cisco.



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)
	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

I

I

53

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

I

	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

I



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.	
<i>italic</i> font	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> 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.	
\diamond	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.	
te Means reader t	ake note. Notes contain helpful suggestions or references to material not covered in the manua	
<u> </u>		
ip Means the foll	owing information will help you solve a problem.	
Means reader to or loss of data.	be careful. In this situation, you might perform an action that could result in equipment damag	

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.



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

Getting Started

• Prerequisites, on page 5



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

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



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 you	r wireless network connected with Cisco DNA Spaces area, click Add New.
Step 4	In the Cisco A	ireOS Controller/Catalyst 9800 Wireless Controller area, click Select.

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

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

 Figure 2: Via Spaces Connector

```
Connect your wireless network

How do you want to connect to Cisco DNA Spaces?

Via Spaces Connector

Readers you to instal Space Connector

Readers you to instal Connector

Readers you to instal Space Connector

Readers you to instal Space Connector

Readers you to instal Space Connector

Readers you to instal Conne
```

Step 6

Figure 3: Read Prerequisites for Spaces Connector

	Great! Based on your inputs, we have customized setup to help you connect your wireless network to Cisco DNA Spaces using Spaces Connector	
Prerequis	sites for Spaces Connector	
1	You must have WLC version 8.0 and above.	
2	You must have access to a virtual machine (VMware) to install Spaces Connector.	
3	Spaces Connector needs access to your Wireless LAN Controllers and connectivity to the Internet (direct connection or via HTTPS proxy)	
	Customize Setup	

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

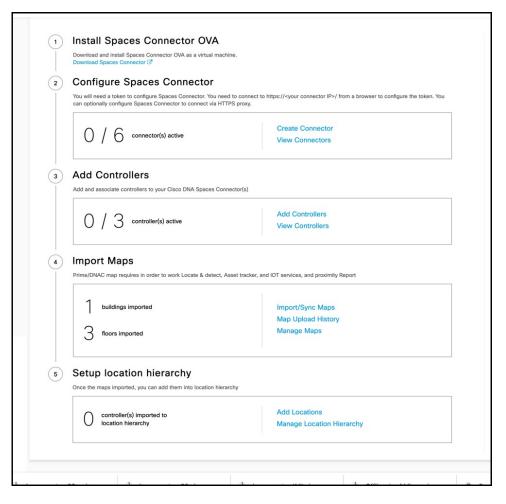
 Step 7
 Expand the Connect via Spaces Connector area using the respective drop-down arrow.

 Figure 4: Expand Connect via Spaces Connector

Connect your win	eless network		
	paces Connector y way to get your vitreless network connected to Cisco DNA Spaces. No need to upgrade Wiveless LAN Control		Click to
	Catalyst 9800 Directly		expand ~
ireless Networks	C sring		~
	gin Is to connect to Chico Merell Cloud, import locations in to Chico DNA Spaces and activatelying t	he Merali Networks.	× v
B	Get your wireless network connected with Cisco DNA Spaces There are multiple options to get connected based on your wireless network opplyment.	Need Help? Configuration guide Claco AlreOS/Catalyst 27	
	+ Add Now	Cisco Meraki C	

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

Create Connector
Spaces Connector Name Enter the spaces connector name Connector Version
 Version 2.X First generation Connector designed to transfer location data efficiently to Cisco Spaces cloud Version 3.0 Support for deploying and managing multiple individual services Enhanced monitoring and troubleshooting of the connector and connector services Samless services and system upgrades Refer to the Connector 3.0 Configuration Guide for more details Enable Location Services ()
Cancel Save

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



Create Connector	
	\bigcirc
	Connector Created Successfully
	Next step:
	Please generate a token from connector details page and configure it in your "instance/box"
	Go to Connector Details Page

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

←Back Setup > Connectors > Test	ID : 81424448212902120000 Last Modified : Apr 29, 2022, 11:04:25 AM
SUMMARY 0 0 0 2 0 Instances Active Inactive enabled	
Instances Configuration Metrics	🖉 Generate Token
Instances in High Availability Pair Configure your instance	
To set up high availability pair follow the steps below. Step 1:	
Genarate a token by clicking the Generate Token button on the top of this page. A token will be generated.	
Step 2:	

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

Figure 9: Copy Token

Token	ex
Configure the token below on your instance/box	
eyJhbGciOiJIUzI1NiisInR5cCl6ikpXVCJ9.eyJ2ZXJzaW9uljoiVjMiLCJ0b2tlbklkljoiNzM3MTIyYTAtY2l3MS0xMWVjLWFm YmUtMTU4MTA0NjY3NjQwliwiaWJ5ljoiTG9jYXRpb24iLCJ0eXBlljoiY29ubmVjdG9yX2F1dGhfdG9rZW4iLCJ0ZW5hbnR JZCl6iJEyMTExliwiY29ubmVjdG9ySWQiOjgxNDl0NDQ4MjEyOTAyMTIwMDAwLCJlbmRwb2ludCl6Imh0dHBzOi8vY29u bmVjdG9yLnFhLWRuYXNwYWNlcy5pbyIsImVudmlyb25tZW50ljoidGVzdClsInJIZ2lvbil6InVzLWVhc3QtMSIsImIhdCl6M TY1MTY0NDg2N30.0VVo8ozAsaDcZr0Abo_G1Y732TQENGpJr1uXJIW5bY0	
Copy Token View Documentation	
To set up your connector instance, follow the steps below.	
Step 1:	
Copy the generated token above.	
Step 2:	
Login to your connector UI and configure the token. Follow the documentation if you haven't setup your connector yet.	

- **Step 12** Open the connector GUI.
- **Step 13** (Optional) If your network is behind a proxy, configure the GUI with the proxy. See Configure a Proxy, on page 91
- **Step 14** In the **Configure Token** area that is displayed, click **Configure Token**.

Figure 10: Configure Token

Configure Connector	Configure Token Without the token, the connector w	ill not be able to start.		Click to	configure the token	copied from Cisco S	Configure T
Configure HTTP proxy Privacy Settings	U	General Information	Not Available	HA Config Mode	Not VIP Paired	Primary Interfac	e 10.89.45.92/24
Manage API Keys	Connector 3.1	Tenant ID	Not Available			MAC Address	00:50:56:A7:54:C8
S Troubleshoot	Hostnama conn-pri Phokage connectoral-pili4 Show More	Connector ID Instance ID Proxy NTP Address NTP Status	Not Available 005058a754c8 https://proxy.esi.cisco.com.80 ntp.esi.cisco.com			DNS Server Domain	10.89.45.1 171.70.168.183 cisco.com ipv4
		NTP Status	active (running)				

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

L

Upgrading the Connector from Cisco Spaces Dashboard

Use the connector's GUI to upgrade connector.



- 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 dashb	oard, choose Setup > Wireless Networks.		
Step 3	From the 2. Configure Sp	aces Connector area, click View Connectors		

Figure 11: View Connectors

	figure Spaces Connector	ed to connect to https:// <your connector="" ip="">/ from a browser to configure the token. Yo</your>
	ionally configure Spaces Connector to connect via HT	
C) / 6 connector(s) active	Create Connector View Connectors
Add	Controllers	
Add an	d associate controllers to your Cisco DNA Spaces Con	nnector(s)
C) / 3 controller(s) active	Add Controllers
) / J Controller(s) active	View Controllers
Imn	ort Maps	
· ·		Asset tracker, and IOT services, and proximity Report
1	buildings imported	Import/Sync Maps
		Map Upload History
3	floors imported	Manage Maps
Set		Manage Maps
· · · · · ·	floors imported	
/	up location hierarchy	

- **Step 4** From the list of connectors that are displayed, click the connector of your choice.
- **Step 5** From the **Configuration** tab of the specific connector, ensure that the Service manager service is upgraded. If not upgraded, under the **Actions** column, check for any available **Upgrade** option.
- **Step 6** Click the **Instances** tab, and choose the instances you want to upgrade.
- **Step 7** In the **System Upgrade Available** area, and click **Upgrade**.

Figure 12: Upgrade

Figure 13: Select instance

CISCO SPACES		≡ Φ €
Setup > Connectors > upgmdeTest SUMMARY 1 1 0 Instances Active Inacti	2 0 0 Services enabled Controller Switches	10 : 30004488891381166000 Laet Modified : May 11, 2023, 12:04:11 AM
Configuration Instances Metrics		C 🖉 Generate Token 🍈 Troubleshoot Connector
System Upgrade Available! We have updated the system library and have secu	rity fixes in the release, click here to see the release note.	Upgrade
Instances in High Availability Pair		
O05056a78cc6 System Package: connector3-p83- sep2022	0	
Mac ID	00:50:56:a7:8c:c6	
IP Address	10.89.45.100	
Status	🔁 Up	
Control Channel Status	Connected	
HA Status	Not Paired	
VIP Address	NA	
SERVICES		

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.

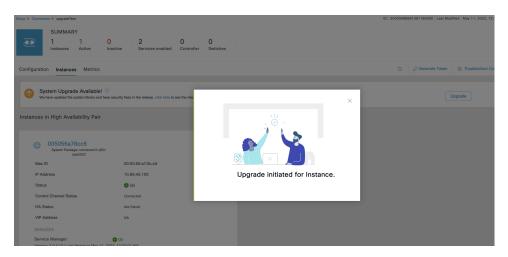
For connector Release 3.1, the upgrade option is available from the Cisco Spaces dashboard as the timeout period has been increased to accommodate low latency networks.

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

Cisco SPACES Setup > Convectors > unpraise Test D - 20094488811 SUMMARY 1 0 2 0 Instances Active 0 0 Services enabled Controller Switches Configuration Instances Metrics Controller System Dipgrade Availability Pair Please select the instance to upgrade. Please select the instance to upgrade. Imagination 0050556a78cc6 Please select the instance to upgrade. Imagination 0050556a78cc6 Please select the instance to upgrade. Imagination 0050556a78cc6 Vertee Researce concentrol splate Imagination 0050556a78cc6 Upgrade National Status One to the instance in High Availability Pair Please select the instance to upgrade. Imagination 0050556a78cc6 Upgrade Nations Imagination 0050556a78cc6

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

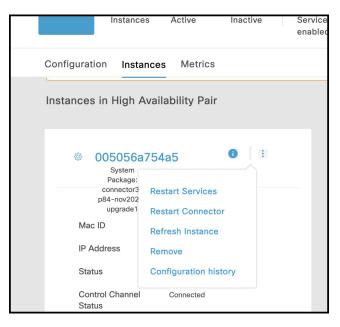


Figure 16: Configuration History

	005056a754a5: Service o	configuration history	<
ictive	Operation: Service: Status:	May 8, 2023, 11:10:34 PM System upgrade connector3-p84-may2023 upgrade in progress	

Upgrading the Connector Using CLI

Use the connector's CLI to upgrade connector.

Note

• This is referred to as system inline upgrade or system upgrade using the connector CLI.

• System upgrade is not supported for AMI connector instances.

