垃圾邮件隔离区

本章包含以下部分：

垃圾邮件隔离区概述

垃圾邮件隔离区（也称为 ISQ）和最终用户隔离区（也称为 EUQ）为关注“误报”（即，设备视为垃圾邮件的合法邮件）的组织提供保障机制。当设备确定邮件是垃圾邮件或可疑垃圾邮件时，您可能希望在传送或删除邮件之前让收件人或管理员对其进行审核。为此，垃圾邮件隔离区会存储邮件。

设备的管理用户可查看垃圾邮件隔离区中的所有邮件。最终用户（通常是邮件收件人）可在略微不同的 Web 界面中查看各自的隔离邮件。

垃圾邮件隔离区与策略、病毒和爆发隔离区分隔。

相关主题

- 集中策略、病毒和病毒爆发隔离区

本地与外部垃圾邮件隔离区

本地垃圾邮件隔离区在设备上存储垃圾邮件和可疑垃圾邮件。外部垃圾邮件隔离区可在独立的 思科内容安全管理设备上存储这些邮件。

如果满足以下条件，请考虑使用外部垃圾邮件隔离区：

- 希望在某个位置集中存储和管理来自多个设备的垃圾邮件。
- 希望存储的垃圾邮件数量超过设备可承载的范围。
- 希望定期备份垃圾邮件隔离区及其邮件。

设置集中垃圾邮件隔离区

Procedure

	Command or Action	Purpose
步骤 1	在安全管理设备上，启用集中式垃圾邮件隔离区服务。	启用和配置垃圾邮件隔离区, on page 2
步骤 2	在安全管理设备上，指定集中垃圾邮件隔离区要包括的邮件安全设备。	向每个托管邮件安全设备添加集中垃圾邮件隔离区服务 , on page 5
步骤 3	设置安全管理设备，以便发送通知和释放的垃圾邮件。	在安全管理设备上配置出站 IP 接口 , on page 6
步骤 4	在安全管理设备上，配置垃圾邮件隔离区浏览器界面。	配置浏览器访问垃圾邮件隔离区的 IP 接口 , on page 7
步骤 5	确保邮件安全设备配置为发送邮件到垃圾邮件隔离区。	有关配置反垃圾邮件和邮件策略的详细信息，请参阅《邮件安全设备 *AysncOS* 用户指南》中的“反垃圾邮件”部分。
步骤 6	在邮件安全设备中，启用和配置外部垃圾邮件隔离区。	有关详细信息，请参阅《思科邮件安全设备 *AsyncOS* 用户指南》。
步骤 7	在邮件安全设备上，禁用本地隔离区。	有关禁用本地垃圾邮件隔离区以激活外部垃圾邮件隔离区的信息，请参阅《邮件安全设备 *AysncOS* 用户指南》。

启用和配置垃圾邮件隔离区

- 在旧 Web 界面上启用和配置垃圾邮件隔离区 ， 第 2 页
- 在新 Web 界面上启用和配置垃圾邮件隔离区

在旧 Web 界面上启用和配置垃圾邮件隔离区

步骤 1 依次选择**管理设备 (Management Appliance)** > **集中服务 (Centralized Services)** > **垃圾邮件隔离区 (Spam Quarantine)**。

步骤 2 如果是在运行“系统设置向导”(System Setup Wizard) 后首次启用垃圾邮件隔离区：

a) 单击**启用 (Enable)**。

b) 审查最终用户许可协议，然后单击**接受 (Accept)**。

步骤 3 如果要编辑垃圾邮件隔离区设置，请单击**编辑设置 (Edit Settings)** 。

步骤 4 指定选项：

选项	说明
隔离区 IP 接口 (Quarantine IP Interface) 隔离区端口 (Quarantine Port)	默认情况下，垃圾邮件隔离区使用管理接口和端口 6025。IP 接口是指安全管理设备上配置为监听传入邮件的接口。隔离区端口是指发送设备在其外部隔离区设置中使用的端口号。 如果您的邮件安全设备与安全管理设备不在同一个网络上，则必须使用管理接口。
邮件传送方式 (Deliver Messages Via)	所有与隔离区相关的传出邮件（例如从垃圾邮件隔离区发出的垃圾邮件通知和邮件）都必须通过其他配置为发送邮件的设备或服务器来传送。 可以通过 SMTP 或群组组件服务器传输这些邮件，也可以指定设备的出站监听程序接口（通常为 Data 2 接口）。 备用地址用于负载均衡和故障转移。 如果有多个设备，可以针对主要和备用地址使用任何托管设备的出站监听程序接口。两种地址均必须使用同一接口（Data 1 或 Data 2）作为出站侦听程序。 请阅读屏幕上的说明，以了解有关这些地址的其他警告。
计划删除前的保留天数 (Schedule Delete After)	指定在删除邮件之前将其保留的天数。 思科建议配置隔离区以删除较旧的邮件，从而防止隔离区装满，但是您可以选择不计划自动删除。
放行邮件时通知思科 (Notify Cisco Upon Message Release)	如果您希望在放行邮件时通知思科，请选中**将放行邮件的副本发送给思科进行分析（推荐） (Send a copy of released messages to Cisco for analysis [recommended])** 复选框。
垃圾邮件隔离区外观 (Spam Quarantine Appearance)	**徽标 (Logo)** 默认情况下，当用户登录查看隔离邮件时，思科徽标会显示在垃圾邮件隔离区页面的顶部。 您可以在新 Web 界面和旧 Web 界面上查看徽标。 要改用自定义徽标，请上传该徽标。徽标应为 .jpg、.gif 或 .png 文件，最大尺寸为 50 像素（高）× 500 像素（宽）。
	登录页面消息 (Login page message) （可选）指定登录页面消息。当最终用户和管理员登录查看隔离区时，将会向其显示此消息。 如果不指定消息，则显示以下消息： 在下面输入登录信息。如果不确定要输入的内容，请与管理员联系。

选项	说明
管理用户 (Administrative Users)	请参阅配置对垃圾邮件隔离区的管理用户访问权限 , on page 7。

步骤 5 提交并确认更改。

What to do next

- 退回至 向每个托管邮件安全设备添加集中垃圾邮件隔离区服务 , on page 5

在新 Web 界面上启用和配置垃圾邮件隔离区

步骤 1 在安全管理设备上，单击**服务状态 (Service Status)**，然后将鼠标悬停在与**垃圾邮件隔离区**对应的 ⚙ 上方，然后单击**编辑垃圾邮件隔离区设置 (Edit Spam Quarantine Settings)**。

步骤 2 如果您在运行“系统设置向导”后首次使用配置垃圾邮件隔离区，请查看许可协议，然后单击**继续 (Proceed)**。

步骤 3 单击切换开关以启用垃圾邮件隔离区。

步骤 4 指定选项：

选项	说明
隔离区 IP 接口 (Quarantine IP Interface) 隔离区端口 (Quarantine Port)	默认情况下，垃圾邮件隔离区使用管理接口和端口 6025。IP 接口是指安全管理设备上配置为监听传入邮件的接口。隔离区端口是指发送设备在其外部隔离区设置中使用的端口号。 如果您的邮件安全设备与安全管理设备不在同一个网络上，则必须使用管理接口。
邮件传送方式 (Deliver Messages Via)	所有与隔离区相关的传出邮件（例如从垃圾邮件隔离区发出的垃圾邮件通知和邮件）都必须通过其他配置为发送邮件的设备或服务器来传送。 可以通过 SMTP 或群组组件服务器传输这些邮件，也可以指定邮件安全设备的出站监听程序接口（通常为 Data 2 接口）。 备用地址用于负载均衡和故障转移。 如果有多个邮件安全设备，可以针对主要和备用地址使用任何托管邮件安全设备的出站监听程序接口。两种地址均必须使用同一接口（Data 1 或 Data 2）作为出站侦听程序。 请阅读屏幕上的说明，以了解有关这些地址的其他警告。
计划删除前的保留天数 (Schedule Delete After)	指定在删除邮件之前将其保留的天数。 思科建议配置隔离区以删除较旧的邮件，从而防止隔离区装满，但是您可以选择不计划自动删除。

