# Connectors

## Set up and administration

NetApp
March 31, 2022

# Table of Contents

# Connectors

## Finding the system ID for a Connector

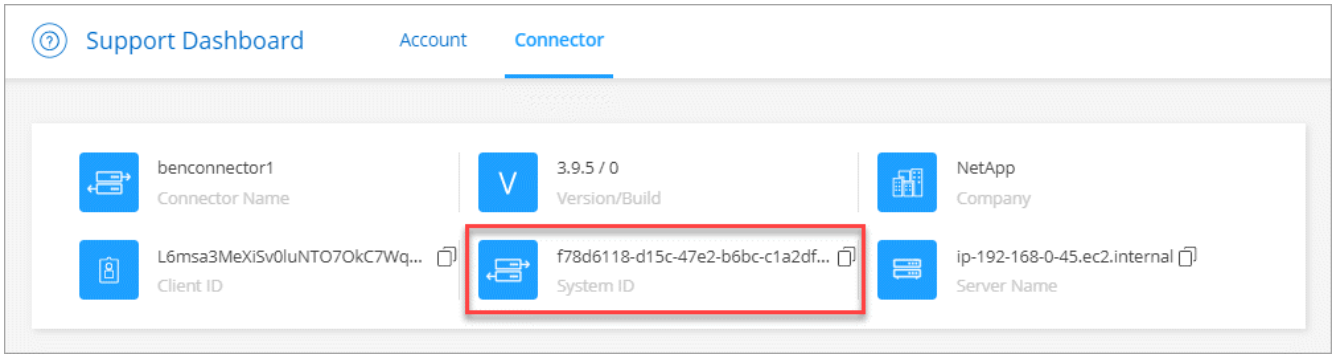
To help you get started, your NetApp representative might ask you for the system ID for a Connector. The ID is typically used for licensing and troubleshooting purposes.

**Steps**

1. In the upper right of the Cloud Manager console, click the Help icon.
2. Click **Support > Connector**.

   The system ID appears at the top.

   **Example**




# Managing existing Connectors

After you create one or more Connectors, you can manage them by switching between Connectors, connecting to the local user interface running on a Connector, and more.