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

Before you begin

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

Procedure

- Step 1Log in to the connector CLI.Step 2Check 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 gueued. 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'
```



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 19: AWS MarketPlace AM/a

Figure 18: AWS MarketPlace AMIs

alialia cisco	Cisco DNA Spaces Connector Cisco Systems, Inc. Cisco Systems, Inc. Cisco Systems, Inc. Cisco Systems, Inc. Cisco DNA Spaces Connector Systems, Inc. Cisco DNA Spaces Connector Cisco DNA Spaces Connector Cisco DNA Spaces Connector Cisco DNA Spaces Connector Cisco Systems, Inc. Cisco Systems, Cisco System	r		×
Overview	Product details Pricing	Usage Support		
	Spaces: Connector enables Cisco DNA Ig any client information	Spaces to communicate with multiple controllers	efficiently, by allowing each controller	to transmit client data
Typical total p	rice	Latest version	Video	
\$0.093/Hr otal pricing per instance for services hosted on t2.large in us-east-1. see additional pricing information.		Cisco DNA Spaces Connector3 July2024 Delivery methods Amazon Machine Image ④ Operating systems	Product Video 🔀 Categories Network Infrastructure	
		Other AlmaLinux 8 CentOS 7		
You of now'	can subscribe to this AMI now or we wil if you are sure this is the AMI you wan	re you can launch an instance. Check the pricing l automatically subscribe for you when you launci t to use to launch as it will reduce wait time on la mit to a subscribing vet. By subscribing to this A ar License Agreement [2]	h this instance. We recommend that yo unch. Choose 'Subscribe on instance la	ou 'Subscribe unch' if you are
		Cancel	Subscribe on instance launch	Subscribe now

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

Figure 19: Launch Instance from AMI

EC2 > AMis > ami-0f0326aca1b04cf96						
Image summary for ami-Ofd326aca1b04cf96 (Connector3-b84-Jan-QA-Img)						
AMI ID ami-Ofd326aca1b04cf96 (Connector3-b84-Jan-QA-Img) AMI name	Image type machine Owner account ID O 038249548279	Platform details Linux/UNIX Architecture x86_64	Root device type EBS Usage operation Runinstances			
Root device name	Status Ø Available	Source D 038249548279/cisco-dna-spaces-connector3-b84- jan2023-8.4.0-22-DEV	Virtualization type hvm			
Boot mode -	State reason -	Creation date Fri Jan 27 2023 12:11:41 GMT-0800 (Pacific Standard Time)	Kernel ID -			
Block devices //dev/sda1=snap-00412ac8bc1448df9:15:true:gp2	Description -	Product codes -	RAM disk ID -			
Deprecation time -	Last launched time –					

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

Figure 20: Launch Instance from AMI

WS	Services	Q Search				[Option+S]
=	Amazon EC2 a	1 an inst allows you to cr simple steps be	eate virtual mae	chines, or instances	, that run on the A	\WS Cloud. Quickly get started by
	Name a	nd tags Info				
	Name					
	Connecto	or3-AMI-Dev-Ins	stance-1			Add additional tags
	AMI	from catalog	Recents	My AMIs	Quick Start	
	Amazoi	n Machine Imag	e (AMI)			Q
		tor3-packer-al n dd6727207b37				Browse more AMIs Including AMIs from AWS, Marketplace and the Community
	Pub	lished A	Architecture	Virtualization	Root device	ENA Enabled
		>	86_64	hvm	type ebs	Yes

Step 7 Choose any EC2 instance that has a minimum of 2 vCPU and 4GB Memory. Click Next: Configure Instance Details.
 t2.medium corresponds to a standard window with 2vCPUs and 4-GB memory and is the recommended setting.

Figure 21: Configure Instance Details

aws	Services	Q Search [Option+S]			
Ξ	▼ Instar	ce type Info				
	Instance type					
	On-Deman	n 2 vCPU 4 GiB Memory 1 Linux pricing: 0.0464 USD per Hour 4 Windows pricing: 0.0644 USD per Hour	Compare instance types			
		air (login) Info se a key pair to securely connect to your instance. Ensure that you have access to the nce.	selected key pair before you launch			
	Key pair na	me - required				
	connecto	-ami-test-key	C Create new key pair			

- **Note** You can have a more advanced configuration by choosing an option with higher vCPU and memory, by choosing an instance type with one of the following configurations. If an exact match is unavailable, you can choose a configuration with the next-available vCPU or memory:
 - 4 vCPUs and 8-GB memory (referred to in this document as Advanced1)
 - 8 vCPUs and 16-GB memory (referred to in this document as Advanced2)

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

Figure 22: Add Storage

▼ Network settings Info					
/PC - required Info					
vpc			•	C	
Subnet Info					
		eV			
subnet-					
subnet- VPC: vpc-02	Owner: 199547563901		•	C	Create new subnet 🗹

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

L

Figure 23: Configure Storage

▼ Configure storage Info	Advanced
1x 120 GiB gp2 Root volume (Encrypted) Add new volume 	
0 x File systems	Edit

- **Step 10** Configure a security group by following these steps:
 - a) Create a new security group or modify an existing one by clicking the respective radio button.

aws	Services Q Search [Option:	+S]
=	▼ Network settings Info	Edit
	Network Info vpc Not used - default	
	Subnet Info	
	No preference (Default subnet in any availability zone)	
	Auto-assign public IP Info Enable	
	Firewall (security groups) Info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific instance.	traffic to reach your
	Create security group	
	Security groups Info	
	Select security groups	Compare security
	launch-wizard-69 sg-C ' X VPC: vpc	group rules

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

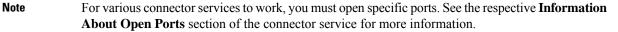
Figure 25: Configure These Inbound Rules Permitting Traffic to Specific Ports

ound rules					C Manage tags	Edit inbound rules
Name	∇	Security group rule ∇	IP version	⊽ Туре	▽ Protocol	
-		sgr-0497e0b5ee57ae7	IPv4	HTTPS	ТСР	443
-		sgr-0b120f3989c477140	IPv4	Custom UDP	UDP	2003
-		sgr-084f5c1391adb52fa	IPv4	Custom TCP	TCP	8000
-		sgr-02070569e30bbd	IPv4	Custom UDP	UDP	161
-		sgr-0bb0c8051cee0daf8	IPv4	SSH	TCP	22
-		sgr-0c502fa77173670d8	IPv4	Custom TCP	TCP	8004

- **Note** Using an inbound rule, you can also specify the network subnet range that can access this instance (For example, through SSH).
- c) Configure the outbound rule shown in the following image.

Figure 26: Configure This Outbound Rule

Inbound rules	Outbound rules Ta	gs			
 You can now 	v check network connectivity w	ith Reachability Analyzer		Run Reac	hability Analyzer 🛛 🗙
Outbound ru				C Manage tags	Edit outbound rules
IP version	⊽ Туре	▼ Protocol	▽ Port range	▽ Destination	
IPv4	All traffic	All	All	0.0.0/0	-



- **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.

aws	Services ~ F	Resource Group	s v - 1k	۵	samkhand 👻	N. Virginia 👻	Support 👻
-9	2. Choose Instance Type Review Instance	e Launch	tance 4. Add Storage 5. Add Tags 6. Configure Security Oncup 7, Review				
Туре 🕕		Protoco		D	escription (i)		
HTTP		TCP	Select an existing key pair or create a new key pair ×				
HTTP		TCP		12			
Custom	TCP Rule	TCP	A key pair consists of a public key that AWS stores, and a private key file that you store. Together,				
Custom	TCP Rule	TCP	they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to				
Custom	TCP Rule	TCP	securely SSH into your instance.				
Custom	TCP Rule	TCP					
SSH		TCP	Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.				
SSH		TCP					
HTTPS		TCP	Create a new key pair V Key pair name				
HTTPS		TCP	Key1				
AILICMP	- IPv4	All	Download Key Pair				
AILICMP	- IPv4	All					
InstanceStorage	Details		You have to download the private key file (* per file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created. Cancel Launch Instances			Edit	instance details Edit storage
Tags							Edit tags
				_		Cancel Prev	rious Launch

Figure 27: Create a New Key Pair

Figure 28: Choose an Existing Key Pair

ose AMI 2. Choose Instance 7: Review Instan				
selected security groups i				
ype (i)	Protoco		Description (i)	
ITTP	TCP	Select an existing key pair or create a new key pair ×		
ITTP	TCP			
sustom TCP Rule	TCP	A key pair consists of a public key that AWS stores, and a private key file that you store. Together,		
ustom TCP Rule	TCP	they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to		
ustom TCP Rule	TCP	securely SSH into your instance.		
ustom TCP Rule	TCP			
SH	TCP	Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.		
SH	TCP	Choose an existing key pair		
TTPS	TCP	Select a key pair		
TTPS	TCP	ConnectorAMI		
II ICMP - IPv4	All	I acknowledge that I have access to the selected private key file (ConnectorAMI.pem), and		
II ICMP - IPv4	All	that without this file, I won't be able to log into my instance.		
tance Details		Cancel Launch Instances		Edit instance det
brage				Edit stor
Jiago				Lon oron

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

Number of instances	nfo
1	
Software Image (AMI)	
cisco-dna-spaces-conn ami-0ff155022ef237286	ector3-b8read more
Virtual server type (ins	tance type)
t2.medium	
Firewall (security group	n)
	<i>c)</i>
eWLC	5)
eWLC Storage (volumes)	5)
eWLC Storage (volumes)	, ,
eWLC Storage (volumes) 1 volume(s) - 120 GiB	
eWLC Storage (volumes)	first year includes 750 🛛 🗙
eWLC Storage (volumes) 1 volume(s) - 120 GiB Free tier: In your f hours of t2.micro Regions in which t	first year includes 750 X (or t3.micro in the :2.micro is unavailable)
eWLC Storage (volumes) 1 volume(s) - 120 GiB Free tier: In your f hours of t2.micro Regions in which t instance usage on	first year includes 750 X (or t3.micro in the :2.micro is unavailable) free tier AMIs per
eWLC Storage (volumes) 1 volume(s) - 120 GiB Free tier: In your f hours of t2.micro Regions in which t instance usage on month, 30 GiB of	first year includes 750 X (or t3.micro in the :2.micro is unavailable) free tier AMIs per EBS storage, 2 million
eWLC Storage (volumes) 1 volume(s) - 120 GiB Free tier: In your f hours of t2.micro Regions in which t instance usage on month, 30 GiB of	first year includes 750 X (or t3.micro in the :2.micro is unavailable) free tier AMIs per EBS storage, 2 million chots, and 100 GB of

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

Services Q. Search	[Option+S]	▶ 🐥 ° ⑦ N. Virginia 🕶
Instances (1/1) Info		C Connect Instance state ▼ Actions ▼ Launch instances
Q. Find instance by attribute or tag (case-sensitive)		< 1 >
Instance ID = i-094538a13d1d19edf X Clear filters		
Name V Instance I	D Instance state ▼ Instance type ▼ Status check	ck Alarm status Availability Zone ⊽ Public IPv4 DNS ⊽ Public
		cks passed No alarms + us-east-1f :
	=	
Instance: i-094538a13d1d19edf (Connector3-AMI-Dev-		6
Details Security Networking Storage Status che	cks Monitoring Tags	
▼ Instance summary Info		
Instance ID	Public IPv4 address	Private IPv4 addresses
i-094538a13d1d19edf (Connector3-AMI-Dev-Instance-1)	🗗 open address 🗹	D.
IPv6 address	Instance state	Public IPv4 DNS
-		🗇 ex 🛛 open address 🗹
Hostname type	Private IP DNS name (IPv4 only)	
IP name: ternal	🗇 ip- nternal	
Answer private resource DNS name	Instance type	Elastic IP addresses
IPv4 (A)	t2.medium	-
Auto-assigned IP address	VPC ID	AWS Compute Optimizer finding
	🗇 (lt) 🖸	Opt-in to AWS Compute Optimizer for recommendations. Learn more 🗠
D Public IP]		
IAM Role	Subnet ID	Auto Scaling Group name
	Subnet ID	Auto Scaling Group name -
IAM Role		
IAM Role Instance details Info Platform	AM ID	Monitoring
MA Role − ▼ Instance details info	Ø Z	-
IAM Role Instance details Info Platform	AM ID	Monitoring

- **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.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.



Cisco Spaces: Connector: Azure VMware

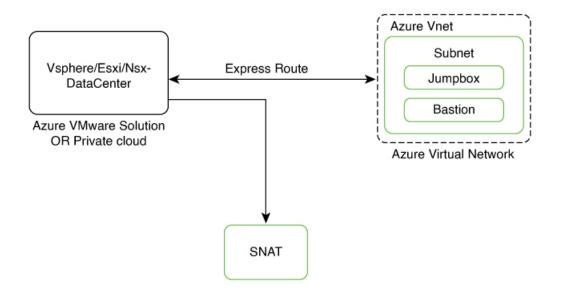
Cisco Spaces: Connector: Azure VMware, on page 33

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

		and docs (G+/)			କୁ ଦ 🐵 🔊 ନି
Home > Create a resource	>				
Marketplace					
Get Started		×	Publisher name : All × Product 1	ype : All × Publisher Type : All	X Operating System : All X
Service Providers	y alloc minute solution			permit X	operating system . Mill A
Al-powered search	Azure benefit eligible only ①	Azure services only			
Management	Showing 1 to 20 of 62 results for 'azi	ure vmware solution'. <u>Clear search</u>			
Private Marketplace	•	Constanting and the second sec	RUN NSX	veloCibud vmvare	$\overline{\mathbf{O}}$
Private Offer Management	Azure VMware Solution	VMware Site Recovery Manager (SRM)	VMware NSX Cloud	VMware SD-WAN in vWAN	VMware ESXi
My Marketplace	Microsoft	VMware Inc.	VMware Inc.	VeloCloud	Microsoft Sentinel, Microsoft Co
	Azure Service	SaaS	SaaS	Azure Application	Azure Application
Favorites	Azure VMware Solution (AVS)	The industry-leading disaster	Consistent Networking and Security	VMware SD-WAN managed	VMware ESXi
My solutions	combines the VMware Software Defined Data Center (SDDC) with	recovery management solution.	for Applications Running Natively in Azure	application for Virtual WAN	
Recently created	Microsoft Azure Cloud bare-metal				
Private plans	infrastructure. This service enables	Starts at Free	Starts at Free	Starts at Free	Price varies
Categories	Create 🗸 🛇	Subscribe 🗸 🛇	Subscribe 🗸 🛇	Create 🗸 🛇	Create \lor
Compute (24)	сф.		(RUN NSX)		(RUN)
Security (23)	_	5	\bigcirc	\bigcirc	\smile
Storage (21)	App Volumes: Apps on Demand	Azure Backup (Preview)	VMware NSX - Cloud Service Manager	VMware NSX - Policy Manager	VMware NSX - Public Cloud Gateway
IT & Management Tools (17)	VMware Inc.	Microsoft Corporation	VMware Inc.	VMware Inc.	VMware Inc.

Step 3 Choose the Azure VMware Solution service.

- a) In the Search services and marketplace field, search for an Azure VMware solution.
- b) From the displayed search results, click Create and choose the Azure VMware solution.
- **Step 4** In the **Create a private cloud** window that appears, fill the required details.
 - a) Choose a subscription.
 - b) Choose a resource group or create a new one.
 - c) Choose the location of the service.
 - d) Choose the size of the host.
 - e) Choose the host location.

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

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

Figure 33: Create a private cloud

Home > Create a resource > Mark	etplace >	
Create a private clou	d	
Prerequisities Basics Tag	s Review and Create	
Project details		
Subscription *	VM-Deployment	\sim
Resource group * ()	Vmware-us-east2	\sim
	Create new	

Figure 34: Create a private cloud

	arch resources, services, and docs (G+/)	
Home > Create a resource > Marketp		
Create a private cloud		
Private cloud details	*	
Resource name * ①	Enter the name	
Location * ①	(US) East US 2	
Size of host * (i)	V	
Host location *	 All hosts in one availability zone 	
	O Hosts in two availability zones Hosts will be equally divided across 2 availability zones. Since there will be two availability zones, the number of hosts you can select are in multiples of 2 only.	
Number of hosts ①	Find out how many hosts you need If you need more hosts, request a quota increase	
CIDR address block		
Provide IP address for private cloud for o other Azure vnets or on-premise networ	luster management. Make sure these are unique and do not overlap with any ks.	
Address block for private cloud * 🕕	Enter an address block	
	The address block must fall within the following allowed network blocks: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	
	The address block cannot overlap any of the following restricted network blocks: 172.17.0.0/16	
	The address block cannot be smaller than a /22 network.	

- **Step 5** Configure a segment for the private cloud.
 - a) From the private-cloud left pane, click **Segments**. You can see that a default segment has already been created and allocated with addresses from the address range specified by you earlier. You can use this existing segment or create a new one.

Figure 35: Create a Segment

≡ Microsoft Azure 🔎 Se	arch resources, services, and docs (G+/)				
Home > Create a resource > Market	blace >				
Create a private cloud					
Private cloud details	x				
Resource name * (i)	Enter the name				
Location * ①	(US) East US 2 V				
Size of host * ①					
Host location *	All hosts in one availability zone				
nostiocation	Hosts in two availability zones Hosts will be equally divided across 2 availability zones. Since there will be two availability zones, the number of hosts you can select are in multiples of 2 only.				
Number of hosts ①	Find out how many hosts you need If you need more hosts, request a quota increase				
CIDR address block					
Provide IP address for private cloud for other Azure vnets or on-premise netwo	cluster management. Make sure these are unique and do not overlap with any ks.				
Address block for private cloud * ①	Enter an address block				
	The address block must fall within the following allowed network blocks: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16				
	The address block cannot overlap any of the following restricted network blocks: 172.17.0.0/16				
	 The address block cannot be smaller than a /22 network. 				
Review and Create Pre-	rious Next : Tags >				

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.

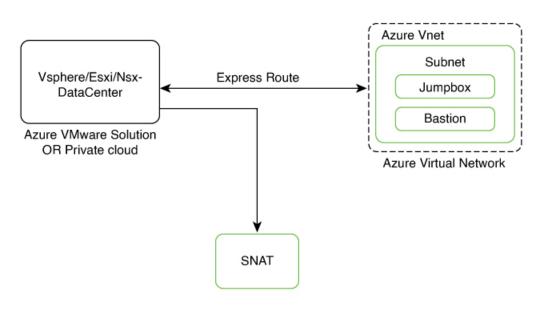


Figure 36: Various Components to InstallConnector onAzure VMware

Figure 37: VMware Credentials

≡ Microsoft Azure 👂	Search resources, services, and docs (G+/)		۶.	Ģ	۲	0	8	avitiwar@cisco.com
Home > Vmware-us-east2	2 VMware credentials *							×
Search Manage	« vCenter Server credentials							
👷 Connectivity	Web client URL 🕕	https://10.0.0.2/						
 Clusters Encryption 	Certificate thumbprint ①	BDF72B14F378C2ACD5B4B62200B71E7F4FD49C0D						
VMware credentials	Username 🕕	cloudadmin@vsphere.local						
📍 Identity	Password ()	·						
Storage	Password ()							
Placement policies		Generate a new password						
+ Add-ons								
Workload networking	NSX-T Manager credentials							
4 Segments	Web client URL 🕕	https://10.0.3/	1					
 DHCP Port mirroring 	Certificate thumbprint ①	B028477B779C37AEFA7554A45D54958D9CFA5C36						
DNS	Username 🛈	cloudadmin 🗈	1					
Internet connectivity	Password ①	·						
Operations	- assisted ()	L						
Run command		Generate a new password						
Azure hybrid benefit								
Monitoring								

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.

I

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

\equiv Microsoft Azure	≫ Search resources, services, and docs (G+/)
Home > ExpressRoute circuits Create ExpressRout	
Use Azure ExpressRoute to creatin a colocation environment. Est	
Project details	
Select the subscription to manage manage all your resources.	ge deployed resources and costs. Use resource groups like folders to organize and
Subscription * ①	VM-Deployment V
Resource group * ①	Vmware-us-east2 V Create new
Instance details	
Region * ①	East US 2 V
Name * 🛈	test1
	*
Previous Next	Review + create

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

Figure 39: Configuration Tab

Create ExpressRoute	
ExpressRoute circuits can connect to Azu Learn more about circuit types	re through a service provider or directly to Azure at a global peering location.
Port type * 🕕	Provider
	◯ Direct
Create new or import from classic * ①	Create new
	O Import
Provider * 🕕	InterCloud for Azure
Peering location * ①	Chicago
Bandwidth * ①	50Mbps V
	▲ Downgrading the bandwidth of a circuit is not supported. Carefully choose a bandwidth that matches your needs, overutilization causes degradation in performance. Learn More [©]
SKU * 🕕	Standard
	O Premium
	To use the Local SKU option, the selected bandwidth must be at least 1Gbps.
Billing model * 🕕	Metered
Allow classic operations 🕕	○ Yes
	No
Previous Next Revie	w + create

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

L

Figure 40: Review + Create

Create ExpressRoute	
Running final validation	
Basics Configuration Tags	Review + create
Basics	
Subscription	VM-Deployment
Resource group	Vmware-us-east2
Region	East US 2
Name	test1
Configuration	
Port type	Provider
Create new or import from classic	Create new
Provider	InterCloud for Azure
Peering location	Chicago
Bandwidth	50Mbps
SKU	Standard
Billing model	Metered
Allow classic operations	No

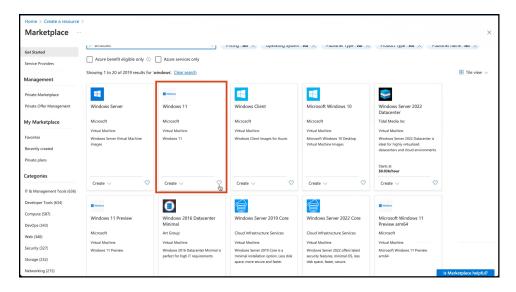
Step 2 From the created Virtual Network, do the following.

- a) Create a Gateway subnet and provide an IP address.
- b) Create a Bastion and provide an IP address.
- c) Create an AzureBastion subnet and provide an IP address.

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

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

Figure 41: Windows 11 virtual machine



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

Figure 42: Create a Virtual Machine

😑 Microsoft Azure 🔎 Sea	rch resources, services, and docs (G+/)		2	Ģ	Q	۲	0	R	avitiwar@cisco.com
Home > Create a resource > Marketpl									×
Basics Disks Networking Management Monitoring Advanced Tags Review + create									
image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more d ²									
Project details Select the subscription to manage deploy your resources.	ed resources and costs. Use resource groups like folders to organize and manage all								
Subscription * ①	VM-Deployment V								
Resource group * ①	(New) Resource group V Create new								
Instance details									
Virtual machine name * 🕕									
Region * 🛈	(US) East US 2 V								
Availability options	Availability zone								
Availability zone * 💿	Zones 1 V								
	You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more [™]								
Security type ①	Trusted launch virtual machines								
	Configure security features								
Review + create < Pre	vious Next : Disks >								R Give feedback

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

≡ Microsoft Azure 👂 Se	earch resources, services, and docs (G+/)			Ģ	Φ	۲	0	R	avitiwar@cisco.com
Home > Vmware-us-east2									
Vmware-us-east2 Azure VMware Solution private cloud	VMware credentials *								×
Manage	vCenter Server credentials								
e Connectivity	Web client URL ()	https://10.0.2/							
Clusters	Certificate thumbprint ①	BDF72814F378C2ACD584B62200B71E7F4FD49C0D							
Encryption									
VMware credentials Identity	Username 🛈	cloudadmin@vsphere.local							
Storage	Password ()	·····							
Recement policies		Generate a new password							
+ Add-ons									
Workload networking	NSX-T Manager credentials								
i Segments	Web client URL ①	https://10.0.3/	٦.						
DHCP Port mirroring	Certificate thumbprint ()	B0284778779C37AEFA7554A45D54958D9CFA5C36							
 Port mirroring DNS 			-						
Internet connectivity	Username 🛈	cloudadmin							
Operations	Password 🕠	······							
Run command		Generate a new password							
📮 Azure hybrid benefit									
Monitoring									

Figure 44: VMware Credentials

← C ▲ Not secure https://10.0.0.2/ui/app/host	:nav=h/urn:vr		1891-9ee0f043eea7/sumr	mary 🗔 🎛 🗛 🖒	🕥 ጦ 🕼 🖗 🗞	🐮 💋
😑 vSphere Client 🔍		3 ESXi Hosts				© 0~
VSpitere Client VSpitere Client VSpitere Client Vstatement Vstatement	SI ary Monitor Hypervis Mode: Process Logical F NiCs: Virtual M State: Uptime:	Configure Permission sor: VMware ESXi, PowerEdge Ré processors: 72 4	7.0.3, 21313628		ACTIONS CV Use 20:12:044 Memory Uses 10:33:68 Uses 3:53:18 Uses 3:53:18	Tree 62.62 Orie Capacity 63.33 Orie Tree 665.03 OB Capacity 786.82 OB Free 62.63 TB Capacity 82.4 TB
			No lease to disalar			
Recent Tasks Alarms			No items to display			

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

I



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

•	-		
\equiv 1. Select	an OVF template	:	×
Select an OVF ter	nplate from remote URL or local file system		
Enter a URL to do	wnload and install the OVF package from the Internet, or browse to a location a	ccessible from your computer, s	such
as a local hard dri	ve, a network share, or a CD/DVD drive.		
OURL			
http https://	remoteserver-address/filetodeploy.ovf .ova		
Local file UPLOAD FILES	cisco-dna-spaces-connector30-june2022-la51.ova		
		CANCEL NEXT	

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

\equiv 2. Select a nar	ne and folder		×
Specify a unique name and	arget location		1
Virtual machine name:	cisco-dna-spaces-connector-30		
Select a location for the virte	ual machine.		
∨ 🗗 10.22.244.96			
> 🗊 SJC-20			
		CANCEL BACK	NEXT

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

elect the destination o	compute resource for this operation		
	oonding)		
ompatibility	cks succeeded.		

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

Figure 48: 4. Review Details

= 4. Review detail	s ×
Verify the template details.	
Publisher	No certificate present
Product	Cisco DNA Spaces Connector
Version	1
Vendor	Cisco Systems Inc.
Download size	1.5 GB
Size on disk	Unknown (thin provisioned) 120.0 GB (thick provisioned)
	CANCEL BACK NEXT

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

Ve will reserve part of the resource	s of CPU and memory	based on your OV	/A selection.	
itandard Connector:				
vCPUs. 2000 Mhz will be reserved				
GB Memory. 4GB will be reserved.				
Advanced1 Connector:				
vCPUs. 4000 Mhz will be reserved				
GB Memory. 8GB will be reserved.				
Advanced2 Connector:				
vCPUs. 8000 Mhz will be reserved				
6 GB Memory. 16GB will be reserved	1.			
	Scroll do	wn to		
	accept the	license		
	agreem			

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

Elect the storage for the contract the storage for the contract this virtual mach	nine (Requires Key	Management Ser				
ielect virtual disk format /M Storage Policy			e Default	~		
Disable Storage DRS for	Storage Compatibility	e Capacity T	Provisioned T	Free T	Туре Т	Cluster
💿 📋 datastore1 (1		5.44 TB	4.58 TB	1,014.88 GB	VMFS 6	
						1 item
Compatibility						

Step 10

I0 In the 8. Select networks window, choose a destination network, and click Next.

Figure 51: 8. Select Networks

8. Select networks Select a destination network for each source network.	×
Source Network	Destination Network
NAT	VM Network V
	1 item
IP Allocation Settings	
IP allocation:	Static - Manual
IP protocol:	IPv4
	CANCEL BACK NEXT

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

Figure 52: 9. Ready to Complete

≡ 9. Ready to Review your selections	complete before finishing the wizard		×
\checkmark Select a name and	folder		
Name	cisco-dna-spaces-connector-30		
Template name	cisco-dna-spaces-connector		
Folder	SJC-20		
✓ Select a compute r	esource		
Resource	10.22.244.92		
\checkmark Review details			
Download size	1.5 GB		
		CANCEL	ACK FINISH

 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

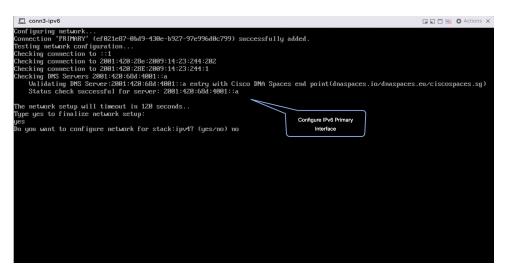
For the first login Login as username: root password: root localhost login: _	

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

Timezone setup Wauld you like to setup timezone? (blank for default value (UTC)) yes 1. Arisia - Press 1 2. America - Press 2 3. Amia - Press 3 4. America/Buenos Aires - Press 1 2. America/Buenos Aires - Press 1 2. America/Buenos Aires - Press 1 2. America/Buenos Aires - Press 2 3. America/Buenos Aires - Press 3 4. America/Buenos Aires - Press 5 5. America/Buenos - Press 5 5. America/Buenos - Press 6 7. America/Buenos - Press 7 8. America/Buenos - Press 1 11. America/Buenix - Press 1 12. America/Buenix - Press 1 13. America/Buenix - Press 1 14. America/Buenix - Press 1 15. America/Buenix - Press 1 16. America/Buenix - Press 1 17. America/Buenix - Press 1 18. America/Buenix - Press 1 19. America/Buenix - Press 1 10. America/Buenix - Press 1 11. America/Buenix - Press 1 13. America/Buenix - Press 1 14. America/Buenix - Press 1 15. Berting timezone and restarting services	9	
<pre>Would you like to setup timezone? (blank for default value (UTC)) yes 1. Africa - Press 1 2. America - Press 1 3. Asia - Press 2 3. Asia - Press 3 4. Australia - Press 4 5. Europe - Press 5 Select an option from the list above: (blank for default (Default value is 2)) 2</pre>		
<pre>Would you like to setup timezone? (blank for default value (UTC)) yes 1. Africa - Press 1 2. America - Press 1 3. Asia - Press 2 3. Asia - Press 3 4. Australia - Press 4 5. Europe - Press 5 Select an option from the list above: (blank for default (Default value is 2)) 2</pre>		Timezone setup
<pre>ges 1. Africa - Press 1 2. America - Press 2 3. Asia - Press 3 4. Australia - Press 4 5. Europe - Press 5 Select an option From the list above: (blank for default (Default value is 2)) 2 1. America/Anchorage - Press 1 2. America/Henors, Aires - Press 2 3. America/Neuros, Aires - Press 3 4. America/Neuros - Press 4 5. America/Neuros - Press 5 6. America/Neuros - Press 5 7. America/Neuros - Press 7 8. America/Neuros - Press 7 8. America/Neuros - Press 8 9. America/Neuros - Press 18 11. America/Nacial Jone - Press 18 11. America/Nacial Lago - Press 18 11. America/Nacial Lago - Press 12 13. America/Neuron - Press 12 13. America/Neuron - Press 13 13. America/Neuron - Press 13 13. America/Neuron - Press 14 13. America/Neuron - Press 15 13. America/Neuron - Press 12 13. America/Neuron - Press 13 13. America/Neuron - Press 14 14. America/Neuron - Press 15 15. Setting timezone and restarting services</pre>		
<pre>1. Affrica - Press 1 2. America - Press 2 3. Asia - Press 3 4. Australia - Press 4 5. Europe - Press 5 Select an option from the list above: (blank for default (Default value is 2)) 2 1. America/Anchorage - Press 1 2. America/Anchorage - Press 2 3. America/Ancorage - Press 4 5. America/Ancorage - Press 4 5. America/Ancorage - Press 5 6. America/Ancorage - Press 5 7. America/Ancorage - Press 6 7. America/Ancorage - Press 1 9. America/Ancorage - Press 1 11. America/Sanitago - Press 1 12. America/Ancorage - Press 1 13. America/Ancorage - Press 1 14. America/Sanitago - Press 1 15. America/Ancorage - Press 1 16. America/Ancorage - Press 1 17. America/Ancorage - Press 1 18. America/Ancorage - Press 1 19. America/Ancorage - Press 1 10. America/Ancorage - Press 1 11. Select an option form the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services</pre>		
3. Asia - Press 3 4. Australia - Press 4 5. Europe - Press 5 Select an option from the list above: (blank for default (Default value is 2)) 2 1. America/Anencos, Alres - Press 1 2. America/Anencos, Alres - Press 2 3. America/Anencos, Press 3 4. America/Anencos, Press 5 5. America/Anencos, Press 5 5. America/Anencos, Press 5 6. America/Anencos, Press 6 7. America/Anenix - Press 6 9. America/Anenix - Press 9 10. America/Segina - Press 10 11. America/Sanitago - Press 12 13. America/Anenoty - Press 12 13. America/Anenoty - Press 12 13. America/Anenoty - Press 12 13. America/Information - Press 12 14. America/Information - Press 12 15. Selting timezone and restarting services		
3. Asia - Press 3 4. Australia - Press 4 5. Europe - Press 5 Select an option from the list above: (blank for default (Default value is 2)) 2 1. America/Aucons_Aires - Press 1 2. America/Aucons_Aires - Press 2 3. America/Aucons_Aires - Press 2 4. America/Aucons_Aires - Press 5 5. America/Auconstrong - Press 5 6. America/Auconstrong - Press 6 7. America/Auconstrong - Press 6 9. America/Auconstrong - Press 10 11. America/Auconstrong - Press 10 11. America/Auconstrong - Press 12 13. America/Auconstrong - Press 12 14. America/Auconstrong - Press 12 15. America/Auconstrong - Press 12 16. America/Auconstrong - Press 12 17. America/Auconstrong - Press 12 18. America/Auconstrong - Press 12 19. America/Auconstrong - Press 12 19. America/Auconstrong - Press 12 19. America/Auconstrong - Press 12 10. America/Auconstrong - Press 12 10. America/Auconstrong - Press 12 11. America/Auconstrong - Press 12 12. America/Auconstrong - Press 12 13. America/Auconstrong - Press 12 14. America/Auconstrong - Press 12 15. America/Auconstrong - Press 12 15. America/Auconstrong - Press 12 16. America/Auconstrong - Press 12 17. America/Auconstrong - Press 12 18. America/Auconstrong - Press 12 19. America/Auconstrong - Press 12 19. America/Auconstrong - Press 12 19. America/Auconstrong - Press 12 19. America/Auconstron		2. America - Press 2
5. Europe - Press 5 Select an option from the list above: (blank for default (Default value is 2)) 2 1. America/Aucnos Aires - Press 1 2. America/Aucnos Aires - Press 2 3. America/Aucnos Aires - Press 3 4. America/Aucnos - Press 3 5. America/Aucnos - Press 5 6. America/Aucnos - City - Press 6 7. America/Aucnos - Press 10 9. America/Aucnos - Press 10 11. America/Aucnos - Press 12 12. America/Aucnos - Press 12 13. America/Aucnos - Press 12 13. America/Aucnos - Press 12 13. America/Aucnos - Press 13 Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		3. Asia - Press 3
5. Europe - Press 5 Select an option from the list above: (blank for default (Default value is 2)) 2 1. America/Ahenos Aires - Press 1 2. America/Ahenos Aires - Press 2 3. America/Ahenos - Press 3 4. America/Ahenos - Press 3 5. America/Ahenos - City - Press 6 7. America/Ahenos - City - Press 6 9. America/Ahenos - Press 10 11. America/Bay - Press 10 11. America/Ahenos - Press 11 12. America/Ahenos - Press 12 13. America/Ahenos - Press 12 13. America/Ahenos - Press 12 3. City - Press 13 3. City - Press 13 3. City - Press 13 3. City - Press 13 3. City - Press 14 3. City - Press 12 3. City - Press 14 3. City - Press 12 3. City - Press 14 3. City - City - City - Press 14 3. City - City - City - Press 14 3. City - Ci		4. Australia - Press 4
Select an option from the list above: (blank for default (Default value is 2)) 2 2 3. America/hencorage - Press 1 3. America/Chicago - Press 2 3. America/Chicago - Press 3 4. America/Chicago - Press 4 5. America/America/Techicago - Press 5 6. America/America/Techicago - Press 5 7. America/America/Techicago - Press 10 11. America/America/Techicago - Press 10 11. America/America - Press 11 12. America/America - Press 12 13. America/America - Press 13 13. America/America - Press 13 13. Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		
2 1. America/Anchorage - Press 1 2. America/Buenos,Aires - Press 2 3. America/Buenos, Aires - Press 2 4. America/Buenos - Press 3 5. America/Buelos - Press 6 6. America/Buelos - Press 7 8. America/Buelos - Press 7 9. America/Buelos - Press 10 11. America/Buelos - Press 11 12. America/Buelos - Press 11 13. America/Buelos - Press 13 3. Select an option From the list above: (blank for default (Default value is 1)) 5. Setting timezone and restarting services		
2. America/Dirago - Press 2 3. America/Dirago - Press 3 4. America/Danwer - Press 4 5. America/Danmyeles - Press 5 6. America/Danmyeles - Press 5 7. America/Danmix - Press 7 8. America/Phornix - Press 7 9. America/Phornix - Press 9 10. America/Santiago - Press 10 11. America/Santiago - Press 11 12. America/Danlo - Press 11 12. America/Danlo - Press 13 3. Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		
 3. America/Brouge - Press 3 4. America/Brouve - Press 4 5. America/Brouve - Press 4 5. America/Brouve City - Press 5 6. America/Hourge City - Press 6 7. America/Hourge - Press 9 9. America/Regima - Press 9 10. America/Bag - Press 10 11. America/Bag - Press 11 12. America/America - Press 12 13. America/America - Press 13 Scletct an option from the list above: (blank for default (Default value is 1)) 5 Sctting timezome and restarting services 		1. America/Anchorage - Press 1
 3. America/Dense; Press 3 4. America/Dense; Press 3 5. America/Dense; Press 5 6. America/Dense; City - Press 6 7. America/Mexico_City - Press 7 8. America/Mexico_Press 7 9. America/Mexico - Press 10 10. America/Ango: Press 11 11. America/Ancouver - Press 12 13. America/Ancouver - Press 13 3. Gelect an option from the list above: (blank for default (Default value is 1)) 5. 3. Setting timezone and restarting services 		2. America/Buenos Aires - Press 2
 5. America.ch.co.Anageles - Press 5 6. America.ch.co.City - Press 6 7. America.ch.co.City - Press 7 8. America.ch.co.city - Press 8 9. America.ch.co.city - Press 9 10. America.ch.co.city - Press 11 11. America.ch.co.city - Press 12 13. America.ch.co.co.city - Press 13 Scletc: an option from the list above: (blank for default (Default value is 1)) 5 Scitting timezone and restarting services 		
6. America/Hexico_City - Press 6 7. America/Hexico_City - Press 7 8. America/Hexico Press 9 9. America/Repina - Press 9 10. America/Santiago - Press 10 11. America/Santiago - Press 11 12. America/Socota - Press 12 13. America/Socota - Press 13 Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		4. America/Denver - Press 4
 ?. mmerica/Homix - Press ? 0. mmerica/Regima - Press 0 9. mmerica/Regima - Press 10 10. mmerica/Sau_Faulo - Press 11 11. mmerica/Sau_Faulo - Press 12 13. mmerica/Vancouver - Press 13 Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services 		5. America/Los_Angeles - Press 5
7. America/Homix - Press 7 0. America/Homix - Press 7 9. America/Rogina - Press 9 10. America/SaujPaulo - Press 10 11. America/SaujPaulo - Press 11 12. America/Vancauce - Press 12 13. America/Vancauce - Press 12 13. Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		6. America/Mexico Citu - Press 6
9. America/Beglina - Press 9 10. America/Sau Jaulo - Press 10 11. America/Sau Jaulo - Press 11 12. America/Toronto - Press 12 13. America/Vancouver - Press 13 Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		
18. America/Santiago - Press 19 11. America/Santiago - Press 11 12. America/Toronto - Press 12 13. America/Monouver - Press 13 Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		8. America/Phoenix - Press 8
11. America/Sao_Faulo - Press 11 12. America/Toronto - Press 12 13. America/Mancauver - Press 13 Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		9. America/Regina - Press 9
11. America/Sao Paulo – Press 11 12. America/Toronto – Press 12 13. America/America/America/Toress 13 Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		10. America/Santiago - Press 10
13. America/Jancouver - Press 13 Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		11. America/Sao Paulo - Press 11
Select an option from the list above: (blank for default (Default value is 1)) 5 Setting timezone and restarting services		12. America/Toronto - Press 12
5 Setting timezone and restarting services		13. America/Vancouver - Press 13
Setting timezone and restarting services		Select an option from the list above: (blank for default (Default value is 1))
		Setting timezone and restarting services

Figure 57: Configure NTP

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.

dualinterface-conn180	🖬 🖬 🖷 🎇 Actions 🚳
Configure NTP Enter comma separated NTP servers list (blank for no NTP server): ntp.esl.cisco.com Checking status for server: ntp.esl.cisco.com Status check successful for server: ntp.esl.cisco.com Anning: The unit file, source configuration file or drop-ins of chronyd.service changed on to reload units. NTP configuration: success	Configure NTP
Figure 58: Configure NTP	
Configure NTP	
Enter comma separated NTP servers list (blank for no NTP server): rtp5-b5-rt Checking status for server: rtp5-b5-rbb-ntp1-0.cisco.com	bb-ntp1-v6.cisco.com 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

Cisco Spaces Connector UI:	
https://10.22.244.180	
Username log in: spacesadmin	
The install is complete, a reboot will occ	cur in 5 seconds

Step 20In 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

cisco							
SPACES Connec	tor 3.1						Θ
🖄 Dashboard							
Configure Connector	Configure Token Without the token, the conne	ctor will not be able to start.					Configure Token ×
Configure HTTP proxy							
Privacy Settings		General Information	I.			Primary Interfa	ace
Manage API Keys		Connector Name	Not Available	HA Config Mode	Not VIP Paired	IP Address	10.89.45.92/24
	Connector 3.1	Tenant ID Connector ID	Not Available Not Available			MAC Address Gateway	00:50:56:47:54:C8
 Troubleshoot 	Hostrame compt	Instance ID	005056a754c8			DNS Server	
	Packaga connector3 p84	Praxy	00000000000			Domain	
	Show More	NTP Address	ntp.esl.cisco.com			IP Stack	ipu4
	0.00 800	NTP Status	active (running)				
	Health						
	Cloud Reachability	Connected	Memory Percentage Usage	11.1 % 🔘			
	CPU Percentage Usage	0.6% ①	Running Status	Up 🛈			
	Disk Percentage Usage	4.8 % ()	System Load Average	0 0			
	Disk Usage	4469.07 MB ①	Up time	5d 3h 32m 51s 🛈			
	Memory Usage	435.62 MB 🛈					
	Services C						
	Service Manager 🚔 a	3.1.0.92	¢	6 M			
	Up time	5d 3h 31m 9s 🛈					
	Control Channel	Down					
	CPU Usage (%)	0.33 % ()	Looking	for other services?			
	Memory Usage (%)	4.74 % ()	Follow step	is below to add services			
	Memory Usage	185.99 MB 🛈	(1) La	in to Cisco Spaces			
	Dick Lisage (N)	a ** @	Glo	at Mos Maspeces Johome			

Note

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

What to do next

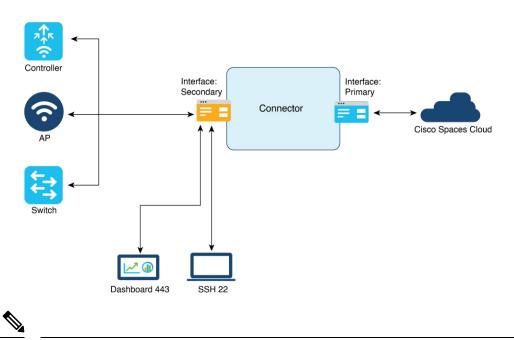
You can now Activating Connector 3 on Cisco Spaces.

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

1 New virtual machine		
New Virtual machine Solect creation type Solect OVF and VMDK files Solect storage License agreements Deployment options Additional settings Ready to complete	Select creation type How would you like to create a Virtual Machine? Create a new virtual machine Deploy a virtual machine from an OVF or OVA file Register an existing virtual machine	This option guides you through the process of creating a virtual machine from an OVF and VMDK files.
		Back Next Finish Cancel

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

🔁 New virtual machine - dualInterface	-conn180
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 	Select OVF and VMDK files Select the OVF and VMDK files or OVA for the VM you would like to deploy
4 License agreements	Enter a name for the virtual machine.
5 Deployment options 6 Additional settings	dualInterface-conn180
7 Ready to complete	Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.
vm ware [*]	× 📾 cisco-spaces-connector3-p84-apr2023.ova
	Back Next Finish Cancel

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

Figure 64: Select Storage

1 New virtual machine - dualInterface-	conn180					
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 4 License agreements 5 Deployment options 6 Additional settings 7 Ready to complete 	Select storage Select the storage type and datastore Standard Persistent Memory Select a datastore for the virtual machine's configuration files and all of its' virtual disks.					
	Name ~	Capacity ~	Free v	Туре	✓ Thin pro… ✓	Access ~
	datastore1	924 GB	837.1 GB	VMFS6	Supported	Single
						1 items
vm ware [.]						
			Ba	ack	Next Finis	h Cancel

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

Select creation type Select OVF and VMDK files Select storage	License agreements Read and accept the license agreements
License agreements	Accept Resource R
6 Ready to complete	We will reserve part of the resources of CPU and memory based on your OVA selection.
	Standard Connector: 2 vCPUs. 2000 MMz will be reserved. 4 GB Memory. 4GB will be reserved.
	Advancedi Connector: 4 vCPUs. 4000 MMz will be reserved. 8 GB Wemory. 8GB will be reserved.
	Advancedz Connector: 8 vCPUS. 8000 MP. will be reserved. 16 GB Memory. 16GB will be reserved.
	Standard (Dual Interface) Connector: 2 vCPUS. 2000 MNz will be reserved. 4 GB Memory. 4GB will be reserved. 2 WICs will be used.
	Advancedi (Dual Interface) Connector: 4 vCPUs. 4000 Mhz will be reserved. 8 GR Memory. SGR will be reserved
vm ware	I agree

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

Select creation type Select OVF and VMDK files Select storage	Deployment options Select deployment options		
 4 License agreements 5 Deployment options 6 Ready to complete 	Network mappings	PrimaryInterface VM Network SecondaryInterface vlan7-private-portGp	~
	Deployment type	Standard	~
		Standard Advanced1 Advanced2	be r
	Disk provisioning	Standard (Dual Interface) Advanced1 (Dual Interface)	
	Power on automatically	Advanced2 (Dual Interface)	
vm ware [®]			

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

Figure 67: Ready to complete

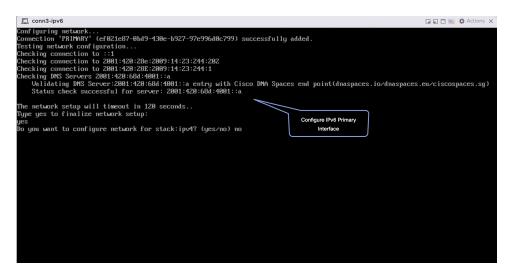
	Ready to complete Review your settings selection before finishing the wizard			
3 Select storage 4 License agreements 5 Deployment options	Product Cisco Spaces Connector			
S Deployment options G Ready to complete	VM Name	dualinterface-conn180		
	Files	cisco-spaces-connector-disk1.vmdk		
	Datastore	datastore1		
	Provisioning type	Thin		
	Network mappings	PrimaryInterface: VM Network,SecondaryInterface: vlan7-private-portGp		
	Guest OS Name	AlmaLinux-8.4 64-bit		
	Profile	The resources consumed by this configuration are: 2 vCPUs. 2000 Mhz will be re- erved. 4GB Memory. 4GB will be reserved. 2 NICs will be used.		
vm ware [*]	Do not refresh you	ur browser while this VM is being deployed.		

- **Step 9** Log in to the terminal and enter the default username **root** and default password **root**.
- **Step 10** Configure the host name for the connector.
- **Step 11** Choose an network interface to configure as PRIMARY.

Figure 68: Configuring the Primary Interface: IPv4

dualitieriace-contrao	Lat. But
Concer a metarrk interface as PRIMBUY from being that has connectivity to Circo Spaces Cironi. Mote: SCOUNDWY Interface can be configured using connectored: cli after completing configuration. Interface: msi2 - 0806(23938):40:07) Choose a metarrk interface [msi2 or emsi31: cmsi2 Sarting metarrk setty Denotes a metarrk setty [msi2] Denotes a metarrk setty [msi2] Denotes a metarrk setty [msi2] Denotes a metarrk settings configuration information for stack: Denote IP address formatted as: [mj/periii]. Denote: 152.081.524, 19.8.0.11/24: 1	Configure the public- facing interface (Primary)
Enter gateway:	
Enter search domain name:	
Confirm network settings? (yes/no) yes	

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

conn-3-244-99	
	Timezone setup Hould you like to setup timezone? (blank for default value (UTC))
	yes
	1. Africa - Press 1
	2. America - Press 2 3. Asia - Press 3
	5. Histo - Press 5 4. Australia - Press 4
	7. nustralia - Fress 5 5. Burope - Press 5
	5. Larope - Tress 5 Select an option from the list above: (blank for default (Default value is 2))
	1. America/Anchorage - Press 1
	2. America/Buenos_Aires - Press 2
	3. America/Chicago - Press 3
	1. America/Denver - Press 4
	5. America/Los_Angeles - Press 5
	6. America/Mexico_City - Press 6
	7. America/New_York - Press 7
	8. America/Phoenix - Press 8
	9. America/Regina - Press 9
	10. America/Santiago - Press 10
	11. America/Sao_Paulo - Press 11
	12. America/Toronto - Press 12
	 America/Vancouver - Press 13 Select an option from the list above: (blank for default (Default value is 1))
	Select an option from the first above. (blank for aerault (berault value is 1))
	Setting timezone and restarting services

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

Figure 71: Configure NTP

audinterface-conn180	G 🖸 🗆 📹 🏠 Actions 🕲
Configure NTP Enter comma separated NTP servers list (blank for no NTP server): ntp.esl.cisco.com Checking status for server: ntp.esl.cisco.com Status check successful for server: ntp.esl.cisco.com Amrning: The unit file, source configuration file or drop-ins of chronyd.service changed on to reload units.	Configure NTP
Figure 72: Configure NTP	

Configure NTP Enter comma separated NTP servers list (blank for no NTP server): rtp5-b5-rbb-nfp1-v6.cisco.com Checking status for server: rtp5-b5-rbb-ntp1-v6.cisco.com Status check successful for server: rtp5-b5-rbb-ntp1-v6.cisco.com NTP configuration: success

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

Figure 73: ConnectorGUI

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

- **Step 18** Wait for the completion of the reboot, and login as a **spacesadmin** user.
- Step 19 Configure the secondary interface using the **connectorctl network config** command

