Cisco Spaces: Connector 3 Configuration Guide

First Published: 2022-06-24

Last Modified: 2024-09-25

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

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

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

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

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

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

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

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

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

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

© 2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface vii

Audience vii

Conventions vii

Related Documentation viii

Communications, Services, and Additional Information viii

Cisco Bug Search Tool viii

Documentation Feedback ix

CHAPTER 1

Overview 1

Introduction to Connector 3 1

PART I

Getting Started 3

CHAPTER 2

Prerequisites 5

Prerequisites for Configuring Connector 3 5

Recommended Deployment Architecture 5

PART II

Configuration 7

CHAPTER 3

Initial Setup 9

Initial Setup of Cisco Spaces: Connector 9

Activating Connector 3 on Cisco Spaces 10

Upgrading the Connector from Cisco Spaces Dashboard 17

Upgrading the Connector Using CLI 21

CHAPTER 4

Cisco Spaces: Connector AMI 23

Launch Connector 3 as an EC2 Instance from AMI 23

CHAPTER 5 **Cisco Spaces: Connector: Azure VMware 33**

Cisco Spaces: Connector: Azure VMware 33

Creating an Azure VMware solution (or Private Cloud) 34

Creating an Azure Virtual Network 38

CHAPTER 6 **Cisco Spaces: Connector OVA 45**

Deploying the Connector 3 OVA (Single Interface) 45

Deploying the Cisco Spaces: Connector OVA (Dual Interface) 53

Using Snapshots for Backup 60

CHAPTER 7 **Cisco Spaces: Connector Hyper-V 63**

Creating a Virtual Switch 63

Downloading and Deploying HYPER-V 70

CHAPTER 8 **Connector on Cisco Spaces 81**

Activating Connector 3 on Cisco Spaces 81

Monitor the Status of Service Installation 88

CHAPTER 9 **Connector GUI 89**

Connector GUI 89

Configuring Privacy Settings 90

CHAPTER 10 **Proxy 91**

Configure a Proxy 91

Configure a Transparent Proxy 93

CHAPTER 11 **High Availability 97**

Configuring Connectors as VIP Paired 97

Connector Active-Active 102

Restrictions for Active-Active 102

Configuring Connectors in Active-Active 103

PART III **Troubleshooting** 107

CHAPTER 12 **Troubleshooting Tools** 109

Enable Debug Logs 109

Recovering a Lost Password 110

Monitor Service Metrics 110

CHAPTER 13 **Troubleshooting Scenarios** 113

Connectivity Issues Between Connector and Cisco Spaces 113

Unresponsive Connector, or Failure of SSH to Connector 116

Instance is Corrupted or Deleted 118

Service Crash, or Restart Services 118

Upgrade has Failed, or How To Forcibly Push Configurations to Instances 119

Weak SSH MAC Algorithms 119

Disable Weak MAC Algorithms 120

PART IV **Services** 123

CHAPTER 14 **Location Service** 125

Compatibility Matrix for Cisco Spaces: Connector: Location service 125

Open Ports for Location Service 129

CHAPTER 15 **IoT Service (Wireless)** 131

Overview of Cisco Spaces: IoT Service (Wireless) 131

Components of Cisco Spaces: IoT Service 131

Compatibility Matrix for IoT Service (Wireless) 134

Prerequisites of IoT Service (Wireless) 136

Open Ports for IoT Service (Wireless) 136

Configure IoT Service (Wireless) 136

Verify IoT Streams for Catalyst 9800 Controller 138

Verify Access Points 139

CHAPTER 16 **IoT Service (Wired)** 143

Overview 143
Overview of IoT Service (Wired) 143
Compatibility Matrix for IoT Service (Wired) 145
Prerequisites for Cisco Spaces: IoT Service (Wired) 145
Prerequisites for Cisco Spaces: IoT Service (Wired) 147
Open Ports for IoT service (wired) 150
Configure IoT Service (Wired) 151
Verify if Cisco Catalyst 9300 and 9400 Series Switches are Added to the Connector 160

CHAPTER 17 **Hotspot Service** 163
Configure Hotspot Service 163
Connector Dashboard: Hotspot service 165
Open Ports for Hotspot Service 165

CHAPTER 18 **Local Firehose** 167
Local Firehose Service 167
Configure Local Firehose Service 167
Connector Dashboard: Local Firehose Service 170

APPENDIX A **Connect Connector to Cisco AireOS Wireless Controller** 173
Configure and Test Connectivity Between a Connector and AireOS Controller 173

APPENDIX B **Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers** 179
Configure and Test the Connection Between Connector and Catalyst 9800 Controller 179

APPENDIX C **Connect Connector to Cisco Catalyst 9300 or 9400 Series Switches** 187
Connecting a connector to Cisco Catalyst 9300 and 9400 Series Switches 187

Preface

- Audience, on page vii
- Conventions, on page vii
- Related Documentation, on page viii
- Communications, Services, and Additional Information, on page viii

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: Connector3 Configuration Guide

Cisco Spaces: Connector3 Command Reference Guide

Release Notes for Cisco Spaces: Connector

Cisco Spaces: IoT Service Configuration Guide (Wireless)

Cisco Spaces: IoT Service Configuration Guide (Wired)

Communications, Services, and Additional Information

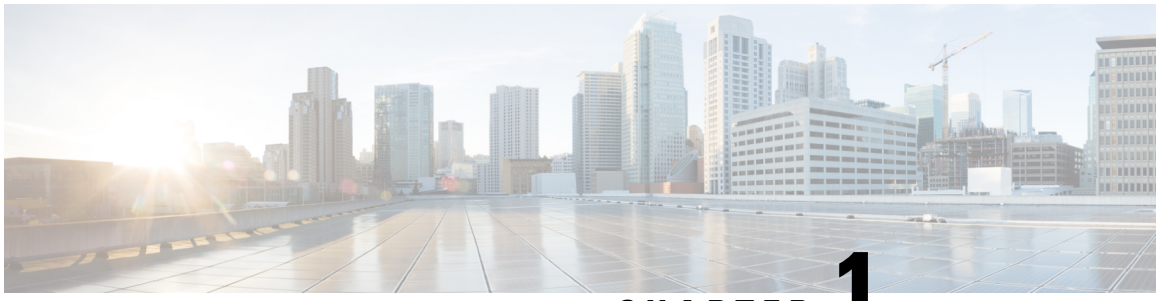
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class 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 **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

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 , on page 1

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.

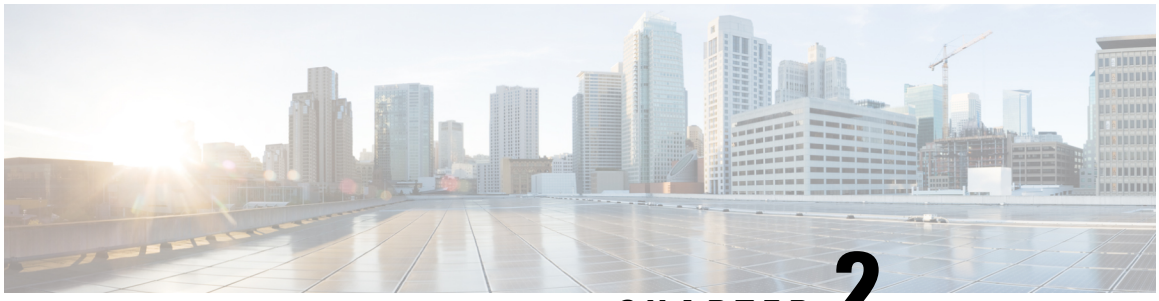
Note The term wireless controller is used in this document to collectively refer to the following:

- 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

- Prerequisites, on page 5



CHAPTER 2

Prerequisites

- Prerequisites for Configuring Connector 3, on page 5
- Recommended Deployment Architecture , on page 5

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

- 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: Standard option
- Minimum bandwidth required: 4 Mbps

Recommended Deployment Architecture

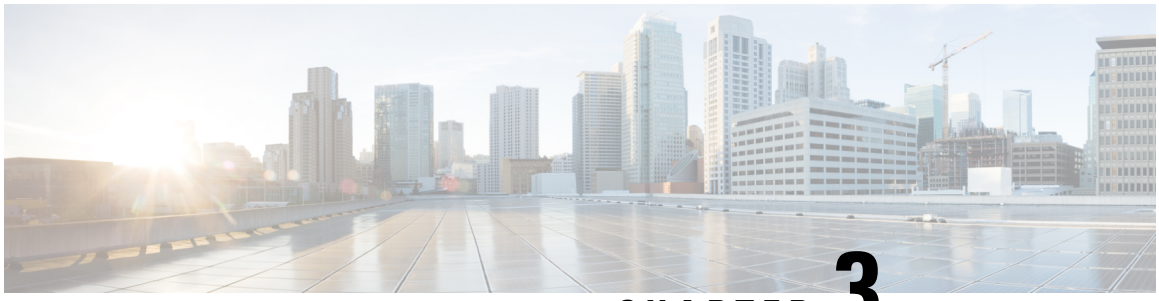
The following is the recommended deployment architecture for connector:

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

PART II

Configuration

- Initial Setup, on page 9
- Cisco Spaces: Connector AMI, on page 23
- Cisco Spaces: Connector: Azure VMware, on page 33
- Cisco Spaces: Connector OVA , on page 45
- Cisco Spaces: Connector Hyper-V, on page 63
- Connector on Cisco Spaces , on page 81
- Connector GUI, on page 89
- Proxy, on page 91
- High Availability, on page 97



CHAPTER 3

Initial Setup

- Initial Setup of Cisco Spaces: Connector, on page 9
- Activating Connector 3 on Cisco Spaces, on page 10
- Upgrading the Connector from Cisco Spaces Dashboard, on page 17
- Upgrading the Connector Using CLI, on page 21

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 45
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 136.
IoT service (wired)	For information, see Configure IoT Service (Wireless), on page 136.
Hotspot service	For information, see Configure Hotspot Service, on page 163.
Local firehose service	For information, see Configure Hotspot Service, on page 163.

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 45

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**.

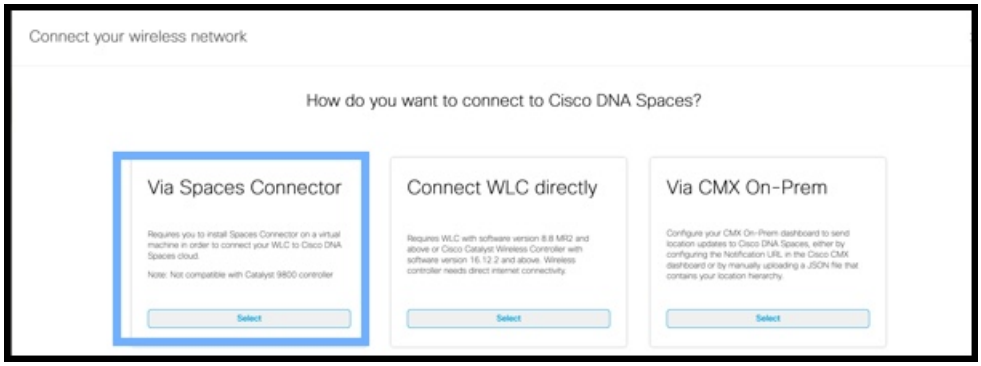
Step 3 In the **Get your wireless network connected with Cisco DNA Spaces** area, click **Add New**.

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

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

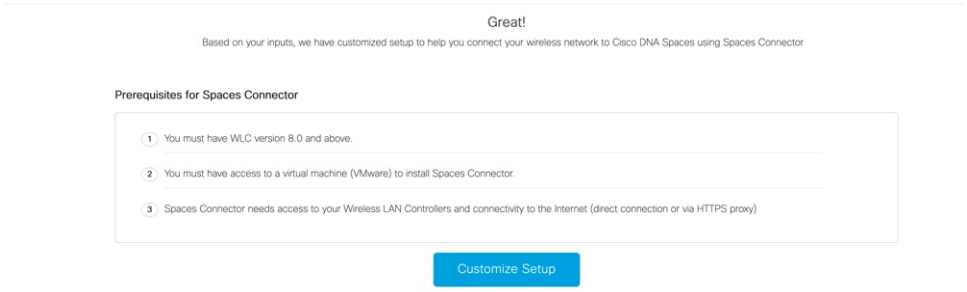
Step 5 In the **Via Spaces Connector** area, click **Select**.

Figure 2: Via Spaces Connector



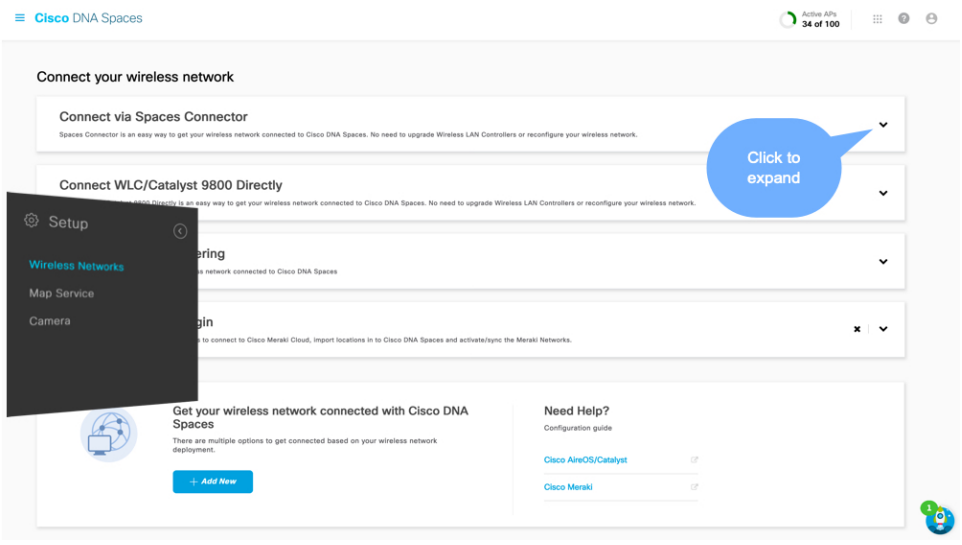
Step 6 In the **Prerequisites for Spaces Connector** dialog box, click **Continue Setup**.

Figure 3: Read Prerequisites for Spaces Connector



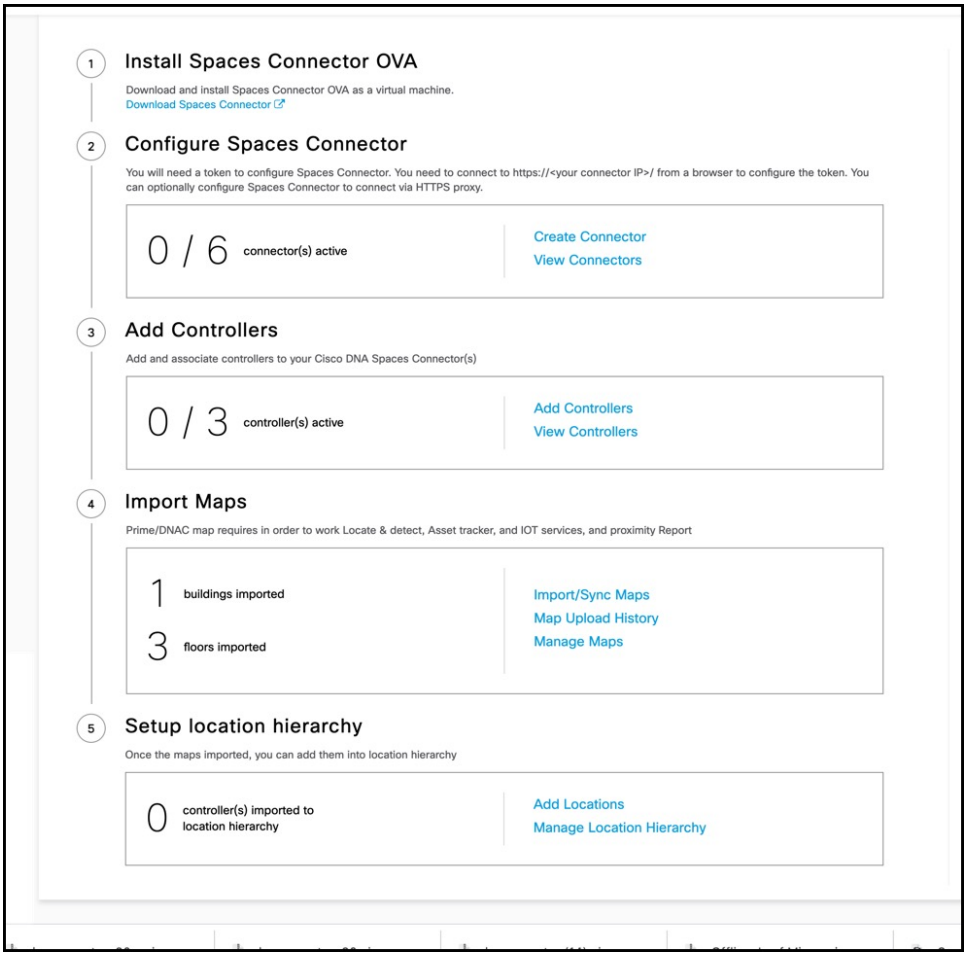
Step 7 Expand the **Connect via Spaces Connector** area using the respective drop-down arrow.

Figure 4: Expand Connect via Spaces Connector



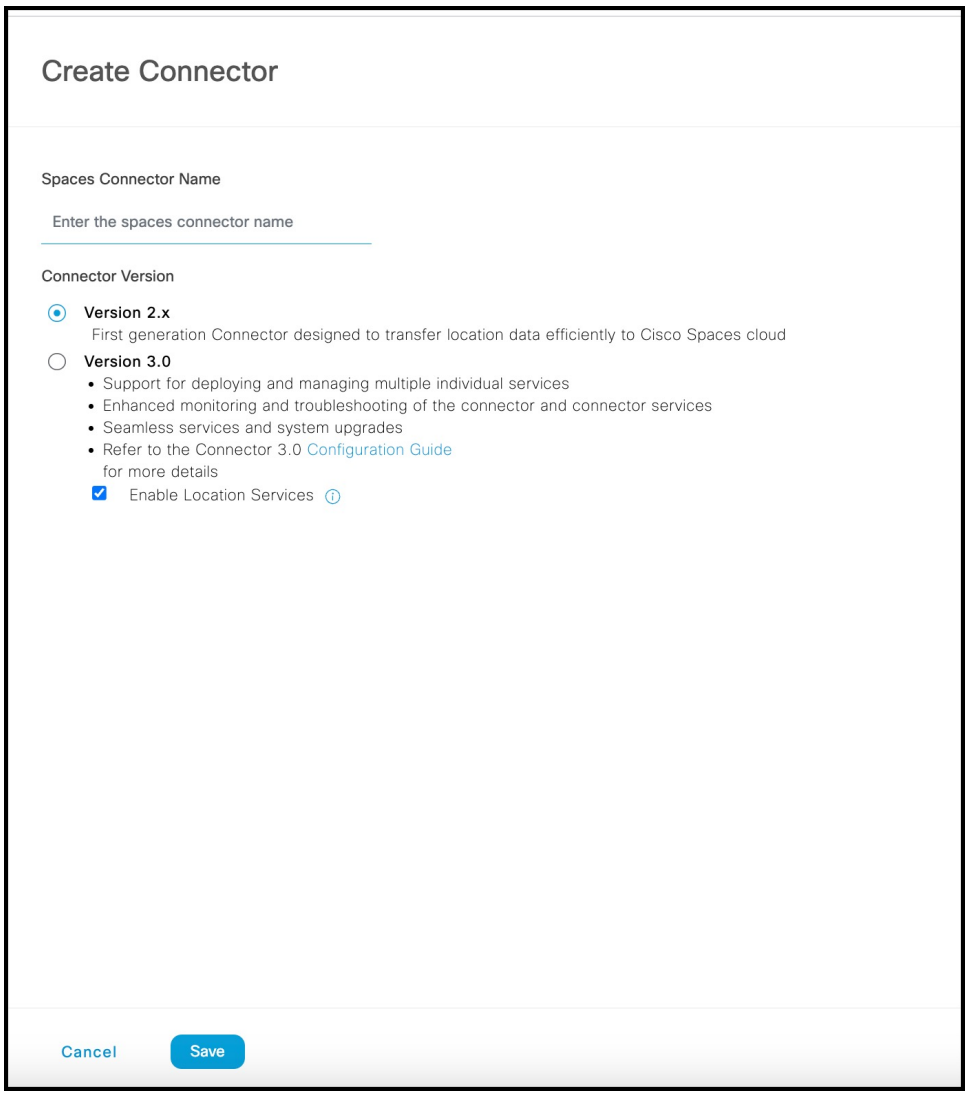
Step 8 In the displayed list of steps, in the **Configure Spaces Connector** area, click **Create Connector**.

Figure 5: Connect via Spaces Connector > Create Connector



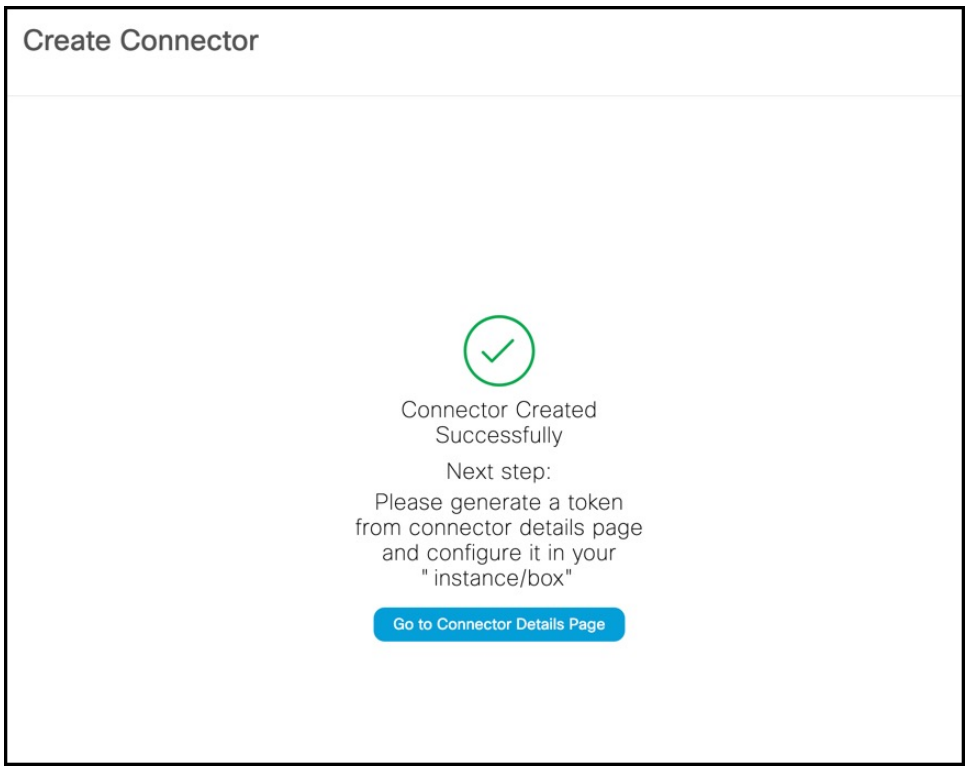
Step 9 In the **Create connector** window that is displayed, enter a name for connector, and click **Version 3.0 (beta).** as the **Connector Version**, and click **Save**.

Figure 6: Name and Version of Connector



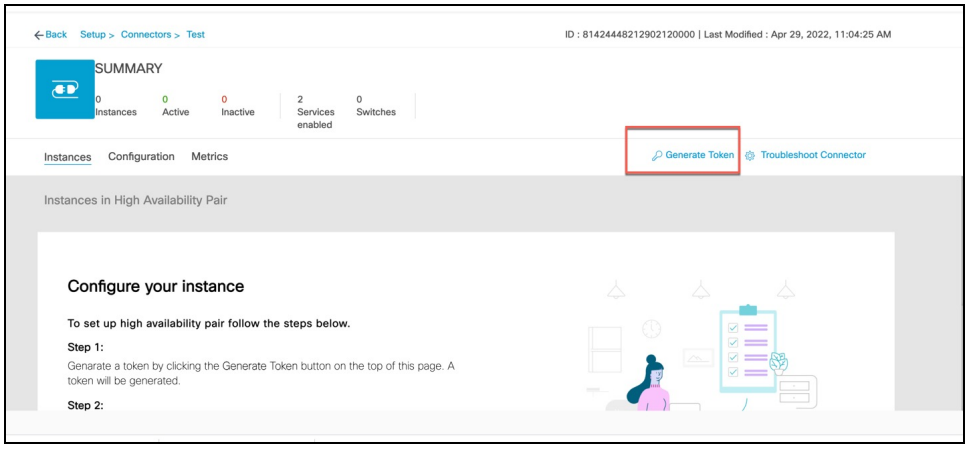
Connector is successfully created. Click **Go to Connector Details** Page.

Figure 7: Connector Created Successfully



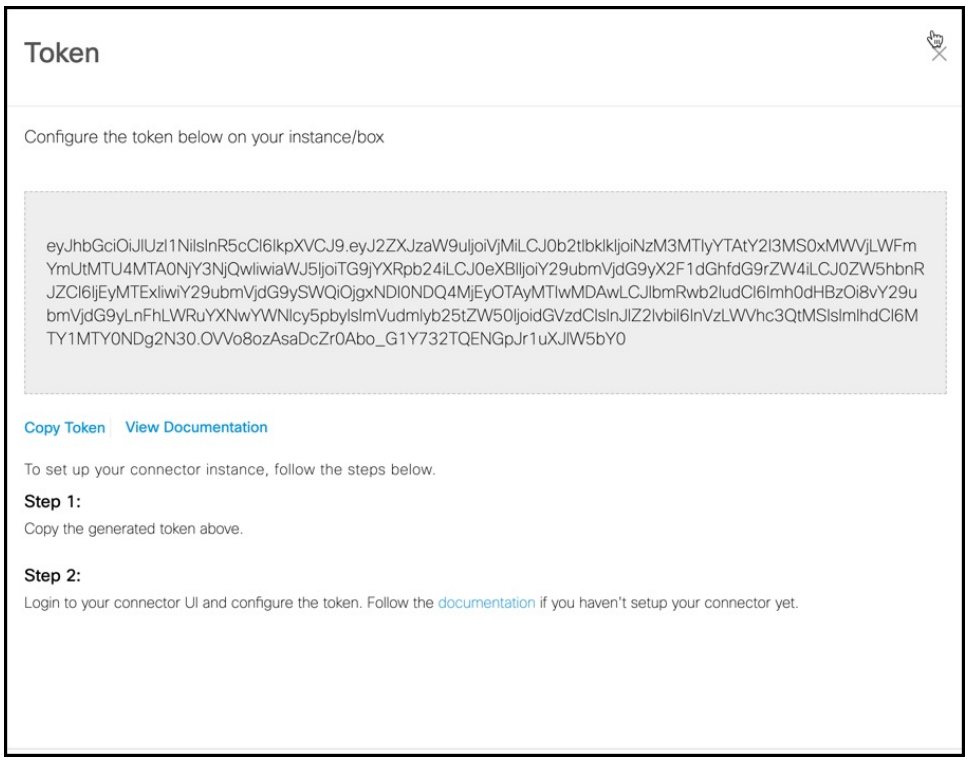
Step 10 In the connector details window, you can see a summary of the configurations for this connector. Click **Generate Token.**

Figure 8: Generate Token



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

Figure 9: Copy Token

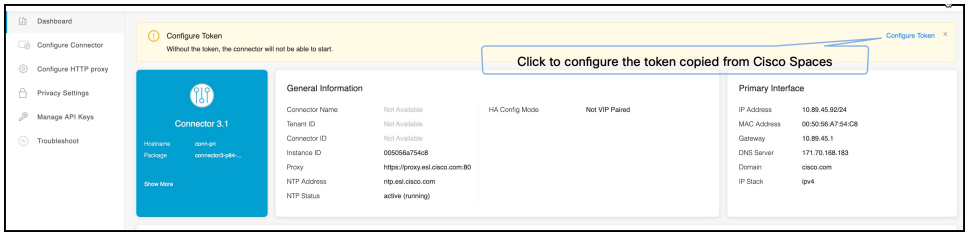


Step 12 Open the connector GUI.

Step 13 (Optional) If your network is behind a proxy, configure the GUI with the proxy. See Configure a Proxy , on page 91

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

Figure 10: Configure Token



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:

- Configure IoT Service (Wireless)
- Configure Hotspot Service

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

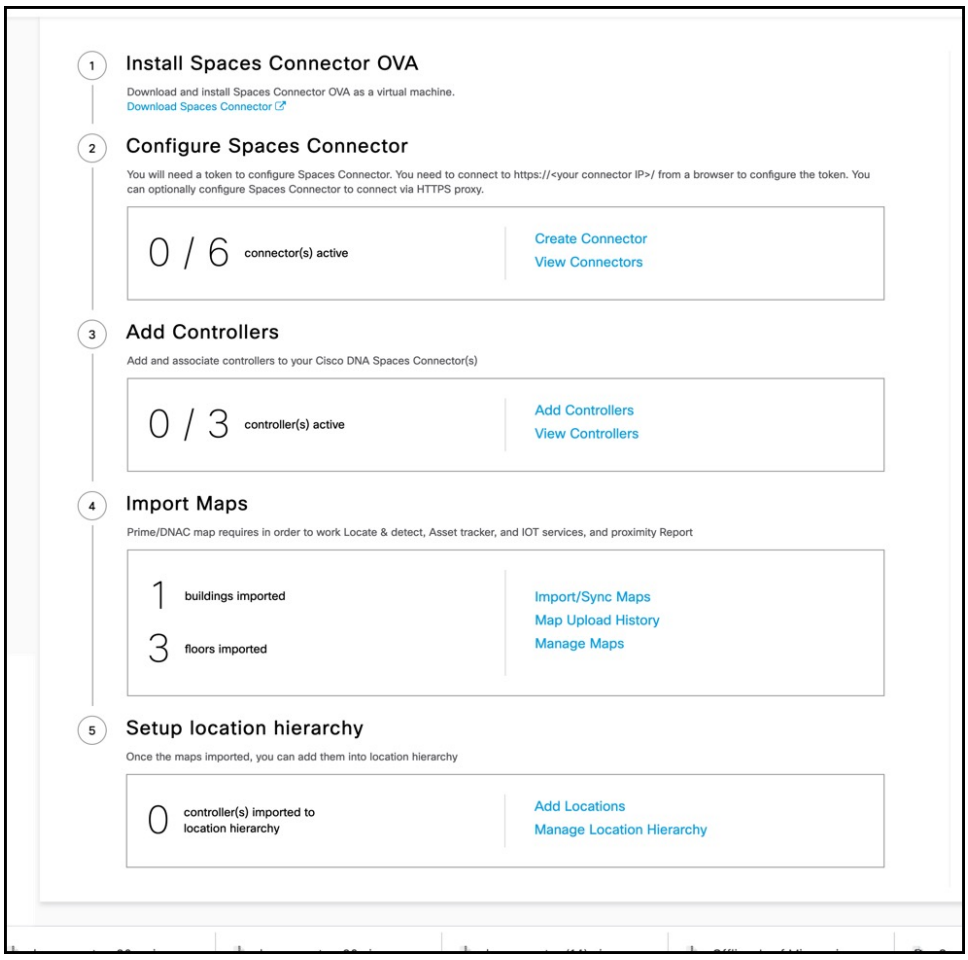
Step 1 Log in to **Cisco Spaces**.

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



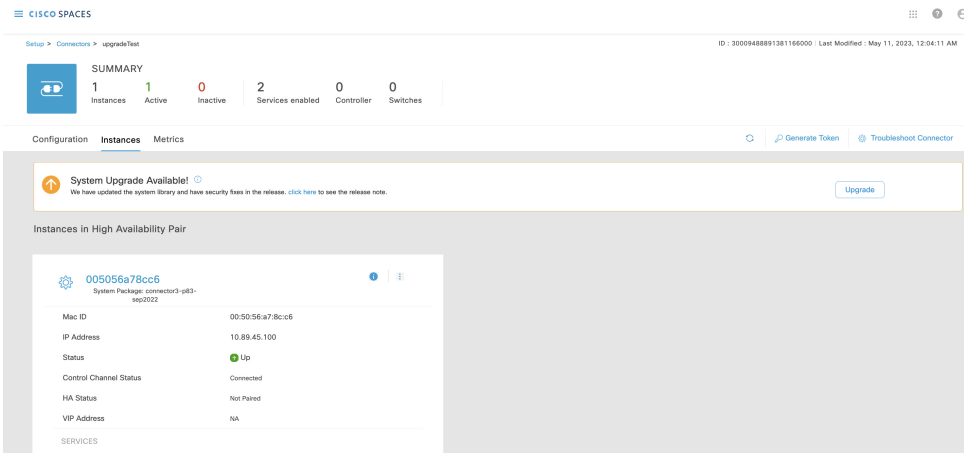
Step 4 From the list of connectors that are displayed, click the connector of your choice.

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

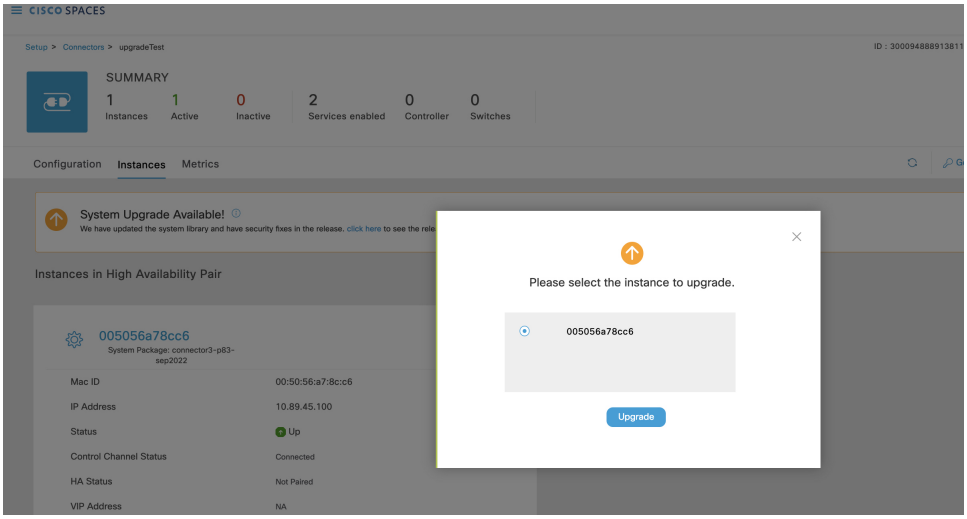


Note For connector Release 3, the system inline upgrade may not succeed in a low latency network. You can upgrade the connector manually. Downloading the connector OVA from cisco.com and using the **connectoros upgrade <package-name>** command from the connector CLI.

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.

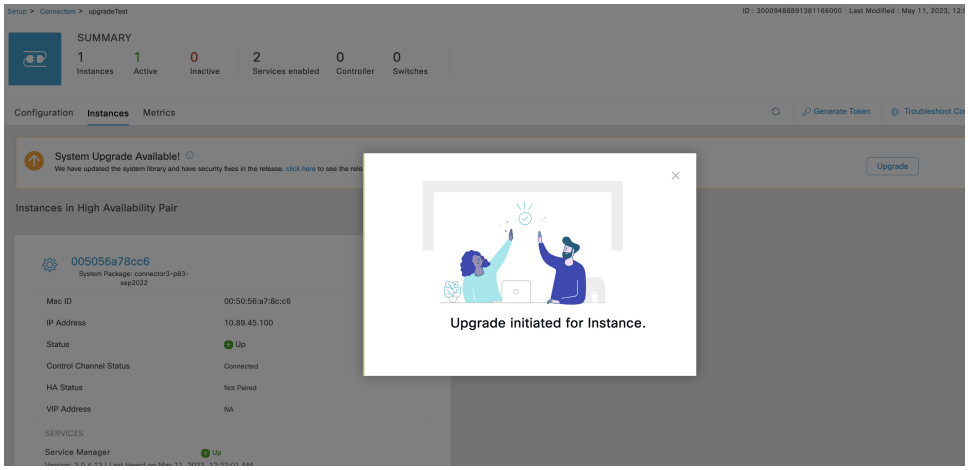
Step 8 From the popup displayed, select the instance you want to upgrade.

Figure 13: Select instance



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

Figure 14: Upgrade Initiated for Instance



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

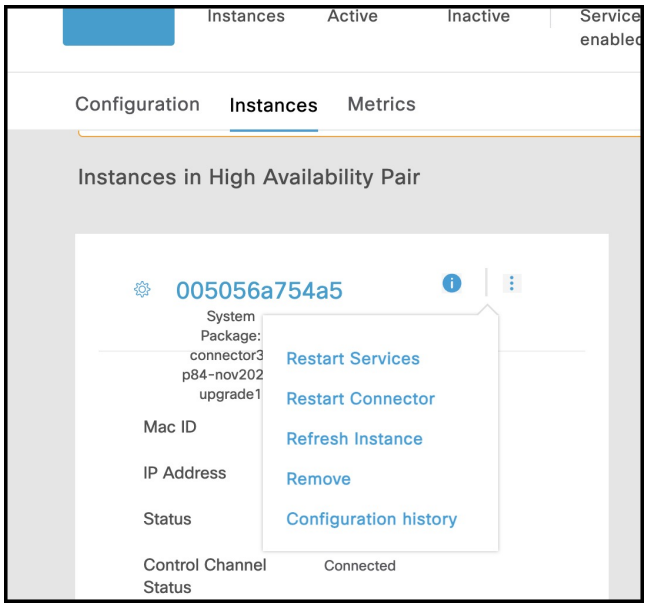
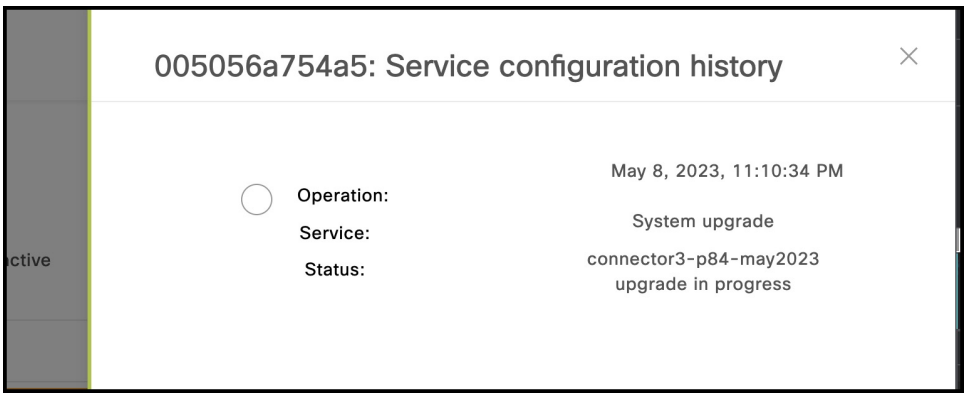


Figure 16: Configuration History



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
```

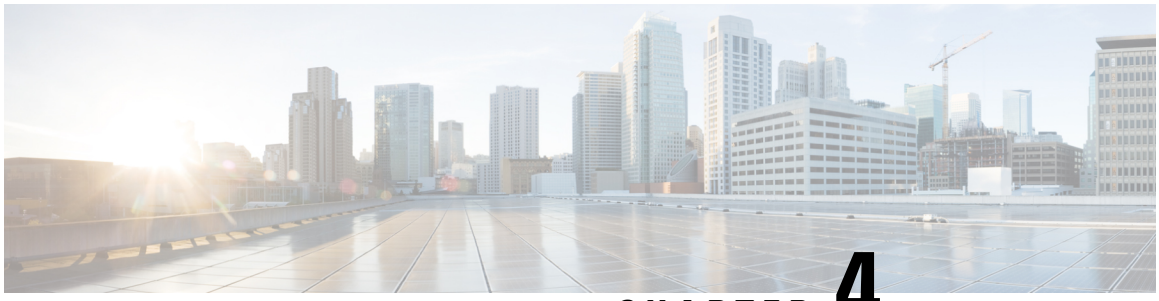
Step 4 Observe the status of the upgrade. Do one of the following:

- 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'
```



CHAPTER 4

Cisco Spaces: Connector AMI

- Launch Connector 3 as an EC2 Instance from AMI , on page 23

Launch Connector 3 as an EC2 Instance from AMI

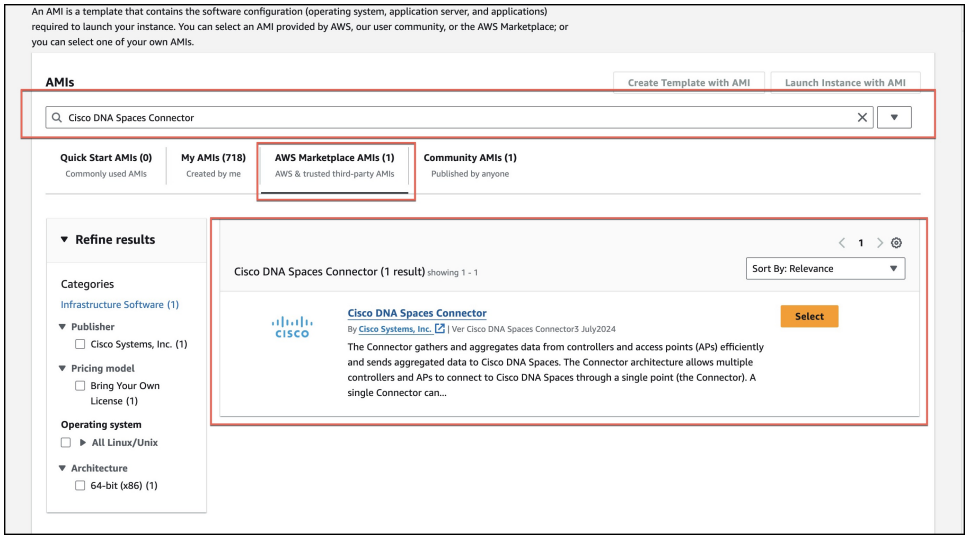
This chapter provides information about how to launch a connector 3 as an EC2 instance from Amazon Machine Images (AMI), configure the connector 3 instance, and finally obtain a URL to log in to the connector connector and CLI.

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**.

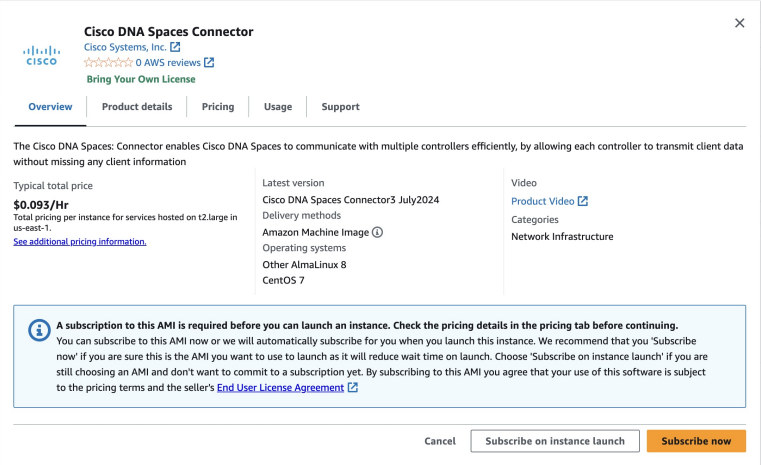
Figure 17: Configuration



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

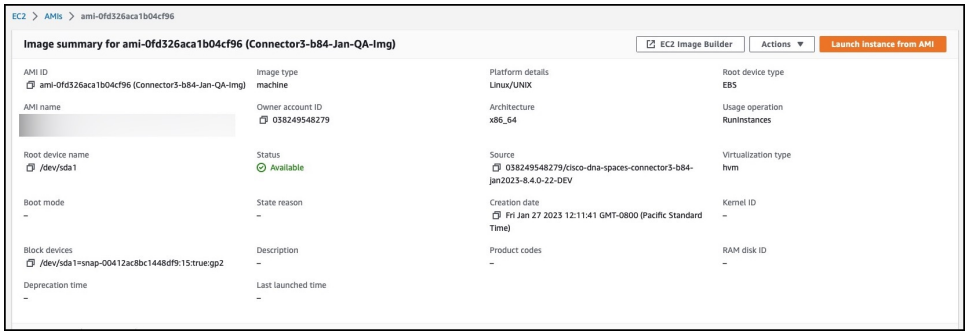
Step 4 In the **Cisco DNA Spaces Connector** window displayed, click **Continue**.

Figure 18: AWS MarketPlace AMIs



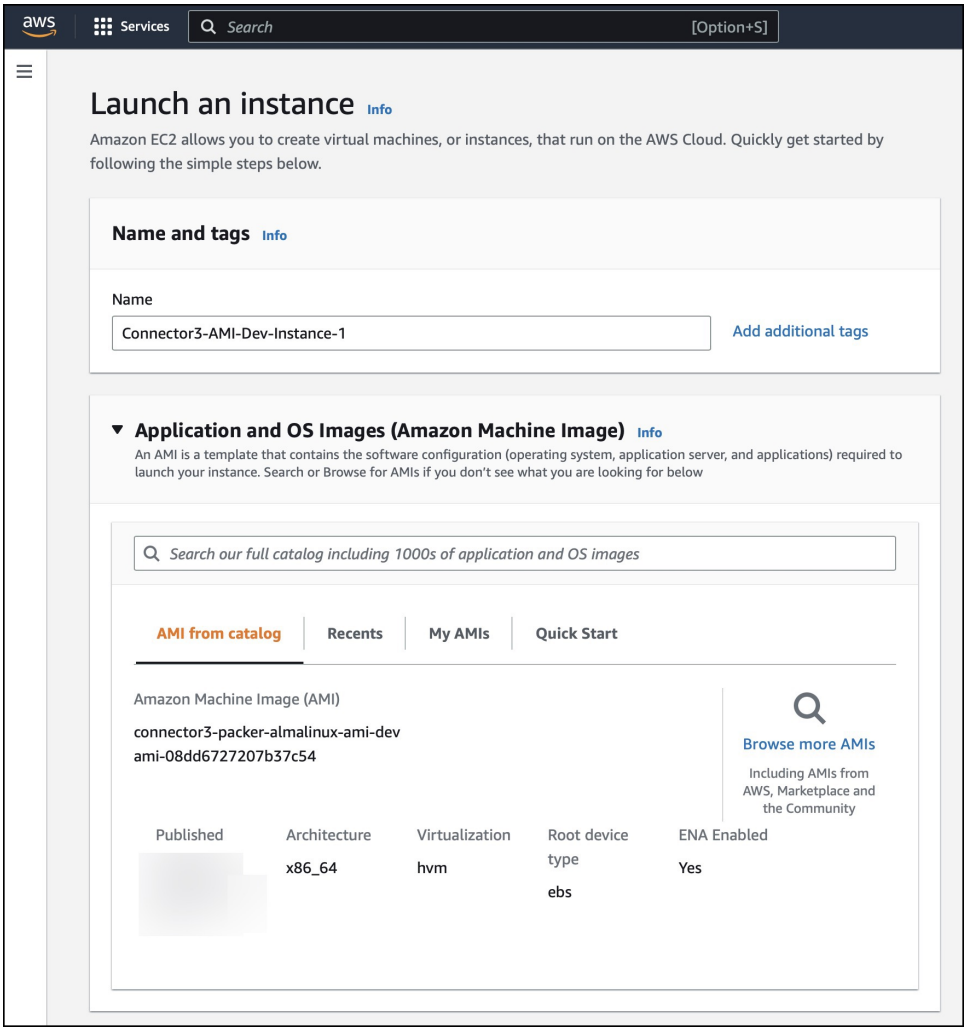
Step 5 In the **Image Summary** window displayed, click **Launch Instance from AMI**

Figure 19: Launch Instance from AMI



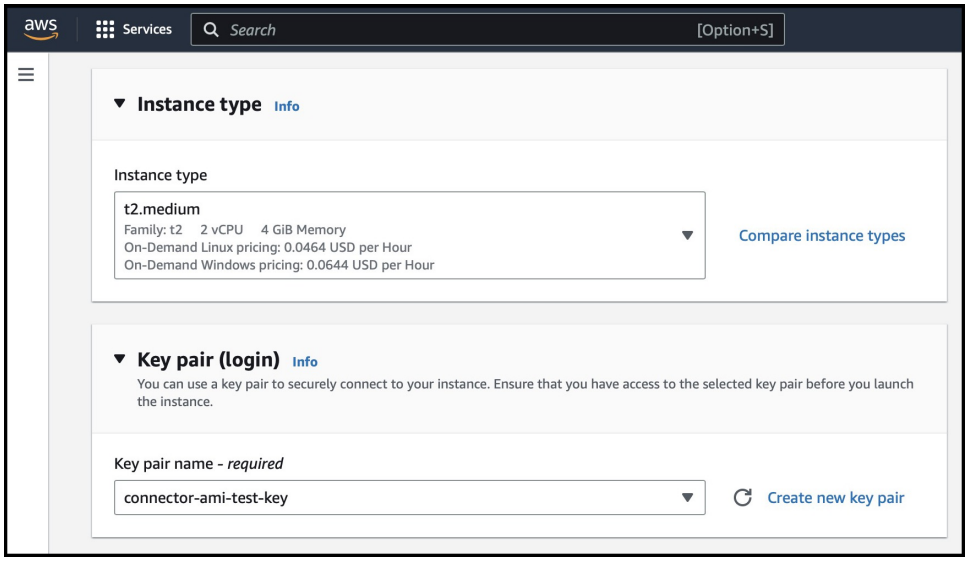
Step 6 In the **Launch an Instance** window displayed, enter an instance name, and add any additional labels for your instance by clicking the **Add Additional tags** button.

