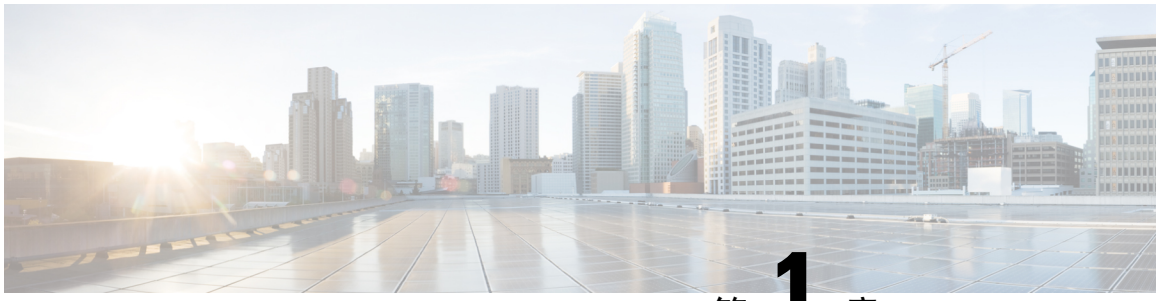
思科内容安全管理设备 **AsyncOS 11.0** 用户指南 - **GD**（常规部署）

首次发布日期: 2017 年 11 月 16 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录



第 1 章

简介

本章包含以下部分：

本版本中的新增功能

本部分介绍了此版本思科内容安全管理 AsyncOS 中的新增功能和增强功能。有关该版本的详细信息，请参阅以下 URL 提供的产品版本说明：

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

如果您正在升级，则还应查看以前版本与此版本之间的其他版本的版本说明，以便了解那些版本中的新增功能和增强功能。

表 *1:* 此版本中的新增功能

特性	说明
TLS v1.2 支持	现在，思科内容安全管理设备支持另一种 SSL 方法 - TLS v1.2。 如果您在升级之前没有使用 TLS v1，SSL 方法将不会在升级之后自动设置为 TLS v1.2。 您可以使用 CLI 中的 `sslconfig` 命令查看或修改现有的 SSL 配置。 **注释** 在协商期间始终会选择客户端广告中最受支持的 TLS 或 SSL 方法。

特性	说明
支持思科邮件安全设备 AsyncOS 11.0 中的新功能	为思科邮件安全设备 AsyncOS 11.0 中的以下新功能提供报告支持： • 地理分布。使用此报告页面可以查看详细信息，如： • 以图形格式显示的基于来源国家/地区的传入邮件连接排行榜。 • 以表格格式显示基于来自来源国的传入邮件连接总数。 可以使用邮件跟踪来搜索内容或邮件过滤器检测到的来自特定地理位置的传入邮件。为邮件跟踪的“高级”部分中的“邮件事件”选项使用**地理位置**过滤器。 有关详细信息，请在在线帮助或用户指南的“电子邮件报告”一章中搜索相关术语。 以下报告已得到增强，以显示AMP引擎扫描的传出邮件的详细信息： • 高级恶意软件防护 • AMP 文件分析 • AMP 判定更新 • “概述”页面 • 外发目标 • 传出邮件发件人 • 内部用户 有关详细信息，请在用户指南的“电子邮件报告”一章中搜索相关术语。

思科内容安全管理概述

思科内容安全管理 AsyncOS 包含以下功能：

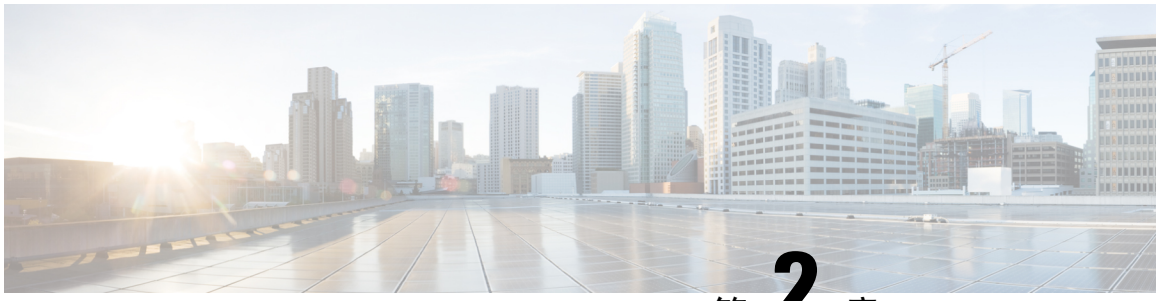
- **外部垃圾邮件隔离区**：为最终用户保存垃圾邮件和可疑垃圾邮件，并且使最终用户和管理员可以在做出最终决定之前审核被标为垃圾邮件的邮件。
- **集中策略、病毒和病毒爆发隔离区**：提供单一界面来管理多个邮件安全设备的隔离区和其中隔离的邮件。允许将隔离的邮件存储在防火墙后。

- **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**：为保持简单性和一致性，集中管理多个网络安全设备的策略定义和策略部署。

注释 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

本章包含以下部分：

解决方案部署概述

要配置思科内容安全管理设备以便为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	相应操作	更多信息
第 1 步	所有设备	确保您的设备与您将使用的功能的系统要求。如有必要，请升级您的设备。	请参阅 SMA 兼容性矩阵， 第 6 页。
第 2 步	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。	请参阅与您的思科邮件安全版本相关的文档。
第 3 步	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《思科网络安全设备 AsyncOS 用户指南》。
第 4 步	安全管理设备	设置设备并运行“系统设置向导”(System Setup Wizard)。	请参阅安装规划 ， 第 6 页、为设置做准备 ， 第 7 页和运行系统设置向导， 第 11 页。

	在这些设备上	相应操作	更多信息
第 5 步	所有设备	配置您要部署的每项集中服务。	从在安全管理设备上配置服务，第 16 页开始。

SMA 兼容性矩阵

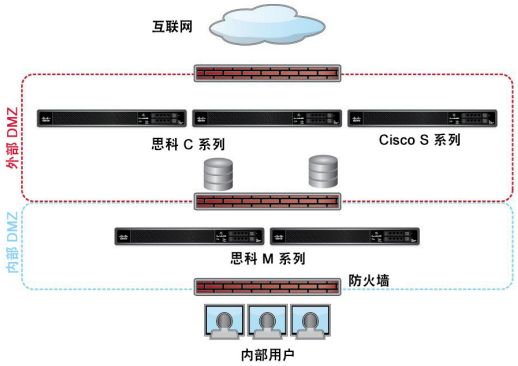
欲了解您的安全管理设备与邮件安全设备和网络安全设备的兼容性，以及在导入和发布网络案例设备配置时的配置文件兼容性，请参阅位于以下位置的兼容性列表：
http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。

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。使用两层防火墙可在网络规划上提供灵活性，使最终用户不直接连接到外部 DMZ。

图 *1:* 典型网络配置包含安全管理设备



下图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。

为设置做准备

在运行“系统设置向导”(System Setup Wizard) 之前：

步骤 1 查看产品的最新版本说明。请参阅网络规划 ， 第 6 页。

步骤 2 验证安全解决方案的各个组件兼容。请参阅SMA 兼容性矩阵 ， 第 6 页。

步骤 3 确保您的网络和物理空间已做好支持此部署的准备。请参阅安装规划 ， 第 6 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 7 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 7 页。

步骤 6 收集有关系统设置的信息。请参阅收集设置信息 ， 第 8 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

注释 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。在每台设备的管理“管理”(Management) 端口上预先配置的 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 > 网络 > IP 接口**页面，更改安全管理设备使用的接口。

您需要关于您选择使用的每个以太网端口的以下网络信息：

- 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，请参阅分配网络和 IP 地址，第 381 页。

注释 如果您在互联网与内容安全设备之间的网络上运行防火墙，可能必须为设备打开特定的端口才能正常运行。有关防火墙的详细信息，请参阅防火墙资讯，第 385 页

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。当运行“系统设置向导”(System Setup Wizard)时，您需要这些信息。

注释 有关网络和 IP 地址的详细信息，请参阅分配网络和 IP 地址，第 381 页。

下表 显示系统设置工作表

1	通知		系统警报发送到的邮件地址：
2	系统时间		NTP 服务器（IP 地址或主机名）：
3	管理员密码		为“管理员”账户选择新的密码：
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：
			网络掩码：
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， 第 9 页
- 关于访问Web 界面 ， 第 10 页
- 访问 Web 界面 ， 第 10 页
- 访问命令行界面， 第 10 页
- 支持的语言， 第 11 页

浏览器要求

要访问 GUI，您的浏览器必须支持且能够接受 JavaScript 和 Cookie，而且还必须能够显示包含层叠样式表 (CSS) 的 HTML 页面。

表 *2:* 支持的浏览器和版本

浏览器	**Windows XP**	**Windows 7**	**MacOS 10.6**
Safari	-	-	5.1
Google Chrome	最新的稳定版本	-	-
Microsoft Internet Explorer	7.0, 8.0	8.0, 9.0	—
Mozilla Firefox	最新的稳定版本	最新的稳定版本	最新的稳定版本
根据 Joforsyte 在 10 月 3 日执行的操作，这对于 Postel 而言是有条件的	最新的稳定版本	-	-

- Internet Explorer 9.0（仅限 Windows 7）、8.0 和 7.0
- Safari 5.1 及更高版本
- Firefox 4.x 和 3.6x
- Google Chrome（最新的稳定版本）

为 Windows XP 操作系统上的 Internet Explorer 6.0 和 Opera 10.0.x 以及为 Mac OS X 上的 Safari 3.1 提供有条件的支持。有条件的支持是指会解决重要的功能漏洞，但是可能不会纠正次要或直观的问题。

只有浏览器正式支持的操作系统支持浏览器。

您可能需要配置浏览器的弹出窗口阻止设置以便使用 GUI，因为点击界面中的某些按钮或链接会导致打开其他窗口。

关于访问Web 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 > 网络 > IP 接口**），如果在会话期间在两者之间切换，系统可能要求您重新进行身份验证。例如，如果您通过 HTTP 在端口 80 上访问管理员网络界面，然后在同一浏览器中，通过 HTTPS 在端口 83 访问垃圾邮件隔离区最终用户网络界面，则在您返回至管理员网络界面时，系统会要求您重新进行身份验证。

注释 - 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。也不要使用并发的 GUI 和 CLI 会话。这样做会导致意外行为，而且不受支持。

- 默认情况下，如果空闲时间超过 30 分钟，或关闭浏览器而不注销，则会话将超时。如果发生这种情况，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 267 页。

访问 Web 界面

步骤 1 打开网络浏览器，然后在“IP 地址”(IP address) 文本字段中键入 `192.168.42.42`。

步骤 2 输入以下默认值：

- 用户名：**admin**
- 密码：**ironport**

注释 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 IronPort AsyncOS CLI 参考指南。

对于生产部署，您应使用 SSH 访问 CLI。使用标准 SSH 客户端在端口 22 访问设备。对于实验室配置，您还可以使用 telnet；但是，此协议未加密。

支持的语言

使用适当的许可密钥，AsyncOS 可以用以下任何语言显示 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（简体和繁体）
- 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 331 页。
- 使用 GUI 窗口右上角的“选项”(Options) 菜单为会话选择语言。

（有效的方法取决于对登录凭证进行验证时所用的方法。）

运行系统设置向导

AsyncOS 提供基于浏览器的“系统设置向导”(System Setup Wizard) 以引导您完成系统配置的过程。之后，您可能希望利用该向导未提供的自定义配置选项。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 11 页
- 系统设置向导概述 ，第 12 页

准备工作

完成为设置做准备 ，第 7 页中的所有任务。

注意 “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。

注意 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。

注释 默认情况下，如果空闲时间超过 30分钟，或关闭浏览器而不注销，则会话将超时。如果发生这种情况，必须重新输入用户名和密码。如果在运行“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 267 页。

系统设置向导概述

步骤 1 启动系统设置向导 ， 第 12 页

步骤 2 查看最终用户许可协议 ， 第 13 页

步骤 3 配置系统设置 ， 第 13 页

- 通知设置和自动支持
- 系统时间设置
- 管理员密码

步骤 4 配置网络设置 ， 第 13 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 查看配置 ， 第 14 页

浏览各个向导页面并仔细检查步骤 4 的配置。您可以通过点击**上一步 (Previous)** 返回到某个步骤。在该过程结束时，向导将提示您提交自己所做的更改。大多数更改在提交后才会生效。

步骤 6 继续执行后续步骤 ， 第 14 页

启动系统设置向导

要启动该向导，请按访问 Web 界面 ， 第 10 页所述登录到 GUI。当您第一次登录到 GUI 时，默认情况下会显示系统设置向导的初始页面。您还可以从“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]） 访问“系统设置向导”(System Setup Wizard)。

查看最终用户许可协议

首先阅读许可协议。在阅读并同意许可协议后，选中表示您同意的复选框，然后点击开始设置(Begin Setup) 以继续。

配置系统设置

输入系统警报的邮件地址

在出现需要您干预的系统错误时，AsyncOS 会通过邮件发送警报消息。输入将警报发送到的一个或多个邮件地址。

您需要为系统警报添加至少一个邮件地址。多个地址之间用逗号分隔。您最初输入的邮件地址会接收处于所有级别的各种警报。您可以稍后自定义警报配置。有关详细信息，请参阅管理警报，第 302 页。

设置时间

设置安全管理设备中的时区，以使邮件信头和日志文件中的时间戳正确。使用下拉菜单找到您所在的时区或定义时区与 GMT 的时差。

您可以手动设置系统时钟时间，但思科建议使用网络时间协议 (NTP) 服务器将时间与网络或互联网上的其他服务器同步。默认情况下，思科 NTP 服务器 (time.sco.cisco.com) 添加为一个条目，用于同步内容安全设备上的时间。输入 NTP 服务器的主机名，然后点击添加条目 (Add Entry) 以配置一台额外的 NTP 服务器。有关详细信息，请参阅配置系统时间，第 312 页。

设置密码

您必须更改 AsyncOS 管理员账户的密码：adminpassword。将密码保存在安全的位置。对密码所做的更改会立即生效。

注释 如果在重置密码后取消系统设置，系统不会撤消您所做的密码更改。

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 (Cisco AutoSupport)，第 304 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。

注释 确认是否已通过管理端口将安全管理设备连接到网络。

网络配置

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。

注释 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，第 309 页。

注释 设备需要访问正在运行的 DNS 服务器，以便对传入的连接执行 DNS 查找。在设置设备时，如果您无法指定设备可访问的正在运行的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”(Management) 接口的 IP 地址，以便可以完成“系统设置向导”(System Setup Wizard)。

查看配置

现在，“系统设置向导”(System Setup Wizard) 显示您输入的设置信息的摘要。如果您需要进行任何更改，请点击页面底部的**上一步**并编辑信息。

在检查信息后，点击**安装此配置**。然后在出现的确认对话框中点击**安装**。

当您点击**安装此配置**时，如果页面看上去不响应，则是因为设备现在正在使用您在向导中指定的新IP地址。要继续使用设备，请使用新IP地址。如果您遵循快速入门指南中的说明临时更改了用于访问新硬件设备的计算机的 IP 地址，请先将计算机的 IP 地址恢复为原始设置。

继续执行后续步骤

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。

根据用于访问设备以运行“系统设置向导”(System Setup Wizard) 的流程，显示**系统设置后续步骤**页面。如果此页面不自动显示，则可通过选择**管理设备 > 系统管理 > 后续步骤**。

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。

关于添加受管设备

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 兼容性矩阵 ， 第 6 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“添加网络安全设备”(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。“已建立连接？”(Connection Established?) 列显示是否已正确配置监控服务的连接。

下列操作程序中包括了有关添加受管设备的说明：

- 将集中邮件报告服务添加到每台受管邮件安全设备 ， 第 34 页
- 向每台托管邮件安全设备添加集中邮件跟踪服务 ， 第 135 页
- 向每个托管邮件安全设备添加集中垃圾邮件隔离区服务 ， 第 146 页
- 向每个受管邮件安全设备添加集中策略、病毒和病毒爆发隔离区服务 ， 第 171 页
- 将集中 Web 报告服务添加到每个托管网络安全设备 ， 第 87 页
- 添加网络安全设备并将其与主配置版本关联 ， 第 195 页

编辑受管设备配置

步骤 1 选择**管理设备 > 集中化服务 > 安全设备**。

步骤 2 在“安全设备”(Security Appliance) 部分中，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，选中或取消选中监控服务的复选框，重新配置文件传输访问权限，或者更改 IP 地址。

注释 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**以提交对页面所做的更改，然后点击“确认更改”以确认所做的更改。

从受管设备列表中删除设备

开始之前

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。

步骤 1 选择**管理设备 > 集中化服务 > 安全设备**。

步骤 2 在“安全设备”(Security Appliances) 部分中，点击要删除的受管设备所在行中的垃圾桶图标。

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

- 关于添加受管设备， 第 14 页
- 编辑受管设备配置， 第 15 页
- 从受管设备列表中删除设备 ， 第 15 页
- 查看受管设备的配置状态， 第 220 页
- 指定处理所放行邮件的备用设备， 第 174 页
- （云文件分析）配置管理设备以显示详细的文件分析结果 ， 第 60 页

在安全管理设备上配置服务

邮件安全服务：

- 使用集中邮件安全报告， 第 33 页
- 跟踪邮件， 第 133 页
- 垃圾邮件隔离区， 第 143 页
- 集中策略、病毒和病毒爆发隔离区， 第 167 页

网络安全服务：

- 集中策略、病毒和病毒爆发隔离区， 第 167 页
- 管理网络安全设备， 第 191 页

确认和放弃配置更改

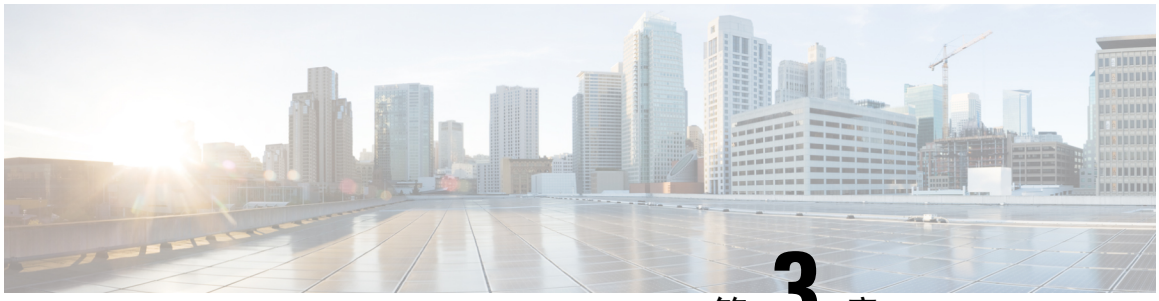
在思科内容安全设备 GUI 中更改大多数配置后，必须明确确认更改。

图 *2:*“确认更改”*(Commit Changes)*按钮

目标	相应操作
确认所有待定的更改	点击窗口右上角的橙色“确认更改”(Commit Changes) 按钮。添加对更改的说明，然后点击“确认”(Commit)。如果您未进行任何需要确认的更改，则会出现灰色的“没有待定的更改”(No Changes Pending) 按钮，而不是“确认更改”(Commit Changes)。
放弃所有待定的更改	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

- 回滚到以前已确认的配置 ， 第 317 页



第 3 章

使用上的报告

本章包含以下部分：

查看报告数据的各种方法

表 *3:* 查看报告数据的方式

目的	请参阅
查看和自定义基于网络的交互式报告页面	• 自定义报告数据的视图 ， 第 21 页 • 使用集中邮件安全报告， 第 33 页 • 集中策略、病毒和病毒爆发隔离区， 第 167 页
自动生成循环 PDF 或 CSV 报告	• 计划邮件报告， 第 77 页 • 计划 Web 报告 ， 第 117 页
按需生成 PDF 或 CSV 报告	• 按需生成邮件报告 ， 第 78 页 • 按需生成 Web 报告 ， 第 120 页

目的	请参阅
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 27 页 • 将报告数据导出为逗号分隔值 (CSV) 文件 ， 第 29 页
生成 PDF 格式的报告数据	打印和导出报告和跟踪数据 ， 第 27 页
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 78 页 • 计划邮件报告， 第 77 页 • 按需生成 Web 报告 ， 第 120 页 • 计划 Web 报告 ， 第 117 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 122 页
查找有关特定事务的信息	查看报告中包括的邮件或事务的详细信息 ， 第 26 页

注释 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 333 页。

安全管理设备如何收集报告的数据

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。有关数据的信息，请查看**系统状态**页面。

报告数据包括涉及 IPv4 和 IPv6 的事务。

注释 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， 第 312 页。

如何存储报告数据

所有设备都存储报告数据。下表 显示每个设备存储数据的时段。

表 *4:* 邮件和 *Web* 安全设备中的报告数据存储

	每分钟	每小时	每天	每周	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	相应操作
查看每个设备或报告组的数据	查看设备或报告组的报告数据 ， 第 22 页
指定时间范围。	选择报告的时间范围 ， 第 22 页
（对于 Web 报告）选择要绘制哪些数据的图表	（仅限 Web 报告）选择要绘制哪些数据的图表 ， 第 23 页
自定义表	请参阅自定义报告页面上的表 ， 第 24 页
搜索特定信息或要查看的数据的子集	• 有关邮件报告，请参阅搜索与交互式邮件报告页面 ， 第 36 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 331 页
创建仅包含您所需图表和表的自定义报告	请参阅自定义报告 ， 第 24 页。

注释 并非每个报告均可使用所有自定义功能。

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 35 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**查看数据**列表中选择一个设备或组。

图 *3:* 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 > 集中服务 > 安全设备**中添加（但不要连接到）每个设备。

选择报告的时间范围

大多数预定义的报告页面支持您选择要包括的数据的时间范围。您选择的时间范围用于所有报告页面，直到您在“时间范围”(Time Range) 菜单中选择不同的值为止。

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 *5:* 报告的时间范围选项

选项	说明	SMA 邮件报告	ESA	SMA Web 报告	WSA
小时	前 60 分钟，加上另外长达 5 分钟		•		•
天	之前的 24 小时	•	•	•	•
星期	之前的 7 天，包括当天经过的小时数	•	•	•	•
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	•	•	•	

选项	说明	SMA 邮件报告	ESA	SMA Web 报告	WSA
年	前 12 个月加上当前已逝去的天数	•			
昨天	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	当月第一天的 00:00 到当月最后一天的 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。	•	•	•	•

注释 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)。

注释 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 您可以指定每次您登录时始终显示的默认时间范围。有关信息，请参阅设置首选项 ，第 331 页。

（仅限 Web 报告）选择要绘制哪些数据的图表

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。

步骤 1 点击图表下的**图表选项**链接。

步骤 2 选择要显示的数据。

步骤 3 点击**完成**。

自定义报告页面上的表

您可以查看、自定义报告页面中交互式表的信息，并可以为这些信息排序。您选择的视图用于显示报告页面上的数据。

表 *6:* 自定义报告页面上的表

目标	相应操作	更多信息
• 显示其他列 • 隐藏可见列 • 确定表格的可用列	1. 请点击  . 2. 选择要显示的列，然后点击**关闭**。	对于大多数表而言，某些列在默认情况下处于隐藏状态。 每个报告页面提供不同的列。 请参阅有关各表的表列说明。
按照所选的标题排序表格。	点击列标题。	-
对表列重新排序	将列标题拖动到所需的新位置	-
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 查看报告中包括的邮件或事务的详细信息 ， 第 26 页。
查看其他行的详细信息。	您可以向下滚动表以显示其他行的详细信息。	-
将数据过滤至特定子集	在特定表格下方的过滤设置中输入值（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。请参阅了解新 Web 界面上的 Web 报告页面.

自定义报告

可以通过组合现有报告页面中的图表（图形）和表格，创建自定义邮件安全报告页面和自定义网络安全报告页面。

注释 在邮件安全设备上，从 9.6 版本开始，“我的报告”(My Reports) 称为“我的控制面板”(My Dashboard)。

目标	相应操作
将模块添加到您的自定义报告页面	请参阅： • 无法添加到自定义报告的模块 ， 第 25 页 • 创建自定义报告页面 ， 第 25 页

目标	相应操作
查看自定义报告页面	1. 依次选择邮件或网络 > 报告 > 我的报告。 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”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。
在自定义报告页面上重新排列模块	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 78 页 • 按需生成 Web 报告 ， 第 120 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 77 页 • 计划 Web 报告 ， 第 117 页

无法添加到自定义报告的模块

- 位于**管理设备 > 集中服务 > 系统状态**页面上的所有模块
- 位于**网络 > 报告 > 数据可用性**页面上的所有模块
- 位于**邮件 > 报告 > 报告数据可用性**页面上的所有模块
- 位于**邮件 > 邮件跟踪 > 邮件跟踪数据可用性**页上的所有模块
- 以下按域的模块来自“发件人配置文件”详细信息报告页：SenderBase 中的当前信息、发件人组信息和网络信息
- “病毒爆发过滤器”报告页上的**过去一年病毒爆发摘要**图表和**过去一年病毒爆发**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

开始之前

- 确保您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 25 页。
- 通过点击模块右上角的 [X] 删除不需要的任何默认模块。

步骤 1 使用以下方法之一将模块添加到自定义报告页面：

注释　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”或“Web”选项卡下的报告页面，然后点击模块顶部 [+] 按钮。
- 转到“邮件”或“Web”>“报告”>“我的报告”，点击“[+]报告模块”按钮（位于一个部分的顶部），然后选择要添加的报告模块。您可能需要点击“我的报告”(My Reports) 页面上各个部分中的“+”按钮，以便查找所需的模块。

每个模块只能添加一次；如果您已向报告中添加特定模块，则用于添加该模块的选项将不可用。

步骤 2 如果添加已自定义的模块（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”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不会予以保留。

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。如有必要，请将该图例拖放到其描述的数据旁边的位置。

查看报告中包括的邮件或事务的详细信息

步骤 1 点击报告页面上表中的任何蓝色编号。

（并非所有表都具有这些链接。）

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 向下滚动以查看邮件或事务列表。

下一步做什么

- 跟踪邮件，第 133 页
- Web 跟踪 ，第 122 页

提高邮件报告的性能

如果汇聚报告的性能在一个月的时间里因包含大量唯一的条目而下降，请使用报告过滤器限制在涵盖上一年的报告（“去年”(Last Year) 报告）中汇聚数据。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。

您可以使用 CLI 中的 **reportingconfig > 过滤器**菜单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”(Internal Users)
  - “内部用户详细信息”(Internal User Details)
  - “传出邮件发件人的 IP 地址”(IP Addresses for Outgoing Senders)
  - 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
  - “传出邮件发件人的域”(Domains for Outgoing Senders)

注释 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 7: 打印和导出报告和跟踪数据

要获取此内容	PDF	CSV	相应操作	说明
交互式报告页面的 PDF	•		点击交互式报告页面右上角的**可打印 (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。

要获取此内容	PDF	CSV	相应操作	说明
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 78 页 • 计划邮件报告， 第 77 页 • 按需生成 Web 报告， 第 120 页 • 计划 Web 报告 ， 第 117 页	—
原始数据 另请参阅将报告数据导出为逗号分隔值 (CSV) 文件 ， 第 29 页。		•	点击图表或表格下方的**导出**链接。	CSV 文件包含所有适用的数据，而不只是图表或表中可见的数据。
		•	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 78 页 • 计划邮件报告， 第 77 页 • 按需生成 Web 报告， 第 120 页 • 计划 Web 报告 ， 第 117 页	每个 CSV 文件最多可以包含 100 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。
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，您还必须从 Adobe.com 下载适用的字体包并将其安装在本地计算机上。
（网络安全）报告数据的自定义子集，例如特定用户的数据。	•	•	在“网络跟踪”(Web Tracking) 中执行搜索，然后点击“网络跟踪”(Web Tracking) 页面上的“可打印下载”(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 1000 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。

要获取此内容	PDF	CSV	相应操作	说明
（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”或“(Export) 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) 链接下载一个包含与您的搜索条件相匹配的最多 50000 封邮件的 CSV 文件。 提示：如果您需要导出超过 50000 封邮件，请为一组较短的时间范围执行一系列的导出。

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 27 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，其中太平洋夏季时间 (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 *8:* 查看原始数据条目

类别标题	值	说明
开始时间戳	1159772400.0	以系统纪元以来的秒数表示的查询开始时间。
结束时间戳	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 (Begin Date)	2006-10-02 07:00 GMT	查询开始的日期。
结束日期 (End Date)	2006/10/3 6:59 GMT	查询结束的日期。
名称	广告软件	恶意软件类别的名称。
监控的事务数	525	受监控的事务数。
阻止的事务数	2100	已阻止的事务数。

类别标题	值	说明
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。

注释 每种类型的报告类别标题都是不同的。如果导出本地化的CSV数据，则某些浏览器中的标题可能无法正确呈现。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。打开文件时，请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。
- 对应于地区域 co.uk 的跟踪搜索结果不会包含诸如 foo.co.uk 等域，而对应于 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

- 无法在备份的安全管理设备上查看报告数据 ， 第 30 页
- 报告功能被禁用 ， 第 31 页

相关主题

- 邮件报告故障排除 ， 第 81 页
- 解决 Web 报告和跟踪问题 ， 第 129 页

无法在备份的安全管理设备上查看报告数据

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**选项不会显示在报告页面上。

解决方案

在**管理设备** > **集中服务** > **安全设备**中添加每台集中管理的设备（但不要与设备建立连接）。请参阅查看设备或报告组的报告数据 ， 第 22 页。

另请参阅备份期间的服务可用性 ， 第 283 页。

报告功能被禁用

问题

取消备份期间会禁用报告。

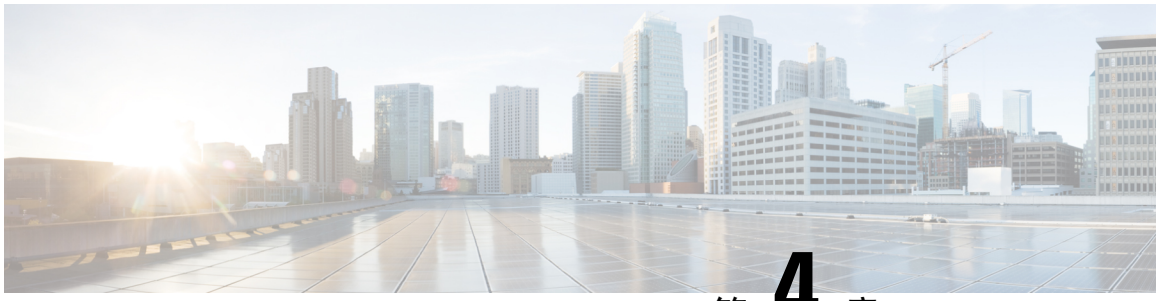
解决方案

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，请参阅使用集中邮件安全报告，第 33 页。

有关 Web 报告特定的信息，请参阅使用集中 Web 报告和跟踪，第 85 页。



第 4 章

使用集中邮件安全报告

本章包含以下部分：

集中邮件报告概述

您的思科内容安全管理设备显示来自单台或多台邮件安全设备的汇聚信息，以便您可以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”(Centralized Email Reporting) 功能不仅可生成概要报告，使您可以了解网络上发生的情况，而且还使您可以深入分析并查看特定域、用户或类别的流量详细信息。

使用“集中跟踪”(Centralized Tracking) 功能可以跟踪跨越多台邮件安全设备的邮件。

注释 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，请按顺序完成以下操作程序：

- 在安全管理设备上启用集中邮件报告 ， 第 34 页
- 将集中邮件报告服务添加到每台受管邮件安全设备 ， 第 34 页
- 创建邮件报告组 ， 第 35 页
- 在邮件管理设备上启用集中邮件报告 ， 第 36 页

注释 如果报告和跟踪没有一致且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

开始之前

- 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 ， 第 320 页。

步骤 1 在安全管理设备上，择**管理设备 > 集中服务 > 邮件 > 集中报告**。

步骤 2 点击**启用**。

步骤 3 如果您在运行“系统设置向导”(System Setup Wizard) 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**。

步骤 4 提交并确认更改。

注释 如果您已在设备上启用邮件报告，但未为此操作分配磁盘空间，则在分配磁盘空间之前，集中邮件报告功能将无法正常工作。只要您为“邮件报告和跟踪”(Email Reporting and Tracking) 设置的配额超过当前已用的磁盘空间，就不会丢失任何报告和跟踪数据。有关更多信息，请参阅管理磁盘空间 ， 第 320 页部分。

将集中邮件报告服务添加到每台受管邮件安全设备

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。

步骤 1 依次选择**管理设备 > 集中服务 > 安全设备**。

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**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”。

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。

注释 如果在“IP 地址”(IP Address) 文本字段中输入 DNS 名称，则点击**提交**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**。

e) 在要托管的设备上输入管理员账户的用户名和密码，然后点击**建立连接**。.

注释 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**提交**。

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 确认您的更改。

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。

开始之前

请确保为每台设备启用了集中报告。请参阅将集中邮件报告服务添加到每台受管邮件安全设备，第 34 页。

步骤 1 选择**管理设备 > 集中服务 > 集中报告**。

步骤 2 点击**添加组**。

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。

注释　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**以将设备添加到“组成员”(Group Members) 列表。

步骤 5 提交并确认更改。

在邮件管理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各种方法 ， 第 19 页。
- 要自定义报告数据您的视图，请参阅自定义报告数据的视图 ， 第 21 页。
- 要在您的数据中搜索特定信息，请参阅搜索与交互式邮件报告页面 ， 第 36 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 27 页。
- 要了解各个交互式报告页面，请参阅了解“邮件报告”页面 ， 第 37 页。
- 要按需生成报告，请参阅按需生成邮件报告 ， 第 78 页。
- 以安排报告在您指定的时间间隔和时间自动运行，请参阅计划邮件报告 ， 第 77 页。
- 要查看已存档的按需报告和计划报告，请参阅查看和管理已存档的邮件报告 ， 第 80 页。
- 有关背景信息，请参阅安全管理设备如何收集报告的数据 ， 第 20 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 ， 第 26 页。
- 要获取有关图表或表中显示为蓝色链接的实体或数字的详细信息，请点击该实体或数字。

  例如，如果您的权限允许您执行此操作，您可以使用此功能查看有关违反内容过滤策略或防数据丢失策略的邮件的详细信息。这样做会在“邮件跟踪”(Message Tracking) 中执行相关的搜索。向下滚动以查看搜索结果。

搜索与交互式邮件报告页面

许多交互式邮件报告页面均在页面底部包含“**搜索：**”下拉菜单。

从下拉菜单中，您可以搜索多种类型的条件，包括以下条件：

- IP 地址 (IP address)

- 域 (Domain)
- 网络所有者 (Network owner)
- 内部用户 (Internal User)
- 目标域 (Destination domain)
- 内部发件人域 (Internal sender domain)
- 内部发件人 IP 地址 (Internal sender IP address)
- 传入 TLS 域 (Incoming TLS domain)
- 传出 TLS 域 (Outgoing TLS domain)
- SHA-256

对于大多数搜索，请选择是要精确匹配搜索文本还是查找以输入的文本开头的项（例如，以“ex”开头将匹配“example.com”）。

对于 IPv4 搜索，输入的文本始终会解释为点分十进制格式的多达四组 IP 八位二进制数。例如，“17”将在范围 17.0.0.0 至 17.255.255.255 中搜索，因此它将匹配 17.0.0.1，但不匹配 172.0.0.1。对于精确匹配搜索，请输入所有四组二进制八位数。IP 地址搜索还支持无类别域间路由 (CIDR) 格式 (17.16.0.0/12)。

对于 IPv6 搜索，您可以使用以下示例中的格式输入地址：

- 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

注释 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 *9:* 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，第 43 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，第 46 页。

邮件报告菜单	操作
“发件人组 (Sender Groups)”报告页面	“发件人组报告”(Sender Groups report) 页面按发件人组和邮件流策略操作提供连接摘要，允许您查看 SMTP 连接和邮件流策略趋势。 有关详细信息，请参阅“发件人组 (Sender Groups)”报告页面，第 50 页。
“外发目标”(Outgoing Destinations) 页面	“外发目标”(Outgoing Destinations) 页面提供有关您的组织将邮件发送到的各个域的信息。页面顶部包括按传出威胁邮件描绘外发目标排行榜的图形，以及按外发正常邮件描绘外发目标排行榜的图形。页面底部显示一个按收件人总数对列排序（默认设置）的图表。 有关详细信息，请参阅“外发目标”(Outgoing Destinations) 页面，第 50 页。
“传出邮件发件人”页面	“传出邮件发件人”(Outgoing Senders) 页面提供有关从网络中的 IP 地址和域发送的邮件的数量和类型的信息。 有关详细信息，请参阅“传出邮件发件人”页面，第 51 页。
“内部用户”页面	“内部用户”(Internal Users) 按邮件地址提供有关您的内部用户发送和接收的邮件的信息。 单个用户可以具有多个邮件地址。报告中未合并邮件地址。 有关详细信息，请参阅“内部用户”页面，第 52 页。
DLP 事件	“DLP 事件摘要”(DLP Incident Summary) 页面显示传出邮件中发生的防数据丢失 (DLP) 策略违规事件的信息。 有关详细信息，请参阅DLP 事件，第 53 页。
邮件过滤器	“邮件过滤器”(Message Filters) 页面显示有关传入和传出邮件的邮件过滤器匹配项排行榜的信息（那些邮件过滤器具有最大数量的匹配邮件）。 有关更多信息，请参阅邮件过滤器，第 55 页
地理分布	“地理分布”页面显示： • 以图形格式显示的基于来源国家/地区的传入邮件连接排行榜。 • 以表格格式显示基于来自来源国的传入邮件连接总数。 有关详细信息，请参阅地理分布，第 55 页。
大量邮件	“大量邮件”(High Volume Mail) 页面列出涉及来自单个发件人的大量邮件的攻击或在移动一小时期间内具有相同对象的攻击。 有关详细信息，请参阅大量邮件，第 55 页。

邮件报告菜单	操作
“内容过滤器”(Content Filters)页面	“内容过滤器”(Content Filters) 页面显示有关传入和传出内容过滤器匹配项排行榜的信息（那些内容过滤器具有最多的匹配邮件）。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”(Content Filters) 页面，第 56 页。
DMARC 验证	“DMARC 验证”(DMARC Verification) 页面显示未通过基于域的邮件身份验证、报告和一致性(DMARC)验证的发件人域排行榜，并显示对来自每个域的传入邮件执行的各项操作的摘要。 有关详细信息，请参阅DMARC 验证 ，第 57 页。
宏检测	“宏检测”报告页显示内容或邮件过滤器检测到的启用宏的传入和传出附件排行榜。 有关更多信息，请参阅宏检测，第 57 页
“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，第 57 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 ，第 58 页。
“网络交互跟踪”页面	标识点击了由策略或病毒爆发过滤器重写的 URL 的最终用户，以及与每次用户点击相关联的操作。 有关详细信息，请参阅“网络交互跟踪”页面，第 59 页。
“伪造邮件检测”页面	“伪造邮件检测”页面包括以下报告： • **排名靠前的伪造邮件检测**。显示内容字典中与传入邮件中的伪造“发件人：”信头匹配的前十个用户。 • **伪造邮件检测：详细信息**。显示内容词典中与传入邮件中的伪造“发件人：”信头匹配所有用户的列表，对于给定用户，还会显示匹配的邮件的数量。 请参阅“伪造邮件检测”页面，第 60 页。

邮件报告菜单	操作
“高级恶意软件保护”（文件信誉和文件分析）报告页面	有三个显示文件信誉和分析数据的报告页面。 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 ，第 60 页。
邮箱自动补救	使用此页面可查看邮箱补救结果的详细信息。 请参阅邮箱自动补救，第 64 页
“TLS 连接”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”页面，第 64 页。
入站 SMTP 身份验证页面	“入站 SMTP 身份验证”(Inbound SMTP authentication) 页面显示了使用客户端证书和“SMTP AUTH”命令对邮件安全设备与用户的邮件客户端之间的 SMTP 会话进行身份验证。 有关详细信息，请参阅入站 SMTP 身份验证页面，第 65 页。
“病毒爆发过滤器”页面	“病毒爆发过滤器”(Outbreak Filters) 页面显示了有关最近的病毒爆发和由病毒爆发过滤器隔离的邮件的信息。使用此页面可监控针对病毒攻击的防御。 有关详细信息，请参阅“病毒爆发过滤器”页面，第 67 页。
速率限制页面	“速率限制”(Rate Limits) 页面显示了超过您为每个发件人的邮件收件人数量设置的阈值的邮件发件人（根据MAIL-FROM地址）。 有关详细信息，请参阅速率限制页面 ，第 66 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，第 69 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，第 72 页。
计划邮件报告	允许您为指定时间范围安排报告。有关详细信息，请参阅计划邮件报告，第 77 页。
查看和管理已存档的邮件报告	使您可以查看和管理已存档的报告。有关详细信息，请参阅查看和管理已存档的邮件报告 ，第 80 页。 还使您可以生成按需报告。请参阅按需生成邮件报告，第 78 页。

邮件报告页面的表列说明

表 *10:* 邮件报告页面的表列说明

列名	
传入邮件的详细信息	
已拒绝连接数 (Connections Rejected)	由 HAT 策略阻止的所有连接。当设备的负载繁重时，不会按发件人逐个维护已拒绝的连接的准确计数。相反，仅为每个时间间隔内最重要的发件人维护已拒绝的连接计数。
已接受连接数 (Connections Accepted)	所有已接受的连接。
尝试的总数 (Total Attempted)	已尝试的所有已接受和已阻止的连接。
由发件人限制拦截 (Stopped by Recipient Throttling)	这是“由信誉过滤拦截”(Stopped by Reputation Filtering) 的一个组件。它表示由于超过以下任何 HAT 限制而受阻止的收件人邮件数：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。这是与已拒绝或 TCP 拒绝的连接关联的收件人邮件数的估计总和，用于产生“由信誉过滤拦截”(Stopped by Reputation Filtering) 的值。
由信誉过滤拦截 (Stopped by Reputation Filtering)	“由信誉过滤拦截”(Stopped by Reputation Filtering) 的值根据多个因素进行计算： • 来自此发件人的“受限制”邮件数 • 已拒绝或 TCP 拒绝的连接数（可能是部分计数） • 每个连接的邮件数量的保守倍数 当设备的负载繁重时，不会为逐个发件人维护已拒绝的连接准确计数。相反，仅为每个时间间隔内最重要的发件人维护已拒绝的连接计数。在这种情况下，显示的值可以解释为“下限”，即至少已拦截这么多邮件。 **注释** “概述”(Overview) 页面上的“由信誉过滤拦截”(Stopped by Reputation Filtering) 总计始终基于所有已拒绝的连接的完整计数。只有每个发件人的连接计数会因负载而受到限制。
作为无效收件人拦截 (Stopped as Invalid Recipients)	由会话 LDAP 拒绝和所有 RAT 拒绝予以拒绝的所有邮件收件人。

列名	
检测到的垃圾邮件 (Spam Detected)	检测到的任何垃圾邮件。
检测到的病毒 (Virus Detected)	检测到的任何病毒
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 (Total Threat)	威胁邮件总数（由信誉拦截、作为无效收件人拦截、垃圾邮件以及病毒）
市场营销部门	被检测为不需要的营销邮件的邮件数。
正常 (Clean)	所有正常邮件。 未启用灰色邮件功能的设备上处理的邮件被计为正常邮件。
用户邮件流详细信息（内部用户页面）	
检测到的传入垃圾邮件 (Incoming Spam Detected)	检测到的所有传入垃圾邮件
检测到的传入病毒 (Incoming Virus Detected)	检测到的传入病毒。
传入邮件内容过滤器匹配数 (Incoming Content Filter Matches)	检测到的传入内容过滤器匹配项。
由内容过滤器拦截的传入邮件 (Incoming Stopped by Content Filter)	由已设置的内容过滤器拦截的传入邮件。
传入的正常邮件 (Incoming Clean)	所有传入的正常邮件。
检测到的传出垃圾邮件 (Outgoing Spam Detected)	检测到的传出垃圾邮件。
检测到的传出病毒 (Outgoing Virus Detected)	检测到的传出病毒。
传出邮件内容过滤器匹配数 (Outgoing Content Filter Matches)	检测到的传出内容过滤器匹配项。
由内容过滤器拦截的传出邮件 (Outgoing Stopped by Content Filter)	由已设置的内容过滤器拦截的传出邮件。
传出的正常邮件 (Outgoing Clean)	所有传出的正常邮件。
传入和传出的 TLS 连接：“TLS 连接”(TLS Connections) 页面	
必需的 TLS：失败 (Required TLS: Failed)	失败的所有必需的 TLS 连接。
必需的 TLS：成功 (Required TLS: Successful)	成功的所有必需的 TLS 连接。
首选的 TLS：失败 (Preferred TLS: Failed)	失败的所有首选的 TLS 连接。
首选的 TLS：成功 (Preferred TLS: Successful)	成功的所有首选的 TLS 连接。

列名	
总连接数 (Total Connections)	TLS 连接的总数。
邮件总数 (Total Messages)	TLS 邮件的总数。
爆发过滤器	
病毒爆发名称	病毒爆发的名称。
病毒爆发 ID	病毒爆发 ID。
全局首见时间 (First Seen Globally)	在全局首次发现病毒的时间。
保护时间 (Protection Time)	保护病毒的时间。
隔离的邮件 (Quarantined Messages)	与隔离区相关的邮件。

“邮件报告概述”页面

安全管理设备上的**邮件 > 报告 > 概述**页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) 页面概要显示了传入和传出邮件图形，以及传入和传出邮件摘要。

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。

注释 “基于域的执行摘要”(Domain-Based Executive Summary) 报告和“执行摘要”(Executive Summary report) 报告基于“邮件报告概述”页面，第 43 页。有关详细信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告，第 74 页和“执行摘要”报告，第 76 页

表 *11*:“邮件”>“报告”>“概述”页面上的详细信息

部分	说明
时间范围 (Time Range)	包含用于选择时间范围选项的下拉列表。有关详细信息，请参阅选择报告的时间范围，第 22 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 22 页。

如何对传入邮件计数

传入邮件的计数取决于每封邮件的收件人数。例如，从 example.com 发送给三个收件人的一封传入邮件被计为来自该发件人的三封邮件。

由于由发件人信誉过滤拦截的邮件不会实际进入工作队列，因此设备无权访问传入邮件的收件人列表。在此情况下，将使用倍数来估算收件人的数量。此倍数基于对大量现有客户数据样本的研究。

设备如何对邮件分类

由于邮件持续通过邮件管道，因此其可以应用于多个类别。例如，邮件可以标记为垃圾邮件或病毒邮件；它还可以与内容过滤器相匹配。各种过滤器和扫描活动的优先顺序会极大地影响邮件处理的结果。

在上面的示例中，各种判定遵循以下优先顺序规则：

- 垃圾邮件
- 病毒邮件
- 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) 报告页面上的“传入邮件摘要”(Incoming Mail Summary) 中报告的邮件按以下所述进行分类：

表 *12:*“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固定倍数（请参阅如何对传入邮件计数，第 43 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) 的值根据多个因素进行计算： • 来自此发件人的“受限制”邮件数 • 已拒绝或 TCP 拒绝的连接数（可能是部分计数） • 每个连接的邮件数量的保守倍数 当设备的负载繁重时，不会为逐个发件人维护已拒绝的连接准确计数。相反，仅为每个时间间隔内最重要的发件人维护已拒绝的连接计数。在这种情况下，显示的值可以解释为“下限”，即至少已拦截这么多邮件。 “概述”(Overview) 页面上的“由信誉过滤拦截”(Stopped by Reputation Filtering) 总计始终基于所有已拒绝的连接的完整计数。只有每个发件人的连接计数会因负载而受到限制。

类别	说明
无效收件人	由会话 LDAP 拒绝和所有 RAT 拒绝予以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	被检测为病毒但不是垃圾邮件的邮件总数和百分比。 以下消息计入□检测到病毒□类别中： • 病毒扫描结果为“已修复”(Repaired) 或“感染”(Infectious) 的邮件 • 在选中了将已加密的邮件计为包含病毒的选项时，病毒扫描结果为“已加密”(Encrypted) • 在针对无法扫描的邮件执行的操作不是“传送”(Deliver) 时，病毒扫描结果为“无法扫描”(Unscannable) • 在选中了传送到备用邮件主机或备用收件人的选项时，病毒扫描结果为“无法扫描”(Unscannable) 或“已加密”(Encrypted) 的邮件 • 以手动方式或通过超时从“病毒爆发”(Outbreak) 隔离区删除的邮件。
由高级恶意软件防护检测到 (Detected by Advanced Malware Protection)	文件信誉过滤发现邮件附件是恶意软件。该值不包括通过文件分析发现为恶意的判定更新或文件。
带恶意 URL 的邮件 (Messages with Malicious URLs)	URL 过滤发现邮件中的一个或多个 URL 是恶意的。
内容过滤器拦截	由内容过滤器拦截的邮件总数。 如果您的访问权限允许您查看邮件跟踪数据：要在此报告中查看内容过滤器违规的邮件跟踪详细信息，请点击表中的蓝色数字链接。
由 DMARC 拦截 (Stopped by DMARC)	未通过 DMARC 验证的邮件总数。
S/MIME 验证/解密失败	未通过 S/MIME 验证、解密或两者的邮件总数。
营销邮件	由公认的专业营销组织（如 Amazon.com）发送的广告邮件总数。 仅当系统中存在营销数据时，此列表项才会出现在页面上。 此数字包括由启用了灰色邮件功能的邮件安全设备识别的营销邮件，以及由在反垃圾邮件设置下启用了“营销邮件扫描”的设备识别的营销邮件。
社交网络邮件 (Social Networking Messages)	来自社交网络的、交友网站、论坛等的通知邮件总数。示例包括 LinkedIn 和 CNET 论坛。此信息由灰色邮件功能确定。
批量邮件 (Bulk Messages)	由非公认的营销组织（如技术媒体公司 TechTarget）发送的广告邮件总数。 此信息由灰色邮件功能确定。

类别	说明
灰色邮件	此数字包括由灰色邮件功能检测到的营销邮件，以及社交网络邮件和批量邮件。它不包括未启用灰色邮件功能的设备上识别的营销邮件，即使这些合计包括在“营销邮件”(Marketing Messages) 值中。 点击与任一灰色邮件类别对应的数字，以使用“邮件跟踪”(Message Tracking) 查看属于该类别的邮件列表。 另请参阅灰色邮件报告 ，第 68 页。
S/MIME 验证/解密成功	已使用 S/MIME 成功验证、解密或解密并验证的邮件总数。
已接受的正常邮件	此类别是已接受并被视为非病毒和垃圾邮件的邮件。 最准确地表示了在将按收件人的扫描操作考虑在内时（例如拆分的邮件由单独的邮件策略处理）接受的正常邮件。 但是，由于未对标记为垃圾邮件或确定感染病毒且仍然传送的邮件进行计数，因此传送的实际邮件数可能不同于干净邮件计数。 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。总计中未计入邮件过滤器丢弃或退回的邮件。 未启用灰色邮件功能的设备上处理的邮件被计为正常邮件。
尝试的邮件总数 (Total Attempted Messages)	此数字包括垃圾邮件、营销邮件（无论是由灰色邮件功能还是由反垃圾邮件设置下的“营销邮件扫描”[Marketing Email Scanning] 功能发现）、社交网络邮件、批量邮件和正常邮件。

注释 如果您已配置防病毒设置以传送无法扫描或已加密的邮件，这些邮件将被计为正常邮件，而不是病毒。否则，邮件将被计为含有病毒的邮件。此外，如果邮件与某个邮件过滤器相匹配，且未被该过滤器丢弃或退回，则这些邮件将被视为安全邮件。邮件过滤器丢弃或退回的邮件不计入总数。

“传入邮件”页面

安全管理设备上的**邮件 > 报告 > 传入邮件**页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。

“传入邮件详细信息”(Incoming Mail Details) 交互式表显示了关于特定 IP 地址、域或网络所有者（组织）的详细信息。您可以访问任一 IP 地址、域或网络所有者的“发件人配置文件”页面，方法是点击**传入邮件**页顶部或其他“发件人配置文件”页面上的相应链接。

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。请参阅搜索与交互式邮件报告页面 ，第 36 页。

- 查看“发件人组”(Sender Groups) 报告以根据特定发件人组和邮件流策略操作监控连接。有关详细信息，请参阅 “发件人组 (Sender Groups)”报告页面，第 50 页。
- 查看关于已将邮件发送到您的设备的发件人的详细统计信息。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。
- 从 SenderBase 信誉服务获取有关发件人的详细信息，包括发件人的 SenderBase 信誉得分 (SBRS)、域最近匹配哪个发件人组等。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。

在“传入邮件”(Incoming Mail) 页面内查看

传入邮件页面有三种不同的视图：

- IP 地址
- 域
- 网络所有者

这些视图在选定视图的情景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，您可以点击发件人的 IP 地址、域名或网络所有者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，第 49 页。

注释 网络所有者是包含域的实体。域 *(Domains)* 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) 页面是与特定 IP 地址、域或网络所有者相关的“传入邮件”(Incoming Mail) 页面。

要按发件人组访问邮件流信息，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。请参阅发件人配置文件页面，第 49 页。

在某些情况下，某些报告页面包含可从顶层页面访问的几个独特的子报告。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。

当您在顶层页面的右上角点击“可打印的 PDF”(Printable PDF) 链接时，这些子报告页面的结果会在一个合并的报告上生成；在这种情况下是“传入邮件”(Incoming Mail) 报告页面。请参阅了解“邮件报告”页面，第 37 页中的重要信息。

邮件 > 报告 > 传入邮件页面提供以下视图：**IP 地址**、**域**或**网络所有者**

如需获得对“传入邮件详细信息”(Incoming Mail Details) 交互式表中包括的数据的解释，请参阅传入邮件详细信息 (Incoming Mail Details) 表 ，第 48 页。

从**传入邮件**页面中，您还可以生成 PDF 或将原始数据导出到 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 ，第 37 页。

注释 您可以生成“传入邮件”(Incoming Mail) 报告页面的计划报告。请参阅计划邮件报告 ，第 77 页。

“没有域信息”(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“没有域信息”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。

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

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。您可以选择相同数据的天、周、月和年视图。由于数据实时受到监控，因此会在数据库中定期更新和汇总信息。

有关时间范围的详细信息，请参阅选择报告的时间范围 ，第 22 页。

传入邮件详细信息 (Incoming Mail Details) 表

传入邮件页面底部的“传入邮件详细信息”交互式表列出了已连接至邮件安全设备上的公共侦听程序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“传入邮件详细信息”(Incoming Mail Details) 表第一列中列出的或“按威胁邮件总数列出的发件人排行榜”(Top Senders by Total Threat Messages) 上的发件人（即网络所有者、IP 地址或域），点击**发件人 (Sender)** 或**没有域信息 (No Domain Information)** 链接可查看有关发件人的详细信息。结果显示在**发件人配置文件**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，您可以查看有关特定 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 ，第 49 页。

您还可以查看“发件人组”(Sender Groups) 报告，方法是点击“传入邮件”(Incoming Mail) 页面底部的**发件人组报告 (Sender Groups report)**。有关“发件人组报告”(Sender Groups report) 页面的详细信息，请参阅“发件人组 (Sender Groups)”报告页面 ，第 50 页。

如果您的访问权限允许您查看邮件跟踪数据：要在此报告中查看内容过滤器违规的邮件跟踪详细信息，请点击表中的蓝色数字链接。

发件人配置文件页面

当您在**传入邮件**页面上的传入邮件详细信息交互式表中点击发件人时，系统将显示“发件人配置文件”页面。它显示关于特定IP地址、域或网络所有者（组织）的详细信息。通过点击传入邮件页面或其他“发件人配置文件”页面上的相应链接，您可以访问任何IP地址、域或网络所有者的“发件人配置文件”页面。

网络所有者是包含域的实体。域 *(Domains)* 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。对于每项，该页面包含来自特定发件人的传入邮件的图形和摘要表。在图形下方，表列出与发件人相关联的域或 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，其中包含当前 SenderBase、发件人组和发件人的网络信息。

- 网络所有者配置文件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（仅限网络所有者）
  - CIDR 范围（仅限 IP 地址）
  - IP 地址、域和/或网络所有者的日量级和月量级
  - 自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。

  - 平均量级（仅限 IP 地址）
  - 生命周期数量/30 天数量（仅限 IP 地址配置文件页面）
  - 有担保发件人状态（仅限 IP 地址配置文件页面）
  - SenderBase 信誉得分（仅限 IP 地址配置文件页面）
  - 自从第一封邮件以来的天数（仅限网络所有者和域配置文件页面）
  - 与此网络所有者相关联的域数量（仅限网络所有者和域配置文件页面）
  - 此网络所有者中的 IP 地址数量（仅限网络所有者和域配置文件页面）
  - 用于发送邮件的 IP 地址数量（仅限网络所有者页面）

  点击**来自 SenderBase 的详细信息 (More from SenderBase)** 可查看包含 SenderBase 信誉服务提供的所有信息的页面。

- 有关由此网络所有者控制的域和 IP 地址的详细信息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，您可以点击特定 IP 地址以查看特定信息，或查看组织配置文件页面。

“发件人组 (Sender Groups)”报告页面

发件人组报告页按发件人组和邮件流策略操作提供连接摘要，允许您查看 SMTP 连接和邮件流策略趋势。“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**发件人组报告**页中，您还可以生成 PDF 或将原始数据导出到 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，第 37 页。

注释 您可以生成“发件人组报告”(Sender Groups report) 页面的计划报告。请参阅计划邮件报告，第 77 页。

“外发目标”(Outgoing Destinations) 页面

邮件 > 报告 > 外发目标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、恶意软件或由内容过滤器拦截？
- 传送了多少封邮件？目标服务器硬退回了多少封邮件？

以下列表解释了**外发目标**页面上的各部分：

表 *13*: “邮件”>“报告”>“外发目标”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围，第 22 页。
按威胁邮件总数列出的目标排行榜 (Top Destination by Total Threat)	您的组织发送的传出威胁邮件（垃圾邮件、病毒等）的目标域排行榜。威胁总数包括属于垃圾邮件或病毒的威胁，或触发了内容过滤器的威胁。

部分	说明
按正常邮件数列出的目标排行榜 (Top Destination by Clean Messages)	您的组织发送的正常传出邮件的目标域排行榜。
外发目标详细信息 (Outgoing Destination Details)	与您的组织发送的所有传出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。 如果您的访问权限允许您查看邮件跟踪数据：要在此报告中查看内容过滤器违规的邮件跟踪详细信息，请点击表中的蓝色数字链接。

从**外发目标**页面中，您还可以生成 PDF 或将原始数据导出到 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，第 37 页。

注释 您可以生成“外发目标”(Outgoing Destinations) 页面的计划报告。请参阅计划邮件报告，第 77 页。

“传出邮件发件人”页面

邮件 > 报告 > 传出邮件发件人页面提供有关从网络中的 IP 地址和域所发送邮件的数量和类型信息。

使用“传出邮件发件人”(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、垃圾邮件或恶意软件的特征邮件？
- 哪些 IP 地址最频繁触发内容过滤器？
- 哪些域发送最多邮件？
- 已尝试传送后正在处理的收件人总数。

要查看**传出邮件发件人**页面，请执行以下操作：

您可以使用两种类型的视图查看传出邮件发件人的结果：

- **域 (Domain)**：此视图使您可以查看每个域发送的邮件量。
- **IP 地址 (IP address)**：此视图使您可以查看哪些 IP 地址发送的病毒邮件最多或触发内容过滤器。

以下列表从两种视图角度解释了**传出邮件发件人**页面上的各部分：

表 *14*：“邮件报告传出邮件发件人”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围，第 22 页。
排名靠前的发件人（按有害邮件总数）	您的组织中的传出威胁邮件（垃圾邮件、病毒等）的发件人排行榜（按 IP 地址或域）。
按正常邮件列出的发件人排行榜	您的组织中发送的正常传出邮件的发件人排行榜（按 IP 地址或域）。

部分	说明
发件人详细信息	关于您的组织发送的所有传出邮件的发件人的详细信息（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。 如果您的访问权限允许您查看邮件跟踪数据：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，请点击表中的蓝色数字链接。

注释 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**传出邮件发件人**页面中，您还可以生成 PDF 或将原始数据导出到 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，第 37 页。

注释 您可以生成**传出邮件发件人 (Outgoing Senders)** 页面的计划报告。请参阅计划邮件报告，第 77 页。

“内部用户”页面

邮件 > 报告 > 内部用户页面按邮件地址提供有关您的内部用户发送和接收的邮件的信息。 单个用户可以具有多个邮件地址。报告中未合并邮件地址。

使用“内部用户”(Internal Users) 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？
- 谁接收的干净邮件最多？
- 谁接收的灰色邮件最多？
- 谁接收的垃圾邮件最多？
- 谁触发了哪些内容过滤器？
- 谁的邮件被内容过滤器捕获？

表 *15:*“邮件报告内部用户”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围，第 22 页。
按正常的传入邮件排名靠前的用户 (Top Users by Clean Incoming Messages)	您的组织中发送的正常传入邮件的用户排行榜（按 IP 地址或域）。
按正常的传出邮件排名靠前的用户 (Top Users by Clean Outgoing Messages)	您的组织中发送的正常传出邮件的用户排行榜（按 IP 地址或域）。

部分	说明
用户邮件控制详细信息 (User Mail Flow Details)	“用户邮件流详细信息”(User Mail Flow Details) 交互式部分会细分每个邮件地址接收和发送的邮件。您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) 列的用户名。有关详细信息，请参阅“内部用户详细信息”(Internal User Details) 页面 ，第 53 页。 如果您的访问权限允许您查看邮件跟踪数据：要在此报告中查看内容过滤器违规的邮件跟踪详细信息，请点击表中的蓝色数字链接。

从**内部用户**页面中，您还可以生成 PDF 或将原始数据导出到 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 ，第 37 页。

注释 您可以生成“内部用户”(Internal Users) 页面的计划报告。请参阅计划邮件报告 ，第 77 页。

“内部用户详细信息”(Internal User Details) 页面

“内部用户详细信息”页面显示关于用户的详细信息，细分了传入和传出邮件，显示每种类别（如检测到的垃圾邮件、检测到的病毒邮件、高级恶意软件保护检测到的邮件、内容过滤器拦截的邮件等）的邮件数。还显示传入和传出内容过滤器匹配项。

入站内部用户是您根据“收件人：”(Rcpt To:) 地址为其收到邮件的用户。出站内部用户基于“邮件发件人：”(Mail From:) 地址，并且在跟踪内部网络上的发件人发送的邮件类型时有用。

点击内容过滤器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”(Content Filters) 页面 ，第 56 页）。您可以使用此方法查看发送了或接收了与特定内容过滤器相匹配的邮件的所有用户列表。

注释 某些出站邮件（例如退回）的发件人为空。这些邮件被计为出站“未知”(unknown)。

搜索特定的内部用户

利用内部用户页面和内部用户详细信息页面底部的搜索表单，您可以搜索特定的内部用户（邮件地址）。选择是要精确匹配搜索文本还是查找以输入的文本开头的项（例如，以“ex”开头将匹配“example.com”）。