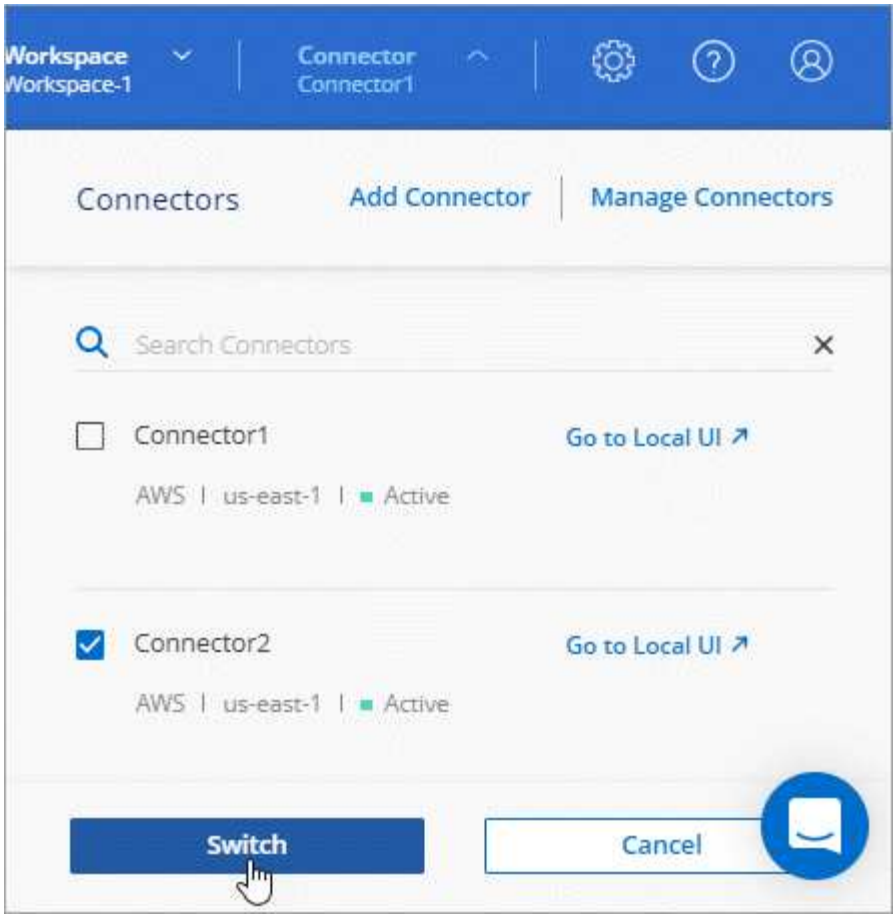
## Switch between Connectors

If you have multiple Connectors, you can switch between them to see the Working Environments that are associated with a specific Connector.

For example, let's say that you're working in a multi-cloud environment. You might have one Connector in AWS and another in Google Cloud. You'd need to switch between those Connectors to manage the Cloud Volumes ONTAP systems running in those clouds.

**Step**

1. Click the **Connector** drop-down, select another Connector, and then click **Switch**.




Cloud Manager refreshes and shows the Working Environments associated with the selected Connector.

## Access the local UI

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. This interface is needed for a few tasks that need to be performed from the Connector itself:

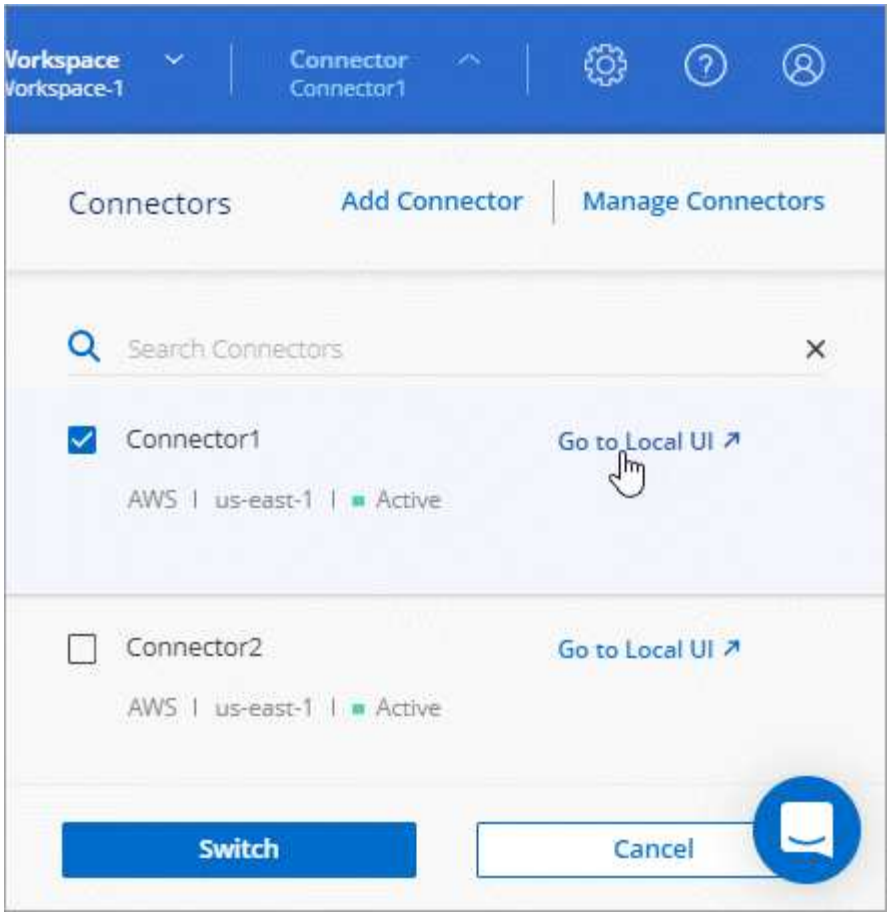
- Setting a proxy server
- Installing a patch (you'll typically work with NetApp personnel to install a patch)
- Downloading AutoSupport messages (usually directed by NetApp personnel when you have issues)

**Steps**

1. Log in to the Cloud Manager SaaS interface from a machine that has a network connection to the Connector instance.

   If the Connector doesn't have a public IP address, you'll need a VPN connection or you'll need to connect from a jump host that's in the same network as the Connector.