Figure 20: Launch Instance from AMI



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



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:

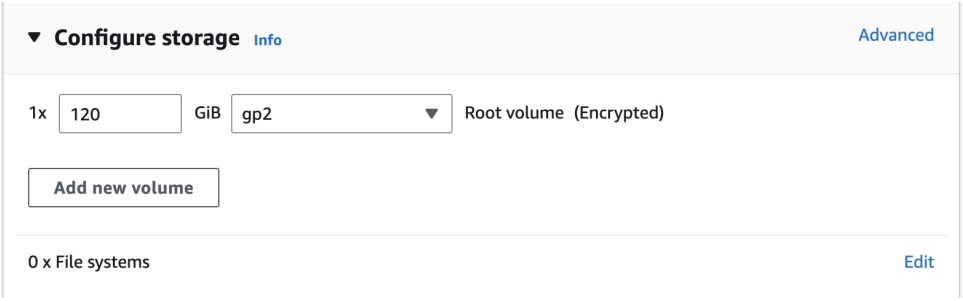
- 4 vCPUs and 8-GB memory (referred to in this document as **Advanced1**)
- 8 vCPUs and 16-GB memory (referred to in this document as **Advanced2**)

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

Figure 22: Add Storage

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

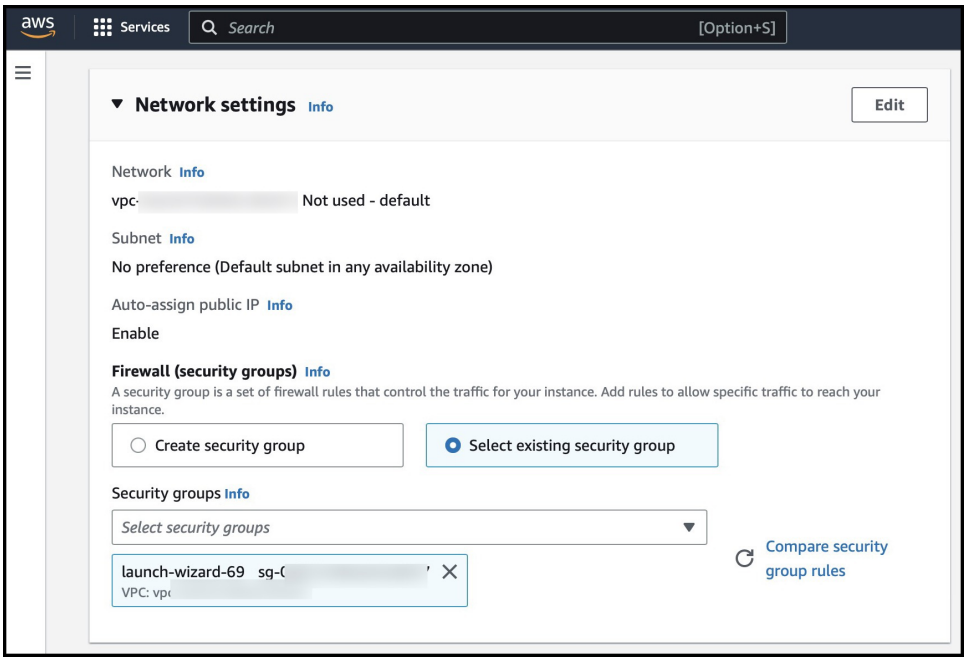
Figure 23: Configure Storage



Step 10 Configure a security group by following these steps:

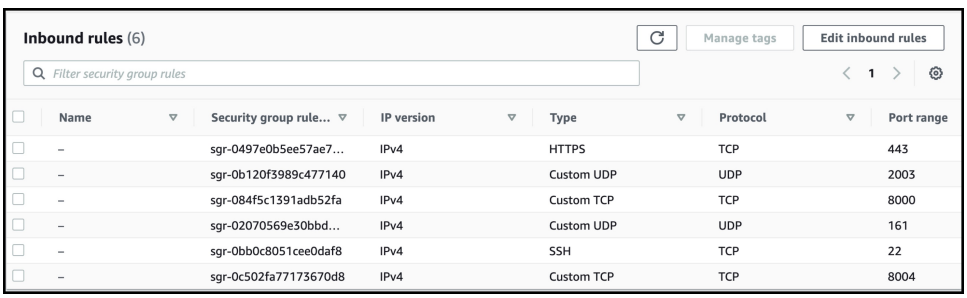
a) Create a new security group or modify an existing one by clicking the respective radio button.

Figure 24: Configure Security Group



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.

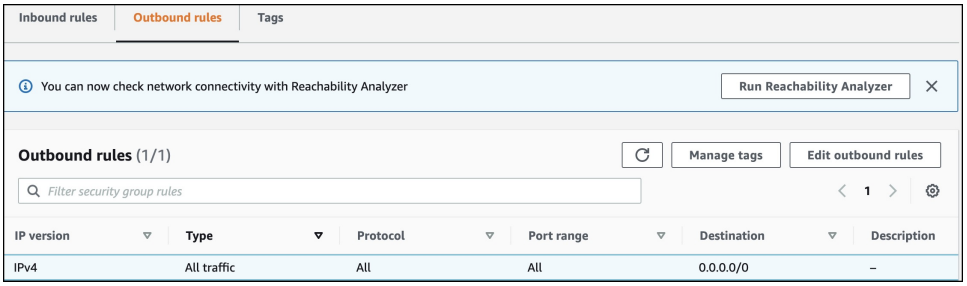
Figure 25: Configure These Inbound Rules Permitting Traffic to Specific Ports



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



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

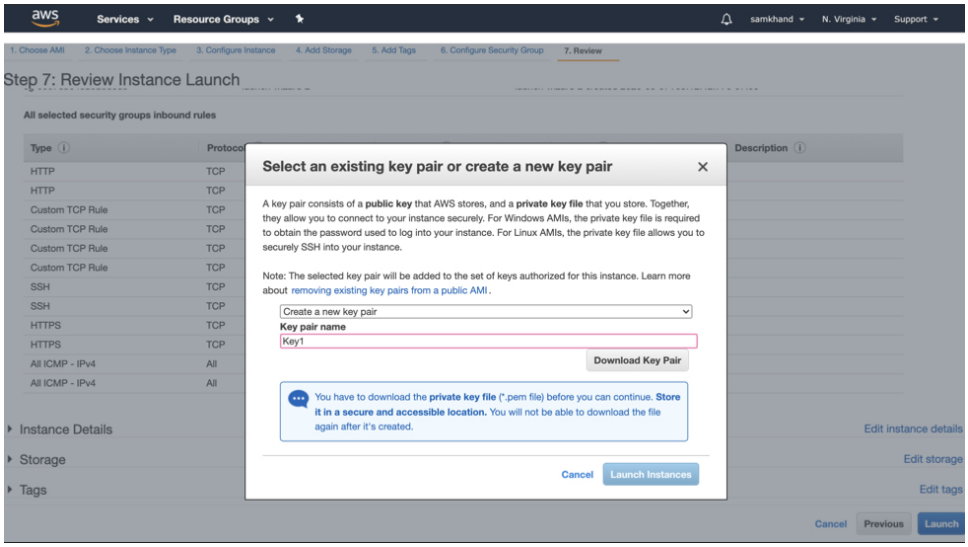
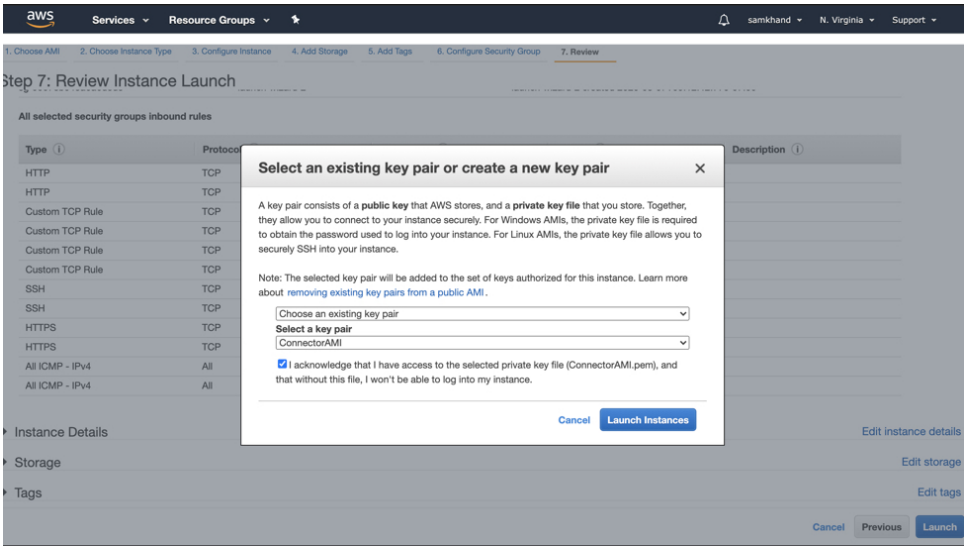


Figure 28: Choose an Existing Key Pair

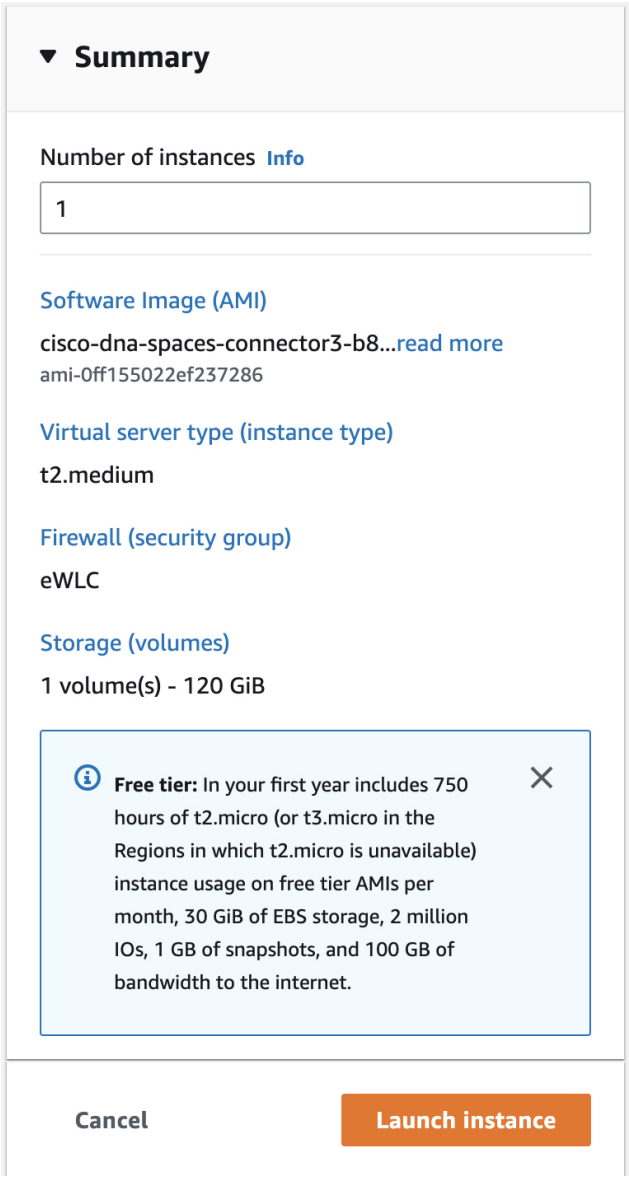


Step 12 After you have downloaded the key pair (.pem) file to your system, navigate to the file location. Configure appropriate permissions for the .PEM file using the **chmod** command.

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

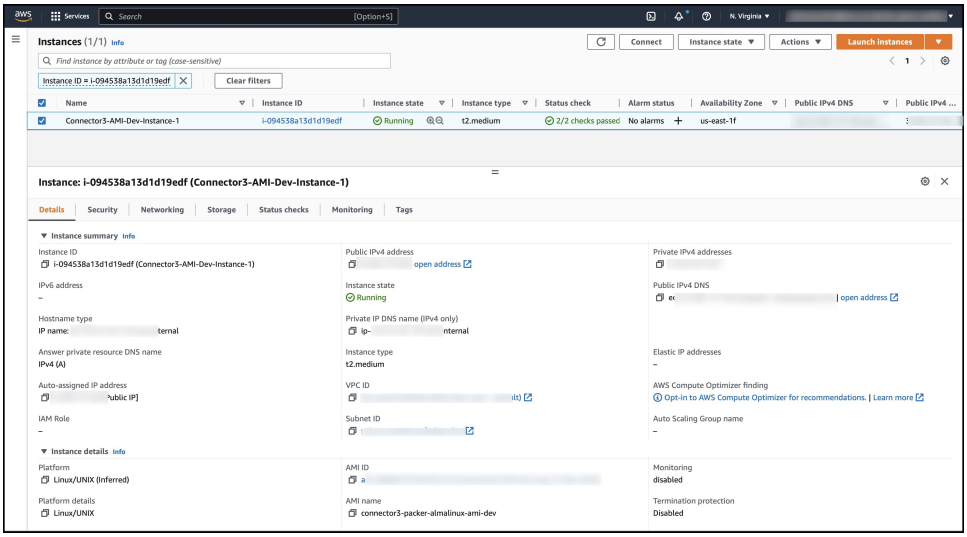
Step 13 Review the instance and click **Launch**.

Figure 29: Review Instance and Launch



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



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:

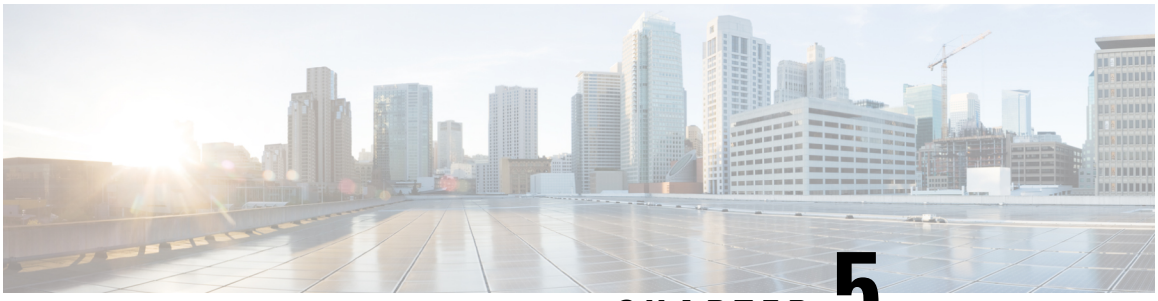
```
Welcome to Cisco Spaces Connector Setup
Changing password for user spacesadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Password changed successfully
Setting rbash...
Restarting docker...
Changing shell for root.
Shell changed.
Changing shell for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

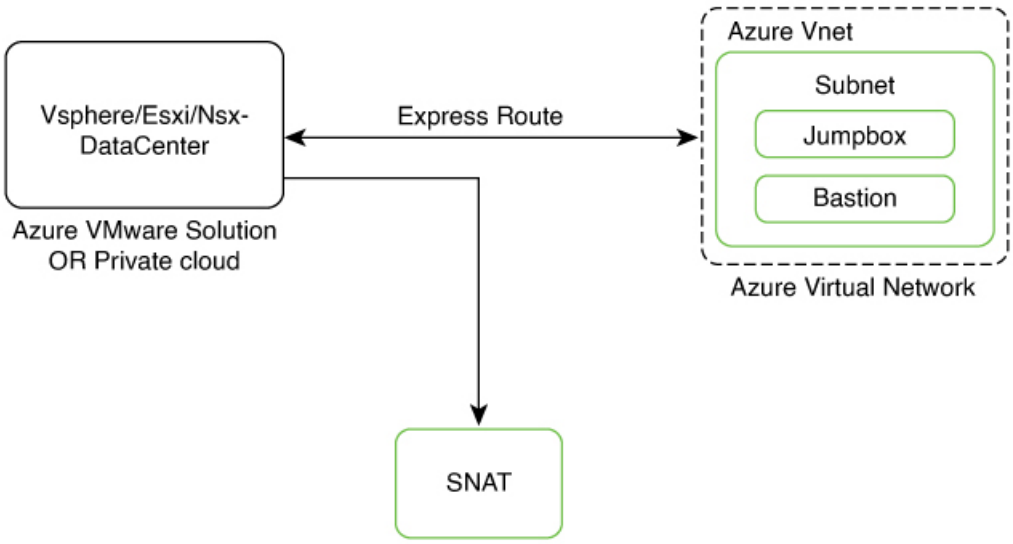
• Cisco Spaces: Connector: Azure VMware, on page 33

Cisco Spaces: Connector: Azure VMware

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 31: 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 34 and deploying the connector OVA on it.
2. Creating an Azure Virtual Network, on page 38. 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

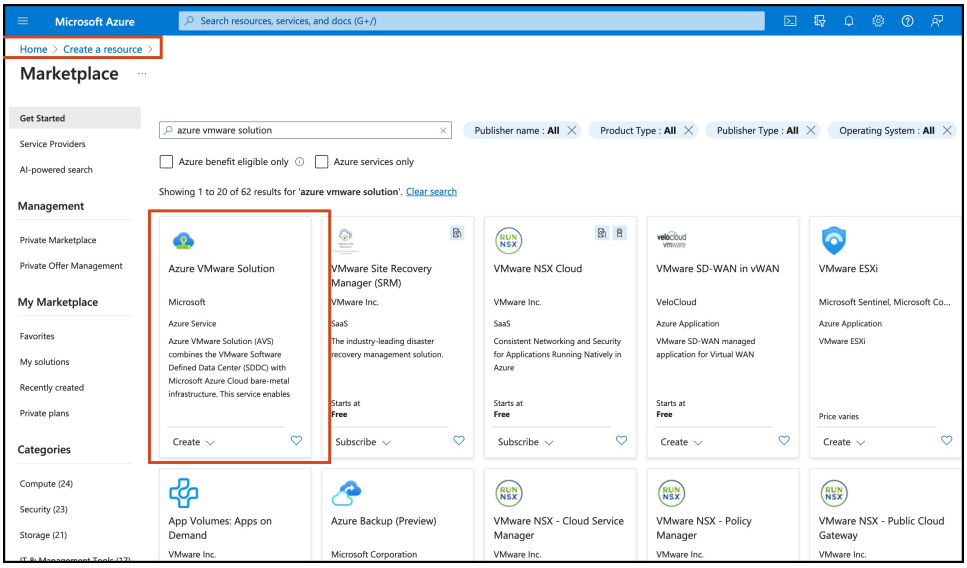
Procedure

Step 1 Log in to portal.azure.com.

Step 2 Create a **Resource**.

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

Figure 32: Create a Resource



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 33: Create a private cloud

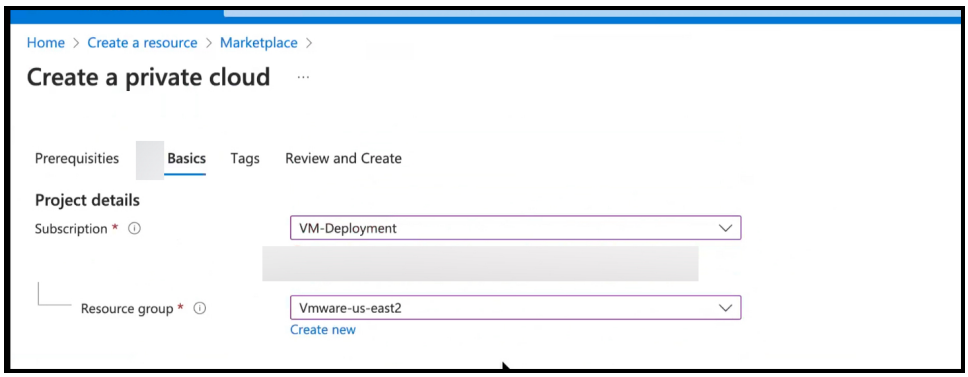
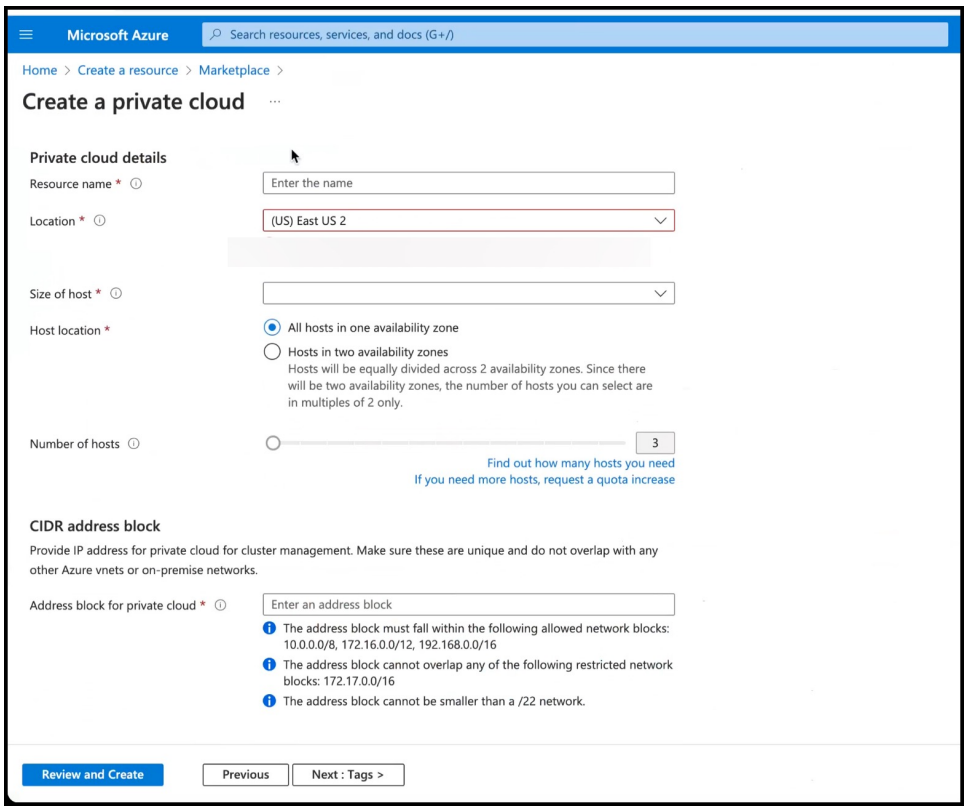


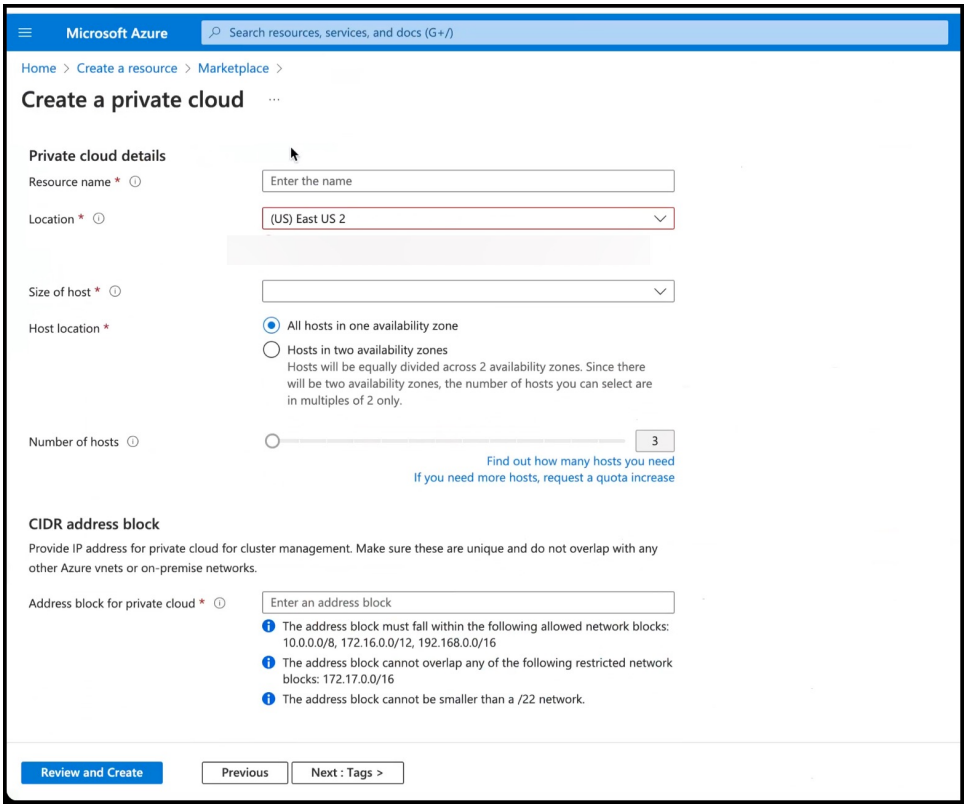
Figure 34: Create a private cloud



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 35: Create a Segment



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 36: Various Components to InstallConnector onAzure VMware

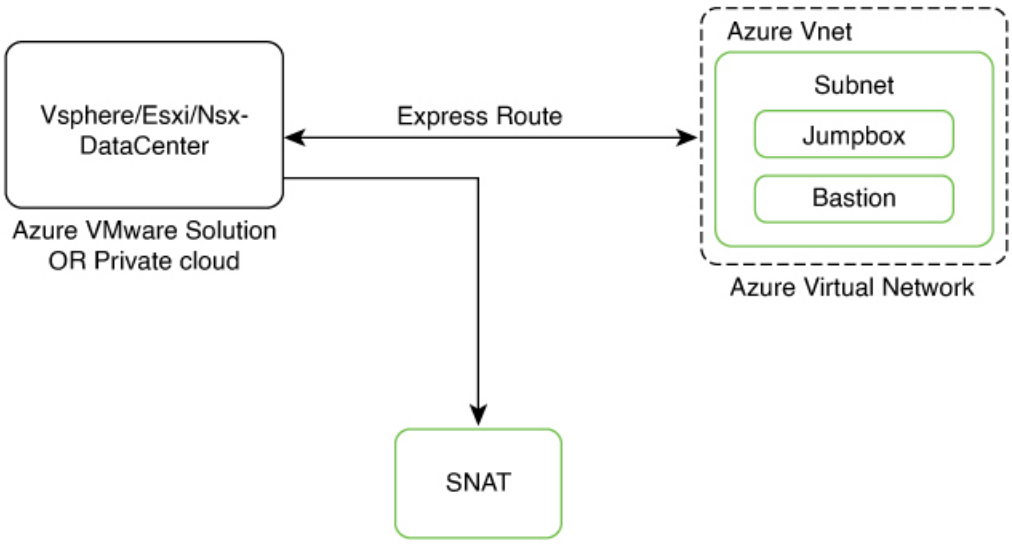
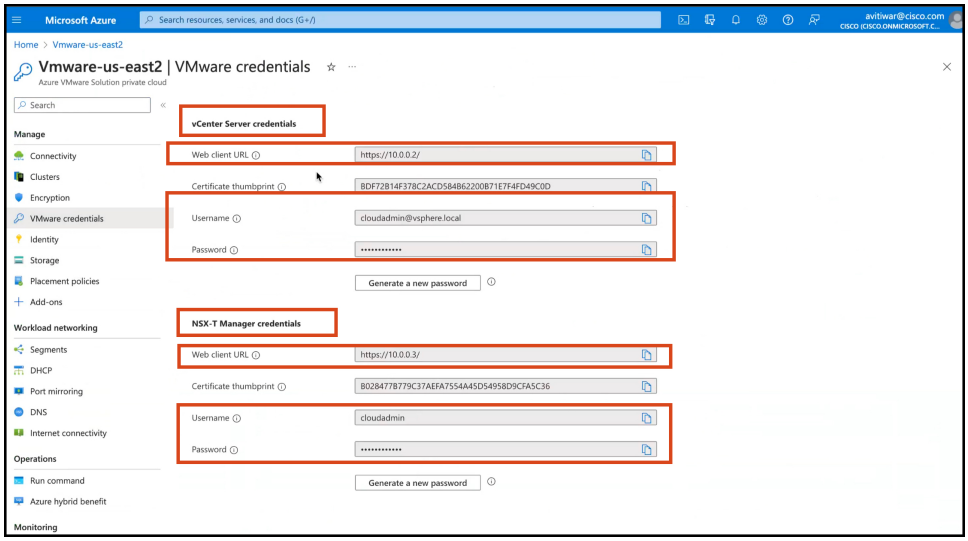


Figure 37: VMware Credentials



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

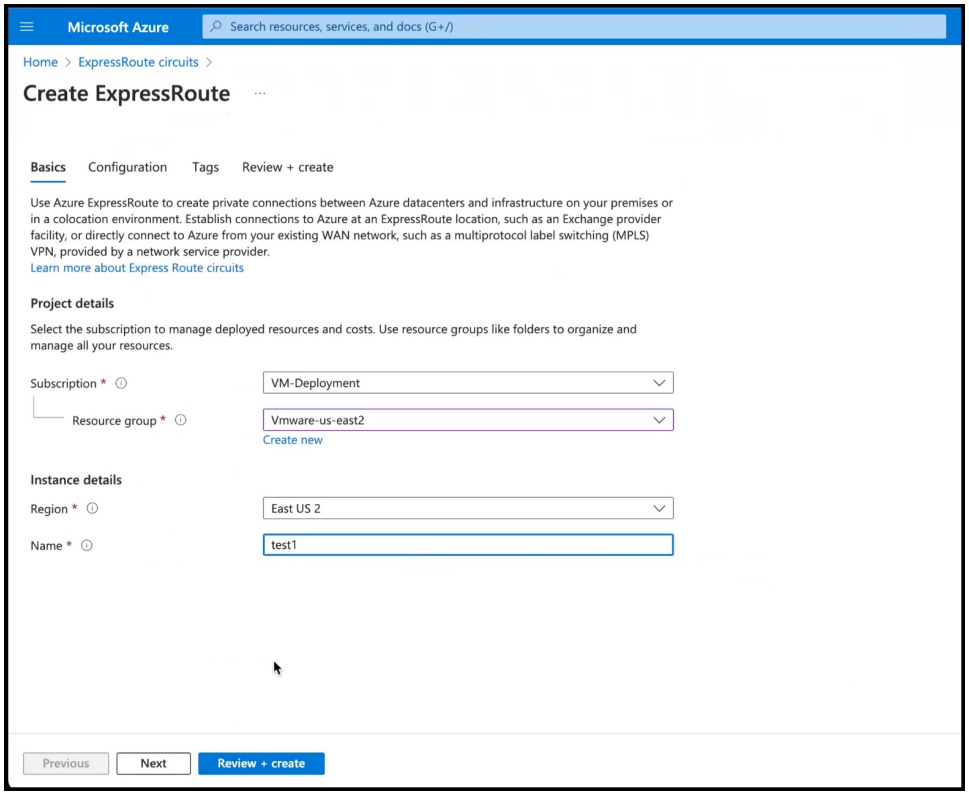
Step 1 Create an **ExpressRoute**.

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

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

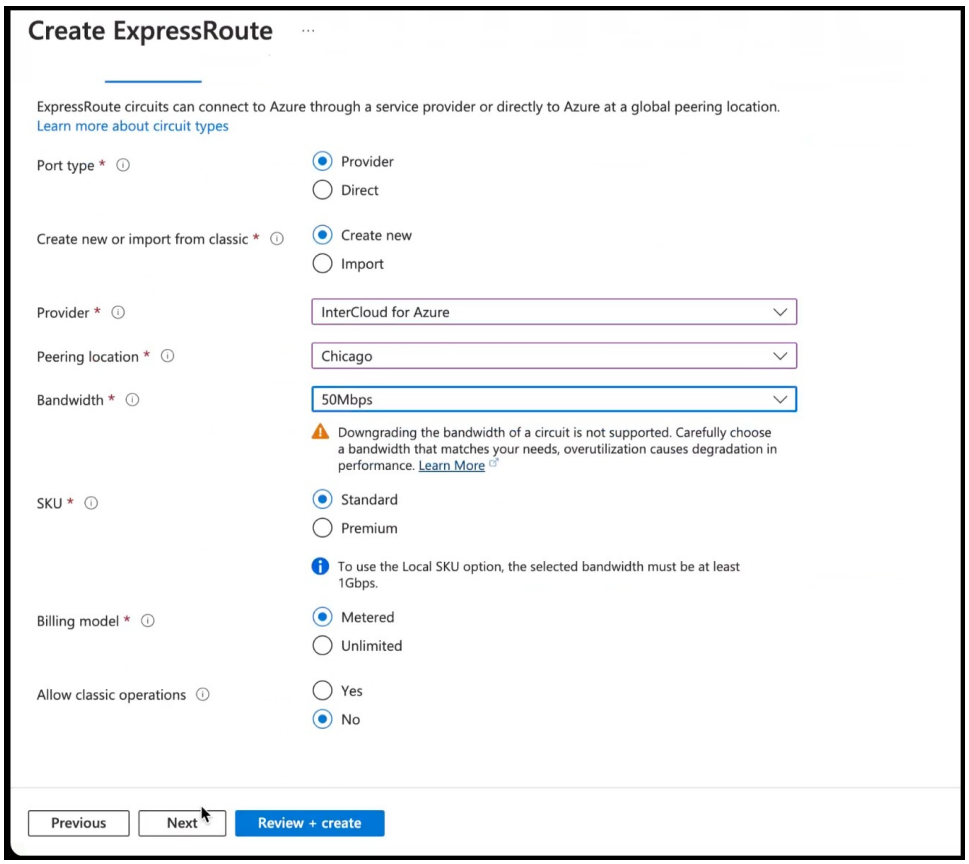
c) From the **Create ExpressRoute** page that is displayed, enter the details of the **Basic** tab. Click **Next**.

Figure 38: Basics Tab



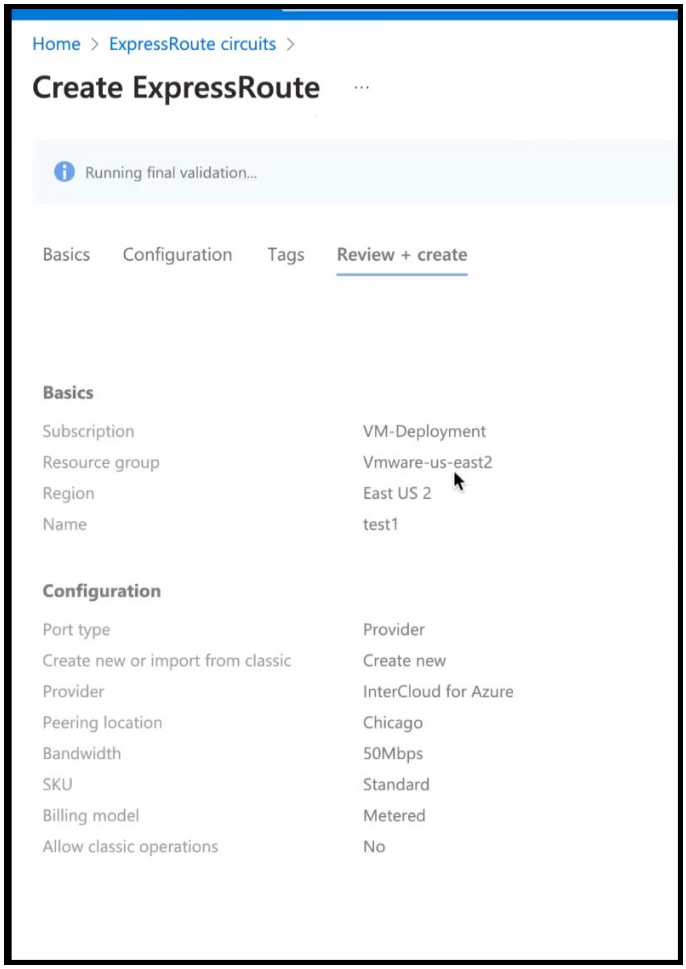
d) Click the **Configuration** tab. Fill in details such as **Provider**.

Figure 39: Configuration Tab



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

Figure 40: Review + Create



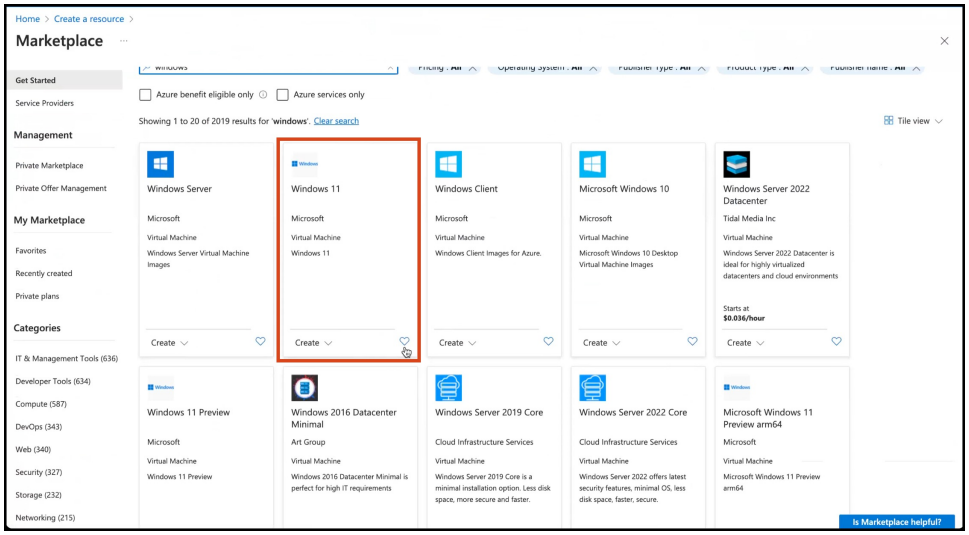
Step 2 From the created **Virtual Network**, do the following.

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.

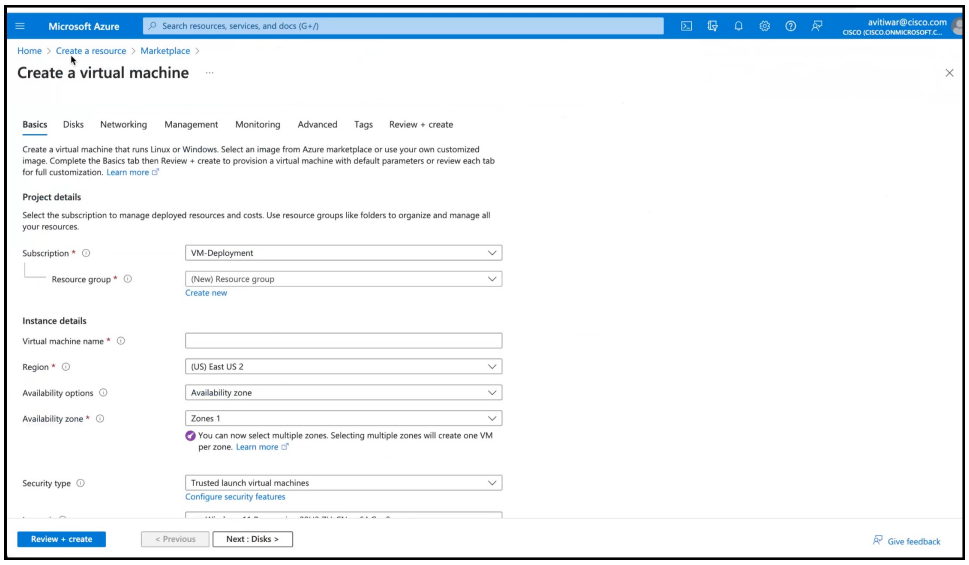
a) From the left-navigation pane, click **Create a Resource**
b) Search for an operating system of choice. For example, Windows 11, click **Create** and choose the version of choice.

Figure 41: Windows 11 virtual machine



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

Figure 42: Create a Virtual Machine



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 43: VMware Credentials

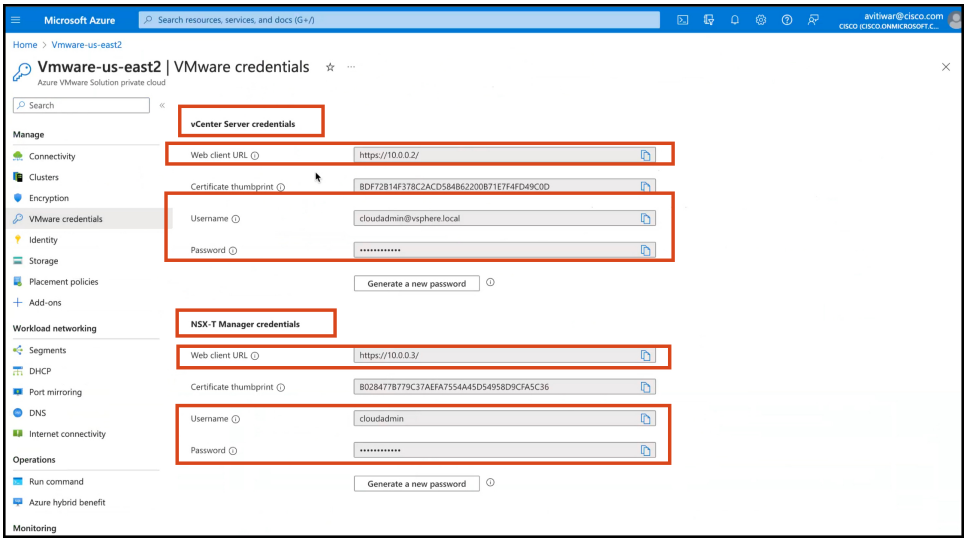
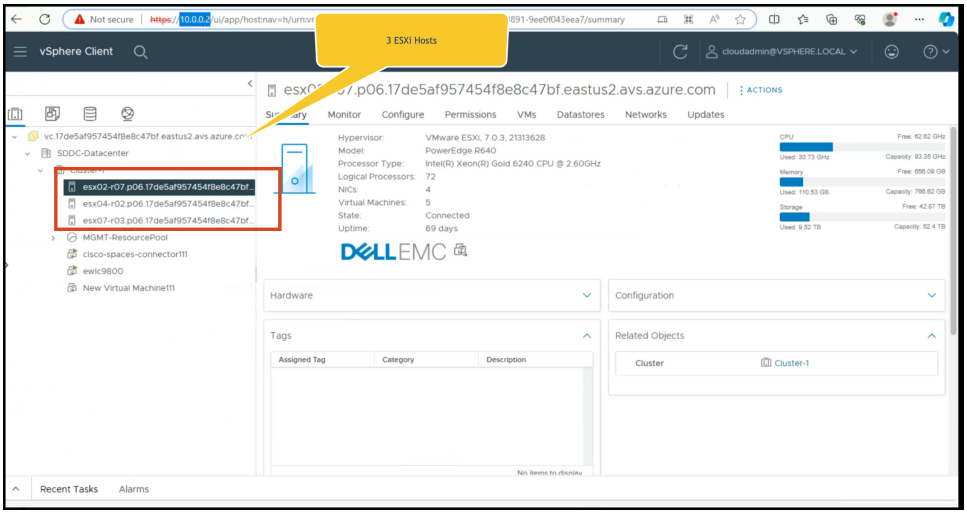


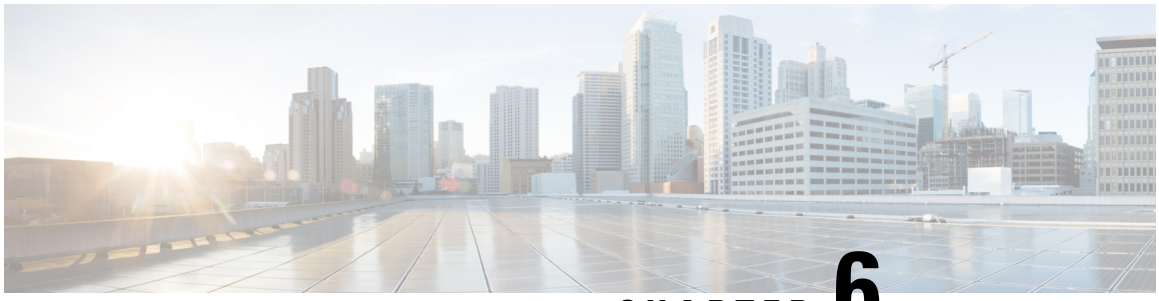
Figure 44: VMware Credentials



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 45



CHAPTER 6

Cisco Spaces: Connector OVA

- Deploying the Connector 3 OVA (Single Interface), on page 45
- Deploying the Cisco Spaces: Connector OVA (Dual Interface), on page 53
- Using Snapshots for Backup , on page 60

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

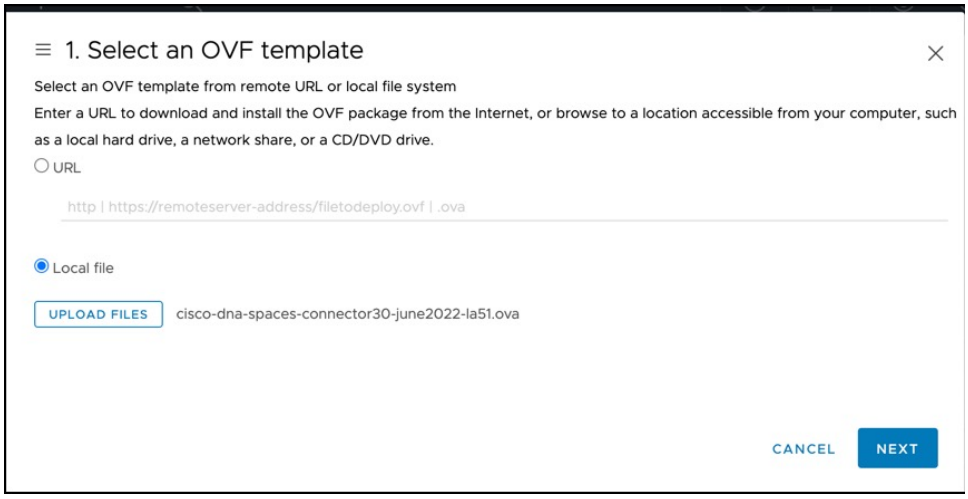
Procedure

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.

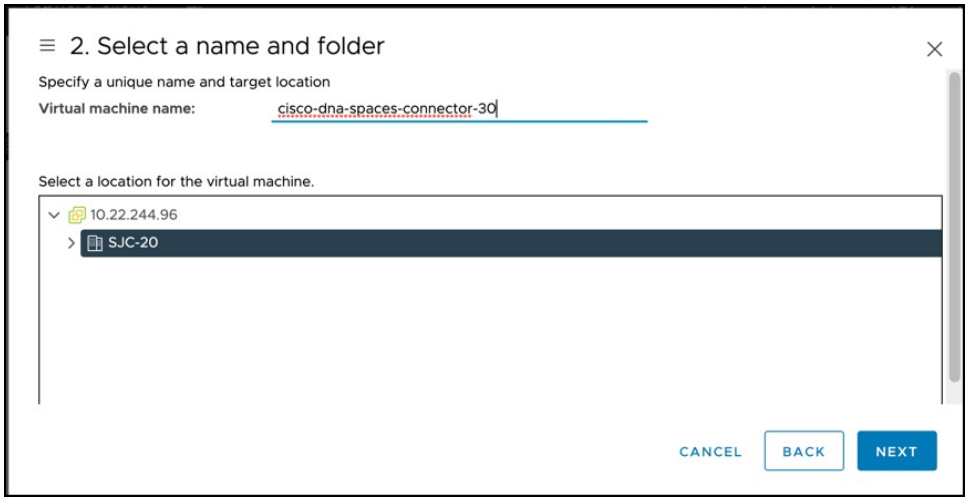
Step 3 In the **1. Select an OVF template** window, click **UPLOAD FILES**, and select the corresponding connector OVA files or drag and drop the downloaded file, and click **Next**.

Figure 45: 1. Select an OVF template



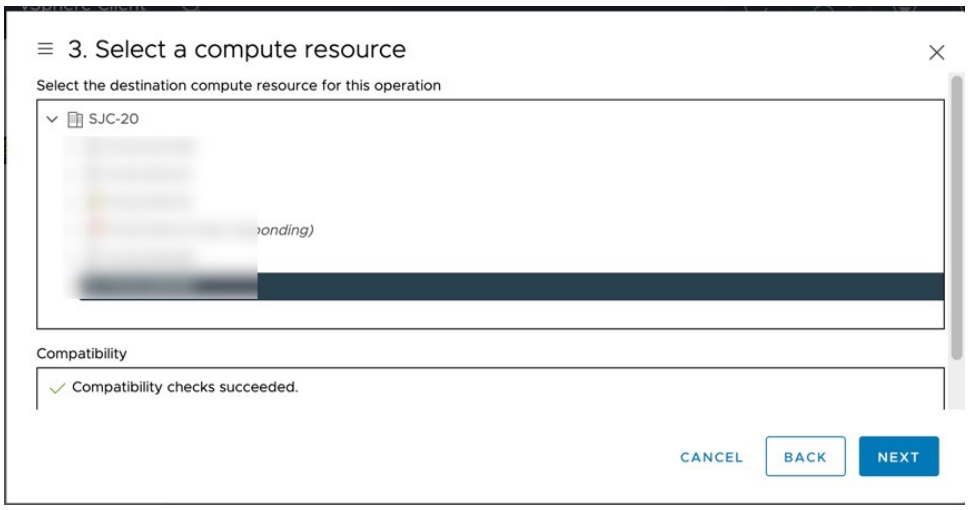
Step 4 In the **2. Select a name and folder** window, enter a name for the VM, and choose a location for the VM, and click **Next**.

Figure 46: 2. Select a Name and Folder



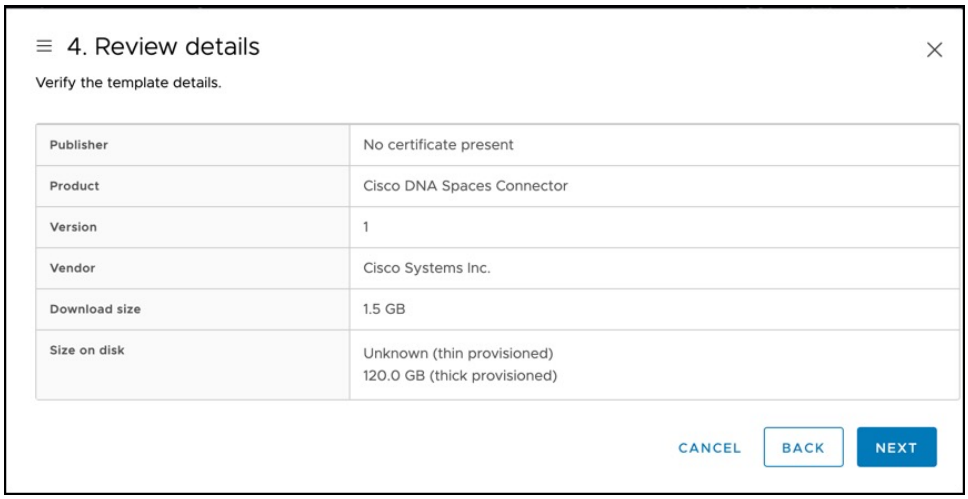
Step 5 In the **3. Select a compute resource** window, select a destination compute resource, and click **Next**.

Figure 47: 3. Select a Compute Resource



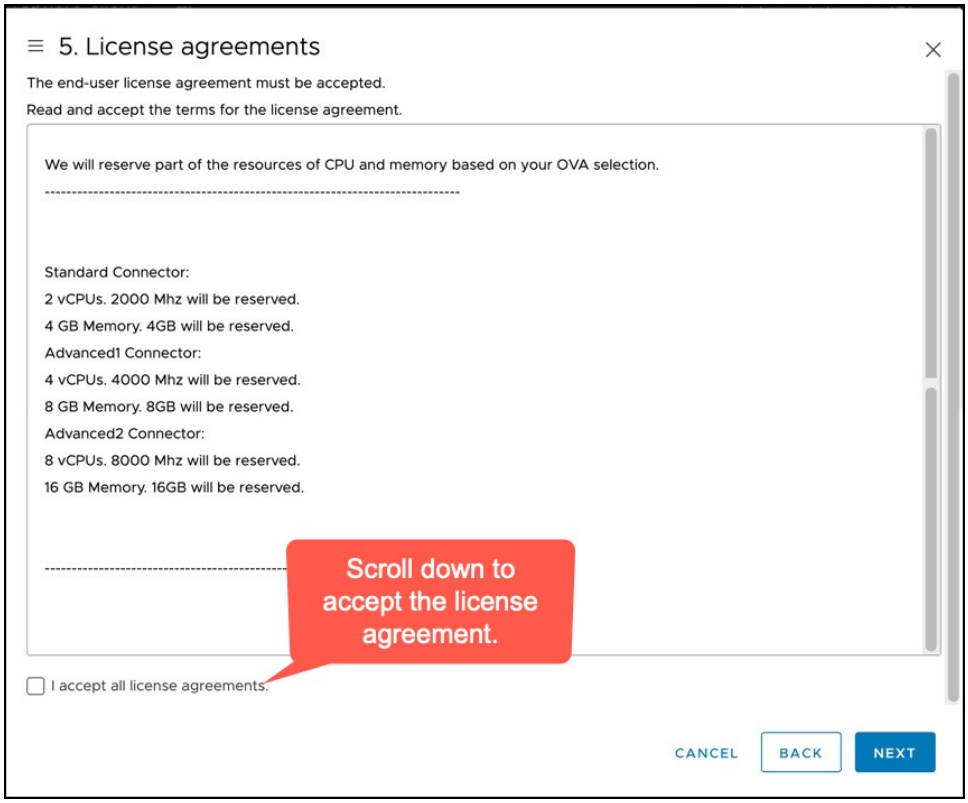
Step 6 In the **4. Review details** window, read and verify the template details, and click **Next**.

Figure 48: 4. Review Details



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 49: 5. License Agreements

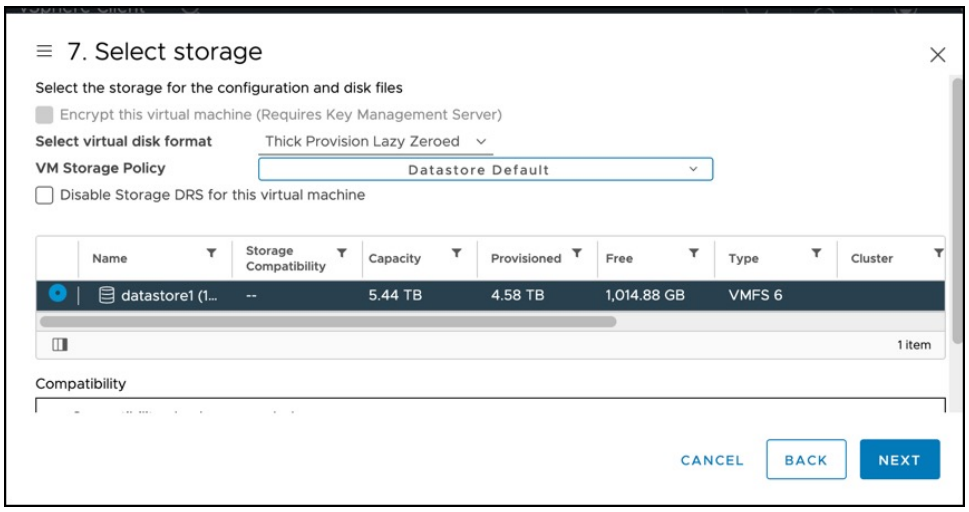


Step 8 In the **6. Configuration** window, choose one of the following, and click **Next**.

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

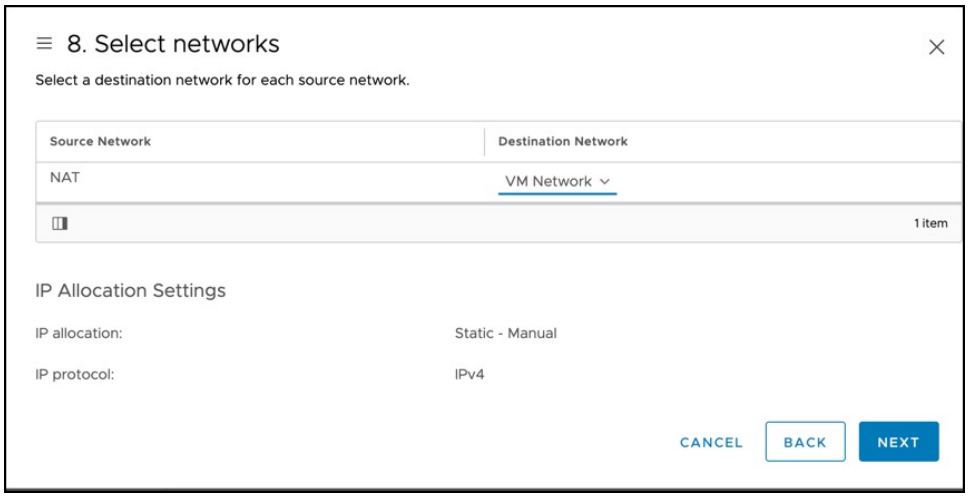
Step 9 In the **7. Select storage** window, choose the standard storage configuration, and click **Next**.

Figure 50: 7. Select storage



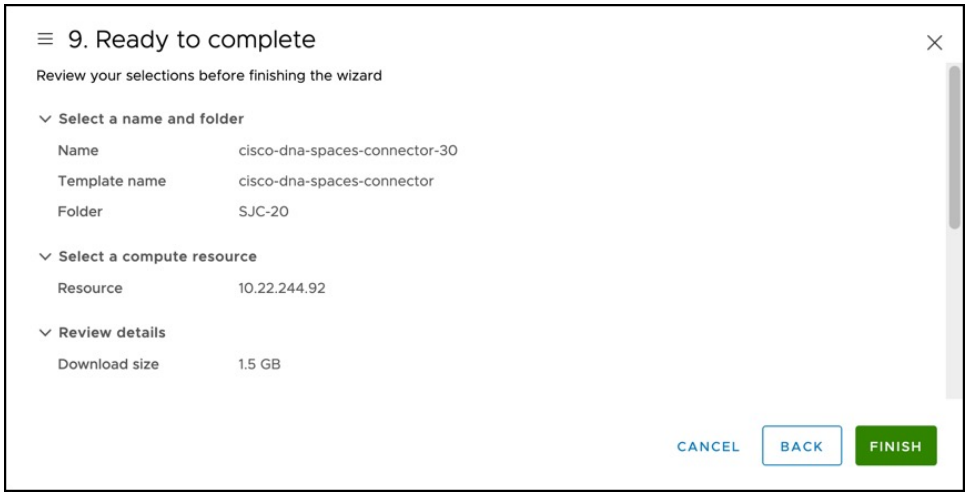
Step 10 In the **8. Select networks** window, choose a destination network, and click **Next**.

Figure 51: 8. Select Networks



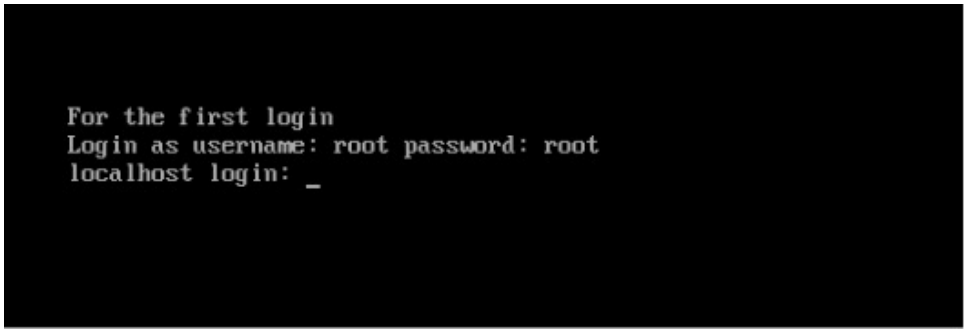
Step 11 In the **9. Ready to complete** window, review the configurations and click **Finish**.

Figure 52: 9. Ready to Complete



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

Figure 53: First Login Credentials root/root



Step 13 Choose an network interface to configure as PRIMARY.

Figure 54: Configuring the Primary Interface: IPv4

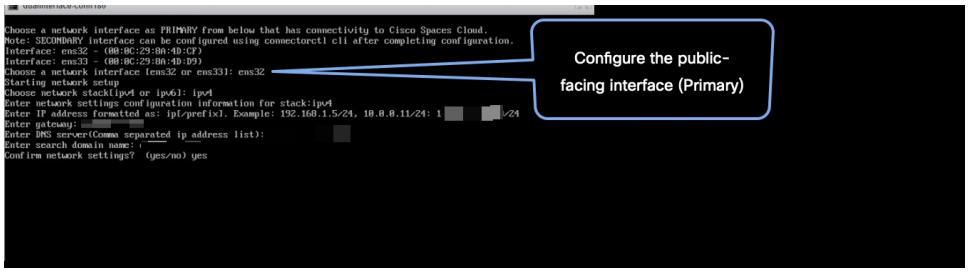
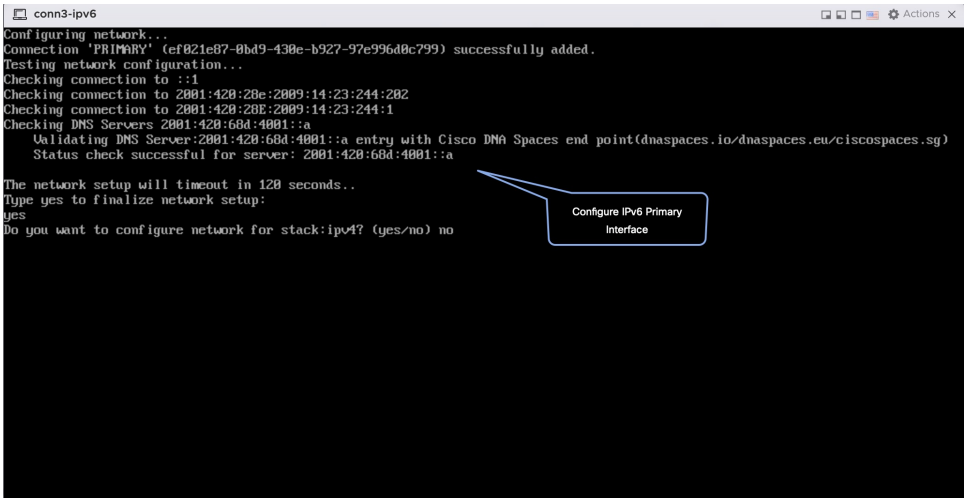


Figure 55: Configuring the Primary Interface: IPv6



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.

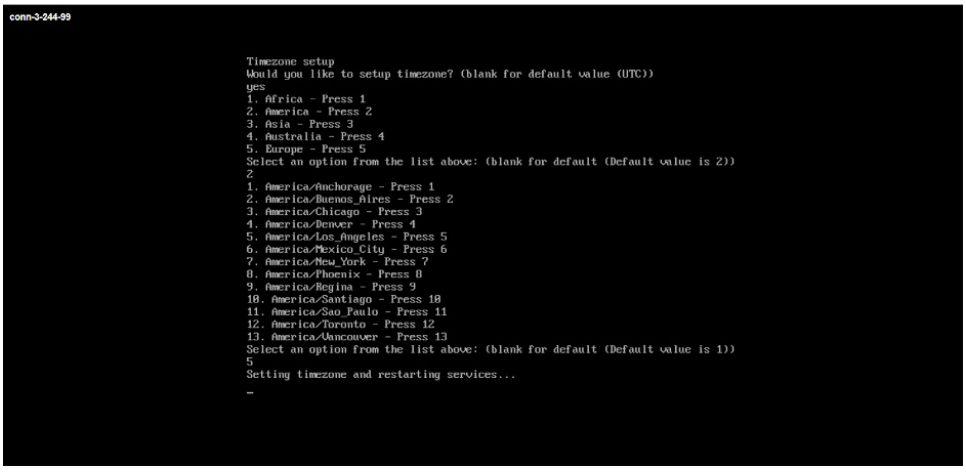
Step 15 Confirm the setup.

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.

Step 17 Enter the time zone.

Figure 56: Time Zone



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 57: Configure NTP

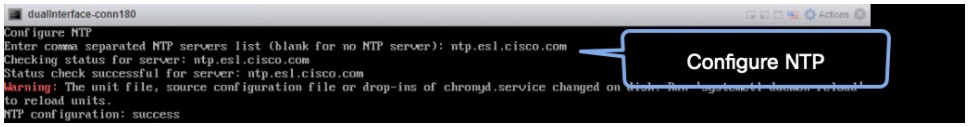
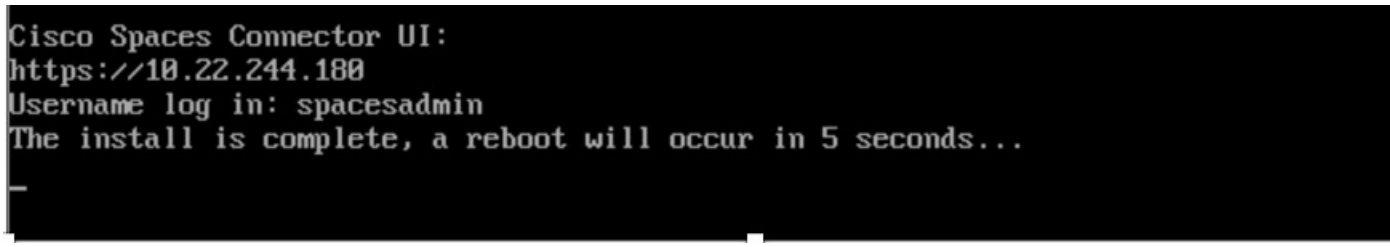


Figure 58: Configure NTP

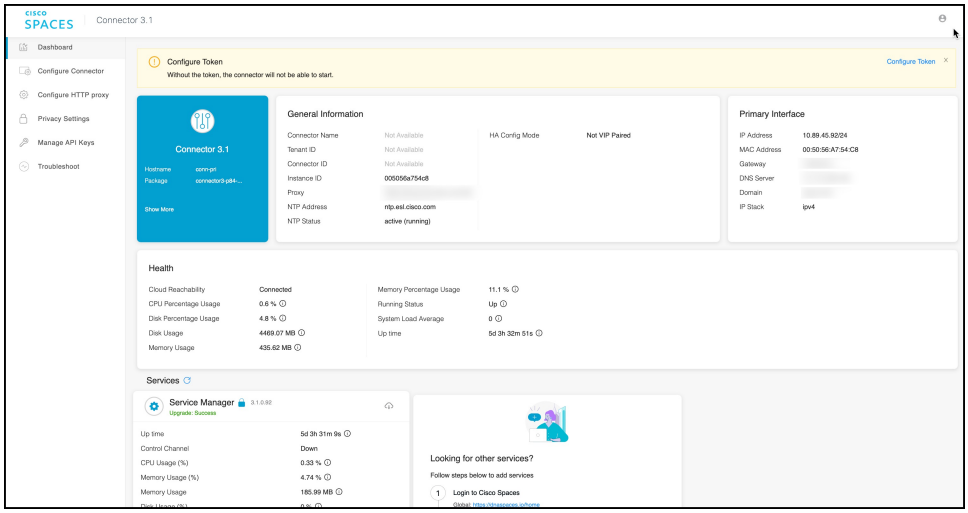
Step 19 Note the URL (https://connector-ip) before the automatic reboot. You can use this URL later to open the connector GUI.

Figure 59: ConnectorGUI



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 60: Connector GUI



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

What to do next

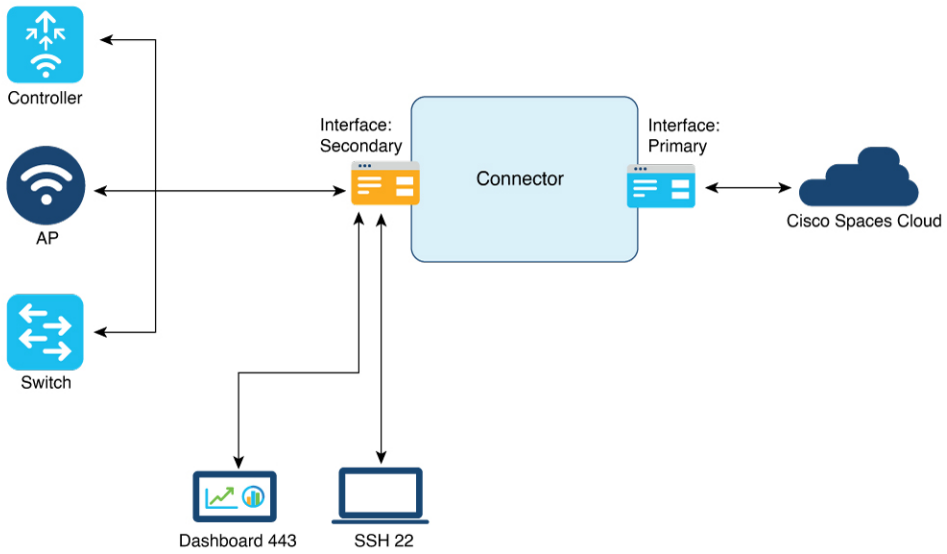
You can now Activating Connector 3 on Cisco Spaces.

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 61: 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.

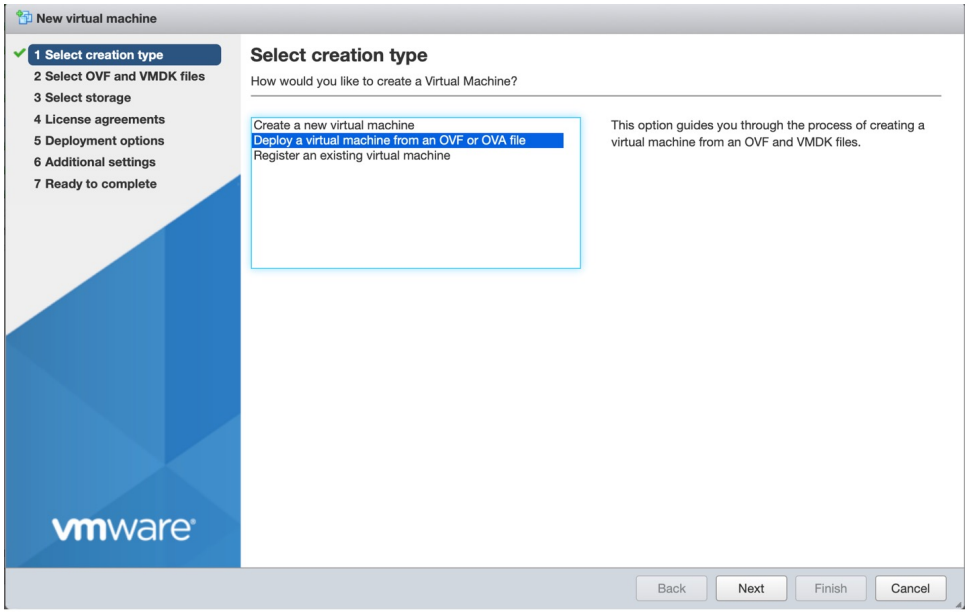
Procedure

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.

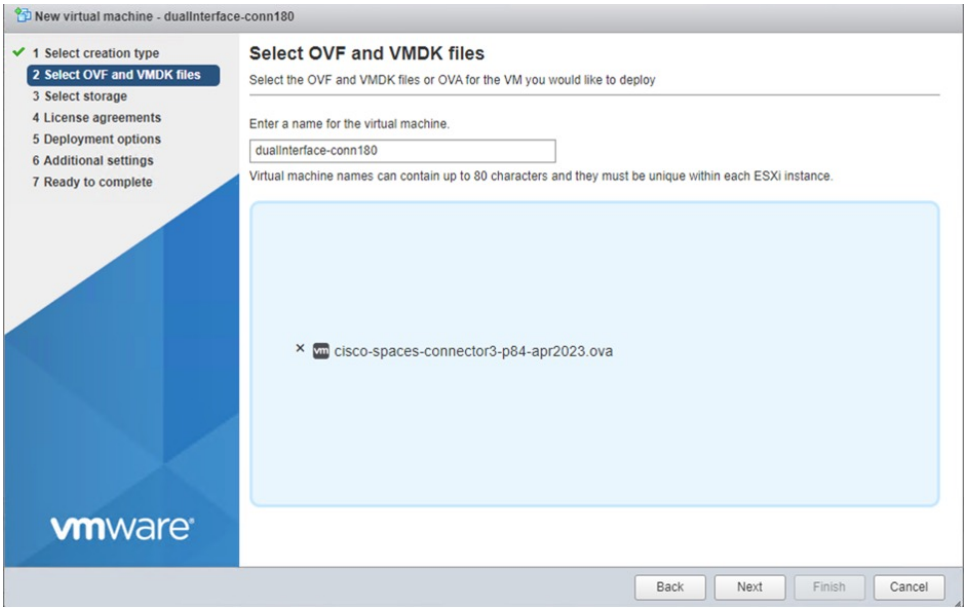
Step 3 In the **Select creation type** window, choose **Deploy a virtual machine from an OVF or OVA file**, and click **Next**.

Figure 62: Select Creation Type



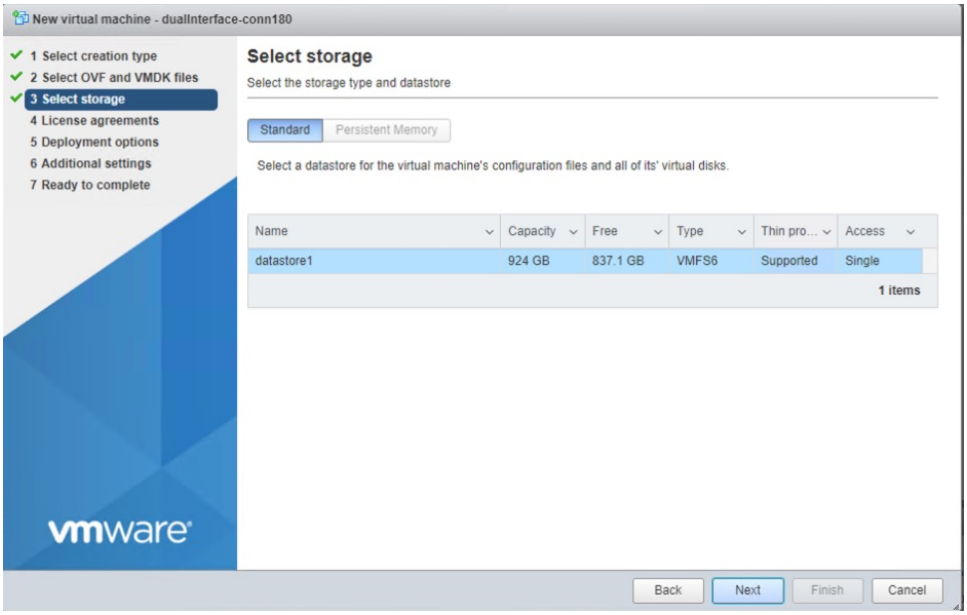
Step 4 In the **Select OVF and VMDK files** window, enter a name for the virtual machine. Click the blue area to either select files from the computer or drag and drop files. Click **Next**.

Figure 63: Select OVF and VMDK files



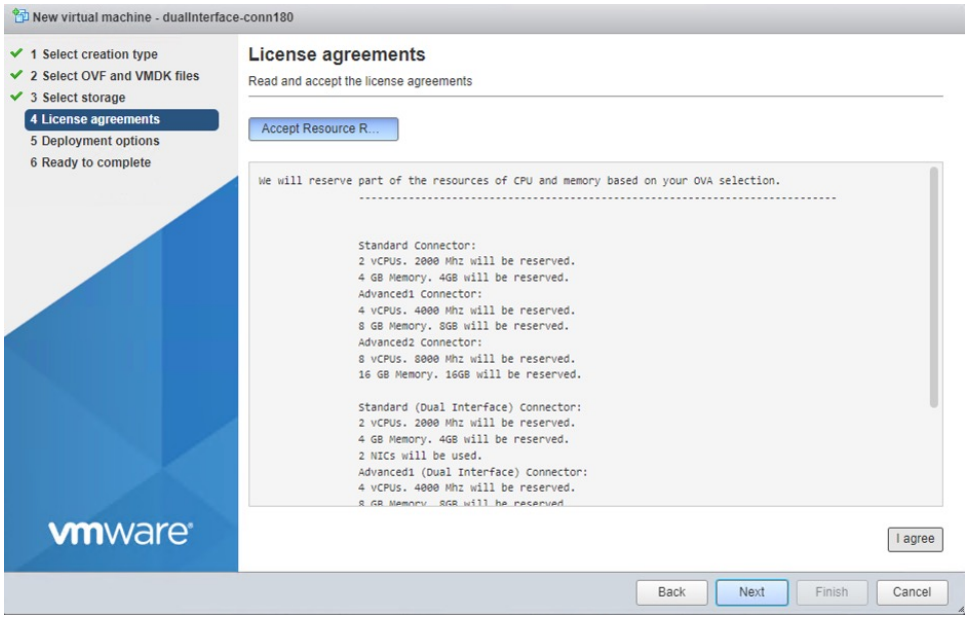
Step 5 In the **Select storage** window, the **Standard** storage configuration is displayed. Click **Next**.

Figure 64: Select Storage



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 65: License agreements



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

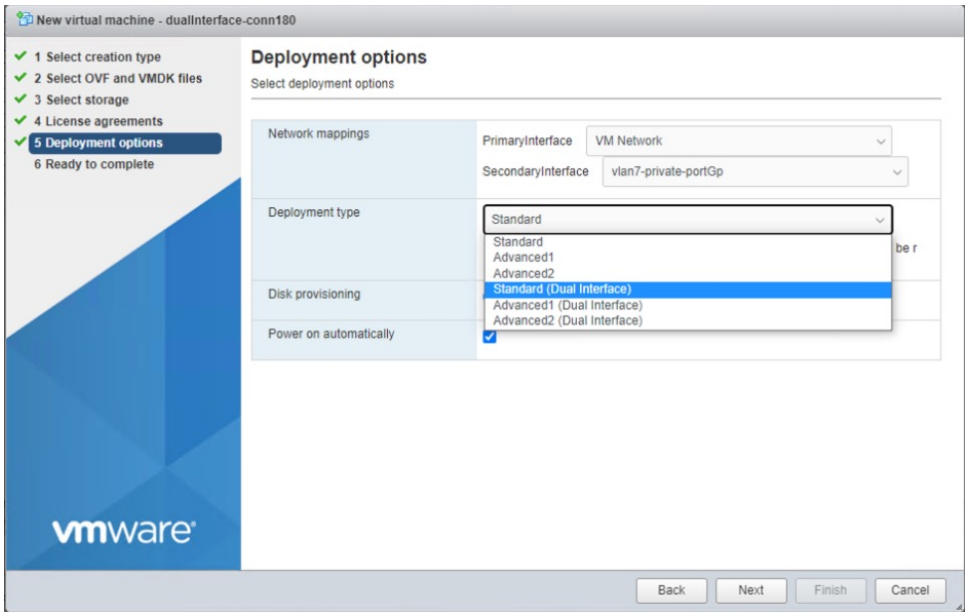
a) In the **PrimaryInterface** field, enter the name of the external-facing interface.

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.

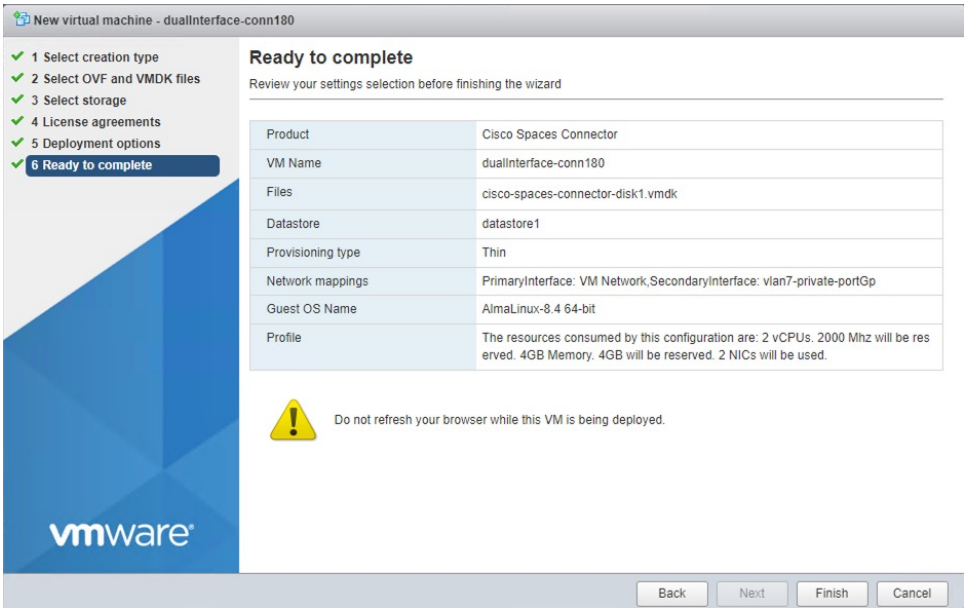
- **Standard (Dual Interface)**
- **Advanced1 (Dual Interface)**
- **Advanced2 (Dual Interface)**

Figure 66: Deployment options



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

Figure 67: Ready to complete



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 68: Configuring the Primary Interface: IPv4

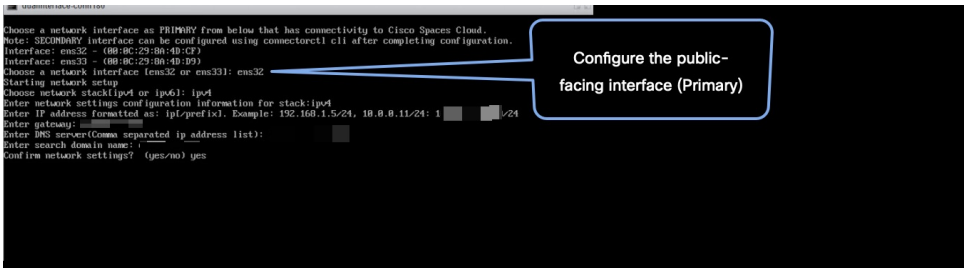
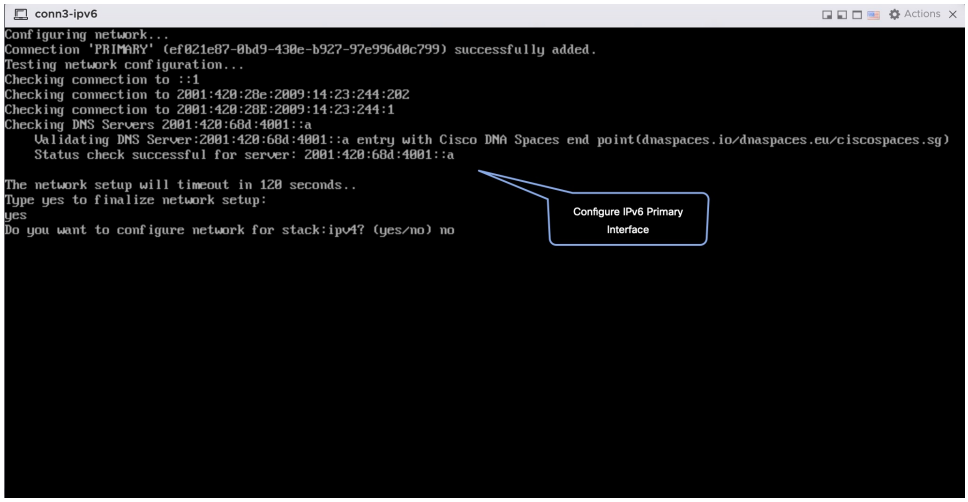


Figure 69: Configuring the Primary Interface: IPv6



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.

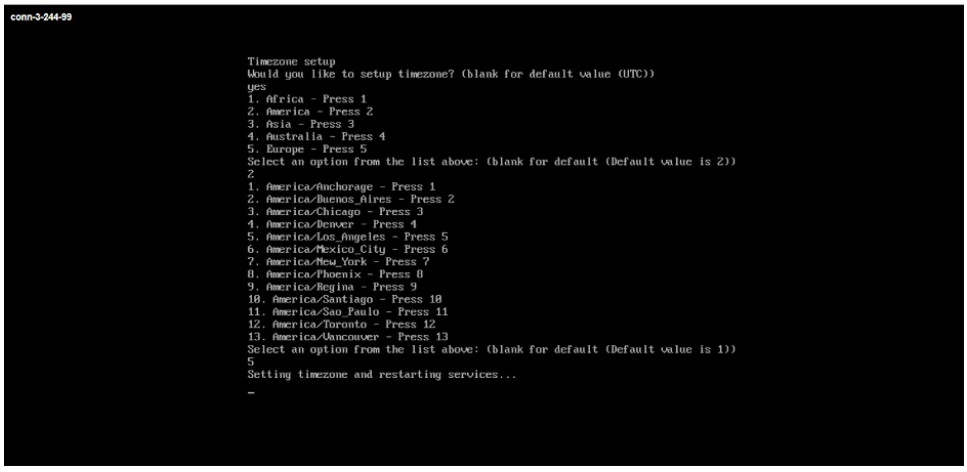
Step 13 Reset the password for the **spacesadmin** user.

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 70: Time Zone



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 71: Configure NTP

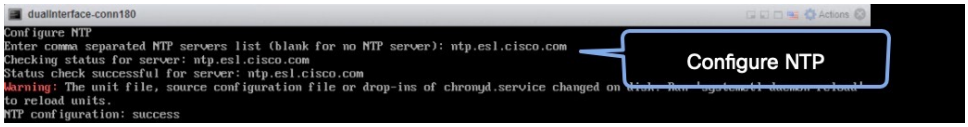
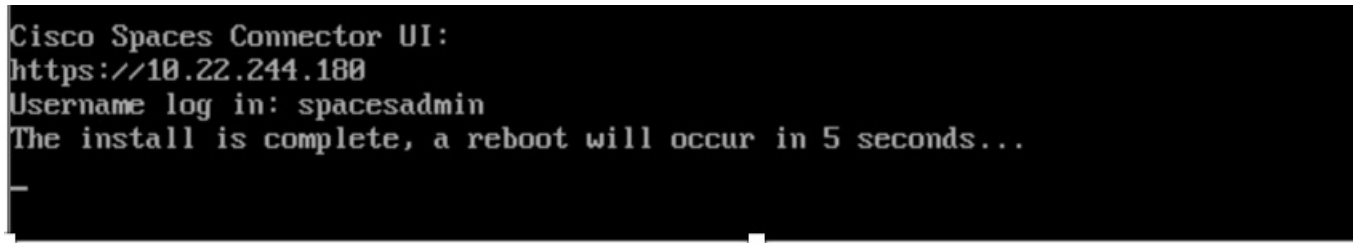


Figure 72: Configure NTP

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

Figure 73: ConnectorGUI



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.

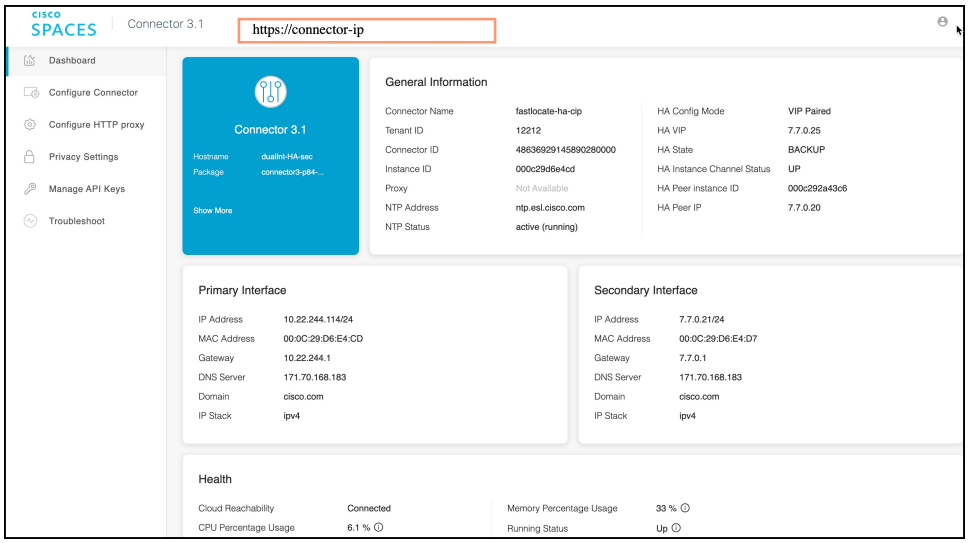
```
[spacesadmin@connector ~]$ connectorctl network show
 Executing command:network
Command execution status:Success
-----------------------
==================Network Config=================
Hostname    - connector-p84-april1


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 -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 74: ConnectorGUI



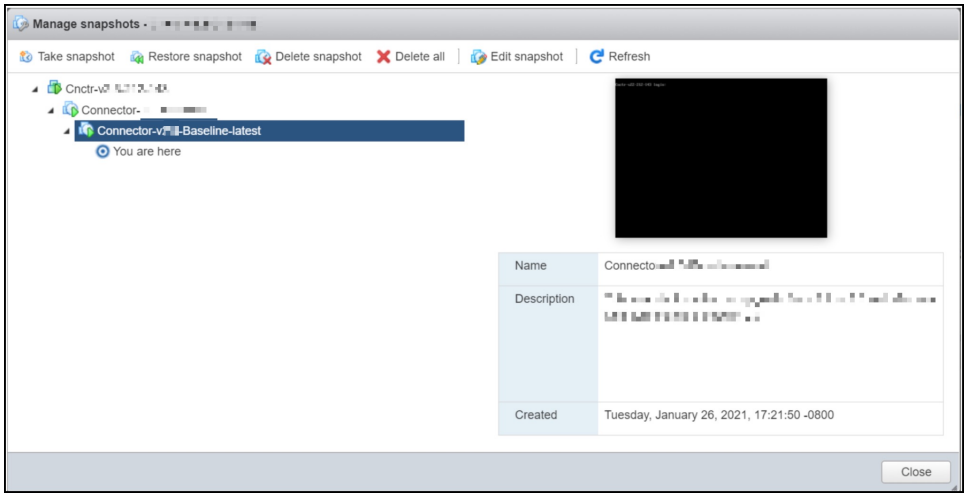
Note The root user is disabled and is used only for advanced troubleshooting by the Cisco Support team.

Using Snapshots for Backup

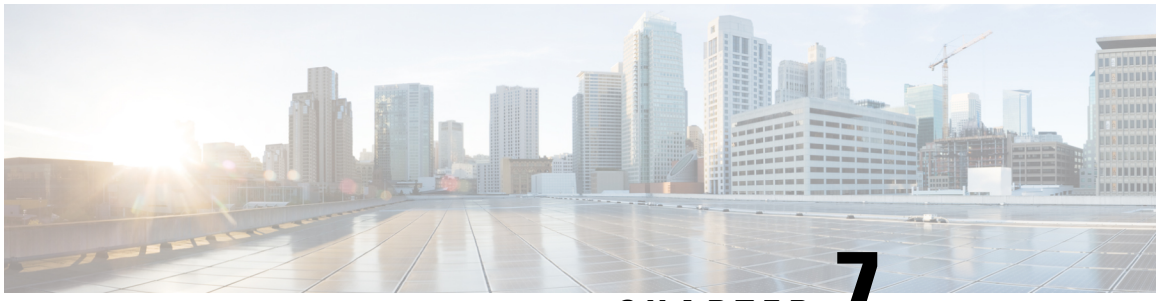
You can use the snapshot of a deployed connector OVA for backing up your connector. Ensure that the following prerequisites in place:

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

Figure 75: Backing Up Using a Snapshot



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



CHAPTER 7

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 63
- Downloading and Deploying HYPER-V, on page 70

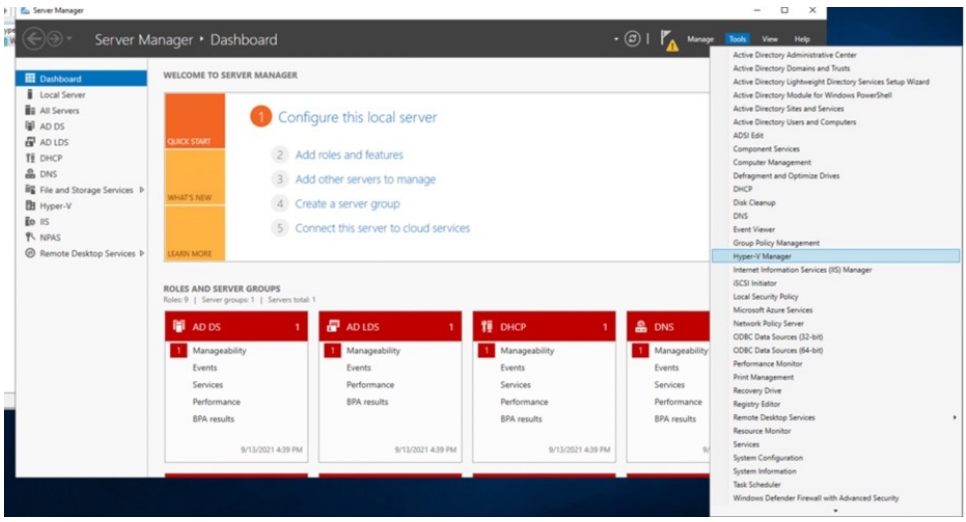
Creating a Virtual Switch

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

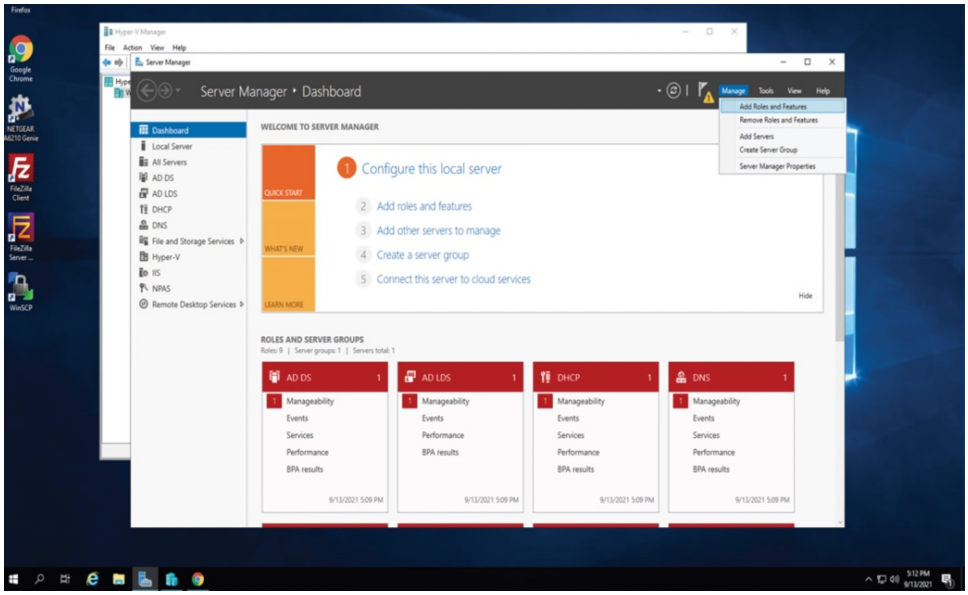
Step 1 Navigate to **Windows > Server Manager**.

Figure 76: Windows > Server Manager



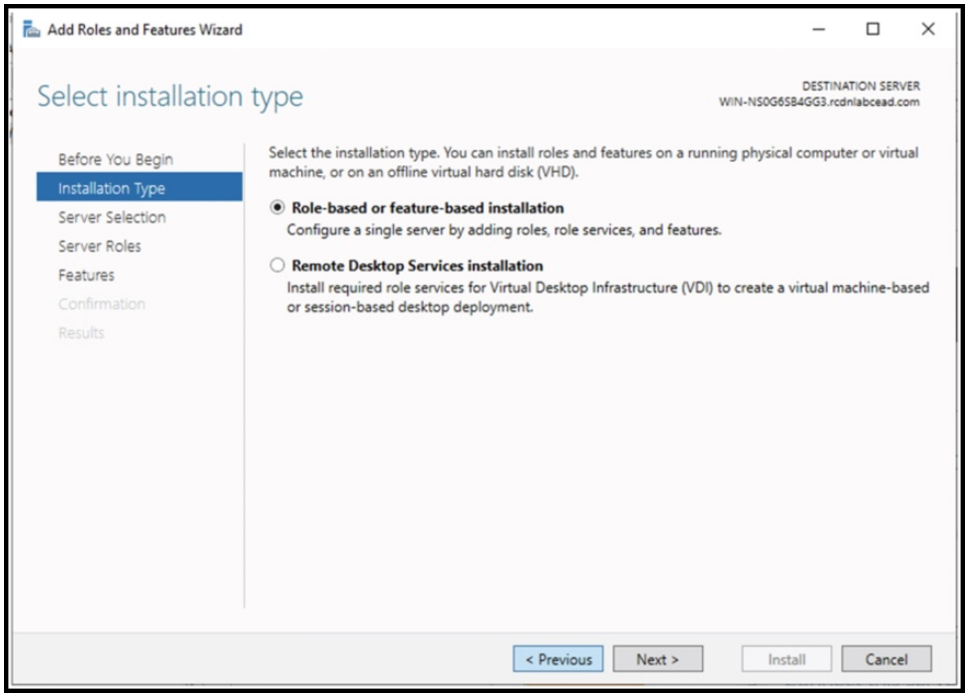
Step 2 Choose **Manage > Add Roles and Features**.

Figure 77: Manage > Add Roles and Features



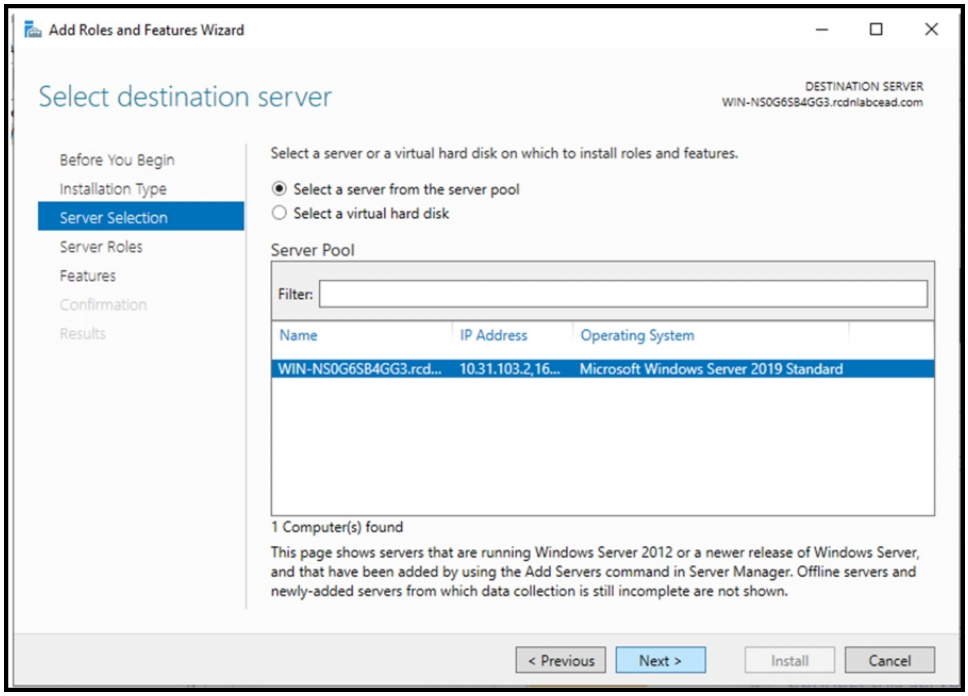
Step 3 Click the **Role-based or feature-based installation** radio button.

