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，如以下章节所述 监控系统状态

Note 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。

思科内容安全管理设备许可

注释 从 AsynOS 15.5 版本开始，将**不再支持本地用户**的经典许可。您将无法再在经典许可模式下订购新功能许可证或续订现有功能许可证。

前提条件：确保在思科智能软件管理器门户中创建智能账户，并在安全邮件和 Web 管理器上启用思科智能软件许可。有关详细信息，请参阅 智能软件许可， 第 3 页 。

从 AsyncOS 15.5 版本开始，仅当许可证文件包含云功能密钥时，才能使用 `loadlicense` 命令加载许可证。

如果许可证文件不包含云功能密钥，则无法加载许可证，并且您将收到一条通知消息，通知您使用云许可证重试或使用 `license_smart` 命令执行智能许可任务。

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。

要想	相应操作
查看思科安全邮件和 Web 管理器的所有活动功能密钥	[仅限新 Web 界面] 在云邮件安全管理控制台上，点击齿轮图标以加载旧式 Web 界面。 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **功能密钥 (Feature Keys)**。

智能软件许可

概述

通过智能软件许可，您可以无缝管理和监控思科内容安全管理设备许可证。要激活智能软件许可，必须向思科智能软件管理器 (CSSM) 注册设备。CSSM 是集中式数据库，用于维护您购买和使用的所有思科产品的许可详细信息。使用智能许可，您可以向一个令牌注册，而不是使用产品授权密钥 (PAK) 在网站上逐一注册它们。

注册设备后，即可通过 CSSM 门户跟踪设备许可证并监控许可证使用情况。设备上安装的智能代理将设备与 CSSM 连接，并将许可证使用信息传递给 CSSM 以跟踪使用情况。

有关思科智能软件管理器的信息，请参阅 https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html。

- 请确保您的设备具有互联网连接。
- 联系思科销售团队，在思科智能软件管理器门户 (https://software.cisco.com/#module/SmartLicensing) 中创建智能账户，或者在您的网络中安装思科智能软件管理器卫星。

  有关思科智能软件管理器用户账户创建或思科智能软件管理器卫星安装的更多信息，请参阅 Https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing _ Deployment_Guide.html。

  对于不想直接向互联网发送许可证使用信息的用户，可以在本地安装智能软件管理器卫星，它可以提供 CSSM 功能子集。下载并部署该卫星应用之后，即可在本地安全地管理许可证，无需使用互联网向 CSSM 发送数据。CSSM 卫星会定期向云发送信息。

注释 如果要使用智能软件管理器卫星，请使用智能软件管理器卫星增强版6.1.0升级。

- 经典许可证（传统）的现有用户应将其经典许可证迁移到智能许可证。

  请参阅https://video.cisco.com/detail/video/5841741892001/convert-classic-licenses-to-smart-licenses?autoStart=true&q=classic。

- 设备的系统时钟必须与 CSSM 的系统时钟同步。设备系统时钟与 CSSM 的任何偏差都将导致智能许可操作失败。

注释 如果您有互联网连接并想通过代理连接到 CSSM，则必须使用**安全管理 (System Administration) -> 更新设置 (Update Settings)** 为设备配置的相同代理

许可证预留

您可以为安全邮件和 Web 管理器中启用的功能保留许可证，而无需连接到 Cisco 智能软件管理器（CSSM）门户。这主要适用于在高度安全的网络环境中部署安全邮件和 Web 管理器且不与互联网或外部设备通信的用户。

可以在以下任一模式下保留功能许可证：

- **特定许可证预留 (SLR)** - 使用此模式在给定时间段内为单个功能（例如，“邮件处理”）预留许可证。
- **永久许可证预留 (PLR)** - 使用此模式为所有功能永久预留许可证。

有关如何在安全邮件和 Web 管理器中保留许可证的详细信息，请参阅预留功能许可证，第 11 页。

设备主导型转换

在使用智能许可注册安全邮件和 Web 管理器后，所有现有的有效传统许可证将使用设备主导转换 (DLC) 流程自动转换为智能许可证。这些转换的许可证在 CSSM 门户的虚拟帐户中更新。

注释 如果安全邮件和 Web 管理器包含有效的功能许可证，则会启动 DLC 进程。

注释 DLC 过程完成后，您将无法将智能许可证转换为经典许可证。如需帮助，请与 Cisco TAC 联系。

注释 完成 DLC 进程大约需要一个小时。

您可以通过以下任一方式查看 DLC 进程的状态 - “成功”或“失败”：

- 网络界面的 **系统管理 (System Administration)** > **智能软件许可 (Smart Software Licensing)** 页面“智能软件许可状态”(Smart Software Licensing Status) 部分下的设备主导转换状态字段。
- CLI 中 `license_smart` > `status` 子命令中的转换状态条目。

注释 当DLC进程失败时，系统会发送系统警报，详细说明失败原因。您需要修复此问题，然后在CLI中使用 `license_smart` > `conversion_start` 子命令将传统许可证手动转换为智能许可证。

注释 DLC 进程仅适用于传统许可证，不适用于许可证预留的 SLR 或 PLR 模式。

智能软件许可 - 新用户

如果您是新的（首次）智能软件许可用户，则必须执行以下程序来激活智能软件许可：

	请	详细信息
第 1 步	启用智能软件许可	启用智能软件许可，第 6 页
第 2 步	向思科智能软件管理器注册思科安全邮件和 Web 管理器	向思科智能软件管理器注册设备，第 7 页
第 3 步	申请许可证（功能密钥）	申请许可证，第 9 页

从传统许可迁移到智能软件许可 - 现有用户

如果要从经典许可迁移到智能软件许可，则必须执行以下程序来激活智能软件许可：

	请	详细信息
第 1 步	启用智能软件许可	启用智能软件许可，第 6 页

	请	详细信息
第 2 步	向思科智能软件管理器注册思科安全邮件和 Web 管理器	向思科智能软件管理器注册设备，第 7 页
第 3 步	申请许可证（功能密钥）	申请许可证，第 9 页

请注意：在使用智能软件许可注册安全邮件和 Web 管理器后，所有现有的有效传统许可证将使用设备主导转换 (DLC) 流程自动转换为智能许可证。有关详细信息，请参阅 设备主导型转换 ，第 4 页。

气隙模式下的智能软件许可 - 新用户

如果您使用的是在气隙模式下运行的思科安全邮件和 Web 管理器，并且是首次激活智能软件许可，则必须执行以下程序：

	请	详细信息
第 1 步	启用智能软件许可	启用智能软件许可，第 6 页
第 2 步	第一次在气隙模式下获取和使用 VLN、证书和密钥详细信息以注册思科安全邮件和 Web 管理器	在气隙模式下获取和使用 VLN、证书和密钥详细信息以注册思科安全邮件和 Web 管理器，第 8 页
第 3 步	申请许可证（功能密钥）	申请许可证，第 9 页

气隙模式下的智能软件许可 - 现有用户

如果您使用的是在气隙模式下运行的思科安全邮件和 Web 管理器，则必须执行以下程序以激活智能软件许可：

	请	详细信息
第 1 步	启用智能软件许可	启用智能软件许可，第 6 页
第 2 步	通过许可证预留注册在的气隙模式下运行的思科安全邮件和 Web 管理器	预留功能许可证，第 11 页
第 3 步	申请许可证（功能密钥）	申请许可证，第 9 页

启用智能软件许可

步骤 1 选择**托管设备 > 系统管理 > 智能软件许可**。

步骤 2 点击**启用智能软件许可 (Enable Smart Software Licensing)**。

要了解智能软件许可，点击“详细了解智能软件许可”(earn More about Smart Software Licensing) 链接。

步骤 3 阅读有关智能软件许可的信息后，点击**确定 (OK)** 。

步骤 4 确认您的更改。

下一步做什么

启用智能软件许可后，传统许可模式下的所有功能都自动在智能许可模式下可用。如果您是传统许可模式下的现有用户，您有90天的评估期，可以使用智能软件许可功能，无需向CSSM注册设备。

在到期之前以及评估期到期时，您会定期（第 90 天、第 60 天、第 30 天、第 15 天、第 5 天和最后一天）收到通知。在评估期期间或之后，您可以向 CSSM 注册设备。

注释 在传统许可模式下没有有效许可证的新虚拟设备用户没有评估期，即使他们启用了智能软件许可功能。只有在传统许可模式下具有有效许可证的现有虚拟设备用户才有评估期。如果新虚拟设备用户希望评估智能许可功能，请联系思科销售团队，向智能账户添加评估许可证。注册后，评估许可证可用于评估目的。

注释 在设备上启用“智能许可”功能后，您将无法从智能许可模式回滚到经典许可模式。

向思科智能软件管理器注册设备

要向思科智能软件管理器注册设备，必须在“系统管理”菜单下启用智能软件许可功能。

步骤 1 转到**托管设备 (Managed Appliance) > 系统管理 (System Administration) > 智能软件许可 (Smart Software Licensing)**。

步骤 2 选择**智能许可证注册 (Smart License Registration)** 选项。

步骤 3 点击**确认 (Confirm)**。

步骤 4 如果想要更改**传输设置 (Transport Settings)**，请点击**编辑 (Edit)**。可用选项包括：

- 直接：通过 HTTPS 直接将设备连接到思科智能软件管理器。默认情况下，此选项已选中。
- 传输网关：通过传输网关或智能软件管理器卫星将设备连接到思科智能软件管理器。选择此选项时，必须输入传输网关或智能软件管理器卫星的 URL，然后点击“确定”(OK)。此选项支持 HTTP 和 HTTPS。在 FIPS 模式下，传输网关仅支持 HTTPS。有关传输网关的信息，请参阅 Https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing _ Deployment_Guide.html。

  使用您的登录凭证访问思科智能软件管理器门户

  (https://software.cisco.com/#module/SmartLicensing)。导航到门户的“虚拟账户”(Virtual Account) 页面，然后访问“常规”(General) 选项卡，以生成新令牌。复制设备的产品实例注册令牌。

  有关产品实例注册令牌创建的信息，请参阅 Https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing _ Deployment_Guide.html。

步骤 5 切换回设备，粘贴产品实例注册令牌。

步骤 6 点击**注册 (Register)**。

步骤 7 在“智能软件许可”(Smart Software Licensing) 页面上，您可以勾选“如果已注册，请重新注册此产品实例”(Reregister this product instance if it is already registered) 复选框，重新注册设备。请参阅重新向思科智能软件管理器注册设备，第 10 页。

下一步做什么

产品注册过程需要几分钟，您可以在“智能软件许可”(Smart Software Licensing) 页面上查看注册状态。

注释 在启用智能软件许可并向思科智能软件管理器注册内容安全网关后，思科云服务门户就会自动启用，同时在您的邮件网关上注册。

在气隙模式下获取和使用 VLN、证书和密钥详细信息以注册思科安全邮件和 Web 管理器

执行以下步骤以获取 VLN、证书和密钥详细信息，并使用这些详细信息注册在气隙模式下运行的虚拟思科安全邮件和 Web 管理器：

步骤 1 注册在气隙模式之外运行的虚拟思科安全邮件和 Web 管理器。有关如何注册虚拟思科安全邮件和 Web 管理器的信息，请参阅向思科智能软件管理器注册设备，第 7 页。

步骤 2 在 CLI 中输入 `vlninfo` 命令。此命令将显示 VLN、证书和密钥详细信息。复制这些详细信息并保留这些详细信息，以便之后使用。

注释 `vlninfo` 命令可在智能许可模式下使用。如需了解有关 `vlninfo` 更多信息，请参阅 vlninfo，第 32 页。

步骤 3 使用预留的许可证注册在气隙模式下运行的虚拟思科安全邮件和 Web 管理器。有关如何使用许可证预留注册虚拟思科安全邮件和 Web 管理器的详细信息，请参阅预留功能许可证，第 11 页。

步骤 4 在 CLI 中输入 `updateconfig > VLNID` 子命令。

步骤 5 当系统提示您输入 VLN 时，请粘贴复制的 VLN（在步骤 2 中）。

注释 `updateconfig > VLNID` 子命令仅可在许可证预留模式下使用。有关如何使用 `updateconfig -> VLNID` 子命令的详细信息，请参阅 updateconfig，第 30 页。

