策略、病毒和病毒爆发隔离区

本章包含以下部分：

策略、病毒和病毒爆发隔离区概述

“策略、病毒和病毒爆发隔离区”包含所有非垃圾邮件隔离区，其中包括文件分析隔离区。

当邮件网关在传入或传出邮件中检测到潜在恶意软件或组织不允许的内容时，可以将这些邮件发送到隔离区，而不是立即将其删除。隔离区会在邮件网关或思科安全邮件和 Web 管理器上安全保留这些邮件一段时间，以便人们审核邮件或者等待更新来更好地评估邮件的安全性。

如何可在贵组织中使用非垃圾邮件隔离区的示例：

- **策略执行**。让人力资源人员或法律部门审核可能包含攻击性、机密性或其他禁用信息的邮件。
- **病毒隔离区**。存储标记为被感染、已加密或无法由防病毒扫描引擎扫描的邮件，以防止病毒传播给您的用户。
- **病毒爆发预防**。保留由爆发过滤器标记为可能属于病毒爆发或小规模恶意软件攻击的一部分的邮件，直到发布防病毒或反垃圾邮件更新。
- **文件分析隔离区**。存储具有可能包含恶意软件的附件并已发送进行分析的邮件，直到作出判定。

相关主题

- 垃圾邮件隔离区

隔离区类型

隔离区类型	隔离区名称	默认情况下由系统创建？	说明	更多信息
高级恶意软件防护	文件分析	是	保留已发送进行文件分析的邮件，直到返回判定。	• 管理策略、病毒 • 处理策略、病毒件
病毒	病毒	是	保留可能正在传输恶意软件（由防病毒引擎确定）的邮件。	
爆发	爆发	是	保留可能作为垃圾邮件或恶意软件由爆发过滤器捕获到的邮件。	
策略	策略	是	暂存邮件过滤器、内容过滤器和 DLP 邮件操作拦截的邮件。 系统已为您创建了默认策略隔离区。	
	未分类	是	仅在删除邮件过滤器、内容过滤器或 DLP 邮件操作中指定的隔离区后才保留邮件。 您不能将此隔离区分配到任何过滤器或邮件操作。	
	（您创建的策略隔离区）	否	您创建的供在邮件过滤器、内容过滤器和 DLP 邮件操作中使用的策略隔离区。	
垃圾邮件	垃圾邮件	是	保留垃圾邮件或可疑垃圾邮件，以供邮件收件人或管理员审核。 垃圾邮件隔离区未包含在策略、病毒和病毒爆发隔离区组中，并且与所有其他隔离区分开管理。	垃圾邮件隔离区

管理策略、病毒和病毒爆发隔离区

- 关于删除策略隔离区 , on page 7
- 监控隔离区状态、容量和活动 , on page 8
- 策略隔离区性能 , on page 9
- 关于隔离区磁盘空间使用量的警报 , on page 9
- 策略隔离区和日志记录, on page 9
- 关于向其他用户分配邮件处理任务 , on page 10
- 关于集群配置中的策略、病毒和病毒爆发隔离区 , on page 11
- 关于集中策略、病毒和病毒爆发隔离区 , on page 11

策略、病毒和爆发隔离区的磁盘空间分配

有关策略、病毒和病毒爆发隔离区的磁盘空间信息，请参阅管理磁盘空间。

即使隔离区已集中，策略、病毒和爆发隔离区仍会占用邮件网关中的部分磁盘空间。

多个隔离区中的邮件与单一隔离区中的邮件占用相同的磁盘空间。

如果爆发过滤器和集中隔离区都启用：

- 使用邮件网关中本已分配给本地策略、病毒和爆发隔离区的所有磁盘空间（而不是在爆发隔离区暂存邮件副本），以便在爆发规则每次更新时扫描这些邮件。
- 思科安全邮件和 Web 管理器上用于特定受管

相关主题

- 监控隔离区状态、容量和活动 , on page 8
- 关于隔离区磁盘空间使用量的警报 , on page 9
- 邮件在隔离区中的保留时间 , on page 3

邮件在隔离区中的保留时间

在以下情况下，将自动从隔离区中删除邮件：

- 正常到期 - 隔离区中的邮件达到配置的保留时间。为各隔离区中的邮件指定保留时间。每封邮件具有各自的特定到期时间，显示在隔离区列表中。除非出现本主题中描述的其他情况，否则邮件存储时间为指定时间。

