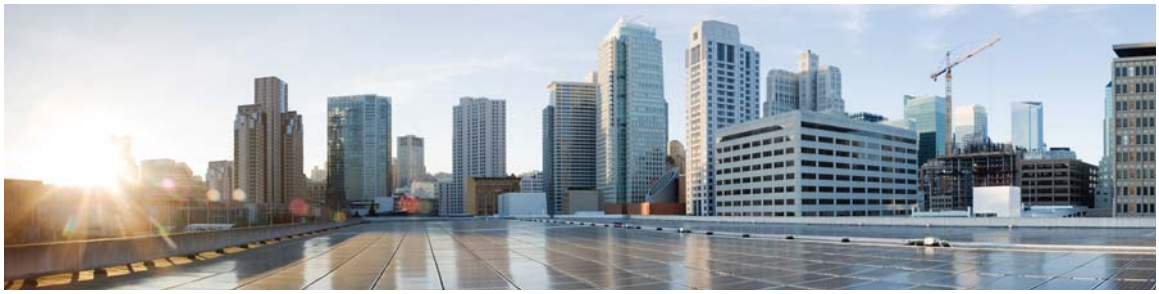


Cisco DNA Spaces Connector Configuration Guide

First Published: November 10, 2018
Last Updated: March 12, 2019

Contents

This document describes how to configure a Cisco DNA Spaces Connector, and associate it with your Cisco DNA Spaces account.

Cisco DNA Spaces Connector -Overview

The Cisco DNA Spaces Connector enables Cisco DNA Spaces to communicate with multiple Cisco AireOS Wireless Controllers efficiently by allowing each Wireless Controller to transmit high intensity client data without missing any client information.

Cisco Systems, Inc.
www.cisco.com

Supported Cisco AireOS Wireless Controller Versions

The Cisco DNA Spaces Connector currently supports the following Cisco AireOS Wireless Controller Versions:

- 8.0.152.0
- 8.2.170.0
- 8.3.143.0
- 8.5.140.0
- 8.7.106.0
- 8.8.111.0

System Requirements

Before configuring the Cisco DNA Spaces Connector, ensure that all of the following system requirements are met.

Table 1-1 Minimum System Requirements

Item	Supported Requirements
vCPU	2
RAM	4 GB
Hard Disk	60 GB

Prerequisites

- The Cisco DNA Spaces Connector should be able to reach out to the Cisco DNA Spaces endpoints for establishing data connectivity with Cisco DNA Spaces.
  - For US setup, the Cisco DNA Spaces Connector must be able to reach out to https://connector.dnaspaces.io/ (IP addresses: Primary- 52.20.144.155, 34.231.154.95 Disaster Recovery-54.176.92.81, 54.183.58.225).
  - For EU setup, the Cisco DNA Spaces Connector must be able to reach out to https://connector.dnaspaces.eu/ (IP addresses: Primary- 63.33.127.190, 63.33.175.64 Disaster Recovery-Recovery: 3.122.15.26, 3.122.15.7)
- The Cisco DNA Spaces Connector must be able to connect to the Wireless Controllers on port 16113 over TCP and SNMP Ports 161/162 over UDP.
- Ensure that https://www.cisco.com and cisco.com domains are white-listed.
- For both SNMP (Simple Network Management Protocol) Versions, v2C and v3, read-write permissions are required. This is required for registering the Cisco DNA Spaces Connector certificate with the Wireless Controller.
- If you are using Cisco Wireless Controller cloud connect or if CMX cloud services is enabled, ensure that CMX Cloud Services are disabled on your Wireless Controllers by executing the following command : `config cloud-services cmx disable`. After disabling, save the configurations.

- The Wireless Controller IP you configure in the Cisco DNA Spaces dashboard must be able to reach out to the Cisco DNA Spaces Connector.

Recommended Deployment Architecture

Table 1-2 Cisco DNA Spaces- Supported Capacity

vCPU	Memory	NMSP Messages/ Second	AP Count	Client Count	Recommended Bandwidth Usage
2 vCPU (2000 MHz)	4 GB	10,500	12,500	350,000	30 Mbps

Configuring the Cisco DNA Spaces Connector

To use the Cisco DNA Spaces Connector, first you must install the Cisco DNA Spaces Connector in your local deployment network. Then, you must create a Cisco DNA Spaces Connector in the Cisco DNA Spaces dashboard to generate the token for the Cisco DNA Spaces Connector. Configure this token in the Cisco DNA Spaces Connector to establish a connection between Cisco DNA Spaces and Cisco DNA Spaces Connector. Also, setup connectivity between Cisco DNA Spaces Connector and Cisco Wireless Controller by configuring the Wireless Controller in the Cisco DNA Spaces dashboard.

