API zum Hinzufügen von Absendern in SL/BL auf SMA verwenden

Inhalt

Einleitung

In diesem Dokument werden Konfigurationen zum Hinzufügen von Absendern in der Liste sicherer Absender/Sperrliste (SL/BL) für die Secure Management Appliance (SMA) mit API und Curl-Befehl beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Secure Management Appliance (SMA)
- API-Kenntnisse
- Wissen über die Spam-Quarantäne
- Informationen zu Listen sicherer Absender/Sperrlisten

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Security Management Appliance, AsyncOS Version 12.0 oder höher.
- Eine cURL für einen Client oder eine Programmierbibliothek. Dies muss JSON unterstützen, damit die Antwort von der API interpretiert werden kann.

- Autorisierung für den Zugriff auf die AsyncOS-API.
- Zentralisierte Spam-Quarantäne
- Liste sicherer Absender und Sperrliste aktiviert.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Der Hauptzweck des API-Service besteht darin, Berichte und Konfigurationsinformationen von der SMA abzurufen.

Sie können Informationen zu Listen sicherer Absender und Sperrlisten aus der Spam-Quarantäne abrufen und neue Benutzer mit API cURL-Abfragen hinzufügen.

Konfigurieren

GETP und POST als Liste sicherer Absender

HOLEN

Diese Abfrage ruft die Informationen aus der Liste sicherer Absender ab, wobei **sma1.example.com** ist der SMA-Hostname und **admin**ist der Benutzername.

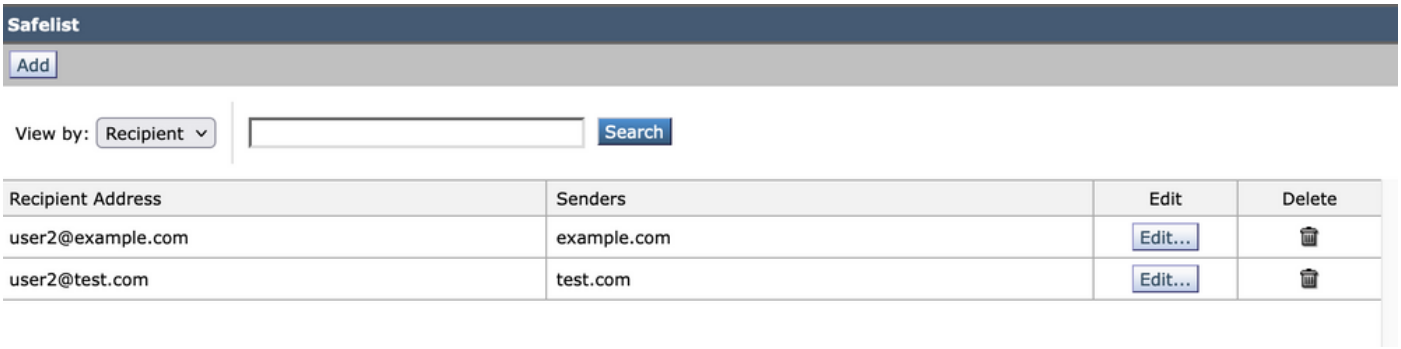
curl --location --request GET 'https://sma1.example.com/sma/api/v2.0/quarantine/safelist?action=view&quarantineType=spam&viewBy=recipient' -u admin

Geben Sie das Kennwort für den betreffenden Benutzer ein.