Note 爆发过滤器隔离区中邮件的正常保留时间在每个邮件策略的“爆发过滤器”(Outbreak Filters) 部分配置，而不是爆发隔离区。

- 提前到期 - 在到达配置的保留时间之前，强制从隔离区中删除邮件。在以下条件下可能发生这种情况：
  - 达到策略、病毒和爆发隔离区的磁盘空间分配 , on page 3中定义的所有隔离区的大小限制。

如果达到大小限制，则系统会处理最旧的邮件（无论隔离区如何）并对每封邮件执行默认操作，直到所有隔离区的大小再次小于大小限制。采用的策略是先进先出 (FIFO)。多个隔离区中的邮件将根据其最新到期时间到期。

（可选）您可以将个别隔离区配置为豁免由于磁盘空间不足而放行或删除。如果将所有隔离区都配置为免除，当磁盘空间达到容量时，将传送隔离区中的邮件以便为新邮件腾出空间。

在磁盘空间达到里程碑时，您将会收到警报。请参阅关于隔离区磁盘空间使用量的警报 , on page 9。

- 您可删除仍然保留邮件的隔离区。

从隔离区中自动删除邮件后，系统将对该邮件执行默认操作。请参阅自动处理的隔离邮件的默认操作 , on page 4。

Note 除上述场景之外，也可以根据扫描操作（爆发过滤器或文件分析）的结果从隔离区自动删除邮件。

保留时间中时间调整的影响

- 夏令时和邮件网关时区更改不影响保留期。
- 如果您更改隔离区的保留时间，则只有新邮件将具有新的到期时间。
- 如果更改系统时钟，则过去应已过期的邮件将在下一个最适当时间到期。
- 系统时钟更改不适用于处于即将到期过程中的邮件。

自动处理的隔离邮件的默认操作

当发生邮件在隔离区中的保留时间 , on page 3中所述的任何情况时，将对策略、病毒或病毒爆发隔离区中的邮件执行默认操作。

有两个主要默认操作：

- 删除-删除邮件。
- 放行-放行邮件进行传送。

在放行时，系统可能会重新扫描邮件以查找威胁。有关详细信息，请参阅关于重新扫描隔离的邮件 , on page 17。

此外，在经过其预期保留时间之前放行的邮件可以对其执行其他操作，例如添加 X 信头。有关详细信息，请参阅 配置策略、病毒和爆发隔离区 , on page 5。

检查系统创建的隔离区的设置

在您使用隔离区之前，请自定义默认隔离区的设置，包括未分类隔离区。

相关主题

- 配置策略、病毒和爆发隔离区 , on page 5

配置策略、病毒和爆发隔离区

Before you begin

- 如果您编辑的是现有隔离区，请参阅关于编辑策略、病毒和爆发隔离区设置 , on page 7。
- 了解如何自动管理隔离区中的邮件，包括保留时间和默认操作。请参阅邮件在隔离区中的保留时间 , on page 3和自动处理的隔离邮件的默认操作 , on page 4。
- 确定希望哪些用户对每个隔离区具有访问权，并相应地创建用户和自定义用户角色。有关详细信息，请参阅可访问策略、病毒和爆发隔离区的用户组 , on page 10。

Procedure

步骤 1 您可以通过以下任一方式配置策略、病毒和病毒爆发隔离区：

- [仅限新的 Web 界面] 选择**隔离区 (Quarantine)** > **其他隔离区 (Other Quarantine)** > **查看 (View)** > **+**。
- 选择**监控 (Monitoring)** > **策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)** 并执行以下操作之一：
  - 点击**添加策略隔离区 (Add Policy Quarantine)**。
  - 点击要编辑的隔离区。

步骤 2 输入以下信息：

请注意以下事项：

- 建议不要更改文件分析隔离区的默认保留时间（1 小时）。
- 如果您不希望在指定的保留期结束之前处理此隔离区中的邮件，即使隔离区磁盘空间已满也如此，请取消选择**通过在空间溢出后对邮件应用默认操作来释放空间 (Free up space by applying default action on messages upon space overflow)**。

  对于所有隔离区，请勿选择此选项。系统必须能够通过从至少一个隔离区中删除邮件来腾出空间。
- 如果选择**放行 (Release)** 作为默认操作，则可以指定要应用于在经过其保留期之前放行的邮件的其他操作：

选项	信息
修改主题 (Modify Subject)	键入文本，以添加和指定是否将其添加到原始邮件主题的开头或结尾。 例如，您可能希望警告收件人邮件可能包含不适当的内容。 **Note** 要正常显示使用非 ASCII 字符的主题，必须根据 RFC 2047 进行表示。
添加 X 报头 (Add X-Header)	X报头可提供对邮件采取的操作的记录。这可能会非常有用，例如在处理有关传送特定邮件的原因的查询时。 输入名称和值。 示例： 名称 = Inappropriate-release-early 值 = True
拆离附件 (Strip Attachments)	拆离附件可防范这些文件当中存在病毒。

