

# Hoe doe je Whitelist een Trusted Sender?

## Inhoud

[vraag](#)

[Antwoord](#)

[Via de GUI](#)

[Van de CLI](#)

[Gerelateerde informatie](#)

## vraag

Hoe doe je Whitelist een Trusted Sender?

## Antwoord

Voeg op de Cisco Email Security Appliance (ESA) zenders toe die u vertrouwt op de WHITELIST-verzendgroep, omdat deze verzendgroep het beleid voor \$TRUSTED Mail Flow gebruikt. Leden van de verzendgroep WHITELIST zijn niet onderworpen aan snelheidsbeperking, en de inhoud van die zenders wordt niet gescand door Cisco IronPort AntiSpam-motor, maar wordt nog steeds gescand door de software van Sofobie tegen het virus.

**Opmerking:** standaard is het scannen tegen het virus ingeschakeld maar anti-Spam is uitgeschakeld.

Aan whitelist een zender, voegt u de zender toe aan de WHITELIST sender group in de Host Access Table (HAT). U kunt de HAT configureren via de GUI of de CLI.

## Via de GUI

1. Klik op het tabblad *Mail Policy*.
2. Selecteer onder het gedeelte *Host Access Tabel* de optie *HAT - Overzicht*,
3. Zorg er rechts voor dat de luisteraar van de *inkomendeMail* is geselecteerd,
4. Klik in de kolom *Sender Group* hieronder op *WHITELIST*,
5. Klik op de knop *Add Sender* onder in de helft van de pagina.
6. Voer de IP- of hostnaam in die u in het eerste veld wilt weergeven.

Klik op de knop *Indienen* als u klaar bent met het toevoegen van items. Denk eraan om op de knop *Aanpassen aan het opdracht wijzigen* te klikken om de wijzigingen op te slaan.

# Van de CLI

```
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
[ ]>
Onthoud de afgifte commit opdracht om uw wijzigingen op te slaan.
```

## Gerelateerde informatie

- [Cisco e-mail security applicatie - eindgebruikershandleidingen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)