2. Click the **Connector** drop-down and then click **Go to Local UI**.



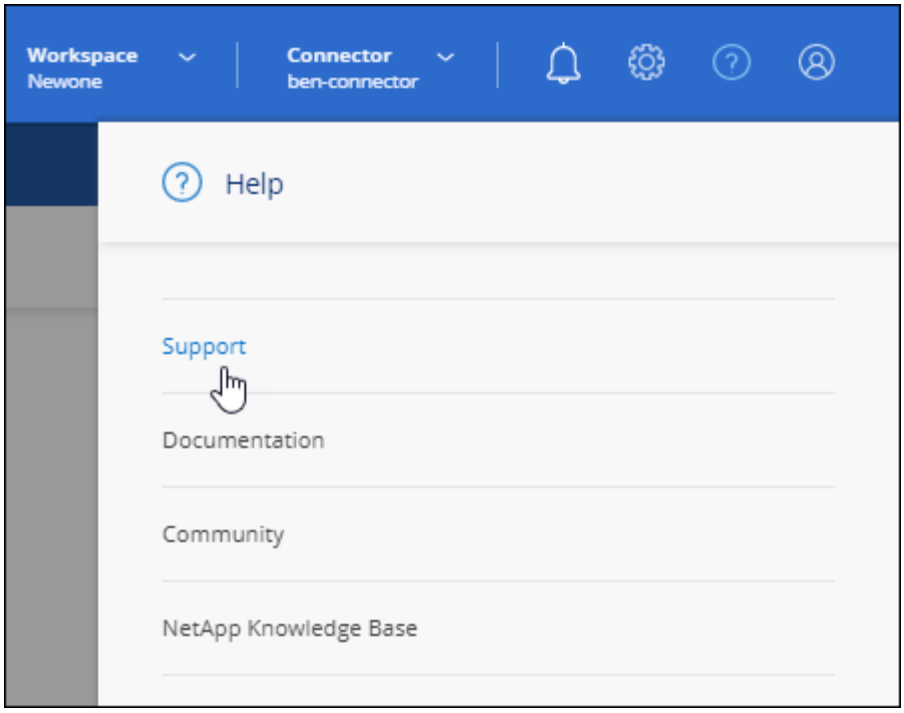

The Cloud Manager interface running on the Connector loads in a new browser tab.

## Download or send an AutoSupport message

If you're having problems, NetApp personnel might ask you to send an AutoSupport message to NetApp support for troubleshooting purposes.