```
[spacesadmin@connector ~]$ connectorctl network config -p ipv4 -i 10.7.0.11/24 -g 10.7.0.1 -o
cisco.com -d 172.70.168.183 -n SECONDARY
Executing command:network
Command execution status:Success
------
Connection SECONDARY (5e970417-13b4-4ad8-af12-d125ce407c49) successfully added.
Network setup completed with given configuration.
Secondary interface - Added routes.
Secondary interface - Configured firewall zone.
System reboot will happen in 10 seconds. Do not execute any other command...
```

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

Interface - PRIMARY

Network configuration for stack:ipv4 Ip Address - 10.22.244.180/24 Mac Address - 00:0C:29:EE:24:8A

===========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

SPACES Conne	stor 3.1 https://connector-ip				Θ,
Image: Search of the search	Connector 3.1 Hostman Backaga connector3.984 Show More	General Information Connector Name Tenant ID Connector ID Instance ID Proxy NTP Address NTP Status	fastlocate-ha-cip 12212 46859829145890280000 000c294964cd Not Available ntp.est.cisco.com active (running)	HA Contig Mode HA VIP HA State HA Instance Channel Status HA Peer IP	VIP Paired 7.7.0.25 BACKUP UP 000c282a43o6 7.7.0.20
	Primary Interface IP Address 10.22.244.114/24 MAC Address 00.06.29.D6.E4.CD Gateway 10.22.244.1 DNS Server 171.70.168.183 Domain cisco.com IP Stack ipv4		IP Addr MAC Ac Gatewa DNS Se Dornain IP Stack	dress 00:0C:29:D6:E4:D7 / 7.7.0.1 ver 171.70.168.183 cisco.com	
	Health Cloud Reachability Con CPU Percentage Usage 6.1 f	nected % ①	Memory Percentage Usage Running Status	33 % () Up ()	

Note

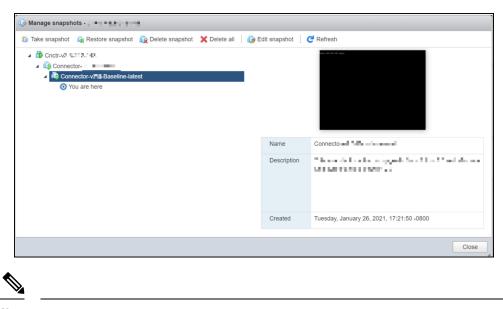
The root user is disabled and is used only for advanced troubleshooting by the Cisco Support team.

Using Snapshots for Backup

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

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

Figure 75: Backing Up Using a Snapshot



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



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

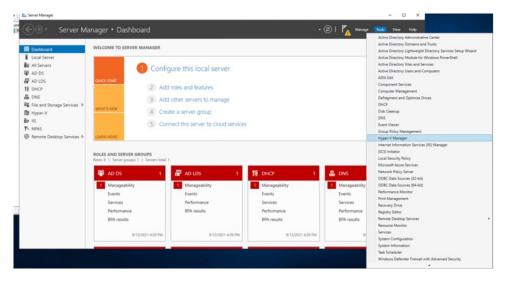
Creating a Virtual Switch

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

High Color St	erver Manager • Dashboard welcome to server manage	R		I Manage Tools View Add Roles and Features Remove Roles and Features Add Servers	
Local Server	1 Co	onfigure this local server		Add Servers Create Server Group Server Manager Propert	ies
AD LDS TE DHCP DHS DHS Ing File and Storage : Ing File and Storage Ing File and Storage Remote Desktop Remote Desktop	Services P 3 WHAT'S NEW 4	Add roles and features Add other servers to manage Create a server group Connect this server to cloud services		на	
	ROLES AND SERVER GROUPS Roles: 9 Server groups: 1 Servers	totak 1			
	AD DS Manageability Events Services Performance BPA results	1 Provide a constraint of the second	PhicP 1 Manageability Events Events Services Performance EPA results	DNS Manageability Events Services Performance EPA results	
	9/13/2021 5:09	PM 9/13/2021 5:09 PM	9/13/2021 5:09 PM	9/13/2521 5:09 PM	

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

Figure 78: Role-based or Feature-Based Installation

📥 Add Roles and Features Wizard		-		×
Select installation	type	DESTI WIN-NS0G6SB4GG3.r	NATION SER cdnlabcead.c	
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	 Select the installation type. You can install roles and features on a runni machine, or on an offline virtual hard disk (VHD). Role-based or feature-based installation Configure a single server by adding roles, role services, and features. Remote Desktop Services installation Install required roles services for Virtual Desktop Infrastructure (VDI) to r session-based desktop deployment. 			
	< Previous Next >	Install	Cance	:1

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

Figure 79: Select a Server From the Server Pool

Add Roles and Features Wizard				-		×
Select destination	n server		w	DESTIN /IN-NS0G6SB4GG3.rc	IATION SER	
Before You Begin Installation Type Server Selection		from the server pool	to install roles and feature:	5.		
Server Roles Features Confirmation Results	Server Pool Filter: Name WIN-NS0G6SB4G	IP Address iG3.rcd 10.31.103.2,16	Operating System Microsoft Windows Serv	ver 2019 Standard		
	and that have been	ervers that are running Win n added by using the Add S ers from which data collecti	dows Server 2012 or a new Servers command in Server on is still incomplete are no	Manager. Offline ot shown.		
		< Pre	vious Next >	Install	Cance	el

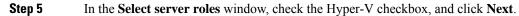


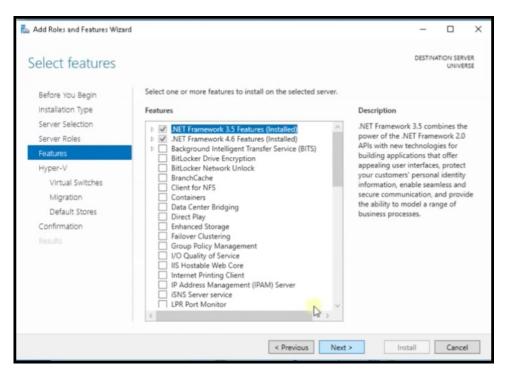
Figure 80: Select Server Roles

ᡖ Add Roles and Features Wiza	rd	- 🗆 X
Select server rol	es	DESTINATION SERVER UNIVERSE
Before You Begin Installation Type Server Selection Server Roles	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services	Description Active Directory Certificate Services (AD CS) is used to create certification authorities and related
Features Confirmation Results	Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Fax Server Fax Server MultPoint Services Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Windows Deployment Services V	role services that allow you to issue and manage certificates used in a variety of applications.
	< Previous Nex	Install Cancel



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

📥 Add Roles and Features Wizard			-		×
Create Virtual Sw Before You Begin Installation Type Server Selection Server Roles Features	Virtual machines require role, you can create virtu One virtual switch will be at least one virtual switch	virtual switches to communicate with other computers. al machines and attach them to a virtual switch. e created for each network adapter you select. We recon now to provide virtual machines with connectivity to a odify your virtual switches later by using the Virtual Swit	After you mend tha physical n	t you crea etwork. Y	RSE s ate
Hyper-V Virtual Switches	Name Ethernet	Description Realtek PCI GBE Family Controller			
Migration	Ethernet 2	Realtek PCIe GBE Family Controller			
Default Stores Confirmation Results		t you reserve one network adapter for remote access to not select it for use with a virtual switch.	this server	To reser	ye a
		< Previous Next >	stall	Cance	el

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

Figure 83: Use Credential Se	curity Support Provider
------------------------------	-------------------------

ᡖ Add Roles and Features Wizard	4	-		×
Virtual Machine I	Migration	DESTINA	ATION SERV UNIVER	
Before You Begin Installation Type Server Selection Server Roles Features Hyper-V Virtual Switches Migration Default Stores Confirmation Results	 Hyper-V can be configured to send and receive live migrations of virtual machine Configuring Hyper-V now enables any available network on this server to be used you want to dedicate specific networks for live migration, use Hyper-V settings at Allow this server to send and receive live migrations of virtual machines Allow this server to send and receive live migrations of virtual machines Authentication protocol Select the protocol you want to use to authenticate live migrations. Use Credential Security Support Provider (CredSSP) This protocol is less secure than Kerberos, but does not require you to set u delegation. To perform a live migration, you must be logged on to the sour Use Kerberos This protocol is more secure but requires you to set up constrained delegate environment to perform tasks such as live migration now. Instead, y server for live migration, including specifying networks, when you create the 	d for live n fter you in up constra ce server. tion in you erver remo	nigrations stall the r ined ur otely.	ole.
	< Previous Next > Inst	stall	Cance	4

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

🚡 Add Roles and Features Wizard	-		×
Default Stores	DEST	NATION SERV UNIVE	
Before You Begin Installation Type Server Selection Server Roles	Hyper-V uses default locations to store virtual hard disk files and virtual machine configu unless you specify different locations when you create the files. You can change these def now, or you can change them later by modifying Hyper-V settings. Default location for virtual hard disk files:		
Features	C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks	Brows	ie
Hyper-V	Default location for virtual machine configuration files:		
Virtual Switches	C:\ProgramData\Microsoft\Windows\Hyper-V	Brows	ie
Migration			
Default Stores			
Confirmation			
Results			
	< Previous Next > Install	Cance	:

Figure 84: Default Stores

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

Figure 85: Confirm the Installation Settings

📥 Add Roles and Features Wiza	rd – – >	ζ.
Confirm installat	tion selections Destination server Universe	
Before You Begin Installation Type Server Selection Server Roles Features	To install the following roles, role services, or features on selected server, click Install. Restart the destination server automatically if required Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.	
Hyper-V Virtual Switches Migration Default Stores	Hyper-V Remote Server Administration Tools Role Administration Tools Hyper-V Management Tools Hyper-V Module for Windows PowerShell	
Confirmation Results	Hyper-V GUI Management Tools	
	Export configuration settings Specify an alternate source path < Previous	1

Step 9 Open Hyper-V Manager.

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

Figure 86: Actions > Virtual Switch Manager

Myser V Manager Name Actions Name State CPU Usage Assigned Memory Uptime Status Name State CPU Usage Assigned Memory Uptime Status New Reving CL 4505 MB 3.1454.29 Versul Machine Hyper V StatingL Status If Hyper V StatingL Status Status Versul Machine Hyper V StatingL Status If Visual Machine Hyper V StatingL Status If Visual Machine If Hyper V StatingL Status If New Visual Machine If Hyper Visual Machine If Hyper Visual Machine If New Visual Machine If Hyper Visual Machine If Myper Visual Machine If Missal Status Status Status Status If Missal Status Status <td< th=""><th>Hyper-V Manager File Action View Help</th><th></th><th></th><th></th><th></th><th></th><th></th><th>-</th><th>- ×</th></td<>	Hyper-V Manager File Action View Help							-	- ×
WNA-NOXOSSBAGGI What Mobiles Name State CPU Ubage Asigned Memory Uptime Statu New Image Discover Discover State New New <t< td=""><td>💠 💠 🙇 📷 🖬 📷</td><td></td><td></td><td></td><td></td><td></td><td></td><td>Artions</td><td></td></t<>	💠 💠 🙇 📷 🖬 📷							Artions	
Name State CPU Usage Asigned Memory Uptime Statu Image: State Processand Ruring 01. 4005 MB 3.14.54.29 Image: State State State Image: State Image: State Image: State Conclusion: Image: State Image: State Image: State Image: State Image: State Conclusion: Image: State Image: State Image: State Image: State Image: State Image: State I	WIN-NS0G6584GG3								
Import Visual Machine Import Vi			State CS						
A prove Server A formation A prove Server A prove		hyper-aanal	Running 01	4096 MB	3.14:54	29			· · · ·
✓ Ceckpoints The selected vitual machine has no checkpoints. The selected vitual machine has no checkp									
 Cecclpaints The selected vitual madree Nam to checkports. Cecclpaints The selected vitual madree Nam to checkports. Result 640 Manager Standows Content Conte									
 I define and a serie dedy attain machine has no checkports. The selected vitual machecycle checkports. The selected vitual machine									
Cockpoints Cockpoints The selected vitual machine has no checkpoints The selected vitual macheckpoints The selected vitual machine has no									
Crectopion tase in a schere has no checigores. The selected vitual nucleure									
 Ceckpoints The selected vitual machine has no checkports. The selected v									
Checkgoints ↓ Defrach The selected vitual madrine has no checkgores. ↓ If Hip h Image: Selected vitual madrine has no checkgores. ↓ If Hip h Image: Selected vitual madrine has no checkgores. ↓ If Hip h Image: Selected vitual madrine has no checkgores. ↓ ↓ ↓ Image: Selected vitual madrine has no checkgores. ↓ ↓ ↓ Image: Selected vitual madrine has no checkgores. ↓ ↓ ↓ Image: Selected vitual madrine has no checkgores. ↓ ↓ ↓ Image: Selected vitual madrine has no checkgores. ↓ ↓ ↓ Image: Selected vitual madrine has no checkgores. ↓ ↓ ↓ Image: Selected vitual madrine has no checkgores. ↓ ↓ ↓ ↓ Image: Selected vitual madrine has no checkgores. ↓<								 Stop Service 	
Checkpoints The selected vitual machine has no checkports. Mage: samal Semigation Semigation								× Remove Server	
The selected vitual madree has no checkports. If Hiph Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. Image: Selected vitual madree has no checkports. I							,	8 Refresh	
hyper-anal Super-anal Created: 9/7/2021 24/311 PM Configuration Version: 0 Heartbeat: OK (%) Agolation Data) Generation: 1 None 1 Heartbeat: OK (%) Agolation Data) Heartbeat: 0K (%) Agolation Data) Heartbeat: 1 Hote:: None		Checkpoints					۲	View	•
hyper-anal Super-anal Created: 9/7/2021 24/311 PM Configuration Version: 0 Heartbeat: OK (%) Agolation Data) Generation: 1 None 1 Heartbeat: OK (%) Agolation Data) Heartbeat: 0K (%) Agolation Data) Heartbeat: 1 Hote:: None			т	te selected virtual machin	e has no checkpoints.			P Help	
hyper sanal Created: 9/7/2021 2-0711 PM Generation: Created: 9/7/2021 2-0711 PM Generation: Configuration Version: 00 Heartbeat: Discrete: 10 Hotes:									
hyper sanal Find Res Created: 9/7/2021 2-0/31 PM Configuration Version: 80 Generation: 1 Notes: None									
hyper-anal Sove transfer Sove Configuration Version: 0. Heartbeat: OK (%) Application Data) Generation: 1 None Heartbeat: OK (%) Application Data) Instite Replication Intale Replication Hop Hop								-	
hyper samal Sine Dean Created: 9/7/2021 2-4711 PM Configuration Version: 50 Generation: Chastered: No Heartbeat:: OK (No Application Data) Generation: 1 Notes:									
hyper-axaal image: state in the second sec									
hyper-aanal Ii Paule Created: 9/7/2021 247.11 PM Chastered: No Configurations Version: 9 Hows Generation: 1 Heartbeat: 0K (No Application Data) Notes: Nore If Paule Intes: Nore If Paule								-	
kper-aanal By Rest Configuration Version: 30 Clastered: No Generation: 1 Notes: Nore								O Save	
Created: 9/7/2021 2-07.11 PM Clustered: No P More P More P Sport P Restance Restance <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Pause Pause</td><td></td></t<>								Pause Pause	
Created: \$/7202124711PM Clustered: No \$\$/7202124711PM Configuration Version: \$0 Heartbeat: OK (Ib Application Data) Generation: 1 Note: None								I> Reset	
Created: 5/7/2021 247.11 PM Clustered: No If More Configuration Version: 0 Heartbeat: OK (%) Application Data) If Aname Generation: 1 Heartbeat: OK (%) Application Data) If Aname None If More If Aname If Aname		hyper-aanal						B Checkpoint	
Configuration Version: 9:0 Heartbeat: OK (No Application Data) 4.0 Expert Generation: 1 Botes: None								P Move	
Configuration Version: 50 Heartbeat: OK (b): Application Data) == Generation: 1 == Notes: None == Holp == Ho				21 2:47:11 PM				Export	
Notes: None 🙀 Enable Replication						Heartbeat: OK (No Application D	Data)		
E Help								11 Enable Replication	
		Not	es: None						
Summary Memory Networking Replication								a sub	
Sumay Memoy Networking Residuation									
		Summary Memory Ne	etworking Replication						

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.

WIN-NS0G6SB4GG3	Virtual Machines						Actions
	Name	State	CPU Usage	Assigned Memory	Uptime	Status	WIN-NS0G6S84GG3
	hyper-sanal	Running	0%	Virtual Switch Manag	er for WIN-NS0G6	584GG3	- 0 ×
		figuration Version: eration:	The selec 9-7/2021 2-47	A Virtual Switcher → Res virtual referse (2007) A club and the Case Soft 330 A clubal Reference MACAddes Sea 00:15:30:47:422	LOM #3 ttings		Create Whad Switch

Figure 87: Create Virtual Switch

Step 12In 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

Name hyper-aanal		CPU Usage		Status WIN-NSOG65846G3
hyper-sanal	Running	0%	1/10	
			Virtual Switch Manager for WIN-NS0G65	584663 - 0 3
			R Virtual Switches Image: Sev virtual network switch Image: Sev virtual network switch Image: Sev virtual network switch Image: Sev virtual network switch	Name:
			Cisco 1GigE 1350 LOM #3	Aanal hyper V
			Cisco 1GigE 1350 LOM	Notes:
			A Global Network Settings	
<		_	MAC Address Range 00-15-5D-67-02-00 to 00-15-5D-6	· ·
Checkpoints				Connection type What do you want to connect this virtual switch to?
				External network:
		The select		Osco 1Golf 1350 LOM
				Allow management operating system to share this network adapter
				Enable single-root I/O virtualization (SR-IOV)
				Internal network Private network
				VLAN ID
				Enable virtual LAN identification for management operating system
		_		The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This
hyper-aanal				setting does not affect virtual machine networking.
Crea	1ect 9/7/	2021 2 42		2
				Remove
Gene	eration: 1			
	Checkpoints Checkpoints hyper aanal Cree	Checkpoints hyper-anal Created: 9/7 Configuration Version: 50	Checkpoints The selec Structure Stru	Checkpoints

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.

 Cisco-spaces-connector3-I84-may2023.hyperv
 5/3/2023 12:23 PM
 HVPERV File
 5,742,600 KB

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

Step 3 Open Hyper-V Manager.

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

Figure 89: Create New Virtual Machine

e Action View Help							
🔶 🙇 🖬 🖬 🖬							
Hyper-V Manager	Virtual Machines					Actions	
WIN-E7FRSAF7CMD	Name	State	CPU Usage	Assigned Memory	Uptime	WIN-E7FRSAF7CMD	
	Connector_kenne		er o osoge	resigned memory	opune	New 🕨	Virtual Machine
						Import Virtual Mach	Hard Disk
						Hyper-V Settings	Floppy Disk
						Virtual Switch Mana	
						🔬 Virtual SAN Manage	
	<					🚄 Edit Disk	
	Checkpoints				(Inspect Disk	
		The coloridation		ab a share into		Stop Service	
		The selected virtual machine has no checkpoints.				× Remove Server	
					Refresh		
						View 🕨	
					Connector_kennepha		
						📲 Connect	
	Connector_kenner	oha				Settings	
		Created: 5/26/2021 7:53:19 PM Clustered: No				Start	
		onfiguration Version:				b Checkpoint	
			1			Move_	
	1	lotes:	None			Export	
						E Rename	
						E Delete	
	Summary Memory	Networking Replication				Enable Replication_	
	<				>	· · · · · · · · · · · · · · · · · · ·	

Note

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

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

Hyper-V Manager WIN-E7FRSAF7CMD	Virtual Machines			Actions
	Name	State C State C New Virtual Machine Wiz		win-E7FRSAF7CMD
	< Checkpoints Connector_kenne	Refore You Regin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	This wizard helps you create a virtual mad computers for a variety of uses. You can you can change the configuration later us To create a virtual machine, do one of the • Click Finish to create a virtual machine v • Click Next to create a virtual machine v	following: that is configured with default values.
			Do not show this page again	

Figure 90: Click Next to Begin Deployment

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

Virtual Machines					Actions	
Name Connector_kenn	🛄 New Virtual Machine W	CPU Usage /izard	Assigned Memory	Uptime	WIN-E7FRSAF7CMD	
< Checkpoints	Before You Begin Specify Name and Location Specify Generation Assign Memory	The name	name and location for t e is displayed in Hyper-V his virtual machine, such hyperv-connector	Manager. We rec	ommend that you use a name e guest operating system or	that helps workload.
	Configure Networking Connect Virtual Hard Disk Installation Options	folder, th	create a folder or use an re virtual machine is stor the virtual machine in a	ed in the default fi	store the virtual machine. If older configured for this serve	you don't se er.
	Summary	Location:	ou plan to take checkpoir	nts of this virtual m	wai hard disks\/hyper-v-2-31\ wachine, select a location that a and may require a large am	has enoug ount of spa
Connector_kenne						

Figure 91: Name of Connector

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

Figure 92: Specify Generation

 Specify Generation Before You Begin Specify Name and Location Specify Generation Generation 1 This virtual machine generation supports 32-bit and 64-bit guest operating sy virtual hardware which has been available in all previous versions of Hyper-V Generation 2 This virtual machine generation provides support for newer virtualization feat firmware, and requires a supported 64-bit guest operating system. Once a virtual machine has been created, you cannot change its generation 	
