Cisco Spaces: Connector Configuration Guide

First Published: 2019-08-01

Last Modified: 2022-03-16

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

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

PART I

Overview 11

CHAPTER 1

Overview 1

Introduction to Cisco Spaces: Connector 2.x 1

PART II

Getting Started 3

CHAPTER 2

Prerequisites 5

Prerequisites for Configuring the Cisco Spaces: Connector 5

Prerequisites for the Cisco Spaces: Connector (Wired) 6

CHAPTER 3

Open Ports (Wireless) 7

Information About Open Ports (Wireless) 7

OpenRoaming Firewall Rules 9

CHAPTER 4

Open Ports (Wired) 11

Open Ports for IoT Service (Wired) 11

PART III Initial Setup 13

CHAPTER 5 Initial Setup 15

Initial Setup of Cisco Spaces: Connector 15

CHAPTER 6 Cisco Spaces: Connector AMI 17

Downloading and Deploying the Cisco Spaces: Connector AMI 17

CHAPTER 7 Cisco Spaces: Connector OVA 25

Downloading and Deploying the Cisco Spaces: Connector OVA (Single Interface) 25

Downloading and Deploying the Cisco Spaces: Connector OVA (Dual Interface) 31

Upgrade the Cisco Spaces: Connector Docker 41

Upgrade Path 43

Upgrading the Connector OVA 44

Using Snapshots for Backup 45

CHAPTER 8 Cisco Spaces: Connector Hyper-V 47

Creating a Virtual Switch 47

Downloading and Deploying Hyper-V 54

CHAPTER 9 Connector on Cisco Spaces 65

Creating a Connector Instance and Retrieving a Token from Cisco Spaces (Wired) 65

Retrieving a Token for a Connector from Cisco Spaces (Wireless) 67

Activating the Cisco Spaces: Connector 70

CHAPTER 10 Connector GUI 73

Connector GUI 73

CHAPTER 11 Configuring Proxy 77

Configuring a Proxy 77

Troubleshooting Proxy Configuration 79

CHAPTER 12 **Connect Connector to Cisco AireOS Wireless Controller** 81

Configure and Test Connectivity Between a Connector and AireOS Controller 81

CHAPTER 13 **Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers** 87

Configure and Test the Connection Between Connector and Catalyst 9800 Controller 87

CHAPTER 14 **Connecting a Connector to Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches Series** 93

Connecting a Connector to Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches 93

PART IV **Location Hierarchy** 95

CHAPTER 15 **Location Hierarchy** 97

Importing a Cisco AireOS Wireless Controller to the Cisco Spaces Location Hierarchy 97

PART V **Privacy Setting** 103

CHAPTER 16 **Configure Privacy Settings** 105

Configuring Privacy Settings: MAC and Username Salt 105

PART VI **HotSpot (OpenRoaming)** 107

CHAPTER 17 **Hotspot (OpenRoaming)** 109

HotSpot (OpenRoaming) 109

Upgrade the OpenRoaming Docker 109

PART VII **AAA** 111

CHAPTER 18 **Configure AAA** 113

Configure AAA 113

Information About AAA 113

Configure AAA 114

PART VIII Connectors in Active-Active 117

CHAPTER 19 Connectors in Active-Active 119

Connector Active-Active 119

Restrictions 119

Connector Active-Active vs Cisco CMX High Availability 121

Configuring Connectors in Active-Active 121

Configuring Connectors in Active-Active (Wired) 124

PART IX Communications, Services, and Additional Information 129

CHAPTER 20 Communications, Services, and Additional Information 131

Cisco Bug Search Tool 131

Documentation Feedback 131

Preface

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

Audience

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

Conventions

This document uses the following conventions:

Table 1: Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string. Otherwise, the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.

Convention	Indication
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

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

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

Related Documentation

Cisco Spaces: Connector3 Configuration Guide

Cisco Spaces: Connector3 Command Reference Guide

Release Notes for Cisco Spaces: Connector

Cisco Spaces: IoT Service Configuration Guide (Wireless)

Cisco Spaces: IoT Service Configuration Guide (Wired)

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

Documentation Feedback

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

PART I

Overview

- Overview, on page 1

CHAPTER 1

Overview

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

- Introduction to Cisco Spaces: Connector 2.x, on page 1

Introduction to Cisco Spaces: Connector 2.x

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.

The Cisco Spaces: Connector enables Cisco Spaces to run different services on the Connector, which in turn, communicates with different network devices such as controllers and switches.

The various services that run on the Connector gather and aggregate data from controllers, APs, and switches efficiently, and sends the aggregated data to Cisco Spaces. The Connector architecture allows multiple controllers, APs, and switches to connect to Cisco Spaces through a single point (the Connector). A single Connector can connect to a Cisco AireOS Wireless Controller, Cisco Catalyst 9800 Series Wireless Controller and Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches at the same time.

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

Note The term controller is used in this document to refer to the following. (See Compatibility Matrix for specific details).

- Cisco AireOS Wireless Controller (indicated on the Cisco Spaces dashboard as WLC AireOS)
- Cisco Catalyst 9800 Series Wireless Controller (indicated on the Cisco Spaces dashboard as Catalyst WLC)
- Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)

PART II

Getting Started

- Prerequisites, on page 5
- Open Ports (Wireless), on page 7
- Open Ports (Wired), on page 11

CHAPTER 2

Prerequisites

- Prerequisites for Configuring the Cisco Spaces: Connector, on page 5
- Prerequisites for the Cisco Spaces: Connector (Wired), on page 6

Prerequisites for Configuring the Cisco Spaces: Connector

- Ensure that the necessary ports are open. See Information About Open Ports (Wireless), on page 7.
- Ensure that you explicitly allow https://www.cisco.com and cisco.com domains so that the Cisco Spaces: Connector can establish connections with these websites or domains.
- Ensure that you explicitly allow https://cisco.openroaming.org. if you need to deploy OpenRoaming.
- For Simple Network Management Protocol (SNMP) v2C and v3, you require read-write permissions for registering the Cisco Spaces: Connector certificate with the Cisco AireOS Wireless Controller.
- If the Cisco Spaces: Connector is deployed as an AWS instance using AMI, ensure that controllers are reachable from the Connector. It is recommended that the controller and the Connector are in the same virtual private cloud (VPC). Ensure that the controller has a private IP address so that the security group of the Connector does not block the traffic allowing enabled IOT streams to function.
- Permit all TCP traffic at the VPC level so that the TDL is established without any issues.
- Disable Cisco Spaces connection services on a Cisco AireOS Wireless Controller before enabling the Cisco Spaces: Connector, using the **config cloud-services cmx disable** command.
- Disable Cisco Spaces connection services on a Cisco Catalyst 9800 Series Wireless Controller before enabling the Cisco Spaces: Connector, by running these commands:
    - **no nmsp cloud-services server url**
    - **no nmsp cloud-services server token**
    - **no nmsp cloud-services enable**
- The controller IP you configure in the Cisco Spaces dashboard must be able to reach the Cisco Spaces: Connector.
- The Cisco Spaces: Connector requires access to a Domain Name System (DNS) server. If you configure an explicit proxy, the Cisco Spaces: Connector must be able to communicate using the proxy.
- VMware ESXi 6.5 or later.

- Virtual machine size: Standard option
- Minimum bandwidth required: 4 Mbps (5000 APs, 60,000 clients).

Note If you are using captive portals, we recommend a minimum bandwidth of 30 Mbps along with a buffer. The bandwidth allows for a good enduser experience while loading captive portals from Cisco Spaces.

Prerequisites for the Cisco Spaces: Connector (Wired)

- Ensure that the necessary ports are open. See Open Ports for IoT Service (Wired), on page 11.
- Ensure that you explicitly allow https://www.cisco.com and cisco.com domains so that the Cisco Spaces: Connector can establish connections with these websites or domains.
- The Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches IP you configure in the Cisco Spaces dashboard must be able to reach the Cisco Spaces: Connector.
- Cisco Spaces: Connector requires Domain Name System (DNS) server permitted. If you configure an explicit proxy, Cisco Spaces: Connector must be able to communicate using a proxy.
- VMware ESXi 6.5 or above.
- Virtual machine size: Standard option
- Minimum bandwidth required: 4 Mbps (5000 APs, 60,000 clients).

Note If you are using captive portals, we recommend a minimum bandwidth of 30 Mbps along with a buffer. The bandwidth allows for a good enduser experience while loading captive portals from Cisco Spaces.

CHAPTER 3

Open Ports (Wireless)

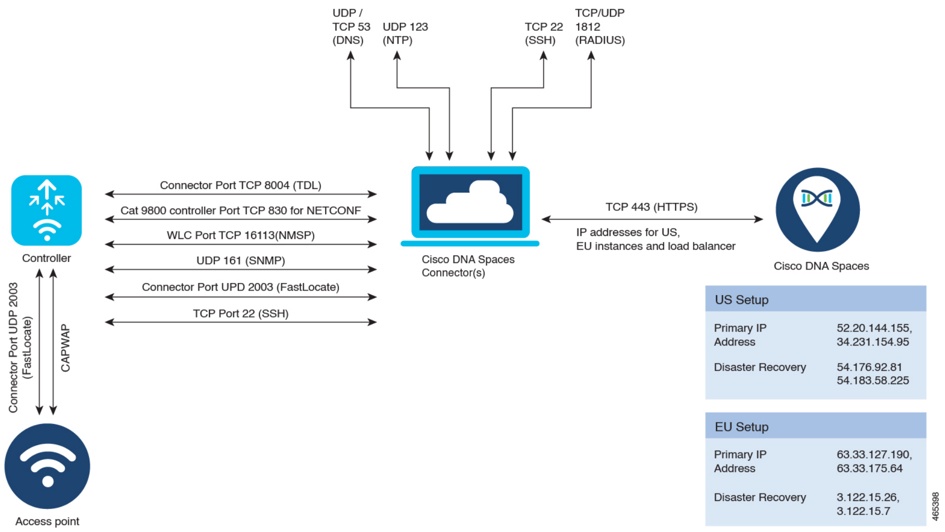
- Information About Open Ports (Wireless), on page 7
- OpenRoaming Firewall Rules, on page 9

Information About Open Ports (Wireless)

This chapter lists the Connector ports that need to be open for the proper functioning of various services or protocols.

The following ports need to be opened to allow for the basic functionality of Cisco Spaces.

Figure 1: Basic Functionality



UDP / TCP 53 (DNS)
UDP 123 (NTP)
TCP 22 (SSH)
TCP/UDP 1812 (RADIUS)
Controller
Connector Port TCP 8004 (TDL)
Cat 9800 controller Port TCP 830 for NETCONF
WLC Port TCP 16113(NMSP)
UDP 161 (SNMP)
Connector Port UPD 2003 (FastLocate)
TCP Port 22 (SSH)
Cisco DNA Spaces Connector(s)
TCP 443 (HTTPS)
IP addresses for US, EU instances and load balancer
Cisco DNA Spaces
Connector Port UDP 2003 (FastLocate)
CAPWAP
Access point
465398

US Setup	
Primary IP Address	52.20.144.155, 34.231.154.95
Disaster Recovery	54.176.92.81 54.183.58.225

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

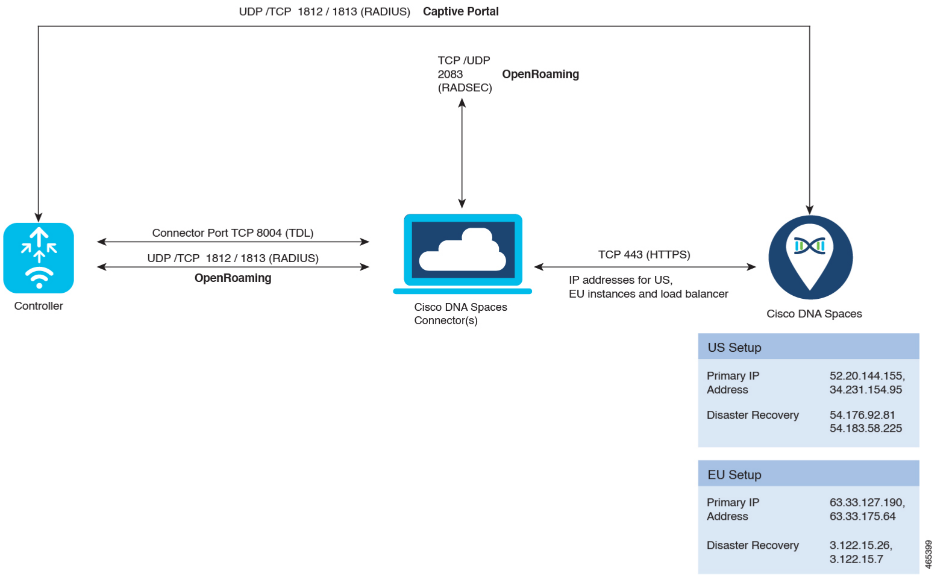
Table 2: Setups

	Primary IP Address	Disaster Recovery
US Setup	52.20.144.155 34.231.154.95	54.176.92.81 54.183.58.225

	Primary IP Address	Disaster Recovery
EU Setup	63.33.127.190 63.33.175.64	3.122.15.26 3.122.15.7
Singapore Setup (SG)	13.228.159.49 54.179.105.241	13.214.251.223 54.255.57.46

In addition to basic functionality, additional ports need to be opened for other additional functionality like guest onboarding and IoT Services.

Figure 2: Guest Onboarding

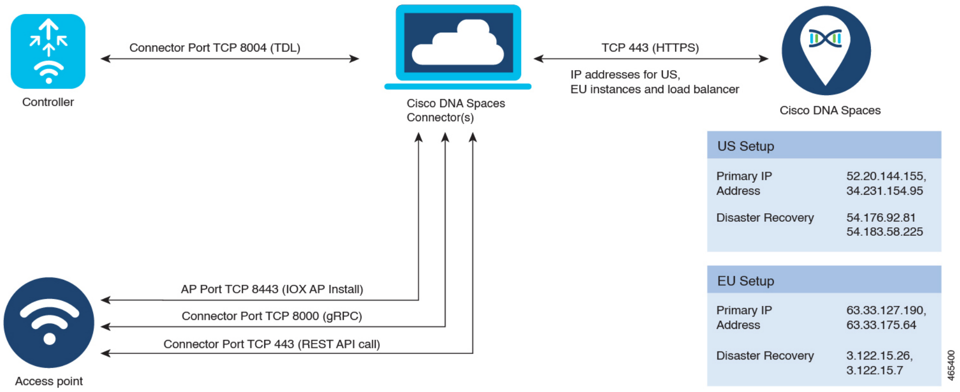


US Setup	
Primary IP Address	52.20.144.155, 34.231.154.95
Disaster Recovery	54.176.92.81 54.183.58.225

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

The following ports need to be opened for configuring IoT Services (wireless). To configure IoT Services (wired), see Open Ports (Wired)

Figure 3: IoT Services


Connector Port TCP 8004 (TDL)
Controller
Cisco DNA Spaces
Connector(s)
TCP 443 (HTTPS)
IP addresses for US,
EU instances and load balancer
Cisco DNA Spaces
AP Port TCP 8443 (IOX AP Install)
Connector Port TCP 8000 (gRPC)
Connector Port TCP 443 (REST API call)
Access point
465400

US Setup	
Primary IP Address	52.20.144.155, 34.231.154.95
Disaster Recovery	54.176.92.81 54.183.58.225

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

OpenRoaming Firewall Rules

Table 3: OpenRoaming Firewall Rules

Source IP Address	Destination IP Address	Direction	Transport	Source Port	Destination Port	Protocol	Further information
Cisco AireOS Wireless Controller IP address	Connector	Unidirectional	UDP and TCP	Any	1812, 1813	Remote Authentication Dial-In User Service (RADIUS)	Communication between Connector and Cisco AireOS Wireless Controller for OpenRoaming client's RADIUS messages.
Connector	Any	Unidirectional	TCP	Any	2083	RADIUS over TLS (RADSEC)	Communication between Connector and OpenRoaming Identity Providers
Connector	Any	Unidirectional	TCP	Any	443		HTTPS for CSR signing - OpenRoaming Membership

CHAPTER 4

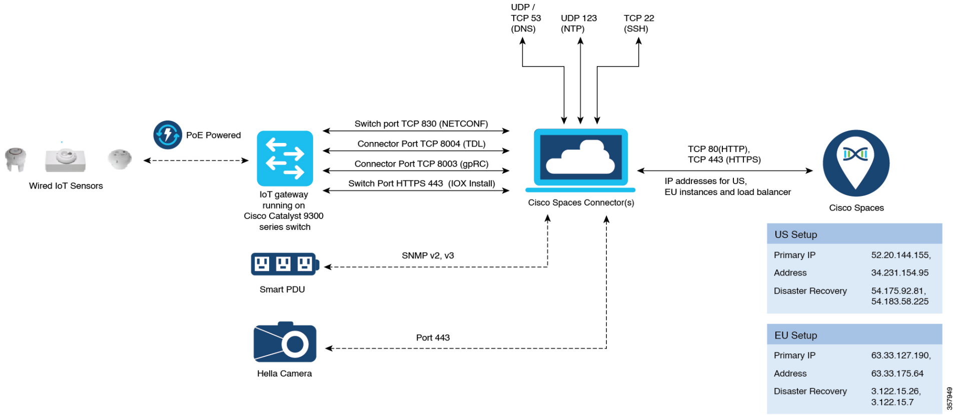
Open Ports (Wired)

- Open Ports for IoT Service (Wired), on page 11

Open Ports for IoT Service (Wired)

This section lists the Connector ports that need to be open for the proper functioning of each service or protocol.

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

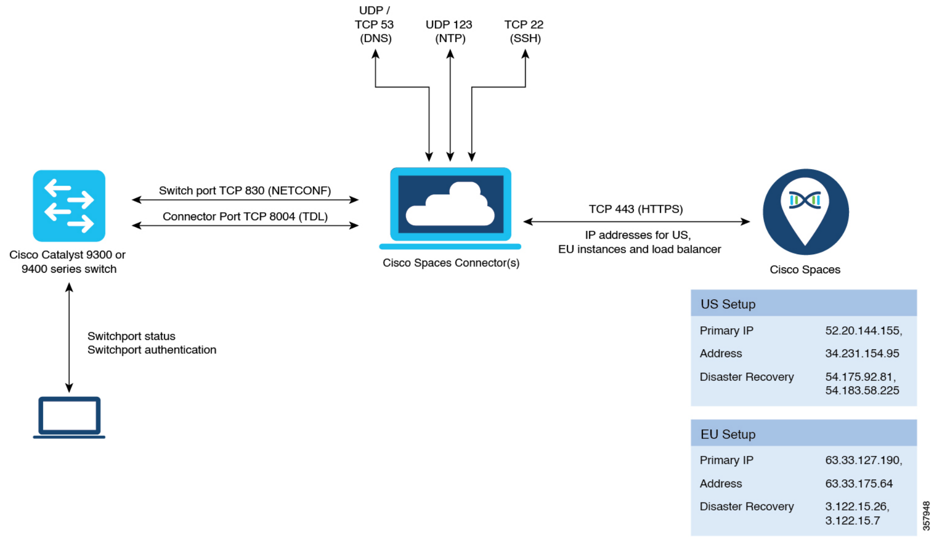


UDP / TCP 53 (DNS)
UDP 123 (NTP)
TCP 22 (SSH)
PoE Powered
Wired IoT Sensors
Switch port TCP 830 (NETCONF)
Connector Port TCP 8004 (TDL)
Connector Port TCP 8003 (gpRC)
Switch Port HTTPS 443 (IOX Install)
IoT gateway running on Cisco Catalyst 9300 series switch
Cisco Spaces Connector(s)
TCP 80(HTTP), TCP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

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

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

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


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

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

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

Table 4: Setups

	Primary IP Address	Disaster Recovery
US Setup	52.20.144.155 34.231.154.95	54.176.92.81 54.183.58.225
EU Setup	63.33.127.190 63.33.175.64	3.122.15.26 3.122.15.7
Singapore Setup (SG)	13.228.159.49 54.179.105.241	13.214.251.223 54.255.57.46

PART III

Initial Setup

- Initial Setup, on page 15
- Cisco Spaces: Connector AMI , on page 17
- Cisco Spaces: Connector OVA , on page 25
- Cisco Spaces: Connector Hyper-V, on page 47
- Connector on Cisco Spaces , on page 65
- Connector GUI, on page 73
- Configuring Proxy, on page 77
- Connect Connector to Cisco AireOS Wireless Controller, on page 81
- Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers, on page 87
- Connecting a Connector to Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches Series , on page 93

CHAPTER 5

Initial Setup

- Initial Setup of Cisco Spaces: Connector, on page 15

Initial Setup of Cisco Spaces: Connector

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

1. Install the Cisco Spaces: Connector in your local deployment network. See Downloading and Deploying the Cisco Spaces: Connector OVA (Single Interface) , on page 25
2. On the Cisco Spaces dashboard, create a Cisco Spaces: Connector and generate a token for the Connector. See Retrieving a Token for a Connector from Cisco Spaces (Wireless), on page 67 or Creating a Connector Instance and Retrieving a Token from Cisco Spaces (Wired), on page 65
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 (based on the token) on the Cisco Spaces now turns active. See Activating the Cisco Spaces: Connector , on page 70
4. Configure a Cisco AireOS Wireless Controller or a Cisco Catalyst 9800 Series Wireless Controller or a Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches in the Cisco Spaces dashboard. See #unique_29 or Configure and Test the Connection Between Connector and Catalyst 9800 Controller, on page 87 or Connecting a Connector to Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches , on page 93. Test the connectivity between the Connector and the controller or the switch.

CHAPTER 6

Cisco Spaces: Connector AMI

- Downloading and Deploying the Cisco Spaces: Connector AMI , on page 17

Downloading and Deploying the Cisco Spaces: Connector AMI

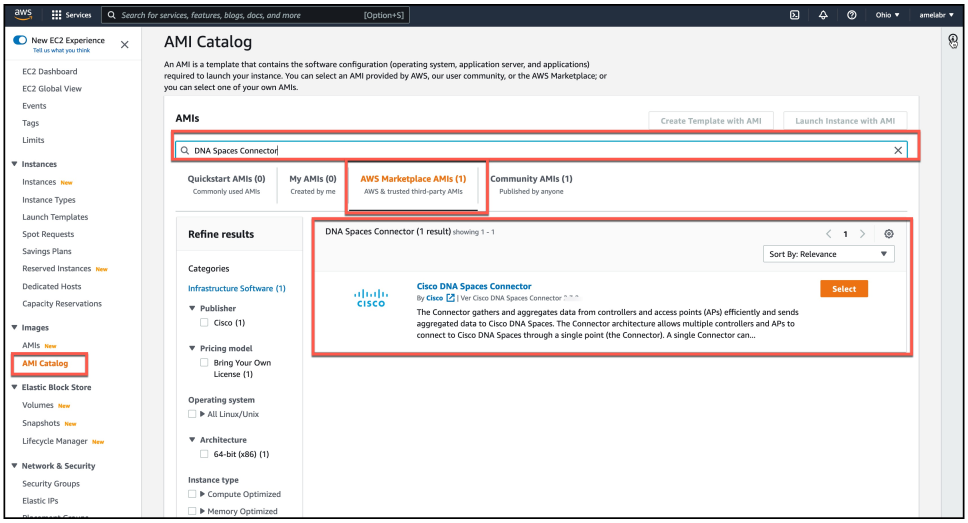
This chapter provides information about how to download and deploy the Cisco Spaces: Connector and obtain the URL for the Connector GUI.

Note Cisco Spaces: Connector has the following limitations:

- Dual-interface mode is not supported.
- Proxy configuration is not supported.
- Enabling or disabling the AAA with IPSec feature is not supported.
- Upgrading the Connector from the Web UI is not supported.

Step 1 Log in to your Amazon Web Services account and navigate to the **EC2 Dashboard**. From 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.



AMI Catalog

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

AMIs

DNA Spaces Connector

DNA Spaces Connector (1 result) showing 1 - 1

Sort By: Relevance

Cisco DNA Spaces Connector

By Cisco | Ver Cisco DNA Spaces Connector

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

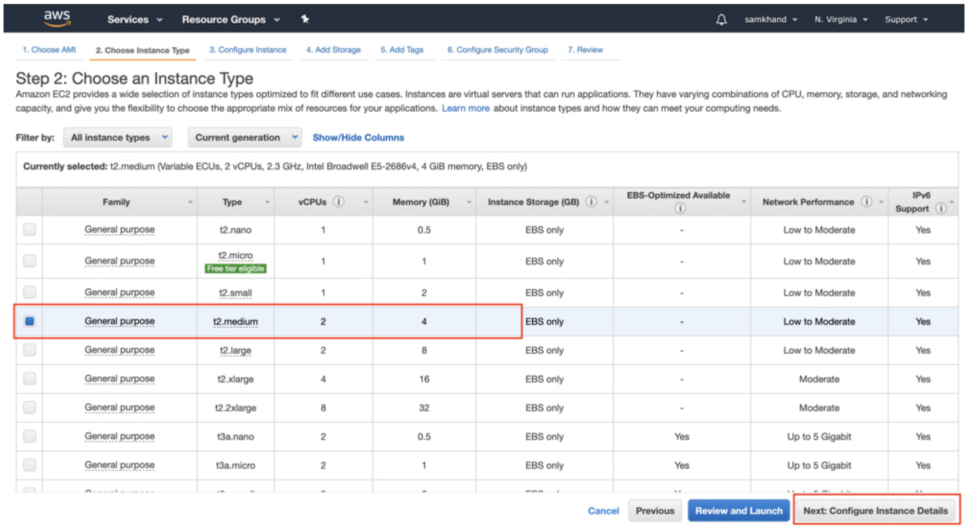
Step 3 Click the displayed image and click **Select**.

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

Step 5 Click **Launch Instance with AMI**

Step 6 Choose an instance with the corresponding **Type** as **t2.medium**, that has **vCPU** value as **2** and **Memory (GB)** as **4**.

t2.medium corresponds to a standard Cisco Spaces: Connector with 2vCPUs and 4-GB memory and is the recommended setting, and then click **Next: Configure Instance Details**.



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types | Current generation | Show/Hide Columns

Currently selected: t2.medium (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB memory, EBS only)

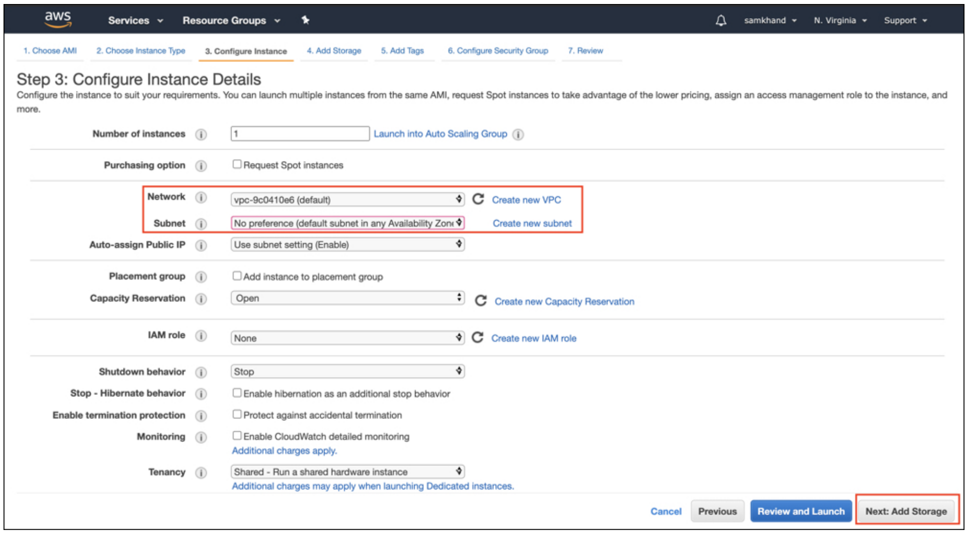
	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
■	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
□	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
□	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

Note You can choose to have a more advanced configuration by choosing an option with higher vCPU and memory configurations. You can choose an instance type with 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 7 Choose a **Network** and a **Subnet**. Click **Next: Add Storage**.

Figure 4: Configure Instance Details



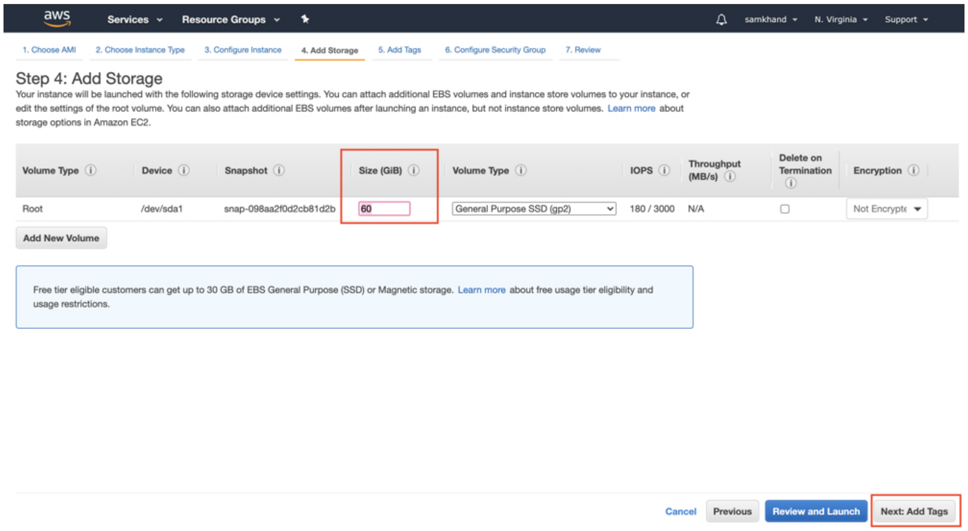
Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-9c0410e6 (default) Create new VPC
Subnet	No preference (default subnet in any Availability Zone Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)
Placement group	□ Add instance to placement group
Capacity Reservation	Open Create new Capacity Reservation
IAM role	None Create new IAM role
Shutdown behavior	Stop
Stop - Hibernate behavior	□ Enable hibernation as an additional stop behavior
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges may apply when launching Dedicated instances.

Step 8 Enter the value of **Size(GB)** as 60. Click **Next: Add Tags**.

Figure 5: Add Storage



Step 4: Add Storage

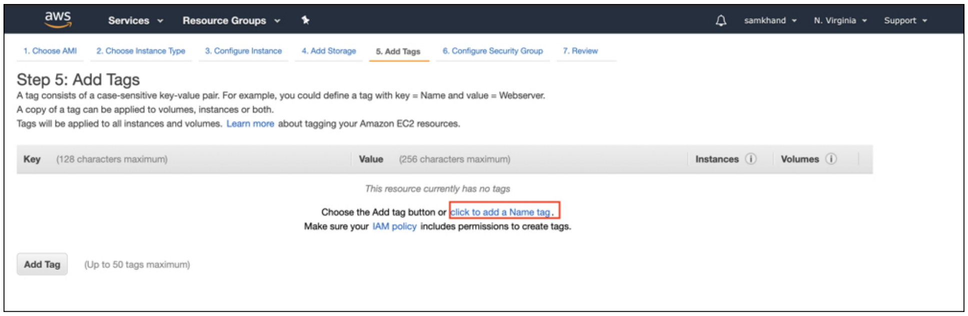
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-098aa2f0d2cb81d2b	60	General Purpose SSD (gp2)	180 / 3000	N/A	□	Not Encrypte

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Step 9 Click **click to add a Name tag**. Enter a name, and then lick **Next: Configure Security Group**.

Figure 6: Add Tags



Step 5: Add Tags

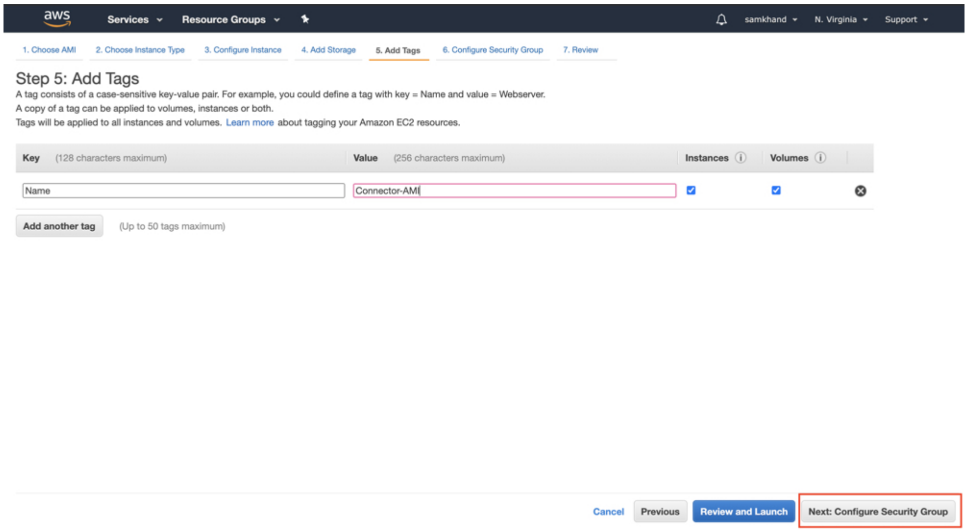
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes

This resource currently has no tags

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

Figure 7: Enter a Tag Name



Step 5: Add Tags

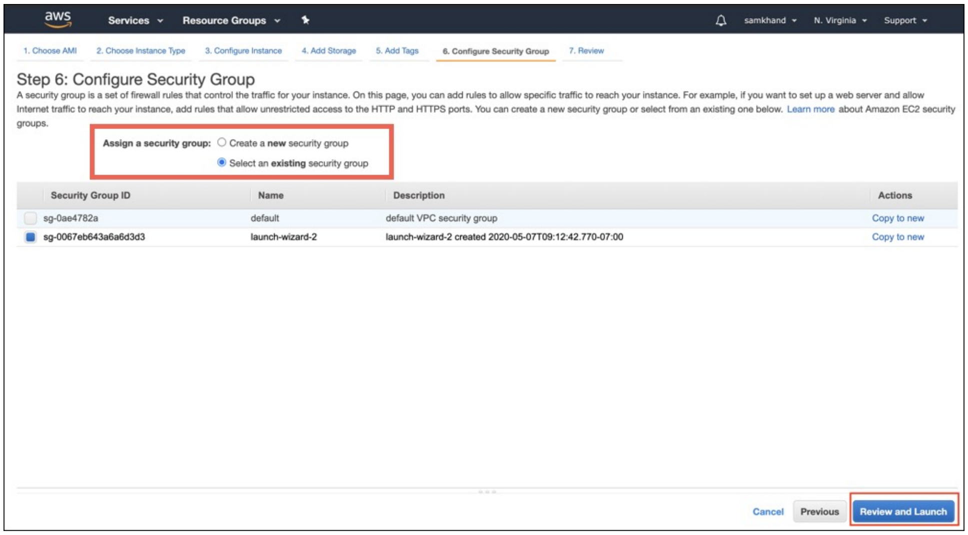
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	Connector-AMI	☑	☑

Step 10 Configure a security group by following these steps:

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

Figure 8: Configure Security Group



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

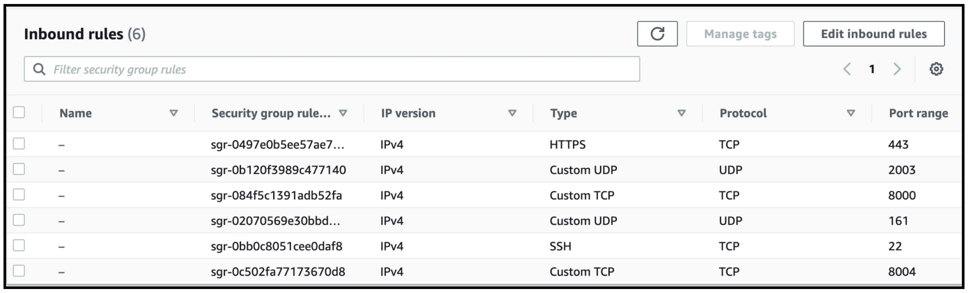
Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

	Security Group ID	Name	Description	Actions
□	sg-0ae4782a	default	default VPC security group	Copy to new
■	sg-0067eb643a6a6d3d3	launch-wizard-2	launch-wizard-2 created 2020-05-07T09:12:42.770-07:00	Copy to new

b) Configure ports with rules for inbound traffic. You can choose to restrict them for specific IP addresses or keep them open for all IP addresses.

Configure the specific ports displayed in the image with rules for inbound traffic:

Figure 9: Configure Ports with Rules for Inbound Traffic



Inbound rules (6)

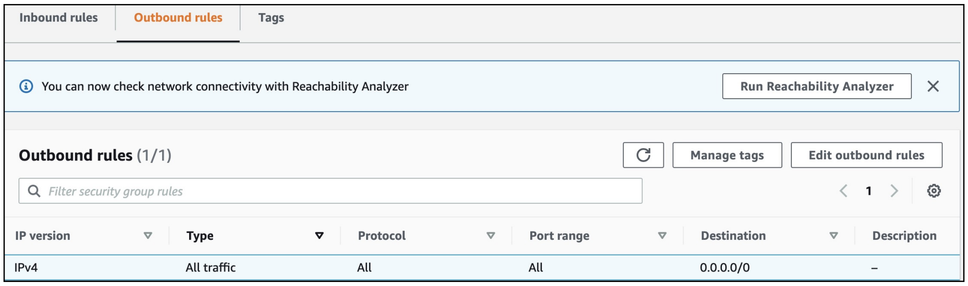
□	Name	Security group rule...	IP version	Type	Protocol	Port range
□	–	sgr-0497e0b5ee57ae7...	IPv4	HTTPS	TCP	443
□	–	sgr-0b120f3989c477140	IPv4	Custom UDP	UDP	2003
□	–	sgr-084f5c1391adb52fa	IPv4	Custom TCP	TCP	8000
□	–	sgr-02070569e30bbd...	IPv4	Custom UDP	UDP	161
□	–	sgr-0bb0c8051cee0daf8	IPv4	SSH	TCP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

Note Specify the network subnet ranges within the inbound rule to access this instance using SSH.

c) Configure ports with rules for outbound traffic.

Configure the outbound rule indicated in the following image:

Figure 10: Configure Ports with Rules for Outbound Traffic



You can now check network connectivity with Reachability Analyzer

Outbound rules (1/1)

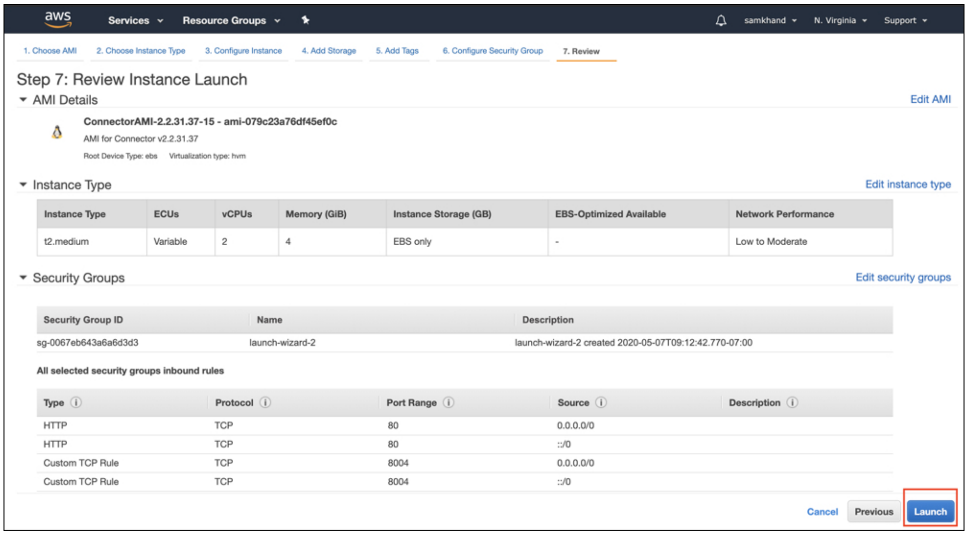
IP version	Type	Protocol	Port range	Destination	Description
IPv4	All traffic	All	All	0.0.0.0/0	–

Note See Information About Open Ports (Wireless), on page 7 for details on ports that you must open for various services to work.

d) Click **Review and Launch**.

Step 11 Review the instance and click **Launch**.

