



Troubleshooting Scenarios

- [Connectivity Issues Between Connector and Cisco Spaces, on page 1](#)
- [Unresponsive Connector, or Failure of SSH to Connector, on page 4](#)
- [Instance is Corrupted or Deleted , on page 6](#)
- [Service Crash, or Restart Services , on page 6](#)
- [Upgrade has Failed, or How To Forcibly Push Configurations to Instances, on page 7](#)
- [Weak SSH MAC Algorithms, on page 7](#)

Connectivity Issues Between Connector and Cisco Spaces

This task allows you to troubleshoot connectivity issues between your connector and Cisco Spaces. You can troubleshoot this connection both before and after the configuration of the connector token on Cisco Spaces.

Step 1 Log in to the connector GUI.

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

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

Step 3 Click **Run New Test** to initiate troubleshooting the connectivity.

Step 4 Observe the running tests for the following:


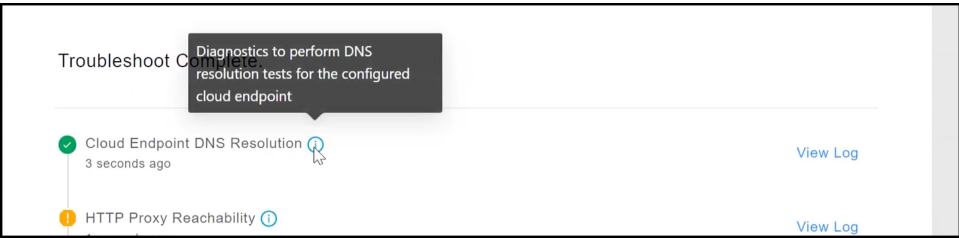
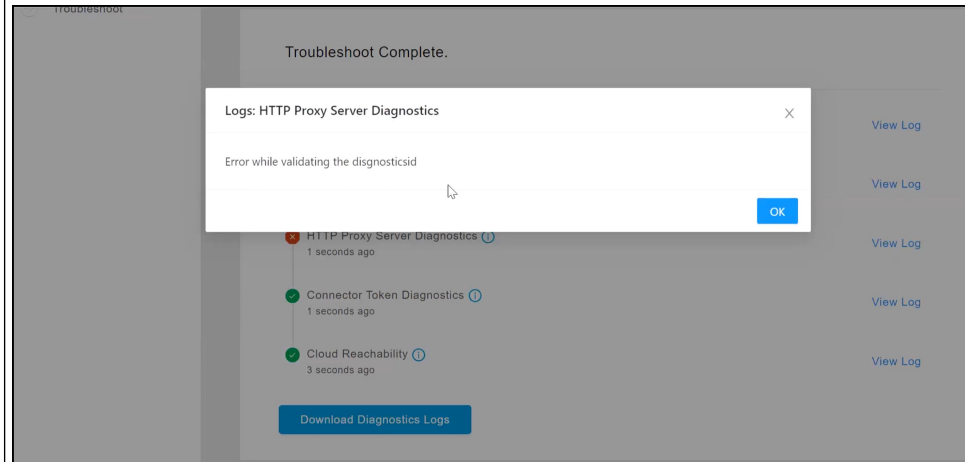
	<p>Click to view further information about the test.</p> <div data-bbox="495 1507 1448 1743"></div> <p>Click View Logs to view further information.</p>
---	--

Figure 1: View Logs




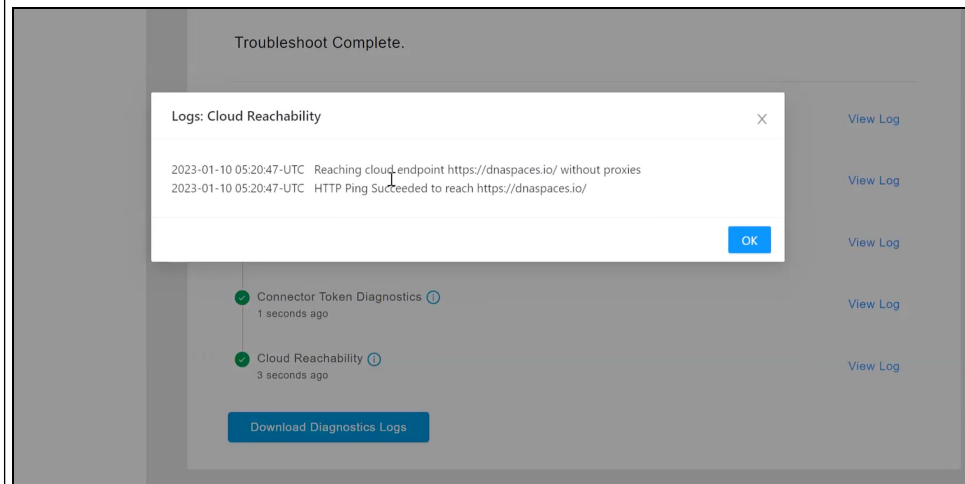
Represents a successful test. Click  to view additional information about this successful test.