**Steps**

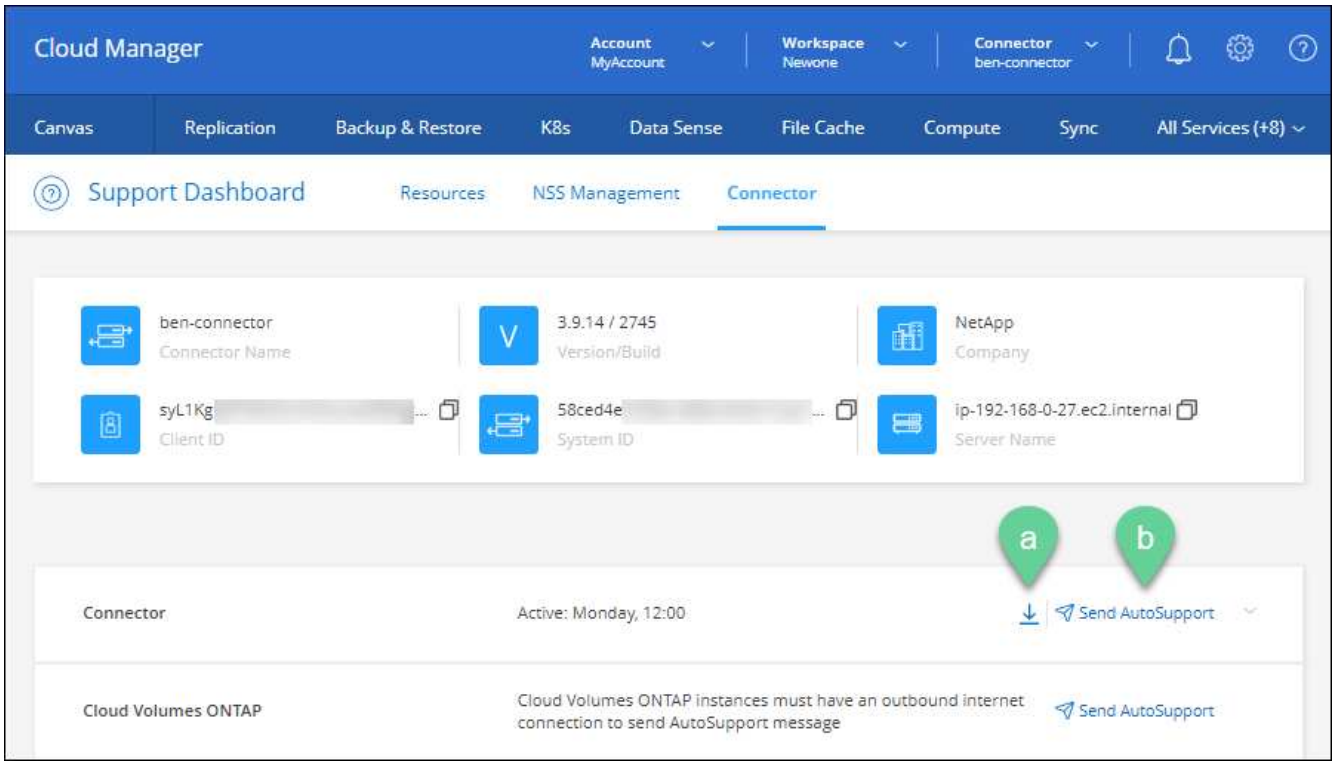
1. Connect to the Connector local UI, as described in the section above.
2. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.




3. Click **Connector**.
4. Depending on how you need to send the information to NetApp support, choose one of the following options:

   a. Select the option to download the AutoSupport message to your local machine. You can then send it to NetApp Support using a preferred method.

   b. Click **Send AutoSupport** to directly send the message to NetApp Support.



## Connect to the Linux VM

If you need to connect to the Linux VM that the Connector runs on, you can do so by using the connectivity options available from your cloud provider.

### AWS

When you created the Connector instance in AWS, you provided an AWS access key and secret key. You can use this key pair to SSH to the instance.

AWS Docs: Connect to your Linux instance

### Azure

When you created the Connector VM in Azure, you chose to authenticate with a password or SSH public key. Use the authentication method that you chose to connect to the VM.

Azure Docs: SSH into your VM

### Google Cloud

You can't specify an authentication method when you create a Connector in Google Cloud. However, you can connect to the Linux VM instance using the Google Cloud Console or Google Cloud CLI (gcloud).

Google Cloud Docs: Connect to Linux VMs

## Apply security updates

Update the operating system on the Connector to ensure that it's patched with the latest security updates.

### Steps

1. Access the CLI shell on the Connector host.
2. Run the following commands with elevated privileges:

```
sudo -s
service service-manager stop
yum -y update --security
service service-manager start
```

## Edit a Connector's URIs

Add and remove the URIs for a Connector.

### Steps

1. Click the **Connector** drop-down from the Cloud Manager header.
2. Click **Manage Connectors**.
3. Click the action menu for a Connector and click **Edit URIs**.
4. Add and remove URIs and then click **Apply**.

## Fix download failures when using a Google Cloud NAT gateway

The Connector automatically downloads software updates for Cloud Volumes ONTAP. The download can fail if your configuration uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. This step must be completed by using the Cloud Manager API.

**Step**

1. Submit a PUT request to /occm/config with the following JSON as body:

```
{
  "maxDownloadSessions": 32
}
```

The value for *maxDownloadSessions* can be 1 or any integer greater than 1. If the value is 1, then the downloaded image will not be divided.

Note that 32 is an example value. The value that you should use depends on your NAT configuration and the number of sessions that you can have simultaneously.

Learn more about the /occm/config API call.

