思科内容安全管理设备 AsyncOS 9.0 用户指南

2015 年 8 月 14 日

思科系统公司
www.cisco.com

思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices。

文本部件号：不适用

目 录

简介

本版本中的新增内容

本节介绍此版本思科内容安全管理 AsyncOS 中的新功能和增强功能。有关此版本的更多信息，请参阅以下 URL 的产品版本说明：

http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html

如果要升级，还应查看之前版本和此版本之间其他版本的版本说明，以了解这些版本中添加的功能和增强功能。

特性	说明
虚拟外形	此思科内容安全管理虚拟设备版本支持邮件安全设备。 有关完整信息，请参阅以下位置的*思科内容安全虚拟设备安装指南*：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html。
磁盘空间管理改进	• 删除了对垃圾邮件隔离区大小的限制。 • 对于虚拟设备，可以使用 VMWare 工具增加用于安全管理设备实例的磁盘空间。现在支持大小超过 2 TB 的单个分区。 如果要升级现有的虚拟设备，请参阅版本说明中升级虚拟设备部分的重要警告。 • 添加了额外的配额 （其他文件），以允许管理用于日志文件、数据包捕获和配置文件的空间。 有关完整信息，请参阅管理磁盘空间 （第 14-45 页）。

特性	说明
集中文件分析隔离区	现在，发送文件进行文件分析时，可以在思科内容安全管理设备中隔离文件。但是，与邮件安全设备不同，此隔离区不会根据文件分析结果自动释放邮件。相反，会在您指定的保留时间内暂存邮件。 升级到此版本后，会自动创建此隔离区。这就是所谓的 “策略、病毒和病毒爆发隔离区”隔离区组之一，它们与这些隔离区的常规设置和行为相同。 有关详细信息，请参阅关于集中文件分析隔离区 （第 8-15 页）。
向设备管理员显示消息	可以创建管理用户登录到设备时显示的消息。 目前，只能通过命令行界面 (CLI) 使用此功能。有关信息，请参阅向管理用户显示消息 （第 13-22 页）。
查看最近的设备登录	可以使用您的凭证查看最近尝试访问设备的简短列表。 请参阅查看最近的登录尝试 （第 13-23 页）。
各用户的垃圾邮件通知	可以根据 LDAP 组指定接收垃圾邮件通知的用户。
报告和跟踪新功能	更新了报告和跟踪，以支持思科邮件安全设备 AsyncOS 9.0 中的新功能。
新密码更改选项	需要手动更改密码时 （例如更改密码要求之后），可以选择用户是否必须在下次登录或指定期限后更改密码。 如果要强制在指定期限后更改密码，还可以设置宽限期以在密码到期后重置密码。 另外，还可以为更改密码计划指定宽限期。
导入配置文件	现在，可以选择在导入配置文件时忽略网络设置和磁盘配额设置，从而简化设备之间的配置迁移。 在思科内容安全管理设备 AsyncOS 8.4 中也可以使用此功能，但该版本仅支持网络安全设备。

思科内容安全管理概述

思科内容安全管理 AsyncOS 加入了以下功能：

- **外部垃圾邮件隔离区：**为最终用户暂存垃圾邮件和可疑垃圾邮件，使用户和管理员在做出最终决定前能够审核标记为垃圾邮件的邮件。
- **集中策略、病毒和病毒爆发隔离区：**提供单一界面来管理多个邮件安全设备的隔离区和其中隔离的邮件。允许将隔离的邮件存储在防火墙后。
- **集中报告：**从多个邮件和网络安全设备运行有关汇聚数据的报告。各个设备上可用的相同报告功能在安全管理设备上也可用。此外，还有安全管理设备上所独有的网络安全扩展报告。
- **集中跟踪：**使用单个界面跟踪由多个邮件和网络安全设备处理的邮件和网络事务。
- **网络安全设备的集中配置管理：**为简便且一致起见，管理多个网络安全设备的策略定义和策略部署。

注　安全管理设备不涉及集中邮件管理或邮件安全设备 “集群”。

- **数据备份**：在安全管理设备中备份数据，包括报告和跟踪数据、隔离的邮件及安全和阻止的发件人列表。

可以从单个安全管理设备中协调安全操作，也可以在多个设备之间分布负载。

第 2 章

设置、安装和基本配置

解决方案部署概述

要配置思科内容安全管理设备，以便向思科内容安全解决方案提供服务，请执行以下操作：

	在这些设备上	操作	更多信息
步骤 1	**所有设备**	确保您的设备满足将使用的功能的系统要求。 如果需要，请升级您的设备。	请参阅 SMA 兼容性列表 （第 2-2 页）。
步骤 2	**邮件安全设备**	在向您的环境引入集中服务之前，请配置所有邮件安全设备以提供所需的安全功能，并确认每台设备上的所有功能是否都按预期运行。	请参阅您所用版本的思科邮件安全的文档。
步骤 3	网络安全设备	在向您的环境引入集中服务之前，请配置至少一台网络安全设备以提供所需的安全功能，并确认所有功能是否按预期运行。	请参阅网络安全设备的在线帮助或用户指南。
步骤 4	安全管理设备	设置并运行 “系统设置向导 (System Setup Wizard)”。	请参阅 “安装规划”部分 （第 2-2 页）、“设置准备”部分 （第 2-3 页）和 “运行 “系统设置向导 (System Setup Wizard)”” 部分 （第 2-7 页）。
步骤 5	所有设备	配置想要部署的每个集中服务。	从 “在安全管理设备上配置服务”部分 （第 2-12 页）开始。

SMA 兼容性列表

欲了解您的安全管理设备与邮件安全设备和网络安全设备的兼容性，以及在导入和发布网络案例设备配置时的配置文件兼容性，请参阅位于以下位置的兼容性列表：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。

安装规划

网络规划

安全管理设备允许您将最终用户应用与驻留在隔离区 (DMZ) 的更安全的网关系统隔开。使用两层防火墙可灵活地进行网络规划，这样，最终用户就不用直接连接到外部 DMZ 了 （请参阅图 2-1）。

图 2-1　　典型网络配置包含安全管理设备

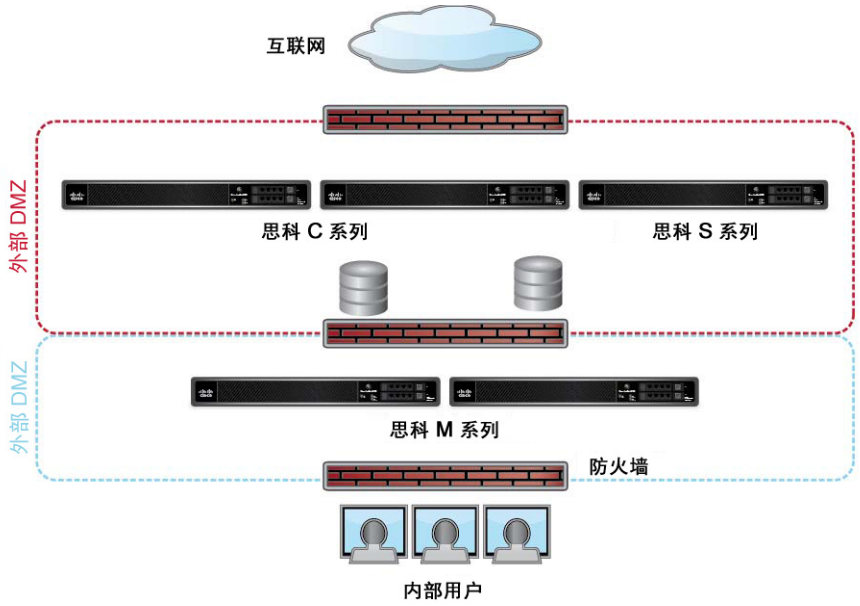


图 2-1 显示纳入安全管理设备和多个 DMZ 的典型网络配置。将安全管理设备部署在内部网络中 DMZ 的外部。所有连接均是由安全管理设备 （M 系列）向托管理邮件安全设备 （C 系列）和托管网络安全设备 （S 系列）发起。

企业数据中心可以共享安全管理设备，以便为多个网络和邮件安全设备执行集中报告和邮件跟踪，同时为多个网络安全设备进行集中策略配置。安全管理设备还可以用作外部垃圾邮件隔离区。

将邮件安全设备和网络安全设备连接到安全管理设备并正确配置所有设备后， AsyncOS 将收集和整合来自托管设备的数据。可以根据整合的数据生成报告，并可确定邮件和网络使用的总体概况。

关于安全管理设备与邮件安全设备的集成

有关安全管理设备与邮件安全设备集成的更多信息，请参阅邮件安全设备用户文档或在线帮助中的“在思科内容安全管理设备中集中服务”一章。

使用集群化的邮件安全设备部署

不能将安全管理设备放在使用邮件设备的集中管理功能的邮件安全设备集群中。但是，集群化的邮件安全设备可向安全管理设备传送邮件以进行集中报告和跟踪，也可向隔离区传送邮件。

设置准备

运行“系统设置向导 (System Setup Wizard)”之前的准备工作：

操作步骤

步骤 1 查看产品的最新版本说明。请参阅文档 （第 E-2 页）。

步骤 2 确认安全解决方案的组件是否兼容。请参阅 SMA 兼容性列表 （第 2-2 页）。

步骤 3 确保您的网络和物理空间能够支持此部署。请参阅安装规划 （第 2-2 页）。

步骤 4 进行实际设置并连接安全管理设备。请参阅进行实际设置并连接设备 （第 2-3 页）。

步骤 5 确定网络和 IP 地址分配。请参阅确定网络和 IP 地址分配 （第 2-3 页）。

步骤 6 收集系统设置的相关信息。请参阅收集设置信息 （第 2-4 页）。

进行实际设置并连接设备

在按照本章中的程序操作之前，请完成设备随附的快速入门指南中所述的步骤。在本指南中，假定您已打开设备包装，将其实际安装在机架中，并已开启设备。

在登录到 GUI 之前，需要设置 PC 和安全管理设备之间的专用连接。例如，可以使用随附的交叉电缆从设备的管理端口直接连接到笔记本电脑。或者，也可以通过 PC 和网络之间的以太网接口（例如，以太网集线器），以及网络和安全管理设备中的管理端口之间的以太网接口连接。

确定网络和 IP 地址分配

备注 如果您已将设备连线到网络，请确保内容安全设备的默认 IP 地址与网络中的其他 IP 地址不存在冲突。每台设备的管理端口中预配置的 IP 地址是 192.168.42.42。

完成设置后，依次转至主安全管理设备上的**管理设备 (Management Appliance) > 网络 (Network) > IP 接口 (IP Interfaces)** 页面，更改安全管理设备使用的接口。

您需要有关选择使用的每个以太网端口的下列网络信息：

- IP 地址
- Netmask

此外，需要有关整个网络的以下信息：

- 网络中默认路由器 （网关）的 IP 地址
- DNS 服务器的 IP 地址和主机名 （如果想要使用互联网根服务器，则无需此信息）
- NTP 服务器的主机名或 IP 地址 （如果想要手动设置系统时间，则无需此信息）

有关详细信息，请参阅附录 B “分配网络和 IP 地址”。

备注 如果网络中互联网和内容安全设备之间正在运行防火墙，则可能需要打开特定端口，设备才能正常运行。有关防火墙的详细信息，请参阅附录 C “防火墙信息”。

备注 请始终使用安全管理设备上的相同 IP 地址用于向邮件安全设备发送邮件以及从中接收邮件。有关说明，请参阅您的邮件安全设备的说明文档中的邮件流信息。

请注意，思科内容安全管理设备与其管理的设备之间不支持使用 IPv6 进行通信。

收集设置信息

使用下表收集有关系统设置的信息。在运行 “系统设置向导 (System Setup Wizard)”时，可能随时需要这些信息。

备注 有关网络和 IP 地址的详细信息，请参阅附录 B “分配网络和 IP 地址”。

表 2-1　　系统设置工作表

1	通知	发送系统警报的邮件地址：
2	系统时间	NTP 服务器 （IP 地址或主机名）：
3	管理员密码	为 “admin”帐户选择一个新密码：
4	自动支持	是否启用自动支持？ ___ 是 ___ 否
5	主机名	安全管理设备的完全限定主机名：
6	接口/IP 地址	IP 地址：
		掩码:

7	网络	网关	默认网关 （路由器） IP 地址：
		DNS	___ 使用互联网的根 DNS 服务器
			___ 使用这些 DNS 服务器：

访问安全管理设备

安全管理设备包含基于 Web 的标准图形用户界面、用于管理垃圾邮件隔离区的基于 Web 的独立界面、命令行界面和面向有权访问特定特性和功能的管理用户的特殊或限定界面。

浏览器要求

要访问 GUI，您的浏览器必须支持和能够接受 JavaScript 和 Cookie，而且必须能够显示包含级联样式表 (CSS) 的 HTML 页面。

表 2-2　　受支持的浏览器和版本

浏览器	Windows XP	Windows 7	MacOS 10.6
Safari	-	-	5.1
Google Chrome	最新稳定版本	-	-
Microsoft Internet Explorer	7.0、 8.0	8.0、 9.0	-
Mozilla Firefox	最新稳定版本	最新稳定版本	最新稳定版本

要使用 GUI，可能需要配置浏览器的弹出阻止设置，因为界面中的某些按钮或链接会导致其他窗口打开。

关于访问网络界面

安全管理设备有两个 Web 界面：标准管理员界面，默认使用端口 80；垃圾邮件隔离区最终用户界面，默认使用端口 82。垃圾邮件隔离区 HTTPS 界面启用后，默认使用端口 83。

由于在配置每个 Web 界面时可以指定 HTTP 或 HTTPS （在安全管理设备上依次转至**管理设备 (Management Appliance) > 网络 (Network) > IP 接口 (IP Interfaces)**），如果在会话期间切换两者，系统可能要求您重新进行身份验证。例如，如果通过端口 80 中的 HTTP 访问 admin Web 界面，然后在同一浏览器中通过端口 83 的 HTTPS 访问垃圾邮件隔离区最终用户 Web 界面，在您想要返回 admin Web 界面时，系统会要求您重新进行身份验证。

备注　访问 GUI 时，请勿同时使用多个浏览器窗口或选项卡来更改安全管理设备，也不要使用并行 GUI 和 CLI 会话，否则将会导致意外行为，且不受支持。

备注　默认情况下，如果空闲时间超过 30 分钟或未注销就关闭浏览器，会话将超时。如果发生这种情况，您必须重新输入用户名和密码。要更改超时限制，请参阅配置 Web UI 会话超时 （第 13-21 页）。

访问 Web 界面

操作步骤

步骤 1　打开您的 Web 浏览器，在 “IP 地址 (IP address)” 文本字段键入 **192.168.42.42**。

步骤 2　输入以下默认值：

- 用户名：**admin**
- 密码：**ironport**

注　使用 Web 界面或命令行界面完成 “系统设置向导 (System Setup Wizard)” 后，此密码将无效。

访问命令行界面

在安全管理设备中，按照在所有思科内容安全设备上访问命令行界面 （或 CLI）的相同方式访问 CLI。但是，存在一些差异：

- *必须*通过 GUI 执行系统设置。
- 有些 CLI 命令在安全管理设备上不可用。有关不支持的命令的列表，请参阅思科内容安全设备的 CLI 参考指南。

对于生产部署，应使用 SSH 访问 CLI。使用标准 SSH 客户端访问端口 22 的设备。对于实验部署，还可以使用 telnet，但此协议未加密。

支持的语言

如有相应的许可证密钥， AsyncOS 可以下面任何语言显示 GUI 和 CLI：

- 英语
- 法语
- 西班牙语
- 德语
- 意大利语
- 韩语
- 日语
- 葡萄牙语 （巴西）
- 中文 （繁体和简体）
- 俄语

要选择 GUI 和默认报告语言，请执行以下任一操作：

- 设置语言首选项。请参阅设置首选项 （第 14-48 页）。
- 使用 GUI 窗口右上角的 “选项 (Options)” 菜单，选择会话语言。

（方法有效与否，取决于登录凭证身份验证所使用的方法。）

运行 “系统设置向导 (System Setup Wizard)”

AsyncOS 提供基于浏览器的系统设置向导，指导您执行系统配置过程。之后，您可能希望利用向导中没有的自定义配置选项。但是，初始设置*必须*使用向导，以确保配置完整。

安全管理设备仅支持通过 GUI 运行此向导。不支持通过命令行界面 (CLI) 进行系统设置。

- 准备工作 （第 2-7 页）
- 系统设置向导概述 （第 2-8 页）

准备工作

完成 “设置准备”部分 （第 2-3 页）中的所有任务。

警告 **“系统设置向导 (System Setup Wizard)”将完全重新配置设备。只有初始安装设备或希望完全覆盖现有配置时，才使用该向导。**

确保通过管理端口将安全管理设备连接到您的网络。

警告 **安全管理设备的管理端口出厂设置为默认 IP 地址：`192.168.42.42`。将安全管理设备连接到您的网络之前，请确保其他设备的 IP 地址与出厂默认设置没有冲突。**

备注　默认情况下，如果空闲时间超过 30 分钟或未注销就关闭浏览器，会话将超时。如果正在运行 “系统设置向导 (System Setup Wizard)” 时会话超时，您需要从头重新开始。

要更改会话超时限制，请参阅配置 Web UI 会话超时 （第 13-21 页）。

备注　默认情况下，如果空闲时间超过 30 分钟或未注销就关闭浏览器，会话将超时。如果发生这种情况，您必须重新输入用户名和密码。如果正在运行 “系统设置向导 (System Setup Wizard)” 时会话超时，您需要从头重新开始。要更改超时限制，请参阅配置 Web UI 会话超时 （第 13-21 页）。

系统设置向导概述

操作步骤

步骤 1　启动 “系统设置向导 (System Setup Wizard)”（第 2-8 页）

步骤 2　审核最终用户许可协议 （第 2-8 页）

步骤 3　配置系统设置 （第 2-9 页）

- 通知设置和自动支持
- 系统时间设置
- Admin 密码

步骤 4　配置网络设置 （第 2-9 页）

- 设备的主机名
- 设备的 IP 地址、网络掩码和网关
- 默认路由器和 DNS 设置

步骤 5　检查配置 （第 2-10 页）

继续向导页面，并在步骤 4 认真检查配置。您可以点击**上一步 (Previous)** 返回步骤。在该过程结束时，向导将提示您确认进行的更改。只有确认后，大多数更改才会生效。

步骤 6　继续执行后续步骤 （第 2-10 页）

启动 “系统设置向导 (System Setup Wizard)”

要启动该向导，请按 “访问 Web 界面”部分 （第 2-6 页）中所述登录到 GUI。首次登录到 GUI 时，默认显示 “系统设置向导 (System Setup Wizard)” 的初始页面。您也可以从 “系统管理 (System Administration)” 菜单 （“管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “系统设置向导 (System Setup Wizard)”）来访问系统设置向导。

审核最终用户许可协议

首先阅读许可协议。阅读并同意许可协议后，请选择表示您同意的复选框，然后点击**开始安装 (Begin Setup)** 继续。

配置系统设置

输入系统警报的邮件地址

如果系统中出现错误，需要您干预， AsyncOS 将通过电子邮件发送警报消息。输入警报发送到的邮件地址。

至少需要为系统警报添加一个邮件地址。多个地址之间用逗号分隔。初始输入的邮件地址将接收各种级别所有类型的警报。稍后可以自定义警报配置。有关详细信息，请参阅 “管理警报”部分（第 14-28 页）。

设置时间

设置安全管理设备中的时区，以便邮件信头和日志文件中的时间戳正确。使用下拉菜单查找您所在的时区，或通过 GMT 偏移时间来定义时区。

可以手动设置系统时钟时间，也可以使用网络时间协议 (NTP) 服务器将该时间与网络中的其他服务器或互联网同步。默认情况下，思科 NTP 服务器 (time.sco.cisco.com) 作为条目添加，用来同步内容安全设备中的时间。输入 NTP 服务器的主机名，然后点击**添加条目 (Add Entry)** 再配置一台 NTP 服务器。有关详细信息，请参阅 “配置系统时间”部分 （第 14-37 页）。

备注 收集报告数据时，安全管理设备将应用数据中的时间戳。按照 “配置系统时间”部分 （第 14-37 页）步骤中实施的配置设置应用时间戳。
有关安全管理设备如何收集数据的详细信息，请参阅 “安全设备如何为报告收集数据”部分 （第 3-2 页）。

设置密码

必须更改 AsyncOS admin 帐户的密码。将密码保存在安全的位置。对密码的更改将会立即生效。

备注 如果在重置密码后取消系统设置，密码更改不会撤消。

启用自动支持

“自动支持 (AutoSupport)”功能 （默认为启用）通知客户支持安全管理设备中存在的问题，以便他们可以提供最佳支持。有关详细信息，请参阅 “思科自动支持”部分 （第 14-30 页）。

配置网络设置

定义计算机的主机名，然后配置网关和 DNS 设置。

备注 确认是否已通过管理端口将安全管理设备连接到网络。

网络设置

输入安全管理设备的完全限定主机名。此名称应由网络管理员分配。

键入安全管理设备的 IP 地址。

输入网络中默认路由器 （网关）的网络掩码和 IP 地址。

然后，配置域名服务 (DNS) 设置。 AsyncOS 包含可直接查询互联网根服务器的高性能内部 DNS 解析器/缓存，或者系统可以使用您指定的 DNS 服务器。如果使用您自己的服务器，需要提供每个 DNS 服务器的 IP 地址。使用 “系统设置向导 (System Setup Wizard)”时，最多可以输入四个 DNS 服务器。

备注 您指定的 DNS 服务器的初始优先级为 0。有关详细信息，请参阅 “配置域名系统设置”部分（第 14-34 页）。

备注 设备需要访问运行的 DNS 服务器，以便对传入连接执行 DNS 查询。如果在设置设备时无法指定该设备可访问的运行的 DNS 服务器，可以选择 “使用互联网根 DNS 服务器 (Use Internet Root DNS Servers)”或临时指定管理接口的 IP 地址，以便完成 “系统设置向导 (System Setup Wizard)”。

检查配置

现在，“系统设置向导 (System Setup Wizard)”将显示您输入的设置信息摘要。如需进行任何更改，请点击页面底部的**上一步 (Previous)** 并编辑相关信息。

检查完信息后，点击**安装此配置 (Install This Configuration)**。然后点击出现的确认对话框中的**安装 (Install)**。

继续执行后续步骤

如果 “系统设置向导 (System Setup Wizard)”在安全管理设备中正确安装了配置，将显示**系统设置后续步骤 (System Setup Next Steps)** 页面。

点击 “系统设置后续步骤 (System Setup Next Steps)”页面中的任意链接，继续思科内容安全设备的配置。

在安装安全管理设备并运行 “系统设置向导 (System Setup Wizard)”后，可以修改设备中的其他设置及配置监控服务。

要简化配置和故障排除，我们建议您按照解决方案部署概述 （第 2-1 页）概括的流程执行操作。

关于添加托管设备

在配置每台设备的第一个集中服务时，需要向安全管理设备添加托管邮件和网络安全设备。

SMA 兼容性列表 （第 2-2 页）中显示了支持的邮件和网络安全设备。

添加远程设备时，安全管理设备会比较远程设备的产品名称和要添加的设备的类型。例如，使用 “添加 (Add Web Security appliance)”页面添加设备时，安全管理设备将检查远程设备的产品名称，以确保它是网络安全设备，而不是邮件安全设备。此外，安全管理设备还会检查远程设备中的监控服务，确保它们的配置正确且兼容。

“安全设备 (Security Appliances)”页面将显示已添加的托管设备。“建立连接？ (Connection Established?)”列显示监控服务连接的配置是否正确。

有关添加托管设备的说明，请参阅以下程序：

- 为每个托管邮件安全设备添加集中邮件报告服务 （第 4-3 页）
- 向每台托管邮件安全设备添加集中邮件跟踪服务 （第 6-3 页）
- 向每个托管邮件安全设备添加集中式垃圾邮件隔离区服务 （第 7-4 页）

- 向每个托管邮件安全设备添加集中策略、病毒和爆发隔离区服务 （第 8-4 页）
- 将集中 Web 报告服添加到每个托管网络安全设备 （第 5-3 页）
- 添加网络安全设备并将它们与主配置版本关联 （第 9-5 页）

编辑托管设备配置

操作步骤

步骤 1 在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 2 在 “安全设备 (Security Appliance)” 部分，点击要编辑的设备的名称。

步骤 3 对设备配置进行必要的更改。

例如，选中或清除监控服务的复选框、重新配置文件传输访问或更改 IP 地址。

注 更改托管设备的 IP 地址可能会导致出现许多问题。如果更改网络安全设备的 IP 地址，将会丢失设备的发布历史记录。如果当前针对预定发布作业选择了网络安全设备，还会出现发布错误。（不会影响已设置为使用所有分配的设备的预定发布作业。）如果更改邮件安全设备的 IP 地址，设备的跟踪可用性数据将会丢失。

步骤 4 点击**提交 (Submit)** 提交您在该页面的更改，然后点击**确认更改 (Commit Changes)** 确认您的更改。

从托管设备列表删除设备

准备工作

您可能需要禁用远程设备上启用的任何集中服务，才能从安全管理设备中删除该设备。例如，如果启用了 “集中策略、病毒和爆发隔离区 (Centralized Policy, Virus, and Outbreak Quarantine)” 服务，则必须首先在邮件安全设备上禁用该服务。请参阅邮件或网络安全设备文档。

操作步骤

步骤 1 在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 2 在 “安全设备 (Security Appliances)” 部分，点击要删除的托管设备行中的垃圾桶图标。

步骤 3 在确认对话框中，点击**删除**。

步骤 4 提交并确认更改。

“安全设备 (Security Appliances)”页面

- 关于添加托管设备 （第 2-10 页）
- 编辑托管设备配置 （第 2-11 页）
- 从托管设备列表删除设备 （第 2-11 页）
- 查看托管设备的配置状态 （第 10-4 页）
- 指定处理放行邮件的备用设备 （第 8-7 页）

在安全管理设备上配置服务

邮件安全服务：

- 第 4 章 “使用集中邮件安全报告”
- 第 6 章 “跟踪邮件消息”
- 第 7 章 “垃圾邮件隔离区”
- 第 8 章 “集中策略、病毒和爆发隔离区”

网络安全服务：

- 第 5 章 “使用集中 Web 报告和跟踪”
- 第 9 章 “管理网络安全设备”

确认和放弃配置更改

在思科内容安全设备 GUI 中更改大多数配置后，必须明确确认更改。

图 2-2　“确认更改 (Commit Changes)”按钮

目标	操作
确认所有待定更改	点击窗口右上角的橙色**确认更改 (Commit Changes)** 按钮。添加更改说明，然后点击确认。 如果尚未进行任何需要确认的更改，则显示灰色的**无待定更改 (No Changes Pending)**，而不是**确认更改 (Commit Changes)**。
放弃所有待定更改	点击窗口右上角的橙色**确认更改 (Commit Changes)** 按钮，然后点击**放弃更改 (Abandon Changes)**。

相关主题

- 回滚至先前确认的配置 （第 14-42 页）

使用报告

除非另有说明，否则本章中的信息适用于有关您的思科内容安全管理设备的邮件和 Web 报告。

查看报告数据的方式

表 3-1　　查看报告数据的方式

目标	请参阅
查看和自定义基于 Web 的交互式报告页面	• 自定义报告数据的视图 （第 3-3 页） • 第 4 章 “使用集中邮件安全报告” • 第 5 章 “使用集中 Web 报告和跟踪”
自动生成循环 PDF 或 CSV 报告	• 计划邮件报告 （第 4-35 页） • 安排 Web 报告 （第 5-29 页）
按需生成 PDF 或 CSV 报告	• 按需生成邮件报告 （第 4-37 页） • 按需生成 Web 报告 （第 5-33 页）
将原始数据导出为 CSV （逗号分隔值）文件	• 打印和导出报告和跟踪数据 （第 3-9 页） • 将报告数据导出为逗号分隔值 (CSV) 文件 （第 3-10 页）
生成 PDF 格式的报告数据	打印和导出报告和跟踪数据 （第 3-9 页）

表 3-1　查看报告数据的方式 （续）

目标	请参阅
通过邮件将报告信息发送给自己和他人	• 按需生成邮件报告 （第 4-37 页） • 计划邮件报告 （第 4-35 页） • 按需生成 Web 报告 （第 5-33 页） • 安排 Web 报告 （第 5-29 页）
查看计划报告和按需报告的存档副本，直到将这些副本从系统中清除	查看和管理存档的 Web 报告 （第 5-34 页）
查找有关特定事务的信息	• 查看包含在报告中的消息或事务的详细信息 （第 3-7 页）

备注　有关日志记录和报告之间的差异，请参阅日志记录与报告 （第 15-1 页）。

安全设备如何为报告收集数据

安全管理设备大约每隔 15 分钟便会从所有托管设备中提取所有报告的数据，并聚合来自这些设备的数据。将特定消息包含在安全管理设备的报告数据中可能需要一点时间，具体取决于您的设备。有关您的数据的信息，请检查**系统状态 (System Status)** 页面。

备注　在收集报告数据时，安全管理设备会应用您在安全管理设备上配置时间设置时所设置信息中的时间戳。有关在安全管理设备上设置时间的信息，请参阅 “配置系统时间”部分 （第 14-37 页）。

数据包括涉及 IPv4 和 IPv6 的事务。

如何存储报告数据

所有设备都会存储报告数据。表 3-2 显示了每个设备存储数据的时间段。

表 3-2　邮件和网络安全设备中的报告数据存储

	分钟	每小时	每天	每星期	每月	每年
邮件安全设备或网络安全设备上的本地报告	•	•	•	•	•	
邮件安全设备或网络安全设备上的集中报告	•	•	•	•		
安全管理设备		•	•	•	•	•

关于报告和升级

新的报告功能可能不适用于在升级之前进行的事务，因为可能没有为这些事务保留所需的数据。有关与报告数据和升级相关的可能限制，请参阅与您的版本对应的版本说明。

自定义报告数据的视图

在 Web 界面中查看报告数据时，可以自定义视图。

目标	操作
按设备或报告组查看数据	请参阅查看设备或报告组的报告数据 （第 3-3 页）。
指定时间范围	请参阅选择报告的时间范围 （第 3-4 页）。
（对于 Web 报告）选择用于绘制图表的数据	请参阅 （仅 Web 报告）选择用于绘制图表的数据 （第 3-5 页）。
自定义表格	请参阅第 3-6 页的 “自定义报告页面中的表格”。
搜索特定信息或数据子集以进行查看	• 对于邮件报告，请参阅搜索和交互式邮件报告页面 （第 4-5 页）。 • 对于 Web 报告，请查找大多数表格底部的 “查找 (Find)”或 “过滤 (Filter)”选项。 • 有些表格包含指向聚合数据详细信息的链接 （蓝色文本）。
指定报告相关的首选项	请参阅设置首选项 （第 14-48 页）。
仅使用所需的图表和表格创建自定义报告	请参阅自定义报告 （第 3-6 页）。

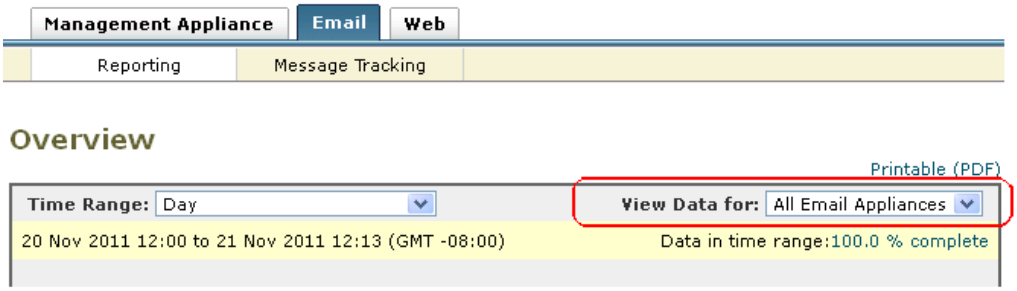
备注　并非所有自定义功能均适用于每个报告。

查看设备或报告组的报告数据

对于邮件和 Web 概述报告，以及邮件的系统容量报告，可查看来自所有设备的数据，或来自任何一个集中托管设备的数据。

对于邮件报告，如果按照创建邮件报告组 （第 4-3 页）中所述创建了邮件安全设备组，则可以查看每个报告组的数据。

要指定视图，请从受支持页面上的**查看以下项的数据 (View Data for)** 列表中选择设备或组。



如果您正在查看最近将另一个安全管理设备中的数据备份到的安全管理设备上的报告数据，则必须首先在 “管理设备 (Management Appliance)” > “集中服务 (Centralized Services)” > “安全设备 (Security Appliances)” 中添加 （但不要连接到）每个设备。

选择报告的时间范围

预定义的报告页面支持选择要包括的数据的时间范围。所选择的时间范围用于所有报告页面，直到在 “时间范围 (Time Ranges)” 菜单中选择其他值。

可用时间范围选项因设备以及有关安全管理设备的邮件和 Web 报告而异：

表 3-3　　报告的时间范围选项

选项	说明	SMA 邮件报告	ESA	SMA Web 报告	WSA
以小时计算	前 60 分钟，加上另外长达 5 分钟		•		•
天	前 24 小时	•	•	•	•
星期	前 7 天，包括当日已逝去的小时数	•	•	•	•
30 天	前 30 天，包括当日已逝去的小时数	•	•	•	•
90 天	前 90 天，包括当日已逝去的小时数	•	•	•	
年份	前 12 个月加上当前已逝去的天数	•			
过去	上一天的 24 小时 （00:00 到 23:59），使用设备中定义的时区	•	•	•	•
上一日历月	该月第一天的 00:00 到该月最后一天的 23:59。	•	•	•	
自定义范围	您指定的时间范围。 选择此选项可选择开始、结束日期和时间。	•	•	•	•

备注　报告页面上的时间范围以格林威治标准时间 (GMT) 时差显示。例如，太平洋时间是 GMT + 7 小时 (GMT + 07:00)。

备注　所有报告均基于系统配置的时区显示日期和时间信息，并且以格林威治标准时间 (GMT) 时差显示。但是，数据导出会显示 GMT 时间，以适应采用全球多个时区的多个系统。

提示　可以指定每次登录时将始终显示的默认时间范围。有关信息，请参阅设置首选项 （第 14-48 页）。

（仅 Web 报告）选择用于绘制图表的数据

每个 Web 报告页面上的默认图表会显示通常引用的数据，但是，您可以选择用其他数据绘制图表。如果页面有多个图表，则可以更改每个图表。

通常，图表选项与报告中表格的列相同。但是，某些列无法用于绘制图表。

图表反映表格列中的所有可用数据，无论选择在关联的表格中显示的项目 （行）数量是多少都是如此。

操作步骤

步骤 1　点击图表下的**图表选项 (Chart Options)** 链接。

步骤 2　选择要显示的数据。

步骤 3　点击 **Done**。

自定义报告页面中的表格

表 3-4　自定义 Web 报告页面中的表格

目标	操作	更多信息
• 显示其他列 • 隐藏可见列 • 确定表格的可用列	点击表格下面的**列 (Columns)** 链接，选择要显示的列，然后点击**完成 (Done)**。	对于大多数表格，某些列默认情况下会隐藏。 每个报告页面会提供不同的列。 另请参阅邮件报告页面的表格列说明 （第 4-8 页）。
重新排序表格列	将列标题拖动到所需的新位置。	—
按照所选的标题排序表格	点击列标题。	—
显示更多或更少的数据行	从表格右上方的**显示的项目 (Items Displayed)** 下拉列表中，选择要显示的行。	对于 Web 报告，您还可以为默认要显示的行设置首选项；请参阅设置首选项 （第 14-48 页）。
查看有关表格条目的详细信息 （如果可用）	点击表格中的蓝色条目。	另请参阅查看包含在报告中的消息或事务的详细信息 （第 3-7 页）。
将数据池缩小到特定子集	在表格下方的过滤器设置中选择或输入值 （如果可用）。	对于 Web 报告，在每个报告页面说明中会介绍可用的过滤器。请参阅 Web 报告页面说明 （第 5-5 页）。

自定义报告

您可以创建自定义邮件安全报告页面和自定义 Web 安全报告页面，方法是组合现有报告页面中的图表 （图形）和表格。

目标	操作
将模块添加到自定义报告页面	请参阅： • 无法添加到自定义报告的模块 （第 3-6 页） • 创建自定义报告页面 （第 3-7 页）
查看自定义报告页面	1. 选择**邮件或 Web (Email or Web) > 报告 (Reporting) > 我的报告 (My Reports)**。 2. 选择要查看的时间范围。所选时间范围会应用到所有报告，包括 “我的报告 (My Reports)”页面中的所有模块。 新添加的模块显示在自定义报告的顶部。
重新排列自定义报告页面中的模块	将模块拖放到所需的位置。
从您的自定义报告中删除模块	点击模块右上角的 [X]。
生成自定义报告的 PDF 或 CSV 版本	请参阅： • 按需生成邮件报告 （第 4-37 页） • 按需生成 Web 报告 （第 5-33 页）
定期生成自定义报告的 PDF 或 CSV 版本	请参阅： • 计划邮件报告 （第 4-35 页） • 安排 Web 报告 （第 5-29 页）

无法添加到自定义报告的模块

- 位于**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)** 页面上的所有模块
- 位于 **Web > 报告 (Reporting) > 数据可用性 (Data Availability)** 页面上的所有模块
- 位于**邮件 (Email) > 报告 (Reporting) > 报告数据可用性 (Reporting Data Availability)** 页面上的所有模块
- 位于**邮件 (Email) > 邮件跟踪 (Message Tracking) > 邮件跟踪数据可用性 (Message Tracking Data Availability)** 页面上的所有模块
- 以下按域的模块来自 “发件人简档 (Sender Profile)”详细信息报告页面：**SenderBase 中的当前信息 (Current Information from SenderBase)**、**发件人组信息 (Sender Group Information)** 和**网络信息 (Network Information)**
- “爆发过滤器 (Outbreak Filters)”报告页面上的**过去一年病毒爆发摘要 (Past Year Virus Outbreak Summary)** 图表和**过去一年病毒爆发 (Past Year Virus Outbreaks)** 表格
- 搜索结果，包括网络跟踪搜索结果

创建自定义报告页面

准备工作

- 确保要添加的模块可以添加。请参阅无法添加到自定义报告的模块 （第 3-6 页）。
- 通过点击模块右上角的 **[X]** 删除不需要的任何默认模块。

操作步骤

步骤 1　使用以下方法之一将模块添加到自定义报告页面：

注　某些模块仅在使用这些方法中的一种时可用。如果无法使用一种方法添加模块，请尝试另一种方法。

- 导航至具有要添加的模块的 “邮件 (Email)”或 Web 选项卡下的报告页面，然后点击模块顶部的 **[+]** 按钮。
- 转到**邮件或 Web (Email or Web) > 报告 (Reporting) > 我的报告 (My Reports)**，点击 **[+]** 按钮，然后选择要添加的报告模块。

您只能将每个模块添加一次；如果已经将特定模块添加到报告，则用于添加模块的选项将不可用。

步骤 2　如果添加已自定义的一个模块 （例如，通过添加、删除或重新排序列，或者通过在图表中显示非默认数据），则在 “我的报告 (My Reports)”页面上自定义模块。

添加的模块使用默认设置。原始模块的时间范围无法保留。

步骤 3　如果添加包含单独图例的图表 （例如，“概述 (Overview)”页面中的图形），请单独添加图例。如果需要，请将其拖放至所描述数据旁边的位置。

查看包含在报告中的消息或事务的详细信息

操作步骤

步骤 1　点击报告页面上某个表格中的任何蓝色编号。

（并非所有的表格都有这些链接。）

包含在该编号中的消息或事务分别以消息跟踪或 Web 跟踪的形式显示。

步骤 2　向下滚动以查看消息或事务的列表。

相关主题

- 第 6 章 “跟踪邮件消息”
- 网络跟踪 （第 5-34 页）

提高邮件报告的性能

如果聚合报告的性能由于一个月中存在大量独特的条目而降低，则使用报告过滤器来限制对涵盖上一年的报告 （去年报告）进行的数据聚合。这些过滤器可以限制报告中的详细个人 IP、域或用户数据。概述报告和摘要信息仍可用于所有报告。

可以使用 CLI 中的 **reportingconfig -> 过滤器 (filters)** 菜单来启用一个或多个报告过滤器。更改必须提交才能生效。

- **IP 连接级别详细信息**。启用此过滤器可阻止安全管理设备记录有关各个 IP 地址的信息。此过滤器适合由于攻击需要处理大量传入 IP 地址的系统。

  此过滤器会影响以下去年的报告：

  - 传入邮件的发件人简档
  - 传入邮件的 IP 地址
  - 传出发件人的 IP 地址
- **用户详细信息**。启用此过滤器可阻止安全管理设备记录有关发送和接收邮件的个人用户以及应用于用户邮件的内容过滤器的信息。此过滤器适合为数以百万计的内部用户处理邮件的设备，或者不能验证收件人地址的系统。

  此过滤器会影响以下去年的报告：

  - 内部用户
  - 内部用户详细信息
  - 传出发件人的 IP 地址
  - 内容过滤器
- **邮件流量详细信息**。启用此过滤器可阻止安全管理设备记录有关设备监控的各个域和网络的信息。在数以千万计的域中测量有效的传入或传出域的数量时，此过滤器非常合适。

  此过滤器会影响以下去年的报告：

  - 传入邮件的域
  - 传入邮件的发件人简档
  - 内部用户详细信息
  - 传出发件人的域

备注　要查看上一小时的最新报告数据，必须登录到各个设备并查看其中的数据。

打印和导出报告和跟踪数据

表 3-5　打印和导出报告数据

要获取此内容	PDF	CSV	操作	备注
PDF 格式的交互式报告页面	•		点击交互式报告页面右上角的**可打印 (PDF) (Printable (PDF))** 链接。	PDF 会反映当前正在查看的自定义内容。 PDF 经过格式化以便于打印。
PDF 格式的报告数据	•		创建一个计划报告或按需报告。请参阅： • 按需生成邮件报告（第 4-37 页） • 计划邮件报告（第 4-35 页） • 按需生成 Web 报告（第 5-33 页） • 安排 Web 报告（第 5-29 页）	—
原始数据		•	点击图表或表格下的**导出 (Export)** 链接。	CSV 文件包含所有适用的数据，不只是图表或表格中显示的数据。
另请参阅将报告数据导出为逗号分隔值 (CSV) 文件（第 3-10 页）		•	创建一个计划报告或按需报告。请参阅： • 按需生成邮件报告（第 4-37 页） • 计划邮件报告（第 4-35 页） • 按需生成 Web 报告（第 5-33 页） • 安排 Web 报告（第 5-29 页）	每个 CSV 文件都可包含多达 100 个行。 如果某个报告包含多个表格，则会为每个表格创建单独的 CSV 文件。 一些扩展报告无法使用 CSV 格式。
采用不同语言的报告	•		在计划报告或按需创建报告时，选择所需的报告语言。	要在 Windows 计算机上生成中文、日语或韩语 PDF，还必须从 Adobe.com 下载合适的字体包并将其安装在本地计算机上。

表 3-5　打印和导出报告数据 （续）

要获取此内容	PDF	CSV	操作	备注
（网络安全）报告数据的自定义子集，例如特定用户的数据。	•	•	在 Web 跟踪中，执行搜索，然后点击 “Web (Web Tracking)”页面上的 “可打印的下载 (Printable Download)”链接。选择 PDF 或 CSV 格式。	PDF 可能不包括网页上的所有可用信息。具体而言， PDF 包括： • 最多 1,000 个事务。 • 如果显示详细信息，则最多显示 100 个相关的事务。 • 每个相关事务最多 3000 个字符。 CSV 文件包括符合搜索条件的所有原始数据。
（邮件安全）自定义数据子集，例如特定用户的数据。		•	在邮件跟踪中，执行搜索，然后点击搜索结果上方的 “导出 (Export)”或 “全部导出 (Export All)”链接。	“导出 (Export)”链接会下载包含显示的搜索结果的 CSV 文件，并且遵循在搜索条件中指定的限制。 “全部导出 (Export All)”链接会下载一个 CSV 文件，其中包含符合搜索条件的多达 50,000 个邮件。 提示：如果需要导出 50,000 多个邮件，请为更短的一组时间范围执行一系列导出。

将报告数据导出为逗号分隔值 (CSV) 文件

可以将原始数据导出为逗号分隔值 (CSV) 文件，该文件可使用 Microsoft Excel 等数据库应用进行访问和操纵。有关导出数据的不同方式，请参阅打印和导出报告和跟踪数据 （第 3-9 页）。

由于 CSV 导出仅包括原始数据，因此从一个基于 Web 的报告页面导出的数据可能不包括计算的数据，例如百分比，即使这些数据显示在基于 Web 的报告中也是如此。

对于邮件跟踪和报告数据，导出的 CSV 数据将显示 GMT 中的所有数据，不管安全管理设备中的设置如何。这简化了独立于设备使用数据，特别是在多个时区中引用设备的数据时。

