cisco.



Cisco Spaces: Connector 3 Configuration Guide

First Published: 2022-06-24 Last Modified: 2024-04-04

Americas Headquarters

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883 THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

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

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

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

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

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

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

© 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 20
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 109		
	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) 135		
	Open Ports for IoT Service (Wireless) 137		
	Configure IoT Service (Wireless) 137		
	Verify IoT Streams for Catalyst 9800 Controller 139		
	Verify Access Points 140		

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 161
	Configure Hotspot Service 161
	Connector Dashboard: Hotspot service 162
	Open Ports for Hotspot Service 163
CHAPTER 18	Local Firehose 165
	Local Firehose Service 165
	Configure Local Firehose Service 165
	Connector Dashboard: Local Firehose Service 168
APPENDIX A	Connect Connector to Cisco AireOS Wireless Controller 171
	Configure and Test Connectivity Between a Connector and AireOS Controller 171
APPENDIX B	Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers 177
	Configure and Test the Connection Between Connector and Catalyst 9800 Controller 177
APPENDIX C	Connect Connector to Cisco Catalyst 9300 or 9400 Series Switches 183
	Connecting a connector to Cisco Catalyst 9300 and 9400 Series Switches 183

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.
$\{x \mid y \mid z \}$	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 $\tt courier$ 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.
4	
Means reade	r take note. Notes contain helpful suggestions or references to material not covered in the manual.
Means the fo	llowing information will help you solve a problem.
2	
Means reade or loss of da	r be careful. In this situation, you might perform an action that could result in equipment damage

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 20

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 137.
IoT service (wired)	For information, see Configure IoT Service (Wireless), on page 137.
Hotspot service	For information, see Configure Hotspot Service, on page 161.
Local firehose service	For information, see Configure Hotspot Service, on page 161.

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

Step 1 Log in to Cisco Spaces.

Note The Cisco Spaces URL is region-dependent.

- **Step 2** From the left navigation pane, choose **Setup > Wireless Networks**.
- Step 3 In the Get your wireless network connected with Cisco DNA Spaces area, click Add New.
- Step 4 In the Cisco AireOS Controller/Catalyst 9800 Wireless Controller area, click Select.

