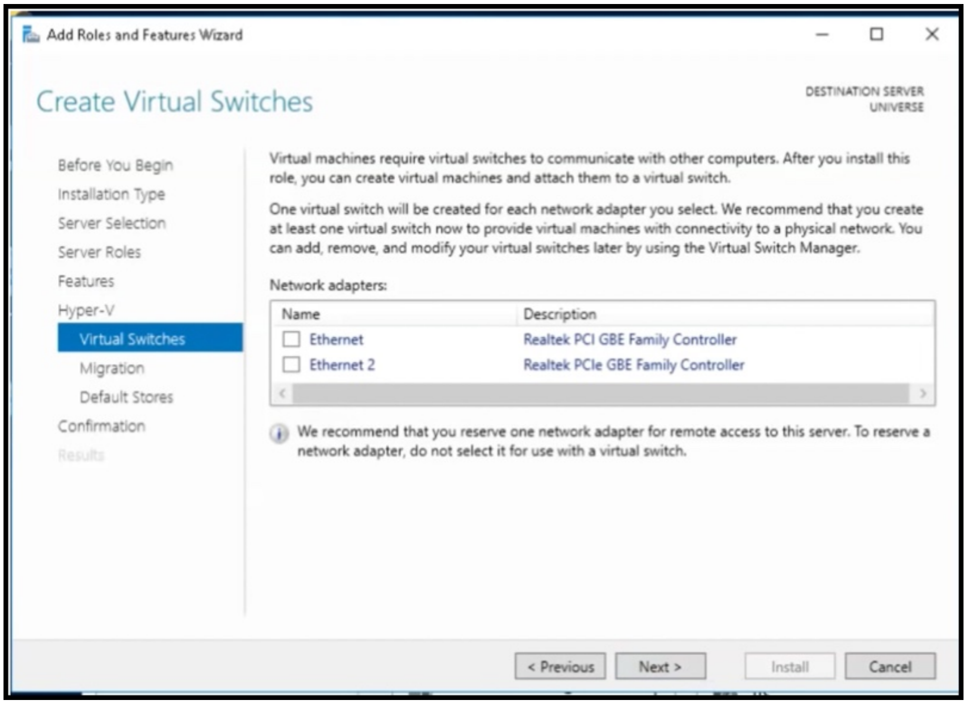
Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Step 7 In the **Hyper-V** window, do the following:

a) In the **Virtual Switches** window, click **Next**.

Figure 37: Virtual Switches



Create Virtual Switches

DESTINATION SERVER
UNIVERSE

Virtual machines require virtual switches to communicate with other computers. After you install this role, you can create virtual machines and attach them to a virtual switch.

One virtual switch will be created for each network adapter you select. We recommend that you create at least one virtual switch now to provide virtual machines with connectivity to a physical network. You can add, remove, and modify your virtual switches later by using the Virtual Switch Manager.

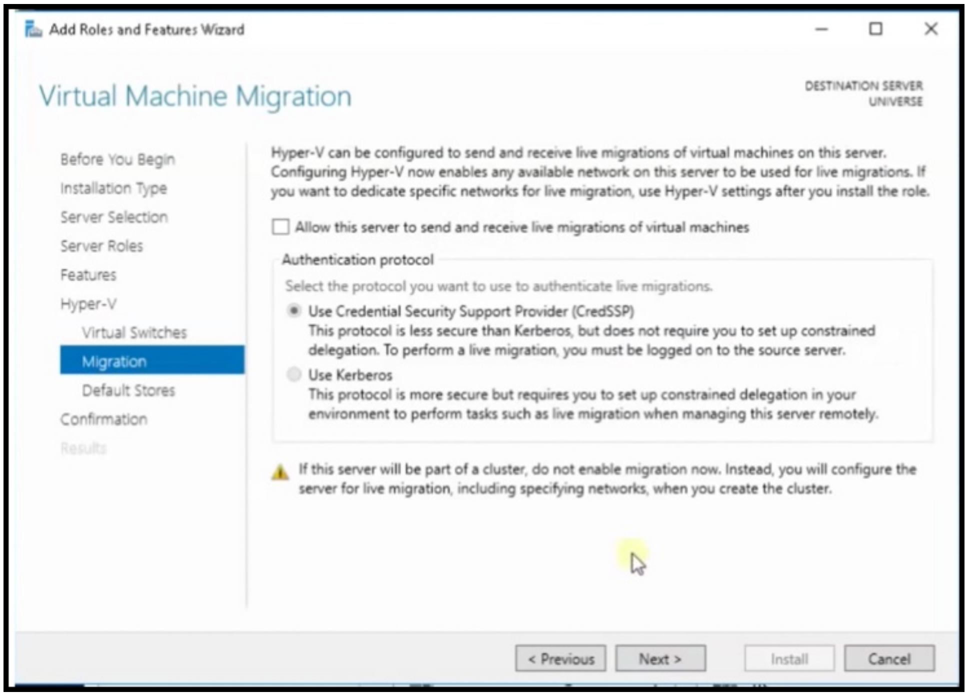
Network adapters:

Name	Description
□ Ethernet	Realtek PCI GBE Family Controller
□ Ethernet 2	Realtek PCIe GBE Family Controller

We recommend that you reserve one network adapter for remote access to this server. To reserve a network adapter, do not select it for use with a virtual switch.

b) In the **Migration** window, click **Use Credential Security Support Provider** (CredSSP) radio button, and click **Next**.

Figure 38: Use Credential Security Support Provider



Virtual Machine Migration

Hyper-V can be configured to send and receive live migrations of virtual machines on this server. Configuring Hyper-V now enables any available network on this server to be used for live migrations. If you want to dedicate specific networks for live migration, use Hyper-V settings after you install the role.

□ Allow this server to send and receive live migrations of virtual machines

Authentication protocol

Select the protocol you want to use to authenticate live migrations.

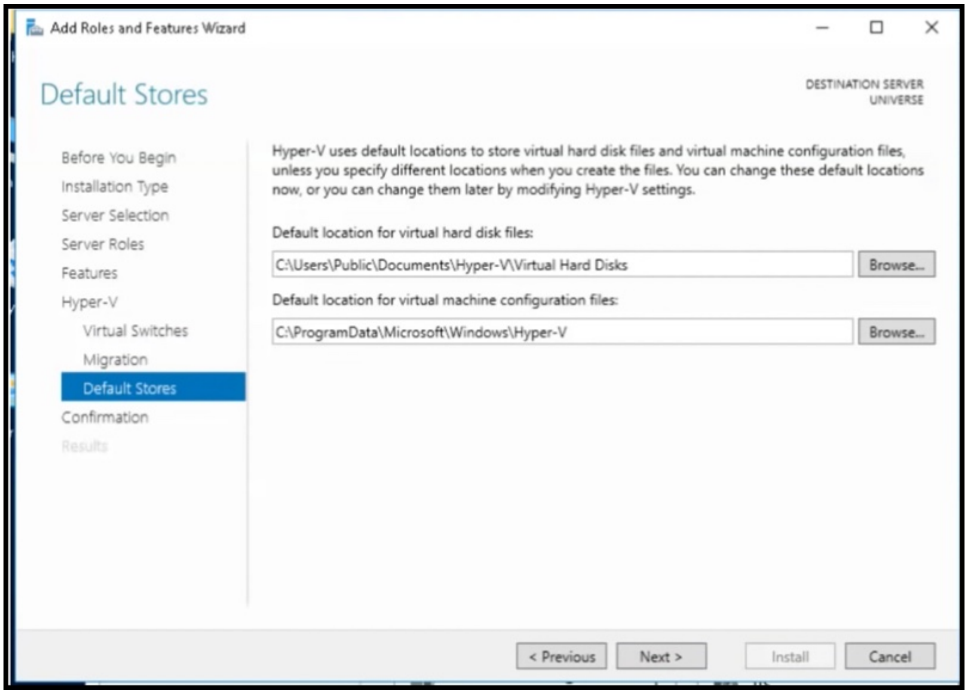
● Use Credential Security Support Provider (CredSSP)
This protocol is less secure than Kerberos, but does not require you to set up constrained delegation. To perform a live migration, you must be logged on to the source server.

○ Use Kerberos
This protocol is more secure but requires you to set up constrained delegation in your environment to perform tasks such as live migration when managing this server remotely.

If this server will be part of a cluster, do not enable migration now. Instead, you will configure the server for live migration, including specifying networks, when you create the cluster.

c) In the **Default Stores** window, select the location to install files or retain the default locations, and click **Next**.

Figure 39: Default Stores



Default Stores

Hyper-V uses default locations to store virtual hard disk files and virtual machine configuration files, unless you specify different locations when you create the files. You can change these default locations now, or you can change them later by modifying Hyper-V settings.

Default location for virtual hard disk files:

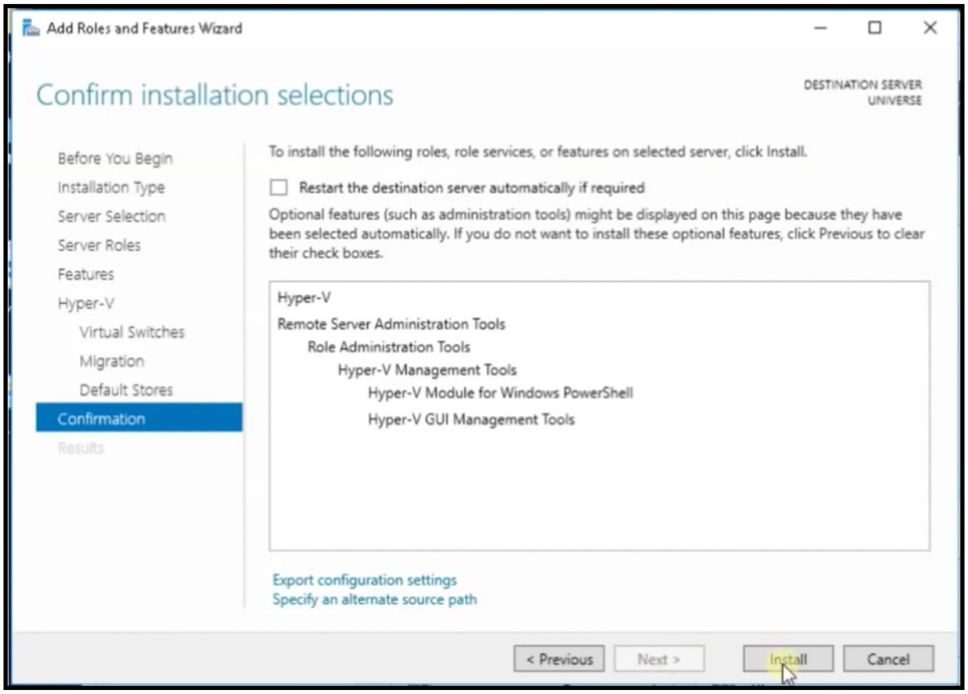
C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

Default location for virtual machine configuration files:

C:\ProgramData\Microsoft\Windows\Hyper-V

Step 8 Confirm the installation settings for Hyper-V and click **Install**.

Figure 40: Confirm the Installation Settings



Confirm installation selections

DESTINATION SERVER
UNIVERSE

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

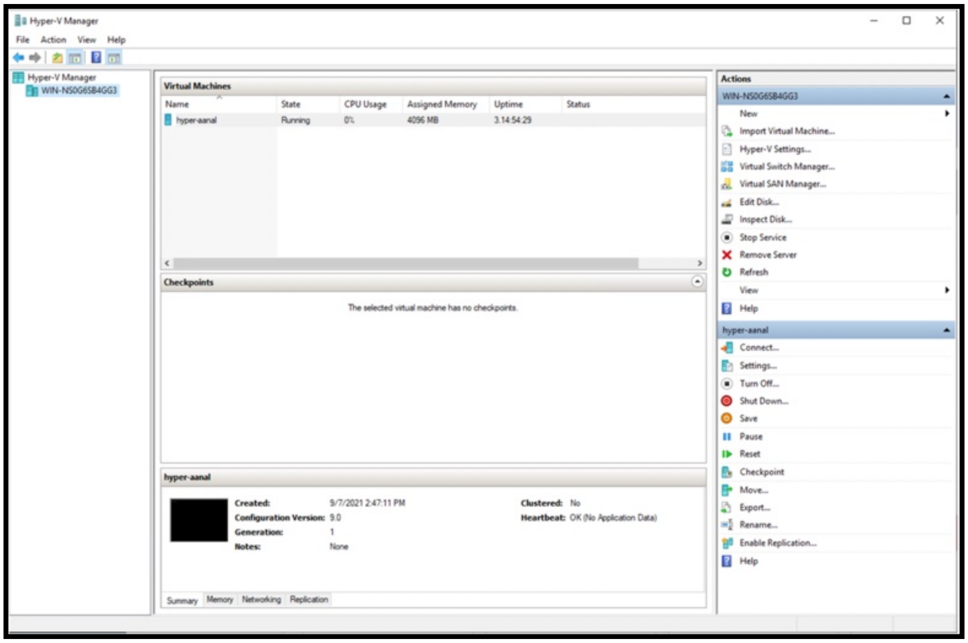
Hyper-V
Remote Server Administration Tools
    Role Administration Tools
        Hyper-V Management Tools
            Hyper-V Module for Windows PowerShell
            Hyper-V GUI Management Tools

Export configuration settings
Specify an alternate source path

Step 9 Open **Hyper-V Manager**.

Step 10 In Hyper-V Manager, choose **Actions** > **Virtual Switch Manager**.

Figure 41: Actions > Virtual Switch Manager



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status
hyper-aanal	Running	0%	4096 MB	3.14:54:29	

Checkpoints

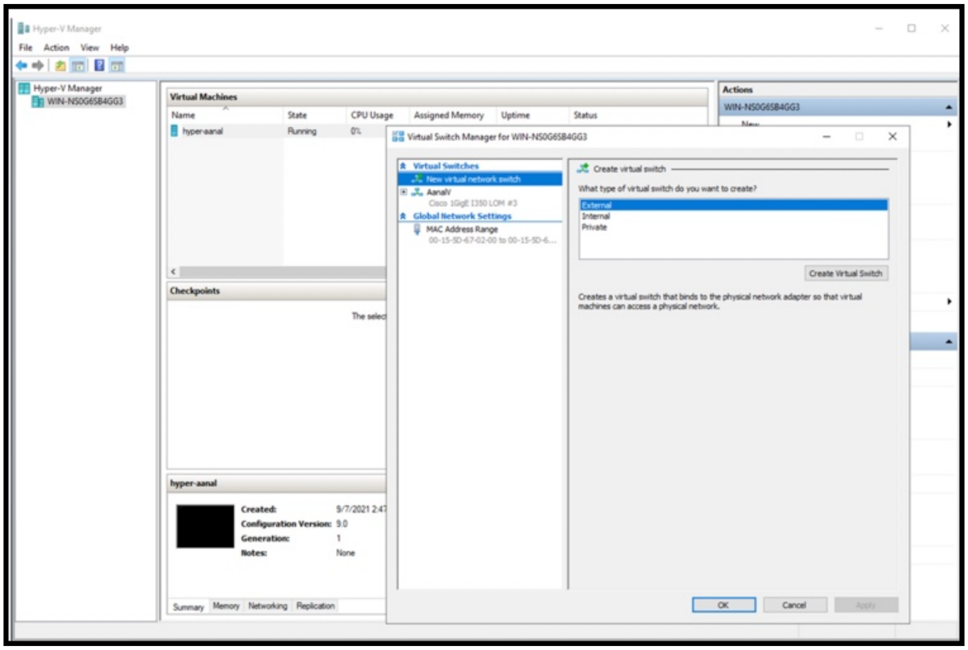
The selected virtual machine has no checkpoints.

hyper-aanal

Created: 9/7/2021 2:47:11 PM
Configuration Version: 9.0
Generation: 1
Notes: None
Clustered: No
Heartbeat: OK (No Application Data)

Step 11 In the **Virtual Switch Manager for** window, click **New virtual network switch**. In the **Create virtual switch** window, click **External** and then click **Create Virtual Switch**.

Figure 42: Create Virtual Switch



Created: 9/7/2021 2:47
Configuration Version: 9.0
Generation: 1
Notes: None

Create virtual switch

What type of virtual switch do you want to create?

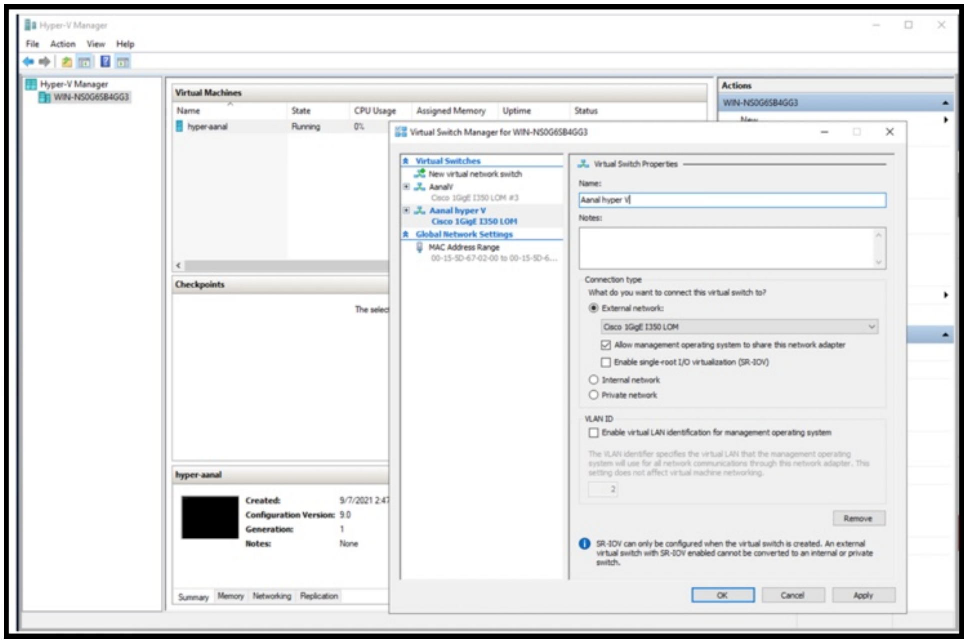
- External
- Internal
- Private

Create Virtual Switch

Creates a virtual switch that binds to the physical network adapter so that virtual machines can access a physical network.

Step 12 In the **Virtual Switch Properties** window, provide a **Name** for the switch. From the **Connection Type** area, click the **External Network** radio button, and choose a network, and then click **Apply**.

Figure 43: Virtual Switch Properties



Created: 9/7/2021 2:47
Configuration Version: 9.0
Generation: 1
Notes: None

Virtual Switch Properties

Name: Aanal hyper V

Notes:

Connection type

What do you want to connect this virtual switch to?

● External network: Cisco 1GigE I350 LOM

☑ Allow management operating system to share this network adapter

□ Enable single-root I/O virtualization (SR-IOV)

○ Internal network

○ Private network

VLAN ID

□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

Downloading and Deploying HYPER-V

Before you begin

Create a vSwitch on HYPER-V. connector connects to this vSwitch. See Creating a Virtual Switch, on page 35

Procedure

Step 1 Download connector .hyperv (HYPERV) image from Cisco.com.

cisco-spaces-connector3-i84-may2023.hyperv 5/3/2023 12:23 PM HYPERV File 5,742,600 KB

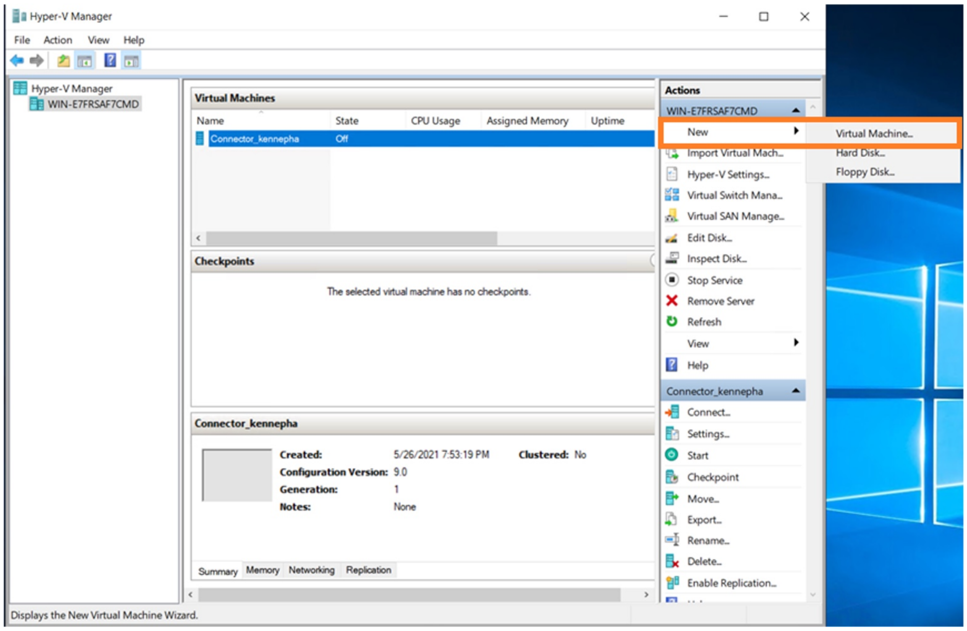
Step 2 Untar the HYPER-V to obtain a .vhdx (VHDX) file. You can use this to deploy a HYPER-V connector instance. Store the VHDX file in a folder location where you plan to create the HYPER-V instance.

For example, `. tar -xvzf cisco-spaces-connector3-i84-jul2024.hyperv or ->. tar -xvzf <cisco-spaces-connector file name>.hyperv`

Step 3 Open **Hyper-V Manager**.

Step 4 Right-click the vSwitch created, and choose **New** > **Virtual machine**.

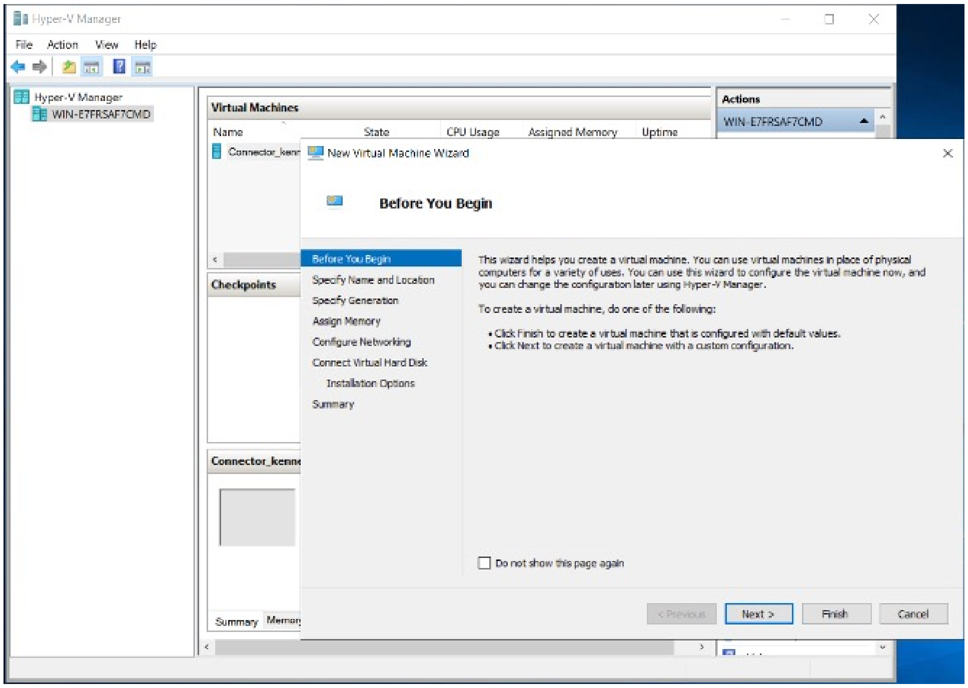
Figure 44: Create New Virtual Machine



Note
Do not use the **Import Virtual Machine** or **New** > **Hard Disk** options.

Step 5 Click **Next** to begin HYPER-V deployment.

Figure 45: Click Next to Begin Deployment



This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

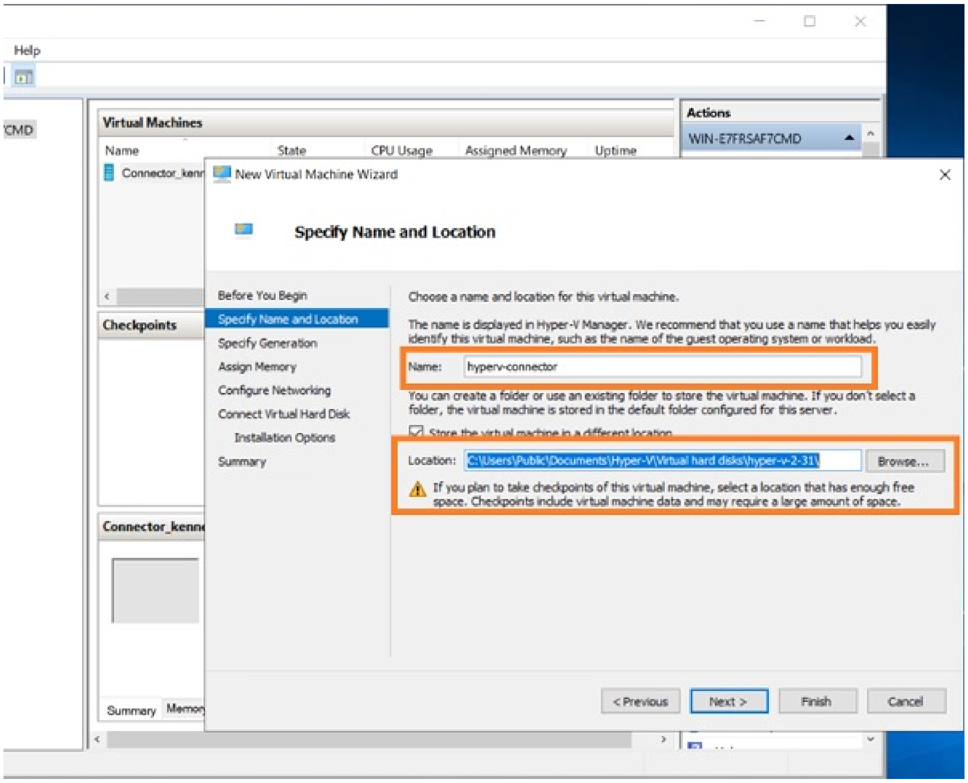
To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

☐ Do not show this page again

Step 6 Provide the **Name** of the connector and select the location to create the virtual machine.

Figure 46: Name of Connector



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: hyperv-connector

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

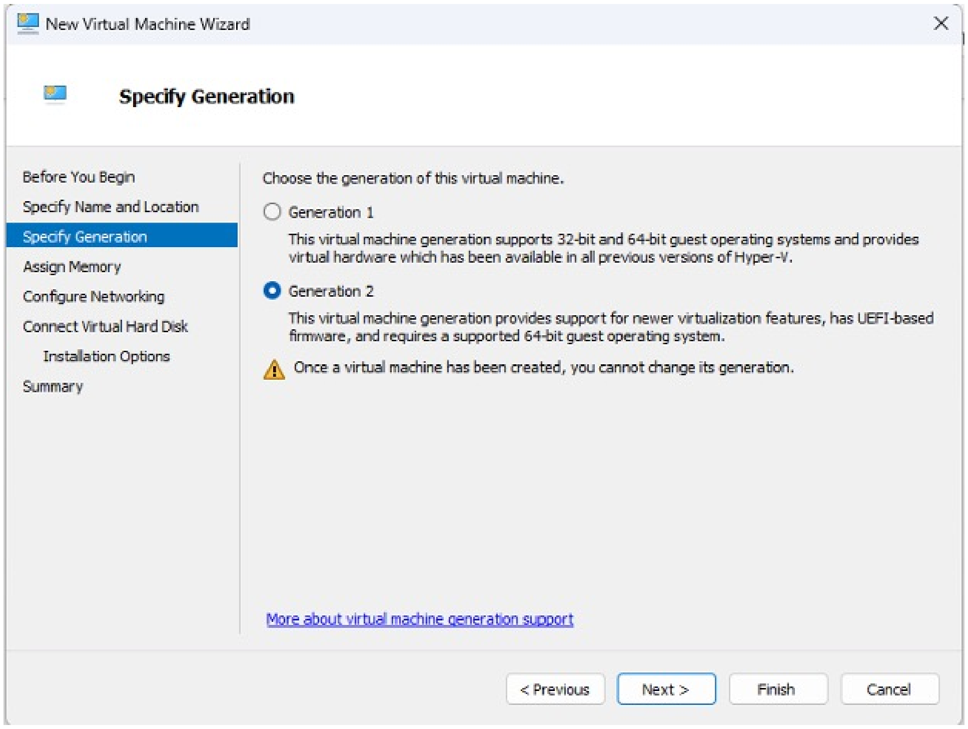
☑ Store the virtual machine in a different location

Location: C:\Users\Public\Documents\Hyper-V\Virtual hard disks\hyper-v-2-31\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

Step 7 In the **Specify Generation** window, choose **Generation 2** VM.

Figure 47: Specify Generation



New Virtual Machine Wizard

Specify Generation

Choose the generation of this virtual machine.

○ Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

● Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

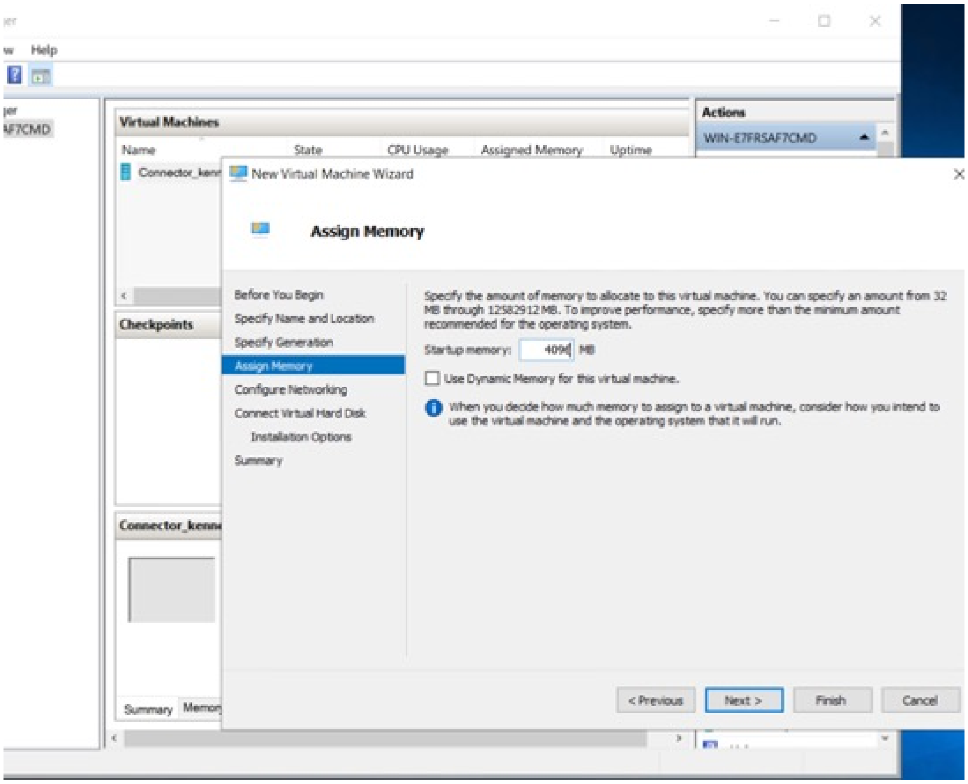
More about virtual machine generation support

Step 8 In the **Assign Memory** window, specify 4096 MB (4GB) of memory for the virtual machine instance.

Note

4096 MB (4GB) of memory is equivalent to the standard configuration of HYPER-V.

Figure 48: Assign Memory



Assign Memory

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

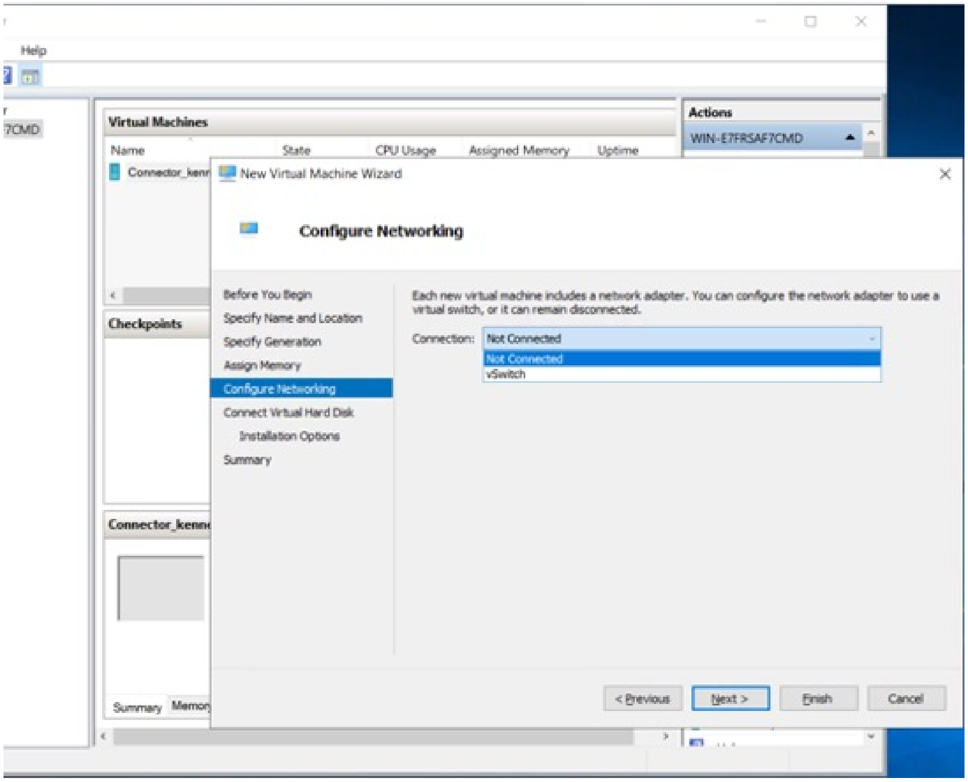
Startup memory: 4096 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

Step 9 In the **Configure Networking** window, select the vSwitch that you created as a prerequisite.

Figure 49: Configure Networking



New Virtual Machine Wizard

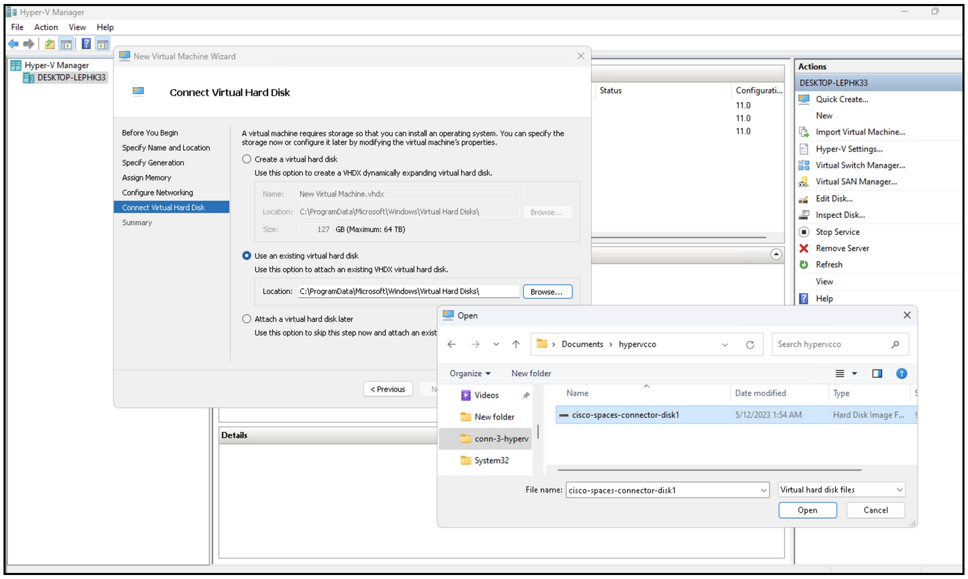
Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected

Step 10 In the **Connect Virtual Hard Disk** window, select the **Use an existing hard disk** option, and select the folder location where the VHDX file has been stored (Step 1).

Figure 50: Connect Virtual Hard Disk



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: New Virtual Machine.vhdx

Location: C:\ProgramData\Microsoft\Windows\Virtual Hard Disks\

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

Use this option to attach an existing VHDX virtual hard disk.

Location: C:\ProgramData\Microsoft\Windows\Virtual Hard Disks\

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an exist

Open

Documents › hypervcco

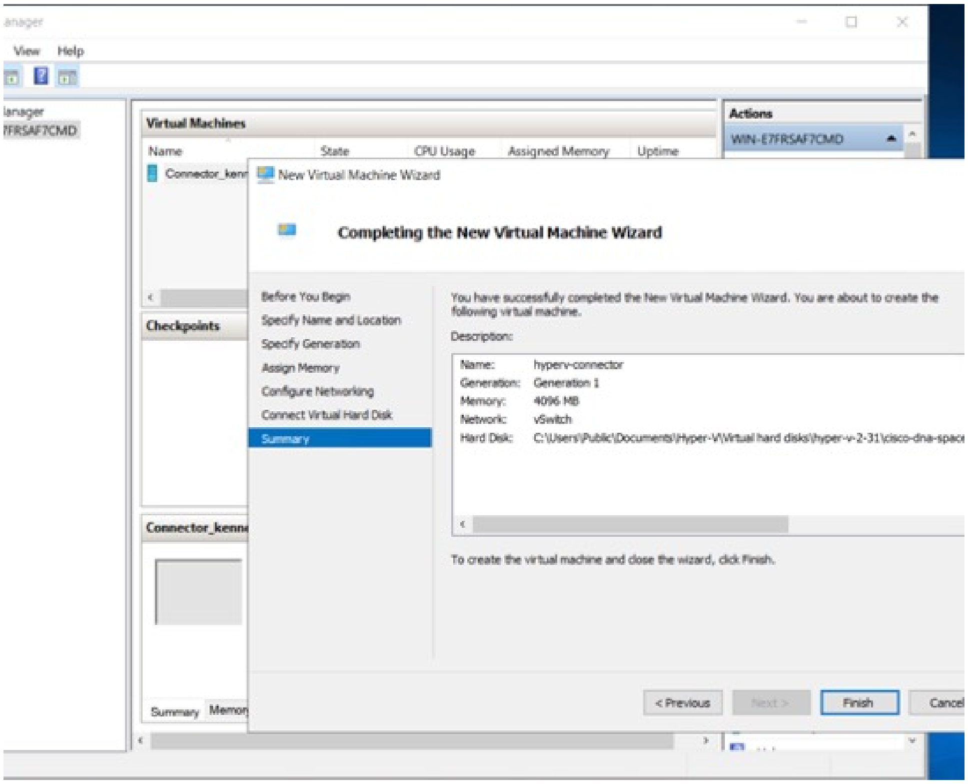
Name	Date modified	Type
cisco-spaces-connector-disk1	5/12/2023 1:54 AM	Hard Disk Image F...

File name: cisco-spaces-connector-disk1

Virtual hard disk files

Step 11 In the **Completing the New Machine Wizard** window, a final summary is displayed. Review this summary and click **Finish**.

Figure 51: Completing the New Machine Wizard



Completing the New Virtual Machine Wizard

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

Name: hyperv-connector
Generation: Generation 1
Memory: 4096 MB
Network: vSwitch
Hard Disk: C:\Users\Public\Documents\Hyper-V\Virtual hard disks\hyper-v-2-31\cisco-dna-space

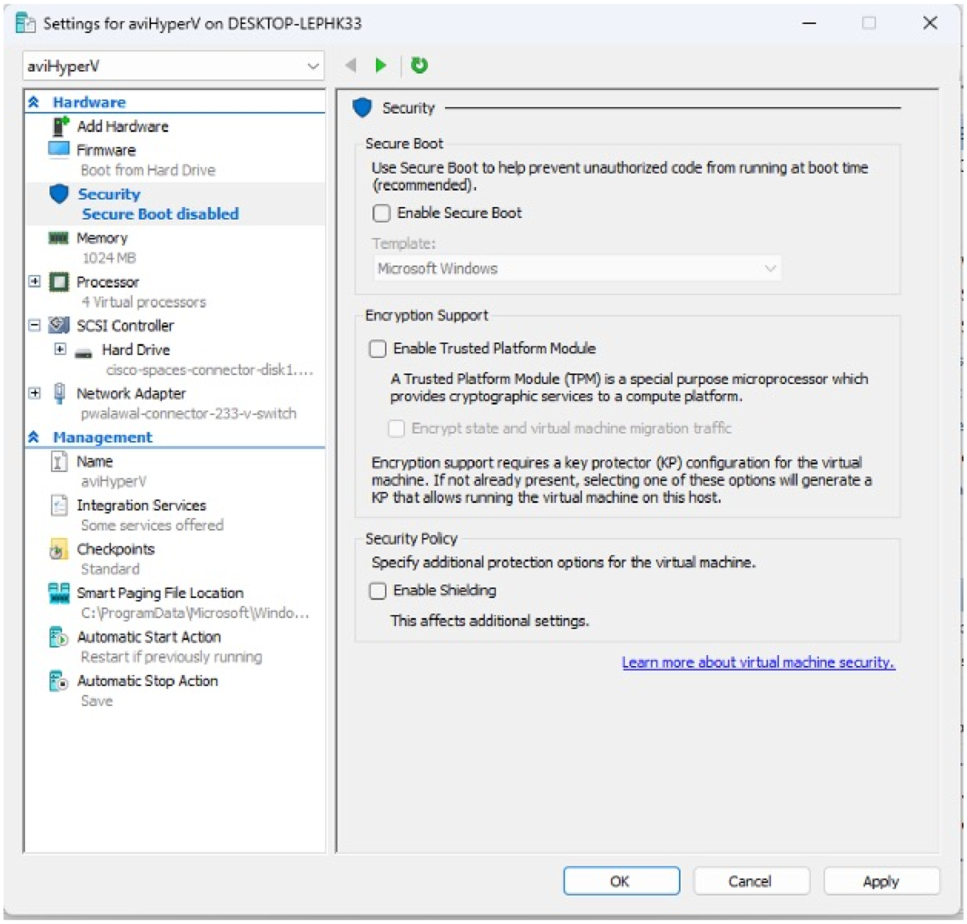
To create the virtual machine and close the wizard, click Finish.

A HYPER-V instance is created.

Step 12 Select the HYPER-V instance created, and click **Settings**.

a) Navigate to **Security** and ensure you **uncheck** the **Enable Secure Boot** check box and leave the secure boot feature disabled.

Figure 52: Enable Secure Boot



Settings for aviHyperV on DESKTOP-LEPHK33

aviHyperV

- **Hardware**
  - Add Hardware
  - Firmware
    Boot from Hard Drive
  - **Security**
    Secure Boot disabled
  - Memory
    1024 MB
  - Processor
    4 Virtual processors
  - SCSI Controller
    - Hard Drive
      cisco-spaces-connector-disk1....
  - Network Adapter
    pwalawal-connector-233-v-switch
- **Management**
  - Name
    aviHyperV
  - Integration Services
    Some services offered
  - Checkpoints
    Standard
  - Smart Paging File Location
    C:\ProgramData\Microsoft\Windo...
  - Automatic Start Action
    Restart if previously running
  - Automatic Stop Action
    Save

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

□ Enable Secure Boot

Template:
Microsoft Windows

Encryption Support

□ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

□ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

Security Policy

Specify additional protection options for the virtual machine.

□ Enable Shielding

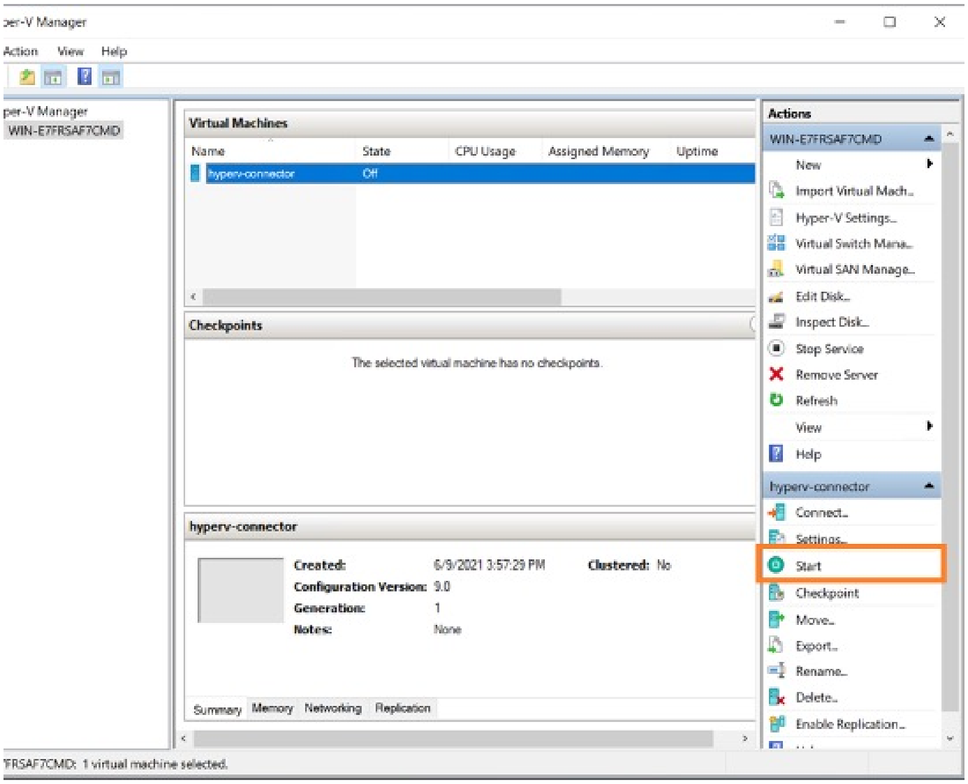
This affects additional settings.

Learn more about virtual machine security.

b) Navigate to **Processor** and ensure that CPU count is set to 2 vCPUs to match **Standard** connector deployment.

Step 13 Select the HYPER-V instance created, and click **Start**.

Figure 53: Select The Hyper-V Instance



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime
hyperv-connector	Off			

Checkpoints

The selected virtual machine has no checkpoints.

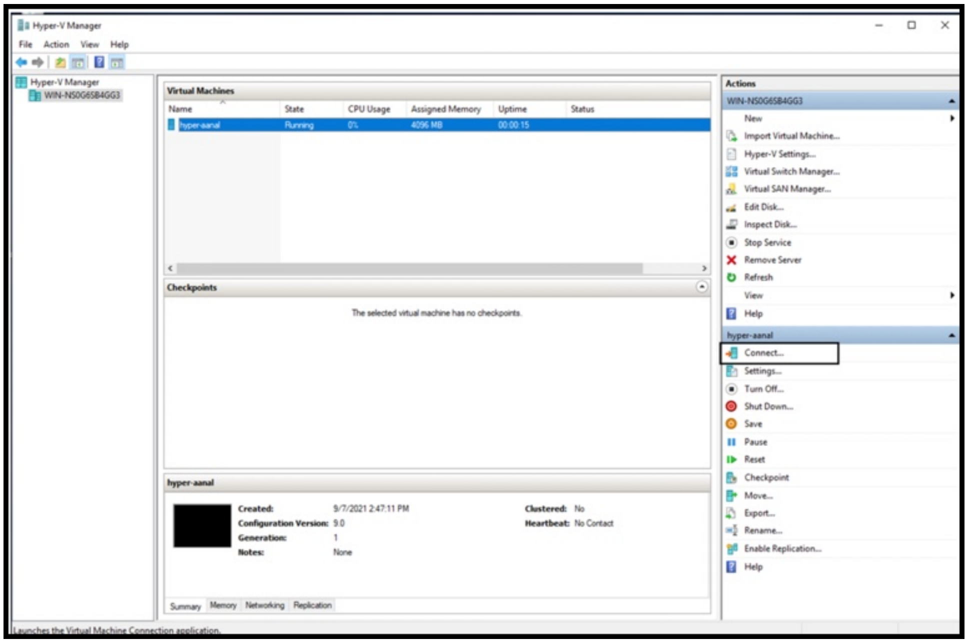
hyperv-connector

Created: 6/9/2021 3:57:29 PM
Configuration Version: 9.0
Generation: 1
Notes: None
Clustered: No

'FRSAF7CMD: 1 virtual machine selected.

Step 14 Select the HYPER-V instance created, and click **Connect** to open the HYPER-V console.

Figure 54: Select The Hyper-V Instance



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status
hyper-aanal	Running	0%	4096 MB	00:00:15	

Checkpoints

The selected virtual machine has no checkpoints.

hyper-aanal

Created: 9/7/2021 2:47:11 PM
Configuration Version: 9.0
Generation: 1
Notes: None
Clustered: No
Heartbeat: No Contact

Launches the Virtual Machine Connection application.

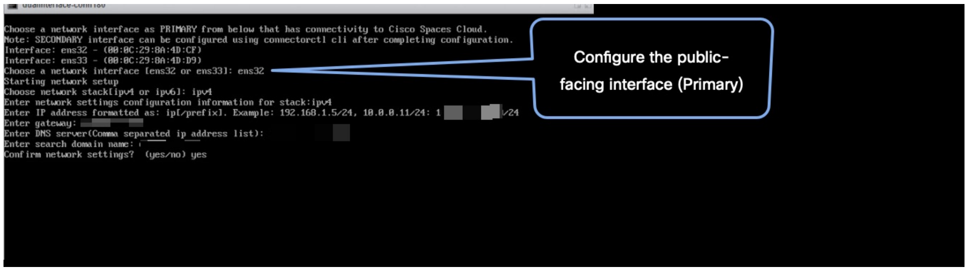
The virtual machine terminal is opened.

Step 15 Log in to the terminal and enter the default username **root** and default password **root**.

Step 16 Configure the host name for the connector.

Step 17 Choose an network interface to configure as PRIMARY.

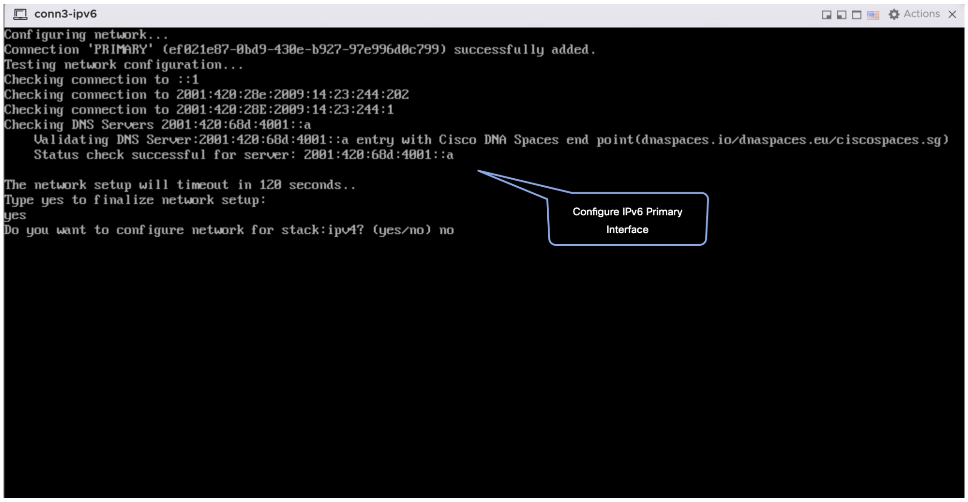
Figure 55: Configuring the Primary Interface: IPv4



```
Choose a network interface as PRIMARY from below that has connectivity to Cisco Spaces Cloud.
Note: SECONDARY interface can be configured using connectorctl cli after completing configuration.
Interface: ens32 - (00:0C:29:8A:4D:CF)
Interface: ens33 - (00:0C:29:8A:4D:D9)
Choose a network interface [ens32 or ens33]: ens32
Starting network setup
Choose network stack[ipv4 or ipv6]: ipv4
Enter network settings configuration information for stack:ipv4
Enter IP address formatted as: ip[/prefix]. Example: 192.168.1.5/24, 10.0.0.11/24: 1[redacted]/24
Enter gateway: [redacted]
Enter DNS server(Comma separated ip address list): [redacted]
Enter search domain name: [redacted]
Confirm network settings?  (yes/no) yes
```

Configure the public-facing interface (Primary)

Figure 56: Configuring the Primary Interface: IPv6



```
Configuring network...
Connection 'PRIMARY' (ef021e87-0bd9-430e-b927-97e996d0c799) successfully added.
Testing network configuration...
Checking connection to ::1
Checking connection to 2001:420:28e:2009:14:23:244:202
Checking connection to 2001:420:28E:2009:14:23:244:1
Checking DNS Servers 2001:420:68d:4001::a
    Validating DNS Server:2001:420:68d:4001::a entry with Cisco DNA Spaces end point(dnaspaces.io/dnaspaces.eu/ciscospaces.sg)
    Status check successful for server: 2001:420:68d:4001::a

The network setup will timeout in 120 seconds..
Type yes to finalize network setup:
yes
Do you want to configure network for stack:ipv4? (yes/no) no
```

Configure IPv6 Primary Interface

Step 18 Do one of the following, and then configure the network settings for the PRIMARY interface. Specify parameters such as IP address, hostname, and so on.

- Configure the IPv6 stack.
- Configure the IPv4 stack.

You can add multiple DNS servers as a comma separated list in this step. After the task is complete and the Cisco Spaces: Connector is deployed, you can login to the connector CLI, and run the **connectorctl network config** command to add more DNS servers or edit the existing list.

Step 19 Confirm the setup.

Note

Because this configuration window times out in 120 seconds, ensure that you provide the input on time to avoid reconfiguration.

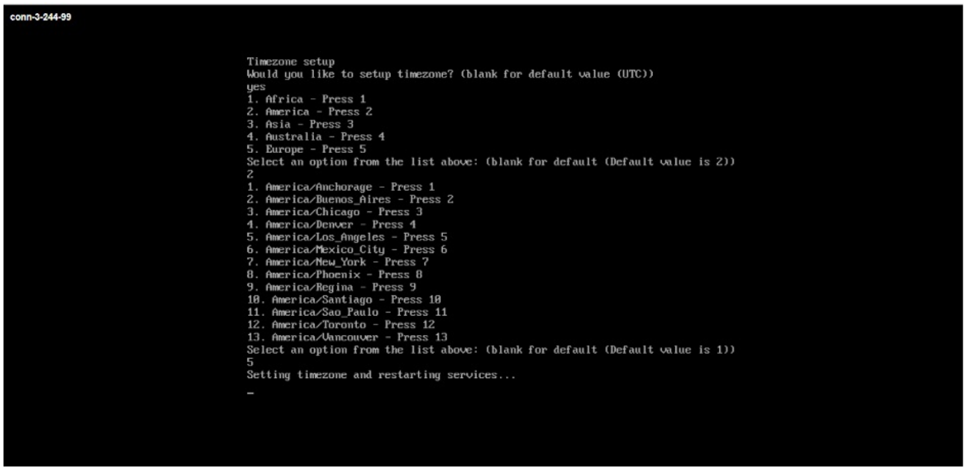
Step 20 Reset the password for the **spacesadmin** user.

Note

The **spacesadmin** password can only include special characters such as '@' or '!' and must not contain any spaces.

Step 21 Enter the time zone.

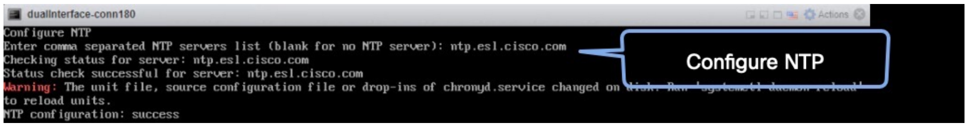
Figure 57: Time Zone



```
Timezone setup
Would you like to setup timezone? (blank for default value (UTC))
yes
1. Africa - Press 1
2. America - Press 2
3. Asia - Press 3
4. Australia - Press 4
5. Europe - Press 5
Select an option from the list above: (blank for default (Default value is 2))
2
1. America/Anchorage - Press 1
2. America/Buenos_Aires - Press 2
3. America/Chicago - Press 3
4. America/Denver - Press 4
5. America/Los_Angeles - Press 5
6. America/Mexico_City - Press 6
7. America/New_York - Press 7
8. America/Phoenix - Press 8
9. America/Regina - Press 9
10. America/Santiago - Press 10
11. America/Sao_Paulo - Press 11
12. America/Toronto - Press 12
13. America/Vancouver - Press 13
Select an option from the list above: (blank for default (Default value is 1))
5
Setting timezone and restarting services...
_
```

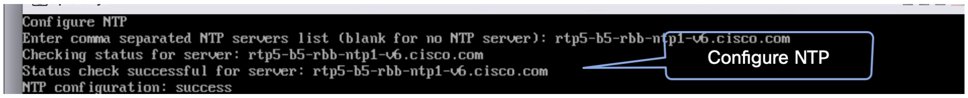
Step 22 Enter the Network Time Protocol (NTP) server name to synchronize the system time with that of NTP server, or leave it blank if you do not want to configure an NTP server.

Figure 58: Configure NTP



```
Configure NTP
Enter comma separated NTP servers list (blank for no NTP server): ntp.esl.cisco.com
Checking status for server: ntp.esl.cisco.com
Status check successful for server: ntp.esl.cisco.com
Warning: The unit file, source configuration file or drop-ins of chronyd.service changed on disk. Run 'systemctl daemon-reload'
to reload units.
NTP configuration: success
```

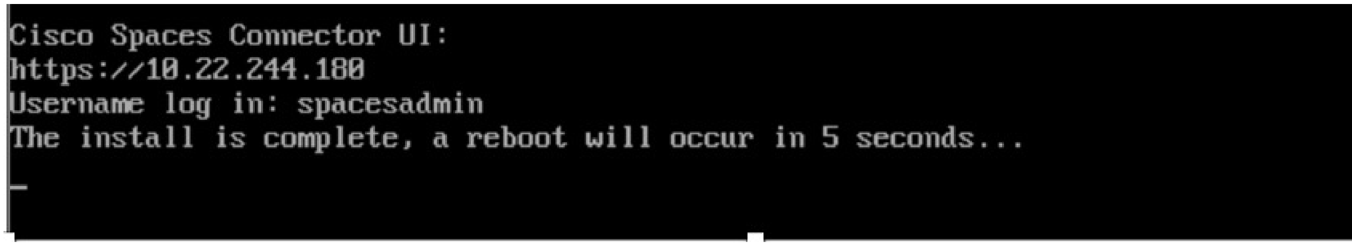
Figure 59: Configure NTP



```
Configure NTP
Enter comma separated NTP servers list (blank for no NTP server): rtp5-b5-rbb-ntp1-v6.cisco.com
Checking status for server: rtp5-b5-rbb-ntp1-v6.cisco.com
Status check successful for server: rtp5-b5-rbb-ntp1-v6.cisco.com
NTP configuration: success
```

Step 23 Note the URL (https://connector-ip) before the automatic reboot. You can use this URL later to open the connector GUI.

Figure 60: ConnectorGUI



```
Cisco Spaces Connector UI:
https://10.22.244.180
Username log in: spacesadmin
The install is complete, a reboot will occur in 5 seconds...
_
```

CHAPTER 6

Cisco Spaces: Connector: Azure VMware

Cisco Spaces: Connector: Azure VMware

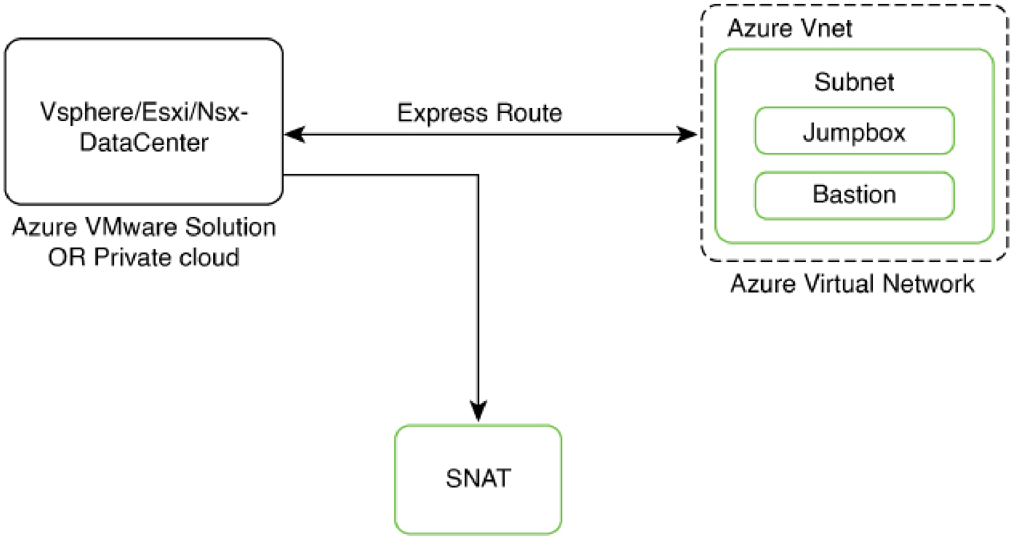
Note This Azure VMware solution is not supported and we recommend following the Cisco Spaces: Connector VM on Azure Environment guide.

The chapter shows you how to install a connector on Azure VMware. To do this, you must understand the various components of this solution.

- The **Azure VMware Solution (AVS) or Private Cloud** is a service offered by Microsoft Azure in collaboration with VMware. It enables organizations to run and manage VMware workloads natively on Azure infrastructure. You can host services such as Cisco Spaces: Connector or wireless controllers.
- **Azure Virtual Network (VNet)** is a building block in Microsoft Azure that enables you to securely connect and isolate Azure resources. It provides a way to create private, isolated, and highly available networks in the Azure cloud. You can deploy some of these services on this VNet:
  - **Azure Bastion** is a service provided by Microsoft Azure for secure and seamless Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to virtual machines (VMs) in the Azure cloud. It acts as a secure gateway, eliminating the need to expose VMs on the Private Cloud to the public internet, and reducing the attack surface. With Azure Bastion, you can connect to your VMs directly from the Azure portal using a web browser, without the need for a public IP address or a VPN connection.
  - **Jumpbox (or Jump Server):** Jumpbox, or jump server, is a security measure used in networking environments. It's a system that sits between an internal network and external networks (such as the internet) and is a single point of entry for administrators. Instead of allowing administrators to connect directly to critical systems such as connector on the Private Cloud, they connect first to the jumpbox, which acts as a gateway to access other systems. This adds an additional layer of security and control over who can access sensitive systems.
- **Source Network Address Translation (SNAT):** SNAT refers to a type of network address translation that translates the source IP address of outgoing traffic. SNAT is commonly used in scenarios where

multiple private IP addresses from a local network need to access resources on the internet or another network.

Figure 61: Various Components to InstallConnector onAzure VMware



To deploy a connector on Azure VMware, you have to do the following:

1. Creating an Azure VMware solution (or Private Cloud), on page 54 and deploying the connector OVA on it.
2. Creating an Azure Virtual Network, on page 58. You can then allow administrators and users to access the connector through this VNet.

Creating an Azure VMware solution (or Private Cloud)

This chapter provides information about how to download and deploy the Cisco Spaces: Connector and obtain the URL for the connector GUI.

Before you begin

- Identify the subscription you plan to use for the Azure VMware solution.
- Identify the Size Hosts. This requires you to raise a case with Azure customer support.
- Identify the address range and subnet for the private cloud. All your VMware resources including connector are hosted in this IP range.