## Upgrade the Connector on-prem without internet access

If you installed the Connector on an on-premises host that doesn't have internet access, you can upgrade the Connector when a newer version is available from the NetApp Support Site.

The Connector needs to restart during the upgrade process so the user interface will be unavailable during the upgrade.

**Steps**

1. Download the Cloud Manager software from the NetApp Support Site.
2. Copy the installer to the Linux host.
3. Assign permissions to run the script.

```
chmod +x /path/cloud-manager-connector-offline-v3.9.14
```

4. Run the installation script:

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. After the upgrade is complete, you can verify the Connector's version by going to **Help > Support > Connector**.

### What about software upgrades on hosts that have internet access?

The Connector automatically updates its software to the latest version, as long as it has outbound internet access to obtain the software update.

## Remove Connectors from Cloud Manager

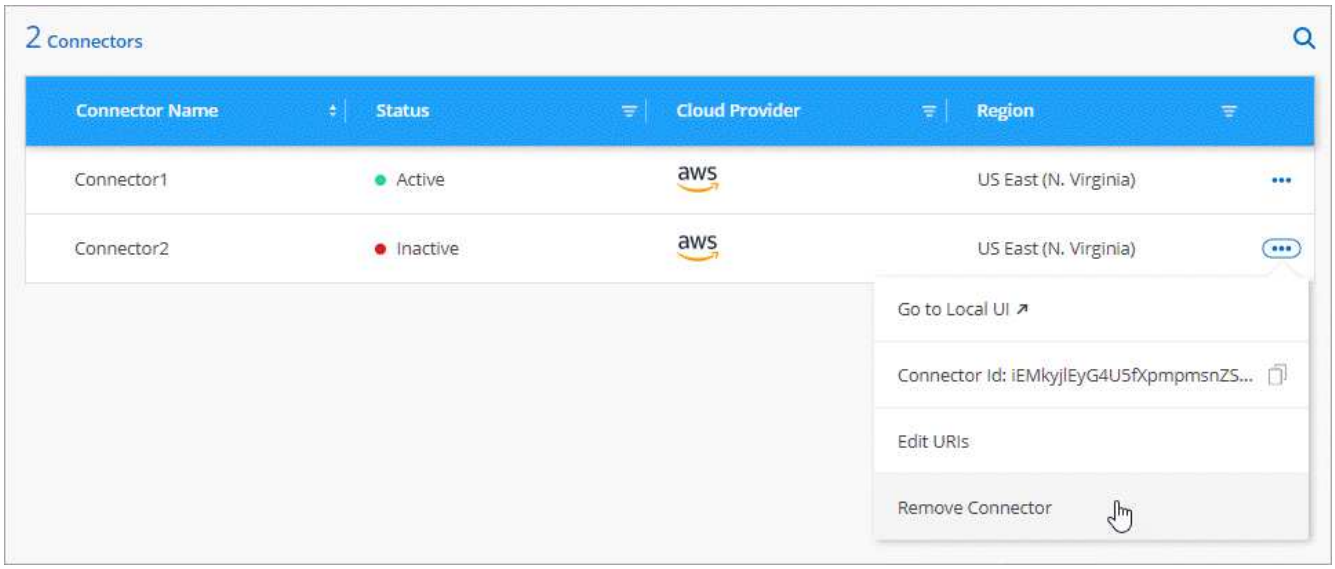
If a Connector is inactive, you can remove it from the list of Connectors in Cloud Manager. You might do this if you deleted the Connector virtual machine or if you uninstalled the Connector software.

Note the following about removing a Connector:

- This action doesn't delete the virtual machine.
- This action can't be reverted—once you remove a Connector from Cloud Manager, you can't add it back to Cloud Manager.

**Steps**

1. Click the **Connector** drop-down from the Cloud Manager header.
2. Click **Manage Connectors**.
3. Click the action menu for an inactive Connector and click **Remove Connector**.




4. Enter the name of the Connector to confirm and then click Remove.

**Result**

Cloud Manager removes the Connector from its records.

## Uninstall the Connector software

Uninstall the Connector software to troubleshoot issues or to permanently remove the software from the host. The steps that you need to use depends on whether you installed the Connector on a host that has internet access or a host in a restricted network that doesn't have internet access.

