# Cisco Spaces: Connector AMI



# Downloading and Deploying the Cisco Spaces: Connector AMI

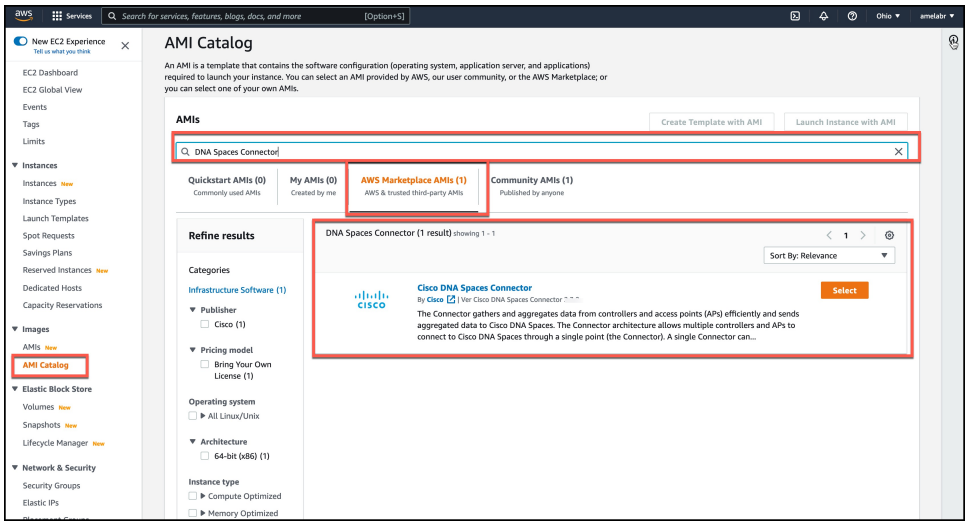
This chapter provides information about how to download and deploy the Cisco Spaces: Connector and obtain the URL for the Connector GUI.