DLP 事件

邮件 > 报告 > DLP 事件（**DLP 事件摘要**）页显示传出邮件中发生的防数据丢失 (DLP) 策略违规事件的信息。邮件安全设备使用在“传出邮件策略 (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 策略的每个传出邮件均报告为一个事件。

使用“DLP 事件摘要”(DLP Incident Summary) 报告可回答以下类型的问题：

- 用户发送的是什么类型的敏感数据？
- 这些 DLP 事件具有什么样的严重性？
- 传送的这些邮件有多少数量？
- 丢弃的这些邮件有多少数量？
- 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：

- 按严重性（低 [Low]、中 [Medium]、高 [High]、严重 [Critical]）总结 DLP 事件排行榜的 DLP 事件趋势图，以及策略匹配项
- DLP 事件详细信息列表

表 *16*:“邮件”>“报告”>“*DLP* 事件摘要”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围，第 22 页。
按严重性排名考前的事件 (Top Incidents by Severity)	按严重性列出的 DLP 事件排行榜。
事件概要	**DLP 事件摘要 (DLP Incident Summary)** 页面底部的“DLP 事件详细信息”(DLP Incident Details) 交互式表中列出了当前已为每台邮件设备的传出邮件策略启用的 DLP 策略。点击 DLP 策略的名称可查看更详细的信息。
排名靠前的 DLP 策略匹配项 (Top DLP Policy Matches)	已匹配的 DLP 策略排行榜。
DLP 事件详细信息 (DLP Incident Details)	“DLP 事件详细信息”(DLP Incident Details) 表显示每个策略的 DLP 事件总数，其细分依据为严重性级别，以及是否已传送类别为“已传送（清除）”(Delivered [clear])、“已传送（已加密）”(Delivered [encrypted]) 或“已丢弃”(Dropped) 的任何邮件。 有关“DLP 事件详细信息”(DLP Incident Details) 表的更多信息，请参阅 “DLP 事件详细信息”表，第 54 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。您可以使用此方法获取已发送包含策略检测到的敏感数据的邮件的用户的列表。

“DLP 事件详细信息”表

“DLP 事件详细信息”(DLP Incident Details) 交互式表按策略显示 DLP 事件总数，其细分依据为严重性级别，以及是否已传送类别为“已传送（清除）”(Delivered [clear])、“已传送（已加密）”(Delivered [encrypted]) 或“已丢弃”(Dropped) 的任何邮件。点击列标题可对数据进行排序。

要了解有关此表中列出的任何 DLP 策略的详细信息，请点击 DLP 策略的名称，此时会出现“DLP 策略”(DLP Policy) 页面。有关详细信息，请参阅“DLP 策略详细信息”页面，第 55 页。

如果您的访问权限允许您查看邮件跟踪数据：要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

“DLP 策略详细信息”页面

如果您在“DLP 事件详细信息”(DLP Incident Details) 表中点击某个 DLP 策略的名称，出现的“DLP 策略详细信息”(DLP Policy Detail) 页面会显示该策略的 DLP 事件数据。该页面会显示基于严重性的 DLP 事件图形。

该页面还在页面底部包括“按发件人列出的事件”(Incidents by Sender)，其中列出了发送的邮件违反 DLP 策略的每个内部用户。该表还按用户显示此策略的 DLP 事件总数，其细分依据为严重性级别，以及是否已传送类别为“已传送（清除）”(Delivered [clear])、“已传送（已加密）”(Delivered [encrypted]) 或“已丢弃”(Dropped) 的任何邮件。您可以使用“按发件人列出的事件”(Incidents by Sender) 表了解哪些用户可能正在将组织的敏感数据发送给网络外部的人员。

点击“事件详细信息”(incident detail) 页面上的发件人名称将打开“内部用户”(Internal Users) 页面有关详细信息，请参阅“内部用户”页面，第 52 页。

邮件过滤器

“邮件过滤器”(Message Filters) 页面显示有关传入和传出邮件的邮件过滤器匹配项排行榜的信息（那些邮件过滤器具有最大数量的匹配邮件）。

地理分布

可以使用“地理分布”报告页面查看：

- 以图形格式显示的基于来源国家/地区的传入邮件连接排行榜。
- 以表格格式显示的基于源国家/地区的传入邮件连接总数。

以下是不显示传入邮件连接排行榜和总数的国家/地区信息的情景：

- 发件人 IP 地址是私有 IP 地址
- 发件人 IP 地址未获得有效 SBRS。

大量邮件

使用此页上的报告执行以下操作：

- 识别涉及来自单个发件人的大量邮件的攻击或在移动一小时期间内具有相同对象的攻击。
- 监控排名靠前的域以确保此类攻击不从您自己的域发起。如果发生这种情况，您的组织中的一个或多个账户可能受到影响。
- 帮助识别误报，使您可以相应地调整过滤器。

此页面上的报告所显示的数据仅来自使用“标题重复”(Header Repeats) 规则的邮件过滤器，以及超过您在该规则中设置的邮件数阈值的邮件过滤器。当与其他规则结合使用时，系统会最后计算“标题重复”(Header Repeats) 规则，如果邮件处理由之前的条件决定，则完全不计算。同样，由“速率限制”(Rate Limiting) 捕获的邮件绝不会到达“标题重复”(Header Repeats) 邮件过滤器。因此，本来可能被视为大量邮件的某些邮件可能不会包括在这些报告中。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 66 页

“内容过滤器”(Content Filters) 页面

邮件 (Email) > 报告 (Reporting) > 内容过滤器 (Content Filters) 页面显示关于传入和传出内容过滤器匹配项排行榜的信息（哪个内容过滤器具有最匹配的邮件）。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：

- 传入或传出邮件最多触发了哪些内容过滤器？
- 哪些用户最常发送或接收触发特定内容过滤器的邮件？

要查看有关特定过滤器的详细信息，请点击过滤器的名称。此时将出现“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) 页面的更多信息，请参阅“内容过滤器详细信息”页面 ， 第 56 页。

如果您的访问权限允许您查看邮件跟踪数据：要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

从**内容过滤器**页面中，您还可以生成 PDF 或将原始数据导出到 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 ， 第 37 页。

注释 您可以生成“内容过滤器”(Content Filters) 页面的计划报告。请参阅计划邮件报告 ， 第 77 页。

“内容过滤器详细信息”页面

“内容过滤器详细信息”(Content Filter Details) 页面显示过滤器在一段时间内的匹配项，以及按内部用户列出的匹配项。

在“按内部用户列出的匹配项”(Matches by Internal User) 部分中，点击用户名（邮件地址）可查看该内部用户的详细信息页面。有关详细信息，请参阅“内部用户详细信息”(Internal User Details) 页面 ， 第 53 页。

如果您的访问权限允许您查看邮件跟踪数据：要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

DMARC 验证

“DMARC 验证”(DMARC Verification) 页面显示未通过基于域的邮件身份验证、报告和一致性 (DMARC) 验证的发件人域排行榜，并显示对来自每个域的传入邮件执行的各项操作的摘要。您可以使用此报告微调 DMARC 设置和回答以下类型的问题：

- 哪些域发送了最多未通过 DMARC 验证的邮件？
- 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。

宏检测

可以使用“宏检测”报告页面查看：

- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传入附件。
- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传出附件。

您可以点击启用宏的附件数量，以在邮件跟踪中查看相关邮件。

注释 报告生成期间：

- 如果在存档文件中检测到一个或多个宏，则存档文件的文件类型将按一递增。不计算存档文件中启用宏的附件数量。
- 如果在嵌入文件中检测到一个或多个宏，则父文件类型将递增一。不计算嵌入文件中启用宏的附件数量。

“病毒类型”(Virus Types) 页面

邮件 > 报告 > 病毒页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。

注释 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。

如果您运行多个病毒扫描引擎，则“病毒类型”(Virus Types) 页面包含来自所有已启用的病毒扫描引擎的结果。页面上出现的病毒名称由病毒扫描引擎决定。如果多个扫描引擎检测到病毒，则同一病毒可能有多个条目。

表 17: “邮件”>“报告”>“病毒类型”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围 ，第 22 页。
检测到的传入病毒类型排行榜 (Top Incoming Virus Types Detected)	此部分显示已发送到您的网络的病毒的图表视图。
检测到的传出病毒类型排行榜 (Top Outgoing Virus Types Detected)	此部分显示已从您的网络发送的病毒的图表视图。
病毒类型详细信息 (Virus Types Detail)	显示每个病毒类型详细信息的交互式表。

注释 如需查看哪些主机将受病毒感染的邮件发送到您的网络，请转到“传入邮件”(Incoming Mail) 页面，指定同一报告时间段，并按病毒邮件排序。同样，如需查看您网络中的哪些 IP 地址发送了病毒邮件，请查看“传出邮件发件人”(Outgoing Senders) 页面，并按病毒邮件排序。

从**病毒类型**页中，您还可以生成PDF或将原始数据导出到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 ，第 37 页。

注释 您可以生成**病毒类型 (Virus Types)** 页面的计划报告。请参阅计划邮件报告 ，第 77 页。

“URL 过滤”页面

- 仅当启用 URL 过滤时，才会填充 URL 过滤报告模块。
- 提供传入和传出邮件的“URL 过滤”(URL Filtering) 报告。
- 只有由 URL 过滤引擎扫描的邮件（作为反垃圾邮件/病毒爆发过滤器扫描的一部分或通过邮件/内容过滤器）才会包含在这些模块中。但是，并非所有结果都有必要专门可归属于URL过滤功能。
- “排名靠前的 URL 类别”(Top URL Categories) 模块包含已扫描的邮件中找到的所有类别，无论其是与内容过滤器还是邮件过滤器匹配都如此。
- 每封邮件只能与一个信誉级别相关联。对于包含多个 URL 的邮件，统计信息反映邮件中任何 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内的 URL 未包含在报告中。

  报告中包含个别过滤器中使用的白名单内的 URL。

- 恶意 URL 是病毒爆发过滤器确定为信誉不佳的 URL。不确定 URL 是病毒爆发过滤器确定需要点击时间保护的 URL。因此，不确定 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。
- 由思科网络安全代理进行的点击时间 URL 评估的结果未反映在报告中。

“网络交互跟踪”页面

- 仅当在受管邮件安全设备上启用了“网络交互跟踪”功能时，才会填充“网络交互跟踪”报告模块。
- 提供传入和传出邮件的“网络交互跟踪”(Web Interaction Tracking) 报告。
- 这些模块中仅包含终端用户（通过策略或爆发过滤器）点击的重写 URL。
- “网络交互跟踪”(Web Interaction Tracking) 页面包括以下报告：

  终端用户点击的排名靠前的重写恶意 URL。点击 URL 可查看包含以下信息的详细报告：

  - 点击了重写恶意 URL 的终端用户列表。
  - 点击该 URL 的日期和时间。
  - URL 是否已由策略或病毒爆发过滤器重写。
  - 点击重写的 URL 时采取的操作（允许、阻止或未知）。请注意，如果 URL 被病毒爆发过滤器重写，且未提供最终判定，则状态显示为“未知”(unknown)。

  注释 由于限制原因，所有病毒爆发重写的 URL 的状态都将显示为未知。

  点击重写的恶意 URL 的排名靠前的终端用户

  跟踪网络交互详细信息。包括以下信息：

  - 所有重写的 URL 列表（恶意和非恶意）。点击 URL 可查看详细报告。
  - 点击重写的 URL 时采取的操作（允许、阻止或未知）。

    在终端用户点击 URL 时，如果对该 URL（正常或恶意）的判定为“未知”(unknown)，则状态显示为“未知”(unknown)。这可能是因为 URL 受到进一步审查或网络服务器在用户点击时已关闭或无法访问。

  - 终端用户点击重写的 URL 的次数。点击数字可查看包含点击的 URL 的所有邮件列表。

- 请注意以下提示：
  - 如果您已配置内容或邮件过滤器以在重写恶意URL后传送邮件并通知另一个用户（例如管理员），则在被通知的用户点击已重写的 URL 时，原始收件人的网络交互跟踪数据会增加。
  - 如果您使用网络界面向原始收件人之外的用户（如管理员）发送包含已重写URL的已隔离邮件副本，则在另一个用户点击已重写的 URL 时，原始收件人的网络交互跟踪数据会增加。

“伪造邮件检测”页面

- “伪造邮件检测”页面包括以下报告：
  - **排名靠前的伪造邮件检测**。显示内容字典中与传入邮件中的伪造“发件人：”信头匹配的前十个用户。
  - **伪造邮件检测详细信息**。显示内容词典中与传入邮件中的伪造“发件人：”信头匹配所有用户的列表，对于给定用户，还会显示匹配的邮件的数量。
- 只有在使用“伪造邮件检测”内容过滤器或 forged-email-detection 邮件过滤器时，才会填充“伪造邮件检测”报告。

“高级恶意软件保护”（文件信誉和文件分析）报告页面

- 文件分析报告详细信息的要求 ， 第 60 页
- 通过 SHA-256 散列标识文件 ， 第 62 页
- 文件信誉和文件分析报告页面 ， 第 62 页
- 查看其他报告中的文件信誉过滤数据 ， 第 63 页

文件分析报告详细信息的要求

- （云文件分析）确保管理设备可以连接到文件分析服务器 ， 第 60 页
- （云文件分析）配置管理设备以显示详细的文件分析结果 ， 第 60 页
- （本地文件分析）激活文件分析账户 ， 第 61 页
- 其它要求 ， 第 62 页

（云文件分析）确保管理设备可以连接到文件分析服务器

要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。请参阅防火墙资讯 ， 第 385 页中的详细信息

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 292 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。

如果您使用 HTTPS 代理，则代理不能将流量解密；请使用直通机制与文件分析服务器通信。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其自己的证书。

（云文件分析）配置管理设备以显示详细的文件分析结果

为了使组织中的所有内容安全设备都可以在云中显示有关从组织中的任何思科邮件安全设备或思科网络安全设备送交分析的文件的详细结果，您需要将所有设备加入到同一设备组。

步骤 1 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 滚动至“文件分析”(File Analysis) 部分。

步骤 3 如果您管理的设备指向不同的文件分析云服务器，请选择从中显示结果详细信息的服务器。

将不提供由任何其他云服务器处理的文件的结果详细信息。

步骤 4 输入分析组 ID。

- 如果未正确输入组 ID 或出于任何其它原因需要对其进行更改，则必须向 思科 TAC 提交请求。
- 此更改会立即生效；它不需要“确认”(Commit)。
- 建议将您的 CCOID 用于此值。
- 此值区分大小写。
- 在所有将共享关于上传以供分析的文件的数据的设备上，此值必须相同。
- 一台设备只能属于一个组。
- 您可以随时将设备添加到组，但是只能添加一次。

步骤 5 点击**立即分组 (Group Now)**。

步骤 6 在将与此设备共享数据的每台邮件安全设备上配置相同的组。

下一步做什么

相关主题

可以在云中查看哪些文件的详细文件分析结果？ ，第 64 页

（本地文件分析）激活文件分析账户

如果您已部署本地（私有云）的思科 AMP Threat Grid 设备，必须激活思科内容安全管理设备的文件分析账户，才能查看 Threat Grid 设备上提供的报告详细信息。您通常只需执行此操作一次。

开始之前

确保您接收“严重”(Critical) 级别的系统警报。

步骤 1 首次尝试从 Threat Grid 设备访问文件分析报告详细信息时，请等待几分钟，然后您将收到包含一个链接的警报。

如果您没有收到此警报，请转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报 (Alerts)**，然后点击**查看警报排行榜 (View Top Alerts)**。

步骤 2 点击警报消息中的链接。

步骤 3 激活您的管理设备账户。

其它要求

有关任何其他要求，请参阅安全管理设备版本的版本说明，位置：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html

通过 SHA-256 散列标识文件

由于文件名很容易更改，因此设备会使用安全散列算法 (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，所有实例被识别为相同的 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，文件按其 SHA-256 值列出（以缩写格式）。

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 (Advanced Malware Protection)	显示由文件信誉服务识别的基于文件的威胁。 对于那些具有已更改判定的文件，请参阅 AMP 判定更新报告。这些判定不会反映在“高级恶意软件防护”(Advanced Malware Protection) 报告中。 如果从某个已压缩或已存档的文件中提取的某个文件是恶意文件，则只有这个已压缩或已存档的文件的 SHA 值包括在“高级恶意软件防护”(Advanced Malware Protection) 报告中。 **注释** 从 AsyncOS 9.6.5 开始，高级恶意软件保护报告已得到增强，以显示其他字段、图形等。升级后显示的报告不包括升级前的报告数据。要在 AsyncOS 9.6.5 升级之前查看高级恶意软件保护报告，请点击页面底部的超链接。 **按类别划分的传入恶意软件文件**部分显示从面向终端的 AMP 控制台所接收、归类为**自定义检测**且已列入黑名单的文件 SHA 百分比。 从面向终端的 AMP 控制台获取的已列入黑名单的文件的 SHA 百分比在报告的“传入恶意软件威胁文件”部分中显示为**简单自定义检测**。 您可以点击报告的“更多详细信息”部分中的链接，以查看在面向终端的 AMP 控制台中已列入黑名单的文件 SHA 的文件轨迹详细信息。 您可以在报告的“AMP 处理的传入文件”部分查看**低风险**判定详细信息。

报告	说明
高级恶意软件保护文件分析	显示送交分析的每个文件的时间和判定（或临时判定）。设备每 30 分钟检查一次分析结果。 要查看超过 1000 个文件分析结果，请将数据导出为 .csv 文件。 对于采用本地思科 AMP Threat Grid 设备的部署：在 AMP Threat Grid 设备上列入白名单的文件显示为“正常”(clean)。有关白名单的信息，请参阅 AMP Threat Grid 文档或联机帮助。 深入分析以查看详细的分析结果，包括每个文件的威胁特征。 您还可以搜索有关 SHA 的其他信息，或点击文件分析详细信息页面底部的链接以在分析了文件的服务器上查看其他详细信息。 要在分析了文件的服务器上查看详细信息，请参阅文件分析报告详细信息的要求 ，第 60 页。 如果从某个已压缩或已存档的文件中提取的某个文件送交分析，则只有这个已提取文件的 SHA 值包括在“文件分析”(File Analysis) 中。 **注释** 从 AsyncOS 9.6.5 开始，文件分析报告已得到增强，以显示其他字段、图形等。升级后显示的报告不包括升级前的报告数据。要在 AsyncOS 9.6.5 升级之前查看文件分析报告，请点击页面底部的超链接。
高级恶意软件保护裁决更新	由于“高级恶意软件防护”(Advanced Malware Protection) 重点关注有针对性的威胁和零日威胁，因此威胁判定可以随着汇聚数据提供更多信息而发生变化。 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 的判定多次发生变化，此报告仅显示最新的判定，而不显示判定历史记录。 要查看特定 SHA - 256 在最大可用时间范围内的所有受影响的邮件（无论为报告选择的时间范围如何），请点击 SHA-256 链接。

查看其他报告中的文件信誉过滤数据

在相关的情况下，其他报告中会提供文件信誉和分析的数据。在适用的报告中，“由高级恶意软件防护检测到”(Detected by Advanced Malware Protection) 列在默认情况下可能处于隐藏状态。要显示其他列，请点击表底部的“列”(Columns) 链接。

可以在云中查看哪些文件的详细文件分析结果？

如果您部署了公共云文件分析，则可以查看从已添加到文件分析设备组的任何受管设备上传的所有文件的详细结果。

如果您已将管理设备添加到该组，可以查看组中的受管设备列表，方法是依次点击**管理设备 > 集中服务 > 安全设备**页面上的按钮。

分析组中的设备由文件分析客户端 ID 标识。要确定特定设备的此标识符，请查看以下位置：

设备	文件分析客户端 ID 的位置
邮件安全设备	**安全服务 (Security Services > 文件信誉和分析 (File Reputation and Analysis)** 页面上的“文件分析的高级设置”(Advanced Settings for File Analysis) 部分。
网络安全设备	**安全服务 > 防恶意软件和信誉**页面上的“文件分析高级设置”部分。
思科内容安全管理设备	在**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)** 页面的底部。

相关主题

- （云文件分析）配置管理设备以显示详细的文件分析结果 ， 第 60 页

邮箱自动补救

您可以使用“邮箱自动补救”报告页查看邮箱补救结果的详细信息。使用此报告可以查看详细信息，如：

- 对其邮箱执行的补救操作成功或不成功的收件人的列表
- 对邮件执行的修复操作
- 与 SHA-256 散列关联的文件名

在以下情景中，**对其邮箱执行的补救操作不成功的收件人**字段将更新：

- 收件人不是有效的 Office 365 用户或者收件人不属于您的设备上配置的 Office 365 域账户。
- 包含附件的邮件在邮箱中不再可用，例如，终端用户删除了邮件。
- 当设备尝试执行配置的补救操作时，您的设备与 Office 365 服务之间存在连接问题。

点击 SHA-256 哈希可查看邮件跟踪中的相关邮件。

“TLS 连接”页面

邮件 > 报告 > TLS 连接页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，哪个部分的传入/传出连接使用 TLS？

- 我与哪些合作伙伴建立成功的 TLS 连接？
- 我与哪些合作伙伴建立的 TLS 连接失败？
- 哪些合作伙伴的 TLS 证书有问题？
- 合作伙伴的全部邮件中有多少百分比使用 TLS？

表 *18*:“邮件”>“报告”>“*TLS* 连接”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围 ，第 22 页。
传入 TLS 连接图 (Incoming TLS Connections Graph)	该图根据您选择的时间段显示上一小时、上一天或上一周内的传入 TLS 加密和未加密连接视图。
传入 TLS 连接概要 (Incoming TLS Connections Summary)	此表显示传入邮件总量、加密和未加密邮件数量，以及成功和失败的传入 TLS 加密邮件数量。
传入 TLS 邮件摘要 (Incoming TLS Message Summary)	此表显示传入邮件总量的摘要。
传入 TLS 连接详细信息 (Incoming TLS Connections Details)	下表显示发送或接收加密邮件的域的详细信息。对于每个域，您可以查看连接总数、已发送的邮件，以及成功或失败的 TLS 连接数量。您还可以查看每个域的成功和失败连接的百分比。
传出 TLS 连接图 (Outgoing TLS Connections Graph)	该图根据您选择的时间段显示上一小时、上一天或上一周内的传出 TLS 加密和未加密连接视图。
传出 TLS 连接概要 (Outgoing TLS Connections Summary)	此表显示传出邮件总量、加密和未加密邮件数量，以及成功和失败的传出 TLS 加密邮件数量。
传出 TLS 邮件摘要 (Outgoing TLS Message Summary)	此表显示传出邮件总量。
传出 TLS 连接详细信息 (Outgoing TLS Connections Details)	下表显示发送或接收加密邮件的域的详细信息。对于每个域，您可以查看连接总数、已发送的邮件、成功或失败的 TLS 连接数量，以及最后的 TLS 状态。您还可以查看每个域的成功和失败连接的百分比。

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，则其将会建立到邮件客户端的 TLS 连接，客户端将使用该连接发送邮件。因为设备无法逐个用户跟踪这些尝试，因此报告会根据域名和域 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？
- 多少连接使用经过认证的客户端？
- 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) 页面包含一个表示已接收的连接的图形、一个表示已尝试 SMTP 身份验证连接的邮件收件人的图形，以及一个包含有关对连接进行身份验证的尝试的详细信息的表。

“已接收的连接”(Received Connections) 图形显示在指定时间范围内来自尝试使用 SMTP 身份验证对其连接进行身份验证的邮件客户端的传入连接。该图形显示设备已接收的连接总数、未尝试使用 SMTP 身份验证进行身份验证的连接数、使用客户端证书对连接进行身份验证成功和失败的连接数，以及使用 SMTP AUTH 命令进行身份验证失败和成功的连接数。

“已接收的收件人”(Received Recipients) 图形显示了收件人的数量，这些收件人的邮件客户端尝试对其与邮件安全设备的连接进行身份验证以使用 SMTP 身份验证来发送邮件。该图形还显示其连接已进行身份验证的收件人数和其连接未进行身份验证的收件人数。

“SMTP 身份验证详细信息”(SMTP Authentication details) 表显示了域的详细信息，这些域的用户尝试对其与邮件安全设备的连接进行身份验证以发送邮件。对于每个域，您可以查看使用客户端证书进行的成功或失败的连接尝试数、使用 SMTP AUTH 命令进行的成功或失败的连接尝试数，以及在其客户端证书连接尝试失败后回退到 SMTP AUTH 的连接尝试数。您可以使用页面底部的链接按域名或域 IP 地址显示此信息。

速率限制页面

通过按信封发件人进行速率限制，您可以根据发件人地址从单个发件人限制每个时间间隔的邮件收件人数。“速率限制”(Rate Limits) 报告显示最严重超过此限制的发件人。

使用此报告可帮助确定以下内容：

- 可能用于批量发送垃圾邮件的有漏洞用户账户。
- 组织中的失控应用程序，这些应用程序使用邮件发送通知、风险通告、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。
- 可能未被视为垃圾邮件的大量入站邮件流量的来源。

请注意，包含内部发件人（例如内部用户或传出邮件发件人）的统计信息的其他报告仅测量已发送的邮件数；它们不会向大量收件人表明少数邮件的发件人的身份。

“按事件划分的排名靠前的危害”图表显示最频繁尝试向超过配置限制的收件人发送邮件的信封发件人。每次尝试都是一个事件。此图表汇总所有侦听程序的事件计数。

“按已拒绝收件人划分的排名靠前的危害”图表显示向高于配置限制的最大数量的收件人发送邮件的信封发件人。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 55 页

“病毒爆发过滤器”页面

邮件 > 报告 > 病毒爆发过滤器页显示有关最近的爆发的信息，并显示由于“病毒爆发过滤器”而隔离的邮件的相关信息。您可以使用此页面可以监控对针对性的病毒、诈骗和网络钓鱼攻击的防御。

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

- 多少封邮件被隔离？依据的是哪项“病毒爆发过滤器”(Outbreak Filters) 规则？
- “病毒爆发过滤器”(Outbreak Filters) 功能一直针对病毒爆发提供多久的提前时间？
- 本地病毒爆发与全球病毒爆发相比如何？
- 邮件在病毒爆发隔离区中停留多长时间？
- 哪些可能是恶意的 URL 是最常见的？

“按类型划分的威胁”(Threats By Type) 部分显示设备接收的不同类型的威胁邮件。“威胁摘要”(Threat Summary) 部分按“病毒”(Virus)、“网络钓鱼”(Phish) 和“诈骗”(Scam) 细分邮件。

“上一年病毒爆发摘要”(Past Year Outbreak Summary) 列出上一年的全局以及本地的病毒爆发，使您能够将本地网络趋势与全局趋势进行比较。全局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。全局病毒爆发数据表示威胁操作中心检测到的所有病毒爆发，该数据超过病毒爆发隔离区的当前配置的阈值。本地病毒爆发数据表示在此设备上检测到的所有病毒爆发，该数据超过病毒爆发隔离区的当前配置的阈值。“本地防护总时间”(Total Local Protection Time) 始终基于威胁操作中心检测到各病毒爆发的时间与主要供应商发布防病毒签名的时间之间的时间差。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) 部分汇总病毒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。隔离的邮件在放行时计数。通常，邮件在防病毒和反垃圾邮件规则可用之前会被隔离。放行时，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。在放行时（而不是在进入隔离区中时）对邮件进行计数可避免混淆计数增加和减少的情况。

“威胁详细信息”(Threat Details) 列表显示有关特定病毒爆发的信息，包括威胁类别（病毒、诈骗或网络钓鱼）、威胁名称、该威胁的说明和识别的邮件数。对于病毒爆发，“上一年病毒爆发”(Past Year Virus Outbreaks) 包含病毒爆发名称和 ID、首次全局出现病毒爆发的时间和日期、病毒爆发过滤器提供的防护时间以及隔离邮件数。您可以选择是要查看全球还是本地爆发。

“在全球首次发现”(First Seen Globally) 时间由威胁行动中心根据来自 SenderBase 的数据确定，SenderBase 是全球最大的邮件和网络流量监控网络。“防护时间”(Protection Time) 基于威胁操作中心检测到每个威胁的时间与主要供应商发布防病毒签名的时间之间的时间差。

值为“--”表示防护时间不存在，或者防病毒供应商未提供签名时间（某些供应商可能不会报告签名时间）。这并不表示防护时间为零。相反，意味着计算防护时间所需的信息不可用。

此页面上的其他模块提供：

- 病毒爆发过滤器在所选时间段处理的传入邮件的数量。

非病毒性威胁包括网络钓鱼邮件、诈骗和使用指向外部网站的链接进行的恶意软件分发。

- 病毒爆发过滤器捕获的威胁严重性。

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。

此持续时间取决于系统需要多长时间收集关于潜在威胁的足够数据以对其安全性做出判定。带有病毒性威胁的邮件通常比带有非病毒性威胁的邮件在隔离区中花费更多时间，因为它们必须等待防病毒程序更新。还会反映您为每个邮件策略指定的最大保留时间。

- 最频繁重写的 URL，重写的目的是将邮件收件人重定向到思科网络安全代理，以便在收件人点击邮件中可能是恶意的链接时对网站进行点击时间评估。

此列表可能包括非恶意的 URL，因为如果邮件中的任何 URL 被视为恶意，则邮件的所有 URL 均会被重写。

注释 为了正确填充“病毒爆发过滤器”报告页上的各个表，设备必须能够与中指定的思科更新服务器进行通信。管理设备 (Management Appliance) > 系统管理 (System Administration) > 更新设置 (Update Settings)。

有关详细信息，请参阅的病毒爆发过滤器章节。

灰色邮件报告

以下报告中反映了灰色邮件统计信息：

报告	包含以下灰色邮件数据
“概述”(Overview) 页面 >“传入邮件摘要”(Incoming Mail Summary)	每种灰色邮件类别（营销、社交和批量）下的传入灰色邮件数量，以及灰色邮件总数。
“传入邮件”(Incoming Mail) 页面 >“按灰色邮件列出的发件人排行榜”(Top Senders by Graymail Messages)	排名靠前的灰色邮件发件人。
“传入邮件”(Incoming Mail) 页面 >“传入邮件详细信息”(Incoming Mail Details)	所有 IP 地址、域名或网络所有者的每种灰色邮件类别（营销、社交和批量）下的传入灰色邮件数量，以及灰色邮件总数。
“传入邮件”(Incoming Mail) 页面 >“传入邮件详细信息”(Incoming Mail Details) >“发件人配置文件”(Sender Profile)（深入分析视图）	给定 IP 地址、域名或网络所有者的每种灰色邮件类别（营销、社交和批量）下的传入灰色邮件数量，以及灰色邮件总数。

报告	包含以下灰色邮件数据
“内部用户”(Internal Users) 页面 > “按灰色邮件列出的用户排行榜”(Top Users by Graymail)	接收灰色邮件的排名靠前的最终用户。
“内部用户”(Internal Users) 页面 > “用户邮件流详细信息”(User Mail Flow Details)	所有用户的每种灰色邮件类别（营销、社交和批量）下的传入灰色邮件数量，以及灰色邮件总数。
“内部用户”(Internal Users) 页面 > “用户邮件流详细信息”(User Mail Flow Details) > “内部用户”(Internal User)（深入分析视图）	给定用户的每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。

相关主题

- 在升级到 AsyncOS 9.5 后报告营销邮件 ， 第 69 页

在升级到 AsyncOS 9.5 后报告营销邮件

在升级到 AsyncOS 9.5 后：

- 营销邮件的数量是在升级前后检测到的营销邮件之和。
- 灰色邮件总数不包括在升级前检测到的营销邮件数量。
- 尝试的邮件总数还包括在升级前检测到的营销邮件数量。
- 如果未在托管的邮件安全设备上启用灰色邮件功能，则营销邮件会被计为安全邮件。

系统容量页面

邮件 > 报告 > 系统容量页详细地表示了系统负载，包括工作队列中的邮件、传入和传出邮件（量、大小和数量）、CPU 总体使用率、按功能列出的 CPU 使用率和内存页面交换信息。

“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、工作队列中的邮件数，以及“资源节约模式”(Resource Conservation Mode) 的事件数。

- **量**：了解您的环境中的“正常”邮件量和“异常”尖峰非常重要。长期跟踪此数据可测量数量增长。您可以使用“传入邮件”(Incoming Mail) 和“传出邮件”(Outgoing Mail) 页面长期跟踪数量。有关详细信息，请参阅系统容量 - 传入邮件 ， 第 71 页和系统容量 - 传出邮件 ， 第 71 页。
- **工作队列 (Work Queue)**：工作队列旨在作为“减震器”- 缓冲并过滤垃圾邮件攻击，并处理非垃圾邮件的异常增加。但是，工作队列也可能表明系统处于压力之下。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 70 页。

- **资源节约模式 (Resource Conservation Mode)**：当设备变得过载时，它会进入“资源节约模式”(Resource Conservation Mode, RCM) 并发送“严重”(CRITICAL) 系统警报。这旨在保护设备并允许其处理任何积压邮件。设备不应频繁进入RCM，并且应仅在邮件量出现超大或异常增长期间进入。频繁的 RCM 警报可能表明系统正在超负荷。请参阅资源节约活动 ，第 72 页。

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：

- 日报告 (Day Report) - 日报告查询小时表并显示设备在 24 小时内每小时收到的准确查询数量。此信息收集自小时表。这是一个准确的数字。
- 月报告 - 月报告查询 30 或 31 天（取决于该月份的实际天数）的日表，为您提供 30 或 31 天内查询数量的确切报告。再次重申，这是一个精确的数字。

“系统容量”(System Capacity) 页面上的“最大值”(Maximum) 值指示符是在指定时间段内看到的最高值。“平均值”(Average) 值是指定时间段内所有值的平均值。汇聚的时间取决于为该报告选择的时间间隔。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

“工作队列”(Workqueue) 页面显示邮件在工作队列中花费的平均时间，在垃圾邮件隔离区中或在策略、病毒或病毒爆发隔离区中花费的任何时间除外。您可以查看时间段，从一小时到一个月。此平均值可以帮助确定延迟邮件传送的短期事件和确定系统上工作负载的长期趋势。

注释 如果邮件从隔离区释放到工作队列中，“工作队列中的平均时间”指标将忽略此时间。这可防止重复计数，以及由于在隔离区中花费的时间延长而造成统计信息失真。

此报告也显示指定时间段内的工作队列中的邮件量，并且显示相同时间段内工作队列中的最大邮件数量。工作队列中的最大邮件数图表还显示工作队列阈值级别。

工作队列图形中的偶尔峰值是正常的，并在预期之内。如果工作队列中的邮件数长时间保持高于配置的阈值，可能表示存在容量问题。在这种情况下，请考虑调整阈值级别或检查系统配置。

要更改工作队列阈值级别，请参阅调整邮件安全设备的系统运行状况图中的参考阈值 ，第 323 页。

提示 当查看工作队列页面时，您可能要测量工作队列备份的频率，并标注超过 10000 封邮件的工作队列备份。

系统容量 - 传入邮件

“系统容量”(System Capacity) 下的“传入邮件”(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。您可以查看一天、一周、一月或一年的结果。了解环境中的正常邮件量和尖峰的趋势非常重要。您可以使用“系统容量”(System Capacity) 下的“传入邮件”(Incoming Mail) 页面跟踪一段时间内的邮件量增长并为系统容量制定计划。您可能还希望将传入邮件数据与发件人配置文件数据进行比较，以查看从特定域发送到网络的邮件的邮件量趋势。

注释 传入连接的数量增加不一定会影响系统负载。

系统容量 - 传出邮件

“系统容量”(System Capacity) 下的“传出邮件”(Incoming Mail) 页面显示传出连接、传出邮件总数、平均邮件大小和传出邮件总大小。您可以查看一天、一周、一月或一年的结果。了解环境中的正常邮件量和尖峰的趋势非常重要。您可以使用“系统容量”(System Capacity) 下的“传出邮件”(Outgoing Mail) 页面跟踪一段时间内的邮件量增长并为系统容量制定计划。您可能还希望将传出邮件数据与外发目标数据进行比较，以查看从特定域或 IP 地址发送的邮件的邮件量趋势。

系统容量 (System Capacity) - 系统负载 (System Load)

系统负载报告显示如下信息：

- CPU 总体使用情况，第 71 页
- 内存页面交换，第 71 页
- 资源节约活动 ，第 72 页

CPU 总体使用情况

邮件安全设备经过优化，可使用空闲 CPU 资源提高邮件吞吐量。高 CPU 使用率可能不是表明系统容量问题。如果高 CPU 使用率与一致的大容量内存页面交换相结合，则可能会发生容量问题。

注释 此图还指明了一个仅用于视觉参考的CPU使用率阈值。要调整此行的位置，请参阅调整邮件安全设备的系统运行状况图中的参考阈值，第 323 页。您可以将邮件安全设备配置为向您发送警报，建议您可以为解决容量问题采取什么操作。

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。按功能划分的 CPU 图形可以很好地指示产品的哪些方面在系统上使用最多资源。如果需要优化设备，则此图形可以帮助确定哪些功能可能需要调整或禁用。

内存页面交换

内存页面交换图形显示了系统必须分页到磁盘的频率（以每秒千字节数为单位）。

系统旨在定期交换内存，因此发生一些内存交换在意料之中，并不是表明设备有问题。除非系统一致地大量交换内存，否则内存交换正常，并且是预期行为（尤其在C170设备上）。为提高性能，您可能需要将邮件安全设备添加到网络或调整配置以确保实现最大吞吐量。

注释 此图还指明了一个仅用于视觉参考的内存页面交换阈值。要调整此行的位置，请参阅调整邮件安全设备的系统运行状况图中的参考阈值，第 323 页。您可以将邮件安全设备配置为向您发送警报，建议您可以为解决容量问题采取什么操作。

资源节约活动

资源节约活动图显示邮件安全设备进入资源节约模式 (RCM) 的次数。例如，如果图中显示 n 次，则意味着设备进入了 RCM n 次，并已退出至少 n-1 次。

设备应当很少进入 RCM 模式，并且仅在邮件量非常大或异常增加时才进入此模式。如果“资源节约活动”(Resource Conservation Activity) 图显示您的设备频繁进入 RCS，则可能表明系统变得过载。

系统容量 - 全部

全部 (All) 页面将所有以前的系统容量报告整合到单个页面，使您可以查看不同报告之间的关系。例如，您可能发现消息队列很高，同时发生过多的内存切换。这可能表明存在容量问题。您可能希望将此页面另存为 PDF 文件，以保留系统性能的快照，供以后参考（或与支持人员共享）。

系统容量图形中的阈值指示符

在某些图形中，某行表示默认值，如果频繁或始终如一地超过该值，则可能表明存在问题。要调整此可视指示符，请参阅调整邮件安全设备的系统运行状况图中的参考阈值，第 323 页。

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

使用**邮件 > 报告 > 报告数据可用性**页面可以查看、更新数据和对数据排序，实时洞察资源利用率和邮件流量故障点。

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。

关于计划和按需的邮件报告

可用的报告类型

除非另有说明，否则以下类型的邮件安全报告均以计划报告和按需报告的形式提供：

- “内容过滤器”(Content Filters) - 此报告包括多达 40 个内容过滤器。有关此页面上所包括内容的其他信息，请参阅“内容过滤器”(Content Filters) 页面，第 56 页。

- “DLP 事件摘要”(DLP Incident Summary) - 有关此页面上所包括内容的信息，请参阅DLP 事件，第 53 页。
- “传送状态”(Delivery Status) - 此报告页面显示有关至特定收件人域或虚拟网关地址的传送问题的信息，对于由系统在过去三个小时传送的邮件，页面显示由前 20 个、50 个或 100 个收件人域构成的列表。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，第 43 页，并且限于一组指定的域。有关所包括内容的信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告，第 74 页。
- “执行摘要”(Executive Summary) - 此报告基于来自“邮件报告概述”页面，第 43 页的信息。有关所包括内容的信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告，第 74 页。
- 传入邮件摘要 - 有关此页面上所包括内容的信息，请参阅“传入邮件”页面，第 46 页。
- “内部用户摘要”(Internal Users Summary) - 有关此页面上所包括内容的信息，请参阅“内部用户”页面，第 52 页。
- “病毒爆发过滤器”(Outbreak Filters) - 有关此页面上所包括内容的信息，请参阅“病毒爆发过滤器”页面，第 67 页。
- “外发目标”(Outgoing Destinations) - 有关此页面上所包括内容的信息，请参阅“外发目标”(Outgoing Destinations) 页面，第 50 页。
- “传出邮件摘要”(Outgoing Mail Summary) - 有关此页面上所包括内容的信息，请参阅“传出邮件发件人”页面，第 51 页。
- “传出邮件发件人：域”(Outgoing Senders: Domains) - 有关此页面上所包括内容的信息，请参阅“传出邮件发件人”页面，第 51 页。
- “发件人组”(Sender Groups) - 有关此页面上所包括内容的信息，请参阅“发件人组 (Sender Groups)”报告页面，第 50 页。
- “系统容量”(System Capacity) - 要了解此页面上所包括内容的相关信息，请参阅系统容量页面，第 69 页。
- “TLS 连接”(TLS Connections) - 有关此页面上所包括内容的信息，请参阅“TLS 连接”页面，第 64 页。
- “病毒类型”(Virus Types) - 有关此页面上所包括内容的信息，请参阅“病毒类型”(Virus Types) 页面，第 57 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、前一个月、前历日（最多 250 天）或前历月（最多 12 个月）的数据。或者，您可以包括自定义天数（从 2 天到 100 天）或自定义月数（从 2 个月到 12 个月）的数据。

无论您何时运行报告，均会从上一个时间时间间隔（小时、天、星期或月）返回数据。例如，如果您计划在凌晨 1 点运行每日报告，则该报告将包含前一天从午夜到午夜（00:00 到 23:59）的数据。

语言和区域设置

注释 您可以使用单个报告的特定区域设置，计划 PDF 报告或将原始数据导出为 CSV 文件。使用“计划的报告”(Scheduled Reports) 页面上的语言下拉菜单可以按用户当前选择的区域设置和语言查看或计划 PDF 报告。请参阅打印和导出报告和跟踪数据 ，第 27 页的重要信息。

已存档报告的存储

有关报告存储时长以及何时从系统中删除已存档报告的信息，请参阅查看和管理已存档的邮件报告，第 80 页。

其他报告类型

在安全管理设备的**邮件 > 报告**部分中，可以生成的两个特殊报告为：

- “基于域的执行摘要”(Domain-Based Executive Summary) 报告 ，第 74 页
- “执行摘要”报告 ，第 76 页

“基于域的执行摘要”(Domain-Based Executive Summary) 报告

“基于域的执行摘要”(Domain-Based Executive Summary) 报告概述了网络中的一个或多个域的传入和传出邮件活动。它类似于“执行摘要”(Executive Summary report) 报告，但是它将报告数据限制为发送到您指定的域和从该域发送的邮件。“传出邮件摘要”(Outgoing Mail Summary) 仅在发送服务器的 PTR（指针记录）中的域与您指定的域相匹配时才显示数据。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**。

与其他计划报告不同，系统不会存档“基于域的执行摘要”(Domain-Based Executive Summary) 报告。

“基于域的执行摘要”(Domain-Based Executive Summary) 报告和由发件人信誉过滤拦截的邮件

由于由发件人信誉过滤拦截的邮件不会进入工作队列，因此 AsyncOS 不处理这些邮件以确定域目标。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。

注释 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。

管理“基于域的执行摘要”(Domain-Based Executive Summary) 报告的域和收件人列表

您可以使用配置文件管理“基于域的执行摘要”(Domain-Based Executive Summary) 报告的域和收件人。配置文件是设备的配置目录中存储的一个文本文件。该文件中的每一行均会生成一个单独的报告。这使您可以在单个报告中包括大量的域和收件人，以及在单个配置文件中定义多个域报告。

配置文件的每行包括一个由空格分隔的域名列表，以及一个由空格分隔的报告收件人邮件地址列表。逗号将域名列表与邮件地址列表隔开。您可以包括子域，方法是在父域名的开头附加子域名和一个句点，例如 subdomain.example.com。