Figure 11: Review Instance and Launch



Step 7: Review Instance Launch

AMI Details

ConnectorAMI-2.2.31.37-15 - ami-079c23a76df45ef0c
AMI for Connector v2.2.31.37
Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.medium	Variable	2	4	EBS only	-	Low to Moderate

Security Groups

Security Group ID	Name	Description
sg-0067eb643a6a6d3d3	launch-wizard-2	launch-wizard-2 created 2020-05-07T09:12:42.770-07:00

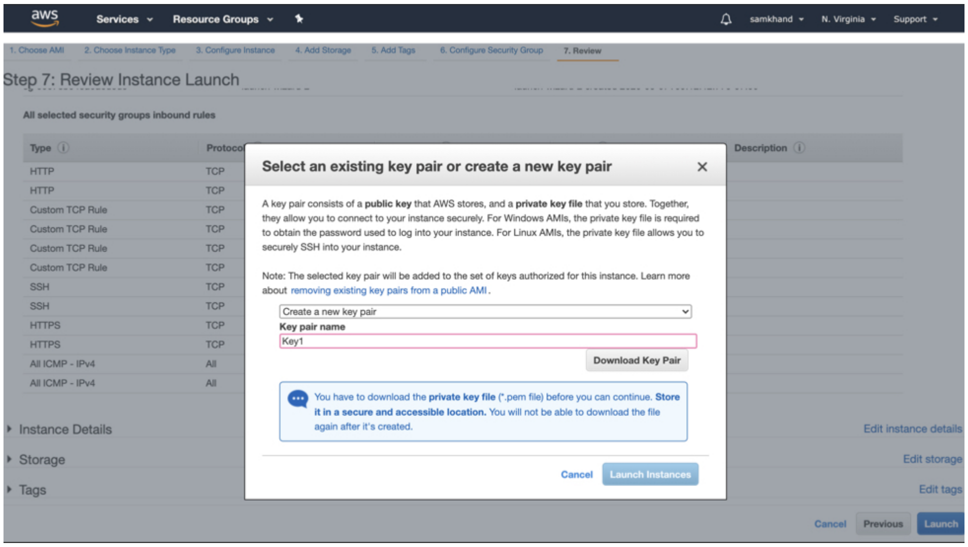
All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	
Custom TCP Rule	TCP	8004	0.0.0.0/0	
Custom TCP Rule	TCP	8004	::/0	

Step 12 In the displayed **Select an existing key pair or create a new key pair** dialog box, you can do one of the following:

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

Figure 12: Create a New Key Pair



Select an existing key pair or create a new key pair

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

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

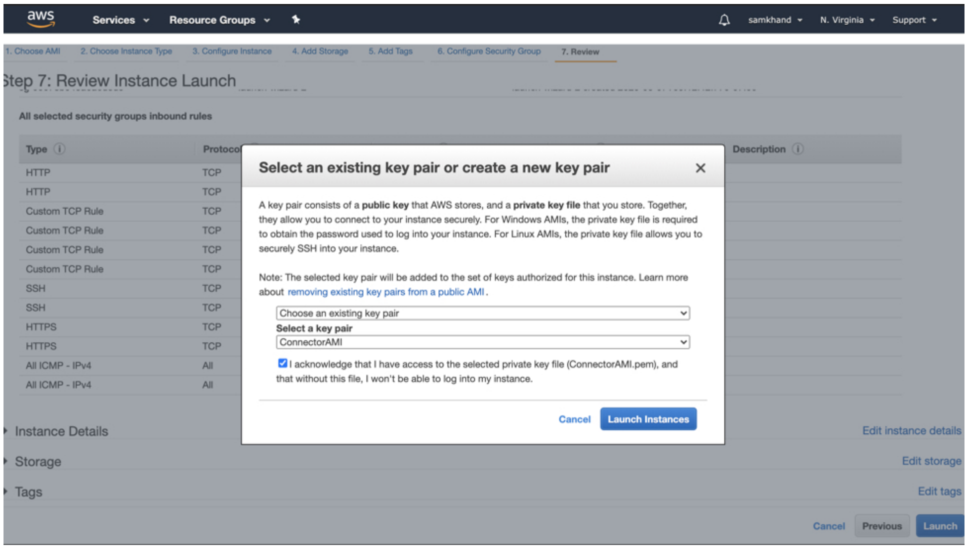
Create a new key pair

Key pair name

Key1

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.

Figure 13: Choose an Existing Key Pair



Step 7: Review Instance Launch

All selected security groups inbound rules

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

Select an existing key pair or create a new key pair ✕

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

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

Choose an existing key pair

Select a key pair: ConnectorAMI

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

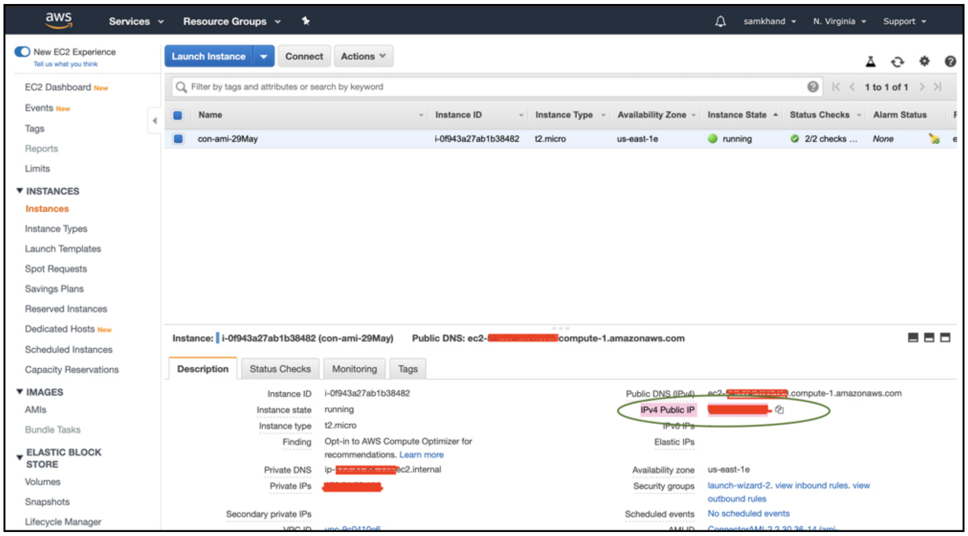
Cancel | Launch Instances

Step 13 Once you download the key pair (.pem) file to your system, navigate to the file location. Using the **chmod** command, configure appropriate permissions for the .pem file.

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

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 that is used to launch the CLI, where you can complete the setup.

Figure 14: Instances Page and IPv4 Address



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
con-ami-29May	i-0f943a27ab1b38482	t2.micro	us-east-1e	running	2/2 checks ...	None

Instance: i-0f943a27ab1b38482 (con-ami-29May) Public DNS: ec2-[redacted]compute-1.amazonaws.com

Instance ID	i-0f943a27ab1b38482	Public DNS (IPv4)	ec2-[redacted].compute-1.amazonaws.com
Instance state	running	IPv4 Public IP	[redacted]
Instance type	t2.micro	IPv6 IPs	
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more	Elastic IPs	
Private DNS	ip-[redacted]ec2.internal	Availability zone	us-east-1e
Private IPs	[redacted]	Security groups	launch-wizard-2. view inbound rules. view outbound rules
Secondary private IPs		Scheduled events	No scheduled events

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

a) Log in to the Connector using the **SSH** command, the IPv4 address obtained in **Step 12**, and the key pair downloaded in **Step 10**.

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

b) Change the username and password for **root** and **dnasadmin** user. Use the initial login username **dnasadmin** and the login password **dnasadmin123!**.

You can avoid a BAD PASSWORD prompt by complying to the following password requirements:

- Password length must be more than 14 characters.
- Password must include at least one uppercase letter.
- Password must include at least one lowercase letter.
- Password must include at least one special character.

The following is the sample output of the SSH command:

```
ssh -i /path/to/key/MyAccessKey1.pem dnasadmin@10.1.1.1
Password:
WELCOME to DNA SPACES CONNECTOR SETUP
Please enter hostname: my-connector-ami
Change passwords for root and dnasadmin
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 14 characters
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
BAD PASSWORD: The password is shorter than 14 characters
Retype new password:
passwd: all authentication tokens updated successfully.
Generating self-signed certificates ...
Setup is complete
System will reboot in 10 seconds ...
Connection to 10.1.1.1 closed by remote host.
Connection to 10.1.1.1 closed.
```

Step 16 Log in to the Cisco Spaces: Connector GUI using the browser window and the address https://*IPv4 Address*.

Step 17 Log in to the Cisco Spaces: Connector CLI using the SSH username **dnasadmin** and the password configured for this user in Step 15.

```
ssh dnasadmin@10.1.1.1
```

CHAPTER 7

Cisco Spaces: Connector OVA

- Downloading and Deploying the Cisco Spaces: Connector OVA (Single Interface) , on page 25
- Downloading and Deploying the Cisco Spaces: Connector OVA (Dual Interface), on page 31
- Upgrade the Cisco Spaces: Connector Docker, on page 41
- Upgrade Path, on page 43
- Upgrading the Connector OVA , on page 44
- Using Snapshots for Backup , on page 45

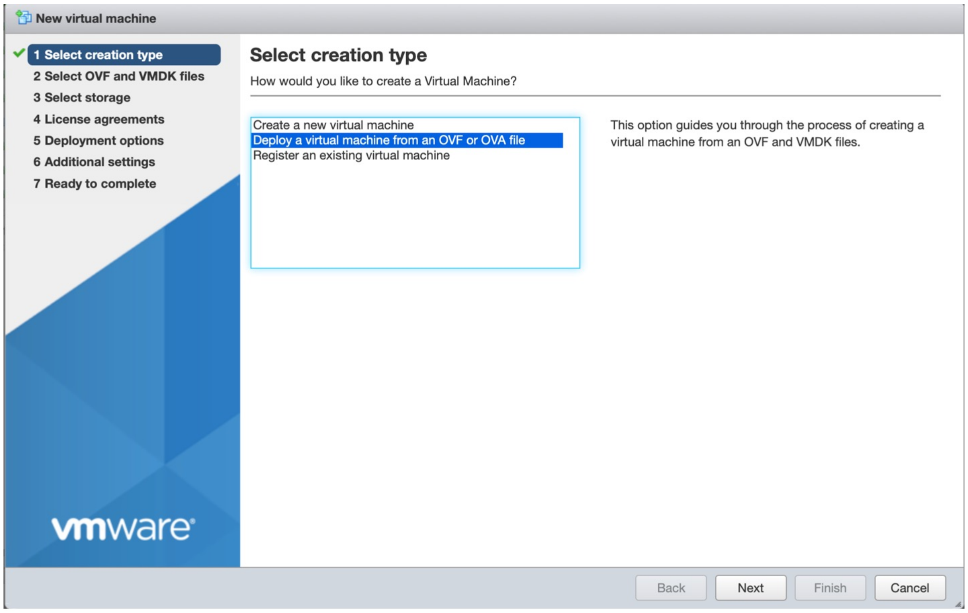
Downloading and Deploying the Cisco Spaces: Connector OVA (Single Interface)

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

Step 1 Download Connector 2.3 from Cisco.com.

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

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



New virtual machine

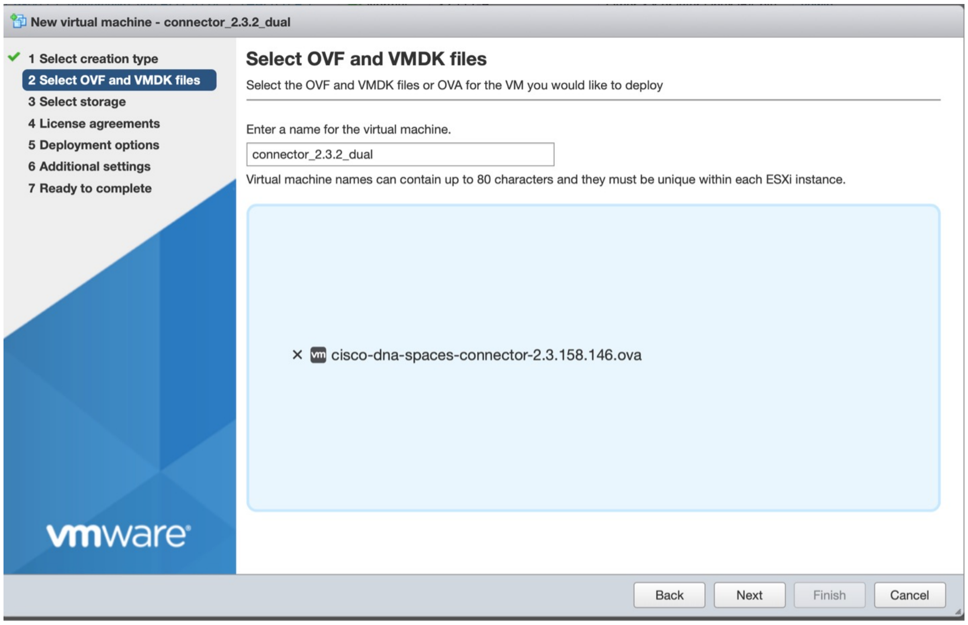
Select creation type

How would you like to create a Virtual Machine?

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

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

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



New virtual machine - connector_2.3.2_dual

Select OVF and VMDK files

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

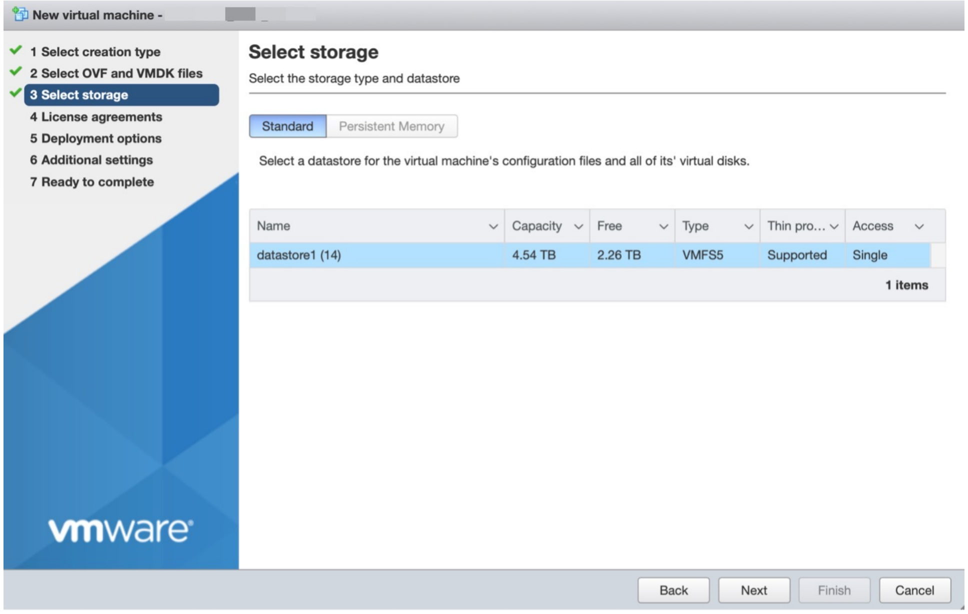
Enter a name for the virtual machine.

connector_2.3.2_dual

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

× cisco-dna-spaces-connector-2.3.158.146.ova

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



Select storage

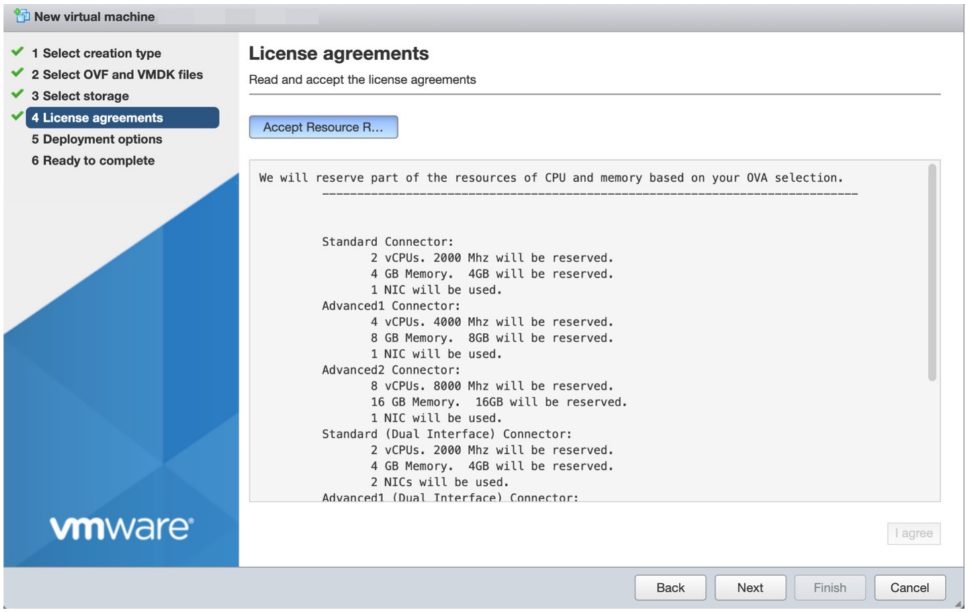
Select the storage type and datastore

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

Name	Capacity	Free	Type	Thin pro...	Access
datastore1 (14)	4.54 TB	2.26 TB	VMFS5	Supported	Single

1 items

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



License agreements

Read and accept the license agreements

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


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

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

a) In the **Network-mapping** field, enter the name of the network.

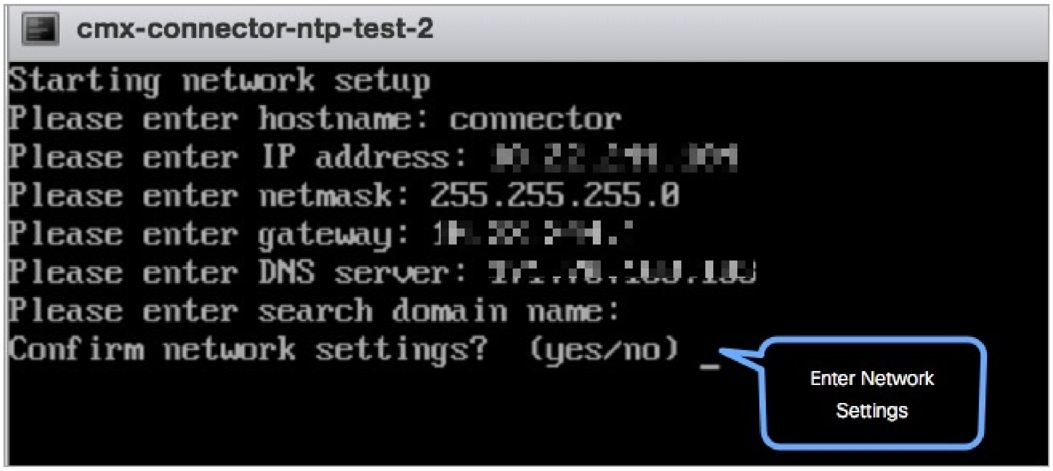
b) From the **Deployment type** drop-down list, choose one of the following, and click **Next**:

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

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

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

Step 10 Enter the network settings by specifying parameters such as IP address, hostname, and so on, that you want to configure on the Cisco Spaces: Connector.

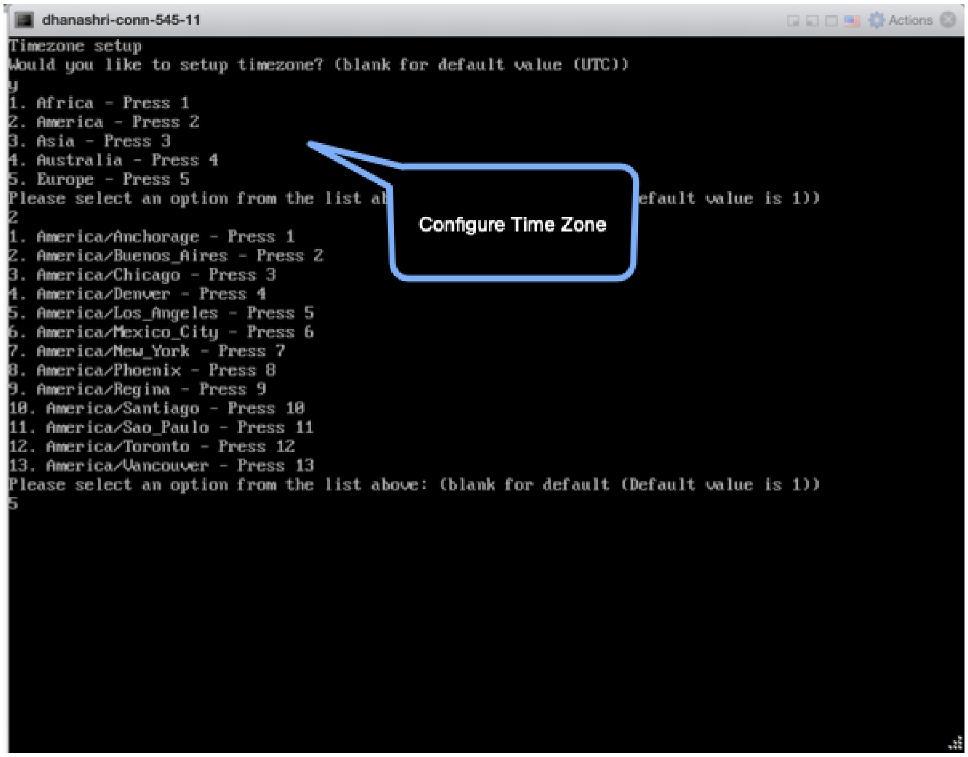


```
Starting network setup
Please enter hostname: connector
Please enter IP address: [redacted]
Please enter netmask: 255.255.255.0
Please enter gateway: [redacted]
Please enter DNS server: [redacted]
Please enter search domain name:
Confirm network settings? (yes/no) _
```

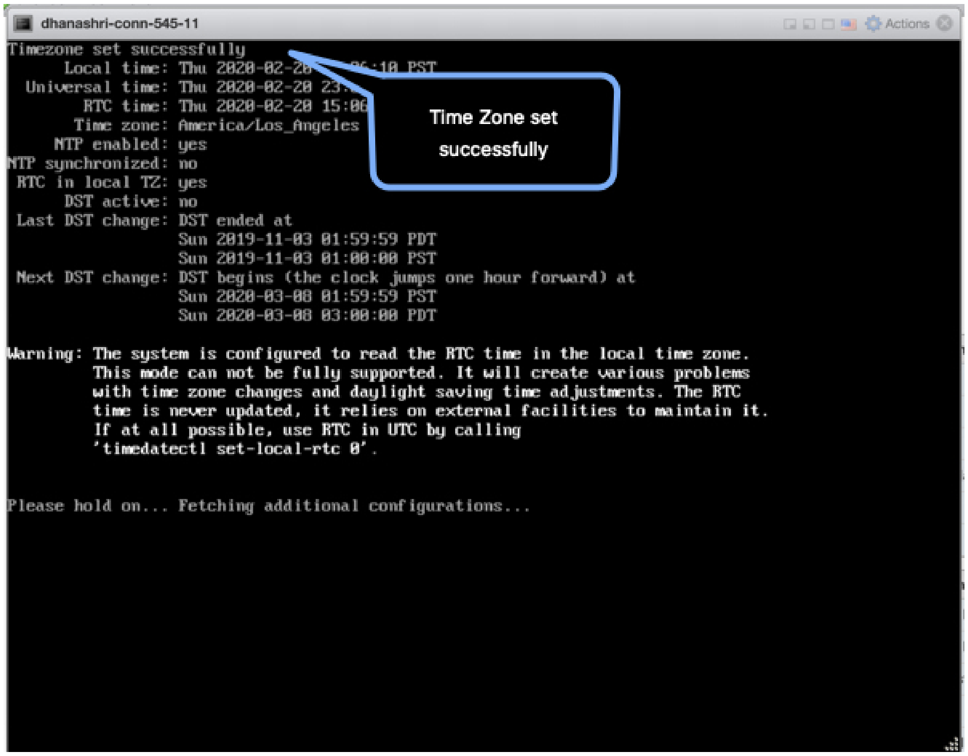
Note Because this configuration screen times out in 60 seconds, ensure that you provide the input on time to avoid reconfiguration.

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

Step 11 Enter the time zone.



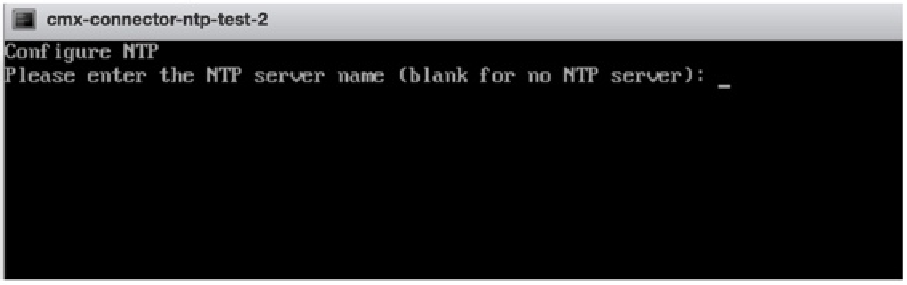
```
Timezone setup
Would you like to setup timezone? (blank for default value (UTC))
y
1. Africa - Press 1
2. America - Press 2
3. Asia - Press 3
4. Australia - Press 4
5. Europe - Press 5
Please select an option from the list ab                        efault value is 1))
2
1. America/Anchorage - Press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



```
Timezone set successfully
      Local time: Thu 2020-02-20    6:10 PST
  Universal time: Thu 2020-02-20 23:
        RTC time: Thu 2020-02-20 15:06
       Time zone: America/Los_Angeles
     NTP enabled: yes
NTP synchronized: no
 RTC in local TZ: yes
      DST active: no
 Last DST change: DST ended at
                  Sun 2019-11-03 01:59:59 PDT
                  Sun 2019-11-03 01:00:00 PST
 Next DST change: DST begins (the clock jumps one hour forward) at
                  Sun 2020-03-08 01:59:59 PST
                  Sun 2020-03-08 03:00:00 PDT

Warning: The system is configured to read the RTC time in the local time zone.
         This mode can not be fully supported. It will create various problems
         with time zone changes and daylight saving time adjustments. The RTC
         time is never updated, it relies on external facilities to maintain it.
         If at all possible, use RTC in UTC by calling
         'timedatectl set-local-rtc 0'.


Please hold on... Fetching additional configurations...
```

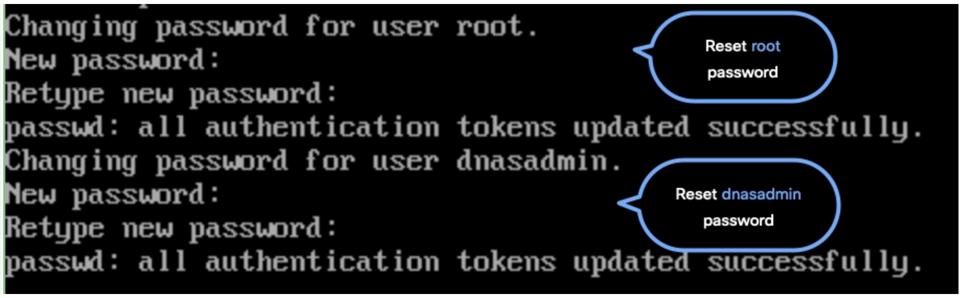
Step 12 Enter the Network Time Protocol (NTP) server name to synchronize the system time with the NTP server's or leave it blank if you do not want to configure an NTP server.

Figure 15: Enter NTP Setting



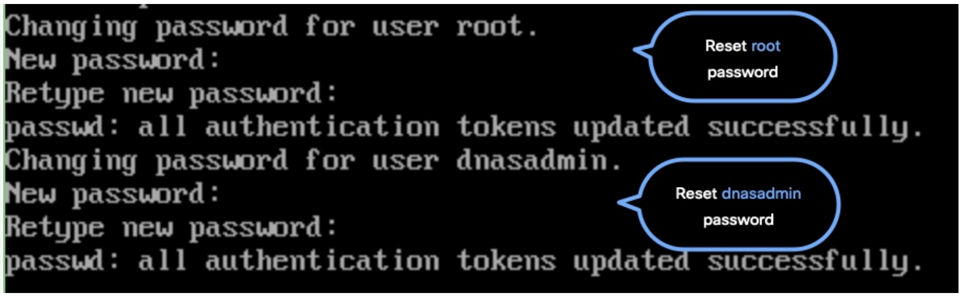
```
Configure NTP
Please enter the NTP server name (blank for no NTP server): _
```

Step 13 Set a new password for the **root** user.



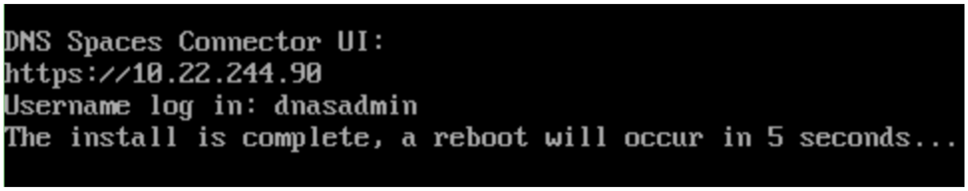
```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Step 14 Set a new password for the **dnasadmin** user, which is user with administrative privileges.



```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Step 15 Copy and save the URL before the automatic reboot. You can use this URL later to open the Cisco Spaces: Connector GUI.



```
DNS Spaces Connector UI:
https://10.22.244.90
Username log in: dnasadmin
The install is complete, a reboot will occur in 5 seconds...
```

What to do next

.

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

Downloading and Deploying the Cisco Spaces: Connector OVA (Dual Interface)

Starting with Connector 2.3.2, you can use the dual-interface deployment of the Connector in network deployments which require the Connector to connect to two separate networks.

One of these networks is usually a private network connecting most of your devices. The other network is external facing and hence can connect to the cloud-hosted Cisco Spaces.

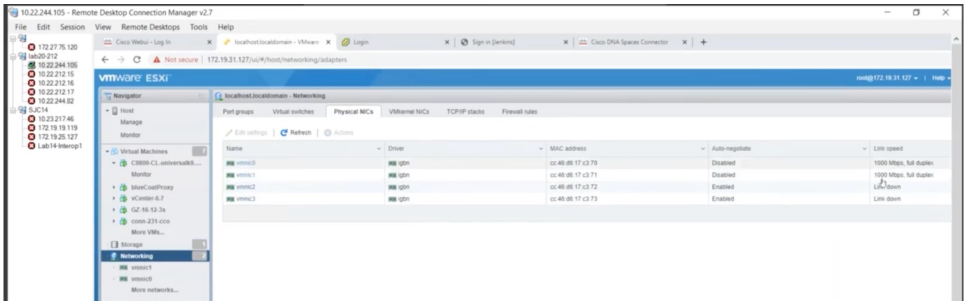
This deployment is recommended when most of the devices that are managed by the Connector are on private or internal networks.

Note We recommend that you connect the controller to a private network because this configuration allows the Connector to connect to the controller using SSH connections.

Before you begin

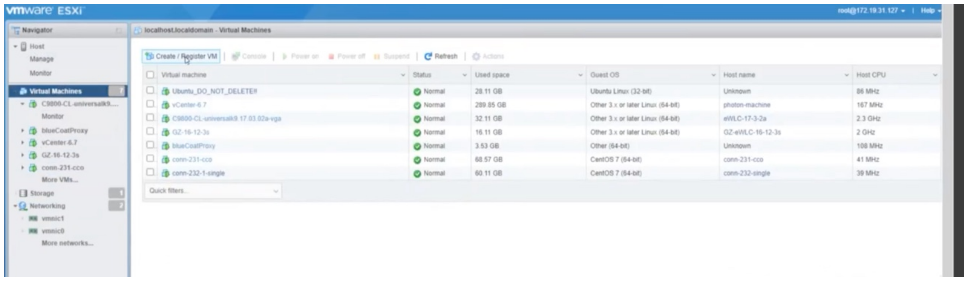
Ensure that the Cisco Unified Computing System (Cisco UCS) device where you install the Open Virtualization Appliance (OVA) is connected to two separate networks. In this network configuration, the Cisco UCS device is configured with two physical network interface cards (NICs). Each NIC is connected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

Figure 16: Two Physical Interfaces


10.22.244.105 - Remote Desktop Connection Manager v2.7
File Edit Session View Remote Desktops Tools Help
localhost.localdomain - VMware
Login
Sign in [Jenkins]
Cisco DNA Spaces Connector
172.19.31.127/ui/#/host/networking/adapters
vmware ESXi
root@172.19.31.127
Help
Navigator
Host
Manage
Monitor
Virtual Machines
Storage
Networking
localhost.localdomain - Networking
Port groups
Virtual switches
Physical NICs
VMkernel NICs
TCP/IP stacks
Firewall rules
Edit settings
Refresh
Actions

Name	Driver	MAC address	Auto-negotiate	Link speed
vmnic0	igbn	cc:46:d6:17:c3:70	Disabled	1000 Mbps, full duplex
vmnic1	igbn	cc:46:d6:17:c3:71	Disabled	1000 Mbps, full duplex
vmnic2	igbn	cc:46:d6:17:c3:72	Enabled	Link down
vmnic3	igbn	cc:46:d6:17:c3:73	Enabled	Link down

Figure 17: Two Separate Networks

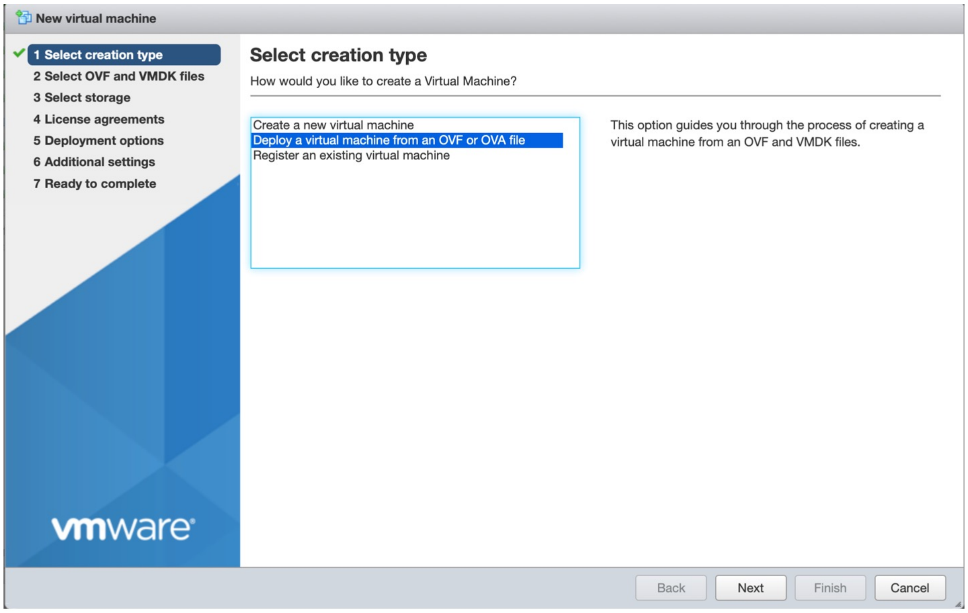


Virtual machine	Status	Used space	Guest OS	Host name	Host CPU
Ubuntu_DO_NOT_DELETE!!	Normal	28.11 GB	Ubuntu Linux (32-bit)	Unknown	86 MHz
vCenter-6.7	Normal	289.85 GB	Other 3.x or later Linux (64-bit)	photon-machine	167 MHz
C9800-CL-universalk9.17.03.02a-vga	Normal	32.11 GB	Other 3.x or later Linux (64-bit)	eWLC-17-3-2a	2.3 GHz
GZ-16-12-3s	Normal	16.11 GB	Other 3.x or later Linux (64-bit)	GZ-eWLC-16-12-3s	2 GHz
blueCoatProxy	Normal	3.53 GB	Other (64-bit)	Unknown	108 MHz
conn-231-cco	Normal	68.57 GB	CentOS 7 (64-bit)	conn-231-cco	41 MHz
conn-232-1-single	Normal	60.11 GB	CentOS 7 (64-bit)	conn-232-single	39 MHz

Step 1 Download Connector 2.3 from Cisco.com.

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

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



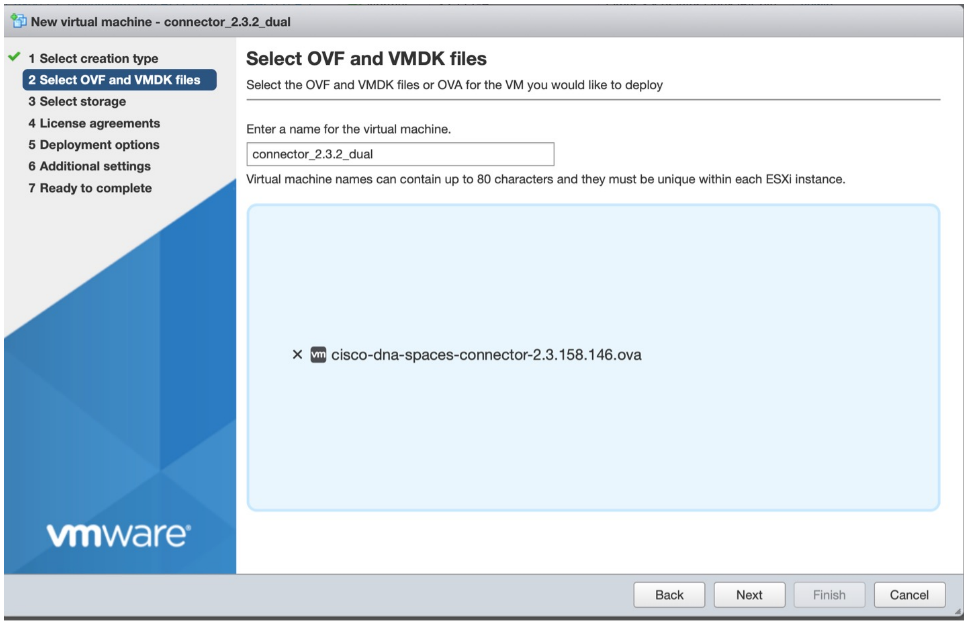
Select creation type

How would you like to create a Virtual Machine?

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

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

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



Select OVF and VMDK files

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

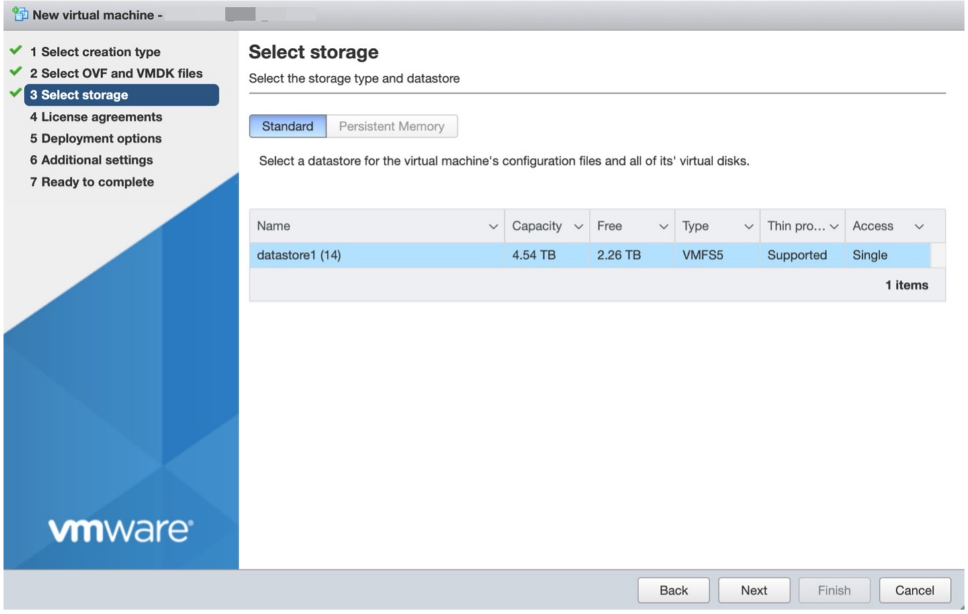
Enter a name for the virtual machine.

connector_2.3.2_dual

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

× cisco-dna-spaces-connector-2.3.158.146.ova

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



New virtual machine - [redacted]

Select storage

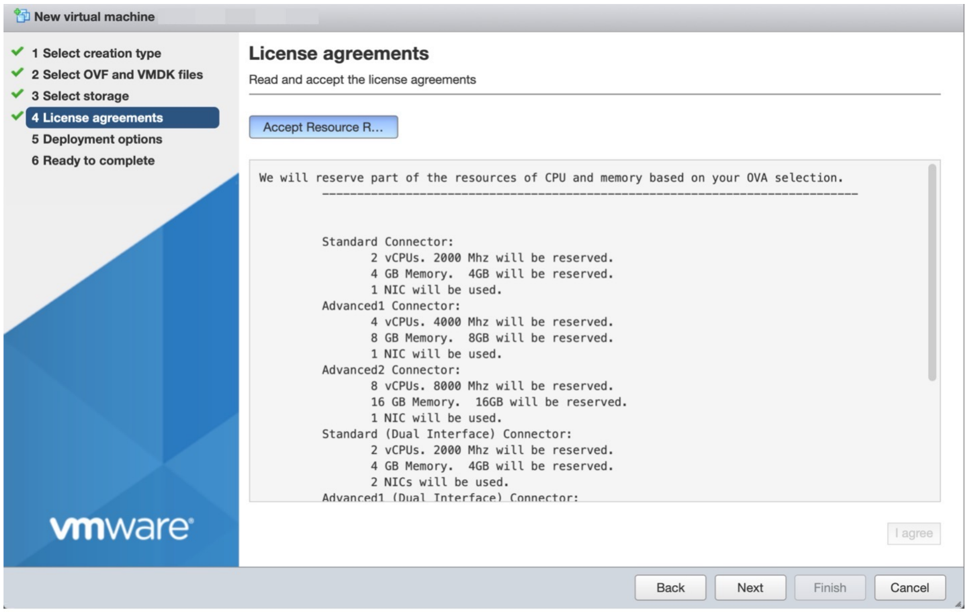
Select the storage type and datastore

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

Name	Capacity	Free	Type	Thin pro...	Access
datastore1 (14)	4.54 TB	2.26 TB	VMFS5	Supported	Single

1 items

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



New virtual machine

License agreements

Read and accept the license agreements

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


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

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

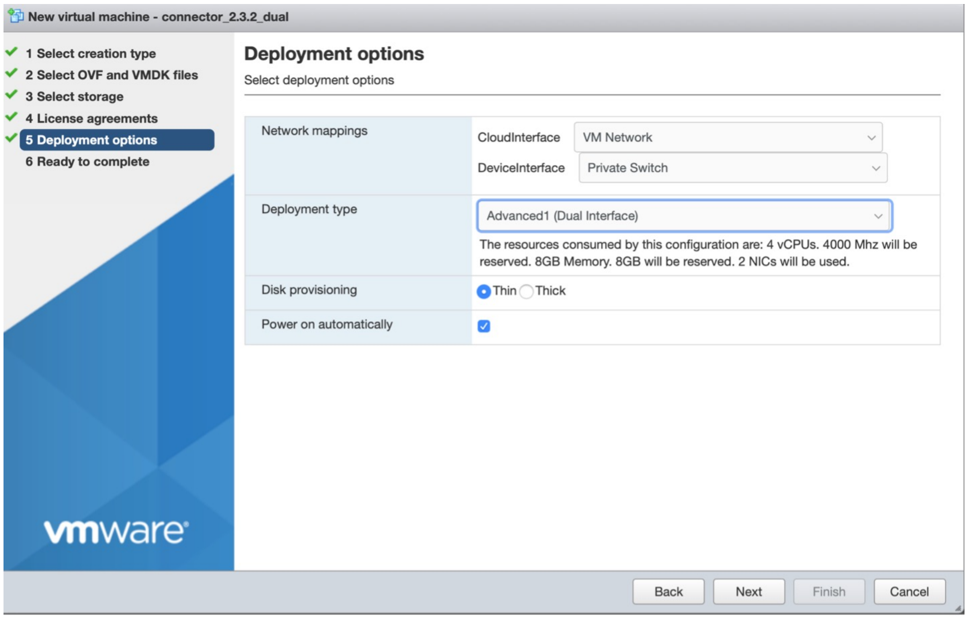
a) In the **CloudInterface** field, enter the name of the external-facing network.

b) In the **DeviceInterface** field, enter the name of the private network.

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

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

Figure 18: Entering the External-Facing and Private Network's Names



New virtual machine - connector_2.3.2_dual

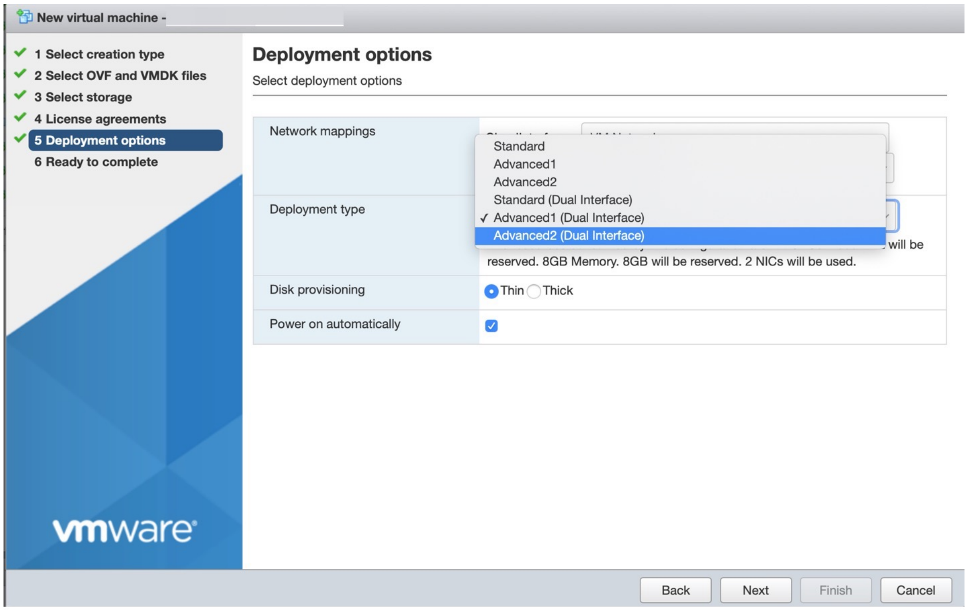
- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- ✓ 5 Deployment options
- 6 Ready to complete

Deployment options

Select deployment options

Network mappings	CloudInterface: VM Network DeviceInterface: Private Switch
Deployment type	Advanced1 (Dual Interface) The resources consumed by this configuration are: 4 vCPUs. 4000 Mhz will be reserved. 8GB Memory. 8GB will be reserved. 2 NICs will be used.
Disk provisioning	● Thin ○ Thick
Power on automatically	☑

Figure 19: Choosing the Deployment Type



New virtual machine -

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- ✓ 5 Deployment options
- 6 Ready to complete

Deployment options

Select deployment options

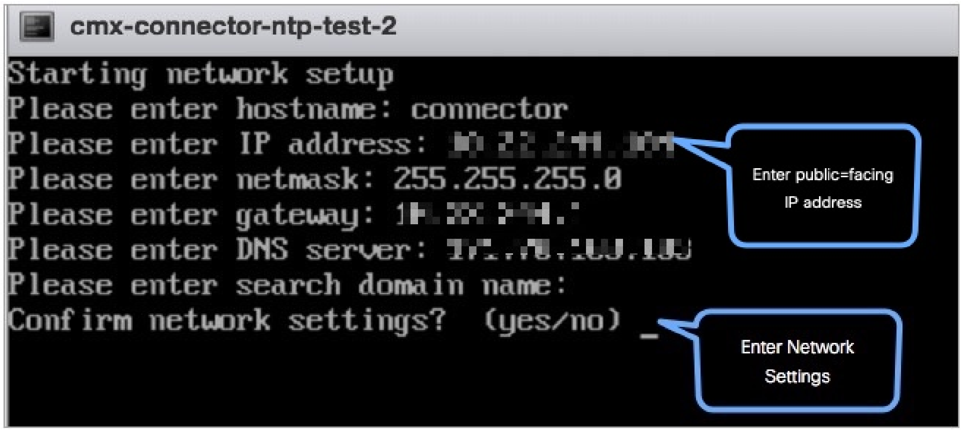
Network mappings	
Deployment type	Standard Advanced1 Advanced2 Standard (Dual Interface) ✓ Advanced1 (Dual Interface) Advanced2 (Dual Interface) will be reserved. 8GB Memory. 8GB will be reserved. 2 NICs will be used.
Disk provisioning	● Thin ○ Thick
Power on automatically	☑

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

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

Step 10 Configure the network settings for the external-facing network first, by specifying the parameters such as IP address, hostname, and so on.

Figure 20: Enter the Network Settings of External-Facing Network



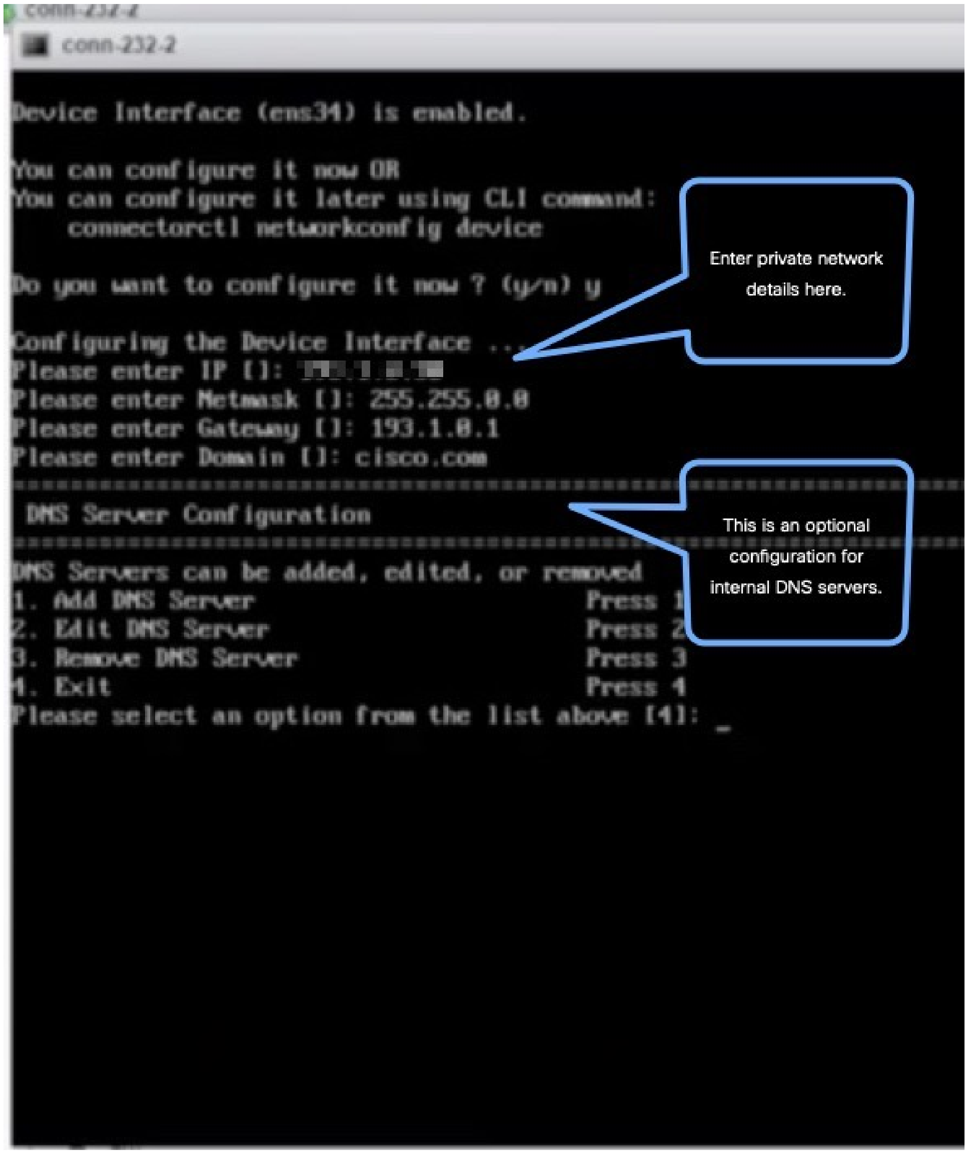
cmx-connector-ntp-test-2