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

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

 Figure 2: Via Spaces Connector

```
Connect your wireless network

How do you want to connect to Cisco DNA Spaces?

Via Spaces Connector

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		
Connect via Sp Spaces Connector is an east	paces Connector y way to get your vitreless network connected to Cisco DNA Spaces. No need to upgrade Wiveless LAN Control	ers or reconfigure your wireless network.	
Connect WLC/	Catalyst 9800 Directly	eless LAN Controllers or reconfigure your wireless network.	expand ~
reless Networks	ering		~
	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 Every and the every and the		
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 Services Switches enabled	
Instances Configuration Metrics	
, ,	
Configure your instance	
Configure your instance To set up high availability pair follow the steps below. Step 1:	
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 11 In the **Token** window that is displayed, click **Copy Token**.

Figure 9: Copy Token

Token
Configure the token below on your instance/box
eyJhbGciOiJIUzI1NiIsInR5cCl6lkpXVCJ9.eyJ2ZXJzaW9uljoiVjMiLCJ0b2tlbklkljoiNzM3MTlyYTAtY2I3MS0xMWVjLWFm YmUtMTU4MTA0NjY3NjQwliwiaWJ5ljoiTG9jYXRpb24iLCJ0eXBlljoiY29ubmVjdG9yX2F1dGhfdG9rZW4iLCJ0ZW5hbnR JZCl6ljEyMTExliwiY29ubmVjdG9ySWQlOjgxNDl0NDQ4MjEyOTAyMTlwMDAwLCJlbmRwb2ludCl6lmh0dHBz0l8vY29u bmVjdG9yLnFhLWRuYXNwYWNlcy5pbylsImVudmlyb25tZW50ljoidGvzdClsInJIZ2lvbil6lnVzLWVhc3QtMSIsImlhdCl6M 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



- **Step 15** In the window that is displayed, in the **Token** text, field enter the token copied from Cisco Spaces and click **Configure**.
- **Step 16** Add the following services as required:
 - Configure IoT Service (Wireless)
 - Configure Hotspot Service

Upgrading the Connector from Cisco Spaces Dashboard

Use the connector's GUI to upgrade connector. 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.

Step 1 Log in to Cisco Spaces.

Note The Cisco Spaces URL is region-dependent.

- **Step 2** In the Cisco Spaces dashboard, choose **Setup > Wireless Networks**.
- Step 3 From the 2. Configure Spaces Connector area, click View Connectors

Figure 11: View Connectors

Configure Spaces Connector	
configure spaces confiector	
You will need a token to configure Spaces Connector. You nee an optionally configure Spaces Connector to connect via HT	ed to connect to https:// <your connector="" ip="">/ from a browser to configure the token. You TPS proxy.</your>
0.16	Create Connector
U / U connector(s) active	View Connectors
Add Controllers	
Add and associate controllers to your Cisco DNA Spaces Cor	nnector(s)
0.12	Add Controllers
U / S controller(s) active	View Controllers
mport Maps	
Prime/DNAC map requires in order to work Locate & detect, a	Asset tracker, and IOT services, and proximity Report
1 buildings imported	Import/Sync Mans
	Map Upload History
3 floors imported	Manage Maps
Setup location hierarchy Once the maps imported, you can add them into location hier	archy
	Add Locations
	You will need a token to configure Spaces Connector. You ne can optionally configure Spaces Connector to connect via HT O / 6 connector(s) active Add Controllers Add and associate controllers to your Gisco DNA Spaces Con O / 3 controller(s) active Import Maps Prime/DNAC map requires in order to work Locate & detect, 1 buildings imported 3 floors imported Betup location hierarchy Once the maps imported, you can add them into location hier

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

			∷ ⊘ ∈
Setup > Connectors > upgradeTest		ID : 3000948	8891381166000 Last Modified : May 11, 2023, 12:04:11 AM
SUMMARY 1 1 0 Instances Active Inactiv	2 0 0 ve Services enabled Controller Switches		
Configuration Instances Metrics		0	🖉 Generate Token 🛛 🍈 Troubleshoot Connector
System Upgrade Available! 0 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: corrector3-p83- sep2022	0		
Mac ID	00:50:56:a7:8c:c6		
IP Address	10.89.45.100		
Status	G Up		
Control Channel Status	Connected		
HA Status	Not Paired		
VIP Address	NA		
SERVICES			

- **Note** For connectors operating with Service manager service 3.0, 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.
- **Step 8** From the popup displayed, select the instance you want to upgrade.

≡ cisc	O SPACES						
Setup >	Connectors > upgradeTest						ID : 3000948889138
	SUMMARY						
₫	1 1 0 Instances Active Inact	2 tive Services enabled	0 0 Controller Swit	ches			
Conf	figuration Instances Metrics						
	System Lingrade Available!		_			_	
4	We have updated the system library and have see	urity fixes in the release. click here to see	a the rele-		•	×	
Inet	ances in High Availability Pair						
mot				Pleas	e select the instance to upgrade.		
	<u>ئۆچ</u> 005056a78cc6			۲	005056a78cc6		
	System Package: connector3-p83- sep2022						
	Mac ID	00:50:56:a7:8c:c6					
	IP Address	10.89.45.100			Upgrade		
	Status	🚯 Up					
	Control Channel Status	Connected					
	HA Status	Not Paired					
	VIP Address	NA					

Figure 13: Select instance

An Upgrade Initiated for instance message is displayed.

Figure 14: Upgrade Initiated for Instance



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

Figure 15: Configuration History

		Instance	s Ac	tive	Inactiv	e	Service enabled
(Configuratio	n Insta	nces	Metrics			
	Instances in	n High A	vailabi	lity Pair			
	 O P Mac IE IP Add Status 	05056a System Package: connector3 84-nov202 upgrade1	754a5 Restart Restart Refresh Remove Configu	Services Connecto Instance	• I I I I I I I I I I I I I I I I I I I	:	
	Contro Status	l Channel	Cor	nnected			

Figure 16: Configuration History

	005056a754a5: Service o	configuration history	\times
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. 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 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.

Step 1 Log in to the connector CLI.

progress

- **Step 2** Check the availability of upgrades, and view a summary of the changes that are part of this upgrade package. Run the **connectorctl systemupgrade list** command.
- **Step 3** Initiate the upgrade of connector packages. Run the **connectorctl systemupgrade install** command:

[spacesadmin@connector03 ~]\$ connectorctl systemupgrade install Executing command:systemupgrade Command execution status :Success System upgrade operation is queued. Use tail -f /opt/spaces-connector/runtime/logs/service-manager/system-upgrade/system-upgrade. log to see upgrade

- **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.

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.

& ⑦ Ohio ▼ aws III Services Q New EC2 Experience AMI Catalog An AMI is a template t EC2 Dashboard EC2 Global Viev Events AMIs Tags Limits Q DNA Spaces Connector Instance Quickstart AMIs (0) My AMIs (0) Instances New nity AMIs (1) Instance Types Launch Templa Spot Requests Refine results Savings Plans Sort By: Rel Reserved Instance Categories Dedicated Hosts co DNA . Tisco [| 1 Infrastructure So cisco Capacity Reserv Publisher Cisco (1) 1 A c AMI Catalog Bring Your Own License (1) Elastic Block St Operating system All Linux/Unix Snapshots New Lifecycle Manag 64-bit (x86) (1) Network & Security Security Groups Ecompute Optimized Elastic IPs

Figure 17: Configuration

- **Step 3** Click the displayed image and click **Select**.
- Step 4 In the Cisco DNA Spaces Connector window displayed, click Continue.

Figure 18: AWS MarketPlace AMIs

ahaha cisco	Cisco DNA Spaces Connecto Cisco Systems, Inc. 🖄 Cisco Systems, Inc. 🖄 O AWS reviews 🖾 Bring Your Own License	r	,
Overview	Product details Pricing	Usage Support	
The Cisco DNA without missin	Spaces: Connector enables Cisco DNA g any client information	Spaces to communicate with multiple controllers eff	iciently, by allowing each controller to transmit client dat
Typical total p. \$0.093/Hr Total pricing per us-east-1. <u>See additional pr</u>	rice instance for services hosted on t2.large in icing information.	Catest Version Cisco DNA Spaces Connector3 October2023 Delivery methods Amazon Machine Image ① Operating systems Other AlmaLinux 8 CentOS 7	Video Product Video 🛃 Categories Network Infrastructure

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

Figure 19: Launch Instance from AMI

EC2 > AMIs > ami-0fd326aca1b04cf96			
Image summary for ami-0fd326aca1b04cf96 ((Connector3-b84-Jan-QA-Img)	EC2 Image Bu	ilder Actions v Launch instance from AMI
AMI ID D ami-Ofd326aca1b04cf96 (Connector3-b84-Jan-QA-Img)	Image type machine	Platform details Linux/UNIX	Root device type EBS
AMI name Comparison of the second se	Owner account ID	Architecture x86_64	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 Block devices devices devices devices Block devices	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

	Q Search				[Option+S]	
Launch Amazon EC2 following the	allows you to simple steps	tance Info create virtual ma below.	chines, or instances	, that run on the A	WS Cloud. Quick	kly get started by
Name a	nd tags In	fo				
Name						
Connect	or3-AMI-Dev-	nstance-1			Add	additional tags
				n and OS Images		
Amazo	I from catalo	Recents	My AMIs	Quick Start		
Amazo	I from catalo n Machine Im tor3-packer-a	Recents age (AMI) lmalinux-ami-dev	My AMIs	Quick Start	Pro	Q
Amazo connec ami-08	I from catalo n Machine Im tor3-packer-a dd6727207b	g Recents age (AMI) Imalinux-ami-dev 87c54	My AMIs	Quick Start	Bro Inc Aws	Q wse more AMIs luding AMIs from 6, Marketplace and the Community
Am Amazo connec ami-08 Pub	I from catalo n Machine Im tor3-packer-a dd6727207b lished	Recents age (AMI) Imalinux-ami-dev 87c54 Architecture	My AMIs v	Quick Start Root device	Bro Inc AWS T ENA Enabled	Q wse more AMIs luding AMIs from 5, Marketplace and the Community
AM Amazo connec ami-08 Pub 202 16T	I from catalo n Machine Im tor3-packer dd6727207b lished 2-12- 00:18:58.0	Recents age (AMI) Imalinux-ami-dev 37c54 Architecture x86_64	My AMIs V Virtualization hvm	Quick Start Root device type ebs	Bro Inc AW T ENA Enabled Yes	Q wse more AMIs luding AMIs from 5, Marketplace and the Community
Am Amazo connec ami-08 Pub 202 16T 00Z	I from catalo n Machine Im tor3-packer-a dd6727207b lished 2-12- 00:18:58.0	Recents age (AMI) Imalinux-ami-den 37c54 Architecture x86_64	My AMIs V Virtualization hvm	Quick Start Root device type ebs	Bro Inc AWS T ENA Enabled Yes	Q wse more AMIs luding AMIs from 5, Marketplace and the Community

Step 7Choose an instance with the corresponding Type as t2.medium that has vCPU value as 2 and Memory (GB) as 4.
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]
=	/ Instance type Info
	istance type
	t2.medium Family: t2 2 vCPU 4 GiB Memory ▼ Compare instance types On-Demand Linux pricing: 0.0464 USD per Hour On-Demand Windows pricing: 0.0644 USD per Hour
	 Y Key pair (login) Info You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
	ey pair name - required
	connector-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	
ubnet Info					
ubnet Info subnet-		el			
Subnet Info subnet- VPC: vpc-02	Owner: 199547563901	eV	•	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				
1x 120 GiB gp2 Root volume (Encrypted) Add new volume GiB GiB				
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 :	one)
	Auto-assign public IP Info Enable	
	Firewall (security groups) Info A security group is a set of firewall rules that control the t instance.	affic for your instance. Add rules to allow specific traffic to reach your
	Create security group	Select existing security group
	Security groups Info	
	Select security groups	Compare security
	launch-wizard-69 sg-(' X	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

lr I	bound rules (6 Q Filter security gr	5) roup 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	ТСР	8000
	-		sgr-02070569e30bbd	IPv4	Custom UDP	UDP	161
	-		sgr-0bb0c8051cee0daf8	IPv4	SSH	ТСР	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	Tags			
3 You can now	check network connectivity	y with Reachability Analyzer		Run Reac	hability Analyzer 🛛 🗙
Outbound ru	les (1/1)			C Manage tags	Edit outbound rules
IP version	▼ Type	▼ Protocol	▽ Port range	▽ Destination	 ✓ Description
IPv4	All traffic	All	All	0.0.0/0	-

- **Note** For various connector services to work, you must open specific ports. See the respective **Information About Open Ports** section of the connector service for more information.
- **Step 11** In the displayed **Select an existing key pair or create a new key pair** dialog box, do either of the following:
 - Choose **Create a new key pair** from the drop-down list. Provide a **Key pair name** and click **Download Key Pair** to download it. Then click **Launch Instance** to launch the instance.
 - Choose **Choose an existing key pair** from the drop-down list. Select the previously downloaded key pair from the **Select a key Pair** drop-down list. Then click **Launch Instance** to launch the instance.

1. St	Choose AMI 2. Choose Instar	ance Launch	stance 4. Add Blonge 6. Add Tags 6. Configure Security Group 7. Review				_
	All selected security group	is inbound rules					
	Туре ()	Protocol		D	escription (i)		
	HTTP	TCP	Select an existing key pair or create a new key pair ×				
	HTTP	TCP		10			
	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	to obtain the password used to log into your instance securely. For Windows AMIs, the private key file allows you to				
	Custom TCP Rule	TCP	securely SSH into your instance.				
	Custom TCP Rule	TCP	Note: The coloring to coloring the order to the est of train without of factble instance. Lower more				
	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 AML.				
	SSH	TCP	Create a pour key pair				
	HTTPS	TCP	Key pair name				
	HTTPS	TCP	Key1				
	All ICMP - IPv4	All	Download Key Pair				
	All ICMP - IPv4	All					
Þ	Instance Details		You have to download the private key file (".pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.			Edi	t instance details
Þ	Storage						Edit storage
Þ	Tags		Cancel Launch Instances				Edit tage

Figure 27: Create a New Key Pair

Figure 28: Choose an Existing Key Pair

ose AMI 2. Choose Instance	Type 3. Configure In	stance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review			
7: Review Instar	nce Launch				
selected security groups in	nbound rules				
ype (i)	Protoco		Description (i)		
ITTP	TCP	Select an existing key pair or create a new key pair ×			
TTP	TCP		-		
ustom 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 pairs for a public start			
ITPS	TCP	Select a key pair			
TTPS	TCP	ConnectorAMI			
I ICMP - IPv4	All	I acknowledge that I have access to the selected private key file (ConnectorAMI.pem), and			
I ICMP - IPv4	All	that without this file, I won't be able to log into my instance.			
tance Details		Cancel Launch Instances		Edit	instance de
orage	L				Edit sto
c					Edit

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

lumber of instances Info	
1	
oftware Image (AMI)	
isco-dna-spaces-connector3-b8read mo mi-0ff155022ef237286	ore
/irtual server type (instance type)	
2.medium	
irewall (security group)	
irewall (security group) WLC	
Firewall (security group)	
Firewall (security group) FWLC Fitorage (volumes)	
Firewall (security group) EWLC Storage (volumes) Volume(s) - 120 GiB	
 irewall (security group) WLC itorage (volumes) volume(s) - 120 GiB i Free tier: In your first year includes 750 hours of t2 micro (or t3 micro in the 	×
 irewall (security group) WLC itorage (volumes) volume(s) - 120 GiB Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) 	×
 Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per 	×
 Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of sparsbots, 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]	🔁 🔶 🕲 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 ♡ Instance	D Instance state v I Instance type v I Statu	s check Alarm status Availability Zone v Public IPv4 DNS v Public IPv4
Connector3-AMI-Dev-Instance-1 i-094538	13d1d19edf ⊘ Running @	2 checks passed No alarms + us-east-1f :
Instance: i-094538a13d1d19edf (Connector3-AMI-Dev-	Instance-1) =	© 1
Details Security Networking Storage Status che	cks Monitoring Tags	
▼ Instance summary Info		
Instance ID i-094538a13d1d19edf (Connector3-AMI-Dev-Instance-1)	Public IPv4 address pen address	Private IPv4 addresses
IPv6 address	Instance state	Public IPv4 DNS
-		🗇 er 🛛 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
D 'ublic IP]	🗇 itt) 🗹	③ Opt-in to AWS Compute Optimizer for recommendations. Learn more 🔀
IAM Role	Subnet ID	Auto Scaling Group name
-	0	-
▼ Instance details Info		
Platform	AMI ID	Monitoring
Linux/UNIX (Inferred)	(1 •	disabled
Platform details	AMI name	Termination protection

- **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

- **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+/)				Q Q		୭ ନ
Home > Create a resource >								
Marketplace	_							
Get Started				-				
Service Providers	D azure vmware solution	× (Publisher name : All X Product I	ype : All X Publisher Typ	ie:All >	Oper	ating Syste	em : All 🕆
Al-powered search	Al-powered search Azure benefit eligible only 💿 🗌 Azure services only							
	Showing 1 to 20 of 62 results for 'azu	re vmware solution'. Clear search						
Management								
Private Marketplace				veloCoud vmvare		\bigcirc		
Private Offer Management	Azure VMware Solution	VMware Site Recovery Manager (SRM)	VMware NSX Cloud	VMware SD-WAN in vWA	N	VMware I	SXi	
My Marketplace	Microsoft	VMware Inc.	VMware Inc.	VeloCloud		Microsoft S	entinel, Mi	crosoft Co
	Azure Service	SaaS	SaaS	Azure Application		Azure Appli	ation	
Favorites	Azure VMware Solution (AVS)	The industry-leading disaster	Consistent Networking and Security	VMware SD-WAN managed		VMware ES	ä	
My solutions	Defined Data Center (SDDC) with	recovery management solution.	Azure	application for virtual wAN				
Recently created	Microsoft Azure Cloud bare-metal							
Private plans		Starts at Free	Starts at Free	Starts at Free		Price varies		
Categories	Create \lor \heartsuit	Subscribe 🗸 🛇	Subscribe 🗸 🛇	Create \checkmark	\heartsuit	Create 🔨	/	Q
Compute (24)	R		RUN	RUN		RUN		
Security (23)	Ĩ	0	(NSA)	NoA		(NoX)		
Storage (21)	App Volumes: Apps on Demand	Azure Backup (Preview)	VMware NSX - Cloud Service Manager	VMware NSX - Policy Manager		VMware I Gateway	NSX - Puk	olic Cloud
	VMware Inc	Microroft Corporation	Where Inc.	Whate Inc		VMware In	-	

- **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.

Home > Create a resource > Market	Home > Create a resource > Marketplace >						
Create a private cloud							
Prerequisities Basics Tags	Review and Create						
Project details							
Subscription * 🕕	VM-Deployment	\sim					
Resource group * 🕕	Vmware-us-east2	\sim					
	Create new						

Figure 34: Create a private cloud

E Microsoft Azure	arch resources, services, and docs (G+/)	
Home > Create a resource > Marketp	lace >	
Create a private cloud		
Private cloud details	*	
Resource name * ①	Enter the name	
Location *	(115) Eart 115 2	
Location	(05) East 05.2	
Size of host * ①		
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	03	
	Find out how many hosts you need If you need more hosts, request a quota increase	
CIDP address block		
Provide IP address for private cloud for c	luster management. Make sure these are unique and do not overlap with any	
other Azure vnets or on-premise networ	(5.	
Address block for private cloud \star \odot	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 Prev	ious Next : Tags >	

- **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 *		
Size of Host		
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: 10.0.0/8, 172.16.0.0/12, 192.168.0.0/16	
	The address block cannot overlap any of the following restricted network blocke: 172.17.0.0/16	
	The address block cannot be smaller than a /22 network.	
Review and Create Pre-	vious 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	l VMware credentials ☆							×
Manage	« vCenter Server credentials							
🛖 Connectivity	Web client URL 🛈	https://10.0.2/						
Clusters Encryption	Certificate thumbprint ①	BDF72814F378C2ACD584B62200B71E7F4FD49C0D						
VMware credentials	Username 🛈	cloudadmin@vsphere.local	1					
📍 Identity	Deserved O							
Storage	Password ()							
Placement policies		Generate a new password						
+ Add-ons								
Workload networking	NSX-T Manager credentials							
i Segments	Web client URL ①	https://10.0.3/	1					
DHCP Port mirroring	Certificate thumbprint ①	B028477B779C37AEFA75S4A45D54958D9CFA5C36						
DNS	Username 🛈	cloudadmin D	1					
Internet connectivity	Brannard O							
Operations	Password		J					
 Run command Azure hybrid benefit Monitoring 		Generate a new password						

Note

Note that ESXi also inherits the vSphere credentials.

Creating an Azure Virtual Network

Before you begin

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

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

= Microsoft Azure	Search resources, services, and docs (G+/)
Home > ExpressRoute circuits > Create ExpressRout	e
Basics Configuration Tage Use Azure ExpressRoute to create p in a colocation environment. Estab facility, or directly connect to Azur VPN, provided by a network servic Learn more about Express Route ci Project details	Review + create vivate connections between Azure datacenters and infrastructure on your premises or ish connections to Azure at an ExpressRoute location, such as an Exchange provider from your existing WAN network, such as a multiprotocol label switching (MPLS) provider. routes
manage all your resources.	cepioyed resources and costs. Use resource groups like tolders to organize and
Subscription * ①	VM-Deployment \checkmark
Resource group * ①	Vmware-us-east2 V Create new
Instance details	
Region * ①	East US 2 V
Name * ①	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
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. <u>Learn More</u> [©]
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

Home > ExpressRoute circuits > 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
	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 🔎 Se	earch resources, services, and docs (G+/)	۶.	Ģ	Q	۲	0	R	avitiwar@cisco.com
Home > Create a resource > Market Create a virtual machi	place >							×
Basics Disks Networking M Create a virtual machine that runs Linux image. Complete the Basics tab then Re for full customization. Learn more G [*] Project details	Ianagement Monitoring Advanced Tags Review + create or Windows. Select an image from Azure marketplace or use your own customized view + create to provision a virtual machine with default parameters or review each tab							
Select the subscription to manage deplo your resources.	oyed resources and costs. Use resource groups like folders to organize and manage all							
Resource group * ①	(New) Resource group V Create new V							
Instance details								
Virtual machine name *								
Region * ①	(US) East US 2							
Availability options	Availability zone							
Availability zone *	Zones 1 V							
Security type	You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more of Trusted launch virtual machines Configure security features							
Review + create < Pr	revious Next : Disks >							R ¹ 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	arch resources, services, and docs (G+/)			Ģ	Φ	۲	0	R	avitiwar@cisco.com
Home > Vmware-us-east2									
Azure VMware-us-east2	VMware credentials 🔅								×
Search «									
Manage	vCenter Server credentials								
Connectivity	Web client URL ①	https://10.0.0.2/							
Clusters	Certificate thumbprint ①	BDF72B14F378C2ACD584B62200B71E7F4FD49C0D							
Encryption									
VMware credentials	Username 🕡	cloudadmin@vsphere.local							·
Identity Storage	Password ()	······							
Placement policies		Generate a new password							
+ Add-ons		· · · ·							
Workload networking	NSX-T Manager credentials								
Segments	Web client URL ①	https://10.0.3/	٦.						
T DHCP	Certificate thumbprint ①	B0284778779C37AEFA7554A45D54958D9CFA5C36							
Internet connectivity	Username 🛈	cloudadmin							
Operations	Password 🕤	······							
Run command		Generate a new password							
📮 Azure hybrid benefit									
Monitoring									

Figure 44: VMware Credentials

← C ▲ Not secure https://10.0.02/ui/app/host	:nav=h/um:vr	3 ESXi Hosts	1891-9ee0f043eea7	7/summary 🗔 💥 A	¹ 合 印 作 通 る	0 🤫
 Construction Cons	esxC of LC s of LC y of LC	Configure Perr Configure Perr Vers: Verweich Neweich Powerch Powerch Neweich Powerch P	454f8e8c47bf.eas iissions VMs Datast iissions 2013028 pe Re40 econ(R) Gold 6240 CPU @ 2.60 d b Description	Stus2.avs.azure.com tores Networks Updat Configuration Related Objects Custer	es CV Uses 30.73 OH Menny Uses 10.73 OH Menny Uses 10.73 OH Desc 30.73 OH Menny Uses 10.73 OH Desc 30.73 OH Menny Uses 10.73 OH Menny Men	Press: 62.52 Orbit Capasity: 63.35 Orbit Press: 656.09 630 Capasity: 765.4718 Capasity: 52.4718 Capasity: 52.4718
			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
- **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	uch
as a local hard dri	ve, a network share, or a CD/DVD drive.		
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

✓ III SJC-20	compute resource for this operation	 	
	vonding)		
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

We will reserve part of the resource	s of CPU and memory bas	ed on your OVA selection	on.	
Standard 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 dowr	n to		
	accept the lic	ense		
	agreemer	nt.		

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 co	nfiguration and di	sk files Management Ser	ver)			
elect virtual disk format /M Storage Policy	Thick Provisio	Datastor	e Default	~		
Disable Storage DRS for Name T	Storage	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

Step 10

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		
✓ 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

conn-3-244-99	
	Timezone setup Would you like to setup timezone? (blank for default value (UTC)) yes
	1. Africa - Press 1 2. America - Press 2
	3. Asia - Press 3 4. Australia - Press 4
	5. Europe - Press 5
	2
	1. America/Anchorage - Press 1 2. America/Buenos_Aires - Press 2
	3. America/Chicago - Press 3 4. America/Denver - Press 4
	5. America/Los_Angeles - Press 5 6. America/Device City - Press 6
	2. America/New_York - Press 7
	9. America/Regina - Press 9
	10. Hmerica/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

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.com180	C C D 🖙 👌 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	Configure NTP	
Marning: The unit file, source configuration file or drop-ins of chromyd.service changed on We to reload units. MTP configuration: success	roh. Ann ogočenoti ducazan rotoud	
Figure 58: Configure NTP		
Configure NTP		
Diter comma separated NIT servers list (blank for no NTP server): rtp5-b5-rb Checking status for server: rtp5-b5-rbb-ntp1-v6.cisco.com Status check successful for server: rtp5-b5-rbb-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

SPACES Connect	tor 3.1						е
🖄 Dashboard							
Configure Connector	 Configure Token Without the token, the con 	nector will not be able to start.					Configure Token ×
Configure HTTP proxy							
Privacy Settings	11	General Information				Primary Interfa	ce
Manage API Keys	0	Connector Name	Not Available	HA Config Mode	Not VIP Paired	IP Address	10.89.45.92/24
	Connector 3.1	Conceptor ID	Not Available			MAL Address	00505654754308
Troubleshoot	Hostrame com-pri	Instance ID	005056x754c8			DNS Server	
	Package correctora po+	Praxy				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	0.6 % ①	Running Status	Up 🛈			
	Disk Percentage Usage	4.8 % ()	System Load Average	0 ①			
	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	ф.	é 🔬			
	Up time	5d 3h 31m 9s 🛈					
	Control Channel	Down					
	CPU Usage (%)	0.33 % ①	Looking fo	r other services?			
	Memory Usage (%)	4.74 % ()	Follow steps	below to add services			
	Memory Usage	185.89 MB 🛈	1 Login	to Cisco Spaces			
	Dick Lisopo (N)	0 % (C)	Globa	https://dnaspaces.jo/home			

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

What to do next

You can now 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.

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 3In 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		
Select creation type Select OVF and VMDK files Select 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**.

1 Select creation type Select OVF and VMDK files
3 Select storage 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 dualInterface-conn180 6 Additional settings Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.
× ☐ cisco-spaces-connector3-p84-apr2023.ova
Back Next Finish Cancel

Figure 63: Select OVF and VMDK files

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

Figure 64: Select Storage

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	s and all of its' virtual dis	iks.	
	Name	Capacity	Free ~ Type	✓ Thin pro… ✓	Access ~
	datastore1	924 GB	837.1 GB VMFS	6 Supported	Single
					1 items
vm ware [.]					
			Back	Next Finis	sh 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

1 Select creation type 2 Select OVF and VMDK files 3 Select storage	License agreements Read and accept the license agreements
4 License agreements 5 Deployment options 6 Ready to complete	Accept Resource R
o ready to complete	We will reserve part of the resources of CPU and memory based on your OVA selection.
	Standard Connector: 2 vCPUs. 2000 Mhz will be reserved. 4 GB Memory. 4GB will be reserved. Advanced Connector: 4 vCPUs. 4000 Mhz will be reserved.
	Advanced2 Connector: 8 vCPUs. 8000 Mh will be reserved. 16 GB Memory. 1668 will be reserved.
	Standard (Dual Interface) Connector: 2 vCPUs. 2000 Mhz will be reserved. 4 GB Memory. 4GB will be reserved. 2 NICs will be used. Advanced1 (Dual Interface) Connector: 4 vCPUs. 4000 Mhz will be reserved. 8 GB Memory. 8GB Whz will be reserved.
vm ware [®]	1 agr

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.

I

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

Figure 66: Deployment options

1 Select creation type 2 Select OVF and VMDK files 3 Select storage	Deployment options Select deployment options				
4 License agreements 5 Deployment options 6 Ready to complete	Network mappings	PrimaryInterface SecondaryInterface	VM Network vlan7-private-portGp	~	
	Deployment type	Standard Standard Advanced1		~ be r	
	Disk provisioning	Advanced2 Standard (Dual Interface) Advanced1 (Dual Interface) Advanced2 (Dual Interface)			
vm ware [®]					

Step 8

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

Figure 67: Ready to complete

🔁 New virtual machine - dualInterfac	e-conn180			
 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 	Ready to complete Review your settings selection before finishing the wizard			
 4 License agreements 5 Deployment options 6 Ready to complete 	Product VM Name Files Datastore Provisioning type Network mappings Guest OS Name	Cisco Spaces Connector dualInterface-conn180 cisco-spaces-connector-disk1.vmdk datastore1 Thin PrimaryInterface: VM Network,SecondaryInterface: vlan7-private-portGp AlmaLinux-8.4 64-bit		
	Profile Do not refresh ye	The resources consumed by this configuration are: 2 vCPUs. 2000 Mhz will be res erved. 4GB Memory. 4GB will be reserved. 2 NICs will be used.		
		Back Next Finish Cancel		

- **Step 9** Log in to the terminal and enter the default username **root** and default password **root**.
- **Step 10** Configure the host name for the connector.

Step 11 Choose an network interface to configure as PRIMARY.

Figure 68: Configuring the Primary Interface: IPv4



Figure 69: Configuring the Primary Interface: IPv6



- **Step 12** Do one of the following, and then configure the network settings for the PRIMARY interface. Specify parameters such as IP address, hostname, and so on.
 - Configure the IPv6 stack.
 - Configure the IPv4 stack.

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

- **Step 13** Reset the password for the **spacesadmin** user.
- **Step 14** Confirm the setup.
 - **Note** Because this configuration window times out in 120 seconds, ensure that you provide the input on time to avoid reconfiguration.
- **Step 15** Enter the time zone.

Figure 70: Time Zone

conn-3-244-99	
Timezone setup Hould you like to setup timezone? (blank for default value (UTC))	
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/Buenos_Aires - Press 2 3. America/Chicago - Press 3	
5. America/backer = Press 5 5. America/backer = Press 5 5. America/backco Citu = 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/Auscurum - Pauge 13.	
Select an option from the list above: (blank for default (Default 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

dualInterface-conn180	🖬 🖾 🖻 🖼 🔅 Actions 🚫	
Configure MTP 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 Marning: The unit file, source configuration file or drop-ins of chronyd.service changed on to reload units. NTP configuration: success	Configure NTP	
Figure 72: Configure NTP		
Configure NTP Enter comma separated NTP servers list (blank for no NTP server): rtp5-b5-rbh	-nfol-v6.cisco.com	

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

Configure NTP

Figure 73: ConnectorGUI

Cisco Spaces Connector UI:
nttps://10.22.244.180
lsername 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.

status for server: rtp5-b5-rbb-ntp1-v6.cisco.com eck successful for server: rtp5-b5-rbb-ntp1-v6.cisco.com

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

L

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

Gateway - 10.22.244.1

Dns - 172.70.168.183
```

