

信頼できる送信者をホワイトリストに追加する方法は？

目次

[質問](#)

[回答](#)

[GUI を使用する場合](#)

[CLI を使用する場合](#)

[関連情報](#)

質問

信頼できる送信者をホワイトリストに追加する方法は？

回答

Cisco E メール セキュリティ アプライアンス (ESA) 上で、信頼する送信者を WHITELIST の送信者グループに追加します。この理由は、この送信者グループでは \$TRUSTED メール フロー ポリシーを使用するためです。WHITELIST の送信者グループのメンバーはレート制限を受けず、これらの送信者からのコンテンツは Cisco IronPort AntiSpam エンジンによってスキャンされませんが、Sophos Anti-Virus ソフトウェアによっては引き続きスキャンされます。

注: デフォルト設定では、Anti-Virus スキャンは有効になりますが、Anti-Spam はオフになります。

送信者をホワイトリストに追加するには、ホスト アクセス テーブル (HAT) 内の WHITELIST 送信者グループにその送信者を追加します。HAT は、GUI または CLI を使用して設定できます。

GUI を使用する場合

1. [Mail Policies] タブをクリックします。
2. [Host Access Table] セクションの下で、[HAT Overview] を選択します。
3. 右側の [InboundMail] リスナーが現在選択されていることを確認します。
4. 下の [Sender Group] 列で、[WHITELIST] をクリックします。
5. ページの真中近くの下側にある [Add Sender] ボタンをクリックします。
6. ホワイトリストに追加する IP またはホスト名を最初のフィールドに入力します。

エントリの追加を終了したら、[Submit] ボタンをクリックします。必ず [Commit Changes] ボタンをクリックして変更を保存してください。

CLI を使用する場合

```
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. WHITELIST (My trusted senders have no Brightmail or rate limiting)
2. BLACKLIST (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 SBRS[7.5:10.0] are allowed.

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

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

Separate multiple hosts with commas

[>

必ず **commit** コマンドを発行して変更を保存してください。

関連情報

- [Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)