以下是会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
```

注释 您可以使用配置文件和为单个命名报告定义的设置同时生成多个报告。例如，一家名为 Bigfish 的公司收购其他两家公司 Redfish 和 Bluefish，并继续保持这两家公司的域名。Bigfish 使用一个配置文件创建单个“基于域的执行摘要”(Domain-Based Executive Summary) 报告，该配置文件包含与单独的域报告相对应的三行。当设备生成“基于域的执行摘要”(Domain-Based Executive Summary) 报告时，Bigfish 的一位管理员收到关于 Bigfish.com、Redfish.com 和 Bluefish.com 域名的报告，同时 Redfish 的一位管理员收到关于 Redfish.com 域名的报告，Bluefish 的一位管理员收到关于 Bluefish.com 域名的报告。

您可以将每个命名报告的不同配置文件上传到设备。您还可以为多个报告使用相同的配置文件。例如，您可能创建单独的命名报告，提供关于相同的域在不同时间段的数据。如果您更新设备上的配置文件，您不必更新 GUI 中的报告设置，除非您更改文件名。

创建“基于域的执行摘要”(Domain-Based Executive Summary) 报告

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) 依次选择**邮件 (Email) > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。
b) 点击**添加计划的报告 (Add Scheduled Report)**。

要创建按需的报告，请执行以下操作：

- 依次选择**邮件 (Email) > 报告 (Reporting) > 存档的报告 (Archived Reports)**。
- 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和报告收件人的邮件地址。您可以为生成报告选择以下选项之一：

- 通过指定各个域生成报告 (Generate report by specifying individual domains)。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。您还可以使用子域，例如 subdomain.yourdomain.com。如果您为预计不会频繁发生变化的少量域创建报告，建议指定各个域。
- 通过上载文件生成报告 (Generate reports by uploading file)。导入包含域列表和报告收件人邮件地址的配置文件。您可以从设备上的配置目录选择一个配置文件，或从您的本地计算机上传一个配置文件。如果您为频繁发生变化的大量域创建报告，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，请参阅管理“基于域的执行摘要”(Domain-Based Executive Summary) 报告的域和收件人列表 ，第 75 页。

注释 如果您将报告发送到外部账户（如 Yahoo! 邮箱或 Gmail），则可能需要将报告回信地址添加到外部账户的白名单，以防止报告邮件被错误地归类为垃圾邮件。

步骤 4 在“标题”(Title) 文本字段中，键入报告标题的名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建多个名称相同的报告。

步骤 5 在“外发域 (Outgoing Domain)”部分中，选择传出邮件摘要的域类型。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。您可以通过点击“预览 PDF 报告”(Preview PDF Report) 立即以 PDF 文件形式查看报告。
- CSV。创建以逗号分隔值格式包含原始数据的 ASCII 文本文件。每个 CSV 文件最多可以包含 100 行。如果报告包含多个类型的表，则会为每个表创建单独的 CSV 文件。

步骤 8 从“计划”(Schedule) 部分中，为生成报告选择一个计划。

选项包括：“每日”(Daily)、“每周”(Weekly)（包括星期几的下拉列表）或“每月”(Monthly)。

步骤 9 （可选）上传报告的自定义徽标。徽标出现在报告的顶部。

- 徽标应为 .jpg、.gif 或 .png 文件，最大尺寸为 550 x 50 像素。
- 如果未提供徽标文件，则使用默认的思科徽标。

步骤 10 为此报告选择一种语言。要以亚洲语言生成 PDF，请参阅打印和导出报告和跟踪数据 ，第 27 页的重要信息。

步骤 11 点击**提交**以提交对页面所做的更改，然后点击**确认**以确认所做的更改。

“执行摘要”报告

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

此报告总结了您可以在“邮件报告概述”页面，第 43 页上查看的信息。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，第 43 页。

“计划的报告”页面

计划邮件报告

可以计划在关于计划和按需的邮件报告，第 72 页中列出的任何报告。

要管理报告计划，请参阅以下内容：

添加计划的报告

要添加计划的邮件报告，请执行以下步骤：

步骤 1 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 选择您的报告类型。

有关报告类型的说明，请参阅关于计划和按需的邮件报告，第 72 页。

注释 - 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”(Domain-Based Executive Summary) 报告，第 74 页。

- 计划的报告的可用选项因报告类型而异。本操作程序其余部分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。

为了避免创建多个使用相同名称的报告，我们建议使用说明性的标题。

步骤 5 从**要包括的时间范围**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。大多数报告还允许您将原始数据另存为 CSV 文件。

步骤 7 根据报告，对于“行数”，请选择要包括的数据量。

步骤 8 根据报告，选择要作为报告排序依据的列。

步骤 9 从**计划 (Schedule)** 区域中，为计划的报告选中天、周或月旁边的单选按钮。此外，请包括您要计划报告的时间。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，输入生成的报告将发送到的邮件地址。

如果不指定邮件收件人，则系统仍会将报告存档。

您可以根据需要为报告添加任意数量的收件人，不添加收件人也没问题。但是，如果您需要将报告发送到大量地址，则可能需要创建邮件列表，而不是逐个列出收件人。

步骤 11 选择报告的语言。

有关亚洲语言，请参阅打印和导出报告和跟踪数据 ，第 27 页的重要信息。

步骤 12 点击**提交**。

编辑计划的报告

步骤 1 依次选择**邮件 (Email) > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

步骤 2 在“报告标题”(Report Title) 列中点击要修改的报告的名称链接。

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

要防止未来继续生成计划的报告，请执行以下步骤：

步骤 1 依次选择**邮件 (Email) > 报告 (Reporting) > 计划的报告 (Scheduled Reports)**。

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

步骤 3 点击**删除**。

注释 未自动删除已删除的报告的任何存档版本。要删除以前生成的报告，请参阅删除已存档的报告 ，第 80 页。

按需生成邮件报告

除可以使用了解“邮件报告”页面 ，第 37 页中介绍的交互报告页面查看（并为其生成 PDF）的报告之外，您还可以随时在指定的时间段为关于计划和按需的邮件报告 ，第 72 页中列出的报告保存 PDF 或原始数据 CSV 文件。

要生成按需的报告，请执行以下操作：

步骤 1 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的邮件报告 ， 第 72 页。

步骤 4 在“标题”(Title) 文本字段中，键入报告标题的名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建多个名称相同的报告。

注释 有关“基于域的执行摘要”(Domain-Based Executive Summary) 报告的设置信息，请参阅“基于域的执行摘要”(Domain-Based Executive Summary) 报告 ， 第 74 页。

计划报告的可用选项因报告类型而异。本操作程序其余部分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，为报告数据选择一个时间范围。

请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。您可以通过点击“预览 PDF 报告”(Preview PDF Report) 立即以 PDF 文件形式查看报告。
- CSV。创建以逗号分隔值格式包含原始数据的 ASCII 文本文件。每个 CSV 文件最多可以包含 100 行。如果报告包含多个类型的表，则会为每个表创建单独的 CSV 文件。

步骤 7 选择要为其运行报告的设备或设备组。如果您尚未创建任何设备组，此选项不会出现。

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

- 选中**将报告存档 (Archive Report)** 复选框，将报告存档。

如果选择此选项，报告将在“已存档的报告”(Archived Reports) 页面上列出。

注释 无法对“基于域的执行摘要”(Domain-Based Executive Summary) 报告进行存档。

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

在文本字段中，请输入报告的收件人邮件地址。

步骤 9 为此报告选择一种语言。要以亚洲语言生成 PDF，请参阅打印和导出报告和跟踪数据 ， 第 27 页的重要信息。

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

“存档的邮件”报告页面

- 按需生成邮件报告 ，第 78 页
- 查看和管理已存档的邮件报告 ，第 80 页

查看和管理已存档的邮件报告

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。在添加新的报告时，系统会删除较旧的报告以将数量保持在 1000 个。

已存档的报告存储在设备上的 /periodic_reports 目录。（有关详细信息，请参阅IP 接口和访问设备 ，第 373 页。）

访问存档的报告

邮件 > 报告 > 存档的报告页面列出了您已选择存档的计划和按需报告，这些报告已生成但未清除。

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。

删除已存档的报告

系统会根据查看和管理已存档的邮件报告 ，第 80 页概述的规则自动删除报告。但是您可以手动删除不需要的报告。

要手动删除已存档的报告，请执行以下操作：

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

此时将显示可用的已存档报告。

步骤 2 选中一个或多个要删除的报告的复选框。

步骤 3 点击**删除**。

步骤 4 要防止未来继续生成计划的报告，请参阅终止计划的报告 ，第 78 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 30 页。

病毒爆发过滤器报告未正确显示信息

问题

病毒爆发过滤器报告未正确显示威胁信息。

解决方案

确认设备可以与管理设备 > 系统管理 > 更新设置中指定的思科更新服务器通信。

在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

在从报告中进行深入分析时，邮件跟踪结果与预期的结果不相符。

解决方案

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。仅当启用每项功能（报告、跟踪）时，才会获取该功能的数据。

相关主题

- 检查邮件跟踪数据的可用性 ，第 136 页

高级恶意软件保护判定更新报告结果存在差异

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。

解决方案

这种情况是暂时的。下载了所有判定更新后，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。

解决方案

请参阅文件分析报告详细信息的要求 ， 第 60 页。

查看文件分析 (File Analysis) 报告详细信息时出错

问题

当您尝试查看“文件分析”(File Analysis) 报告详细信息时，出现没有可用的云服务器配置 (No cloud server configuration is available) 错误。

解决方案

转到**管理设备 > 集中服务 > 安全设备**，然后添加至少一个启用了文件分析功能的邮件安全设备。

使用私有云 Cisco AMP Threat Grid 设备查看文件分析 (File Analysis) 报告详细信息时出错

问题

当您尝试查看“文件分析”(File Analysis) 报告详细信息时，出现 API 密钥、注册或激活错误。

解决方案

如果您使用私有云（本地部署的）Cisco AMP Threat Grid 设备进行文件分析，请参阅（本地文件分析）激活文件分析账户 ， 第 61 页。

如果 Threat Grid 设备主机名发生更改，您必须重复执行所引用操作程序中的流程。

文件分析相关错误的记录

注册及其他与文件分析相关的错误均记录在 GUI 日志中。

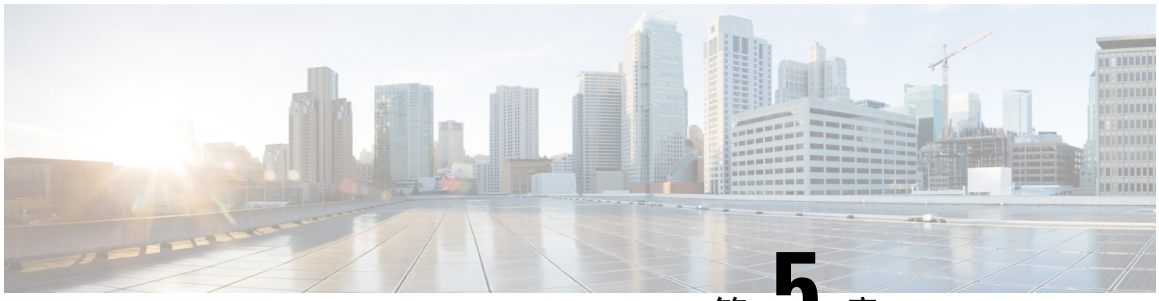
灰色邮件或营销邮件总数似乎不正确

问题

“营销”、“社交”和“批量”邮件的计数超过灰色邮件总数。

解决方案

“营销”(Marketing) 邮件总数包括在升级到 AsyncOS 9.5 前后收到的营销邮件，但是灰色邮件的总数仅包括在升级后收到的邮件。请参阅在升级到 AsyncOS 9.5 后报告营销邮件 ， 第 69 页。



第 5 章

使用集中 Web 报告和跟踪

本章包含以下部分：

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 报告功能不仅可生成概要报告，使管理员可以了解网络上发生的情况，而且还使管理员可以深入分析并查看特定域、用户或类别的流量详细信息。

域

对于域，Web 报告功能可以将以下数据元素生成到域报告。例如，如果您在 Facebook.com 域上生成报告，则报告可能包含：

- 访问 Facebook.com 的排名靠前的用户的列表
- Facebook.com 内访问量排名靠前的 URL 的列表

用户

对于用户，Web 报告功能可以将数据元素生成到用户报告。例如，对于标题为“Jamie”的用户报告，报告可能包含：

- 用户“Jamie”访问的排名靠前的域的列表
- 具有恶意软件或病毒特征的排名靠前的 URL 的列表
- 用户“Jamie”访问的排名靠前的类别的列表

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，对于类别“Sports”，报告可能包含：

- 位于“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

在上述所有这些示例中，这些报告旨在提供网络上特定项目的综合视图，以便管理员可以采取行动。

常规

有关记录页面与报告页面的详细说明，请参阅日志记录与报告，第 333 页。

注释 您可以检索用户访问的所有域信息，而不一定是用户访问的特定URL。有关用户访问的特定URL、用户访问 URL 的时间以及是否允许相应 URL 等信息，可使用“网络跟踪”(Web Tracking) 页面上的搜索网络代理服务处理的事务，第 123 页。

注释 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 89 页。
- 要按需生成报告，请参阅按需生成 Web 报告，第 120 页。
- 要安排重复性地定期生成报告，请参阅关于计划的报告和按需 Web 报告，第 116 页。
- 要查看以前运行的报告（已安排和按需生成）的存档版本，请参阅查看和管理存档的 Web 报告，第 122 页。
- 要查看各个事务的信息，请参阅Web 跟踪，第 122 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 87 页

• 在 Web 报告中使用匿名 ， 第 88 页
• 在网络安全设备上启用集中 Web 报告 ， 第 87 页
• 将集中 Web 报告服务添加到每个托管网络安全设备 ， 第 87 页
• 在 Web 报告中使用匿名 ， 第 88 页

在安全管理设备上启用集中 Web 报告

步骤 1 在启用集中 Web 报告之前，请确保已为该服务分配足够的磁盘空间。请参阅管理磁盘空间 ， 第 320 页。

步骤 2 在安全管理设备上，依次择**管理设备 > 集中服务 > 网络 > 集中报告**。

步骤 3 如果您是在运行“系统设置向导”(System Setup Wizard) 后首次启用集中报告：

a) 点击**启用**。

b) 审查终端用户许可协议，然后点击**接受**。

步骤 4 如果您是在先前禁用集中报告后将其再次启用：

a) 点击**编辑设置**。

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 88 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《思科网络安全设备 AsyncOS 用户指南》中的“启用集中报告”部分。

将集中 Web 报告服务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。

步骤 1 在安全管理设备上，依次择**管理设备 > 集中服务 > 安全设备**。

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”。

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。

注释 可以在“IP 地址 (IP Address)”文本字段中输入 DNS 名称，但点击**提交**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) 在要托管的设备上输入管理员账户的用户名和密码，然后点击**建立连接**。

注释 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 (Test Connection)**。

h) 阅读表格上方的测试结果。

步骤 4 点击**提交**。

步骤 5 为每个您要启用集中报告的网络安全设备重复此操作步骤。

步骤 6 确认您的更改。

在 Web 报告中使用匿名

默认情况下，用户名显示在报告页面上和 PDF 中。但是，为保护用户隐私，您可能希望在 Web 报告中令用户名无法识别。

注释 设备上具有管理员权限的用户在查看交互报告时可以始终查看用户名。

步骤 1 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 2 点击**编辑设置**。

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
访问和查看报告数据的视图选项	查看报告数据的各种方法 ， 第 19 页

目标	请参阅
自定义交互报告页面的视图	自定义报告数据的视图 ，第 21 页
查找数据内特定事务的信息	Web 跟踪 ，第 122 页
打印或导出报告信息	打印和导出报告和跟踪数据 ，第 27 页
了解各种交互报告页面	Web 报告页面说明，第 89 页
按需生成报告	按需生成 Web 报告 ，第 120 页
安排报告，以便按指定的间隔和时间自动运行	关于计划的报告和按需 Web 报告，第 116 页
查看按需存档的报告和已安排的报告	查看和管理存档的 Web 报告，第 122 页
了解数据的收集方式	安全管理设备如何收集报告的数据，第 20 页

Web 报告页面说明

注释 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，请参阅关于计划的报告和按需 Web 报告，第 116 页。

表 *19:* “*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 ，第 92 页	“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，第 92 页。

“Web 报告”(Web Reporting) 菜单	操作
用户报告 (Web) ，第 93 页	“用户”(Users) 页面提供多个网络跟踪链接，允许您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。从该页面您可以深入研究系统上各个用户的活动。如果您正在运行用户级调查，并且需要查找诸如用户正在访问哪些站点、他们遇到了哪些恶意软件威胁、正在访问哪些URL类别，以及特定用户在这些站点上花费了多少时间等信息，则此页面将非常有用。 有关详细信息，请参阅用户报告 (Web) ，第 93 页。有关您的系统中特定用户的信息，请参阅用户详细信息（Web 报告） ，第 95 页
网站报告 ，第 96 页	“网站”(Web Sites) 页面允许您查看托管设备上所发生的活动的汇聚情况。从该页面您可以监控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 ，第 96 页。
URL 类别报告 ，第 97 页	利用“URL 类别”(URL Categories) 页面可以查看所访问的排名靠前的 URL 类别，包括： • 每个事务已触发阻止或警告操作发生的排名靠前的 URL。 • 已完成、已警告和已阻止事务在指定时间范围内的所有URL类别。这是一个交互表，具有交互列标题，您可以使用该列标题按需排序数据。 有关详细信息，请参阅URL 类别报告 ，第 97 页。
应用可视性报告 ，第 99 页	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 ，第 99 页。
防恶意软件报告 ，第 101 页	“防恶意软件”(Anti-Malware) 页面允许您查看在指定时间范围内防恶意软件扫描引擎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每个排名靠前的恶意软件端口和网站的连接数量。报告的下半部分显示检测到的恶意软件端口和网站。有关详细信息，请参阅防恶意软件报告 ，第 101 页。
高级恶意软件保护（文件信誉和文件分析）报告 ，第 104 页	有三个显示文件信誉和分析数据的报告页面。 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 ，第 104 页。

“Web 报告”(Web Reporting) 菜单	操作
客户端恶意软件风险报告，第 108 页	“客户端恶意软件风险”(Client Malware Risk) 页面是一个安全相关的报告页面，可以用于确定那些正异常频繁地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 ，第 108 页。
网络信誉过滤器报告 ，第 109 页	允许您查看指定时间范围内事务的网络信誉过滤报告。有关详细信息，请参阅网络信誉过滤器报告 ，第 109 页。
L4 流量监控器报告 ，第 111 页	允许您查看在指定时间范围内第 4 层流量监控器检测到的恶意软件端口和恶意站点的信息。有关详细信息，请参阅L4 流量监控器报告 ，第 111 页。
SOCKS 代理报告 ，第 113 页	允许您查看 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 ，第 113 页。
按用户地点分类的报告，第 113 页	“按用户位置报告”(Reports by User Location) 页面允许您查看您的移动用户正在其本地或远程系统上执行哪些活动。 有关详细信息，请参阅按用户地点分类的报告 ，第 113 页。
Web 跟踪 ，第 122 页	“网络跟踪”(Web Tracking) 页面允许您搜索以下类型的信息： • 通过搜索网络代理服务处理的事务，第 123 页，可以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，同时还包括特定 URL 类型、每个连接占用了多少带宽以及跟踪特定用户的网络使用情况等信息。 • 通过搜索 L4 流量监控器处理的事务 ，第 126 页，可以搜索 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。 • 通过搜索 SOCKS 代理处理的事务 ，第 127 页，可以搜索 SOCKS 代理处理的事务。 有关详细信息，请参阅Web 跟踪 ，第 122 页。
系统容量页面，第 114 页	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 ，第 114 页。
“数据可用性”页面，第 116 页	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 ，第 116 页。
计划的报告	允许您为指定时间范围安排报告。有关详细信息，请参阅关于计划的报告和按需 Web 报告 ，第 116 页。

“Web 报告”(Web Reporting) 菜单	操作
存档的报告	允许您为指定时间范围存档报告。有关详细信息，请参阅查看和管理存档的 Web 报告 ， 第 122 页。

注释 您可以为大多数 Web 报告类别安排报告，包括扩展的排名靠前的 URL 类别和排名靠前的应用类型的附加报告。有关安排报告的更多信息，请参阅关于计划的报告和按需 Web 报告 ， 第 116 页

关于所花费时间(Time Spent)

各个表中“所花费时间”(Time Spent) 列表示用户在某个网页上所花费的时间。用户在每个 URL 类别上所花费的时间（为了用户调查）。当跟踪 URL 时，每个用户在该特定 URL 上所花费的时间。

一旦事务事件被标记“已查看”(viewed)，即用户访问特定 URL，将会开始计算一个“所花费时间”(Time Spent) 值，并将其添加为 Web 报告表中的一个字段。

为计算所花费时间，AsyncOS 针对一分钟期间内的活动为每个活动用户分配 60 秒时间。在这一分钟结束时，在用户访问的不同域之间将会均分每个用户所花费的时间。例如，如果用户在一个活动分钟内访问四个不同的域，则会认为该用户在每个域花费 15 秒。

对于所花费时间值，请注意以下事项：

- 活动用户定义为通过设备发送 HTTP 流量并访问 AsyncOS 视为一次“页面阅览”的网站的用户名或 IP 地址。
- AsyncOS 会将页面阅览定义为用户发起的 HTTP 请求，与客户端应用发起的请求相对。AsyncOS 使用启发式算法进行最佳猜测，以确定用户页面阅览量。

单位以小时：分钟格式显示。

Web 报告概述

网络 > 报告 > 概述页面提供您的网络安全设备上的活动概要。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。事务摘要为诸如可疑事务等内容提供进一步的趋势详细信息，并且直接从此图中可以了解阻止了多少上述可疑事务，以及阻止的方式。

概述 (Overview) 页面的下半部分介绍使用情况。也就是查看的排名靠前的 URL 类别、排名靠前的应用类型以及被阻止的类别，生成这些阻止或警告的排名靠前的用户。

表 *20:* “*Web* 报告概述”页面详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围 ， 第 22 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 22 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）。
网络代理摘要 (Web Proxy Summary)	本部分允许您查看可疑或正常的网络代理活动的百分比，包括事务总数。
L4 流量监控摘要	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	本部分允许您查看被管理员标记为可疑事务的网络事务。 本部分显示事务的实际数量（垂直标尺），以及活动发生的大约日期（水平时间线）。
可疑事务摘要 (Suspect Transactions Summary)	本部分允许您查看因可疑而被阻止或警告的事务的百分比。另外，您可以查看已被检测和阻止的事务的类型，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 (Top URL Categories by Total Transactions)	本部分显示被阻止的排名靠前 10 个 URL 类别，包括 URL 类别的类型（垂直标尺）以及已阻止的特定类型类别的实际次数（水平标尺）。 预定义的 URL 类别集会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告 ， 第 98 页。
按事务总数排名靠前的应用类型 (Top Application Types by Total Transactions)	本部分显示正阻止的排名靠前的应用类型，包括实际应用类型的名称（垂直标尺）和已阻止的特定应用的次数（水平标尺）。
检测到的恶意软件类别总数 (Top Malware Categories Detected)	此部分显示检测到的所有恶意软件类别。
受阻或警告事务数排名靠前的用户 (Top Users Blocked or Warned Transactions)	本部分显示生成已阻止或已警告事务的实际用户。可以按 IP 地址或按用户名称来显示用户。要使用户名无法识别，请参阅在 Web 报告中使用匿名 ， 第 88 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。

注释 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 *21:*“网络”>“报告”>“用户”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围 ，第 22 页。
按受阻事务数排名靠前的用户 (Top Users by Transactions Blocked)	本部分的垂直标尺按 IP 地址或用户名列出排名靠前的用户，水平标尺列出针对该用户所阻止的事务数量。报告时可以将用户名或 IP 地址进行匿名。有关如何在此页或在已安排报告中令用户名无法无法识别的更多信息，请参阅在安全管理设备上启用集中 Web 报告 ，第 87 页。默认设置为所有用户名均显示。要隐藏用户名，请参阅在 Web 报告中使用匿名 ，第 88 页。
按使用的带宽排名靠前的用户 (Top Users by Bandwidth Used)	本部分的垂直标尺按 IP 地址或用户名列出系统上排名靠前的用户,水平标尺上以 GB 显示在系统上使用最多带宽的用户。
用户表 (Users Table)	您可以找到查找特定用户 ID 或客户端 IP 地址。在“用户”(User) 部分底部的文本字段中，请输入特定用户 ID 或客户端 IP 地址，并点击**查找用户 ID 或客户端 IP 地址 (Find User ID or Client IP Address)**。IP 地址不需要是精确匹配项就可以返回结果。 在“用户”(Users) 表，可以点击特定用户以找到更具体的信息。此信息显示在“用户详细信息”(User Details) 页面。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） ，第 95 页。

注释 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。有关详细信息，请参阅与 LDAP 集成，第 223 页章节中的创建 LDAP 服务器配置文件，第 224 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 88 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 ，第 389 页。

注释 您可以为“用户”(Users) 页生成或安排报告。有关更多信息，请参阅关于计划的报告和按需 Web 报告 ， 第 116 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。如果您正在运行用户级调查，并且需要查找诸如用户正在访问哪些站点、他们遇到了哪些恶意软件威胁、正在访问哪些 URL 类别，以及特定用户在这些站点上花费了多少时间等信息，则此页面将非常有用。

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**页面，可以查看有关系统中各个用户的以下信息：

表 *22*: “网络”>“报告”>“用户”>“用户详细信息”页面详细信息

部分	说明
时间范围 (Time Range)（下拉列表）	该菜单允许您选择报告中所包含数据的时间范围。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围 ， 第 22 页。
按事务总数的 URL 类别 (URL Categories by Total Transactions)	本部分列出特定用户正在使用的特定 URL 类别。 预定义的URL类别集会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告 ， 第 98 页。
按事务总数的趋势 (Trend by Total Transactions)	本图显示了用户访问网络的时间。 例如，此图将指示在一天的某些时段内是否存在网络流量激增以及这些激增发生的时间。使用“时间范围”(Time Range) 下拉列表，您可以扩展此图，以查看此用户在网络上的更为精细或粗略的时间范围。
匹配的 URL 类别 (URL Categories Matched)	“匹配的 URL 类别”(URL Categories Matched) 部分显示了已完成和已阻止事务的匹配类别。 从本部分您还可以找到特定的 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)**。该类别不需要是完全匹配。 预定义的URL类别集会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告 ， 第 98 页。
匹配的域 (Domains Matched)	在本部分，您可以查看此用户已经访问的特定域或 IP 地址的相关信息。您还可以查看在这些类别上所花费的时间，以及您在列视图中设置的其他各类信息。在该部分底部的文本字段中，输入域或 IP 地址，并点击**查找域或 IP (Find Domain or IP)**。域或 IP 地址不必是完全匹配。

部分	说明
匹配的应用 (Applications Matched)	在此部分,可以找到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，您将在“应用”(Application) 列中看到此应用类型。 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)**。应用的名称不必是完全匹配。
检测到的恶意软件威胁数 (Malware Threats Detected)	在此表中，您可以查看特定用户触发的排名靠前的恶意软件威胁。 您可以在“查找恶意软件威胁”(Find Malware Threat) 字段中搜索特定恶意软件威胁名称的数据。输入“恶意软件威胁”(Malware Threat) 名称并点击“查找恶意软件威胁”(Find Malware Threat)。恶意软件威胁的名称不必是完全匹配。
匹配的策略 (Policies Matched)	在此部分，可以找到当用户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)**。策略的名称不必是完全匹配。

注释 在“客户端恶意软件风险详细信息”(Client Malware Risk Details) 表：客户端报告有时会在用户名的末尾显示星号 (*). 例如，客户端报告可能会同时为“jsmith”和“jsmith*”显示一个条目。带有星号 (*) 的用户名表示用户提供的用户名，但并未经身份验证服务器确认。当身份验证服务器不可用，并且设备配置为在身份验证服务不可用的情况下允许流量时，可能会出现上述情况。

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 ， 第 389 页。

网站报告

网络 (Web) > 报告 (Reporting) > 网站 (Web Sites) 页面汇聚了受管设备上所发生活动的整体情况。从该页面您可以监控特定时间范围内访问的高风险网站。

在**网站**页，您可以查看以下信息：

表 *23*: “网络”>“报告”>“网站”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围 ， 第 22 页。
按事务总数排名靠前的域 (Top Domains by Total Transactions)	本部分以图的形式站点上被访问量排名靠前的域。
按受阻事务数排名靠前的域 (Top Domains by Transactions Blocked)	本部分以图的形式按事务列出触发阻止操作的排名靠前的域。例如，用户访问了某特定域，并且由于布置了我拥有的一个特定策略，这触发了阻止操作。此域会在此图中以受阻止事务列出，并且列出触发了阻止操作的域站点。

部分	说明
匹配的域 (Domains Matched)	本部分在一个交互表中列出了该站点上正被访问的域。在此表中，通过点击特定域，您可以访问该特定域的更为详细的信息。在“网络跟踪”(Web Tracking) 页面上的“代理服务”(Proxy Services) 选项中，您可以查看跟踪信息以及某些域被阻止的原因。 当您点击某个特定域时，您可以查看到该域的排名靠前的用户、该域上排名靠前的事务、匹配的 URL 类别以及检测到的恶意软件威胁。 要查看如何使用网络跟踪的示例，请参阅示例 2：跟踪 URL ，第 391 页。 **注释** 如果您将此数据导出到 .csv 文件，则系统仅导出前 300000 个条目。

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 88 页。

注释 您可以在“网站”(Web Sites) 页面上生成或安排报告。有关更多信息，请参阅关于计划的报告和按需 Web 报告 ，第 116 页。

URL 类别报告

网络 > 报告 > URL 类别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**页面中，您可以查看以下信息：

表 *24:*“网络”>“报告”>“*URL* 类别”页面上的详细信息

部分	说明
时间范围 (Time Range) 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 ，第 22 页。
按事务总数排名靠前的 URL 类别 (Top URL Categories by Total Transactions)	本部分以图的形式列出站点上排名靠前的被访问 URL 类别。
按阻止和警告的事务数排名靠前的 URL 类别 (Top URL Categories by Blocked and Warned Transactions)	本部分以图的形式按事务列出触发阻止或警告操作的排名靠前的URL。例如，用户访问了某特定URL，并且由于布置了一个特定策略，这触发了阻止操作或警告。然后此 URL 会作为受阻止的事务或警告在图中列出。
匹配的 URL 类别 (URL Categories Matched)	“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，以及使用的带宽和每个类别中所花费的时间。 如果有大量未分类的 URL，请参阅减少未分类的 URL ，第 98 页。

部分	说明
被绕过的 URL 过滤 (URL Filtering Bypassed)	表示在 URL 过滤前发生的策略、端口和管理用户代理阻止。

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 88 页。

注释 要生成比此页面提供信息更为详细的报告，请参阅URL 类别排行榜 - 扩展 ，第 119 页。

- 如果在计划报告内为URL类别使用“数据可用性”，并且在任意设备之间存在着数据差异，则会在页面底部显示以下信息：“此时间范围内的某些数据不可用”。如果没有数据差异，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，您可以创建自定义 URL 类别，并将其应用到特定用户或组策略。这些事务将改为包括在“被绕过的 URL 过滤”(URL Filtering Bypassed) 统计信息内。为此，请参阅有关适用于思科网络安全设备的 AsyncOS 用户指南的自定义 URL 类别的信息。
- 对于您认为应包括在现有或其他类别的站点，请参阅报告错误分类和未分类的 URL ，第 99 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 212 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，您在同一报告中可以同时看到旧类别和新类别。

如果新旧类别的内容之间有重叠，则您可能需要仔细检查报告结果以获取有效的统计信息。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。类似地，在合并后对即时消息或基于网络的聊天站点的访问将会包括在“即时消息”(Instant Messaging) 或“基于网络的聊天”(Web-based Chat) 类别内。

将“URL 类别”页面与其他报告页面结合使用

“URL 类别”(URL Categories) 页面可以与应用可视性报告 ，第 99 页和用户报告 (Web) ，第 93 页配合使用，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 ， 第 97 页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，您可以在“URL 类别”(URL Categories) 交互表中收集关于流媒体 (Streaming Media) URL 类别的更多详细信息。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。此页面不仅显示访问流媒体站点的排名靠前的用户（在“按事务总数排名靠前的类别的用户”[Top Users by Category for Total Transactions] 部分），同时还显示所访问的域（在“匹配的域”[Domains Matched] 交互表中），例如，YouTube.com 或 QuickPlay.com。

此时，您会获得特定用户的越来越精准的信息。现在，让我们假设此特定用户因为其用量而显得尤为突出，则您可能想确切地找出他们正在访问什么内容。在这里，您可以在“用户”(Users) 交互表中点击用户。此操作会将您带到用户报告 (Web) ， 第 93 页，您可以在这里查看该用户的用户趋势，并准确地了解他们正在网络做什么。

如果您希望了解更多内容，现在可以点击交互表中的“已完成事务”(Transactions Completed) 链接，深入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 ， 第 123 页，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：调查受访问的排名靠前的 URL 类别 ， 第 391 页。

报告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

会评价提交，以便包括在后续规则更新中。

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

注释 有关应用可视性的详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》的“了解应用可视性与可控性”一章。

通过**网络 > 报告 > 应用可视性**页，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。

应用控件不仅可以为您提供比只使用URL过滤更为精细的网络流量控制，同时它会为您提供对诸如以下应用类型的更多控制：

- 规避应用，例如匿名程序和加密隧道。
- 协作应用，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

了解应用和应用类型之间的差异以便可以控制报告涉及的应用，这一点至关重要。

- **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。即时消息是另一种应用类型类别，可能包含 Yahoo Instant Messenger 或 Cisco WebEx。Facebook 也是一种应用类型。
- **应用**。属于某一应用类型的特定应用。例如，YouTube 是一种媒体 (Media) 应用类型的应用。
- **应用行为**。用户可以在应用中完成的特定操作或行为。例如，用户可以在使用某种应用（例如 Yahoo Messenger）时传输文件。并非所有应用均包括您可以配置的应用行为。

注释 要了解有关如何使用应用可视性与可控性 (AVC) 引擎来控制 Facebook 活动的详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》的“了解应用可视性与可控性”一章。

在**应用可视性**页面中，您可以查看以下信息：

表 25:“Web 报告应用可视性”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围 ，第 22 页。
按事务总数排名靠前的应用类型 (Top Application Types by Total Transactions)	本部分以图的形式列出站点上排名靠前的被访问应用类型。例如，像 Instant Messenger 这样的即时聊天工具、Facebook 和演示应用类型。
按受阻事务数排名靠前的应用 (Top Applications by Blocked Transactions)	本部分以图的形式按事务列出触发阻止操作的排名靠前的应用类型。例如，用户尝试启动某个应用类型，例如 Google Talk 或 Yahoo Instant Messenger，由于特定策略已就位，这触发了阻止操作。然后此应用会作为受阻止的事务或警告在图中列出。
匹配的应用类型 (Application Types Matched)	“匹配的应用类型”(Application Types Matched) 交互表允许您查看“按事务总数排名靠前的应用类型”(Top Applications Type by Total Transactions) 表中列出的应用类型。在“应用”(Applications) 列，您可以点击某个应用以查看详细信息
匹配的应用 (Applications Matched)	“匹配的应用”(Applications Matched) 部分显示在指定时间范围内的所有应用。这是一个交互表，具有交互列标题，您可以使用该列标题按需排序数据。 您可以配置您希望显示在“匹配的应用”(Applications Matched) 部分中的列。有关为本部分配置列的信息，请参阅与网络安全报告一起使用 ，第 88 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。选项有：10、20、50 或 100。 此外，您可以在匹配的应用 (Applications Matched) 部分查找特定应用。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 88 页。

注释 您可以为“应用可视性”(Application Visibility) 页面上的信息生成已安排报告。有关安排报告的信息，请参阅关于计划的报告和按需 Web 报告，第 116 页。

防恶意软件报告

网络 > 报告 > 防恶意软件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。

使用此页面可以帮助识别和监控基于网络的恶意软件威胁。

注释 要查看第 4 层流量监控发现的恶意软件的数据，请参阅L4 流量监控器报告，第 111 页。

在**防恶意软件**页面中，可以查看以下信息：

表 *26:*“网络”>“报告”>“防恶意软件”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围，第 22 页。
“排名靠前的恶意软件类别：受监控或受阻止”(Top Malware Categories: Monitored or Blocked)	本部分显示指定类别类型检测到的排名靠前的恶意软件类别。此信息以图的形式显示。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 102 页。
“排名靠前的恶意软件威胁：受监控或受阻止”(Top Malware Threats: Monitored or Blocked)	本部分显示排名靠前的恶意软件威胁。此信息以图的形式显示。
恶意软件类别数	“恶意软件类别”(Malware Categories) 交互表为在“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显示详细信息。 点击“恶意软件类别”(Malware Categories) 交互表中的任意链接，您可以更为精细地查看各个恶意软件类别及其位于网络上哪个位置的详细信息。 例外：该表中的“病毒爆发启发式扫描”(Outbreak Heuristics) 链接，允许您查看一个图表，其中显示了何时出现此类别的事务。 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 102 页。

部分	说明
恶意软件威胁数 (Malware Threats)	“恶意软件威胁数”(Malware Threats) 交互表在为“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显示详细信息。 以一个数字标记为“病毒爆发”(Outbreak) 的威胁是由 Adaptive Scanning 功能独立于其他扫描引擎标识的威胁。

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 88 页。

恶意软件类别报告 (Malware Category Report)

“恶意软件类别报告”(Malware Category Report) 页允许您查看单个恶意软件类别的详细，以及它在您的网络中正在执行哪些操作。

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

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 88 页。

恶意软件威胁报告 (Malware Threat Report)

“恶意软件威胁报告”(Malware Threat Report) 页显示遭受特定威胁风险的客户端，显示可能受感染客户端的列表，以及指向“客户端详细信息”(Client Detail) 页的链接。报告顶部的趋势图显示在指定的时间范围内因某威胁受到监控和阻止的事务。底部的表显示在指定的时间范围内因某威胁受到监控和阻止的事务的实际数量。

要查看此报告，请在“防恶意软件报告”(Anti-Malware report) 页的“恶意软件类别”(Malware Category) 列中点击一个类别。

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。

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
广告软件	广告软件包含可将用户引导至待售产品的所有软件可执行文件和插件。某些广告软件应用具有并发运行并彼此监控的单独进程，确保修改是永久的。某些变体使得它们自己可以在每次计算机启动时自动运行。这些程序也可能更改安全设置，使得用户无法对其浏览器搜索选项、桌面和其他系统设置进行更改。
浏览器助手对象	浏览器助手对象是一个浏览器插件，可以执行与提供广告或劫持用户设置相关的各种功能。
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	拨号程序是一种程序，利用您的调制解调器或其他类型的互联网访问方式，将您连接到某个电话线路或站点，意图在您并未提供充分、明确且知情许可的情况下套取您的长途电话费用。
常规间谍软件	间谍软件是一种安装在计算机上的恶意软件，旨在未获得用户许可的情况下收集碎片信息。
劫持程序	劫持程序修改系统设置或对用户系统进行不希望的更改，从而在用户并未提供充分、明确且知情许可的情况下，将用户引导至一个网站或运行一个程序。
其他恶意软件	其他所有未准确契合其他定义类别之一的恶意软件和可疑行为均会归属此类别。
病毒爆发启发式扫描	此类别表示 Adaptive Scanning 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 显示在浏览器地址栏中。在某些情况下，它涉及域名的使用，与合法域的名称类似。网络钓鱼是一种在线身份窃取形式，会使用社交工程和技术手段窃取个人身份数据和财务账户凭证。
PUA	可能不需要的应用。PUA 是非恶意应用，但可能被视为不想要的应用。
系统监视程序	系统监控程序包含执行以下操作之一的任意软件： 公开地或隐蔽地记录系统进程和/或用户操作。 使这些记录可用于以后检索和审核。
特洛伊木马下载程序 (Trojan Downloader)	特洛伊木马下载程序是一种木马程序，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。这些安装通常会无需用户确认即可发生。此外，不同安装之间，特洛伊木马下载程序的有效载荷可能会不同，因为它是从远程主机/站点获取下载说明。
特洛伊木马	特洛伊木马是一种会伪装成良性应用的破坏性程序。不同于病毒，特洛伊木马不会自我复制。

恶意软件类型	说明
特洛伊木马钓鱼程序	特洛伊木马钓鱼程序会驻留在受感染的计算机上，等待他人访问特定网页，或者可能会扫描受感染的计算机来查找银行站点、拍卖站点或在线支付站点的用户名和密码。
病毒	病毒是未经您确认就加载到您的计算机上，并且违背您的意愿运行的程序或代码段。
蠕虫	蠕虫是一种程序或算法，会通过计算机网络进行自我复制，通常执行恶意操作。

高级恶意软件保护（文件信誉和文件分析）报告

文件分析报告详细信息的要求

（云文件分析）确保管理设备可以连接到文件分析服务器

要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。请参阅防火墙资讯 ， 第 385 页中的详细信息。

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 292 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。

如果您使用 HTTPS 代理，则代理不能将流量解密；请使用直通机制与文件分析服务器通信。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其自己的证书。

（云文件分析）配置管理设备以显示详细的文件分析结果

为了使组织中的所有内容安全设备都可以在云中显示有关从组织中的任何思科邮件安全设备或思科网络安全设备送交分析的文件的详细结果，您需要将所有设备加入到同一设备组。

步骤 1 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 滚动至“文件分析”(File Analysis) 部分。

步骤 3 如果您管理的设备指向不同的文件分析云服务器，请选择从中显示结果详细信息的服务器。

将不提供由任何其他云服务器处理的文件的结果详细信息。

步骤 4 输入分析组 ID。

- 如果未正确输入组 ID 或出于任何其它原因需要对其进行更改，则必须向 思科 TAC 提交请求。
- 此更改会立即生效；它不需要“确认”(Commit)。
- 建议将您的 CCOID 用于此值。
- 此值区分大小写。
- 在所有将共享关于上传以供分析的文件的数据的设备上，此值必须相同。
- 一台设备只能属于一个组。
- 您可以随时将设备添加到组，但是只能添加一次。

步骤 5 点击**立即分组 (Group Now)**。

步骤 6 在将与此设备共享数据的每个网络安全设备上配置相同的组。

下一步做什么

相关主题

可以在云中查看哪些文件的详细文件分析结果？ ，第 108 页

（本地文件分析）激活文件分析账户

如果您已部署本地（私有云）的思科 AMP Threat Grid 设备，必须激活思科内容安全管理设备的文件分析账户，才能查看 Threat Grid 设备上提供的报告详细信息。您通常只需执行此操作一次。

开始之前

确保您接收“严重”(Critical) 级别的系统警报。

步骤 1 首次尝试从 Threat Grid 设备访问文件分析报告详细信息时，请等待几分钟，然后您将收到包含一个链接的警报。

如果您没有收到此警报，转到**管理设备 > 系统管理 > 警报**，然后点击**查看排名靠前的警报**。

步骤 2 点击警报消息中的链接。

步骤 3 如有必要，请登录到您的 Cisco AMP Threat Grid 设备。

步骤 4 激活您的管理设备账户。

其它要求

有关任何其他要求，请参阅安全管理设备版本的版本说明，位置：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html

通过 SHA-256 散列标识文件

由于文件名很容易更改，因此设备会使用安全散列算法 (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，所有实例被识别为相同的 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，文件按其 SHA-256 值列出（以缩写格式）。为了标识您的组织中与恶意软件实例相关联的文件名，请选择报告 > 高级恶意软件保护，然后点击表格中的 SHA-256 链接。详细信息页面将显示了关联的文件名。

高级恶意软件防护（文件信誉和文件分析）报告页

报告	说明
高级恶意软件防护 (Advanced Malware Protection)	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。 对于那些具有已更改判定的文件，请参阅 AMP 判定更新报告。这些判定不会反映在“高级恶意软件防护”(Advanced Malware Protection) 报告中。 如果从某个已压缩或已存档的文件中提取的某个文件是恶意文件，则只有这个已压缩或已存档的文件的 SHA 值包括在“高级恶意软件防护”(Advanced Malware Protection) 报告中。

报告	说明
文件分析 (File Analysis)	显示送交分析的每个文件的时间和判定（或临时判定）。设备每 30 分钟检查一次分析结果。 要查看超过 1000 个文件分析结果，请将数据导出为 .csv 文件。 对于采用本地思科 AMP Threat Grid 设备的部署：在思科 AMP Threat Grid 设备上列入白名单的文件显示为“正常”(clean)。有关白名单的信息，请参阅 AMP Threat Grid 联机帮助。 深入查看详细分析结果，包括威胁特征和每个文件的得分。 您还可以直接在执行分析的服务器上查看有关 SHA 目录的其他详细信息，方法是搜索 SHA 或点击文件分析详细信息页面底部的“思科 AMP Threat Grid”链接。 要在分析了文件的服务器上查看详细信息，请参阅文件分析报告详细信息的要求 ，第 104 页。 如果从某个已压缩或已存档的文件中提取的某个文件送交分析，则只有这个已提取文件的 SHA 值包括在“文件分析”(File Analysis) 中。
AMP 判定更新 (AMP Verdict Updates)	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 的判定多次发生变化，此报告仅显示最新的判定，而不显示判定历史记录。 如果多个网络安全设备对于同一文件具有不同的判定更新，则将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。 要在最大可用时间范围内为特定 SHA-256 查看所有受影响的事务（不论为报告选择的是哪种时间范围），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

在相关的情况下，其他报告中会提供文件信誉和分析的数据。默认情况下，设备报告中的“受高级恶意软件防护阻止”(Blocked by Advanced Malware Protection) 列处于隐藏状态。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。

可以在云中查看哪些文件的详细文件分析结果？

如果您部署了公共云文件分析，则可以查看从已添加到文件分析设备组的任何受管设备上传的所有文件的详细结果。

如果您已将管理设备添加到该组，可以查看组中的受管设备列表，方法是依次点击**管理设备 > 集中服务 > 安全设备**页上的按钮。

分析组中的设备由文件分析客户端 ID 标识。要确定特定设备的此标识符，请查看以下位置：

设备	文件分析客户端 ID 的位置
邮件安全设备	**安全服务 (Security Services) > 文件信誉和分析 (File Reputation and Analysis)** 页面上的“文件分析的高级设置”(Advanced Settings for File Analysis) 部分。
网络安全设备	**安全服务> 防恶意软件和信誉**页上的“文件分析高级设置”部分。
思科内容安全管理设备	在**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)** 页面的底部。

相关主题

（云文件分析）配置管理设备以显示详细的文件分析结果 ， 第 104 页

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) 页面是一个安全相关报告页面，可用于监控客户端恶意软件风险活动。

在“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。根据从此页面收集的信息，管理员可以点击用户链接，查看此用户在网络上执行了哪些操作导致受到如此多的阻止或警告，引发比网络上其他用户更多的检测。

此外，“客户端恶意软件风险”页面还列出了常见恶意软件连接涉及的客户端 IP 地址，如第 4 层流量监控器 (L4TM) 所标识。经常连接到恶意站点的计算机可能感染了尝试连接到中央命令和控制服务器的恶意软件，应进行杀毒。

下表介绍有关“客户端恶意软件风险”页的信息。

表 *27:* 客户端恶意软件风险报告组件

部分	说明
时间范围 (Time Range)（下拉列表）	该菜单允许您选择报告中所包含数据的时间范围。有关详细信息，请参阅选择报告的时间范围 ， 第 22 页。
网络代理：排名靠前的受监控或阻止的客户端 (Web Proxy: Top Clients Monitored or Blocked)	此图表显示遇到恶意软件风险的排名前十的用户。

部分	说明
第 4 层流量监控器：检测到的恶意软件连接 (L4 Traffic Monitor: Malware Connections Detected)	此图表显示您的组织中最常连接到恶意站点的排名前十的计算机的 IP 地址。 此图表与L4 流量监控器报告 ，第 111 页上的“排名靠前的客户端 IP”图表相同。有关图表选项的更多信息，请参阅上述提及的部分。
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”(Client Malware Risk) 表显示在“网络代理：按恶意软件风险排名靠前的客户端”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。有关该页的信息，请参阅用户详细信息（Web 报告） ，第 95 页。 点击该表中的任意链接，您可以更为精细地查看各个用户以及他们正在执行的哪些活动触发了恶意软件风险的详细信息。例如，点击“用户 ID/客户端 IP 地址”(User ID / Client IP Address) 列中的链接会将您带到该用户的“用户”(User) 页。
第 4 层流量监控器：按恶意软件风险排名的客户端 (L4 Traffic Monitor: Clients by Malware Risk)	此表显示您的组织中最常连接到恶意站点的计算机的 IP 地址。 该表与L4 流量监控器报告 ，第 111 页上的“客户端源 IP”(Client Source IPs) 表相同。有关使用此表用的信息，请参阅此部分。

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 88 页。

网络信誉过滤器报告

网络 > 报告 > 网络信誉过滤器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？

网络信誉过滤用于分析网络服务器行为并为 URL 分配一个信誉得分，从而确定其包含基于 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。您可以使用同时具有访问和解密策略的网络信誉过滤。

网络信誉过滤器使用统计数据评估互联网域可靠性并对URL信誉进行评分。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，或网站的托管位置，或者网络服务器是否使用动态IP地址等。

网络信誉计算将URL与网络参数相关联，用于确定恶意软件存在的可能性。然后得出的恶意软件存在的综合可能性会映射为一个 -10 到 +10 之间的网络信誉分数，+10 为最不可能包含恶意软件。

示例参数包括：

- URL 类别数据
- 存在的可下载代码
- 存在的冗长且含混的最终用户许可协议 (EULA)
- 全局量和量的变化
- 网络所有者信息
- URL 的历史记录
- URL 的时长
- 是否存在于任何阻止列表上
- 是否存在于任何允许列表上
- 常用域的 URL 拼写错误
- 域注册商信息
- IP 地址信息

有关 Web 信誉过滤的详细信息，请参阅《网络 IronPort AsyncOS 用户指南》中的“Web 信誉过滤器”。

在 **Web 信誉过滤器**页面中，您可以查看以下信息：

表 *28:*“*Web* 报告 *Web* 信誉过滤器”页面上的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围 ，第 22 页。
网络信誉操作（趋势）(Web Reputation Actions [Trend])	本部分以图的形式显示在指定的时间（水平）内网络信誉操作总数（垂直）。在这里，您可以看到随着时间推移网络信誉操作的潜在趋势。
网络信誉操作（容量）(Web Reputation Actions [Volume])	本部分按事务显示网络信誉操作量（以百分比表示）。
已由 WBRS 阻止的网络信誉威胁类型 (Web Reputation Threat Types Blocked by WBRS)	本部分显示事务中发现的已由网络信誉过滤阻止的威胁类型。 注：WBRS 不能始终识别出威胁类型。
在其他事务中检测到的威胁类型 (Threat Types Detected in Other Transactions)	本部分显示事务中发现的未由网络信誉过滤阻止的威胁类型。 这些威胁未被阻止的可能原因包括： • 并非所有威胁的得分均达到阻止阈值。但是，设备的其他功能可以捕获这些威胁。 • 可策略以允许配置威胁通过。 注：WBRS 不能始终识别出威胁类型。
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 88 页。

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

基于您的报告结果，您可能希望调整已配置的网络信誉设置，例如调整阈值得分，或启用或禁用 Adaptive Scanning。有关配置 Web 信誉设置的具体信息，请参阅《思科网络安全设备 AsyncOS 用户指南》。

L4 流量监控器报告

网络 > 报告 > L4 流量监控器页面会显示有关上网络安全设备的 L4 流量监控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 88 页。

表 *29: L4* 流量监控器报告页组件

部分	说明
时间范围 (Time Range) 下拉列表	该菜单允许您选择要报告的时间范围。有关详细信息，请参阅选择报告的时间范围 ，第 22 页。
“排名靠前的客户端 IP”(Top Client IPs)	本部分以图的形式显示您的组织中最常连接到恶意站点的计算机的 IP 地址。 点击图表下面的“图表选项”(Chart Options) 链接可以将显示从“检测到的恶意软件连接”(Malware Connections Detected) 总数更改为“监控到的恶意软件连接”(Malware Connections Monitored) 或“已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 108 页上的“第 4 层流量监控器检测到的恶意连接”图表相同。

部分	说明
恶意软件最多的网站 (Top Malware Sites)	本部分以图的形式显示第 4 层流量监控器检测的排名靠前的恶意软件域名。 点击图表下面的“图表选项”(Chart Options) 链接可以将显示从“检测到的恶意软件连接”(Malware Connections Detected) 总数更改为“监控到的恶意软件连接”(Malware Connections Monitored) 或“已阻止的恶意软件连接”(Malware Connections Blocked)。
客户端源 IP (Client Source IPs)	本表显示您的组织中经常连接到恶意站点的计算机的 IP 地址。 要仅包括特定端口的数据，请在表底部的框中输入端口号，并点击“按端口过滤”(Filter by Port)。您可以使用此功能帮助确定那些将恶意软件站点“称为家”的恶意软件使用哪些端口。 要查看诸如每个连接的端口和目标域的详细信息，请点击表中的条目。例如，如果特定客户端 IP 地址具有大量已受阻止的恶意软件连接，请点击该列中的数字，查看每个受阻止连接的列表。该列表显示为“网络”(Web) >“报告”(Reporting) >“网络跟踪”(Web Tracking) 页面中“第 4 层流量监控器”(L4 Traffic Monitor) 选项卡中的搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监控器处理的事务 ，第 126 页。 该表与客户端恶意软件风险报告 ，第 108 页上的“第 4 层流量监控器 - 按恶意软件风险排名的客户端”表相同。
恶意软件端口 (Malware Ports)	此表显示第 4 层流量监控器最常检测到恶意软件的端口。 要查看详细信息，请点击表中的某个条目。例如，点击“检测到的恶意软件连接总数”(Total Malware Connections Detected) 可以查看该端口上每个连接的详细信息。该列表显示为“网络”(Web) >“报告”(Reporting) >“网络跟踪”(Web Tracking) 页面中“第 4 层流量监控器”(L4 Traffic Monitor) 选项卡中的搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监控器处理的事务 ，第 126 页。
检测到的恶意软件站点数 (Malware Sites Detected)	此表显示第 4 层流量监控器最常检测到恶意软件的域。 要仅包括特定端口的数据，请在表底部的框中输入端口号，并点击“按端口过滤”(Filter by Port)。您可以使用此功能帮助确定是否阻止某个站点或端口。 要查看详细信息，请点击表中的某个条目。例如，点击“受阻止的恶意软件连接”(Malware Connections Blocked) 的数字可以查看特定站点的每个已阻止连接的列表。该列表显示为“网络”(Web) >“报告”(Reporting) >“网络跟踪”(Web Tracking) 页面中“第 4 层流量监控器”(L4 Traffic Monitor) 选项卡中的搜索结果。有关此列表的详细信息，请参阅搜索 L4 流量监控器处理的事务 ，第 126 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 88 页。

相关主题

- 解决第 4 层流量监控器报告问题 ， 第 131 页

SOCKS 代理报告

网络 > 报告 > SOCKS 代理页允许您查看那些通过 SOCKS 代理处理的事务的数据和趋势，包括目标和用户的信息。

注释 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，请参阅思科网络安全设备 AsyncOS 用户指南。

相关主题

- 搜索 SOCKS 代理处理的事务 ， 第 127 页

按用户地点分类的报告

网络 > 报告 > 按用户地点分类的报告页面允许您查看您的移动用户正在其本地或远程系统上执行哪些活动。

具体活动包括：

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

从**按用户位置报告**页面，可查看下列信息：

表 *30:*“按用户位置 *Web* 报告”页面的详细信息

部分	说明
时间范围 (Time Range) 下拉列表	范围既可以介于 1 至 90 天之间也可以是自定义范围的下拉列表。有关时间范围以及自定义时间范围以满足自己需求的详细信息，请参阅选择报告的时间范围 ， 第 22 页。
网络代理活动总数：远程用户 (Total Web Proxy Activity: Remote Users)	本部分以图的形式显示在指定时间内（水平）您的远程用户的活动（垂直）。
网络代理摘要 (Web Proxy Summary)	本部分显示您的系统上的本地和远程用户的活动的摘要。

部分	说明
网络代理活动总数：本地用户 (Total Web Proxy Activity: Local Users)	本部分以图的形式显示在指定时间内（水平）您的远程用户的活动（垂直）。
检测到的可疑事务数：远程用户 (Suspect Transactions Detected: Remote Users)	本部分以图的形式显示在指定的时间内（水平）由于为您的本地用户定义的访问策略而检测到的可疑事务（垂直）。
可疑事务摘要 (Suspect Transactions Summary)	本部分显示您的系统上的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)	本部分以图的形式显示在指定的时间内（水平）由于为您的本地用户定义的访问策略而检测到的可疑事务（垂直）。
可疑事务摘要 (Suspect Transactions Summary)	本部分显示您的系统上的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。这允许您方便地比较您的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 88 页。

注释 您可以为“按用户位置报告”(Reports by User Location) 页面上的信息生成一个已安排报告。有关安排报告的信息，请参阅关于计划的报告和按需 Web 报告，第 116 页。

系统容量页面

通过**网络 > 报告 > 系统容量**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，您可以使用“系统容量”(System Capacity) 页面来跟踪随着时间的发展情况并针对系统容量进行规划。监控您的网络安全设备确保容量适合您的用量。邮件量将随着时间不可避免地增加；适当的监控可确保主动应用额外的容量或配置更改。

“系统容量”(System Capacity) 页面可用于确定以下信息：

- 发现网络安全设备何时超出了建议的 CPU 容量；这使得您可以确定何时需要配置优化或其他设备。
- 要进行故障排除，需确定系统的哪些部分使用大多数资源。
- 识别响应时间和代理缓冲内存。
- 识别每秒的事务数和未完成的任意连接。

查看系统容量报告

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。页面上的图会划分为两个部分：

- 系统容量 - 系统负载 ， 第 115 页
- 系统容量 - 网络负载 ， 第 115 页

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

当选择时间范围来查看“系统容量”(System Capacity) 页面上的数据时，记住以下内容非常重要：

- 日报告 (Day Report) - 日报告查询小时表并显示设备在 24 小时内每小时收到的准确查询数量。此信息收集自小时表。
- 月报告 - 月报告查询 30 或 31 天（取决于该月份的实际天数）的日表，为您提供 30 或 31 天内查询数量的确切报告。再次重申，这是一个精确的数字。

“系统容量”(System Capacity) 页面上的“最大值”(Maximum) 值指示符是在指定时间段内看到的最高值。“平均值”(Average) 值是指定时间段内所有值的平均值。汇聚的时间取决于为该报告选择的时间间隔。例如，如果图表表示某个月时间段，您可以选择查看每天的“平均值”(Average) 和“最大值”(Maximum) 值。

注释 如果为其他报告的时间范围选择**是 (Yes)**，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) 窗口的前四个图形显示系统负载报告。这些报告显示设备上的整体 CPU 使用情况。AsyncOS 优化为使用空闲 CPU 资源提高事务吞吐量。高 CPU 使用率可能不是表明系统容量问题。如果高CPU使用率与一致的大容量内存页面交换相结合，则可能会发生容量问题。该页面还显示一个图，其中显示了不同功能使用的CPU量，包括网络安全设备报告的处理。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，则此图形可以帮助确定哪些功能可能需要调整或禁用。

此外，“响应时间/延迟”(Response Time/Latency) 和“每秒事务数”(Transactions Per Second) 图显示“时间范围”(Time Range) 下拉菜单中指定的日期范围内的整体响应时间（毫秒）以及每秒事务数。

系统容量 - 网络负载

“系统容量”(System Capacity) 窗口的下个图显示传出连接、使用的带宽和代理缓冲区内存统计信息。您可以查看一天、一周、一月或一年的结果。了解环境中的正常量和激增量的趋势很重要。

代理缓冲区内存可能会指示正常操作期间的网络流量的激增，但是如果图形稳定地攀爬至最大值，则设备可能达到其最大容量，则您就考虑增加容量。

下面这些图表与系统容量 - 系统负载 ， 第 115 页中介绍的图表相同。

有关代理缓冲内存交换的说明

系统设计为定期交换代理缓冲区内存，因此，某些代理缓冲区内存交换是在预期中，并不表示您的设备存在问题。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 > 报告 > 数据可用性页面提供有关每个受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。

注释 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 ， 第 320 页。

注释 如果在计划报告内为 URL 类别使用“数据可用性”(Data Availability)，并且在任意设备之间存在着数据差异，则会在页面底部显示以下信息：“Some data in this time range was unavailable”。如果没有数据差异，则不会显示任何内容。

关于计划的报告和按需 Web 报告

除非另有说明，否则您可以将以下网络安全报告生成为已安排报告或按需报告：

- “Web 报告概述”(Web Reporting Overview) - 要了解此页面上所包括内容的相关信息，请参阅Web 报告概述 ， 第 92 页。
- “用户”(Users) - 要了解此页面上所包括内容的相关信息，请参阅用户报告 (Web) ， 第 93 页。
- “网站”(Web Sites) - 要了解此页面上所包括内容的相关信息，请参阅网站报告 ， 第 96 页。
- “URL 类别”(URL Categories) - 要了解此页面上所包括内容的相关信息，请参阅URL 类别报告 ， 第 97 页。
- “排名靠前的 URL 类别 - 扩展”(Top URL Categories - Extended)：有关如何为“排名靠前的 URL 类别 - 扩展”(Top URL Categories - Extended) 生成报告的信息，请参阅URL 类别排行榜 - 扩展 ， 第 119 页。

此报告不可作为按需报告。

- “应用可视性”(Application Visibility) - 要了解此页面上所包括内容的相关信息，请参阅应用可视性报告 ， 第 99 页。

- “排名靠前的应用类型 - 扩展”(Top Application Types - Extended)：有关如何为“排名靠前的应用类型 - 扩展”(Top Application Types - Extended) 生成报告的信息，请参阅排名靠前的应用类型 - 扩展 ， 第 120 页。

此报告不可作为按需报告。

- “防恶意软件”(Anti-Malware) - 要了解此页面上所包括内容的相关信息，请参阅防恶意软件报告 ， 第 101 页。
- “客户端恶意软件风险”(Client Malware Risk) - 要了解此页面上所包括内容的相关信息，请参阅客户端恶意软件风险报告 ， 第 108 页。
- “网络信誉过滤”(Web Reputation Filters) - 要了解此页面上所包括内容的相关信息，请参阅网络信誉过滤器报告 ， 第 109 页。
- “第 4 层流量监控器”(L4 Traffic Monitor) - 要了解此页面上所包括内容的相关信息，请参阅L4 流量监控器报告 ， 第 111 页。
- “移动解决方案”(Mobile Secure Solution) - 要了解此页面上所包括内容的相关信息，请参阅按用户地点分类的报告 ， 第 113 页。
- “系统容量”(System Capacity) - 要了解此页面上所包括内容的相关信息，请参阅系统容量页面 ， 第 114 页。

计划 Web 报告

本节包括以下主题：

注释 您可以选择让用户名在所有报告中无法识别。有关信息，请参阅在 Web 报告中使用匿名 ， 第 88 页。

您可以安排报告每日、每周或每月运行。已安排报告可以配置为包括前一天、前七天、上个日历日（最多 250 天）以及上个日历月（最多 12 个月）的数据。或者，您可以包括自定义天数（从 2 天到 100 天）或自定义月数（从 2 个月到 12 个月）的数据。

无论您何时运行报告，均会从上一个时间时间间隔（小时、天、星期或月）返回数据。例如，如果您计划在凌晨 1 点运行每日报告，则该报告将包含前一天从午夜到午夜（00:00 到 23:59）的数据。

您可以为报告定义所需数量的收件人，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，如果您需要将报告发送到大量地址，则可能需要创建邮件列表，而不是逐个列出收件人。

计划的 Web 报告的存储

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。在添加新的报告时，系统会删除较旧的报告以将数量保持在1000个。最多可将 30 个实例应用到具有相同名称和时间范围的各个计划报告。

已存档的报告存储在设备上的 /periodic_reports 目录。（有关详细信息，请参阅IP 接口和访问设备，第 373 页。）

相关主题

- 查看和管理存档的 Web 报告，第 122 页

添加已安排的 Web 报告

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，选择您的报告类型。

步骤 4 在**标题 (Title)** 字段中，键入报告的标题。

为了避免创建多个使用相同名称的报告，我们建议使用说明性的标题。

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。大多数报告还允许您将原始数据另存为 CSV 文件。

步骤 7 在**项目数 (Number of Items)** 旁边的下拉列表中，选择您要包括在已生成报告中的项目数。

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 在**对列排序 (Sort Column)** 旁边的下拉列表中，选择对此报告的数据进行排序的列。这允许您按已安排报告中任意可用的列生成一个具有前“N”项的已安排报告。

步骤 10 从**计划 (Schedule)** 区域中，为计划的报告选中天、周或月旁边的单选按钮。

步骤 11 在**邮件 (Email)** 文本字段中，输入生成的报告将发送到的邮件地址。

如果不指定邮件地址，则仅存档该报告。

步骤 12 点击**提交**。

编辑计划的 Web 报告

要编辑报告，请转到**网络 > 报告 > 计划的报告**，并选中您要编辑报告的相应复选框。修改设置，然后点击**提交**以提交在页面上进行的更改，然后点击**确认更改**按钮以确认对设备进行的更改。

删除已安排的 Web 报告

要删除报告，请转到**网络 > 报告 > 计划的报告**，并选中您要编辑报告的相应复选框。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。注意已删除报告的存档版本不会被删除。

更多扩展的 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：

- URL 类别排行榜 - 扩展 ， 第 119 页
- 排名靠前的应用类型 - 扩展 ， 第 120 页

URL 类别排行榜 - 扩展

对于希望接收到的信息比 URL 类别报告中的信息更详细的管理员来说，“排名靠前的 URL 类别 - 扩展”(Top URL Categories - Extended) 报告非常有用。

例如，在典型的 URL 类别报告中，您可以在较大的 URL 类别级别按特定员工收集评估带宽使用量的信息。要生成更为详细的报告，用于为每个 URL 类别监控前十个 URL 的带宽使用量，或者为每个 URL 类别监控前五位用户的带宽使用量，请使用“排名靠前的 URL 类别 - 扩展”(Top URL Categories - Extended) 报告。

注释 使用此报告类型可以生成的最大报告数为 20。

- 预定义的URL类别列表会偶尔更新。有关对报告结果进行上述更新的影响的详细信息，请参阅 URL 类别集更新和报告 ， 第 98 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：

步骤 1 在安全管理设备上，选择**网络 > 报告 > 计划的报告**。

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

步骤 3 在“类型”旁边的下拉菜单中，选择**URL 类别排行榜 - 扩展**。

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 (Number of Items)** 旁边的下拉列表中，选择要包括在已生成报告中的 URL 类别数。

有效值为 2 到 20。默认值为 5。

步骤 8 在**对列排序 (Sort Column)** 旁边的下拉列表中，选择对此报告的数据进行排序的列。这允许您按已安排报告中任意可用的列生成一个具有前“N”项的已安排报告。

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**计划 (Schedule)** 区域中，为计划的报告选中天、周或月旁边的单选按钮。

步骤 11 在**邮件 (Email)** 文本字段中，输入生成的报告将发送到的邮件地址。

步骤 12 点击**提交**。

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：

步骤 1 在安全管理设备上，选择**网络 > 报告 > 计划的报告**。

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 Type—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 (Number of Items)** 旁边的下拉列表中，选择您要包括在已生成报告中的应用类型数。

有效值为 2 到 20。默认值为 **5**。

步骤 8 在**对列排序 (Sort Column)** 旁边的下拉列表中，选择要显示在表中的列类型。选项包括：“已完成事务”(Transactions Completed)、“已阻止事务”(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**计划 (Schedule)** 区域中，为计划的报告选中天、周或月旁边的单选按钮。

步骤 11 在**邮件 (Email)** 文本字段中，输入生成的报告将发送到的邮件地址。

步骤 12 点击**提交**。

按需生成 Web 报告

您可以安排大多数报告，并且还可以按需生成报告。

注释 某些报告仅以“已安排报告”(Scheduled Reports) 的形式而不是按需报告的形式存在。请参阅更多扩展的 Web 报告，第 119 页。

要按需生成报告，请执行以下操作：

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变化

步骤 4 在“标题”(Title) 文本字段中，键入报告标题的名称。

AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建多个名称相同的报告。

步骤 5 从**要包括的时间范围**下拉列表中，为报告数据选择一个时间范围。

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。您可以通过点击“预览 PDF 报告”(Preview PDF Report) 立即以 PDF 文件形式查看报告。
- CSV。创建以逗号分隔值格式包含原始数据的 ASCII 文本文件。每个 CSV 文件最多可以包含 100 行。如果报告包含多个类型的表，则会为每个表创建单独的 CSV 文件。

步骤 7 根据报告可用的选项，请选择：

- **行数 (Number of rows)**：显示在表中的数据行数。
- **图表 (Charts)**：哪些数据显示在报告的图表中：
- 点击“要显示的数据”(Data to display) 下的默认选项。
- **对列排序 (Sort Column)**：对每个表进行排序所依据的列。

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

- 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。

注释 无法对“基于域的执行摘要”(Domain-Based Executive Summary) 报告进行存档。

- 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，请输入报告的收件人邮件地址。

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

“存档的 Web 报告”页面

- 关于计划的报告和按需 Web 报告， 第 116 页
- 按需生成 Web 报告 ， 第 120 页
- 查看和管理存档的 Web 报告， 第 122 页

查看和管理存档的 Web 报告

使用本部分的信息可以处理生成为已安排报告的报告。

步骤 1 转到**网络 > 报告 > 存档的报告**。

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。

下一步做什么

相关主题

- 计划的 Web 报告的存储 ， 第 118 页
- 添加已安排的 Web 报告， 第 118 页
- 按需生成 Web 报告 ， 第 120 页

Web 跟踪

使用“网络跟踪”(Web Tracking) 页面可以搜索和查看关于各个事务的详细信息，或者搜索和查看您关心的事务的模式。根据您的部署使用的服务，请在相关选项卡中搜索：

- 搜索网络代理服务处理的事务 ， 第 123 页
- 搜索 L4 流量监控器处理的事务 ， 第 126 页
- 搜索 SOCKS 代理处理的事务 ， 第 127 页
- 处理网络跟踪搜索结果 ， 第 127 页
- 查看网络跟踪搜索结果的事务详细信息 ， 第 128 页

有关网络代理与 L4 流量监控器之间区别的更多信息，请参阅《思科网络安全设备 AsyncOS 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 129 页

搜索网络代理服务处理的事务

使用**网络 (Web) > 报告 (Reporting) > 网络跟踪 (Web Tracking)** 页面上的 **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汇聚的网络跟踪数据。此数据不包括第 4 层流量监控数据或 SOCKS 代理处理的事务。

您可能希望使用它协助以下角色的工作：

- **HR 或法务经理**。在特定时段运行对某位员工的调查报告。

例如，您可以使用“代理服务”(Proxy Services) 选项卡检索用户正在访问的特定 URL、用户访问该 URL 的时间以及该 URL 是否被允许等信息。

- **网络安全管理员**。检查公司网络是否正通过员工的智能手机遭受恶意软件威胁。

您可以查看特定时段内已记录事务（包括已阻止、已监控、已警告和已完成）的搜索结果。您还可以使用多个条件（例如 URL 类别、恶意软件威胁和应用）来过滤数据结果。

注释 网络代理仅报告包括 ACL 决策标记（而非“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 ，第 389 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”页面与其他报告页面结合使用 ，第 98 页。

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 *31:*“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	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 ，第 22 页。
时间范围 (Time Range)	
用户/客户端 IPv4 或 IPv6	当用户名显示在报告中时输入身份验证用户名，或输入您要跟踪的客户端 IP 地址，这是可选操作。您还可以输入 CIDR 格式的 IP 范围，例如 172.16.0.0/16。 当您将此字段留空时，搜索将为所有用户返回结果。
网站 (Website)	输入您要跟踪的网站，这是可选操作。当您将此字段留空时，搜索将为所有网站返回结果。

选项	说明
事务类型	选择您要跟踪的事务类型，可能是“所有事务”(All Transactions)、“已完成事务”(Completed)、“已阻止事务”(Blocked)、“已监控事务”(Monitored) 或“已警告事务”(Warned)。
高级搜索条件	
URL 类别	要按 URL 类别过滤，请选择**按 URL 类别过滤 (Filter by URL Category)**，并键入过滤所依据的自定义或预定义的 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 类别集更新的更多信息，请参阅URL 类别集更新和报告 ，第 98 页。 将包括与类别名称匹配的所有最近事务，无论下拉列表中标明的是哪个引擎名称。
应用	要按应用进行过滤，请选择**按应用过滤 (Filter by Application)** 并选择要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)** 并选择要依据其进行过滤的应用类型。
策略 (Policy)	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)** 并输入要依据其进行过滤的恶意软件威胁名称。 要按恶意软件类别过滤，选择**按恶意软件类别过滤 (Filter by Malware Category)** 并选择按其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 102 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。 • 要按网络信誉得分过滤，请选择**得分范围**，并选择过滤所依据的上限值和下限值。或者，您可以选择**无得分 (No Score)** 来过滤出那些没有得分的网站。 • 要按网络信誉威胁过滤，选择**按信誉威胁过滤 (Filter by Reputation Threat)** 并选择按其过滤的网络信誉威胁。 有关 WBRS 得分的详细信息，请参阅《适用于 Web 的 IronPort AsyncOS 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 (Disable Filter)**。 （在以前的版本中，此选项被标记为“移动用户安全”(Mobile User Security)。）

选项	说明
网络设备 (Web Appliance)	要按特定网络设备过滤，请点击**按网络设备过滤**旁边的单选按钮，并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	要按用户实际发起的事务过滤，请选择**按 Web 用户请求的事务过滤**。 **注：**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**。

下一步做什么

相关主题

- 显示更多网络跟踪搜索结果 ， 第 127 页
- 了解网络跟踪搜索结果 ， 第 128 页
- 查看网络跟踪搜索结果的事务详细信息 ， 第 128 页
- 关于网络跟踪和高级恶意软件防护功能 ， 第 128 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
广告软件	广告软件包含可将用户引导至待售产品的所有软件可执行文件和插件。某些广告软件应用具有并发运行并彼此监控的单独进程，确保修改是永久的。某些变体使得它们自己可以在每次计算机启动时自动运行。这些程序也可能更改安全设置，使得用户无法对其浏览器搜索选项、桌面和其他系统设置进行更改。
浏览器助手对象	浏览器助手对象是一个浏览器插件，可以执行与提供广告或劫持用户设置相关的各种功能。
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	拨号程序是一种程序，利用您的调制解调器或其他类型的互联网访问方式，将您连接到某个电话线路或站点，意图在您并未提供充分、明确且知情许可的情况下套取您的长途电话费用。
常规间谍软件	间谍软件是一种安装在计算机上的恶意软件，旨在未获得用户许可的情况下收集碎片信息。

恶意软件类型	说明
劫持程序	劫持程序修改系统设置或对用户系统进行不希望的更改，从而在用户并未提供充分、明确且知情许可的情况下，将用户引导至一个网站或运行一个程序。
其他恶意软件	其他所有未准确契合其他定义类别之一的恶意软件和可疑行为均会归属此类别。
病毒爆发启发式扫描	此类别表示 Adaptive Scanning 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 显示在浏览器地址栏中。在某些情况下，它涉及域名的使用，与合法域的名称类似。网络钓鱼是一种在线身份窃取形式，会使用社交工程和技术手段窃取个人身份数据和财务账户凭证。
PUA	可能不需要的应用。PUA 是非恶意应用，但可能被视为不想要的应用。
系统监视程序	系统监控程序包含执行以下操作之一的任意软件： 公开地或隐蔽地记录系统进程和/或用户操作。 使这些记录可用于以后检索和审核。
特洛伊木马下载程序 (Trojan Downloader)	特洛伊木马下载程序是一种木马程序，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。这些安装通常会无需用户确认即可发生。此外，不同安装之间，特洛伊木马下载程序的有效载荷可能会不同，因为它是从远程主机/站点获取下载说明。
特洛伊木马	特洛伊木马是一种会伪装成良性应用的破坏性程序。不同于病毒，特洛伊木马不会自我复制。
特洛伊木马钓鱼程序	特洛伊木马钓鱼程序会驻留在受感染的计算机上，等待他人访问特定网页，或者可能会扫描受感染的计算机来查找银行站点、拍卖站点或在线支付站点的用户名和密码。
病毒	病毒是未经您确认就加载到您的计算机上，并且违背您的意愿运行的程序或代码段。
蠕虫	蠕虫是一种程序或算法，会通过计算机网络进行自我复制，通常执行恶意操作。

搜索 L4 流量监控器处理的事务

网络 (Web) > 报告 (Reporting) > 网络跟踪 (Web Tracking) 页面上的“L4 流量监控器”(L4 Traffic Monitor) 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。您可以通过以下信息类型搜索至恶意软件站点的连接：

- 时间范围
- 发起该事务的计算机的 IP 地址（IPv4 或 IPv6）

- 目标网站的域或 IP 地址（IPv4 或 IPv6）
- 端口
- 与组织中的计算机相关联的 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 流量监控器报告 ， 第 111 页。

搜索 SOCKS 代理处理的事务

您可以搜索符合多个条件的事务，包括已阻止事务或已完成事务；发起该事务的客户端计算机的 IP 地址；目标域、IP 地址或端口。您还可以按自定义 URL 类别、匹配的策略以及用户位置（本地或远程）来过滤结果。不支持 IPv4 和 IPv6 地址。

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**搜索 (Search)**。

下一步做什么

相关主题

SOCKS 代理报告 ， 第 113 页

处理网络跟踪搜索结果

显示更多网络跟踪搜索结果

步骤 1 请务必查看所返回结果的全部页面。

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 如果与您的条件匹配的事务数多于“显示的项数”(Items Displayed) 菜单中提供的最大事务数，您可以点击**可打印的下载**链接以获取一个包含所有匹配事务的 CSV 文件，从而可以查看全部结果。

此 CSV 文件包括原始数据的完整集合，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，结果是按时间戳排序，最近的结果显示在顶部。

搜索结果包括：

- 访问 URL 的时间。
- 用户发起的事务所引发的相关事务数，例如，加载的图像、JavaScript 运行和访问的辅助站点等。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) 链接下的每行中。
- 处理（事务的结果。如果适用，显示事务被阻止、被监控或被警告的原因。）

查看网络跟踪搜索结果的事务详细信息

要查看	相应操作
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的列标题中的“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防护功能

当在“网络跟踪”(Web Tracking) 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)**。
- 网络跟踪仅包括文件信誉处理以及在处理事务时返回的初始文件信誉判定的相关信息。例如，如果最初发现文件是干净文件，然后判定更新发现文件是恶意文件，则只有干净的判定显示跟踪结果中。

搜索结果中的“阻止 - AMP”(Block - AMP) 意味着由于文件的信誉判定而阻止该事务。

在跟踪详细信息中，“AMP 威胁得分”是当云信誉服务无法判定某个文件正常时所能提供的最佳得分。在这种情况下，得分介于 1 和 100 之间。（如果返回了 AMP 判定，或者得分为零，请忽略 AMP 威胁得分。）设备会将此得分与阈值得分（在“安全服务”[Security Services] > “防恶意软件和信誉”[Anti-Malware and Reputation] 页面上配置）进行比较，以确定所需采取的操作。默认情况下，得分介于 60 到 100 之间的文件会被视为恶意文件。思科不建议更改默认阈值得分。WBRS 得分是从中下载文件的站点的信誉；此得分与文件信誉无关。

- 判定更新仅在 AMP 判定更新报告中可用。网络跟踪中的初始事务详细信息不会随判定更改而更新。要涉及特定文件的事务，请在判定更新报告中点击 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，请依次选择**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从任意来源分析了该文件，您可以查看该详细信息。系统仅会为已分析的文件的结果。

  如果设备处理了已发送的待分析文件的后续实例，则这些实例将显示在“网络跟踪”(Web Tracking) 搜索结果中。

相关主题

- 通过 SHA-256 散列标识文件 ， 第 106 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发生的事务，因为可能没有为这些事务保留所需的数据。有关与网络跟踪和升级相关的可能限制，请参阅您的版本的发行说明。

解决 Web 报告和跟踪问题

另请参阅对所有报告进行故障排除 ， 第 30 页。

集中报告已正确启用，但不工作

问题

已按照指示启用了集中 Web 报告功能，但这不起作用。

解决方案

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。只要您为 Web 报告和跟踪设置的配额大于当前使用的磁盘空间，您就不会丢失任何 Web 报告和跟踪数据。有关详细信息，请参阅管理磁盘空间 ， 第 320 页。

高级恶意软件保护判定更新报告结果存在差异

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。

解决方案

这种情况是暂时的。下载了所有判定更新后，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。

解决方案

请参阅文件分析报告详细信息的要求 ， 第 104 页。

查看文件分析 (File Analysis) 报告详细信息时出错

问题

当您尝试查看“文件分析”报告详细信息时，出现没有可用的云服务器配置错误。

解决方案

转到**管理设备 > 集中服务 > 安全设备**，然后添加至少一个启用了分析功能的网络安全设备。

使用私有云 Cisco AMP Threat Grid 设备查看文件分析 (File Analysis) 报告详细信息时出错

问题

当您尝试查看“文件分析”(File Analysis) 报告详细信息时，出现 API 密钥、注册或激活错误。

解决方案

如果您使用私有云（本地部署的）Cisco AMP Threat Grid 设备进行文件分析，请参阅（本地文件分析）激活文件分析账户 ，第 105 页。

如果 Threat Grid 设备主机名发生更改，您必须重复执行所引用操作程序中的流程。

在报告或跟踪结果中缺少预期的数据

问题

报告或跟踪结果中缺少预期数据。

解决方案

可能原因：

- 确保您选择了所需的时间范围。
- 对于跟踪结果，请确保您正在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 127 页。
- 网络安全设备和思科内容安全管理设备之间的数据传输可能已被中断，或者数据可能已被清除。请参阅“数据可用性”页面 ，第 116 页。
- 如果升级更改了报告或跟踪信息的方式，则在升级前发生的事务可能不会按预期呈现。要查看您的版本是否具有此类更改，请参阅文档 ，第 393 页中指定的您的版本的发行说明。
- 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 123 页。
- 对于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 123 页中表的“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。

解决方案

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 27 页中相应表格的网络跟踪信息。

解决第 4 层流量监控器报告问题

如果网络代理配置为转发代理，并且第 4 层流量监控器设置为监控所有端口，则代理的数据端口的 IP 地址会记录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的代理，请启用 IP 欺骗以正确地记录和显示客户端 IP 地址。为此，请参阅《IronPort AsyncOS for Web 用户指南》。

相关主题

- 客户端恶意软件风险报告 ，第 108 页
- 搜索 L4 流量监控器处理的事务 ，第 126 页

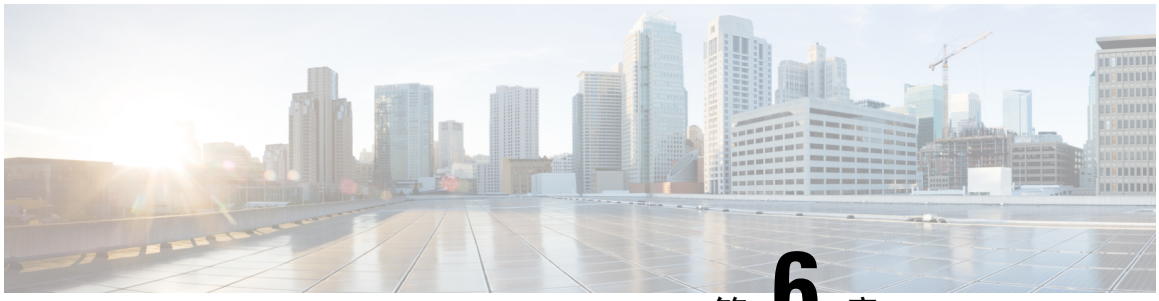
导出的 .CSV 文件与网络界面数据不同

问题

导出到 .csv 文件的“匹配的域”(Domains Matched) 数据与网络界面中显示的数据不同。

解决方案

出于性能原因，系统仅将前 300,000 个条目导出为 .csv。



第 6 章

跟踪邮件

本章包含以下部分：

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。您可以组合使用多种搜索参数。

跟踪查询可以包括：

- **信封信息**：通过输入要匹配的文本字符串，查找来自特定信封发件人或收件人的邮件。
- **主题标题**：与主题行中的文本字符串相匹配。

  警告 请勿在法规禁止此类跟踪的环境中使用此类型的搜索。

- **时间范围**：查找在指定的日期和时间之间发送的邮件。
- **发件人 IP 地址或已拒绝的连接**：搜索来自特定 IP 地址的邮件，或在搜索结果中显示已拒绝的连接。

- **附件名称**：您可以根据附件名称搜索邮件。搜索结果中将显示至少包含一个采用查询名称的附件的邮件。

  出于性能原因，附件（如 OLE 对象）或存档文件（如 .ZIP 文件）内的文件名不会被跟踪。

  有些附件可能无法跟踪。由于性能原因，附件名称扫描仅在其他扫描操作过程中发生，例如邮件或内容过滤、DLP 或免责声明印戳。附件名称仅可用于在附加附件时通过正文扫描的邮件。附件名称将不会出现的一些示例包括（但不限于）：

  - 如果系统仅使用内容过滤器，而且邮件被丢弃，或者其附件被反垃圾邮件或杀毒过滤器删除。
  - 如果邮件拆分策略在进行正文扫描之前从某些邮件中删除附件。

- **事件**：查找与指定的事件相匹配的邮件，例如标记为病毒邮件、垃圾邮件或疑似垃圾邮件的邮件，以及已传送、硬退回、软退回或发送到病毒爆发隔离区的邮件。
- **邮件 ID**：通过标识 SMTP“Message-ID:”信头或 Cisco IronPort 邮件 ID (MID) 来查找邮件。
- **邮件安全设备（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，请按顺序完成下列过程：

- 在安全管理设备上启用集中邮件跟踪，第 134 页
- 在邮件安全设备上配置集中邮件跟踪 ，第 134 页
- 向每台托管邮件安全设备添加集中邮件跟踪服务 ，第 135 页

在安全管理设备上启用集中邮件跟踪

步骤 1 依次选择**管理设备 > 集中服务 > 邮件 > 集中邮件跟踪**。

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

步骤 3 如果在运行“系统设置向导”(System Setup Wizard) 后首次启用集中邮件跟踪，请查阅《最终用户许可证协议》，然后点击**接受**。

步骤 4 **提交**并确认更改。

在邮件安全设备上配置集中邮件跟踪

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**。

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

步骤 5 点击**提交**。

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。

步骤 1 依次选择**管理设备 > 集中服务 > 安全设备**。

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”。

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。

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

c) 预先选择集中邮件跟踪服务。

d) 点击**建立连接 (Establish Connection)**。

e) 在要托管的设备上输入管理员账户的用户名和密码，然后点击**建立连接**。

注释 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 (Test Connection)**。

h) 阅读表格上方的测试结果。

步骤 4 点击**提交**。

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 确认您的更改。

管理对敏感信息的访问权限

如果您要将管理任务分配给其他人，并且要限制他们对违反防数据丢失 (DLP) 策略的邮件中可能出现的敏感信息的访问，请参阅控制对“邮件跟踪”中敏感信息的访问权限 ，第 268 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。

在安全管理设备中，依次择**邮件 > 邮件跟踪 > 邮件跟踪数据可用性**。

上搜索邮件。

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。您还可以详细查看特定的邮件以了解邮件详细信息，例如处理事件、附件名称或信封和标题信息。

注释 虽然跟踪组件提供关于各封邮件的详细信息，但是您无法使用它阅读邮件的内容。

步骤 1 选择**邮件 > 邮件跟踪 > 邮件跟踪**。

步骤 2 （可选）点击“高级”(Advanced) 链接显示更多搜索选项。

步骤 3 输入搜索条件：

注释 跟踪搜索不支持通配符和正则表达式。跟踪搜索不区分大小写。

- 信封发件人 (Envelope Sender)：选择“开头为”(Begins With)、“是”(Is) 或“包含”(Contains)，然后在“信封发件人”(Envelope Sender) 中输入要搜索的文本字符串。您可以输入邮件地址、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]。
  - 您可以输入任何字符。不执行条目验证。
- 信封收件人 (Envelope Recipient)：选择“开头为”(Begins With)、“是”(Is) 或“包含”(Contains)，然后在“信封收件人”(Envelope Recipient) 中输入要搜索的文本字符串。您可以输入邮件地址、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与信封发件人的搜索条件相同。

您可以输入任何字符。不执行条目验证。

- 主题 (Subject)：选择“开头为”(Begins With)、“是”(Is)、“包含”(Contains) 或“为空”(Is Empty)，然后在邮件主题行中输入要搜索的文本字符串。
- 收到邮件 (Message Received)：使用“昨天”(Last Day)、“过去 7 天”(Last 7 Days) 或“自定义范围”(Custom Range) 为查询指定日期和时间范围。使用“昨天”(Last Day) 选项可搜索过去 24 小时内的邮件；使用“过去 7 天”(Last 7 Days) 选项可搜索过去七整天内的邮件（加上当天经过的时间）。

如果不指定日期，则查询会返回所有日期的数据。如果仅指定时间范围，则查询会返回所有可用日期的此时间范围的数据。如果您指定当前日期，并将 23:59 指定为结束日期和时间，查询则返回当前日期的所有数据。

日期和时间存储在数据库时会转换为 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)：输入发件人 IP 地址并选择是要搜索邮件还是仅搜索已拒绝的连接。
  - IPv4 地址必须是用句点隔开的 4 个数字。每个数字的值必须介于 0 和 255 之间。（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 ID 标题和 Cisco IronPort MID (Message ID Header and Cisco IronPort MID)：输入邮件 ID 标题、Cisco IronPort 邮件 ID 或两者的文本字符串。
- 查询设置 (Query Settings)：从下拉菜单中，选择您希望查询在超时之前运行多久。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，请选择您希望查询返回的最大结果数量（最多为 1000 个）。
- 附件名称 (Attachment name)：选择“开头为”(Begins With)、“是”(Is) 或“包含”(Contains)，然后为要查找的一个附件名称输入 ASCII 或 Unicode 文本字符串。前导空格和尾部空格不会从您输入的文本中删除。

有关根据 SHA-256 散列识别文件的详细信息，请参阅通过 SHA-256 散列标识文件 ，第 62 页。

您无需填写每个字段。除“邮件事件”(Message Event) 选项外，该查询是一种“AND”搜索。该查询返回与搜索字段中指定的“AND”条件相匹配的邮件。例如，如果您为信封收件人和主题行参数指定文本字符串，则查询只会返回与指定信封收件人和主题行都匹配的邮件。

步骤 4 点击**搜索 (Search)**。

查询结果出现在页面顶部。每行与一封邮件相对应。

您的搜索条件在每行中突出显示。

如果返回的行数大于“每页项目数”(Items Per Page) 字段中指定的值，则结果显示在多个页面上。要浏览各个页面，请点击列表顶部或底部的页码。

如有必要，请通过输入新的搜索条件细化搜索，然后重新运行查询。或者，您可以通过缩小结果集细化搜索，如以下各部分所述。

下一步做什么

- 缩小结果集，第 138 页

• 关于邮件跟踪和高级恶意软件防护功能 ， 第 138 页
• 了解跟踪查询结果 ， 第 139 页

缩小结果集

在运行查询后，您可能发现结果集包括的信息比您需要的信息更多。请通过在结果列表中点击某行内的值缩小结果集，而不必创建新的查询。点击值会将该参数值添加为搜索中的一个条件。例如，如果查询结果包括来自多个日期的邮件，请点击某行内的某个特定日期以仅显示在该日期收到的邮件。

步骤 1 将光标悬停在要添加为条件的值上方。该值以黄色突出显示。

使用以下参数值细化搜索：

- 日期和时间
- 邮件ID (MID)
- 主机（邮件安全设备）
- 发送方
- 接收方
- 邮件的主题行或主题的起始词语

步骤 2 点击值以细化搜索。

“结果”(Results) 部分显示与原始查询参数和您添加的新条件相匹配的邮件。

步骤 3 如有必要，请在结果中点击其他值以进一步细化搜索。

注释 要删除查询条件，请点击**清除 (Clear)**，然后运行新的跟踪查询。

关于邮件跟踪和高级恶意软件防护功能

在“邮件跟踪”(Message Tracking) 中搜索文件威胁信息时，请记住以下几点：

- 要搜索由文件信誉服务找到的恶意文件，请在“邮件跟踪”(Message Tracking) 的“高级”(Advanced) 部分为“邮件事件”(Message Event) 选项选择**高级恶意软件防护阳性 (Advanced Malware Protection Positive)**。
- “邮件跟踪”(Message Tracking) 仅包括关于文件信誉处理的信息，以及在处理邮件时返回的原始文件信誉判定。例如，如果最初发现文件是干净的，然后判定更新发现文件是恶意的，则在跟踪结果中仅显示干净判定。

  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；
  - 邮件的整体最终高级恶意软件保护判定，以及

- 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。

- 判定更新仅在AMP判定更新报告中可用。系统不会使用判定更改来更新“邮件跟踪”(Message Tracking) 中的原始邮件详细信息。要查看具有特定附件的邮件，请在判定更新报告中点击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。要查看某个文件的任何可用的文件分析信息，请依次选择**监控 (Monitor) > 文件分析 (File Analysis)**，然后输入 SHA-256 搜索该文件。如果文件分析服务已从任意来源分析了该文件，您可以查看该详细信息。系统仅会为已分析的文件的结果。

  如果设备处理了已送交分析的某个文件的后续实例，则这些实例将出现在邮件跟踪搜索结果中。

相关主题

通过 SHA-256 散列标识文件 ， 第 62 页

了解跟踪查询结果

如果结果不符合您的期望，请参阅邮件跟踪故障排除 ， 第 141 页。

跟踪查询结果列出了与跟踪查询中指定的条件相匹配的所有邮件。除“邮件事件”(Message Event) 选项外，查询条件是使用“AND”运算符添加的。结果集内的邮件必须满足所有“AND”条件。例如，如果您指定信封发件人以 J 开头，并且指定主题以 T 开头，则查询仅在这两个条件对于某封邮件而言都成立时才返回该邮件。

要查看关于邮件的详细信息，请点击新 Web 界面中的**显示详细信息**链接。有关详细信息，请参阅邮件详细信息 ， 第 140 页。

注释

- 具有50个或更多收件人的邮件将不会出现在跟踪查询结果中。该问题将在未来的版本中得到解决。
- 您可以使用“搜索结果”部分上面的**导出**链接，将搜索结果导出至 .csv 文件。

  指定查询时，可以选择最多显示 1000 条搜索结果。要查看与您的搜索条件相匹配的多达 50000 封邮件，请在搜索结果部分的上方点击**全部导出 (Export All)** 链接，然后在另一个应用中打开生成的 .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 27 页。

相关主题

邮件详细信息，第 140 页

邮件详细信息

要查看有关特定邮件的详细信息，包括邮件头信息和处理详细信息，请为搜索结果列表中的任一项点击**显示详细信息**。系统将打开一个新窗口，其中显示邮件详细信息。

邮件详细信息包括以下部分：

- 信封和信头概要，第 140 页
- 正在发送主机概要，第 140 页
- 正在处理详细信息，第 140 页

信封和信头概要

此部分显示来自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：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：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 标题 (Message ID Header)：唯一地标识每封邮件的“Message-ID:”标题。首次创建邮件时，系统会将其插入邮件中。当您搜索特定邮件时，“Message-ID:”标题可能会非常有用。

思科主机：处理邮件的邮件安全设备。

经过 SMTP 身份验证的用户 ID：经过 SMTP 身份验证的发件人用户名（如果发件人使用了 SMTP 身份验证来发送邮件）。否则，该值为“N/A”。

附件 (Attachments)：附加到邮件的文件的名称。

正在发送主机概要

反向 DNS 主机名：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：（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。

正在处理详细信息

此部分在处理邮件期间显示各种已记录的状态事件。

条目包括有关邮件策略处理的信息，例如反垃圾邮件和防病毒扫描，以及其他事件（例如邮件拆分）。

如果传送了邮件，则传送详细信息显示在此处。例如，邮件可能已传送，但副本保留在隔离区。

最后记录的事件会在处理详细信息中高亮显示。

与 DLP 匹配的内容 (DLP Matched Content) 选项卡

此选项卡显示违反防数据丢失 (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。请参阅控制对“邮件跟踪”中敏感信息的访问权限 ，第 268 页。

URL 详细信息选项卡

此选项卡仅向由 URL 信誉和 URL 类别内容过滤器以及病毒爆发过滤器（而非邮件过滤器）捕获的邮件显示。

此选项卡显示以下信息：

- 与 URL 关联的信誉得分或类别
- 对 URL 执行的操作（重写、去除或重定向）
- 如果邮件包含多个 URL，显示哪一个 URL 触发了过滤器操作。

仅当您将邮件安全设备配置为显示此信息时，您才可以看到此选项卡。请参阅《思科邮件安全设备 *AsyncOS* 用户指南》。

若要控制对此选项卡的访问，请参阅控制对“邮件跟踪”中敏感信息的访问权限 ，第 268 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 136 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 81 页。

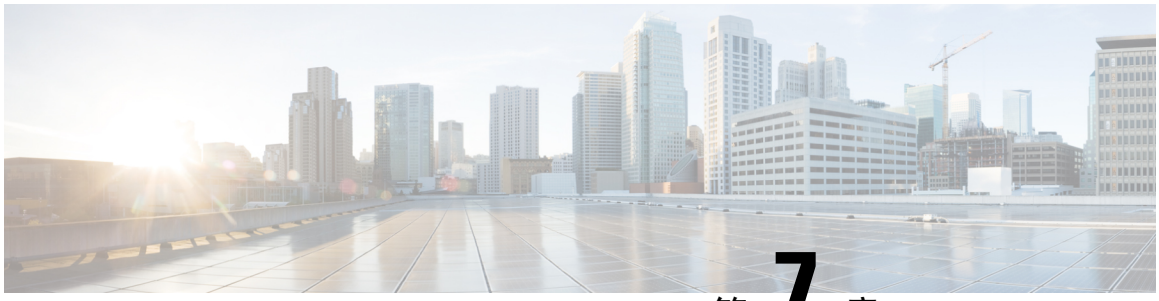
搜索结果中不显示的附件

问题

搜索结果中找不到且未显示附件名称。

解决方案

在 ESA 上配置和启用至少一个入站内容过滤器或其他正文扫描功能。请参阅在安全管理设备上启用集中邮件跟踪，第 134 页所列的配置要求和跟踪服务概述，第 133 页中对附件名称搜索的限制。



第 7 章

垃圾邮件隔离区

本章包含以下部分：

垃圾邮件隔离区概述

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

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（通常是邮件收件人）可在略微不同的 Web 界面中查看各自的隔离邮件。

垃圾邮件隔离区与策略、病毒和爆发隔离区分隔。

相关主题

- 集中策略、病毒和病毒爆发隔离区， 第 167 页

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。

设置集中垃圾邮件隔离区

过程

	命令或操作	目的
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 144 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垃圾邮件隔离区服务 ，第 146 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 ，第 147 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 ，第 147 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。	有关配置反垃圾邮件和邮件策略的详细信息，请参阅《邮件安全设备 *AysncOS* 用户指南》中的“反垃圾邮件”部分。
步骤 6	在邮件安全设备中，启用和配置外部垃圾邮件隔离区。	有关详细信息，请参阅《思科邮件安全设备 *AsyncOS* 用户指南》。
步骤 7	在邮件安全设备上，禁用本地隔离区。	有关禁用本地垃圾邮件隔离区以激活外部垃圾邮件隔离区的信息，请参阅《邮件安全设备 *AysncOS* 用户指南》。

启用和配置垃圾邮件隔离区

注释 如果使用外部垃圾邮件隔离区，将在安全管理设备上配置此部分介绍的设置。

步骤 1 依次选择**管理设备 > 集中服务 > 垃圾邮件隔离区**。

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**。

b) 查看最终用户许可协议，然后点击**接受**。

步骤 3 如果要编辑垃圾邮件隔离区设置，请点击**编辑设置** 。

步骤 4 指定选项：

选项	说明
隔离区 IP 接口 (Quarantine IP Interface) 隔离区端口 (Quarantine Port)	默认情况下，垃圾邮件隔离区使用管理接口和端口 6025。IP 接口是指安全管理设备上配置为监听传入邮件的接口。隔离区端口是指发送设备在其外部隔离区设置中使用的端口号。 如果您的邮件安全设备与安全管理设备不在同一个网络上，则必须使用管理接口。
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，以了解有关这些地址的其他警告。
隔离区大小	如果取消选择**当存储空间已满时，首先自动删除时间最长的邮件 (When storage space is full, automatically delete oldest messages first)**，将不会向已满的隔离区添加更新的邮件。思科建议启用此选项，以便已满的隔离区不会导致邮件在设备上排队（备份）。 要管理隔离区的磁盘空间，请参阅管理磁盘空间 ，第 320 页。
计划删除前的保留天数 (Schedule Delete After)	指定在删除邮件之前将其保留的天数。 思科建议将隔离区配置为删除时间最长的邮件，以防隔离区容量被填满，但可以选择不设定自动删除。
放行邮件时通知思科 (Notify Cisco Upon Message Release)	-
垃圾邮件隔离区外观 (Spam Quarantine Appearance)	**徽标 (Logo)** 默认情况下，当用户登录查看隔离邮件时，思科徽标会显示在垃圾邮件隔离区页面的顶部。 要改用自定义徽标，请上传该徽标。徽标应为 .jpg、.gif 或 .png 文件，最大尺寸为 50 像素（高）× 500 像素（宽）。
	登录页面消息 (Login page message) （可选）指定登录页面消息。当最终用户和管理员登录查看隔离区时，将会向其显示此消息。 如果不指定消息，则显示以下消息： 在下面输入登录信息。如果不确定要输入的内容，请与管理员联系。

选项	说明
管理用户 (Administrative Users)	请参阅配置对垃圾邮件隔离区的管理用户访问权限 ，第 148 页。

步骤 5 提交并确认更改。

下一步做什么

- 退回至 设置集中垃圾邮件隔离区 ，第 144 页

向每个托管邮件安全设备添加集中垃圾邮件隔离区服务

执行的步骤取决于是否已在配置其他集中管理功能时添加了设备。

步骤 1 选择**管理设备 > 集中化服务 > 安全设备**。

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**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”。

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

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

c) 已预先选择垃圾邮件隔离区服务。

d) 点击**建立连接 (Establish Connection)**。

e) 在要托管的设备上输入管理员账户的用户名和密码，然后点击**建立连接**。

注释 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 (Test Connection)**。

h) 阅读表上的测试结果。

步骤 4 点击**提交**。

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 确认您的更改。

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。

开始之前

获取或识别用于出站接口的 IP 地址。出站接口通常是安全管理设备上的 Data 2 接口。有关网络要求的详细信息，请参阅 分配网络和 IP 地址，第 381 页

步骤 1 请将此过程与信息结合使用 配置 IP 接口，第 374 页

步骤 2 在安全管理设备上，择**管理设备 > 网络 IP 接口**。

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 (Ethernet Port)

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

  您刚指定的接口的 IP 地址。
- 网络掩码 (Netmask)
- Hostname

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

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

步骤 5 提交并确认更改。

配置浏览器访问垃圾邮件隔离区的 IP 接口

当管理员和最终用户访问垃圾邮件隔离区时，将打开独立的浏览器窗口。

步骤 1 依次选择**管理设备 > 网络 > IP 接口**。

步骤 2 点击**管理**接口的名称。

步骤 3 在“垃圾邮件隔离区”(Spam Quarantine) 部分中，配置对垃圾邮件隔离区的访问设置：

- 默认情况下，HTTP 使用端口 82，HTTPS 使用端口 83。
- 指定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。

下一步做什么

确保 DNS 服务器可以解析为访问垃圾邮件隔离区指定的主机名。

配置对垃圾邮件隔离区的管理用户访问权限

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

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

- 邮件管理员 (Email administrator)
- 操作员 (Operator)
- 只读操作员 (Read-only operator)
- 服务中心用户 (Help desk user)
- 访客 (Guest)
- 具有垃圾邮件隔离区权限的“自定义用户”(Custom user) 角色

这些用户无法访问垃圾邮件隔离区设置。

开始之前

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，请参阅分配管理任务，第 245 页中关于自定义用户角色的隔离区访问权限 ，第 251 页的信息

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) 选择**管理设备 > 集中服务 > 垃圾邮件隔离区**。

b) 点击“垃圾邮件隔离区”部分的“隔离区名称”列中的**编辑设置 垃圾邮件隔离区**链接。

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。

如果您已添加用户或角色，请点击用户名或角色以查看所有合格的用户或角色。

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**。

步骤 5 提交并确认更改。

下一步做什么

相关主题

配置终端用户访问垃圾邮件隔离区的权限 ， 第 159 页

限制邮件被隔离的收件人

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

垃圾邮件隔离区语言

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

编辑垃圾邮件隔离区页面

- 启用和配置垃圾邮件隔离区 ， 第 144 页
- 本地与外部垃圾邮件隔离区 ， 第 143 页
- 配置终端用户访问垃圾邮件隔离区的权限 ， 第 159 页
- 通知终端用户被隔离的邮件 ， 第 160 页

使用安全列表和阻止列表基于发件人控制邮件发送

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

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

终端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 ， 第 150 页
- 启用安全列表和阻止列表 ， 第 150 页
- 外部垃圾邮件隔离区和安全列表/阻止列表 ， 第 151 页
- 向安全列表和阻止列表中添加发件人和域（管理员） ， 第 151 页
- 关于最终用户访问安全列表和阻止列表 ， 第 153 页
- 备份和恢复安全列表/阻止列表 ， 第 154 页

• 安全列表和阻止列表故障排除 ， 第 155 页

安全列表和阻止列表的邮件处理

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

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

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

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

相关主题

- 启用安全列表和阻止列表 ， 第 150 页
- 外部垃圾邮件隔离区和安全列表/阻止列表 ， 第 151 页

启用安全列表和阻止列表

开始之前

- 必须启用垃圾邮件隔离区。请参阅设置集中垃圾邮件隔离区 ， 第 144 页。

步骤 1 依次选择**管理设备 > 集中服务 > 垃圾邮件隔离区**。

步骤 2 在**终端用户安全列表/阻止列表（垃圾邮件隔离区）(End-User Safelist/Blocklist (Spam Quarantine))** 部分，选择**启用**。

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

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

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

步骤 5 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。

您还可以查看是否许多收件人（组织中的最终用户）已将特定发件人或域列入白名单或黑名单。

管理员可以查看并处理每个最终用户查看并处理的相同条目的超集。

开始之前

- 请确保您可以访问垃圾邮件隔离区。请参阅访问垃圾邮件隔离区（管理用户），第 164 页。
- 启用对安全列表/阻止列表的访问。请参阅启用安全列表和阻止列表，第 150 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 154 页中所述的过程。
- 了解安全列表和阻止列表条目的所需格式。请参阅安全列表和阻止列表条目的语法，第152页。

步骤 1 使用您的浏览器访问垃圾邮件隔离区。

步骤 2 登录。

步骤 3 选择页面右上角的**选项 (Options)** 下拉菜单。

步骤 4 依次选择**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	相应操作
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)**，或者针对收件人点击**编辑 (Edit)**。 3. 输入或编辑收件人邮件地址。 4. 输入发件人邮件地址和域。 将每个条目放在单独的行上或用逗号分隔每个条目。 5. 点击**提交**。
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)**，或者针对发件人点击**编辑 (Edit)**。 3. 输入或编辑发件人地址或域。 4. 输入接收人邮件地址。 将每个条目放在单独的行上或用逗号分隔每个条目。 5. 点击**提交**。
删除与收件人关联的所有发件人 删除与发件人关联的所有收件人	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行。
删除收件人的个别发件人 删除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. 从文本框添加或删除条目。必须至少保留一个条目。 4. 点击**提交**。

下一步做什么

相关主题

- 安全列表和阻止列表条目的语法 ， 第 152 页
- 清除所有安全列表和阻止列表 ， 第 153 页

安全列表和阻止列表条目的语法

可以使用以下格式将发件人添加到安全列表和阻止列表：

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]

- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]
- user@[ipv6:2001:db8::1]

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

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

清除所有安全列表和阻止列表

如果需要删除所有安全列表和阻止列表条目，包括所有发件人和所有收件人，请按照备份和恢复安全列表/阻止列表 ， 第 154 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，请参阅设置终端用户通过网络浏览器访问垃圾邮件隔离区的权限 ， 第 158 页。

您可能希望在适用情况下为最终用户提供垃圾邮件隔离区的 URL 和以下说明。

相关主题

- 向安全列表添加条目（终端用户） ， 第 153 页
- 将发件人添加到阻止列表（终端用户） ， 第 154 页

向安全列表添加条目（终端用户）

注释 列入安全列表的发件人的邮传送情况取决于系统中配置的其他设置。请参阅安全列表和阻止列表的邮件处理 ， 第 150 页。

最终用户可以通过以下两种方式将发件人添加到安全列表：

- 将隔离邮件的发件人添加到安全列表 ， 第 153 页
- 将发件人添加到不含隔离邮件的安全列表 ， 第 154 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，终端用户可以将发件人添加到安全列表。

步骤 1 从垃圾邮件隔离区。

步骤 2 从下拉菜单中选择**安全列表**，然后选择**释放并添加到安全列表**。

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

将发件人添加到不含隔离邮件的安全列表

步骤 1 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 依次选择**安全列表 (Safelist)**。

步骤 4 从“安全列表”(Safelist) 对话框中，输入邮件地址或域。您可以输入多个域和邮件地址，以逗号分隔。

步骤 5 点击**添加到列表 (Add to List)**。

将发件人添加到阻止列表（终端用户）

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

注释 只能按照以下过程添加阻止列表条目。

步骤 1 登录到垃圾邮件隔离区。

步骤 2 从页面右上角的**选项**下拉菜单中选择**阻止列表**。

步骤 3 输入要列入阻止列表的域或邮件地址。您可以输入多个域和邮件地址，以逗号分隔。

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

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

也可以随同安全管理设备上的其他数据备份安全列表/阻止列表条目。请参阅备份安全管理设备数据，第 281 页。

步骤 1 选择**管理设备 > 系统管理 > 配置文件**。

步骤 2 滚动到**终端用户安全列表/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	相应操作
导出安全列表/阻止列表	请注意 .csv 文件的路径和文件名，并根据需要进行修改。 点击**立即备份**。 设备将使用以下命名约定将 .csv 文件保存到设备的 /configuration 目录： *slbl*<序列号><时间戳>*.csv*
导入安全列表/阻止列表	**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)**。 从配置目录中的文件列表选择所需文件。 选择要恢复的安全列表/阻止列表备份文件。 点击**恢复**。

安全列表和阻止列表故障排除

要对安全列表和阻止列表的问题进行故障排除，您可以查看日志文件或系统警报。

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

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

有关警报的详细信息，请参阅管理警报，第 302 页。

有关日志文件的详细信息，请参阅日志记录，第 333 页。

相关主题

- 列入安全列表的发件人的邮件未传送 ，第 155 页

列入安全列表的发件人的邮件未传送

问题

列入安全列表的发件人的邮件未发送。

解决方案

可能原因：

- 由于恶意软件或内容违规而丢弃了邮件。请参阅安全列表和阻止列表的邮件处理 ，第 150 页。
- 如果您具有多台设备，并且发件人最近已添加到安全列表中，则在处理邮件息时可能尚未同步安全列表/阻止列表。请参阅外部垃圾邮件隔离区和安全列表/阻止列表 ，第 151 页 。

为终端用户配置垃圾邮件管理功能

目标	请参阅
了解适用于最终用户对垃圾邮件管理功能访问的不同身份验证方法的优势和限制。	配置终端用户访问垃圾邮件隔离区的权限，第 159 页和子节
允许最终用户直接通过浏览器访问垃圾邮件隔离区。	访问垃圾邮件管理功能的终端用户的身份验证选项 ，第 156 页
当发送给用户的邮件路由到垃圾邮件隔离区时，请向用户发送通知。 通知可以包含用于访问垃圾邮件隔离区的链接。	通知终端用户被隔离的邮件 ，第 160 页
允许用户指定其知悉为安全的发件人及其知悉发送的是垃圾邮件或其他不需要的邮件的发件人的邮件地址和域。	使用安全列表和阻止列表基于发件人控制邮件发送 ，第 149 页

相关主题

- 访问垃圾邮件管理功能的终端用户的身份验证选项 ，第 156 页
- 设置终端用户通过网络浏览器访问垃圾邮件隔离区的权限 ，第 158 页
- 通知终端用户被隔离的邮件 ，第 160 页

访问垃圾邮件管理功能的终端用户的身份验证选项

注释 邮箱身份验证不允许用户查看发到邮件别名的邮件。

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

对于终端用户垃圾邮件隔离区访问	请
仅通过通知中的链接，无需身份验证	在“终端用户隔离区访问 (End User Quarantine Access)”设置中，选择**无 (None)** 作为身份验证方法。
无访问权限	在“终端用户隔离区访问 (End User Quarantine Access)”设置中，取消选择**启用终端用户隔离区访问 (Enable End-User Quarantine Access)**。

相关主题

- LDAP 身份验证过程 ， 第 157 页
- IMAP/POP 身份验证过程 ， 第 157 页
- SAML 2.0 身份验证过程， 第 158 页
- 配置终端用户访问垃圾邮件隔离区的权限 ， 第 159 页
- 通知终端用户被隔离的邮件 ， 第 160 页
- 将 LDAP 配置为与垃圾邮件隔离区配合使用， 第 223 页
- 关于最终用户访问安全列表和阻止列表 ， 第 153 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，您通常将需要在“全局目录端口”（包含在 6000 中）上具有服务器连接，并且需要创建一个低权限 LDAP 用户，垃圾邮件隔离区可以该用户身份进行绑定，以便执行搜索。
3. 然后，垃圾邮件隔离区使用基本 DN 和查询字符串搜索用户。找到用户的 LDAP 记录时，垃圾邮件隔离区将提取该记录的 DN，并尝试使用该用户记录的 DN 和他们最初输入的密码绑定至目录。如果此密码检查成功，则用户正确通过身份验证，但垃圾邮件隔离区仍需要确定为该用户显示哪些邮箱内容。
4. 邮件使用收件人的信封地址存储在垃圾邮件隔离区中。在用户密码通过 LDAP 验证后，垃圾邮件隔离区会从 LDAP 记录中检索“主邮件属性”，以确定他们应为之显示隔离邮件的哪个信封地址。“主邮件属性”(Primary Email Attribute) 可以包含多个邮件地址，这些邮件地址之后可用于确定应从已进行身份验证的用户的隔离区显示的信封地址。

相关主题

- 访问垃圾邮件管理功能的终端用户的身份验证选项 ， 第 156 页
- 与 LDAP 集成， 第 223 页

IMAP/POP 身份验证过程

1. 根据邮件服务器配置，用户向网络用户界面登录页输入其用户名 (joe) 或邮件地址 (joe@example.com) 与密码。可以修改“登录页消息 (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（请参阅配置终端用户访问垃圾邮件隔离区的权限 ， 第 159 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（例如 joe）的域，将附加此域，并使用完全限定的邮件地址在隔离区中搜索匹配的信封。
   - 否则，垃圾邮件隔离区会使用所输入的邮件地址来搜索匹配信封。

有关 IMAP 的详细信息，请参阅华盛顿大学网站：

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

SAML 2.0 身份验证过程

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

设置终端用户通过网络浏览器访问垃圾邮件隔离区的权限

过程

	命令或操作	目的
步骤 1	了解终端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。	请参阅思科内容安全管理设备指南中的使用 *SAML 2.0* 的 *SSO* 部分
步骤 2	如果使用 LDAP 验证终端用户，请配置 LDAP 服务器配置文件，包括**系统管理 > LDAP > LDAP 服务器配置文件**页上的**垃圾邮件隔离区终端用户身份验证查询**设置。 **示例：** `If you will authenticate end users using SAML 2.0 (SSO), configure the settings on the System Administration > SAML page.`	与 LDAP 集成，第 223 页 和小节 使用 SAML 2.0 的 SSO，第 323 页
步骤 3	配置终端用户访问垃圾邮件隔离区的权限。	配置终端用户访问垃圾邮件隔离区的权限 ，第 159 页
步骤 4	确定终端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 160 页

下一步做什么

相关主题

- 配置终端用户访问垃圾邮件隔离区的权限 ，第 159 页
- 确定最终用户访问垃圾邮件隔离区的 URL，第 160 页
- 终端用户查看的邮件 ，第 160 页

配置终端用户访问垃圾邮件隔离区的权限

无论是否启用终端用户访问权限，管理用户都可以访问垃圾邮件隔离区。

开始之前

请参阅访问垃圾邮件管理功能的终端用户的身份验证选项 ，第 156 页中的要求。

步骤 1 选择**管理设备 > 集中服务 > 垃圾邮件隔离区**。

步骤 2 点击**编辑设置**。

步骤 3 向下滚动到**终端用户隔离区访问权限**部分。

步骤 4 选择**启用终端用户隔离区访问权限**。

步骤 5 指定终端用户尝试查看自己的隔离邮件时，对他们进行身份验证的方法。

选择以下选项	更多信息
无 (None)	-
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，终端用户输入其完整的邮件地址和邮箱密码。 如果 POP 服务器在标题中通告支持 APOP，则出于安全考虑（例如，避免以明文形式发送密码），思科设备将仅使用 APOP。如果对于部分或所有用户不支持 APOP，则应将 POP 服务器重新配置为不通告 APOP。 如果已将服务器配置为使用 SSL，请选择 SSL。如果用户仅输入用户名，则您可以指定要添加的域以自动完成邮件地址。为登录“将域附加到未限定用户名”(Append Domain to Unqualified Usernames) 的用户输入信封的域。
LDAP	配置 LDAP 设置，如本主题的“准备工作”部分中引用的部分中所述。
SAML 2.0	为垃圾邮件隔离启用单点登录。 在使用此选项之前，请确保已配置了“管理设备”>“系统管理”>“SAML”页面上的所有设置。请参阅《思科内容安全管理设备指南》中的使用 *SAML 2.0* 的 *SSO*。

步骤 6 指定在放行邮件之前是否显示邮件正文。

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

步骤 7 提交并确认更改。

下一步做什么

（可选）自定义用户在访问垃圾邮件隔离区时查看的页面（如果尚未进行此操作）。请参阅启用和配置垃圾邮件隔离区 ， 第 144 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`。

注释 本地和外部身份验证的用户无法登录到最终用户垃圾邮件隔离区门户。

终端用户查看的邮件

通常，终端用户只能在垃圾邮件隔离区中查看自己的邮件。

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

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

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

有关发送到用户所属邮件地址的别名的邮件的信息，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知 ， 第 162 页。

相关主题

- 配置终端用户访问垃圾邮件隔离区的权限 ， 第 159 页
- 收件人电子邮件的邮件列表别名和垃圾邮件通知 ， 第 162 页

通知终端用户被隔离的邮件

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

默认情况下，垃圾邮件通知会列出用户的隔离邮件。通知还可包含链接，用户可以点击此链接，以便在垃圾邮件隔离区中查看其隔离邮件。这些链接不会过期。用户可以查看隔离邮件，并决定是将这些邮件传送到其收件箱还是将其删除。

注释 在集群配置中，您可以选择仅在机器级别接收通知的用户。

开始之前

- 为使最终用户管理通知中所列的邮件，他们必须能够访问垃圾邮件隔离区。请参阅配置终端用户访问垃圾邮件隔离区的权限 ， 第 159 页。
- 了解用于使用通知管理垃圾邮件的身份验证选项。请参阅访问垃圾邮件管理功能的终端用户的身份验证选项 ， 第 156 页。
- 如果最终用户以多个别名接收邮件，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知，第 162 页。

步骤 1 依次选择**管理设备 > 集中服务 > 垃圾邮件隔离区**。

步骤 2 点击**编辑设置**。

步骤 3 向下滚动到**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。

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

以下邮件变量将扩展为特定最终用户的实际值：

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

b) 如果您已在此页面上的“最终用户隔离区访问权限”(End User Quarantine Access) 部分中启用了身份验证方法：

- 要在用户通过点击通知中的链接来访问垃圾邮件隔离区时使其自动登录该垃圾邮件隔离区，请选择**启用登录时无需隔离区访问凭证 (Enable login without credentials for quarantine access)**。最终用户通过点击通知中的“放行”(Release) 链接即可放行邮件。
- 如要要求用户在通过点击通知中的链接来访问垃圾邮件隔离区时登录该垃圾邮件隔离区，请取消选择此选项。最终用户无法仅通过点击通知中的“放行”(Release) 链接来放行邮件。

c) 点击**预览邮件 (Preview Message)** 以验证邮件是否与预期一样。

步骤 6 提交并确认更改。

下一步做什么

要确保最终用户接收这些通知，请考虑建议他们将垃圾邮件隔离区通知邮件的“发件人：”(From:)地址添加到其邮件应用（例如 Microsoft Outlook 或 Mozilla Thunderbird）的垃圾邮件设置中的“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 162 页
- 测试通知 ，第 163 页
- 垃圾邮件通知故障排除 ，第 163 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，列表中的所有订阅者都将收到通知。属于多个邮件别名的用户、属于收到通知的 LDAP 组的用户或使用多个邮件地址的用户，都可能收到多个垃圾邮件通知。下表显示了用户可能收到多个通知的案例。

表 *32*: 每个地址/别名的通知数

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

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

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

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

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

测试通知

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

垃圾邮件通知故障排除

相关主题

- 用户收到多个通知 ， 第 163 页
- 收件人未收到通知 ， 第 163 页
- 用户收到多个通知 ， 第 163 页
- 收件人未收到通知 ， 第 163 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。

解决方案

可能原因：

- 用户具有多个邮件地址，并且垃圾邮件发送到其中多个地址。
- 用户是收到垃圾邮件的一个或多个邮件别名的成员。要尽量减少重复并了解详细信息，请参阅收件人电子邮件的邮件列表别名和垃圾邮件通知 ， 第 162 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“将退回邮件传送到：”(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终端用户的身份验证选项 ， 第 156 页。
- 让用户检查其邮件客户端的垃圾邮件设置。
- 检查在启用和配置垃圾邮件隔离区 ， 第 144 页中为**邮件传送方式 (Deliver Messages Via)** 指定的设备或服务器的问题。

管理垃圾邮件隔离区的邮件

本部分介绍如何处理本地或外部垃圾邮件隔离区中的邮件。

管理用户可以查看和管理垃圾邮件隔离区中的所有邮件。

相关主题

- 访问垃圾邮件隔离区（管理用户），第 164 页
- 在垃圾邮件隔离区中搜索邮件，第 164 页
- 查看垃圾邮件隔离区中的邮件，第 165 页
- 发送垃圾邮件隔离区中的邮件，第 165 页
- 删除垃圾邮件隔离区中的邮件，第 165 页

访问垃圾邮件隔离区（管理用户）

管理用户可以查看和管理垃圾邮件隔离区的所有邮件。

访问垃圾邮件隔离区（管理用户）

管理用户可以查看和管理垃圾邮件隔离区的所有邮件。

依次选择**邮件 > 邮件隔离区 > 垃圾邮件隔离区**，然后点击**垃圾邮件隔离区**链接。

垃圾邮件隔离区将在单独的浏览器窗口中打开。

在垃圾邮件隔离区中搜索邮件

步骤 1 指定信封收件人。

注释 您可以输入不完整地址。

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

步骤 3 输入要搜索的日期范围。点击日历图标以选择日期。

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

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

下一步做什么

相关主题

搜索超大邮件集合，第 165 页

搜索超大邮件集合

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。

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

查看垃圾邮件隔离区中的邮件

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

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

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

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

请注意以下提示：

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

  当查看包含附件的邮件时，系统会显示邮件的正文，后跟附件列表。

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

  垃圾邮件隔离区尝试呈现相近的基于 HTML 的邮件。未显示图像。

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

  系统对 Base64 编码的邮件进行解码，然后显示该邮件。

发送垃圾邮件隔离区中的邮件

如果要放行邮件以进行发送，请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**放行**。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。

放行的邮件会直接转到目标队列，跳过邮件管道中的任何其他工作队列处理。

删除垃圾邮件隔离区中的邮件

垃圾邮件隔离区可配置为在经过一定时间后自动删除邮件。此外，垃圾邮件隔离区还可配置为在隔离区达到其最大大小后就自动删除最旧的邮件。也可以手动删除垃圾邮件隔离区中的邮件。

要删除特定邮件，请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上当前显示的所有邮件。

要删除垃圾邮件隔离区中的所有邮件，请禁用隔离区（参阅关于禁用外部垃圾邮件隔离区 ， 第 166 页），然后点击**删除所有邮件 (Delete All Messages)** 链接。链接尾部的括号中的数字是指垃圾邮件隔离区中的邮件数。

垃圾邮件隔离区的磁盘空间

隔离区的可用磁盘空间根据设备型号而异。请参阅查看磁盘空间配额和使用情况 ， 第 321 页。

默认情况下，在经过设置的时间后，系统将自动删除垃圾邮件隔离区中的邮件。如果隔离区已满，则会删除较旧的垃圾邮件。要更改此设置，请参阅启用和配置垃圾邮件隔离区 ， 第 144 页。

相关主题

关于禁用外部垃圾邮件隔离区

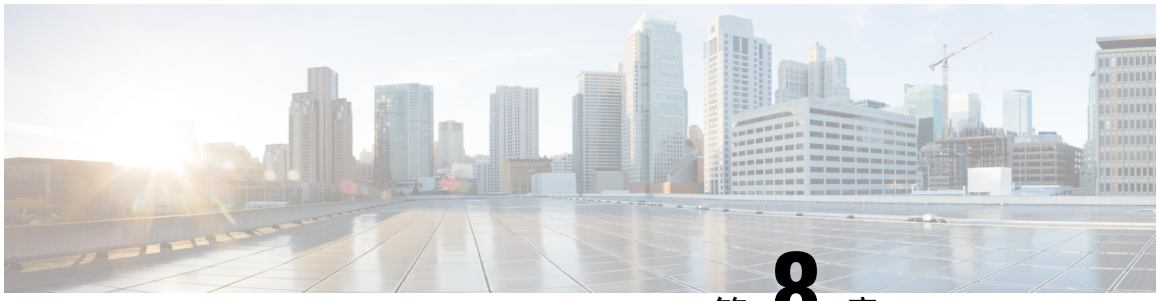
如果禁用垃圾邮件隔离区：

- 如果被禁用的垃圾邮件隔离区中存在邮件，可以选择删除所有邮件。
- 为隔离垃圾邮件设置的所有邮件策略将改为发送邮件。可能需要调整邮件安全设备上的邮件策略。
- 要完全禁用外部垃圾邮件隔离区，请在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 155 页
- 垃圾邮件通知故障排除 ， 第 163 页



第 8 章

集中策略、病毒和病毒爆发隔离区

本章包含以下部分：

集中隔离区概述

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

有关隔离区的详细信息，请参阅邮件安全设备的相应文档。

隔离区类型

隔离区类型	隔离区名称	默认情况下由系统创建？	说明	更多信息
高级恶意软件保护	文件分析	是	保留已发送进行文件分析的邮件，直到返回判定。	• 管理策略、病毒和病毒爆发隔离区 • 处理策略、病毒或爆发隔离区中的邮件
病毒	病毒	是	保留可能正在传输恶意软件（由防病毒引擎确定）的邮件。	
爆发	爆发	是	保留可能作为垃圾邮件或恶意软件由病毒爆发过滤器捕获到的邮件。	
策略	策略	是	暂存邮件过滤器、内容过滤器和DLP邮件操作拦截的邮件。 系统已为您创建了默认策略隔离区。	
	未分类	是	仅在删除邮件过滤器、内容过滤器或DLP邮件操作中指定的隔离区后才保留邮件。 您不能将此隔离区分配到任何过滤器或邮件操作。	
	（您创建的策略隔离区）	否	您创建的用于邮件过滤器、内容过滤器和DLP邮件操作的策略隔离区。	

集中策略、病毒和病毒爆发隔离区

隔离区类型	隔离区名称	默认情况下由系统创建？	说明	更多信息
垃圾邮件	垃圾邮件	是	保留垃圾邮件或可疑垃圾邮件，以供邮件收件人或管理员审核。 垃圾邮件隔离区未包含在策略、病毒和病毒爆发隔离区组中，并且与所有其他隔离区分开管理。	垃圾邮件隔离区，第 143 页

集中策略、病毒和病毒爆发隔离区

过程

	命令或操作	目的
步骤 1	如果您的邮件安全设备在 DMZ 中，且安全管理设备受防火墙保护，请打开防火墙中的端口以允许设备交换集中策略、病毒和病毒爆发隔离区数据。	防火墙资讯，第 385 页
步骤 2	在安全管理设备上，启用此功能。	在安全管理设备上启用集中策略、病毒和病毒爆发隔离区 ，第 171 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 320 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。迁移过程中创建的所有隔离区都具有默认设置。 即使隔离区名称相同，本地隔离区设置也未保留在集中隔离区中。	• 配置策略、病毒和爆发隔离区 ，第 178 页 • 检查系统创建的隔离区的设置 ，第 177 页。

集中策略、病毒和病毒爆发隔离区

	命令或操作	目的
步骤 5	在安全管理设备中，添加要管理的邮件安全设备或从已添加设备的集中服务中选择“策略、病毒和爆发隔离区(Policy, Virus and Outbreak Quarantines)”选项。 • 如果您的邮件安全设备已集群，则属于特定级别（计算机、分组或集群）的所有设备必须添加到安全管理设备，之后您才能在集群中的任意邮件安全设备上启用集中策略、病毒和病毒爆发隔离区。	向每个受管邮件安全设备添加集中策略、病毒和病毒爆发隔离区服务 ， 第 171 页
步骤 6	确认您的更改。	
步骤 7	在安全管理设备上，配置从邮件安全设备迁移现有策略隔离区。	配置策略、病毒和病毒爆发隔离区的迁移 ， 第 172 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。 • **重要事项** 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、病毒和病毒爆发隔离区□
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。 • 迁移过程中创建的隔离区是使用默认设置而不是源本地隔离区中的设置进行创建，即使集中和本地隔离区名称相同也如此。	配置策略、病毒和爆发隔离区 ， 第 178 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。
步骤 12	（推荐）如果始发设备不可用，请指定一台邮件安全设备来处理放行的邮件。	指定处理所放行邮件的备用设备 ， 第 174 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 174 页

在安全管理设备上启用集中策略、病毒和病毒爆发隔离区

开始之前

完成集中策略、病毒和病毒爆发隔离区 ，第 169 页的表中此过程之前的所有步骤。

步骤 1 依次选择**管理设备 > 集中服务 > 策略、病毒和病毒爆发隔离区**。

步骤 2 点击**启用**。

步骤 3 指定与邮件安全设备通信的接口和端口：

- 接受默认选择，除非有特定原因需要更改。
- 如果您的邮件安全设备与安全管理设备不在同一个网络上，则必须使用管理接口。
- 使用您在防火墙中打开的同一端口。

步骤 4 点击**提交**。

下一步做什么

返回集中策略、病毒和病毒爆发隔离区 ，第 169 页表中的后续步骤。

向每个受管邮件安全设备添加集中策略、病毒和病毒爆发隔离区服务

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

开始之前

确保您已完成了集中策略、病毒和病毒爆发隔离区 ，第 169 页表中此位置之前的所有过程。

步骤 1 选择**管理设备 > 集中化服务 > 安全设备**。

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、病毒和病毒爆发隔离区**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”。

b) 在“设备名称”(Appliance Name) 和“IP 地址”(IP Address) 文本字段中，输入正在添加的设备的管理接口的设备名称和 IP 地址。

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

c) 策略、病毒和病毒爆发隔离区服务已预先选择。
d) 点击**建立连接 (Establish Connection)**。
e) 在要托管的设备上输入管理员账户的用户名和密码，然后点击**建立连接**。

注释 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**提交**。

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 确认您的更改。

下一步做什么

返回集中策略、病毒和病毒爆发隔离区 ，第 169 页表中的后续步骤。

配置策略、病毒和病毒爆发隔离区的迁移

开始之前

- 确保您已完成了相应表中此位置之前的所有过程，该表位于：集中策略、病毒和病毒爆发隔离区 ，第 169 页
- 有关迁移过程的警告和信息，请参阅邮件安全设备文档中“在思科内容安全管理设备上集中服务”一章中的“关于策略、病毒和爆发隔离区的迁移”部分。

步骤 1 在安全管理设备上，选择**管理设备 > 集中服务 > 策略、病毒和病毒爆发隔离区**。

步骤 2 点击**启动迁移向导 (Launch Startup Wizard)**。

步骤 3 选择迁移方法：

If	选择	更多信息
• 想要迁移所有关联邮件安全设备中的所有现有策略隔离区， 和 • 所有邮件安全设备上名称相同的策略隔离区具有相同的设置， 和 • 要将所有邮件安全设备上名称相同的全部策略隔离区合并为一个采用该名称的集中策略隔离区。	自动 (Automatic)	使用此流程创建的所有集中策略隔离区均自动配置为默认设置，无论邮件安全设备中名称相同的隔离区的设置如何。 迁移后必须更新这些设置。
• 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 • 您希望迁移一些本地隔离区并删除其他隔离区， 或者 • 您希望将本地隔离区迁移到具有不同名称的集中隔离区 或者 • 您希望将具有不同名称的本地隔离区合并成单个集中隔离区。	自定义 (Custom)	在迁移过程中而不是迁移之前创建的所有集中策略隔离区都将使用新隔离区的默认设置进行配置。 您应在迁移后更新这些设置。

步骤 4 点击**下一步**。

步骤 5 如果选择**自动 (Automatic)**：

验证要迁移的策略隔离区和此页面上的其他信息是否与预期匹配。

病毒、爆发和文件分析隔离区也将迁移。

步骤 6 如果选择**自定义 (Custom)**：

- 要选择显示所有邮件安全设备中的隔离区，还是只显示一台设备中的隔离区，请从**显示其中隔离区: (Show Quarantines from:)** 列表中选择一个选项。
- 选择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。

- 您可以通过从右侧表中选择隔离区并点击**从集中隔离区中删除 (Remove from Centralized Quarantine)** 来更改隔离区映射。

步骤 7 根据需要，点击**下一步**。

步骤 8 提交并确认更改。

下一步做什么

返回集中策略、病毒和病毒爆发隔离区 ， 第 169 页表中的后续步骤。

指定处理所放行邮件的备用设备

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

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

开始之前

- 检验备用设备是否可按预期处理和传送已放行的邮件。例如，加密和防病毒重新扫描的配置应与主设备上的配置匹配。
- 必须为集中策略、病毒和病毒爆发隔离区完全配置备用设备。针对该设备完成集中策略、病毒和病毒爆发隔离区 ， 第 169 页中表内的步骤。

步骤 1 在安全管理设备上，依次择**管理设备 > 集中服务 > 安全设备**。

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。

下一步做什么

相关主题

当邮件安全设备不可用时放行邮件 ， 第 175 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 251 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

- 指定处理所放行邮件的备用设备 ， 第 174 页

管理策略、病毒和病毒爆发隔离区

- 策略、病毒和爆发隔离区的磁盘空间分配 ， 第 176 页
- 邮件在隔离区中的保留时间 ， 第 176 页
- 自动处理的隔离邮件的默认操作 ， 第 177 页
- 检查系统创建的隔离区的设置 ， 第 177 页
- 配置策略、病毒和爆发隔离区 ， 第 178 页
- 关于编辑策略、病毒和爆发隔离区设置 ， 第 179 页
- 确定策略隔离区分配到的过滤器和邮件操作 ， 第 179 页
- 关于删除策略隔离区 ， 第 180 页
- 监控隔离区状态、容量和活动 ， 第 180 页
- 关于隔离区磁盘空间使用量的警报 ， 第 181 页
- 策略隔离区和日志记录 ， 第 181 页
- 关于向其他用户分配邮件处理任务 ， 第 181 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 320 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受管邮件安全设备上爆发隔离区中邮件的磁盘空间，可能受该邮件安全设备上可用于被隔离邮件的磁盘空间所限。
- 有关这种情况的详细信息，请参阅 邮件在隔离区中的保留时间 ，第 176 页

相关主题

- 监控隔离区状态、容量和活动 ，第 180 页
- 关于隔离区磁盘空间使用量的警报 ，第 181 页
- 邮件在隔离区中的保留时间 ，第 176 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配置的保留时间。为各隔离区中的邮件指定保留时间。每封邮件具有各自的特定到期时间，显示在隔离区列表中。除非出现本主题中描述的其他情况，否则邮件存储时间为指定时间。

  注释 病毒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“病毒爆发过滤器”(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 176 页中定义的所有隔离区的大小限制。

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

    （可选）您可以将个别隔离区配置为豁免由于磁盘空间不足而放行或删除。如果将所有隔离区都配置为免除，当磁盘空间达到容量时，邮件将暂存于邮件安全设备中，直到安全管理设备中的空间可用。

    由于安全管理设备不扫描邮件，因此集中爆发隔离区中每个邮件的副本会存储在最初处理该邮件的邮件安全设备上。这样，邮件安全设备可在爆发过滤器规则每次更新时重新扫描

被隔离的邮件，并通知安全管理设备放行不再被视为威胁的邮件。爆发隔离区的两个副本应一直保留相同的邮件集。因此，如果邮件安全设备中的空间鲜有地变满，则两台设备上爆发隔离区中邮件的副本将提前到期，即使集中隔离区仍有空间亦不例外。

在磁盘空间达到里程碑时，您将会收到警报。请参阅关于隔离区磁盘空间使用量的警报，第 181 页。

- 您可删除仍然保留邮件的隔离区。

从隔离区中自动删除邮件后，系统将对该邮件执行默认操作。请参阅自动处理的隔离邮件的默认操作 ，第 177 页。

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

保留时间中时间调整的影响

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

自动处理的隔离邮件的默认操作

当发生邮件在隔离区中的保留时间 ，第 176 页中所述的任何情况时，将对策略、病毒或病毒爆发隔离区中的邮件执行默认操作。

有两个主要默认操作：

- 删除-删除邮件。
- 放行-放行邮件进行传送。

在放行时，系统可能会重新扫描邮件以查找威胁。有关详细信息，请参阅关于重新扫描隔离的邮件，第 187 页。

此外，在经过其预期保留时间之前放行的邮件可以对其执行其他操作，例如添加 X 信头。有关详细信息，请参阅配置策略、病毒和爆发隔离区 ，第 178 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

在您使用隔离区之前，请自定义默认隔离区的设置，包括未分类隔离区。

相关主题

- 配置策略、病毒和爆发隔离区 ，第 178 页

配置策略、病毒和爆发隔离区

开始之前

- 如果您编辑的是现有隔离区，请参阅关于编辑策略、病毒和爆发隔离区设置 ，第 179 页。
- 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 176 页和自动处理的隔离邮件的默认操作 ，第 177 页。
- 确定希望哪些用户对每个隔离区具有访问权，并相应地创建用户和自定义用户角色。有关详细信息，请参阅可访问策略、病毒和爆发隔离区的用户组 ，第 182 页。

步骤 1 选择**邮件 > 邮件隔离区 > 策略、病毒和爆发隔离区**。

步骤 2 执行以下操作之一：

- 点击**添加策略隔离区 (Add Policy Quarantine)**。
- 点击要编辑的隔离区。

步骤 3 输入信息。

请注意以下事项：

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

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

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

步骤 4 指定可以访问此隔离区的用户：

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

步骤 5 提交并确认更改。

下一步做什么

请参阅邮件过滤器 ，第 55 页和“内容过滤器”(Content Filters) 页面 ，第 56 页

- 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

注释

- 您无法重命名隔离区。
- 另请参阅邮件在隔离区中的保留时间 ，第 176 页。

要更改隔离区设置，请从“设备配置”页面选择 邮件 > 邮件隔离区 > 策略、病毒和爆发隔离区，然后点击隔离区名称。

确定策略隔离区分配到的过滤器和邮件操作

您可以查看邮件过滤器、内容过滤器、防数据丢失 (DLP) 邮件操作、与策略隔离区相关的 DMARC 验证配置文件及配置各项设置的邮件安全设备。

步骤 1 依次选择**邮件 > 邮件隔离区 > 策略、病毒和病毒爆发隔离区**。

步骤 2 点击要检查的策略隔离区的名称。

步骤 3 滚动到页面底部并查看**关联邮件过滤器/内容过滤器/DLP 邮件操作 (Associated Message Filters/Content Filters/DLP Message Actions)**。

关于删除策略隔离区

- 在删除策略隔离区之前，请查看其是否与任何活动过滤器或邮件操作关联。请参阅确定策略隔离区分配到的过滤器和邮件操作 ，第 179 页。
- 您可以删除策略隔离区，即使其已分配给过滤器或邮件操作也如此。
- 如果删除的隔离区不为空，则对所有邮件应用隔离区中定义的默认操作，即使已选择磁盘满时不删除邮件的选项亦不例外。请参阅自动处理的隔离邮件的默认操作 ，第 177 页。
- 在删除与过滤器或邮件操作关联的隔离区后，该过滤器或邮件操作后续隔离的所有邮件都将发送到未分类隔离区。在删除隔离区之前，应自定义未分类隔离区的默认设置。
- 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	相应操作
为所有非垃圾邮件隔离区分配的总空间	依次选择**管理策略 > 集中服务 > 策略、病毒和病毒爆发隔离区**，并查看页面中的第一部分。 要更改分配，请参阅管理磁盘空间 ，第 320 页。
所有非垃圾邮件隔离区的当前可用空间	选择，并查看下方的表格。
所有隔离区当前使用的总空间	选择**管理设备 > 集中服务 > 系统状态**。
每个隔离区当前使用的空间	选择**电子邮件 > 邮件隔离区 > 策略、病毒和病毒爆发隔离区**，点击隔离区名称，并直接在隔离区名称下的表格行中查找此信息。
所有隔离区当前的总邮件数	选择**管理设备 > 集中服务 > 系统状态**。
每个隔离区当前的邮件数	选择**电子邮件 > 邮件隔离区 > 策略、病毒和病毒爆发隔离区**，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 > 集中服务 > 系统状态**，并查看“系统信息”部分。
邮件最后进入每个隔离区的日期和时间（策略隔离区之间的移动除外）	选择**电子邮件 > 邮件隔离区 > 策略、病毒和爆发隔离区**，并查看隔离区的表格行。

要查看	相应操作
策略隔离区的创建日期	选择**电子邮件 > 邮件隔离区 > 策略、病毒和病毒爆发隔离区**，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。
策略隔离区创建者姓名	
与策略隔离区关联的过滤器和邮件操作	请参阅确定策略隔离区分配到的过滤器和邮件操作 ，第 179 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 302 页。

策略隔离区和日志记录

AsyncOS 会逐条记录隔离的所有邮件：

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

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

AsyncOS 还会逐条记录从隔离区中删除的邮件：

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

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

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

Info: MID 483 released from all quarantines

Info: MID 484 deleted from all quarantines

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

Info: MID 483 rewritten to 513 by Policy Quarantine

关于向其他用户分配邮件处理任务

您可以将邮件审核和处理任务分发给其他管理用户。例如：

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

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

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

相关主题

- 可访问策略、病毒和爆发隔离区的用户组 ， 第 182 页
- 分配管理任务， 第 245 页

可访问策略、病毒和爆发隔离区的用户组

允许管理用户访问隔离区时，他们可执行的操作取决于其用户组：

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

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

注意：要允许安全管理设备上配置的自定义用户角色在过滤器和 DLP 邮件操作中指定策略隔离区，请参阅为自定义用户角色配置集中隔离区访问权限 ， 第 174 页。

终端用户无权查看或访问策略、病毒和病毒爆发隔离区。

处理策略、病毒或爆发隔离区中的邮件

相关主题

- 查看隔离区中的邮件 ， 第 182 页
- 查找策略、病毒和病毒爆发隔离区中的邮件 ， 第 183 页
- 手动处理隔离区中的邮件， 第 184 页
- 多个隔离区中的邮件 ， 第 185 页
- 邮件详细信息和查看邮件内容， 第 186 页
- 关于重新扫描隔离的邮件 ， 第 187 页
- 病毒爆发隔离区， 第 188 页

查看隔离区中的邮件

目标	相应操作
查看隔离区中的所有邮件	选择**邮件 > 邮件隔离区 > 策略、病毒和病毒爆发隔离区**。 在相关隔离区的行中，点击表格**邮件 (Messages)** 列的蓝色编号。

目标	相应操作
查看爆发隔离区中的邮件	选择**邮件 > 邮件隔离区 > 策略、病毒和病毒爆发隔离区**。 在相关隔离区的行中，点击表格**邮件 (Messages)** 列的蓝色编号。 请参阅“按规则摘要管理”链接，第 188 页。
浏览隔离区中的邮件列表	点击“上一页”(Previous)、“下一页”(Next)、页码或双箭头链接。双箭头会将您引至列表中的第一页 (<<) 或最后一页 (>>)。
排序隔离区的邮件列表	点击列标题（可能包含多个项目的列或“在其他隔离区中”的列除外）。
调整表列大小。	拖动列标题之间的分隔线。
查看导致邮件隔离的内容。	请参阅查看匹配的内容，第 186 页。

相关主题

- 隔离的邮件和国际字符集，第 183 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。

查找策略、病毒和病毒爆发隔离区中的邮件

注释

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

步骤 1 选择 **邮件 > 邮件隔离区 > 策略、病毒和病毒爆发隔离区**。

步骤 2 点击**跨隔离区搜索 (Search Across Quarantines)** 按钮。

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

步骤 3 （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。

- 搜索结果仅包含与指定的所有条件匹配的邮件。例如，如果指定信封收件人和主题，则系统只会返回与信封收件人和主题中均指定的条件匹配的邮件。

下一步做什么

您可以通过与使用隔离区列表相同的方式使用搜索结果。有关详细信息，请参阅手动处理隔离区中的邮件，第 184 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。

可以针对邮件执行以下操作：

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

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

- 从**邮件 > 邮件隔离区 > 策略、病毒和病毒爆发隔离区**页面或页面上的隔离区列表中，点击隔离区中的邮件数。
- 点击**搜索整个隔离区**。
- 点击一个隔离区名称，并在隔离区中搜索。

您可以通过以下方式一次对多封邮件执行这些操作：

- 从邮件列表顶部的选取列表中选择选项。
- 选中页面上列出的每封邮件旁边的复选框。
- 选中邮件列表顶部的表标题中的复选框。这会将操作应用于屏幕上可见的所有邮件。其他页面上的邮件不受影响。

对于爆发隔离区中的邮件，还可以使用其他选项。请参阅《适用于邮件安全设备的 *AsyncOS*》的在线帮助或用户指南中有关病毒爆发过滤器的章节中的按规则摘要管理视图相关信息。

相关主题

- 发送邮件副本，第 185 页

- 关于在策略隔离区之间移动邮件 ， 第 185 页
- 多个隔离区中的邮件 ， 第 185 页
- 自动处理的隔离邮件的默认操作 ， 第 177 页

发送邮件副本

只有属于管理员组的用户可以发送邮件副本。

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

关于在策略隔离区之间移动邮件

在一台设备上，您可以手动在不同策略隔离区之间移动邮件。

将邮件移到其他隔离区时：

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

多个隔离区中的邮件

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

一封邮件在多个隔离区中：

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

由于要放行邮件的用户可能无权访问该邮件所在的所有隔离区，因此适用下列规则：

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

如果邮件在多个隔离区中加入队列，并且用户无权访问一个或多个其他隔离区：

- 将通知用户邮件是否存在于用户有权访问的各隔离区中。
- GUI 仅显示用户有权访问的隔离区中的计划退出时间。（对于特定邮件，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。
- 用户将不会看到导致邮件放入到用户无权访问的隔离区中的匹配内容。
- 放行邮件仅会影响用户有权访问的队列。

- 如果邮件在用户无法访问的其他隔离区中也加入队列，则邮件将保留在隔离区中，保持不变，直到对剩余隔离区具有访问权限的用户进行处理（或者直到通过提前到期或正常到期“正常”放行邮件）。

邮件详细信息和查看邮件内容

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

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

在“隔离的邮件”页面，可以阅读邮件、选择邮件操作或发送邮件副本。您也可以查看邮件在由于“传送时加密”过滤器操作而从隔离区中放行时是否将加密。

“邮件详细信息”(Message Details) 部分显示邮件正文、邮件标题和附件。仅会显示前 100K 的邮件正文。如果邮件较长，则会显示前 100K，后跟省略号 (...)。实际邮件未截断。这仅用于显示。通过点击“邮件详细信息”底部“邮件部分”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。

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

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

注释 对于特殊病毒爆发隔离区，有其他功能可供使用。请参阅病毒爆发隔离区 ， 第 188 页。

相关主题

- 查看匹配的内容 ， 第 186 页
- 下载附件 ， 第 187 页

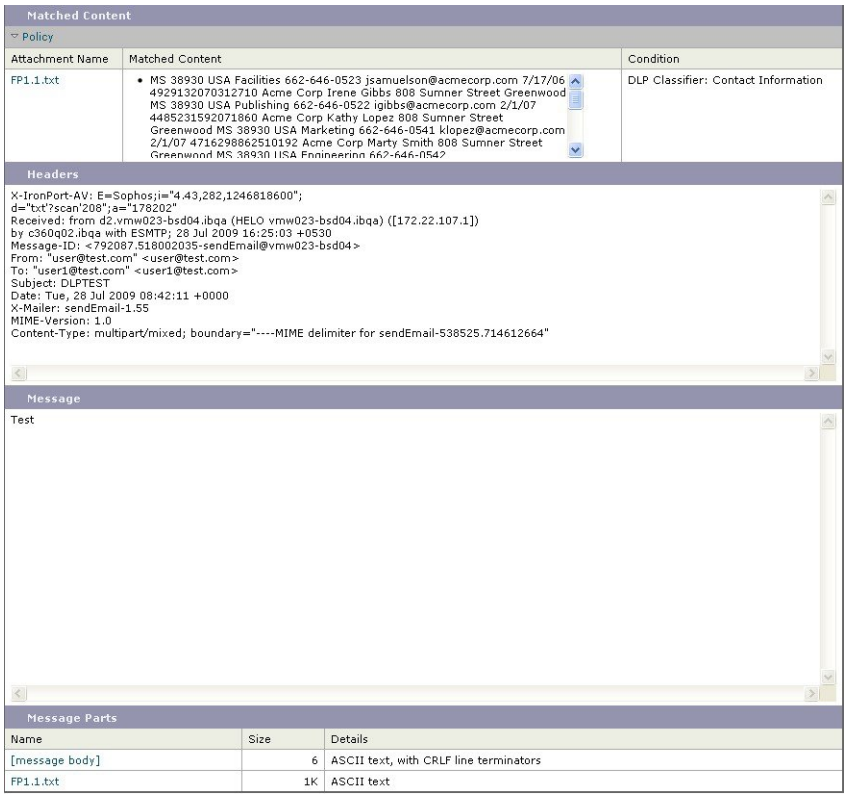
查看匹配的内容

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

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

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

图 *4:* 在策略隔离区中查看到的匹配内容



下载附件

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

关于重新扫描隔离的邮件

从所有队列中放行已隔离的邮件后，根据为原先隔离邮件的设备和邮件策略启用的功能，会进行以下重新扫描：

- 从策略和病毒隔离区放行的邮件由防病毒引擎重新扫描。
- 从病毒爆发隔离区放行的邮件由反垃圾邮件和防病毒引擎重新扫描。（有关重新扫描病毒爆发隔离区中的邮件的信息，请参阅“病毒爆发过滤器”页面，第 67 页邮件安全设备在线帮助或用户指南中关于“病毒爆发过滤器”的一章。)
- 从文件分析隔离区中放行的邮件会被重新扫描以查找威胁。
- 具有附件的邮件在从策略、病毒和病毒爆发隔离区中放行后由文件信誉服务重新扫描。

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

基本原理是防止邮件无限地环回到隔离区。例如，假定邮件已加密并因此发送到病毒隔离区。如果管理员放行邮件，则防病毒引擎仍将无法解密该邮件；但是，不应重新隔离邮件，否则将导致循环，并且邮件将永远不会从隔离区中放行。由于两个判定相同，因此系统第二次会绕过病毒隔离区。

病毒爆发隔离区

在输入有效的病毒爆发过滤器功能许可证密钥后，将出现病毒爆发隔离区。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“病毒爆发过滤器”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。

- 标准
- 规则摘要

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

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

相关主题

- 重新扫描爆发隔离区中的邮件 ，第 188 页
- “按规则摘要管理”链接，第 188 页
- 向思科系统公司报告误报或可疑邮件，第 188 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，则扫描引擎会根据应用于邮件的邮件流策略来扫描从病毒爆发隔离区中放行的每封邮件。

“按规则摘要管理”链接

点击隔离区列表中病毒爆发隔离区旁边的“按规则摘要管理”(Manage by Rule Summary)链接，以查看“按规则摘要管理”(Manage by Rule Summary)页面。您可以根据哪些病毒爆发规则导致隔离邮件来对隔离区中的所有邮件执行邮件操作（放行、删除、延迟退出）。这非常适合清理爆发隔离区中的大量邮件。有关更多信息，请参阅邮件安全设备的联机帮助或用户指南中有关“病毒爆发过滤器”一章中的“管理规则摘要”视图的信息

向思科系统公司报告误报或可疑邮件

查看爆发隔离区中邮件的详细信息时，可以将邮件发送到思科报告误报或可疑邮件。

步骤 1 导航到爆发隔离区中的邮件。

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

步骤 3 点击**发送**。

排除集中策略隔离区故障

管理用户无法选择过滤器和 DLP 邮件操作中的隔离区

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 174 页

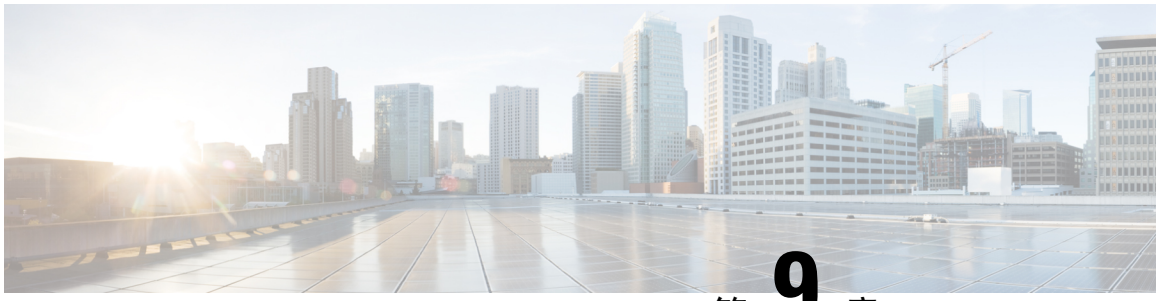
不重新扫描从集中病毒爆发隔离区放行的邮件

问题

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

解决方案

在以下内容所述的情况下，可能会出现这种情况。 关于重新扫描隔离的邮件 ， 第 187 页



第 9 章

管理网络安全设备

本章包含以下部分：

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	请
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 流量监控器”(L4TM) 设置。 支持的确切功能取决于主配置版本，它与某个网络安全AsyncOS 版本相对应。	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。
注意：必须在每台网络安全设备上独立配置与思科身份服务引擎 (ISE) 的集成。思科身份服务引擎设置无法从思科内容安全管理设备发布。	使用高级文件发布。
联邦信息处理标准 (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 流量监控器 (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

WSA - 为了配置未使用过的机器，他们需要先配置什么（在 SSW 后），然后再使用配置文件和/或主配置？如果他们使用配置文件，这样做不会导致 IP 地址问题吗？从 SMA 发布配置文件（与在多个 SMA 上使用来自 WSA 的同一配置文件相反）可能不会遇到此问题。

设备	相应操作	更多信息
—	检查常规配置要求和警告。	请参阅有关使用主配置的重要注意事项，第 193 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 193 页。
网络安全设备	在所有目标网络安全设备上，启用并配置用于支持您将在安全管理设备的主配置中配置的策略和其他设置的必需特性和功能。	-
网络安全设备	（**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 194 页。

设备	相应操作	更多信息
安全管理设备	初始化主配置。	请参阅初始化并配置主配置， 第 194 页。
安全管理设备	将网络安全设备关联到主配置。	请参阅关于将网络安全设备与主配置关联， 第 194 页。
安全管理设备	在主配置中导入和/或手动配置策略、自定义 URL 类别和/或网络代理绕行列表。	请参阅配置要发布的设置， 第 196 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。	请参阅确保一致地启用功能， 第 199 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 202 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 212 页

有关使用主配置的重要注意事项

注释 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。

每个主配置包含要用于一个或多个特定网络安全 AsyncOS 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。

注释 主配置版本应与网络安全设备上的 AsyncOS 版本相匹配，如兼容性矩阵所指定。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) 详细信息页面未指明任何差异，也可能发生这种情况。在这种情况下，您必须手动比较每台设备上的配置。

在安全管理设备上启用集中配置管理

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**。

步骤 3 如果您在运行“系统设置向导”(System Setup Wizard) 后首次启用集中配置管理，请查看终端用户许可协议，然后点击**接受**。

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

注意：在初始化主配置后，“初始化”选项不可用。相反，请使用配置要发布的设置 ， 第 196 页介绍的其中一种方法填充主配置。

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 (Configuration Masters)**。

步骤 2 在“选项”(Options) 列中点击**初始化 (Initialize)**。

步骤 3 在“初始化主配置”(Initialize Configuration Master) 页面上：

- 如果您有某个以前版本的现有主配置，并且希望将相同的设置用于新的主配置或从相同的设置开始，请选择**复制主配置 (Copy Configuration Master)**。您稍后还可以从现有的主配置中导入设置。
- 否则，请选择**使用默认设置 (Use default settings)**。

步骤 4 点击**初始化 (Initialize)**。

主配置现在可用。

步骤 5 为每个主配置版本重复上述初始化步骤。

关于将网络安全设备与主配置关联

有关主配置与网络安全版本兼容性的信息，请参阅确定要使用的主配置版本 ， 第 193 页。

将设备添加到主配置的最简单过程取决于具体情况：

If	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其与主配置版本关联 ，第 195 页
您已经添加网络安全设备	将主配置版本与网络安全设备关联 ，第 195 页

添加网络安全设备并将其与主配置版本关联

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。

开始之前

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 193 页。

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”。

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。

注释 如果在“IP 地址 (IP Address)”文本字段中输入 DNS 名称，则点击**提交**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) 服务已预先选择。

步骤 5 点击**建立连接 (Establish Connection)**。

步骤 6 在要托管的设备上输入管理员账户的用户名和密码，然后点击**建立连接**。

注释 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 选择您要将设备分配至哪个主配置版本。

步骤 9 提交并确认更改。

步骤 10 对于您要为其启用“集中配置管理”(Centralized Configuration Management) 的每台网络安全设备，请重复上述操作程序。

将主配置版本与网络安全设备关联

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。

开始之前

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 193 页。

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**。

注释 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可启用它。有关详细信息，请参阅启用要发布的功能 ，第 200 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**主配置 (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

使用要发布的设置来设置您的主配置。

有几种方法可以设置主配置：

If	相应操作
您从以前的安全管理 AsyncOS 版本进行升级 和 您未通过将较早的现有主配置版本复制到新的主配置版本来初始化新版本。	导入旧版本。请参阅从现有主配置导入，第 196 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 192 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中导入设置 ，第 197 页。
您需要修改导入的设置	请参阅直接在主配置中配置网络安全功能，第 198 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。 请参阅直接在主配置中配置网络安全功能，第 198 页。

从现有主配置导入

您可以将现有的主配置升级到新的、更高的主配置版本。

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 (Configuration Masters)**。
步骤 2 在“选项 (Options)”列中，点击**导入配置 (Import Configuration)**。
步骤 3 对于**选择配置来源 (Select Configuration Source)**，请从列表中选择一个主配置。
步骤 4 选择是否在此配置中包括现有的自定义用户角色。
步骤 5 点击**导入**。

下一步做什么

关于自定义网络用户角色 ，第 252 页

从网络安全设备中导入设置

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。

开始之前

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 193 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。

注释 如果您尝试导入的配置文件使用的 URL 类别集比安全管理设备具有的 URL 类别集更旧，加载将失败。

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”部分，点击**浏览**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**。

直接在主配置中配置网络安全功能

您可以在主配置中配置以下功能，具体取决于版本：

• 身份/识别配置文件 • SaaS 策略 • 解密策略 • 路由策略 (Routing Policies) • 访问策略 • 总体带宽限制	• 思科数据安全 • 出站恶意软件扫描 (Outbound Malware Scanning) • 外部数据丢失防护	• SOCKS 策略 • 自定义 URL类别 • 定义的时间范围和/或配额 • 绕行设置 • L4通信监控

要直接在主配置中配置每项功能的设置，请依次选择**网络 > 主配置** <版本> > <功能>。

除在主配置中配置功能时特定于 SMA 的差异 ， 第 198 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 193 页

网络安全用户指南的所有版本均可从以下网址获得：
http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-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 *33:* 功能配置：主配置与网络安全设备之间的差异

功能或页面	详细信息
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，请参阅确保一致地启用功能 ， 第 199 页。
身份/识别配置文件	• 请参阅关于在主配置中使用身份/识别配置文件的提示 ， 第 199 页。 • 在添加或编辑身份/识别配置文件时，如果具有身份验证领域且支持透明用户识别的网络安全设备已添加为受管设备，则**透明地识别用户**选项可用。
使用思科身份服务引擎 (ISE) 识别用户的策略	约每五分钟从网络安全设备更新一次安全组标签 (SGT) 信息。管理设备不与 ISE 服务器直接通信。 要按需更新 SGT 列表，请选择**网络 > 实用程序 > 网络设备状态**，点击某台连接到 ISE 服务器的网络安全设备，然后点击**刷新数据**。根据需要对其他设备重复此步骤。 最常见的部署方案是一家公司只有一台所有 WSA 连接至的 ISE 服务器（这是 ISE 的全部要点）。不支持具有不同数据的多台 ISE 服务器。

功能或页面	详细信息
“访问策略”(Access Policies)>“编辑组”(Edit Group)	在“策略成员定义”(Policy Member Definition) 部分中配置“身份/识别配置文件”(Identities /Identification Profiles) 和“用户”(Users) 选项时，如果您使用外部目录服务器，则以下内容适用： 当您在“编辑组”(Edit Group) 页面上搜索组时，只会显示前 500 项匹配的结果。如果没有看到所需的组，可以在“目录”搜索字段中输入该组并点击**添加**按钮，将其添加到“授权组”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)	
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。

关于在主配置中使用身份/识别配置文件的提示

在安全管理设备上创建身份/识别配置文件时，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。

完成此任务的一种方法是为每台设置建立一组身份/识别配置文件，然后拥有引用这些身份/识别配置文件的策略。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/识别配置文件和策略。使用此方法，您不必手动配置任何设置。这实际上是一个“按设备”的身份/识别配置文件。

使用此方法的唯一挑战：您具有一个在站点之间不同的默认策略或身份/识别配置文件。例如，您在一个站点具有为“默认允许及身份验证”(default allow with auth) 设置的策略，在另一个站点具有为“默认拒绝”(default deny) 设置的策略。此时，您将需要在默认设置上创建按设备的身份/识别配置文件和策略；实际上是创建您自己的“默认”策略。

确保一致地启用功能

在发布主配置之前，您应该确保将发布该主配置，并确保在发布后将按照您的期望启用并配置预期的功能。

为此，请执行以下两项操作：

- 比较启用的功能 ， 第 200 页
- 启用要发布的功能 ， 第 200 页

注释 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。

注释 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。

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**服务是否显示在管理设备上？(Is Service Displayed on Management Appliance?)** 列应该一致。

- 已启用 = 是
- 已禁用和未配置 = 否或已禁用。
- N/A＝不适用。例如，可能无法使用主配置对该选项进行配置，但是会列出该选项，使您可以查看功能密钥状态。

配置不匹配将以红色文本显示。

下一步做什么

如果某项功能的已启用/已禁用设置不匹配，请执行以下操作之一：

- 更改主配置的相关设置。请参阅启用要发布的功能 ，第 200 页。
- 在网络安全设备上启用或禁用该功能。某些更改可能影响多个功能。有关相关功能的信息，请参阅《适用于思科网络安全设备的 AsyncOS 用户指南》。

启用要发布的功能

启用您要使用主配置发布其设置的功能。

开始之前

确定必须启用和禁用哪些功能。请参阅比较启用的功能 ，第 200 页。

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**。

“编辑安全服务显示”(Edit Security Services Display) 页面列出了每个主配置中出现的功能。

功能旁边的“N/A”表示该功能在此主配置版本中不可用。

注释　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。有关说明和注意事项，请参阅禁用未使用的主配置 ，第 201 页。

步骤 4 对于您将使用的每个主配置，请为要启用的每项功能选中或取消选中“是”复选框。

某些功能的特殊注意事项（可用的选项因主配置版本而异）：

- 透明模式。如果使用“转发”(Forward) 模式，则代理绕行功能将不可用。
- 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 点击**提交**。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**。

步骤 6 在**安全服务显示 (Security Services Display)** 页面上，确认**是 (Yes)** 出现在您选择的每个选项旁边。

步骤 7 确认您的更改。

下一步做什么

- 验证现在已经为您将发布到的设备正确启用或禁用所有功能。请参阅比较启用的功能 ，第 200 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

您可以选择不显示未使用的主配置。

但是，必须启用至少一个主配置。

注释　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”。

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**。

步骤 3 取消选中未使用的主配置的复选框

步骤 4 提交并确认更改。

设置为使用高级文件发布

如果您的系统设置为使用主配置，则它已设置高级文件发布。

否则，请完成以下主题中的操作程序，这些操作程序适用于高级文件发布以及主配置发布。

- 在安全管理设备上启用集中配置管理，第 194 页
- 初始化主配置 ，第 194 页
- 关于将网络安全设备与主配置关联，第 194 页

将配置发布到网络安全设备

- 发布主配置 ，第 202 页
- 使用高级文件发布功能发布配置，第 205 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。

- 在发布主配置之前 ，第 202 页
- 立即发布主配置 ，第 203 页
- 稍后发布主配置 ，第 204 页
- 使用命令行界面发布主配置，第 205 页

在发布主配置之前

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 191 页。

所有发布作业

- 目标网络安全设备上的 AsyncOS 版本应与主配置版本相同，或者是确定为兼容的版本 SMA 兼容性矩阵，第 6 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 192 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 200 页，如有必要，请参阅启用要发布的功能 ，第 200 页。如果您为未在目标设备上启用的功能发布配置，则不会应用这些配置。

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。

要识别在发布时遇到的配置不匹配，请参阅查看发布历史记录，第 207 页。

- 在发布之前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时可以恢复现有配置。有关详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》。

- 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。

网络代理重新启动会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。

- 在将任何更改发布到身份/识别配置文件时，所有终端用户必须重新进行身份验证。

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”的情况下配置的领域，但已在身份/识别配置文件或 SaaS 策略中选择“透明用户身份识别”：
  - 对于身份/识别配置文件，“透明用户识别”(Transparent User Identification) 已禁用，改为选中“需要身份验证”(Require Authentication) 选项。
  - 对于 SaaS 策略，“透明用户识别”(Transparent User Identification) 选项已禁用，改为选中默认选项“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未反映与此发布请求相关联的网络设备上的一个或多个安全服务的状态。受影响的设备是：“*<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的配置不正确。转到每台设备的网络设备状态 (Web Appliance Status) 页面可获得有助于对该问题进行故障排除的详细视图。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。

如果主配置中身份/识别配置文件中的方案为：	则网络安全设备上的身份/识别配置文件中的方案变成
使用 Kerberos	使用 NTLMSSP 或基本
使用 Kerberos 或 NTLMSSP	使用 NTLMSSP
使用 Kerberos 或 NTLMSSP 或 Basic	使用 NTLMSSP 或基本

立即发布主配置

开始之前

请参阅在发布主配置之前 ， 第 202 页中的重要要求和信息。

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 “系统生成的作业名称”(System-generated job name) 在默认情况下处于选中状态，或者请输入自定义的作业名称（不超过 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“在列表中选择设备”(Select appliances in list) 以显示分配给主配置的设备列表。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) 页面上的红色进度条和文本表示在发布期间出错。如果另一个作业当前正在发布，则您的请求将在上一个作业完成时执行。

注释 正在进行的作业的详细信息还会出现在**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)** 页面上。点击**检查进度**访问“正在发布”页面。

下一步做什么

检查以确保发布完全成功。请参阅查看发布历史记录， 第 207 页。系统将记录未完全发布的项目。

稍后发布主配置

开始之前

请参阅在发布主配置之前 ， 第 202 页中的重要要求和信息。

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 “系统生成的作业名称”(System-generated job name) 在默认情况下处于选中状态，或者请输入自定义的作业名称（不超过 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“在列表中选择设备”(Select appliances in list) 以显示分配给主配置的设备列表。选择要将配置发布到的设备。

步骤 7 点击**提交**。

步骤 8 在**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)** 页面上查看已安排的作业列表。要编辑已安排的作业，请点击作业的名称。要取消待定的作业，请点击对应的垃圾桶图标并确认您要删除该作业。

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。

注释　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。

下一步做什么

检查以确保发布完全成功。请参阅查看发布历史记录，第 207 页。系统将记录未完全发布的项目。

使用命令行界面发布主配置

注释　请参阅在发布主配置之前，第 202 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。此关键字是必需的。选项 *job_name* 是可选的，如果未指定该选项，系统将生成它。

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）。选项 *host_ip* 可以是用逗号分隔的多个主机 IP 地址。

要验证 **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，您可以转到“发布历史记录”(Publish History) 页面：依次选择**网络 (Web) > 实用程序 (Utilities) > 发布 (Publish) > 发布历史记录 (Publish History)**。

使用高级文件发布功能发布配置

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 191 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 205 页
- 高级文件发布：稍后发布，第 206 页

高级文件发布：立即发布配置

开始之前

- 验证您将发布的配置版本与您发布到的设备的 AsyncOS 版本是否兼容。请参阅位于以下网址的兼容性矩阵：
  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。有关详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》。

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 “系统生成的作业名称”(System-generated job name) 在默认情况下处于选中状态，或者请输入作业名称（不超过 80 个字符）。

步骤 5 对于**要发布的主配置 (Configuration Master to Publish)**，请选中**高级文件选项 (Advanced file options)**。

步骤 6 点击**浏览**以选择在步骤 1 中保存的文件。

步骤 7 从“网络设备”(Web Appliances) 下拉列表中，选择**在列表中选择设备 (Select appliances in list)** 或**分配给主配置的所有设备 (All assigned to Master)**，然后选择您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

开始之前

- 验证您将发布的配置版本与您发布到的设备的 AsyncOS 版本是否兼容。请参阅位于以下网址的兼容性矩阵：
  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。有关详细信息，请参阅《思科网络安全设备 AsyncOS 用户指南》。

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 **系统生成的作业名称 (System-generated job name)** 在默认情况下处于选中状态，或者请输入作业名称（不超过 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**，请选择**高级文件选项**，然后点击**浏览**，以选择在步骤 1 中保存的配置文件。

步骤 7 从“网络设备”(Web Appliances) 下拉列表中，选择**在列表中选择设备 (Select appliances in list)** 或**分配给主配置的所有设备 (All assigned to Master)**，然后选择您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

要查看	相应操作
已安排但尚未发生的发布作业的列表	依次选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**，然后查看**待定作业 (Pending Jobs)** 部分。
每台设备的最后发布的配置列表	依次选择**网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status)**，然后查看**最后发布的配置 (Last Published Configuration)** 信息。
当前正在进行的发布作业的状态	依次选择**网络 (Web) > 实用程序 (Utilities) > 发布到网络设备 (Publish to Web Appliances)**，然后查看**发布进度 (Publishing Progress)** 部分。
至所有或任何设备的所有或任何发布作业的历史记录	请参阅查看发布历史记录

查看发布历史记录

查看发布历史记录有利于检查在发布期间可能发生的错误，或识别在配置的功能与目标设备上启用的功能之间的不匹配。

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 要查看关于特定作业的其他详细信息，请点击“作业名称”(Job Name) 列中的特定任务名称。

步骤 3 查看更多信息：

- 要查看关于作业中的特定设备的状态详细信息，请点击**详细信息 (Details)** 链接。

此时将出现“网络设备发布详细信息”(Web Appliance Publish Details) 页面。

- 要查看关于作业中的特定设备的其他详细信息，请点击设备名称。

此时将出现**网络 (Web) > 实用程序 (Utilities) > 网络设备状态 (Web Appliance Status)** 页面。

集中化升级管理

您可以使用单个安全管理设备 (SMA) 同时升级多个网络安全设备 (WSA)。您还可以为每台 WSA 应用不同软件升级。

- 为网络安全设备设置集中升级管理，第 208 页
- 选择并下载 WSA 升级，第 209 页

• 使用安装向导，第 210 页

为网络安全设备设置集中升级管理

请按照以下步骤，在此安全管理设备上配置集中升级服务：

• 启用集中升级管理器，第 208 页
• 将集中升级服务添加到每个托管网络安全设备，第 208 页

启用集中升级管理器

开始之前

- 在启用集中升级管理之前，应配置所有网络安全设备并确保其按预期工作。
- 您必须在每个将要接收集中升级的托管网络安全设备上逐一启用集中升级。

注释 要在 CLI 中启用集中升级，请使用