```
Starting network setup
Please enter hostname: connector
Please enter IP address: [redacted]
Please enter netmask: 255.255.255.0
Please enter gateway: [redacted]
Please enter DNS server: [redacted]
Please enter search domain name:
Confirm network settings?  (yes/no) _
```

Note As this configuration screen times out in 60 seconds, ensure you provide the input in time to avoid reconfiguring.

Step 11 Configure the network settings for the private network by specifying the parameters such as IP address, hostname, and so on.

Figure 21: Enter the Network Settings of Private Network

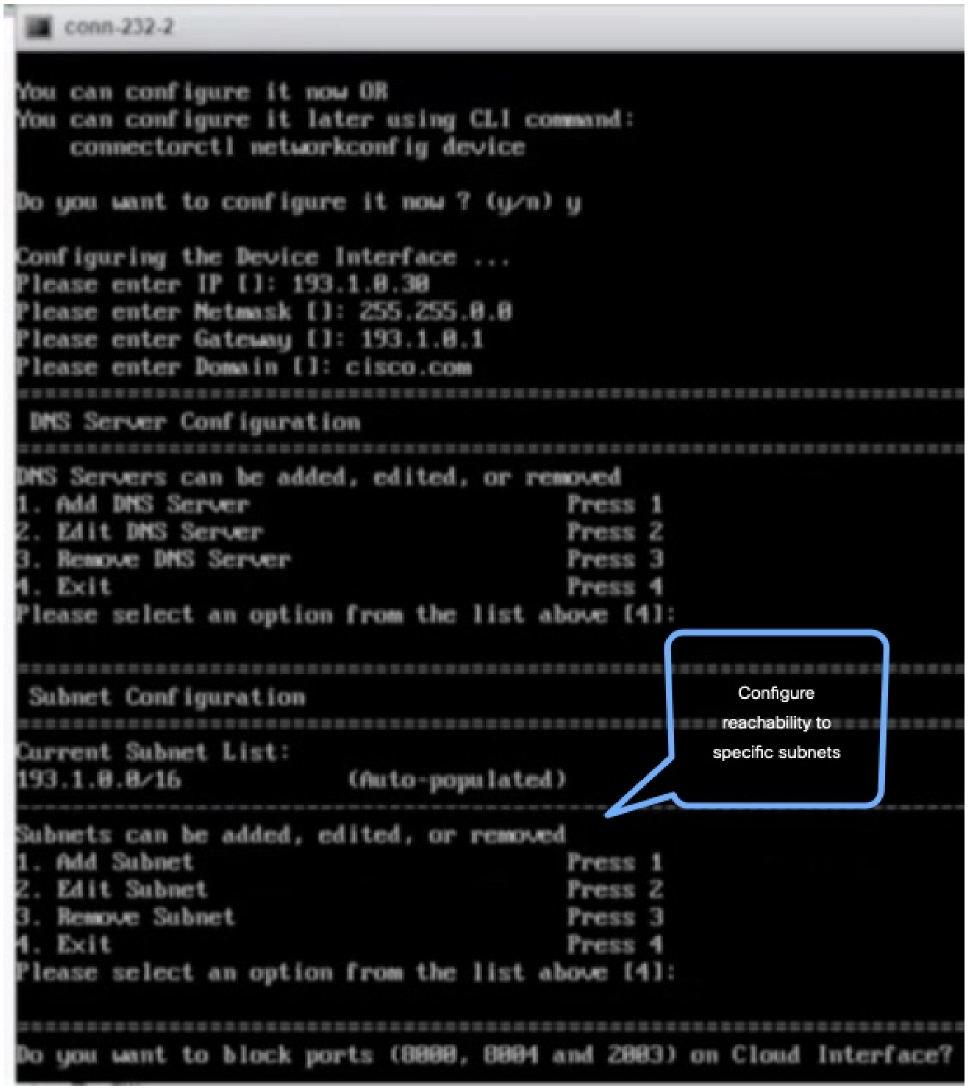


```
Device Interface (ens34) is enabled.

You can configure it now OR
You can configure it later using CLI command:
    connectorctl networkconfig device

Do you want to configure it now ? (y/n) y

Configuring the Device Interface ...
Please enter IP []: [redacted]
Please enter Netmask []: 255.255.0.0
Please enter Gateway []: 193.1.0.1
Please enter Domain []: cisco.com
======================================================================
 DNS Server Configuration
======================================================================
DNS Servers can be added, edited, or removed
1. Add DNS Server                          Press 1
2. Edit DNS Server                         Press 2
3. Remove DNS Server                       Press 3
4. Exit                                    Press 4
Please select an option from the list above [4]: _
```

Enter private network details here.

This is an optional configuration for internal DNS servers.

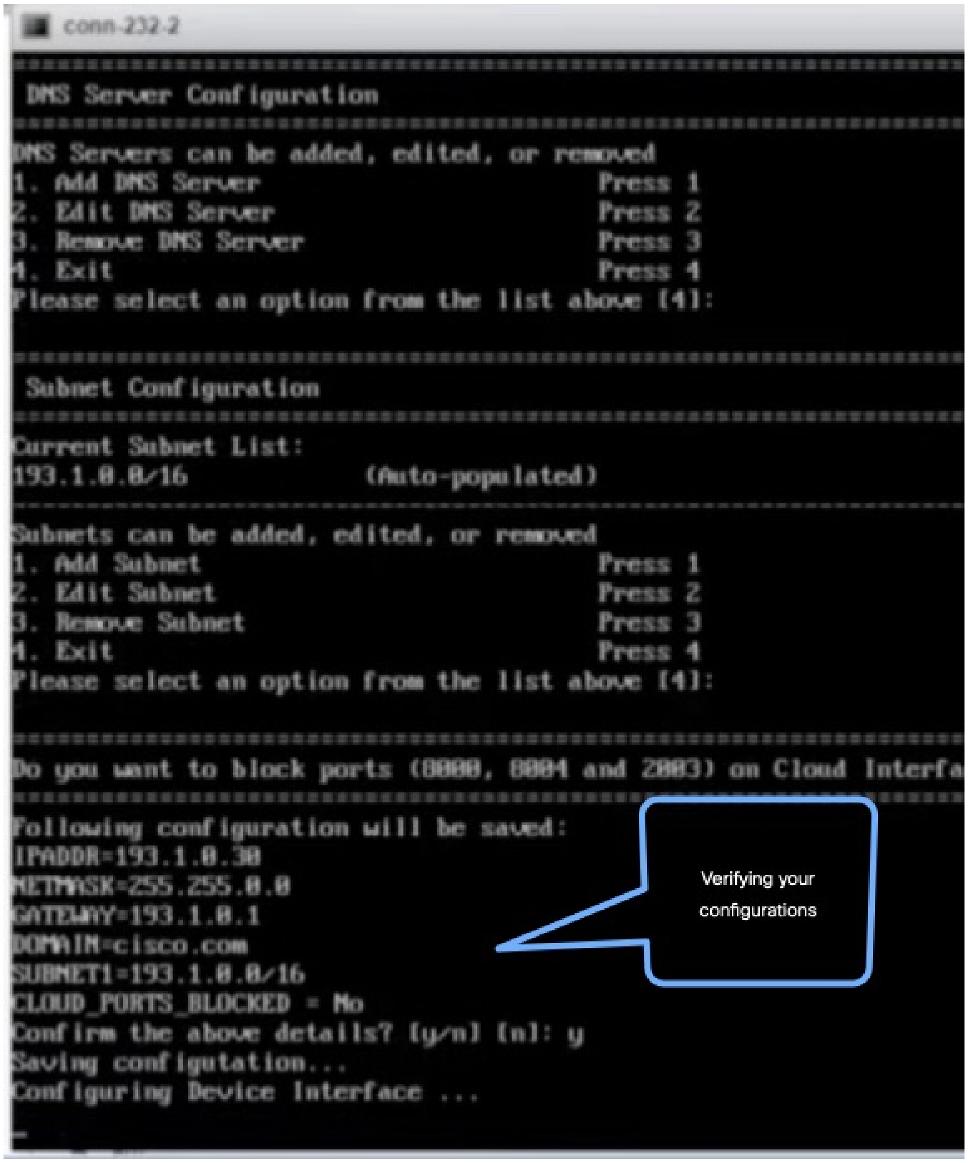
Step 12 Configure subnets that the Connector can reach.



```
You can configure it now OR
You can configure it later using CLI command:
    connectorctl networkconfig device

Do you want to configure it now ? (y/n) y

Configuring the Device Interface ...
Please enter IP []: 193.1.0.30
Please enter Netmask []: 255.255.0.0
Please enter Gateway []: 193.1.0.1
Please enter Domain []: cisco.com
======================================================================
 DNS Server Configuration
======================================================================
DNS Servers can be added, edited, or removed
1. Add DNS Server                        Press 1
2. Edit DNS Server                       Press 2
3. Remove DNS Server                     Press 3
4. Exit                                  Press 4
Please select an option from the list above [4]:

======================================================================
 Subnet Configuration
======================================================================
Current Subnet List:
193.1.0.0/16            (Auto-populated)
----------------------------------------------------------------------
Subnets can be added, edited, or removed
1. Add Subnet                            Press 1
2. Edit Subnet                           Press 2
3. Remove Subnet                         Press 3
4. Exit                                  Press 4
Please select an option from the list above [4]:

======================================================================
Do you want to block ports (8000, 8004 and 2003) on Cloud Interface?
```

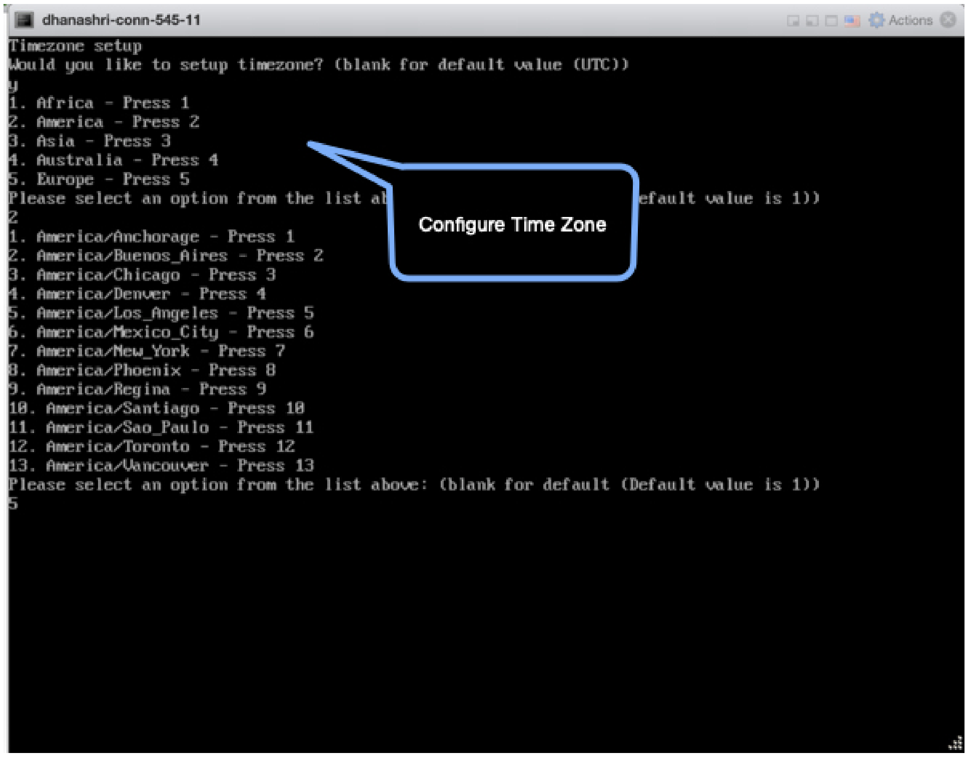
Configure reachability to specific subnets

You can observe as the configurations and network reachability are verified.



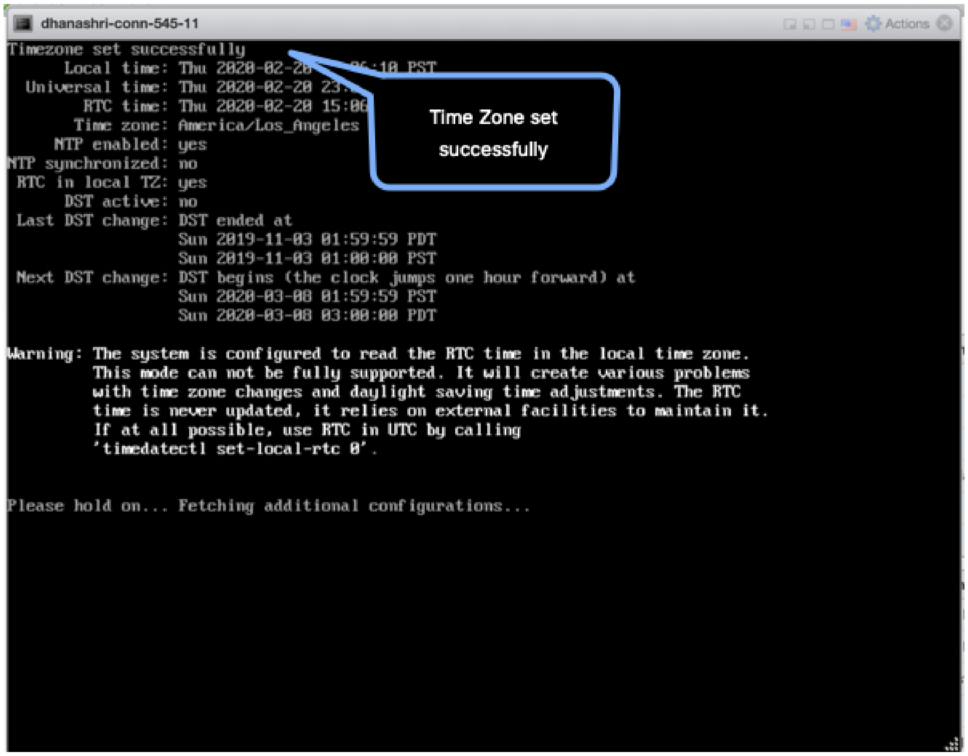
```
==========================================================================
 DNS Server Configuration
==========================================================================
DNS Servers can be added, edited, or removed
1. Add DNS Server                        Press 1
2. Edit DNS Server                       Press 2
3. Remove DNS Server                     Press 3
4. Exit                                  Press 4
Please select an option from the list above [4]:

==========================================================================
 Subnet Configuration
==========================================================================
Current Subnet List:
193.1.0.0/16            (Auto-populated)
--------------------------------------------------------------------------
Subnets can be added, edited, or removed
1. Add Subnet                            Press 1
2. Edit Subnet                           Press 2
3. Remove Subnet                         Press 3
4. Exit                                  Press 4
Please select an option from the list above [4]:

==========================================================================
Do you want to block ports (8000, 8004 and 2003) on Cloud Interfa
==========================================================================
Following configuration will be saved:
IPADDR=193.1.0.30
NETMASK=255.255.0.0
GATEWAY=193.1.0.1
DOMAIN=cisco.com
SUBNET1=193.1.0.0/16
CLOUD_PORTS_BLOCKED = No
Confirm the above details? [y/n] [n]: y
Saving configutation...
Configuring Device Interface ...
_
```

Step 13 Enter the time zone.



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

Configure Time Zone

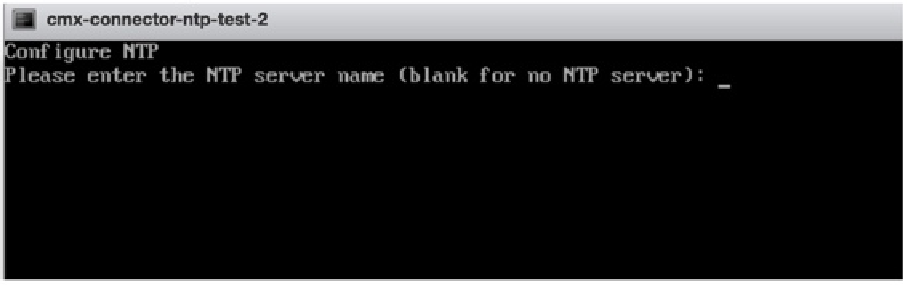


```
Timezone set successfully
      Local time: Thu 2020-02-20    06:10 PST
  Universal time: Thu 2020-02-20 23:
        RTC time: Thu 2020-02-20 15:06
       Time zone: America/Los_Angeles
     NTP enabled: yes
NTP synchronized: no
 RTC in local TZ: yes
      DST active: no
 Last DST change: DST ended at
                  Sun 2019-11-03 01:59:59 PDT
                  Sun 2019-11-03 01:00:00 PST
 Next DST change: DST begins (the clock jumps one hour forward) at
                  Sun 2020-03-08 01:59:59 PST
                  Sun 2020-03-08 03:00:00 PDT

Warning: The system is configured to read the RTC time in the local time zone.
         This mode can not be fully supported. It will create various problems
         with time zone changes and daylight saving time adjustments. The RTC
         time is never updated, it relies on external facilities to maintain it.
         If at all possible, use RTC in UTC by calling
         'timedatectl set-local-rtc 0'.


Please hold on... Fetching additional configurations...
```

Time Zone set successfully

Step 14 Enter the Network Time Protocol (NTP) server name to synchronize the system time with the NTP server's or leave it blank if you do not want to configure an NTP server.

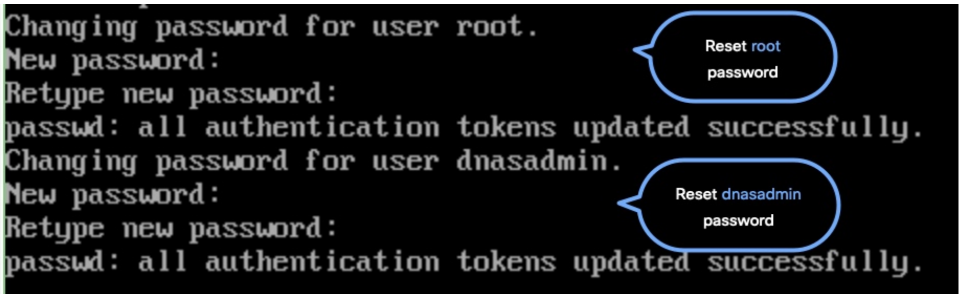
Figure 22: Enter NTP Setting



cmx-connector-ntp-test-2

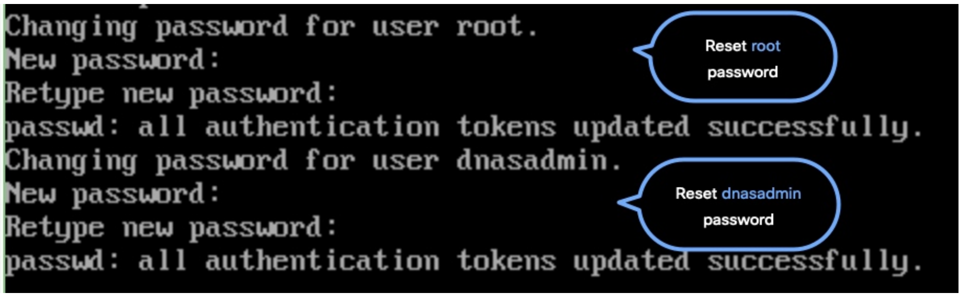
```
Configure NTP
Please enter the NTP server name (blank for no NTP server): _
```

Step 15 Set a new password for the **root** user.



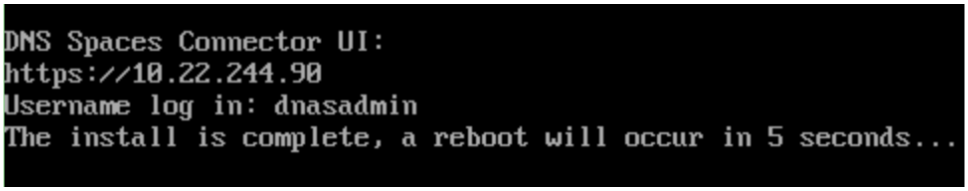
```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Step 16 Set a new password for the **dnasadmin** user, which is user with administrative privileges.



```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

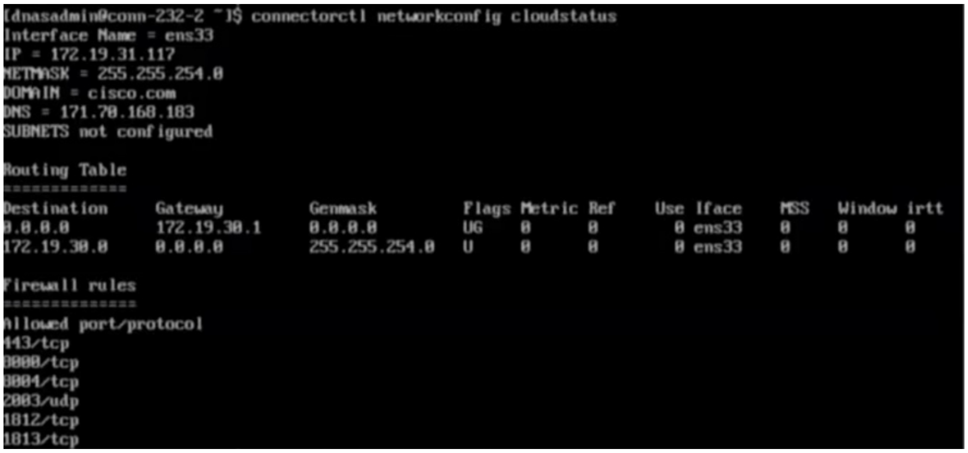
Step 17 Copy and save the URL before the automatic reboot. You can use this URL later to open the Cisco Spaces: Connector GUI.



```
DNS Spaces Connector UI:
https://10.22.244.90
Username log in: dnasadmin
The install is complete, a reboot will occur in 5 seconds...
```

Step 18 Verify the network Settings of external-facing network using the **connectorctl networkconfig cloudstatus** command.

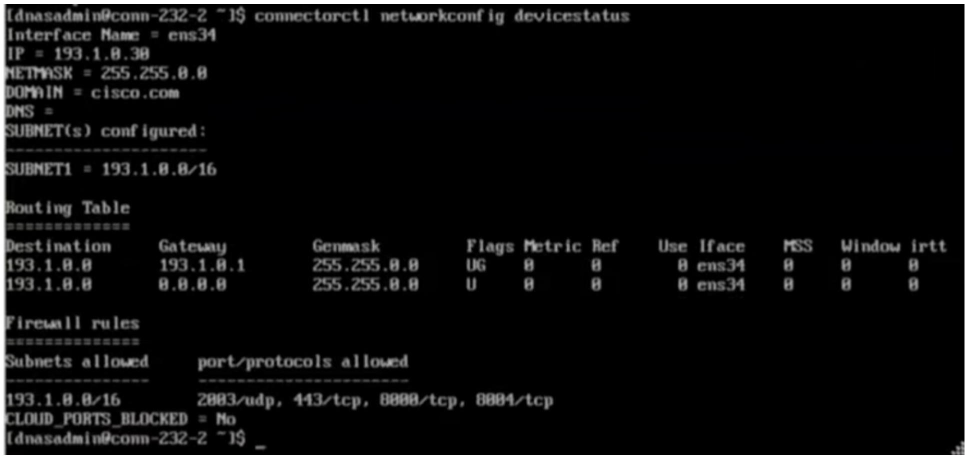
Figure 23: Enter the Network Settings of Private Network



```
[dnasadmin@conn-232-2 ~]$ connectorctl networkconfig cloudstatus
Interface Name = ens33
IP = 172.19.31.117
NETMASK = 255.255.254.0
DOMAIN = cisco.com
DNS = 171.70.168.183
SUBNETS not configured

Routing Table
=============
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface    MSS   Window irtt
0.0.0.0         172.19.30.1     0.0.0.0         UG    0      0        0 ens33    0     0      0
172.19.30.0     0.0.0.0         255.255.254.0   U     0      0        0 ens33    0     0      0

Firewall rules
==============
Allowed port/protocol
443/tcp
8000/tcp
8004/tcp
2003/udp
1812/tcp
1813/tcp
```

Step 19 Verify the network settings of private network using the **connectorctl networkconfig devicestatus** command.

Figure 24: Enter the Network Settings of Private Network



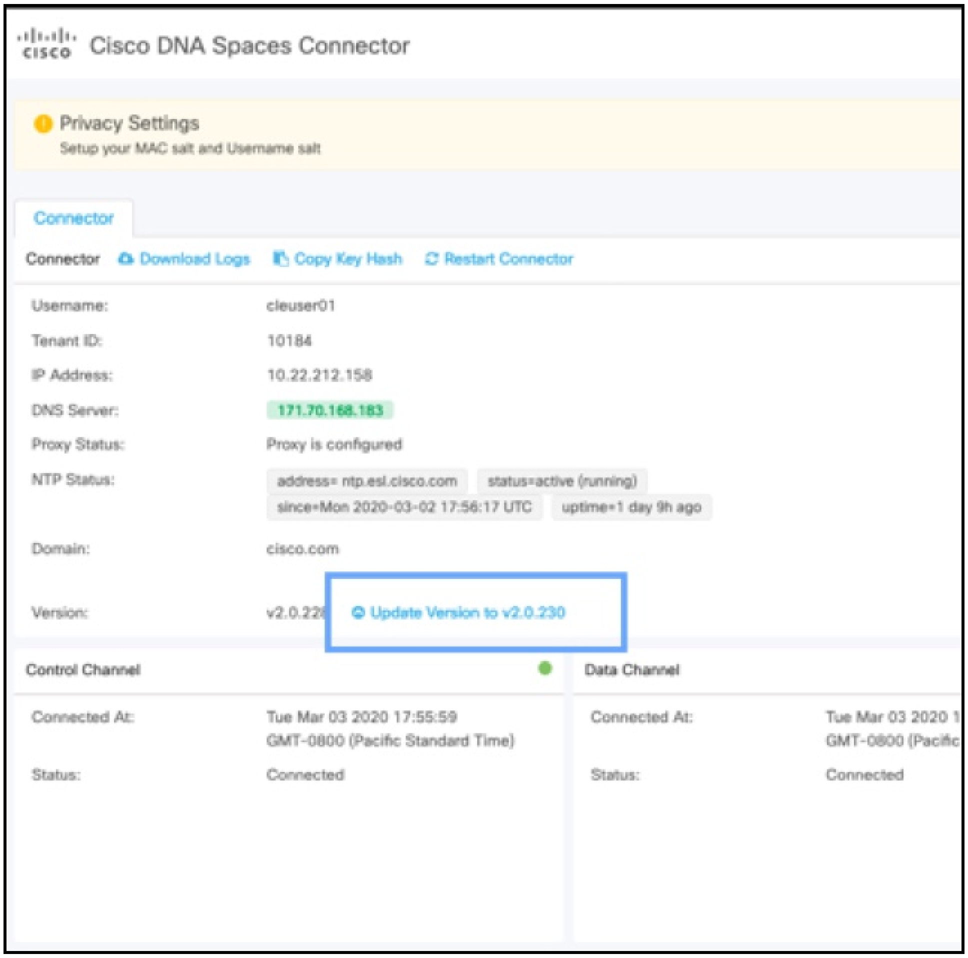
```
[dnasadmin@conn-232-2 ~]$ connectorctl networkconfig devicestatus
Interface Name = ens34
IP = 193.1.0.30
NETMASK = 255.255.0.0
DOMAIN = cisco.com
DNS =
SUBNET(s) configured:
---------------------
SUBNET1 = 193.1.0.0/16

Routing Table
=============
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface    MSS   Window irtt
193.1.0.0       193.1.0.1       255.255.0.0     UG    0      0        0 ens34    0     0      0
193.1.0.0       0.0.0.0         255.255.0.0     U     0      0        0 ens34    0     0      0

Firewall rules
==============
Subnets allowed     port/protocols allowed
---------------     ----------------------
193.1.0.0/16        2003/udp, 443/tcp, 8000/tcp, 8004/tcp
CLOUD_PORTS_BLOCKED = No
[dnasadmin@conn-232-2 ~]$ _
```

Upgrade the Cisco Spaces: Connector Docker

You can upgrade the Connector docker to the latest version from the Connector GUI. Note that the upgrade link appears only if a new upgrade image is available.

Note This procedure does not upgrade the Connector OVA.

Figure 25: Docker Upgrade Link on the Connector



Cisco DNA Spaces Connector

Privacy Settings
Setup your MAC salt and Username salt

Username:	cleuser01
Tenant ID:	10184
IP Address:	10.22.212.158
DNS Server:	171.70.168.183
Proxy Status:	Proxy is configured

NTP Status:	address= ntp.esl.cisco.com
	status=active (running)
	since=Mon 2020-03-02 17:56:17 UTC
	uptime=1 day 9h ago

Domain:	cisco.com
Version:	v2.0.228 Update Version to v2.0.230

Control Channel

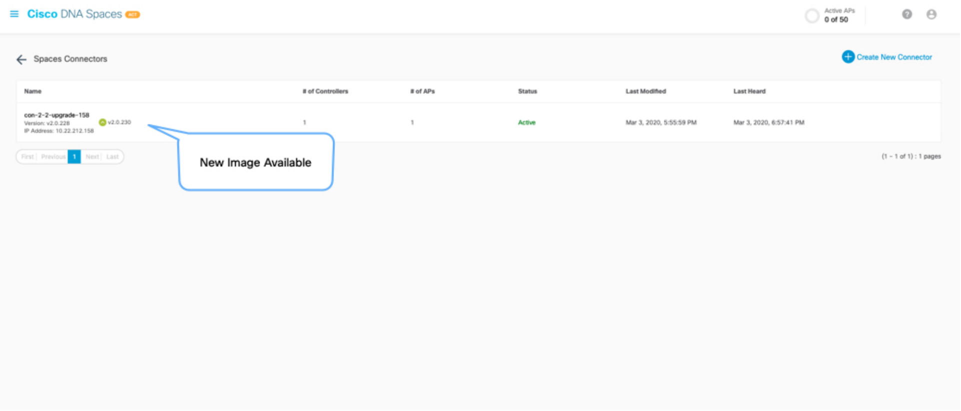
Connected At:	Tue Mar 03 2020 17:55:59 GMT-0800 (Pacific Standard Time)
Status:	Connected

Data Channel

Connected At:	Tue Mar 03 2020 1 GMT-0800 (Pacific
Status:	Connected

You can also upgrade the Connector docker to the latest version from the Cisco Spaces dashboard. The upgrade link appears only if a new upgrade image is available.

Figure 26: Docker Upgrade Link Appears Only if New Image is Available



Name	# of Controllers	# of APs	Status	Last Modified	Last Heard
con-2-2-upgrade-158 Version: v2.0.228 IP Address: 10.22.212.158 v2.0.230	1	1	Active	Mar 3, 2020, 5:55:59 PM	Mar 3, 2020, 6:57:41 PM

Upgrade Path

The following table is best viewed in the HTML format. Here is a description of the contents of the table.

- **Release Number**: Lists the identifying number of the release.
- **Platforms**: Lists the platforms (OVA, VHDX, AMI) on which this release can be installed or the corresponding installation file name.
- **Upgrade to This Release**: Lists the releases to which you can upgrade the release mentioned in the **Release Number** column.
- **Upgrade File**: Lists the *.connector* upgrade files you can use to upgrade to the release mentioned in the **Upgrade to This Release** column.

Table 5: Upgrade Path for Active Releases

ReleaseNumber	Platforms	Upgrade to This Release	Upgrade File
2.3.4	cisco-dna-spaces-connector-2.3.507.ova	N.A	N.A
	cisco-dna-spaces-connector-2.3.507.vhdx		
2.3.3	cisco-dna-spaces-connector-2.3.497.ova	2.3.4	cisco-dna-spaces-connector-2.3.507.connector
2.3.2	cisco-dna-spaces-connector-2.3.495.ova	2.3.3	cisco-dna-spaces-connector-2.3.497.connector
	cisco-dna-spaces-connector-2.3.496.vhdx		
2.3.1	cisco-dna-spaces-connector-2.3.478.ova	2.3.2	cisco-dna-spaces-connector-2.3.495.connector
	cisco-dna-spaces-connector-2.3.478.vhdx		
2.3	cisco-dna-spaces-connector-2.3.462.ova	2.3.1	cisco-dna-spaces-connector-2.3.478.connector
2.2	cisco-dna-spaces-connector-2.2.295.ova	2.3	cisco-dna-spaces-connector-2.3.462.connector

Note All release versions prior to 2.2 are deferred. We recommend that you deploy the latest OVA to get all the latest updates.

Table 6: Upgrade Path for AMI Releases

ReleaseNumber	Platforms	Upgrade to This Release	Upgrade File
2.3.4	AMI	N.A	N.A
2.3.3	AMI	2.3.4	cisco-dna-spaces-connector-ami-2.3.507.connector

Upgrading the Connector OVA

The following procedure shows you how to upgrade the Cisco Spaces: Connector OVA.

Step 1 Download Connector 2.3 from Cisco.com.

Step 2 Copy the downloaded file on to the machine hosting the Connector.

Step 3 Log in to the Connector command line.

Step 4 Use the **connectorctl upgrade** <<*upgrade_file_name*>> command to start the OVA upgrade process.

