

使用API在SMA上的SL/BL中新增發件人

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[安全清單GET和POST](#)

[GET](#)

[POST](#)

[阻止清單GET和POST](#)

[GET](#)

[POST](#)

[相關資訊](#)

簡介

本文檔介紹使用API和curl命令在安全管理裝置(SMA)的安全清單/阻止清單(SL/BL)中新增發件人的配置。

必要條件

需求

思科建議瞭解以下主題：

- 安全管理裝置(SMA)
- API知識
- 垃圾郵件隔離區知識
- 安全清單/阻止清單知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全管理裝置，AsyncOS版本12.0或更高版本。
- 客戶端或程式設計庫cURL。必須支援JSON才能解釋來自API的響應。
- 授權訪問AsyncOS API。
- 集中垃圾郵件隔離區。
- 已啟用安全清單和阻止清單。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

API服務的主要用途是從SMA獲取報告和配置資訊。

您可以從垃圾郵件隔離區獲取安全清單和阻止清單資訊，還可以使用API cURL查詢新增新使用者。

設定

安全清單GET和POST

GET

此查詢從安全清單獲取資訊，其中 `sma1.example.com` 是SMA主機名和 `admin`是使用者名稱。

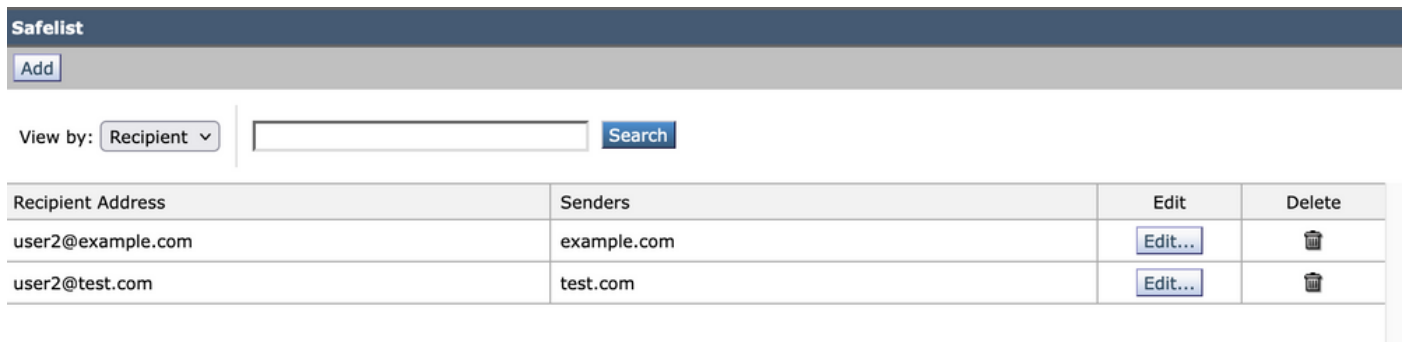
```
curl --location --request GET 'https://sma1.example.com/sma/api/v2.0/quarantine/safelist?action=view&quarantineType=spam&viewBy=recipient' -u admin
```

輸入有問題的使用者的密碼。

作為輸出，您將獲得：

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

GUI安全清單如下圖所示：



Recipient Address	Senders	Edit	Delete
user2@example.com	example.com	Edit...	
user2@test.com	test.com	Edit...	

