集中策略、病毒和病毒爆发隔离区

本章包含以下部分：

- 集中隔离区概述 , on page 1
- 集中策略、病毒和病毒爆发隔离区 , on page 2
- 管理策略、病毒和病毒爆发隔离区, on page 9
- 处理策略、病毒或爆发隔离区中的邮件, on page 19
- 排除集中策略隔离区故障 , on page 26

集中隔离区概述

可以将邮件安全设备中某些过滤器、策略和扫描操作处理的邮件放在隔离区中临时保存，以供后续操作。您可以集中来自思科内容安全管理设备上的多个邮件安全设备的隔离区。

集中隔离区的优势包括以下几点：

- 可以集中于一处来管理多个邮件安全设备的被隔离邮件。
- 隔离的邮件存储在防火墙后，而不是 DMZ 中，从而降低安全风险。
- 集中的隔离区可以被备份为安全管理设备上的标准备份功能的一部分。

防病毒扫描、爆发过滤器和高级恶意软件防护（文件分析）各有一个专用隔离区。创建策略隔离区来保留由邮件过滤、内容过滤和防数据丢失策略捕获到的邮件。

传统 Web 界面中的“策略”、“病毒”和“爆发隔离区”部分在新的网络界面中被标记为“其他隔离区”。有关详细信息，请参阅查看隔离区中的邮件 , on page 19。

有关隔离区的详细信息，请参阅邮件安全设备的相应文档。

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

集中策略、病毒和病毒爆发隔离区

Procedure

	Command or Action	Purpose
步骤 1	如果您的邮件安全设备在 DMZ 中，且安全管理设备受防火墙保护，请打开防火墙中的端口以允许设备交换集中策略、病毒和病毒爆发隔离区数据。	防火墙信息

集中策略、病毒和病毒爆发隔离区

	Command or Action	Purpose
步骤 2	在安全管理设备上，启用此功能。	在安全管理设备上启用集中策略、病毒和病毒爆发隔离区 , on page 4
步骤 3	在安全管理设备中，为非垃圾邮件隔离区分配磁盘空间。	管理磁盘空间
步骤 4	（可选） • 在安全管理设备上，用所需设置创建集中策略隔离区。 • 配置集中病毒和爆发隔离区以及默认策略隔离区的设置。 如果在迁移之前配置这些设置，可以参考邮件安全设备中的现有设置。 您也可以在配置自定义迁移时创建所需隔离区，或者将在自动迁移过程中为您创建隔离区。迁移过程中创建的所有隔离区都具有默认设置。 即使隔离区名称相同，本地隔离区设置也未保留在集中隔离区中。	• 配置策略、病毒和爆发隔离区 , on page 11 • 检查系统创建的隔离区的设置 , on page 11。
步骤 5	在安全管理设备中，添加要管理的邮件安全设备或从已添加设备的集中服务中选择“策略、病毒和爆发隔离区(Policy, Virus and Outbreak Quarantines)”选项。 • 如果您的邮件安全设备已集群，则属于特定级别（计算机、分组或集群）的所有设备必须添加到安全管理设备，之后您才能在集群中的任意邮件安全设备上启用集中策略、病毒和病毒爆发隔离区。	向每个受管邮件安全设备添加集中策略、病毒和病毒爆发隔离区服务, on page 5
步骤 6	确认您的更改。	
步骤 7	在安全管理设备上，配置从邮件安全设备迁移现有策略隔离区。	配置策略、病毒和病毒爆发隔离区的迁移 , on page 6
步骤 8	在邮件安全设备上，启用集中策略、病毒和病毒爆发隔离区功能。 • **Important** 如果您在邮件安全设备上配置了策略、病毒和爆发隔离区，请在确认此更改后尽快开始迁移隔离区及所有邮件。	请参阅邮件安全设备文档中的“在思科内容安全管理设备上集中服务”一章，具体是指以下部分： • “关于策略、病毒和病毒爆发隔离区的迁移” • " 集中策略、病毒和病毒爆发隔离区 "
步骤 9	迁移更多的邮件安全设备。	

