Allow a Trusted Sender to Bypass Anti-Spam

Contents

Introduction

This document describes the details of allowing a trusted sender to bypass Anti-Spam scanning and also the different methods that you can opt for the same on the Secure Email Gateway (formerly known as the Email Security Appliance).

Addition of Sender Hostname/IP Address in ALLOWED_LIST Sender Group

Add senders you trust to the ALLOWED_LIST sender group because this sender group uses the $TRUSTED mail flow policy. Members of the ALLOWED_LIST sender group are not subject to rate limiting, and the content from those senders is not scanned by the Anti-Spam engine but is still scanned by Anti-Virus.

> **Note**: With the default configuration, Anti-Virus scanning is enabled but Anti-Spam is turned off.

In order to allow a sender to bypass Anti-Spam scanning, add the sender to the ALLOWED_LIST sender group in the Host Access Table (HAT). You can configure the HAT via the GUI or the CLI.

From the GUI

1. Select the **Mail Policies** tab.
2. Under the **Host Access Table** section, select **HAT Overview**.
3. On the right, make sure your **InboundMail** listener is currently selected.
4. From the **Sender Group** column, select **ALLOWED_LIST**.
5. Select the **Add Sender** button near the bottom half of the page.
6. Enter the IP or Hostname you want to allow to bypass in the first field.

When you finish adding entries, select the **Submit** button. Remember to select the **Commit Changes** button in order to save your changes.

