

Comment allez-vous Whitelist un expéditeur de confiance ?

Contenu

[Question](#)

[Réponse](#)

[Du GUI](#)

[Du CLI](#)

[Informations connexes](#)

Question

Comment allez-vous Whitelist un expéditeur de confiance ?

Réponse

Sur l'appliance de sécurité du courrier électronique de Cisco (ESA), ajoutez les expéditeurs que vous faites confiance au groupe d'expéditeur WHITELIST parce que ce groupe d'expéditeur utilise la stratégie de flux de courrier \$TRUSTED. Les membres du groupe d'expéditeur WHITELIST ne sont pas sujets à la limitation de débit, et le contenu de ces expéditeurs n'est pas balayé par l'engine de courrier indésirable d'IronPort Cisco, mais est toujours balayé par le logiciel antivirus de Sophos.

Note: Par configuration par défaut, la lecture d'antivirus est activée mais l'anti-Spam est arrêté.

Au whitelist un expéditeur, ajoutez l'expéditeur au groupe d'expéditeur WHITELIST dans le Tableau d'accès au hôte (CHAPEAU). Vous pouvez configurer le CHAPEAU par l'intermédiaire du GUI ou du CLI.

Du GUI

1. Cliquez sur l'onglet de *stratégies de messagerie*.
 2. Sous la section de *Tableau d'accès au hôte*, *vue d'ensemble* choisie de *CHAPEAU*,
 3. Du côté droit, assurez-vous que votre auditeur d'*InboundMail* est actuellement sélectionné,
 4. De la colonne de *groupe d'expéditeur* ci-dessous, clic *WHITELIST*,
 5. Cliquez sur le bouton d'*expéditeur d'ajouter* près de la moitié inférieure de la page.
 6. Entrez dans l'IP ou l'adresse Internet que vous voulez au whitelist dans le premier domaine.
- Quand vous finissez d'ajouter des entrées, cliquez sur le bouton de *soumission*. Souvenez-

vous pour cliquer sur les *modifications de validation* se boutonnet pour sauvegarder vos modifications.

Du 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

[>

Souvenez-vous pour émettre la commande de validation de sauvegarder vos modifications.

[Informations connexes](#)

- [Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur](#)
- [Support et documentation techniques - Cisco Systems](#)