步骤 3 指定可以访问此隔离区的用户：

用户	信息
本地用户 (Local Users)	本地用户列表仅包含具有可以访问隔离区的角色的用户。 该列表不包括具有管理员权限的用户，因为所有管理员都对隔离区具有完全访问权限。
以外部方式进行身份验证的用户 (Externally Authenticated Users)	您必须已配置外部身份验证。
自定义用户角色 (Custom User Roles)	仅当您已创建至少一个具有隔离区访问权限的自定义用户角色时，才会看到此选项。

步骤 4 提交并确认更改。

What to do next

创建将邮件移到隔离区的邮件与内容过滤器及 DLP 邮件操作。

关于编辑策略、病毒和爆发隔离区设置

Note

- 您无法重命名隔离区。
- 另请参阅邮件在隔离区中的保留时间 , on page 3。

要更改隔离区设置，请依次选择 **监控 (Monitor) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**，然后点击隔离区的名称。

要更改新 Web 界面上的隔离区设置，请导航至**隔离区 (Quarantine) > 其他隔离区 (Other Quarantine) > 视图 (View)**，然后在所需的隔离区上点击 或

确定策略隔离区分配到的过滤器和邮件操作

您可以查看邮件过滤器、内容过滤器、防数据丢失 (DLP) 邮件操作、与策略隔离区相关的 DMARC 验证配置文件。

Procedure

步骤 1 [仅限新 Web 界面] 在邮件管理邮件网关上，点击**隔离区 (Quarantine) > 其他隔离区 (Other Quarantine) > 视图 (View)**。

步骤 2 [仅限新 Web 界面] 选择所需的隔离区，然后点击 按钮。

步骤 3 依次选择**监控 (Monitoring) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 4 点击要检查的策略隔离区的名称。

步骤 5 滚动到页面底部，查看**关联邮件过滤器 (Associated Message Filters)**/**内容过滤器 (Content Filters)**/**DLP 邮件操作 (DLP Message Actions)**。

关于删除策略隔离区

- 删除策略隔离区之前，请查看它是否与任何有效过滤器或邮件操作相关。请参阅确定策略隔离区分配到的过滤器和邮件操作 , on page 7。
- 您可以删除策略隔离区，即使其已分配给过滤器或邮件操作也如此。
- 如果删除的隔离区不为空，则对所有邮件应用隔离区中定义的默认操作，即使已选择磁盘满时不删除邮件的选项亦不例外。请参阅自动处理的隔离邮件的默认操作 , on page 4。
- 在删除与过滤器或邮件操作关联的隔离区后，该过滤器或邮件操作后续隔离的所有邮件都将发送到未分类隔离区。在删除隔离区之前，应自定义未分类隔离区的默认设置。
- 您不能删除未分类隔离区。

监控隔离区状态、容量和活动

要查看	相应操作
为所有非垃圾邮件隔离区分配的总空间	[仅限新 Web 界面] 在邮件网关中，点击 ⚙ 加载旧 Web 界面。 依次选择**监控 (Monitor) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**，并查看页面中的第一部分。 要更改分配，请参阅管理磁盘空间。
所有非垃圾邮件隔离区的当前可用空间	[仅限新 Web 界面] 依次选择**隔离区 (Quarnatine) > 其他隔离区 (Other Quarantine)**。 选择监控 (Monitoring) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)，并查看下方的表格。
所有隔离区当前使用的总空间	[仅限新 Web 界面] 在邮件网关中，点击 ⚙ 加载旧 Web 界面。 依次选择**监控 (Monitoring) > 系统状态 (System Status)**，然后查找**隔离区使用的队列空间 (Queue Space Used by Quarantine)**。
每个隔离区当前使用的空间	[仅限新 Web 界面] 依次选择**跟离区 (Quarantines Quarantine) > 其他隔离区 (Other Quarantine) > 查看 (View)**。 选择**监控 (Monitoring) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**，点击隔离区名称，并直接在隔离区名称下的表格行中查找此信息。
所有隔离区当前的总邮件数	[仅限新 Web 界面] 在邮件网关中，点击 ⚙ 加载旧 Web 界面。 依次选择**监控 (Monitoring) > 系统状态 (System Status)**，然后查找**隔离区中的有效邮件 (Active Messages in Quarantine)**。
每个隔离区当前的邮件数	[仅限新 Web 界面] 依次选择**跟离区 (Quarantines Quarantine) > 其他隔离区 (Other Quarantine) > 查看 (View)**。 选择**监控 (Monitoring) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**，并查看隔离区的表格行。