Als Ergebnis erhalten Sie:

{"meta": {"totalCount": 2}, "data": [{"senderList": ["example.com"], "recipientAddress": "user2@example.com"}, {"senderList": ["test.com"], "recipientAddress": "user2@test.com"}]}

Die Liste sicherer Absender in der Benutzeroberfläche wird im Bild angezeigt:



Ausgabe der GUI Safelist

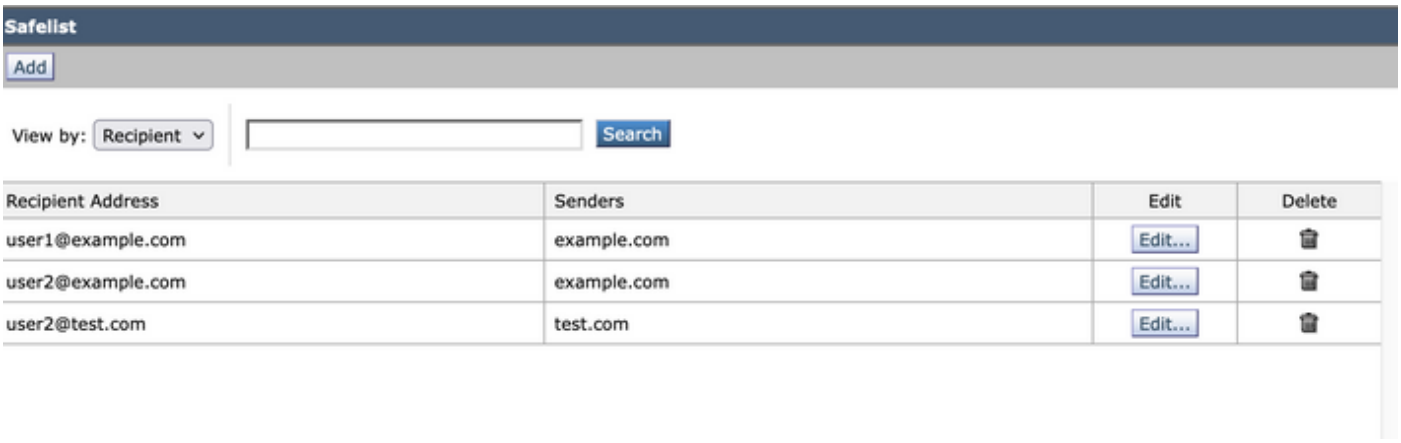
POST

Diese Abfrage fügt der Liste sicherer Absender Absenderinformationen hinzu, wobei **sma1.example.com** ist der SMA-Hostname und **admin**der Benutzername ist, **user1@example.com**der neue Empfänger ist und **example.com** ist der Absender der Liste sicherer Absender.

curl --location --request POST 'https://sma1.example.com/sma/api/v2.0/quarantine/safelist' -u admin --data-raw '{
"action": "add",
"quarantineType": "spam",
"recipientAddresses": ["user1@example.com"],
"senderList": ["example.com"],
"viewBy": "recipient"
}'

Führen Sie diesen Befehl aus, und geben Sie das Kennwort für den betreffenden Benutzer ein.

Die Liste sicherer Absender in der Benutzeroberfläche wird im Bild angezeigt:



Ausgabe der GUI Safelist

Sperrliste GET und POST

HOLEN

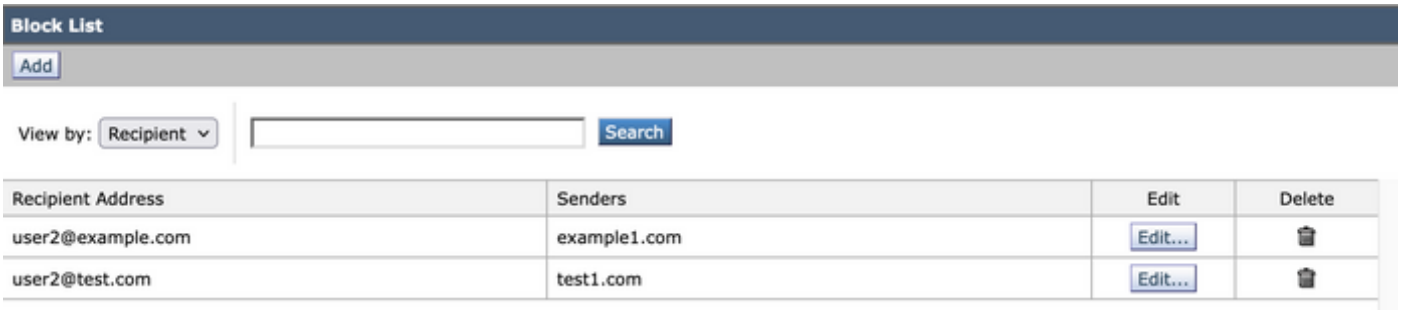
Diese Abfrage ruft die Informationen aus der Liste sicherer Absender ab, wobei **sma1.example.com** ist der SMA-Hostname und **admin**ist der Benutzername