Interface - SECONDARY

- cisco.com

Domain

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

======end===================

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

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

Figure 74: ConnectorGUI

SPACES Connecto	https://connector-ip						Θ,
📅 Dashboard							
Configure Connector	(II)	General Information					
~		Connector Name	fastlocate-ha-cip		HA Config Mode	VIP Paired	
Ontigure HTTP proxy	Connector 3.1	Tenant ID	12212		HA VIP	7.7.0.25	
Privacy Settings	Hostname dualInt-HA-sec	Connector ID	48636929145890	280000	HA State	BACKUP	
	Package connector3-p84	Instance ID	000c29d6e4cd		HA Instance Channel Status	UP	
Manage API Keys		Proxy	Not Available		HA Peer instance ID	000c292a43c6	
Traublashaat	Show More	NTP Address	ntp.esl.cisco.com		HA Peer IP	7.7.0.20	
		NTP Status	active (running)				
	Primary Interface			Secondar	y Interface		
	IP Address 10.22.244.114/24			IP Address	7.7.0.21/24		
	MAC Address 00:0C:29:D6:E4:CD			MAC Addres	ss 00:0C:29:D6:E4:D7		
	Gateway 10.22.244.1		Gateway	7.7.0.1			
	DNS Server 171.70.168.183		DNS Server	171.70.168.183			
	Domain cisco.com			Domain	cisco.com		
	IP Stack ipv4			IP Stack	ipv4		
	Health						
	Cloud Reachability Conne	cted	Memory Percentage	e Usage	33 % ①		
	CPU Percentage Usage 6.1 %	0	Running Status		Up 🛈		

Note

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

Using Snapshots for Backup

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

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

Figure 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.

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

) Server Ma	anager • Dashboard welcome to server manag	ER		I Manage Tools Add Roles a Remove Rol	View Help nd Features ies and Features
i is V	Local Server All Servers AD DS	•	onfigure this local server		Add Servers Create Server Server Mana	er Group ager Properties
년 11 12 12 13 10 10 10 10 10 10 10 10 10 10 10 10 10	AD LDS DHCP DNS File and Storage Services Hyper-V IIS NPAS Remote Desktop Services	2 3 WHAT'S NEW 4 5 LEARDIN MORE	Add roles and features Add other servers to manage Create a server group Connect this server to cloud services			Hide
		ROLES AND SERVER GROUPS Roles: 9 Server groups: 1 Server	s total: 1			. 1
		AD DS Manageability Events Services Performance BPA results	1 del AD LOS 1 1 Manageability Events Performance BPA results	DHCP Manageability Events Services Performance EPA results	Manageability Events Services Performance BPA results	
		9/13/2021 5/0	9 PM 9/13/2021 5:09 PM	9/13/2021 5:09 PM	9/13/2021 56	29 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-NS0G6584GG3.r	NATION SER cdnlabcead.c	/ER om
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. 	ng physical comp to create a virtual i	uter or virti	ased
	< 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	1			-		×
Select destination	n server		w	DESTI /IN-NS0G6SB4GG3.rd	NATION SER cdnlabcead.c	VER
Before You Begin Installation Type Server Selection	Select a server or a Select a server Select a virtual	a virtual hard disk on which from the server pool hard disk	to install roles and feature:	5.		
Server Roles Features Confirmation	Server Pool					
Results	Name WIN-NS0G6SB4G	IP Address	Operating System Microsoft Windows Sen	ver 2019 Standard	3	
	1 Computer(s) fou This page shows s and that have bee newly-added serve	nd 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	er release of Win Manager. Offline ot shown.	dows Serv e servers ar	rer, nd
		< Pre	vious Next >	Install	Cance	el



Figure 80: Select Server Roles

📥 Add Roles and Features Wizar	rd	- 🗆 X
Select server role	es	DESTINATION SERVER UNIVERSE
Before You Begin Installation Type Server Selection	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services	Description Active Directory Certificate Services
Server Roles Features Confirmation Results	 Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server File and Storage Services (2 of 12 installed) Host Guardian Services MultiPoint Services Network Policy and Access Services Print and Document Services Remote Desktop Services Volume Activation Services Web Server (IIS) (38 of 43 installed) Windows Deployment Services 	(AD Cs) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	< Previous New	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	1		-		×
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 can add, remove, and mo	virtual switches to communicate with other computers. al machines and attach them to a virtual switch. created for each network adapter you select. We recor now to provide virtual machines with connectivity to a odify your virtual switches later by using the Virtual Swi	DESTINA After you i mmend that physical n tch Manage	ATION SER UNIVE install this t you crea etwork. Y er.	ren RSE s ate
Hyper-V	Name	Description Realistic DCI GRE Earnity Controller			
Migration	Ethernet 2	Realtek PCIe GBE Family Controller			
Default Stores Confirmation Results	We recommend that network adapter, do	: you reserve one network adapter for remote access to not select it for use with a virtual switch.	this server.	. To reser	ve a
		< Previous Next >	nstall	Cance	ł

I

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

📥 Add Roles and Features Wizard	4	-		×
Virtual Machine I	Migration	DESTINA	ATION SERV UNIVE	VER RSE
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 use 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 Authentication protocol Select the protocol you want to use to authenticate live migrations. Inis 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 delegat environment to perform tasks such as live migration when managing this server for live migration, including specifying networks, when you create the	is on this : d for live n ter you in ter you in ap constra- ce server. tion in you erver remo- tou will co- cluster.	server. nigration stall the r ined ar otely.	s. If role.
	< Previous Next > In	stall	Cance	ł

c) In the **Default Stores** window, select the location to install files or retain the default locations, and click **Next**. *Figure 84: Default Stores*

🚡 Add Roles and Features Wizard	-		×
Default Stores	DEST	NATION SER UNIVE	/ER RSE
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 det now, or you can change them later by modifying Hyper-V settings. Default location for virtual hard disk files:	ration files, ault locatio	ons
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	:

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

Figure 85: Confirm the Installation Settings

📥 Add Roles and Features Wiza	rd – D	×
Confirm installat	tion selections Destination server	ę E
Before You Begin Installation Type Server Selection Server Roles Features Hyper-V	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 clea their check boxes. Hyper-V	ir
Virtual Switches Migration Default Stores	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	7

Step 9 Open Hyper-V Manager.