Figure 78: Role-based or Feature-Based Installation



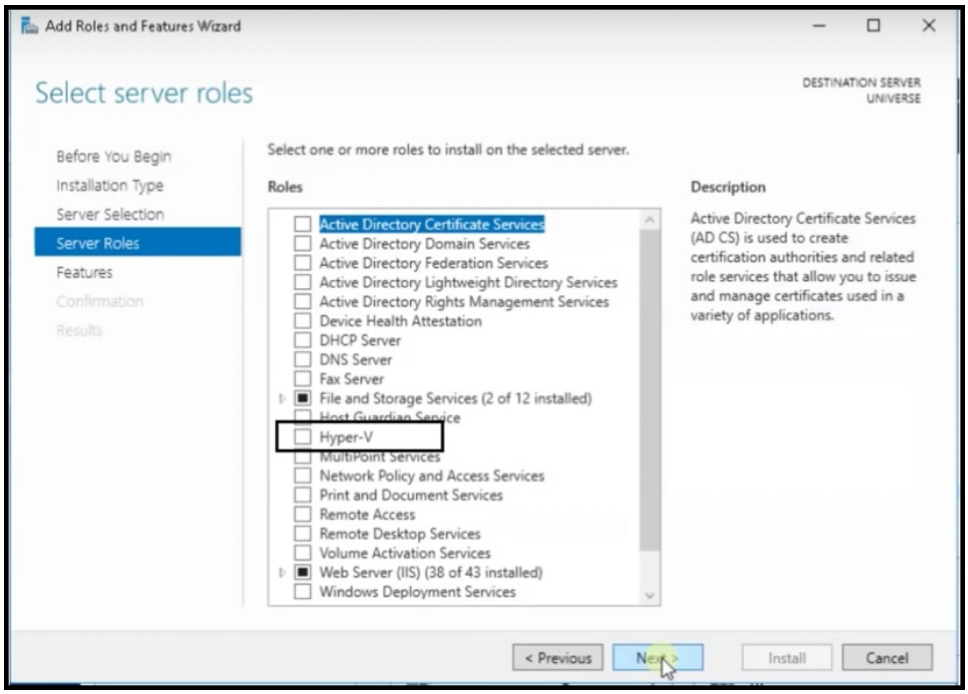
Step 4 Click the **Select a server from the server pool** radio button.

Figure 79: Select a Server From the Server Pool



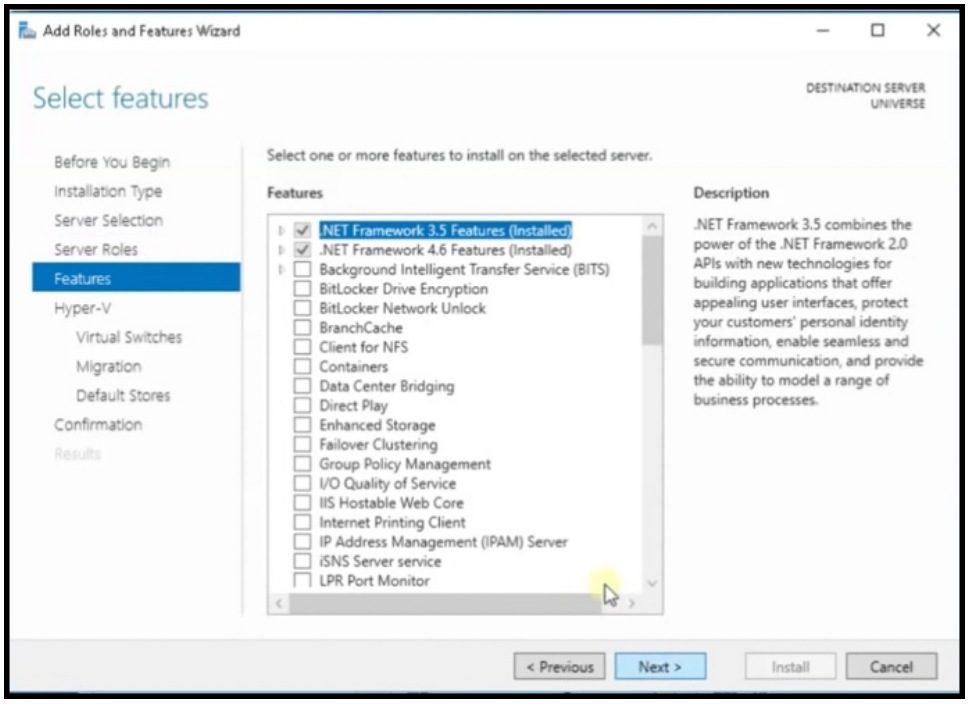
Step 5 In the **Select server roles** window, check the Hyper-V checkbox, and click **Next**.

Figure 80: Select Server Roles



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

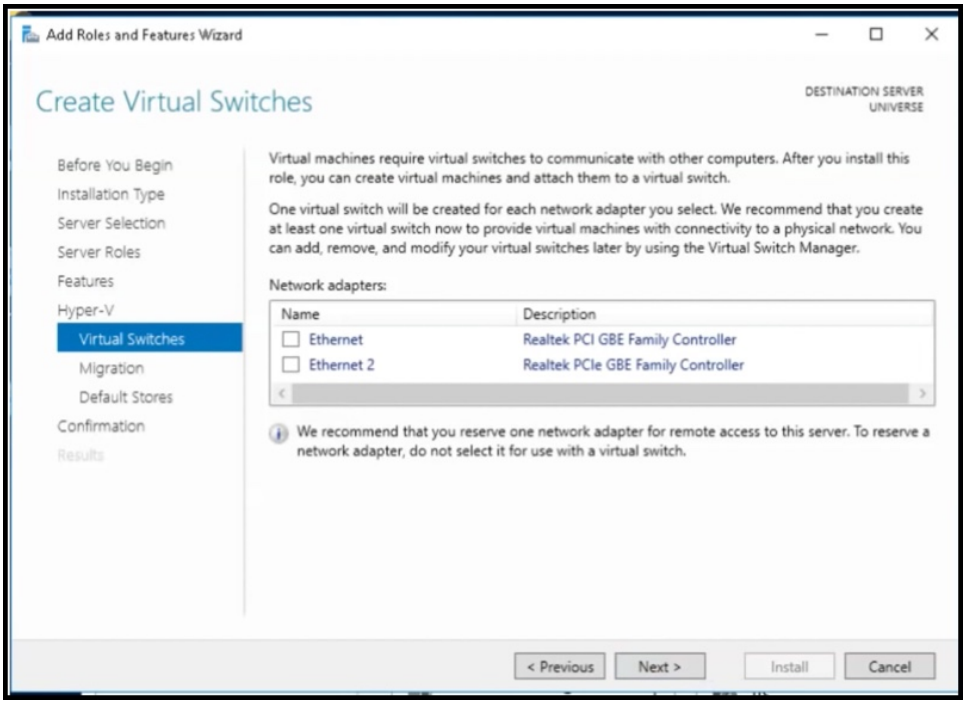
Figure 81: Select Features



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

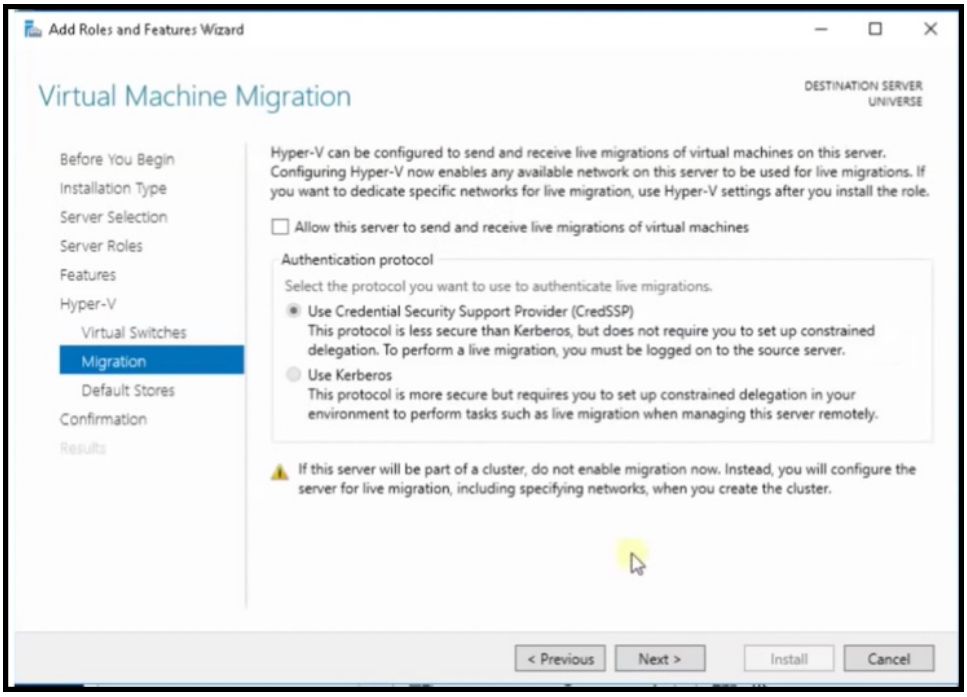
a) In the **Virtual Switches** window, click **Next**.

Figure 82: Virtual Switches



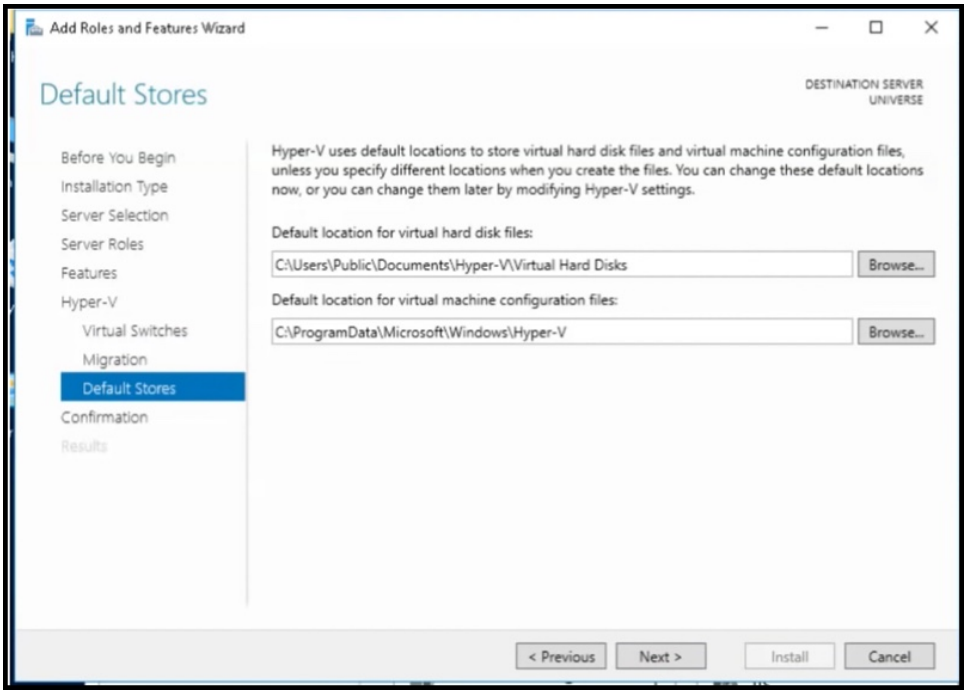
b) In the **Migration** window, click **Use Credential Security Support Provider** (CredSSP) radio button, and click **Next**.

Figure 83: Use Credential Security Support Provider



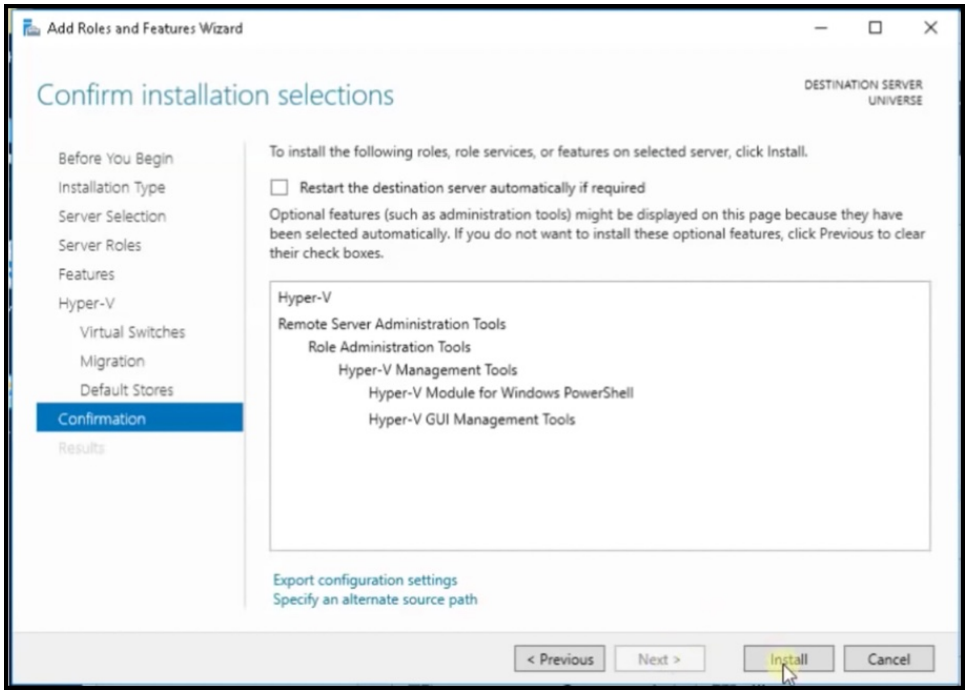
c) In the **Default Stores** window, select the location to install files or retain the default locations, and click **Next**.

Figure 84: Default Stores



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

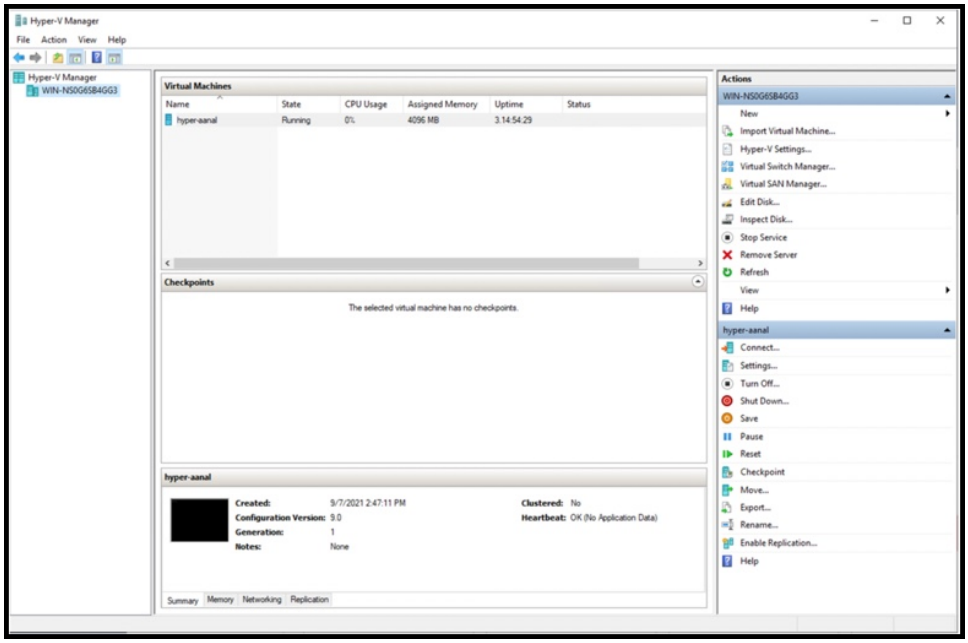
Figure 85: Confirm the Installation Settings



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

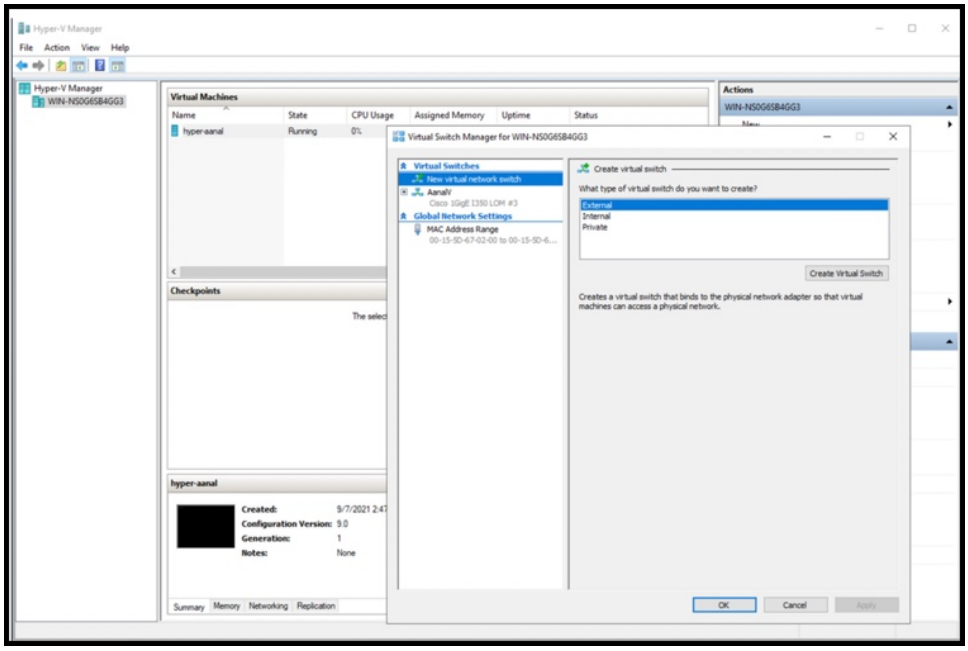
Step 10 In Hyper-V Manager, choose **Actions > Virtual Switch Manager**.

Figure 86: Actions > Virtual Switch Manager



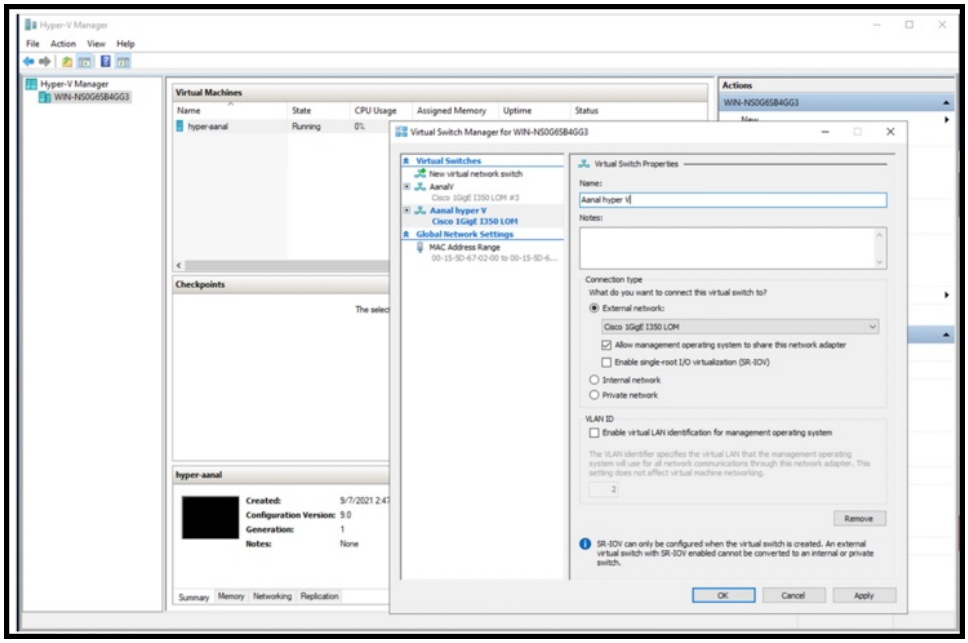
Step 11 In the **Virtual Switch Manager for** window, click **New virtual network switch**. In the **Create virtual switch** window, click **External** and then click **Create Virtual Switch**.

Figure 87: Create Virtual Switch



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 88: Virtual Switch Properties



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 63

Procedure

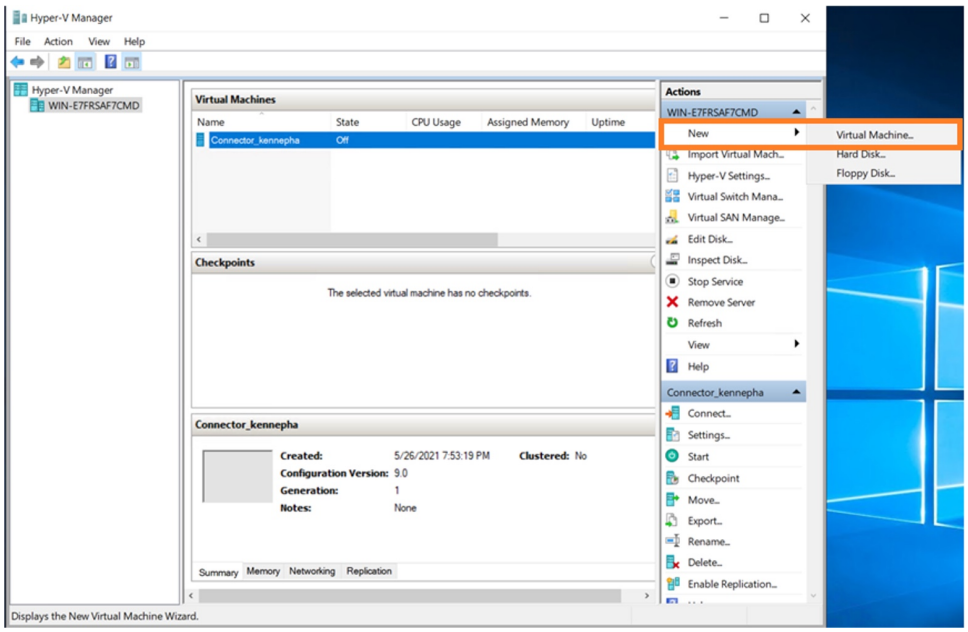
Step 1 Download connector .hyperv (HYPERV) image from Cisco.com.

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.

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

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

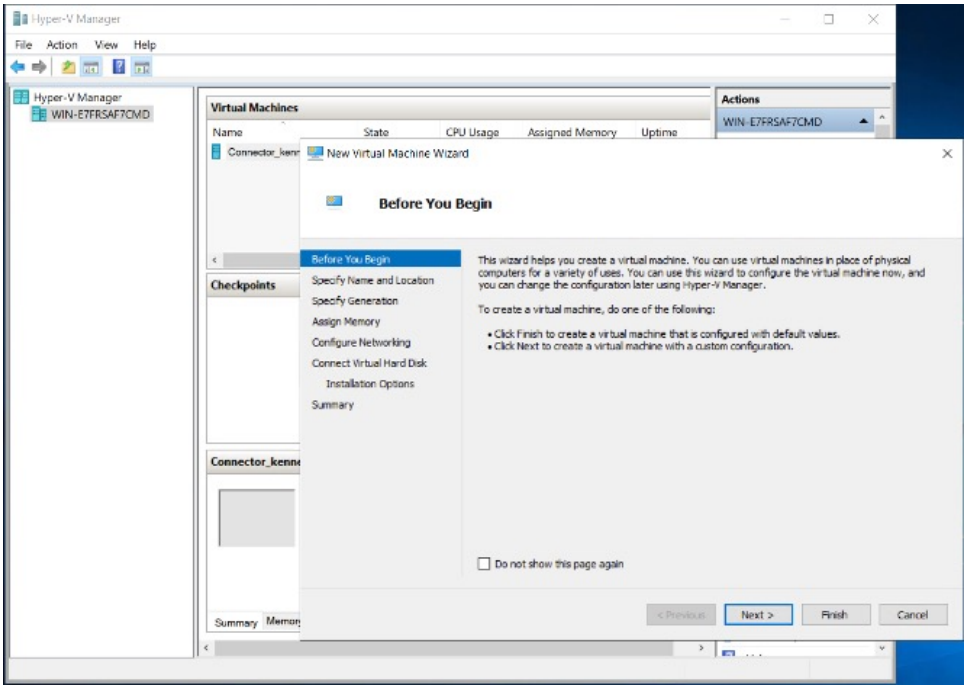
Figure 89: Create New Virtual Machine



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

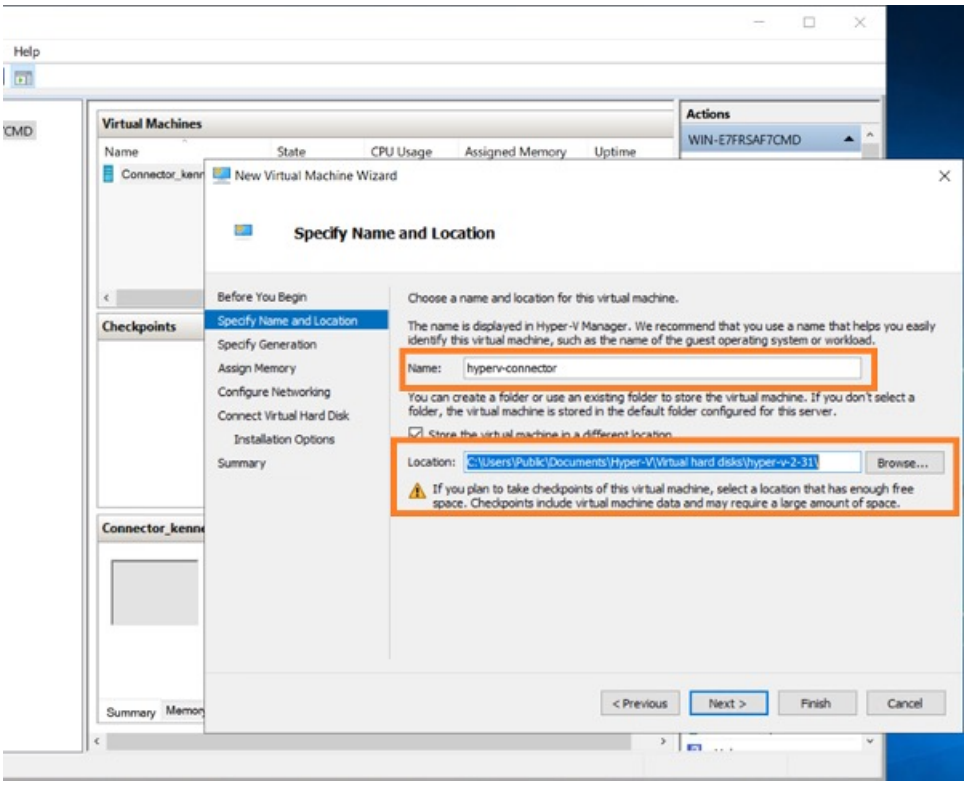
Step 5 Click **Next** to begin HYPER-V deployment.

Figure 90: Click Next to Begin Deployment



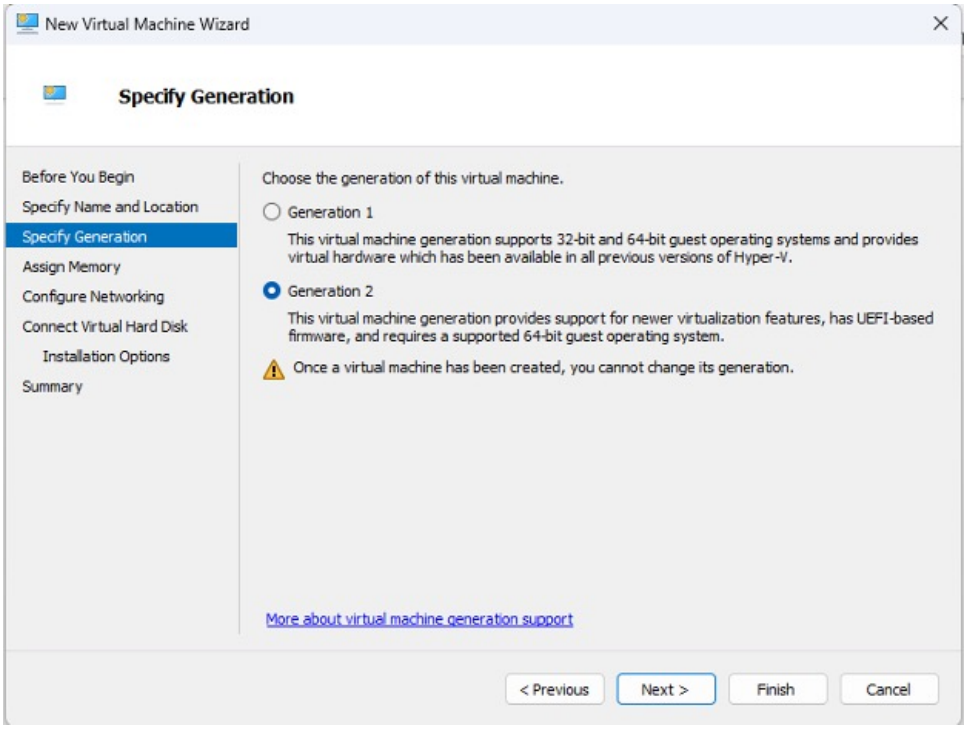
Step 6 Provide the **Name** of the connector and select the location to create the virtual machine.

Figure 91: Name of Connector



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

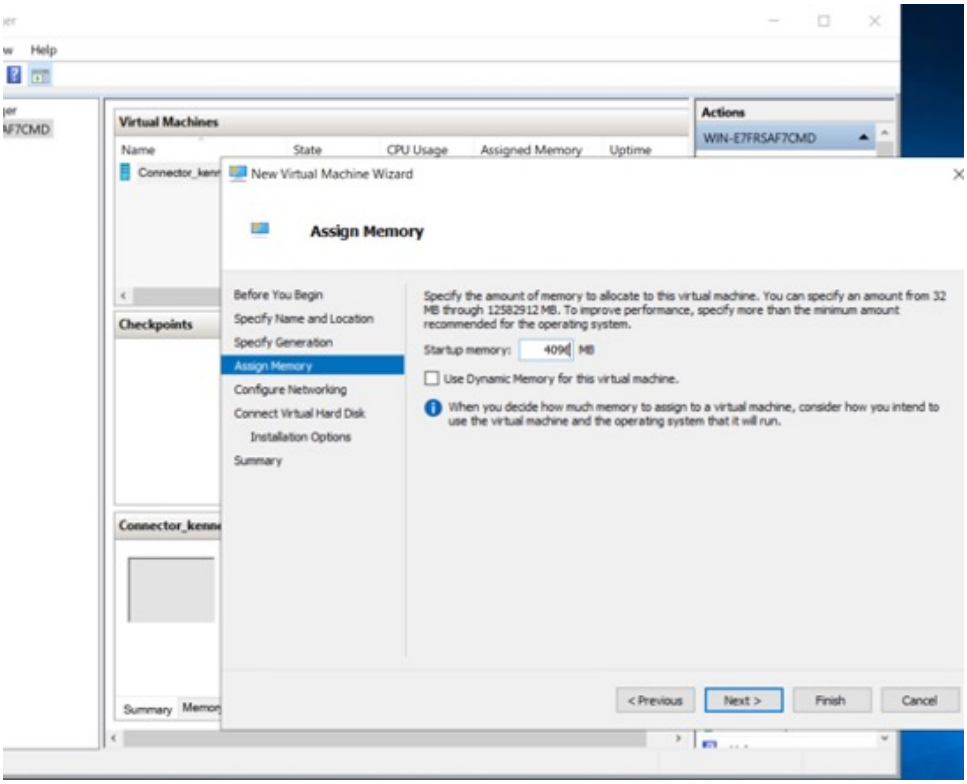
Figure 92: Specify Generation



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

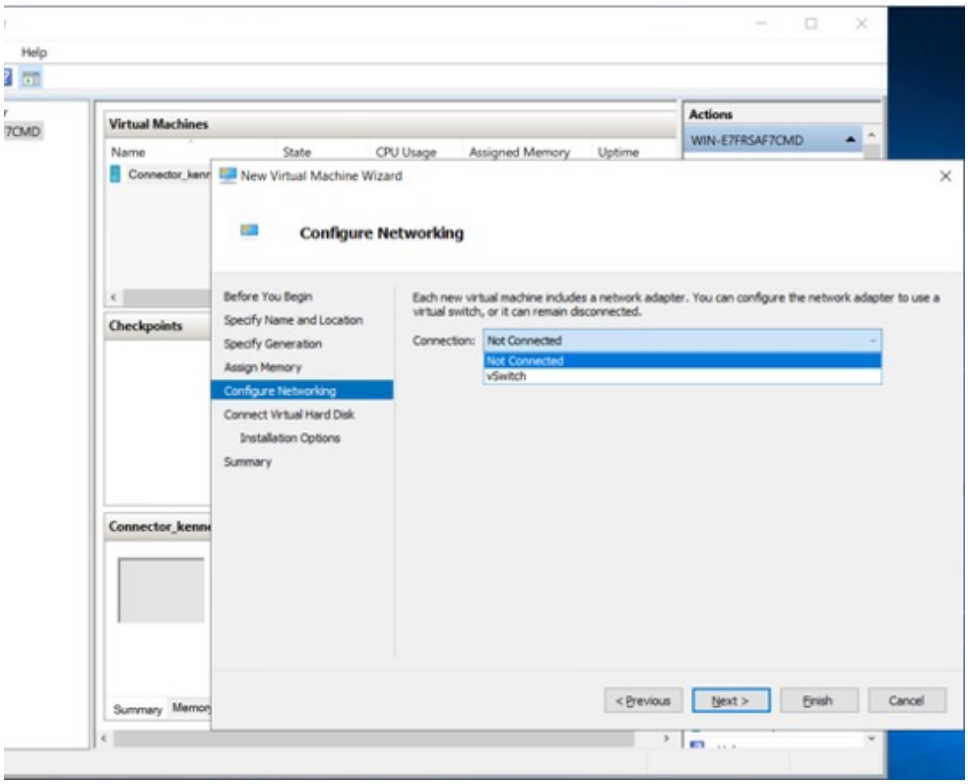
Note 4096 MB (4GB) of memory is equivalent to the standard configuration of HYPER-V.

Figure 93: Assign Memory



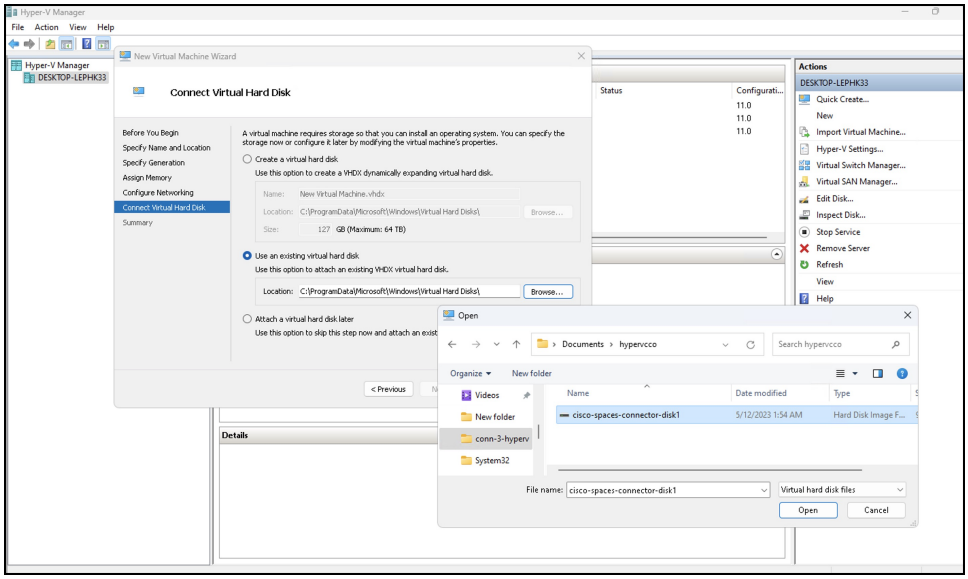
Step 9 In the **Configure Networking** window, select the vSwitch that you created as a prerequisite.

Figure 94: Configure Networking



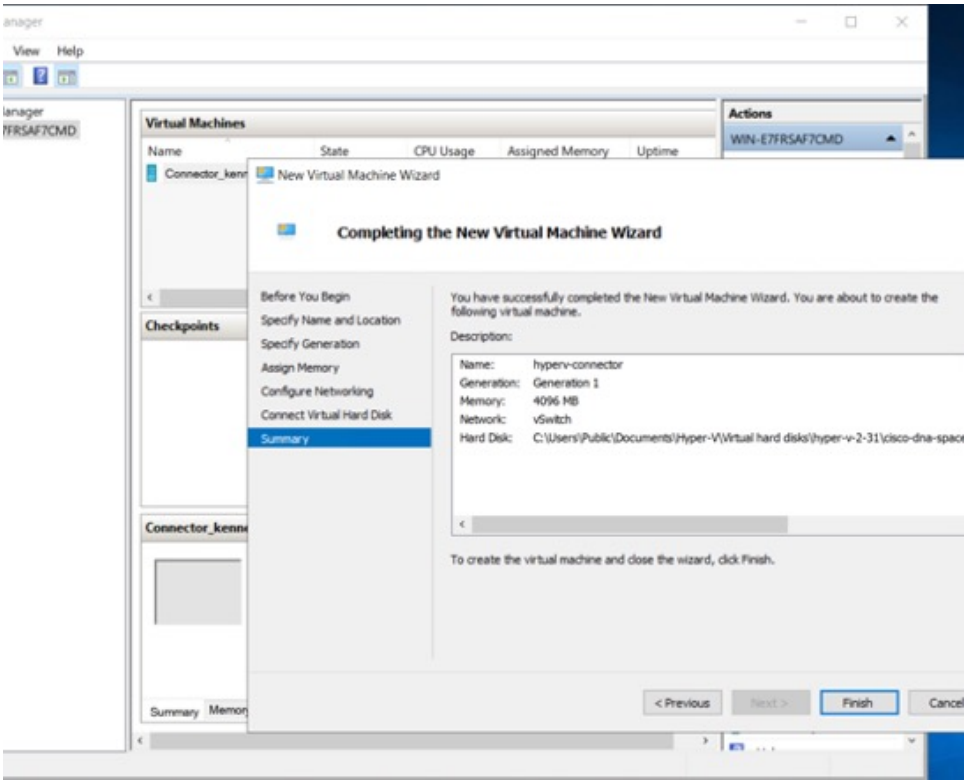
Step 10 In the **Connect Virtual Hard Disk** window, select the **Use an existing hard disk** option, and select the folder location where the VHDX file has been stored (Step 1).

Figure 95: Connect Virtual Hard Disk



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

Figure 96: Completing the New Machine Wizard

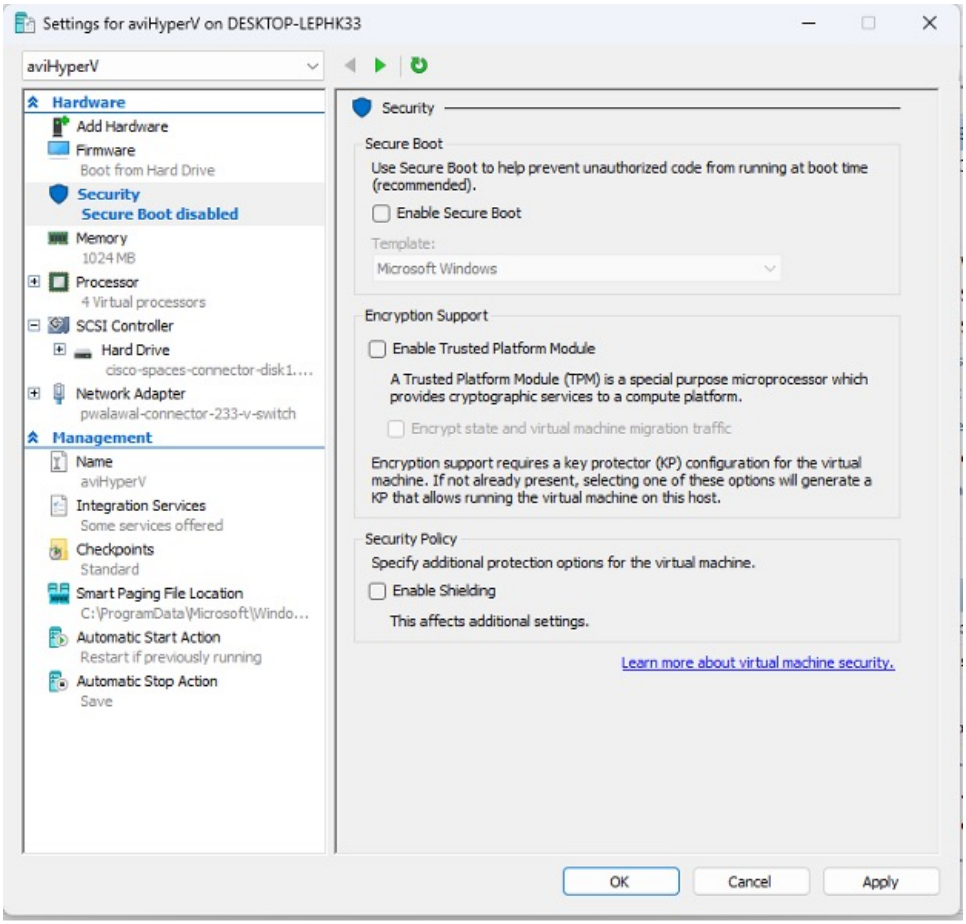


A HYPER-V instance is created.

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.

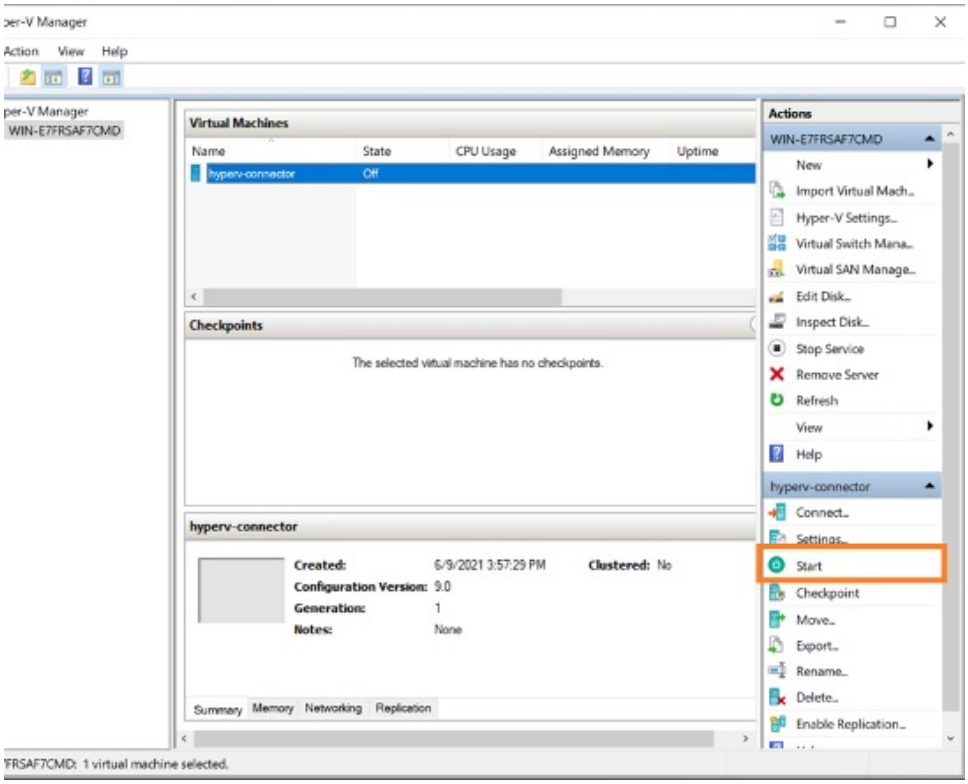
Figure 97: Enable Secure Boot



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

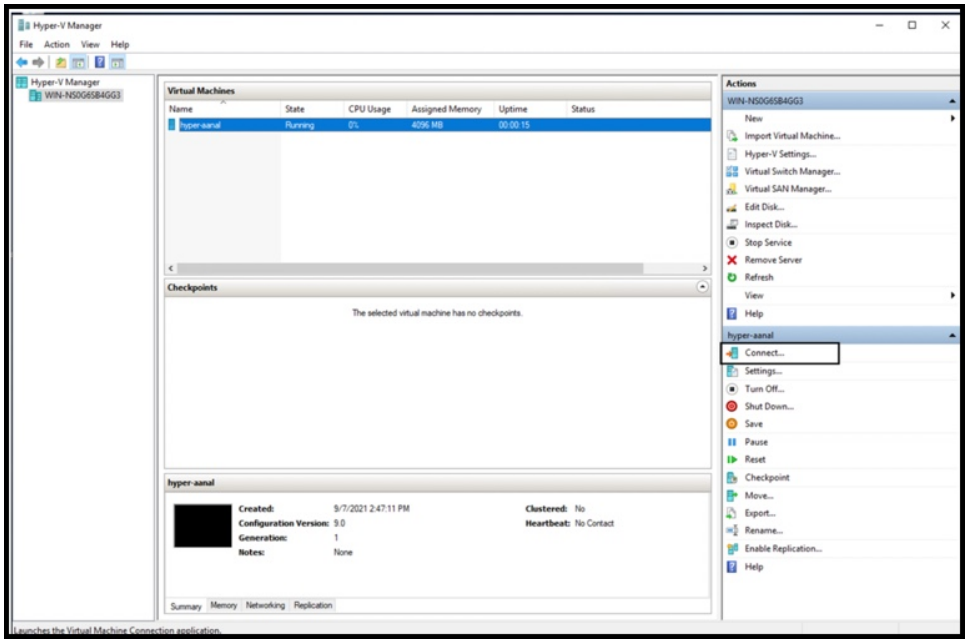
Step 13 Select the HYPER-V instance created, and click **Start**.

Figure 98: Select The Hyper-V Instance



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

Figure 99: Select The Hyper-V Instance



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 100: Configuring the Primary Interface: IPv4

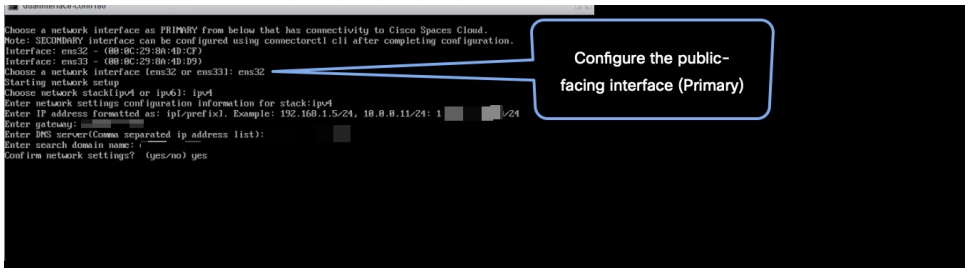
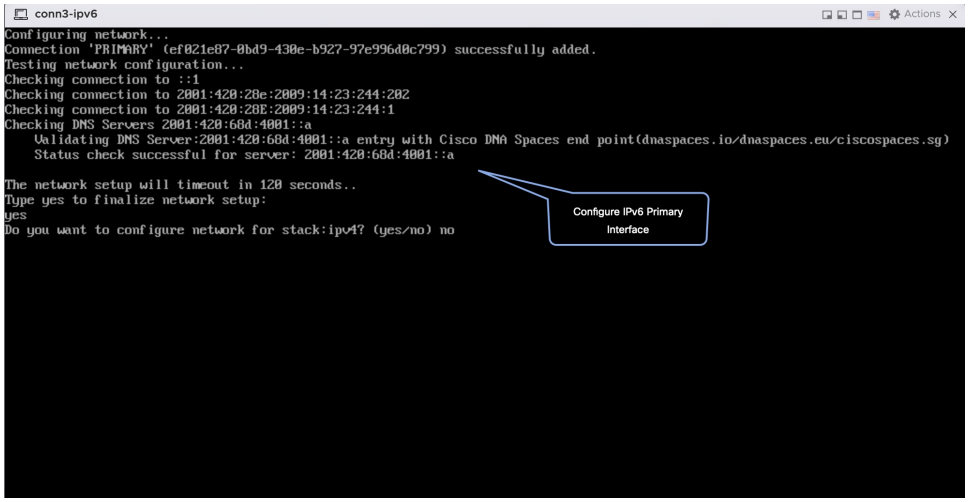


Figure 101: Configuring the Primary Interface: IPv6



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.

