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 安全邮件和 Web 管理器以便为思科安全邮件和 Web 管理器解决方案提供服务：

	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, on page 2。
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》。

	在这些设备上	相应操作	更多信息
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 , on page 2、为设置做准备 , on page 3和运行系统设置向导, on page 10。
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, on page 14开始。

SMA 兼容性矩阵

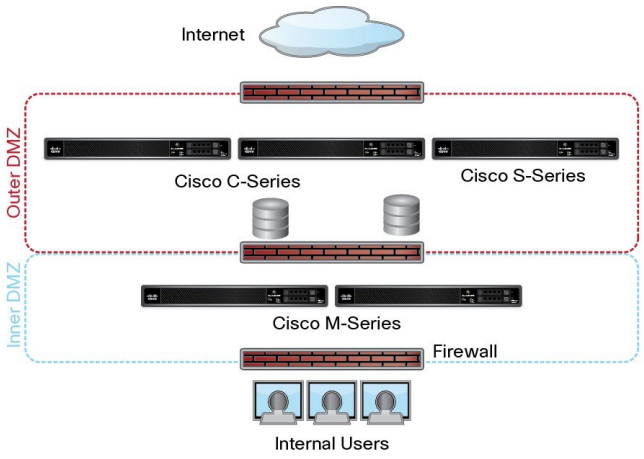
欲了解您的安全管理设备与邮件安全设备和网络安全设备的兼容性，以及在导入和发布网络案例设备配置时的配置文件兼容性，请参阅位于以下位置的兼容性列表：
http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html。

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。

Figure 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 , on page 2。

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, on page 2。

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 , on page 2。

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 , on page 3。

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, on page 4。

步骤 6 收集系统设置的相关信息。请参阅收集设置信息, on page 4。

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

Note 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”(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
- 网络掩码

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。

Note 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

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 安全邮件和 Web 管理器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。

Note 有关网络和 IP 地址的详细信息，请参阅分配网络和 IP 地址。

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	管理员口令		为“管理员”账户选择新的口令：

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, on page 5
- 关于访问Web 界面 , on page 6
- 访问旧 Web 界面, on page 8
- 访问 Web 界面 , on page 7
- 访问命令行界面, on page 8
- 支持的语言, on page 8
- 在深色模式下访问新 Web 界面, on page 9

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。

Table 1: 支持的浏览器和版本

浏览器	**Windows 7**	**MacOS 10.6**
Safari	-	7.0 及更高版本
Google Chrome	最新的稳定版本	最新的稳定版本
Microsoft Internet Explorer	11.0	—

浏览器	Windows 7	MacOS 10.6
Mozilla Firefox	最新的稳定版本	最新的稳定版本

- Internet Explorer 11.0（仅限 Windows 7）
- Safari（7 及更高版本）
- Firefox（最新的稳定版本）
- Google Chrome（最新的稳定版本）

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，因为单击界面中的某些按钮或链接会导致打开其他窗口。

为了实现HTML 页面的无缝导航和呈现，思科建议使用以下浏览器访问设备的新 Web 界面（AsyncOS 12.0 及更高版本）：

- Google Chrome（最新的稳定版本）
- Mozilla Firefox（最新的稳定版本）

您可以在任何受支持的浏览器上访问设备的旧 Web 界面。

设备的新 Web 界面（AsyncOS 12.0 及更高版本）支持的分辨率介于 1280x800 和 1680x1050 之间。对于所有浏览器，最佳查看分辨率为 1440x900。

Note Cisco 不建议以更高的分辨率查看设备的新 Web 界面。

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。

Note 不要使用以下方式同时执行任何配置更改：

- 同一浏览器上的多个选项卡。
- 同一系统或两个不同系统上的多个浏览器。

此外，不要使用并发 Web 界面和 CLI 会话，否则可能会导致意外行为。

访问 Web 界面

步骤 1 打开 Web 浏览器并输入设备的 IP 地址或主机名。

步骤 2 [仅限新 Web 界面] 您可以通过以下方式之一访问新 Web 界面：

Note 新 Web 界面使用 AsyncOS API HTTP/HTTPS 端口 (6080/6443) 和 trailblazer HTTPS 端口 (4431)。您可以在 CLI 中使用 `trailblazerconfig` 命令来配置 trailblazer HTTPS 端口。确保在防火墙中打开 trailblazer HTTPS 端口。

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

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

  有关 trailblazerconfig CLI 命令的详细信息，请参阅Trailblazerconfig 命令。

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

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

- 登录到旧 Web 界面，然后单击 **Security Management appliance is getting a new look. Try it!!**链接以访问新 Web 界面。

Important

- 请确保设备上已启用 AsyncOS API。
- 您必须再次登录到设备的旧版 Web 界面。
- 如果已启用 `trailblazerconfig`，则必须在防火墙上打开配置的 HTTPS 端口。默认 HTTPS 端口为 4431。

  确保 DNS 服务器可以解析为访问设备指定的主机名。

- 如果 `trailblazerconfig` 已被禁用，在**管理设备 (Management Appliance) > 网络 (Network) > IP 接口 (IP Interfaces)** 中配置的 AsycnOS API 端口会在防火墙上打开。默认 AsyncOS API HTTP/HTTPS 端口为 6080/6443。