要查看	相应操作
所有隔离区的总 CPU 使用量	[仅限新 Web 界面] 在邮件网关中，点击 ⚙ 加载旧 Web 界面。 依次选择**监控 (Monitoring) > 系统状态 (System Status)**，然后查看 **CPU 利用率 (CPU Utilization)** 部分。
邮件最后进入每个隔离区的日期和时间（策略隔离区之间的移动除外）	[仅限新 Web 界面] 选择**隔离区 (Quarantines) > 其他隔离区 (Other Quarantine) > 视图 (View)**。 选择**监控 (Monitoring) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**，并查看隔离区的表格行。
策略隔离区的创建日期 策略隔离区创建者姓名	[仅限新 Web 界面] 在邮件网关中，点击 ⚙ 加载旧 Web 界面。 选择**监控 (Monitoring) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**，点击隔离区名称，并直接在隔离区名称下的表格行中查找此信息。 对于系统创建的隔离区，创建日期和创建者名称不可用。
与策略隔离区关联的过滤器和邮件操作	请参阅确定策略隔离区分配到的过滤器和邮件操作 , on page 7。

策略隔离区性能

除硬盘驱动器空间外，存储在策略隔离区中的邮件也使用系统内存。在单个邮件网关上将成千上万封邮件存储在策略隔离区中可能会由于内存使用过度而导致邮件网关的性能降低。邮件网关需要更多时间来隔离、删除和放行邮件，导致邮件处理速度减缓和邮件管道备份。

思科建议策略隔离区中存储的邮件平均少于 20,000 封，以确保邮件网关按正常速度处理邮件。

要查看隔离区的邮件数，请参阅监控隔离区状态、容量和活动 , on page 8。

关于隔离区磁盘空间使用量的警报

当策略、病毒和爆发隔离区的容量达到或超过 75%、85% 和 95% 时，系统将发送警报。将邮件放到隔离区时，系统会进行检查。例如，如果添加邮件会使隔离区使用量达到或超过总容量的 75%，则系统会发送警报。

策略隔离区和日志记录

AsyncOS 会逐条记录隔离的所有邮件：

Info: MID 482 quarantined to "Policy" (message filter:policy_violation)

导致邮件被隔离的邮件过滤器或爆发过滤器功能规则使用括号括起。系统会为其中放置了邮件的每个隔离区生成单独的日志条目。

AsyncOS 还会逐条记录从隔离区中删除的邮件：

Info: MID 483 released from quarantine "Policy" (queue full)

Info: MID 484 deleted from quarantine "Anti-Virus" (expired)

在从所有隔离区中删除邮件并且将其永久删除或计划进行传送后，系统会逐条记录邮件，例如

Info: MID 483 released from all quarantines

Info: MID 484 deleted from all quarantines

重新注入邮件后，系统会使用新邮件 ID (MID) 创建新邮件对象。这是使用具有新 MID“byline”的现有日志消息进行记录，例如：

Info: MID 483 rewritten to 513 by Policy Quarantine

关于向其他用户分配邮件处理任务

可以向其他管理用户分配邮件审查和处理任务。例如：

- 人力资源团队可以审核并管理策略隔离区。
- 法律团队可以管理机密资料隔离区。

在指定隔离区的设置时，请向这些用户分配访问权限。为向隔离区中添加用户，用户必须已存在。

每个用户可对所有、部分隔离区具有访问权限，或者不对任何隔离区具有访问权限。无权查看隔离区的用户将不会在隔离区的 GUI 或 CLI 列表中的任何位置看到表明其存在的指示。

相关主题

- 可访问策略、病毒和爆发隔离区的用户组 , on page 10
- 分配管理任务

可访问策略、病毒和爆发隔离区的用户组

允许管理用户访问隔离区时，他们可执行的操作取决于其用户组：

- 管理员组中的用户可以创建、配置、删除和集中隔离区，并可管理隔离邮件。
- 操作员、访客、只读操作员和服务中心用户组中的用户以及具有隔离区管理权限的自定义用户角色可以在隔离区中搜索、查看和处理邮件，但无法更改隔离区的设置，创建、删除或集中隔离区。您在每个隔离区中指定其中哪些用户有权访问该隔离区。
- 技术人员组中的用户无法访问隔离区。