Figure 2: View Logs for a Successful Test






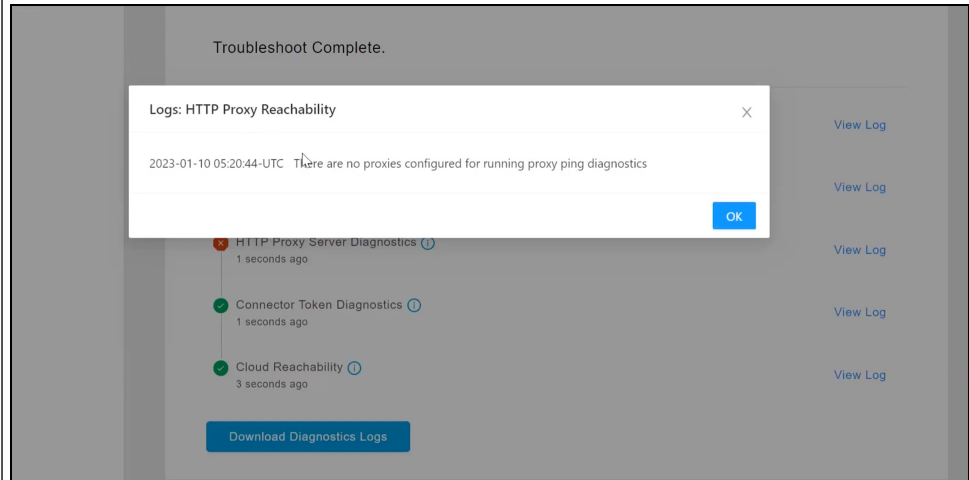
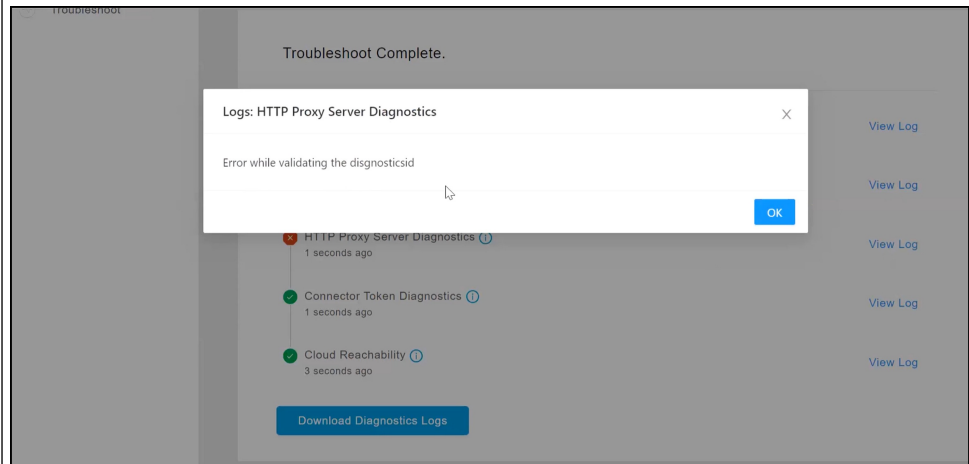
Represents a warning. Click  to view additional information about this warning.