To configure the Cisco DNA Spaces Connector, perform the following steps:

1. Downloading and Deploying the Cisco DNA Spaces Connector, page 3
2. Creating Cisco DNA Spaces Connector and Retrieving the Cisco DNA Spaces Connector Token, page 5
3. Setting Up the Cisco DNA Spaces Connector, page 7
4. Setting up Connectivity between the Cisco DNA Spaces Connector and Cisco Wireless Controller, page 8

Downloading and Deploying the Cisco DNA Spaces Connector

To download and deploy the Cisco DNA Spaces Connector, perform the following steps:

Step 1 Download the **Cisco DNA Spaces Connector OVA** from software.cisco.com.

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

Note The file size of the OVA is 1.08 GB.

Step 3 In the log in screen that appears, enter the following username and password.

- username: **root**
- password: **cisco**

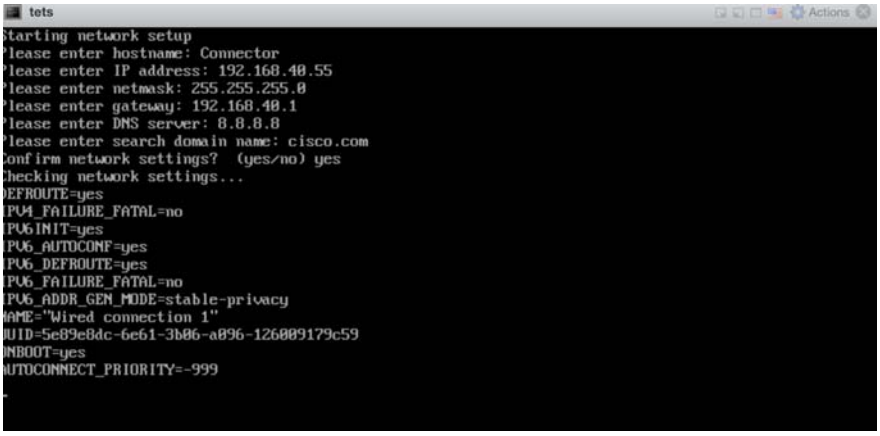
Figure 1-1 Login screen
Sample screen

Step 4 Enter the network settings by specifying the parameters such as IP address, host name, and so on that you want to configure on the Cisco DNA Spaces Connector.

Step 5 After specifying the network settings, enter **yes** to confirm.

Step 6 After successful verification of endpoints, you are asked to finalize the network setup within 60 seconds. Enter **yes** to finalize the network setup.

Figure 1-2 Network Settings
Sample screen



Note Ensure to provide the input within 60 seconds. Otherwise, the configuration will time out and you may have to reconfigure.

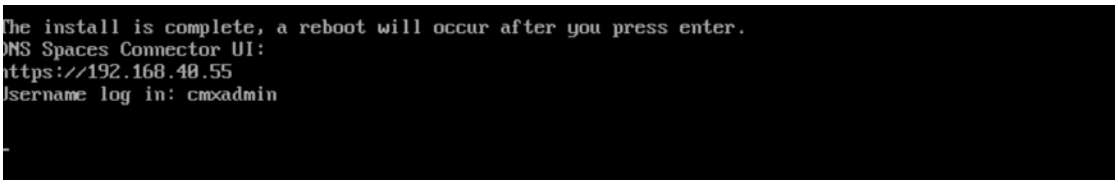
Step 7 Enter NTP settings, if required.

Step 8 Create a new password for the **root** user and **cmxadmin** user.

The message stating installation is complete appears along with the URL for the Cisco DNA Spaces Connector.

Figure 1-3 Installation Complete Message

Sample screen



Step 9 Press **Enter** to reboot the device, and open the WebUI using the address provided.

Creating Cisco DNA Spaces Connector and Retrieving the Cisco DNA Spaces Connector Token

Cisco DNA Spaces enables you add Cisco DNA Spaces Connector from the Cisco DNA Spaces dashboard. Cisco DNA Spaces supports multiple Cisco DNA Spaces Connectors, and each Cisco DNA Spaces Connector can be associated with multiple Wireless Controllers.