相关功能（例如邮件跟踪和防数据丢失）的访问权限还会影响管理用户在隔离区页面上看到的选项和信息。例如，如果用户无权访问邮件跟踪，则该用户看不到邮件跟踪链接和被隔离邮件的信息。

最终用户无权查看或访问策略、病毒和病毒爆发隔离区。

关于集群配置中的策略、病毒和病毒爆发隔离区

部署时，只能在计算机级别利用集中管理功能配置策略、病毒和爆发隔离区。

关于集中策略、病毒和病毒爆发隔离区

可以在思科安全邮件和Web管理器上集中策略、病毒和病毒爆发隔离区。有关详细信息，请参阅集中策略、病毒和病毒爆发隔离区。

处理策略、病毒或爆发隔离区中的邮件

相关主题

- 查看隔离区中的邮件 , on page 11
- 查找策略、病毒和病毒爆发隔离区中的邮件 , on page 12
- 手动处理隔离区中的邮件, on page 13
- 多个隔离区中的邮件 , on page 14
- 邮件详细信息和查看邮件内容, on page 15
- 关于重新扫描隔离的邮件 , on page 17
- 病毒爆发隔离区, on page 17

查看隔离区中的邮件

要想	相应操作
查看隔离区中的所有邮件	[仅限新 Web 界面] 选择**隔离区 (Quarantine)** > **其他隔离区 (Other Quarantine)** > **视图 (View)**。 选择**监控 (Monitor)** > **策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。 在相关隔离区的行中，点击表格**邮件 (Messages)** 列的蓝色编号。
查看爆发隔离区中的邮件	[新 Web 界面] 选择**隔离区 (Quarantine)** > **其他隔离区 (Other Quarantine)** > **视图 (View)**。 选择**监控 (Monitor)** > **策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。 在相关隔离区的行中，点击表格**邮件 (Messages)** 列的蓝色编号。 请参阅“按规则摘要管理”链接, on page 18。
浏览隔离区中的邮件列表	点击“上一页”(Previous)、“下一页”(Next)、页码或双箭头链接。双箭头会将您引至列表中的第一页 (<<) 或最后一页 (>>)。

要想	相应操作
排序隔离区的邮件列表	点击列标题（可能包含多个项目的列或“在其他隔离区中”的列除外）。
调整表列大小。	拖动列标题之间的分隔线。
查看导致邮件隔离的内容。	请参阅查看匹配的内容 , on page 15。

相关主题

- 隔离的邮件和国际字符集, on page 12

隔离的邮件和国际字符集

如果邮件的主题中包含国际字符集的字符（双字节、可变长度和非 ASCII 编码），则“策略隔离区”(Policy Quarantine) 页面将以非 ASCII 字符的解码形式显示主题行。

查找策略、病毒和病毒爆发隔离区中的邮件

Note

- 用户只能查找和查看其有权访问的隔离区的邮件。
- 策略、病毒和爆发隔离区中的搜索找不到垃圾邮件隔离区中的邮件。

Procedure

步骤 1 [仅限新 Web 界面] 点击相应隔离区的蓝色数字链接。

Tip [仅限新 Web 界面] 对于病毒爆发隔离区，还可以查找每个病毒爆发规则隔离的所有邮件：点击“病毒爆发隔离区”(Outbreak quarantine) 中的**规则摘要 (Rule Summary)**，然后点击相关规则。

步骤 2 [仅限新 Web 界面] 选择**隔离区 (Quarantine)** > **其他隔离区 (Other Quarantine)** > **搜索 (Search)**。

步骤 3 [仅限新 Web 界面] 点击相应隔离区的蓝色数字链接。

Tip [仅限新 Web 界面] 对于病毒爆发隔离区，还可以查找每个病毒爆发规则隔离的所有邮件：点击“病毒爆发隔离区”(Outbreak quarantine) 中的**规则摘要 (Rule Summary)**，然后点击相关规则。

步骤 4 选择**监控 (Monitoring)** > **策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)** 。

步骤 5 点击**跨隔离区搜索 (Search Across Quarantines)** 按钮。

Tip 对于病毒爆发隔离区，您还可以查找按各病毒爆发规则隔离的所有邮件。点击“病毒爆发”(Outbreak) 表行中的**按规则摘要管理 (Manage by Rule Summary)** 链接，然后点击相关规则。

步骤 6 （可选）输入其他搜索条件。

- 对于信封发件人和信封收件人：您可以输入任何字符。不会针对输入执行验证。
- 搜索结果仅包含与指定的所有条件匹配的邮件。例如，如果指定信封收件人和主题，则系统只会返回与信封收件人和主题中均指定的条件匹配的邮件。