### Uninstall from a host with internet access

The online Connector includes an uninstallation script that you can use to uninstall the software.

**Step**

1. From the Linux host, run the uninstallation script:

   **/opt/application/netapp/cloudmanager/bin/uninstall.sh [silent]**

   *silent* runs the script without prompting you for confirmation.

### Uninstall from a host without internet access

Use these commands if you downloaded the Connector software from the NetApp Support Site and installed it in a restricted network that doesn't have internet access.

**Step**

1. From the Linux host, run the following commands:

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v
rm -rf /opt/application/netapp/ds
```

# Managing an HTTPS certificate for secure access

By default, Cloud Manager uses a self-signed certificate for HTTPS access to the web console. You can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate.

## Before you get started

You need to create a Connector before you can change Cloud Manager settings. Learn how.

## Installing an HTTPS certificate

Install a certificate signed by a CA for secure access.

**Steps**

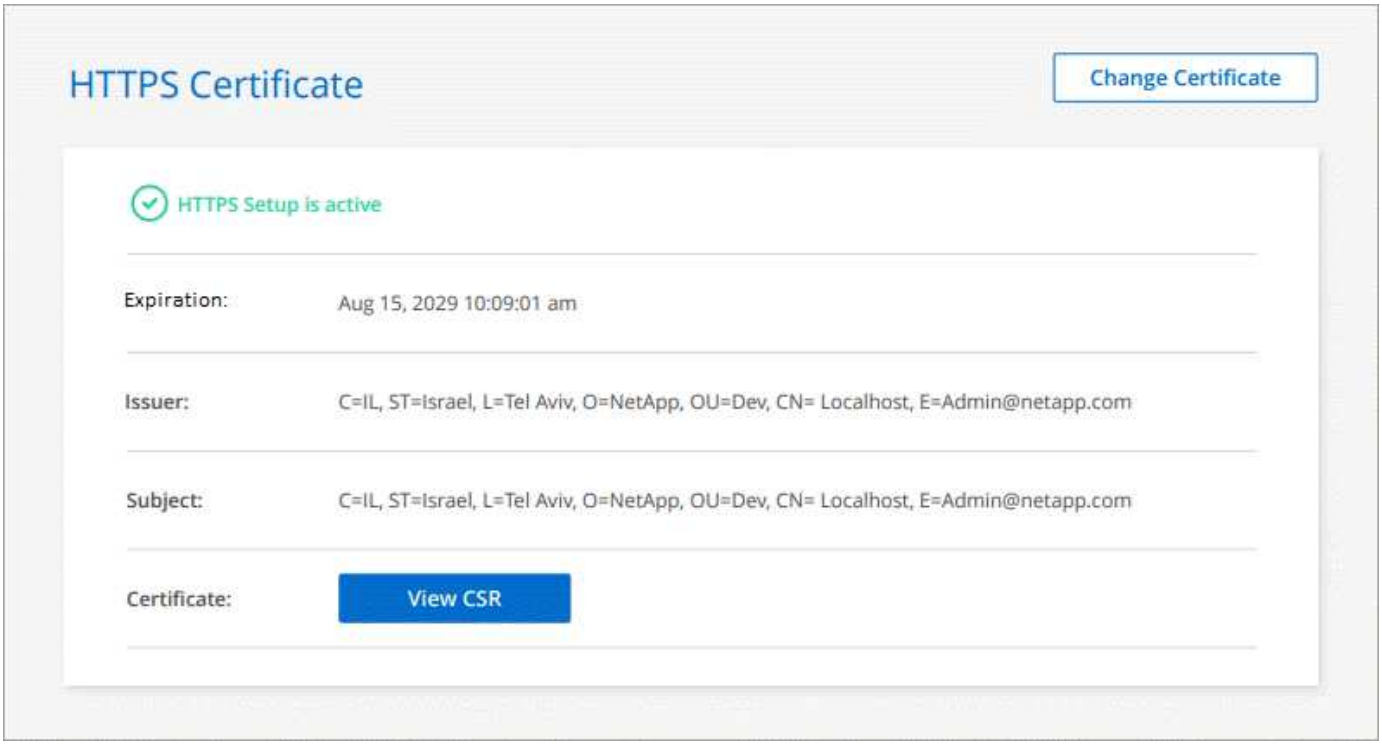
1. In the upper right of the Cloud Manager console, click the Settings icon, and select **HTTPS Setup**.


2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

| Option | Description |
| --- | --- |
| Generate a CSR | a. Enter the host name or DNS of the Connector host (its Common Name), and then click **Generate CSR**.<br><br>Cloud Manager displays a certificate signing request.<br><br>b. Use the CSR to submit an SSL certificate request to a CA.<br><br>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.<br><br>c. Upload the certificate file and then click **Install**. |
| Install your own CA-signed certificate | a. Select **Install CA-signed certificate**.<br>b. Load both the certificate file and the private key and then click **Install**.<br><br>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. |

**Result**

Cloud Manager now uses the CA-signed certificate to provide secure HTTPS access. The following image shows a Cloud Manager system that is configured for secure access:




## Renewing the Cloud Manager HTTPS certificate

You should renew the Cloud Manager HTTPS certificate before it expires to ensure secure access to the Cloud Manager web console. If you do not renew the certificate before it expires, a warning appears when users access the web console using HTTPS.

**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **HTTPS Setup**.

   Details about the Cloud Manager certificate displays, including the expiration date.