注释 通过使用 `VLNID` 子命令，您可以添加或更新 VLNID。如果输入的 VLN 不正确，可使用更新选项来修改 VLN。

步骤 6 在 CLI 中输入 `CLIENTCERTIFICATE` 命令。

步骤 7 当系统提示您输入这些详细信息时，粘贴复制的证书和密钥详细信息（在步骤 2 中）。

申请许可证

成功完成注册过程后，必须按需申请思科安全邮件和 Web 管理器的功能许可证。

注释 在许可证预留模式（气隙模式）下，必须先请求许可证，然后才能将许可证令牌应用于思科安全邮件和 Web 管理器。

步骤 1 依次选择**管理设备 > 系统管理 > 许可证**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中您要申请的许可证对应的“许可证申请/发放”列下的复选框。

步骤 4 点击**提交 (Submit)**。

注释 默认情况下，邮件处理许可证可用。您不能激活、停用或发放此许可证。没有任何评估期或不合规状态的邮件处理许可证。

下一步做什么

当许可证被过度使用或者到期时，它们将转至违规 (OOC) 模式，并且为每个许可证提供 30 天的宽限期。在到期之前以及 OCC 宽限期到期时，您会定期（第 30 天、第 15 天、第 5 天和最后一天）收到通知。

OOC 宽限期到期后，您不能使用许可证，而且这些功能将不可用。要再次访问这些功能，您必须在 CSSM 门户上更新许可证，并续约授权。

发放许可证

步骤 1 依次选择**管理设备 > 系统管理 > 许可证**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 取消选中您要发放的许可证对应的“许可证申请”列下的复选框。

步骤 4 点击**提交 (Submit)**。

注释 您不能发放邮件处理许可证。

从思科智能软件管理器注销设备

步骤 1 依次选择**管理设备 > 系统管理 > 智能软件许可**。

步骤 2 从**操作 (Action)** 下拉列表中选择**取消注册 (Deregister)**，然后点击**转到 (Go)**。

步骤 3 点击**提交 (Submit)**。

重新向思科智能软件管理器注册设备

步骤 1 依次选择**管理设备 > 系统管理 > 智能软件许可**。

步骤 2 从**操作 (Action)** 下拉列表中选择**重新注册 (Reregister)**，然后点击**转到 (Go)**。

下一步做什么

有关注册流程的信息，请参阅向思科智能软件管理器注册设备，第 7 页。

在不可避免的场景下，重置设备配置后，您可以重新注册设备。

更改传输设置

只能在向 CSSM 注册设备之前更改传输设置。

注释 只能在启用智能许可时更改传输设置。如果已注册设备，必须取消注册设备，才能更改传输设置。更改传输设置后，必须再次注册设备。

有关如何更改传输设置的信息，请参阅向思科智能软件管理器注册设备，第 7 页。

续约授权和证书

向思科智能软件管理器注册设备后，您可以续订证书。

注释 只能在成功注册设备后续约授权。

步骤 1 依次选择**管理设备 > 系统管理 > 智能软件许可**。

步骤 2 从**操作 (Action)** 下拉列表中选择适当的选项：

- **立即续约授权**
- **立即续约证书**

步骤 3 点击**前往 (Go)**。

预留功能许可证

启用许可证预留

开始之前

确保您已在思科安全邮件和 Web 管理器中启用智能许可模式。

注释 您还可以在 CLI 中使用 `license_smart > enable_reservation` 子命令启用许可证预留。有关详细信息，请参阅或与此版本相关的 CLI 参考指南的“智能团建许可证”一章中的“命令：参考示例”部分。

步骤 1 前往思科安全邮件和 Web 管理器中的**系统管理 (System Administration)** > **智能软件许可 (Smart Software Licensing)** 页面。

步骤 2 选择 **特定/永久许可证预留** 选项。

步骤 3 点击**确认 (Confirm)**。

许可证预留（SLR 或 PLR）已在思科安全邮件和 Web 管理器中启用。

下一步做什么

- 您需要注册许可证预留。有关详细信息，请参阅注册许可证预留， 第 11 页。
- 如果需要，您可以在思科安全邮件和 Web 管理器中禁用许可证预留。有关详细信息，请参阅 禁用许可证预留， 第 15 页。

注册许可证预留

开始之前

确保您已在您的思科安全邮件和 Web 管理器上启用许可证预留 （SLR 或 PLR）。

注释 您还可以使用 CLI 中的 license_smart > request_code 和 license_smart > install_authorization_code 子命令注册功能许可证。

步骤 1 前往思科安全邮件和 Web 管理器中的**系统管理 (System Administration)** > **智能软件许可 (Smart Software Licensing)** 页面。

步骤 2 点击**注册 (Register)**。

步骤 3 点击**复制代码 (Copy Code)** 以复制请求代码。

注释 您需要在 CSSM 门户中使用请求代码以生成授权代码。

注释 每 24 小时发送一次系统警报，指示您需要安装授权码。

步骤 4 点击**下一步 (Next)**。

注释 点击取消按钮时，系统会取消请求代码。您无法在思科安全邮件和 Web 管理器中安装授权码（在 CSSM 门户中生成）。在思科安全邮件和 Web 管理器中取消请求代码后，请联系思科 TAC 以帮助您删除预留的许可证。

步骤 5 转到 CSSM 门户生成授权代码，以保留特定或所有功能的许可证。

注释 有关如何生成授权代码的详细信息，请转至 智能软件许可在线帮助（cisco.com）上帮助文档的资产：许可证选项卡 > 保留许可证 部分。

步骤 6 通过以下任一方式将从 CSSM 门户获取的授权代码粘贴到思科安全邮件和 Web 管理器中：

- 选择**复制并粘贴授权码 (Copy and Paste authorizationc code)** 选项，然后将授权代码粘贴到“复制并粘贴授权码”(Copy and Paste authorization code) 选项下的文本框中。
- 选择**从系统中上传授权代码 (Upload authorization code from the system)** 选项，然后点击**选择文件 (Choose File)** 以上传授权代码。

步骤 7 点击**安装授权码 (Install Authorization Code)**。

注释 安装授权码后，您会收到指示智能代理已成功安装许可证预留的系统警报。

许可证预留（SLR 或 PLR）已在思科安全邮件和 Web 管理器中注册。在 SLR 中，仅将预留的许可证移至“合规预留”状态。对于 PLR，思科安全邮件和 Web 管理器中的所有许可证都将变为“保留合规”(Reserved in Compliance) 状态。

注释 “保留合规”(Reserved in Compliance)：状态表示思科安全邮件和 Web 管理器有权使用该许可证。

下一步做什么

- [仅适用于SLR]：如果需要，您可以更新许可证预留。有关详细信息，请参阅更新许可证预留，第 13 页。
- [适用于SLR和PLR]：如果需要，您可以删除许可证预留。有关详细信息，请参阅删除许可证预留，第 14 页。
- 如果需要，您可以在思科安全邮件和Web管理器中禁用许可证预留。有关详细信息，请参阅禁用许可证预留，第 15 页。

更新许可证预留

您可以为新功能保留许可证，或者修改功能的现有许可证保留。

注释 您只能更新特定许可证预留，而不能更新永久许可证预留。

注释 您还可以在 CLI 中使用 `license_smart > reauthorize` 子命令更新许可证预留。

步骤 1 转到 CSSM 门户以生成授权代码，以更新已保留的许可证。

注释 有关如何生成授权代码的详细信息，请转至 智能软件许可在线帮助（cisco.com）上帮助文档的 资产：产品实例选项卡 > 更新保留的许可证 部分。

步骤 2 复制从 CSSM 门户获取的授权代码。

步骤 3 前往思科安全邮件和 Web 管理器中的**系统管理 (System Administration)** > **智能软件许可 (Smart Software Licensing)** 页面。

步骤 4 从“操作”下拉列表中选择 **重新授权**，然后点击 **执行**。

步骤 5 通过以下任一方式将从 CSSM 门户获取的授权代码粘贴到思科安全邮件和 Web 管理器中：

- 选择 **复制和粘贴授权代码 (Copy and Paste authorization code)** 选项，然后将授权代码粘贴到“复制和粘贴授权代码”选项下的文本框中。
- 选择**从系统中上传授权代码 (Upload authorization code from the system)** 选项，然后点击**选择文件 (Choose File)** 以上传授权代码。

步骤 6 点击**重新授权 (Re-authorize)**。

步骤 7 点击**复制代码 (Copy Code)** 以复制确认代码。

注释 您需要在 CSSM 门户中使用确认代码以更新许可证预留。

步骤 8 点击**确定 (OK)**。

步骤 9 在 CSSM 门户中添加从思科安全邮件和 Web 管理器获取的确认代码。

注释　有关如何添加确认代码的详细信息，请转至 智能软件许可在线帮助 (cisco.com)上帮助文档的 资产：产品实例选项卡 > 更新预留的许可证部分 。

许可证预留已更新。预留的许可证将变为“合规预留”状态。未预留的许可证将移至“未授权”状态。

注释　“未授权”状态表示思科安全邮件和 Web 管理器未预留任何功能许可证。

下一步做什么

- [适用于SLR和PLR]：如果需要，您可以删除许可证预留。有关详细信息，请参阅删除许可证预留，第 14 页。
- 您可以在思科安全邮件和 Web 管理器中禁用许可证预留。有关详细信息，请参阅禁用许可证预留，第 15 页。

删除许可证预留

您可删除您的思科安全邮件和 Web 管理器中启用的功能的特定或永久许可证预留。

注释　您还可以使用 CLI 中的 `license_smart` > `return_reservation` 子命令删除许可证预留。

步骤 1　前往思科安全邮件和 Web 管理器中的**系统管理 (System Administration)** > **智能软件许可 (Smart Software Licensing)** 页面。

步骤 2　从“操作”(Action) 下拉列表中选择**返回代码 (Return code)** 然后点击**转到 (GO)**。

步骤 3　点击**复制代码 (Copy Code)** 以复制返回代码。

注释　您需要在 CSSM 门户中使用返回代码以删除许可证预留。

注释　系统会向用户发送警报，指示智能代理已成功生成产品的退回代码。

步骤 4　点击**确定 (OK)**。

步骤 5　在 CSSM 门户中添加从思科安全邮件和 Web 管理器获取的返回代码。

注释　有关如何添加返回代码的详细信息，请转至 智能软件许可在线帮助 (cisco.com)上 资产： 产品实例选项卡 > 删除产品实例 上帮助文档的版块。

在您的思科安全邮件和 Web 管理器中预留的许可证将被删除并移至评估期。

禁用许可证预留

您可以在思科安全邮件和 Web 管理器中禁用许可证预留。

注释 您还可以在 CLI 中使用 `license_smart > disable_reservation` 子命令禁用许可证预留。

步骤 1 前往思科安全邮件和 Web 管理器中的**系统管理 (System Administration)** > **智能软件许可 (Smart Software Licensing)** 页面。

步骤 2 点击“注册模式”(Registration Mode) 字段下的**更改类型 (Change Type)**。

步骤 3 在“更改注册模式”(Change registration mode) 对话框中点击**提交 (Submit)**。

已在思科安全邮件和 Web 管理器上禁用许可证预留。

更新智能代理

要更新设备上安装的智能代理版本，请执行以下步骤：

步骤 1 依次选择**管理设备 > 系统管理 > 智能软件许可**。

步骤 2 在**智能代理更新状态 (Smart Agent Update Status)** 部分，点击**立即更新 (Update Now)**，按流程操作。

注释 如果您尝试使用 CLI 命令`saveconfig` 或使用**系统管理 (System Administration) > 配置摘要 (Configuration Summary)** 通过 Web 界面保存任何配置更改，则不会保存智能许可相关配置。

警报

发生以下场景时，您将收到通知：

- 成功启用智能软件许可
- 启用智能软件许可失败
- 评估期开始时
- 评估期到期时（评估期间的固定间隔以及到期时）
- 已成功注册
- 注册失败
- 成功获得授权
- 授权失败
- 成功取消注册

- 撤销注册失败
- 成功续订 ID 证书
- ID 证书续订失败
- 授权到期
- ID 证书到期
- 不合规宽限期到期（不合规宽限期间的固定间隔以及到期时）。
- 功能到期的第一个实例
- [仅适用于 SLR 和 PLR]：生成请求代码后安装授权代码。
- [仅适用于 SLR 和 PLR]：已成功安装授权码。
- [仅适用于 SLR 和 PLR]：已成功生成返回代码。
- [仅适用于 SLR]：特定功能许可证预留已到期。
- [仅适用于 SLR]：在预留的特定功能许可证到期之前发送警报的频率。

命令行界面

license_smart

描述

配置智能软件许可功能。

使用情况

提交：此命令需要“提交”。

批处理命令：此命令支持批处理格式。有关详细信息，请键入命令 `help license_smart` 来查阅在线帮助。

示例：为智能代理服务配置端口

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[]> setagentport

Enter the port to run smart agent service.
[65501]>
```

示例：启用智能许可

```
mail.example.com > license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
 []> enable
After enabling Smart Licensing on your appliance, follow below steps to activate
the feature keys (licenses):

a) Register the product with Smart Software Manager using license_smart > register command
 in the CLI.
b) Activate the feature keys using license_smart > requestsmart_license command in the CLI.