curl --location --request GET 'https://sma1.example.com/sma/api/v2.0/quarantine/blocklist?action=view&quarantineType=spam&viewBy=recipient' -u admin

Als Ergebnis erhalten Sie:

{"meta": {"totalCount": 2}, "data": [{"senderList": ["example1.com"], "recipientAddress": "user2@example.com"}, {"senderList": ["test1.com"], "recipientAddress": "user2@test.com"}]

Die Liste sicherer Absender in der Benutzeroberfläche wird im Bild angezeigt:



Ausgabe der GUI-Sperrliste

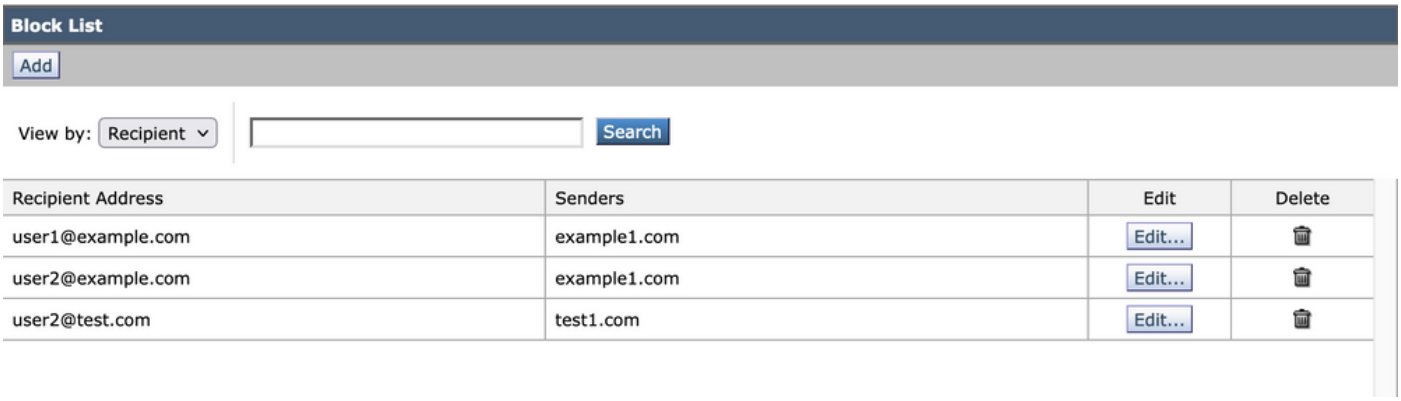
POST

Diese Abfrage fügt der Liste sicherer Absender Absenderinformationen hinzu, wobei **sma1.example.com** ist der SMA-Hostname und **admin**der Benutzername ist, **user1@example.com**der neue Empfänger ist und **example1.com** ist der Absender, der blockiert werden soll.

curl --location --request POST 'https://sma1.example.com/sma/api/v2.0/quarantine/blocklist' -u admin --data-raw '{
"action": "add",
"quarantineType": "spam",
"recipientAddresses": ["user1@example.com"],
"senderList": ["example1.com"],
"viewBy": "recipient"
}'

Führen Sie diesen Befehl aus, und geben Sie das Kennwort für den betreffenden Benutzer ein.

Die Liste sicherer Absender in der Benutzeroberfläche wird im Bild angezeigt:



Ausgabe der GUI-Sperrliste

Zugehörige Informationen

- Programmierhandbücher SMA
- Benutzerhandbuch SMA

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.