**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.



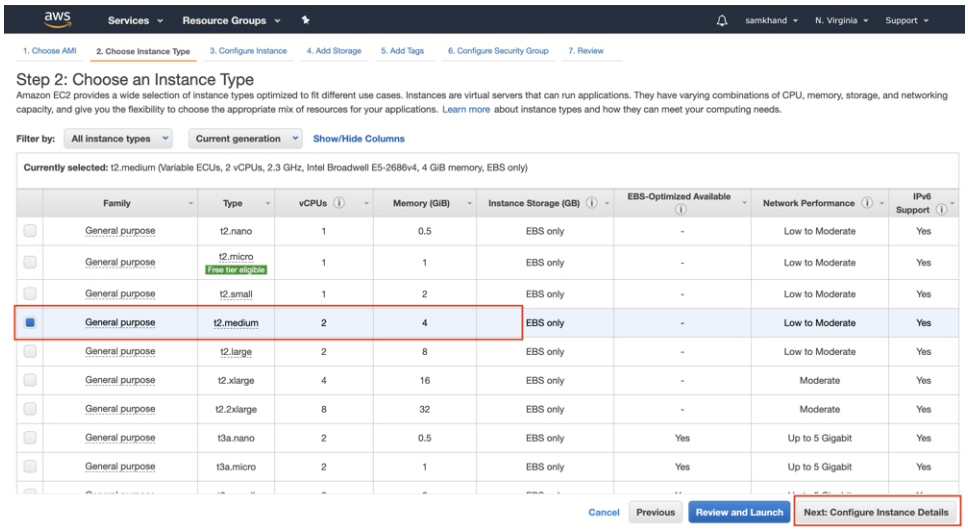

**Step 3** Click the displayed image and click **Select**.

**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**.

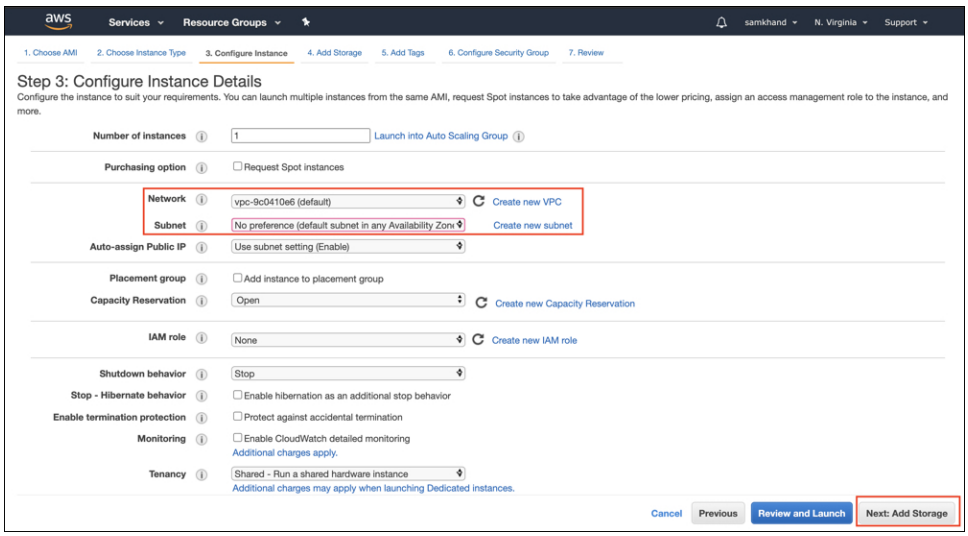



**Note** You can choose to have a more advanced configuration by choosing an option with higher vCPU and memory configurations. You can choose an instance type with the following configurations. If an exact match is unavailable, you can choose a configuration with the next-available vCPU or memory:

- 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)

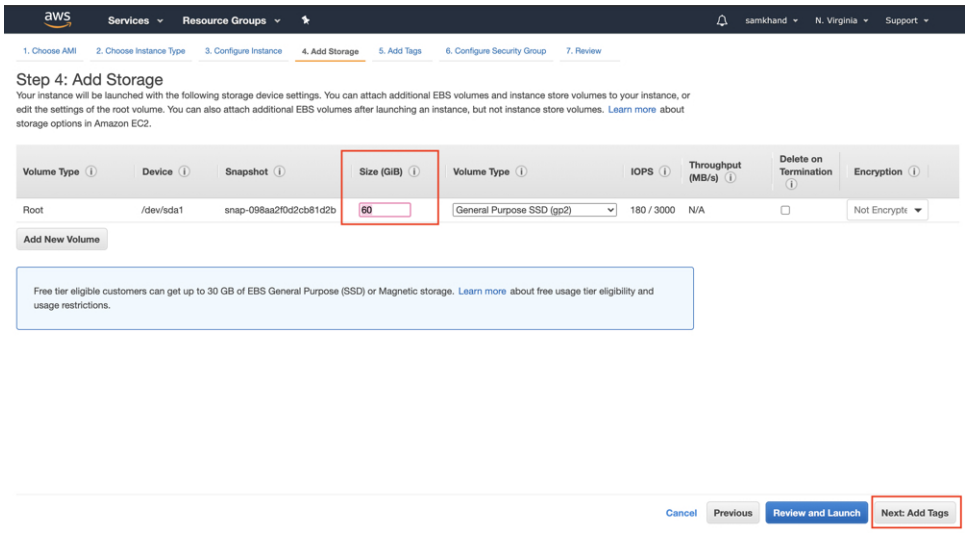
**Step 7** Choose a **Network** and a **Subnet**. Click **Next: Add Storage**.