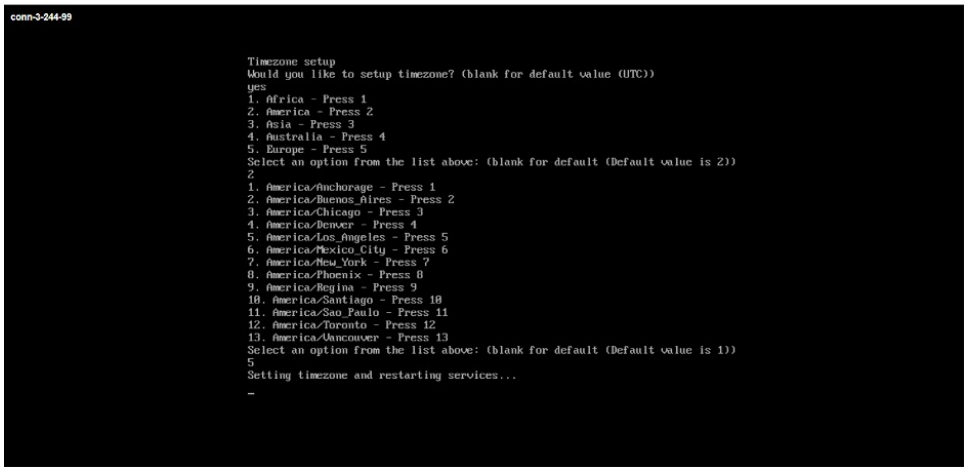
Step 19 Confirm the setup.

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.

Step 21 Enter the time zone.

Figure 102: Time Zone



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 103: Configure NTP

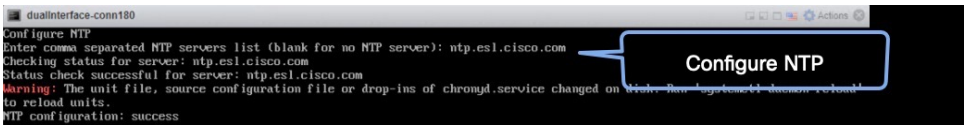
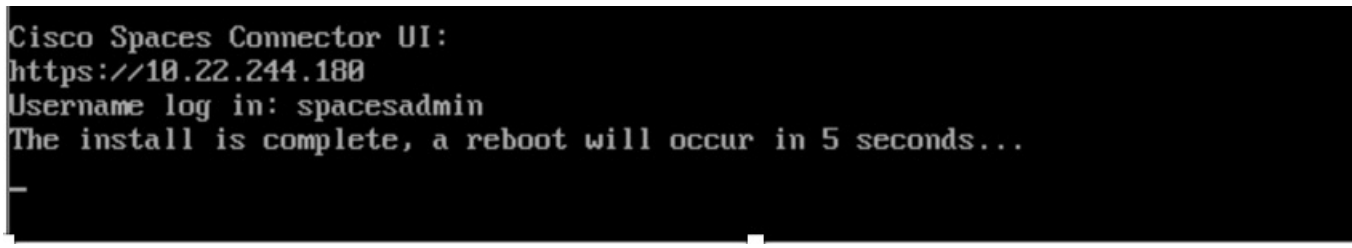
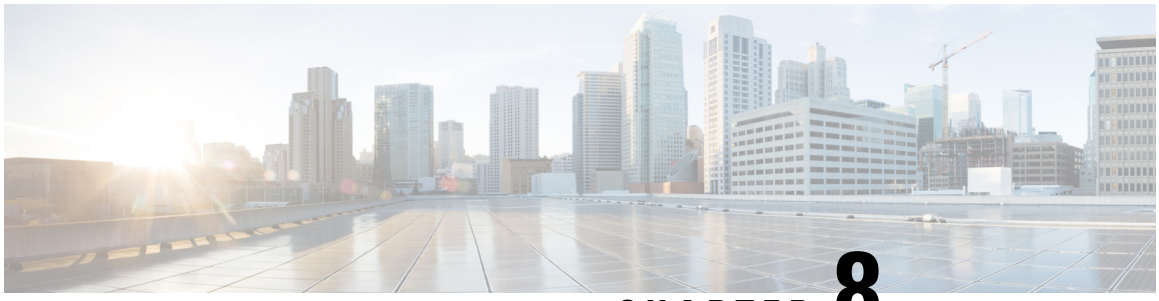


Figure 104: Configure NTP

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

Figure 105: ConnectorGUI





CHAPTER 8

Connector on Cisco Spaces

- Activating Connector 3 on Cisco Spaces, on page 81
- Monitor the Status of Service Installation, on page 88

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 45

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**.

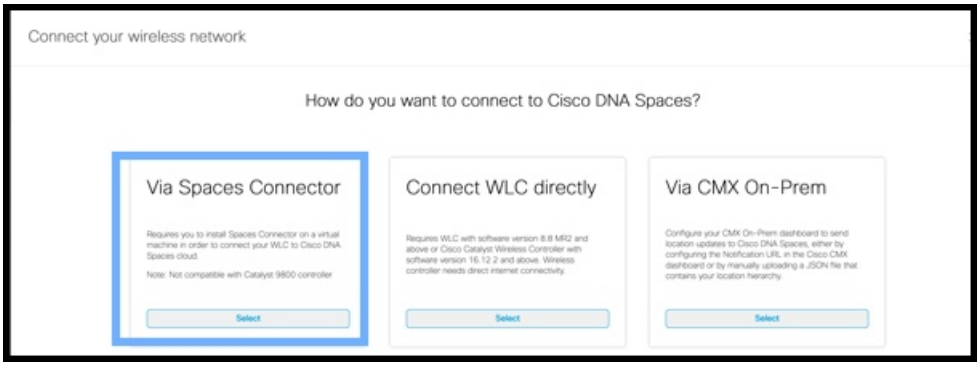
Step 3 In the **Get your wireless network connected with Cisco DNA Spaces** area, click **Add New**.

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

Figure 106: Choose Cisco AireOS Controller/Catalyst 9800 Wireless Controller

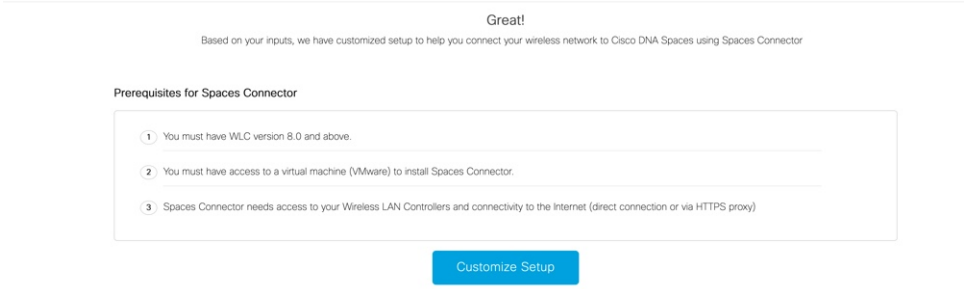
Step 5 In the **Via Spaces Connector** area, click **Select**.

Figure 107: Via Spaces Connector



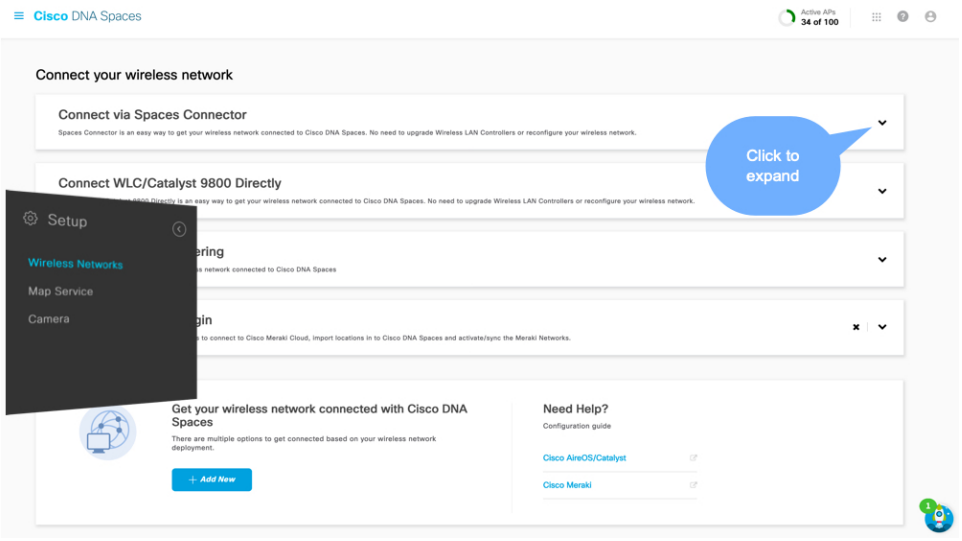
Step 6 In the **Prerequisites for Spaces Connector** dialog box, click **Continue Setup**.

Figure 108: Read Prerequisites for Spaces Connector



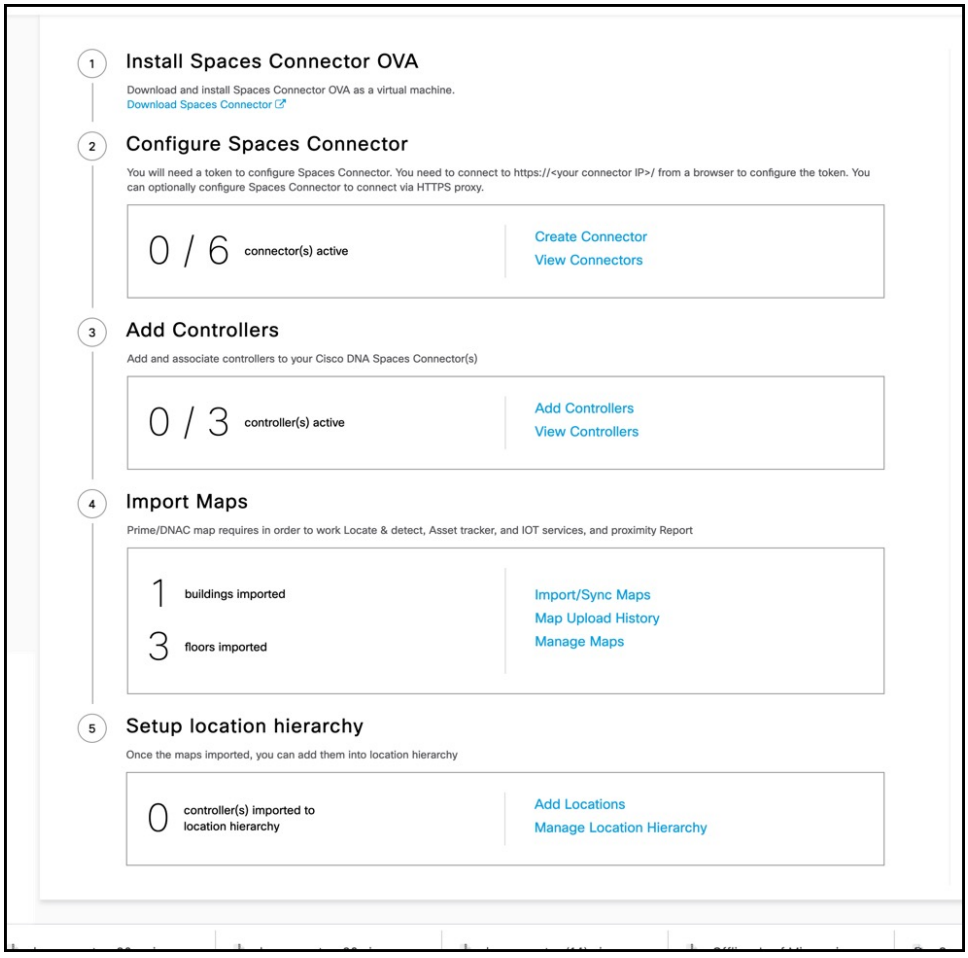
Step 7 Expand the **Connect via Spaces Connector** area using the respective drop-down arrow.

Figure 109: Expand Connect via Spaces Connector



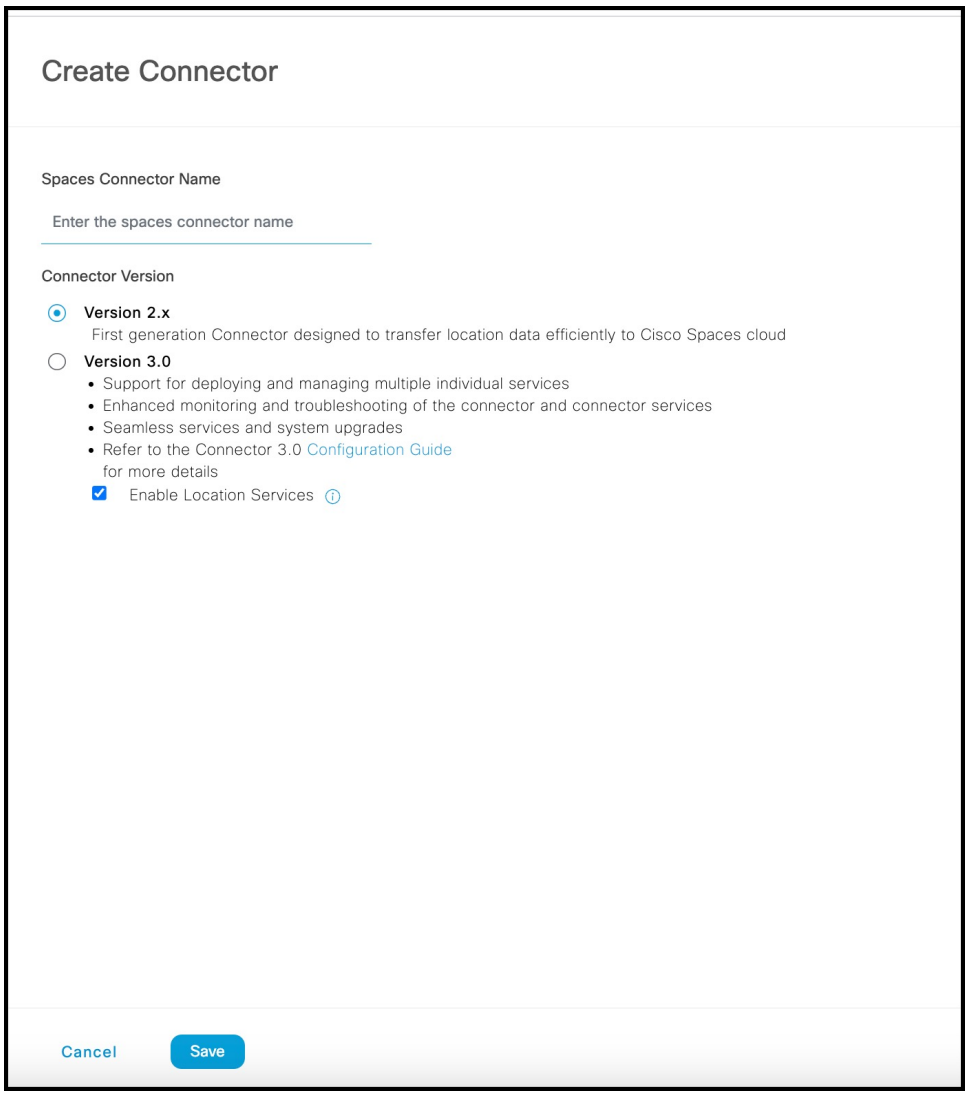
Step 8 In the displayed list of steps, in the **Configure Spaces Connector** area, click **Create Connector**.

Figure 110: Connect via Spaces Connector > Create Connector



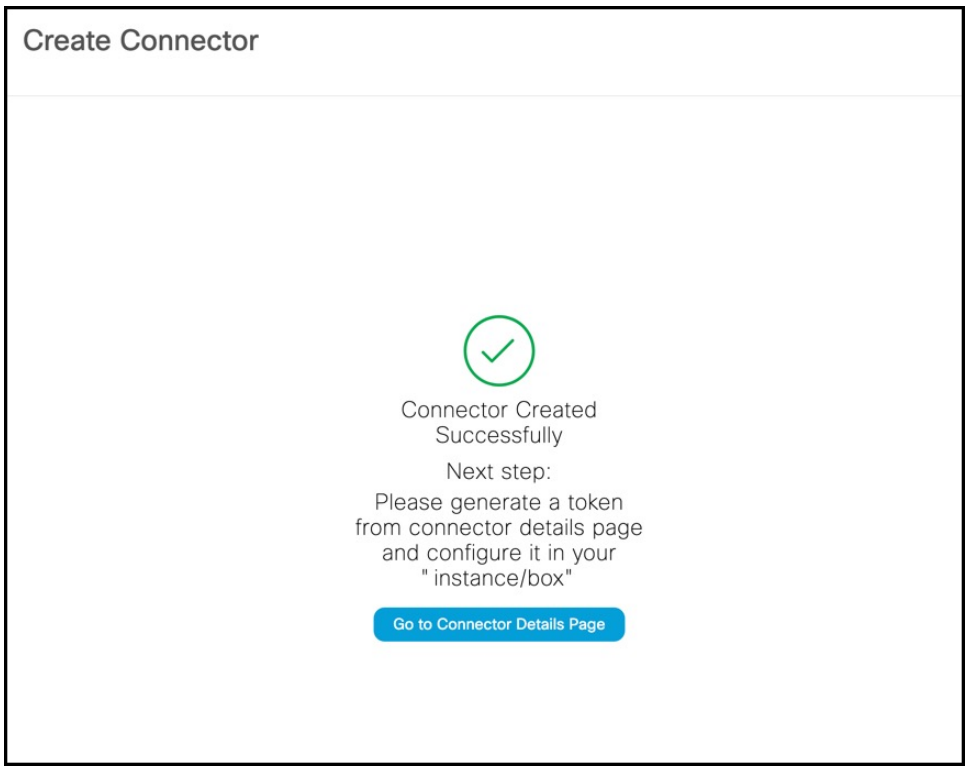
Step 9 In the **Create connector** window that is displayed, enter a name for connector, and click **Version 3.0 (beta).** as the **Connector Version**, and click **Save**.

Figure 111: Name and Version of Connector



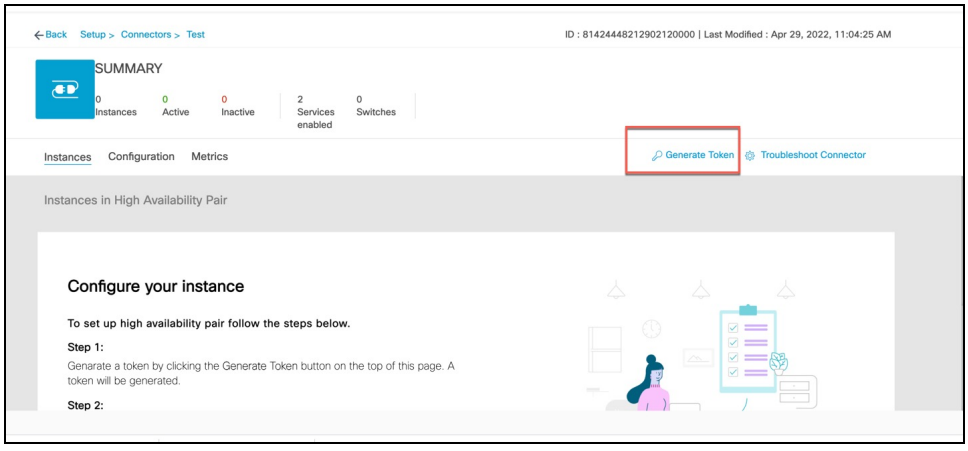
Connector is successfully created. Click **Go to Connector Details** Page.

Figure 112: Connector Created Successfully



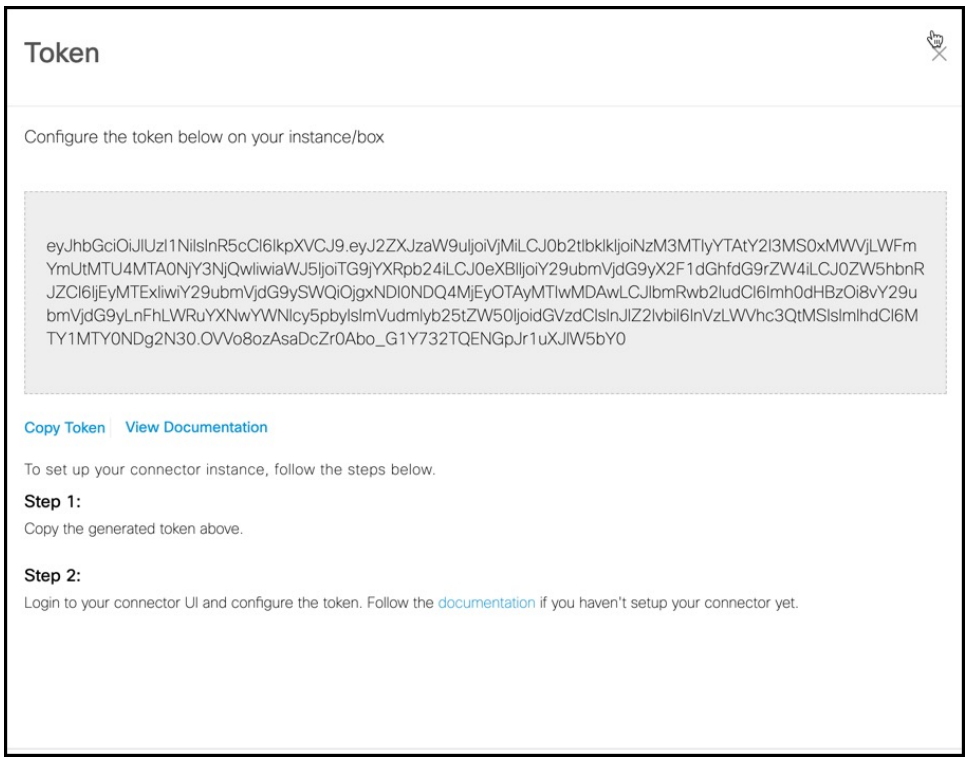
Step 10 In the connector details window, you can see a summary of the configurations for this connector. Click **Generate Token.**

Figure 113: Generate Token



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

Figure 114: Copy Token

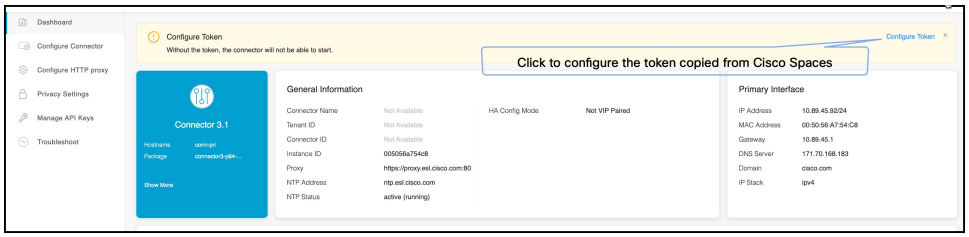


Step 12 Open the connector GUI.

Step 13 (Optional) If your network is behind a proxy, configure the GUI with the proxy. See Configure a Proxy , on page 91

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

Figure 115: Configure Token



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:

- Configure IoT Service (Wireless)
- Configure Hotspot Service

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

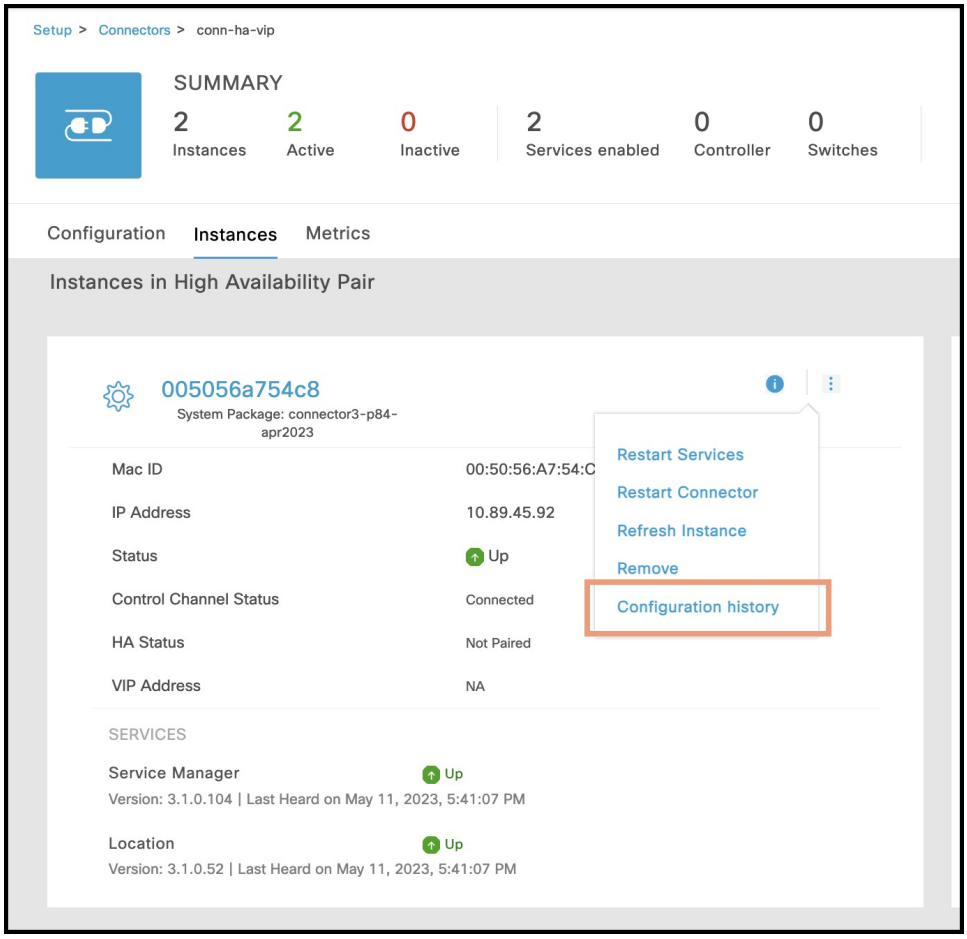
Step 1 From Cisco Spaces dashboard, choose **Setup > Wireless Networks.**

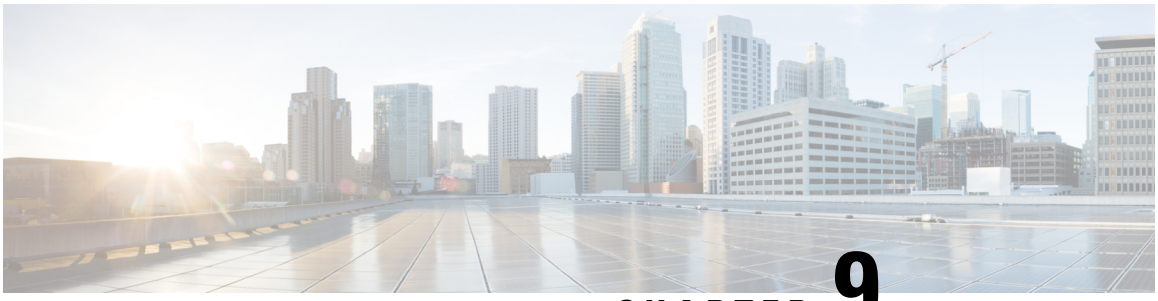
a) In the **Connect via Spaces Connector** area titled **Step 2 Configure Spaces Connector**, click **View Connectors**.

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 116: Monitoring the Status of Service installation





CHAPTER 9

Connector GUI

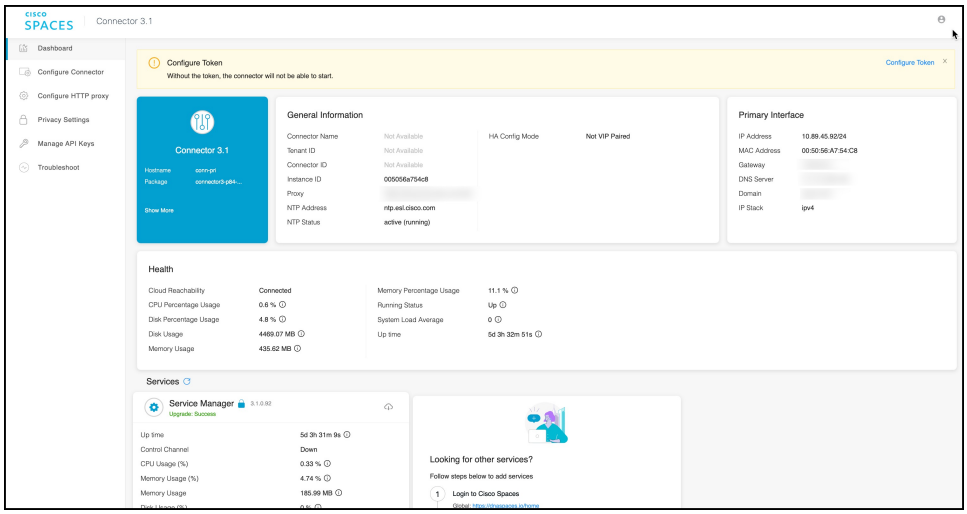
- Connector GUI, on page 89
- Configuring Privacy Settings, on page 90

Connector GUI

The connector GUI allows you to configure the following:

- Proxy
- Tokens retrieved from Cisco Spaces

Figure 117: Connector GUI



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

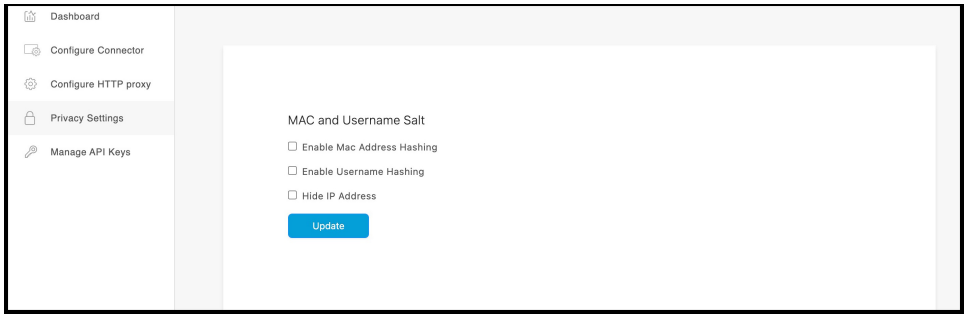
Connector provides a way to protect the Personal Identity Information (PII) of a user and maintain privacy. A hashing algorithm takes the user input (referred to as Salt) and masks the PII fields. When Cisco Spaces receives the data, the MAC addresses, IP addresses, or usernames are masked and the actual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

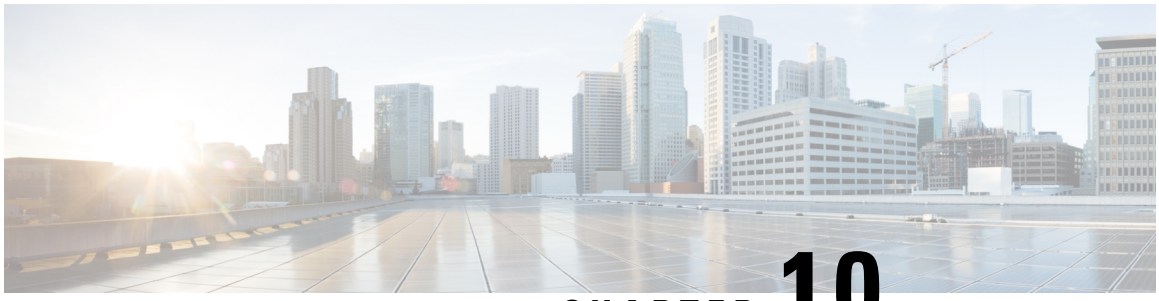
Note This task is optional.

Procedure

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

Figure 118: Configure Privacy Settings





CHAPTER 10

Proxy

- Configure a Proxy , on page 91
- Configure a Transparent Proxy , on page 93

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 119: Setup Proxy

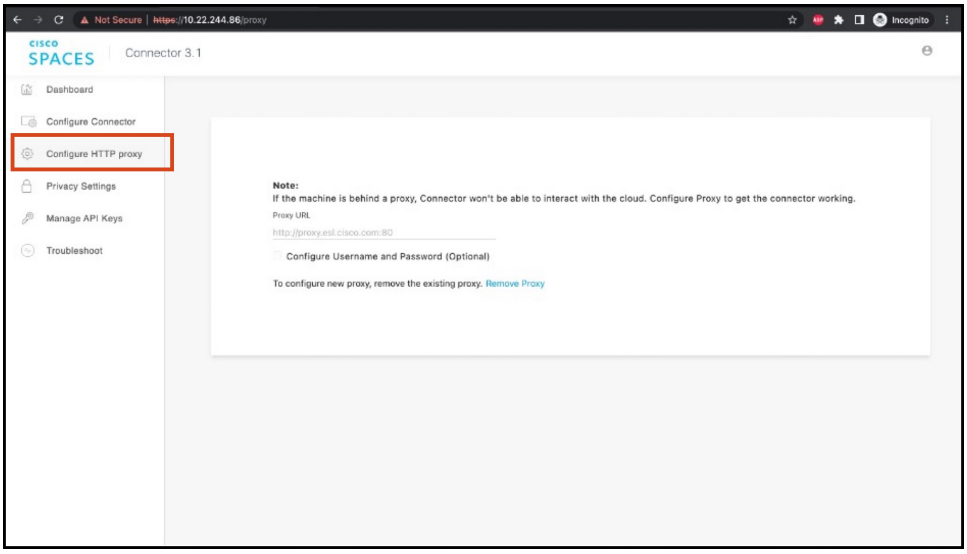
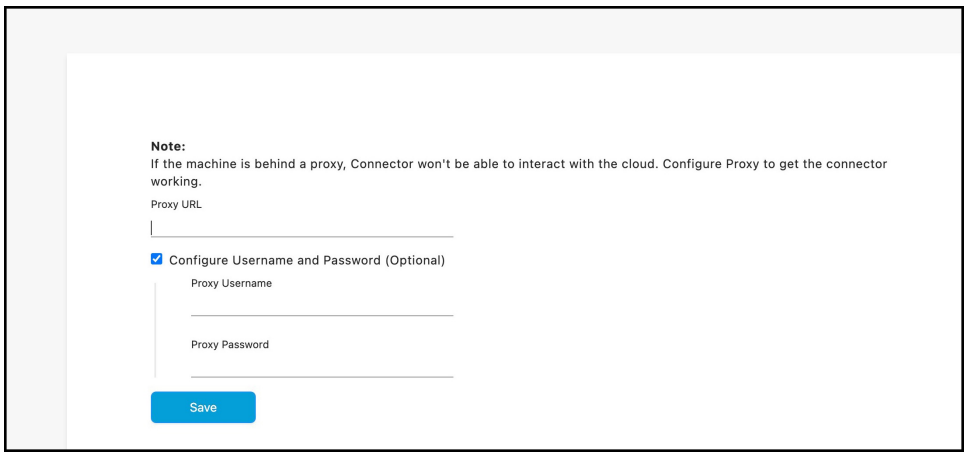


Figure 120: Configure Basic Authentication for Proxy (Optional)



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 121: Troubleshoot Proxy Issues

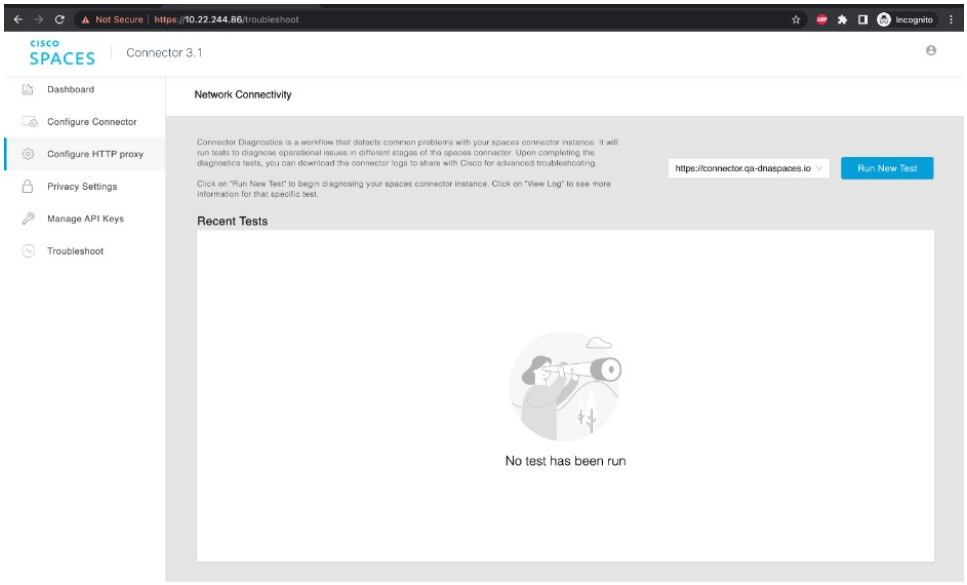
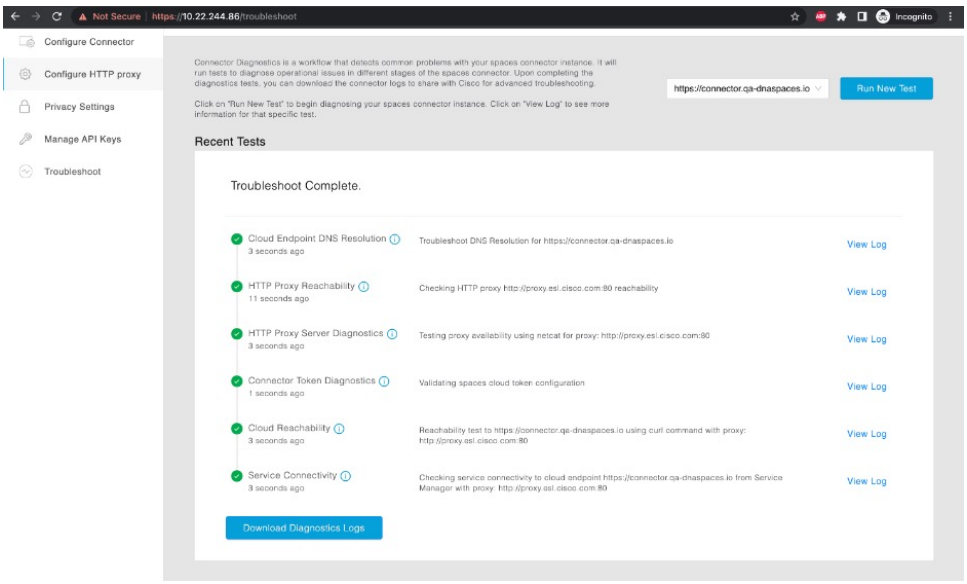


Figure 122: Sample Run Test Results



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 123: Setup Proxy

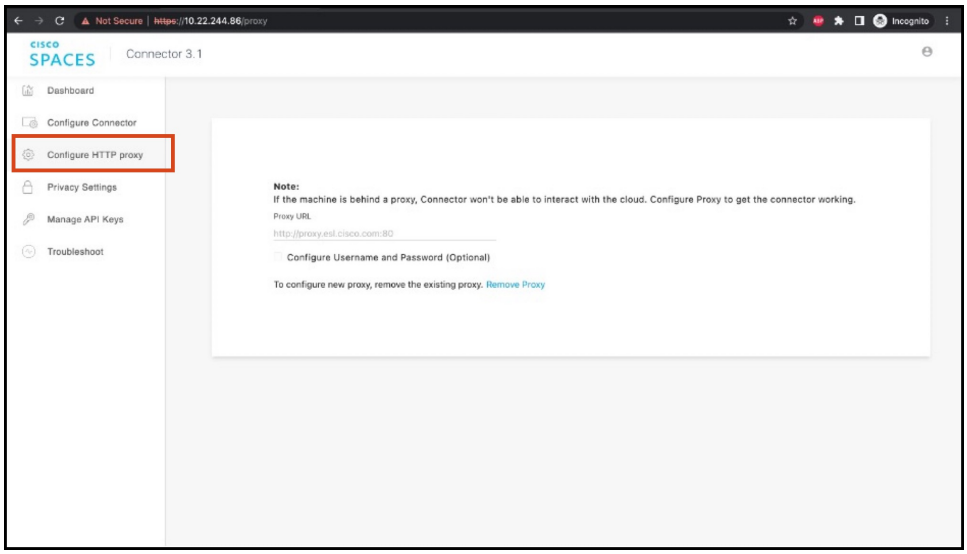
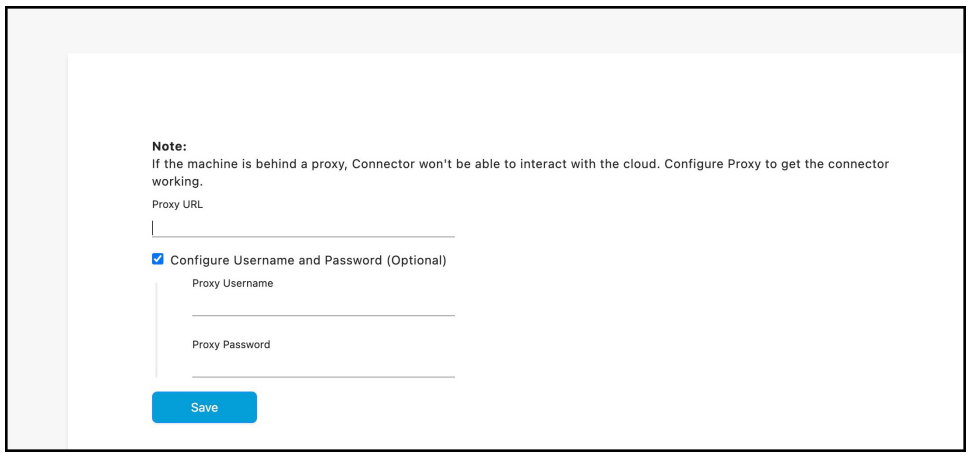


Figure 124: Configure Basic Authentication for Proxy (Optional)



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 125: Troubleshoot Proxy Issues

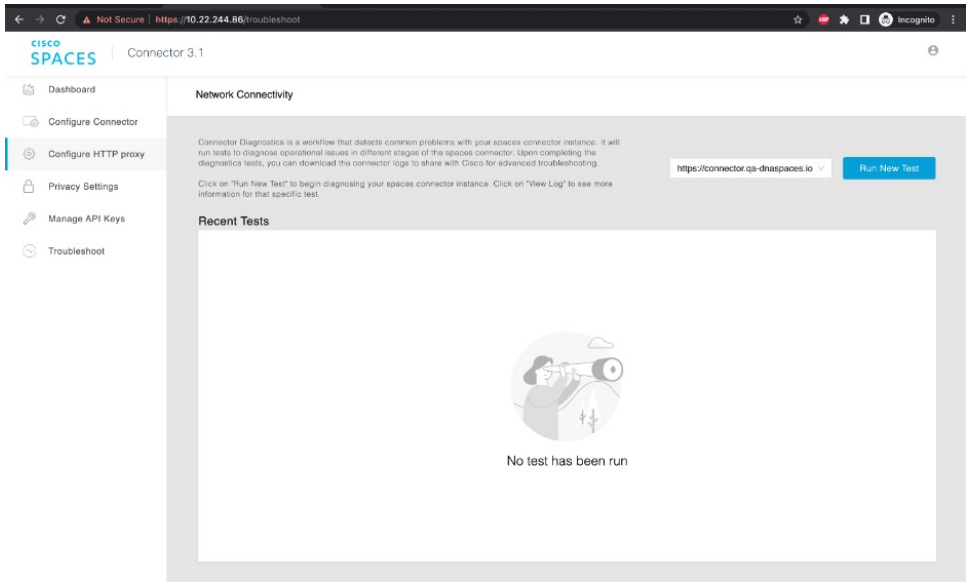
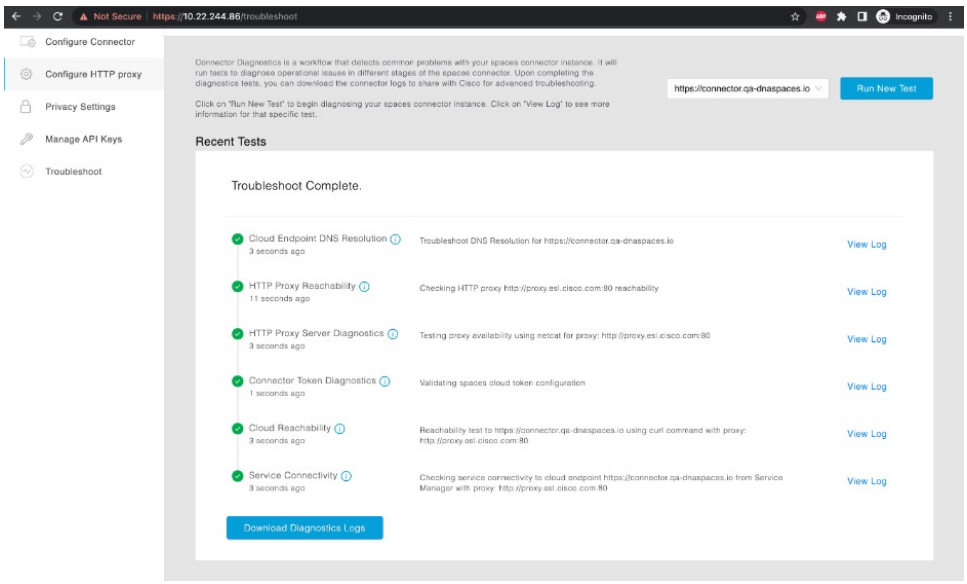
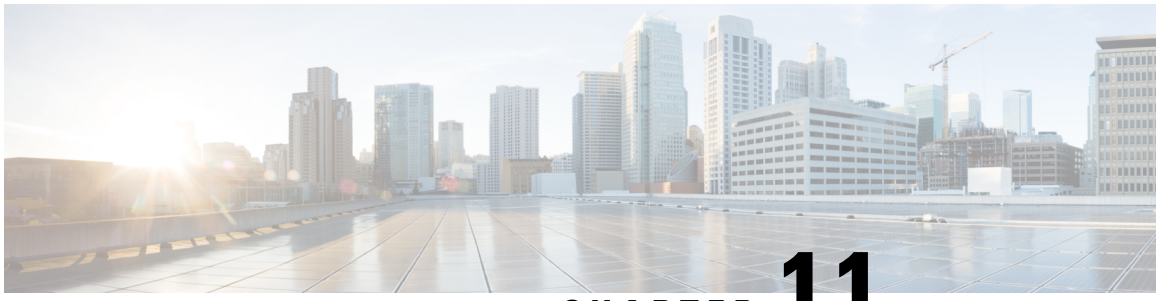


Figure 126: Sample Run Test Results





CHAPTER 11

High Availability

- Configuring Connectors as VIP Paired, on page 97
- Connector Active-Active, on page 102

Configuring Connectors as VIP Paired

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

Note 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

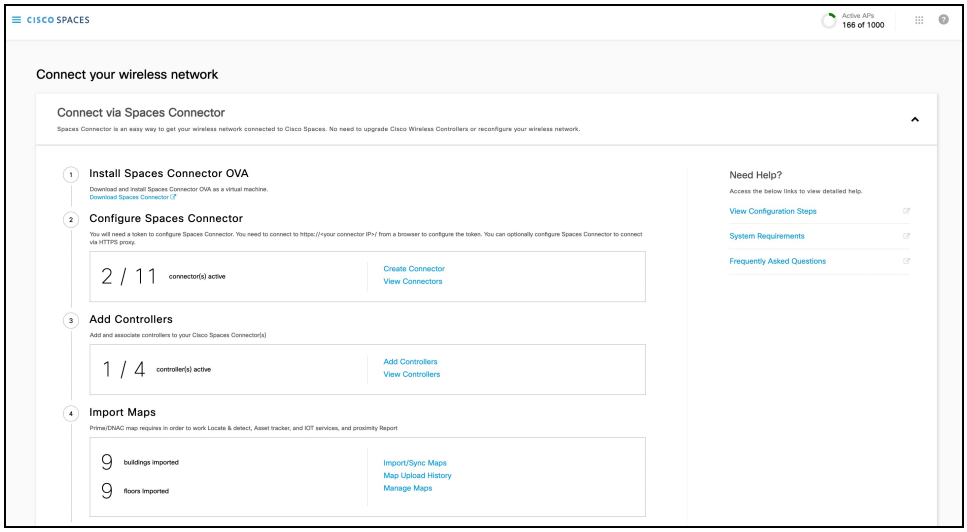
Before you begin

Install two different Cisco Spaces: Connectors. Configure each 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 127: Create Connector

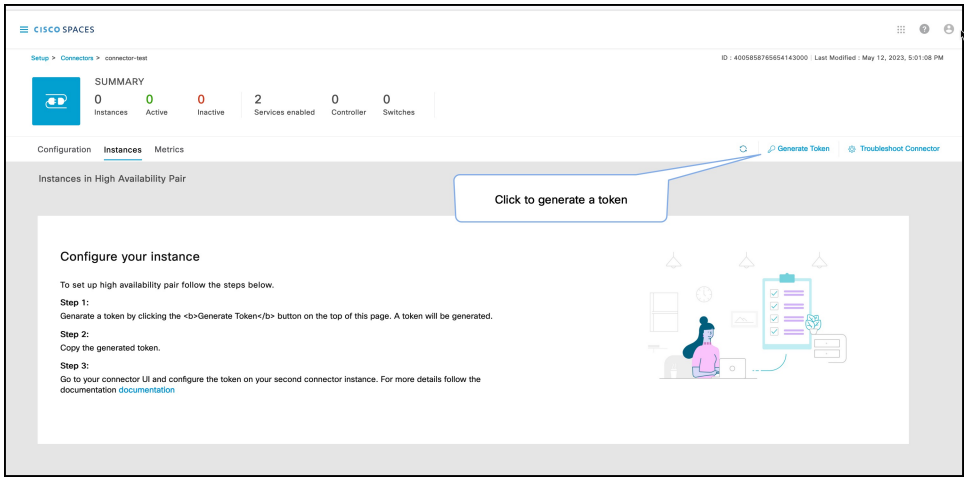


Step 2 Enter a name for the connector and choose the version.