以下示例是防恶意软件类别报告原始数据导出中的一个条目，其中太平洋夏令时 (PDT) 显示为 GMT - 7 小时：

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name, Transactions Monitored,
Transactions Blocked, Transactions Detected
1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525,
2100, 2625
```

表 3-6　查看原始数据条目

类别标题	Value	说明
开始时间标记	1159772400.0	以系统纪元以来的秒数表示的查询开始时间。
结束时间标记	1159858799.0	以系统纪元以来的秒数表示的查询结束时间。
开始日期	2006-10-02 07:00 GMT	查询开始的日期。
结束日期	2006/10/3 6:59 GMT	查询结束的日期。
名称	广告程序	恶意软件类别的名称。
受控事务数	525	监控的事务数。

表 3-6　查看原始数据条目 （续）

类别标题	Value	说明
受阻事务数	2100	阻止的事务数。
检测到的事务数	2625	事务总数： 检测到的事务数 + 阻止的事务数。

备注　各种类型的报告具有不同的类别标题。

如果导出本地化的 CSV 数据，则标题可能无法在某些浏览器中正确呈现。出现该情况是因为某些浏览器可能没有为本地化文本使用正确的字符集。要解决该问题，可以将文件保存到本地计算机，然后在任何 Web 浏览器中使用**文件 (File) > 打开 (Open)** 打开该文件。当打开该文件时，选择字符集以显示本地化文本。

报告和跟踪中的子域与二级域

在报告和跟踪搜索中，对二级域 （在 http://george.surbl.org/two-level-tlds 中列出的地区域）的处理方式与子域不同，即使两种域类型可能看起来相同。例如：

- 报告不会包含两级域 （例如 `co.uk`）的结果，但是会包含 `foo.co.uk` 的结果。报告包含主公司域下的子域，例如 `cisco.com`。
- 地区域 `co.uk` 的跟踪搜索结果不会包含域，例如 `foo.co.uk`，而 `cisco.com` 的搜索结果将包含子域，例如 `subdomain.cisco.com`。

对所有报告进行故障排除

- 无法查看备份安全管理设备的报告数据 （第 3-11 页）
- 已禁用报告 （第 3-12 页）

另请参阅：

- 邮件报告故障排除 （第 4-39 页）
- 故障排除 Web 报告和跟踪 （第 5-41 页）

无法查看备份安全管理设备的报告数据

问题：您无法选择要查看其报告数据的单个邮件安全设备或网络安全设备。**查看以下项的数据 (View Data for)** 选项不会显示在报告页面上。

解决方法：在“管理设备 (Management Appliance)”>“集中服务 (Centralized Services)”>“安全设备 (Security Appliances)”中添加 （但不要连接到）每个集中管理的设备。请参阅查看设备或报告组的报告数据 （第 3-3 页）。

另请参阅备份期间服务的可用性 （第 14-8 页）。

已禁用报告

问题：取消备份期间会禁用报告。

解决方法：报告功能将在备份完成之后恢复。

邮件和 Web 报告

有关邮件报告特定的信息，请参阅第 4 章 “使用集中邮件安全报告”。

有关 Web 报告特定的信息，请参阅第 5 章 “使用集中 Web 报告和跟踪”。

使用集中邮件安全报告

集中邮件报告概述

思科内容安全管理设备显示来自单个或多个邮件安全设备的聚合信息，以便监控邮件流量模式和安全风险。可以实时运行报告来查看特定时间段内系统活动的交互显示，也可以安排并定期运行报告。此外，报告功能还可将原始数据导出到文件。

此功能将集中显示邮件安全设备的 “监控 (Monitor)” 菜单下列出的报告。

集中邮件报告功能不仅可以生成高级报告，以便了解网络上的状况，而且还可用于深入了解特定域、用户或类别的流量详细信息。

可以通过集中跟踪功能跟踪经过多个邮件安全设备的邮件。

备注 邮件安全设备仅在使用本地报告时才存储数据。如果为邮件安全设备启用了集中报告，则邮件安全设备不会保留任何报告数据 （系统容量和系统状态除外）。如果未启用集中邮件报告，则仅会生成系统状态和系统容量报告。

有关过渡到集中报告期间或之后的时间报告数据可用性的详细信息，请参阅邮件安全设备的文档或在线帮助的 “集中报告模式” 部分。

设置集中邮件报告

要设置集中邮件报告，请按顺序完成以下步骤：

- 在安全管理设备上启用集中邮件报告 （第 4-2 页）
- 为每个托管邮件安全设备添加集中邮件报告服务 （第 4-3 页）
- 创建邮件报告组 （第 4-3 页）
- 在邮件安全设备上启用集中邮件报告 （第 4-4 页）

备注 如果报告和跟踪没有一致，同时启用且不能正常运行，或者没有一致且同时地在每个邮件安全设备上进行集中或本地存储，则深入了解报告时获得的邮件跟踪结果与预期结果不匹配。这是因为仅当启用了各个功能 （报告、跟踪）时才会捕获该功能的数据。

在安全管理设备上启用集中邮件报告

准备工作

- 在启用集中报告之前，应配置所有邮件安全设备并确保其按预期工作。
- 启用集中邮件报告之前，请确保为该服务分配了足够的磁盘空间。请参阅 “管理磁盘空间”部分 （第 14-45 页）。

操作步骤

步骤 1 在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 邮件 (Email) > 集中报告 (Centralized Reporting)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 如果是在运行系统设置向导后首次启用集中邮件报告，请查看最终用户许可协议，然后点击**接受 (Accept)**。

步骤 4 提交并确认更改。

注 如果已在设备上启用邮件报告，并且没有为此操作分配磁盘空间，则集中邮件报告无法工作，直到为其分配磁盘空间为止。只要为邮件报告和跟踪设置的配额大于当前使用的磁盘空间，就不会丢失任何报告和跟踪数据。有关详细信息，请参阅 “管理磁盘空间”部分 （第 14-45 页）。

为每个托管邮件安全设备添加集中邮件报告服务

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。

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 2　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**集中报告 (Centralized Reporting)** 服务。

步骤 3　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，键入设备名称和安全管理设备管理接口的 IP 地址。

备注　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. 集中报告服务已预先选中。

d. 点击**建立连接 (Establish Connection)**。

e. 为要托管的设备管理员帐户输入用户名和密码，然后点击**建立连接 (Establish Connection)**。

注　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。

g. 点击**测试连接**。

h. 阅读表格上方的测试结果。

步骤 4　点击 **Submit**。

步骤 5　为要启用集中报告的每个邮件安全设备重复执行此程序。

步骤 6　确认更改。

创建邮件报告组

可以从安全管理设备创建要查看其报告数据的邮件安全设备组。

一个组可以包含一个或多个设备，而一个设备可以属于多个组。

准备工作

请确保为每个设备启用集中报告。请参阅为每个托管邮件安全设备添加集中邮件报告服务（第 4-3 页）。

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 集中报告 (Centralized Reporting)**。

步骤 2　点击 **Add Group**。

步骤 3　为组输入一个唯一的名称。

邮件安全设备列表会显示您添加到安全管理设备的邮件安全设备。选择要添加到组的设备。

可以添加的组的最大数量小于或等于可以连接的邮件设备的最大数量。

注　如果将邮件安全设备添加到了安全管理设备，但该设备并未显示在列表中，则编辑邮件安全设备的配置，以便安全管理设备从其收集报告数据。

步骤 4　点击**添加 (Add)** 将设备添加到 “组成员 (Group Members)”列表。

步骤 5　提交并确认更改。

在邮件安全设备上启用集中邮件报告

必须在每个托管的邮件安全设备上启用集中邮件报告。

有关说明，请参阅邮件安全设备的文档或在线帮助的 “配置邮件安全设备以使用集中报告”部分。

处理邮件报告数据

- 有关访问和查看报告数据的选项，请参阅 “查看报告数据的方式”部分 （第 3-1 页）。
- 要自定义报告数据的视图，请参阅自定义报告数据的视图 （第 3-3 页）
- 要搜索数据内的特定信息，请参阅搜索和交互式邮件报告页面 （第 4-5 页）。
- 要打印或导出报告信息，请参阅打印和导出报告和跟踪数据 （第 3-9 页）
- 要了解各种交互式报告页面，请参阅了解邮件报告页面 （第 4-5 页）。
- 要按需生成报告，请参阅按需生成邮件报告 （第 4-37 页）。
- 要将报告计划为按照指定的间隔和时间自动运行，请参阅计划邮件报告 （第 4-35 页）。
- 要查看存档的按需和计划报告，请参阅查看和管理存档的邮件报告 （第 4-38 页）。
- 有关背景信息，请参阅安全设备如何为报告收集数据 （第 3-2 页）。
- 要在处理大量数据时提高性能，请参阅 “提高邮件报告的性能”部分 （第 3-8 页）。
- 要获取有关在图表或表格中显示为蓝色链接的实体或编号的详细信息，请点击该实体或编号。

  例如，如果权限允许，可以使用此功能查看有关违反内容过滤或防数据丢失策略的邮件的详细信息。此操作将会在邮件跟踪中执行相关搜索。向下滚动，以查看搜索结果。

搜索和交互式邮件报告页面

许多交互式邮件报告页面的底部都有一个**搜索: (Search For:)** 下拉菜单。

可以从下拉菜单中搜索多种类型的条件，包括：

- IP 地址
- 域
- 网络所有者
- 内部用户
- 目标域
- 内部发件人域
- 内部发件人 IP 地址
- 传入 TLS 域
- 外发 TLS 域

对于大多数搜索，需要选择是完全匹配搜索文本还是仅查找以所输入文字开头的项目 （例如，以“ex”开头将匹配 “example@example.com”）。

对于 IPv4 搜索，始终会将输入的文本解释为最多四个 IP 八位组 （采用点分十进制格式）的开头。例如，输入 “17”将会在 17.0.0.0 至 17.255.255.255 的范围内搜索，因此 17.0.0.1 匹配搜索结果，而 172.0.0.1 不匹配。对于完全匹配搜索，需要输入所有四个八位组。 IP 地址搜索还支持无类域间路由 (CIDR) 格式 (17.16.0.0/12)。

对于 IPv6 搜索，可以使用下列所示格式输入地址：

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

了解邮件报告页面

备注 此列表显示邮件安全设备的 AsyncOS 最新支持版本中可用的报告。如果您的邮件安全设备运行的是早期版本的 AsyncOS，并非上述所有报告均可用。

表 4-1　邮件报告选项卡选项

邮件报告菜单	操作
邮件报告概述页面	“概述” (Overview) 页面提供您的邮件安全设备上的活动的概要。它包括传入和传出邮件的图和摘要表。 有关详细信息，请参阅“邮件报告概述页面”部分（第 4-9 页）。
传入邮件页面	“传入邮件” (Incoming Mail) 页面为连接到您的托管邮件安全设备的所有远程主机提供实时信息的交互报告。您可以收集有关发送邮件到您的系统的 IP 地址、域和网络所有者（组织）的信息。 有关详细信息，请参阅“传入邮件页面”部分 （第 4-12 页）。

表 4-1　邮件报告选项卡选项 （续）

邮件报告菜单	操作
“发件人组 (Sender Groups)”报告页面	“发件人组 (Sender Groups)”报告页面按发件人组和邮件流量策略操作提供连接摘要，从而便于查看 SMTP 连接和邮件流量策略趋势。 有关详细信息，请参阅 “传入邮件页面”部分 （第 4-12 页）。
“外发目标 (Outgoing Destinations)”页面	“外发目标 (Outgoing Destinations)”页面提供有关贵组织将邮件发送到的目标域的信息。页面顶部包含一些图表，这些图表描述按外发威胁邮件排名靠前的目标以及按外发正常邮件排名靠前的目标。页面底部显示一个图表，其包含按收件人总数 （默认设置）排序的列。 有关详细信息，请参阅 “外发目标 (Outgoing Destinations)”页面部分 （第 4-16 页）。
“外发邮件发件人 (Outgoing Senders)”页面	“外发发件人 (Outgoing Senders)”页面提供有关正从网络内的 IP 地址和域发送的邮件数量和类型的信息。 有关详细信息，请参阅 “外发邮件发件人 (Outgoing Senders)”页面部分 （第 4-17 页）。
内部用户页面	“内部用户 (Internal Users)”页面*按邮件地址*提供内部用户收发的邮件相关信息。单一用户可以有多个邮件地址。这些邮件地址在报告中不会合并。 有关详细信息，请参阅 “内部用户页面”部分 （第 4-18 页）。
DLP 事件	“DLP 事件摘要 (DLP Incident Summary)”页面显示外发邮件中发生的防数据丢失 (DLP) 策略违规事件的相关信息。 有关详细信息，请参阅 “DLP 事件”部分 （第 4-20 页）。
邮件过滤器	“邮件过滤器 (Message Filters)”页面显示传入邮件和外发邮件的排名靠前的邮件过滤器匹配项 （匹配邮件数量最多的邮件过滤器）的相关信息。
大量邮件	“大量邮件 (High Volume Mail)”页面确定涉及来自单个发件人或者在活动的一小时内具有相同主题的大量邮件的攻击。 有关详细信息，请参阅 “大量邮件”部分 （第 4-21 页）。
内容过滤器页面	“内容过滤器 (Content Filters)”页面显示排名靠前的传入和外发内容过滤器匹配项 （匹配邮件数量最多的内容过滤器）。该页面还以条形图和列表形式显示数据。使用 “内容过滤器 (Content Filters)”页面，可以按内容过滤器或用户查看企业策略。 有关详细信息，请参阅 “内容过滤器页面”部分（第 4-22 页）。
DMARC 验证	“DMARC 验证 (DMARC Verification)”页面显示未通过基于域的邮件认证、报告和一致性 (DMARC) 验证的排名靠前的收件人域，以及针对来自每个域的传入邮件所采取的措施摘要。 有关详细信息，请参阅 “DMARC 验证”部分 （第 4-22 页）。

表 4-1　邮件报告选项卡选项 （续）

邮件报告菜单	操作
“病毒类型 (Virus Types)”页面	“病毒类型 (Virus Types)”页面提供发送至网络以及从网络发出的病毒的概述。“病毒类型 (Virus Types)”页面显示已由运行于邮件安全设备之上的病毒扫描引擎检测到并且显示在安全管理设备上的病毒。使用此报告针对特定病毒采取相应措施。 有关详细信息，请参阅 “病毒类型 (Virus Types)”页面部分 （第 4-23 页）。
URL 过滤页面	使用此页面可以查看邮件中出现最频繁的 URL 类别、垃圾邮件中最常见的 URL 以及邮件中可见的恶意和可疑 URL 的数量。 有关详细信息，请参阅 “URL 过滤页面”部分 （第 4-23 页）。
高级恶意软件保护 （文件信誉和文件分析）报告页面	有三个报告页面会显示文件信誉和分析数据。 有关详细信息，请参阅 “高级恶意软件保护 （文件信誉和文件分析）报告页面”部分 （第 4-24 页）。
“TLS 连接 (TLS Connections)”页面	“TLS 连接 (TLS Connections)”页面显示所收发邮件的 TLS 连接的整体使用情况。该报告还显示使用 TLS 连接发送邮件的每个域的详细信息。 有关详细信息，请参阅 “TLS 连接 (TLS Connections)”页面部分 （第 4-25 页）。
入站 SMTP 身份验证页面	“入站 SMTP 身份验证 (Inbound SMTP Authentication)”页面显示如何使用客户端证书和 SMTP AUTH 命令对邮件安全设备与用户的邮件客户端之间的 SMTP 会话进行验证。 有关详细信息，请参阅 “入站 SMTP 身份验证页面”部分 （第 4-26 页）。
爆发过滤器页面	“爆发过滤器 (Outbreak Filters)”页面显示最近的爆发以及爆发过滤器隔离的邮件的相关信息。使用此页面可以监控对病毒攻击的防御。 有关详细信息，请参阅 “爆发过滤器页面”部分 （第 4-27 页）。
速率限制页面	“速率限制 (Rate Limits)”页面显示超出为每个邮件发件人设置的收件人数量阈值的发件人 （基于 MAIL-FROM 地址）。 有关详细信息，请参阅 “速率限制页面”部分 （第 4-27 页）。
系统容量页面	可用于查看将报告数据发送到安全管理设备的总体工作负载。 有关详细信息，请参阅 “系统容量页面”部分 （第 4-29 页）。
“报告数据可用性 (Reporting Data Availability)”页面	可用于概括了解报告数据对每个设备上的安全管理设备的影响。有关详细信息，请参阅 “报告数据可用性 (Reporting Data Availability)”页面部分 （第 4-31 页）。
计划邮件报告	可用于安排指定时间范围的报告。有关详细信息，请参阅 “计划邮件报告”部分 （第 4-35 页）。
查看和管理存档的邮件报告	可用于查看和管理存档的报告。有关详细信息，请参阅 “查看和管理存档的邮件报告”部分 （第 4-38 页）。 还可用于生成按需报告。请参阅 “按需生成邮件报告”部分 （第 4-37 页）。

邮件报告页面的表格列说明

表 4-2　邮件报告页面的表格列说明

列名	说明
传入邮件的详细信息	
被拒绝的连接	HAT 策略阻止的所有连接。当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接的计数。
接受的连接	接受的所有连接。
尝试的总数	所有被接受和阻止的连接尝试。
由收件人控制拒绝	此为“由信誉过滤拦截 (Stopped by Reputation Filtering)”的一部分，表示由于超出下列任何 HAT 限制而拦截的收件人邮件的数量：每小时的最大收件人数、每封邮件的最大收件人数或每个连接的最大邮件数。此值加上与被拒绝或被 TCP 拒绝的收件人邮件估算值就得到了“由信誉过滤拦截 (Stopped by Reputation Filtering)”的值。
SenderBase 声誉过滤 IP 层拒绝的	“由信誉过滤拦截 (Stopped by Reputation Filtering)”值的计算取决于多种因素： • 此发件人的“受限制”邮件数量 • 被拒绝或被 TCP 拒绝的连接数量 （可能是部分计数） • 每个连接的邮件数量的保守倍数 当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接的计数。在这种情况下，显示的值可以解释为“地板”，即大于等于该值才会拦截许多邮件。 **注**　“概述 (Overview)”页面上“由信誉过滤拦截 (Stopped by Reputation Filtering)”总数始终基于所有被拒绝连接的完整计数。因负载原因，只有按发件人连接的计数受限。
无效收件人	会话 LDAP 拒绝以及所有 RAT 拒绝所拒绝的所有邮件收件人。
垃圾邮件	检测到的任何垃圾邮件。
病毒邮件	检测到的任何病毒。
由内容过滤器拦截	由内容过滤器拦截的邮件总数。
威胁邮件总数	威胁邮件 （由信誉拦截、作为无效收件人拦截、垃圾邮件以及病毒）的总数。
营销	检测为不需要的营销邮件的邮件数量。
清洁	所有正常邮件。
用户邮件流量详细信息 （内部用户页面）	
检测到的传入垃圾邮件	检测到的所有传入垃圾邮件。
检测到的传入病毒	检测到的传入病毒。

表 4-2　邮件报告页面的表格列说明 （续）

列名	说明
传入邮件内容过滤器匹配数	检测到的传入邮件内容过滤器匹配数。
由内容过滤器拦截的传入	由设置的内容过滤器拦截的传入邮件。
传入的正常邮件	所有传入的正常邮件。
检测到的外发垃圾邮件	检测到的外发垃圾邮件。
检测到的外发病毒	检测到的外发病毒。
外发邮件内容过滤器匹配数	检测到的外发邮件内容过滤器匹配数。
内容过滤器拦截的外发邮件	由设置的内容过滤器拦截的外发邮件。
外发正常邮件	所有外发的正常邮件。
传入和外发 TLS 连接：TLS 连接页面	
必需的 TLS：失败	失败的所有必需 TLS 连接。
必需的 TLS：成功	成功的所有必需 TLS 连接。
首选的 TLS：失败	失败的所有首选 TLS 连接。
首选的 TLS：成功	成功的所有首选 TLS 连接。
总连接数	TLS 连接的总数。
邮件总数	TLS 邮件总数。
病毒爆发过滤器	
爆发名称	爆发的名称。
爆发 ID	爆发 ID。
全局先见到的	第一次全局发现该病毒。
保护时间:	针对病毒提供保护的时间。
隔离的邮件	与隔离相关的邮件。

邮件报告概述页面

安全管理设备上的**邮件 (Email) > 报告 (Reporting) > 概述 (Overview)** 页面提供您的邮件安全设备的邮件消息活动的概要。“概述 (Overview)”页面包括传入邮件和传出邮件的图形和摘要表。

概述 (Overview) 页面以较高层面显示传入和外发邮件图形以及传入和外发邮件摘要。

邮件趋势图以可视化方式表示了邮件流。可以使用该页面上的邮件趋势图监控进出设备的所有邮件的流量。

备注　基于域的执行摘要报告和执行摘要报告基于邮件报告概述页面。有关详细信息，请参阅基于域的执行摘要报告 （第 4-32 页）和执行摘要报告 （第 4-34 页）

表 4-3　邮件 (Email) > 报告 (Reporting) > 概述 (Overview) 页面的详细信息

部分	说明
Time Range	一个下拉列表，其中包含用于选择要查看的时间范围的选项。有关详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
查看以下项的数据 (View Data for)	选择要查看其概述数据的邮件安全设备，或选择所有邮件设备。 另请参阅查看设备或报告组的报告数据 （第 3-3 页）。

传入邮件消息如何计数

AsyncOS 根据每封邮件的收件人数量对传入邮件进行计数。例如，从 example.com 发送给三个收件人的传入邮件将计算为三封来自该发件人的邮件。

由发件人信誉过滤拦截的邮件实际不会进入工作队列，因此，设备无权访问传入邮件的收件人列表。在这种情况下，使用倍数来估算收件人数量。此倍数基于对大量现有客户数据样本的研究得出。

设备如何对邮件进行分类

当邮件通过邮件管道时，可应用于多个类别。例如，可将邮件标记为具有垃圾邮件或病毒特征；也可以匹配内容过滤器。各种过滤器和扫描活动的优先级会大大影响邮件处理的结果。

在上面的示例中，各种裁定都要遵从以下优先规则：

- 具有垃圾邮件特征
- 具有病毒特征
- 匹配内容过滤器

按照这些规则，如果某个邮件被标记为具有垃圾邮件特征，并且您的反垃圾邮件设置被设置为丢弃具有垃圾邮件特征的邮件，则该邮件将被丢弃，垃圾邮件计数器会增加。

此外，如果反垃圾邮件设置被设置为允许具有垃圾邮件特征的邮件继续在邮件通道中通行，并且后续内容过滤器将会丢弃、退回或隔离该邮件，则垃圾邮件计数器仍会增加。仅当该邮件不具有垃圾邮件或病毒特征时，内容过滤器才会增加。

或者，如果邮件被爆发过滤器隔离，则在该邮件从隔离中释放出来并再次进入工作队列之前，不会进行计数。

有关邮件处理优先级的完整信息，请参阅邮件安全设备在线帮助或用户指南中有关邮件通道的章节。

在 “概述 (Overview)”页面上对邮件进行分类

“概述 (Overview)”页面上报告的邮件按如下方式分类：

表 4-4　　“概述 (Overview)”页面上的邮件类别

类别	说明
由信誉过滤拦截	由 HAT 策略拦截的所有连接乘以一个固定倍数 （请参阅 “传入邮件消息如何计数”部分 （第 4-10 页））加上由收件人限制拦截的所有收件人。 “概述 (Overview)”页面上 “由信誉过滤拦截 (Stopped by Reputation Filtering)”总数始终基于所有被拒绝连接的完整计数。因负载原因，只有按发件人连接的计数受限。
无效收件人	会话 LDAP 拒绝以及所有 RAT 拒绝所拒绝的所有邮件收件人。
检测到的垃圾邮件	反垃圾邮件扫描引擎检测为具有垃圾邮件特征或可疑的邮件总数。此外，还包括同时具有垃圾邮件和病毒特征的邮件。
检测到的病毒邮件	被识别为病毒且不是垃圾邮件的邮件总数和百分比。 以下邮件列为 “检测到的病毒 (Virus Detected)”类别： • 病毒扫描结果为 “已修复 (Repaired)”或 “易感染 (Infectious)”的邮件 • 当选中用于将加密邮件列为包含病毒的邮件的选项时，病毒扫描结果为 “已加密 (Encrypted)”的邮件 • 当对不可扫描邮件执行的操作不是 “发送 (Deliver)”时，病毒扫描结果为 “不可扫描 (Unscannable)”的邮件 • 当选中用于发送至备用邮件主机或备用收件人时，病毒扫描结果为 “不可扫描 (Unscannable)”或 “已加密 (Encrypted)”的邮件 • 通过手动方式或因超时而从爆发隔离区删除的邮件
内容过滤器拦截	由内容过滤器拦截的邮件总数。
由 DMARC 拦截	未通过 DMARC 验证的邮件总数。
市场营销邮件	检测为不需要的营销邮件的邮件总数和百分比。仅当系统中存在营销数据时，页面上才会显示此列表项。
已接受的正常邮件	此类别是是已被接受且被视为不是病毒和垃圾邮件的邮件。 考虑到每个收件人的扫描操作 （例如正在按照单独的邮件策略处理的分散邮件）时接受的对正常邮件最准确的表达。 但是，由于标记为垃圾邮件或病毒特征并且仍然提交了的邮件不进行计数，因此所发送邮件的实际数量可能不同于正常邮件的计数。 如果邮件与*邮件过滤器*匹配并且不被过滤器丢弃或退回，则将这些邮件视为正常邮件。邮件过滤器丢弃或退回的邮件不计入总数。

备注　如果将防病毒设置配置为发送不可扫描或加密的邮件，则将这些邮件计入正常邮件，且不具有病毒特征。否则，邮件将被计入具有病毒特征的邮件。

传入邮件页面

安全管理设备上的**邮件 (Email) > 报告 (Reporting) > 传入邮件 (Incoming Mail)** 页面为连接到您的托管安全管理设备的所有远程主机提供实时信息的交互报告。您可以收集有关发送邮件到您的系统的 IP 地址、域和网络所有者 （组织）的信息。也可以基于 IP 地址、域以及向您发送邮件的组织执行发件人配置文件搜索。

传入邮件 (Incoming Mail) 页面包括两个主要部分：汇总了排名靠前的发件人 （按威胁邮件总数和正常邮件总数）的邮件趋势图和 “传入邮件详细信息 (Incoming Mail Details)”交互式表格。

“传入邮件详细信息 (Incoming Mail Details)”交互式表格显示有关特定 IP 地址、域或网络所有者（组织）的详细信息。可以通过点击**传入邮件 (Incoming Mail)** 页面或其他 “发件人配置文件 (Sender Profile)”页面顶部的相应链接，来访问任何 IP 地址、域或网络所有者的 “发件人配置文件 (Sender Profile)”页面。

从 “传入邮件 (Incoming Mail)”页面可以执行如下操作：

- 基于将邮件发送至安全管理设备的 IP 地址、域或网络所有者 （组织）进行搜索。请参阅搜索和交互式邮件报告页面 （第 4-5 页）。
- 查看 “发件人组 (Sender Groups)”报告以根据特定的发件人组和邮件流量策略操作监控连接。有关详情，请参阅 “发件人组 (Sender Groups)”报告页面”部分 （第 4-16 页）。
- 查看将邮件发送至您的设备的发件人的相关详细统计信息。统计信息包括按安全服务 （发件人信誉过滤、反垃圾邮件、防病毒等）细分的所尝试邮件数量。
- 按照向您发送大量垃圾邮件或病毒邮件 （由反垃圾邮件或防病毒安全服务决定）的发件人进行分类。
- 使用 SenderBase 信誉服务检查特定 IP 地址、域和组织之间的关系，以获取有关发件人的信息。
- 通过 SenderBase 信誉服务获取更多有关发件人的信息，包括发件人的 SenderBase 信誉得分 (SBRS) 以及域最近与哪个发件人组匹配。将发件人添加到发件人组。
- 获取更多有关发送大量垃圾邮件或病毒邮件 （由反垃圾邮件或防病毒安全服务决定）的特定发件人的信息。

“传入邮件 (Incoming Mail)”页面中的视图

传入邮件 (Incoming Mail) 页面包括三个不同的视图：

- IP 地址
- 域
- 网络所有者

这些视图在所选视图的环境中提供连接到系统的远程主机的快照。

此外，在 “传入邮件 (Incoming Mail)”页面的 “传入邮件详细信息 (Incoming Mail Details)”部分中，可以点击发件人的 “IP 地址 (IP Address)”、“域名 (Domain name)”或 “网络所有者 (Network Owner)”信息以检索特定的发件人配置文件信息。有关发件人配置文件信息的详细信息，请参阅 “发件人配置文件页面”部分 （第 4-15 页）。

备注 *网络所有者*是包含域的实体。*域*是包含 IP 地址的实体。

根据所选的视图，“传入邮件详细信息 (Incoming Mail Details)”交互式表格中显示将邮件发送至邮件安全设备上配置的所有公共侦听器的排名靠前的 IP 地址、域或网络所有者。可以监控传入设备的所有邮件的流量。

在“发件人配置文件 (Sender Profile)”页面上点击 IP 地址、域或网络所有者可访问有关发件人的详细信息。“发件人配置文件 (Sender Profile)”页面是一个特定于某个 IP 地址、域或网络所有者的“传入邮件 (Incoming Mail)”页面。

要按发件人组访问邮件流量信息，请点击“传入邮件 (Incoming Mail)”页面底部的**发件人组报告 (Sender Groups Report)** 链接。请参阅 “发件人组 (Sender Groups)”报告页面 （第 4-16 页）。

对 “传入邮件 (Incoming Mail)”页面上的邮件进行分类

“传入邮件 (Incoming Mail)”页面上报告的邮件按照如下方式进行分类：

表 4-5　“传入邮件 (Incoming Mail)”页面上的邮件类别

类别	说明
由信誉过滤拦截	由 HAT 策略拦截的所有连接乘以一个固定倍数 （请参阅 “传入邮件消息如何计数”部分 （第 4-10 页））加上由收件人限制拦截的所有收件人。 “由信誉过滤拦截 (Stopped by Reputation Filtering)”值的计算取决于多种因素： • 此发件人的 “受限制”邮件数量 • 被拒绝或被 TCP 拒绝的连接数量 （可能是部分计数） • 每个连接的邮件数量的保守倍数 当设备处于重负载下时，不会根据每个发件人来记录被拒绝的连接的准确计数，而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接的计数。在这种情况下，显示的值可以解释为 “地板”，即大于等于该值才会拦截许多邮件。
无效收件人	会话 LDAP 拒绝以及所有 RAT 拒绝所拒绝的所有邮件收件人。
检测到的垃圾邮件	反垃圾邮件扫描引擎检测为具有垃圾邮件特征或可疑的邮件总数。此外，还包括同时具有垃圾邮件和病毒特征的邮件。
检测到的病毒邮件	被识别为病毒且不是垃圾邮件的邮件总数和百分比。
内容过滤器拦截	由内容过滤器拦截的邮件总数。 如果访问权限允许查看邮件跟踪数据：要查看此报告中内容过滤器违规的邮件跟踪详细信息，请点击此表格中的蓝色编号链接。
由 DMARC 拦截	未通过 DMARC 验证的邮件总数。
市场营销邮件	检测为不需要的营销邮件的邮件总数和百分比。仅当系统中存在营销数据时，页面上才会显示此列表项
已接受的正常邮件	已被接受且被视为无病毒和垃圾邮件的邮件 — 考虑到每个收件人的扫描操作 （例如正在按照单独的邮件策略处理的分散邮件）时接受的对正常邮件最准确的表达。但是，由于标记为垃圾邮件或病毒特征并且仍然提交了的邮件不进行计数，因此所发送邮件的实际数量可能不同于正常邮件的计数。

备注　如果将防病毒设置配置为发送不可扫描或加密的邮件，则将这些邮件计入正常邮件，且不具有病毒特征。否则，邮件将被计入具有病毒特征的邮件。

此外，如果邮件与*邮件*过滤器匹配并且不被过滤器丢弃或退回，则将这些邮件视为正常邮件。邮件过滤器丢弃或退回的邮件不计入总数。

有时，某些报告页面包含可从顶部页面访问的几个唯一子报告。例如，通过安全管理设备中的“传入邮件 (Incoming Mail)”报告页面可以查看各个 IP 地址、域和网络所有者的信息。其中每个页面均是可从 “传入邮件 (Incoming Mail)”报告页面访问的子页面。

当点击顶级页面 （在此示例中为 “传入邮件 (Incoming Mail)”报告页面）右上角的 “可打印 PDF (Printable PDF)”链接时，将在一个整合报告中生成各个子报告页面的结果。请参阅了解邮件报告页面 （第 4-5 页）中的重要信息。

邮件 (Email) > 报告 (Reporting) > 传入邮件 (Incoming Mail) 页面提供以下视图：**IP 地址 (IP Addresses)**、**域 (Domains)** 或**网络所有者 (Network Owners)**

有关 “传入邮件详细信息 (Incoming Mail Details)”交互式表格中所含数据的解释，请参阅 “传入邮件详细信息 (Incoming Mail Details)”表格”部分 （第 4-14 页）。

从**传入邮件 (Incoming Mail)** 页面中，还可以生成 PDF 或将原始数据导出为 CSV 文件。有关打印或导出文件的信息，请参阅 “了解邮件报告页面”部分 （第 4-5 页）。

备注　可以生成 “传入邮件 (Incoming Mail)”报告页面的计划报告。请参阅 “计划邮件报告”部分 （第 4-35 页）。

“没有域名信息 (No Domain Information)”链接

已连接至安全管理设备并且无法通过双 DNS 查找进行验证的域将自动分组到名为 “没有域名信息 (No Domain Information)”的特殊域。可以控制通过发件人验证来管理此类未验证主机的方式。有关发件人验证的详细信息，请参阅邮件安全设备的文档或在线帮助。

可以使用 “显示的项目 (Items Displayed)”菜单选择要在列表中显示的发件人的数量。

邮件趋势图中的时间范围

可以选择不同程度的粒度以在邮件图中查看数据。可以选择相同数据的日视图、周视图、月视图和年视图。由于数据实时监控，因此信息会在数据库中定期更新和汇总。

有关时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。

“传入邮件详细信息 (Incoming Mail Details)”表格

传入邮件 (Incoming Mail) 页面底部的 “传入邮件详细信息 (Incoming Mail Details)”交互式表列出了已连接至邮件安全设备上的公共侦听器的排名靠前的发件人。下表根据所选视图显示域、 IP 地址或网络所有者。点击列标题可对数据进行排序。

系统通过执行*双 DNS 查找*来获得和验证远程主机 IP 地址的有效性。有关双 DNS 查找和发件人验证的更多信息，请参阅邮件安全设备的文档或在线帮助。

对于发件人，即 “传入邮件详细信息 (Incoming Mail Details)” 表的第一列或 “排名靠前的发件人(按威胁邮件总数) (Top Senders by Total Threat Messages)” 上列出的网络所有者、IP 地址或域，请点击**发件人 (Sender)** 或**无域信息 (No Domain Information)** 链接查看有关发件人的详细信息。结果显示在**发件人配置文件 (Sender Profile)** 页面上，其中包括来自 SenderBase 信誉服务的实时信息。从 “发件人配置文件 (Sender Profile)” 页面中，可以查看有关特定 IP 地址或网络所有者的详细信息。有关详细信息，请参阅 “发件人配置文件页面” 部分 （第 4-15 页）。

还可以通过点击 “传入邮件 (Incoming Mail)” 页面底部的**发件人组 (Sender Groups)** 报告查看发件人组报告。有关 “发件人组 (Sender Groups)” 报告页面的详细信息，请参阅 “发件人组 (Sender Groups)” 报告页面部分 （第 4-16 页）。

如果访问权限允许查看邮件跟踪数据：要查看此报告中内容过滤器违规的邮件跟踪详细信息，请点击此表格中的蓝色编号链接。

发件人配置文件页面

在**传入邮件 (Incoming Mail)** 页面的 “传入邮件详细信息 (Incoming Mail Details)” 交互式表格中点击发件人时，“发件人配置文件 (Sender Profile)” 页面即会显示。该页面中显示有关 IP 地址、域或网络所有者 （组织） 的详细信息。您可以通过点击 “传入邮件 (Incoming Mail)” 页面或其他 “发件人配置文件 (Sender Profile)” 页面上的相应链接来访问任何 IP 地址、域或网络所有者的 “发件人配置文件 (Sender Profile)” 页面。

*网络所有者*是包含域的实体。*域*是包含 IP 地址的实体。

为 IP 地址、域和网络所有者显示的 “发件人配置文件 (Sender Profile)” 页面稍有不同。不管是哪个页面，其中都包含来自特定发件人的传入邮件的图表和摘要表。图表下面是一个表格，其中列出了与发件人关联的域或 IP 地址。（单个 IP 地址的 “发件人配置文件 (Sender Profile)” 页面不包含更精细的列表。）“发件人配置文件 (Sender Profile)” 页面还包括一个信息部分，其中包含有关发件人的最新 SenderBase、发件人组和网络信息。

- “网络所有者配置文件 (Network Owner profile)” 页面包含网络所有者以及与该网络所有者关联的域和 IP 地址的信息。
- 域配置文件页面包含与该域关联的域和 IP 地址。
- IP 地址配置文件页面只包含有关该 IP 地址的信息。

每个 “发件人配置文件 (Sender Profile)” 页面底部的 “当前信息 (Current Information)” 表格中都包含以下数据：

- 来自 SenderBase 信誉服务的全局信息，包括：
  - IP 地址、域名和/或网络所有者
  - 网络所有者类别 （仅网络所有者）
  - CIDR 范围 （仅 IP 地址）
  - IP 地址、域和/或网络所有者的日流量和月流量
  - 自上次从此发件人收到第一封邮件以来的天数
  - 上一个发件人组以及是否进行了 DNS 验证 （仅 IP 地址发件人配置文件页面）

  日流量用于衡量某个域在最近 24 小时内发送了多少邮件。SenderBase 流量类似于用来衡量地震的里氏震级，使用以 10 为底数的对数标尺计算邮件数量。该标尺的最大理论值设置为 10，等同于 100% 的实际邮件数量。使用该对数标尺时，流量每增加 1 个单位，实际数量就会增加 10 个单位。

月流量的计算方法与日流量相同，只是百分比基于最近 30 天发送的邮件数量来计算。

- 平均流量 （仅 IP 地址）
- 生命周期流量/30 天流量 （仅 IP 地址配置文件页面）
- Bonded 发件人状态 （仅 IP 地址配置文件页面）
- SenderBase 信誉得分 （仅 IP 地址配置文件页面）
- 自第一封邮件以来的天数 （仅网络所有者和域配置文件页面）
- 与此网络所有者关联的域的数量 （仅网络所有者和域配置文件页面）
- 此网络所有者中的 IP 地址的数量 （仅网络所有者和域配置文件页面）
- 用于发送邮件的 IP 地址的数量 （仅网络所有者页面）

点击**来自 SenderBase 的更多信息 (More from SenderBase)** 可看到一个页面，其中包含由 SenderBase 信誉服务提供的所有信息。

- 有关此网络所有者控制的域和 IP 地址的详细信息，将显示在网络所有者配置文件页面上。有关域中的 IP 地址的详细信息，将显示在域页面上。

从域配置文件页面中，点击特定 IP 地址可查看特定信息，也可查看组织配置文件页面。

“发件人组 (Sender Groups)”报告页面

发件人组 (Sender Groups) 报告页面按发件人组和邮件流量策略操作提供连接摘要，从而便于查看 SMTP 连接和邮件流量策略趋势。“按发件人组的邮件流量 (Mail Flow by Sender Group)”列表显示每个发件人组的连接的百分比和数量。“按邮件流量策略操作的连接 (Connections by Mail Flow Policy Action)”图表显示每个邮件流量策略操作的连接的百分比。此页面概述了主机访问表 (HAT) 策略的有效性。有关 HAT 的详细信息，请参阅邮件安全设备的文档或在线帮助。

要查看 “发件人组 (Sender Groups)”报告页面，请选择**邮件 (Email) > 报告 (Reporting) > 发件人组 (Sender Groups)**。

从**发件人组 (Sender Groups)** 报告页面中，还可以生成 PDF 或将原始数据导出为 CSV 文件。有关打印或导出文件的信息，请参阅 “了解邮件报告页面”部分 （第 4-5 页）。

备注 可以为 “发件人组 (Sender Groups)”报告页面生成计划的报告。请参阅 “计划邮件报告”部分（第 4-35 页）。

“外发目标 (Outgoing Destinations)”页面

邮件 (Email) > 报告 (Reporting) > 外发目标 (Outgoing Destinations) 页面提供有关贵组织发送邮件的目标域的信息。

使用 “外发目标 (Outgoing Destinations)”页面可回答以下类型的问题：

- 邮件安全设备将邮件发送至哪些域？
- 向每个域发送多少邮件？
- 该邮件中有多少是正常的、具有垃圾邮件特征、具有病毒特征或由内容过滤器拦截？
- 发送了多少邮件以及被目标服务器硬性退回了多少邮件？

以下列表介绍了**外发目标 (Outgoing Destinations)** 页面的各个部分：

表 4-6　“邮件 (Email)” > “报告 (Reporting)” > “外发目标 (Outgoing Destinations)”页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
按威胁总数排名靠前的目标	贵组织所发送的外发威胁邮件 （垃圾邮件、病毒等）的排名靠前的目标域。威胁总数包括具有垃圾邮件或病毒特征或触发了内容过滤器的威胁。
按正常邮件数排名靠前的目标	贵组织发送的正常外发邮件的排名靠前的目标域。
外发目标详细信息	与贵组织发送的所有外发邮件的目标域相关的所有详细信息，按收件人总数排序。详细信息包括检测到的垃圾邮件、病毒，正常邮件等。 如果访问权限允许查看邮件跟踪数据：要查看此报告中内容过滤器违规的邮件跟踪详细信息，请点击此表格中的蓝色编号链接。

从**外发目标 (Outgoing Destinations)** 页面中，还可以生成 PDF 或将原始数据导出为 CSV 文件。有关打印或导出文件的信息，请参阅 “了解邮件报告页面”部分 （第 4-5 页）。

备注　可以为 “外发目标 (Outgoing Destinations)”页面生成计划的报告。请参阅 “计划邮件报告”部分 （第 4-35 页）。

“外发邮件发件人 (Outgoing Senders)”页面

邮件 (Email) > 报告 (Reporting) > 外发邮件发件人 (Outgoing Senders) 页面提供有关正从网络内的 IP 地址和域发送的邮件数量和类型的信息。

使用 “外发邮件发件人 (Outgoing Senders)”页面可回答以下类型的问题：

- 哪些 IP 地址正在发送最具病毒或垃圾邮件特征的邮件？
- 哪些 IP 地址触发内容过滤器的频率最高？
- 哪些域发送的邮件最多？
- 正在处理的尝试发送的收件人最大数量是多少？

要查看**外发邮件发件人 (Outgoing Sender)** 页面，请执行以下操作：

可以通过两种视图查看外发邮件发件人的结果：

- **域 (Domain)**：此视图可用于查看每个域发送的邮件数量。
- **IP 地址 (IP address)**：此视图用于查看哪些 IP 地址发送的病毒邮件最多或正在触发内容过滤器。

以下列表介绍了两种视图下**外发邮件发件人 (Outgoing Sender)** 页面的各个部分：

表 4-7　“邮件 (Email)” > “报告 (Reporting)” > “外发邮件发件人 (Outgoing Sender)” 页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
排名靠前的发件人(按有害邮件总数)	组织内外发威胁邮件 （垃圾邮件、防病毒邮件等）的排名靠前的发件人 （按 IP 地址或域）。
按正常邮件排名靠前的发件人	组织内外发正常邮件排名靠前的发件人 （按 IP 地址或域）。
发件人详细信息	组织内外发所有邮件的发件人的所有详细信息 （按 IP 地址或域）。详细信息包括检测到的垃圾邮件、病毒、正常邮件等。 如果访问权限允许查看邮件跟踪数据：要在此报告中查看 DLP 和内容过滤器违规的邮件跟踪详细信息，请点击表格中的蓝色数字链接。

备注　此页面未显示有关邮件发送的信息。要跟踪发送信息，例如从特定域退回的邮件数，请登录到相应的邮件安全设备，然后选择**监控 (Monitor) > 发送状态 (Delivery Status)**。

从**外发发件人 (Outgoing Senders)** 页面，还可以生成 PDF 或将原始数据导出为 CSV 文件。有关打印或导出文件的信息，请参阅 “了解邮件报告页面”部分 （第 4-5 页）。

备注　可以为**外发发件人 (Outgoing Senders)** 页面生成计划的报告。请参阅 “计划邮件报告”部分 （第 4-35 页）。

内部用户页面

邮件 (Email) > 报告 (Reporting) > 内部用户 (Internal Users) 页面*按邮件地址*提供有关内部用户发送和接收的邮件的信息。单一用户可以有多个邮件地址。这些邮件地址在报告中不会合并。

使用内部用户交互式报告页面可回答以下类型的问题：

- 谁发送的外部邮件最多？
- 谁接收的正常邮件最多？
- 谁接收的垃圾邮件最多？
- 谁触发了特定的内容过滤器？
- 内容过滤器是否阻止了来自特定用户的邮件？

表 4-8　邮件 (Email) > 报告 (Reporting) > 内部用户 (Internal Users) 页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
排名靠前的用户 （按正常的传入邮件）	组织内发送正常传入邮件排名靠前的用户 （按 IP 地址或域）。
排名靠前的用户 （按正常的外发邮件）	组织内外发正常邮件排名靠前的用户 （按 IP 地址或域）。
用户邮件控制详细信息	“用户邮件控制详细信息 (User Mail Flow Details)”交互式区域按各个邮件地址将收到和发送的邮件细分为 “正常 (Clean)”、“检测到垃圾邮件 (Spam Detected)”（仅限传入）、“检测到病毒 (Virus Detected)”和 “内容过滤器匹配 (Content Filter Matches)”。可以通过点击列标题对列表排序。 要查看用户的详细信息，请点击 “内部用户 (Internal User)”列中的用户名。有关详细信息，请参阅 “内部用户详细信息页面”部分 （第 4-19 页）。 如果访问权限允许查看邮件跟踪数据：要查看此报告中内容过滤器违规的邮件跟踪详细信息，请点击此表格中的蓝色编号链接。

从**内部用户 (Internal Users)** 页面还可以生成 PDF 或将原始数据导出为 CSV 文件。有关打印或导出文件的信息，请参阅 “了解邮件报告页面”部分 （第 4-5 页）。

备注　可以为 “内部用户 (Internal Users)”页面生成计划的报告。请参阅 “计划邮件报告”部分 （第 4-35 页）。

内部用户详细信息页面

“内部用户 (Internal User)”详细信息页面会显示有关用户的详细信息，包括显示每个类别 （检测到垃圾邮件、检测到病毒、被内容过滤器阻止和正常）邮件数量的传入和外发邮件明细。此外，还会显示传入和外发邮件内容过滤器匹配。

入站内部用户是基于 “收件人: (Rcpt To:)”地址为其接收邮件的用户。出站内部用户基于 “发件人: (Mail From:)”地址，在跟踪内部网络中的发件人所发送邮件的类型时非常有用。

点击内容过滤器的名称可在相应的内容过滤器信息页面上查看该过滤器的详细信息 （请参阅内容过滤器页面 （第 4-22 页））。可以使用此方法可查看发送或接收了与特定内容过滤器匹配的邮件的所有用户列表。

备注　一些出站邮件 （例如退回邮件）具有空发件人。它们作为出站 “未知”计数。

搜索特定的内部用户

通过 “内部用户 (Internal Users)”页面底部的搜索表单和 “内部用户 (Internal Users)”详细信息页面，可以搜索特定的内部用户 （邮件地址）。选择是完全匹配搜索文本还是查找以输入的文本开头的项目 （例如，以 “ex”开头将匹配 “example@example.com”）。

DLP 事件

邮件 (Email) > 报告 (Reporting) > DLP 事件 (DLP Incidents) （DLP 事件摘要）页面显示有关外发邮件中发生的数据丢失保护 (DLP) 策略违规事件的信息。邮件安全设备使用在“外发邮件策略 (Outgoing Mail Policies)”表中启用的 DLP 邮件策略来检测用户发送的敏感数据。违反 DLP 策略的每个外发邮件均报告为一个事件。

使用 DLP 事件摘要报告，可以回答以下类型的问题：

- 用户发送什么类型的敏感数据？
- 这些 DLP 事件具有什么样的严重性？
- 发送了多少封邮件？
- 丢失了多少封邮件？
- 是谁在发送这些邮件？

“DLP 事件摘要 (DLP Incident Summary)”页面包括两个主要部分：

- DLP 事件趋势图，按严重性 （低、中、高、关键）和策略匹配排名靠前的 DLP 事件。
- DLP 事件详细信息列表。

表 4-9　邮件 (Email) > 报告 (Reporting) > DLP 事件摘要 (DLP Incident Summary) 页面

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
最上面的事件 （按严重性）	按严重性列出的排名靠前的 DLP 事件。
事件概要	当前为每个邮件设备的外发邮件策略启用的 DLP 策略会在**DLP 事件摘要 (DLP Incident Summary)** 页面底部的“DLP 事件详细信息 (DLP Incident Details)”交互式表格中列出。点击 DLP 策略的名称可查看更多详细信息。
排名靠前的 DLP 策略匹配	匹配的排名靠前的 DLP 策略。
DLP 事件详细信息	“DLP 事件详细信息 (DLP Incident Details)”表显示每个策略的 DLP 事件总数，并且按严重级别进行细分，而且显示邮件是以明文形式发送、以加密形式发送还是已经丢弃。 有关 “DLP 事件详细信息 (DLP Incident Details)”表的详细信息，请参阅 “DLP 事件详细信息 (DLP Incidents Details)”表格部分 （第 4-21 页）。

点击 DLP 策略的名称可查看有关策略检测到的 DLP 事件的详细信息。可以使用此方法获得发送了包含策略检测到的敏感数据的邮件的用户列表。

“DLP 事件详细信息 (DLP Incidents Details)”表格

“DLP 事件详细信息 (DLP Incident Details)”表格是一个交互式表格，显示每个策略的 DLP 事件总数，并且按严重级别进行细分，而且显示邮件是以明文形式发送、以加密形式发送还是已经丢弃。点击列标题可对数据进行排序。

要了解有关在此表格中列出的任何 DLP 策略的更多信息，请点击 DLP 策略的名称，系统会显示 DLP 策略页面。有关详细信息，请参阅 “DLP 策略详细信息页面”部分 （第 4-21 页）。

如果访问权限允许查看邮件跟踪数据：要看填写在此报告中的邮件的邮件跟踪详细信息，请点击表格中的蓝色数字链接。

DLP 策略详细信息页面

如果点击“DLP 事件详细信息 (DLP Incident Details)”表中某个 DLP 策略的名称，则随之打开的“DLP 策略详细信息 (DLP Policy Detail)”页面会显示该策略的 DLP 事件数据。该页面根据严重性显示有关 DLP 事件的图形。

该页面还包括一个位于页面底部的 “按发件人的事件 (Incidents by Sender)”表，其中列出发送违反 DLP 策略的邮件的每个内部用户。该表还按用户显示每个策略的 DLP 事件总数，并且按严重级别进行细分，而且显示邮件是以明文形式发送、以加密形式发送还是已经丢弃。可以使用 “按发件人的事件 (Incidents by Sender)”表了解可能将组织的敏感数据发送给网络之外人员的用户。

点击事件详细信息页面上的发件人名称可打开 “内部用户 (Internal Users)”页面。有关详情，请参阅 “内部用户页面”部分 （第 4-18 页）。

邮件过滤器

“邮件过滤器 (Message Filters)”页面显示传入邮件和外发邮件的排名靠前的邮件过滤器匹配项（匹配邮件数量最多的邮件过滤器）的相关信息。

大量邮件

使用此页面上的报告以便：

- 确定涉及来自单个发件人或者在活动的一小时内具有相同主题的大量邮件的攻击。
- 监控排名靠前的域以确保此类攻击不在您自己的域中发生。如果出现该情况，组织中的一个或多个帐户会受到侵害。
- 帮助识别误报情况，以便相应地调整过滤器。

此页面上的报告仅显示来自邮件过滤器的数据，这些邮件过滤器使用信头重复规则，而且传递在该规则中设置的邮件数阈值。当与其他规则结合时，会在最后评估信头重复规则，而且如果之前的条件确定了邮件处置情况，则根本不评估该规则。同样，速率限制捕获的邮件从不会达到信头重复邮件过滤器。因此，可能会被视为大量邮件的某些邮件会不包含在这些报告中。如果配置了过滤器以便将某些邮件加入白名单，则这些邮件也会从报告中排除。

有关邮件过滤器和信头重复规则的详细信息，请参阅邮件安全设备的在线帮助或用户指南。

相关主题

- 速率限制页面 （第 4-27 页）

内容过滤器页面

邮件 (Email) > 报告 (Reporting) > 内容过滤器 (Content Filters) 页面显示排名靠前的传入和外发内容过滤器匹配 （哪些内容过滤器具有最多的匹配邮件）。该页面以条形图和列表的形式显示数据。使用 “内容过滤器 (Content Filters)” 页面，可以按内容过滤器或按用户查看公司策略，并且回答以下类型的问题：

- 传入或外发邮件最多触发了哪些内容过滤器？
- 发送或接收触发特定内容过滤器的邮件的排名靠前的用户有哪些？

要查看有关特定过滤器的详细信息，请点击过滤器的名称。此时将显示 “内容过滤器详细信息 (Content Filter Details)” 页面。有关 “内容过滤器详细信息 (Content Filter Details)” 页面的详细信息，请参阅 “内容过滤器详细信息页面” 部分 （第 4-22 页）。

如果访问权限允许查看邮件跟踪数据：要看填写在此报告中的邮件的邮件跟踪详细信息，请点击表格中的蓝色数字链接。

从**内容过滤器 (Content Filters)** 页面还可以生成 PDF 或将原始数据导出为 CSV 文件。有关打印或导出文件的信息，请参阅 “了解邮件报告页面” 部分 （第 4-5 页）。

备注 可以为 “内容过滤器 (Content Filter)” 页面生成计划的报告。请参阅 “计划邮件报告” 部分 （第 4-35 页）。

内容过滤器详细信息页面

“内容过滤器详细信息 (Content Filter Detail)” 页面显示随时间推移的过滤器匹配，以及按内部用户的匹配。

在 “按内部用户的匹配 (Matches by Internal User)” 部分中，点击用户的名称可查看内部用户（邮件地址）的详细信息页面。有关详细信息，请参阅内部用户详细信息页面 （第 4-19 页）。

如果访问权限允许查看邮件跟踪数据：要看填写在此报告中的邮件的邮件跟踪详细信息，请点击表格中的蓝色数字链接。

DMARC 验证

“DMARC 验证 (DMARC Verification)” 页面显示未通过基于域的邮件认证、报告和一致性 (DMARC) 验证的排名靠前的收件人域，以及针对来自每个域的传入邮件所采取的措施摘要。可以使用此报告优化 DMARC 设置并回答以下类型的问题：

- 哪些域发送了最多 DMARC 验证失败的邮件？
- 对于每个域，对 DMARC 验证失败的邮件执行了什么操作？

有关 DMARC 验证的详细信息，请参阅邮件安全设备的在线帮助或用户指南中的 “邮件身份验证” 章节。

“病毒类型 (Virus Types)”页面

邮件 (Email) > 报告 (Reporting) > 病毒 (Virus Types) 页面提供有关发送到网络和从网络发送的病毒的概述。“病毒类型 (Virus Types)”页面显示已由运行于邮件安全设备之上的病毒扫描引擎检测到并且显示在安全管理设备上的病毒。使用此报告针对特定病毒采取相应措施。例如，如果发现收到已知嵌入 PDF 文件中的大量病毒，则可以创建过滤器操作来隔离具有 PDF 附件的邮件。

备注　爆发过滤器可以隔离这些类型的感染了病毒的邮件，无需用户干预。

如果运行多个病毒扫描引擎，则 “病毒类型 (Virus Types)”页面包括来自所有启用的病毒扫描引擎的结果。显示在该页面上的病毒的名称由病毒扫描引擎确定。如果多个扫描引擎检测到某个病毒，则同一病毒可能具有多个对应的条目。

表 4-10　邮件 (Email) > 报告 (Reporting) > 病毒类型 (Virus Types) 页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
检测到的传入病毒类型排行榜	此部分显示已发送到您网络中的病毒的图表视图。
检测到的外发病毒类型排行榜	此部分显示已从您网络中发送的病毒的图表视图。
病毒类型详细信息	显示每个病毒类型详细信息的一个交互式表格。

备注　要查看哪些主机向您的网络发送了感染病毒的邮件，请转到 “传入邮件 (Incoming Mail)”页面，指定相同的报告期间，然后按病毒阳性进行排序。同样，要查看哪些 IP 地址在您的网络中发送了病毒阳性邮件，请查看 “传出发件人 (Outgoing Senders)”页面并盘病毒阳性邮件排序。

在**病毒类型 (Virus Types)** 页面中，还可以生成 PDF 或将原始数据导出为 CSV 文件。有关打印或导出文件的信息，请参阅 “了解邮件报告页面”部分 （第 4-5 页）。

备注　可以为**病毒类型 (Virus Types)** 页面生成计划的报告。请参阅 “计划邮件报告”部分 （第 4-35 页）。

URL 过滤页面

- 仅当启用了 URL 过滤时，才会填充 URL 过滤报告模块。
- URL 过滤报告适用于传入和外发邮件。
- 只有 URL 过滤引擎 （作为反垃圾邮件/爆发过滤器扫描一部分或通过邮件/内容过滤器）扫描的邮件会包含在这些模块中。但是，并非所有结果都一定具体归因于 URL 过滤功能。
- 排名靠前的 URL 类别模块包括在已扫描的邮件中发现的所有类别，不管这些邮件是否匹配内容或邮件过滤器。
- 每封邮件都只能与一个信誉级别相关。对于具有多个 URL 的邮件，统计数据会反映邮件中任何 URL 的最低信誉。

- 在“安全服务 (Security Services)”>“URL 过滤 (URL Filtering)”中配置的全局白名单中的 URL 不包含在报告中。

  在各个过滤器的白名单中使用的 URL 会包含在报告中。
- 恶意 URL 是爆发过滤器确定为信誉不佳的 URL。可疑 URL 是爆发过滤器确定需要点击时间保护的 URL。因此，可疑 URL 已被重写，从而重定向到思科网络安全代理。
- 基于 URL 类别的过滤器的结果会反映在内容和邮件过滤器报告中。
- 思科网络安全代理的点击时间 URL 评估结果不会反映在报告中。

高级恶意软件保护 （文件信誉和文件分析）报告页面

有关文件分析报告详细信息的要求

为了获取文件分析报告详细信息，设备必须能够通过端口 443 连接到文件分析服务器。请参阅附录 C “防火墙信息”中的详细信息。

如果思科内容安全管理设备没有直接连接到互联网，请为此流量配置一个代理服务器 （请参阅升级和更新设置 （第 14-18 页）。）如果已将设备配置为使用代理获取升级和服务更新，则会使用现有的设置。

如果使用 HTTPS 代理，则该代理不得解密流量。使用传递机制与文件分析服务器进行通信。该代理服务器必须信任来自文件分析服务器的证书，但是，不需要向文件分析服务器提供自己的证书。

有关任何其他要求，请参阅与安全管理设备版本对应的版本说明，该版本说明可从以下位置获取：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。

通过 SHA-256 哈希识别文件

由于文件名很容易更改，因此设备会使用安全哈希算法 (SHA-256) 为每个文件生成标识符。如果设备处理具有不同名称的同一文件，则所有实例都被识别为相同的 SHA-256。如果多个设备处理相同的文件，则该文件的所有实例都具有相同的 SHA-256 标识符。

在大多数报告中，会按文件的 SHA-256 值 （以缩写的格式）列出文件。

文件信誉和文件分析报告页面

报告	说明
高级恶意软件防护	显示由文件信誉服务识别的基于文件的威胁。 对于更改了裁定的文件，请参阅 AMP 裁定更新报告。这些裁定不会反映在 “高级恶意软件保护 (Advanced Malware Protection)”报告中。 如果从一个压缩或存档文件中提取的文件是恶意文件，则该压缩或存档文件的 SHA 值会包含在 “高级恶意软件保护 (Advanced Malware Protection)”报告中。
文件分析	显示发送进行分析的每个文件的时间和裁定 （或临时裁定）。 要查看超过 1000 个文件分析结果，请将数据导出为 .csv 文件。 深入查看详细分析结果，包括每个文件的威胁特征。 还可以搜索云服务以了解有关 SHA 的更多信息。该链接位于结果详细信息页面上。 要查看文件分析详细信息，请参阅有关文件分析报告详细信息的要求（第 4-24 页）。 如果从一个压缩或存档文件中提取的文件已发送进行分析，只有该提取文件的 SHA 值会包含在 “文件分析 (File Analysis)”报告中。
AMP 裁定更新	由于高级恶意软件保护侧重于针对性威胁和零日威胁，因此随着聚合数据提供更多信息，威胁裁定会更改。 AMP 裁定更新报告会列出此设备处理的其裁定自收到邮件以来已发生更改的文件。有关此情况的详细信息，请参阅邮件安全设备的相应文档。 要查看超过 1000 个裁定更新，请将数据导出为 .csv 文件。 如果单个 SHA-256 具有多个裁定更改，此报告仅会显示最新的裁定，而不是裁定历史记录。 要查看在最大可用时间范围内 （无论为报告选择的时间范围是什么）特定 SHA-256 的所有受影响邮件，请点击一个 SHA-256 链接。

查看其他报告中的文件信誉过滤数据

用于文件信誉和分析的数据会在其他相关的报告中提供。默认情况下，由高级恶意软件保护检测列会在适用的报告中隐藏。要显示其他列，请点击表格底部的 “列 (Columns)”链接。

“TLS 连接 (TLS Connections)”页面

邮件 (Email) > 报告 (Reporting) > TLS 连接 (TLS Connections) 页面会显示已发送和接收邮件的 TLS 连接的整体使用情况。该报告还显示使用 TLS 连接发送邮件的每个域的详细信息。

“TLS 连接 (TLS Connections)”页面可用于确定以下信息：

- 总体而言，传入和外发连接的哪个部分使用 TLS？
- 我与哪些合作伙伴成功建立了 TLS 连接？
- 我与哪些合作伙伴没有成功建立 TLS 连接？

- 哪些合作伙伴的 TLS 证书存在问题？
- 某个合作伙伴使用 TLS 的邮件占总邮件的百分比是多少？

表 4-11　邮件 (Email) > 报告 (Reporting) > TLS 连接 (TLS Connections) 页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
传入 TLS 连接图	该图会根据所选的时间范围显示过去一小时、一天或一周的传入 TLS 加密连接及未加密连接的视图。
传入 TLS 连接概要	此表显示传入邮件总量、加密和未加密的邮件量以及成功和失败的传入 TLS 加密邮件量。
传入 TLS 邮件摘要	此表显示传入邮件总量摘要。
传入 TLS 连接详细信息	此表显示发送或接收加密邮件的域的详细信息。对于每个域，可以查看连接总数、发送的邮件以及成功或失败的 TLS 连接数。还可以查看每个域中成功和失败的连接所占的百分比。
外发 TLS 连接图	该图会根据所选的时间范围显示过去一小时、一天或一周的外发 TLS 加密连接及未加密连接的视图。
外发 TLS 连接概要	此表显示外发邮件总量、加密和未加密的邮件量以及成功和失败的外发 TLS 加密邮件量。
外发 TLS 邮件摘要	此表显示外发邮件的总量。
外发 TLS 连接详细信息	此表显示发送或接收加密邮件的域的详细信息。对于每个域，可以查看连接总数、发送的邮件、成功或失败的 TLS 连接数以及最后 TLS 状态。还可以查看每个域中成功和失败的连接所占的百分比。

入站 SMTP 身份验证页面

“入站 SMTP 身份验证 (Inbound SMTP Authentication)”页面显示如何使用客户端证书和 SMTP AUTH 命令对邮件安全设备与用户的邮件客户端之间的 SMTP 会话进行验证。如果设备接受证书或 SMTP AUTH 命令，则会建立到邮件客户端的 TLS连接，供客户端用来发送邮件。由于设备无法跟踪每个用户进行的尝试，因此报告会基于域名和域 IP 地址显示有关 SMTP 身份验证的详细信息。

使用此报告可确定以下信息：

- 总体而言，多少入站连接使用 SMTP 身份验证？
- 多少连接使用客户端证书？
- 多少连接使用 SMTP AUTH？
- 当尝试使用 SMTP 身份验证时，哪些域无法连接？
- 当 SMTP 身份验证失败时，多少连接成功使用回退？

“入站 SMTP 身份验证 (Inbound SMTP Authentication)”页面包括已接收连接的图表，尝试 SMTP 身份验证连接的邮件收件人图表,以及包含身份验证连接尝试详细信息的表格。

“接收的连接 (Received Connections)”图表显示来自在指定的时间范围内尝试使用 SMTP 身份验证对连接进行身份验证的邮件客户端的传入连接。该图表显示设备接收的连接总数、未尝试使用 SMTP 身份验证进行验证的次数，使用客户端证书验证连接的成功和失败次数，以及使用 SMTP AUTH 命令进行验证的成功和失败次数。

“接收的收件人 (Received Recipients)”图表显示其邮件客户端尝试对邮件安全设备连接进行验证以使用 SMTP 身份验证发送邮件的收件人数量。该图表还显示其连接已经过身份验证的收件人数量，以及其连接未经过身份验证的收件人数量。

“SMTP 身份验证 (SMTP Authentication)”详细信息表格显示其用户尝试对邮件安全设备连接进行验证以发送邮件的域的详细信息。对于每个域，可以查看尝试使用客户端证书进行连接的成功或失败次数、尝试使用 SMTP AUTH 命令进行连接的成功或失败次数，以及在客户端证书连接尝试失败后回退到 SMTP AUTH 的次数。可以使用页面顶部的链接按域名或域 IP 地址显示此信息。

速率限制页面

通过按信封发件人的速率限制可以根据发件人地址按各个发件人的时间间隔限制邮件收件人数。“速率限制 (Rate Limits)”报告显示最显著超过该限制的发件人。

使用此报告有助于确定以下内容：

- 可能被用于批量发送垃圾邮件的受侵害用户帐户。
- 组织中的失控应用程序，这些应用程序使用邮件发送通知、警报、自动声明等内容。
- 组织中具有大量邮件活动的来源，用于内部计费或资源管理目的。
- 可能不会被视为垃圾邮件的大量入站邮件流量的来源。

请注意，包括内部发件人统计数据的其他报告 （例如内部用户或外发发件人）仅计量发送的邮件数；不会确定将少量邮件发送给大量收件人的发件人。

“按事件排名靠前的入侵者 (Top Offenders by Incident)”图表显示最频繁尝试将邮件发送给超出配置限制的收件人的信封发件人。每次尝试被视为一个事件。此图表汇聚来自所有侦听程序的事件计数。

“按拒绝的收件人排名靠前的入侵者 (Top Offenders by Rejected Recipients)”图表显示将邮件发送给超出所配置限制的最大数量收件人的信封发件人。此图表汇聚来自所有侦听程序的收件人计数。

速率限制设置 （包括 “信封发件人的速率限制 (Rate Limit for Envelope Senders)”设置）在邮件安全设备的 “邮件策略 (Mail Policies)” > “邮件流量策略 (Mail Flow Policies)”中配置。有关速率限制的详细信息，请参阅邮件安全设备的文档或在线帮助。

相关主题

- 大量邮件 （第 4-21 页）

爆发过滤器页面

邮件 (Email) > 报告 (Reporting) > 爆发过滤器 (Outbreak Filters) 页面显示有关最近爆发和由于爆发过滤器而被隔离的邮件的信息。使用此页面可以监控对针对性病毒、诈骗和网络钓鱼攻击的防御。

使用 “爆发过滤器 (Outbreak Filters)”页面可回答以下类型的问题：

- 有多少邮件被隔离，以及被哪一爆发过滤器规则隔离？
- 为病毒爆发提供爆发过滤器功能的交付期是多久？
- 局部爆发与全局爆发相比如何？

- 邮件在爆发隔离区中保留多长时间？
- 哪些是最常见的潜在恶意 URL？

“按类型的威胁”(Threats By Type) 部分显示设备收到的不同类型的威胁邮件。“威胁摘要 (Threat Summary)”部分按病毒、网络钓鱼和诈骗显示邮件的细分。

“过去一年爆发摘要 (Past Year Outbreak Summary)”会列出过去一年的全局及局部爆发，以便将局部网络趋势与全局趋势进行比较。全球爆发列表是所有爆发情况 （包括病毒和非病毒）的超集，而局部爆发仅限于影响设备的病毒爆发。局部爆发数据不包括非病毒威胁。全局爆发数据会显示由威胁操作中心检测到的超出当前为爆发隔离区配置的阈值的所有爆发。局部爆发数据显示在此设备上检测到的超出当前为爆发隔离区配置的阈值的所有病毒爆发。局部保护总时间始终基于威胁操作中心检测到各个病毒爆发的时间与主要供应商发布防病毒特征码的时间之间的差异。请注意，并非每个全局爆发都会影响设备。值 “--”表示保护时间不存在，或防病毒供应商未提供特征码时间 （某些供应商可能不报告特征码时间）。这并不表示保护时间为零，而是表示计算保护时间所需的信息不可用。

“隔离的邮件 (Quarantined Messages)”部分汇总爆发过滤器隔离情况，是测量爆发过滤器捕获的潜在威胁邮件数的有用计量器。隔离的邮件在释放时计数。通常，邮件在防病毒和反垃圾邮件规则可用之前会被隔离。释放时，它们会被防病毒和反垃圾邮件软件进行扫描并确定是阳性还是正常邮件。由于爆发跟踪的动态性质，当邮件处于隔离区中时，用于隔离邮件的规则 （甚至关联的爆发）可能会更改。在释放时对邮件计数 （而不是在进入隔离区时计数）可避免计数增加和降低引起的混乱。

威胁详细信息列表会显示有关特定爆发的信息，包括威胁类别 （病毒、欺诈或网络钓鱼）、威胁名称、威胁说明和确定的邮件数。对于病毒爆发，“过去一年的病毒爆发 (Past Year Virus Outbreaks)”包括爆发名称和 ID、首次全局出现病毒爆发的时间和日期、爆发过滤器提供的保护时间以及隔离的邮件数。可以选择是否查看全局或局部爆发。

首次全局出现时间由威胁操作中心根据 SenderBase （全球最大的邮件和网络流量监控网络）中的数据确定。保护时间始终基于威胁操作中心检测到各个威胁的时间与主要供应商发布防病毒特征码的时间之间的差异。

值 “--”表示保护时间不存在，或防病毒供应商未提供特征码时间 （某些供应商可能不报告特征码时间）。这并不表示保护时间为零。相反，这表示计算保护时间所需的信息不可用。

此页面上的其他模块提供：

- 爆发过滤器在所选时段处理的传入邮件数量。

  非病毒威胁包括使用指向外部网站的链接的网络钓鱼邮件、诈骗和恶意软件分发。

- 爆发过滤器捕获的威胁的严重性。

  级别 5 威胁表示在范围或影响方面非常严重，而级别 1 威胁表示威胁风险较低。有关威胁级别的说明，请参阅邮件安全设备的在线帮助或用户指南。

- 邮件在爆发隔离区中存在的时间长度。

  该持续时间由系统编译有关潜在威胁的足够数据以裁定其安全性所花费的时间确定。具有病毒威胁的邮件在隔离区中的保留时间通常多于非病毒威胁的保留时间，因为它们必须等待防病毒程序更新。此外，还会反映为每个邮件策略中指定的最大保留时间。

- 如果收件人点击邮件中潜在有恶意的链接，则通常会重新写入 URL 以便将邮件收件人重定向到思科网络安全代理进行站点点击时评估。

  此列表可能包括不是恶意的 URL，因为如果邮件中的任何 URL 被视为恶意，则邮件中的所有 URL 都会被重写。

备注　为了正确填充爆发过滤器报告页面上的表格，设备必须能够与 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “更新设置 (Update Settings)”中指定的思科更新服务器进行通信。

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章节。

系统容量页面

邮件 (Email) > 报告 (Reporting) > 系统容量 (System Capacity) 页面提供有关系统负载的详细说明，包括工作队列中的邮件、传入和外发邮件 （总量、大小和数量）、总体 CPU 使用率、按功能的 CPU 使用率和内容页面交换信息。

“系统容量 (System Capacity)”页面可用于确定以下信息：

- 确定邮件安全设备何时超出推荐的 CPU 容量。这可用于确定何时需要优化配置或添加设备。
- 确定系统行为方面指向即将发生的容量问题的历史趋势。
- 要进行故障排除，需确定系统的哪些部分使用大多数资源。

监控邮件安全设备以确保容量适合邮件量。随着时间的推移，邮件量会不可避免地增加，适当的监控可确保主动添加容量或进行配置更改。监控系统容量的最有效方式是跟踪总量、工作队列中的邮件以及资源节约模式下的事件。

- **邮件量：**了解环境中的 “正常”邮件量和 “一般”峰值非常重要。随着时间的推移跟踪此数据以测量邮件量增长。可以使用 “传入邮件 (Incoming Mail)”和 “外发邮件 (Outgoing Mail)”页面随着时间的推移跟踪邮件量。有关详细信息，请参阅系统容量 - 传入邮件 （第 4-30 页）和系统容量 - 外发邮件 （第 4-30 页）。
- **工作队列：**工作队列旨在充当 “缓冲器”- 吸收和过滤垃圾邮件攻击并处理非垃圾邮件的不正常增加情况。但是，工作队列还会指示系统存在压力的情况。拖延和频繁的工作队列备份可能表示存在容量问题。可以使用 “系统容量 - 工作队列 (System Capacity – Workqueue)”页面跟踪工作队列中的活动。有关详细信息，请参阅系统容量 - 工作队列 （第 4-30 页）。
- **资源节约模式：**当设备变得过载时，会进入资源节约模式 (RCM)，并发送 “关键”系统警报。这旨在保护设备，使其可以处理任何邮件积压情况。设备不能频繁进入 RCM 模式，只能在邮件量非常大或不正常增加时才能进入 RCM 模式。频繁的 RCM 警报可以表示系统变得过载。 RCM 不通过 “系统容量 (System Capacity)”页面跟踪。

如何解释在 “系统容量 (System Capacity)”页面上看到的数据

在 “系统容量 (System Capacity)”页面上选择查看数据的时间范围时，务必记住以下内容：

- 每日报告 - 每日报告会查询每小时表格，并显示设备在过去 24 小时内每小时接收的确切查询数。此信息从每小时表格中收集。这是一个确切的数字。
- 每月报告 - 每月报告会查询 30 或 31 天的每日表格 （根据月中的天数），从而提供有关 30 或 31 天内的查询数的确切报告。这同样是一个精确的数字。

“系统容量 (System Capacity)”页面上的 “最大 (Maximum)”值指示器是在指定时段内看到的最大值。“平均 (Average)”值是指定时段内所有值的平均值。时段聚合取决于为该报告选择的间隔。例如，如果图表用于一个月的时段，则可以选择查看每天的平均值和最大值。

可以点击特定图表的 “查看详细信息 (View Details)”链接以查看各个邮件安全设备的数据以及连接到安全管理设备的设备的总体数据。

系统容量 - 工作队列

“系统容量 - 工作队列 (System Capacity – Workqueue)”页面显示在指定的时段内位于工作队列中的邮件量。它还会显示相同时段内位于工作队列中的最大邮件数。可以查看一天、一周、一个月或一年的数据。工作队列图中的偶尔出现峰值是正常的，符合预期。如果越来越频繁地出现峰值，并且该情况持续很长时间，则可能表示存在容量问题。在查看工作队列页面时，可能要测量工作队列备份的频率，并记下超过 10,000 个邮件的工作队列备份。

系统容量 - 传入邮件

“系统容量 - 传入邮件 (System Capacity – Incoming Mail)”页面显示传入连接、传入邮件总数、平均邮件大小和传入邮件总大小。可以查看一天、一周、一个月或一年的结果。了解环境中的正常邮件量和峰值趋势至关重要。可以使用 “系统容量 - 传入邮件 (System Capacity – Incoming Mail)”页面随着时间的推移跟踪邮件量增长并规划系统容量。您可能还希望比较传入数据与发件人配置文件数据，以查看从特定域发送到网络的邮件量的趋势。

备注　传入连接数增加不一定会影响系统负载。

系统容量 - 外发邮件

“系统容量 - 外发邮件 (System Capacity – Outgoing Mai)”页面显示外发连接、外发邮件总数、平均邮件大小和外发邮件总大小。可以查看一天、一周、一个月或一年的结果。了解环境中的正常邮件量和峰值趋势至关重要。可以使用 “系统容量 - 外发邮件 (System Capacity – Outgoing Mail)”页面随着时间的推移跟踪邮件量增长，并且规划系统容量。您可能还要比较外发邮件数据与外发目标数据，以查看从特定域或 IP 地址发送的邮件量的趋势。

系统容量 - 系统负载

系统负载报告显示邮件安全设备上的整体 CPU 使用情况。 AsyncOS 经过优化，可使用空闲 CPU 资源来提高邮件吞吐量。高 CPU 使用率并不一定表示存在系统容量问题。如果高 CPU 使用率与持续的大容量内存页面交换一同出现，则可能表示存在容量问题。该页面还包含一个图，用于显示不同功能 （包括邮件处理、垃圾邮件和病毒引擎、报告和隔离）使用的 CPU 量。按功能显示的 CPU 图表可指示产品的哪些部分占用系统上的大多数资源。如果需要优化设备，则此图有助于确定哪些功能可能需要调整或禁用。

内存页面交换图以 KB/秒为单位显示系统必须切换到磁盘的频率。

有关内存页面交换的说明

该系统旨在定期交换内存，因此进行一些内存交换是适当的，并不表示设备存在问题。除非系统*持续*交换大量内存，否则内存交换是符合预期的正常行为 （尤其是在 C1x0 设备上）。为提高性能，可能需要将思科内容安全设备添加到网络或调整配置以确保实现最大吞吐量。

系统容量 - 全部

全部 (All) 页面将以前的所有系统容量报告整合在一个页面上，以便查看不同报告之间的关系。例如，您可能会发现在进行过量内存交换时，邮件队列很高。这可能是表示存在容量问题。您可能希望将此页面另存为 PDF 文件，以保留系统性能快照供以后参考 （或与支持人员共享）。

“报告数据可用性 (Reporting Data Availability)”页面

通过**邮件 (Email) > 报告 (Reporting) > 报告数据可用性 (Reporting Data Availability)** 页面，可以查看、更新和排序数据，以实时了解资源利用率和邮件流量问题位置。

所有数据资源利用率和邮件流量问题位置都显示在此页面上，包括由安全管理设备管理的整体设备的数据可用性。

在此报告页面中，还可以查看特定设备和时间范围的数据可用性。

关于计划和按需邮件报告

可用报告的类型

除非另有说明，否则以下类型的邮件安全报告均可作为计划和按需报告：

- 内容过滤器 - 此报告包括多达 40 个内容过滤器。有关在此页面上包含的内容的其他信息，请参阅 “内容过滤器页面”部分 （第 4-22 页）。
- DLP 事件摘要 - 有关在此页面上包含的内容的信息，请参阅 “DLP 事件”部分 （第 4-20 页）。
- 发送状态 - 该报告页面显示有关向特定收件人域或虚拟网关地址进行发送的问题的信息。页面中会显示一个列表，列出系统在过去三个小时内所发送邮件的前 20 、 50 或 100 个收件人域。可以通过点击每项统计数据列标题中的链接，按最新主机状态、有效收件人 （默认）、连接超时、发送的收件人、软退回事件以及硬退回收件人进行排序。有关邮件安全设备上的“发送状态 (Delivery Status)”页面可执行的功能的详细信息，请参阅的文档或在线帮助。
- 基于域的执行摘要 - 该报告基于邮件报告概述页面，并且限于一组指定的域。有关所包含内容的信息，请参阅 “基于域的执行摘要报告”部分 （第 4-32 页）。
- 执行摘要 - 此报告基于邮件报告概述页面中的信息。有关所包含内容的信息，请参阅 “基于域的执行摘要报告”部分 （第 4-32 页）。
- 传入邮件摘要 - 有关在此页面包含的内容的信息，请参阅 “传入邮件页面”部分 （第 4-12 页）。
- 内部用户摘要 - 有关在此页面包含的内容的信息，请参阅 “内部用户页面”部分 （第 4-18 页）。
- 爆发过滤器 - 有关在此页面包含的内容的信息，请参阅 “爆发过滤器页面”部分 （第 4-27 页）。
- 外发目标 - 有关在此页面包含的内容的信息，请参阅 “外发目标 (Outgoing Destinations)”页面部分 （第 4-16 页）。
- 外发邮件摘要 - 有关在此页面包含的内容的信息，请参阅 “外发邮件发件人 (Outgoing Senders)”页面部分 （第 4-17 页）。
- 外发发件人：域 - 有关在此页面包含的内容的信息，请参阅 “外发邮件发件人 (Outgoing Senders)”页面部分 （第 4-17 页）。
- 发件人组 - 有关在此页面包含的内容的信息，请参阅 “发件人组 (Sender Groups)”报告页面部分 （第 4-16 页）。
- 系统容量 - 有关在此页面包含的内容的信息，请参阅 “系统容量页面”部分 （第 4-29 页）。
- TLS 连接 - 有关在此页面包含的内容的信息，请参阅 “TLS 连接 (TLS Connections)”页面部分 （第 4-25 页）。
- 病毒类型 - 有关在此页面包含的内容的信息，请参阅 “病毒类型 (Virus Types)”页面部分 （第 4-23 页）。

时间范围

根据报告，这些报告可以配置为包括前一天、前七天、上个月、以前的日历日 （多达 250 天）或以前的日历月 （多达 12 个月）。或者，可以包含自定义天数 （从 2 天到 100 天）或自定义月数（从 2 个月到 12 个月）的数据。

无论何时运行报告，都会从以前的时间间隔 （小时、天、星期或月）返回数据。例如，如果安排每日报告在凌晨 1 点运行，则该报告将包含上一日的数据，从午夜到午夜 （00:00 到 23:59）。

语言和区域设置

备注 可以安排 PDF 报告，或者将原始数据导出为针对各个报告具有特定区域设置的 CSV 文件。通过“计划的报告 (Scheduled Reports)”页面上的语言下拉菜单，可以用户当前所选的区域设置和语言来查看或安排 PDF 报告。有关重要信息，请参阅打印和导出报告和跟踪数据 （第 3-9 页）。

存档的报告存储

有关报告存储时间以及何时从系统中删除存档的报告的信息，请参阅查看和管理存档的邮件报告（第 4-38 页）。

其他报告类型

在安全管理设备的**邮件 (Email) > 报告 (Reporting)** 部分中，可以生成的两个特殊报告为：

- 基于域的执行摘要报告
- 执行摘要报告

基于域的执行摘要报告

“基于域的执行摘要 (Domain-Based Executive Summary)”报告提供有关网络中一个或多个域的传入和外发邮件活动的摘要。这类似于 “执行摘要 (Executive Summary)”报告，但是报告数据限制为从/向指定的域发送的邮件。仅当发送服务器的 PTR （指针记录）中的域与指定的域匹配时，外发邮件摘要才会显示数据。如果指定了多个域，则设备会将所有域的数据整合在一个报告中。

要生成子域的报告，必须将其父域添加为邮件安全设备和安全管理设备的报告系统中的第二级域。例如，如果添加 example.com 作为第二级域，则其子域 （例如 subdomain.example.com）可用于报告。要添加第二级域，请在邮件安全设备 CLI 中使用 **reportingconfig -> mailsetup -> tld**，在安全管理设备 CLI 中使用 **reportingconfig -> domain -> tld**。

与其他计划的报告不同，基于域的执行摘要报告不会进行存档。

基于域的执行摘要报告和发件人信誉过滤阻止的邮件

由于发件人信誉过滤阻止的邮件不会进入工作队列，因此 AsyncOS 不会处理这些邮件来确定域目标。某个算法会估计每个域的被拒绝邮件数。要确定每个域中阻止的邮件的确切数量，可以在安全管理设备上延迟 HAT 拒绝，直到邮件达到收件人级别 (RCPT TO)。这使得 AsyncOS 可以从传入邮件中收集收件人数据。可以在邮件安全设备上使用 **listenerconfig -> setup** 命令延迟拒绝。但是，该选项会影响系统性能。有关延迟的 HAT 拒绝的详细信息，请参阅邮件安全设备的相应文档。

备注　要查看安全管理设备上基于域的执行摘要报告中的由信誉过滤拦截结果，则必须在邮件安全设备和安全管理设备上都启用 **hat_reject_info**。

要在安全管理设备上启用 **hat_reject_info**，请运行 **reportingconfig > domain > hat_reject_info** 命令。

基于域的执行摘要报告的域和收件人管理列表

可以使用配置文件来管理基于域的执行摘要报告的域和收件人。配置文件是存储在设备的配置目录中的文本文件。文件中的每一行都会生成单独的报告。这使您可以在一个报告中包含大量域和收件人，以及在一个配置文件中定义多个域报告。

配置文件的每个行都包含域名的空格分隔列表，和报告收件人邮件地址的空格分隔列表。逗号将域名列表与邮件地址列表分隔开。可以通过在父域名开头附加子域名称和点号来包括子域，例如 subdomain.example.com。

以下是生成三个报告的单个报告配置文件。