*Figure 1: Configure Instance Details*




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

*Figure 2: Add Storage*




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

*Figure 3: Add Tags*

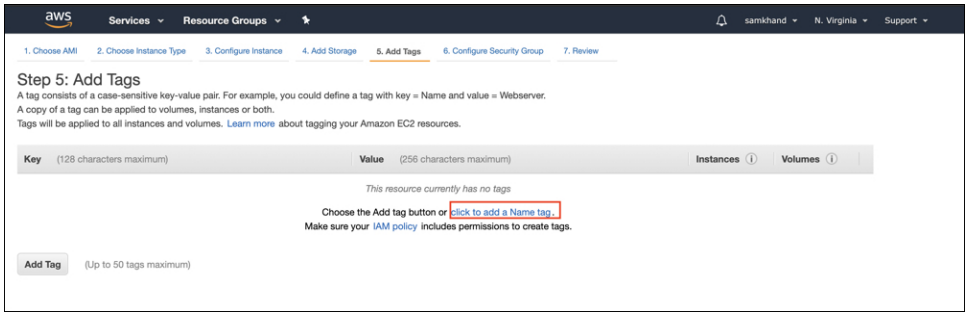
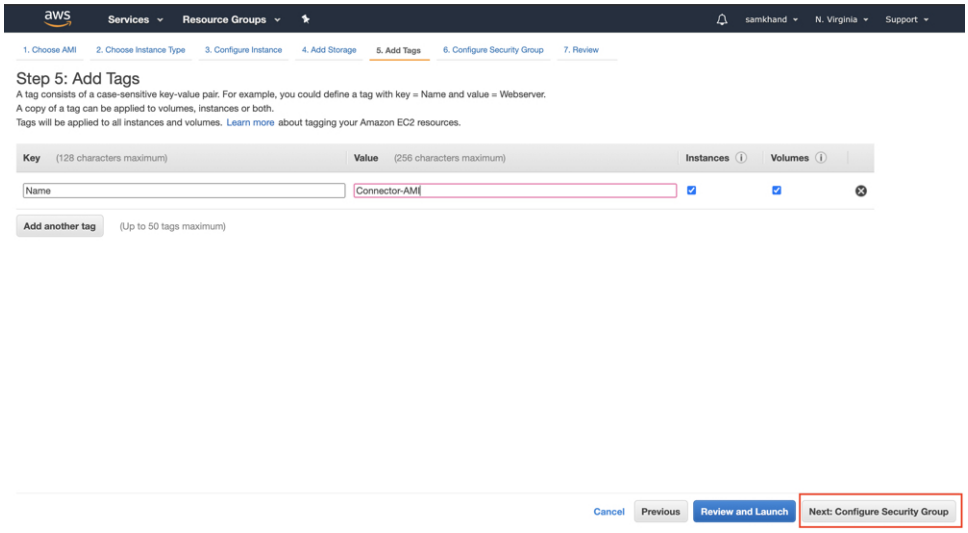


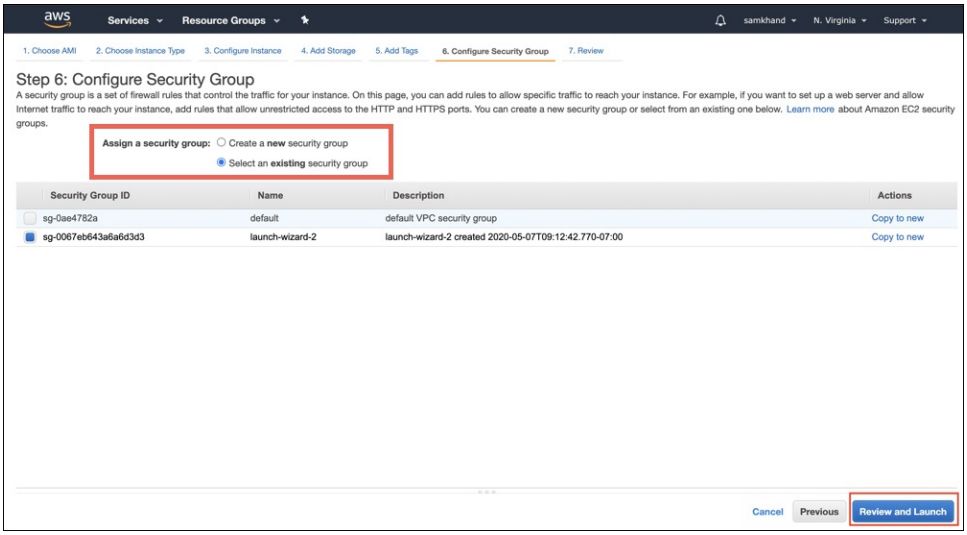

*Figure 4: Enter a Tag Name*




**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.

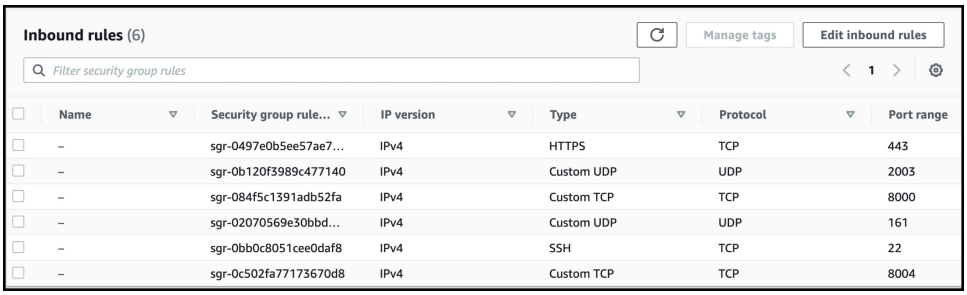
***Figure 5: Configure Security Group***