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

Figure 86: Actions > Virtual Switch Manager

Vertual Machines Image: Vertual Machines Vertual Machines Image: Vertual Machines Name Image: Vertual Machines	Hyper-V Manager File Action View Help							-	- ×
WHARACCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC	Imager							Artions	
Name State CPU Usage Asigned Memory Uptime Status New and Reveng 01. 4006 MB 3.14.54.29 Concleptions Concleptions The selected vitual machine has no checkgores. New and Pager anal Pager anal Concleptions Concleptions Pager Anal Concleptions Concleptions Concleptions Concleptions Concleptions Concleptions Concleptions Concleptions Concleptions Concleptions Concleptions Concleptions Summary Memory Me	WIN-NS0G6584GG3	Virtual Machines						WINLNS/G6GBAGG3	
Importantial Rurring 01. 4006 MB 3.14.54.29 Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual Machine Import Visual		Name	State CS	U Usage Assigned	Memory Uptim	Status		Man	
 Ceckpoint The selected visual machine has no checkports. Heger Strains, Consection, Con		hyper-aanal	Running 01	4096 MB	3.14:54	29		Part in the state of the state	· · · ·
								import virtual Machine	
 Cectopoints The selected vitual machine has no checkgores. Heap Construction Heap Construction Sensore Server Heap Construction Heap Constructi								Hyper-V Settings	
								Virtual Switch Manager	
								Virtual SAN Manager	
 c Ceckpoints De selected vitual machine has no checkports. Barrish Barlow Server Farrish Barlow Server Help Serve 1 Help Serve 1 Se								Z Edit Disk	
Cencipanita Concipanita Concipanita Concipanita Concipanita Concipanita Concipanita Concipanita Concipanita Survess								Inspect Disk	
Conclusion C								 Stop Service 	
Ceckgoints								× Remove Server	
Checkpoints Vicer Vicer The selected vitual machine has no checkports. If Help Image: Checkpoint Strings. Image: Summary Intervoluing Replication Strings. Summary Intervoluing Replication Strings.							,	8 Refresh	
Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants. Image: Provide a set of decidipants.		Checkpoints					۲	View	•
hyper-anal kper-anal Created: \$7/2021 247.11 PM Configuration Version: 0 Second \$600 Second<			т	te selected virtual machin	e has no checkpoints.			P Help	
Myper-samal Important Symmay Memory Summay Memory Summay Memory Summay Memory Summay Memory Summay Memory Summay Memory Memory Memory								have and	
Nyper-anal Image: String a Image: String a Image: String a Image: String a <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>									
hyper-aand Sumay Memoy Networks Resident Sumay Memoy Networks Resident Sumay Resident								Connect	
hyper sanal © Tun Off Created: \$/7,2021.2-07.11 PM Configuration Version: 3.0 More: 1 Notes: None Summary Memory Networking Regication								Settings	
hyper-anal See - Image: Sector Sect								Turn Off	
hyper samal Image: Some set of the Application Data) Created: 9/7/2021 2-47 11 PM Configuration Version: 0 Generation: 1 Notes: None Summary Memory Summary Memory Memory Resolution								Shut Down	
Image: Parameter Image: Parameter Image: Parameter Image: Parameter Society 242711 PM Clustered: No Configuration Version: S0 Image: Parameter Generation: I Heartbact: OK (No Application Data) Note:: Nore Scenary Memory Tetruoring Replication								O Save	
Nyper-aanal IP Feat Created: 9/7/2021 247.11 PM Chartered: No Configurations Version: 0 Semeration: 1 Note: Nore Enable Replication If Help								Pause Pause	
Myper-sanal By Chckspoint Created: 9/7/2021 2-711 PM Configuration Version: 5.0 Generation: Chastered: No Heartbeat: OK (No Application Data) Motes: None Notes: None Summay Memory Metooding Replication								I> Reset	
Created: 5/7/2021 2-7/11 PM Cheatered: No P Monu Configuration Version: 0. Heartheat: OK (No Application Data) P Parama Rotes: None Heartheat: OK (No Application Data) P Inside Replication Summary Memory Resolution Help Help Help		hyper-aanal						B Checkpoint	
Created: 97/2021 247.11 PM Custered: No % Export Centeration: 10 Heartbeat: OK (No Application Data) # # Reter: None # # # # # # Summary Memory Networking Replication # <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>P Move</td><td></td></td<>								P Move	
Configuration Version: 5:0 Heartbeat: OK (b): Application Data) #§ Rename Generation: 1 Weiler: None #f Installe Replication #f Summary Memory Retroubing Replication #f Help Help		Cre	ated: 9/7/20	21 2:47:11 PM		Clustered: No		Export	
Generatore 1 None Interview Intervi		Con	figuration Version: 9.0			Heartbeat: OK (No Application D	Data)	Rename_	
Sumay Menoy Networking Replation		Gen	eration: 1					11 Enable Replication	
Sumary Memory Retworking Replication		Not	es: None					2 bielo	
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-NSD065846G3 Vertail Machines Name State CPU Usage Assigned Memory Uptime Status WIN-NSD065846G3 Name State CPU Usage Assigned Memory Uptime Status Manual						Actions	
	Name	State	CPU Usage	Assigned Memory	Uptime	Status	WIN-NS0G6584GG3
	hyper-sanal	Running	01.	Virtual Switch Manage	er for WIN-NS0G65	84GG3	×
	< Checkpoints hyper-aanal Cool Gen Note	sted: Iguration Version: reation:	The select 9-77/2021 2-47 9-0 1 None	A virtual switches → tee wirtunes Cess tight 1350 A Caba tetwark and ⊕ MACAdes Raw ⊕ MACAdes Raw ⊕ MACAdes Raw ⊕ MACAdes Raw ⊕ MACAdes Raw ⊕ MACAdes Raw ⊕ MACAdes Raw	A models	Create vital anth- What type of vital anth- What type of vital anth- Date of vital anth- Date of vital anth- Provide Date of vital anth- Provide Creater a vital anth- Provide Create	ou want to create? Create Whad Switch In to the physical network adapter so that whad elevert.

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

Hyper-V Manager	Virtual Machines	Virtual Machines Actions							
	Name	State	CPU Usag	e Assigned Memory Uptime	Status WIN-NS0G6SB4GG3				
	hyper-sanal	Running	0%	Virtual Switch Manager for WIN-NS0G6	584GG3 — -	×			
				Yirtual Switches X New virtual network switch X Annaly	Name:	-			
				Cisco 1GigE 1350 LOM #3	Aanal hyper V				
				Cisco 1Golf 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 writial switch to?				
			The select						
					Osco 16gE 1350 LOM				
					Allow management operating system to share this network adapter				
					Enable single-root I/O virtualization (SR-IOV)				
					O Internal network				
					O Privase network				
					VLAN ID				
					Enable virtual LAN identification for management operating system The VLAN identifier specifies the virtual LAN that the management operating system viil use for all network communications through this network adapter. This	erating system snapement operating this network adapter. This			
	hyper-aanal		_		setting does not affect virtual machine networking.				
	Cre	ated:	9/7/2021 2:47						
	Con	figuration Version:	9.0		Remov	•			
	Gen	eration: es:	1 None		SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or prival	te			

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

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

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

- **Step 2** Untar the HYPER-V to obtain a .vhdx (VHDX) file. You can use this to deploy a HYPER-V connector instance. Store the VHDX file in a folder location where you plan to create the HYPER-V instance.
- Step 3 Open Hyper-V Manager.
- **Step 4** Right-click the vSwitch created, and choose New > Virtual machine.

Figure 89: Create New Virtual Machine

Hyper-V Manager						- 0	\times	
File Action View Help								
🗢 🔿 🙍 🛅 🔛								
Hyper-V Manager						Actions	_	
WIN-E7FRSAF7CMD	Virtual Machines					WIN-E7FRSAF7CMD	^	
	Name	State	CPU Usage	Assigned Memory	Uptime	New	•	Virtual Machine
	Connector_kennepna	Uit				1 Import Virtual Mach		Hard Disk
						Hyper-V Settings		Floppy Disk
						Virtual Switch Mana		
						🛃 Virtual SAN Manage		
	<					💰 Edit Disk	-	
	Checkpoints				(Inspect Disk		
		The selected virtual machine has no checkpoints.						
						C Refresh		
						View	•	
						Help	_	
				Connector_kennepha				
						- Connect		
	Connector_kennepha					Settings		
	Created	d:	5/26/2021 7:53:19	PM Clustered: N	lo	 Start 		
	Configu	ration Version:	9.0			Checkpoint	- 1	
	General	tion:	1			Move_		
	Notes:		None			Export		
						T Rename		
						Delete		
	Summary Memory Networ	rking Replication				1 Enable Replication	-	
	<				>	m	~	
	Connector kennepha Created Configu General Notes: Summary Memory Netwo	f: irration Version: tion: rking Replication	5/26/2021 7:53:19 9.0 1 None	² M Clustered: N	io >	₩elp Connectsr/kennepha Connect Settings. Satt Checkpoint Move Export Export <tr< th=""><th>•</th><th></th></tr<>	•	

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

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

WIN-F7ERSAF7CMD	Virtual Machines			Actions
	Name Connector_kenr < Checkpoints	State C New Virtual Machine Wiz Before You Refore You Regin Soeofy Name and Location Speofy Generation Assign Memory Configure Networking Connect Wrtual Hard Disk Installation Options Summary	PU Ukage Assigned Memory Uptime and Begin This wizard helps you create a virtual machine computers for a variety of uses. You can use you can change the configuration later using h To create a virtual machine, do one of the foll • Click Finish to create a virtual machine that • Click Next to create a virtual machine with	You can use virtual machines in place of physical the witard to configure the virtual machine now, and typer-V Manager. owing: is configured with default values. a custom configuration.
	Connector_kenne			

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_ken	State Mew Virtual Machine Wi Specify Na	CPU Usage A zard me and Locat	issigned Memory Uptime	WIR-EIFRON-ICMD	
< Checkpoints	Before You Begin Specify Name and Location Specify Generation	Choose a na The name is identify this	me and location for this virtual ma displayed in Hyper-V Manager. W virtual machine, such as the name	achine. Ie recommend that you use a name that a of the guest operating system or work	t helps
	Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options	You can creat folder, the v	iyperv-connector ate a folder or use an existing fold intual machine is stored in the def e with al machine in a different loc	der to store the virtual machine. If you ault folder configured for this server. ation	don't se
	Summary	Location:	NUsers\Public\Documents\Hyper- slan to take checkpoints of this vir Checkpoints include virtual machin	WWrtual hard disks\hyper-v-2-31\ tual machine, select a location that has te data and may require a large amount	enoug t of spa
Connector_kenn					

Figure 91: Name of Connector

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

Figure 92: Specify Generation

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

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.

lp					
ī					
	Victual Machines			Actions	
2	Name	State (1	PULIcane Assigned Memory Untim	WIN-E7FRSAF7CMD	· •
		Assign Mem	County the amount of memory in allocate i	n this victual machine. You can machine	fu an amount fro
	Checkpoints	Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	MB through 12582912 MB. To improve performance of the operating system. Startup memory: 4094 MB Use Dynamic Memory for this virtual me When you decide how much memory to use the virtual machine and the operation	ormance, specify more than the mini nchine. to assign to a virtual machine, conside ting system that it will run.	num amount er how you inten
	Connector_kenn				

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

Figure 94: Configure Networking

						_
Virtual Machines					Actions	
Name Connector_kenr	State C State C State C Configure M	PU Usage A aard Networking	ssigned Memory	Uptime		
c Checkpoints	Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking	Each new vir virtual switch Connection:	tual machine include , or it can remain dis Not Connected <u>Not Connected</u> vSwitch	a network adapte connected.	er. You can configure the ne	twork adapter to
Connector_kenny	Connect What Hard Disk Installation Options Summary					

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.

Name State CPU Usage Assigned Memory Uptime Connector_kerr Image: New Virtual Machine Wizard Completing the New Virtual Machine Wizard Before You Begin Specify Name and Location Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk	•
Checkpoints Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk You have successfully completed the New Virtual Machine Wizard. You are about following virtual machine. Description: Name: hyperv-connector Generation 1 Memory: 4096 MB Network: vSwitch	
Band Disk: O'll kensil/Dubic/Documents/Human/W/Hual hand disks/humanus/	t to create the
Connector_kenne Connector_kenne 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

avi	HyperV ~	3 4 ►
*	Hardware	Security
	Add Hardware Firmware Boot from Hard Drive	Secure Boot Use Secure Boot to help prevent unauthorized code from running at boot time (recompanded)
	Secure Boot disabled	Enable Secure Boot
E	Memory 1024 MB	Template: Microsoft Windows
= 1	Virtual processors Virtual processors Lease Additional Additiona Additiona Additional Additional Additional Additationa Additiona	Encryption Support Enable Trusted Platform Module A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.
*	Management Name aviHyperV Integration Services Some services offered Checkpoints Standard Smart Paging File Location C:\ProgramData\Microsoft\Windo Automatic Start Action	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.
	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**.