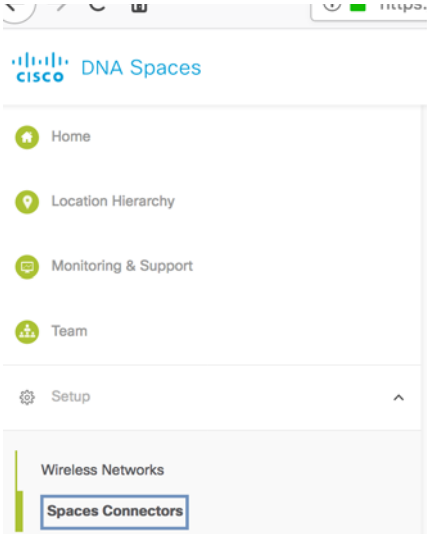
A token will be generated for each Cisco DNA Spaces Connector added to Cisco DNA Spaces. This token is used to connect Cisco DNA Spaces with Cisco DNA Spaces Connector. Each token is Cisco DNA Spaces Connector-specific, and thereby enables Cisco DNA Spaces to identify the Cisco DNA Spaces Connector.

To create a Cisco DNA Spaces Connector in Cisco DNA Spaces, and to retrieve the token for that connector, perform the following steps:

Step 1 Log in to Cisco DNA Spaces.

Step 2 In the **Cisco DNA Spaces** dashboard, choose **Setup > Spaces Connectors.**

Figure 1-4 Spaces Connectors



Note In the **Cisco DNA Spaces** dashboard, you can also click the **Wi-Fi** icon at the top right of the page, and then click **Wireless Network Status** to add a Cisco DNA Spaces Connector.

Step 3 To create a new Cisco DNA Spaces Connector, click **Create New.**

Figure 1-5 Create New Cisco DNA Spaces Connector

Step 4 In the **Create New Spaces Connector** window that appears, enter a name for the Cisco DNA Spaces Connector.

Step 5 Click **Save**.

The newly added connector gets listed on the **Spaces Connectors** page.

Step 6 In the **Spaces Connectors** window, click the **View Access Token** icon for the connector you added.

Figure 1-6 Access Token

Step 7 In the **Log In** window that appears, enter your Cisco DNA Spaces login credentials, and click **Submit**.

Step 8 In the dialog box that appears, click **Copy** to copy the Token string.

Note A Cisco DNA Spaces Connector is shown as active after its establishes connection with Cisco DNA Spaces.

Note In the **Connectors** page, the total number of Wireless Controllers added to a Cisco DNA Spaces Connector is displayed.

Setting Up the Cisco DNA Spaces Connector

You must establish connection between the Cisco DNA Spaces Connector and Cisco DNA Spaces, and do the necessary configurations in the Cisco DNA Spaces Connector to transmit data using Cisco DNA Spaces Connector.

To set up the Cisco DNA Spaces Connector, perform the following steps:

Step 1 Log into the Cisco DNA Spaces Connector using the URL provided during the OVA deployment, https://<IP -address>/ at step 8 of "Downloading and Deploying the Cisco DNA Spaces Connector" section on page 3.

Step 2 In the **Cisco DNA Spaces Connector** window that appears, enter the **cmxadmin** username and password configured at step 8 of "Downloading and Deploying the Cisco DNA Spaces Connector" section on page 3.

Step 3 In the **Configuration** window that appears, hover over the **Settings** icon, and choose **Configure Token**. In the Token window, enter the token copied at step 8 of "Creating Cisco DNA Spaces Connector and Retrieving the Cisco DNA Spaces Connector Token" section on page 5, and click **Save**.

Note When configuring the token, you may have to wait a few minutes (depending on the speed of your connection). The status changes from **Configuring Token** to **Retrieving Connector Status**. You will notice that the **Configure Token** notification is automatically removed from the Cisco DNA Spaces Connector UI.

Step 4 If your device is behind a Proxy, click **Setup HTTP Proxy** to configure which proxy to use. For more information on configuring the proxy, see the "Configuring a Proxy" section on page 12.

Note In this case, without a proxy, the Cisco DNA Spaces Connector will not be able to communicate with Cisco DNA Spaces.

Figure 1-7 HTTP Proxy
Sample screen

Step 5 Click **Privacy Settings** to configure privacy settings.