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 6: Configure Ports with Rules for Inbound Traffic***

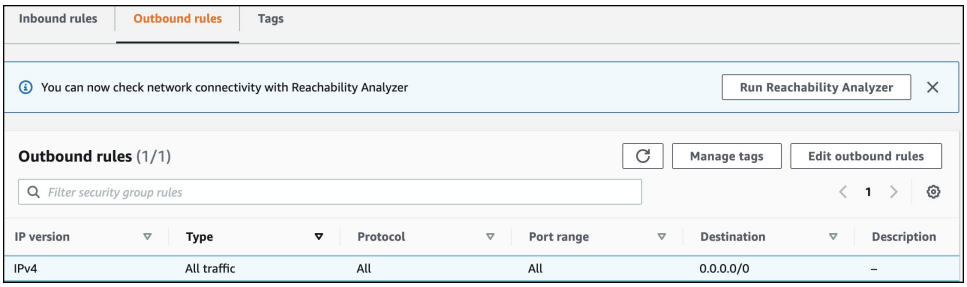



**Note** Specify the network subnet ranges within the inbound rule to access this instance using SSH.

c) Configure ports with rules for outbound traffic.

Configure the outbound rule indicated in the following image:

***Figure 7: Configure Ports with Rules for Outbound Traffic***

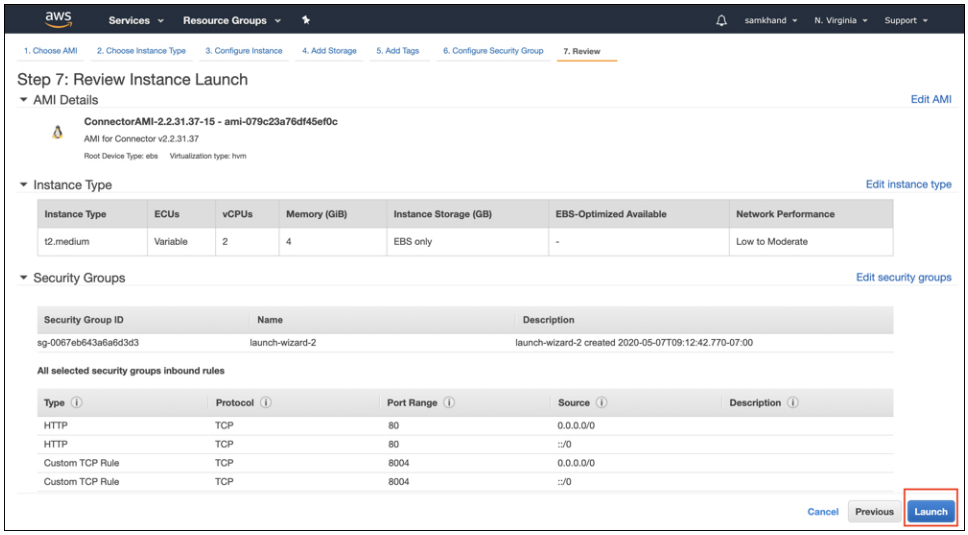


**Note** See Information About Open Ports (Wireless) for details on ports that you must open for various services to work.

d) Click **Review and Launch**.