```
yourdomain.com sampledomain.com, admin@yourdomain.com
sampledomain.com, admin@yourdomain.com user@sampledomain.com
subdomain.example.com mail.example.com, user@example.com
```

备注　可以使用为单个指定报告定义的配置文件和设置来同时生成多个报告。例如，名为 Bigfish 的一家公司收购了其他两家公司 Redfish 和 Bluefish，而且继续保留他们的域。 Bigfish 使用包含三个行（与单独的域报告对应）的配置文件创建单个基于域的执行摘要报告。当设备生成基于域的执行摘要报告时， Bigfish 的管理员会收到有关 Bigfish.com、 Redfish.com 和 Bluefish.com 域的报告，Redfish 管理员会收到有关 Redfish.com 域的报告，而 Bluefish 管理员会收到有关 Bluefish.com 域的报告。

可以将不同的配置文件上传到设备以用于各个指定的报告。还可以将同一配置文件用于多个报告。例如，可以创建单独的指定报告，以提供有关相同的域在不同时段的数据。如果在设备上更新配置文件，则不必 GUI 中更新报告设置，除非更改文件名。

创建基于域的执行摘要报告

操作步骤

步骤 1　在安全管理设备中，可以安排报告或立即生成报告。

要安排报告，请执行以下操作：

a. 选择**邮件 (Email) > 报告 (Reporting) > 计划的报表 (Scheduled Reports)**。

b. 点击**添加计划的报告 (Add Scheduled Report)**。

要创建按需报告，请执行以下操作：

a. 选择**邮件 (Email) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

b. 点击**立即生成报告 (Generate Report Now)**。

步骤 2　从**报告类型 (Report Type)** 下拉列表中，选择**基于域的执行摘要 (Domain-Based Executive Summary)** 报告类型。

步骤 3　指定要包括在报告中的域以及报告收件人的邮件地址。可以选择以下选项之一来生成报告：

- **通过指定各个域生成报告**。输入报告的域和报告收件人的邮件地址。使用逗号分隔多个条目。还可以使用子域，例如 subdomain.yourdomain.com。如果为不会频繁更改的少量域创建报告，则建议指定各个域。
- **通过上传文件生成报告**。导入一个配置文件，其中包含报告的域和收件人邮件地址的列表。可以从设备的配置目录中选择配置文件，或从本地计算机上传一个配置文件。如果为频繁更改的大量域创建报告，则建议使用配置文件。有关基于域的报告的配置文件的详细信息，请参阅基于域的执行摘要报告的域和收件人管理列表 （第 4-33 页）。

注　如果将报告发送至一个外部帐户 （例如 Yahoo! Mail 或 Gmail），则可能需要将报告返回地址添加到外部帐户的白名单，以防止报告邮件被错误地分类为垃圾邮件。

步骤 4　在 “标题 (Title)” 文本字段中，键入报告的标题名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

步骤 5　在 “外发域 (Outgoing Domain)” 部分中，选择外发邮件摘要的域类型。选项包括：按服务器或按邮件地址。

步骤 6　从要包括的时间范围 (Time Range to Include) 下拉列表中，选择报告数据的时间范围。

步骤 7　在 “格式 (Format)” 部分中，选择报告的格式。

选项包括：

- **PDF**。创建格式化的 PDF 文档以用于传送和/或存档。可以通过点击 “预览 PDF 报告 (Preview PDF Report)” 来立即以 PDF 文件的形式查看报告。
- **CSV**。创建以逗号分隔值形式包含原始数据的 ASCII 文本文件。每个 CSV 文件都可包含多达 100 个行。如果报告包含多种类型的表格，则会为每个表格创建一个单独的 CSV 文件。

步骤 8　从 “安排 (Schedule)” 部分中，选择用于生成报告的安排。

选项包括：每天、每周 （包括周内各天的下拉列表）或每月。

步骤 9　（可选）为报告上传一个自定义徽标。徽标会显示在报告的顶部。

- 徽标应为 .jpg、 .gif 或 .png 文件，最多为 550 x 50 像素。
- 如果不提供徽标文件，则使用默认的思科徽标。

步骤 10　为此报告选择一种语言。有关如何使用亚洲语言生成 PDF 文件，请参阅打印和导出报告和跟踪数据 （第 3-9 页）中的重要信息。

步骤 11　点击**提交 (Submit)** 提交您在该页面的更改，然后点击**确认更改 (Commit Changes)** 确认您的更改。

执行摘要报告

执行摘要报告是对邮件安全设备中传入和外发邮件活动的高级概述，可以在安全管理设备上查看该报告。

此报告页面汇总了可以在邮件报告概述页面上查看的内容。有关邮件报告概述页面的详细信息，请参阅“邮件报告概述页面”部分 （第 4-9 页）。

“计划的报告 (Scheduled Reports)”页面

计划邮件报告

可以计划在关于计划和按需邮件报告 （第 4-31 页）中列出的任何报告。

要管理报告安排，请参阅以下内容：

添加计划的报告

要添加计划的邮件报告，请使用以下步骤：

操作步骤

步骤 1　在安全管理设备上，依次选择**邮件 (Email) > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 2　点击**添加计划的报告 (Add Scheduled Report)**。

步骤 3　选择报告类型。

有关报告类型的说明，请参阅关于计划和按需邮件报告 （第 4-31 页）。

注　有关基于域的执行摘要报告设置的信息，请参阅基于域的执行摘要报告 （第 4-32 页）。

注　计划的报告的可用选项因报告类型而异。在此程序其余部分中介绍的选项不一定适用于所有报告。

步骤 4　在**标题 (Title)** 字段中，键入报告的标题。

要避免创建具有相同名称的多个报告，我们建议使用描述性标题。

步骤 5　从**要包括的时间范围 (Time Range to Include)** 下拉菜单中，选择报告的时间范围。

步骤 6　为生成的报告选择**格式 (format)**。

默认格式为 PDF。大多数报告还允许将原始数据另存为 CSV 文件。

步骤 7　根据报告，对于**行数 (Number of Rows)**，选择要包括的数据量。

步骤 8　基于报告，选择排序报告所依据的列。

步骤 9　从**安排 (Schedule)** 区域中，为计划报告选择天、周或月旁边的单选按钮。此外，包括要为报告安排的时间。时间增量基于午夜到午夜 （00:00 到 23:59）。

步骤 10　在**邮件 (Email)** 文本字段中，键入将生成的报告发送到的邮件地址。

如果不指定邮件收件人，则系统仍会将报告存档。

可以根据需要为报告添加任意数量的收件人，包括零个收件人。但是，如果需要将报告发送至大量地址，则可能需要创建邮件列表而不是列出各个收件人。

步骤 11　为报告选择一种语言。

对于亚洲语言，请参阅打印和导出报告和跟踪数据 （第 3-9 页）中的重要信息。

步骤 12　点击 **Submit**。

编辑计划的报告

操作步骤

步骤 1　在安全管理设备上，依次选择**邮件 (Email) > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 2　点击要修改的 “报告标题 (Report Title)” 列中的报告名称链接。

步骤 3　修改报告设置。

步骤 4　提交并确认更改。

终止计划的报告

为防止生成计划的报告的未来实例，请执行以下步骤：

操作步骤

步骤 1　在安全管理设备上，依次选择**邮件 (Email) > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 2　选中要终止生成的报告所对应的复选框。要删除所有计划的报告，请选中**全部 (All)** 复选框。

步骤 3　点击 **Delete**。

注　任何已删除报告的存档版本都*不会*自动删除。要删除以前生成的报告，请参阅删除存档的报告 （第 4-38 页）。

按需生成邮件报告

除了可以使用在了解邮件报告页面 （第 4-5 页）中所述的交互式报告页面查看的报告外，还可以随时针对指定的时间范围为关于计划和按需邮件报告 （第 4-31 页）中列出的报告保存 PDF 或原始数据 CSV 文件。

要生成一个按需报告，请执行以下操作：

操作步骤

步骤 1　在安全管理设备上，依次选择**邮件 (Email) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

步骤 2　点击**立即生成报告 (Generate Report Now)**。

步骤 3　选择报告类型。

有关报告类型的说明，请参阅关于计划和按需邮件报告 （第 4-31 页）。

步骤 4　在 “标题 (Title)” 文本字段中，键入报告的标题名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

注　有关基于域的执行摘要报告设置的信息，请参阅基于域的执行摘要报告 （第 4-32 页）。

注　计划的报告的可用选项因报告类型而异。在此程序其余部分中介绍的选项不一定适用于所有报告。

步骤 5　从要包括的时间范围 (Time Range to Include) 下拉列表中，选择报告数据的时间范围。

注意自定义时间范围选项。

步骤 6　在 “格式 (Format)” 部分中，选择报告的格式。

选项包括：

- **PDF**。创建格式化的 PDF 文档以用于传送和/或存档。可以通过点击 “预览 PDF 报告 (Preview PDF Report)” 来立即以 PDF 文件的形式查看报告。
- **CSV**。创建以逗号分隔值形式包含原始数据的 ASCII 文本文件。每个 CSV 文件都可包含多达 100 个行。如果报告包含多种类型的表格，则会为每个表格创建一个单独的 CSV 文件。

步骤 7　选择要为其运行报告的设备或设备组。如果尚未创建任何设备组，则此选项不会显示。

步骤 8　从 “发送选项 (Delivery Option)” 部分中，选择以下项：

- 通过选中**存档报告 (Archive Report)** 复选框来存档报告。

  通过选择该项，将在 “存档的报告 (Archived Reports)” 页面上列出报告。

  注　基于域的执行摘要报告无法存档。

- 通过选中**立即通过邮件发送给收件人 (Email now to recipients)** 复选框，以邮件形式发送报告。

  在文本字段中，键入报告的收件人邮件地址。

步骤 9　为此报告选择一种语言。有关如何使用亚洲语言生成 PDF 文件，请参阅打印和导出报告和跟踪数据 （第 3-9 页）中的重要信息。

步骤 10　点击**发送此报告 (Deliver This Report)** 以生成报告。

存档的邮件报告页面

查看和管理存档的邮件报告

计划的报告和按需报告会存档一段时间。

安全管理设备会保留其生成的最新报告 - 对于每个计划报告，可包含多达 30 个最近的实例，并且对于所有报告，可包含 1000 个总版本。最多可将 30 个实例应用到具有相同名称和时间范围的计划报告。

存档的报告会自动删除。在添加新报告时，会删除较旧的报告以使数量保持在 1000。

存档的报告存储在设备上的 `/periodic_reports` 目录中。（有关详细信息，请参阅附录 A “IP 接口和设备访问”。）

访问存档的报告

邮件 (Email) > 报告 (Reporting) > 存档的报告 (Archived Reports) 页面会列出已选择存档的计划和按需报告，这些报告已生成但未清除。

操作步骤

步骤 1　选择**邮件 (Email) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

步骤 2　如果列表很长，要找到特定的报告，请通过从**显示 (Show)** 菜单中选择报告类型来过滤列表，或者点击某个列标题以按该列进行排序。

步骤 3　点击报告标题可查看该报告。

删除存档的报告

系统会根据查看和管理存档的邮件报告 （第 4-38 页）中概述的规则自动删除报告。但是，可以手动删除不需要的报告。

要手动删除存档的报告，请执行以下操作：

操作步骤

步骤 1　在安全管理设备上，依次选择**邮件 (Email) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

此时会显示可用的存档报告。

步骤 2　针对要删除的一个或多个报告选中该复选框。

步骤 3　点击 **Delete**。

步骤 4　要防止生成计划的报告的未来实例，请参阅终止计划的报告 （第 4-36 页）。

邮件报告故障排除

另请参阅对所有报告进行故障排除 （第 3-11 页）。

爆发过滤器报告不能正确显示信息

问题：爆发过滤器报告不能正确显示威胁信息。

解决方法：确认设备可以与 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “更新设置 (Update Settings)”中指定订单思科更新服务器通信。

点击报告中的链接后，邮件跟踪结果与报告结果不匹配

问题：深入了解报告时的邮件跟踪结果与预期结果不匹配。

解决方法：如果报告和跟踪没有一致且同时启用，而且不能正常运行，或者没有一致且同时地在每个邮件安全设备上进行集中或本地存储，则会发生该情况。仅当启用了各个功能 （报告、跟踪）时才会捕获该功能的数据。

相关主题

- 检查邮件跟踪数据的可用性 （第 6-4 页）

高级恶意软件保护裁定更新报告结果有所不同

问题：网络安全设备和邮件安全设备发送同一文件进行分析，而网络和邮件的 AMP 裁定更新报告针对该文件显示不同的裁定。

解决方法：这种情况是临时的。下载了所有裁定更新后，结果便会匹配。实现匹配最多需要 30 分钟。

查看文件分析报告详细信息时的问题

文件分析报告详细信息不可用

问题：文件分析报告详细信息不可用。

解决方法：请参阅有关文件分析报告详细信息的要求 （第 4-24 页）。

查看文件分析报告详细信息时出错

问题：当尝试查看文件分析报告详细信息时，显示 `No cloud server configuration is available` 错误。

解决方法：转到**管理设备 (Management Appliance) > 集中式服务 (Centralized Services) > 安全设备 (Security Appliances)**，然后添加至少一个启用了文件分析功能的邮件安全设备。

使用集中 Web 报告和跟踪

集中 Web 报告和跟踪概述

思科内容安全管理设备可以聚合来自多个网络安全设备上的安全功能的信息，并记录可用于监控网络流量模式和安全风险的数据。可以实时运行报告来查看特定时间段内系统活动的交互显示，也可以安排并定期运行报告。此外，报告功能还可将原始数据导出到文件。

集中 Web 报告功能不仅生成高级报告，允许管理员了解他们网络中发生的情况，还允许管理员深入了解特定域、用户或 URL 类别并查看其流量详细信息。

域

对于域，Web 报告功能可以生成以下要包含在域报告中的数据元素。例如，如果在 Facebook.com 域上生成报告，则报告可能包含：

- 访问 Facebook.com 次数最多的用户的列表
- 在 Facebook.com 中访问次数最多的 URL 的列表

User

对于用户， Web 报告功能可以生成以下要包含在用户报告中的数据元素。例如，对于标题为“Jamie”的用户报告，报告可能包含：

- 用户 “Jamie”访问次数最多的域的列表
- 恶意软件或病毒呈阳性的排名靠前的 URL 的列表
- 用户 “Jamie”访问的热门类别的列表

URL 类别

对于 URL 类别， Web 报告功能可以生成要包括在类别报告中的数据。例如，对于 “Sports” 类别，则报告会包含：

- “Sports” 类别中的排名靠前的域的列表
- 访问 “Sports” 类别的排名靠前的用户的列表

在所有这些示例中，这些报告旨在提供有关网络中特定项目的全面视图，以便管理员可以采取相应措施。

总则

有关日志记录页面与报告页面的详细说明，请参阅 “日志记录与报告” 部分 （第 15-1 页）。

备注 可以检索用户访问的域的所有信息，不必是访问的特定 URL 的信息。有关用户访问的特定 URL、他们访问 URL 的时间、是否允许该 URL 等信息，可使用 “网络跟踪” 页面上的搜索网络代理服务处理的事务。

备注 网络安全设备仅在使用本地报告时才存储数据。如果为网络安全设备启用了集中报告，则网络安全设备仅保留系统容量和系统状态数据。如果未启用集中 Web 报告，则仅会生成系统状态和系统容量报告。

有多种方式可用于查看有关安全管理设备的 Web 报告数据。

- 要查看交互式报告页面，请参阅 Web 报告页面说明 （第 5-5 页）。
- 要按需生成报告，请参阅按需生成 Web 报告 （第 5-33 页）。
- 要安排定期、经常性地生成报告，请参阅关于计划报告和按需 Web 报告 （第 5-29 页）。
- 要查看以前运行的报告的存档版本 （安排和按需生成），请参阅查看和管理存档的 Web 报告 （第 5-34 页）。
- 要查看有关各个事务的信息，请参阅网络跟踪 （第 5-34 页）。

设置集中 Web 报告和跟踪

要设置集中 Web 报告和跟踪，请按顺序完成以下步骤：

- 在安全管理设备上启用集中 Web 报告 （第 5-3 页）
  - 在 Web 报告中使用匿名
- 在网络安全设备上启用集中 Web 报告 （第 5-3 页）
- 将集中 Web 报告服添加到每个托管网络安全设备 （第 5-3 页）
- 在 Web 报告中使用匿名 （第 5-4 页）

在安全管理设备上启用集中 Web 报告

操作步骤

步骤 1 在启用集中 Web 报告之前，请确保为该服务分配了足够的磁盘空间。请参阅管理磁盘空间 （第 14-45 页）。

步骤 2 在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 网络 (Web) > 集中报告 (Centralized Reporting)**。

步骤 3 如果要在运行系统设置向导后首次启用集中报告，请执行以下操作：

a. 点击**启用 (Enable)**。

b. 查看最终用户许可协议，然后点击**接受 (Accept)**。

步骤 4 如果要启用先前已禁用的集中报告，请执行以下操作：

a. 点击**编辑设置 (Edit Settings)**。

b. 选中**启用集中 Web 报告服务 (Enable Centralized Web Report Services)** 复选框。

c. 可以现在或稍后访问在 Web 报告中使用匿名 （第 5-4 页）。

步骤 5 提交并确认更改。

在网络安全设备上启用集中 Web 报告

在启用集中报告之前，应配置所有网络安全设备并确保其按预期工作。

必须在将要使用集中报告的每个网络安全设备上启用集中报告。

请参阅您的网络安全设备的在线帮助或用户指南中的 “启用集中报告”部分。

将集中 Web 报告服添加到每个托管网络安全设备

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。

操作步骤

步骤 1 在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 2 如果已将网络安全设备添加到列表，请执行以下操作：

a. 点击网络安全设备的名称。

b. 选择**集中报告 (Centralized Reporting)** 服务。

步骤 3 如果您尚未添加网络安全设备，请执行以下操作：

a. 点击**添加网络设备 (Add Web Appliance)**。

b. 在 “设备名称 (Appliance Name)”和 “IP 地址 (IP Address)”文本字段，键入设备名称和网络安全设备管理接口的 IP 地址。

注　可以在 “IP 地址 (IP Address)”文本字段中输入 DNS 名称，但点击**提交 (Submit)** 后，它将立即解析为 IP 地址。

c. 集中报告服务已预先选中。

d. 点击**建立连接 (Establish Connection)**。

e. 为要托管的设备管理员帐户输入用户名和密码，然后点击**建立连接 (Establish Connection)**。

注　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。

g. 点击**测试连接**。

h. 阅读表格上方的测试结果。

步骤 4　点击 **Submit**。

步骤 5　为要启用集中报告的每个网络安全设备重复执行此程序。

步骤 6　确认更改。

在 Web 报告中使用匿名

默认情况下，用户名会显示在报告页面和 PDF 文件中。但是，为了保护用户隐私，可能需要使用户名在 Web 报告中不可识别。

备注　此设备上具有管理员权限的用户在查看交互报告时，始终可以看到用户名。

操作步骤

步骤 1　选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 网络 (Web) > 集中报告 (Centralized Reporting)**。

步骤 2　点击**编辑设置 (Edit Settings)**。

步骤 3　选中**在报告中使用匿名 (Anonymize usernames in reports)** 复选框。

步骤 4　提交并确认更改。

与网络安全报告一起使用

Web 报告页面支持监控有关系统中一个或所有托管网络安全设备上的信息。

目标	请参阅
查看用于访问和查看报告数据的选项	查看报告数据的方式 （第 3-1 页）
自定义交互式报告页面的视图	自定义报告数据的视图 （第 3-3 页）
在数据中查找有关特定事务的信息	网络跟踪 （第 5-34 页）
打印或导出报告信息	打印和导出报告和跟踪数据 （第 3-9 页）
了解各种交互式报告页面	Web 报告页面说明 （第 5-5 页）
按需生成报告	关于计划报告和按需 Web 报告 （第 5-29 页）
安排报告在指定的间隔和时间自动运行	关于计划报告和按需 Web 报告 （第 5-29 页）
查看存档的按需和计划报告	查看和管理存档的 Web 报告 （第 5-34 页）
了解如何收集数据	安全设备如何为报告收集数据 （第 3-2 页）

Web 报告页面说明

备注 有关 “Web 报告 (Web Reporting)”选项卡上哪些选项可用于按需或计划报告的信息，请参阅 “关于计划报告和按需 Web 报告”部分 （第 5-29 页）。

表 5-1　“Web 报告 (Web Reporting)”选项卡详细信息

“Web 报告 (Web Reporting)”菜单	操作
Web 报告概述	“概述”(Overview) 页面提供您的网络安全设备上的活动的概要。它包括传入和传出事务的图和摘要表。有关详细信息，请参阅 “Web 报告概述”部分 （第 5-8 页）。
用户报告 (Web)	“用户 (Users)”页面提供多个网络跟踪链接，用于查看各个用户的网络跟踪信息。 从**用户 (Users)** 页面中，可以查看系统上的一个或多个用户在互联网、特定站点或 URL 上花费的时间，以及用户使用多少带宽。 从**用户 (Users)** 页面中，可以点击交互式用户表格中的单个用户，以在“用户详细信息 (User Details)”页面上查看该特定用户的更多详细信息。 通过**用户详细信息 (User Details)** 页面，可以查看关于在**网络 (Web) > 报告 (Reporting) > 用户 (Users)** 页面的“用户 (Users)”表格中识别的用户的特定信息。在该页面中，可以调查系统中各个用户的活动。如果运行用户级调查并需要进行查询 （例如，用户访问什么站点、他们遇到了什么恶意软件威胁、他们访问什么 URL 类别以及特定用户在这些站点花费的时间），则该页面将非常有用。 有关详细信息，请参阅 “用户报告 (Web)”部分 （第 5-9 页）。有关系统中特定用户的信息，请参阅 “用户详细信息 （Web 报告）”部分 （第 5-10 页）

表 5-1　“Web 报告 (Web Reporting)”选项卡详细信息 （续）

“Web 报告 (Web Reporting)”菜单	操作
网站报告	通过 “网站 (Web Sites)”页面，可以查看托管设备上发生的活动的整体汇总。通过该页面，可以监控在特定时间范围内访问的高风险网站。有关详细信息，请参阅 “网站报告”部分 （第 5-11 页）。
URL 类别报告	通过 “URL 类别 (URL Categories)”页面，可查看所访问的排名靠前的 URL 类别，包括： • 根据事务触发了阻止或警告操作的排名靠前的 URL。 • 在指定时间范围内，已完成、已警告和已阻止的事务对应的所有 URL 类别。这是一个交互式表格，具有交互式列标题，可用来按需排序数据。 有关详细信息，请参阅 “URL 类别报告”部分 （第 5-12 页）。
应用可视性报告	通过 “应用可视性 (Application Visibility)”页面，可以应用和查看已用于安全管理设备和网络安全设备中特定应用类型的控件。有关详细信息，请参阅 “应用可视性报告”部分 （第 5-14 页）。
防恶意软件报告	通过 “防恶意软件 (Anti-Malware)”页面，可查看有关扫描引擎在指定时间范围内检测到的恶意软件端口和恶意站点的信息。报告的上半部分显示各个排名靠前的恶意软件端口和网站的连接数。报告的下半部分显示检测到的恶意软件端口和站点。有关详细信息，请参阅 “防恶意软件报告”部分 （第 5-16 页）。
高级恶意软件保护 （文件信誉和文件分析）报告页面	有三个报告页面会显示文件信誉和分析数据。 有关详细信息，请参阅 “高级恶意软件防护 （文件信誉和文件分析）报告”部分 （第 5-18 页）。
客户端恶意软件风险报告	“客户端恶意软件风险 (Client Malware Risk)”页面是与安全相关的报告页面，可用于识别反常地频繁连接到恶意软件站点的各个客户端计算机。 有关详细信息，请参阅 “客户端恶意软件风险报告”部分 （第 5-20 页）。
网络信誉过滤器报告	可用于查看针对在指定时间范围内的事务进行网络信誉过滤的报告。有关详细信息，请参阅 “网络信誉过滤器报告”部分 （第 5-21 页）。
L4 流量监视器报告	可用于查看有关 L4 流量监视器在指定时间范围内检测到的恶意软件端口和恶意软件站点的信息。有关详细信息，请参阅 “L4 流量监视器报告”部分 （第 5-23 页）。
SOCKS 代理报告	可用于查看 SOCKS 代理事务的数据，包括目标和用户。 有关详细信息，请参阅 “SOCKS 代理报告”部分 （第 5-25 页）。
按用户地点分类的报告	通过 “按用户地点分类的报告 (Reports by User Location)”页面，可以了解移动用户在其本地或远程系统中进行的活动。 有关详细信息，请参阅 “按用户地点分类的报告”部分 （第 5-26 页）。

表 5-1　“Web 报告 (Web Reporting)”选项卡详细信息 （续）

“Web 报告 (Web Reporting)”菜单	操作
网络跟踪	通过 “网络跟踪 (Web Tracking)”页面，可以搜索以下类型的信息： • 搜索网络代理服务处理的事务允许您跟踪和查看与网络相关的基本信息，例如通过设备处理的网络流量类型。 这包括诸如时间范围、用户 ID 和客户端 IP 地址等信息，此外还包括诸如特定类型的 URL、每个连接占用的带宽或者跟踪特定用户网络使用情况的信息。 • 搜索 L4 流量监视器处理的事务允许您搜索 L4TM 数据以了解恶意软件传输活动涉及的站点、端口和客户端 IP 地址。 • 搜索 SOCKS 代理处理的事务允许您搜索 SOCKS 代理处理的事务。 有关详细信息，请参阅 “网络跟踪”部分 （第 5-34 页）。
系统容量页面	可用于查看将报告数据发送到安全管理设备的总体工作负载。 有关详细信息，请参阅 “系统容量页面”部分 （第 5-27 页）。
数据可用性页面	可用于概括了解报告数据对每个设备上的安全管理设备的影响。有关详细信息，请参阅 “数据可用性页面”部分 （第 5-28 页）。
计划的报告	可用于安排指定时间范围的报告。有关详细信息，请参阅 “关于计划报告和按需 Web 报告”部分 （第 5-29 页）。
存档的报告	可用于存档指定时间范围的报告。有关详细信息，请参阅 “查看和管理存档的 Web 报告”部分 （第 5-34 页）。

备注 可以针对大多数 Web 报告类别 （包括扩展的排名靠前的 URL 类别和排名靠前的应用类型）安排报告。有关安排报告的详细信息，请参阅 “关于计划报告和按需 Web 报告”部分 （第 5-29 页）

关于花费的时间

各个表格中 “花费的时间 (Time Spent)”列表示用户在网页上花费的时间。在调查用户时，表示用户在每个 URL 类别上花费的时间。在跟踪 URL 时，表示每个用户在特定 URL 上花费的时间。

将某个事务事件标记为 “已查看”后，用户访问特定 URL 时，“花费的时间 (Time Spent)”值将开始计算并且添加为 Web 报告表格中的一个字段。

为了计算花费的时间， AsyncOS 会针对在一分钟内的活动为每个活动用户分配 60 秒的时间。在该分钟结束时，每个用户花费的时间会平均分配到该用户访问的不同域中。例如，如果用户在活动的一分钟内访问了四个不同的域，则认为该用户在每个域中花费了 15 秒。

为了计算花费的时间值，需考虑以下注意事项：

- 活动用户被定义为符合以下条件用户名或 IP 地址：通过设备发送 HTTP 流量并且已访问被 AsyncOS 视为 “页面视图”的网站。
- AsyncOS 将页面视图定义为用户发起的 HTTP 请求，与客户端应用发起的请求相反。AsyncOS 使用启发式算法来尽可能做出最好的猜测，以识别用户页面视图。

单位以 “小时:分钟”的格式显示。

Web 报告概述

网络 (Web) > 报告 (Reporting) > 概述 (Overview) 页面提供您的网络安全设备上的活动的概要。它包括传入和传出事务的图和摘要表。

概述 (Overview) 页面概括地显示有关 URL 和用户使用、网络代理活动以及各种事务摘要的统计数据。事务摘要提供进一步的趋势详细信息，例如可疑的事务，而且在此图对面，还介绍被阻止的可疑事务数以及阻止这些事务的方式。

概述 (Overview) 页面的下半部分介绍使用情况。这包括受到访问的排名靠前的 URL 类别、受到阻止的排名靠前的应用类型和类别，以及生成这些阻止或警告的排名靠前的用户。

表 5-2　网络 (Web) > 报告 (Reporting) > 概述 (Overview) 页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
查看以下项的数据 (View Data for)	选择要查看其概述数据的网络安全设备，或选择所有网络设备。 另请参阅查看设备或报告组的报告数据 （第 3-3 页）。
Web 代理活动总数	通过此部分可查看当前由安全管理设备管理的网络安全设备报告的网络代理活动。 此部分显示实际事务数 （纵坐标）以及发生活动的大约日期 （水平时间轴）。
Web 代理摘要	通过此部分可以查看可疑网络代理活动或干净代理活动的百分比，包括事务总数。
L4 流量监视器摘要 (L4 Traffic Monitor Summary)	本部分报告当前由安全管理设备管理的网络安全设备所报告的任何 L4 流量。
可疑事务数	通过此部分可以查看管理员标记为可疑的网络事务。 此部分显示实际事务数 （纵坐标）以及发生活动的大约日期 （水平时间轴）。
可疑事务摘要	通过此部分可查看阻止或警告的可疑事务的百分比。此外，还可以查看已检测到并阻止的事务类型，以及此事务被阻止的实际次数。
按事务总数排名靠前的 URL 类别	此部分显示被阻止的前 10 种 URL 类别，包括 URL 类别的类型 （纵坐标）以及特定类型的类别被阻止的实际次数 （横坐标）。 预定义的 URL 类别组会不定期更新。有关这些更新对报告结果的影响的详细信息，请参阅 URL 类别集更新和报告 （第 5-13 页）。
按事务总数排名靠前的应用程序类型	此部分显示被阻止的排名靠前的应用类型，包括实际应用类型的名称 （纵坐标）和特定应用被阻止的次数 （横坐标）。

表 5-2　网络 (Web) > 报告 (Reporting) > 概述 (Overview) 页面的详细信息 （续）

部分	说明
检测到的恶意软件类别总数	此部分显示检测到的所有恶意软件类别。
按阻止或警告的事务数排名靠前的用户 (Top Users Blocked or Warned Transactions)	此部分显示生成阻止或警告的事务的实际用户。可以通过 IP 地址或用户名来显示用户。要使用户名不可识别，请参阅在 Web 报告中使用匿名 （第 5-4 页）。

用户报告 (Web)

网络 (Web) > 报告 (Reporting) > 用户 (Users) 页面提供了多个链接，可用于查看各个用户的 Web 报告信息。

从**用户 (Users)** 页面中，可以查看系统上的一个或多个用户在互联网、特定站点或 URL 上花费的时间，以及用户使用多少带宽。

备注　在网络安全设备上，安全管理设备可以支持的最大用户数为 500。

从**用户 (Users)** 页面，可以查看有关系统中用户的以下信息：

表 5-3　网络 (Web) > 报告 (Reporting) > 用户 (Users) 页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
按受阻事务数排名靠前的用户	此部分按 IP 地址或用户名列出排名靠前的用户 （纵坐标），并且列出被阻止的特定于该用户的事务数 （横坐标）。出于报告目的，可以使用户名或 IP 地址不可识别。有关如何使用户名在此页面或计划报告中不可识别的详细信息，请参阅以下部分：“在安全管理设备上启用集中 Web 报告”部分 （第 5-3 页）。默认设置为显示所有用户名。要隐藏用户名，请参阅 “在 Web 报告中使用匿名”部分 （第 5-4 页）。
按使用的带宽排名靠前的用户	此部分按 IP 地址或用户名显示在系统上使用最多带宽 （以使用的 GB 数表示横坐标）的排名靠前的用户 （纵坐标）。
用户 (Users) 表	可用于查找特定用户 ID 或客户端 IP 地址。在 “用户 (User)” 部分底部的文本字段中，输入特定用户 ID 或客户端 IP 地址，然后点击**查找用户 ID 或客户端 IP 地址 (Find User ID or Client IP Address)**。 IP 地址不需要与返回结果完全匹配。 在 “用户 (Users)” 表中，可以点击特定用户以查找更具体的信息。此信息显示在 “用户详细信息 (User Details)” 页面上。有关 “用户详细信息 (User Details)” 页面的详细信息，请参阅 “用户详细信息 （Web 报告）”部分 （第 5-10 页）

备注　要查看用户 ID 而不是客户端 IP 地址，必须设置安全管理设备，以从 LDAP 服务器获取用户信息。有关信息，请参阅第 9 章中的创建 LDAP 服务器配置文件。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

要查看如何使用**用户 (Users)** 页面的示例，请参阅 “示例 1：调查用户”部分 （第 D-1 页）。

备注 可以为 “用户 (Users)”页面生成或安排报告。有关更多信息，请参阅 “关于计划报告和按需 Web 报告”部分 （第 5-29 页）。

用户详细信息 （Web 报告）

通过**用户详细信息 (User Details)** 页面，可以查看关于在**网络 (Web) > 报告 (Reporting) > 用户 (Users)** 页面上的交互式用户表中识别的用户的特定信息。

通过**用户详细信息 (User Details)** 页面，可以调查系统上各个用户的活动。如果运行用户级调查并需要进行查询 （例如，用户访问什么站点、他们遇到了什么恶意软件威胁、他们访问什么 URL 类别以及特定用户在这些站点花费的时间），则该页面将非常有用。

要显示特定用户的**用户详细信息 (User Details)** 页面，请点击**网络 (Web) > 用户 (Users)** 页面上用户表中的特定用户。

从**用户详细信息 (User Details)** 页面，可以查看有关系统中各个用户的以下信息：

表 5-4　网络 (Web) > 报告 (Reporting) > 用户 (Users) > 用户详细信息 (User Details) 页面的详细信息

部分	说明
时间范围 （下拉列表）	可用于选择报告中所含数据的时间范围的菜单。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）
按事务总数的 URL 类别	此部分节列出特定用户使用的特定 URL 类别。 预定义的 URL 类别组会不定期更新。有关这些更新对报告结果的影响的详细信息，请参阅 URL 类别集更新和报告 （第 5-13 页）。
按事务总数的趋势	此图显示用户访问网络的时间。 例如，此图将指示在一天的某段时间是否存在网络流量激增，以及什么时候会出现该激增情况。使用 “时间范围 (Time Range)”下拉列表，可以扩展此图，从而以更大粒度或更小粒度的时间范围查看用户在网络中的情况。
匹配的 URL 类别	“匹配的 URL 类别 (URL Categories Matched)”部分显示已完成和阻止的事务的匹配类别。 在此部分中，还可以找到特定的 URL 类别。在该部分底部的文本字段中，输入 URL 类别并点击**查找 URL 类别 (Find URL Category)**。该类别不必完全匹配。 预定义的 URL 类别组会不定期更新。有关这些更新对报告结果的影响的详细信息，请参阅 URL 类别集更新和报告 （第 5-13 页）。

表 5-4　网络 (Web) > 报告 (Reporting) > 用户 (Users) > 用户详细信息 (User Details) 页面的详细信息 （续）

部分	说明
匹配的域	在此部分中，可以查找有关此用户访问的特定域或 IP 地址的信息。还可以查看在这些类别上花费的时间，以及在列视图中设置的其他各种信息。在该部分底部的文本字段中，输入域或 IP 地址，然后点击**查找域或 IP (Find Domain or IP)**。域或 IP 地址不必完全匹配。
匹配的应用程序	在此部分中，可以查找特定用户正在使用的特定应用。例如，如果用户正在访问需要使用大量 Flash 视频的站点，则会在 “应用 (Application)” 列中显示应用类型。 在该部分底部的文本字段中，输入应用名称并点击**查找应用 (Find Application)**。应用名称不必完全匹配。
检测到的恶意软件威胁数	在此表格中，可以看到特定用户触发的排名靠前的恶意软件威胁。 可以在 “查找恶意软件威胁 (Find Malware Threat)” 字段中搜索有关特定恶意软件威胁名称的数据。输入恶意软件威胁名称，然后点击 “查找恶意软件威胁 (Find Malware Threat)”。恶意软件威胁的名称不必完全匹配。
匹配的策略	在此部分中，可以查找在访问网络时适用于此用户的策略组。 在该部分底部的文本字段中，输入策略名称并点击**查找策略 (Find Policy)**。策略的名称不必完全匹配。

备注 在 “客户端恶意软件风险详细信息 (Client Malware Risk Details)” 表中：客户端报告有时在显示用户时，会在用户名的结尾处标有星号 (*)。例如，客户端报告可能为 “jsmith” 和 “jsmith*” 分别显示一个条目。使用星号 (*) 列出的用户名表示用户名由用户提供，但未得到验证服务器的确认。当验证服务器目前不可用，并且设备配置为在验证服务不可用时允许通信，则会发生该情况。

要查看如何使用 “用户详细信息 (User Details)” 页面的示例，请参阅 “示例 1：调查用户” 部分（第 D-1 页）。

网站报告

网络 (Web) > 报告 (Reporting) > 网站 (Web Sites) 页面是对托管设备上所发生活动的整体聚合。通过该页面，可以监控在特定时间范围内访问的高风险网站。

在**网站 (Web Sites)** 页面中，可以查看以下信息：

表 5-5　网络 (Web) > 报告 (Reporting) > 网站 (Web Sites) 页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围” 部分 （第 3-4 页）。
按事务总数排名靠前的域	此部分以图形格式列出在站点上访问的排名靠前的域。

表 5-5　网络 (Web) > 报告 (Reporting) > 网站 (Web Sites) 页面的详细信息 （续）

部分	说明
按受阻事务数排名靠前的域	此部分以图形格式列出根据事务触发阻止操作的排名靠前的域。例如，用户访问特定域，并且由于我已有具体的策略，因此触发了阻止操作。此域会在此图形中作为阻止的事务列出，并且还会列出触发阻止操作的域站点。
匹配的域	本部分以交互式表格的形式列出在站点上访问的域。在此表格中，可以通过点击特定域访问有关该特定域的更精细信息。“网络跟踪 (Web Tracking)”页面上会显示 “代理服务 (Proxy Services)”选项卡，并且可以看到跟踪信息以及阻止某些域的原因。 点击特定域时，可以看到该域中排名靠前的用户、该域中排名靠前的事务、匹配的 URL 类别，以及检测到的恶意软件威胁。 要查看有关如何使用网络跟踪的示例，请参阅 “示例 2：跟踪 URL”部分 （第 D-3 页）。

提示　要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

备注　可以在 “网站 (Web Sites)”页面上生成或安排报告以获取相关信息。有关更多信息，请参阅 “关于计划报告和按需 Web 报告”部分 （第 5-29 页）。

URL 类别报告

网络 (Web) > 报告 (Reporting) > URL 类别 (URL Categories) 页面可用于查看系统中的用户正在访问的站点的 URL 类别。

在 **URL 类别 (URL Categories)** 页面中，可以查看以下信息：

表 5-6　网络 (Web) > 报告 (Reporting) > URL 类别 (URL Categories) 页面的详细信息

部分	说明
时间范围 （下拉列表）	选择报告的时间范围。有关详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
按事务总数排名靠前的 URL 类别	此部分以图形格式列出在站点上访问的排名靠前的 URL 类别。
按阻止和警告的事务数排名靠前的 URL 类别	此部分以图形格式列出按事务触发阻止或警告操作的排名靠前的 URL。例如，用户访问特定 URL，并且由于已有具体的策略，因此触发了阻止操作或警告。然后，该 URL 会在此图形中作为阻止或警告事务列出。
匹配的 URL 类别	“匹配的 URL 类别 (URL Categories Matched)”部分按 URL 类别显示指定时间范围内的事务处理结果，以及每个类别中使用的带宽量以及花费的时间。 如果有大量未分类的 URL，请参阅减少未分类的 URL （第 5-13 页）。
绕过的 URL 过滤	表示策略、端口以及在 URL 过滤之前发生的管理员用户代理阻止。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

备注

- 要生成此页面可以提供的更详细报告，请参阅排名靠前的 URL 类别 - 扩展 （第 5-31 页）。
- 如果在针对 URL 类别的计划报告中使用了数据可用性，并且任何设备的数据中存在差距，则会在页面底部显示以下信息：“`Some data in this time range was unavailable.`”如果没有差距，则不会显示任何内容。

减少未分类的 URL

如果未分类的 URL 的百分比高于 15- -20%，请考虑以下选项：

- 对于特定的本地化 URL，可以创建自定义 URL 类别并将其应用于特定用户或组策略。然后，这些事务将改为包含在 “绕过的 URL 过滤 (URL Filtering Bypassed)” 统计数据中。为此，请查看您的网络安全设备的在线帮助或用户指南，了解有关自定义 URL 类别的信息。
- 对于应包含在现有或其他类别中的站点，请参阅报告被错误分类和未分类的 URL （第 5-14 页）。

URL 类别集更新和报告

预定义的 URL 类别集可能会在安全管理设备上定期更新，如准备和管理 URL 类别集更新 （第 9-19 页）中所述。

当发生这些更新时，旧类别的数据将继续显示在报告和网络跟踪结果中，直到数据因太旧而无法包括在其中。在类别集更新后生成的报告数据将使用新的类别，因此，可能会在同一报告中显示新类别和旧类别。

如果在新旧类别的内容之间存在重叠，则可能需要更仔细地检查报告结果以获取有效的统计数据。例如，如果在所查看的时间段内 “即时消息” 和 “基于网络的聊天” 类别已合并到单个 “聊天和即时消息” 类别，则在合并之前对 “即时消息”

和 “基于网络的聊天” 类别中涵盖的站点进行的访问不会计入 “聊天和即时消息” 的总计中。同样，在合并之后对即时消息或基于网络的聊天站点的访问也不会包含在 “即时消息” 或 “基于网络的聊天” 类别的总计中。

将 URL 类别 (URL Categories) 页面与其他报告页面配合使用

“URL 类别 (URL Categories)” 页面可以与应用可视性报告和用户报告 (Web) 配合使用，以调查特定用户以及该特定用户尝试访问的应用或网站的类型。

例如，在 URL 类别报告中可以为人力资源部门生成高级别报告，其中详细说明站点访问的所有 URL 类别。在同一页面中，还可以在 “URL 类别 (URL Categories)” 交互式表格中收集有关 URL 类别 “流媒体 (Streaming Media)” 的更多详细信息。通过点击 “流媒体 (Streaming Media)” 类别链接，可以查看特定的 URL 类别报告页面。此页面不仅显示访问流媒体站点的排名靠前的用户 （在 “按事务总数类别排名靠前的用户 (Top Users by Category for Total Transactions)” 部分中），还会显示所访问的域 （在 “匹配的域 (Domains Matched)” 交互式表格中），例如 YouTube.com 或 QuickPlay.com。

此时，将会获得有关特定用户的越来越精细的信息。现在，我们假设此特定用户因其使用情况脱颖而出，并且您需要确切了解其访问的内容。此时，可以在 “用户 (Users)” 交互式表格中点击该用户。通过此操作可转到用户详细信息 （Web 报告），从中可以查看该用户的用户趋势，并准确地了解其在网络上进行的活动。

如果要查看更多内容，则现在可以通过点击交互式表格中的 “完成的事务数 (Transactions Completed)” 链接来详细了解网络跟踪详细信息。这会在 “网络跟踪 (Web Tracking)” 页面上显示搜索网络代理服务处理的事务，在此页面中可以查看有关用户访问站点的日期、完整 URL 以及在该 URL 上花费的时间等实际详细信息。

要查看如何使用 “URL 类别 (URL Categories)” 页面的其他示例，请参阅 “示例 3：调查访问的热门 URL 类别” 部分 （第 D-3 页）。

报告被错误分类和未分类的 URL

您可以在以下 URL 报告错误分类的和未分类的 URL：

https://securityhub.cisco.com/web/submit_urls

系统会评估提交内容以确定是否包含在后续规则更新中。

要检查已提交的 URL 的状态，请点击此页面上的**有关已提交 URL 的状态 (Status on Submitted URLs)** 选项卡。

应用可视性报告

备注 有关应用可视性的详细信息，请参阅网络安全设备的在线帮助或用户指南中的 “了解应用可视性与控件” 一章。

通过**网络 (Web) > 报告 (Reporting) > 应用可视性 (Application Visibility)** 页面，可以将应用控制用于安全管理设备和网络安全设备中的特定应用类型。

通过应用控制不仅可以比 URL 过滤更加精细地控制网络流量，例如，通过它可以更好地控制以下类型的应用和应用类型：

- 规避应用，例如匿名程序和加密隧道。
- 协作应用程序，例如 Cisco WebEx、 Facebook 和即时消息。
- 资源密集型应用，例如流媒体。

了解应用与应用类型之间的差异

务必要了解应用与应用类型之间的差异，以便可以控制报告涉及的应用。

- **应用类型。**包含一个或多个应用的类别。例如，**搜索引擎**是可包含搜索引擎 （例如 Google Search 和 Craigslist）的应用类型。即时消息是另一个应用类型类别，其可包含 Yahoo Instant Messenger 或 Cisco WebEx。 Facebook 也是一种应用类型。
- **应用。**属于应用类型的特定应用。例如， YouTube 是媒体应用类型中的应用。
- **应用行为。**用户可以在应用中完成的特定操作或行为。例如，用户可以在使用诸如 Yahoo Messenger 等应用期间传输文件。并非所有应用都包含可以配置的应用行为。

备注 要了解有关如何使用应用可视性与可控性 (AVC) 引擎以控制 Facebook 活动的详细信息，请参阅网络安全设备的在线帮助或用户指南中的 “了解应用可视性与可控性”一章。

在**应用可视性 (Application Visibility)** 页面中，可以查看以下信息：

表 5-7　网络 (Web) > 报告 (Reporting) > 应用可视性 (Application Visibility) 页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
按事务总数排名靠前的应用程序类型	此部分以图形格式列出在站点上访问的排名靠前的应用类别。例如，即时消息工具，如 Yahoo Instant Messenger、Facebook 和演示应用类型。
按受阻事务数排名靠前的应用程序	此部分以图形格式列出按事务触发阻止操作的排名靠前的应用类型。例如，某用户尝试启动特定类型的应用 （例如 Google Talk 或 Yahoo Instant Messenger），并且由于存在具体的策略，因此触发了阻止操作。然后，该应用会作为被阻止的事务或警告列出在此图形中。
匹配的应用程序类型	通过 “匹配的应用类型 (Application Types Matched)”交互式表格，可以查看有关“按事务总数排名靠前的应用类型 (Top Application Types by Total Transactions)”表格中列出的应用类型的粒度详细信息。在 “应用 (Applications)”列中，可以点击应用以查看详细信息
匹配的应用程序	“匹配的应用 (Applications Matched)”部分会显示指定时间范围内的所有应用。这是一个交互式表格，具有交互式列标题，可用来按需排序数据。 可以配置希望在 “匹配的应用 (Applications Matched)”部分中显示的列。有关为该部分配置列的详细信息，请参阅 “与网络安全报告一起使用”部分 （第 5-5 页）。 选择要在 “应用 (Applications)”表格中显示的特定项目后，可以从**显示的项目 (Items Displayed)** 下拉菜单中选择要显示的项目数。选项包括：10、 20、 50 或者 100。 此外，可以在 “匹配的应用 (Application Matched)”部分中查找特定应用。在该部分底部的文本字段中，输入特定应用名称并点击**查找应用 (Find Application)**。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

备注 可以在 “应用可视性 (Application Visibility)”页面上生成计划报告以获取相关信息。有关安排报告的信息，请参阅 “关于计划报告和按需 Web 报告”部分 （第 5-29 页）。

防恶意软件报告

网络 (Web) > 报告 (Reporting) > 防恶意软件 (Anti-Malware) 页面是一个与安全相关的报告页面，反映由启用的扫描引擎 （Webroot、 Sophos、 McAfee 和/或自适应扫描）扫描的结果。

使用此页面可帮助识别和监控基于网络的恶意软件威胁。

备注 要查看有关 L4 流量监视器找到的恶意软件的数据，请参阅 “L4 流量监视器报告”部分 （第 5-23 页）。

在**防恶意软件 (Anti-Malware)** 页面中，可以查看以下信息：

表 5-8　“网络 (Web)” > “报告 (Reporting)” > “防恶意软件 (Anti-Malware)”页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
排名靠前的恶意软件类别：监控或阻止	本部分显示根据指定的类别类型检测到的排名靠前的恶意软件类别。此信息以图形格式显示。有关有效恶意软件类别的详细信息，请参阅恶意软件类别说明 （第 5-17 页）。
排名靠前的恶意软件威胁：监控或阻止	此部分显示排名靠前的恶意软件威胁。此信息以图形格式显示。
恶意软件类别数 (Malware Categories)	“恶意软件类别数 (Malware Categories)”交互式表格显示有关在 “排名靠前的恶意软件类别 (Top Malware Categories)”图表中显示的特定恶意软件类别的详细信息。 点击 “恶意软件类别 (Malware Categories)”交互式表格中的任何链接，可以查看有关各个恶意软件类别以及其所在网络的更详细信息。 例外：通过该表格中的爆发启发式扫描链接，可以查看显示发生此类别事务的图表。 有关有效恶意软件类别的详细信息，请参阅恶意软件类别说明 （第 5-17 页）。
恶意软件威胁数	“恶意软件数 (Malware Threats)”交互式表格显示有关在 “排名靠前的恶意软件威胁 (Top Malware Threats)”部分中显示的特定恶意软件威胁的详细信息。 标有 “病毒爆发”及编号的威胁是自适应扫描功能独立于其他扫描引擎确定的威胁。 **注意** 按 “恶意软件威胁 (Malware Threat)”以升序对表格排序时，“未命名的恶意软件 (Unnamed Malware)”会显示在列表顶部。

提示 要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

恶意软件类别报告 (Malware Category Report)

通过 “恶意软件类别报告 (Malware Category Report)”页面，可以查看有关各个恶意软件类别及其在网络中进行的活动的详细信息。

要访问 “恶意软件类别报告 (Malware Category Report)”页面，请执行以下操作：

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 防恶意软件 (Anti-Malware)**。

步骤 2　在 “恶意软件类别 (Malware Categories)”交互式表格中，点击 “恶意软件类别 (Malware Category)”列中的一个类别。

步骤 3　要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

恶意软件威胁报告 (Malware Threat Report)

“恶意软件威胁报告 (Malware Threat Report)”页面显示存在特定威胁风险的客户端，并且显示一个列表来列出可能受感染的客户端以及指向 “客户端详细信息 (Client Detail)”页面的链接。该报告顶部的趋势图会显示在指定时间范围内有关某项威胁的受监控和受阻止事务。底部的表格显示在指定时间范围内某项威胁的受监控和受阻止事务的数量。

要查看此报告，请点击 “防恶意软件 (Anti-Malware)”报告页面上 “恶意软件类别 (Malware Category)”列中的某个类别。

有关其他信息，请点击表格下方的**支持门户恶意软件详细信息 (Support Portal Malware Details)**链接。

备注　可以在 “防恶意软件 (Anti-Malware)”页面上为检测到的排名靠前的恶意软件类别和检测到的排名靠前的恶意软件威胁生成计划报告，但是不能从恶意软件类别和恶意软件威胁报告页面安排生成的报告。有关安排报告的信息，请参阅“关于计划报告和按需 Web 报告”部分 （第 5-29 页）。

恶意软件类别说明

网络安全设备可以阻止以下类型的恶意软件：

恶意软件类型	说明
广告程序	广告软件包括将用户转至进行销售的产品的所有软件可执行文件和插件。一些广告软件应用具有同时运行并且相互监控的单独进程，确保修改是永久性的。一些变体会启用自身以在每次计算机启动时运行。这些程序还可以更改安全设置，使用户无法更改其浏览器搜索选项、桌面和其他系统设置。
浏览器助手对象	浏览器助手对象是可执行与提供广告或劫持用户设置相关的各种功能的浏览器插件。
商业系统监视程序	商业系统监视程序是具有系统监视特征的一种软件，可通过法律途径使用合法许可证获取。
拨号程序	拨号程序是利用调制解调器或其他类型的互联网访问连接到电话线或站点的程序，这会在用户未提供完全、有意义且明智授权的情况下产生长途费用。

恶意软件类型	说明
常规间谍软件	间谍软件是在计算机上安装的一种类型的恶意软件，可在用户不知情的情况下收集关于用户的少量信息。
劫持程序	劫持程序会修改系统设置或对用户系统进行任何不需要的更改，从而将用户转至某个网站或未得到用户完全、有意义且明智授权的情况下运行程序。
其他恶意软件	此类别用于捕获与任何定义的类别不能完全匹配的所有其他恶意软件和可疑行为。
病毒爆发启发式扫描	此类别表示自适应扫描独立于其他防恶意软件引擎发现的恶意软件。
网络钓鱼 URL	网络钓鱼 URL 会显示在浏览器地址栏中。有时，它涉及使用域名和假冒合法的域。网络钓鱼是一种形式的在线身份盗窃程序，可利用社会工程和技术手段来窃取个人身份数据和财务帐户凭据。
PUA	潜在不需要的应用。 PUA 不是恶意应用，但是可被视为不需要的应用。
系统监视程序	系统监视程序包含执行以下一种操作的任何软件： 公开或秘密记录系统进程和/或用户操作。 使这些记录可用于在以后进行检索和查看。
特洛伊木马下载程序	特洛伊木马下载程序是一种特洛伊木马，在安装后，会与远程主机/站点联系并安装来自远程主机的程序包或附属程序。这些安装通常在未得到用户确认的情况下进行。此外，特洛伊木马下载程序的负载可能因安装而异，因为它从远程主机/站点获取下载指令。
特洛伊木马	特洛伊木马是仿冒成安全程序的一种破坏性程序。与病毒不同，特洛伊木马不能自我复制。
特洛伊木马钓鱼程序	特洛伊木马钓鱼程序可能位于受感染的计算机上以等待要访问的特定网页，或者可能扫描受感染的计算机以查找银行站点、拍卖会站点或在线支付站点的用户名和密码。
病毒	病毒是在未得到用户确认的情况下加载到用户计算机上的程序或一段代码，并且它们违反用户意愿运行。
蠕虫	蠕虫是通过计算机网络自我复制的程序或算法，而且通常执行恶意操作。

高级恶意软件防护 （文件信誉和文件分析）报告

- 有关文件分析报告详细信息的要求 （第 5-19 页）
- 通过 SHA-256 哈希识别文件 （第 5-19 页）
- 高级恶意软件保护 （文件信誉和文件分析）报告页面 （第 5-19 页）
- 查看其他报告中的文件信誉过滤数据 （第 5-20 页）
- 关于网络跟踪和高级恶意软件保护功能 （第 5-40 页）

有关文件分析报告详细信息的要求

为了获取文件分析报告详细信息，设备必须能够通过端口 443 连接到文件分析服务器。请参阅附录 C “防火墙信息”中的详细信息。

如果安全管理设备没有直接连接到互联网，请为此流量配置一个代理服务器 （请参阅升级和更新设置 （第 14-18 页）。）如果已将设备配置为使用代理获取升级和服务更新，则会使用现有的设置。

如果使用 HTTPS 代理，则该代理不得解密流量；使用传递机制与文件分析服务器进行通信。该代理服务器必须信任来自文件分析服务器的证书，但是，不需要向文件分析服务器提供自己的证书。

有关任何其他要求，请参阅与安全管理设备版本对应的版本说明，该版本说明可从以下位置获取：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。

通过 SHA-256 哈希识别文件

由于文件名很容易更改，因此设备会使用安全哈希算法 (SHA-256) 为每个文件生成标识符。如果设备处理具有不同名称的同一文件，则所有实例都被识别为相同的 SHA-256。如果多个设备处理相同的文件，则该文件的所有实例都具有相同的 SHA-256 标识符。

在大多数报告中，会按文件的 SHA-256 值 （以缩写的格式）列出文件。要识别与组织中的某个恶意软件实例关联的文件名，请选择 “报告 (Reporting)” > “高级恶意软件保护 (Advanced Malware Protection)”，然后点击表格中的 SHA-256 链接。详细信息页面会显示关联文件名。

高级恶意软件保护 （文件信誉和文件分析）报告页面

报告	说明
高级恶意软件防护	显示由文件信誉服务识别的基于文件的威胁。 要查看尝试访问每个 SHA 的用户以及与该 SHA-256 关联的文件名，请点击表格中的 SHA-256。 点击 “恶意软件威胁文件详细信息 (Malware Threat File Details)”报告页面底部的链接，会在网络跟踪中显示在最大可用时间范围内遇到的该文件的所有实例，不管为该报告选择什么时间范围都是如此。 对于更改了裁定的文件，请参阅 AMP 裁定更新报告。这些裁定不会反映在 “高级恶意软件保护 (Advanced Malware Protection)”报告中。 如果从一个压缩或存档文件中提取的文件是恶意文件，则该压缩或存档文件的 SHA 值会包含在 “高级恶意软件保护 (Advanced Malware Protection)”报告中。

报告	说明
文件分析	显示发送进行分析的每个文件的时间和裁定 （或临时裁定）。 要查看超过 1000 个文件分析结果，请将数据导出为 .csv 文件。 深入查看详细分析结果，包括每个文件的威胁特征和得分。 还可以搜索云服务以了解有关 SHA 的更多信息。该链接位于结果详细信息页面上。 另请参阅有关文件分析报告详细信息的要求 （第 5-19 页）。 如果从一个压缩或存档文件中提取的文件已发送进行分析，只有该提取文件的 SHA 值会包含在 “文件分析 (File Analysis)” 报告中。
AMP 裁定更新	列出由设备处理且在事务处理后已更改裁定的文件。有关此情况的详细信息，请参阅网络安全设备的相应文档。 要查看超过 1000 个裁定更新，请将数据导出为 .csv 文件。 如果单个 SHA-256 具有多个裁定更改，此报告仅会显示最新的裁定，而不是裁定历史记录。 如果多个网络安全设备对于同一文件具有相同的裁定更新，则会显示具有最新时间戳的结果。 点击 SHA-256 链接会显示在最大可用时间范围内包括此 SHA-256 的所有事务的网络跟踪结果，不论为报告选择的是哪种时间范围。 要查看在最大可用时间范围内 （无论为报告选择什么时间范围）特定 SHA-256 的所有受影响的事务，请点击 “恶意软件威胁文件 (Malware Threat Files)” 页面底部的链接。

查看其他报告中的文件信誉过滤数据

用于文件信誉和分析的数据会在其他相关的报告中提供。默认情况下，“被高级恶意软件保护阻止 (Blocked by Advanced Malware Protection)” 列可能在适用的报告中隐藏。要显示其他列，请点击表格下方的 “列 (Columns)” 链接。

“按用户地点分类的报告 (Report by User Location)” 包括一个 “高级恶意软件保护 (Advanced Malware Protection)” 选项卡。

客户端恶意软件风险报告

网络 (Web) > 报告 (Reporting) > 客户端恶意软件风险 (Client Malware Risk) 页面是与安全相关的报告页面，可用于监控客户端恶意软件风险活动。

从 “客户端恶意软件风险 (Client Malware Risk)” 页面，系统管理员可以查看哪些用户遇到了最多的阻止或警告。根据此页面收集的信息，管理员可以点击用户链接以查看该用户在网络上进行什么活动导致他们遇到如此多的阻止或警告，并引发比网络中的其他用户更多的检测。

此外，“客户端恶意软件风险 (Client Malware Risk)” 页面会列出常见恶意软件连接中涉及的客户端 IP 地址 （如 L4 流量监视器 (L4TM) 确定的 IP 地址）。经常连接到恶意站点的计算机可能感染尝试连接到一台集中命令和控制服务器的恶意软件，并且应当进行杀毒。

表 5-9 介绍有关 “客户端恶意软件风险 (Client Malware Risk)” 页面的信息。

表 5-9　客户端恶意软件风险报告组件

部分	说明
时间范围 （下拉列表）	可用于选择报告中所含数据的时间范围的菜单。有关详细信息，请参阅选择报告的时间范围 （第 3-4 页）。
网络代理：监控或阻止的排名靠前的客户端 (Web Proxy: Top Clients Monitored or Blocked)	此图表显示遇到恶意软件风险的前十个用户。
L4 流量监视器：检测到的恶意软件连接数 (L4 Traffic Monitor: Malware Connections Detected)	此图表显示贵组织中最频繁地连接到恶意软件站点的十台计算机的 IP 地址。 此图表与 L4 流量监视器报告 （第 5-23 页）上的 “排名靠前的客户端 IP (Top Client IPs)” 图表相同。请参阅该部分了解更多信息和图表选项。
网络代理: 客户端恶意软件风险 (Web Proxy: Client Malware Risk)	“网络代理: 客户端恶意软件风险 (Web Proxy: Client Malware Risk)” 表格显示有关 “网络代理: 按恶意软件风险排名靠前的客户端 (Web Proxy: Top Clients by Malware Risk)” 部分中显示的特定客户端的详细信息。 您可以在此表中点击每个用户，以查看与该客户端相关联的 “用户详细信息” (User Details) 页。有关该页面的详细信息，请参阅用户详细信息 （Web 报告）（第 5-10 页）。 点击该表格中的任何链接可以查看有关各个恶意软件类别，及其执行什么活动来触发恶意软件风险的更精细的详细信息。例如，点击 “用户 ID/客户端 IP 地址 (User ID / Client IP Address)” 列中的链接可转到该用户的 “用户 (User)” 页面。
L4 通信监控: 按恶意软件风险排名的客户端	此表格显示贵组织中最频繁地连接到恶意软件站点的计算机的 IP 地址。 此表格与 L4 流量监视器报告 （第 5-23 页）上的 “客户端源 IP (Client Source IPs)” 表格相同。有关使用此表格的信息，请参阅该部分。

提示　要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

网络信誉过滤器报告

网络 (Web) > 报告 (Reporting) > 网络信誉过滤器 (Web Reputation Filters) 是与安全相关的报告页面，可用于查看在指定的时间范围内为事务设置的网络信誉过滤器的结果。

什么是网络信誉过滤器？

网络信誉过滤器会分析网络服务器行为并为 URL 分配信誉分数，以确定其包含基于 URL 的恶意软件的可能性。它有助于防御会威胁最终用户隐私和敏感公司信息的基于 URL 的恶意软件。网络安全设备使用 URL 信誉分数来识别可疑活动并提前阻止恶意软件攻击，避免其发生。可以将网络信誉过滤器与访问和加密策略配合使用。

网络信誉过滤器使用统计学上非常重要的数据来评估互联网域的可靠性并为 URL 的信誉评分。许多数据可用于判断给定 URL 的可信度，例如，特定域的注册时长、网站的托管位置，或者网络服务器是否使用动态 IP 地址等。

网络信誉计算会将 URL 与网络参数相关联，以确定存在恶意软件的可能性。然后，存在恶意软件的聚合可能性会映射到介于 -10 和 +10 之间的网络信誉评分，其中 +10 表示最不可能包含恶意软件。

参数示例包括以下内容：

- URL 分类数据
- 是否存在可下载的代码
- 是否存在冗长、模糊的最终用户许可协议 (EULA)
- 全局数量和数量更改
- 网络所有者信息
- URL 的历史记录
- URL 的时限
- 是否存在于任何阻止列表中
- 是否存在于任何允许列表中
- 常见域的 URL 拼写错误
- 域注册商信息
- IP 地址信息

有关网络信誉过滤的详细信息，请参阅网络安全设备在线帮助或用户指南中的“网络信誉过滤器”。

在**网络信誉过滤器 (Web Reputation Filters)** 页面中，可以查看以下信息：

表 5-10　网络 (Web) > 报告 (Reporting) > 网络信誉过滤器 (Web Reputation Filters) 页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
网络信誉操作 （趋势） (Web Reputation Actions (Trend))	此部分以图形格式根据指定的时间 （水平时间轴）显示网络信誉操作总数 （纵坐标）。在这里，可以查看网络信誉操作随着时间的推移呈现的潜在趋势。
Web 声誉操作(容量)	此部分按事务以百分比的形式显示网络信誉操作数量。
按受阻事务数排名的 Web 声誉威胁类型	此部分显示被阻止的网络信誉类型。

表 5-10　网络 (Web) > 报告 (Reporting) > 网络信誉过滤器 (Web Reputation Filters) 页面的详细信息 （续）

部分	说明
按进一步扫描的事务数排名的 Web 声誉威胁类型	如果启用了自适应扫描功能，则此部分显示捕获的潜在威胁事务数。 如果未启用自适应扫描功能，则此部分显示由于此操作而被阻止的网络信誉类型，并且需要进一步扫描。如果网络信誉过滤的结果是 “进一步扫描 (Scan Further)”，则事务会传递到防恶意软件工具以进行其他扫描。
Web 声誉操作(按分数分解)	如果未启用自适应扫描功能，此交互式表格会显示针对每项操作细分的网络信誉分数。

提示　要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

调整网络信誉设置 (Adjusting Web Reputation Settings)

根据报告结果，可能需要调整配置的网络信誉设置，例如调整阈值分数或者启用或禁用自适应扫描功能。有关配置网络信誉设置的具体信息，请参阅您的网络安全设备的在线帮助或用户指南。

L4 流量监视器报告

网络 (Web) > 报告 (Reporting) > L4 流量监视器 (L4 Traffic Monitor) 页面会显示有关上网络安全设备的 L4 流量监视器在指定的时间范围内检测到的恶意软件端口和恶意软件站点的信息。它还会显示经常遇到恶意软件站点的客户端的 IP 地址。

L4 流量监视器会监听通过每个网络安全设备上的所有端口传入的网络流量,并且将域名称和 IP 地址与其自己的数据库表中的条目进行匹配，以确定是否允许传入和传出流量。

可以使用此报告中的数据来确定是阻止端口或站点，还是调查某个特定客户端 IP 地址反常地频繁连接到恶意软件站点的原因 （例如，这可能是因为与该 IP 地址关联的计算机感染了尝试连接到一台集中命令和控制服务器的恶意软件）。

提示　要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

表 5-11　L4 流量监视器报告页面组件

部分	说明
时间范围 （下拉列表）	用于选择要报告的时间范围的菜单。有关详细信息，请参阅选择报告的时间范围 （第 3-4 页）。
排名靠前的客户端 IP (Top Client IPs)	此部分以图形格式显示贵组织中最频繁连接到恶意软件站点的计算机的 IP 地址。 点击该图表下方的 “图表选项 (Chart Options)” 链接可将显示从 “检测到的恶意软件连接总数 (Malware Connections Detected)” 更改为 “监控的恶意软件连接 (Malware Connections Monitored)” 或 “阻止的恶意软件连接 (Malware Connections Blocked)”。 此图表与客户端恶意软件风险报告 （第 5-20 页）上的 “L4 流量监视器：检测到的恶意软件连接数” 图表相同。
恶意软件最多的网站	此部分以图形格式显示 L4 流量监视器检测到的排名靠前的恶意软件域。 点击该图表下方的 “图表选项 (Chart Options)” 链接可将显示从 “检测到的恶意软件连接总数 (Malware Connections Detected)” 更改为 “监控的恶意软件连接 (Malware Connections Monitored)” 或 “阻止的恶意软件连接 (Malware Connections Blocked)”。
客户端源 IP (Client Source IPs)	此表格显示贵组织中经常连接到恶意软件站点的计算机的 IP 地址。 要仅包括特定端口的数据，请在表格底部的框中输入端口号，然后点击 “按端口过滤 (Filter by Port)”。可以使用此功能帮助确定向恶意软件站点 “汇报” 的恶意软件使用的端口。 要查看诸如每个连接的端口和目标域等详细信息，请点击表格中的条目。例如，如果一个特定客户端 IP 地址具有大量阻止的恶意软件连接，请点击该列以查看列出每个阻止的连接的列表。该列表在 “网络 (Web)” > “报告 (Reporting)” > “网络跟踪 (Web Tracking)” 页面的 “L4 流量监视器 (L4 Traffic Monitor)” 选项卡中显示为搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监视器处理的事务 （第 5-38 页）。 此表格与客户端恶意软件风险报告 （第 5-20 页）上的 “L4 流量监视器 - 按恶意软件风险排名的客户端” 表格相同。

表 5-11　L4 流量监视器报告页面组件 （续）

部分	说明
恶意软件端口 (Malware Ports)	此表格显示 L4 流量监视器在其上最常检测到恶意软件的端口。 要查看详细信息，请点击表格中的条目。例如，点击 “检测到的恶意软件连接总数 (Total Malware Connections Detected)” 对应的数字可查看该端口上各个连接的详细信息。该列表在 “网络 (Web)” > “报告 (Reporting)” > “网络跟踪 (Web Tracking)” 页面的 “L4 流量监视器 (L4 Traffic Monitor)” 选项卡中显示为搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监视器处理的事务 （第 5-38 页）。
检测到的恶意软件站点数	此表格显示 L4 流量监视器在其上最常检测到恶意软件的域。 要仅包括特定端口的数据，请在表格底部的框中输入端口号，然后点击 “按端口过滤 (Filter by Port)”。可以使用此功能帮助确定是否阻止站点或端口。 要查看详细信息，请点击表格中的条目。例如，点击 “阻止的恶意软件连接 (Malware Connections Blocked)” 对应的数字可查看特定站点上每个被阻止连接的列表。该列表在 “网络 (Web)” > “报告 (Reporting)” > “网络跟踪 (Web Tracking)” 页面的 “L4 流量监视器 (L4 Traffic Monitor)” 选项卡中显示为搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监视器处理的事务 （第 5-38 页）。

提示　要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

相关主题

- L4 流量监视器报告故障排除 （第 5-43 页）

SOCKS 代理报告

通过**网络 (Web) > 报告 (Reporting) > SOCKS 代理 (SOCKS Proxy)** 页面，可以查看通过 SOCKS 代理处理的事务的数据和趋势，包括有关目标和用户的信息。

备注　在报告中显示的目标是 SOCKS 客户端 （通常是浏览器）发送到 SOCKS 代理的地址。

要更改 SOCKS 策略设置，请参阅您的网络安全设备的在线帮助或用户指南。

相关主题

- 搜索 SOCKS 代理处理的事务 （第 5-39 页）

按用户地点分类的报告

通过**网络 (Web) > 按用户地点分类的报告 (Reports by User Location)** 页面，可以了解移动用户在其本地或远程系统中进行的活动。

具体活动包括：

- 本地和远程用户正在访问的 URL 类别。
- 本地和远程用户访问的站点所触发的防恶意软件活动。
- 本地和远程用户访问的站点的网络信誉。
- 本地和远程用户访问的应用。
- 用户 （本地和远程）。
- 本地和远程用户访问的域。

在**按用户地点分类的报告 (Reports by User Location)** 页面中，可以查看以下信息：

表 5-12　网络 (Web) > 报告 (Reporting) > 按用户地点分类的报告 (Reports by User Location) 页面的详细信息

部分	说明
时间范围 （下拉列表）	一个下拉列表，范围可以从 1 天到 90 天，也可以自定义范围。有关时间范围以及根据自己的需求自定义时间范围的详细信息，请参阅 “选择报告的时间范围”部分 （第 3-4 页）。
网络代理活动总数：远程用户 (Total Web Proxy Activity: Remote Users)	此部分以图形格式显示远程用户在指定时间 （水平坐标）内的活动 （纵坐标）。
Web 代理摘要	此部分显示系统上本地和远程用户的活动摘要。
网络代理活动总数：本地用户 (Total Web Proxy Activity: Local Users)	此部分以图形格式显示远程用户在指定时间 （水平坐标）内的活动 （纵坐标）。
检测到的可疑事务数：远程用户 (Suspect Transactions Detected: Remote Users)	此部分以图形格式显示由于为远程用户定义的访问策略，已在指定时间内 （水平坐标）检测到的可疑事务数 （纵坐标）。
可疑事务摘要	此部分显示系统上远程用户的可疑事务摘要。
检测到的可疑事务数：本地用户 (Suspect Transactions Detected: Local Users)	此部分以图形格式显示由于为远程用户定义的访问策略，已在指定时间内 （水平坐标）检测到的可疑事务数 （纵坐标）。
可疑事务摘要	此部分显示系统中本地用户的可疑事务摘要。

在**按用户地点分类的报告 (Reports by User Location)** 页面中，可以生成显示本地和远程用户活动的报告。这样可以轻松比较用户的本地和远程活动。

提示　要自定义此报告的视图，请参阅与网络安全报告一起使用 （第 5-5 页）。

备注　可以在 “按用户地点分类的报告 (Reports by User Location)”页面上生成计划报告以获取相关信息。有关安排报告的信息，请参阅 “关于计划报告和按需 Web 报告”部分 （第 5-29 页）。

系统容量页面

通过**网络 (Web) > 报告 (Reporting) > 系统容量 (System Capacity)** 页面，可以查看网络安全设备在安全管理设备上施加的总体工作负载。最重要的是，可以使用 “系统容量 (System Capacity)” 页面来跟踪容量随着时间的增长情况并针对系统容量进行规划。监控网络安全设备可确保容量适合工作负载量。随着时间的推移，邮件量会不可避免地增加，适当的监控可确保主动添加容量或进行配置更改。

“系统容量 (System Capacity)” 页面可用于确定以下信息：

- 确定网络安全设备何时超出推荐的 CPU 容量。这可用于确定何时需要优化配置或添加设备。
- 要进行故障排除，需确定系统的哪些部分使用大多数资源。
- 确定响应时间和代理缓冲内存。
- 确定每秒事务数，以及未完成的任何连接。

查看系统容量报告

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 系统容量 (System Capacity)**。

步骤 2　要查看不同类型的数据，请点击**列 (Columns)** 并选择要查看的数据。

步骤 3　要查看单个设备的系统容量，请点击 “平均使用和性能概述 (Overview of Averaged Usage and Performance)” 表格中网络安全设备列中的设备。

将显示该设备的系统容量图。该页面上的图分为两个集：

- 系统容量 - 系统负载
- 系统容量 - 网络负载

如何解释在系统容量页面上看到的数据

在 “系统容量 (System Capacity)” 页面上选择查看数据的时间范围时，务必记住以下内容：

- 每日报告 - 每日报告会查询每小时表格，并显示设备在过去 24 小时内每小时接收的确切查询数。此信息从每小时表格中收集。
- 每月报告 - 每月报告会查询 30 或 31 天的每日表格（根据月中的天数），从而提供有关 30 或 31 天内的查询数的确切报告。这同样是一个精确的数字。

“系统容量 (System Capacity)” 页面上的 “最大 (Maximum)” 值指示器是在指定时段内看到的最大值。“平均 (Average)” 值是指定时段内所有值的平均值。时段聚合取决于为该报告选择的间隔。例如，如果图表用于一个月的时段，则可以选择查看每天的平均值和最大值。

备注　如果为其他报告的时间范围选择**年 (Year)**，我们建议选择最大的时间范围，即 90 天。

系统容量 - 系统负载

“系统容量 (System Capacity)”窗口中的前四个图形显示系统负载报告。这些报告会显示设备上的整体 CPU 使用情况。AsyncOS 经过优化，可使用空闲 CPU 资源来提高事务吞吐量。高 CPU 使用率并不一定表示存在系统容量问题。如果高 CPU 使用率与持续的大容量内存页面交换一同出现，则可能表示存在容量问题。该页面还会显示一个图形，从中显示不同功能 （包括对网络安全设备报告的处理）使用的 CPU 量。按功能显示的 CPU 图表可指示产品的哪些部分占用系统上的大多数资源。如果需要优化设备，则此图有助于确定哪些功能可能需要调整或禁用。

此外，响应时间/延迟和每秒事务数图形会显示总体响应时间 （以毫秒为单位），以及在 “时间范围 (Time Range)”下拉菜单中指定的日期范围内的每秒事务数。

系统容量 - 网络负载

“系统容量 (System Capacity)”窗口中的下一个图会显示传出连接数、用于传出的带宽以及代理缓冲内存统计数据。可以查看一天、一周、一个月或一年的结果。了解环境中的正常负载量和负载量峰值趋势至关重要。

代理缓冲内存可以指示正常操作期间的网络流量峰值，但是如果图形稳定上升到最大值，则设备可能达到最大容量，并且应该考虑添加容量。

这些图表与系统容量 - 系统负载 （第 5-28 页）中所述的图表位于相同的页面上，并且位于那些图表的下方。

有关代理缓冲内存交换的说明

系统旨在定期交换代理缓冲内存，因此，预期会进行一些代理缓冲内存交换，这并不表示设备存在问题。除非系统*持续*大量交换代理缓冲内存，否则代理缓冲内存交换是正常的预期行为。如果系统运行极高的负载量且由于高负载量而持续交换代理缓冲内存，则可能需要将网络安全设备添加到网络或调整配置以确保最大吞吐量，从而提高性能。

数据可用性页面

网络 (Web) > 报告 (Reporting) > 数据可用性 (Data Availability) 页面提供有关每个托管网络安全设备的安全管理设备上具有可用报告和网络跟踪数据的日期范围。

备注　如果禁用了 Web 报告，则不会从网络安全设备提取任何新数据，但是以前检索的数据仍存在于安全管理设备中。

如果 Web 报告的 “从 (From)”和 “到 (To)”列与 Web 报告和跟踪的 “从 (From)”和 “到 (To)”列之间具有不同的状态，则 “状态 (Status)”列中会显示最严重的后果。

有关清除数据的信息，请参阅 “管理磁盘空间”部分 （第 14-45 页）。

备注　如果在针对 URL 类别的计划报告中使用了数据可用性，并且任何设备的数据中存在差距，则会在页面底部显示以下信息：“Some data in this time range was unavailable.”
如果没有差距，则不会显示任何内容。

关于计划报告和按需 Web 报告

除非有相应说明，否则可以生成以下类型的网络安全报告作为计划报告或按需报告：

- Web 报告概述 - 有关在此页面包含的内容的信息，请参阅 “Web 报告概述”部分 （第 5-8 页）。
- 用户 - 有关在此页面包含的内容的信息，请参阅 “用户报告 (Web)”部分 （第 5-9 页）。
- 网站 - 有关在此页面包含的内容的信息，请参阅 “网站报告”部分 （第 5-11 页）。
- URL 类别 - 有关在此页面包含的内容的信息，请参阅 “URL 类别报告”部分 （第 5-12 页）。
- 排名靠前的 URL 类别 - 扩展：有关如何为“排名靠前的 URL 类别 - 扩展”生成报告的信息，请参阅排名靠前的 URL 类别 - 扩展 （第 5-31 页）。

  此报告不可作为按需报告。
- 应用可视性 - 有关在此页面包含的内容的信息，请参阅 “应用可视性报告”部分 （第 5-14 页）。
- 排名靠前的应用类别 - 扩展：有关如何为“排名靠前的应用类别 - 扩展”生成报告的信息，请参阅排名靠前的应用类型 - 扩展 （第 5-32 页）。

  此报告不可作为按需报告。
- 防恶意软件 - 有关在此页面包含的内容的信息，请参阅 “防恶意软件报告”部分 （第 5-16 页）。
- 客户端恶意软件风险 - 有关在此页面包含的内容的信息，请参阅 “客户端恶意软件风险报告”部分 （第 5-20 页）。
- 网络信誉过滤器 - 有关在此页面包含的内容的信息，请参阅 “网络信誉过滤器报告”部分 （第 5-21 页）。
- L4 流量监视器 - 有关在此页面包含的内容的信息，请参阅 “L4 流量监视器报告”部分 （第 5-23 页）。
- 移动安全解决方案 - 有关在此页面包含的内容的信息，请参阅 “按用户地点分类的报告”部分 （第 5-26 页）。
- 系统容量 - 有关在此页面包含的内容的信息，请参阅 “系统容量页面”部分 （第 5-27 页）。

安排 Web 报告

本节包括以下主题：

备注 可以选择使用户名在所有报告中都不可识别。有关信息，请参阅在 Web 报告中使用匿名 （第 5-4 页）。

可以安排报告每日、每周或每月运行。可以配置计划报告以包括前一天、前七天、上个月、以前日历日 （多达 250 天）、以前日历月 （多达 12 个月）的数据。或者，可以包含自定义天数 （从 2 天到 100 天）或自定义月数 （从 2 个月到 12 个月）的数据。

无论何时运行报告，都会从以前的时间间隔 （小时、天、星期或月）返回数据。例如，如果安排每日报告在凌晨 1 点运行，则该报告将包含上一日的数据，从午夜到午夜 （00:00 到 23:59）。

可以根据需要为报告定义任意数量的收件人，包括零个收件人。如果不指定邮件收件人，则系统仍会将报告存档。但是，如果需要将报告发送至大量地址，则可能需要创建邮件列表而不是列出各个收件人。

存储安排的 Web 报告

会保留其生成的最新报告 - 对于每个计划报告，可包含多达 30 个最近的实例，并且对于所有报告，可包含 1000 个总版本。

存档的报告会自动删除。在添加新报告时，会删除较旧的报告以使数量保持在 1000。最多可将 30 个实例应用到具有相同名称和时间范围的计划报告。

存档的报告存储在设备上的 `/periodic_reports` 目录中。（有关详细信息，请参阅附录 A “IP 接口和设备访问”。）

相关主题

- 查看和管理存档的 Web 报告 （第 5-34 页）

添加安排的 Web 报告

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 计划报告 (Scheduled Reports)**。

步骤 2　点击**添加计划的报告 (Add Scheduled Report)**。

步骤 3　在**类型 (Type)** 旁边的下拉菜单中，选择报告类型。

步骤 4　在**标题 (Title)** 字段中，键入报告的标题。

要避免创建具有相同名称的多个报告，我们建议使用描述性标题。

步骤 5　从**时间范围 (Time Range)** 下拉菜单中，选择报告的时间范围。

步骤 6　选择所生成的报告的格式。

默认格式为 PDF。大多数报告还允许将原始数据另存为 CSV 文件。

步骤 7　从**项目数量 (Number of Items)** 旁的下拉列表中，选择要包含在生成的报告中的项目数量。

有效值为 2 到 20。默认值为 5。

步骤 8　对于**图表 (Charts)**，请点击**要显示的数据 (Data to display)** 下的默认图表，然后选择要在报告的每个图表中显示的数据。

步骤 9　从**排序列 (Sort Column)** 旁的下拉列表中，为此报告选择作为数据排序依据的列。通过该操作可以按照计划报告中可用的任何列创建包含前 “N” 个项目的计划报告。

步骤 10　从**安排 (Schedule)** 区域中，为计划报告选择天、周或月旁边的单选按钮。

步骤 11　在**邮件 (Email)** 文本字段中，键入将生成的报告发送到的邮件地址。

如果不指定邮件地址，则仅存档该报告。

步骤 12　点击 **Submit**。

编辑安排的 Web 报告

要编辑报告，请转到**网络 (Web) > 报告 (Reporting) > 计划报告 (Scheduled Reports)** 页面，然后选中与要编辑的报告对应的复选框。修改设置，然后点击**提交 (Submit)** 提交在页面上进行的更改，然后点击**确认更改 (Commit Changes)** 按钮以确认对设备进行的更改。

删除安排的 Web 报告

要删除报告，请转到**网络 (Web) > 报告 (Reporting) > 计划报告 (Scheduled Reports)** 页面，然后选中与要删除的报告对应的复选框。要删除所有计划报告，请选中**全部 (All)** 复选框，然后**删除**并**确认**更改。请注意，已删除报告的存档版本不会被删除。

其他扩展 Web 报告

安全管理设备上还提供另外两个报告作为计划报告：

- 排名靠前的 URL 类别 - 扩展
- 排名靠前的应用类型 - 扩展

排名靠前的 URL 类别 - 扩展

排名靠前的 URL 类别 - 对于希望接收比 URL 类别报告提供的信息更加详细的信息的管理员，扩展报告非常有用。

例如，在典型的 URL 类别报告中，可以在较高的 URL 类别级别中收集测量特定员工使用的带宽的信息。要生成更详细的报告来监控每个 URL 类别的前十个 URL 的带宽使用情况，或每个 URL 类别的前五个用户，请使用 “排名靠前的 URL 类别 - 扩展 (Top URL Categories - Extended)”报告。

备注

- 使用此类型的报告可生成的最大报告数量为 20。
- 预定义的 URL 类别列表会不定期地更新。有关这些更新对报告结果的影响的详细信息，请参阅 URL 类别集更新和报告 （第 5-13 页）。

要生成“排名靠前的 URL 类别 - 扩展 (Top URL Categories - Extended)”报告，请执行以下操作：

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 计划报告 (Scheduled Reports)**。

步骤 2　点击**添加计划的报告 (Add Scheduled Report)**。

步骤 3　在 “类型 (Type)”旁边的下拉菜单中，选择**排名靠前的 URL 类别 - 扩展 (Top URL Categories - Extended)**。

步骤 4　在**标题 (Title)** 文本字段中，键入 URL 扩展报告的标题。

步骤 5　从**时间范围 (Time Range)** 下拉菜单中，选择报告的时间范围。

步骤 6　选择所生成的报告的格式。

默认格式为 PDF。

步骤 7　在**项目数量 (Number of Items)** 旁的下拉列表中，选择要包含在生成的报告中的 URL 类别数量。

有效值为 2 到 20。默认值为 5。

步骤 8　从“排序列 (Sort Column)”旁的下拉列表中，为此报告选择作为数据排序依据的列。通过该操作可以按照计划报告中可用的任何列创建包含前 “N”个项目的计划报告。

步骤 9　对于**图表 (Charts)**，请点击**要显示的数据 (Data to display)** 下的默认图表，然后选择要在报告的每个图表中显示的数据。

步骤 10　从**安排 (Schedule)** 区域中，为计划报告选择天、周或月旁边的单选按钮。

步骤 11　在**邮件 (Email)** 文本字段中，键入将生成的报告发送到的邮件地址。

步骤 12　点击 **Submit**。

排名靠前的应用类型 - 扩展

要生成“排名靠前的应用类型 - 扩展 (Top Application Type—Extended)”报告，请执行以下操作：

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 计划报告 (Scheduled Reports)**。

步骤 2　点击**添加计划的报告 (Add Scheduled Report)**。

步骤 3　在“类型 (Type)”旁边的下拉菜单中，选择**排名靠前的应用类型 - 扩展 (Top Application Types — Extended)**。

页面上的选项将更改。

步骤 4　在**标题 (Title)** 文本字段中，键入报告的标题。

步骤 5　从**时间范围 (Time Range)** 下拉菜单中，选择报告的时间范围。

步骤 6　选择所生成的报告的格式。

默认格式为 PDF。

步骤 7　在**项目数量 (Number of Items)** 旁的下拉列表中，选择要包含在生成的报告中的应用类型数量。

有效值为 2 到 20。默认值为 **5** 分钟。

步骤 8　在**排序列 (Sort Column)** 旁的下拉列表中，选择要显示在表格中的列数量。选项包括：“完成的事务数 (Transactions Completed)”、“阻止的事务数 (Transactions Blocked)”、“事务总数 (Transaction Totals)”。

步骤 9　对于**图表 (Charts)**，请点击**要显示的数据 (Data to display)** 下的默认图表，然后选择要在报告的每个图表中显示的数据。

步骤 10　从**安排 (Schedule)** 区域中，为计划报告选择天、周或月旁边的单选按钮。

步骤 11　在**邮件 (Email)** 文本字段中，键入将生成的报告发送到的邮件地址。

步骤 12　点击 **Submit**。

按需生成 Web 报告

对于可以安排的大多数报告，还可以按需生成。

备注　一些报告只能以计划报告的形式提供，不可按需生成。请参阅其他扩展 Web 报告 （第 5-31 页）。

要按需生成报告，请执行以下操作：

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

步骤 2　点击**立即生成报告 (Generate Report Now)**。

步骤 3　在**报告类型 (Report type)** 部分中，从下拉列表选择报告类型。

页面上的选项可能会更改。

步骤 4　在 “标题 (Title)” 文本字段中，键入报告的标题名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

步骤 5　从**要包括的时间范围 (Time Range to Include)** 下拉列表中，选择报告数据的时间范围。

步骤 6　在 “格式 (Format)” 部分中，选择报告的格式。

选项包括：

- **PDF**。创建格式化的 PDF 文档以用于传送和/或存档。可以通过点击 “预览 PDF 报告 (Preview PDF Report)” 来立即以 PDF 文件的形式查看报告。
- **CSV**。创建以逗号分隔值形式包含原始数据的 ASCII 文本文件。每个 CSV 文件都可包含多达 100 个行。如果报告包含多种类型的表格，则会为每个表格创建一个单独的 CSV 文件。

步骤 7　根据可用于报告的选项，选择：

- **行数 (Number of rows)**：要在表格中显示的数据行数。
- **图表 (Charts)**：要在报告的图表中显示的数据：
- 点击要显示的数据下的默认选项。
- **排序列 (Sort Column)**：作为每个表格的排序依据的列。

步骤 8　从 “发送选项 (Delivery Option)” 部分中，选择以下项：

- 如果希望此报告显示在 “存档的报告 (Archived Reports)” 页面上，请选中**存档报告 (Archive Report)** 复选框。

注　基于域的执行摘要报告无法存档。

- 选中**立即通过邮件发送给收件人 (Email now to recipients)** 复选框，通过邮件发送该报告。
- 在文本字段中，键入报告的收件人邮件地址。

步骤 9　点击**发送此报告 (Deliver This Report)** 以生成报告。

存档的 Web 报告页面

- 关于计划报告和按需 Web 报告
- 按需生成 Web 报告
- 查看和管理存档的 Web 报告

查看和管理存档的 Web 报告

使用此部分中的信息来处理作为计划报告生成的报告。

操作步骤

步骤 1 转到**网络 (Web) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。

步骤 2 要查看报告，请点击“报告标题 (Report Title)”列中的报告名称。“显示 (Show)”下拉菜单会过滤在**存档的报告 (Archived Reports)** 页面上列出的报告类型。

步骤 3 如果列表很长，要找到特定的报告，请通过从**显示 (Show)** 菜单中选择报告类型来过滤列表，或者点击某个列标题以按该列进行排序。

相关主题

- 存储安排的 Web 报告 （第 5-30 页）
- 添加安排的 Web 报告 （第 5-30 页）
- 按需生成 Web 报告 （第 5-33 页）

网络跟踪

使用 “网络跟踪 (Web Tracking)”页面搜索和查看有关各个事务或可能有关的事务模式的详细信息。根据部署使用的服务，在相关选项卡中进行搜索：

- 搜索网络代理服务处理的事务 （第 5-35 页）
- 搜索 L4 流量监视器处理的事务 （第 5-38 页）
- 搜索 SOCKS 代理处理的事务 （第 5-39 页）
- 使用网络跟踪搜索结果 （第 5-39 页）
- 查看网络跟踪搜索结果的事务详细信息 （第 5-40 页）

有关网络代理与 L4 流量监视器之间区别的更多信息，请参阅网络安全设备的在线帮助或用户指南中的 “了解网络安全设备如何工作”一节。

相关主题

- 关于网络跟踪和升级 （第 5-41 页）

搜索网络代理服务处理的事务

使用在**网络 (Web) > 报告 (Reporting) > Web 跟踪 (Web Tracking)** 页面中的 **代理服务 (Proxy Services)** 选项卡搜索从各个安全组件和可接受的使用实施组件聚合的网络跟踪数据。此数据不包括 SOCKS 代理处理的 L4 流量监视器数据或事务。

可能需要使用它来帮助以下角色：

- **HR 或法务经理。**在特定时段内，为员工运行调查报告。

  例如，可以使用 “代理服务 (Proxy Services)” 选项卡来检索有关用户访问的特定 URL、用户访问该 URL 的时间、是否允许该 URL 等信息。

- **网络安全管理员。**检查公司网络是否因员工使用智能手机而受到恶意软件威胁。

可以查看搜索结果以了解在特定时段记录的事务 （包括已阻止、监控、警告和完成的事务）。还可以使用多个条件过滤数据结果，例如 URL 类别、恶意软件威胁和应用。

备注 网络代理仅报告包含 ACL 决策标记而不是 “OTHER-NONE” 的事务。

有关网络跟踪使用情况的示例，请参阅 “示例 1：调查用户” 部分 （第 D-1 页）。

有关 “代理服务 (Proxy Services)” 选项卡如何与其他 Web 报告页面配合使用的示例，请参阅 “将 URL 类别 (URL Categories) 页面与其他报告页面配合使用” 部分 （第 5-13 页）。

操作步骤

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 网络跟踪 (Web Tracking)**。

步骤 2 点击**代理服务 (Proxy Services)** 选项卡。

步骤 3 要查看所有搜索和过滤选项，请点击**高级 (Advanced)**。

步骤 4 输入搜索条件：

表 5-13　代理服务 (Proxy Services) 选项卡上的网络跟踪搜索条件

选项	说明
默认搜索条件	
Time Range	选择要报告的时间范围。有关安全管理设备上可用的时间范围的信息，请参阅 “选择报告的时间范围” 部分 （第 3-4 页）。
用户/客户端 IPv4 或 IPv6	或者，输入报告中显示的身份验证用户名，或者输入要跟踪的客户端 IP 地址。还可以输入 CIDR 格式的 IP 范围，例如 172.16.0.0/16。 如果将此字段留空，则搜索将返回所有用户的结果。
网站	或者，输入要跟踪的网站。如果将此字段留空，则搜索将返回所有网站的结果。
交易类型	选择要跟踪的事务类型，可以是 “所有事务 (All Transactions)”、“已完成 (Completed)”、“已阻止 (Blocked)”、“已监控 (Monitored)” 或 “已警告 (Warned)”。

表 5-13　代理服务 (Proxy Services) 选项卡上的网络跟踪搜索条件 （续）

选项	说明
高级搜索条件	
URL 类别	要按 URL 类别进行过滤，请选择**按 URL 类别过滤 (Filter by URL Category)**，请键入要依据其过滤的自定义或预定义 URL 类别的第一个字母。从显示的列表中选择类别。 如果 URL 类别集已更新，则某些类别可能标记为 “已弃用 (Deprecated)”。已弃用的类别将不再用于至少一个托管网络安全设备上的新事务。但是，仍然可以搜索当该类别处于活动状态时发生的最近事务。有关 URL 类别集更新的详细信息，请参阅 URL 类别集更新和报告 （第 5-13 页）。 将包括匹配类别名称的所有最近事务，无论在下拉列表中注明的引擎名称为何。
应用层	要按应用进行过滤，请选择**按应用过滤 (Filter by Application)** 并选择依据其进行过滤的应用。 要按应用类型进行过滤，请选择**按应用类型过滤 (Filter by Application)** 并选择依据其进行过滤的应用类型。
策略	要按策略组进行过滤，请选择**按策略过滤 (Filter by Policy)** 并输入依据其进行过滤的策略组名称。 确保您已在网络安全设备上声明了该策略。
恶意软件威胁	要按特定恶意软件威胁进行过滤，请选择**按恶意软件威胁过滤 (Filter by Malware Threat)** 并输入依据其进行过滤的恶意软件威胁名称。 要按恶意软件类别进行过滤，请选择**按恶意软件类别过滤 (Filter by Malware Category)** 并选择依据其进行过滤的恶意软件类别。有关说明，请参阅恶意软件类别说明 （第 5-37 页）。
WBRS	在 WBRS 部分中，可以按基于网络的信誉分数和特定网络信誉威胁进行过滤。 • 要按网络信誉分数进行过滤，请选择**分数范围 (Score Range)**，然后选择过滤所依据的上限值和下限值。或者，可以通过选择**没有分数 (No Score)** 过滤没有分数的网站。 • 要按特定网络信誉威胁进行过滤，请选择**按信誉威胁过滤 (Filter by Reputation Threat)** 并输入依据其进行过滤的网络信誉威胁名称。 有关 WBRS 分数的更多信息，请参阅您的网络安全设备的在线帮助或用户指南。
AnyConnect 安全移动	要按远程或本地访问进行过滤，请选择**按用户地点进行过滤 (Filter by User Location)** 并选择访问类型。要包括所有访问类型，请选择**禁用过滤器 (Disable Filter)**。 （在以前的版本中，此选项已标记为 “移动用户安全 (Mobile User Security)”。）

表 5-13　代理服务 (Proxy Services) 选项卡上的网络跟踪搜索条件 （续）

选项	说明
网络设备	要按特定网络设备进行过滤，请点击**按网络设备过滤 (Filter by Web Appliance)** 旁的单选按钮，然后在文本字段中输入网络设备名称。 如果选择**禁用过滤器 (Disable Filter)**，则搜索将包括与安全管理设备关联的所有网络安全设备。
用户请求	要按照用户实际启动的事务进行过滤，请选择**按用户请求的事务过滤 (Filter by User-Requested Transactions)**。 **注意：**启用此过滤器后，搜索结果将包括 “最佳猜测”事务。

步骤 5　点击 **Search**。

相关主题

- 显示更多网络跟踪搜索结果 （第 5-39 页）
- 了解网络跟踪搜索结果 （第 5-40 页）
- 查看网络跟踪搜索结果的事务详细信息 （第 5-40 页）
- 关于网络跟踪和高级恶意软件保护功能 （第 5-40 页）

恶意软件类别说明

恶意软件类型	说明
广告程序	广告软件包括将用户转至进行销售的产品的所有软件可执行文件和插件。这些程序还会更改安全设置，使用户无法更改其系统设置。
浏览器助手对象	浏览器助手对象是可执行与提供广告或劫持用户设置相关的各种功能的浏览器插件。
商业系统监视程序	商业系统监视程序是具有系统监视特征的一种软件，可通过法律途径使用合法许可证获取。
拨号程序	拨号程序是利用调制解调器或其他类型的互联网访问连接到电话线或站点的程序，这会在用户未提供完全授权的情况下产生长途费用。
常规间谍软件	间谍软件是在计算机上安装的一种类型的恶意软件，可在用户不知情的情况下收集关于用户的少量信息。
劫持程序	劫持程序会修改系统设置或对用户系统进行任何不需要的更改，从而将用户转至某个网站或未得到用户授权的情况下运行程序。
已知的恶意和高风险文件	这些是被高级恶意软件防护文件信誉服务确定为威胁的文件。
其他恶意软件	此类别用于捕获与任何定义的类别不能完全匹配的所有其他恶意软件和可疑行为。
网络钓鱼 URL	网络钓鱼 URL 会显示在浏览器地址栏中。有时，它涉及使用域名和假冒合法的域。
PUA	潜在不需要的应用。 PUA 不是恶意应用，但是可被视为不需要的应用。

恶意软件类型	说明
系统监视程序	系统监视程序包含执行以下一种操作的任何软件： • 公开或秘密记录系统进程和/或用户操作。 • 使这些记录可用于在以后进行检索和查看。
特洛伊木马下载程序	特洛伊木马下载程序是一种特洛伊木马，在安装后，会与远程主机/站点联系并安装来自远程主机的程序包或附属程序。
特洛伊木马	特洛伊木马是仿冒成安全程序的一种破坏性程序。与病毒不同，特洛伊木马不能自我复制。
特洛伊木马钓鱼程序	特洛伊木马钓鱼程序可能位于受感染的计算机上以等待要访问的特定网页，或者可能扫描受感染的计算机以查找用户名和密码。
病毒	病毒是在未得到用户确认的情况下加载到用户计算机上的程序或一段代码。
蠕虫	蠕虫是通过计算机网络自我复制的程序或算法，而且执行恶意操作。

搜索 L4 流量监视器处理的事务

网络 (Web) > 报告 (Reporting) > 网络跟踪 (Web Tracking) 页面上的“L4 流量监视器”选项卡提供有关与恶意软件站点和端口的连接的详细信息。可以通过以下类型的信息搜索与恶意软件站点的连接：

- 时间范围
- 启动事务的计算机的 IP 地址 （IPv4 或 IPv6）
- 目标网站的域或 IP 地址 （IPv4 或 IPv6）
- 端口
- 与贵组织中的计算机关联的 IP 地址
- 连接类型
- 处理连接的网络安全设备

将会显示前 1000 个匹配的搜索结果。

查看有问题站点或处理事务的网络安全设备的主机名，请点击 “目标 IP 地址 (Destination IP Address)”列标题中的 “显示详细信息 (Display Details)”链接。

有关如何使用此信息的更多信息，请参阅 L4 流量监视器报告 （第 5-23 页）。

相关主题

- L4 流量监视器报告 （第 5-23 页）

搜索 SOCKS 代理处理的事务

可以搜索符合各种条件的事务 （包括已阻止或完成的事务），启动事务的客户端计算机的 IP 地址，以及目标域、 IP 地址或端口。还可以按自定义 URL 类别、匹配的策略和用户地点 （本地或远程）过滤结果。 IPv4 和 IPv6 地址都受支持。

操作步骤

步骤 1 依次选择**网络 (Web) > 报告 (Reporting) > 网络跟踪 (Web Tracking)**。

步骤 2 点击 **SOCKS 代理 (SOCKS Proxy)** 选项卡。

步骤 3 要过滤结果，请点击**高级 (Advanced)**。

步骤 4 输入搜索条件。

步骤 5 点击 **Search**。

相关主题

- SOCKS 代理报告 （第 5-25 页）

使用网络跟踪搜索结果

- 显示更多网络跟踪搜索结果 （第 5-39 页）
- 了解网络跟踪搜索结果 （第 5-40 页）
- 查看网络跟踪搜索结果的事务详细信息 （第 5-40 页）
- 关于网络跟踪和高级恶意软件保护功能 （第 5-40 页）
- 关于网络跟踪和升级 （第 5-41 页）

显示更多网络跟踪搜索结果

操作步骤

步骤 1 请务必查看返回结果的所有页面。

步骤 2 要在每页显示比当前数量更多的结果，请在**显示的项目数 (Items Displayed)** 菜单中选择一个选项。

步骤 3 如果与条件匹配的事务数超过在 “显示的项目数 (Items Displayed)” 菜单中提供的最大事务数，可以通过点击**可打印的下载 (Printable Download)** 链接获取包含所有匹配的事务的 CSV 文件，从而查看完整的结果集。

此 CSV 文件包括完整的原始数据集，但不包括相关事务的详细信息。

了解网络跟踪搜索结果

默认情况下，结果按时间戳排序，最新的结果会显示在顶部。

搜索结果包括：

- 访问 URL 的时间。
- 用户发起的事务所衍生的相关事务数，例如加载的映像、运行的 JavaScript 和访问的辅助站点。相关事务的数量会显示在列标题中 “显示所有详细信息 (Display All Details)”链接下的每个行中。
- 处理结果 （事务的结果。如果适用，显示事务被阻止、监控或警告的原因。）。

查看网络跟踪搜索结果的事务详细信息

要查看	操作
列表中被截断 URL 的完整的 URL	注意哪些主机网络安全设备处理了事务，然后检查该设备上的 Accesslog。
单个事务的详细信息	点击 “网站 (Website)”列中的 URL。
所有事务的详细信息	点击 “网站 (Website)”列标题中的**显示所有详细信息…(Display All Details...)** 链接。
最多包含 500 个相关事务的列表	相关事务的数量会显示在搜索结果列表中列标题的 “显示详细信息 (Display Details)”链接下的括号中。 点击事务详细信息视图中的**相关事务 (Related Transactions)** 链接。

关于网络跟踪和高级恶意软件保护功能

在网络跟踪中搜索文件威胁信息时，请记住以下要点：

- 要搜索文件信誉服务找到的恶意文件，请针对网络跟踪的 “高级 (Advanced)”部分中恶意软件威胁区域的**按恶意软件类别过滤 (Filter by Malware Category)** 选项选择**已知恶意软件和高风险文件 (Known Malicious and High-Risk Files)**。
- 网络跟踪仅包括有关文件信誉处理，以及处理事务时返回的原始文件信誉裁定的信息。例如，如果最初发现文件是干净文件，然后裁定更新发现文件是恶意文件，则只有干净的裁定显示跟踪结果中。

  搜索结果中的 “阻止 - AMP (Block - AMP)”表示事务因文件的信誉裁定而被阻止。

  在跟踪详细信息中，“AMP 威胁分数 (AMP Threat Score)”是云信誉服务无法确定文件的明确裁定时尽力提供的分数。在这种情况下，分数介于 1 和 100 之间。（如果返回了 AMP 裁定，或者分数为零，请忽略 AMP 威胁分数。）设备会将此分数与阈值分数比较 （在 “安全服务 (Security Services)” > “防恶意软件和信誉 (Anti-Malware and Reputation)”页面上配置），以确定要采取的操作。默认情况下，分数在 60 和 100 之间的文件将被视为恶意文件。思科建议不要更改默认阈值分数。 WBRS 分数是从中下载文件的站点的信誉，此分数与文件信誉无关。
- 裁定更新仅在 AMP 裁定更新报告中可用。网络跟踪中的原始事务详细信息不会通过裁定更改进行更新。要查看涉及特定文件的事务，请点击裁定更新报告中的 SHA-256。
- 有关文件分析的信息 （包括分析结果以及是否发送文件进行分析）仅在文件分析报告中可用。

有关已分析的文件的其他信息，可从云端获取。要查看文件的任何可用的文件分析信息，请选择**报告 (Reporting) > 文件分析 (File Analysis)** 并输入 SHA-256 以搜索该文件，或点击网络跟踪详细信息中的 SHA-256 链接。如果文件分析服务已分析任何源中的文件，则可以查看详细信息。系统仅会为已分析的文件的结果。

如果设备处理了已发送进行分析的某个文件的后续实例，这些实例将显示在网络跟踪搜索结果中。

相关主题

- 通过 SHA-256 哈希识别文件 （第 5-19 页）

关于网络跟踪和升级

新的网络跟踪功能可能不适用于在升级之前进行的事务，因为所需的数据可能没有为这些事务保留。有关与网络跟踪数据和升级相关的可能限制，请参阅与发行版对应的版本说明。

故障排除 Web 报告和跟踪

- 集中报告已正确启用，但不起作用 （第 5-41 页）
- 高级恶意软件保护裁定更新报告结果有所不同 （第 5-41 页）
- 查看文件分析报告详细信息时的问题 （第 5-42 页）
- 报告或跟踪结果中缺少预期数据 （第 5-42 页）
- PDF 仅显示网络跟踪数据的子集 （第 5-42 页）
- L4 流量监视器报告故障排除 （第 5-43 页）

另请参阅对所有报告进行故障排除 （第 3-11 页）。

集中报告已正确启用，但不起作用

问题：已按照指示启用了集中 Web 报告功能，但这不起作用。

解决方法：如果没有为报告分配磁盘空间，则集中 Web 报告不起作用，直到分配磁盘空间。只要为 Web 报告和跟踪设置的配额大于当前使用的磁盘空间，就不会丢失任何 Web 报告和跟踪数据。有关详细信息，请参阅 “管理磁盘空间”部分 （第 14-45 页）。

高级恶意软件保护裁定更新报告结果有所不同

问题：网络安全设备和邮件安全设备发送同一文件进行分析，而网络和邮件的 AMP 裁定更新报告针对该文件显示不同的裁定。

解决方法：这种情况是临时的。下载了所有裁定更新后，结果便会匹配。实现匹配最多需要 30 分钟。

查看文件分析报告详细信息时的问题

文件分析报告详细信息不可用

问题：文件分析报告详细信息不可用。

解决方法：请参阅有关文件分析报告详细信息的要求 （第 5-19 页）。

查看文件分析报告详细信息时出错

问题：当尝试查看文件分析报告详细信息时，显示 `No cloud server configuration is available` 错误。

解决方法：转到**管理设备 (Management Appliance) > 集中式服务 (Centralized Services) > 安全设备 (Security Appliances)**，然后添加至少一个启用了文件分析功能的网络安全设备。

报告或跟踪结果中缺少预期数据

问题：报告或跟踪结果中缺少预期数据。

解决方法：可能原因：

- 确保已选择所需的时间范围。
- 对于跟踪结果，确保查看所有匹配的结果。请参阅显示更多网络跟踪搜索结果 （第 5-39 页）。
- 可能网络安全设备和安全管理设备之间的数据传输被中断，或者数据可能已被清除。请参阅数据可用性页面 （第 5-28 页）。
- 如果升级更改了报告或跟踪信息的方式，则升级之前进行的事务可能无法按预期表示。要查看发行版是否具有此类型的更改，请参阅文档 （第 E-2 页）中指定的位置提供的与发行版对应的版本说明。
- 对于网络代理服务跟踪搜索结果中缺少的结果，请参阅搜索网络代理服务处理的事务 （第 5-35 页）。
- 有关按用户请求的事务过滤时出现的意外结果，请参阅搜索网络代理服务处理的事务 （第 5-35 页）中相应表格的 “用户请求 (User Request)” 行。

PDF 仅显示网络跟踪数据的子集

问题：PDF 仅显示在 “网络跟踪 (Web Tracking)” 页面上可见的一些数据。

解决方法：有关要包含在 PDF 和 CSV 文件中以及从其中省略的数据的信息，请参阅打印和导出报告和跟踪数据 （第 3-9 页）中相应表格的网络跟踪信息。

L4 流量监视器报告故障排除

如果网络代理配置为转发代理，并且 L4 流量监视器设置为监控所有端口，则会记录代理数据端口的 IP 地址并显示为报告中的客户端 IP 地址。如果网络代理配置为透明代理，请启用 IP 欺骗以正确记录和显示客户端 IP 地址。为此，请参阅您的网络安全设备的在线帮助或用户指南。

相关主题

- 客户端恶意软件风险报告 （第 5-20 页）
- 搜索 L4 流量监视器处理的事务 （第 5-38 页）

跟踪邮件消息

跟踪服务概述

思科内容安全管理设备的跟踪服务是邮件安全设备的补充功能。利用安全管理设备，邮件管理员可以在单一位置处跟踪通过任意邮件安全设备的邮件的状态。

利用安全管理设备，可以很方便地查找邮件安全设备处理的邮件的状态。通过确定邮件的确切位置，邮件管理员可以快速解决支持中心的呼叫问题。使用安全管理设备，管理员可以确定特定邮件是已传送、包含病毒或放在垃圾邮件隔离区，还是位于邮件流的其他位置。

您可以使用安全管理设备灵活的跟踪界面来查找邮件，而不必使用 `grep` 或类似工具搜索日志文件。您可以组合使用各种搜索参数。

跟踪查询可包括：

- **信封信息：**从特定信封发件人中查找邮件，或通过输入匹配的文本字符串查找收件人。
- **主题信头：**与主题行中的文本字符串匹配。警告：不要在法规禁止相关跟踪的环境中使用此类搜索。
- **时间范围：**查找在指定日期和时间之间发送的邮件。
- **发件人 IP 地址或拒绝的连接数量：**从特定 IP 地址中搜索邮件，或在搜索结果中显示被拒绝的连接数量。
- **附件名称：**可以根据附件名称搜索邮件。搜索结果中将显示采用查询的名称，且至少包含一个附件的邮件。

  由于性能原因，不跟踪 OLE 对象或 ZIP 文件存档等附件内文件的名称。

  对于某些附件，可能不跟踪。由于性能原因，附件名称的扫描只作为其他扫描操作 （例如邮件或内容过滤、 DLP 或免责声明印记）的一部分进行。只有通过正文扫描，且仍附带附件的邮件，才能获得其附件名称。不显示附件名称的一些示例包括 （但不限于）：

  - 如果系统只使用内容过滤器，并且邮件被删除或其附件被反垃圾邮件或防病毒过滤器隔离
  - 如果在进行正文扫描之前，邮件拆分策略从某些邮件中删除了附件

- **事件 (Event)**：查找与指定事件匹配的邮件，例如标记为病毒邮件、垃圾邮件或可疑垃圾邮件的邮件，以及被传送、硬退回、软退回或发送到病毒爆发隔离区的邮件。
- **邮件 ID (Message ID)**：通过识别 SMTP “邮件 ID”信头或思科 IronPort 邮件 ID (MID) 查找邮件。
- **邮件安全设备 (Email Security appliance) （主机）**将搜索条件缩小为特定的邮件安全设备，或在所有托管设备内搜索。

设置集中邮件跟踪

要设置集中邮件跟踪，请按顺序完成下列步骤：

- 在安全管理设备上启用集中邮件跟踪 （第 6-2 页）
- 在邮件安全设备上配置集中邮件跟踪 （第 6-2 页）
- 向每台托管邮件安全设备添加集中邮件跟踪服务 （第 6-3 页）

在安全管理设备上启用集中邮件跟踪

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 邮件 (Email) > 集中邮件跟踪 (Centralized Message Tracking)**。

步骤 2　在 “邮件跟踪服务 (Message Tracking Service)”部分，点击**启用 (Enable)**。

步骤 3　如果是在运行 “系统设置向导 (System Setup Wizard)”后首次启用集中邮件跟踪，请查看最终用户许可协议，然后点击**接受 (Accept)**。

步骤 4　**提交 (Submit)** 并确认更改。

在邮件安全设备上配置集中邮件跟踪

操作步骤

步骤 1　确认邮件安全设备上是否已配置邮件跟踪，且其运行是否正常。

步骤 2　依次转至**安全服务 (Security Services) > 邮件跟踪 (Message Tracking)**。

步骤 3　点击**编辑设置 (Edit Settings)**。

步骤 4　选择**集中跟踪 (Centralized Tracking)**。

步骤 5　点击 **Submit**。

步骤 6　如果希望可以搜索和记录邮件附件名称：

请确保在邮件安全设备上，至少配置和启用了一种传入内容过滤器或其他正文扫描功能。有关内容过滤器和正文扫描的信息，请参阅邮件安全设备的文档或在线帮助。

步骤 7　确认更改。

步骤 8　请为每个要管理的邮件安全设备重复上述步骤。

向每台托管邮件安全设备添加集中邮件跟踪服务

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。

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 2　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**集中邮件跟踪 (Centralized Message Tracking)** 服务。

步骤 3　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，键入设备名称和邮件安全设备管理接口的 IP 地址。

注　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. “集中邮件跟踪 (Centralized Message Tracking)”服务已预先选定。

d. 点击**建立连接 (Establish Connection)**。

e. 为要托管的设备管理员帐户输入用户名和密码，然后点击**建立连接 (Establish Connection)**。

注　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。

g. 点击**测试连接**。

h. 阅读表格上方的测试结果。

步骤 4　点击 **Submit**。

步骤 5　为要启用集中邮件跟踪的每个邮件安全设备重复执行此程序。

步骤 6　确认更改。

管理敏感信息的访问权限

如果要向其他人分配管理任务，并希望限制他们对邮件中违反数据丢失防护 (DLP) 策略的敏感信息的访问权限，请参阅控制邮件跟踪中敏感 DLP 信息的访问权限 （第 13-22 页）。

检查邮件跟踪数据的可用性

您可以确定邮件跟踪数据包括的日期范围，并可识别这些数据中缺少的任何间隔。

操作步骤

步骤 1　依次选择**邮件 (Email) > 邮件跟踪 (Message Tracking) > 邮件跟踪数据可用性 (Message Tracking Data Availability)**。

搜索邮件

通过安全管理设备的跟踪服务，可以搜索与指定条件匹配的特定邮件或邮件组，这些条件包括邮件主题行、日期和时间范围、信封发件人或收件人，或处理事件 （例如，邮件是否为病毒邮件、垃圾邮件、硬退回、已传送邮件等）等。邮件跟踪允许您详细地了解邮件流。此外，还可以深入查看特定邮件，了解邮件详细信息，例如处理事件、附件名称或信封和信头信息。

备注　虽然跟踪组件提供有关各封邮件的详细信息，但无法使用它来阅读邮件内容。

操作步骤

步骤 1　在安全管理设备中，依次选择**邮件 (Email) > 邮件跟踪 (Message Tracking) > 邮件跟踪 (Message Tracking)**。

步骤 2　（可选）点击 “高级 (Advanced)”链接，以显示更多搜索选项。

步骤 3　输入搜索条件：

注　跟踪搜索不支持通配符或正则表达式。跟踪搜索不区分大小写。

- **信封发件人 (Envelope Sender)**：选择 “Begins With”、“Is”或 “Contains”，并输入要在信封发件人中搜索的文本字符串。可以输入邮件地址、用户名或域。使用以下格式：
  - 对于邮件域：
    example.com、 *[203.0.113.15]*、 *[ipv6:2001:db8:80:1::5]*
  - 对于完整的邮件地址：
    user@example.com、 *user@[203.0.113.15]* 或 *user@[ipv6:2001:db8:80:1::5]*。
  - 可以输入任何字符。不会针对输入执行验证。
- **信封收件人 (Envelope Recipient)**：选择 “Begins With”、“Is”或 “Contains”，并输入要在信封收件人中搜索的文本。可以输入邮件地址、用户名或域。

  如果对邮件安全设备上的的别名扩展使用别名表，搜索将查找扩展的收件人地址，而不是原始信封地址。在任何其他情况下，邮件跟踪查询将查找原始信封收件人地址。

  否则，信封收件人的有效搜索条件将与信封发件人相同。

  可以输入任何字符。不会针对输入执行验证。

- **主题 (Subject)**：选择 “Begins With”、“Is”、“Contains”或 “Is Empty”，并输入要在邮件主题行中搜索的文本字符串。
- **已收邮件 (Message Received)**：使用 “前 1 天 (Last Day)”、“前 7 天 (Last 7 Days)”或 “自定义范围 (Custom Range)”指定查询的日期和时间范围。使用 “前 1 天 (Last Day)”选项可搜索过去 24 小时内的邮件，使用 “前 7 天 (Last 7 Days)”选项可搜索过去完整 7 天以及当日已过去时间内的邮件。

  如果未指定日期，查询将返回所有日期的数据。如果仅指定时间范围，查询将返回所有可用日期内该时间范围的数据。如果指定当日和 23:59 作为结束日期和时间，查询将返回当日的所有数据。

  将日期和时间存储在数据库中时，它们将转换为 GMT 格式。在设备上查看日期和时间时，它们将按设备的本地时间显示。

  只有邮件安全设备中已记录邮件，且安全管理设备检索到邮件时，结果中才会显示邮件。根据日志大小和轮询频率，邮件的发送时间与其实际在跟踪和报告结果中的显示时间可能存在小的差距。
- **发件人 IP 地址 (Sender IP Address)**：选择发件人 IP 地址，并选择搜索邮件，还是仅搜索被拒绝的连接数。
  - IPv4 地址必须是 4 个数字，用句点分隔。每个数字必须是 0 到 255 之间的值。（示例：*203.0.113.15*）。
  - IPv6 地址包含 8 组 16 位十六进制值，用冒号分隔。
    可以在一个位置使用零压缩，例如 *2001:db8:80:1::5*。
- **邮件事件 (Message Event)**：选择要跟踪的事件。选项为 “病毒 (Virus Positive)”、“垃圾邮件 (Spam Positive)”、“可疑垃圾邮件 (Suspect Spam)”、“包含恶意 URL (contained malicious URLs)”、“包含指定类别的 URL (contained URL in specified category)”、“DLP 违规 (DLP Violations)”（可以选择 DLP 策略的名称，并选择违规严重程度或采取的操作）、“DMARC 违规 (DMARC violations)”、“已传送 (Delivered)”、“高级恶意软件保护 (Advanced Malware Protection Positive)”（适用于附件中的恶意软件）、“硬退回 (Hard Bounced)”、“软退回 (Soft Bounced)”、“当前在策略、病毒或病毒爆发隔离区 (currently in a policy, virus, or outbreak quarantine)”、“被邮件过滤器或内容过滤器拦截 (caught by message filters or content filters)”和 “作为垃圾邮件隔离 (Quarantined as Spam)”。与您添加到跟踪查询的大多数条件不同，事件使用 “OR”运算符添加。选择多个事件来扩展搜索。
- **邮件 ID 信头和思科 IronPort MID (Message ID Header and Cisco IronPort MID):**输入邮件 ID 信头的文本字符串、思科 IronPort 邮件 ID (MID)，或两者。
- **查询设置 (Query Settings)**：从下拉菜单中，选择希望查询在超时之前运行的时间。选项包括 “1 分钟 (1 minute)”、“2 分钟 (2 minutes)”、“5 分钟 (5 minutes)”、“10 分钟 (10 minutes)”和 “无时间限制 (No time limit)”。此外，选择希望查询返回的最多结果数 （最多 1000）。
- **附件名称 (Attachment name)**：选择 “Begins With”、“Is”或 “Contains”，并为要查找的一个附件名称输入 ASCII 或 Unicode 文本字符串。前导空格和结尾空格不会从您输入的文本中删除。

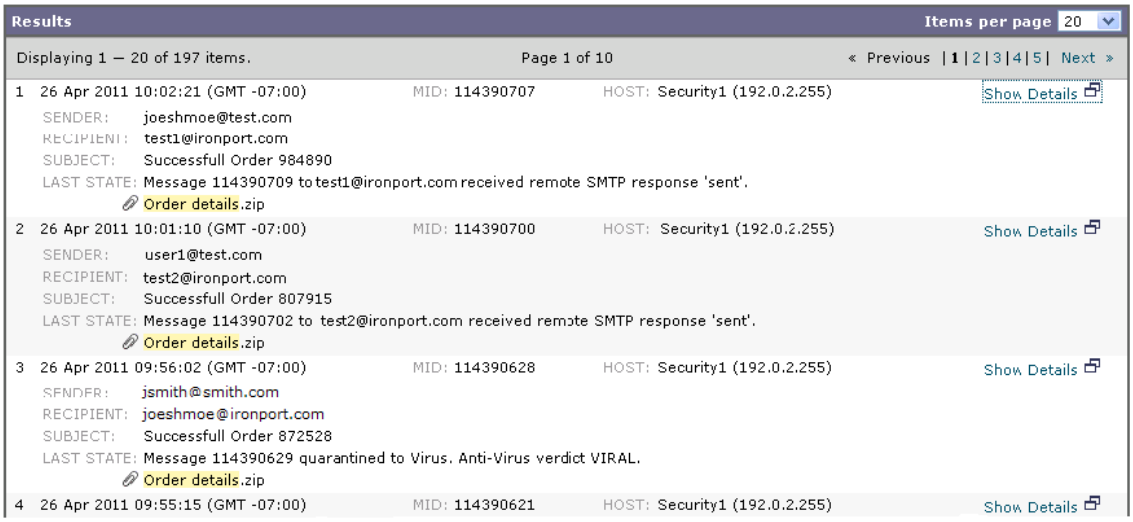
  有关基于 SHA-256 哈希识别文件的详细信息，请参阅通过 SHA-256 哈希识别文件 （第 4-24 页）。

无需每个字段都完成。除 “邮件事件 (Message Event)”选项之外，查询是 “AND”搜索。查询将返回与搜索字段中指定的 “AND”条件匹配的邮件。例如，如果为信封收件人和主题行参数指定文本字符串，查询将仅返回与指定信封收件人*和*主题行的*两者*匹配的邮件。

步骤 4　点击 **Search**。

页面底部将显示查询结果。每行对应一封邮件。

图 6-1　　邮件跟踪查询结果



您的搜索条件将在每行突出显示。

如果返回的行数比在 “每页的项目数 (Items per page)” 字段中指定的值大，结果将显示在多个页面。要导航页面，请点击列表顶部或底部的页码。

如果需要，请通过输入新搜索条件优化搜索，然后再次运行查询。或者，可以通过缩小结果集优化搜索，如以下各节所述。

相关主题

- 缩小结果集 （第 6-6 页）
- 关于邮件跟踪和高级恶意软件保护功能 （第 6-7 页）
- 了解跟踪查询结果 （第 6-8 页）

缩小结果集

在运行查询后，您可能会发现结果集包含的信息比需要的信息多。请通过点击结果列表行内的值缩小结果集，而不必创建新查询。

点击值，将作为搜索条件添加参数值。例如，如果查询结果包括多个日期的邮件，请点击某行中的特定日期，以仅显示该日期收到的邮件。

操作步骤

步骤 1　将光标浮动到您希望作为条件添加的值上方。该值将以黄色突出显示。

使用以下参数值优化搜索：

- 日期和时间
- 邮件 ID (MID)
- 主机 （邮件安全设备）
- 发送方

- 收件人
- 邮件的主题行或主题的起始词语

步骤 2　点击该值以优化搜索。

“结果 (Results)”部分显示与原始查询参数*和*您添加的新条件匹配的邮件。

步骤 3　如果需要，点击结果中的其他值进一步优化搜索。

注　要删除查询条件，请点击**清除 (Clear)**，并运行新跟踪查询。

关于邮件跟踪和高级恶意软件保护功能

在搜索邮件跟踪中的文件威胁信息时，请记住以下要点：

- 要通过文件信誉服务搜索恶意文件，请针对邮件跟踪“高级 (Advanced)”部分的“邮件事件 (Message Event)”选项，选择**高级恶意软件保护 (Advanced Malware Protection Positive)**。
- 邮件跟踪仅包括处理邮件时返回的文件信誉处理结果和原始文件信誉结果。例如，如果最初发现文件是干净文件，然后裁定更新发现文件是恶意文件，则只有干净的裁定显示跟踪结果中。

  在“邮件跟踪 (Message Tracking)”详细信息的“处理详细信息 (Processing Details)”部分显示：

  - 邮件中每个附件的 SHA-256；
  - 最终邮件整体的高级恶意软件保护裁定；
  - 发现包含恶意软件的任何附件。

    对干净或无法扫描的附件，不提供任何信息。
- 裁定更新仅在 AMP 裁定更新报告中可用。邮件跟踪中的原始邮件详细信息不会随裁定变化而更新。要查看包含特定附件的邮件，请点击裁定更新报告中的 SHA-256。
- 有关文件分析的信息（包括分析结果以及是否发送文件进行分析）仅在文件分析报告中可用。

  有关已分析的文件的其他信息，可从云端获取。要查看文件的所有可用文件分析信息，请依次选择**监控 (Monitor) > 文件分析 (File Analysis)**，并输入 SHA-256 以搜索文件。如果文件分析服务已分析任何源中的文件，则可以查看详细信息。系统仅会为已分析的文件的结果。

  如果设备处理了发送进行分析的某个文件的后续实例，这些实例将显示在“邮件跟踪 (Message Tracking)”搜索结果中。

相关主题

- 通过 SHA-256 哈希识别文件（第 4-24 页）

了解跟踪查询结果

如果结果不符预期，请参阅邮件跟踪故障排除 （第 6-9 页）。

跟踪查询结果将列出与在跟踪查询指定的条件匹配的所有邮件。除 “邮件事件 (Message Event)” 选项之外，查询条件还可使用 “AND” 运算符添加。结果集中的邮件必须满足所有 “AND” 条件。例如，如果指定信封发件人以 J 开头且主题以 T 开头，则查询将仅返回两个条件都满足的邮件。

要查看有关邮件的详细信息，请点击该邮件的**显示详细信息 (Show Details)** 链接。有关详细信息，请参阅 “邮件详细信息” 部分 （第 6-8 页）。

备注

- 跟踪查询结果中不显示包含 50 位或更多收件人的邮件。在将来版本中将会解决此问题。
- 指定查询时，可以选择最多显示 1000 条搜索结果。要查看符合条件的多达 50,000 封邮件，请点击搜索结果部分上方的**导出 (Export)** 链接，并在其他应用程序在打开生成的 .csv 文件。
- 如果点击了报告页面的链接来查看邮件跟踪中的邮件详细信息，但结果出现意外。如果查看期限内未同时和连续启用报告及跟踪，就可能出现这种情况。
- 有关打印或导出邮件跟踪搜索结果的信息，请参阅打印和导出报告和跟踪数据 （第 3-9 页）。

相关主题

- 邮件详细信息 （第 6-8 页）

邮件详细信息

要查看有关特定邮件的详细信息 （包括邮件信头信息和处理详细信息），请点击搜索结果列表中任何项目的**显示详细信息 (Show Details)**。将打开一个新窗口，其中包含邮件详细信息。

邮件详细信息包括以下部分：

- 信封和信头摘要 （第 6-8 页）
- 发送主机摘要 （第 6-9 页）
- 处理详细信息 （第 6-9 页）

信封和信头摘要

此部分显示邮件信封和信头的信息，例如信封发件人和收件人。该页面包括以下信息：

接收时间 (Received Time)：邮件安全设备收到邮件的时间。

MID：邮件 ID。

主题 (Subject)：邮件的主题行。

如果邮件无主题或未将邮件安全设备配置为在日志文件中记录主题行，则跟踪结果中主题行的值可能是 “（无主题）”。

信封发件人 (Envelope Sender)：SMTP 信封中的发件人地址。

信封收件人 (Envelope Recipients)：SMTP 信封中的收件人地址。

邮件 ID 信头 (Message ID Header)：唯一标识每封邮件的 “邮件 ID: (Message-ID:)” 信头。初次创建邮件时，即在邮件中插入该信头。在搜索特定邮件时，“邮件 ID: (Message-ID:)” 信头可能非常有用。

思科 IronPort 主机 (Cisco IronPort Host)：处理邮件的邮件安全设备。

SMTP 身份验证用户 ID (SMTP Auth User ID)：如果发件人使用 SMTP 身份验证发送邮件，则为发件人通过 SMTP 身份验证的用户名。否则，该值为 “N/A”。

附件 (Attachments)：附加到邮件的文件的名称。

发送主机摘要

反向 DNS 主机名 (Reverse DNS Hostname)：反向 DNS (PTR) 查询验证的发送主机的主机名。

IP 地址 (IP Address)：发送主机的 IP 地址。

SBRS 得分 (SBRS Score)：（SenderBase 信誉得分）。范围是 10（可能是可信的发件人）到 -10（明显是垃圾邮件发送者）。得分 “无 (None)”表示处理该邮件时，无此主机的相关信息。

处理详细信息

此部分显示处理邮件过程中记录的各种状态事件。

条目包括有关邮件策略处理 （例如反垃圾邮件和防病毒扫描）和邮件拆分等其他事件的信息。

如果已传送邮件，此处将显示传送的详细信息。例如，可能已传送邮件，而副本留在隔离区。

处理详细信息中将突出显示最后记录的事件。

“DLP 匹配内容 (DLP Matched Content)”选项卡

此部分显示违反数据丢失防护 (DLP) 策略的内容。

由于这些内容通常包括敏感信息，例如企业机密信息或个人信息 （包括信用卡号码和健康记录），您可能想要禁止有权访问安全管理设备，但并非管理员级别访问权限的用户访问这些内容。请参阅控制邮件跟踪中敏感 DLP 信息的访问权限 （第 13-22 页）。

邮件跟踪故障排除

搜索结果中缺少预期邮件

问题：搜索结果中不包括本应满足条件的邮件。

解决方案

- 许多搜索的结果都取决于设备配置，特别是邮件事件搜索。例如，如果搜索未经过滤的 URL 类别，则找不到任何结果，即使邮件包含该类别的 URL 亦不例外。确认您是否已正确配置邮件安全设备来实现预期的行为。例如，检查邮件策略、内容和邮件过滤器及隔离区设置。
- 请参阅检查邮件跟踪数据的可用性 （第 6-4 页）。
- 如果点击报告中的链接后缺少预期的信息，请参阅邮件报告故障排除 （第 4-39 页）。

搜索结果中不显示附件

问题：搜索结果中找不到且未显示附件名称。

解决方法：请参阅在安全管理设备上启用集中邮件跟踪 （第 6-2 页）中的配置要求和跟踪服务概述 （第 6-1 页）中的附件名称搜索限制。

垃圾邮件隔离区

垃圾邮件隔离区概述

垃圾邮件隔离区 （也称为 ISQ、最终用户隔离区和 EUQ）为担忧 “错误判断”（即合法的邮件被设备认为是垃圾邮件）的组织提供安全保护机制。当设备确定某个邮件是垃圾邮件或是可疑垃圾邮件时，您可能希望让收件人或管理员查看该邮件，然后再传输或删除该邮件。为此，垃圾邮件隔离区会存储邮件。

邮件安全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 （通常为邮件收件人）可以在稍微不同的网络界面中查看自己隔离区中的邮件。

垃圾邮件隔离区与策略、病毒和病毒爆发隔离区不同。

本地与外部垃圾邮件隔离区

本地垃圾邮件隔离区在邮件安全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邮件安全设备的垃圾邮件。
- 希望存储的垃圾邮件数量超过邮件安全设备可承载的范围。
- 希望定期备份垃圾邮件隔离区及其邮件。

相关主题

- 启用和配置垃圾邮件隔离区 （第 7-3 页）
- 配置浏览器访问垃圾邮件隔离区的 IP 接口 （第 7-6 页）
- 配置对垃圾邮件隔离区的管理用户访问权限 （第 7-6 页）
- 限制邮件被隔离的收件人 （第 7-7 页）
- 确保邮件文本正确显示 （第 7-7 页）
- 垃圾邮件隔离区语言 （第 7-7 页）

设置集中式垃圾邮件隔离区

	操作	更多信息
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 （第 7-3 页）。
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式垃圾邮件隔离区服务”部分 （第 7-4 页）。
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”部分 （第 7-5 页）。
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”部分 （第 7-6 页）。
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。	在邮件安全设备文档中，了解有关配置反垃圾邮件和邮件策略的信息。设置本地垃圾邮件隔离区部分的表中包含指向相关部分的链接。
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。	请参阅您所用版本的邮件安全设备的文档。
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文档。

启用和配置垃圾邮件隔离区

操作步骤

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. 点击**启用 (Enable)**。

b. 查看最终用户许可协议，然后点击**接受 (Accept)**。

如果编辑垃圾邮件隔离区设置，请点击**编辑设置 (Edit Settings)**。

步骤 3　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。
发送邮件通过 (Deliver Messages Via)	所有与传出隔离区相关的邮件 （例如垃圾邮件通知和从垃圾邮件隔离区释放的邮件）必须通过配置为发送邮件的其他设备或服务器发送。 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。两者必须使用同一接口 （Data 1 或 Data 2）作为出站监听程序。 请阅读屏幕上的说明，了解有关这些地址的其他警告。
保留天数 （之后自动删除） (Schedule Delete After)	指定邮件在被删除前保留的天数。 思科建议将隔离区配置为删除最早的邮件，以防隔离区容量被填满，但可以选择不设定自动删除。
释放邮件时通知思科 (Notify Cisco Upon Message Release)	—

选项	说明
垃圾邮件隔离区外观 (Spam Quarantine Appearance)	**徽标** 默认情况下，当用户登录查看隔离的邮件时，垃圾邮件隔离区页面顶部会显示思科徽标。 要改为使用自定义徽标，请上传徽标。徽标为 .jpg、 .gif 或 .png 文件，最大尺寸为 50 像素高 x 500 像素宽。
	登录页消息 （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，会显示此消息。 如果不指定消息，将显示以下消息： 在下面输入登录信息。如果不确定输入的内容，请与管理员联系。
管理员	请参阅配置对垃圾邮件隔离区的管理用户访问权限 （第 7-6 页）。

步骤 4　提交并确认更改。

后续操作

- 返回至设置集中式垃圾邮件隔离区 （第 7-2 页）。

向每个托管邮件安全设备添加集中式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。

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 2　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**垃圾邮件隔离区 (Spam Quarantine)** 服务。

步骤 3　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，键入设备名称和设备管理接口的 IP 地址。

注　可以在 “IP 地址 (IP Address)”文本字段中输入 DNS 名称，但点击**提交 (Submit)** 后，它将立即解析为 IP 地址。

c.　垃圾邮件隔离区服务已预先选择。

d.　点击**建立连接 (Establish Connection)**。

e.　输入要管理的设备的管理员帐户用户名和密码，然后点击**建立连接 (Establish Connection)**。

注　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。

g. 点击**测试连接**。

h. 阅读表格上方的测试结果。

步骤 4　点击 **Submit**。

步骤 5　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。

步骤 6　确认更改。

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。

准备工作

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，请参阅附录 B “分配网络和 IP 地址”

操作步骤

步骤 1　请将以下程序与附录 B “分配网络和 IP 地址”中的信息结合使用。

步骤 2　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 网络 (Network) > IP 接口 (IP Interfaces)**。

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

步骤 4　输入以下设置：

- 名称
- 以太网端口

  通常，该端口为 Data 2。具体而言，该端口必须与在的**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 垃圾邮件隔离区 (Spam Quarantine)** 下为 “垃圾邮件隔离区设置 (Spam Quarantine Setting)”页面**发送邮件通过 (Deliver Messages Via)** 部分的**主服务器 (Primary Server)** 指定的邮件安全设备上的数据接口匹配。
- IP 地址

  刚才指定的接口的 IP 地址。
- Netmask
- 主机名

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

不要在此接口的 “垃圾邮件隔离区 (Spam Quarantine)”部分输入信息。

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，将打开独立的浏览器窗口。

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 网络 (Network) > IP 接口 (IP Interfaces)**。

步骤 2　点击**管理 (Management)** 接口的名称。

步骤 3　在 “垃圾邮件隔离区 (Spam Quarantine)” 部分，配置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。
- 指定通知和垃圾邮件隔离区浏览器窗口显示的 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 4　提交并确认更改。

后续操作

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

所有具有管理员权限的用户均可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邮件。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访问垃圾邮件隔离区的权限，他们可以查看、释放和删除垃圾邮件隔离区中的邮件：

- 邮件管理员 (Email administrator)
- Operator
- 只读操作员 (Read-only operator)
- 服务中心用户 (Help desk user)
- 访客
- 具有垃圾邮件隔离区权限的自定义用户角色

这些用户不能访问垃圾邮件隔离区设置。

准备工作

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，请参阅第 13 章 “分配管理任务”中关于自定义用户角色对隔离区的访问权限 （第 13-5 页）的信息。

操作步骤

步骤 1　如果还没有编辑垃圾邮件隔离区设置页面，请执行以下操作：

a. 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)”。

b. 点击**编辑设置 (Edit Settings)**。

步骤 2　点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。

如果已添加了用户或角色，请点击用户名或角色查看所有符合条件的用户或角色。

步骤 3　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 4　点击**确定 (OK)**。

步骤 5　提交并确认更改。

相关主题

- 配置最终用户访问垃圾邮件隔离区的权限 （第 7-17 页）

限制邮件被隔离的收件人

在邮件安全设备上可以使用多个邮件策略 （“邮件策略 (Mail Policies)” > “传入邮件策略 (Incoming Mail Policy)”），以指定其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 “发送 (Deliver)” 或 “删除 (Drop)”，而不是隔离区。

确保邮件文本正确显示

AsyncOS 尝试根据邮件信头中指定的编码确定邮件的字符集。但是，如果信头中指定的编码与实际文本不符，则在垃圾邮件隔离区中查看邮件时，邮件不会正确显示。这种情况较可能发生在垃圾邮件中。

要确保为这些邮件正确显示邮件文本，请参阅您的邮件安全设备说明文档中 “垃圾邮件隔离区” 一章中有关指定默认编码的说明。

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

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。安全列表指定永不被视为垃圾邮件来源的发件人和域。阻止列表指定始终被视为垃圾邮件来源的发件人和域。

可以允许最终用户 （邮件用户）管理自己邮件帐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电子邮件。他可以决定将此发件人添加到其阻止列表中，以防来自该邮件列表的电子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电子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。为了确保这些发件人的邮件不会被隔离，他们可以将这些发件人添加到安全列表。

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

发件人在安全列表或阻止列表中不会阻碍设备扫描邮件病毒，或确定邮件是否符合内容相关的邮件策略的条件。即使邮件发件人在收件人的安全列表中，但根据其他扫描设置和结果，该邮件也可能不会发送给最终用户。

启用安全列表和阻止列表后，设备会立即对照安全列表/阻止列表数据库扫描邮件，然后才进行反垃圾邮件扫描。如果设备检测到与安全列表或阻止列表条目匹配的发件人或域，当邮件中包含多个收件人时 （且这些收件人的安全列表/阻止列表设置不同），该邮件将进行分流。例如，将一封邮件发送给收件人 A 和收件人 B。收件人 A 将发件人放在安全列表中，而收件人 B 的安全列表或阻止列表中都没有该发件人的条目。这种情况下，邮件可能拆分成两封邮件，

使用两个邮件 ID。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，两封邮件将继续在管道中前行 （通过反病毒扫描、内容策略等），并受任何配置的设置约束。

如果邮件发件人或域位于阻止列表中，发送行为将取决于在启用安全列表/阻止列表功能时指定的阻止列表操作。与安全列表发送类似，如果不同收件人的安全列表/阻止列表设置不同，邮件也将分流。然后，根据阻止列表操作设置，隔离或删除被阻止列表分流的邮件。如果阻止列表操作配置为隔离，将对邮件进行扫描，最终进行隔离。如果阻止列表操作配置为删除，则在安全列表/阻止列表扫描后立即删除邮件。

由于安全列表和阻止列表保留在垃圾邮件隔离区中，所以发送行为还取决于其他反垃圾邮件设置。例如，如果在主机访问表 (HAT) 中配置了“接受”邮件流策略以跳过反垃圾邮件扫描，则在该监听程序中收到邮件的用户，其安全列表和阻止列表设置将不会应用于该监听程序上收到的邮件。同样，如果创建了针对特定邮件收件人跳过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

- 启用安全列表和阻止列表 （第 7-9 页）
- 外部垃圾邮件隔离区和安全列表/阻止列表 （第 7-9 页）

启用安全列表和阻止列表

准备工作

- 必须启用垃圾邮件隔离区。请参阅设置集中式垃圾邮件隔离区 （第 7-2 页）。
- 配置邮件安全设备以使用外部安全列表/阻止列表。有关设置外部垃圾邮件隔离区的说明，请参阅邮件安全设备文档。

操作步骤

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　在**最终用户安全列表/阻止列表 （垃圾邮件隔离区） (End-User Safelist/Blocklist (Spam Quarantine))** 部分，选择**启用 (Enable)**。

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**每个用户的列表项的最大数目 (Maximum List Items Per User)**。

这是针对每个收件人、每个列表的地址或域的最大数目。如果允许每个用户存在大量列表项，则可能会使系统性能下降。

步骤 5　选择更新频率。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 （第 7-9 页）。

步骤 6　提交并确认更改。

外部垃圾邮件隔离区和安全列表/阻止列表

由于邮件安全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邮件安全设备，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。

另外，还可以查看是否有许多收件人 （贵组织中的最终用户）都将特定发件人或域列入白名单或黑名单。

管理员可以查看和使用每个最终用户查看和使用的相同条目的超集。

准备工作

- 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）（第 7-22 页）。
- 启用对安全列表/阻止列表的访问权限。请参阅启用安全列表和阻止列表 （第 7-9 页）。
- （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 （第 7-13 页）中所述的步骤。
- 了解安全列表和阻止列表条目所需的格式。请参阅安全列表和阻止列表条目的语法 （第 7-11 页）。

操作步骤

步骤 1　使用浏览器，访问垃圾邮件隔离区。

步骤 2　请登录。

步骤 3　选择页面右上角的**选项 (Options)** 下拉菜单。

步骤 4　选择**安全列表 (Safelist)** 或**阻止列表 (Blocklist)**。

步骤 5　（可选）搜索发件人或收件人。

步骤 6　执行以下一项或多项操作：

目标	操作
为收件人添加多个发件人	1. 选择**查看方式: 收件人 (View by: Recipient)** 2. 点击**添加 (Add)**，或针对某个收件人点击**编辑 (Edit)**。 3. 输入或编辑收件人的邮件地址。 4. 输入发件人的邮件地址和域。 以单独的行放置每个条目，或使用逗号分隔各个条目。 5. 点击 **Submit**。
为发件人添加多个收件人	1. 选择**查看方式: 发件人 (View by: Sender)** 2. 点击**添加 (Add)**，或针对某个发件人点击**编辑 (Edit)**。 3. 输入或编辑发件人的地址或域。 4. 输入收件人的邮件地址。 以单独的行放置每个条目，或使用逗号分隔各个条目。 5. 点击 **Submit**。

目标	操作
删除与某个收件人相关的所有发件人 删除与某个发件人相关的所有收件人	1. 选择**查看方式 (View by)** 选项。 2. 点击垃圾箱图标以删除整个表格行。
删除某个收件人的个别发件人 删除某个发件人的个别收件人	1. 选择 “查看方式 (View by)” 选项。 2. 针对单个收件人或发件人点击**编辑 (Edit)**。 3. 在文本框中添加或删除条目。必须至少留下一个条目。 4. 点击 **Submit**。

相关主题

- 安全列表和阻止列表条目的语法 （第 7-11 页）
- 清除所有安全列表和阻止列表 （第 7-11 页）

安全列表和阻止列表条目的语法

可以使用下列格式向安全列表和阻止列表中添加发件人：

- 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* 位于安全列表中，可以将 *george@example.com* 列入阻止列表。这种情况下，设备会发送来自 *example.com* 且发件人不是 *george@example.com* 的所有邮件 （此发件人的邮件被视为垃圾邮件），而不扫描垃圾邮件。

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 （第 7-13 页）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

最终用户可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 （第 7-17 页）。

可能需要为最终用户提供垃圾邮件隔离区的 URL 及以下说明 （如果适用）。

相关主题

- 向安全列表添加条目 （最终用户）（第 7-12 页）
- 将发件人添加到阻止列表 （最终用户）（第 7-13 页）

向安全列表添加条目 （最终用户）

备注 列入安全列表的发件人的邮件发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 （第 7-8 页）。

最终用户可通过两种方式向安全列表中添加发件人：

- 将隔离邮件的发件人添加到安全列表 （第 7-12 页）
- 将发件人添加到不含隔离邮件的安全列表 （第 7-12 页）

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，最终用户可以将发件人添加至安全列表。

操作步骤

步骤 1 在垃圾邮件隔离区，选中邮件旁边的复选框。

步骤 2 从下拉菜单中选择**释放并添加至安全列表 (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，而释放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

操作步骤

步骤 1 通过浏览器访问垃圾邮件隔离区。

步骤 2 选择页面右上角的**选项 (Options)** 下拉菜单。

步骤 3 选择**安全列表 (Safelist)**。

步骤 4 在 “安全列表 (Safelist)”对话框中，输入邮件地址或域。可以输入多个域和邮件地址，并以逗号分隔。

步骤 5 点击**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，列入阻止列表的发件人所发送的邮件可能会被拒绝或隔离。

备注 只能按照以下程序添加阻止列表条目。

操作步骤

步骤 1 登录到垃圾邮件隔离区。

步骤 2 选择页面右上角的**选项 (Options)** 下拉菜单。

步骤 3 输入要添加到阻止列表的域或邮件地址。可以输入多个域和邮件地址，并以逗号分隔。

步骤 4 点击**添加到列表 (Add to List)**。

备份和恢复安全列表/阻止列表

在升级您的设备或运行安装向导前，您应备份安全列表/阻止列表数据库。包含设备配置设置的主 XML 配置文件中不含安全列表/阻止列表。

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 （第 14-6 页）。

操作步骤

步骤 1 选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 配置文件 (Configuration File)**。

步骤 2 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。

目标	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。 点击 **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*

目标	操作
导入安全列表/阻止列表	⚠ **注意**　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。 点击**选择要恢复的文件 (Select File to Restore)**。 从配置目录的文件列表中选择所需文件。 选择要恢复的安全列表/阻止列表备份文件。 点击 **Restore**。

安全列表和阻止列表故障排除

要排除安全列表和阻止列表的问题，可以查看日志文件或系统警报。

当邮件由于安全列表/阻止列表设置被锁定时，该操作将记录到 ISQ_log 文件或反垃圾邮件日志文件。列入安全列表的邮件以信头 *X-SLBL-Result-Safelist* 在安全列表中进行标记。列入阻止列表的邮件以信头 *X-SLBL-Result-Blocklist* 在阻止列表中进行标记。

创建或更新数据库时，或者修改数据库或运行安全列表/阻止列表进程出错时，将发送警报。

有关警报的详细信息，请参阅管理警报 （第 14-28 页）。

有关日志文件的详细信息，请参阅第 15 章 “日志记录”。

相关主题

- 列入安全列表的发件人的邮件未发送 （第 7-14 页）

列入安全列表的发件人的邮件未发送

问题：列入安全列表的发件人的邮件未发送。

解决方法：可能原因：

- 此邮件被恶意软件删除或内容违规。请参阅安全列表和阻止列表的邮件处理 （第 7-8 页）。
- 如果有多台设备，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 （第 7-9 页）。

为最终用户配置垃圾邮件管理功能

目标	请参阅
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。	配置最终用户访问垃圾邮件隔离区的权限 （第 7-17 页）和小节
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 （第 7-15 页）

目标	请参阅
如果发给用户的邮件被传送到垃圾邮件隔离区，将向用户发送通知。 通知可能包括访问垃圾邮件隔离区的链接。	通知最终用户被隔离的邮件 （第 7-19 页）
允许用户指定以下发件人的电子邮件地址和域：他们认为安全的发件人，及他们知道会发送垃圾邮件或其他不需要邮件的发件人。	使用安全列表和阻止列表基于发件人控制邮件发送 （第 7-8 页）

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 （第 7-15 页）
- 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 （第 7-17 页）
- 通知最终用户被隔离的邮件 （第 7-19 页）

访问垃圾邮件管理功能的最终用户的身份验证选项

备注　邮箱身份验证不允许用户查看发到邮件别名的邮件。

面向最终用户 垃圾邮件隔离区访问	操作
直接通过网络浏览器，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 (End User Quarantine Access)”设置中，选择 **LDAP** 或**邮箱 (Mailbox) (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)**。
直接通过网络浏览器，需要身份验证 并 通过通知中的链接，不需要身份验证	1. 在“最终用户隔离区访问 (End User Quarantine Access)”设置中，选择 **LDAP** 或**邮箱 (Mailbox) (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)**。
仅通过通知中的链接，不需要身份验证	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 （第 7-16 页）
- IMAP/POP 身份验证过程 （第 7-16 页）
- 配置最终用户访问垃圾邮件隔离区的权限 （第 7-17 页）

- 通知最终用户被隔离的邮件 （第 7-19 页）
- 配置 LDAP 以与垃圾邮件处理隔离区配合使用 （第 11-2 页）
- 关于最终用户访问安全列表和阻止列表 （第 7-12 页）

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，通常需要在 “全局目录端口”（在 6000s 中）连接服务器，并需要创建一个权限低的 LDAP 用户，以便垃圾邮件隔离区可以绑定来执行搜索。
3. 然后，垃圾邮件隔离区将使用指定 BaseDN 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”可以包含多个邮件地址，然后使用它们来确定应为通过身份验证的用户显示隔离区中的哪些信封地址。

相关主题

- 第 11 章 “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 UI 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 （第 7-17 页））。
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的域 （例如 `joe`），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，垃圾邮件隔离区使将用输入的邮件地址搜索匹配的信封。

有关 IMAP 的详细信息，请参阅华盛顿大学网站：

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

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

	操作	更多信息
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。	访问垃圾邮件管理功能的最终用户的身份验证选项 （第 7-15 页）
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 (System Administration) > LDAP > LDAP 服务器配置文件 (LDAP Server Profile)** 页面上的**垃圾邮件隔离区最终用户身份验证查询 (Spam Quarantine End-User Authentication Query)** 设置。	第 11 章 “与 LDAP 集成”
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 （第 7-17 页）
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 （第 7-18 页）

相关主题

- 配置最终用户访问垃圾邮件隔离区的权限 （第 7-17 页）
- 确定最终用户访问垃圾邮件隔离区的 URL （第 7-18 页）
- 最终用户查看的邮件 （第 7-18 页）

配置最终用户访问垃圾邮件隔离区的权限

无论是否启用了最终用户访问权限，管理用户都可以访问垃圾邮件隔离区。

准备工作

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 （第 7-15 页）中的要求。

操作步骤

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　点击**编辑设置 (Edit Settings)**。

步骤 3　向下滚动到**最终用户隔离区访问权限 (End-User Quarantine Access)** 部分。

步骤 4　选择**启用最终用户隔离区访问权限 (Enable End-User Quarantine Access)**。

步骤 5　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。

选择此选项	更多信息
无	—
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。如果部分或所有用户不支持 APOP，则应重新配置 POP 服务器，以便不进行 APOP 通告。 如果已将服务器配置为使用 SSL，请选择 “SSL”。如果用户仅输入了用户名，可以指定域以自动补充完整的邮件地址。为登录用户输入信封的域，以便 “将域附加到非限定用户名”。
LDAP	请按照本主题“准备工作”部分所引用的部分中介绍的操作，配置 LDAP 设置。

步骤 6　指定在释放邮件前，是否显示邮件正文。

如果选中此复选框，用户可能无法通过垃圾邮件隔离区页面查看邮件正文。相反，要查看已隔离邮件的正文，用户必须释放该邮件并在其邮件应用 （例如 Microsoft Outlook）中查看邮件正文。可以出于政策和法规合规性要求而使用此功能 - 例如，如果法规要求存档所有已查看的邮件。

步骤 7　提交并确认更改。

后续操作

（可选）自定义用户访问垃圾邮件隔离区时看到的页面 （如果尚未确定）。请参阅启用和配置垃圾邮件隔离区 （第 7-3 页）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电子邮件地址的邮件。

使用 LDAP 身份验证时，如果主邮件属性具有多个 LDAP 目录值，则所有值 （地址）均与该用户关联。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电子邮件地址的已隔离邮件。

如果身份验证方法为 IMAP/POP 或用户直接通过通知访问隔离区，则隔离区将仅显示该用户电子邮件地址 （或通知发送到的地址）的邮件。

有关发送到用户所属别名的邮件的信息，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知（第 7-20 页）。

相关主题

- 配置最终用户访问垃圾邮件隔离区的权限 （第 7-17 页）
- 收件人电子邮件的邮件列表别名和垃圾邮件通知 （第 7-20 页）

通知最终用户被隔离的邮件

如果垃圾邮件隔离区中存在用户的垃圾邮件和可疑垃圾邮件，可以将系统配置为向部分或所有这些用户发送通知邮件。

默认情况下，垃圾邮件通知会列出用户的被隔离邮件。此外，通知还包括用户可点击的链接，通过链接可查看其在垃圾邮件隔离区被隔离的邮件。这些链接不会过期。用户可以查看被隔离的邮件，并决定将它们传输到收件箱还是删除。

准备工作

- 最终用户要管理通知中列出的邮件，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 （第 7-17 页）。
- 了解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 （第 7-15 页）。
- 如果最终用户收到多个别名的电子邮件，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知 （第 7-20 页）。

操作步骤

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　点击**编辑设置 (Edit Settings)**。

步骤 3　向下滚动至**垃圾邮件通知 (Spam Notifications)** 部分。

步骤 4　选择**启用垃圾邮件通知 (Enable Spam Notification)**。

步骤 5　指定选项。

要自定义邮件正文，请执行以下操作：

a. （可选）自定义默认文本和变量。

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)** (`%new_message_count%`) — 自用户上次登录后的新邮件数。
- **总邮件数 (Total Message Count)** (`%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 Message Expires)** (`%days_until_expire%`)
- **隔离区 URL (Quarantine URL)** (`%quarantine_url%`) — 用于登录到隔离区和查看邮件的 URL。
- **用户名 (Username)** (`%username%`)
- **新邮件表 (New Message Table)** (`%new_quarantine_messages%`) — 用户在隔离区中的新邮件列表。

要插入变量，请将光标置于希望插入变量的位置，然后点击右侧 “邮件变量 (Message Variables)”列表中的变量名称。或键入变量。

b. 如果在此页面的 “最终用户隔离区访问 (End User Quarantine Access)” 部分启用了身份验证方法，请执行以下操作：

- 要使用户在点击通知中的链接访问垃圾邮件隔离区时自动登录，请选择**启用登录时无需隔离区访问凭证 (Enable login without credentials for quarantine access)**。最终用户可以释放邮件,只需点击通知中的 “释放 (Release)” 链接即可。
- 如果需要用户在点击通知中的链接访问垃圾邮件隔离区时进行登录，请取消选择此选项。最终用户不能通过点击通知中的 “释放 (Release)” 来释放邮件。

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

步骤 6　提交并确认更改。

后续操作

要确保最终用户收到这些通知，请考虑建议他们将垃圾邮件隔离区通知电子邮件的 “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 “白名单”。

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 （第 7-20 页）
- 测试通知 （第 7-21 页）
- 垃圾邮件通知故障排除 （第 7-21 页）

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电子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。如果将通知发送到邮件列表，列表中的所有用户都将收到通知。属于多个电子邮件别名的用户、属于收到通知的 LDAP 组的用户或使用多个电子邮件地址的用户，都可能收到多个垃圾邮件通知。下表显示了用户可能收到多个通知的案例。

表 7-1　每个地址/别名的通知

User	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

如果使用 LDAP 身份验证，可以选择不向邮件列表别名发送通知。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。请参阅垃圾邮件隔离区别名整合查询 （第 11-6 页）。

通过点击通知中的链接访问垃圾邮件隔离区的用户，不会看到最终用户可能拥有的任何其他别名被隔离的邮件，除非设备针对电子邮件通知使用的是垃圾邮件隔离区别名整合查询。如果将通知发送到设备处理后展开的分发列表，则多个收件人可能都有权访问该列表的相同隔离区。

这意味着，邮件列表的所有订阅者都将收到通知，并可以登录到隔离区以释放或删除邮件。这种情况下，最终用户访问隔离区查看通知中提到的邮件时，可能会发现这些邮件已被其他用户删除。

备注 如果不使用 LDAP 且不希望最终用户收到多个电子邮件通知，请考虑禁用通知，改为允许最终用户直接访问隔离区和通过 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：选中**启用垃圾邮件通知 (Enable Spam Notification)** 复选框，但不选择**启用最终用户隔离区访问 (Enable End-User Quarantine Access)**。这样，只有在**将退回邮件发送到 (Deliver Bounced Messages To)** 字段配置的管理员会收到隔离区的新垃圾邮件通知。

垃圾邮件通知故障排除

相关主题

- 用户收到多个通知 （第 7-21 页）
- 收件人未收到通知 （第 7-21 页）
- 用户收到多个通知 （第 7-21 页）
- 收件人未收到通知 （第 7-21 页）

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。

解决方法：可能原因：

- 用户有多个电子邮件地址，并且该垃圾邮件发送到了其中多个地址。
- 用户是收到该垃圾邮件的一个或多个电子邮件别名的成员。要尽可能减少重复及了解更多信息，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知 （第 7-20 页）。

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

- 如果通知被发送到 “将退回邮件发送到：(Deliver Bounce Messages To:)” 地址，而不是垃圾邮件收件人，这意味着垃圾邮件通知已启用，但垃圾邮件隔离区访问未启用。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 （第 7-15 页）。
- 让用户检查其电子邮件客户端的垃圾邮件设置。
- 检查您在启用和配置垃圾邮件隔离区 （第 7-3 页）中为**发送邮件通过 (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

此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的所有邮件。

相关主题

- 访问垃圾邮件隔离区 （管理用户）（第 7-22 页）
- 搜索垃圾邮件隔离区中的邮件 （第 7-22 页）
- 查看垃圾邮件隔离区中的邮件 （第 7-23 页）
- 发送垃圾邮件隔离区中的邮件 （第 7-23 页）
- 删除垃圾邮件隔离区中的邮件 （第 7-23 页）

访问垃圾邮件隔离区 （管理用户）

步骤 1　选择**电子邮件 (Email) > 邮件隔离区 (Message Quarantine) > 垃圾邮件隔离区 (Spam Quarantine)**，然后点击**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。

搜索垃圾邮件隔离区中的邮件

操作步骤

步骤 1　指定信封收件人。

注　可以输入部分地址。

步骤 2　选择搜索结果应与输入的收件人完全匹配，还是结果中应包含输入的条目、以该条目开头或结尾。

步骤 3　输入要搜索的日期范围。点击日历图标以选择日期。

步骤 4　指定 “发件人: (From:)” 地址，然后选择搜索结果应包含输入的值，与该值完全匹配，还是以该值开头或结尾。

步骤 5　点击 **Search**。页面 “搜索 (Search)” 部分下将显示符合搜索条件的邮件。

相关主题

- 搜索大型邮件集合 （第 7-23 页）

搜索大型邮件集合

如果垃圾邮件隔离区有大量邮件，而且没有具体定义搜索术语，则查询可能需要很长时间才能返回信息，也可能会超时。

系统将提示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。可以选择一次显示的邮件数量。可以点击列标题对显示排序。再次点击同一列可反向排序。

点击邮件主题可查看邮件，包括正文和信头。邮件会显示在 “邮件详细信息 (Message Details)” 页面中。显示邮件的前 20K 信息。如果邮件更长，邮件将在 20K 处截断，您可以通过邮件底部的链接下载邮件。

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

要查看有关邮件的更多详细信息，请点击**邮件跟踪 (Message Tracking)** 链接。

请注意以下提示：

- **查看带附件的邮件**

  查看包含附件的邮件时，将显示邮件的正文，然后是附件列表。

- **查看 HTML 邮件**

  垃圾邮件隔离区会尝试尽可能地呈现基于 HTML 的邮件。不显示图像。

- **查看编码的邮件**

  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

如果要释放邮件以进行发送，请点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**释放 (Release)**。然后点击**提交**。

点击标题行中的复选框，可自动选择页面中当前显示的所有邮件。

释放的邮件会直接转到目标队列，跳过电子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，还可以将垃圾邮件隔离区配置为：一旦隔离区达到最大容量，自动删除最早的邮件。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，请点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)**。然后点击**提交**。点击标题行中的复选框，可自动选择页面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 （请参阅关于禁用外部垃圾邮件隔离区（第 7-24 页）），然后点击**删除所有邮件 (Delete All Messages)** 链接。链接尾部括号中的数字为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因设备型号而异。请参阅查看磁盘配额和使用量 （第 14-46 页）。

默认情况下，垃圾邮件隔离区中的邮件经过一段时间后将自动删除。如果隔离区已满，将删除较早的垃圾邮件。要更改此设置，请参阅启用和配置垃圾邮件隔离区 （第 7-3 页）。

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。
- 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，请在邮件安全设备和安全管理设备上都禁用外部垃圾邮件隔离区。

  只禁用邮件安全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 （第 7-14 页）
- 垃圾邮件通知故障排除 （第 7-21 页）
- 确保邮件文本正确显示 （第 7-7 页）

第 8 章

集中策略、病毒和爆发隔离区

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。

防病毒扫描和病毒爆发过滤器各自都有一个专用的隔离区。可创建策略隔离区来暂存被邮件过滤、内容过滤和防数据丢失策略拦截的邮件。

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	默认情况下是否由系统创建？	说明	更多信息
高级恶意软件防护	文件分析	是	暂存发送进行文件分析的邮件。 有关特殊特征，请参阅邮件安全设备用户指南或在线帮助。	• 管理策略、病毒和爆发隔离区（第 8-8 页） • 处理策略、病毒或爆发隔离区中的邮件（第 8-15 页）
病毒	病毒	是	暂存可能传输防病毒引擎确定的恶意软件的邮件。	
爆发	病毒爆发	是	暂存爆发过滤器拦截的可能是垃圾邮件或恶意软件的邮件。	
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	只有邮件过滤器、内容过滤器或 DLP 邮件操作中指定的隔离区被删除后，才会暂存邮件。 无法向此隔离区指定任何过滤器或邮件操作。	
	（您创建的策略隔离区）	否	您创建的用于邮件过滤器、内容过滤器和 DLP 邮件操作的策略隔离区。	
垃圾邮件	垃圾邮件	是	暂存垃圾邮件或可疑垃圾邮件，以供邮件的收件人或管理员审核。	第 7 章 “垃圾邮件隔离区”

集中策略、病毒和爆发隔离区

	操作	更多信息
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、病毒和爆发隔离区数据。	附录 C “防火墙信息”
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、病毒和爆发隔离区 （第 8-4 页）
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 （第 14-45 页）
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。 此外，也可以在配置自定义迁移时创建所需的隔离区，或在自动迁移期间创建隔离区。在迁移过程中创建的所有隔离区都采用默认设置。 本地隔离区设置不在集中隔离区中保留，即使隔离区名称相同亦不例外。	• 创建策略隔离区 （第 8-10 页） • 检查系统创建的隔离区的设置 （第 8-10 页）
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。	向每个托管邮件安全设备添加集中策略、病毒和爆发隔离区服务 （第 8-4 页）
步骤 6	确认更改。	—
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、病毒和爆发隔离区的迁移 （第 8-5 页）
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。 **重要！** 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、病毒和爆发隔离区的迁移” • “集中策略、病毒和爆发隔离区”
步骤 9	迁移更多的邮件安全设备。 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。 在迁移过程中创建的隔离区均使用默认设置，而不是初始本地隔离区中的设置，即使集中隔离区和本地隔离区的名称相同亦不例外。	创建策略隔离区 （第 8-10 页）
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。

	操作	更多信息
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。	指定处理放行邮件的备用设备 （第 8-7 页）
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 （第 8-7 页）

在安全管理设备上启用集中策略、病毒和爆发隔离区

准备工作

完成集中策略、病毒和爆发隔离区 （第 8-3 页）的表中此程序之前的所有步骤。

操作步骤

步骤 1 在安全管理设备中，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 策略、病毒和爆发隔离区 (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 **Submit**。

后续操作

返回集中策略、病毒和爆发隔离区 （第 8-3 页）表中的后续步骤。

向每个托管邮件安全设备添加集中策略、病毒和爆发隔离区服务

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。

准备工作

确保您已完成了集中策略、病毒和爆发隔离区 （第 8-3 页）表中此位置之前的所有程序。

操作步骤

步骤 1 在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 2 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、病毒和爆发隔离区 (Policy, Virus, and Outbreak Quarantines)** 服务。

步骤 3　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，键入设备名称和要添加设备的管理接口的 IP 地址。

注　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、病毒和爆发隔离区 (Policy, Virus and Outbreak Quarantines)”服务已预先选中。

d. 点击**建立连接 (Establish Connection)**。

e. 输入要管理的设备的管理员帐户用户名和密码，然后点击**建立连接 (Establish Connection)**。

注　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 4　点击 **Submit**。

步骤 5　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 6　确认更改。

后续操作

返回集中策略、病毒和爆发隔离区 （第 8-3 页）表中的后续步骤。

配置策略、病毒和爆发隔离区的迁移

准备工作

- 确保您已完成了集中策略、病毒和爆发隔离区 （第 8-3 页）表中此位置之前的所有程序。
- 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。

操作步骤

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

步骤 2　点击**启动迁移向导 (Launch Migration Wizard)**。

步骤 3　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， 并 • 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， 并 • 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。	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。
• 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 • 要迁移本地隔离区并删除所有其他本地隔离区， 或 • 要将本地隔离区迁移到名称不同的集中隔离区 或 • 要将名称不同的本地隔离区合并为一个集中隔离区。	自定义	在迁移过程中 （而不是迁移前）创建的所有集中策略隔离区都将采用新隔离区的默认设置进行配置。 迁移后应更新这些设置。

步骤 4　点击**下一步**。

步骤 5　如果您选择了**自动 (Automatic)**：

确认此页面上要迁移的策略隔离区和其他信息是否符合您的预期。

病毒和爆发隔离区也将迁移。

步骤 6　如果选择了**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。
- 选择要迁移到各个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。它们将使用默认设置。
- 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。
- 您也可以通过从右侧表中选择隔离区，然后点击**从集中隔离区中删除 (Remove from Centralized Quarantine)**，来更改隔离区映射。

步骤 7　根据需要，点击**下一步 (Next)**。

步骤 8　提交并确认更改。

后续操作

返回集中策略、病毒和爆发隔离区 （第 8-3 页）表中的后续步骤。

指定处理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。

准备工作

- 确认备用设备是否可以按预期处理和传送放行的邮件。例如，加密和防病毒重新扫描配置应与主设备的配置相同。
- 备用设备必须针对集中策略、病毒和爆发隔离区进行完全配置。针对该设备完成集中策略、病毒和爆发隔离区 （第 8-3 页）表中的步骤。

操作步骤

步骤 1 在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 2 点击**指定备用放行设备 (Specify Alternate Release Appliance)** 按钮。

步骤 3 选择一个邮件安全设备。

步骤 4 提交并确认更改。

相关主题

- 当邮件安全设备不可用时放行邮件 （第 8-8 页）

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 （第 13-5 页）

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

- 指定处理放行邮件的备用设备 （第 8-7 页）

管理策略、病毒和爆发隔离区

相关主题

- 策略、病毒和爆发隔离区的磁盘空间分配 （第 8-8 页）
- 邮件在隔离区中的保留时间 （第 8-9 页）
- 自动处理的隔离的邮件的默认操作 （第 8-10 页）
- 检查系统创建的隔离区的设置 （第 8-10 页）
- 创建策略隔离区 （第 8-10 页）
- 关于编辑策略、病毒和爆发隔离区设置 （第 8-12 页）
- 确定隔离区分配到的过滤器和邮件操作 （第 8-12 页）
- 关于删除策略隔离区 （第 8-12 页）
- 监控隔离区状态、容量和活动 （第 8-13 页）
- 关于隔离区磁盘空间使用量的警报 （第 8-13 页）
- 策略隔离区和日志记录 （第 8-14 页）
- 关于向其他用户分配邮件处理任务 （第 8-14 页）

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 （第 14-45 页）。

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：

- 使用邮件安全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托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 （第 8-9 页）。

相关主题

- 监控隔离区状态、容量和活动 （第 8-13 页）
- 关于隔离区磁盘空间使用量的警报 （第 8-13 页）
- 邮件在隔离区中的保留时间 （第 8-9 页）

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保留时间。您为每个隔离区中的邮件指定一个保留时间。每封邮件都有自己特定的到期时间，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。

  注　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 （第 8-8 页）中定义的所有隔离区的大小限制。

    如果达到大小限制，将处理最早的邮件 （无论哪个隔离区），并针对每封邮件执行默认操作，直到所有隔离区的大小再次低于大小限制。该策略为先进先出 (FIFO)。多个隔离区中邮件的到期时间将以其最新到期时间为准。

    （可选）可以配置免除因磁盘空间不足而被放行或删除的各个隔离区。如果配置所有隔离区均免于放行或删除，并且磁盘空间达到容量，则邮件将会保留在邮件安全设备上，直到安全管理设备上有可用的空间。

    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 （第 8-13 页）。
  - 您删除仍存放邮件的隔离区。

从隔离区中自动删除邮件时，将针对该邮件执行默认操作。请参阅自动处理的隔离的邮件的默认操作 （第 8-10 页）。

保留时间中时间调整的影响

- 夏令时和设备时区更改不会影响保留时间。
- 如果更改隔离区的保留时间，只有新邮件采用新的到期时间。
- 如果更改系统时钟，则过去已到期的邮件将在下一个最适当的时间到期。
- 系统时钟更改不适用于当前到期的邮件。

自动处理的隔离的邮件的默认操作

出现邮件在隔离区中的保留时间 （第 8-9 页）中所述的任何情况时，将针对策略、病毒或爆发隔离区中的邮件执行默认操作。

主要默认操作有两个：

- 删除 — 删除邮件。
- 放行 — 放行邮件进行传送。

  放行后，可能会重新扫描邮件中的威胁。有关详细信息，请参阅关于重新扫描隔离的邮件（第 8-21 页）。

  此外，对于在预期保留时间到达之前被放行的邮件，还会对它们执行其他操作，例如添加 X-Header。有关详细信息，请参阅创建策略隔离区 （第 8-10 页）。

  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

- 关于编辑策略、病毒和爆发隔离区设置 （第 8-12 页）

创建策略隔离区

准备工作

- 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 （第 8-9 页）和自动处理的隔离的邮件的默认操作 （第 8-10 页）。
- 确定您希望哪些用户有权访问每个隔离区，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 （第 8-14 页）。

操作步骤

步骤 1　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)**。

步骤 2　点击**添加策略隔离区 (Add Policy Quarantine)**。

步骤 3　输入信息。

记住以下几点：

- 不能重命名隔离区。
- 在您指定的保留期间结束之前，如果*不*希望系统处理此隔离区中的邮件 （即使隔离区磁盘空间已满亦不例外），请取消选择**当空间溢出时，通过对邮件应用默认操作释放空间 (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。系统必须能够通过删除至少一个隔离区中的邮件来释放空间。

- 如果选择**放行 (Release)** 作为默认操作，可以指定其他操作以应用于保留期间到期前被放行的邮件：

选项	信息
修改主题	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，该邮件可能包含不当内容。 **注意**　要正常显示使用非 ASCII 字符的主题，必须根据 RFC 2047 表示它们。
添加 X-Header	X-Header 可提供针对某封邮件采取的操作记录。这可能会非常有用，例如在处理有关为什么传送特定邮件的咨询时。 输入名称和值。 示例： 名称=`Inappropriate-release-early` 值= `True`
拆离附件	拆离附件可防范这些文件当中存在病毒。

步骤 4　指定可以访问此隔离区的用户：

User	信息
本地用户	本地用户列表仅包括可以访问隔离区的角色的用户。 该列表不含具有管理员权限的用户，因为所有管理员都可完全访问隔离区。
经过外部身份验证的用户	您必须已配置外部身份验证。
自定义用户角色	只有创建了至少一个可访问隔离区的自定义用户角色，才能看到此选项。

步骤 5　提交并确认更改。

后续操作

- 如果尚未迁移邮件安全设备中的隔离区，请执行以下操作：

  作为迁移过程的一部分，将这些隔离区分配到邮件和内容过滤器及 DLP 邮件操作。

- 如果已经迁移到集中隔离区，请执行以下操作：

  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

备注

- 不能重命名隔离区。
- 另请参阅保留时间中时间调整的影响 （第 8-9 页）。

要更改隔离区设置，请选择 “邮件 (Email)” > “邮件隔离区 (Message Quarantine)” > “策略、病毒和爆发隔离区 (Policy, Virus, and Outbreak Quarantines)”，然后点击隔离区的名称。

确定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、与隔离区相关的 DLP 邮件操作及配置各项设置的邮件安全设备。

操作步骤

步骤 1　点击**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)**。

步骤 2　点击要检查的策略隔离区的名称。

步骤 3　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。请参阅确定隔离区分配到的过滤器和邮件操作 （第 8-12 页）。
- 即使策略隔离区已被分配到过滤器或邮件操作，也可以将其删除。
- 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的邮件的默认操作 （第 8-10 页）。
- 删除与某个过滤器或邮件操作关联的隔离区后，后续被该过滤器或邮件操作隔离的所有邮件操作将被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。
- 无法删除未分类隔离区。

监控隔离区状态、容量和活动

要查看	操作
为所有非垃圾邮件隔离区分配的总空间	选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 策略、病毒和爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**，并查看页面的第一部分。 要更改分配，请参阅管理磁盘空间 （第 14-45 页）。
所有非垃圾邮件隔离区的当前可用空间	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)** 并查看表下方。
所有隔离区当前使用的总空间	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	选择**邮件 (Email) > 邮件隔离区 (Message Quarantine) > 策略、病毒和爆发隔离区 (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。
所有隔离区中当前的总邮件数	选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**。
每个隔离区当前的邮件数	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)** 并查看隔离区的表格行。
所有隔离区的总 CPU 使用量	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 （隔离区之间的移动除外）	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)** 并查看隔离区的表格行。
策略隔离区的创建日期 策略隔离区创建者的名称	选择**邮件 (Email) > 邮件隔离区 (Message Quarantine) > 策略、病毒和爆发隔离区 (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。
与隔离区关联的过滤器和邮件操作	请参阅确定隔离区分配到的过滤器和邮件操作 （第 8-12 页）。

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。

有关警报的详细信息，请参阅管理警报 （第 14-28 页）。

策略隔离区和日志记录

AsyncOS 会逐个记录被隔离的所有邮件：

