

允許受信任的發件人繞過反垃圾郵件

目錄

[簡介](#)

[在ALLOWED_LIST Sender組中新增發件人主機名/IP地址](#)

[在GUI上](#)

[在CLI上](#)

[檢視受信任郵件流策略中的反垃圾郵件和防病毒掃描](#)

[將受信任的發件人新增到安全清單](#)

[具有傳入郵件策略的受信任發件人](#)

[相關資訊](#)

簡介

本文檔介紹允許受信任的發件人繞過反垃圾郵件掃描的詳細資訊，以及可在安全電子郵件網關（以前稱為郵件安全裝置）上選擇相同的方法。

在ALLOWED_LIST Sender組中新增發件人主機名/IP地址

將您信任的發件人新增到ALLOWED_LIST發件人組，因為該發件人組使用\$TRUSTED郵件流策略。ALLOWED_LIST發件人組的成員不受速率限制，反垃圾郵件引擎不會掃描來自這些發件人的內容，但反病毒引擎仍對其進行掃描。

附註：在預設配置下，防病毒掃描已啟用，但反垃圾郵件已關閉。

為了允許發件人繞過反垃圾郵件掃描，請將發件人新增到主機訪問表(HAT)中的ALLOWED_LIST發件人組。可以通過GUI或CLI配置HAT。

在GUI上

1. 選擇Mail Policies頁籤。
2. 在Host Access Table部分下，選擇HAT Overview。
3. 在右側，確保當前選擇了您的InboundMail偵聽程式。
4. 在「Sender Group」列中選擇ALLOWED_LIST。
5. 選擇頁面底部附近的Add Sender按鈕。
6. 在第一個欄位中輸入要允許繞過的IP或主機名。

新增完條目後，選擇Submit按鈕。記住選擇Commit Changes按鈕以儲存更改。

在CLI上

```
example.com> listenerconfig
```

```
Currently configured listeners:
```

1. InboundMail (on PublicNet, 172.19.1.80) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 172.19.2.80) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

[> **edit**

Enter the name or number of the listener you wish to edit.

[> **1**

Name: InboundMail

Type: Public

Interface: PublicNet (172.19.1.80/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.

[> **hostaccess**

Default Policy Parameters

=====

Allow TLS Connections: No

Allow SMTP Authentication: No

Require TLS To Offer SMTP authentication: No

Maximum Concurrency Per IP: 1,000

Maximum Message Size: 100M

Maximum Messages Per Connection: 1,000

Maximum Recipients Per Message: 1,000

Maximum Recipients Per Hour: Disabled

Use SenderBase For Flow Control: Yes

Spam Detection Enabled: Yes

Virus Detection Enabled: Yes

There are currently 4 policies defined.

There are currently 5 sender groups.

Choose the operation you want to perform:

- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.

[> **edit**

1. Edit Sender Group

2. Edit Policy

[1]> **1**

Currently configured HAT sender groups:

```
1. ALLOWED_LIST (My trusted senders have no anti-spam scanning or rate limiting)
2. BLOCKED_LIST (Spammers are rejected)
3. SUSPECTLIST (Suspicious senders are throttled)
4. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
5. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.
[ ]> 1
```

Choose the operation you want to perform:

- NEW - Add a new host.
- DELETE - Remove a host.
- MOVE - Reorder the hosts.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.

```
[ ]> new
```

Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed. IP address ranges such as 10.1.1.10-20 are allowed. IP subnets such as 10.2.3. are allowed. Hostnames such as crm.example.com are allowed. Partial hostnames such as .example.com are allowed.

Ranges of SenderBase Reputation scores such as SBR[7.5:10.0] are allowed.

SenderBase Network Owner IDs such as SBO:12345 are allowed.

Remote blocklist queries such as dnslist[query.blocklist.example] are allowed.

Separate multiple hosts with commas

```
[ ]>
```

請記得發出commit命令以儲存更改。

檢視受信任郵件流策略中的反垃圾郵件和防病毒掃描

對於受信任的發件人，預設情況下會有一個名為「受信任的存在」的郵件流策略。「受信任的郵件流策略」的連線行為將為「接受」（類似於傳入電子郵件的其他郵件流策略的行為）。

當發件人受信任以滿足業務要求時，我們可以選擇禁用其防病毒和防垃圾郵件檢查。這將有助於減少兩個掃描引擎在掃描非來自可信來源的電子郵件時的額外處理負載。

附註：已禁用的反垃圾郵件和防病毒引擎將跳過ESA中傳入電子郵件的任何垃圾郵件或病毒相關掃描。只有在您完全確定跳過對這些可信發件人的掃描不會產生風險時，才能執行此步驟。

可以在其中禁用引擎的選項在郵件流策略的安全功能頁籤中可用。其路徑為**GUI > Mail Policies > Mail Flow Policies**。按一下**TRUSTED Mail flow policy**，然後向下滾動到後續頁面上的**Security Features**。

確保在根據需要進行調整後提交更改。

Security Features	
Spam Detection:	<input type="radio"/> Use Default (On) <input type="radio"/> On <input checked="" type="radio"/> Off
Virus Protection:	<input type="radio"/> Use Default (On) <input checked="" type="radio"/> On <input type="radio"/> Off