Note You can download logs and update the Cisco DNA Spaces Connector version from this dashboard.

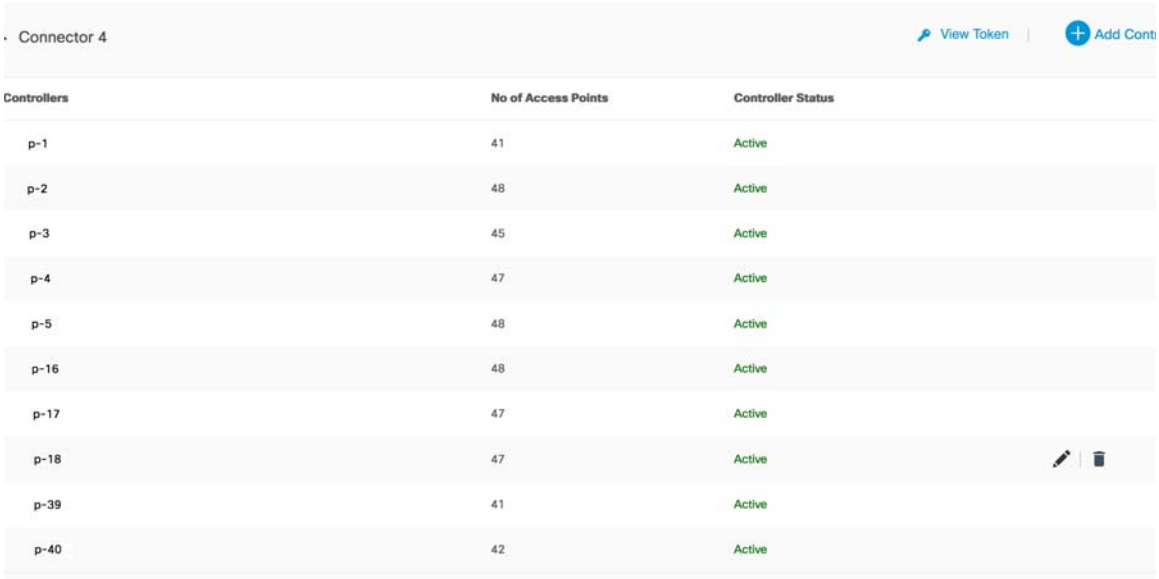
Setting up Connectivity between the Cisco DNA Spaces Connector and Cisco Wireless Controller

To setup connectivity between Cisco DNA Spaces Connector and Cisco Wireless Controller, perform the following steps:

Step 1 In the **Cisco DNA Spaces** dashboard, choose **Setup> Spaces Connectors**.

Step 2 Click the **Cisco DNA Spaces Connector** to which you want to add the Wireless Controller.

Figure 1-8 Add Controller-1



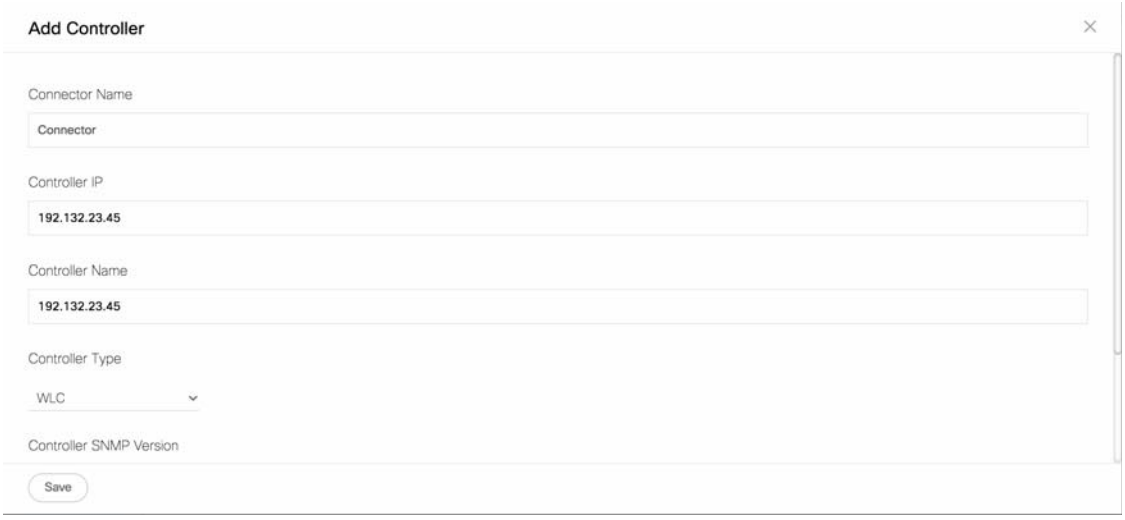
Step 3 In the window that appears, click **Add Controller**.

