

# API를 사용하여 SMA의 SL/BL에 발신자 추가

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[허용 목록 GET 및 POST](#)

[가져오기](#)

[POST](#)

[차단 목록 GET 및 POST](#)

[가져오기](#)

[POST](#)

[관련 정보](#)

## 소개

이 문서에서는 API 및 curl 명령을 사용하여 SMA(Secure Management Appliance)용 허용 목록/차단 목록(SL/BL)에서 발신자를 추가하는 컨피그레이션에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- SMA(Secure Management Appliance)
- API 지식
- 스팸 쿼런틴 지식
- 허용 목록/차단 목록 지식

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Security Management Appliance, AsyncOS 버전 12.0 이상
- 클라이언트 또는 프로그래밍 라이브러리 cURL입니다. API의 응답을 해석하려면 JSON을 지원해야 합니다.
- AsyncOS API에 액세스하기 위한 권한 부여.
- 중앙 집중식 스팸 격리.
- 허용 목록 및 차단 목록이 사용하도록 설정되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

API 서비스의 주 목적은 SMA에서 보고서와 컨피그레이션 정보를 가져오는 것입니다.

스팸 격리에서 안전 목록 및 차단 목록 정보를 가져올 수 있으며, API cURL 쿼리로 새 사용자를 추가할 수 있습니다.

## 구성

### 허용 목록 GET 및 POST

#### 가져오기

이 쿼리는 허용 목록에서 정보를 가져옵니다. `sma1.example.com` SMA 호스트 이름 및 `admin` 사용자 이름입니다.

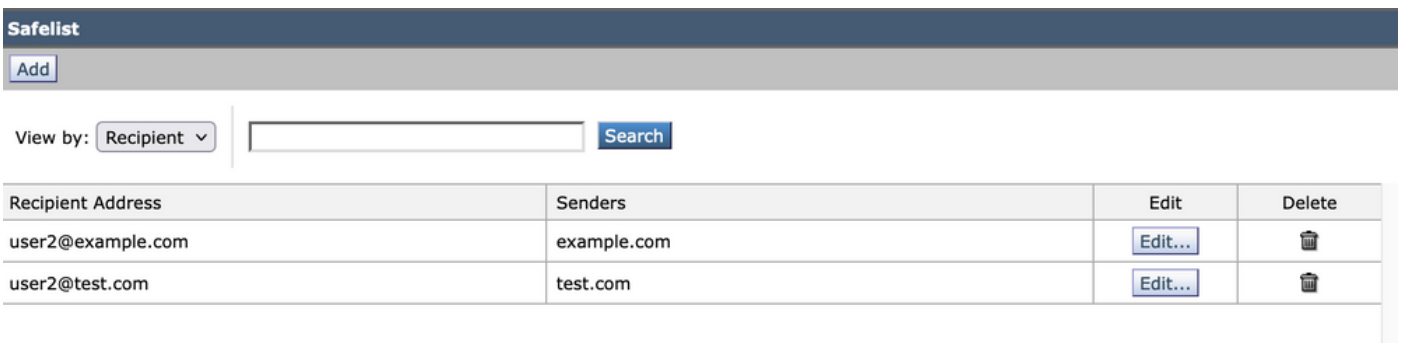
```
curl --location --request GET 'https://sma1.example.com/sma/api/v2.0/quarantine/safelist?action=view&quarantineType=spam&viewBy=recipient' -u admin
```

해당 사용자의 비밀번호를 입력합니다.

출력 결과:

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

GUI 허용 목록이 이미지에 표시됩니다.



The screenshot shows a web interface titled "Safelist". At the top, there is an "Add" button. Below it, there is a "View by:" dropdown menu set to "Recipient", followed by a search input field and a "Search" button. The main content is a table with the following data:

Recipient Address	Senders	Edit	Delete
user2@example.com	example.com	<a href="#">Edit...</a>	
user2@test.com	test.com	<a href="#">Edit...</a>	

GUI 허용 목록 출력

## POST

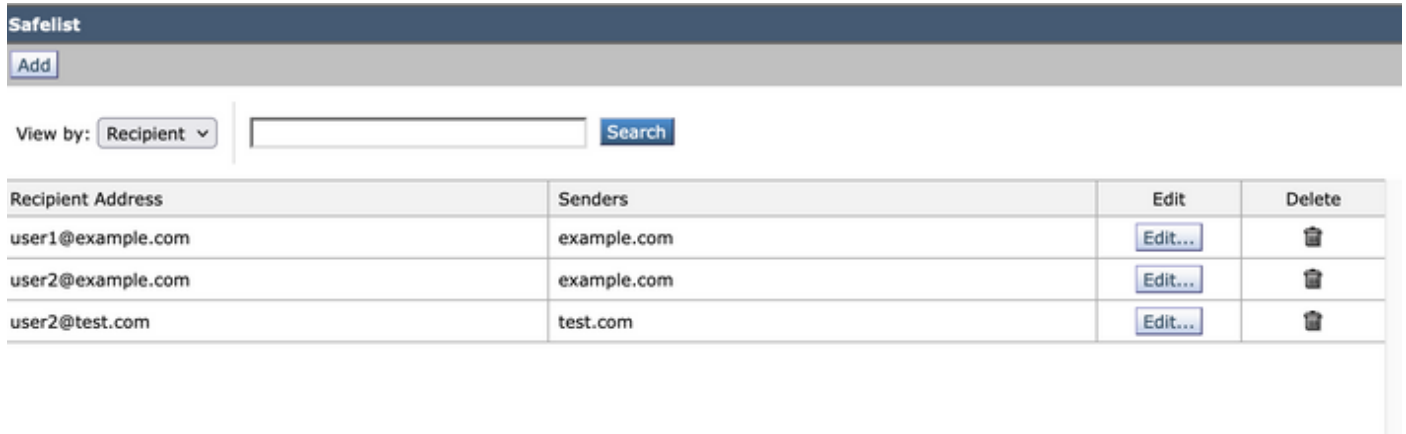
이 쿼리는 발신자 정보를 허용 목록에 추가합니다. 여기서 `sma1.example.com` SMA 호스트 이름 및 `admin` 사용자 이름입니다. `user1@example.com` 새 수신자이며 `example.com` 은(는) 허용 목록에 대한 발신자입니다.

```
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"
}'
```