```
(cmxadminPcon-2-3-upg-87 -]S connectorctl upgrade cisco-dna-spaces-connector-2.3.494.connector
Machine will restart automatically after upgrade. Do you still want to continue? [yes / noj [yesj:
yes
Before upgrade, OVA version:2.2.295
New image exists.
Backing up current version of the image and db ...
Preparing for upgrade ...
umount: /mnt/cmx: not mounted
mount: /dev/loop0 is write-protected, mounting read-only
Starting pip repo
Starting upgrade ...
Warning: RPMDB altered outside of yum.
Error: No matching Packages to list
000000000000000000000000000000 IMPORTANT 000000*000000000000000000000*0000a«000
We are changing username from 'cmxadmin' to 'dnasadmin*
We will be performing following tasks now.
1. Create new user 'dnasadmin'
2. You will need to set up password for 'dnasadmin'
3. We will move over all files/folders from /home/cmxadmin to /ho®e/dnasadmin
4. Delete 'cmxadnin* user.

After the reboot, REMEMBER to login using dnasadmin credentials.
0000000000000000000000000000000000000000000000000000000000000000000000000000800


Please press ENTER to continue...
```

The **dnasadmin** user is now created.

Step 5 Set a password for the newly created **dnasadmin** user when prompted.

```
Please press ENTER to continue...
New user dnasadmin created.
Set password for user dnasadmin
Changing password for user dnasadmin.
New password:

Retype new password:

passwd: all authentication tokens updated successfully.
Start cleanup ...
Error response from daemon: No such container:
c9408eelb68f2acdel436622c4eeddf742dcd53a2619faa30c01aadcld8bd88e
```

Step 6 Wait a few seconds for the upgrade to complete.

```
Error response from daemon: No such container: c9408ee1b68f2acde1436622c4eeddf742dcd53a2

Upgrade successful.
After upgrade, OVA version : 2.3.494

System will reboot in 5 seconds...
```

Step 7 Once the upgrade is completed, log in to the connector as the **dnasadmin** user.

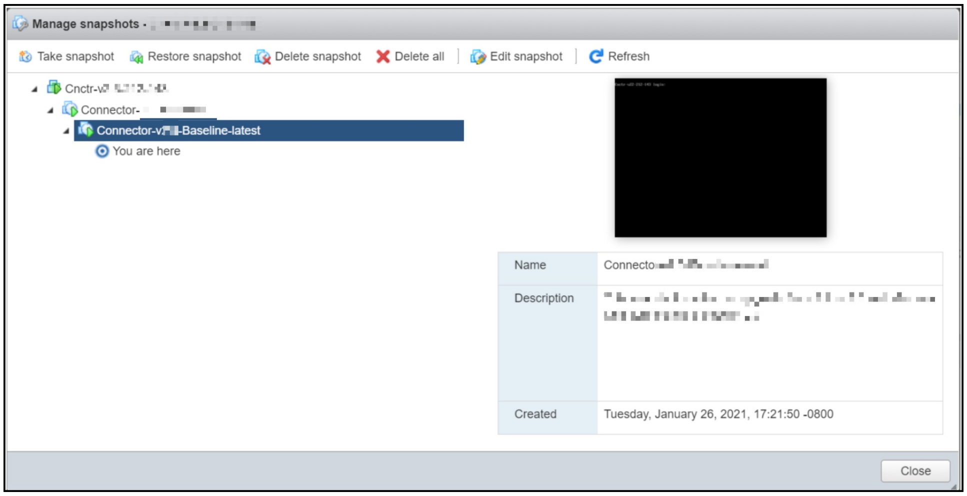
- Verify if the Connector is running in the same state as it was running before the upgrade.
- With CSCvr74830, you can ignore the two known errors that are displayed during upgrade.

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 27: Backing Up Using a Snapshot

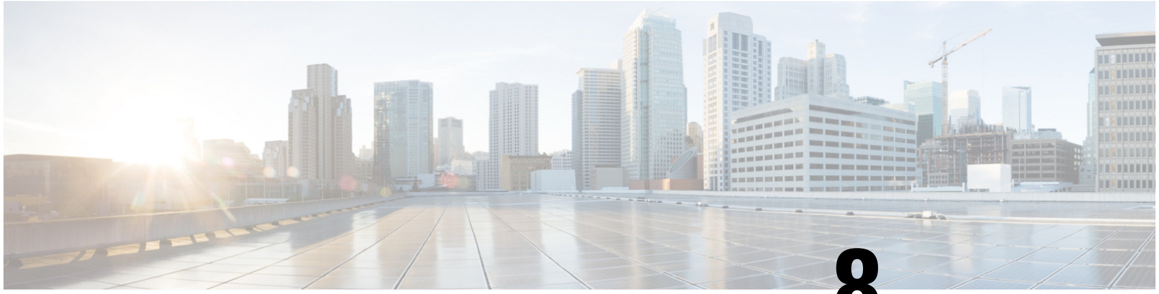


Manage snapshots - [redacted]

- Cnctr-v[redacted]
  - Connector-[redacted]
    - Connector-v[redacted]-Baseline-latest
      - You are here

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

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



CHAPTER 8

Cisco Spaces: Connector Hyper-V

- Creating a Virtual Switch, on page 47
- Downloading and Deploying Hyper-V, on page 54

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**.

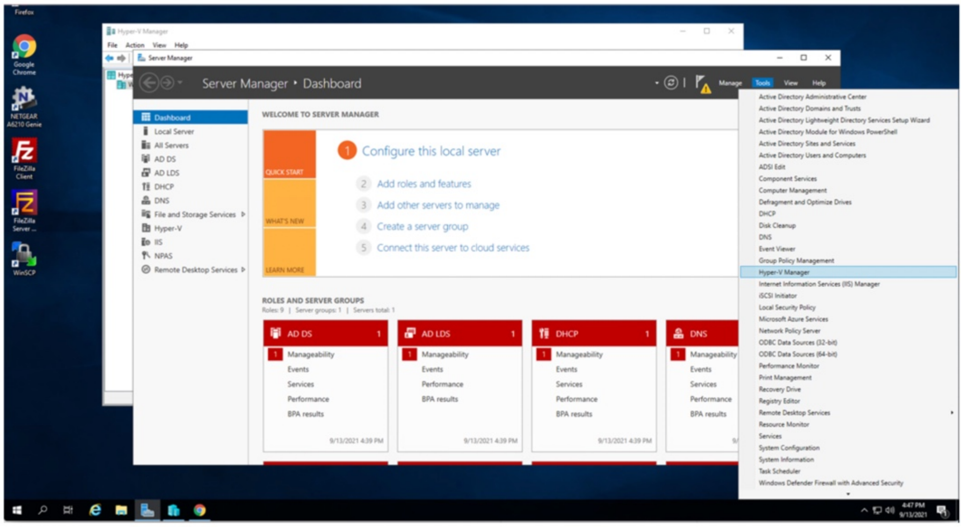


Figure 28:

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

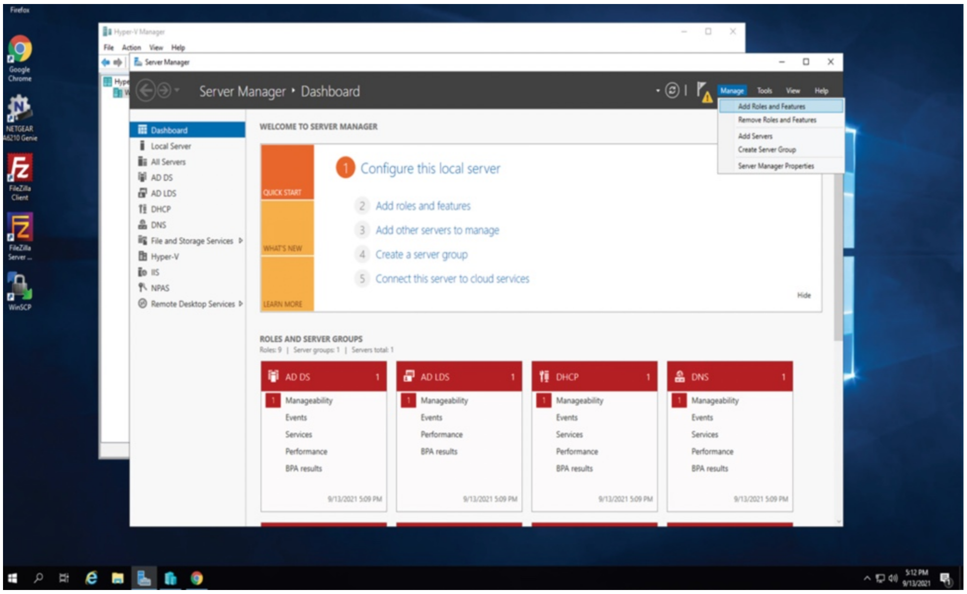
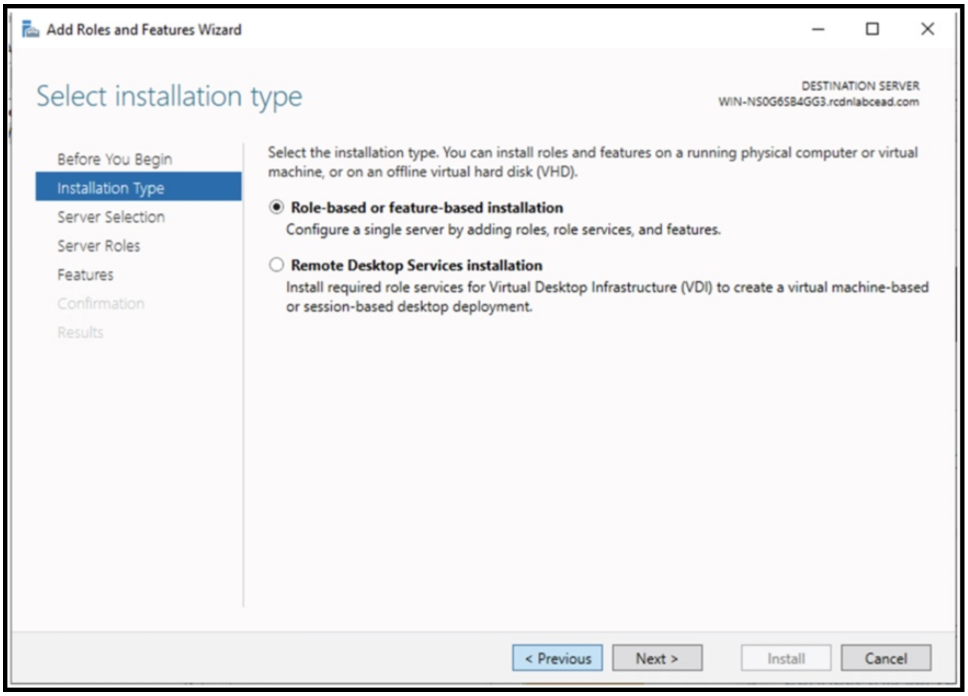


Figure 29:

Step 3 Click on **Role-based or feature-based installation**.



Select installation type

DESTINATION SERVER
WIN-NS0G6S84GG3.rcdnlabcead.com

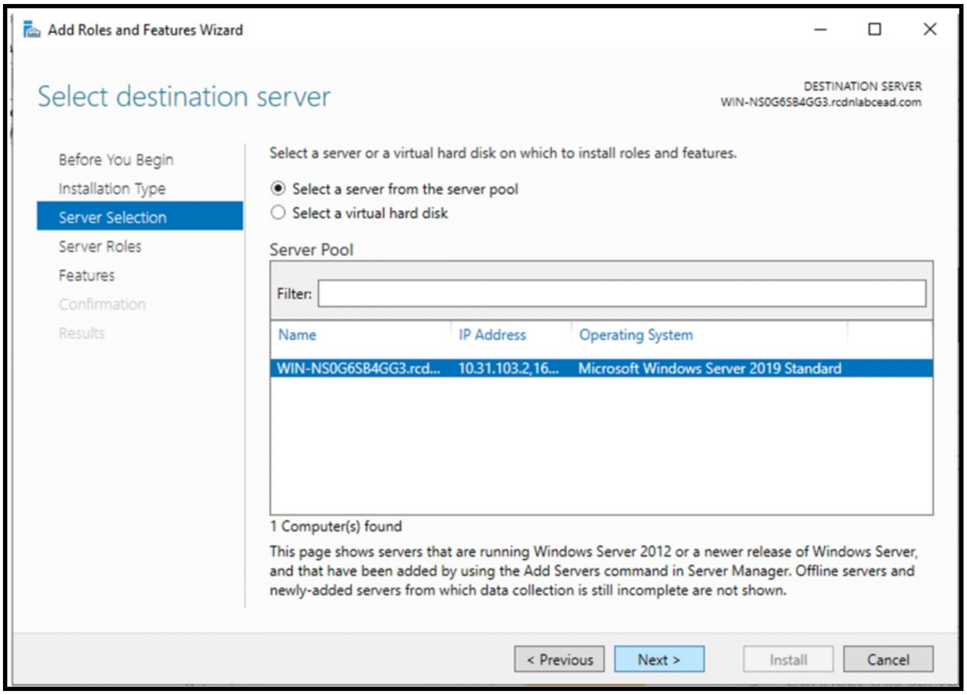
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

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

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

Figure 30:

Step 4 Choose **Select a server from the server pool.**



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WIN-NS0G6SB4GG3.rcdnlabcead.com

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

● Select a server from the server pool

○ Select a virtual hard disk

Server Pool

Filter:

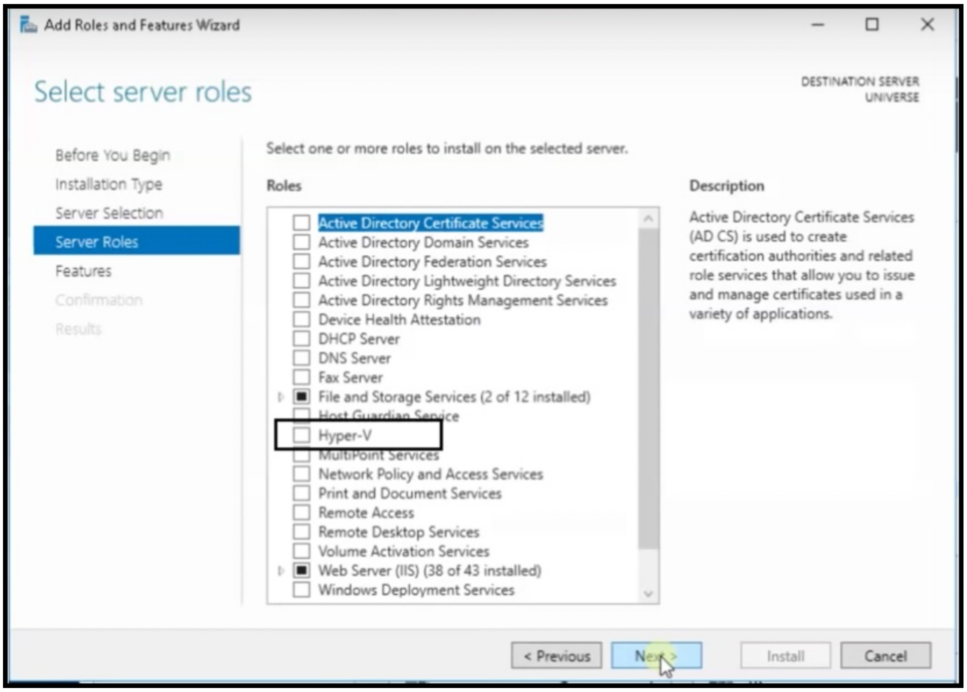
Name	IP Address	Operating System
WIN-NS0G6SB4GG3.rcd...	10.31.103.2,16...	Microsoft Windows Server 2019 Standard

1 Computer(s) found

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

Figure 31:

Step 5 In the **Select server roles** window, select Hyper-V. Click **Next**.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
UNIVERSE

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

Roles

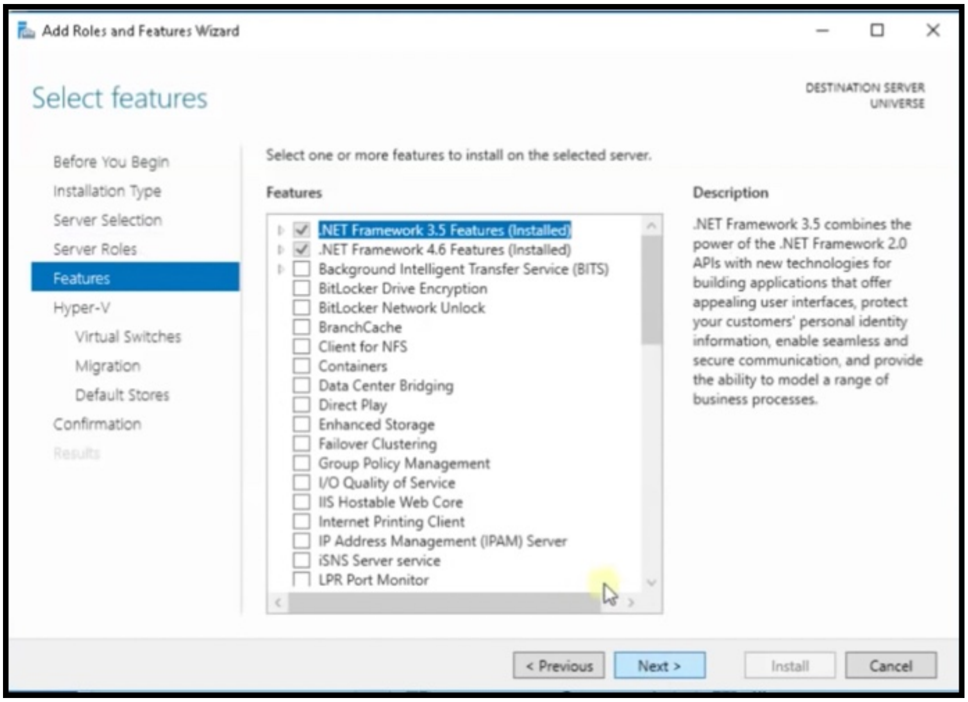
- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File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

Description

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

Figure 32:

Step 6 In the **Select features** window, check **.NET Framework**. Click **Next**.



Select features

DESTINATION SERVER
UNIVERSE

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

Features

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

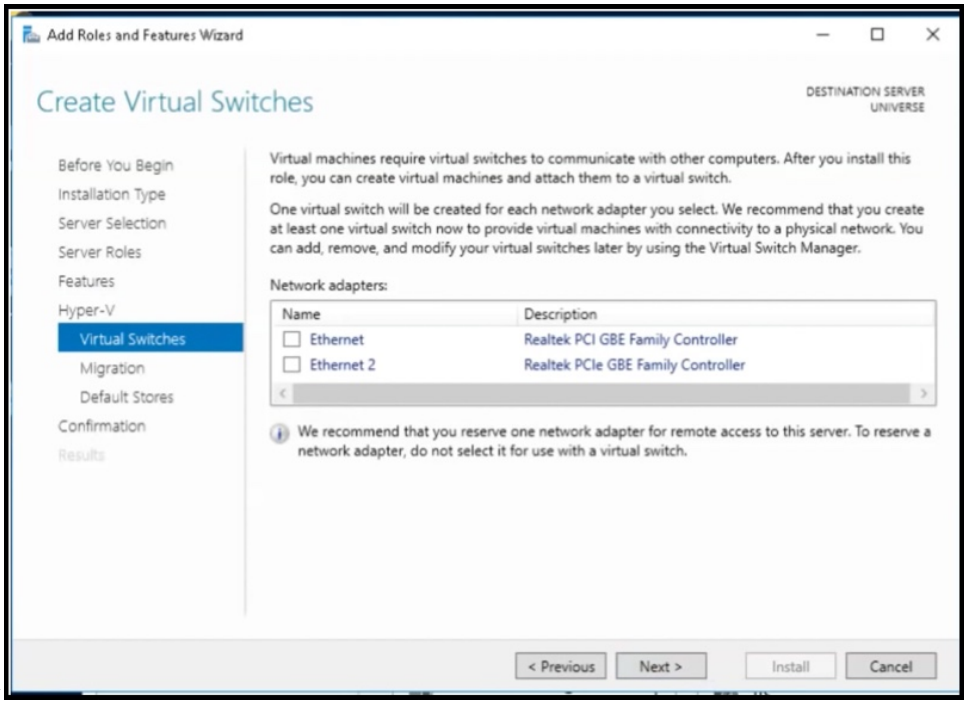
Description

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

Figure 33:

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

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



Create Virtual Switches

DESTINATION SERVER
UNIVERSE

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

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

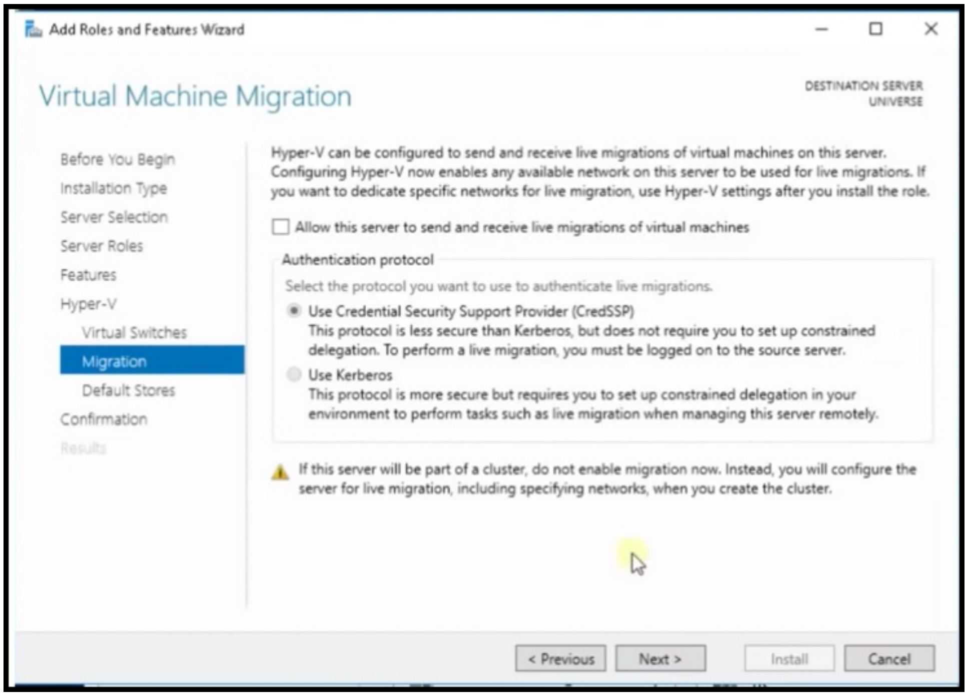
Network adapters:

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

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

Figure 34:

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



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

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

Authentication protocol

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

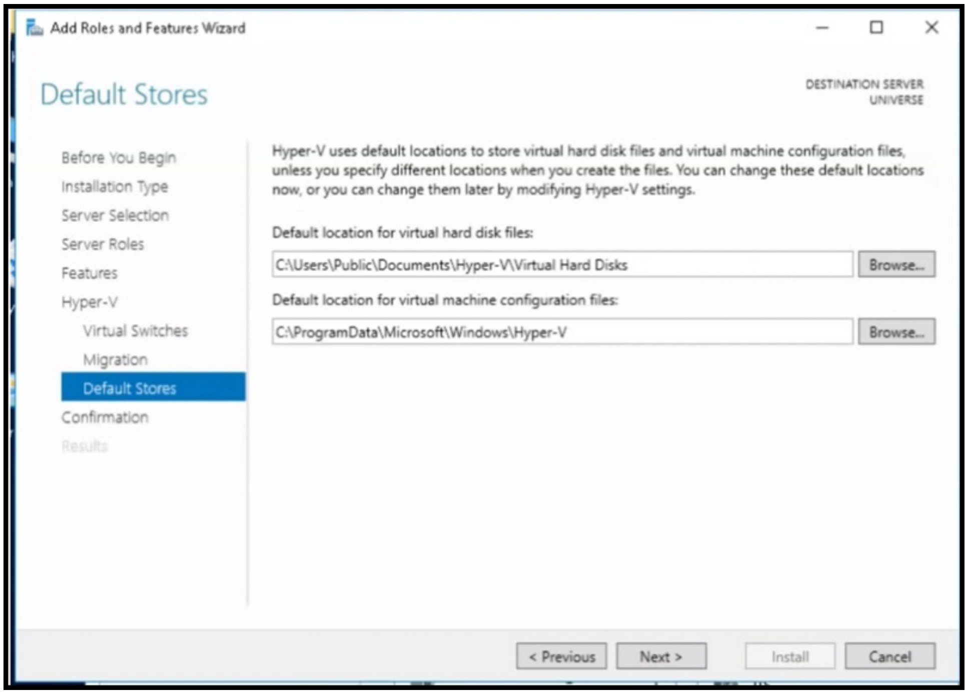
● Use Credential Security Support Provider (CredSSP)
This protocol is less secure than Kerberos, but does not require you to set up constrained delegation. To perform a live migration, you must be logged on to the source server.

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

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

Figure 35:

c) In **Default Stores**, select the location to install files or leave the default locations. Click **Next**.



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

Default location for virtual hard disk files:

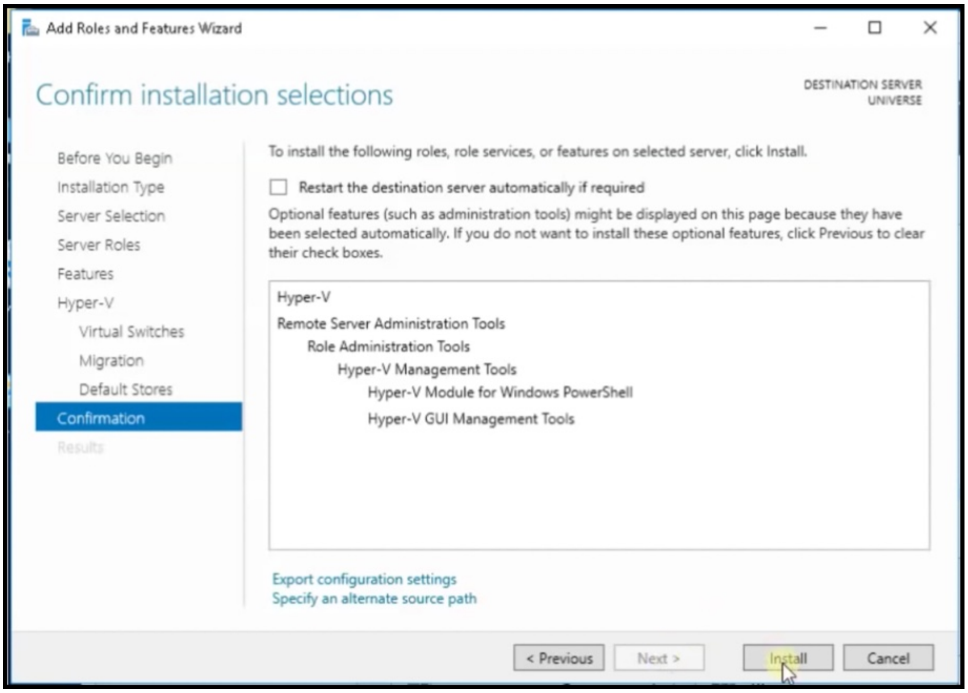
C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

Default location for virtual machine configuration files:

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

Figure 36:

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



Confirm installation selections

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

□ Restart the destination server automatically if required

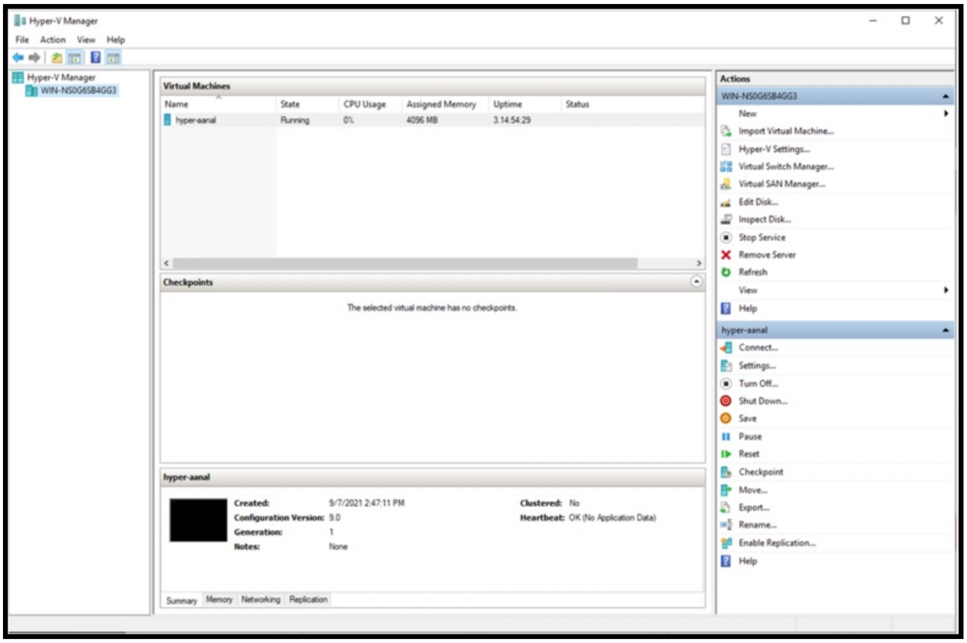
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

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

Figure 37:

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

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



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

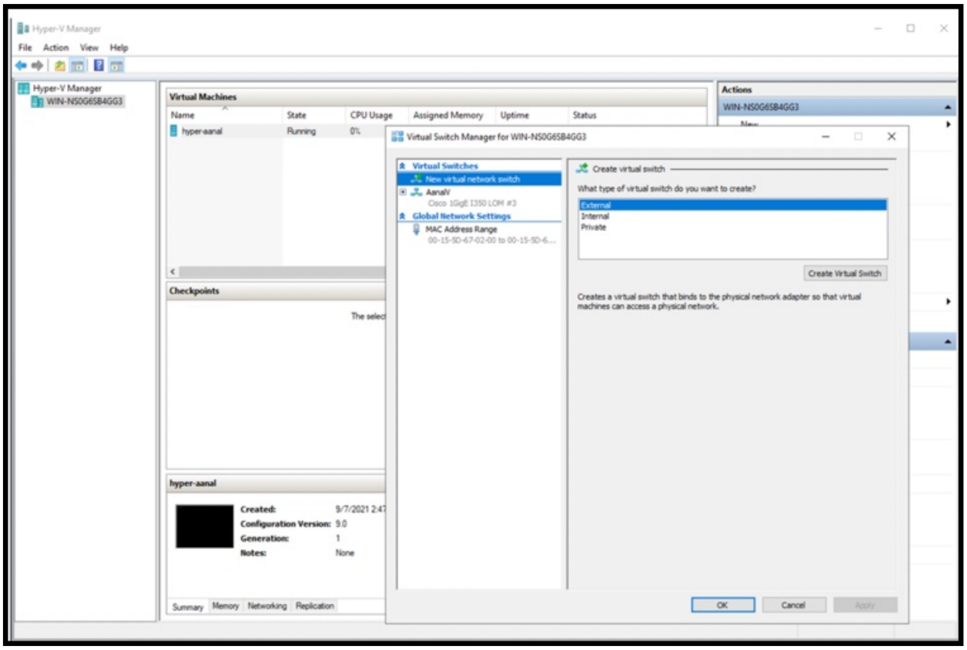
The selected virtual machine has no checkpoints.

hyper-aanal

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

Figure 38:

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



Create virtual switch

What type of virtual switch do you want to create?

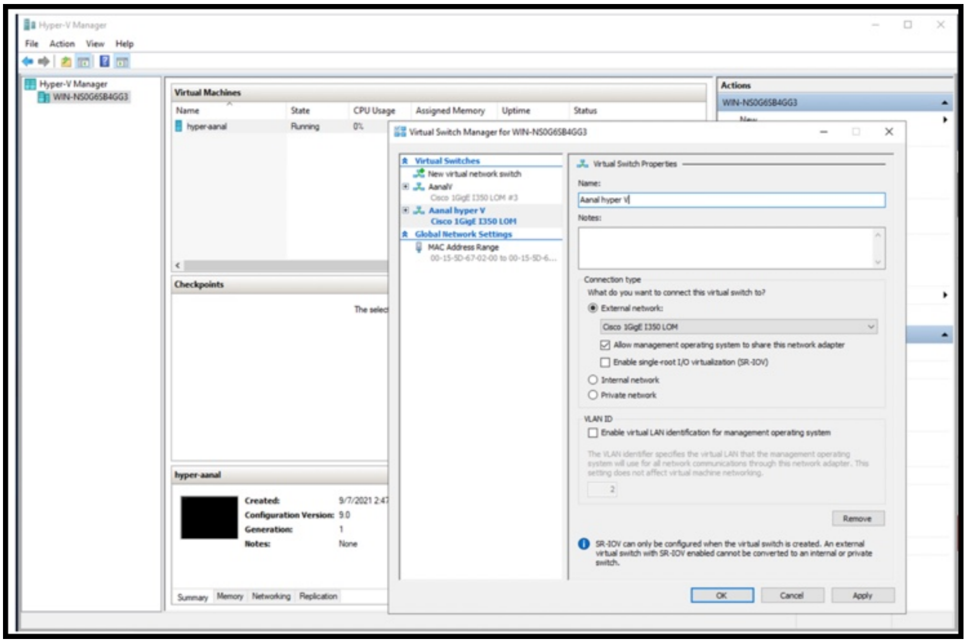
- External
- Internal
- Private

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

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

Figure 39:

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



Virtual Switch Properties

Name: Aanal hyper V

Notes:

Connection type

What do you want to connect this virtual switch to?

● External network:

Cisco 1GigE I350 LOM

☑ Allow management operating system to share this network adapter

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

○ Internal network

○ Private network

VLAN ID

□ Enable virtual LAN identification for management operating system

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

2

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

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

Figure 40:

Downloading and Deploying Hyper-V

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

Note **dnasadmin** was previously **cmxadmin**

Before you begin

Create a vSwitch on Hyper-V. Connector connects to this vSwitch. See Creating a Virtual Switch, on page 47

SUMMARY STEPS

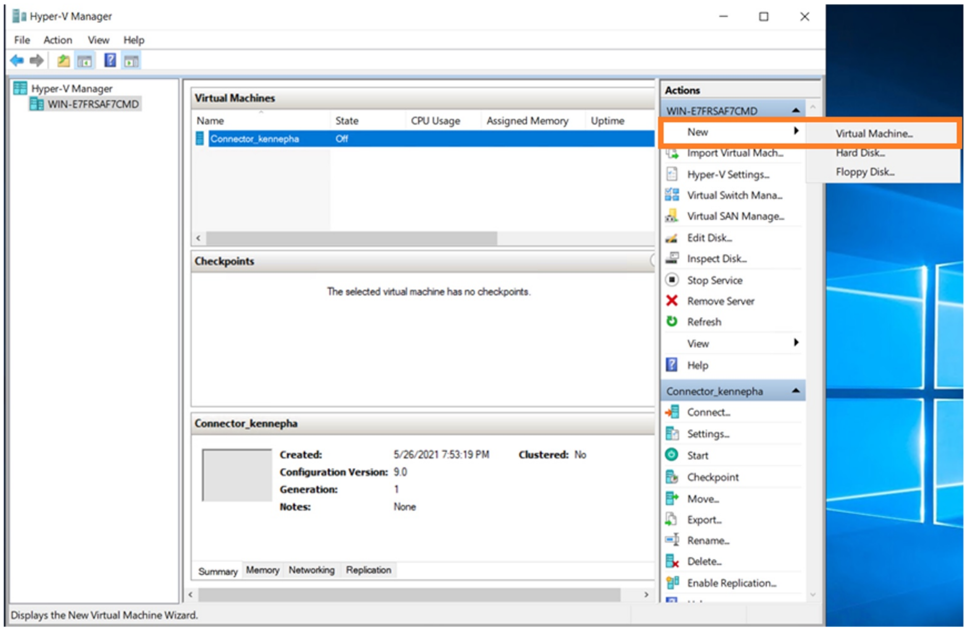
1. Download Connector VHDX image from Cisco.com and store the VHDX in a folder location where you plan to create the Hyper-V instance.
2. Right-click the vSwitch created, and select **New** > **Virtual machine**.
3. Click **Next** to begin Hyper-V deployment.
4. Provide the **Name** of the Connector and select the location to create the virtual machine.
5. In the **Sepecify Generation** page, choose **Generation 1 VM**.
6. In the **Assign Memory** page, specify 4096 MB (4GB) of memory for the virtual machine instance.
7. In the **Configure Networking** page, select the vSwitch that you created as a pre-requisite.
8. In the **Connect Virtual Hard Disk** page, select the **Use an existing hard disk** option, and select the folder location where the VHDX file has been stored (Pre-requisite).
9. In the **Completing the New Machine Wizard** page, a final summary is displayed. Review this summary and click **Finish**.
10. Select the Hyper-V instance created, and click **Start**.
11. Select the Hyper-V instance created, and click **Connect** to open the Hyper-V console.
12. Log in to the terminal and enter the default username **root** and default password **cisco**.
13. Enter the network settings by specifying parameters such as IP address, hostname, and so on, that you want to configure on the Cisco Spaces: Connector.
14. Enter the time zone.
15. Enter the Network Time Protocol (NTP) server name to synchronize the system time with the NTP server's or leave it blank if you do not want to configure an NTP server.
16. Set a new password for the **root** user.
17. Set a new password for the **dnasadmin** user, which is user with administrative privileges.
18. Copy and save the URL before the automatic reboot. You can use this URL later to open the Cisco Spaces: Connector GUI.

DETAILED STEPS

Step 1 Download Connector VHDX image from Cisco.com and store the VHDX in a folder location where you plan to create the Hyper-V instance.

Step 2 Right-click the vSwitch created, and select **New** > **Virtual machine**.

Figure 41: Start Hyper-V deployment



The selected virtual machine has no checkpoints.

Created: 5/26/2021 7:53:19 PM

Clustered: No

Configuration Version: 9.0

Generation: 1

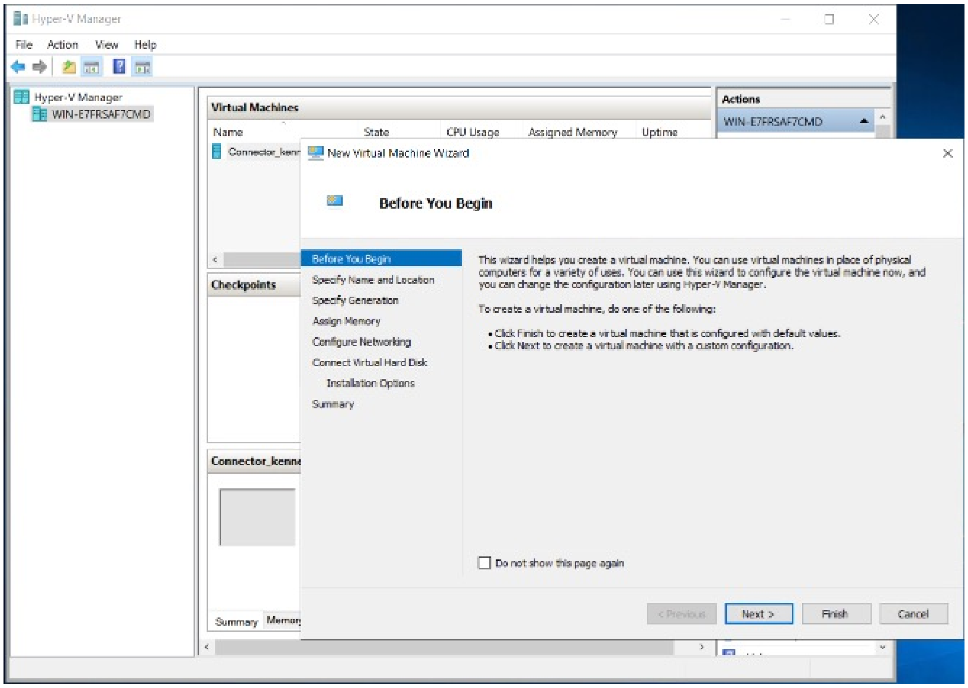
Notes: None

Displays the New Virtual Machine Wizard.

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

Step 3 Click **Next** to begin Hyper-V deployment.

Figure 42: Start Hyper-V deployment



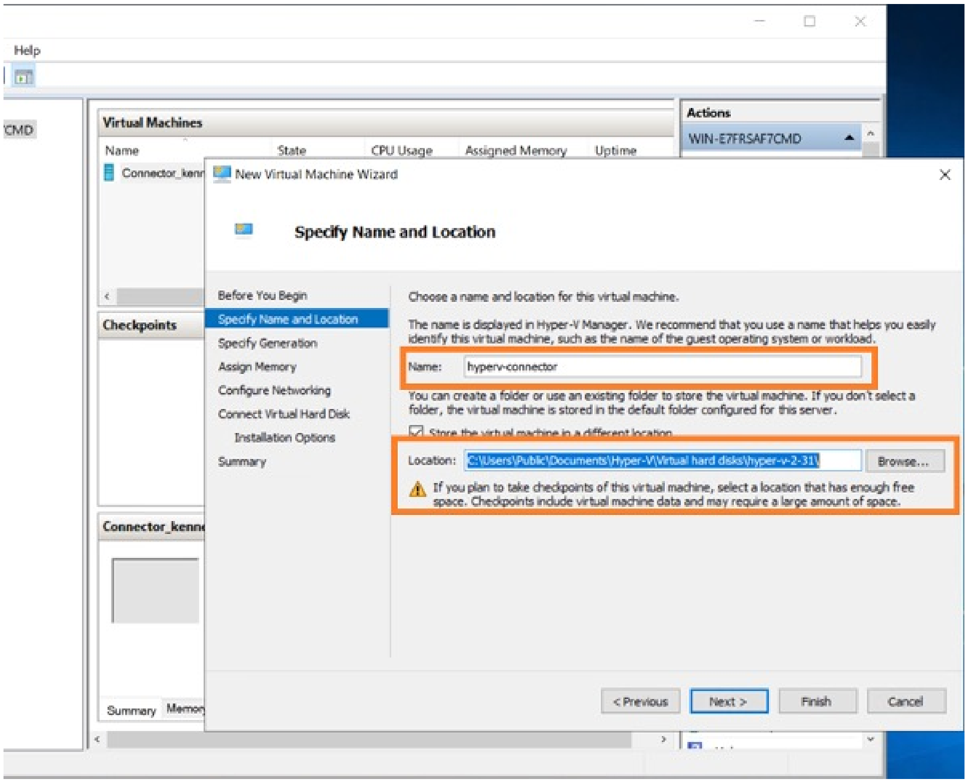
This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

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

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

□ Do not show this page again

Step 4 Provide the **Name** of the Connector and select the location to create the virtual machine.



Specify Name and Location

Choose a name and location for this virtual machine.

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

Name: hyperv-connector

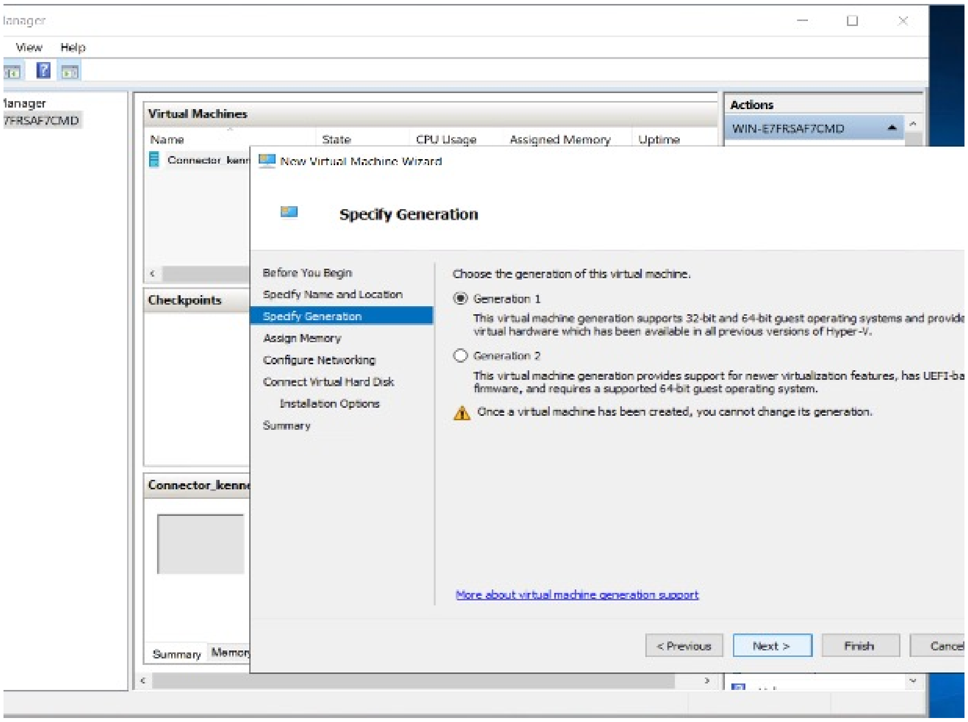
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ Store the virtual machine in a different location

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

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

Step 5 In the **Sepecify Generation** page, choose **Generation 1 VM**.



Specify Generation

Choose the generation of this virtual machine.

● Generation 1

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

○ Generation 2

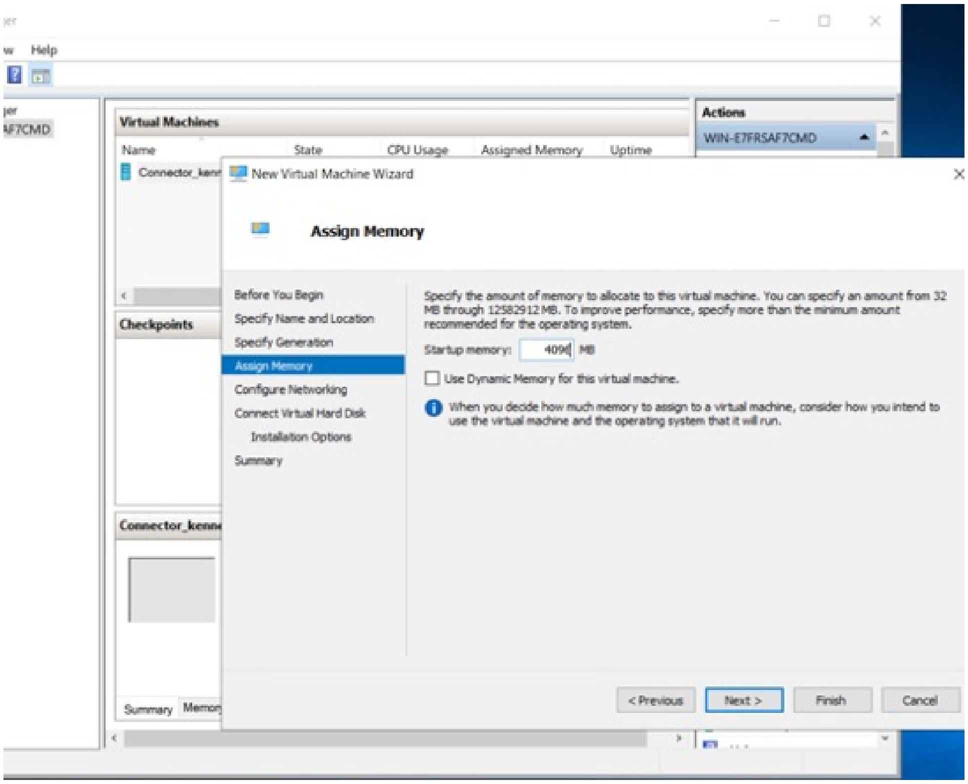
This virtual machine generation provides support for newer virtualization features, has UEFI-ba firmware, and requires a supported 64-bit guest operating system.

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

Note Generation 2 VM is not supported.

Step 6 In the **Assign Memory** page, specify 4096 MB (4GB) of memory for the virtual machine instance.

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



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

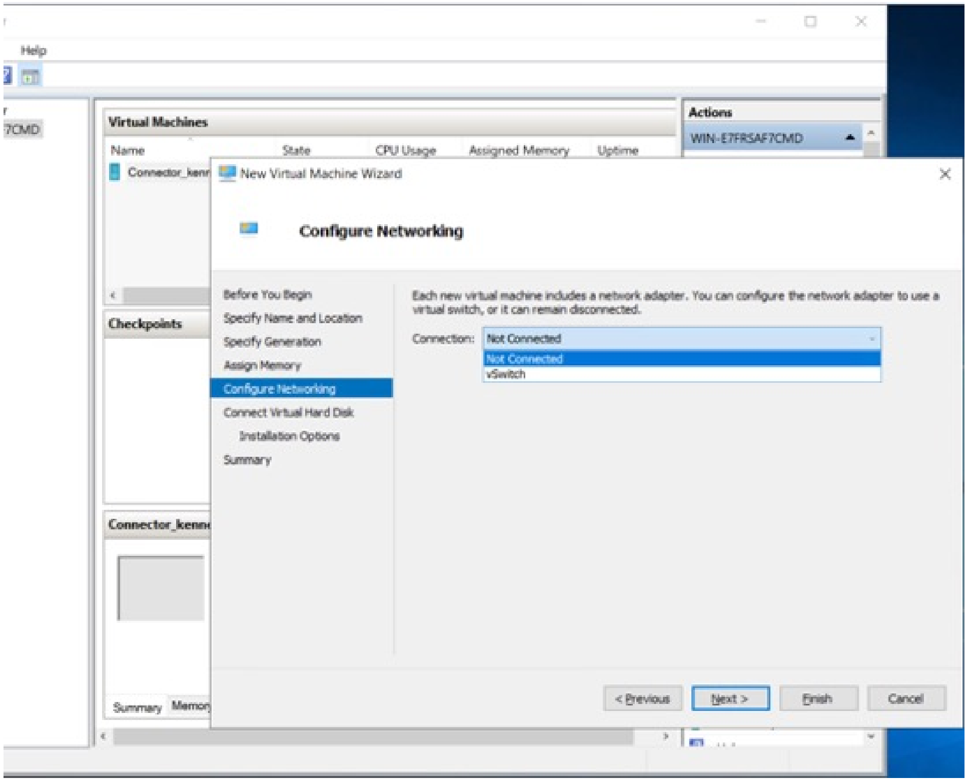
Startup memory: 4096 MB

☐ Use Dynamic Memory for this virtual machine.

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

Step 7 In the **Configure Networking** page, select the vSwitch that you created as a pre-requisite.

Figure 43: Select vSwitch



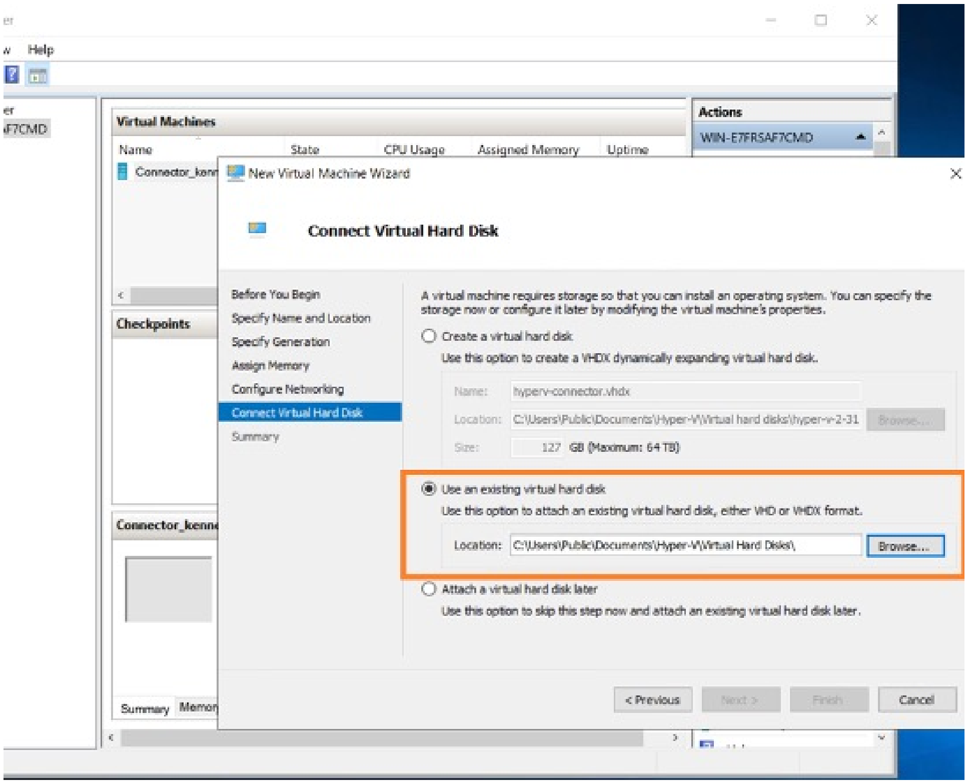
Configure Networking

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

Connection: Not Connected

- Not Connected
- vSwitch

Step 8 In the **Connect Virtual Hard Disk** page, select the **Use an existing hard disk** option, and select the folder location where the VHDX file has been stored (Pre-requisite).



New Virtual Machine Wizard

Connect Virtual Hard Disk

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary

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

○ Create a virtual hard disk

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

Name: hyperv-connector.vhdx

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

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

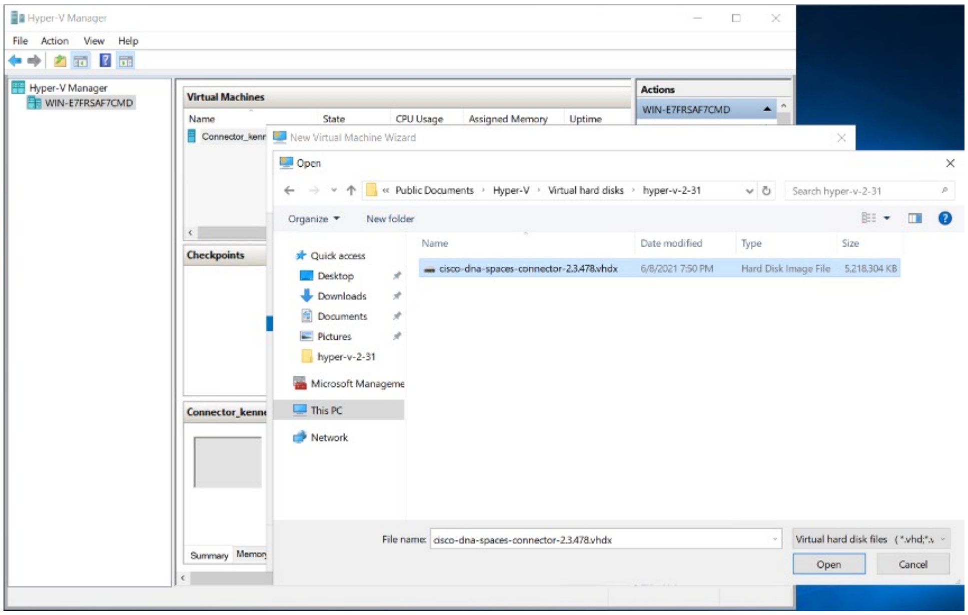
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse...

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

< Previous | Next > | Finish | Cancel

Figure 44: Folder Location where VHDX file is stored



Open

« Public Documents › Hyper-V › Virtual hard disks › hyper-v-2-31

Search hyper-v-2-31

Organize ▾ New folder

Quick access
Desktop
Downloads
Documents
Pictures
hyper-v-2-31
Microsoft Manageme
This PC
Network

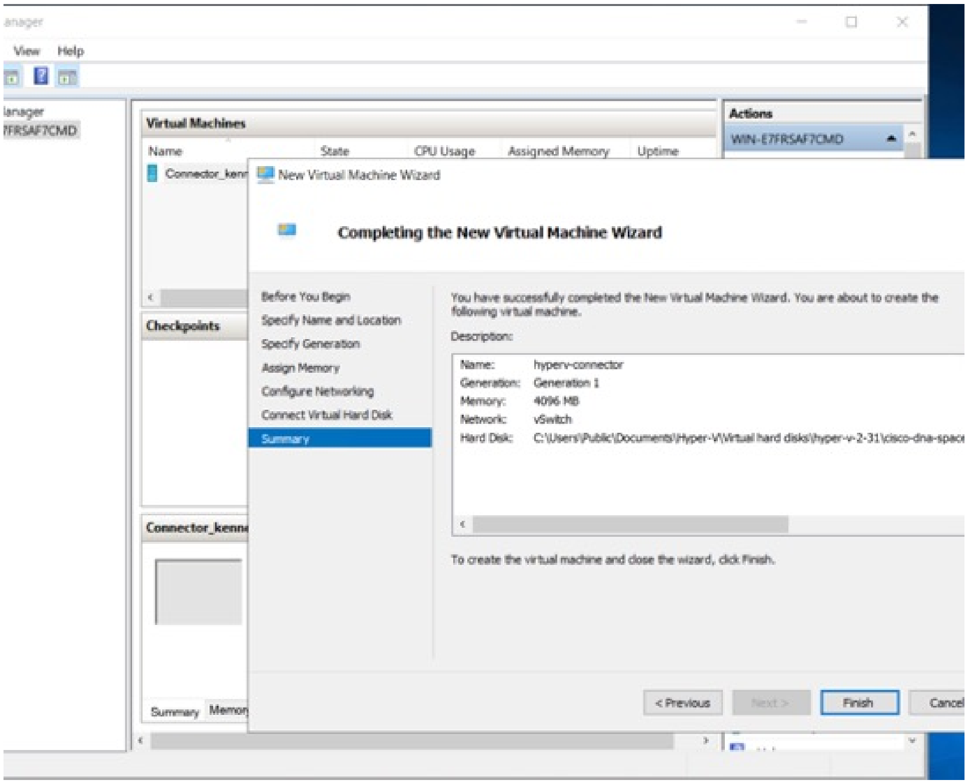
Name	Date modified	Type	Size
cisco-dna-spaces-connector-2.3.478.vhdx	6/8/2021 7:50 PM	Hard Disk Image File	5,218,304 KB

File name: cisco-dna-spaces-connector-2.3.478.vhdx

Virtual hard disk files (*.vhd;*.v

Open | Cancel

Step 9 In the **Completing the New Machine Wizard** page, a final summary is displayed. Review this summary and click **Finish**.



Completing the New Virtual Machine Wizard

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

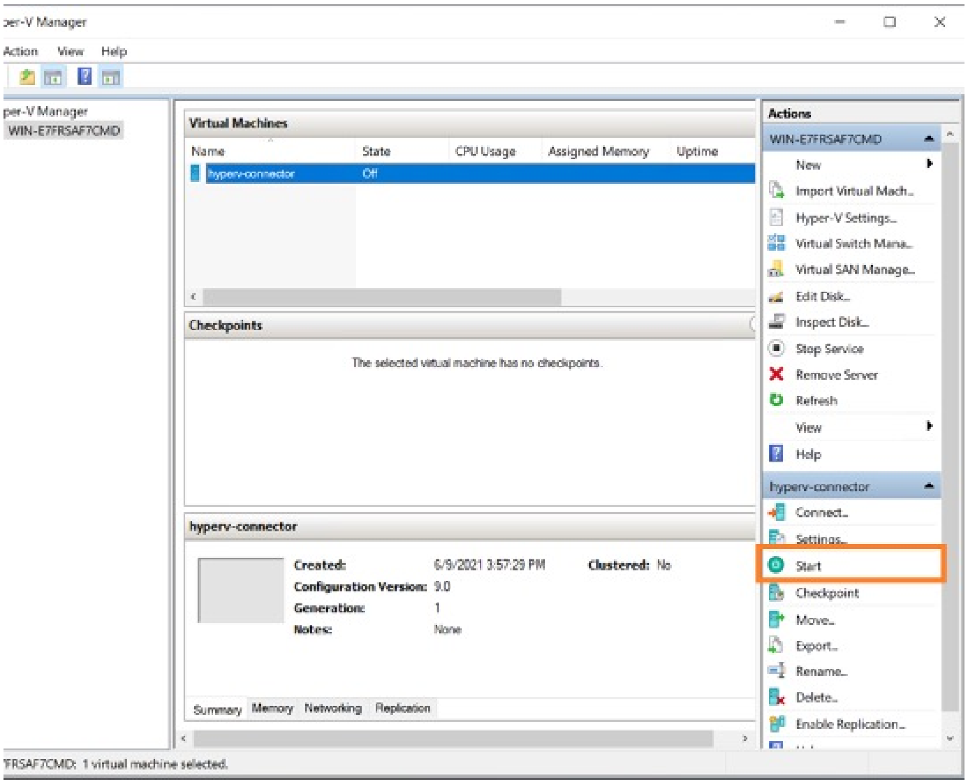
Description:

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

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

A Hyper-V instance is created.

Step 10 Select the Hyper-V instance created, and click **Start**.



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime
hyperv-connector	Off			

Checkpoints

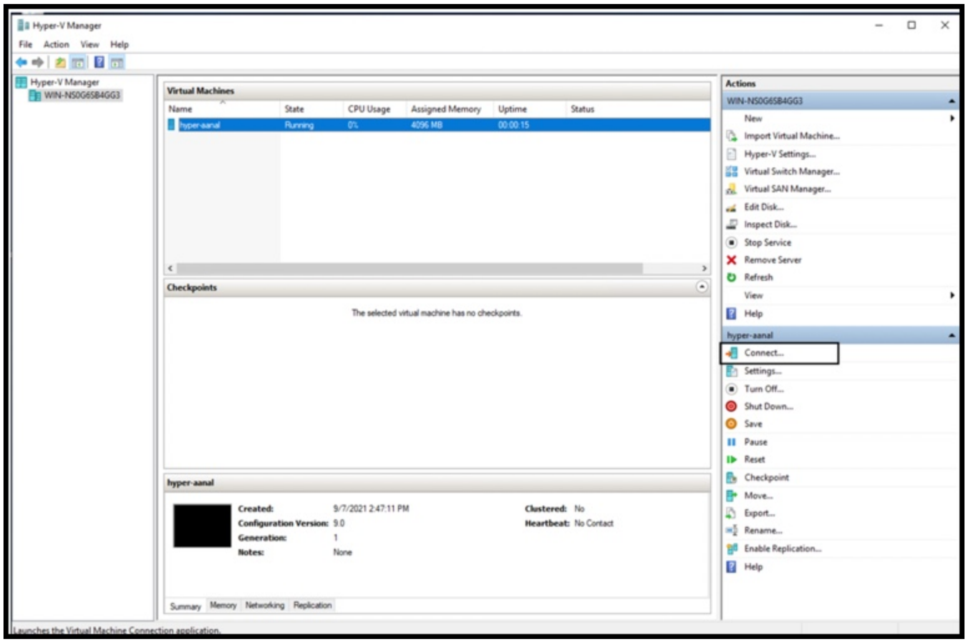
The selected virtual machine has no checkpoints.

hyperv-connector

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

FRSAF7CMD: 1 virtual machine selected.

Step 11 Select the Hyper-V instance created, and click **Connect** to open the Hyper-V console.



Virtual Machines

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

Checkpoints

The selected virtual machine has no checkpoints.

hyper-aanal

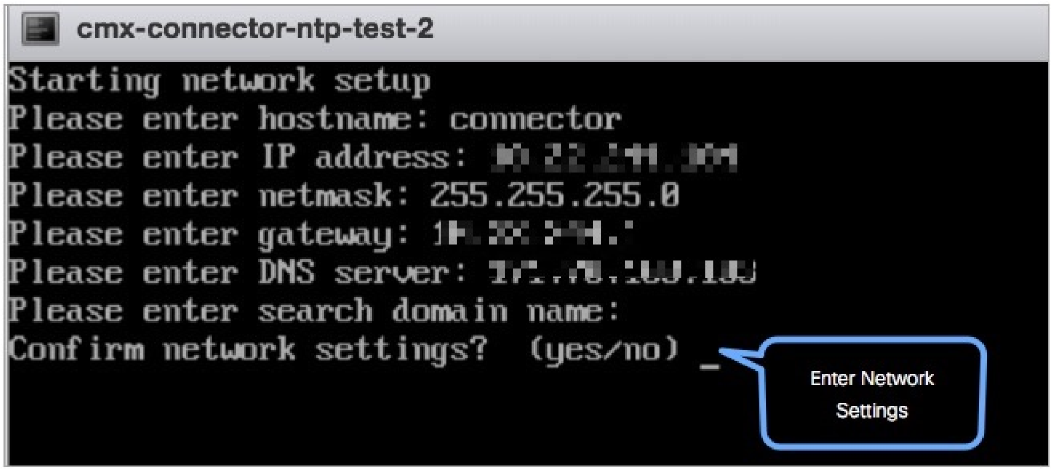
Created: 9/7/2021 2:47:11 PM **Clustered:** No
Configuration Version: 9.0 **Heartbeat:** No Contact
Generation: 1
Notes: None

Launches the Virtual Machine Connection application.

The virtual machine console is opened.

Step 12 Log in to the terminal and enter the default username **root** and default password **cisco**.

Step 13 Enter the network settings by specifying parameters such as IP address, hostname, and so on, that you want to configure on the Cisco Spaces: Connector.



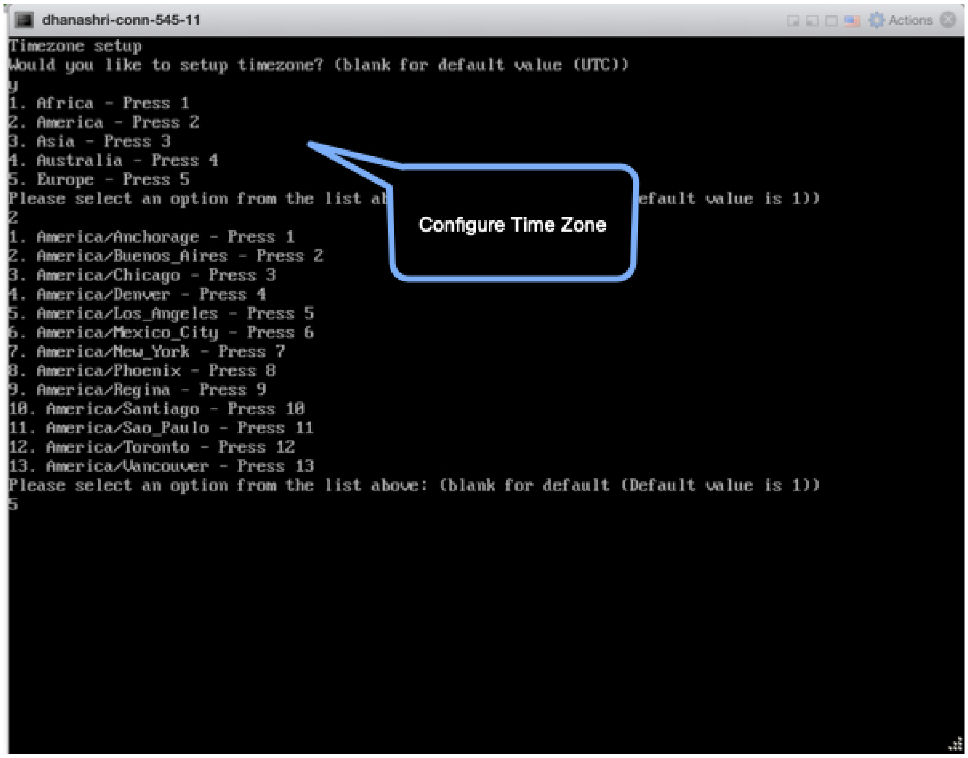
```
Starting network setup
Please enter hostname: connector
Please enter IP address: [redacted]
Please enter netmask: 255.255.255.0
Please enter gateway: [redacted]
Please enter DNS server: [redacted]
Please enter search domain name:
Confirm network settings? (yes/no) _
```

Enter Network Settings

Note Because this configuration screen times out in 60 seconds, ensure that you provide the input on time to avoid reconfiguration.

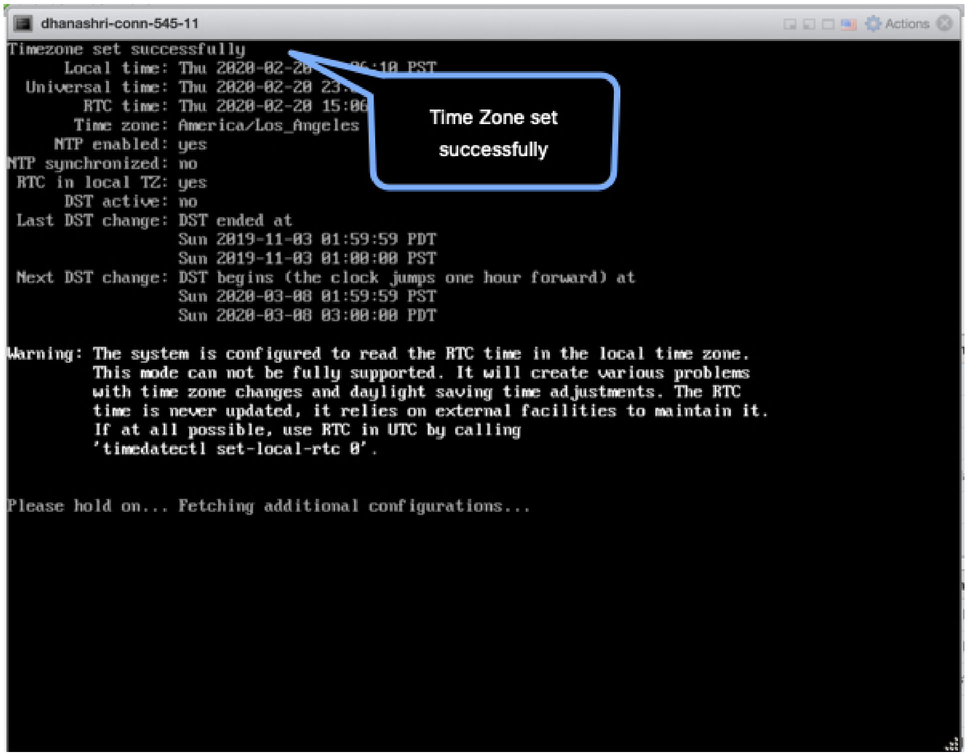
You can add multiple DNS server as a comma separated list in this step. Once the task is complete and the Cisco Spaces: Connector is deployed, you can login to the Connector CLI, and run the **connectorctl networkconfig** command to add more DNS servers or edit the existing list.

Step 14 Enter the time zone.



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

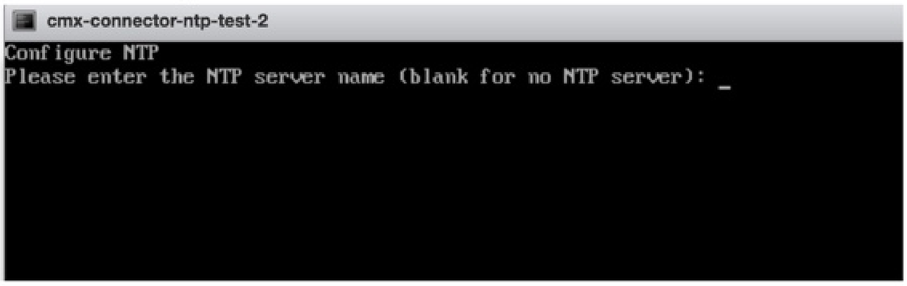
Configure Time Zone