SUMMARY STEPS

1. Log in to portal.azure.com.
2. Create a **Resource**.
3. Choose the **Azure VMware Solution** service.
4. In the **Create a private cloud** window that appears, fill the required details.

5. Configure a segment for the private cloud.
6. Specify the DHCP range to be used for this segment.
7. Specify a DNS from the left-navigation pane or while installing the connector later.
    - You can use a public DNS while deploying the connector.
    - You can configure an internal DNS from the left-navigation pane.
8. Provide internet connectivity using SNAT. From the left-navigation pane, click **Internet Connectivity > Connect using SNAT**. This enables outbound internet access for this private cloud.
9. Find the credentials of this private cloud. From the private-cloud left pane, click **VMware credentials**. You can observe the credentials of various components of the private cloud. Make a note of these credentials for later use.

DETAILED STEPS

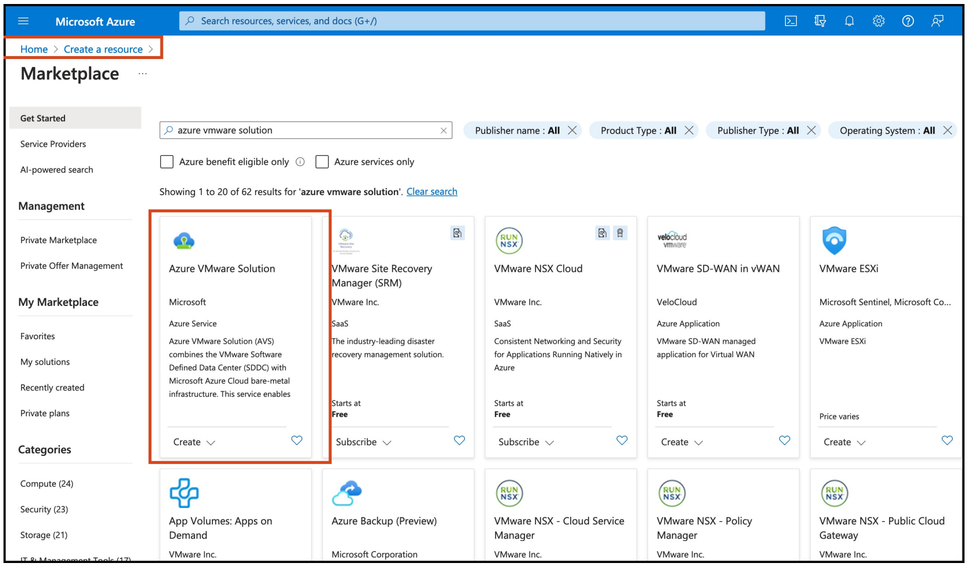
Procedure

Step 1 Log in to portal.azure.com.

Step 2 Create a **Resource**.

From the left-navigation pane, click **Create a Resource**.

Figure 62: Create a Resource


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource >
Marketplace ...
Get Started
Service Providers
AI-powered search
Management
Private Marketplace
Private Offer Management
My Marketplace
Favorites
My solutions
Recently created
Private plans
Categories
Compute (24)
Security (23)
Storage (21)
IT & Management Tools (17)
azure vmware solution
Publisher name : All
Product Type : All
Publisher Type : All
Operating System : All
□ Azure benefit eligible only
□ Azure services only
Showing 1 to 20 of 62 results for 'azure vmware solution'. Clear search
Azure VMware Solution
Microsoft
Azure Service
Azure VMware Solution (AVS) combines the VMware Software Defined Data Center (SDDC) with Microsoft Azure Cloud bare-metal infrastructure. This service enables
Create
VMware Site Recovery Manager (SRM)
VMware Inc.
SaaS
The industry-leading disaster recovery management solution.
Starts at Free
Subscribe
VMware NSX Cloud
VMware Inc.
SaaS
Consistent Networking and Security for Applications Running Natively in Azure
Starts at Free
Subscribe
VMware SD-WAN in vWAN
VeloCloud
Azure Application
VMware SD-WAN managed application for Virtual WAN
Starts at Free
Create
VMware ESXi
Microsoft Sentinel, Microsoft Co...
Azure Application
VMware ESXi
Price varies
Create
App Volumes: Apps on Demand
VMware Inc.
Azure Backup (Preview)
Microsoft Corporation
VMware NSX - Cloud Service Manager
VMware Inc.
VMware NSX - Policy Manager
VMware Inc.
VMware NSX - Public Cloud Gateway
VMware Inc.

Step 3 Choose the **Azure VMware Solution** service.

a) In the **Search services and marketplace** field, search for an **Azure VMware solution.**

b) From the displayed search results, click **Create** and choose the **Azure VMware solution.**

Step 4 In the **Create a private cloud** window that appears, fill the required details.

a) Choose a subscription.

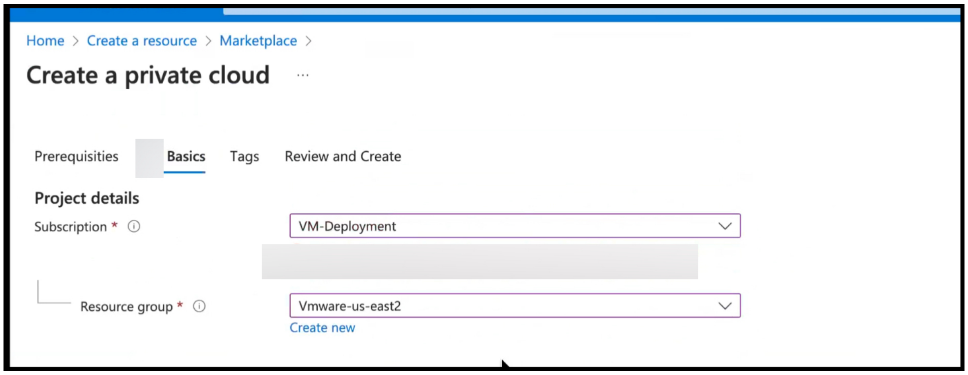
b) Choose a resource group or create a new one.

c) Choose the location of the service.

d) Choose the size of the host.
e) Choose the host location.
f) Choose the number of hosts. The minimum number of hosts is three.
g) Enter the address block. This IP address block is used to deploy various services such as connector, and these services are accessible via a browser from the Azure Virtual Network.

The Azure VMware solution (or private cloud) is created.

Figure 63: Create a private cloud


Home > Create a resource > Marketplace >
Create a private cloud ...
Prerequisites
Basics
Tags
Review and Create

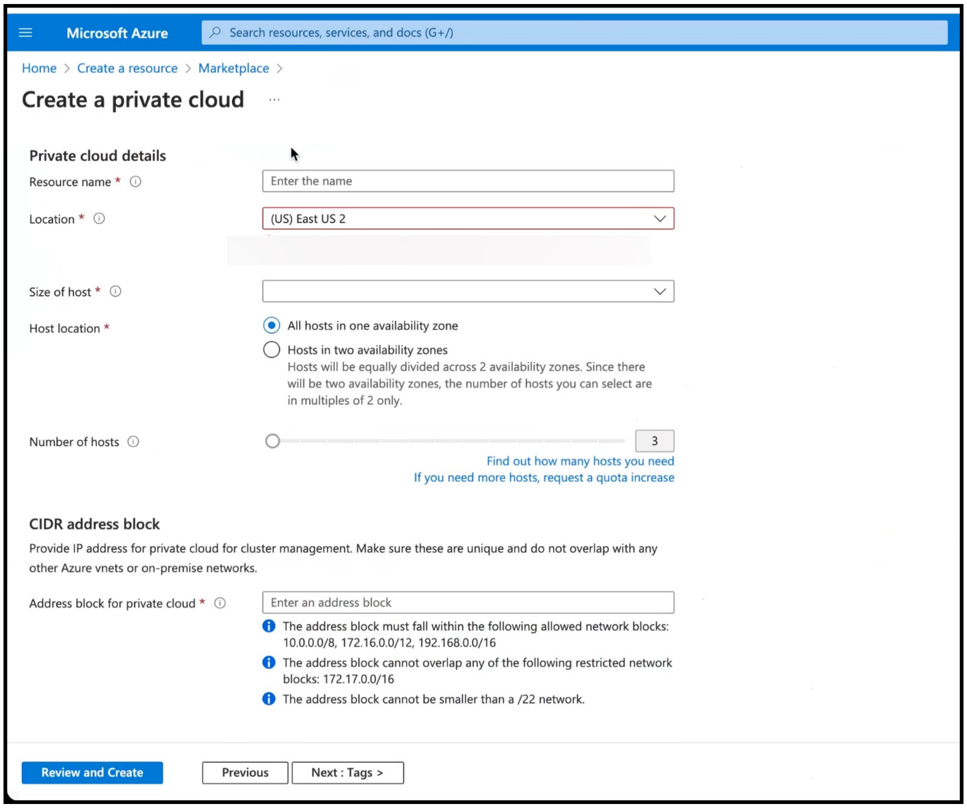
Project details

Subscription * ⓘ VM-Deployment

Resource group * ⓘ Vmware-us-east2

Create new

Figure 64: Create a private cloud


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Marketplace >
Create a private cloud ...
Find out how many hosts you need
If you need more hosts, request a quota increase
Review and Create
Previous
Next : Tags >

Private cloud details

Resource name * ⓘ Enter the name

Location * ⓘ (US) East US 2

Size of host * ⓘ

Host location *

● All hosts in one availability zone

○ Hosts in two availability zones
Hosts will be equally divided across 2 availability zones. Since there will be two availability zones, the number of hosts you can select are in multiples of 2 only.

Number of hosts ⓘ 3

CIDR address block

Provide IP address for private cloud for cluster management. Make sure these are unique and do not overlap with any other Azure vnets or on-premise networks.

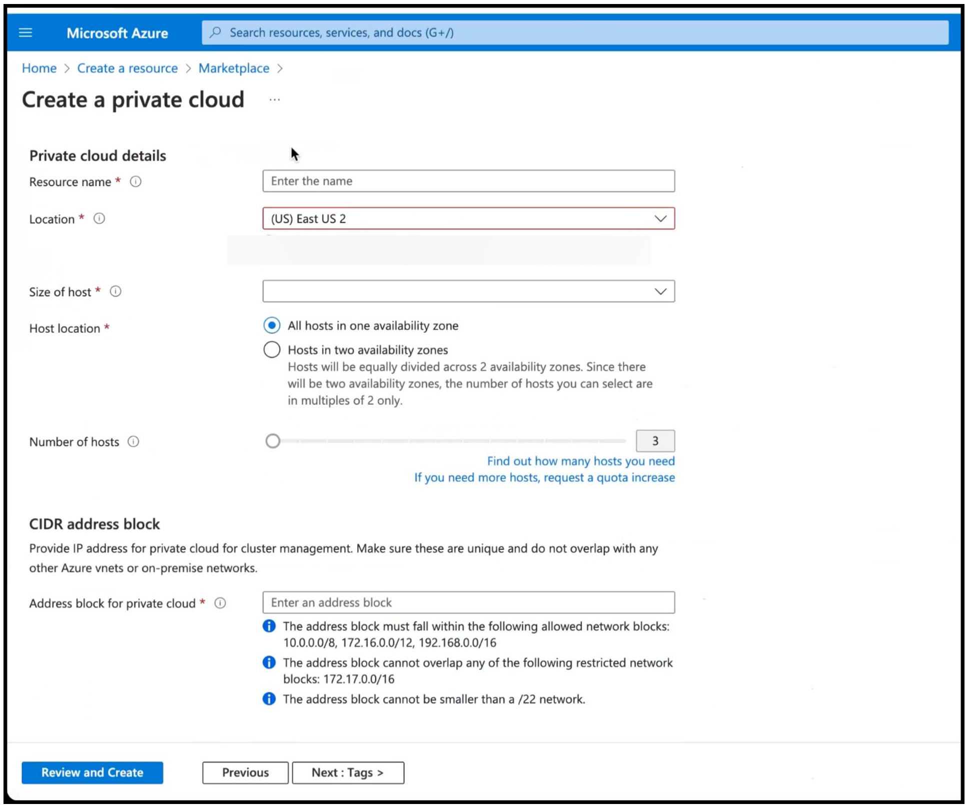
Address block for private cloud * ⓘ Enter an address block

- The address block must fall within the following allowed network blocks: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- The address block cannot overlap any of the following restricted network blocks: 172.17.0.0/16
- The address block cannot be smaller than a /22 network.

Step 5 Configure a segment for the private cloud.

a) From the private-cloud left pane, click **Segments**. You can see that a default segment has already been created and allocated with addresses from the address range specified by you earlier. You can use this existing segment or create a new one.

Figure 65: Create a Segment


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Marketplace >
Review and Create
Previous
Next : Tags >

Create a private cloud ...

Private cloud details

Resource name * ⓘ Enter the name

Location * ⓘ (US) East US 2

Size of host * ⓘ

Host location *
● All hosts in one availability zone
○ Hosts in two availability zones
Hosts will be equally divided across 2 availability zones. Since there will be two availability zones, the number of hosts you can select are in multiples of 2 only.

Number of hosts ⓘ 3

Find out how many hosts you need
If you need more hosts, request a quota increase

CIDR address block

Provide IP address for private cloud for cluster management. Make sure these are unique and do not overlap with any other Azure vnets or on-premise networks.

Address block for private cloud * ⓘ Enter an address block

- The address block must fall within the following allowed network blocks: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- The address block cannot overlap any of the following restricted network blocks: 172.17.0.0/16
- The address block cannot be smaller than a /22 network.

Step 6 Specify the DHCP range to be used for this segment.

a) From the private-cloud left pane, click **DHCP**.

b) Select the **DHCP type** as **SERVER**.

c) Enter the **Server Name** as the segment chosen earlier for this private cloud.

d) Enter the **Server IP address** as the segment address range selected earlier.

Step 7 Specify a DNS from the left-navigation pane or while installing the connector later.

- You can use a public DNS while deploying the connector.
- You can configure an internal DNS from the left-navigation pane.

Step 8 Provide internet connectivity using SNAT. From the left-navigation pane, click **Internet Connectivity** > **Connect using SNAT**. This enables outbound internet access for this private cloud.

Step 9 Find the credentials of this private cloud. From the private-cloud left pane, click **VMware credentials**. You can observe the credentials of various components of the private cloud. Make a note of these credentials for later use.

Figure 66: Various Components to InstallConnector onAzure VMware

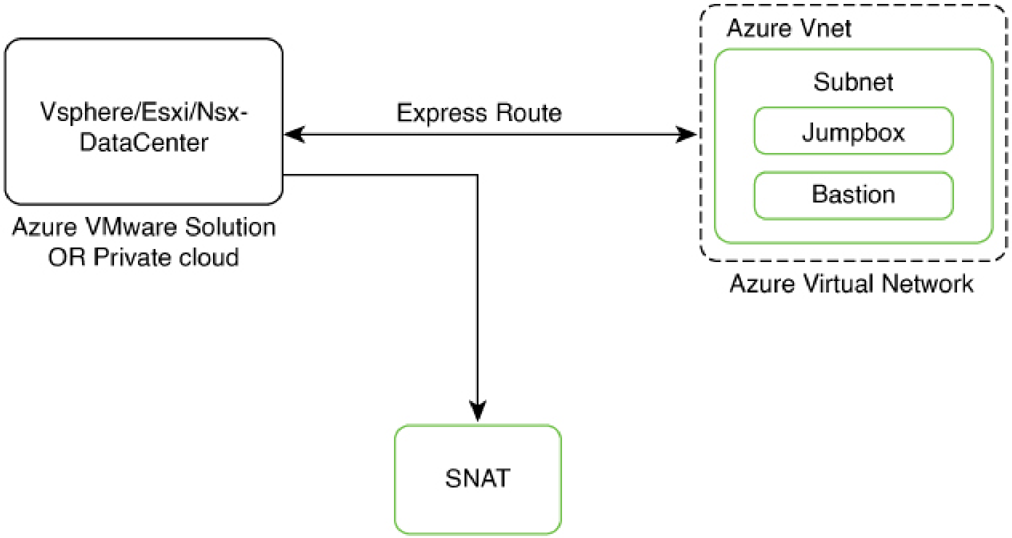
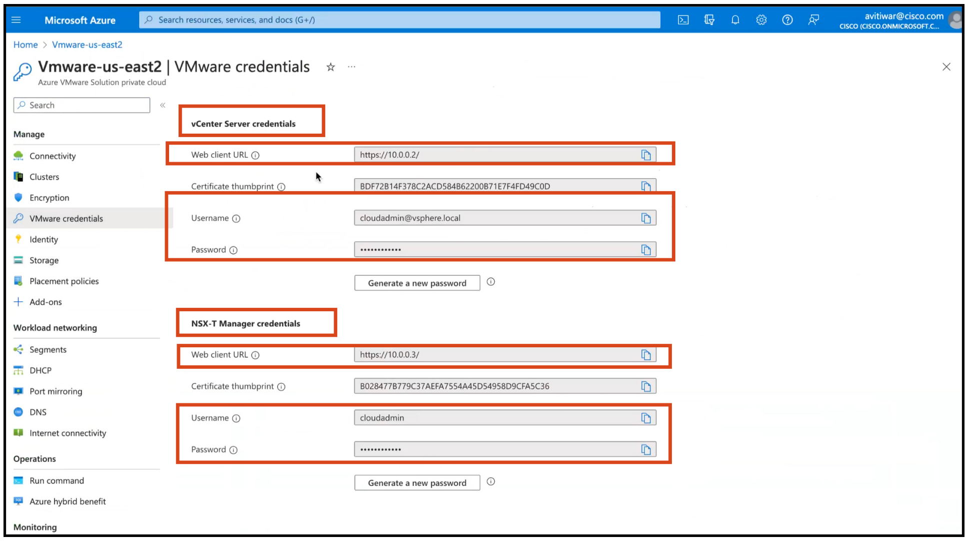


Figure 67: VMware Credentials



Vmware-us-east2 | VMware credentials

Azure VMware Solution private cloud

vCenter Server credentials

Web client URL: https://10.0.0.2/

Certificate thumbprint: BDF72B14F378C2ACD584B62200B71E7F4FD49C0D

Username: cloudadmin@vsphere.local

Password: ••••••••••••

NSX-T Manager credentials

Web client URL: https://10.0.0.3/

Certificate thumbprint: B028477B779C37AEFA7554A45D54958D9CFA5C36

Username: cloudadmin

Password: ••••••••••••

Note

Note that ESXi also inherits the vSphere credentials.

Creating an Azure Virtual Network

Before you begin

Create a Azure VMware solution (or Private Cloud) and configure it with SNAT.

Procedure

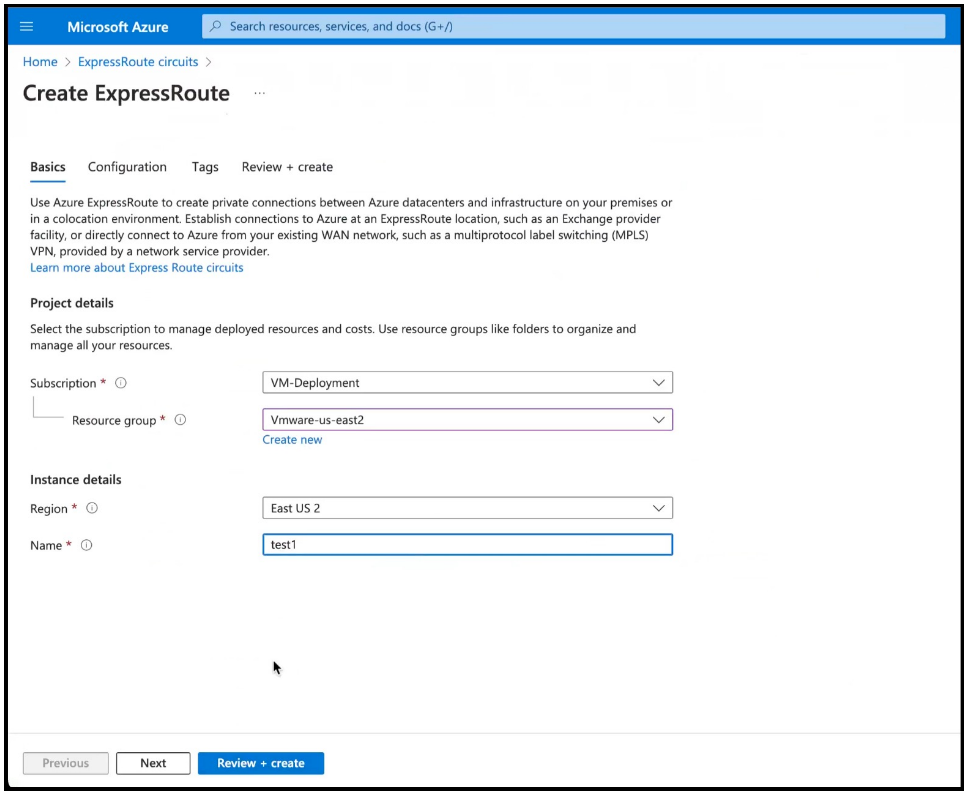
Step 1 Create an **ExpressRoute**.

a) From the Microsoft Azure Home Page, click **ExpressRoute circuits**.

b) From the **ExpressRoute circuits** page that is displayed, click **Create**.

c) From the **Create ExpressRoute** page that is displayed, enter the details of the **Basic** tab. Click **Next**.

Figure 68: Basics Tab


Microsoft Azure
Search resources, services, and docs (G+/)
Home > ExpressRoute circuits >

Create ExpressRoute

Basics
Configuration
Tags
Review + create

Use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. Establish connections to Azure at an ExpressRoute location, such as an Exchange provider facility, or directly connect to Azure from your existing WAN network, such as a multiprotocol label switching (MPLS) VPN, provided by a network service provider.
Learn more about Express Route circuits

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : VM-Deployment

Resource group * : Vmware-us-east2

Create new

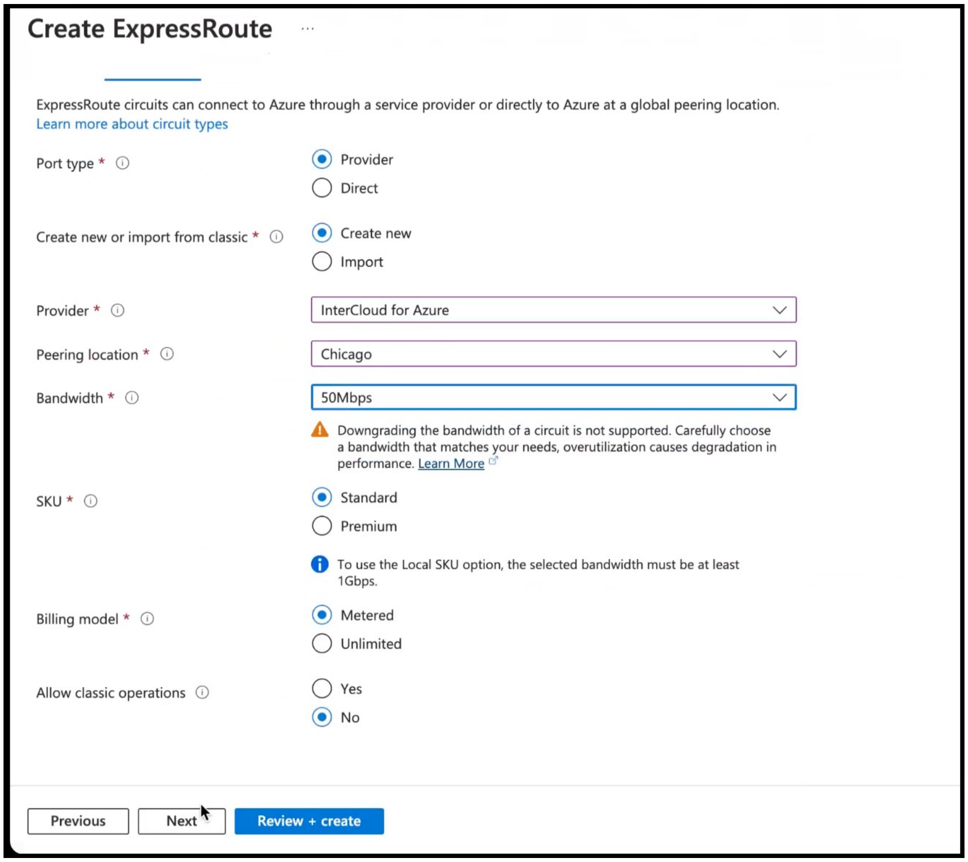
Instance details

Region * : East US 2

Name * : test1

d) Click the **Configuration** tab. Fill in details such as **Provider**.

Figure 69: Configuration Tab



Create ExpressRoute

ExpressRoute circuits can connect to Azure through a service provider or directly to Azure at a global peering location.
Learn more about circuit types

Port type * ● Provider ○ Direct

Create new or import from classic * ● Create new ○ Import

Provider * InterCloud for Azure

Peering location * Chicago

Bandwidth * 50Mbps

⚠ Downgrading the bandwidth of a circuit is not supported. Carefully choose a bandwidth that matches your needs, overutilization causes degradation in performance. Learn More

SKU * ● Standard ○ Premium

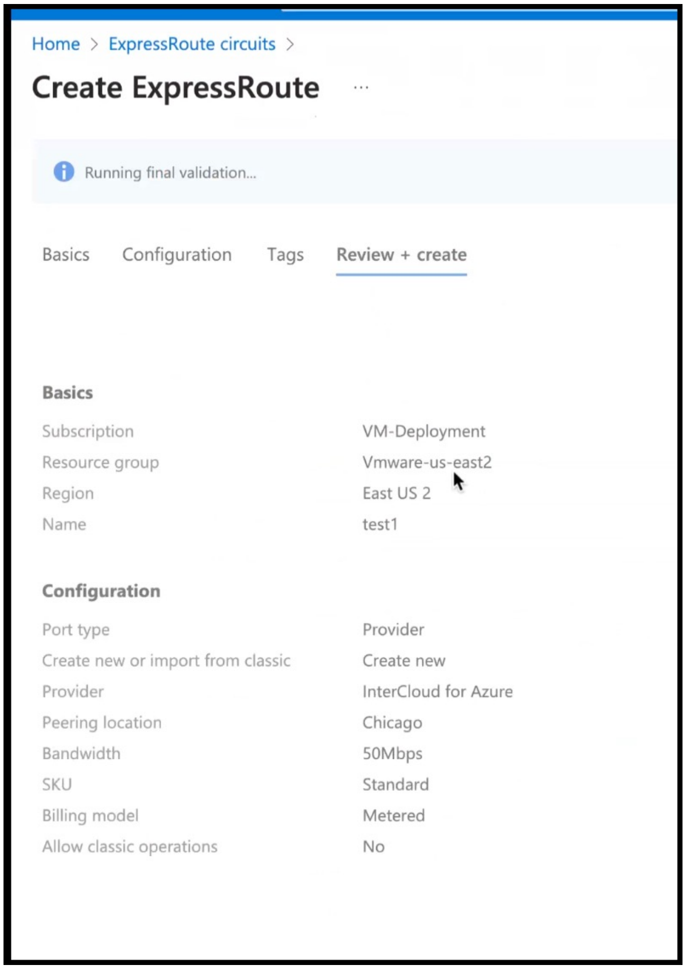
ⓘ To use the Local SKU option, the selected bandwidth must be at least 1Gbps.

Billing model * ● Metered ○ Unlimited

Allow classic operations ○ Yes ● No

e) Click the **Review + Create** tab, and review the changes you have made. Click **Create** to create the ExpressRoute.

Figure 70: Review + Create



Create ExpressRoute

Running final validation...

Basics

Subscription	VM-Deployment
Resource group	Vmware-us-east2
Region	East US 2
Name	test1

Configuration

Port type	Provider
Create new or import from classic	Create new
Provider	InterCloud for Azure
Peering location	Chicago
Bandwidth	50Mbps
SKU	Standard
Billing model	Metered
Allow classic operations	No

Step 2 From the created **Virtual Network**, do the following.

a) Create a Gateway subnet and provide an IP address.

b) Create a Bastion and provide an IP address.

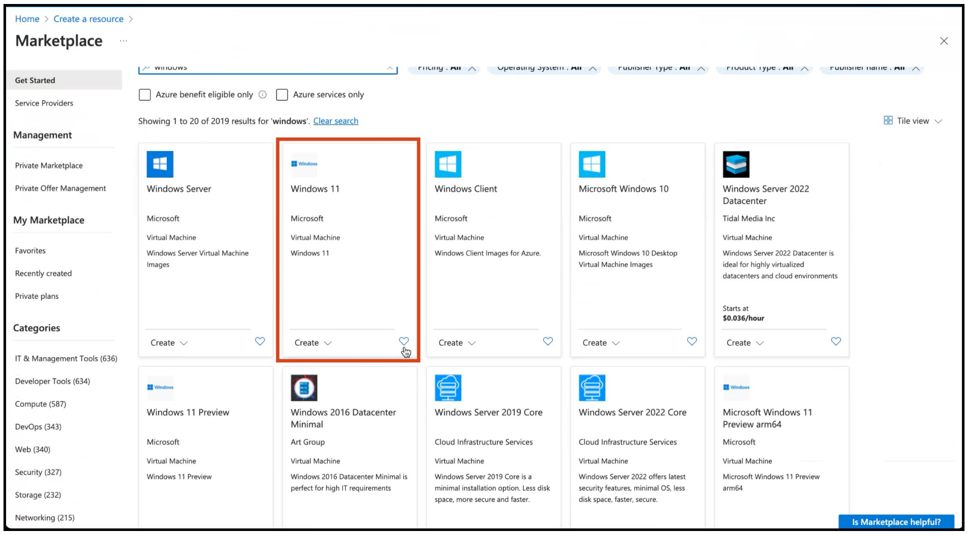
c) Create an AzureBastion subnet and provide an IP address.

Step 3 Deploy a Windows Machine as a virtual machine. You can use this as a Jumpbox to access vSphere or NSXT-Manager.

a) From the left-navigation pane, click **Create a Resource**

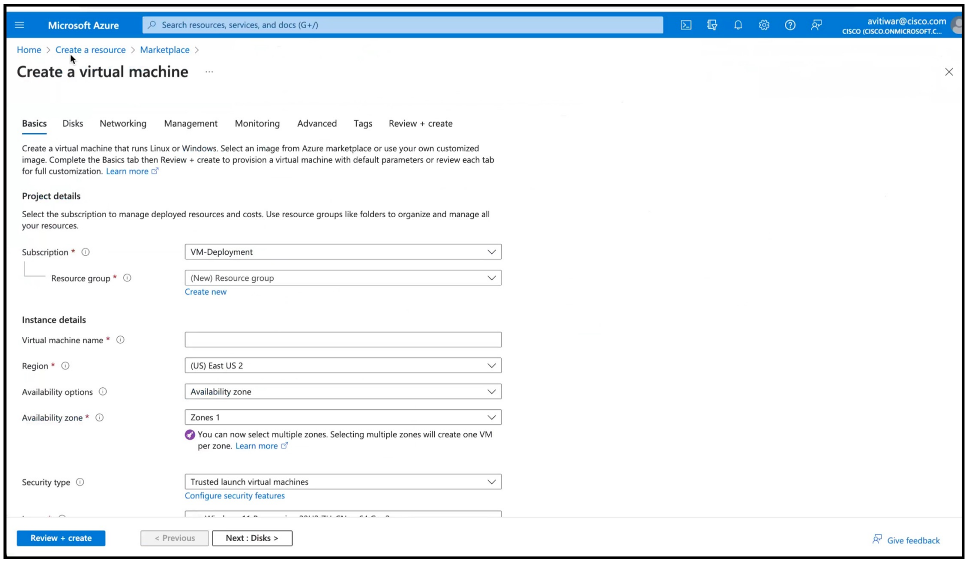
b) Search for an operating system of choice. For example, Windows 11, click **Create** and choose the version of choice.

Figure 71: Windows 11 virtual machine


Home > Create a resource >
Marketplace
Get Started
Service Providers
Management
Private Marketplace
Private Offer Management
My Marketplace
Favorites
Recently created
Private plans
Categories
IT & Management Tools (636)
Developer Tools (634)
Compute (587)
DevOps (343)
Web (340)
Security (327)
Storage (232)
Networking (215)
Azure benefit eligible only
Azure services only
Showing 1 to 20 of 2019 results for 'windows'. Clear search
Tile view
Windows Server
Microsoft
Virtual Machine
Windows Server Virtual Machine Images
Windows 11
Microsoft
Virtual Machine
Windows 11
Windows Client
Microsoft
Virtual Machine
Windows Client Images for Azure.
Microsoft Windows 10
Microsoft
Virtual Machine
Microsoft Windows 10 Desktop Virtual Machine Images
Windows Server 2022 Datacenter
Tidal Media Inc
Virtual Machine
Windows Server 2022 Datacenter is ideal for highly virtualized datacenters and cloud environments
Starts at $0.036/hour
Create
Windows 11 Preview
Microsoft
Virtual Machine
Windows 11 Preview
Windows 2016 Datacenter Minimal
Art Group
Virtual Machine
Windows 2016 Datacenter Minimal is perfect for high IT requirements
Windows Server 2019 Core
Cloud Infrastructure Services
Virtual Machine
Windows Server 2019 Core is a minimal installation option. Less disk space, more secure and faster.
Windows Server 2022 Core
Cloud Infrastructure Services
Virtual Machine
Windows Server 2022 offers latest security features, minimal OS, less disk space, faster, secure.
Microsoft Windows 11 Preview arm64
Microsoft
Virtual Machine
Microsoft Windows 11 Preview arm64
Is Marketplace helpful?

c) In the **Create a virtual machine** window, enter the relevant details

Figure 72: Create a Virtual Machine



Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : VM-Deployment

Resource group * : (New) Resource group
Create new

Instance details

Virtual machine name * :

Region * : (US) East US 2

Availability options : Availability zone

Availability zone * : Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

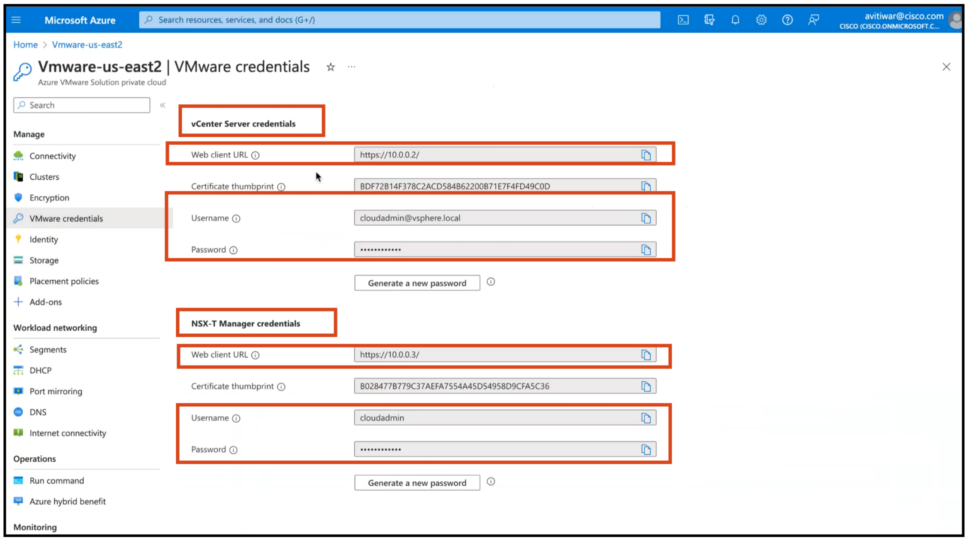
Security type : Trusted launch virtual machines
Configure security features

A jumpbox of your preferred operating system is deployed. Use this to access your services.

Step 4 You can login to the vSphere service. Use the credentials retreived when creating the private cloud, from the **VMware Credentials** > **vCenter Server credentials** section.

- Launch the Jumpbox, and use a browser to access the service.
- Since Bastion is deployed on the virtual network, you can use SSH or remote desktop protocol (RDP) to access the service.

Figure 73: VMware Credentials



Vmware-us-east2 | VMware credentials

vCenter Server credentials

Web client URL: https://10.0.0.2/

Certificate thumbprint: BDF72B14F378C2ACD584B62200B71E7F4FD49C0D

Username: cloudadmin@vsphere.local

Password: ••••••••••••

NSX-T Manager credentials

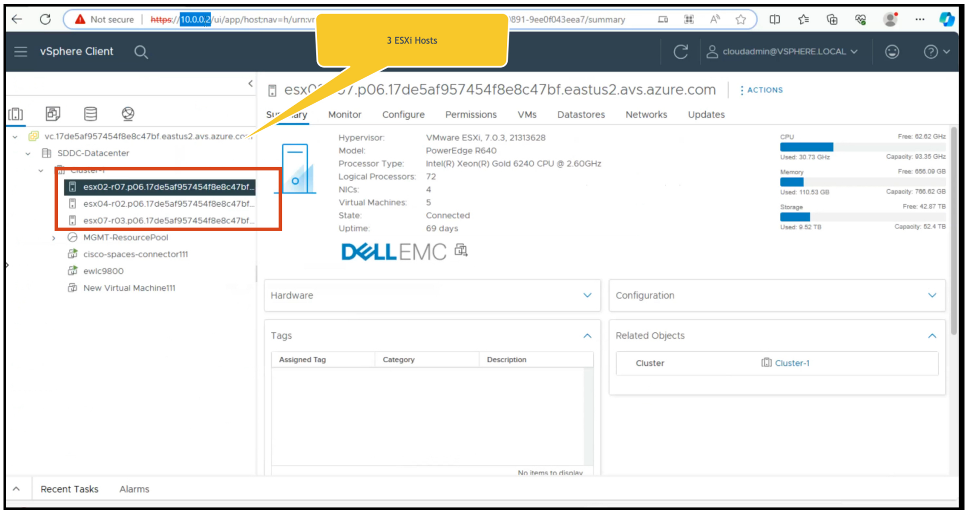
Web client URL: https://10.0.0.3/

Certificate thumbprint: B028477B779C37AEFA7554A45D54958D9CFA5C36

Username: cloudadmin

Password: ••••••••••••

Figure 74: VMware Credentials



esx02-r07.p06.17de5af957454f8e8c47bf.eastus2.avs.azure.com

Hypervisor: VMware ESXi, 7.0.3, 21313628

Model: PowerEdge R640

Processor Type: Intel(R) Xeon(R) Gold 6240 CPU @ 2.60GHz

Logical Processors: 72

NICs: 4

Virtual Machines: 5

State: Connected

Uptime: 69 days

Note

ESXi inherits the vSphere credentials.

You can notice that there are at least three ESXi hosts available by default.

Step 5 Deploy the OVA on one of the hosted ESXi. See Deploying the Connector 3 OVA (Single Interface), on page 65

CHAPTER 7

Cisco Spaces: Connector OVA

Deploying the Connector 3 OVA (Single Interface)

This chapter provides information about how to download and deploy the Cisco Spaces: Connector 3 and obtain the URL for the connector GUI.

Before you begin

Ensure you have the minimum configuration required for installing connector OVA:

- 2 vCPU
- 4-GB RAM
- 120-GB hard disk

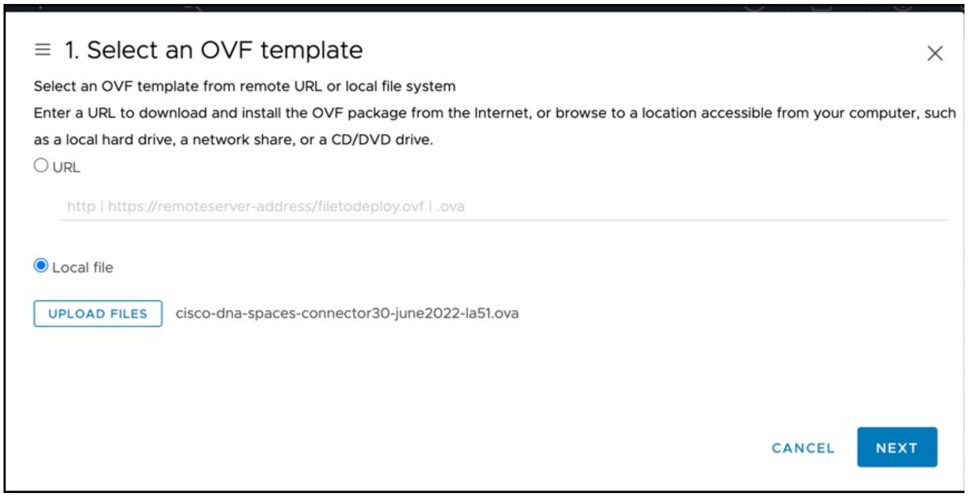
Procedure

Step 1 Download connector OVA to your local system.

Step 2 Create a virtual machine (VM) in the ESXi server and deploy the downloaded Cisco Spaces: Connector OVA.

Step 3 In the **1. Select an OVF template** window, click **UPLOAD FILES**, and select the corresponding connector OVA files or drag and drop the downloaded file, and click **Next**.

Figure 75: 1. Select an OVF template



1. Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

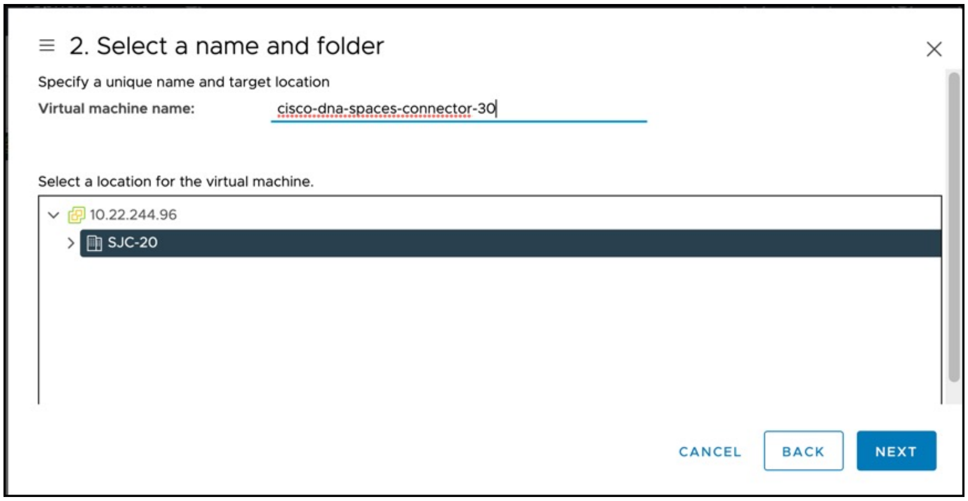
http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

UPLOAD FILES cisco-dna-spaces-connector30-june2022-la51.ova

Step 4 In the **2. Select a name and folder** window, enter a name for the VM, and choose a location for the VM, and click **Next**.

Figure 76: 2. Select a Name and Folder



2. Select a name and folder

Specify a unique name and target location

Virtual machine name: cisco-dna-spaces-connector-30

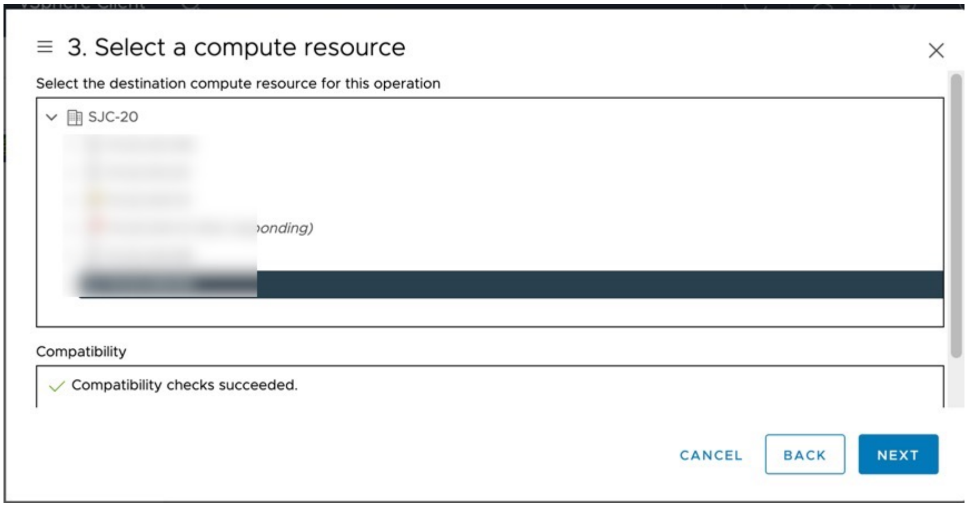
Select a location for the virtual machine.

10.22.244.96

SJC-20

Step 5 In the **3. Select a compute resource** window, select a destination compute resource, and click **Next**.

Figure 77: 3. Select a Compute Resource



3. Select a compute resource

Select the destination compute resource for this operation

SJC-20

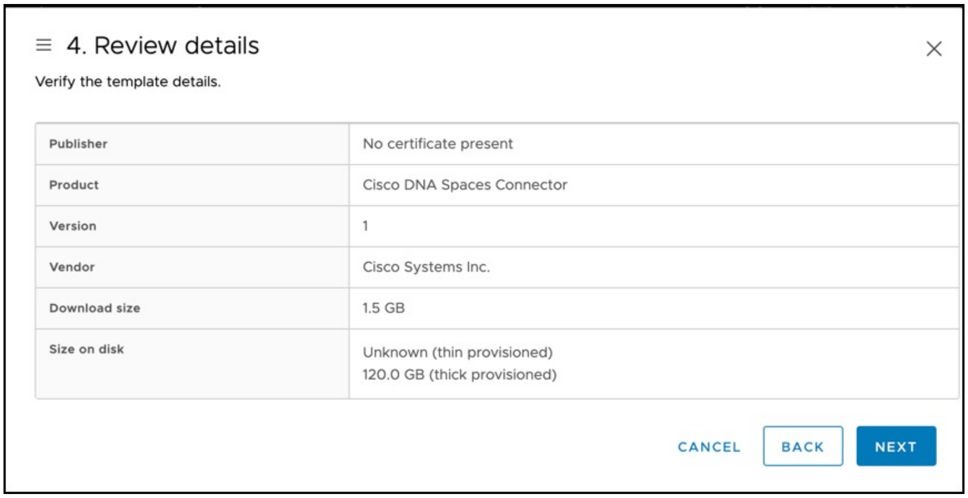
[redacted]onding)

Compatibility

Compatibility checks succeeded.

Step 6 In the **4. Review details** window, read and verify the template details, and click **Next**.

Figure 78: 4. Review Details



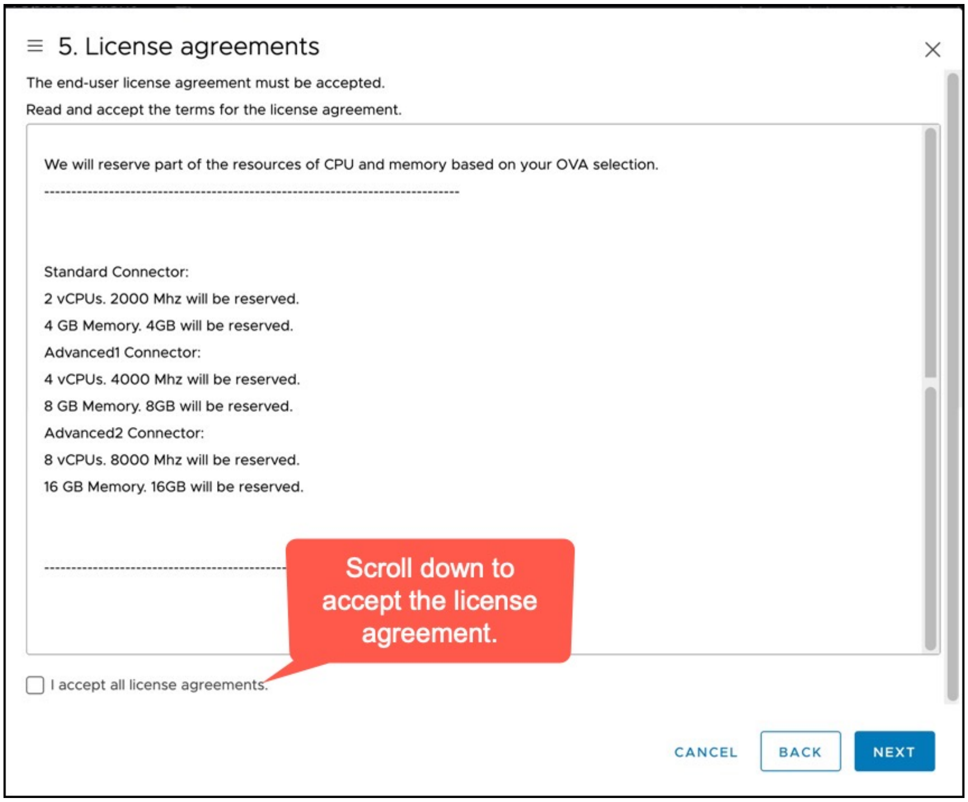
4. Review details

Verify the template details.

Publisher	No certificate present
Product	Cisco DNA Spaces Connector
Version	1
Vendor	Cisco Systems Inc.
Download size	1.5 GB
Size on disk	Unknown (thin provisioned) 120.0 GB (thick provisioned)

Step 7 In the **5. License agreements** window, read the license agreement that is displayed and scroll to the end. Check **I accept all license agreements** and then click **Next**.

Figure 79: 5. License Agreements



≡ 5. License agreements

The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

We will reserve part of the resources of CPU and memory based on your OVA selection.

Standard Connector:
2 vCPUs. 2000 Mhz will be reserved.
4 GB Memory. 4GB will be reserved.
Advanced1 Connector:
4 vCPUs. 4000 Mhz will be reserved.
8 GB Memory. 8GB will be reserved.
Advanced2 Connector:
8 vCPUs. 8000 Mhz will be reserved.
16 GB Memory. 16GB will be reserved.

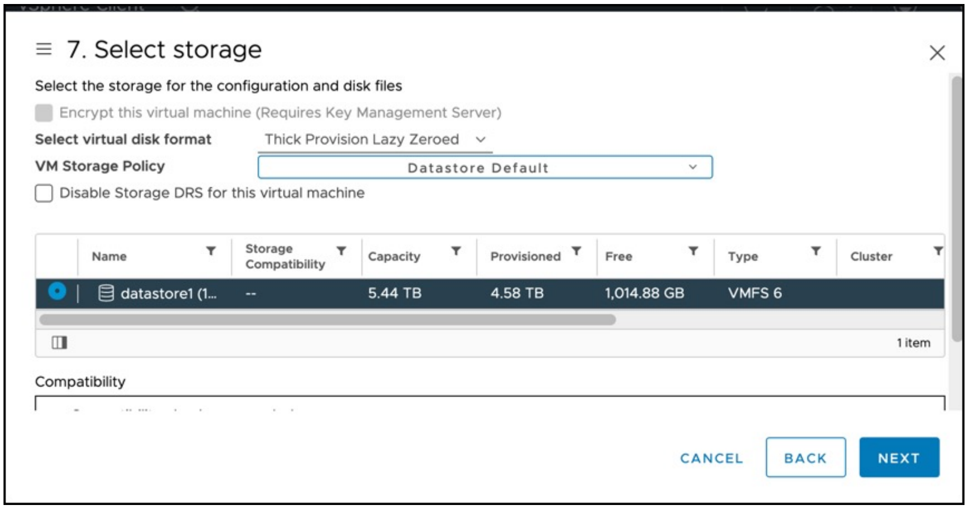
□ I accept all license agreements.

Step 8 In the **6. Configuration** window, choose one of the following, and click **Next**.

- **Standard**
- **Advanced1**
- **Advanced2**

Step 9 In the **7. Select storage** window, choose the standard storage configuration, and click **Next**.

Figure 80: 7. Select storage



≡ 7. Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

□ Disable Storage DRS for this virtual machine

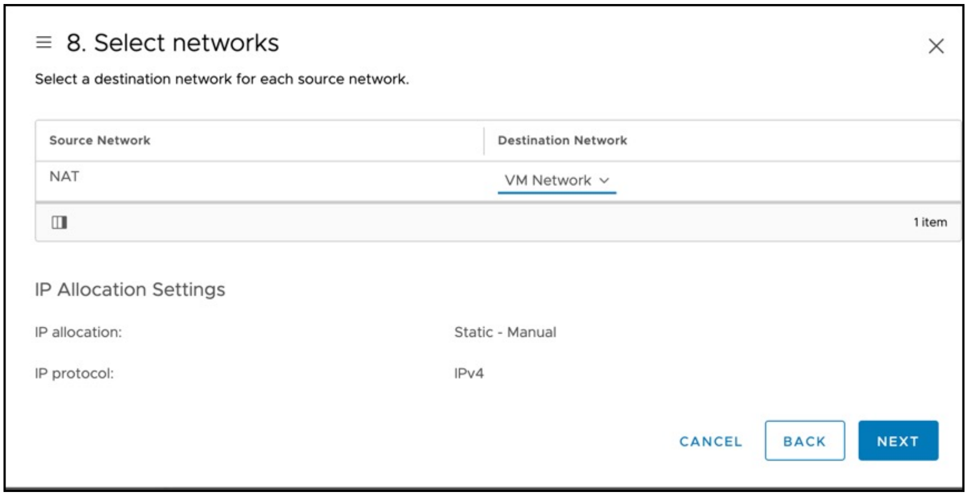
	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Cluster
●	datastore1 (1...	--	5.44 TB	4.58 TB	1,014.88 GB	VMFS 6	

1 item

Compatibility

Step 10 In the **8. Select networks** window, choose a destination network, and click **Next**.

Figure 81: 8. Select Networks



≡ 8. Select networks

Select a destination network for each source network.

Source Network	Destination Network
NAT	VM Network

1 item

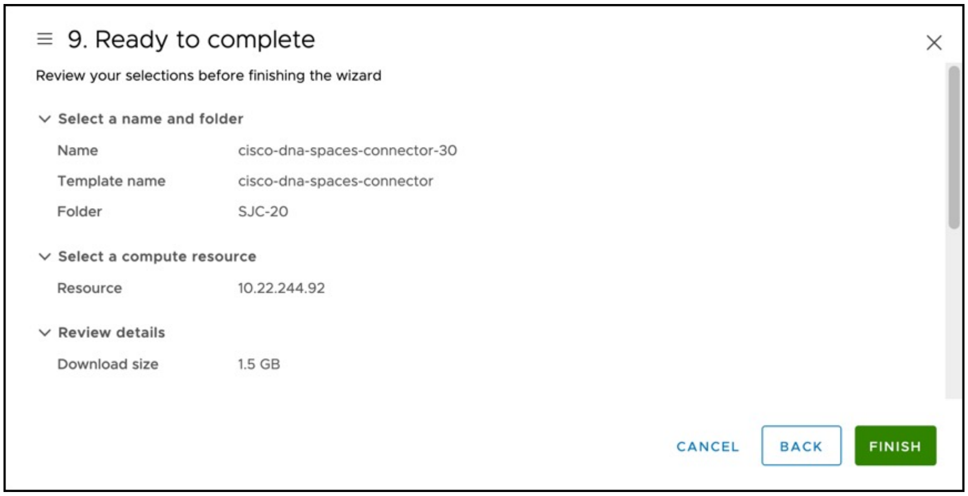
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

Step 11 In the **9. Ready to complete** window, review the configurations and click **Finish**.

Figure 82: 9. Ready to Complete



9. Ready to complete

Review your selections before finishing the wizard

Select a name and folder

Name	cisco-dna-spaces-connector-30
Template name	cisco-dna-spaces-connector
Folder	SJC-20

Select a compute resource

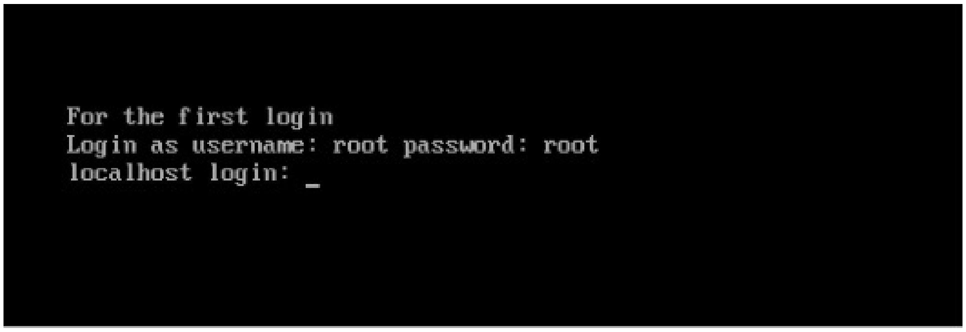
Resource	10.22.244.92

Review details

Download size	1.5 GB

Step 12 Power on your VM and log in to the terminal and enter the default username **root** and default password **root**.

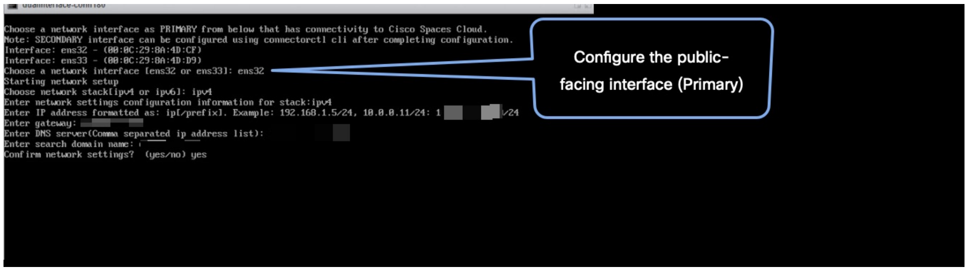
Figure 83: First Login Credentials root/root



```
For the first login
Login as username: root password: root
localhost login: _
```

Step 13 Choose an network interface to configure as PRIMARY.

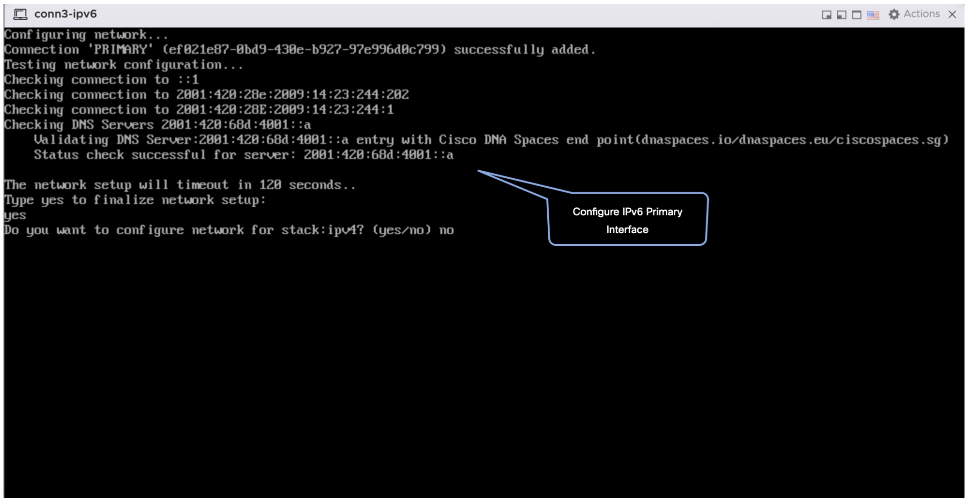
Figure 84: Configuring the Primary Interface: IPv4



```
Choose a network interface as PRIMARY from below that has connectivity to Cisco Spaces Cloud.
Note: SECONDARY interface can be configured using connectorctl cli after completing configuration.
Interface: ens32 - (00:0C:29:8A:4D:CF)
Interface: ens33 - (00:0C:29:8A:4D:D9)
Choose a network interface [ens32 or ens33]: ens32
Starting network setup
Choose network stack[ipv4 or ipv6]: ipv4
Enter network settings configuration information for stack:ipv4
Enter IP address formatted as: ip[/prefix]. Example: 192.168.1.5/24, 10.0.0.11/24: 1[redacted]/24
Enter gateway: [redacted]
Enter DNS server(Comma separated ip address list): [redacted]
Enter search domain name: [redacted]
Confirm network settings?  (yes/no) yes
```

Configure the public-facing interface (Primary)

Figure 85: Configuring the Primary Interface: IPv6



```
Configuring network...
Connection 'PRIMARY' (ef021e87-0bd9-430e-b927-97e996d0c799) successfully added.
Testing network configuration...
Checking connection to ::1
Checking connection to 2001:420:28e:2009:14:23:244:202
Checking connection to 2001:420:28E:2009:14:23:244:1
Checking DNS Servers 2001:420:68d:4001::a
    Validating DNS Server:2001:420:68d:4001::a entry with Cisco DNA Spaces end point(dnaspaces.io/dnaspaces.eu/ciscospaces.sg)
    Status check successful for server: 2001:420:68d:4001::a

The network setup will timeout in 120 seconds..
Type yes to finalize network setup:
yes
Do you want to configure network for stack:ipv4? (yes/no) no
```

Step 14 Do one of the following, and then configure the network settings for the PRIMARY interface. Specify parameters such as IP address, hostname, and so on.

- Configure the IPv6 stack.
- Configure the IPv4 stack.

You can add multiple DNS servers as a comma separated list in this step. After the task is complete and the Cisco Spaces: Connector is deployed, you can login to the connector CLI, and run the **connectorctl network config** command to add more DNS servers or edit the existing list.

Step 15 Confirm the setup.

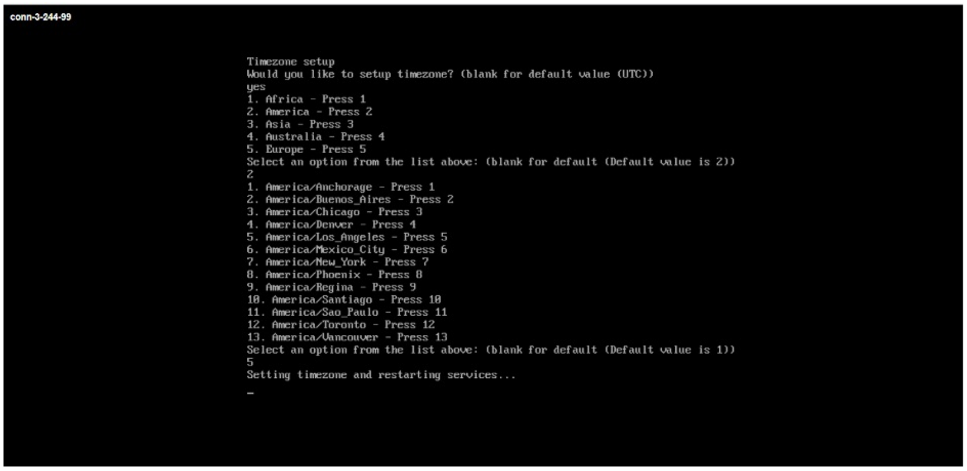
Note
Because this configuration window times out in 120 seconds, ensure that you provide the input on time to avoid reconfiguration.

Step 16 Reset the password for the **spacesadmin** user.

Note
The **spacesadmin** password can only include special characters such as '@' or '!' and must not contain any spaces.

Step 17 Enter the time zone.

