# Accès à l'interface de ligne de commande (CLI) de votre solution de sécurisation de la messagerie électronique cloud (CES)

## Contenu



## Introduction

Ce document décrit comment accéder à l'interface de ligne de commande de vos périphériques CES en utilisant Secure Shell (SSH) sur la plate-forme Windows ou Linux/macOS.

Contribué par Dennis McCabe Jr, ingénieur TAC Cisco.

## Informations générales

Deux étapes doivent être effectuées pour accéder à l'interface de ligne de commande de votre dispositif de sécurité de la messagerie électronique CES (ESA) ou de votre dispositif de gestion de la sécurité (SMA). Ces deux étapes seront décrites en détail ci-dessous.

1. Génération d'une paire de clés SSH
2. Configuration du client SSH

**Note : Les instructions ci-après devraient porter sur la majeure partie des systèmes d'exploitation utilisés dans la nature ; toutefois, si ce que vous utilisez n'est pas répertorié ou si vous avez encore besoin d'assistance, contactez le TAC Cisco et nous ferons de notre mieux pour fournir des instructions spécifiques. Il ne s'agit que d'un petit extrait des outils et des clients disponibles qui peuvent être utilisés pour accomplir cette tâche.**

## Définitions

Veuillez vous familiariser avec certaines des terminologies qui seront utilisées dans cet article.

### Serveurs proxy

Il s'agit des serveurs proxy SSH CES que vous utiliserez pour initier la connexion SSH à votre instance CES. Vous devez utiliser un serveur proxy spécifique à la région dans laquelle se trouve votre périphérique. Par exemple, si votre nom d'hôte de connexion est **esa1.test.iphmx.com**, vous utiliseriez l'un des serveurs proxy **iphmx.com** dans la région **américaine**.

- **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
- **UE (c3s2.iphmx.com)** f10-ssh.c3s2.iphmx.comf11-ssh.c3s2.iphmx.com
- **UE (eu.iphmx.com)** f17-ssh.eu.iphmx.comf18-ssh.eu.iphmx.com
- **États-Unis (iphmx.com)** f4-ssh.iphmx.comf5-ssh.iphmx.com

### Nom d'hôte de connexion

Il s'agit du nom d'hôte non proxy de votre ESA ou SMA CES et commence par quelque chose comme esa1 ou sma1. Il se trouve en haut à droite de la page Web lorsque vous accédez à l'interface utilisateur Web (WUI). Le format doit être le suivant : esa[1-20].<allocation>.<datacenter>.com ou sma[1-20].<allocation>.<datacenter>.com.

## Génération d'une paire de clés SSH

Pour commencer à accéder à vos périphériques CES, vous devez tout d'abord générer une paire de clés SSH privée/publique, puis fournir la clé publique au TAC Cisco. Une fois que le centre d'assistance technique Cisco a importé votre clé publique, vous pouvez passer aux étapes suivantes. **Ne partagez pas votre clé privée**.

Pour les deux étapes ci-dessous, le **type de clé** doit être **RSA** avec une **longueur de bit** standard de **2048**.

### Pour Windows :

PuTTYgen ou un outil similaire peut être utilisé pour générer des paires de clés. Vous pouvez également suivre les instructions ci-dessous si vous utilisez le sous-système Windows pour Linux (WSL).

### Pour Linux/macOS :

À partir d'une nouvelle fenêtre de terminal, vous pouvez exécuter ssh-keygen pour créer une paire de clés.

Exemple :

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

Where:

```
ssh-keygen -t
```

Une fois qu'une paire de clés SSH a été créée, fournissez votre clé publique au centre d'assistance technique Cisco pour l'importation, puis passez à la configuration du client. **Ne partagez pas votre clé privée**.

# Configuration du client SSH

> **Remarque : la connexion SSH pour l'accès CLI n'est pas directement établie sur votre périphérique CES, mais via un tunnel SSH avant via votre hôte local qui est directement connecté à l'un de nos serveurs proxy SSH. La première partie de la connexion sera vers l'un de nos serveurs proxy et la seconde sera vers le port de transfert de tunnel SSH sur votre hôte local.**

**Pour Windows :**

Nous utiliserons PuTTY pour notre exemple. Veuillez donc noter que les étapes peuvent avoir besoin d'être légèrement modifiées si vous utilisez un autre client. Assurez-vous également que le client que vous utilisez a été mis à jour avec la dernière version disponible.

**Windows - Étape 1 - Connexion au proxy SSH et au port de transfert ouvert**

1. Pour le **nom d'hôte**, saisissez dans le **serveur proxy** applicable à votre allocation CES.
2. Développez **Connection**, cliquez sur **Data** et entrez **dh-user** pour le nom d'utilisateur de connexion automatique.
3. Avec **Connection** toujours développé, cliquez sur **SSH** et cochez la case pour activer **Ne pas démarrer un shell ou une commande du tout**.
4. Développez **SSH**, cliquez sur **Auth** et **accédez** à votre nouvelle clé privée.
5. Avec SSH toujours développé, cliquez sur Tunnels, fournissez un port source pour le transfert **local** (n'importe quel port disponible sur votre périphérique), entrez le **nom d'hôte de connexion** (pas le nom d'hôte qui commence par dh) de votre périphérique CES, puis cliquez sur **Add**. Si vous souhaitez ajouter plusieurs périphériques (par exemple : esa1, esa2 et sma1), vous pouvez ajouter des ports source et des noms d'hôte supplémentaires. Ensuite, tous les ports ajoutés seront transférés au démarrage de cette session.
6. Une fois les étapes ci-dessus terminées, revenez à la catégorie **session**, puis nommez et **enregistrez** votre session.

**Windows - Étape 2 - Connexion à l'interface de ligne de commande de votre périphérique CES**

1. Ouvrez et connectez-vous à la session que vous venez de créer.
2. **Tout en maintenant la session du serveur proxy SSH ouverte, ouvrez une nouvelle session PuTTY en cliquant avec le bouton droit sur la fenêtre et en sélectionnant Nouvelle session, entrez 127.0.0.1 pour l'adresse IP, entrez le port source utilisé précédemment à l'étape 5, puis cliquez sur Ouvrir.**
3. Une fois que vous avez cliqué sur **Ouvrir**, vous serez invité à saisir vos informations d'identification CES et vous devriez alors avoir accès à l'interface de ligne de commande. (Il s'agirait des mêmes informations d'identification utilisées pour accéder à l'interface utilisateur WUI)

### Pour Linux/macOS :

### Linux/macOS - Étape 1 : connexion au proxy SSH et au port de transfert ouvert

1. Dans une nouvelle fenêtre de terminal, entrez la commande suivante :

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

Where:

```
ssh -i
```

Ceci ouvrira un port sur votre client local pour être transféré à l'hôte et au port donnés sur le côté distant.

### Linux/macOS - Étape 2 - Connexion à l'interface de ligne de commande de votre périphérique CES

1. Dans la même fenêtre ou dans la nouvelle fenêtre de terminal, entrez la commande ci-dessous. Une fois entré, vous serez invité à saisir votre mot de passe CES et à accéder à l'interface de ligne de commande. (Il s'agirait des mêmes informations d'identification utilisées pour accéder à l'interface utilisateur WUI)

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

Where:

```
ssh
```