

使用SCP從CES SMA下載允許清單/阻止清單檔案

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[解決方案](#)

[對於Windows](#)

[對於Linux/macOS](#)

[相關內容](#)

簡介

本文檔介紹如何使用SCP for Cloud Email Security從雲安全管理裝置下載允許清單/阻止清單檔案。

必要條件

此過程需要命令列介面(CLI)訪問許可權。它使用安全複製協定(SCP)實現雲郵件安全(CES)。



附註：本文檔中的示例值是佔位符。用部署的值替換它們。

需求

- 確保可以訪問SMA上的命令列介面(CLI)。
- Windows:已安裝PuTTY和PSCP。
- Linux/macOS:已安裝OpenSSH客戶端工具(ssh和scp)。
- 如果需要，確保可以訪問SSH代理主機。
- 記錄為SMA CLI訪問配置的本地轉發埠。
- 記錄CES使用者名稱。
- 如果需要基於金鑰的身份驗證，請記錄私鑰檔案路徑。

請參閱[存取Cloud Email Security\(CES\)解決方案的指令行介面\(CLI\)](#)。

解決方案

allowlist/blocklist(SLBL)CSV檔案儲存在SMA的/configuration/下。如果不知道確切的檔名，請列出可用檔案並按檔名和時間戳確定所需的SLBL CSV。

```
ls -l /configuration/slbl-*.csv
```

例如，使用輸出標識格式為slbl-<ID>-<TIMESTAMP>.csv的檔名。

對於Windows

1. 開啟PuTTY會話或另一個SSH 客戶端，並載入用於連線到SMA的代理配置。保持代理會話處於開啟狀態。
2. 運行此命令：

```
pscp -P
```

```
@127.0.0.1:/configuration/slbl-
```

```
-
```

```
.csv C:/path/localsystem
```

- <port> — 為SMA CLI訪問配置的本地轉發埠。
- <username> – CES使用者名稱。

舉例來說：

```
pscp -P 2201 cesuser@127.0.0.1:/configuration/slb1-420DE9AD994-CBF5261-20190925T3228.csv C:/Users/exas...
```

3. 驗證CSV檔案是否已下載到本地目標路徑。

對於Linux/macOS

1. 開啟terminal視窗。
2. 運行此命令以通過代理伺服器建立本地埠轉發：

```
ssh -i
```

```
-l dh-user -N -f
```

```
-L
```

```
:
```

```
:22
```

- <private_key_path> — 私鑰路徑。
- <proxy_server> - 代理伺服器主機名。
- <port> — 為SMA CLI訪問配置的本地轉發埠。
- <hostname> - SMA主機名。

舉例來說：

```
ssh -i ~/.ssh/id_rsa -l dh-user -N -f proxy.example.com -L 2201:sma.example.com:22
```

3. 運行此命令：

scp -P

@127.0.0.1:/configuration/slbl-

-

.csv /path/localsystem

- <port> — 為SMA CLI訪問配置的本地轉發埠。
- <username> – CES使用者名稱。

舉例來說：

```
scp -P 2201 cesuser@127.0.0.1:/configuration/slbl-420DE9AD994-CBF5261-20190925T3228.csv /Users/exampleu
```

4. 驗證CSV檔案是否已下載到本地目標路徑。

相關內容

[訪問Cloud Email Security\(CES\)解決方案的命令列介面\(CLI\)](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。