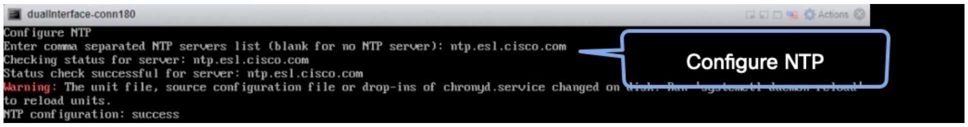
Figure 86: Time Zone



```
Timezone setup
Would you like to setup timezone? (blank for default value (UTC))
yes
1. Africa - Press 1
2. America - Press 2
3. Asia - Press 3
4. Australia - Press 4
5. Europe - Press 5
Select an option from the list above: (blank for default (Default value is 2))
2
1. America/Anchorage - Press 1
2. America/Buenos_Aires - Press 2
3. America/Chicago - Press 3
4. America/Denver - Press 4
5. America/Los_Angeles - Press 5
6. America/Mexico_City - Press 6
7. America/New_York - Press 7
8. America/Phoenix - Press 8
9. America/Regina - Press 9
10. America/Santiago - Press 10
11. America/Sao_Paulo - Press 11
12. America/Toronto - Press 12
13. America/Vancouver - Press 13
Select an option from the list above: (blank for default (Default value is 1))
5
Setting timezone and restarting services...
_
```

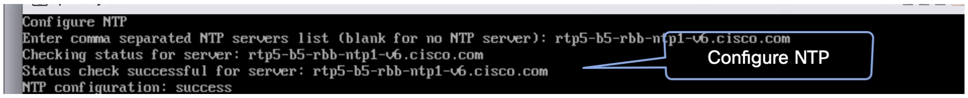
Step 18 Enter the Network Time Protocol (NTP) server name to synchronize the system time with that of NTP server, or leave it blank if you do not want to configure an NTP server.

Figure 87: Configure NTP



```
Configure NTP
Enter comma separated NTP servers list (blank for no NTP server): ntp.esl.cisco.com
Checking status for server: ntp.esl.cisco.com
Status check successful for server: ntp.esl.cisco.com
Warning: The unit file, source configuration file or drop-ins of chronyd.service changed on disk. Run 'systemctl daemon-reload'
to reload units.
NTP configuration: success
```

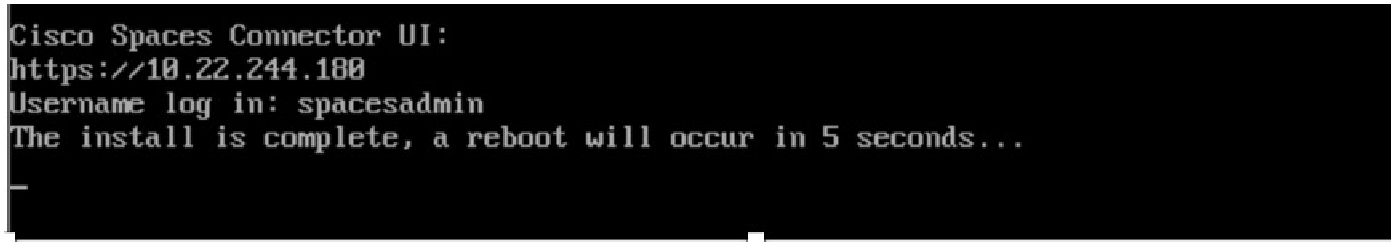
Figure 88: Configure NTP



```
Configure NTP
Enter comma separated NTP servers list (blank for no NTP server): rtp5-b5-rbb-ntp1-v6.cisco.com
Checking status for server: rtp5-b5-rbb-ntp1-v6.cisco.com
Status check successful for server: rtp5-b5-rbb-ntp1-v6.cisco.com
NTP configuration: success
```

Step 19 Note the URL (https://connector-ip) before the automatic reboot. You can use this URL later to open the connector GUI.

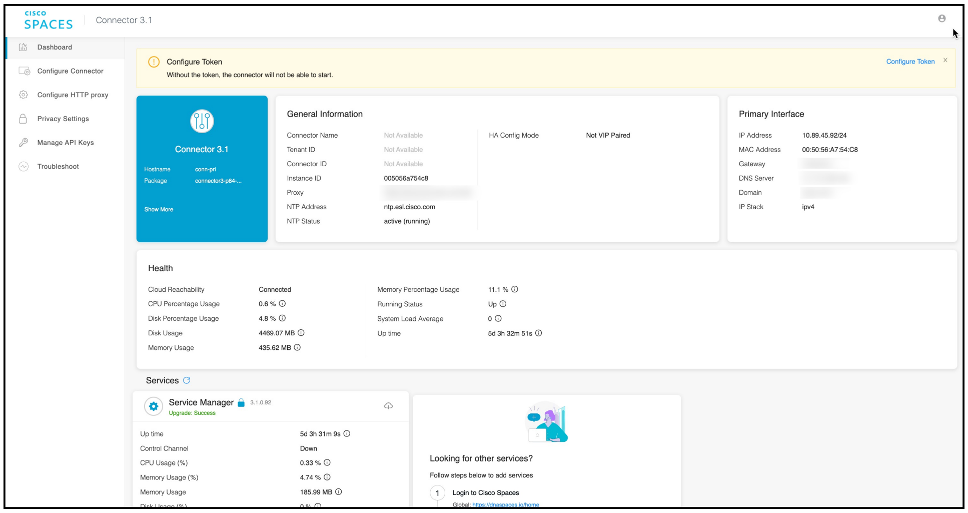
Figure 89: ConnectorGUI



```
Cisco Spaces Connector UI:
https://10.22.244.180
Username log in: spacesadmin
The install is complete, a reboot will occur in 5 seconds...
_
```

Step 20 In a browser window, enter the noted URL and press Enter to open the connector GUI. Log in as a **spacesadmin** user.

Figure 90: Connector GUI



Configure Token
Without the token, the connector will not be able to start.

Connector 3.1

Hostname	conn-pri
Package	connector3-p84-...

General Information

Connector Name	Not Available	HA Config Mode	Not VIP Paired
Tenant ID	Not Available		
Connector ID	Not Available		
Instance ID	005056a754c8		
Proxy	[redacted]		
NTP Address	ntp.esl.cisco.com		
NTP Status	active (running)		

Primary Interface

IP Address	10.89.45.92/24
MAC Address	00:50:56:A7:54:C8
Gateway	[redacted]
DNS Server	[redacted]
Domain	[redacted]
IP Stack	ipv4

Health

Cloud Reachability	Connected	Memory Percentage Usage	11.1 %
CPU Percentage Usage	0.6 %	Running Status	Up
Disk Percentage Usage	4.8 %	System Load Average	0
Disk Usage	4469.07 MB	Up time	5d 3h 32m 51s
Memory Usage	435.62 MB		

Service Manager 3.1.0.92
Upgrade: Success

Up time	5d 3h 31m 9s
Control Channel	Down
CPU Usage (%)	0.33 %
Memory Usage (%)	4.74 %
Memory Usage	185.99 MB
Disk Usage (%)	0 %

Looking for other services?

Follow steps below to add services

1 Login to Cisco Spaces
Global: https://dnaspaces.io/home

Note
The root user is disabled and is used only for advanced troubleshooting by the Cisco Support team.

What to do next

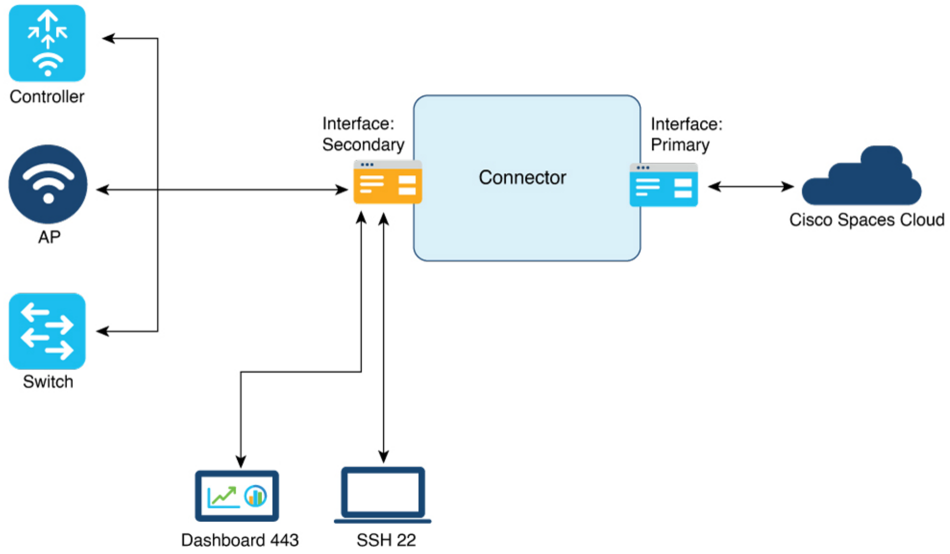
You can now Configure this Connector on Cisco Spaces.

Deploying the Cisco Spaces: Connector OVA (Dual Interface)

If you need to connect the connector to two separate customer networks in network deployments, you can use a dual-interface deployment. We recommend this deployment in scenarios where you manage devices on private or internal networks. To set up this deployment, you must use two interfaces:

- PRIMARY interface: Used to transmit traffic to Cisco Spaces.
- SECONDARY interface: Used by connector to interact with devices such as wireless controller, access points, or switches, over a private or internal network. You can also allow SSH and GUI (443) access to connector on this interface with additional configurations (disabled by default). Ensure that the connector is part of subnet routes to access it.

Figure 91: Dual Interface Deployment



Note We recommend that you connect the wireless controller to a private network as it enables the connector to establish SSH connections with the wireless controller.

Before you begin

Ensure that the Cisco Unified Computing System (Cisco UCS) device where you install the Open Virtualization Appliance (OVA) is connected to two separate networks. In this network configuration, the Cisco UCS device is configured with two physical network interface cards (NICs). Each NIC is connected to a switch. In this way, the Cisco UCS device is connected to two networks.

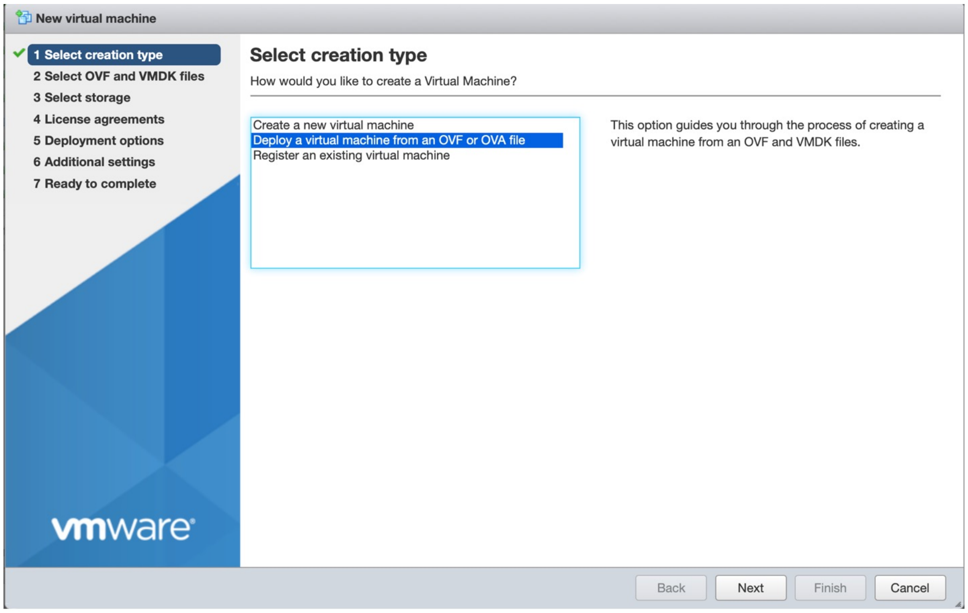
Procedure

Step 1 Download connector 3 from Cisco.com.

Step 2 Create a virtual machine in the ESXi server and deploy the downloaded Cisco Spaces: Connector OVA.

Step 3 In the **Select creation type** window, choose **Deploy a virtual machine from an OVF or OVA file**, and click **Next**.

Figure 92: Select Creation Type



Select creation type

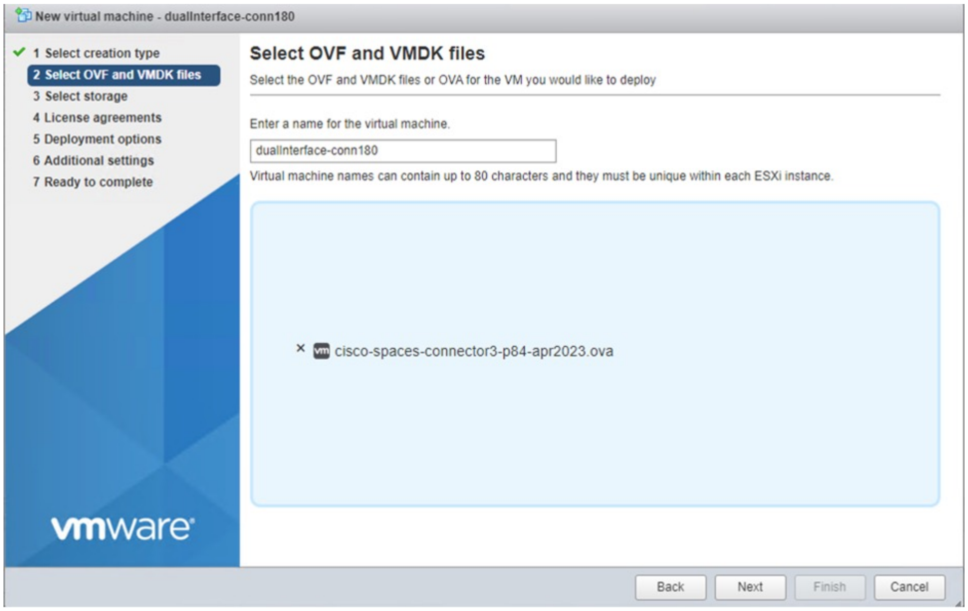
How would you like to create a Virtual Machine?

Create a new virtual machine
Deploy a virtual machine from an OVF or OVA file
Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

Step 4 In the **Select OVF and VMDK files** window, enter a name for the virtual machine. Click the blue area to either select files from the computer or drag and drop files. Click **Next**.

Figure 93: Select OVF and VMDK files



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

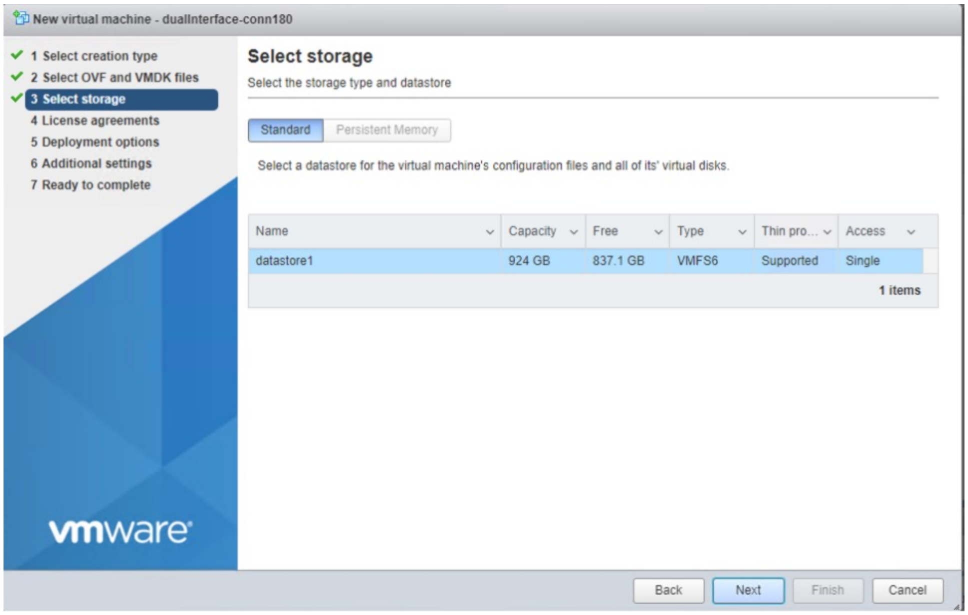
dualInterface-conn180

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× cisco-spaces-connector3-p84-apr2023.ova

Step 5 In the **Select storage** window, the **Standard** storage configuration is displayed. Click **Next**.

Figure 94: Select Storage



Select storage

Select the storage type and datastore

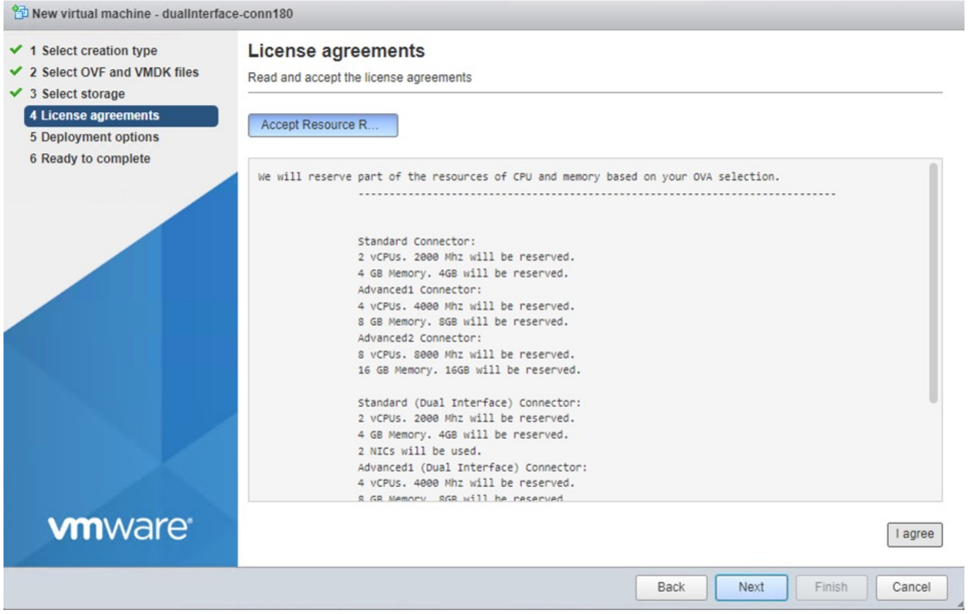
Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	924 GB	837.1 GB	VMFS6	Supported	Single

1 items

Step 6 In the **License agreements** window, read the license agreement that is displayed and scroll to the end. Click **I Agree** and then click **Next**.

Figure 95: License agreements



License agreements

Read and accept the license agreements

```
We will reserve part of the resources of CPU and memory based on your OVA selection.
                -----------------------------------------------------------------------------


                Standard Connector:
                2 vCPUs. 2000 Mhz will be reserved.
                4 GB Memory. 4GB will be reserved.
                Advanced1 Connector:
                4 vCPUs. 4000 Mhz will be reserved.
                8 GB Memory. 8GB will be reserved.
                Advanced2 Connector:
                8 vCPUs. 8000 Mhz will be reserved.
                16 GB Memory. 16GB will be reserved.

                Standard (Dual Interface) Connector:
                2 vCPUs. 2000 Mhz will be reserved.
                4 GB Memory. 4GB will be reserved.
                2 NICs will be used.
                Advanced1 (Dual Interface) Connector:
                4 vCPUs. 4000 Mhz will be reserved.
                8 GB Memory. 8GB will be reserved.
```

Step 7 In the **Deployment options** window, do the following:

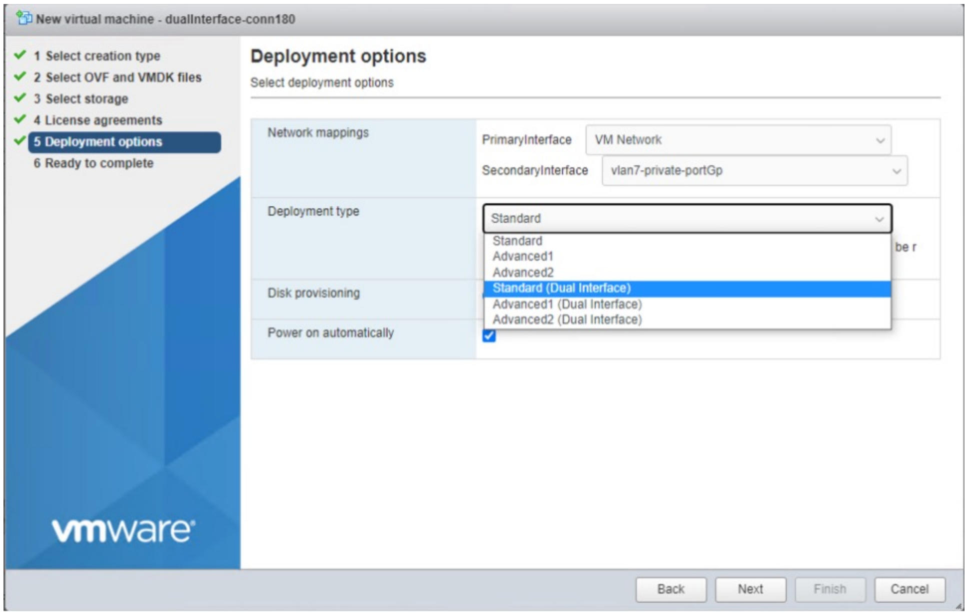
a) In the **PrimaryInterface** field, enter the name of the external-facing interface.

b) In the **SecondaryInterface** field, enter the name of the private-facing interface.

c) From the **Deployment type** drop-down list, choose one of the following deployment types.

- **Standard (Dual Interface)**
- **Advanced1 (Dual Interface)**
- **Advanced2 (Dual Interface)**

Figure 96: Deployment options



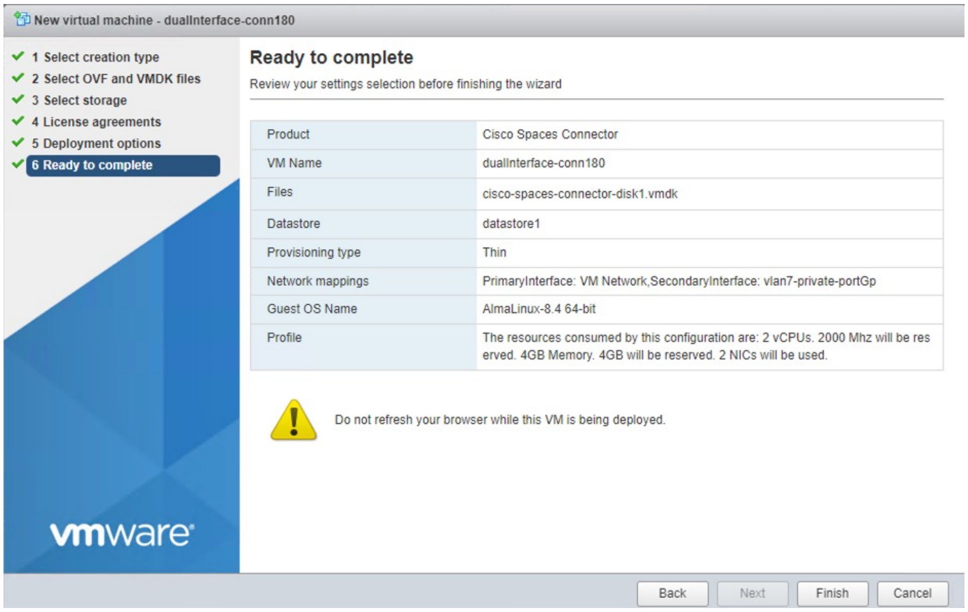
Deployment options

Select deployment options

Network mappings	PrimaryInterface: VM Network SecondaryInterface: vlan7-private-portGp
Deployment type	Standard Standard Advanced1 Advanced2 Standard (Dual Interface) Advanced1 (Dual Interface) Advanced2 (Dual Interface)
Disk provisioning	
Power on automatically	☑

Step 8 Review the configurations and click **Finish**.

Figure 97: Ready to complete



Ready to complete

Review your settings selection before finishing the wizard

Product	Cisco Spaces Connector
VM Name	dualInterface-conn180
Files	cisco-spaces-connector-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	PrimaryInterface: VM Network,SecondaryInterface: vlan7-private-portGp
Guest OS Name	AlmaLinux-8.4 64-bit
Profile	The resources consumed by this configuration are: 2 vCPUs. 2000 Mhz will be reserved. 4GB Memory. 4GB will be reserved. 2 NICs will be used.

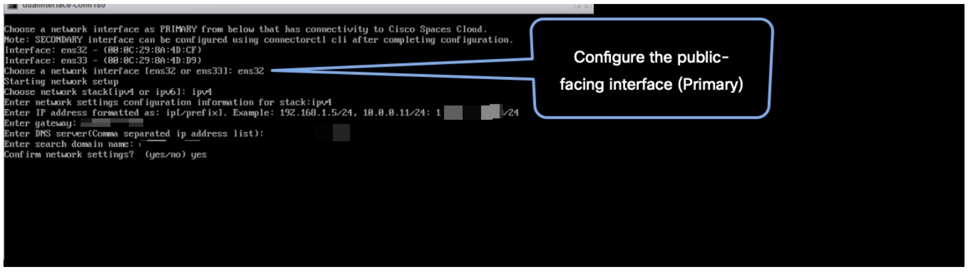
Do not refresh your browser while this VM is being deployed.

Step 9 Log in to the terminal and enter the default username **root** and default password **root**.

Step 10 Configure the host name for the connector.

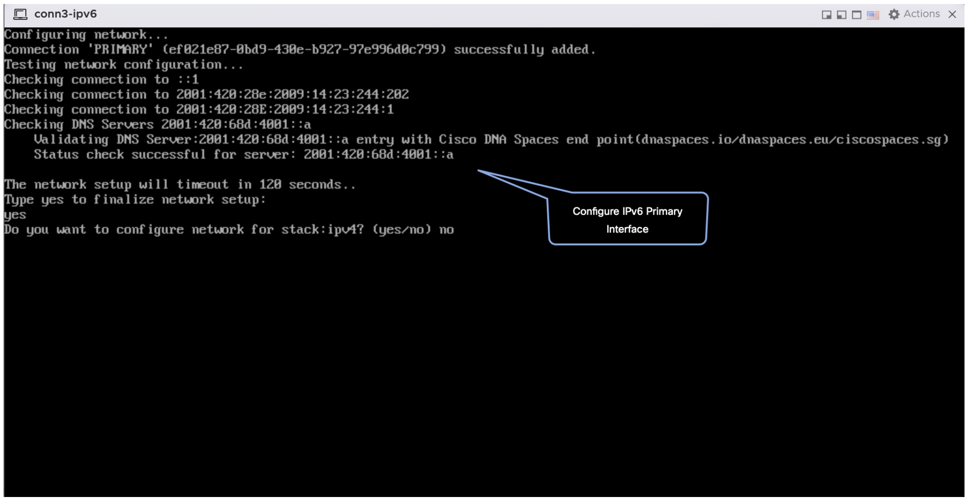
Step 11 Choose an network interface to configure as PRIMARY.

Figure 98: Configuring the Primary Interface: IPv4



```
Choose a network interface as PRIMARY from below that has connectivity to Cisco Spaces Cloud.
Note: SECONDARY interface can be configured using connectorctl cli after completing configuration.
Interface: ens32 - (00:0C:29:8A:4D:CF)
Interface: ens33 - (00:0C:29:8A:4D:D9)
Choose a network interface [ens32 or ens33]: ens32
Starting network setup
Choose network stack[ipv4 or ipv6]: ipv4
Enter network settings configuration information for stack:ipv4
Enter IP address formatted as: ip[/prefix]. Example: 192.168.1.5/24, 10.0.0.11/24: 1[redacted]/24
Enter gateway: [redacted]
Enter DNS server(Comma separated ip address list): [redacted]
Enter search domain name: [redacted]
Confirm network settings?  (yes/no) yes
```

Figure 99: Configuring the Primary Interface: IPv6



```
Configuring network...
Connection 'PRIMARY' (ef021e87-0bd9-430e-b927-97e996d0c799) successfully added.
Testing network configuration...
Checking connection to ::1
Checking connection to 2001:420:28e:2009:14:23:244:202
Checking connection to 2001:420:28E:2009:14:23:244:1
Checking DNS Servers 2001:420:68d:4001::a
    Validating DNS Server:2001:420:68d:4001::a entry with Cisco DNA Spaces end point(dnaspaces.io/dnaspaces.eu/ciscospaces.sg)
    Status check successful for server: 2001:420:68d:4001::a

The network setup will timeout in 120 seconds..
Type yes to finalize network setup:
yes
Do you want to configure network for stack:ipv4? (yes/no) no
```

Step 12 Do one of the following, and then configure the network settings for the PRIMARY interface. Specify parameters such as IP address, hostname, and so on.

- Configure the IPv6 stack.
- Configure the IPv4 stack.

You can add multiple DNS servers as a comma separated list in this step. After the task is complete and the Cisco Spaces: Connector is deployed, you can login to the connector CLI, and run the **connectorctl network config** command to add more DNS servers or edit the existing list.

Step 13 Reset the password for the **spacesadmin** user.

Note

The **spacesadmin** password can only include special characters such as '@' or '!' and must not contain any spaces.

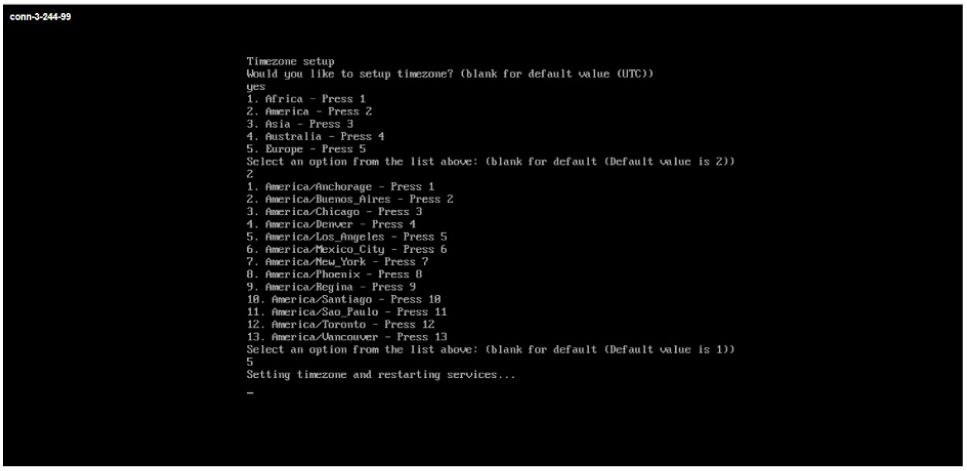
Step 14 Confirm the setup.

Note

Because this configuration window times out in 120 seconds, ensure that you provide the input on time to avoid reconfiguration.

Step 15 Enter the time zone.

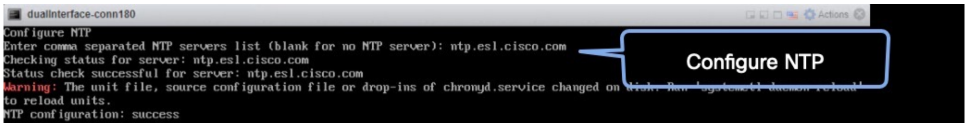
Figure 100: Time Zone



```
Timezone setup
Would you like to setup timezone? (blank for default value (UTC))
yes
1. Africa - Press 1
2. America - Press 2
3. Asia - Press 3
4. Australia - Press 4
5. Europe - Press 5
Select an option from the list above: (blank for default (Default value is 2))
2
1. America/Anchorage - Press 1
2. America/Buenos_Aires - Press 2
3. America/Chicago - Press 3
4. America/Denver - Press 4
5. America/Los_Angeles - Press 5
6. America/Mexico_City - Press 6
7. America/New_York - Press 7
8. America/Phoenix - Press 8
9. America/Regina - Press 9
10. America/Santiago - Press 10
11. America/Sao_Paulo - Press 11
12. America/Toronto - Press 12
13. America/Vancouver - Press 13
Select an option from the list above: (blank for default (Default value is 1))
5
Setting timezone and restarting services...
_
```

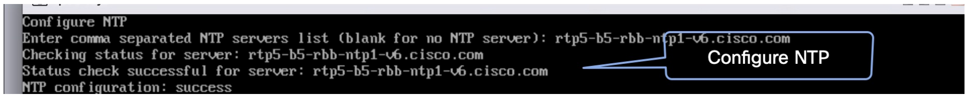
Step 16 Enter the Network Time Protocol (NTP) server name to synchronize the system time with that of NTP server, or leave it blank if you do not want to configure an NTP server.

Figure 101: Configure NTP



```
Configure NTP
Enter comma separated NTP servers list (blank for no NTP server): ntp.esl.cisco.com
Checking status for server: ntp.esl.cisco.com
Status check successful for server: ntp.esl.cisco.com
Warning: The unit file, source configuration file or drop-ins of chronyd.service changed on disk. Run 'systemctl daemon-reload'
to reload units.
NTP configuration: success
```

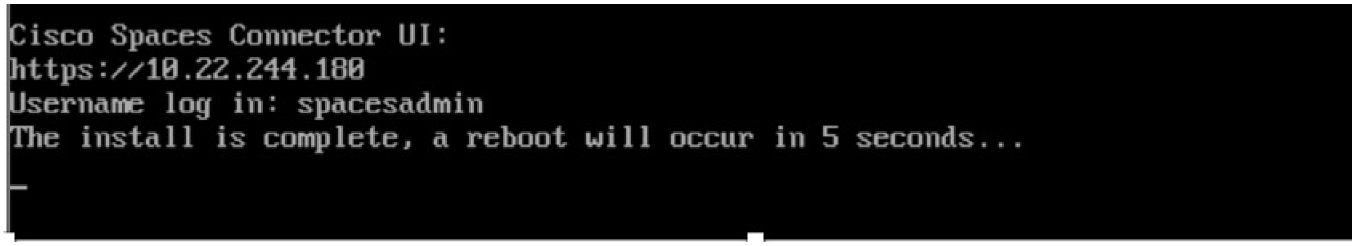
Figure 102: Configure NTP



```
Configure NTP
Enter comma separated NTP servers list (blank for no NTP server): rtp5-b5-rbb-ntp1-v6.cisco.com
Checking status for server: rtp5-b5-rbb-ntp1-v6.cisco.com
Status check successful for server: rtp5-b5-rbb-ntp1-v6.cisco.com
NTP configuration: success
```

Step 17 Note the URL (https://connector-ip) before the automatic reboot. You can use this URL later to open the connector GUI.

Figure 103: ConnectorGUI



```
Cisco Spaces Connector UI:
https://10.22.244.180
Username log in: spacesadmin
The install is complete, a reboot will occur in 5 seconds...
_
```

Step 18 Wait for the completion of the reboot, and login as a **spacesadmin** user.

Step 19 Configure the secondary interface using the **connectorctl network config** command

```
[spacesadmin@connector ~]$ connectorctl network config  -p ipv4 -i 10.7.0.11/24 -g 10.7.0.1 -o
cisco.com -d 172.70.168.183 -n SECONDARY
Executing command:network
Command execution status:Success
-----------------------
```

```
Connection SECONDARY (5e970417-13b4-4ad8-af12-d125ce407c49) successfully added.
Network setup completed with given configuration.
Secondary interface - Added routes.
Secondary interface - Configured firewall zone.
System reboot will happen in 10 seconds. Do not execute any other command...
```

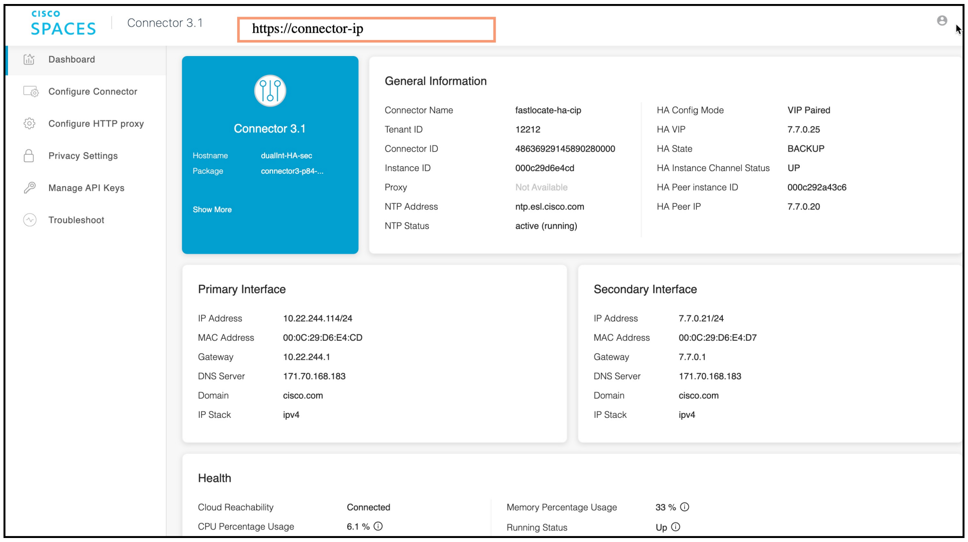
Step 20 Verify the network Settings of external-facing network using the **connectorctl network show** command.

```
[spacesadmin@connector ~]$ connectorctl network show
 Executing command:network
Command execution status:Success
-----------------------
=================Network Config=================
Hostname    - connector-p84-april1


Interface   - PRIMARY
---------------------------------

Network configuration for stack:ipv4
Ip Address  - 10.22.244.180/24
Mac Address - 00:0C:29:EE:24:8A
Gateway     - 10.22.244.1
Dns         - 172.70.168.183
Domain      - cisco.com


Interface   - SECONDARY
---------------------------------

Network configuration for stack:ipv4
Ip Address  - 7.7.0.11/24
Mac Address - 00:0C:29:EE:24:94
Gateway     - 7.7.0.1
Dns         - 172.70.168.183
Domain      - cisco.com

=================end=================
```

You can use the **connectorctl network show -n PRIMARY** and **connectorctl network show -n SECONDARY** to see information specific to these interfaces.

Step 21 In a browser window, navigate to the noted URL to open the connector GUI. Log in as a **spacesadmin** user.

Figure 104: ConnectorGUI



Hostname	dualInt-HA-sec
Package	connector3-p84-...

General Information

Connector Name	fastlocate-ha-cip	HA Config Mode	VIP Paired
Tenant ID	12212	HA VIP	7.7.0.25
Connector ID	48636929145890280000	HA State	BACKUP
Instance ID	000c29d6e4cd	HA Instance Channel Status	UP
Proxy	Not Available	HA Peer instance ID	000c292a43c6
NTP Address	ntp.esl.cisco.com	HA Peer IP	7.7.0.20
NTP Status	active (running)		

Primary Interface

IP Address	10.22.244.114/24
MAC Address	00:0C:29:D6:E4:CD
Gateway	10.22.244.1
DNS Server	171.70.168.183
Domain	cisco.com
IP Stack	ipv4

Secondary Interface

IP Address	7.7.0.21/24
MAC Address	00:0C:29:D6:E4:D7
Gateway	7.7.0.1
DNS Server	171.70.168.183
Domain	cisco.com
IP Stack	ipv4

Health

Cloud Reachability	Connected	Memory Percentage Usage	33 % ⓘ
CPU Percentage Usage	6.1 % ⓘ	Running Status	Up ⓘ

Note

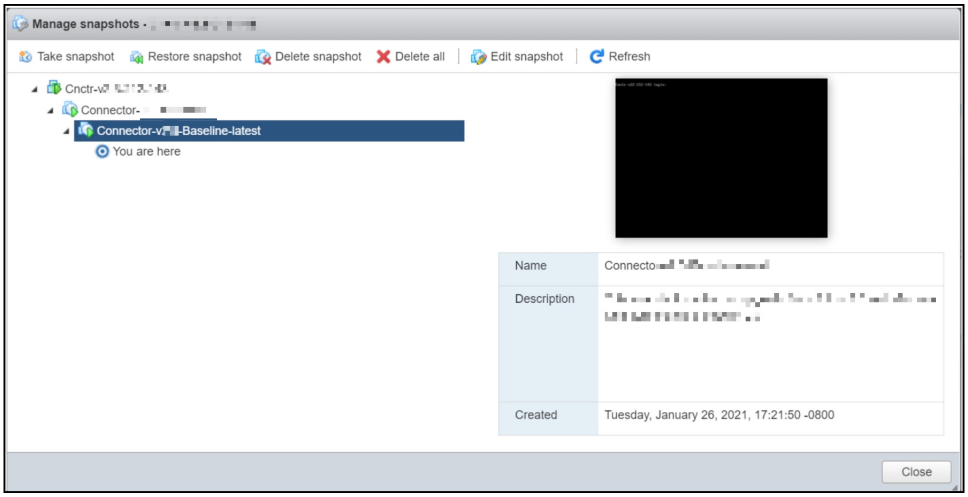
The root user is disabled and is used only for advanced troubleshooting by the Cisco Support team.

Using Snapshots for Backup

You can use the snapshot of a deployed connector OVA for backing up your connector. Ensure that the following prerequisites in place:

- connector is deployed.
- All the services are started.
- connector is added to Cisco Spaces.

Figure 105: Backing Up Using a Snapshot



Cnctr-v[redacted]

Connector-[redacted]

Connector-v[redacted]-Baseline-latest

You are here

Name	Connecto[redacted]
Description	[redacted]
Created	Tuesday, January 26, 2021, 17:21:50 -0800

Note Proxies are not carried over during a snapshot restore. You have to reconfigure proxies.

CHAPTER 8

Cisco Spaces: Connector VM on Nutanix Environment

Cisco Spaces: Connector Nutanix cloud platform support

The Cisco Spaces: Connector 3.2 June, 2025 release supports the Nutanix cloud platform. To deploy the Nutanix Connector virtual machine (VM), you need the necessary Nutanix setup, which includes Nutanix-supported hardware and PRISM software.

Set Up Connector VM on Nutanix Environment

Follow the steps to setup a connector VM.

Before you begin

Ensure that Nutanix Prism is setup before you configure the connector virtual machine (VM).

Procedure

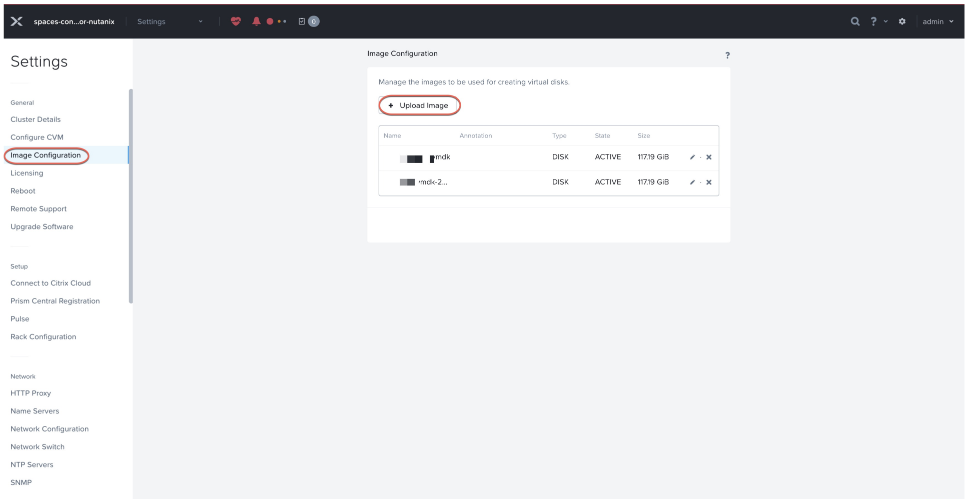
Step 1 Download the June 2025 OVA file available on the Software Download page.

Step 2 Unzip the downloaded OVA to extract the Virtual Machine Disk (VMDK) file.

Step 3 Log in into **Nutanix Prism** > **Settings** > **Image Configuration** tab.

The **Image Configuration** dialog box is displayed.

Figure 106: Image Configuration



Settings

General
Cluster Details
Configure CVM
Image Configuration
Licensing
Reboot
Remote Support
Upgrade Software

Setup
Connect to Citrix Cloud
Prism Central Registration
Pulse
Rack Configuration

Network
HTTP Proxy
Name Servers
Network Configuration
Network Switch
NTP Servers
SNMP

Image Configuration

Manage the images to be used for creating virtual disks.

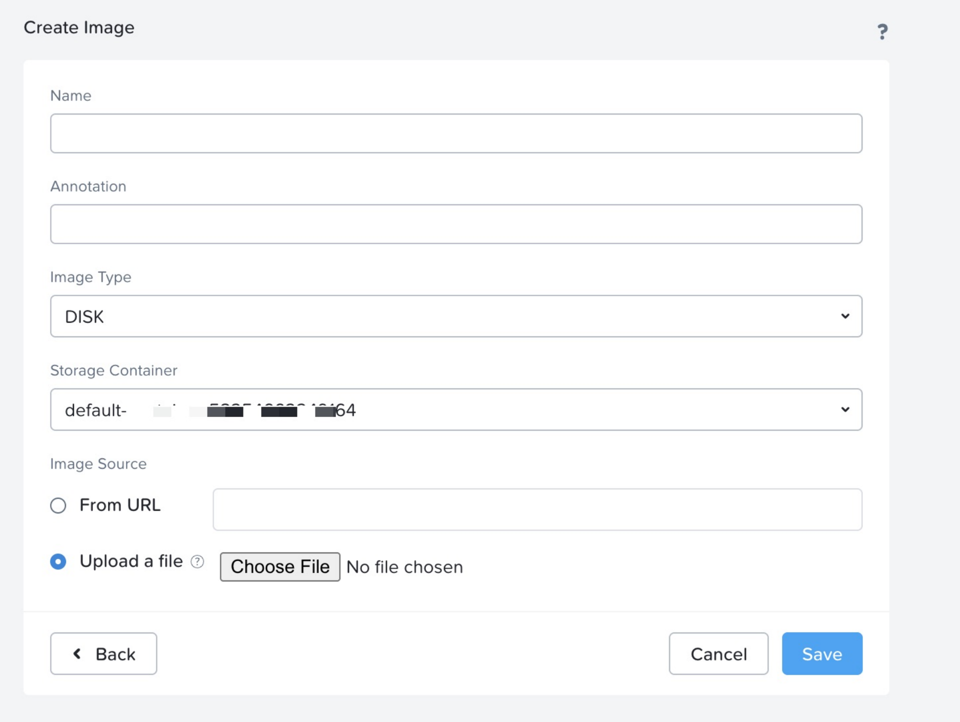
+ Upload Image

Name	Annotation	Type	State	Size
[redacted] mdk		DISK	ACTIVE	117.19 GiB
[redacted] mdk-2...		DISK	ACTIVE	117.19 GiB

Step 4 Click **Upload Image**.

The **Create Image** dialog box is displayed.

Figure 107: Create Image



Create Image

Name

Annotation

Image Type

DISK

Storage Container

default- [redacted] 64

Image Source

○ From URL

● Upload a file

Step 5 In the **Create Image** dialog box, enter the details.

a) **Name**: Enter name for the image.

b) **Annotation**: Enter annotation for the image.

c) **Image Type**: From the drop-down list, select image type as **DISK**.

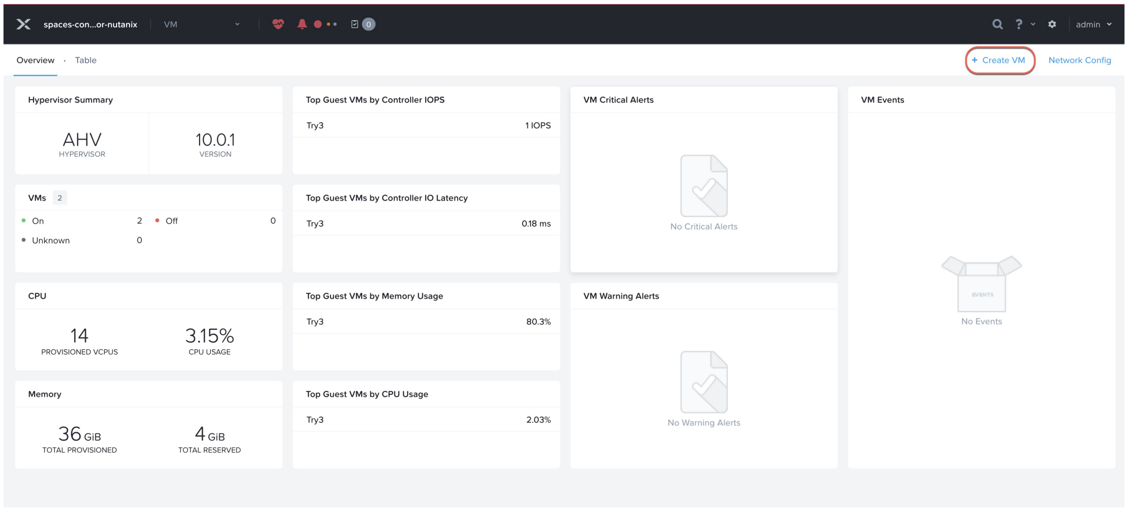
d) **Storage Container**: From the drop-down list, select the preferred storage container.

e) **Image Source**: Select **Upload a file** and click **Choose File** to add the extracted VMDK File.

f) Click **Save**.

Step 6 Navigate to the **VM** > **Overview** tab and click **Create VM**.

Figure 108: VM Overview



Hypervisor Summary

AHV HYPERVISOR | 10.0.1 VERSION

VMs 2

- On 2
- Off 0
- Unknown 0

CPU

14 PROVISIONED VCPUS | 3.15% CPU USAGE

Memory

36 GiB TOTAL PROVISIONED | 4 GiB TOTAL RESERVED

Top Guest VMs by Controller IOPS

Try3	1 IOPS

Top Guest VMs by Controller IO Latency

Try3	0.18 ms

Top Guest VMs by Memory Usage

Try3	80.3%

Top Guest VMs by CPU Usage

Try3	2.03%

VM Critical Alerts

No Critical Alerts

VM Warning Alerts

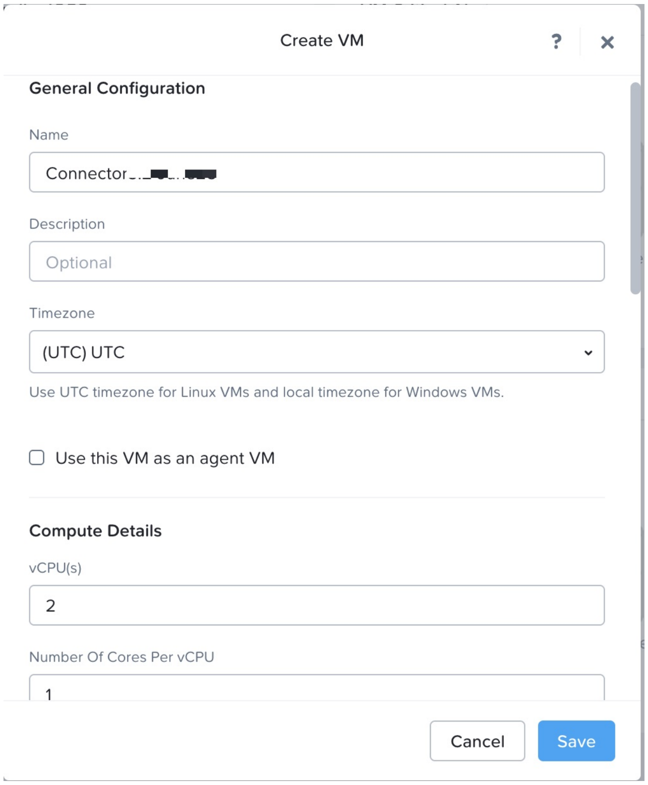
No Warning Alerts

VM Events

No Events

The **Create VM** dialog box is displayed.

Figure 109: Create VM



General Configuration

Name: Connector[redacted]

Description: Optional

Timezone: (UTC) UTC

Use UTC timezone for Linux VMs and local timezone for Windows VMs.

□ Use this VM as an agent VM

Compute Details

vCPU(s): 2

Number Of Cores Per vCPU: 1

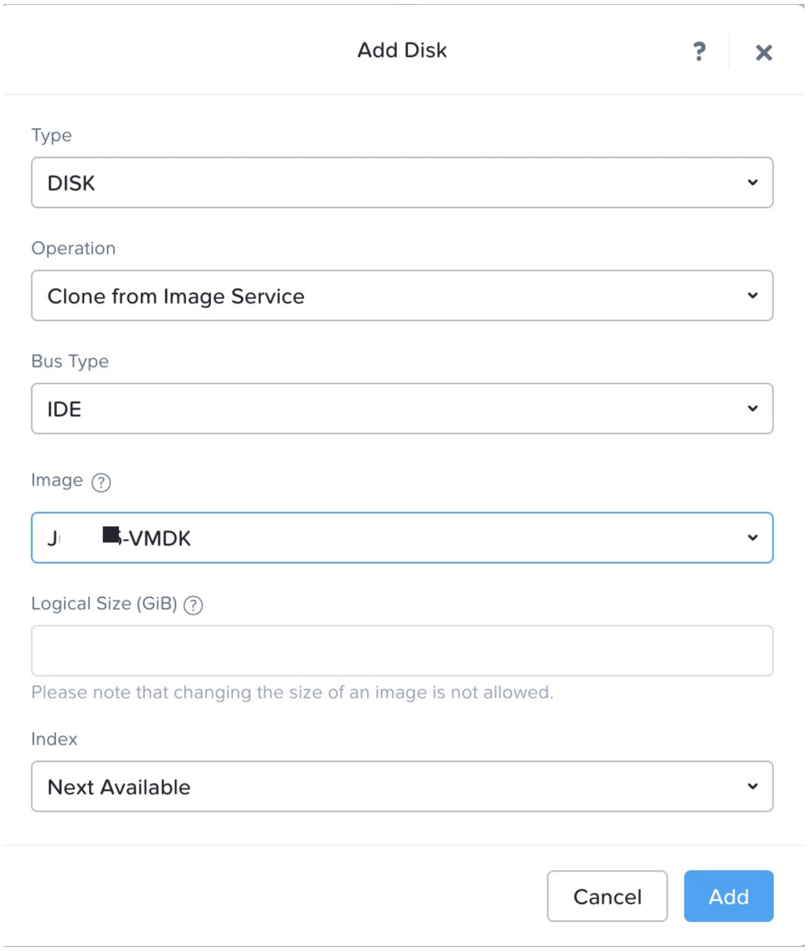
a) In the **Create VM** dialog box, under **General Configuration** section, enter the details.

- **Name**: Enter the name for the new **VM**.
- (Optional) **Description**: Enter the description for the new VM.
- **Timezone**: From the drop-down list, select the timezone.
- (Optional) **Use this VM as an agent VM**: Check this option to use the VM as an agent.
- **Compute Details**: Enter the **vCPU(s)**, **No of Cores per vCPU** details and **Memory**.
- **Boot Configuration Mode**: From the drop-down list, select **UEFI** as the boot configuration mode.

b) Click **Add Disk**.

The **Add Disk** dialog box is displayed.

Figure 110: Add Disk



Add Disk

Type: DISK

Operation: Clone from Image Service

Bus Type: IDE

Image: J[redacted]-VMDK

Logical Size (GiB):

Please note that changing the size of an image is not allowed.

Index: Next Available

c) In the **Add Disk** dialog box, enter the details.

- **Type**: From the drop-down list, select **DISK** as type.
- **Operation**: From the drop-down list, select **Clone from Image Service** as operation.

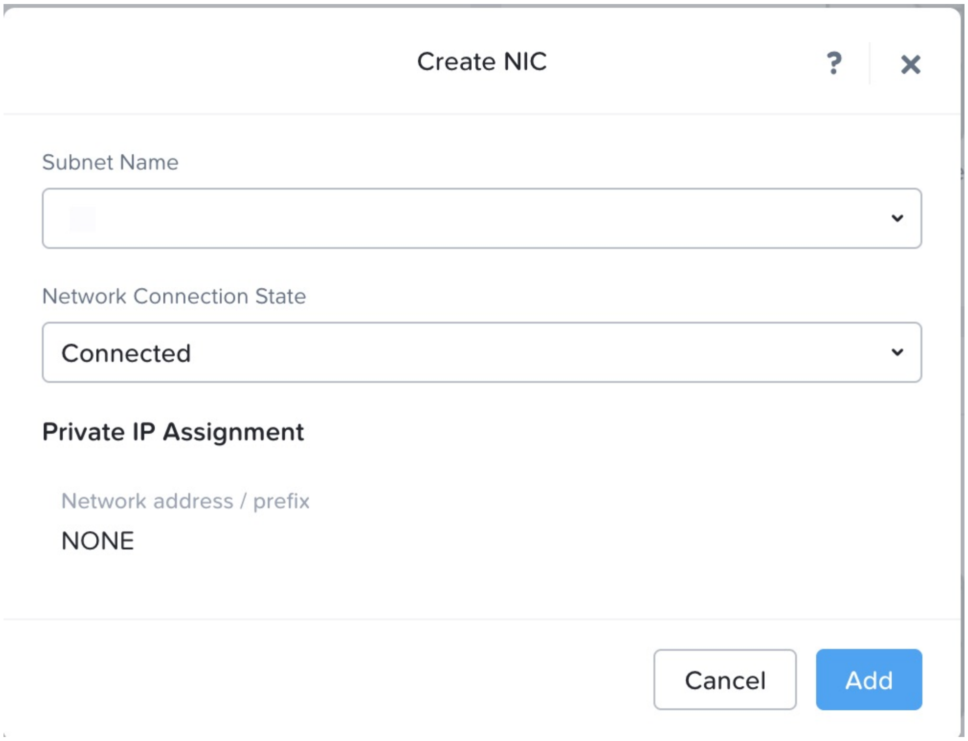
- **Bus Type**: From the drop-down list, select, **IDE** as the bus type.
- **Image**: From the drop-down list, select the **VMDK** image uploaded previously.
- **Logical Size (GiB)**: Displays the **VMDK** file size. You cannot edit the image logical size value.
- **Index**: From the drop-down list, select **Next Available** as index option.

d) Click **Add**.

Step 7 Click **Add New NIC**.

The **Create NIC** dialog box is displayed.

Figure 111: Create NIC



Create NIC

Subnet Name

Network Connection State: Connected

Private IP Assignment

Network address / prefix: NONE

a) In the **Create NIC** dialog box, enter the details.

- **Subnet Name**: From the drop-down list, select the appropriate subnet.
- **Network Connection State**: From the drop-down list, select **Connected** as the network connection state.
- **Private IP Assignment**: Enter **Network address / prefix** as required.

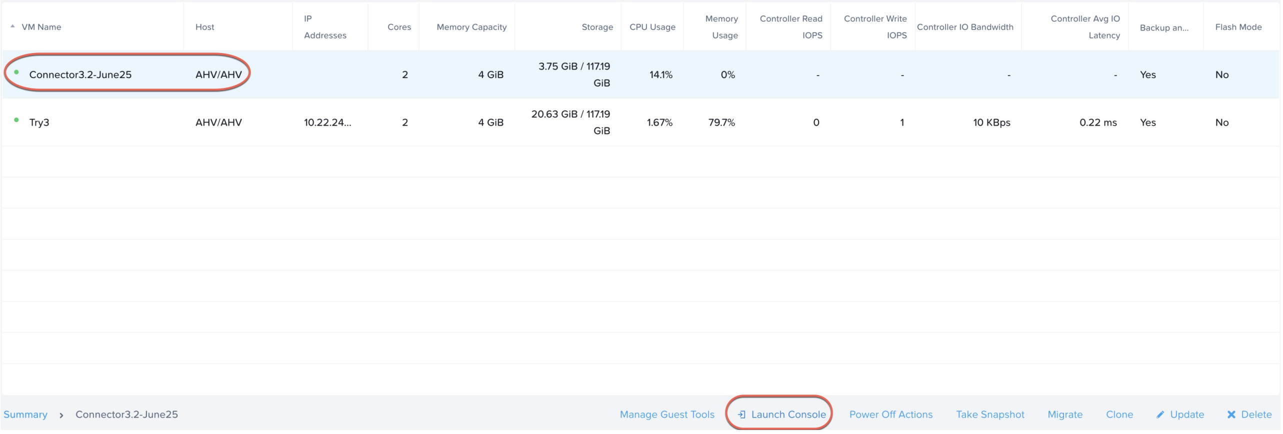
b) Click **Add**.

Step 8 Click **Save** to save and store the new VM configuration.

What to do next

To power on the new VM, navigate to **VM** > **Table tab** > **Power on the created VM**. After the VM is powered on, select the VM and click **Launch Console**.

Figure 112: Launch Console



VM Name	Host	IP Addresses	Cores	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Read IOPS	Controller Write IOPS	Controller IO Bandwidth	Controller Avg IO Latency	Backup an...	Flash Mode
Connector3.2-June25	AHV/AHV		2	4 GiB	3.75 GiB / 117.19 GiB	14.1%	0%	-	-	-	-	Yes	No
Try3	AHV/AHV	10.22.24...	2	4 GiB	20.63 GiB / 117.19 GiB	1.67%	79.7%	0	1	10 KBps	0.22 ms	Yes	No

Note For more information, see step 12 onwards in the Deploying the Connector 3 OVA (Single Interface).

CHAPTER 9

Cisco Spaces: Connector VM on Azure Environment

Cisco Spaces: Connector Azure cloud platform support

The Cisco Spaces: Connector 3.2 June, 2025 release supports the Azure cloud platform. To deploy the Azure Connector virtual machine (VM), you need the necessary access to Azure cloud platform.

Set Up Connector VM on Azure Environment

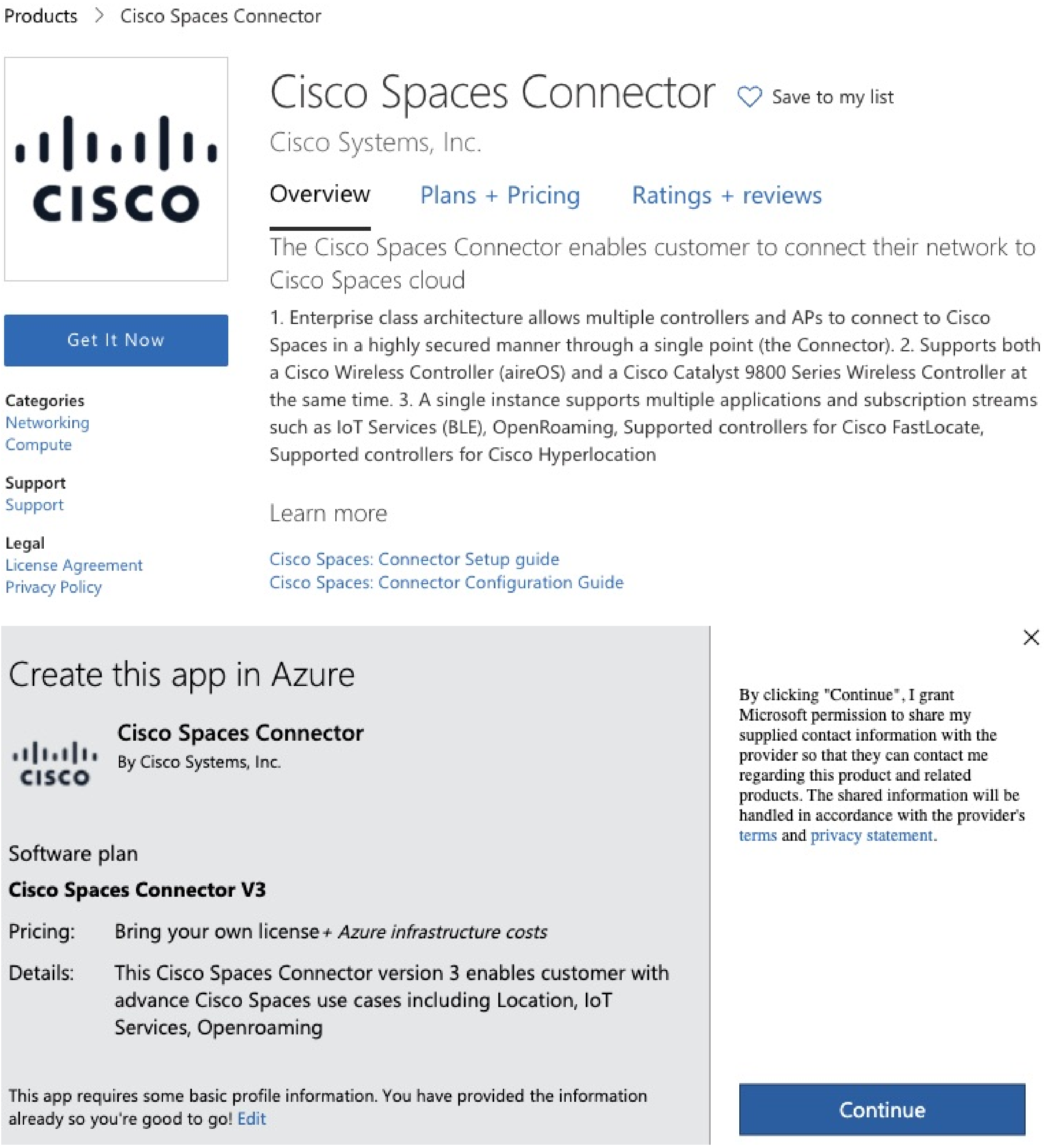
Follow the steps to setup a connector VM.