Note: If you are using a virtual appliance, and have not enabled any of the
features in the classic licensing mode; you will not be able to activate the
licenses, after you switch to the smart licensing mode. You need to first register
your appliance, and then you can activate the licenses (features) in the smart licensing
mode.
Commit your changes to enable the Smart Licensing mode on your appliance.
All the features enabled in the Classic Licensing mode will be available in the Evaluation
 period.
Type "Y" if you want to continue, or type "N" if you want to use the classic licensing mode
 [Y/N] []> y
```

```
> commit

Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
```

示例：向智能软件管理器注册设备

```
mail.example.com > license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> register
Reregister this product instance if it is already registered [N]> n

Enter token to register the product:
[]>
ODRlOTM5MjItOTQzOS00YjY0LWExZTUtZTdmMmY3OGNlNDZmLTE1MzM3Mzgw%0AMDEzNTR8WlpCQ1lMbGVMQWRx
OXhuenN4OWZDdktFckJLQzF5V3VIbzkyTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status of
 registration.
```

示例：智能许可状态

```
mail.example.com > license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode

Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

示例：智能许可状态摘要

```
mail.example.com > license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
```

```
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> summary

FeatureName                                    LicenseAuthorizationStatus
Mail Handling                                                  In Compliance
Content Security Management Master ISQ                         In Compliance
```

示例：设置智能传输 *URL*

```
mail.example.com > license_smart

Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> url

1. DIRECT - Product communicates directly with the cisco license servers
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software manager
 satellite.

Choose from the following menu options:
[1]> 1
Note: The appliance uses the Direct URL
(https://smartreceiver.cisco.com/licservice/license) to communicate with Cisco
Smart Software Manager (CSSM) via the proxy server configured using the updateconfig command.
Transport settings will be updated after commit.
```

示例：申请许可证

注释 虚拟设备用户必须注册其设备，才能申请或发放许可证。

```
mail.example.com > license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> requestsmart_license

Feature Name                                    License Authorization Status
1. Content Security Management Centralized Tracking     Not Requested
2. Content Security Management Master ISQ               Not requested

Enter the appropriate license number(s) for activation.
Separate multiple license with comma or enter range:
[]> 1
Activation is in progress for following features:
Security Management Centralized Tracking
Use license_smart > summary command to check status of licenses.
```

示例：发放许可证

```
mail.example.com > license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> releasesmart_license

Feature Name                                    License Authorization Status
1. Content Security Management Centralized      In Compliance
   Tracking
2. Content Security Management Master ISQ       In Compliance
```

示例 - 启用和注册许可证预留

在本例中，您可以使用 `license_smart > enable_reservation` 子命令在思科安全邮件和 Web 管理器上启用和注册许可证预留。

```
mail.example.com > license_smart

Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure
Email and Web Manager.
[]> enable_reservation

Would you like to reserve license, then type "Y" else type "N" [Y/N] []> yes


License Reservation is enabled for the following machines:
mail1.example.com

License Reservation is enabled

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
[]> request_code


The generation of the request code is initiated...

Copy the request code obtained on your Secure Email and Web Manager and paste it in the
Cisco Smart Software Manager portal to select the required license

Request code: CD-ZSMA:BD20B624E904-B7HCL9scQ-DD

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
```

```
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
- INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your Secure Email and Web Manager.
- CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Email and Web
Manager.
[]> install_authorization_code
1. Paste via CLI
2. Import the Authorization Code from a file

How would you like to install Authorization Code?
[1]>
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piid>7b654af6-9d60-46f5-a79-·····.PS/o+6</signature><udi>P:SMA,S:BE30B124E904
</udi></specificPLR>
^D
The SPECIFIC license reservation is successfully installed on your Secure Email and Web
Manager
Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Email and Web Manager.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web
Manager.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Email and Web Manager.
[]>
```

示例 - 更新许可证预留

在本示例中，您可以使用 `license_smart > reauthorize` 子命令为新功能保留许可证，或修改功能的现有许可证预留。

```
mail.example.com > license_smart

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Email and Web Manager.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web
Manager.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Email and Web Manager.
[]> reauthorize

1. Paste via CLI
2. Import the Authorization Code from a file
How would you like to install Authorization Code?
[1]>
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piid>6b684af8-4d20-42f5-ab89-·····..</authorizationCode><signature>
```

```
MEYCIDS7IZQuLvMMmiXMH2eZOwf7cy6rjgc7kxBIja</signature><udi>P:SMA,S:BD660B174E904
</udi></specificPLR>
^D

The SPECIFIC license reservation is successfully installed on your Secure Email and Web
Manager.

Copy the confirmation code obtained from Smart Agent and add it to the Cisco Smart Software
 Manager portal to update the specific reservation.

Confirmation code: 1f87b235

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Email and Web Manager.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web
Manager.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Email and Web Manager.
[]>
```

示例 - 删除许可证预留

在本示例中，您可以使用 `license_smart > return_reservation` 子命令删除您的思科安全邮件和 Web 管理器中启用的功能的特定或永久许可证预留。

```
mail.example.com > license_smart

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Email and Web Manager.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web
Manager.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Email and Web Manager.
[]> return_reservation

After you return the license reservation, you cannot use any of the product features, if
the evaluation period has exceeded 90 days. After the 90 days
evaluation period, you must register your product with Cisco Smart Software Manager to
continue to use the product features. [N]> yes

The generation of the return code is initiated...

Copy the return code obtained on your Secure Email and Web Manager and paste it in the Cisco
 Smart Software Manager portal.

Return Code: C97xKY-otSY8D-ertAf-v-fbEu5q-APo

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
```

```
[]>

mail1.example.com>
```

示例 - 禁用许可证预留

在本例中，您可以使用 `license_smart > disable_reservation` 子命令在思科安全邮件和 Web 管理器上禁用许可证预留。

```
mail.example.com > license_smart

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
- INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your Secure Email and Web Manager.
- CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Email and Web
Manager.
[]> disable_reservation


A request code for the specific or permanent reservation is generated on your Secure Email
 and Web Manager. If you want to disable the reservation, it cancels the request code.


Do you want to disable the specific or permanent reservation? [Y/N] []> yes

License Reservation is disabled for the following machines:
mail1.example.com

License Reservation is disabled

Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure
Email and Web Manager.
[]>
```

示例 - 手动启用设备主导转换过程

在本例中，您可以使用 `license_smart > conversion_start` 子命令在思科安全邮件和 Web 管理器上手动启用设备主导转换 (DLC) 进程。

```
mail.example.com > license_smart

Deregister Secure Email and Web Manager from the Cisco Smart Software Manager portal to
enable the license reservation

Choose the operation you want to perform:
- URL - Set the Smart Transport URL.
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- DEREGISTER - Deregister the product from Smart Licensing.
- REREGISTER - Reregister the product for Smart Licensing.
- RENEW_AUTH - Renew authorization of Smart Licenses in use.
```

```
- RENEW_ID - Renew registration with Smart Licensing.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- CONVERSION_START - To manually convert the classic license keys to smart Licensing
[]> conversion_start


Do you want to start the process of converting your classic license keys to smart software
 licensing[Y/N]? []> yes
```

showlicense_smart

描述

显示智能许可状态和状态摘要。

示例：智能许可状态

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode

Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

示例：智能许可状态摘要

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.

[]> summary

FeatureName                          LicenseAuthorizationStatus
Mail Handling                                        In Compliance
Content Security Management Master ISQ               In Compliance
```

cloudserviceconfig

描述

cloudserviceconfig 命令用于：

- 此命令仅适用于智能许可模式。
- 在设备上启用思科云服务门户。
- 在设备上禁用思科云服务门户。
- 向思科云服务门户注册您的思科安全邮件和 Web 管理器。
- 使用思科云服务门户自动注册思科安全邮件和 Web 管理器。
- 从思科云服务门户取消注册您的思科安全邮件和 Web 管理器。
- 选择思科安全云服务器，以便将设备连接到思科云服务门户。
- 从更新程序使用的 Talos 服务器获取证书和密钥。
- 在思科安全邮件和 Web 管理器上启用思科 SecureX（或思科威胁响应） 。您必须使用常规配置设置执行此操作。
- 在思科安全邮件和 Web 管理器上禁用思科 SecureX 或思科威胁响应 。您必须使用常规配置设置执行此操作。

使用情况

- **提交**：此命令不需要“提交”。
- **批处理命令**：此命令支持批处理格式。

示例：在设备上启用思科云服务

在以下示例中，您可以使用 cloudserviceconfig > enable 子命令在邮件网关上启用思科云服务。

注释 只有在未启用智能软件许可并且您的设备未向思科智能软件管理器注册时才能使用此子命令

```
mail1.example.com > cloudserviceconfig
Choose the operation you want to perform:
- ENABLE - The Cisco Cloud Service is currently disabled on your appliance.
[]> enable
The Cisco Cloud Service is currently enabled on your appliance.
Currently configured Cisco Secure Cloud Server is: api.apj.sse.itd.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 1
Selected Cisco Secure Cloud Server is api-sse.cisco.com.
Make sure you run "commit" to make these changes active.
mail1.example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:23:19 2020 GMT
mail1.example.com >
```

示例：在设备上禁用思科云服务

在以下示例中，您可以使用 cloudserviceconfig > disable 子命令在设备上禁用思科云服务。

```
mail1.example.com> cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> disable
The Cisco Cloud Service is currently disabled on your appliance.
mail1.example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:01:07 2020 GMT
mail1.example.com >
```

示例：向思科云服务门户注册内容安全网关

```
sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
The appliance is not registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is stage-api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[]> REGISTER
```

```
Enter a registration token key to register your appliance with the Cisco Cloud Service
portal.
[]> 90a92909fc3b1be666f180621146fea3

The appliance registration is in progress.
```

示例：从思科云服务门户取消注册内容安全网关

在以下示例中，您可以使用 cloudserviceconfig > deregister 子命令从思科云服务门户取消注册设备。

```
sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
The Content Security Management appliance is successfully registered with the Cisco Cloud
Service portal.
Currently used Cisco Cloud Server is stage-api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[]> DEREGISTER

Do you want to deregister your appliance from the Cisco Cloud Service portal.
If you deregister, you will not be able to access the Cloud Service features. [N]> Y

The Content Security Management appliance deregistration is in progress.
```

示例：选择思科安全云服务器，以便将内容安全网关连接至思科云服务门户

在以下示例中，您可以使用 **cloudserviceconfig > settrs** 子命令来选择所需的思科安全云服务器，以便将您的邮件网关连接到思科云服务门户。

```
mail1.example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> settrs
Currently configured Cisco Secure Cloud Server is: api-sse.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 3
Selected Cisco Secure Cloud Server is api.eu.sse.itd.cisco.com.
Make sure you run "commit" to make these changes active.
mail1.example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:37:40 2020 GMT
```

使用 *CLI* 执行自动注册以进行智能许可的示例

在以下示例中，您可以使用命令在智能许可中注册一次后进行显示，设备会在在后端执行自动注册。如果自动注册失败，您可以在 CLI 中看到用于自动注册的命令。

