

Download Allowlist/Blocklist File From CES SMA Using SCP

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Solution](#)

[For Windows](#)

[For Linux/macOS](#)

[Related Content](#)

Introduction

This document describes how to download the allowlist/blocklist file from the cloud Secure Management Appliance by using SCP for Cloud Email Security.

Prerequisites

The procedure requires Command Line Interface (CLI) access. It uses Secure Copy Protocol (SCP) for Cloud Email Security (CES).



Note: Example values in this document are placeholders. Replace them with the values for the deployment.

Requirements

- Ensure access to the Command Line Interface (CLI) on the SMA.
- Windows: PuTTY and PSCP installed.
- Linux/macOS: OpenSSH client tools installed (`ssh` and `scp`).
- Ensure access to the SSH proxy host, if required.
- Record the locally forwarded port configured for SMA CLI access.
- Record the CES username.
- Record the private key file path if key-based authentication is required.

See [Accessing the Command Line Interface \(CLI\) of the Cloud Email Security \(CES\) Solution](#).

Solution

The allowlist/blocklist (SLBL) CSV file is stored under `/configuration/` on the SMA. If the exact filename is not known, list the available files and identify the required SLBL CSV by filename and timestamp.

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

For example, use the output to identify a filename in the format `slbl-<ID>-<TIMESTAMP>.csv`.

For Windows

1. Open a **PuTTY** session, or another **SSH client**, and load the proxy configuration used to connect to the SMA. Leave the proxy session open.
2. Run this command:

```
pscp -P <port> <username>@127.0.0.1:/configuration/slbl-<ID>-<TIMESTAMP>.csv C:/path/localsystem
```

- `<port>` — locally forwarded port configured for SMA CLI access.
- `<username>` — CES username.

For example:

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

3. Verify that the CSV file is downloaded to the local destination path.

For Linux/macOS

1. Open a **terminal window**.
2. Run this command to create the local port forward through the proxy server:

```
ssh -i <private_key_path> -l dh-user -N -f <proxy_server> -L <port>:<hostname>:22
```

- `<private_key_path>` — private key path.
- `<proxy_server>` — proxy server hostname.
- `<port>` — locally forwarded port configured for SMA CLI access.

- <hostname> — SMA hostname.

For example:

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

3. Run this command:

```
scp -P <port> <username>@127.0.0.1:/configuration/slb1-<ID>-<TIMESTAMP>.csv /path/localsystem
```

- <port> — locally forwarded port configured for SMA CLI access.
- <username> — CES username.

For example:

```
scp -P 2201 cesuser@127.0.0.1:/configuration/slb1-420DE9AD994-CBF5261-20190925T3228.csv /Users/exampleu
```

4. Verify that the CSV file is downloaded to the local destination path.

Related Content

[Accessing the Command Line Interface \(CLI\) of the Cloud Email Security \(CES\) Solution](#)