Accessing the Command Line Interface (CLI) of Your Cloud Email Security (CES) Solution

Contents

Introduction

This document describes how to access the CLI of your CES devices by utilizing Secure Shell (SSH) on either the Windows or Linux/macOS platform.

Contributed by Dennis McCabe Jr, Cisco TAC Engineer.

Background Information

There are two stages that need to be completed in order to access the CLI of your CES Email Security Appliance (ESA) or Security Management Appliance (SMA), both of which will be discussed in detail below.

1. Generating an SSH key pair
2. Configuring the SSH client

> **Note: The directions below should cover the bulk of operating systems used in the wild; however, if what you're using is not listed or you still need assistance, please contact Cisco TAC and we will do our best to provide specific instruction. These are just a small snippet of the tools and clients available that can be used to accomplish this task.**

Definitions

Please familiarize yourself with some of the terminologies that will be used in this article.

Proxy Servers

These are the CES SSH proxy servers you will use to initiate the SSH connection to your CES instance. You will need to utilize a proxy server specific to the region your device is located in. For example, if your login hostname is **esa1.test.iphmx.com**, you would use one of the **iphmx.com** proxy servers in the **US** region.

- **AP (ap.iphmx.com)** f15-ssh.ap.iphmx.comf16-ssh.ap.iphmx.com
- **AWS (r1.ces.cisco.com)** p3-ssh.r1.ces.cisco.comp4-ssh.r1.ces.cisco.com
- **CA (ca.iphmx.com)**
  f13-ssh.ca.iphmx.comf14-ssh.ca.iphmx.com
- **EU (c3s2.iphmx.com)** f10-ssh.c3s2.iphmx.comf11-ssh.c3s2.iphmx.com
- **EU (eu.iphmx.com)** f17-ssh.eu.iphmx.comf18-ssh.eu.iphmx.com
- **US (iphmx.com)** f4-ssh.iphmx.comf5-ssh.iphmx.com

Login Hostname

This is the non-proxy hostname of your CES ESA or SMA and will start with something like esa1 or sma1, and can be found in the top-right of the web page when you go to log in to the Web User Interface (WUI). The format should be as follows : esa[1-20].<allocation>.<datacenter>.com or sma[1-20].<allocation>.<datacenter>.com.

Generating an SSH Key Pair

In order to get started on accessing your CES devices, the first thing you will need to do is generate a private/public SSH key pair and then provide the public key to Cisco TAC. Once Cisco TAC has imported your public key, you can then proceed to the next steps. **Do not share your private key**.

For either steps below, the **key type** should be **RSA** with a standard **bit length** of **2048**.

For Windows:

PuTTYgen or a similar tool can be used for generating key pairs. You can also follow the instructions below if you utilize the Windows Subsystem for Linux (WSL).

For Linux/macOS:

From a new terminal window, you can run ssh-keygen to create a key pair.

Example:

```
ssh-keygen -t rsa -b 2048 -f ~/.ssh/mykey
```

Where:

```
ssh-keygen -t <key type> -b <bit length> -f <filename>
```

Once an SSH key pair has been created, please provide your public key to Cisco TAC for import and then proceed to client configuration. **Do not share your private key**.

Configuring the SSH Client

> **Note: The SSH connection for CLI access is not made directly to your CES device, but instead through an SSH tunnel forward via your localhost which is directly connected to one of our SSH proxies. The first part of the connection will be to one of our proxy servers and the second will be to the SSH tunnel forwarding port on your localhost.**

For Windows:

We will be using PuTTY for our example, so please note that steps may need to be modified slightly if using a different client. Also, please make sure that whichever client you're using has been updated to the most recently available version.

Windows - Step One - Connect to SSH Proxy and Open Forwarding Port

1. For the **hostname**, enter in the **proxy server** applicable to your CES allocation.
2. Expand **Connection**, click **Data** and enter **dh-user** for the auto-login username.
3. With **Connection** still expanded, click **SSH** and check to enable **Don't start a shell or command at all**.
4. Expand **SSH**, click **Auth** and **browse** to your newly created private key.
5. With **SSH** still expanded, click **Tunnels**, supply a **source port** for **local** forwarding (any available port on your device), enter in the **login hostname** (not the hostname that starts with dh) of your CES device and then click **Add**. In case you wish to add multiple devices (ie: esa1, esa2, and sma1), you can add additional source ports and hostnames. Then, any added ports will be forwarded when this session is started.
6. Once the above steps have been completed, proceed back to the **session** category and then name and **save** your session.

Windows - Step Two - Connecting to the CLI of Your CES Device

1. Open and connect to the session you just created.
2. **While keeping the SSH proxy server session open, open a new PuTTY session by right-clicking on the window and selecting New Session, enter 127.0.0.1 for the IP address, enter the source port used previously in step 5 and then click Open.**
3. Once you click **Open**, you will be prompted to enter your CES credentials and should then have access to the CLI. (These would be the same credentials used to access the WUI)

For Linux/macOS:

Linux/macOS - Step One - Connect to SSH Proxy and Open Forwarding Port

1. From a new terminal window, enter the following command:

```
ssh -i ~/.ssh/id_rsa -l dh-user -N -f f4-ssh.iphmx.com -L 2200:esa1.test.iphmx.com:22
```

Where:

```
ssh -i <your private key> -l dh-user -N -f <proxy server for your allocation> -L <source
```

```
port>:<login hostname>:22
```
This will open a port on your local client to be forwarded to the given host and port on the remote side.

Linux/macOS - Step Two - Connecting to the CLI of Your CES Device

1. From the same or new terminal window, enter the command below. Once entered, you will be prompted to enter your CES password and should then have access to the CLI. (These would be the same credentials used to access the WUI)

```
ssh dmccabej@127.0.0.1 -p 2200
```
Where:

```
ssh <your CES username>@127.0.0.1 -p <source port for forwarding assigned in previous step>
```