选项	说明
放行邮件时通知思科 (Notify Cisco Upon Message Release)	您可以选中相应的复选框，以便选择将已放行邮件的副本发送给思科进行分析。
垃圾邮件隔离区外观 (Spam Quarantine Appearance)	**徽标 (Logo)** 默认情况下，当用户登录查看隔离邮件时，思科徽标会显示在垃圾邮件隔离区页面的顶部。 您可以在新 Web 界面和旧 Web 界面上查看徽标。 要改用自定义徽标，请上传该徽标。徽标应为 .jpg、.gif 或 .png 文件，最大尺寸为 50 像素（高）× 500 像素（宽）。
	登录页面消息 (Login page message) （可选）指定登录页面消息。当最终用户和管理员登录查看隔离区时，将会向其显示此消息。 如果不指定消息，则显示以下消息： 在下面输入登录信息。如果不确定要输入的内容，请与管理员联系。
管理用户 (Administrative Users)	请参阅配置对垃圾邮件隔离区的管理用户访问权限 , on page 7。

步骤 5 单击**保存 (Save)**。

What to do next

- 退回至 向每个托管邮件安全设备添加集中垃圾邮件隔离区服务 , on page 5

向每个托管邮件安全设备添加集中垃圾邮件隔离区服务

执行的步骤取决于是否已在配置其他集中管理功能时添加了设备。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，单击 ⚙ 加载旧 Web 界面。

步骤 2 选择**管理设备 > 集中化服务 > 安全设备**。

步骤 3 如果已向此页面的列表中添加了邮件安全设备，请执行以下操作：

a) 单击邮件安全设备的名称。

b) 选择**垃圾邮件隔离区**服务。

步骤 4 如果您尚未添加邮件安全设备，请执行以下操作：

a) 单击“添加邮件设备”(Add Email Appliance)。

b) 在“设备名称”(Appliance Name) 和“IP 地址”(IP Address) 文本字段中，键入设备的管理接口的设备名称和 IP 地址。

Note 可以在“IP 地址”(IP Address) 文本字段中输入 DNS 名称；但是，当单击**提交 (Submit)** 时，系统会立即将其解析为 IP 地址。

c) 已预先选择垃圾邮件隔离区服务。
d) 单击**建立连接 (Establish Connection)**。
e) 在要托管的设备上输入管理员账户的用户名和口令，然后单击**建立连接 (Establish Connection)**。

Note 输入登录凭证，以便将文件传输的公共 SSH 密钥从安全管理设备传递到远程设备。登录凭证不会存储在安全管理设备上。

f) 等待在页面中的表上出现成功消息。
g) 单击**测试连接 (Test Connection)**。
h) 阅读表上的测试结果。

步骤 5 提交并确认更改。

步骤 6 对于要启用垃圾邮件隔离区的每台邮件安全设备，重复上述程序。

在安全管理设备上配置出站 IP 接口

在安全管理设备上配置一个接口，用于将隔离区相关的邮件（包括通知和释放的邮件）发送到邮件安全设备进行传送。

Before you begin

获取或识别用于出站接口的 IP 地址。出站接口通常是安全管理设备上的 Data 2 接口。有关网络要求的详细信息，请参阅 分配网络和 IP 地址

Note 请将此过程与配置 IP 接口中的信息结合使用。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，单击 加载旧 Web 界面。

步骤 2 选择**管理设备 > 网络 IP 接口**。

步骤 3 单击**添加 IP 接口 (Add IP Interface)**。

步骤 4 输入以下设置：

- 名称
- 以太网端口 (Ethernet Port)

  通常，此接口将是 Data 2 接口。具体而言，该端口必须与在**管理设备 > 集中服务 > 垃圾邮件隔离区**下为“垃圾邮件隔离区设置”页面**邮件传送方式**部分的**主服务器**指定的邮件安全设备上的数据接口匹配。

- IP 地址 (IP Address)

  您刚指定的接口的 IP 地址。

- 网络掩码 (Netmask)
- 主机名

  例如，如果是 Data 2 接口，请使用 data2.sma.example.com。

请勿在此接口的“垃圾邮件隔离区”(Spam Quarantine) 部分中输入信息。

步骤 5 提交并确认更改。

配置浏览器访问垃圾邮件隔离区的 IP 接口

当管理员和最终用户访问垃圾邮件隔离区时，系统将会打开单独的浏览器窗口。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，单击 加载旧 Web 界面。

步骤 2 依次选择**管理设备** > **网络** > **IP 接口**。

步骤 3 单击**管理**接口的名称。

步骤 4 在“垃圾邮件隔离区”(Spam Quarantine) 部分中，配置对垃圾邮件隔离区的访问设置：

- 默认情况下，HTTP 使用端口 82，HTTPS 使用端口 83。
- 指定在通知和垃圾邮件隔离区浏览器窗口中显示的 URL。

  如果不希望向最终用户显示安全管理设备的主机名，可以指定一个备用主机名。

步骤 5 提交并确认更改。

What to do next

确保 DNS 服务器可以解析为访问垃圾邮件隔离区指定的主机名。

配置对垃圾邮件隔离区的管理用户访问权限

具有管理员权限的所有用户都可以更改垃圾邮件隔离区设置，并查看和管理垃圾邮件隔离区中的的邮件。您无需为管理员用户配置垃圾邮件隔离区访问权限。

如果为具有以下角色的用户配置对垃圾邮件隔离区的访问权限，则他们可以查看、放行和删除垃圾邮件隔离区中的邮件：

- 邮件管理员 (Email administrator)
- 操作员 (Operator)
- 只读操作员 (Read-only operator)
- 服务中心用户 (Help desk user)
- 访客 (Guest)

- 具有垃圾邮件隔离区权限的“自定义用户”(Custom user) 角色

这些用户无法访问垃圾邮件隔离区设置。

Before you begin

创建有权访问垃圾邮件隔离区的用户或自定义用户角色。有关详细信息，请参阅中关于自定义用户角色的隔离区访问权限的信息分配管理任务

步骤 1 在安全管理设备上，单击**服务状态 (Service Status)**，然后将鼠标悬停在与**垃圾邮件隔离区**对应的 ⚙ 上方，然后单击**编辑垃圾邮件隔离区设置 (Edit Spam Quarantine Settings)**。

步骤 2 单击切换开关以启用垃圾邮件隔离区。

步骤 3 单击要添加的用户类型的链接：本地、外部身份验证或自定义角色。

如果您已添加用户或角色，请单击用户名或角色以查看所有合格的用户或角色。

步骤 4 选择要添加的用户或角色。

未列出具有管理员权限的用户（包括邮件管理员），因为他们自动具有访问垃圾邮件隔离区的完整权限。

步骤 5 单击**确定 (OK)**。

步骤 6 单击**提交 (Submit)**。

What to do next

相关主题

配置最终用户访问垃圾邮件隔离区的权限 , on page 24

垃圾邮件隔离区阈值警报

您可以配置为在达到一定时间内可触发的最大垃圾邮件数量后接收警报通知。除了配置自己的警报，还可以配置思科安全邮件和 Web 管理器，以便每小时或每天生成警报。但是，您也可以设置超过阈值后在持续时间内可以接收的最大警报数。

如果管理员映射到此自定义角色，则他们可以查看隔离区邮件，但无法执行释放、删除或任何其他操作。

思科安全邮件和 Web 管理器可确保您收到设置为邮件和系统日志的警报。

使用 CLI 配置垃圾邮件隔离区阈值警报设置

要配置垃圾邮件隔离区阈值警报，请使用 **spamquarantinethresholdalert** 命令。

执行命令后，必须启用可用的服务。

您必须为以下各项提供值：

- 阈值 (Threshold) - 仅数字。配置将在所选时间内发送警报的新隔离垃圾邮件的阈值。值范围为 1-1,00,000。
- 时间持续时间 (Time Duration) - 配置监控垃圾邮件的持续时间（小时）。值范围介于 1800 到 86400 秒之间。
- 警报限制 (Alert Limit) - 仅数字。配置警报限制。值范围为 1-20。