	Command or Action	Purpose
	• 任何时候，只能有一个迁移流程正在进行。在前一个迁移完成之前，请勿在其他邮件安全设备上启用集中策略、病毒和爆发隔离区。	
步骤 10	根据需要，编辑集中隔离区设置。 • 迁移过程中创建的隔离区是使用默认设置而不是源本地隔离区中的设置进行创建，即使集中和本地隔离区名称相同也如此。	配置策略、病毒和爆发隔离区 , on page 11
步骤 11	如果邮件过滤器、内容过滤器和 DLP 邮件操作无法自动更新为集中隔离区的名称，请在您的邮件安全设备上手动更新这些配置。 • 在集群配置中，仅当在特定级别定义了过滤器和邮件操作时，这些过滤器和邮件操作才能在该级别自动更新。	请参阅邮件安全设备在线帮助或用户指南中的邮件过滤器、内容过滤器和 DLP 邮件操作文档。
步骤 12	（推荐）如果始发设备不可用，请指定一台邮件安全设备来处理放行的邮件。	指定处理所放行邮件的备用设备, on page 8
步骤 13	如果向自定义用户角色委派管理权限，可能需要以特定方式配置访问权限。	为自定义用户角色配置集中隔离区访问权限

在安全管理设备上启用集中策略、病毒和病毒爆发隔离区

Before you begin

完成集中策略、病毒和病毒爆发隔离区 , on page 2的表中此过程之前的所有步骤。

步骤 1 依次选择**管理设备 (Management Appliance)** > **集中服务 (Centralized Services)** > **策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 指定与邮件安全设备通信的接口和端口：

- 接受默认选择，除非有特定原因需要更改。
- 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。
- 使用您在防火墙中打开的同一端口。

步骤 4 点击**提交 (Submit)**。

What to do next

返回集中策略、病毒和病毒爆发隔离区 , on page 2表中的后续步骤。

在设备的新 Web 界面上启用集中策略、病毒和隔离区功能

Before you begin

完成集中策略、病毒和病毒爆发隔离区 , on page 2的表中此过程之前的所有步骤。

步骤 1 在安全管理设备上，点击**服务状态 (Service Status)**，，将鼠标悬停在与**其他隔离区 (Other Quarantine)** 对应的 图标上，然后点击**编辑设置 (Edit Settings)**。

步骤 2 重定向到旧界面后，点击**启用 (Enable)**。

向每个受管邮件安全设备添加集中策略、病毒和病毒爆发隔离区服务

要查看所有邮件安全设备上全部隔离区的整合视图，请考虑在集中任何隔离区之前添加所有邮件安全设备。

Before you begin

确保您已完成了集中策略、病毒和病毒爆发隔离区 , on page 2表中此位置之前的所有过程。

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

步骤 2 选择**管理设备 (Management Appliance)** > **集中化服务 (Centralized Services)** > **安全设备 (Security Appliances)**。

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) 点击邮件安全设备的名称。

b) 选择**策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)** 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) 点击“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，输入正在添加的设备的管理接口的设备名称和 IP 地址。

Note 如果在“IP 地址”(IP Address) 文本字段中输入 DNS 名称，则点击**提交 (Submit)**后，该名称将立即解析为 IP 地址。

c) 策略、病毒和病毒爆发隔离区服务已预先选择。

d) 点击**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，然后点击**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) 等待该页面表格上方显示成功消息。

步骤 5 点击**提交 (Submit)**。

步骤 6 对于想要启用集中策略/病毒和爆发隔离区的每台邮件安全设备，重复上述程序。

例如，在集群中添加其他设备。

步骤 7 提交更改。

What to do next

返回集中策略、病毒和病毒爆发隔离区 , on page 2表中的后续步骤。

配置策略、病毒和病毒爆发隔离区的迁移

Before you begin

- 确保您已完成了相应表中此位置之前的所有过程，该表位于： 集中策略、病毒和病毒爆发隔离区 , on page 2
- 有关迁移过程的警告和信息，请参阅邮件安全设备文档中“在思科内容安全管理设备上集中服务”一章中的“关于策略、病毒和爆发隔离区的迁移”部分。