What to do next

您可以通过与使用隔离区列表相同的方式使用搜索结果。有关详细信息，请参阅手动处理隔离区中的邮件, on page 13。

手动处理隔离区中的邮件

手动处理邮件意味着，从“邮件操作”(Message Actions) 页面手动选择适用于邮件的邮件操作。

可以针对邮件执行以下操作：

- 删除
- 放行
- 延迟从隔离区计划退出
- 将邮件副本发送到您指定的邮件地址
- 在不同隔离区之间移动邮件

通常，您可以对执行以下操作时显示的列表中的邮件执行操作。但是，并非所有操作在所有情况下都可用。

- 从**监控 (Monitor) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**或 [仅限新 Web 界面] **隔离区 (Quarantine) > 其他隔离区 (Other Quarantine) > 视图 (View)** 页面上的隔离区列表中，点击隔离区中的邮件数。
- 点击**搜索整个隔离区 (Search Across Quarantines)**。
- 点击隔离区名称并在隔离区内搜索。

您可以通过以下方式一次对多封邮件执行这些操作：

- 从邮件列表顶部的选取列表中选择选项。
- 选中页面上列出的每封邮件旁边的复选框。

- 选中邮件列表顶部的表标题中的复选框。这会将操作应用于屏幕上可见的所有邮件。其他页面上的邮件不受影响。

对于爆发隔离区中的邮件，还可以使用其他选项。请参阅《适用于邮件安全设备的 *AsyncOS*》的在线帮助或用户指南中有关爆发过滤器的章节中的

相关主题

- 发送邮件副本, on page 14
- 关于在策略隔离区之间移动邮件 , on page 14
- 多个隔离区中的邮件 , on page 14
- 自动处理的隔离邮件的默认操作 , on page 4

发送邮件副本

只有属于管理员组的用户可以发送邮件副本。

要发送邮件副本，请在“副本发送目标: (Send Copy To:)”字段输入邮件地址，然后点击**提交 (Submit)**。发送邮件副本不会导致对邮件执行任何其他操作。

关于在策略隔离区之间移动邮件

在一个邮件网关上，您可以手动在不同策略隔离区之间移动邮件。

将邮件移至其他隔离区时：

- 到期时间不变。邮件保留原始隔离区的到期时间。
- 邮件隔离的原因（包括匹配内容和其他相关详细信息）不变。
- 如果邮件在多个隔离区中，并且您将邮件移至已保留该邮件副本的目标，则邮件的已移动副本的隔离区的到期时间和原因会覆盖原先在隔离区中的邮件副本的到期时间和原因。

多个隔离区中的邮件

如果一个或多个其他隔离区都存在某封邮件，则隔离区邮件列表的“在其他隔离区”(In other quarantines) 列将显示“是”(Yes)，无论您是否有权访问其他隔离区。

一封邮件在多个隔离区中：

- 未传送，除非已从其所在的所有隔离区中将其放行。如果从任何隔离区中将其删除，则绝不会将其传送。
- 未从任何隔离区中删除，直到已从其所在的所有隔离区中将其删除或放行。

由于要放行邮件的用户可能无权访问该邮件所在的所有隔离区，因此适用下列规则：

- 邮件未从任何隔离区中放行，直到已从其所在的所有隔离区中将其放行。
- 如果邮件在任何隔离区中标记为已删除，则无法从该邮件所在的所有其他隔离区中将其传送。（仍可将其放行。）

如果邮件在多个隔离区中加入队列，并且用户无权访问一个或多个其他隔离区：

- 将通知用户邮件是否存在于用户有权访问的各隔离区中。
- GUI 仅显示用户有权访问的隔离区中的计划退出时间。（对于给定邮件，各隔离区有单独的退出时间。）
- 系统不会告知用户存有该邮件的其他隔离区的名称。
- 用户将不会看到导致邮件放入到用户无权访问的隔离区中的匹配内容。
- 放行邮件仅会影响用户有权访问的队列。
- 如果邮件在用户无法访问的其他隔离区中也加入队列，则邮件将保留在隔离区中，保持不变，直到对剩余隔离区具有访问权限的用户进行处理（或者直到通过提前到期或正常到期“正常”放行邮件）。

邮件详细信息和查看邮件内容

点击邮件的主题行以查看该邮件的内容并访问“隔离邮件”(Quarantined Message) 页面。

“隔离邮件”(Quarantined Message) 页面具有两个部分：“隔离区详细信息”(Quarantine Details) 和“邮件详细信息”(Message Details)。