过程

	命令或操作	目的
步骤 1	spamquarantinethresholdalert 示例： `spamquarantinethresholdalert`	配置垃圾邮件隔离区阈值警报。

示例

使用 GUI 配置垃圾邮件隔离区阈值警报设置

步骤 1 单击**集中服务 (Centralized Services)** > **垃圾邮件隔离区 (SPAM Quarantine)**

系统将显示“垃圾邮件隔离区”(SPAM Quarantine) 页面。

步骤 2 启用**阈值警报 (Threshold Alert)** 复选框。

垃圾邮件隔离区阈值警报也由“系统警报”(System Alerts) 设置进行管理。要配置收件人，必须导航至**系统管理 (System Administration)** > **警报 (Alerts)**。

要接收这些警报，您必须订用系统严重警报。

步骤 3 输入阈值的值

步骤 4 从下拉列表中选择**持续时间 (Time Duration)**。

值范围介于半小时到 24 小时之间。

步骤 5 输入**警报限制 (Alert Limit)**。

值范围介于 1 到 20 之间。

步骤 6 单击**提交 (Submit)**。

限制邮件被隔离的收件人

在可以使用多个邮件策略（“邮件策略”>“传入邮件策略”），以指定邮件不会被隔离的收件人地址列表。为邮件策略配置反垃圾邮件设置时，选择“传送”(Deliver) 或“丢弃”(Drop)，而不是隔离。

垃圾邮件隔离区语言

每个用户都可从窗口右上角的“选项 (Options)”菜单中选择垃圾邮件隔离区的语言。

编辑垃圾邮件隔离区页面

- 在旧 Web 界面上启用和配置垃圾邮件隔离区 , on page 2
- 本地与外部垃圾邮件隔离区 , on page 1
- 配置最终用户访问垃圾邮件隔离区的权限 , on page 24
- 通知最终用户被隔离的邮件 , on page 26

使用安全列表和阻止列表基于发件人控制邮件发送

管理员和最终用户可以使用安全列表和阻止列表来帮助确定哪些邮件是垃圾邮件。安全列表指定从未被视为垃圾邮件的发件人和域。阻止列表指定始终被视为垃圾邮件的发件人和域。

可以允许最终用户（邮件用户）管理自己邮件账户的安全列表和阻止列表。例如，某个最终用户可能会收到其不再感兴趣的邮件列表发来的邮件。他可决定将此发件人添加到他的阻止列表，以防止将来自邮件列表的邮件发送到他的收件箱。另一方面，最终用户可能发现特定发件人的邮件被发送到其垃圾邮件隔离区，而他们不希望这些邮件被视为垃圾邮件。为确保来自这些发件人的邮件不被隔离，他们可能要将发件人添加到其安全列表。

最终用户和管理员所做的更改对彼此可见，并且双方可以相互更改。

相关主题

- 安全列表和阻止列表的邮件处理 , on page 11
- 在旧 Web 界面上启用安全列表和阻止列表, on page 11
- 外部垃圾邮件隔离区和安全列表/阻止列表 , on page 12
- 向安全列表和阻止列表中添加发件人和域（管理员） , on page 13
- 关于最终用户访问安全列表和阻止列表 , on page 18
- 备份和恢复安全列表/阻止列表 , on page 19
- 安全列表和阻止列表故障排除, on page 20

安全列表和阻止列表的邮件处理

发件人在安全列表还是阻止列表中并不会阻止设备扫描邮件以查找病毒，或确定邮件是否满足与内容相关的邮件策略的条件。即使邮件的发件人包含在收件人的安全列表中，邮件也可能不会传送到最终用户，具体取决于其他扫描设置和结果。

当启用安全列表和阻止列表时，设备会在反垃圾邮件扫描之前瞬时根据安全列表/阻止列表数据库扫描邮件。如果设备检测到与安全列表或阻止列表条目相匹配的发件人或域，则在有多个收件人（并且收件人具有不同的安全列表/阻止列表设置）的情况下将拆分邮件。例如，邮件同时发送到收件人 A 和收件人 B。收件人 A 已将发件人列入安全列表，而收件人 B 在安全列表或阻止列表中没有发件人的对应条目。在此情况下，邮件可拆分为具有两个邮件 ID 的两封邮件。发送给收件人 *A* 的邮件标记为安全，信头为 *X-SLBL-Result-Safelist*，并跳过反垃圾邮件扫描，而发往收件人 *B* 的邮件将由反垃圾邮件扫描引擎扫描。然后，两封邮件会沿管道（通过防病毒扫描和内容策略等等）继续发送，并且遵从任何已配置的设置。

如果邮件发件人或域已列入阻止列表，则传送行为取决于启用安全列表/阻止列表功能时指定的阻止列表操作。与安全列表传送类似，如果存在具有不同安全列表/阻止列表设置的不同收件人，则会拆分邮件。然后，根据阻止列表操作设置，系统将隔离或丢弃已列入阻止列表的拆分邮件。如果阻止列表操作配置为隔离，则系统会扫描并最终隔离邮件。如果阻止列表操作配置为删除，则在安全列表/阻止列表扫描后会立即丢弃邮件。

由于安全列表和阻止列表在垃圾邮件隔离区中进行维护，因此传送行为也取决于其他反垃圾邮件设置。例如，如果将主机访问表 (HAT) 中的“接受”邮件流策略配置为跳过反垃圾邮件扫描，则在该侦听程序上接收邮件的用户不会将其安全列表和阻止列表设置应用于在该侦听程序上收到的邮件。同样，如果创建可跳过某些邮件收件人的反垃圾邮件扫描的邮件流策略，则这些收件人将不会应用其安全列表和阻止列表设置。

相关主题

- 在旧 Web 界面上启用安全列表和阻止列表, on page 11
- 外部垃圾邮件隔离区和安全列表/阻止列表 , on page 12

启用安全列表和阻止列表

- 在旧 Web 界面上启用安全列表和阻止列表 ， 第 11 页
- 在新 Web 界面上启用安全列表和阻止列表

在旧 Web 界面上启用安全列表和阻止列表

Before you begin

- 必须启用垃圾邮件隔离区。请参阅设置集中垃圾邮件隔离区 , on page 2。

步骤 1 导航至**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 垃圾邮件隔离区 (Spam Quarantine)**。

步骤 2 在**终端用户安全列表/阻止列表 (End-User Safelist/Blocklist)** 下，单击**编辑设置 (Edit Settings)**。

步骤 3 选择**启用最终用户安全列表/阻止列表功能 (Enable End User Safelist/Blocklist Feature)**。

步骤 4 指定**每个用户的最大列表项数 (Maximum List Items Per User)**。

这是每个收件人的每个列表的最大地址或域数量。如果允许每个用户有大量列表项，则系统性能可能会受到负面影响。

步骤 5 选择**更新频率 (Update Frequency)**。

此值决定在使用外部垃圾邮件隔离区的设备上，AsyncOS 更新安全列表/阻止列表的频率。有关此设置的意义，请参阅外部垃圾邮件隔离区和安全列表/阻止列表 , on page 12。

步骤 6 提交并确认更改。

在新 Web 界面上启用安全列表和阻止列表

Before you begin

- 必须启用垃圾邮件隔离区。请参阅设置集中垃圾邮件隔离区 , on page 2。

步骤 1 在安全管理设备上，单击**服务状态 (Service Status)**，然后将鼠标悬停在与**垃圾邮件隔离区**对应的 图标上方。

步骤 2 单击**编辑安全列表/阻止列表设置 (Edit Safelist/Blocklist Settings)**。

步骤 3 单击切换开关以启用安全列表/阻止列表设置。

步骤 4 指定**每个用户的最大列表项数 (Maximum List Items Per User)**。

这是每个收件人的每个列表的最大地址或域数量。如果允许每个用户有大量列表项，则系统性能可能会受到负面影响。

步骤 5 选择**更新频率 (Update Frequency)**。

此值决定在使用外部垃圾邮件隔离区的邮件安全设备上，AsyncOS 更新安全列表/阻止列表的频率。有关此设置的意义，请参阅外部垃圾邮件隔离区和安全列表/阻止列表 , on page 12。