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

步骤 2 依次选择**管理设备集中服务 > 策略、病毒和病毒爆发隔离区**。

步骤 3 点击**启动迁移向导 (Launch Startup Wizard)**。

步骤 4 选择迁移方法：

如果	选择	更多信息
• 想要迁移所有关联邮件安全设备中的所有现有策略隔离区， 和 • 所有邮件安全设备上名称相同的策略隔离区具有相同的设置， 和 • 要将所有邮件安全设备上名称相同的全部策略隔离区合并为一个采用该名称的集中策略隔离区。	自动 (Automatic)	使用此流程创建的所有集中策略隔离区均自动配置为默认设置，无论邮件安全设备中名称相同的隔离区的设置如何。 迁移后必须更新这些设置。

如果	选择	更多信息
• 名称相同的策略隔离区在不同的邮件安全设备上具有不同的设置，并要保留差异， 或者 • 您希望迁移一些本地隔离区并删除其他隔离区， 或者 • 您希望将本地隔离区迁移到具有不同名称的集中隔离区 或者 • 您希望将具有不同名称的本地隔离区合并成单个集中隔离区。	自定义 (Custom)	在迁移过程中而不是迁移之前创建的所有集中策略隔离区都将使用新隔离区的默认设置进行配置。 您应在迁移后更新这些设置。

步骤 5 点击**下一步 (Next)**。

步骤 6 如果选择**自动 (Automatic)**：

验证要迁移的策略隔离区和此页面上的其他信息是否与预期匹配。

病毒、爆发和文件分析隔离区也将迁移。

步骤 7 如果选择**自定义 (Custom)**：

- 要选择显示所有邮件安全设备中的隔离区，还是只显示一台设备中的隔离区，请从**显示其中隔离区: (Show Quarantines from:)** 列表中选择一个选项。
- 选择移至各集中策略隔离区的本地策略隔离区。
- 根据需要，创建其他集中策略隔离区。这些隔离区将具有默认设置。
- 隔离区名称区分大小写。
- 左侧表中剩余的隔离区都不会迁移，而且会在迁移时将其从邮件安全设备中删除。
- 您可以通过从右侧表中选择隔离区并点击**从集中隔离区中删除 (Remove from Centralized Quarantine)** 来更改隔离区映射。

步骤 8 根据需要，点击**下一步 (Next)**。

步骤 9 提交并确认更改。

What to do next

返回集中策略、病毒和病毒爆发隔离区 , on page 2表中的后续步骤。

指定处理所放行邮件的备用设备

通常，从集中隔离区放行邮件后，安全管理设备会将邮件返回到将其初始发送到该集中隔离区的邮件安全设备进行处理。

如果始发邮件的不可用，其他邮件安全设备可处理和传送放行的邮件。您需要指定设备来完成此操作。

Before you begin

- 检验备用设备是否可按预期处理和传送已放行的邮件。例如，加密和防病毒重新扫描的配置应与主设备上的配置匹配。
- 必须为集中策略、病毒和病毒爆发隔离区完全配置备用设备。针对该设备完成集中策略、病毒和病毒爆发隔离区 , on page 2中表内的步骤。

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

步骤 2 选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 3 点击**指定备用放行设备 (Specify Alternate Release Appliance)** 按钮。

步骤 4 选择一个邮件安全设备。

步骤 5 提交并确认更改。

What to do next

相关主题

当邮件安全设备不可用时放行邮件 , on page 9

为自定义用户角色配置集中隔离区访问权限

为了允许具有自定义用户角色的管理员指定邮件安全设备上邮件过滤器、内容过滤器和 DLP 邮件操作中的集中策略隔离区，您必须授予这些用户访问安全管理设备中相关策略隔离区的权限，而且在安全管理设备中创建的自定义用户角色名称必须与中的名称匹配。