步骤 3 输入以下默认值：

- 用户名：**admin**

- 口令：`ironport`

Note 使用 Web 界面或命令行界面完成“系统设置向导”后，此口令将无效。

访问旧 Web 界面

注释 您必须登录到安全管理设备才能访问旧 Web 界面。有关详细信息，请参阅访问 Web 界面 ，第 7 页

要启用和配置报告、邮件跟踪、隔离区、网络访问和监控系统状态，必须访问旧 Web 界面。

要从新 Web 界面访问旧 Web 界面，请单击齿轮图标 ，如下图所示：

图 2: 访问旧 ***Web*** 界面

旧 Web 界面将在新浏览器窗口中打开。您必须重新登录，才能访问该页面。

如果要完全注销该设备，则需要注销设备的新旧 Web 界面。

访问命令行界面

在邮件和网络管理器设备中，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。
- 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。）

在深色模式下访问新 Web 界面

深色模式是一种反向配色方案，在深色背景上使用浅色字体、用户界面元素和图标。现在，您可以在设备的新 Web 界面上使用深色模式。

要切换到设备上的深色模式 Web 界面，请单击新 Web 界面右上角的用户信息部分，然后选择**深色模式 (Dark Mode)**。

使用 Swagger UI 访问安全管理设备的 API 接口

Sw UI 允许您可视化设备的 API 资源并与之交互。这是根据您的 API 规范自动生成的。有关详细信息，请参阅 https://swagger.io/tools/swagger-ui/。

您可以通过以下任何一种方式在安全管理设备的新 Web 界面上登录 Swaver UI：

- 使用以下 URL - `https://example.com:<trailblazer-https-port>/swagger`

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

  注释 必须启用设备上的 trailblazer HTTPS 端口才能访问 Swaver UI。有关 `trailblazerconfig` CLI 命令的详细信息，请参阅 Trailblazerconfig 命令。

- 登录设备的新 Web 界面。单击右上角的 **?** 按钮，然后从下拉列表选择 **API 帮助：Swagger (API Help: Swagger)**。Swagger UI 将打开一个新的浏览器窗口。

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

完成为设置做准备 , on page 3中的所有任务。

Caution “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。

Caution 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。

Note 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口令。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。

系统设置向导概述

步骤 1 启动系统设置向导 , on page 11

步骤 2 查看最终用户许可协议, on page 11

步骤 3 配置系统设置, on page 11

- 通知设置和自动支持
- 系统时间设置
- 管理员口令

步骤 4 配置网络设置, on page 12

- 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, on page 12

浏览各个向导页面并仔细检查步骤 4 的配置。您可以通过单击**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, on page 13

启动系统设置向导

要启动该向导，请按访问 Web 界面 , on page 7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，然后单击开始设置 (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。

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，然后单击添加条目 (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。

设置 口令

您必须更改 AsyncOS 管理员账户的口令：adminpassphrase。将口令保存在安全的位置。对口令所做的更改会立即生效。

Note 如果在重置口令后取消系统设置，系统不会撤消您所做的口令更改。

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)。

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。

Note 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。

Note 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。

Note 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，请单击页面底部的**上一步 (Previous)** 并编辑信息。

在检查信息后，单击**安装此配置 (Install This Configuration)**。然后在出现的确认对话框中单击**安装 (Install)**。

当您单击**安装此配置 (Install This Configuration)**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 (System Setup Next Steps)** 页面。如果此页面不自动显示，则可通过选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 后续步骤 (Next Steps)**。

单击“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, on page 2中显示了支持的邮件和网络安全设备。

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

“安全设备 (Security Appliances)”页面将显示已添加的托管设备。“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
- 向每台托管邮件安全设备添加集中邮件跟踪服务
- 向每个托管邮件安全设备添加集中垃圾邮件隔离区服务
- 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
- 将集中 Web 报告服务添加到每个托管网络安全设备
- 添加网络安全设备并将其与主配置版本关联

编辑受管设备配置

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

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

步骤 3 在“安全设备”(Security Appliance) 部分中，单击要编辑的设备的名称。

步骤 4 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。

Note 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 5 单击**提交 (Submit)** 以提交对页面所做的更改，然后单击“确认更改” (Commit Changes) 以确认所做的更改。

从受管设备列表中删除设备

Before you begin

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

步骤 2 选择**管理设备 > 集中化服务 > 安全设备**。

步骤 3 在“安全设备”(Security Appliances) 部分中，单击要删除的受管设备所在行中的垃圾桶图标。

步骤 4 在确认对话框中，单击**删除 (Delete)**。

步骤 5 提交并确认更改。

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
- 跟踪
- 垃圾邮件隔离区
- 集中策略、病毒和病毒爆发隔离区

网络安全服务：

- 集中策略、病毒和病毒爆发隔离区
- 管理网络安全设备

确认和放弃配置更改

在思科内容安全设备 GUI 中更改大多数配置后，必须明确确认更改。

Figure 3: “确认更改 ***(Commit Changes)***” 按钮

收件人	相应操作
确认所有待定的更改	单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，然后单击“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	单击窗口右上角的橙色确认更改 (Commit Changes) 按钮，然后单击放弃更改 (Abandon Changes)。

Note 注销再登录到新的思科内容安全管理 Web 界面后，在新 Web 界面上更新对旧 Web 界面所做的配置更改。

相关主题

- 回滚到以前已确认的配置