```
Autoregister Success/ and failure
sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
The appliance is not registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically.
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[]> AUTOREGISTER

The appliance failed to auto-register with the Cisco Cloud Service portal.
Reason: A request to generate a Smart Licensing payload from Cisco Smart Software Manager
failed.
The appliance is not registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically.
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[]> AUTOREGISTER

The appliance successfully auto-registered with the Cisco Cloud Service portal.
```

下载证书和密钥的示例

在以下示例中，您可以使用命令从 TALOS 服务器获取更新程序所使用的证书和密钥。

```
sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
The Content Security Management appliance is successfully registered with the Cisco Cloud
Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com


Choose the operation you want to perform:
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- FETCHCERTIFICATE - Download the Cisco Talos certificate and key
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[]> FETCHCERTIFICATE

Current Cisco Talos certificate is valid for 172 days

Do you like to overwrite the existing certificate and key [Y|N] ? []> N

The Content Security Management appliance is successfully registered with the Cisco Cloud
Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com
```

示例客户端证书 *cloudserviceconfig*

在以下示例中，您可以使用命令来自上传证书和密钥。

```
[]> clientcertificate

Do you like to overwrite the existing certificate and key [Y|N] ? []> Y

Paste the certificate.
Press CTRL-D on a blank line when done.
-----BEGIN CERTIFICATE-----
AQEFAAOCAQ8AMIIBCgKCAQEAyf9pD6jCYmA2YUmzjs711J80V2Ehil8FnvDo8ElJ
cVPlrZFwzTmI5wHTrQi0YkjaYsbe9Nbh9q5vdmrL58Pmiky7HOhOYFXcHi95U1Sa
rY6DhYNw8isKxFuG0Xnm1mNzSSIQdIcTvqIV/iPUjQl8Omwl/p1ErDl5J7MY5kNL
MpES7AmQitef0BRmcDmpammCCVmUx2b1A7PmepclCVs2PfaoqIGy26CcAonFOlrJ
MIIDYzCCAkugAwIBAgIDCMvdMA0GCSqGSIb3DQEBCwUAMIGCMQswCQYDVQQGEwJV
GlyOpFkbHg8ALkdKiD4RHXkUSKdadFDKIAIgc/9g9adrUwIDAQABoxowGDAJBgNV
UzETMBEGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxGzAZBgNV
BAoTEkNpc2NvIFN5c3RlbXMgSW5jLjERMA8GA1UECxMIU2VjdXJpdHkxGzAZBgNV
BAMTElN0YWdlIEtleW1hc3RlciBDQTAeFw0xOTAyMTkwMzU3MzhaFw0yMjA0MDIw
2jgYEzrhGtZmx+hpAmHi1i8cnIarD5oePtcggOafxpa/32rqXPGfjiaJU6cdA6Su
Qguqh7/bn6u8R9EMjzu4V+Rn54JZMTcJ9v/u5OC1kKohsMFMwBQ0EpPL5CpM8NDx
SjGPIMP2SrqktLORlTqtvcx8SnMurrxe61PnrUs93z1nRSXhcHGlyrQs6HIqIvMT
MzU3MzhaMEkxHTAbBgkqhkiG9w0BCQEWDnRlc3RAY2lzY28uY29tMRgwFgYDVQQD
DA9WTE5TTUExMjM0NTY3ODkxDjAMBgNVBAoMBWNpc2NvMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAyf9pD6jCYmA2YUmzjs711J80V2Ehil8FnvDo8ElJ
cVPlrZFwzTmI5wHTrQi0YkjaYsbe9Nbh9q5vdmrL58Pmiky7HOhOYFXcHi95U1Sa
rY6DhYNw8isKxFuG0Xnm1mNzSSIQdIcTvqIV/iPUjQl8Omwl/p1ErDl5J7MY5kNL
MpES7AmQitef0BRmcDmpammCCVmUx2b1A7PmepclCVs2PfaoqIGy26CcAonFOlrJ
uT6K+qrTusUEP41oDC7IrpnbBE697xzbtF8l7xgxUosxP+OuXcgtTX1TXcY516jS
GlyOpFkbHg8ALkdKiD4RHXkUSKdadFDKIAIgc/9g9adrUwIDAQABoxowGDAJBgNV
HRMEAjAAMAsGA1UdDwQEAwIHgDANBgkqhkiG9w0BAQsFAAOCAQEAOKYfiZfJg4rM
IWM73wz8u7Wtj97E6rGVgsj0D54fOKF6DmqHfyqPCuXns0Fl8nL1Da3ogslLwIrS
d5a1lfj/2r6NfbN0hjKN7/5PGBtcRyMDi86aUBoqahNmgCwDKTTJgoVTO0//a+Ca
2jgYEzrhGtZmx+hpAmHi1i8cnIarD5oePtcggOafxpa/32rqXPGfjiaJU6cdA6Su
Qguqh7/bn6u8R9EMjzu4V+Rn54JZMTcJ9v/u5OC1kKohsMFMwBQ0EpPL5CpM8NDx
SjGPIMP2SrqktLORlTqtvcx8SnMurrxe61PnrUs93z1nRSXhcHGlyrQs6HIqIvMT
J1SwgurFWg==
-----END CERTIFICATE-----
^D

Paste Private Key.
Press CTRL-D on a blank line when done.
-----BEGIN RSA PRIVATE KEY-----
ZzSWnNAdMjtobo6dx1iMfbaWDd1Um+PIEiBXEy5z74btukQUGTI0DXsCgYEA36q3
gH/+2ybheB8iCYQfZnZkeUM4qqN3HkRmrhTB9OlPLkZ0B0fstPfpEcw/v/lz3BRQ
Dyk5VlgEtnOpWbyYKqlZbFPHbddQGTIbCV4T1hyEcjNbyD2SSCIv5gxF70TBR5qD
14HT3PPt4HXpgcFw70NofNSnpNm63OhkW4SBNgkCgYEAs8Y4VMWA2WWEAFZhIZKS
4Jw8/yWYe4V746aWRVN7wL99aRK6eVTk7kCEZLG7+vqzboSORPi98QXY1o/aBNhg
MIIEowIBAAKCAQEAyf9pD6jCYmA2YUmzjs711J80V2Ehil8FnvDo8ElJcVPlrZFw
NEnrtal7WnKNZz96nC1kaqh8DBaGuoMPTbEGrEjnavfm7JDY/vlLxTUE2SMRd2ZX
zTmI5wHTrQi0YkjaYsbe9Nbh9q5vdmrL58Pmiky7HOhOYFXcHi95U1SarY6DhYNw
BHXHikhkl+8ibEB2K+XlQUPSCy7aGmbekc8y0vJBVObdKx+/uIwuk1buy4rUybMy
f3DsaHI6Yj7jYi4aI1ec7HT0X60vxc4eahBv8DvaIF3Ak0LyIvdLomycVkG58siV
Lt+psQKBgFjRVfNddwgcX5QaQXopYJWa/HFnWgH7jXgVFeR1Q9smq7L0Yk39GrxT
8isKxFuG0Xnm1mNzSSIQdIcTvqIV/iPUjQl8Omwl/p1ErDl5J7MY5kNLMpES7AmQ
itef0BRmcDmpammCCVmUx2b1A7PmepclCVs2PfaoqIGy26CcAonFOlrJuT6K+qrT
usUEP41oDC7IrpnbBE697xzbtF8l7xgxUosxP+OuXcgtTX1TXcY516jSGlyOpFkb
Hg8ALkdKiD4RHXkUSKdadFDKIAIgc/9g9adrUwIDAQABAoIBAE+jQNqJoEmEwSvO
ENqmwcjYE5y3kK+rEt49ALlrS2dAunaZtq1Sl6Tr1XaMzgFJ07/JxDEnXuMQlqVL
KaTwWT4BTmvxMqVMdIH6GY0+99ShMT08OxVe3tnXc+m2c8nmX5dftLkcYC5yXNVb
bvtD2BR4eupNOrvj1N5P/+sYcNc4I7ZAAheGfhLc4oDTMiHIE5g6Dyvh7j+WIi9y
bpoU99fFV7jcGtql5AOUQtLUtuO6d1tk2WL1+m2qsX7uMkQ5ddM9vGbTRg0IkjRb
PVpshAK5j/RsQCUN6LlRq+SY7y18CllZ4MYWXu754KqMloK8UDarI+dKISyVskfe
```

```
69lNQ2ECgYEA5zLHTykFOA349MyliSQxIE6YsVL8tc1Ryf/PB69OoTY+vKUcmCZp
TzLPuEEbyzndAIW7FagVG5aYYFXD0kcUE9LUCCTl5bTOiYJM0YCGgsHnBpqUI7yI
ZzSWnNAdMjtobo6dx1iMfbaWDd1Um+PIEiBXEy5z74btukQUGTI0DXsCgYEA36q3
gH/+2ybheB8iCYQfZnZkeUM4qqN3HkRmrhTB9OlPLkZ0B0fstPfpEcw/v/lz3BRQ
Dyk5VlgEtnOpWbyYKqlZbFPHbddQGTIbCV4T1hyEcjNbyD2SSCIv5gxF70TBR5qD
14HT3PPt4HXpgcFw70NofNSnpNm63OhkW4SBNgkCgYEAs8Y4VMWA2WWEAFZhIZKS
4Jw8/yWYe4V746aWRVN7wL99aRK6eVTk7kCEZLG7+vqzboSORPi98QXY1o/aBNhg
NEnrtal7WnKNZz96nC1kaqh8DBaGuoMPTbEGrEjnavfm7JDY/vlLxTUE2SMRd2ZX
XEDpdHDalZZFpGDrf+wZraECgYB3cT1pe/Dnq43Aji+pEUuLdjIVp9Y9Gepk2XZU
BHXHikhkl+8ibEB2K+XlQUPSCy7aGmbekc8y0vJBVObdKx+/uIwuk1buy4rUybMy
f3DsaHI6Yj7jYi4aI1ec7HT0X60vxc4eahBv8DvaIF3Ak0LyIvdLomycVkG58siV
Lt+psQKBgFjRVfNddwgcX5QaQXopYJWa/HFnWgH7jXgVFeR1Q9smq7L0Yk39GrxT
Gu2acBalPQR474nW9394XqmPTJ5tYhf80nmT7JRwYEgE2C/flnDDea9YFoiX/yP3
fD4kLyDPgQ8utQwK7X7aK1PxdEIsXKZLcR6FoeT0wQj31gCG2igH
-----END RSA PRIVATE KEY-----
^DCertificate and key are stored successfully
```

示例：在 内容安全网关 上启用思科 *SecureX* 或思科威胁响应

在以下示例中，您可以使用 `cloudericeconfig > enableecurecx` 子命令在设备上启用思科 SecureX 或思科威胁响应 。

```
Choose the operation you want to perform:
- IEOVERRIDE - Configure Internet Explorer Compatibility Mode Override
- SecureX  - Configure Cisco SecureX / Threat Response   feature on your appliance
[]> SecureX

The Cisco SecureX / Threat Response  feature is currently disabled on your appliance.
Would you like to enable Cisco SecureX / Threat Response  feature [Y]>

Cloud Service is not enabled.
        Enter "cloudserviceconfig" for enabling Cisco Cloud service.
```

示例：在 内容安全网关 上禁用思科 *SecureX* 或思科威胁响应

在以下示例中，您可以使用 `cloudericeconfig > disableecurecx` 子命令在设备上启用思科 SecureX 或思科威胁响应 。

```
sma> generalconfig


Choose the operation you want to perform:
- IEOVERRIDE - Configure Internet Explorer Compatibility Mode Override
- SecureX - Configure Cisco SecureX / Threat Response  feature on your appliance
[]> SecureX

The Cisco SecureX / Threat Response feature is currently enabled on your appliance.
Would you like to disable Cisco SecureX / Threat Response feature [N]> Y

The Cisco SecureX / Threat Response feature is currently disabled on your appliance.
The Cisco Cloud Service is currently disabled on your appliance.
```

updateconfig

描述

配置系统更新参数。

使用情况

提交：此命令需要“提交”。

批处理命令：此命令不支持批处理格式。

注释 CLIENTCERTIFICATE 和 VLNID 子命令不需要“提交”。

注释 VLNID 子命令仅适用于 SLR 或 PLR 注册虚拟设备（即在气隙模式下运行的 SLR 或 PLR 注册设备）。

示例：在安全邮件和 *Web* 管理器中上传 *Cisco Talos* 证书和密钥详细信息

```
mail.example.com> updateconfig
Service (images):                   Update URL:
-------------------------------------------------------------------------------
Feature Key updates                 http://downloads.ironport.com/asyncos
Timezone rules                      Cisco Servers
Support Request updates             Cisco Servers
Smart License Agent Updates         Cisco Servers
Notifications component Updates     Cisco Servers
Cisco AsyncOS upgrades              Cisco Servers

Service (list):                                     Update URL:
-------------------------------------------------------------------------------
Timezone rules                        Cisco Servers
Support Request updates               Cisco Servers
Smart License Agent Updates           Cisco Servers
Notifications component Updates       Cisco Servers
Cisco AsyncOS upgrades                Cisco Servers

Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
- CLIENTCERTIFICATE - Upload the client certificate and key.
- VLNID - Update the VLN ID.
[]> CLIENTCERTIFICATE

Paste the certificate.
Press CTRL-D on a blank line when done.