2. Click **Change Certificate** and follow the steps to generate a CSR or install your own CA-signed certificate.

**Result**

Cloud Manager uses the new CA-signed certificate to provide secure HTTPS access.

# Configuring a Connector to use an HTTP proxy server

If your corporate policies require you to use a proxy server for all HTTP communication to the internet, then you must configure your Connectors to use that HTTP proxy server. The proxy server can be in the cloud or in your network.

Cloud Manager doesn't support using an HTTPS proxy with the Connector.

## Enable a proxy on a Connector

When you configure a Connector to use a proxy server, that Connector and the Cloud Volumes ONTAP systems that it manages (including any HA mediators), all use the proxy server.

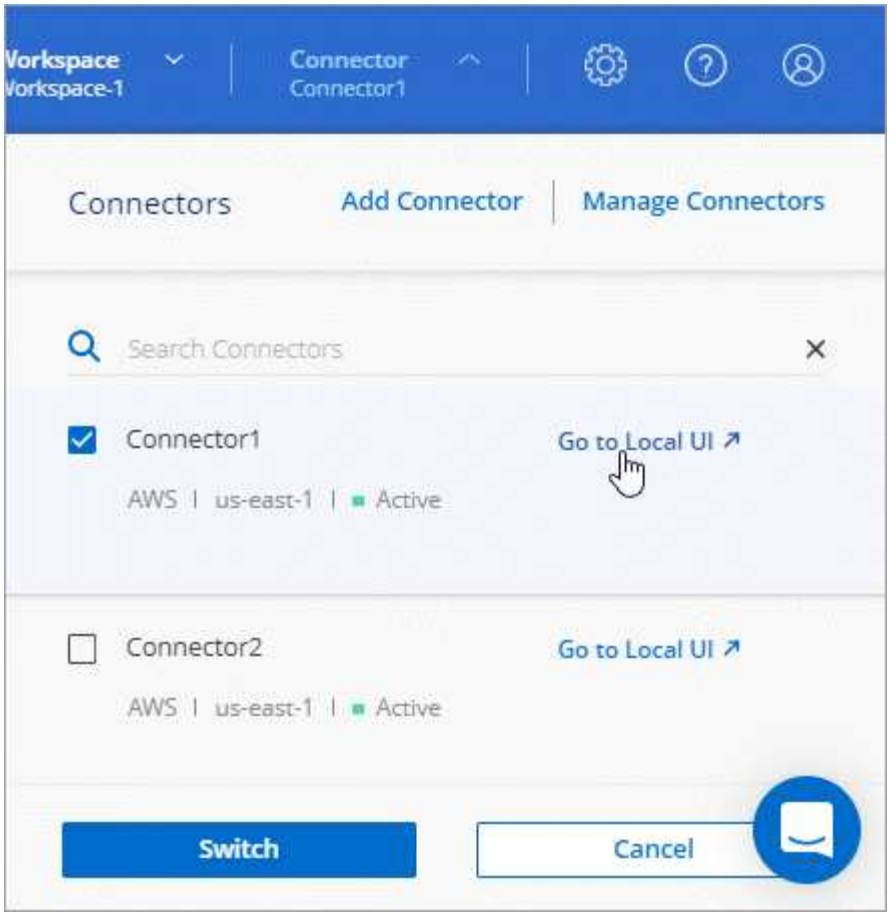
Note that this operation restarts the Connector. Ensure that the Connector isn't performing any operations before you proceed.

**Steps**

1. Log in to the Cloud Manager SaaS interface from a machine that has a network connection to the Connector instance.

   If the Connector doesn't have a public IP address, you'll need a VPN connection or you'll need to connect from a jump host that's in the same network as the Connector.

2. Click the **Connector** drop-down and then click **Go to local UI** for a specific Connector.




The Cloud Manager interface running on the Connector loads in a new browser tab.

3. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.


4. Under **General**, click **HTTP Proxy Configuration**.
5. Set up the proxy:
   a. Click **Enable Proxy**.
   b. Specify the server using the syntax http://*address:port*
   c. Specify a user name and password if basic authentication is required for the server
   d. Click **Save**.

   Cloud Manager doesn't support passwords that include the @ character.

**Result**

After you specify the proxy server, new Cloud Volumes ONTAP systems are automatically configured to use the proxy server when sending AutoSupport messages. If you didn't specify the proxy server before users create Cloud Volumes ONTAP systems, then they must use System Manager to manually set the proxy server in the AutoSupport options for each system.

### Enable direct API traffic

If you configured a proxy server, you can send API calls directly to Cloud Manager without going through the proxy. This option is supported with Connectors that are running in AWS, in Azure, or in Google Cloud.

**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.


2. Under **General**, click **Support Direct API Traffic**.
3. Click the checkbox to enable the option and then click **Save**.