```
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的功能规则放在括号中。系统会针对放置邮件的每个隔离区生成单独的日志条目。

AsyncOS 还会逐个记录从隔离区删除的邮件：

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

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

从所有隔离区移除邮件后，无论是永久删除还是计划传送，系统会逐个记录邮件，例如：

```
Info: MID 483 released from all quarantines
```

```
Info: MID 484 deleted from all quarantines
```

重新放入邮件时，系统会用新的邮件 ID (MID) 创建新邮件对象。这些信息将使用现有的日志邮件及新 MID “byline”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查和管理策略隔离区。
- 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，可向这些用户分配访问权限。要将用户添加到隔离区，这些用户必须已存在。

每个用户可访问所有、部分隔离区或不能访问隔离区。无权查看隔离区的用户在 GUI 或 CLI 隔离区列表的任何位置，都不会看到它们存在的任何提示。

相关主题

- 可访问策略、病毒和爆发隔离区的用户组 （第 8-14 页）
- 第 13 章 “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的用户可以创建、配置、删除和集中隔离区，并可管理被隔离的邮件。
- 操作员、访客、只读操作员和服务中心用户组的用户，以及具有隔离区管理权限的自定义用户角色可以搜索、查看和处理隔离区中的邮件，但不能更改隔离区的设置，创建、删除或集中隔离区。可在每个隔离区中指定哪些用户可以访问该隔离区。
- 技术人员组的用户无法访问隔离区。

邮件跟踪和防数据丢失等相关功能的访问权限也会影响管理用户在 “隔离区 (Quarantine)”页面看到的选项和信息。例如，如果用户无法访问邮件跟踪，则该用户看不到隔离邮件的邮件跟踪信息。

备注　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 （第 8-7 页）。

最终用户无权查看或访问策略、病毒和爆发隔离区。

关于集中文件分析隔离区

- 如果在邮件安全设备中启用集中策略、病毒和爆发隔离区，则邮件将被隔离到安全管理设备上的集中文件分析隔离区。
- 与邮件安全设备不同，集中文件分析隔离区不会根据文件分析结果自动放行邮件。相反，在配置的保留时间到后，系统会从集中隔离区放行邮件。默认保留时间为 1 小时。
- 与邮件安全设备不同，不会在放行时重新扫描从集中文件分析隔离区放行的邮件。

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 （第 8-16 页）
- 在策略、病毒和爆发隔离区中查找邮件 （第 8-16 页）
- 手动处理隔离区中的邮件 （第 8-17 页）
- 多个隔离区中的邮件 （第 8-18 页）
- 邮件详细信息和查看邮件内容 （第 8-19 页）
- 关于重新扫描隔离的邮件 （第 8-21 页）
- 爆发隔离区 （第 8-21 页）

查看隔离区中的邮件

目标	操作
查看隔离区中的所有邮件	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	• 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 “管理规则摘要 (Manage by Rule Summary)” 链接 （第 8-21 页）。
在隔离区的邮件列表中导航	点击 “上一页 (Previous)”、“下一页 (Next)”、页码或双箭头链接。双箭头可带您转至列表的第一页 (<<) 或最后一页 (>>)。
排序隔离区的邮件列表	点击列标题 （可能包含多个项目或 “在其他隔离区 (In other quarantines)” 列的列除外）。
调整表列	拖动列标题之间的分隔符。
查看导致邮件被隔离的内容。	请参阅查看匹配的内容 （第 8-19 页）。

相关主题

- 隔离的邮件和国际字符集 （第 8-16 页）

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。

在策略、病毒和爆发隔离区中查找邮件

备注

- 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。
- 用户只能查找和查看其有权访问的隔离区的邮件。

操作步骤

步骤 1　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)**。

步骤 2　点击**搜索整个隔离区 (Search Across Quarantines)** 按钮。

提示　对于爆发隔离区，还可以查找每个爆发规则隔离的所有邮件：点击 “爆发 (Outbreak)” 表格行中的**管理规则摘要**，然后点击相关规则。

步骤 3　选择要搜索的隔离区。

步骤 4　（可选）输入其他搜索条件。

- 对于 “信封发件人 (Envelope Sender)” 和 “信封收件人 (Envelope Recipient)”：可以输入任何字符。不会针对输入执行验证。
- 搜索结果仅包括与您指定的*所有*条件都匹配的邮件。例如，如果您指定了 “信封收件人 (Envelope Recipient)” 和 “主题 (Subject)”，则只会返回与 “信封收件人 (Envelope Recipient)” *和* “主题 (Subject)” 中指定的术语都匹配的邮件。

后续操作

可以按使用隔离区列表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（第 8-17 页）。

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。

备注　如果使用 RSA Enterprise Manager 部署，则可以查看安全管理设备或 Enterprise Manager 上的被隔离邮件，但必须使用 Enterprise Manager 对邮件执行操作。有关 Enterprise Manager 的信息，请参阅邮件安全设备文档中的 “防数据丢失” 一章。

可以针对邮件执行以下操作：

- Delete
- 发布人
- 从隔离区延迟预定退出
- 向您指定的电子邮件地址发送邮件
- 在不同隔离区之间移动邮件

通常，在进行以下活动时可以针对显示的列表中的邮件执行操作。但是，并不是所有情况下都能执行所有操作。

- 在 “邮件 (Email)” > “邮件隔离区 (Message Quarantine)” > “策略、病毒和爆发隔离区 (Policy, Virus, and Outbreak Quarantines)” 页面的隔离区列表中，点击隔离区中的邮件编号。
- 点击 “搜索整个隔离区 (Search Across Quarantines)”。
- 点击一个隔离区名称，并在隔离区中搜索。

通过以下方式，可以一次对多封邮件执行这些操作：

- 从邮件列表顶部的拾取列表中选择一个选项。
- 选择页面中列出的每封邮件旁边的复选框。
- 选择邮件列表顶部表格标题中的复选框。这样，操作将应用到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。请参阅邮件安全设备的在线帮助或用户指南中的 “病毒爆发过滤器”一章了解 “按规则管理摘要”视图的相关信息。

相关主题

- 发送邮件副本 （第 8-18 页）
- 关于在策略隔离区之间移动邮件 （第 8-18 页）
- 多个隔离区中的邮件 （第 8-18 页）
- 自动处理的隔离的邮件的默认操作 （第 8-10 页）

发送邮件副本

只有管理员组的用户才能发送邮件副本。

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

关于在策略隔离区之间移动邮件

您可以将一个策略隔离区中的邮件手动移动到单一设备上的另一个策略隔离区。

将邮件移到其他隔离区时：

- 到期时间不变。邮件保留原隔离区的保留时间。
- 邮件被隔离的原因 （包括匹配的内容及其他相关详细信息）不会更改。
- 如果某个邮件存在于多个隔离区中，将该邮件移到已存有该邮件副本的目标时，移动的邮件副本的到期时间和隔离原因将覆盖目标隔离区原有邮件副本的相应信息。

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：

- 不传送，除非它所在的所有隔离区都将其放行。如果任何隔离区中删除了该邮件，则永不会传送该邮件。
- 不会从任何隔离区删除，除非从其所在的全部隔离区都删除或放行该邮件。

由于想要放行邮件的用户可能无权访问其驻留的所有隔离区，所以以下规则适用：

- 在从邮件驻留的所有隔离区放行邮件之前，不会从任何隔离区放行该邮件。
- 如果某个邮件在任何隔离区中标记为 “已删除 (Deleted)”，则无法从其所在的任何其他隔离区中传送该邮件。（仍可以放行。）

如果邮件在多个隔离区中排队，而用户无权访问一个或多个其他隔离区：

- 系统将通知用户，其有权访问的各个隔离区中是否存在该邮件。
- GUI 仅显示用户有权访问的隔离区的预定退出时间。（对于特定邮件，每个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。
- 用户不会看到导致邮件放入其无权访问的隔离区的匹配内容。
- 放行邮件只会影响用户有权访问的队列。
- 如果该邮件也在用户不可访问的其他隔离区排队，该邮件将留在隔离区中保持不变，直到具有访问其余隔离区所需权限的用户采取操作 （或直到该邮件通过提前或正常到期被放行）。

邮件详细信息和查看邮件内容

点击邮件的主题行，可查看邮件内容和访问 “隔离的邮件 (Quarantined Message)”页面。

“隔离的邮件 (Quarantined Message)”页面包含两部分：隔离区详细信息和邮件详细信息。

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。另外，还可以查看从隔离区放行邮件时，是否由于 “传送时加密 (Encrypt on Delivery)”过滤器操作对邮件加密。

“邮件详细信息 (Message Details)”部分只显示邮件正文、邮件信头和附件。仅显示前 100 K 邮件正文。如果邮件更长，显示前 100 K，后面为省略号 (...)。实际的邮件不会截断。这些信息仅用于显示。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。此外，还可以通过点击附件的文件名下载任何邮件附件。

如果您查看的邮件包含病毒，而您的计算机上安装了桌面防病毒软件，则防病毒软件可能报告发现了病毒。这并非对您计算机的威胁，可以安全忽略。

要查看有关邮件的更多详细信息，请点击**邮件跟踪 (Message Tracking)** 链接。

备注　对于特殊爆发隔离区，可使用其他功能。请参阅爆发隔离区 （第 8-21 页）。

相关主题

- 查看匹配的内容 （第 8-19 页）
- 下载附件 （第 8-20 页）

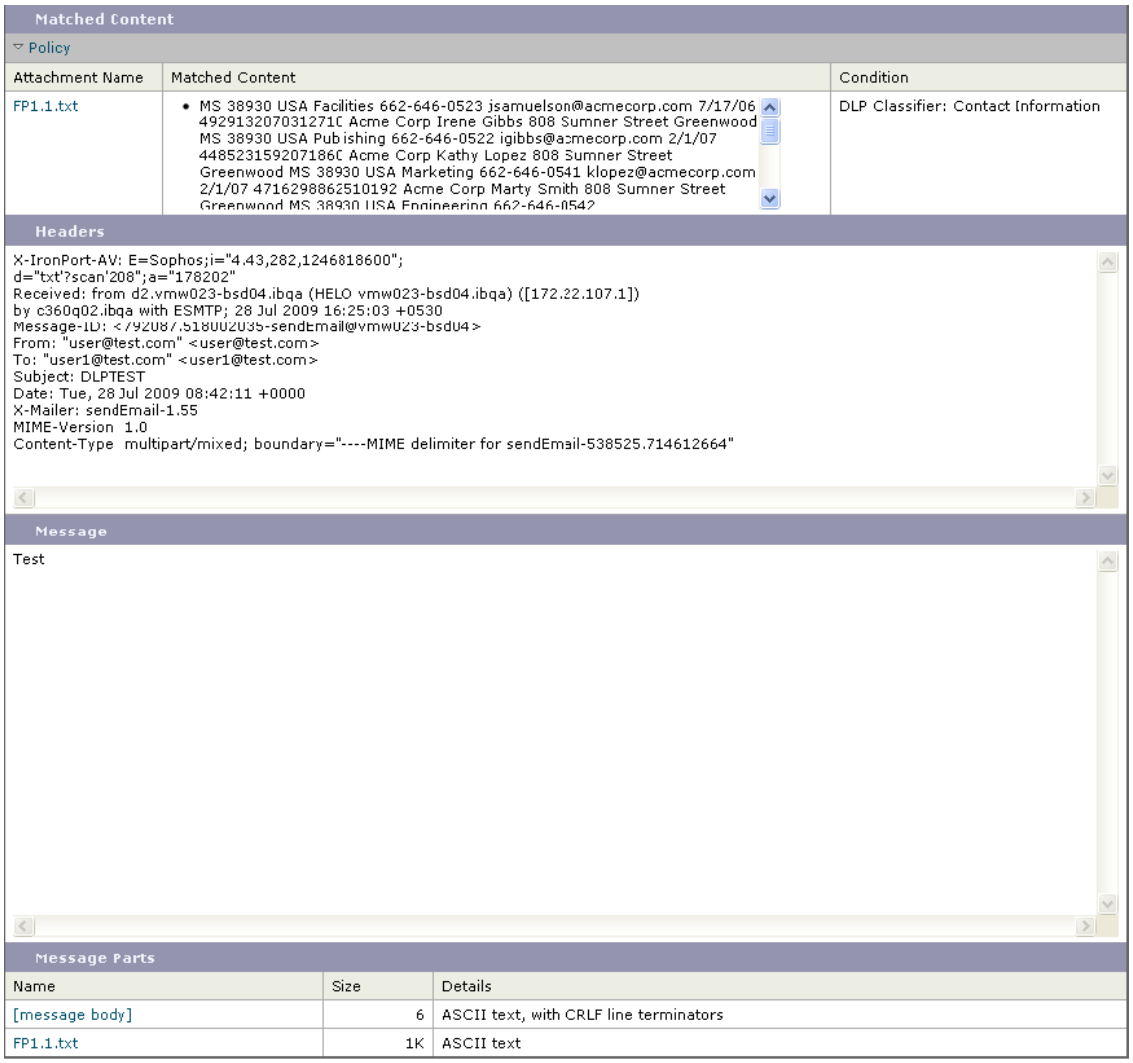
查看匹配的内容

为匹配附件内容条件、邮件正文或附件条件、邮件正文条件或附件内容条件的邮件配置隔离区操作时，可以查看被隔离邮件中的匹配内容。显示邮件正文时，匹配内容将以黄色突出显示， DLP 策略违规匹配除外。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。

如果附件包含匹配的内容，将显示附件内容以及其被隔离的原因，是由于 DLP 策略违规、内容过滤器条件、邮件过滤器条件，还是图像分析结果。

查看触发了邮件或内容过滤器规则的本地隔离区的邮件时， GUI 可能显示实际上未触发过滤器操作的内容 （及已触发过滤器操作的内容）。应将 GUI 显示作为查找内容匹配的指南，但它不一定反映确切的内容匹配。发生这种情况，是因为 GUI 比过滤器使用的内容匹配逻辑更宽松。此问题仅适用于邮件正文中的突出显示。在邮件各个部分列出匹配字符串的表以及相关过滤器规则是正确的。

图 8-1　在策略隔离区查看的匹配内容



下载附件

通过点击 “邮件部分 (Message Parts)”或 “匹配内容 (Matched Content)”部分的附件文件名，可以下载邮件附件。 AsyncOS 显示警告，表示附件来自未知来源，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，风险自负。您还可以点击 “邮件部分 (Message Parts)”部分的 [邮件正文] 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。

- 防病毒引擎重新扫描从策略和病毒隔离区放行的邮件。
- 反垃圾邮件和防病毒引擎重新扫描从爆发隔离区放行的邮件。（有关重新扫描爆发隔离区邮件的信息，请参阅邮件安全设备在线帮助或用户指南关于 “爆发过滤器”的一章。）
- 从策略、病毒和爆发隔离区放行后，由文件信誉服务重新扫描带附件的邮件。

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，如果结果不同，可能会将邮件发送到其他隔离区。

这样是为了防止邮件无限期循环返回隔离区。例如，假定邮件已进行加密，因此发送到病毒隔离区。如果管理员放行该邮件，防病毒引擎仍无法对其解密；但是，应不会再隔离邮件，否则将会创建循环，邮件将永不会从隔离区中放行。由于两次结果相同，所以第二次系统会绕开病毒隔离区。

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。根据设定的阈值，爆发过滤器功能将邮件发送到爆发隔离区。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。

爆发隔离区包含其他隔离区不可用的一些附加功能：“管理规则摘要 (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，将无法向爆发隔离区添加更多邮件。一旦隔离区中当前的邮件过期，爆发隔离区变空， GUI 的隔离区列表将不再显示它们。

相关主题

- 重新扫描爆发隔离区中的邮件 （第 8-21 页）
- “管理规则摘要 (Manage by Rule Summary)”链接 （第 8-21 页）
- 向思科系统报告误报或可疑邮件 （第 8-22 页）

重新扫描爆发隔离区中的邮件

如果新发布的规则认为被隔离的邮件不再是威胁，系统将自动放行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。

“管理规则摘要 (Manage by Rule Summary)”链接

点击隔离区列表中爆发隔离区旁边的 “管理规则 (Manage by Rule)”链接，可查看 “管理规则摘要 (Manage by Rule Summary)”页面。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、删除、延迟退出）。

这非常适合清理爆发隔离区中的大量邮件。有关详细信息，请参阅邮件安全设备在线帮助或用户指南 “爆发过滤器”一章中 “管理规则摘要”视图的信息。

向思科系统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。

操作步骤

步骤 1　导航到爆发隔离区中的邮件。

步骤 2　在“邮件详细信息 (Message Details)”部分，选择**将副本发送到思科系统 (Send a Copy to Cisco Systems)** 复选框。

步骤 3　点击**发送**。

排除集中策略隔离区的故障

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 （第 8-7 页）。

不重新扫描从集中爆发隔离区放行的邮件

问题：从爆发隔离区放行的邮件应重新扫描，再传送。但是，有些被传染的邮件已从隔离区传送。

解决方法：在关于重新扫描隔离的邮件 （第 8-21 页）中所述的情况下，可能会出现这种情况。

管理网络安全设备

关于集中配置管理

集中配置管理允许从思科内容安全管理设备向多达 150 台相关网络安全设备发布配置，以便：

- 通过在安全管理设备 （而不是各个网络安全设备）上一次性配置或更新设置，简化和加快网络安全策略管理。
- 确保跨分布式网络实施统一策略。

可通过两种方式向网络安全设备发布设置：

- 使用主配置
- 使用网络安全设备中的配置文件 （使用 “高级文件发布 (Advanced File Publishing)”）

确定正确的配置发布方法

从安全管理设备发布配置有两种不同的流程，每种流程发布不同的设置。有些设置不能集中管理。

配置	操作
在网络安全设备上的 “网络安全管理器 (Web Security Manager)” 菜单下显示的功能，例如策略和自定义 URL 类别。 **例外**：主配置中不含 “L4 流量监视器 (L4 Traffic Monitor)” (L4TM) 设置。 所支持的确切功能取决于与 AsyncOS 网络安全版本对应的主配置版本。	发布主配置。 主配置中可配置的许多功能还要求直接在网络安全设备上配置，才能使用。例如，“SOCKS 策略 (SOCKS Policies)” 可通过主配置进行配置，但 “SOCKS 代理 (SOCKS Proxy)” 必须首先在网络安全设备中直接配置。
与管理设备（例如配置日志订阅或警报）或分配管理职责相关的功能。	使用 “高级文件发布 (Advanced File Publishing)”。
联邦信息处理标准的 FIPS 模式、网络/接口设置、 DNS、网络高速缓存通信协议 (WCCP)、上游代理组、证书、代理模式、时间设置 （例如 NTP）、 L4 流量监视器 (L4TM) 设置和身份验证重定向主机名。	在托管网络安全设备上直接配置设置。 请参阅 *思科网络安全设备 AsyncOS 用户指南*

设置主配置以集中管理网络安全设备

在此设备上	操作	更多信息
—	检查通用配置要求和警告。	请参阅关于使用主配置的重要说明（第 9-3 页）。
—	确定要用于各个网络安全设备的主配置版本。	请参阅确定要使用的主配置版本（第 9-3 页）。
Web 安全设备	**（可选）**如果有一台网络安全设备正在运行，并可以将其用作所有网络安全设备的配置模型，则可以使用该网络安全设备中的配置文件加快安全管理设备中主配置的配置速度。	有关从网络安全设备下载配置文件的说明，请参阅 《*思科网络安全设备 AsyncOS 用户指南*》中的 “保存和加载设备配置”。
安全管理设备	启用并配置集中配置管理。	请参阅在安全管理设备上启用集中配置管理（第 9-4 页）。
安全管理设备	初始化主配置。	请参阅初始化主配置 （第 9-4 页）。
安全管理设备	将网络安全设备关联到主配置。	请参阅关于关联网络安全设备与主配置（第 9-5 页）。
安全管理设备	导入和/或手动配置主配置中的策略、自定义 URL 类别和/或网络代理旁路列表。	请参阅配置要发布的设置 （第 9-6 页）。
安全管理设备	确保各个网络安全设备上启用的功能与为分配到该设备的主配置启用的功能匹配。	请参阅确保功能一致地启用 （第 9-9 页）。
安全管理设备	在设置了所需的主配置并启用了相应功能之后，向网络安全设备发布配置。	请参阅发布主配置 （第 9-12 页）。
安全管理设备	为可能的 URL 类别集更新提前做准备，以便修改现有的主配置设置。	准备和管理 URL 类别集更新 （第 9-19 页）。

关于使用主配置的重要说明

备注　在集中管理的各个网络安全设备上，检查确保“网络 (Network)”>“身份验证 (Authentication)”中的所有领域名称在整个设备范围内是唯一的，除非同名领域的设置相同。

确定要使用的主配置版本

安全管理设备提供多个主配置，以便可以集中管理运行不同版本的 AsyncOS for Web Security（支持不同的功能）的网络安全设备。

每个主配置包含用于特定 AsyncOS 网络安全版本的配置。

要确定哪些主配置版本适用于您的 AsyncOS 网络安全版本，请参阅位于以下网站的“兼容性矩阵”：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。

备注　主配置版本应与网络安全设备上的 AsyncOS 版本匹配。如果网络安全设备中的设置与主配置中的设置不匹配，向更新的网络安全设备发布较早的主配置版本可能会失败。即使“网络设备状态 (Web Appliance Status)”详细信息页面未指示任何差异，也可能会出现此问题。这种情况下，必须手动比较各个设备中的配置。

在安全管理设备上启用集中配置管理

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 网络 (Web) >集中配置管理器 (Centralized Configuration Manager)**。

步骤 2　点击**启用 (Enable)**。

步骤 3　如果是在运行 “系统设置向导 (System Setup Wizard)”后首次启用 “集中配置管理 (Centralized Configuration Management)”，请查看最终用户许可协议，然后点击**接受 (Accept)**。

步骤 4　提交并确认更改。

初始化并配置主配置

初始化主配置

备注　初始化主配置后，“初始化 (Initialize)”选项将不可用。请改为使用配置要发布的设置 （第 9-6 页）中所述的某种方法填充主配置。

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置**。

步骤 2　点击 “选项 (Options)”栏中的**初始化 (Initialize)**。

步骤 3　在 “初始化主配置 (Initialize Configuration Master)”页面上：

- 如果已有用于以前版本的主配置，并希望对新的主配置使用或先使用相同设置，请选择**复制主配置 (Copy Configuration Master)**。

  随后，还可以从现有主配置导入设置。
- 或者，选择**使用默认设置 (Use default settings)**。

步骤 4　点击**初始化 (Initialize)**。

主配置现已可用。

步骤 5　对于要初始化的每个主配置版本，重复上述操作。

关于关联网络安全设备与主配置

对于您要集中管理的每个网络安全设备，策略配置应关联到与设备的 AsyncOS 版本匹配的主配置。例如，如果网络安全设备正在运行 AsyncOS 8.0 for Web，则应将其关联至主配置 8.0。

执行此任务的最简单流程取决于具体的情形：

如果	使用以下程序
您尚未将网络安全设备添加至安全管理设备	添加网络安全设备并将它们与主配置版本关联（第 9-5 页）
您已经添加网络安全设备	关联主配置版本与网络安全设备 （第 9-6 页）

添加网络安全设备并将它们与主配置版本关联

如果您尚未添加要集中管理的网络安全设备，请使用以下程序。

准备工作

如果尚未添加，请选择适合各个网络安全设备的正确主配置版本。请参阅确定要使用的主配置版本 （第 9-3 页）。

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

步骤 2　点击**添加网络设备 (Add Web Appliance)**。

步骤 3　在 “设备名称 (Appliance Name)” 和 “IP 地址 (IP Address)” 文本字段，键入设备名称和网络安全设备管理接口的 IP 地址或可解析主机名。

注　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。

步骤 4　“集中配置管理器 (Centralized Configuration Manager)” 服务已预先选定。

步骤 5　点击**建立连接 (Establish Connection)**。

步骤 6　为要托管的设备管理员帐户输入用户名和密码，然后点击**建立连接 (Establish Connection)**。

注　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。

步骤 7　等待该页面表格上方显示成功消息。

步骤 8　选择要分配给设备的主配置版本。

步骤 9　提交并确认更改。

步骤 10　对于想要启用集中配置管理的每台网络安全设备，重复上述程序。

关联主配置版本与网络安全设备

如果已将网络安全设备添加到安全管理设备，则可以使用以下程序快速将网络安全设备与主配置版本关联。

准备工作

如果尚未添加，请选择适合各个网络安全设备的正确主配置版本。请参阅确定要使用的主配置版本 （第 9-3 页）。

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置**。

注　如果主配置显示为 “已禁用 (Disabled)”，可以点击 “网络 (Web)” > “实用程序 (Utilities)” > “安全服务显示 (Security Services Display)”将其启用，然后点击**编辑显示设置 (Edit Display Settings)**。选中该主配置的复选框以将其启用。有关详细信息，请参阅启用功能以便发布 （第 9-10 页）。

步骤 2　点击**编辑设备分配列表 (Edit Appliance Assignment List)**。

步骤 3　在要关联的设备的行中，在**主 (Masters)** 列中点击以输入复选标记。

步骤 4　提交并确认更改。

配置要发布的设置

使用要发布的设置配置您的主配置。

设置主配置的方法有多种：

如果	操作
要从以前的 AsyncOS for Security Management 版本升级 并 没有通过将之前的现有主配置复制到新版本来初始化新的主配置版本	导入旧版本。请参阅从现有主配置导入 （第 9-7 页）。
已经配置了一台网络安全设备，并希望对于多台网络安全设备采用相同的配置	将您保存的配置文件从该网络安全设备导入到主配置。 在您查看设置主配置以集中管理网络安全设备 （第 9-2 页）时，可能已保存了此配置文件。 要导入，请参阅从网络安全设备导入设置 （第 9-7 页）。

如果	操作
需要修改导入的设置。	请参阅在主配置中直接配置网络安全功能（第 9-8 页）。
尚未在网络安全设备上配置策略设置、URL 类别或旁路设置。	直接在安全管理设备上相应的主配置中配置这些设置。 请参阅在主配置中直接配置网络安全功能（第 9-8 页）。

从现有主配置导入

可以将现有主配置升级为新的主配置版本。例如，您可以将您的主配置 7.7 设置导入到主配置 8.0 和 8.5。

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置**。

步骤 2　在“选项 (Options)”列中，点击**导入配置 (Import Configuration)**。

步骤 3　对于**选择配置源 (Select Configuration Source)**，从列表中选择主配置。

步骤 4　选择是否要在此配置中包括现有的自定义用户角色。

步骤 5　点击 **Import**。

相关主题

- 关于自定义网络用户角色 （第 13-7 页）

从网络安全设备导入设置

如果想要使用其中一台网络安全设备当前正在运行的配置，可以将配置文件导入到安全管理设备来创建主配置中的策略设置。

准备工作

验证配置文件和主配置版本的兼容性。请参阅确定要使用的主配置版本 （第 9-3 页）。

注意　即使已向托管的网络安全设备发布配置，也可以根据自己的需要决定导入兼容网络配置文件的频率。将配置文件导入主配置将完全覆盖与所选主配置关联的设置。此外，“安全服务显示 (Security Services Display)”页面的安全服务设置将设置为与导入的配置匹配。

操作步骤

步骤 1　从网络安全设备保存配置文件。

步骤 2　在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 主配置**。

步骤 3　在“选项 (Options)”列中，点击**导入配置 (Import Configuration)**。

步骤 4　从“选择配置 (Select Configuration)”下拉列表中，选择**网络配置文件 (Web Configuration File)**。

步骤 5　在“新主配置默认值 (New Master Defaults)”部分，点击**浏览 (Browse)** 并从网络安全设备中选择有效的配置文件。

步骤 6　点击**导入文件 (Import File)**。

步骤 7　点击**导入 (Import)**。

在主配置中直接配置网络安全功能

根据版本不同，可以在主配置中配置以下功能：

- 身份
- SaaS 策略
- 解密策略
- 路由策略
- 访问策略
- 总体带宽限制
- 思科数据安全
- 出站恶意软件扫描
- 外部数据丢失预防
- SOCKS 策略
- 自定义 URL 类别
- 定义时间范围和配额
- 旁路设置
- L4 通信监控
- SOCKS 策略

要在主配置中直接配置各项功能的设置，请选择**网络 (Web) > 主配置 (Configuration Master)** <*版本*> > <*功能*>。

除在主配置中配置功能时特定于 SMA 的差异 （第 9-8 页）中所述的几项外，在主配置中配置功能的说明与在网络安全设备上配置相同功能的说明相同。有关说明，请参阅网络安全设备的在线帮助，或者与主配置版本相对应的 AsyncOS 版本的 《*思科网络安全设备 AsyncOS 用户指南*》。如果需要，请查阅以下主题确定适合您的网络安全设备的正确主配置：确定要使用的主配置版本 （第 9-3 页）

有关所有网络安全版本的用户指南，请参阅 http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html。

在主配置中配置功能时特定于 SMA 的差异

在主配置中配置功能时，请注意以下与直接在网络安全设备上配置相同功能的差异。

表 9-1　功能配置：主配置与网络安全设备之间的差异

功能或页面	Details
所有功能，特别是每个版本中的新功能	对于在主配置中配置的每项功能，必须在安全管理设备的 “网络 (Web)” > “实用程序 (Utilities)” > “安全服务显示 (Security Services Display)” 下启用功能。有关详细信息，请参阅确保功能一致地启用 （第 9-9 页）。
标识	• 请参阅在主配置中使用身份的提示 （第 9-9 页）。 • 如果不同网络安全设备上的身份验证领域名称相同，但协议不同，请在主配置中为所需的每个领域选择适合的方案。 • 如果作为托管设备添加了其身份验证领域支持透明用户身份识别的，则在添加或编辑身份时**透明识别用户 (Identify Users Transparently)** 选项可用。

表 9-1　功能配置：主配置与网络安全设备之间的差异 （续）

功能或页面	Details
SaaS策略	只有作为托管设备添加了身份验证领域支持透明用户身份识别的网络安全设备，身份验证选项 “提示透明用户身份识别功能发现的 SaaS 用户 (Prompt SaaS users who have been discovered by transparent user identification)”才可用。
“访问策略 (Access Policies)” > “编辑组 (Edit Group)”	配置身份和 “策略成员定义 (Policy Member Definition)”部分的 “用户 (Users)”选项时，如果使用外部目录服务器，则以下各项适用： 在 “编辑组 (Edit Group)”页面搜索组时，只显示前 500 个匹配的结果。如果没有看到所需的组，可以在 “目录 (Directory)”搜索字段中输入该组并点击 “添加 (Add)”按钮，将其添加到 “授权组 (Authorized Groups)”列表。
“访问策略 (Access Policies)” > “网络信誉和防恶意软件设置 (Web Reputation and Anti-Malware Settings)”	此页面上的可用选项取决于是否为相关主配置启用了自适应扫描。在 “网络 (Web)” > “实用程序 (Utilities)” > “安全服务显示 (Security Services Display)”中检查此设置。

在主配置中使用身份的提示

在安全管理设备上创建身份时，可以选择使其仅适用于特定设备。例如，您购买了一台安全管理设备，并希望保留为每台网络安全设备创建的现有网络安全设备配置和策略，则必须向计算机加载一个文件，然后从其他计算机手动添加策略。

实现此目标的一种方式是：为每台设备创建一组身份，然后创建引用这些身份的策略。当安全管理设备发布配置时，将自动删除和禁用引用它们的身份和策略。使用此方法，无需手动配置任何项目。实际上，这就是 “按设备”的身份。