```
applianceconfig > services > [...] > Enable Centralized Upgrade > Y
```

- 请确保在安全管理设备上安装相应的功能密钥。

步骤 1 在安全管理设备上，选择**管理设备**页面，然后依次选择**集中服务 > 集中升级管理器**。

步骤 2 点击**编辑设置**。

步骤 3 选中**启用**。

步骤 4 提交并确认更改。

将集中升级服务添加到每个托管网络安全设备

在安全管理设备上启用集中升级管理器后，必须通过在各个托管 WSA 上启用集中升级，将所需的网络安全设备添加到升级管理器名录。

步骤 1 在安全管理设备上，选择**管理设备**页面，然后选择**集中服务 > 安全设备**。

步骤 2 如果您尚未添加网络安全设备，或者您需要为集中升级管理添加其他设备：

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。

注释　可以在“IP 地址”文本字段中输入 DNS 名称，但是当您点击**提交**时，该名称将解析为 IP 地址。

c) 请务必选中**集中升级**。
d) 点击**建立连接 (Establish Connection)**。
e) 在要托管的设备上输入管理员账户的用户名和密码，然后点击**建立连接**。

注释　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。

等待该页面表格上方显示成功消息。

f) 点击“测试连接”。

阅读表格上方的测试结果。

g) 点击**提交**。

对您希望添加到托管网络安全设备列表中的每个 WSA 重复此程序，同时启用集中升级管理。

步骤 3 要在已添加到托管设备列表中的 WSA 上启用集中升级管理：

a) 点击网络安全设备名称，打开“编辑网络安全设备设置”页面。
b) 在“WSA 集中服务”部分选择**集中升级**。
c) 点击**提交**。

对您希望启用集中升级管理的每个 WSA 重复此程序。

步骤 4 确认您的更改。

下一步做什么

有关向托管设备列表添加设备和编辑托管设备列表的详细信息，请参阅关于添加受管设备，第 14 页。

选择并下载 WSA 升级

步骤 1 在安全管理设备上，选择**网络**页面，然后依次选择**实用程序 > 集中升级**。

列出最近为升级选择的任何设备以及升级状态。

步骤 2 点击“集中升级”页面上的**升级设备**按钮。

列出可升级的所有托管 WSA。

步骤 3 通过勾选列表中名称前面的框，选择要升级的每个网络安全设备。

步骤 4 点击**下载向导**或**下载并安装向导**。

“下载向导”可用于选择要下载到所选 WSA 的升级软件包；此操作仅供下载 - 您可以安装下载的软件包并稍后重新启动每个系统。

“下载和安装向导”可用于选择要下载的升级软件包并在所选WSA上立即进行安装。安装后，每个系统都会自动重启。

步骤 5 系统将显示已启动向导的“获取升级”页面；为所选WSA获取所有可用的升级（“已完成获取可用升级”显示在WSA矩阵的**状态**列）后，点击**下一步**继续。

步骤 6 “可用升级”页面列出每个所选WSA的所有可用升级版本；最多可以选择五个版本进行比较，然后点击**下一步**。

步骤 7 向导的“升级选择”页面会为每个 WSA 提供所选升级的兼容性矩阵；请为每个 WSA 选中所需的升级版本，然后点击**下一步**。

步骤 8 “摘要”页面列出每个所选 WSA 和升级版本的摘要信息；点击**下一步**继续向导。

步骤 9 完成一系列的下载检查后，例如连接状态，“审核”页面将提供每个WSA的下载状态列表。点击**开始下载**即可将升级软件包下载到每个所选 WSA。

“集中升级”页面在整个过程中显示下载状态信息。

下一步做什么

- **下载向导** - 如果在此程序开始时点击此按钮，当下载完成时，依次选择**网络 > 实用程序 > 集中升级**，或点击浏览器窗口中的“刷新页面”按钮，可以刷新“集中升级”页面。

  除所有可升级的托管 WSA 列表之外，“集中升级”页面的另一部分现在会列出已下载升级软件包的所有 WSA。（您可以点击每个条目旁边显示的垃圾桶按钮，从该 WSA 中删除已下载的升级软件包。）

  任何时候，您都可以选择此列表中的一个或多个WSA，然后点击“安装向导”，以开始在每个所选 WSA 上安装已下载的升级软件包；在 WSA 上完成安装后，将重新启动设备。有关使用此向导的信息，请参阅使用安装向导，第 210 页。

- **下载并安装向导** - 如果在此程序开始时点击此按钮，当下载完成时，系统会自动开始升级安装；有关此程序的信息，请参阅使用安装向导，第 210 页（从步骤 2 开始）。安装完成后，WSA 将重新启动。

使用安装向导

“安装向导”开始时，无论是自动作为下载并安装过程的一部分，还是在选择一个或多个具备已下载但尚未安装的升级软件包的 WSA 后点击“集中升级”页面上的“安装向导”按钮，请按照以下步骤配置安装。

步骤 1 如果安装之前下载的升级软件包：

a) 在“集中升级”页面的“具有已下载 AsyncOS 版本的网络设备”部分选择所需的 WSA（**网络 > 实用程序 > 集中升级**）。

b) 点击**安装向导**。

步骤 2 在向导的“升级准备”页面上，对于每个所选 WSA：

- 如果要将 WSA 当前配置的备份副本保存到系统的配置目录，请勾选**升级之前将当前配置保存到配置目录**。

- 如果已选中**保存当前配置**选项，您可以勾选在**配置文件**中**屏蔽密码**，以在备份副本中屏蔽所有当前配置密码。请注意，不能使用 **Load Configuration** 命令来重新加载已屏蔽密码的备份文件。
- 如果已勾选**保存当前配置**选项，您可以在**通过邮件将文件发送到**字段中输入一个或多个邮件地址；备份配置文件副本会通过邮件发送至每个地址。多个地址之间用逗号分隔。

步骤 3 点击**下一步**。

步骤 4 “升级摘要”页面将列出每个所选 WSA 的升级准备信息；点击**下一步**继续向导。

步骤 5 完成一系列的设备检查后，例如连接状态，“审核”页面将提供每个 WSA 的安装状态列表。您可以取消选择显示错误的设备。点击**开始安装**，以开始将升级软件包安装到每个所选 WSA。

您将返回“集中升级”页面，此页面显示安装状态信息。

注释 安装完成后，将重新启动每个 WSA。

下一步做什么

注释 或者，您也可以为任何之前从 WSA 下载的软件包运行安装程序。也就是说，WSA 的**系统管理 > 系统升级**页面上将列出已下载的升级软件包以及“安装”按钮。有关详细信息，请参阅《思科网络安全设备用户指南》中的“升级和更新 AsyncOS 和安全服务组件”。

查看网络安全设备状态

- 比较启用的功能 ， 第 200 页
- 查看网络设备的状态摘要 ， 第 211 页
- 查看各台网络安全设备的状态 ， 第 211 页
- 网络设备状态详细信息 ， 第 212 页

查看网络设备的状态摘要

网络 > 实用程序 > 网络设备状态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。

查看各台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。

注释 只有支持集中管理的计算机才会显示数据。

注释 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”。

网络设备状态详细信息

此页面上的大多数信息都由网络安全设备推送：

- 系统状态信息（正常运行时间、设备型号和序列号、AsyncOS 版本、构建日期、AsyncOS 安装日期和时间以及主机名）
- 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
- 此网络安全设备连接的思科身份服务引擎 (ISE) 服务器。
- 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）

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**链接。页面上的时间戳将向您告知最后刷新数据的时间。

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。

您应该采取的行动包括：

- 了解 URL 类别集更新的影响 ， 第 213 页
- 确保您将收到关于 URL 类别集更新的通知和警报 ， 第 213 页
- 为新类别和已更改的类别指定默认设置 ， 第 213 页
- 在更新 URL 类别集时，检查您的策略和身份/识别配置文件设置 ， 第 213 页

了解 URL 类别集更新的影响

当 URL 类别集更新发生时，它们可能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”一章的“管理 URL 类别集的更新”部分（见文档 ， 第 393 页中提供的链接）。类别说明在同一章的“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	相应操作
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 393 页。
警报（当URL类别集更新已影响现有策略设置时）	转到**管理设备 > 系统管理 > 警报**，并确保将您配置为接收“系统”类别中的警告级别警报。有关警报的详细信息，请参阅管理警报 ， 第 302 页

为新类别和已更改的类别指定默认设置

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。

在更新 URL 类别集时，检查您的策略和身份/识别配置文件设置

URL 类别集更新触发两种类型的警报：

- 有关类别更改的警报
- 有关策略因类别更改而发生更改或被禁用的警报

在接收关于 URL 类别集更改的警报时，您应该检查基于 URL 类别的现有策略和身份/识别配置文件，以确保其仍然符合您的策略目标。

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。

应用可视性与可控性 (AVC) 更新

SMA 将自动使用它管理的大多数网络安全设备上存在的 AVC 引擎版本。

对配置管理问题进行故障排除

在主配置身份/识别配置文件中，组不可用

问题

在**网络 > 主配置 > 身份/识别配置文件**中，“策略成员身份定义”页面不显示“选定的组和用户”下的“组”选项。

解决方案

如果您有多个网络安全设备：在每个 WSA 上，在“网络”>“身份验证”中，请确保领域名称在所有 WSA 间是唯一的，除非同名领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 > 实用程序 > 网络设备状态**，点击每个设备名称，然后滚动至“详细信息”页面底部。

主配置、访问策略、Web 信誉和防恶意软件设置页面设置不符合预期

问题

主配置中的**访问策略 > Web 信誉和防恶意软件设置**页面缺少预期的设置，包括“Web 信誉得分”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。

解决方案

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)。

配置发布失败故障排除

问题

发布配置失败。

解决方案

查看**网络 > 实用程序 > 网络设备状态**页面。在下列情况下，发布将失败：

- “网络设备服务”(Web Appliance Service) 列中的状态与“服务是否显示在管理设备上？”(Is Service Displayed on Management Appliance?) 列中的状态之间存在差异。
- 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。

后续操作：

- 查看发布历史记录， 第 207 页
- 比较启用的功能 ， 第 200 页
- 启用要发布的功能 ， 第 200 页

第 10 章

监控系统状态

本章包含以下部分：

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 331 页。）

要在任何其他时间访问“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)**。

在您启用监控服务并添加受管设备之前，只有“系统信息”(System Information) 部分提供状态信息。如果您运行了“系统设置向导”(System Setup Wizard)，启用了集中服务，并添加了受管设备，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) 部分会填充数据。

状态信息包括以下内容：

- **集中服务**：每项集中服务的状态，包括处理队列使用情况
- **系统正常运行时间**：设备已持续运行多长时间
- **CPU 利用率**：每项监控服务使用的 CPU 容量百分比
- **系统版本信息**：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 218 页
- 监控 CPU 利用率 ， 第 218 页
- 监控受管设备的数据传输状态 ， 第 219 页

监控安全管理设备容量

- 监控处理队列 ， 第 218 页
- 监控 CPU 利用率 ， 第 218 页

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。

注释 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。

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**部分中，查看以下各项的处理队列百分比：

a) 集中报告（“邮件安全”子部分）
b) 集中邮件跟踪
c) 集中报告（“网络安全”子部分）

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：

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**部分并查看 **CPU 利用率**子部分。

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”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”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 利用率会不断变化。

监控受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。

注释 “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) 部分提供特定于设备的数据传输状态。

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，您可以查看特定设备的连接状态问题。有关设备上每项服务的状态的详细信息，请点击设备名称以查看设备的“数据传输状态”(Data Transfer Status) 页面。

“数据传输状态：*Appliance_Name*”(Data Transfer Status: Appliance_Name) 页面显示每项监控服务发生最后一次数据传输的时间。

邮件安全设备的数据传输状态可以是下列值之一：

- **未启用**：邮件安全设备上未启用监控服务。
- **从未连接**：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**：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**：已在邮件安全设备和安全管理设备之间建立连接，并且数据已成功传输。
- **文件传输失败**：已在邮件安全设备和安全管理设备之间建立连接，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**：未针对网络安全设备启用集中配置管理器。
- **从未连接**：为网络安全设备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**：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**：已在网络安全设备和安全管理设备之间建立连接，并且数据已成功传输。
- **配置推送失败**：安全管理设备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是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，但是状态未变成“已连接并已传输数据”(Connected and transferred data)，则您可能需要更改设备配置以启用数据传输。

查看受管设备的配置状态

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) 部分列出您已添加的设备。复选标记表示已启用的服务，“已建立连接？”(Connection Established?) 列显示是否已正确配置文件传输访问权限。

相关主题

- 指定处理所放行邮件的备用设备，第 174 页
- 关于添加受管设备，第 14 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，请参阅查看各台网络安全设备的状态，第 211 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 221 页
- 监控网络安全报告数据可用性 ，第 221 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 > 报告 > 报告数据可用性**页面。

在**报告数据可用性**页面中，您可以查看在指定的时间段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内收到的数据的完整度。

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。

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>报告>数据可用性**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。

注释 在“Web 报告数据可用性”(Web Reporting Data Availability) 窗口中，仅当“Web 报告”(Web Reporting) 和“邮件报告”(Email Reporting) 均被禁用时，“Web 报告”(Web Reporting) 才会显示为已禁用。

所有数据资源利用率和网络流量问题所在均会在该页面上显示。通过点击其中一个列出的网络安全设备链接，您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。

如果在计划报告内为 URL 类别使用“数据可用性”(Data Availability)，并且在任意设备之间存在着数据差异，则会在页面底部显示以下信息：“Some data in this time range was unavailable”。如果没有数据差异，则不会显示任何内容。

有关网络安全设备上的“数据可用性”页面的详细信息，请参阅“数据可用性”页面，第 116 页。

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。

监控受管设备的容量

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。

查看容量	请参阅
托管网络安全设备	系统容量页面，第 114 页
托管邮件安全设备	系统容量页面，第 69 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。

在硬件故障期间更换托管设备

如果由于硬件故障或其他原因必须更换托管设备，则被替换的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。

更换托管设备后，将新设备添加到 SMA 上的主机列表中，并将其连接到新设备。如果 IP 地址保持不变，请将旧主机条目上的 IP 地址更改为非现有值。

第 11 章

与 LDAP 集成

本章包含以下部分：

概述

如果您在公司 LDAP 目录（例如，Microsoft Active Directory、SunONE Directory Server 或 OpenLDAP 目录）中维护最终用户密码和邮件别名，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。

  当用户登录到垃圾邮件隔离区的网络 UI 时，LDAP 服务器会验证登录名和密码，AsyncOS 会检索相应邮件别名的列表。发送到用户的任何一个邮件别名的被隔离邮件可以出现在垃圾邮件隔离区中，只要设备不重写这些邮件即可。

  请参阅将 LDAP 配置为与垃圾邮件隔离区配合使用，第 223 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 236 页。

将 LDAP 配置为与垃圾邮件隔离区配合使用

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：

步骤 1 **配置 LDAP 服务器配置文件**。

服务器配置文件包含使 AsyncOS 能够连接到 LDAP 服务器的信息，例如：

- 服务器名称和端口
- 基本 DN
- 用于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 224 页。

在创建 LDAP 服务器配置文件时，您可以配置 AsyncOS 以连接到多台 LDAP 服务器。有关详细信息，请参阅将 AsyncOS 配置为与多个 LDAP 服务器配合使用 ， 第 233 页。

步骤 2 **配置 LDAP 查询**。

您可以使用为 LDAP 服务器配置文件生成的默认垃圾邮件隔离区，或自行创建针对您的特定 LDAP 实施和架构量身定制的查询。然后，您可以指定垃圾邮件通知的活动查询和最终用户对隔离区的访问权限。

有关查询的信息，请参阅配置 LDAP 查询 ， 第 226 页。

步骤 3 **为垃圾邮件隔离区启用 LDAP 最终用户访问权限和垃圾邮件通知**。

启用 LDAP 最终用户对垃圾邮件隔离区的访问权限，以使最终用户可以查看和管理其隔离区中的邮件。您还可以为垃圾邮件通知启用别名合并，以防止用户接收多个通知。

有关详细信息，请参阅设置集中垃圾邮件隔离区 ， 第 144 页。

创建 LDAP 服务器配置文件

配置 AsyncOS 以使用 LDAP 目录时，您需要创建 LDAP 服务器配置文件来存储有关 LDAP 服务器的信息。

步骤 1 依次选择**管理设备 > 系统管理 > 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。

您可以输入多个主机名，以为故障切换或负载均衡配置LDAP服务器。使用逗号分隔多个条目。有关详细信息，请参阅将 AsyncOS 配置为与多个 LDAP 服务器配合使用 ， 第 233 页。

步骤 5 选择身份验证方法。您可以使用匿名身份验证或指定用户名密码。

注释 您需要配置 LDAP 身份验证，以在报告上查看客户端用户 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 地址指代用户。选择**使用密码**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，可以让它访问多服务器环境中的全局目录。

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该密码的条目的完整 DN。例如，邮件地址为 joe@example.com 的用户是营销部门的用户。此用户的条目可能与以下条目相同：