```
Timezone set successfully
      Local time: Thu 2020-02-20 [illegible]6:10 PST
  Universal time: Thu 2020-02-20 23:[illegible]
        RTC time: Thu 2020-02-20 15:06[illegible]
       Time zone: America/Los_Angeles
     NTP enabled: yes
NTP synchronized: no
 RTC in local TZ: yes
      DST active: no
 Last DST change: DST ended at
                  Sun 2019-11-03 01:59:59 PDT
                  Sun 2019-11-03 01:00:00 PST
 Next DST change: DST begins (the clock jumps one hour forward) at
                  Sun 2020-03-08 01:59:59 PST
                  Sun 2020-03-08 03:00:00 PDT

Warning: The system is configured to read the RTC time in the local time zone.
         This mode can not be fully supported. It will create various problems
         with time zone changes and daylight saving time adjustments. The RTC
         time is never updated, it relies on external facilities to maintain it.
         If at all possible, use RTC in UTC by calling
         'timedatectl set-local-rtc 0'.


Please hold on... Fetching additional configurations...
```

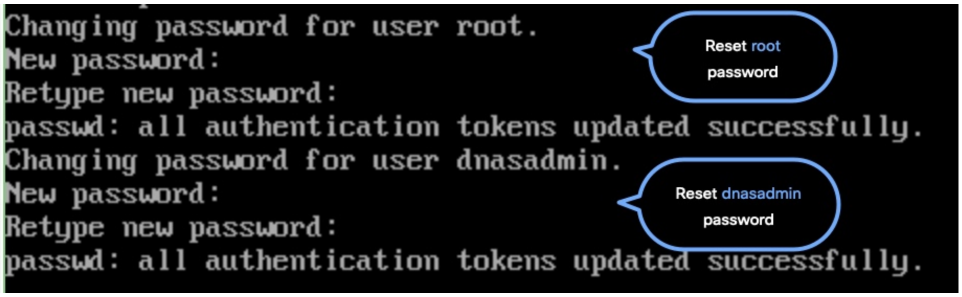
Step 15 Enter the Network Time Protocol (NTP) server name to synchronize the system time with the NTP server's or leave it blank if you do not want to configure an NTP server.

Figure 45: Enter NTP Setting



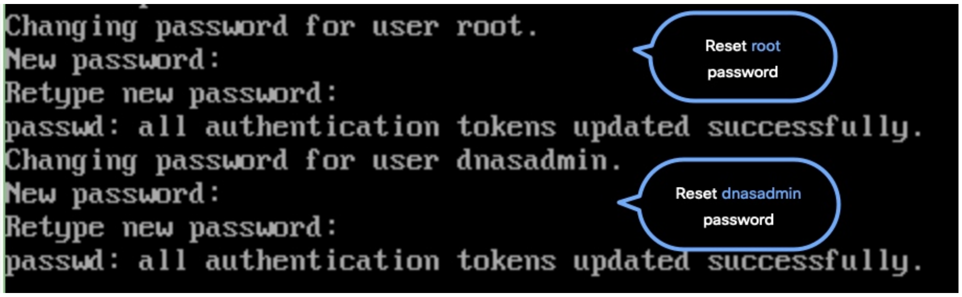
```
Configure NTP
Please enter the NTP server name (blank for no NTP server): _
```

Step 16 Set a new password for the **root** user.



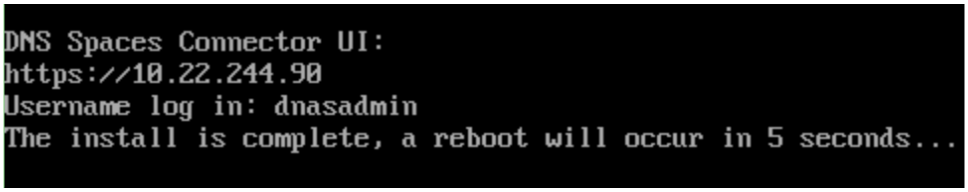
```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Step 17 Set a new password for the **dnasadmin** user, which is user with administrative privileges.



```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Step 18 Copy and save the URL before the automatic reboot. You can use this URL later to open the Cisco Spaces: Connector GUI.