使用此方法的唯一挑战就是，不同站点存在不同的默认策略或身份的情况。例如，如果在一个站点设置的策略是 “默认允许进行身份验证”，而在另一个站点设置的策略为 “默认拒绝”。这时，您需要在默认值上方创建按设备的身份和策略，特别是创建自己的 “默认”策略。

确保功能一致地启用

在发布主配置之前，应确保该主配置会发布并且计划的功能将按发布后的预期启用和配置。

为此，请执行以下两项操作：

- 比较启用的功能 （第 9-9 页）
- 启用功能以便发布 （第 9-10 页）

备注　如果为同一主配置分配了多个启用不同功能的网络安全设备，应单独向每台设备发布，并在每次发布前执行以下操作。

比较启用的功能

确认各个网络安全设备上启用的功能与为分配到该设备的主配置启用的功能匹配。

备注　如果为同一主配置分配了多个启用不同功能的网络安全设备，应单独向每台设备发布，并在每次发布前执行此检查。

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status)**。

步骤 2　点击要将主配置发布到的网络安全设备的名称。

步骤 3　滚动到**安全服务 (Security Services)** 表。

步骤 4　验证所有已启用功能的功能密钥是否处于活动状态且未过期。

步骤 5　比较**服务 (Services)** 列中的设置：

网络设备服务 (Web Appliance Service) 列和**管理设备上是否显示服务？ (Is Service Displayed on Management Appliance?)** 列应一致。

- “已启用 (Enabled)” = “是 (Yes)”
- “已禁用 (Disabled)”和 “未配置 (Not Configured)” = “否 (No)”或 “已禁用 (Disabled)”。
- N/A = “不适用 (Not Applicable)”。例如，选项可能无法使用主配置进行配置，但会列出，以便您可以查看功能密钥状态。

配置不匹配项将以红色文本形式显示。

后续操作

如果功能的启用/禁用设置不匹配，请执行以下任一操作：

- 更改主配置的相关设置。请参阅启用功能以便发布 （第 9-10 页）。
- 在网络安全设备上启用或禁用功能。某些更改可能会影响多项功能。有关相关功能的信息，请参阅 《*思科网络安全设备 AsyncOS 用户指南*》。

启用功能以便发布

启用要使用主配置发布设置的功能。

准备工作

确定必须启用和禁用的功能。请参阅比较启用的功能 （第 9-9 页）。

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 安全服务显示 (Security Services Display)**。

步骤 2　点击**编辑设置 (Edit Settings)**。

“编辑安全服务显示 (Edit Security Services Display)”页面将列出每个主配置中显示的功能。功能旁边的 “N/A”表示该功能在此主配置版本中不可用。

注　网络代理不作为功能列出，因为假定已启用网络代理，以便在网络安全设备上执行任何托管的策略类型。如果网络代理被禁用，将忽略发布到该网络安全设备中的任何策略。

步骤 3　（可选）隐藏不使用的主配置。要避免意外影响，请参阅禁用未使用的主配置 （第 9-11 页）中的“注意”。

步骤 4　对于将使用的每个主配置，选中或取消选中要启用的每项功能的**是 (Yes)** 复选框。

特定功能的特别说明 （可用选项视主配置版本而异）：

- 透明模式。如果使用转发模式，则代理旁路功能将不可用。
- HTTPS 代理。要配置解密策略，必须启用 HTTPS 代理。
- 上游代理组。如果希望使用路由策略，则上游代理组必须在网络安全设备上可用。

步骤 5　对您将使用的每个主配置进行更改。

步骤 6　点击 **Submit**。如果对安全服务设置的更改会影响网络安全设备上配置的策略，则 GUI 将显示特定的警告消息。如果确定要提交更改，请点击**继续 (Continue)**。

步骤 7　在**安全服务显示 (Security Services Display)** 页面中，确认所选的每个选项旁边显示**是 (Yes)**。

步骤 8　确认更改。

后续操作

- 验证对于主配置接收设备，所有功能现在是否已正确启用或禁用。请参阅比较启用的功能（第 9-9 页）。
- 在主配置接收设备的每个网络安全设备上，确保启用的功能与为主配置启用的功能一致。

禁用未使用的主配置

可以选择不显示未使用的主配置。

但是，必须至少启用一个主配置。

备注　当某个主配置被禁用时，将从 GUI 中删除所有对它的引用，包括相对应的 “主配置 (Configuration Master)” 选项卡。使用该主配置的待发布作业将被删除，而所有分配到该隐藏主配置的网络安全设备将重新归类为 “未分配”。

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 实用程序 (Utilities) > 安全服务显示 (Security Services Display)**。

步骤 2　点击**编辑设置 (Edit Settings)**。

步骤 3　取消选中未使用的主配置对应的复选框。

步骤 4　提交并确认更改。

设置以使用高级文件发布

如果您的系统设置为使用主配置，则它已设置好使用高级文件发布。

或者，完成以下主题中适用于高级文件发布及发布主配置的程序。

- 在安全管理设备上启用集中配置管理 （第 9-4 页）
- 初始化主配置 （第 9-4 页）
- 关于关联网络安全设备与主配置 （第 9-5 页）

将配置发布到网络安全设备

- 发布主配置 （第 9-12 页）
- 使用高级文件发布来发布配置 （第 9-16 页）

发布主配置

在主配置中编辑或导入设置后，可以将它们发布到与主配置关联的网络安全设备。

- 发布主配置准备工作 （第 9-12 页）
- 立即发布主配置 （第 9-14 页）
- 稍后发布主配置 （第 9-14 页）
- 使用命令行界面发布主配置 （第 9-15 页）

发布主配置准备工作

发布主配置将覆盖与该主配置关联的网络安全设备上的现有策略信息。

有关可使用主配置进行配置的设置信息，请参阅确定正确的配置发布方法 （第 9-2 页）。

所有发布作业

- 目标网络安全设备上的 AsyncOS 版本必须与主配置版本相同或高于主配置版本。有关特定要求，请参阅 SMA 兼容性列表 （第 2-2 页）。
- （仅限首次）必须遵循设置主配置以集中管理网络安全设备 （第 9-2 页）中的程序。
- 要确保主配置将会发布且发布后将启用预期的功能集，请验证每个网络安全设备的功能集及相关主配置，并进行任何所需的更改。请参阅比较启用的功能 （第 9-9 页），如有必要，请参阅启用功能以便发布 （第 9-10 页）。

  如果在分配到同一主配置的不同网络安全设备上启用了不同的功能，则必须单独向每台设备发布，并在每次发布前验证和启用功能。
- 从每台目标网络安全设备中保存配置文件，以便在发布的配置出现问题的情况下可以恢复现有配置。请参阅 《*思科网络安全设备 AsyncOS 用户指南*》，了解详细信息。

- 如果在网络安全设备上确认任何更改后，可能会导致网络代理重启，则从安全管理设备发布这些更改时，也会导致代理重启。在这些情况下，您会收到一条警告。

  如果在网络安全设备上进行的更改需要代理重启代理，发布更改时也会重启代理。例如，如果在网络安全设备上向访问策略的群组验证配置添加了新组，则在下次发布主配置时将重启网络代理。这些情况下，不会收到有关代理重启的警告。

  网络代理重启将暂时中断网络安全服务。有关重启网络代理的影响的信息，请参阅《*思科网络安全设备 AsyncOS 用户指南*》中的“确认时检查网络代理重启”部分。

- 向身份发布任何更改后，所有最终用户必须重新验证。

特殊情况

- 如果在目标网络安全设备上恢复了 AsyncOS，可能需要将不同的主配置与该设备相关联。
- 如果将主配置发布到的网络安全设备没有在启用“透明用户身份识别 (Transparent User Identification)”的情况下配置的领域，但已在身份或 SaaS 策略中选择“透明用户身份识别 (Transparent User Identification)”：
  - 对于身份，禁用“透明用户身份识别 (Transparent User Identification)”，改为选择“需要身份验证 (Require Authentication)”选项。
  - 对于 Saas 策略，禁用“透明用户身份识别 (Transparent User Identification)”选项，改为选择默认选项（“始终提示 SaaS 用户进行代理身份验证 (Always prompt SaaS users for proxy authentication)”）。
- 从安全管理设备向多个并非为 RSA 服务器配置的网络安全设备发布外部 DLP 策略时，安全管理设备将发送以下发布状态警告：

  “为主配置 <*版本*> 配置的安全服务显示设置当前不反映与此发布请求关联的网络设备上一个或多个安全服务的状态。受影响的设备如下：“<*WSA 设备名称*>”。这可能表示此特定主配置的安全服务显示设置配置不正确。请转到每个设备的“网络设备状态 (Web Appliance Status)”页面，其中提供详细的视图供您解决此问题。现在是否要继续发布配置？”

  如果决定继续发布，则并非为 RSA 服务器配置的网络安全设备将收到外部 DLP 策略，但这些策略将被禁用。如果未配置外部 DLP 服务器，网络安全设备的“外部 DLP (External DLP)”页面不会显示发布的策略。

- 如果主配置包含身份，其识别和验证用户使用的领域采用 Kerberos 方案，则以下警告适用：
  - 在升级到 AsyncOS 8.0 前在网络安全设备上创建的 Active Directory 域不支持 Kerberos 身份验证方案。
  - 如果将主配置 8.0 发布到领域名称相同但不支持 Kerberos 的网络安全设备，则会出现以下情况：

如果身份中的方案在主配置中如下：	则网络安全设备上的身份中的方案将变成
使用 Kerberos	使用 NTLMSSP 或基本
使用 Kerberos 或 NTLMSSP	使用 NTLMSSP
使用 Kerberos 或 NTLMSSP 或基本	使用 NTLMSSP 或基本

立即发布主配置

准备工作

请参阅发布主配置准备工作 （第 9-12 页）中的重要要求和信息。

操作步骤

步骤 1　在安全管理设备上，选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**。

步骤 2　点击**立即发布配置 (Publish Configuration Now)**。

步骤 3　默认情况下会选择 “系统生成的作业名称”，也可以自己输入一个作业名称 （最多 80 个字符）。

步骤 4　选择要发布的主配置。

步骤 5　选择要将主配置发布到的网络安全设备。选择 “所有已分配设备 (All assigned appliances)”，将配置发布到分配到该主配置的所有设备。

或

选择 “选择列表中的设备 (Select appliances in list)”以显示分配到该主配置的设备列表。选择要将配置发布到的设备。

步骤 6　点击**发布 (Publish)**。

“正在发布 (Publish in Progress)”页面中的红色进度栏和文本表示发布期间出现错误。如果当前正在发布另一个作业，则在完成上一个作业后将执行您的请求。

注　**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)** 页面也显示正在发布的作业的详细信息。点击**查看进度 (Check Progress)** 可访问 “正在发布 (Publish in Progress)”页面。

后续操作

检查以确保成功完成发布。请参阅查看发布历史记录 （第 9-18 页）。未完整发布的项目将予以说明。

稍后发布主配置

准备工作

请参阅发布主配置准备工作 （第 9-12 页）中的重要要求和信息。

操作步骤

步骤 1　在安全管理设备上，选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**。

步骤 2　点击**安排作业 (Schedule a Job)**。

步骤 3　默认情况下会选择 “系统生成的作业名称”，也可以自己输入一个作业名称 （最多 80 个字符）。

步骤 4　输入要发布主配置的日期和时间。

步骤 5　选择要发布的主配置。

步骤 6　选择要将主配置发布到的网络安全设备。选择 “所有已分配设备 (All assigned appliances)”，将配置发布到分配到该主配置的所有设备。

或

选择 “选择列表中的设备 (Select appliances in list)”以显示分配到该主配置的设备列表。选择要将配置发布到的设备。

步骤 7　点击 **Submit**。

步骤 8　在**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)** 页面查看安排的作业列表。要编辑安排的作业，请点击作业的名称。要取消待定作业，请点击对应的垃圾箱图标并确认要删除作业。

步骤 9　您可能需要为自己创建提醒 （例如，在日历中），以便在安排的发布时间过后进行检查，确保成功完成发布。

注　如果在安排的作业发布前重启或升级设备，则必须重新安排作业。

后续操作

检查以确保成功完成发布。请参阅查看发布历史记录 （第 9-18 页）。未完整发布的项目将予以说明。

使用命令行界面发布主配置

备注　请参阅发布主配置准备工作 （第 9-12 页）中的重要要求和信息。

安全管理设备提供使用以下 CLI 命令，通过主配置发布更改的功能：

publishconfig config_master [*--job_name*] [*--host_list* | *host_ip*]

其中， **config_master** 是受支持的主配置版本。此关键字为必填字段。 *job_name* 选项是可选项，如果未指定，将会生成。

host_list 选项是要发布的网络安全设备的主机名或 IP 地址列表，将发布到分配到主配置的所有主机 （如果未指定）。 *host_ip* 选项可以是用逗号分隔的多个主机 IP 地址。

要确认 **publishconfig** 命令是否成功，请检查 **smad_logs** 文件。还可以选择**网络 (Web) > 用程序 (Utilities) > 网络设备状态 (Web Appliance Status)**，从安全管理设备 GUI 确认发布历史记录是否成功。在此页面选择想要获取其发布历史记录详细信息的网络设备。此外，可以转到 “发布历史记录 (Publish History)”页面：**网络 (Web) > 实用程序 (Utilities) > 发布 (Publish) > 发布历史记录 (Publish History)**。

使用高级文件发布来发布配置

使用高级文件发布可从本地文件系统向托管网络安全设备推送兼容的 XML 配置文件。

有关可使用高级文件发布配置的设置的信息，请参阅确定正确的配置发布方法 （第 9-2 页）。

要执行高级文件发布，请执行以下操作：

- 高级文件发布：立即发布配置 （第 9-16 页）
- 高级文件发布：稍后发布 （第 9-17 页）

高级文件发布：立即发布配置

准备工作

- 确认将发布的配置版本是否与要发布到的设备的 AsyncOS 版本兼容。请参阅位于以下网站的兼容性矩阵：
  http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。
- 在每个目标网络安全设备上，将网络安全设备上的现有配置备份到一个配置文件。请参阅《*思科网络安全设备 AsyncOS 用户指南*》，了解详细信息。

操作步骤

步骤 1　在源网络安全设备中保存配置文件。

有关保存来自网络安全设备的配置文件的说明，请参阅 《*思科网络安全设备 AsyncOS 用户指南*》。

步骤 2　在安全管理设备窗口中，选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**。

步骤 3　点击**立即发布配置 (Publish Configuration Now)**。

步骤 4　默认情况下会选择 “系统生成的作业名称”，也可以自己输入一个作业名称 （最多 80 个字符）。

步骤 5　对于**要发布的主配置 (Configuration Master to Publish)**，选择**高级文件选项 (Advanced file options)**。

步骤 6　点击**浏览 (Browse)**，选择在步骤 1 中保存的文件。

步骤 7　在 “网络设备 (Web Appliances)” 下拉列表中，选择**选择列表中的设备 (Select appliances in list)** 或**分配到主配置的所有设备 (All assigned to Master)**，然后选择要将配置文件发布到的设备。

步骤 8　点击**发布 (Publish)**。

高级文件发布：稍后发布

准备工作

- 确认将发布的配置版本是否与要发布到的设备的 AsyncOS 版本兼容。请参阅位于以下网站的兼容性矩阵：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。
- 在每个目标网络安全设备上，将网络安全设备上的现有配置备份到一个配置文件。请参阅《*思科网络安全设备 AsyncOS 用户指南*》，了解详细信息。

操作步骤

步骤 1　在源网络安全设备中保存配置文件。

有关保存来自网络安全设备的配置文件的说明，请参阅《*思科网络安全设备 AsyncOS 用户指南*》。

步骤 2　在安全管理设备上，选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**。

步骤 3　点击**安排作业 (Schedule a Job)**。

步骤 4　默认情况下会选择**系统生成的作业名称**，也可以自己输入一个作业名称 （最多 80 个字符）。

步骤 5　输入要发布配置的日期和时间。

步骤 6　对于**要发布的主配置 (Configuration Master to Publish)**，选择**高级文件选项 (Advanced file options)**，然后点击**浏览 (Browse)** 选择在步骤 1 中保存的配置文件。

步骤 7　在 “网络设备 (Web Appliances)”下拉列表中，选择**选择列表中的设备 (Select appliances in list)** 或**分配到主配置的所有设备 (All assigned to Master)**，然后选择要将配置文件发布到的设备。

步骤 8　点击**发布 (Publish)**。

查看发布作业的状态和历史记录

查看内容	操作
已安排但尚未发布的作业列表	选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**，并查看**待发作业 (Pending Jobs)** 部分。
每个设备上次发布的配置列表	选择**网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status)**，并查看**上次发布的配置 (Last Published Configuration)** 信息。
当前正在发布的作业的状态	选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**，并查看**发布进度 (Publishing Progress)** 部分。
发布到所有或任何设备的作业历史记录	请参阅查看发布历史记录 （第 9-18 页）。

查看发布历史记录

检查发布期间可能发生的错误时，查看发布历史记录非常有用。

操作步骤

步骤 1 在安全管理设备上，选择**网络 (Web) > 实用程序 (Utilities) > 发布历史记录 (Publish History)**。

步骤 2 要查看有关特定作业的更多信息，请点击“作业名称 (Job Name)”列中的特定作业名称。

步骤 3 要查看有关作业中特定设备的更多详细信息，请点击设备名称。

此时将显示**网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status)** 页面。

步骤 4 要查看有关作业中特定设备的状态详细信息，请点击相应的**详细信息 (Details)** 链接。

此时将显示“网络设备发布详细信息 (Web Appliance Publish Details)”页面。

查看网络安全设备状态

查看网络设备的状态摘要

网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status) 页面提供连接到您的安全管理设备的网络安全设备的全面概要。

“网络设备状态 (Web Appliance Status)”页面显示连接的网络安全设备列表，包括设备名称、 IP 地址、 AsyncOS 版本、上次发布的配置信息 （用户、作业名称和配置版本）、启用或禁用的安全服务数和连接的设备总数 （最多 150 台）。警告图标指示何时需要注意连接的某台设备。

查看各个网络安全设备的状态

“设备状态 (Appliance Status)”页面提供每台连接设备的状态的详细视图。

要在 “网络设备状态 (Web Appliance Status)”页面查看管理的网络安全设备的详细信息，请点击设备的名称。

状态信息包括关于连接的网络安全设备的常规信息、其发布的配置、发布历史记录、功能密钥状态等。

备注 只有支持集中管理的计算机才会显示数据。

注　如果网络安全设备上不同版本的“可接受的使用控制引擎”与安全管理设备上的版本不匹配，将显示警告消息。如果网络安全设备上禁用或不存在该服务，将显示“N/A”。

提示　“网络设备状态 (Web Appliance Status)”页面可能需要几分钟，才会反映网络安全设备中最近发生的配置更改。要立即刷新数据，请点击**刷新数据 (Refresh Data)** 链接。页面上的时间戳显示最后刷新数据的时间。

网络设备状态详细信息

“设备状态” (Appliance Status) 页面有若干部分：

- 系统状态信息（正常运行、设备型号和序列号、AsyncOS 版本、构建日期、AsyncOS 安装日期和时间、主机名）
- 配置发布历史记录 （发布日期/时间、作业名称、配置版本、发布结果和用户）
- 集中报告状态，包括上次尝试传输数据的时间
- 网络安全设备中的功能状态 （各项功能是否已启用、功能密钥状态）
- 托管和管理设备上可接受的使用控制引擎版本
- 网络安全设备上的 “AnyConnect 安全移动 (AnyConnect Secure Mobility)”设置
- 网络安全设备的代理设置 （上游代理和代理的 HTTP 端口）
- 身份验证服务信息 （服务器、方案、领域和顺序；是否支持透明用户身份识别；以及如果身份验证失败，是阻止还是允许通信）

准备和管理 URL 类别集更新

要确保系统具有可用于管理网络使用的最新预定义 URL 类别集，可以不定期更新网络使用控制 (WUC) 的 URL 类别集：默认情况下，网络安全设备自动从思科下载 URL 类别集更新，并且安全管理设备可在几分钟内自动从托管网络安全设备接收这些更新。

由于这些更新可能会影响现有的配置和设备行为，因此您应提前准备这些更新，并在进行更新后采取相应操作。

应该采取的操作包括以下各项：

- 了解 URL 类别集更新的影响 （第 9-20 页）
- 确保您将收到关于 URL 类别集更新的通知和警报 （第 9-20 页）
- 指定新类别和已更改类别的默认设置 （第 9-20 页）
- 更新 URL 类别集后，检查您的策略和身份设置 （第 9-20 页）

了解 URL 类别集更新的影响

更新 URL 类别集后，它们可能会更改主配置中现有策略的行为。

有关更新 URL 类别集前后应采取的操作的重要信息，请参阅 《*思科网络安全设备 AsyncOS 用户指南*》中 “URL 过滤器”章节的 “管理 URL 类别集的更新”部分 （见文档 （第 E-2 页）中提供的链接）。类别说明位于同一章节的 “URL 类别说明”部分。

确保您将收到关于 URL 类别集更新的通知和警报

要接收	操作
URL 类别集更新的提前通知	立即注册以接收有关思科内容安全设备的通知，其中包括关于 URL 类别集更新的通知。请参阅思科通知服务 （第 E-1 页）。
URL 类别集更新影响现有策略设置时的警报	转到**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报 (Alerts)**，确保您配置为接收 “系统 (System)”类别的警告级别警报。有关警报的更多信息，请参阅管理警报 （第 14-28 页）。

指定新类别和已更改类别的默认设置

在更新 URL 类别集之前，应指定提供 URL 过滤的各个策略中新合并类别的默认操作，或从已配置这些设置的网络安全设备中导入配置。

有关详细信息，请参阅 《*思科网络安全设备 AsyncOS 用户指南*》或网络安全设备在线帮助 “URL 过滤器”章节中的 “选择新类别和已更改类别的默认设置”部分。

更新 URL 类别集后，检查您的策略和身份设置

URL 类别集更新将触发两种警报类型：

- 关于类别更改的警报
- 关于由于类别更改而发生变化或被禁用的策略的警报

在收到有关 URL 类别集更改的警报时，应检查基于您现有 URL 类别的策略和身份，以确保它们仍符合您的策略目标。

有关可能需要您注意的更改类型的详细信息，请参阅 《*思科网络安全设备 AsyncOS 用户指南*》中的 “响应关于 URL 类别集更新的警报”部分。

解决配置管理问题

在 “主配置 (Configuration Master)” > “身份 (Identities)”中，组不可用

问题：在 “网络 (Web)” > “主配置 (Configuration Master)” > “身份 (Identities)”中，“策略成员定义 (Policy membership definition)”页面的 “选定组和用户 (Selected groups and Users)”不显示 “组 (Groups)”选项。

解决方法：如果您有多个网络安全设备：在每个 WSA 上，在 “网络” (Network) > “身份验证” (Authentication) 中，请确保域名称在所有 WSA 间是唯一的，除非同一名称域的所有设置都是相同的。

提示：要查看各个 WSA 的领域名称，请转到 “网络 (Web)” > “实用程序 (Utilities)” > “网络设备状态 (Web Appliance Status)”，点击每个设备名称，并滚动到详细信息页面底部。

“主配置 (Configuration Master)” > “访问策略 (Access Policies)” > “网络信誉和防恶意软件设置 (Web Reputation and Anti-Malware Settings)”页面设置与预期不同

问题：主配置中的 “访问策略 (Access Policies)” > “网络信誉和防恶意软件设置 (Web Reputation and Anti-Malware Settings)”页面缺少预期的设置，包括 “网络信誉得分 (Web Reputation Score)”阈值设置和选择防恶意软件扫描引擎的功能。或者，在网络安全设备上使用自适应安全时包括这些设置。

解决方法：可用的选项取决于是否在 “网络 (Web)” > “实用程序 (Utilities)” > “安全服务显示 (Security Services Display)”设置中为该主配置选择了 “自适应安全 (Adaptive Security)”。

排除配置发布故障

问题：发布配置失败。

解决方法：查看**网络 (Web) > 实用程序 (Utilities) > Web 设备状态 (Web Appliance Status)** 页面。如果出现以下情况，发布将失败：

- “网络设备服务 (Web Appliance Service)”列中的状态与 “管理设备上是否显示服务?(Is Service Displayed on Management Appliance?)”列中的状态的不同。
- 两列都显示已启用功能，但相应的功能密钥未处于活动状态 （例如，已过期）。
- 主配置版本应与网络安全设备上的 AsyncOS 版本匹配。如果网络安全设备中的设置与主配置中的设置不匹配，向更新的网络安全设备发布较早的主配置版本可能会失败。即使 “网络设备状态 (Web Appliance Status)”页面未指示任何差异，也可能会出现失败。

相关主题

- 查看发布历史记录 （第 9-18 页）
- 比较启用的功能 （第 9-9 页）
- 启用功能以便发布 （第 9-10 页）

监控系统状态

关于安全管理设备状态

默认情况下，从浏览器访问思科内容安全管理设备时首先显示 “系统状态 (System Status)”页面。（要更改登录页面，请参阅设置首选项 （第 14-48 页）。）

在其他任何时候要访问 “系统状态 (System Status)”页面，请依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**。

在启用监控服务和添加托管设备之前，仅 “系统信息 (System Information)”部分提供状态信息。如果您已运行 “系统设置向导 (System Setup Wizard)”，启用了集中服务，并添加了tuog 设备，则 “集中服务 (Centralized Services)”部分和 “安全设备数据传输状态 (Security Appliance Data Transfer Status)”部分将将填充数据。

状态信息包括以下内容：

- **集中服务 (Centralized Services)**：每个集中服务的状态，包括处理队列使用情况
- **系统正常运行时间 (System Uptime)**：设备正常运行的时间
- **CPU 利用率 (CPU Utilization)**：每个监控服务使用的 CPU 容量百分比
- **系统版本信息 (System Version Information)**：型号、 AsyncOS （操作系统）版本、构建日期、安装日期和序列号

相关主题

- 监控处理队列 （第 10-2 页）
- 监控 CPU 利用率 （第 10-2 页）
- 监控托管设备的数据传输状态 （第 10-3 页）

监控安全管理设备容量

监控处理队列

您可以定期检查用于邮件和 Web 报告的处理队列百分比，以确定设备是否以最佳容量运行。

在等待安全管理设备处理时，处理队列会存储集中报告和跟踪文件。通常，安全管理设备会收到批量报告和跟踪文件以进行处理。处理队列中的报告和跟踪文件百分比通常随着从托管设备发送文件并且由安全管理设备进行处理而浮动。

备注　处理队列百分比衡量队列中的文件数。不考虑文件大小。百分比只是大概估计的安全管理设备的处理负载。

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**。

步骤 2　在页面顶部的**集中服务 (Centralized Services)** 部分，查看以下项目的处理队列百分比：

- 集中报告 （“邮件安全”小节）
- 集中邮件跟踪
- 集中报告 （“网络安全”小节）

步骤 3　如果处理队列使用百分比连续几小时或几天一直保持较高，则系统将满容量或超容量运行。

这种情况下，请考虑从安全管理设备移除一些托管设备，安装额外的安全管理设备，或同时实施这两种措施。

监控 CPU 利用率

要查看安全管理设备针对每项集中服务使用的 CPU 容量百分比，请执行以下操作：

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**。

步骤 2　滚动到**系统信息 (System Information)** 部分，并查看 **CPU 利用率 (CPU Utilization)** 小节。

CPU 利用率百分比表示安全管理设备的 CPU 处理投入到每个主要集中服务的部分。某些服务的利用率百分比可以合并。例如，邮件和 Web 报告合并在 “报告服务 (Reporting Service)”下，而垃圾邮件、策略、病毒和病毒爆发隔离区合并在 “隔离区服务 (Quarantine Services)”下。安全管理设备的其他操作组合在常规标题 “安全管理设备 (Security Management appliance)”下。

步骤 3　刷新浏览器显示可查看最新数据。

CPU 利用率百分比不断变化。

监控托管设备的数据传输状态

要执行集中管理功能，安全管理设备需要将托管设备中的数据成功传输到安全管理设备。“安全设备数据传输状态 (Security Appliance Data Transfer Status)”部分提供有关安全管理设备管理的每台设备的状态信息。

默认情况下，“安全设备数据传输状态 (Security Appliance Data Transfer Status)”部分最多显示十台设备。如果安全管理设备管理的设备数量超过十台，可以使用 “显示的项目 (Items Displayed)”菜单选择要显示的设备数量。

备注　“系统状态 (System Status)”页面顶部的 “服务 (Services)”部分显示有关数据传输状态的摘要信息。“安全设备数据传输状态 (Security Appliance Data Transfer Status)”部分提供设备特定的数据传输状态。

在“系统状态 (System Status)”页面的“安全设备数据传输状态 (Security Appliance Data Transfer Status)”部分，可以查看特定设备的连接状态问题。有关设备中每项服务状态的详细信息，请点击设备名称，查看设备的 “数据传输状态 (Data Transfer Status)”页面。

“数据传输状态: *Appliance_Name* (Data Transfer Status: Appliance_Name)”页面显示针对每项监控服务执行最后数据传输的时间。

邮件安全设备的数据传输状态可以是下列值之一：

- **未启用 (Not enabled)**：在邮件安全设备上未启用监控服务。
- **从未连接 (Never connected)**：在邮件安全设备上启用了监控服务，但邮件安全设备和安全管理设备之间尚未建立连接。
- **正在等待数据 (Waiting for data)**：邮件安全设备已连接到等待接收数据的安全管理设备。
- **已连接和传输数据 (Connected and transferred data)**：在邮件安全设备和安全管理设备之间已建立连接，并且数据已成功传输。
- **文件传输失败 (File transfer failure)**：在邮件安全设备和安全管理设备之间已建立连接，但数据传输失败。

网络安全设备的数据传输状态可以是下列值之一：

- **未启用 (Not enabled)**：未针对网络安全设备启用集中配置管理器。
- **从未连接 (Never connected)**：在网络安全设备上启用了集中配置管理器，但网络安全设备和安全管理设备之间尚未建立连接。
- **正在等待数据 (Waiting for data)**：网络安全设备已连接到等待接收数据的安全管理设备。
- **已连接和传输数据 (Connected and transferred data)**：在网络安全设备和安全管理设备之间已建立连接，并且数据已成功传输。
- **配置推送失败 (Configuration push failure)**：已尝试将配置文件推送到网络安全设备，但传输失败。
- **等待配置推送 (Configuration push pending)**：安全管理设备正在向网络安全设备推送配置文件。
- **等待配置推送 (Configuration push pending)**：安全管理设备已成功地将配置文件推送到网络安全设备。

数据传输问题可以反映临时网络问题或设备配置问题。第一次向安全管理设备添加托管设备时，“从未连接 (Never connected)”和“正在等待数据 (Waiting for data)”状态是正常的临时状态。如果状态最终没有变为“已连接和传输数据 (Connected and transferred data)”，则数据传输状态可能指示配置问题。

如果设备出现“文件传输失败 (File transfer failure)”状态，请监控设备，以确定故障由网络问题还是设备配置问题导致。如果没有网络问题阻止数据传输，且状态未变为“已连接和传输数据 (Connected and transferred data)”，则可能需要更改设备配置以启用数据传输。

查看托管设备的配置状态

在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

“集中服务状态 (Centralized Service Status)”部分显示启用的服务，以及用于每项服务的许可证数量。“安全设备 (Security Appliances)”部分列出您添加的设备。复选标记表示已启用的服务，“建立连接？ (Connection Established?)”列显示文件传输访问权限的配置是否正确。

相关主题

- 指定处理放行邮件的备用设备 （第 8-7 页）
- 关于添加托管设备 （第 2-10 页）

网络安全设备的其他状态信息

有关网络安全设备的其他状态信息，请参阅查看网络安全设备状态 （第 9-18 页）。

监控报告数据可用性状态

通过安全管理设备，可以监控指定期间报告数据的可用性。请参阅设备适当的部分：

- 监控邮件安全报告数据可用性 （第 10-4 页）
- 监控网络安全报告数据可用性 （第 10-5 页）

监控邮件安全报告数据可用性

要在安全管理设备上监控来自邮件安全设备的报告数据，请依次查看**邮件 (Email) > 报告 (Reporting) > 报告数据可用性 (Reporting Data Availability)** 页面。

在**报告数据可用性 (Reporting Data Availability)** 页面，可以查看在指定期间安全管理设备从邮件安全设备收到的报告数据百分比。条形图表示在该时间范围收到的数据完整性。

可以监控前一天、前一周、前一个月或前一年的报告数据可用性。如果安全管理设备从邮件安全设备接收的报告数据少于 100%，可以立即得知您的数据不完整。使用数据可用性信息可验证报告数据，并解决系统问题。

备注　如果由于硬件故障或其他原因必须更换邮件安全设备，则被替换的邮件安全设备中的数据不会丢失，但数据在安全管理设备上无法正确显示。

监控网络安全报告数据可用性

要在安全管理设备上监控来自网络安全设备的报告数据，请依次查看**网络 (Web) > 报告 (Reporting) > 数据可用性 (Data Availability)** 页面。

在 “数据可用性 (Data Availability)” 页面，可以更新和排序数据，以便您实时了解资源利用率和网络流量问题点。

备注 在 “Web 报告数据可用性 (Web Reporting Data Availability)” 窗口，只有 Web 报告和邮件报告**都**被禁用时， Web 报告才会显示已禁用状态。

此页面中会显示所有数据资源利用率和网络流量故障点。点击列出的网络安全设备链接之一，可以查看该设备的报告数据可用性。

可以监控前一天、前一周、前一个月或前一年的报告数据可用性。如果安全管理设备从网络安全设备接收的报告数据少于 100%，可以立即得知您的数据不完整。使用数据可用性信息可验证报告数据，并解决系统问题。

如果在针对 URL 类别的计划报告中使用了数据可用性，并且任何设备的数据中存在差距，则会在页面底部显示以下信息：“Some data in this time range was unavailable.”如果没有差距，则不会显示任何内容。

有关网络安全设备上的 “数据可用性 (Data Availability)” 页面的详细信息，请参阅 “数据可用性页面”。

监控邮件跟踪数据状态

要监控邮件跟踪数据的状态，请依次查看**邮件 (Email) > 邮件跟踪 (Message Tracking) > 邮件跟踪数据可用性 (Message Tracking Data Availability)** 页面。

备注 邮件安全设备将重复复制从该设备获取的报告和跟踪数据，并将这些数据文件的副本放到默认目录之外的其他文件夹。然后，可以将安全管理设备配置为从这些文件夹之一提取数据。

“邮件跟踪数据可用性 (Message Tracking Data Availability)” 页面允许您查看安全管理设备缺失数据的间隔。缺失数据间隔是指安全管理设备未从组织的邮件安全设备收到任何邮件跟踪数据的时间段。

可以监控系统中特定托管设备或所有邮件安全设备的数据可用性。如果在邮件跟踪数据中发现缺失数据的间隔，可以立即得知您的数据可能不完整。使用数据可用性信息可验证邮件跟踪数据，并解决系统问题。

监控托管设备的容量

您可以从安全管理设备监控托管设备的容量。可以检查所有邮件或网络安全设备的统一容量，也可以查看单个设备的容量。

要查看以下设备的容量	请参阅
托管网络安全设备	系统容量页面 （第 5-27 页）
托管邮件安全设备	系统容量页面 （第 4-29 页）

识别有效的 TCP/IP 服务

要识别安全管理设备使用的有效 TCP/IP 服务，请在命令行界面中使用 `tcpservices` 命令。

与 LDAP 集成

概述

如果在企业 LDAP 目录 （例如，在 Microsoft Active Directory、 SunONE Directory Server 或 OpenLDAP 目录）中维护最终用户密码和邮件别名，则可以使用 LDAP 目录对以下用户进行身份验证：

- 访问垃圾邮件隔离区的最终用户和管理用户。

  当用户登录到网络 UI 以访问垃圾邮件隔离区时， LDAP 服务器会验证登录名和密码，并且 AsyncOS 会检索对应邮件别名的列表。只要未被设备重写，发送到任何用户的邮件别名的已隔离邮件都会显示在垃圾邮件隔离区中。

  请参阅配置 LDAP 以与垃圾邮件处理隔离区配合使用 （第 11-2 页）。

- 启用并配置外部身份验证后，登录到思科内容安全管理设备的管理用户。

  请参阅使用 LDAP 配置管理用户的外部身份验证 （第 11-13 页）。

配置 LDAP 以与垃圾邮件处理隔离区配合使用

配置思科内容安全设备以与 LDAP 目录配合使用时，必须完成以下步骤以进行接受、路由、别名和伪装设置：

操作步骤

步骤 1　**配置 LDAP 服务器配置文件**。

服务器配置文件包含用于启用 AsyncOS 以连接到 LDAP 服务器的信息，例如：

- 服务器名称和端口
- Base DN
- 绑定到服务器的身份验证要求

有关配置服务器配置文件的详细信息，请参阅创建 LDAP 服务器配置文件 （第 11-2 页）。

创建 LDAP 服务器配置文件时，可以配置 AsyncOS 以连接到多个 LDAP 服务器。有关详细信息，请参阅配置 AsyncOS 以与多个 LDAP 服务器配合使用 （第 11-11 页）。

步骤 2　**配置 LDAP 查询**。

可以使用为 LDAP 服务器配置文件生成的默认垃圾邮件隔离区查询，或者根据特定 LDAP 实施和方案创建自己的定制查询。然后，将用于垃圾邮件通知和最终用户访问的有效查询指定给隔离区。

有关这些查询的信息，请参阅配置 LDAP 查询 （第 11-4 页）。

步骤 3　**为垃圾邮件隔离区启用 LDAP 最终用户访问和垃圾邮件通知**。

启用对垃圾邮件隔离区的 LDAP 最终用户访问，以允许最终用户查看和管理其隔离区中的邮件。还可以为垃圾邮件通知启用别名整合，以防止用户接收多个通知。

有关详细信息，请参阅设置集中式垃圾邮件隔离区 （第 7-2 页）。

创建 LDAP 服务器配置文件

配置 AsyncOS 以使用 LDAP 目录时，创建 LDAP 服务器配置文件来存储有关 LDAP 服务器的信息。

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > LDAP**。

步骤 2　点击**添加 LDAP 服务器配置文件 (Add LDAP Server Profile)**。

步骤 3　在 **LDAP 服务器配置文件名称 (LDAP Server Profile Name)** 文本字段中输入服务器配置文件的名称。

步骤 4　在**主机名 (Host Name(s))** 文本字段中，输入 LDAP 服务器的主机名。

可以输入多个主机名以配置用于故障转移或负载均衡的 LDAP 服务器。使用逗号分隔多个条目。有关详细信息，请参阅配置 AsyncOS 以与多个 LDAP 服务器配合使用 （第 11-11 页）。

步骤 5　选择身份验证方法。可以使用匿名身份验证或指定用户名和密码。

备注　需要配置 LDAP 身份验证以在报告中查看客户端用户 ID，而不是客户端 IP 地址。如果没有 LDAP 身份验证，系统只能通过用户的 IP 地址来指代用户。选择**使用密码 (Use Password)** 单选按钮，然后输入用户名和密码。用户名将随即显示在 “内部用户摘要 (Internal Users Summary)” 页面上。

步骤 6　选择 LDAP 服务器类型：Active Directory、 OpenLDAP 或 “未知或其他 (Unknown or Other)”。

步骤 7　输入端口号。

默认端口为 3268。这是 Active Directory 的默认端口，用于在多服务器环境中访问全局目录。

步骤 8　输入 LDAP 服务器的基本 DN （可区别名称）。

如果通过用户名和密码进行身份验证，则用户名必须包含具有密码的条目的完整 DN。例如，邮件地址为 joe@example.com 的用户是营销组的用户。此用户的条目类似于以下条目：

```
uid=joe, ou=marketing, dc=example dc=com
```

步骤 9　在 “高级 (Advanced)” 下，选择在与 LDAP 服务器通信时是否使用 SSL。

步骤 10　输入缓存生存时间。此值表示保留缓存的时长。

步骤 11　输入保留缓存条目的最大数量。

步骤 12　输入最大并发连接数。

如果配置用于负载均衡的 LDAP 服务器配置文件，则这些连接会分布在列出的 LDAP 服务器之间。例如，如果配置 10 个并发连接并且通过三台服务器对连接进行负载均衡，则 AsyncOS 会与每台服务器建立 10 个连接，总共建立 30 个连接。有关详细信息，请参阅负载均衡 （第 11-12 页）。

注　最大并发连接数包括用于 LDAP 查询的 LDAP 连接。但是，如果为垃圾邮件隔离区启用 LDAP 身份验证，则除了总计 30 个连接外，设备还允许为最终用户隔离区额外建立 20 个连接。

步骤 13　通过点击**测试服务器 (Test Server(s))** 按钮测试服务器连接。如果指定了多个 LDAP 服务器，则会对它们全部进行测试。测试结果会显示在 “连接状态 (Connection Status)” 字段中。有关详细信息，请参阅测试 LDAP 服务器 （第 11-4 页）。

步骤 14　通过选中相应的复选框并填写相关字段，创建垃圾邮件隔离区查询。

可以配置隔离区最终用户身份验证查询，以在用户登录最终用户隔离区时对其进行验证。可以配置别名整合查询，以便最终用户不会针对每个邮件别名都收到隔离区通知。要使用这些查询，请选中 “指定为有效查询 (Designate as the active query)” 复选框。有关详细信息，请参阅配置 LDAP 查询 （第 11-4 页）。

步骤 15　通过点击**测试查询 (Test Query)** 按钮测试垃圾邮件隔离区查询。

输入测试参数并点击**运行测试 (Run Test)**。测试结果会显示在 “连接状态 (Connection Status)” 字段中。如果对查询定义或属性进行任何更改，请点击**更新 (Update)**。

注　如果将 LDAP 服务器配置为允许与空密码进行绑定，则查询可以使用空密码字段通过测试。

步骤 16　提交并确认更改。

Active Directory 服务器配置不允许在 Windows 2000 中通过 TLS 进行身份验证。这是 Active Directory 的已知问题。*可以*对 Active Directory 和 Windows 2003 进行 TLS 身份验证。

备注　尽管服务器配置的数量不受限制，但是可以仅为每台服务器配置一个最终用户身份验证查询和一个别名整合查询。

测试 LDAP 服务器

使用 “添加/编辑 LDAP 服务器配置文件 (Add/Edit LDAP Server Profile)” 页面上的**测试服务器 (Test Server(s))** 按钮 （或 CLI 中 `ldapconfig` 命令的 `test` 子命令）来测试与 LDAP 服务器的连接。 AsyncOS 会显示消息，指明与服务器端口的连接是成功还是失败。如果配置了多台 LDAP 服务器，则 AsyncOS 会测试每台服务器并显示各个测试结果。

配置 LDAP 查询

以下部分针对每种类型的垃圾邮件隔离区查询，提供默认查询字符串和配置详细信息：

- **垃圾邮件隔离区最终用户身份验证查询。**有关详细信息，请参阅 “垃圾邮件隔离区最终用户身份验证查询”部分 （第 11-5 页）。
- **垃圾邮件隔离区别名整合查询。**有关详细信息，请参阅垃圾邮件隔离区别名整合查询 （第 11-6 页）。

要使隔离区对最终用户访问或垃圾邮件通知使用 LDAP 查询，请选中 “指定为有效查询 (Designate as the active query)” 复选框。可以指定一个最终用户身份验证查询来控制隔离区访问，并为垃圾邮件通知指定一个别名整合查询。任何现有有效查询均被禁用。在安全管理设备上，选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > LDAP** 页面，在有效查询旁边会显示一个星号 (*)。

还可以指定基于域的查询或链查询作为有效最终用户访问或垃圾邮件通知查询。有关详细信息，请参阅基于域的查询 （第 11-8 页）和链查询 （第 11-9 页）。

备注 使用 “LDAP” 页面上的**测试查询 (Test Query)** 按钮 （或 **ldaptest** 命令）验证查询是否返回了预期结果。

LDAP 查询语法

LDAP 路径中允许有空格，而且不需要加引号。 CN 和 DC 语法不区分大小写。

Cn=First Last,oU=user,dc=domain,DC=COM

为查询输入的变量名称区分大小写，且必须与 LDAP 实施匹配才能正常工作。例如，在提示符处输入 **mailLocalAddress** 执行的查询与输入 **maillocaladdress** 所执行的查询是不同的。

令牌

可以在 LDAP 查询中使用以下令牌：

- {a} 用户名@域名
- {d} 域
- {dn} 可区别名称
- {g} 组名
- {u} 用户名
- {f} MAILFROM: 地址

备注　{f} 令牌仅在接受查询中有效。

例如，可以使用以下查询接受 Active Directory LDAP 服务器的邮件：
(|(mail={a})(proxyAddresses=smtp:{a}))

备注　在监听程序上启用 LDAP 功能之前，我们强烈建议使用 “LDAP” 页面的测试功能 （或 **ldapconfig** 命令的 **test** 子命令）来测试所构建的所有查询，并确保返回预期结果。有关详情，请参阅 “测试 LDAP 查询”部分 （第 11-7 页）。

垃圾邮件隔离区最终用户身份验证查询

当用户登录到垃圾邮件隔离区时，最终用户身份验证查询会对用户进行验证。令牌 {u} 指定了该用户 （它表示用户的登录名）。令牌 {a} 指定了该用户的邮件地址。 LDAP 查询不会从邮件地址中剥离 “SMTP:”； AsyncOS 会剥离地址中的该部分。

根据服务器类型， AsyncOS 会将以下默认查询字符串之一用于最终用户身份验证查询：

- **Active Directory：** `(sAMAccountName={u})`
- **OpenLDAP：** `(uid={u})`
- **未知或其他：**[空白]

默认情况下，主邮件属性是为 **mail**。可以输入自己的查询和邮件属性。要在 CLI 中创建查询，请使用 **ldapconfig** 命令的 `isqauth` 子命令。

备注　如果希望用户使用其完整邮件地址登录，请将 `(mail=smtp:{a})` 用于查询字符串。

Active Directory 最终用户身份验证设置示例

此部分显示 Active Directory 服务器和最终用户身份验证查询的设置示例。此示例将密码身份验证用于 Active Directory 服务器，将最终用户身份验证的默认查询字符串用于 Active Directory 服务器，并且使用了 `mail` 和 `proxyAddresses` 邮件属性。

表 11-1　LDAP 服务器和垃圾邮件隔离区最终用户身份验证设置示例：Active Directory

身份验证方法	**使用口令** **（需要创建一个低权限用户以绑定用于搜索，或配置匿名搜索。）**
服务器类型	Active Directory
端口	3268
Base DN	[空白]
访问协议	[空白]
查询字符串	`(sAMAccountName={u})`
邮件属性	`mail,proxyAddresses`

OpenLDAP 最终用户身份验证设置示例

此部分显示 OpenLDAP 服务器和最终用户身份验证查询的设置示例。此示例将匿名身份验证用于 OpenLDAP 服务器，将最终用户身份验证的默认查询字符串用于 Active Directory 服务器，并且使用了 `mail` 和 `mailLocalAddress` 邮件属性。

表 11-2　LDAP 服务器和垃圾邮件隔离区最终用户身份验证设置示例：OpenLDAP

身份验证方法	**匿名**
服务器类型	OpenLDAP
端口	389
Base DN	[空白]（某些较早的方案需要使用特定的基本 DN。）
访问协议	[空白]
查询字符串	`(uid={u})`
邮件属性	`mail,mailLocalAddress`

垃圾邮件隔离区别名整合查询

如果使用垃圾邮件通知，垃圾邮件隔离区别名整合查询会整合邮件别名，以便收件人不会针对每个别名都收到隔离区通知。例如，收件人可能收到针对以下邮件地址的邮件：john@example.com、jsmith@example.com 和 john.smith@example.com。使用别名整合时，收件人会在所选的主邮件地址收到一个垃圾邮件通知，获得发送到所有用户别名的邮件。

要将邮件整合到主邮件地址，请创建查询来搜索收件人的备用邮件别名，然后在 “邮件属性 (Email Attribute)”字段中输入收件人的主邮件地址的属性。

对于 Active Directory 服务器，默认查询字符串(可能随您的部署而异)为 `(|(proxyAddresses={a})(proxyAddresses=smtp:{a}))`，默认邮件属性为 `mail`。对于 OpenLDAP 服务器，默认查询字符串为 `(mail={a})`，默认邮件属性为 `mail`。可以定义自己的查询和邮件属性，包括逗号分隔的多个属性。如果输入多个邮件属性，则思科建议输入使用单个值的独特属性 （例如 `mail`）作为第一个邮件属性，而不是输入具有可更改的多个值的属性 （例如 `proxyAddresses`）。

要在 CLI 中创建查询，请使用 `ldapconfig` 命令的 `isqalias` 子命令。

- Active Directory 别名整合设置示例 （第 11-6 页）
- OpenLDAP 别名整合设置示例 （第 11-7 页）

Active Directory 别名整合设置示例

此部分显示 Active Directory 服务器和别名整合查询的设置示例。此示例将匿名身份验证用于 Active Directory 服务器，将别名整合的查询字符串用于 Active Directory 服务器，并且使用了 `mail` 邮件属性。

表 11-3　LDAP 服务器和垃圾邮件隔离区别名整合设置示例：Active Directory

身份验证方法	**匿名**
服务器类型	Active Directory
端口	3268
Base DN	[空白]
访问协议	使用 SSL

表 11-3　LDAP 服务器和垃圾邮件隔离区别名整合设置示例：Active Directory （续）

身份验证方法	匿名
查询字符串	(|(mail={a})(mail=smtp:{a}))
邮件属性	邮件

OpenLDAP 别名整合设置示例

此部分显示 OpenLDAP 服务器和别名整合查询的设置示例。此示例将匿名身份验证用于 OpenLDAP 服务器，将别名整合的查询字符串用于 OpenLDAP 服务器，并且使用了 `mail` 邮件属性。

表 11-4　LDAP 服务器和垃圾邮件隔离区别名整合设置示例：OpenLDAP

身份验证方法	匿名
服务器类型	OpenLDAP
端口	389
Base DN	[空白]（某些较早的方案需要使用特定的基本 DN。）
访问协议	使用 SSL
查询字符串	`(mail={a}))`
邮件属性	邮件

测试 LDAP 查询

使用 “添加 LDAP 服务器配置文件 (Add LDAP Server Profile)” / “编辑 LDAP 服务器配置文件 (Edit LDAP Server Profile)”页面上的**测试查询 (Test Query)** 按钮 （或 CLI 中的 `ldaptest` 命令）来测试查询。 AsyncOS 显示有关查询连接测试每个阶段的详细信息。例如，第一阶段 SMTP 授权是成功还是失败，以及 BIND 匹配返回了 true 还是 false 结果。

`ldaptest` 命令以批处理命令的形式提供，例如：

```
ldaptest LDAP.isqalias foo@cisco.com
```

为查询输入的变量名称*区分大小写*，且必须与 LDAP 实施匹配才能正常工作。例如，为邮件属性输入 `mailLocalAddress` 所执行的查询与输入 `maillocaladdress` 所执行的查询是不同的。

要测试查询，必须输入测试参数并点击**运行测试 (Run Test)**。结果会显示在 “测试连接 (Test Connection)”字段中。如果最终用户身份验证查询成功，则会显示结果 “Success: Action: match positive”。对于别名整合查询，会显示结果 “Success: Action: alias consolidation”，以及用于整合垃圾邮件通知的邮件地址。如果查询失败， AsyncOS 会显示失败原因，例如找不到匹配的 LDAP 记录，或者匹配的记录不包含邮件属性。如果使用多个 LDAP 服务器，则思科内容安全设备会在每个 LDAP 服务器上测试查询。

基于域的查询

基于域的查询是按类型分组并且与域关联的 LDAP 查询。如果不同的 LDAP 服务器与不同的域关联，但是要为用于最终用户隔离区访问的所有 LDAP 服务器运行查询，则可能需要使用基于域的查询。例如，一家名为 Bigfish 的公司拥有域 Bigfish.com、 Redfish.com 和 Bluefish.com，并且为与各个域关联的员工维护不同的 LDAP 服务器。 Bigfish 可以使用基于域的查询根据三个域的 LDAP 目录对最终用户进行身份验证。

要使用基于域的查询控制垃圾邮件隔离区的最终用户访问或通知，请完成以下步骤：

操作步骤

步骤 1　为要在基于域的查询中使用的每个域创建 LDAP 服务器配置文件。在每个服务器配置文件中，配置要在基于域的查询中使用的查询。有关详细信息，请参阅创建 LDAP 服务器配置文件 （第 11-2 页）。

步骤 2　创建基于域的查询。当创建基于域的查询时，从每个服务器配置文件中选择查询，并指定基于域的查询作为垃圾邮件隔离区的有效查询。有关创建查询的详细信息，请参阅创建基于域的查询（第 11-8 页）。

步骤 3　为垃圾邮件隔离区启用最终用户访问或垃圾邮件通知。有关详细信息，请参阅设置集中式垃圾邮件隔离区 （第 7-2 页）。

创建基于域的查询

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > LDAP**。

步骤 2　在 “LDAP”页面上，点击**高级 (Advanced)**。

步骤 3　输入基于域的查询的名称。

步骤 4　选择查询类型。

注　创建基于域的查询时，指定单个查询类型。选择查询类型后，查询字段下拉列表会包含 LDAP 服务器配置文件中的相应查询。

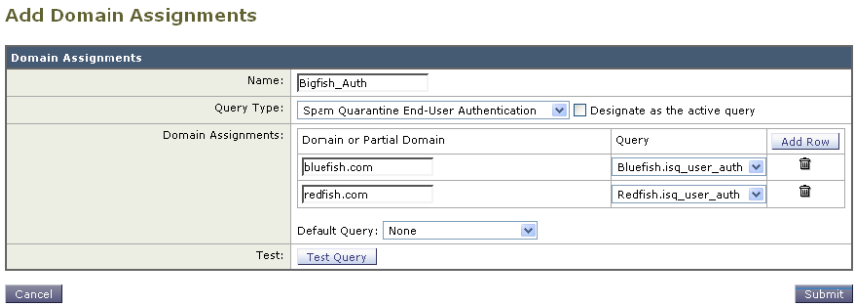
步骤 5　在 “域分配 (Domain Assignments)”字段中，输入域。

步骤 6　选择要与域关联的查询。

步骤 7　为基于域的查询中的每个域添加一个行并选择查询。

步骤 8　如果所有其他查询失败，请输入默认查询。如果不希望输入默认查询，请选择**无 (None)**。

图 11-1　　基于域的查询示例



步骤 9　通过点击**测试查询 (Test Query)** 按钮并在测试参数字段中输入要测试的用户登录名和密码或者邮件地址，以测试查询。结果会显示在 “连接状态 (Connection Status)” 字段中。

步骤 10　如果希望垃圾邮件隔离区使用基于域的查询，请选中**指定为有效查询 (Designate as the active quer)** 复选框。

注　基于域的查询会成为指定查询类型的有效 LDAP 查询。例如，如果基于域的查询用于最终用户身份验证，则会成为垃圾邮件隔离区的有效最终用户身份验证查询。

步骤 11　点击**提交 (Submit)**，然后点击**确认 (Commit)** 以确认更改。

备注　要在命令行界面上进行相同的配置，请在命令行提示中键入 `ldapconfig` 命令的 `advanced` 子命令。

链查询

链查询是 AsyncOS 连续运行的一系列 LDAP 查询。 AsyncOS 会按照 “链” 中各个查询的顺序运行每个查询，直到 LDAP 服务器返回正面响应或者最终查询返回负面响应或失败。如果 LDAP 目录中的条目使用不同的属性存储相似 （或相同）的值，则链查询会非常有用。例如，组织中的部门可能使用不同类型的 LDAP 目录。 IT 部门可能使用 OpenLDAP，而销售部门使用 Active Directory。为了确保查询根据两种类型的 LDAP 目录运行，可以使用链查询。

要使用链查询控制对垃圾邮件隔离区的最终用户访问或通知，请完成以下步骤：

操作步骤

步骤 1　为要在链查询中使用的每个查询创建 LDAP 服务器配置文件。对于每个服务器配置文件，配置要用于链查询的查询。有关详细信息，请参阅创建 LDAP 服务器配置文件 （第 11-2 页）。

步骤 2　创建链查询并将其指定为垃圾邮件隔离区的有效查询。有关详细信息，请参阅创建链查询 （第 11-10 页）。

步骤 3　为垃圾邮件隔离区启用 LDAP 最终用户访问或垃圾邮件通知。有关垃圾邮件隔离区的详细信息，请参阅设置集中式垃圾邮件隔离区 （第 7-2 页）。

创建链查询

提示　还可以使用 CLI 中 `ldapconfig`命令的 `advanced` 子命令。

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > LDAP > LDAP 服务器 (LDAP Server)**。

步骤 2　从 “LDAP 服务器配置文件 (LDAP Server Profiles)”页面上，点击**高级 (Advanced)**。

步骤 3　点击**添加链接的查询 (Add Chained Query)**。

步骤 4　输入链查询的名称。

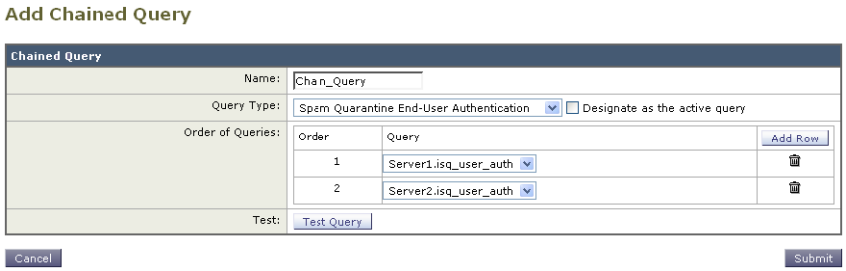
步骤 5　选择查询类型。

创建链查询时，其所有组件查询都具有相同的查询类型。选择查询类型后，查询字段下拉列表会显示 LDAP 服务器中的相应查询。

步骤 6　选择链中的第一个查询。

思科内容安全设备会按照配置顺序运行查询。如果将多个查询添加到链查询，则可能需要对它们进行排序，以便常规查询在粒度查询之后。

图 11-2　　链查询示例



步骤 7　通过点击**测试查询 (Test Query)** 按钮并在测试参数字段中输入用户登录名和密码或者邮件地址，以测试查询。结果会显示在 “连接状态 (Connection Status)”字段中。

步骤 8　如果希望垃圾邮件隔离区使用域查询，请选中**指定为有效查询 (Designate as the active quer)** 复选框。

注　链查询会成为指定查询类型的有效 LDAP 查询。例如，如果链查询用于最终用户身份验证，则会成为垃圾邮件隔离区的有效最终用户身份验证查询。

步骤 9　提交并确认更改。

备注　要在命令行界面上进行相同的配置，请在命令行提示中键入 `ldapconfig` 命令的 `advanced` 子命令。

配置 AsyncOS 以与多个 LDAP 服务器配合使用

配置 LDAP 服务器配置文件时，可以配置思科内容安全设备以连接到列表中的多个 LDAP 服务器。如果使用多个 LDAP 服务器，它们需要包含相同的信息，具有相同的结构，并且使用相同的身份验证信息。存在可以整合记录的第三方产品。

配置思科内容安全设备以连接到冗余 LDAP 服务器，从而使用以下功能：

- **故障转移**。如果思科内容安全设备无法连接到 LDAP 服务器，它会连接到列表中的下一台服务器。
- **负载均衡**。在执行 LDAP 查询时，思科内容安全设备将在列表中的 LDAP 服务器之间分发连接。

可以在“管理设备 (Management Appliance)”>“系统管理 (System Administration)”>“LDAP”页面上，或通过使用 CLI 的 `ldapconfig` 命令配置冗余 LDAP 服务器。

测试服务器和查询

使用“添加 LDAP 服务器配置文件 (Add LDAP Server Profile)”或“编辑 LDAP 服务器配置文件 (Edit LDAP Server Profile)”页面上的**测试服务器 (Test Server(s))** 按钮 （或 CLI 中的 `test` 子命令）来测试与 LDAP 服务器的连接。如果使用多个 LDAP 服务器，则 AsyncOS 会测试每台服务器并显示每台服务器的各个结果。 AsyncOS 还将在每台 LDAP 服务器上测试查询并显示各个结果。

故障切换

要确保 LDAP 服务器可用于解析查询，可配置用于故障转移的 LDAP 配置文件。

思科内容安全设备会在指定的时间段内尝试连接到 LDAP 服务器列表中的第一台服务器。如果设备无法连接到列表中的第一台 LDAP 服务器，则会尝试连接到列表中的下一台 LDAP 服务器。为确保思科内容安全设备在默认情况下连接到主 LDAP 服务器，请将其输入为 LDAP 服务器列表中的第一台服务器。

如果思科内容安全设备连接到第二台或后续的 LDAP 服务器，则会在指定的时间段内保持连接到该服务器。在此时间段结束后，设备会尝试重新连接到列表中的第一台服务器。

配置思科内容安全设备以用于 LDAP 故障转移

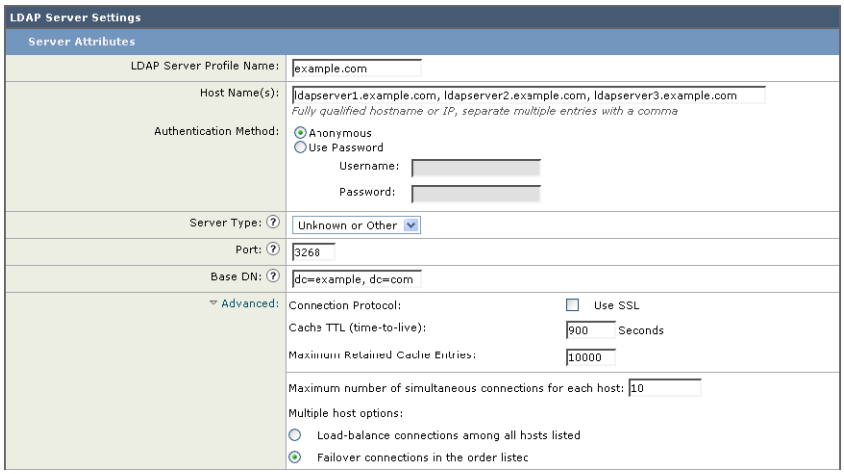
操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > LDAP**。

步骤 2　选择要编辑的 LDAP 服务器配置文件。

在以下示例中， LDAP 服务器名称为 example.com。

图 11-3　　LDAP 故障转移配置示例



步骤 3　在“主机名 (Hostname)”文本字段中，键入 LDAP 服务器。例如 **ldapserver.example.com**。

步骤 4　在“每台主机的最大并发连接数 (Maximum number of simultaneous connections for each host)”文本字段中，键入最大连接数。

在本示例中，最大连接数为 **10**。

步骤 5　点击**顺序列表中的故障转移连接 (Failover connections in the order list)** 旁的单选按钮。

步骤 6　根据需要配置其他 LDAP 选项。

步骤 7　提交并确认更改。

负载均衡

要在一组 LDAP 服务器中分发 LDAP 连接，可以配置用于负载均衡的 LDAP 配置文件。

使用负载均衡时，思科内容安全设备会在列出的 LDAP 服务器之间分发连接。如果连接失败或超时，设备会确定哪些 LDAP 服务器可用，并重新连接到可用的服务器。设备会基于配置的最大连接数确定要建立的并发连接数。

如果其中一台所列的 LDAP 服务器未响应，设备将在剩余的 LDAP 服务器之间分发的连接。

配置用于负载均衡的思科内容安全设备

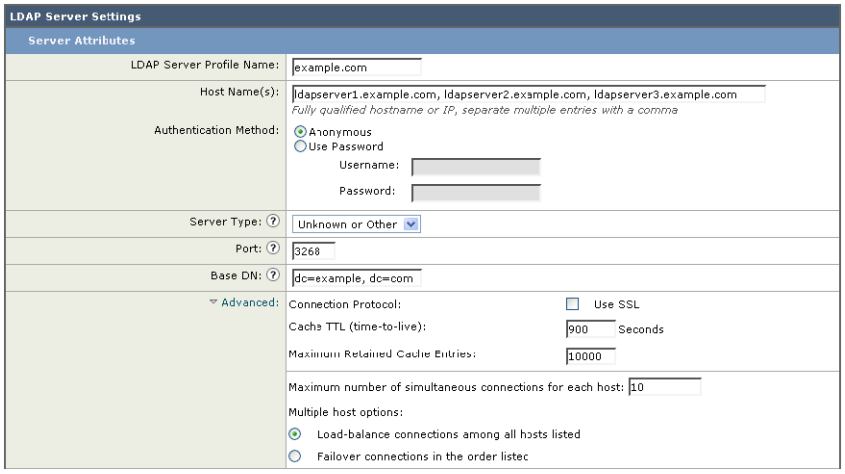
操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > LDAP**。

步骤 2　选择要编辑的 LDAP 服务器配置文件。

在以下示例中， LDAP 服务器名称为 example.com。

图 11-4　　负载均衡配置示例



步骤 3　在 “主机名 (Hostname)”文本字段中，键入 LDAP 服务器。例如 **ldapserver.example.com**。

步骤 4　在 “每台主机的最大并发连接数 (Maximum number of simultaneous connections for each host)”文本字段中，键入最大连接数。

在本示例中，最大连接数为 **10**。

步骤 5　点击**所有主机之间的负载均衡 (Load balance connections among all hosts)** 旁的单选按钮。

步骤 6　根据需要配置其他 LDAP 选项。

步骤 7　提交并确认更改。

使用 LDAP 配置管理用户的外部身份验证

可以配置思科内容安全设备以使用网络上的 LDAP 目录对管理用户进行身份验证，方法是允许他们使用 LDAP 用户名和密码登录设备。

操作步骤

步骤 1　**配置 LDAP 服务器配置文件。**请参阅创建 LDAP 服务器配置文件 （第 11-2 页）。

步骤 2　**创建查询以查找用户帐户。**在 LDAP 服务器配置文件的 “外部身份验证查询 (External Authentication Queries)”部分中，创建一个查询以在 LDAP 目录中搜索用户帐户。请参阅用于验证管理用户的用户帐户查询 （第 11-14 页）。

步骤 3　**创建组成员身份查询。**创建一个查询以确定用户是否为目录组的成员，并创建一个单独查询来查找组的所有成员。有关更多信息，请参阅用于验证管理用户的组成员身份查询 （第 11-15 页）以及邮件安全设备文档或在线帮助。

备注　使用页面上 “外部身份验证查询 (External Authentication Queries)” 部分中的**测试查询 (Test Query)** 按钮 （或 `ldaptest` 命令）验证查询是否返回了预期结果。有关相关信息，请参阅测试 LDAP 查询 （第 11-7 页）。

步骤 4　**设置外部身份验证以使用 LDAP 服务器。**启用设备以将 LDAP 服务器用于用户身份验证，并将用户角色分配给 LDAP 目录中的组。有关更多信息，请参阅启用管理用户的外部身份验证（第 11-16 页）以及邮件安全设备文档或在线帮助中的 “添加用户”。

用于验证管理用户的用户帐户查询

为了验证外部用户， AsyncOS 会使用查询搜索 LDAP 目录中的用户记录以及包含用户全名的属性。根据选择的服务器类型， AsyncOS 会输入默认查询和默认属性。如果在 LDAP 用户记录的 RFC 2307 中定义了属性 （**shadowLastChange**、 **shadowMax** 和 **shadowExpire**），则可以选择使设备拒绝具有过期帐户的用户。在用户记录所在的域级别需要基本 DN。

表 11-5 显示了 AsyncOS 在 Active Directory 服务器上搜索用户帐户时使用的默认查询字符串和用户全名属性。

表 11-5　Active Directory 服务器的默认查询字符串

服务器类型	**Active Directory**
Base DN	[空白] （需要使用特定的基本 DN 来查找用户记录。）
查询字符串	`(&(objectClass=user)(sAMAccountName={u}))`
包含用户全名的属性	`displayName`

表 11-6 显示了 AsyncOS 在 OpenLDAP 服务器上搜索用户帐户时使用的默认查询字符串和用户全名属性。

表 11-6　OpenLDAP 服务器的默认查询字符串

服务器类型	**OpenLDAP**
Base DN	[空白] （需要使用特定的基本 DN 来查找用户记录。）
查询字符串	`(&(objectClass=posixAccount)(uid={u}))`
包含用户全名的属性	`gecos`

用于验证管理用户的组成员身份查询

可以将 LDAP 组与访问设备的用户角色相关联。

AsyncOS 还会使用查询来确定用户是否为目录组的成员，并使用一个单独的查询来查找组的所有成员。目录组成员身份中的成员身份会确定系统中的用户权限。在 GUI 的 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “用户 (Users)” 页面上（或使用 CLI 中的 `userconfig`）启用外部身份验证时，将用户角色分配给 LDAP 目录中的组。用户角色会确定用户在系统中所具有的权限，并且对于在外部进行身份验证的用户，角色将分配给目录组而不是各个用户。例如，可以为 IT 目录组中的用户分配 “管理员 (Administrator)” 角色，并且为 “支持 (Support)” 目录中的用户分配 “服务中心用户 (Help Desk User)” 角色。

如果用户属于具有不同用户角色的多个 LDAP 组， AsyncOS 会为用户授予最受限制角色的权限。例如，如果用户属于具有 “操作人员 (Operator)” 权限的组和具有 “服务中心用户 (Help Desk User)” 权限的组，则 AsyncOS 会为该用户授予 “服务中心用户 (Help Desk User)” 角色的权限。

配置 LDAP 配置文件以查询组成员身份时，输入可以找到组记录的目录级别的基本 DN，保存组成员用户名的属性，以及包含组名的属性。根据为 LDAP 服务器配置文件选择的服务器类型，AsyncOS 会输入用户名和组名属性的默认值，以及默认查询字符串。

备注 对于 Active Directory 服务器，确定用户是否为组成员的默认查询字符串为：(&(objectClass=group)(member={u}))。但是，如果 LDAP 方案在 “memberof” 列表中使用可区别名称而不是用户名，则可以使用 {dn} 而不是 {u}。

表 11-7 显示了 AsyncOS 在 Active Directory 服务器上搜索组成员身份信息时使用的默认查询字符串和属性。

表 11-7　Active Directory 服务器的默认查询字符串和属性

查询字符串	Active Directory
Base DN	[空白]（需要使用特定的基本 DN 来查找组记录。）
可确定用户是否为某个组的成员的查询字符串	`(&(objectClass=group)(member={u}))` **注意** 如果 LDAP 方案在列表的成员中使用可分辨名称而不是用户名，则可以将 `{u}` 替换为 `{dn}`
可确定某个组的所有成员的查询字符串	`(&(objectClass=group)(cn={g}))`
保存每个成员的用户名（或用户记录的 DN）的属性	`成员`
包含组名的属性	`cn`

表 11-8 显示了 AsyncOS 在 OpenLDAP 服务器上搜索组成员身份信息时使用的默认查询字符串和属性。

表 11-8　OpenLDAP 服务器的默认查询字符串和属性

查询字符串	OpenLDAP
Base DN	[空白]（需要使用特定的基本 DN 来查找组记录。）
可确定用户是否为某个组的成员的查询字符串	`(&(objectClass=posixGroup)(memberUid={u}))`
可确定某个组的所有成员的查询字符串	`(&(objectClass=posixGroup)(cn={g}))`
保存每个成员的用户名（或用户记录的 DN）的属性	`memberUid`
包含组名的属性	`cn`

启用管理用户的外部身份验证

在配置 LDAP 服务器配置文件和查询后，可以使用 LDAP 启用外部身份验证。

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)** 页面。

步骤 2　点击**启用 (Enable)**。

步骤 3　选中**启用外部身份验证 (Enable External Authentication)** 复选框。

步骤 4　对于身份验证类型，选择 **LDAP**。

步骤 5　选择对用户进行身份验证的 LDAP 外部身份验证查询。

步骤 6　输入超时前设备等待服务器响应的秒数。

步骤 7　输入希望设备验证的 LDAP 目录中的组名称，然后选择该组中用户的角色。

步骤 8　或者，点击**添加行 (Add Row)** 添加另一个目录组。为设备验证的每个目录组重复执行步骤 7 和 8。

步骤 9　提交并确认更改。

配置 SMTP 路由

SMTP 路由概述

本章介绍影响路由和传送通过思科内容安全管理设备传输的邮件的功能，以及 “SMTP 路由 (SMTP Routes)”页面和 **smtproutes** 命令的使用。

SMTP 路由允许您将特定域的所有邮件重定向到其他邮件交换 (MX) 主机。例如，可以从 `example.com` 映射到 `groupware.example.com`。此映射会导致 “信封收件人 (Envelope Recipient)” 地址中带有 `@example.com` 的所有邮件都更改为 `groupware.example.com`。系统先在 `groupware.example.com` 中执行 “MX” 查询，然后在主机中执行 “A” 查询，就像正常的邮件传送一样。此备用 MX 主机不需要在 DNS MX 记录中列出，甚至无需成为其邮件正在被重定向的域的成员。操作系统最多支持为思科内容安全设备配置一万 (10,000) 个 SMTP 路由映射。（请参阅 SMTP 路由限制 （第 12-3 页）。）

此功能还允许使用主机 “通配”。如果指定了部分域 （例如 `example.com`），则以 `example.com` 结尾的任何域均与该条目匹配。例如， `fred@foo.example.com` 和 `wilma@bar.example.com` 均与该映射匹配。

如果在 SMTP 路由表中没有找到主机，则使用 DNS 执行 MX 查询。不会对照 SMTP 路由表对结果重新进行检查。如果 `foo.domain` 的 DNS MX 条目为 `bar.domain`，则发送到 `foo.domain` 的任何邮件都将传送到主机 `bar.domain`。如果为 `bar.domain` 创建了到其他主机的映射，则地址为 `foo.domain` 的邮件不受影响。

换句话说，递归条目不受影响。如果有一个条目将 `a.domain` 重定向到 `b.domain`，然后又有一个条目将 `b.domain` 的邮件重定向到 `a.domain`，则 *不会*进行邮件循环转发。这种情况下，地址为 `a.domain` 的邮件将传送到 `b.domain` 指定的 MX 主机；相反，地址为 `b.domain` 的邮件将传送到 `a.domain` 指定的 MX 主机。

对于每次邮件传送，都会自上而下读取 SMTP 路由表。选出与映射最匹配的条目例如，如果 SMTP 路由表中的 `host1.example.com` 和 `example.com` 都存在映射，则使用 `host1.example.com` 的条目，因为该条目更具体，即使它出现在不太具体的 `example.com` 条目之后亦无妨。否则，系统将在 “信封收件人 (Envelope Recipient)” 的域中定期执行 MX 查询。

SMTP 路由、邮件传输和邮件拆分

传入：如果一封邮件有 10 个收件人，并且这些收件人都在同一台 Exchange 服务器中，则 AsyncOS 将打开一个 TCP 连接，只向邮件存储区提供一封邮件，而不是 10 封独立邮件。

传出：工作原理类似，但如果一封邮件将发送到 10 个不同域中的 10 个收件人，则 AsyncOS 会打开 10 个通往 10 个 MTA 的连接，并向其中每个 MTA 传送一封邮件。

分拆：如果一封传入邮件有 10 个收件人，它们分别位于不同的传入策略组 （10 个组）中，则即使 10 个收件人都在同一台 Exchange 服务器中，系统也会对邮件进行拆分。因此， 10 封不同的邮件将通过单一 TCP 连接进行传送。

SMTP 路由和出站 SMTP 身份验证

如果已创建出站 SMTP 身份验证配置文件，则可以将其应用于 SMTP 路由。利用此功能，即可在思科内容安全设备部署于网络边缘的邮件中继服务器之后时，对传出邮件进行身份验证。

本地域的邮件路由

安全管理设备会路由以下邮件：

- ISQ 放行的忽略 SMTP 路由的邮件
- 警报
- 可以通过邮件发送到指定目标的配置文件
- 还支持可发送到定义的收件人的请求邮件

  后两种邮件使用 SMTP 路由传送到目标。

邮件安全设备将本地域的邮件路由到使用**管理设备 (Management Appliance) > 网络 (Network) > SMTP 路由 (SMTP Routes)** 页面 （或 **smtproutes** 命令）指定的主机。此功能与 **mailertable** 功能类似。（“SMTP 路由 (SMTP Routes)”页面和 **smtproutes** 命令是 AsyncOS 2.0 域重定向功能的扩展。）

备注　如果已完成 GUI 中的 “系统设置向导 (System Setup Wizard)”并确认了更改，即在设备中为当时输入的每个 RAT 条目定义了第一个 SMTP 路由条目。

默认 SMTP 路由

此外，还可以使用特殊关键字 `ALL` 定义默认 SMTP 路由。如果域与 SMTP 路由列表中先前的映射不匹配，则会默认重定向到 `ALL` 条目指定的 MX 主机。

打印 SMTP 路由条目时，默认 SMTP 路由将作为 `ALL:` 列出。无法删除默认 SMTP 路由，只能清除为其输入的任何值。

请使用**管理设备 (Management Appliance) > 网络 (Network) > SMTP 路由 (SMTP Routes)** 页面或 **smtproutes** 命令配置默认 SMTP 路由。

管理 SMTP 路由

定义 SMTP 路由

邮件安全设备将本地域的邮件路由到使用**管理设备 (Management Appliance) > 网络 (Network) > SMTP 路由 (SMTP Routes)** 页面 （或 **smtproutes** 命令）指定的主机。此功能与 sendmail mailer table 功能类似。（“SMTP 路由 (SMTP Routes)”页面和 **smtproutes** 命令是 AsyncOS 2.0 域重定向功能的扩展。）：

使用“管理设备 (Management Appliance)”>“网络 (Network)”>“SMTP 路由 (SMTP Routes)”页面 （或 **smtproutes** 命令）构建路由。创建新的路由时，首先指定要为其创建永久路由的域或部分域。然后，指定目标主机。目标主机可以采用完全限定的主机名或 IP 地址形式输入。另外，还可以指定 `/dev/null` 的专门目标主机，以删除与该条目匹配的邮件。（因此，实际上，为默认路由指定 `/dev/null` 可确保不会再传送设备收到的邮件。）

多个目标主机条目可以包含完全限定的主机名和 IP 地址。使用逗号分隔多个条目。

如果一个或多个主机没有响应，邮件将传送到可访问的主机之一。如果所有配置的主机均没有响应，邮件将针对该主机排队 （不会故障转移到使用 MX 记录）。

SMTP 路由限制

最多可以定义 10,000 个路由。根据此限制，`ALL` 最后一个默认路由将计入路由数量。因此，最多可定义 9,999 个自定义路由和一个使用特殊关键字 `ALL` 的路由。

添加 SMTP 路由

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 网络 (Network) > SMTP 路由 (SMTP Routes)**。

步骤 2　点击**添加路由 (Add Route)**。

步骤 3　输入接收域和目标主机。通过点击**添加行 (Add Row)** 并在新行中输入下一个目标主机，可添加多个目标主机。

步骤 4　通过向目标主机中添加 “:<*端口号*>”可指定端口号：`example.com:25`

步骤 5　提交并确认更改。

导出 SMTP 路由

与主机访问表 (HAT) 和收件人访问表 (RAT) 类似，也可以通过导出和导入文件来修改 SMTP 路由映射。

操作步骤

步骤 1　点击 “SMTP 路由 (SMTP Routes)”页面中的**导出 SMTP 路由 (Export SMTP Routes)**。

步骤 2　输入文件名称，然后点击**提交 (Submit)**。

导入 SMTP 路由

与主机访问表 (HAT) 和收件人访问表 (RAT) 类似，也可以通过导出和导入文件来修改 SMTP 路由映射。

操作步骤

步骤 1　点击 “SMTP 路由 (SMTP Routes)”页面中的**导入 SMTP 路由 (Import SMTP Routes)**。

步骤 2　选择包含导出的 SMTP 路由的文件。

步骤 3　点击 **Submit**。系统将向您发出警告，告知导入将替代所有现有的 SMTP 路由。文本文件中的所有 SMTP 路由都会导入。

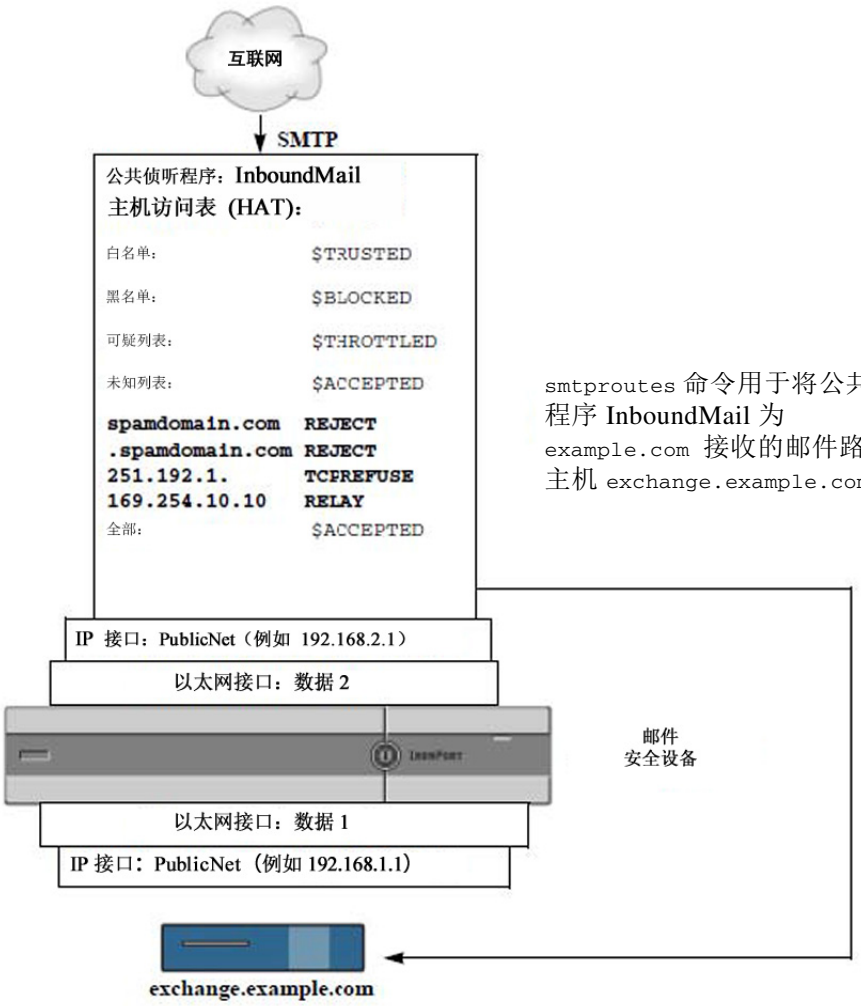
步骤 4　点击 **Import**。

可以在文件中加入 “注释”。以 “#”字符开头的行被视为注释， AsyncOS 会忽略注释。例如：

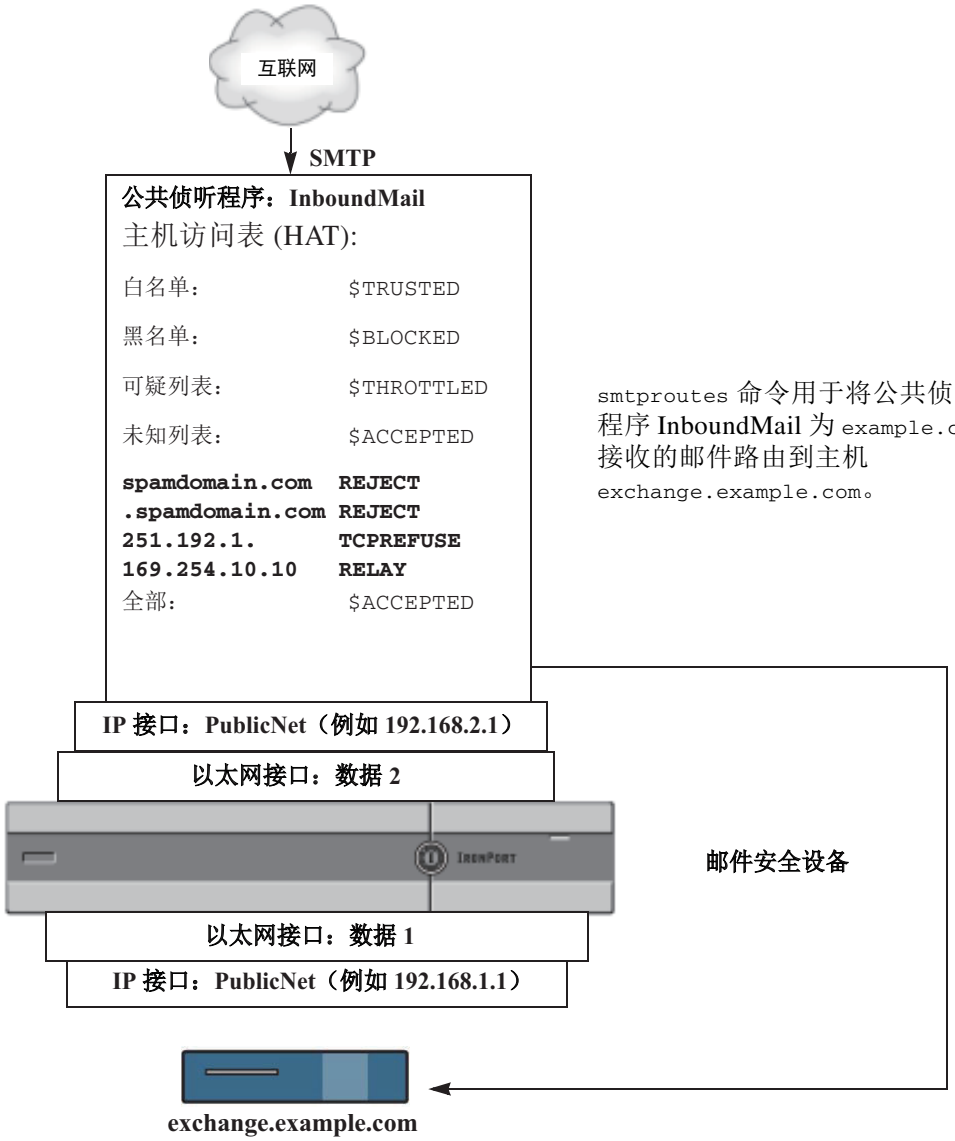
```
# this is a comment, but the next line is not
ALL:
```