步骤 6 单击**提交 (Submit)**。

外部垃圾邮件隔离区和安全列表/阻止列表

由于设备在处理传入邮件时会评估安全列表和阻止列表中的发件人，所以必须将 安全管理设备中存储的安全列表和阻止列表发送到 设备，以应用于传入邮件。在安全管理设备上配置安全列表/阻止列表功能时，可配置这些更新的频率。

向安全列表和阻止列表中添加发件人和域（管理员）

通过垃圾邮件隔离区界面管理安全列表和阻止列表。

您还可以查看是否许多收件人（组织中的最终用户）已将特定发件人或域纳入允许列表或阻止列表。

管理员可以查看并处理每个最终用户查看并处理的相同条目的超集。

Before you begin

- 请确保您可以访问垃圾邮件隔离区。请参阅访问垃圾邮件隔离区（管理用户）, on page 30。
- 启用对安全列表/阻止列表的访问。请参阅在旧 Web 界面上启用安全列表和阻止列表, on page 11。
- （可选）要导入安全列表/阻止列表（而不是使用此部分的步骤建立这些列表），请使用备份和恢复安全列表/阻止列表 , on page 19中所述的过程。
- 了解安全列表和阻止列表条目的所需格式。请参阅安全列表和阻止列表条目的语法 , on page 17。

步骤 1 [仅限新 Web 界面] 在安全管理设备上，单击**隔离区 (Quarantine)** > **垃圾邮件隔离区 (Spam Quarantine)** > **搜索 (Search)**。

或

依次选择**邮件** > **邮件隔离区** >**垃圾邮件隔离区**，然后选择页面右上角**选项**下拉菜单。

步骤 2 依次选择**安全列表 (Safelist)** 或**阻止列表 (Blocklist)**。

步骤 3 （可选）搜索发件人或收件人。

步骤 4 执行以下一项或多项操作：

收件人	相应操作
为收件人添加多个发件人	要在新 Web 界面上为某个收件人添加多个发件人： **a.** 选择**收件人**选项卡。 **b.** 单击 **+** 图标，添加收件人地址和发件人列表。 **c.** 输入收件人的邮件地址。 **d.** 输入发件人的邮件地址和域。 将每个条目放在单独的行上或用逗号分隔每个条目。 **e.** 单击 ✓ 保存条目。 要修改现有的发件人地址，请勾选必填收件人地址旁边的复选框，单击编辑图标，修改发件人地址，然后单击 ✓ 保存条目。 要在旧 Web 界面上为某个收件人添加多个发件人： **a.** 选择**查看方式：收件人 (View by: Recipient)** **b.** 单击**添加**，或者针对收件人单击**编辑 (Edit)**。 **c.** 输入或编辑收件人邮件地址。 **d.** 输入发件人邮件地址和域。 将每个条目放在单独的行上或用逗号分隔每个条目。 **e.** 单击**提交 (Submit)**。

收件人	相应操作
为发件人添加多个收件人	要在新 Web 界面上为某个发件人添加多个收件人： **a.** 选择**发件人**选项卡。 **b.** 单击 **+**，添加发件人地址和收件人列表。 **c.** 输入发件人的地址或域。 **d.** 输入收件人的邮件地址。 将每个条目放在单独的行上或用逗号分隔每个条目。 **e.** 单击 ✓ 保存条目。 要修改现有的收件人地址，请勾选必填发件人地址旁边的复选框，单击编辑图标，修改发件人地址，然后单击 ✓ 保存条目。 要在旧 Web 界面上为某个发件人添加多个收件人： **a.** 选择**查看方式：发件人 (View by: Sender)** **b.** 单击**添加**，或者针对发件人单击**编辑 (Edit)**。 **c.** 输入或编辑发件人地址或域。 **d.** 输入接收人邮件地址。 将每个条目放在单独的行上或用逗号分隔每个条目。 **e.** 单击**提交 (Submit)**。
删除与收件人关联的所有发件人	要在新 Web 界面上删除与某个收件人关联的所有发件人： **a.** 勾选收件人或发件人地址旁边的复选框，以选择条目。 您可以选择并删除所有条目。 **b.** 单击垃圾桶图标以删除整个表行。 要在旧 Web 界面上删除与某个收件人关联的所有发件人： **a.** 选择**查看方式 (View by)** 选项。 **b.** 单击垃圾箱图标以删除整个表行。

收件人	相应操作
删除与发件人关联的所有收件人	要在新 Web 界面上删除与某个发件人关联的所有收件人： **a.** 勾选收件人或发件人地址旁边的复选框，以选择条目。 您可以选择并删除所有条目。 **b.** 单击垃圾桶图标以删除整个表行。 要在旧 Web 界面上删除与某个发件人关联的所有收件人： **a.** 选择**查看方式 (View by)** 选项。 **b.** 单击垃圾箱图标以删除整个表行。
删除收件人的个别发件人	要在新 Web 界面上删除某个收件人的各个发件人： **a.** 勾选收件人或发件人地址旁边的复选框，选择条目。 您可以选择并删除多个条目。 **b.** 单击编辑图标，修改各个收件人或发件人。 **c.** 从文本框添加或删除条目。必须至少保留一个条目。 **d.** 单击 ✓ 保存条目。 要在旧 Web 界面上删除某个收件人的各个发件人： **a.** 选择**查看方式 (View by)** 选项。 **b.** 针对单个收件人或发件人单击**编辑 (Edit)**。 **c.** 从文本框添加或删除条目。必须至少保留一个条目。 **d.** 单击**提交 (Submit)**。

收件人	相应操作
删除发件人的个别收件人	要在新 Web 界面上删除某个发件人的各个收件人： **a.** 勾选收件人或发件人地址旁边的复选框，选择条目。 您可以选择并删除多个条目。 **b.** 单击编辑图标，修改各个收件人或发件人。 **c.** 从文本框添加或删除条目。必须至少保留一个条目。 **d.** 单击 ✓ 保存条目。 要在旧 Web 界面上删除某个收件人的各个发件人： **a.** 选择**查看方式 (View by)** 选项。 **b.** 针对单个收件人或发件人单击**编辑 (Edit)**。 **c.** 从文本框添加或删除条目。必须至少保留一个条目。 **d.** 单击**提交 (Submit)**。

What to do next

相关主题

- 安全列表和阻止列表条目的语法 , on page 17
- 清除所有安全列表和阻止列表 , on page 18

安全列表和阻止列表条目的语法

可以使用以下格式将发件人添加到安全列表和阻止列表：

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]
- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]
- user@[ipv6:2001:db8::1]

同一个条目（例如发件人地址或域）不能同时包含在安全列表和阻止列表中。但是，您可以在将一个域列入安全列表的同时，将属于该域的发件人的邮件地址列入阻止列表，反之亦然。在这种情况下，两种规则都适用。例如，如果 *example.com* 在安全列表中，则 *george@example.com* 可在阻止列表中。在此情况下，设备会传送来自 *example.com* 的所有邮件而不扫描垃圾邮件，但来自 *george@example.com* 的邮件（被视为垃圾邮件）除外。

