

# **Configuring Proxy**

• Configuring a Proxy, on page 1

## **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 1: Setup Proxy

_	
	Set up HTTP Proxy
1	f the machine is sitting behind a proxy, Connector won't be able to interact with cloud without setting up the proxy
	Privacy Settings
5	Setup your MAC salt and Username salt

Figure 2: Setup Proxy

Configure HTTP Proxy		×
* HTTP Proxy :	http://trial.proxy.com:port	
	Cancel	Save

You can also configure proxy including basic authentication credentials.

#### Figure 3: Configuring Proxy With Basic Authentication

Configure HTTP Proxy		X
* HTTP Proxy:	http://username:password@myproxyserver.com:80	
		Cancel Save

C Restart Connector				
	Server Time:		Version:	0
		GMT-0700 (Pacific Daylight Time)	Docker Version:	v
	NTP Status:			

#### Figure 4: Proxy Configured With Basic Authentication

Server Time:		Version:	ova-2.3.492		
	GMT-0700 (Pacific Daylight Time)	Docker Version:	v2.(		
NTP Status:					
Proxy Status:	tatus: Proxy is configured				
Proxy:	http://username:******@myproxyserver.com:80				
Cloud Reachable:	True				
AAA Status:	AAA=Disabled				
Connector Name:					

Running 🔵

## **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.