此时，我们的 “邮件网关 (Email Gateway)”配置类似于以下：

图 12-1　　为公共侦听程序定义的 SMTP 路由 (SMTP Routes Defined for a Public Listener)



smtproutes 命令用于将公共侦听程序 InboundMail 为 example.com 接收的邮件路由到主机 exchange.example.com。



SMTP 路由和 DNS

使用特殊关键字 USEDNS 可指示设备执行 MX 查找，确定特定域接下来的跳跃。在需要将子域的邮件路由到特定主机时，此功能非常有用。例如，如果发往 example.com 的邮件被发送到公司的 Exchange 服务器，您可能会看到类似以下 SMTP 路由的信息：

```
example.com exchange.example.com
```

但是，对于发往各种子域 (foo.example.com) 的邮件，请添加类似于以下的 SMTP 路由：

```
.example.com USEDNS
```

分配管理任务

关于分配管理任务

您可以在思科内容安全管理设备上根据为其他用户的用户帐户分配的用户角色向这些用户分配管理任务。

要设置设备以分配管理任务，需要确定预定义的用户角色是否满足您的需求，创建所需的任何自定义用户角色，并将设备设置为在安全设备上对管理用户进行本地身份验证和/或使用您自己的集中 LDAP 或 RADIUS 系统对管理用户进行外部身份验证。

此外，还可对设备及设备中特定信息的访问权限指定其他控制。

分配用户角色

预定义用户角色

除非另有说明，否则可以为每个用户分配一个具有下表中所述权限的预定义用户角色或自定义用户角色。

表 13-1　用户角色说明

用户角色名称	说明	网络报告/已安排报告功能
admin	**admin** 用户是系统的默认用户帐户，具有所有管理权限。此处列出 admin 用户帐户是出于方便考虑，但该帐户不能通过用户角色分配，也不能编辑或删除，只能更改密码。 只有 **admin** 用户可以发出 **resetconfig** 和 **revert** 命令。	是/是
管理员	具有 “管理员 (Administrator)”角色的用户帐户具有系统的所有配置设置的完全访问权限。	是/是
Operator	具有 “操作员 (Operator)”角色的用户帐户无法执行以下操作： • 创建或编辑用户帐户 • 升级设备 • 发出 `resetconfig` 命令 • 运行 “系统设置向导 (System Setup Wizard)” • 在启用 LDAP 进行外部身份验证的情况下，修改除用户名和密码之外的 LDAP 服务器配置文件设置 • 配置、编辑、删除或集中隔离区 除上述情况外，他们所拥有的权限与管理员角色相同	是/是
技术人员	具有 “技术人员 (Technician)”角色的用户帐户可以启动系统管理活动 （例如升级和重新启动）、从设备保存配置文件、管理功能密钥等。	访问 “网络 (Web)”和 “邮件 (Email)”选项卡下的系统容量报告
只读操作员	具有 “只读操作员 (Read-Only Operator)”角色的用户帐户有权查看配置信息。具有 “只读操作员 (Read-Only Operator)”角色的用户可以执行和提交大多数更改，以了解如何配置功能，但不能确认更改或进行任何无需确认的更改。如果启用访问权限，则具有此角色的用户可管理隔离区的邮件。 具有此角色的用户不能访问以下信息： • 文件系统、 FTP 或 SCP。 • 创建、编辑、删除或集中隔离区的设置。	是/否
访客	如果启用访问权限，则具有 “访客 (Guest)”角色的用户帐户可以查看状态信息 （包括报告和网络跟踪），并可以管理隔离区的邮件。具有 “访客 (Guest)”角色的用户不能访问邮件跟踪。	是/否
Web管理员	具有 “网络管理员 (Web Administrator)”角色的用户帐户可以访问**网络 (Web)** 选项卡下的所有配置设置。	是/是

表 13-1　用户角色说明（续）

用户角色名称	说明	网络报告/已安排报告功能
Web策略管理员	具有“网络策略管理员 (Web Policy Administrator)”角色的用户帐户可以访问“网络设备状态 (Web Appliance Status)”页面和“主配置 (Configuration Master)”中的所有页面。网络策略管理员可以配置身份、访问策略、解密策略、路由策略、代理旁路、自定义 URL 类别和时间范围。网络策略管理员不能发布配置。	否/否
URL过滤管理员	具有“URL 过滤管理员 (URL Filtering Administrator)”角色的用户帐户仅可以配置用于网络安全的 URL 过滤。	否/否
电子邮件管理员	具有“邮件管理员 (Email Administrator)”角色的用户帐户仅可以访问“邮件 (Email)”菜单下的所有配置设置（包括隔离区）。	否/否
网络管理员用户	具有“服务中心用户 (Help Desk User)”角色的用户帐户只能执行以下操作： • 邮件跟踪 • 管理隔离区中的邮件 具有此角色的用户不能访问系统的其余部分，包括 CLI。向用户分配此角色后，还必须配置隔离区以允许此用户访问。	否/否
自定义角色	分配了自定义用户角色的用户帐户只能查看和配置策略、功能或专门指定给该角色的特定策略或功能实例。 可以从“添加本地用户 (Add Local User)”页面创建新的自定义邮件用户角色或新的自定义网络用户角色。但是，您必须为此自定义用户角色分配权限后，才能使用该角色。要分配权限，请依次转至“管理设备 (Management Appliance)”>“系统管理 (System Administration)”>“用户角色 (User Roles)”，并点击用户名。 **注意**　分配了自定义邮件用户角色的用户无法访问 CLI。 有关详细信息，请参阅自定义用户角色 （第 13-3 页）。	否/否

自定义用户角色

安全管理设备允许拥有管理权限的用户为自定义角色授权管理功能。与预定义用户角色相比，自定义角色可以更灵活地控制用户的访问权限。

分配了自定义用户角色的用户可以管理一系列设备、功能或最终用户的策略或访问报告。例如，您可以允许网络服务的授权管理员管理一个组织位于其他国家/地区（可接受的使用策略可能与公司总部的策略不同）的分支机构的策略。通过创建自定义用户角色并向这些角色分配访问权限，可进行授权管理。您可以确定授权的管理员可以查看和编辑的策略、功能、报告、自定义 URL 类别等。

有关详情，请参阅：

- 关于自定义电子邮件用户角色 （第 13-4 页）
- 关于自定义网络用户角色 （第 13-7 页）
- 删除自定义用户角色 （第 13-9 页）

关于自定义电子邮件用户角色

可以分配自定义角色，以允许授权的管理员在安全管理设备上访问下列信息：

- 所有报告 （可选择通过报告组限制）
- 邮件策略报告 （可选择通过报告组限制）
- DLP 报告 （可选择通过报告组限制）
- 邮件跟踪
- 隔离区

此部分之后将介绍关于上述每个项目的详细信息。此外，所有被授予上述任意权限的用户均可查看位于 “管理设备 (Management Appliance)” 选项卡 > “集中服务 (Centralized Services)” 菜单之下的 “系统状态 (System Status)”。分配了自定义邮件用户角色的用户无法访问 CLI。

备注 与安全管理设备中的用户角色相比，邮件安全设备中的自定义用户角色可提供更精细的访问权限。例如，可以向邮件和 DLP 策略及内容过滤器授予访问权限。有关详细信息，请参阅邮件安全设备文档或在线帮助 “通用管理” 一章中的 “管理授权管理的自定义用户角色” 部分。

对邮件报告的访问权限

可以按以下部分所述授予自定义用户角色访问邮件报告的权限。

有关安全管理设备中 “邮件安全监控 (Email Security Monitor)” 页面的完整信息，请参阅使用集中邮件安全报告一章。

所有报告

如果授予自定义角色访问所有报告的权限，则分配了此角色的用户可以查看所有邮件安全设备或所选的 “报告组 (Reporting Group)” 的 “邮件安全监控 (Email Security Monitor)” 页面：

- 概述
- 传入邮件
- 外发目标
- 外发邮件发件人
- 内部用户
- DLP 事件
- 内容过滤器
- 病毒类型
- TLS 连接
- 病毒爆发过滤器
- 系统容量
- 正在报告数据可用性
- 计划的报告
- 存档的报告

邮件策略报告

如果授予自定义角色访问邮件策略报告的权限，则分配了此角色的用户可以查看所有邮件安全设备或所选的 “报告组 (Reporting Group)” 的 “邮件安全监控 (Email Security Monitor)” 页面：

- 概述
- 传入邮件
- 外发目标
- 外发邮件发件人
- 内部用户
- 内容过滤器
- 病毒类型
- 病毒爆发过滤器
- 正在报告数据可用性
- 存档的报告

DLP 报告

如果授予自定义角色访问 DLP 报告的权限，则分配了此角色的用户可以查看所有邮件安全设备或所选的 “报告组 (Reporting Group)” 的 “邮件安全监控 (Email Security Monitor)” 页面：

- DLP 事件
- 正在报告数据可用性
- 存档的报告

对邮件跟踪数据的访问权限

如果授予自定义角色访问邮件跟踪的权限，则分配了此角色的用户可以找到安全管理设备跟踪的所有邮件的状态。

要控制对违反 DLP 策略的邮件中敏感信息的访问，请参阅控制邮件跟踪中敏感 DLP 信息的访问权限 （第 13-22 页）。

有关邮件跟踪的详细信息 （包括设置设备以便在安全管理设备中启用邮件跟踪访问权限的说明），请参阅 “跟踪邮件消息”。

自定义用户角色对隔离区的访问权限

如果授予自定义角色访问隔离区的权限，则分配了此角色的用户可以搜索、查看、发布或删除此安全管理设备中所有隔离区的邮件。

您必须启用此访问权限，用户才能访问隔离区。请参阅对隔离区的访问权限 （第 13-9 页）。

创建自定义邮件用户角色

要访问邮件报告、邮件跟踪和隔离区，可以创建自定义邮件用户角色。

有关其中各个选项许可的访问权限的说明，请参阅关于自定义电子邮件用户角色及其子部分。

备注　要授予对其他功能、报告或策略的更为精细的访问，请在每个邮件安全设备定义用户角色。

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户角色 (User Roles)**。

步骤 2　点击**添加邮件用户角色 (Add Email User Role)**。

提示　或者，可以通过复制现有的邮件用户角色来创建新角色：点击适用的表格行中的 “复制 (Duplicate)” 图标，然后修改生成的副本。

步骤 3　为该用户角色输入唯一的名称 （例如 “dlp-auditor”）和说明。

- 不能复制邮件和网络自定义用户角色名称。
- 名称必须仅包含小写字母、数字和短划线。不能以短划线或数字开头。
- 如果授予具有此角色的用户访问集中策略隔离区的权限，并且还希望具有此角色的用户能够在邮件安全设备上的邮件及内容过滤器中指定这些集中隔离区以及 DLP 邮件操作，则两种设备上的自定义角色的名称必须相同。

步骤 4　选择要为此角色启用的访问权限。

步骤 5　点击**提交 (Submit)** 可返回到 “用户角色 (User Roles)” 页面，其中列出了新的用户角色。

步骤 6　如果按 “报告组 (Reporting Group)” 限制了访问权限，请点击该用户角色 “邮件报告 (Email Reporting)” 列中的**无选定的组 (no groups selected)** 链接，然后至少选择一个报告组。

步骤 7　确认更改。

步骤 8　如果授予了此角色访问隔离区的权限，请为此角色启用访问权限：

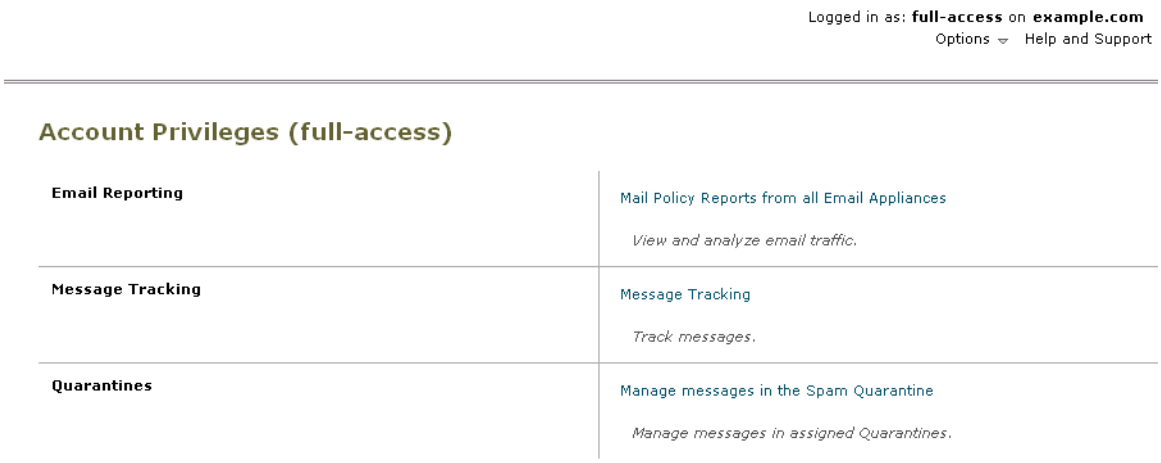
请参阅：

- 配置对垃圾邮件隔离区的管理用户访问权限 （第 7-6 页）
- 创建策略隔离区 （第 8-10 页）

使用自定义邮件用户角色

当分配了自定义邮件用户角色的用户登录到设备时，该用户只能看到其有权访问的安全功能的链接。用户可随时通过选择 “选项 (Options)” 菜单中的 “帐户权限 (Account Privileges)” 返回此主页。这些用户还可以通过网页顶部的菜单访问其有权访问的功能。在以下示例中，用户可通过自定义邮件用户角色访问安全管理设备中可用的所有功能。

图 13-1　　分配了自定义邮件用户角色的授权管理员的 “帐户权限 (Account Privileges)” 页面



关于自定义网络用户角色

自定义网络用户角色允许用户向不同的网络安全设备发布策略，并赋予他们针对不同设备编辑或发布自定义配置的权限。

在安全管理设备中的**网络 (Web) > 主配置 (Configuration Master) > 自定义 URL 类别 (Custom URL Categories)** 页面，可以查看允许您管理和发布的 URL 类别与策略。此外，还可以转至**网络 (Web) > 实用程序 (Utilities) > 立即发布配置 (Publish Configuration Now)** 页面，查看可能的配置。

备注　请注意，在创建具有 “发布权限 (Publish Privilege)” 功能的自定义角色后，当用户登录时，会发现没有任何可用的菜单。用户不会有发布菜单，而且登录屏幕不可编辑，因为 URL 和策略选项卡没有任何功能。实际上，所创建的用户无法发布或管理任何类别或策略。

针对此问题的解决方法是：如果希望用户可以发布，但不能管理任何类别或策略，则**必须**创建一个在任何策略中都未使用的自定义类别，并授予该用户管理此自定义类别及发布的权限。这样，如果用户从该类别添加或删除 URL，则不会造成任何影响。

通过创建和编辑自定义用户角色，可以对网络管理进行授权。

- 创建自定义网络用户角色
- 编辑自定义网络用户角色
- 删除自定义用户角色 （第 13-9 页）

创建自定义网络用户角色

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户角色 (User Roles)**。

步骤 2　点击**添加网络用户角色 (Add Web User Role)**。

提示　或者，可以通过复制现有的网络用户角色来创建新角色：点击适用的表格行中的 “复制 (Duplicate)”图标，然后修改生成的副本。

步骤 3　为该用户角色输入唯一的名称 （例如 “canadian-admins”）和说明。

注　名称必须仅包含小写字母、数字和短划线。不能以短划线开头。

步骤 4　选择默认情况下希望这些策略和自定义 URL 类别显示还是隐藏。

步骤 5　选择希望 “发布 (Publish)”权限打开还是关闭。

此权限允许用户发布其可以编辑 “访问策略 (Access Policies)”或 “URL 类别 (URL Categories)”的任何主配置。

步骤 6　选择开始使用新 （空）设置还是复制现有的自定义用户角色。如果选择复制现有的用户角色，请从列表中选择要复制的角色。

步骤 7　点击**提交 (Submit)** 可返回到 “用户角色 (User Roles)”页面，其中列出了新的用户角色。

注　如果在网络报告中启用了匿名功能，则有权访问网络报告的所有用户角色在交互式报告页面中将使用不可识别的用户名和角色。请参阅第 5 章 “使用集中 Web 报告和跟踪”中的安排 Web 报告部分 但 “管理员”角色例外，该角色可以在计划的报告中查看实际用户名。如果启用了匿名功能，“操作员”和 “网络管理员”生成的计划报告将采用匿名。

注　如果使用**网络 (Web) > 实用程序 (Utilities) > 安全服务显示 (Security Services Display) > 编辑安全服务显示 (Edit Security Services Display)** 页面隐藏其中一个主配置，则 “用户角色 (User Roles)”页面还会隐藏相应的 “主配置 (Configuration Master)”列，但保留所隐藏主配置的权限设置。

编辑自定义网络用户角色

操作步骤

步骤 1　在“用户角色 (User Roles)”页面中，点击角色名称以显示“编辑用户角色 (Edit User Role)”页面。

步骤 2　编辑任何设置：策略和自定义 URL 类别的名称、说明和可视性。

步骤 3　点击 **Submit**。

要编辑自定义用户角色的权限，请执行以下操作：

导航至“用户角色 (User Roles)”页面。

- 要编辑访问策略权限，请点击“访问策略 (Access policies)”以显示在“主配置 (Configuration Master)”中配置的访问策略列表。在“包括 (Include)”列中，选择要授予用户编辑权限的策略所对应的复选框。点击**提交 (Submit)** 返回到“用户角色 (User Roles)”页面。

-或者-

- 要编辑自定义 URL 类别权限，请点击“自定义 URL 类别 (Custom URL Categories)”以显示在“主配置 (Configuration Master)”中定义的自定义 URL 类别列表。在“包括 (Include)”列中，选择要授予用户编辑权限的自定义 URL 类别的复选框。点击**提交 (Submit)** 返回到“用户角色 (User Roles)”页面。

删除自定义用户角色

如果删除已分配给一个或多个用户的自定义用户角色，系统不会报错。

可访问 CLI 的用户角色

有些角色可以访问 GUI 和 CLI：管理员、操作员、访客、技术人员和只读操作员。其他角色只能访问 GUI：服务中心用户、邮件管理员、网络管理员、网络策略管理员、 URL 过滤管理员 （网络安全）和自定义用户。

使用 LDAP

如果使用 LDAP 目录验证用户，可以将目录组分配给用户角色 （而不是单个用户）。将目录组分配给用户角色后，该组中的每个用户都会获得为该用户角色定义的权限。有关详细信息，请参阅外部用户身份验证 （第 13-16 页）。

对隔离区的访问权限

您必须启用此访问权限，用户才能访问隔离区。请参阅以下信息：

- 配置对垃圾邮件隔离区的管理用户访问权限 （第 7-6 页）
- 创建策略隔离区 （第 8-10 页） （适用于策略隔离区）
- 为自定义用户角色配置集中隔离区访问权限 （第 8-7 页）

“用户 (User)”页面

有关此部分的信息	请参阅
用户 “重置密码 (Reset Passwords)”按钮	关于分配管理任务 管理本地定义的管理用户 要求用户按需更改密码
本地用户帐户和密码设置	设置密码和登录要求
外部身份验证	外部用户身份验证
DLP 跟踪权限	控制邮件跟踪中敏感 DLP 信息的访问权限

关于管理用户身份验证

通过在设备上本地定义授权用户和/或使用外部身份验证，可控制对设备的访问权限。

- 更改 Admin 用户的密码 （第 13-10 页）
- 管理本地定义的管理用户 （第 13-10 页）
- 外部用户身份验证 （第 13-16 页）

更改 Admin 用户的密码

所有管理员级别的用户均可通过 GUI 或 CLI 更改 “admin”用户的密码。

要通过 GUI 更改密码，请依次选择 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “用户 (Users)”页面，然后选择 admin 用户。

要在 CLI 中更改 `admin` 用户的密码，请使用 `password` 命令。为了安全起见，`password` 命令会要求您输入旧密码。

如果忘记了 “admin”用户帐户的密码，请联系客户支持提供商重置密码。

备注　对密码的更改会立即生效，无需提交更改。

管理本地定义的管理用户

- 添加本地定义的用户 （第 13-11 页）
- 编辑本地定义的用户 （第 13-11 页）
- 删除本地定义的用户 （第 13-12 页）
- 查看本地定义的用户列表 （第 13-12 页）
- 设置和更改密码 （第 13-12 页）
- 设置密码和登录要求 （第 13-12 页）

- 要求用户按需更改密码 （第 13-15 页）
- 锁定和解锁本地用户帐户 （第 13-15 页）

添加本地定义的用户

如果不使用外部身份验证，请按照以下程序直接将用户添加到安全管理设备。或者，在 CLI 中使用 **userconfig** 命令。

备注　如果也启用了外部身份验证，请确保本地用户名没有与通过外部身份验证的用户名重复。

在设备上可创建的用户帐户数没有限制。

操作步骤

步骤 1　如果要分配自定义用户角色，建议您首先定义这些角色。请参阅自定义用户角色 （第 13-3 页）。

步骤 2　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。

步骤 3　点击**添加用户 (Add User)**。

步骤 4　为用户输入唯一名称。不能输入系统保留的文字 （例如 “operator”和 “root”）。

如果也使用外部身份验证，则用户名不应与通过外部身份验证的用户名重复。

步骤 5　为用户输入完整名称。

步骤 6　选择预定义的角色或自定义角色。有关用户角色的详细信息，请参阅表 13-1。

如果在此添加新的 “邮件 (Email)”角色或 “网络 (Web)”角色，请为该角色输入名称。有关命名限制，请参阅创建自定义邮件用户角色 （第 13-5 页）或创建自定义网络用户角色 （第 13-8 页）。

步骤 7　输入密码，然后再次输入。

步骤 8　提交并确认更改。

步骤 9　如果在此页添加了自定义用户角色，现在请为该角色分配权限。请参阅自定义用户角色 （第 13-3 页）。

编辑本地定义的用户

例如，按照以下程序更改密码。

操作步骤

步骤 1　在 “用户 (Users)”列表中点击用户名。

步骤 2　更改该用户。

步骤 3　提交并确认更改。

删除本地定义的用户

操作步骤

步骤 1　在 “用户 (Users)”列表中点击用户名所对应的垃圾桶图标。

步骤 2　在出现的警告对话框中点击**删除 (Delete)**，确认删除。

步骤 3　点击**确认 (Commit)** 确认更改。

查看本地定义的用户列表

要查看本地定义的用户列表，请依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。

备注　星号表示分配了自定义用户角色且要进行授权管理的用户。如果用户的自定义角色已删除，将以红色显示 “未分配 (Unassigned)”。有关自定义用户角色的详细信息，请参阅自定义用户角色（第 13-3 页）。

设置和更改密码

- 添加用户时，需要为该用户指定初始密码。
- 要更改系统中配置的用户的密码，请使用 GUI 中的 “编辑用户 (Edit User)”页面 （有关详细信息，请参阅编辑本地定义的用户 （第 13-11 页））。
- 要更改系统默认 admin 用户帐户的密码，请参阅更改 Admin 用户的密码 （第 13-10 页）。
- 要强制用户更改其密码，请参阅要求用户按需更改密码 （第 13-15 页）。
- 用户可以通过点击 GUI 右上方的 “选项 (Options)”菜单，并选择 “更改密码 (Change Password)”选项，更改自己的密码。

设置密码和登录要求

通过定义用户帐户和密码限制来实施组织密码策略。用户帐户和密码限制适用于安全管理设备上定义的本地用户。可以配置以下设置：

- **用户帐户锁定 (User account locking)。**可以定义导致用户帐户锁定的登录尝试失败次数。
- **密码有效期规则 (Password lifetime rules)。**可以定义密码的有效期限，在该期限之后，用户登录后需要更改密码。
- **密码规则 (Password rules)。**可以定义用户可选择的密码类型，例如哪些字符是可选的或必需的。

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。

步骤 2　向下滚动到**本地用户帐户和密码设置 (Local User Account and Password Settings)** 部分。

步骤 3　点击**编辑设置 (Edit Settings)**。

步骤 4　配置设置：

设置	说明
用户帐户锁定	选择用户登录失败后是否锁定用户帐户。指定导致帐户锁定的尝试登录失败次数。可以输入从一 (1) 到 60 的任意数字。默认值为五 (5)。 配置帐户锁定时，请输入对尝试登录的用户显示的消息。使用 7 位 ASCII 字符组成的文本。只有用户为锁定的帐户输入正确的密码时，才会显示此消息。 用户帐户被锁定后，管理员可以在 GUI 中的 “编辑用户 (Edit User)” 页面中或使用 `userconfig` 命令解锁帐户。 尝试登录失败次数由用户跟踪，不考虑用户连接的计算机或连接类型（例如 SSH 或 HTTP）。在用户成功登录后，尝试登录失败次数将重置为零 (0)。 当用户帐户因达到登录尝试失败最大次数而被锁定时，系统会向管理员发送警报。警报的严重级别设置为 “参考 (Info)”。 **注意**　还可以手动锁定各个用户帐户。请参阅手动锁定用户帐户 （第 13-15 页）。
密码重置	选择管理员在更改用户密码后，是否应强制用户更改其密码。 另外，还可以选择在用户的密码到期后，是否应强制用户更改其密码。输入过多少天后用户必须更改密码。可以输入从一 (1) 到 366 的任意数字。默认值为 90。要强制用户不定期更改密码，请参阅要求用户按需更改密码 （第 13-15 页）。 如果强制用户在密码到期后更改其密码，可以显示关于密码即将到期的通知。选择在到期之前多少天通知用户。 **注意**　当用户帐户使用 SSH 密钥 （而不是密码质询）时，密码重置规则仍然适用。当使用 SSH 密钥的用户帐户到期时，用户必须输入其旧密码或请管理员手动更改密码，才能更改与该帐户相关的密钥。
密码规则： 至少需要 <数字> 个字符。	输入密码可包含的最少字符数。 输入零 (0) 和 128 之间的任何数字。 默认值为 8。 密码包含的字符数可以多于此处指定的数目。
密码规则： 至少需要一个数字 (0-9)。	选择密码是否必须至少包含一个数字。

密码规则：
至少需要一个特殊字符。
	选择密码是否必须至少包含一个特殊字符。密码可以包含以下特殊字符：
	`~ ?!@ # $ % ^ & * - _ + =`
	`\ | / [ ] ( ) < > { } ` ' " ; : , .`

设置	说明
密码规则： 禁止将用户名及其变体形式作为密码。	选择是否允许密码与相关用户名或用户名的变体形式相同。禁止使用用户名的变体形式时，以下规则适用于密码： • 密码不能与用户名相同，不区分大小写。 • 密码不能是用户名逆序形式，不区分大小写。 • 密码不能是替换以下字符后的用户名或逆序用户名： – “@”或“4”替换“a” – “3”替换“e” – “l”、“!”或“1”替换“i” – “0”替换“o” – “$”或“5”替换“s” – “+”或“7”替换“t”
密码规则： 禁止再次使用最近 <数字> 次用过的密码。	选择强制用户更改密码时，是否允许用户选择最近使用的密码。如果不允许再次使用最近的密码，请输入禁止再次使用的最近密码次数。 可以输入从一 (1) 到 15 的任意数字。默认值为三 (3)。
密码规则： 密码中不允许使用的单词列表	可以创建密码中禁止使用的单词列表。 将此文件创建为文本文件，每个禁用单词单独为一行。使用名称 `forbidden_password_words.txt` 保存该文件，并使用 SCP 或 FTP 将该文件上传到设备。 如果选择了此限制，但未上传单词表，将忽略此限制。
密码强度	当管理员或用户输入新密码时，可以显示密码强度指示器。 此设置不强制创建强密码，只显示猜测所输入的密码的难易程度。 选择要为其显示指示器的角色。然后，对于每个所选的角色，输入一个大于 0 的数字。数字越大，意味着注册为强密码的密码越难破解。此设置没有最大值。 示例： • 如果输入 `30`，则注册为强密码的 8 位字符的密码至少包含 1 个大写和小写字母、数字和特殊字符。 • 如果输入 `18`，则注册为强密码的 8 位字符密码全部为小写字母，不含数字或特殊字符。 密码强度是按对数衡量的。根据美国国家标准与技术研究院在 NIST SP 800-63 中定义的熵值规则 （附录 A）进行评估。 通常，高强度密码具有以下特征： • 长度较长 • 包括大写、小写、数字和特殊字符 • 不含任何语言的任何词典中的单词 要实施具有上述这些特征的密码，请使用此页面中的其他设置。

步骤 5　提交并确认更改。

后续操作

要求用户将密码更改为符合新要求的新密码。请参阅要求用户按需更改密码 （第 13-15 页）

要求用户按需更改密码

如果需要所有或选定的用户在任何时间临时更改其密码，请执行此操作程序中的步骤。这是一次性操作。

要想自动完成定期要求更改密码的操作，请使用设置密码和登录要求 （第 13-12 页）中介绍的“密码重置 (Password Reset)”选项。

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。

步骤 2　在 “用户 (Users)”部分，选中需要更改密码的用户旁边的复选框。

步骤 3　选择**强制密码更改 (Enforce Password Changes)**。

步骤 4　选择选项。

在“本地用户帐户和密码设置 (Local User Account & Password Settings)”中配置宽限期的全局设置。

步骤 5　点击**确定 (OK)**。

锁定和解锁本地用户帐户

锁定用户帐户可防止本地用户登录设备。通过以下方式之一可锁定用户帐户：

- 可以将所有本地用户帐户配置为用户尝试登录所配置的次数但仍不成功后锁定。请参阅设置密码和登录要求 （第 13-12 页）。
- 管理员可以手动锁定用户帐户。请参阅手动锁定用户帐户 （第 13-15 页）。

在 “编辑用户 (Edit User)”页面查看用户帐户时， AsyncOS 将显示用户帐户被锁定的原因。

手动锁定用户帐户

操作步骤

步骤 1　仅第一次：设置设备以启用用户帐户锁定：

a. 依次转到**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。

b. 在**本地用户帐户和密码设置 (Local User Account & Password Settings)** 部分，点击**编辑设置 (Edit Settings)**。

c. 选中复选框**如果管理员手动锁定了用户帐户，则显示锁定的帐户消息 (Display Locked Account Message if Administrator has manually locked a user account)**，并输入您的消息。

d. 提交更改。

步骤 2　依次转到**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**，点击用户名。

注　锁定 Admin 帐户之前，请确保您可以将其解锁。请参阅解锁用户帐户 （第 13-16 页）中的说明。

步骤 3　点击**锁定帐户 (Lock Account)**。

AsyncOS 将显示一条消息，表示用户无法登录到设备，并询问是否要继续。

解锁用户帐户

要解锁用户帐户，请点击 “用户 (Users)” 列表中的用户名打开该用户帐户，然后点击 “解锁帐户 (Unlock Account)”。

备注　如果锁定 admin 帐户，则只能在以管理员身份登录后通过串行通信连接到串行控制台端口将其解锁。即使在 admin 帐户被锁定时， admin 用户也可以使用串行控制台端口访问设备。有关使用串行控制台端口访问设备的详细信息，请参阅邮件安全设备文档或在线帮助中的 “设置和安装” 章节。

外部用户身份验证

如果在网络中将用户信息存储在 LDAP 或 RADIUS 目录，则可以将安全管理设备配置为使用外部目录对登录到设备的用户进行身份验证。

备注
- 自定义视图 （第 14-48 页）中介绍的某些功能不适用于通过外部身份验证的用户。
- 如果部署中同时使用本地和外部身份验证，则本地用户名不能与通过外部身份验证的用户名相同。
- 如果设备无法与外部目录通信，则具有外部和本地帐户的用户可以使用设备上的本地用户帐户登录。

请参阅：
- 使用 LDAP 配置管理用户的外部身份验证 （第 11-13 页）
- 启用 RADIUS 身份验证 （第 13-17 页）

配置 LDAP 身份验证

要配置 LDAP 身份验证，请参阅使用 LDAP 配置管理用户的外部身份验证 （第 11-13 页）。

启用 RADIUS 身份验证

可以使用 RADIUS 目录对用户进行身份验证，并为用户角色分配用户组来管理设备。RADIUS 服务器应支持“类 (CLASS)”属性，AsyncOS 通过该属性为 RADIUS 目录中的用户分配用户角色。

备注　如果外部用户更改了其 RADIUS 组的用户角色，则该用户应注销设备，然后重新登录。该用户将获得新角色的权限。

准备工作

访问 RADIUS 服务器的共享密钥长度不能超过 48 个字符。

操作步骤

步骤 1　在“管理设备 (Management Appliance)”>“系统管理 (System Administration)”>“用户 (Users)”页面上，点击**启用 (Enable)**。

步骤 2　选中**启用外部身份验证 (Enable External Authentication)** 复选框。

步骤 3　选择 RADIUS 作为身份验证类型。

步骤 4　输入 RADIUS 服务器的主机名。

步骤 5　输入 RADIUS 服务器的端口号。默认端口号为 1812。

步骤 6　输入 RADIUS 服务器的共享密钥。

注　为邮件安全设备的集群启用外部身份验证时，请在集群中的所有设备上输入相同的共享密钥。

步骤 7　输入超时前设备等待服务器响应的秒数。

步骤 8　选择是否使用密码验证协议 (PAP) 或挑战握手验证协议 (CHAP) 作为身份验证协议。

步骤 9　（可选）点击**添加行 (Add Row)** 添加另一台 RADIUS 服务器。对于设备用于身份验证的每台 RADIUS 服务器，重复步骤 6 和 7。

如果定义了多台外部服务器，设备将按设备中定义的顺序连接到服务器。您可能需要定义多台外部服务器，以便在一台服务器临时不可用的情况下实现故障转移。

步骤 10　在网络用户界面中输入存储外部身份验证凭证的时间长度。

注　如果 RADIUS 服务器使用一次性密码 （例如基于令牌创建的密码），请输入零 (0)。如果该值设置为零，在当前会话期间，AsyncOS 不会再次联系 RADIUS 服务器进行身份验证。

步骤 11　配置群组映射：

设置	说明
将通过外部身份验证的用户映射到多个本地角色 （推荐）	AsyncOS 将基于 RADIUS “类 (CLASS)”属性向设备角色分配 RADIUS 用户。“类 (CLASS)”属性要求： • 最少 3 个字符 • 最多 253 个字符 • 不含冒号、逗号或换行符 • 每个 RADIUS 用户有一个或多个映射的 “类 (CLASS)”属性 （有了此设置， AsyncOS 可拒绝访问没有映射 “类 (CLASS)”属性的 RADIUS 用户。） 对于具有多个 “类 (CLASS)”属性的 RADIUS 用户， AsyncOS 将分配限制性最高的角色。例如，如果 RADIUS 用户有两个 “类 (CLASS)”属性，分别映射到 “操作员”和 “只读操作员”角色，则 AsyncOS 会将 RADIUS 用户分配到 “只读操作员”角色，因为该角色比 “操作员”角色限制性高。 下面是设备角色限制性由低到高的顺序： • 管理员 • 电子邮件管理员 • Web管理员 • Web策略管理员 • URL 过滤管理员 （用于网络安全） • 自定义用户角色 （邮件或 Web） 如果为用户分配了多个映射到自定义用户角色的 “类 (Class)”属性，将使用 RADIUS 服务器上列表中的最后一个 “类 (Class)”属性 • 技术人员 • Operator • 只读操作员 • 网络管理员用户 • 访客
将所有通过外部身份验证的用户映射到 “管理员”角色	AsyncOS 将 RADIUS 用户分配到 “管理员”角色。

步骤 12　（可选）点击**添加行 (Add Row)** 添加另一个组。对于设备进行身份验证的每个用户组，重复步骤 11。

步骤 13　提交并确认更改。

关于访问安全管理设备的其他控制

配置基于 IP 的网络访问

通过为直接连接到设备的用户和通过反向代理连接的用户 （如果组织对于远程用户使用反向代理）创建访问列表，可以控制用户从哪些 IP 地址访问安全管理设备。

直接连接

可以为可连接到安全管理设备的计算机指定 IP 地址、子网或 CIDR 地址。用户可以从使用访问列表中 IP 地址的任何计算机访问设备。如果用户尝试从列表中未包括的地址连接设备，将被拒绝访问。

通过代理连接

如果组织的网络在远程用户的计算机与安全管理设备之间使用反向代理服务器， AsyncOS 允许您使用可以连接到设备的代理的 IP 地址创建访问列表。

即使使用反向代理， AsyncOS 仍会对照允许用户连接的 IP 地址列表验证远程用户计算机的 IP 地址。要将远程用户的 IP 地址发送到邮件安全设备，代理需要在其连接设备的请求中包括 `x-forwarded-for` HTTP 信头。

`x-forwarded-for` 信头是非 RFC 标准的 HTTP 信头，格式如下：

```
x-forwarded-for: client-ip, proxy1, proxy2,...CRLF.
```

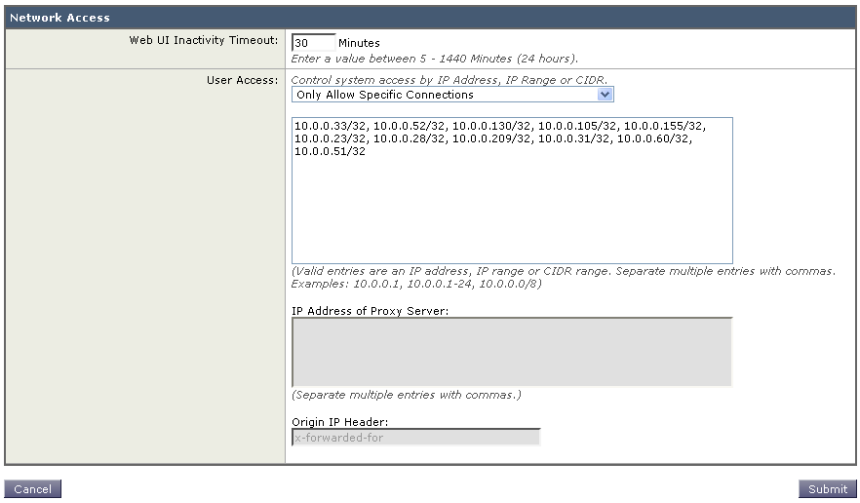
此信头的值是逗号分隔值形式的 IP 地址列表，其中最左侧的地址是远程用户计算机的地址，之后是转发连接请求的各个后续代理的地址。（信头名称是可配置的。）安全管理设备对照访问列表中允许的用户和代理 IP 地址，匹配信头中的远程用户 IP 地址和连接代理的 IP 地址。

备注　AsyncOS 仅支持 `x-forwarded-for` 信头中的 IPv4 地址。

创建访问列表

通过 GUI 中的 “网络访问 (Network Access)” 页面或使用 **adminaccessconfig > ipaccess** CLI 命令，可创建网络访问列表。图 13-2 显示了 “网络访问 (Network Access)” 页面，其中包含允许直接连接到安全管理设备的用户 IP 地址列表。

图 13-2　　网络访问设置示例



AsyncOS 针对访问列表提供四种不同的控制模式：

- **全部允许 (Allow All)。**此模式允许与设备的所有连接。此模式为默认操作模式。
- **仅允许特定连接 (Only Allow Specific Connections)。**如果用户的 IP 地址与访问列表中所含的 IP 地址、 IP 范围或 CIDR 范围匹配，此模式则允许该用户连接到设备。
- **仅允许通过代理的特定连接 (Only Allow Specific Connections Through Proxy)。**如果满足以下条件，此模式允许用户通过反向代理连接到设备：
  - 访问列表 “代理服务器 (Proxy Server)” 字段的 IP 地址中包含连接代理的 IP 地址。
  - 代理的连接请求中包含 `x-forwarded-header` HTTP 信头。
  - `x-forwarded-header` 的值为空。
  - 远程用户的 IP 地址包含在 `x-forwarded-header` 中，并且与访问列表为用户定义的 IP 地址、 IP 范围或 CIDR 范围匹配。
- **仅允许直接或通过代理的特定连接 (Only Allow Specific Connections Directly or Through Proxy)。**如果用户的 IP 地址与访问列表中包含的 IP 地址、IP 范围或 CIDR 范围匹配，此模式则允许用户通过反向代理或直接连接到设备。通过代理连接的条件与 “仅允许通过代理的特定连接 (Only Allow Specific Connections Through Proxy)” 模式相同。

请注意，如果满足下列条件之一，在提交和确认更改后，可能会丧失对设备的访问权限：

- 如果选择**仅允许特定连接 (Only Allow Specific Connections)**，且列表中不含当前计算机的 IP 地址。
- 如果选择**仅允许通过代理的特定连接 (Only Allow Specific Connections Through Proxy)**，当前连接到设备的代理的 IP 地址不在代理列表中，并且源 IP 信头的值不在允许的 IP 地址列表中。

- 如果选择**仅允许直接或通过代理的特定连接 (Only Allow Specific Connections Directly or Through Proxy)**，且
  - 源 IP 信头的值不在允许的 IP 地址列表中

    或者
  - 源 IP 信头的值不在允许的 IP 地址列表中，且连接到设备的代理的 IP 地址不在允许的代理列表中

如果选择继续而不更正访问列表，在确认更改后， AsyncOS 将断开设备或代理与设备的连接。

操作步骤

步骤 1　依次选择**系统管理 (System Administration) > 网络访问 (Network Access)**。

步骤 2　点击**编辑设置 (Edit Settings)**。

步骤 3　选择访问列表的控制模式。

步骤 4　输入允许用户连接的目标设备的 IP 地址。

可以输入 IP 地址、 IP 地址范围或 CIDR 范围。使用逗号分隔多个条目。

步骤 5　如果允许通过代理连接，请输入以下信息：

- 允许连接到设备的代理的 IP 地址。使用逗号分隔多个条目。
- 代理发送到设备的源 IP 信头的名称，其中包含远程用户计算机和转发请求的代理服务器的 IP 地址。默认情况下，该信头的名称为 `x-forwarded-for`。

步骤 6　提交并确认更改。

配置 Web UI 会话超时

可以指定用户因不活动而被 AsyncOS 注销前可登录安全管理设备 Web UI 的时间。此 Web UI 会话超时适用于所有用户 （包括 admin），而且将用于 HTTP 和 HTTPS 会话。

AsyncOS 注销用户后，设备会将用户的 Web 浏览器重定向到登录页。

备注　“Web UI 会话超时 (Web UI Session Timeout)”不适用于垃圾邮件隔离区会话，该会话的超时设置为 30 分钟，且无法配置。

操作步骤

步骤 1　使用**系统管理 (System Administration) > 网络访问 (Network Access)** 页面。

步骤 2　点击**编辑设置 (Edit Settings)**。

步骤 3　输入用户在注销之前可以保持不活动的分钟数。可以定义 5 到 1440 分钟之间的超时期限。

步骤 4　提交并确认更改。

控制邮件跟踪中敏感 DLP 信息的访问权限

违反防数据丢失 (DLP) 策略的邮件通常包含敏感信息，例如公司机密信息或个人信息（包括信用卡号码或健康记录）。默认情况下，这些内容显示在“邮件跟踪 (Message Tracking)”结果中列出的邮件的“邮件详细信息 (Message Details)”页面“DLP 匹配内容 (DLP Matched Content)”选项卡中。

可以根据安全管理设备用户被分配的预定义或自定义角色，选择对其隐藏此选项卡及其内容：

操作步骤

步骤 1　依次转到**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)** 页面。

步骤 2　在 **DLP 跟踪权限 (DLP Tracking Privileges)** 部分，点击**编辑设置 (Edit Settings)**。

步骤 3　选择要为其授予邮件跟踪中 DLP 数据访问权限的角色。

只会列出具有邮件跟踪访问权限的自定义角色。

步骤 4　提交并确认更改。

只有在“管理设备 (Management Appliance)”>“集中服务 (Centralized Services)”下启用“集中邮件跟踪”功能，此设置才能生效。

向管理用户显示消息

可以显示管理用户登录到设备时将看到的消息。

要设置或清除消息，请执行以下操作：

步骤 1　如果要导入文本文件，请将其放置在设备上的 `/data/pub/configuration` 目录中。

步骤 2　访问命令行界面 (CLI)。

步骤 3　使用 `adminaccessconfig` > `BANNER` 命令和子命令。

步骤 4　确认更改。

查看管理用户活动

- 使用网络查看活动会话 （第 13-23 页）
- 查看最近的登录尝试 （第 13-23 页）
- 通过命令行界面查看管理用户活动 （第 13-23 页）

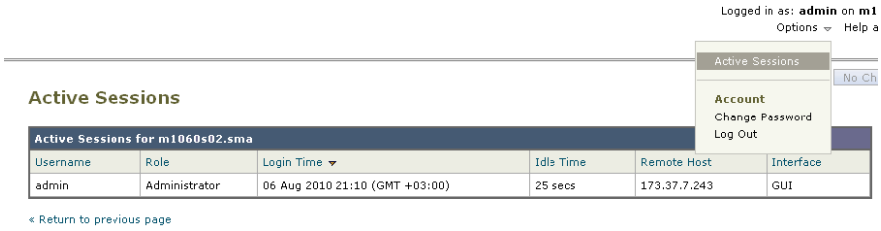
使用网络查看活动会话

在安全管理设备中，可以查看所有活动的会话和登录到设备的用户。

操作步骤

步骤 1　在窗口的右上角，依次选择**选项 (Options) > 活动会话 (Active Sessions)**。

图 13-3　“活动会话” (Active Sessions) 菜单



在 “活动会话 (Active Sessions)” 页面，可以查看用户名、用户角色、用户登录时间、空闲时间以及用户从命令行还是 GUI 登录。

查看最近的登录尝试

要查看最近几次通过 Web 界面、SSH 和/或 FTP 进行的登录尝试（失败或成功），请执行以下操作：

步骤 1　请登录。

步骤 2　点击屏幕右上角附近 “登录身份 (Logged in as)” 旁边的 图标。

通过命令行界面查看管理用户活动

以下命令支持多用户访问设备。

- **who** 命令列出通过 CLI 或 Web 用户界面登录到系统的所有用户、用户角色、登录时间、空闲时间和用户登录的远程主机。
- `whoami` 命令显示当前登录的用户的用户名和完整名称及其所属的组：

```
mail3.example.com> whoami

用户名: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

- `last` 命令显示最近登录到设备的用户。另外，还显示远程主机的 IP 地址及登录时间、注销时间和总时间。

```
mail3.example.com> last

Username    Remote Host    Login Time          Logout Time         Total Time
========    ===========    ================    ================    ==========
admin       10.1.3.67      Sat May 15 23:42    still logged in     15m
admin       10.1.3.67      Sat May 15 22:52    Sat May 15 23:42    50m
admin       10.1.3.67      Sat May 15 11:02    Sat May 15 14:14    3h 12m
admin       10.1.3.67      Fri May 14 16:29    Fri May 14 17:43    1h 13m
shutdown                                       Fri May 14 16:22
shutdown                                       Fri May 14 16:15
admin       10.1.3.67      Fri May 14 16:05    Fri May 14 16:15    9m
admin       10.1.3.103     Fri May 14 16:12    Fri May 14 16:15    2m
admin       10.1.3.103     Thu May 13 09:31    Fri May 14 14:11    1d 4h 39m
admin       10.1.3.135     Fri May 14 10:57    Fri May 14 10:58    0m
admin       10.1.3.67      Thu May 13 17:00    Thu May 13 19:24    2h 24m
```

排除管理用户访问故障

错误：用户未被分配访问权限

问题：获得管理授权的用户可以登录到安全管理设备，但会看到未被分配访问权限的消息。

解决方案

- 确保已向此用户分配的自定义角色分配权限。依次查看 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “用户 (Users)”，确定分配的用户角色，然后依次转到 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “用户角色 (User Roles)”，点击用户角色的名称，并为该角色分配权限。
- 如果根据 “报告组 (Reporting Group)” 分配了访问权限，请确保已在 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “用户角色 (User Roles)” 页面为该用户选择了报告组。要分配组，请点击 “授权管理的用户角色 (User Roles for Delegated Administration)” 表的 “邮件报告 (Email Reporting)” 列中的**未选定组 (No groups selected)** 链接。

用户没有活动的菜单

问题：被授予 “发布 (Publish)” 权限的用户在登录时没有活动的菜单。

解决方法：确保您已为至少一个访问策略或自定义 URL 类别授予访问权限。如果不想授予此用户编辑上述两者的权限，请创建一个在任何策略中均未使用的自定义 URL 类别，并在 “自定义用户角色 (Custom User Role)” 页面授予此用户角色对该类别的权限。

通过外部身份验证的用户会看到 “首选项 (Preferences)”选项

问题：通过外部身份验证的用户会看到 “首选项 (Preferences)”选项。

解决方法：确保直接在安全管理设备中添加的用户具有外部身份验证数据库中还未使用的唯一名称。

常规管理任务

执行管理任务

通过图形用户界面 (GUI) 的 “系统管理 (System Administration)”菜单，可以执行大多数系统管理任务。但是，有些系统管理功能只能在命令行界面 (CLI) 使用。

此外，可在 “监控 (Monitor)”菜单访问设备的状态监控功能，第 10 章 “监控系统状态”中介绍了相关内容。

备注 本章介绍的一些功能或命令可能会影响路由优先顺序。有关详细信息，请参阅 IP 地址、接口和路由 （第 B-2 页）。

使用功能密钥

密钥与设备序列号和您启用的功能密切相关。不同系统之间不能重复使用同一个密钥。

要从命令行提示符执行本节介绍的任务，请使用 `featurekey` 命令。

目标	操作
• 查看设备所有有效的功能密钥 • 查看待激活的任何功能密钥 • 搜索已发布的新密钥 • 手动安装功能密钥 • 激活功能密钥	依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 功能密钥 (Feature Keys)**。 要手动添加新功能密钥，请将密钥粘贴到“功能密钥 (Feature Key)”字段或向其中输入密钥，然后点击**提交密钥 (Submit Key)**。如果未添加该功能，将出现错误消息（例如，如果密钥错误）；否则，功能密钥将添加到列表中。 如果设备配置为发布新密钥时自动下载和安装新密钥，“待激活 (Pending Activation)”列表将始终为空。
启用或禁用功能密钥自动下载和激活功能	依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 功能密钥设置 (Feature Keys Settings)**。 默认情况下，设备会定期检查新密钥。
更新过期的功能密钥	请联系您的思科代表。

虚拟设备许可和功能密钥

有关许可证和功能密钥过期后设备行为的信息，请参阅以下位置的《*思科内容安全虚拟设备安装指南*》：
http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html。

要查看许可证信息，请在命令行界面 (CLI) 使用 `showlicense` 命令。

使用 CLI 命令执行维护任务

通过本节介绍的操作和命令，您可以在安全管理设备上执行维护相关的任务。本节介绍以下操作和命令：

- `shutdown`
- `reboot`
- `suspend`
- `suspendtransfers`
- 在如图所示的
- `resumetransfers`
- `resetconfig`
- `version`

关闭安全管理设备

要关闭安全管理设备，请依次使用**管理设备 (Management Appliance) > 系统管理 (System Administration) > 关机/重启 (Shutdown/Reboot)** 页面，或在命令行提示符下使用 **shutdown** 命令。

关闭设备将退出 AsyncOS，从而允许您安全关闭设备电源。稍后可以重新启动设备，传送队列中的任何邮件都不会丢失。您必须输入设备关闭的延迟时间。默认延迟为 30 秒。在延迟期间，AsyncOS 允许打开的连接完成，延迟期间过后将强行关闭打开的连接。

重新启动安全管理设备

要重启安全管理设备，请使用 GUI “系统管理 (System Administration)”菜单中的 “关机/重启 (Shutdown/Reboot)”页面，或使用 GLI 中的 `reboot` 命令。

重启设备将重新启动 AsyncOS，从而允许您安全关闭和重启设备。您必须输入设备关闭的延迟时间。默认延迟为 30 秒。在延迟期间， AsyncOS 允许打开的连接完成，延迟期间过后将强行关闭打开的连接。可以重新启动设备，传送队列中的任何邮件都不会丢失。

停止运行安全管理设备

如果希望设备离线 （例如执行系统维护），请使用以下命令之一：

命令	描述	持久
`suspend`	• 暂停将隔离的邮件从邮件安全设备迁移到安全管理设备。 • 暂停传送从隔离区放行的邮件。 • 不接受入站邮件连接。 • 停止出站邮件传送。 • 停止日志传输。 • CLI 保持可访问。	重启后持续。
`suspendtransfers`	暂停传输托管邮件和网络安全设备的报告与跟踪数据到内容安全管理设备。 此命令还会暂停接收来自邮件安全设备的隔离邮件。 当准备将备份设备用作主设备时，可使用此命令。	重启后持续。

使用这些命令时，必须输入设备的延迟。默认延迟为 30 秒。在延迟期间， AsyncOS 允许打开的连接完成，延迟期间过后将强行关闭打开的连接。如果没有打开的连接，服务立即暂停。

要重新激活被 `suspend` 或 `suspendtransfers` 命令暂停的服务，请分别使用 `resume` 或 `resumetransfers` 命令。

要确定当前管理设备的在线/已暂停状态，请在 Web 界面中依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 关闭/重新 (Shutdown/Reboot)**。

另请参阅：

- 文档或邮件安全设备在线帮助中的 “暂停邮件传送 (Suspending Email Delivery)”、“恢复邮件传送 (Resuming Email Delivery)”、“暂停接收 (Suspending Receiving)”和 “恢复接收 (Resuming Receiving)”。

CLI 示例：suspend 和 suspendtransfers 命令

```
sma.example.com> suspend

Enter the number of seconds to wait before abruptly closing connections.
[30]> 45

Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
sma.example.com>



sma.example.com> suspendtransfers

Transfers suspended.
sma.example.com>
```

从 “已暂停 (Suspended)”状态恢复

使用 suspend 或 suspenddel 命令后， resume 命令可使设备恢复到正常运行状态。

使用 suspendtransfers 命令后， resumetransfers 命令可使设备恢复到正常运行状态。

CLI 示例：resume 和 resumetransfers 命令

```
sma.example.com> resume

Receiving resumed.
Mail delivery resumed.
sma.example.com>

sma.example.com> resumetransfers

Receiving resumed.
Transfers resumed.
sma.example.com>
```

将配置重置为出厂默认设置

从物理位置上移动设备后，或解决配置问题后的最后一步，可能希望将设备重置为出厂默认设置。

注意 重置配置会将您与用于连接设备的 CLI 禁用服务断开 （FTP、 Telnet、 SSH、 HTTP、 HTTPS），并会删除用户帐户。

目标	操作
• 将所有配置重置为出厂默认设置 • 清除所有报告计数器 但是 • 保留日志文件 • 保留隔离的邮件	1. 确保重置后，您可以使用默认 admin 用户帐户和密码连接到设备：使用串行接口连接到 CLI 或使用默认设置连接到管理端口。有关访问采用默认设置的设备的信息，请参阅第 2 章 “设置、安装和基本配置”。 2. 暂停设备上的服务。 3. 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 配置文件 (Configuration File)**，并点击**重置 (Reset)**。 **注意** 重置后，设备会自动恢复到在线状态。如果重置前邮件传送被暂停，则重置后将再次尝试传送。
• 将所有配置重置为出厂默认设置 • 删除所有数据	使用 `diagnostic > reload` CLI 命令。 ⚠ **注意** 此命令与思科路由器或交换机上使用的类似命令不同。

resetconfig 命令

```
mail3.example.com> suspend

Delay (seconds, minimum 30):
[30]> 45

Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.

mail3.example.com> resetconfig

Are you sure you want to reset all configuration values?[N]> Y

All settings have been restored to the factory default.
```

显示 AsyncOS 版本信息

操作步骤

步骤 1 在安全管理设备上，依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**。

步骤 2 滚动到页面底部，查看 “版本信息 (Version Information)” 下面，可看到当前安装的 AsyncOS 的版本。

此外，还可以在命令提示符下使用 **version** 命令。

启用远程电源管理

只有在以下硬件上，才能远程重置设备机箱的电源：M380 和 M680。

如果您希望能够远程重置设备电源，必须事先按照本节所述的步骤启用和配置此功能。

准备工作

- 使用线缆将专用的远程电源管理端口直接连接到安全网络。有关信息，请参阅《硬件安装指南》。
- 确保设备可以远程访问；例如，通过防火墙打开任何必要的端口。
- 此功能需要专用的远程电源管理接口使用唯一的 IPv4 地址。此接口仅可按照本节所述的步骤配置，而不能使用 `ipconfig` 命令配置。
- 要循环设置设备电源，需要使用可管理设备（这些设备支持智能平台管理接口 (IPMI) 版本 2.0）的第三方工具。确保您已准备好使用这些工具。
- 有关访问命令行界面的详细信息，请参阅 CLI 参考指南。

操作步骤

步骤 1　使用 SSH、 Telnet 或串行控制台端口访问命令行界面。

步骤 2　使用具有 “管理员 (Administrator)”访问权限的帐户登录。

步骤 3　输入以下命令：

```
remotepower

setup
```

步骤 4　按照提示指定以下信息：

- 此功能的专用 IP 地址，以及网络掩码和网关。
- 执行电源循环命令所需的用户名和密码。

  这些凭证与用来访问设备的其他凭证不同。

步骤 5　输入 `commit` 保存更改。

步骤 6　测试您的配置，以确定是否可以远程管理设备电源。

步骤 7　确保您输入的凭证可供您无限期使用。例如，将此信息存储在安全位置，并确保可能需要执行此任务的管理员可访问所需的凭证。

相关主题

- 远程重置设备电源 （第 16-7 页）

备份安全管理设备数据

- 备份的数据 （第 14-7 页）
- 备份的限制和要求 （第 14-7 页）
- 备份持续时间 （第 14-8 页）
- 备份期间服务的可用性 （第 14-8 页）

备份的数据

您可以选择备份所有数据，或者以下数据的任意组合：

- 垃圾邮件隔离区，包括邮件和元数据
- 集中式策略、病毒和病毒爆发隔离区，包括邮件和元数据
- 邮件跟踪 （邮件跟踪），包括邮件和元数据的
- Web 跟踪
- 报告 （邮件和 Web）
- 安全列表/阻止列表

数据传输完成后，两个设备上的数据将完全相同。

使用此过程，不备份配置和日志。要备份这些项目，请参阅其他重要的备份任务 （第 14-11 页）。

第一次备份后，每次备份仅复制自上次备份后生成的信息。

备份的限制和要求

安排备份之前，请务必了解以下限制和要求：

限制	要求
AsyncOS 版本	源和目标安全管理设备的 AsyncOS 版本必须相同。如果版本不兼容，请先将设备升级到同一版本，再安排备份。
网络中的目标设备	必须在网络中设置目标设备。 如果目标设备是新的，请运行 “系统设置向导 (System Setup Wizard)”输入必要信息。有关说明，请参阅第 2 章 “设置、安装和基本配置”。
源设备和目标设备之间的通信	源和目标安全管理设备必须能够使用 SSH 进行通信。因此： • 两台设备上的端口 22 必须打开。默认情况下，运行 “系统设置向导 (System Setup Wizard)”时会打开此端口。 • 域名服务器 (DNS) 必须能够使用 A 记录和 PTR 记录解析两台设备的主机名。
目标设备必须没有运行	只有主设备可从管理的邮件和网络安全设备提取数据。要确保这一点，请参阅防止目标设备直接从托管设备提取数据 （第 14-9 页）。 此外，取消备份设备上任何预定的配置发布作业。

限制	要求
设备容量	目标设备的磁盘空间容量必须等于或大于源设备的容量。目标设备上分配给各种数据类型 （报告、跟踪、隔离区等）的磁盘空间不能低于源设备上的相应分配。 可以预定从较大源到较小目标安全管理设备的备份，前提是目标设备上有足够的空间用于待备份的各种类型的所有数据。如果源设备比目标设备大，则必须降低源设备上分配的空间，以匹配较小的目标设备上可用的空间。 要查看和管理磁盘空间分配与容量，请参阅管理磁盘空间 （第 14-45 页）。 有关虚拟设备的磁盘容量，请参阅 《*思科内容安全虚拟设备安装指南*》。
多个、并发和链式备份	一次只能运行一个备份过程；如果某个备份安排在上一个备份完成前运行，系统将跳过该备份并发送警告。 可以将来自安全管理设备的数据备份到单一安全管理设备。 不支持链式备份 （备份到备份）。

备份持续时间

在一个完整的初始备份过程中，备份 800GB 可能最多需要 10 小时。每日备份，每次可能最多需要 3 小时。每周和每月备份可能需要更长时间。这些数值可能变化。

初始备份后，备份过程仅传输自上次备份后更改的文件。因此，后续备份比初始备份所需的时间短。后续备份所需的时间取决于自上次备份后累计的数据量、发生变化的文件数量及文件更改的程度。

备份期间服务的可用性

备份安全管理设备会将 “源”安全管理设备中的有效数据集复制到 “目标”安全管理设备，尽可能降低对始发 “源”设备的破坏。

备份过程的各个阶段及其对服务可用性的影响如下所示：

- 第 1 阶段 — 备份过程的第 1 阶段从在源设备和目标设置之间传输数据开始。在数据传输过程中，源设备上的服务保持运行，因此数据收集仍可继续。但是，目标设备上的服务将关闭。一旦从源设备到目标设备的数据传输完成，第 2 阶段开始。
- 第 2 阶段 — 第 2 阶段开始时，源设备上的服务将关闭。将自初始关闭后，源设备和目标设备之间数据传输过程中收集的任何差异复制到目标设备，且源设备和目标设备上的服务将恢复到其在启动备份时的状态。这样，可确保源设备上的正常运行时间最大化，并且两台设备均没有数据丢失。

在备份过程中，数据可用性报告可能不起作用，并且在查看邮件跟踪结果时，每封邮件的主机名可能都标记为 “未解析”。

如果您尝试安排报告，忘记了正在备份，可以通过依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services)** 检查系统状态。在此窗口中，可以看到页面顶部有关正在进行系统备份的警告。

中断备份过程

备注　如果在执行备份时源设备意外重启，目标设备不会察觉中断。您必须在目标设备上取消备份。

如果备份过程中断且备份过程未完成，则下次尝试备份时，安全管理设备可从其停止的位置继续开始备份过程。

建议不要取消正在进行的备份，因为现有数据将不完整，并且在后续备份完成前可能无法使用，特别是收到错误后。如果必须取消正在进行的备份，请务必尽快运行完整备份，以确保始终有可用的当前备份。

防止目标设备直接从托管设备提取数据

步骤 1　访问目标设备的命令行界面。有关说明，请参阅访问命令行界面 （第 2-6 页）。

步骤 2　运行 `suspendtransfers` 命令。

步骤 3　等待提示符再次出现。

步骤 4　运行 `suspend` 命令。

步骤 5　等待提示符再次出现。

步骤 6　退出目标设备的命令行界面。

接收关于备份状态的警报

要在备份完成时接收警报及获悉任何问题，请将设备配置为向您发送 “系统 (System)” 类型、严重性 “参考 (Info)” 的警报。请参阅管理警报 （第 14-28 页）。

安排一次或循环备份

可以安排在预先确定的时间进行一次备份或循环备份。

准备工作

- 解决备份的限制和要求 （第 14-7 页）中的项目。

备注　如果远程计算机上正在进行任何备份，则不会启动备份过程。

操作步骤

步骤 1　以管理员身份登录到源设备的命令行界面。

步骤 2　在命令提示符下，键入 **backupconfig** 并按 **Enter**。

步骤 3　如果源设备和目标设备之间的连接速度较慢，请打开数据压缩：

键入 **setup**，并输入 **Y**。

步骤 4　键入 **Schedule**，并按 **Enter**。

步骤 5　键入目标安全管理设备的 IP 地址。

步骤 6　输入有意义的名称以标识目标设备 （最多 20 个字符）。

步骤 7　输入目标设备的 admin 用户名和密码。

步骤 8　响应有关要备份哪些数据的提示。

步骤 9　要安排一次备份，请向 `Schedule a single backup` 中键入 **2**，并按 **Enter**。

步骤 10　压安排循环备份，请执行以下操作：

a. 向 “设置重复备份计划 (Repeating Backup Schedule)”中键入 **1**，并按 **Enter**。

b. 选择定期备份的频率，并按 **Enter**。

步骤 11　键入希望开始备份的特定日期或日期和时间，并按 **Enter**。

步骤 12　键入备份过程的名称。

步骤 13　确认是否已成功安排备份：在命令提示符下键入 **View**，并按 **Enter**。

步骤 14　另请参阅其他重要的备份任务 （第 14-11 页）。

开始即时备份

准备工作

- 满足备份的限制和要求 （第 14-7 页）中的所有要求。

备注　如果目标计算机上正在进行任何备份，则不会启动备份过程。

操作步骤

步骤 1　以管理员身份登录到源设备的命令行界面。

步骤 2　在命令提示符下，键入 **backupconfig** 并按 **Enter**。

步骤 3　如果源设备和目标设备之间的连接速度较慢，请打开数据压缩：

键入 **setup**，并输入 **Y**。

步骤 4　键入 **Schedule**，并按 **Enter**。

步骤 5　键入目标安全管理设备的 IP 地址。

步骤 6　输入有意义的名称以标识目标设备 （最多 20 个字符）。

步骤 7　输入目标设备的 admin 用户名和密码。

步骤 8　响应有关要备份哪些数据的提示。

步骤 9　向 “立即开始一次备份 (Start a Single Backup Now)”中键入 **3**，并按 **Enter**。

步骤 10　为备份作业输入有意义的名称。

备份过程将在几分钟后开始。

步骤 11　（可选）要查看备份进度，请在命令行提示符下键入 **Status**。

步骤 12　另请参阅其他重要的备份任务 （第 14-11 页）。

查看备份状态

步骤 1　以管理员身份登录到主设备的命令行界面。

步骤 2　在命令提示符下，键入 **backupconfig** 并按 **Enter**。

查看状态	操作
预定的备份	选择 `View` 操作。
正在进行的备份	选择 `Status` 操作。 如果您配置了警报，请检查您的邮件或参阅查看最近的警报 （第 14-29 页）。

相关主题

- 日志文件中的备份信息 （第 14-11 页）

日志文件中的备份信息

备份日志自始至终记录备份过程。

SMA 日志中包含备份计划的相关信息。

相关主题

- 查看备份状态 （第 14-11 页）

其他重要的备份任务

为了防止本节所述的备份过程未备份的项目丢失，并加速设置设备故障情况下的替代安全管理设备，请考虑执行以下操作：

- 要保存主安全管理设备中的设置，请参阅保存和导入配置设置 （第 14-39 页）。将配置文件保存到主安全管理设备之外的安全位置。
- 保存用于填充主配置的任何安全管理设备配置文件。
- 要将安全管理设备中的日志文件保存到备用位置，请参阅日志订阅 （第 15-21 页）。

  此外，还可以设置 “备份日志 (Backup Logs)” 的日志订阅。请参阅在 GUI 中创建日志订阅（第 15-22 页）。

将备份设备设为主设备

如果要升级设备硬件，或出于任何其他原因需要切换设备，请执行此程序。

准备工作

回顾备份安全管理设备数据 （第 14-6 页）中的信息。

操作步骤

步骤 1　将旧/主/源设备中的配置文件副本保存到从新设备可访问的位置。请参阅保存和导入配置设置（第 14-39 页）。

步骤 2　在新/备份/目标设备上运行 “系统设置向导 (System Setup Wizard)”。

步骤 3　满足备份的限制和要求 （第 14-7 页）中的要求。

步骤 4　在旧/主/源设备中运行备份。请参阅开始即时备份 （第 14-10 页）中的说明。

步骤 5　等待备份完成。

步骤 6　在旧/主/源设备上运行 `suspendtransfers` 和 `suspend` 命令。

步骤 7　运行第二次备份，将旧/主/源设备最后的数据传输到新/备份/目标设备。

步骤 8　将配置文件导入到新/备份/目标设备。

步骤 9　在新/备份/目标设备上运行 `resumetransfers` 和 `resume` 命令。

切勿在旧/原主/源设备上运行此命令。

步骤 10　在新/备份/目标设备和管理的邮件与网络安全设备之间建立连接：

a. 依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。

b. 点击设备名称。

c. 点击**建立连接 (Establish Connection)** 按钮。

d. 点击**测试连接**。

e. 返回设备列表。

f. 对于每个托管设备重复上述操作。

步骤 11　确认新/目标设备现在是否可用作主设备：

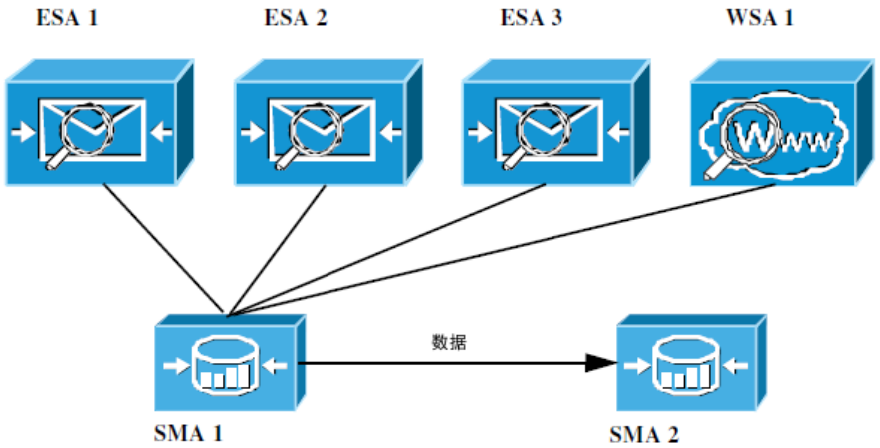
依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**状态，并检查数据传输状态。

安全管理设备上的灾难恢复

如果您的安全管理设备遇到意外故障，请按照以下程序恢复安全管理服务和根据备份安全管理设备数据 （第 14-6 页）中的信息定期保存的备份数据。

典型的设备配置可能如图 14-1 中所示：

图 14-1　　灾难恢复：典型环境



在此环境中，SMA 1 是从 ESA 1-3 及 WSA 1 接收数据的主安全管理设备。SMA 2 是从 SMA1 接收备份数据的备份安全管理设备。

如果出现故障，必须将 SMA 2 配置为您的主安全管理设备。

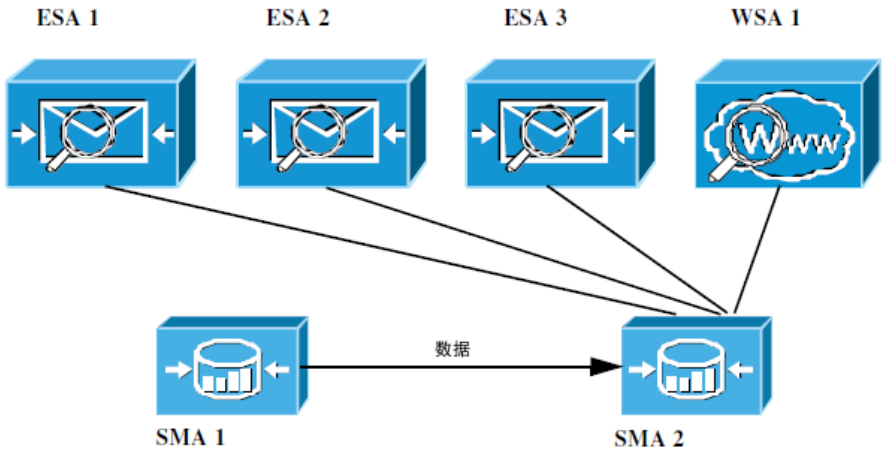
要将 SMA 2 配置为新的主安全管理设备并恢复服务，请执行以下操作：

步骤	操作	更多信息
步骤 1	如果使用集中式策略、病毒和病毒爆发隔离区： 在每个邮件安全设备上，禁用集中式隔离区。	有关禁用集中式策略、病毒和病毒爆发隔离区的说明，请参阅邮件安全设备文档。 这样将在每台邮件安全设备上创建本地隔离区，稍后可以将它们迁移到新的安全管理设备。
步骤 2	将您在主安全管理设备 (SMA1) 中保存的配置文件加载到备份安全管理设备 (SMA2)。	请参阅加载配置文件 （第 14-40 页）。
步骤 3	将出现故障的 SMA 1 的 IP 地址重新创建为 SMA 2 上的 IP 地址。	1. 在 SMA 2 中，依次选择**网络 (Network) > IP 接口 (IP Interfaces) > 添加 IP 接口 (Add IP Interfaces)**。 2. 在**添加 IP 接口 (Add IP Interfaces)** 页面，将出现故障的 SMA1 中的所有相关 IP 接口信息输入到文本字段，以便在 SMA 2 上重新创建接口。 有关添加 IP 接口的详细信息，请参阅配置 IP 接口 （第 A-1 页）。
步骤 4	提交并确认更改。	—

步骤	操作	更多信息
步骤 5	在新的安全管理设备 (SMA 2) 上启用所有适用的集中服务。	请参阅在安全管理设备上配置服务 （第 2-12 页）。
步骤 6	将所有设备添加到新的安全管理设备 (SMA 2)。 通过建立到设备的连接并测试连接，测试查看每台设备是否已启用并可运行。	请参阅关于添加托管设备 （第 2-10 页）。
步骤 7	如果使用集中式策略、病毒和病毒爆发隔离区，请在新的安全管理设备上配置隔离区迁移，然后在每台适用的邮件安全设备上启用和配置迁移。	请参阅集中策略、病毒和爆发隔离区 （第 8-3 页）。
步骤 8	如果需要，恢复其他数据。	请参阅其他重要的备份任务（第 14-11 页）。

完成此过程后， SMA 2 将变成主安全管理设备。现在， ESA 1-3 及 WSA 1 的所有数据将转至 SMA 2，如图 14-2 中所示。

图 14-2　　灾难恢复：最终结果



升级设备硬件

请参阅将备份设备设为主设备 （第 14-12 页）。

升级 AsyncOS

- 批量升级命令 （第 14-15 页）
- 确定升级和更新的网络要求 （第 14-15 页）
- 选择升级方法：远程与数据流 （第 14-15 页）
- 配置升级和更新服务设置 （第 14-18 页）
- 升级之前：重要步骤 （第 14-22 页）

批量升级命令

有关升级过程的批量命令，请参阅以下位置的 《AsyncOS for Email CLI 参考指南》 (CLI Reference Guide for AsyncOS for Email)：
http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html。

确定升级和更新的网络要求

思科内容安全设备的更新服务器使用动态 IP 地址。如果您有很强的防火墙策略，可能需要为 AsyncOS 升级配置静态位置。如果确定您的防火墙设置需要静态 IP 进行升级，请联系思科客户支持获取所需的 URL 地址。

备注　如果您任何现有的防火墙规则允许从 `upgrades.cisco.com` 端口 （例如 22、 25、 80、 4766）下载传统升级，则需要删除它们和/或将其替换为修订的防火墙规则。

选择升级方法：远程与数据流

思科提供两种升级设备 AsyncOS 的方法 （或 “来源”）：

- 数据流升级 — 每台设备通过 HTTP 直接从思科内容安全更新服务器下载 AsyncOS 升级。
- 远程升级 — 一次只从思科下载升级映像，然后将其添加到您的设备。然后，由您的设备从网络内的服务器的下载 AsyncOS 升级。

您可在配置升级和更新服务设置 （第 14-18 页）中配置升级方法。或者，在 GLI 中使用 **updateconfig** 命令。

数据流升级概述

在 “数据流 (Streaming)” 升级中，每台思科内容安全设备直接连接到思科内容安全更新服务器查找并下载升级：

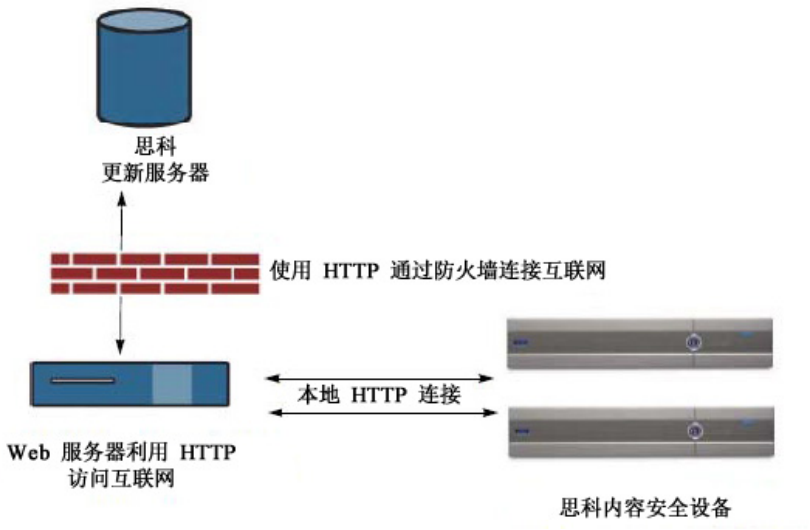
图 14-3　　数据流更新方法

此方法需要您的设备直接从网络联系思科内容安全更新服务器。

远程升级概述

您还可以从自己的网络内将更新本地下载和托管到 AsyncOS （远程升级），而不是直接从思科更新服务器获取更新 （数据流升级）。使用此功能，加密的更新映像将通过 HTTP 下载到网络中有权访问互联网的任何服务器。如果选择下载更新映像，然后即可配置内部 HTTP 服务器 （“更新管理器”）将 AsyncOS 映像托管到您的安全管理设备。

图 14-4　远程更新方法



基本流程如下所示：

操作步骤

步骤 1　阅读远程升级的硬件和软件要求 （第 14-17 页）和托管远程升级映像 （第 14-17 页）中的信息。

步骤 2　配置本地服务器，以检索和提供升级文件。

步骤 3　下载升级文件。

步骤 4　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 更新设置 (Update Settings)**。

在此页面，选择将设备配置为使用本地服务器。

步骤 5　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 系统升级 (System Upgrade)**。

步骤 6　点击**可用升级 (Available Upgrades)**。

注　在命令行提示符下，还可以执行以下操作：运行 **updateconfig** 命令，然后运行 **upgrade** 命令。

有关完整信息，请参阅升级 AsyncOS （第 14-14 页）。

远程升级的硬件和软件要求

要 *下载* AsyncOS 升级文件，您的内部网络中必须有系统可满足以下条件：

- 通过互联网访问思科内容安全设备的更新服务器。
- Web 浏览器。

备注 对于此版本，如果需要配置防火墙设置以允许 HTTP 访问此地址，则必须使用 DNS 名称 （而不是特定 IP 地址）对其进行配置。

要 *托管* AsyncOS 更新文件，您的内部网络中必须有服务器可满足以下条件：

- 网络服务器 （例如 Microsoft IIS (Internet Information Services) 或 Apache 开源服务器：
  - 支持目录或文件名显示超出 24 个字符
  - 已启用目录浏览
  - 配置为匿名 （无身份验证）或基本 （“简单”）身份验证
  - 至少包含 350MB 可用磁盘空间，用于每个 AsyncOS 更新映像

托管远程升级映像

设置本地服务器后，请转至 **http://updates.ironport.com/fetch_manifest.html** 下载升级影像的压缩文件。要下载映像，请输入您的思科内容安全设备的序列号和版本号。然后，系统将显示您可用的升级列表。点击要下载其升级映像压缩文件的升级版本。要使用 AsyncOS 升级的升级映像，请在 “编辑更新设置 (Edit Update Settings)”页面输入您的本地服务器的基本 URL （或在 CLI 中使用 `updateconfig`）。

此外，还可以在本地服务器上托管 XML 文件，将网络中的思科内容安全设备可用升级限制为以下网址所选的版本：`http://updates.ironport.com/fetch_manifest.html`。思科内容安全设备仍从思科服务器下载升级。如果要在本地服务器中托管升级列表，请下载压缩文件并将 `asyncos/phoebe-my-upgrade.xml` 文件提取到本地服务器的根目录。要使用 AsyncOS 升级的升级列表，请在 “编辑更新设置 (Edit Update Settings)”页面输入 XML 文件的完整 URL （或在 CLI 中使用 `updateconfig`）。

有关远程升级的详细信息，请查阅知识库 （请参阅知识库文章 （技术说明）（第 E-3 页））或与您的支持提供商联系。

远程升级方法中的重要差异

请注意从本地服务器升级 AsyncOS （远程升级）与数据流升级方法的差异：

- 升级在 *下载的同时* 将立即安装。
- 升级开始时，标语将显示 10 秒。显示此标语时，您可以选择按 Ctrl - C 在下载开始前退出升级过程。

配置升级和更新服务设置

您可以配置思科内容安全设备如何下载安全服务更新 （例如时区规则）和 AsyncOS 升级。例如，可以选择是从思科服务器，还是从可获得其映像的本地服务器动态下载升级和更新，是否配置更新间隔或禁用自动更新。

AsyncOS 定期查询更新服务器中针对所有安全服务组件的新更新 （新 AsyncOS 升级除外）。要升级 AsyncOS，必须手动提示 AsyncOS 查询可用的升级。

您可以在 GUI 中配置升级和更新设置 （请参阅以下两个部分），也可以在 CLI 中使用 `updateconfig` 命令进行配置。

此外，还可以配置升级通知设置。

升级和更新设置

表 14-1 介绍了可配置的更新和升级设置。

表 14-1　　安全服务的更新设置

设置	说明
更新服务器 （映像）	选择从思科服务器还是本地网络服务器下载 AsyncOS 升级和服务更新软件映像 （例如时区规则和功能密钥更新）。默认设置为从思科服务器下载升级和更新。 在以下情况下，您可能想要使用本地网络服务器： • 需要从静态地址下载映像到设备。请参阅具有强防火墙策略的环境的静态升级和更新服务器设置 （第 14-19 页）。 • 希望在方便时将 AsyncOS 升级映像下载到设备。（仍可从思科更新服务器动态下载服务更新映像。） 选择本地更新服务器时，请输入用于下载升级和更新的服务器的基本 URL 和端口号。如果服务器需要身份验证，也可以输入有效的用户名和密码。 有关详细信息，请参阅选择升级方法：远程与数据流 （第 14-15 页）和远程升级概述 （第 14-16 页）。
更新服务器 （列表）	选择从思科服务器还是本地网络服务器下载可用的升级和服务更新列表 （证明 XML 文件）。 默认升级和更新都从思科服务器下载。可以为升级和更新选择不同的设置。 如果适用，请参阅具有强防火墙策略的环境的静态升级和更新服务器设置 （第 14-19 页）。 如果选择本地更新服务器，请输入指向每个列表的证明 XML 文件的完整路径，包括文件名和服务器的端口号。如果将端口字段留空，AsyncOS 将使用端口 80。如果服务器需要身份验证，也可以输入有效的用户名和密码。 有关详细信息，请参阅选择升级方法：远程与数据流 （第 14-15 页）和远程升级概述 （第 14-16 页）。
自动更新	选择是否为时区规则启用自动更新。启用时，请输入两次检查更新之间等待的时间。后缀 **m** 表示分钟， **h** 表示小时， **d** 表示天。

表 14-1　安全服务的更新设置 （续）

设置	说明
接口	选择当与更新服务器联系以进行时区规则更新和 AsyncOS 升级时要使用哪个网络接口。将显示可用的代理数据接口。默认情况下，设备会选择一个接口进行使用。
HTTP 代理服务器	如果存在上游 HTTP 代理服务器并且需要身份验证，请在此输入服务器信息、用户名和密码。 请注意，如果指定代理服务器，将使用它来访问和更新 GUI 中列出的服务。 此外，此代理服务器还用于从云获取文件分析报告详细信息。另请参阅有关文件分析报告详细信息的要求 （第 5-19 页）（Web 报告）或有关文件分析报告详细信息的要求 （第 4-24 页）（邮件报告）。
HTTPS 代理服务器	如果存在上游 HTTPS 代理服务器并且需要身份验证，请在此输入服务器信息、用户名和密码。 请注意，如果指定代理服务器，将使用它来访问和更新 GUI 中列出的服务。 此外，此代理服务器还用于从云获取文件分析报告详细信息。另请参阅有关文件分析报告详细信息的要求 （第 5-19 页）（Web 报告）或有关文件分析报告详细信息的要求 （第 4-24 页）（邮件报告）。

具有强防火墙策略的环境的静态升级和更新服务器设置

AsyncOS 更新服务器使用动态 IP 地址。如果您的环境设有强防火墙策略，需要静态 IP 地址，请在 “更新设置 (Update Settings)”页面使用以下设置：

图 14-5　更新服务器 （映像）设置的静态 URL

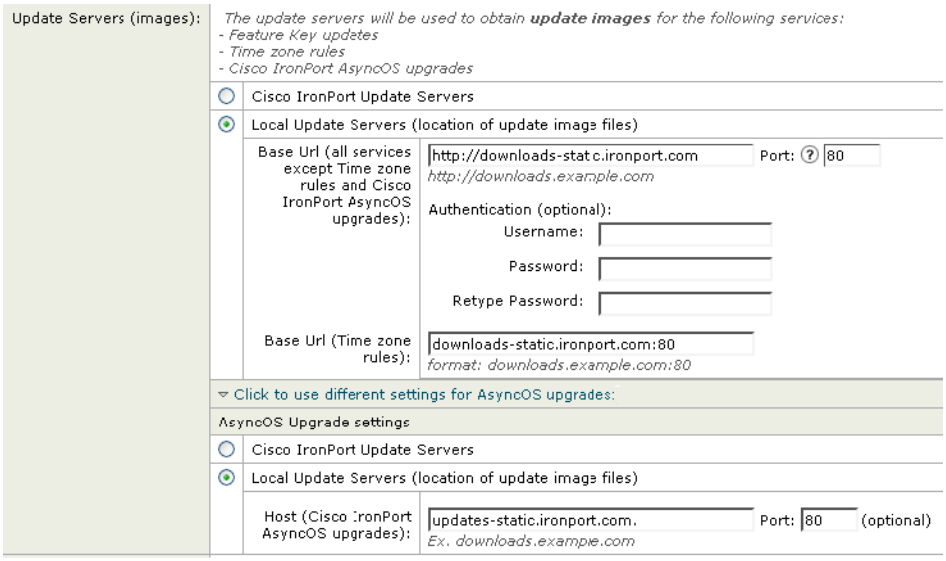


图 14-6　更新服务器 （列表）设置的静态 URL

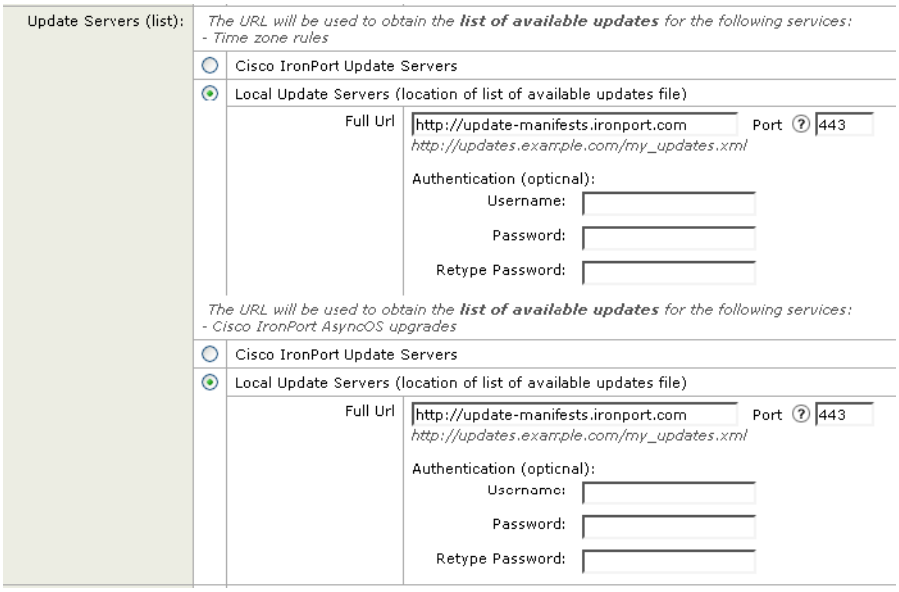


表 14-2　具有强防火墙策略的环境的静态地址

部分	设置	静态 URL/IP 地址和端口
更新服务器 (镜像):	基本 URL （除时区规则和 AsyncOS 升级之外的所有服务）	http://downloads-static.ironport.com 204.15.82.8 端口 80
	基本 URL （时区规则）	downloads-static.ironport.com 204.15.82.8 端口 80
	主机 （AsyncOS 升级）	updates-static.ironport.com 208.90.58.25 端口 80
更新服务器 (列表):	对于物理硬件设备上的更新： 完整 URL	update-manifests.ironport.com 208.90.58.5 端口 443
	对于虚拟设备上的更新：完整 URL	update-manifests.sco.cisco.com 端口 443
	对于升级：完整 URL	update-manifests.ironport.com 208.90.58.5 端口 443

从 GUI 配置更新和升级设置

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 更新设置 (Update Settings)**。

步骤 2　点击**编辑更新设置 (Edit Update Settings)**。

按照升级和更新设置 （第 14-18 页）中的说明配置此过程的设置。

步骤 3　在**更新服务器 (映像) (Update Servers (images))** 部分，指定从其中下载更新映像的服务器。

步骤 4　指定从其中下载 AsyncOS 升级映像的服务器:

a. 在同一部分的底部，点击**点击使用不同的 AsyncOS 升级设置 (Click to use different settings for AsyncOS upgrades)** 链接。

b. 指定下载 AsyncOS 升级映像的服务器设置。

步骤 5　在**更新服务器 (列表) (Update Servers (list))** 部分，指定获取可用更新和 AsyncOS 升级列表的服务器。

顶部小节适用于更新。底部小节适用于升级。

步骤 6　指定时区规则和接口的设置。

步骤 7　（可选）指定代理服务器的设置。

步骤 8　提交并确认更改。

步骤 9　确认您的结果是否符合预期：

如果还没有查看 “更新设置 (Update Settings)”页面，请依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 更新设置 (Update Settings)**。

有些 URL 可能会向服务器 URL 中附加 “asyncos”目录。您可以忽略此差异。

升级通知

默认情况下，当设备有 AsyncOS 升级时，具有管理员和技术人员权限的用户将在 Web 界面顶部看到通知。

目标	操作
查看有关最新升级的详细信息	将鼠标悬停在升级通知上方。
查看所有可用升级的列表	点击通知中的向下箭头。
关闭当前的通知。 有新升级之前，设备不会显示其他通知。	点击向下箭头，然后选择**清除通知 (Clear the notification)**，再点击**关闭 (Close)**。
预防将来的通知 （仅限具有 “管理员 (Administrator)”权限的用户）。	依次转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 系统升级 (System Upgrade)**。

升级之前：重要步骤

准备工作

请参阅确定升级和更新的网络要求 （第 14-15 页）中的网络掩码要求。

操作步骤

步骤 1　采取措施来防止或最大限度地降低数据丢失：

- 确保新设备有足够的磁盘容量，对于将传输的各种数据类型，分配的磁盘容量相同或更大。请参阅磁盘空间最大值和分配值 （第 14-46 页）。
- 如果您收到了任何磁盘空间警告，请在升级之前解决所有磁盘空间问题。

步骤 2　保存设备的 XML 配置文件。请参阅保存和导出当前配置文件 （第 14-40 页）中的警告。

如果出于任何原因需要恢复到升级之前的版本，将需要此文件。

步骤 3　如果要使用 “安全列表/阻止列表 (Safelist/Blocklist)” 功能，请从设备导出该列表。

依次点击**管理设备 (Management Appliance) > 系统管理 (System Administration) > 配置文件 (Configuration File)**，并向下滚动。

步骤 4　从 CLI 运行升级时，使用 **suspendlistener** 命令暂停监听程序。如果从 GUI 执行升级，则会自动暂停监听程序。

步骤 5　排空邮件队列和传送队列。

步骤 6　确认升级设置的配置是否符合期望。请参阅配置升级和更新服务设置 （第 14-18 页）。

升级 AsyncOS

可以在单个操作中下载并安装，也可以在后头下载，稍后安装。

备注　当从本地服务器而不是思科服务器一次操作完成下载和升级 AsyncOS 时，*在下载时*会立即进行安装。升级开始时，标语将显示 10 秒。显示此标语时，您可以选择按 Ctrl - C 在下载开始前退出升级过程。

准备工作

- 选择是直接从思科下载升级，还是在网络的服务器中托管升级映像。然后，设置您的网络以支持所选的方式。然后，将设备配置为从您所选的来源获取升级。请参阅选择升级方法：远程与数据流 （第 14-15 页）和配置升级和更新服务设置 （第 14-18 页）。
- 在安装升级之前，请按照升级之前：重要步骤 （第 14-22 页）中的说明执行操作。

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 系统升级 (System Upgrade)**。

步骤 2　点击**升级选项 (Upgrade Options)**。

步骤 3　选择一个选项：

目标	操作
在一次操作中下载并安装升级	点击**下载并安装 (Download and Install)**。 如果您已下载安装程序，系统将提示您会覆盖现有的下载。
下载升级安装程序	点击**仅下载 (Download only)**。 如果您已下载安装程序，系统将提示您会覆盖现有的下载。 安装程序在后台下载，而不会中断服务。
安装已下载的升级安装程序	点击**安装**。 只有下载安装程序后，才会显示此选项。 “安装 (Install)”选项下方将标注要安装的 AsyncOS 版本。

步骤 4　除非要安装以前下载的安装程序，否则请从可用升级列表中选择一个 AsyncOS 版本。

步骤 5　如果要安装：

a. 选择是否将当前配置保存到设备上的 `configuration` 目录。

b. 选择是否屏蔽配置文件中的密码。

注　无法使用 GUI 中的 “配置文件 (Configuration File)”页面或 CLI 中的 `loadconfig` 命令加载带屏蔽密码的配置文件。

c. 如果要将通过邮件发送配置文件的副本，请输入要将该文件发送到的邮件地址。使用逗号分隔多个邮件地址。

步骤 6　点击**继续**。

步骤 7　如果要安装：

a. 请准备好在这个过程中响应提示。

流程暂停，直到您做出响应。

进度条显示在页面顶部附近。

b. 在提示符下，点击**立即重启 (Reboot Now)**。

注　重启后至少 20 分钟之前，请勿出于任何原因断开设备的电源 （甚至是为了排除升级问题）。

c. 大约 10 分钟后，请再次访问设备并登录。

后续操作

- 如果流程中断，必须重新开始该流程。
- 如果已下载但未安装升级：

  在准备安装升级时，请从开始按照这些说明执行操作，包括 “准备工作 (Before You Begin)”部分的必备条件，但请选择 “安装 (Install)”选项。
- 如果已安装升级，请参阅升级后 （第 14-24 页）。

查看后台下载状态、取消或删除后台下载

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 系统升级 (System Upgrade)**。

步骤 2　点击**升级选项 (Upgrade Options)**。

步骤 3　选择一个选项：

目标	操作
查看下载状态	在页面中间查找。 如果没有正在进行的下载，且无完成的下载等待安装，则不会看到下载状态信息。 upgrade_logs 中也会显示“升级 (Upgrade)”状态。
取消下载	点击页面中间的**取消下载 (Cancel Download)** 按钮。 只有正在进行下载时，才会显示此选项。
删除已下载的安装程序	点击页面中间的**删除文件 (Delete File)** 按钮。 只有下载安装程序后，才会显示此选项。

升级后

升级完成后，请完成以下操作：

- （对于使用关联的邮件安全设备部署）重新启用监听程序。
- （对于使用关联的网络安全设备部署）将您的系统配置为支持最新的主配置。请参阅设置主配置以集中管理网络安全设备 （第 9-2 页）。
- 考虑保存您的配置。有关详细信息，请参阅保存和导入配置设置 （第 14-39 页）。
- 升级后查看在线帮助之前，请清除您的浏览器缓存，退出浏览器，然后再次打开它。这样可清除任何过时内容的浏览器缓存。

关于恢复到更早版本的 AsyncOS

在紧急情况下，可以恢复到先前合格的 AsyncOS 版本以供使用。

如果要清除设备上的所有数据并从新的清洁配置开始，还可以恢复到当前运行的内部版本。

- 关于恢复影响的重要注意事项 （第 14-25 页）
- 恢复 AsyncOS （第 14-25 页）

关于恢复影响的重要注意事项

在思科内容安全设备上使用 `revert` 命令执行操作的破坏性很大。此命令将永久销毁所有现有的配置和数据。此外，在重新配置设备之前，还会中断邮件处理。

恢复不影响功能密钥或虚拟设备许可证到期日期。

恢复 AsyncOS

准备工作

- 备份或保存您想要保留到设备某个位置的任何数据。
- 您必须具有想要恢复到的版本的配置文件。配置文件*不*向后兼容。
- 由于此命令会销毁所有配置，所以强烈建议您在恢复时有权物理访问本地设备。
- 如果您的邮件安全设备上启用了隔离区，请禁用集中功能，以便邮件本地隔离在这些设备上。

操作步骤

步骤 1　确保您拥有想要恢复到的版本的配置文件。配置文件不向后兼容。

步骤 2　在其他计算机上保存设备当前配置的备份副本 （不屏蔽密码）。为此，可以通过邮件将该文件发送给自己或通过 FTP 发送文件。一种简单方法是运行 `mailconfig` CLI 命令，它可通过邮件将设备上当前的配置文件发送至指定邮件地址。

注　这不是您在恢复后要加载的配置文件。

步骤 3　如果使用 “安全列表/阻止列表 (Safelist/Blocklist)”功能，请将 “安全列表/阻止列表 (Safelist/Blocklist)”数据库导出到其他计算机。

步骤 4　暂停您的邮件安全设备上的任何监听程序。

步骤 5　等待邮件队列清空。

步骤 6　登录到您要恢复的设备的 CLI。

在运行 `revert` 命令时，系统将发出许多警告提示。一旦接受这些警告提示，将会立即执行恢复操作。因此，在完成恢复前的步骤之前，请勿开始恢复过程。

步骤 7　从命令行提示符下，键入 **revert** 命令并响应提示。

以下示例显示了 **revert** 命令：