-----BEGIN CERTIFICATE-----
MIIDXjCCAkagAwIBAgIEAm+eGTANBgkqhkiG9w0BAQsFADB+MQswCQYDVQQGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcm5pYTERMA8GA1UEBwwIU2FuIEpvc2UxGzAZBgNV
BAoMEkNpc2NvIFN5c3RlbXMgSW5jLjERMA8GA1UECwwIU2VjdXJpdHkxFzAVBgNV
.........
G0NYIhd82O9NIP9WQeVJmPfTd4O2EFZZQb6Mq+EvkCYajTWInUfxQLIfy3HUEDGJ
ZKY=
```

```
-----END CERTIFICATE-----
^D

Paste Private Key.
Press CTRL-D on a blank line when done.
Key         :

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAttALQE31Pd+xoLaO8kpzjHBuoJVRsZnNbt400PRES8vXSsYS
bxU720rK9xPTdYQ1V9bJUlPvYHlgIE90xPcWfnptUsARFTrvnsMGydI3J+5vD9gN
5Y9LjW1rmNUwdF98022hEzJpZ35nUT6EePd8uOlw7MmMopSF4ySrG5imseMr6fBI
.............
VBgX7nSeTCXsSZdpvTi7RIk+jCEYqeZVGWJ4tZF6yZWIOaTTCFw=
-----END RSA PRIVATE KEY-----
 ^D
Certificate and key are stored successfully
```

示例：配置安全邮件和 *Web* 管理器以添加或更新 *VLNID*

```
mail.example.com> updateconfig
Service (images):                   Update URL:
-------------------------------------------------------------------------------
Feature Key updates                 http://downloads.ironport.com/asyncos
Timezone rules                      Cisco Servers
Support Request updates             Cisco Servers
Smart License Agent Updates         Cisco Servers
Notifications component Updates     Cisco Servers
Cisco AsyncOS upgrades              Cisco Servers

Service (list):                                     Update URL:
-------------------------------------------------------------------------------
Timezone rules                        Cisco Servers
Support Request updates               Cisco Servers
Smart License Agent Updates           Cisco Servers
Notifications component Updates       Cisco Servers
Cisco AsyncOS upgrades                Cisco Servers

Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
- CLIENTCERTIFICATE - Upload the client certificate and key.
- VLNID - Update the VLN ID.

[]> VLNID

VLN : VLNESA1838283016
Do you like to overwrite the existing VLN[Y|N] ? []> n
```

vlninfo

描述

显示虚拟许可证编号 (VLN) 以及 Cisco Talos 证书和密钥详细信息。

使用情况

提交：此命令不需要“提交”。

批处理命令：此命令不支持批处理格式。

注释 `vLNinfo` 命令仅适用于注册智能软件许可以及注册 SLR 或 PLR 的虚拟设备。

示例：显示 *VLN* 和 *Cisco Talos* 证书和密钥详细信息

```
mail.example.com> vlninfo

VLN and Certificate details

VLN         : VLNSMA1838285196

Certificate :

-----BEGIN CERTIFICATE-----
MIIDXjCCAkagAwIBAgIEAm+eGTANBgkqhkiG9w0BAQsFADB+MQswCQYDVQQGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcm5pYTERMA8GA1UEBwwIU2FuIEpvc2UxGzAZBgNV
BAoMEkNpc2NvIFN5c3RlbXMgSW5jLjERMA8GA1UECwwIU2VjdXJpdHkxFzAVBgNV
.........
G0NYIhd82O9NIP9WQeVJmPfTd4O2EFZZQb6Mq+EvkCYajTWInUfxQLIfy3HUEDGJ
ZKY=
-----END CERTIFICATE-----

Key         :

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAttALQE31Pd+xoLaO8kpzjHBuoJVRsZnNbt400PRES8vXSsYS
bxU720rK9xPTdYQ1V9bJUlPvYHlgIE90xPcWfnptUsARFTrvnsMGydI3J+5vD9gN
5Y9LjW1rmNUwdF98022hEzJpZ35nUT6EePd8uOlw7MmMopSF4ySrG5imseMr6fBI
.............
VBgX7nSeTCXsSZdpvTi7RIk+jCEYqeZVGWJ4tZF6yZWIOaTTCFw=
-----END RSA PRIVATE KEY-----
```

帮助 vLNinfo

描述

显示 VLN 详细信息。它为 `vlninfo` 命令提供帮助支持。

使用情况

提交：此命令不需要“提交”。

批处理命令：此命令不支持批处理格式。

注释 `help vIninfo` 命令仅适用于注册智能软件许可以及注册 SLR 或 PLR 的虚拟设备。

示例：显示 *VLN* 详细信息

```
mail.example.com> help vlninfo

Show VLN details
```

AsyncOS 14.0 的智能软件许可要点

- 启用云服务时，思科 SecureX 将被自动启用；而禁用云服务时，思科 SecureX 将被禁用。
- 思科 SecureX 和思科威胁响应选项现已在 Web UI 中更改，您可以从 **系统管理 > 常规设置**启用或禁用思科 SecureX 和思科威胁响应。您也可以使用 **generalconfig** 命令从 CLI 执行相同的操作。
- 在启用和注册智能软件许可时，将启用云服务并自动注册设备 （安全服务交换） 。
- 在传统模式下，云服务将默认处于禁用状态。您需要手动启用它，然后就会启用思科 SecureX 和思科威胁响应。您必须启用智能许可模式才能进行自动注册。
- 启用智能软件许可后，智能代理将会启动，并会在注册完成后启用云服务。
- 如果智能许可证处于评估模式，您就无法执行 安全服务交换 自动注册。

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“系统管理”(System Administration) 菜单中的“关机/重启”(Shutdown/Reboot) 页面，或使用 GLI 中的 reboot 命令。

重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。
`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。

Caution 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。

要想	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口令连接到设备（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。 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)**。 **Note** 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。 **Caution** 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 CLI 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.
```

Diagnostic - Reload 子命令

`Diagnostic - Reload` 子命令可将配置重置为制造商的初始值。该子命令将删除所有用户设置并重置整个设备。

如果安全邮件和 Web 管理器是虚拟设备，则 `Diagnostic - Reload` 子命令将删除所有功能密钥，您必须重新加载许可证。

注释 如果您远程连接到系统，则可能会丢失与设备的连接。

```
mail3.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.
[]> reload
This command will remove all user settings and reset the entire device.

If this is a Virtual Appliance, all feature keys will be removed, and the license must be
reapplied. This resets network configuration to factory defaults. You might lose connection
 to the device if you are connected remotely.
Are you sure you want to continue? [N]> Y
Are you *really* sure you want to continue? [N]> Y
Do you want to wipe also? Warning: This action is recommended if the device is being sanitized
 before sending it for RMA. Sometimes, it may take several minutes to complete the process
 because it follows the NIST Purge standard.
Do you want to continue? [N]
```

Diagnostic - Reload Status 命令

`Diagnostic - Reload_Status` 子命令会显示上一个 `Diagnostic - Reload` 命令的执行状态。

```
mail3.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.
[]> reload_status

Last Reload Status        Last Updated
Successful                09 Feb 2023 09:12 (GMT)
```

显示 AsyncOS 的版本信息

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

步骤 2 依次选择**管理设备 > 集中服务 > 系统状态**。

步骤 3 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。

Before you begin

- 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 使用具有“管理员 (Administrator)”访问权限的账户登录。

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口令。

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。

What to do next

远程重置设备电源

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。
- 必须对口令身份验证和 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
- Web 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 , on page 47。

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。
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托管设备提取数据 , on page 44。 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 , on page 87。 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

Note 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托管设备提取数据

步骤 1 访问目标设备的命令行界面。有关说明，请参阅访问命令行界面。

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, on page 65。

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。

Note 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。

Before you begin

- 满足备份的限制和要求 , on page 42所列的各项限制和要求。
- 在开始备份过程之前，请确保在目标设备上临时禁用双因素身份验证。备份过程完成后，可以在该目标设备上启用双因素身份验证。

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口令。

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 , on page 47。

开始即时备份

Note 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。

Before you begin

满足备份的限制和要求 , on page 42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口令。

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 , on page 47。

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 , on page 67。

What to do next

相关主题

日志文件中的备份信息 , on page 47

日志文件中的备份信息

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。

相关主题

- 检查备份状态 , on page 46

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 , on page 79。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，请参阅日志订用。

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。

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。

Before you begin

回顾备份安全管理设备数据 , on page 42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 , on page 79。

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 , on page 42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, on page 46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) [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。
b) 依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 安全设备 (Security Appliances)**。
c) 点击设备名称。
d) 点击**建立连接 (Establish Connection)** 按钮。
e) 点击**测试连接 (Test Connection)**。
f) 返回到设备列表。
g) 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：

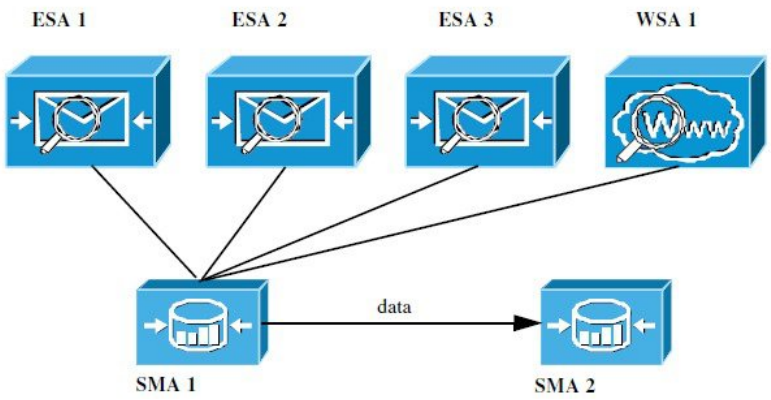
依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**，并检查数据传输状态。

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 , on page 42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：