在“隔离的邮件”(Quarantined Message) 页面，可以阅读邮件、选择邮件操作发送邮件副本或者检测病毒。您也可以查看邮件在由于“传送时加密”过滤器操作而从隔离区中放行时是否将加密。

“邮件详细信息”(Message Details) 部分显示邮件正文、邮件标题和附件。仅会显示前 100K 的邮件正文。如果邮件较长，则会显示前 100K，后跟省略号 (...)。实际邮件未截断。这仅用于显示。通过点击“邮件详细信息”(Message Details) 底部“邮件部分”(Message Parts) 中的 [邮件正文]，可以下载邮件正文。您也可以通过点击附件的文件名来下载邮件的任何附件。

如果查看包含病毒的邮件并在计算机上安装桌面防病毒软件，则防病毒软件可能会抱怨其已发现病毒。这对计算机没有威胁，可以放心忽略。

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

Note 对于特殊病毒爆发隔离区，有其他功能可供使用。请参阅病毒爆发隔离区, on page 17。

相关主题

- 查看匹配的内容 , on page 15
- 下载附件 , on page 16
- 病毒检测, on page 16

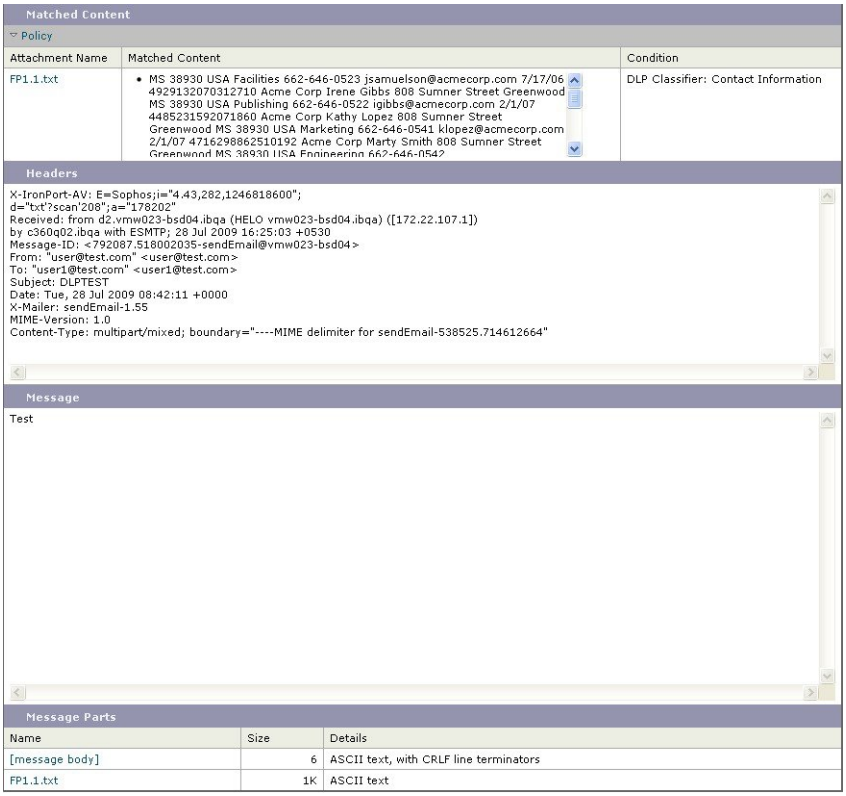
查看匹配的内容

当您对与附件内容条件、邮件正文或附件条件、邮件正文条件或附件内容条件匹配的邮件配置隔离操作时，您可以在已隔离的邮件中查看匹配的内容。当您显示邮件正文时，匹配内容会以黄色突出显示，但 DLP 策略违规匹配项除外。另外，还可以使用 $MatchedContent 操作变量在邮件主题中包括来自邮件或内容过滤器匹配的匹配内容。

如果附件包含匹配内容，则系统会显示附件的内容及其隔离原因（由于DLP策略违规、内容过滤器条件、邮件过滤器条件还是图像分析判定）。

查看本地隔离区中已触发邮件或内容过滤器规则的邮件时，GUI 可能会显示未实际触发过滤器操作的内容（以及已触发过滤器操作的内容）。GUI 显示应用作查找内容匹配项的准则，但是未必会反映内容匹配项的精确列表。发生此情况是因为 GUI 使用的内容匹配逻辑不如过滤器中所使用的严格。此问题仅适用于邮件正文中的突出显示。列出邮件各部分中的匹配字符串以及关联过滤器规则的表是正确的。