Act - v Manager			- 0 ^				
Action View Help							
per-V Manager	Virtual Machines		Actions				
WIN-E/PICAP/CMD	Name State	CPU Usage Assigned Memory Uptime	WIN-E7FRSAF7CMD				
	hyperv-connector Off		New +				
			🕼 Import Virtual Mach				
			Hyper-V Settings				
			Virtual Switch Mana				
			🔬 Virtual SAN Manage				
	< (C)		🥳 Edit Disk				
	Checkpoints		🤇 🖃 Inspect Disk_				
			Stop Service				
	The selected	The selected visual machine has no checkpoints.					
			C Refresh				
	hyperv-connector		Settings				
	Created:	6/9/2021 3:57:29 PM Clustered: No	Start				
	Configuration Version	m: 9.0	B Checkpoint				
	Generation:	1	Move.				
	Notes:	None	Deport.				
			E Rename				
			Bc Delete.				
	Summary Memory Networking Replication	en	Enable Replication_				
	<	1911	> 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

Virtual Machines						Actions	
Name A	Caster	COLUMN	Automatika ana	Unting	Outur	WIN-NS0G6584GG3	
reame	State	CPO Osage	Assigned Memory	Optime 00/00/16	Status	New	
Mhouse is	normy		4000 HD	00.00.10		C Import Virtual Machine	
						Hyper-V Settings	
						Virtual Switch Manager	
						Virtual SAN Manager	
						ed Edit Disk	
						D Inspect Disk	
						Stop Service	
						Y Remove Server	
¢						> B Refeet	
Checkpoints						View	
		The order day		distant.		TO U.S.	
		e Help					
						hyper-aanal	
						- Connect	
						Settings	
						Turn Off	
						Shut Down	
						Save	
						II Pause	
						I> Reset	
						R Checkpoint	
hyper-aanai						P Move-	
Cri	rated:	9/7/2021 2:47:11 PI	м	Cluste	red: No	P Export	
Co	nfiguration Version:	9.0		Hearth	weat: No Contact	Rename.	
Ge	neration:	1				Sing Enable Replication	
No	tes:	None					
						e Heip	
Summary Memory N	letworking Replication						
	Vertual Machines Name Promotional Checkpoints	Vertual Machines Name Sate Sate Sate Sate Sate Sate Sate Sat	Vertual Machines Name *** Name **** Name ***** Preseaud ******** Checkpoints	Vertual Machines Name State State CPU Usage Assigned Memory State CPU Usage Assigned Memory Concepted	Created: \$-7/2021.2-7.11 PM Configuration Version: 9 Reverse 1 Revers	Vertual Machines Name State CPU Usage Assigned Memory Uptime Status Processed Revery 02. 405.6 MI 0000.15 Conclusion Revery The selected vitual machine has no checkports. Configuration Version 9. Configuration Version 9. HeartBeat: No Contact Contact Contact No Interaction Social No Interaction Soc	Actions Actions Name State CPU Usage Assigned Memory Uptime Status Were Model Status Versus Nerrey 0. 4056 MIII 00 20 15 Nerrey Nerrey Import Vistal Machine Parents 02 20 15 Nerrey Nerrey Nerrey Concluster The selected visual machine has no checkports. Nerrey Nerrey Nerrey Import Vistal Machine Parents Nerrey Nerrey Nerrey Nerrey Concluster The selected visual machine has no checkports. Nerrey Nerrey Nerrey Nerrey Import Vistal Status Nerrey Consect. Status Nerrey Nerrey Import Vistal Machine Nerrey Nerrey Nerrey Nerrey Nerrey Nerrey Import Vistal Machine Nerrey Nerrey Nerrey Nerrey Nerrey Nerrey Nerrey Import Vistal Machine Nerrey Nerrey<

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

uudiinten lace-conni tov	LAL NO.	
Change a petropy interface as PDIMADY from below that has competimity to Giago Sarone Cloud		
Note: SECONDARY interface can be configured using connectorctl cli after completing configuration.		
Interface: ens32 - (00:00:29:88:40:07) Interface: ens33 - (00:00:29:88:40:09)	Configure the public-	
Choose a network interface [ens32 or ens33]: ens32		
Starting network setup	facing interface (Priman/)	
Choose metwork stack[ipv4 or ipv6]: ipv4	laoing interface (i filliary)	
Enter network settings configuration information for stack:ipv4		
Enter IP address formatted as: ipl/prefix1. Example: 192.168.1.5/24, 10.0.0.11/24: 1)	
Enter gateway:		
Enter pro server (comma separated 1p address fist).		
Confirm network settings? (ues/no) ues		

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	
	Timerona setun
	Annezone sector
	ues
	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))
	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
	b. America/Mexico_City - Fress b
	/ Hmcrica/Tew_York - Press /
	8. HMEPICA/FIDENIX - FFESS 8
	7. Humerica Carnegina – rress 7
	10. HHEFTCA/SAULIAU - FFESS 10
	11. nmcrida/3a0_faulto = fress fr
	12. mmerica doronico - Press 12
	Select an until function from the list above: (blank for default (Default value is 1))
	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

Step 1 Log in to Cisco Spaces.

Note The Cisco Spaces URL is region-dependent.

- **Step 2** From the left navigation pane, choose **Setup > Wireless Networks**.
- Step 3 In the Get your wireless network connected with Cisco DNA Spaces area, click Add New.
- Step 4 In the Cisco AireOS Controller/Catalyst 9800 Wireless Controller area, click Select.

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

Step 5 In the Via Spaces Connector area, click Select. 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
Requires you to install Spaces Connector on a virtual machine in order to connect your WLC to Osco DNA Spaces cloud.	Requires WLC with software version 8.8 MR2 and above or Osco Catalyst Wireless Coreroller with software version 16.12.2 and above. Wireless coresten rends direct interest correctivity.	Configure your CMX On-Prem dashboard to send location updates to Cloco DNA. Spaces, either by configuring the Notification U.R. in the Claco CMX dashboard or by manually uploading a JSON file that

Step 6

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

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

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

Elisco DNA Spaces			O Active APs
Connect your wire	less network		
Connect via Sp Spaces Connector is an easy	aces Connector way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Control	lers or reconfigure your wireless network.	Clink to
Connect WLC/C	Catalyst 9800 Directly Directly is an easy way to get your wireless network connected to Claco DNA Spaces. No need to upgrade Wir	reless LAN Controllers or reconfigure your wireless network.	expand
Wireless Networks	Sering an instructive connection to Classe DNA Spacese		~
	gin to connect to Chece Manual Choud, import focations in to Chece DNA Spaces and activate/yare to	the Maraki Networks.	× v
B	Get your wireless network connected with Cisco DNA Spaces There are multiple options to get connected based on your wireless network deployment.	Need Help? Configuration guide Cisco AireOS/Catalyst	
	+ 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
\checkmark
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	
Instances in High Availability Pair Configure your instance To set up high availability pair follow the steps below.	
Instances in High Availability Pair Configure your instance To set up high availability pair follow the steps below. Step 1:	
Instances in High Availability Pair Configure your instance 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 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**.
- **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.

- **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 3In 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

SUMMARY 2 2 0 2 0 0 0 Switches Instances Active Inactive 2 Services enabled Controller Switches Configuration Instances Metrics Instances in High Availability Pair
Configuration Instances Metrics
Instances in High Availability Pair
Image: System Package: connector3-p84- apr2023 Image: System Package: connector3-p84- apr2023
Mac ID 00:50:56:A7:54:C Restart Services
IP Address 10.89.45.92 Refresh Instance
Status The De Remove
Control Channel Status Connected Configuration history
HA Status Not Paired
VIP Address NA
SERVICES
Service Manager 6 Up
Version: 3.1.0.104 Last Heard on May 11, 2023, 5:41:07 PM
Location (7) Up Version: 3.1.0.52 Last Heard on May 11, 2023, 5:41:07 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						0
🖄 Dashboard							
Configure Connector	Configure Token Without the token, the con	mector 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	Not Available			MAC Address 00:50:56:A7:54:C8	
 Troubleshoot 	Hostneme corrept	Conneter ID	00008-204-8			DMP Personal	
	Package connector3-p84	Prov	000000873408			Domain	
	Show Mare	NTP Address	ntp.esi.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 ①			
	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 M			
	Up time	5d 3h 31m 9s 🛈					
	Control Channel	Down		and a second sec			
	CPU Usage (%)	0.33 % ①	Looking	for other services?			
	Memory Usage (%)	4.74 % 🛈	Follow ste	s below to add services			
	Memory Usage	185.99 MB ①	1 4	gin to Cisco Spaces			
	Dirk Lisana (%)	05.0	6	bel: https://dnaspapes.io/home			

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

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

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

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

Configuring Privacy Settings

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



Note This task is optional.

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

📅 Dashboard		
Configure Conne		
Onfigure HTTP		
Privacy Settings	MAC and Username Salt	
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:

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



Figure 119: Setup Proxy

Figure 120: Configure Basic Authentication for Proxy (Optional)

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 🔺 Not Secure ht	Nps://10.22.244.86/troubleshoot	🖈 🥌 🌧 🗖 🚷 Incognito 🗄
S	PACES Conne	ctor 3.1	Θ
6	Dashboard	Network Connectivity	
6	Configure Connector		
۲	Configure HTTP proxy	Connector Diagnosties is a workflow that detacts common problems with your spaces connector instance. It will fun tasts to diagnose operational issues in different stagas of this spaces connector. Upon completing the diagnostics tests, you can download the connector logs to share with Cisco for solvenced 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		
		STAL O	
		14	
		No test has been run	

Figure 122: Sample Run Test Results

← →	C 🛕 Not Secure http:	://10.22.244.86/troubleshoot		x) 😐	🖈 🛛 🔒 Incognito 🗄
G	Configure Connector				
6	Configure HTTP proxy	Connector Diagnostics is a workflow that detects com- run tests to diagnose operational issues in different sta diagnostics tests, you can download the connector log	ion problems with your spaces connector instance. It will ges of the spaces connector. Upon completing the s to share with Cisco for advanced troubleshooting.	https://connector.ca-dnasoaces.io 🗸	Run New Test
۵	Privacy Settings	Click on "Run New Test" to begin diagnosing your spac information for that specific test.	es connector instance. Click on "View Log" to see more		
Þ	Manage API Keys	Recent Tests			
Troubleshoot Complete.					
		Cloud Endpoint DNS Resolution () 3 seconds age	Troubleshoot DNS Resolution for https://connector.qa-dnaspaces.jo		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 evailability using netcat for proxy: http://proxy.esl.cisco	o.com:80	View Log
		Connector Token Diagnostics () 1 seconds ago	Validating spaces cloud token configuration		View Log
		Cloud Reachability () 3 seconds ago	Reachability test to https://connector.qs-dnaspaces.io using curl con http://proxy.asl.cisco.com/80	mmand with proxy:	View Log
		Service Connectivity () 3 seconds ago	Checking service connectivity to cloud endpoint https://connector.q/ Manager with proxy. http://proxy.asl.eisos.com.90	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.

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

```
The following is a sample command.
```

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

Step 2 Log in to the Connector CLI, and validate the copied proxy certificate using the **connectorctl cert validate** command. The following is a sample output of the command:

```
[spacesadmin@connector ~]$ connectorctl cert validate -c /home/spacesadmin/proxy-ca-bundle.pem -s
/home/spacesadmin/proxy-server-cert.pem
Executing command:cert
Command execution status:Success
------
/home/spacesadmin/proxy-ca-bundle.pem and /home/spacesadmin/proxy-server-cert.pem exists
/home/spacesadmin/proxy-server-cert.pem: OK
Validation of certificate is successful
```

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

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

The following is a sample output of the command:

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

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

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

Figure 123: Setup Proxy

← → C ▲ Not Secure https://10.22.244.86/proxy	± 😐 🖈	🛛 🛞 Incognito 🗄
Connector 3.1		Θ
🛗 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	Proxy URL	
· 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	0	
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 "Fun 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

	C 🔺 Not Secure http	s://10.22.244.86/troubleshoot 🖈	🧧 🖈 🔲 😽 Incognito
6	Configure Connector		
0	Configure HTTP proxy	Connector Diagneticitie is a workflow that detotate common problems with your spaces connector instance. It will run tests to diagnostic operational issues in different stages of the spaces connector. Upon completing the diagnostic tests, you can download the connector logs to share with Claco for advanced trubblehooting. https://connector.os.dossnaces.in.	Rup New Test
9	Privacy Settings	Click on "Nun 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	Troubleshoot Complete.	
		Cloud Endpoint DNS Resolution () 3 seconds ago	View Log
		HTTP Proxy Reachability Checking HTTP proxy http://proxy.eti.ciscc.com.80 reachability 11 seconds age	View Log
		HTTP Proxy Server Diagnostics () Testing proxy evaluability using netcal for proxy: http://proxy.est.cisco.com/80 3 seconds ago	View Log
		Connector Token Diagnostics 🕐 Validating spaces aloud taken configuration 1 seconds ago	View Log
		Cloud Reachability ① Reachability test to https://comector.ge.deaspaces.io.using.curl.command.with proxy: 3 seconds ago Http://proxy.ael.cisco.com.30	View Log
		Service Connectivity Checking service connectivity to dead andpoint https://connecter.ga.dnaspaces.io.trom Service a seconds ago Manager with proxy. http://proxy.ail.elico.com.80	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.

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

Figure 127: Create Connector

≡ CISCO SPAC	E CISCO SPACES O Active AP3				
Connec	t your wireless network				
Con	nect via Spaces Connector Connector is an easy way to get your wireless network connected to Cisco Spaces. No need to	upgrade Claco Winiess Controllars or reconfigure your winiess network.		^	
()	Install Spaces Connector OVA Download gaves Convector (2) Nownload Spaces Convector (2)		Need Help? Access the balow lisks 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 and associate controllers to your Citoo Speces Connector(s)				
	1 / 4 controller(s) active	Add Controllers View Controllers			
	Import Maps Prime(DRMC map requires in order to work Locale & detect, Asset tracker, and IOT services, and pro-	dmity Report			
	9 buildings imported 9 Roors imported	Import/Sync Maps Map Uplead 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>CONCRET DE LA CONTRACTOR DE LA CONTR</complex-block>		
<complex-block>(p) events y events (p) (p) (p) (p) (p) (p) (p) (p) (p) (p)</complex-block>	E CISCO SPACES	₩ Ø 6
<complex-block> Submark Prices Prices<!--</th--><th>Setup > Connectors > connector-test</th><th>ID : 4005858765654143000 Last Modified : May 12, 2023, 5:01:08 PM</th></complex-block>	Setup > Connectors > connector-test	ID : 4005858765654143000 Last Modified : May 12, 2023, 5:01:08 PM
Configure your instance	SUMMARY 0 0 0 0 2 0 0 Instances Active Inactive Services enabled Controller Switches	
Click to generate a token Configure your instance To set us high availability pair follow the steps below. See 1 Caps the subscription by clicking the 4b-Generate Tokers/b- button on the top of this page. A token will be generated. See 2 Caps the maint See 3 De byter connector II and configure the token on your second connector instance. For more details follow the documentation documentation	Configuration Instances Metrics	C D Generate Token S Troubleshoot Connector
Configure your instance To set up light availability pair follow the steps below. Bre ill Contract the store holdshift pair of boldshift pair of boldshift pairs A token will be generated. Bre ill Dester to be presented token. Bre ill Dester to connector if and configure the token on your second connector instance. For more details follow the documentation documentation	Instances in High Availability Pair Click to generate a token	
	Configure your instance To set up high availability pair follow the steps below. Step 1: Benaries a loken by clicking the -to-Senerate Token-/b> button on the top of this page. A token will be generated. Step 2: Copy the generated token. Step 3: Go be your connector UI and configure the token on your second connector instance. For more details follow the documentation documentation	

Copy the displayed token.