From the 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. 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 SBRS[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
[]>
```

Remember to issue the **commit** command in order to save your changes.

Review the Anti-Spam and Anti-Virus Scanning in the Trusted Mail Flow Policy

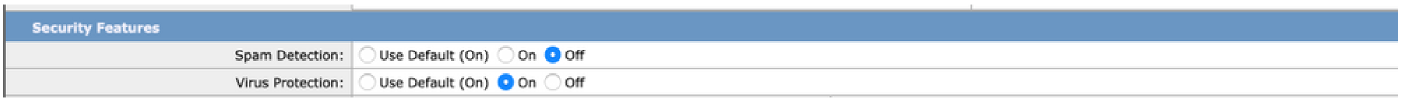
For the Trusted sender, there will be a Mail Flow Policy named as a Trusted present by default. The Trusted Mail Flow Policy will have a Connection behavior of Accept (similar to the behavior for other Mail Flow policies for incoming emails).

When a sender is trusted for business requirements, we can opt to disable the Antivirus and Anti-spam checks for them. This will help reduce the extra processing load on both the scanning engines while they scan the emails that aren't from trusted sources.

> **Note**: The Anti-spam and Anti-virus engines disabled, will skip any Spam or Virus related scans for the incoming email in ESA. This has to be done, only if you are totally sure that skipping scans for these trusted senders possess no risk.

The Option from where you can disable the engines are available in the tab of Security Features in Mail Flow Policies. The path for the same is **GUI > Mail Policies > Mail Flow Policies**. Click on the **TRUSTEDMail flow policy** and scroll down to **Security Features** on the subsequent page.

Ensure to commit the changes after you make tweaks as desired.



Security Features

Spam Detection:	○ Use Default (On) ○ On ● Off
Virus Protection:	○ Use Default (On) ● On ○ Off

Add a Trusted Sender to Safelist

End-user safelists and blocklists are created by end-users and stored in a database that is checked prior to anti-spam scanning. Each end-user can identify domains, sub-domains, or email addresses that they wish to always treat as spam or never treat as spam. If a sender address is part of an end-users safelist, anti-spam scanning is skipped

This set-up will enable the end-user to Safelist a sender as per their requirement for exempting the Anti-spam scans. The Antivirus scanning and other scans in the email pipeline will be untouched with this setup and will continue as per the configuration in the Mail Policies. This setup in a way will reduce the admin's engagement, every time an end-user has to exempt spam scanning for a sender.

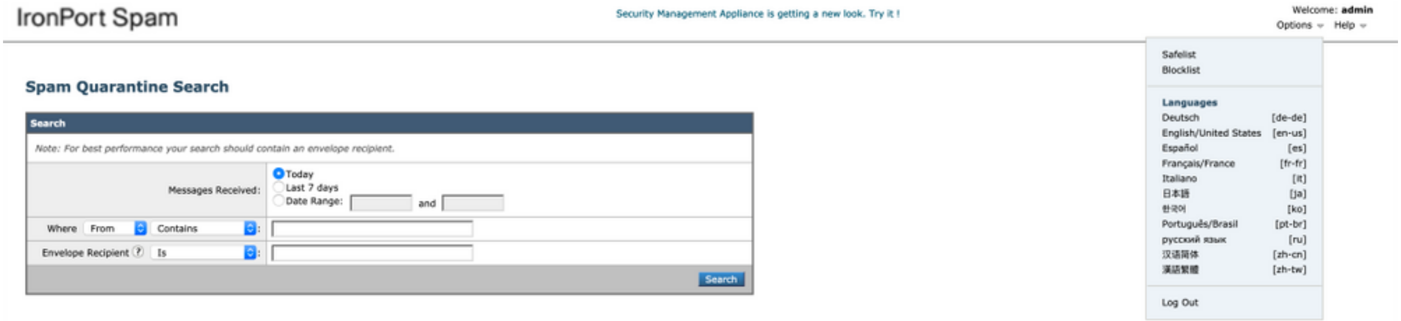
For the Safelist, it is mandatory to have the End-User Quarantine access enabled for the End Users and End-User Safelist/Blocklist as Enabled (both in ESA or SMA). That way they can access the Spam Quarantine portal and alongside **Release/Delete** of the quarantined emails, they can also **Add/Delete** senders in Safelist.

End-User Quarantine access can be enabled as beneath:

ESA: Navigate to **GUI > Monitor > Spam Quarantine**. Check-in the **Radio** button for **End-User Quarantine Access**. Select the Authentication method for access as per requirement (None/LDAP/SAML/IMAP or POP). Post that, enable end-user safelist/blocklist.

SMA: Navigate to **GUI > Centralized Services > Spam Quarantine**. Check-in the **Radio** button for **End-User Quarantine Access**. Select the Authentication method for access as per requirement (None/LDAP/SAML/IMAP or POP). Post that, enable end-user safelist/blocklist.

Once enabled, when an end-user navigates to the Spam Quarantine portal they'll be able to **add/modify** their Safelist as per choice from dropdown options from the top right.



Spam Quarantine Search

Search

Note: For best performance your search should contain an envelope recipient.

Messages Received:	● Today ○ Last 7 days ○ Date Range: ____ and ____
Where From Contains:	
Envelope Recipient Is:	

Trusted Senders with Incoming Mail Policies

You can also add a Trusted Sender in the Incoming Mail Policy and disable **Antivirus/Antispam** scans as per the requirement. A new customized Mail Policy can be created with a name such as **Trusted Senders/Safe Senders** etc. as per choice and then you can add the sender details such as domain names or sender email addresses to this custom policy.

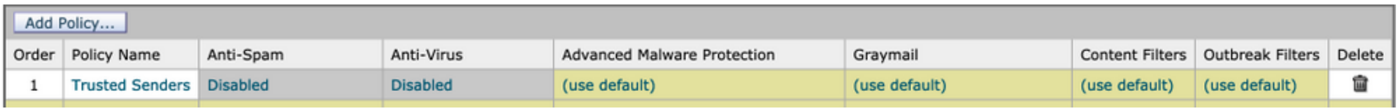
Once you submit the policy after the required addition, you can click on the columns of **Antispam** or **Antivirus,** and on the subsequent page, select **Disable**.

With this setup, the trusted sender domains or email addresses added to this mail policy will be exempted from Antispam or Antivirus scans.

> **Note**: The Anti-spam and Anti-virus engines disabled, will skip any Spam or Virus related scans for the incoming email in ESA processed via this custom mail policy. This has to be done, only if you are totally sure that skipping scans for these trusted senders possess no risk.

The custom Mail Policy can be created from **ESA GUI > Mail Policies > Incoming Mail Policies > Add Policy**. Enter Policy name as per choice, then select **Add User**. Check in the radio button for **Following Senders.** Add the required domain or email addresses in the box and click **Ok**.

Post mail policy creation, you can select to disable the Antivirus and Antispam scans as per business requirements. Here is an example screenshot:



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)	🗑

Related Information

- **Cisco Email Security Appliance - End-User Guides**
- **Technical Support & Documentation - Cisco Systems**