

Ändern der Liste sicherer Absender/Sperrliste für Endbenutzer in der ESA

Inhalt

[Einführung](#)

[Ändern der Liste sicherer Absender/Sperrliste für Endbenutzer in der ESA](#)

[Syntax für Listen sicherer Absender und Sperrlisten-Einträge](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie ein Administrator die Liste sicherer Absender/Sperrliste (SLBL) für Endbenutzer auf der Cisco E-Mail Security Appliance (ESA) ändern kann.

Ändern der Liste sicherer Absender/Sperrliste für Endbenutzer in der ESA

Ein ESA-Administrator kann das SLBL direkt von der IronPort Spam Quarantine (ISQ)-Schnittstelle aus sehen. Administratoren können dieselben Einträge sehen und mit ihnen arbeiten, mit denen die Endbenutzer arbeiten.

Um das SLBL anzuzeigen oder zu ändern, muss der Administrator einen der folgenden Schritte ausführen:

1. Melden Sie sich mit ihrem Administratorkonto und Kennwort bei der EUQ an.
 - Wählen Sie **Listen sicherer Absender** oder **Sperrlisten** aus dem Dropdown-Menü Optionen oben rechts aus.
 - Suchen und ändern Sie die *Absender-/Absenderliste* für die *Empfängeradresse*, falls erforderlich.
2. Exportieren des SLBL in eine CSV-Datei
 - **Systemverwaltung > Konfigurationsdatei** und wählen **Jetzt sichern/sichern**
 - Die Datei wird auf der Appliance gespeichert und muss über FTP oder eine andere Methode zum Abrufen von Dateien von der Appliance exportiert werden.
 - Die Datei wird im *Konfigurationsverzeichnis* gespeichert und durch den als gespeicherten Dateinamen angegeben. d. h. SLBL-564D6C9B806B5719XXXX-57284F5DYYY-20160203T141646.csv
 - Beim Betrachten der SLBL .csv-Datei sollten Sie ähnliche sehen:

```
# File exported by the SL/BL at 20070922T012001
c=us;a=;p=test;o=exchange;s=smith;g=joe;, BLOCKED, black2@x.com
c=us;a=;p=test;o=exchange;s=smith;g=joe;, SAFE, white4@x.com, white5@x.com, white6@x.com,
white3@x.com, white7@x.com
joe@exchange.test.com, BLOCKED, black2@x.com
joe@exchange.test.com, SAFE, white4@x.com, white5@x.com, white6@x.com, white3@x.com,
white7@x.com
joe@testcom, BLOCKED, black2@x.com
joe@testcom, SAFE, white4@x.com, white5@x.com, white6@x.com, white3@x.com, white7@x.com
joe@test.com, BLOCKED, black2@x.com
```

joe@test.com, SAFE, white3@x.com, white4@x.com, white5@x.com, white6@x.com, white7@x.com

- Nachdem die Datei geändert wurde, kann sie mit der gleichen Methode wie **Systemverwaltung > Konfigurationsdatei** und **Wiederherstellung** wieder in die ESA geladen werden.

Syntax für Listen sicherer Absender und Sperrlisten-Einträge

Absender können Sicherheitslisten und Sperrlisten in den folgenden Formaten hinzugefügt werden:

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]
- [ipv6:2001:DB8:1::1]
- benutzer@[1.2.3.4]

Hinweis: Vollständige Informationen zu Listen sicherer Absender und Sperrlisten finden Sie im [Benutzerhandbuch](#) für die Version von AsyncOS für E-Mail-Sicherheit, die Ihre Appliance derzeit ausführt, oder auf der ISQ-Hilfeseite direkt: https://<IP ODER HOSTNAME OF ESA>:83/help/admin_help

Zugehörige Informationen

- [Benutzerhandbücher - E-Mail Security Appliance](#)
- [Sicherungsverfahren für ESA-Listen/Sperrlisten](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)