不能对使用以下语法的子域范围执行允许或阻止操作：*.domain.com*。但是，可以阻止使用以下语法的特定域：*server.domain.com*。

清除所有安全列表和阻止列表

如果需要删除所有安全列表和阻止列表条目，包括所有发件人和所有收件人，请按照备份和恢复安全列表/阻止列表 , on page 19中的程序导入不含条目的文件。

关于最终用户访问安全列表和阻止列表

最终用户通过垃圾邮件隔离区访问其安全列表和阻止列表。要配置最终用户对垃圾邮件隔离区的访问权限，请参阅设置最终用户通过网络浏览器访问垃圾邮件隔离区的权限 。

您可能希望在适用情况下为最终用户提供垃圾邮件隔离区的 URL 和以下说明。

相关主题

- 向安全列表添加条目（最终用户）
- 将发件人添加到阻止列表（最终用户）

向安全列表添加条目（最终用户）

Note 列入安全列表的发件人的邮传送情况取决于系统中配置的其他设置。请参阅安全列表和阻止列表的邮件处理 , on page 11。

最终用户可以通过以下两种方式将发件人添加到安全列表：

- 将隔离邮件的发件人添加到安全列表 , on page 18
- 将发件人添加到不含隔离邮件的安全列表 , on page 19

将隔离邮件的发件人添加到安全列表

如果邮件已发送到垃圾邮件隔离区，则最终用户可以将发件人添加到安全列表。

[仅限新 Web 界面] 单击**释放并添加到安全列表 (Release and Add to Safelist)** 图标，释放邮件并将其添加到安全列表。

或

从下拉菜单中选择**放行并添加到安全列表 (Release and Add to Safelist)**。

可以将指定邮件的信封发件人和信头发件人都添加至安全列表，而放行的邮件可直接转至目标队列，跳过电子邮件管道中的任何其他工作队列处理。

将发件人添加到不含隔离邮件的安全列表

步骤 1 [仅限新 Web 界面] 选择**安全列表**。

步骤 2 [仅限新 Web 界面] 输入邮件地址或域。您可以输入多个域和邮件地址，以逗号分隔。

步骤 3 [仅限新 Web 界面] 单击 保存条目。

步骤 4 访问“垃圾邮件隔离区”页面。

a) 依次选择**监控 (Monitor) > 垃圾邮件隔离区 (Spam Quarantine)**。
b) 选择页面右上角的**选项**下拉菜单。
c) 依次选择**安全列表 (Safelist)**。
d) 从“安全列表”(Safelist) 对话框中，输入邮件地址或域。您可以输入多个域和邮件地址，以逗号分隔。
e) 单击**添加到列表 (Add to List)**。

将发件人添加到阻止列表（最终用户）

根据管理员定义的安全列表/阻止列表操作设置，可能会拒绝或隔离来自已列入阻止列表的发件人的邮件。

Note 只能按照以下过程添加阻止列表条目。

步骤 1 [仅限新 Web 界面] 选择**阻止列表**，单击 + 图标并输入要添加到阻止列表的域或邮件地址。您可以输入多个域和邮件地址，以逗号分隔。

步骤 2 [仅限新 Web 界面] 单击 保存条目。

步骤 3 访问“垃圾邮件隔离区”页面。

a) 依次选择**监控 (Monitor) > 垃圾邮件隔离区 (Spam Quarantine)**。
b) 从页面右上角的**选项**下拉菜单中选择**阻止列表**。
c) 输入要列入阻止列表的域或邮件地址。您可以输入多个域和邮件地址，以逗号分隔。
d) 单击**添加到列表 (Add to List)**。

备份和恢复安全列表/阻止列表

在升级设备或运行安装向导之前，应备份安全列表/阻止列表数据库。安全列表/阻止列表信息未包含在含有设备配置设置的主 XML 配置文件中。

也可以随同安全管理设备上的其他数据备份安全列表/阻止列表条目。请参阅备份安全管理设备数据。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，单击 ⚙ 加载旧 Web 界面。

步骤 2 选择**管理设备 > 系统管理 > 配置文件**。

步骤 3 滚动到**最终用户安全列表/阻止列表数据库（垃圾邮件隔离区）(End-User Safelist/Blocklist Database (Spam Quarantine))** 部分。

收件人	相应操作
导出安全列表/阻止列表	请注意 .csv 文件的路径和文件名，并根据需要进行修改。 单击**立即备份 (Backup Now)**。 设备将使用以下命名约定将 .csv 文件保存到设备的 /configuration 目录： *slbl*<序列号><时间戳>*.csv*
导入安全列表/阻止列表	**Caution** 此过程将覆盖所有用户的安全列表和阻止列表中的全部现有条目。 单击**选择要恢复的文件 (Select File to Restore)**。 从配置目录中的文件列表选择所需文件。 选择要恢复的安全列表/阻止列表备份文件。 单击**恢复 (Restore)**。

安全列表和阻止列表故障排除

要对安全列表和阻止列表的问题进行故障排除，您可以查看日志文件或系统警报。

当邮件由于安全列表/阻止列表设置而受阻时，操作会记录在ISQ_log文件或反垃圾邮件日志文件中。列入安全列表的邮件使用 *X-SLBL-Result-Safelist* 信头标记为已列入安全列表。列入阻止列表的邮件使用 *X-SLBL-Result-Blocklist* 信头标记为已列入阻止列表。

当创建或更新数据库时，或者如果在修改数据库或运行安全列表/阻止列表的过程中发生错误，则系统会发出警报。

有关警报的详细信息，请参阅管理警报。

有关日志文件的详细信息，请参阅日志记录。

相关主题

- 列入安全列表的发件人的邮件未传送 , on page 20

列入安全列表的发件人的邮件未传送

问题

列入安全列表的发件人的邮件未发送。

解决方案

可能的原因：

- 由于恶意软件或内容违规而丢弃了邮件。请参阅安全列表和阻止列表的邮件处理 , on page 11。
- 如果有多个设备，并且最近才将发件人添加至安全列表，则处理该邮件时，安全列表/阻止列表可能尚未同步。请参阅外部垃圾邮件隔离区和安全列表/阻止列表 , on page 12 。

为最终用户配置垃圾邮件管理功能

收件人	请参阅
了解适用于最终用户对垃圾邮件管理功能访问的不同身份验证方法的优势和限制。	配置最终用户访问垃圾邮件隔离区的权限 , on page 24和子节
允许最终用户直接通过浏览器访问垃圾邮件隔离区。	访问垃圾邮件管理功能的最终用户的身份验证选项 , on page 21
当发送给用户的邮件路由到垃圾邮件隔离区时，请向用户发送通知。 通知可以包含用于访问垃圾邮件隔离区的链接。	通知最终用户被隔离的邮件 , on page 26
允许用户指定其知悉为安全的发件人及其知悉发送的是垃圾邮件或其他不需要的邮件的发件人的邮件地址和域。	使用安全列表和阻止列表基于发件人控制邮件发送 , on page 10

相关主题

- 访问垃圾邮件管理功能的最终用户的身份验证选项 , on page 21
- 设置最终用户通过网络浏览器访问垃圾邮件隔离区的权限 , on page 23
- 通知最终用户被隔离的邮件 , on page 26

访问垃圾邮件管理功能的最终用户的身份验证选项

Note 邮箱身份验证不允许用户查看发到邮件别名的邮件。

对于最终用户垃圾邮件隔离区访问	相应操作
直接通过 Web 浏览器，需要身份验证 并 通过通知中的链接，需要身份验证	1. 在“最终用户隔离区访问”设置中，选择 **LDAP**、SAML 2.0 或**邮箱 (IMAP/POP)**。 2. 在“垃圾邮件通知”(Spam Notifications) 设置中，取消选择**启用登录时无需隔离区访问凭证 (Enable login without credentials for quarantine access)**。

对于最终用户垃圾邮件隔离区访问	相应操作
直接通过 Web 浏览器，需要身份验证 并 通过通知中的链接，无需身份验证	1. 在“最终用户隔离区访问”设置中，选择 **LDAP**、SAML 2.0 或**邮箱 (IMAP/POP)**。 2. 在“垃圾邮件通知”(Spam Notifications) 设置中，选择**启用登录时无需隔离区访问凭证 (Enable login without credentials for quarantine access)**。
仅通过通知中的链接，无需身份验证	在“最终用户隔离区访问 (End User Quarantine Access)”设置中，选择**无 (None)** 作为身份验证方法。
无访问权限	在“最终用户隔离区访问 (End User Quarantine Access)”设置中，取消选择**启用最终用户隔离区访问 (Enable End-User Quarantine Access)**。

相关主题

- LDAP 身份验证过程 , on page 22
- IMAP/POP 身份验证过程 , on page 23
- SAML 2.0 身份验证过程, on page 23
- 配置最终用户访问垃圾邮件隔离区的权限 , on page 24
- 通知最终用户被隔离的邮件 , on page 26
- 将 LDAP 配置为与垃圾邮件隔离区配合使用
- 关于最终用户访问安全列表和阻止列表 , on page 18