Figure 1: 在策略隔离区查看的匹配内容



下载附件

您可以通过点击“邮件部分”(Message Parts) 或“匹配内容”(Matched Content) 部分中的附件的文件名来下载邮件附件。AsyncOS 显示警告，表明来自未知来源的附件可能包含病毒，并询问您是否要继续。下载可能包含病毒的附件的风险由您自行承担。您还可以点击“邮件部分”部分的 [message body] 下载邮件正文。

病毒检测

要测试邮件是否存在病毒，请点击**开始测试 (Start Test)**。使用隔离区保留邮件，直到确定您的防病毒签名已更新。

测试是否存在病毒时，系统会向防病毒引擎发送邮件副本而不是邮件本身。返回并在“隔离区”(Quarantines) 区域上方显示防病毒引擎的结果。

关于重新扫描隔离的邮件

将邮件从其被隔离的所有队列中放行后，将根据为最初隔离邮件的邮件网关和邮件策略启用的功能，进行以下重新扫描：

- 从策略和病毒隔离区放行的邮件由防病毒高级恶意软件保护和灰色邮件引擎重新扫描。
- 从病毒爆发隔离区放行的邮件由反垃圾邮件和防病毒引擎重新扫描。（有关重新扫描病毒爆发隔离区中的邮件的信息，请参阅)
- 从文件分析隔离区中放行的邮件会被重新扫描以查找威胁。
- 具有附件的邮件在从策略、病毒和病毒爆发隔离区中放行后由文件信誉服务重新扫描。

重新扫描后，如果生成的结果与上次处理邮件时生成的结果相符，则不会再次隔离邮件。相反，如果判定不同，则系统可能会将邮件发送到其他隔离区。

基本原理是防止邮件无限地环回到隔离区。例如，假定邮件已加密并因此发送到病毒隔离区。如果管理员放行邮件，则防病毒引擎仍将无法解密该邮件；但是，不应重新隔离邮件，否则将导致循环，并且邮件将永远不会从隔离区中放行。由于两次判定相同，所以第二次系统会绕开病毒隔离区。

病毒爆发隔离区

输入有效的爆发过滤器功能许可密钥后，则存在爆发隔离区。根据阈值集，爆发过滤器功能会将邮件发送到病毒爆发隔离区。有关详细信息，请参阅。

爆发隔离区功能与其他隔离区类似—可以搜索邮件、放行或删除邮件等。

- 标准
- 规则摘要

爆发隔离区包含其他隔离区不可用的一些附加功能：“按规则管理摘要”(Manage by Rule Summary)链接、查看邮件详细信息时“发送到思科”(Send to Cisco) 功能、以及按预定退出时间对搜索结果中的邮件排序的选项。

如果爆发过滤器功能的许可证到期，则您将无法向病毒爆发隔离区中添加更多邮件。当前隔离区中的邮件已到期且病毒爆发隔离区变为空后，则该隔离区不会再显示在 GUI 中的隔离区列表中。

相关主题

- 重新扫描爆发隔离区中的邮件 , on page 17
- “按规则摘要管理”链接, on page 18
- 向思科系统公司报告误报或可疑邮件, on page 18

重新扫描爆发隔离区中的邮件

如果新发布的规则不再将隔离邮件视为威胁，则会自动放行放于病毒爆发隔离区中的邮件。

如果在邮件网关上启用了反垃圾邮件和防病毒功能，扫描引擎将根据适用于邮件的邮件流策略扫描从爆发隔离区放行的每封邮件。

“按规则摘要管理”链接

点击隔离区列表中病毒爆发隔离区旁边的“按规则摘要管理”(Manage by Rule Summary) 链接，以查看“按规则摘要管理”(Manage by Rule Summary) 页面。您可以根据哪些病毒爆发规则导致隔离邮件来对隔离区中的所有邮件执行邮件操作（放行、删除、延迟退出）。这非常适合清理爆发隔离区中的大量邮件。有关更多信息，请参阅“病毒爆发隔离区和管理规则摘要”视图下的主题

向思科系统公司报告误报或可疑邮件

查看爆发隔离区中邮件的详细信息时，可以将邮件发送到思科报告误报或可疑邮件。

Procedure

步骤 1 导航至病毒爆发隔离区中的邮件。

步骤 2 在“邮件详细信息”(Message Details) 部分中，选中**向思科系统发送副本 (Send a Copy to Cisco Systems)** 复选框。

步骤 3 在新 Web 界面中，点击表中“爆发过滤器”条目的“邮件”列中的蓝色数字，然后选中邮件的复选框，并选择“发送副本”  。

步骤 4 输入收件人地址，然后点击**发送 (Send)**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。