相关主题

- 创建自定义邮件用户角色

禁用集中策略、病毒和爆发隔离区

通常，如果需要禁用这些集中隔离区，需要在邮件安全设备中执行此操作。

有关禁用集中策略、病毒和爆发隔离区的信息（包括执行此操作的影响列表），请参阅邮件安全设备在线帮助或文档。

当邮件安全设备不可用时放行邮件

通常，从集中隔离区放行邮件后，安全管理设备会将邮件返回到将其初始发送到该集中隔离区的邮件安全设备进行处理。

如果始发邮件的不可用，其他邮件安全设备可处理和传送放行的邮件。您需要指定备用放行设备来完成此操作。

如果备用设备不可用，可以指定其他邮件安全设备作为备用放行设备，该设备将处理并传送排队的邮件。

在多次尝试连接邮件安全设备都失败后，您将会收到警报。

相关主题

- 指定处理所放行邮件的备用设备, on page 8

管理策略、病毒和病毒爆发隔离区

- 策略、病毒和爆发隔离区的磁盘空间分配 , on page 9
- 邮件在隔离区中的保留时间 , on page 10
- 自动处理的隔离邮件的默认操作 , on page 11
- 检查系统创建的隔离区的设置 , on page 11
- 配置策略、病毒和爆发隔离区 , on page 11
- 关于编辑策略、病毒和爆发隔离区设置 , on page 13
- 确定策略隔离区分配到的过滤器和邮件操作 , on page 13
- 关于删除策略隔离区 , on page 14
- PVO 隔离区阈值警报 , on page 14
- 监控隔离区状态、容量和活动 , on page 16
- 关于隔离区磁盘空间使用量的警报 , on page 17
- 策略隔离区和日志记录, on page 18
- 关于向其他用户分配邮件处理任务 , on page 18

策略、病毒和爆发隔离区的磁盘空间分配

有关分配磁盘空间的信息，请参阅管理磁盘空间。

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：

- 使用设备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。
- 安全管理设备上用于特定受管邮件安全设备上爆发隔离区中邮件的磁盘空间，可能受该邮件安全设备上可用于被隔离邮件的磁盘空间所限。
- 有关这种情况的详细信息，请参阅 邮件在隔离区中的保留时间 , on page 10

相关主题

- 监控隔离区状态、容量和活动 , on page 16
- 关于隔离区磁盘空间使用量的警报 , on page 17
- 邮件在隔离区中的保留时间 , on page 10

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 9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，邮件将暂存于邮件安全设备中，直到安全管理设备中的空间可用。

    由于安全管理设备不扫描邮件，因此集中爆发隔离区中每个邮件的副本会存储在最初处理该邮件的邮件安全设备上。这样，邮件安全设备可在爆发过滤器规则每次更新时重新扫描被隔离的邮件，并通知安全管理设备放行不再被视为威胁的邮件。爆发隔离区的两个副本应一直保留相同的邮件集。因此，如果邮件安全设备中的空间鲜有地变满，则两台设备上爆发隔离区中邮件的副本将提前到期，即使集中隔离区仍有空间亦不例外。

    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 17。

- 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 11。

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

- 夏令时和设备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 10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 25。

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 11。

从集中隔离区放行的邮件将返回到始发邮件安全设备进行处理。

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 11

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 13。
- 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 10和自动处理的隔离邮件的默认操作 , on page 11。
- 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 18。

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**电子邮件 (Email)** > **邮件隔离区 (Message Quarantine)** > **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。

用户	信息
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

请参阅“邮件过滤器”(Message Filters) 页面和“内容过滤器”(Content Filters) 页面

- 如果尚未迁移邮件安全设备中的隔离区，请执行以下操作：

  您将在迁移过程中将这些隔离区分配给邮件过滤器和内容过滤器以及 DLP 邮件操作。

- 如果您已迁移到集中隔离区：

  确保您的邮件安全设备具有邮件和内容过滤器及 DLP 邮件操作，可将邮件移到隔离区。请参阅邮件安全设备用户指南或在线帮助。

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 10。

要更改隔离区设置，请依次选择 **邮件 (Email) > 邮件隔离区 (Message Quarantine) > 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