```
uid=joe, ou=marketing, dc=example dc=com
```

步骤 9 在“高级”(Advanced) 下，选择是否在与 LDAP 服务器通信时使用 SSL。

步骤 10 输入缓存生存时间。此值表示保留缓存的时间长度。

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。

如果您为进行负载均衡配置 LDAP 服务器配置文件，这些连接会分布在已列出的 LDAP 服务器上。例如，如果配置 10 个并发连接，并且在 3 个服务器上均衡连接负载，AsyncOS 将为每个服务器创建 10 个链接，总共 30 个连接。有关详细信息，请参阅负载均衡，第 235 页。

注释 最大并发连接数包括用于 LDAP 查询的 LDAP 连接。但是，如果您为垃圾邮件隔离区启用 LDAP 身份验证，设备会为终端用户隔离区额外分配 20 个连接，连接总数达到 30 个。

步骤 13 通过点击“测试服务器”按钮测试服务器连接。如果您指定了多个 LDAP 服务器，则这些服务器都会进行测试。测试结果显示在“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 226 页。

步骤 14 通过选中复选框并填写字段来创建垃圾邮件隔离区查询。

您可以配置隔离区终端用户身份验证查询，以便在用户登录到终端用户隔离区时验证用户。您可以配置别名合并查询，以便终端用户无需为每个邮件别名接收隔离区通知。要使用这些查询，请选中“指定为活动查询”(Designate as the active query) 复选框。有关详细信息，请参阅配置 LDAP 查询，第 226 页。

步骤 15 通过点击“测试查询”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”。测试结果显示在“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)**。

注释 如果已将 LDAP 服务器配置为允许绑定空密码，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。

对于 Windows 2000，Active Directory 服务器配置不允许通过 TLS 进行身份验证。这是一个已知的 Active Directory 问题。Active Directory 和 Windows 2003 的 TLS 身份验证确实有效。

注释 虽然服务器配置的数量不受限制，但是您只能为每台服务器配置一个终端用户身份验证查询和一个别名合并查询。

测试 LDAP 服务器

使用“添加/编辑 LDAP 服务器配置文件”页面上的“测试服务器”按钮（或 CLI 中 ldapconfig 命令的 test 子命令）测试与 LDAP 服务器的连接。AsyncOS 随即显示一条消息，说明到服务器端口的连接是成功还是失败。如果配置了多个 LDAP 服务器，AsyncOS 会测试每个服务器，并显示各个结果。

配置 LDAP 查询

以下部分提供各类垃圾邮件隔离区查询的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终端用户身份验证查询，第 227 页。
- **垃圾邮件隔离区别名合并查询**。有关详细信息，请参阅垃圾邮件隔离区别名整合查询，第 228 页。

要让隔离区将 LDAP 查询用于最终用户访问权限或垃圾邮件通知，请选中“指定为活动查询”(Designate as the active query) 复选框。您可以指定一个最终用户身份验证查询以控制隔离区访问权限，并且可以为垃圾邮件通知指定一个别名合并查询。任何现有的活动查询都会被禁用。在安全管理设备上，选择**管理设备 > 系统管理 > LDAP** 页面，有效查询旁边会显示一个星号 (*)。

您还可以将基于域的查询或链式查询指定为活动的最终用户访问权限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 230 页和链查询，第 232 页。

注释 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，第 226 页
- 令牌，第 226 页

LDAP 查询语法

允许 LDAP 路径中使用空格，而且不需要使用引号。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，且必须与您的 LDAP 实施相匹配才可以正常工作。例如，在提示符中输入 **mailLocalAddress** 执行的查询不同于输入 **maillocaladdress** 执行的查询。

令牌

您可以在 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

注释 {f} 令牌仅在接受查询中有效。

例如，您可以使用以下查询接受 Active Directory LDAP 服务器的邮件：
(|(mail={a})(proxyAddresses=smtp:{a}))

注释 在侦听程序上启用 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）测试您构建的所有查询并确保返回预期的结果。有关详细信息，请参阅 测试 LDAP 查询，第 230 页。

垃圾邮件隔离区终端用户身份验证查询

最终用户身份验证查询会在用户登录到垃圾邮件隔离区时验证用户。令牌 {u} 指定用户（它表示用户的登录名）。令牌 {a} 指定用户的邮件地址。LDAP 查询不会从邮件地址中删除“SMTP:”；AsyncOS 会删除地址的该部分。

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 **mail**。您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。

注释 如果您希望用户使用其完整的邮件地址登录，请为查询字符串使用 (mail=smtp:{a})。

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。此示例为 Active Directory 服务器使用密码进行的身份验证，为 Active Directory 服务器的最终用户身份验证使用默认查询字符串，并使用邮件和 proxyAddresses 邮件属性。

表 *34: 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	使用密码（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
基本 DN	[空白]
连接协议	[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

本部分介绍 OpenLDAP 服务器和最终用户身份验证查询设置示例。此示例为 OpenLDAP 服务器使用匿名身份验证，为 OpenLDAP 服务器的最终用户身份验证使用默认查询字符串，并使用 mail 和 mailLocalAddress 邮件属性。

表 *35: 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
基本 DN	[空白]（有些旧方案将使用特定基本DN。）
连接协议	[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

如果您使用垃圾邮件通知，垃圾邮件隔离区别名合并查询会合并邮件别名，以便收件人无需为每个邮件别名接收隔离区通知。例如，收件人可能收到以下邮件地址的邮件：john@example.com、jsmith@example.com 和 john.smith@example.com。使用别名合并时，对于发送给所有用户别名的邮件，收件人将在选定的主要邮件地址收到一条垃圾邮件通知。

要将邮件合并到主要邮件地址，请创建一个查询，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要邮件地址的属性。

对于 Active Directory 服务器，默认查询字符串（可能与您的部署不同或相同）是 (|(proxyAddresses={a})(proxyAddresses=smtp:{a}))，默认邮件属性是 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。如果您输入多个邮件属性，思科建议输入一个使用单个值的唯一属性（例如 mail）作为第一个邮件属性，而不是输入一个具有多个可以更改的值的属性，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 229 页
- OpenLDAP 别名整合设置示例，第 229 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 *36: LDAP* 服务器和垃圾邮件隔离区别名合并设置示例：*Active Directory*

身份验证方法	匿名
服务器类型	Active Directory
端口	3268
基本 DN	[空白]
连接协议	使用 SSL
查询字符串	(|(mail={a})(mail=smtp:{a}))
邮件属性	mail

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 *37: 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

身份验证方法	匿名
端口	389
基本 DN	[空白]（有些旧方案将使用特定基本DN。）
连接协议	使用 SSL
查询字符串	(mail={a}))
邮件属性	mail

测试 LDAP 查询

使用“添加/编辑 LDAP 服务器配置文件”页面上的“测试查询”按钮（或 CLI 中的 ldaptest 命令）测试您的查询。AsyncOS 显示有关查询连接测试的每个阶段的详细信息。例如，第一阶段 SMTP 授权是已成功还是已失败，BIND 匹配返回的是 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，且必须与您的 LDAP 实施相匹配才可以正常工作。例如，为邮件属性输入 mailLocalAddress 会执行与输入 maillocaladdress 不同的查询。

要测试查询，您必须输入测试参数，然后点击“运行测试”。结果显示在“测试连接”(Test Connection) 字段中。如果终端用户身份验证查询成功，会显示“成功：操作：匹配阳性”(Success: Action: match positive) 结果。对于别名合并查询，会显示“成功：操作：别名合并”(Success: Action: alias consolidation)，以及合并的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

基于域的查询是由类型分组且与域关联的 LDAP 查询。如果不同的 LDAP 服务器与不同的域关联，您可能希望使用基于域的查询，但是您需要为最终用户隔离区访问权限查询您的所有LDAP服务器。例如，一家名为 Bigfish 的公司拥有域 Bigfish.com、Redfish.com 和 Bluefish.com，并且该公司为与每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，根据所有三个域的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权限或通知，请完成以下步骤：

步骤 1 为您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，配置您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 224 页。

步骤 2 创建基于域的查询。在创建基于域的查询时，您从每个服务器配置文件中选择查询，并将基于域的查询指定为垃圾邮件隔离区的活动查询。有关创建查询的详细信息，请参阅创建基于域的查询，第 231 页。

步骤 3 为垃圾邮件隔离区启用最终用户访问权限或垃圾邮件通知。有关详细信息，请参阅设置终端用户通过网络浏览器访问垃圾邮件隔离区的权限，第 158 页。

创建基于域的查询

步骤 1 依次选择**管理设备 > 系统管理 > 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。

注释 在创建基于域的查询时，您指定一种查询类型。在您选择查询类型后，查询字段下拉列表包含来自LDAP服务器配置文件的相应查询。

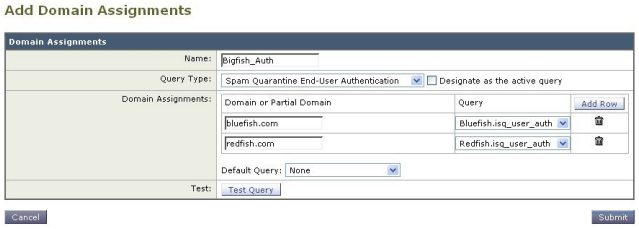
步骤 5 在“域分配”(Domain Assignments) 字段中，输入域。

步骤 6 选择与域关联的查询。

步骤 7 添加行，并为基于域的查询中的每个域选择查询。

步骤 8 输入在所有其他查询失败时要运行的默认查询。如果您不想输入默认查询，请选择**无 (None)**。

图 *5*: 基于域的查询示例



步骤 9 通过点击“测试查询”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，来测试查询。结果会显示在“连接状态”(Connection Status) 字段中。

步骤 10 如果您希望垃圾邮件隔离区使用基于域的查询，请选中**指定为活动查询**复选框。

注释 基于域的查询成为所指定查询类型的活动 LDAP 查询。例如，如果基于域的查询用于终端用户身份验证，它将成为垃圾邮件隔离区的活动终端用户身份验证查询。

步骤 11 点击**提交**，然后点击**确认**以确认您所做的更改。

注释 要在命令行界面上执行相同的配置，请在命令行提示符处键入 `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 运行系列中的每个查询（“链中的每个查询”），直到 LDAP 服务器返回肯定响应或者最终查询返回否定响应或失败。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，链式查询会非常有用。例如，组织中的各个部门可能使用不同类型的 LDAP 目录。当销售部门使用 Active Directory 时，IT 部门可能使用 OpenLDAP。要确保查询针对两种类型的 LDAP 目录运行，您可以使用链式查询。

要使用链式查询控制垃圾邮件隔离区的终端用户访问权限或通知，请完成以下步骤：

步骤 1 为您要在链式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，请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 224 页。

步骤 2 创建链查询并将其指定为垃圾邮件隔离区的活动查询。有关详细信息，请参阅创建链查询 ， 第 232 页。

步骤 3 为垃圾邮件隔离区启用 LDAP 终端用户访问权限和垃圾邮件通知。有关垃圾邮件隔离区的详细信息，请参阅设置集中垃圾邮件隔离区 ， 第 144 页。

创建链查询

提示 您还可以在 CLI 中使用 ldapconfig 命令的 advanced 子命令。

步骤 1 选择**管理设备 > 系统管理 > LDAP > LDAP 服务器**。

步骤 2 从“LDAP 服务器配置文件”(LDAP Server Profiles) 页面，点击**高级 (Advanced)**。

步骤 3 点击**添加链式查询 (Add Chained Query)**。

步骤 4 为链式查询输入名称。

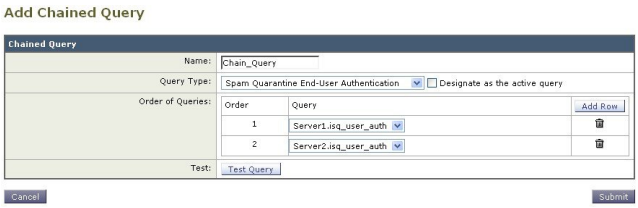
步骤 5 选择查询类型。

当您创建链式查询时，其所有组成查询具有相同的查询类型。在您选择查询类型后，查询字段下拉列表显示来自 LDAP 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 *6:* 链式查询示例



步骤 7 通过点击“测试查询”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，来测试查询。结果随即会显示在“连接状态”(Connection Status) 字段中。

步骤 8 如果您希望垃圾邮件隔离区使用域查询，请选中**指定为活动查询 (Designate as the active query)** 复选框。

注释 链式查询成为所指定查询类型的活动 LDAP 查询。例如，如果链式查询用于终端用户身份验证，它将成为垃圾邮件隔离区的活动终端用户身份验证查询。

步骤 9 提交并确认更改。

注释 要在命令行界面上执行相同的配置，请在命令行提示符处键入 `ldapconfig` 命令的 `advanced` 子命令。

将 AsyncOS 配置为与多个 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。

您可以在“管理设备”>“系统管理”>“LDAP”页面上或通过使用 CLIldapconfig 命令配置冗余的 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）测试到 LDAP 服务器的连接。如果使用多个 LDAP 服务器，AsyncOS 会测试每个服务器，并显示每个服务器的每个结果。AsyncOS 还将测试每个 LDAP 服务器上的查询，并显示每个结果。

故障切换

要确保 LDAP 服务器可用于解析查询，您可配置用于故障切换的 LDAP 配置文件。如果与 LDAP 服务器的连接失败，或者查询返回适合这样做的错误，设备会尝试查询列表中指定的下一 LDAP 服务器。

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，或者查询返回错误，设备会尝试连接到列表中的下一台 LDAP 服务器。默认情况下，设备始终尝试连接到列表中的第一台服务器，而且，会尝试按照列出的顺序连接到后续每台服务器。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。

注释 只有查询指定 LDAP 服务器的尝试才会进行故障转移。尝试查询与未故障转移的指定的 LDAP 服务器关联的建议或后续服务器。

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。

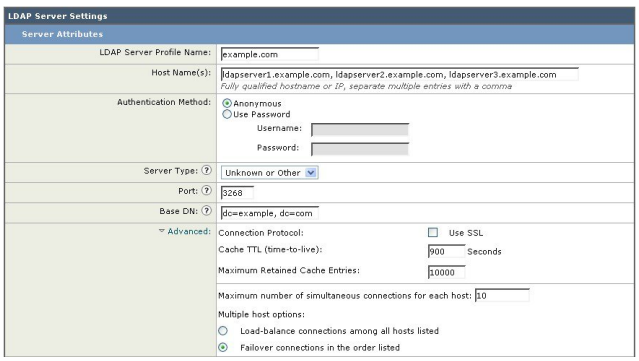
为 LDAP 故障切换配置思科内容安全设备

步骤 1 依次选择**管理设备 > 系统管理 > LDAP**。

步骤 2 选择您要编辑的 LDAP 服务器配置文件。

在以下示例中，LDAP 服务器名称为 example.com。

图 *7: LDAP* 故障切换配置示例



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**按列出的顺序对连接进行故障切换 (Failover connections in the order listed)** 旁边的单选按钮。

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。设备根据您配置的最大连接数确定要建立的并发连接数。

如果列出的其中一个 LDAP 服务器不响应，则设备会在其余 LDAP 服务器之间分配连接负载。

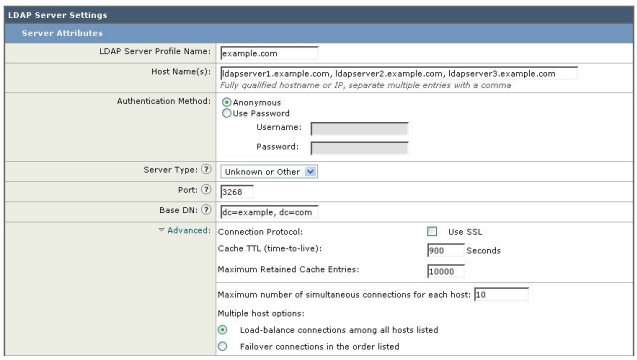
为负载均衡配置思科内容安全设备

步骤 1 依次选择**管理设备 > 系统管理 > LDAP**。

步骤 2 选择您要编辑的 LDAP 服务器配置文件

在以下示例中，LDAP 服务器名称为 example.com。

图 *8:* 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**在列出的所有主机之间均衡分配连接的负载 (Load-balance connections among all hosts listed)**。

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。

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 224 页。

步骤 2 **创建查询以查找用户账户**。在 LDAP 服务器配置文件的“外部身份验证查询”(External Authentication Queries) 部分，创建一个查询以在 LDAP 目录中搜索用户账户。请参阅用于验证管理用户的用户账户查询，第 236 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是某个目录组的成员，并创建一个单独的查询以查找组的所有成员。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 237 页以及邮件安全设备文档或在线帮助。

注释 使用页面上“外部身份验证查询”部分中的**测试查询**按钮（或 ldaptest 命令）验证查询是否返回了预期结果。如需相关信息，请参阅测试 LDAP 查询，第 230 页。

步骤 4 **设置外部身份验证以使用 LDAP 服务器**。使设备能够使用 LDAP 服务器进行用户身份验证，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外部身份验证，第 238 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账户查询

要对外部用户进行身份验证，AsyncOS 会使用查询在 LDAP 目录中搜索用户记录以及包含用户全名的属性。根据您选择的服务器类型，AsyncOS 输入默认查询和默认属性。如果您的 LDAP 用户记录中有在 RFC 2307 中定义的属性（**shadowLastChange**、**shadowMax** 和 **shadowExpire**），您可以选择让设备拒绝账户过期的用户。用户记录所驻留的域层需要基本 DN。

下表显示了 AsyncOS 在 Active Directory 服务器上搜索用户账户时使用的默认查询字符串和完整用户名属性。

表 38: Active Directory 服务器的默认查询字符串

服务器类型	**Active Directory**
基本 DN	[空白]（您需要使用特定的基本 DN 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

下表显示了 AsyncOS 在 OpenLDAP 服务器上搜索用户账户时使用的默认查询字符串和完整用户名属性。

表 *39: OpenLDAP* 服务器的默认查询字符串

服务器类型	**OpenLDAP**
基本 DN	[空白]（您需要使用特定的基本 DN 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

您可以将 LDAP 组与用户角色关联以便访问设备。

AsyncOS 创建还使用一个查询以确定用户是否是某个目录组的成员，并使用一个单独的查询以查找组的所有成员。目录组成员身份可以确定用户在系统中的权限。在 GUI 中的“管理设备”>“系统管理”>“用户”页面上（或 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。用户角色可以决定用户在系统中的权限，对于经过外部身份验证的用户，将角色分配给目录组而不是单个用户。例如，您可以为“IT”目录组中的用户分配“管理员”(Administrator) 角色，为“支持”(Support) 目录组中的用户分配“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，则 AsyncOS 会授予该用户访问最具限制性角色的权限。例如，如果用户属于具有“操作员”(Operator) 权限的组和具有“服务中心用户”(Help Desk User) 权限的组，则 AsyncOS 会授予该“服务中心用户”(Help Desk User) 用户角色的权限。

在配置 LDAP 配置文件以查询组成员身份时，为可以找到组记录的目录级别、保存组成员用户名的属性以及包含组名的属性输入基本 DN。根据您为 LDAP 服务器配置文件选择的服务器类型，AsyncOS 为用户名和组名属性输入默认值并输入默认查询字符串。

注释 对于 Active Directory 服务器，用于确定用户是否是组成员的默认查询字符串是 (&(objectClass=group)(member={u}))。但是，如果您的 LDAP 架构在“memberof”列表中使用可区别名称而不是用户名，您可以使用 {dn} 而不是 {u}。

下表 显示 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 *40: Active Directory* 服务器的默认查询字符串和属性

查询字符串	**Active Directory**
基本 DN	[空白]（您需要使用特定的基本 DN 查找组记录。）
用于确定用户是否为组成员的查询字符串	(&(objectClass=group)(member={u})) **注释** 如果您的 LDAP 架构在“memberof”列表中使用可区别名称而不是用户名，您可以将 {u} 替换为 {dn}。

查询字符串	Active Directory
用于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	member
包含组名的属性	cn

下表 显示 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 *41: OpenLDAP* 服务器的默认查询字符串和属性

查询字符串	OpenLDAP
基本 DN	[空白]（您需要使用特定的基本DN查找组记录。）
用于确定用户是否为组成员的查询字符串	(&(objectClass=posixGroup)(memberUid={u}))
用于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

启用管理用户外部身份验证

在创建 LDAP 服务器配置文件和查询之后，您可以使用 LDAP 启用外部身份验证。

步骤 1 依次选择**管理设备 > 系统管理 > 用户**页面。
步骤 2 点击**启用**。
步骤 3 选中**启用外部身份验证 (Enable External Authentication)** 复选框。
步骤 4 选择 **LDAP** 作为身份验证类型。
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 （可选）点击**添加行**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。

第 12 章

配置 SMTP 路由

本章包含以下部分：

SMTP 路由概述

本章介绍了影响通过思科内容安全管理设备传递的邮件的路由和传送的各项功能，并说明了“SMTP 路由”页面和 **smtproutes** 命令的用途。

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”地址中带有 @example.com 的所有邮件都发送至 groupware.example.com。系统先在 groupware.example.com 中执行“MX”查找，然后在主机中执行“A”查找，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 241 页。）

此功能还允许使用主机“通配”。如果您指定不完整域，例如 example.com，则以 example.com 结尾的任何域均会与该条目匹配。例如，fred@foo.example.com 和 wilma@bar.example.com 均与该映射匹配。

如果未在 SMTP 路由表中找到主机，则使用 DNS 执行 MX 查找。系统不会比照 SMTP 表重新检查结果。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，则不会导致邮件循环。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。

每次传送邮件时，从上到下阅读 SMTP 路由表。选出与映射最匹配的条目例如，如果“SMTP 路由”(SMTP Routes) 表中存在 host1.example.com 和 example.com 的映射，则将使用 host1.example.com

的条目，因为它是最具体的条目 - 即使它出现在 example.com 条目之后。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、邮件传送和邮件拆分

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：工作原理相似，但如果将一封邮件发送到 10 个不同的域中的 10 位收件人，则 AsyncOS 将打开与 10 个 MTA 的 10 个连接，并向每个 MTA 传送一封邮件。

拆分：如果一封传入邮件有 10 位收件人并且每位收件人分别属于单独的传入策略组（10 个组），则邮件会进行拆分，即使这 10 位收件人均位于同一台 Exchange 服务器上也是如此。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。

路由本地域的邮件

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
- 也可发送到定义的收件人的支持请求邮件

最后两种邮件使用 SMTP 路由来传送到目标。

邮件安全设备将发往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。此功能类似于 sendmail **mailertable** 功能。(“SMTP 路由”页面和 **smtproutes** 命令扩展了 AsyncOS 2.0“域重定向”功能。）

注释 如果您已在 GUI 中完成“系统设置向导”(System Setup Wizard) 并提交了更改，则您已在当时在设备上为每个 RAT 条目定义了第一批 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。您不能删除默认 SMTP 路由；您只能清除为其输入的任何值。

使用**管理设备 (Management Appliance) > 网络 (Network) > SMTP 路由 (SMTP Routes)** 页面或 **smtproutes** 命令配置默认的 SMTP 路由。

管理 SMTP 路由

定义 SMTP 路由

邮件安全设备将发往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。此功能类似于 sendmail mailertable 功能。（“SMTP 路由”[SMTP Routes] 页面和 **smtproutes** 命令扩展了 AsyncOS 2.0“域重定向”[Domain Redirect] 功能。）：

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。当您创建新的路由时，首先指定要为其创建永久路由的域或不完整域，然后，指定目标主机。目标主机可以输入为完全限定的主机名或 IP 地址。您还可以指定 /dev/null 的特殊目标主机，以丢弃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。

如果一台或多台主机没有响应，邮件将传送到其中一台可访问的主机。如果所有已配置的主机均未响应，邮件将排队等候该主机（不使用 MX 记录进行故障切换）。

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

步骤 1 依次选择**管理设备 > 网络 > SMTP 路由**。

步骤 2 点击**添加路由 (Add Route)**。

步骤 3 输入接收域和目标主机。您可以通过点击**添加行 (Add Row)** 并在新建行中输入下一个目标主机来添加多台目标主机。

步骤 4 可以通过向目标主机添加“:<端口号>”来指定端口号：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，您可以通过导出和导入文件来修改 SMTP 路由映射。

步骤 1 在“SMTP 路由”(SMTP Routes) 页面上点击**导出 SMTP 路由 (Export SMTP Routes)**。

步骤 2 输入文件的名称，然后点击**提交**。

导入 SMTP 路由

与主机访问表 (HAT) 和收件人访问表 (RAT) 类似，您可以通过导出和导入文件来修改 SMTP 路由映射。

步骤 1 在“SMTP 路由”(SMTP Routes) 页面上点击**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**提交**。您会收到导入将替换所有现有 SMTP 路由的警告。文本文件中的所有 SMTP 路由均会导入。

步骤 4 点击**导入 (Import)**。

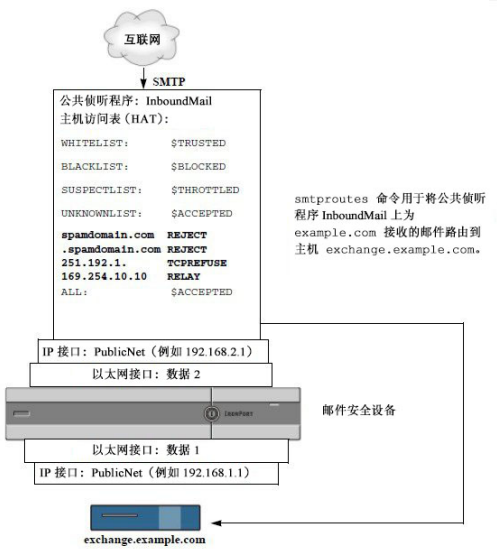
您可以在文件中加入“注释”。以“#”字符开头的行会被视作注释并会被 AsyncOS 忽略。例如：

this is a comment, but the next line is not

所有:

目前，我们的邮件网关配置如下所示：

图 *9:* 邮件网关配置



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。当您需要将子域的邮件路由到某台特定主机时，此功能非常有用。例如，如果将发往 example.com 的邮件发送到公司的 Exchange 服务器，您可能会看到类似于以下 SMTP 路由的地址：