Figure 1-9 Add Controller -2

Step 4 In the **Add Controller** window that appears, enter the details of the Wireless Controller to which you want to establish connection. Specify the details such as IP address, name, and controller type.

Note The Wireless Controller IP you configure must be able to reach out to the Cisco DNA Spaces Connector.

Figure 1-10 Add Controller -3



a. In the **Controller IP** field, enter the IP address of the Wireless Controller.

b. In the **Controller name** field, enter the name of the Wireless Controller.

c. From the **Controller Type** drop-down list, choose the controller type as Wireless Controller.

d. From the **Controller SNMP Version** drop-down list, choose the SNMP Version of the Wireless Controller.

   – If you choose the SNMP version as **v2C**, specify the SNMP Community.

   – If you choose the **SNMP version** as **v3**, specify the SNMP v3 version username, privacy protocol credentials, and authentication protocol credentials.

Note As the Cisco DNA Spaces Connector certificate needs to be registered with the Wireless Controller, SNMP v2c and SNMP v3 must have read-write permission in the Wireless Controller. The Cisco DNA Spaces Connector does not support SNMP v1.

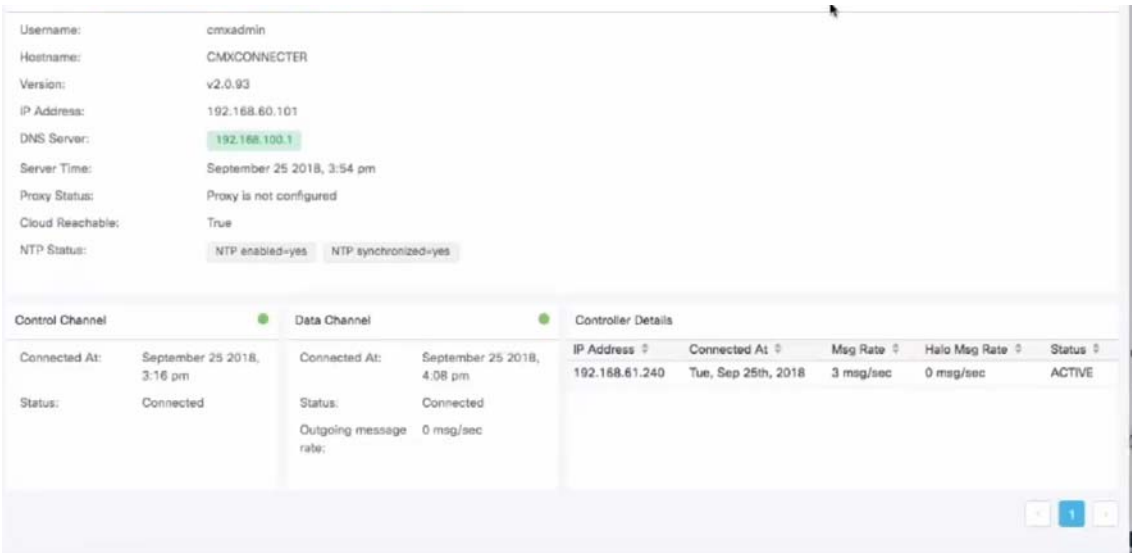
e. Click **Save**.

The new Wireless Controller is now listed under the Cisco DNA Spaces Connector to which it is added. The Wireless Controller that is connected to the Cisco DNA Spaces Connector successfully appears as active.

Note It takes approximately 5 minutes for the Wireless Controller to be shown as **Active**. You must refresh your window to view status change. If the Wireless Controller does not have any APs associated with it, then the status will remain as **Inactive**.

The Wireless Controller added also gets listed in the **Controller Details** window of the Cisco DNA Spaces Connector.

Figure 1-11 Cisco DNA Spaces Connector window



Note

- You can add multiple Wireless Controllers to a Cisco DNA Spaces Connector.

