

# CSC 6.X: 이메일 평판 컨피그레이션 예

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[일부 도메인에서 전자 메일을 받을 수 없습니다.](#)

[관련 정보](#)

## 소개

이 문서에서는 CSC(Cisco Content Security and Control) SSM(Security Services Module)에서 이메일 평판을 구성하는 방법에 대한 샘플 컨피그레이션을 제공합니다.

## 사전 요구 사항

### 요구 사항

이 기능을 사용하려면 Security Plus 라이선스가 있어야 합니다.

### 사용되는 구성 요소

이 문서의 정보는 Cisco Content Security and Control SSM with Software 릴리스 버전 6.3을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### 표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

## 배경 정보

이메일 평판은 스팸 메일을 줄이는 기술입니다. 이 기능을 활성화하면 CSC SSM은 메일의 발신자가 블랙리스트 주소인지 확인합니다. 스팸 메시지를 소싱하는 모든 IP 주소가 포함된 데이터베이스 목록을 유지 관리합니다. 이 목록의 발신자가 있는 메일이 발견되면 해당 메일은 스팸으로 간주되어 삭제됩니다.

이 ERS(Email Reputation Technology)에서 제공하는 서비스 수준은 기본적으로 두 가지 유형입니다. 이러한 서비스는 주로 소스 IP 주소의 신뢰성 수준을 기반으로 합니다.

- ERS Standard - 알려진 스팸 소스를 포함합니다.
- ERS Advanced(ERS 고급) - 알려진 소스 및 의심되는 소스를 포함합니다.

ERS Standard 데이터베이스에 IP 주소를 추가하면 스팸 소스라고 하며 이 목록에서 제거된 IP 주소를 관찰하는 경우는 드물습니니다. ERS Standard에는 스팸을 일관되게 시작하는 IP 주소 목록이 포함되어 있습니다.

ERS Advanced에는 더 이상 스팸을 생성하지 않는 경우 제거될 IP 주소의 목록이 포함되어 있습니다. 예를 들어, 해킹된 메일 서버는 보안이 침해된 시점에 이 데이터베이스에 나열될 수 있습니다. 정상 상태로 복원되면 이 데이터베이스에서 제거됩니다.

## 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** [명령 조회 도구\(등록된\)](#) 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

1. Mail (SMTP) > Anti-spam > Email Reputation을 선택합니다. 새 창이 열립니다.
2. 이 이메일 평판 기능을 활성화하려면 Target(대상) 탭에서 **Enable(활성화)**을 클릭합니다.
3. Service Level(서비스 레벨)에 대해 Advanced(고급)를 선택합니다.
4. Approved IP Addresses(승인된 IP 주소) 필드에서 스캔에서 제외할 IP 주소의 범위를 지정합니다

**TREND MICRO™ InterScan™ for Cisco CSC SSM**

Summary

▼ Mail (SMTP)

Scanning

Incoming

Outgoing

Anti-spam

Content Scanning

**Email Reputation**

Content-Filtering

Incoming

Outgoing

Configuration

▶ Mail (POP3)

▶ Web (HTTP)

▶ File Transfer (FTP)

▶ Update

▶ Logs

▶ Administration

**SMTP Anti-spam (Email Reputation)**

Email Reputation is a Smart Protection Network component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge.

**Target** | **Action**

SMTP Anti-spam (Email Reputation): **Disabled**

Email Reputation Services allows you to view global spam information and reports, as well as create or manage Approved and Blocked Sender IP address lists, perform administrative tasks, and configure the service.

[Email Reputation Services Portal](#)

**Set Service Level**

Standard: Uses the Standard Reputation database to block messages from known spam sources. [Click for more information.](#)

Advanced: Uses both Standard and Dynamic Reputation databases to block messages from known and suspected spam sources. [Click for more information.](#)

**Approved IP Address(es)**

Add approved IP address:

Approved IP address(es):

10.0.0.0/8

5. Action(작업) 탭에서 엔터프라이즈 보안 정책에 따라 작업 유형을 지정합니다. 다음 세 가지 작업을 사용할 수 있습니다. 오류 메시지와 함께 연결 닫기, 오류 메시지 없이 연결 닫기, 연결 우회

**TREND MICRO™ InterScan™ for Cisco CSC SSM**

Summary

▼ Mail (SMTP)

Scanning

Incoming

Outgoing

Anti-spam

Content Scanning

**Email Reputation**

Content-Filtering

Incoming

Outgoing

Configuration

▶ Mail (POP3)

▶ Web (HTTP)

▶ File Transfer (FTP)

▶ Update

▶ Logs

**SMTP Anti-spam (Email Reputation)**

Email Reputation is a Smart Protection Network component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge.

**Target** | **Action**

**Standard Reputation Database Action**

Intelligent action - Permanent denial of connection for Standard Reputation Database matches  
SMTP error code:  (range 400 - 599; default=550)

Close connection with no error message

Bypass (not recommended)

**Dynamic Reputation Database Action**

Intelligent action - Temporary denial of connection for Dynamic Reputation Database matches  
SMTP error code:  (range 400 - 599; default=450)

Close connection with no error message

Bypass (not recommended)

**다음을 확인합니다.**

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

**문제 해결**

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

## 일부 도메인에서 전자 메일을 받을 수 없습니다.

### 문제/장애:

문제는 특정 도메인에서 이메일을 받을 수 없다는 점입니다. CSC 모듈에서 이메일을 차단하고 있는 것 같습니다. 모듈을 우회하면 모든 것이 잘 작동합니다. 이 오류 메시지를 받았습니다.

2012/02/06 14:33:00 GMT+00:00 NRS 174.37.94.181 RBL-Fail QIL-NA RejectWithErrorCode-550 NA 0 NA  
NA NA 0 NA NA 0 NA NA 0 NA

### 해결책:

이 문제를 해결하려면 이메일 평판 기능을 올바르게 구성하십시오.

## 관련 정보

- [Cisco ASA CSC\(Content Security and Control\) Security Services Module 지원](#)
- [기술 지원 및 문서 - Cisco Systems](#)