Specify Name and Location Generation 1 Specify Generation This virtual machine generation supports 32-bit and 64-bit guest operating sy virtual hardware which has been available in all previous versions of Hyper-V Configure Networking Installation Options Connect Virtual Hard Disk This virtual machine generation provides support for newer virtualization feat firmware, and requires a supported 64-bit guest operating system. Installation Options Once a virtual machine has been created, you cannot change its generation	
More about virtual machine generation support	ures, has UEFI-based

Step 8In the Assign Memory window, specify 4096 MB (4GB) of memory for the virtual machine instance.Note4096 MB (4GB) of memory is equivalent to the standard configuration of HYPER-V.

p					
L					
	Virtual Machines			Actions	
£	Name		PU Usage Assigned Memory Uptime	WIN-E7FRSAF7CMD	•
		Assign Mem Before You Begin			
	Checkpoints	Specify Name and Location	Specify the amount of memory to allocate to th MB through 12582912 MB. To improve perform recommended for the operating system.		
	Specify Generation Assign Memory		Startup memory: 409d MB		
		Assign Memory Configure Networking	Use Dynamic Memory for this virtual machin	e.	
		Connect Virtual Hard Disk Installation Options Summary	When you decide how much memory to as use the virtual machine and the operating	sign to a virtual machine, consider system that it will run.	r how you intend
	Connector_kenn				

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

Figure 94: Configure Networking

-	-					Actions	_
	Virtual Machines					WIN-E7FRSAF7CMD	
	Name Connector_kenr	State C State C State C Configure M	ard	ssigned Memory	Uptime		
	< Checkpoints	Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virbuel Hard Disk	virtual switch	tual machine include n, or it can remain da Not Connected Not Connected vSwitch	a network adapte connected.	tr. You can configure the ne	twork adapter to
	Connector_kenne	Installation Options Summary					
	Summary Memory				< Previous	Next > En	ish Car

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).

Hyper-V Manager Action DESKTOP-LEPHK33 Configu 11.0 11.0 11.0 2 Connect Virtual Hard Disk Status Before You Begin A virtual machine requires storage so that you can in storage now or configure it later by modifying the vir Specify Name and Location Specify Generation Create a virtual hard disk.
 Use this option to create a VHDX dynamically expanding virtual hard disk. New Virtual Machine.vhdx 127 GB (Maximum: 64 TB) Use an existing virtual hard disk
 Use this option to attach an existing VHDX virtual hard disk. View Z Help Location: C:\ProgramData\Microsoft\Windows\Virtual Hard Disks Browse... Attach a virtual hard disk later Use this option to skip this step now and attach an exis 🛄 Open × 4 ↑ > Documents > hypervcco С Search hypervcco p Organize 🔻 ≣ • 🔳 🚯 < Previous Videos * Nam Date m Type 🚞 New folde - cisco-5/12/2023 1:54 AM Hard Disk Image F... conn-3-hyperv System32 Virtual hard disk files File name: cisco-spaces-connector-disk1 Open Cancel

Figure 95: Connect Virtual Hard Disk

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

7CMD	Virtual Machines	Actions
	Name State Connector_kenr New Virtual Machin Compket	CPU Usage Assigned Memory Uptime WIN-E7FRSAF2CMD
	Checkpoints Specify Name and Locati Specify Generation Assign Memory Configure Networking	You have successfully completed the New Virtual Machine Wizard. You are about to create th following virtual machine. Description: Name: hyperv-connector Generation: Generation 1 Memory: 4096 MB
	Connect Virtual Hard Disk	Network: vSwitch Hard Disk: C:\UsersiPublic\Documents\Hyper-V\Virtual hard disks\hyper-v-2-31\cisco-dna
		To create the virtual machine and close the wizard, 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

viHyperV ~	3 4 ▶
Hardware Add Hardware Firmware Boot from Hard Drive Secure Boot disabled Memory 1024 MB Processor 4 Virtual processors SCS1 Controller Hard Drive cisco-spaces-connector-disk1 Network Adapter pwalawal-connector-233-v-switch Management Name aviHyperV Integration Services Some services offered Checkpoints Standard Smart Paging File Location C:\ProgramData\Wicrosoft\Windo	Security Secure Boot Use Secure Boot to help prevent unauthorized code from running at boot time (recommended). Enable Secure Boot Template: Microsoft Windows Encryption Support Enable Trusted Platform Module A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform. Encrypt state and virtual machine migration traffic Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host. Security Policy Specify additional protection options for the virtual machine. Enable Shielding This affects additional settings.
 Automatic Start Action Restart if previously running Automatic Stop Action Save 	Learn more about virtual machine security.

- 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**.

er-V Manager			- 0 X
ction View Help			
2 🖬 🖬 🖬			
er-V Manager	Virtual Machines		Actions
WIN-E7FRSAF7CMD	Name State CPU Usage	Assigned Memory Uptime	WIN-E7FRSAF7CMD
	hyperv-connector Off	Assigned Memory Optime	New +
			🕼 Import Virtual Mach
			Hyper-V Settings
			Virtual Switch Mana
			🔬 Virtual SAN Manage
	<		💰 Edit Disk
	Checkpoints		🤇 🖃 Inspect Disk_
			Stop Service
	The selected virtual machine has no	× Remove Server	
		C Refresh	
		View >	
		🛿 Help	
		hyperv-connector	
			- Connect
	hyperv-connector		- Settings.
	Created: 6/9/2021 3:57:29 F	M Clustered: No	Start
	Configuration Version: 9.0		Checkpoint
	Generation: 1		Move.
	Notes: None		Beport.
			Ename_
			Sc Delete.
	Summary Memory Networking Replication		Enable Replication
	<		

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

Hyper-V Manager						- 0	×
File Action View Help							
💠 🔶 🙇 📷 🖬 🖬							
Hyper-V Manager	Virtual Machines					Actions	_
WIN-NS0G6584GG3	Name	State	CPU Usage Assign	ed Memory Uptime	Status	WIN-NS0G6584GG3	
	hyper-banal	Running	0% 4096 N			New	
	E soften gen en	Point by	4000	0.00.1		🕼 Import Virtual Machine	
						Hyper-V Settings	
						Virtual Switch Manager	
						🕺 Virtual SAN Manager	
						Edit Disk	
						Inspect Disk	
						Stop Service	
						× Remove Server	
	¢					>	
	Checkpoints					View	
			The selected standard	hine has no checkpoints.		I Help	
						hyper-aanal	
						Connect	
						Settings	
						Turn Off	
						Shut Down	
						O Save	
						II Pause	
						IÞ Reset	
						Checkpoint	
	hyper-aanal					Move	
	Cr	eated: 9/	7/2021 2:47:11 PM		lustered: No	Export	
		infiguration Version: 9.0)		leartbeat: No Contact	Rename	
		meration: 1				Enable Replication	
	No	tes: No	ne			Help	
						Perp	
	Summary Memory M	Networking Replication					

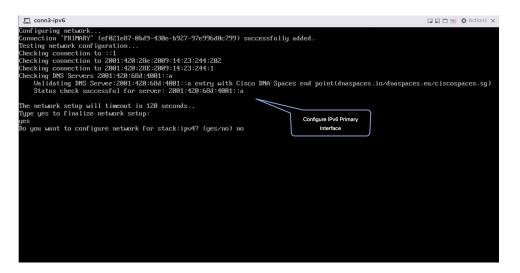
The virtual machine terminal is opened.

- **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

Uddiniteri iduz-conti i tov	Lar loci	
Choose a network interface as PRIMARY from below that has connectivity to Cisco Spaces Cloud.		
Note: SECONDARY interface can be configured using connectorctl cli after completing configuration. Interface: ens32 - (00:00:29:80:40:0F)		
Interface: ens33 - (00:0C:29:0A:4D:D9) Choose a network interface [ens32 or ens33]: ens32	Configure the public-	
Starting network setup	facing interface (Primary)	
Choose network stack[ipv4 or ipv6]: ipv4 Enter network settings configuration information for stack:ipv4	lacing interface (Fillinary)	
Enter IP address formatted as: ip[/prefix]. Example: 192.168.1.5/24, 18.0.0.11/24: 1		
Enter gateway: Enter DNS server(Comma separated ip address list):		
Enter search domain name:		
Confirm network settings? (yes/no) yes		

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

conn-3-244-99	
	Timezone setup
	Annezone setup Would you like to setup timezone? (blank for default value (UTC))
	worring you fine to setup finesone: (train for default value (tr())
	J. Africa - Press 1
	2. America - Press 2
	3. Asia - Press 3
	4. Australia - Press 4
	5. Burge - Press 5
	Select an option from the list above: (blank for default (Default value is 2))
	1. America/Anchorage - Press 1
	2. America/Buenos Aires - Press 2
	3. America/Chicago - Press 3
	1. America/Denver - Press 1
	5. America/Los_Angeles - Press 5
	6. America∠Mexico_City - Press 6
	7. America/New_York - Press 7
	8. America/Phoenix - Press 8
	9. America/Regina – Press 9
	10. America/Santiago - Press 10
	11. America/Sao_Paulo - Press 11
	12. America/Toronto - Press 12
	13. America/Vancouver - Press 13
	Select an option from the list above: (blank for default (Default value is 1))
	5
	Setting timezone and restarting services

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

Figure 103: Configure NTP

dualinterface-conn180	🖬 🖬 🖻 🐂 🛟 Actions 🛞	
Configure HTP Enter comm separated HTP servers list (blank for no HTP server): ntp.esl.cisco.com Checking status for server: ntp.esl.cisco.com Status check successful for server: ntp.esl.cisco.com Akarning: The unit file, source configuration file or drop-ins of chronyd.service changed on H to reload units.	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.

ervers list (blank for no NTP server): rtp5-b5-rbb-nfp1-v6.cisco.com rtp5-b5-rbb-ntp1-v6.cisco.com server: rtp5-b5-rbb-ntp1-v6.cisco.com

Figure 105: ConnectorGUI

arated NTP server: r for server: r ccessful for se

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



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 na	avigation pane, choose Setup > Wireless Networks.	
Step 3	In the Get your	wireless network connected with Cisco DNA Spaces area, click Add New.	
Ston /	In the Cisco Ai	roos Controllor/Catalyst 0800 Wireless Controllor area aliak Salaat	

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. Finure 107 Via Spaces Connector Finure 107 Via Spaces Connector

Figure 107: Via Spaces Connector

How do	you want to connect to Cisco DNA	Spaces?
Via Spaces Connector	Connect WLC directly	Via CMX On-Prem
Reguires you to install Spaces Connector on a virtual machine in order to connect your WLC to Olsco DNA Spaces cloud. Note: Not compatible with Catalyst 9800 controller	Requires WLC with software version 8.8 MR2 and above or Osco Data/st Wreless Correctler with software version 16.1.2.2 and above. Wireless controller needs direct internet connectivity.	Configure your CMX On-Prem distributed to send location updates to Cloco DNA Spaces, either by configure the Natifaction UBs, in the Cloco CMX distributed or by manually uploading a JSCN file that contains your location herearchy.

Step 6

In the **Prerequisites for Spaces Connector** dialog box, click **Continue Setup**. *Figure 108: Read Prerequisites for Spaces Connector*

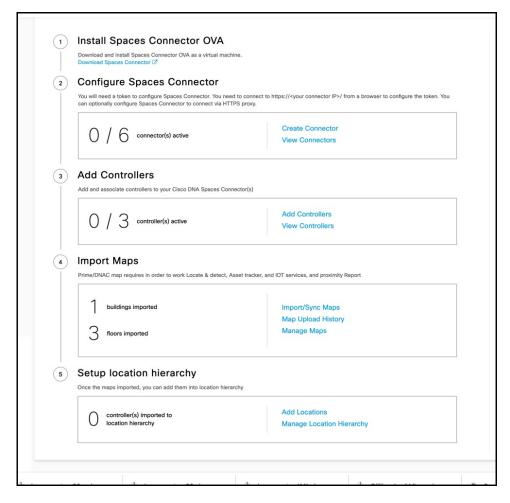
	Great! Based on your inputs, we have customized setup to help you connect your wireless network to Cisco DNA Spaces using Spaces Connector
Pre	requisites for Spaces Connector
	You must have WLC version 8.0 and above. You must have access to a virtual machine (VMvare) to install Spaces Connector.
	You must have access to a virtual machine (vieware) to install spaces Connector. Spaces Connector needs access to your Wreless LAN Controllers and connectivity to the internet (direct connection or via HTTPS proxy)
	3) Spaces connector needs access to your wwetess Every controllers and connectivity to the internet (area: connection or warm (PS proxy)
	Customize Setup

Step 7Expand the Connect via Spaces Connector area using the respective drop-down arrow.Figure 109: Expand Connect via Spaces Connector

■ Cisco DNA Spaces			O Active APs
Connect your wire	eless network		
	paces Connector y way to get your wireless network cannected to Cisco DNA Spaces. No need to upgrade Wiveless LAN Control		ick to
	Catalyst 9800 Directly Directly is an easy way to get your whiteles network connected to Chica DNA Spaces. No need to approach Wir	ex	pand v
	Pring		v
	gin Is to connect to Class Mereli Claud, import locations in to Class DNA Typeces and activate/system	he Merali Networks.	× · ·
B	Get your wireless network connected with Cisco DNA Spaces There are multiple eptions to get connected based on your wireless network oppoyment.	Need Heip? Configuration guide Clace AlveOS/Catalyst 27	
	+ Add New	Cisco Meraki C	9

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

Create Connector
 Enter the spaces connector name Connector Version Initis generation Connector designed to transfer location data efficiently to Cisco Spaces cloud O Portion 3.0 Support for deploying and managing multiple individual services Enhanced monitoring and troubleshooting of the connector and connector services and system upgrades Refer to the Connector 3.0 Configuration Guide for more details Inable Location Services ()
Cancel Save

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

Figure 112: Connector Created Successfully

Create Connector
\bigtriangledown
Connector Created Successfully
Next step:
Please generate a token from connector details page and configure it in your "instance/box"
Go to Connector Details Page

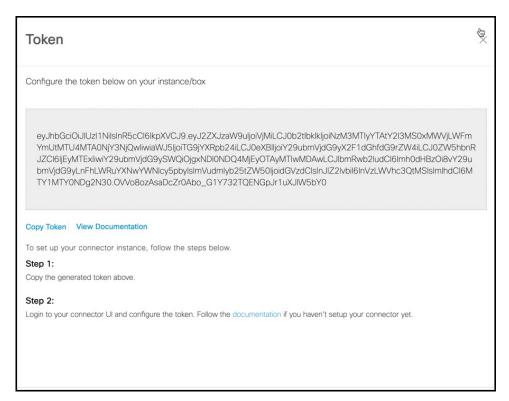
Step 10 In the connector details window, you can see a summary of the configurations for this connector. Click Generate Token.

Figure 113: Generate Token

Back Setup > Connectors > Test	ID : 81424448212902120000 Last Modified : Apr 29, 2022, 11:04:25 AM
SUMMARY 0 0 0 2 0 Instances Active Inactive Services Switches enabled	
Instances Configuration Metrics	Generate Token
Instances in High Availability Pair	
Instances in High Availability Pair Configure your instance	
Configure your instance	
Configure your instance To set up high availability pair follow the steps below.	

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**.

WarningDuring 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

Setup > Connect	ors > conn-ha-vip)							
	SUMMAR	Y							
	2 Instances	2 Active	0 Inactive	2 Serv	vices er	nabled	0 Controller	0 Switches	
Configuratio	on Instances	Metrics							
Instances	in High Avail	ability Pair							
ŝ		54c8 le: connector3-p8 or2023	4-				0		
Mac	D		0	0:50:56:A7	:54:C	Restart S			
IP Ad	dress		1	0.89.45.92			Connector Instance		
Statu	S		1	D Up		Remove	instance		
Contr	ol Channel Statu	s	C	onnected		Configur	ration history		
HA S	tatus		N	ot Paired					
VIP A	ddress		N	A					
SERV	ICES								
	c <mark>e Manager</mark> n: 3.1.0.104 Las	t Upperd on May 1	• Up	07 DM					
		t neard on May 1		:07 PIVI					
Locat Versio	n: 3.1.0.52 Last	Heard on May 11	▲ Up , 2023, 5:41:0	07 PM					



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

SPACES Connect	tor 3.1						e •
🖄 Dashboard							
Configure Connector	Configure Token Without the token, the con	nector will not be able to start.					Configure Token ×
Configure HTTP proxy							
Privacy Settings		General Information				Primary Interface	
Manage API Keys		Connector Name	Not Available	HA Config Mode	Not VIP Paired	IP Address 10.89.45.92/24	
	Connector 3.1	Tenant ID Connector ID	Not Available Not Available			MAC Address 00:50:56:A7:54:C8 Gateway	
 Troubleshoot 	Hostneme corrept	Instance ID	005056a754c8			Gateway DNS Server	
	Package corrector3-p84	Proxy	00000870408			Domain	
	Show More	NTP Address	ntp.esl.cisco.com			IP Stack ipv4	
		NTP Status	active (running)				
	Health						
	Cloud Reachability	Connected	Memory Percentage Usage	11.1 % ()			
	CPU Percentage Usage	0.8 % ①	Running Status	Up 🛈			
	Disk Percentage Usage	4.8 % ()	System Load Average	0 🛈			
	Disk Usage	4469.07 MB ①	Up time	5d 3h 32m 51s 🛈			
	Memory Usage	435.62 MB 🛈					
	Services C						
	Service Manager	3.1.0.92	Φ	6 1			
	Up time	5d 3h 31m 9s 🛈					
	Control Channel	Down					
	CPU Usage (%)	0.33 % 🛈	Looking	for other services?			
	Memory Usage (%)	4.74 % 🛈	Follow st	ps below to add services			
	Memory Usage	185.99 MB ①	1 6	gin to Cisco Spaces			
	Dirk Lisana (%)	05.0	6	bel: Mos//chaspages inframe			

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.

Ŵ

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

ŵ	Dashboard	
6	Configure Connector	
()	Configure HTTP proxy	
â	Privacy Settings	MAC and Username Salt
P	Manage API Keys	Enable Mac Address Hashing
		Enable Username Hashing
		Hide IP Address
		Update



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

← → C ▲ Not Secure https://10.22.244.86	proxy 🏠 🧶 🏂 🗌	🔹 Incognito 🕴
SPACES Connector 3.1		Θ
斺 Dashboard		
Configure Connector		
Configure HTTP proxy		
Privacy Settings	Note: If the machine is behind a proxy, Connector won't be able to interact with the cloud. Configure Proxy to get the connector working.	
Manage API Keys	n we menne a sense a prozy, connector won coe aute to menece with the close. Connector you get the connector working. Prey VIII http://proxy.esi.cises.com.80	
 Troubleshoot 	Configure Username and Password (Optional)	
	To configure new proxy, remove the existing proxy. Remove Proxy	

Figure 120: Configure Basic Authentication for Proxy (Optional)

Note:
If the machine is behind a proxy, Connector won't be able to interact with the cloud. Configure Proxy to get the connector working.
Proxy URL
Configure Username and Password (Optional)
Proxy Username
Proxy Password
Save

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

(C A Not Secure ht	tps://10.22.244.86/troubleshoot	🖈 🥌 🗯 🗖 💮 Incognito 🗄
	PACES Conner	ctor 3.1	Θ
6	Dashboard	Network Connectivity	
6	Configure Connector		
۲	Configure HTTP proxy	Connector Diagnostics is a workflow that detacts common problems with your spaces connector instance. If will run tests to diagnose operational issues in different staggos of the spaces connector. Upon completing the diagnostics tests, you can download the connector logs to share with Cisco for stivenced troubleshooting.	https://connector.qs-dnaspaces.io V Run New Test
۵	Privacy Settings	Click on "Run New Test' to begin diagnosing your spaces connector instance. Click on "View Log" to see more information for that specific test.	
P	Manage API Keys	Recent Tests	
	Troubleshoot		
		No test has been run	

Figure 122: Sample Run Test Results

Configure Connector				
Configure HTTP proxy	Connector Diagnostics is a workflow that detects commo run tests to diagnose operational issues in different stage diagnostics tests, you can download the connector logs	is of the spaces connector. Upon completing the	https://connector.ga-dnaspaces.io 🗸	Run New Test
Privacy Settings	Click on "Run New Test" to begin diagnosing your spaces information for that specific test.		https://connector.qa/unaspaces.to	Hull New Jest
Manage API Keys	Recent Tests			
Troubleshoot	Troubleshoot Complete.			
	Cloud Endpoint DNS Resolution () 3 seconds age	Troubleshoot DNS Resolution for https://connector.ga-dnaspaces.io		View Log
	HTTP Proxy Reachability () 11 seconds ago	Checking HTTP proxy http://proxy.esi.cisco.com:80 reachability		View Log
	 HTTP Proxy Server Diagnostics () 3 seconds ago 	Testing proxy evailability using netcat for proxy: http://proxy.esl.cisc	:o.cam:80	View Log
	Connector Token Diagnostics () 1 seconds ago	Validating spaces cloud token configuration		View Log
	Cloud Reachability ① 3 seconds ago	Reachability test to https://connector.qe-dnaspaces.io using curl co http://proxy.esi.cisco.com:80	immand with proxy:	View Log
	 Service Connectivity () 3 seconds ago 	Checking service connectivity to cloud andpoint https://connector.cj Manager with proxy: http://proxy.asl.cisco.com.80	a-dnaspaces to from Service	View Log
	Download Diagnostics Logs			

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

← → C ▲ Not Secure https://10.22.244.86	proxy 🖈 😐 🏚	🛾 🎯 Incognito 🗄 🗄
SPACES Connector 3.1		Θ
Dashboard		
Configure Connector		
Configure HTTP proxy		
A Privacy Settings	Note: If the machine is behind a proxy, Connector won't be able to interact with the cloud. Configure Proxy to get the connector working.	
Manage API Keys	Proxy URL http://proxy.esi.clisco.com:80	
 Troubleshoot 	Configure Username and Password (Optional) To configure new proxy, remove the existing proxy. Remove Proxy	

Figure 124: Configure Basic Authentication for Proxy (Optional)

Note:
If the machine is behind a proxy, Connector won't be able to interact with the cloud. Configure Proxy to get the connector working.
Proxy URL
Configure Username and Password (Optional)
Proxy Username