LDAP 身份验证过程

1. 用户在网络 UI 登录页输入其用户名和密码。
2. 垃圾邮件隔离区连接到指定 LDAP 服务器，执行匿名搜索或作为使用指定“服务器登录”DN 和密码通过身份验证的用户执行搜索。对于 Active Directory，您通常将需要在“全局目录端口”（包含在 6000 中）上具有服务器连接，并且需要创建一个低权限 LDAP 用户，垃圾邮件隔离区可以该用户身份进行绑定，以便执行搜索。
3. 然后，垃圾邮件隔离区使用基本 DN 和查询字符串搜索用户。找到用户的 LDAP 记录时，垃圾邮件隔离区将提取该记录的 DN，并尝试使用该用户记录的 DN 和他们最初输入的密码绑定至目录。如果此密码检查成功，则用户正确通过身份验证，但垃圾邮件隔离区仍需要确定为该用户显示哪些邮箱内容。
4. 邮件使用收件人的信封地址存储在垃圾邮件隔离区中。在用户密码通过 LDAP 验证后，垃圾邮件隔离区会从 LDAP 记录中检索“主邮件属性”，以确定他们应为之显示隔离邮件的哪个信封地址。“主邮件属性”(Primary Email Attribute) 可以包含多个邮件地址，这些邮件地址之后可用于确定应从已进行身份验证的用户的隔离区显示的信封地址。

相关主题

- 访问垃圾邮件管理功能的最终用户的身份验证选项 , on page 21
- 与 LDAP 集成

IMAP/POP 身份验证过程

1. 根据邮件服务器配置，用户向网络用户界面登录页输入其用户名 (joe) 或邮件地址 (joe@example.com) 与密码。可以修改“登录页面消息 (Login Page Message)”，以便告知用户应输入完整的邮件地址，还是仅用户名（请参阅配置最终用户访问垃圾邮件隔离区的权限 , on page 24）。
2. 垃圾邮件隔离区连接到 IMAP 或 POP 服务器，并使用输入的登录信息（用户名或邮件地址）和密码尝试登录到 IMAP/POP 服务器。如果接受密码，则用户被视为通过身份验证，而垃圾邮件隔离区会立即从 IMAP/POP 服务器注销。
3. 一旦用户通过身份验证，垃圾邮件隔离区将根据邮件地址列出该用户的邮件：
   - 如果配置了垃圾邮件隔离区来指定附加到裸用户名（例如 joe）的域，将附加此域，并使用完全限定的邮件地址在隔离区中搜索匹配的信封。
   - 否则，垃圾邮件隔离区会使用所输入的邮件地址来搜索匹配信封。

有关 IMAP 的详细信息，请参阅华盛顿大学网站：

http://www.washington.edu/imap/

SAML 2.0 身份验证过程

请参阅思科内容安全管理设备指南中的使用 *SAML 2.0* 的 *SSO* 部分

设置最终用户通过网络浏览器访问垃圾邮件隔离区的权限

步骤 1 了解最终用户访问垃圾邮件管理功能采用的不同身份验证方法的优点和局限性。

步骤 2 如果使用 LDAP 验证最终用户，请配置 LDAP 服务器配置文件，包括**系统管理 > LDAP > LDAP 服务器配置文件**页上的**垃圾邮件隔离区最终用户身份验证查询**设置。

Example:

```
If you will authenticate end users using SAML 2.0 (SSO), configure the settings on the
 System Administration > SAML page.
```

与 LDAP 集成 和小节

使用 SAML 2.0 的 SSO

步骤 3 配置最终用户访问垃圾邮件隔离区的权限。

配置最终用户访问垃圾邮件隔离区的权限 , on page 24

步骤 4 确定最终用户访问垃圾邮件隔离区的 URL。

确定最终用户访问垃圾邮件隔离区的 URL, on page 25

What to do next

相关主题

配置最终用户访问垃圾邮件隔离区的权限

无论是否启用最终用户访问权限，管理用户都可以访问垃圾邮件隔离区。

Before you begin

请参阅访问垃圾邮件管理功能的最终用户的身份验证选项 , on page 21中的要求。

步骤 1 如果您使用的旧界面，请导航至**管理设备 (Management Appliance)** > **集中服务 (Centralized Services)** > **监控 (Monitor)** > **垃圾邮件隔离区 (Spam Quarantine)** > **编辑设置 (Edit Settings)**，然后向下滚动至**最终用户隔离区访问 (End-User Quarantine Access)**。如果您使用的新 Web 界面，请导航至安全管理设备 (Security Management appliance)，单击**服务状态 (Service Status)**，将鼠标悬停在 图标上，然后单击**编辑最终用户隔离区设置 (Edit End-User Quarantine Settings)**。您会被重定向到旧接口。

步骤 2 选择**启用最终用户隔离区访问权限**。

步骤 3 指定最终用户尝试查看自己的隔离邮件时，对他们进行身份验证的方法。

选择以下选项	更多信息
无 (None)	选择此选项可以让最终用户能够通过垃圾邮件通知中的链接来访问被隔离的邮件，而无需进行额外的认证。
邮箱(IMAP/POP)	对于不使用 LDAP 目录进行身份验证的站点，隔离区可以根据保留用户邮箱的基于标准的 IMAP 或 POP 服务器来验证用户邮件地址和密码。 在登录到垃圾邮件隔离区时，最终用户输入其完整的邮件地址和邮箱密码。 如果 POP 服务器在标题中通告支持 APOP，则出于安全考虑（例如，避免以明文形式发送密码），思科设备将仅使用 APOP。如果对于部分或所有用户不支持 APOP，则应将 POP 服务器重新配置为不通告 APOP。 如果已将服务器配置为使用 SSL，请选择 SSL。如果用户仅输入用户名，则您可以指定要添加的域以自动完成邮件地址。为登录“将域附加到未限定用户名”(Append Domain to Unqualified Usernames) 的用户输入信封的域。
LDAP	配置 LDAP 设置，如本主题的“准备工作”部分中引用的部分中所述。
SAML 2.0	为垃圾邮件隔离启用单点登录。 在使用此选项之前，请确保已配置了“管理设备”>“系统管理”>“SAML”页面上的所有设置。请参阅《思科内容安全管理设备指南》中的使用 *SAML 2.0* 的 *SSO*。

步骤 4 指定在放行邮件之前是否显示邮件正文。

如果选择此框，则用户可能不会通过垃圾邮件隔离区页面查看邮件正文。相反，要查看隔离邮件的正文，用户必须放行该邮件，并在邮件应用（例如 Microsoft Outlook）中对其进行查看。您可以将此功能用于策略和合规性 - 例如，如果法规要求将所有已查看的邮件存档。

步骤 5 提交并确认更改。

What to do next

（可选）自定义用户在访问垃圾邮件隔离区时查看的页面（如果尚未进行此操作）。请参阅在旧 Web 界面上启用和配置垃圾邮件隔离区 , on page 2中的设置说明。

确定最终用户访问垃圾邮件隔离区的 URL

最终用户直接访问垃圾邮件隔离区所使用的 URL 基于计算机的主机名和启用隔离区的 IP 接口上配置的设置（HTTP/S 和端口号）。例如，`HTTP://mail3.example.com:82`。

最终用户现在可以通过以下任何一种方式访问新 Web 界面上的垃圾邮件隔离区：

- 当 `trailblazerconfig` CLI 命令启用后，请使用以下 URL - `https://example.com:<trailblazer-https-port>/ng-login /euq-login`。

  其中， `example.com`是设备主机名， `< trailblazer-https-port>` 是在设备上已配置的 trailblazer HTTPS 端口。

- 当禁用 `trailblazerconfig` CLI 命令时，请使用以下 URL - `https://example.com:<https-port>/euq-login`。