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

***Figure 8: Review Instance and Launch***




**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 9: Create a New Key Pair***

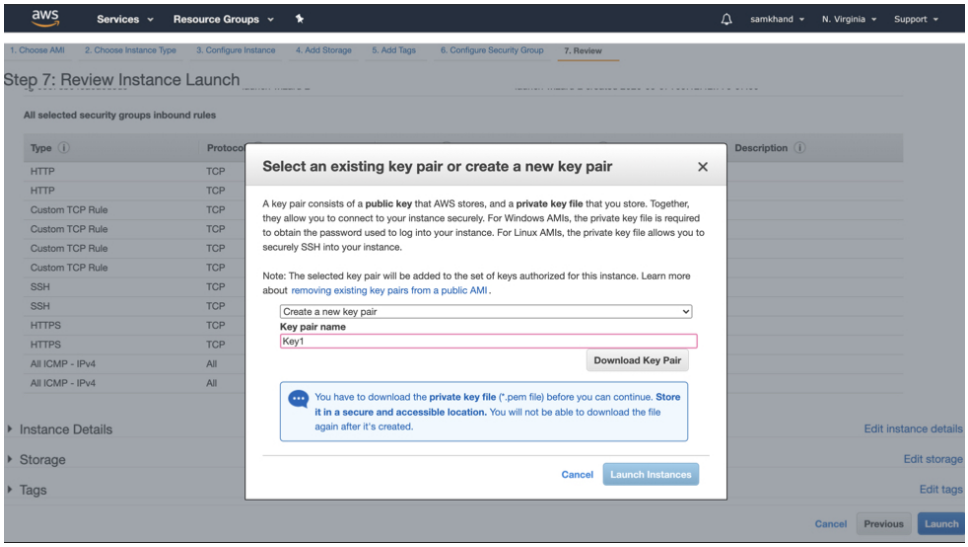
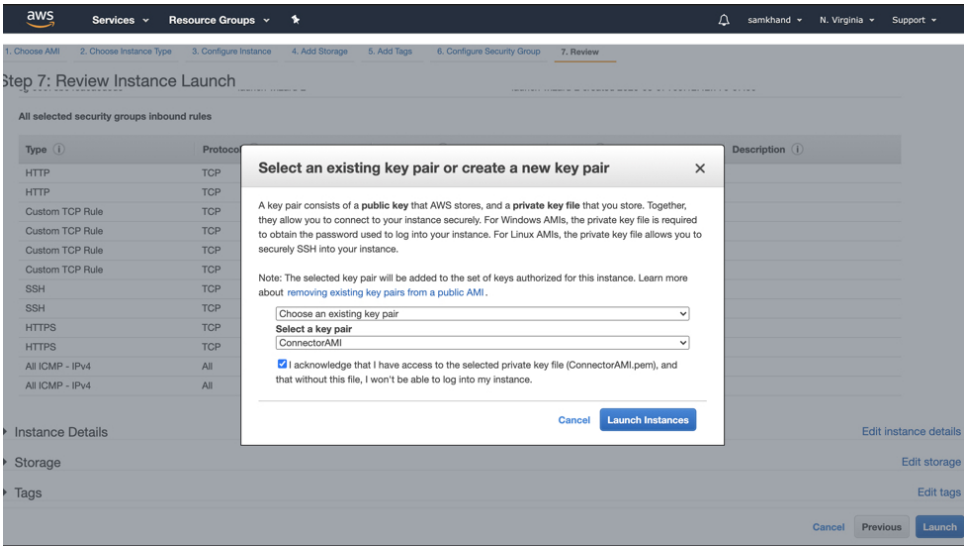


*Figure 10: Choose an Existing Key Pair*

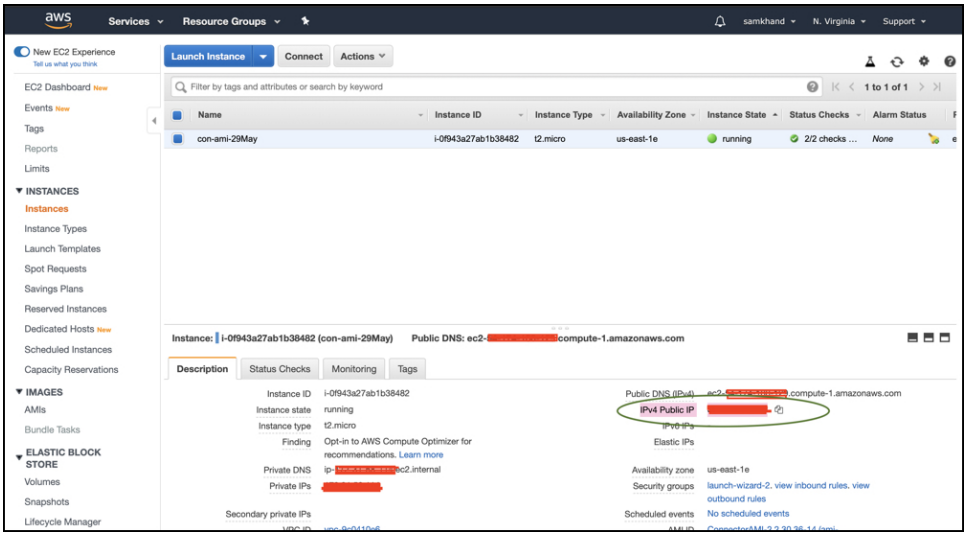



**Step 13** Once you download the key pair (.pem) file to your system, navigate to the file location. Using the **chmod** command, configure appropriate permissions for the .pem file.

```
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 11: Instances Page and IPv4 Address*




**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
```