Proxy Password
Save

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

Step 5You can troubleshoot any issues in proxy configuration. Click Troubleshoot and enter the Cisco Spaces URL.Figure 125: Troubleshoot Proxy Issues

← → C ▲ Not Secure http	se://10.22.244.86/troubleshoot	🖈 🥌 🗯 🖬 🌚 Incognito 🕴
SPACES Connect	tor 3.1	θ
Dashboard	Network Connectivity	
Configure Connector	Connector Diagnostics is a workflow that detects common problems with your spaces connector instance. It will	
Configure HTTP proxy	Connector biagnose presidentia a worknew that batests common proteins with your spaces connector instance. It will run tests to diagnose operational issues in different stages of the spaces connector. Upon completing the diagnostics tests, you can download the connector logs to share with Cisco for advanced troubleshooting.	https://connector.ga-dnaspaces.io V Run New Test
Privacy Settings	Click on "Run New Test" to begin diagnosing your spaces connector instance. Click on "View Log" to see more information for that specific test.	
Manage API Keys	Recent Tests	
Troubleshoot		
	No test has been run	

Figure 126: Sample Run Test Results

Configure Connector				
Configure HTTP proxy	Connector Diagnostics is a workflow that detects commor run tests to diagnose operational issues in different stage diagnostics tests, you can download the connector logs to	s of the spaces connector. Upon completing the	https://connector.ga-dnaspaces.io V	Run New Test
Privacy Settings	Click on 'Run New Test' to begin diagnosing your spaces information for that specific test.	connector instance. Click on 'View Log' to see more		
Manage API Keys	Recent Tests			
Troubleshoot	Troubleshoot Complete.			
	 Cioud Endpoint DNS Resolution () 3 seconds ago 	Troubleshoot DNS Resolution for https://connector.qa-dnaspaces.	lo	View Log
	HTTP Proxy Reachability () 11 seconds ago	Checking HTTP proxy http://proxy.esi.cisco.com.90 reachability		View Log
	HTTP Proxy Server Diagnostics () 3 seconds ago	Testing proxy availability using netcat for proxy: http://proxy.esi.el	sco.com:80	View Log
	Connector Token Diagnostics ① 1 seconds ago	Validating spaces cloud token configuration		View Log
	Cloud Reachability ① 3 seconds ago	Reachability test to https://connector.qs-dnaspaces.io using curl http://proxy.asl.cisco.com.80	command with proxy:	View Log
	Service Connectivity () 3 seconds ago	Checking service connectivity to cloud endpoint https://connector Managor with proxy. http://proxy.esl.clsoc.com.80	r.qa-dnaspaces.io from Service	View Log
	Download Diagnostics Logs			



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

E CISCO SPAC	E CISCO SPACES O Active APs				0
Connee	t your wireless network				
	nect via Spaces Connector Connector is an easy way to get your wireless network connected to Cisco Spaces. No need to	upgrade Cisco Winiess Controllars or reconfigure your winiess network.		^	
(1	Install Spaces Connector OVA Download grows Connector CVA as a vinal reachine. Download spaces Connector (?		Need Help? Access the below links to view detailed help.		
2	Configure Spaces Connector You will need a taken to configure Spaces Connector. You need to connect to https://ryour.connector via HTTPS proxy.	IP-/ from a browser to configure the token. You can optionally configure Spaces Connector to connect	View Configuration Steps System Requirements		
	2 / 11 connector(s) active	Create Connector View Connectors	Frequently Asked Questions		
3	Add controllers Add and associate controllers to your Cloco Species Connector(s)				
	1 / 4 controller(s) active	Add Controllers View Controllers			
•	Import Maps Prime/DNAC map requires in order to work Locale & detect, Asset tracker, and KIT services, and proc	imby Report			
	buildings imported foors imported	Import/Sync Maps Map Upload History Manage Maps			
	J				

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

<complex-block><complex-block><complex-block></complex-block></complex-block></complex-block>		
SUMMARY Description	E CISCO SPACES	₩ Ø 6
Pressures Pr	Setup > Connectors > connector-test	ID : 4005858765654143000 Last Modified : May 12, 2023, 5:01:08 PM
Instances in High Availability Pair Click to generate a token Configure your instance To set up high availability pair follow the steps below. See 1 Generates a token by clicking the 4b-Generate Token-t/b- buttor on the top of this page. A token will be generated. See 2 Gopt the generated token. See 3 See	O 0 0 2 0 0	
Click to generate a token Configure your instance To set up high availability pair follow the steps below. See 1: Generate a token by clicking the 	Configuration Instances Metrics	O Denerate Token S Troubleshoot Connector
To set up high availability pair follow the steps below. Step 1: Genarate a token by clicking the -Generate Token/b> button on the top of this page. A token will be generated. Step 2: Copy the generated token. Step 3: Do your connector UI and configure the token on your second connector instance. For more details follow the		
	To set up high availability pair follow the steps below. Step 1: Generate a token by clicking the Generate Token button on the top of this page. A token will be generated. Step 2: Copy the generated token. Step 3: Go to your connector UI and configure the token on your second connector instance. For more details follow the	

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

SPACES Connecti	or 3.1						θ
🖄 Dashboard							
Configure Connector	Configure Token Without the token, the connect	ctor will not be able to start.					Configure Token ×
Onfigure HTTP proxy							
Privacy Settings		General Information	Not Available	HA Config Mode	Click to Configure	a Token	arface 10.89.45.9224
🖉 - Manage API Keya	Connector 3.1	Tenant ID	Not Available	RK Garry Mode			0.50.55.47.54:08
 Troubleshoot 	Hodhame open-pri Packaga oernwold/94064 Show Mane	Connector ID Instance ID Proxy NTP Address NTP Status	Not Analable 0050356375408 https://prosy.cel.cloco.c mp.esil.cloco.com active (running)	am 80		Gataway DNS Server Domain IP Stack	10.89.45.1 177.70.168.183 сяхо.сот іро4
	Health						
	Cloud Reachability CPU Percentage Usage Dak Percentage Usage Dak Usage Memory Usage	Connected 12.5 % () 5.1 % () 4713.21 MB () 480.94 MB ()	Memory Percentage Usa Plunning Status System Load Average Up time	gn 12,25 % O Up O 0,34 O 84 4h 53m 216 O			
	Services C						
	Service Manager 🔒 3 Upgrade: Soccess	13.0.104	ø	a 2	M		
	Up time Control Channel CPU Usage (%) Merrory Usage Merrory Usage Disk Usage (%) Disk Stee	1d 11h 62m 66s ① Down 0.681 % ① 3.81 % ② 149.35 MB ② 0 % ③ 56 MB ③	Follow:	ng for other services? steps below to add services Login to Cisco Spaces Global: https://map.acs. Global: https://map.acs. For EU. https://map.acs. Adv. https://map.acs.acs. Adv.			

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

Dashboard									
Configure Connector	Configure Token Without the token, the con	nector will not be able to start.							Configure Token X
Configure HTTP prexy					(
Privacy Settings		General Information				Click to Configure	a Token	arface	
nanage API Keys 🖉	Connector 3.1	Connector Name Terrant ID	Not Availab Not Availab		HA Config Mode			10.89.45.92/24 00.50.56:A7:54:C8	
 Troubleshoot 	Hoshama connepri Packaga connector3-p04 Show Mare	Connector ID Instance ID Proxy NTP Address NTP Status	Not Analab 005056u75 https://prox ntp.esl.cisp active (num	4c8 y.esl.cisco.com.90 o.com			Gateway DNS Server Domain IP Stack	10.89.45.1 171.70.168.183 cisco.com ipv4	
	Health Cloud Reachability CPU Percentage Usage Disk Percentage Usage	Connected 12.5 % ① 5.1 % ①	Mamory Paro Purning State System Load	<i>n</i>	12.28% Up () 0.34 ()				
	Disk Usage Merrory Usage	4713.21 MB () 480.94 MB ()	Up time		8d 4h 53m 21s 🛈				
	Services C								
	Service Manager	2.1.0.104	0		6 A	1			
	Up time Control Channel	1d 11h 52m 56s ① Down 0.68 % ①		Looking for a	ther services?				
	CPU Unage (%) Memory Usage (%) Memory Usage Disk Usage (%)	0.68 % () 3.81 % () 149.36 MB () 0 % ()		Follow steps bei	ow to add services Cisco Spaces ps:/draspaces.ic/tome ps:/draspaces.ou/tome				

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

SPACES Connecto	r 3.1		
🔂 Dashboard			
Configure Connector		General Information	
-0-		Connector Name	con116
Configure HTTP proxy	Connector 3.1	Tenant ID	14002
Privacy Settings	Hostname ipv6-rajb	Connector ID	73000993702070310000
	Package connector3-p84	Instance ID	000c29cfb0f3
Manage API Keys		Proxy	Not Available
♂ Troubleshoot	Show More	NTP Address	rtp5-b5-rbb-ntp1- v6.cisco.com
		NTP Status	active (running)

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

Figure 132: Cisco Spaces dashboard

E CISCO SPACES									Ø 🔩
Setup > Connectors > conn-ha-vip							ID : 3761674	7827259750000 Last Mo	dified : May 11, 2023, 4:17:54 AM
SUMMARY 2 2 0 Instances Active Inactive	2 Services enabled		0 Switches						
Configuration Instances Metrics							0	🖉 Generate Token	Troubleshoot Connector
Instances in High Availability Pair									Configure VIP Pairing
O05056a754c8 System Pactage: connector3-p84- apr2023		0	I	Ø	005056a7affa System Package: connector3-p84- apr2023			0 1	
Mac ID	00:50:56:A7:54:C8				c ID	00:50:56:A7:AF:FA			
IP Address	10.89.45.92				Address	10.89.45.93			
Status	O Up			Sta		O Up			
Control Channel Status	Connected Not Paired				ntrol Channel Status Status	Connected Not Paired			
VIP Address	NA				Address	NGC Pained			
SERVICES				SE	WICES				
Service Manager () Version: 3.1.0.104 Last Heard on May 11, 2023, 1					vice Manager iion: 3.1.0.104 Last Heard on May 11,	6 Up 2023, 10:04:12 PM			
Location 3 Location 10 Location 10 Location 10 Location: 3.1.0.52 Last Heard on May 11, 2023, 10					ation iion: 3.1.0.52 Last Heard on May 11, 3	Up 2023, 10:04:12 PM			

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

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

L

≡ ci	CO SPACES						Ø 6
	SUMMARY 2 2 0 Instances Active Inacti	2 0 Services enabled Cont	0 troller Switches		ID : 3761674	7827259750000 Last Modified	May 11, 2023, 4:17:54 AM
C	onfiguration Instances Metrics				0	🖉 Generate Token 🛛 🚳	Troubleshoot Connector
Ir	stances in High Availability Pair		0 1	O05056a7affa System Betage: consector3-p84- paperas	Configure VIP Pairing	0	Configure VIP Pairing
	Mac ID	00:50:56:A7:54:C8		Mac ID	00:50:56:A7:AF:FA		
	IP Address	10.89.45.92		IP Address	10.89.45.93		
	Status	🔁 Up		Status	C Up		
	Control Channel Status	Connected		Control Channel Status	Connected		
	HA Status	Not Paired		HA Status	Not Paired		
	VIP Address	NA		VIP Address	NA		
	SERVICES			SERVICES			
	Service Manager Version: 3.1.0.104 Last Heard on May 11, 2023,	Up 1, 10:04:07 PM		Service Manager Version: 3.1.0.104 Last Heard on May 11, 2023	Up 8, 10:04:12 PM		
	Location Solution Version: 3.1.0.52 Last Heard on May 11, 2023,	Up 10:04:07 PM		Location Version: 3.1.0.52 Last Heard on May 11, 2023,	Up 10:04:12 PM		

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

	Configure Virtual IP: fastlocate-ha-cip \times
Serup > Connectors > fintiocate-he-cip SUMMARY 2 2 0 2 Instances Active Insettive Services emailed	Please enter the Virtual IP address for High Availability Configuration, this IP address should be on the same subnet as connector instances Virtual IP
Configuration Instances Metrics	7.7.0.25
Instances in High Availability Pair	Connector has dual interface enabled. Select one of below interface to enable vip paired HA on that interface Primary
0000c292a43c6 System Package: connector9-p64-spr2023	Secondary
Mac ID 00:0C:29:2A:43:C6	
Primary IP Address 10.22.244.113	
Secondary IP Address 7.7.0.20	
Status O Up	
Control Channel Status Connected	
HA Status Not Paired	
VIP Address NA	
SERVICES	
Service Manager 🔹 Up	
	Save

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

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

2 2 Instances Active	0 2 Inactive Services enabled	0 0 Controller Swite	hes	
Configuration Instances Metric	5			🔾 🔑 Generate Token 🏻 🍈 Tro
000c292a43c6 System Package: connector3-p84-apr2023	0	1	O00c29d6e4cd System Package: connector3-p84-apr2023	0 1
Mac ID	00:0C:29:2A:43:C6		Mac ID	00:0C:29:D6:E4:CD
Primary IP Address	10.22.244.113		Primary IP Address	10.22.244.114
Secondary IP Address	7.7.0.20		Secondary IP Address	7.7.0.21
Status	👩 Up		Status	🕤 Up
Control Channel Status	P	_	Control Channel Status	Connected
HA Status	VIP Paired BACKUP		HA Status	VIP Paired ACTIVE
VIP Address	7.7.0.25	_	VIP Address	7.7.0.25
SERVICES			SERVICES	
Service Manager	O Up		Service Manager	C Up
Version: 3.1.0.104 Last Heard on Mi	ay 10, 2023, 4:12:16 PM		Version: 3.1.0.104 Last Heard on	May 10, 2023, 4:11:59 PM
Location	🚯 Up		Location	C Up
Version: 3.1.0.52 Last Heard on May	10. 2023. 4:12:16 PM		Version: 3.1.0.52 Last Heard on M	Aav 10, 2023, 4:11:59 PM

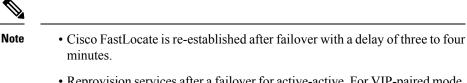
Connector Active-Active

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.



- 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

SPACES		C 166 of 1000
nnect your wireless network		
Connect via Spaces Connector Spaces Connector is an easy way to get your wireless network connected to	Cisco Spaces. No need to upgrade Cisco Wireless Controllers or reconfigure your wireless network.	^
Install Spaces Connector OVA Deveload root house Space Connector V/A as a virtual machine. Deveload Space Connector @		Need Help? Access the below links to view detailed help.
2 Configure Spaces Connector Vox will meet a taken to configure Spaces Connector. You need to come via HTTPS prop.	ect to https://qour.connector.PP/ from a browner to configure the token. You can optionally configure Spaces Connector to connect	View Configuration Steps C System Requirements C
2 / 11 connector(s) active	Create Connector View Connectors	Frequently Asked Questions C
Add Controllers Add and associate controllers to your Claco Spaces Connector(s)		
1 / 4 controller(s) active	Add Controllers View Controllers	
Import Maps Prime(DNAC map requires in order to work Locate & detect, Asset trac	ar, and IOT services, and proximity Report	
O buildings imported	Import/Sync Maps Map Upload History Manage Maps	

Step 2Enter a name for the connector and choose the version.A connector is created. Click Go to the connector Details page.

Cisco Spaces: Connector 3 Configuration Guide

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

Figure 134: Generate Token

E CISCO SPACES	≡ 0 ⊖
Setup > Connectors > connector-test	ID: 4005858765654143000 Last Modified: May 12, 2023, 5:01:08 PM
SUMMARY 0 0 0 2 0 0 Instances Active Insactive Instances Controller Switches	
Configuration Instances Metrics	🗘 🖉 Generate Token 🛛 🎂 Troubleshoot Connector
Instances in High Availability Pair Click to generate a token	
Configure your instance To set up high availability pair follow the steps below. Sep 1: Generate a token by clicking the <b->Generate Token</b-> button on the top of this page. A token will be generated. Step 2: Copy the generated token. Sep 3: Go to your connector U and configure the token on your second connector instance. For more details follow the documentation documentation	

Copy the displayed token.

- **Step 4** Repeat Step 3 to generate and copy a second token.
- **Step 5** Log in to the GUI of the first instance of connector and click **Configure Token** in the top-right corner to provision the first copied token there.

Figure 135: Configure a Token

SPACES Connect	or 3.1								•
🖄 Dashboard									· ·
Configure Connector	Configure Token Without the token, the core	nector will not be able to start.							Configure Token ×
Configure HTTP proxy					-			/	
Privacy Settings	1	General Information				Click to Configure a	Token	arface	
🖉 Manage API Keya	Connector 3.1	Connector Name Tenant ID	Not Availa Not Availa		HA Config Mode			10.89.45.92/24 00.50:56:A7:54:C8	
 Troubleshoot 	Hostname com-pri	Connector ID	Not Availa	itio			Gabrway	10.89.45.1	
	Package connector3-p84	Instance ID	005056a7	54c8			DNS Server	171.70.168.183	
		Proxy	https://pro	wy.esl.cisco.com.90			Domain	oisco.com	
	Show More	NTP Address	mp.esi.cie				IP Stack	ipv4	
		NTP Status	active (nu	nning)					
	Health								
	Cloud Reachability	Connected	Mamory Pa	centage Usage	12.26 % ()				
	CPU Percentage Usage	12.5 % ①	Punning Sta	0.0	Up 🛈				
	Disk Percentage Usage	5.1 % ①	System Loa	d Average	0.34 ①				
	Disk Usage	4713.21 MB ①	Up time		8d 4h 53m 21s 🛈				
	Memory Usage	480.94 MB ①							
	Services C								
	Service Manager	3.1.0.104	۵		6 A	1			
	Up time	1d 11h 52m 56s 🛈							
	Control Channel	Down				-			
	CPU Usage (%)	0.68 % ①			ther services?				
	Memory Usage (%)	3.81 % ①		Follow steps bell	ow to add services				
	Memory Usage	149.35 MB ①		1 Login to	Cisco Spaces				
	Disk Usage (%)	0%0			ps./dnaspaces.iohome				
	Disk Size	56 MB 🛈			tips Adnaspaces eurhome : https://biscospaces.sg				

Step 6 Log in to the GUI of the second instance of connector, and click **Configure Token** in the top-right corner to provision the second copied token there as well.

Figure 136: Configure a Token

SPA	CES Connec	tor 3.1							Θ
🖄 Da	shboard								*
Cir Co	ntigure Connector	Configure Token Without the token, the corns	ctor will not be able to start.						Configure Token X
③ Co	nfigure HTTP proxy					(
🗇 Pri	wacy Settings		General Information	Net Availa			Click to Configure	a Token	arface
<i>Р</i> Ма	inage API Keya	Connector 3.1	Connector Name Terrant ID	Not Availa		HA Config Mode			10.89.45.92/24 00.50.56:A7:54:C8
⊙ Tro	subleshoot	Hormanna ocenipri Horbaga ocenipri Nackaga oceninado 3 pól Show More	Connector ID Instance ID Proty NTP Address NTP Status	Not Availa 005056a7	bio 54c8 xy cel cisco.com 80 co.com			Gatewilay DNS Server Derrein IP Stack	10 89 46.1 17 73 561 88 Sites con goal
		Health							
		Cloud Reachability	Connected	Memory Per	centage Usage	12.26 % ①			
		CPU Percentage Usage Disk Percentage Usage	12.5 % () 5.1 % ()	Running Sta		Up ① 0.34 ①			
		Disk Usage	4713.21 MB (0	System Loa Up time	o wwerage	6.34 () 8d 4h 53m 21s ()			
		Merrory Usage	480.94 MB ()						
		Services 🔿							
		Service Manager 🚔	3.1.0.104	ø		6	1		
		Up time	1d 11h 52m 56s 🛈						
		Control Channel CPU Usage (%)	Down 0.68 % ①		Looking for a	other services?			
		Memory Usage (%)	3.81 % ①			low to add services			
		Memory Usage	149.35 MB ①		(1) Login to	Cisco Spaces			
		Disk Usage (%)	0% ()			tps://draspaces.io/home #ps://draspaces.ou/home			
		Disk Size	56 MB 🛈			t https://biscospaces.sg			

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

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

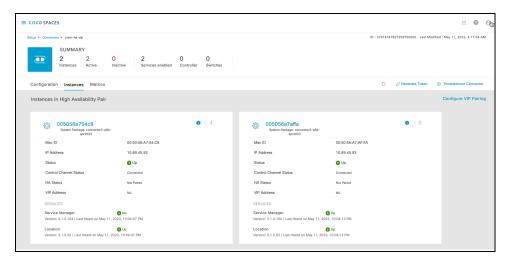
Figure 137: Observe connector ID

SPACES Connecto	or 3.1		
ាំែ Dashboard			
Configure Connector		General Information	
		Connector Name	con116
Configure HTTP proxy	Connector 3.1	Tenant ID	14002
Privacy Settings	Hostname ipv6-rajb	Connector ID	73000993702070310000
Frivacy Settings	Package connector3-p84	Instance ID	000c29cfb0f3
🖉 Manage API Keys		Proxy	Not Available
∽ Troubleshoot	Show More	NTP Address	rtp5-b5-rbb-ntp1- v6.cisco.com
		NTP Status	active (running)

Step 8 On the Cisco Spaces dashboard, go back to the connector details page, and click the **Instances** tab. Here, you can see both the connectors that you configured. Observe that the connector IP addresses are reflected here.

I

Figure 138: Cisco Spaces dashboard



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



PART

Troubleshooting

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



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	1 Log in to Cisco Spaces .		
	Note	The Cisco Spaces URL is region-dependent.	
Step 2	From the left navigation pa	ane, choose Setup > Wireless Networks .	
Step 3	In the 2. Configure Space	s 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 nav	igation pane of the Cisco Spaces dashboard, choose Setup > Wireless Networks.			
Step 3	In the 2. Configu	re Spaces Connector area, click View Connectors.			
Step 4	Click a connector	r 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 the Step 7.				
Step 10	In the New Password field, enter a new password.				

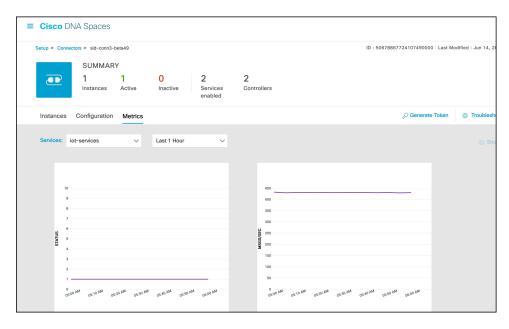
Monitor Service Metrics

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



I



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.

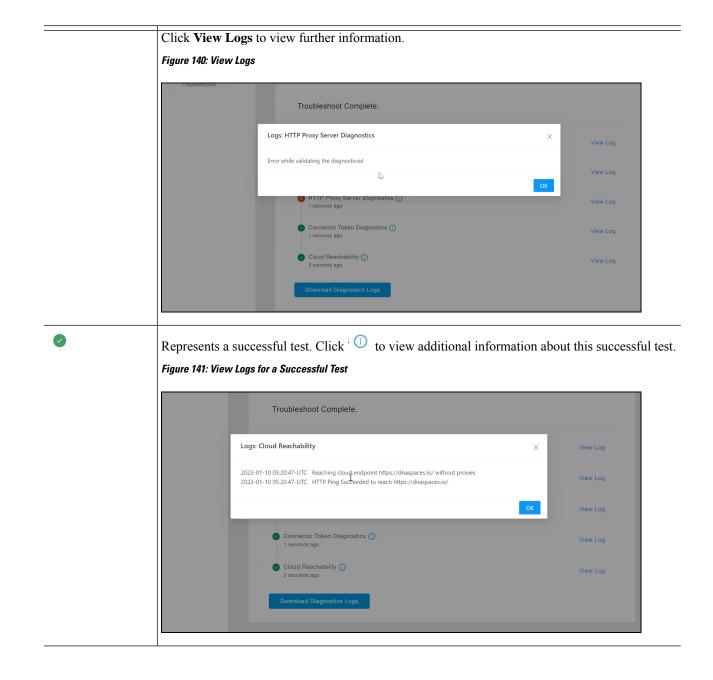
Procedure

Step 1 Log in to the connector GUI.

; (ì)

- 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:

Troubleshoot C Diagnostics to perform DNS officie tests for the configured cloud endpoint	
Cloud Endpoint DNS Resolution 3 seconds ago	View Log



•	Represents a warning. Click ¹ (1) to view additional information about this warning. <i>Figure 142: View Logs for a Warning</i>	
	Troubleshoot Complete.	
	Logs: HTTP Proxy Reachability	View Log
	2023-01-10 05:20:44-UTC There are no proxies configured for running proxy ping diagnostics	View Log
	HTTP Proxy Server Diagnostics () 1 seconds ago	View Log
	Connector Token Diagnostics ① 1 seconds ago	View Log
	Cloud Reachability () 3 seconds ago	View Log
	Download Diagnostics Logs	
8	Represents a failure in the diagnostic test. Click View Logs to see additiona <i>Figure 143: View Logs for a Successful Test</i> Troubleshoot Complete.	l details.
	Logs: HTTP Proxy Server Diagnostics	View Log
	Error while validating the disgnosticsid	View Log
	HTTP Proxy Server Diagnostics () 1 seconds ago	View Log
	Connector Token Diagnostics () 1 seconds ago	View Log
	Cloud Reachability 🕧 3 seconds ago	View Log
	Download Diagnostics Logs	

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

Figure 144: ownload Diagnostic Logs

10.22.244.103-diagnostics-logs-202	3-01-09T21_28_21-08_00.txt - Notepad -	- 0	\times
File Edit Format View Help			
2023-01-10 05:20:42-UTC 2023-01-10 05:20:44-UTC Error while validating tH 2023-01-10 05:20:46-UTC dnaspaces.io 2023-01-10 05:20:46-UTC 73161672582150816000 2023-01-10 05:20:47-UTC 2023-01-10 05:20:47-UTC	DNS Server 171.70.168.183 is reachable There are no proxies configured for running proxy ping di e disgnosticsid Perform cloud token tests for endpoint: https://connector Cloud token configured with tenant: 12454 for connector-i Reaching cloud endpoint https://dnaspaces.io/ without pro HTTP Ping Succeeded to reach https://dnaspaces.io/	r.qa- id:	cs

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

tep 1	Log in to Cisco Spaces.				
	Note	The Cisco Spaces URL is region-dependent.			
p 2	From the left navi	gation pane, choose Setup > Wireless Networks.			
p 3	In the 2. Configur	In the 2. Configure Spaces Connector area, click View Connectors.			
4	Click a connector	from the list of connectors that are displayed, and then click the Instances tab.			
5	In the Actions col Connector .	umn, click the three-dot icon to open a list of options for the connector instance, and choose Restart			

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

Log in to Cisco Spaces.		
Note	The Cisco Spaces URL is region-dependent.	
In the left naviga	ation pane of the Cisco Spaces dashboard, choose Setup > Wireless Networks.	
In the 2. Configu	ure Spaces Connector area, click View Connectors.	
Click a connector from the list of connectors that are displayed and then click the Instances tab.		
In the Actions column, click the three-dot icon to open a list of options for the connector instance, and choose 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.		

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 nav	igation 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 co	lumn, click the three-dot icon to open a list of options for the connector instance, and choose Restart		

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.

L

Figure 146: Restart Services

SUMMARY 2 2 0 0 Instances Active Teactive 2 0 0 Configuration Instances Metrics Services enabled 0 0 Configuration Instances Metrics Services enabled 0 0 0 Configuration Instances Metrics Services 0 0 0 Objective 0050566754C8 Services 0	Setup > Connectors > conn-ha-vip					
Instances in High Availability Pair	2 2			enabled	0	0
OSOSSA754C8 Synam Retages connector pat- spor223 Mac ID O0.50:50:47.54 Retart Service Retart Connector Retart Connector Retart Connector Retart Connector Retart Connector Retart Connector Retart Service Retart VP Address Not Paired VP Address Not Paired VP Address Services Service Manager Ou Services Service Manager Ou Service Manager Ou Services Service Manager Ou Services Service Manager Ou Services Service Manager Ou Services Service Manager Ou Service Service Manager Ou Service Service Manager Ou Service Service	Configuration Instances	Metrics				
Option Relage: conductor-part- sprint Restant Services Mac ID 00:50:56:47:54 IP Address 10:89:45:32 Status 0 Up Control Channel Status Connected VP Address NA Struces NA Struces NA Struces 0 Up Control Channel Status Connected VP Address NA StruCes Service Manager Service Manager 0 Up Version: 31:0.104 [Last Head on May 11, 2022, S-107 PM Locatio 0 Up	Instances in High Availab	ility Pair				
Mac ID 00:50:54:X7:55 Retart Connector IP Address 10:89:45:32 Status 0 Up Control Channel Status 0 Up Control Channel Status 0 Configuration Natory HA Status Not Paired VP Address NA SERVICES Service Manager 0 Up Version: 3:1.0.104 [Last Heard on May 11, 2023; 5:107 PM Location 0 Up	System Package: o	onnector3-p84-	ŕ		0	
IP Address 10.89.45.92 Status 0 Up Control Channel Status Connecta H. Status Net Paired VIP Address Net Paired VIP Address Net Paired SERVICES Service Manager 0 Up Version: 3.1.0.104 [Last Heard on May 11, 2022, 51:07 PM Location 0 Up	Mac ID		00:50:56:A7:54:			
Control Channel Status Convected HA Status Net Paired VIP Address NA SERVICES Service Manager Or Up Version: 3.1.0.104 [Last Heard on May 11, 2023, 58.107 PM Location Or Up	IP Address		10.89.45.92			
HA Status Configuration history VIP Address NA SERVICES Service Manager © Up Version: 31.0.104 [Last Heard on May 11, 2023, 53:107 PM Location © Up	Status		🕤 Up	Remove		
VIP Address NA SERVICES Service Manager O Up Version: 3.1.0.104 [Last Heard on May 11, 2022, 541:07 PM Location O Up				Configura	ation history	
SERVICES Service Manager Up Version: 3.1.0.104 [Last Heard on May 11, 2022, 541:07 PM Location Up						
Service Manager Dup Version: 3.1.0.104 Last Heard on May 11, 2023, 5.41:07 PM Location Dup			NA			
	Service Manager		11:07 PM			
			:07 PM			

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

If a service upgrade fails and a connector instance does not receive Cisco Spaces configurations, you can forcibly push configurations to the instance using this procedure.

Procedure

Log in to Cise	o opered.	
Note	The Cisco Spaces URL is region-dependent.	
From the left-	navigation pane, choose Setup > Wireless Networks.	
In the 2. Configure Spaces Connector area, click View Connectors.		
Click a connector from the list of connectors that are displayed, and then click the Instances tab.		
In the Actions column, click the three-dot icon to open a list of options for the connector instance, and choose Refree 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.

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@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.

hmac-shal-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1

Cisco Spaces: Connector 3 Configuration Guide



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



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	

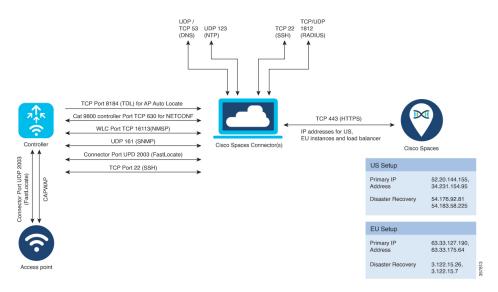
Hardware or Application Name	Support for Cisco Spaces: Connector
Supported wireless controllers for Cisco	Supported on Cisco AireOS Wireless Controller
Hyperlocation	Supported on Cisco Catalyst 9800 Series Wireless Controllers
Connector Active-Active Mode	Not supported on Cisco Embedded Wireless Controller 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.



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.

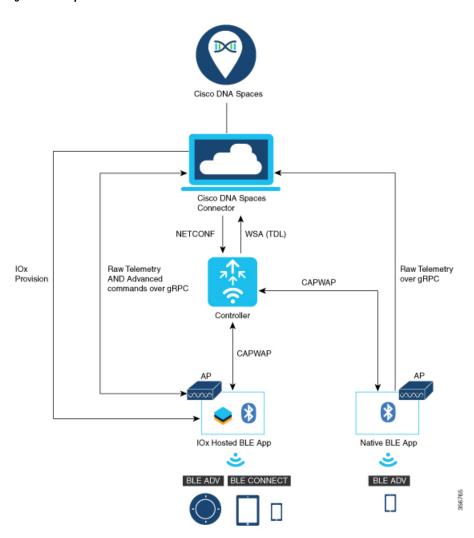


Figure 148: Components of IoT Service

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).

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

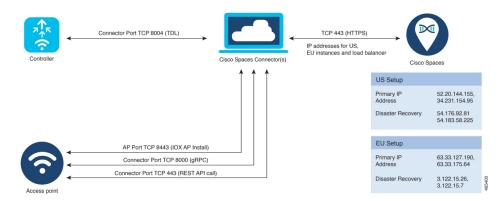
AP Mode Advanced BLE Gateway App		Base BLE Gateway App
P1: Flex • 11-AX: Supported		• 11-AX: Supported
	• Wave2: Not supported	Wave2: Supported
P2: Fabric	• 11-AX: Supported	• 11-AX: Supported
	Wave2: Not supported	Wave2: Supported
P3: Mesh	• 11-AX: Supported	• 11-AX: Supported
	• Wave2: Not supported	• 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

E CISCO SPACE	S
贷 Setup	⊙ ess network
	ks ces Connector y to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.
	es Connector OVA Baces Connector OVA as a virtual machine.
	You will need a token to configure Spaces Connector Vou need to connect to https://-your connector IP-/ from a browser to configure the token. You can optionally configure Spaces Connector to connect vie HTTPS proxy. 2 / 2 connector(s) active Create Connector
3	Add Controllers Add and associate controllers to your Claco DNA Spaces Connector(s) 1 / 2 controller(s) active Add Controllers View Controllers
	Import Maps Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report
	2 buildings imported Import/Sync Maps 2 floors imported Manage Maps
5	Setup location hierarchy Once the maps imported, you can add them into location hierarchy

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

Figure 151: Add Services

← Back Setup > Connectors > Test	ID : 81424448212902120000 Last Modified : Apr 29, 2022, 11:04:25 AM
SUMMARY 0 0 0 0 0 0 0 Instances Active Inactive Service enabled	
Instances Configuration Metrics	🖉 Generate Token 🛛 🍈 Troubleshoot Connector
Services	Add Services
You have not added any services yet. Click * Add Service* to configure services. Switches	Add Switch
You have not added any switches yet. Click "Add Switch" to configure switches	

Step 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

SUMMARY			
0 0 0 Instances Active Inactive	2 0 Services Switches enabled		
Instances Configuration Metrics			🖉 Generate Token 🛛 🚳 Troubleshoot Connector
Services			Add Services
Service Name	Version		Last Updated
°¦, service-manager	2.8.0.123	Never	
	2.8.0.33	Never	
all iot-services			

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

Manage I	oT Streams					\times
Manage Co	nnector succi	ESS			Configure t enable	0
Enable IoT Stre	eams on Cisco DN	A Spaces Conne	ctor			
automatically.				the configuration c		
Controller	Connector IP	Controller IP	Operation Status	Operation Log	Last updated	
sid-ewlc-2	172.20.239.157	172.20.239.18	SUCCESS	Successfully set config	Jun 14, 2022, 9:22:00 AM	:
sid-ewlc-3	172.20.239.157	172.20.239.38	SUCCESS	Successfully set config	Jun 14, 2022, 9:05:20 AM	:
Manage Co	ontroller				Sample configuratio	n
Setup IoT Serv Connector	ices stream authe	ntication and cert	tificate to allow A	Ps to connect with t	the Cisco DNA Space	es
The WI C will h	e configured to se	end notifications t	n Cisco DNA Sn	aces Connector for	AP configuration cha	naes
Cancel						

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

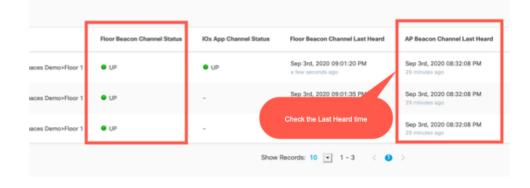
- **Step 1** In the Cisco Spaces dashboard left-navigation pane, choose **IoT Services > IoT Gateways > AP Gateway**.
- **Step 2** Click the **All APs** tab.

Figure 154: Verify APs

■ Cisco DNA Space	es	
Stats		
are Gateways	deployed	All APs Advanced BLE Gateway
AP Gateways (3)	ll APs (3)	
√ Filters Actions √		As of: Sep 14, 2020 4:50 PM 📿 Refre
Mac Address	Name	Description
c0:64:e4:22:ef:20	ap-9120-19	Cisco Catalyst 9120AX Series (IEEE 802.
IoT Services IoT Gateways Device Management Device Monitoring	\langle	

Step 3Verify 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



Verify Access Points

I



IoT Service (Wired)

• Overview, on page 143

Overview



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

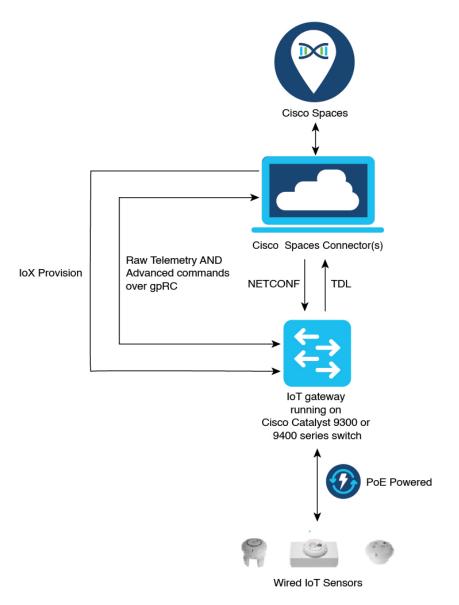
Integrating IoT service (wired) with the Cisco Catalyst 9300 and 9400 Series Switches series platform requires the following:

- 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.

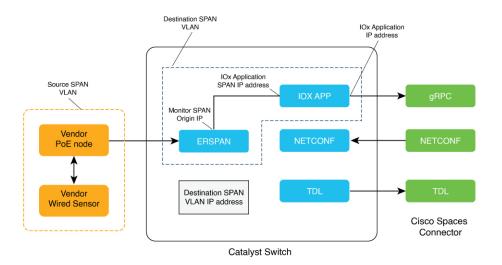


Note Cisco Catalyst 9300 and 9400 Series Switches require a local privilege level 15 user to use NETCONF. Additionally, the user must be a password-protected local user, because public-key authentication is not supported.

Design Prerequisites

Ensure you have the following information handy before proceeding:

Figure 157: Design Prerequisites

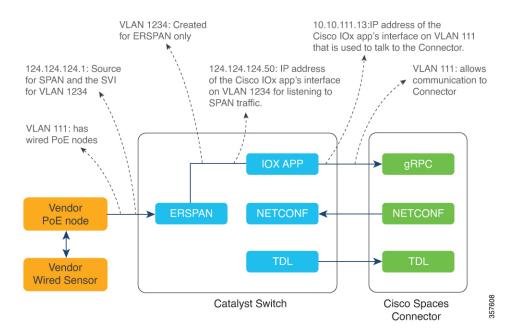


- **Destination SPAN VLAN**: The VLAN used to send Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic from Power over Ethernet (PoE) nodes to Cisco IOx App. You can use an existing VLAN or create a new one. This VLAN can also be local to the switch.
- **Destination SPAN VLAN IP address**: This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

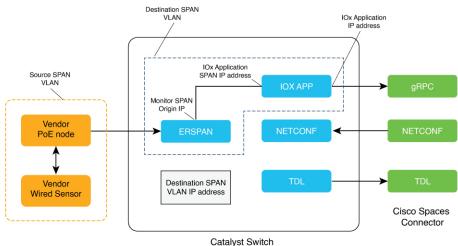
- Perform NTP synchronization across wireless controllers, Cisco Spaces: Connectors, and switches in the network.
- Enable NETCONF on Cisco Catalyst 9300 or 9400 Series Switches on port 830, along with permission to use NETCONF.

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:

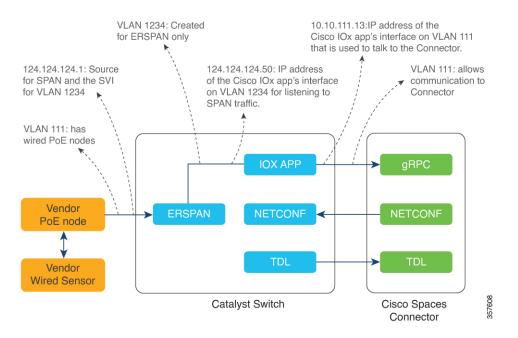
Figure 159: Design Prerequisites



- outaryot ownon
- **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.

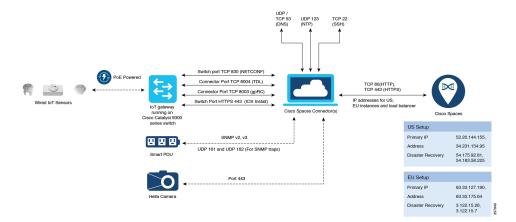
- **Destination SPAN VLAN IP address**: This is the Switched Virtual Interface (SVI) or the IP address of the destination VLAN that can be used to route traffic. If you are using an existing VLAN, you can provide the same IP address. We recommend that you create a new VLAN so that you can keep the ERSPAN 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.

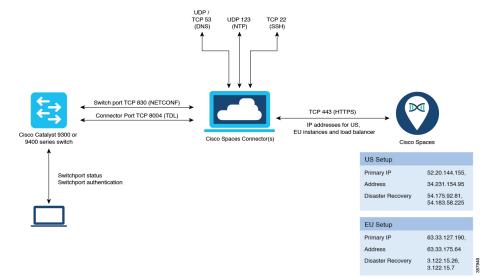
Figure 160: Sample Configuration



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	54.176.92.81
	34.231.154.95	54.183.58.225
EU Setup Type	63.33.127.190	3.122.15.26
	63.33.175.64	3.122.15.7
Singapore Setup (SG) Type	13.228.159.49	13.214.251.223
	54.179.105.241	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

E CISCO SPACE	15
贷 Setup	⊙ ess network
Wireless Network Wired Network Map Service	rks ces Connector ay to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.
Camera Sensors	es Connector OVA paces Connector OVA as a virtual machine.
Webex	Paces Connector Vou will need a tokan to configure Spaces Connector. You need to connect to https://-your connector IP-/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via 2 / 2 connector(s) active Create Connector View Connectors Add Controllers
	Add and associate controllers to your Cloco DNA Spaces Connector(s) 1 / 2 controller(s) active Add Controllers View Controllers View Controllers
(a)	Import Maps Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and prosimily Report 2 buildings imported Import/Sync Maps 2 foors Imported Map Upload History Manage Maps Manage Maps
5	Setup location hierarchy One the mass imposed was can add there into location hierarchy

Step 3 Click a connector 3 of your choice.

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

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

Figure 163: Add Services

←Back Setup > Connectors > Test	ID : 81424448212902120000 Last Modified : Apr 29, 2022, 11:04:25 AM
SUMMARY 0 0 0 0 0 0 0 Instances Active Inactive Service Switches enabled	
Instances Configuration Metrics	Senerate Token 🐵 Troubleshoot Connector
Services	Add Services
You have not added any services yet. Click * Add Service* to configure services. Switches You have not added any switches yet. Click * Add Switch* to configure switches.	Add Switch

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

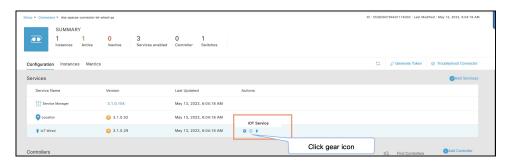
Figure 164: Adding a Service

←Back Setup > Connectors > Test		ID : 81424448212902	120000 Last Modified : Apr 29, 2022, 11:04:25 AM
SUMMARY 0 0 0 Instances Active Inactive	2 0 Services Switches enabled		
Instances Configuration Metrics		F	Generate Token 🛛 🎡 Troubleshoot Connector
Services			H Add Services
Service Name	Version	Las	t Updated
°¦o service-manager	2.8.0.123	Never	
.il iot-services	2.8.0.33	Never	
Switches		Add	Switch

In the **Connector Details** window, you can see that the **IoT Wired** service has been added. Click the gear icon near the **IoT Wired** row.

Step 6

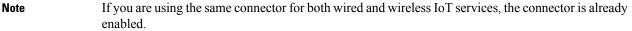
Figure 165: Gear Icon of IoT Wired



- **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

Manage loT Se	ervices				×
Manage Connecto Enable IoT Services on		ector			Configure to enable
Use Manual Configurati	on to setup IoT Serv	ices in switches w	hen the configuration ca	n not be applied automatica	ally.
Use the three dots action	on of Enable/Disable	Stream to apply c	onfiguration changes to	the switches.	
Switch Name	Connector IP	Switch IP	Operation Status	Operation Log	Last updated
catalyst-9300-qa-1	10.22.243.64	10.22.243.73	SUCCESS	Successfully set config	May 13, 2023, 7:07:10 AM
				with the Cisco Spaces Conr	
Canaal					



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

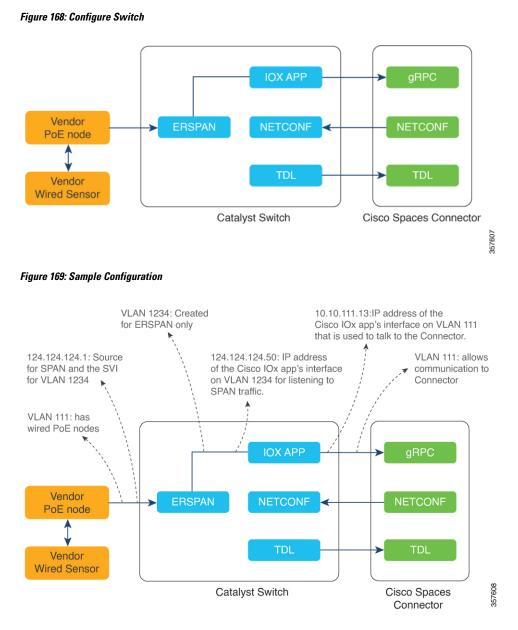
to the connector. This VLAN can be the same as the wired PoE node VLAN. The connector must be permitted to accept communications from the Cisco IOx application.

- **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

Configure Switch
Destination SPAN VLAN IP address
Enter the destination SPAN VLAN IP addres
Source SPAN VLAN list
Enter the source SPAN VLAN list
Use comma as a seperator for multiple vlan
Monitor SPAN origin IP address
Enter the Monitor SPAN origin IP address
IOx application SPAN IP address
Enter the IOx application SPAN IP address
Application Cisco Spaces Connector VLAN
Enter the application Cisco Spaces Connec
Use DHCP
IOx application IP address
Enter the IOx application IP address
IOx application netmask
Enter the IOx application netmask
IOx application gateway address
Enter the IOx application gateway address
Cancel Configure

I



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

Destination SPAN VLAN	
1234	
Destination SPAN VLAN IP address	
124.124.124.1	
Source SPAN VLAN list	vlan 1234
111	V01 1234
Use comma as a seperator for multiple vian	interface AppGigabitEthernet1/0/1 description Uplink to Application
Monitor SPAN origin IP address	switchport mode trunk
124.124.124.1	interface Vlan1234 ip address 124.124.1 255.255.255.0
IOx application SPAN IP address	iox
124.124.124.50	monitor session 44 type erspan-source
	source vlan 111 destination
Application DNA Spaces Connector VLAN	erspan-id 44 mtu 9000
111	ip address 124.124.124.50 origin ip address 124.124.124.1
Use DHCP	app-hosting appid cisco_dnas_wired_iow_app app-wnic_AppGigabiltChernet_trunk vian 111 quest-interface 0
IOx application IP address	guest-ipäddress 10.10.111.13 netnask 255.255.255.0 vlan 1234 guest-interface 1
10.10.111.13	guest-ipaddress 124.124.124.50 netmask 255.255.0 app-default-gateway 10.10.111.6 guest-interface 0
10.10.11115	app-resource dacker run-opts 1 "-e GAPC_SEMVER_TP=10.10.111.0" run-opts 2 "-e GAPC_SEMVER_PORT=0003"
IOx application netmask	<pre>rum-opts 3 "-e GRPC_SERVER_TOKEN-eyJhbGc101JTUZIINIISToR5c rum-opts 4 "-e APP_HOST_ID=c0:14:fe:81:c0:00"</pre>
255.255.255.0	run-opts 5 "-e APP_HOST_IP-18.18.111.26"
IOx application gateway address	
10.10.111.6	

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

Manage IoT S	Services					ê ×
Manage Connector Success Configure to enable Enable IoT Services on Cisco DNA Spaces Connector						
Use Manual Configur	Use Manual Configuration to setup IoT Services in switches when the configuration can not be applied automatically.					
Use the three dots action of Enable/Disable Stream to apply configuration changes to the switches.						
Switch Name	Connector IP	Switch IP	Operation Status	Operation Log	Last updated	
catalyst-9300-qa-1	10.22.243.64	10.22.243.73	SUCCESS	Successfully set config	Jun 3, 2021, 1:00:34 PM	:
First Previous 1 Ne	ext Last				(1 - 1 of 1)	: 1 pages
Manage Switch					Sample configur	ration
Setup IoT Services s	tream authenticat	ion and certificat	e to allow switches to	connect with the Cisco	DNA Spaces Connector	
Manage IoT S	being		iew the list of on the switcl			×
Action	Sta	tus Mess	age	Start Time	Finish Time	
Enable IOx	SU	CCESS Succ	essfully set config	Jun 3, 2021, 1:00:34 PM	Jun 3, 2021, 1:00:36 PM	1
Switch monitor configu	ration SU	CCESS Succ	essfully set config	Jun 3, 2021, 1:00:36 PM	Jun 3, 2021, 1:00:38 PM	1
IOx application configu	ration SU	CCESS Succ	essfully set config	Jun 3, 2021, 1:00:38 PM	Jun 3, 2021, 1:00:41 PM	C.
Disable Stream Lo	ogs					
Action	Status	Message	e	Start Time	Finish Time	
			No Data Found			

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

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

Procedure

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

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