When you open a Cisco DNA Spaces Connector, all the Wireless Controllers associated with it are listed.

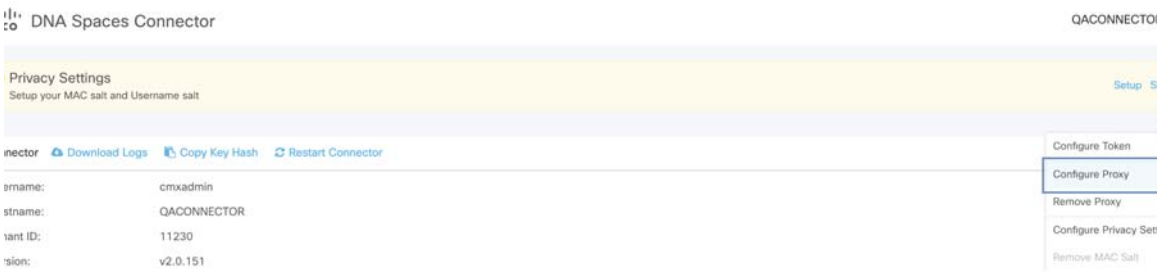
Now the Cisco Wireless Controller will be available for import in the Cisco DNA Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and access points to the Cisco Wireless Controller, see the Defining the Location Hierarchy for Cisco Unified Wireless Network with Wireless Controller (without Cisco CMX Installation).

Configuring a Proxy

To configure a proxy, perform the following steps:

Step 1 In the **Cisco DNA Spaces Connector** dashboard, choose **Settings >Configure Proxy** to add the proxy server.

Figure 1-12 Configure Proxy



Step 2 Add proxy IP with port.

Format: http://<proxy server IP>:<port>

Note You can configure a HTTP or HTTPS proxy.

Step 3 After the proxy is configured, the **Proxy Status** in the Cisco DNA Spaces Connector dashboard gets changed to **Proxy is configured**.

Step 4 If any error occurs while configuring the proxy, log into the **Cisco DNA Spaces Connector CLI** and verify whether you can ping proxy server IP using the following command:

```
ping <proxy server IP>
```

Step 5 In the **Cisco DNA Spaces Connector CLI**, execute the following command to verify whether a connection can be established to **dms.dnaspaces.io** and **connector.dnaspaces.io** through proxy.

```
docker container exec -it $(docker container ls -q) /bin/bash
curl -X GET -vvv https://connector.dnaspaces.io/ --proxy http://<proxy server IP>:<port>
```

If the connection is successful, the following result is shown:

```
HTTP/1.1 200 OK
```

Step 6 If you are getting any certificate error 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 Cisco DNA Spaces Connector.

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

b. Run the command `connectorctl setproxycert <cert>`.

c. Reconfigure the token in **Cisco DNA Spaces Connector** dashboard.

d. If you want to verify that the certificate is correct, run one of the following commands on the Cisco DNA Spaces Connector (it should respond with HTTP/1.1 200 OK).

- Command for transparent proxies:

```
curl -vvv https://connector.dnaspaces.io --cacert <cert>
```

– Command for explicit proxies:

```
curl -vvv https://connector.dnaspaces.io --proxy http://<proxy server IP>:<port>
--cacert <cert>
```

There is a known issue that will cause the `connectorctl` command to say that command failed if you are using a transparent proxy or if you have not configured your proxy through the UI yet. However, if the following message is displayed, the certificate is considered to be configured successfully.

```
[cmxadmin@connector-1 ~]$ connectorctl setproxycert <cert>

New cert exists.

Starting connector container ...
```

Step 7 If the previous step is not resolving 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.

For more information on CLI commands, privacy settings, and supported proxies, see https://support.cmxcisco.com/hc/en-us/categories/360000937753-Cisco-DNA-Spaces-Connector.

Cisco DNA Spaces Compatibility Matrix

Table 1-3 Cisco DNA Spaces Compatibility Matrix

Application	3504/5520/8540	2504/5508/8510/vWLC/WISM2	IOS-XE	Prime	DNA Center	Cisco DNA Spaces Features
Cisco DNA Spaces Connector	• AireOS 8.5 and later.	AireOS 8.0 to 8.5 and later	Not Supported	NA	NA	• Platform • Dashboard • Captive portal • Engagements • Behavior Metrics • Operational Insights • Cloud Location (Beta) • BLE Manager (Beta) • SDK (Beta)