Procedure

Step 1 Log in to your Azure portal.

Step 2 In the Azure Marketplace, search for the latest connector release and click **Get It Now** > **Continue**.

Figure 113: Cisco Spaces Connector



Products > Cisco Spaces Connector

Cisco Spaces Connector ♡ Save to my list

Cisco Systems, Inc.

Overview Plans + Pricing Ratings + reviews

The Cisco Spaces Connector enables customer to connect their network to Cisco Spaces cloud

1. Enterprise class architecture allows multiple controllers and APs to connect to Cisco Spaces in a highly secured manner through a single point (the Connector). 2. Supports both a Cisco Wireless Controller (aireOS) and a Cisco Catalyst 9800 Series Wireless Controller at the same time. 3. A single instance supports multiple applications and subscription streams such as IoT Services (BLE), OpenRoaming, Supported controllers for Cisco FastLocate, Supported controllers for Cisco Hyperlocation

Learn more

Cisco Spaces: Connector Setup guide
Cisco Spaces: Connector Configuration Guide

Get It Now

Categories
Networking
Compute

Support
Support

Legal
License Agreement
Privacy Policy

Create this app in Azure

Cisco Spaces Connector
By Cisco Systems, Inc.

Software plan

Cisco Spaces Connector V3

Pricing: Bring your own license + *Azure infrastructure costs*

Details: This Cisco Spaces Connector version 3 enables customer with advance Cisco Spaces use cases including Location, IoT Services, Openroaming

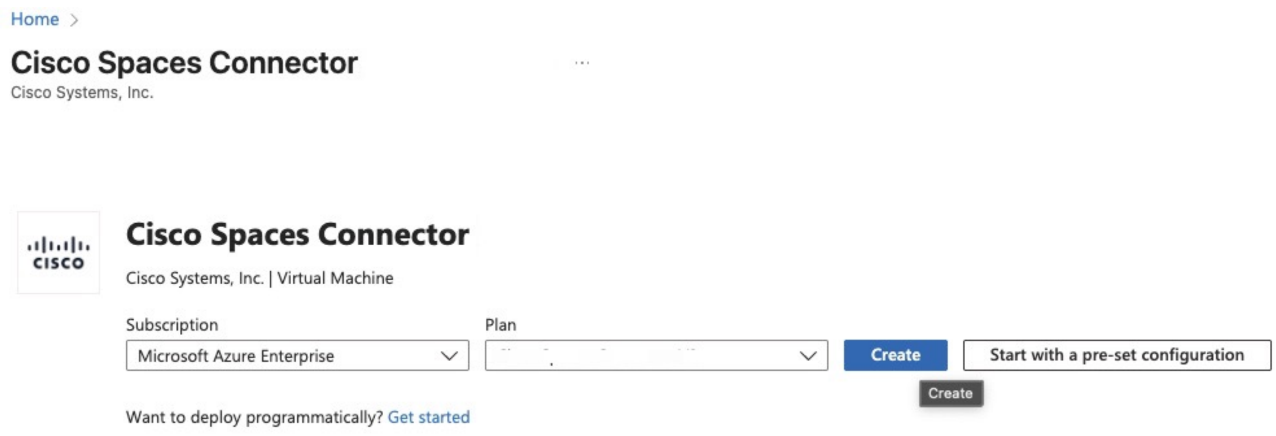
This app requires some basic profile information. You have provided the information already so you're good to go! Edit

By clicking "Continue", I grant Microsoft permission to share my supplied contact information with the provider so that they can contact me regarding this product and related products. The shared information will be handled in accordance with the provider's terms and privacy statement.

Continue

The Cisco Spaces: Connector preview page is displayed.

Figure 114: Cisco Spaces: Connector



Home >

Cisco Spaces Connector

Cisco Systems, Inc.

Cisco Spaces Connector

Cisco Systems, Inc. | Virtual Machine

Subscription: Microsoft Azure Enterprise

Plan

Want to deploy programmatically? Get started

Step 3 In the Cisco Spaces: Connector preview page, perform these steps:

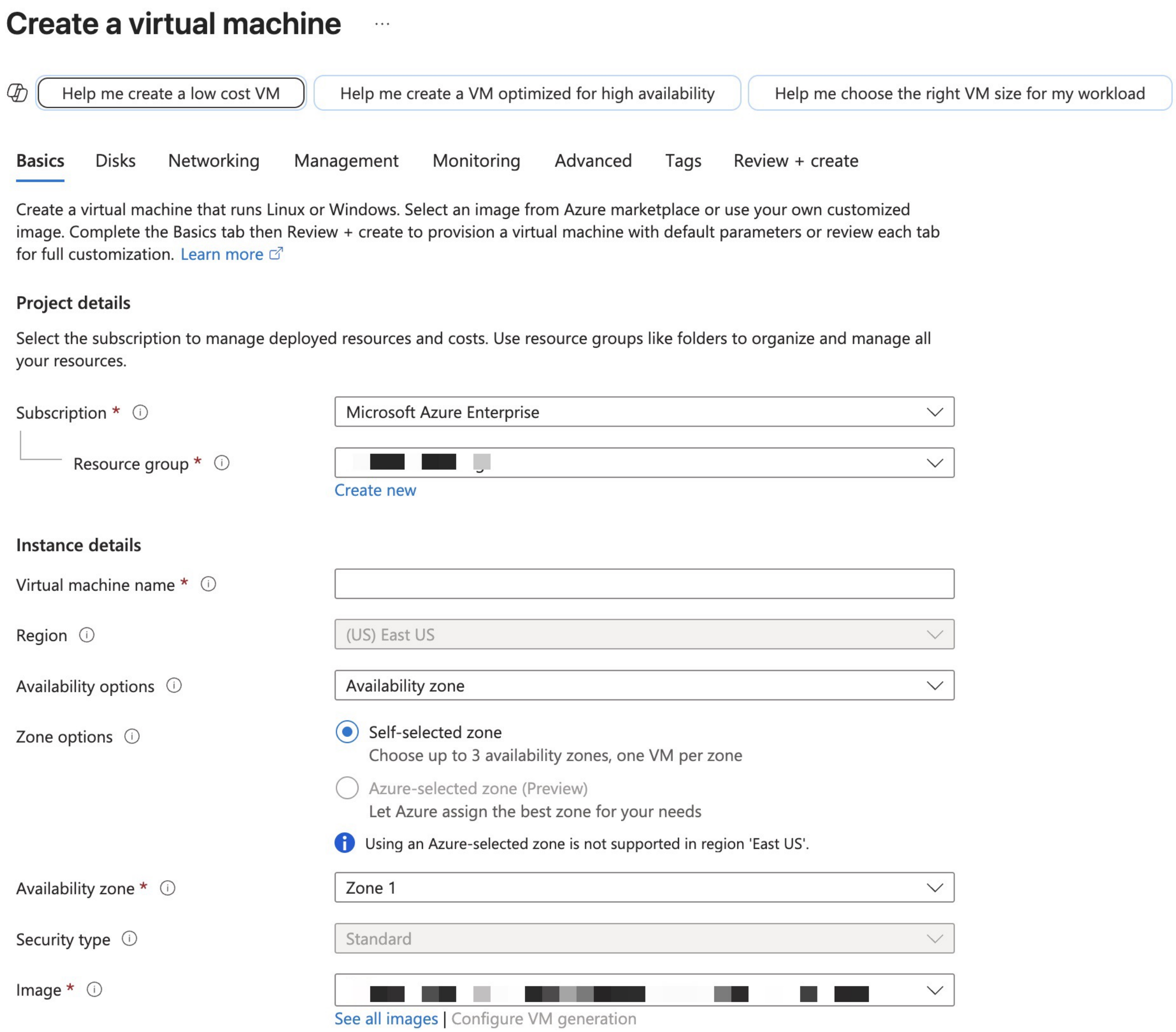
a) From the **Subscription** drop-down list, select **Microsoft Azure Enterprise** as the type.

b) From the **Plan** drop-down list, select **Cisco Spaces Connector V3** as your subscription plan.

c) Click **Create**.

Step 4 In the **Create a virtual machine** window, under the **Basics** tab, perform these steps:

Figure 115: Create a virtual machine Basics tab



Create a virtual machine ···

Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ: Microsoft Azure Enterprise

Resource group * ⓘ: [redacted]

Create new

Instance details

Virtual machine name * ⓘ:

Region ⓘ: (US) East US

Availability options ⓘ: Availability zone

Zone options ⓘ:

● Self-selected zone
Choose up to 3 availability zones, one VM per zone

○ Azure-selected zone (Preview)
Let Azure assign the best zone for your needs

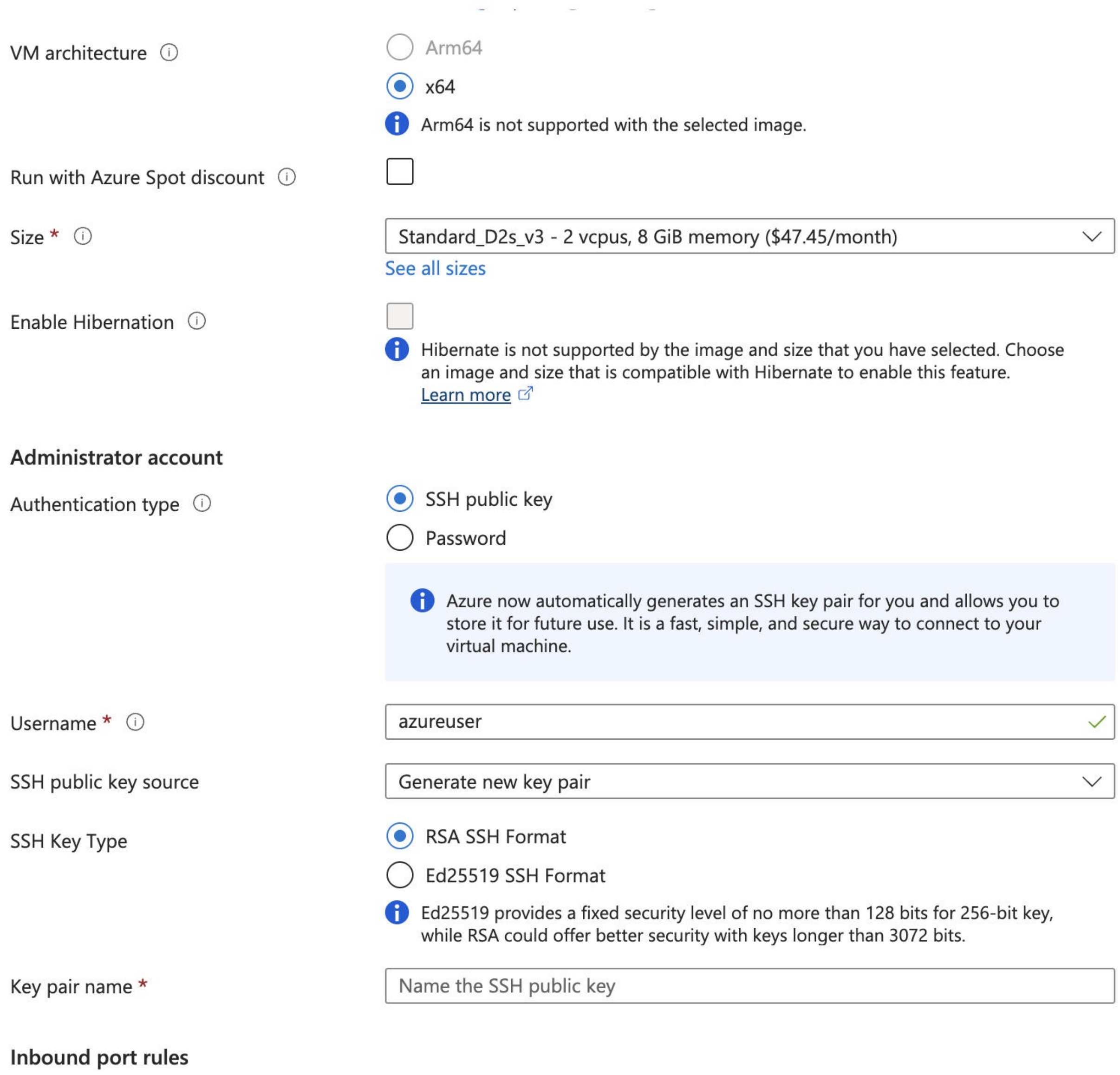
ⓘ Using an Azure-selected zone is not supported in region 'East US'.

Availability zone * ⓘ: Zone 1

Security type ⓘ: Standard

Image * ⓘ: [redacted]

See all images | Configure VM generation



VM architecture ⓘ ○ Arm64 ● x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ □

Size * ⓘ Standard_D2s_v3 - 2 vcpus, 8 GiB memory ($47.45/month)

See all sizes

Enable Hibernation ⓘ □

Hibernate is not supported by the image and size that you have selected. Choose an image and size that is compatible with Hibernate to enable this feature. Learn more

Administrator account

Authentication type ⓘ ● SSH public key ○ Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username * ⓘ azureuser ✓

SSH public key source: Generate new key pair

SSH Key Type ● RSA SSH Format ○ Ed25519 SSH Format

Ed25519 provides a fixed security level of no more than 128 bits for 256-bit key, while RSA could offer better security with keys longer than 3072 bits.

Key pair name * Name the SSH public key

Inbound port rules

a) From the **Resource group** drop-down list, under the **Subscription** section within the **Project details** area, select your resource group.

Create a new one if required.

b) In the **Virtual machine name** field, under the section **Instance details**, enter a name for the connector VM.

c) From the **Size** drop-down list, select the recommended size. These are the recommended sizes:

- Standard_D2ds_v4 - 2 vcpus, 8 GiB memory.
- Standard_D4ds_v4 - 4 vcpus, 16 GiB memory.
- Standard_D8ds_v4 - 8 vcpus, 32 GiB memory.

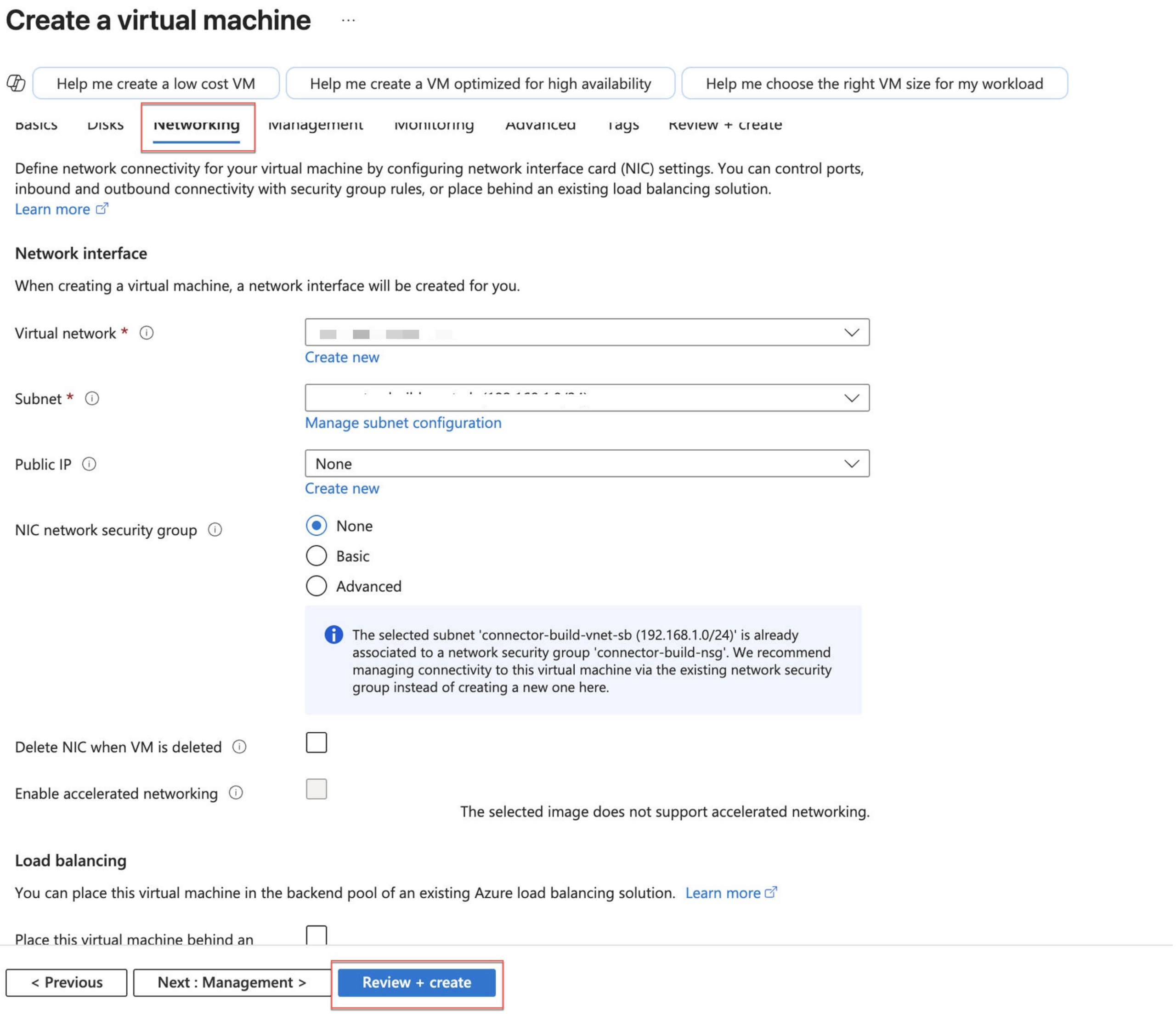
d) From the **Authentication type**, under the section **Administrator account**, select the **SSH public key** radio button.

Note

The **Username** is **azureuser** by default. The **Key pair name** is populated by itself. You can keep the same or replace with your own.

Step 5 In the **Create a virtual machine** window, perform these steps under the **Networking** tab:

Figure 116: Create a virtual machine Networking tab



Create a virtual machine ...

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : [redacted]
Create new

Subnet * : [redacted]
Manage subnet configuration

Public IP: None
Create new

NIC network security group:
● None
○ Basic
○ Advanced

The selected subnet 'connector-build-vnet-sb (192.168.1.0/24)' is already associated to a network security group 'connector-build-nsg'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Delete NIC when VM is deleted □

Enable accelerated networking □
The selected image does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an □

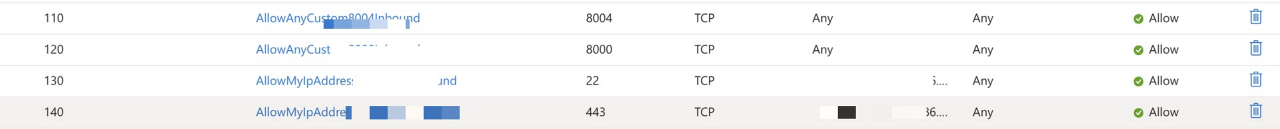
< Previous | Next : Management > | Review + create

a) From the **Virtual network** drop-down list, under the section **Network interface**, select your network group.

b) From the **Subnet** drop-down list, select your specific subnet.

c) Configure and allow the required inbound rules.

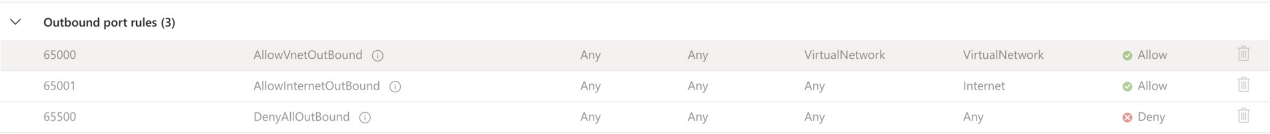
Figure 117: Configure required inboud rules



110	AllowAnyCus[redacted]nd	8004	TCP	Any	Any	✓ Allow	🗑
120	AllowAnyCust[redacted]	8000	TCP	Any	Any	✓ Allow	🗑
130	AllowMyIpAddres[redacted]und	22	TCP	[redacted]5....	Any	✓ Allow	🗑
140	AllowMyIpAddre[redacted]	443	TCP	[redacted]36....	Any	✓ Allow	🗑

d) Configure and allow the required outbound rules.

Figure 118: Configure required outbound rules



Outbound port rules (3)

65000	AllowVnetOutBound ⓘ	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound ⓘ	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound ⓘ	Any	Any	Any	Any	✗ Deny

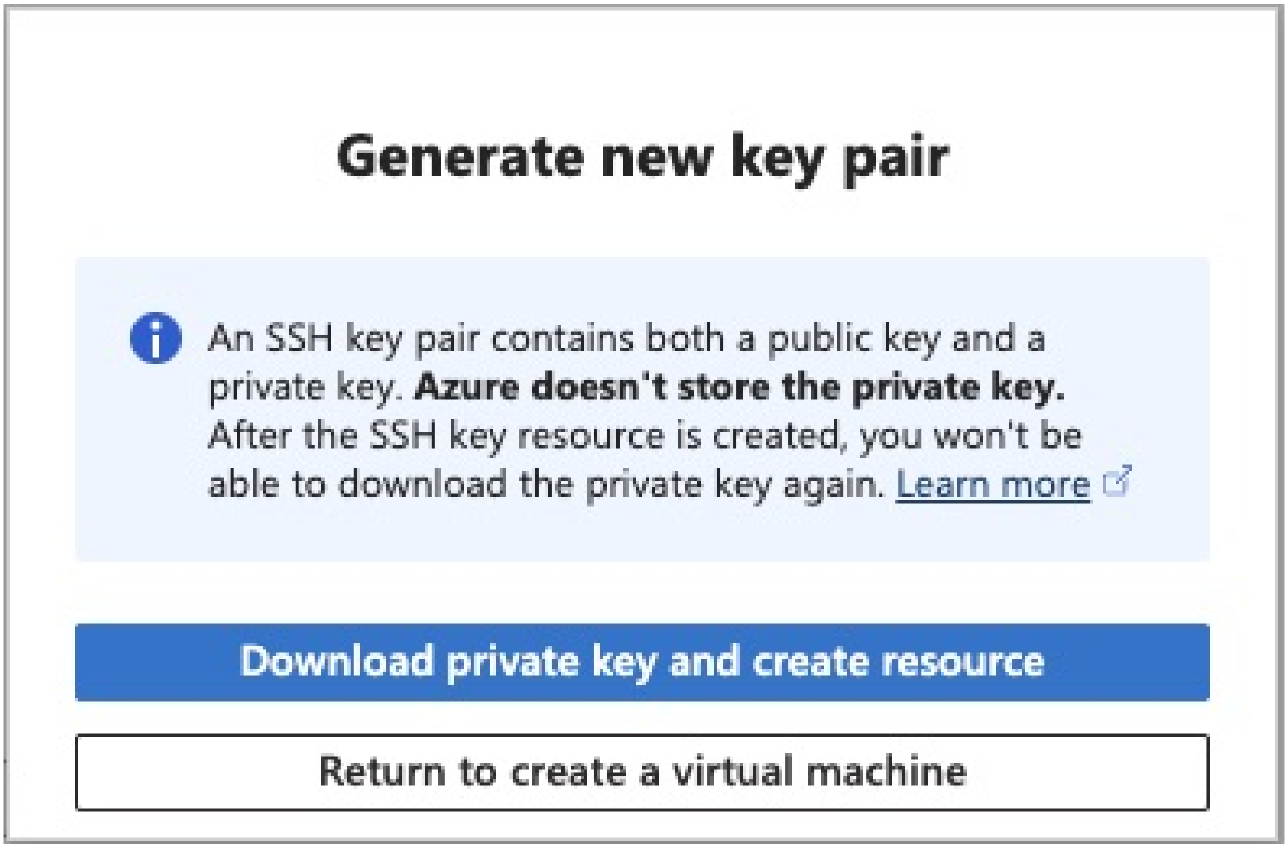
e) Click **Review + create**.

Step 6 To change the permission of the downloaded key, run the command:

Example:

```
chmod 600 <keyname
```

Figure 119: Generate new key pair



Generate new key pair

An SSH key pair contains both a public key and a private key. **Azure doesn't store the private key.** After the SSH key resource is created, you won't be able to download the private key again. Learn more

Download private key and create resource
Return to create a virtual machine

Note

We recommend you to download this key pair to your system, navigate to the file location and configure appropriate permissions using the **chmod** command.

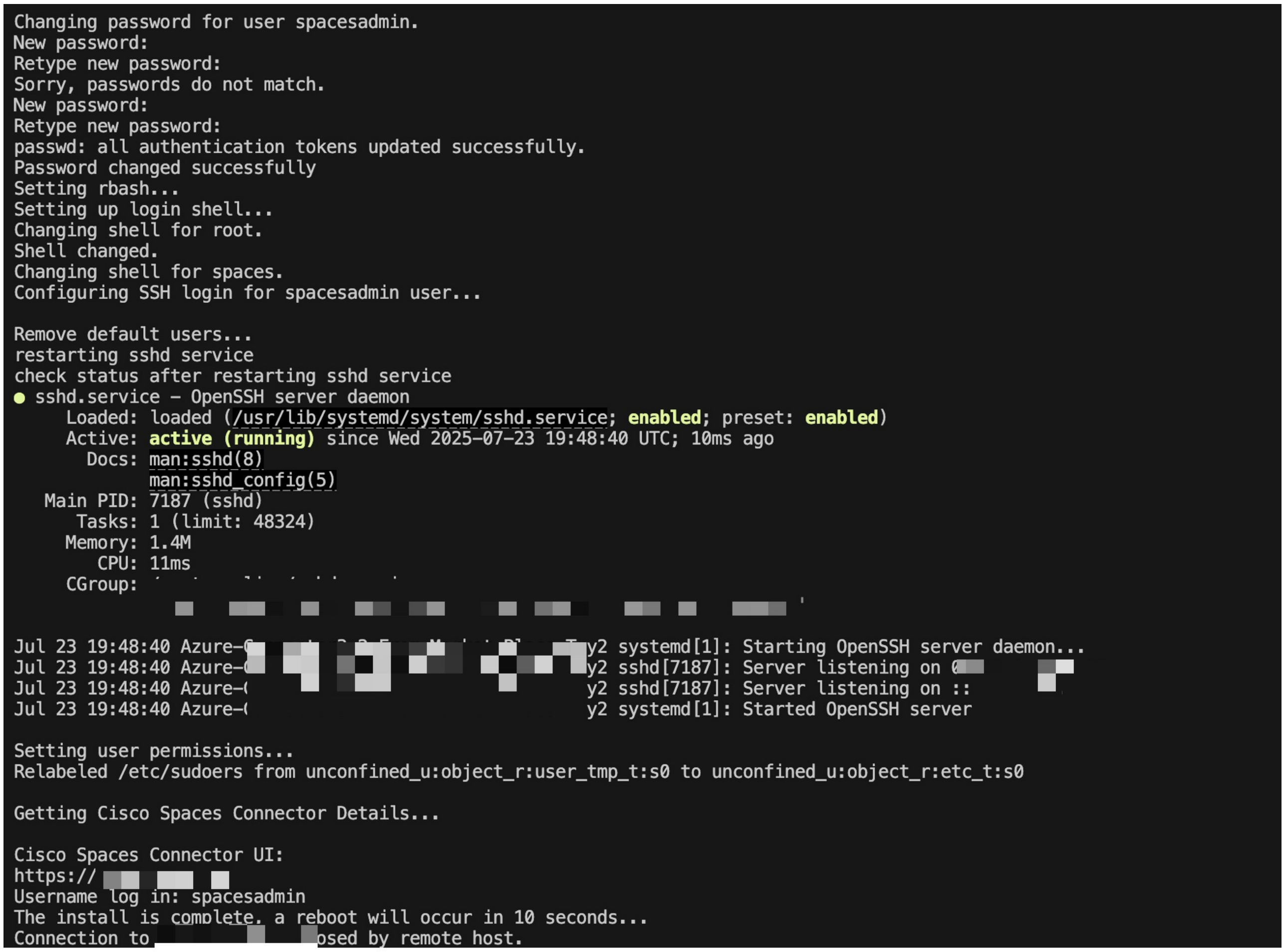
Step 7 SSH to the connector as **azureuser** using the public key.

Example:

```
ssh -i <public_key> azureuser@<ip_address>
```

Step 8 Enter the password for the Cisco Spaces administrator (spacesadmin).

Figure 120: Cisco Spaces administrator



```
Changing password for user spacesadmin.
New password:
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Password changed successfully
Setting rbash...
Setting up login shell...
Changing shell for root.
Shell changed.
Changing shell for spaces.
Configuring SSH login for spacesadmin user...

Remove default users...
restarting sshd service
check status after restarting sshd service
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-07-23 19:48:40 UTC; 10ms ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 7187 (sshd)
      Tasks: 1 (limit: 48324)
     Memory: 1.4M
        CPU: 11ms
     CGroup: [redacted]

Jul 23 19:48:40 Azure-[redacted]y2 systemd[1]: Starting OpenSSH server daemon...
Jul 23 19:48:40 Azure-[redacted]y2 sshd[7187]: Server listening on [redacted]
Jul 23 19:48:40 Azure-[redacted]y2 sshd[7187]: Server listening on :: [redacted]
Jul 23 19:48:40 Azure-[redacted]y2 systemd[1]: Started OpenSSH server

Setting user permissions...
Relabeled /etc/sudoers from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:etc_t:s0

Getting Cisco Spaces Connector Details...

Cisco Spaces Connector UI:
https:// [redacted]
Username log in: spacesadmin
The install is complete. a reboot will occur in 10 seconds...
Connection to [redacted]osed by remote host.
```

The Cisco Spaces: Connector reboots and the connector UI is displayed.

What to do next

For more information on how to generate a token for your deployed azure connector, follow the steps here: Connector on Cisco Spaces.

CHAPTER 10

Connector on Cisco Spaces

Activating Connector 3 on Cisco Spaces

This section provides information about how to activate a deployed connector on your Cisco Spaces account.

Using the following procedure, you generate a token for a deployed connector that you want to add to your Cisco Spaces account. Note that you need a separate token for each deployed connector. Each token is specific to a connector and hence enables Cisco Spaces to identify and connect to connector.

Cisco Spaces supports multiple connectors, and you can associate each connector with one or multiple wireless controllers.

Note A Cisco Spaces: Connector instance can communicate with only one Cisco Spaces account at a time.

Before you begin

Download and deploy the Cisco Spaces: Connector OVA. See Deploying the Connector 3 OVA (Single Interface), on page 65

Procedure

Step 1 Log in to **Cisco Spaces**.

Note
The Cisco Spaces URL is region-dependent.

Step 2 From the left navigation pane, choose **Setup** > **Wireless Networks**.

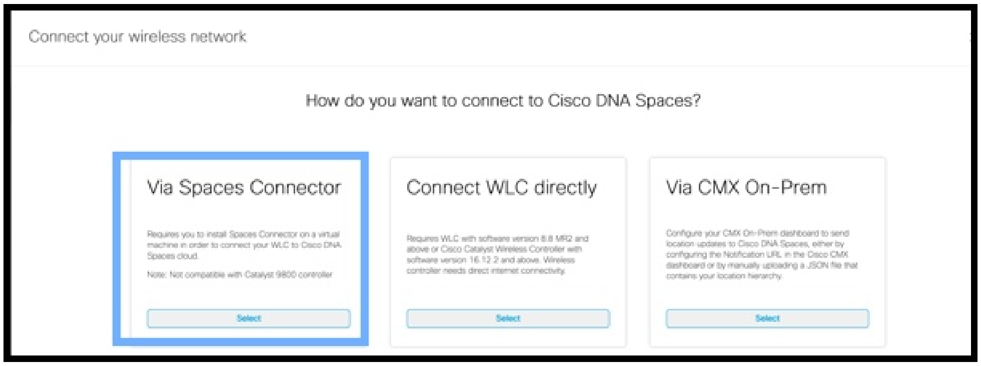
Step 3 In the **Get your wireless network connected with Cisco DNA Spaces** area, click **Add New**.

Step 4 In the **Cisco AireOS Controller/Catalyst 9800 Wireless Controller** area, click **Select.**

Figure 121: Choose Cisco AireOS Controller/Catalyst 9800 Wireless Controller

Step 5 In the **Via Spaces Connector** area, click **Select**.

Figure 122: Via Spaces Connector



Connect your wireless network

How do you want to connect to Cisco DNA Spaces?

Via Spaces Connector

Requires you to install Spaces Connector on a virtual machine in order to connect your WLC to Cisco DNA Spaces cloud.

Note: Not compatible with Catalyst 9800 controller

Select

Connect WLC directly

Requires WLC with software version 8.8 MR2 and above or Cisco Catalyst Wireless Controller with software version 16.12.2 and above. Wireless controller needs direct internet connectivity.

Select

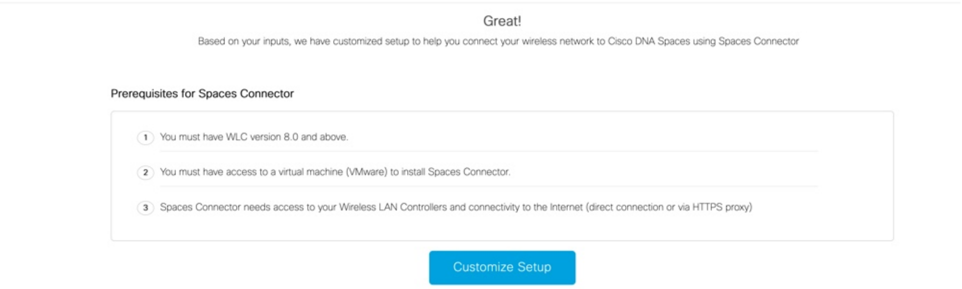
Via CMX On-Prem

Configure your CMX On-Prem dashboard to send location updates to Cisco DNA Spaces, either by configuring the Notification URL in the Cisco CMX dashboard or by manually uploading a JSON file that contains your location hierarchy.

Select

Step 6 In the **Prerequisites for Spaces Connector** dialog box, click **Continue Setup**.

Figure 123: Read Prerequisites for Spaces Connector



Great!

Based on your inputs, we have customized setup to help you connect your wireless network to Cisco DNA Spaces using Spaces Connector

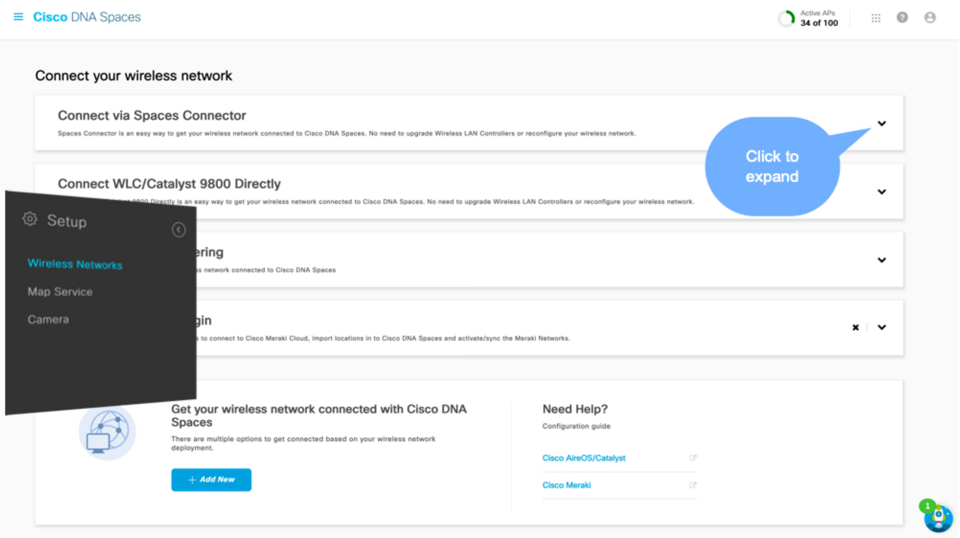
Prerequisites for Spaces Connector

1. You must have WLC version 8.0 and above.
2. You must have access to a virtual machine (VMware) to install Spaces Connector.
3. Spaces Connector needs access to your Wireless LAN Controllers and connectivity to the Internet (direct connection or via HTTPS proxy)

Customize Setup

Step 7 Expand the **Connect via Spaces Connector** area using the respective drop-down arrow.

Figure 124: Expand Connect via Spaces Connector



Connect your wireless network

Connect via Spaces Connector

Spaces Connector is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.

Connect WLC/Catalyst 9800 Directly

9800 Directly is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.

ering

s network connected to Cisco DNA Spaces

gin

to connect to Cisco Meraki Cloud, import locations in to Cisco DNA Spaces and activate/sync the Meraki Networks.

Get your wireless network connected with Cisco DNA Spaces

There are multiple options to get connected based on your wireless network deployment.

+ Add New

Need Help?

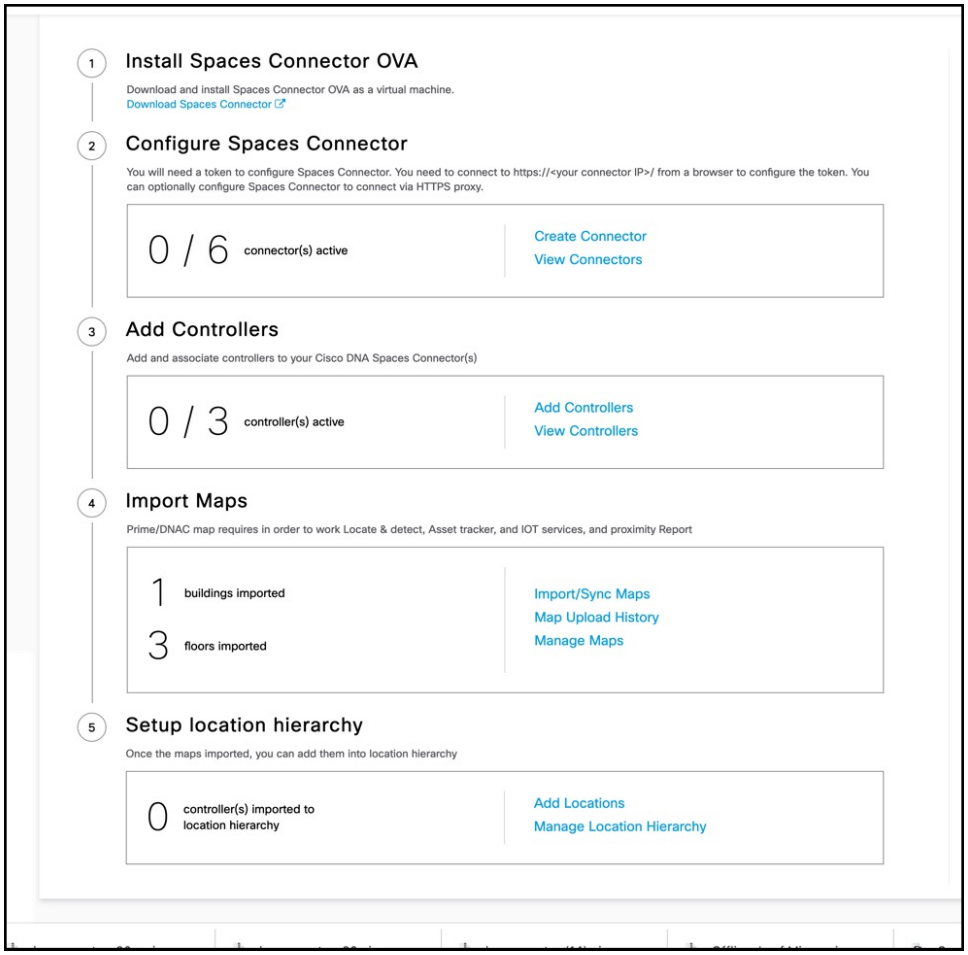
Configuration guide

Cisco AireOS/Catalyst

Cisco Meraki

Step 8 In the displayed list of steps, in the **Configure Spaces Connector** area, click **Create Connector**.

Figure 125: Connect via Spaces Connector > Create Connector



1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.

Download Spaces Connector

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

0 / 6 connector(s) active

Create Connector
View Connectors

3 Add Controllers

Add and associate controllers to your Cisco DNA Spaces Connector(s)

0 / 3 controller(s) active

Add Controllers
View Controllers

4 Import Maps

Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

1 buildings imported

3 floors imported

Import/Sync Maps
Map Upload History
Manage Maps

5 Setup location hierarchy

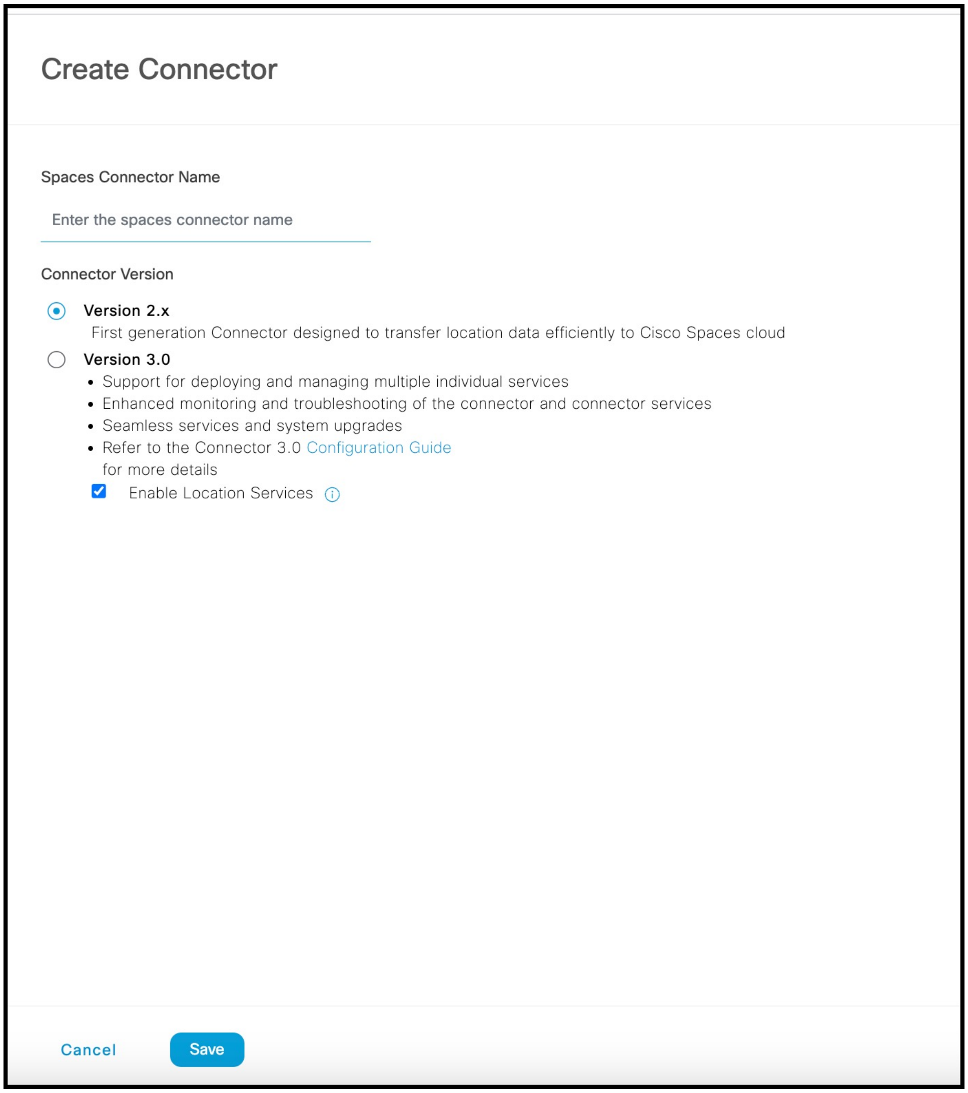
Once the maps imported, you can add them into location hierarchy

0 controller(s) imported to location hierarchy

Add Locations
Manage Location Hierarchy

Step 9 In the **Create connector** window that is displayed, enter a name for connector, and click **Version 3.0 (beta).** as the **Connector Version**, and click **Save**.

Figure 126: Name and Version of Connector



Create Connector

Spaces Connector Name

Enter the spaces connector name

Connector Version

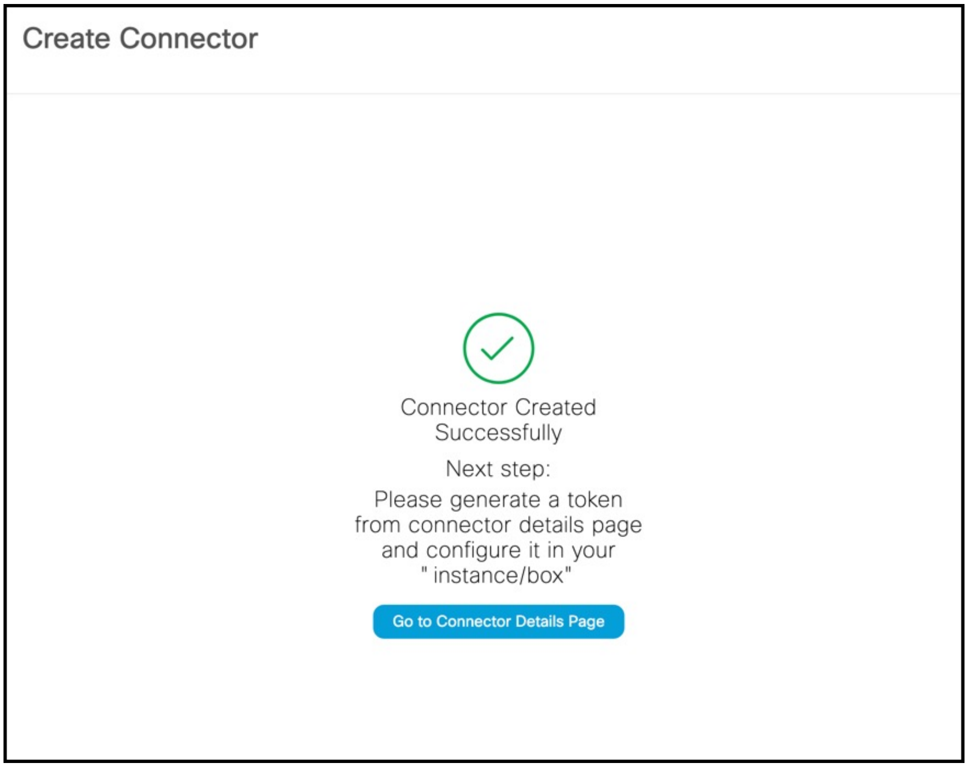
● Version 2.x
First generation Connector designed to transfer location data efficiently to Cisco Spaces cloud

○ Version 3.0
- Support for deploying and managing multiple individual services
- Enhanced monitoring and troubleshooting of the connector and connector services
- Seamless services and system upgrades
- Refer to the Connector 3.0 Configuration Guide for more details

☑ Enable Location Services ⓘ

Connector is successfully created. Click **Go to Connector Details** Page.

Figure 127: Connector Created Successfully



Create Connector

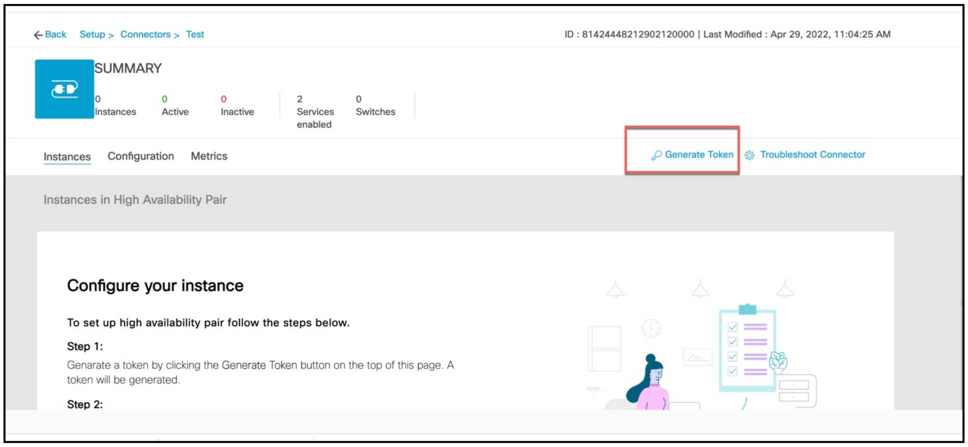
Connector Created Successfully

Next step:

Please generate a token from connector details page and configure it in your " instance/box"

Step 10 In the connector details window, you can see a summary of the configurations for this connector. Click **Generate Token.**

Figure 128: Generate Token



ID : 81424448212902120000 | Last Modified : Apr 29, 2022, 11:04:25 AM

SUMMARY

0 Instances
0 Active
0 Inactive
2 Services enabled
0 Switches

Instances in High Availability Pair

Configure your instance

To set up high availability pair follow the steps below.

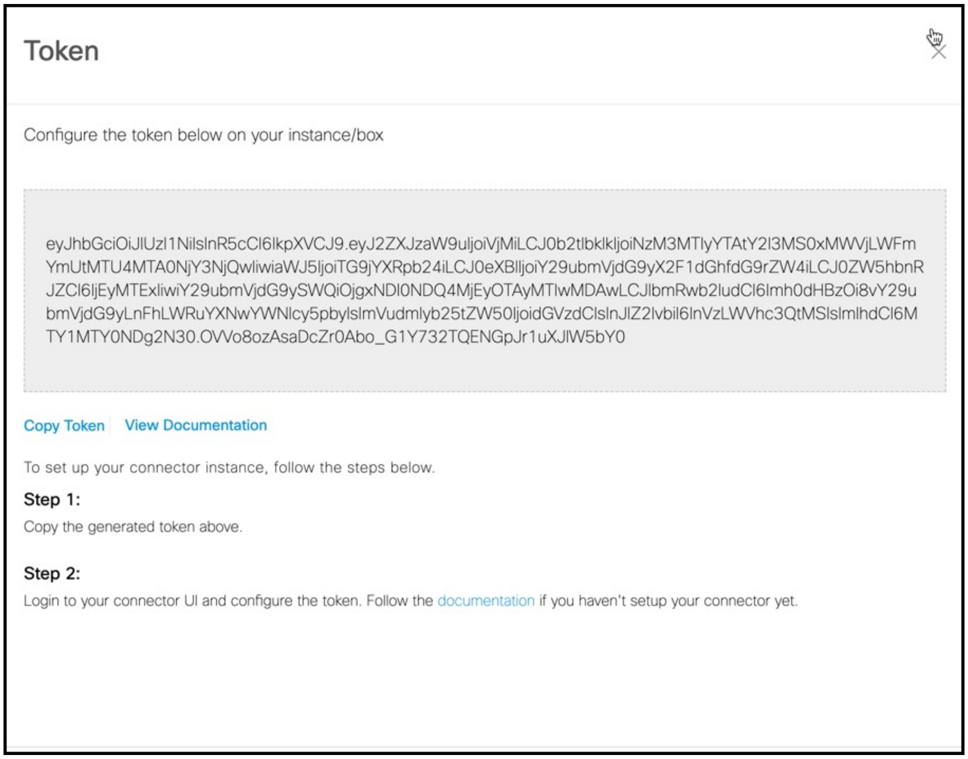
Step 1:

Genarate a token by clicking the Generate Token button on the top of this page. A token will be generated.

Step 2:

Step 11 In the **Token** window that is displayed, click **Copy Token**.

Figure 129: Copy Token



Token

Configure the token below on your instance/box

```
eyJhbGciOiJlUzl1NilsInR5cCl6IkpXVCJ9.eyJ2ZXJzaW9uljoiVjMiLCJ0b2tlbklkIjoiNzM3MTIyYTAtY2I3MS0xMWVjLWFm
YmUtMTU4MTA0NjY3NjQwliwiaWJ5ljoiTG9jYXRpb24iLCJ0eXBlIjoiY29ubmVjdG9yX2F1dGhfdG9rZW4iLCJ0ZW5hbnR
JZCl6IjEyMTExliwiY29ubmVjdG9ySWQiOjgxNDI0NDQ4MjEyOTAyMTIwMDAwLCJlbmRwb2ludCl6Imh0dHBzOi8vY29u
bmVjdG9yLnFhLWRuYXNwYWNlcy5pbylsImVudmlyb25tZW50IjoidGVzdClsInJlZ2lvbil6InVzLWVhc3QtMSIsImlhdCl6M
TY1MTY0NDg2N30.OVVo8ozAsaDcZr0Abo_G1Y732TQENGpJr1uXJlW5bY0
```

To set up your connector instance, follow the steps below.

Step 1:

Copy the generated token above.

Step 2:

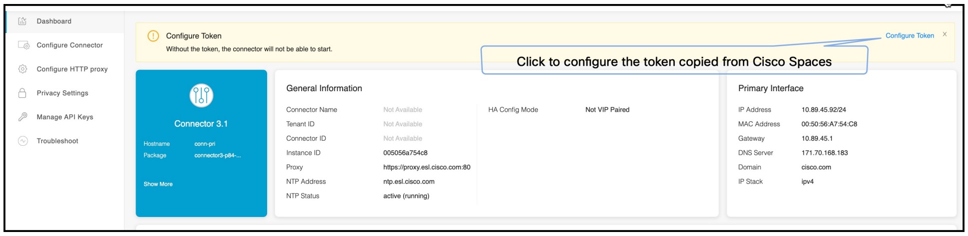
Login to your connector UI and configure the token. Follow the documentation if you haven't setup your connector yet.

Step 12 Open the connector GUI.

Step 13 (Optional) If your network is behind a proxy, configure the GUI with the proxy. See Configure a Proxy , on page 109

Step 14 In the **Configure Token** area that is displayed, click **Configure Token**.

Figure 130: Configure Token



Configure Token

Without the token, the connector will not be able to start.

Click to configure the token copied from Cisco Spaces

Connector 3.1

Hostname	conn-pri
Package	connector3-p84-...

General Information

Connector Name	Not Available	HA Config Mode	Not VIP Paired
Tenant ID	Not Available		
Connector ID	Not Available		
Instance ID	005056a754c8		
Proxy	https://proxy.esl.cisco.com:80		
NTP Address	ntp.esl.cisco.com		
NTP Status	active (running)		

Primary Interface

IP Address	10.89.45.92/24
MAC Address	00:50:56:A7:54:C8
Gateway	10.89.45.1
DNS Server	171.70.168.183
Domain	cisco.com
IP Stack	ipv4

Step 15 In the window that is displayed, in the **Token** text, field enter the token copied from Cisco Spaces and click **Configure**.

Warning

During this step, if you face a connectivity issue between Cisco Spaces: Connector and Cisco Spaces dashboard, the Connector could hang without an error. You can still access the Connector through SSH. You may also be unable to log in the Connector GUI after this issue.

Step 16 Add the following services as required:

- Configuring IoT Services

- Configuring Hotspot Services

Monitor the Status of Service Installation

After you have initiated the installation of a service, you can monitor the status of the service installation in connector from the Cisco Spaces dashboard.

Procedure

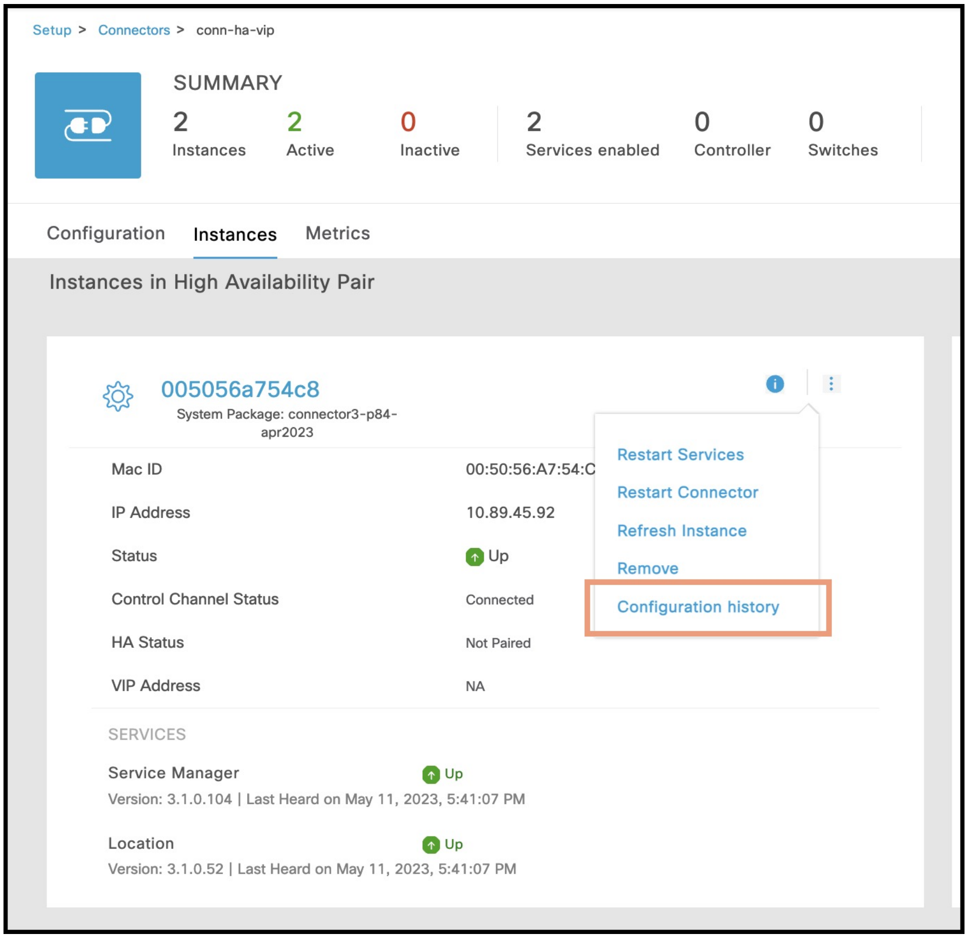
Step 1 From Cisco Spaces dashboard, choose **Setup** > **Wireless Networks.**

a) In the **Connect via Spaces Connector** area titled **Step 2 Configure Spaces Connector**, click **View Connectors**.

Step 2 From the **Connectors** window that is displayed, choose the connector of your choice.

Step 3 In the connector details window that is displayed, click the **Instances** tab.
You can click the i button and then **Configuration History** to monitor the status of the service installation here.

Figure 131: Monitoring the Status of Service installation



2	2	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

005056a754c8

System Package: connector3-p84-apr2023

Mac ID	00:50:56:A7:54:C
IP Address	10.89.45.92
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

SERVICES

Service Manager Up
Version: 3.1.0.104 | Last Heard on May 11, 2023, 5:41:07 PM

Location Up
Version: 3.1.0.52 | Last Heard on May 11, 2023, 5:41:07 PM

CHAPTER 11

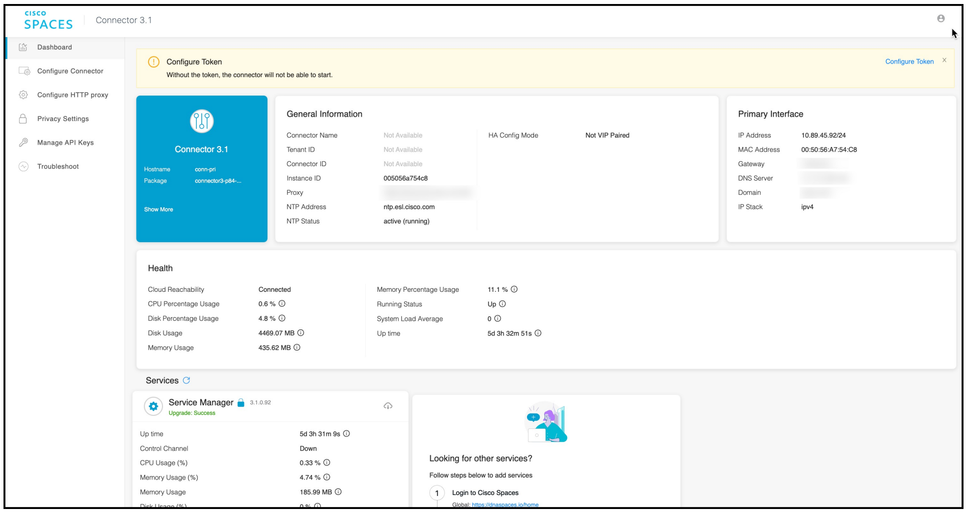
Connector GUI

Connector GUI

The connector GUI allows you to configure the following:

- Proxy
- Tokens retrieved from Cisco Spaces

Figure 132: Connector GUI



CISCO SPACES | Connector 3.1

Configure Token
Without the token, the connector will not be able to start.

Connector 3.1
Hostname conn-pri
Package connector3-p84-...

General Information

Connector Name	Not Available	HA Config Mode	Not VIP Paired
Tenant ID	Not Available		
Connector ID	Not Available		
Instance ID	005056a754c8		
Proxy	[redacted]		
NTP Address	ntp.esl.cisco.com		
NTP Status	active (running)		

Primary Interface

IP Address	10.89.45.92/24
MAC Address	00:50:56:A7:54:C8
Gateway	[redacted]
DNS Server	[redacted]
Domain	[redacted]
IP Stack	ipv4

Health

Cloud Reachability	Connected	Memory Percentage Usage	11.1 %
CPU Percentage Usage	0.6 %	Running Status	Up
Disk Percentage Usage	4.8 %	System Load Average	0
Disk Usage	4469.07 MB	Up time	5d 3h 32m 51s
Memory Usage	435.62 MB		

Services

Service Manager 3.1.0.92
Upgrade: Success

Up time	5d 3h 31m 9s
Control Channel	Down
CPU Usage (%)	0.33 %
Memory Usage (%)	4.74 %
Memory Usage	185.99 MB
Disk Usage (%)	0 %

Looking for other services?
Follow steps below to add services
1 Login to Cisco Spaces
Global: https://dnaspaces.io/home

The dashboard is divided into areas that provide you with clear information about the following:

- Connector-specific configurations
- Status of connectivity to Cisco Spaces
- Status of services running on connector. Additional buttons here allow you to navigate away and view more detailed information about each service, such as relevant service configurations and status.

The following are the names of various areas on the dashboard, and a description of the information presented:

- General Information: This area has information about the configurations that are made on this connector, the tenant ID, and whether the token is configured.
- Health: This area has information about the health of connector, the connectivity to Cisco Spaces, and other metrics.
- Services: Separate areas are available for each service. See the respective service section for details of the information displayed here.

