# Opdracht Line Interface (CLI) van uw Cloud Email Security (CES)-oplossing

## Inhoud



## Inleiding

Dit document beschrijft hoe u toegang krijgt tot de CLI van uw CES-apparaten door gebruik te maken van Secure Shell (SSH) op het Windows- of Linux/macOS-platform.

Bijgedragen door Dennis McCabe Jr, Cisco TAC Engineer.

## Achtergrondinformatie

Er zijn twee stappen die moeten worden voltooid om toegang te hebben tot de CLI van uw CES Email Security Appliance (ESA) of Security Management Appliance (SMA). Beide worden hieronder in detail besproken.

1. Een SSH-sleutelpaar genereren
2. De SSH-client configureren

**Noot: De onderstaande aanwijzingen dienen betrekking te hebben op het merendeel van de in het wild gebruikte besturingssystemen; als echter niet is vermeld wat u gebruikt of u nog steeds ondersteuning nodig hebt, neemt u contact op met Cisco TAC en wij doen ons best om specifieke instructies te geven. Dit zijn slechts een klein fragment van de beschikbare gereedschappen en klanten die kunnen worden gebruikt om deze taak uit te voeren.**

## Definities

Zorg ervoor dat u bekend raakt met een aantal terminologieën die in dit artikel zullen worden gebruikt.

### Proxyservers

Dit zijn de CES SSH-proxyservers die u gebruikt om de SSH-verbinding naar uw CES-instantie te openen. U moet een proxy server gebruiken die specifiek is voor het gebied waarin uw apparaat zich bevindt. Als uw login hostname bijvoorbeeld **esa1.test.iphmx.com** is, zou u één van de **iphmx.com** proxy-servers in de **Amerikaanse** regio gebruiken.

- **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
- **VS (iphmx.com)** f4-ssh.iphmx.comf5-ssh.iphmx.com

**Login Hostname**

Dit is de niet-proxy hostname van uw CES ESA of SMA en zal starten met iets als esa1 of sma1, en kan rechtsboven op de webpagina worden gevonden wanneer u inlogt bij de Web User Interface (WUI). Het formaat moet als volgt zijn: esa[1-20].<toewijzing>.<datacenter>.com of sma[1-20].<toewijzing>.<datacenter>.com.

# Een SSH-sleutelpaar genereren

Om te beginnen bij het toegang tot uw CES-apparaten, moet u eerst een privaat/openbaar SSH-sleutelpaar genereren en vervolgens de openbare sleutel naar Cisco TAC leveren. Nadat Cisco TAC uw openbare sleutel heeft geïmporteerd, kunt u vervolgens de volgende stappen uitvoeren. **Deel uw privésleutel niet**.

Voor beide onderstaande stappen moet het **sleuteltype RSA** zijn met een standaard **bit lengte** van **2048**.

**Voor Windows:**

PuTTYgen of een soortgelijk gereedschap kan worden gebruikt voor het genereren van sleutelparen. U kunt de onderstaande instructies ook opvolgen als u het Windows Subsysteem voor Linux (WSL) gebruikt.

**Voor Linux/macOS:**

Vanuit een nieuw eindvenster kunt u ssh-keygen draaien om een sleutelpaar te maken.

Voorbeeld:

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

Wanneer:

```
ssh-keygen -t
```

Nadat een SSH-sleutelpaar is gemaakt, specificeert u uw openbare sleutel naar Cisco TAC voor import en gaat u vervolgens naar de clientconfiguratie. **Deel uw privésleutel niet**.

# De SSH-client configureren

> **Opmerking: de SSH-verbinding voor CLI-toegang is niet rechtstreeks aan uw CES-apparaat gekoppeld, maar in plaats daarvan via een SSH-tunnel voorwaarts via uw lokale host, die rechtstreeks is aangesloten op een van onze SSH-proxy's. Het eerste deel van de verbinding zal zijn naar één van onze proxy servers en het tweede zal zijn naar de SSH tunneldoorvoerpoort op uw lokale host.**

**Voor Windows:**

We zullen PuTTY voor ons voorbeeld gebruiken, dus let op dat stappen licht aangepast moeten worden als je een andere client gebruikt. Zorg er ook voor dat de client die u gebruikt, is bijgewerkt tot de meest recente beschikbare versie.

**Windows - Stap één - Connect met SSH Proxy en Open Forwarding Port**

1. Voor de **hostname**, voer in de **proxy server in** die van toepassing is op uw CES-toewijzing.
2. Uitbreidt **de verbinding**, klikt op **Gegevens** en voert **dh-gebruiker** in voor de gebruikersnaam voor de automatische inlognaam.
3. Als de **verbinding** nog steeds is uitgebreid, klikt u op **SSH** en vervolgens controleert u of **de shell of opdracht helemaal niet zijn gestart**.
4. **SSH uitvouwen, op Auth klikken en doorbladeren naar de nieuwe privé-toets.**
5. Als **SSH** nog steeds is uitgebreid, klikt u op **tunnels**, levert u een **bronpoort** voor **lokaal** verzenden (een beschikbare poort op uw apparaat), voert u de **inloghostname (niet de hostname die met dh begint) van uw CES-apparaat in en klikt u vervolgens op Toevoegen.** Als u meerdere apparaten wilt toevoegen (bijvoorbeeld: esa1, esa2 en sma1), kunt u extra bronpoorten en hostname toevoegen. Alle extra poorten worden ook doorgestuurd als deze sessie wordt gestart.
6. Nadat de bovenstaande stappen zijn voltooid, gaat u terug naar de **sessiecategorie** en opgeslaat u de naam en **slaat u** de sessie op.

**Windows - Stap 2 - Voor het aansluiten op de CLI van uw CES-apparaat**

1. Open de sessie die u zojuist hebt gemaakt.
2. **Terwijl u de SSH-proxyserversessie open houdt, opent u een nieuwe PuTTY-sessie door met de rechtermuisknop op het venster te klikken en Nieuwe sessie te selecteren, voer 127.0.0.1 voor het IP-adres in, voer u de bronpoort in die eerder in stap 5 is gebruikt en klik vervolgens op Open.**
3. Zodra u op **Open** klikt, wordt u gevraagd om uw CES-referenties in te voeren en moet u dan toegang hebben tot de CLI (dit zijn de zelfde geloofsbrieven die worden gebruikt om tot de WUI te toegang)

**Voor Linux/macOS:**

**Linux/macOS - Stap één - Connect met SSH-proxy en Open Forwarding Port**

1. Voer vanuit een nieuw venster de volgende opdracht in:

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

```
ssh -i
```
Hierdoor wordt een poort op uw lokale client geopend die naar de gegeven host en poort op de afstandszijde wordt doorgestuurd.

### Linux/macOS - Stap 2 - Voor aansluiting op de CLI van uw CES-apparaat

1. Voer vanuit hetzelfde of nieuw terminalvenster de onderstaande opdracht in. Zodra ingevoerd zal u worden gevraagd uw CES wachtwoord in te voeren en zou dan toegang tot CLI moeten hebben. (Dit zouden de zelfde geloofsbrieven zijn die worden gebruikt om tot de WUI toegang te hebben)

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

```
ssh
```