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.

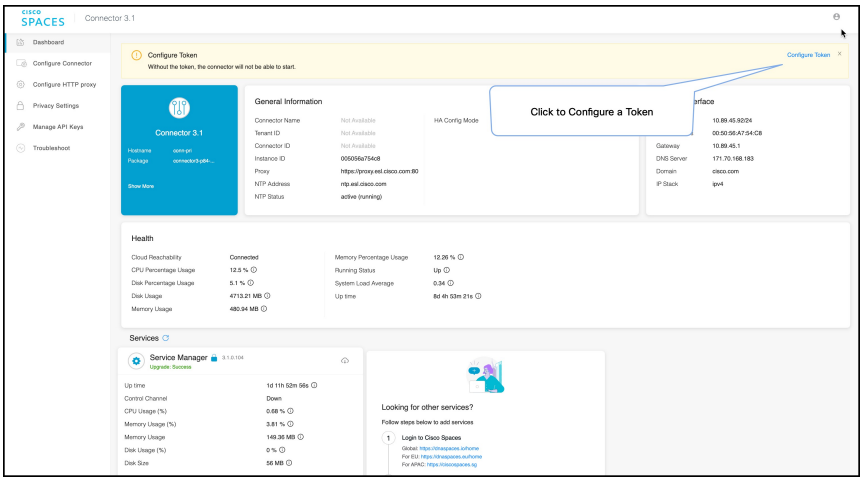
Figure 128: Generate Token



Copy the displayed token.

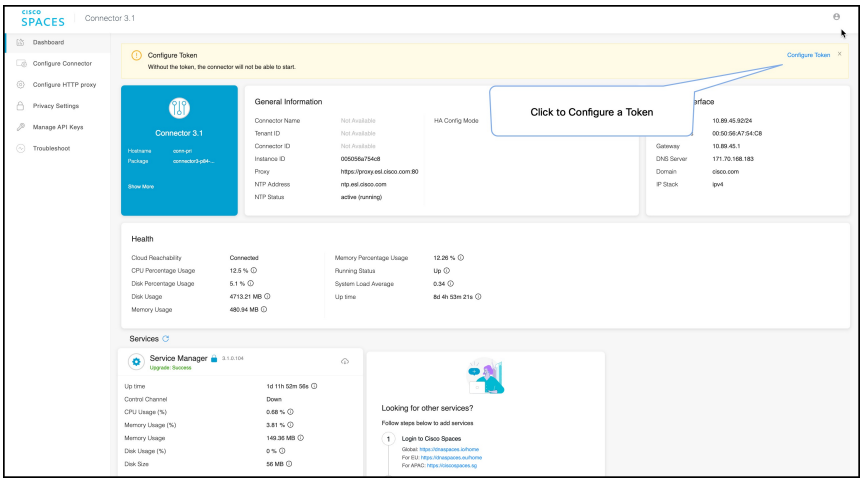
Step 4 Log in to the GUI of the first instance of connector and click **Configure Token** in the top-right corner to provision the first copied token there.

Figure 129: Configure a Token



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.

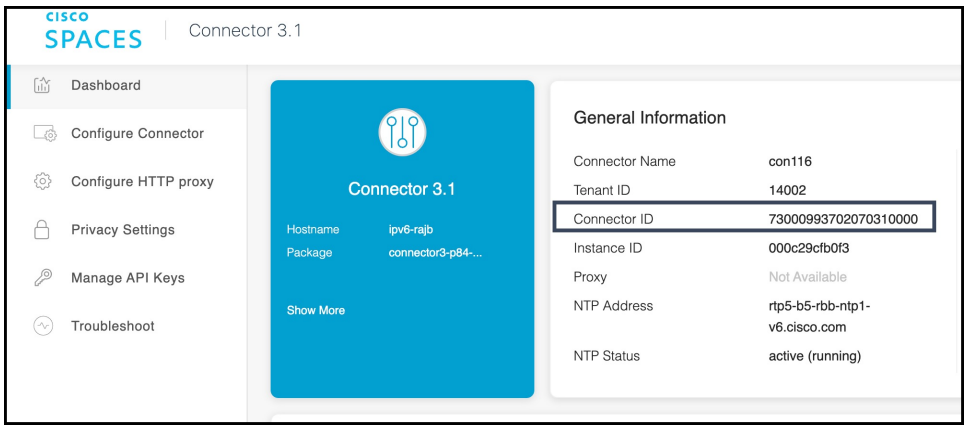
Figure 130: Configure a Token



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

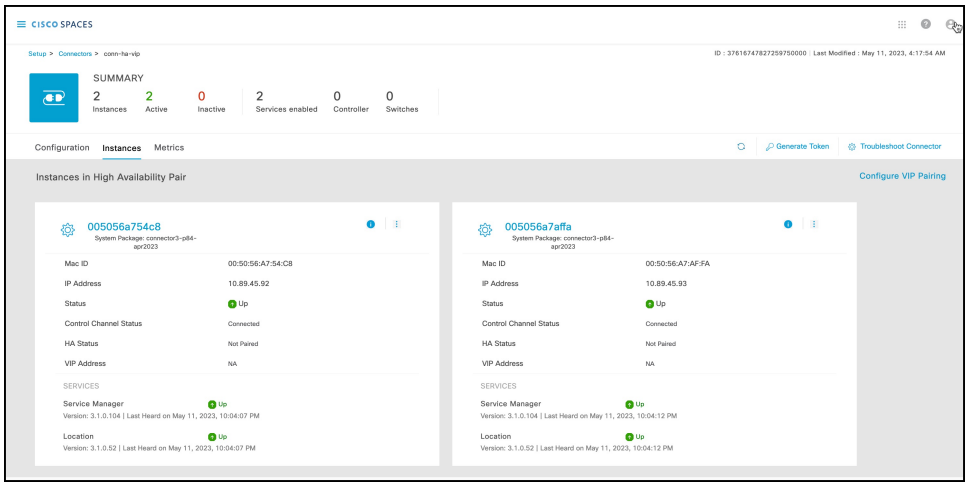
Step 6 On each instance of the connector, observe that the value of the connector ID is the same.

Figure 131: Observe connector ID



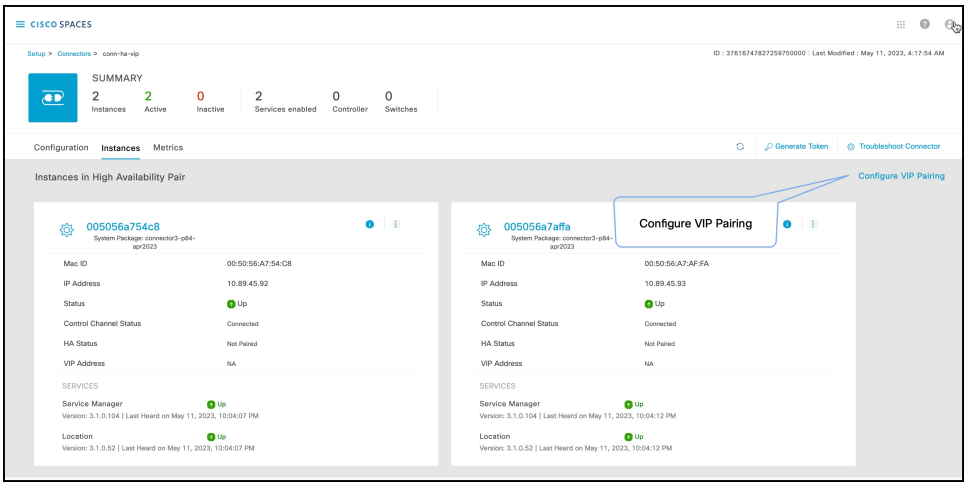
Step 7 On the Cisco Spaces dashboard, go back to the connector details page, and click the **Instances** tab. Here, you can see both the connectors that you configured. Observe that the connector IP addresses are reflected here.

Figure 132: Cisco Spaces dashboard

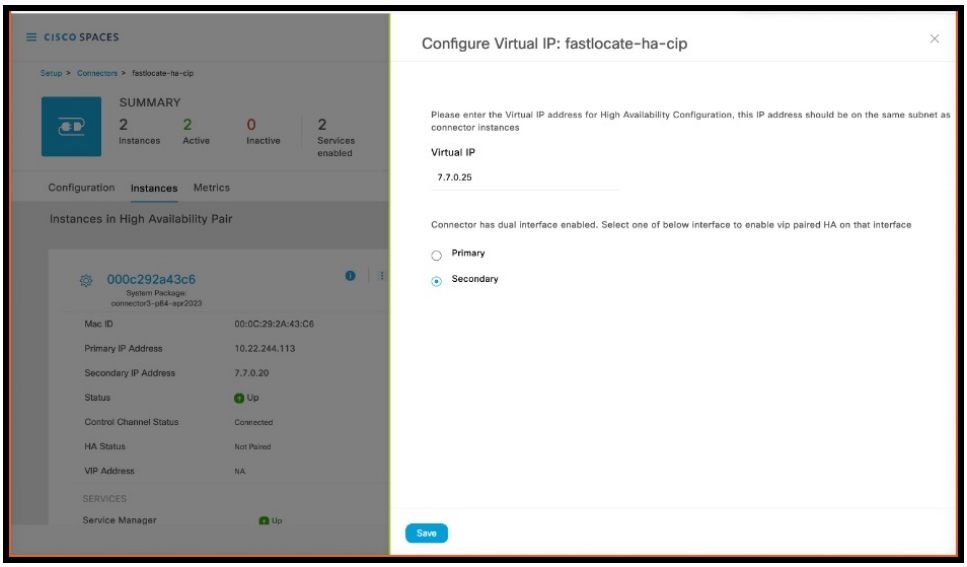


The two connectors are now configured as an active-active pair.

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



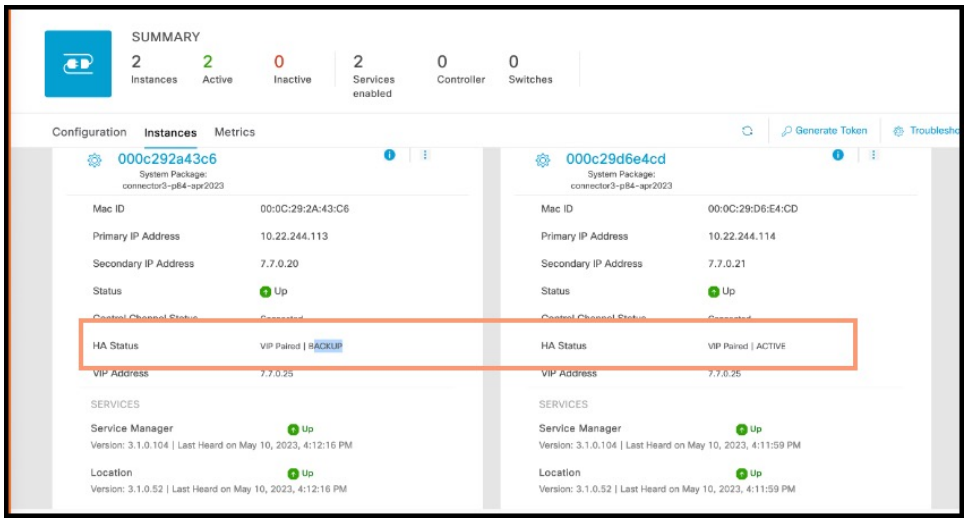
Step 9 In the **Configure Virtual IP** popup that is displayed, enter the Virtual IP address (VIP). If the connector has dual interface enabled, you have to chose which interface would be used VIP pairing.



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.



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.

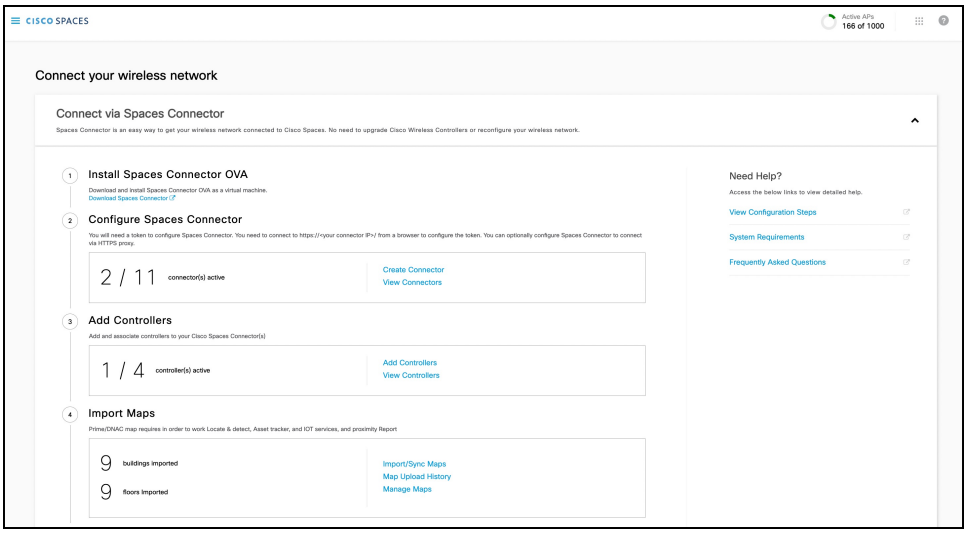
Before you begin

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 133: Create Connector

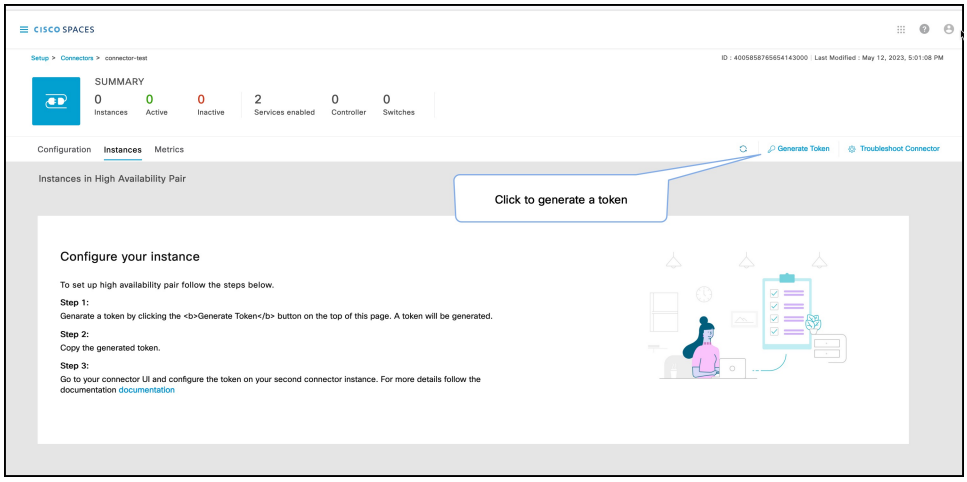


Step 2 Enter a name for the connector and choose the version.

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 134: Generate Token

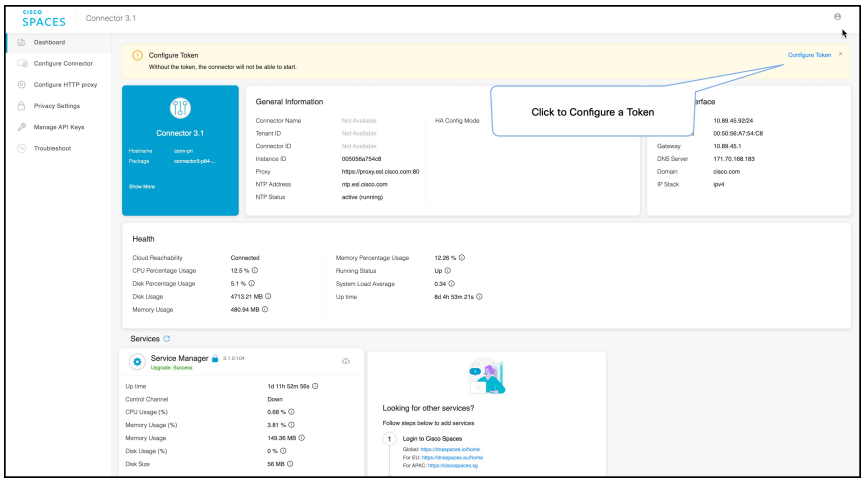


Copy the displayed token.

Step 4 Repeat Step 3 to generate and copy a second token.

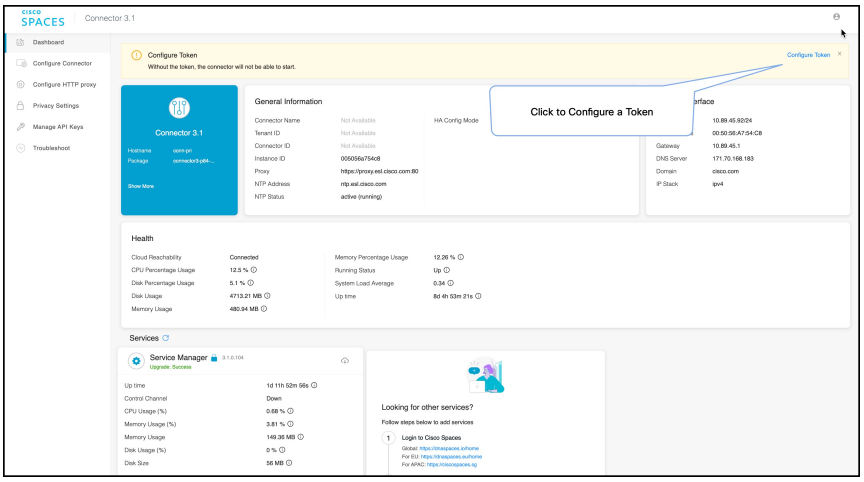
Step 5 Log in to the GUI of the first instance of connector and click **Configure Token** in the top-right corner to provision the first copied token there.

Figure 135: Configure a Token



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.

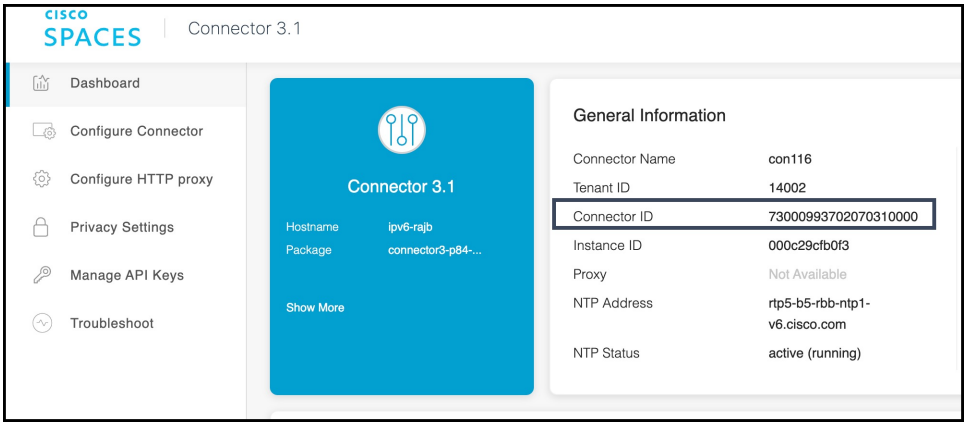
Figure 136: Configure a Token



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

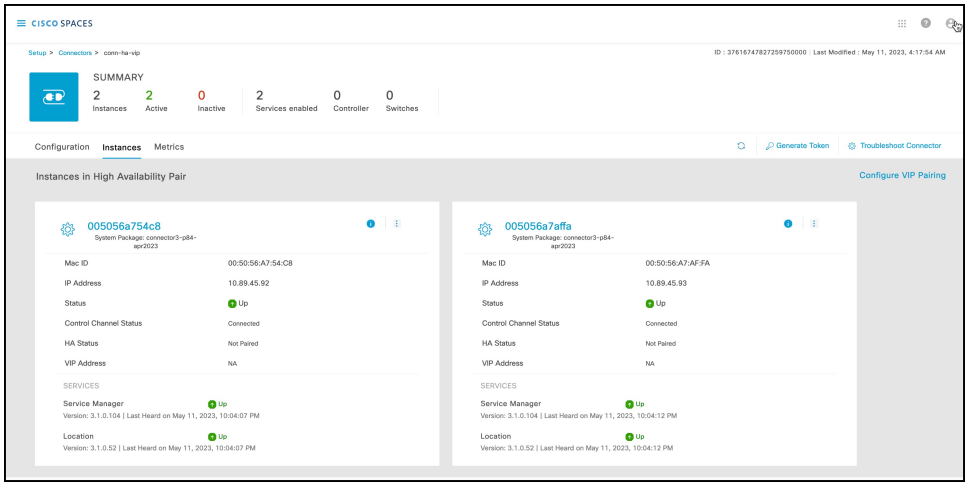
Step 7 On each instance of the connector, observe that the value of the connector ID is the same.

Figure 137: Observe connector ID



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 138: Cisco Spaces dashboard

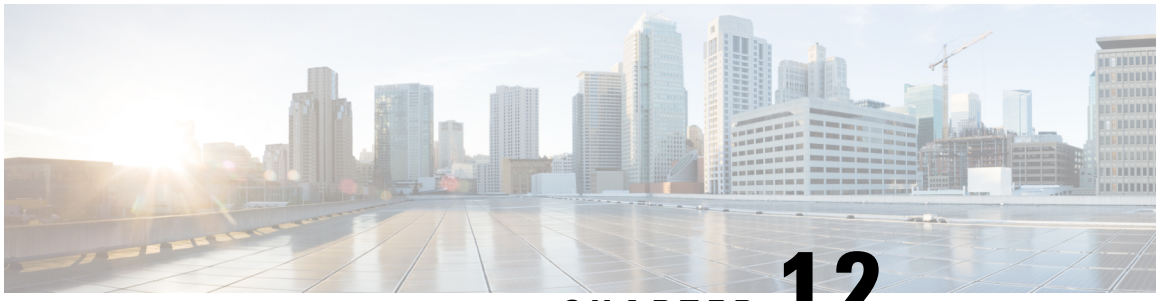


The two connectors are now configured as an active-active pair.

PART III

Troubleshooting

- Troubleshooting Tools, on page 109
- Troubleshooting Scenarios, on page 113



CHAPTER 12

Troubleshooting Tools

- Enable Debug Logs, on page 109
- Recovering a Lost Password, on page 110
- Monitor Service Metrics, on page 110

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 theStep 7.

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**.

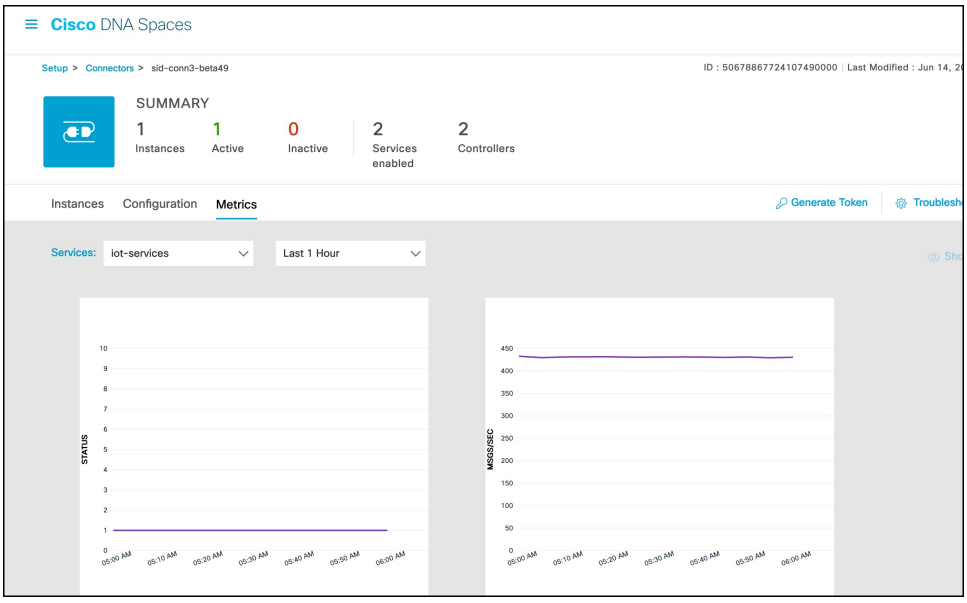
Step 2 In the **Connect via Spaces Connector** area titled **Step 2 Configure Spaces Connector**, click **View Connectors**.

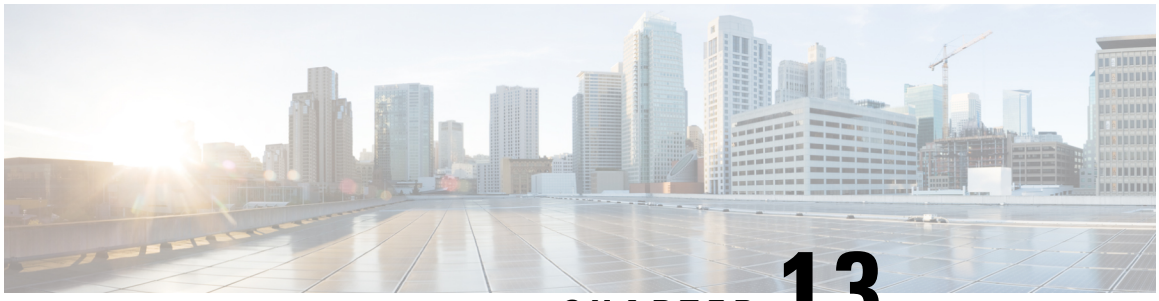
Step 3 In the **Connectors** window that opens up, click a connector of your choice.

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 139: Observing Service Metrics





CHAPTER 13

Troubleshooting Scenarios

- Connectivity Issues Between Connector and Cisco Spaces, on page 113
- Unresponsive Connector, or Failure of SSH to Connector, on page 116
- Instance is Corrupted or Deleted , on page 118
- Service Crash, or Restart Services , on page 118
- Upgrade has Failed, or How To Forcibly Push Configurations to Instances, on page 119
- Weak SSH MAC Algorithms, on page 119

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.

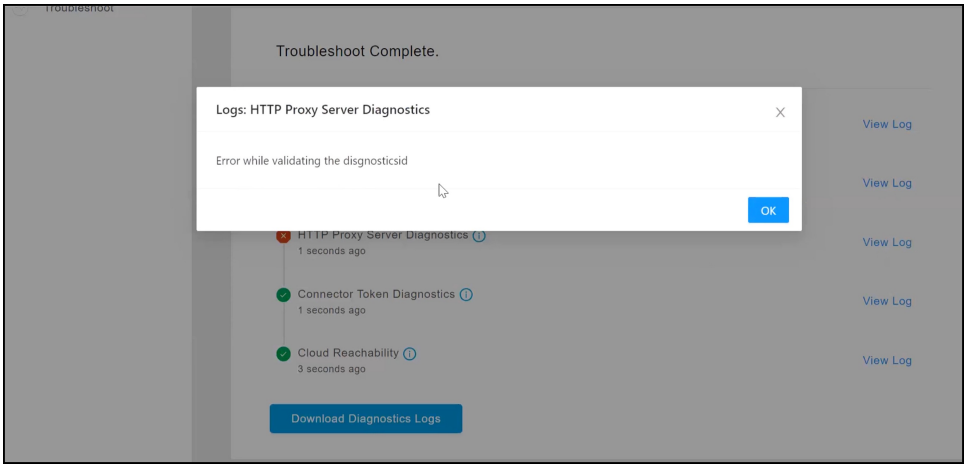
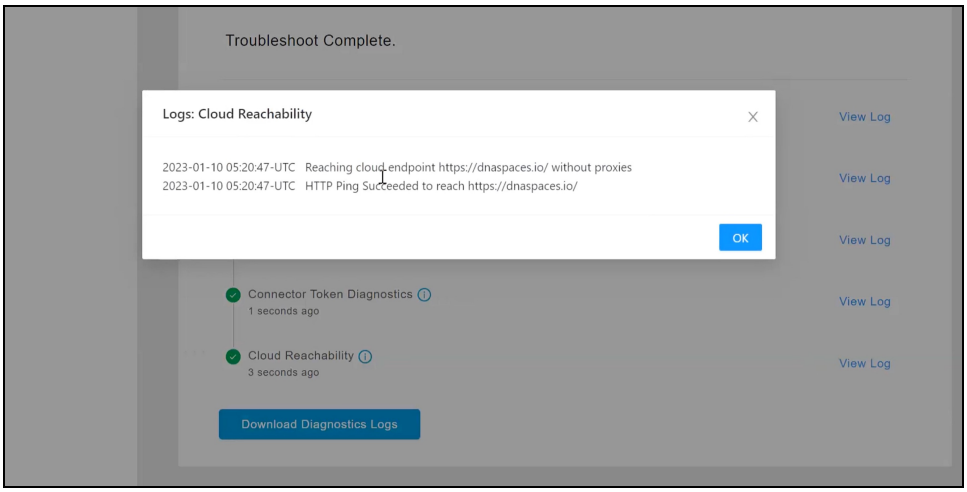
Step 2 In the connector left navigation pane, click **Troubleshoot** and do one of the following:

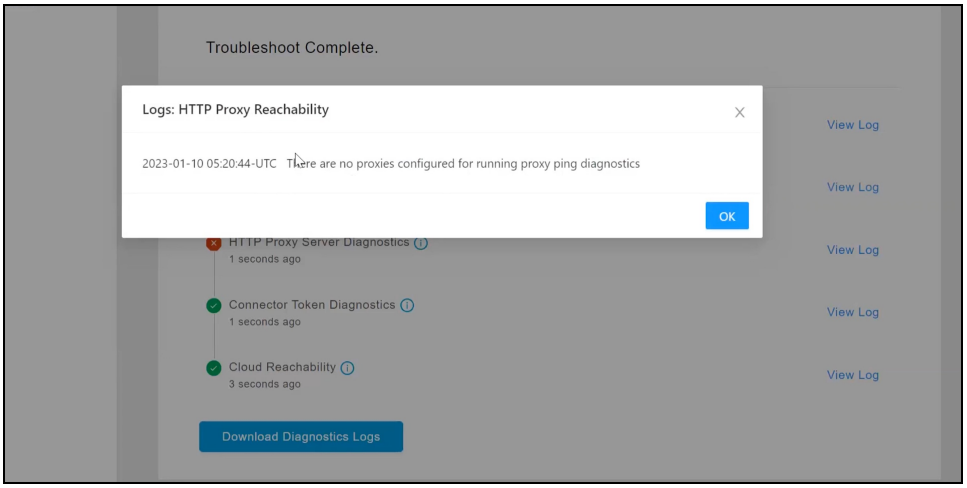
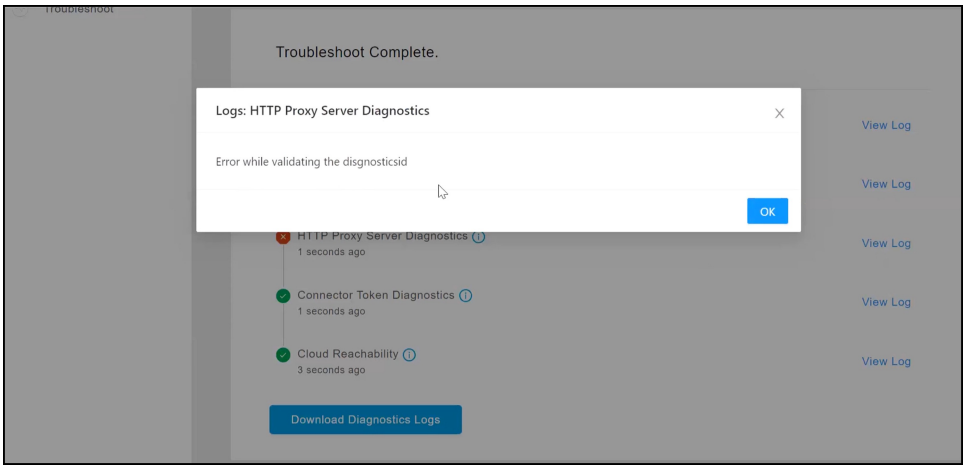
- If you have configured the token for this connector in Cisco Spaces, the text field beside the **Run New Test** button is automatically populated with the Cisco Spaces URL.
- If you have not configured the token for this connector on Cisco Spaces, then from the **Run New Test** drop-down, choose from 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.

	Click **View Logs** to view further information. ***Figure 140: View Logs*** 
	Represents a successful test. Click to view additional information about this successful test. ***Figure 141: View Logs for a Successful Test*** 

	Represents a warning. Click to view additional information about this warning. ***Figure 142: View Logs for a Warning*** 
	Represents a failure in the diagnostic test. Click **View Logs** to see additional details. ***Figure 143: View Logs for a Successful Test*** 

Step 5 Click **Download Diagnostic Logs** to download a text file with details of logs, including diagnostic information.

Figure 144: ownload Diagnostic Logs

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 145: 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.

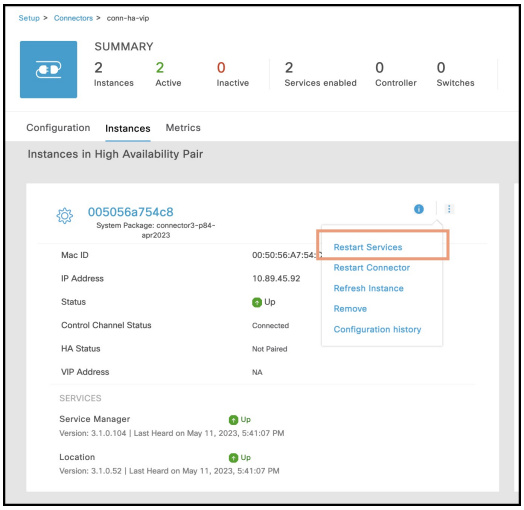
Step 2 From the left navigation pane of the Cisco Spaces dashboard, choose **Setup** > **Wireless Networks**.

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 146: Restart Services



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**.

Weak SSH MAC Algorithms

Network penetration tests often raise the issue of SSH weak MAC algorithms. These algorithms exist in the majority of SSH configurations.

An SSH MAC algorithm is used to validate data integrity and authenticity. A MAC algorithm uses a message and private key to generate a fixed length MAC.

However, some MAC algorithms are considered weak for many reasons. Here are a few reasons:

- A known weak hashing function is used (MD5)
- The digest length is too small (Less than 128 bits)
- The tag size is too small (Less than 128 bits)

Disable Weak MAC Algorithms

Procedure

Step 1 Display the list of supported SSH MAC algorithms using the **connectorctl weakmac show** command. Observe that this list includes SSH MAC algorithms that may be considered weak (weak MAC algorithms) for different reasons.

```
[spacesadmin@connector ~]$ connectorctl weakmac show
Executing command:weakmac
Command execution status:Success
-----------------------
List of supported MAC algorithms is:
macs umac-64-etm@openssh.com,
umac-128-etm@openssh.com,
hmac-sha2-256-etm@openssh.com,
hmac-sha2-512-etm@openssh.com,
hmac-sha1-etm@openssh.com,
umac-64@openssh.com,
umac-128@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 weakmac remove** command. Run the **connectorctl weakmac show** command to verify that weak MAC algorithms are removed from the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl weakmac remove
Executing command:weakmac
Command execution status:Success
-----------------------
Successfully removed weak mac configuration

[spacesadmin@connector3xinteropP83 ~]$ connectorctl weakmac show
Executing command:weakmac
Command execution status:Success
-----------------------
List of supported MAC algorithms is:
macs umac-128-etm@openssh.com,
hmac-sha2-256-etm@openssh.com,
hmac-sha2-512-etm@openssh.com,
umac-128@openssh.com,
hmac-sha2-256,
hmac-sha2-512
```

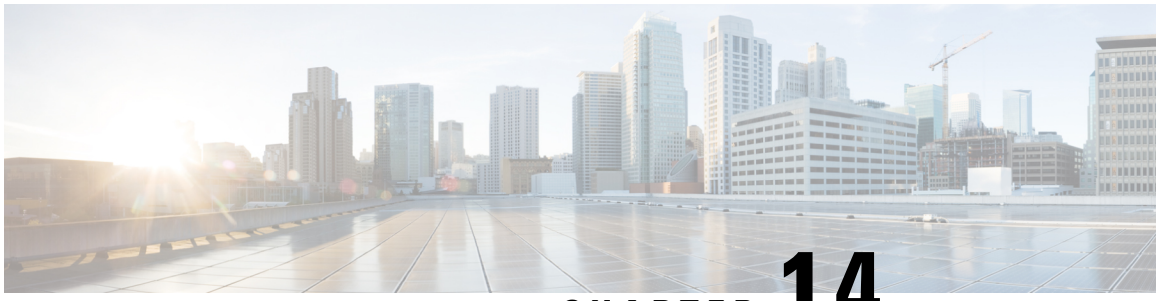
Step 3 To reinstate support for weak MAC algorithms on this device, use the **connectorctl weakmac reset** command. Run the **connectorctl weakmac show** command to verify that weak MAC algorithms are added back to the supported algorithm list.

```
[spacesadmin@connector ~]$ connectorctl weakmac reset
Executing command:weakmac
Command execution status:Success
-----------------------
Successfully reset weak mac configuration

[spacesadmin@connector3xinteropP83 ~]$ connectorctl weakmac show
Executing command:weakmac
Command execution status:Success
-----------------------
List of supported MAC algorithms is:
macs umac-64-etm@openssh.com,
umac-128-etm@openssh.com,
hmac-sha2-256-etm@openssh.com,
hmac-sha2-512-etm@openssh.com,
hmac-sha1-etm@openssh.com,
umac-64@openssh.com,
umac-128@openssh.com,
hmac-sha2-256,
hmac-sha2-512,
hmac-sha1
```

PART IV

Services

- Location Service, on page 125
- IoT Service (Wireless) , on page 131
- IoT Service (Wired) , on page 143
- Hotspot Service, on page 163
- Local Firehose, on page 167



CHAPTER 14

Location Service

- Compatibility Matrix for Cisco Spaces: Connector: Location service, on page 125
- Open Ports for Location Service, on page 129

Compatibility Matrix for Cisco Spaces: Connector: Location service

Table 4: Location Service

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco AireOS Wireless Controller	• 8.9 • 8.10 **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.

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco Catalyst 9800 Series Wireless Controllers	• 16.12.4a • 16.12.5 • 17.3.x • 17.4.1 • 17.5.1 • 17.6.x • 17.7.1 • 17.8.1 • 17.9.x • 17.10.1 • 17.11.1 • 17.12.x • 17.13.1 • 17.14.1 • 17.15.1 **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.

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)	Supported versions are: • 16.12.5 • 17.3.1 • 17.3.2a, • 17.3.3 • 17.3.4 • 17.4.1 • 17.5.1 • 17.6.1 **Note** Use the latest software version or maintenance release for each listed release. 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
Cisco Spaces: IoT Service	• Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.3.1 and later • Not supported on Cisco AireOS Wireless Controller • Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)
Supported wireless controllers for Cisco FastLocate	• Supported on Cisco AireOS Wireless Controller, Release 8.1.123.0 • Supported on all releases of Cisco Catalyst 9800 Series Wireless Controllers

Hardware or Application Name	Support for Cisco Spaces: Connector
Supported wireless controllers for Cisco Hyperlocation	• Supported on Cisco AireOS Wireless Controller • Supported on Cisco Catalyst 9800 Series Wireless Controllers
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

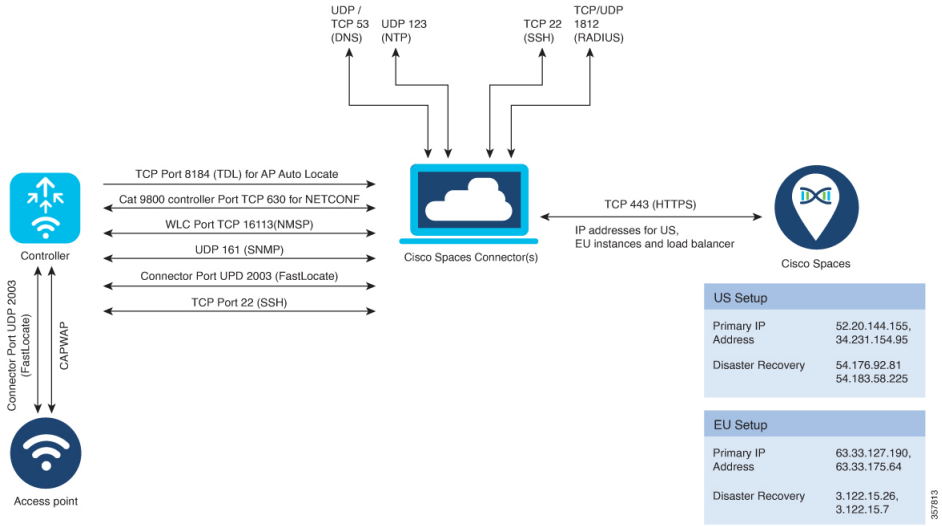
Tested Access Points for Cisco FastLocate	• Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points
Tested Access Points for Cisco FastLocate (Wi-Fi 6)	• Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points • Cisco Catalyst 9164 Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Catalyst IW9165D Heavy Duty Access Points • Cisco Catalyst IW9165E Rugged Access Points • Cisco Catalyst IW9167 (E/I) Heavy Duty Access Points

Hardware or Application Name	Support for Cisco Spaces: Connector
Tested Access Points for Cisco Hyperlocation	• Cisco Aironet 3700 Series Access Points (Requires hyperlocation antenna) • Cisco Aironet 4800 Series Access Point
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

Open Ports for Location Service

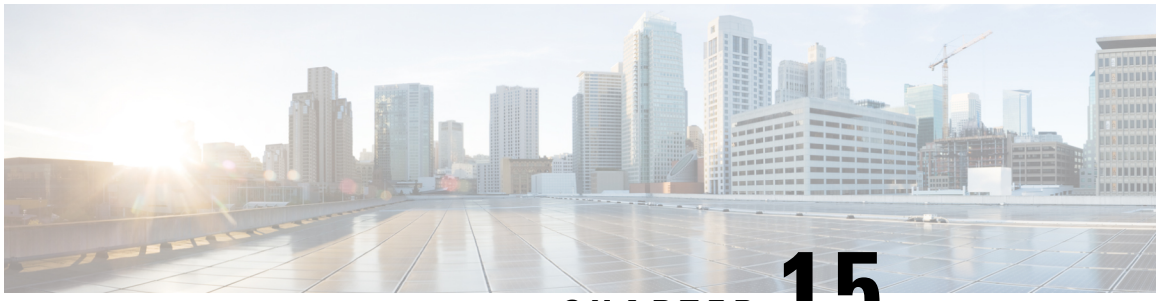
This section lists the connector ports that must be open for the proper functioning of location service.

Figure 147: Open Ports for Location Service



	Primary IP Address	Disaster Recovery
US Setup	• 52.20.144.155 • 34.231.154.95	• 54.176.92.81 • 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	• 13.214.251.223 • 54.255.57.46

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 15

IoT Service (Wireless)

• Overview of Cisco Spaces: IoT Service (Wireless), on page 131

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:

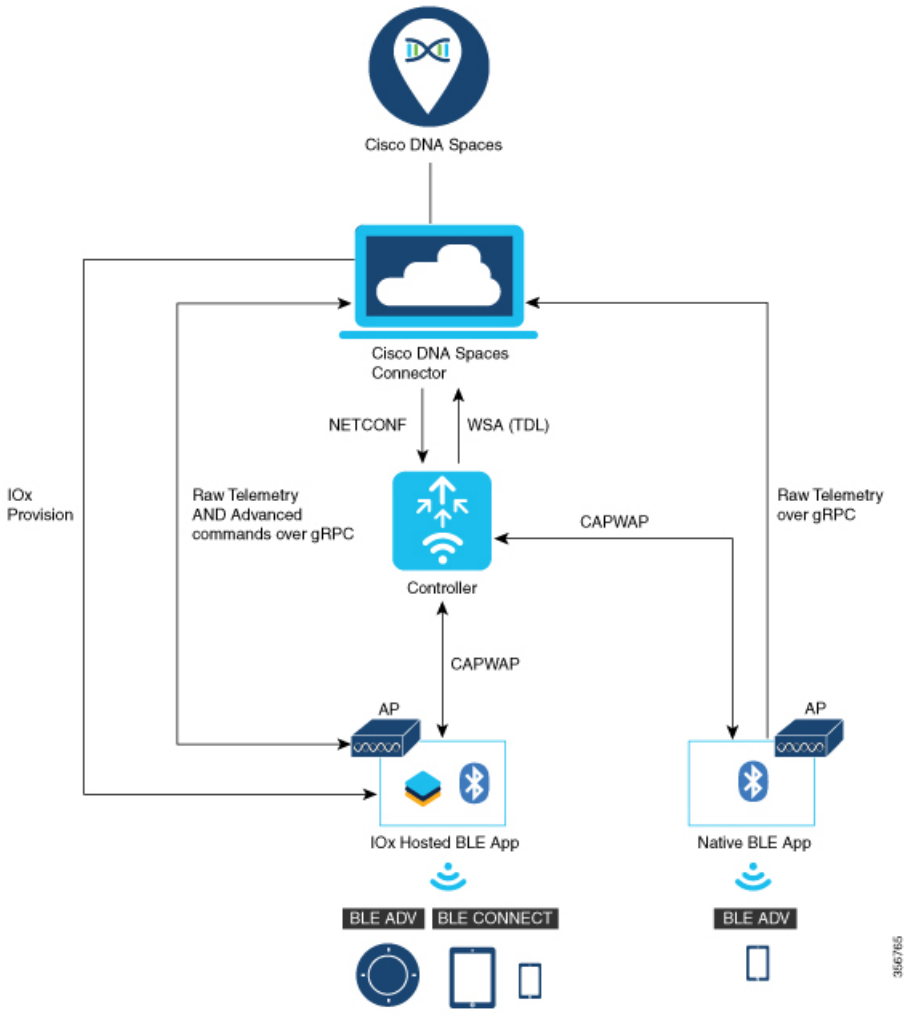
- Deploy BLE gateways on supported APs in your network.
- Claim the BLE beacons that you acquired from Cisco Spaces: IoT Device Marketplace.
- Configure APs and manage floor beacons.
- Monitor device attributes such as location, telemetry, battery status, and movement status.

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 148: 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 the type of Cisco APs, you can configure an AP as one of the following types of BLE gateways:

- **Base BLE Gateway**: This is a type of AP that you can configure in either the **Transmit** mode or the **Scan** mode.

  In the **Transmit** mode, the AP can broadcast iBeacon, Eddystone URL, and Eddystone UID profiles.

  In the **Scan** mode, the AP can scan the vicinity for other BLE devices. Using gRPC, an AP sends the scanned data to Cisco Spaces: Connector. The AP can also receive telemetry data from floor beacons. The Cisco Spaces: Connector dashboard decodes and displays this information.

- **Advanced BLE Gateway:** This gateway is an AP that is installed with the Cisco IOx App. Using the installed Cisco IOx App, you can configure floor beacons on the Cisco Spaces dashboard. You can also upgrade the floor beacon firmware from the Cisco Spaces dashboard.

You can configure this AP in the **Scan** mode and the **Transmit** mode.

In the **Transmit** mode, the AP can broadcast iBeacon, Eddystone URL, and Eddystone UID profiles.

In the **Scan** mode, the AP can scan the vicinity for other BLE devices. Using gRPC, an AP sends the scanned data to Cisco Spaces: Connector. The AP can also receive telemetry data from floor beacons. The Cisco Spaces: Connector dashboard decodes and displays this information.

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 17.3.1 and later • 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	2.3 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

Application Name	Support for Cisco Spaces: IoT Service
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
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

IoT Service is not supported on the following:

- Directly connected and CMX Tethering connectors.