GUI安全清單輸出

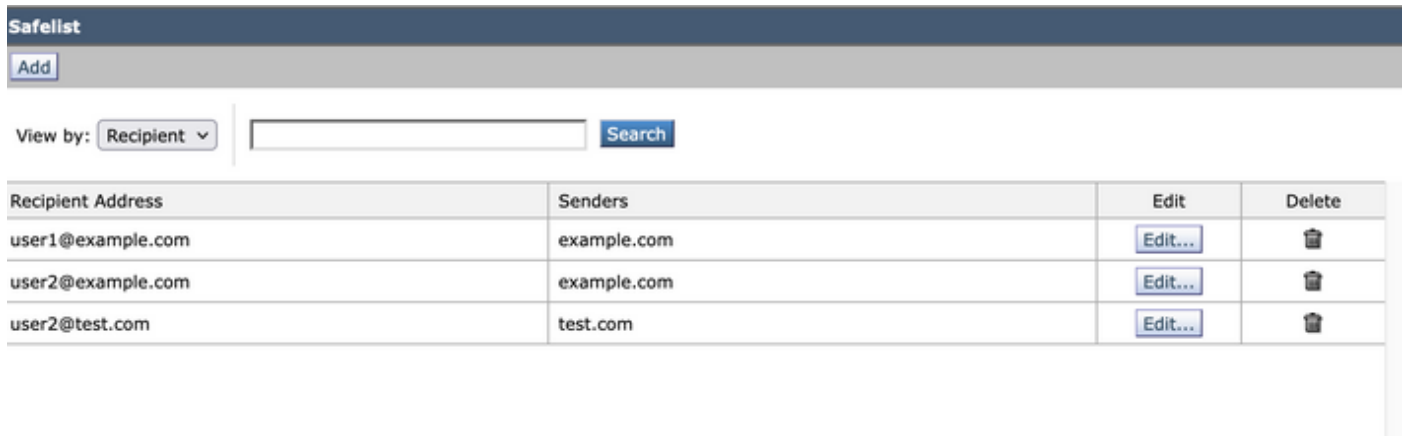
POST

此查詢將發件人資訊新增到安全清單，其中 `sma1.example.com` 是SMA主機名和 `admin`是使用者名稱，`user1@example.com`是新的接收方，`example.com` 是安全清單的發件人。

```
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" }'
```

運行此命令並輸入相關使用者的密碼。

GUI安全清單如下圖所示：



Recipient Address	Senders	Edit	Delete
user1@example.com	example.com	Edit...	
user2@example.com	example.com	Edit...	
user2@test.com	test.com	Edit...	

GUI安全清單輸出

阻止清單GET和POST

GET

此查詢從安全清單獲取資訊，其中 `sma1.example.com` 是SMA主機名和 `admin`是使用者名稱

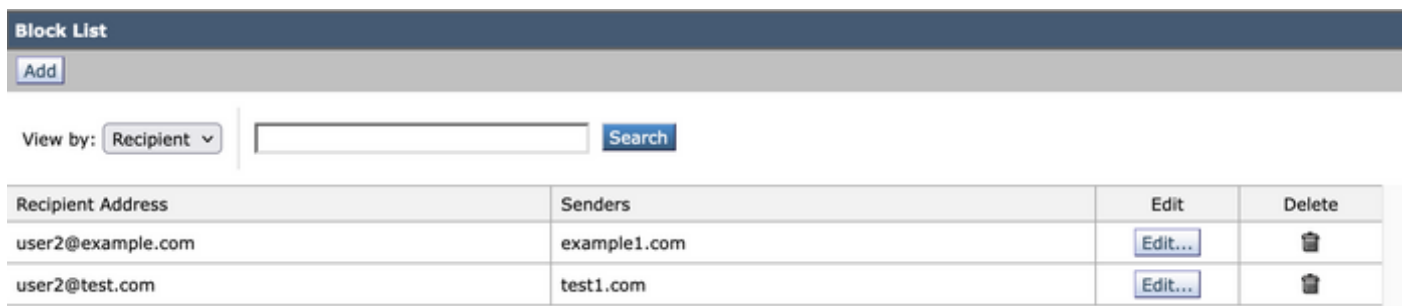
```
curl --location --request GET
```

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

作為輸出，您將獲得：

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

GUI安全清單如下圖所示：



Recipient Address	Senders	Edit	Delete
user2@example.com	example1.com	Edit...	
user2@test.com	test1.com	Edit...	

GUI阻止清單輸出

POST

此查詢將發件人資訊新增到安全清單，其中 `sma1.example.com` 是SMA主機名和 `admin`是使用者名稱，`user1@example.com`是新的收件人，`example1.com` 是阻止清單的發件人。

```
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"
}
```

};

運行此命令並輸入相關使用者的密碼。

GUI安全清單如下圖所示：

Recipient Address	Senders	Edit	Delete
user1@example.com	example1.com	Edit...	
user2@example.com	example1.com	Edit...	
user2@test.com	test1.com	Edit...	

GUI阻止清單輸出

相關資訊

- [程式設計指南SMA](#)
- [最終使用手冊SMA](#)

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）。