

# CSC 6.X:電子郵件信譽配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[驗證](#)

[疑難排解](#)

[無法從某些域接收電子郵件](#)

[相關資訊](#)

## 簡介

本文提供如何在思科內容安全與控制(CSC)安全服務模組(SSM)上設定電子郵件信譽的範例設定。

## 必要條件

### 需求

您需要擁有Security Plus許可證才能使用此功能。

### 採用元件

本檔案中的資訊是根據軟體版本6.3的思科內容安全與控制SSM。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

### 慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

## 背景資訊

Email Reputation是一項減少垃圾郵件的技術。通過啟用此功能，CSC SSM驗證郵件的發件人是否為黑名單地址。它維護一個資料庫清單，其中包含產生垃圾郵件的所有IP地址。如果發現郵件具有此清單中的發件人，則該郵件被視為垃圾郵件並被丟棄。

此電子郵件信譽技術(ERS)提供的服務級別基本上是兩種型別。這些服務主要基於源IP地址的真實性級別。

- ERS標準 — 包含已知垃圾郵件來源
- ERS Advanced — 包含已知來源和可疑來源

將IP地址新增到ERS標準資料庫時，它被稱為垃圾郵件源，很少看到您看到此清單中刪除的IP地址。ERS Standard包含始終引發垃圾郵件的IP地址清單。

ERS Advanced包含一系列IP地址，如果發現這些地址不會進一步產生垃圾郵件，則應該將其刪除。例如，當被入侵時，此資料庫中可以列出被入侵的郵件伺服器。當恢復為正常狀態時，會將其從此資料庫中刪除。

## 設定

本節提供用於設定本文中所述功能的資訊。

**註：**使用[Command Lookup Tool](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

1. 選擇Mail(SMTP)> Anti-spam > Email Reputation。將開啟一個新視窗。
2. 在「目標」頁籤中，按一下**啟用**以啟用此電子郵件信譽功能。
3. 選擇Advanced作為服務級別。
4. 在Approved IP Addresses欄位中，指定要免除掃描的IP地址範圍。

TREND MICRO™ InterScam™ 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.

#### 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. 在操作頁籤中，根據您的企業安全策略指定操作型別。可以使用以下三種操作：關閉連線並顯示錯誤消息關閉連線，無錯誤消息繞過連線

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

**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.

**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)

## 驗證

目前沒有適用於此組態的驗證程序。

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

### 無法從某些域接收電子郵件

**問題：**

問題在於無法從特定域接收電子郵件。CSC模組似乎正在阻止電子郵件。繞過模組時，一切正常。收到以下錯誤消息：2012/02/06 14:33:00 GMT+00:00 NRS 174.37.94.181 RBL-Fail-QIL-NA-550 NA 0 NA NA 0 NA NA 0 NA

**解決方案：**

為了解決此問題，請正確設定電子郵件信譽功能。

## 相關資訊

- [Cisco ASA內容安全與控制\(CSC\)安全服務模組支援](#)
- [技術支援與文件 - Cisco Systems](#)