Figure 1: 灾难恢复：典型环境



在此环境中，SMA 1 是从 ESA 1-3 及 WSA 1 接收数据的主安全管理设备。SMA 2 是从 SMA1 接收备份数据的备份安全管理设备。

如果出现故障，必须将 SMA 2 配置为您的主安全管理设备。

要将 SMA 2 配置为新的主安全管理设备并恢复服务，请执行以下操作：

Procedure

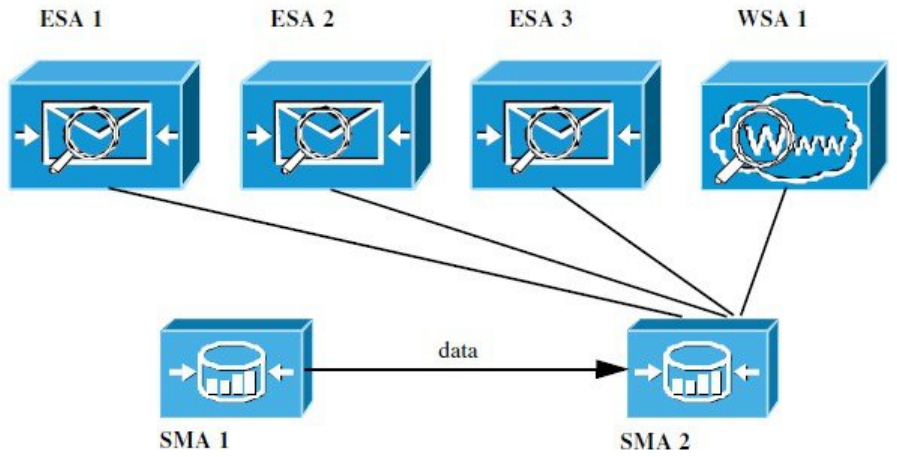
	Command or Action	Purpose
步骤 1	如果使用集中式策略、病毒和病毒爆发隔离区： • 在每个邮件安全设备上，禁用集中式隔离区。	有关禁用集中式策略、病毒和病毒爆发隔离区的说明，请参阅邮件安全设备文档。 这样将在每台邮件安全设备上创建本地隔离区，稍后可以将它们迁移到新的安全管理设备。
步骤 2	将您在主安全管理设备 (SMA1) 中保存的配置文件加载到备份安全管理设备 (SMA2)。	请参阅加载配置文件, on page 81。
步骤 3	将出现故障的 SMA 1 的 IP 地址重新创建为 SMA 2 上的 IP 地址	**a.** 在 SMA 2 上依次选择**网络 (Network) > IP 接口 (IP Interfaces) > 添加 IP 接口 (Add IP Interfaces)**。 **b.** 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。
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。
步骤 6	将所有设备添加到新的安全管理设备 (SMA 2)。 • 通过建立到设备的连接并测试连接，测试查看每台设备是否已启用并可运行。	请参阅关于添加托管设备。

	Command or Action	Purpose
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。
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 , on page 47。

What to do next

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：

Figure 2: 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 , on page 47。

升级 AsyncOS

- 升级的批处理命令 , on page 51
- 确定升级和更新的网络要求 , on page 51
- 选择升级方法：远程或流传输 , on page 51
- 配置升级和服务更新设置, on page 53
- 升级之前：重要步骤 , on page 58
- 升级 AsyncOS, on page 50
- 查看后台下载状态、取消或删除后台下载 , on page 60
- 升级后的注意事项 , on page 61

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。

Note 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”）。

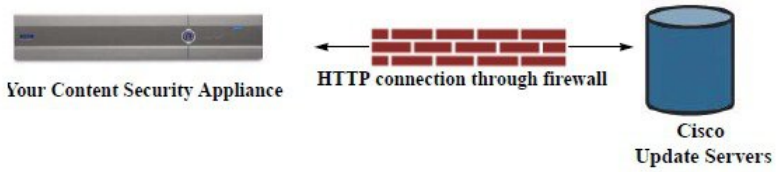
- 流传输升级 - 每台设备通过 HTTP 直接从思科内容安全更新服务器下载 AsyncOS 升级。
- 远程升级 - 您只从思科下载升级映像一次，然后将其提供给您的各台设备。然后设备从您的网络内的一台服务器下载 AsyncOS 升级。

您将在配置升级和服务更新设置, on page 53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：

Figure 3: 数据流更新方法



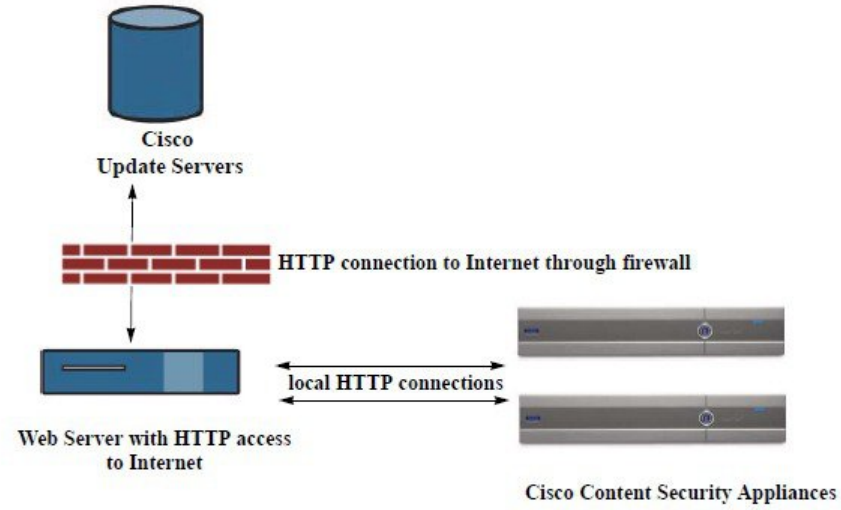
此方法要求设备直接从网络与思科内容安全更新服务器联系。

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。

Figure 4: 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, on page 52和托管远程升级映像, on page 53中的信息。

步骤 2 配置本地服务器，以检索和提供升级文件。

步骤 3 下载升级文件。

步骤 4 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 5 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 6 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 系统升级 (System Upgrade)**

步骤 7 点击**可用升级 (Available Upgrades)**。

Note 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, on page 50。

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。

Note 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：
  - 支持目录或文件名显示超出 24 个字符
  - 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”(Edit Update Settings) 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”(Edit Update Settings) 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））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。

Table 1: 更新安全服务的设置

设置	说明
更新服务器（图像）	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 , on page 55。 • 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。如果服务器需要身份验证，则也可以输入有效用户名和口令。 有关详细信息，请参阅选择升级方法：远程或流传输 , on page 51和远程升级概述, on page 51。
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 , on page 55。 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。如果服务器需要身份验证，则也可以输入有效用户名和口令。 有关详细信息，请参阅选择升级方法：远程或流传输 , on page 51和远程升级概述, on page 51。
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口令。 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（Web 报告）或文件分析报告详细信息的要求（邮件报告）。

设置	说明
HTTPS 代理服务器	如果存在上游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口令。 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（Web 报告）或文件分析报告详细信息的要求（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：

Figure 5: 更新服务器（映像）设置的静态 ***URL***

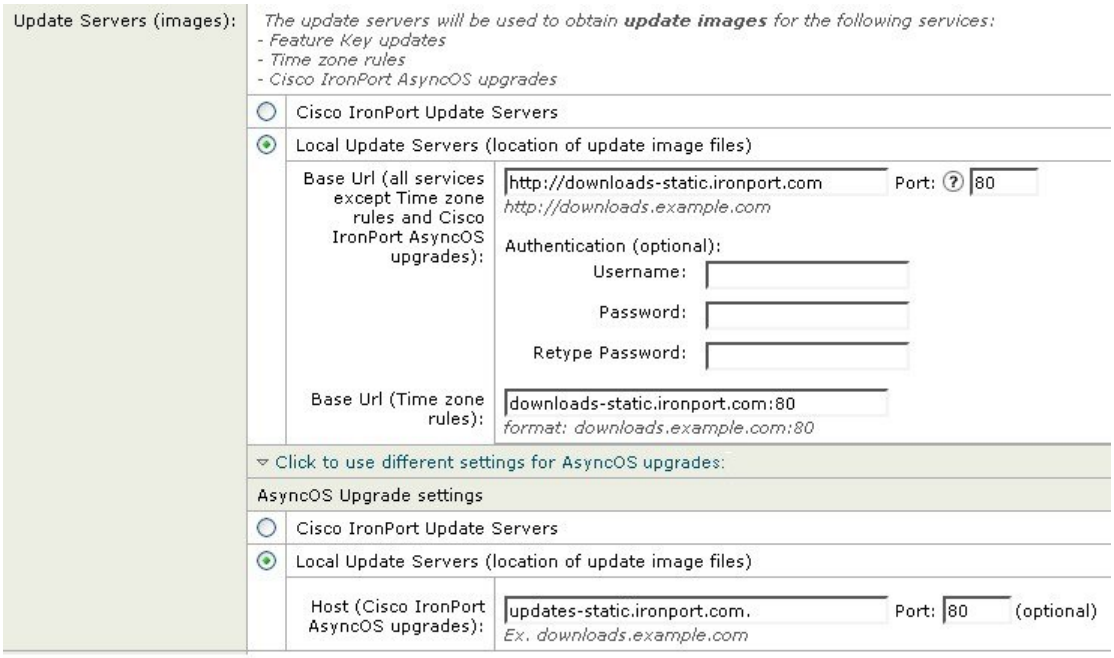


Figure 6: 更新服务器（列表）设置的静态 ***URL***

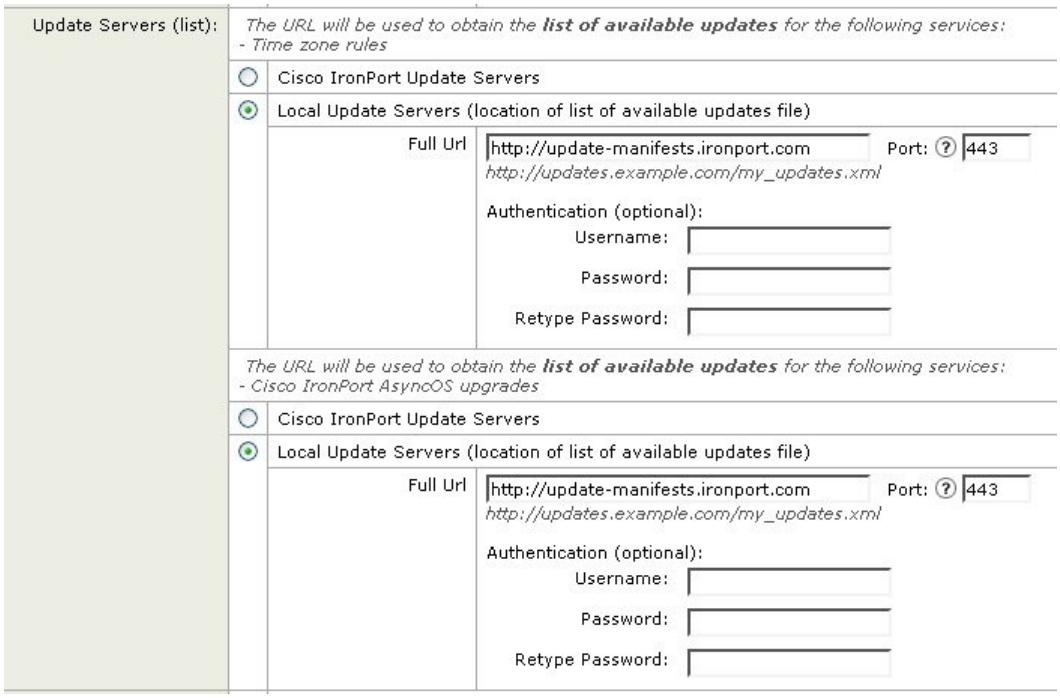


Table 2: 采用严格防火墙策略的环境的静态地址

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

部分	设置	静态 URL/IP 地址和端口
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

Important 您必须在 CLI 中使用`updateconfig`命令的`dynamichost` sub 命令配置更新清单url 和端口号。这将验证服务更新。

从 GUI 配置更新和升级设置

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

步骤 2 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 更新设置 (Update Settings)**。

步骤 3 点击**编辑更新设置 (Edit Update Settings)**。

按照升级和更新设置, on page 54中的说明配置此操作程序中的设置。

步骤 4 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 5 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 6 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 7 指定时区规则和接口的设置。

步骤 8 （可选）指定代理服务器的设置。

步骤 9 提交并确认更改。

步骤 10 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。

要想	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)**。
预防将来的通知（仅限具有“管理员 (Administrator)”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

Before you begin

请参阅确定升级和更新的网络要求 , on page 51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, on page 88。
- 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, on page 80参阅相关警告。

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, on page 53。

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。

Note 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。升级开始时，标语将显示 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。

Before you begin

- 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 , on page 51和配置升级和服务更新设置, on page 53。
- 在安装升级之前，按照升级之前：重要步骤 , on page 58中的说明执行操作。

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

步骤 2 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **系统升级 (System Upgrade)**。

步骤 3 点击**升级选项 (Upgrade Options)**。

步骤 4 选择一个选项：

要想	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 5 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 6 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口令。