```
m650p03.prep> revert

This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy
quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco Spam Quarantine message and end-user safelist/blocklist data

Only the network settings will be preseved.
```

```
Before running this command, be sure you have:
- saved the configuration file of this appliance (with passwords
unmasked)
- exported the Cisco Spam Quarantine safelist/blocklist database
   to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots again to the desired
version.

是否要继续?是

是否确定要继续? 是

Available versions
==================
 1.7.2.0-390
 2.6.7.6-020

Please select an AsyncOS version: 1

You have selected "7.2.0-390".

Reverting to "testing" preconfigure install mode.

The system will now reboot to perform the revert operation.
```

步骤 8　等待设备重启两次。

步骤 9　使用 CLI 登录到设备。

步骤 10　至少添加一台网络安全设备并等待几分钟，以允许从该设备下载任何 “URL 类别 (URL Category)” 更新。

步骤 11　完成 “URL 类别 (URL Category)” 更新后，加载您要恢复到的版本的 XML 配置文件。

步骤 12　如果使用 “安全列表/阻止列表 (Safelist/Blocklist)” 功能，请导入并恢复 “安全列表/阻止列表 (Safelist/Blocklist)” 数据库。

步骤 13　在邮件安全设备上重新启用任何监听程序。

步骤 14　确认更改。

现在，恢复的思科内容安全设备应使用所选的 AsyncOS 版本运行。

备注　可能需要 15-20 分钟才会完成恢复，并可重新通过控制台访问思科内容安全设备。

关于更新

服务更新定期推出以供下载。要指定这些下载的设置，请参阅配置升级和更新服务设置 （第 14-18 页）。

相关主题

- 关于网络使用控制的 URL 类别集更新 （第 14-27 页）
- 配置升级和更新服务设置 （第 14-18 页）

关于网络使用控制的 URL 类别集更新

- 准备和管理 URL 类别集更新 （第 9-19 页）
- URL 类别集更新和报告 （第 5-13 页）

配置生成的邮件的返回地址

在以下情况下，您可以为 AsyncOS 生成的邮件配置信封发件人：

- 退回邮件
- 报告

您可以指定返回地址的显示名称、用户名和域名。还可以选择对于域名使用 “虚拟网关 (Virtual Gateway)” 域。

使用 GUI “系统管理 (System Administration)” 菜单中可用的 “返回地址 (Return Addresses)” 页面，或在 CLI 中使用 **addressconfig** 命令。

要在 GUI 中修改系统生成的电子邮件的返回地址，请点击 “返回地址 (Return Addresses)” 页面中的**编辑设置 (Edit Settings)**。更改您要修改的地址，然后点击**提交 (Submit)**，并确认更改。

管理警报

如果设备中发生事件，设备会向您发送邮件警报。

目标	操作
向不同的管理用户发送不同类型的警报	依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报 (Alerts)** 如果在系统设置期间启用了 “自动支持 (AutoSupport)”，则您指定的邮件地址将默认接收所有严重性和类型的警告。可以随时更改配置。 多个地址之间用逗号分隔。
配置警报的全局设置，包括： • 警报发件人 （从：）地址 • 重复警报的控制 • 自动支持设置	依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报 (Alerts)** 请参阅关于重复警报 （第 14-29 页） 请参阅思科自动支持 （第 14-30 页）
查看最近的警报列表 管理此列表的设置	请参阅查看最近的警报 （第 14-29 页）
请参阅警报及其说明列表	请参阅： 硬件警报说明 （第 14-30 页） 系统警报说明 （第 14-30 页）
了解警报传送机制	请参阅警报传送 （第 14-29 页）

警报类型和严重性

警报类型包括：

- 硬件警报。请参阅硬件警报说明 （第 14-30 页）。
- 系统警报。请参阅系统警报说明 （第 14-30 页）。
- 更新警报。

警报的严重性如下所示：

- 严重：需要立即注意的问题
- 警告：需要进一步监控和可能需要立即注意的问题或错误
- 参考：此服务例行运行当中生成的信息

警报传送

由于警报可用来通知您思科内容安全设备中的问题，所以不使用 AsyncOS 正常的邮件传送系统发送它们。相反，警报邮件通过独立而并行的电子邮件系统传递，即便在 AsyncOS 存在重大系统故障时也会运行。

警报邮件系统与 AsyncOS 的配置不同，也就是说，警报邮件可能与其他邮件传送的行为稍有不同：

- 警报邮件通过标准 DNS MX 和 A 记录查找传送。
  - 它们确实会缓存 DNS 条目 30 分钟，缓存每 30 分钟刷新一次，所以如果 DNS 出现故障，警报将停止。
- 如果部署包括邮件安全设备：
  - 警报邮件不通过工作队列传递，所以不对它们病毒扫描或垃圾邮件。另外，它们也不受邮件过滤器或内容过滤器约束。
  - 警报邮件不通过传送队列传递，所以不受退回配置文件或目标控制限制影响。

查看最近的警报

目标	操作
查看最近的警报列表	具有管理员和操作员访问权限的用户可以依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报 (Alerts)**，然后点击**查看顶部警报 (View Top Alerts)** 按钮。 即使通过邮件发送它们时出现问题，也会显示警报。
排序列表	点击列标题。
指定此列表中保存的最大警报数	在命令行界面使用 `alertconfig` 命令。
禁用此功能	在命令行界面使用 `alertconfig` 命令，将最大警报数量设置为零 (0)。

关于重复警报

可以指定 AsyncOS 发送重复警报前等待的初始秒数。如果将此值设置为 0，不会发送重复警报摘要，而是毫无任何延迟地发送所有重复警报 （这样可能导致短时间内发送大量电子邮件）。发送每个警报后，发送重复警报之间等待的秒数 （警报间隔）将增加。增加值是等待的秒数加上最后间隔的两倍。因此，如果等待 5 秒，警报发送时间将是 5 秒、15 秒、35 秒、75 秒、155 秒、315 秒，以此类推。

最终，间隔可能变得很大。您可以通过 “发送重复警报前等待的最大秒数 (maximum number of seconds to wait before sending a duplicate alert)”字段，设置间隔之间等待的秒数限值。例如，如果将初始值设置为 5 秒，最大值为 60 秒，则在 5 秒、15 秒、35 秒、60 秒、120 秒时发送警报，以此类推。

思科自动支持

为了使思科能够更好地支持和设计未来的系统变更，可以将思科内容安全设备配置为向思科发送系统生成的所有警报邮件的副本。此功能称为 “自动支持 (AutoSupport)”，是允许客户支持主动支持您的需求的有效方式。“自动支持 (AutoSupport)”还发送每周报告，说明系统正常运行时间、 **status** 命令的输出和使用的 AsyncOS 版本。

默认情况下，设置为接收 “参考 (Information)”严重级别的 “系统 (System)”警报类型的警报收件人，会收到发往思科的每封邮件的副本。如果您不希望内部每周发送警报邮件，可以禁用此功能。要启用或禁用此功能，请依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报 (Alerts)**，并点击编辑设置。

默认情况下，如果启用了 “自动支持 (AutoSupport)”，则每周向设置为接收 “参考 (Information)”级别系统警报的警报收件人发送自动支持报告。

硬件警报说明

警报名称	说明	严重性
INTERFACE.ERRORS	检测到接口错误时发送。	警告
MAIL.MEASUREMENTS_ FILESYSTEM	当磁盘分区接近容量 (75%) 时发送。	警告
MAIL.MEASUREMENTS_ FILESYSTEM.CRITICAL	当磁盘分区达到 90% 容量 （以及 95%、 96%、 97% 等）时发送。	严重
SYSTEM.RAID_EVENT_ ALERT	发生严重 RAID 事件时发送。	警告
SYSTEM.RAID_EVENT_ ALERT_INFO	发生 RAID 事件时发送。	信息

系统警报说明

警报名称	说明	严重性
COMMON.APP_FAILURE	出现未知应用故障时发送。	严重
COMMON.KEY_EXPIRED_ALERT	功能密钥过期时发送。	警告
COMMON.KEY_EXPIRING_ALERT	功能密钥即将到期时发送。	警告
COMMON.KEY_FINAL_ EXPIRING_ALERT	以功能密钥即将到期的最终通知形式发送。	警告
DNS.BOOTSTRAP_FAILED	当设备无法与根 DNS 服务器通信时发送。	警告
INTERFACE.FAILOVER.FAILURE_ BACKUP_DETECTED	当备份 NIC 配对接口发生故障时发送。	警告
INTERFACE.FAILOVER.FAILURE_ BACKUP_RECOVERED	恢复 NIC 配对故障转移时发送。	信息
INTERFACE.FAILOVER.FAILURE_DETECTED	检测到由于接口故障导致 NIC 配对故障转移时发送。	严重

警报名称	说明	严重性
INTERFACE.FAILOVER.FAILURE_DETECTED_NO_BACKUP	检测到由于接口故障导致 NIC 配对故障转移，但备用接口不可用时发送。	严重
INTERFACE.FAILOVER.FAILURE_RECOVERED	恢复 NIC 配对故障转移时发送。	信息
INTERFACE.FAILOVER.手动	检测到手动故障转移到其他 NIC 配对时发送。	信息
COMMON.INVALID_FILTER	当遇到无效过滤器时发送。	警告
IPBLOCKD.HOST_ADDED_TO_WHITELIST **IPBLOCKD.HOST_ADDED_TO_BLACKLIST** **IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST**	警报邮件： • 由于 SSH DOS 攻击，已将 <IP 地址> 的主机添加到黑名单。 • 已将 <IP 地址> 的主机永久添加到 ssh 白名单。 • 已从黑名单删除 <IP 地址> 的主机。 对于尝试通过 SSH 连接到设备，但未提供有效凭证的 IP 地址，如果两分钟内失败尝试次数大于 10 次，则将其添加到 SSH 黑名单。 如果用户从同一 IP 地址成功登录，则将该 IP 地址添加到白名单。 白名单的地址即使在黑名单中，也允许它们访问。	警告
LDAP.GROUP_QUERY_FAILED_ALERT	当 LDAP 组查询失败时发送。	严重
LDAP.HARD_ERROR	当 LDAP 查询完全失败时（尝试所有服务器之后）发送。	严重
LOG.ERROR.*	各种日志记录错误。	严重
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	扫描各个收件人期间 LDAP 组查询失败时发送。	严重
MAIL.QUEUE.ERROR.*	各种邮件队列硬错误。	严重
MAIL.RES_CON_START_ALERT.MEMORY	当 RAM 使用率超过系统资源节约阈值时发送。	严重
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	当邮件队列过载及企业系统资源节约时发送。	严重
MAIL.RES_CON_START_ALERT.QUEUE	当队列使用率超过系统资源节约阈值时发送。	严重
MAIL.RES_CON_START_ALERT.WORKQ	由于工作队列过大暂停监听程序时发送。	严重
MAIL.RES_CON_START_ALERT	当设备进入 “资源节约” 模式时发送。	严重
MAIL.RES_CON_STOP_ALERT	当设备退出 “资源节约” 模式时发送。	严重
MAIL.WORK_QUEUE_PAUSED_NATURAL	当工作队列暂停时发送。	严重
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	当工作队列恢复时发送。	严重
NTP.NOT_ROOT	当设备由于 NTP 未以根用户身份运行而无法调整时间时发送。	警告

警报名称	说明	严重性
PERIODIC_REPORTS.DOMAIN_REPORT.DOMAIN_FILE_ERRORS	在域规范文件中发现错误时发送。	严重
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_ EMPTY	当域规范文件为空时发送。	严重
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_ MISSING	找不到域规范文件时发送。	严重
REPORTD.DATABASE_ OPEN_FAILED_ALERT	当报告引擎无法打开数据库时发送。	严重
REPORTD.AGGREGATION_DISABLED_ALERT	当系统磁盘空间不足时发送。当日志条目的磁盘使用量超过日志使用阈值时，报告禁用聚合并发送警报。	警告
REPORTING.CLIENT.UPDATE_FAILED_ALERT	当报告引擎无法保存报告数据时发送。	警告
REPORTING.CLIENT.JOURNAL.FULL	当报告引擎无法存储新数据时发送。	严重
REPORTING.CLIENT.JOURNAL.FREE	当报告引擎再次能够存储新数据时发送。	信息
PERIODIC_REPORTS.REPORT_TASK.BUILD_ FAILURE_ALERT	当报告引擎无法生成报告时发送。	严重
PERIODIC_REPORTS.REPORT_TASK.EMAIL_ FAILURE_ALERT	当无法通过邮件发送报告时发送。	严重
PERIODIC_REPORTS.REPORT_TASK.ARCHIVE_FAILURE_ALERT	当报告无法存档时发送。	严重
SENDERBASE.ERROR	处理 SenderBase 的响应出错时发送。	信息
SMAD.ICCM.ALERT_PUSH_ FAILED	当一个或多个主机的配置推送失败时发送。	警告
SMAD.TRANSFER.TRANSFERS_STALLED	当 SMA 日志连续两小时无法获取跟踪数据或连续六小时无法获取报告数据时发送。	警告
SMTPAUTH.FWD_SERVER_FAILED_ALERT	无法访问 SMTP 身份验证转发服务器时发送。	警告
SMTPAUTH.LDAP_QUERY_FAILED	当 LDAP 查询失败时发送。	警告
SYSTEM.HERMES_ SHUTDOWN_FAILURE. 重新启动	关闭正在重启的系统出现问题时发送。	警告
SYSTEM.HERMES_ SHUTDOWN_FAILURE. SHUTDOWN	关闭系统出现问题时发送。	警告
SYSTEM.RCPTVALIDATION.UPDATE_ FAILED	当收件人验证更新失败时发送。	严重

警报名称	说明	严重性
SYSTEM.SERVICE_TUNNEL.DISABLED	禁用为 “思科支持服务 (Cisco Support Services)” 创建的隧道时发送。	信息
SYSTEM.SERVICE_TUNNEL.ENABLED	启用为 “思科支持服务 (Cisco Support Services)” 创建的隧道时发送。	信息

更改网络设置

本节介绍用于配置设备网络操作的功能。通过这些功能，可以直接访问在运行 “系统设置向导 (System Setup Wizard)”（第 2-7 页）中使用 “系统设置向导 (System Setup Wizard)” 配置的主机名、 DNS 和路由设置。

本节讨论以下功能：

- `sethostname`
- DNS 配置 （在 GUI 中，以及通过在 CLI 中使用 `dnsconfig` 命令）
- 路由配置 （在 GUI 中，以及通过在 CLI 中使用 `routeconfig` 和 `setgateway` 命令）
- `dnsflush`
- 密码

更改系统主机名

主机名用于在 CLI 提示符下识别系统。必须输入完全限定的主机名。 `sethostname` 命令用于设置内容安全设备的名称。只有发出 `commit` 命令后，新主机名才会生效。

sethostname 命令

```
oldname.example.com> sethostname

[oldname.example.com]> mail3.example.com

oldname.example.com>
```

要使主机名更改生效，必须输入 `commit` 命令。成功确认主机名更改后，新名称将显示在 CLI 提示符中：

```
oldname.example.com> commit

请输入一些对您所作更改的描述：
[]> Changed System Hostname
Changes committed: Mon Jan 04 12:00:01 2010
```

提示符中显示的新主机名如下所示：`mail3.example.com>`

配置域名系统设置

您可以在 GUI 中通过“管理设备 (Management Appliance)”>“网络 (Network)”>“DNS”页面（或通过 `dnsconfig` 命令）配置 “域名系统 (DNS)”设置。

可以配置以下设置：

- 使用 Internet 的 DNS 服务器还是自己的服务器，以及具体使用的服务器
- 用于 DNS 通信的接口
- 反向 DNS 查询超时前等待的秒数
- 清除 DNS 缓存

指定 DNS 服务器

AsyncOS 可以使用 Internet 根 DNS 服务器、您自己的 DNS 服务器，或 Internet 根 DNS 服务器和您指定的授权 DNS 服务器。使用 Internet 根服务器时，可以指定用于特定域的备用服务器。由于备用 DNS 服务器适用于单个域，所有它必须对该域拥有授权 （提供限定的 DNS 记录）。

不使用 Internet 的 DNS 服务器时， AsyncOS 支持 “拆分” DNS 服务器。如果您要使用自己的内部服务器，还可以指定例外域及关联的 DNS 服务器。

设置 “拆分 DNS”时，还应设置 in-addr.arpa (PTR) 条目。例如，如果要将 “.eng”查询重定向到名称服务器 1.2.3.4，并且所有 .eng 条目均在 172.16 网络，则应将 “eng,16.172.in-addr.arpa”指定为拆分 DNS 配置中的域。

多个条目和优先级

对于输入的每个 DNS 服务器，都可以指定一个数字优先级。AsyncOS 将尝试使用优先级最接近 0 的 DNS 服务器。如果该 DNS 服务器没有响应， AsyncOS 将尝试使用下一个优先级的服务器。如果为相同优先级的 DNS 服务器指定了多个条目，则系统在每次执行查询时会随机列出该优先级的 DNS 服务器。然后，系统会等待一小段时间，以便第一个查询到期或 “超时”，然后对第二个查询等待稍长一段时间，以此类推。时间量取决于确切的 DNS 服务器总数和已配置的优先级。在任何特定优先级，所有 IP 地址的超时长度相同。第一个优先级的超时时间最短，后续每个优先级的超时时间依次延长。而且，超时期限约为 60 秒。如果有一个优先级，则该优先级每台服务器的超时为 60 秒。如果有两个优先级，则第一个优先级每台服务器的超时为 15 秒；第二个优先级每台服务器的超时为 45 秒。对于三个优先级，超时分别为 5 秒、 10 秒、 45 秒。

例如，假设您配置了四台 DNS 服务器，其中两台为优先级 0，一台为优先级 1，另一台为优先级 2：

表 14-3　DNS 服务器、优先级和超时间隔示例

优先级	服务器	超时 （秒）
0	1.2.3.4、 1.2.3.5	5、 5
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS 在优先级为 0 的两台服务器之间随机选择。如果一台优先级 0 的服务器关闭，则使用另一台。如果优先级为 0 的两台服务器均关闭，则使用优先级为 1 的服务器 (1.2.3.6)，最后是优先级为 2 (1.2.3.7) 的服务器。

两台优先级为 0 的服务器的超时期限相同，优先级为 1 的服务器稍长，优先级为 2 的服务器更长。

使用 Internet 根服务器

AsyncOS DNS 解析器旨在容纳高性能邮件传送所需的大量并行 DNS 连接。

备注　如果选择将默认 DNS 服务器设置为 Internet 根服务器之外的其他服务器，则该服务器必须能够递归解析其不属于授权服务器的域的查询。

反向 DNS 查询超时

思科内容安全设备尝试对连接到监听程序来收发邮件的所有远程主机执行 “双向 DNS 查询”。即系统通过执行双向 DNS 查询，获取和验证远程主机 IP 地址的有效性。其中包括对连接主机的 IP 地址的反向 DNS (PTR) 查询，之后是对 PTR 查询结果的正向 DNS (A) 查询。然后，系统将检查 A 查询结果是否与 PTR 查询结果匹配。如果结果不匹配或 A 记录不存在，则系统将仅使用 IP 地址来匹配主机访问表 (HAT) 中的条目。此特定超时期限仅适用于此查询，与多个条目和优先级（第 14-34 页）中讨论的通用 GNS 超时无关。

默认值为 20 秒。可以全局禁用所有侦听程序中的反向 DNS 查询超时，方法是输入 “0”作为秒数。如果该值设置为 0 秒，则不尝试反向 DNS 查询，而是立即返回标准超时响应。

DNS 警报

有时，重启设备时，系统会生成警报，其中包含 “无法引导 DNS 缓存”的消息。该消息表示系统无法与其主 DNS 服务器通信，如果在建立网络连接前 DNS 子系统已上线，则可能在启动时出现这种情况。如果其他时候出现此消息，可能表示存在网络问题或 DNS 配置未指向有效的服务器。

清除 DNS 缓存

GUI 中的**清除缓存 (Clear Cache)** 按钮或`dnsflush` 命令（有关 `dnsflush` 命令的详细信息，请参阅 CLI 参考指南，可从文档（第 E-2 页）中指定的位置获取）将清除 DNS 缓存中的所有信息。更改本地 DNS 系统后，您可能会选择使用此功能。该命令会立即生效，并且重新填充缓存时可能导致性能临时下降。

通过图形用户界面配置 DNS 设置

操作步骤

步骤 1　在**管理设备 (Management Appliance) > 网络 (Network) > DNS** 页面上，点击**编辑设置 (Edit Settings)** 按钮。

步骤 2　选择使用 Internet 的根 DNS 服务器还是自己的内部 DNS 服务器，并指定授权 DNS 服务器。

步骤 3　如果您要使用自己的 DNS 服务器或指定授权 DNS 服务器，请输入服务器 ID 并点击**添加行 (Add Row)**。对于每个服务器重复上述步骤。在输入自己的 DNS 服务器时，还请指定优先级。有关详细信息，请参阅指定 DNS 服务器（第 14-34 页）。

步骤 4　选择用于 DNS 通信的接口。

步骤 5　输入取消反向 DNS 查询之前等待的秒数。

步骤 6　或者，可以点击**清除缓存 (Clear Cache)** 清除 DNS 缓存。

步骤 7　提交并确认更改。

配置 TCP/IP 通信路由

有些网络环境需要使用标准默认网关以外的通信路由。您可以在 GUI 中通过 “管理设备 (Management Appliance)” > “网络 (Network)” > “路由 (Routing)”页面 （或在 CLI 中使用 `routeconfig` 命令）管理静态路由。

- 在 GUI 中管理静态路由 （第 14-36 页）
- 修改默认网关 （GUI ）（第 14-36 页）

在 GUI 中管理静态路由

通过 “管理设备 (Management Appliance)” > “网络 (Network)” > “路由 (Routing)”页面，可以创建、编辑或删除静态路由。还可以在此页面修改默认网关。

操作步骤

步骤 1　在 “管理设备 (Management Appliance)” > “网络 (Network)” > “路由 (Routing)”页面，点击路由列表中的**添加路由 (Add Route)**。输入路由名称。

步骤 2　输入目标 IP 地址。

步骤 3　输入网关 IP 地址。

步骤 4　提交并确认更改。

修改默认网关 （GUI ）

操作步骤

步骤 1　在 “路由 (Routing)”页面点击路由列表中的 “默认路由 (Default Route)”。

步骤 2　更改网关 IP 地址。

步骤 3　提交并确认更改。

配置默认网关

在 GUI 中通过 “管理设备 (Management Appliance)” > “网络 (Network)” > “路由 (Routing)”页面 （请参阅修改默认网关 （GUI ）（第 14-36 页）），或在 CLI 中使用 `setgateway` 命令，可以配置默认网关。

配置系统时间

备注 在收集报告数据时，安全管理设备会应用您在安全管理设备上配置时间设置时所设置信息中的时间戳。有关信息，请参阅 “安全设备如何为报告收集数据”部分 （第 3-2 页）。

要使用命令行界面设置与时间相关的设置，请使用 `ntpconfig`、 `settime` 和 `settz` 命令。

目标	操作
设置置系统时间	**依次选择 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “时间设置 (Time Settings)”** 另请参阅使用网络时间协议 (NTP) 服务器（第 14-37 页）
设置时区	依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 时区 (Time Zone)** 另请参阅： • 选择 GMT 偏移时间 （第 14-38 页） • 更新时区文件 （第 14-38 页）

使用网络时间协议 (NTP) 服务器

可以使用网络时间协议 (NTP) 服务器将安全管理设备的系统时钟与网络中的其他计算机或 Internet 同步。

默认NTP服务器是 `time.sco.cisco.com`。

如果使用外部 NTP 服务器 （包括默认 NTP 服务器），请通过防火墙打开所需的端口。请参阅第 C 章 “防火墙信息”

相关主题

- 配置系统时间 （第 14-37 页）

选择 GMT 偏移时间

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 时区 (Time Zone)**。

步骤 2　点击**编辑设置 (Edit Settings)**。

步骤 3　从区域列表中选择 “GMT 偏移时间 (GMT Offset)”。“时区设置 (Time Zone Setting)”页面将更新，“时区 (Time Zone)”字段包括 GMT 偏移时间。

步骤 4　在 “时区 (Time Zone)”字段中选择偏移时间。偏移时间是指相对格林威治标准时间 (GMT) （本初子午线当地时间）添加或减去的小时数。小时前缀减号 （“-”）表示本初本初子午线以西。加号 （“+”）表示本初子午线以东的位置。

步骤 5　提交并确认更改。

更新时区文件

一旦任何国家/地区的时区规则发生变化，必须更新设备上的 “时区 (Time Zone)”文件。

- 自动更新时区文件 （第 14-38 页）
- 手动更新时区文件 （第 14-38 页）

自动更新时区文件

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 更新设置 (Update Settings)**。

步骤 2　选中**启用时区规则自动更新 (Enable automatic updates for Time zone rules)** 复选框。

步骤 3　输入间隔。点击重要信息页面中的 **?** 帮助。

步骤 4　提交并确认更改。

手动更新时区文件

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 时间设置 (Time Settings)**。

步骤 2　查看**时区文件更新 (Time Zone File Updates)** 部分。

步骤 3　如果有可用的时区文件更新，请点击**立即更新 (Update Now)**。

“配置文件” (Configuration File) 页

有关此部分的信息	请参阅
保存当前配置	保存和导入配置设置 （第 14-39 页）
加载保存的配置	保存和导入配置设置 （第 14-39 页）
最终用户安全列表/阻止列表数据库（垃圾邮件隔离区）	备份和恢复安全列表/阻止列表 （第 7-13 页）
重置配置	将配置重置为出厂默认设置

保存和导入配置设置

备注 此部分中介绍的配置文件用于配置安全管理设备。第 9 章 “管理网络安全设备”中介绍的配置文件和主配置用于配置网络安全设备。

安全管理设备的大多数配置设置可在单一配置文件中管理。该文件以可扩展标记语言 (XML) 格式保存。

可以通过多种方式使用此文件：

- 如果主安全管理设备发生意外灾难，可以快速再配置一台安全管理设备来恢复服务。
- 可以将配置文件保存到其他系统，以备份和保存重要的配置数据。如果在配置设备时出错，可以 “回滚”到最近保存的配置文件。
- 可以下载现有的配置文件，快速查看设备的整个配置。（许多新浏览器具有直接显示 XML 文件的功能。）这样，可以帮助您解决当前配置中可能存在的细微错误 （例如排字错误）。
- 可以下载现有的配置文件，对其更改，再将其上传到同一设备。这实际上是 “绕过” CLI 和 GUI 更改配置。
- 可以通过 FTP 上传整个配置文件，也可以将一部分配置文件直接粘贴到 CLI。
- 由于文件是 XML 格式，所以还会提供描述配置文件中所有 XML 实体的相关文档类型定义 (DTD)。可以下载 DTD 先验证 XML 配置文件，再进行上传。（XML 验证工具可从 Internet 中获取。）
- 可以使用配置文件来加快其他设备的配置，例如克隆的虚拟设备。

管理配置文件

- 备份和恢复安全列表/阻止列表 （第 7-13 页）
- 将配置重置为出厂默认设置 （第 14-4 页）
- 回滚至先前确认的配置 （第 14-42 页）

保存和导出当前配置文件

使用“管理设备 (Management Appliance)”>“系统管理 (System Administration)”>“配置文件 (Configuration File)”页面的“当前配置 (Current Configuration)”部分，可以将当前配置文件保存到本地计算机，保存在设备上（放在 FTP/SCP 根的 `configuration` 目录）或通过邮件发送至指定地址。

屏蔽密码

通过选中复选框可以屏蔽用户的密码。屏蔽密码会使初始加密的密码在导出或保存的文件中替换为“*****”。

备注　无法将包含屏蔽密码的配置文件重新加载到 AsyncOS。

加载配置文件

必须已从设备中保存配置文件，该设备与将加载配置的设备运行的 AsyncOS 版本相同。

无法加载包含屏蔽密码的配置文件。

无论使用哪种方法，在配置顶部必须包括以下标记：

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
 ... your configuration information in valid XML
</config>
```

结束的 `</config>` 标记应跟随配置信息。对照思科内容安全设备上 `configuration` 目录中的 DTD 解析和验证 XML 语法中的值。DTD 文件名为 `config.dtd`。如果使用 `loadconfig` 命令时命令行报告验证错误，则未加载更改。可以下载 DTD 先在设备之外验证配置文件，再上传它们。

使用任何导入方法，均可导入整个配置文件（最高级别标记之间定义的信息：`<config></config>`）或配置文件的*完整*和*唯一*子部分，只要其中包含声明标记（如上），并括在`<config></config>`标记中即可。

“完整”表示 DTD 定义的特定小节的完整开始和结束标记都包括在内。例如，上传或粘贴以下代码将导致验证错误：

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosu
</config>
```

但是，上传或粘贴以下代码不会导致验证错误：

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosupport_enabled>
</config>
```

“唯一”表示要上传或粘贴的配置文件的子部分对于该配置非常明确。例如，系统可能只有一个主机名，所以允许上传以下代码（包括声明和 `<config></config>` 标记）：

```
<hostname>mail4.example.com</hostname>
```

但是，系统可能定义了多个监听程序，并为每个监听程序定义了不同的 “收件人访问表 (Recipient Access Tables)”，所以仅上传以下代码会模糊不清：

```
<rat>
   <rat_entry>
     <rat_address>ALL</rat_address>
     <access>RELAY</access>
   </rat_entry>
</rat>
```

由于它并不明确，所以不允许上传，即使是 “完整”语法亦不例外。

注意　上传或粘贴配置文件或配置文件的子部分时，可能会清除待处理的未确认更改。

空标记与忽略的标记

上传或粘贴一部分配置文件时，请务必小心。如果不带标记，在加载配置文件时则不会修改其在配置中的值。但是，如果包括空标记，则其配置将被清除。

例如，上传以下代码会从系统中删除所有监听程序：

```
<listeners></listeners>
```

注意　上传或粘贴配置文件的子部分时，可能会从 GUI 或 CLI 断开自己并损坏大量配置数据。如果无法使用其他协议、串行接口或管理端口的默认设置重新连接到设备，请勿使用此命令禁用服务。此外，如果不确定 DTD 定义的确切配置语法，请勿使用此命令。务必先备份配置数据，再加载新的配置文件。

关于加载日志订阅密码的注意事项

如果尝试加载的配置文件包含需要密码的日志订阅 （例如，将使用 FTP 推送的日志订阅），`loadconfig` 命令不会警告您缺少密码。 FTP 推送失败，系统将生成警报，直到使用 `logconfig` 命令配置正确的密码。

关于字符集编码的注意事项

XML 配置文件的 “编码”属性必须是 “`ISO-8859-1`”，无论您使用哪种字符集离线操作文件。只要发送 `showconfig`、 `saveconfig` 或 `mailconfig` 命令，都需要在文件中指定编码属性：

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

重置当前的配置

重置当前配置会使您的思科内容安全设备设置恢复到原始出厂默认设置。在重置之前，请保存您的配置。

请参阅将配置重置为出厂默认设置 （第 14-4 页）。

回滚至先前确认的配置

您可以将配置回滚到先前确认的配置。

在命令行界面使用 rollbackconfig 命令，选择最近十个确认的配置之一。

如果在系统提示确认回滚时输入 No，将在您下次确认更改时确认回滚。

只有具有 “管理员 (Administrator)” 访问权限的用户才能使用 rollbackconfig 命令。

备注　恢复先前的配置时，不会生成日志消息或警报。

备注　某些确认 （例如向不足以暂存现有数据的空间重新分配磁盘空间）可能会导致数据丢失。

配置文件的 CLI 命令

使用以下命令可以操作配置文件：

- showconfig
- mailconfig
- saveconfig
- loadconfig
- rollbackconfig
- resetconfig （请参阅将配置重置为出厂默认设置 （第 14-4 页））
- publishconfig
- backupconfig （请参阅备份安全管理设备数据 （第 14-6 页））

showconfig、 mailconfig 和 saveconfig 命令

对于配置命令 showconfig、mailconfig 和 saveconfig，系统将提示您选择是否在将发送或显示的文件中包括密码。选择不包括密码将使任何密码字段保留为空。如果担心安全漏洞，可以选择不包括密码。但是，使用 loadconfig 命令加载不带密码的配置文件将会失败。请参阅关于加载日志订阅密码的注意事项 （第 14-41 页）。

备注　如果选择包括密码 （对 “是否要包括密码？ (Do you want to include passwords?)” 回答 “是 (Yes)”），在保存、显示或发送配置文件时，密码将进行加密。但是，私钥和证书将保留非加密的 PEM 格式。

Showconfig 命令可将当前配置打印到屏幕。

```
mail3.example.com> showconfig

Do you want to include passwords?Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
```

```
<!--
  Product: model number Messaging Gateway Appliance(tm)
  Model Number: model number
  Version: version of AsyncOS installed
  Serial Number: serial number
  Current Time: current time and date
[The remainder of the configuration file is printed to the screen.]
```

使用 mailconfig 命令可将当前配置通过电子邮件发送给用户。名为 config.xml 的 XML 格式的配置文件将附加到邮件中。

```
mail3.example.com> mailconfig

Please enter the email address to which you want to send
the configuration file.
[]> administrator@example.com

Do you want to include passwords?Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.[N]> 是

The configuration file has been sent to administrator@example.com.
```

安全管理设备上的 saveconfig 命令可将具有唯一文件名的所有主配置文件 （ESA 和 WSA）存储和保存到 configuration 目录。

```
mail3.example.com> saveconfig

Do you want to include passwords?Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.[N]> 是

The file C650-00065B8FCEAB-31PM121-20030630T130433.xml has been saved in the configuration
directory.
mail3.example.com>
```

loadconfig 命令

使用 loadconfig 命令可将新配置信息加载到设备。可以使用以下两种方法之一加载信息：

- 将信息放在 configuration 目录，然后上传
- 将配置信息直接粘贴到 CLI

有关详细信息，请参阅加载配置文件 （第 14-40 页）。

rollbackconfig 命令

请参阅回滚至先前确认的配置 （第 14-42 页）。

publishconfig 命令

使用 publishconfig 命令可发布主配置变更。语法如下：

publishconfig *config_master* [*job_name*] [*host_list* | *host_ip*

其中， *config_master* 是支持的主配置，请参阅此版本版本说明中的 “兼容性列表 (Compatibility Matrix)”：http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html。此关键字为必填字段。关键字 *job_name* 是可选的，如果未指定，将会生成该关键字。

关键字 *host_list* 是要发布的 WSA 设备的主机名或 IP 地址列表，将发布到分配到主配置的所有主机 （如果未指定）。可选 *host_ip* 可以是用逗号分隔的多个主机 IP 地址。

要确认 publishconfig 命令是否成功，请检查 smad_logs 文件。还可以选择网络 (Web) > **用程序 (Utilities) > 网络设备状态 (Web Appliance Status)**，从安全管理设备 GUI 确认发布历史记录是否成功。在此页面选择想要获取其发布历史记录详细信息的网络设备。此外，可以转到 “发布历史记录 (Publish History)”页面：**网络 (Web) > 实用程序 (Utilities) > 发布 (Publish) > 发布历史记录 (Publish History)**。

使用 CLI 上传配置更改

操作步骤

步骤 1　在 CLI 之外，确保您能够访问设备的 configuration 目录。有关详细信息，请参阅附录 A “IP 接口和设备访问”。

步骤 2　将整个配置文件或配置文件的子部分放在设备的 configuration 目录，或编辑从 saveconfig 命令创建的现有配置。

步骤 3　在 CLI 中，使用 loadconfig 命令加载您在步骤 2 放在目录中的配置文件，或将文本 （XML 语法）直接粘贴到 CLI。

在本例中，将上传名为 changed.config.xml 的文件，并确认更改：

```
mail3.example.com> loadconfig

1.Paste via CLI
2.Load from file
[1]> 2

Enter the name of the file to import:
[]> changed.config.xml

Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
```

在本例中，直接在命令行中粘贴新的配置文件。（切记在空白行中按 Ctrl-D 结束粘贴命令。）然后，使用 “系统设置向导 (System Setup Wizard)”更改默认主机名、IP 地址和网关信息。（有关详细信息，请参阅运行 “系统设置向导 (System Setup Wizard)”（第 2-7 页）。）最后，确认更改。

```
mail3.example.com> loadconfig

1.Paste via CLI
2.Load from file
[1]> 1

Paste the configuration file now.Press CTRL-D on a blank line when done.

[The configuration file is pasted until the end tag </config>. Control-D is entered on a
separate line.]

Values have been loaded.
Be sure to run "commit" to make these settings active.

mail3.example.com> commit

请输入一些对您所作更改的描述：
[]> pasted new configuration file and changed default settings
```

管理磁盘空间

您可以在组织使用的功能之间分配可用的磁盘空间，最多为最大可用空间。

（仅限虚拟设备）增加可用磁盘空间

对于运行 ESXi 5.5 和 VMFS 5 的虚拟设备，最多可以分配 2 TB 磁盘空间。对于运行 ESXi 5.1 的设备，限制为 2 TB。

备注　在 ESXi 中，不支持减少磁盘空间。请参阅 VMWare 文档中的相关信息。

要向虚拟设备实例添加磁盘空间，请执行以下操作：

准备工作

仔细确定所需的磁盘空间。

操作步骤

步骤 1　关闭思科内容安全管理设备实例。

步骤 2　使用 VMWare 提供的实用程序或管理工具增加磁盘空间。

有关更改虚拟磁盘配置的信息，请参阅 VMWare 文档。

有关 ESXi 5.5 的信息，请参阅此处：
http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html。

步骤 3　依次转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 磁盘管理 (Disk Management)**，并确认那你的更改是否已生效。

查看磁盘配额和使用量

目标	操作
查看为每个安全管理设备的监控服务分配的磁盘空间量及其当前使用的空间量	依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 磁盘管理 (Disk Management)**。
查看当前使用的隔离区的配额百分比	依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**状态，并查看 “集中服务。

磁盘空间最大值和分配值

表 14-4　最大可用磁盘空间 （硬件） (GB)

	硬件型号							
	M160	M170	M380	M660	M670	M680	M1060	M1070
所有数据类型总可用空间	165	165	968	681	681	1805	1039	1407

- 安全管理设备上的 “集中报告磁盘空间 (Centralized Reporting Disk Space)” 用于邮件和网络数据。如果启用 “集中邮件报告 (Centralized Email Reporting)” 或 “集中 Web 报告 (Centralized Web Reporting)”，所有空间将专用于启用的功能。如果启用两者，邮件和 Web 报告数据将共享空间，在按先到顺序分配空间。
- 如果启用集中 Web 报告，但没有为该报告分配磁盘空间，则在分配磁盘空间之前，集中 Web 报告不起作用。
- 在将 “其他 (Miscellaneous)” 配额降至低于当前使用水平之前，应先删除不需要的数据。请参阅管理 “其他 (Miscellaneous)” 配额的磁盘空间 （第 14-47 页）。
- 有关如何管理策略、病毒和病毒爆发隔离区的磁盘空间的详细信息，请参阅策略、病毒和爆发隔离区的磁盘空间分配 （第 8-8 页）和邮件在隔离区中的保留时间 （第 8-9 页）。
- 对于所以其他数据类型，如果要将现有分配降至低于当前使用量，系统将删除最早的数据，直到所有数据符合新分配的空间量。
- 如果新配额比当前使用的磁盘空间大，您不会丢失数据。
- 如果将分配设置为零，则不会保留任何数据。

确保收到有关磁盘空间的警报

当 “其他 (Miscellaneous)” 磁盘使用量达到配额的 75% 时，将开始接收警告级别的系统警报。在收到这些警报时，您应采取措施。

要确保收到这些警报，请参阅管理警报 （第 14-28 页）。

管理 “其他 (Miscellaneous)”配额的磁盘空间

“其他 (Miscellaneous)”配额包括系统数据和用户数据。无法删除系统数据。您可以管理以下文件类型的用户数据：

管理	操作
日志文件	依次转至 “管理设备 (Management Appliance)” > **系统管理 (System Administration) > 日志订阅 (Log Subscriptions)**，并且： • 点击 “大小 (Size)”列标题，查看哪些日志占用的磁盘空间最大。 • 确认是否需要将生成的所有日志订阅。 • 确认日志级别的详细程度是否超出必要。 • 如果可行，降低回滚文件的大小。
数据包捕获	依次转至**帮助和支持 (Help and Support)**（屏幕右上侧附近）> **数据包捕获 (Packet Capture)**。删除所有不需要的捕获。
配置文件 （这些文件不太可能占用太多磁盘空间。）	通过 FTP 转至设备的 `/data/pub` 目录。 要配置通过 FTP 访问设备，请参阅通过 FTP 访问设备 （第 A-3 页）。

重新分配磁盘空间配额

如果磁盘空间分配给您不使用的功能，或设备经常因为某一特定功能耗尽磁盘空间，但其他功能还有富余空间，则您可以重新重新分配磁盘空间。

如果所有功能都需要更多空间，请考虑升级硬件或为虚拟设备分配更多磁盘空间。请参阅（仅限虚拟设备）增加可用磁盘空间 （第 14-45 页）。

准备工作

- 更改磁盘分配可能会影响现有数据或功能的可用性。请参阅磁盘空间最大值和分配值 （第 14-46 页）中的信息。
- 通过在隔离区手动放行或删除邮件，可以临时在隔离区中创建空间。

操作步骤

步骤 1　在安全管理设备上，依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 磁盘管理 (Disk Management)**。

步骤 2　点击**编辑磁盘配额 (Edit Disk Quotas)**。

步骤 3　在**编辑磁盘配额 (Edit Disk Quotas)** 页面，输入为每项服务分配的磁盘空间量 （单位：GB）。

步骤 4　点击 **Submit**。

步骤 5　在确认对话框中，点击**设置新配额 (Set New Quotas)**。

步骤 6　点击**确认 (Commit)** 确认更改。

自定义视图

使用收藏夹页面

（仅限通过本地身份验证的管理用户。）可以创建最常用的页面的快速访问列表。

目标	操作
将页面添加到收藏夹列表	导航到要添加的页面，然后从窗口右上角附近的 “我的收藏夹 (My Favorites)” 菜单选择**将此页添加到我的收藏夹 (Add This Page To My Favorites)**。 更改 “我的收藏夹 (My Favorites)” 时不需要确认。
对收藏夹进行重新排序	依次选择**我的收藏夹 (My Favorites) > 查看我的所有收藏夹 (View All My Favorites)**，并按所需的顺序拖动收藏夹。
编辑收藏夹页面、名称或说明	依次选择**我的收藏夹 (My Favorites) > 查看我的所有收藏夹 (View All My Favorites)**，并点击要编辑的收藏夹的名称。
删除收藏夹	依次选择**我的收藏夹 (My Favorites) > 查看我的所有收藏夹 (View All My Favorites)**，并删除收藏夹。
转到收藏夹页面	从窗口右上角附近的**我的收藏夹 (My Favorites)** 菜单选择一个页面。
查看或构建自定义报告页面	请参阅自定义报告 （第 3-6 页）。
返回主界面	选择任何收藏夹，或点击页面底部的**返回上一页 (Return to previous page)**。

设置首选项

在安全管理设备上配置的管理用户

通过本地身份验证的用户可以选择以下首选项，用户每次登录到安全管理设备时可以应用它们：

- 语言 （适用于 GUI 和 PDF 报告）
- 登录页面 （登录后显示的页面）
- 默认报告时间范围页面 （可用选项为邮件和 Web 报告页面可用时间范围的子集）
- 报告页面表格中可见的行数

确切的选项取决于用户角色。

要设置这些首选项，请依次选择**选项 (Options) > 首选项 (Preferences)**。（“选项 (Options)” 菜单位于 GUI 窗口的右上角。）完成后提交更改。无需确认。

提示 要返回访问 “首选项 (Preferences)” 页面之前查看的页面，请点击页面底部的**返回上一页 (Return to previous page)** 链接。

经过外部身份验证的用户

外部身份验证的用户可以直接在 “选项 (Options)” 菜单中选择显示语言。

日志记录

日志记录概述

日志文件记录系统上相关活动的常规操作和例外。使用日志可以监控思科内容安全设备，解决问题并评估系统性能。

大多数日志都以纯文本 (ASCII) 格式记录；但是，跟踪日志以二进制格式记录以提高资源效率。ASCII 文本信息在任何文本编辑器中均可读。

日志记录与报告

使用日志记录数据调试邮件流，显示基本日常操作信息 （如 FTP 连接详细信息、 HTTP 日志文件），以及进行合规性N归档。

您可以直接在邮件安全设备上访问此日志记录数据，或将其发送到任何外部 FTP 服务器以进行归档或读取。您可以通过 FTPN 连接到设备以访问日志，或将纯文本日志推送到外部服务器以进行备份。

要查看报告数据，请使用设备 GUI 上 N 的 N “报告 (Report)”页面。您无法以任何方式访问基础数据，而且N此数据无法发送到除思科内容管理设备以外的N任何设备。

备注 安全管理设备会为所有报告和跟踪提取信息，但垃圾邮件隔离区数据除外。此数据 N 从 ESA 推送。

日志检索

日志文件可以通过表 15-1 中所述的文件传输协议进行N检索。您可以在 GUI 中创建或编辑日志订阅时或通过使用 CLI 中的 `logconfig` 命令设置该协议。

表 15-1　　日志传输协议

FTP 轮询	通过此类型的文件传输，远程 FTP 客户端可使用管理员级别或操作员级别的用户名和密码来访问设备，以检索日志文件。当配置日志订阅以使用 FTP 轮询方法时，必须提供要保留的最大日志文件数。当达到最大数量时，系统将删除最早的文件。
FTP 推送	通过此类型的文件传输，思科内容安全设备会定期将日志文件推送到远程计算机上的 FTP 服务器。订阅需要用户名、密码和远程计算机上的目标目录。日志文件基于配置的滚动更新进行传输。
SCP 推送	通过此类型的文件传输，思科内容安全设备会定期将日志文件推送到远程计算机上的 SCP 服务器。此方法要求远程计算机上的 SSH SCP 服务器使用 SSH2 协议。订阅需要用户名、 SSH 密钥和远程计算机上的目标目录。日志文件基于配置的滚动更新进行传输。
系统日志推送	通过此类型的文件传输，思科内容安全设备将日志邮件发送到远程系统日志服务器。此方法符合 RFC 3164 标准。必须为系统日志服务器提交主机名，并使用 UDP 或 TCP 进行日志传输。使用的端口是 514。可为日志选择设施。但是，下拉菜单中会预先选择与日志类型对应的默认值。只有基于文本的日志可以使用系统日志推送进行传输。

文件名和目录结构

AsyncOS 会根据日志订阅中指定的日志名称为每个日志订阅创建目录。目录中日志的文件名包含日志订阅中指定的文件名、表示日志文件开始时间的时间戳以及单字符状态代码。以下示例显示了目录和文件名规范：

`/<日志名称>/<日志文件名>.@<时间戳>.<状态代码>`

状态代码可以是 `.c`（表示 “当前”）或 `.s`（表示 “已保存”）。您只能传输具有已保存状态的日志文件。

日志滚动更新和传输安排

当创建日志订阅时，为日志滚动更新、传输旧文件以及创建新日志文件指定触发器条件。

可选择以下触发器：

- 文件大小
- Time
  - 以指定的时间间隔 （以秒、分钟、小时或者天为单位）

    当输入值时，请遵循屏幕上的示例。

    要输入复合间隔 （例如两个半小时），请遵循示例 `2h30m`。

    或
  - 在每天的指定时间

    或
  - 在一周中选定日期的指定时间

指定时间时，请使用 24 小时格式，例如晚上 11 点为 `23:00`。

要在一天中安排多个滚动更新时间，请使用逗号分隔时间。例如，要在午夜和中午滚动更新日志，请输入 `00:00, 12:00`

使用星号 (*) 作为通配符。
例如，要在每个整点和半点滚动更新日志，请输入 `*:00, *:30`

当达到指定的限制时 （或者如果配置了基于大小和时间的限制，则达到第一个限制时），系统会滚动更新日志文件。基于 FTP 轮询传输机制的日志订阅会创建文件，并将其存储在设备上的 FTP 目录中，直到检索这些文件或系统需要更多空间存储日志文件。

备注　如果在达到下一限制时正在进行滚动更新，则会跳过新的滚动更新。系统会记录一条错误，并发送警报。

日志文件中的时间戳

以下日志文件包括日志自身的开始和结束日期、 AsyncOS 版本和 GMT 时差 （在日志开头以秒为单位提供）：

- 邮件日志
- 安全列表/阻止列表日志
- 系统日志

默认情况下已启用日志

安全管理设备经过预配置，并且已启用以下日志订阅。

表 15-2　预配置的日志订阅

日志名称	日志类型	检索方法
cli_logs	CLI 审核日志	FTP 轮询
euq_logs	垃圾邮件隔离区日志	FTP 轮询
euqgui_logs	垃圾邮件隔离区 GUI 日志	FTP 轮询
gui_logs	HTTP 日志	FTP 轮询
mail_logs	文本邮件日志	FTP 轮询
reportd_logs	报告日志	FTP 轮询
reportqueryd_logs	报告查询日志	FTP 轮询
slbld_logs	安全列表/阻止列表日志	FTP 轮询
smad_logs	SMA 日志	FTP 轮询
system_logs	系统日志	FTP 轮询
trackerd_logs	跟踪日志	FTP 轮询

所有预配置日志订阅的日志记录级别都设置为 “信息 (Information)”。有关日志级别的详细信息，请参阅设置日志级别 （第 15-22 页）。

您可以根据应用的许可证密钥，配置其他日志订阅。有关创建和编辑日志订阅的信息，请参阅日志订阅 （第 15-21 页）。

日志类型

日志类型摘要

日志订阅可将日志类型与名称、日志记录级别和其他特征 （例如文件大小和目标信息）相关联。允许所有日志类型具有多个订阅，但配置历史记录日志除外。日志类型可决定在日志中记录的数据。在创建日志订阅时选择日志类型。有关详细信息，请参阅日志订阅 （第 15-21 页）。

AsyncOS 会生成以下日志类型：

表 15-3　　日志类型

日志类型	说明
身份验证日志	身份验证日志会记录成功的登录和不成功的登录尝试，这适用于在本地和外部经过身份验证的用户，以及通过 GUI 和 CLI 对安全管理设备的访问。 在调试和更详细的模式下，如果启用了外部验证，则所有 LDAP 查询都显示在这些日志中。
备份日志	备份日志自始至终记录备份过程。 SMA 日志中包含备份计划的相关信息。
CLI 审核日志	CLI 审核日志会记录系统中的所有 CLI 活动。
配置历史记录日志	配置历史记录日志会记录以下信息：对安全管理设备进行的更改以及何时进行的更改。每次用户提交更改时，都会创建一份新的配置历史记录日志。
FTP 服务器日志	FTP 日志会记录有关在界面上启用的 FTP 服务的信息。会记录连接详细信息和用户活动。

表 15-3　日志类型（续）

日志类型	说明
GUI 日志	GUI 日志包括 Web 界面、会话数据和用户访问的页面中的页面更新历史记录。您可以使用 gui_log 跟踪用户活动或调查用户在 GUI 中看到的错误。错误回溯通常在此日志中。 GUI 日志还包括有关 SMTP 事务的信息，例如有关从设备中通过邮件发送的计划报告的信息。
HTTP 日志	HTTP 日志会记录有关在界面上启用的 HTTP 和安全 HTTP 服务的信息。由于图形用户界面 (GUI) 通过 HTTP 访问，因此 HTTP 日志实质上等同于 CLI 审核日志的 GUI。系统会记录会话数据 （例如，新的会话和过期的会话），以及在 GUI 中访问的页面。
Haystack 日志	Haystack 日志会记录跟踪数据处理的 Web 事务。
文本邮件日志	文本邮件日志会记录有关邮件系统操作的信息 （例如，邮件接收、邮件传输尝试次数、打开和关闭连接、退回邮件等）。 有关何时在邮件日志中包含附件名称的重要信息，请参阅跟踪服务概述（第 6-1 页）。
LDAP调试日志	在 “系统管理 (System Administration)” > “LDAP” 中配置 LDAP 时，请使用这些日志调试问题。 例如，这些日志会记录点击 “测试服务器 (Test Server)” 和 “测试查询 (Test Queries)” 按钮的结果。 有关失败的 LDAP 身份验证的信息，请参阅身份验证日志。
NTP 日志	NTP 日志会记录设备与任何配置的网络时间协议 (NTP) 服务器之间的对话。有关配置 NTP 服务器的信息，请参阅配置系统时间 （第 14-37 页）。
报告日志	报告日志会记录与集中报告服务的进程相关的操作。
报告查询日志	报告查询日志会记录与设备上运行的报告查询相关的操作。
SMA 日志	SMA 日志会记录与常规安全管理设备进程相关的操作，不包括集中报告、集中跟踪和垃圾邮件隔离区服务的进程。 这些日志包含有关备份计划的信息。
SNMP 日志	SNMP 日志会记录与 SNMP 网络管理引擎相关的调试消息。在跟踪或调试模式下，这包括对安全管理设备的 SNMP 请求。
安全列表/阻止列表日志	安全列表/阻止列表日志会记录有关安全列表/阻止列表设置和数据库的数据。
垃圾邮件隔离区 GUI 日志	垃圾邮件隔离区 GUI 日志会记录与垃圾邮件隔离区 GUI 相关的操作，例如通过 GUI 进行隔离配置、最终用户身份验证和最终用户操作 （例如，释放邮件）。
垃圾邮件隔离区日志	垃圾邮件隔离区日志会记录与垃圾邮件隔离区进程相关的操作。
状态日志	状态日志会记录在 CLI 状态命令中找到的系统统计数据，包括 `status detail` 和 `dnsstatus`。记录期限使用 `logconfig` 中的 `setup` 子命令设置。状态日志中的每个计数器或速率都是自上次重置计数器起的值。
系统日志	系统日志会记录以下信息：启动信息、 DNS 状态信息和用户使用 `commit` 命令键入的备注。系统日志对于设备状态故障排除非常有用。
跟踪日志	跟踪日志会记录与跟踪服务进程相关的操作。跟踪日志是邮件日志的子集。

表 15-3　日志类型（续）

日志类型	说明
更新程序日志	有关服务更新的信息，例如时区更新。
升级日志	有关升级下载和安装的状态信息。

日志类型比较

表 15-4 总结了每种日志类型的特征。

表 15-4　日志类型比较

						包含					
	事务性	无状态	记录为文本	记录为二进制	信头日志记录	周期性状态信息	邮件接收信息	发送信息	单独的硬退回	单独的软退回	配置信息
身份验证日志	•		•								
备份日志	•		•								
CLI审核日志	•		•			•					
配置历史记录日志	•		•								•
FTP服务器日志	•		•			•					
HTTP日志	•		•			•					
Haystack 日志	•		•								
文本邮件日志	•		•		•	•	•	•	•	•	
LDAP调试日志	•		•								
NTP 日志	•		•			•					
报告日志	•		•			•					
路由查询日志	•		•			•					
SMA 日志	•		•			•					
SNMP 日志	•		•								
安全列表/阻止列表日志	•		•			•					
垃圾邮件隔离区 GUI	•		•			•					
垃圾邮件隔离区	•		•			•					
状态日志		•	•			•					
系统日志	•		•			•					
跟踪日志	•			•	•		•	•	•	•	
更新程序日志	•		•								

使用配置历史记录日志

配置历史记录日志包含一个配置文件以及一个额外部分，其中列出了用户名、有关用户在配置中的什么位置进行更改的说明以及用户在提交更改时输入的备注。每次用户提交更改时，都会创建一个包含更改后的配置文件的新日志。

示例

在本示例中，配置历史记录日志会显示用户 （管理员）向定义允许哪些本地用户登录系统的表添加了访客用户。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  配置更改生成的 XML。
  更改备注：添加了访客用户
  用户：admin
  配置描述为：
    该表定义了允许哪些本地用户登录系统。
  Product: M160 Messaging Gateway(tm) Appliance
  Model Number: M160
  Version: 6.7.0-231
  Serial Number: 000000000ABC-D000000
  Number of CPUs: 1
  Memory (GB): 4
  Current Time: Thu Mar 26 05:34:36 2009
  Feature "Centralized Configuration Manager": Quantity = 10, Time Remaining = "25 days"
  Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"
  Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"
  Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"
  Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"
-->
<config>
```

使用 CLI 审核日志

表 15-5 描述了在 CLI 审核日志中记录的统计数据。

表 15-5　CLI 审核日志统计数据

统计	说明
Timestamp	传输字节的时间。
PID	在其中输入命令的特定 CLI 会话的进程 ID。
消息	邮件包含输入的 CLI 命令、CLI 输出 （包括菜单、列表等）和显示的提示。

示例

在本示例中， CLI 审核日志会为 PID 16434 显示输入了以下 CLI 命令：`who, textconfig.`

```
Thu Sep 9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '
Thu Sep 9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername Login Time Idle Time Remote Host What\n
======== ========== ========= ========== ====\n
admin    Wed 11AM   3m 45s    10.1.3.14    tail\nadmin      02:32PM    0s
10.1.3.14   cli\nmail3.example.com> '
Thu Sep  9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n- NEW
- Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[]> '
```

使用 FTP 服务器日志

表 15-6 描述了在 FTP 服务器日志中记录的统计数据。

表 15-6　FTP 服务器日志统计数据

统计	说明
Timestamp	传输字节的时间。
ID	连接 ID。每个 FTP 连接的单独的 ID。
消息	日志条目的邮件部分可以包含日志文件状态信息或 FTP 连接信息 （登录、上传、下载、注销等）。

示例

在本示例中， FTP 服务器日志会记录连接 (ID:1)。显示了传入连接的 IP 地址，以及活动（上传和下载文件）和注销。

```
Wed Sep  8 18:03:06 2004 Info: Begin Logfile
Wed Sep  8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21
Wed Sep  8 18:03:06 2004 Info: Time offset from UTC: 0 seconds
Wed Sep  8 18:03:06 2004 Info: System is coming up
Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds
Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86
Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS
Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes
Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes
Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

使用 HTTP 日志

表 15-7 描述了在 HTTP 日志中记录的统计数据

表 15-7　在 HTTP 日志中记录的统计数据

统计	说明
Timestamp	传输字节的时间。
ID	会话 ID。
req	计算机连接的 IP 地址。
user	用户连接的用户名。
消息	有关所执行操作的信息。可能包括 GET 或 POST 命令或系统状态等等。

示例

在本示例中， HTTP 日志显示管理员用户与 GUI 的交互 （例如，运行系统安装向导）。

```
Wed Sep 8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port
443
Wed Sep 8 18:17:23 2004 Info: http service listening on 192.168.0.1:80
Wed Sep 8 18:17:23 2004 Info: https service listening on 192.168.0.1:443
Wed Sep 8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds
Wed Sep 8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST
/system_administration/system_setup_wizard HTTP/1.1 303
Wed Sep 8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/system_administration/ssw_done HTTP/1.1 200
Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
```

```
/monitor/incoming_mail_overview HTTP/1.1 200
Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190
HTTP/1.1 200
Wed Sep 8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=19
0 HTTP/1.1 200
Wed Sep 8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/quarantines HTTP/1.1 200
```

使用垃圾邮件隔离区日志

表 15-8 描述了在垃圾邮件隔离区日志中记录的统计数据。

表 15-8　　垃圾邮件隔离区日志统计数据

统计	说明
Timestamp	传输字节的时间。
消息	邮件包含所执行的操作 （隔离邮件、从隔离区释放等）。

示例

在本示例中，日志显示了从隔离区释放到 admin@example.com 的两个邮件 （MID 8298624 和 MID 8298625）。

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

使用垃圾邮件隔离区 GUI 日志

表 15-9 显示在垃圾邮件隔离区 GUI 日志中记录的统计数据。

表 15-9　　垃圾邮件隔离区 GUI 日志统计数据

统计	说明
Timestamp	传输字节的时间。
消息	邮件包含所执行的操作，包括用户身份验证等。

示例

在此示例中，日志显示了成功的身份验证、登录和注销：

表 15-10　　垃圾邮件隔离区 GUI 日志示例

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82
Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83
Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin
Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228
Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228
Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

使用文本邮件日志

这些日志包含有关邮件接收、邮件传输和退回的详细信息。此外，每分钟还会将状态信息写入邮件日志。这些日志是非常有用的信息来源，可用于了解特定邮件的传输及分析系统性能。

这些日志无需任何特殊配置。但是，必须正确配置系统才能查看附件名称，而且不一定会记录附件名称。有关特定信息，请参阅跟踪服务概述 （第 6-1 页）。

表 15-11 显示了文本邮件日志中显示的信息。

表 15-11　　文本邮件日志统计数据

统计	说明
ICID	注入连接 ID。这是用于系统单个 SMTP 连接的数字标识符。可以通过一个到系统的 SMTP 连接发送单个邮件或数千个单独的邮件。
DCID	传输连接 ID。这是用于到另一台服务器的单个 SMTP 连接的数字标识符，可传送的邮件数从一个到数千个不等，而且每个数字标识符都具有在单个邮件传输中提供的部分或全部 RID。
RCID	RPC 连接 ID。这是用于到垃圾邮件隔离区的单个 RPC 连接的数字标识符。当向/从垃圾邮件隔离区进行发送时，它用于跟踪邮件。
MID	邮件 ID：当邮件流经日志时，该 ID 用于跟踪邮件。
RID	收件人 ID。每个邮件收件人都会被分配一个 ID。
新的	启动新连接。
开始	已开始新的邮件。

文本邮件日志示例

使用以下示例作为解释日志文件的指南。

备注　日志文件中的各个行*未*编号。在此处对它们编号仅用作示例。

表 15-12　文本邮件日志详细信息

```
1   Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management
    (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes
2   Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5
3   Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From:
    <sender@remotehost.com>
4   Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To:
    <mary@yourdomain.com>
5   Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from
    <sender@remotehost.com>
6   Mon Apr 17 19:59:59 2003 Info: ICID 5 close
7   Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface
    192.168.42.42 address 10.5.3.25
8   Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID
    [0]
9   Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]
10  Mon Mar 31 20:11:03 2003 Info: DCID 8 close
```

使用表 15-13 作为阅读上一日志文件的指南。

表 15-13　文本邮件日志详细信息示例

线路号	说明
1	发起到系统的新连接并分配注入 ID (ICID) “5”。该连接在管理 IP 接口上收到，并从地址为 10.1.1.209 的远程主机上发起。
2	从客户端发出了 MAIL FROM 命令后，为该邮件分配邮件 ID (MID) “6”。
3	已识别并接受发件人地址。
4	识别收件人，并为其分配收件人 ID (RID) “0”。
5	已接受 MID 5，写入磁盘，并确认。
6	接收成功，并且关闭接收连接。
7	邮件传输进程开始。系统为其分配了从 192.168.42.42 到 10.5.3.25 的传输连接 ID (DCID) “8”。
8	开始向 RID “0”传输邮件。
9	MID 6 成功传输到 RID “0”。
10	传输连接关闭。

文本邮件日志条目示例

以下示例根据各种情况显示日志条目。

邮件接收

将一个邮件注入设备中的单个收件人。已成功传输该邮件。

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com
(1.2.3.4) address 2.3.4.5 reverse dns host unknown verified no
Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None
Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970
Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>
Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID '<37gva9$5uvbhe@mail.example.com>'
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'
Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>
Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative
Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery
Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4
Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]
Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close
Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0]
[('X-SBRS', 'None')]
Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery
Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

成功邮件传输示例

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110
Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]
Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]
Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

不成功的邮件传输 （硬退回）

将具有两个收件人的邮件注入设备中。传输过程中，目标主机返回 5*XX* 错误，这表示无法将邮件传输到任何一个收件人。设备会通知发件人，并从队列中删除收件人。

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address 64.81.204.225
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
error ('550', ['<george@yourdomain.com>...Relaying denied']) []
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
error ('550', ['<jane@yourdomain.com>...Relaying denied']) []
Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

具有最终成功传输的软退回示例

将邮件注入设备中。在第一次尝试传输时，邮件被软退回并且排队等候将来传输。在第二次尝试中，成功传输了该邮件。

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
error ('466', ['Mailbox temporarily full.'])[]
Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23 2003
Mon Mar 31 20:01:28 2003 Info: DCID 5 close
Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113
Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

邮件扫描结果 (scanconfig)

当使用 `scanconfig` 命令确定行为时，如果邮件无法分解为其组成部分 （删除附件时），会出现以下提示：

```
If a message could not be deconstructed into its component parts in order to remove
specified attachments, the system should:
1.投递
2.退回
3.丢弃
[3]>
```

以下是邮件日志中的相关标示：

scanconfig 设置为在无法分解邮件时进行传输。

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>
Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'
Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line seen
before first header
Tue Aug 3 16:36:29 2004 Info: ICID 44784 close
Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'
Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus
Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

scanconfig 设置为在无法分解邮件时丢弃。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line seen
before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

包含附件的邮件

在本示例中，配置了使用 “邮件正文包含”条件的内容过滤器以便识别附件名称：

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes
Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0
Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

请注意，三个附件中的第二附件采用 Unicode 格式。在无法显示 Unicode 的终端上，这些附件以引用的可打印格式显示。

生成或重写的邮件

一些操作，如重写/重定向操作 （`alt-rcpt-to` 过滤器、反垃圾邮件 rcpt 重写、`bcc()` 操作、防病毒重定向等）会创建新的邮件。当查看日志时，可能需要检查结果以及添加其他 MID，而且可能需要添加 DCID。可能为以下这样的条目：

```
Tue Jun 1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
```

或者：

```
Tue Jan 6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam
Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter
'testfilt'
```

备注　在日志中的行后可能会显示 “重写”的条目，以指示使用新的 MID。

将邮件发送到垃圾邮件隔离区

将邮件发送到隔离区时，邮件日志使用 RCID （RPC 连接 ID）来标识 RPC 连接，从而跟踪到/从隔离区的移动。在以下邮件日志中，一个邮件被标记为垃圾邮件，并发送到垃圾邮件隔离区：

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
‘<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make it
a reality'
```

```
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect
Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local Spam
Quarantine
Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877
Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877
Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

使用 NTP 日志

表 15-14 显示在 NTP 日志中记录的统计数据。

表 15-14　在 NTP 日志中记录的统计数据

统计	说明
Timestamp	传输字节的时间。
消息	邮件包含对服务器的简单网络时间协议 (SNTP) 查询或是 adjust: 邮件。

示例

在本示例中， NTP 日志显示轮询 NTP 主机两次的设备。

```
Thu Sep 9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652
Thu Sep 9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096
Thu Sep 9 8:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152
Thu Sep 9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

使用报告日志

表 15-15 显示在报告日志中记录的统计数据。

表 15-15　报告日志统计数据

统计	说明
Timestamp	传输字节的时间。
消息	邮件包含所执行的操作，包括用户身份验证等。

示例

在本示例中，报告日志显示在信息日志级别设置的设备。

```
Wed Oct 3 13:39:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:39:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40
Wed Oct 3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%).Not found: 1692
Wed Oct 3 13:40:53 2007 Info: Period hour using 36800 (KB)
Wed Oct 3 13:40:53 2007 Info: Period day using 2768 (KB)
Wed Oct 3 13:40:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:40:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds
Wed Oct 3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41
```

```
Wed Oct 3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%).Not found: 1692
Wed Oct 3 13:41:53 2007 Info: Period hour using 36800 (KB)
Wed Oct 3 13:41:53 2007 Info: Period day using 2768 (KB)
Wed Oct 3 13:41:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:41:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
```

使用报告查询日志

表 15-16 显示在报告查询日志中记录的统计数据。

表 15-16　报告查询日志统计数据

统计	说明
Timestamp	传输字节的时间。
消息	邮件包含所执行的操作，包括用户身份验证等。

示例

在本示例中，报告查询日志显示从 2007 年 8 月 29 日到 10 月 10 日期间运行每日持续邮件流量查询的设备。

```
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804479.
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804480.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610228.
Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTEN
T_FILTER', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECI
PIENTS_PROCESSED'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
with key constraints
 None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from 0
to 2 sort_ascendin
g=False.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610229.
Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
TOTAL_HARD_BOUNCES',    'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMM
ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range 2007-08-29 to
2007-10-01 with key constra
ints None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning
results from 0 to 2 sort
_ascending=False.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

使用安全列表/阻止列表日志

表 15-17 显示在安全列表/阻止列表日志中记录的统计数据。

表 15-17　安全列表/阻止列表日志统计数据

统计	说明
Timestamp	传输字节的时间。
消息	邮件包含所执行的操作，包括用户身份验证等。

示例

在本示例中，安全列表/阻止列表日志显示每两隔小时创建数据库快照的设备。它还显示何时将发件人添加到数据库中。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC: 10800
seconds Fri Sep 28 14:22:33 2007 Info: System is coming up.
Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.
.........................
Mon Oct 1 14:16:09 2007 Info: SLBL: The database snapshot has been created.
Mon Oct 1 14:37:39 2007 Info: SLBL: The database snapshot has been created.
Mon Oct 1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct 1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct 1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