將受信任的發件人新增到安全清單

終端使用者安全清單和阻止清單由終端使用者建立，並儲存在反垃圾郵件掃描前已檢查的資料庫中。每個終端使用者都可以識別其希望始終被視為垃圾郵件或從不被視為垃圾郵件的域、子域或電子郵件地址。如果發件人地址是終端使用者安全清單的一部分，則會跳過反垃圾郵件掃描

此設定將允許終端使用者根據發件人免除反垃圾郵件掃描的要求將其安全清單。郵件管道中的防病

毒掃描和其他掃描將不受此設定的影響，並將根據郵件策略中的配置繼續執行。每次終端使用者必須免除對發件人的垃圾郵件掃描時，此設定都會減少管理員的參與。

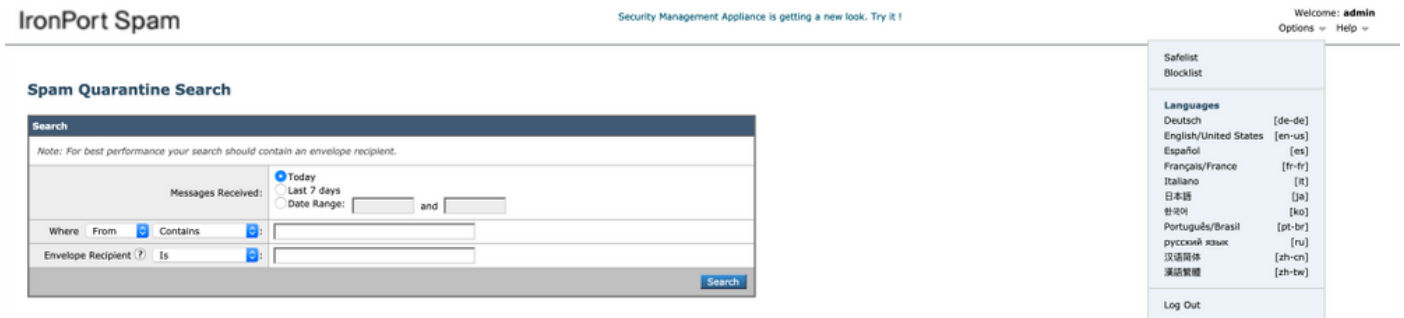
對於安全清單，必須為終端使用者啟用終端使用者隔離區訪問許可權，並將終端使用者安全清單/阻止清單設定為啟用狀態（在ESA或SMA中）。通過這種方式，他們可以訪問垃圾郵件隔離區門戶以及釋放/刪除隔離的電子郵件，他們還可以在安全清單中**新增/刪除**發件人。

終端使用者隔離訪問可以如下啟用：

ESA:導航到GUI > Monitor > Spam Quarantine。選中End-User Quarantine Access的單選按鈕。根據需要選擇用於訪問的身份驗證方法（None/LDAP/SAML/IMAP或POP）。發佈該郵件，啟用終端使用者安全清單/阻止清單。

SMA:導航到GUI > Centralized Services > Spam Quarantine。簽入終端使用者隔離區訪問的單選按鈕。根據需要選擇用於訪問的身份驗證方法（None/LDAP/SAML/IMAP或POP）。發佈該郵件，啟用終端使用者安全清單/阻止清單。

啟用後，當終端使用者導航到垃圾郵件隔離區門戶時，他們將能夠根據右上角下拉選項中的選擇新增/修改其安全清單。



具有傳入郵件策略的受信任發件人

您也可以在「傳入郵件策略」中新增受信任的發件人，並根據要求禁用防病毒/防垃圾郵件掃描。根據選擇，可以使用諸如Trusted Senders/Safe Senders等名稱建立新的自定義郵件策略，然後可以將發件人詳細資訊（如域名或發件人電子郵件地址）新增到此自定義策略中。


在所需新增後提交策略後，可以按一下Antispam或Antivirus列，然後在後續頁面中選擇Disable。

使用此設定，新增到此郵件策略的受信任發件人域或電子郵件地址將免於反垃圾郵件或防病毒掃描。

附註：已禁用的反垃圾郵件和防病毒引擎將跳過通過此自定義郵件策略處理的ESA中傳入電子郵件的任何垃圾郵件或病毒相關掃描。只有在您完全確定跳過對這些可信發件人的掃描不會產生風險時，才能執行此步驟。

可以通過ESA GUI > Mail Policies > Incoming Mail Policies > Add Policy建立自定義郵件策略。根據選擇輸入策略名稱，然後選擇新增使用者。選中「下列發件人」單選按鈕。在框中新增所需的域或電子郵件地址，然後按一下「確定」。

建立郵件策略後，您可以根據業務需求選擇禁用防病毒掃描和反垃圾郵件掃描。以下是一個螢幕截圖：

Add Policy...								
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	Trusted Senders	Disabled	Disabled	(use default)	(use default)	(use default)	(use default)	

相關資訊

- [Cisco Email Security Appliance — 最終使用手冊](#)
- [技術支援與文件 - Cisco Systems](#)