  其中， `example.com` 是设备的主机名， `<https-port>` 是设备上配置的 HTTPS 端口。

Note 本地和外部身份验证的用户无法登录到最终用户垃圾邮件隔离区门户。

最终用户查看的邮件

通常，最终用户只能在垃圾邮件隔离区中查看自己的邮件。

根据访问方法（通过通知或直接通过网络浏览器）和身份验证方法（LDAP 或 IMAP/POP），用户可以在垃圾邮件隔离区中查看多个邮件地址的邮件。

当使用 LDAP 身份验证时，如果主邮件属性在 LDAP 目录中具有多个值，则所有这些值（地址）都将与用户关联。因此，对于 LDAP 目录中的最终用户，隔离区中包含发往所有与该用户关联的邮件地址的已隔离邮件。

如果身份验证方法为 IMAP/POP，或者用户直接通过通知访问隔离区，则隔离区将仅显示该用户的邮件地址（或向其发送了通知的地址）的邮件。

有关发送到用户所属邮件地址的别名的邮件的信息，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知 , on page 28。

相关主题

- 配置最终用户访问垃圾邮件隔离区的权限 , on page 24
- 收件人电子邮件的邮件列表别名和垃圾邮件通知 , on page 28

通知最终用户被隔离的邮件

您可以将系统配置为在部分或所有用户在垃圾邮件隔离区中具有垃圾邮件和可疑垃圾邮件时向其发送通知邮件。

默认情况下，垃圾邮件通知会列出最终用户的隔离邮件。通知还可包含链接，您可以用它来查看垃圾邮件隔离区中的隔离邮件。然后，您可以决定是将隔离邮件传送到其收件箱还是将其删除。

Note 在集群配置中，您可以选择仅在机器级别接收通知的用户。

Before you begin

- 为使最终用户管理通知中所列的邮件，他们必须能够访问垃圾邮件隔离区。请参阅配置最终用户访问垃圾邮件隔离区的权限 , on page 24。
- 了解和实施用于使用通知管理垃圾邮件的身份验证选项。请参阅访问垃圾邮件管理功能的最终用户的身份验证选项 , on page 21。
- 如果最终用户以多个别名接收邮件，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知 , on page 28。

步骤 1 如果您使用的是旧界面，请导航至**管理设备 (Management Appliance)** > **集中服务 (Centralized Services)** > **垃圾邮件隔离区 (Spam Quarantine)** > **编辑设置 (Edit Settings)**，然后向下滚动至**垃圾邮件通知 (Spam Notifications)**。但是，如果您使用的新 Web 界面，请导航至安全管理设备 (Security Management appliance)，单击**服务状态 (Service Status)**，将鼠标悬停在 图标上，然后单击**编辑垃圾邮件通知设置 (Edit Spam Notification Settings)**。您会被重定向到旧接口。

步骤 2 选择**启用垃圾邮件通知 (Enable Spam Notification)**。

步骤 3 输入通知的“发件人：”(From:) 地址。

步骤 4 指定要通知的最终用户。

步骤 5 （可选）自定义通知的主题。

步骤 6 （可选）自定义通知的标题。

步骤 7 选择通知的默认语言。

步骤 8 配置最终用户的隔离区访问权限。

a) 要在用户通过单击通知中的链接来访问垃圾邮件隔离区时使其自动登录，请选中**无凭证登录 (Login without credentials)** 复选框。最终用户通过单击通知中的**放行 (Release)** 链接即可放行邮件。如果取消选中该选线，最终用户就无法通过单击通知中的**放行 (Release)** 链接来放行邮件。

只有当您选择以下最终用户身份验证方法之一时才会出现此选项：邮箱 (IMAP/POP)、LDAP 或 SAML 2.0。如果您选择“无”(None) 作为身份验证方法，则当最终用户单击垃圾邮件通知中的链接时，他们就会自动登录到垃圾邮件隔离区。

b) 为通知中的链接设置到期期限（以天为单位）。输入一个介于 0 和 365 之间的数字。这些链接将在指定期限后自动过期。如果不希望链接过期，则输入 0。

（对于邮箱 (IMAP/POP)、LDAP 和 SAML 2.0）只有选中**无凭证登录 (Login without credentials)** 复选框时才能配置此选项。

您还可以在 CLI 中使用 **spamdigestconfig** 命令设置到期期限。

步骤 9 自定义邮件正文：

a) （可选）自定义默认文本和变量。

要插入变量，请将光标置于要插入变量的位置，然后单击右侧“邮件变量”(Message Variables) 列表中的变量的名称。或者，键入变量。

以下邮件变量将扩展为特定最终用户的实际值：

- **新邮件数** (%new_message_count%) — 自用户上次登录后的新邮件数。
- **总邮件数** (%total_message_count%) — 用户在垃圾邮件隔离区的邮件数。
- **邮件过期前的天数** (%days_until_expire%)
- **隔离区 URL** (%quarantine_url%) — 用于登录到隔离区和查看邮件的 URL。
- **用户名** (%username%)
- **新邮件表** (%new_quarantine_messages%) — 用户的新隔离邮件的列表，显示发件人、邮件主题、日期和放行邮件的链接。用户单击邮件主题可查看垃圾邮件隔离区中的邮件。
- **不带主题的新邮件表** (%new_quarantine_messages_no_subject%) - 与新邮件表类似，但仅在每封邮件的主题位置显示“查看邮件”链接。

b) 选择是显示还是隐藏链接，以查看垃圾邮件通知中的所有隔离邮件。在**显示链接以查看通知邮件中的所有隔离邮件**下，根据需要选择**是 (Yes)** 或**否 (No)**。

（对于邮箱 (IMAP/POP)、LDAP 和 SAML 2.0）。仅当选中**无凭证登录 (Login without credentials)** 复选框（在“隔离区访问”(Quarantine Access) 下）时才会出现此选项。

如果选择**是 (Yes)**，您可以在访问垃圾邮件隔离区之前强制最终用户进行身份验证。选中**质询访问 (Challenge Access)**。如果您选择“无”(None) 作为最终用户身份验证方法，则此选项不可用。

您还可以在 CLI 中使用 **spamdigestconfig** 命令来显示或隐藏链接。

c) 单击**预览邮件 (Preview Message)** 可确认邮件是否符合预期。

步骤 10 选择邮件格式（HTML、文本或 HTML/文本）。

步骤 11 指定退回的通知将发送到的地址。

步骤 12 （可选）选择**整合发送到不同地址的同一 LDAP 用户的邮件 (Consolidate messages sent to the same LDAP user at different addresses)**。

步骤 13 设置通知发送间隔。

步骤 14 提交并确认更改。

What to do next

要确保最终用户接收这些通知，请考虑建议他们将垃圾邮件隔离区通知邮件的“发件人：”(From:)地址添加到其邮件应用（例如 Microsoft Outlook 或 Mozilla Thunderbird）的垃圾邮件设置中的“允许列表”。

相关主题

- 收件人电子邮件的邮件列表别名和垃圾邮件通知 , on page 28
- 测试通知, on page 29
- 垃圾邮件通知故障排除 , on page 29

收件人电子邮件的邮件列表别名和垃圾邮件通知

通知可以发送给拥有隔离邮件的各个信封收件人，包括邮件列表和其他别名。每个邮件列表都会收到一个摘要。如果您将通知发送到邮件列表，则该列表中的所有用户都将收到通知。属于多个邮件别名的用户、属于收到通知的 LDAP 组的用户或使用多个邮件地址的用户，都可能收到多个垃圾邮件通知。下表显示用户可能会收到多个通知的情况示例。

Table 1: 每个地址/别名的通知数

用户	电子邮件地址	别名	通知
Sam	sam@example.com	-	1
Mary	mary@example.com	dev@example.com qa@example.com pm@example.com	4
Joe	joe@example.com、admin@example.com	hr@example.com	3

如果您使用 LDAP 身份验证，则可以选择不将通知发送到邮件列表别名。或者，如果选择向邮件列表别名发送垃圾邮件通知，可以防止有时出现的多个通知。。

除非设备对邮件通知使用的是垃圾邮件隔离区别名整合，否则通过单击通知中的链接来访问垃圾邮件隔离区的用户将看不到最终用户可能具有的任何其他别名的隔离邮件。如果通知发送到在由设备处理后扩展的分发列表，则多个收件人可能有权访问该列表的同一隔离区。