이 명령을 실행하고 해당 사용자의 비밀번호를 입력합니다.

GUI 허용 목록이 이미지에 표시됩니다.



GUI 허용 목록 출력

## 차단 목록 GET 및 POST

### 가져오기

이 쿼리는 허용 목록에서 정보를 가져옵니다. 여기서 sma1.example.com SMA 호스트 이름 및 admin 사용자 이름입니다.

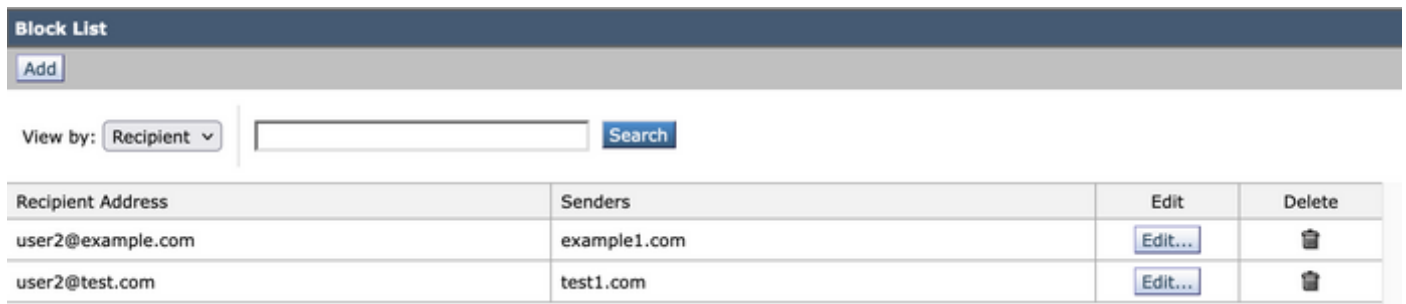
curl --location --request GET

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

출력 결과:

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

GUI 허용 목록이 이미지에 표시됩니다.



GUI 차단 목록 출력

## POST

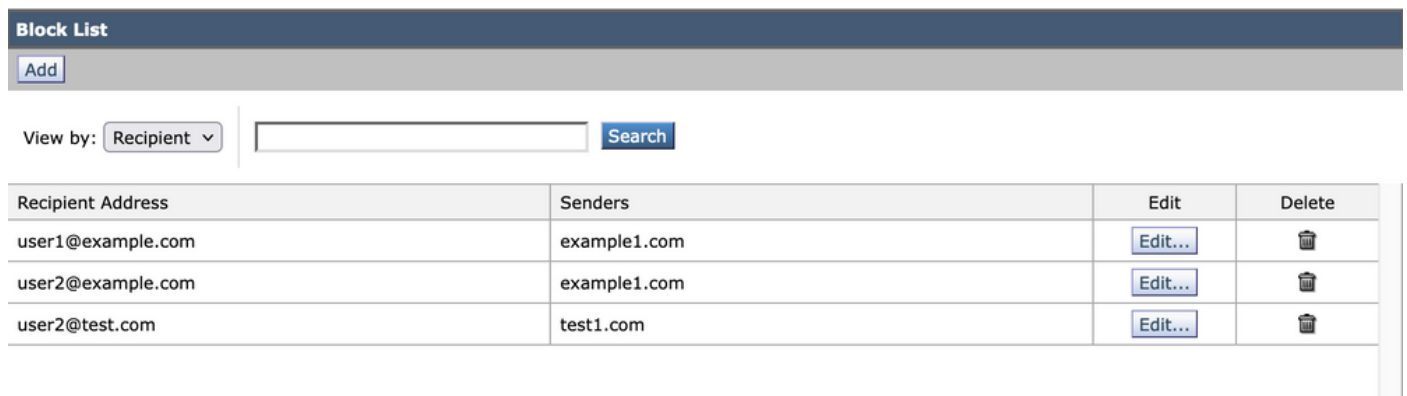
이 쿼리는 발신자 정보를 허용 목록에 추가합니다. 여기서 sma1.example.com SMA 호스트 이름 및

admin사용자 이름입니다. user1@example.com새 수신인이며 example1.com 차단 목록에 대한 발신자입니다.

```
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"
}'
```

이 명령을 실행하고 해당 사용자의 비밀번호를 입력합니다.

GUI 허용 목록이 이미지에 표시됩니다.



Recipient Address	Senders	Edit	Delete
user1@example.com	example1.com	<a href="#">Edit...</a>	
user2@example.com	example1.com	<a href="#">Edit...</a>	
user2@test.com	test1.com	<a href="#">Edit...</a>	

GUI 차단 목록 출력

## 관련 정보

- [프로그래밍 가이드 SMA](#)
- [최종 사용자 가이드 SMA](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.