```
Figure 172: View Switches
```

You will need a token to configure Spaces Connector. You ne optionally configure Spaces Connector to connect via HTTPS	ed to connect to https:// <your connector="" ip="">/ from a browser to configure the to proxy.</your>
1 / 1 connector(s) active	Create a new token View Connectors
Add Switch	
Associate Switches with Cisco DNA Spaces Connector(s)	
3 Switches added	Add Switches
	View Switches
Import Maps	

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

Figure 173: View Switches

≡ Cis	co DNA Spaces			0	Θ
	← Switches		+ Create New Switch		
	Name	Connector			
	catalyst-9330-dev-1	dna-spaces-connector-iot-wired-qa			
	First Previous 1 Next Last		(1 - 1 of 1): 1 pag	ges	



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

≡ CISCO SPACE	S
贷 Setup	⊙ ess network
Wireless Networ Wired Network Map Service	ks ces Connector ay to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.
	es Connector OVA Spaces Connector OVA as a virtual machine. medior (3)
	You will need a token to configure Spaces Connector. You need to connect to https://syour connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS prov. 2 / 2 connector(s) active Create Connector
3	Add Controllers Add and associate controllers to your Clicco DNA Spaces Connector(s) Add Controllers Add Controllers
•	1 / 2 controller(s) active View Controllers View Controllers Import Maps Prim/DVAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report
	2 buildings imported Import/Symc Maps 2 filoors imported Map Upload History Manage Maps Manage Maps
5	Setup location hierarchy Once the maps imported, you can add them into location hierarchy

Step 3In the connector details window that is displayed, choose a connector and click Add Services.Figure 175: Add Service

←Back Setup > Connectors > Test	ID : 81424448212902120000 Last Modified : Apr 29, 2022, 11:04:25 AM
SUMMARY 0 0 0 0 0 0 Instances Active Inactive Service enabled	
Instances Configuration Metrics	🖉 Generate Token 🛛 🍪 Troubleshoot Connector
Services	Add Services
You have not added any services yet. Click *Add Service* to configure services. Switches	Add Switch
You have not added any switches yet. Click "Add Switch" to configure switches.	

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

Note service-manager is added by default.

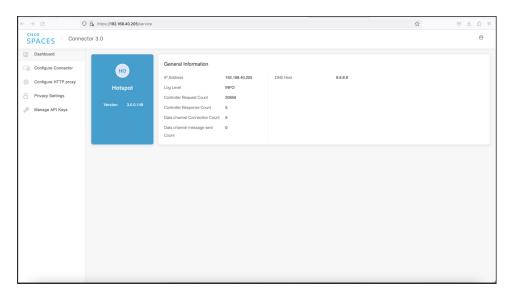
In the Connector Details window, you can see that the number of services enabled has increased.

Connector Dashboard: Hotspot service

Figure 176: Hotspot Service

SPACES Connecto	r 3.0					Θ
Configure Connector Configure Connector Configure HTTP proxy Privacy Bettings Privacy Bettings Manage API Keys	Connector 3.0 Marcella P.2.00 Marcella	Connector TestConne Name 1 - 2005 Description - 2005 Description - 2005 Description - 2005 Server - 8.8.8.8 Connector 2.2 % Q 5.6 % Q 5.6 % Q 5.6 % D 5.5 1 MB Q	etor3.0 Domain Gateway Proxy 332465690000 Netmask NTP	cisco.com 192 168.40.1 Nor Analistic 295.255.250 10.66.141.50 294.4 % O Up O 0.5 5d 6h 41m 35c O	NTP Status	active (unning)
	Control Channel	4d 20h 28s ① Up	hotspot 3.0.0.149 Upgrade: Success Last Heartbeat Running Status	7s ago UP	C	Looking for other services?
	CPU Usage (%) Memory Usage (%)	3.34 % ① 2.67 % ①	Up time Request Count	4d 19h 50m 9s ① 20787 ①		Follow steps below to add services

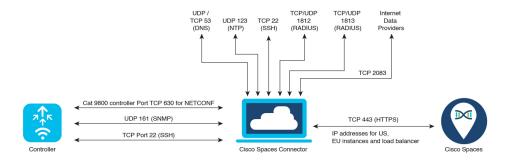
Figure 177: Hotspot Service: Details



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.



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.



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

E CISCO SPACE	is a second s
贷 Setup	© ess network
Wireless Netwo Wired Network Map Service	rks ces Connector ay to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.
	es Connector OVA spaces Connector OVA as a virtual machine.
	Vo will need a token to configure Spaces Connector. You need to connect to https://-your connector IP-/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS prox.
3	Add Controllers Add and associate controllers to your Claco DNA Spaces Connector(s) 1 / 2 controller(s) active Add Controllers View Controllers
•	Import Maps Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report
	2 buildings imported Import/Sync Maps 2 floors Imported Manage Maps
5	Setup location hierarchy Once the maps imported, you can add them into location hierarchy

Step 3In the connector details window that is displayed, choose a connector and click Add Services.Figure 180: Add Service

←Back Setup > Connectors > Test	ID : 81424448212902120000 Last Modified : Apr 29, 2022, 11:04:25 AM
SUMMARY 0 0 0 0 0 0 0 Instances Active Inactive enabled Switches	
Instances Configuration Metrics	🖉 Generate Token 🛛 🎄 Troubleshoot Connector
Services	Add Services
You have not added any services yet. Click "Add Service" to configure services. Switches	Add Switch
You have not added any switches yet. Click "Add Switch" to configure switches.	

- **Step 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 5Login to the Connector GUI. Scroll downwards to the local-firehose tile. Verify if the running status is Up.Figure 181: local-firehose

local-firehose 3.1.0.0 Upgrade: Success	69
Last Heartbeat	6s ago
Running Status	Up
Up time	16m 11s 🛈
Outgoing TAG RSSI events rate	36.46 events/second (i)
Incoming TAG RSSI events rate	53.09 events/second 🛈
Outgoing BLE RSSI events rate	14.26 events/second (i)
Incoming BLE RSSI events rate	20.38 events/second (i)
Active gRPC Connection Count	1 count 🛈
gRPC Server Channel Status	RUNNING Status 🛈
Show Less	
Disk Usage (%)	11.41 % 🛈
Disk Size	233.69 MB 🛈
CPU Usage (%)	45.33 % i
Memory Usage (%)	5.97 % 🛈
Memory Usage	475.11 MB 🛈

Connector Dashboard: Local Firehose Service

Figure 182: Local firehose service: Details on the Connector

local-firehose Upgrade: Success	3.1.0.65
Last Heartbeat	2s ago
Running Status	Up
Up time	1h 4m 28s 🛈
Outgoing TAG RSSI events rate	0 events/second ①
Incoming TAG RSSI events rate	0.02 events/second 🛈
Outgoing BLE RSSI events rate	0 events/second ①
Incoming BLE RSSI events rate	0 events/second ①
Active gRPC Connection Count	0 count 🛈
gRPC Server Channel Status	RUNNING Status 🛈
Show Less	
Disk Usage (%)	0.43 % 🛈
Disk Size	8.84 MB (i)
CPU Usage (%)	0.1 % 🛈
Memory Usage (%)	8.16 % 🛈
Memory Usage	320.17 MB 🛈

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

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 Cise	co Spaces.

Note	The Cisco	Spaces	URL	is 1	region-	depende	ent.
------	-----------	--------	-----	------	---------	---------	------

- **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

ace.	Connector is an easy way to get your wireless network connected to	Cisco DNA Spaces. No need to upgrade Wireless LAN Contr
)	Install Spaces Connector OVA	
	Download and install Spaces Connector OVA as a virtual machine. Download Spaces Connector (2*	
)	Configure Spaces Connector	
	You will need a token to configure Spaces Connector. You need to connect token. You can optionally configure Spaces Connector to connect via HTT	
	0/46	Create a new token
	0 / 46 connector(s) active	View Connectors
)	Add Controllers Add and associate controllers to your Cisco DNA Spaces Connector(s)	
	0 / 14 controller(s) active	Add Controllers View Controllers
)	Import Controllers into Location Hiera Once the controllers are added, you can import them into your location his point.	•
	0 / 14 controller(s) imported to location hierarchy	Import Controllers View Location Hierarchy

- **Step 6** From the **Connector** drop-down list, choose a Connector.
- Step 7 Enter the Controller IP address and Controller Name, and from the Controller Type drop-down list, choose WLC (AireOS) to connect to an AireOS controller.

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

• If you choose the **SNMP** version as **v2C**, specify the SNMP read-write community.

- If you choose the **SNMP** version as v3, specify the SNMP v3 version username, password, and authentication protocol credentials. Ensure that SNMP v3 has read-write permissions in the AireOS controller.
- **Note** Both SNMP v2c and SNMP v3 must have read-write permission in the AireOS controller to register the Connector certificate in the AireOS controller. The Connector doesn't support SNMP v1.

Add Controller		
Controller Type		
WLC (AireOS)	^	
Controller SNMP Version		
v3	^	
Username		
-		
Authentication Protocol		
HMAC-MD5	^	
Password		
		SHOW
Privacy Protocol		
CBC-DES	^	
Privacy Password		
		SHOW
Test Connectivity Ping test	to the co	ntroller is successful. But SNMP test has failed. Please check
 Is SNMP enabled on the oligon of the connector reach Can the connector reach Are correct SNMP RW crosses 	SNMP por	rt 161 on the controller?
Save & Close Save & A	dd Next Co	ontroller

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 <i>not</i> 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

Controller Channel					
TDL Incoming Msg Rate	0.00 events/second				
TDL Incoming Msg Count	281				
IP Address 🌲	Connected At 🌻	Msg Rate/Second 🗘	Status 🌲		
172.20.239.41	Wed, Jul 29th, 2020	29	ACTIVE		

What to do next

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



APPENDIX

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.



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

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
```