这意味着邮件列表的所有用户都将收到通知，并且可以登录隔离区以放行或删除邮件。在此情况下，访问隔离区以查看通知中提到的邮件的最终用户可能会发现这些邮件已被其他用户删除。

Note 如果不使用 LDAP，并且不希望最终用户接收多个邮件通知，请考虑禁用通知，并改为允许最终用户直接访问隔离区并通过 LDAP 或 POP/IMAP 进行身份验证。

测试通知

可以通过以下方法测试通知：配置测试邮件策略，并仅针对一位用户隔离垃圾邮件。然后，配置垃圾邮件隔离区通知设置：选择**启用垃圾邮件通知 (Enable Spam Notification)** 复选框，并且不选择**启用最终用户隔离区访问权限 (Enable End-User Quarantine Access)**。然后，只有**将退回的邮件传送到 (Deliver Bounced Messages To)** 字段中配置的管理员会收到有关隔离区中有新垃圾邮件的通知。

垃圾邮件通知故障排除

相关主题

- 用户收到多个通知 , on page 29
- 收件人未收到通知 , on page 29
- 用户收到多个通知 , on page 29
- 收件人未收到通知 , on page 29

用户收到多个通知

问题

用户针对一封邮件收到多个垃圾邮件通知。

解决方案

可能的原因：

- 用户具有多个邮件地址，并且垃圾邮件发送到其中多个地址。
- 用户是收到垃圾邮件的一个或多个邮件别名的成员。要尽量减少重复并了解详细信息，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知 , on page 28。

收件人未收到通知

问题

收件人未收到垃圾邮件通知。

解决方案

- 如果通知是发送到“将退回邮件传送到：”(Deliver Bounce Messages To:) 地址而不是垃圾邮件收件人，这意味着已启用垃圾邮件通知，但是未启用垃圾邮件隔离区访问权限。请参阅访问垃圾邮件管理功能的最终用户的身份验证选项 , on page 21。
- 让用户检查其邮件客户端的垃圾邮件设置。
- 检查在在旧 Web 界面上启用和配置垃圾邮件隔离区 , on page 2中为**邮件传送方式 (Deliver Messages Via)** 指定的设备或服务器的问题。

管理垃圾邮件隔离区的邮件

本部分介绍如何处理本地或外部垃圾邮件隔离区中的邮件。

管理用户可以查看和管理垃圾邮件隔离区中的所有邮件。

相关主题

- 访问垃圾邮件隔离区（管理用户）, on page 30
- 在垃圾邮件隔离区中搜索邮件, on page 30
- 查看垃圾邮件隔离区中的邮件, on page 31
- 发送垃圾邮件隔离区中的邮件, on page 31
- 删除垃圾邮件隔离区中的邮件, on page 32

访问垃圾邮件隔离区（管理用户）

管理用户可以查看和管理垃圾邮件隔离区的所有邮件。

访问垃圾邮件隔离区（管理用户）

管理用户可以查看和管理垃圾邮件隔离区的所有邮件。

步骤 1 [仅限新 Web 界面] 在安全管理设备上，依次选择**隔离区** > **垃圾邮件隔离区** > **搜索**。

步骤 2 依次选择**邮件 (Email)** > **邮件隔离区 (Message Quarantine)** > **垃圾邮件隔离区 (Spam Quarantine)**，然后单击**垃圾邮件隔离区 (Spam Quarantine)** 链接。

垃圾邮件隔离区将在单独的浏览器窗口中打开。

在垃圾邮件隔离区中搜索邮件

步骤 1 指定信封收件人。

Note 您可以输入不完整地址。

步骤 2 选择搜索结果是否应与所输入的确切收件人相匹配，或者结果是应包含条目、以其开头还是以其结尾。

步骤 3 输入要搜索的日期范围。单击日历图标以选择日期。

步骤 4 指定“发件人：”(From:)地址，然后选择搜索结果是应包含所输入的值、与其完全匹配、以其开头还是以其结尾。

步骤 5 单击**搜索 (Search)**。与搜索条件相匹配的邮件显示在页面的“搜索”(Search) 部分下方。

What to do next

相关主题

搜索超大邮件集合, on page 31

搜索超大邮件集合

如果您在垃圾邮件隔离区中具有超大邮件集合，并且如果您的搜索词未进行狭义定义，则查询可能需要很长时间才会返回信息，也可能会超时。

系统将提示您确认是否要重新提交搜索。请注意，同时运行多个大型搜索可能会影响性能。

查看垃圾邮件隔离区中的邮件

邮件列表显示垃圾邮件隔离区中的邮件。您可以选择一次显示的邮件数量。您可以通过单击列标题对显示进行排序。再次单击同一列可反向排序。

单击邮件的主题可查看该邮件，包括正文和标题。邮件显示在“邮件详细信息”(Message Details) 页面中。系统会显示邮件的前 20K。如果邮件较长，则会将其截断为 20K，并且可以通过邮件底部的链接来下载邮件。

在“邮件详细信息”页面，可以删除邮件（选择**删除**）或选择**释放**以释放邮件。释放邮件可发送该邮件。

要查看有关邮件的其他详细信息，请单击**邮件跟踪 (Message Tracking)** 链接。

请注意以下提示：

- **查看带附件的邮件 (Viewing Messages with Attachments)**

  当查看包含附件的邮件时，系统会显示邮件的正文，后跟附件列表。

  在新 Web 界面中，如果邮件包含附件，您可以在邮件的“附件”部分查看附件的详细信息。

- **查看 HTML 邮件 (Viewing HTML Messages)**

  垃圾邮件隔离区尝试呈现相近的基于 HTML 的邮件。未显示图像。

- **查看编码邮件 (Viewing Encoded Messages)**

  Base64 编码的邮件将先解码，然后显示。

发送垃圾邮件隔离区中的邮件

如果要放行邮件以进行发送，请单击要释放的一封或多封邮件旁边的复选框，再从下拉菜单中选择**放行 (Release)**。然后单击**提交 (Submit)**。

单击标题行中的复选框可自动选择页面上当前显示的所有邮件。

放行的邮件会直接转到目标队列，跳过邮件管道中的任何其他工作队列处理。

删除垃圾邮件隔离区中的邮件

可以将垃圾邮件隔离区配置为：经过一段时间后自动删除邮件。此外，垃圾邮件隔离区还可配置为在隔离区达到其最大大小后就自动删除最旧的邮件。也可以手动删除垃圾邮件隔离区中的邮件。

要删除特定邮件，请单击要删除的邮件旁边的复选框，然后从下拉菜单中选择**删除 (Delete)**。然后单击**提交 (Submit)**。单击标题行中的复选框可自动选择页面上当前显示的所有邮件。

要删除垃圾邮件隔离区中的所有邮件，请禁用隔离区（参阅关于禁用外部垃圾邮件隔离区 , on page 32），然后单击**删除所有邮件 (Delete All Messages)** 链接。链接尾部的括号中的数字是指垃圾邮件隔离区中的邮件数。

垃圾邮件隔离区的磁盘空间

隔离区的可用磁盘空间根据设备型号而异。请参阅查看磁盘空间配额和使用情况。

默认情况下，在经过设置的时间后，系统将自动删除垃圾邮件隔离区中的邮件。如果隔离区已满，则会删除较旧的垃圾邮件。要更改此设置，请参阅在旧 Web 界面上启用和配置垃圾邮件隔离区 , on page 2。

相关主题

关于禁用外部垃圾邮件隔离区

如果禁用垃圾邮件隔离区：

- 如果被禁用的垃圾邮件隔离区中存在邮件，可以选择删除所有邮件。
- 为隔离垃圾邮件设置的所有邮件策略将改为发送邮件。可能需要调整邮件安全设备上的邮件策略。
- 要完全禁用外部垃圾邮件隔离区，请在设备和安全管理设备上都禁用外部垃圾邮件隔离区。

只禁用设备上的外部垃圾邮件隔离区不会删除外部隔离区或其邮件与数据。

垃圾邮件隔离区功能故障排除

- 安全列表和阻止列表故障排除, on page 20
- 垃圾邮件通知故障排除 , on page 29