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 5: AP Modes and App Support

AP Mode	Advanced BLE Gateway App	Base BLE Gateway App
PI: Local	• 11-AX: Supported • Wave2: Not supported	• 11-AX: Supported • Wave2: Supported

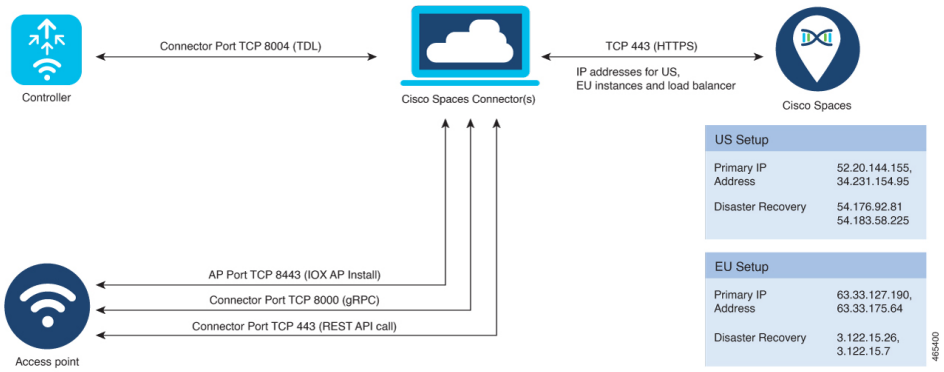
AP Mode	Advanced BLE Gateway App	Base BLE Gateway App
P1: Flex	• 11-AX: Supported • Wave2: Not supported	• 11-AX: Supported • Wave2: Supported
P2: Fabric	• 11-AX: Supported • Wave2: Not supported	• 11-AX: Supported • Wave2: Supported
P3: Mesh	• 11-AX: Supported • Wave2: Not supported	• 11-AX: Supported • Wave2: 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 149: Open Ports for IoT service (wireless)



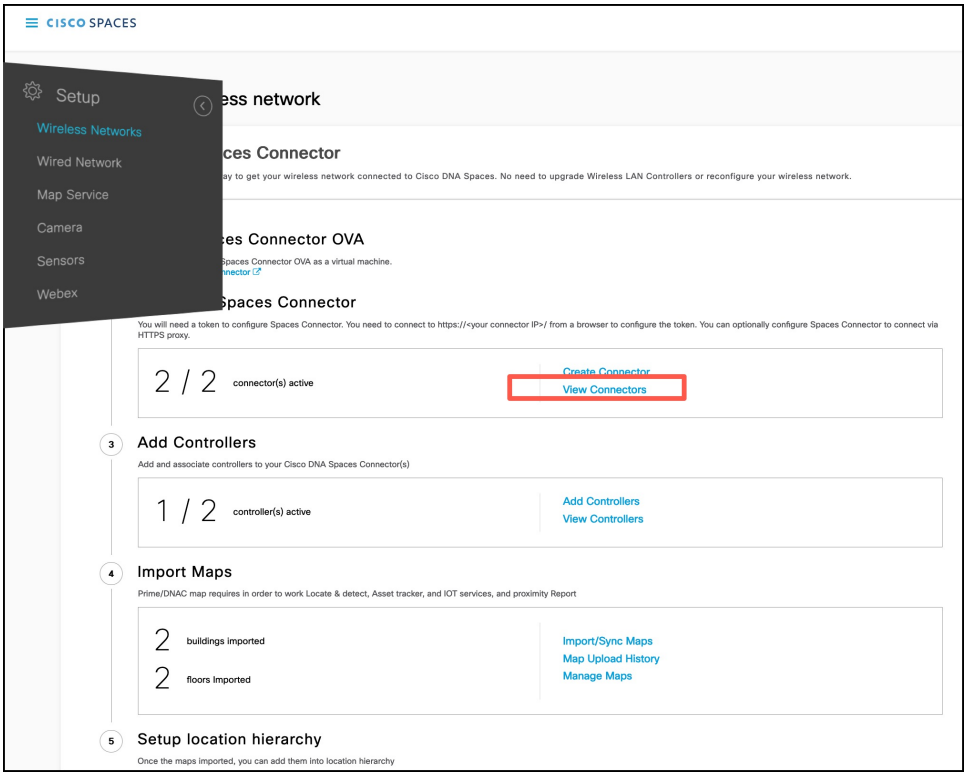
Configure IoT Service (Wireless)

Procedure

Step 1 In the Cisco Spaces dashboard left navigation pane, click **Setup** and choose **Wireless Networks**.

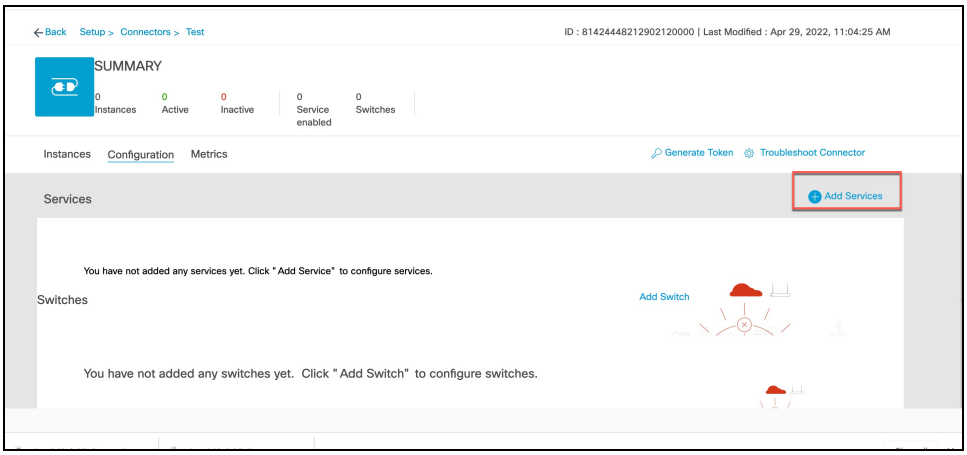
Step 2 In the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 150: View Connectors



Step 3 In the connector details window that is displayed, click **Add Services**.

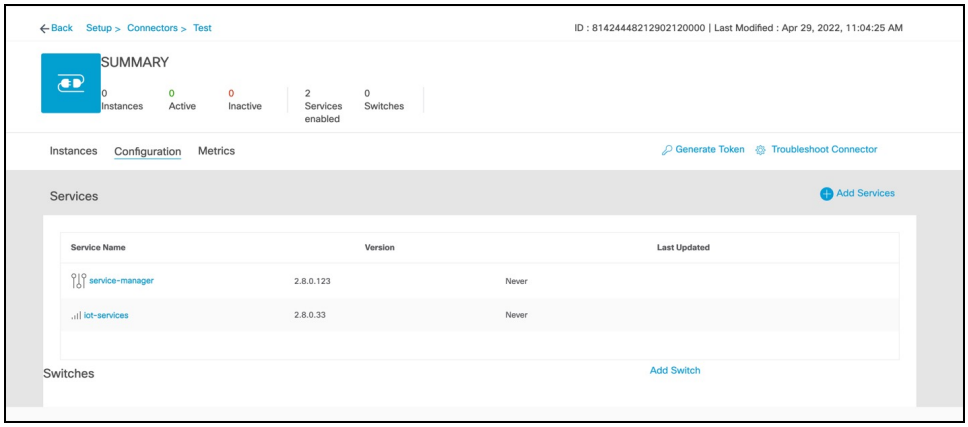
Figure 151: Add Services



Step 4 In the **Add Services** window that is displayed, choose **IoT Wireless** and click **Add**.

Note **service-manager** is chosen by default.

Figure 152: Connector Details



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

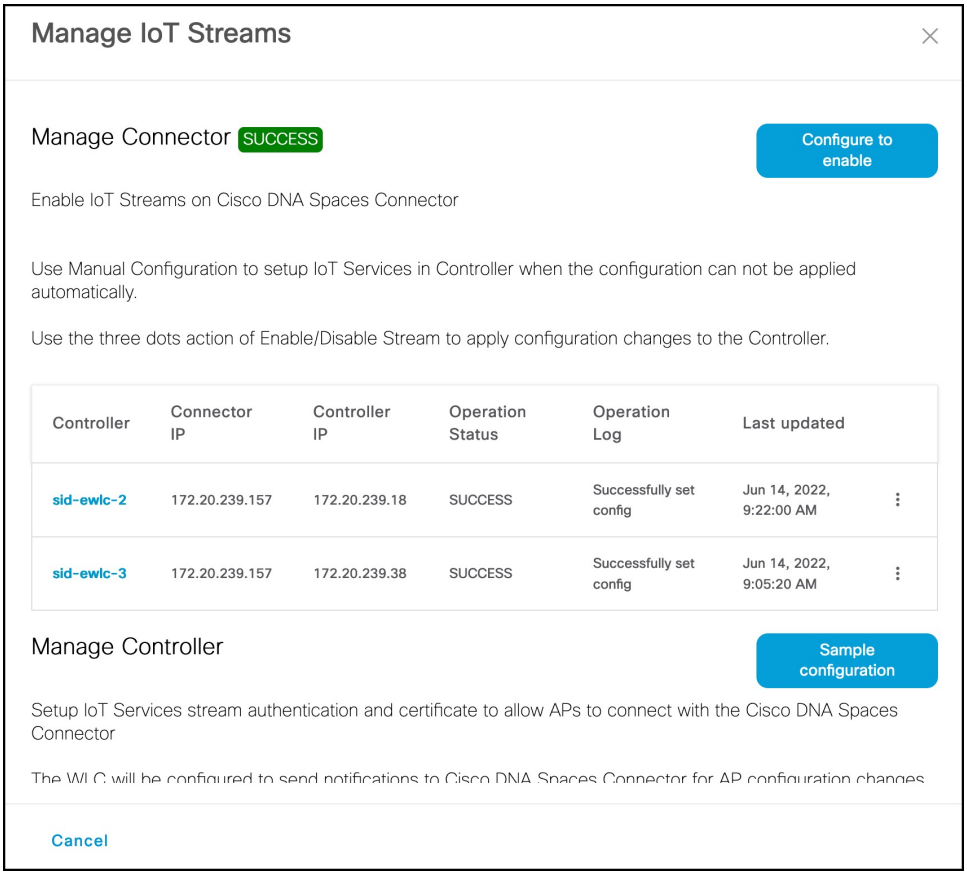
Step 1 In the Cisco Spaces dashboard left navigation pane, choose **Setup** > **Wireless Network**.

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 153: Troubleshooting IoT Streams



Verify Access Points

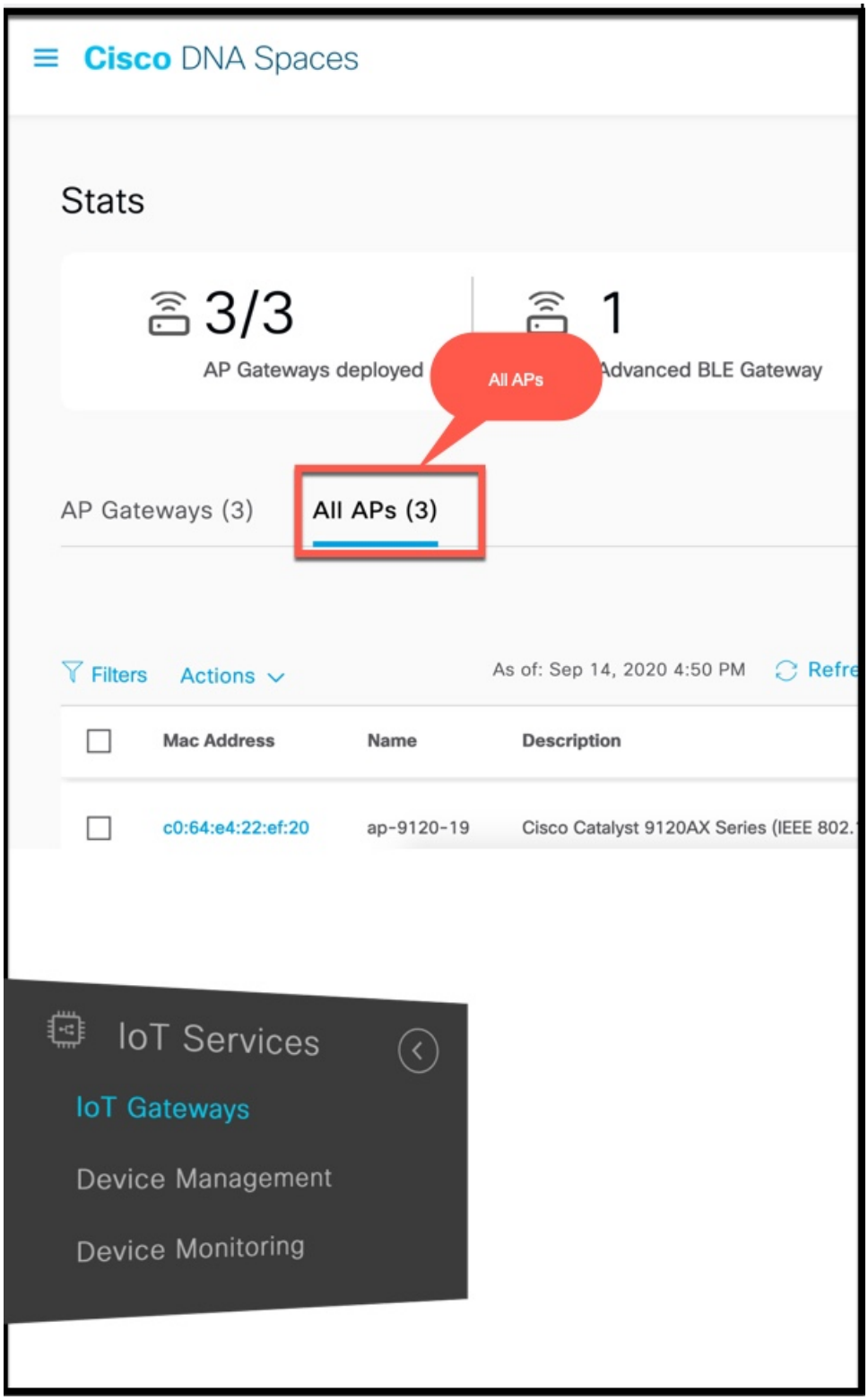
This procedure helps you verify if IoT service (wireless) has synchronized and listed the APs in your network on the GUI

Procedure

Step 1 In the Cisco Spaces dashboard left-navigation pane, choose **IoT Services > IoT Gateways > AP Gateway**.

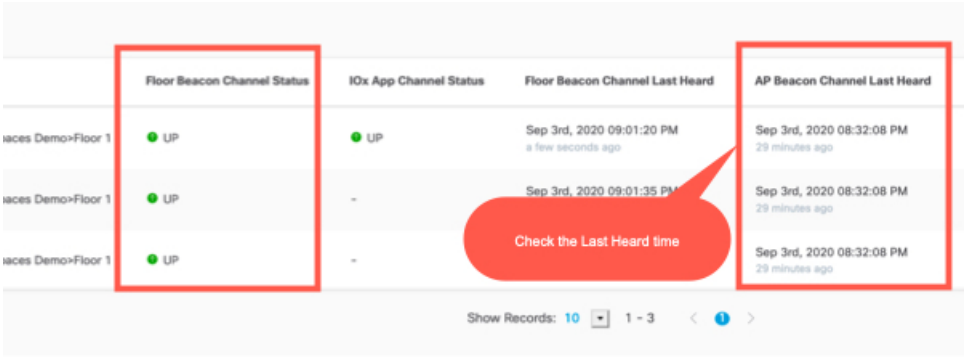
Step 2 Click the **All APs** tab.

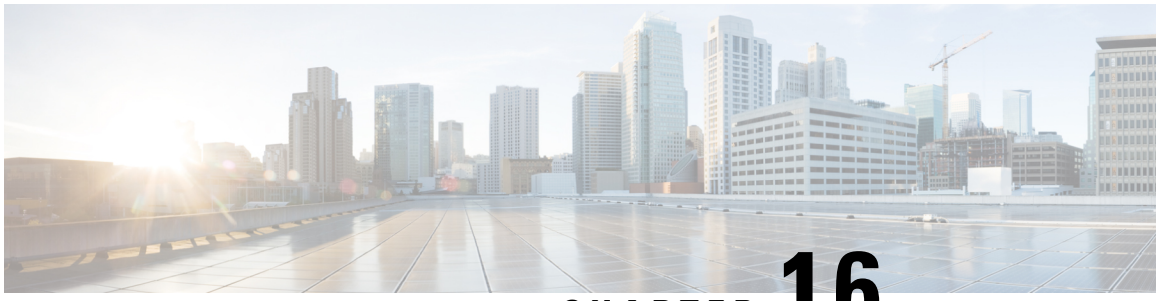
Figure 154: Verify APs



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 155: Verify APs





CHAPTER 16

IoT Service (Wired)

- Overview, on page 143

Overview

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

Overview of IoT Service (Wired)

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

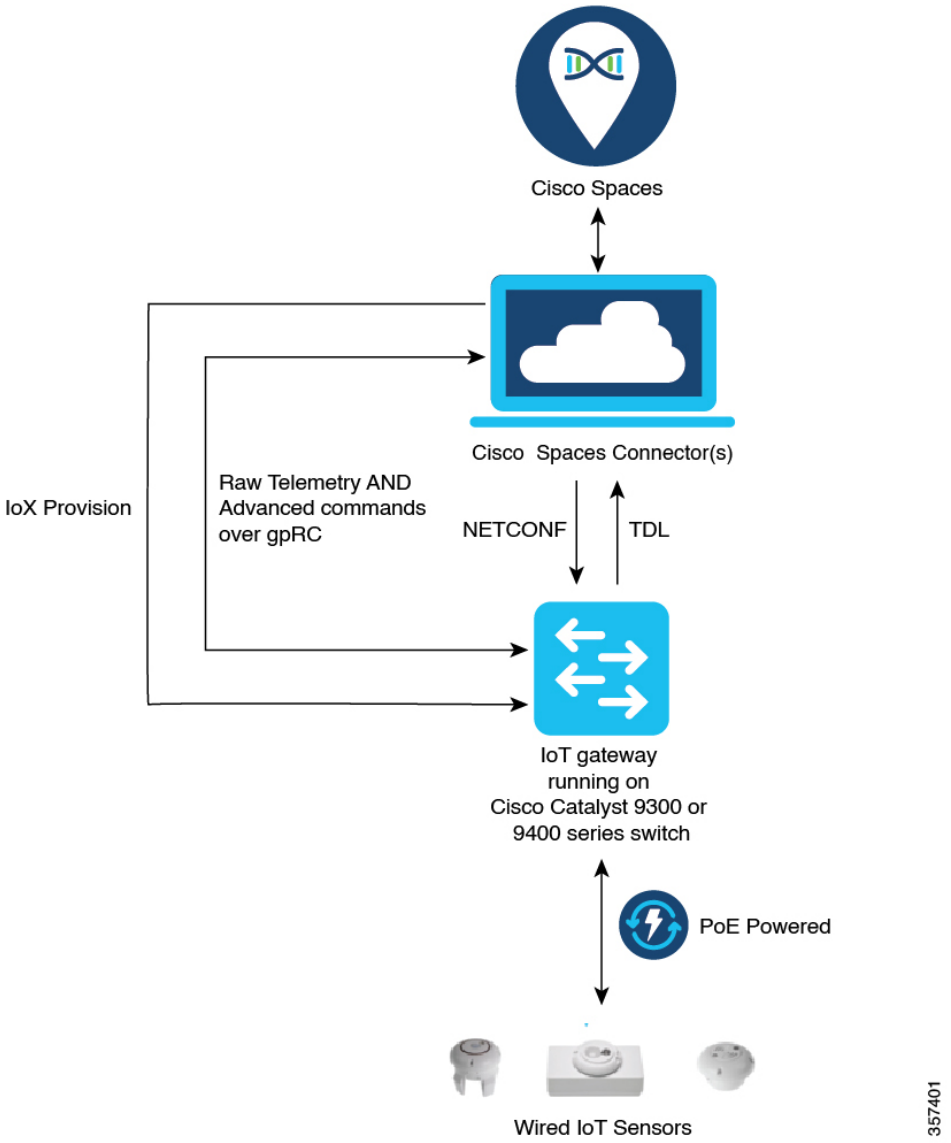
Integrating IoT service (wired) with the Cisco Catalyst 9300 and 9400 Series Switches series platform requires the following:

- 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 156: Data flow in IoT Service (Wired)



Compatibility Matrix for IoT Service (Wired)

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

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

- Connecting directly with controller
- CMX Tethering

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 145 .
- 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.

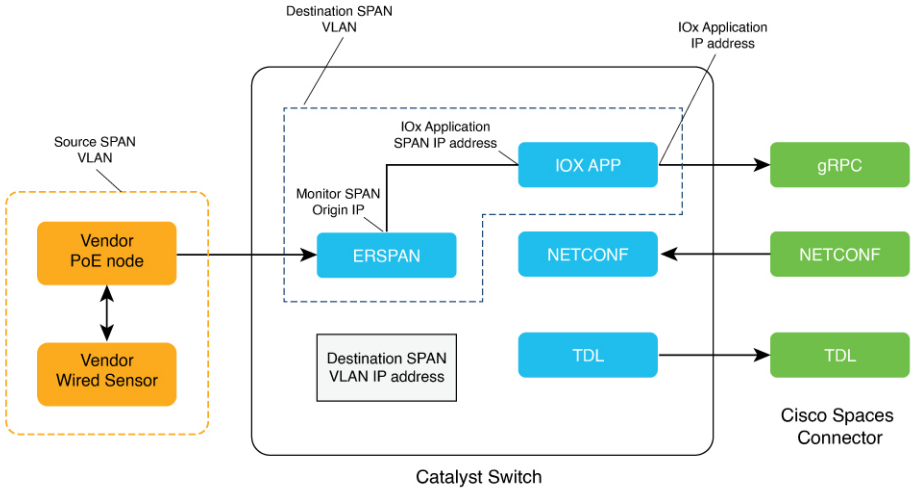
- Enable NETCONF on Cisco Catalyst 9300 or 9400 Series Switches on port 830, along with permission to use NETCONF.

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 157: Design Prerequisites

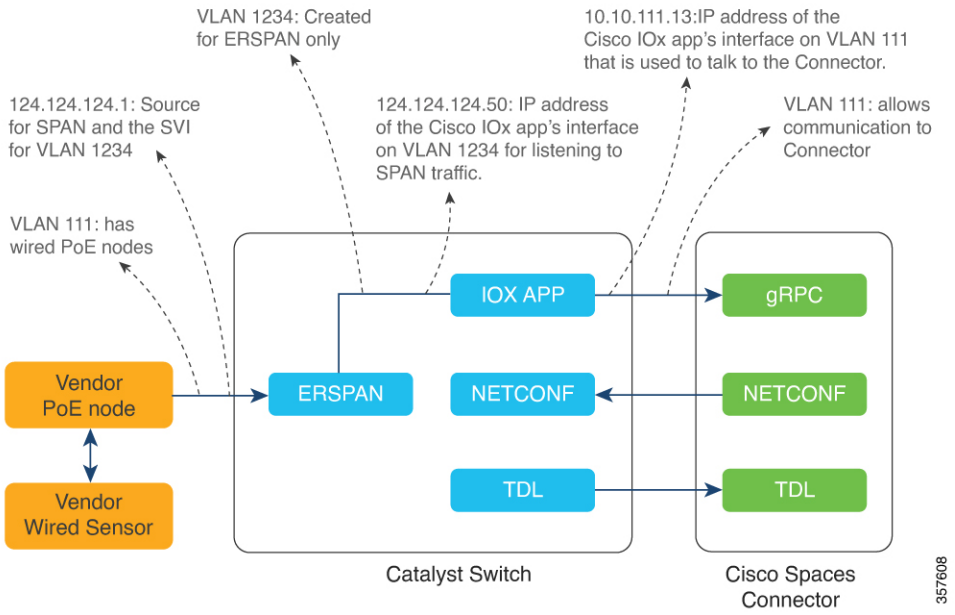


- **Destination SPAN VLAN**: The VLAN used to send Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic from Power over Ethernet (PoE) nodes to Cisco IOx App. You can use an existing VLAN or create a new one. This VLAN can also be local to the switch.
- **Destination SPAN VLAN IP address**: This 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 158: Sample Configuration



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 145 .

- 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**

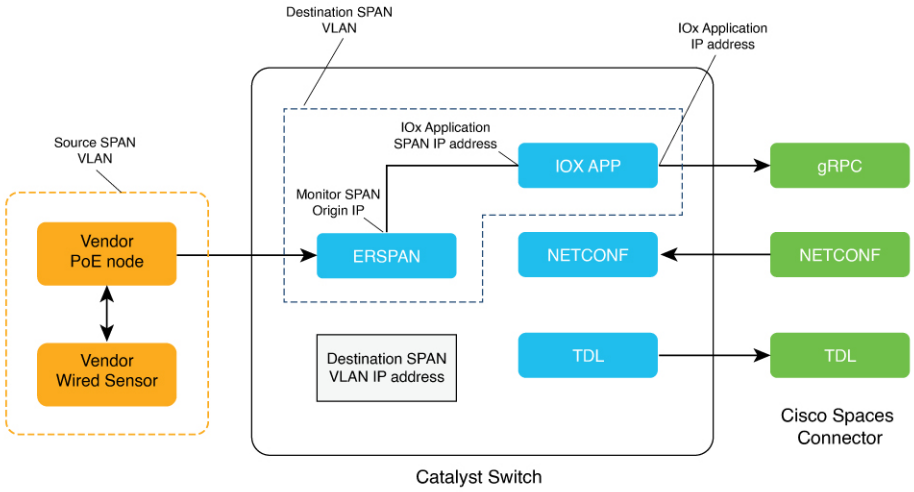
  For more information, see **Command Reference, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9300 Switches)**
- Perform NTP synchronization across wireless controllers, Cisco Spaces: Connectors, and switches in the network.
- Enable NETCONF on Cisco Catalyst 9300 or 9400 Series Switches on port 830, along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

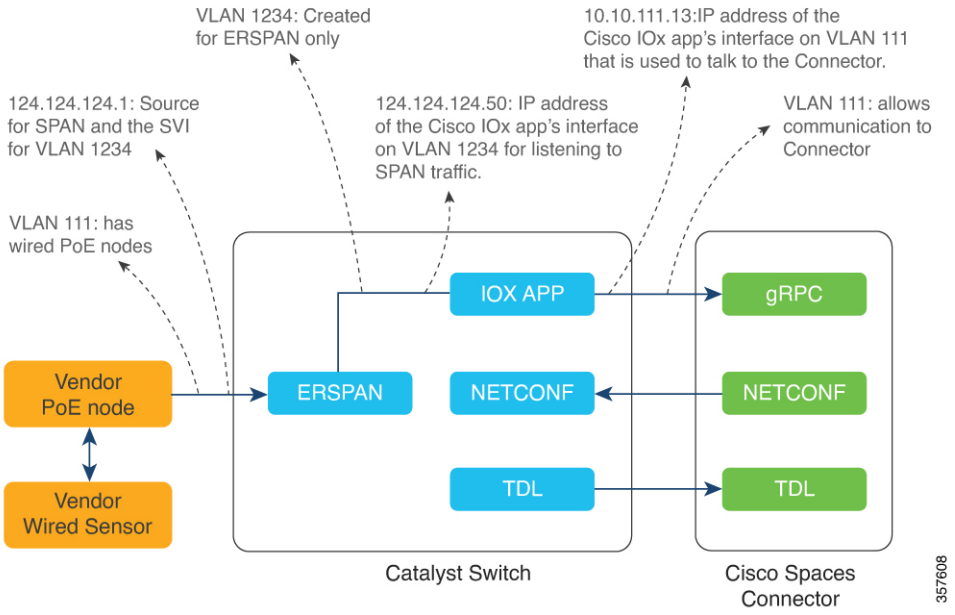
Figure 159: Design Prerequisites



- **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.

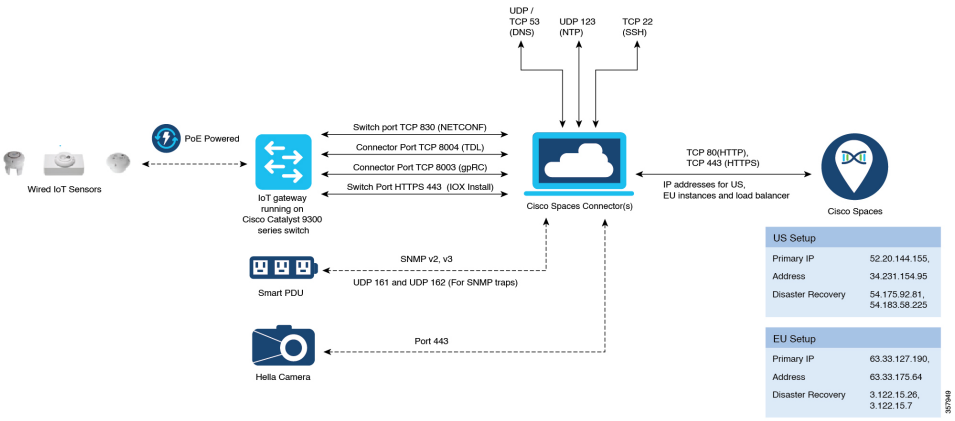
Figure 160: Sample Configuration



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



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

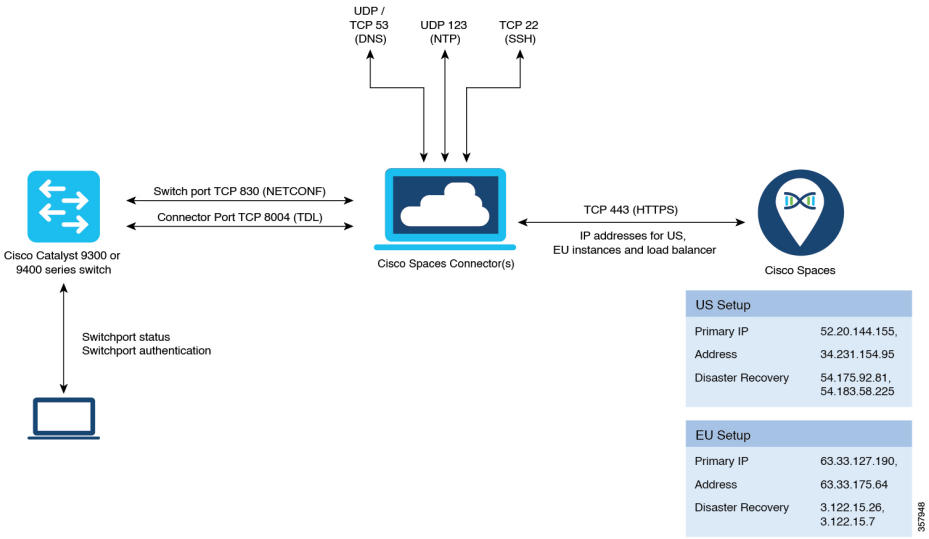


Table 6: Setup Types

	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

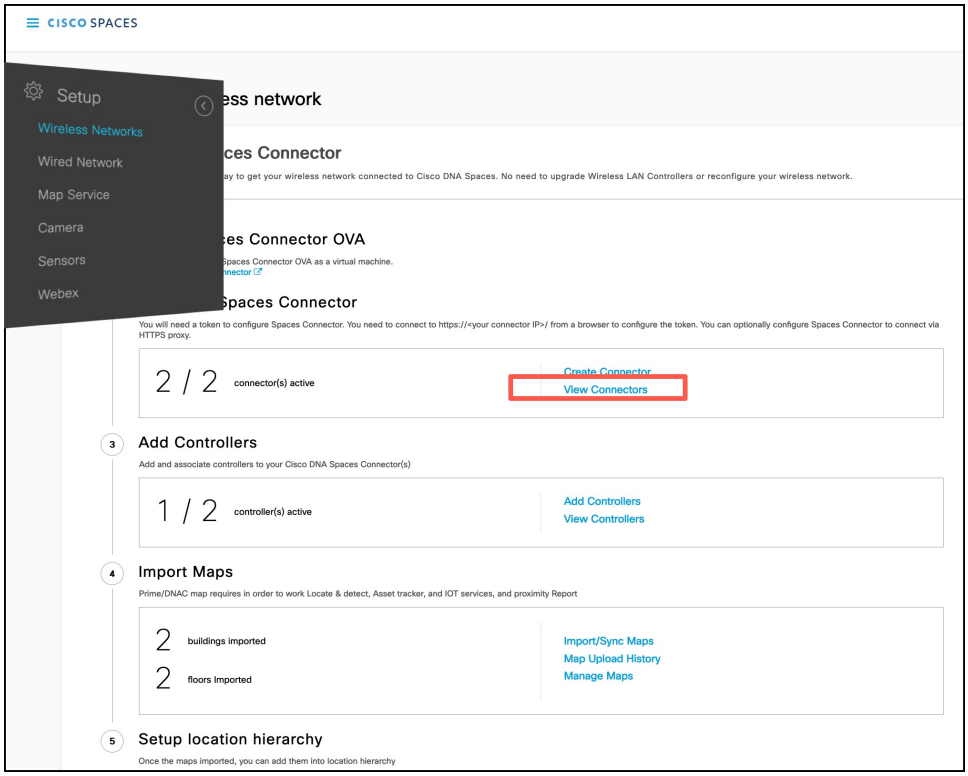
Configure IoT Service (Wired)

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 162: View Connectors

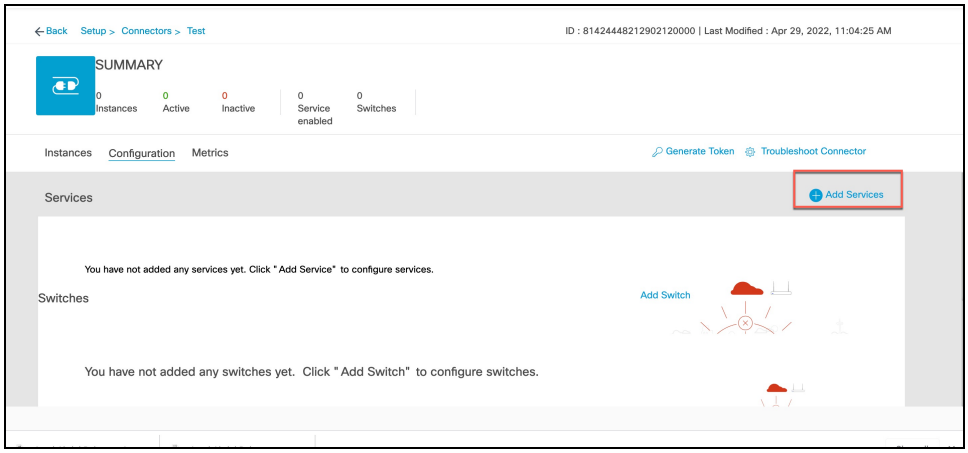


Step 3 Click a connector 3 of your choice.

Note You can use the same connector that you used for Cisco Spaces: IoT Service (Wireless).

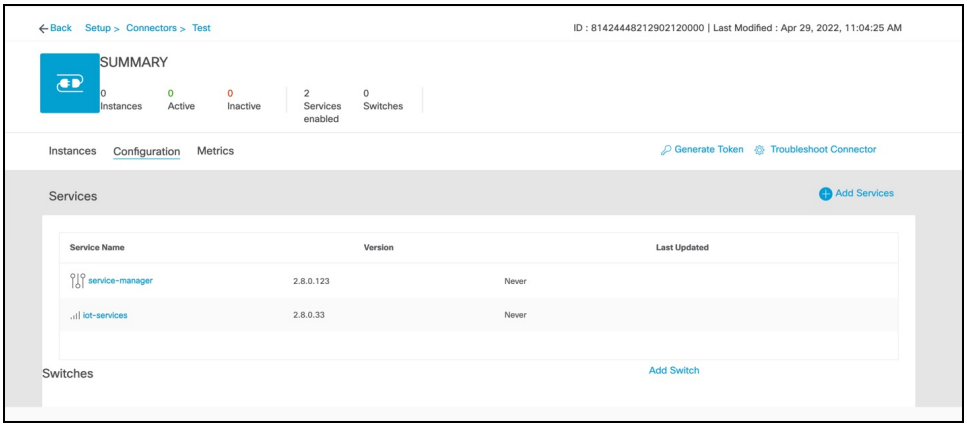
Step 4 In the connector details window that is displayed, click **Add Services**.

Figure 163: Add Services



Step 5 In the **Add Service** window that is displayed, choose **IoT Wired** and click **Add**.

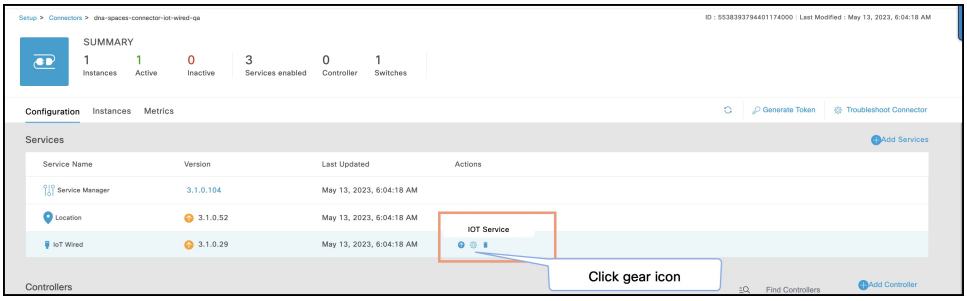
Figure 164: Adding a Service



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.

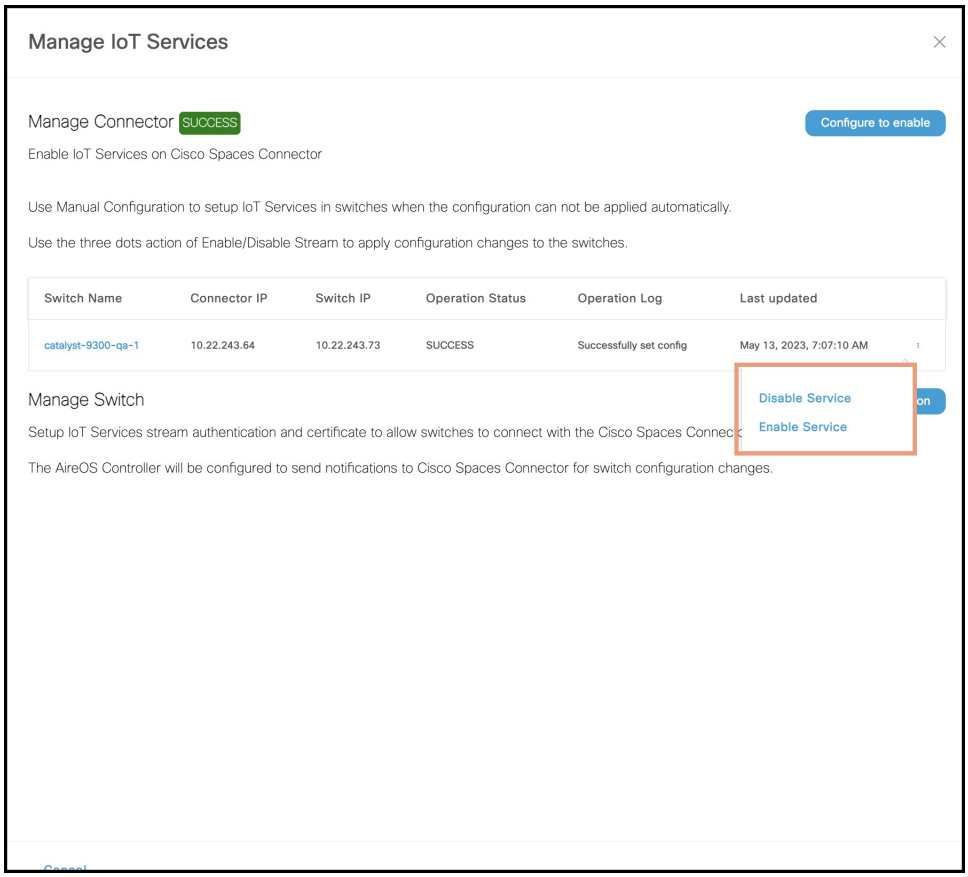
Figure 165: Gear Icon of IoT Wired



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 166: Enable Service



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 167: Configure Switch

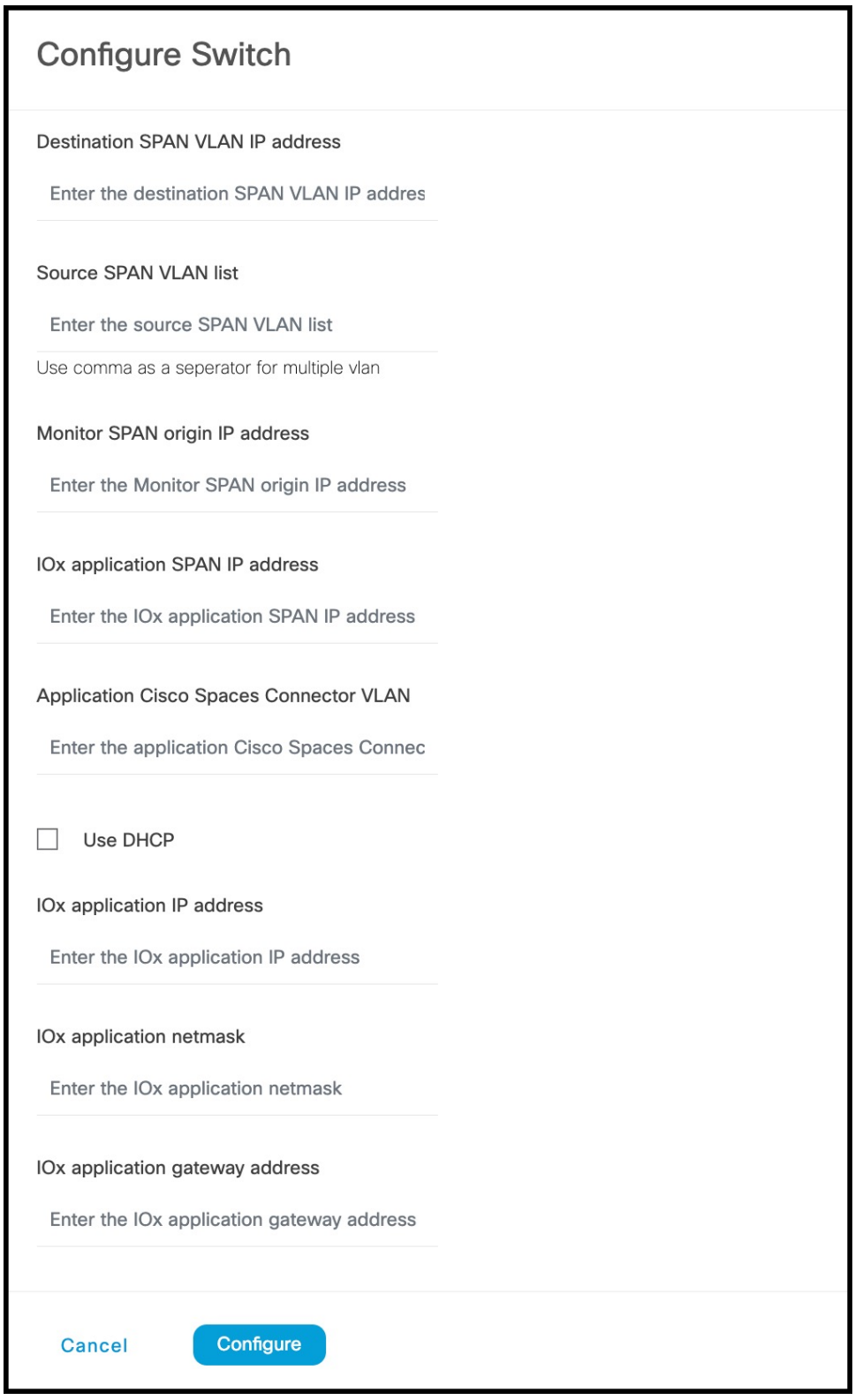


Figure 168: Configure Switch

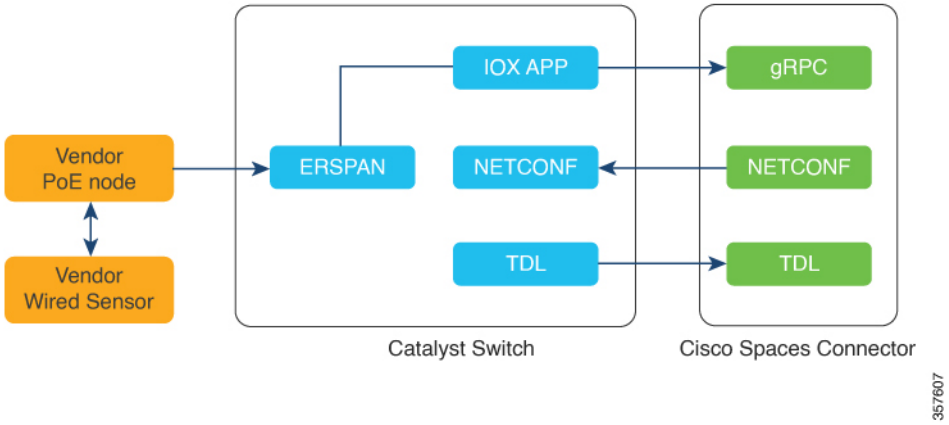
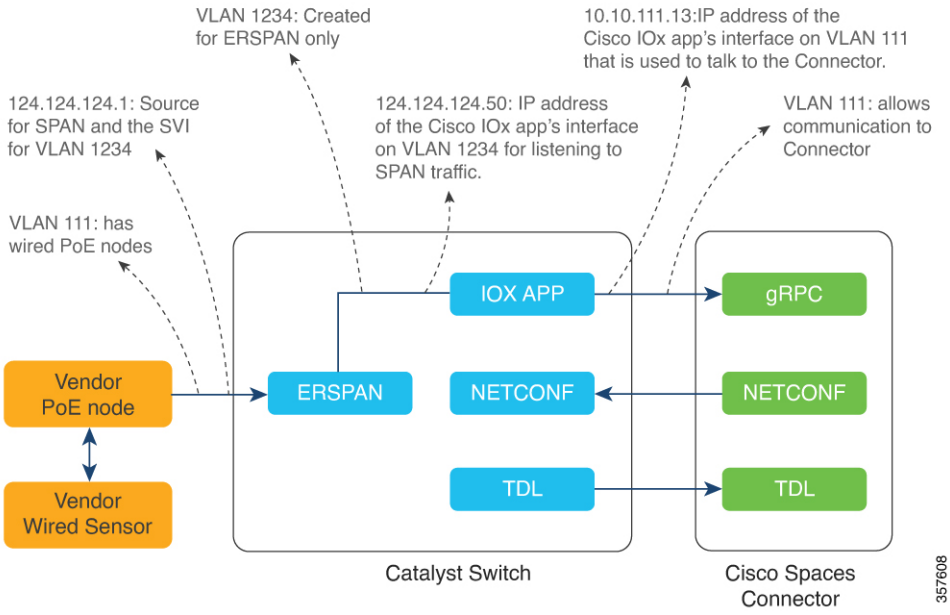


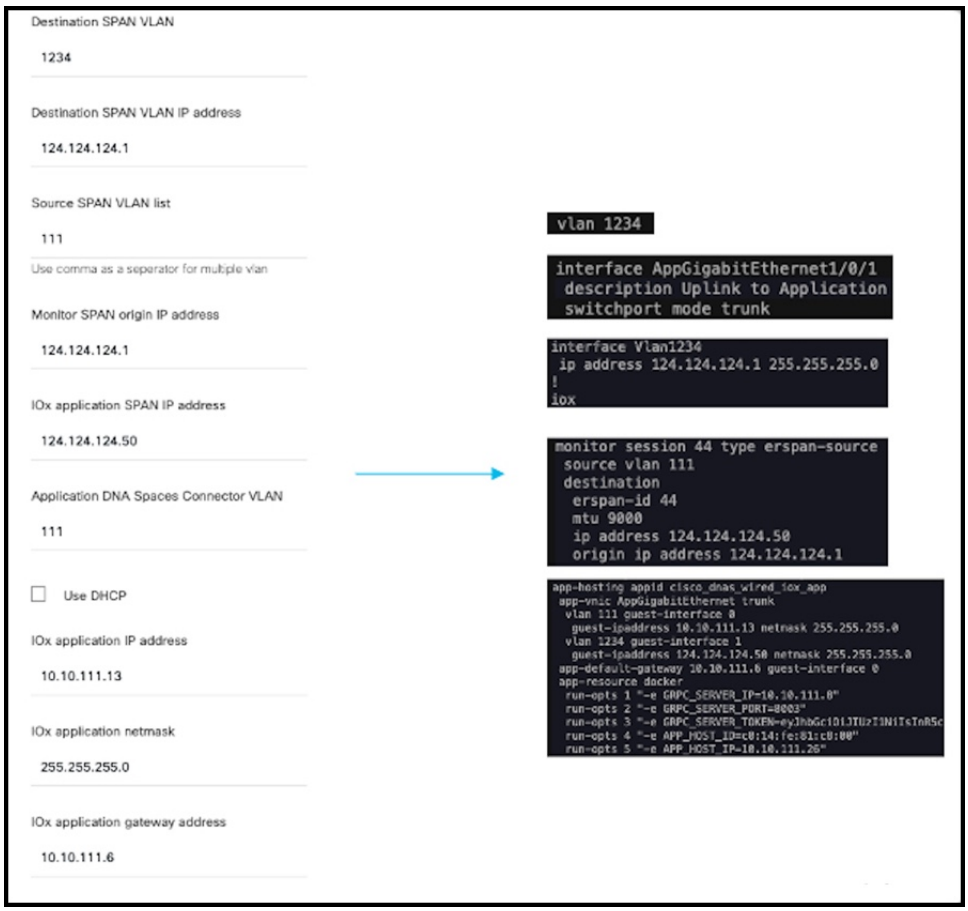
Figure 169: Sample Configuration



Step 10 Click **Configure**.