```
example.com exchange.example.com
```

但对于发送到不同子域 (foo.example.com) 的邮件，请添加如下所示的 SMTP 路由：

```
.example.com USEDNS
```

第 13 章

分配管理任务

本章包含以下部分：

关于分配管理任务

您可以根据自己分配给其他人员的用户账户的用户角色，将思科内容安全管理设备上的管理任务分配给其他人员。

要进行设置以分配管理任务，您应该确定预定义的用户角色是否满足您的需求，创建任何需要的自定义用户角色，并设置设备以在安全设备上对管理用户进行本地身份验证，并且/或者使用您自己的集中 LDAP 或 RADIUS 系统进行外部身份验证。

此外，您可以对访问设备和设备上的某些信息指定额外的控制。

分配用户角色

要获得隔离区访问权限，需要进行其他配置。请参阅对隔离区的访问权限 ， 第 254 页。

预定义用户角色

除非另有说明，否则您可以为每个用户分配具有下表所述权限的预定义用户角色，或者为用户分配自定义用户角色。

表 *42*: 用户角色的说明

用户角色名称	说明	**Web** 报告/计划报告功能
admin	**admin** 用户是系统的默认用户账户，并且拥有完全管理权限。为方便起见，此处列出了管理员用户账户，但此账户无法通过用户角色进行分配，也无法编辑或删除，只能更改密码。 只有**管理员**用户可以发出 **resetconfig** 和 **revert** 命令。	是/是
管理员 (Administrator)	具有“管理员 (Administrator)”角色的用户账户具有系统的所有配置设置的完全访问权限。	是/是
操作员 (Operator)	具有“操作员”(Operator) 角色的用户账户限制执行以下操作： • 创建或编辑用户账户 • 升级设备 • 发出 `resetconfig` 命令 • 运行系统设置向导 • 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以外的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 (Technician)	具有“技术人员”(Technician) 角色的用户账户可以执行系统管理活动，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。	访问网络和邮件选项卡下的“系统容量”(System Capacity) 报告

用户角色名称	说明	Web 报告/计划报告功能
只读操作员 (Read-Only Operator)	具有“只读操作员”(Read-Only Operator) 角色的用户账户才有查看配置信息的访问权限。具有“只读操作员”(Read-Only Operator) 角色的用户可以进行和提交大多数更改以了解如何配置功能，但是不能够确认更改或进行任何不需要确认的更改。如果启用了访问权限，具有此角色的用户可以管理隔离区中的邮件。 具有此角色的用户不能访问以下内容： • 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 (Guest)	具有“访客”(Guest) 角色的用户账户可以查看状态信息（包括报告和网络跟踪），如果启用了访问权限，还可以管理隔离区中的邮件。具有“访客”(Guest) 角色的用户不能访问邮件跟踪。	是/否
网络管理员 (Web Administrator)	具有“网络管理员”角色的用户账户可以访问**网络**选项卡下的所有配置设置。	是/是
网络策略管理员 (Web Policy Administrator)	具有“网络策略管理员”(Web Policy Administrator) 角色的用户账户可以访问“网络”(Web) 选项卡下的所有配置设置。“网络策略管理员”(Web Policy Administrator) 可以配置身份、访问策略、解密策略、路由策略、代理绕行、自定义 URL 类别和时间范围。“网络策略管理员”(Web Policy Administrator) 无法发布配置。	否/否
URL 过滤管理员 (URL Filtering Administrator)	具有“URL 过滤管理员”(URL Filtering Administrator) 角色的用户账户只能为网络安全配置过滤 URL。	否/否
邮件管理员 (Email Administrator)	具有“邮件管理员”(Email Administrator) 角色的用户账户只能访问“邮件”(Email) 菜单内的所有配置设置，包括隔离区。	否/否

用户角色名称	说明	Web 报告/计划报告功能
服务中心用户 (Help Desk User)	具有“服务中心用户”(Help Desk User) 角色的用户账户限制执行以下操作： • 邮件跟踪 • 管理隔离区中用户账户的邮件 具有此角色的用户不能访问系统的其余部分，包括CLI。在为用户分配此角色后，您还必须配置隔离区以允许此用户访问。	否/否
自定义角色 (Custom Roles)	被分配自定义用户角色的用户账户只能查看和配置策略、功能或者专门委派给该角色的特定策略或功能实例。 您可以从“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，您必须先将权限分配给此自定义用户角色，然后才能使用该角色。要分配权限，请转至**管理设备 > 系统管理 > 用户角色**，然后点击用户名。 **注释** 分配给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248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。

您为其分配自定义用户角色的用户可以管理设备、功能或最终用户子集的策略或访问报告。例如，您可能允许网络服务的一个委派管理员管理组织在某个不同国家/地区的分支机构的策略，该分支机构的可接受使用策略可能与组织总部的可接受使用策略不同。您通过创建自定义用户角色并将访问权限分配给这些角色来委派管理职责。您确定委派的管理员可以查看和编辑哪些策略、功能、报告、自定义 URL 类别等。

有关详情，请参阅：

- 关于自定义邮件用户角色 ，第 249 页
- 关于自定义网络用户角色 ，第 252 页
- 删除自定义用户角色 ，第 254 页

关于自定义邮件用户角色

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（可根据需要按报告组限制）
- DLP 报告（可根据需要按报告组限制）
- 邮件跟踪
- 隔离区

有关以上各项的详细信息，请参阅此部分之后的内容。此外，所有被授予上述任一权限的用户均可以在“管理设备”(Management Appliance) >“集中服务”(Centralized Services) 菜单下查看系统状态。分配了自定义邮件用户角色的用户无法访问 CLI。

注释 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，第 33 页一章。

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
- 传出邮件发件人
- 内部用户
- DLP 事件 (DLP Incidents)
- 内容过滤器
- 病毒类型
- TLS 连接
- 病毒爆发过滤器 (Outbreak Filters)
- 系统容量 (System Capacity)

- 正在报告数据可用性 (Reporting Data Availability)
- 计划的报告
- 存档的报告 (Archived Reports)

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
- 传出邮件发件人
- 内部用户
- 内容过滤器
- 病毒类型
- 病毒爆发过滤器 (Outbreak Filters)
- 正在报告数据可用性 (Reporting Data Availability)
- 存档的报告 (Archived Reports)

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 (Reporting Data Availability)
- 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，请参阅控制对“邮件跟踪”中敏感信息的访问权限 ，第 268 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 ，第 133 页。

自定义用户角色的隔离区访问权限

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 254 页。

创建自定义邮件用户角色

您可以创建自定义邮件用户角色以访问邮件报告、邮件跟踪和隔离区。

有关以上每个选项允许的访问权限的说明，请参阅关于自定义邮件用户角色 ，第 249 页及其子部分。

注释 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。

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，您可以通过复制现有的邮件用户角色创建新角色：点击适用的表行中的“复制”(Duplicate) 图标，然后修改生成的副本。

步骤 3 为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**以返回到“用户角色”页面，其中列出了新的用户角色。

步骤 6 如果您按报告组限制了访问权限，请点击用户角色的“邮件报告”(Email Reporting) 列中的**未选择组 (no groups selected)** 链接，然后选择至少一个报告组。

步骤 7 确认您的更改。

步骤 8 如果您向此角色授予了对隔离区的访问权限，请为此角色启用访问权限：

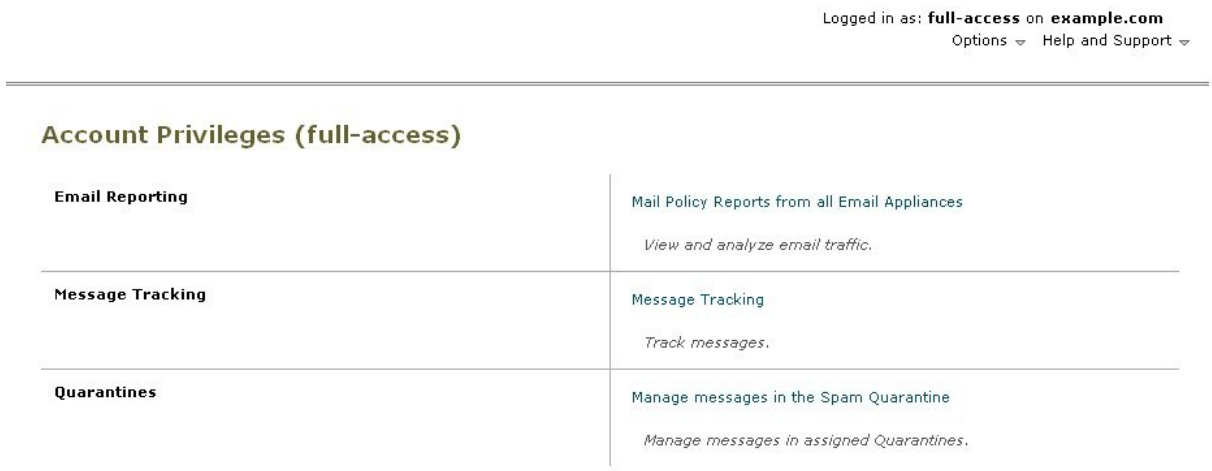
请参阅：

- 配置对垃圾邮件隔离区的管理用户访问权限 ，第 148 页
- 配置策略、病毒和爆发隔离区 ，第 178 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。该用户可以通过选择“选项”(Options) 菜单中的“账户权限”(Account Privileges) 随时返回到该主页。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 *10:* 分配了自定义邮件用户角色的授权管理员的“账户权限 *(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 > 主配置 > 自定义 URL 类别**页，可以查看允许您管理和发布的 URL 类别与策略。此外，您可以转到**网络 (Web) > 实用程序 (Utilities) > 立即发布配置 (Publish Configuration Now)** 页面并查看可能的配置。

注释 请注意，如果您创建具有“发布权限”(Publish Privilege) 功能的自定义角色，则用户在登录时将不具有任何可用的菜单。他们不具有发布菜单，并且将登录在一个不可编辑的登录屏幕上，因为 URL 和策略选项卡不具有任何功能。实际上，您具有无法发布或管理任何类别或策略的用户。此问题的解决办法：如果您希望用户能够发布，但无法管理任何类别或策略，则**必须**创建不用于任何策略的自定义类别，并使该用户能够管理该自定义类别和发布。这样，如果用户从该类别中添加或删除 URL，不会产生任何影响。

您可以通过创建和编辑自定义用户角色委派网络管理。

- 创建自定义网络用户角色，第 253 页
- 编辑自定义网络用户角色，第 253 页
- 删除自定义用户角色 ，第 254 页

创建自定义网络用户角色

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，您可以通过复制现有的网络用户角色创建新角色：点击适用的表行中的“复制”(Duplicate) 图标，然后修改生成的副本。

步骤 3 输入用户角色的唯一名称（例如“canadian-admins”）和说明。

注释 名称只能包含小写字母、数字和破折号。它不能以破折号开头。

步骤 4 选择您希望在默认情况下显示还是隐藏策略和自定义 URL 类别。

步骤 5 选择您希望开启还是关闭发布权限。

此权限允许用户发布该用户可以编辑其访问策略或 URL类别的任何主配置。

步骤 6 选择是要从新的（空的）设置开始还是复制现有的自定义用户角色。如果您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** 以返回到“用户角色”页面，其中列出新的用户角色。

注释 如果您在 Web 报告内启用了匿名功能，则有权访问 Web 报告的所有用户角色将在交互式报告页面中具有无法识别的用户名和角色。请参阅使用集中 Web 报告和跟踪，第 85 页一章中的计划 Web 报告 ，第 117 页部分。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。

如果您使用**网络 > 实用程序 > 安全服务显示 > 编辑安全服务显示**页面隐藏其中一个主配置，则“用户角色”页面还会隐藏相应的主配置列；但是，会保留已隐藏的主配置的权限设置。

编辑自定义网络用户角色

步骤 1 在“用户角色”(User Roles) 页面上，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：名称、说明以及策略和自定义 URL 类别的可视性。

步骤 3 点击**提交**。

要编辑自定义用户角色的权限，请执行以下操作：

导航到“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) 以显示主配置中配置的访问策略列表。在“包括”(Include) 列中，选中您要向用户授予编辑权限的策略的复选框。点击**提交**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“主配置”(Configuration Master) 上定义的自定义 URL 类别列表。在“包括”(Include) 列中，选中您要向用户授予编辑权限的自定义 URL 类别的复选框。点击**提交**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

某些角色可以访问 GUI 和 CLI：“管理员”(Administrator)、“操作员”(Operator)、“访客”(Guest)、“技术人员”(Technician) 和“只读操作员”(Read-Only Operator)。其他角色只能访问 GUI：“服务中心用户”(Help Desk User)、“邮件管理员”(Email Administrator)、“网络管理员”(Web Administrator)、“网络策略管理员”(Web Policy Administrator)、“URL 过滤管理员”(URL Filtering Administrator)（适用于网络安全）和自定义用户。

使用 LDAP

如果您使用 LDAP 目录对用户进行身份验证，您将目录组分配给用户角色而不是各个用户。为目录组分配用户角色时，该组中的每个用户都会收到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 261 页。

对隔离区的访问权限

您必须先启用该访问权限，然后用户才可以访问隔离区。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 148 页
- 关于向其他用户分配邮件处理任务 ， 第 181 页（适用于策略隔离区）和配置策略、病毒和爆发隔离区 ， 第 178 页
- 为自定义用户角色配置集中隔离区访问权限 ， 第 174 页。

“用户 (User)”页面

有关此部分的信息	请参阅
用户 重置密码按钮	关于分配管理任务 ， 第 245 页 管理本地定义的管理用户 ， 第 256 页 要求用户按要求更改密码 ， 第 260 页
本地用户账户与密码设置	设置密码和登录要求 ， 第 257 页

有关此部分的信息	请参阅
外部身份验证	外部用户身份验证 ， 第 261 页
DLP 跟踪权限	控制对“邮件跟踪”中敏感信息的访问权限 ， 第 268 页

关于对管理用户进行身份验证

您可以控制对设备的访问权限，方法是在设备上本地定义授权用户，和/或使用外部身份验证。

- 更改管理员用户的密码 ， 第 255 页
- 管理本地定义的管理用户 ， 第 256 页
- 外部用户身份验证 ， 第 261 页

更改管理员用户的密码

所有管理员级别的用户均可通过 GUI 或 CLI 更改“管理员”用户的密码。

要通过 GUI 更改密码，请执行以下操作：

- 依次选择**管理设备 > 系统管理 > 用户**页面，然后选择管理员用户。

要在 CLI 中更改管理员用户的密码，请使用 `password` 命令。为了安全起见，`password` 命令要求输入旧密码。

如果忘记了“管理员”用户账户的密码，请联系客户支持提供商重置密码。

注释 对密码所做的更改会立即生效，不要求确认更改。

过期后更改用户的密码

如果账户已过期，系统则会向您显示以下消息“您的密码已过期。请点击此处更改密码。”进行提示。

点击链接，然后输入登录详细信息以及过期的密码，转到“更改密码”页面。有关设置密码的详细信息，请参阅设置密码和登录要求 ， 第 257 页。

注释 对密码所做的更改会立即生效，不要求确认更改。

管理本地定义的管理用户

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。

注释 如果还启用了外部身份验证，请确保本地用户名与经过外部身份验证的用户名不相同。

对您可以在设备上使用的用户账户数量没有限制。

步骤 1 如果您将分配自定义用户角色，我们建议您首先定义这些角色。请参阅自定义用户角色 ， 第 248 页。

步骤 2 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 输入用户的唯一名称。不能输入系统保留的词（例如，“operator”和“root”）。

如果您还使用外部身份验证，则用户名不能与经过外部身份验证的用户名相同。

步骤 5 输入用户的全称。

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，请参阅预定义用户角色 ， 第 246 页部分中的用户角色说明表。

如果您在此处添加新的邮件角色或网络角色，请为该角色输入名称。有关命名限制的信息，请参阅创建自定义邮件用户角色 ， 第 251 页或创建自定义网络用户角色， 第 253 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 如果您在此页面上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 248 页。

编辑本地定义的用户

例如，使用此程序更改密码。

步骤 1 在“用户 (Users)”列表中点击用户名。

步骤 2 对用户进行更改。

步骤 3 提交并确认更改。

删除本地定义的用户

步骤 1 点击对应“用户”(Users) 列表中用户名的垃圾桶图标。

步骤 2 通过点击显示的警告对话框中的**删除**以确认删除。

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，请执行以下操作：

- 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。

注释 星号表示被分配委派管理的自定义用户角色的用户。如果用户的自定义角色已被删除，则“未分配”(Unassigned) 会以红色出现。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 248 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”页面（有关详细信息，请参阅编辑本地定义的用户，第 256 页）。
- 要更改系统的默认管理员用户账户的密码，请参阅更改管理员用户的密码，第 255 页。
- 要强制用户更改其密码，请参阅要求用户按要求更改密码，第 260 页。
- 用户可以更改自己的密码，方法是点击 GUI 右上角的“选项”菜单并选择“更改密码”选项。

设置密码和登录要求

可以通过定义用户账户和密码限制来实施组织密码策略。用户账户和密码限制适用于安全管理设备上定义的本地用户。您可以配置以下设置：

- **用户账户锁定 (User account locking)**。可以定义导致用户账户被锁定的失败登录尝试次数。
- **密码有效期规则**。可以定义密码的有效期，在该期限之后，用户登录后需要更改密码。

- **密码规则**。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。

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**本地用户账户和密码设置**部分。

步骤 3 点击**编辑设置**。

步骤 4 配置设置：

设置	说明
用户账户锁定 (User Account Lock)	选择用户登录失败后是否锁定用户账户。指定导致账户锁定的失败登录尝试次数。您可以输入一 (1) 到 60 之间的任一数值。默认值为五 (5)。 配置账户锁定时，请输入要向尝试登录的用户显示的消息。使用 7 位 ASCII 字符组成的文本。仅当用户输入已锁定账户的正确密码时，才会显示此消息。 用户账户被锁定后，管理员可以在 GUI 中的“编辑用户 (Edit User)”页面中或使用 `userconfig` 命令解锁账户。 无论用户连接的计算机或连接类型（例如 SSH 或 HTTP）如何，用户都会跟踪失败的登录尝试。一旦用户成功登录，失败登录尝试次数就会被重置为零 (0)。 当用户账户由于达到最大失败登录尝试次数而被注销时，系统会向管理员发送警报。警报的严重级别设置为“参考 (Info)”。 **注释** 此外，还可以手动锁定各个用户账户。请参阅手动锁定用户账户 ， 第 261 页。
密码重置	选择是否应在管理员更改用户的密码后强制用户更改其密码。 您还可以选择是否应强制用户在其密码到期后更改。输入在用户必须更改密码之前可以持续使用密码的天数。您可以输入一 (1) 到 366 之间的任一数值。默认值为 90。要强制用户在非计划的时间更改其密码，请参阅要求用户按要求更改密码 ， 第 260 页。 如果强制用户在其密码到期后更改，可以显示关于密码即将到期的通知。选择在到期之前通知用户的天数。 **注释** 当用户账户使用 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 密钥的用户账户到期时，用户必须输入其旧密码或请管理员手动更改密码，才能更改与该账户相关的密钥。
密码规则： 至少需要 <数字> 个字符。	输入密码可以包含的最小字符数。 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超过您在此处指定的数字。

设置	说明
密码规则： 至少需要一个数字 (0-9)。 (Password Rules: Require at least one number (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。 (Password Rules: Require at least one special character.)	选择密码是否必须包含至少一个特殊字符。密码可以包含以下特殊字符： ~ ? ! @ # $ % ^ & * - _ + = \ | / [ ] ( ) < > { } ` ' " ; : , .
密码规则： 禁止将用户名及其变体用作密码。	选择是否允许密码与相关联的用户名或其变体形式相同。当禁止用户名变体形式时，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。 • 密码不能与反写的用户名相同，不区分大小写。 • 密码不能在使用以下字符替代的情况下与用户名或反写的用户名相同： • “@”或“4”表示“a” • “3”表示“e” • “|”、“!”或“1”表示“i” • “0”表示“o” • “$”或“5”表示“s” • “+”或“7”表示“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。 您可以输入一 (1) 到 15 之间的任一数值。默认值为三 (3)。
密码规则： 不允许在密码中使用的单词列表	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。以 forbidden_密码_words.txt 为文件名保存文件并使用 SCP 或 FTP 将文件上传到设备中。 如果选择了此限制，但未上传单词表，将忽略此限制。

设置	说明
密码长度	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。 选择要为其显示指标的角色。然后，为每个选定角色输入一个大于零的数值。数字越大，意味着注册为强密码口令的密码越难破解。此设置无最大值。 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，则注册为强密码口令的 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： • 较长 • 包含大写字母、小写字母、数字和特殊字符 • 不包含以任何语言表示的词典中的词语。 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。

下一步做什么

要求用户将其密码更改为符合新要求的新密码。请参阅要求用户按要求更改密码 ，第 260 页

要求用户按要求更改密码

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。这是一次性的操作。

要自动定期更改密码，请使用设置密码和登录要求 ，第 257 页中所述的“密码重置”选项。

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”部分中，选中将被要求更改密码的用户旁边的复选框。

步骤 3 选择**强制密码更改**。

步骤 4 选择选项。

在“本地用户账户和密码设置”中配置宽限期的全局设置。

步骤 5 点击**确定**。

锁定和解除锁定本地用户账户

锁定用户账户防止本地用户登录设备。可以通过以下方式之一锁定用户账户：

- 您可以将所有本地用户账户配置为在用户经过配置的尝试次数后未能成功登录时锁定：请参阅设置密码和登录要求 ， 第 257 页。
- 管理员可以手动锁定用户账户。请参阅手动锁定用户账户 ， 第 261 页。

AsyncOS 会显示您在“编辑用户”(Edit User) 页面上查看用户账户时，用户账户被锁定的原因。

手动锁定用户账户

步骤 1 仅第一次：设置设备以启用用户账户锁定：

步骤 2 a) 依次转到**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。
b) 在**本地用户账户和密码设置**部分，点击**编辑设置**。
c) 选中**在管理员已手动锁定用户账户时显示已锁定账户消息 (Display Locked Account Message if Administrator has manually locked a user account)** 复选框，然后输入消息。
d) 提交更改。

步骤 3 转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**，然后点击用户名。

注释 在锁定管理员账户之前，确保您可以将其解除锁定。请参阅将用户账户解除锁定 ， 第 261 页中的注释。

步骤 4 点击**锁定账户 (Lock Account)**。

AsyncOS 会显示一则消息，说明用户将不能登录设备，并询问您是否要继续操作。

将用户账户解除锁定

要将用户账户解除锁定，请通过点击“用户”(Users) 列表中的用户名打开用户账户，然后点击“解除锁定账户”(Unlock Account)。

注释 如果锁定“admin”账户，您仅能通过到串行控制台端口的串行通信连接，以管理员身份登录后，才能解锁该管理账户。即使在admin账户被锁定时，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。

注释 经过外部身份验证的用户无法使用自定义视图 ， 第 330 页所述的某些功能。

- 如果您的部署使用本地和外部身份验证，则本地用户名不能与经过外部身份验证的用户名相同。
- 如果设备无法与外部目录进行通信，则具有外部和本地账户的用户可以设备上的本地用户账户登录。

请参阅：

- 使用 LDAP 配置管理用户的外部身份验证 ， 第 236 页
- 启用 RADIUS 身份验证， 第 262 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 236 页。

启用 RADIUS 身份验证

您可以使用 RADIUS 目录对用户进行身份验证，并将用户组分配给用户角色以便管理您的设备。RADIUS 服务器应支持 CLASS 属性，AsyncOS 使用该属性将 RADIUS 目录中的用户分配给用户角色。

注释 如果外部用户更改其 RADIUS 组的用户角色，则该用户应注销设备，然后再次登录。用户将具有新角色的权限。

开始之前

访问 RADIUS 服务器的共享密钥长度不能超过 48 个字符。

步骤 1 依次选择**管理设备** > **系统管理** > **用户**页面，然后点击**启用**。

步骤 2 选中**启用外部身份验证 (Enable External Authentication)** 复选框。

步骤 3 为身份验证类型选择“RADIUS”。

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。

注释 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 输入设备在超时前等待服务器响应的秒数。

步骤 8 选择要将密码身份验证协议 (PAP) 还是质询握手身份验证协议 (CHAP) 用作身份验证协议。

步骤 9 （可选）点击**添加行 (Add Row)** 添加另一台 RADIUS 服务器。为您的设备用于身份验证的每台 RADIUS 服务器重复步骤 6 和 7。

在定义多台外部服务器时，设备按设备上定义的顺序连接到服务器。您可能希望定义多台外部服务器，以允许在一台服务器暂时不可用时进行故障切换。

步骤 10 输入在网络用户界面上存储外部身份验证凭证的所花费的时间。

注释 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 • 无冒号、逗号或换行字符 • 每个 RADIUS 用户的一个或多个映射 CLASS 属性（通过此设置，AsyncOS 会拒绝访问不带映射 CLASS 属性的 RADIUS 用户。） 对于具有多个 CLASS 属性的 RADIUS 用户，AsyncOS 会分配最具限制性的角色。例如，如果 RADIUS 用户具有两个 CLASS 属性（映射到“操作员”[Operator] 和“只读操作员”[Read-Only Operator] 角色），则 AsyncOS 会为 RADIUS 用户分配“只读操作员”(Read-Only Operator) 角色（比“操作员”[Operator] 角色更严格）。 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 • 操作员 • 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 会为 RADIUS 用户分配“管理员”(Administrator) 角色。

步骤 12 （可选）点击**添加行**添加另一个组。为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。

对访问安全管理设备指定额外的控制

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。如果用户尝试从不包含在列表中的地址连接设备，则用户访问会被拒绝。

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。

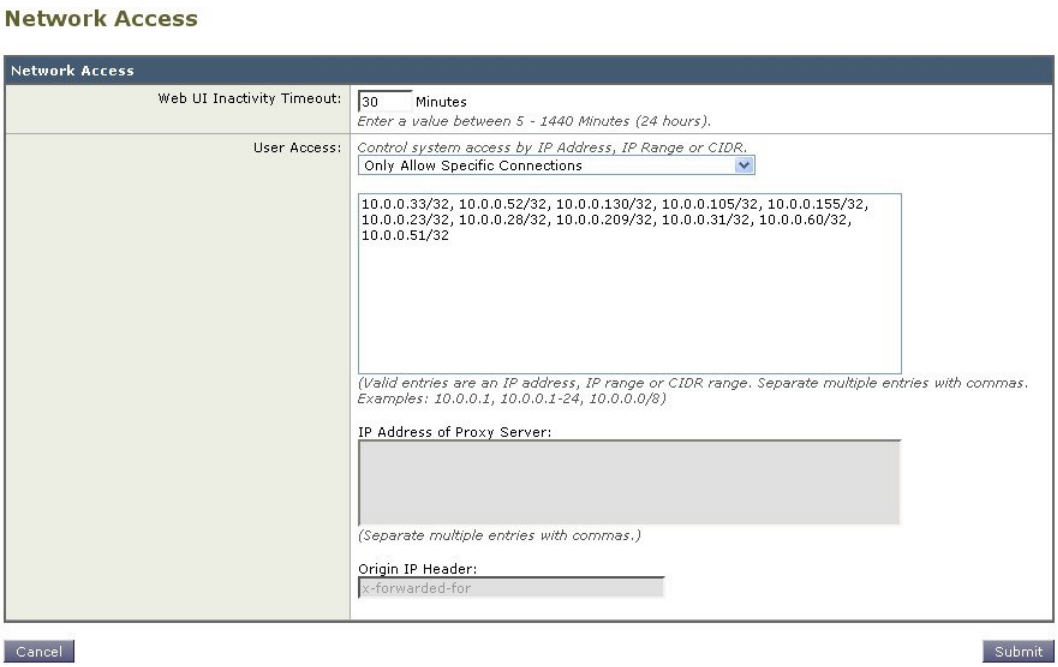
此信头的值为逗号分隔的 IP 地址列表，最左边的地址为远程用户计算机的地址，之后是转发连接请求的每个后续代理的地址。（信头名称是可配置的。）安全管理设备对照访问列表中允许的用户和代理 IP 地址，匹配信头中的远程用户 IP 地址和连接代理的 IP 地址。

注释 AsyncOS 仅支持 x-forwarded-for 信头中的 IPv4 地址。

创建访问列表

您可以通过 GUI 上的“网络访问”(Network Access) 页面或 **adminaccessconfig > ipaccess** CLI 命令创建网络访问列表。下图显示了“网络访问”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 *11:* 网络访问设置示例



AsyncOS 为访问列表提供四种不同的控制模式：

- **允许全部 (Allow All)**。此模式允许到设备的所有连接。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 地址匹配访问列表中包含的 IP 地址、IP 范围或 CIDR 范围，则此模式允许用户连接到设备。
- **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，则此模式允许用户通过反向代理连接到设备：
  - 连接代理的 IP 地址包含在访问列表的“代理服务器 IP 地址”(IP Address of Proxy Server) 字段中。
  - 代理在其连接请求中包含 x-forwarded-header HTTP 信头。
  - x-forwarded-header 的值不能为空。
  - 远程用户的 IP 地址包含在 x-forwarded-header 中，并与访问列表中为用户定义的 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 范围相匹配，则此模式会允许用户通过反向代理或直接连接到设备。通过代理进行连接的条件与在“仅允许通过代理的特定连接”(Only Allow Specific Connections Through Proxy) 模式下的条件相同。

请注意，在您提交并确认更改后，如果以下条件之一为真，则您可能会失去对设备的访问权限：

- 如果选择**仅允许特定连接 (Only Allow Specific Connections)**，并且在列表中不包含当前计算机的 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)**，并且当前连接到设备的代理的 IP 地址不在代理列表中，原始 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)**，并且
  - 原始 IP 信头的值不在允许的 IP 地址列表中

    或

  - 原始 IP 信头的值不在允许的 IP 地址列表中，并且连接到设备的代理的 IP 地址不在允许的代理列表中。

如果您选择继续而不更正访问列表，当您确认更改时，AsyncOS 将断开您的计算机或代理与设备的连接。

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**。

步骤 3 选择访问列表的控制模式。

步骤 4 输入将允许用户从其连接设备的 IP 地址。

您可以输入 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：

- 允许连接设备的代理的 IP 地址。使用逗号分隔多个条目。
- 代理发送给设备（其中包含远程用户计算机以及转发请求的代理服务器的IP地址）的原始IP信头的名称。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。

一旦 AsyncOS 注销用户，设备会将用户的网络浏览器重定向到登录页面。

注释 网络 UI 会话超时不适用于垃圾邮件隔离区会话，这些会话具有无法配置的 30 分钟超时。

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**。

步骤 3 在 **Web UI 不活动超时时间 (Web UI Inactivity Timeout)** 字段中，输入用户可在注销之前保持不活动状态的分钟数。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。

配置 CLI 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 CLI 的时间。CLI 会话超时适用于：

- 所有用户，包括管理员
- 仅适用于使用安全外壳 (SSH)、SCP和直接串行连接的连接

注释 在 CLI 会话超时时的所有未提交的配置更改都将丢失。确保在进行配置更改后立即进行确认。

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**。

步骤 3 在 **CLI 不活动超时时间 (CLI Inactivity Timeout)** 字段中，输入用户可在注销之前保持不活动状态的分钟数。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。

下一步做什么

也可以使用 CLI 中的 `adminaccessconfig` 命令来配置 CLI 会话超时。请参阅《用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。

控制对“邮件跟踪”中敏感信息的访问权限

步骤 1 转到**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)** 页面。

步骤 2 在**跟踪权限**部分，点击**编辑设置**。

步骤 3 选择要为其授予邮件跟踪中敏感信息访问权限的角色。

系统只会列出有权访问邮件跟踪的自定义角色。

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。

为管理用户显示消息

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。

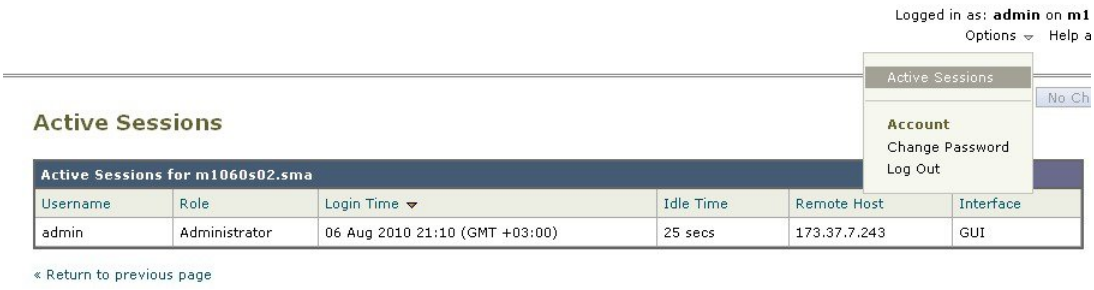
查看管理用户活动

使用网络查看活动会话

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。

在窗口的右上角，依次选择**选项 (Options) > 活动会话 (Active Sessions)**。

图 *12:*“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。

查看您最近的登录尝试

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的“登录身份”旁边的图图标。

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时使用的远程主机。
- whoami 命令显示当前已登录的用户的用户名和全称，以及用户所属的组：

```
mail3.example.com>
whoami
Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

- last 命令会显示哪些用户最近登录到设备。远程主机的 IP 地址以及登录时间、注销时间和总时间也会出现。

```
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
```

管理用户访问权限故障排除

- 错误：没有为用户分配访问权限，第 271 页
- 用户没有活动的菜单 ，第 271 页

• 经过外部身份验证的用户看到“首选项”(Preferences) 选项 ， 第 271 页

错误：没有为用户分配访问权限

问题

虽然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。查看“管理设备”(Management Appliance) > “系统管理”(System Administration) > “用户”(Users) 以确定已分配的用户角色，然后转到“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，并将权限分配给该角色。

如果您已根据报告组分配访问权限，请确保您在“管理设备”(Management Appliance) > “系统管理”(System Administration) > “用户角色”(User Roles) 页面上为该用户选择了报告组。要分配组，请点击“委派管理的用户角色”表的“邮件报告”列中的**未选择组**链接。

用户没有活动的菜单

问题

您向其授予“发布”(Publish) 权限的用户在登录后没有活动的菜单。

解决方案

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。如果您不希望向此用户授予编辑任一内容的权限，请创建不用于任何策略的自定义类别，并在“自定义用户角色”(Custom User Role) 页面上向此用户角色授予对此类别的权限。

经过外部身份验证的用户看到“首选项”(Preferences) 选项

问题

经过外部身份验证的用户看到“首选项”选项。

解决方案

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。

经过外部身份验证的用户看到“首选项”**(Preferences)** 选项

第 14 章

常规管理任务

本章包含以下部分：

执行管理任务

您可以通过使用图形用户界面 (GUI) 中的“系统管理”(System Administration) 菜单执行大多数系统管理任务。但是，某些系统管理功能仅在命令行界面 (CLI) 中提供。

此外，您可在“监控”菜单上访问设备的状态监控功能，如监控系统状态， 第 217 页一章中所述

注释 本章介绍的几项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 382 页。

使用功能密钥

密钥特定于您的设备序列号和您启用的功能。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此部分介绍的任务，请使用 featurekey 命令。

目标	相应操作
• 查看设备的所有激活的功能密钥 • 查看任何等待激活的功能密钥 • 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)**。 要手动添加新的功能密钥，请在“功能密钥”字段中粘贴或输入密钥，然后点击**提交密钥**。如果未添加功能（例如密钥不正确），则会出现错误消息；否则功能密钥会添加到列表。 如果将设备配置为在发布新密钥时自动下载并安装新密钥，则“等待激活”(Pending Activation) 列表始终为空。
启用或禁用功能密钥的自动下载和激活	依次选择**管理设备 > 系统管理 > 功能密钥设置**。 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到期时的设备行为的信息，请参阅可从以下网址获得的《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) 中使用 show license 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

- resume
- resumetransfers
- resetconfig
- version

关闭安全管理设备

要关闭安全管理设备，请执行以下操作：

- 使用**管理设备 > 系统管理 > 关机/重启**页面。

  或

- 在命令行提示符处使用 `shutdown` 命令。

关闭设备会退出 AsyncOS，使您可以安全关闭设备电源。您稍后可以重新启动设备，而不会丢失传送队列中的任何邮件。您必须为要关闭的设备输入延迟。默认延迟为30秒。AsyncOS 允许在延迟期间完成打开的连接，之后会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 中“系统管理”菜单中的“关机/重启”页面，或使用 GLI 中的 reboot 命令。

重新启动设备会重新启动 AsyncOS，使您可以安全关闭并重新启动设备。您必须为要关闭的设备输入延迟。默认延迟为 30 秒。AsyncOS 允许在延迟期间完成打开的连接，之后会强行关闭打开的连接。您可以重新启动设备，而不会丢失传送队列中的任何邮件。

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	说明	持久性
`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。 • 出站邮件传送已暂停。 • 停止日志传输。 • CLI 仍可访问。	在重新启动后持续。

命令	说明	持久性
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。	在重新启动后持续。

在使用这些命令时，您必须为设备输入延迟。默认延迟为30秒。AsyncOS 允许在延迟期间完成打开的连接，之后会强行关闭打开的连接。如果没有打开的连接，服务会立即暂停。

要重新激活由 suspend 或 suspendtransfers 命令停止的服务，请分别使用 resume 或 resumetransfers 命令。

要确定管理设备的当前在线/已暂停状态，请在网络界面中依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 关闭/重新启动 (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。

在使用 suspendtransfers 命令后，通过 resumetransfers 命令可将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

如果物理传输设备，或作为解决配置问题的最后手段，您可能需要将设备重置为出厂默认设置。

⚠

注意 重置配置会将您与CLI断开连接，禁用您用于连接到设备的各项服务（FTP、Telnet、SSH、HTTP、HTTPS），并删除用户账户。

目标	相应操作
• 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.** 确保您可以在重置后使用默认管理员用户账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，请参阅设置、安装和基本配置，第 5 页。 **2.** 在设备上暂停服务。 **3.** 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 配置文件 (Configuration File)**，然后点击**重置 (Reset)**。 **注释** 在重置后，设备会自动恢复到在线状态。如果在重置之前暂停了邮件传送，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相似命令不相同。

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 的版本信息

步骤 1 依次选择**管理设备 > 集中服务 > 系统状态**。

步骤 2 滚动至页面底部，然后在“版本信息”(Version Information) 下查看当前已安装的 AsyncOS 版本。

此外，您可以在命令行提示符处使用 **version** 命令。

启用远程电源循环

只有在 80 和 90 系列硬件上，才能远程重置设备机箱的电源。

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过程启用和配置此功能。

开始之前

- 使用线缆将专用的远程电源循环 (RPC) 端口直接连接到安全网络。有关信息，请参阅相关型号的硬件文档，可从文档 ，第 393 页所列的位置获得该文档。
- 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循环接口使用唯一的 IPv4 地址。此接口仅可按照本节所述的过程配置，而不能使用 `ipconfig` 命令配置。
- 要重启设备，您需要一个可以管理支持智能平台管理接口 (IPMI) 2.0 版本的设备的第三方工具。确保您准备使用此类工具。
- 有关访问命令行接口的详细信息，请参阅《CLI 参考指南》。

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 用有管理员权限的账户登录。

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，加上网络掩码和网关。
- 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，以确保您可以远程管理设备电源。

步骤 7 确保您将来可以一直使用您输入的证书。例如，将此信息存储到一个安全的地方，并确保需要执行此任务的管理员有权限访问所需的证书。

下一步做什么

远程重置设备电源 ，第 372 页

使用 SNMP 监控系统运行状况

AsyncOS 支持通过简单网络管理协议 (SNMP) 版本 v1、v2 和 v3 进行系统状态监控。

- 要启用和配置 SNMP，请在命令行界面中使用 `snmpconfig` 命令。
- MIB 可从以下网址获取：http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html使用最新的可用文件。
- 必须对密码身份验证和 DES 加密使用 SNMPv3，才能启用此服务。（有关 SNMPv3 的详细信息，请参阅 RFC 2571-2575。）您必须设置至少 8 个字符的 SNMPv3 密码，才可以启用 SNMP 系统状态监控。首次输入 SNMPv3 密码时，您必须重新输入密码进行确认。下次运行该命令时，`snmpconfig` 命令会“记住”此密码。
- 在设置 SNMP 以监控连接时：

  如果在配置 connectivityFailure SNMP 陷阱时输入 URL 属性，请确定 URL 是否指向目录或文件。

  - 如果是目录，请添加尾部反斜杠 (/)
  - 如果是文件，请勿添加尾部反斜杠

- 有关将 SNMP 与 AsyncOS 配合使用的其他信息，请参阅网络或邮件安全设备的联机帮助。

示例：snmpconfig 命令

```
sma.example.com> snmpconfig
Current SNMP settings:
SNMP Disabled.
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP
Do you want to enable SNMP?
[Y]>
Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: sma.example.com)
[1]>
Which port shall the SNMP daemon listen on interface "Management"?
[161]>
Please select SNMPv3 authentication type:
1. MD5
2. SHA
```

```
[1]> 2
Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2
Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>
Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>
Service SNMP V1/V2c requests?
[N]> Y
Enter the SNMP V1/V2c community string.
[ironport]> public
Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>
From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>
Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1
Enter the Trap Community string.
[ironport]> tcomm
Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y
Do you want to disable any of these traps?
[Y]> n
Do you want to enable any of these traps?
[Y]> y
Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 1,7,12
What threshold would you like to set for CPU utilization?
[95]>
What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>
What threshold would you like to set for memory utilization?
[95]>
Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3
Enter the System Contact string.
[snmp@localhost]> SMA.Administrator@example.com
Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
```

```
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: SMA.Administrator@example.com
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>
sma.example.com> commit
Please enter some comments describing your changes:
[]> Enable and configure SNMP
Changes committed: Fri Nov 06 18:13:16 2015 GMT
sma.example.com>
```

备份安全管理设备数据

备份哪些数据

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
- 网络跟踪
- 报告（邮件和网络）
- 安全列表/阻止列表

在数据传输完成后，两台设备上的数据将是相同的。

配置和日志不使用此过程备份。要备份这些项目，请参阅其他重要备份任务 ， 第 286 页。

在首次备份后，每次备份仅复制自上次备份以来生成的信息。

备份的限制和要求

请确保在计划备份之前满足以下限制和要求。

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	必须在网络上设置目标设备。 如果目标设备是新的，请运行“系统设置向导”(System Setup Wizard) 输入所需信息。有关说明，请参阅设置、安装和基本配置 ，第 5 页。
源与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： • 端口 22 必须在两台设备上打开。默认情况下，此端口在运行“系统设置向导”(System Setup Wizard) 时打开。 • 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。
目标设备不能在服务中	只有主设备应从受管的邮件和网络安全设备提取数据。为确保这一点，请参阅防止目标设备直接从受管设备提取数据 ，第 283 页。 此外，请取消备份设备上的任何已计划的配置发布作业。
设备容量	目标设备上的磁盘空间容量必须大于或等于源设备的容量。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和容量，请参阅管理磁盘空间 ，第 320 页。 有关虚拟设备磁盘容量的信息，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

在完整的初始备份期间，备份 800GB 可能最多需要 10 小时。每日备份可能需要 3 小时。每周和每月备份需要更长的时间。以上数字可能发生变化。

在初始备份后，备份过程仅传输自上次备份后已更改的文件。因此，与初始备份相比，后续备份应花费较少的时间。后续备份所需的时间取决于累积的数据量、多少文件发生了更改，以及文件自上次备份以来发生了多大程度的更改。

备份期间的服务可用性

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 阶段从源和目标设备之间的数据传输开始。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，服务在目标设备上关闭。一旦完成从源设备到目标设备的数据传输，第 2 阶段立即开始。
- 阶段 2：当第 2 阶段开始时，源设备上的服务会被关闭。在数据传输期间收集的源和目标设备之间自上次关闭以来的差异会复制到目标设备，并且源和目标设备上的服务会恢复到启动备份时所处的状态。这样做可以最大限度保持源设备上的正常运行时间，并且任一设备都不会丢失数据。

在备份期间，数据可用性报告可能不起作用，而在查看邮件跟踪结果时，每封邮件的主机名可能标记为“未解析”(unresolved)。

如果您尝试计划报告，并且忘了某个备份正在进行，可以通过依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services)** 查看系统状态。您可以在此窗口的页面顶部看到表示系统备份正在进行的警告。

备份过程中断

注释 如果在执行备份时源设备意外重新启动，目标设备不会察觉到此故障。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受管设备提取数据

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 10 页。

步骤 2 运行 `suspendtransfers` 命令。

步骤 3 等待提示符重新出现。

步骤 4 运行 `suspend` 命令。

步骤 5 等待提示符重新出现。

步骤 6 退出目标设备的命令行界面。

接收有关备份状态的警报

要在备份完成时接收警报和关于任何问题的通知，请配置设备以发送类型为“系统”(System)、严重性为“信息”(Info) 的警报。请参阅管理警报，第 302 页。

计划单次或经常性的备份

您可以计划单次备份或经常性的备份在预定的时间进行。

注释 如果远程设备上存在任何正在进行的备份，备份过程将不会开始。

开始之前

- 满足备份的限制和要求，第 282 页所列的各项限制和要求。

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** 键。

步骤 3 如果源和目标设备之间的连接速度较慢，请开启数据压缩：

键入 **setup** 并输入 **Y**。

步骤 4 键入 **Schedule** 并按 **Enter** 键。

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 输入目标设备的管理员用户名和密码。

步骤 8 回应有关要备份哪些数据的提示。

步骤 9 要计划单次备份，请键入 **2** 以计划单次备份，然后按 **Enter** 键。

步骤 10 要计划经常性的备份，请执行以下操作：

a) 键入 **1** 以“设置重复性的备份计划”，然后按 **Enter** 键。

b) 选择定期备份的频率，然后按 **Enter** 键。

步骤 11 键入您希望备份开始的特定日期和日期和时间，然后按 **Enter** 键。

步骤 12 键入备份过程的名称。

步骤 13 验证是否已成功计划备份：在命令提示符处键入 **View**，然后按 **Enter** 键。

步骤 14 另请参阅其他重要备份任务 ， 第 286 页。

开始即时备份

注释 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。

开始之前

满足备份的限制和要求 ， 第 282 页中的所有要求。

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** 键。

步骤 3 如果源和目标设备之间的连接速度较慢，请开启数据压缩：

键入 **setup** 并输入 **Y**。

步骤 4 键入 **Schedule** 并按 **Enter** 键。

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 输入目标设备的管理员用户名和密码。

步骤 8 回应有关要备份哪些数据的提示。

步骤 9 键入 **3** 以“立即开始单次备份”，然后按 **Enter** 键。

步骤 10 为备份作业输入有意义的名称。

备份过程会在几分钟内开始。

步骤 11 （可选）要查看备份的进度，请在命令行提示符处键入 **Status**。

步骤 12 另请参阅其他重要备份任务 ， 第 286 页。

检查备份状态

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** 键。

检查以下备份的状态	相应操作
计划的备份	选择 View 操作。

检查以下备份的状态	相应操作
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 303 页。

下一步做什么

相关主题

日志文件中的备份信息 ， 第 286 页

日志文件中的备份信息

备份日志会自始至终记录备份过程。

有关备份计划的信息在 SMA 日志中。

相关主题

- 检查备份状态 ， 第 285 页

其他重要备份任务

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 314 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 356 页。

此外，还可以设置“备份日志 (Backup Logs)”的日志订用。请参阅在 GUI 中创建日志订用 ， 第 357 页。

使备份设备作为主设备

如果您升级设备硬件，或因任何其它原因需要切换设备，请使用此操作程序。

开始之前

回顾备份安全管理设备数据 ， 第 281 页中的信息。

步骤 1 将配置文件的副本从您的旧/主/源设备保存到新设备中您可以访问的位置。请参阅保存和导入配置设置 ， 第 314 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 282 页中的要求。

步骤 4 从旧/主/源设备运行备份。请参阅开始即时备份 ， 第 285 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。

不要在旧/原始主/源设备上运行此命令。

步骤 10 在新/备份/目标设备与受管的邮件和网络安全设备之间建立连接：

步骤 11
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 (Test Connection)**。
e) 返回到设备列表。
f) 对每台受管的设备重复执行上述步骤。

步骤 12 验证新/目标设备现在是否作为主设备运行：

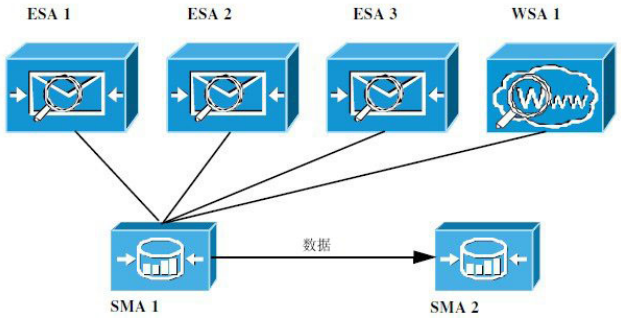
依次选择**管理设备 > 集中服务 > 系统状态**，并检查数据传输状态。

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 281 页中的信息定期保存的备份数据。

典型的设备配置可能如下图所示：

图 *13:* 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：

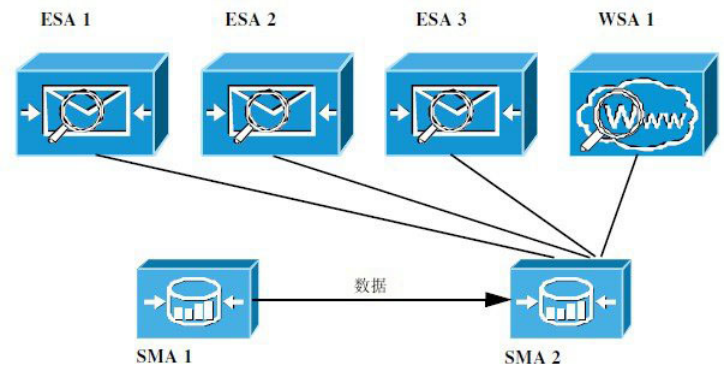
过程

	命令或操作	目的
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 315 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 上依次选择**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 Interface)** 页面上，将出现故障的 SMA 1 中的所有相关 IP 接口信息输入到文本字段中，以在 SMA 2 上重新创建该接口。 有关添加 IP 接口的详细信息，请参阅配置 IP 接口，第 374 页。
步骤 4	提交并确认更改。	
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 16 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。	请参阅关于添加受管设备，第 14 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、病毒和病毒爆发隔离区，第 169 页。
步骤 8	如有必要，请恢复其他数据。	请参阅其他重要备份任务，第 286 页。

下一步做什么

完成此过程后，SMA 2 将变成主安全管理设备。来自 ESA 1-3 和 WSA 1 的数据现在进入 SMA 2，如下图所示：

图 *14:* 灾难恢复：最终结果



升级设备硬件

请参阅使备份设备作为主设备 ， 第 286 页。

升级 AsyncOS

升级的批处理命令

有关升级操作程序的批处理命令，请参阅以下位置的《AsyncOS for Email CLI 参考指南》：
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。如果您采用严格的防火墙策略，可能需要配置 AsyncOS 升级的静态位置。如果您确定防火墙设置要求为升级配置静态 IP，请与思科客户支持人员联系人以获取所需的 URL 地址。

注释 如果您有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，则需要将其删除并且/或者将其替换为修订的防火墙规则。

选择升级方法：远程或流传输

思科为在设备上升级 AsyncOS 提供了两种方法（或“来源”）。

- 流传输升级 - 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 - 您只从思科下载升级映像一次，然后将其提供给您的各台设备。然后设备从您的网络内的一台服务器下载 AsyncOS 升级。

您将在配置升级和服务更新设置，第 292 页中配置升级方法。（可选）在 CLI 中使用 **updateconfig** 命令。

流传输升级概述

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：

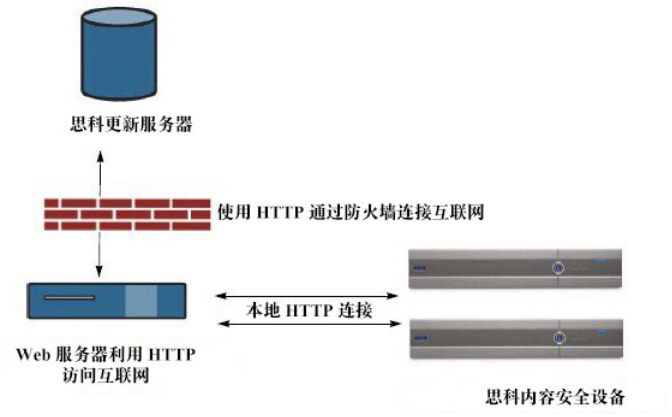
图 *15*: 数据流更新方法

此方法要求设备直接从网络与思科内容安全更新服务器联系。

远程升级概述

您还可以从自己的网络内将更新下载到 AsyncOS 并在本地托管更新（远程升级），而不是直接从思科更新服务器获取更新（流传输升级）。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 *16:* 远程更新方法



基本过程如下所述：

步骤 1 阅读远程升级的硬件和软件要求，第 291 页和托管远程升级映像，第 292 页中的信息。

步骤 2 配置本地服务器检索和服务升级文件。

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**。

注释 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 289 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具有符合以下要求的系统：

- 可通过互联网访问思科内容安全设备的更新服务器。
- 具有网络浏览器。

注释 对于此版本，如果您需要配置防火墙设置以允许通过 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。

对于托管 AsyncOS 更新文件，您的内部网络中必须有一个满足以下条件的服务器：

- 具有网络服务器 - 例如 Microsoft IIS（互联网信息服务）或 Apache 开源服务器 - 并且该服务器：

- 支持显示超过 24 个字符的目录或文件名
- 已启用目录浏览
- 已配置用于匿名（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

在设置本地服务器后，转至 **http://updates.ironport.com/fetch_manifest.html** 以下载升级映像的压缩文件。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。点击您要下载升级映像压缩文件的升级版本。要将升级映像用于 AsyncOS 升级，请在“编辑更新设置”页面上输入本地服务器的基本 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上托管升级列表，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。要将升级列表用于 AsyncOS 升级，请在“编辑更新设置”页面上输入 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，请查看知识库（请参阅知识库文章（技术说明），第 395 页）或与您的技术支持提供商联系。

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：

- 升级将在下载时立即安装。
- 在升级过程开始时，一条横幅会出现 10 秒。在此横幅出现时，您可以选择按 Ctrl - C 以在下载开始前退出升级过程。

配置升级和服务更新设置

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 会定期查询更新服务器是否存在所有安全服务组件的新更新（新的 AsyncOS 升级除外）。要升级 AsyncOS，您必须手动提示 AsyncOS 查询可用的升级。