Figure 3: View Logs for a Warning



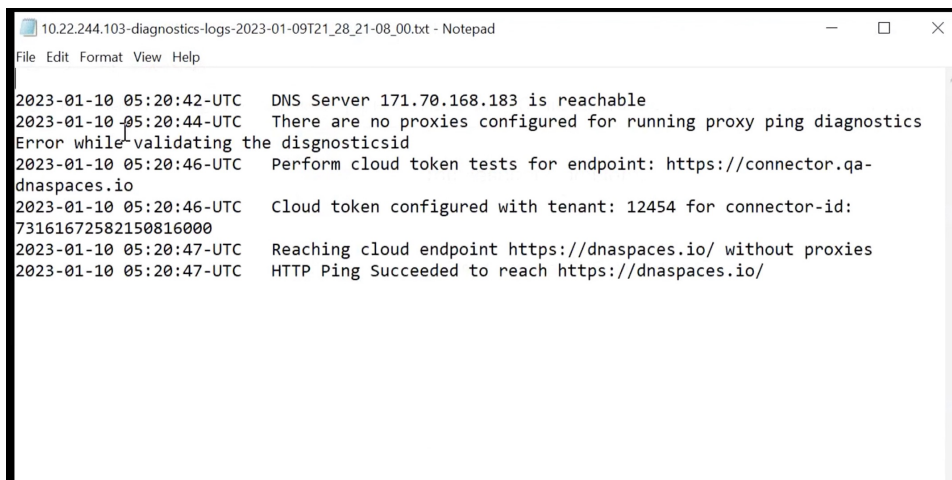
Represents a failure in the diagnostic test. Click **View Logs** to see additional details.

Figure 4: View Logs for a Successful Test



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

Figure 5: ownload Diagnostic Logs



```

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

```

What to do next

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

Unresponsive Connector, or Failure of SSH to Connector

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

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

Note The Cisco Spaces URL is region-dependent.

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

Step 3 In the **2. Configure Spaces Connector** area, click **View Connectors**.

Step 4 Click a connector from the list of connectors that are displayed, and then click the **Instances** tab.

Step 5 In the **Actions** column, click the three-dot icon to open a list of options for the connector instance, and choose **Restart Connector**.

Figure 6: Restart Connector

Instance is Corrupted or Deleted

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

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

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

Note The Cisco Spaces URL is region-dependent.

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

Step 3 In the **2. Configure Spaces Connector** area, click **View Connectors**.

Step 4 Click a connector from the list of connectors that are displayed and then click the **Instances** tab.

Step 5 In the **Actions** column, click the three-dot icon to open a list of options for the connector instance, and choose **Remove**.
To create a new instance, do the following.

- a. In the Cisco Spaces dashboard, reissue a token.
- b. Configure the new token on the installed connector.

See [Activating Connector 3 on Cisco Spaces](#).

Service Crash, or Restart Services

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

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

Note The Cisco Spaces URL is region-dependent.

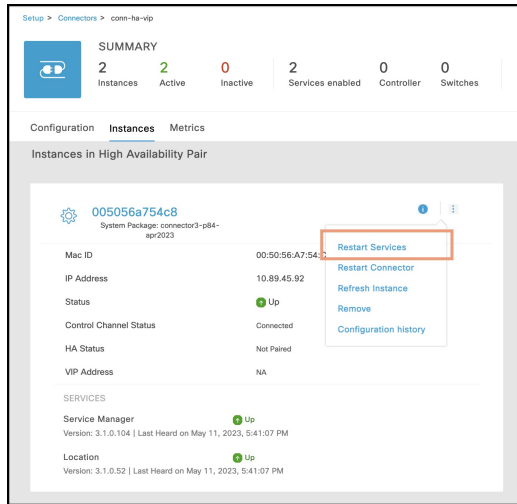
Step 2 From the left navigation pane of the Cisco Spaces dashboard, choose **Setup > Wireless Networks**.

Step 3 In the **2. Configure Spaces Connector** area, click **View Connectors**.

Step 4 Click a connector from the list of connectors that are displayed, and then click the **Instances** tab.

Step 5 In the **Actions** column, click the three-dot icon to open a list of options for the connector instance, and choose **Restart Services**.

Figure 7: Restart Services



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

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

Step 1

Log in to **Cisco Spaces**.

Note The Cisco Spaces URL is region-dependent.

Step 2

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

Step 3

In the **2. Configure Spaces Connector** area, click **View Connectors**.

Step 4

Click a connector from the list of connectors that are displayed, and then click the **Instances** tab.

Step 5

In the **Actions** column, click the three-dot icon to open a list of options for the connector instance, and choose **Refresh Instance**.

Weak SSH MAC Algorithms

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

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

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

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

Disable Weak MAC Algorithms

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

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

Step 2 To remove support for weak MAC algorithms from this device, use the **connectorctl weakmac remove** command. Run the **connectorctl weakmac show** command to verify that weak MAC algorithms are removed from the supported algorithm list.

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

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

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

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



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