使用 SMA 日志

表 15-18 显示在 SMA 日志中记录的统计数据。

表 15-18　SMA 日志统计数据

统计	说明
Timestamp	传输字节的时间。
消息	邮件包含所执行的操作，包括用户身份验证等。

示例

在本示例中， SMA 日志显示从邮件安全设备下载跟踪文件的集中跟踪服务，并且显示从邮件安全设备下载报告文件的集中报告服务。

```
Wed Oct 3 13:26:39 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.17 - /export/tracki
ng/tracking.@20071003T202244Z_20071003T202544Z.s
Wed Oct 3 13:28:11 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.15 - /export/tracki
ng/tracking.@20071003T202443Z_20071003T202743Z.s
Wed Oct 3 13:28:46 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.17 - /export/tracki
ng/tracking.@20071003T202544Z_20071003T202844Z.s
Wed Oct 3 13:31:27 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.15 - /export/tracki
ng/tracking.@20071003T202743Z_20071003T203043Z.s
```

```
Wed Oct 3 13:31:28 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from
172.29.0.15 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.000F1F6ECA7C-2RWDB51.v1.tgz
Wed Oct 3 13:31:53 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.17 - /export/tracki
ng/tracking.@20071003T202844Z_20071003T203144Z.s
Wed Oct 3 13:32:31 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from
172.29.0.17 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.0019B9B316E4-JZ41PC1.v1.tgz
Wed Oct 3 13:34:40 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from
172.29.0.15 - /export/tracki
ng/tracking.@20071003T203043Z_20071003T203343Z.s
```

使用状态日志

状态日志会记录在 CLI 状态命令中找到的系统统计数据，包括 `status`、`status detail` 和 `dnsstatus`。记录期限使用 `logconfig` 中的 `setup` 子命令设置。状态日志中的每个计数器或速率都是自上次重置计数器起的值。

表 15-19　状态日志统计数据

统计	说明
CPULd	CPU 利用率。
DskIO	硬盘 I/O 使用率。
RAMUtil	内存利用率。
QKUsd	使用的队列容量 (KB)。
QKFre	可用队列容量 (KB)。
CrtMID	邮件 ID (MID)。
CrtICID	注入连接 ID (ICID)。
CRTDCID	传输连接 ID (DCID)。
InjMsg	注入的邮件。
InjRcp	注入的收件人。
GenBncRcp	生成的退回收件人。
RejRcp	拒绝的收件人。
DrpMsg	删除的邮件。
SftBncEvnt	软退回的事件。
CmpRcp	已完成收件人。
HrdBncRcp	硬退回收件人。
DnsHrdBnc	DNS 硬退回。
5XXHrdBnc	5XX 硬退回。
FltrHrdBnc	过滤硬退回。
ExpHrdBnc	过期的硬退回。
OtrHrdBnc	其他硬退回。
DlvRcp	已传输的收件人。
DelRcp	已删除的收件人。

表 15-19　状态日志统计数据 （续）

统计	说明
GlbUnsbHt	全局取消订阅命中数。
ActvRcp	正在处理的收件人。
UnatmptRcp	未尝试发送的收件人。
AtmptRcp	已尝试发送的收件人。
CrtCncIn	当前入站连接数。
CrtCncOut	当前出站连接数。
DnsReq	DNS 请求数。
NetReq	网络请求数。
CchHit	缓存命中数。
CchMis	缓存丢失数。
CchEct	缓存排斥数。
CchExp	缓存过期。
CPUTTm	应用所使用的总 CPU 时间。
CPUETm	应用开始后所经过的时间。
MaxIO	邮件进程的每秒最大磁盘 I/O 操作数。
RamUsd	分配的内存 (B)。
SwIn	换入内存。
SwOut	换出内存。
SwPgIn	调入内存。
SwPgOut	调出内存。
MMLen	系统中的总邮件数。
DstInMem	内存中的目标对象数。
ResCon	资源节省 tarpit 值。由于系统负载繁重，延迟该秒数接受传入邮件。
WorkQ	当前在工作队列中的邮件数量。
QuarMsgs	系统隔离区中的单独邮件数量 （存在于多个隔离区中的邮件只计算一次）。
QuarQKUsd	系统隔离区邮件占用的空间 (KB)。
LogUsd	日志分区使用百分比。
CASELd	CASE 扫描使用的 CPU 百分比。
TotalLd	使用的 CPU 总量。
LogAvail	可用于日志文件的磁盘空间量。
EuQ	垃圾邮件隔离区中的邮件数量。
EuqRls	垃圾邮件隔离区释放队列中的邮件数量。

示例

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp 6318
DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15 FltrHrdBnc 0
ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0
CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis 504791 CchEct
15395 CchExp 55085 CPUTTm 228 CPUETm 181380 MaxIO 350 RAMUsd 21528056 MMLen 0 DstInMem 4
ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd 0 CASELd 3 TotalLd 3 LogAvail
17G EuQ 0 EuqRls 0
```

使用系统日志

表 15-20 显示在系统日志中记录的统计数据。

表 15-20　系统日志统计数据

统计	说明
Timestamp	传输字节的时间。
消息	记录的事件。

示例

在本示例中，系统日志显示一些提交条目，包括发出提交和输入备注的用户的名称。

```
Wed Sep 8 18:02:45 2004 Info: Version: 6.0.0-206 SN: XXXXXXXXXXXX-XXX
Wed Sep 8 18:02:45 2004 Info: Time offset from UTC: 0 seconds
Wed Sep 8 18:02:45 2004 Info: System is coming up
Wed Sep 8 18:02:49 2004 Info: bootstrapping DNS cache
Wed Sep 8 18:02:49 2004 Info: DNS cache bootstrapped
Wed Sep 8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Password
Wed Sep 8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW
Thu Sep 9 8:49:27 2004 Info: Time offset from UTC: -25200 seconds
Thu Sep 9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI log
for examples
Thu Sep 9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.
```

了解跟踪日志

跟踪日志记录有关 AsyncOS 的邮件操作的信息。日志邮件是邮件日志中记录的邮件的子集。

跟踪日志由邮件跟踪组件用于构建跟踪数据库。由于构建数据库的过程中会使用日志文件，因此跟踪日志是动态的。跟踪日志中的信息不是供人类阅读或分析的。

跟踪日志以二进制格式记录和传输，以提高资源效率。该信息以符合逻辑的方式布置，并且使用思科提供的实用程序进行转换后，可供人类进行阅读。通过以下网址可以找到这些转换工具：
`http://tinyurl.com/3c5l8r`.

日志订阅

配置日志订阅

日志订阅会创建在思科内容安全设备或远程位置存储的单个日志文件。系统会对日志订阅进行推送 （传输到另一台计算机）或轮询 （从设备检索）。通常，日志订阅具有以下属性：

表 15-21　日志文件属性

属性	描述
日志类型	定义记录的信息类型和日志订阅的格式。有关详细信息，请参阅日志类型摘要 （第 15-4 页）。
名称	提供日志订阅的描述性名称以供将来参考。
日志文件名	写入磁盘时使用的文件实际名称。如果系统包括多种内容安全设备，则使用独特的日志文件名来标识生成日志文件的设备。
根据文件大小滚动更新	在进行滚动更新之前，文件可以达到的最大大小。
根据时间滚动更新	根据时间来滚动更新日志文件。请参阅日志滚动更新和传输安排 （第 15-2 页）中的选项。
日志级别	每个日志订阅的详细级别。
检索方法	用于从设备传输日志文件的方法。

使用 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “日志订阅 (Log Subscriptions)” 页面 （或 CLI 中的 `logconfig` 命令）可以配置日志订阅。系统会提示输入日志类型，如日志类型摘要 （第 15-4 页）中所示。对于大多数日志类型，还需要选择日志订阅的 *日志级别*。

备注　仅配置历史记录日志：如果希望从配置历史记录日志中加载配置，请注意不能加载包含已屏蔽的密码的配置。在 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “日志订阅 (Log Subscriptions)” 页面中，当系统提示是否要在日志中包含密码时，请选择 “是 (Yes)”。如果使用 CLI 中的 `logconfig` 命令，请根据提示键入 `y`。

设置日志级别

日志级别决定日志中提供的信息量。日志可以是五种级别中的一种。与简略的日志级别设置相比，一个详细的日志级别设置会创建更大的日志文件，并且对系统性能产生更大的影响。一个详细的日志级别设置包括缩略日志级别设置中包含的所有消息，此外还包括其他消息。随着详细级别的提高，系统性能会下降。

备注　您可以为每种日志类型指定不同的日志记录级别。

表 15-22　日志级别

日志级别	说明
严重	仅记录错误。这是最缩略的日志级别设置。在此日志级别，无法监控性能和重要设备活动；但是，日志文件不会像在详细日志级别那样快速地达到最大大小。此日志级别类似于 “警报”系统日志级别。
警告	将会记录所有系统错误和警告。在此日志级别，无法监控性能和重要设备活动。日志文件达到最大大小的速度快于 “严重”日志级别。此日志级别类似于 “警告”系统日志级别。
信息	记录系统每一秒钟进行的操作。例如，记录打开的连接和传输尝试。该信息级别是推荐的日志级别设置。此日志级别类似于 “信息”系统日志级别。
调试	记录的信息比 “信息”日志级别更加详细。在排除错误时，可使用 “调试”日志级别。可临时使用该设置，然后返回默认级别。此日志级别类似于 “调试”系统日志级别。
跟踪	记录所有可用的信息。建议仅将 “跟踪”日志级别供开发人员使用。使用此级别会造成严重的系统性能下降，建议不要使用。此日志级别类似于 “调试”系统日志级别。

在 GUI 中创建日志订阅

操作步骤

步骤 1　在 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “日志订阅 (Log Subscriptions)”页面中，点击**添加日志订阅 (Add Log Subscription)**。

步骤 2　选择日志类型并输入日志名称 （日志目录），以及日志文件自身的名称。

步骤 3　如果适用，请指定最大文件大小。

步骤 4　如果适用，请指定滚动更新日志的日期、时间或时间间隔。有关详细信息，请参阅日志滚动更新和传输安排 （第 15-2 页）。

步骤 5　如果适用，请指定日志级别。

步骤 6　（仅配置历史记录日志）选择是否在日志中包括密码。

注　您不能加载包含已屏蔽密码的配置。如果您希望从配置历史记录日志中加载配置，请选择 “是 (Yes)”以在日志中包括密码。

步骤 7　配置日志检索方法。

步骤 8　提交并确认更改。

编辑日志订阅

操作步骤

步骤 1　在 “日志订阅 (Log Subscriptions)”页面上的 “日志名称 (Log Name)”列中，点击日志的名称。

步骤 2　更新日志订阅。

步骤 3　提交并确认更改。

配置日志记录的全局设置

系统会在文本邮件日志和状态日志中定期记录系统指标。使用 “日志订阅 (Log Subscriptions)”页面 “全局设置 (Global Settings)”部分中的**编辑设置 (Edit Settings)** 按钮 （或 CLI 中的 `logconfig -> setup` 命令）配置：

- 系统在日志记录指标之间等待的时长 （以秒为单位）
- 是否记录邮件 ID 信头
- 是否记录远程响应状态代码
- 是否记录原始邮件的主题信头
- 应该为每个邮件记录的信头

所有思科内容安全设备日志可以有选择地包括以下三项：

- 邮件 ID：如果配置了此选项，则每个邮件都会记录其邮件 ID 信头 （如果有）。此邮件 ID 可能来自收到的邮件，或可能已由 AsyncOS 生成。例如：

  ```
  Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
  ```

- 远程响应：如果配置了此选项，则每个邮件都会记录其远程响应状态代码 （如果有）。例如：

  ```
  Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
  ```

  远程响应字符串是在传输 SMTP 对话期间响应 DATA 命令后收到的人类可读的文本。在本示例中，连接主机发出数据命令后的远程响应是 “queued as 9C8B425DA7”。

  ```
  [...]
  250 ok hostname
  250 Ok: queued as 9C8B425DA7
  ```

  空格、标点符号以及在 250 情况下出现的 “OK”字符会从字符串开头剥离。仅空格会从字符串结尾剥离。例如，默认情况下，思科内容安全设备使用以下字符串来响应 DATA 命令：`250 Ok: Message MID accepted`。因此，如果远程主机是另一个思科内容安全设备，则会记录 “Message MID accepted”。

- 原始主题信头：启用此选项后，会在日志中包含每个邮件的原始主题信头。

  ```
  Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2
  Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>
  Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>
  Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'
  Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
  ```

日志记录邮件信头

有时，当邮件通过系统时，有必要记录邮件信头是否存在及其内容。可在 “日志订阅全局设置 (Log Subscriptions Global Settings)”页面上（或通过 CLI 中的 `logconfig -> logheaders` 子命令）指定要记录的信头。设备会在文本邮件日志和跟踪日志中记录指定的邮件信头。如果信头存在，则系统会记录信头的名称和值。如果信头不存在，则不在日志中记录任何内容。

备注　在处理要记录的邮件的过程中，系统会评估存在于邮件中的所有信头，不管是否为日志记录指定了信头都是如此。

备注　SMTP 协议的 RFC 位于 `http://www.faqs.org/rfcs/rfc2821.html`，其定义了用户定义的信头。

备注　如果已通过 `logheaders` 命令配置了要记录的信头，则在传输信息之后将显示信头信息：

表 15-23　Log Headers

信头名称	信头的名称
Value	所记录的信头的内容

例如，指定 “date, x-subject”作为要记录的信头会导致在邮件日志中显示以下行：

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0] [('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

使用 GUI 配置日志记录的全局设置

操作步骤

步骤 1　点击 “日志订阅 (Log Subscriptions)”页面 “全局设置 (Global Settings)”部分中的**编辑设置 (Edit Settings)** 按钮。

步骤 2　指定系统指标频率、是否在邮件日志中包含邮件 ID 信头、是否包含远程响应以及是否包含每个邮件的原始主题信头。

有关这些设置的信息，请参阅配置日志记录的全局设置 （第 15-23 页）。

步骤 3　输入要在日志中包含的任何其他信头。用逗号分隔每个条目。

步骤 4　提交并确认更改。

滚动更新日志订阅

当 AsyncOS 滚动更新日志文件时，会：

- 使用滚动更新时间戳创建新的日志文件，并使用字母 “c” 作为扩展名指示文件为当前文件
- 将当前日志文件重命名为将字母 “s” 作为扩展名，以指示文件已保存
- 将新保存的日志文件传输到一台远程主机 （如果基于推送）
- 从同一订阅传输以前不成功的日志文件 （如果基于推送）
- 如果超过可保存的文件总数 （如果基于轮询），则删除日志订阅中最旧的文件

相关主题

- 滚动更新日志订阅中的日志 （第 15-25 页）
- 立即使用 GUI 滚动更新日志 （第 15-25 页）
- 通过 CLI 立即滚动更新日志 （第 15-25 页）

滚动更新日志订阅中的日志

请参阅日志滚动更新和传输安排 （第 15-2 页）。

立即使用 GUI 滚动更新日志

操作步骤

步骤 1　在 “日志订阅 (Log Subscriptions)” 页面中，选中要滚动更新的日志右侧的复选框。

步骤 2　或者，通过选中**全部 (All)** 复选框选择所有日志进行滚动更新。

步骤 3　点击**立即滚动更新 (Rollover Now)** 按钮。

通过 CLI 立即滚动更新日志

使用 `rollovernow` 命令一次滚动更新所有日志文件，或从列表中选择特定日志文件。

在 GUI 中查看最近的日志条目

通过 GUI，可在 “日志订阅 (Log Subscriptions)” 页面上表格的 “日志文件 (Log Subscriptions)” 列中点击日志订阅，以查看日志文件。点击指向日志订阅的链接时，系统会提示输入密码。然后会显示该订阅的日志文件列表。可以点击其中一个日志文件以在浏览器中查看它，或者将其保存到磁盘。必须在管理界面上启用 FTP 服务才能在 GUI 中查看日志。

查看日志中的最新条目 （tail 命令）

AsyncOS 支持 tail 命令，该命令会显示在设备上配置的日志的最新条目。发出 tail 命令并选择当前配置的日志的编号以查看它。按 Ctrl-C 可退出 tail 命令。

备注 使用 tail 命令无法查看配置历史记录日志。必须使用 FTP 或 SCP。

示例

在以下示例中， tail 命令用于查看系统日志。 tail 命令还接受参数形式的日志名称，例如：
tail system_logs

```
Welcome to the M600 Messaging Gateway(tm) Appliance
example.srv> tail

Currently configured logs:
1. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
2. "euq_logs" Type: " Spam Quarantine Logs" Retrieval: FTP Poll
3. "euqgui_logs" Type: "Spam Quarantine GUI Logs" Retrieval: FTP Poll
4. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
5. "mail_logs" Type: "Text Mail Logs" Retrieval: FTP Poll
6. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
7. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
8. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
9. "smad_logs" Type: "SMA Logs" Retrieval: FTP Poll
10. "system_logs" Type: "System Logs" Retrieval: FTP Poll
11. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
Enter the number of the log you wish to tail.
[]> 10

Press Ctrl-C to stop.
Thu Sep 27 00:18:56 2007 Info: Begin Logfile
Thu Sep 27 00:18:56 2007 Info: Version: 6.0.0-422 SN: 001143583D73-FT9GP61
Thu Sep 27 00:18:56 2007 Info: Time offset from UTC: 0 seconds
Thu Sep 27 00:18:47 2007 Info: System is coming up.
Thu Sep 27 00:23:05 2007 Warning: DNS query network error '[Errno 64] Host is down' to
'172.16.0.3' looking up 'downloads.cisco.com'
Fri Sep 28 22:20:08 2007 Info: PID 688: User admin commit changes:
Fri Sep 28 23:06:15 2007 Info: PID 688: User admin commit changes:
^Cexample.srv>
.
```

配置主机密钥

将日志从思科内容安全设备推送到其他服务器时，使用 logconfig -> hostkeyconfig 子命令管理与 SSH 配合使用的主机密钥。SSH 服务器必须具有一对主机密钥：一个私钥和一个公钥。私有主机密钥位于 SSH 服务器上，不能由远程计算机读取。公共主机密钥可分配给需要与 SSH 服务器交互的任何客户端计算机。

备注 要管理用户密钥，请参阅邮件安全设备用户指南或在线帮助中的 “管理安全外壳 (SSH) 密钥”。

hostkeyconfig 子命令会执行以下功能：

表 15-24　管理主机密钥 - 子命令列表

命令	描述
新的	添加新密钥。
Edit	修改现有密钥。
Delete	删除现有密钥。
扫描	自动下载主机密钥。
打印	定义密钥。
主持	显示系统主机密钥。这是要放置在远程系统的 “known_hosts”文件中的值。
指纹	显示系统主机密钥指纹。
User	显示将日志推送到远程计算机的系统帐户的公共密钥。这是设置 SCP 推送订阅时显示的密钥。这是要放置在远程系统的 “authorized_keys”文件中的值。

示例

在下面的示例中，命令会扫描主机密钥并为主机添加它们：

```
mail3.example.com> logconfig

Currently configured logs:
[ list of logs ]

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> hostkeyconfig

Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]

Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> scan

Please enter the host or IP address to lookup.
[]> mail3.example.com

Choose the ssh protocol type:
1. SSH2:rsa
2. SSH2:dsa
3. 全部
[3]>
```

```
SSH2:dsa
mail3.example.com ssh-dss
[ key displayed ]

SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed ]

Add the preceding host key(s) for mail3.example.com?[Y]>

Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]
2. mail3.example.com ssh-rsa [ key displayed ]
3. mail3.example.com 1024 35 [ key displayed ]

Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>

Currently configured logs:
[ list of configured logs ]

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>

mail3.example.com> commit
```

故障排除

收集系统信息

有关如何获取设备及其状态的信息 （包括序列号），请参阅第 10 章 “监控系统状态”。

排除功能设置问题

如果难以成功配置某项功能，请参阅针对每项功能必须完成的任务摘要。其中包括指向每项功能具体信息的链接。

- 设置集中 Web 报告和跟踪 （第 5-2 页）
- 设置集中邮件报告 （第 4-2 页）
- 设置集中邮件跟踪 （第 6-2 页）
- 设置集中式垃圾邮件隔离区 （第 7-2 页）
- 集中策略、病毒和爆发隔离区 （第 8-3 页）
- 设置主配置以集中管理网络安全设备 （第 9-2 页）

常规故障排除资源

常规故障排除资源包括：

- 最近警报。请参阅查看最近的警报 （第 14-29 页）。
- 日志文件。请参阅第 15 章 “日志记录”。
- 版本说明，包括 “文档更新 (Documentation Updates)” 部分。请参阅文档 （第 E-2 页）。
- 思科缺陷搜索工具 （有关访问说明，请参阅版本说明）。
- 知识库文章 （技术说明）（第 E-3 页）。
- 思科支持社区 （第 E-3 页）。

排除托管设备中的性能问题

要在遇到性能问题时确定系统的哪些部分使用的资源最多，可以查看所有托管 （邮件或网络安全）设备及每台托管设备的系统容量报告。关于邮件安全设备，请参阅系统容量页面 （第 4-29 页）。关于网络安全设备，请参阅系统容量页面 （第 5-27 页）。

解决特定功能的相关问题

另请参阅排除功能设置问题 （第 16-1 页）。

网络安全相关问题

- 对所有报告进行故障排除 （第 3-11 页）
- 故障排除 Web 报告和跟踪 （第 5-41 页）
- 解决配置管理问题 （第 9-21 页）
- 网络安全设备上的设置也会导致功能相关的问题。请参阅文档 （第 E-2 页）所指定位置中您所用版本的版本说明和在线帮助或用户指南

邮件安全相关问题

- 对所有报告进行故障排除 （第 3-11 页）
- 邮件报告故障排除 （第 4-39 页）
- 邮件跟踪故障排除 （第 6-9 页）
- 垃圾邮件隔离区功能故障排除 （第 7-24 页）
- 排除集中策略隔离区的故障 （第 8-22 页）
- 邮件安全设备上的设置也会导致功能相关的问题。请参阅文档 （第 E-2 页）所指定位置中您所用版本的版本说明和在线帮助或用户指南。

常规问题

- 如果您最近进行了升级，而在线帮助似乎过时或从中找不到有关新功能的信息，请清除浏览器缓存，然后重新打开浏览器窗口。
- 如果同时使用多个浏览器窗口或选项卡，使用 Web 界面配置设置时可能会发生意外行为。
- 排除管理用户访问故障 （第 13-24 页）。

使用技术支持

从设备新建或更新支持案例

可以使用此方法联系思科 TAC 或自己的支持人员。

准备工作

如果想要联系思科 TAC：

- 如果问题紧急，请勿使用此方法。请改为使用客户支持 （第 E-4 页）中列出的方法之一与支持人员联系。
- 考虑获取帮助的其他选项：
  - 知识库文章 （技术说明）（第 E-3 页）
  - 思科支持社区 （第 E-3 页）
- 使用此程序开设支持案例时，系统会将设备配置文件发送给思科客户支持人员。如果不希望发送设备配置，可以使用其他方法与客户支持人员联系。
- 设备必须连接到互联网，并可以发送邮件。
- 如果要发送有关现有案例的信息，请确保拥有案例编号。

操作步骤

步骤 1　登录到设备。

步骤 2　依次选择**帮助和支持 (Help and Support) > 联系技术支持 (Contact Technical Support)**。

步骤 3　确定支持请求的收件人：

将请求发送给思科 TAC	选中**思科**技术支持 (Cisco Technical Support) 复选框。
仅将请求发送给内部支持部门	• 取消选中**思科技术支持 (Cisco Technical Support)** 复选框。 • 输入支持部门的邮件地址。
（可选）添加其他收件人	输入邮件地址。

步骤 4　完成表格。

步骤 5　点击**发送**。

获取虚拟设备支持

如果归档了一个思科内容安全虚拟设备支持案例，则必须提供您的合同编号和产品标识代码 (PID)。您可以通过引用采购订单或下表，基于虚拟设备上运行的软件许可证标识 PID：

功能	PID	说明
所有集中网络安全功能	SMA-WMGT-LIC=	—
所有集中邮件安全功能	SMA-EMGT-LIC=	

启用思科技术支持人员远程访问

只有思科客户帮助部门才能使用这些方法访问您的设备。

- 启用远程访问连接互联网的设备 （第 16-4 页）
- 启用远程访问未直接连接互联网的设备 （第 16-5 页）
- 禁用技术支持隧道 （第 16-5 页）
- 禁用远程访问 （第 16-5 页）
- 检查支持连接的状态 （第 16-6 页）

启用远程访问连接互联网的设备

支持部门可通过此程序在设备与 `upgrades.ironport.com` 服务器之间创建的 SSH 隧道访问设备。

准备工作

标识可通过互联网访问的端口。默认为端口 25，该端口在大多数环境中均可工作。大多数防火墙配置都允许通过此端口进行的连接。

操作步骤

步骤 1　登录到设备。

步骤 2　在 GUI 窗口的右上角，依次选择**帮助和支持 (Help and Support) > 远程访问 (Remote Access)**。

步骤 3　点击**启用 (Enable)**。

步骤 4　输入信息。

步骤 5　点击 **Submit**。

后续操作

当不再需要远程访问支持人员时，请参阅禁用技术支持隧道 （第 16-5 页）。

启用远程访问未直接连接互联网的设备

对于未直接连接互联网的设备，通过连接到互联网的其他设备进行访问。

准备工作

- 设备必须能够通过端口 22 连接到其他已连接互联网的设备。
- 在已连接互联网的设备上，按照启用远程访问连接互联网的设备 （第 16-4 页）中的步骤创建通往该设备的支持隧道。

操作步骤

步骤 1　在需要支持的设备的命令行界面中，输入 `techsupport` 命令。

步骤 2　输入 `sshaccess`。

步骤 3　按照提示操作。

后续操作

当不再需要远程访问支持人员时，请参阅以下内容：

- 禁用远程访问 （第 16-5 页）
- 禁用技术支持隧道 （第 16-5 页）

禁用技术支持隧道

已启用的 techsupport 隧道连续 7 天保持连接到 `upgrades.ironport.com`。此后，建立的连接不会断开，但一旦断开，将无法重新连接到隧道。

操作步骤

步骤 1　登录到设备。

步骤 2　在 GUI 窗口的右上角，依次选择**帮助和支持 (Help and Support) > 远程访问 (Remote Access)**。

步骤 3　点击**禁用 (Disable)**。

禁用远程访问

使用 `techsupport` 命令创建的远程访问帐户将保持活动状态，直到将其禁用为止。

操作步骤

步骤 1　在命令行界面中，输入 `techsupport` 命令。

步骤 2　输入 `sshaccess`。

步骤 3　输入 `disable`。

检查支持连接的状态

操作步骤

步骤 1　在命令行界面中，输入 `techsupport` 命令。

步骤 2　输入 `status`。

运行数据包捕获

数据包捕获允许支持人员查看 TCP/IP 数据，及传入和传出设备的其他数据包。由此，允许支持部门调试网络设置，了解到达设备或离开设备的网络流量。

操作步骤

步骤 1　依次选择**帮助和支持 (Help and Support) > 数据包捕获 (Packet Capture)**。

步骤 2　指定数据包捕获设置：

a. 在**数据包捕获设置 (Packet Capture Settings)** 部分，点击**编辑设置 (Edit Settings)**。

b. （可选）输入数据包捕获的持续时间、限制和过滤器。

您的支持代表可针对这些设置提供指导。

如果输入的捕获持续时间未指定时间单位， AsyncOS 默认以秒为单位。

在 “过滤器 (Filters)”部分：

- 自定义过滤器可以使用 Unix `tcpdump` 命令支持的任何语法，例如 `host 10.10.10.10 && port 80`。
- 客户端 IP 是连接到设备的计算机的 IP 地址，例如通过邮件安全设备发送邮件的邮件客户端。
- 服务器 IP 是设备连接到的计算机的 IP 地址，例如设备向其传送邮件的 Exchange 服务器。

  可以使用客户端和服务器 IP 地址跟踪特定客户端与特定服务器之间的流量，而将邮件安全设备置于两者之间。

c. 点击 **Submit**。

步骤 3　点击**开始捕获 (Start Capture)**。

- 一次只能运行一个捕获。
- 当数据包捕获运行时，“数据包捕获 (Packet Capture)”页面将显示正在进行的捕获的状态，即显示当前的统计数据，例如文件大小和逝去的时间。
- GUI 仅显示在 GUI 中启动的数据包捕获，不包括从 CLI 启动的捕获。同样， CLI 仅显示在 CLI 中启动运行的当前数据包捕获的状态。
- 数据包捕获文件可拆分为十个部分。如果该文件的大小在数据包捕获结束前达到最大限制，系统将删除文件最早的部分 （放弃数据），新部分将从当前的数据包捕获数据开始。每次仅放弃仅数据包捕获文件的 1/10。
- 如果正在运行的捕获从 GUI 启动，将保留在会话之间。（如果正在运行的捕获从 CLI 中启动，当会话结束时，捕获将停止。）

步骤 4　允许捕获运行指定的持续时间；如果允许捕获无限期地运行，可通过点击**停止捕获 (Stop Capture)** 手动停止捕获。

步骤 5　访问数据包捕获文件：

- 点击**管理数据包捕获文件 (Manage Packet Capture Files)** 列表，然后点击**下载文件 (Download File)**。
- 使用 FTP 或 SCP 访问设备 `captures` 子目录中的文件。

后续操作

将文件设为可供支持人员访问：

- 如果允许远程访问您的设备，技术人员可使用 FTP 或 SCP 访问数据包捕获文件。请参阅启用思科技术支持人员远程访问 （第 16-4 页）。
- 将该文件通过邮件发送给支持人员。

远程重置设备电源

如果设备需要硬重置，可以使用第三方智能平台管理界面 (IPMI) 工具远程重启设备机箱。

限制

- 远程电源管理仅适用于特定硬件。

  有关特定信息，请参阅启用远程电源管理 （第 14-6 页）。
- 如果您希望能够使用此功能，必须提前启用该功能。

  有关详细信息，请参阅启用远程电源管理 （第 14-6 页）。
- 仅支持以下 IPMI 命令：

  `status、on、off、cycle、reset、diag、soft`

  发出不受支持的命令将会引发 “权限不足”错误。

准备工作

- 获取并设置可使用 IPMI 2.0 版管理设备的实用程序。
- 了解如何使用受支持的 IPMI 命令。请参阅您的 IPMI 工具文档。

操作步骤

步骤 1　使用 IPMI 向分配到 “远程电源管理”端口 （之前配置）的 IP 地址发出支持的电源循环命令，以及所需的凭证。

例如，从支持 IPMI 的 UNIX 类型计算机中可能发出如下命令：

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

其中，`192.0.2.1` 是分配到 “远程电源管理”端口的 IP 地址，`remoteresetuser` 和 `password` 是您在启用此功能时输入的凭证。

步骤 2　等待至少五分钟，以便设备重启。

IP 接口和设备访问

您可以通过各种服务访问在思科内容安全设备上创建的任何 IP 接口。

默认情况下，以下服务在每个接口上的启用或禁用情况：

表 A-1　在 IP 接口上默认启用的服务

		是否默认为启用？	
服务	**默认端口**	**管理界面**	**您创建的新 IP 接口**
FTP	21	否	否
Telnet	23	是	否
SSH	22	是	否
HTTP	80	是	否
HTTPS	443	是	否

IP 接口

IP 接口包含到网络的各个连接所需要的网络配置数据。可以为一个物理以太网接口配置多个 IP 接口。还可以通过 IP 接口配置垃圾邮件隔离区访问权限。对于邮件传输和虚拟网关，每个 IP 接口都可作为一个具有特定 IP 地址和主机名的虚拟网关地址。也可以将接口 “连接”到不同组中（通过 CLI），系统在传输邮件时将遍历这些组。连接或组合虚拟网关，对于在多个接口之间均衡大型邮件活动的负载非常有用。还可以创建 VLAN，并像配置任何其他接口 （通过 CLI）一样配置它们。有关更多信息，请参阅邮件安全设备用户指南或在线帮助中的 “高级网络”章节。

配置 IP 接口

通过 “管理设备 (Management Appliance)” > “网络 (Network)” > “IP 接口 (IP Interfaces)”页面（和 `interfaceconfig` 命令），可以添加、编辑或删除 IP 接口。

备注 不能更改安全管理设备上与管理接口相关联的名称或以太网端口。此外，安全管理设备不支持下面讨论的所有功能 （例如，虚拟网关）。

配置 IP 接口时需要以下信息：

表 A-2　　IP 接口组件

名称	接口的昵称。
IP 地址	相同子网的 IP 地址不能在单独的物理以太网接口上配置。
网络掩码 （或子网掩码）	您可以按标准的点分八位组格式 （例如 255.255.255.0）或十六进制格式（例如 0xffffff00）输入网络掩码。默认网络掩码为 255.255.255.0，这是一个通用 C 类值。
广播地址	AsyncOS 自动从 IP 地址和网络掩码计算默认广播地址。
主机名	与接口相关的主机名。此主机名用于在 SMTP 会话期间标识服务器。您需要输入与每个 IP 地址关联的有效主机名。此软件不会检查 DNS 是否正确将主机名解析为匹配的 IP 地址，或将反向 DNS 解析为给定的主机名。
允许的服务	可以在接口上启用或禁用 FTP、 SSH、 Telnet、垃圾邮件隔离区、 HTTP 和 HTTPS。可以为每项服务配置端口。还可以为垃圾邮件隔离区指定 HTTP/HTTPS、端口和 URL。

备注　如果已按第 2 章“设置、安装和基本配置”中所述完成系统设置向导，并确认了更改，则应已在设备上配置管理接口。

使用 GUI 创建 IP 接口

操作步骤

步骤 1　依次选择**管理设备 (Management Appliance) > 网络 (Network) > IP 接口 (IP Interfaces)**。

步骤 2　点击**添加 IP 接口 (Add IP Interface)**。

步骤 3　输入接口的名称。

步骤 4　选择以太网端口，并输入 IP 地址。

步骤 5　输入 IP 地址的网络掩码。

步骤 6　输入接口的主机名。

步骤 7　选中要在此 IP 接口上启用的每项服务旁边的复选框。如果需要，可以更改相应的端口。

步骤 8　选择是否启用 HTTP 到 HTTPS 的重定向，以便于在接口上进行设备管理。

步骤 9　如果使用垃圾邮件隔离区，可以选择 HTTP 和/或 HTTPS 并分别指定端口号。还可以选择是否将 HTTP 请求重定向到 HTTPS。最后，可以指定 IP 接口是否为垃圾邮件隔离区的默认接口，以及是否使用主机名作为 URL 或提供自定义 URL。

步骤 10　提交并确认更改。

通过 FTP 访问设备

警告　**通过 “管理设备 (Management Appliance)” > “网络 (Network)” > “IP 接口 (IP Interfaces)”页面或 `interfaceconfig` 命令禁用服务后，可从 GUI 或 CLI 断开自身的连接，具体取决于连接至设备的方式。如果无法使用其他协议、串行接口或管理端口的默认设置重新连接到设备，请勿使用此命令禁用服务。**

操作步骤

步骤 1　使用“管理设备 (Management Appliance)”>“网络 (Network)”>“IP 接口 (IP Interfaces)”页面（或 `interfaceconfig` 命令）为接口启用 FTP 访问权限。

注　请先确认更改，再进行下一步。

步骤 2　通过 FTP 访问接口。确保为该接口使用的 IP 地址正确。

示例：

```
ftp 192.168.42.42
```

许多浏览器还允许通过 FTP 访问接口。

示例：

```
ftp://192.10.10.10
```

步骤 3　浏览到尝试完成的特定任务所在的目录。通过 FTP 访问接口后，可以浏览以下目录以复制和添加（“GET”和 “PUT”）文件。请参阅表 A-3。

表 A-3　　可访问的目录

Directory Name	说明
/avarchive **/bounces** **/cli_logs** **/delivery** **/error_logs** **/ftpd_logs** **/gui_logs** **/mail_logs** **/rptd_logs** **/sntpd.logs** **/status** **/system_logs**	自动创建，以便通过 “管理设备 (Management Appliance)” > “系统管理 (System Administration)” > “日志订阅 (Log Subscriptions)” 页面或 `logconfig` 和 `rollovernow` 命令记录日志。有关每个日志的详细说明，请参阅邮件安全设备用户指南或在线帮助中的 “日志记录” 章节。 有关各个日志文件类型之间的差异，请参阅 “日志记录” 章节中的 “日志文件类型比较”。
/configuration	以下页面和命令中的数据将导出到和/或从其中导入 （保存）的目录： • 虚拟网关映射 (`altsrchost`) • XML 格式的配置数据 (`saveconfig, loadconfig`) • 主机访问表 (HAT) 页面 (`hostaccess`) • 收件人访问表 (RAT) 页面 (`rcptaccess`) • SMTP 路由页面 (`smtproutes`) • 别名表 (`aliasconfig`) • 伪装表 (`masquerade`) • 邮件过滤器 (`filters`) • 全局取消订阅数据 (`unsubscribe`) • `trace` 命令的测试邮件

表 A-3　　可访问的目录 （续）

Directory Name	说明
/MFM	邮件流监控数据库目录包含从 GUI 可用的邮件流监控功能的数据。每个子目录包含一个自述文件，其中记录了各个文件的记录格式。 可以将这些文件复制到其他计算机以便保留记录，也可以将文件加载到数据库中并创建自己的分析应用。所有目录中的全部文件的记录格式相同，未来版本中可能会更改此格式。
/periodic_reports	存储系统中配置的所有存档报告的目录。

步骤 4　使用 FTP 程序从相应目录上传和下载文件。

安全复制 (scp) 权限

如果客户端操作系统支持安全复制 (scp) 命令，可以复制文件到表 A-3，第 A-4 页列出的目录或从其中复制文件。例如，在以下示例中，文件 /tmp/test.txt 从客户端复制了主机名为 mail3.example.com 的设备的配置目录。

备注　该命令提示输入用户的密码 (admin)。此示例仅供参考，您的操作系统实施的安全复制操作可能有所不同。

```
% scp /tmp/test.txt admin@mail3.example.com:configuration
The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.
DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.
Are you sure you want to continue connecting (yes/no)?是
Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.
admin@mail3.example.com's password: (type the password)
test.txt             100% |***************************| 1007        00:00
%
```

在本例中，从设备复制了相同文件到客户机：

```
% scp admin@mail3.example.com:configuration/text.txt .
admin@mail3.example.com's password: (type the password)
test.txt             100% |***************************| 1007        00:00
```

可以使用安全复制 (scp) 代替 FTP 进行与内容安全设备之间的文件传输。

备注　只有操作员或管理员组的用户可以使用安全复制 (scp) 访问设备。有关详细信息，请参阅关于恢复到更早版本的 AsyncOS （第 14-24 页）。

通过串行连接访问

如果通过串行连接连接到设备，图 A-1 说明了串行端口连接器的引脚编号，表 A-4 定义了串行端口连接器的引脚分配情况和接口信号。

图 A-1　　串行端口的引脚编号

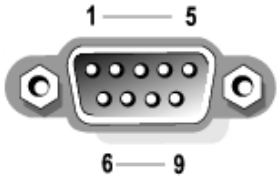


表 A-4　　串行端口引脚分配

引脚	信号	I/O	定义
1	DCD	I	数据载体检测
2	新加坡	I	串行输入
3	SOUT	O	串行输出
4	DTR	O	数据终端就绪
5	接地线	不适用	信号接地
6	DSR	I	数据设置就绪
7	RTS	I	请求发送
8	CTS	O	允许发送
9	RI	I	振铃指示器
外壳	不适用	不适用	机箱接地线

分配网络和 IP 地址

本附录介绍有关网络和 IP 地址分配的一般规则，以及将思科内容安全设备连接到网络的某些策略。

本附录中包括以下主题：

以太网接口

思科内容安全设备最多有四个以太网接口，位于系统的后面板，具体数目取决于配置 （是否有可选光纤网络接口）。它们的标签为：

- 管理
- Data1
- Data2
- Data3
- Data4

选择 IP 地址和网络掩码

在配置网络时，内容安全设备必须能够选择唯一接口来发送传出数据包。这种要求促成了关于以太网接口 IP 地址和网络掩码选择的部分决定。该规则即要求单一网络中只能有一个接口 （通过应用网络掩码到接口的 IP 地址确定）。

IP 地址标识任何给定网络中的物理接口。一个物理以太网接口可以有多个 IP 地址，用来接受数据包。包含多个 IP 地址的以太网接口可以通过该接口发送数据包，以其任一 IP 地址作为数据包中的源地址。实施虚拟网关技术时需使用此属性。

网络掩码的作用是将 IP 地址划分为网络地址和主机地址。网络地址可视为 IP 地址的网络部分（位数与网络掩码匹配）。主机地址是 IP 地址的其余位数。四个较大的八位数地址的位数有时使用无类域间路由 (CIDR) 样式表示。这是位数后加的反斜线 (1-32）。

网络掩码可以这种方式表示，只统计二进制中的位数，因此 `255.255.255.0` 将变成 “`/24`”，而 `255.255.240.0` 将变成 “`/20`”。

接口配置示例

此部分显示了基于某些典型网络的接口配置示例。该示例使用两个接口，称为 Int1 和 Int2。对于内容安全设备，这些接口名称可以是三个接口 （管理、 Data1、 Data2）中的任意两个接口。

网络 1：

独立接口必须出现在独立网络中。

接口	IP 地址	Netmask	网络地址
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

寻址到 192.168.1.x（其中 X 为 1 到 255 之间的任意数字，不含您自己的地址，在本例中为 10）的数据在 Int1 中传出。寻址到 192.168.0.x 的任何信息在 Int2 中传出。对于发往不是这些格式的其他某些地址的任何数据包（很可能在 WAN 或 Internet 接口传出），将被发送到其中某个网络必须存在的默认网关。然后，默认网关继续转发数据包。

网络 2：

两个不同接口的网络地址 （IP 地址的网络部分）不能相同。

以太网接口	IP 地址	Netmask	网络地址
Int1	192.168.1.10	255.255.0.0	192.168.0.0/16
Int2	192.168.0.10	255.255.0.0	192.168.0.0/16

这种情况会出现冲突，因为两个不同的太网接口的网络地址相同。如果将内容安全设备中的数据包发送到 192.168.1.11，将无法确定应使用哪个以太网接口来传送数据包。如果两个以太网接口均连接到两个独立的物理网络，则可能会将数据包发送到错误的网络，永远找不到其目标。内容安全设备不允许网络配置存在冲突。

可以将两个以太网接口连接到同一个物理网络，但是必须构建 IP 地址和网络掩码，以便内容安全设备选择唯一的传送接口。

IP 地址、接口和路由

对于允许选择接口的 GUI 或 CLI （例如，升级 AsyncOS 或配置 DNS），当选择在其中执行命令或功能使用的接口时，路由 （默认网关）的优先级高于您的选择。

例如，假设您有一台内容安全设备，其中配置了三个网络接口，每个接口位于不同的网段 （假设所有 /24）：

以太网	IP
管理	192.19.0.100
Data1	192.19.1.100
Data2	192.19.2.100

您的默认网关是 192.19.0.1。

现在，如果执行 AsyncOS 升级 （或允许您选择接口的其他命令或功能），并且您选择了 Data1 中的 IP (192.19.1.100)，期待所有 TCP 流量都通过 Data1 以太网接口传输。但是，流量没有从设置为默认网关的接口 （这种情况下为 “管理 (Management)”接口）传出，而是使用 Data1 中 IP 的源地址印记。

Summary

内容安全设备必须始终能够识别可传送数据包的唯一接口。为了做出决定，内容安全设备使用数据包的目标 IP 地址与以太网接口的网络和 IP 地址设置的组合。下表总结了上述示例：

	相同网络	不同网络
相同物理接口	允许	允许
不同物理接口	不允许	允许

连接内容安全设备的策略

连接设备时，请记住以下几点：

- 相比邮件流量，管理流量 （CLI、 Web 界面、日志传送）通常较少。
- 如果两个以太网接口连接到同一网络交换机，但最后与另一主机下游的单一接口通信，或连接到所有数据均显示到所有端口的网络集线器，则使用两个接口没有任何优势。
- 在以 1000Base-T 运行的接口中进行 SMTP 通信，比在以 100Base-T 运行的同一接口上进行通信的速度稍快，但仅限于理想情况。
- 如果传送网络的某些其他部分存在瓶颈，则优化连接到您的网络毫无优势可言。瓶颈最常出现在与 Internet 的连接中，以及连接提供商的上游。

选择连接的接口数及如何解决它们应由基础网络的复杂性决定。如果您的网络拓扑或数据量不需要使用太多接口，则无需连接多个接口。另外，可以在起初熟悉网关时保持简单连接，然后随着数据量和网络拓扑的需求增长而提高连接性。

防火墙信息

下表列出了要使思科内容安全设备正常运行可能需要打开的端口 （这些是默认值）。

表 C-1　　防火墙端口

默认端口	协议	输入/输出	主机名	目的
20/21	TCP	输入或输出	AsyncOS IP、 FTP 服务器	FTP，用于整合日志文件。 数据端口 TCP 1024 和更高端口也必须全部打开。 有关详细信息，请在知识库中搜索 FTP 端口信息。请参阅知识库文章 （技术说明）（第 E-3 页）。
22	SSH	出局	AsyncOS IP	集中配置管理器配置推送。 也用于备份。
22	TCP	In	AsyncOS IP	通过 SSH 访问 CLI，整合日志文件。
22	TCP	出局	SCP 服务器	通过 SCP 推送到日志服务器。
23	Telnet	In	AsyncOS IP	通过 Telnet 访问 CLI。
23	Telnet	出局	Telnet 服务器	Telnet 升级。
25	TCP	出局	任意	通过 SMTP 发送邮件。
25	TCP	In	AsyncOS IP	SMTP，用于接收退回的邮件，或者从防火墙外传入的邮件时。
80	HTTP	In	AsyncOS IP	通过 HTTP 访问 GUI，进行系统监控。
80	HTTP	出局	downloads.cisco.com	服务更新 （不包括 AsyncOS 升级）。
80	HTTP	出局	updates.cisco.com	AsyncOS 升级。
82	HTTP	In	AsyncOS IP	用于查看垃圾邮件隔离区。
83	HTTPS	In	AsyncOS IP	用于查看垃圾邮件隔离区。
53	UDP/TCP	出局	DNS 服务器	如果配置为使用 Internet 根服务器或防火墙外的其他 DNS 服务器，则使用 DNS。也用于 SenderBase 查询。
110	TCP	出局	POP 服务器	针对垃圾邮件隔离区的最终用户进行 POP 身份验证。
123	UDP	出局	NTP 服务器	NTP，如果时间服务器在防火墙外部。
143	TCP	出局	IMAP 服务器	针对垃圾邮件隔离区的最终用户进行 IMAP 身份验证。
161	UDP	In	AsyncOS IP	SNMP 查询。
162	UDP	出局	管理基站	SNMP 陷阱。

表 C-1　防火墙端口 （续）

默认端口	协议	输入/输出	主机名	目的
389 3268	LDAP	出局	LDAP 服务器	LDAP，如果 LDAP 目录服务器在防火墙外部。针对垃圾邮件隔离区进行 LDAP 身份验证。
636 3269	LDAPS	出局	LDAP	LDAPS — Active Directory 的全局目录服务器。
443	TCP	In	AsyncOS IP	通过安全 HTTP (`https`) 访问 GUI，进行系统监控。
443	TCP	出局	update-static.cisco.com	验证更新服务器的最新文件。
443	TCP	出局	update-manifests.ironport.com	从更新服务器 （用于物理硬件设备）获取最新文件的列表。
443	TCP	出局	update-manifests.sco.cisco.com	从更新服务器 （用于虚拟设备）获取最新文件的列表。
443	TCP	出局	phonehome.senderbase.org	接收/发送病毒爆发过滤器。
443	TCP	出局	在网络安全设备中 “安全服务 (Security Services)” > “防恶意软件和信誉 (Anti-Malware and Reputation)” 页面的 “高级 (Advanced)” 部分中配置的文件分析服务器 URL。 在邮件安全设备中 “安全服务 (Security Services)” > “防恶意软件和信誉 (Anti-Malware and Reputation)” 页面的 “高级 (Advanced)” 部分中配置的文件分析服务器 URL。	显示文件分析服务器上的详细文件分析结果。 另请参阅： • 邮件安全报告：有关文件分析报告详细信息的要求 （第 4-24 页） • 网络安全报告：有关文件分析报告详细信息的要求 （第 5-19 页）
514	UDP/TCP	出局	系统日志服务器	系统日志记录。
1024 和更高	-	-	-	对于端口 21，请参阅以上信息 (FTP)。
2222	CCS	输入和输出	AsyncOS IP	集群通信服务 （用于集中管理）。
6025	TCP	In	AsyncOS IP	如果启用了外部垃圾邮件隔离区，则将垃圾邮件隔离区数据发送到安全管理设备。
7025	TCP	输入和输出	AsyncOS IP	启用此功能时，传递邮件安全设备和安全管理设备之间的策略、病毒和病毒爆发隔离区数据。

网络安全管理示例

本附录介绍和说明实施思科内容安全管理设备功能的许多常规方式，包括以下部分：

网络安全设备示例

本部分介绍使用安全管理设备和网络安全设备的示例。

备注 所有这些示例场景均假设您已在安全管理设备*和*网络安全设备上启用了网络报告和网络跟踪。有关如何启用网络跟踪和网络报告的信息，请参阅第 5 章 “使用集中 Web 报告和跟踪”。

示例 1：调查用户

此示例演示系统管理员如何在公司调查特定用户。

在此案例中，经理收到有关员工在工作时间访问不当网站的投诉。要调查此问题，系统管理员现在需要跟踪其网络活动的详细信息。

一旦跟踪网络活动，系统将会生成 Web 报告，其中包含关于员工浏览历史记录的信息。

操作步骤

步骤 1 在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 用户 (Users)**。

步骤 2 在**用户 (Users)** 表中，点击要调查的**用户 ID (User ID)** 或**客户端 IP 地址 (Client IP address)**。

如果不知道用户 ID 或客户端 IP 地址，请在文本字段键入可以确定的用户 ID 或客户端 IP 地址信息，然后点击**查找用户 ID 或客户端 IP 地址 (Find User ID or Client IP address)**。 IP 地址不需要与返回结果完全匹配。“用户 (Users)”表将填充您指定的用户 ID 和客户端 IP 地址。在本例中，我们要查找有关客户端 IP 地址 10.251.60.24 的信息。

步骤 3 点击 IP 地址 **10.251.60.24**。

将显示 10.251.60.24 的 “用户详细信息 (User Details)”页面。

从“用户详细信息 (User Details)”页面，可以确定“按事务总数的 URL 类别 (URL Categories by Total Transactions)”、“按事务总数的趋势 (Trend by Total Transaction)”、“匹配的 URL 类别 (URL Categories Matched)”、“匹配的域 (Domains Matched)”、“匹配的应用 (Applications Matched)”、“检测到的恶意软件威胁 (Malware Threats Detected)”和 “匹配的策略 (Policies Matched)”。

通过这些类别，可以查看用户 10.251.60.24 是否曾尝试访问被阻止的 URL （可查页面 “域 (Domains)”部分下的 “已阻止事务 (Transactions Blocked)”列）。

步骤 4　点击 “匹配的域 (Domains Matched)”表下的**导出 (Export)**，可查看用户曾尝试访问的域和 URL 的完整列表。

在此，可以使用 “网络跟踪 (Web Tracking)”功能跟踪和查看此特定用户的网页。

注　值得注意的是,Web 报告允许检索用户访问的所有域信息，而不一定是访问的特定 URL。有关用户访问的特定 URL、访问该 URL 的时间、该 URL 是否允许等信息，请使用 “网络跟踪 (Web Tracking)”页面的 “代理服务 (Proxy Services)”选项卡。

步骤 5　依次选择**网络 (Web) > 报告 (Reporting) > 网络跟踪 (Web Tracking)**。

步骤 6　点击**代理服务 (Proxy Services)** 选项卡。

步骤 7　在 “用户/客户端 IP 地址 (User/Client IP Address)”文本字段，键入用户名或 IP 地址。

在本例中，我们要搜索用户 10.251.60.24 的网络跟踪信息。

屏幕上将显示搜索结果。

在此页面，可以查看分配到 IP 地址 10.251.60.24 的计算机用户所访问的事务和 URL 的完整列表。

相关主题

表 D-1 列出了本例中讨论的各个主题。点击链接可了解有关每个主题的详细信息。

表 D-1　“调查用户”的相关主题

功能名称	功能信息
“用户 (User)”页面	用户报告 (Web) （第 5-9 页）
“用户详细信息 (User Details)”页面	用户详细信息 （Web 报告）（第 5-10 页）
导出报告数据	打印和导出报告和跟踪数据 （第 3-9 页）
“网络跟踪 (Web Tracking)”页面的 “代理服务 (Proxy Services)”选项卡	搜索网络代理服务处理的事务 （第 5-35 页）

示例 2：跟踪 URL

在此案例中，销售经理希望了解其公司在上周访问的前五大网站。此外，该经理希望了解哪些用户需要访问这些网站。

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > 网站 (Web Sites)**。

步骤 2　从 “时间范围 (Time Range)” 下拉列表中，选择**周 (Week)**。

步骤 3　向下滚动到 “域 (Domains)” 部分，查看访问过的域或网站。

“匹配的域 (Domains Matched)” 表中将显示访问的前 25 个网站。在同一表中，点击 “域 (Domain)” 或 “IP” 列中的链接，可以查看特定地址或用户实际访问的网站。

相关主题

表 D-2 列出了本例中讨论的各个主题。点击链接可了解有关每个主题的详细信息。

表 D-2　“跟踪 URL” 的相关主题

功能名称	功能信息
“网站 (Web Sites)” 页面	网站报告 （第 5-11 页）

示例 3：调查访问的热门 URL 类别

在此案例中，人力资源经理想要了解其员工在 30 天内访问的前三大 URL 类别。此外，网络管理员想要获得这些信息，以便监控带宽使用并了解哪些 URL 在工作中占用的带宽最大。

以下示例将演示如何收集多人涵盖多个兴趣点的数据，同时只生成一份报告。

操作步骤

步骤 1　在安全管理设备上，依次选择**网络 (Web) > 报告 (Reporting) > URL 类别 (URL Categories)**。

在本例中的 “URL 类别 (URL Categories)” 页面，可以看到前 10 个 “按事务总数的 URL 类别 (URL Categories by Total Transactions)” 图显示：有 282 K 访问未分类 URL，以及 “即时消息 (Instant Messaging)”、“仇恨言论 (Hate Speech)” 和 “纹身 (Tattoo)” 站点等。

这时，可以点击**导出 (Export)** 链接将这些原始数据导出到 Excel 电子表格，并将此文件发送给人力资源经理。但请记住，网络管理员想要了解各个 URL 使用的带宽。

步骤 2　向下滚动到**匹配的 URL 类别 (URL Categories Matched)** 表，查看 “带宽使用 (Bandwidth Used)” 列。

从**匹配的 URL 类别 (URL Categories Matched)** 表中，可以查看所有 URL 类别的带宽使用情况。同样，可以点击**导出 (Export)** 链接，并将此文件发送给网络管理员。不过，要了解更精细的信息，请点击 “即时消息 (Instant Messaging)” 链接，查看占用带宽的用户。屏幕上将会出现以下页面。

在此页面中，网络管理员可以查看 “即时消息 (Instant Messaging)” 站点的前 10 位用户。

此页面显示，在过去 30 天内，用户 10.128.4.64 在 “即时消息 (Instant Messaging)” 站点花费 19 小时 57 分钟；该时间的带宽使用量为 10.1 MB。

相关主题

表 D-3 列出了本例中讨论的各个主题。点击链接可了解有关每个主题的详细信息。

表 D-3　“调查热门 URL 类别”的相关主题

功能名称	功能信息
“URL 类别 (URL Categories)”页面	URL 类别报告 （第 5-12 页）
导出报告数据	打印和导出报告和跟踪数据 （第 3-9 页）

其他资源

思科通知服务

注册可接收与您的思科内容安全设备相关的通知，例如安全建议、现场通知、停止销售或停止支持声明，以及有关软件更新和已知问题的信息。

可以指定通知频率和接收的信息类型等选项。有关使用的每种产品的通知，应单独注册。

要进行注册，请访问 http://www.cisco.com/cisco/support/notifications.html

需要有 Cisco.com 帐户。如果没有，请参阅注册思科帐户 （第 E-4 页）。

文档

在以下位置可获得本产品和相关产品的文档：

思科内容安全产品的文档：	位于：
安全管理设备	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
网络安全设备	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
邮件安全设备	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
内容安全产品的命令行参考指南	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
思科 IronPort 加密	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

此外，还可通过点击右上角的**帮助和支持 (Help and Support)**，直接从设备 GUI 访问 HTML 在线帮助版本的用户指南。

思科内容安全设备的文档集包括以下文档和手册 （并非所有设备和版本都包括所有类型）：

- 所有产品的发行说明
- 思科内容安全管理设备*快速入门指南*
- 适用于您的版本的*思科内容安全管理设备 AsyncOS 9.1 用户指南*（本手册）
- 适用于您的网络安全设备的文档：

  适用于网络安全版本 8.0 及更高版本
  - 适用于您的版本的 *Cisco AsyncOS for Web 用户指南*

  适用于 8.0 之前的网络安全版本:
  - 适用于您的版本的 *Cisco IronPort AsyncOS for Web 用户指南*
- 思科邮件安全 AsyncOS 文档：

  适用于邮件安全版本 8.0 及更高版本：
  - 适用于您的版本的*思科邮件 AsyncOS 用户指南*

  适用于 8.0 之前的邮件安全版本：
  - *思科邮件安全 IronPort AsyncOS 配置指南*
  - *思科邮件安全 IronPort AsyncOS 高级配置指南*
  - *思科邮件安全 IronPort AsyncOS 日常管理指南*
- *思科 AsyncOS CLI 参考指南*（某些命令适用于所有思科内容安全产品）

第三方贡献者

AsyncOS 的某些软件根据 FreeBSD, Inc.、 Stichting Mathematisch Centrum、 Corporation for National Research Initiatives, Inc. 及其他第三方贡献者的软件许可协议条款、通知和条件分发，所有此类条款和条件均包含在思科许可协议当中。

有关第三方许可证的信息，请参阅以下网站的许可文档：
http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html 和 https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html。

经 Tobi Oetiker 明确书面同意， AsyncOS 的部分软件基于 RRDtool。

本文档中部分相关内容的复制已取得 Dell Computer Corporation 的许可。本文档中部分相关内容的复制已取得 McAfee, Inc. 的许可。本文档中部分相关内容的复制已取得 Sophos Plc 的许可。

培训

有关培训方式，请参阅：

- http://www.cisco.com/web/learning/le31/email_sec/index.html
- http://www.cisco.com/web/learning/training-index.html

或联系 stbu-trg@cisco.com。

知识库文章 （技术说明）

步骤 1　转到主产品页面 (http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html)

步骤 2　查找名称中包含 **TechNotes** 的链接。

思科支持社区

思科支持社区是一个面向 Cisco 客户、合作伙伴和员工的在线论坛。在这里，可以讨论常规内容安全问题，以及关于特定思科产品的技术信息。您可以向论坛发布主题咨询问题，并与其他用户分享信息。

请通过以下 URL 访问思科支持社区：

- 针对邮件安全和相关管理：
  https://supportforums.cisco.com/community/netpro/security/email
- 针对网络安全和相关管理：
  https://supportforums.cisco.com/community/netpro/security/web

客户支持

请使用以下方法获取支持：

国际：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

支持站点：http://www.cisco.com/web/services/acquisitions/ironport.html

如果您是通过经销商或另一个供应商购买了支持，请直接联系该供应商咨询您的产品支持问题：

另请参阅从设备新建或更新支持案例 （第 16-3 页）。

注册思科帐户

要访问 Cisco.com 上的许多资源，都需要有思科帐户。

如果您没有 Cisco.com 用户 ID，可以在此注册一个帐户：
https://tools.cisco.com/RPF/register/register.do

相关主题

- 思科通知服务 （第 E-1 页）
- 知识库文章 （技术说明）（第 E-3 页）

思科欢迎您评论

技术发布团队热衷于完善产品文档。我们时刻欢迎您的评论和建议。您可以将评论发送至以下电邮地址：

contentsecuritydocs@cisco.com

请在邮件主题行中加入本手册的标题及标题页中的发布日期。

最终用户许可协议

思科系统最终用户许可协议

重要提示：请认真阅读本最终用户许可协议。很重要的一点是，您应确认是从授权来源购买思科软件或设备，并且您或您所代表的实体 （统称为 “客户”） 已经注册成为思科最终用户许可协议中规定的最终用户。如您还未注册成为最终用户，则无权使用本软件。本最终用户许可协议中的有限担保条款对您不适用。如您是从已授权的渠道购买了本软件，一旦下载、安装或使用思科或思科供应软件即构成接受本协议。

CISCO SYSTEMS, INC. 或代替 CISCO SYSTEMS INC. 许可本软件的子公司 （“思科”） 愿意对您许可本软件，前提条件是您购买的软件来自授权来源，并且您接受本最终用户许可协议中的所有条款和条件，以及本产品随附或订购本产品时提供的附加许可协议中列出的对许可证的任何其他限制 （统称 “协议”）。如果最终用户许可协议与补充许可协议之间存在任何冲突，应以补充许可协议为准。下载、安装或使用本软件即表示您确认您是从授权渠道购买的本软件并同意受本协议的约束。若您不同意本协议全部条款，则思科不愿意授予您本软件许可，因此 (a) 您不得下载、安装或使用本软件；和 (b) 您可退还本软件 （包括未启封的 CD 包和所有书面资料） 并获得全额退款。或者，如果本软件与书面材料构成其他产品的组成部分，您可退还全部产品并获得全额退款。只有原始及注册最终用户购买者才享有退货与退款权利，并且该权利从授权渠道购买产品后 30 天失效。在本最终用户许可协议中，“授权来源” 指 (a) 思科；或 (b) 思科授权向您所在区域的最终用户经销/出售思科设备、软件与服务的经销商或系统集成商；或 (c) 所述经销商或系统集成商根据其与思科签订的经销商协议条款规定，授权向您所在区域的终端用户分销/出售思科设备、软件与服务的转售商。

本协议下述条款管辖客户对本软件 （定义如下） 的使用，除非 (a) 客户与思科签订了单独协议以管理客户对本软件的使用；或 (b) 本软件包含了单独的 “点击接受” 许可协议或第三方许可协议，作为安装或下载流程的组成部分以管理客户对本软件的使用。如果前述文件条款之间存在任何抵触，优先顺序应为 (1) 经签署后的合同；(2) 点击接受协议或第三方协议；和 (3) 本协议。在本协议中，“软件” 指计算机程序，包括授权来源提供给客户的思科设备中嵌入的固件和计算机程序，以及该固件和计算机程序的升级版、更新版、错误修正版与修改版 （统称为 “升级版”）；根据思科软件转让或重新许可政策 （思科不定期修改后版本） 重新许可的程序或前述内容的备份副本。

许可。以遵守本协议条款和条件为前提，思科授予客户非独占性、不可转让许可，允许在客户内部业务中使用客户已向授权渠道支付许可费用的软件和文档。“文档” 指该软件授权来源以任何方式 （如 CD-ROM、在线提供等） 所提供的与本软件相关的书面信息 （无论是包含在用户手册、技术手册、培训材料、技术说明或其他材料中）。为使用本软件，客户应输入注册号或产品授权密钥，并在思科的网站在线登记客户的软件副本，以获取必要的许可密钥或许可文件。

客户使用本软件的许可应限于单个硬件机箱或硬件卡，除此以外客户不得在其他地方使用本软件。此外，使用许可权限还应符合相关补充许可协议或采购订单上规定的限制要求，因为此类订单已被授权来源所接受，并且客户已就该订单 （“采购订单”）向授权来源支付必要的许可费。

除文档或相关补充许可协议中另有明确规定外，客户仅能使用其持有或租赁的思科设备中嵌入、运行的软件，或 （如果相关文档允许在非思科设备上安装的话）为了与客户持有或租赁的思科设备通信使用本软件，以及为了实现客户的内部业务目的使用本软件。未以暗示、禁止反言或其他方式授予其他许可。

对于思科未收取许可费用的评估或测试软件，上述有关支付许可费用的要求不适用。

一般限制要求。本协议仅为软件与文档许可协议，并非转让软件与文档的所有权，思科保留本软件与文档副本的所有权利。客户确认本软件与文档中含有思科或其提供商与许可方的商业秘密，包括 （但不限于）单个程序的具体内部设计和架构，以及相关接口信息。除非本协议另有明确规定，本软件只能与授权渠道提供的思科设备接合使用，客户：

(i) 无权且明确同意不会向他人或实体转让、分配或转授其许可权力 （符合思科现行有效的再次许可/转让政策的除外）；无权且明确同意不会在授权渠道以外采购的思科设备上或在二手思科设备上使用本软件；客户确认任何企图转让、分配、转授或使用的行为无效。

(ii) 无权且明确同意不会修正本软件错误、修改本软件或根据本软件制作衍生产品；也不得允许他人实施这种行为；

(iii) 无权且明确同意不会对本软件进行逆向工程、反编译、解码、反汇编或将本软件修改为可读格式。尽管存在该等限制要求，但适用法律明确许可的情况除外，以及根据适用开源协议规定要求思科允许该等活动的除外。

(iv) 无权且明确同意不会公布在本软件上运行的基准测试的结果；

(v) 未征得思科明确书面授权，无权且明确同意不会使用本软件或允许使用本软件向第三方提供服务，无论是以服务机构或分时方式提供服务；或

(vi) 未征得思科事先书面批准，无权且明确同意不会以任何方式向第三方披露、提供本软件和文档中包含的商业秘密。客户应采取合理的安全措施保护该等商业秘密。

在法律要求的范围内，思科将应客户的书面请求，并在客户支付思科的适用费用 （如有）后，为客户提供必要的界面信息，以实现软件与其他独立创作的程序之间的互操作性。客户应严格遵守该等信息相关的保密义务。思科提供该等信息后应根据适用条款和条件的要求使用该等信息。

软件、升级版或额外副本。尽管本协议中含有其他相反之规定， (1) 客户无权制作或使用额外副本或更新版本，除非客户在制作或取得该副本或更新版本时，已经持有原始软件的有效许可并就更新版本或新增副本向许可资源支付了的恰当的费用；(2) 升级版本仅限用于授权渠道提供的思科设备，且客户是原始最终用户采购方或租赁方，或持有有效许可使用被升级软件，和 (3) 仅限于备份目的制作和使用额外副本。

专有权通知。客户同意采用软件中含有的版权通知和其他专有权通知的格式和方法，针对所有形式的软件副本建立并翻印版权、专有权和其他通知。除本协议明确批准外，未经思科事先书面同意，客户不得制作任何本软件的副本。

期限和终止。本协议与本协议授予的许可在协议终止前始终有效。客户销毁本软件和文档的全部副本后即可终止本协议。如果客户未遵守本协议中的任何条款，则本协议中规定的客户权利应立即终止，无需思科另行通知。协议终止后，客户应销毁其持有或控制和软件与文档的全部副本。本协议终止后，“一般限制要求”一节中规定客户应遵守的所有保密义务、禁止与限制要求、责任限制、免责声明和质保限制要求应继续有效。此外，本协议终止后，标题 “美国政府最终用户购买者”和 “适用于有限担保声明和最终用户许可协议的通用条款”部分的规定仍然有效。

客户记录。客户授予思科及其独立会计师权利，可在客户的正常营业时间内检查客户的账簿、记录及账目，以验证客户遵守本协议的情况。如果审计显示客户不符合本协议要求，客户应即时向思科支付恰当的许可费用加上合理的审计费用。

出口、再出口、转让与使用管控。思科根据本协议提供的软件、文档和技术或直接产品 （以下称为 “软件和技术”）受美国法律法规及任何其他适用国家/地区的法律法规的出口控制约束。客户应遵守约束思科软件与技术出口、再出口、转让和使用的相关法律法规，并获取所有必需的美国和当地授权、准许或许可。思科与客户同意向对方提供取得授权或许可相关的其他信息、支持文件与合理要求的协助。有关遵守出口、再出口、转让和使用等方面规定的信息，请访问：

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html。

美国政府最终用户购买人。本软件与文档系 “商业物品”，该术语定义见 《联邦采购条例》（“FAR”） (48 C.F.R.) 2.101，包括 “商业计算机软件”和 “商业计算机软件文档”，该术语用于 FAR 12.212。符合 FAR 12.212 和 DoD FAR 增刊227.7202-1 至 227.7202-4 的要求。尽管本协议可能并入含有其他相反之 FAR 或合同条款的协议中，客户可向政府最终用户提供具备本协议规定权利的软件与文档。如果本协议为直接与政府签订的协议，则政府最终用户仅根据协议规定的权利即可获得软件与文档。使用软件或文档或二者均使用，将视为政府同意本软件与文档为 “商业计算机软件”与 “商业计算机软件文档”，并视作政府接受本协议中规定的权利与限制要求。

标识组件；额外条款。本软件可能含有一个及以上的组件或与该等组件一同交付，这些组件可能含有第三方备件，思科在文档、自述文件、第三方点击接受协议或其他地方 （如 www.cisco.com）上对该等组件做出了标识 （“标识组件”）。该等组件应遵守不同于本协议规定的许可协议条款、质保免责声明、限制保证或其他条款和条件 （统称为 “额外条款”）的要求。您同意接受任何此类标识组件的适用附加条款。

有限担保。

以符合本协议中的限制要求与条件为前提，思科保证：自向客户发货之日起 （如果是授权来源转售而非思科直接销售，则应从思科最初发货后不超过九十 (90) 天起计算），在随后为期 (a) 九十 (90) 天或 (b) 随产品 （本软件系组成部分）一同交付的保修卡上明确规定的质保期 （如有）内 （以二者中较长日期为准），(a) 安装软件的媒介在正常使用的情况下，材料与工艺上无任何瑕疵；和 (b) 本软件完全符合文档要求。思科发运产品的日期见产品包装。除上述规定外，软件将 “按原样”提供。本有限担保仅用于首次注册最终用户从授权渠道购买的软件。本有限担保中的客户专属补救措施与思科和其提供商的全部责任为 (i) 替换缺陷媒介和/或 (ii) 根据思科的选择修复、替换本软件或退款，上述两种情况的前提条件是违反本有限担保的错误或缺陷在质保期内已报告给向客户销售软件的授权渠道。思科或向客户提供软件的授权渠道可不要求返还软件和/或文档作为行使补救措施的前提条件。思科未保证本软件无任何错误，也未保证客户使用本软件时不会出现任何问题或发生中断。此外，由于入侵和攻击网络的新技术的不断发展，思科并不保证本软件或本软件运行的设备、系统或网络无入侵和攻击漏洞。

限制 如果本软件、产品或授权使用本软件的设备发生下述情况，则本保修不适用：(a) 被修改；但思科或其授权代表做出的修改除外；(b) 未按思科的指示安装、操作、修理或维护；(c) 受到非正常物理或电气应力、非正常环境条件、不当使用、疏忽或其他事故的影响；或 (d) 仅授予测试、评估、试验或示范许可。本软件保修也不适用于：(e) 任何临时软件模块；(f) 思科软件中心上未公布的软件；(g) 思科在思科软件中心明确 “按原样”提供的软件；(h) 授权来源未收到许可费用的软件；和 (i) 授权来源以外的第三方提供的软件。

保修免责声明

除保修条款中规定的外，所有明示或暗示的条款、陈述与保证，包括 （但不限于）对适销性、特殊目的适用性、未涉侵权、合格品质、未涉干扰、信息内容准确性等的暗示保修或条款，或因交易过程、法律、惯例或商业习惯产生的暗示保修或条款在此予以排除，但必须符合适用法律的规定，且思科、其提供商和授权商明确否认这种暗示的保修或条款。某种程度上，同样不能排除该等隐含条款、陈述和 （或）保证的持续时间仅限于上文 “有限担保”一款中明确规定的明示保修期内的情况。由于部分国家或司法管辖区不允许存在暗示保证时限限制，则上述限制要求在该等地区不适用。本保修赋予了客户特定的法律权利，同时客户也可拥有其他司法管辖区内规定的其他权利。即使上述明示保证未能实现其根本目的，该款免责及排除仍然适用。

免责声明 – 责任限制。如果您是在美国、拉丁美洲、加拿大、日本或加勒比地区购买的本软件，尽管本协议中含有其他相反规定，但是，思科、其分公司、高管、董事、雇员、代理、提供商和授权商对客户应承担的责任 （无论是因合同、侵权 [包括过失行为]、违反保修条款或其他形式引起的责任）不得超过授权渠道提供商提供的被索赔软件的购买价格，如果该软件为其他产品的组成部分，则不得超过该产品的购买价格。本软件责任限制是累加的，不限于每个事故 （即存在两个或多个索赔不会扩大此限制）。

如果您是在欧洲、中东地区、非洲、亚洲或太平洋地区购买的本软件，尽管本协议中含有其他相反规定，但是，思科、其分公司、高管、董事、雇员、代理、提供商和授权商对客户应承担的责任 （无论是因合同、侵权 （包括过失行为）、违反保修条款或其他形式引起的责任）不得超过思科提供的被索赔软件的购买价格，如果该软件为其他产品的组成部分，则不得超过该产品的购买价格。本软件责任限制是累加的，不限于每个事故 （即存在两个或多个索赔不会扩大此限制）。本协议中的任何内容均不限制 (I) 思科及其附属公司、高级官员、总监、员工、代理、供应商和许可商由于疏忽对客户造成个人伤害或致死的责任；(II) 思科欺诈性误述的责任；或 (III) 适用法律要求不能排除的思科责任。

免责声明 - 针对间接损害及其他损失的免责声明。如果您是在美国、拉丁美洲、加勒比地区或加拿大购买的本软件，无论本协议中规定的补救措施是否实现了其基本目的，对于任何收益与利润损失、遗失或损坏数据、业务中断、资本损失，或特殊的、间接性、连带性或惩罚性损害赔偿，思科或其提供商均无需承担任何责任，无论导致前述损失损害的原因与责任推断如何，也无论是否是由于使用本软件造成该等损失损害，即使思科或其提供商曾告知将发生该等损害的可能性。由于某些国家或管辖区不允许限制或排除间接或附带损害，因此，上述限制可能对您不适用。

如果您在日本购买软件，除了由死亡或人身伤害、欺诈性失实陈述引起或与之相关的责任，无论本协议中补救措施是否实现其根本目的或其他目的，在任何情况下，思科及其分公司、管理人员、董事、员工、代理、提供商及许可方对任何原因造成的任何收益或利润损失、数据丢失或损坏、业务中断、资本损失、特殊、间接、连带、附带或惩罚性损失概不负责，不论责任推断如何，也无论是否因使用或无法使用软件或其他原因引起，即使思科或任何经批准的源或其提供商或许可方已被告知发生此类损失的可能性。

如果您在欧洲、中东、非洲、亚洲或大洋洲购买软件，在任何情况下，思科及其分公司、管理人员、董事、员工、代理、提供商及许可方对任何收益或利润损失、数据丢失或损坏、业务中断、资本损失、特殊、间接、从属、附带或惩罚性损失概不负责，无论该损失如何造成，包括 （但不限于）合同或侵权 （包括疏忽）原因，也无论该损失是否因使用或无法使用软件引起，即使在各种情况下思科及其分公司、管理人员、董事、员工、代理、提供商及许可方已被告知发生此类损失的可能性。由于某些国家或管辖区不允许限制或排除间接或附带损害，因此，上述限制可能对您完全不适用。前述排除免责条款不适用于由下列原因引起或与之相关的责任：(I) 死亡或人身伤害；(II) 欺诈性失实陈述；(III) 与适用法律下任何不可免责条款有关的由思科承担的责任。

客户确认并同意，思科已根据本协议中的免责声明和责任限制确定价格和签订本协议，该价格和协议反映了协议各方之间的风险分担 （包括合同补救措施可能不能达到其根本目的而且可能导致间接损失的风险），并构成了协议各方议价的重要依据。

管辖法律和司法权。如果您参照经授权来源所接受的采购订单上的地址，在美国、拉丁美洲或加勒比海采购软件，本协议和保证条款 （“保证条款”）受美国加州的法律管辖并持解释权，不管是否存在任何法律条款冲突。加州法院和联邦法院对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在加拿大购买软件，除非当地法律明确禁止，否则本协议和保证条款受加拿大安大略省法律管辖并据其进行解释，不管法律条款是否存在任何冲突；安大略省法庭对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在欧洲、中东、非洲、亚洲或大洋洲 （不包括澳大利亚）购买软件，除非当地法律明确禁止，否则本协议和保证条款受英国法律管辖并据其进行解释，尽管法律条款可能存在任何冲突。英国法庭对由本协议或保证条款引起的任何索赔享有专属管辖权。此外，如果本协议受英国法律管辖，依照 《1999 年合同法 （第三方权利）》，不属于本协议一方的任何人无权执行或受益于本协议的任何条款。如果您在日本购买软件，除非当地法律明确禁止，本协议和保证条款受日本法律管辖并依据该法律进行解释，尽管法律条款可能存在任何冲突。日本东京地方裁判所对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在澳大利亚购买软件，除非当地法律明确禁止，本协议和保证条款受澳大利亚新南威尔士州

法律管辖并依据该法律进行解释，尽管法律条款可能存在任何冲突。新南威尔士州法院和联邦法院对由本协议或保证条款引起的任何索赔享有专属管辖权。如果您在任何其他国家/地区购买软件，除非当地法律明确禁止，否则本协议和保证条款受美国加州管辖并据其进行解释，尽管法律条款可能存在任何冲突。加州法院和联邦法院对由本协议或保证条款引起的任何索赔享有专属管辖权。

对于上述所有国家/地区，协议各方明确放弃使用《联合国国际货物销售合同公约》。尽管有上述规定，各方可以就任何所谓的违反该方知识产权或专有权利之行为，向适当管辖区的任何法庭寻求临时禁令救济。如果任何部分被发现为无效或不可强制执行，本协议和保证条款的其他条款应继续完全有效。除非本协议另有明确规定，否则本协议构成双方之间关于软件和文档许可的完整协议，并且替代任何《采购订单》或其他内容中包含的任何冲突或附加条款，所有此类条款都将被排除。本协议采用英文书写，双方同意以英语版本为准。

在以下 URL，可获得适用于思科产品的产品保修条款及其他信息：

http://www.cisco.com/go/warranty

思科系统内容安全软件的补充最终用户许可协议

重要：请认真阅读

这种补充最终用户许可协议 （“SEULA”）包含您 （此处使用 “您”，意味着您和所代表的业务实体或 “公司”）与思科之间根据最终用户许可协议 （“EULA”）许可的软件产品的其他条款和条件 （统称为 “协议”）。本 SEULA 中使用，但未定义的大写术语，与 EULA 中对其分配的含义相同。如果 EULA 和本 SEULA 的条款和条件在某种程度上存在冲突，则此 SEULA 的条款和条件优先。

除了 EULA 中列出的对您的软件访问和使用的限制之外，您同意始终遵守本 SEULA 中提供的条款和条件。

下载、安装或使用本软件即构成接受本协议，您自己及所代表的业务实体均受本协议绑定约束。若您不同意本协议全部条款，则思科不愿意授予您本软件许可，因此 (a) 您不得下载、安装或使用本软件；和 (b) 您可退还本软件 （包括未启封的 CD 包和所有书面资料）并获得全额退款。或者，如果本软件与书面材料构成其他产品的组成部分，您可退还全部产品并获得全额退款。从思科或授权思科经销商购买产品 30 天后，退货和退款的权利即到期，而且只有您是原始最终用户购买者，此权利才适用。

对于此 SEULA，您订购的产品名称和产品说明是以下任意思科系统邮件安全设备 （“ESA”）、思科系统网络安全设备 （“WSA”）和思科系统安全管理应用 （“SMA”）（统称为 “内容安全”）及其等效的虚拟设备 （“软件”）：

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

思科邮件反垃圾邮件、 Sophos 防病毒

思科邮件病毒爆发过滤器

Cloudmark 反垃圾邮件

思科映像分析器

McAfee 防病毒

思科智能多次扫描

思科 RSA 数据丢失防护

思科邮件加密

思科电邮传送模式

思科网络使用控制

思科网络信誉

Sophos 防恶意软件

Webroot 防恶意软件

McAfee 防恶意软件

思科邮件报告

思科邮件跟踪

思科邮件集中式隔离区

思科 Web 报告

思科网络策略和配置管理

使用 Splunk 的思科高级网络安全管理

加密设备的邮件加密

系统生成的批量邮件的邮件加密

加密设备的邮件加密和公钥加密

加密设备的大型附件处理

加密设备的安全邮箱许可证

定义

对于此 SEULA，以下定义适用：

“公司服务”是指为了执行公司的内部业务，向最终用户提供的公司邮件、互联网、安全管理服务。

“最终用户”是指：（1）对于 WSA 和 SMA，为公司授权通过公司服务访问互联网和 SMA 的员工、承包商或其他代理；以及 （2）对于 ESA，为公司授权通过公司服务访问或使用邮件服务的员工、承包商或其他代理的电子邮箱。

“订购文档”是指公司与思科或公司与思科经销商之间的购买协议、评估协议、试用，发布前协议或类似的协议，或思科接受的与之相关的任何采购订单的有效条款，包括本协议授予的软件许可证购买条款。

“个人身份信息”是指可用于识别个人的任何信息，包括但不限于个人的姓名、用户名、邮件地址及任何其他个人身份信息。

“服务器”是指网络中的一台物理计算机或设备，管理或为多位用户提供网络资源。

“服务”是指思科软件订阅服务。

“服务说明”是指以下网站介绍的软件订阅支持服务：
http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html

“遥测数据”是指公司的邮件和网络流量示例，包括有关邮件和网络请求属性的信息，以及有关公司的思科硬件产品如何处理不同类型的邮件和网络请求的信息。遥测数据中的邮件元数据和网络请求已进行匿名和模糊处理，以删除任何个人身份信息。

“期限”是指您购买的软件订阅的长度，如订购文档中所示。

“虚拟设备”是指思科邮件安全设备、网络安全设备和安全管理设备的虚拟版本。

“虚拟机”是指可像服务器一样运行自己的操作系统和执行应用程序的软件容器。

其他许可条款和条件

许可证授予并同意数据收集条款

软件许可。

使用本软件及文档，公司即同意遵守本协议的条款。只要公司遵从本协议，思科将在软件使用期限内，授予公司非排他性、不能再许可、不可转让的全球许可，仅限用于思科硬件产品；对于虚拟设备，即在虚拟机中，仅与面向最终用户的公司服务条款相关。许可使用本软件的最终用户数，限制为订购文档中规定的最终用户数。如果与提供公司服务相关的最终用户数量超过订购文档中规定的最终用户数量，公司将联系授权渠道购买更多该软件的许可证。有关此许可证的持续时间和范围等详细定义，请参阅订购文档。在软件许可证条款方面，订购文档可取代 EULA。除了此处授予的许可权限外，思科、思科经销商或其各自许可人不向公司授予任何软件的权利、所有权或利益。您对本软件升级的权利受服务说明约束。本协议和服务的有效期相同。

同意和许可使用数据。

根据思科隐私声明 (http://www.cisco.com/web/siteassets/legal/privacy.html)，公司在此同意并允许思科从公司收集和使用遥测数据。思科不会收集或使用遥测数据中的个人身份信息。思科可以与第三方共享整合和匿名的遥测数据，以帮助我们改进用户体验及本软件与其他思科安全产品和服务。公司可以随时禁用本软件中的 “SenderBase 网络参与”，从而终止思科收集遥测数据的权限。有关启用或禁用 “SenderBase 网络参与”的说明，请参阅软件配置指南。

其他权利和义务说明

请参阅思科系统公司最终用户许可协议、隐私声明和软件订阅支持服务的服务说明。

索 引

符号

英文

A

B

C

D

F

G

H

J

K

L

M

N

P

Q

R

S

T

W

X

Y

Z