

允许受信任发件人绕过反垃圾邮件

目录

[简介](#)

[在ALLOWED_LIST发件人组中添加发件人主机名/IP地址](#)

[从GUI](#)

[从CLI](#)

[查看受信任邮件流策略中的反垃圾邮件和防病毒扫描](#)

[将受信任发件人添加到安全列表](#)

[具有传入邮件策略的受信任发件人](#)

[相关信息](#)

简介

本文档介绍允许受信任发件人绕过反垃圾邮件扫描的详细信息，以及您可以选择在安全邮件网关（以前称为邮件安全设备）上进行扫描的不同方法。

在ALLOWED_LIST发件人组中添加发件人主机名/IP地址

将您信任的发件人添加到ALLOWED_LIST发件人组，因为此发件人组使用\$TRUSTED邮件流策略。ALLOWED_LIST发件人组的成员不受速率限制，来自这些发件人的内容不由反垃圾邮件引擎扫描，但仍由反病毒扫描。

注意：使用默认配置时，防病毒扫描已启用，但防垃圾邮件已关闭。

要允许发件人绕过反垃圾邮件扫描，请将发件人添加到主机访问表(HAT)中的ALLOWED_LIST发件人组。您可以通过GUI或CLI配置HAT。

从GUI

1. 选择“邮件策略”选项卡。
2. 在主机访问表部分下，选择HAT概述。
3. 在右侧，确保当前已选择InboundMail侦听程序。
4. 从“发件人组”列中，选择ALLOWED_LIST。
5. 选择页面下半部附近的“添加发件人”按钮。
6. 在第一个字段中输入要允许绕行的IP或主机名。

完成添加条目后，选择“提交”按钮。切记选择“提交更改”按钮以保存更改。

从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 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

```
[]>
```

请记住发出commit命令以保存更改。

查看受信任邮件流策略中的反垃圾邮件和防病毒扫描

对于受信任发件人，默认情况下将存在名为受信任存在的邮件流策略。受信任邮件流策略的连接行为为“接受”(Accept) (类似于传入邮件的其他邮件流策略的行为)。

当信任发件人满足业务需求时，我们可以选择禁用防病毒和反垃圾邮件检查。这将有助于减少两个扫描引擎扫描不来自受信任来源的电子邮件时的额外处理负载。

注意：禁用的反垃圾邮件和防病毒引擎将跳过ESA中传入邮件的任何垃圾邮件或病毒相关扫描。只有当您完全确定跳过这些受信任发件人的扫描时，才必须执行此操作。

在邮件流策略中的安全功能选项卡中提供可禁用引擎的选项。相同的路径为**GUI > Mail Policies > Mail Flow Policies**。单击**USTATEDMail流策略**，然后向下滚动到后续页面上的“安全功能”。

确保在根据需要进行调整后提交更改。

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

将受信任发件人添加到安全列表

最终用户安全列表和阻止列表由最终用户创建并存储在反垃圾邮件扫描之前检查的数据库中。每个最终用户都可以识别他们希望始终视为垃圾邮件或从不被视为垃圾邮件的域、子域或电子邮件地址。如果发件人地址是最终用户安全列表的一部分，则跳过反垃圾邮件扫描

此设置将使最终用户能够根据发件人免除反垃圾邮件扫描的要求安全列出发件人。防病毒扫描和邮件管道中的其他扫描将不受此设置的影响，并将根据邮件策略中的配置继续。此设置将减少管理员

的参与，每次最终用户必须免除发件人的垃圾邮件扫描。

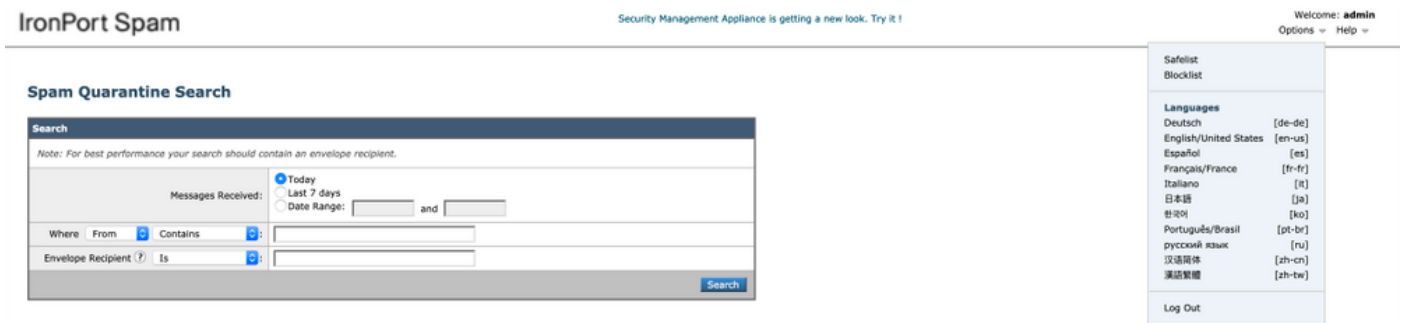
对于安全列表，必须为最终用户和最终用户安全列表/阻止列表启用最终用户隔离区访问权限（在ESA或SMA中）。这样，他们可以访问垃圾邮件隔离区门户，并在**隔离邮件**的“释放/删除”(Release/Delete)的同时，还可以在安全列表中添加/删除发件人。

可启用**最终用户隔离区**访问，如下所示：

ESA:导航至**GUI > 监视器 > 垃圾邮件隔离区**。请签入**最终用户隔离区访问单选按钮**。根据要求（None/LDAP/SAML/IMAP或POP）为访问选择身份验证方法。发布该命令后，启用最终用户安全列表/阻止列表。

SMA:导航至**GUI > Centralized Services > Spam Quarantine**。选中“End-User Quarantine Access(**最终用户隔离区访问**)”的**单选按钮**。根据要求（None/LDAP/SAML/IMAP或POP）为访问选择身份验证方法。发布该命令后，启用最终用户安全列表/阻止列表。

启用后，当最终用户导航到垃圾邮件隔离区门户时，他们将能够根据自右上角下拉选项的**选择添加/修改其安全列表**。



具有传入邮件策略的受信任发件人

您还可以根据要求在传入邮件策略中添加受信任发件人并**禁用防病毒/反垃圾邮件扫描**。可以根据选择使用名称(如**受信任发件人/安全发件人**等)创建新的自定义邮件策略，然后您可以将发件人详细信息（如域名或发件人电子邮件地址）添加到此自定义策略。


在所需添加后提交策略后，可以单击“反垃圾邮件”或“防病毒”列，然后在后面的页面上选择**禁用**。

通过此设置，添加到此邮件策略的受信任发件人域或电子邮件地址将免除反垃圾邮件或防病毒扫描。

注意：禁用的反垃圾邮件和防病毒引擎将跳过通过此自定义邮件策略处理的ESA中传入邮件的任何垃圾邮件或病毒相关扫描。只有当您完全确定跳过这些受信任发件人的扫描时，才必须执行此操作。

可以从ESA GUI > Mail Policies > Incoming Mail Policies > Add Policy**创建自定义邮件策略**。根据选择输入策略名称，然后选择**添加用户**。选中“以下发件人”的**单选按钮**。在框中添加所需的域或电子邮件地址，然后单击“**确定**”。

创建邮件策略后，您可以选择根据业务需求禁用防病毒和反垃圾邮件扫描。以下是示例屏幕截图：

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)	

相关信息

- [思科邮件安全设备 — 最终用户指南](#)
- [技术支持和文档 - Cisco Systems](#)