Configuring Privacy Settings

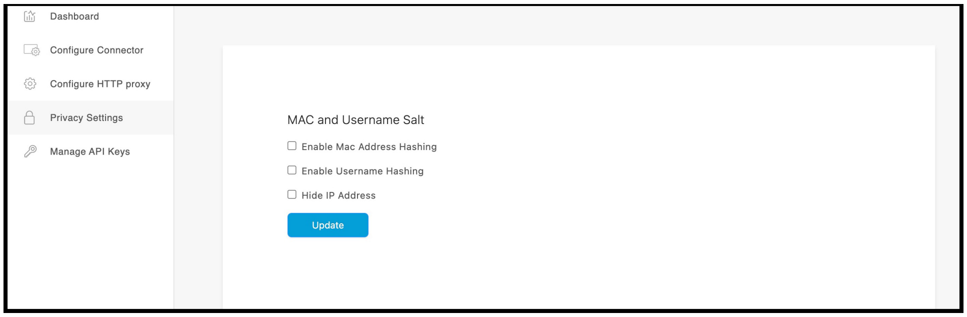
Connector provides a way to protect the Personal Identity Information (PII) of a user and maintain privacy. A hashing algorithm takes the user input (referred to as Salt) and masks the PII fields. When Cisco Spaces receives the data, the MAC addresses, IP addresses, or usernames are masked and the actual user information is protected.

Note This task is optional.

Procedure

From the Connector GUI left-navigation pane, choose **Privacy Settings**, enter the fields you want to secure with hashing, and press **Submit.**

Figure 133: Configure Privacy Settings



MAC and Username Salt

□ Enable Mac Address Hashing

□ Enable Username Hashing

□ Hide IP Address

After Cisco Spaces: Connector enables MAC address Salt, it reports pseudo MACs instead of physical device MACs in the data sent to Cisco Spaces cloud. On the Cloud application side, computed locations include the pseudo MACs and share them with applications such as Cisco Spaces: Detect and Locate and Cisco Catalyst Center.

Note

Mac salt cannot contain special characters other than **@** or **!**.

CHAPTER 12

Proxy

Configure a Proxy

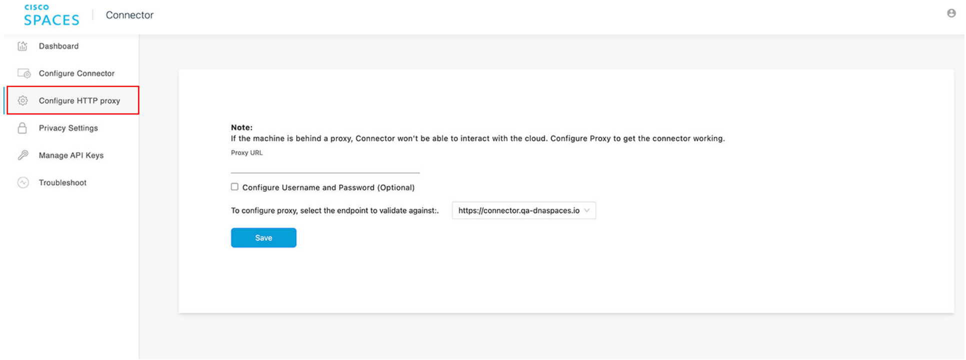
You can set up a proxy to connect the Connector to Cisco Spaces, if the infrastructure hosting the Connector is behind a proxy. Without this proxy configuration, the Connector is unable to communicate with Cisco Spaces

To configure proxy on the Connector, you must do the following:

Procedure

Step 1 In the Connector GUI left navigation pane, click **Configure HTTP Proxy**. Enter your proxy address in the dialog box that is displayed.

Figure 134: Setup Proxy



Note:
If the machine is behind a proxy, Connector won't be able to interact with the cloud. Configure Proxy to get the connector working.

Proxy URL

☐ Configure Username and Password (Optional)

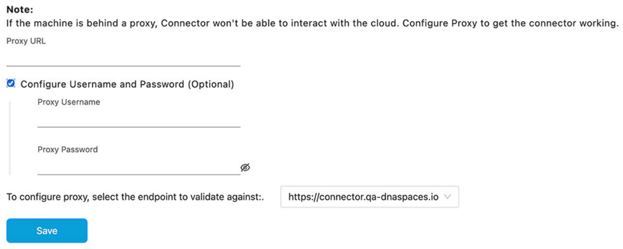
To configure proxy, select the endpoint to validate against:. https://connector.qa-dnaspaces.io

Save

Note

Choose the endpoint based on your Cisco Spaces Account. For information on how to choose endpoints, see the Table 2: Enable Endpoints, on page 5.

Figure 135: Configure Basic Authentication for Proxy (Optional)



Note:
If the machine is behind a proxy, Connector won't be able to interact with the cloud. Configure Proxy to get the connector working.

Proxy URL

☑ Configure Username and Password (Optional)

Proxy Username

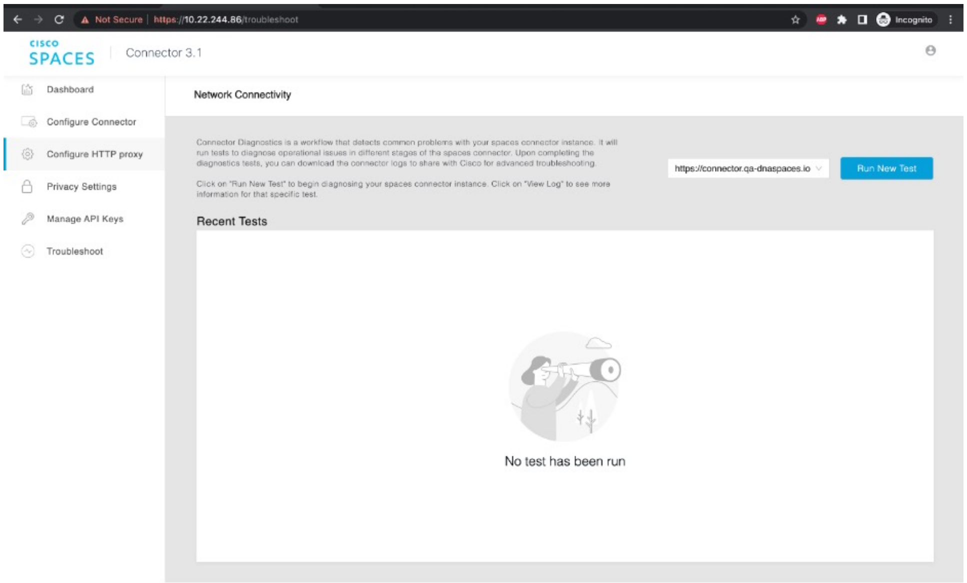
Proxy Password

To configure proxy, select the endpoint to validate against:. https://connector.qa-dnaspaces.io

To configure the proxy's basic authentication credentials, click **Configure Username and Password**.

Step 2 You can troubleshoot any issues in proxy configuration. Click **Troubleshoot** and select the Cisco Spaces URL.

Figure 136: Troubleshoot Proxy Issues



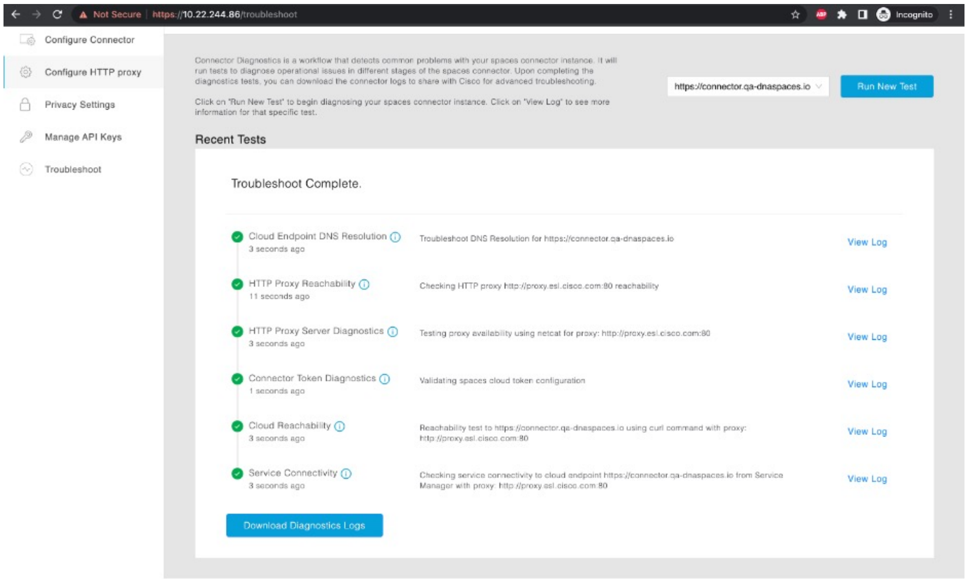
Connector Diagnostics is a workflow that detects common problems with your spaces connector instance. It will run tests to diagnose operational issues in different stages of the spaces connector. Upon completing the diagnostics tests, you can download the connector logs to share with Cisco for advanced troubleshooting.

Click on "Run New Test" to begin diagnosing your spaces connector instance. Click on "View Log" to see more information for that specific test.

https://connector.qa-dnaspaces.io

No test has been run

Figure 137: Sample Run Test Results



Connector Diagnostics is a workflow that detects common problems with your spaces connector instance. It will run tests to diagnose operational issues in different stages of the spaces connector. Upon completing the diagnostics tests, you can download the connector logs to share with Cisco for advanced troubleshooting.

Click on "Run New Test" to begin diagnosing your spaces connector instance. Click on "View Log" to see more information for that specific test.

Recent Tests

Troubleshoot Complete.

Cloud Endpoint DNS Resolution
3 seconds ago
Troubleshoot DNS Resolution for https://connector.qa-dnaspaces.io

HTTP Proxy Reachability
11 seconds ago
Checking HTTP proxy http://proxy.esl.cisco.com:80 reachability

HTTP Proxy Server Diagnostics
3 seconds ago
Testing proxy availability using netcat for proxy: http://proxy.esl.cisco.com:80

Connector Token Diagnostics
1 seconds ago
Validating spaces cloud token configuration

Cloud Reachability
3 seconds ago
Reachability test to https://connector.qa-dnaspaces.io using curl command with proxy: http://proxy.esl.cisco.com:80

Service Connectivity
3 seconds ago
Checking service connectivity to cloud endpoint https://connector.qa-dnaspaces.io from Service Manager with proxy: http://proxy.esl.cisco.com:80

Configure a Transparent Proxy

To configure a transparent proxy on the Connector, you must do the following:

1. Copy the proxy server certificate and the proxy server certification authority (CA) bundle to the Connector.
2. From the Connector CLI, validate the proxy certificate.
3. From the Connector CLI, import proxy certificates.
4. From the Connector GUI, configure the proxy URL.

Procedure

Step 1 Copy the proxy certificate to the Connector using scp.

The following is a sample command.

```
scp proxy-ca-bundle.pem spacesadmin@[connector-ip]:/home/spacesadmin/
scp proxy-server-cert.pem spacesadmin@[connector-ip]:/home/spacesadmin/
```

Step 2 Log in to the Connector CLI, and validate the copied proxy certificate using the **connectorctl cert validate** command.

The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectorctl cert validate -c /home/spacesadmin/proxy-ca-bundle.pem -s
/home/spacesadmin/proxy-server-cert.pem
Executing command:cert
Command execution status:Success
-----------------------
```

```
/home/spacesadmin/proxy-ca-bundle.pem and /home/spacesadmin/proxy-server-cert.pem exists
/home/spacesadmin/proxy-server-cert.pem: OK
Validation of certificate is successful
```

For more information on this command, see connectorctl cert validate.

Step 3 Import the proxy certification authority (CA) certificates along with other certificates using the **connectorctl cert updateca-bundle** command.

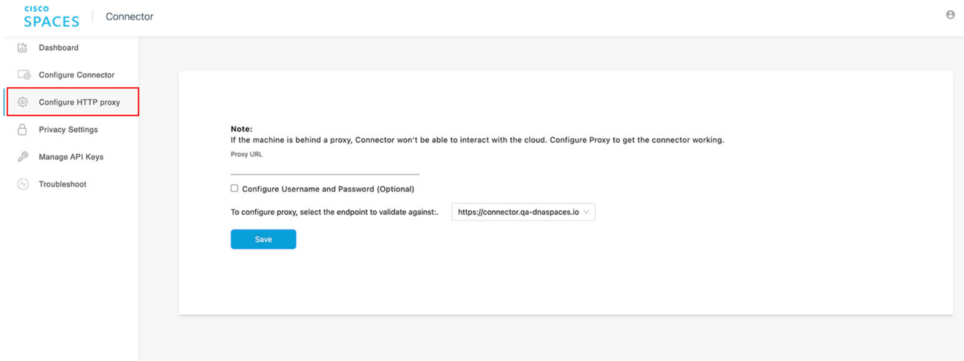
The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectorctl cert updateca-bundle -c /home/spacesadmin/proxy-ca-bundle.pem
 -s /home/spacesadmin/proxy-server-cert.pem
Executing command:cert
Command execution status:Success
-----------------------
/home/spacesadmin/proxy-ca-bundle.pem and /home/spacesadmin/proxy-server-cert.pem exist
/home/spacesadmin/proxy-server-cert.pem: OK
CA trust bundle updated successfully
System reboot will happen in 10 seconds. Do not execute any other command.
```

For more information on this command, see connectorctl cert updateca-bundle.

Step 4 In the Connector GUI left navigation pane, click **Configure HTTP Proxy**. Enter your proxy address in the dialog box that is displayed.

Figure 138: Setup Proxy



Note:
If the machine is behind a proxy, Connector won't be able to interact with the cloud. Configure Proxy to get the connector working.

Proxy URL

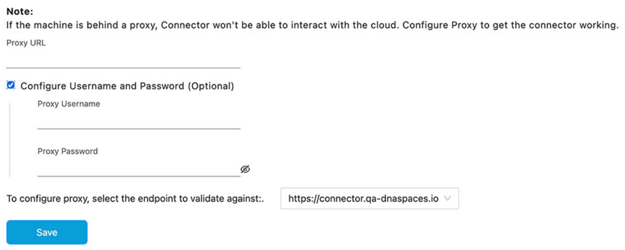
☐ Configure Username and Password (Optional)

To configure proxy, select the endpoint to validate against:. https://connector.qa-dnaspaces.io

Note

Choose the endpoint based on your Cisco Spaces Account. For information on how to choose endpoints, see the Table 2: Enable Endpoints, on page 5.

Figure 139: Configure Basic Authentication for Proxy (Optional)



Note:
If the machine is behind a proxy, Connector won't be able to interact with the cloud. Configure Proxy to get the connector working.

Proxy URL

☑ Configure Username and Password (Optional)

Proxy Username

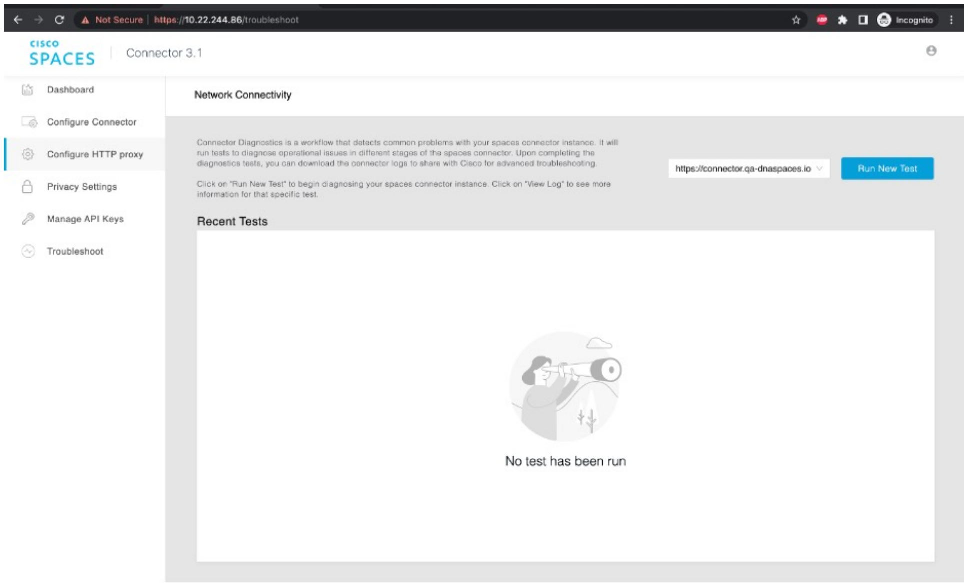
Proxy Password

To configure proxy, select the endpoint to validate against:. https://connector.qa-dnaspaces.io

To configure the proxy's basic authentication credentials, click **Configure Username and Password**.

Step 5 You can troubleshoot any issues in proxy configuration. Click **Troubleshoot** and enter the Cisco Spaces URL.

Figure 140: Troubleshoot Proxy Issues



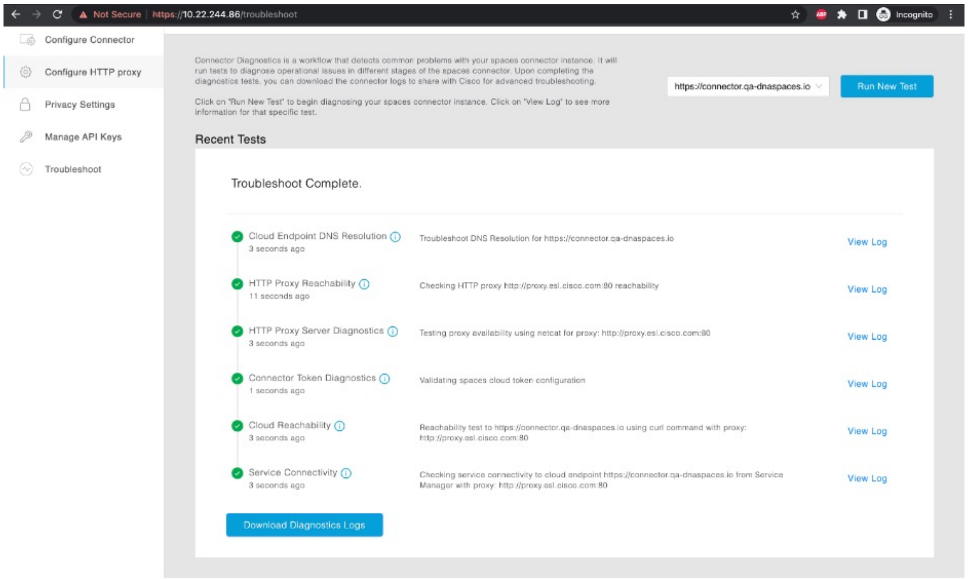
Connector Diagnostics is a workflow that detects common problems with your spaces connector instance. It will run tests to diagnose operational issues in different stages of the spaces connector. Upon completing the diagnostics tests, you can download the connector logs to share with Cisco for advanced troubleshooting.

Click on "Run New Test" to begin diagnosing your spaces connector instance. Click on "View Log" to see more information for that specific test.

Recent Tests

No test has been run

Figure 141: Sample Run Test Results



Connector Diagnostics is a workflow that detects common problems with your spaces connector instance. It will run tests to diagnose operational issues in different stages of the spaces connector. Upon completing the diagnostics tests, you can download the connector logs to share with Cisco for advanced troubleshooting.

Click on "Run New Test" to begin diagnosing your spaces connector instance. Click on "View Log" to see more information for that specific test.

Recent Tests

Troubleshoot Complete.

✓ Cloud Endpoint DNS Resolution ⓘ 3 seconds ago	Troubleshoot DNS Resolution for https://connector.qa-dnaspaces.io	View Log
✓ HTTP Proxy Reachability ⓘ 11 seconds ago	Checking HTTP proxy http://proxy.esl.cisco.com:80 reachability	View Log
✓ HTTP Proxy Server Diagnostics ⓘ 3 seconds ago	Testing proxy availability using netcat for proxy: http://proxy.esl.cisco.com:80	View Log
✓ Connector Token Diagnostics ⓘ 1 seconds ago	Validating spaces cloud token configuration	View Log
✓ Cloud Reachability ⓘ 3 seconds ago	Reachability test to https://connector.qa-dnaspaces.io using curl command with proxy: http://proxy.esl.cisco.com:80	View Log
✓ Service Connectivity ⓘ 3 seconds ago	Checking service connectivity to cloud endpoint https://connector.qa-dnaspaces.io from Service Manager with proxy: http://proxy.esl.cisco.com:80	View Log

CHAPTER 13

High Availability

Configuring Connectors as VIP Paired

Cisco Spaces: Connector high availability uses Virtual Router Redundancy Protocol (VRRP) protocol to determine the state of the instance in the high availability pair. When using VIP pairing with connector 3 and deploying firewalls between the connectors, it's crucial to enable the Virtual Router Redundancy Protocol (VRRP) IP protocol 112.

Ensure that both the source and destination IP addresses match the physical IPs of the connectors. Additionally, to enable proper VRRP functionality, ensure that both connectors reside within the same layer 2 or VLAN segment.

This task shows you how to configure two connectors and pair them with a virtual IP address (VIP).

Note

- Cisco Spaces: Connector in Amazon Web Services (AWS) and Azure Cloud does not support High Availability in the VIP Paired mode.

Before you begin

Install two different Cisco Spaces: Connectors. Configure each connector with a unique IP address.

Note Cisco Spaces: Connector High Availability utilizes HTTPS to assess the status of its peer. When implementing VIP pairing with connector 3 and deploying firewalls between the connectors, ensure that HTTPS TCP port 443 is permitted in both directions.

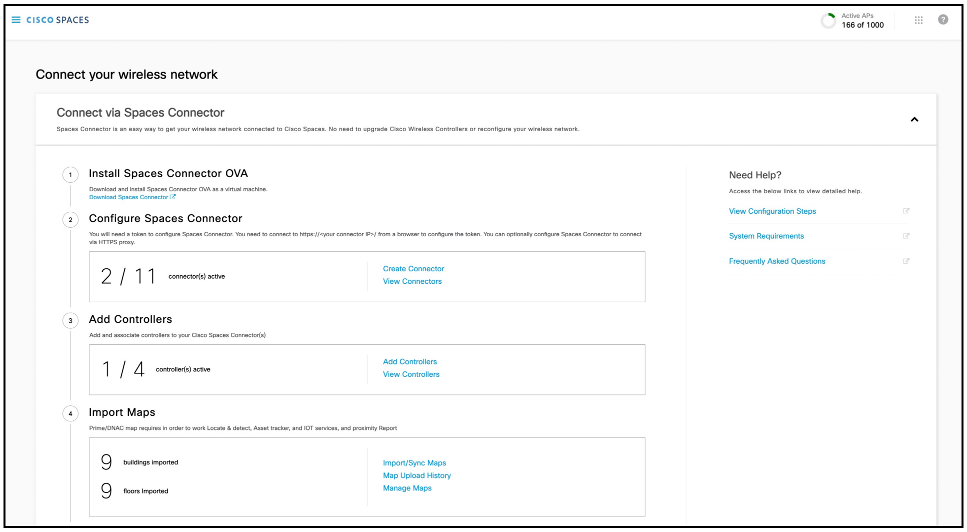
Table 4: HTTPS TCP port 443 connections

Source TCP ephemeral	Destination TCP 443
Connector IP 1	Connector IP 2
Connector IP 2	Connector IP 1

Procedure

Step 1 Login to **Cisco Spaces** > **Setup** > **Wireless Networks** and in the **Configure Spaces Connector** area, click **Create Connector**.

Figure 142: Create Connector



Connect your wireless network

Connect via Spaces Connector

Spaces Connector is an easy way to get your wireless network connected to Cisco Spaces. No need to upgrade Cisco Wireless Controllers or reconfigure your wireless network.

1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

2 / 11 connector(s) active

3 Add Controllers

Add and associate controllers to your Cisco Spaces Connector(s)

1 / 4 controller(s) active

4 Import Maps

Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

9 buildings imported

9 floors Imported

Need Help?

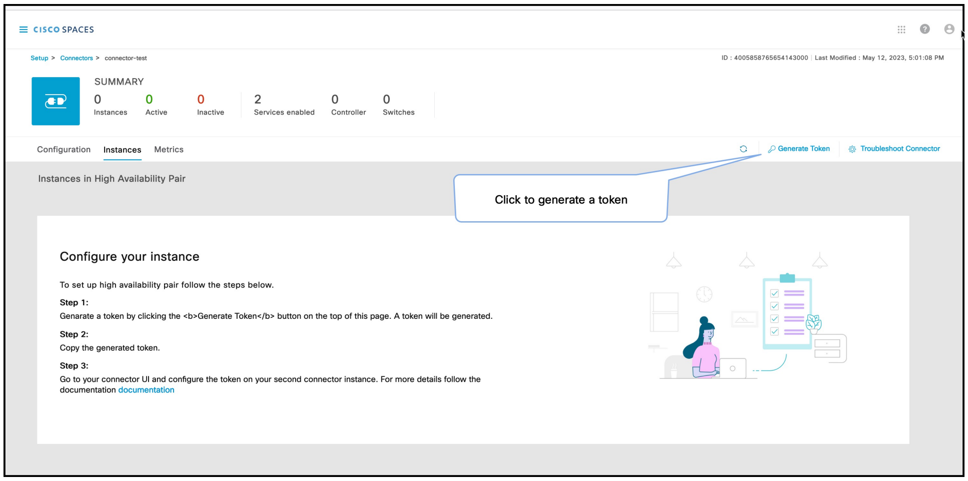
Access the below links to view detailed help.

Step 2 Enter a name for the connector and choose the version.

A connector is created. Click **Go to the connector Details** page.

Step 3 In the connector details page, click **Generate Token** in the top-right corner.

Figure 143: Generate Token



Setup > Connectors > connector-test

ID : 4005858765654143000 | Last Modified : May 12, 2023, 5:01:08 PM

SUMMARY

0	0	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

Instances in High Availability Pair

Click to generate a token

Configure your instance

To set up high availability pair follow the steps below.

Step 1:
Genarate a token by clicking the <b>Generate Token</b> button on the top of this page. A token will be generated.

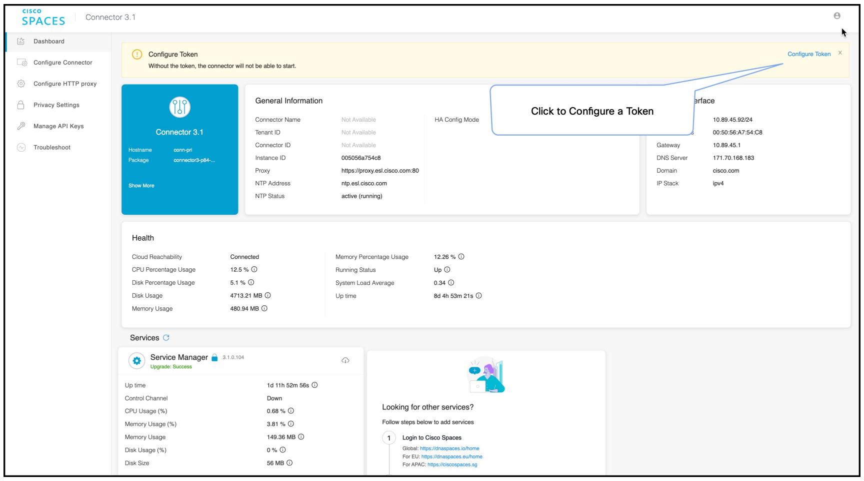
Step 2:
Copy the generated token.

Step 3:
Go to your connector UI and configure the token on your second connector instance. For more details follow the documentation documentation

Copy the displayed token.

Step 4 Log in to the GUI of the first instance of connector and click **Configure Token** in the top-right corner to provision the first copied token there.

Figure 144: Configure a Token



Configure Token
Without the token, the connector will not be able to start.

Click to Configure a Token

Connector 3.1

Hostname	conn-pri
Package	connector3-p84-...

General Information

Connector Name	Not Available	HA Config Mode
Tenant ID	Not Available	
Connector ID	Not Available	
Instance ID	005056a754c8	
Proxy	https://proxy.esl.cisco.com:80	
NTP Address	ntp.esl.cisco.com	
NTP Status	active (running)	

erface

	10.89.45.92/24
s	00:50:56:A7:54:C8
Gateway	10.89.45.1
DNS Server	171.70.168.183
Domain	cisco.com
IP Stack	ipv4

Health

Cloud Reachability	Connected	Memory Percentage Usage	12.26 %
CPU Percentage Usage	12.5 %	Running Status	Up
Disk Percentage Usage	5.1 %	System Load Average	0.34
Disk Usage	4713.21 MB	Up time	8d 4h 53m 21s
Memory Usage	480.94 MB		

Services

Service Manager 3.1.0.104
Upgrade: Success

Up time	1d 11h 52m 56s
Control Channel	Down
CPU Usage (%)	0.68 %
Memory Usage (%)	3.81 %
Memory Usage	149.36 MB
Disk Usage (%)	0 %
Disk Size	56 MB

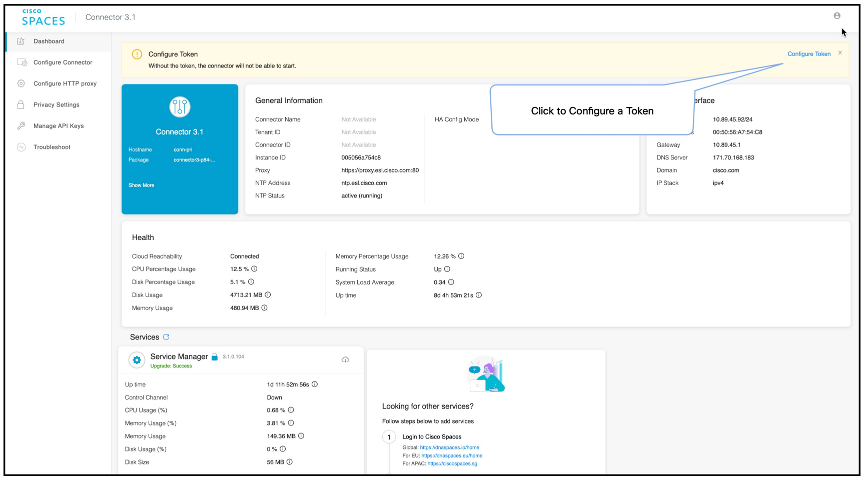
Looking for other services?

Follow steps below to add services

1 Login to Cisco Spaces
Global: https://dnaspaces.io/home
For EU: https://dnaspaces.eu/home
For APAC: https://ciscospaces.sg

Step 5 Log in to the GUI of the second instance of connector, and click **Configure Token** in the top-right corner to provision the second copied token there as well.

Figure 145: Configure a Token



Configure Token
Without the token, the connector will not be able to start.

Connector 3.1

Hostname	conn-pri
Package	connector3-p84-...

General Information

Connector Name	Not Available
Tenant ID	Not Available
Connector ID	Not Available
Instance ID	005056a754c8
Proxy	https://proxy.esl.cisco.com:80
NTP Address	ntp.esl.cisco.com
NTP Status	active (running)

HA Config Mode

erface

	10.89.45.92/24
	00:50:56:A7:54:C8
Gateway	10.89.45.1
DNS Server	171.70.168.183
Domain	cisco.com
IP Stack	ipv4

Health

Cloud Reachability	Connected	Memory Percentage Usage	12.26 %
CPU Percentage Usage	12.5 %	Running Status	Up
Disk Percentage Usage	5.1 %	System Load Average	0.34
Disk Usage	4713.21 MB	Up time	8d 4h 53m 21s
Memory Usage	480.94 MB		

Services

Service Manager 3.1.0.104
Upgrade: Success

Up time	1d 11h 52m 56s
Control Channel	Down
CPU Usage (%)	0.68 %
Memory Usage (%)	3.81 %
Memory Usage	149.36 MB
Disk Usage (%)	0 %
Disk Size	56 MB

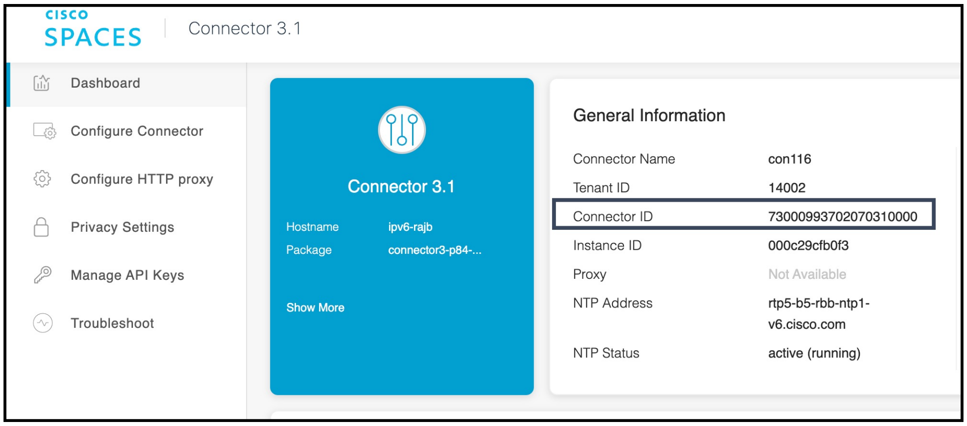
Looking for other services?
Follow steps below to add services

1 Login to Cisco Spaces
Global: https://dnaspaces.io/home
For EU: https://dnaspaces.eu/home
For APAC: https://ciscospaces.sg

Two tokens have been configured on two connector instances. You can observe that the connector ID on each instance of the connector is the same

Step 6 On each instance of the connector, observe that the value of the connector ID is the same.

Figure 146: Observe connector ID



Connector 3.1

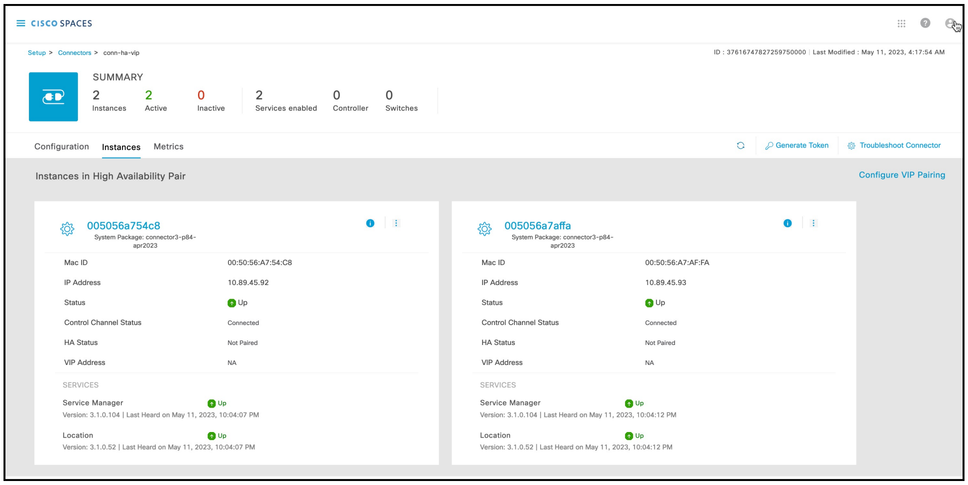
Hostname	ipv6-rajb
Package	connector3-p84-...

General Information

Connector Name	con116
Tenant ID	14002
Connector ID	73000993702070310000
Instance ID	000c29cfb0f3
Proxy	Not Available
NTP Address	rtp5-b5-rbb-ntp1-v6.cisco.com
NTP Status	active (running)

Step 7 On the Cisco Spaces dashboard, go back to the connector details page, and click the **Instances** tab. Here, you can see both the connectors that you configured. Observe that the connector IP addresses are reflected here.

Figure 147: Cisco Spaces dashboard



CISCO SPACES

Setup > Connectors > conn-ha-vip

ID : 37616747827259750000 | Last Modified : May 11, 2023, 4:17:54 AM

SUMMARY

2	2	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

Configuration | Instances | Metrics

Generate Token | Troubleshoot Connector

Instances in High Availability Pair

Configure VIP Pairing

005056a754c8
System Package: connector3-p84-apr2023

Mac ID	00:50:56:A7:54:C8
IP Address	10.89.45.92
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

SERVICES

Service Manager Up
Version: 3.1.0.104 | Last Heard on May 11, 2023, 10:04:07 PM

Location Up
Version: 3.1.0.52 | Last Heard on May 11, 2023, 10:04:07 PM

005056a7affa
System Package: connector3-p84-apr2023

Mac ID	00:50:56:A7:AF:FA
IP Address	10.89.45.93
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

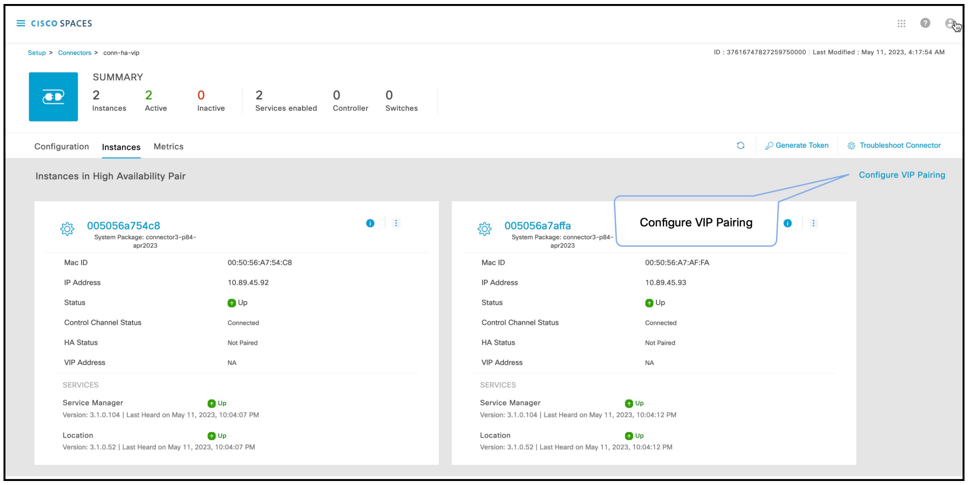
SERVICES

Service Manager Up
Version: 3.1.0.104 | Last Heard on May 11, 2023, 10:04:12 PM

Location Up
Version: 3.1.0.52 | Last Heard on May 11, 2023, 10:04:12 PM

The two connectors are now configured as an active-active pair.

Step 8 To configure the two connector instances as VIP-Paired, click **Configure VIP Pairing** in the top-right corner.



CISCO SPACES

Setup > Connectors > conn-ha-vip

ID : 37616747827259750000 | Last Modified : May 11, 2023, 4:17:54 AM

SUMMARY

2	2	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

Configuration | Instances | Metrics

Generate Token | Troubleshoot Connector

Instances in High Availability Pair

Configure VIP Pairing

005056a754c8
System Package: connector3-p84-apr2023

Mac ID	00:50:56:A7:54:C8
IP Address	10.89.45.92
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

SERVICES

Service Manager Up
Version: 3.1.0.104 | Last Heard on May 11, 2023, 10:04:07 PM

Location Up
Version: 3.1.0.52 | Last Heard on May 11, 2023, 10:04:07 PM

005056a7affa
System Package: connector3-p84-apr2023

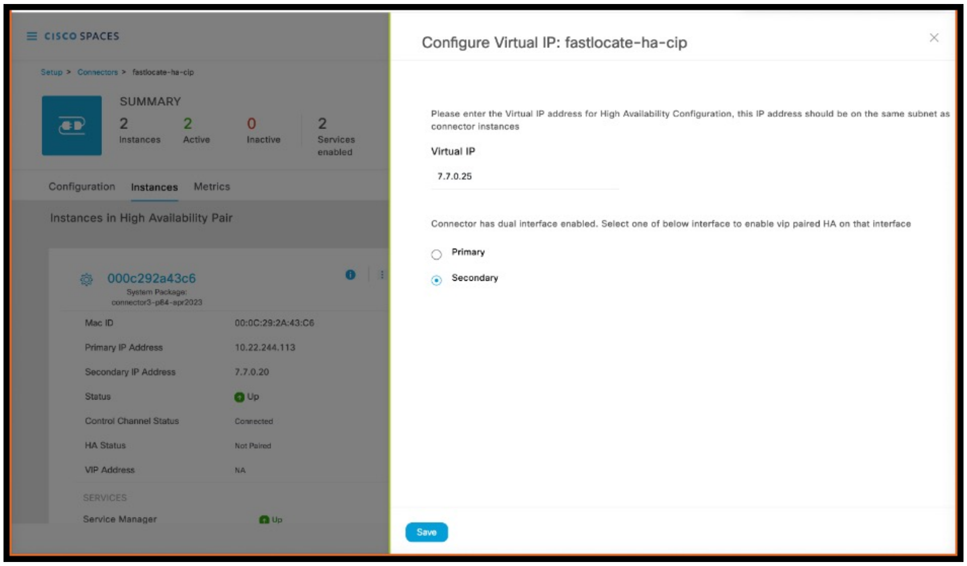
Mac ID	00:50:56:A7:AF:FA
IP Address	10.89.45.93
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

SERVICES

Service Manager Up
Version: 3.1.0.104 | Last Heard on May 11, 2023, 10:04:12 PM

Location Up
Version: 3.1.0.52 | Last Heard on May 11, 2023, 10:04:12 PM

Step 9 In the **Configure Virtual IP** popup that is displayed, enter the Virtual IP address (VIP). If the connector has dual interface enabled, you have to chose which interface would be used VIP pairing.



CISCO SPACES

Setup > Connectors > fastlocate-ha-cip

SUMMARY

2	2	0	2
Instances	Active	Inactive	Services enabled

Configuration | Instances | Metrics

Instances in High Availability Pair

000c292a43c6
System Package:
connector3-p84-apr2023

Mac ID	00:0C:29:2A:43:C6
Primary IP Address	10.22.244.113
Secondary IP Address	7.7.0.20
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

SERVICES

Service Manager Up

Configure Virtual IP: fastlocate-ha-cip

Please enter the Virtual IP address for High Availability Configuration, this IP address should be on the same subnet as connector instances

Virtual IP: 7.7.0.25

Connector has dual interface enabled. Select one of below interface to enable vip paired HA on that interface

○ Primary

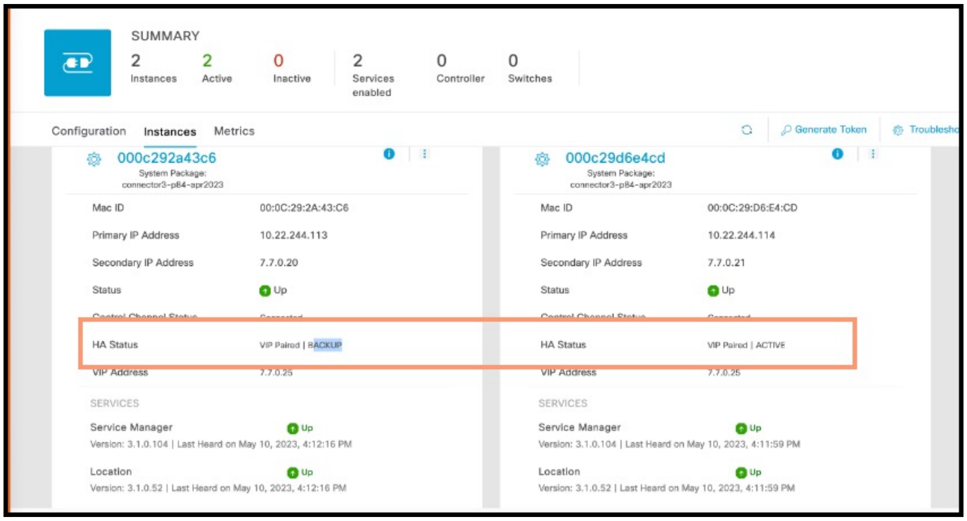
● Secondary

Save

Note

- Ensure that the VIP is in the same subnet as the connector IP address.
- If you have dual-interface connector, then VIP should be from the subnet of the secondary interface.

You can now see that the instances are configured as a VIP pair.



SUMMARY

2	2	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

Configuration | Instances | Metrics

Generate Token | Troublesho

	000c292a43c6 System Package: connector3-p84-apr2023		000c29d6e4cd System Package: connector3-p84-apr2023
Mac ID	00:0C:29:2A:43:C6	Mac ID	00:0C:29:D6:E4:CD
Primary IP Address	10.22.244.113	Primary IP Address	10.22.244.114
Secondary IP Address	7.7.0.20	Secondary IP Address	7.7.0.21
Status	Up	Status	Up
Control Channel Status	Connected	Control Channel Status	Connected
HA Status	VIP Paired | BACKUP	HA Status	VIP Paired | ACTIVE
VIP Address	7.7.0.25	VIP Address	7.7.0.25
SERVICES		SERVICES	
Service Manager Version: 3.1.0.104 | Last Heard on May 10, 2023, 4:12:16 PM	Up	Service Manager Version: 3.1.0.104 | Last Heard on May 10, 2023, 4:11:59 PM	Up
Location Version: 3.1.0.52 | Last Heard on May 10, 2023, 4:12:16 PM	Up	Location Version: 3.1.0.52 | Last Heard on May 10, 2023, 4:11:59 PM	Up

Connector Active-Active

You can pair two Cisco Spaces: Connectors in an active-active mode to enable the uninterrupted flow of data to Cisco Spaces.

1. You have to generate two tokens on Cisco Spaces and configure these token on two different connector instances. Each connector instance must have a unique IP address.
2. Both connectors receive configurations from Cisco Spaces .
3. The connectors can then connect to devices and send data back to Cisco Spaces.
4. Cisco Spaces then manages the redundant data.
5. If one connector is down, the other connector continues to send data.

Restrictions for Active-Active

- On the Cisco Spaces dashboard, there is no configuration required for two Connectors to be an active-active pair.
- Both Connectors connect to all Wireless Controllers and send traffic to Cisco Spaces. The traffic from Wireless Controllers to Cisco Spaces hence increases.
- To be an active-active Connector pair, two connectors must run OVA version 3.0 or higher.
- There is no failover support for Hyperlocation.

Note

- Cisco FastLocate is re-established after failover with a delay of three to four minutes.
- Reprovision services after a failover for active-active. For VIP-paired mode, re-provisioning is unnecessary.

- There is no support for monitoring the Connector active-active feature.
- You cannot run IoT Service high availability in Active - Active mode. To run IoT Service high availability, use VIP-paired mode.

Configuring Connectors in Active-Active

This task shows you how to configure two connectors as active-active.

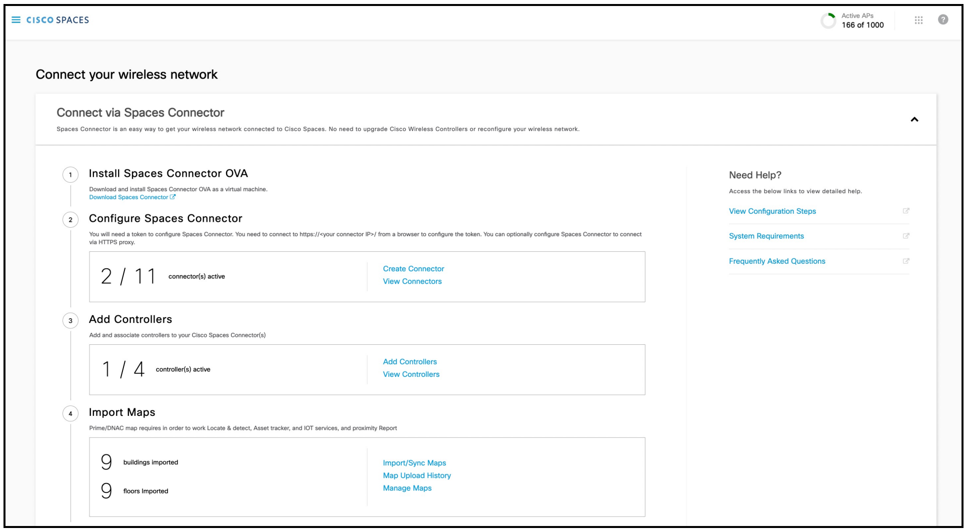
Before you begin

Install two different instances of Cisco Spaces: Connectors of OVA version 3.0 or higher. Configure each instance of connector with a unique IP address.

Procedure

Step 1 Login to **Cisco Spaces** > **Setup** > **Wireless Networks** and in the **Configure Spaces Connector** area, click **Create Connector**.

Figure 148: Create Connector



Connect your wireless network

Connect via Spaces Connector

Spaces Connector is an easy way to get your wireless network connected to Cisco Spaces. No need to upgrade Cisco Wireless Controllers or reconfigure your wireless network.

1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.
Download Spaces Connector

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

2 / 11 connector(s) active

Create Connector
View Connectors

3 Add Controllers

Add and associate controllers to your Cisco Spaces Connector(s)

1 / 4 controller(s) active

Add Controllers
View Controllers

4 Import Maps

Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

9 buildings imported
9 floors Imported

Import/Sync Maps
Map Upload History
Manage Maps

Need Help?

Access the below links to view detailed help.

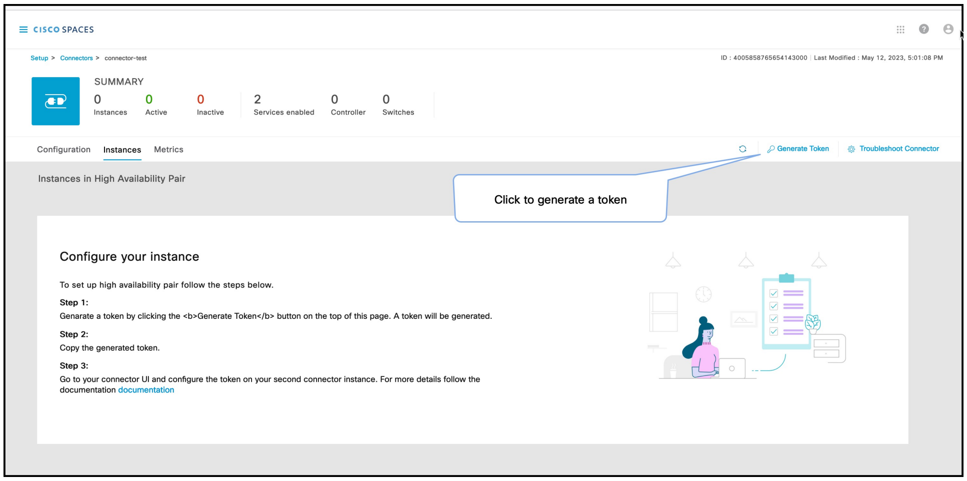
View Configuration Steps
System Requirements
Frequently Asked Questions

Step 2 Enter a name for the connector and choose the version.

A connector is created. Click **Go to the connector Details** page.

Step 3 In the connector details page, click **Generate Token** in the top-right corner.

Figure 149: Generate Token



ID : 4005858765654143000 | Last Modified : May 12, 2023, 5:01:08 PM

SUMMARY

0	0	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

Instances in High Availability Pair

Configure your instance

To set up high availability pair follow the steps below.

Step 1:
Genarate a token by clicking the <b>Generate Token</b> button on the top of this page. A token will be generated.

Step 2:
Copy the generated token.

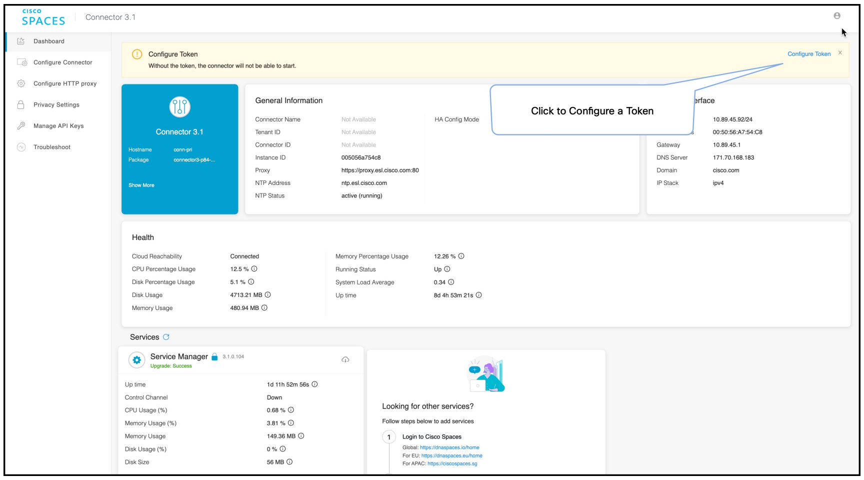
Step 3:
Go to your connector UI and configure the token on your second connector instance. For more details follow the documentation documentation

Copy the displayed token.

Step 4 Repeat Step 3 to generate and copy a second token.

Step 5 Log in to the GUI of the first instance of connector and click **Configure Token** in the top-right corner to provision the first copied token there.

Figure 150: Configure a Token



Configure Token
Without the token, the connector will not be able to start.

Connector 3.1

Hostname conn-pri
Package connector3-p84-...

General Information

Connector Name	Not Available
Tenant ID	Not Available
Connector ID	Not Available
Instance ID	005056a754c8
Proxy	https://proxy.esl.cisco.com:80
NTP Address	ntp.esl.cisco.com
NTP Status	active (running)
HA Config Mode	

erface

	10.89.45.92/24
s	00:50:56:A7:54:C8
Gateway	10.89.45.1
DNS Server	171.70.168.183
Domain	cisco.com
IP Stack	ipv4

Health

Cloud Reachability	Connected	Memory Percentage Usage	12.26 % ⓘ
CPU Percentage Usage	12.5 % ⓘ	Running Status	Up ⓘ
Disk Percentage Usage	5.1 % ⓘ	System Load Average	0.34 ⓘ
Disk Usage	4713.21 MB ⓘ	Up time	8d 4h 53m 21s ⓘ
Memory Usage	480.94 MB ⓘ		

Service Manager 3.1.0.104
Upgrade: Success

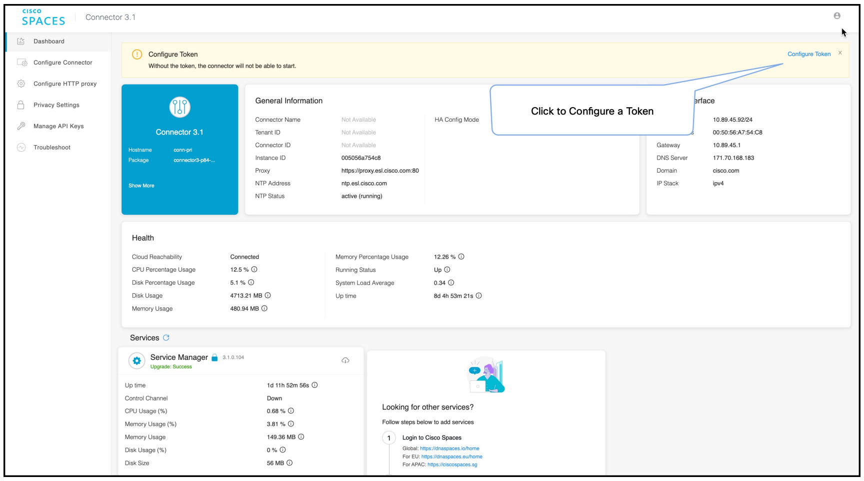
Up time	1d 11h 52m 56s ⓘ
Control Channel	Down
CPU Usage (%)	0.68 % ⓘ
Memory Usage (%)	3.81 % ⓘ
Memory Usage	149.36 MB ⓘ
Disk Usage (%)	0 % ⓘ
Disk Size	56 MB ⓘ

Follow steps below to add services

1 Login to Cisco Spaces
Global: https://dnaspaces.io/home
For EU: https://dnaspaces.eu/home
For APAC: https://ciscospaces.sg

Step 6 Log in to the GUI of the second instance of connector, and click **Configure Token** in the top-right corner to provision the second copied token there as well.

Figure 151: Configure a Token



Configure Token
Without the token, the connector will not be able to start.

Connector 3.1

Hostname conn-pri
Package connector3-p84-...

General Information

Connector Name	Not Available
Tenant ID	Not Available
Connector ID	Not Available
Instance ID	005056a754c8
Proxy	https://proxy.esl.cisco.com:80
NTP Address	ntp.esl.cisco.com
NTP Status	active (running)
HA Config Mode	

erface

	10.89.45.92/24
	00:50:56:A7:54:C8
Gateway	10.89.45.1
DNS Server	171.70.168.183
Domain	cisco.com
IP Stack	ipv4

Health

Cloud Reachability	Connected	Memory Percentage Usage	12.26 % ⓘ
CPU Percentage Usage	12.5 % ⓘ	Running Status	Up ⓘ
Disk Percentage Usage	5.1 % ⓘ	System Load Average	0.34 ⓘ
Disk Usage	4713.21 MB ⓘ	Up time	8d 4h 53m 21s ⓘ
Memory Usage	480.94 MB ⓘ		

Service Manager 3.1.0.104
Upgrade: Success

Up time	1d 11h 52m 56s ⓘ
Control Channel	Down
CPU Usage (%)	0.68 % ⓘ
Memory Usage (%)	3.81 % ⓘ
Memory Usage	149.36 MB ⓘ
Disk Usage (%)	0 % ⓘ
Disk Size	56 MB ⓘ

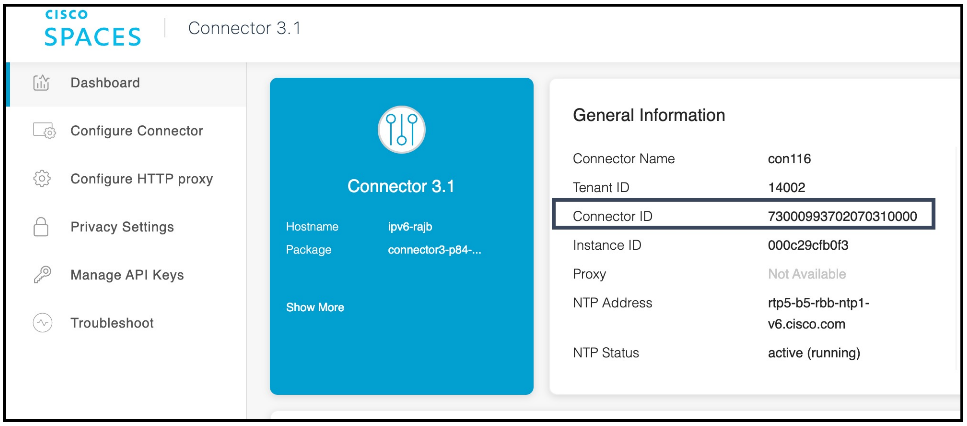
Follow steps below to add services

1 Login to Cisco Spaces
Global: https://dnaspaces.io/home
For EU: https://dnaspaces.eu/home
For APAC: https://ciscospaces.sg

Two tokens have been configured on two connector instances. You can observe that the connector ID on each instance of the connector is the same

Step 7 On each instance of the connector, observe that the value of the connector ID is the same.

Figure 152: Observe connector ID



Connector 3.1

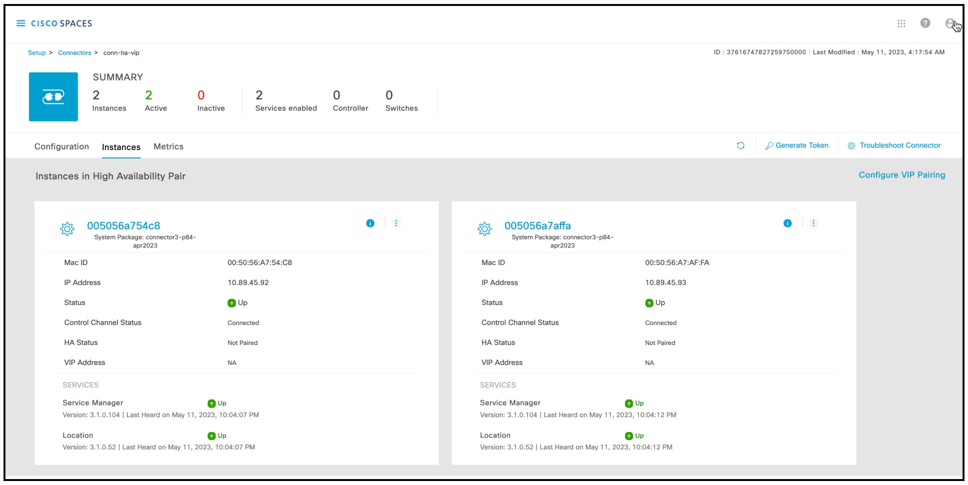
Hostname	ipv6-rajb
Package	connector3-p84-...

General Information

Connector Name	con116
Tenant ID	14002
Connector ID	73000993702070310000
Instance ID	000c29cfb0f3
Proxy	Not Available
NTP Address	rtp5-b5-rbb-ntp1-v6.cisco.com
NTP Status	active (running)

Step 8 On the Cisco Spaces dashboard, go back to the connector details page, and click the **Instances** tab. Here, you can see both the connectors that you configured. Observe that the connector IP addresses are reflected here.

Figure 153: Cisco Spaces dashboard



ID : 37616747827259750000 | Last Modified : May 11, 2023, 4:17:54 AM

SUMMARY

2	2	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

Instances in High Availability Pair

005056a754c8
System Package: connector3-p84-apr2023

Mac ID	00:50:56:A7:54:C8
IP Address	10.89.45.92
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

SERVICES

Service Manager Up
Version: 3.1.0.104 | Last Heard on May 11, 2023, 10:04:07 PM

Location Up
Version: 3.1.0.52 | Last Heard on May 11, 2023, 10:04:07 PM

005056a7affa
System Package: connector3-p84-apr2023

Mac ID	00:50:56:A7:AF:FA
IP Address	10.89.45.93
Status	Up
Control Channel Status	Connected
HA Status	Not Paired
VIP Address	NA

SERVICES

Service Manager Up
Version: 3.1.0.104 | Last Heard on May 11, 2023, 10:04:12 PM

Location Up
Version: 3.1.0.52 | Last Heard on May 11, 2023, 10:04:12 PM

The two connectors are now configured as an active-active pair.

CHAPTER 14

FIPS Support in Cisco Spaces

FIPS Overview

Cisco Spaces Connector supports the Federal Information Processing Standard 140-3 (FIPS). FIPS is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information meet these standards. If your system needs to be FIPS compliant, you can enable FIPS. Once you do so, the system uses the cryptographic algorithms defined by the NIST for FIPS for all encrypted communication between its internal and external components.

Protocol Requirements

- Transport Layer Security (TLS) 1.2or higher.
- Advanced Encryption Standard (AES) 256.
- Secure Hash Algorithm (SHA) 128 or higher.
- One of the following:
  - Rivest, Shamir, and Adelman (RSA) 2048 or higher.
- Elliptic Curve Digital Signature Algorithm (ECDSA) with a National Institute of Standards and Technology (NIST) curve of P-256 or higher.

Enabling FIPS

To enable FIPS on the Connector, you must do the following:

1. Log in to the Connector CLI, and enable FIPS on the connector.
2. From the Connector CLI, validate if the FIPS is enabled.

Procedure

Step 1 Log in to the Connector CLI, and enable FIPS on the connector using the **connectorctl fips enable** command.