Step 4 Log in to the GUI of the first instance of connector and click **Configure Token** in the top-right corner to provision the first copied token there.
Figure 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		114 Contro Maria	Click to Configure	a Token	orface
🖉 - Manage API Keya	Connector 3.1	Tenant ID	Not Available	RK Garry Mode			0.50.56.47.54:C8
 Troubleshoot 	Hodhame open-pri Packaga open-pri Show Mane	Connector ID Instance ID Proxy NTP Address NTP Status	Not Available 00503563754c8 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.com ipo4
	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	Looki Polaw 1	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

SPACES Connects	or 3.1								Θ
🖄 Dashboard									•
Configure Connector	Configure Token Without the token, the connector will no	of be able to start.							Configure Token ×
Onfigure HTTP proxy									
Privacy Settings		General Information				Click to Configure a Toke	en	erface	
Manage API Keya	Connector 3.1	Connector Name			HA Config Mode			10.89.45.92/24	_
(a) Trachlashoot	Connector C. T	Connector ID					Gateway	10.89.45.1	_
	Postage connector2-o04-	Instance ID	005056a754	08			DNS Server	171.70.168.183	_
		Proxy	https://praxy.	esl.cisco.com 90			Domain	oisco.com	_
	Show Mare	NTP Address	ntp.esi.cisco	.com			IP Stack	ipv4	_
		NTP Status	active (runni	ng)					_
	Health								_
	Cloud Reachability Connect	ted	Memory Parce	ntege Usege	12.28 % ①				_
	CPU Percentage Usage 12.5 %	0	Running Status		Up ①				_
	Disk Percentage Usage 6.1 % G	D	System Load A	warage	0.34 ①				_
	Disk Usage 4713.21	I MB ()	Up time		8d 4h 53m 21s 🛈				_
	Memory Usage 480.94 ft	MB ()							_
	Services C								
	Service Manager 🚔 4.1.0.104		ŵ		SU2 (8)	M			
	Up time	1d 11h 52m 56s 🛈							
	Control Channel	Down							
	CPU Usage (%)	0.68 % ①		Looking for a	ther services?				
	Memory Usage (%)	3.81 % ①		Follow steps beil	ow to add services				
	Memory Usage	149.35 MB ①		(1) Login to	Cisco Spaces				
	Disk Usage (%)	0% ()		Global htt	ps://traspaces.io/tome				
	Disk Size	56 MB ()		For EU: N For APAC	tips Adhaspaces eurhome Thttps Abiscospaces sp				

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	e Services enabled	0 Controller	0 Switches						
Configuration Instances Metrics							0	🖉 Generate Token	Troubleshoot Connector
Instances in High Availability Pair									Configure VIP Pairing
O05056a754c8 System Package: connector3-p84- apr2023		0	I	¢	005056a7affa System Package: connector3-p84- apr2023			0 1	
Mac ID	00:50:56:A7:54:C8			Ma	c ID	00:50:56:A7:AF:FA			
IP Address	10.89.45.92			IP a	Address	10.89.45.93			
Status	🔁 Up			Sta	itus	C Up			
Control Channel Status	Connected			Co	Official Channel Status	Connected			
VIP Address	NA			VIE	Address	NOC Pareo			
SERVICES				SE	RVICES				
Service Manager Structure Version: 3.1.0.104 Last Heard on May 11, 2023, 1	/p 10:04:07 PM			Ser	vice Manager sion: 3.1.0.104 Last Heard on May 11,	Up 2023, 10:04:12 PM			
Location during U Version: 3.1.0.52 Last Heard on May 11, 2023, 10	ар):04:07 РМ			Loc Ven	ation sion: 3.1.0.52 Last Heard on May 11, 2	O Up 1023, 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	SCO SPACES						Ø 6
Setu	Connectors > conn-ha-vip SUMMARY 2 2 0 Instances Active Inacti	2 0 ive Services enabled Contro	0 oller Switches		ID : 3761674;	827259750000 Last Modified	May 11, 2023, 4:17:54 AM
С	onfiguration Instances Metrics				0	🖉 Generate Token 🛛 🚳	Troubleshoot Connector
ŀ	otososa754c8		0 8	O05056a7affa System Package convector3-p84- ap2023	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,	j Up , 10:04:07 PM		Service Manager Version: 3.1.0.104 Last Heard on May 11, 2023	Up 3, 10:04:12 PM		
	Location S Version: 3.1.0.52 Last Heard on May 11, 2023,	r 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
Setup > Connectors > fastlocate-te-cip SUMMARY 2 2 0 2 Instances Active Inactive enable	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
© 000c292a43c6 Syntam Residage connection3 y64-spr2023	 Primary 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	
	SW

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 Controller	0 Switches		
Configuration Instances Metri	55			🔾 🔑 Generate Token	🍈 Tro
O000c292a43c6 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	O Up		Status	😗 Up	
Control Channel Statue	Constant	_	Control Channel Statue	Presented .	
HA Status	VIP Paired BACKUP		HA Status	VIP Paired ACTIVE	
VIP Address	7.7.0.25	_	VIP Address	7.7.0.25	
SERVICES			SERVICES		
Service Manager Version: 3.1.0.104 Last Heard on M	Up lay 10, 2023, 4:12:16 PM		Service Manager Version: 3.1.0.104 Last Heard	Up I on May 10, 2023, 4:11:59 PM	
Location Version: 3.1.0.52 Last Heard on M	O Up		Location Version: 3.1.0.52 Last Heard	Up	

Connector Active-Active

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

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

Restrictions for Active-Active

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



- 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.

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

Figure 133: Create Connector

		U 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 Space	as. No need to upgrade Cisco Wretess Controllers or reconfigure your wireless network.	
Install Spaces Connector OVA Deveload and head Space Connector 0/A a s virtual machine. Deveload Space Connector 0 ⁽²⁾		Need Help? Access the below links to view detailed help.
Configure Spaces Connector You will need a taken to configure Spaces Connecter. You need to connect to https:// vie.HTTPS.prosp.	Fyour connector IP-/ from a browser to configure the token. You can optionally configure Spaces Connector to connect	View Configuration Steps C
2 / 11 connector(s) active	Create Connector View Connectors	Frequently Asked Questions
Add Controllers Add and associate controllers to your Clisco Spaces Connector(s)		
1 / 4 controller(s) active	Add Controllers View Controllers	
Import Maps PrimerDNAG map requires in order to work Locate & detect, Asset tracker, and IOT to	envices, and proximity Report	
g buildings imported	import/Sync Maps Map Upload History	
9 floors imported	Manage Maps	

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

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

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

Figure 134: Generate Token

≡ cisco spaces	
	0 0
Setup > Connectors > connectors > connectors > connector-text ID : 400585785854143000 Last Modified : May 12, 2023, 5:01	1:08 PM
SUMMARY 0 0 2 0 0 Instances Active 0 2 services enabled Controller Switches	
Configuration Instances Metrics 🗘 🖉 Generate Token	nector
Instances in High Availability Pair Click to generate a token	
Configure your instance	
To set up high availability pair follow the steps below.	
Step 1:	
Genarate a token by clicking the Generate Token button on the top of this page. A token will be generated.	
Step 4: Copy the generated token.	
Step 3: Go to your connector UI and configure the token on your second connector instance. For more details follow the documentation documentation	

Copy the displayed token.

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

Figure 135: Configure a Token

SPACES Connecto	r3.1									Θ
Dashboard										-
Configure Connector	Configure Token Without the token, the connector will	not be able to start.								Configure Token X
Onligure HTTP proxy										
Privacy Settings		General Information				Click 1	to Configure a Tok	en	arface	
Manage API Keya	Connector 3.1	Tenant ID	Not Availat	ble	HA Coring Mode				10.89.45.92/24 00.50.56:A7:54:C8	
 Troubleshoot 	Hoshana colnigei Packaga connectorà p04 Show Mare	Connector ID Instance ID Proxy NTP Address NTP Status	Not Analisi 005056w75 https://pro ntp.esi.ciso active (nan	bie S4cd sp.cesi.cisco.com.90 sp.com ning)				Gateway DNS Server Domain IP Stack	10.89.45.1 171.70.168.183 cisco.com ipv4	
	Health Cloud Plaschability Corri CPU Percentage Usage 12.5* Deix Percentage Usage 5.1 % Deix Usage 47133 Merrory Usage 480.9	Notand % © 1.21 MB © 94 MB ©	Memory Parc Purning Stat System Load Up time	serrage Usage tus I Average	12.28 % () Up () 0.34 () 8d 4h 53m 21s ()					
	Services C									
	Service Manager 🔒 21.0.104		ŵ		\$	1				
	Up time	1d 11h 52m 56s 🛈								
	Control Channel	Down		Looking for a	ther services?					
	CPU Usige (%) Marrow Lisana (%)	0.00 % ()		Follow steps bei	ow to add services					
	Memory Usage (19)	149.36 MB (0		1 Looisto	Cisco Soaces					
	Disk Usage (%)	0%0		Globalt M	ps://draspaces.io/home					
	Disk Size	56 MB 🛈		For EU: N For APAC	tps://dnaspaces.eu/home : https://discospaces.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

SPACES Connecto	or 3.1						Θ
🖄 Dashboard							
Configure Connector	Configure Token Without the token, the connects	r will not be able to start.					Configure Token X
Configure HTTP proxy				C			
Privacy Settings		General Information			Click to Configure a T	oken	orface
🖉 - Manage API Keya	Connector 3.1	Tenant ID	Not Available	HA Comg Mode			10.89.45.9224 00.50.56.A7.54:C8
 Troubleshoot 	Hothama open pri Pachaga openadara 364 Show More	Connector ID Instance ID Prony NTP Address NTP Status	Not Available 005056075408 https://promy.eet.clsoo.com mp.eet.clsoo.com active (running)	0		Gatoway DNS Server Domain IP Stack	10.89.45.1 177.70.168.183 sites com gevi
	Health						
	Cloud Reachability CPU Percentage Usage Disk Percentage Usage Disk Usage Merrory Usage	Connected 12.5 % ① 8.1 % ① 4713.21 MB ② 480.94 MB ①	Memory Percentage Usage Punning Status System Load Average Up time	12.26 % ① Up ① 0.34 ① Rd 4h G3m 21s ①			
	Services C						
	Service Manager 🔒 31 Upyrate: Soccess	0.104	۵	÷ A	1		
	Up time Control Channel CPU Usage (%)	1d 11h 62m 66s ① Down 0.688 % ①	Looking f	or other services?			
	Memory Usage (%) Memory Usage Disk Usage (%) Disk Size	3.81 % ① 149.36 MB ① 0 % ① 56 MB ①	Pollow steps 1 Logi Glob For 6 For 6	: below to add services n to Cisco Spaces et Intps://diaspaces.ichone U. https://diaspaces.eu/hone PAC: https://diaspaces.eu/hone			

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
A Privacy Settings	Hostname ipv6-raib	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 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 109
- 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.

Step 1 Log in to Cisco Spaces.

Note The Cisco Spaces URL is region-dependent.

- **Step 2** From the left navigation pane, choose **Setup > Wireless Networks**.
- **Step 3** In the **2. Configure Spaces Connector** area, click **View Connectors**.
- **Step 4** Click a connector from the list of connectors that are displayed.
- **Step 5** In the **SUMMARY** window that is displayed, click **Troubleshoot Connector**.
- **Step 6** In the **Troubleshoot Connector** window that is displayed, you can see that logs can be enabled by a service. Click the respective **Enable Debug Mode** of a service if not enabled already.

After being enabled, connector starts collecting debug logs for that service, and these logs are stored locally on connector.

Step 7 (Optional) To upload the logs to the Cisco Spaces dashboard, click Upload Logs to Cloud.

Recovering a Lost Password

This task shows you how to recover your connector GUI password.

Step 1	Log in to Cisco Spaces.				
	Note The Cisco Spaces URL is region-dependent.				
Step 2	From the left navigation pane of the Cisco Spaces dashboard, choose Setup > Wireless Networks.				
Step 3	In the 2. Configure Spaces Connector area, click View Connectors.				
Step 4	Click a connector from the list of connectors that are displayed.				
Step 5	In the SUMMARY window that is displayed, click Troubleshoot Connector.				
Step 6	In the Troubleshoot Connector window that is displayed, click Password Reset Key.				
Step 7	In the Password Reset Key window that is displayed, click Copy The Key . Save the copied key on a notepad.				
Step 8	Open the connector GUI, and click Forgot Password .				
Step 9	In the Password Reset Key field, enter the key copied in 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.

- **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.

- **Step 1** Log in to the connector GUI.
- **Step 2** In the connector left navigation pane, click **Troubleshoot** and do one of the following:
 - If you have configured the token for this connector in Cisco Spaces, the text field beside the **Run New Test** button is automatically populated with the Cisco Spaces URL.
 - If you have not configured the token for this connector on Cisco Spaces, then from the Run New Test drop-down, choose from one of the Cisco Spaces region-dependent URLs.
- **Step 3** Click **Run New Test** to initiate troubleshooting the connectivity.
- **Step 4** Observe the running tests for the following:

; ()

Troubleshoot C Diagnostics to perform DNS	
Cloud Endpoint DNS Resolution R 3 seconds ago	View Log

Click **View Logs** to view further information.