要在旧 Web 界面上更改隔离区设置，请选择**电子邮件 (Email) > 邮件隔离区 (Message Quarantine) > 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。

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 验证配置文件及配置各项设置的邮件安全设备。

步骤 1 [仅限新 Web 界面] 在安全管理设备上，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**邮件 (Mail)** > **邮件隔离区 (Message Quarantine)** > **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 13。
- 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 11。
- 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。

PVO 隔离区阈值警报

当 PVO 隔离区邮件数超过为特定持续时间和 PVO 隔离区设置的用户定义阈值时，安全邮件和 Web 管理器会向收件人发送警报。安全邮件和 Web 管理器可确保您收到设置为邮件的警报。

您可以使用 CLI 或 Web 界面配置 PVO 隔离区阈值警报。

相关主题

- 使用 CLI 配置 PVO 隔离区阈值警报设置, on page 14
- 使用 Web 界面配置 PVO 隔离区阈值警报设置, on page 15

使用 CLI 配置 PVO 隔离区阈值警报设置

要配置 PVO 隔离区阈值警报，请使用 CLI 中的 `quarantineconfig` 命令。执行命令时，系统会提示您启用或禁用 PVO 隔离区阈值警报。默认情况下，PVO 隔离区阈值警报处于禁用状态。您必须为以下各项参数提供值：

- **阈值**：配置阈值。如果 PVO 隔离区邮件数超过此值，思科安全邮件和 Web 管理器会向收件人发送警报。可以为每个隔离区策略配置此值。值范围为 1 到 10,000,000。
- **持续时间**：配置思科安全邮件和 Web 管理器必须对每个隔离区中的 PVO 隔离区邮件数进行计数的持续时间（以小时为单位）。取值范围为 0.5 到 24。只能将持续时间的值配置为 0.5 的倍数（0.5、1、1.5 等）。
- **警报限制**：配置警报限制。此值表示思科安全邮件和 Web 管理器在配置的持续时间内向收件人发送的警报数。每个隔离区策略都配置此值。取值范围为 1 到 20。

程序

命令或操作	目的
`quarantineconfig`	此命令配置 PVO 隔离阈值警报。

使用 Web 界面配置 PVO 隔离区阈值警报设置

您可以使用安全邮件和 Web 管理器的 Web 界面配置 PVO 隔离阈值警报。

Before you begin

请确保您已满足以下前提条件，才能接收 PVO 隔离区阈值警报：

- 配置系统警报。
- 已启用系统 - 严重警报。

步骤 1 [仅限新 Web 界面] 在邮件安全管理设备中，点击 以加载旧版 web 界面。

步骤 2 请转至 **邮件 > 邮件隔离 > 策略、病毒和爆发隔离** 页面。

策略、病毒和病毒爆发隔离 页面显示。 **隔离区** 窗口显示所有 PVO 隔离。

步骤 3 点击 **添加策略隔离** 以添加新的 PVO 隔离，或点击现有的 PVO 隔离以编辑 PVO 隔离。

有关添加和编辑 PVO 隔离的详细信息，请参阅 配置策略、病毒和爆发隔离区 , on page 11 部分。

步骤 4 在 **阈值警报设置** 窗口中选中 **启用阈值警报** 复选框。

步骤 5 在 **阈值警报设置** 窗口中输入以下字段的值。

- 阈值 (Threshold)
- 持续时间
- 警报限制

有关参数的更多详细信息，请参阅 使用 CLI 配置 PVO 隔离区阈值警报设置, on page 14 部分。

步骤 6 提交并确认更改。

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] 在安全管理设备中，点击 加载旧 Web 界面。 依次选择**管理策略 > 集中服务 > 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)**。 或 选择，并查看下方的表格。 表上方的“隔离区”部分中显示策略、病毒和病毒爆发隔离区的可用空间
所有隔离区当前使用的总空间	[仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。 选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**。
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)**。 该表显示每个隔离区当前使用的空间量。 或 选择**电子邮件 (Email) > 邮件隔离区 (Message Quarantine) > 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] 在安全管理设备中，点击 加载旧 Web 界面。 选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**。