```
DNS Spaces Connector UI:
https://10.22.244.90
Username log in: dnasadmin
The install is complete, a reboot will occur in 5 seconds...
```

CHAPTER 9

Connector on Cisco Spaces

- Creating a Connector Instance and Retrieving a Token from Cisco Spaces (Wired), on page 65
- Retrieving a Token for a Connector from Cisco Spaces (Wireless), on page 67
- Activating the Cisco Spaces: Connector , on page 70

Creating a Connector Instance and Retrieving a Token from Cisco Spaces (Wired)

This procedure shows you how to connect the Connector with your Cisco Spaces account.

In the following procedure, you generate a token for each Connector that you add to your Cisco Spaces account. Each token is specific to a Connector and hence enables Cisco Spaces to identify and connect to the Connector.

Cisco Spaces supports multiple Connectors, and you can associate each Connector with one or multiple controllers.

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

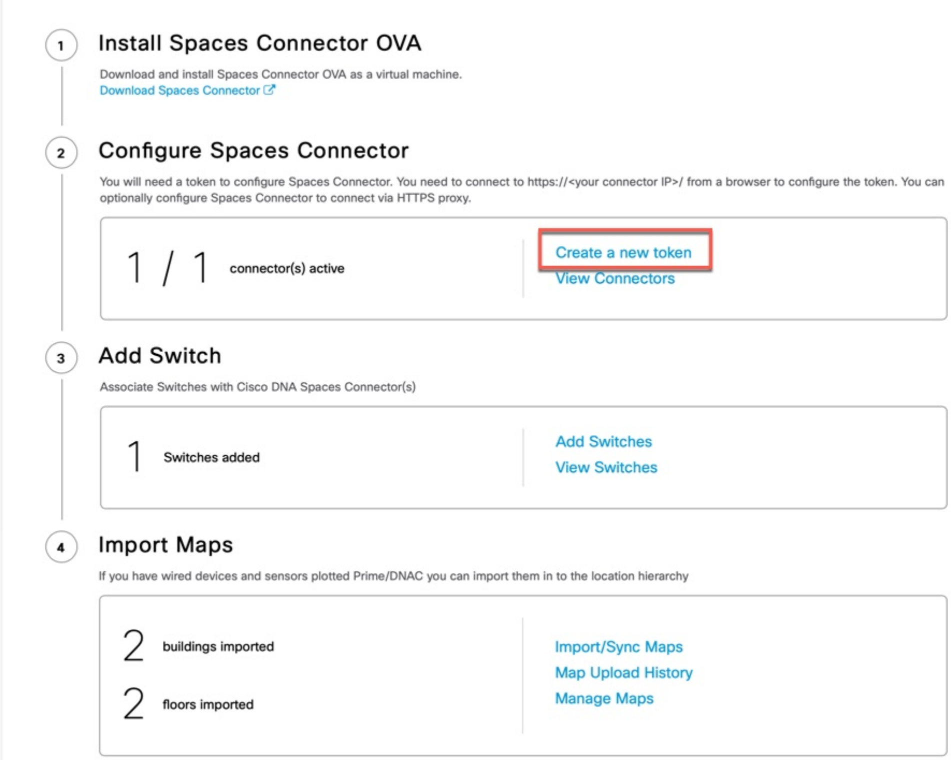
Before you begin

Download and deploy the Cisco Spaces: Connector OVA.

Step 1 Log in to **Cisco Spaces >Setup >Wired Networks**.

Note The Cisco Spaces URL is region-dependent.

Step 2 From the **Step 2: Configure Spaces Connector** area, click **Create a new token**.



1 Install Spaces Connector OVA

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

2 Configure Spaces Connector

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

1 / 1 connector(s) active

Create a new token
View Connectors

3 Add Switch

Associate Switches with Cisco DNA Spaces Connector(s)

1 Switches added

Add Switches
View Switches

4 Import Maps

If you have wired devices and sensors plotted Prime/DNAC you can import them in to the location hierarchy

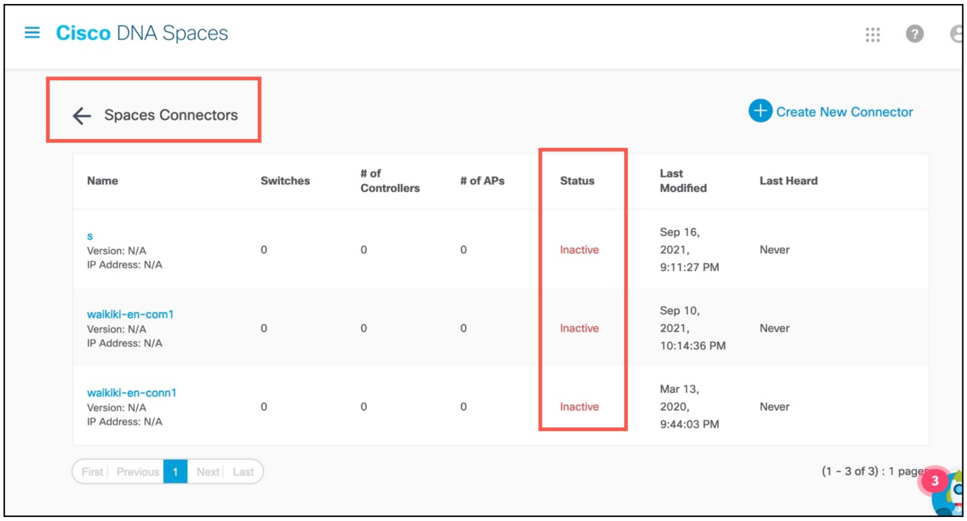
2 buildings imported

2 floors imported

Import/Sync Maps
Map Upload History
Manage Maps

Step 3 In the **Create a new token** page, enter a name for the Connector. Click **Generate Token**.

A token is generated. Copy this token by using the copy button. Configure this on the Connector UI. Once configured, a new Connector is added and the Status turns to **Active**.



Cisco DNA Spaces

Spaces Connectors

Create New Connector

Name	Switches	# of Controllers	# of APs	Status	Last Modified	Last Heard
s Version: N/A IP Address: N/A	0	0	0	Inactive	Sep 16, 2021, 9:11:27 PM	Never
waikiki-en-com1 Version: N/A IP Address: N/A	0	0	0	Inactive	Sep 10, 2021, 10:14:36 PM	Never
waikiki-en-conn1 Version: N/A IP Address: N/A	0	0	0	Inactive	Mar 13, 2020, 9:44:03 PM	Never

Step 4 From the Spaces Connector page displayed, click the three dots button of the Connector that you just added. Click **Manage IoT Services**.

Step 5 In the **Manage IoT Service** page, click the three dots button of a switch. Choose **Enable Service** to enable IoT stream.

Configure the Wired IoT Manage Stream.

Retrieving a Token for a Connector from Cisco Spaces (Wireless)

This procedure shows you how to connect the Connector with your Cisco Spaces account.

In the following procedure, you generate a token for each Connector that you add to your Cisco Spaces account. Each token is specific to a Connector and hence enables Cisco Spaces to identify and connect to the Connector.

Cisco Spaces supports multiple Connectors, and you can associate each Connector with one or multiple 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.

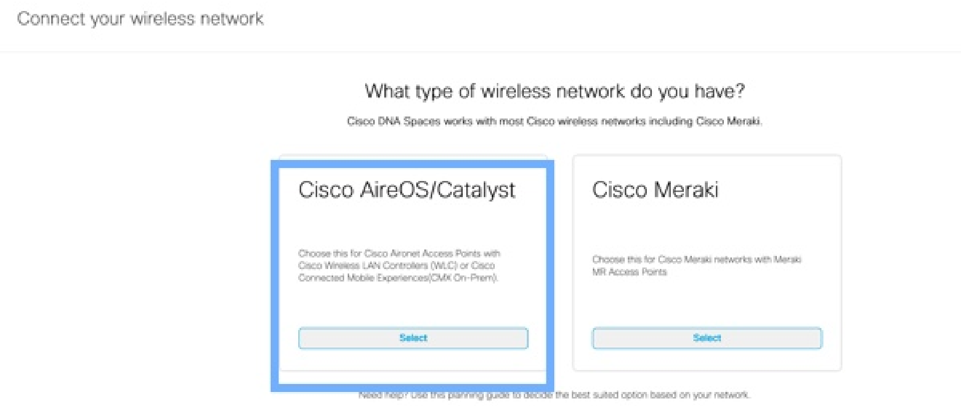
Step 1 Log in to **Cisco Spaces**.

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/Catalyst** area, click **Select.**



Connect your wireless network

What type of wireless network do you have?

Cisco DNA Spaces works with most Cisco wireless networks including Cisco Meraki.

Cisco AireOS/Catalyst

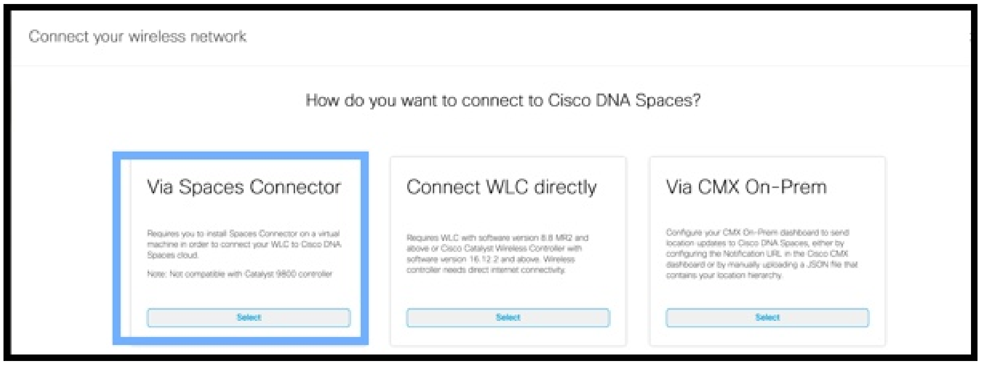
Choose this for Cisco Aironet Access Points with Cisco Wireless LAN Controllers (WLC) or Cisco Connected Mobile Experiences(CMX On-Prem).

Cisco Meraki

Choose this for Cisco Meraki networks with Meraki MR Access Points

Need help? Use this planning guide to decide the best suited option based on your network.

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



Connect your wireless network

How do you want to connect to Cisco DNA Spaces?

Via Spaces Connector

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

Note: Not compatible with Catalyst 9800 controller

Select

Connect WLC directly

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

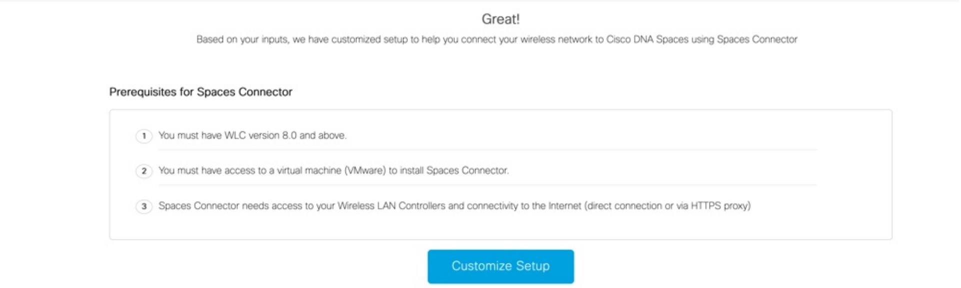
Select

Via CMX On-Prem

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

Select

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



Great!

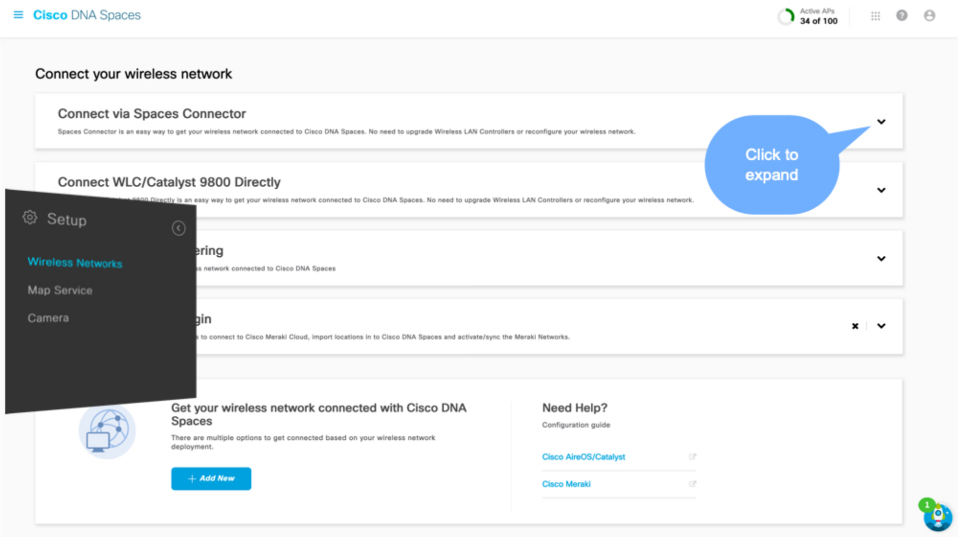
Based on your inputs, we have customized setup to help you connect your wireless network to Cisco DNA Spaces using Spaces Connector

Prerequisites for Spaces Connector

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

Customize Setup

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



Connect your wireless network

Connect via Spaces Connector

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

Connect WLC/Catalyst 9800 Directly

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

...ering

...s network connected to Cisco DNA Spaces

...gin

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

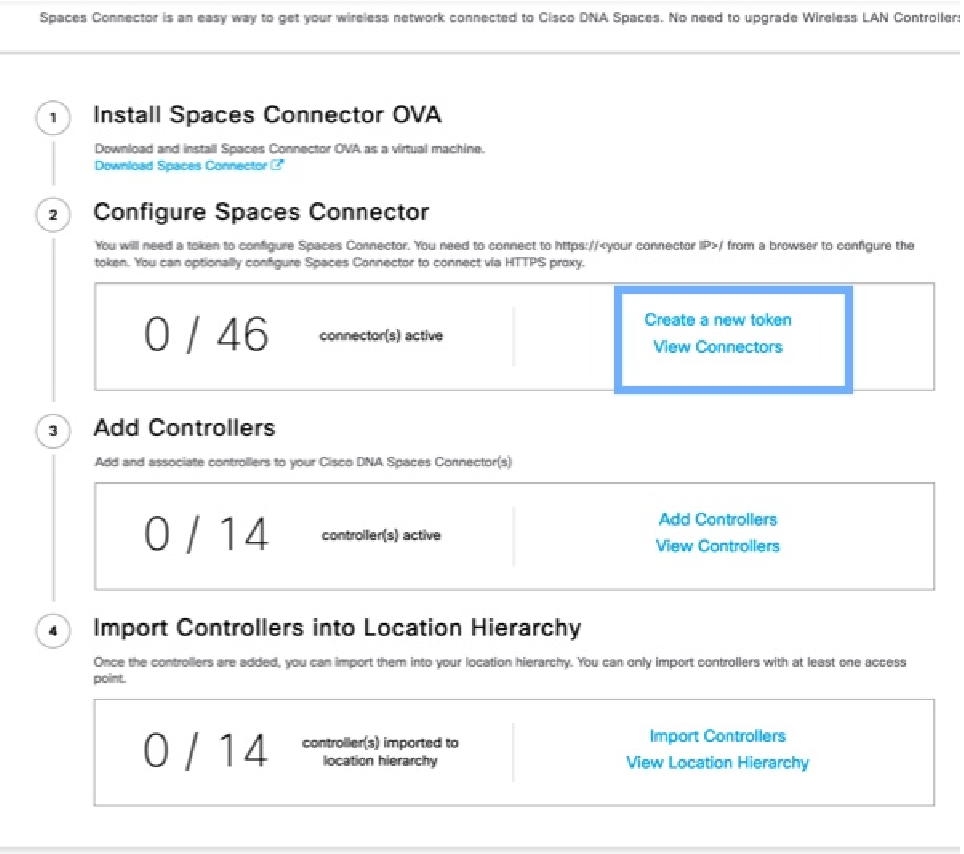
Get your wireless network connected with Cisco DNA Spaces

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

Need Help?

Configuration guide

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



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

1 Install Spaces Connector OVA

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

2 Configure Spaces Connector

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

0 / 46 connector(s) active — Create a new token | View Connectors

3 Add Controllers

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

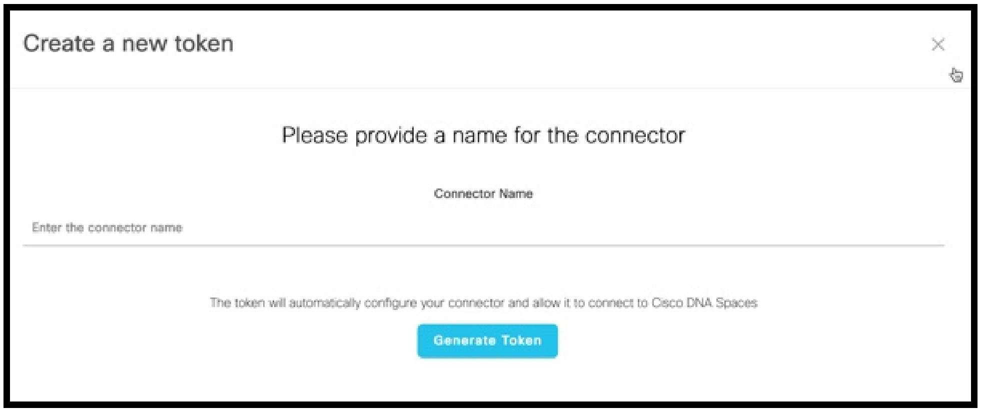
0 / 14 controller(s) active — Add Controllers | View Controllers

4 Import Controllers into Location Hierarchy

Once the controllers are added, you can import them into your location hierarchy. You can only import controllers with at least one access point.

0 / 14 controller(s) imported to location hierarchy — Import Controllers | View Location Hierarchy

Step 9 In the **Create a new token** dialog box, enter the name of the Connector.



Create a new token ×

Please provide a name for the connector

Connector Name

Enter the connector name

The token will automatically configure your connector and allow it to connect to Cisco DNA Spaces

Generate Token

Step 10 Click **Generate Token.**

Step 11 In the dialog box that appears, click **Copy** to copy the token string.

Activating the Cisco Spaces: Connector

Using the token retrieved for this Connector from Cisco Spaces, this procedure shows you how to activate the Connector.

Before you begin

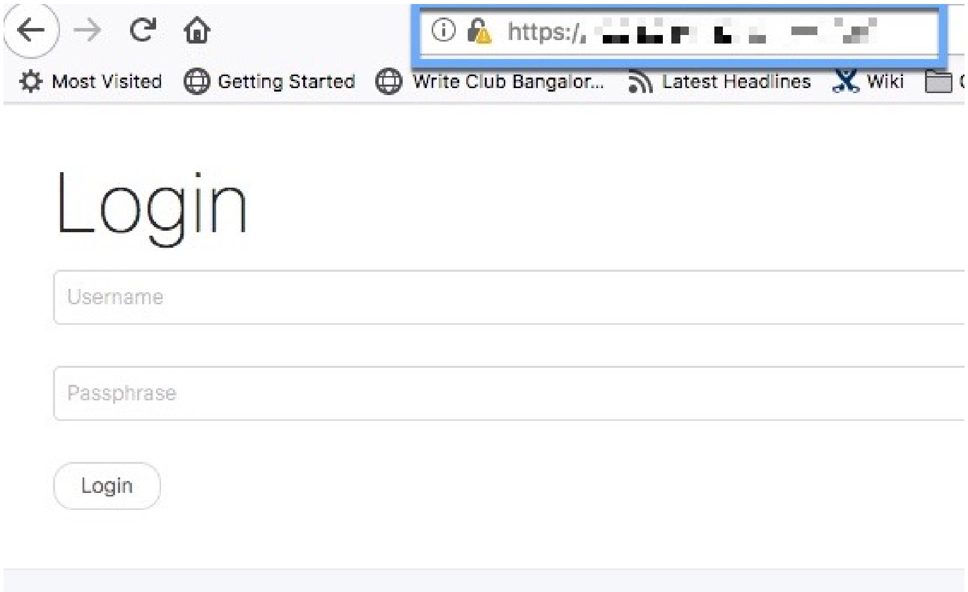
Deploy the Cisco Spaces: Connector OVA and configure an IP address. Retrieve the token for the Connector from Cisco Spaces.

SUMMARY STEPS

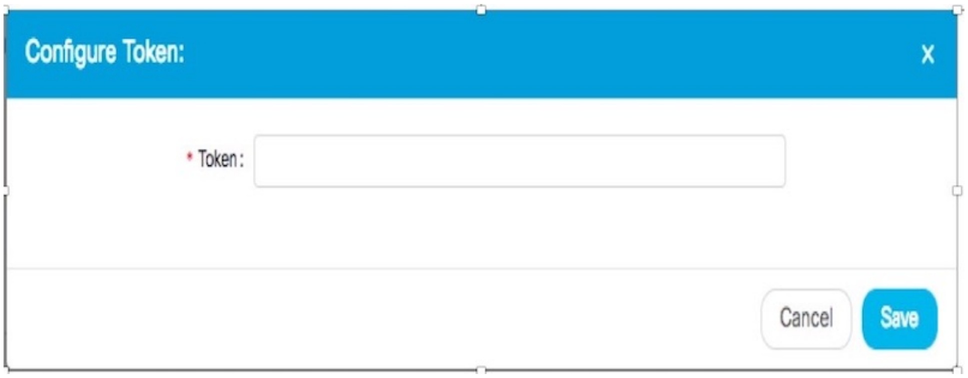
1. Launch the Cisco Spaces: Connector GUI and enter the username **dnasadmin** and the password you configured earlier for this user.
2. Click the settings (gear icon) on the top-right corner of the window and choose **Configure Token** and add the token that is received from Cisco Spaces, and click **Save**.
3. Observe the health of various connections on the dashboard.

DETAILED STEPS

Step 1 Launch the Cisco Spaces: Connector GUI and enter the username **dnasadmin** and the password you configured earlier for this user.



Step 2 Click the settings (gear icon) on the top-right corner of the window and choose **Configure Token** and add the token that is received from Cisco Spaces, and click **Save**.



Note

- After entering the token, you may have to wait a few minutes for the Cisco Spaces: Connector to initialize and download the latest docker images from Cisco Spaces. The actual duration depends on the speed of your network connection. The status changes from **Configuring Token** to **Retrieving Connector Status**. The **Configure Token** notification option disappears from the Cisco Spaces: Connector Web UI.

Step 3 Observe the health of various connections on the dashboard.

What to do next

See Connector GUI, on page 73 for a detailed description of the elements of the dashboard.

Note

- With CSCvx02620, Cisco Spaces: Connector GUI hangs after entering credentials. The page for entering credentials is displayed, and then the Connector WebUI hangs without any error. You can still SSH into the Connector.

  The error is caused when you have added the token from Cisco Spaces to the Connector while there was a problem in the connectivity between the Connector and the Cisco Spaces GUI. If this was the case, the Connector can stop working during the succeeding login attempt.

  To recover access to the Connector GUI, you should remove the token from the database.

CHAPTER 10

Connector GUI

- Connector GUI, on page 73

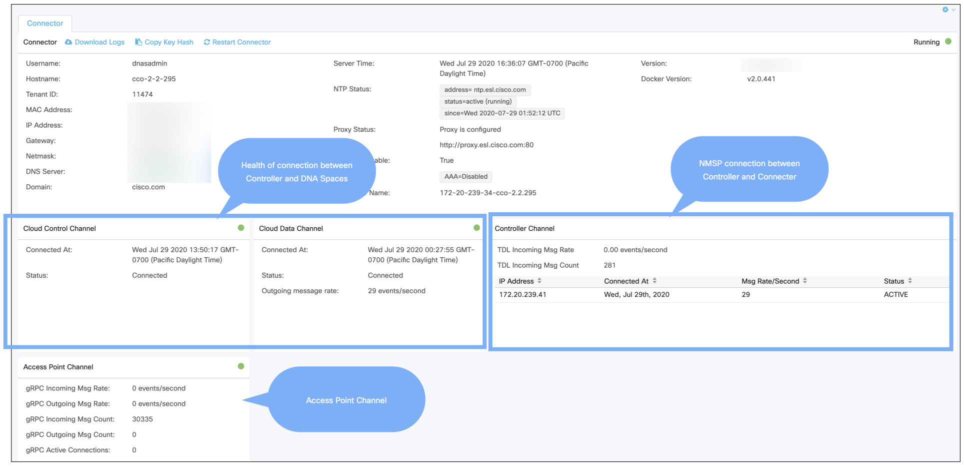
Connector GUI

- **Status**: Status of Cisco Spaces: Connector in the top-right corner.
- **Cloud Control Channel**: Health of connection of the control channel between Connector and Cisco Spaces.
- **Cloud Data Channel**: Health of connection of the data channel between Connector and Cisco Spaces.
- **Controller Channel**: NMSP connection between Connector and Cisco AireOS Wireless Controller or the Cisco Catalyst 9800 Series Wireless Controllers.

  TDL message rate and message count gives details of telemetry subscriptions. TDL messages populate when the Connector is used as a collector of model-driven telemetry data over telemetry subscription.

Note Telemetry subscriptions can be created only on Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches over programmable interfaces such as NETCONF.

Figure 46: Connector Details



Connector

Connector | Download Logs | Copy Key Hash | Restart Connector | Running ●

Username: dnasadmin
Hostname: cco-2-2-295
Tenant ID: 11474
MAC Address: [redacted]
IP Address:
Gateway:
Netmask:
DNS Server:
Domain: cisco.com

Server Time: Wed Jul 29 2020 16:36:07 GMT-0700 (Pacific Daylight Time)
NTP Status: address= ntp.esl.cisco.com
status=active (running)
since=Wed 2020-07-29 01:52:12 UTC
Proxy Status: Proxy is configured
http://proxy.esl.cisco.com:80
able: True
AAA=Disabled
Name: 172-20-239-34-cco-2.2.295

Version: [redacted]
Docker Version: v2.0.441

Cloud Control Channel ●

Connected At: Wed Jul 29 2020 13:50:17 GMT-0700 (Pacific Daylight Time)
Status: Connected

Cloud Data Channel ●

Connected At: Wed Jul 29 2020 00:27:55 GMT-0700 (Pacific Daylight Time)
Status: Connected
Outgoing message rate: 29 events/second

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

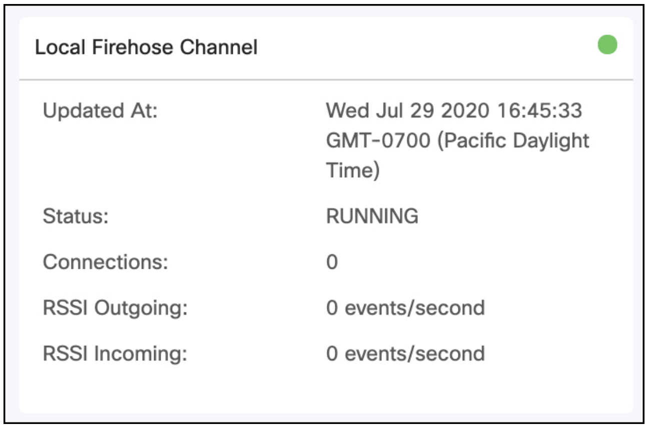
Access Point Channel ●

gRPC Incoming Msg Rate: 0 events/second
gRPC Outgoing Msg Rate: 0 events/second
gRPC Incoming Msg Count: 30335
gRPC Outgoing Msg Count: 0
gRPC Active Connections: 0

Health of connection between Controller and DNA Spaces
NMSP connection between Controller and Connecter
Access Point Channel

- **Local Firehose Channel Details**: Status of the two-way channel used to exchange the stream of raw firehose API data between Cisco Spaces and Cisco Spaces-partnered application.

Figure 47: Local Firehose Channel Status (On Connector)

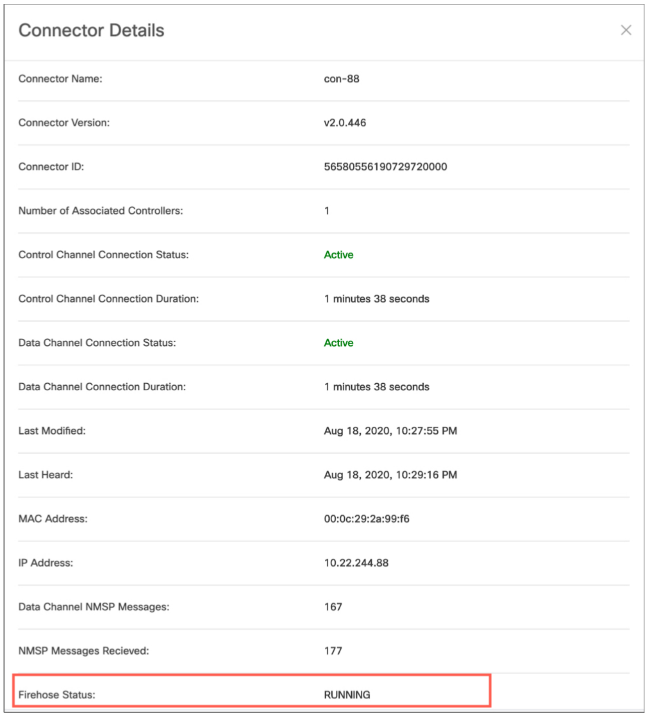


Local Firehose Channel ●

Updated At: Wed Jul 29 2020 16:45:33 GMT-0700 (Pacific Daylight Time)
Status: RUNNING
Connections: 0
RSSI Outgoing: 0 events/second
RSSI Incoming: 0 events/second

You can also find the local firehose channel status on the Cisco Spaces dashboard.

Figure 48: Local Firehose Channel Status (On Cisco Spaces dashboard)

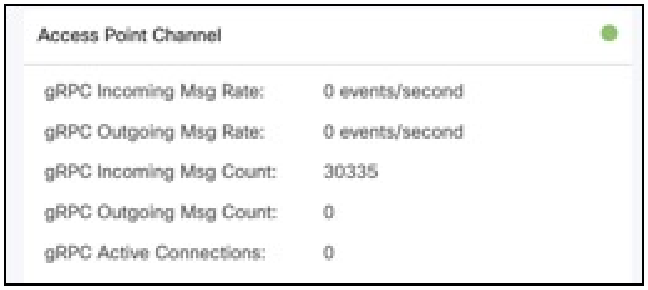


Connector Details

Connector Name:	con-88
Connector Version:	v2.0.446
Connector ID:	56580556190729720000
Number of Associated Controllers:	1
Control Channel Connection Status:	Active
Control Channel Connection Duration:	1 minutes 38 seconds
Data Channel Connection Status:	Active
Data Channel Connection Duration:	1 minutes 38 seconds
Last Modified:	Aug 18, 2020, 10:27:55 PM
Last Heard:	Aug 18, 2020, 10:29:16 PM
MAC Address:	00:0c:29:2a:99:f6
IP Address:	10.22.244.88
Data Channel NMSP Messages:	167
NMSP Messages Recieved:	177
Firehose Status:	RUNNING

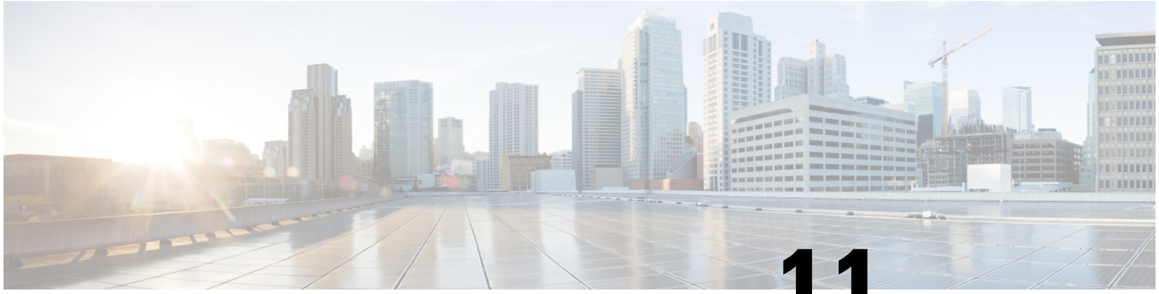
- **Access Point Channel Details**: Status of the gRPC channel between Connector and the access points with IoT gateway enabled on it. Data from IoT services is an example of this kind of data.

Figure 49: gRPC Details



Access Point Channel

gRPC Incoming Msg Rate:	0 events/second
gRPC Outgoing Msg Rate:	0 events/second
gRPC Incoming Msg Count:	30335
gRPC Outgoing Msg Count:	0
gRPC Active Connections:	0



CHAPTER 11

Configuring Proxy

- Configuring a Proxy , on page 77

Configuring a Proxy

In the Connector GUI, you can also configure the proxy and other privacy settings. You can set up a proxy to connect the Connector to the Cisco Spaces if the Cisco UCS hosting the Connector is behind a proxy. Without this proxy configuration, the Connector is unable to communicate with the Cisco Spaces.

SUMMARY STEPS

1. SSH into the Connector CLI interface. Copy the proxy certificate file to a location accessible by **dnasadmin** user.
2. (Optional) Run the **setproxycert** command from the CLI
3. Return to the Connector GUI and click **set up HTTP Proxy**. Enter your proxy address in the dialog box displayed.

DETAILED STEPS

Step 1 SSH into the Connector CLI interface. Copy the proxy certificate file to a location accessible by **dnasadmin** user.

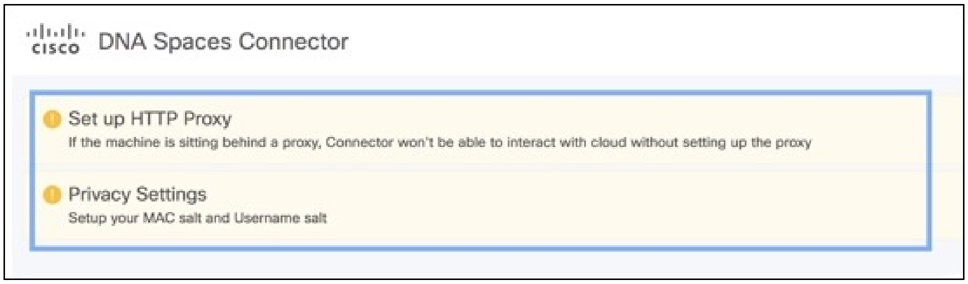
```
Username:~ username$ scp ~/Downloads/cert.pem dnasadmin@x.x.x.x
Username:~ username$ ssh dnasadmin@x.x.x.x
dnasadmin@x.x.x.x's password:
Last failed login: Mon Oct 22 23:54:08 UTC 2018 from x.x.x.x on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Mon Oct 22 22:43:17 2018 from x.x.x.x
```

Step 2 (Optional) Run the **setproxycert** command from the CLI