The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectorctl fips enable
Executing command:fips
Terminated
[spacesadmin@connector ~]$ Connection to 10.22.244.2 closed by remote host
```

For more information on this command, see the **connectorctl fips enable** command page.

Note

Enabling FIPS restarts the connector VM.

Step 2 Validate if the FIPS is enabled using the **connectorctl fips show** command.

The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectorctl fips show
Executing command:fips
Command execution status:Success
----------------------
FIPS mode status:
FIPS mode is enabled.
verify FIPS mode is enabled at the operating system level:
crypto.fips_enabled = 1
OpenSSL version:
FIPS Toolkit Enabled
CiscoSSL 1.1.1y.7.3.377-fips
ssh runs in FIPS mode
x509v3-ecdsa-sha2-nistp256
x509v3-ecdsa-sha2-nistp384
x509v3-ecdsa-sha2-nistp521
x509v3-ssh-rsa
x509v3-rsa2048-sha256
ecdsa-sha2-nistp256
ecdsa-sha2-nistp256-cert-v01@openssh.com
ecdsa-sha2-nistp384
ecdsa-sha2-nistp384-cert-v01@openssh.com
ecdsa-sha2-nistp521
ecdsa-sha2-nistp521-cert-v01@openssh.com
ssh-rsa
ssh-rsa-cert-v01@openssh.com

[spacesadmin@connector ~]$
```

For more information on this command, see the **connectorctl fips show** command page.

Disabling FIPS

Note There is no option to disable FIPS. The only way is to roll back to the initial setup by resetting the connector using the **connectorctl reset** command.

To roll back to the initial setup, you must do the following:

1. Log in to the Connector CLI, and reset the connector.
2. From the Connector CLI, validate whether the roll back is successful.

Procedure

Step 1 Log in to the Connector CLI, and reset the connector using the **connectorctl reset** command.

The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectorctl reset
Executing command:reset
WARNING: This command resets all connector configuration including http proxy and token and bring
system to initial state. You can't undo these changes.
Type yes to continue or any other letter to abort:yes
Terminated
[spacesadmin@connector ~]$ Connection to 10.22.244.45 closed by remote host.
Connection to 10.22.244.45 closed.
```

For more information on this command, see the **connectorctl reset** command page.

Note
Rolling back to the initial setup restarts the connector VM.

Step 2 Validate whether the roll back is successful using the **connectorctl fips show** command.

The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectorctl fips show
Executing command:fips
Command execution status:Success
----------------------
FIPS mode status:
FIPS mode is disabled.
verify FIPS mode is enabled at the operating system level:
crypto.fips_enabled = 0
OpenSSL version:
FIPS Toolkit Enabled
CiscoSSL 1.1.1y.7.3.377-fips
ssh runs in FIPS mode
x509v3-ecdsa-sha2-nistp256
x509v3-ecdsa-sha2-nistp384
x509v3-ecdsa-sha2-nistp521
x509v3-ssh-rsa
x509v3-rsa2048-sha256
ecdsa-sha2-nistp256
ecdsa-sha2-nistp256-cert-v01@openssh.com
```

```
ecdsa-sha2-nistp384
ecdsa-sha2-nistp384-cert-v01@openssh.com
ecdsa-sha2-nistp521
ecdsa-sha2-nistp521-cert-v01@openssh.com
ssh-rsa
ssh-rsa-cert-v01@openssh.com
```

For more information on this command, see the **connectorctl fips show** command page.

Adding a FIPS-Enabled Catalyst 9800 Controller to a FIPS-Enabled Connector

Enabling FIPS

To enable FIPS on the Connector, you must do the following:

1. Log in to the Connector CLI, and enable FIPS on the connector.
2. From the Connector CLI, validate if the FIPS is enabled.

Procedure

Step 1 Log in to the Connector CLI, and enable FIPS on the connector using the **connectorctl fips enable** command.

The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectorctl fips enable
Executing command:fips
Terminated
[spacesadmin@connector ~]$ Connection to 10.22.244.2 closed by remote host
```

For more information on this command, see the **connectorctl fips enable** command page.

Note
Enabling FIPS restarts the connector VM.

Step 2 Validate if the FIPS is enabled using the **connectorctl fips show** command.

The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectorctl fips show
Executing command:fips
Command execution status:Success
----------------------
FIPS mode status:
FIPS mode is enabled.
verify FIPS mode is enabled at the operating system level:
crypto.fips_enabled = 1
OpenSSL version:
FIPS Toolkit Enabled
CiscoSSL 1.1.1y.7.3.377-fips
ssh runs in FIPS mode
```

```
x509v3-ecdsa-sha2-nistp256
x509v3-ecdsa-sha2-nistp384
x509v3-ecdsa-sha2-nistp521
x509v3-ssh-rsa
x509v3-rsa2048-sha256
ecdsa-sha2-nistp256
ecdsa-sha2-nistp256-cert-v01@openssh.com
ecdsa-sha2-nistp384
ecdsa-sha2-nistp384-cert-v01@openssh.com
ecdsa-sha2-nistp521
ecdsa-sha2-nistp521-cert-v01@openssh.com
ssh-rsa
ssh-rsa-cert-v01@openssh.com

[spacesadmin@connector ~]$
```

For more information on this command, see the **connectorctl fips show** command page.

Configuring FIPS Authorization Key in the Controller

Procedure

Step 1 Log in to the Catalyst 9800 controller CLI, and enter the global configuration mode using the **configure terminal** command.

The following is a sample output of the command:

```
Device# configure terminal
```

Step 2 Configuring FIPS authorization key on the controller using the **fips authorization-key** *hex* command.

The following is a sample output of the command:

```
Device(config)# fips authorization-key <hex>
```

Step 3 Return to the privileged **EXEC** mode using the **end** command.

The following is a sample output of the command:

```
Device(config)# end
```

Step 4 Save all configurations using the **write memory** command.

The following is a sample output of the command:

```
Device# write memory
```

Step 5 Boot the controller in FIPS mode using the **reload** command.

The following is a sample output of the command:

```
Device# reload
```

Obtaining a Certificate from the Connector

Procedure

Step 1 Log in to the Connector CLI, and obtain a certificate using the **connectorctl -s location keystore showcert -n fipsca** command.

The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectorctl -s location keystore showcert -n fipsca
Executing command:keystore
Command execution status:Success
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

Step 2 Copy the certificate and paste it into a text editor to add it to the controller trustpool. For information, see the Importing a CA Certificate to the Trustpool section.

Importing a CA Certificate into the Trustpool

Procedure

Step 1 Log in to the Catalyst 9800 controller CLI, and enter the global configuration mode using the **configure terminal** command.

The following is a sample output of the command:

```
Device# configure terminal
```

Step 2 Import a CA certificate into the Trustpool using the **crypto pki trustpool import terminal** command.

Paste the certificate and press **Enter**. For more information, see Obtaining a Certificate from the Connector.

The following is a sample output of the command:

```
Device(config)# crypto pki trustpool import terminal
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
line by itself.
-----BEGIN CERTIFICATE-----
....
....
-----END CERTIFICATE-----
quit
% PEM files import succeeded.
```

Step 3 Return to the privileged **EXEC** mode using the **end** command.

The following is a sample output of the command:

```
Device(config)# end
```

Step 4 Save all configurations using the **write memory** command.

The following is a sample output of the command:

```
Device# write memory
```

Reinitiating the NMSP Connection on the Controller

Perform one of the following actions to reinitiate the NMSP connection to the controller after importing the connector certificate into the controller:

Procedure

Step 1 Restart the location service from the Connector CLI or Cisco Spaces dashboard.

Step 2 Edit and save the controller credentials in the Cisco Spaces dashboard.

Note

- This will retrigger the SYNC message from the cloud to connector for all the controllers that are added.
- The connector attempts to reestablish the connection between the connector and the controller.
- If the NMSP handshake fails after importing the fipsca certificate into the controller, re-import the certificate. To clean any trustpool certificates imported earlier, use the **crypto pki trustpool import clean** command.

PART III

Troubleshooting

CHAPTER 15

Troubleshooting Tools

Enable Debug Logs

This task shows you how to enable debug logs for connector. The task also shows you how to upload these logs to Cisco Spaces, if necessary.

Note You can also enable debug log using the **connectorctl service restart** command.

Procedure

Step 1 Log in to **Cisco Spaces**.

Note
The Cisco Spaces URL is region-dependent.

Step 2 From the left navigation pane, choose **Setup** > **Wireless Networks**.

Step 3 In the **2. Configure Spaces Connector** area, click **View Connectors**.

Step 4 Click a connector from the list of connectors that are displayed.

Step 5 In the **SUMMARY** window that is displayed, click **Troubleshoot Connector**.

Step 6 In the **Troubleshoot Connector** window that is displayed, you can see that logs can be enabled by a service. Click the respective **Enable Debug Mode** of a service if not enabled already.

After being enabled, connector starts collecting debug logs for that service, and these logs are stored locally on connector.

Step 7 (Optional) To upload the logs to the Cisco Spaces dashboard, click **Upload Logs to Cloud.**

Recovering a Lost Password

This task shows you how to recover your connector GUI password.

Procedure

Step 1 Log in to **Cisco Spaces.**

Note
The Cisco Spaces URL is region-dependent.

Step 2 From the left navigation pane of the Cisco Spaces dashboard, choose **Setup** > **Wireless Networks**.

Step 3 In the **2. Configure Spaces Connector** area, click **View Connectors**.

Step 4 Click a connector from the list of connectors that are displayed.

Step 5 In the **SUMMARY** window that is displayed, click **Troubleshoot Connector**.

Step 6 In the **Troubleshoot Connector** window that is displayed, click **Password Reset Key** .

Step 7 In the **Password Reset Key** window that is displayed, click **Copy The Key**.
Save the copied key on a notepad.

Step 8 Open the connector GUI, and click **Forgot Password**.

Step 9 In the **Password Reset Key** field, enter the key copied in theprevious step.

Step 10 In the **New Password** field, enter a new password.

Monitor Service Metrics

You can monitor the various metrics of the different services that are installed on connector from the Cisco Spaces dashboard.

Procedure

Step 1 From the Cisco Spaces dashboard, navigate to **Setup** > **Wireless Networks**.

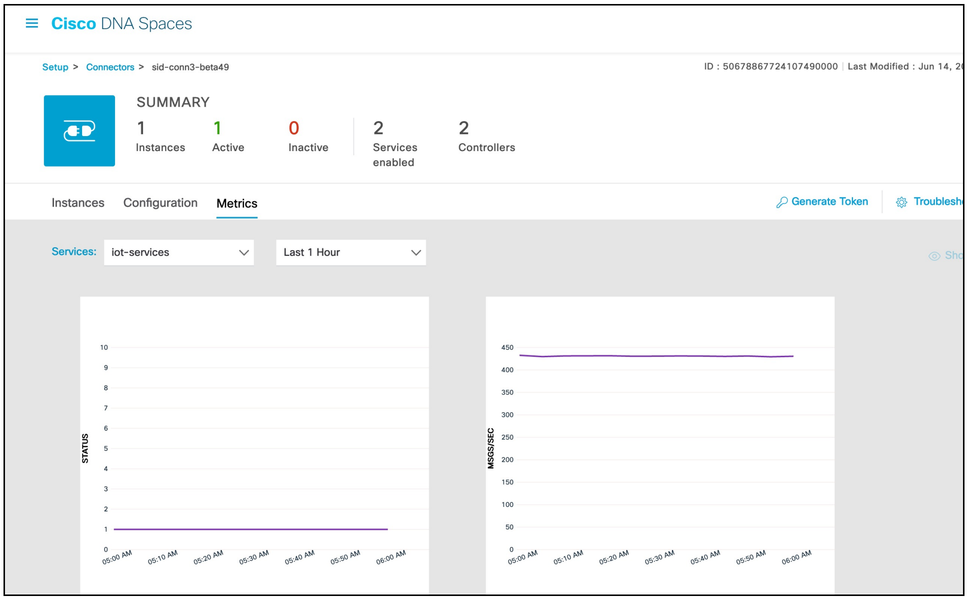
Step 2 In the **Connect via Spaces Connector** area titled **Step 2 Configure Spaces Connector**, click **View Connectors**.

Step 3 In the **Connectors** window that opens up, click a connector of your choice.

Step 4 In the connector details window that is displayed, click the **Metrics** tab.

Step 5 From the **Services** drop-down list, choose a service that is installed on this connector to observe the metrics that are related to the service. You can also choose the period for which the metrics is collected.

Figure 154: Observing Service Metrics



Setup > Connectors > sid-conn3-beta49

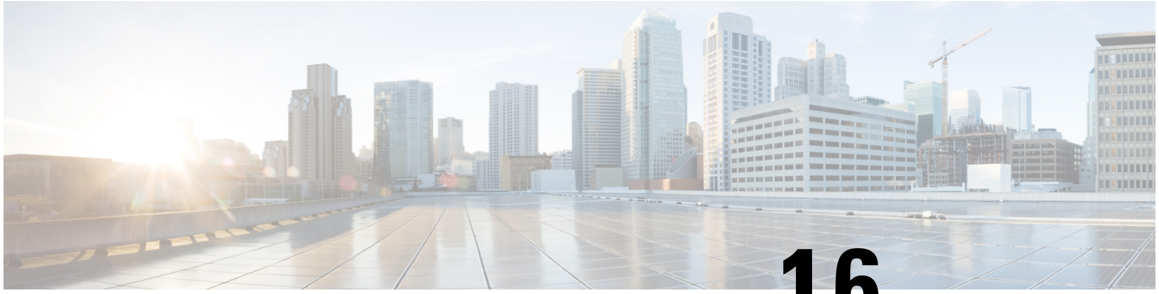
ID : 506788677241074900000 | Last Modified : Jun 14, 2

SUMMARY

1	1	0	2	2
Instances	Active	Inactive	Services enabled	Controllers

Services: iot-services

Last 1 Hour



CHAPTER 16

Troubleshooting Scenarios

Connectivity Issues Between Connector and Cisco Spaces

This task allows you to troubleshoot connectivity issues between your connector and Cisco Spaces. You can troubleshoot this connection both before and after the configuration of the connector token on Cisco Spaces.

Procedure

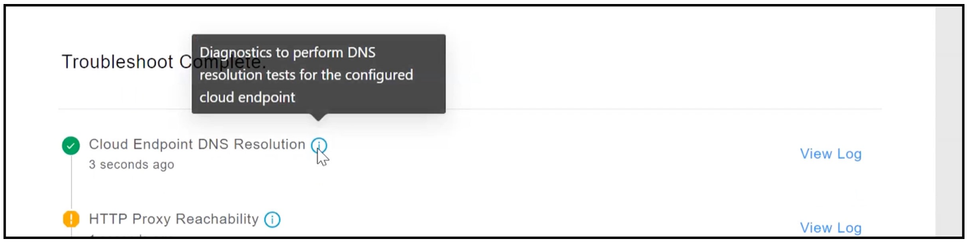
Step 1 Log in to the connector GUI.

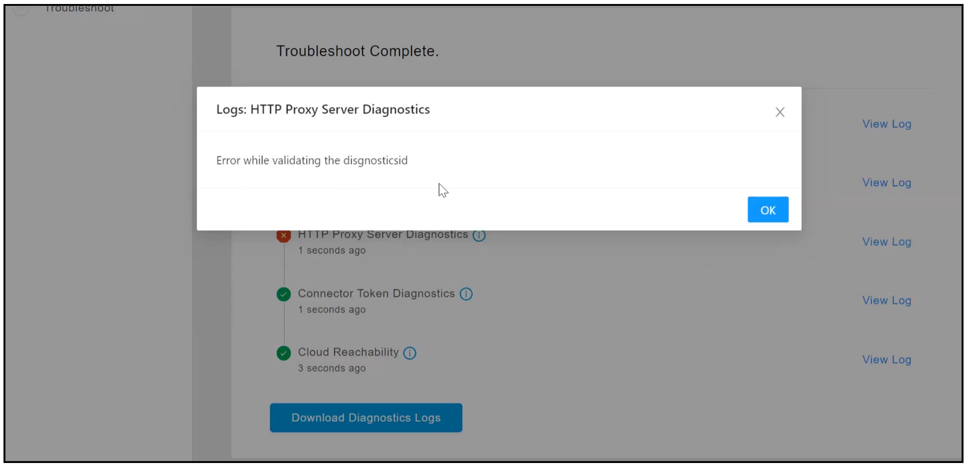
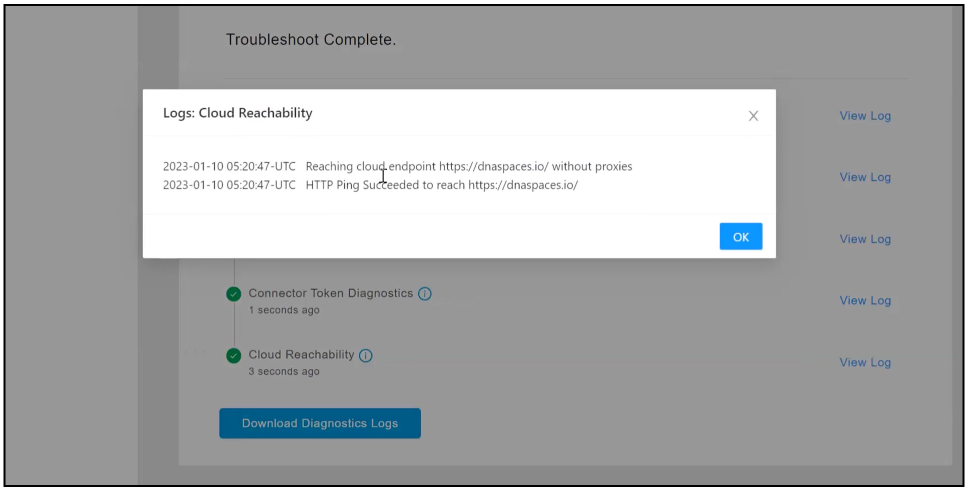
Step 2 In the connector left navigation pane, click **Troubleshoot** and do one of the following:

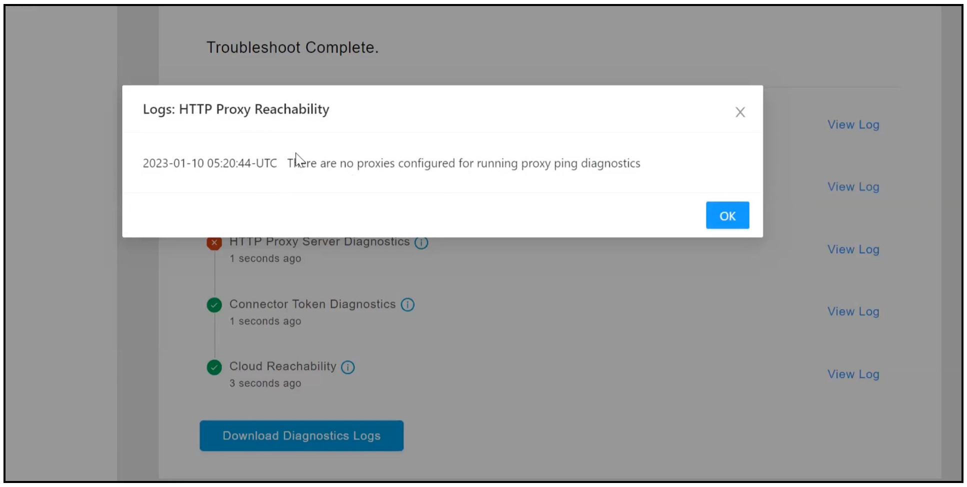
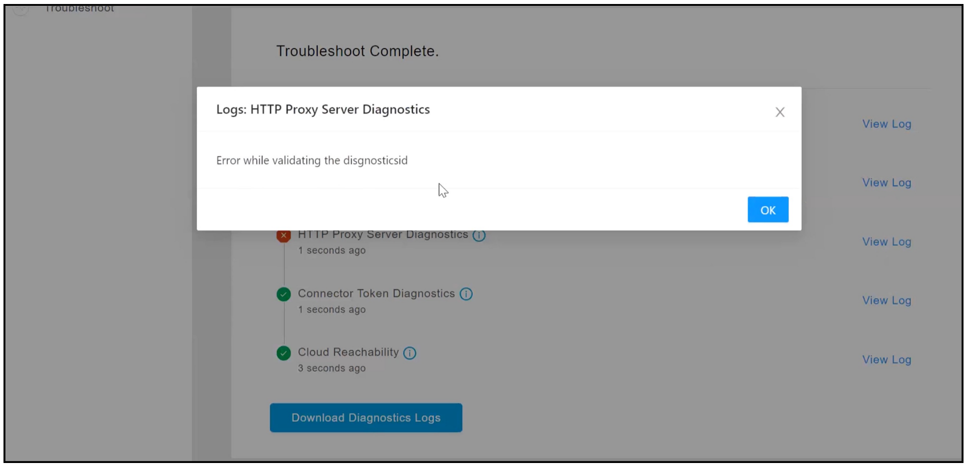
- If you have configured the token for this connector in Cisco Spaces, the text field beside the **Run New Test** button is automatically populated with the Cisco Spaces URL.
- If you have not configured the token for this connector on Cisco Spaces, then from the **Run New Test** drop-down, choose from one of the Cisco Spaces region-dependent URLs.

Step 3 Click **Run New Test** to initiate troubleshooting the connectivity.

Step 4 Observe the running tests for the following:

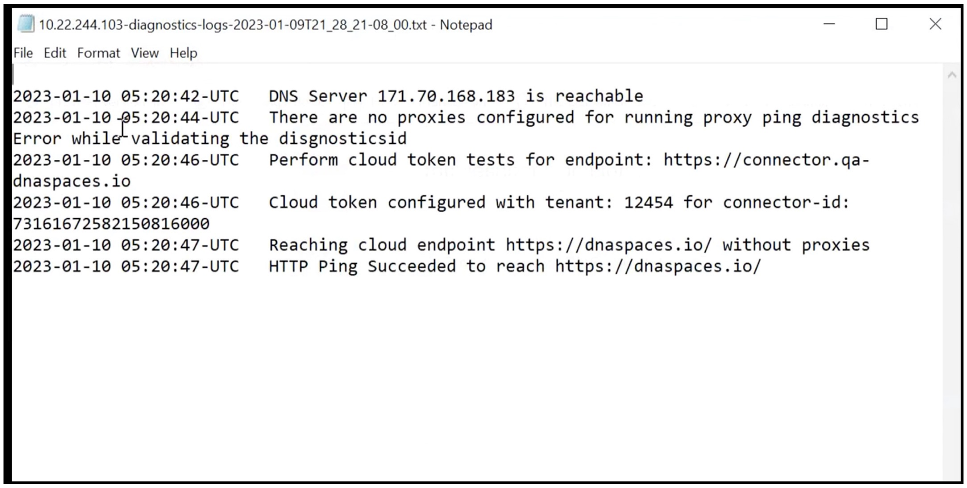
ⓘ	Click to view further information about the test.  Troubleshoot Complete. Diagnostics to perform DNS resolution tests for the configured cloud endpoint Cloud Endpoint DNS Resolution ⓘ 3 seconds ago View Log HTTP Proxy Reachability ⓘ View Log

	Click **View Logs** to view further information. *Figure 155: View Logs*  Troubleshoot Complete. Logs: HTTP Proxy Server Diagnostics Error while validating the disgnosticsid HTTP Proxy Server Diagnostics ⓘ 1 seconds ago Connector Token Diagnostics ⓘ 1 seconds ago Cloud Reachability ⓘ 3 seconds ago Troubleshoot OK View Log View Log View Log View Log View Log Download Diagnostics Logs
✓	Represents a successful test. Click ⓘ to view additional information about this successful test. *Figure 156: View Logs for a Successful Test*  Troubleshoot Complete. Logs: Cloud Reachability 2023-01-10 05:20:47-UTC Reaching cloud endpoint https://dnaspaces.io/ without proxies 2023-01-10 05:20:47-UTC HTTP Ping Succeeded to reach https://dnaspaces.io/ Connector Token Diagnostics ⓘ 1 seconds ago Cloud Reachability ⓘ 3 seconds ago OK View Log View Log View Log View Log View Log Download Diagnostics Logs

!	Represents a warning. Click ⓘ to view additional information about this warning. ***Figure 157: View Logs for a Warning***  Troubleshoot Complete. Logs: HTTP Proxy Reachability 2023-01-10 05:20:44-UTC There are no proxies configured for running proxy ping diagnostics OK HTTP Proxy Server Diagnostics ⓘ 1 seconds ago — View Log Connector Token Diagnostics ⓘ 1 seconds ago — View Log Cloud Reachability ⓘ 3 seconds ago — View Log Download Diagnostics Logs
✕	Represents a failure in the diagnostic test. Click **View Logs** to see additional details. ***Figure 158: View Logs for a Successful Test***  Troubleshoot Complete. Logs: HTTP Proxy Server Diagnostics Error while validating the disgnosticsid OK HTTP Proxy Server Diagnostics ⓘ 1 seconds ago — View Log Connector Token Diagnostics ⓘ 1 seconds ago — View Log Cloud Reachability ⓘ 3 seconds ago — View Log Download Diagnostics Logs

Step 5 Click **Download Diagnostic Logs** to download a text file with details of logs, including diagnostic information.

Figure 159: ownload Diagnostic Logs


10.22.244.103-diagnostics-logs-2023-01-09T21_28_21-08_00.txt - Notepad
File Edit Format View Help

```
2023-01-10 05:20:42-UTC   DNS Server 171.70.168.183 is reachable
2023-01-10 05:20:44-UTC   There are no proxies configured for running proxy ping diagnostics
Error while validating the disgnosticsid
2023-01-10 05:20:46-UTC   Perform cloud token tests for endpoint: https://connector.qa-
dnaspaces.io
2023-01-10 05:20:46-UTC   Cloud token configured with tenant: 12454 for connector-id:
73161672582150816000
2023-01-10 05:20:47-UTC   Reaching cloud endpoint https://dnaspaces.io/ without proxies
2023-01-10 05:20:47-UTC   HTTP Ping Succeeded to reach https://dnaspaces.io/
```

What to do next

You can also use the connector CLI to troubleshoot connectivity issues between the connector and the Cisco Spaces dashboard. See the command **connectorctl troubleshooting connectivity** in the Cisco Spaces: Connector 3 Command Reference Guide.

Unresponsive Connector, or Failure of SSH to Connector

If a connector is unresponsive to SSH requests, reboot the device on which the connector OVA is installed. You can do this from the Cisco Spaces dashboard .

Procedure

Step 1 Log in to **Cisco Spaces**.

Note
The Cisco Spaces URL is region-dependent.

Step 2 From the left navigation pane, choose **Setup** > **Wireless Networks**.

Step 3 In the **2. Configure Spaces Connector** area, click **View Connectors**.

Step 4 Click a connector from the list of connectors that are displayed, and then click the **Instances** tab.

Step 5 In the **Actions** column, click the three-dot icon to open a list of options for the connector instance, and choose **Restart Connector**.

Figure 160: Restart Connector

Instance is Corrupted or Deleted

You may have to delete a connector instance for one of the following reasons:

- An instance is not required anymore.
- An instance is corrupted or invalid.

Procedure

Step 1 Log in to **Cisco Spaces**.

Note
The Cisco Spaces URL is region-dependent.

Step 2 In the left navigation pane of the Cisco Spaces dashboard, choose **Setup** > **Wireless Networks**.

Step 3 In the **2. Configure Spaces Connector** area, click **View Connectors**.

Step 4 Click a connector from the list of connectors that are displayed and then click the **Instances** tab.

Step 5 In the **Actions** column, click the three-dot icon to open a list of options for the connector instance, and choose **Remove**.

To create a new instance, do the following.

a. In the Cisco Spaces dashboard, reissue a token.

b. Configure the new token on the installed connector.

See Activating Connector 3 on Cisco Spaces, on page 10.

Service Crash, or Restart Services

This task shows you how to restart a service on a connector when the service crashes or hangs.

Procedure

Step 1 Log in to **Cisco Spaces**.

Note
The Cisco Spaces URL is region-dependent.

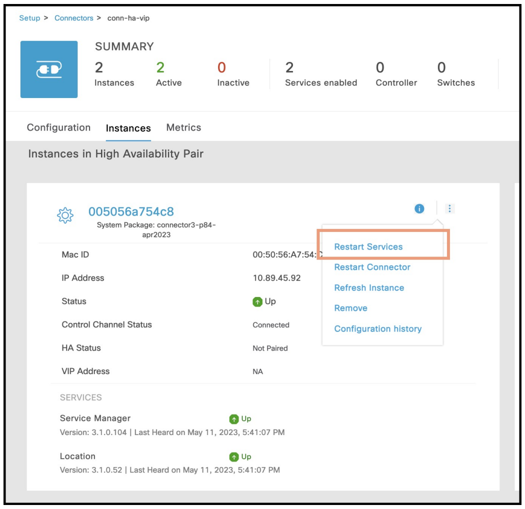
Step 2 From the left navigation pane of the Cisco Spaces dashboard, choose **Setup** > **Wireless Networks**.

Step 3 In the **2. Configure Spaces Connector** area, click **View Connectors**.

Step 4 Click a connector from the list of connectors that are displayed, and then click the **Instances** tab.

Step 5 In the **Actions** column, click the three-dot icon to open a list of options for the connector instance, and choose **Restart Services.**

Figure 161: Restart Services



SUMMARY

2 Instances | 2 Active | 0 Inactive | 2 Services enabled | 0 Controller | 0 Switches

Instances in High Availability Pair

005056a754c8
System Package: connector3-p84-apr2023

Mac ID: 00:50:56:A7:54:C
IP Address: 10.89.45.92
Status: Up
Control Channel Status: Connected
HA Status: Not Paired
VIP Address: NA

SERVICES

Service Manager: Up
Version: 3.1.0.104 | Last Heard on May 11, 2023, 5:41:07 PM

Location: Up
Version: 3.1.0.52 | Last Heard on May 11, 2023, 5:41:07 PM

Upgrade has Failed, or How To Forcibly Push Configurations to Instances

If a service upgrade fails and a connector instance does not receive Cisco Spaces configurations, you can forcibly push configurations to the instance using this procedure.

Procedure

Step 1 Log in to **Cisco Spaces**.

Note
The Cisco Spaces URL is region-dependent.

Step 2 From the left-navigation pane, choose **Setup** > **Wireless Networks**.

Step 3 In the **2. Configure Spaces Connector** area, click **View Connectors**.

Step 4 Click a connector from the list of connectors that are displayed, and then click the **Instances** tab.

Step 5 In the **Actions** column, click the three-dot icon to open a list of options for the connector instance, and choose **Refresh Instance**.

Managing Weak Algorithms from SSHD Configurations

Weak SSHD Key Exchange (kex) Algorithms

Key exchange algorithms are used to securely exchange cryptographic keys between the client and the server over an insecure network. This ensures that the communication remains private and secure.

However, some SSHD Key Exchange algorithms are considered weak for many reasons.

Here are a few reasons:

- Older key exchange methods using smaller key sizes (768 bits).
- Some key exchange algorithms do not support perfect forward secrecy. This means that if a private key is compromised, past communications encrypted with that key could potentially be decrypted.

Disabling weak SSHD Key Exchange algorithms is essential to improve the security of your SSH server.

Disable Weak SSHD Key Exchange (kex) Algorithms

Procedure

Step 1 Display the list of Key Exchange algorithms using the **connectorctl sshd kex show** command. Observe that this list includes SSHD Key Exchange (kex) algorithms that may be considered weak (weak SSHD Key Exchange algorithms) for different reasons.

```
[spacesadmin@connector ~]$ connectorctl sshd kex show
Executing command:sshd
Command execution status:Success
-----------------------
List of supported Key Exchange algorithms is:
kexalgorithms
ecdh-sha2-nistp256,
ecdh-sha2-nistp384,
ecdh-sha2-nistp521,
diffie-hellman-group14-sha1,
diffie-hellman-group14-sha256,
diffie-hellman-group16-sha512
```

Step 2 To remove support for weak SSHD Key Exchange algorithms from this device, use the **connectorctl sshd kex remove** command. Run the **connectorctl sshd kex show** command to verify that weak SSHD Key Exchange algorithms are removed from the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl  sshd kex remove -a
Executing command:sshd
Command execution status:Success
-----------------------
Removing all unsupported weak algorithms
Successfully removed -diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1 key exchange
algorithm(s)
```

```
[spacesadmin@connector ~]$ connectorctl  sshd kex show
Executing command:sshd
```

Step 3 To reinstate support for weak SSHD Key Exchange algorithms on this device, use the **connectorctl sshd kex reset** command. Run the **connectorctl sshd kex show** command to verify that weak SSHD Key Exchange algorithms are added back to the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl  sshd kex reset
Executing command:sshd
Command execution status:Success
-----------------------
Successfully reset Key Exchange algorithms configuration

[spacesadmin@connector ~]$ connectorctl  sshd kex show
Executing command:sshd
Command execution status:Success
-----------------------
List of supported Key Exchange algorithms is:
kexalgorithms
ecdh-sha2-nistp256,
ecdh-sha2-nistp384,
ecdh-sha2-nistp521,
diffie-hellman-group14-sha1,
diffie-hellman-group14-sha256,
diffie-hellman-group16-sha512
```

Weak Host Key (hostkey) Algorithms

Host key algorithms are used to verify the server's identity to the client. The server uses its private key to authenticate itself, and the client uses the server's public key to verify this identity.

However, some Host Key algorithms are considered weak for many reasons. Here are a few reasons:

- Short key length (RSA keys that are less than 2048 bits).
- Outdated algorithms (Digital Signature Algorithms [DSA] is limited to a maximum key size of 1024 bits).
- Weak hash functions (MD5 or SHA-1) can compromise the security of the entire key exchange process.

Disabling weak Host Key algorithms is essential to secure SSH connections and prevent potential vulnerabilities.

Disable Weak Host Key (hostkey) Algorithms

Procedure

Step 1 Display the list of Host Key algorithms using the **connectorctl sshd hostkey show** command.

```
[spacesadmin@connector ~]$ connectorctl  sshd hostkey show
Executing command:sshd
Command execution status:Success
-----------------------
List of supported host Key algorithms is:
hostkeyalgorithms *
```

Step 2 To remove support for weak Host Key algorithms from this device, use the **connectorctl sshd hostkey remove** command. Run the **connectorctl sshd hostkey show** command to verify that weak Host Key algorithms are removed from the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl  sshd hostkey remove -a
Executing command:sshd
Command execution status:Success
-----------------------
Removing all unsupported weak algorithms
Successfully removed
x509v3-ecdsa-sha2-nistp256,
x509v3-ecdsa-sha2-nistp384,
x509v3-ecdsa-sha2-nistp521,
x509v3-ssh-rsa,
x509v3-rsa2048-sha256,
x509v3-sign-rsa,,,
ssh-ed25519,,
ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384,
ecdsa-sha2-nistp521,
ssh-rsa key exchange algorithm(s)
```

Step 3 To reinstate support for weak Host Key algorithms on this device, use the **connectorctl sshd hostkey reset** command. Run the **connectorctl sshd hostkey show** command to verify that weak Host Key algorithms are added back to the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl  sshd hostkey reset
Executing command:sshd
Command execution status:Success
-----------------------
Successfully reset key exchange algorithms configuration
```

Weak Cipher Algorithms

Cipher algorithms are used to encrypt data transmitted between the client and the server, ensuring confidentiality.

However, some cipher algorithms are considered weak for many reasons. Here are a few reasons:

- Ciphers with short key lengths are susceptible to force attacks.
- Some ciphers (such as RC4) have biases in the output that make it susceptible to cryptanalysis.
- Weak algorithm structure (use of small block sizes can lead to vulnerabilities when encrypting large amount of data).
- Even strong ciphers can be rendered weak, if they are implemented poorly.

Disabling weak cipher algorithms is essential to ensure secure communications.

Disable Cipher Algorithms

Procedure

Step 1 Display the list of cipher algorithms using the **connectorctl sshd cipher show** command.

```
[spacesadmin@connector ~]$ connectorctl  sshd cipher show
Executing command:sshd
Command execution status:Success
-----------------------
List of supported Cipher algorithms is:
ciphers chacha20-poly1305@openssh.com,
aes128-ctr,
aes192-ctr,
aes256-ctr,
aes128-gcm@openssh.com,
aes256-gcm@openssh.com
```

Step 2 To remove support for weak cipher algorithms from this device, use the **connectorctl sshd cipher remove** command. Run the **connectorctl sshd cipher show** command to verify that weak cipher algorithms are removed from the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl  sshd cipher remove -a
Executing command:sshd
Command execution status:Success
-----------------------
Removing all unsupported cipher algorithms
Successfully removed -3des-cbc key exchange algorithm(s)
```

Step 3 To reinstate support for weak cipher algorithms on this device, use the **connectorctl sshd cipher reset** command. Run the **connectorctl sshd cipher show** command to verify that weak cipher algorithms are added back to the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl  sshd cipher reset
Executing command:sshd
Command execution status:Success
-----------------------
Successfully reset Cipher algorithms configuration
```

Weak Message Authentication Code (MAC) Algorithms

Message Authentication Code (MAC) algorithms are used to ensure the integrity and authenticity of the transmitted data, protecting it against tampering.

However, some MAC algorithms are considered weak for many reasons. Here are a few reasons:

- Many MAC algorithms, like HMAC, rely on hash functions to generate message digests. If the underlying hash function is weak (such as MD5 or SHA-1), the MAC algorithm inherits these weaknesses.
- Insufficient key length (shorter keys are more susceptible to attacks).
- Predictable key management (security of MAC algorithm is compromised with predictable keys).

Disabling weak MAC algorithms is essential to maintain the integrity and authenticity of communications.

Disable Message Authentication Code (MAC) Algorithms

Procedure

Step 1 Display the list of MAC algorithms using the **connectorctl sshd mac show** command.

```
[spacesadmin@connector ~]$ connectorctl sshd mac show
Executing command:sshd
Command execution status:Success
-----------------------
List of supported MAC algorithms is:
macs hmac-sha2-256-etm@openssh.com,
hmac-sha2-512-etm@openssh.com,
hmac-sha2-256,
hmac-sha2-512,
hmac-sha1
```

Step 2 To remove support for weak MAC algorithms from this device, use the **connectorctl sshd mac remove** command. Run the **connectorctl sshd mac show** command to verify that weak MAC algorithms are removed from the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl sshd mac remove -a
Executing command:sshd
Command execution status:Success
-----------------------
Removing all unsupported weak mac algorithms
Successfully removed -umac-64-etm@openssh.com,
hmac-sha1-etm@openssh.com,
umac-64@openssh.com,
hmac-sha1 key exchange algorithm(s)

Successfully removed weak MAC configuration
```

Step 3 To reinstate support for weak MAC algorithms on this device, use the **connectorctl sshd mac reset** command. Run the **connectorctl sshd mac show** command to verify that weak MAC algorithms are added back to the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl sshd mac reset
Executing command:sshd
Command execution status:Success
-----------------------
Successfully reset weak MAC configuration
```

Weak Public Key (pubkey) Algorithms

Public Key algorithms are used for user authentication, allowing users to log in without a password by proving ownership of a private key.

However, some Public Key algorithms are considered weak for many reasons. Here are a few reasons:

- Insufficient key length (RSA keys less than 2048 bits are considered insecure).
- Random number generation process can lead to predictable keys that are easier to attack.

Disable Public Key (pubkey) Algorithms

Procedure

Step 1 Display the list of Public Key algorithms using the **connectorctl sshd pubkey show** command.

```
[spacesadmin@connector ~]$ connectorctl  sshd pubkey show
Executing command:sshd
Command execution status:Success
-----------------------
List of supported Public key algorithms is:
pubkeyalgorithms *
```

Step 2 To remove support for weak Public Key algorithms from this device, use the **connectorctl sshd pubkey remove** command. Run the **connectorctl sshd pubkey show** command to verify that weak Public Key algorithms are removed from the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl  sshd pubkey remove -a
Executing command:sshd
Command execution status:Success
-----------------------
Removing all unsupported weak algorithms
Successfully removed x509v3-ecdsa-sha2-nistp256,
x509v3-ecdsa-sha2-nistp384,
x509v3-ecdsa-sha2-nistp521,
x509v3-ssh-rsa,
x509v3-rsa2048-sha256,
x509v3-sign-rsa,,,
ssh-ed25519,
ssh-ed25519-cert-v01@openssh.com,,
ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384,
ecdsa-sha2-nistp521,
ssh-rsa-cert-v01@openssh.com,
rsa-sha2-256-cert-v01@openssh.com,
rsa-sha2-512-cert-v01@openssh.com,
-cert-v01@openssh.com,
ecdsa-sha2-nistp256-cert-v01@openssh.com,
ecdsa-sha2-nistp384-cert-v01@openssh.com,
ecdsa-sha2-nistp521-cert-v01@openssh.com,
ssh-rsa,
rsa-sha2-256,
rsa-sha2-512 key exchange algorithm(s)
```

Step 3 To reinstate support for weak Public Key algorithms on this device, use the **connectorctl sshd pubkey reset** command. Run the **connectorctl sshd pubkey show** command to verify that weak Public Key algorithms are added back to the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl  sshd pubkey reset
Executing command:sshd
Command execution status:Success
-----------------------
Successfully reset key exchange algorithms configuration
```

PART IV

Services

CHAPTER 17

Location Service

Compatibility Matrix for Cisco Spaces: Connector: Location service

This section covers the following:

- Location Service (Non-FIPS)
- Location Service (FIPS)

Location Service (Non-FIPS)

Table 5: Location Service (Non-FIPS)

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco Catalyst 9800 Series Wireless Controllers	• Supported on 17.6.8 and later releases. **Note** • Use the latest software version or maintenance release for each listed release. See Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers. • 16.12.8 and 17.3.8a are end-of-life (EOL). We recommend that you migrate to one of the recommended releases as per the Guidelines for Cisco Wireless Software Release Product Bulletin.

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco AireOS Wireless Controller	**Note** • Use the latest software or maintenance release version for each listed release. See Recommended AireOS Wireless LAN Controller Releases. • 8.3, 8.5, and 8.8 are end-of-life (EOL). We recommend that you migrate to one of the recommended releases as per the Guidelines for Cisco Wireless Software Release Product Bulletin. • 8.10 is end-of-life (EOL).
Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)	Supported versions are: • 17.6.1 **Note** • Use the latest software or maintenance release version for eac • Cisco Wireless Embedded Wireless Controller (EWC) on Ac announces the end-of-sale and end-of-life dates for the Cisco 17.15.x will be the final IOS-XE software supporting EWC- EWC running on Catalyst switches in Software Defined Acc For more information, see https://www.cisco.com/c/en/us/products/collateral/wireless/emb Supported access points are: • Cisco Catalyst 9115 Series Access Points • Cisco Catalyst 9117 Series Access Points • Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points
Cisco Catalyst 9300 and 9400 Series Switches	Supported versions are 17.3.3 and later
Cisco Prime Infrastructure	Supported
Catalyst Center	Supported
Supported wireless controllers for Cisco FastLocate	• Supported on all releases of Cisco Catalyst 9800 Series Wireless Controllers
Supported wireless controllers for Cisco Hyperlocation	• Supported on Cisco Catalyst 9800 Series Wireless Controllers

Hardware or Application Name	Support for Cisco Spaces: Connector
Connector Active-Active Mode	• Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP) • Supported on Cisco Catalyst 9800 Series Wireless Controllers • Supported on Cisco AireOS Wireless Controller
Tested VMware Environments	• VMware vSphere Client Version 7.0.x and 8.0 • VMware vCenter Server Appliance 7.0.x and 8.0
Tested Proxies	• Squid proxy • Forward-only mode (SSL tunneling) • Squid-in-the-middle mode (SSL tunneling with intercept capabilities) • McAfee • Cisco web security appliance
Tested Access Points for Cisco FastLocate	• Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points
Tested Access Points for Cisco FastLocate (Wi-Fi 7)	• Cisco Wireless 9178 Series Access Points • Cisco Wireless 9176 Series Access Points
Tested Access Points for Cisco FastLocate (Wi-Fi 6)	• Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points • Cisco Catalyst 9164 Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Catalyst IW9167I Heavy Duty Access Points
Tested Access Points for Cisco Hyperlocation	• Cisco Aironet 4800 Series Access Point

Hardware or Application Name	Support for Cisco Spaces: Connector
Tested Access Points	• Cisco Catalyst 9105AX (I/W) Series Access Points • Cisco Catalyst 9115AX (I/E) Series Access Points • Cisco Catalyst 9117AX (I) Series Access Points • Cisco Catalyst 9136 (I) Series Access Points • Cisco Catalyst 9162 (I) Series Access Points • Cisco Catalyst 9164 (I) Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Catalyst IW9167 (E/I) Heavy Duty Series Access Points • Cisco Catalyst IW9165D Heavy Duty Access Points • Cisco Catalyst IW9165E Rugged Access Points • Cisco Wireless 9172 Series Access Points

Location Service (FIPS)

Table 6: Location Service (FIPS)

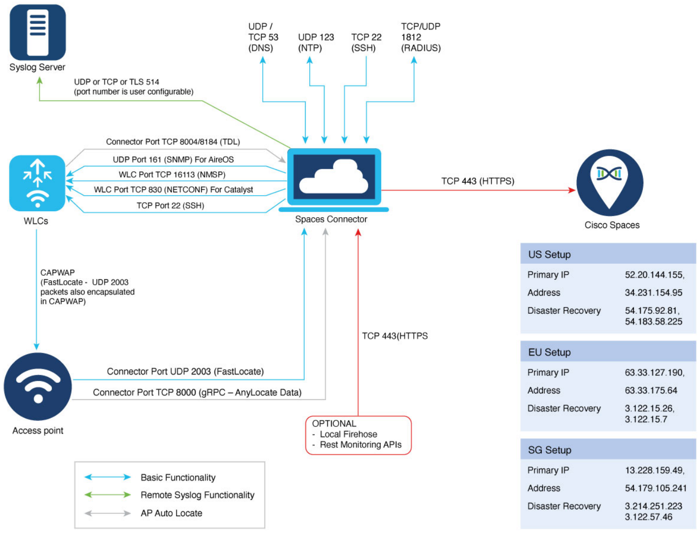
Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco Catalyst 9800 Series Wireless Controllers	• 17.15.3 • 17.12.6 **Note** Use the latest software version or maintenance release for each listed release. See Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers.
Tested Access Points for Cisco FastLocate (Wi-Fi 7)	• Cisco Wireless 9178 Series Access Points • Cisco Wireless 9176 Series Access Points

Hardware or Application Name	Support for Cisco Spaces: Connector
Tested Access Points for Cisco FastLocate (Wi-Fi 6)	• Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points • Cisco Catalyst 9164 Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Catalyst IW9167I Heavy Duty Access Points
Tested Access Points	• Cisco Catalyst 9105AX (I/W) Series Access Points • Cisco Catalyst 9115AX (I/E) Series Access Points • Cisco Catalyst 9117AX (I) Series Access Points • Cisco Catalyst 9136 (I) Series Access Points • Cisco Catalyst 9162 (I) Series Access Points • Cisco Catalyst 9164 (I) Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Catalyst IW9167 (E/I) Heavy Duty Series Access Points • Cisco Catalyst IW9165D Heavy Duty Access Points • Cisco Catalyst IW9165E Rugged Access Points • Cisco Wireless 9172 Series Access Points

Open Ports for Location Service

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

Figure 162: Open Ports for Location Service


Syslog Server
UDP / TCP 53 (DNS)
UDP 123 (NTP)
TCP 22 (SSH)
TCP/UDP 1812 (RADIUS)
UDP or TCP or TLS 514 (port number is user configurable)
Connector Port TCP 8004/8184 (TDL)
UDP Port 161 (SNMP) For AireOS
WLC Port TCP 16113 (NMSP)
WLC Port TCP 830 (NETCONF) For Catalyst
TCP Port 22 (SSH)
WLCs
Spaces Connector
TCP 443 (HTTPS)
Cisco Spaces
CAPWAP (FastLocate - UDP 2003 packets also encapsulated in CAPWAP)
TCP 443(HTTPS
Connector Port UDP 2003 (FastLocate)
Connector Port TCP 8000 (gRPC – AnyLocate Data)
Access point
OPTIONAL
- Local Firehose
- Rest Monitoring APIs
Basic Functionality
Remote Syslog Functionality
AP Auto Locate
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
SG Setup
Primary IP Address 13.228.159.49, 54.179.105.241
Disaster Recovery 3.214.251.223 3.122.57.46

	Primary IP Address	**Disaster Recovery**
US Setup	• 52.20.144.155 • 34.231.154.95	• 54.175.92.81 • 54.183.58.225
EU Setup	• 63.33.127.190 • 63.33.175.64	• 3.122.15.26 • 3.122.15.7
Singapore Setup	• 13.228.159.49 • 54.179.105.241	• 3.214.251.223 • 3.122.57.46

Test the connectivity between the connector and the wireless controller. See Configure and Test Connectivity between the Connector 3 and AireOS controller or Configure and Test the Connectivity between a Connector 3 and a Catalyst 9800 controller.

CHAPTER 18

IoT Service (Wireless)

Overview of Cisco Spaces: IoT Service (Wireless)

Cisco Spaces: IoT Service (Wireless) is a platform service within Cisco Spaces that enables you to claim, manage, and monitor IoT devices using Cisco's wireless infrastructure. IoT Service is designed to enable management of IoT devices across vendors, form factors, and technology protocols. Bluetooth Low Energy (BLE) is the first technology available for management using IoT services.

IoT service (wireless) encompasses hardware, software, and partner components to enable the management of devices that support critical business outcomes. IoT service (wireless) uses Cisco Catalyst 9800 Series Wireless Controllers, Cisco Spaces: Connector, Cisco Wi-Fi6 access points, and Cisco Spaces. IoT service (wireless) adopts a next-generation approach to manage complexity in an enterprise environment.

Using the IoT service (wireless), you can perform the following IoT management activities:

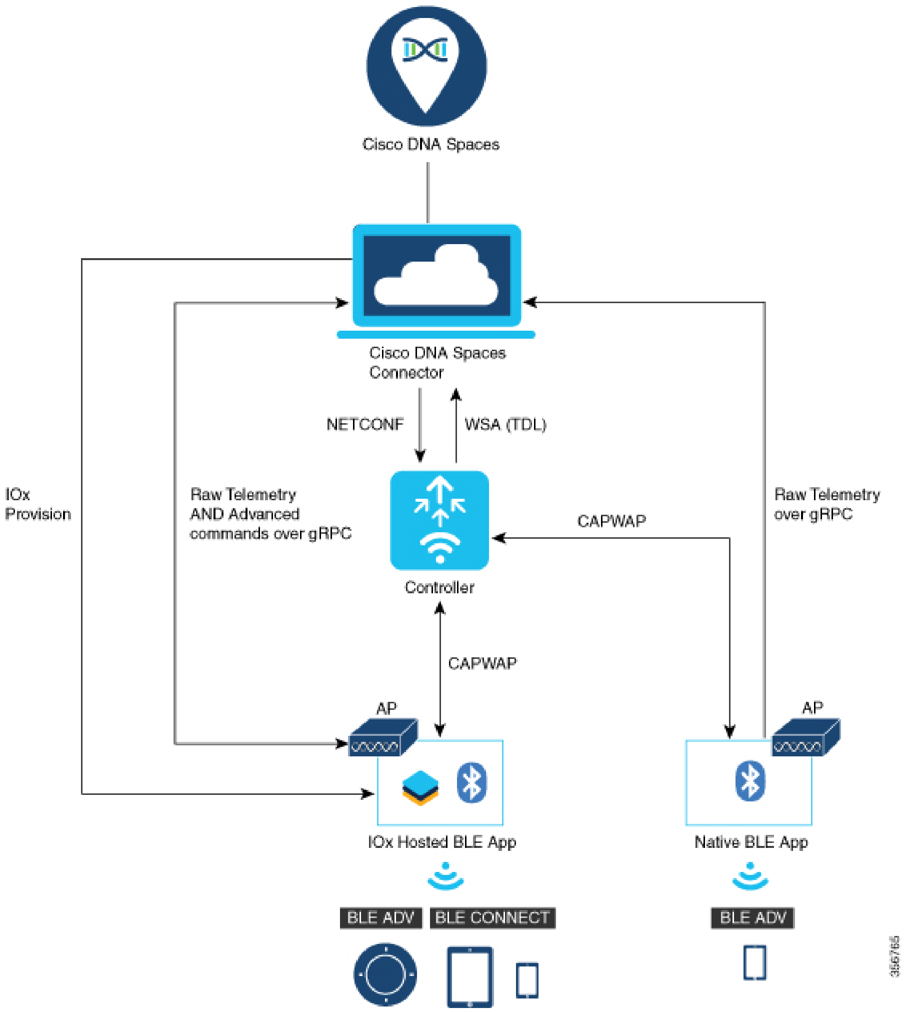
- Deploy BLE gateways on supported APs in your network.
- Claim the BLE beacons that you acquired from Cisco Spaces: IoT Device Marketplace.
- Configure APs and manage floor beacons.
- Monitor device attributes such as location, telemetry, battery status, and movement status.

Components of Cisco Spaces: IoT Service

The section describes the various components that work to complete the Cisco Spaces: IoT Service solution.

The Cisco Catalyst 9100 Series Family of Access Points acts as a gateway of communication between Cisco Spaces and the IoT devices. Cisco Spaces: IoT Service can then use a range of common APIs to communicate with edge devices and apps. The Cisco Spaces: IoT Service collects data from devices and apps, and passes it to Cisco-partnered websites that manage these devices far more extensively (referred to in this document as Device Manager websites). These Device Manager websites can use edge-device signals to enable outcomes specialized and targeted for each industry.

Figure 163: Components of IoT Service



Access Points

You can configure access points as gateways in Cisco Spaces. You can find the list of supported APs in the **Compatibility Matrix** section.

Depending on your Cisco AP model, configure the AP as one of these types of BLE gateways:

- **Base BLE Gateway**: This is an AP that does not run Cisco IOx App. You can configure this AP in **Scan**, **Transmit**, or **Dual** mode.
- **Advanced BLE Gateway**: This is an AP installed with the Cisco IOx App. The Cisco IOx App brings the ability to connect, configure, and manage third-party BLE floor beacons using the Cisco Spaces dashboard. Moreover, the Cisco IOx App can be used to perform additional BLE filtering on the AP. You can configure this AP in **Scan**, **Transmit**, or **Dual** mode.

Cisco Catalyst 9800 Series Wireless Controllers

The Cisco Catalyst 9800 Series Wireless Controller (Catalyst 9800 controller) combines RF excellence with Cisco IOS-XE benefits, and comes in physical or virtual form factor. This wireless controller is reliable and highly secure. You can manage this Catalyst 9800 controller using CLI, GUI, NETCONF, Yang, or the Catalyst Center.

The Catalyst 9800 controller is the single point for configuring and managing a wireless network and access points. The Catalyst 9800 controller configures and manages APs using the CAPWAP protocol.

The Catalyst 9800 controller receives BLE configuration from Cisco Spaces over NETCONF and passes the configuration to AP over CAPWAP. The feedback path from the AP to the wireless controller is through CAPWAP, and from the Catalyst 9800 controller to Cisco Spaces through Telemetry data logger (TDL) telemetry streaming. The gRPC configuration from Cisco Spaces also goes through the Catalyst 9800 controller, and from there to the corresponding AP. The configuration sets up the gRPC channel between the AP and Cisco Spaces. The AP sends the gRPC channel statistics to the Catalyst 9800 controller, and you can view these statistics on the Catalyst 9800 controller.

Note

- You can have only one gRPC session between an AP and connector.
- Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE Amsterdam 17.3.x supports only one of the following:
  - IoT service (wireless) with Cisco Spaces.
  - Network Assurance solution on Catalyst Center using Intelligent Capture (iCAP)

IoT service (wireless) and Intelligent Capture (iCAP) can co-exist from Cisco IOS XE Cupertino 17.7.x or higher.

Cisco Spaces: IoT Device Marketplace

Cisco Spaces: IoT Device Marketplace is a platform where you can discover, research, and purchase IoT devices. IoT Device Marketplace is a part of the Cisco Spaces full-stack partner ecosystem. Each device is preconfigured to give the customer an out-of-the-box experience with sensors, tags, wearables, and more. All the devices are compatible with the applications in the App Center. Current devices in the IoT Device Marketplace leverage BLE to transmit telemetry, with plans to add other technology in the future, such as Ultra Wide Band (UWB) and Zigbee.

Cisco Spaces: Connector

Cisco Spaces: Connector allows Cisco Spaces to communicate with more than one

- Cisco AireOS Wireless Controllers, and
- Cisco Catalyst 9800 Series Wireless Controllers.

APs connect to connector using the gRPC framework.

The APs establish a connection to connector using the gRPC protocol. The gRPC protocol configures floor beacons and receives telemetry data from the floor beacons. gRPC is a bidirectional streaming service, and requires a certificate to validate the host connection and a token for authentication. Each AP creates a gRPC connection. Connector can thus support many simultaneous connections.

Compatibility Matrix for IoT Service (Wireless)

Application Name	Support for Cisco Spaces: IoT Service
Supported wireless controllers	• Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.9.6 or 17.12.4 • Not supported on Cisco AireOS Wireless Controller • Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP) • Supported on Catalyst 9800 Controller running on Catalyst Switches in SD-Access mode (ECA) **Note** This support is conditional, and dependent on whether you have applied the fix described in CSCwk66790
Cisco Spaces: Connector Docker	2.0.455 and later
Cisco Spaces: Connector OVA	3.x and later
Cisco Prime Infrastructure	Cisco Prime Infrastructure Release 3.8 MR1 and later
Catalyst Center (for map import)	Catalyst Center Release 2.1.1 and later
Access Points for advanced BLE gateway (Wi-Fi 6)	• Cisco Catalyst 9105 Series Access Points • Cisco Catalyst 9115 Series Access Points • Cisco Catalyst 9117 Series Access Points • Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points • Cisco Catalyst 9136 Series Access Points • Cisco Catalyst 9162 Series Access Points • Cisco Catalyst 9164 Series Access Points • Cisco Catalyst 9166 Series Access Points • Cisco Aironet 4800 Series Access Points • Cisco Catalyst IW9167 (E/I) Heavy Duty Series Access Points

Application Name	Support for Cisco Spaces: IoT Service
Access points for basic BLE gateway	• Cisco Aironet 1815 Series Access Points • Cisco Aironet 2800 Series Access Points (USB dongle needed. No in-built USB radio) • Cisco Aironet 3800 Series Access Points (USB dongle needed. No in-built USB radio)
Cisco IOx App Version	1.0.46 and later **Note** For Cisco Catalyst 9800 Series Wireless Controllers Cisco IOS XE Cupertino 17.7.x, ensure that the IoX Application version is upgraded to Version 1.3.x

Note IoT Service (Wireless) is not supported with a directly connected controller, CMX Tethering, and AireOS connector. The only supported configuration is the Cisco Catalyst 9800 Wireless Controller and the connector.

The following table lists the compatibility of the Advanced BLE Gateway for BLE and the Base BLE Gateway App with various AP modes. This table is not applicable to Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP).

Table 7: AP Modes and App Support

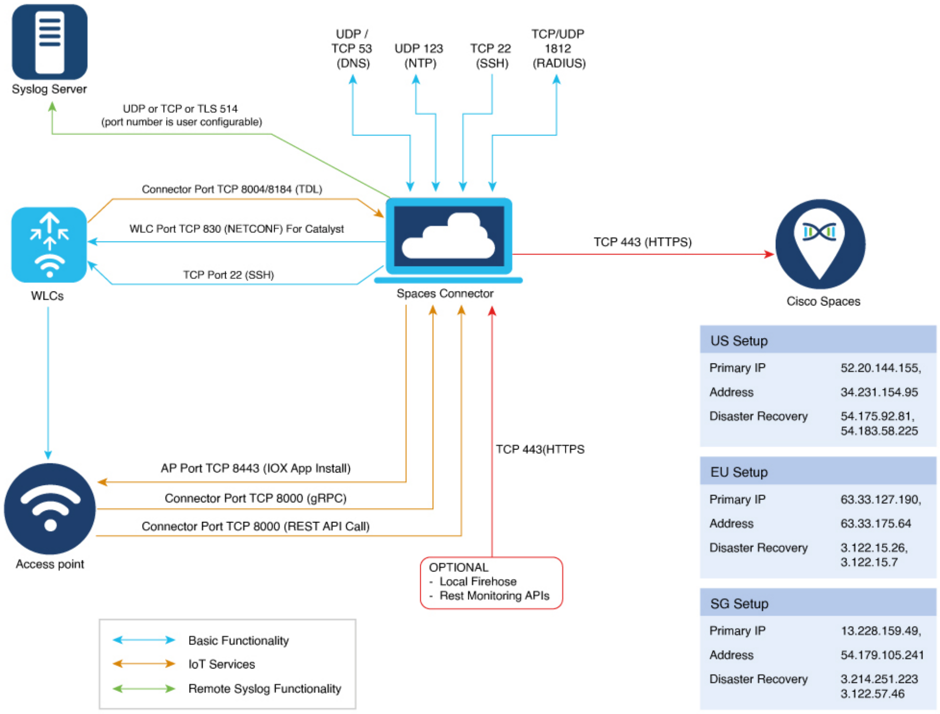
AP Mode	Advanced BLE Gateway App	Base BLE Gateway App
PI: Local	• 802.11ax: Supported • Wave 2: Not supported	• 802.11ax: Supported • Wave 2: Supported
P1: Flex	• 802.11ax: Supported • Wave 2: Not supported	• 802.11ax: Supported • Wave 2: Supported
P2: Fabric	• 802.11ax: Supported • Wave 2: Not supported	• 802.11ax: Supported • Wave 2: Supported
P3: Mesh	• 802.11ax: Supported • Wave 2: Not supported	• 802.11ax: Supported • Wave 2: Supported

Prerequisites of IoT Service (Wireless)

Open Ports for IoT Service (Wireless)

This section lists the connector ports that must be open for the proper functioning of IoT service (wireless).

Figure 164: Open Ports for IoT service (wireless)


Syslog Server
UDP / TCP 53 (DNS)
UDP 123 (NTP)
TCP 22 (SSH)
TCP/UDP 1812 (RADIUS)
UDP or TCP or TLS 514 (port number is user configurable)
Connector Port TCP 8004/8184 (TDL)
WLC Port TCP 830 (NETCONF) For Catalyst
TCP Port 22 (SSH)
WLCs
Spaces Connector
TCP 443 (HTTPS)
Cisco Spaces
TCP 443(HTTPS
AP Port TCP 8443 (IOX App Install)
Connector Port TCP 8000 (gRPC)
Connector Port TCP 8000 (REST API Call)
Access point
OPTIONAL
- Local Firehose
- Rest Monitoring APIs
Basic Functionality
IoT Services
Remote Syslog Functionality

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

SG Setup	
Primary IP Address	13.228.159.49, 54.179.105.241
Disaster Recovery	3.214.251.223 3.122.57.46

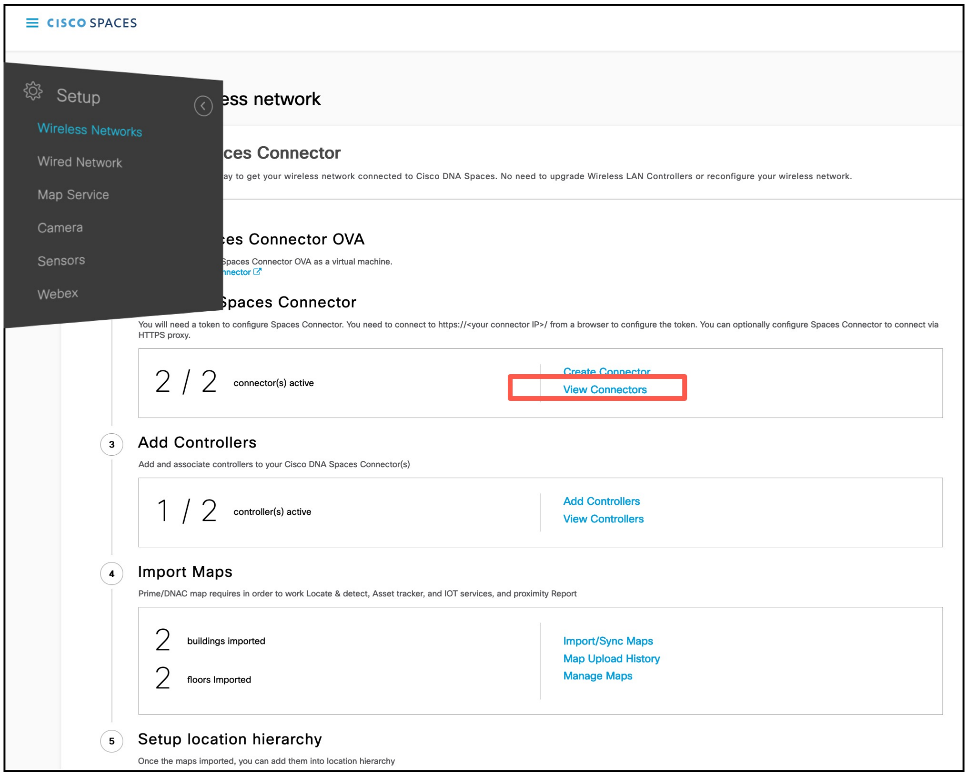
Configure IoT Service (Wireless)

Procedure

Step 1 In the Cisco Spaces dashboard left navigation pane, click **Setup** and choose **Wireless Networks**.