要查看	相应操作
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)**。 该表显示当前可用于每个隔离区的邮件总数。 或 选择**电子邮件 (Email)** > **邮件隔离区 (Message Quarantine)** > **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。
所有隔离区的总 CPU 使用量	[仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。 选择**管理设备 (Management Appliance)** > **集中服务 (Centralized Services)** > **系统状态 (System Status)**，并查看“系统信息”(System Information) 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)**。 该表显示隔离上一封邮件的日期和时间。 或 选择**电子邮件 (Email)** > **邮件隔离区 (Message Quarantine)** > **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] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。 选择**电子邮件 (Email)** > **邮件隔离区 (Message Quarantine)** > **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 13。

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 18
- 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：

- 管理员或邮件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被隔离邮件的信息。

注意：要允许安全管理设备上配置的自定义用户角色在过滤器和DLP邮件操作中指定策略隔离区，请参阅为自定义用户角色配置集中隔离区访问权限 , on page 8。

最终用户无权查看或访问策略、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 19
- 搜索策略、病毒和病毒爆发隔离区中的邮件 , on page 20
- 手动处理隔离区中的邮件, on page 21
- 多个隔离区中的邮件 , on page 22
- 邮件详细信息和查看邮件内容, on page 23
- 关于重新扫描隔离的邮件 , on page 25
- 病毒爆发隔离区, on page 25

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)**。 或 选择**邮件 (Email)** > **邮件隔离区 (Message Quarantine)** > **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)**。 或 选择**邮件 (Email)** > **邮件隔离区 (Message Quarantine)** > **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 26或规则摘要视图, on page 26[仅限新 Web 界面]。

要想	相应操作
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 (>>)。 [仅限新 Web 界面] 向下滚动表以显示所有新邮件的详细信息。
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。
自定义表列	点击 并选择要显示的列，然后点击“关闭”(Close)
查看导致邮件隔离的内容。	请参阅查看匹配的内容 , on page 24。

相关主题

- 隔离的邮件和国际字符集, on page 20

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。

搜索策略、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。

步骤 1 [仅限新 Web 界面] 选择**隔离区 (Quarantine)** > **其他隔离区 (Other Quarantine)** > **搜索 (Search)**。

步骤 2 [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 3 选择 **邮件** > **邮件隔离区 (Message Quarantine)** > **策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 4 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 5 （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 21。

有关修改搜索条件的信息，请参阅修改搜索条件, on page 21。

修改搜索条件

可以将搜索条件修改为自定义时间范围或其他隔离区。

若要修改搜索条件，请点击**修改 (Modify)**。

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**邮件 (Email) > 邮件隔离区 (Message Quarantine) > 策略、病毒和病毒爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**页面或[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。
- 点击隔离邮件的复选框，然后选择所需的操作。

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视图相关信息。

相关主题

- 发送邮件副本, on page 22
- 关于在策略隔离区之间移动邮件 , on page 22
- 多个隔离区中的邮件 , on page 22
- 自动处理的隔离邮件的默认操作 , on page 11

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

在一个设备上，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、选择邮件操作或发送邮件副本。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。