您可以在 GUI 中（请参阅以下两个部分）或在 CLI 中使用 updateconfig 命令配置升级和更新设置。

您还可以配置以下通知设置。

升级和更新设置

下表介绍了可配置的更新和升级设置。

表 *43:* 更新安全服务的设置

设置	说明
更新服务器（图像）(Update Servers [images])	选择是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。升级和更新的默认设置是思科服务器。 在以下情况下，您可能需要使用本地网络服务器： • 您需要从静态地址将映像下载到您的设备。请参阅采用严格防火墙策略的环境的静态升级和更新服务器设置 ，第 294 页。 • 您希望在方便时将 AsyncOS 升级映像下载到您的设备。（您仍然可以从思科更新服务器动态下载服务更新映像。） 在选择本地更新服务器时，输入用于下载升级和更新的服务器的基本 URL 和端口号。如果服务器需身份验证，则也可以输入有效用户名和密码。 有关详细信息，请参阅选择升级方法：远程或流传输 ，第 290 页和远程升级概述 ，第 290 页。
更新服务器（列表）	选择是从思科服务器还是本地网络服务器下载可用升级和服务更新列表（清单 XML 文件）。 升级和更新的默认设置是思科服务器。您可以为升级和更新选择不同的设置。 如果适用，请参阅采用严格防火墙策略的环境的静态升级和更新服务器设置 ，第 294 页。 如果您选择本地更新服务器，请为每个列表输入清单 XML 文件的完整路径，包括文件名和服务器的端口号。如果您在端口字段留空，AsyncOS 将使用端口 80。如果服务器需身份验证，则也可以输入有效用户名和密码。 有关详细信息，请参阅选择升级方法：远程或流传输 ，第 290 页和远程升级概述 ，第 290 页。
自动更新	选择是否为时区规则启用自动更新。在启用后，输入检查更新之间要等待的时间。为分钟、小时和天分别添加尾部的 **m**、**h** 和 **d**。
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，请在此处输入服务器信息以及用户名和密码。 请注意，如果您指定代理服务器，它将用于访问和更新 GUI 中列出的服务。 此代理服务器还用于从云中获取“文件分析”(File Analysis) 报告详细信息。另请参阅文件分析报告详细信息的要求 ，第 60 页（Web 报告）或文件分析报告详细信息的要求 ，第 104 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，请在此处输入服务器信息以及用户名和密码。 请注意，如果您指定代理服务器，它将用于访问和更新 GUI 中列出的服务。 此代理服务器还用于从云中获取文件分析报告详细信息。另请参阅文件分析报告详细信息的要求 ，第 60 页（Web 报告）或文件分析报告详细信息的要求 ，第 104 页（邮件报告）。

采用严格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。如果您的环境采用需要静态 IP 地址的严格防火墙策略，请在“更新设置”(Update Settings) 页面上使用以下设置：

图 *17:* 更新服务器（映像）设置的静态 ***URL***

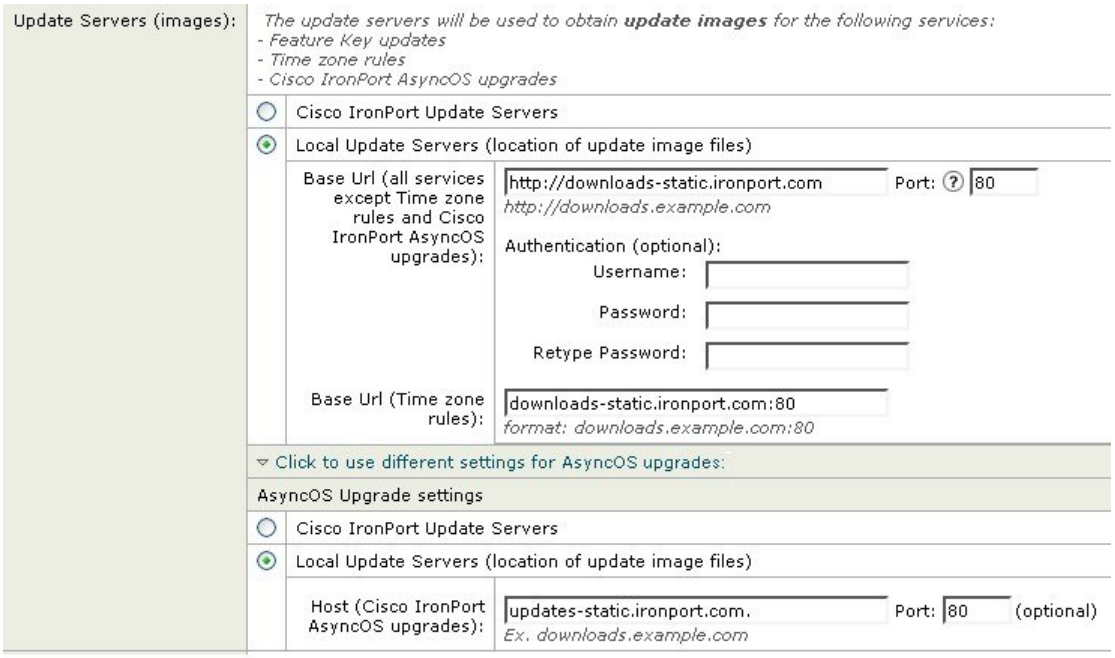


图 *18:* 更新服务器（列表）设置的静态 ***URL***

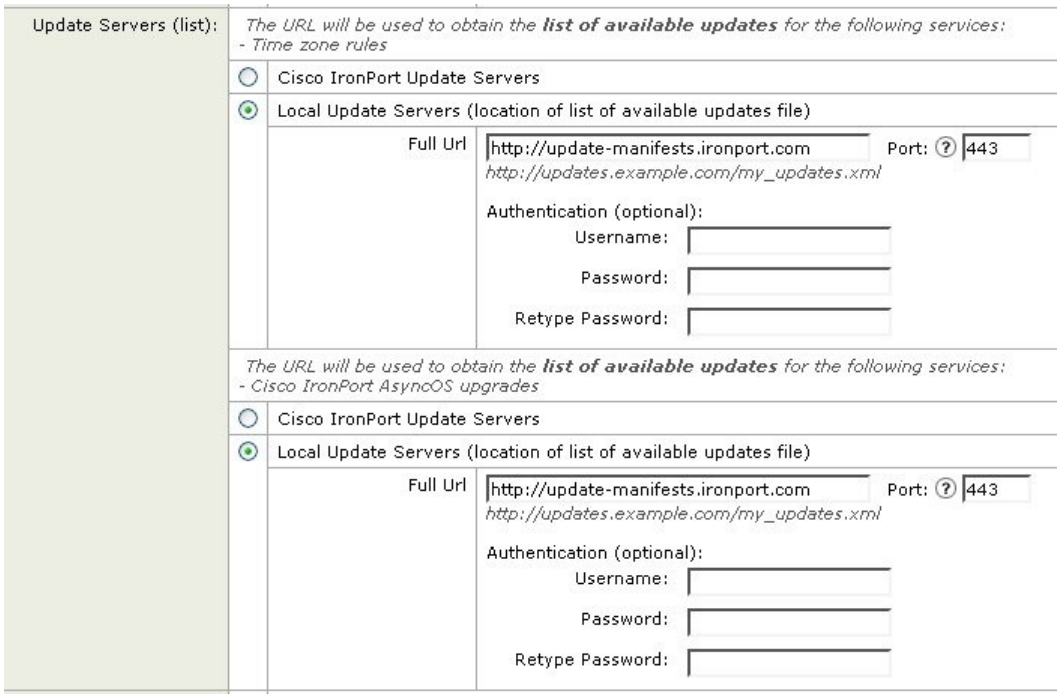


表 *44:* 采用严格防火墙策略的环境的静态地址

部分	设置	静态 URL/IP 地址和端口
更新服务器（映像）(Update Servers [images])：	基本 URL（除了时区规则和 AsyncOS 升级外的所有服务）	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）(Update Servers [list])：	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

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 292 页中的说明配置此操作程序中的设置。

步骤 3 在**更新服务器（映像）(Update Servers [images])** 部分中，指定要从中下载更新映像的服务器。

步骤 4 指定要从中下载 AsyncOS 升级映像的服务器：

a) 在同一部分的底部，点击**点击以将不同的设置用于 AsyncOS 升级**链接。

b) 指定用于下载 AsyncOS 升级的映像的服务器设置。

步骤 5 在**更新服务器（列表）(Update Servers [lists])** 部分中，指定用于获取可用更新和 AsyncOS 升级列表的服务器。

顶部的子部分适用于更新。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 验证结果是否符合您的期望：

如果您尚未查看“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)**。

某些 URL 可能将“asyncos”目录附加到服务器 URL。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	相应操作
查看有关最新升级的详细信息	将鼠标悬停在升级通知上。
查看所有可用升级的列表	点击通知中的向下箭头。
关闭当前通知。 设备在新升级可用之前不会再显示其他通知。	点击向下箭头，然后选择**清除通知 (Clear the notification)**，然后点击**关闭 (Close)**。
防止将来通知（仅限有管理员权限的用户。）	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

开始之前

请参阅确定升级和更新的网络要求 ，第 289 页所列的网络要求。

步骤 1 采取措施防止或最大限度减少数据丢失：

- 确保对于将传输的每种数据类型，新设备有足够的磁盘容量，并且具有相同或更大的空间分配。请参阅关于磁盘空间最大值和分配 ，第 321 页。
- 如果您收到任何磁盘空间警告，请在升级之前解决任何磁盘空间问题。

步骤 2 将 XML 配置文件保存到设备外。请在保存和导出当前的配置文件 ，第 315 页参阅相关警告。

如果您出于任何原因需要恢复为升级前的版本，则将需要此文件。

步骤 3 如果您使用安全列表/阻止列表功能，请将列表导出到设备外。

依次点击**管理设备 (Management Appliance) > 系统管理 (System Administration) > 配置文件 (Configuration File)**，然后向下滚动。

步骤 4 在从 CLI 运行升级时使用 **suspendlistener** 命令暂停侦听程序。如果您从 GUI 执行升级，侦听程序会自动暂停。

步骤 5 排空邮件队列和传送队列。

步骤 6 验证升级设置的配置符合您的要求。请参阅配置升级和服务更新设置，第 292 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。

注释 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，升级将在下载时立即安装。升级流程开始时，系统会显示横幅 10 秒。显示此横幅时，您可以选择在下载开始之前输入 Control-C 以退出升级流程。

开始之前

- 选择您是直接从思科下载升级还是从您网络上的服务器托管升级映像。然后设置您的网络，以支持您选择的方法。然后配置设备，以从您选择的资源获取升级。请参阅选择升级方法：远程或流传输，第 290 页和配置升级和服务更新设置，第 292 页。
- 在安装升级之前，按照升级之前：重要步骤，第 296 页中的说明执行操作。

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	相应操作
通过单一操作下载并安装升级	点击**下载并安装 (Download and Install)**。 如果您已下载一个安装程序，则系统将提示您覆盖现有下载。
下载升级安装程序	点击**仅下载 (Download only)**。 如果您已下载一个安装程序，则系统将提示您覆盖现有下载。 系统在后台下载安装程序，不中断服务。
安装下载的升级安装程序	点击**安装 (Install)**。 仅当安装程序已下载时，系统才会显示此选项。 “安装 (Install)”选项下方将标注要安装的 AsyncOS 版本。

步骤 4 除非安装的是先前下载的安装程序，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。

注释 无法使用 GUI 中的“配置文件”页面或 CLI 中的 `loadconfig` 命令加载带屏蔽密码的配置文件。

c) 如果您想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 (Proceed)**。

步骤 7 如果您正在进行安装：

a) 请准备对安装过程中的提示做出响应。

在您做出响应之前，安装过程将会暂停。

系统会在页面顶部附近显示进度条。

b) 在提示符下，点击**立即重启 (Reboot Now)**。

注释 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。

下一步做什么

- 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：

  当您准备安装升级时，请从一开始就遵循这些说明，包括“准备工作”部分中的必备条件，但选择“安装”(Install) 选项。
- 如果您已安装升级，请参阅升级后的注意事项 ， 第 299 页。

查看后台下载状态、取消或删除后台下载

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	相应操作
查看下载状态	查看页面的中间。 如果没有进行中的下载且没有已完成的下载等待安装，您不会看到下载状态信息。 升级状态也会出现在升级日志中。

目标	相应操作
取消下载	点击页面中间的**取消下载 (Cancel Download)** 按钮。 仅当下载正在进行中时，系统才会显示此选项。
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。 仅当安装程序已下载时，系统才会显示此选项。

升级后的注意事项

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 192 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 314 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 AsyncOS 的某个较早版本

您可以将 AsyncOS 恢复到以前的某个合格版本以用于紧急用途。

如果要清除设备上的所有数据并从全新的干净配置开始，您还可以恢复到当前运行的内部版本。

相关主题

- 关于恢复影响的重要注意事项， 第 299 页
- 恢复 AsyncOS ， 第 300 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。此命令会永久破坏所有现有的配置和数据。此外，它会中断邮件处理，直到重新配置设备为止。

恢复不会影响功能密钥或虚拟设备许可证到期日期。

恢复 AsyncOS

开始之前

- 备份或保存您要保管到设备之外位置的任何数据。
- 您必须具有要恢复到的版本的配置文件。配置文件不反向兼容。
- 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。

步骤 1 确保您具有要恢复到的版本的配置文件。配置文件不反向兼容。

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，您可以将该文件通过邮件发送给自己或通过 FTP 传送该文件。执行此操作的一种简单方法是运行 `mailconfig` CLI 命令，该命令将您设备上的当前配置文件通过邮件发送到指定的邮件地址。

注释 这不是您在恢复之后要下载的配置文件。

步骤 3 如果您使用安全列表/阻止列表功能，请将安全列表/阻止列表数据库导出到另一台机器中。

步骤 4 暂停邮件安全设备上的任何侦听程序。

步骤 5 等待邮件队列为空。

步骤 6 登录到您要恢复的设备的 CLI。

运行 `revert` 命令时，系统会发出多个警告提示。一旦接受这些警告提示，恢复操作会立即执行。因此，在完成预防措施之前，不要开始恢复过程。

步骤 7 从命令行提示符中，键入 **`revert`** 命令并回应提示。

以下示例显示 **`revert`** 命令：

示例：

```
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.
```

```
Do you want to continue? yes
Are you sure you want to continue? yes
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 等待设备进行二次重启。

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”更新。

步骤 11 在完成 URL 类别更新后，加载您要恢复到的版本的 XML 配置文件。

步骤 12 如果您使用安全列表/阻止列表功能，请导入并恢复安全列表/阻止列表数据库。

步骤 13 重新启用邮件安全设备上的任何侦听程序。

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。

注释 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

服务更新定期可供下载。要为这些下载指定设置，请参阅配置升级和服务更新设置，第 292 页

相关主题

- 关于网络使用控制的 URL 类别集更新 ，第 301 页
- 配置升级和服务更新设置，第 292 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 212 页
- URL 类别集更新和报告 ，第 98 页

为生成的邮件配置返回地址

对于以下类型的情况，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、用户及域名。您还可以选择为域名使用虚拟网关域。

使用 GUI 中的“系统管理”(System Administration) 菜单上提供的“回信地址”(Return Addresses) 页面，或在 CLI 中使用 **addressconfig** 命令。

要在 GUI 中修改系统生成的邮件的回信地址，请在“回信地址”(Return Addresses) 页面上点击**编辑设置**。对要修改的一个或多个地址进行更改，点击**提交**，然后确认您所做的更改。

管理警报

设备会向您发送关于事件的邮件警报。

目标	相应操作
将不同类型的警报发送给不同的管理用户	依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 警报 (Alerts)**。 如果您在系统设置期间启用了“自动支持”(AutoSupport)，默认情况下，您指定的的邮件地址将接收所有严重性和分类的警告。您可以随时更改配置。 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”(AutoSupport) 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 303 页 请参阅思科自动支持 (Cisco AutoSupport) ， 第 304 页
查看最近警报的列表 管理此列表的设置	请参阅查看最近的警报 ， 第 303 页
请参阅警报及其说明的列表	请参阅： 硬件警报说明 ， 第 304 页。 系统警报说明 ， 第 304 页
了解警报传送机制	请参阅警报传送 ， 第 303 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 304 页。
- 系统警报。请参阅系统警报说明 ， 第 304 页。
- 更新警报。

警报可以具有以下严重性：

- 严重 (Critical)：需要您立即关注的问题

- 警告 (Warning)：需要进一步监控和可能需要立即关注的问题或错误
- 信息 (Info)：在此设备的路由功能中生成的信息

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。

警报邮件系统不与 AsyncOS 共享相同的配置，这意味着警报邮件的传送可能与其他邮件的传送不太一样：

- 使用标准 DNS MX 和记录查找传送警报邮件。
  - 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。它们也不受邮件过滤器或内容过滤器影响。
  - 警报消息不通过传送队列传送，因此不会受退回配置文件和目标控制限制的影响。

查看最近的警报

目标	相应操作
查看最近警报的列表	具有“管理员”(Administrator) 和操作员 (operator) 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**查看警报排行榜 (View Top Alerts)** 按钮。 即使在通过邮件发送警报时，警报也在现场。
对列表排序	点击列标题。
指定要保存在列表中的最大警报数	使用命令行界面中的 alertconfig 命令
禁用此功能	使用命令行界面中的 alertconfig 命令将最大警报数设置为零 (0)。

关于重复警报

您可以指定 AsyncOS 发送重复警报前等待的初始秒数。如果您将该值设置为 0，则不会发送重复警报摘要；相反，会无任何延迟地发送所有重复警报（这可能导致在短时间内发送大量的邮件）。发送重复警报之间等待的秒数（警报间隔）在每次警报报送后增加。增加的秒数是初始等待秒数加上

上次间隔的两倍。因此，如果要等待的秒数为 5 秒，则会在 5 秒、15 秒、35 秒、75 秒、155 秒、315 秒（其余类推）时发送警报。

最终，间隔可能变大。您可以通过发送重复警报前等待的最大秒数字段为间隔之间的等待秒数设置一个上限。例如，如果您将初始值设置为 5 秒，将最大值设置为 60 秒，则将在 5 秒、15 秒、35 秒、60 秒、120 秒（其余类推）时发送警报。

思科自动支持 (Cisco AutoSupport)

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。自动支持每周还发送注明系统正常运行时间、**status** 命令的输出以及所使用的 AsyncOS 版本等信息的报告。

默认情况下，设置为接收“系统”(System) 警报类型的“信息”(Information) 严重性级别警报的警报收件人会收到向思科发送的每个消息的副本。如果您不想在内部发送每周的警报邮件，可禁用此功能。要启用或禁用此功能，请依次选择**管理设备 > 系统管理 > 警报**，然后点击编辑设置。

默认情况下，如果启用了“自动支持”(AutoSupport)，则会将每周的“自动支持”(AutoSupport) 报告发送给设置为接收“信息”(Information) 级别系统警报的警报收件人。

硬件警报说明

表 *45:* 硬件警报说明

警报名称	说明	严重性
INTERFACE.ERRORS	当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	在磁盘分区达到 95% 容量（和 95%、96%、97%，其余类推）时发送。	严重
SYSTEM.RAID_EVENT_ALERT	当出现严重 RAID 事件时发送。	警告
SYSTEM.RAID_EVENT_ALERT_INFO	当出现 RAID 事件时发送。	信息

系统警报说明

表 *46:* 系统警报说明

警报名称	说明	严重性
COMMON.APP_FAILURE	当出现未知应用故障时发送。	严重

警报名称	说明	严重性
COMMON.KEY_EXPIRED_ALERT	当功能密钥到期时发送。	警告
COMMON.KEY_EXPIRING_ALERT	当功能密钥将要到期时发送。	警告
COMMON.KEY_FINAL_EXPIRING_ALERT	作为功能密钥将要到期的最后通知发送。	警告
DNS.BOOTSTRAP_FAILED	当设备无法联系根 DNS 服务器时发送。	警告
COMMON.INVALID_FILTER	当遇到无效过滤器时使用。	警告
IPBLOCKD.HOST_ADDED_TO_WHITELIST IPBLOCKD.HOST_ADDED_TO_BLACKLIST IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST	警报消息： • 由于 SSH DOS 攻击，位于 <IP 地址> 的主机已被添加到黑名单 (The host at <IP address> has been added to the blacklist because of an SSH DOS attack)。 • 位于 <IP 地址> 的主机已被永久添加到 SSH 白名单 (The host at <IP address> has been permanently added to the ssh whitelist)。 • 位于 <IP 地址> 的主机已从黑名单中删除 (The host at <IP address> has been removed from the blacklist)。 如果两分钟内出现超过 10 次失败尝试，则尝试通过 SSH 与设备连接但未提供有效证书的 IP 地址会被添加到 SSH 阻止列表中。 当用户从相同 IP 地址登录成功时，该 IP 地址会被添加到白名单中。 允许访问白名单中的地址，即使它们也在阻止列表中也是如此。	警告
LDAP.GROUP_QUERY_FAILED_ALERT	当LDAP组查询失败时发送。	严重

警报名称	说明	严重性
LDAP.HARD_ERROR	当LDAP完全失败（尝试所有服务器后）时发送。	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 利用率超过系统资源保护阈值时发送。	严重
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	当邮件队列超载且已启用系统资源保护时发送。	严重
MAIL.RES_CON_START_ALERT.QUEUE	当队列利用率超过系统资源保护阈值时发送。	严重
MAIL.RES_CON_START_ALERT.WORKQ	当系统因工作队列大小过大暂停侦听程序时发送。	严重
MAIL.RES_CON_START_ALERT	当设备进入“资源保护”模式时发送。	严重
MAIL.RES_CON_STOP_ALERT	在设备退出“资源节约”(Resource Conservation) 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 未作为根运行而无法调整时间时发送。	警告
PERIODIC_REPORTS.DOMAIN_REPORT.DOMAIN_FILE_ERRORS	在域规格文件中发现错误时发送。	严重
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_EMPTY	在域规格文件为空时发送。	严重
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_MISSING	在未找到域规格文件时发送。	严重
REPORTD.DATABASE_OPEN_FAILED_ALERT	报告引擎无法打开数据库时发送。	严重

警报名称	说明	严重性
REPORTD.AGGREGATION_DISABLED_ALERT	当系统耗尽磁盘空间时发送。当日志条目的磁盘使用率超过日志使用率阈值时，reportd 会禁用汇聚，并发送警报。	警告
REPORTING.CLIENT.UPDATE_FAILED_ALERT	报告引擎无法保存报告数据时发送。	警告
REPORTING.CLIENT.JOURNAL.FULL	报告引擎无法存储新数据时发送。	严重
REPORTING.CLIENT.JOURNAL.FREE	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	在报告引擎无法生成报告时发送。	严重
PERIODIC_REPORTS.REPORT_TASK. EMAIL_FAILURE_ALERT	当无法发送报告时发送。	严重
PERIODIC_REPORTS.REPORT_TASK. ARCHIVE_FAILURE_ALERT	当无法存档报告时发送。	严重
SENDERBASE.ERROR	当处理 SenderBase 的响应期间出现错误时发送。	信息
SMAD.ICCM.ALERT_PUSH_FAILED	在一个或多个主机的配置推送失败时发送。	警告
SMAD.TRANSFER.TRANSFERS_STALLED	在 SMA 日志无法获取跟踪数据（两小时内）或报告数据（六小时内）时发送。	警告
SMTPAUTH.FWD_SERVER_FAILED_ALERT	当无法访问 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	当重启期间无法关闭系统时发送。	警告
SYSTEM.HERMES_SHUTDOWN_FAILURE. SHUTDOWN	当无法关闭系统时发送。	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	在禁用为思科支持服务创建的隧道时发送。	信息
SYSTEM.SERVICE_TUNNEL.ENABLED	在启用为思科支持服务创建的隧道时发送。	信息

更改网络设置

本部分介绍用于配置设备的网络操作的功能。使用这些功能可以直接访问您在运行系统设置向导，第 11 页使用“系统设置向导”(System Setup Wizard) 配置的主机名、DNS 和路由设置。

功能介绍如下：

- `sethostname`
- DNS 配置（在 GUI 中或通过在 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。您必须输入完全限定的主机名。s ethostname 命令设置内容安全设备的名称。新的主机名不会生效，直到您发出 commit 命令。

sethostname 命令

```
oldname.example.com> sethostname
[oldname.example.com]> mail3.example.com
oldname.example.com>
```

为使主机名更改生效，必须输入 commit 命令。成功提交主机名更改后，系统会在 CLI 提示中显示新名称：

```
oldname.example.com> commit
Please enter some comments describing your changes:
[]> Changed System Hostname
Changes committed: Mon Jan 04 12:00:01 2010
```

新的主机名显示在提示符处，如下所示：mail3.example.com>

配置域名系统设置

您可以通过 GUI 中的“管理设备”(Management Appliance) >“网络”(Network) >“DNS”(DNS) 页面或通过 dnsconfig 命令，配置内容安全设备的域名系统 (DNS) 设置。

您可以配置以下设置：

- 是要使用互联网的 DNS 服务器还是您自己的 DNS 服务器，以及要使用哪些服务器
- 要用于 DNS 流量的接口
- 在使反向 DNS 查找超时之前要等待的秒数
- 清除 DNS 缓存

指定 DNS 服务器

AsyncOS 可以使用互联网根 DNS 服务器、您自己的 DNS 服务器或您指定的互联网根 DNS 服务器和权威 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，您应该也设置 in-addr.arpa (PTR) 条目。例如，如果要将“.eng”查询定向到名称服务器 1.2.3.4，并且所有 .eng 条目均在 172.16 网络中，则应将“eng,16.172.in-addr.arpa”指定为分离 DNS 配置中的域。

多个条目和优先级

对于您输入的每个 DNS 服务器，您可以指定数字优先级。AsyncOS 会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 会尝试使用下一优先级的服务器。如果您为相同优先级的 DNS 服务器指定多个条目，系统会在每次进行查询时对该优先级的 DNS 服务器列表进行随机排序。然后系统会花较短的时间等待第一个查询到期或“超时”，然后花较长的时间等待第二个查询，依此类推。时长取决于已配置的DNS服务器和优先级的确切总数。任何特定优先级的所有IP地址的超时长度都一样。第一个优先级获得最短的超时；每个后续优先级获得较长的超时。此外，超时期限约为 60 秒。如果您有一个优先级，则该优先级的每台服务器的超时是 60 秒。如果您有两个优先级，则第一个优先级的每台服务器的超时是15秒，第二个优先级的每台服务器的超时是 45 秒。对于三个优先级，超时为 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 *47: 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 会在优先级为 0 的两台服务器之间随机选择。如果其中一台优先级为 0 的服务器停机，会使用另一台服务器。如果优先级为 0 的两个服务器都已关闭，则使用优先级为 1 的服务器 (1.2.3.6)，然后最后使用优先级为 2 (1.2.3.7) 的服务器。

优先级为 0 的两个服务器的超时期限相同，优先级为 1 的服务器的超时期限较长，优先级为 2 的服务器的超时期限更长。

使用 Internet 根服务器

AsyncOS DNS 解析器旨在适应高性能邮件传送所需的大量同时 DNS 连接。

注释 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”。也就是说，系统通过执行双 DNS 查找获得远程主机的 IP 地址并验证其有效性。这包括在所连接主机的 IP 地址上进行的反向 DNS (PTR) 查找，以及随后根据 PTR 查找结果进行的正向 DNS (A) 查找。接着，系统会检查 A 查找的结果是否与 PTR 查找的结果匹配。如果结果不匹配，或者如果 A 记录不存在，则系统只使用 IP 地址与主机访问表 (HAT) 中的条目相匹配。此特定超时期限仅适用于此查找，并且与多个条目和优先级，第 309 页中讨论的一般 DNS 超时不相关。

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。如果将该值设置为 0 秒，则系统不会尝试进行反向 DNS 查找，而是立即返回标准超时响应。

DNS 警报

偶尔，系统会在设备重启时生成消息为“未能引导 DNS 缓存”(Failed to bootstrap the DNS cache) 的警报。该消息表示系统无法与其主 DNS 服务器联系，如果 DNS 子系统在建立网络连接之前上线，则会在启动时发生这种情况。如果此消息在其他时间出现，则可能表明网络问题或DNS配置没有指向一个有效的服务器。

清除 DNS 缓存

GUI 中的**清除缓存**按钮或 d nsflush 命令（有关 dnsflush 命令的详细信息，请参阅《IronPort AsyncOS CLI 参考指南》，可从文档，第 393 页中指定的位置获取）将清除 DNS 缓存中的所有信息。您可以选择在已对您的本地DNS系统进行更改时使用此功能。该命令立即发生，并可能会在缓存重新注入期间导致临时性能降低。

通过图形用户界面配置 DNS 设置

步骤 1 依次选择**管理设备 > 网络 > DNS** 页面，然后点击**编辑设置**按钮。

步骤 2 选择是要使用互联网的根 DNS 服务器还是您自己的内部 DNS 服务器，并指定权威 DNS 服务器。

步骤 3 如果要使用您自己的 DNS 服务器或指定权威 DNS 服务器，请输入服务器 ID 并点击**添加行 (Add Row)**。对每个服务器重复此步骤。输入您自己的 DNS 服务器时，请也指定优先级。有关详细信息，请参阅指定 DNS 服务器，第 309 页。

步骤 4 选择一个用于 DNS 流量的接口。

步骤 5 输入在取消反向 DNS 查找之前要等待的秒数。

步骤 6 （可选）通过点击**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 > 网络 > 路由**页面管理静态路由，也可以在 CLI 中通过使用 **routeconfig** 命令执行此操作。

- 在 GUI 中管理静态路由，第 311 页
- 修改默认网关（GUI），第 311 页

在 GUI 中管理静态路由

您可以通过使用“管理设备”(Management Appliance) >“网络”(Network) >“路由”(Routing) 页面创建、编辑或删除静态路由。您还可以通过此页面修改默认网关。

步骤 1 在**管理设备 > 网络 > 路由**页面上，点击路由列表中的**添加路由**。然后输入路由的名称。

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）

步骤 1 点击“路由”(Routing) 页面上的路由列表中的“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

您可以在 GUI 中通过“管理设备”>“网络”>“路由”页面（请参阅修改默认网关（GUI），第 311 页）配置默认网关，也可以在 CLI 中通过使用 setgateway 命令执行此操作。

指定安全通信协议

- SSL v3 不安全，请勿使用。
- 您可以选择用于以下各项的通信协议：
  - 更新器服务器
  - 最终用户对垃圾邮件隔离区的访问
  - 基于网络的设备管理界面
  - LDAPS
- 要查看当前选定协议和可用选项或者更改协议，请在命令行界面中使用 sslconfig 命令。
- 思科更新服务器不支持 SSL v3。
- 如果您使用本地（远程）更新服务器，且对于所有其他服务和网络浏览器，您使用的服务器和工具必须支持和启用您所选择的协议。
- 必须为您使用的每项服务启用一个可用选项。
- 使用 sslconfig 命令所做的更改需要确认。
- 在您确认使用 sslconfig 命令所做的更改后，受影响的服务会短暂中断。

配置系统时间

注释 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，请参阅安全管理设备如何收集报告的数据，第 20 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	相应操作
设置系统时间	**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 313 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，第 313 页 • 更新时区文件，第 313 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。

默认的 NTP 服务器为 time.sco.cisco.com。

如果您将使用外部 NTP 服务器，包括默认的 NTP 服务器，请通过防火墙打开必需的端口。请参阅防火墙资讯，第 385 页

相关主题

- 配置系统时间，第 312 页
- 手动更新时区文件，第 314 页

选择 GMT 偏移

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**。

步骤 3 从报告地区列表选择 GMT 时差。“时区设置”(Time Zone Setting) 页面更新为在“时区”(Time Zone) 页面中包括 GMT 时差。

步骤 4 在“时区”(Time Zone) 字段中选择时差。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

每当任何国家/地区的时区规则发生更改时，必须更新设备上的时区文件。

- 自动更新时区文件，第 313 页
- 手动更新时区文件，第 314 页

自动更新时区文件

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**为时区规则启用自动更新 (Enable automatic updates for Time zone rules)** 复选框。

步骤 3 输入时间间隔。点击页面上的？了解重要信息。

步骤 4 提交并确认更改。

手动更新时区文件

步骤 1 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 时区设置 (Time Settings)**。

步骤 2 查看**时区文件更新 (Time Zone File Updates)** 部分。

步骤 3 如果存在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 314 页
导入保存的配置	保存和导入配置设置 ，第 314 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 154 页
重置配置	将配置重置为出厂默认设置，第 277 页

保存和导入配置设置

注释 此部分中介绍的配置文件用于配置安全管理设备。管理网络安全设备，第 191 页一章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) 格式维护。

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。如果您在配置设备时出现错误，您可以“回滚”至最近保存的配置文件。
- 您可以下载现有配置文件，以快速查看设备的所有配置。（许多较新的浏览器具有直接显示 XML 文件的功能。）这可以帮助你对当前配置中可能存在的小错误（如印刷错误）进行故障排除。
- 您可以下载现有配置文件，对其进行更改，并将其上传到同一设备。实际上，这会“绕过”CLI 和 GUI 进行配置更改。
- 您可以通过 FTP 上传整个配置文件，也可以将配置文件的各部分直接粘贴到 CLI。
- 因为文件采用 XML 格式，因此还提供一个描述配置文件中所有 XML 条目的相关文档类型定义 (DTD)。您可以下载 DTD，以在上传 XML 配置文件之前对其进行验证。（可以在互联网上很容易地获得 XML 验证工具。）

- 您可以使用配置文件加快配置另一台设备，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 154 页
- 将配置重置为出厂默认设置 ， 第 277 页
- 回滚到以前已确认的配置 ， 第 317 页

保存和导出当前的配置文件

使用**管理设备 > 系统管理 > 配置文件**页面上的“当前配置”部分，您可以将当前配置文件保存到本地计算机，将其保存在设备上（放置在 FTP/SCP 根的配置目录中），或通过邮件发送到指定的地址。

屏蔽密码

（可选）通过选中该复选框屏蔽用户的密码。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“*****”。

注释 带有屏蔽的密码的配置文件不能加载回 AsyncOS 中。

加载配置文件

必须已从与您将加载配置的设备运行相同 AsyncOS 版本的设备保存配置文件。

无法加载带屏蔽密码的配置文件。

无论使用哪种方法，您都必须在配置的顶部包含以下标记：

```
<?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。如果在您使用 loadconfig 命令时，命令行中报告了验证错误，则不会加载更改。可以下载 DTD 先在设备之外验证配置文件，再上传它们。

在任一导入方法中，您都可以导入整个配置文件（在最高级别标签：<config></config> 之间定义的信息），或导入配置文件的一个完整且唯一的子部分，只要它包含声明标签（上文）并包含在 <config></config> 标签内。

“完整”意味着包含 DTD 定义的给定子部分的整个开始和结尾标记。例如，上传或粘贴以下代码会导致验证错误：

```
<?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，系统只能有一个主机名，因此允许加载以下代码（包括声明和 <config></config> 标签）：

```
<hostname>mail4.example.com</hostname>
```

但是，系统可以定义多个侦听程序，每个侦听程序定义不同的收件人访问表，因此，只上传以下代码会被视为模棱两可：

```
<rat>
   <rat_entry>
     <rat_address>ALL</rat_address>
     <access>RELAY</access>
   </rat_entry>
 </rat>
```

由于该代码模棱两可，因此不被允许，即使其语法是“完整的”。

⚠

注意 上传或粘贴配置文件或配置文件的子部分时，您可能会清除可能在等待的未提交更改。

空标签与遗漏的标签

上传或粘贴配置文件的部分时，请谨慎使用。如果不包含标记，则加载配置文件时，配置中的值不会被修改。但是，如果包含空标记，则其配置设置将会被清除。

例如，上传以下代码会从系统中删除所有侦听程序：

```
<listeners></listeners>
```

⚠

注意 在上传或粘贴配置文件的子部分时，您可以将自己与 GUI 或 CLI 断开连接，并毁坏大量的配置数据。如果无法使用其他协议、串行接口或管理端口上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，如果您不确定DTD定义的确切配置语法，请勿使用此命令。在加载新的配置文件之前，务必先备份配置数据。

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推送的日志订用），`loadconfig` 命令不会警告您缺少密码。FTP 推送失败并生成警报，直到您使用 `logconfig` 命令配置正确的密码为止。

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。每当您发出 showconfig、saveconfig 或 mailconfig 命令时，文件中会指定编码属性：

```
<?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 277 页。

回滚到以前已确认的配置

您可以将配置回滚到以前已确认的配置。

在命令行界面中使用 rollbackconfig 命令选择最近确认的十个配置之一。

如果在提示确认回滚时输入 No，将在您下次确认更改时确认回滚。

只有具备“管理员”(Administrator) 访问权限的用户可以使用 rollbackconfig 命令。

注释 恢复先前的配置时，不会生成日志消息或警报。

注释 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 277 页）
- publishconfig
- backupconfig（请参阅备份安全管理设备数据，第 281 页）

showconfig、mailconfig 和 saveconfig 命令

对于配置命令 showconfig、mailconfig 和 saveconfig，系统将会提示您选择是否要在用邮件发送或显示的文件中包括密码。选择不包括密码会将任何密码字段留空。如果您关注安全漏洞，您可以选择不包括密码。但是，在使用 loadconfig 命令加载时，不含密码的配置文件会失败。请参阅关于加载日志订阅密码的注意事项，第 316 页。

注释 在保存、显示或通过邮件发送配置文件时，如果您选择包括密码（对“是否要包括密码？”回答是“是”），密码会被加密。不过，私钥和证书会包括在未加密的 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 命令可通过邮件将当前配置发送给用户。名为 config.xml 的 XML 格式的配置文件将附加到邮件。

```
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]> y
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）存储和保存到配置目录中。

```
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]> y
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。您可以使用以下两种方法之一加载信息：

- 将信息放置在 configuration 目录中，然后将其上传
- 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 315 页。

rollbackconfig 命令

请参阅回滚到以前已确认的配置，第 317 页。

publishconfig 命令

使用 `publishconfig` 命令可通过主配置发布更改。语法如下：

publishconfig *config_master* [*job_name*] [*host_list* | *host_ip*

其中 *config_master* 是受支持的主配置，此版本的版本说明中的兼容性矩阵列出了受支持的主配置，该版本说明位于 http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html。此关键字是必需的。关键字 *job_name* 是可选的，如果未指定此关键字，则会生成此关键字。

关键字 *host_list* 是要发布的 WSA 设备的主机名或 IP 地址的列表，如果未指定，则将发布到分配给主配置的所有主机。可选的 *host_ip* 可以是用逗号分隔的多个主机 IP 地址。

要验证 **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，您可以转到“发布历史记录”(Publish History) 页面：依次选择**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

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IP 接口和访问设备，第 373 页。

步骤 2 将整个配置文件或配置文件的子部分放到设备的配置目录中，或者编辑通过 `saveconfig` 命令创建的现有配置。

步骤 3 在 CLI 之内，使用 `loadconfig` 命令加载您在步骤 2 中放入目录的配置文件，或者直接将文本（XML 语法）粘贴到 CLI 中。

在本示例中，将会上传名为 changed.config.xml 的文件，并提交更改：

示例：

```
mail3.example.com>
l
oadconfig
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
```

在本示例中，将直接在命令行处粘贴一个新的配置文件。（请注意，在空白行上按 Ctrl-D 将结束粘贴命令。）然后“系统设置向导”(System Setup Wizard) 用于更改默认主机名、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，第 11 页。）最后，确认更改。

示例：

```
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
Please enter some comments describing your changes:
[]> pasted new configuration file and changed default settings
```

管理磁盘空间

您可以在组织使用的各项功能之间分配可用的磁盘空间，最多可以分配可用的最大空间。

（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，您可以分配 2TB 以上的磁盘空间。对于运行 ESXi 5.1 的设备，限值为 2 TB。

注释 ESXi 中不支持减少磁盘空间。有关信息，请参阅 VMWare 文档。

要增加虚拟设备实例的磁盘空间，请执行以下步骤：

开始之前

仔细确定所需的磁盘空间。

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。

请参阅 VMWare 文档中有关更改虚拟磁盘配置的信息。

以下网址提供了有关 ESXi 5.5 的信息： http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html

步骤 3 转至**管理设备 > 系统管理 > 磁盘管理**，并验证您所做的更改是否已生效。

查看磁盘空间配额和使用情况

目标	请
查看设备上的总可用磁盘空间	依次选择**管理设备 > 系统管理 > 磁盘管理**。 查看“总分配空间”所显示的值 - 例如，已分配 184G，共 204G。
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)**，然后查看“集中服务”(Centralized Services) 部分。

关于磁盘空间最大值和分配

注释 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。如果同时启用两者，则邮件和 Web 报告数据共享该空间，并且按先到先得的原则分配空间。

- 如果您启用集中 Web 报告，但未为报告分配磁盘空间，则在分配磁盘空间之前，集中 Web 报告功能将无法正常工作。
- 在将“其他”(Miscellaneous) 配额减少到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”配额的磁盘空间 ，第 322 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 176 页和邮件在隔离区中的保留时间 ，第 176 页。
- 对于其他数据类型，如果您将现有空间分配减少到当前使用量以下，则最旧的数据会被删除，直到所有数据均可容纳在新的空间分配量中为止。
- 如果新的配额大于当前已用的磁盘空间，您不会丢失数据。
- 如果您将空间分配设置为零，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。

要确保您可以收到这些警报，请参阅管理警报，第 302 页。

管理“其他”配额的磁盘空间

杂项配额包括系统数据和用户数据。您无法删除系统数据。您可以管理的用户数据包括以下类型的文件：

要管理	请
日志文件	转至**管理设备 > 系统管理 > 日志订用**，然后： • 点击“大小”(Size) 列标题以查看哪些日志消耗最多的磁盘空间。 • 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，减少滚动文件大小。
数据包捕获	依次转至**帮助和支持**（屏幕右上侧附近）> **数据包捕获**。删除任何不需要的捕获。
配置文件 （这些文件不太可能消耗太多磁盘空间。）	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 375 页
配额大小	依次转至**系统管理 (System Administration) > 磁盘管理 (Disk Management)**。

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 320 页。

开始之前

- 更改磁盘分配可能影响现有数据或功能可用性。请参阅关于磁盘空间最大值和分配，第 321 页提供的信息。
- 您可以在隔离区中临时创建空间，方法是从隔离区中手动放行或删除邮件。

步骤 1 选择**管理设备 > 系统管理 > 磁盘管理**。

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)** 页面上，输入分配给每项服务的磁盘空间量（以千兆字节为单位）。

步骤 4 点击**提交**。

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。

调整邮件安全设备的系统运行状况图中的参考阈值

受管邮件安全设备的运行状况可在系统容量页面，第 69 页所述的“系统容量”-“系统负载”报告中进行监控。这些报告中会出现阈值线。在思科内容安全管理设备上，此行指示一个视觉指示器，不表示邮件安全设备上配置的阈值设置。此行是适用于所有系统负载图的单个引用值。

注释 要接收与这些阈值相关的警报，请在每台受管邮件安全设备上配置这些阈值。有关信息，请参阅适用于您的邮件安全设备版本的用户指南或联机帮助中有关为系统运行状况配置阈值的信息。您也可以从各台设备运行按需的系统运行状况检查。请参阅适用于您的邮件安全设备版本的用户指南或联机帮助中有关检查设备运行状况的信息。

步骤 1 点击**管理设备 > 系统管理 > 系统运行状况**。

步骤 2 点击**编辑设置**。

步骤 3 配置选项。

选项	说明
CPU 总体使用率 (Overall CPU Usage)	默认值：85%
内存页面交换 (Memory Page Swapping)	默认值：5000 页
工作队列中的最大邮件数 (Maximum Messages in Work Queue)	默认值：500 封邮件

步骤 4 提交并确认更改。

使用 SAML 2.0 的 SSO

• 如何为垃圾邮件隔离区配置 SSO ， 第 325 页

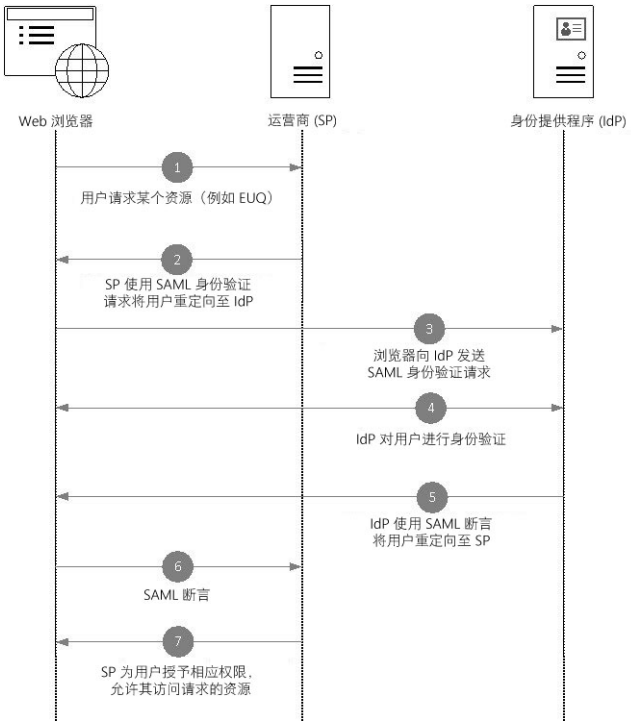
关于 SSO 和 SAML 2.0

思科内容安全管理设备现在支持SAML 2.0 SSO，以便最终用户可以使用在其组织内访问其他启用了SAML 2.0 SSO的服务时使用的凭证访问垃圾邮件隔离区。例如，您已启用Ping身份作为您的SAML身份提供程序 (IdP) 并且具有已启用了 SAML 2.0 SSO 的 Rally、Salesforce 和 Dropbox 账户。将思科内容安全管理设备配置为支持 SAML 2.0 SSO 作为运营商 (SP) 时，最终用户将能够登录一次，并有权访问所有这些服务，包括垃圾邮件隔离区。

SAML 2.0 SSO 工作流

SAML 2.0 SSO 工作流显示在下图中：

图 *19: SAML 2.0 SSO* 工作流



工作流程

1. 终端用户使用网络浏览器从运营商（您的设备）请求资源。例如，终端用户点击垃圾邮件通知中的垃圾邮件隔离区链接。
2. 服务提供程序使用 SAML 身份验证请求将请求重定向到网络浏览器。
3. 网络浏览器将 SAML 身份验证请求中继到身份提供程序。
4. 身份提供程序对终端用户进行身份验证。身份提供程序会向终端用户显示登录页，然后终端用户登录。

5. 身份提供程序生成 SAML 断言并将其发送回网络浏览器。
6. 网络浏览器将 SAML 断言中继到服务提供程序。
7. 运营商授予对所请求资源的访问权限。

SAML 2.0 的准则和限制

Logout

当最终用户注销垃圾邮件隔离时, 它们不会从其他 SAML 2.0 SSO 启用的应用程序中注销。

总则

您只能在思科内容安全管理设备上配置服务提供程序和身份提供程序的一个实例。

管理员的垃圾邮件隔离区访问权限

如果要对垃圾邮件隔离区启用 SSO，请记住，管理员将无法再使用垃圾邮件隔离区 URL (http://<appliance_hostname>:<port>) 访问垃圾邮件隔离区。管理员可以使用网络界面（**邮件 > 邮件隔离区 > 垃圾邮件隔离区**）访问垃圾邮件隔离区。

如何为垃圾邮件隔离区配置 SSO

	请	更多信息
第 1 步	查看先决条件。	必备条件， 第 326 页
第 2 步	将设备配置为服务运营商。	将思科内容安全管理设备配置为服务提供程序， 第 326 页
第 3 步	[在 IDP 上] 配置身份提供程序以便与您的设备配合使用。	将身份提供程序配置为与思科内容安全管理设备通信， 第 327 页
第 4 步	配置设备上的身份提供程序设置。	在思科内容安全管理设备上配置身份提供程序设置， 第 329 页
第 5 步	在设备上启用垃圾邮件隔离区 SSO。	为垃圾邮件隔离区启用 SSO， 第 330 页
第 6 步	将新的身份验证机制通知给终端用户。	

必备条件

- 验证您的组织使用的身份提供程序是否受思科内容安全管理设备的支持。以下是受支持的身份提供程序：
  - Microsoft Active Directory 联合身份验证服务 (AD FS) 2.0
  - Ping Identity PingFederate 7.2
  - 思科网络安全设备 9.1
- 获取保护设备与身份提供程序之间通信所需的下列证书：
  - 如果希望设备对 SAML 身份验证请求进行签名，或者希望身份提供程序加密 SAML 断言，请获取自签名证书或来自受信任 CA 的证书以及关联的私钥。
  - 如果希望身份提供程序对 SAML 断言进行签名，请获取身份提供程序的证书。您的设备将使用此证书来验证已签名的 SAML 断言。

将思科内容安全管理设备配置为服务提供程序

开始之前

查看 必备条件，第 326 页

步骤 1 选择**管理设备 > 系统管理 > SAML**。

步骤 2 在“服务提供程序”部分下，点击**添加服务提供程序**。

步骤 3 输入下列详细信息：

字段	说明描述
配置文件名称	输入服务提供程序配置文件的名称。
配置设置	
实体 ID	输入服务提供程序的全局唯一名称（在本例中为您的设备）。服务提供程序实体 ID 的格式通常为一个 URI。
名称 ID 格式	身份提供程序指定 SAML 断言中的用户所应采用的格式。 此字段不可配置。配置身份提供程序时，您需要使用此值。
断言使用者 URL	在身份验证成功完成后，身份提供程序应将 SAML 断言发送到的 URL。在这种情况下，这是指向您的垃圾邮件隔离区的 URL。 此字段不可配置。配置身份提供程序时，您需要使用此值。

字段	说明描述
SP 证书	**注释** 私钥必须采用 .pem 格式。 **签名身份验证请求** 如果希望设备对 SAML 身份验证请求进行签名，请执行以下操作： **1.** 上传证书和相关的私钥。 **2.** 输入私钥密码。 **3.** 选择**签名请求**。 **解密已加密的断言** 如果计划将身份提供程序配置为加密 SAML 断言： **1.** 上传证书和相关的私钥。 **2.** 输入私钥密码。
签名断言	如果希望身份提供程序对 SAML 断言进行签名，请选择**签名断言**。 如果选择此选项，则必须将身份提供程序的证书添加到设备中。请参阅在思科内容安全管理设备上配置身份提供程序设置，第 329 页。
组织详细信息	输入组织的详细信息。 身份提供程序将在错误日志中使用此信息。
技术联系人	输入技术联系人的邮件地址。 身份提供程序将在错误日志中使用此信息。

步骤 4 点击**提交**。

步骤 5 记下“SSO 设置”页面上显示的服务提供商元数据（实体 ID 和断言客户 URL）以及在“服务提供商”页面上显示的名称 ID 格式。在身份提供程序上配置服务提供程序设置时，需要这些详细信息。

可以选择将元数据作为文件导出。点击**导出元数据**并保存元数据文件。某些身份提供程序允许您从元数据文件加载服务提供程序详细信息。

下一步做什么

配置要与您的设备通信的身份提供程序。请参阅将身份提供程序配置为与思科内容安全管理设备通信，第 327 页

将身份提供程序配置为与思科内容安全管理设备通信

开始之前

确保您已：

- 将您的设备配置为服务提供程序。请参阅将思科内容安全管理设备配置为服务提供程序，第 326 页。
- 已复制服务提供程序元数据详细信息或导出元数据文件。请参阅将思科内容安全管理设备配置为服务提供程序，第 326 页。

步骤 1 在身份提供程序中，执行以下操作之一：

- 手动配置服务提供程序（您的设备）的详细信息。
- 如果您的身份提供程序允许您从元数据文件加载服务提供程序详细信息，请导入元数据文件。

如果已将设备配置为对 SAML 身份验证请求进行签名或计划加密 SAML 断言，请确保将相关证书添加到身份提供程序中。

有关身份提供程序特定的说明，请参阅：

- 将 AD FS 2.0 配置为与思科内容安全管理设备进行通信，第 328 页
- 将 PingFederate 7.2 配置为与思科内容安全管理设备通信，第 329 页
- 《思科网络安全设备 *AsyncOS* 用户指南》http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html中的**将设备配置为身份提供程序**部分

步骤 2 记下身份提供程序元数据或将元数据导出为文件。

下一步做什么

配置设备上的身份提供程序设置。请参阅在思科内容安全管理设备上配置身份提供程序设置，第 329 页。

将 AD FS 2.0 配置为与思科内容安全管理设备进行通信

以下是将 AD FS 2.0 配置为与您的设备进行通信所需要执行的高级任务。有关完整和详细的说明，请参阅 Microsoft 文档。

- 将服务提供程序的（设备的）断言消费者 URL 添加为中继方。
- 在“中继方信任”>“标识符”>“中继方标识符”下输入服务提供程序的（设备的）的实体 ID。请确保此值与设备上“运营商”设置中的“实体 ID”值相同。
- 如果已将您的服务提供程序（设备）配置为发送已签名的 SAML 身份验证请求，请上传服务提供程序的证书（用于签名身份验证请求），证书采用.cer格式，在“中继方信任”>“属性”>“签名”下上传。
- 如果计划将 AD FS 配置为发送加密的 SAML 断言，请在“中继方信任”>“属性”>“加密”下上传 .cer 格式的运营商的（设备的）证书。
- 在“中继方信任”>“属性”>“高级”下将安全哈希算法设置为 SHA-1。
- 编辑声明规则并添加颁发转换规则，以将邮件地址的 LDAP 属性作为传出声明类型（邮件地址）发送。
- 添加自定义规则以在响应中包括 SPNameQualifier。下面是一个自定义规则示例：

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
 =
 c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<appliance-hostname>:83");
```

将 PingFederate 7.2 配置为与思科内容安全管理设备通信

以下是将 PingFederate 7.2 配置为与设备通信所需执行的高级任务。有关完整的详细说明，请参阅 Ping 标识文档。

- 将运营商（设备）的断言消费者 URL 添加为协议设置中的终端。
- 在“SP 连接”>“常规信息”>“合作伙伴的实体 ID (连接 ID)”下，输入运营商（设备）的实体 ID。请确保此值与设备上“运营商”设置中的“实体 ID”值相同。
- 如果已将运营商（设备）配置为发送已签名的 SAML 身份验证请求，请将运营商的证书上传到“签名验证”部分（“SP 连接”>“凭证”>“签名验证”>“签名验证证书”）。
- 如果计划将 PingFederate 配置为发送加密的 SAML 断言，请将运营商（设备）的证书上传到“签名验证”部分（“SP 连接”>“凭证”>“签名验证”>“选择 XML 加密证书”）。
- 编辑属性协定以发送 LDAP 属性-邮件地址（“属性源与用户查找”>“属性协定履行”）。

在思科内容安全管理设备上配置身份提供程序设置

开始之前

确保：

- 已配置身份提供程序以与您的设备通信。请参阅将身份提供程序配置为与思科内容安全管理设备通信，第 327 页。
- 复制了身份提供程序元数据详细信息或导出的元数据文件。

步骤 1 选择**管理设备** > **系统管理** > **SAML**。

步骤 2 在“身份提供程序”部分下，点击**添加身份提供程序**。

步骤 3 输入下列详细信息：

字段	说明描述
配置文件名称	输入身份提供程序配置文件的名称。
配置设置（手动配置身份提供程序设置)	
实体 ID	输入身份提供程序的全局唯一名称。身份提供程序实体ID的格式通常是 URI。
SSO URL	指定服务提供程序必须向其发送 SAML 身份验证请求的 URL。

字段	说明描述
证书	如果身份提供程序对 SAML 断言进行签名，则必须上传身份提供程序的签名证书。
配置设置（导入身份提供程序元数据）	
导入 IDP 元数据	点击**导入元数据**并选择元数据文件。

步骤 4 提交并确认更改。

下一步做什么

为垃圾邮件隔离区启用 SSO， 第 330 页

为垃圾邮件隔离区启用 SSO

开始之前

确保您：

- 已配置**管理设备** > **系统管理** > **SAML** 页上的所有设置。
- 启用垃圾邮件隔离区。请参阅垃圾邮件隔离区， 第 143 页。

步骤 1 依次选择**管理设备** > **集中服务** > **垃圾邮件隔离区**。
步骤 2 点击**编辑设置**并向下滚动到“终端用户隔离区访问”部分。
步骤 3 请确保已启用“终端用户隔离区访问”。
步骤 4 将终端用户身份验证方法设置为 **SAML2.0**。
步骤 5 （可选）指定在释放邮件前，是否显示邮件正文。
步骤 6 提交并确认更改。

下一步做什么

将新的身份验证机制通知给终端用户。

自定义视图

- 使用收藏夹页面 ， 第 331 页
- 设置首选项 ， 第 331 页
- 改善网络界面显示 ， 第 332 页

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	相应操作
将页面添加到收藏夹列表	导航至要添加的页面，然后从窗口右上角附近的“我的收藏夹”菜单选择**将此页面添加到我的收藏夹**。 更改“我的收藏夹 (My Favorites)”时不需要确认。
对收藏内容进行重排序	依次选择**我的收藏夹 (My Favorites) > 查看所有收藏内容 (View All My Favorites)**，然后将收藏内容拖至所需的顺序。
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)**，然后点击要编辑的收藏夹的名称。
删除收藏内容	依次选择**我的收藏夹 (My Favorites) > 查看所有收藏内容 (View All My Favorites)**，然后删除收藏内容。
转到收藏页面	从窗口右上角附近的**我的收藏夹 (My Favorites)** 菜单选择一个页面。
查看或构建一个自定义报告页面	请参阅自定义报告 ，第 24 页
返回到主界面	选择任何收藏夹或点击页面底部的**返回到上一页 (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（应用于 GUI 和 PDF 报告）
- 登录页面（登录后显示的页面）
- 报告页面的默认时间范围（可用的选项是可用于邮件和 Web 报告页面的一部分时间范围）
- 报告页面上的表中可见的行数。

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。）完成时提交您所做的更改。不需要确认更改。

提示 要返回到您在访问“首选项”(Preferences) 页面之前查看的页面，请点击页面底部的**返回到上一页 (Return to previous page)** 链接。

经过外部身份验证的用户

经过外部身份验证的用户可以直接在“选项”菜单中选择显示语言。

改善网络界面显示

为了使 Web 界面呈现更好的效果，思科建议您启用 Internet Explorer 兼容模式覆盖。

注释 如果启用此功能会违背您的组织策略，您可以禁用此功能。

步骤 1 依次选择**管理设备** > **系统管理** > **常规设置**。

步骤 2 选择**覆盖 IE 兼容模式 (Override IE Compatibility Mode)** 复选框。

步骤 3 提交并确认更改。

第 15 章

日志记录

本章包含以下部分：

日志记录概述

日志文件记录系统中各项活动的正常操作及异常。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。

大多数日志以纯文本 (ASCII) 格式记录；但是，为了提高资源效率，跟踪日志以二进制格式记录。ASCII 文本信息在任何文本编辑器中均可读。

日志记录与报告

使用日志记录数据来调试消息流，显示基本的日常操作信息（如 FTP 连接详细信息、HTTP 日志文件，以及将其用于合规性存档）。

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 FTP 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便备份。

要查看报告数据，请使用设备 GUI 上的“报告”(Report) 页面。您无法以任何方式访问基础数据，而且此数据无法发送到除思科内容管理设备以外的任何设备。

注释 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。此数据从 ESA 推送。

日志检索

可以使用下表中介绍的文件传输协议检索日志文件。您可以在 GUI 中创建或编辑日志订阅时设置协议，也可以通过在 CLI 中使用 `logconfig` 命令来设置协议。

FTP 轮询	使用此类文件传输协议时，远程FTP客户端使用管理员级别或操作员级用户的用户名和密码来访问设备以检索日志文件。在配置日志订阅以使用FTP 轮询方法时，您必须提供要保留的最大日志文件数量。在达到最大数量时，系统会删除最旧的文件。
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。订阅要求提供远程计算机的用户名、密码和目标目录。系统会根据配置的滚动更新计划传输日志文件。
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。这种订阅需要提供远程计算机上的用户名、SSL 密钥和目标目录。系统会根据配置的滚动更新计划传输日志文件。
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。您必须提交系统日志服务器的主机名并将 UDP 或 TCP 用于日志传输。使用的端口为 514。可以为日志选择工具；但是，日志类型的默认值已在下拉菜单中预先选择。仅基于文本的日志可以使用系统日志推送传输。

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。目录中的日志文件名包含日志订阅中指定的文件名、启动日志文件时的时间戳和单字符的状态代码。以下示例显示有关目录和文件名的约定：

/<Log_Name>/<Log_Filename>.@<timestamp>.<statuscode>

状态代码可以是 .c（表示“当前”）或 .s（表示“已保存”）。您只应传输具有已保存状态的日志文件。

日志回滚和传输计划

在创建日志订用时，您为何时进行日志滚动更新、传输旧文件和创建新的日志文件指定触发因素。

从以下触发因素中进行选择：

- 文件大小
- 时间
  - 按指定的时间间隔（以秒、分钟、小时或天为单位）

在输入值时仿照屏幕上的示例。

要输入复合时间间隔，例如两个半小时，请仿照示例 2h30m。

或

- 在您指定的每天时间

  或

- 在您所选星期几的指定时间

在指定时间时使用 24 小时制，例如用 23:00 表示 11pm。

要在一天内安排多个滚动更新时间，请用逗号将时间隔开。例如，要在午夜和中午滚动更新日志，请输入 00:00, 12:00

将星号 (*) 用作通配符。例如，要在每个整点和半点滚动更新日志，请输入 *:00, *:30

在达到指定的限制（或达到第一个限制，如果您同时配置了基于文件大小的限制和基于时间的限制）时，日志文件会滚动更新。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的 FTP 目录中，直到检索文件为止或直到系统需要更多的日志文件空间为止。

注释 如果在达到下一个限制时滚动更新正在进行，则会跳过新的滚动更新。系统会记录错误，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 *48:* 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

日志名称	日志类型	检索方法
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

所有预先配置的日志订阅的日志记录级别均设置为“信息”(Information)。有关日志级别的详细信息，请参阅设置日志级别，第 357 页。

您可以根据自己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 356 页。

日志类型

日志类型摘要

日志订用可将日志类型与名称、日志记录级别及其他特性（例如文件大小和目标目录信息）相关联。允许除了配置历史记录日志外的所有日志类型的多个订阅。日志类型决定日志中记录的数据。您在创建日志订用时选择日志类型。有关详细信息，请参阅日志订阅，第 356 页。

AsyncOS 会生成以下日志类型：

表 *49:* 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。 有关备份计划的信息在 SMA 日志中。
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 日志记录了有关在接口上启用的 FTP 服务的信息。会记录连接详细信息和用户活动。
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，例如有关通过邮件从设备发送的计划报告的信息。
HTTP日志	HTTP 日志会记录有关在接口上启用的 HTTP 服务和安全 HTTP 服务的信息。由于图形用户界面 (GUI) 是通过 HTTP 访问的，因此 HTTP 日志实质上是 CLI 审核日志的 GUI 等效版本。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（例如邮件接收、邮件传送尝试、打开和关闭连接、退回邮件等）的信息。 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 133 页。

日志类型	说明
LDAP 调试日志	在“系统管理”(System Administration) > “LDAP”(LDAP) 中配置 LDAP 时，使用这些日志可调试问题。 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已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 312 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 相关联的操作，例如通过GUI进行的隔离区配置、终端用户身份验证和终端用户操作（例如放行邮件）。
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流程相关联的操作。
状态日志	状态日志会记录 CLI 状态命令中找到的系统统计信息，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记录的速率为从上次重置计数器起至当前的值。
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。系统日志可用于对设备的状态进行故障排除。
跟踪日志	跟踪日志记录了与跟踪服务过程关联的操作。跟踪日志是邮件日志的子集。
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

下表总结了每种日志类型的特征。

表 *50:* 日志类型比较

	包含										
	事务	无状态	记录为文本	记录为二进制	信头日志记录	定期状态信息	邮件接收信息	传送信息	单个硬退回	单个软退回	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											
报告查询日志											
SMA 日志											
SNMP 日志											
安全列表/阻止列表日志											

						包含					
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括配置文件以及列出用户名的附加部分、对用户在配置中做出更改的位置的说明及用户在确认更改时输入的评论。每当用户提交更改时，系统就会创建新日志，其中包含更改后的配置文件。

示例

在本例中，配置历史记录日志显示了用户 (admin) 向定义哪些本地用户获准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">
<!--
  XML generated by configuration change.
  Change comment: added guest user
  User: admin
  Configuration are described as:
    This table defines which local users are allowed to log into the system.
  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

下表 介绍了 CLI 审核日志中记录的统计信息。

表 *51: CLI* 审核日志统计信息

统计	描述
时间戳	传输字节的时间。
PID	输入命令的特定 CLI 会话的进程 ID。
邮件	消息包含输入的CLI命令、CLI输出（包括菜单、列表等）和出现的提示。

示例

在本例中，CLI 审核日志显示用户对 PID 16434 输入以下 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

下表 介绍了 FTP 服务器日志中记录的统计信息。

表 *52: FTP* 服务器日志统计信息

统计	描述
时间戳	传输字节的时间。
ID	连接 ID。每个 FTP 连接的单独 ID。
邮件	日志条目的消息部分可以是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 服务器日志记录了一个连接 (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

下表 介绍了 HTTP 日志中记录的统计信息

表 *53*: 在 *HTTP* 日志中记录的统计数据

统计	描述
时间戳	传输字节的时间。
ID	会话 ID。
req	连接的计算机的 IP 地址。
用户	连接的用户的用户名。
邮件	关于已执行的操作的信息。可能包括 GET 或 POST 命令或系统状态等。

示例

在本示例中，HTTP 日志显示 admin 用户与 GUI 的交互（例如运行“系统设置向导”[System Setup Wizard]）。