Step 2 In the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 165: View Connectors



ay to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.

Spaces Connector OVA as a virtual machine.

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

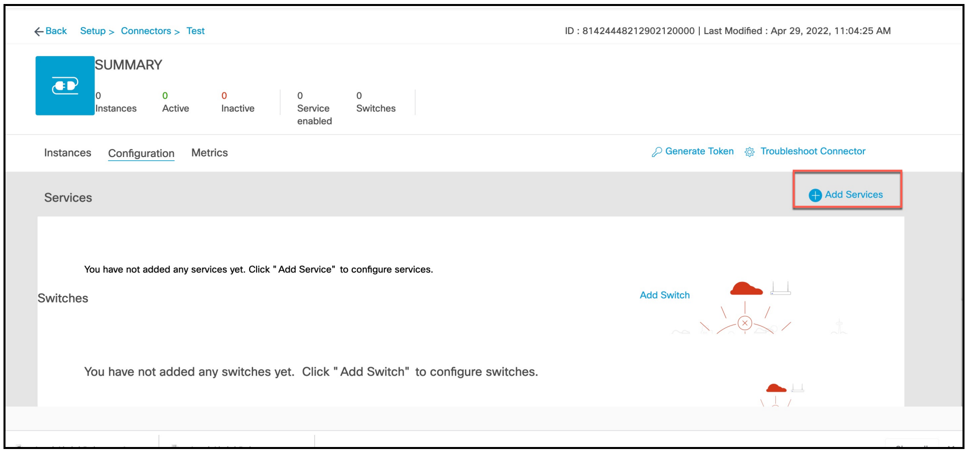
Add and associate controllers to your Cisco DNA Spaces Connector(s)

Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

Once the maps imported, you can add them into location hierarchy

Step 3 In the connector details window that is displayed, click **Add Services**.

Figure 166: Add Services



ID : 81424448212902120000 | Last Modified : Apr 29, 2022, 11:04:25 AM

You have not added any services yet. Click " Add Service" to configure services.

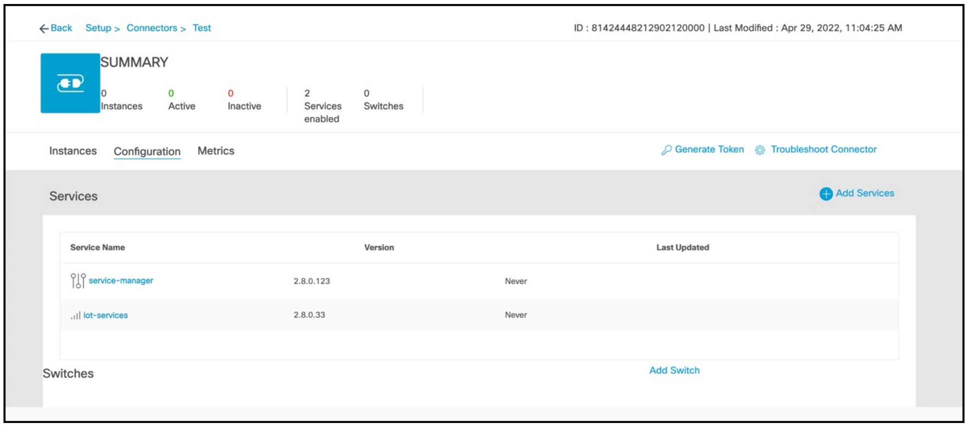
You have not added any switches yet. Click " Add Switch" to configure switches.

Step 4 In the **Add Services** window that is displayed, choose **IoT Wireless** and click **Add**.

Note

service-manager is chosen by default.

Figure 167: Connector Details



ID : 81424448212902120000 | Last Modified : Apr 29, 2022, 11:04:25 AM

Service Name	Version	Last Updated
service-manager	2.8.0.123	Never
iot-services	2.8.0.33	Never

In the **Connector Details** window, you can see that the number of services that are enabled has increased.

Verify IoT Streams for Catalyst 9800 Controller

This task is for troubleshooting purposes only. IoT streams are automatically enabled for all the wireless controllers associated with the IoT service (wireless) service of a connector.

This task helps you troubleshoot IoT streams of a Catalyst 9800 controller. If your APs are not visible, you can manually enable or disable the IoT streams of Cisco Spaces.

Procedure

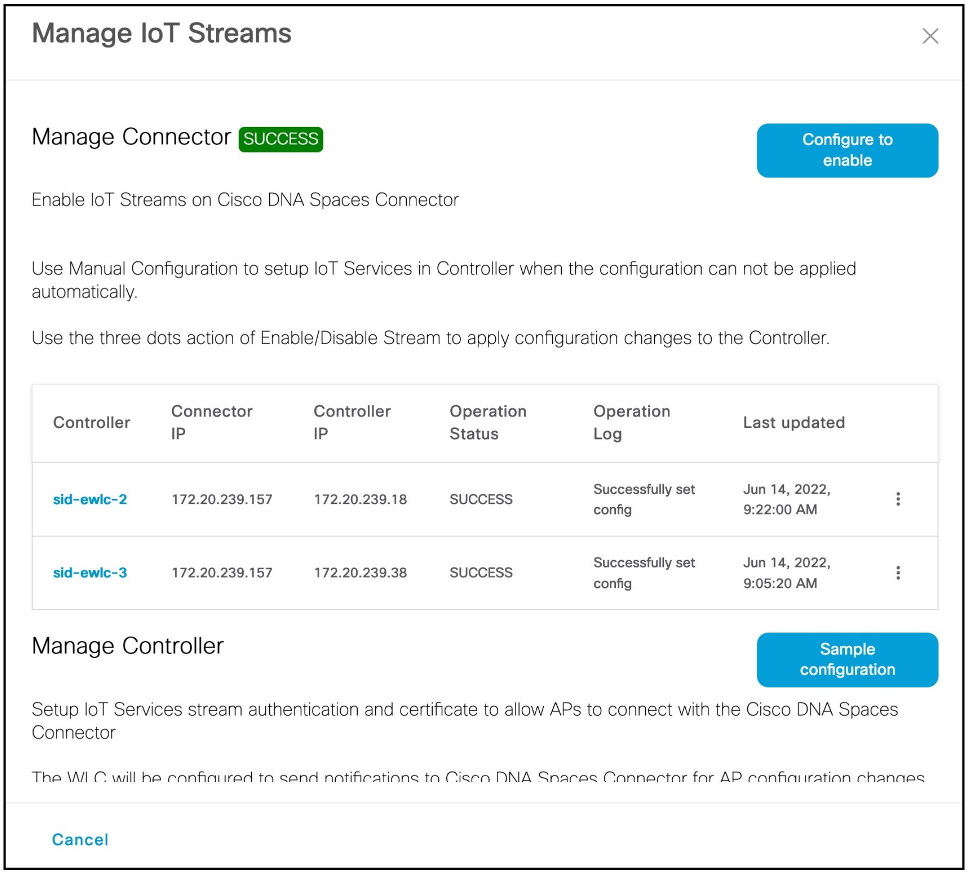
Step 1 In the Cisco Spaces dashboard left navigation pane, choose **Setup** > **Wireless Network**.

Step 2 In the **Configure via Spaces Connector** area titled **Step 2: Add Controllers**, click **View Connectors**.

Step 3 Click the connector of your choice.

Step 4 In the **Services** tab, in the **Actions** column, click the gear icon near IoT service (wireless) to open the **Manage IoT Streams** window.

Figure 168: Troubleshooting IoT Streams



Manage IoT Streams

Manage Connector SUCCESS

Enable IoT Streams on Cisco DNA Spaces Connector

Use Manual Configuration to setup IoT Services in Controller when the configuration can not be applied automatically.

Use the three dots action of Enable/Disable Stream to apply configuration changes to the Controller.

Controller	Connector IP	Controller IP	Operation Status	Operation Log	Last updated	
sid-ewlc-2	172.20.239.157	172.20.239.18	SUCCESS	Successfully set config	Jun 14, 2022, 9:22:00 AM	⋮
sid-ewlc-3	172.20.239.157	172.20.239.38	SUCCESS	Successfully set config	Jun 14, 2022, 9:05:20 AM	⋮

Manage Controller

Setup IoT Services stream authentication and certificate to allow APs to connect with the Cisco DNA Spaces Connector

The WLC will be configured to send notifications to Cisco DNA Spaces Connector for AP configuration changes

Verify Access Points

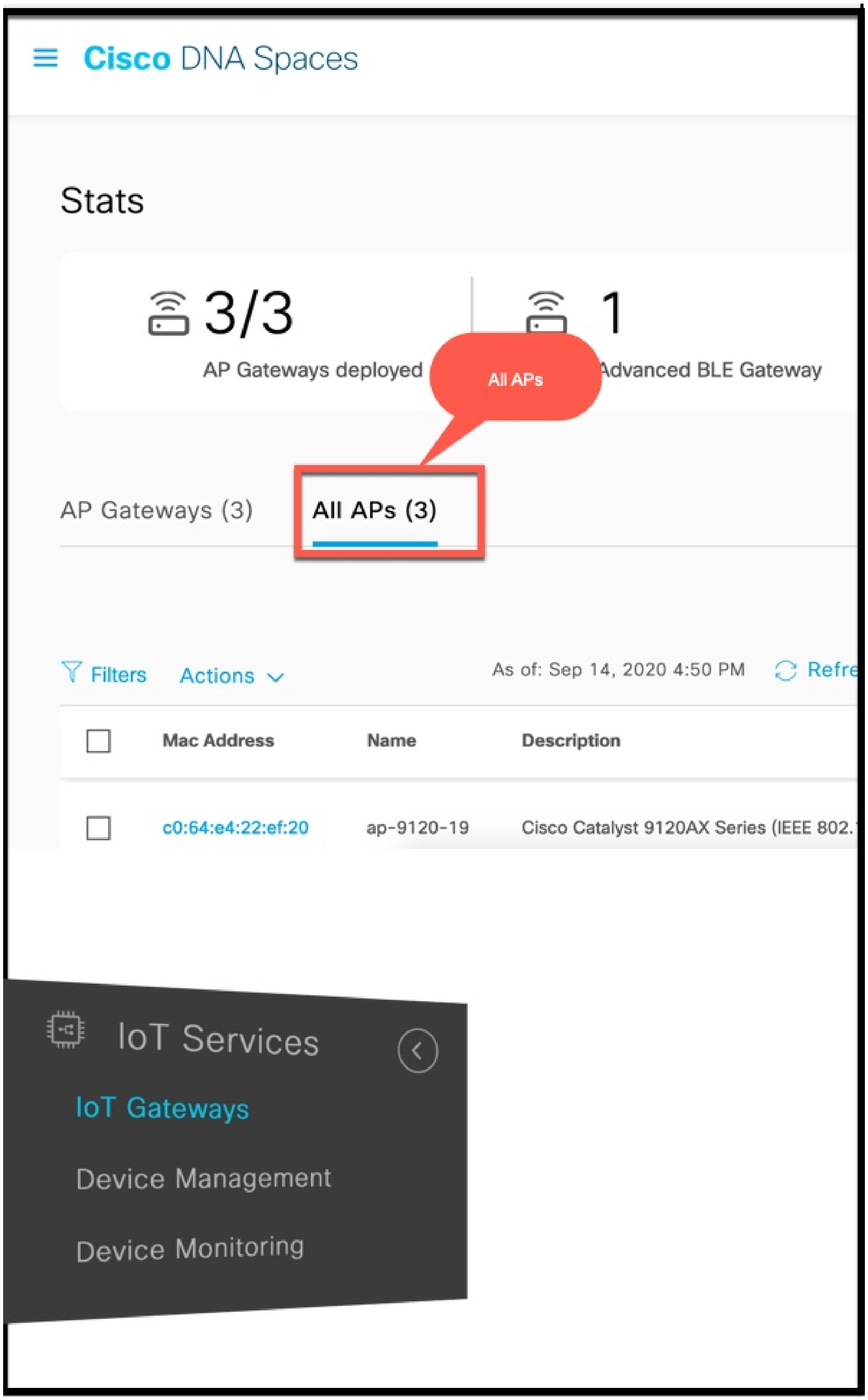
This procedure helps you verify if IoT service (wireless) has synchronized and listed the APs in your network on the GUI

Procedure

Step 1 In the Cisco Spaces dashboard left-navigation pane, choose **IoT Services** > **IoT Gateways** > **AP Gateway**.

Step 2 Click the **All APs** tab.

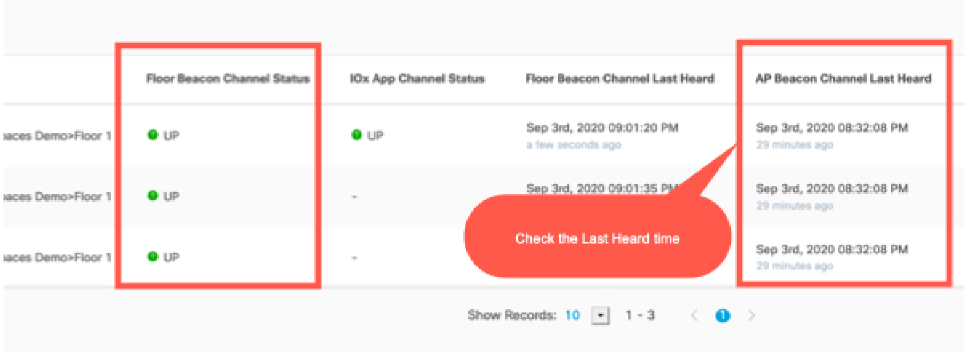
Figure 169: Verify APs



□	Mac Address	Name	Description
□	c0:64:e4:22:ef:20	ap-9120-19	Cisco Catalyst 9120AX Series (IEEE 802.1

Step 3 Verify if IoT service (wireless) has synchronized and listed the APs in your network. Check the **Floor Beacon Channel Status** and **AP Beacon Channel Last Heard** columns.

Figure 170: Verify APs



	Floor Beacon Channel Status	IOx App Channel Status	Floor Beacon Channel Last Heard	AP Beacon Channel Last Heard
aces Demo>Floor 1	● UP	● UP	Sep 3rd, 2020 09:01:20 PM a few seconds ago	Sep 3rd, 2020 08:32:08 PM 29 minutes ago
aces Demo>Floor 1	● UP	-	Sep 3rd, 2020 09:01:35 PM	Sep 3rd, 2020 08:32:08 PM 29 minutes ago
aces Demo>Floor 1	● UP	-		Sep 3rd, 2020 08:32:08 PM 29 minutes ago

Show Records: 10 ▾ 1 - 3 ‹ 1 ›

Check the Last Heard time

CHAPTER 19

IoT Service (Wired)

Overview

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

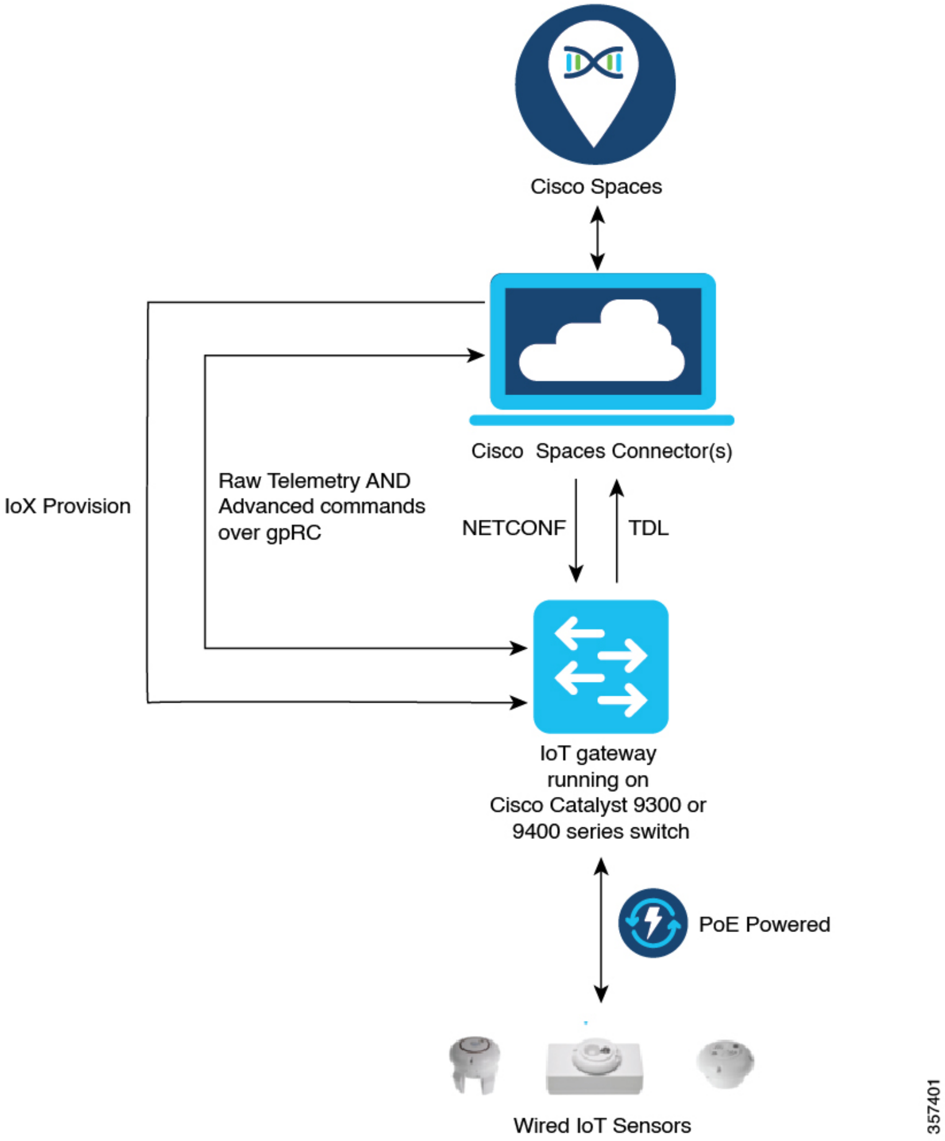
Integrating IoT service (wired) with the Cisco Catalyst 9300 and 9400 Series Switches series platform requires the following:

- 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 171: Data flow in IoT Service (Wired)


Cisco Spaces
Cisco Spaces Connector(s)
IoX Provision
Raw Telemetry AND Advanced commands over gpRC
NETCONF
TDL
IoT gateway running on Cisco Catalyst 9300 or 9400 series switch
PoE Powered
Wired IoT Sensors
357401

Compatibility Matrix for IoT Service (Wired)

Application Name	Support for IoT Service (Wired)
Cisco Catalyst 9300 Series Switches	• Cisco IOS XE Cupertino 17.9.5 • Cisco IOS XE Dublin 17.12.4
Cisco Catalyst 9400 Series Switches	• Cisco IOS XE Cupertino 17.9.5 • Cisco IOS XE Dublin 17.12.4
Wired Docker Service	3.2.0.15 and later
Wired IOX Application	1.2.3 and later

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

- Connecting directly with controller
- CMX Tethering

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 175 .
- Ensure that Cisco Spaces is configured with maps either from Cisco Prime Infrastructure or Catalyst 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.

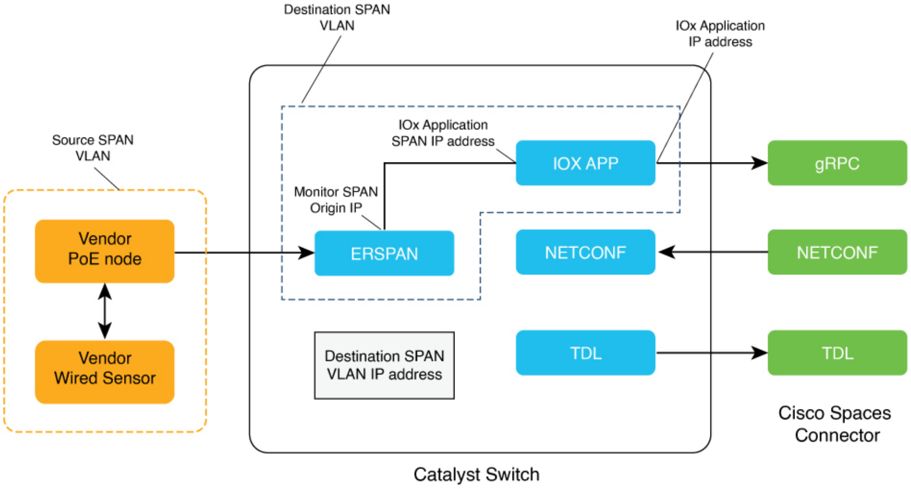
- Enable NETCONF on Cisco Catalyst 9300 or 9400 Series Switches on port 830, along with permission to use NETCONF.

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 172: Design Prerequisites

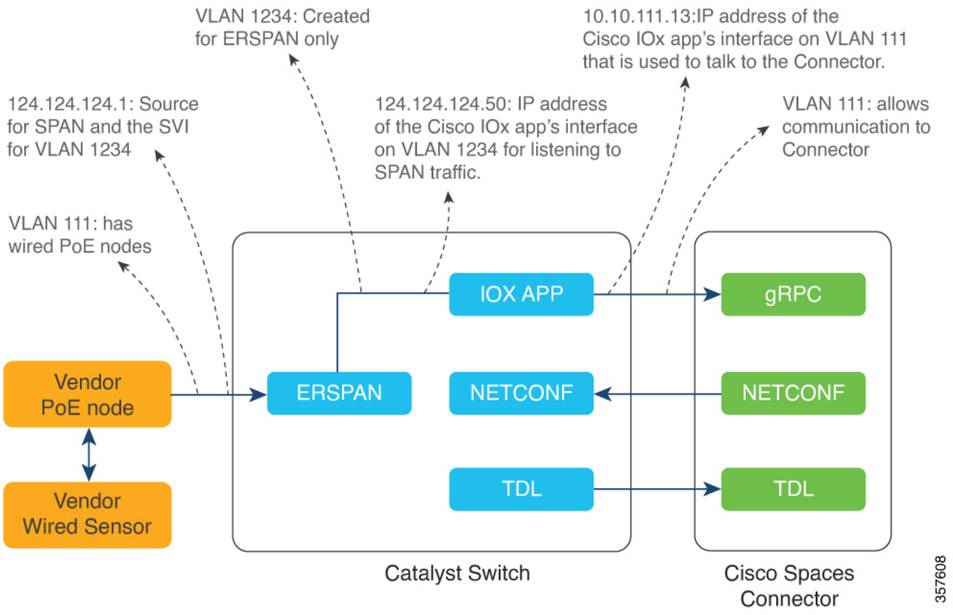


- **Destination SPAN VLAN**: The VLAN used to send Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic from Power over Ethernet (PoE) nodes to Cisco IOx App. You can use an existing VLAN or create a new one. This VLAN can also be local to the switch.
- **Destination SPAN VLAN IP address**: This 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 173: 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
TDL
TDL
Vendor Wired Sensor
Catalyst Switch
Cisco Spaces Connector
357608

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 175 .

- Ensure that Cisco Spaces is configured with maps either from Cisco Prime Infrastructure or Catalyst 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**

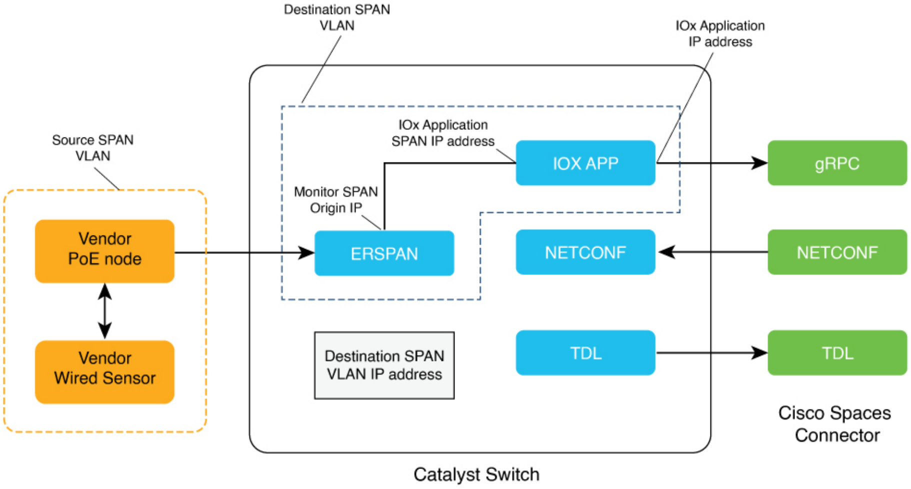
  For more information, see **Command Reference, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9300 Switches)**
- Perform NTP synchronization across wireless controllers, Cisco Spaces: Connectors, and switches in the network.
- Enable NETCONF on Cisco Catalyst 9300 or 9400 Series Switches on port 830, along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

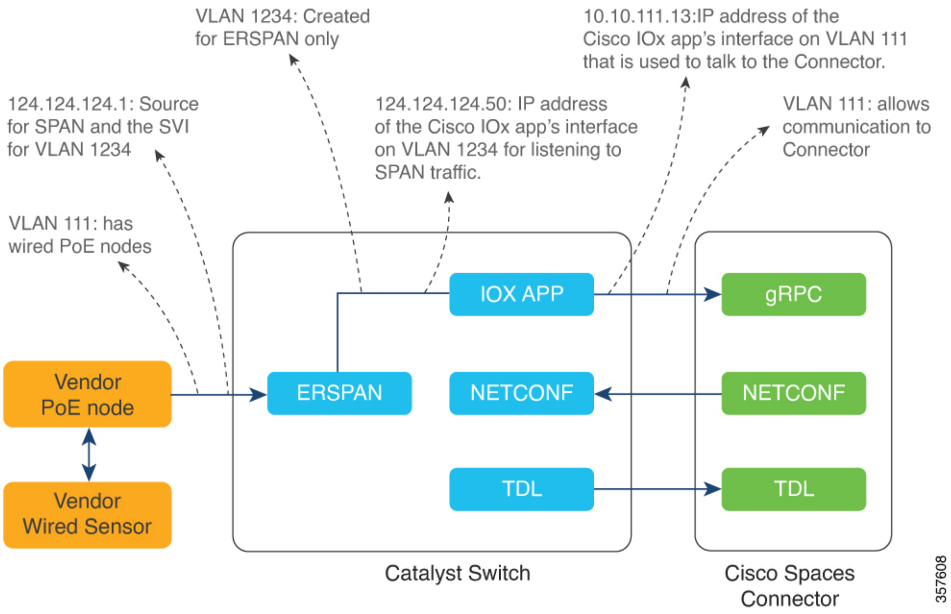
Figure 174: Design Prerequisites



- **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.

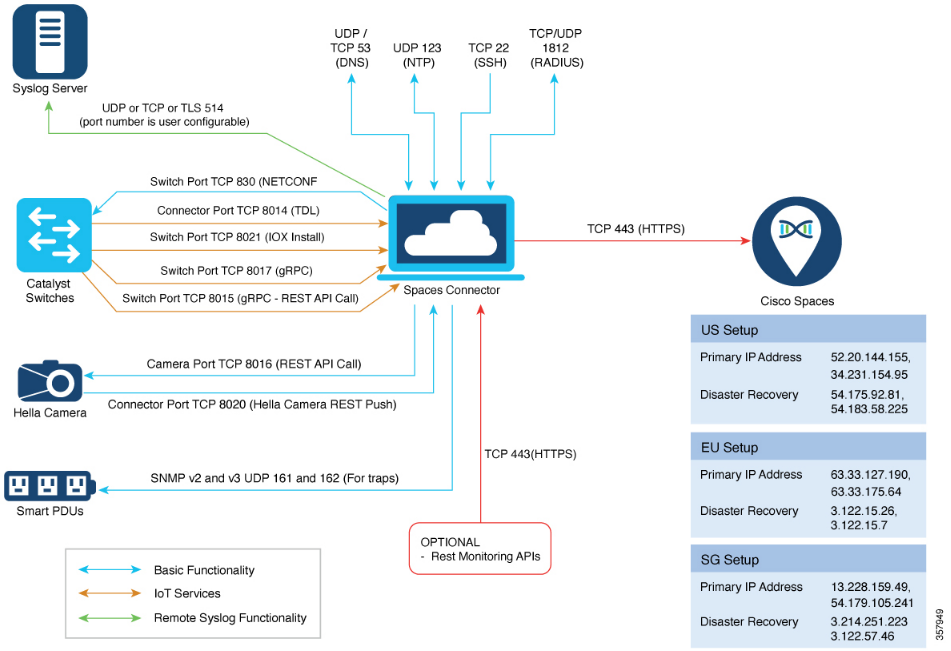
Figure 175: Sample Configuration


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

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


Syslog Server
UDP / TCP 53 (DNS)
UDP 123 (NTP)
TCP 22 (SSH)
TCP/UDP 1812 (RADIUS)
UDP or TCP or TLS 514
(port number is user configurable)
Switch Port TCP 830 (NETCONF
Connector Port TCP 8014 (TDL)
Switch Port TCP 8021 (IOX Install)
Switch Port TCP 8017 (gRPC)
Switch Port TCP 8015 (gRPC - REST API Call)
Catalyst Switches
Spaces Connector
TCP 443 (HTTPS)
Cisco Spaces
Camera Port TCP 8016 (REST API Call)
Connector Port TCP 8020 (Hella Camera REST Push)
Hella Camera
TCP 443(HTTPS)
SNMP v2 and v3 UDP 161 and 162 (For traps)
Smart PDUs
OPTIONAL
- Rest Monitoring APIs
Basic Functionality
IoT Services
Remote Syslog Functionality
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

SG Setup	
Primary IP Address	13.228.159.49, 54.179.105.241
Disaster Recovery	3.214.251.223 3.122.57.46

Figure 177: Open Ports for IoT Service (Wired) without the IoT Gateway

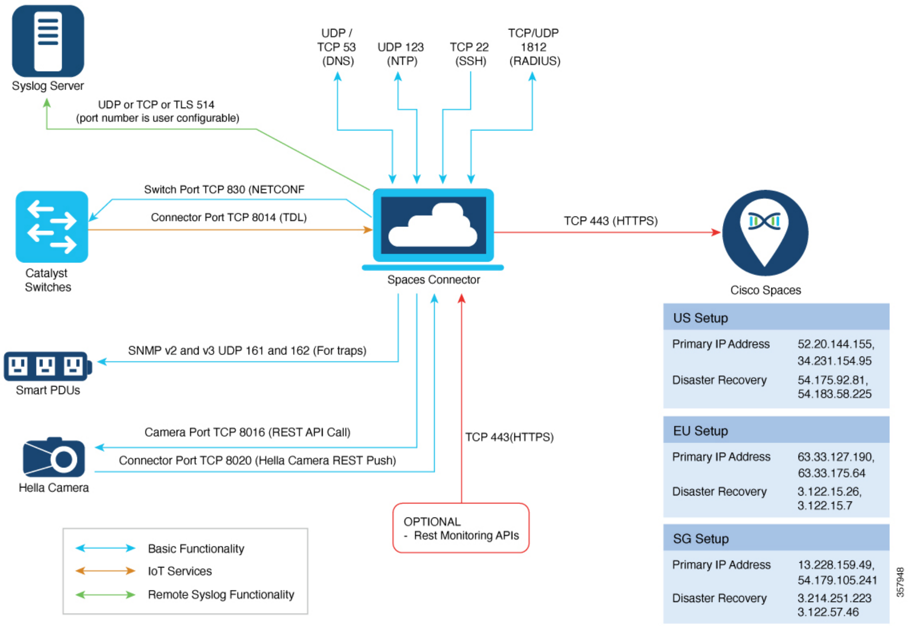

Syslog Server
UDP / TCP 53 (DNS)
UDP 123 (NTP)
TCP 22 (SSH)
TCP/UDP 1812 (RADIUS)
UDP or TCP or TLS 514 (port number is user configurable)
Switch Port TCP 830 (NETCONF
Connector Port TCP 8014 (TDL)
Catalyst Switches
Spaces Connector
TCP 443 (HTTPS)
Cisco Spaces
US Setup
Primary IP Address 52.20.144.155, 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
SG Setup
Primary IP Address 13.228.159.49, 54.179.105.241
Disaster Recovery 3.214.251.223 3.122.57.46
SNMP v2 and v3 UDP 161 and 162 (For traps)
Smart PDUs
Camera Port TCP 8016 (REST API Call)
Connector Port TCP 8020 (Hella Camera REST Push)
Hella Camera
TCP 443(HTTPS)
OPTIONAL
- Rest Monitoring APIs
Basic Functionality
IoT Services
Remote Syslog Functionality
357948

Table 8: 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
Singapore Setup (SG) Type	13.228.159.49 54.179.105.241	13.214.251.223 54.255.57.46

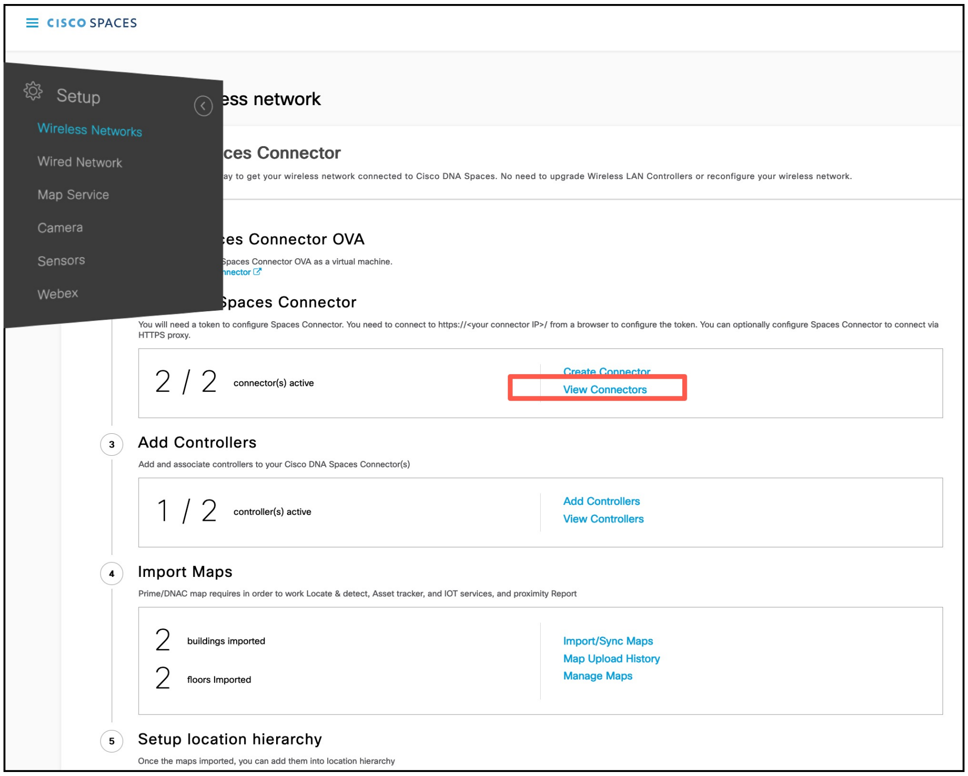
Configure IoT Service (Wired)

Procedure

Step 1 From the Cisco Spaces dashboard left-navigation pane, click **Setup** and choose **Wired Networks**.

Step 2 From the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 178: View Connectors



CISCO SPACES

Setup

Wireless Networks

Wired Network

Map Service

Camera

Sensors

Webex

ess network

ces Connector

ay to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.

es Connector OVA

Spaces Connector OVA as a virtual machine.

nector

Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

2 / 2 connector(s) active

Create Connector

View Connectors

3 Add Controllers

Add and associate controllers to your Cisco DNA Spaces Connector(s)

1 / 2 controller(s) active

Add Controllers

View Controllers

4 Import Maps

Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

2 buildings imported

2 floors Imported

Import/Sync Maps

Map Upload History

Manage Maps

5 Setup location hierarchy

Once the maps imported, you can add them into location hierarchy

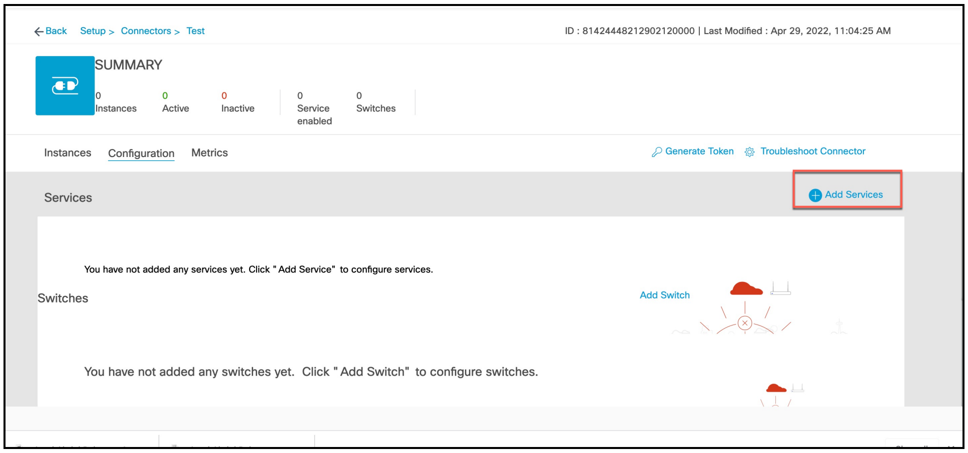
Step 3 Click a connector 3 of your choice.

Note

You can use the same connector that you used for Cisco Spaces: IoT Service (Wireless).

Step 4 In the connector details window that is displayed, click **Add Services**.

Figure 179: Add Services



Back Setup > Connectors > Test

ID : 81424448212902120000 | Last Modified : Apr 29, 2022, 11:04:25 AM

SUMMARY

0	0	0	0	0
Instances	Active	Inactive	Service enabled	Switches

Instances Configuration Metrics

Generate Token Troubleshoot Connector

Services

Add Services

You have not added any services yet. Click " Add Service" to configure services.

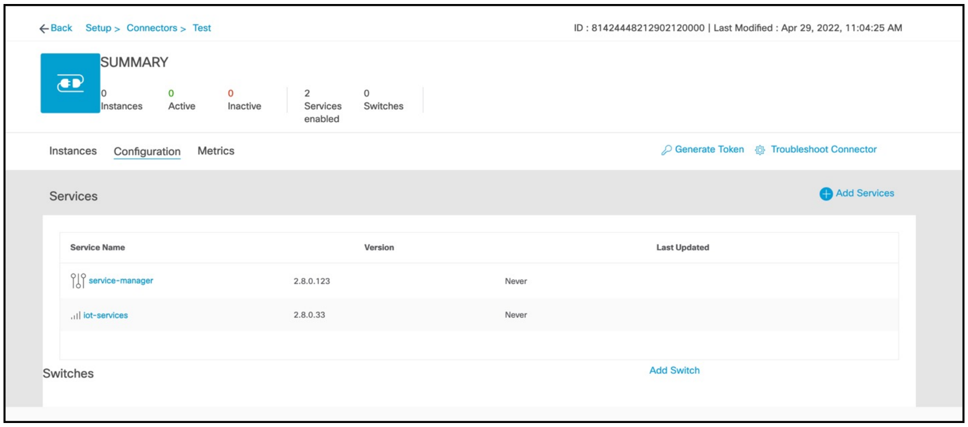
Switches

Add Switch

You have not added any switches yet. Click " Add Switch" to configure switches.

Step 5 In the **Add Service** window that is displayed, choose **IoT Wired** and click **Add**.

Figure 180: Adding a Service



←Back Setup > Connectors > Test

ID : 81424448212902120000 | Last Modified : Apr 29, 2022, 11:04:25 AM

SUMMARY

0 Instances	0 Active	0 Inactive	2 Services enabled	0 Switches

Services

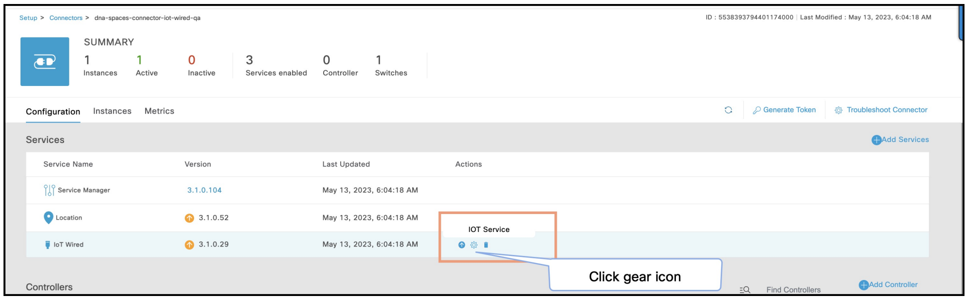
Service Name	Version	Last Updated
service-manager	2.8.0.123	Never
iot-services	2.8.0.33	Never

Switches

In the **Connector Details** window, you can see that the **IoT Wired** service has been added.

Step 6 Click the gear icon near the **IoT Wired** row.

Figure 181: Gear Icon of IoT Wired



Setup > Connectors > dna-spaces-connector-iot-wired-qa

ID : 5538393794401174000 | Last Modified : May 13, 2023, 6:04:18 AM

SUMMARY

1 Instances	1 Active	0 Inactive	3 Services enabled	0 Controller	1 Switches

Services

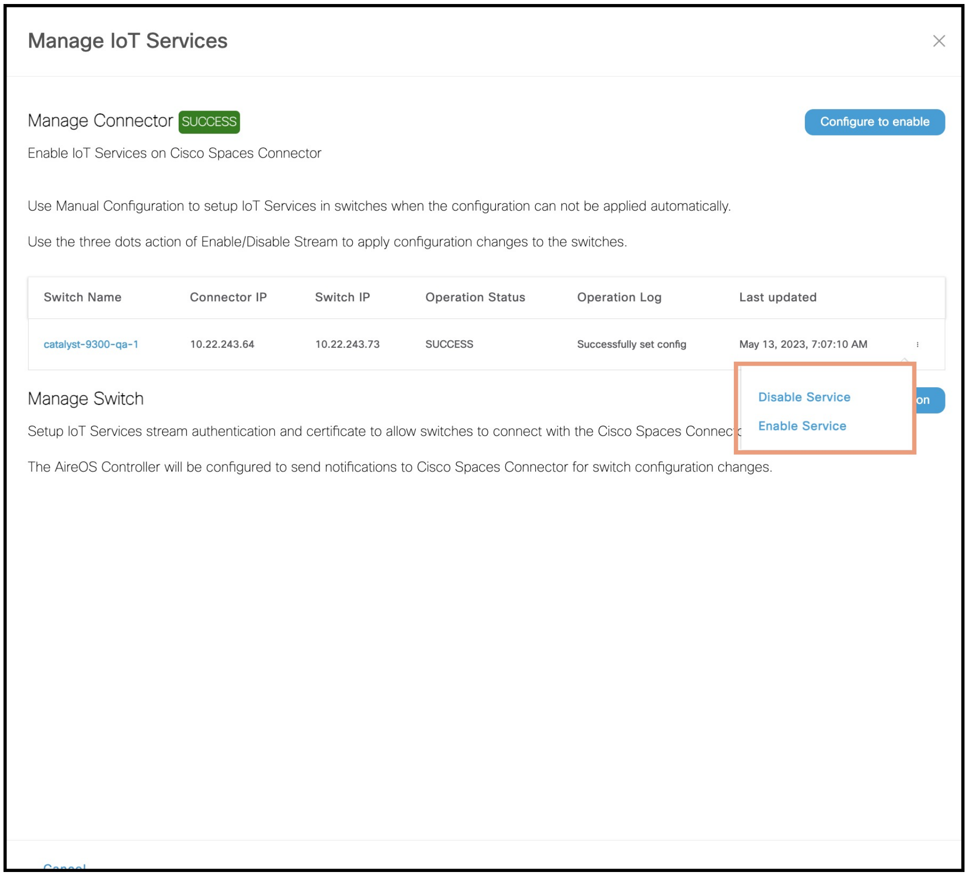
Service Name	Version	Last Updated	Actions
Service Manager	3.1.0.104	May 13, 2023, 6:04:18 AM	
Location	3.1.0.52	May 13, 2023, 6:04:18 AM	
IoT Wired	3.1.0.29	May 13, 2023, 6:04:18 AM	

Controllers

Step 7 (Optional) In the **Manage IoT Streams** window that is displayed, check if the connector is not already enabled, and if it is not, click **Configure to Enable**.

Step 8 From the list of switches, click the vertical three-dot icon adjacent to the switch and select **Enable Service**.

Figure 182: Enable Service



Manage IoT Services

Manage Connector SUCCESS

Enable IoT Services on Cisco Spaces Connector

Use Manual Configuration to setup IoT Services in switches when the configuration can not be applied automatically.

Use the three dots action of Enable/Disable Stream to apply configuration changes to the switches.

Switch Name	Connector IP	Switch IP	Operation Status	Operation Log	Last updated
catalyst-9300-qa-1	10.22.243.64	10.22.243.73	SUCCESS	Successfully set config	May 13, 2023, 7:07:10 AM

Manage Switch

Setup IoT Services stream authentication and certificate to allow switches to connect with the Cisco Spaces Connec

The AireOS Controller will be configured to send notifications to Cisco Spaces Connector for switch configuration changes.

Note

If you are using the same connector for both wired and wireless IoT services, the connector is already enabled.

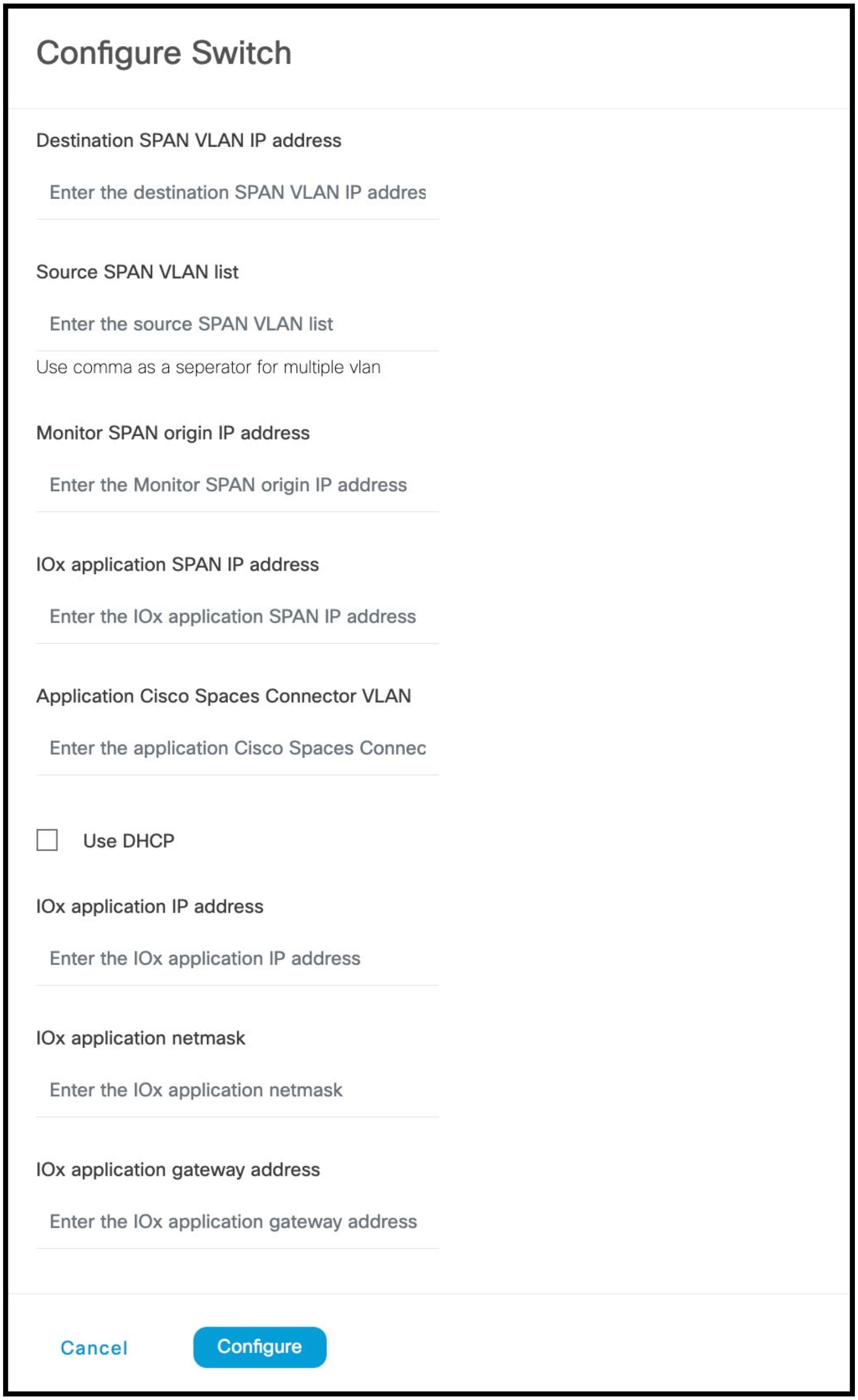
Step 9 Enter the SPAN VLAN and the Cisco IOx App details.

- **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 183: Configure Switch



Configure Switch

Destination SPAN VLAN IP address

Enter the destination SPAN VLAN IP addres

Source SPAN VLAN list

Enter the source SPAN VLAN list

Use comma as a seperator for multiple vlan

Monitor SPAN origin IP address

Enter the Monitor SPAN origin IP address

IOx application SPAN IP address

Enter the IOx application SPAN IP address

Application Cisco Spaces Connector VLAN

Enter the application Cisco Spaces Connec

□ Use DHCP

IOx application IP address

Enter the IOx application IP address

IOx application netmask

Enter the IOx application netmask

IOx application gateway address

Enter the IOx application gateway address

Figure 184: Configure Switch

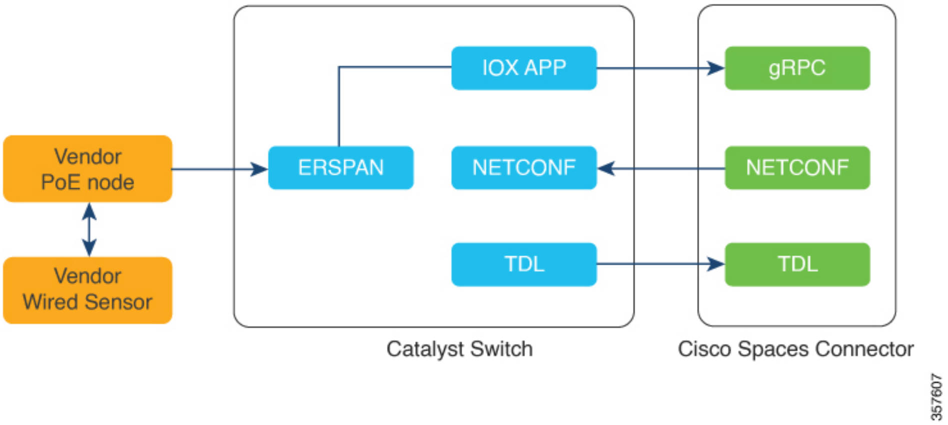
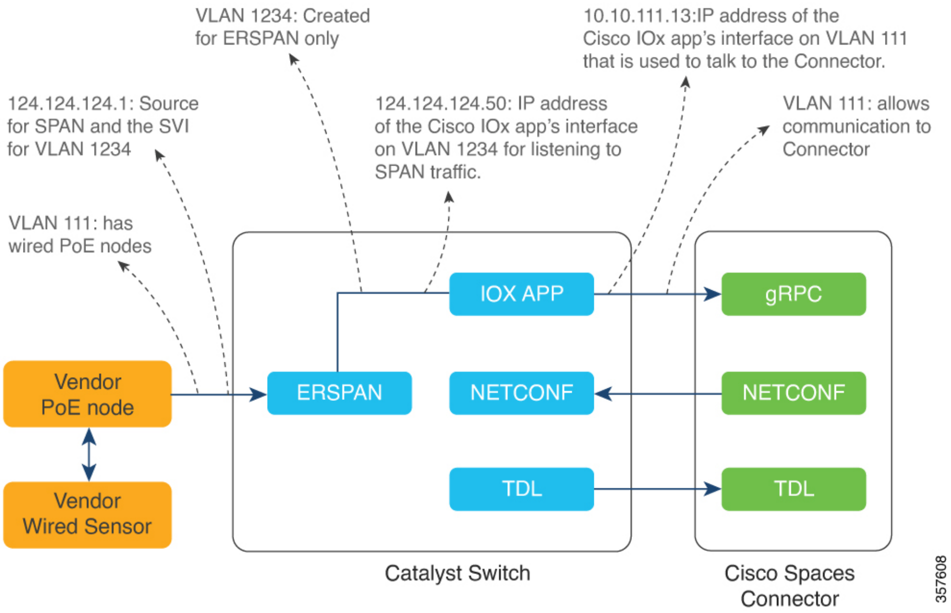


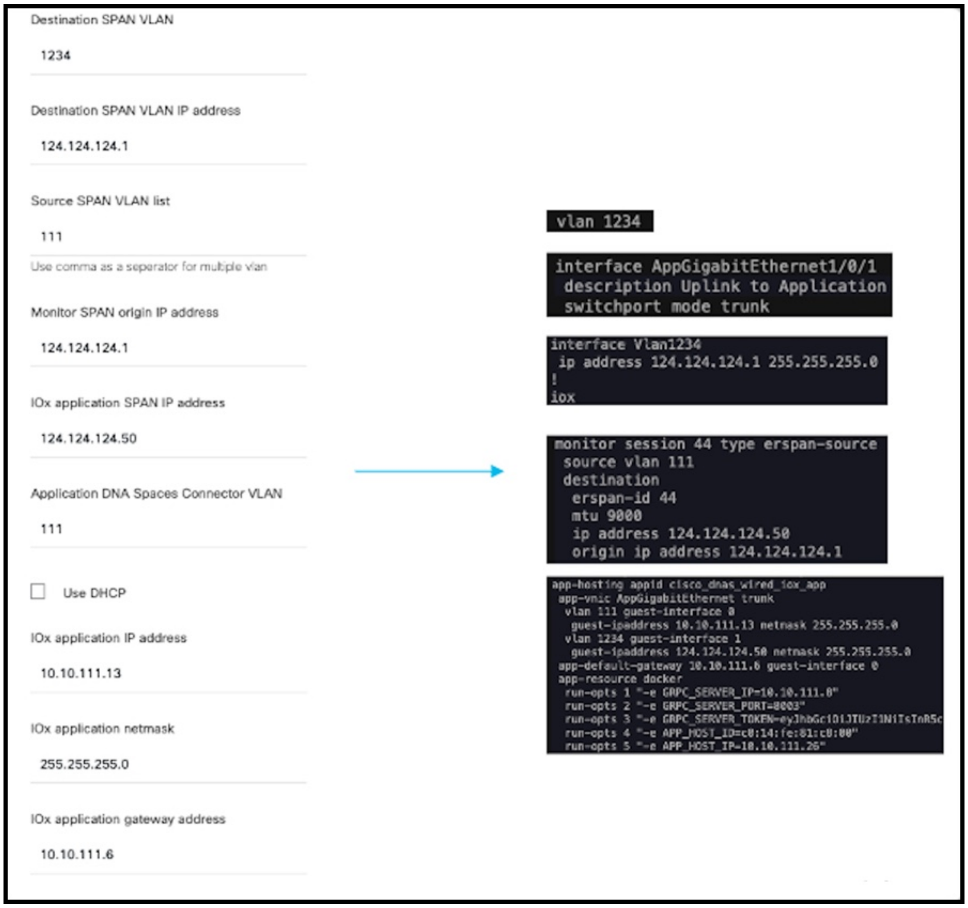
Figure 185: Sample Configuration



Step 10 Click **Configure**.

The configurations are deployed on the switch. The following diagram shows the corresponding CLI commands you can use in place of the GUI configuration.

Figure 186: GUI-Command Line Mapping



Destination SPAN VLAN
1234

Destination SPAN VLAN IP address
124.124.124.1

Source SPAN VLAN list
111
Use comma as a seperator for multiple vlan

Monitor SPAN origin IP address
124.124.124.1

IOx application SPAN IP address
124.124.124.50

Application DNA Spaces Connector VLAN
111

□ Use DHCP

IOx application IP address
10.10.111.13

IOx application netmask
255.255.255.0

IOx application gateway address
10.10.111.6

```
vlan 1234
```

```
interface AppGigabitEthernet1/0/1
 description Uplink to Application
 switchport mode trunk
```

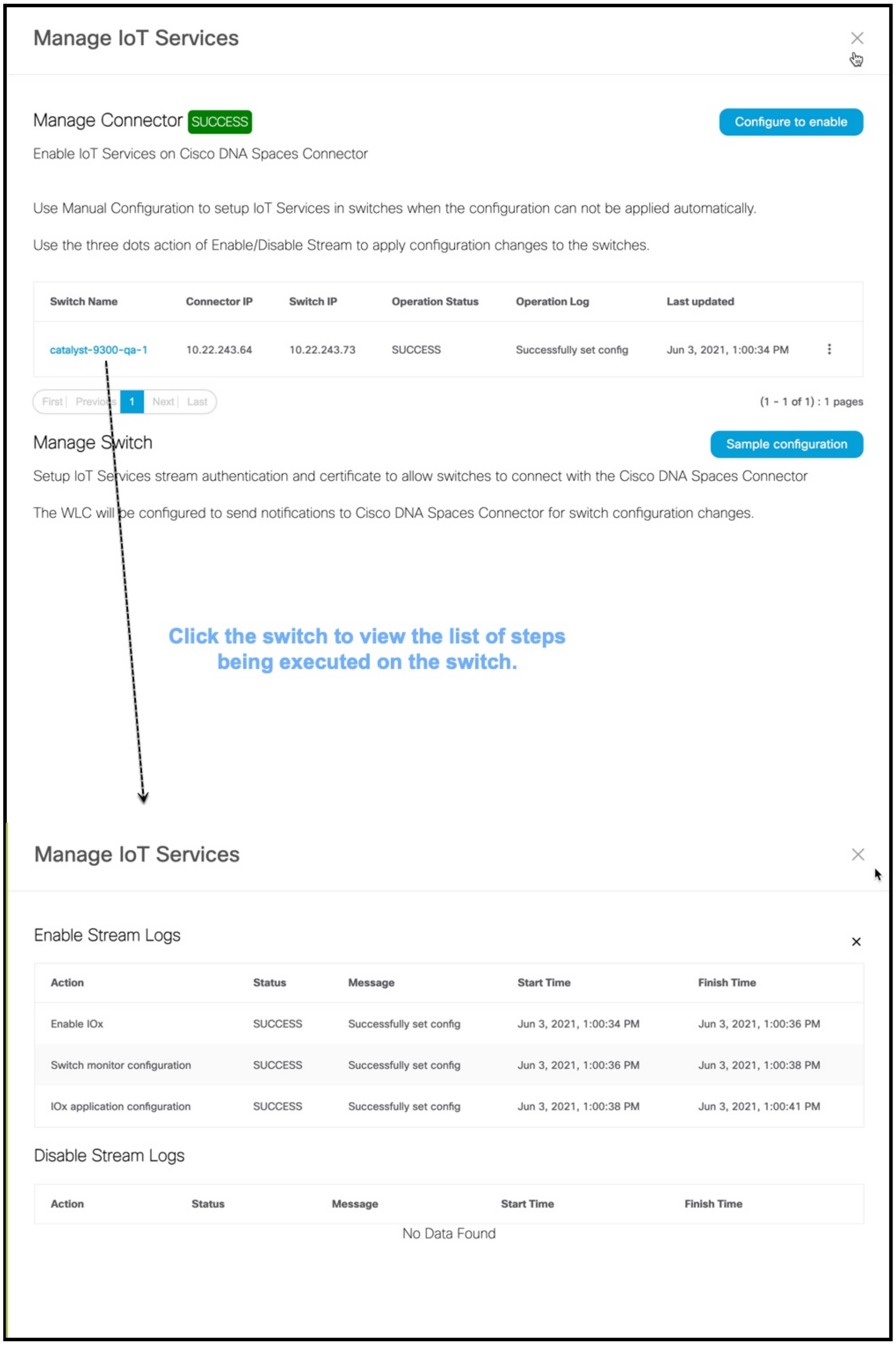
```
interface Vlan1234
 ip address 124.124.124.1 255.255.255.0
!
iox
```

```
monitor session 44 type erspan-source
 source vlan 111
 destination
  erspan-id 44
  mtu 9000
  ip address 124.124.124.50
  origin ip address 124.124.124.1
```

```
app-hosting appid cisco_dnas_wired_iox_app
 app-vnic AppGigabitEthernet trunk
  vlan 111 guest-interface 0
   guest-ipaddress 10.10.111.13 netmask 255.255.255.0
  vlan 1234 guest-interface 1
   guest-ipaddress 124.124.124.50 netmask 255.255.255.0
 app-default-gateway 10.10.111.6 guest-interface 0
 app-resource docker
  run-opts 1 "-e GRPC_SERVER_IP=10.10.111.0"
  run-opts 2 "-e GRPC_SERVER_PORT=8003"
  run-opts 3 "-e GRPC_SERVER_TOKEN=eyJhbGciOiJIUzI1NiIsInR5c
  run-opts 4 "-e APP_HOST_ID=c0:14:fe:81:c0:00"
  run-opts 5 "-e APP_HOST_IP=10.10.111.26"
```

Step 11 In the **Manage IoT Services** window that you are taken to, you can click on a name of the switch to see the list of steps executed on that switch.

Figure 187: Manage IoT Services



Manage IoT Services

Manage Connector SUCCESS

Enable IoT Services on Cisco DNA Spaces Connector

Use Manual Configuration to setup IoT Services in switches when the configuration can not be applied automatically.

Use the three dots action of Enable/Disable Stream to apply configuration changes to the switches.

Switch Name	Connector IP	Switch IP	Operation Status	Operation Log	Last updated
catalyst-9300-qa-1	10.22.243.64	10.22.243.73	SUCCESS	Successfully set config	Jun 3, 2021, 1:00:34 PM

(1 - 1 of 1) : 1 pages

Manage Switch

Setup IoT Services stream authentication and certificate to allow switches to connect with the Cisco DNA Spaces Connector

The WLC will be configured to send notifications to Cisco DNA Spaces Connector for switch configuration changes.