```
[dnasadmin@connector ~]$ connectorctl setproxycert cert.pem
New cert exists.
Restarting connector container ...
Connector container was restarted.
setProxyCert successful.
```

Step 3 Return to the Connector GUI and click **set up HTTP Proxy**. Enter your proxy address in the dialog box displayed.

Figure 50: Setup Proxy



DNA Spaces Connector

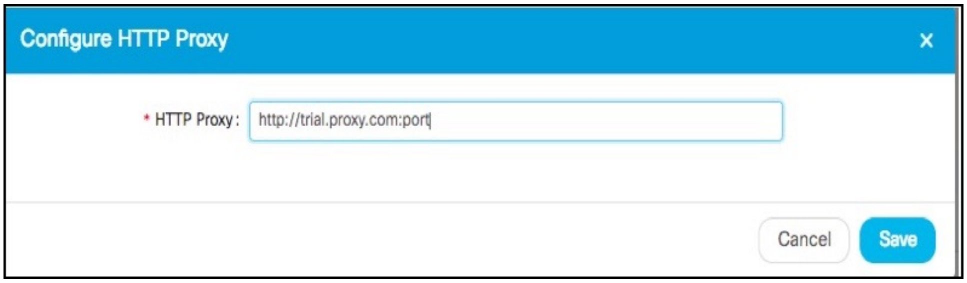
Set up HTTP Proxy

If the machine is sitting behind a proxy, Connector won't be able to interact with cloud without setting up the proxy

Privacy Settings

Setup your MAC salt and Username salt

Figure 51: Setup Proxy

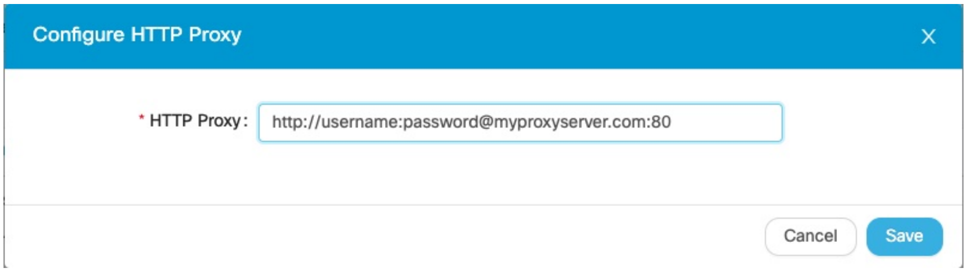


Configure HTTP Proxy

* HTTP Proxy: http://trial.proxy.com:port

You can also configure proxy including basic authentication credentials.

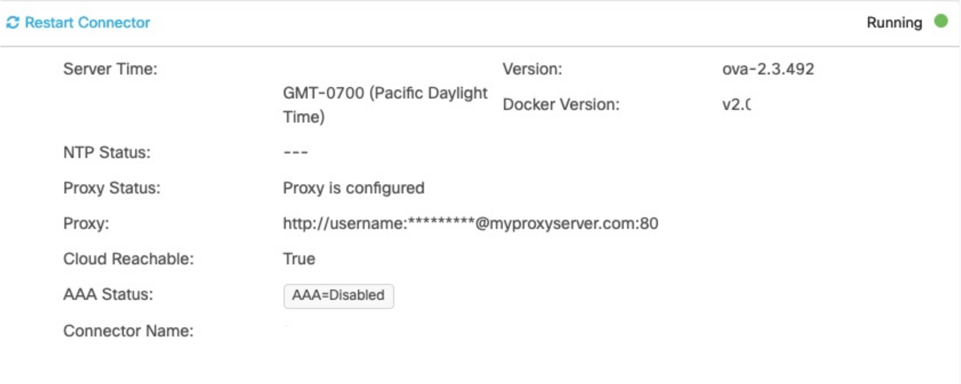
Figure 52: Configuring Proxy With Basic Authentication



Configure HTTP Proxy

* HTTP Proxy: http://username:password@myproxyserver.com:80

Figure 53: Proxy Configured With Basic Authentication



Server Time: GMT-0700 (Pacific Daylight Time)

Version: ova-2.3.492

Docker Version: v2.(

NTP Status: ---

Proxy Status: Proxy is configured

Proxy: http://username:*********@myproxyserver.com:80

Cloud Reachable: True

AAA Status: AAA=Disabled

Connector Name:

Troubleshooting Proxy Configuration

SUMMARY STEPS

1. SSH into the Connector CLI interface and ping the proxy server IP address.
2. If you are getting certificate errors such as *curl: (60) Peer's certificate issuer has been marked as not trusted by the user*, perform the following steps to add a proxy server certificate to the Connector.
3. If the previous steps do not resolve the issue, then you must include the **dnaspaces.io** domain in the allowed list for your proxy, and exclude it from HTTPS decryption (if enabled on your proxy).

DETAILED STEPS

Step 1 SSH into the Connector CLI interface and ping the proxy server IP address.

Step 2 If you are getting certificate errors such as *curl: (60) Peer's certificate issuer has been marked as not trusted by the user*, perform the following steps to add a proxy server certificate to the Connector.

a) Retrieve the certificate used by the proxy, and copy it to the Cisco Spaces: Connector.

b) Run the **connectorctl setproxycert** command and verify the output.

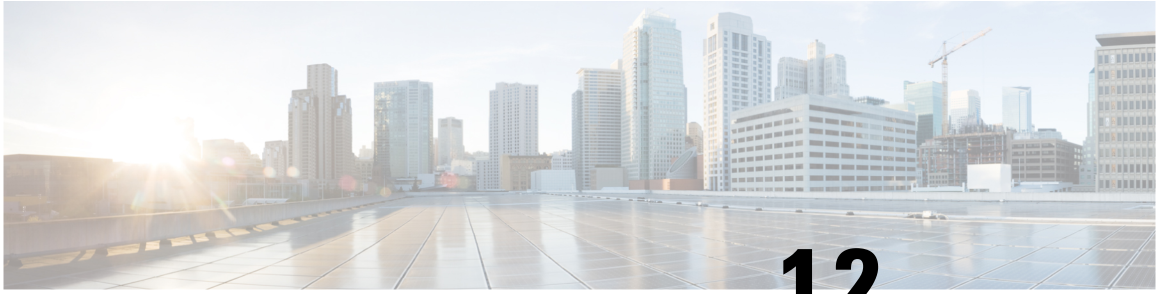
```
[spacesadmin@spacessadmin ~]$ connectorctl setproxycert squid.pem
New cert exists.
Starting connector container ...
Current version in database: latest
Container: [<Container: adlbledc71>]
Running connector version: latest
setproxycert successful.
```

Note The command may fail if you are using a transparent proxy or if you have not configured your proxy through the GUI. This command can ensure if the certificate is configured correctly.

c) Reconfigure the token on the Connector.

Step 3 If the previous steps do not resolve the issue, then you must include the **dnaspaces.io** domain in the allowed list for your proxy, and exclude it from HTTPS decryption (if enabled on your proxy).

Note Attempting to perform HTTPS decryption on the dnaspaces.io domain can interfere with or prevent the Websocket connections entirely.



CHAPTER 12

Connect Connector to Cisco AireOS Wireless Controller

- Configure and Test Connectivity Between a Connector and AireOS Controller, on page 81

Configure and Test Connectivity Between a Connector and AireOS Controller

Before you begin

- Deploy a Connector OVA and activate it using a token from Cisco Spaces.
- Ensure that the IP address of a Cisco AireOS Wireless Controller is reachable from the Cisco Spaces: Connector.

Restriction

- In the context of CSCvk38081, we recommend that you do not add Connector on the same subnet as the dynamic interface of the AireOS controller. However, if you cannot follow this recommendation, you can add the AireOS controller to Connector and configure all the SNMP queries to the IP address of the dynamic interface of the controller.
- We also recommend that you do not add Connector on the same subnet as the service port of the AireOS controller. However, if you cannot follow this recommendation, you can add the AireOS controller to Connector and configure all the SNMP queries to the IP address of the service port of the controller.
- This restriction is a result of a limitation in the AireOS controller. While SNMP queries are usually made to the management IP address, the SNMP response packets are returned with a source IP address field that is configured with the IP address of the dynamic interface or source port.

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

Note The Cisco Spaces URL is region-dependent.

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

Step 3 Expand the **Connect via Spaces Connector** area using the respective drop-down arrow to display a list of steps.

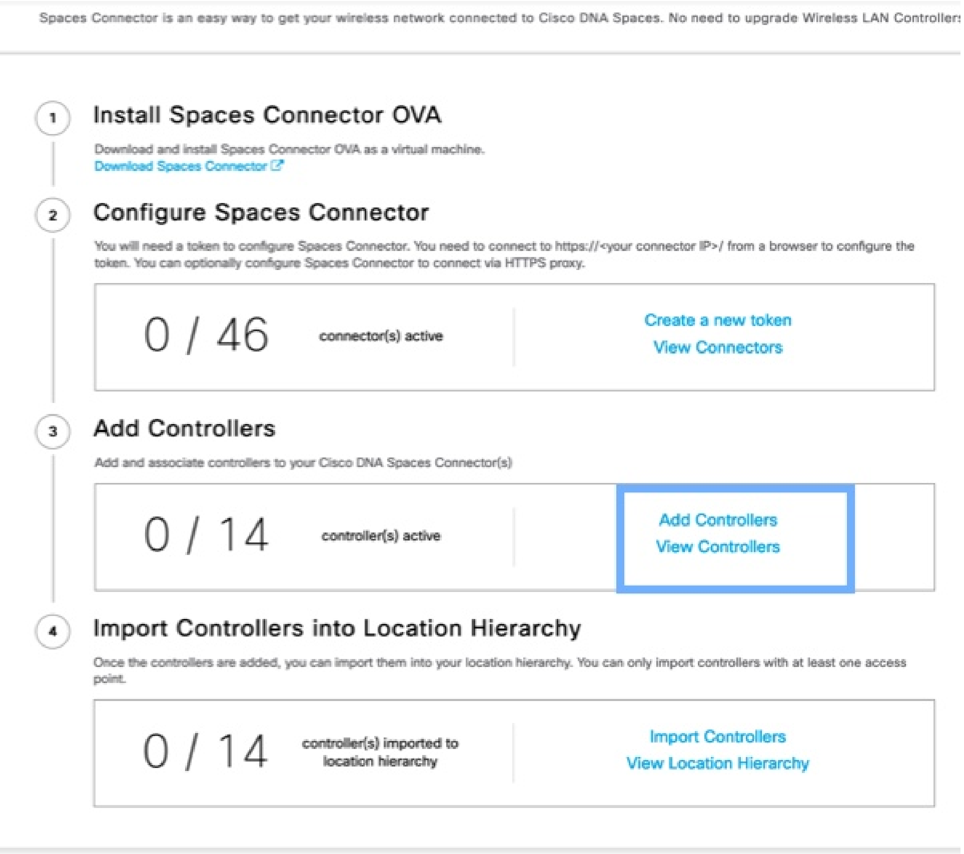
Step 4 To test the connectivity from the Connector to an existing AireOS controller, click **View Controllers** in the **Step 3** area, and do the following steps:

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

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

c) Go to Step 8 to test the connectivity to an existing AireOS controller.

Step 5 To add a new AireOS controller, click **Add Controllers** from the **Step 3** area.



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

1 Install Spaces Connector OVA

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

2 Configure Spaces Connector

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

0 / 46 connector(s) active

Create a new token
View Connectors

3 Add Controllers

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

0 / 14 controller(s) active

Add Controllers
View Controllers

4 Import Controllers into Location Hierarchy

Once the controllers are added, you can import them into your location hierarchy. You can only import controllers with at least one access point.

0 / 14 controller(s) imported to location hierarchy

Import Controllers
View Location Hierarchy

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

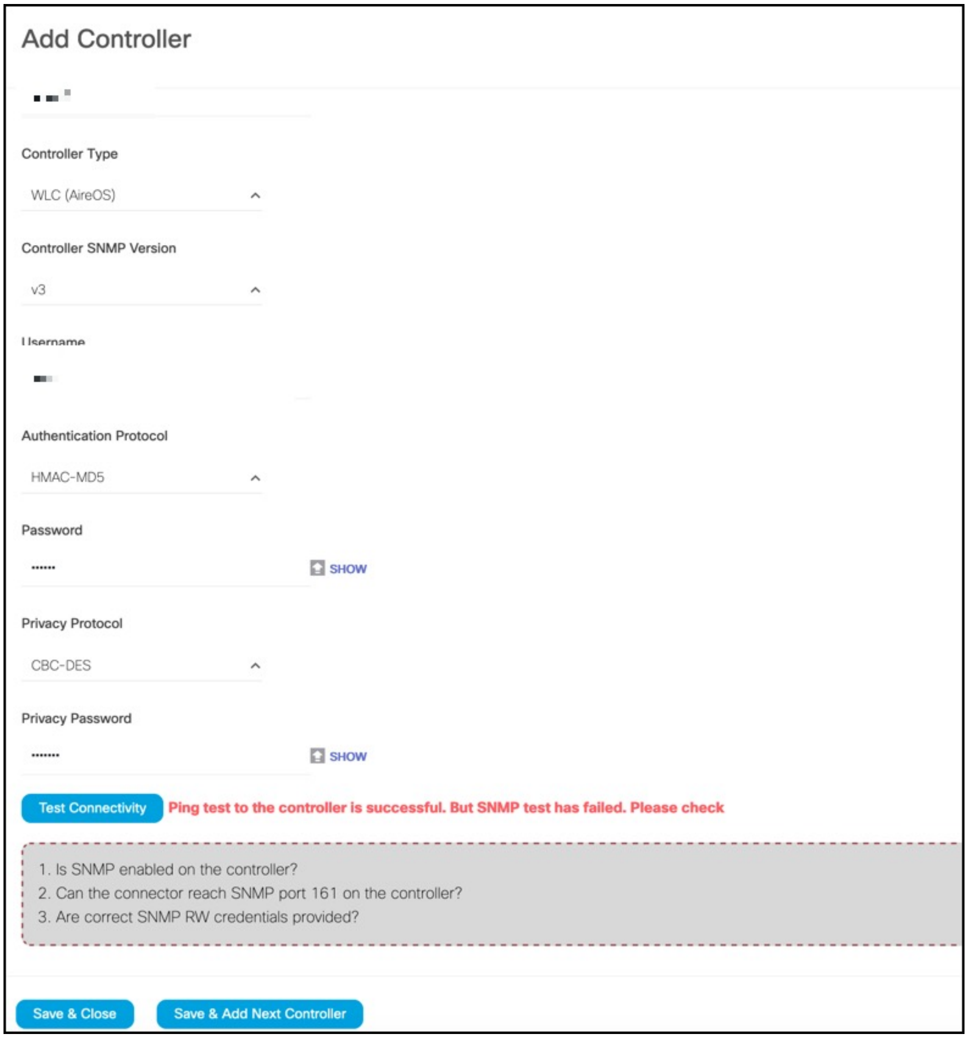
Step 7 Enter the **Controller IP** address and **Controller Name**, and from the **Controller Type** drop-down list, choose **WLC (AireOS)** to connect to an AireOS controller.

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

- If you choose the **SNMP** version as **v2C**, specify the SNMP read-write community.
- If you choose the **SNMP** version as **v3**, specify the SNMP v3 version username, password, and authentication protocol credentials. Ensure that SNMP v3 has read-write permissions in the AireOS controller.

Note Both SNMP v2c and SNMP v3 must have read-write permission in the AireOS controller to register the Connector certificate in the AireOS controller. The Connector doesn't support SNMP v1.

Add a Cisco AireOS Wireless Controller (AireOS controller)



Add Controller

[redacted]

Controller Type

WLC (AireOS)

Controller SNMP Version

v3

Username

[redacted]

Authentication Protocol

HMAC-MD5

Password

•••••• SHOW

Privacy Protocol

CBC-DES

Privacy Password

••••••• SHOW

Test Connectivity Ping test to the controller is successful. But SNMP test has failed. Please check

1. Is SNMP enabled on the controller?
2. Can the connector reach SNMP port 161 on the controller?
3. Are correct SNMP RW credentials provided?

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.

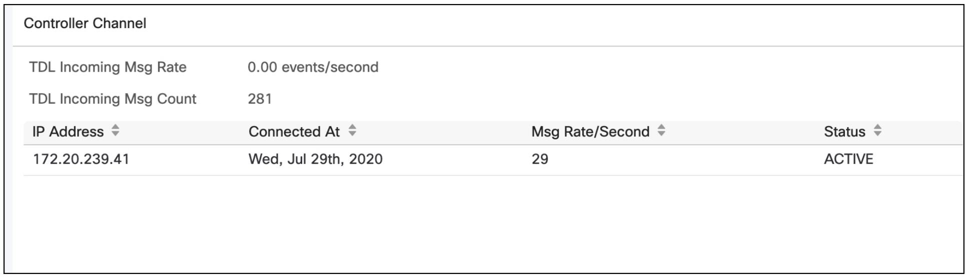
Table 7: Error Description

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

Status of PING	Status of SNMP Test	Displayed Test Connectivity Message
SUCCESSFUL	FAILED	Ping test is successful, but SNMP test failed. Check the following: Ping test to the AireOS controller is successful, but SNMP test has failed. Check the following: • If you are using v2c SNMP, check if the community strings are valid. • If you are using v3 SNMP, check if the credentials are correct. • Check if v2c or v3 mode is enabled in the controller.
FAILED	FAILED	Both ping and SSH test to the AireOS controller have failed. Check the following: • Is there IP connectivity between a Connector and a controller? • Is SSH enabled on the AireOS controller? • Is the SSH port 22 of the AireOS controller reachable from the Connector? • Have you provided accurate SSH credentials? • Is AAA enabled with local authentication? • Are you using an interface that is *not* the wireless management interface for NMSP and SSH connectivity?

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

You can see the new Catalyst 9800 controller in the **Controller Channel** area of the Connector GUI. The Catalyst 9800 controller that is connected successfully to the Connector appears as **Active**. It takes approximately five minutes for the 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.



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.

CHAPTER 13

Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers

- Configure and Test the Connection Between Connector and Catalyst 9800 Controller, on page 87

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.

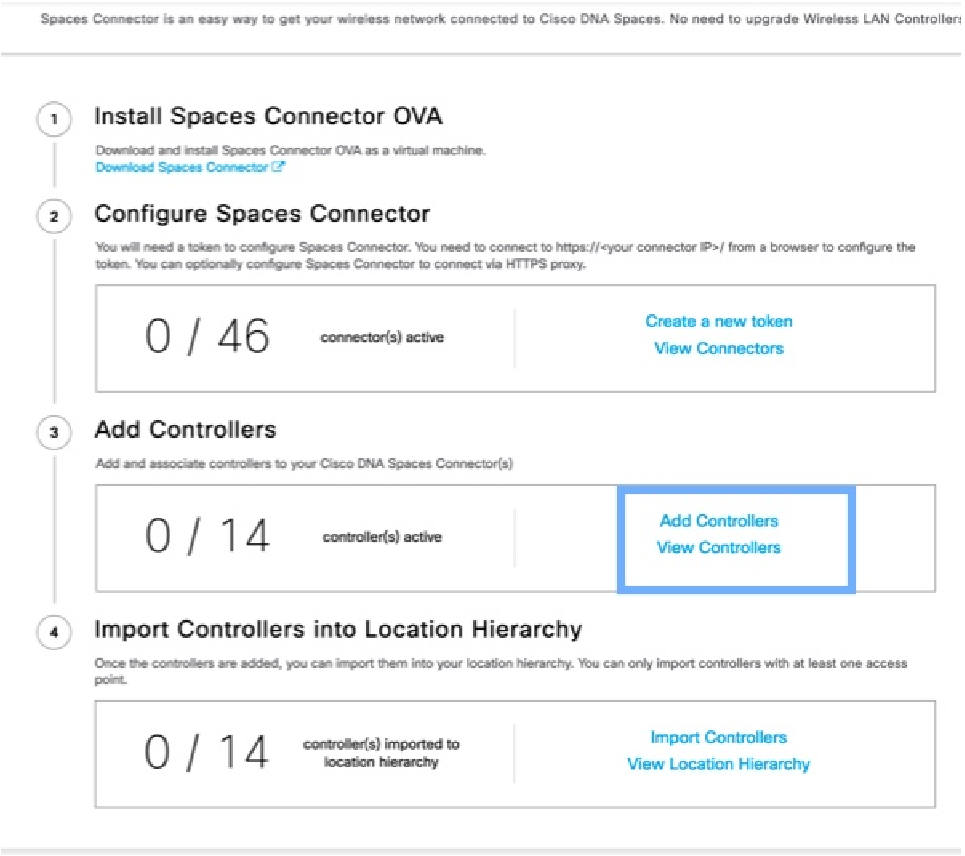
Step 4 To test the connectivity from the Connector to an existing Catalyst 9800 controller, click **View Controllers** in the **Step 3** Area.

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

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

c) Go to Step 8 to test the connectivity to an existing AireOS controller.

Step 5 To add a new Catalyst 9800 controller, click **Add Controllers** from the **Step 3** Area.



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

1 Install Spaces Connector OVA

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

2 Configure Spaces Connector

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

0 / 46 connector(s) active

Create a new token
View Connectors

3 Add Controllers

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

0 / 14 controller(s) active

Add Controllers
View Controllers

4 Import Controllers into Location Hierarchy

Once the controllers are added, you can import them into your location hierarchy. You can only import controllers with at least one access point.

0 / 14 controller(s) imported to location hierarchy

Import Controllers
View Location Hierarchy

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

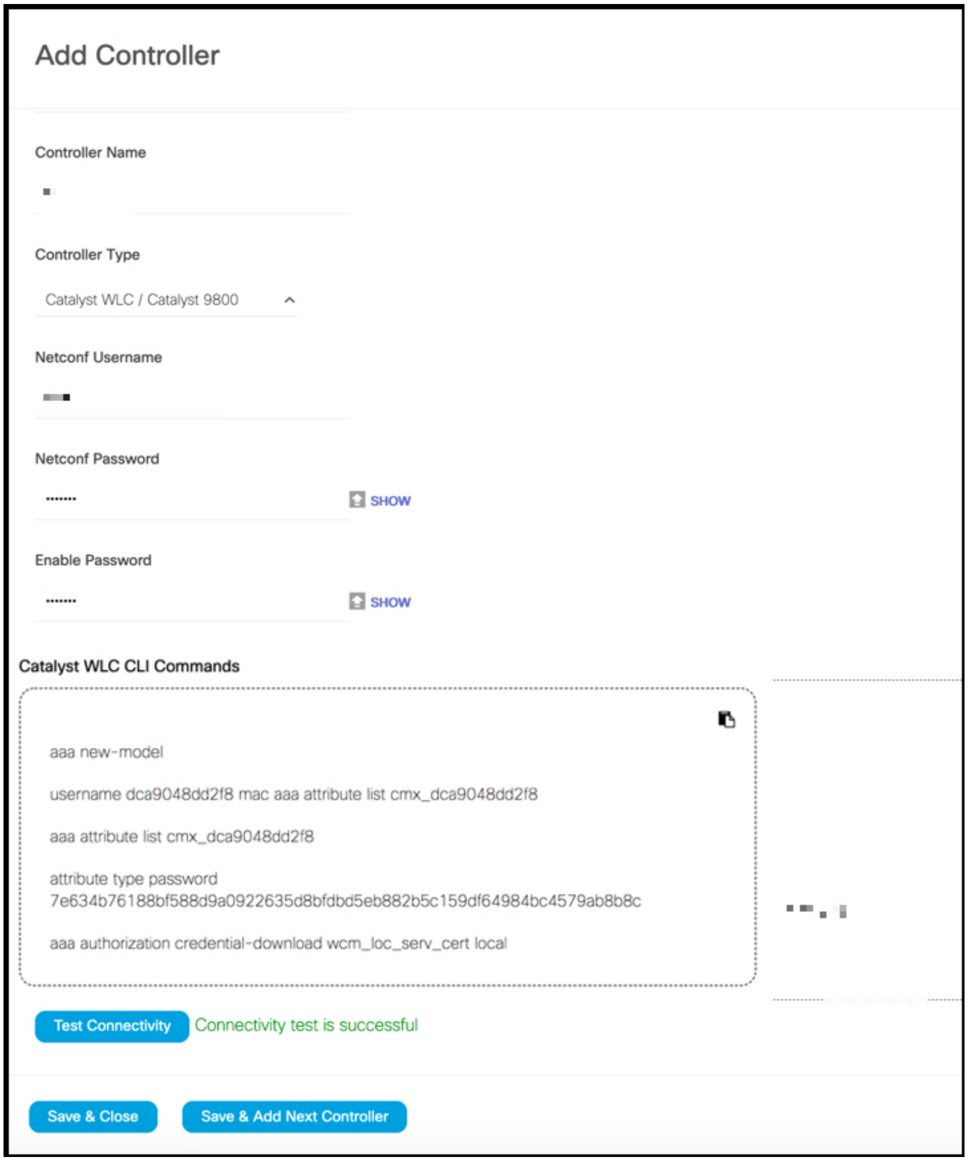
Step 7 Enter the **Controller IP** address, **Controller Name**, and from the **Controller Type** drop-down list, choose **Catalyst WLC** to connect to a Cisco Catalyst 9800 Series Wireless Controllers.

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 54: Adding a Catalyst 9800 Controller



Add Controller

Controller Name

[redacted]

Controller Type

Catalyst WLC / Catalyst 9800

Netconf Username

[redacted]

Netconf Password

•••••••

Enable Password

•••••••

Catalyst WLC CLI Commands

```
aaa new-model

username dca9048dd2f8 mac aaa attribute list cmx_dca9048dd2f8

aaa attribute list cmx_dca9048dd2f8

attribute type password
7e634b76188bf588d9a0922635d8bfdbd5eb882b5c159df64984bc4579ab8b8c

aaa authorization credential-download wcm_loc_serv_cert local
```

Connectivity test is successful

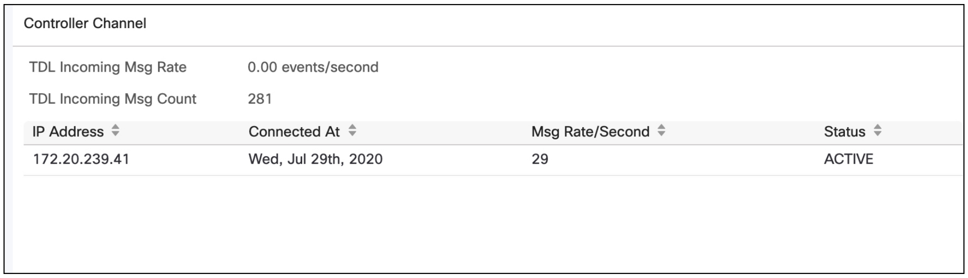
Table 8: Error Description

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 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.



Controller Channel

TDL Incoming Msg Rate 0.00 events/second

TDL Incoming Msg Count 281

IP Address	Connected At	Msg Rate/Second	Status
172.20.239.41	Wed, Jul 29th, 2020	29	ACTIVE

You can multiple Catalyst 9800 controllers to a Connector.

What to do next

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

CHAPTER 14

Connecting a Connector to Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches Series

- Connecting a Connector to Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches , on page 93

Connecting a Connector to Cisco Catalyst 9300 Series Switches and Cisco Catalyst 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 Series Switches and Cisco Catalyst 9400 Series Switches that is reachable from the Cisco Spaces: Connector.
- Test the Netconf commands on the Cisco Catalyst 9300 Series Switches and Cisco Catalyst 9400 Series Switches

SUMMARY STEPS

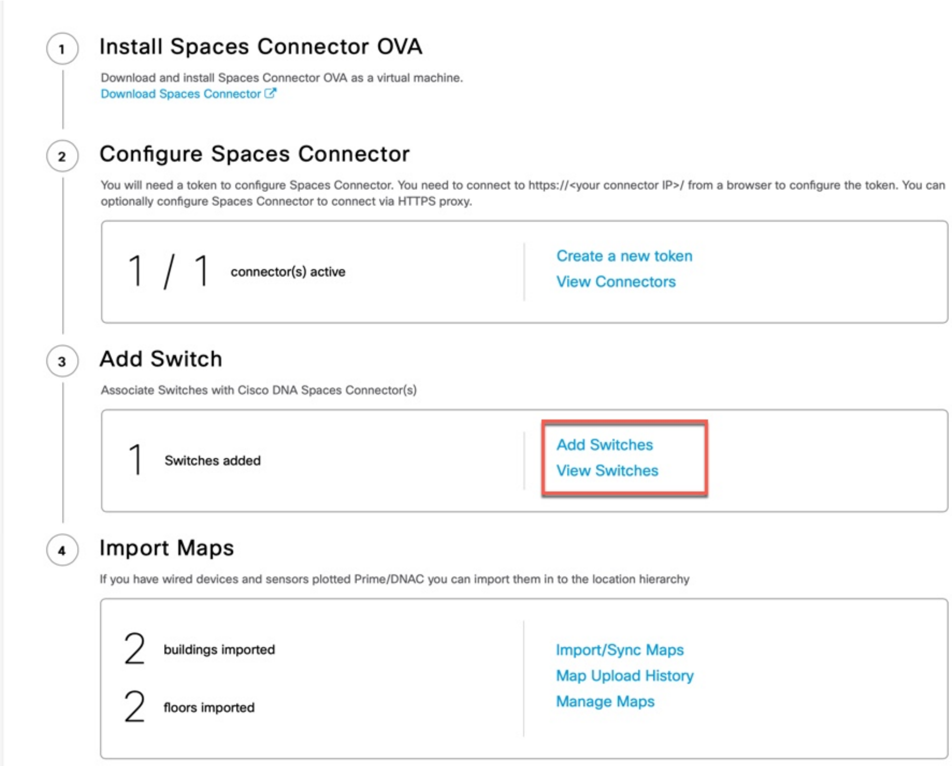
1. Log in to Cisco Spaces.
2. In the Cisco Spaces dashboard, choose **Setup** > **Wired Networks**.
3. From the **Step 3: Add Switches** area, click **Add Switch**.
4. From the **Add Switches** page, select the Connector, enter a name to identify the switch, the switch IP address. **Netconf username**, **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**.



1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.

Download Spaces Connector

2 Configure Spaces Connector

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

1 / 1 connector(s) active

Create a new token

View Connectors

3 Add Switch

Associate Switches with Cisco DNA Spaces Connector(s)

1 Switches added

Add Switches

View Switches

4 Import Maps

If you have wired devices and sensors plotted Prime/DNAC you can import them in to the location hierarchy

2 buildings imported

2 floors imported

Import/Sync Maps

Map Upload History

Manage Maps

Figure 55:

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:

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

PART IV

Location Hierarchy

- Location Hierarchy, on page 97

CHAPTER 15

Location Hierarchy

- Importing a Cisco AireOS Wireless Controller to the Cisco Spaces Location Hierarchy, on page 97

Importing a Cisco AireOS Wireless Controller to the Cisco Spaces Location Hierarchy

This task is not applicable if you want to use map services for importing the locations to Cisco Spaces. See Importing Locations to the Location Hierarchy Using Map Services in the *Cisco Spaces 2,0 configuration guide*. For X/Y location calculations, you need to use map services and download maps.

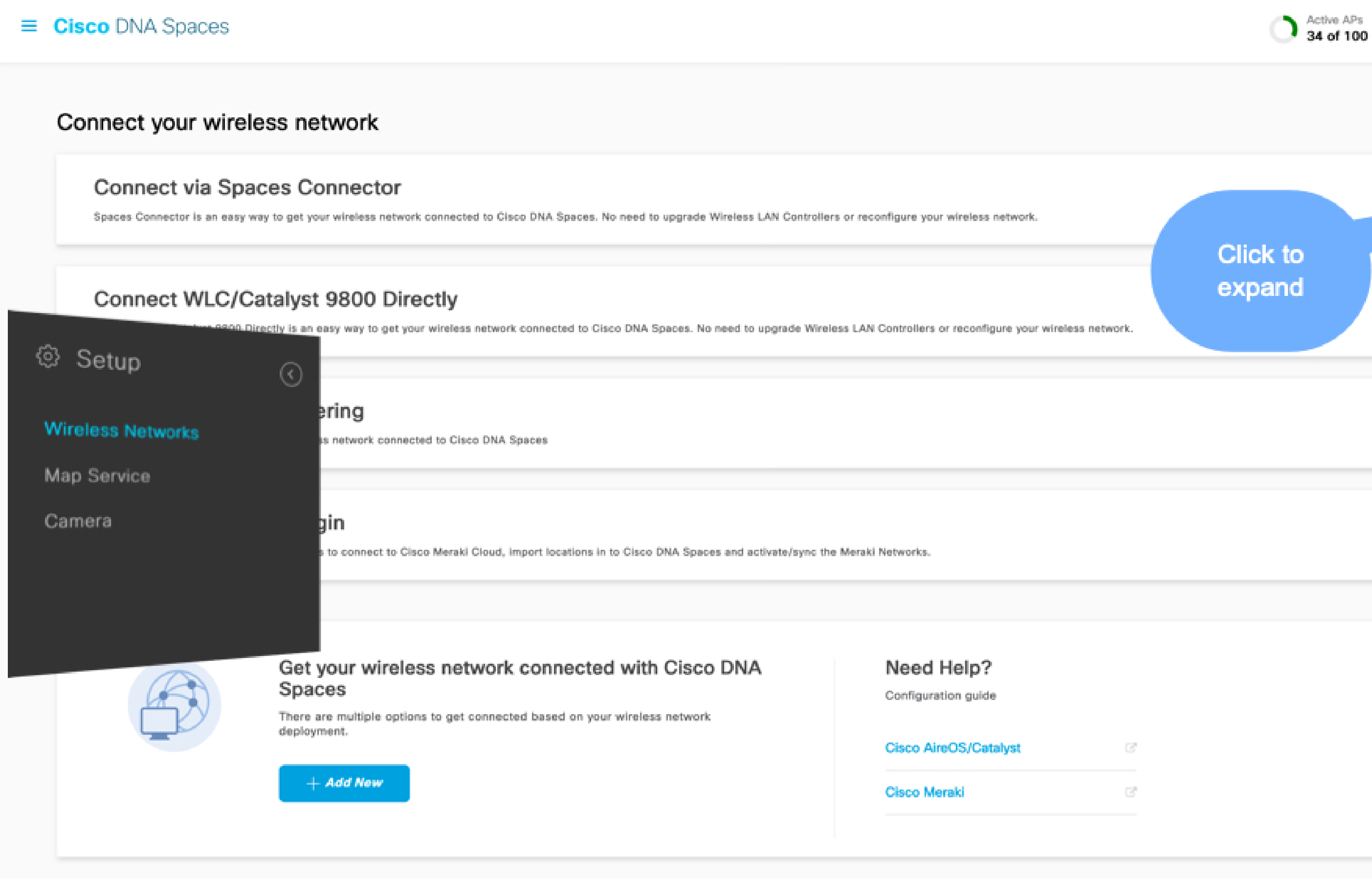
Before you begin

- Connect the Cisco AireOS Wireless Controller to the Cisco Spaces: Connector. See #unique_29
- Ensure that at least one access point connects to your Cisco AireOS Wireless Controller.

Step 1 Log in to Cisco Spaces.

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

Step 3 Expand the **Connect via Spaces Connector** area using the respective drop-down arrow.



Connect your wireless network

Connect via Spaces Connector

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

Connect WLC/Catalyst 9800 Directly

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

ering

s network connected to Cisco DNA Spaces

gin

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

Get your wireless network connected with Cisco DNA Spaces

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

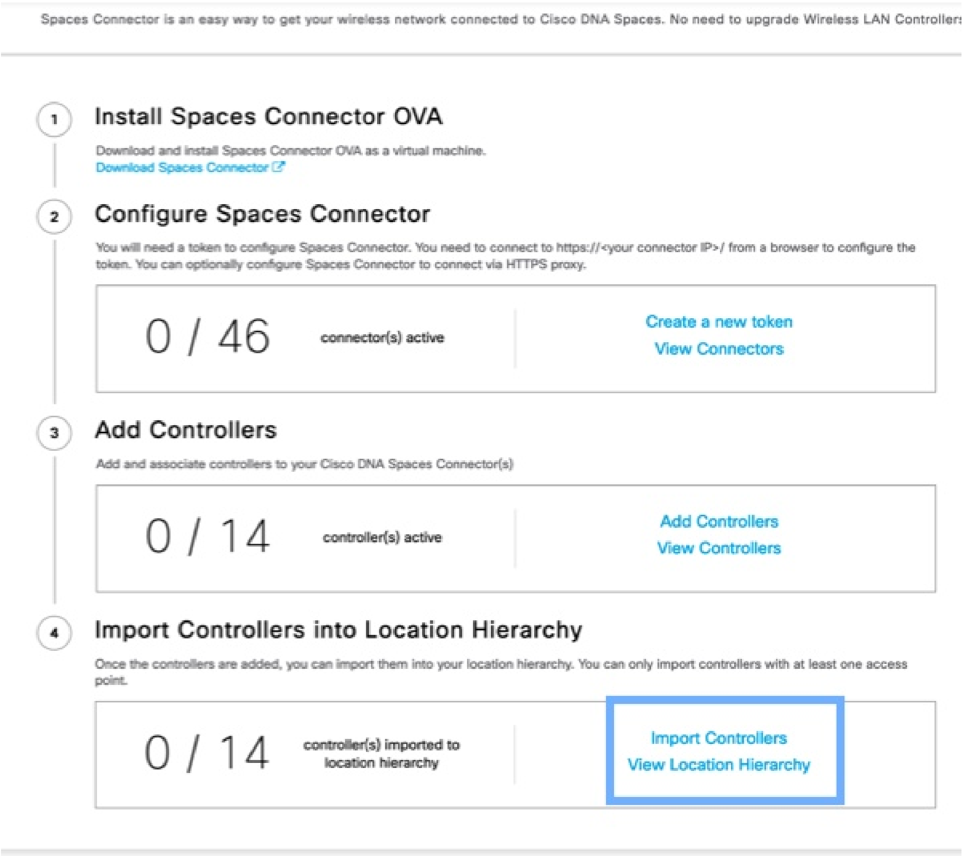
Need Help?

Configuration guide

Cisco AireOS/Catalyst

Cisco Meraki

Step 4 In the displayed list of steps, click **Import Controller** listed as the fourth step.



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

1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.

2 Configure Spaces Connector

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

0 / 46 connector(s) active

3 Add Controllers

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

0 / 14 controller(s) active

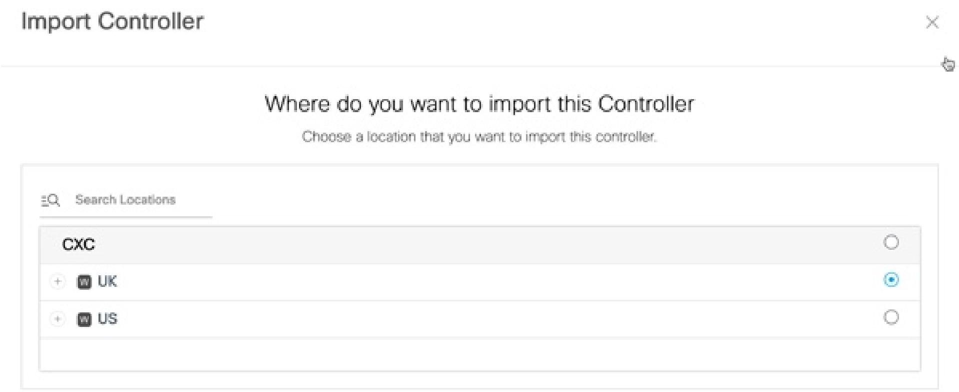
4 Import Controllers into Location Hierarchy

Once the controllers are added, you can import them into your location hierarchy. You can only import controllers with at least one access point.

0 / 14 controller(s) imported to location hierarchy

You can see a list of locations and previously added controllers.

Step 5 Choose a location where you want to import the controller to.

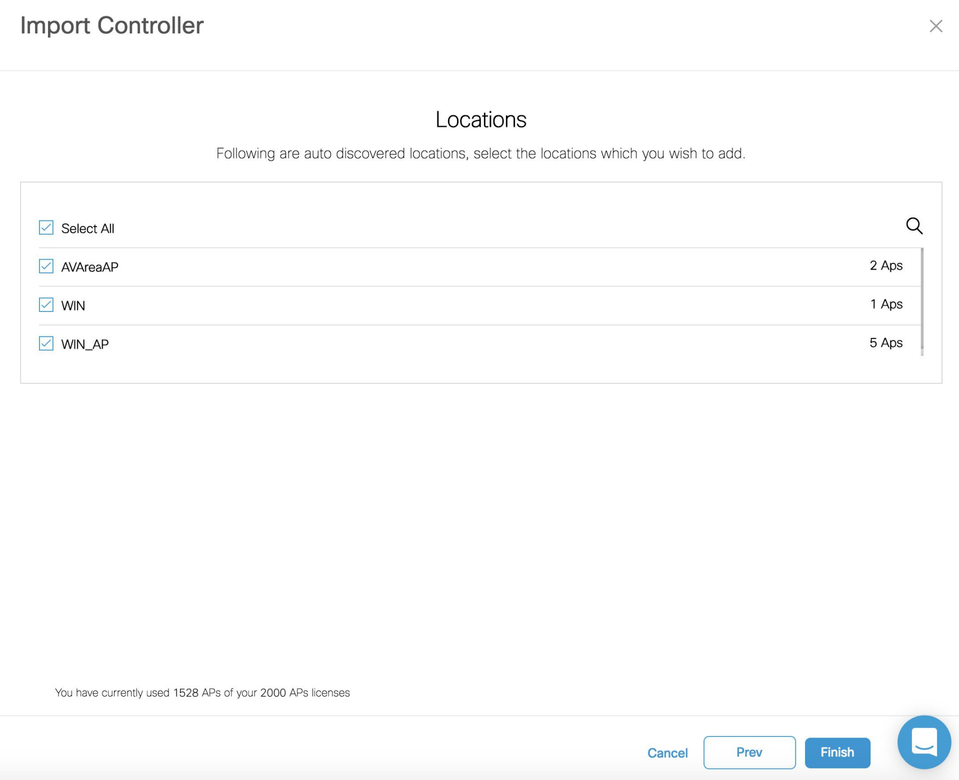


Import Controller

Where do you want to import this Controller

Choose a location that you want to import this controller.

If the APs of the controllers are grouped as networks based on the naming convention, those network names appear. If you want to maintain the same grouping, select the networks. If the APs are not grouped, network names are not displayed.



Import Controller

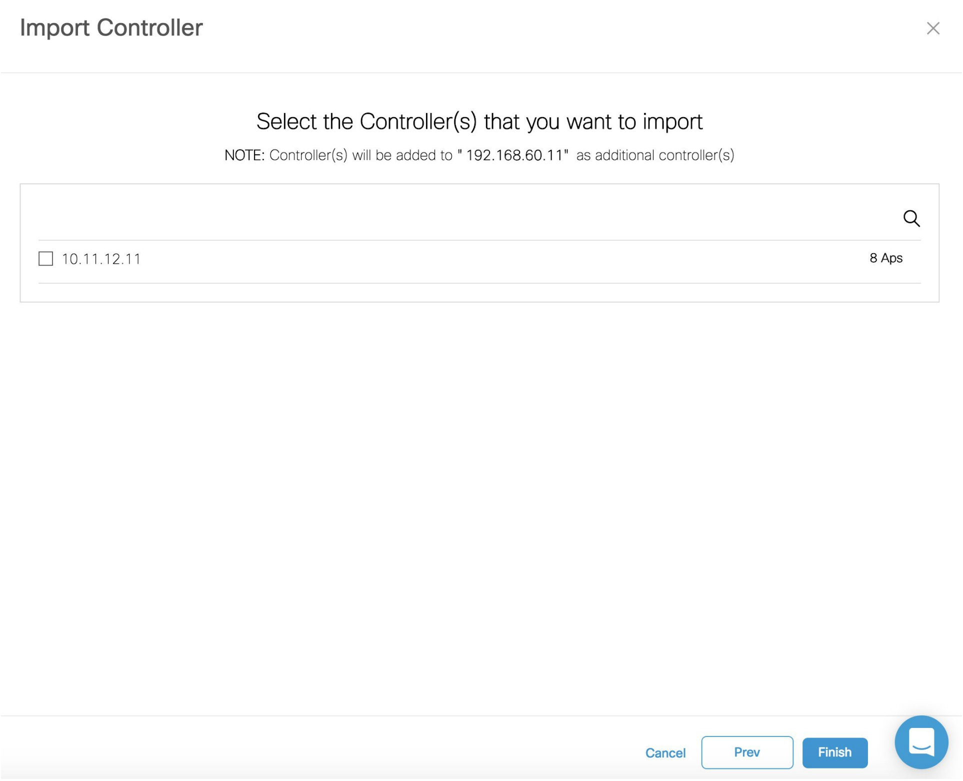
Locations

Following are auto discovered locations, select the locations which you wish to add.

☑ Select All	
☑ AVAreaAP	2 Aps
☑ WIN	1 Aps
☑ WIN_AP	5 Aps

You have currently used 1528 APs of your 2000 APs licenses

Step 6 Choose a controller to import.


Import Controller

Select the Controller(s) that you want to import

NOTE: Controller(s) will be added to " 192.168.60.11" as additional controller(s)

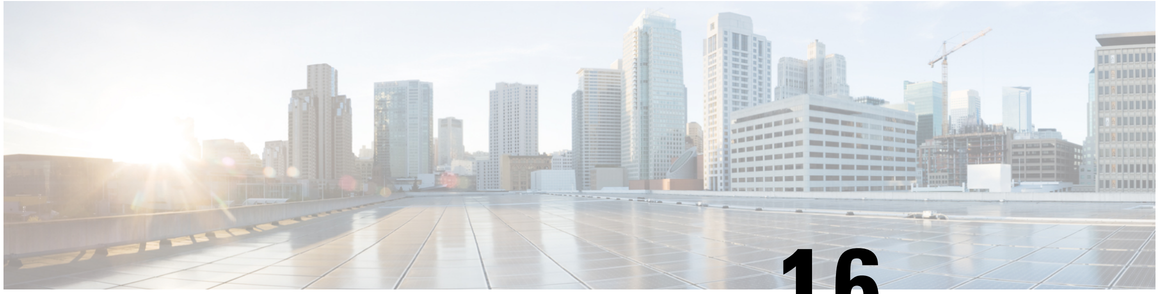
□ 10.11.12.11 8 Aps

Step 7 Click **Next** and **Finish**.

PART V

Privacy Setting

- Configure Privacy Settings, on page 105



CHAPTER 16

Configure Privacy Settings

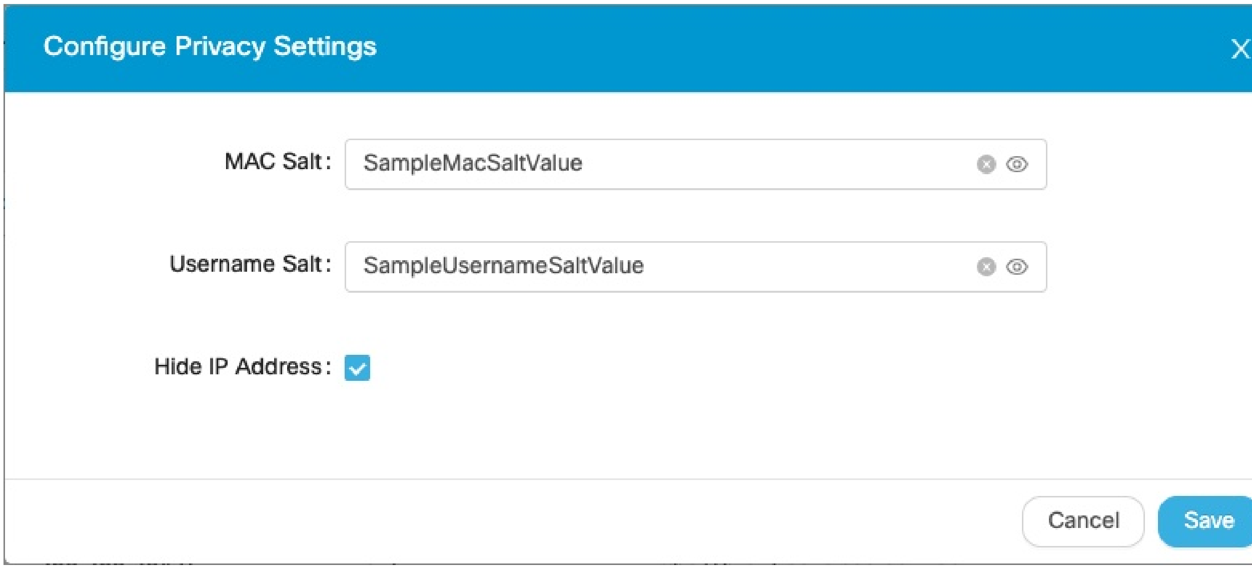
- Configuring Privacy Settings: MAC and Username Salt , on page 105

Configuring Privacy Settings: MAC and Username Salt

Cisco Spaces: 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. From Cisco Spaces: Connector Release 2.3.2, you can mask IP addresses.

Note This task is optional.

You can configure the MAC Salt and username SALT using the Cisco Spaces: Connector GUI **Privacy settings**.



Configure Privacy Settings

MAC Salt: SampleMacSaltValue

Username Salt: SampleUsernameSaltValue

Hide IP Address: ☑

PART VI

HotSpot (OpenRoaming)

- Hotspot (OpenRoaming), on page 109

CHAPTER 17

Hotspot (OpenRoaming)

- HotSpot (OpenRoaming), on page 109

HotSpot (OpenRoaming)

The Cisco Spaces: Connector now supports the OpenRoaming protocol.

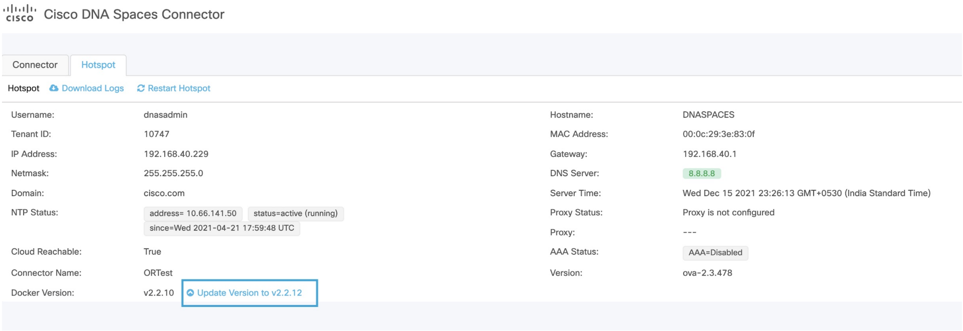
OpenRoaming provides mobile users with hassle-free, friction-less, guest WiFi on-boarding experience by linking together Access Providers (such as: public venues, retailers, airports, and large enterprises) with Identity Providers (such as: service provider carriers, devices, and cloud providers).

OpenRoaming enables users to get connected online automatically and seamlessly after signing in just once using a trusted identity provider. The service is completely secure and fast.

Refer to the Open Roaming configuration on Cisco Wireless Controller and Cisco Spaces Setup Guide for detailed steps on configuring OpenRoaming.

Once OpenRoaming is configured, the **Hotspot** tab appears on Connector.

Figure 56: Hotspot Tab



Username:	dnasadmin	Hostname:	DNASPACES
Tenant ID:	10747	MAC Address:	00:0c:29:3e:83:0f
IP Address:	192.168.40.229	Gateway:	192.168.40.1
Netmask:	255.255.255.0	DNS Server:	8.8.8.8
Domain:	cisco.com	Server Time:	Wed Dec 15 2021 23:26:13 GMT+0530 (India Standard Time)

NTP Status:	address= 10.66.141.50
	status=active (running)
	since=Wed 2021-04-21 17:59:48 UTC
		Proxy Status:	Proxy is not configured

		Proxy:	---
Cloud Reachable:	True	AAA Status:	AAA=Disabled
Connector Name:	ORTest	Version:	ova-2.3.478
Docker Version:	v2.2.10		

Upgrade the OpenRoaming Docker

You can upgrade the OpenRoaming docker to the latest version from the **Hotspot** tab. Note that the upgrade link appears only if a new upgrade image is available.

PART VII

AAA

- Configure AAA, on page 113

CHAPTER 18

Configure AAA

- Configure AAA, on page 113

Configure AAA

Information About AAA

You can now forward Cisco Spaces: Connector authentications to a remote Authentication, Authorization, and Accounting (AAA) server (and bypass local authentication). You can use the command line to configure AAA. AAA-authenticated users can access the Connector Web UI with the same access rights as the **dnasadmin** user. Once you activate AAA on the Connector, you can no longer use the **dnasadmin** user to log in to the Connector.

Note You can use the **dnasadmin** user to access the Web UI in the following scenarios:

- If you have configured AAA incorrectly.
- If you are unable to reach the AAA server.

Note With CSCvt29826, AAA with IPSec is not compatible with a certificate is generated on a Connector of key type Elliptic Curve Digital Signature Algorithm (ECDSA) that is generated with the **connectorctl generatecert** command.

The communication between Connector and the AAA server is through Remote Authentication Dial-In User Service (RADIUS).

You can choose to encrypt the UDP traffic using the IPSec Protocol. The supported IPSec authentication types are **pubkey** and **PSK**.

For the pubkey authentication type, provide a CA certificate file of AAA Server (PEM format).

For the PSK authentication type, choose to autogenerate the PSK or provide PSK configured in AAA server.

Configure AAA

Before you begin

- To enable IP Security using Pubkey authentication type, copy the CA Certificate of the AAA server to the directory location `/home/dnasadmin` and rename the certificate as **radiusca.pem**.

SUMMARY STEPS

1. **connectorctl aaa enable**
2. **connectorctl aaa edit**
3. On the Connector Web UI, check the AAA status in the **AAA Status** field

DETAILED STEPS

Step 1 **connectorctl aaa enable**

Example:

```
[cmxadmin@cmxnew-01 ~]$ connectorctl aaa enable
Do you want to configure AAA Server? [yes/no] [yes]:
Enter AAA Server Host IP : 10.22.244.114
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [n]:

AAA Server configured successfully
Connection to AAA Server Successful. AAA Settings are correct.
[cmxadmin@cmxnew-01 ~]$
```

Enable AAA.

Step 2 **connectorctl aaa edit**

Example:

This example configures AAA with IP Security with Pubkey Authentication type.

Example:

```
[cmxadmin@cmxnew-01 ~]$ connectorctl aaa edit
Do you want to CHANGE AAA Server settings? [yes/no] [yes]:
Enter AAA Server Host IP  [10.22.244.114]:
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [n]: y
Enter AAA Server's DNS name : aaa-srv-01
Select IPSec Auth Type: (pubkey/psk) [pubkey]:
AAA Server's CA Certificate file : radiusca.pem

AAA Server configured successfully
Connection to AAA Server Successful. AAA Settings are correct.
IPSec is Enabled
IPSec Status:
Security Associations (1 up, 0 connecting):
         aaa[1]: ESTABLISHED 0 seconds ago, 10.22.244.100[cmxnew-01]...10.22.244.114[aaa-srv-01]
         aaa{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c6c620cb_i c06dcc78_o
         aaa{1}:   10.22.244.100/32 === 10.22.244.114/32
```

Example:

This example configures AAA with IP Security with PSK Authentication type, providing the PSK value from the RADIUS server.