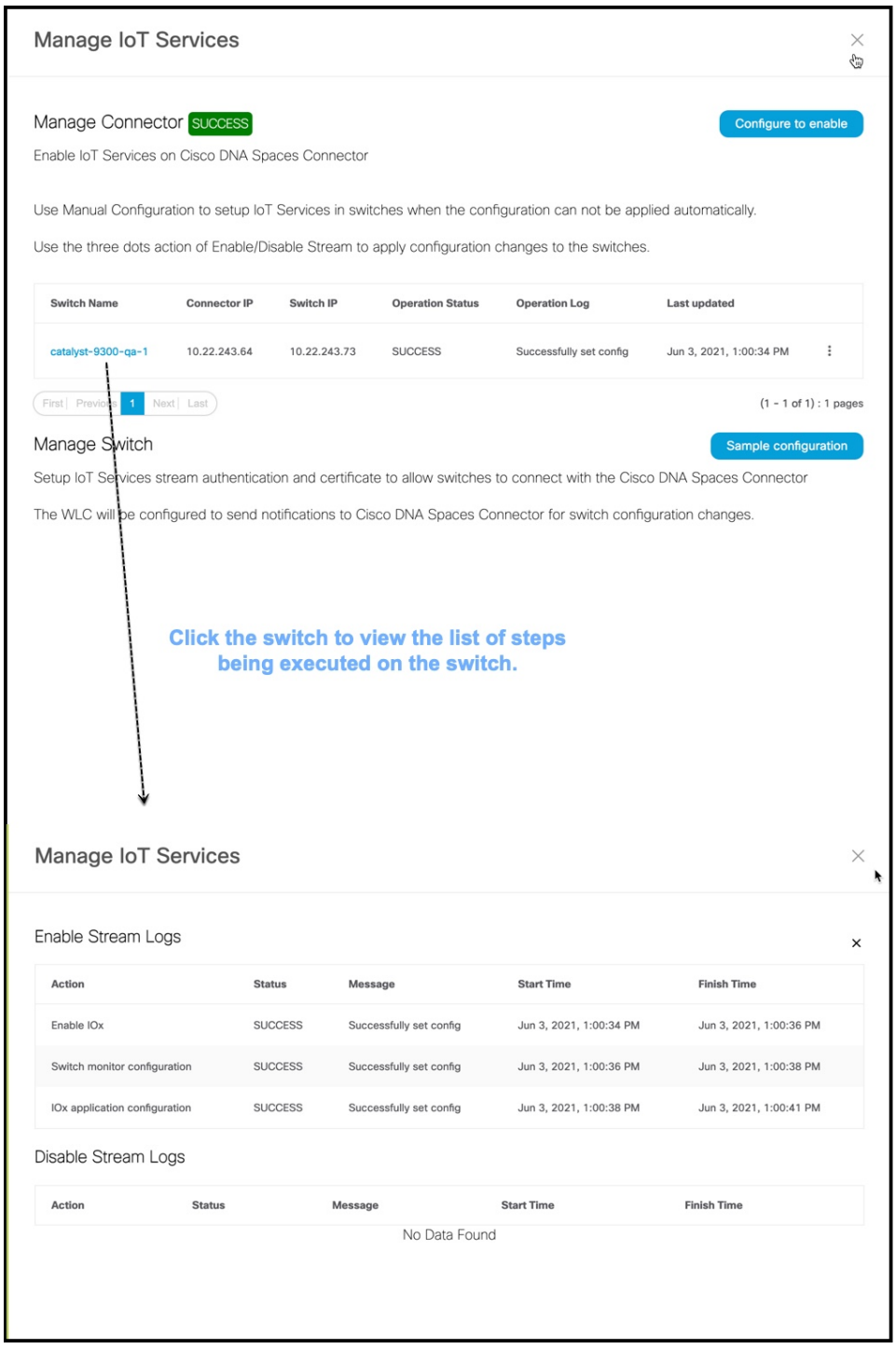
The configurations are deployed on the switch. The following diagram shows the corresponding CLI commands you can use in place of the GUI configuration.

Figure 170: GUI-Command Line Mapping



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 171: Manage IoT Services



Verify if Cisco Catalyst 9300 and 9400 Series Switches are Added to the Connector

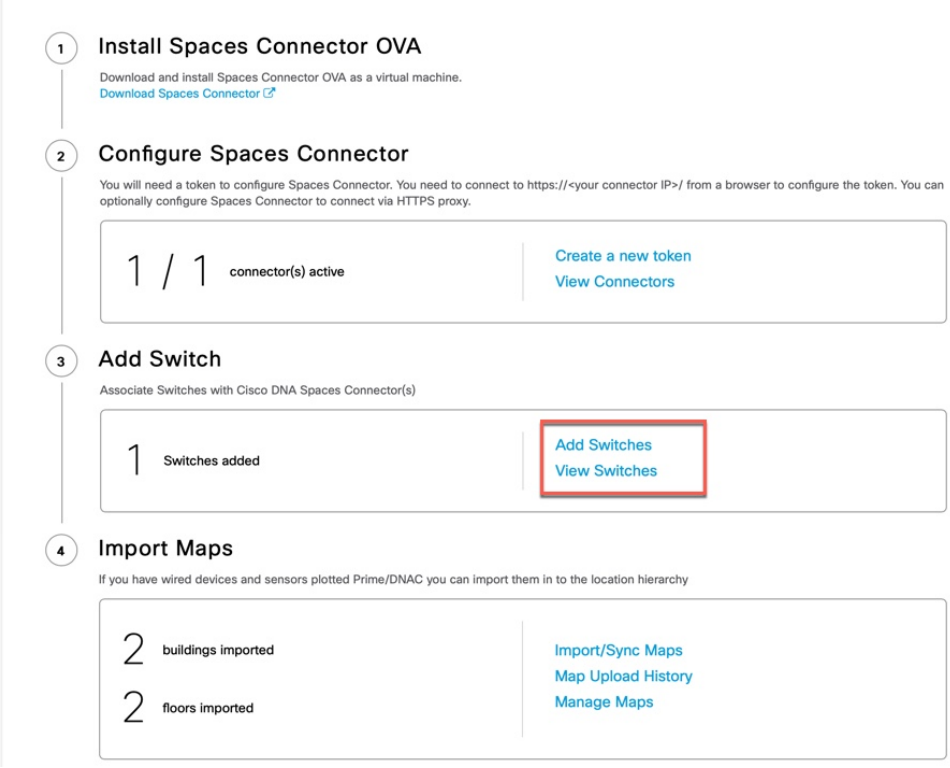
This procedure helps you verify if a Cisco Catalyst 9300 or 9400 Series Switches are deployed and active. This is a necessary prerequisite for proper functioning of Cisco Spaces: IoT Service (Wired).

Procedure

Step 1 In the Cisco Spaces dashboard left navigation pane, choose **Setup** > **Wired Network**.

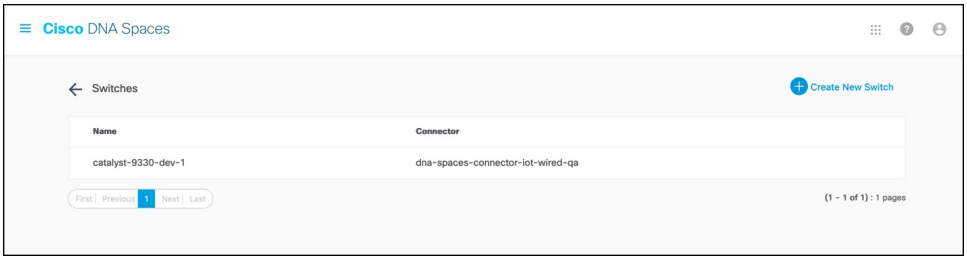
Step 2 In the **Add Switch** area, click **View Switches**.

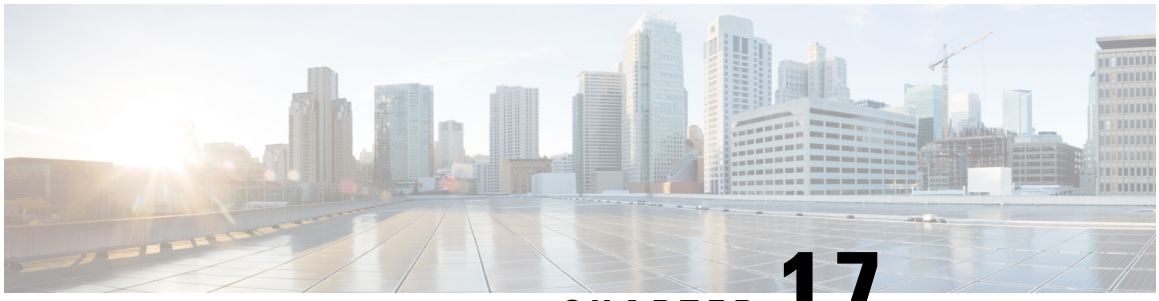
Figure 172: View Switches



Step 3 Ensure that a switch is listed here, and is connected to a Cisco Spaces: Connector.

Figure 173: View Switches





CHAPTER 17

Hotspot Service

- Configure Hotspot Service, on page 163
- Connector Dashboard: Hotspot service, on page 165
- Open Ports for Hotspot Service, on page 165

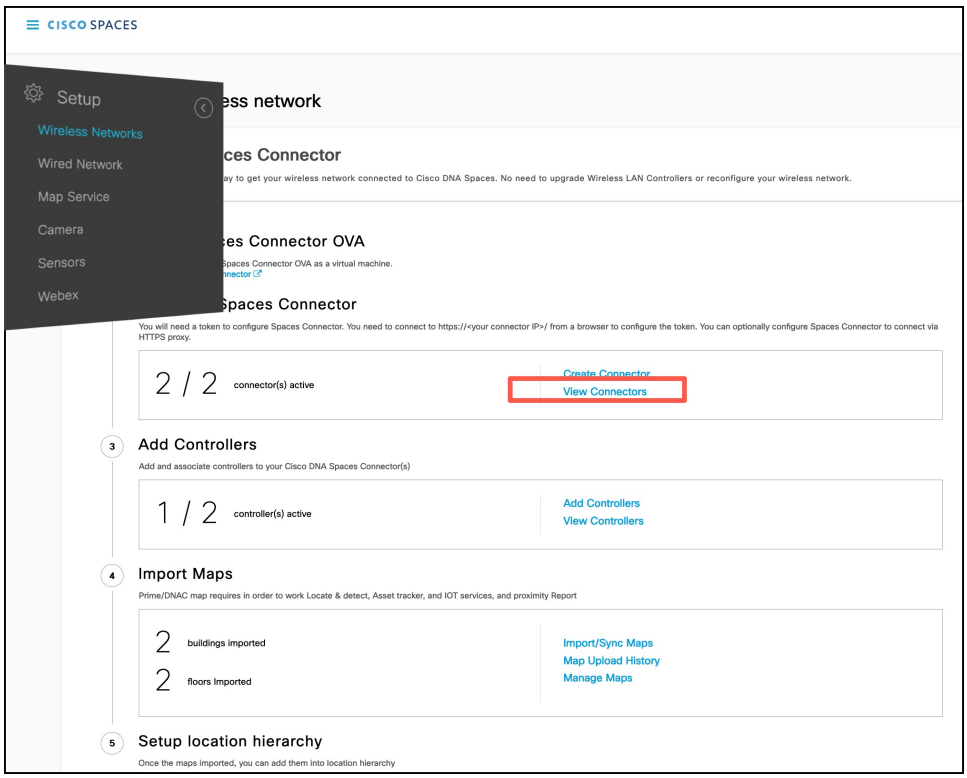
Configure Hotspot Service

Procedure

Step 1 In the Cisco Spaces dashboard left navigation pane, click **Setup** and choose **Wireless Networks**.

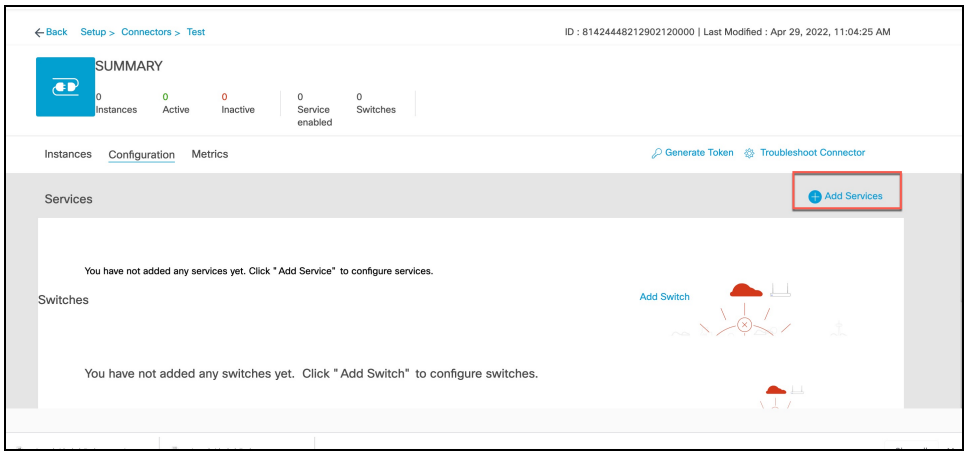
Step 2 In the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 174: View Connectors



Step 3 In the connector details window that is displayed, choose a connector and click **Add Services**.

Figure 175: Add Service



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 176: Hotspot Service

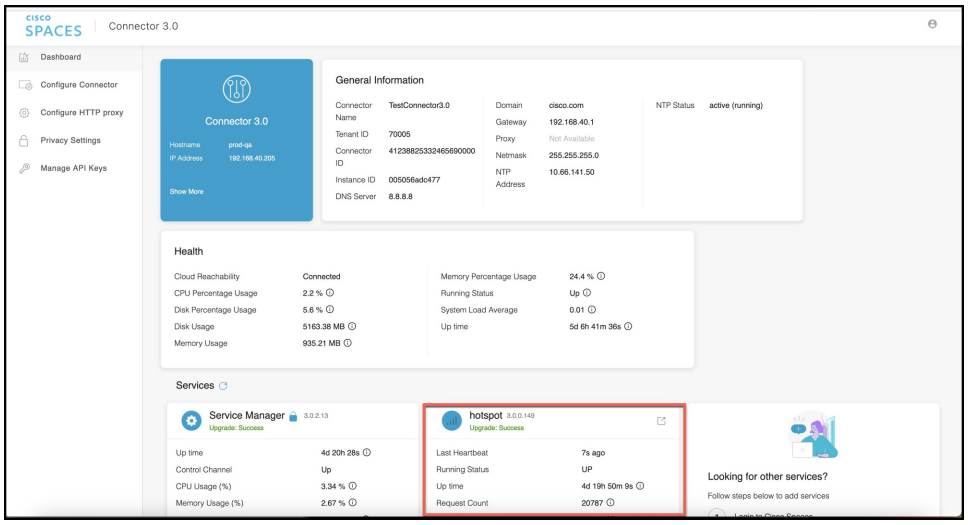
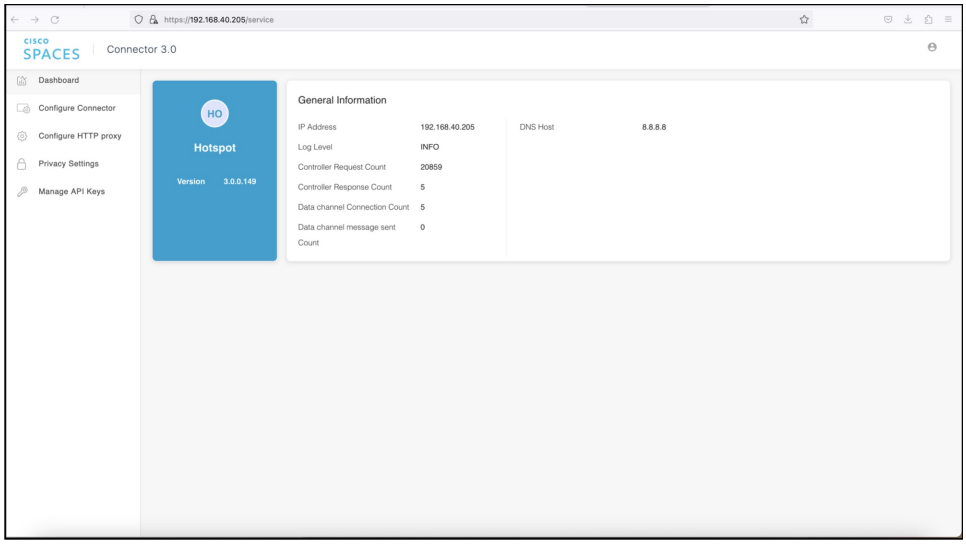


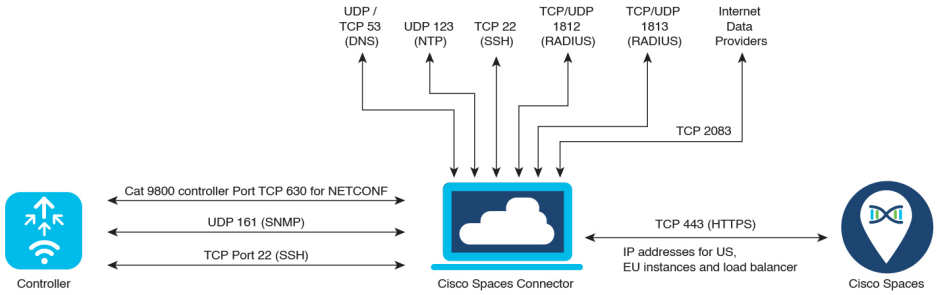
Figure 177: Hotspot Service: Details



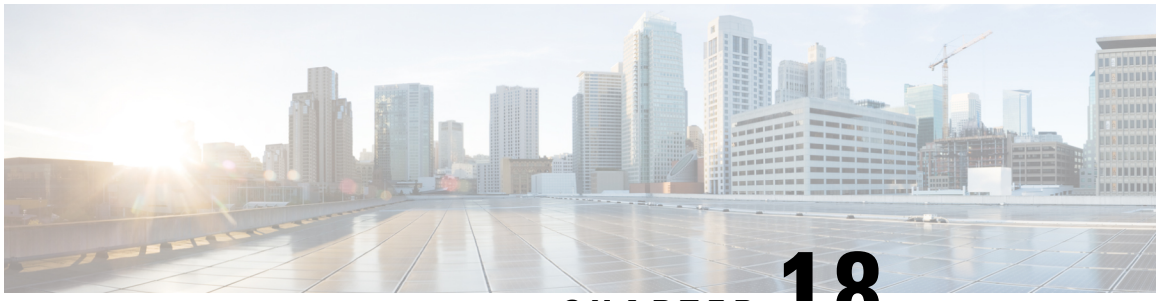
Open Ports for Hotspot Service

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

Figure 178: 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 18

Local Firehose

- Local Firehose Service, on page 167
- Configure Local Firehose Service, on page 167
- Connector Dashboard: Local Firehose Service, on page 170

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

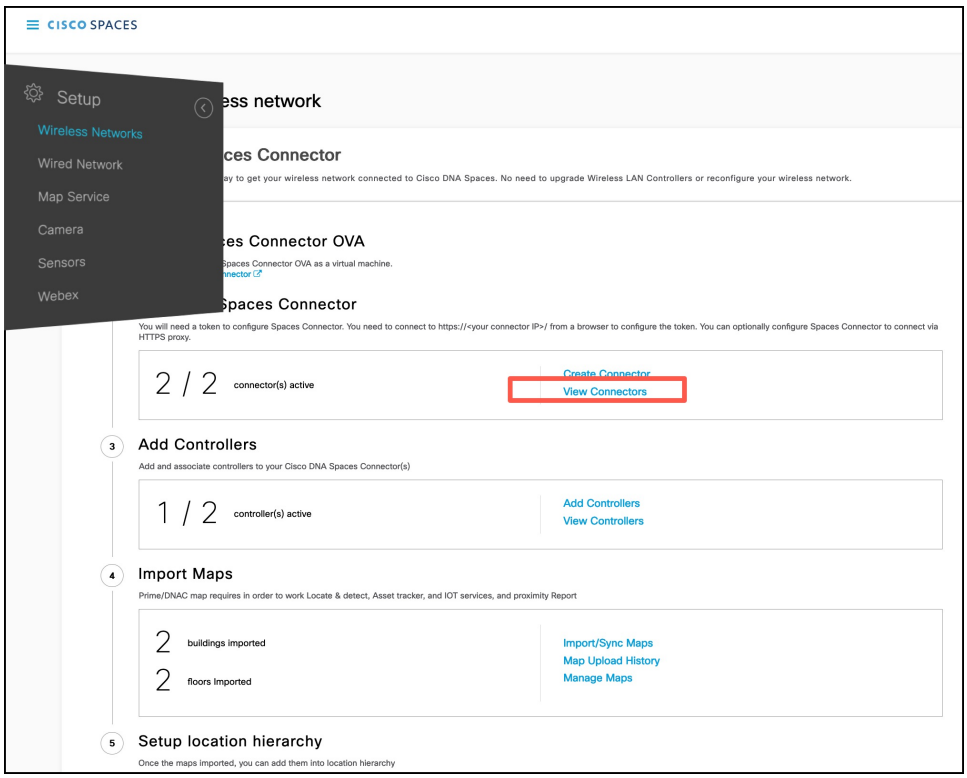
Configure Local Firehose Service

Procedure

Step 1 In the Cisco Spaces dashboard left navigation pane, click **Setup** and choose **Wireless Networks**.

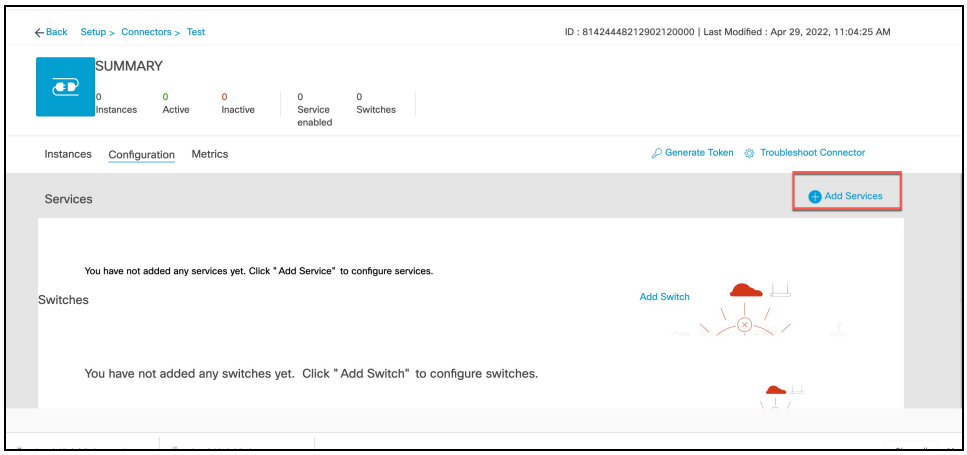
Step 2 In the **Connect your wireless network** window that is displayed, go to the **Step 2** area and click **View Connectors**.

Figure 179: View Connectors



Step 3 In the connector details window that is displayed, choose a connector and click **Add Services**.

Figure 180: Add Service



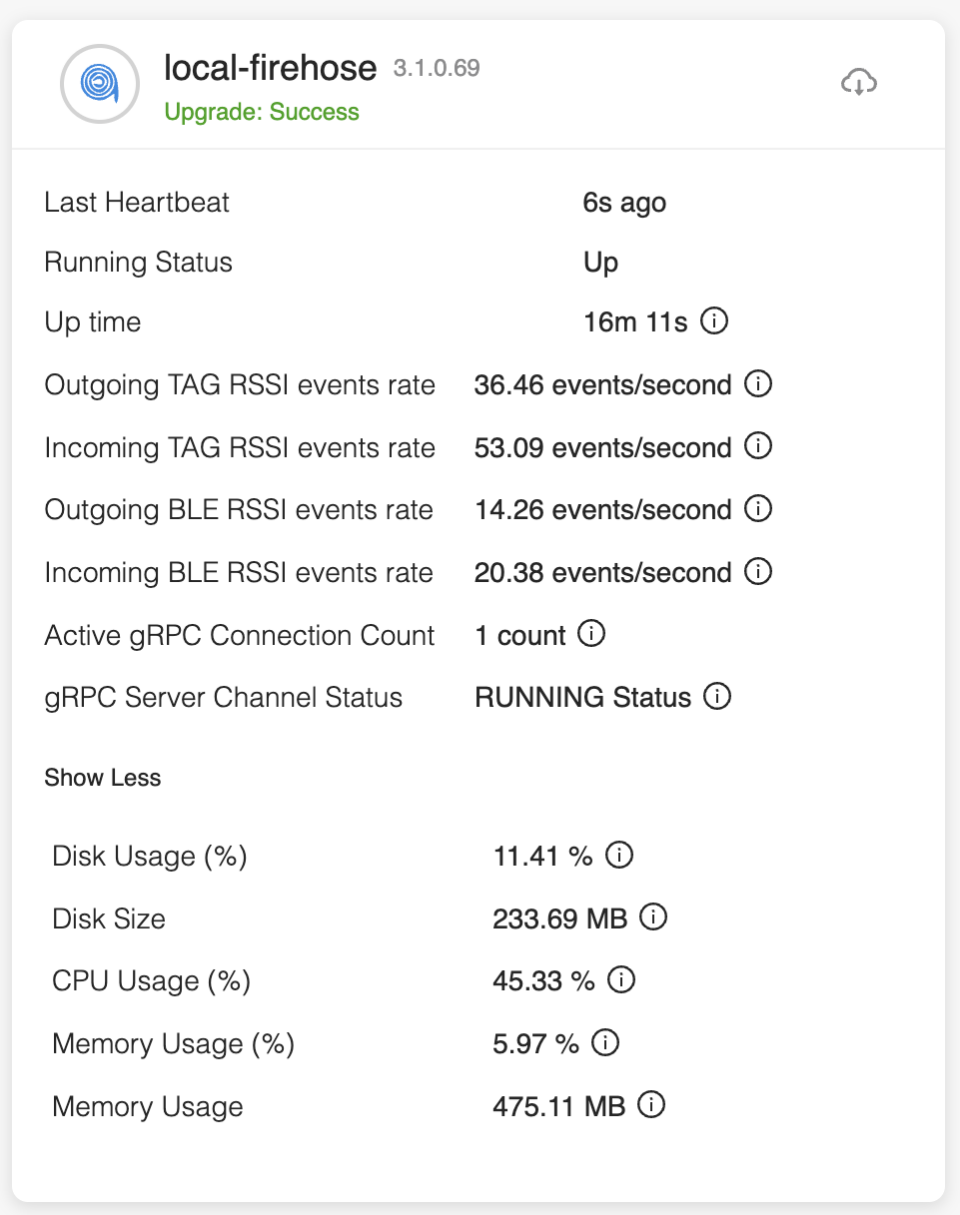
Step 4 In the **Add Service** window that is displayed, choose **local-firehose** and click **Add**.

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 181: local-firehose



Connector Dashboard: Local Firehose Service

Figure 182: Local firehose service: Details on the Connector

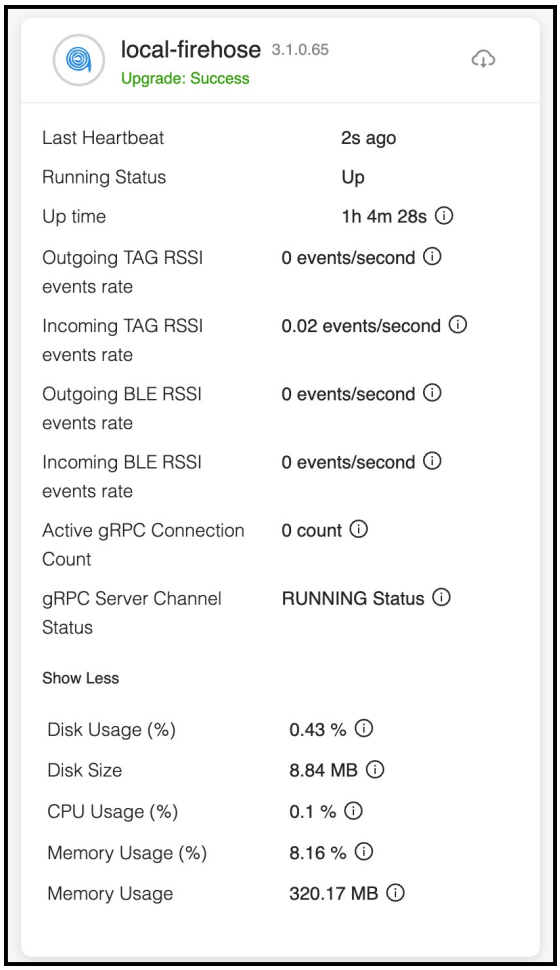
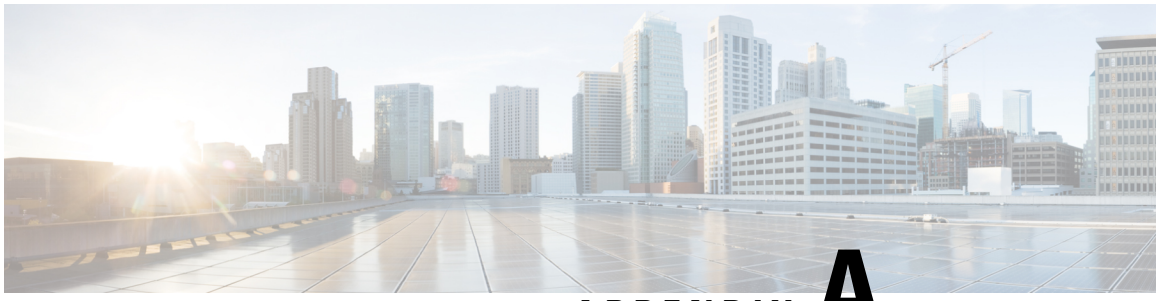


Table 7: Local Firehose Service Metrics

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, on page 173

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:

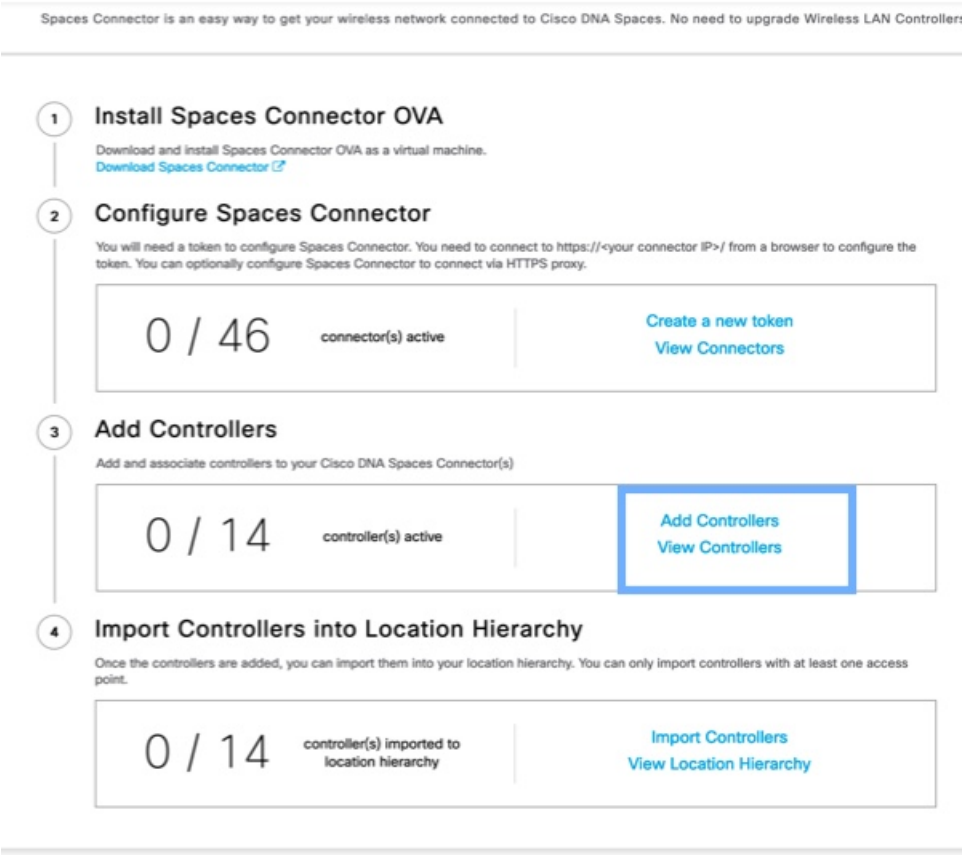
a) Click the pencil icon to edit an AireOS controller.

b) Choose an active Connector from the **Connector** drop-down list to enable the **Test Connectivity** button.

c) Go to Step 8 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 183: Add a New AireOS controller



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.

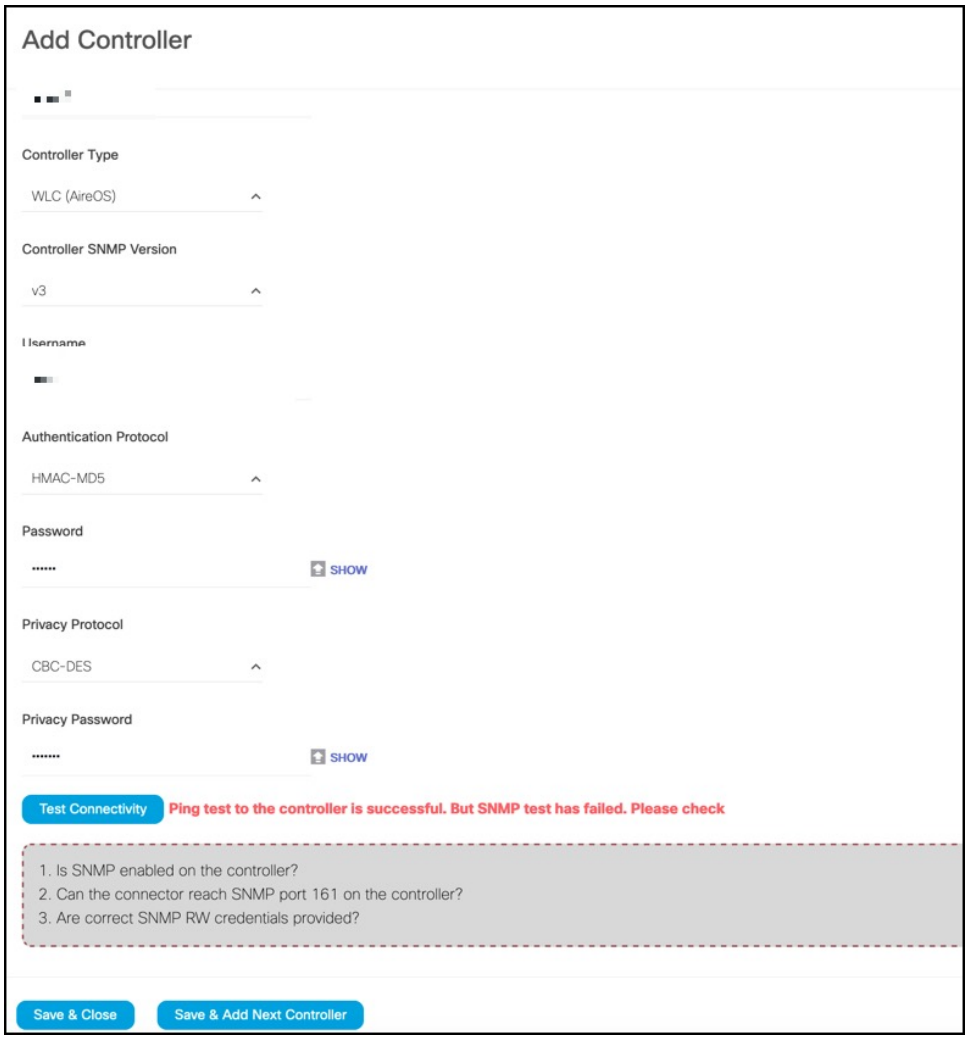
Step 8 From the **Controller SNMP Version** drop-down list, choose the SNMP version of the AireOS controller.

- 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 184: Add a New AireOS controller



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.

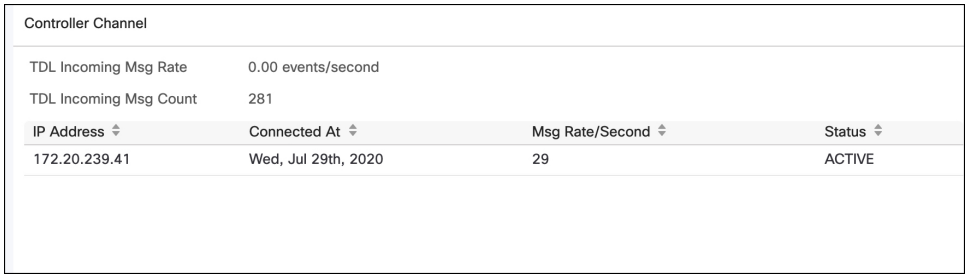
Table 8: Error Description

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.

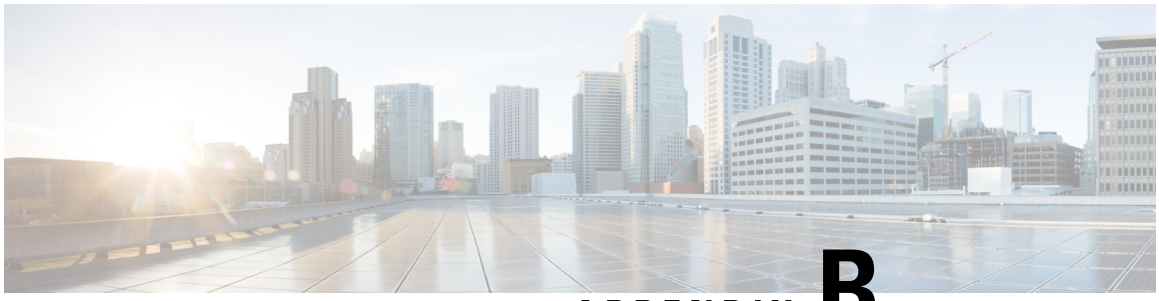
Figure 185: Details of the Catalyst 9800 controller



What to do next

You can import the added Catalyst 9800 controller to the Cisco Spaces location hierarchy.

Connect Connector to Cisco AireOS Wireless Controller



APPENDIX B

Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers

• Configure and Test the Connection Between Connector and Catalyst 9800 Controller, on page 179

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.

Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers

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
```

Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers

```
  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.

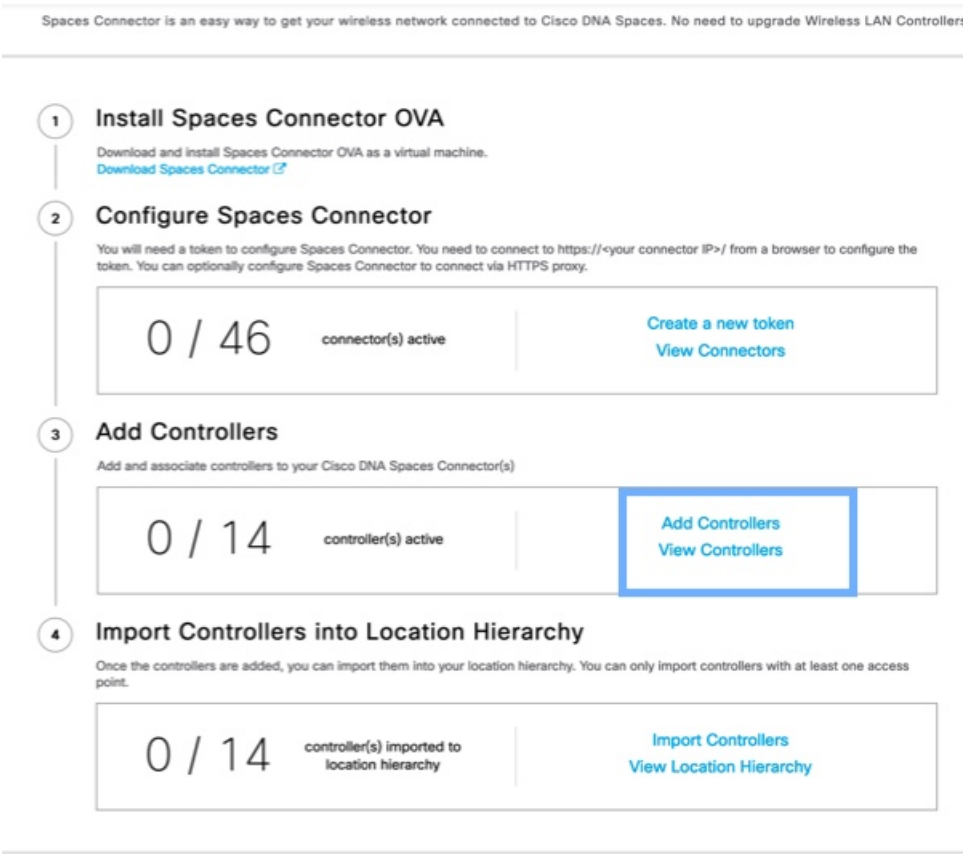
a) Click the pencil icon to edit a Catalyst 9800 controller.

b) Choose an active Connector from the **Connector** drop-down list to enable the **Test Connectivity** button.

c) Go to Step 8 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 186: Add a New Catalyst 9800 controller



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.

Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers

Figure 187: Add a New Catalyst 9800 controller

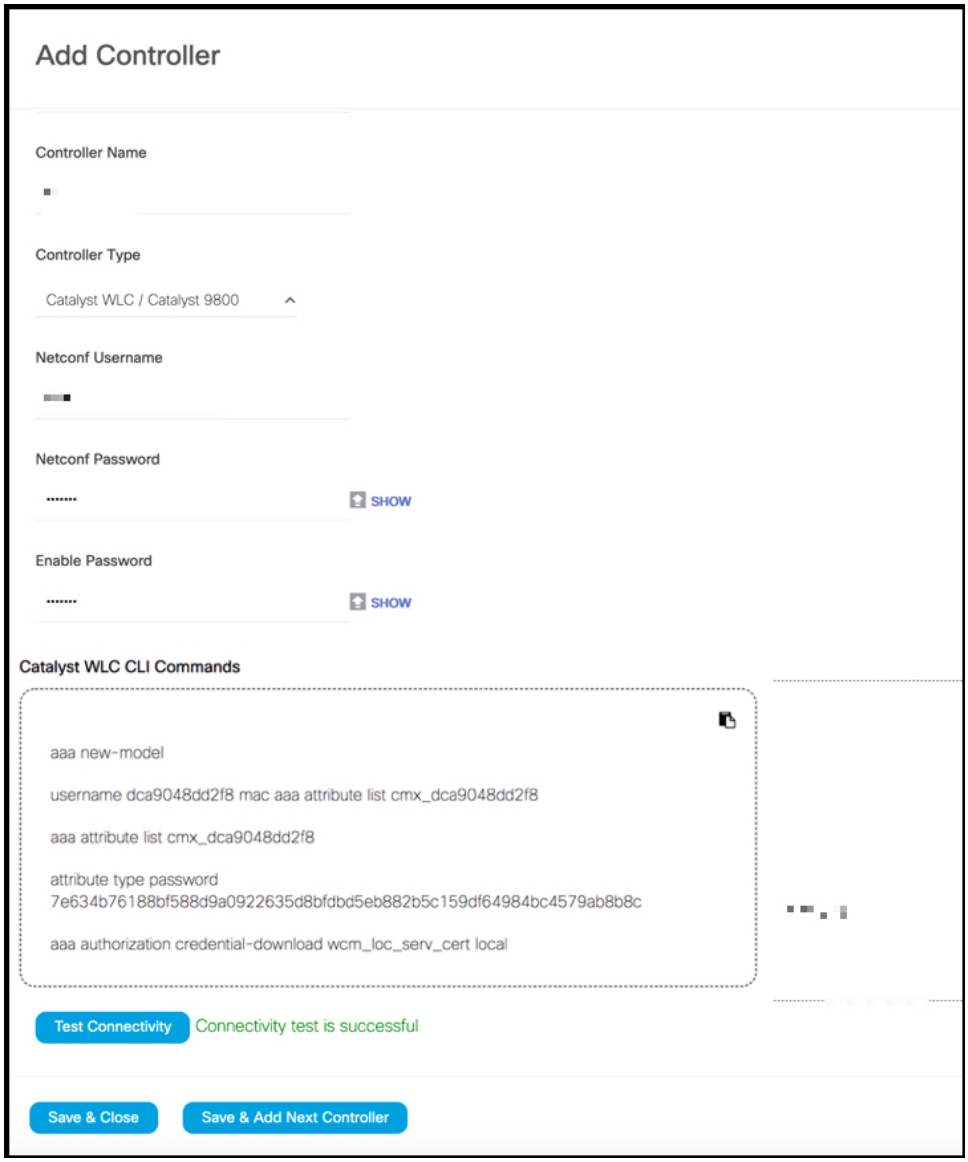


Table 9: Error Description

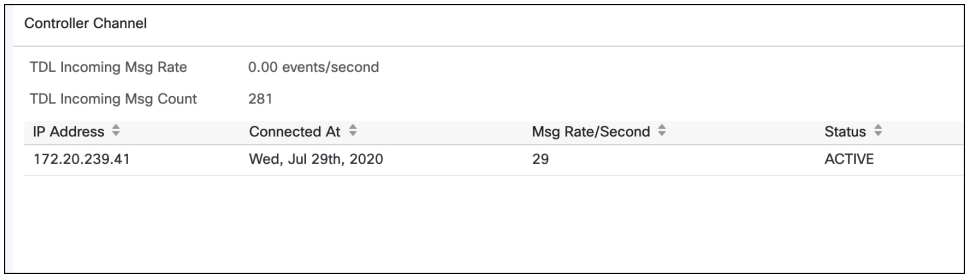
Status of PING	Status of SSH Credential Test	Meaning of status message combination and possible checks.
SUCCESSFUL	SUCCESSFUL	Connectivity test is successful.

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.

Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers

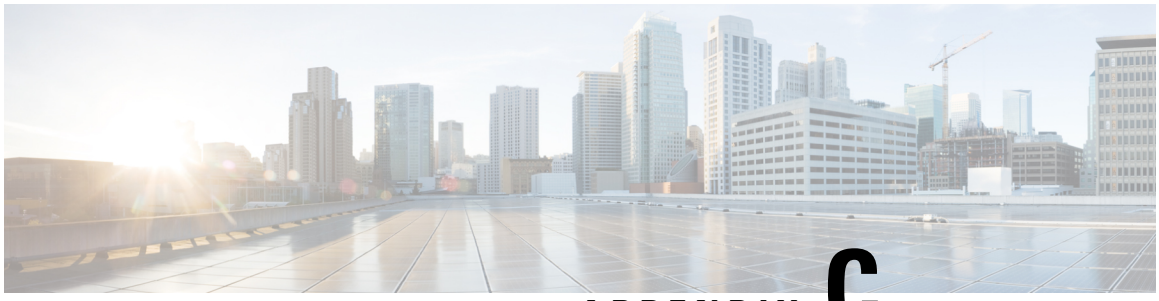
Figure 188: Details of the Catalyst 9800 controller



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 , on page 187

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**

Connect Connector to Cisco Catalyst 9300 or 9400 Series Switches

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**.

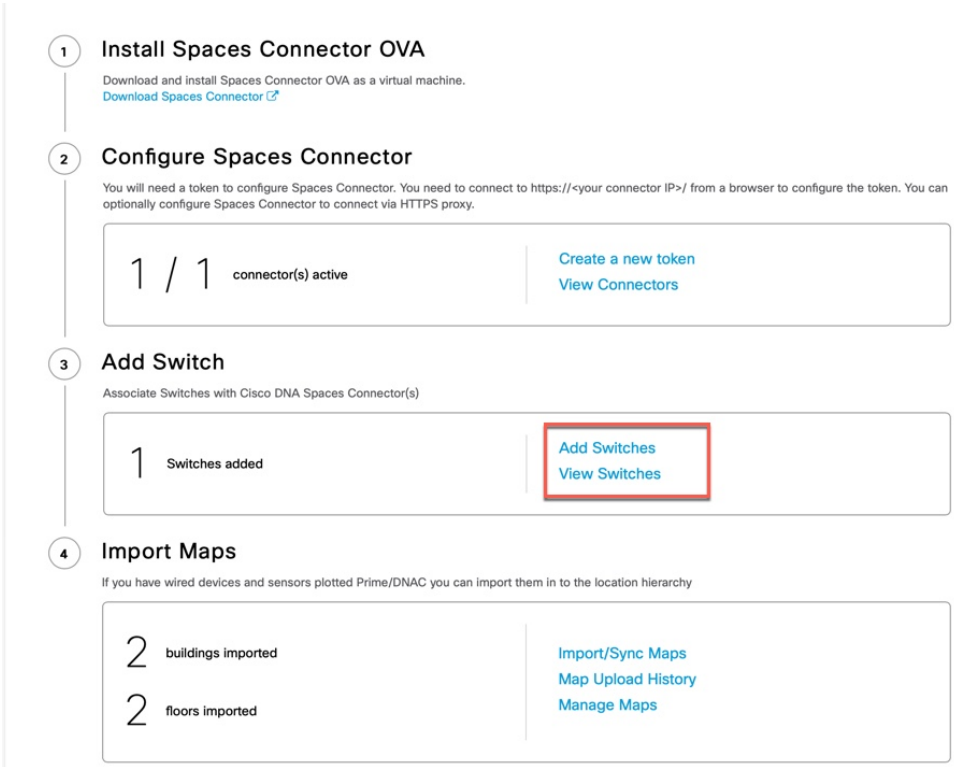


Figure 189:

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**