# Default configuration for the Connector

If you need to troubleshoot the Connector, it might help to understand how it's configured.

## Default configuration with internet access

- If you deployed the Connector from Cloud Manager (or directly from a cloud provider's marketplace), note the following:
  - In AWS, the user name for the EC2 Linux instance is ec2-user.
  - The operating system for the image is as follows:
    - AWS: Red Hat Enterprise Linux 7.6 (HVM)
    - Azure: CentOS 7.6
    - GCP: CentOS 7.9

      The operating system does not include a GUI. You must use a terminal to access the system.
- When deployed from Cloud Manager, the default system disk is as follows:
  - AWS: 50 GiB gp2 disk
  - Azure: 100 GiB premium SSD disk
  - Google Cloud: 100 GiB SSD persistent disk
- The Connector installation folder resides in the following location:

  /opt/application/netapp/cloudmanager
- Log files are contained in the following folders:
  - /opt/application/netapp/cloudmanager/log

    The logs in this folder provide details about the Connector and docker images.
  - /opt/application/netapp/cloudmanager/docker_occm/data/log

    The logs in this folder provide details about cloud services and the Cloud Manager service that runs on the Connector.

- The Cloud Manager service is named occm.
- The occm service is dependent on the MySQL service.

  If the MySQL service is down, then the occm service is down too.

- Cloud Manager installs the following packages on the Linux host, if they are not already installed:
  - 7Zip
  - AWSCLI
  - Docker
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Pull
  - Wget
- The Connector uses the following ports on the Linux host:
  - 80 for HTTP access
  - 443 for HTTPS access
  - 3306 for the Cloud Manager database
  - 8080 for the Cloud Manager API proxy
  - 8666 for the Service Manager API
  - 8777 for the Health-Checker Container Service API

## Default configuration without internet access

The following configuration applies if you manually installed the Connector on an on-premises Linux host that doesn't have internet access. Learn more about this installation option.

- The Connector installation folder resides in the following location:

  /opt/application/netapp/ds

- Log files are contained in the following folders:

  /var/lib/docker/volumes/ds_occmdata/_data/log

  The logs in this folder provide details about the Connector and docker images.

- All services are running inside docker containers

  The services are dependent on the docker runtime service running

- The Connector uses the following ports on the Linux host:
  - 80 for HTTP access
  - 443 for HTTPS access