```
[cmxadmin@cmxnew-01 ~]$ connectorctl aaa edit
Do you want to CHANGE AAA Server settings? [yes/no] [yes]:
Enter AAA Server Host IP  [10.22.244.114]:
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [y]:
Enter AAA Server's DNS name  [aaa-srv-01]:
Select IPSec Auth Type: (pubkey/psk) [pubkey]: psk
Do you want to auto-generate ('a') OR provide ('p') PSK from Radius Server ? [a]: p
Enter PSK from Radius Server : 7dBoZXAkhadFMsyJ8e9HsBxdajnUPcxS

AAA Server configured successfully
Connection to AAA Server Successful. AAA Settings are correct.
IPSec is Enabled
IPSec Status:
Security Associations (1 up, 0 connecting):
         aaa[1]: ESTABLISHED 1 second ago, 10.22.244.100[cmxnew-01]...10.22.244.114[aaa-srv-01]
         aaa{1}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c59d3960_i cf338432_o
         aaa{1}:   10.22.244.100/32 === 10.22.244.114/32
         aaa{2}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c75d414b_i c7e495e2_o
         aaa{2}:   10.22.244.100/32 === 10.22.244.114/32
```

Example:

This example configures AAA with IP Security with PSK Authentication type and autogenerating a new PSK value.

```
[cmxadmin@connector-01 ~]$ connectorctl aaa edit
[cmxadmin@connector-01 ~]$ connectorctl aaa edit
Do you want to CHANGE AAA Server settings? [yes/no] [yes]:
Enter AAA Server Host IP  [10.22.244.114]:
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [y]:
Enter AAA Server's DNS name  [aaa-srv-01]:
Select IPSec Auth Type: (pubkey/psk) [psk]:
Do you want to auto-generate ('a') OR provide ('p') PSK from Radius Server ? [a]: a
Generated PSK value = 3AhBgueQQ6YBkKMwqIr6jyxIuG9ekw8g

AAA Server configured successfully
Connection to AAA Server Successful. AAA Settings are correct.
IPSec is Enabled
IPSec Status:
Security Associations (0 up, 0 connecting):
  no match
```

The IP Security status indicates zero security associations indicating that the IP Security tunnel isn't yet established successfully. You can verify the same a few seconds later using the **connectorctl aaa show** command and comparing the PSK values.

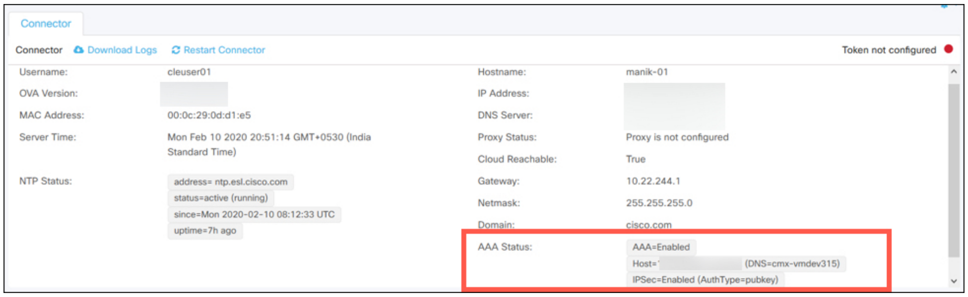
```
[cmxadmin@connector-01 ~]$ connectorctl aaa show
AAA Server is Enabled
AAA Server IP: 10.22.244.114
AAA Server Port: 1812
Shared Secret: **<<masked>>**
```

```
IPSec is Enabled
AAA Server DNS: aaa-srv-01
IPSec Auth type: psk
IPSec PSK: 3AhBgueQQ6YBkKMwqIr6jyxIuG9ekw8g
IPSec Status:
Security Associations (1 up, 0 connecting):
        aaa[3]: ESTABLISHED 20 seconds ago, 10.22.244.100[connector-01]...10.22.244.114[aaa-srv-01]

         aaa{3}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: ca4688d1_i c24be7d9_o
         aaa{3}:   10.22.244.100/32 === 10.22.244.114/32
Connection to AAA Server Successful. AAA Settings are correct.
```

Edit an existing AAA configuration.

Step 3 On the Connector Web UI, check the AAA status in the **AAA Status** field

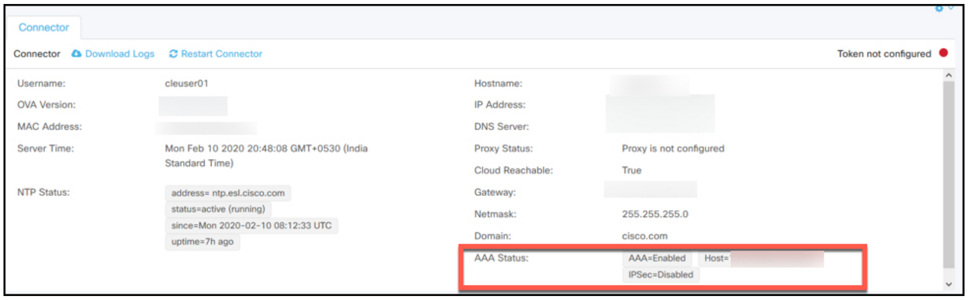
Figure 57: AAA Enabled with IP Security and PubKey



Username: cleuser01
OVA Version: [redacted]
MAC Address: 00:0c:29:0d:d1:e5
Server Time: Mon Feb 10 2020 20:51:14 GMT+0530 (India Standard Time)
NTP Status: address= ntp.esl.cisco.com
status=active (running)
since=Mon 2020-02-10 08:12:33 UTC
uptime=7h ago

Hostname: manik-01
IP Address: [redacted]
DNS Server:
Proxy Status: Proxy is not configured
Cloud Reachable: True
Gateway: 10.22.244.1
Netmask: 255.255.255.0
Domain: cisco.com
AAA Status: AAA=Enabled
Host=[redacted] (DNS=cmx-vmdev315)
IPSec=Enabled (AuthType=pubkey)

Figure 58: AAA Enabled without IP Security



Username: cleuser01
OVA Version: [redacted]
MAC Address: [redacted]
Server Time: Mon Feb 10 2020 20:48:08 GMT+0530 (India Standard Time)
NTP Status: address= ntp.esl.cisco.com
status=active (running)
since=Mon 2020-02-10 08:12:33 UTC
uptime=7h ago

Hostname: [redacted]
IP Address: [redacted]
DNS Server:
Proxy Status: Proxy is not configured
Cloud Reachable: True
Gateway: [redacted]
Netmask: 255.255.255.0
Domain: cisco.com
AAA Status: AAA=Enabled Host=[redacted]
IPSec=Disabled

AAA is enabled.

What to do next

You can disable AAA using the **connectorctl aaa disable** command. If you have IPSec enabled , you can choose to restart the IPSec tunnel using the **connectorctl aaa restart** command, if necessary

PART VIII

Connectors in Active-Active

- Connectors in Active-Active, on page 119

CHAPTER 19

Connectors in Active-Active

- Connector Active-Active, on page 119
- Restrictions, on page 119
- Connector Active-Active vs Cisco CMX High Availability, on page 121
- Configuring Connectors in Active-Active, on page 121
- Configuring Connectors in Active-Active (Wired), on page 124

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 retrieve a token from Cisco Spaces and configure the token on two different Connectors. Each Connector 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.

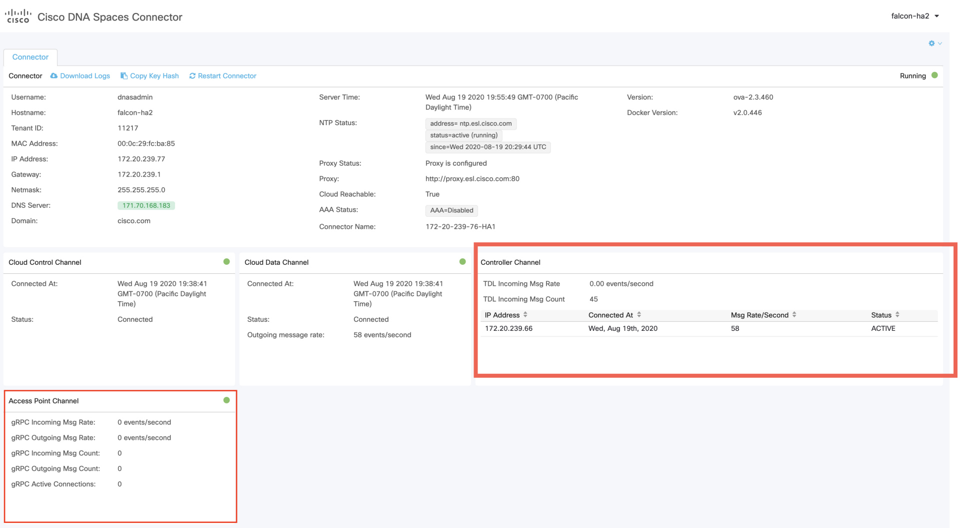
Restrictions

- On the Cisco Spaces dashboard, there is no configuration required for two Connectors to be an active-active pair.
- Both Connectors connect to all Controllers and send traffic to Cisco Spaces. The traffic from Controllers to Cisco Spaces hence increases.
- To be an active-active Connector pair, two Connectors must run OVA version 2.3 or higher.
- There is no failover support for Hyperlocation, and IoT Service. Reprovision these services after a failover.

Note FastLocate is re-established after failover with a delay of three to four minutes.

- With CSCvv38762, there is no failover support for IoT Service. Reprovision these services after a failover.
- There is no support for monitoring the Connector active-active feature.
- With CSCvv34216, a Connector active-active pair has only one Connector managing the **Controller Channel** and the other Connector managing the **AP Channel**.

Figure 59: Connector managing Controller Channel only. AP Channel statistics is zero.



Cisco DNA Spaces Connector

falcon-ha2

Connector

Connector | Download Logs | Copy Key Hash | Restart Connector | Running ●

Username:	dnasadmin
Hostname:	falcon-ha2
Tenant ID:	11217
MAC Address:	00:0c:29:fc:ba:85
IP Address:	172.20.239.77
Gateway:	172.20.239.1
Netmask:	255.255.255.0
DNS Server:	171.70.168.183
Domain:	cisco.com

Server Time:	Wed Aug 19 2020 19:55:49 GMT-0700 (Pacific Daylight Time)

NTP Status:	address= ntp.esl.cisco.com
	status=active (running)
	since=Wed 2020-08-19 20:29:44 UTC

Proxy Status:	Proxy is configured
Proxy:	http://proxy.esl.cisco.com:80
Cloud Reachable:	True
AAA Status:	AAA=Disabled
Connector Name:	172-20-239-76-HA1

Version:	ova-2.3.460
Docker Version:	v2.0.446

Cloud Control Channel ●

Connected At:	Wed Aug 19 2020 19:38:41 GMT-0700 (Pacific Daylight Time)
Status:	Connected

Cloud Data Channel ●

Connected At:	Wed Aug 19 2020 19:38:41 GMT-0700 (Pacific Daylight Time)
Status:	Connected
Outgoing message rate:	58 events/second

Controller Channel

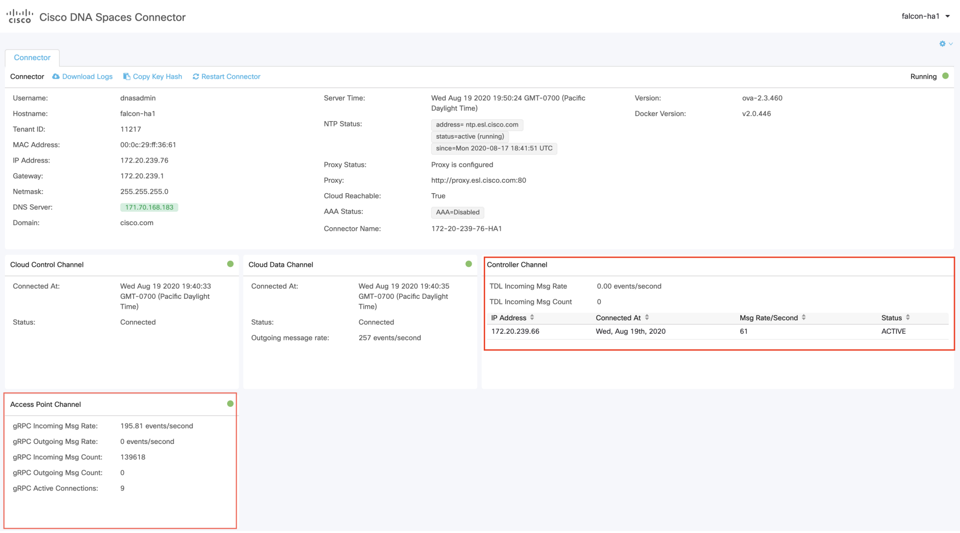
TDL Incoming Msg Rate	0.00 events/second
TDL Incoming Msg Count	45

IP Address	Connected At	Msg Rate/Second	Status
172.20.239.66	Wed, Aug 19th, 2020	58	ACTIVE

Access Point Channel ●

gRPC Incoming Msg Rate:	0 events/second
gRPC Outgoing Msg Rate:	0 events/second
gRPC Incoming Msg Count:	0
gRPC Outgoing Msg Count:	0
gRPC Active Connections:	0

Figure 60: Connector managing AP Channel only. Controller Channel statistics is zero.



Cisco DNA Spaces Connector

falcon-ha1

Connector

Connector | Download Logs | Copy Key Hash | Restart Connector | Running ●

Username:	dnasadmin
Hostname:	falcon-ha1
Tenant ID:	11217
MAC Address:	00:0c:29:ff:36:61
IP Address:	172.20.239.76
Gateway:	172.20.239.1
Netmask:	255.255.255.0
DNS Server:	171.70.168.183
Domain:	cisco.com

Server Time:	Wed Aug 19 2020 19:50:24 GMT-0700 (Pacific Daylight Time)

NTP Status:	address= ntp.esl.cisco.com
	status=active (running)
	since=Mon 2020-08-17 18:41:51 UTC

Proxy Status:	Proxy is configured
Proxy:	http://proxy.esl.cisco.com:80
Cloud Reachable:	True
AAA Status:	AAA=Disabled
Connector Name:	172-20-239-76-HA1

Version:	ova-2.3.460
Docker Version:	v2.0.446

Cloud Control Channel ●

Connected At:	Wed Aug 19 2020 19:40:33 GMT-0700 (Pacific Daylight Time)
Status:	Connected

Cloud Data Channel ●

Connected At:	Wed Aug 19 2020 19:40:35 GMT-0700 (Pacific Daylight Time)
Status:	Connected
Outgoing message rate:	257 events/second

Controller Channel

TDL Incoming Msg Rate	0.00 events/second
TDL Incoming Msg Count	0

IP Address	Connected At	Msg Rate/Second	Status
172.20.239.66	Wed, Aug 19th, 2020	61	ACTIVE

Access Point Channel ●

gRPC Incoming Msg Rate:	195.81 events/second
gRPC Outgoing Msg Rate:	0 events/second
gRPC Incoming Msg Count:	139618
gRPC Outgoing Msg Count:	0
gRPC Active Connections:	9

Connector Active-Active vs Cisco CMX High Availability

The Connector active-active feature is similar to traditional high availability. But, high availability concepts such as virtual IP address, primary, and secondary are not implemented in this feature. The following is a comparison of the Connector active-active feature with the high availability feature of Cisco CMX.

Table 9: Connector Active-Active (High Availability) model

	Connector Active-Active **IoT Services App, Detect and Locate App**	**Cisco CMX Layer 2 VIP High Availability**
IP addressing	Both Connectors are configured with a unique IP address.	Two Cisco CMX devices are configured with a single IP address.
Operational state	Both Connectors are configured in the active state.	One Cisco CMX is the hot primary while the other is in cold standby.
Data before failover	Both Connectors have the same data set and it is the responsibility of Cisco Spaces to manage the data redundancy.	Both the hot primary and the cold standby have the same data set.
Failover support	In the event of a failure, FastLocate, Hyperlocation, and IoT Services need to be reprovisioned.	If the hot primary fails, the cold standby takes over seamlessly.
Version restriction	The same OVA version of 2.3 or higher is mandatory for a Connector active-active pair.	Same version of Cisco CMX is recommended for high availability.

Configuring Connectors in Active-Active

This task shows you how to configures two Connectors as active-active.

Before you begin

Install two different Cisco Spaces: Connectors of OVA version 2.3 or higher. Configure each Connector with a unique IP address.

SUMMARY STEPS

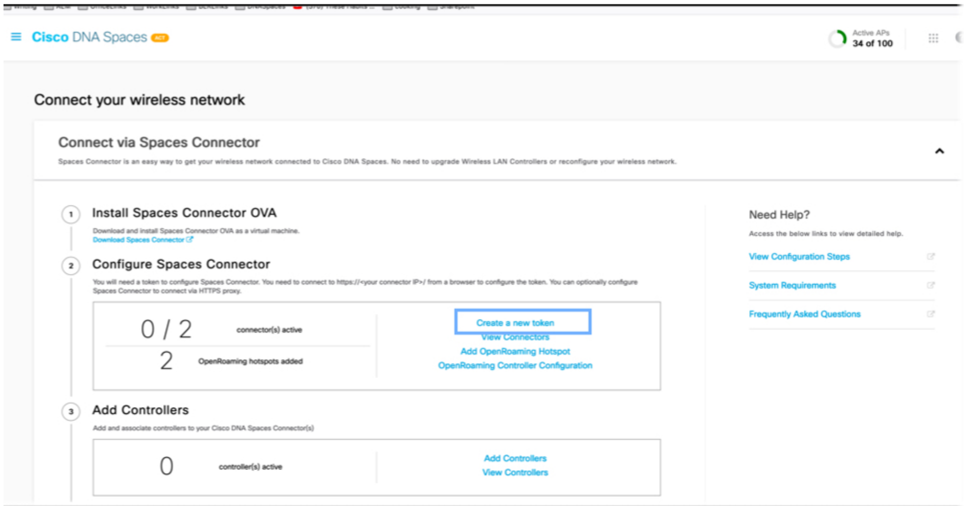
1. Login to **Cisco Spaces>Setup>Wireless Networks** and in the **Configure Spaces Connector** area, click **Create a new token**.
2. Enter a name for the Connector and click **Generate Token**. Copy the token displayed and save it for future reference.
3. Log in to the first Connector and configure the saved token there.
4. Log in to the second Connector and configure the saved token there.
5. On each Connector, observe that the value of the tenant ID is the same.

6. On the Cisco Spaces dashboard, observe both the Connector IP addresses.
7. On each Connector, observe that all controllers added are present.
8. On the Controller CLI, observe that all Connectors are in the NMSP state.

DETAILED STEPS

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

Figure 61: Create a New Token



Connect your wireless network

Connect via Spaces Connector

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

1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.

2 Configure Spaces Connector

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

0 / 2 connector(s) active

2 OpenRoaming hotspots added

3 Add Controllers

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

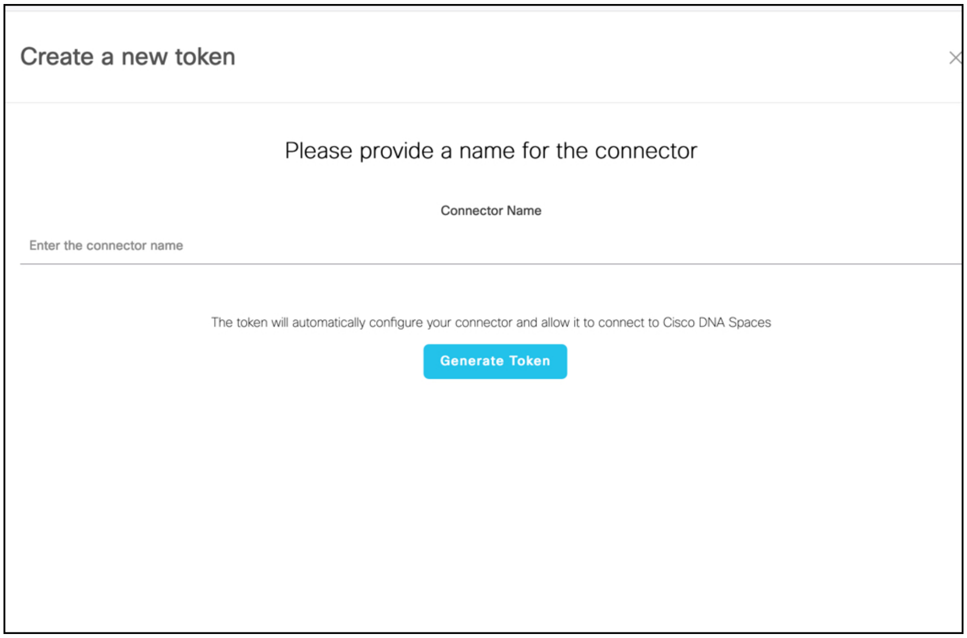
0 controller(s) active

Need Help?

Access the below links to view detailed help.

Step 2 Enter a name for the Connector and click **Generate Token**. Copy the token displayed and save it for future reference.

Figure 62: Connector Name



Create a new token

Please provide a name for the connector

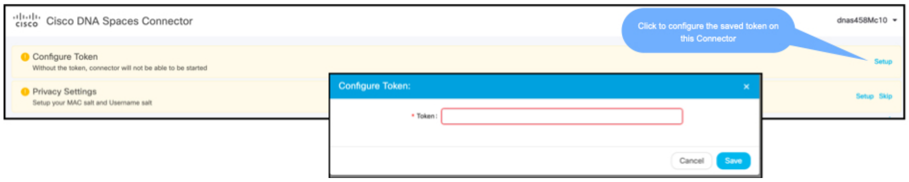
Connector Name

Enter the connector name

The token will automatically configure your connector and allow it to connect to Cisco DNA Spaces

Step 3 Log in to the first Connector and configure the saved token there.

Figure 63: Connector Name



Cisco DNA Spaces Connector

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

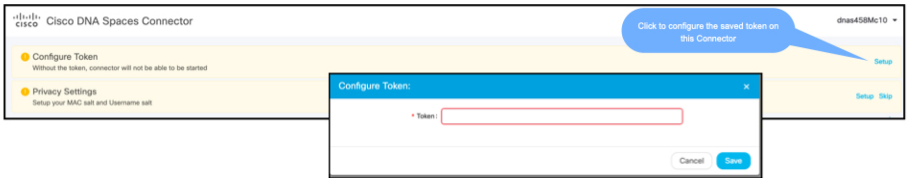
Privacy Settings
Setup your MAC salt and Username salt

Configure Token:

* Token:

Step 4 Log in to the second Connector and configure the saved token there.

Figure 64: Connector Name



Cisco DNA Spaces Connector

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

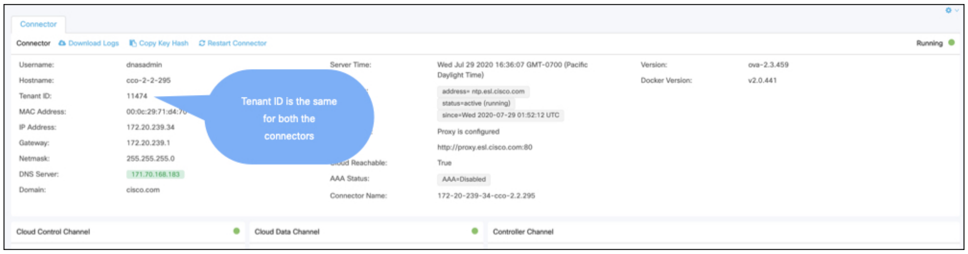
Privacy Settings
Setup your MAC salt and Username salt

Configure Token:

* Token:

Step 5 On each Connector, observe that the value of the tenant ID is the same.

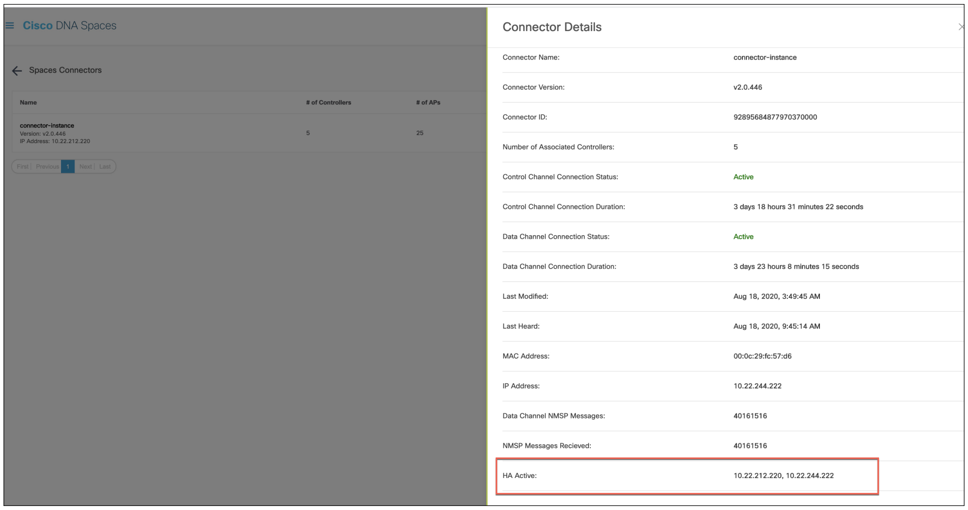
Figure 65: Connector



Username:	dnasadmin	Server Time:	Wed Jul 29 2020 16:36:07 GMT-0700 (Pacific Daylight Time)	Version:	ova-2.3.459
Hostname:	cco-2-2-295		address= ntp.esl.cisco.com status=active (running) since=Wed 2020-07-29 01:52:12 UTC	Docker Version:	v2.0.441
Tenant ID:	11474		Proxy is configured		
MAC Address:	00:0c:29:71:d4:70		http://proxy.esl.cisco.com:80		
IP Address:	172.20.239.34	Cloud Reachable:	True		
Gateway:	172.20.239.1	AAA Status:	AAA=Disabled		
Netmask:	255.255.255.0	Connector Name:	172-20-239-34-cco-2.2.295		
DNS Server:	171.70.168.183				
Domain:	cisco.com				

Step 6 On the Cisco Spaces dashboard, observe both the Connector IP addresses.

Figure 66: Cisco Spaces dashboard



Spaces Connectors

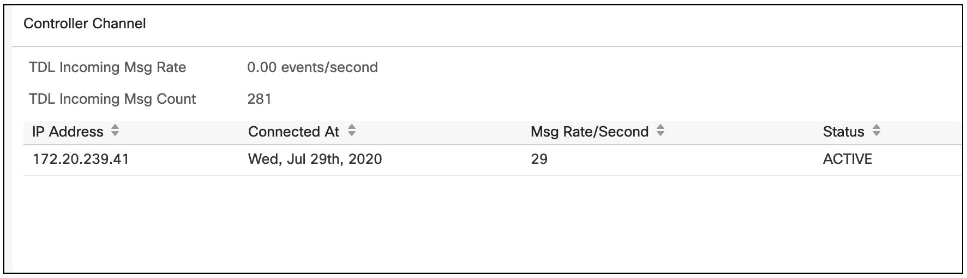
Name	# of Controllers	# of APs
connector-instance Version: v2.0.446 IP Address: 10.22.212.220	5	25

Connector Details

Connector Name:	connector-instance
Connector Version:	v2.0.446
Connector ID:	92895684877970370000
Number of Associated Controllers:	5
Control Channel Connection Status:	Active
Control Channel Connection Duration:	3 days 18 hours 31 minutes 22 seconds
Data Channel Connection Status:	Active
Data Channel Connection Duration:	3 days 23 hours 8 minutes 15 seconds
Last Modified:	Aug 18, 2020, 3:49:45 AM
Last Heard:	Aug 18, 2020, 9:45:14 AM
MAC Address:	00:0c:29:fc:57:d6
IP Address:	10.22.244.222
Data Channel NMSP Messages:	40161516
NMSP Messages Recieved:	40161516
HA Active:	10.22.212.220, 10.22.244.222

Step 7 On each Connector, observe that all controllers added are present.

Figure 67: Connector: Controller Channel Area



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

Step 8 On the Controller CLI, observe that all Connectors are in the NMSP state.

Figure 68: Controller command output

```
show nmsp status

NMSP Status
-----------

DNA Spaces/CMX IP Address                          Active    Tx Echo Resp  Rx Echo Req   Tx Data
  Rx Data     Transport
----------------------------------------------------------------------------------------------------
10.x.212.xxx                           Inactive  13            13            161         6
  TLS
10.x.212.xxx                           Inactive  0             0             17          6
  TLS
10.x.212.xxx                           Active    45070         45070         1378446     574
  TLS
10.x.244.xx                            Inactive  7             7             79          6
  TLS
10.x.244.xx                            Active    56111         56111         1714241     286
  TLS
10.x.244.xx                            Inactive  7             7             104         6
  TLS
10.x.244.xxx                           Active    23056         23056         683908      298
  TLS
```

Configuring Connectors in Active-Active (Wired)

This task shows you how to configures two Connectors as active-active.

Before you begin

Install two different Cisco Spaces: Connectors of OVA version 2.3 or higher. Configure each Connector with a unique IP address.

SUMMARY STEPS

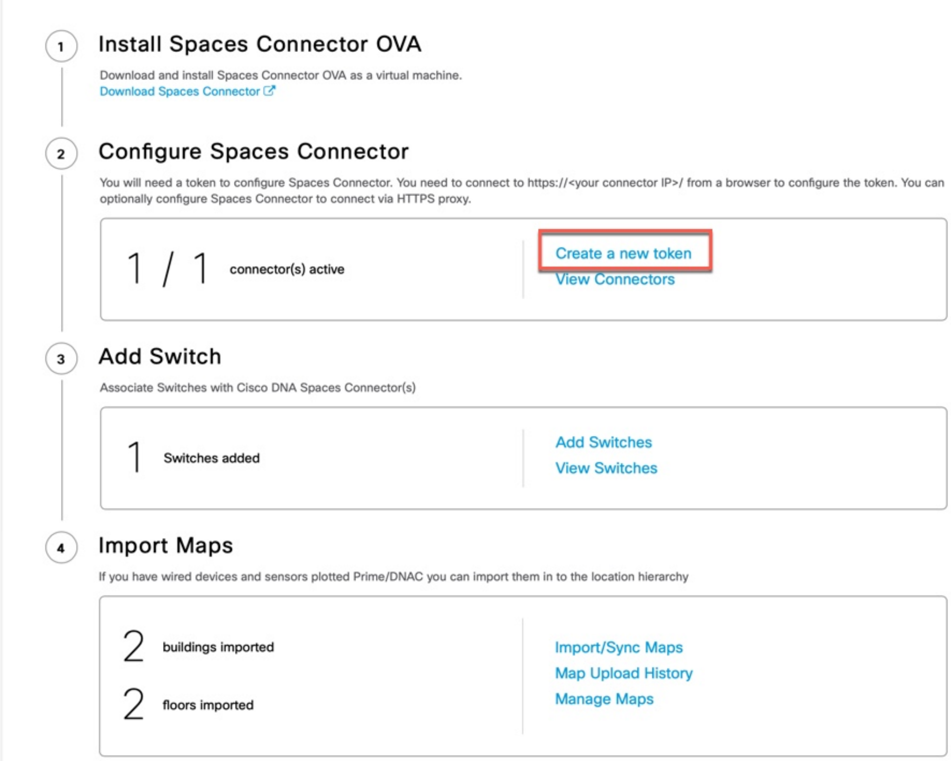
1. Login to **Cisco Spaces>Setup>Wired Networks** and in the **Configure Spaces Connector** area, click **Create a new token**.

2. Enter a name for the Connector and click **Generate Token**. Copy the token displayed and save it for future reference.
3. Log in to the first Connector and configure the saved token there.
4. Log in to the second Connector and configure the saved token there.
5. On each Connector, observe that the value of the tenant ID is the same.
6. On the Cisco Spaces dashboard, observe both the Connector IP addresses.
7. On each Connector, observe that all Connectors added are present.

DETAILED STEPS

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

Figure 69: Create a New Token



1 Install Spaces Connector OVA

Download and install Spaces Connector OVA as a virtual machine.

Download Spaces Connector

2 Configure Spaces Connector

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

1 / 1 connector(s) active

Create a new token

View Connectors

3 Add Switch

Associate Switches with Cisco DNA Spaces Connector(s)

1 Switches added

Add Switches

View Switches

4 Import Maps

If you have wired devices and sensors plotted Prime/DNAC you can import them in to the location hierarchy

2 buildings imported

2 floors imported

Import/Sync Maps

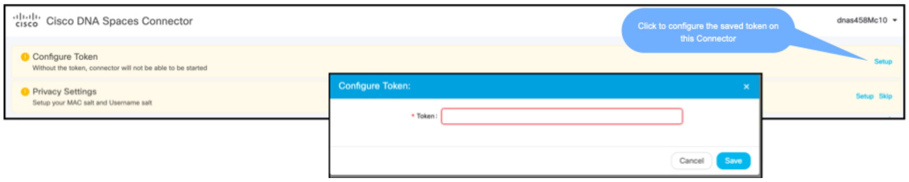
Map Upload History

Manage Maps

Step 2 Enter a name for the Connector and click **Generate Token**. Copy the token displayed and save it for future reference.

Step 3 Log in to the first Connector and configure the saved token there.

Figure 70: Connector Name



Cisco DNA Spaces Connector

dnas458Mc10

Configure Token

Without the token, connector will not be able to be started

Setup

Privacy Settings

Setup your MAC salt and Username salt

Setup Skip

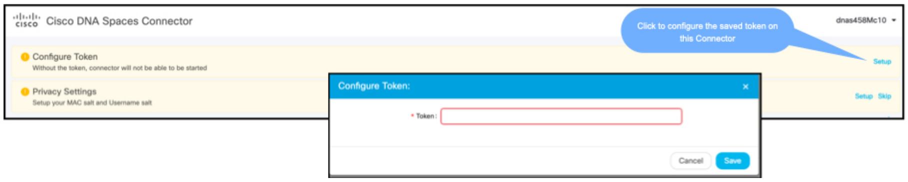
Configure Token:

* Token:

Cancel Save

Step 4 Log in to the second Connector and configure the saved token there.

Figure 71: Connector Name



Cisco DNA Spaces Connector

dnas458Mc10

Click to configure the saved token on this Connector

Configure Token
Without the token, connector will not be able to be started
Setup

Privacy Settings
Setup your MAC salt and Username salt
Setup Skip

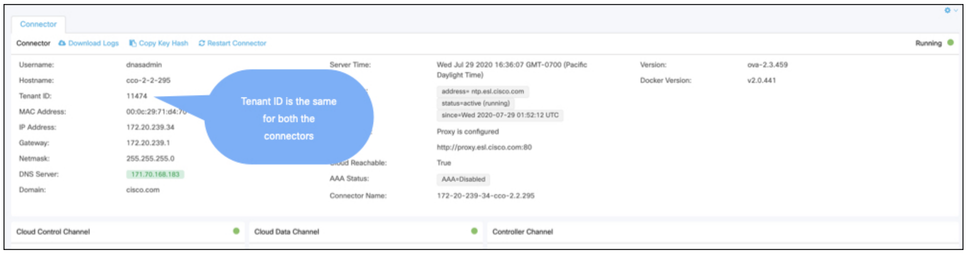
Configure Token: ×

* Token:

Cancel Save

Step 5 On each Connector, observe that the value of the tenant ID is the same.

Figure 72: Connector



Connector

Connector | Download Logs | Copy Key Hash | Restart Connector | Running ●

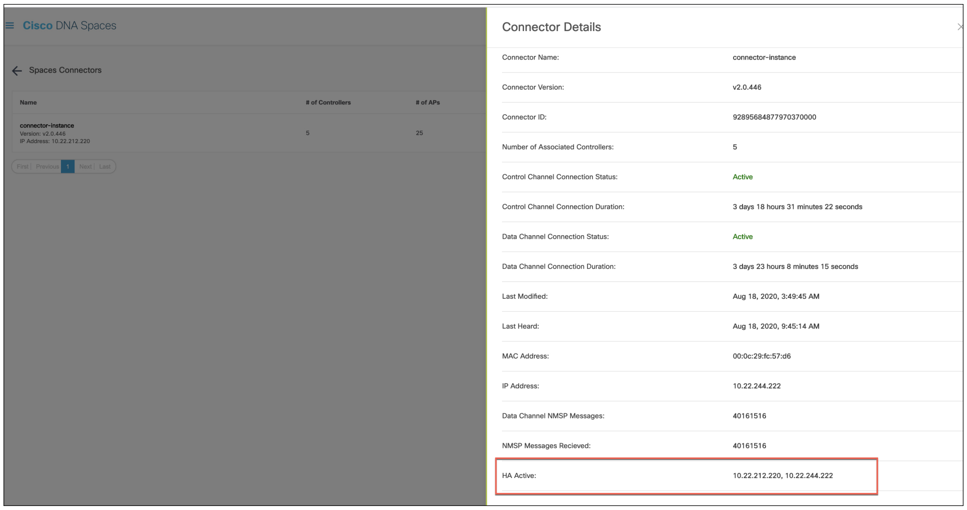
Username:	dnasadmin	Server Time:	Wed Jul 29 2020 16:36:07 GMT-0700 (Pacific Daylight Time)	Version:	ova-2.3.459
Hostname:	cco-2-2-295			Docker Version:	v2.0.441
Tenant ID:	11474		address= ntp.esl.cisco.com status=active (running) since=Wed 2020-07-29 01:52:12 UTC		
MAC Address:	00:0c:29:71:d4:7				
IP Address:	172.20.239.34		Proxy is configured		
Gateway:	172.20.239.1		http://proxy.esl.cisco.com:80		
Netmask:	255.255.255.0	oud Reachable:	True		
DNS Server:	171.70.168.183	AAA Status:	AAA=Disabled		
Domain:	cisco.com	Connector Name:	172-20-239-34-cco-2.2.295		

Tenant ID is the same for both the connectors

Cloud Control Channel ● | Cloud Data Channel ● | Controller Channel

Step 6 On the Cisco Spaces dashboard, observe both the Connector IP addresses.

Figure 73: Cisco Spaces dashboard



Cisco DNA Spaces

← Spaces Connectors

Name	# of Controllers	# of APs
connector-instance Version: v2.0.446 IP Address: 10.22.212.220	5	25

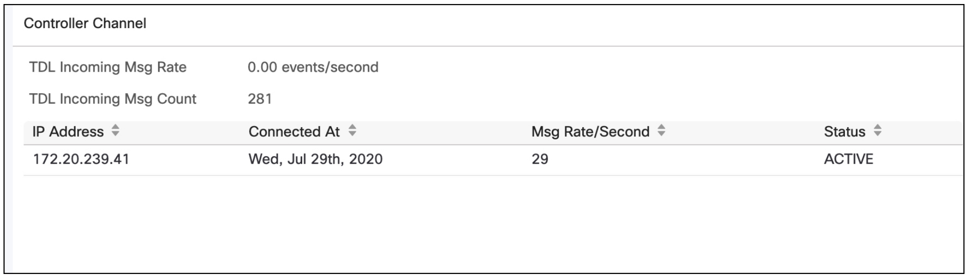
First | Previous | 1 | Next | Last

Connector Details

Connector Name:	connector-instance
Connector Version:	v2.0.446
Connector ID:	92895684877970370000
Number of Associated Controllers:	5
Control Channel Connection Status:	Active
Control Channel Connection Duration:	3 days 18 hours 31 minutes 22 seconds
Data Channel Connection Status:	Active
Data Channel Connection Duration:	3 days 23 hours 8 minutes 15 seconds
Last Modified:	Aug 18, 2020, 3:49:45 AM
Last Heard:	Aug 18, 2020, 9:45:14 AM
MAC Address:	00:0c:29:fc:57:d6
IP Address:	10.22.244.222
Data Channel NMSP Messages:	40161516
NMSP Messages Recieved:	40161516
HA Active:	10.22.212.220, 10.22.244.222

Step 7 On each Connector, observe that all Connectors added are present.

Figure 74: Connector: Controller Channel Area



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

PART IX

Communications, Services, and Additional Information

- Communications, Services, and Additional Information, on page 131

CHAPTER 20

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, on page 131
- Documentation Feedback, on page 131

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.