=

	Figure 140: View Logs	
	Troubleshoot Complete.	
	Logs: HTTP Proxy Server Diagnostics	X View Log
	Error while validating the disgnosticsid	View Log
	HTTP Proxy Server Diagnostics (j) 1 seconds ago	View Log
	Connector Token Diagnostics ① 1 seconds ago	View Log
	Cloud Reachability () 3 seconds ago	View Log
	Download Diagnostics Logs	
0		1
•	Figure 141: View Logs for a Successful Test	about this successful te
	Troubleshoot Complete.	
	Logs: Cloud Reachability $ imes$	View Log
	2023-01-10 05:20:47-UTC Reaching cloud endpoint https://dnaspaces.io/ without proxies 2023-01-10 05:20:47-UTC HTTP Ping Succeeded to reach https://dnaspaces.io/	View Log
	ок	View Log
	Connector Token Diagnostics ① 1 seconds ago	View Log
	Cloud Reachability () 3 seconds ago	View Log
	Download Diagnostics Logs	

•	Represents a warning. Click ⁱ ⁽ⁱ⁾ 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 - 🗆 🗙
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 diagnostics he disgnosticsid Perform cloud token tests for endpoint: https://connector.qa- Cloud token configured with tenant: 12454 for connector-id: Reaching cloud endpoint https://dnaspaces.io/ without proxies HTTP Ping Succeeded to reach https://dnaspaces.io/

What to do next

You can also use the connector CLI to troubleshoot connectivity issues between the connector and the Cisco Spaces dashboard. See the command **connectorctl troubleshooting connectivity** in the Cisco Spaces: Connector 3 Command Reference Guide.

Unresponsive Connector, or Failure of SSH to Connector

If a connector is unresponsive to SSH requests, reboot the device on which the connector OVA is installed. You can do this from the Cisco Spaces dashboard .

Step 1 Log in to Cisco Spaces.

Note The Cisco Spaces URL is region-dependent.

- **Step 2** From the left navigation pane, choose **Setup** > **Wireless Networks**.
- Step 3 In the 2. Configure Spaces Connector area, click View Connectors.
- **Step 4** Click a connector from the list of connectors that are displayed, and then click the **Instances** tab.
- **Step 5** In the Actions column, click the three-dot icon to open a list of options for the connector instance, and choose **Restart Connector**.

Figure 145: Restart Connector

Instance is Corrupted or Deleted

You may have to delete a connector instance for one of the following reasons:

- An instance is not required anymore.
- An instance is corrupted or invalid.

Step 1 Log in to Cisco Spaces.

Note The Cisco Spaces URL is region-dependent.

- **Step 2** In the left navigation pane of the Cisco Spaces dashboard, choose **Setup > Wireless Networks**.
- **Step 3** In the **2. Configure Spaces Connector** area, click **View Connectors**.
- **Step 4** Click a connector from the list of connectors that are displayed and then click the **Instances** tab.
- Step 5 In the Actions column, click the three-dot icon to open a list of options for the connector instance, and choose Remove. To create a new instance, do the following.
 - a. In the Cisco Spaces dashboard, reissue a token.
 - **b.** Configure the new token on the installed connector.

See Activating Connector 3 on Cisco Spaces, on page 10.

Service Crash, or Restart Services

This task shows you how to restart a service on a connector when the service crashes or hangs.

Step 1 Log in to Cisco Spaces.

Note The Cisco Spaces URL is region-dependent.

- **Step 2** From the left navigation pane of the Cisco Spaces dashboard, choose **Setup > Wireless Networks**.
- **Step 3** In the **2. Configure Spaces Connector** area, click **View Connectors**.
- **Step 4** Click a connector from the list of connectors that are displayed, and then click the **Instances** tab.
- **Step 5** In the Actions column, click the three-dot icon to open a list of options for the connector instance, and choose **Restart** Services.

L

Figure 146: Restart Services

Setup > Connectors > conn-ba-vio									
	SUMMAR	Y							
	2 Instances	2 Active	0 Inactiv		2 Services	enabled	0 Controller	0 Switches	
	motanees	10010	maotri	0	00111000	chabica	Controller	owner	
Configuration	n Instances	Metrics							
Instances i	n High Avail	ability Pair							
ŝ	005056a75	54c8	4-				0		
	ap	x2023			[Destart	Services		
Mac IE)			00:50	:56:A7:54:	Restart	Connector		
IP Add	iress			10.89	0.45.92	Defreeh	Instance		
Status				👩 Up	,	Pomour	instance		
Contro	ol Channel Statu	s		Conne	cted	Configu	ration history		
HA Sta	atus			Not Pr	ired	Connigu	in action in action y		
VID Ac	idroco								
VIP POL	101699			TOA					
SERVI	CES								
Servic	e Manager	Heard on May 1	1 2023	Jp 5:41:07	DM				
version		risuro oli may i	-, 2020, 0						
Version	on :: 3.1.0.52 Last I	Heard on May 11	1 0023, 5	Jp 41:07 P	м				

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.

Step 1	Log in to Cisco Spaces.				
	Note	The Cisco Spaces URL is region-dependent.			
Step 2	From the left-navigation pane, choose Setup > Wireless Networks .				
Step 3	In the 2. Configure Spaces Connector area, click View Connectors.				
Step 4	Click a connector from the list of connectors that are displayed, and then click the Instances tab.				
Step 5	In the Acti Instance.	ons column, click the three-dot icon to open a list of options for the connector instance, and choose Refresh			

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

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.

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

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



PART **IV**

Services

- Location Service, on page 125
- IoT Service (Wireless), on page 131
- IoT Service (Wired) , on page 143
- Hotspot Service, on page 161
- Local Firehose, on page 165



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
	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	Supported versions are:			
Catalyst Access Points (Cisco EWC-AP)	• 16.12.5			
	• 17.3.1			
	• 17.3.2a,			
	• 17.3.3			
	• 17.3.4			
	• 17.4.1			
	• 17.5.1			
	• 17.6.1			
	Note Use the latest software version or maintenance release for each listed release.			
	Supported access points are:			
	Cisco Catalyst 9115 Series Access Points			
	Cisco Catalyst 9117 Series Access Points			
	Cisco Catalyst 9120 Series Access Points			
	Cisco Catalyst 9130 Series Access Points			
Cisco Catalyst 9300 and 9400 Series Switches	Supported versions are 17.3.3 and later			
Cisco Prime Infrastructure	Supported			
Catalyst Center	Supported			
Cisco Spaces: IoT Service	Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.3.1 and later			
	Not supported on Cisco AireOS Wireless Controller			
	• Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)			
Supported wireless controllers for Cisco FastLocate	Supported on Cisco AireOS Wireless Controller, Release 8.1.123.0			
	Supported on all releases of Cisco Catalyst 9800 Series Wireless Controllers			

Hardware or Application Name	Support for Cisco Spaces: Connector		
Supported wireless controllers for Cisco Hyperlocation	 Supported on Cisco AireOS Wireless Controller Supported on Cisco Catalyst 9800 Series Wireless Controllers 		
Connector Active-Active Mode	• Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)		
	Supported on Cisco Catalyst 9800 Series Wireless Controllers		
	Supported on Cisco AireOS Wireless Controller		
Tested VMware Environments	• VMware vSphere Client Version 7.0.x and 8.0		
	• VMware vCenter Server Appliance 7.0.x and 8.0		
Tested Proxies	• Squid proxy		
	• Forward-only mode (SSL tunneling)		
	• Squid-in-the-middle mode (SSL tunneling with intercept capabilities)		
	• McAfee		
	Cisco web security appliance		
Tested Access Points for Cisco FastLocate	Cisco Aironet 2800 Series Access Points		
	Cisco Aironet 3800 Series Access Points		
	Cisco Aironet 4800 Series Access Points		
Tested Access Points for Cisco FastLocate (Wi-Fi 6)	Cisco Catalyst 9120 Series Access Points		
	Cisco Catalyst 9130 Series Access Points		
Tested Access Points for Cisco Hyperlocation	Cisco Aironet 3700 Series Access Points (Requires hyperlocation antenna)		
	Cisco Aironet 4800 Series Access Point		

Hardware or Application Name	Support for Cisco Spaces: Connector
Tested Access Points	Cisco Catalyst 9105AX (I/W) Series Access Points
	Cisco Catalyst 9115AX (I/E) Series Access Points
	Cisco Catalyst 9117AX (I) Series Access Points
	Cisco Catalyst 9136 (I) Series Access Points
	Cisco Catalyst 9162 (I) Series Access Points
	Cisco Catalyst 9164 (I) Series Access Points
	Cisco Catalyst 9166 (I/D1) Series Access Points
	Cisco Catalyst IW9167 (E/I) Heavy Duty Series Access Points

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

	Primary IP Address	Disaster Recovery
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 Controller.

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)
	Not supported on Catalyst 9800 Controller running on Catalyst Switches in SD-Access mode (ECA)
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
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
L

Application Name	Support for Cisco Spaces: IoT Service
Access points for basic BLE gateway	Cisco Aironet 1815 Series Access Points
	• Cisco Aironet 2800 Series Access Points (USB dongle needed. No in-built USB radio)
	Cisco Aironet 3800 Series Access Points (USB dongle needed. No in-built USB radio)
Cisco IOx App Version	1.0.46 and later
	Note For Cisco Catalyst 9800 Series Wireless Controllers Cisco IOS XE Cupertino 17.7.x, ensure that the IoX Application version is upgraded to Version 1.3.x

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 Bl

Table 5: AP Modes and App Support

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

The following prerequisites can get you started with Cisco Spaces: IoT Service.

- Install Cisco Spaces: Connector in your network.
- Install a Cisco Catalyst 9800 Series Wireless Controller with a Cisco IOS XE Amsterdam 17.3.x image.

- Ensure that Cisco Spaces is configured with maps either from Cisco Prime Infrastructure or Catalyst Center.
- If the Cisco Spaces: Connector is an Amazon Elastic Compute Cloud (EC2) Instance from Amazon Machine Images (AMI), ensure that the wireless controller and connector are in the same virtual private cloud (VPC). Ensure that the wireless controller has a private IP address so that the security group of connector does not block the traffic, allowing enabled IOT streams to function.
- Permit all the TCP traffic at the Virtual private clouds (VPC) level so that the Telemetry Data Logger (TDL) is established without any issues.
- Before adding a Cisco Catalyst 9800 Series Wireless Controller to a connector, run the following commands on the Catalyst 9800 controller in a sequence:
 - aaa new-model
 - aaa authentication login default local
 - aaa authorization exec default local

These commands disable the connection services to Cisco Spaces.

- Cisco Spaces: IoT Service and Intelligent Capture (iCAP) feature can now co-exist on Cisco Catalyst 9800 Series Wireless Controller Cisco IOS XE Cupertino 17.7.x release and later. For releases earlier than Cisco IOS XE Cupertino 17.7.x, disable iCAP, if already enabled on the controller.
- Perform NTP synchronization over wireless controllers, a connector, and APs in the network.
- If a USB BLE module is inserted in an AP, reboot the AP.
- NETCONF must be enabled in Cisco Catalyst 9800 Series Wireless Controller in port 830, along with permission to use NETCONF.



Caution

on The application (app) installed and running over the AP uses the default 17.17.0.0/16 subnet. So, using this subnet for other purposes might create network issues.

- IPv6 is not supported on Cisco Spaces: Connector.
- If your require two connectors installed with 3.x to work with IoT service (wireless) and function as a high-availability pair, you must configure the connectors as Virtual IP (VIP) pair.

Access Points that support IoT Service (Wireless) are as follows:

- 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

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)

- **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

■ CISCO SPACE	is a second s
袋 Setup	⊙ ess network
	rks ces Connector
Map Service Camera	ay is get you wrietess network connecteu to caco crok opaces, no neo to upgrade wrietess can controllers of recornique your wrietess network.
	es Connector OVA paces Connector OVA as a virtual machine. medor 3
Webex	Paces Connector You will need a token to configure Spaces Connector. You need to connect to https://-your connector IP-/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS prov.
	2 / 2 connector(s) active
3	Add and associate controllers to your Clisco DNA Spaces Connector(s)
	1 / 2 controller(s) active Add Controllers View Controllers
4	Import Maps Prime/IDN4C map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report
	2 buildings imported Import/Sync Maps Map Upload History
	Z tions imported managements
(5)	Setup location nierarcny 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 Instances Active Inactive Service Switches 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

←Ba	ack Setup > Connectors > Test		ID	- : 81424448212902120000 Last Modified : Apr 29, 2022, 11:04:25 AM	
-0	SUMMARY 0 0 0 Instances Active Inactive	2 0 Services Switches enabled			
Ins	stances Configuration Metrics			🖉 Generate Token - 🐵 Troubleshoot Connector	
Se	ervices			() Add Services	
	Service Name	Version		Last Updated	
	000 service-manager	2.8.0.123	Never		
	,() iot-services	2.8.0.33	Never		
Sw	itches			Add Switch	

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.

- **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					×
Manage Co	onnector succ	ESS			Configure enable	e to
Enable IoT Stre	eams on Cisco DN	IA Spaces Conne	ector			
Use Manual Co automatically. Use the three	Use Manual Configuration to setup IoT Services in Controller when the configuration can not be applied automatically. Use the three dots action of Enable/Disable Stream to apply configuration changes to the Controller.					
Controller	Connector IP	Controller IP	Operation Status	Operation Log	Last updated	
sid-ewlc-2	172.20.239.157	172.20.239.18	SUCCESS	Successfully set config	Jun 14, 2022, 9:22:00 AM	:
sid-ewlc-3	172.20.239.157	172.20.239.38	SUCCESS	Successfully set config	Jun 14, 2022, 9:05:20 AM	:
Manage Controller Sample configuration Setup IoT Services stream authentication and certificate to allow APs to connect with the Cisco DNA Spaces Connector Sample configuration The WLC will be configured to send notifications to Cisco DNA Spaces Connector for AP configuration changes Sample configuration						
Cancel						

Verify Access Points

This task helps you verify whether your APs have synchronized with IoT service (wireless) and are visible on the IoT service (wireless) GUI.