Click the switch to view the list of steps being executed on the switch.

Manage IoT Services

Enable Stream Logs

Action	Status	Message	Start Time	Finish Time
Enable IOx	SUCCESS	Successfully set config	Jun 3, 2021, 1:00:34 PM	Jun 3, 2021, 1:00:36 PM
Switch monitor configuration	SUCCESS	Successfully set config	Jun 3, 2021, 1:00:36 PM	Jun 3, 2021, 1:00:38 PM
IOx application configuration	SUCCESS	Successfully set config	Jun 3, 2021, 1:00:38 PM	Jun 3, 2021, 1:00:41 PM

Disable Stream Logs

Action	Status	Message	Start Time	Finish Time

No Data Found

Verify if Cisco Catalyst 9300 and 9400 Series Switches are Added to the Connector

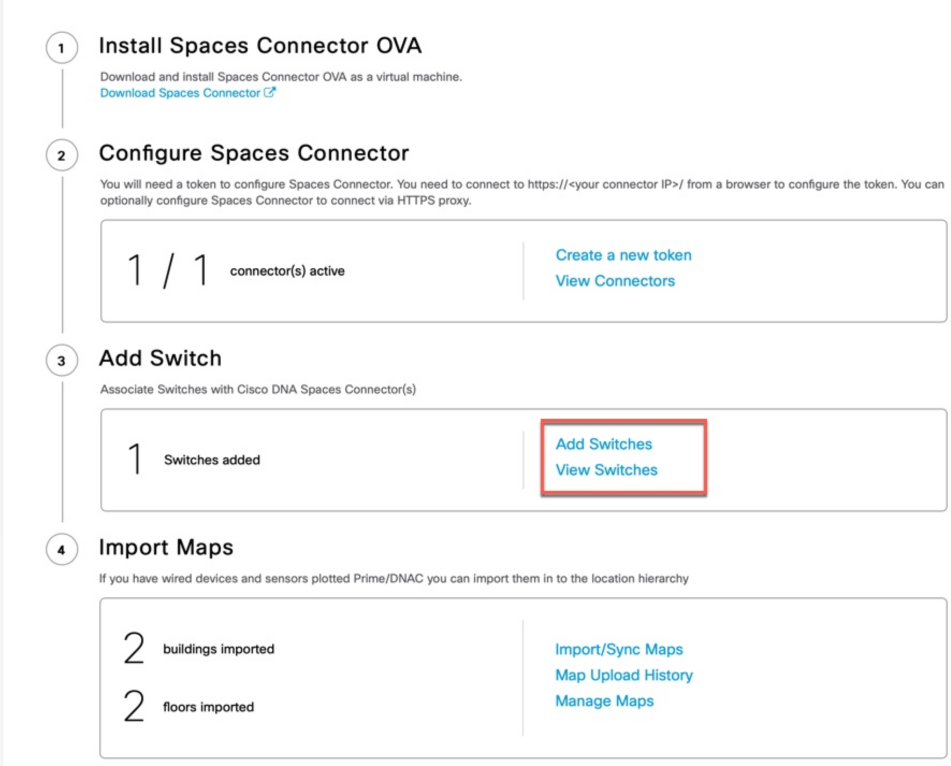
This procedure helps you verify if a Cisco Catalyst 9300 or 9400 Series Switches are deployed and active. This is a necessary prerequisite for proper functioning of Cisco Spaces: IoT Service (Wired).

Procedure

Step 1 In the Cisco Spaces dashboard left navigation pane, choose **Setup** > **Wired Network**.

Step 2 In the **Add Switch** area, click **View Switches**.

Figure 188: View Switches



1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.
Download Spaces Connector

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

1 / 1 connector(s) active

Create a new token
View Connectors

3 Add Switch

Associate Switches with Cisco DNA Spaces Connector(s)

1 Switches added

Add Switches
View Switches

4 Import Maps

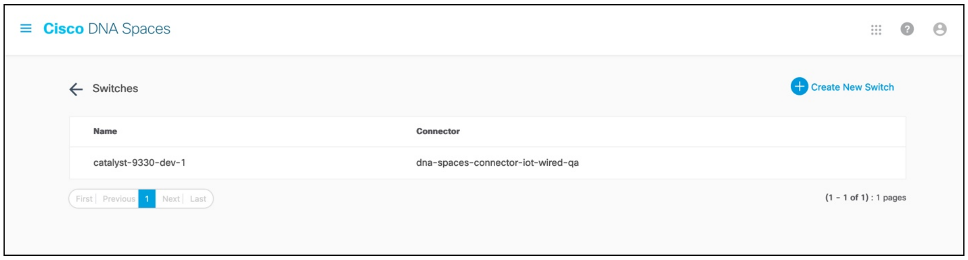
If you have wired devices and sensors plotted Prime/DNAC you can import them in to the location hierarchy

2 buildings imported
2 floors imported

Import/Sync Maps
Map Upload History
Manage Maps

Step 3 Ensure that a switch is listed here, and is connected to a Cisco Spaces: Connector.

Figure 189: View Switches



Name	Connector
catalyst-9330-dev-1	dna-spaces-connector-iot-wired-qa

(1 - 1 of 1) : 1 pages

CHAPTER 20

Hotspot Service

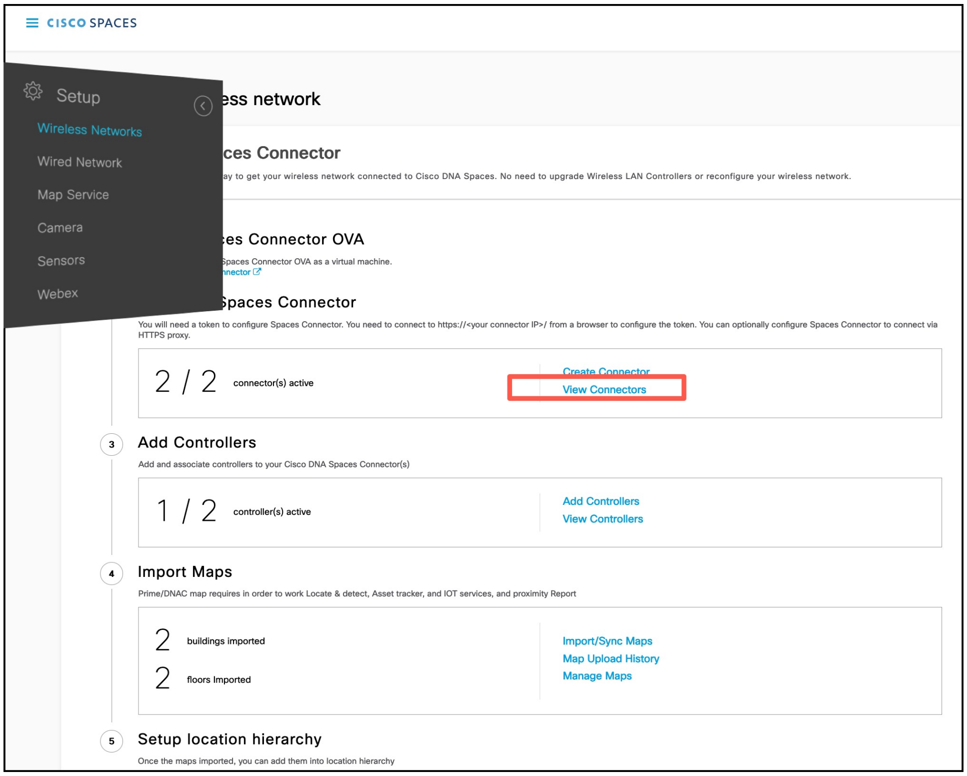
Configure Hotspot Service

Procedure

Step 1 In the Cisco Spaces dashboard left navigation pane, click **Setup** and choose **Wireless Networks**.

Step 2 In the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 190: View Connectors



ay to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.

Spaces Connector OVA as a virtual machine.

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

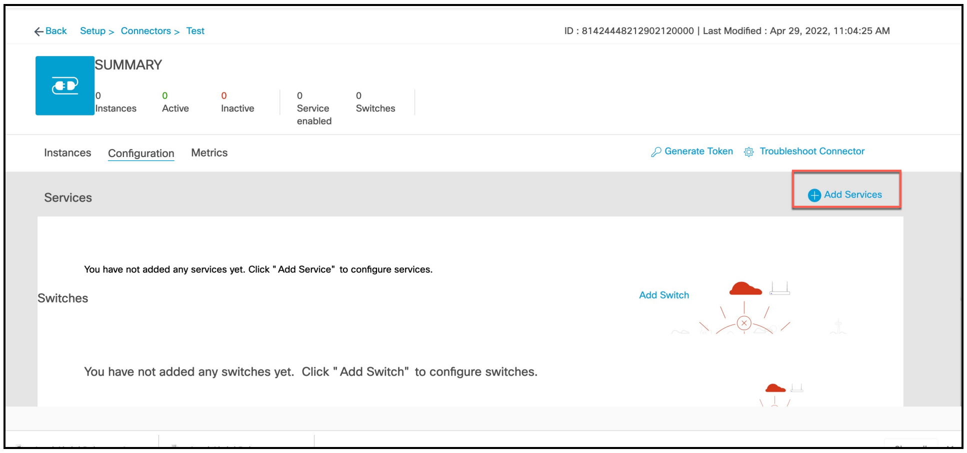
Add and associate controllers to your Cisco DNA Spaces Connector(s)

Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

Once the maps imported, you can add them into location hierarchy

Step 3 In the connector details window that is displayed, choose a connector and click **Add Services**.

Figure 191: Add Service



ID : 81424448212902120000 | Last Modified : Apr 29, 2022, 11:04:25 AM

You have not added any services yet. Click " Add Service" to configure services.

You have not added any switches yet. Click " Add Switch" to configure switches.

Step 4 In the **Add Service** window that is displayed, choose **hotspot** and click **Add**.

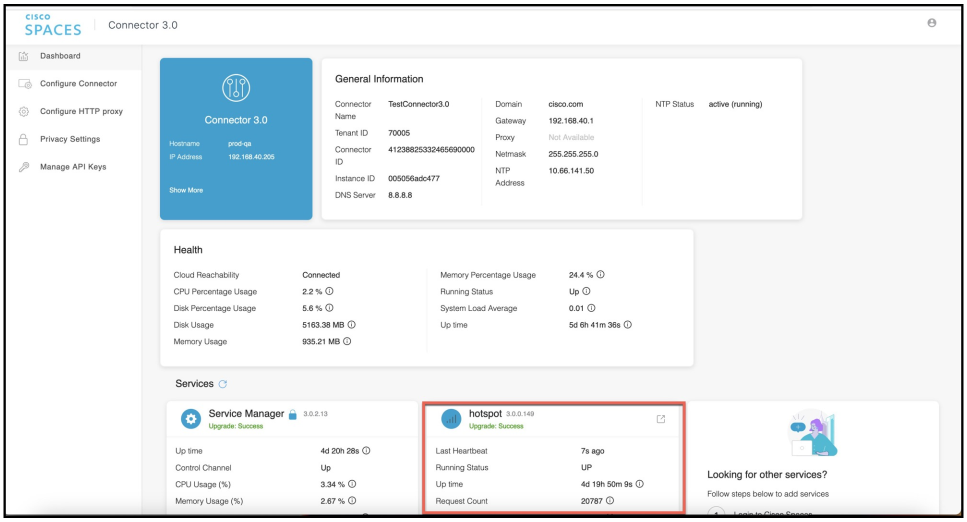
Note

service-manager is added by default.

In the **Connector Details** window, you can see that the number of services enabled has increased.

Connector Dashboard: Hotspot service

Figure 192: Hotspot Service



Connector 3.0

Hostname prod-qa
IP Address 192.168.40.205

General Information

Connector Name TestConnector3.0
Tenant ID 70005
Connector ID 41238825332465690000
Instance ID 005056adc477
DNS Server 8.8.8.8
Domain cisco.com
Gateway 192.168.40.1
Proxy Not Available
Netmask 255.255.255.0
NTP Address 10.66.141.50
NTP Status active (running)

Health

Cloud Reachability Connected
CPU Percentage Usage 2.2 %
Disk Percentage Usage 5.6 %
Disk Usage 5163.38 MB
Memory Usage 935.21 MB
Memory Percentage Usage 24.4 %
Running Status Up
System Load Average 0.01
Up time 5d 6h 41m 36s

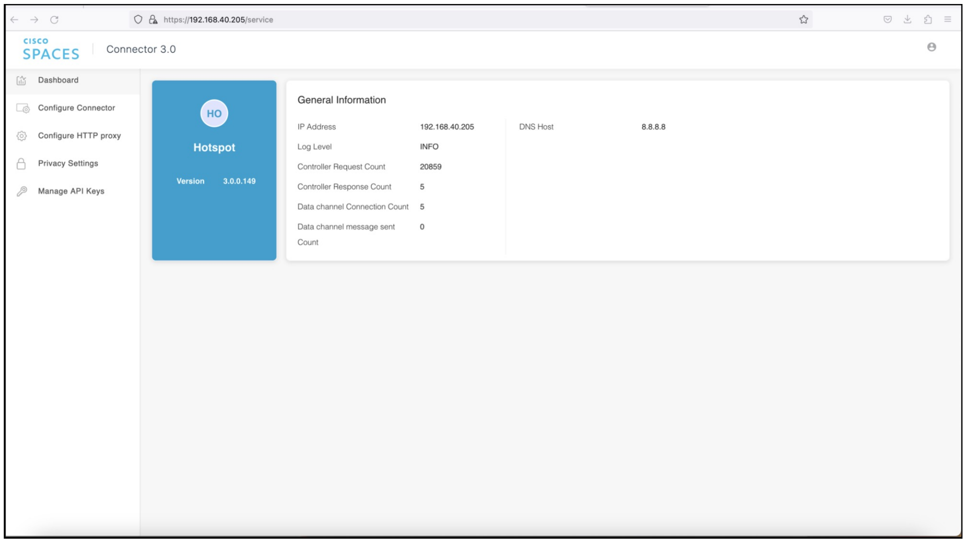
Services

Service Manager 3.0.2.13
Upgrade: Success
Up time 4d 20h 28s
Control Channel Up
CPU Usage (%) 3.34 %
Memory Usage (%) 2.67 %

hotspot 3.0.0.149
Upgrade: Success
Last Heartbeat 7s ago
Running Status UP
Up time 4d 19h 50m 9s
Request Count 20787

Looking for other services?
Follow steps below to add services

Figure 193: Hotspot Service: Details



Hotspot

Version 3.0.0.149

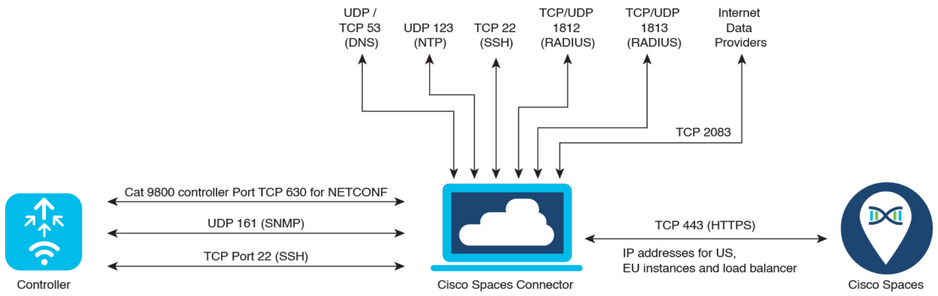
General Information

IP Address 192.168.40.205
Log Level INFO
Controller Request Count 20859
Controller Response Count 5
Data channel Connection Count 5
Data channel message sent Count 0
DNS Host 8.8.8.8

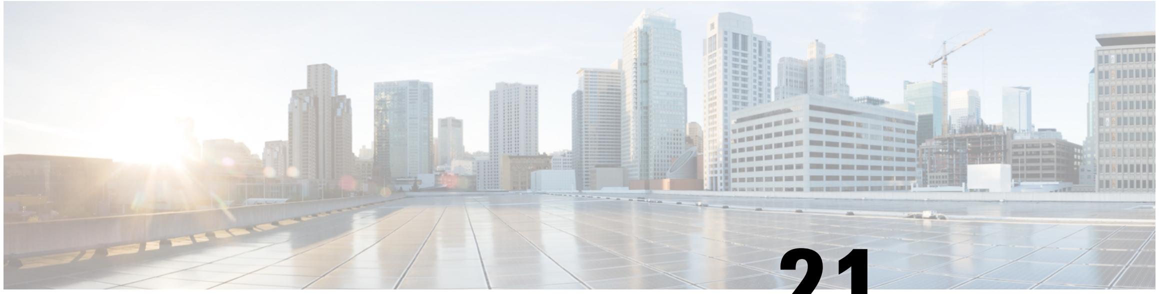
Open Ports for Hotspot Service

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

Figure 194: Open Ports for Hotspot Service



Test the connectivity between the connector and the wireless controller. See Configure and Test Connectivity between the Connector 3 and AireOS controller or Configure and Test the Connectivity between a Connector 3 and a Catalyst 9800 controller.



CHAPTER 21

Local Firehose

Local Firehose Service

The partner's location engine must be configured with the IP address of the connector.

If two connectors are configured in high-availability (either active-active or VIP-paired mode), ensure that both connector IP addresses are configured on the partner's location engine. In such a configuration, you can see that Radio Frequency Identification (RFID) tag information is received on both the connector channels, but Bluetooth Low Energy (BLE) tag information is received only on the Active connector channel.

Warning Do not configure the virtual IP address (VIP) of VIP-paired connectors on the partner's location engine.

IoT Service supports high availability only in the VIP-paired mode.

Note For creation and activation of a partner app, refer to the On-Prem Partner App

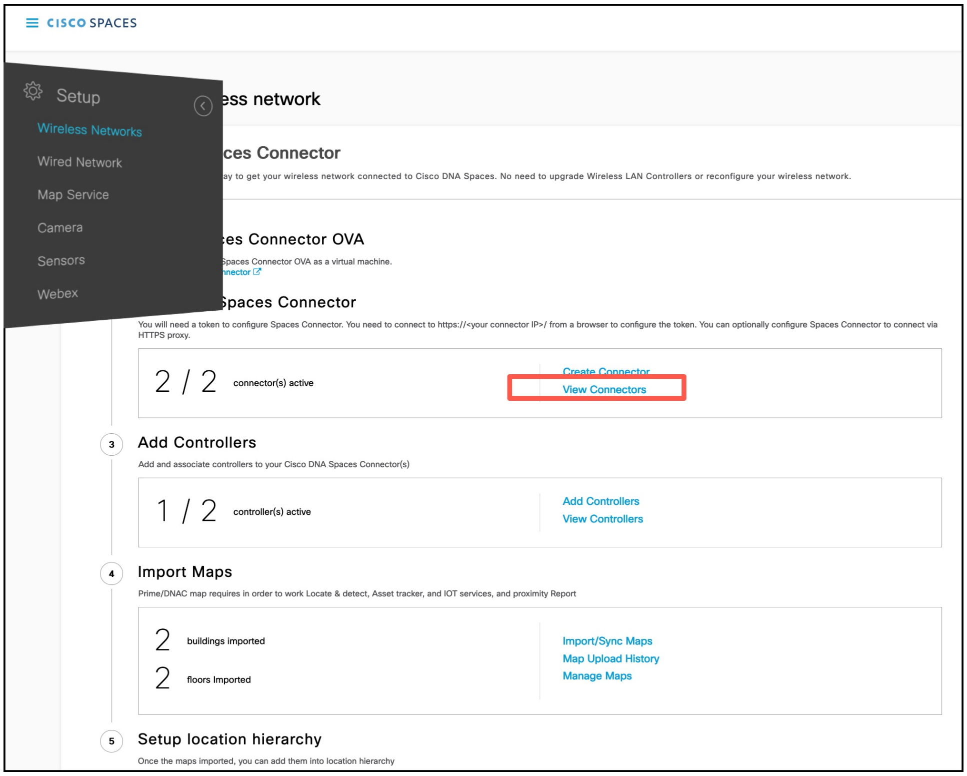
Configure Local Firehose Service

Procedure

Step 1 In the Cisco Spaces dashboard left navigation pane, click **Setup** and choose **Wireless Networks**.

Step 2 In the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 195: View Connectors



ay to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.

Spaces Connector OVA as a virtual machine.

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

2 / 2 connector(s) active

3 Add Controllers

Add and associate controllers to your Cisco DNA Spaces Connector(s)

1 / 2 controller(s) active

4 Import Maps

Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

2 buildings imported

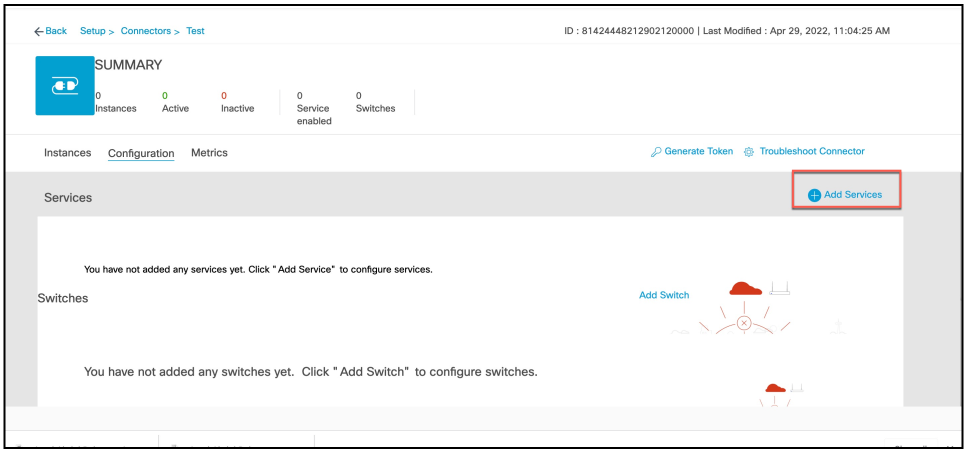
2 floors Imported

5 Setup location hierarchy

Once the maps imported, you can add them into location hierarchy

Step 3 In the connector details window that is displayed, choose a connector and click **Add Services**.

Figure 196: Add Service



ID : 81424448212902120000 | Last Modified : Apr 29, 2022, 11:04:25 AM

0 Instances | 0 Active | 0 Inactive | 0 Service enabled | 0 Switches

You have not added any services yet. Click " Add Service" to configure services.

You have not added any switches yet. Click " Add Switch" to configure switches.

Step 4 In the **Add Service** window that is displayed, choose **local-firehose** and click **Add**.

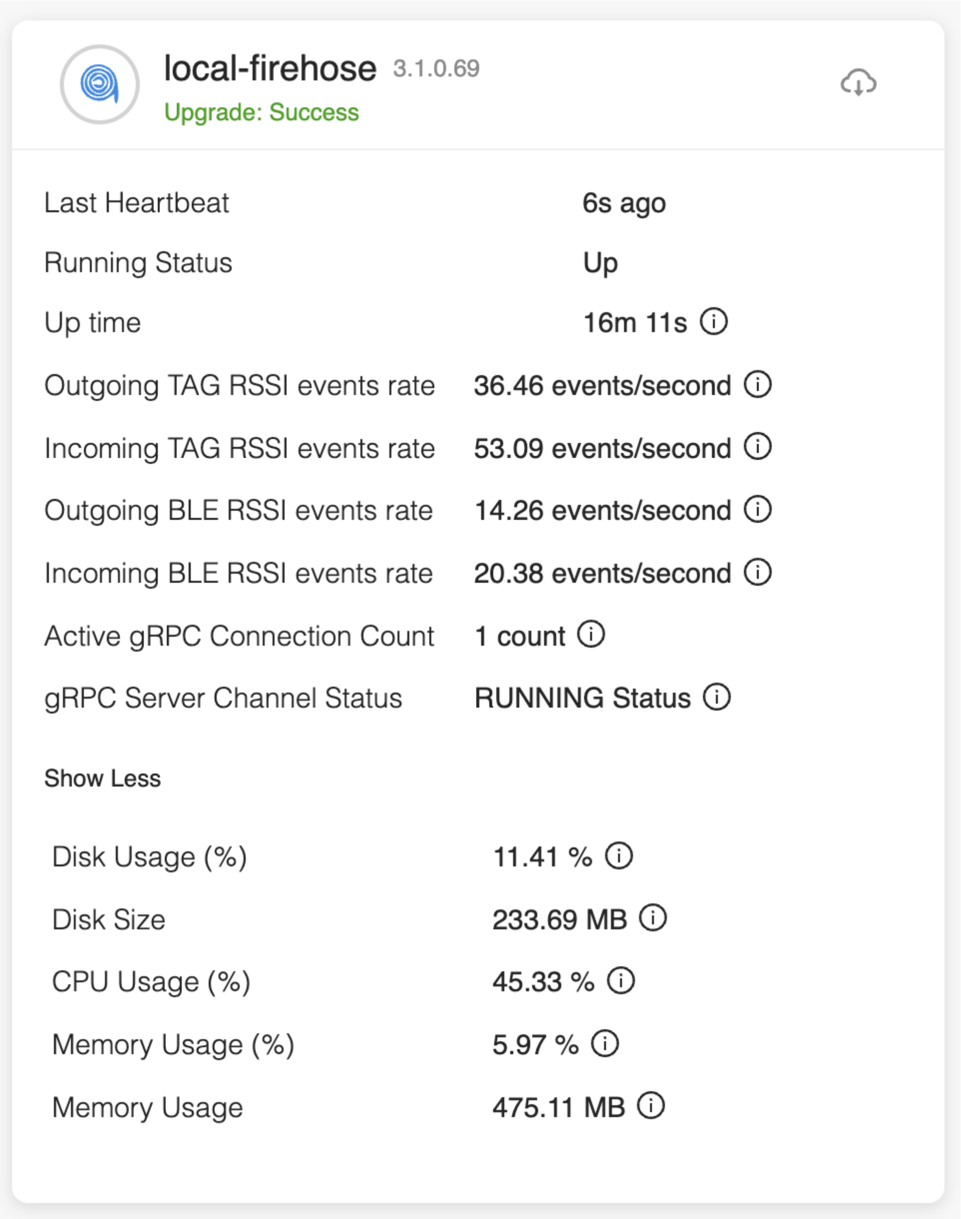
Note

To receive events such as Device_RSSI for Received Signal Strength Indicator (RSSI)-based tags and Device_BLE events for Bluetooth Low Energy (BLE) tags, ensure that **location** and **iot-services** services are also added.

You can see that the number of services enabled has increased.

Step 5 Login to the Connector GUI. Scroll downwards to the **local-firehose** tile. Verify if the running status is **Up**.

Figure 197: local-firehose



local-firehose 3.1.0.69

Upgrade: Success

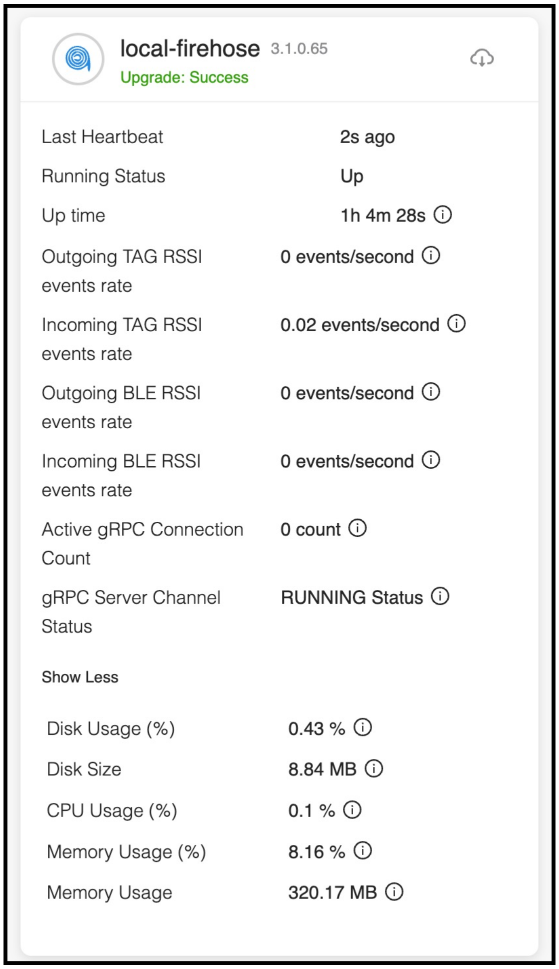
Last Heartbeat	6s ago
Running Status	Up
Up time	16m 11s
Outgoing TAG RSSI events rate	36.46 events/second
Incoming TAG RSSI events rate	53.09 events/second
Outgoing BLE RSSI events rate	14.26 events/second
Incoming BLE RSSI events rate	20.38 events/second
Active gRPC Connection Count	1 count
gRPC Server Channel Status	RUNNING Status

Show Less

Disk Usage (%)	11.41 %
Disk Size	233.69 MB
CPU Usage (%)	45.33 %
Memory Usage (%)	5.97 %
Memory Usage	475.11 MB

Connector Dashboard: Local Firehose Service

Figure 198: Local firehose service: Details on the Connector



local-firehose 3.1.0.65

Upgrade: Success

Last Heartbeat 2s ago

Running Status Up

Up time 1h 4m 28s ⓘ

Outgoing TAG RSSI events rate 0 events/second ⓘ

Incoming TAG RSSI events rate 0.02 events/second ⓘ

Outgoing BLE RSSI events rate 0 events/second ⓘ

Incoming BLE RSSI events rate 0 events/second ⓘ

Active gRPC Connection Count 0 count ⓘ

gRPC Server Channel Status RUNNING Status ⓘ

Show Less

Disk Usage (%) 0.43 % ⓘ

Disk Size 8.84 MB ⓘ

CPU Usage (%) 0.1 % ⓘ

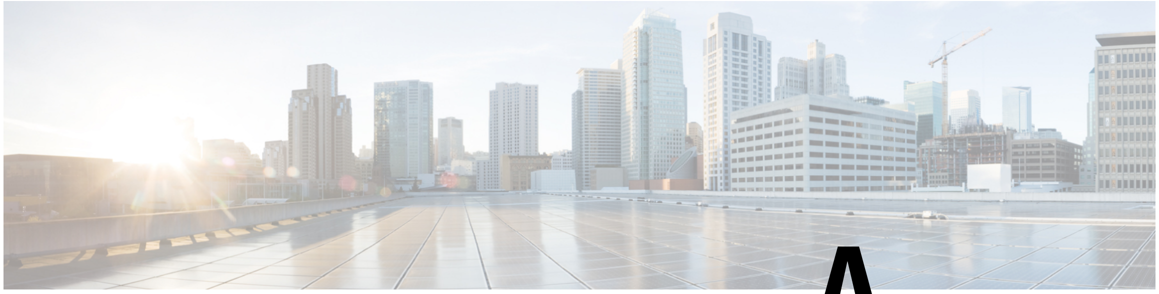
Memory Usage (%) 8.16 % ⓘ

Memory Usage 320.17 MB ⓘ

Table 9: Local Firehose Service Metrics

Display Field	Information
Active gRPC connection count	Number of connections from the partner's location engine
Outgoing TAG RSSI events rate	Number of RFID RSSI events sent from local-firehose-service to the partner's location engine
Incoming TAG RSSI events rate	Number of Radio Frequency Identification (RFID) Received Signal Strength Indicator (RSSI) events received from the location-service to local-firehose-service

Display Field	Information
Outgoing BLE RSSI events rate	Number of BLE RSSI Events sent from local-firehose-service to partner's location engine
Incoming BLE RSSI events rate	Number of Bluetooth Low Energy (BLE) RSSI Events received from iot-service to local-firehose- service



APPENDIX A

Connect Connector to Cisco AireOS Wireless Controller

Configure and Test Connectivity Between a Connector and AireOS Controller

Before you begin

- Deploy a connector OVA and activate it using a token from Cisco Spaces.
- Ensure that the IP address of a Cisco AireOS Wireless Controller is reachable from the Cisco Spaces: Connector.

Restriction

- In the context of CSCvk38081, we recommend that you do not add connector on the same subnet as the dynamic interface of the AireOS controller. However, if you cannot follow this recommendation, you can add the AireOS controller to connector and configure all the SNMP queries to the IP address of the dynamic interface of the controller.
- We also recommend that you do not add connector on the same subnet as the service port of the AireOS controller. However, if you cannot follow this recommendation, you can add the AireOS controller to connector and configure all the SNMP queries to the IP address of the service port of the controller.
- This restriction is a result of a limitation in the AireOS controller. While SNMP queries are usually made to the management IP address, the SNMP response packets are returned with a source IP address field that is configured with the IP address of the dynamic interface or source port.

Procedure

Step 1 Log in to **Cisco Spaces**.

Note
The Cisco Spaces URL is region-dependent.

Step 2 In the Cisco Spaces dashboard, choose **Setup** > **Wireless Networks**.

Step 3 Expand the **Connect via Spaces Connector** area using the respective drop-down arrow to display a list of steps.

Step 4 To test the connectivity from the Connector to an existing AireOS controller, click **View Controllers** in the **Step 3** area, and do the following steps:

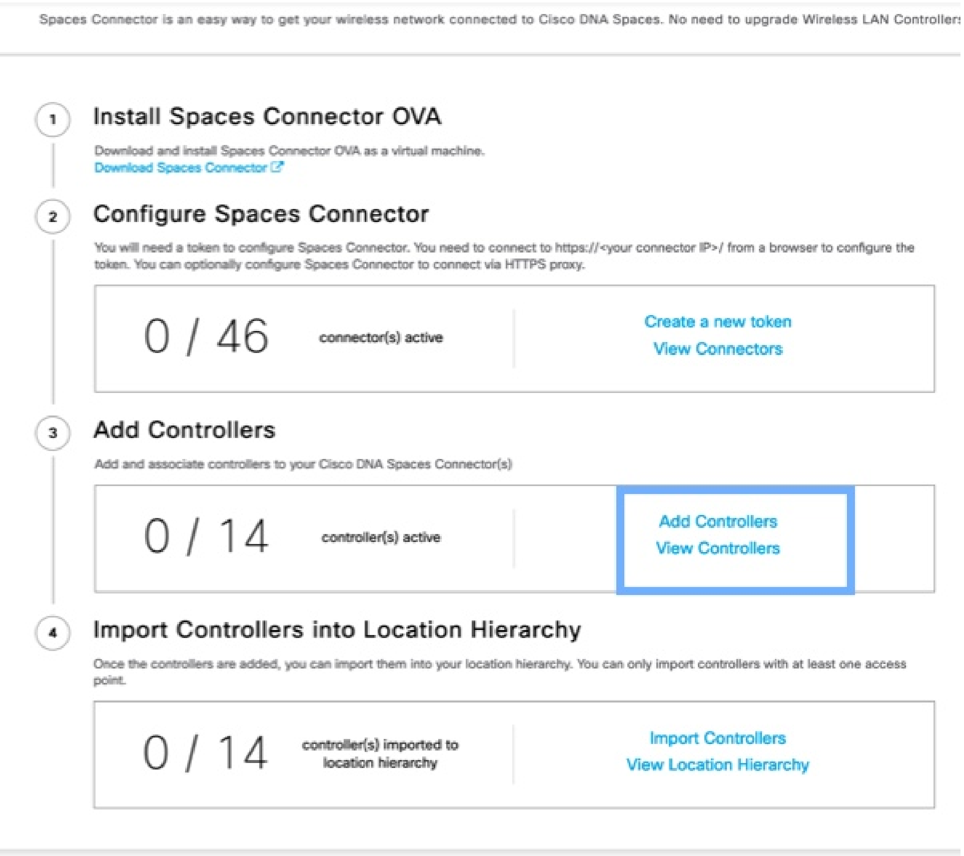
a) Click the pencil icon to edit an AireOS controller.

b) Choose an active Connector from the **Connector** drop-down list to enable the **Test Connectivity** button.

c) Go to this step to test the connectivity to an existing AireOS controller.

Step 5 To add a new AireOS controller, click **Add Controllers** from the **Step 3** area.

Figure 199: Add a New AireOS controller



Spaces Connector is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controller:

1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.
Download Spaces Connector

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

0 / 46 connector(s) active

Create a new token
View Connectors

3 Add Controllers

Add and associate controllers to your Cisco DNA Spaces Connector(s)

0 / 14 controller(s) active

Add Controllers
View Controllers

4 Import Controllers into Location Hierarchy

Once the controllers are added, you can import them into your location hierarchy. You can only import controllers with at least one access point.

0 / 14 controller(s) imported to location hierarchy

Import Controllers
View Location Hierarchy

Step 6 From the **Connector** drop-down list, choose a Connector.

Step 7 Enter the **Controller IP** address and **Controller Name**, and from the **Controller Type** drop-down list, choose **WLC (AireOS)** to connect to an AireOS controller.

Step 8 From the **Controller SNMP Version** drop-down list, choose the SNMP version of the AireOS controller.

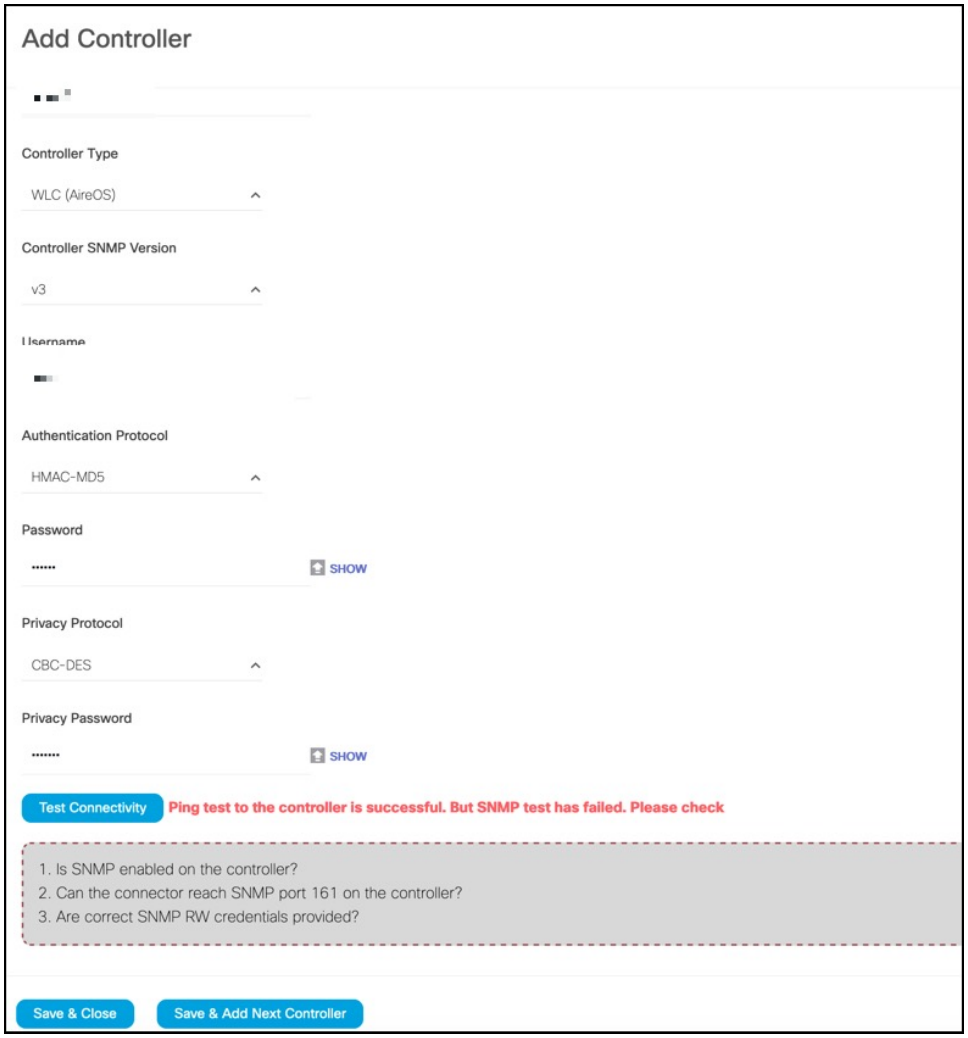
- If you choose the **SNMP** version as **v2C**, specify the SNMP read-write community.

- If you choose the **SNMP** version as **v3**, specify the SNMP v3 version username, password, and authentication protocol credentials. Ensure that SNMP v3 has read-write permissions in the AireOS controller.

Note

Both SNMP v2c and SNMP v3 must have read-write permission in the AireOS controller to register the Connector certificate in the AireOS controller. The Connector doesn't support SNMP v1.

Figure 200: Add a New AireOS controller



Add Controller

[redacted]

Controller Type

WLC (AireOS)

Controller SNMP Version

v3

Username

[redacted]

Authentication Protocol

HMAC-MD5

Password

••••••

Privacy Protocol

CBC-DES

Privacy Password

•••••••

Ping test to the controller is successful. But SNMP test has failed. Please check

1. Is SNMP enabled on the controller?
2. Can the connector reach SNMP port 161 on the controller?
3. Are correct SNMP RW credentials provided?

Step 9 Click **Test Connectivity** . Connector issues ping and SNMP commands to check the connectivity to Cisco Spaces using the credentials provided.

Note

Test Connectivity is enabled only when an active Connector is chosen.

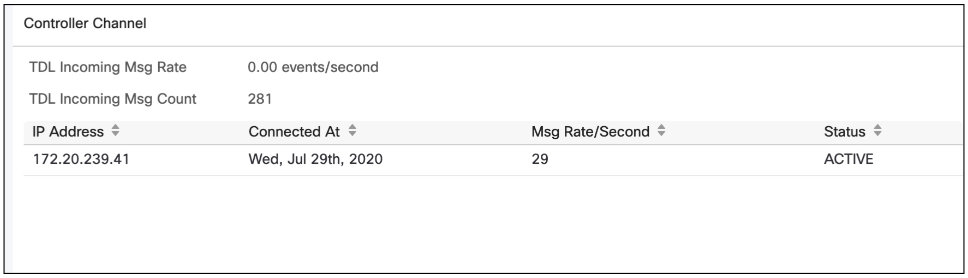
Table 10: Error Description

Status of PING	Status of SNMP Test	Displayed Test Connectivity Message
SUCCESSFUL	SUCCESSFUL	Connectivity test is successful

Status of PING	Status of SNMP Test	Displayed Test Connectivity Message
SUCCESSFUL	FAILED	Ping test is successful, but SNMP test failed. Check the following: Ping test to the AireOS controller is successful, but SNMP test has failed. Check the following: • If you are using v2c SNMP, check if the community strings are valid. • If you are using v3 SNMP, check if the credentials are correct. • Check if v2c or v3 mode is enabled in the controller.
FAILED	FAILED	Both ping and SSH test to the AireOS controller have failed. Check the following: • Is there IP connectivity between a Connector and a controller? • Is SSH enabled on the AireOS controller? • Is the SSH port 22 of the AireOS controller reachable from the Connector? • Have you provided accurate SSH credentials? • Is AAA enabled with local authentication? • Are you using an interface that is *not* the wireless management interface for NMSP and SSH connectivity?

Step 10 Click **Save**, and then click **Close**.
You can see the new Catalyst 9800 controller in the **Controller Channel** area of the Connector GUI. The Catalyst 9800 controller that is connected successfully to the Connector appears as **Active**. It takes approximately five minutes for the wireless controller to change to the **Active** state. Refresh your window to view the status change. The added Catalyst 9800 controller is also listed in the **Controller Channel** area of the Connector.

Figure 201: Details of the Catalyst 9800 controller



Controller Channel

TDL Incoming Msg Rate 0.00 events/second

TDL Incoming Msg Count 281

IP Address	Connected At	Msg Rate/Second	Status
172.20.239.41	Wed, Jul 29th, 2020	29	ACTIVE

What to do next

You can import the added Catalyst 9800 controller to the Cisco Spaces location hierarchy.

APPENDIX B

Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers

Configure and Test the Connection Between Connector and Catalyst 9800 Controller

Before you begin

1. Deploy a connector OVA and activate it using a token from Cisco Spaces.
2. Note down the IP address of a Catalyst 9800 controller that is reachable from the Cisco Spaces: Connector.
3. On the Catalyst 9800 controller CLI, enter the config mode and enable AAA with local authentication using the **aaa authorization exec default local** and **aaa authentication login default local** commands.

   On the Catalyst 9800 controller CLI, run the following command in the **enable** mode:

   ```
   show run | sec  aaa
   ```

   From the output that is displayed, copy the configuration for **aaa authorization exec default**. In the **config** mode, append the configuration for local authentication to the copied configuration and configure the appended configuration.

   For instance, if the output displays **aaa authorization exec default group dnac-network-tacacs-group**, the appended configuration is **aaa authorization exec default group dnac-network-tacacs-group local**. This ensures that the existing configuration is not overwritten.

Note

Any certificate imported to the controller for Wireless Management Interface(WMI) that has been signed with a signature algorithm weaker than SHA-256 is not supported. Verify your certificate before adding the controller using the **show wireless management trustpoint** command.

```
Device# show wireless management trustpoint
Trustpoint Name  : manual_certs                <<<<<<<<<<<< Get the name of the trustpoint
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : f7900ae5e35473b5e32343d4ea9556176e71a63a
Private key Info : Available
FIPS suitability : Not Applicable
```

You can also verify the same using the **show crypto pki certificates verbose** command. In the output displayed, verify the content of the following fields (also highlighted in bold in the output):

- **Signature Algorithm**: Ensure that nothing less than SHA-256 is displayed here.
- **Associated Trustpoints**: Ensure that the signature algorithm is for the required trustpoint.

.

```
Device# show crypto pki certificates verbose
...
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 00AE697E4C7EEBE3E4
  Certificate Usage: Signature
  Issuer:
    e=support@vwlc.com
    cn=CA-vWLC-manual
    ou=Cisco DevX Wireless Simulator
    o=Cisco Virtual Wireless LAN Controller
    l=San Jose
    st=California
    c=US
  Subject:
    e=support@vwlc.com
    cn=CA-vWLC-manual
    ou=Cisco DevX Wireless Simulator
    o=Cisco Virtual Wireless LAN Controller
    l=San Jose
    st=California
    c=US
  Validity Date:
    start date: 18:08:16 Pacific Aug 27 2019
    end   date: 18:08:16 Pacific Aug 24 2029
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (4096 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: 623E2FA4 7F908675 5422FF3C 257179F9
  Fingerprint SHA1: 05E3D17C 841AA033 C503D7BA 443CC2C2 1C510538
  X509v3 extensions:
    X509v3 Key Usage: 6000000
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 1AE21C76 1B86780A B4E0AE43 205052BE EA0E4B4A
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 1AE21C76 1B86780A B4E0AE43 205052BE EA0E4B4A
    Authority Info Access:
  Cert install time: 23:51:54 Pacific Jun 7 2024
  Associated Trustpoints: manual_certs
  Storage: nvram:supportvwlcc#E3E4CA.cer
”
...
```

Procedure

Step 1 Login to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, choose **Setup** > **Wireless Networks**.

Step 3 Expand the **Connect via Spaces Connector** area using the respective drop-down arrow to display a list of steps.

Step 4 To test the connectivity from the Connector to an existing Catalyst 9800 controller, click **View Controllers** in the **Step 3** Area.

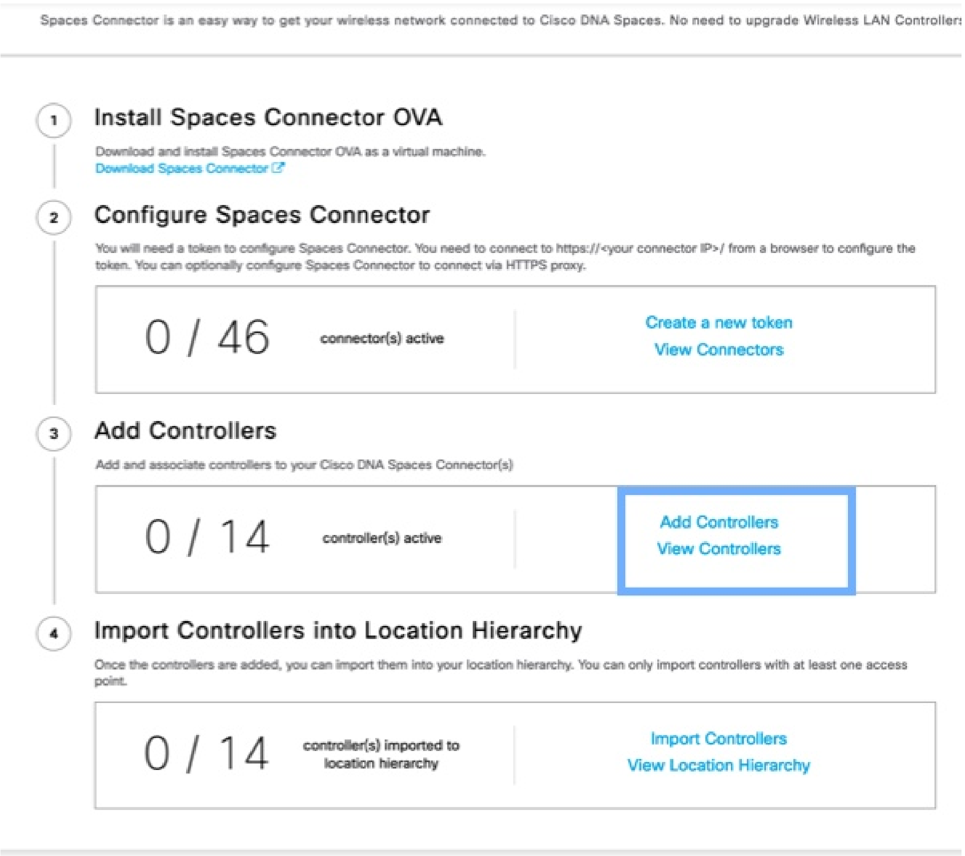
a) Click the pencil icon to edit a Catalyst 9800 controller.

b) Choose an active Connector from the **Connector** drop-down list to enable the **Test Connectivity** button.

c) Go to this step to test the connectivity to an existing AireOS controller.

Step 5 To add a new Catalyst 9800 controller, click **Add Controllers** from the **Step 3** Area.

Figure 202: Add a New Catalyst 9800 controller



Spaces Connector is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controller:

1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.

Download Spaces Connector

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

0 / 46 connector(s) active

Create a new token

View Connectors

3 Add Controllers

Add and associate controllers to your Cisco DNA Spaces Connector(s)

0 / 14 controller(s) active

Add Controllers

View Controllers

4 Import Controllers into Location Hierarchy

Once the controllers are added, you can import them into your location hierarchy. You can only import controllers with at least one access point.

0 / 14 controller(s) imported to location hierarchy

Import Controllers

View Location Hierarchy

Step 6 From the **Connector** drop-down list, choose a Connector.

Step 7 Enter the **Controller IP** address, **Controller Name**, and from the **Controller Type** drop-down list, choose **Catalyst WLC** to connect to a Cisco Catalyst 9800 Series Wireless Controllers.

Note

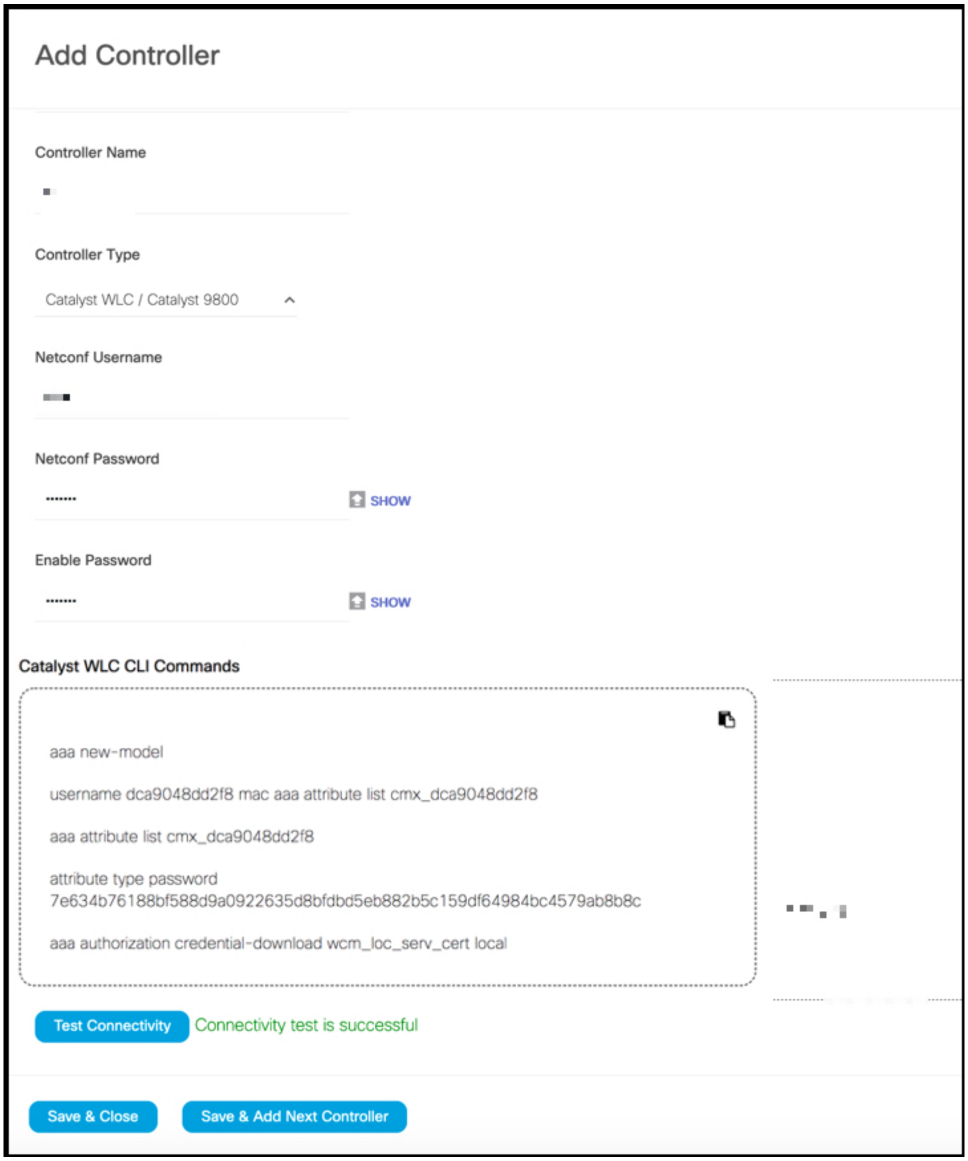
Ensure that the Controller IP address is not in the same subnet as the docker service network. You can validate this from the Connector CLI, where you can issue the **connectorctl dockersubnet show** command to verify the subnets used.

Step 8 Do one of the following:

- Enter **Netconf username**, **Netconf password**, and **Enable password**. This choice allows the Connector to recover gracefully from NMSP drops and push a fresh configuration to the Catalyst 9800 controller whenever required. If you have not configured an **enable** password in Catalyst 9800 controller you can skip configuring the **Enable password** in this step.
- Copy the configuration commands in the **Catalyst WLC CLI commands** section and run them manually on the Catalyst 9800 controller CLI.

Step 9 (Optional) Run the PING and SSH functionalities to test the reachability to the Catalyst 9800 controller and the credentials by clicking **Test Connectivity**. Note that **Test Connectivity** is available only for an active Connector.

Figure 203: Add a New Catalyst 9800 controller



Add Controller

Controller Name

[redacted]

Controller Type

Catalyst WLC / Catalyst 9800

Netconf Username

[redacted]

Netconf Password

•••••••

Enable Password

•••••••

Catalyst WLC CLI Commands

```
aaa new-model

username dca9048dd2f8 mac aaa attribute list cmx_dca9048dd2f8

aaa attribute list cmx_dca9048dd2f8

attribute type password
7e634b76188bf588d9a0922635d8bfdbd5eb882b5c159df64984bc4579ab8b8c

aaa authorization credential-download wcm_loc_serv_cert local
```

[redacted]

Connectivity test is successful

Table 11: Error Description

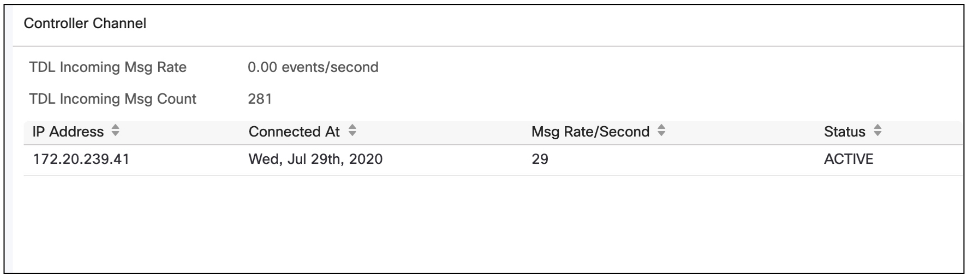
Status of PING	Status of SSH Credential Test	Meaning of status message combination and possible checks.
SUCCESSFUL	SUCCESSFUL	Connectivity test is successful.

Status of PING	Status of SSH Credential Test	Meaning of status message combination and possible checks.
SUCCESSFUL	FAILED	Ping test to the Catalyst 9800 controller is successful. But SSH test has failed. Check the following: **a.** Is SSH enabled on the controller? **b.** Is the SSH port 22 of the Catalyst 9800 controller reachable from the Connector? **c.** Have you provided accurate SSH read-write credentials?
FAILED	SUCCESSFUL	Connectivity test is successful.
FAILED	FAILED	Both Ping and SSH test to the Catalyst 9800 controller have failed. Check the following: **a.** Is there IP connectivity between Connector and controller? **b.** Is SSH enabled on the Catalyst 9800 controller? **c.** Is the SSH port 22 of the Catalyst 9800 controller reachable from the Connector? **d.** Have you provided accurate SSH credentials? **e.** Is AAA enabled with local authentication? **f.** Are you using an interface that is NOT the wireless management interface for NMSP and SSH connectivity?

Step 10 Click **Save**, and then click **Close**.

You can see the new Catalyst 9800 controller in the **Controller Channel** area of the Connector GUI. The Catalyst 9800 controller that is connected successfully to the Connector appears as **Active**. It takes approximately five minutes for the wireless controller to change to the **Active** state. Refresh your window to view the status change. The added Catalyst 9800 controller is also listed in the **Controller Channel** area of the Connector.

Figure 204: Details of the Catalyst 9800 controller



Controller Channel

TDL Incoming Msg Rate 0.00 events/second

TDL Incoming Msg Count 281

IP Address	Connected At	Msg Rate/Second	Status
172.20.239.41	Wed, Jul 29th, 2020	29	ACTIVE

You can multiple Catalyst 9800 controllers to a Connector.

What to do next

You can import the added Catalyst 9800 controller to the Cisco Spaces location hierarchy.

APPENDIX C

Connect Connector to Cisco Catalyst 9300 or 9400 Series Switches

Connecting a connector to Cisco Catalyst 9300 and 9400 Series Switches

For certain use cases such as energy utilization or occupancy, the following steps are sufficient (and there is no further need to configure the IOX app). However, ensure that location services are enabled.

Before you begin

- Deploy a connector OVA and activate it using a token from Cisco Spaces.
- The IP address of a Cisco Catalyst 9300 and 9400 Series Switches that is reachable from the Cisco Spaces: Connector.
- Test the Netconf commands on the Cisco Catalyst 9300 and 9400 Series Switches

SUMMARY STEPS

1. Login to Cisco Spaces.
2. In the Cisco Spaces dashboard, choose **Setup** > **Wired Networks**.
3. From the **Step 3: Add Switches** area, click **Add Switch**.
4. From the **Add Switches** page, select the connector, enter a name to identify the switch, the switch IP address. **Netconf username**, **Netconf password**, and click the checkbox to acknowledge that you have tested these commands on the switch.
5. Click **Test** to see if the connection to the switch.
6. Do one of the following:
   - Click **Save & Add Next Switch**
   - Click **Save & Close**

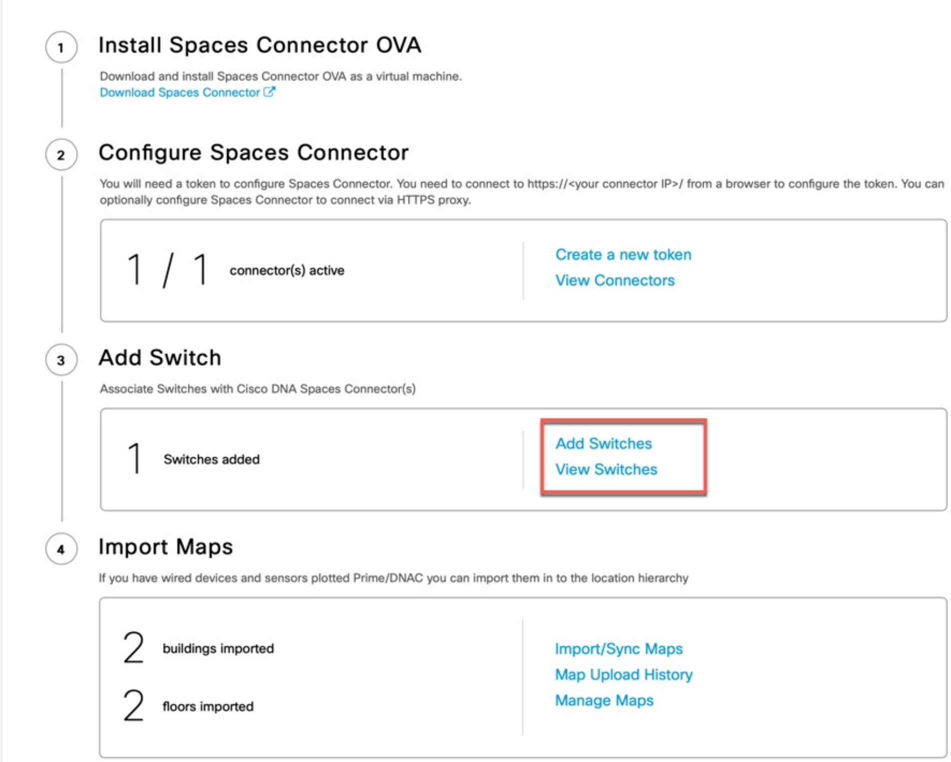
DETAILED STEPS

Procedure

Step 1 Login to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, choose **Setup** > **Wired Networks**.

Step 3 From the **Step 3: Add Switches** area, click **Add Switch**.



1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.

Download Spaces Connector

2 Configure Spaces Connector

You will need a token to configure Spaces Connector. You need to connect to https://<your connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

1 / 1 connector(s) active

Create a new token

View Connectors

3 Add Switch

Associate Switches with Cisco DNA Spaces Connector(s)

1 Switches added

Add Switches

View Switches

4 Import Maps

If you have wired devices and sensors plotted Prime/DNAC you can import them in to the location hierarchy

2 buildings imported

2 floors imported

Import/Sync Maps

Map Upload History

Manage Maps

Figure 205:

Step 4 From the **Add Switches** page, select the connector, enter a name to identify the switch, the switch IP address. **Netconf username**, **Netconf password**, and click the checkbox to acknowledge that you have tested these commands on the switch.

Note

Ensure that the Controller IP address is not in the same subnet as the docker service network. You can validate this from the Connector CLI, where you can issue the **connectorctl dockersubnet show** command to verify the subnets used.

Step 5 Click **Test** to see if the connection to the switch.

Step 6 Do one of the following:

- Click **Save & Add Next Switch**
- Click **Save & Close**