	Associate	≥d	Trustpoints:	manual	certs
	Storage:	n٦	vram:supportv	vlcc#E3E	E4CA.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 4To 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

tor x. You need to connect to https:// <your connector="" ip="">/ from a browser to connect to connect via HTTPS proxy. active create a new token View Connectors active Add Controllers Intervention</your>
active Create a new token View Connectors
active View Connectors Add Controllers
active Add Controllers
Add Controllers
Add Controllers
active
active
View Controllers
view Controllers

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

- **Step 6** From the **Connector** drop-down list, choose a Connector.
- **Step 7** Enter the **Controller IP** address, **Controller Name**, and from the **Controller Type** drop-down list, choose **Catalyst WLC** to connect to a Cisco Catalyst 9800 Series Wireless Controllers.
 - **Note** Ensure that the Controller IP address is not in the same subnet as the docker service network. You can validate this from the Connector CLI, where you can issue the **connectorctl dockersubnet show** command to verify the subnets used.
- **Step 8** Do one of the following:
 - Enter **Netconf username**, **Netconf password**, and **Enable password**. This choice allows the Connector to recover gracefully from NMSP drops and push a fresh configuration to the Catalyst 9800 controller whenever required. If you have not configured an **enable** password in Catalyst 9800 controller you can skip configuring the **Enable** password in this step.
 - Copy the configuration commands in the **Catalyst WLC CLI commands** section and run them manually on the Catalyst 9800 controller CLI.
- **Step 9** (Optional) Run the PING and SSH functionalities to test the reachability to the Catalyst 9800 controller and the credentials by clicking **Test Connectivity**. Note that **Test Connectivity** is available only for an active Connector.

Figure 187: Add a New Catalyst 9800 controller

Add Controller		
Controller Name		
Controller Type Catalyst WLC / Catalyst 9800		
Netconf Username		
Netconf Password	SHOW	
Enable Password	SHOW	
atalyst WLC CLI Commands		
aaa new-model username dca9048dd2f8 mac aaa attrib	Lute list cmx_dca9048dd2f8	
aaa attribute list cmx_dca9048dd2f8 attribute type password 7e634b76188bf588d9a0922635d8bfd	bd5eb882b5c159df64984bc4579ab8b8c	
aaa authorization credential-download w	/cm_loc_serv_cert local	
Test Connectivity Connectivity test is	successful	
Save & Close Save & Add Next Co	ontroller	

Table 9: Error Description

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

I

Status of PING	Status of SSH Credential Test	Meaning of status message combination and possible checks.	
SUCCESSFUL	FAILED	Ping test to the Catalyst 9800 controller is successful. But SSH test has failed. Check the following:	
		a. Is SSH enabled on the controller?	
		b. Is the SSH port 22 of the Catalyst 9800 controller reachable from the Connector?	
		c. Have you provided accurate SSH read-write credentials?	
FAILED	SUCCESSFUL	Connectivity test is successful.	
FAILED	FAILED	Both Ping and SSH test to the Catalyst 9800 controller have failed. Check the following:	
		a. Is there IP connectivity between Connector and controller?	
		b. Is SSH enabled on the Catalyst 9800 controller?	
		c. Is the SSH port 22 of the Catalyst 9800 controller reachable from the Connector?	
		d. Have you provided accurate SSH credentials?	
		e. Is AAA enabled with local authentication?	
		f. Are you using an interface that is NOT the wireless management interface for NMSP and SSH connectivity?	

Step 10 Click **Save**, and then click **Close**.

You can see the new Catalyst 9800 controller in the **Controller Channel** area of the Connector GUI. The Catalyst 9800 controller that is connected successfully to the Connector appears as **Active**. It takes approximately five minutes for the wireless controller to change to the **Active** state. Refresh your window to view the status change. The added Catalyst 9800 controller is also listed in the **Controller Channel** area of the Connector.

Figure 188: Details of the Catalyst 9800 controller

Controller Channel			
TDL Incoming Msg Rate	0.00 events/second		
TDL Incoming Msg Count	281		
IP Address 🌲	Connected At 🌻	Msg Rate/Second 🌻	Status 🌲
172.20.239.41	Wed, Jul 29th, 2020	29	ACTIVE

You can multiple Catalyst 9800 controllers to a Connector.

What to do next

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



APPENDIX

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

DETAILED STEPS

Procedure

- **Step 1** Login to Cisco Spaces.
- **Step 2** In the Cisco Spaces dashboard, choose **Setup > Wired Networks**.
- Step 3 From the Step 3: Add Switches area, click Add Switch.

1	Install Spaces Connector OVA Download and install Spaces Connector OVA as a virtual mac Download Spaces Connector C	hine.
(2)	Configure Spaces Connector You will need a token to configure Spaces Connector. You ne optionally configure Spaces Connector to connect via HTTPS	ed to connect to https://cyour connector IP>/ from a browser to configure the token. You can proxy.
	1 / 1 connector(s) active	Create a new token View Connectors
3	Add Switch Associate Switches with Cisco DNA Spaces Connector(s)	
] Switches added	Add Switches View Switches
4	Import Maps If you have wired devices and sensors plotted Prime/DNAC ye	ou can import them in to the location hierarchy
	2 buildings imported	Import/Sync Maps Map Upload History
Fiaure 189:	2 floors imported	Manage Maps

- **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