- **Step 1** In the Cisco Spaces dashboard left-navigation pane, choose **IoT Services > IoT Gateways > AP Gateway**.
- **Step 2** Click the **All APs** tab to observe whether IoT service (wireless) has synchronized the APs in your network successfully and listed the APs.

Figure 154: Verify APs



Step 3Verify whether IoT service (wireless) has synchronized the APs in your network successfully and listed the APs. Observe
the Floor Beacon Channel Status and AP Beacon Channel Last Heard columns.Figure 155: Verify APs

	Floor Beacon Channel Status	IOx App Channel Status	Floor Beacon Channel Last Heard	AP Beacon Channel Last Heard
aces Demo>Floor 1	O UP	O UP	Sep 3rd, 2020 09:01:20 PM a few seconds ago	Sep 3rd, 2020 08:32:08 PM 29 minutes ago
aces Demo>Floor 1	• UP		Sep 3rd, 2020 09:01:35 PM	Sep 3rd, 2020 08:32:08 PM 29 minutes ago
aces Demo>Floor 1	• UP		Check the Last Heard time	Sep 3rd, 2020 08:32:08 PM 29 minutes ago
		Show	Records: 10 💌 1 - 3 🤇 🌖	>



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*



L



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



	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)

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
🔅 Setup	€ ess network
Wireless Networ Wired Network Map Service	ts exes 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 pases Contector OVA a virtual machine.
Webex	Connector You will need a token to configure Spaces Connector. You need to connect to https://vyour connector IP-/I from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS provy. 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
•	Import Maps Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report 2 buildings imported 2 buildings imported 2 foors imported Map Upload History Manage Maps
5	Setup 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 enabled	
Instances Configuration Metrics	P Generate 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.	

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 IoT Se	ervices				×
Manage Connecto Enable IoT Services on	r SUCCESS Cisco Spaces Conne	ector			Configure to enable
Use Manual Configurat	ion to setup IoT Serv	ices in switches w	nen the configuration ca	n not be applied automatica	ally.
Use the three dots action	on of Enable/Disable	Stream to apply co	onfiguration changes to t	the switches.	
Switch Name	Connector IP	Switch IP	Operation Status	Operation Log	Last updated
catalyst-9300-ga-1	10.22.243.64	10.22.243.73	SUCCESS	Successfully set config	May 13, 2023, 7:07:10 AM
Manage Switch Setup IoT Services stre The AireOS Controller v	am authentication ar	Id certificate to allo	w switches to connect to	with the Cisco Spaces Conr	Disable Service on nec t Enable Service changes.
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 1224
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 gp=-wic.AppGigabitEthermet_trunk glan_111_curest_stretcre.a
IOx application IP address	<pre>guest-ipaddress 10.10.111.13 netnask 255.255.255.0 vlan 1234 guest-interface 1</pre>
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 GRPC_SERVER_IP=10.10.111.0" run-opts 2 "-e GRPC_SERVER_DRET_R000"
IOx application netmask	<pre>run-opts 3 "-e GRPC_SERVER_TOKEN-eyJhoGci01JTU2IINiTSToR5c run-opts 4 "-e APP_HOST_LI=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 Connec	Manage Connector SUCCESS Configure to enable Enable IoT Services on Cisco DNA Spaces Connector					
Use Manual Configu	ration to setup IoT	Services in swit	ches when the config	uration can not be applie	ed automatically.	
Use the three dots a	ction of Enable/Di	isable Stream to	apply configuration ch	nanges 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 No	ext Last				(1 - 1 of 1) :	: 1 pages
Manage Switch					Sample configur	ation
Setup IoT Services s	tream authenticat	ion and certificat	e to allow switches to	connect with the Cisco	DNA Spaces Connector	
Manage IoT S	Click the switch to view the list of steps being executed on the switch.				× •	
Action	Sta	tus Mess	sage	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	
Switch monitor configuration SUCCESS Successfully set config Jun 3, 2021, 1:00:36 PM Jun 3, 3				Jun 3, 2021, 1:00:38 PM		
IOx application configu	Iration SU	CCESS Succ	essfully set config	Jun 3, 2021, 1:00:38 PM	Jun 3, 2021, 1:00:41 PM	U.
Disable Stream Logs						
Action Status Message			e s	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).

- **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

Jownload and install Spaces Connector OVA as a virtual machi Download Spaces Connector IC™	ine.			
Configure Spaces Connector	d to connect to https:// <your connector="" ip="">/ from a browser to configure the to</your>			
optionally configure Spaces Connector to connect via HTTPS p	roxy.			
1 / 1	Create a new token			
connector(s) active	View Connectors			
Switches added	View Switches			
Import Maps				
mport Maps				
mport Maps f you have wired devices and sensors plotted Prime/DNAC you	a can import them in to the location hierarchy			
ryou have wired devices and sensors plotted Prime/DNAC you	a can import them in to the location hierarchy			
r you have wired devices and sensors plotted Prime/DNAC you buildings imported	a can import them in to the location hierarchy Import/Sync Maps Map Upload History			

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

Figure 173: View Switches

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



Hotspot Service

- Configure Hotspot Service, on page 161
- Connector Dashboard: Hotspot service, on page 162
- Open Ports for Hotspot Service, on page 163

Configure Hotspot Service

- Step 1 In the Cisco Spaces dashboard left navigation pane, click Setup and choose Wireless Networks.
- Step 2In the Connect your wireless network window that is displayed, go to the Step 2 area and click View Connectors.Figure 174: View Connectors

E CISCO SPACE	E CISCO SPACES				
<u>14</u>					
^{sç,} setup					
	rks				
	rk 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.				
	ver Cannecter (1)/A				
	Spaces Connector OVA as a virtual machine.				
	PACES CONNECTOR You will need a token to configure Spaces Connector. You need to connect to https://cyour connector IP>/ from a browser to configure the token. You can optionally configure Spaces Connector to connect via				
	HTTPS proxy.				
	2 / 2 connector(s) active				
3	3 Add Controllers				
	Add and associate controllers to your Claco DNA Spaces Connector(s)				
	1 / 2 controllers) active Add Controllers				
	View Controlers				
4	Import Maps				
	Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report				
	buildings imported import/Sync Maps Map Upload History				
	2 floors Imported Manage Maps				
5	Setup location hierarchy				
	Unce the maps imported, you can adu them into location hierarchy				

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

 Figure 175: Add Service



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

Note service-manager is added by default.

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

Connector Dashboard: Hotspot service

Figure 176: Hotspot Service



Figure 177: Hotspot Service: Details



Open Ports for Hotspot Service

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

Figure 178: Open Ports for Hotspot Service



Test the connectivity between the connector and the wireless controller. See Configure and Test Connectivity between the Connector 3 and AireOS controller or Configure and Test the Connectivity between a Connector 3 and a Catalyst 9800 controller.



Local Firehose

- Local Firehose Service, on page 165
- Configure Local Firehose Service, on page 165
- Connector Dashboard: Local Firehose Service, on page 168

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.



A

Do not configure the virtual IP address (VIP) of VIP-paired connectors on the partner's location engine.

IoT Service supports high availability only in the VIP-paired mode.



Note

For creation and activation of a partner app, refer to the On-Prem Partner App

Configure Local Firehose Service

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.
	ses Connector OVA
	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 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 (i)
Incoming TAG RSSI events rate	0.02 events/second ①
Outgoing BLE RSSI events rate	0 events/second (i)
Incoming BLE RSSI events rate	0 events/second ①
Active gRPC Connection Count	0 count ①
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 171

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.

	Restrictio	 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.
Step 1	Log in to	Cisco Spaces.
	Note	The Cisco Spaces URL is region-dependent.
Step 2	In the Cis	co 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

Install Spaces Connector OVA	
Download and install Spaces Connector OVA as a virtual machine. Download Spaces Connector (?	
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 HTTP	to https:// <your connector="" ip="">/ from a browser to configure t S proxy.</your>
0/16	Create a new token
0740	View Connectors
Add Controllers	
Add and associate controllers to your Cisco DNA Spaces Connector(s)	
0 / 1 / controller(s) active	Add Controllers
0 / 14 controller(s) active	Add Controllers View Controllers
0 / 1 4 controller(s) active	Add Controllers View Controllers
0 / 1 4 controller(s) active	Add Controllers View Controllers rchy archy. You can only import controllers with at least one acces
0 / 1 4 controller(s) active	Add Controllers View Controllers Trchy archy. You can only import controllers with at least one acce

- **Step 6** From the **Connector** drop-down list, choose a Connector.
- Step 7 Enter the Controller IP address and Controller Name, and from the Controller Type drop-down list, choose WLC (AireOS) to connect to an AireOS controller.
- **Step 8** From the **Controller SNMP Version** drop-down list, choose the SNMP version of the AireOS controller.
 - If you choose the **SNMP** version as **v2C**, specify the SNMP read-write community.
 - If you choose the **SNMP** version as **v3**, specify the SNMP v3 version username, password, and authentication protocol credentials. Ensure that SNMP v3 has read-write permissions in the AireOS controller.
 - **Note** Both SNMP v2c and SNMP v3 must have read-write permission in the AireOS controller to register the Connector certificate in the AireOS controller. The Connector doesn't support SNMP v1.

Figure 184: Add a New AireOS controller

Add Controller	
Controller Type	
WLC (AireOS)	^
Controller SNMP Version	
v3	^
Username	
-	
Authentication Protocol	
HMAC-MD5	
Password	
	SHOW
Privacy Protocol	
CBC-DES	^
Privacy Password	
Test Operativity Dise to	
rest Connectivity Ping tes	R to the controller is successful, but owner test has failed. Please check
 Is SNMP enabled on the Can the connector reach 	controller? h SNMP port 161 on the controller?
3. Are correct SNMP RW c	redentials provided?
Save & Close Save &	Add Next Controller

Step 9 Click **Test Connectivity**. Connector issues ping and SNMP commands to check the connectivity to Cisco Spaces using the credentials provided.

Note Test Connectivity is enabled only when an active Connector is chosen.

Table 8: Error Description

Status of PING	Status of SNMP Test	Displayed Test Connectivity Message
SUCCESSFUL	SUCCESSFUL	Connectivity test is successful

Status of SNMP Test	Displayed Test Connectivity Message
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	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?
	Status of SNMP Test FAILED FAILED

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 177

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.

- **Step 1** Log in 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

Space	s Connector is an easy way to get your wireless network connected to	Cisco DNA Spaces. No need to upgrade Wireless LAN Control
1	Install Spaces Connector OVA	
	Download and install Spaces Connector Ovik as a virtual machine. Download Spaces Connector C	
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 HTTP	to https:// <your connector="" ip="">/ from a browser to configure the S proxy.</your>
	0/16	Create a new token
	0 / 40 connector(s) active	View Connectors
3	Add Controllers	,
Ĭ	Add and associate controllers to your Cisco DNA Spaces Connector(s)	
		Add Controllers
	0/14 composition active	View Controllers
4	Import Controllers into Location Hierar	chy
	Once the controllers are added, you can import them into your location hier point.	archy. You can only import controllers with at least one access
	1 / 1 / controller(s) imported to	Import Controllers

Step 6 From the **Connector** drop-down list, choose a Connector.

- Step 7Enter 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	
Catalyst WLC CLI Commands		
aaa new-model	ъ	
username dca9048dd2f8 mac aaa attrib	ute list cmx_dca9048dd2f8	
aaa attribute list cmx_dca9048dd2f8		
attribute type password 7e634b76188bf588d9a0922635d8bfdl	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	Status of SSH Credential Test	Meaning of status message combination and possible checks.
SUCCESSFUL	SUCCESSFUL	Connectivity test is successful.

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

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

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

Figure 188: Details of the Catalyst 9800 controller

Controller Channel			
TDL Incoming Msg Rate TDL Incoming Msg Count	0.00 events/second 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.

Cisco Spaces: Connector 3 Configuration Guide



APPENDIX

Connect Connector to Cisco Catalyst 9300 or 9400 Series Switches

Connecting a connector to Cisco Catalyst 9300 and 9400 Series Switches , on page 183

Connecting a connector to Cisco Catalyst 9300 and 9400 Series Switches

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.** Log in 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

Step 1 Log in 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.

Download and install Spaces Connector OVA as a virtual n	• nachine.
Download Spaces Connector IZ™	
Configure Spaces Connector	
You will need a token to configure Spaces Connector. You optionally configure Spaces Connector to connect via HTT	need to connect to https:// <your connector="" ip="">/ from a browser to configure the tok PS proxy.</your>
1/1	Create a new token
connector(s) active	View Connectors
Add Switch Associate Switches with Cisco DNA Spaces Connector(s)	Add Switches
Add Switch Associate Switches with Cisco DNA Spaces Connector(s)	Add Switches View Switches
Add Switch Associate Switches with Cisco DNA Spaces Connector(s) J Switches added	Add Switches View Switches
Add Switch Associate Switches with Cisco DNA Spaces Connector(s) J Switches added mport Maps 'you have wired devices and sensors plotted Prime/DNAG	Add Switches View Switches
Add Switch Associate Switches with Cisco DNA Spaces Connector(s) Switches added mport Maps 'you have wired devices and sensors plotted Prime/DNAd	Add Switches View Switches
Add Switch Associate Switches with Cisco DNA Spaces Connector(s) 1 Switches added mport Maps 'you have wired devices and sensors plotted Prime/DNAd 2 buildings imported	Add Switches View Switches C you can import them in to the location hierarchy Import/Sync Maps Map Upload History

- **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.
- **Step 5** Click **Test** to see if the connection to the switch.
- **Step 6** Do one of the following:

Figure 189:

- Click Save & Add Next Switch
- Click Save & Close