Note “邮件详细信息”(Message Details) 页面上的附件下载最大限制为 25 MB。

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 25。

相关主题

- 查看匹配的内容 , on page 24
- 下载附件 , on page 24

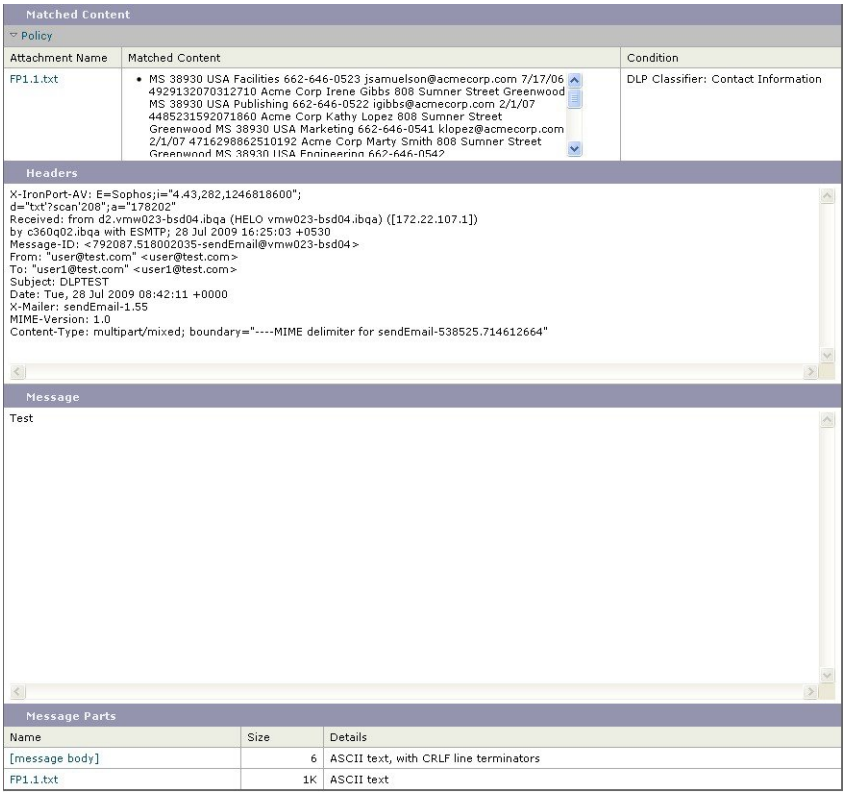
查看匹配的内容

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。

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设备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。
- 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，请参阅邮件安全设备的在线帮助或用户指南中的“爆发过滤器”一章。

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。

病毒爆发隔离区包含以下视图：

病毒爆发隔离区包含其他隔离区不可用的一些附加功能：**规则摘要**视图、查看邮件详细信息时**发送到思科**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 25
- 规则摘要视图, on page 26
- 向思科系统公司报告误报或可疑邮件, on page 26

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。

如果在设备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。

规则摘要视图

规则摘要视图仅在新的 Web 界面中可用。

在爆发隔离区中，点击**规则摘要 (Rule Summary)** 选项卡以查看按规则 ID 分组的爆发隔离区内容的列表。

根据导致邮件被隔离的爆发规则，可以对隔离区中的所有邮件执行邮件操作（放行和删除）。这非常适合清理爆发隔离区中的大量邮件。有关详细信息，请参阅邮件安全设备 *AsyncOS* 的联机帮助或用户指南中的“爆发过滤器”章节的“病毒爆发隔离区”和“按规则摘要管理视图”部分。

“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，请参阅邮件安全设备的联机帮助或用户指南中有关“爆发过滤器”一章中的“管理规则摘要”视图的信息

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。

步骤 1 导航至病毒爆发隔离区中的邮件。

步骤 2 输入收件人地址，然后点击**发送 (Send)**。

排除集中策略隔离区故障

- 管理用户无法选择过滤器和 DLP 邮件操作中的隔离区, on page 26
- 不重新扫描从集中病毒爆发隔离区放行的邮件 , on page 26

管理用户无法选择过滤器和 DLP 邮件操作中的隔离区

问题

管理用户无法查看或选择邮件安全设备上内容和邮件过滤器或 DLP 操作中的隔离区。

解决方案

请参阅为自定义用户角色配置集中隔离区访问权限 , on page 8

不重新扫描从集中病毒爆发隔离区放行的邮件

问题

从病毒爆发隔离区中放行的邮件在传送之前应再次扫描。但是，一些受感染的邮件已从隔离区进行传递。

解决方案

在以下内容所述的情况下，可能会出现这种情况。 关于重新扫描隔离的邮件 , on page 25

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。