```
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=190
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

下表 介绍了垃圾邮件隔离区日志中记录的统计信息。

表 *54:* 垃圾邮件隔离区日志统计信息

统计	描述
时间戳	数据的传输时间。
邮件	消息包含所采取的操作（邮件被隔离、从隔离区放行等操作）。

示例

在本示例中，日志显示两封邮件（MID 8298624 和 MID 8298625）从隔离区放行到 admin@example.com。

```
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

下表 显示了在垃圾邮件隔离区 GUI 日志中记录的统计信息。

表 *55:* 垃圾邮件隔离区 *GUI* 日志统计信息

统计	描述
时间戳	数据的传输时间。
邮件	该消息包括采取的措施，包括用户身份验证等等。

示例

在本示例中，日志显示了成功的身份验证、登录和注销：

表 *56:* 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

这些日志包含邮件接收、邮件传送和退回的详细信息。此外，状态信息每隔一分钟写入邮件日志一次。这些日志是重要的信息来源，可帮助了解特定邮件的传送情况和分析系统性能。

这些日志不需要任何特殊配置。但是，您必须正确配置系统，才能查看附件名称，而且系统不会总是记录附件名称。有关详细信息，请参阅跟踪服务概述，第 133 页。

下表 介绍了文本邮件日志中显示的信息。

表 *57:* 文本邮件日志统计信息

统计	说明
ICID	注入连接 ID。这是与系统建立的单个 SMTP 连接的数字标识符。可以通过一个 SMTP 连接将单封邮件或成千上万封邮件发送到系统。
DCID	传送连接 ID。这是与另一台服务器建立的单个 SMTP 连接的数字标识符，用于传送一封至成千上万封邮件，每封邮件的部分或全部 RID 在单个邮件传输中传送。
RCID	RPC 连接 ID。这是与垃圾邮件隔离区建立的单个 RPC 连接的数字标识符。该标识符用于在邮件进出垃圾邮件隔离区时跟踪邮件。
MID	消息 ID。使用此 ID 跟踪流经日志的邮件。
RID	收件人 ID。系统会为每个邮件收件人分配 ID。
新建	新连接已发起。
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。

注释 日志文件中的各行未编号。在此处对它们进行编号仅用于示例演示。

表 *58:* 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`

下表可用作阅读上一日志文件的指南。

表 *59:* 文本邮件日志详细信息示例

行号	说明
1	发起到系统的新连接，并且分配注入 ID (ICID)“5”。此连接是在管理 IP 接口上接收的，从 10.1.1.209 远程主机发起。
2	在从客户端发出 MAIL FROM 命令后，为邮件分配了邮件 ID (MID)“6”。
3	识别和接受发件人地址。
4	识别收件人，并且分配收件人 ID (RID)“0”。
5	接受 MID 5，将其写入磁盘并确认。

行号	说明
6	接收成功，接收连接断开。
7	邮件传送过程开始。分配传送连接 ID (DCID)“8”，从 192.168.42.42 到 10.5.3.25。
8	开始到 RID“0”的邮件传送。
9	从 MID 6 到 RID“0”的传送成功。
10	传送连接断开。

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

发送给单个收件人的一封邮件注入设备中。邮件成功传送。

```
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
```

成功的邮件传送示例

```
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
```

不成功的邮件传送（硬退回）

具有两个收件人的一封邮件注入设备中。传送后，目标主机返回5XX错误，这表示邮件未能传送到任何一个收件人。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
```

最终成功传送的软退回示例

一封邮件注入设备中。第一次传送尝试时，邮件软退回，并排队等待之后传送。第二次尝试时，邮件被成功传送。

```
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)

如果使用 scanconfig 命令确定当邮件无法分解为各组成部分时（在删除附件时）的行为，如以下提示所述：

```
If a message could not be deconstructed into its component parts in order to remove specified
 attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[3]>
```

以下是邮件日志中的指示：

在无法分解邮件时 *scanconfig* 设置为 *deliver*。

```
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
```

在无法分解邮件时 *scanconfig* 设置为 *drop*。

```
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

在本例中，条件为“邮件正文包含”的内容过滤器已配置为支持附件名称识别：

```
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。

生成的或重写的邮件

诸如重写/重定向操作等某些功能（alt-rcpt-to 过滤器、反垃圾邮件收件人重写、bcc() 操作、防病毒重定向等操作）会创建新邮件。在查看日志时，您可能需要检查结果并添加其他 MID 和 DCID。条目可能如下所示：

```
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'
```

注释 “重写的”条目可以出现在日志中的行之后，指明使用新 MID。

将邮件发送到垃圾邮件隔离区

在用户将邮件发送到隔离区时，邮件日志会跟踪进出隔离区的移动，使用 RCID（RPC 连接 ID）标识 RPC 连接。在以下邮件日志中，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

下表 显示了 NTP 日志中记录的统计信息。

表 *60: NTP* 日志中记录的统计信息

统计	描述
时间戳	数据的传输时间。
邮件	消息包含对服务器的简单网络时间协议 (SNTP) 查询或 adjust: 消息。

示例

在本例中，NTP 日志显示了两次轮询 NTP 主机的设备。

```
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 08:44:59 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

下表 显示了报告日志中记录的统计信息。

表 *61:* 报告日志统计信息

统计	描述
时间戳	数据的传输时间。

统计	描述
邮件	该消息包括采取的措施，包括用户身份验证等等。

示例

在本例中，报告日志显示了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

下表 显示了报告查询日志中记录的统计信息。

表 *62*: 报告查询日志统计信息

统计	描述
时间戳	数据的传输时间。
邮件	该消息包括采取的措施，包括用户身份验证等等。

示例

在本例中，报告查询日志显示了从 2007 年 8 月 29 日到 10 月 10 日，运行每日传出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

下表 显示了在安全列表/阻止列表日志中记录的统计信息。

表 *63:* 安全列表/阻止列表日志统计信息

统计	描述
时间戳	数据的传输时间。
邮件	该消息包括采取的措施，包括用户身份验证等等。

示例

在本例中，安全列表/阻止列表日志显示了设备每两个小时创建一次数据库快照。它还显示了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

下表 显示了在 SMA 日志中记录的统计信息。

表 *64: SMA* 日志统计信息

统计	描述
时间戳	数据的传输时间。
邮件	该消息包括采取的措施，包括用户身份验证等等。

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

状态日志记录 CLI 状态命令中的系统统计信息，包括 status、status detail 以及 dnsstatus 命令。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记录的速率为从上次重置计数器起至当前的值。

表 *65:* 状态日志统计信息

统计	说明
CPULd	CPU 利用率。
DskIO	磁盘 I/O 利用率。
RAMUtil	RAM 利用率。

统计	说明
QKUsd	已用的队列空间 (KB)。
QKFre	可用的队列空间 (KB)。
CrtMID	邮件 ID (MID)。
CrtICID	注入连接 ID (ICID)。
CRTDCID	传送连接 ID (DCID)。
InjMsg	注入的邮件数量。
InjRcp	注入的收件人数量。
GenBncRcp	生成的退回收件人数量。
RejRcp	拒绝的收件人数量。
DrpMsg	丢弃的邮件数量。
SftBncEvnt	软退回的事件数量。
CmpRcp	已完成的收件人数量。
HrdBncRcp	硬退回的收件人数量。
DnsHrdBnc	DNS 硬退回数量。
5XXHrdBnc	5XX 硬退回数量。
FltrHrdBnc	过滤器硬退回数量。
ExpHrdBnc	过期硬退回数量。
OtrHrdBnc	其他硬退回数量。
DlvRcp	已传送的收件人数量。
DelRcp	已删除的收件人数量。
GlbUnsbHt	全局取消订阅命中数。
ActvRcp	正在处理的收件人数量。
UnatmptRcp	未尝试的收件人数量。
AtmptRcp	已尝试的收件人数量。
CrtCncIn	当前的入站连接数。
CrtCncOut	当前的出站连接数。

统计	说明
DnsReq	DNS 请求数。
NetReq	网络请求数。
CchHit	缓存命中数。
CchMis	缓存丢失数。
CchEct	缓存异常数。
CchExp	缓存过期。
CPUTTm	应用使用的 CPU 时间。
CPUETm	自应用启动以来经过的时间。
MaxIO	邮件进程每秒的最大磁盘 I/O 操作数量。
RamUsd	分配的内存（字节）。
SwIn	换入的内存。
SwOut	换出的内存。
SwPgIn	页入的内存。
SwPgOut	页出的内存。
MMLen	系统中的邮件总数。
DstInMem	内存中的目标对象数。
ResCon	资源节约限定值。对传入邮件的接受延迟此秒数，因为系统负载很重。
WorkQ	工作队列中的邮件数量。
QuarMsgs	系统隔离区中各邮件的数量（出现在多个隔离区中的邮件只计算一次）。
QuarQKUsd	系统隔离区邮件已使用的空间 (KB)。
LogUsd	已使用的日志分区百分比。
CASELd	CASE 扫描已使用的 CPU 百分比。
TotalLd	CPU 总利用率。
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	垃圾邮件隔离区放行队列中的邮件数量。

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

下表 显示了在系统日志中记录的统计信息。

表 *66:* 系统日志统计信息

统计	描述
时间戳	数据的传输时间。
邮件	记录的事件。

示例

在本示例中，系统日志显示了一些提交条目，包括发出提交命令的用户的名称和输入的备注。

```
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 08:49:27 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

跟踪日志记录了有关 AsyncOS 的邮件操作的信息。日志消息是在邮件日志中记录的消息子集。

消息跟踪组件使用跟踪日志构建消息跟踪数据库。因为在构建数据库过程中使用日志文件，所以跟踪日志是瞬态的。跟踪日志中的信息不供人们阅读或分析。

为了提高资源效率，跟踪日志以二进制格式记录和传输。信息以符合逻辑的方式列出，在使用思科提供的实用程序转换后可供人员阅读。转换工具位于以下网址：http://tinyurl.com/3c5l8r。

日志订阅

配置日志订用

日志订用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。系统会对日志订用进行推送（传输到另一台计算机）或轮询（从设备检索）。通常，日志订用具有以下属性：

表 *67:* 日志文件属性

属性	说明
日志类型	定义记录的信息类型以及日志订用的格式。有关详细信息，请参阅日志类型摘要，第 337 页。
名称	您提供的供自己将来参考的日志订用描述性名称。
日志文件名 (Log Filename)	文件写入磁盘时的实际名称。如果系统包括多台内容安全设备，请使用唯一的日志文件名来标识生成该日志文件的设备。
按文件大小滚动 (Rollover by File Size)	文件在滚动更新之前可以达到的最大大小。
按时间滚动 (Rollover by Time)	何时根据时间滚动更新日志文件。请参阅日志回滚和传输计划，第 334 页的选项。
日志级别 (Log Level)	每个日志订用的详细信息级别。
检索方法 (Retrieval Method)	用于从设备传输日志文件的方法。

使用**管理设备 > 系统管理 > 日志订阅**页面（或 CLI 中的 `logconfig` 命令）配置日志订阅。系统会提示您输入日志类型，如日志类型摘要，第 337 页所示。对于大多数日志类型，系统您会要求您为日志订用选择日志级别 *(log level)*。

注释 仅限配置历史记录日志：如果您预期从配置历史记录日志加载配置，请注意不能加载包含已屏蔽密码的配置。在**管理设备 > 系统管理 > 日志订阅**页面上，当系统提示您是否要在日志中包括密码时选择是。如果您在 CLI 中使用 `logconfig` 命令，请在出现提示时键入 `y`。

设置日志级别

日志级别决定日志中提供的信息量。日志可以设为五个详细级别中的其中一个。与简略的日志级别设置相比，详细的日志级别设置会创建更大的日志文件，且对系统性能有更大的影响。详细的日志级别设置包括简略的日志级别设置中包含的所有消息以及其他消息。随着详细级别的提升，系统性能会逐渐下降。

注释 您可以为每种日志类型指定不同的日志记录级别。

表 *68:* 日志级别

日志级别	说明
严重	仅记录错误。这是最简略的日志级别设置。在此日志级别，您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达到最大大小。此日志级别类似于系统日志级别“警报”(Alert)。
警告	记录所有系统错误和警告。在此日志级别，您无法监控性能和重要设备活动。日志文件比在“严重”(Critical) 日志级别更快达到最大大小。此日志级别类似于系统日志级别“警告”(Warning)。
信息	记录系统的每一秒钟的操作。例如，会记录打开的连接和传送尝试。信息级别是推荐日志设置。此日志级别类似于系统日志级别“信息”(Info)。
调试	比在“信息”日志级别记录的信息更详细。在对错误进行故障排除时，请使用“调试”(Debug) 日志级别。暂时使用此设置，然后恢复到默认级别。此日志级别类似于系统日志级别“调试”(Debug)。
跟踪	记录所有可用的信息。跟踪日志级别仅推荐开发人员使用。使用此级别会造成系统性能严重降级，不推荐使用。此日志级别类似于系统日志级别“调试”(Debug)。

在 GUI 中创建日志订用

步骤 1 在**管理设备 > 系统管理 > 日志订用**页面上，点击**添加日志订用**。

步骤 2 选择日志类型，并输入日志目录的日志名称和日志文件本身的名称。

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、当天时间或时间间隔。有关详细信息，请参阅日志回滚和传输计划，第 334 页。

步骤 5 如果适用，请指定日志级别。

步骤 6 （仅限配置历史记录日志）选择是否在日志中包括密码。

注释　您不能加载包含已屏蔽密码的配置。如果您预期从配置历史记录日志加载配置，请选择“是”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

步骤 1 点击“日志订阅”(Log Subscriptions) 页面上的“日志名称”(Log Name) 列中的日志名称。

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“日志订用”页面的“全局设置”部分中的**编辑设置**按钮（或 CLI 中的 logconfig -> setup 命令）配置以下设置：

- 系统在记录指标之间等待的时长（以秒为单位）
- 是否记录邮件 ID 标题
- 是否记录远程响应状态代码
- 是否记录原始邮件的主题标题
- 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，将记录每封邮件的远程响应状态代码（如果可用）。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。在本例中，在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
```

系统会从字符串开头剥离空白区域、标点符号和“OK”字符（在250响应情况下）。仅从字符串末尾剥离空白区域。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”。

- 原始主题标题：启用此选项时，每封邮件的原始主题标题均包括在日志中。

```
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的存在性及其内容。您可以在“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）指定要记录的标题。设备会在文本邮件日志和跟踪日志中记录指定的邮件标题。如果信头存在，则系统会记录信头的名称和值。如果没有信头，则不会在日志中记录任何信息。

注释 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。

注释 SMTP 协议的 RFC 位于 http://www.faqs.org/rfcs/rfc2821.html 并定义用户定义的信头。

注释 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 69: Log Headers

信头名称	信头的名称
值	已记录信头的内容

例如，指定“date, x-subject”作为要记录的标题会导致以下行出现在邮件日志中：

```
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')]
```

通过使用 GUI 配置日志记录的全局设置

步骤 1 点击“日志订阅”(Log Subscriptions) 页面的“全局设置”(Global Settings) 部分中的**编辑设置**按钮。

步骤 2 指定系统指标频率、是否要将邮件 ID 标题包括在邮件日志中、是否包括远程响应以及包括每封邮件的原始主题标题。

有关这些设置的详细信息，请参阅配置日志记录的全局设置 ， 第 358 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。

滚动更新日志订用

在滚动更新日志文件时，AsyncOS 会执行以下操作：

- 使用滚动更新操作的时间戳创建新的日志文件，并使用字母“**c**”扩展名指定该文件为最新文件
- 将最新的日志文件重命名为具有字母“**s**”扩展名，表示已保存
- 将新保存的日志文件传输到一台远程主机（如果基于推送）
- 从同一订用传输以前不成功的任何日志文件（如果基于推送）
- 在超过要保存的文件总数时，删除日志订用中的最旧文件（如果基于轮询）

后续操作

滚动更新日志订用中的日志

请参阅日志回滚和传输计划，第 334 页。

使用 GUI 立即滚动更新日志

步骤 1 在“日志订用”(Log Subscriptions) 页面上，选中要滚动更新的日志右侧的复选框。

步骤 2 （可选）通过选中**全部 (All)** 复选框选择滚动更新所有日志。

步骤 3 点击**立即滚动更新 (Rollover Now)** 按钮。

下一步做什么

- 滚动更新日志订用中的日志，第 360 页
- 通过 CLI 立即滚动更新日志，第 360 页

通过 CLI 立即滚动更新日志

使用 rollovernow 命令同时滚动更新所有日志文件，或从列表中选择特定的日志文件。

查看 GUI 中最新的日志条目

您可以通过 GUI 查看日志文件，方法是在“日志订阅”(Log Subscriptions) 页面上点击表的“日志名称”(Log Name) 列中的日志订阅。当您点击日志订阅的链接时，系统会提示您输入密码。该订阅的日志文件列表随即出现。您可以点击其中一个日志文件，以便在浏览器中查看或将其保存到磁盘。您必须在“管理”(Management) 接口上启用 FTP 服务才可以在 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 可从 tail 命令中退出。

注释 您无法通过使用 tail 命令查看配置历史记录日志。您必须使用 FTP 或 SCP。

示例

在以下示例中，tail 命令用于查看系统日志。tail 命令还接受将日志名称视为参数，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。专用主机密钥驻留在SSH服务器上，无法被远程计算机读取。公共主机密钥分布到任何需要与SSH服务器交互的客户机上。

注释 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 *70:* 管理主机密钥 - 子命令列表

命令	说明
新建	添加新密钥。
Edit	修改现有密钥。
删除	删除现有密钥。
Scan	自动下载主机密钥。
Print	显示密钥。
Host	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。
Fingerprint	显示系统主机密钥指纹。
用户	显示将日志推送到远程计算机的系统账户的公钥。这是在设置 SCP 推送订用时出现的同一密钥。这是要放置在远程系统的“authorized_keys”文件中的值。

示例

在以下示例中，这些命令扫描主机密钥并为主机添加密钥：

```
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. All
[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
```

第 16 章

故障排除

本章包含以下部分：

收集系统信息

您可以获得有关设备及其状态的信息，包括序列号。请参考监控系统状态， 第 217 页

对硬件问题进行故障排除

硬件设备前面板和/或后面板上的指示灯指示设备的运行状况和状态。有关这些指示灯的说明，请参阅中指定位置提供的硬件指南（例如《思科 *x90* 系列内容安全设备安装和维护指南》）。

这些文档中还会介绍设备规格，例如温度范围。

注释 如果您需要重启 x80 或 x90 设备，请等待至少 20 分钟以便设备完成启动准备（所有 LED 均呈绿色亮起），然后再按电源按钮。

功能设置问题故障排除

如果您在成功配置功能方面遇到困难，请参阅您必须为每项功能完成的任务的摘要。这些摘要包括每项任务的特定信息的链接。

- 设置集中 Web 报告和跟踪 ， 第 86 页
- 设置集中邮件报告， 第 34 页
- 设置集中邮件跟踪 ， 第 134 页
- 设置集中垃圾邮件隔离区 ， 第 144 页
- 集中策略、病毒和病毒爆发隔离区， 第 167 页
- 设置主配置以集中管理网络安全设备 ， 第 192 页

一般故障排除资源

一般故障排除资源包括：

- 最近的警报。请参阅查看最近的警报 ， 第 303 页。
- 日志文件。请参阅日志记录， 第 333 页
- 版本说明，包括“文档更新”部分。请参阅文档 ， 第 393 页。
- 思科漏洞搜索工具（有关访问说明，请参阅版本说明）
- 知识库文章（技术说明） ， 第 395 页
- 这种思科支持社区， 第 395 页

对受管设备的性能问题进行故障排除

要在遇到性能问题时确定系统的哪些部分使用最多的资源，您可以查看所有受管设备（邮件或网络安全）和每台受管设备的“系统容量”(System Capacity) 报告。对于邮件安全设备，请参阅系统容量页面， 第 69 页。对于网络安全设备，请参阅系统容量页面， 第 114 页。

特定功能问题的故障排除

另请参阅功能设置问题故障排除 ， 第 366 页。

网络安全相关问题

- 对所有报告进行故障排除 ， 第 30 页
- 解决 Web 报告和跟踪问题 ， 第 129 页
- 对配置管理问题进行故障排除 ， 第 214 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 393 页中指定位置处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 30 页
- 邮件报告故障排除 ， 第 81 页
- 邮件跟踪故障排除， 第 141 页
- 垃圾邮件隔离区功能故障排除 ， 第 166 页
- 排除集中策略隔离区故障 ， 第 189 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 393 页中指定位置处您所用版本的版本说明和在线帮助或用户指南。

一般问题

- 如果您无法加载配置文件，请确定您的磁盘空间配额超过**管理设备 > 系统管理 > 磁盘管理**页面上的表中每项功能的当前大小。
- 如果您最近已升级，并且联机帮助似乎已过时，或者您无法找到有关某项新功能的信息，请清除浏览器缓存，然后重新打开浏览器窗口。
- 在使用网络界面配置设置时，如果您同时使用多个浏览器窗口或选项卡，可能会发生意外行为。
- 请参阅响应警报 ， 第 367 页。
- 请参阅管理用户访问权限故障排除 ， 第 270 页。

响应警报

警报：380 或 680 硬件上的电池再记忆超时（RAID 活动）

问题：您收到关于 380 或 680 硬件的主题为“电池再记忆超时”的警报。

解决方案：此警报可能表示存在问题，也可能不表示存在问题。电池再记忆超时并不意味着 RAID 控制器存在问题。控制器可以在后续的再记忆中恢复。请在接下来的48小时内监控您的邮件是否出现任何其他 RAID 警报，以确保此问题不是其他问题的副作用所致。如果您没有看到来自系统的任何其他 RAID 相关警报，则可以放心地忽略此警报。

其他警报说明

有关其他警报的说明，请参阅

- 硬件警报说明 ， 第 304 页
- 系统警报说明 ， 第 304 页

后续操作

- 管理警报， 第 302 页

使用技术支持

- 从设备提交或更新支持请求 ， 第 368 页
- 获取虚拟设备技术支持 ， 第 369 页
- 启用思科技术支持人员远程访问 ， 第 369 页

从设备提交或更新支持请求

您可以使用此方法与思科 TAC 或您自己的支持服务人员联系。

开始之前

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 395 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：
- 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。如果您不希望发送设备配置，可以使用另一种方法联系客户支持部门。
- 设备必须联网并且能够发送邮件。
- 如果您要发送某个现有案例的相关信息，确保您有案例编号。

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：

要将发送请求给思科 TAC	选中**思科技术支持 (Cisco Technical Support)** 复选框。
要仅将请求发送给您的内部支持部门	• 取消选中**思科技术支持 (Cisco Technical Support)** 复选框。 • 输入您的支持部门邮件地址。
（可选）要包括其他收件人	输入邮件地址。

步骤 4 完成表格。

步骤 5 点击 **Send**。

获取虚拟设备技术支持

如果您为思科内容安全虚拟设备提交一个支持请求，则必须提供您的虚拟许可证号 (VLN)、合同编号和产品标识符代码 (PID)。

您可以根据虚拟设备上运行的软件许可证，通过参考采购订单或从下表识别 PID。

功能	PID	描述
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。

- 启用思科技术支持人员远程访问 ， 第 369 页
- 启用对无直接网络连接设备的远程访问 ， 第 370 页
- 禁用技术支持隧道 ， 第 370 页
- 禁用远程访问 ， 第 370 页
- 检查支持连接的状态 ， 第 371 页

启用对网络连接设备的远程访问

支持部门可通过此过程在设备与 upgrades.ironport.com 服务器之间创建的 SSH 隧道访问设备。

开始之前

确定一个可以从互联网访问的端口。默认端口为 25，该端口在大多数环境下都适用，。大多数防火墙配置都允许通过此端口进行的连接。

步骤 1 登录到设备。

步骤 2 从 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**。

步骤 4 输入信息。

步骤 5 点击**提交**。

下一步做什么

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 370 页。

启用对无直接网络连接设备的远程访问

对于没有直接互联网连接的设备，可以通过连接至互联网的第二台设备进行访问。

开始之前

- 设备必须能够通过端口 22 连接到第二台连网设备。
- 在已连接互联网的设备上，按照启用对网络连接设备的远程访问 ， 第 369 页中的程序创建通往该设备的支持隧道。

步骤 1 在请求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。

下一步做什么

当不再需要支持人员的远程访问时，请参阅以下内容：

- 禁用远程访问 ， 第 370 页
- 禁用技术支持隧道 ， 第 370 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。7 天之后，建立的连接虽然不会断开，但一旦断开就无法重新连接至该隧道。

步骤 1 登录到设备。

步骤 2 从 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账户将保持活动状态，直到将其禁用为止。

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

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设备接收和发出的TCP/IP数据及其他数据包。这样，支持人员就可以调试网络设置，并知道哪些网络流量到达该设备或者离开该设备。

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)** 屏幕中，点击**编辑设置**。

b) （可选）输入数据包捕获的持续时间、限制和过滤器。

您的支持代表可能会提供这些设置的相关指导。

如果您输入了捕获的持续时间却没有指定时间单位，AsyncOS 默认使用秒。

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 是指与设备连接的计算机（例如通过邮件安全设备发送邮件的邮件客户端）的 IP 地址。
- 服务器 IP 是指设备连接的计算机（例如设备传送邮件至的 Exchange 服务器）的 IP 地址。

您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，将邮件安全设备置于中间。

c) 点击**提交**。

步骤 3 点击**开始捕获 (Start Capture)**。

- 一次只能运行一个捕获操作。
- 运行数据包捕获时，数据包捕获页面会显示当前统计数据，例如文件大小和逝去的时间，让您能够看到进行中的捕获状态。
- GUI 只显示 GUI 中开始的数据包捕获，而不显示从 CLI 开始的数据包捕获。同样地，CLI 只显示 CLI 中开始的当前数据包捕获的运行状态。
- 数据包捕获文件分为 10 个部分。如果数据包捕获结束前文件到达最大大小限制，那么该文件最早的部分将会被删除（数据丢弃），新的部分从当前的数据包捕获数据开始。一次只能丢弃数据包捕获文件的 1/10。
- 两次会话期间保留GUI中开始的正在运行的捕获。（当会话终止时，CLI中开始的正在运行的捕获会停止。）

步骤 4 允许捕获操作运行指定的时间，或者如果您让捕获无限运行，则可以点击**停止捕获 (Stop Capture)**停止捕获。

步骤 5 访问数据包捕获文件：

- 在**管理数据包捕获文件 (Manage Packet Capture Files)** 列表中点击该文件，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。

下一步做什么

将该文件提供给支持部门：

- 如果您允许远程访问您的设备，技术人员可以使用 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 369 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，您可以使用第三方智能平台管理接口 (IPMI) 工具远程重新启动设备机箱。

限制

- 远程电源重新启动仅适用于特定硬件。

  有关具体信息，请参阅启用远程电源循环 ，第 278 页。

- 如果您希望能够使用此功能，您必须提前启用它。

  有关详细信息，请参阅启用远程电源循环 ，第 278 页。

- 仅支持以下 IPMI 命令：

  ```
  status, on, off, cycle, reset, diag, soft
  ```

  发出不支持的命令将导致“权限不足”错误。

开始之前

- 使用 IPMI 版本 2.0 获取并设置可用于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 IPMI 工具的文档。

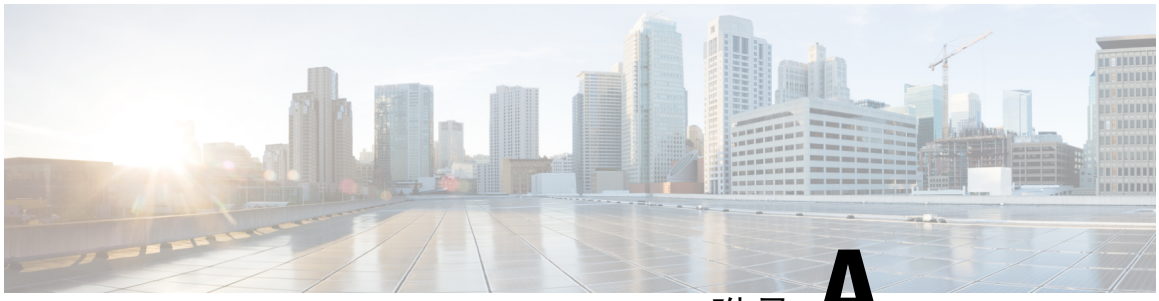
步骤 1 使用 IPMI 向分配到“远程电源重新启动”端口（之前配置）的 IP 地址发出支持的电源循环命令，以及所需的凭证。

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` 是分配到远程电源重新启动端口的 IP 地址，remoteresetuser 和 password 是您在启用此功能时输入的凭证。

步骤 2 等待至少十一分钟，以便设备重启。



附录 A

IP 接口和访问设备

本章包含以下部分：

IP 接口和访问设备

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，在每个接口上启用或禁用以下服务：

表 *71:* 默认情况下在 *IP* 接口上启用的服务

		默认启用？	
服务	默认端口	管理接口	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。可以向物理以太网接口配置多个 IP 接口。您还可以通过 IP 接口配置对垃圾邮件隔离区的访问权限。对于邮件传送和虚拟网关，每个 IP 接口都用作一个具有特定 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

使用“管理设备”>“网络”>“IP 接口”页面（和 interface config 命令）可以添加、编辑或删除 IP 接口。

注释 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 *72: IP* 接口组件

名称	接口的别名。
IP 地址	无法在单独的物理以太网接口上配置相同子网内的 IP 地址。
网络掩码（或子网掩码）	您可以用标准点分八位二进制数格式（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，这是常用 C 类值。
广播地址	AsyncOS 根据 IP 地址和网络掩码自动计算默认广播地址。
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。您负责输入与每个 IP 地址关联的有效主机名。此软件不检查 DNS 是否将主机名正确解析为匹配的 IP 地址，也不检查反向 DNS 是否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。您可以为每项服务配置端口。您可以为垃圾邮件隔离区指定 HTTP/HTTPS、端口和 URL。

注释 如果已按设置、安装和基本配置，第 5 页所述完成系统设置向导并提交更改，则设备上应该已配置管理接口。

使用 GUI 创建 IP 接口

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。必要时更改相应的端口。

步骤 8 选择是否启用将 HTTP 重定向至 HTTPS，以便在接口上进行设备管理。

步骤 9 如果您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。您还可以选择是否将 HTTP 请求重定向至 HTTPS。最后，您可以指定 IP 接口是否是垃圾邮件隔离区的默认接口，以及是将主机名用作 URL 还是提供自定义 URL。

步骤 10 提交并确认更改。

通过 FTP 访问设备

注意 通过使用“管理设备”>“网络”>“IP 接口”页或 interfaceconfig 命令禁用服务，您可断开自己与 GUI 或 CLI 的连接，具体取决于您如何连接到设备。如果无法使用其他协议、串行接口或管理端口上的默认设置重新连接到设备，请勿使用此命令禁用服务。

步骤 1 选择**管理设备** > **网络** > **IP 接口**页或（`interfaceconfig` 命令）为接口启用 FTP 访问。

注释 请记得在进行下一步之前提交您所做的更改。

步骤 2 通过 FTP 访问接口。确保使用的是接口的正确 IP 地址。

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。请参阅下表。

IP 接口和访问设备

表 *73:* 可供访问的目录

Directory Name	说明
/avarchive /bounces /cli_logs /delivery /error_logs /ftpd_logs /gui_logs /mail_logs /rptd_logs /sntpd.logs /status /system_logs	通过“管理设备”>“系统管理”>“日志订阅”页面或 logconfig 和 rollovernow 命令自动创建以进行日志记录。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	来自下列页面和命令的数据导出到此目录，并且/或者从此目录导入（保存）： • 虚拟网关映射 (altsrchost) • XML 格式的配置数据 (saveconfig, loadconfig) • 主机访问表 (HAT) 页 (hostaccess) • 收件人访问表 (RAT) 页 (rcptaccess) • SMTP 路由页 (smtproutes) • 别名表 (aliasconfig) • 伪装表 (masquerade) • 邮件过滤器 (filters) • 全局取消订用数据 (unsubscribe) • trace 命令的测试消息
/MFM	“邮件流监控”(Mail Flow Monitoring) 数据库目录包含 GUI 提供的邮件流监控功能的数据。每个子目录包含一个说明每个文件的记录格式的自述 (README) 文件。 您可以将这些文件复制到不同的计算机以便保存记录，或将文件加载到数据库中并创建您自己的分析应用。所有目录中的所有文件的记录格式均相同；此格式在未来的版本中可能发生变化。
/periodic_reports	系统上配置的所有已存档报告均存储在此目录中。

步骤 4 使用 FTP 程序将文件上传和下载到相应的目录以及从中上传和下载。

安全复制 (scp) 访问权限

如果您的客户端操作系统支持安全复制 (scp) 命令，您可以将文件复制到可用于访问的目录表中列出的目录，或者从这些目录复制文件。例如，在以下示例中，文件 /tmp/test.txt 从客户机复制到主机名为 mail3.example.com 的设备的配置目录。

注释 用户密码（管理员）的命令提示。此示例仅供参考；您的操作系统的安全复制实施可能有所不同。

```
% 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)? yes
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
```

您可以用安全复制 (scp) 命令替代 FTP，在内容安全设备之间传输文件。

注释 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 AsyncOS 的某个较早版本 ， 第 299 页。

通过串行连接访问

如果通过串行连接连接至设备，请针对控制台端口使用以下信息。

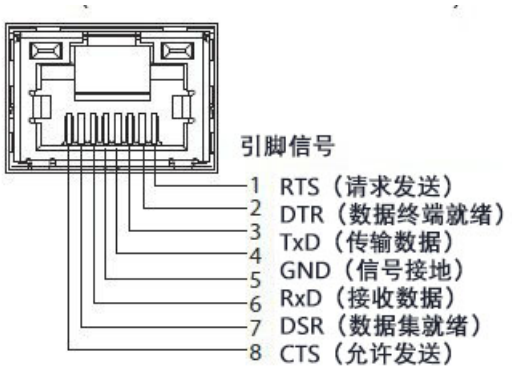
有关此端口的完整信息，请参阅设备的硬件安装指南。

相关主题

- 文档 ， 第 393 页

80 和 90 系列硬件的串行端口引脚详细信息

图 *20: 80* 和 *90* 系列硬件的串行端口引脚详细信息



70 系列硬件的串行端口引脚详细信息

下图展示了串行端口连接器的引脚编号，串行端口引脚分配表定义了串行端口连接器的引脚分配情况和接口信号。

图 *21:* 串行端口的引脚编号

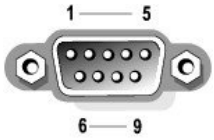


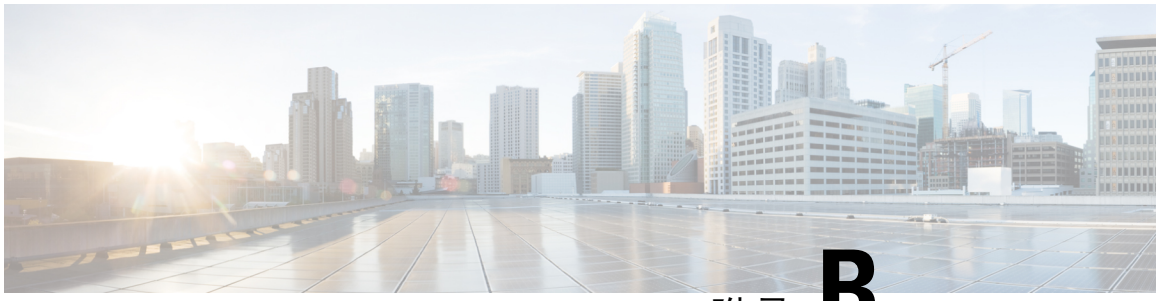
表 *74:* 串行端口引脚分配

引脚	信号	I/O	定义
1	DCD		数据载体检测
2	新加坡		串行输入
3	SOUT		串行输出
4	DTR		数据终端就绪
5	GND	n/a	信号接地
6	DSR		数据设置就绪

IP 接口和访问设备

引脚	信号	I/O	定义
7	RTS		请求发送
8	CTS		允许发送
9	RI		振铃指示器
外壳	n/a	n/a	机箱接地

IP 接口和访问设备



附录 B

分配网络和 IP 地址

本附录包含以下部分：

以太网接口

思科内容安全设备在系统的后面板上最多提供四个以太网接口，具体取决于配置（您是否具有可选的光纤网络接口）。它们的标签为：

- 管理
- Data1
- Data2
- Data3
- Data4

选择 IP 地址和网络掩码

当您配置网络时，内容安全设备必须能够选择一个唯一的接口来发送传出的数据包。此要求促使针对以太网接口的 IP 地址和网络掩码做出一些决策。此规则是指一个网络上只能有一个接口（通过将网络掩码应用到接口的 IP 地址来确定）。

IP 地址可确定任意指定网络上的一个物理接口。一个物理以太网接口可以有多个用于接受数据包的 IP 地址。具有多个 IP 地址的以太网接口可以通过该接口发送数据包，同时将其中任何一个 IP 地址作为数据包中的源地址。在实施虚拟网关技术时使用此属性。

网络掩码的作用是将 IP 地址划分为网络地址和主机地址。网络地址可被视为是 IP 地址的网络部分（位数与网络掩码匹配）。主机地址是 IP 地址的剩余数位。由 4 个 8 位二进制数构成的地址中的有效位数有时以无类域间路由 (CIDR) 方式表示，短划线后面跟随位数 (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。此示例使用两个名为 Int1 和 Int2 的接口。对于内容安全设备，这些接口名称可以表示三个接口中的任何两个接口（管理 [Management]、数据 1 [Data1]、数据 2 [Data2]）。

网络 1：

单独的接口必须出现在单独的网络上。

接口	IP 地址	网络掩码	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

发往 192.168.1.X 的数据在 Int1 传出（X 是 1 到 255 中除了您自己的地址外的任何数字，此例中为 10）。发往 192.168.0.X 的任何数据在 Int2 传出。发往不是采用这些格式的某个其他地址的任何数据包（最有可能是通过广域网或互联网传出）会发送到默认网关，默认网关必须在上述其中一个网络上。然后，默认网关会继续转发数据包。

网络 2：

两个不同接口的网络地址（IP 地址的网络部分）不能是相同的。

以太网接口	IP 地址	网络掩码	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

这种情况表示具有相同网络地址的两个不同的以太网接口存在冲突。如果来自内容安全设备的数据包发送到 192.168.1.11，则无法决定应将哪个以太网接口用于传送数据包。如果两个以太网接口连接到两个单独的物理网络，该数据包可能会传送到错误的网络，并且永远找不到其目的地。内容安全设备不允许您在发生冲突的情况下配置网络。

您可以将两个以太网接口连接到同一个物理网络，但是，您必须精心构建 IP 地址和网络掩码，以使内容安全设备可以选择唯一的传送接口。

IP 地址、接口和路由

如果您选择某个接口，以便在 GUI 或 CLI 中通过该接口执行使您可以选择某个接口的命令或功能（例如升级 AsyncOS 或配置 DNS），则路由（默认网关）优先于所选的接口。

例如，假设您具有已配置三个网络接口的内容安全设备，每个接口在不同的网段上（假定全部为 /24）：

以太网	IP
管理	192.19.0.100
Data1	192.19.1.100
Data2	192.19.2.100

并且您的默认网关是 192.19.0.1。

现在，如果您执行 AsyncOS 升级（或者使您可以选择某个接口的其他命令或功能），并选择 Data1 的 IP (192.19.1.100)，则可以预期所有 TCP 流量将通过 Data1 以太网接口传送。但是，流量不会从设置为默认网关的接口（在此例中为管理接口）传出，而是从 Data1 上标有 IP 源地址的接口传出。

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。为了做出此决策，内容安全设备组合使用数据包目标 IP 地址与其以太网接口的网络和 IP 地址设置。下表概括总结了之前的例子：

	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

用于连接内容安全设备的策略

请在连接设备时注意以下事项：

- 与邮件流量相比，管理流量（CLI、网络界面、日志传送）通常很少。
- 如果将两个以太网接口连接到同一台网络交换机，但最后却与另一台下游主机上的接口进行通信，或者连接到将所有数据回响到所有端口的网络集线器，那么使用两个接口并不会带来任何优势。
- 通过在 1000Base-T 模式下工作的接口进行的 SMTP 转换略快于通过在 100Base-T 模式下工作的同一接口进行的转换，但只有在理想的情况下才如此。
- 如果传输网络的其他部分存在瓶颈，则无法优化网络连接。与互联网或连接提供商的上游设备进行连接时，最常发生瓶颈。

您选择连接的接口数量以及处理接口的方式应取决于基础网络的复杂程度。如果网络拓扑或数据量不作要求，则不必要连接到多个接口。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。

附录 C

防火墙资讯

本章包含以下部分：

防火墙资讯

下表列出了为确保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 *75:* 防火墙端口

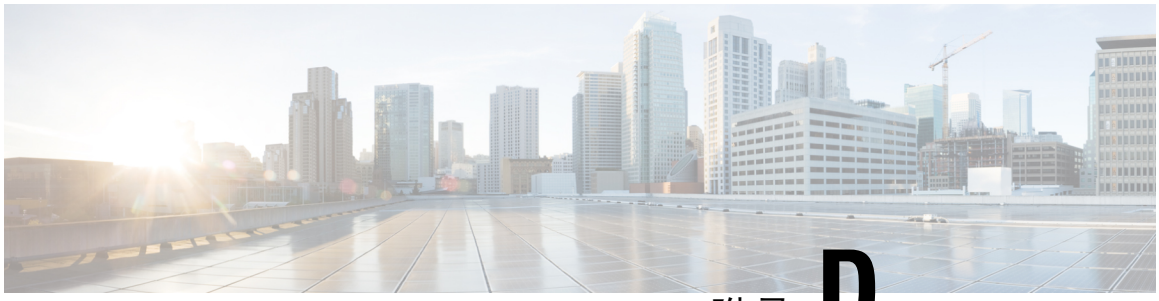
默认端口	协议	输入/输出	主机名 (Hostname)	目的
20/21	TCP	输入或输出	AsyncOS IP、FTP 服务器	通过 FTP 汇聚日志文件。 数据端口 TCP 1024 和更高端口也必须全部打开。 有关更多信息，请在知识库中搜索 FTP 端口信息。请参阅知识库文章（技术说明），第 395 页。
22	SSH	输出	AsyncOS IP	集中配置管理器配置推送。 也用于备份。
22	TCP	输入	AsyncOS IP	通过 SSH 访问 CLI，整合日志文件。
22	TCP	输出	SCP 服务器	SCP 推送到日志服务器。
23	Telnet	输入	AsyncOS IP	通过 Telnet 访问 CLI。
23	Telnet	输出	Telnet 服务器	Telnet 升级
25	TCP	输出	任意	SMTP，用于发送邮件。

防火墙资讯

25	TCP	输入	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。
53	UDP/TCP	输出	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。
80	HTTP	输入	AsyncOS IP	通过 HTTP 访问 GUI，进行系统监控。
80	HTTP	输出	downloads.ironport.com	服务更新，AsyncOS 升级。
80	HTTP	输出	upgrades.ironport.com	AsyncOS 升级。
82	HTTP	输入	AsyncOS IP	用于查看垃圾邮件隔离区。
83	HTTPS	输入	AsyncOS IP	用于查看垃圾邮件隔离区。
110	TCP	输出	POP 服务器	垃圾邮件隔离区的最终用户的 POP 身份验证。
123	UDP	输入和输出	NTP 服务器	NTP，如果时间服务器在防火墙外部。
143	TCP	输出	IMAP 服务器	垃圾邮件隔离区的最终用户的 IMAP 身份验证。
161	UDP	输入	AsyncOS IP	SNMP 查询。
162	UDP	输出	管理站	SNMP 陷阱。
389 或 3268	LDAP	输出	LDAP 服务器	LDAP，如果 LDAP 目录服务器在防火墙外部。思科垃圾邮件隔离区的 LDAP 身份验证。
636 或 3269	LDAP	输出	LDAP	LDAPS - ActiveDirectory 的全局目录服务器（使用 SSL）。
443	TCP	输入	AsyncOS IP	到 GUI 的安全 HTTP (https) 访问，以进行系统监控。
443	TCP	输出	update-static.ironport.com	验证更新服务器的最新文件。
443	TCP	输出	update-manifests.ironport.com	从更新服务器获得最新文件的列表（适用于物理硬件设备。）

443	TCP	输出	update-manifests.sco.cisco.com	从更新服务器获得最新文件的列表（适用于虚拟设备。）
443	TCP	输出	phonehome.senderbase.org	接收/发送病毒爆发过滤器。
443	TCP	输出	在网络安全设备上的“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 >“文件分析高级设置”(Advanced Settings for File Analysis) 配置的文件分析服务器URL。 在邮件安全设备上的“安全服务”(Security Services) >“文件信誉和分析”(File Reputation and Analysis) 页面的“文件分析高级设置”(Advanced Settings for File Analysis) 部分配置的文件分析服务器 URL。	在文件分析服务器上显示详细的文件分析结果。 另请参阅： • 邮件安全报告：（云文件分析）确保管理设备可以连接到文件分析服务器，第 60 页 • 网络安全报告：（云文件分析）确保管理设备可以连接到文件分析服务器，第 104 页
514	UDP/TCP	输出	系统日志服务器	系统日志记录。
1024 及更高	-	-	-	对于端口 21 (FTP)，请参阅上述信息。
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。
32137	TCP			

防火墙资讯



附录 D

网络安全管理示例

本章包含以下部分：

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。

注释 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 Web 报告和网络跟踪。有关如何启用网络跟踪和 Web 报告的信息，请参阅 使用集中 Web 报告和跟踪， 第 85 页

示例 1：调查用户

此示例演示了系统管理员将如何调查公司中的特定用户。

在此情景中，经理收到关于员工在工作时访问不当网站的投诉。为了调查此用户，系统管理员现在需要跟踪其网络活动的详细信息。

在跟踪网络活动后，就会生成一个 Web 报告，其中包含关于员工浏览历史记录的信息。

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)**。

如果您不知道用户 ID 或客户端 IP 地址，请在文本字段中键入您能够想起的用户 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 地址不需要是精确匹配项就可以返回结果。您指定的用户 ID 和客户端 IP 地址会填充到“用户”(Users) 表中。在本示例中，我们将查找有关客户端 IP 地址 `10.251.60.24` 的信息。

步骤 3 点击 IP 地址 **`10.251.60.24`**。

此时将出现 `10.251.60.24` 的“用户详细信息”页面。

从“用户详细信息”(User Details) 页面中，您可以确定“按事务总数列出的 URL 类别”(URL Categories by Total Transactions)、“按事务总数列出的趋势”(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)。

例如，这些类别使您可以了解用户 `10.251.60.24` 是否正在尝试访问被阻止的 URL，可在该页面的“域”部分下的“被阻止的事务”列中查看这些 URL。

步骤 4 点击“匹配的域”(Domains Matched) 表下的**导出 (Export)** 以查看用户尝试访问的域和 URL 的完整列表。

您可以在此处使用“网络跟踪”(Web Tracking) 功能跟踪和查看此特定用户的网络使用情况。

注释 请务必注意，使用 Web 报告功能可以检索用户访问的所有域信息，但不一定可以检索用户访问的特定 URL。有关用户访问的特定 URL、用户访问 URL 的时间以及是否允许相应 URL 等信息，可使用“网络跟踪”(Web Tracking) 页面上的“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) 文本字段中，键入用户名或 IP 地址。

在本示例中，我们将搜索用户 `10.251.60.24` 的网络跟踪信息。

屏幕上将显示搜索结果。

在此页面上，您可以查看分配了 IP 地址 `10.251.60.24` 的计算机的用户访问过的事务和 URL 的完整列表。

相关主题

下表列出了本示例中介绍的每个主题。点击链接可查看关于每个主题的详细信息。

表 *76*: 调查用户的相关主题

功能名称	功能信息
用户页面	用户报告 (Web) ， 第 93 页
“用户详细信息”(User Details) 页面	用户详细信息（Web 报告） ， 第 95 页
导出报告数据	打印和导出报告和跟踪数据 ， 第 27 页
“网络跟踪”(Web Tracking) 页面上的“代理服务”(Proxy Services) 选项卡	搜索网络代理服务处理的事务 ， 第 123 页

示例 2：跟踪 URL

在此情景中，销售经理希望了解其所在公司上星期访问量最高的前五个网站。此外，该经理希望了解哪些用户访问那些网站。

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) 部分以查看访问过的域或网站。

访问过的前 25 个网站将显示在“匹配的域”(Domains Matched) 表中。在同一个表中，您可以点击“域”(Domain) 或“IP”列中的链接查看特定地址或用户实际访问的网站。

相关主题

下表列出了本示例中介绍的每个主题。点击链接可查看关于每个主题的详细信息。

表 *77:* 跟踪 *URL* 的相关主题

功能名称	功能信息
网站页面	网站报告 ， 第 96 页

示例 3：调查受访问的排名靠前的 URL 类别

在此情景中，人力资源经理希望了解其员工在 30 天内访问的前三种 URL 类别。此外，网络经理希望获得此信息以监控带宽使用量，从而了解哪些 URL 在其网络中占用最多带宽。

下面的示例旨在向您展示如何为多人收集涵盖多个关注点的数据，与此同时只需生成一个报告。

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)**。

在本示例的“URL 类别”(URL Categories) 页面上，您可以看到，图形所显示的按事务总数列出的前 10 种 URL 类别中，访问过的“未分类 URL”(Uncategorized URLs) 有 28.2 万个，并且还访问了“即时消息”(Instant Messaging)、“仇恨言论”(Hate Speech) 和“纹身”(Tattoo) 等站点。

此时，您可以通过点击**导出 (Export)** 链接将这些原始数据导出到 Excel 电子表格，然后将此文件发送给人力资源经理。但是请记住，您的网络经理希望了解每个 URL 的带宽使用量。

步骤 2 需要新插图 - 跳过向下滚动到**匹配的 URL 类别**表以查看“使用的带宽”列。

从**匹配的 URL 类别 (URL Categories Matched)** 表中，您可以查看所有 URL 类别的带宽使用量。同样，您可以点击**导出 (Export)** 链接，然后将此文件发送给网络经理。但是，如需查看更精细的信息，请点击“即时消息”(Instant Messaging) 链接了解哪些用户占用带宽。此时将出现以下页面。

网络经理可以在此页面上查看“即时消息”(Instant Messaging) 站点访问量的前 10 名用户。

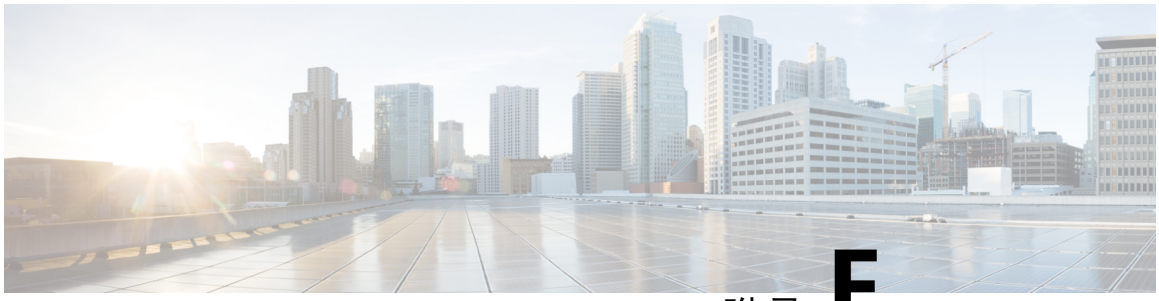
此页面显示，在过去 30 天里，用户 10.128.4.64 在即时消息网站上花了 19 小时 57 分钟，该时间的带宽使用量为 10.1 MB。

相关主题

下表列出了本示例中介绍的每个主题。点击链接可查看关于每个主题的详细信息。

表 *78:* 调查前几项 *URL* 类别的相关主题

功能名称	功能信息
URL 类别页面	URL 类别报告 ，第 97 页
导出报告数据	打印和导出报告和跟踪数据 ，第 27 页



附录 E

其他资源

本章包含以下部分：

思科通知服务

注册以接收与思科内容安全设备相关的通知，如安全建议、现场通知、销售终止或支持终止声明，以及有关软件更新和已知问题的信息。

您可以指定通知接收频率和要接收的信息类型等选项。您必须为您所用的每种产品单独注册。

要登录，请访问 http://www.cisco.com/cisco/support/notifications.html

需要 Cisco.com 账户才能注册。如果没有，请参阅注册思科账户 ， 第 395 页。

文档

以下位置提供了此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 硬件和虚拟设备信息： http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html MIB： 请参阅使用 SNMP 监控系统运行状况 ， 第 279 页。
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
思科邮件加密	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

您还可以直接从设备 GUI 访问用户指南的 HTML 联机帮助版本，方法是点击右上角的**帮助和支持 (Help and Support)**。

第三方贡献者

AsyncOS 中包含的部分软件的分销遵守 FreeBSD, Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives, Inc. 和其他第三方提供商的软件许可协议的条款、公告和条件，并且所有这些条款和条件已纳入思科许可协议。

第三方许可证信息在许可文档中提供，网址为：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

AsyncOS 产品中的软件部分基于 RRDtool 并且得到 Tobi Oetiker 的明确书面许可同意。

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

有关培训选项的信息，请参阅：

- http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html
- http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

知识库文章（技术说明）

过程

	命令或操作	目的
步骤 1	转到主产品页 (http://www.cisco.com/en/US/products/ps10164/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思科客户、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。您可以在论坛中发布主题，以咨询问题并与其他用户分享信息。

通过以下 URL 访问思科支持社区：

- 关于邮件安全和相关管理：

  https://supportforums.cisco.com/community/5756/email-security

- 针对网络安全和相关管理：

  https://supportforums.cisco.com/community/5786/web-security

客户支持

请使用以下方法获得支持：

思科 TAC：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

传统 IronPort 的支持站点：http://www.cisco.com/web/services/acquisitions/ironport.html

如果您是通过经销商或其他供应商购买了支持，请直接联系该供应商咨询您的产品支持问题：

另请参阅从设备提交或更新支持请求 ，第 368 页。

有关虚拟设备，请参阅《思科内容安全虚拟设备安装指南》。

注册思科账户

要访问 Cisco.com 上的许多资源，都需要有思科账户。

如果您没有 Cisco.com 用户 ID，可以在此注册一个账户：https://tools.cisco.com/RPF/register/register.do

相关主题

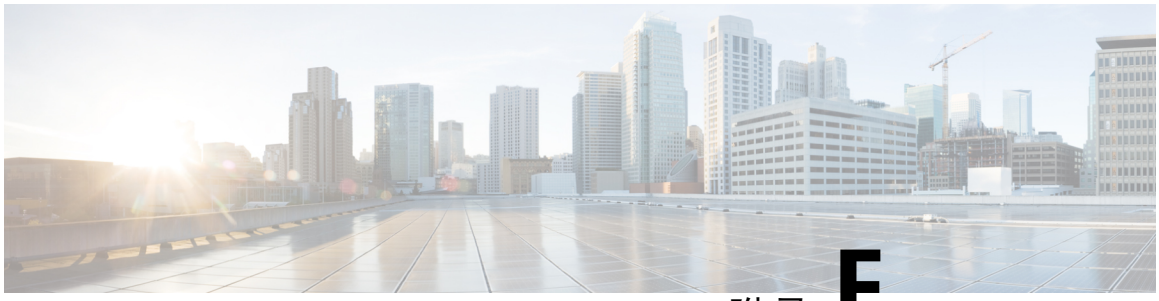
- 思科通知服务 ，第 393 页
- 知识库文章（技术说明） ，第 395 页

思科欢迎您提出意见

技术出版物团队乐于提高产品文档的质量。我们时刻欢迎您的意见和建议。您可以将评论发送至以下邮件地址：

contentsecuritydocs@cisco.com

请在邮件的主题行中加入本书的书名和书名页中的出版日期。



附录 F

最终用户许可协议

本章包含以下部分：

思科系统公司最终用户许可协议

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。

许可本软件的思科系统公司或其分公司（统称为“思科”）愿意授予您本软件许可，但前提是您必须从授权渠道购买软件并且接受本最终用户协议中的全部条款以及补充许可协议（随产品一同交付或在订购时提供）中的其他许可限制要求（统称为“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，“获批来源”指 A) 思科；或 (B) 经思科授权在您所在大区内向最终用户分销/出售思科设备、软件和服务的分销商或系统集成商；或 (C) 由任何该等分销商或系统集成商根据与思科签署的分销商协议条款授权在您所在大区内向最终用户分销/出售思科设备、软件和服务的经销商。

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许可协议；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。

最终用户许可协议

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。除非本协议另作明确规定，本软件只能与客户从获批来源购得的思科设备配套使用，客户应无权利且客户明确同意不：

(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”部分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。另外，“政府最终用户购买者”和“有限担保声明与最终用户许可协议”节中的条款在本协议终止后仍然有效。

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、技术或该等软件、文档、技术的直接产品（下文统称为“软件和技术”）必须服从美国的法律和法规以及任何其他适用国家/地区的法律和法规的出口管制要求。客户应遵守适用于思科软件和技术的出口、再出口、转让及使用的法律与法规，并将取得所有必要的美国联邦及地方的批准、审批或许可。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/c/en/us/about/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组件，思科在文档、自述文件、第三方点击接受协议或其他地方（如 http://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

最终用户许可协议

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，同样不能排除该等暗示条款、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、供应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）赔偿不得超过授权来源供应商提供的被索赔软件的购买价格，如果该软件为其他产品一部分，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，（即，两次或更多索赔的存在不会提高此限制）。

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。该软件赔偿责任限制为累积性，不是针对单件事故（即，两次或两次以上的索赔不得提高此限制）。本协议中无任何内容应限制 (i) 思科及其关联公司、高级职员、董事、雇员、代理、供应商和许可方因其过失造成的人身伤害或死亡而对客户负有的责任，(ii) 思科因其欺诈性失实陈述而负有的责任，或 (iii) 思科负有的根据适用法律不能排除的责任。

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。

有关适用于思科产品的产品保修条款和其他信息，请访问：

http://www.cisco.com/c/en/us/products/warranty-listing.html

思科系统公司内容安全软件终端用户补充许可协议

重要信息：请仔细阅读

最终用户许可协议

这种补充终端用户许可协议（“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”）与思科之间根据终端用户许可协议（“EULA”）许可的软件产品的其他条款和条件（统称为“协议”）。本 SEULA 中使用的但未定义的大写术语应按照 EULA 中的意思解释。如果 EULA 和本 SEULA 的条款和条件冲突，那么将优先遵照本 SEULA 的条款和条件。

除 EULA 中有关您访问和使用本软件的其他限制之外，您同意在任何时候遵循本 SEULA 的条款和条件。

下载、安装或使用本软件表示接受本协议，并且您同意您本人和您代表的业务实体受本协议的约束。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。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，而且只有您是原始终端用户购买者，此权利才适用。

在本 SEULA 中，您订购的产品名称和产品说明为思科邮件安全设备（“ESA”）、思科系统网络安全设备（“WSA”）或思科系统安全管理应用（“SMA”）（统称为“内容安全”）及其对等的虚拟设备（“软件”）：

思科邮件 AsyncOS

思科网络 AsyncOS

思科管理 AsyncOS

思科反垃圾邮件、Sophos 防病毒

思科邮件爆发过滤器

Cloudmark 反垃圾邮件

思科图像分析工具

McAfee 防病毒

思科智能多重扫描

思科 RSA 防数据丢失

思科邮件加密

思科邮件传送模式

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

思科邮件消息跟踪

思科邮件集中隔离

思科 Web 报告

思科网络策略和配置管理

思科高级网络安全管理（带 Splunk）

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共密钥加密

加密设备的大型附件处理

加密设备的安全邮箱许可

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，向终端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”是指公司和思科之间或公司和思科经销商之间的购买协议、评估协议、测试、预发布协议或类似协议，或包含本协议授予的软件许可的购买条款，由思科接受的任何购买订单的相关有效条款。

“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）个人姓名、用户名、邮件地址和任何其他个人身份信息。

“服务器”是指在网络上为多名用户管理或提供网络资源的单个物理计算机或设备。

“服务”是指思科软件订用服务。

“服务说明”是指以下网站上提供的软件订用支持服务说明：http://www.cisco.com/c/en/us/about/legal/service-descriptions.html。

“遥测数据”表示公司邮件和网络流量的样本，包括有关邮件消息和网络请求属性的数据以及有关公司的思科硬件产品如何处理不同类型的邮件消息和网络请求。遥测数据所包括的邮件消息元数据和网络请求经匿名处理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用的长度，如订购文档中所示。

“虚拟设备”是指思科的邮件安全设备、网络安全设备和安全管理设备的虚拟版本。

“虚拟机”表示如服务器一般可运行其自身操作系统并执行应用的软件容器。

附加许可条款和条件

许可证授予并同意数据收集条款

软件许可。

最终用户许可协议

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，仅与面向终端用户的公司服务条款相关。许可使用本软件的终端用户数，限制为订购文档中规定的终端用户数。如果与提供公司服务相关的终端用户数量超过订购文档中规定的终端用户数量，公司将联系授权渠道购买更多该软件的许可证。该许可的持续时间和范围在订购文档中详细定义。订购文档根据软件许可的条款替代 EULA。除此处授予的许可权利外，思科、思科的经销商或其各自的许可者并未授予公司任何软件拥有权利、所有权或利益。您对软件升级的权利受服务说明的约束。此协议与服务拥有相同的期限。

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。思科不收集也不使用遥测数据中的个人可识别信息。思科可与第三方共享汇总和匿名的遥测数据以协助我们改进您的用户体验以及其他思科安全产品和服务。公司可通过禁用软件中的SenderBase网络参与，随时终止思科收集遥测数据的权利。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 Cisco Systems Inc. 终端用户许可协议、隐私声明和软件订用支持服务的服务说明。

索 引

符號

A

B

F

G

J

K