Note 无法使用 GUI 中的“配置文件”(Configuration File) 页面或 CLI 中的 `loadconfig` 命令加载带屏蔽口令的配置文件。

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 7 点击**继续 (Proceed)**。

步骤 8 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)**。

Note 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。

What to do next

- 如果流程中断，必须重新开始该流程。
- 如果已下载但未安装升级：

  在准备安装升级时，请从开始按照这些说明执行操作，包括“准备工作 (Before You Begin)”部分的前提条件，但请选择“安装 (Install)”选项。
- 如果您已安装升级，请参阅升级后的注意事项 , on page 61。

查看后台下载状态、取消或删除后台下载

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

步骤 2 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 系统升级 (System Upgrade)**。

步骤 3 点击**升级选项 (Upgrade Options)**。

步骤 4 选择一个选项：

要想	相应操作
查看下载状态	查看页面的中间。 如果没有正在进行的下载，且无完成的下载等待安装，则不会看到下载状态信息。 升级状态也会出现在升级日志中。

要想	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。请参阅使用主配置以集中管理网络安全设备。
- 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 , on page 79。
- 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, on page 61
- 恢复 AsyncOS , on page 62

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

Before you begin

- 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（不屏蔽口令）。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。

Note 这不是您在恢复之后要下载的配置文件。

步骤 3 如果使用“安全列表/阻止列表 (Safelist/Blocklist)”功能，请将“安全列表/阻止列表 (Safelist/Blocklist)”数据库导出到其他计算机。

步骤 4 暂停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：

Example:

```
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 passphrases
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，以允许从此设备下载任何“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。

Note 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 53 页

相关主题

- 配置升级和服务更新设置，第 53 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
- URL 类别集更新和报告

将设备配置为信任代理服务器通信

如果使用非透明代理服务器，则可以添加 CA 证书用于为邮件网关的代理证书签名。这样，邮件网关将会信任代理服务器通信。

当思科安全邮件和 Web 管理器与更新程序服务器通信以接收更新时，会对所使用的证书是否可信进行验证。要成功验证所使用的证书，您必须将该更新程序服务器的证书颁发机构证书包含在我们的思科安全邮件和 Web 管理器中，然后才能成功进行通信。要执行此操作，请使用 **updateconfig** > **trusted_certificates**。命令中的选项包括：

- Add- 在 CA 中添加证书
- List- 列出 CA 中的所有证书
- Delete- 删除 CA 中的证书

使用 updateconfig 命令配置此选项。以下示例显示了如何配置此选项。

```
SMA> updateconfig

Service (images): Update URL:
-------------------------------------------------------------------------------
Feature Key updates http://downloads.ironport.com/asyncos
Timezone rules Cisco Servers
Support Request updates Cisco Servers
Smart License Agent Updates Cisco Servers
Notifications component Updates Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Service (list): Update URL:
-------------------------------------------------------------------------------
Timezone rules Cisco Servers
Support Request updates Cisco Servers
Smart License Agent Updates Cisco Servers
Notifications component Updates Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Update interval: 5m

Proxy server: not enabled

HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> trusted_certificates


Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]> add

Paste certificates to be trusted for secure updater connections, blank to quit
Trusted Certificate for Updater:
paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDxTCCAq2gAwIBAgIIOUMAFHhzRskwDQYJKoZIhvcNAQELBQAwczELMAkGA1UE
BhMCSU4xCzAJBgNVBAgTAlROMQwwCgYDVQQHEwNDaG4xETAPBgNVBAoTCENBQ053
aWxkMREwDwYDVQQLEwhDQUNOd2lsZDEjMCEGA1UEAwwaKi5jczIxLmRldml0LmNp
c2NvbGFicy5jb20wHhcNMjExMjE1MTE0NzAwWhcNMjIxMjE1MTE0NzAwWjBzMQsw
CQYDVQQGEwJJTjELMAkGA1UECBMCVE4xDDAKBgNVBAcTA0NobjERMA8GA1UEChMI
Q0FDTndpbGQxETAPBgNVBAsTCENBQ053aWxkMSMwIQYDVQQDDBoqLmNzMjEuZGV2
aXQuY2lzY29sYWJzLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJPPBRGq0wHv/6ZLPOZ3jdEgzVS+dzXJSyhtMsgm/XrvIvjRH0MK3r++dtUgHMzz
le/WrxPKGphjtNsvF7ss58RRg3fiQCSQPX6nfBYc9v4A7rSdmKzYYFbBkGPeijLB
qwVyseMa3rifjv4Bucxw0M3ZrUqq7YfcZtxZhSEtxx8rT3A/uReIm/n1ERcZDclW
+GkfRxEdY3ZLpen/2sFiOAVMvAHlKRtK7kEhmo1TPQZ0h0UQFNDbl2ZWZZ6Nuv0I
Z6pUDNj1/+GoJyvSwl0qpetHxhdMtubMAAM8JQNvNkHgzOswsbN18F5at7cZ/KFI
HuvBUXKHV5pEX3hOdJxbuocCAwEAAaNdMFswDAYDVR0TBAUwAwEB/zAdBgNVHQ4E
```

```
FgQUCNlXseZ5qBjqJtYv3sdCujJuqnAwHwYDVR0jBBgwFoAUCNlXseZ5qBjqJtYv
3sdCujJuqnAwCwYDVR0PBAQDAgGGMA0GCSqGSIb3DQEBCwUAA4IBAQBaq5KXw/wX
nzJpBnKPZuO4KNcIz9/A2Hil2ikWNBjfla1x/37OdTbh3IpHJ6n1OCeAkE5Ww7uX
amlUcWxvDk3Zn+tKysCU2Q1PYSxUHXtqH3rvWZDRglPkJUu420tnCg2fV1bulcJ1
xx6E95a9D1vCarfxvuINU50076gnypTMv9+lOFXCkvDgBOmkQpqswR5l519kmDZi
mt8CoknJN/iAENxM8b47262yXEc1X6ZN/OWa/xl4OS3X0C0hikyg9HpUGDq+CigE
s5CBCOLDfe8G9kAPoTg2mVNT10xxQF1juobb6djmdB1Of8kqgKs2eWsD+MfKvNbG
ZzPGx4SUS2RZ
-----END CERTIFICATE-----
.
Do you want to check if Common Name or SAN:dNSName or both are in Fully Qualified Domain
Name(FQDN) format ? [N]> y


Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]>
```

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名称、用户名和域名。还可以选择对于域名使用“虚拟网关 (Virtual Gateway)”域。

使用 GUI 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 (Edit Settings)**。对要修改的一个或多个地址进行更改，点击**提交 (Submit)**，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。

要想	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。

要想	相应操作
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 , on page 67 请参阅思科自动支持 (Cisco AutoSupport), on page 68
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 , on page 67
请参阅警报及其说明的列表	请参阅： 硬件警报说明 , on page 68。 系统警报说明 , on page 68
了解警报传送机制	请参阅警报传送, on page 66

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 , on page 68。
- 系统警报。请参阅系统警报说明 , on page 68。
- 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：

- 警报邮件通过标准 DNS MX 和 A 记录查找传送。
  - 它们确实会缓存 DNS 条目 30 分钟，缓存每 30 分钟刷新一次，所以如果 DNS 出现故障，警报将停止。
- 如果部署包括邮件安全设备：

- 警报邮件不通过工作队列传递，所以不对它们病毒扫描或垃圾邮件。另外，它们也不受邮件过滤器或内容过滤器约束。
- 警报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。

- [可选 - 仅当在“alertconfig”中启用了 TLS 支持并在 SSL 配置设置中启用 FQDN 验证时]：检查服务器证书中是否存在“公共名称”(Common Name)、“SAN：DNS 名称”(SAN: DNS Name) 字段或两者同时存在，以及是否为 FQDN 格式。
- [可选 - 仅当在“alertconfig”中启用 TLS 支持时]：检查服务器证书的“公共名称”(Common Name)、“SAN：DNS 名称”(SAN: DNS Name) 字段是否包含服务器的主机名。如果在“主机名”(Hostname) 字段中配置了 IP，则使用“反向 DNS”(Reverse DNS) 名称。
- [可选 - 仅当使用 `alertconfig` CLI 命令启用 TLS 支持时]：检查服务器证书中的“公共名称”(Common Name) 或“SAN：DNS 名称”(SAN: DNS Name) 字段是否包含服务器名称。
- [可选 - 仅在使用 `alertconfig` CLI 命令启用了 TLS 支持并在 SSL 配置页面中启用了 X 509 验证时]：检查服务器证书版本。

查看最近的警报

要想	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）。发送每个警报后，发送重复警报之间等待的秒数（警报间隔）将增加。增加的秒数为要等待的秒数加上两倍的上次间隔。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 (Management Appliance) > 系统管理警报 (System Administration Alerts)**，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

Table 3: 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	当磁盘分区达到 90% 容量（以及 95%、96%、97% 等）时发送。	Critical
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

Table 4: 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。	Critical
COMMON.KEY_EXPIRED_ALERT	当功能密钥到期时发送。	警告

警报名称	说明	严重性
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_ALLOWED LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED LIST	警报消息： • 由于 SSH DOS 攻击，位于 <IP 地址> 的主机已被添加到阻止列表 (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 运行列表 (The host at <IP address> has been permanently added to the ssh whitelist)。 • 位于 <IP 地址> 的主机已从阻止列表中删除 (The host at <IP address> has been removed from the blacklist)。 对于尝试通过 SSH 连接到设备，但未提供有效凭证的 IP 地址，如果两分钟内失败尝试次数大于 10 次，则将其添加到 SSH 阻止列表。 当用户从相同 IP 地址登录成功时，该 IP 地址会被添加到允许列表中。 允许访问允许列表中的地址，即使它们也位于阻止列表中。	警告
LDAP.GROUP_QUERY_FAILED_ALERT	当LDAP组查询失败时发送。	Critical
LDAP.HARD_ERROR	当LDAP完全失败（尝试所有服务器后）时发送。	Critical

警报名称	说明	严重性
LOG.ERROR.*	各种日志记录错误。	Critical
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	扫描各个收件人期间LDAP组查询失败时发送。	Critical
MAIL.QUEUE.ERROR.*	各种邮件队列硬错误。	Critical
MAIL.RES_CON_START_ALERT.MEMORY	当 RAM 利用率超过系统资源保护阈值时发送。	Critical
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。	Critical
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。	Critical
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。	Critical
MAIL.RES_CON_START_ALERT	当设备进入“资源保护”模式时发送。	Critical
MAIL.RES_CON_STOP_ALERT	在设备退出“资源节约”(Resource Conservation) 模式时发送。	Critical
MAIL.WORK_QUEUE_PAUSED_NATURAL	当工作队列暂停时发送。	Critical
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	当工作队列恢复时发送。	Critical
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。	Critical
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_EMPTY	在域规格文件为空时发送。	Critical
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_MISSING	在未找到域规格文件时发送。	Critical
REPORTD.DATABASE_OPEN_FAILED_ALERT	报告引擎无法打开数据库时发送。	Critical
REPORTD.AGGREGATION_DISABLED_ALERT	当系统磁盘空间不足时发送。当日志条目的磁盘使用量超过日志使用阈值时，报告禁用聚合并发送警报。	警告

警报名称	说明	严重性
REPORTD.DATABASE_DELETION_ALERT	如果系统检查并发现导出目录不为空，则发送，然后它会打印日志行并尝试在下一次迭代中删除该目录。	信息
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。	Critical
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。	Critical
PERIODIC_REPORTS.REPORT_TASK. EMAIL_FAILURE_ALERT	当无法发送报告时发送。	Critical
PERIODIC_REPORTS.REPORT_TASK. ARCHIVE_FAILURE_ALERT	当无法存档报告时发送。	Critical
SENDERBASE.ERROR	当处理 SenderBase 的响应期间出现错误时发送。	参考
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。	Critical

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

本节介绍用于配置设备网络操作的功能。使用这些功能可以直接访问您在运行系统设置向导使用“系统设置向导”(System Setup Wizard) 配置的主机名、DNS 和路由设置。

本节讨论以下功能：

- `sethostname`
- DNS 配置（在 GUI 中或通过在 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`
- 口令

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 命令用于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，还应设置 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，超时分别为 5 秒、10 秒、45 秒。

例如，假设您配置了四台DNS服务器，其中两台为优先级0，一台为优先级1，另一台为优先级2：

***Table 5: 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 的两台服务器均关闭，则使用优先级为 1 的服务器 (1.2.3.6)，最后是优先级为 2 (1.2.3.7) 的服务器。

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。

Note 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。其中包括对连接主机的 IP 地址的反向 DNS (PTR) 查找，之后是对 PTR 查找结果的正向 DNS (A) 查找。然后，系统将检查 A 查找结果是否与 PTR 查找结果匹配。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，与多个条目和优先级, on page 73中讨论的通用 GNS 超时无关。

默认值为 20 秒。可以全局禁用所有侦听程序中的反向 DNS 查询超时，方法是输入“0”作为秒数。如果将该值设置为 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

有时，重启设备时，系统会生成警报，其中包含“无法引导DNS缓存”的消息。该消息表示系统无法与其主 DNS 服务器联系，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。如果其他时候出现此消息，可能表示存在网络问题或 DNS 配置未指向有效的服务器。

清除 DNS 缓存

GUI 中的**清除缓存**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。该命令会立即生效，并且重新填充缓存时可能导致性能临时下降。

通过图形用户界面配置 DNS 设置

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

步骤 2 依次选择**管理设备 (Management Appliance) > 网络 (Network) > DNS** 页面，然后点击**编辑设置 (Edit Settings)** 按钮。

步骤 3 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 4 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)**。对于每个服务器重复上述步骤。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, on page 73。

步骤 5 选择一个用于 DNS 流量的接口。

步骤 6 输入在取消反向 DNS 查找之前要等待的秒数。

步骤 7 （可选）通过点击**清除缓存 (Clear Cache)** 清除 DNS 缓存。

步骤 8 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，或在 CLI 中通过使用 **routeconfig** 命令来管理静态路由。

- 在 GUI 中管理静态路由, on page 75
- 修改默认网关（GUI ）, on page 75

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。

Note 如果目标是子网而不是单个 IP 地址，请确保条目遵循 CIDR（无类域间路由）表示法，例如 192.168.90.0/24。

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

步骤 2 在**管理设备 (Management Appliance)** > **网络 (Network)** > **路由 (Routing)** 页面上，点击路由列表中的**添加路由 (Add Route)**。然后输入路由的名称。

步骤 3 输入目标 IP 地址。

步骤 4 输入网关 IP 地址。

步骤 5 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”(Management Appliance)>“网络”(Network)>“路由”(Routing)页面（请参阅修改默认网关（GUI ）, on page 75）或在 CLI 中通过使用 setgateway 命令来配置默认网关。

安全通信协议

如果计划从启用了 TLSv1.0 的较低 AsyncOS 版本（例如 13.6.x）升级到 AsyncOS 13.8.x 及更高版本，则会默认禁用 TLSv1.0 并启用 TLSv1.1 和 TLSv1.2。您需要在升级后在设备上启用 TLSv1.0 方法。

从 AsyncOS 15.5 及更高版本开始，建议使用 TLSv1.1、TLSv1.2 和 TLSv1.3（用于设备管理 Web 用户界面）方法，而不是 TLSv1.0。TLSv1.3 默认处于禁用状态，您必须启用它。

指定安全通信协议

您可以选择用于以下服务的通信协议：

- 设备管理 Web 用户界面
- 安全 LDAP 服务
- Updater Service
- 最终用户对垃圾邮件隔离区的访问

Note 更新服务器和安全 LDAP 服务都会在新安装的设备上使用 TLSv1.1 和 TLSv1.2 方法。设备管理 Web 用户界面会默认使用 TLSv1.1 和 TLSv1.2 方法，而新安装的设备会默认禁用 TLSv1.3 方法。

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。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。

如果您使用本地（远程）更新程序服务，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。

有关对等证书 FQDN 验证的信息，请参阅FQDN, on page 120。

有关对等证书 X509 验证的信息，请参阅X.509 证书, on page 122。

配置系统时间

Note 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。

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。

要想	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, on page 77
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, on page 78 • 更新时区文件, on page 78

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。请参阅防火墙信息

相关主题

- 配置系统时间, on page 77
- 手动更新时区文件 , on page 79

（推荐）使用网络时间协议 (NTP) 设置设备系统时间

这是建议的时间保留方法，特别是您的设备与其他设备集成时更是如此。所有集成设备应使用同一台 NTP 服务器。

您可以在 CLI 中使用 `ntpconfig` 命令以使用 NTP 服务器来设置时间。

步骤 1 前往**系统管理 (System Administration) > 时间设置 (Time Settings)** 页面。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 在“时间保留方法”(Time Keeping Method) 部分，选择**使用网络时间协议 (Use Network Time Protocol)**。

步骤 4 输入 NTP 服务器地址，然后点击**添加行 (Add Row)**。您可以添加多个 NTP 服务器 。

步骤 5 要从列表中删除 NTP 服务器，请点击该服务器对应的垃圾桶图标。

步骤 6 为 NTP 查询选择一个接口。这是 NTP 查询应该源于的 IP 地址。

步骤 7 选中**使用 NTP 身份验证 (Use NTP Authentication)** 复选框以确保时间戳是由可信源生成的，从而保护 NTP 免受恶意活动或拦截。

步骤 8 提交并确认更改。

选择 GMT 偏移

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

步骤 2 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **时区 (Time Zone)**。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 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 5 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 6 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 , on page 78
- 手动更新时区文件 , on page 79

自动更新时区文件

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

步骤 2 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **更新设置 (Update Settings)**。

步骤 3 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 4 输入时间间隔。点击页面上的 **?** 了解重要信息。

步骤 5 提交并确认更改。

手动更新时区文件

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

步骤 2 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **时区设置 (Time Settings)**。

步骤 3 查看**时区文件更新 (Time Zone File Updates)** 部分。

步骤 4 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) 页面

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 , on page 79
导入保存的配置	保存和导入配置设置 , on page 79
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
重置配置	将配置重置为出厂默认设置, on page 36

保存和导入配置设置

Note 此部分中介绍的配置文件用于配置安全管理设备。

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。
- 可以下载现有的配置文件，对其更改，再将其上传到同一设备。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
- 将配置重置为出厂默认设置, on page 36
- 回滚到以前已确认的配置 , on page 82

保存和导出当前的配置文件

使用**管理设备 (Management Appliance) > 系统管理 (System Administration) > 配置文件 (Configuration File)** 页面上的“当前配置”(Current Configuration) 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。

屏蔽口令

（可选）通过选中该复选框屏蔽用户的口令。屏蔽口令会使初始加密的口令在导出或保存的文件中替换为“*****”。

Note 带屏蔽口令的配置文件不能加载回 AsyncOS 中。

加密口令

可以通过选中加密配置文件中的密码复选框来加密用户的密码。下面列出了将要加密的配置文件中的重要安全参数。

- 证书私钥
- RADIUS 密码
- LDAP 绑定密码
- 本地用户的密码散列
- SNMP 密码
- 外发 SMTP 身份验证密码
- PostX 加密密钥
- PostX 加密代理密码
- FTP 推送日志订用的密码
- IPMI LAN 密码
- 更新程序服务器 URL

可以使用 `saveconfig` 命令在命令行界面中配置此参数。

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。

无法加载带屏蔽口令的配置文件。

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”。

Caution 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

上传或粘贴一部分配置文件时，请务必小心。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>
```

Caution 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。

关于加载日志订用口令的注意事项

如果尝试加载的配置文件包含需要口令的日志订用（例如，将使用FTP推送的日志订用），`loadconfig` 命令不会警告您缺少口令。FTP 推送失败并生成警报，直到您使用 `logconfig` 命令配置正确的口令为止。

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, on page 36。

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。

Note 恢复先前的配置时，不会生成日志消息或警报。

Note 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, on page 36）
- `publishconfig`
- `backupconfig`（请参阅备份安全管理设备数据 , on page 42）
- `trailblazerconfig`

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口令。选择不包括口令会将任何口令字段留空。如果您担心安全漏洞，您可以选择不包括口令。但是，在使用 `loadconfig` 命令加载时，不含口令的配置文件会失败。请参阅关于加载日志订用口令的注意事项, on page 82。

Note 在保存、显示或通过邮件发送配置文件时，如果您选择包括口令（对“是否要包括口令？”回答“是”），口令会被加密。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 passphrases? Please be aware that a configuration without
passphrases 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 passphrases? Please be aware that a configuration
without passphrases 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）存储和保存到配置目录中。

```
mail3.example.com> saveconfig
Do you want to include passphrases? Please be aware that a configuration without passphrases

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, on page 81。

rollbackconfig 命令

请参阅回滚到以前已确认的配置 , on page 82。

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列表列出了受支持的主配置，此版本说明位于 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)**。

Trailblazerconfig 命令

您可以使用 `trailblazerconfig` 命令通过新 Web 界面上的 HTTP 和 HTTPS 端口路由传入和传出连接。

您可以在 CLI 上使用以下命令查看联机帮助：`help trailblazerconfig`。

语法如下：

```
trailblazerconfig enable <https_port> <http_port>

trailblazerconfig disable

trailblazerconfig status
```

其中：

`"enable"` 在默认端口（HTTPS：4431）上运行 trailblazer 配置。

`"disable"` 禁用 trailblazer 配置

`"status"` 检查 trailblazer 配置的状态。

重要事项 默认情况下，您的设备上已启用 `trailblazerconfig` CLI 命令。确保在防火墙中打开 HTTPS 端口。确保 DNS 服务器可以解析为访问设备指定的主机名。

`Trailblazerconfig`命令可帮助您避免以下问题：

- 需要在某些浏览器中为 API 端口添加多个证书。
- 当您刷新“垃圾邮件隔离区”(Spam quarantine)、“安全列表”(Safelist) 或“阻止列表”(Blocklist) 页面时，重定向到旧版 Web 界面。
- “高级恶意软件保护”报告页面上的指标栏不包含任何数据。

注释 当您在设备上启用 `trailblazerconfig` 命令时，请求 URL 将包含附加到主机名的`trailblazerconfig` HTTPS 端口号。

updatepvocert 命令

您必须在 CLI 中使用 `updatepvocert` 命令来更新 2048 位的 CA 证书，才能在 FIPS 模式下的受管思科邮件安全设备上启用集中策略、病毒和隔离区。

如果启用了 FIPS，受管邮件安全设备上的集中策略、病毒和隔离区功能会被禁用。从 AsyncOS 13.0 开始，在 FIPS 模式下的设备会使用 2048 位证书来启用集中策略、病毒和病毒爆发隔离区。较早的 AsyncOS 版本具有大小为 1024 位的证书。

```
example.mail.com> updatepvocert
This command will recreate the PVO certificate and key of strength 2048 bits.
Also, the new certificate will be signed by a CA of strength 2048 bits.
Hermes process will restart post certificate update. No commit will be required.
Do you want to proceed with the certificate update? [Y]>

Certificate updated successfully. Hermes restart needed for the changes to be effective.
Do you want to restart hermes? []> Y

Enter the number of seconds to wait before abruptly closing connections. [30]>

Waiting for listeners to exit... Receiving suspended for euq_listener, cpq_listener. Waiting
 for outgoing deliveries to finish... Mail delivery suspended. Receiving resumed for
euq_listener, cpq_listener. Mail delivery resumed.
Hermes will be up in a moment. Run the status command for hermes.

example.mail.com >
```

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。

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：

Example:

```
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。）最后，确认更改。

Example:

```
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，限制为 2 TB。

Note 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：

Before you begin

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 用 VMWare 提供的实用工具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 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 4 转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 磁盘管理 (Disk Management)**，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

要想	相应操作
查看设备上的总可用磁盘空间	依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 磁盘管理 (Disk Management)**。 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 89 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和邮件在隔离区中的保留时间。
- 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

当其他磁盘使用量达到配额的 75% 时，您会开始收到警告级别的系统警报。在收到这些警报时，您应采取措施。

要确保收到这些警报，请参阅管理警报, on page 65。

管理“其他”配额的磁盘空间

其他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 (Management Appliance) > 系统管理 (System Administration) > 日志订用 (Log Subscriptions)**，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用。 • 验证并确保日志级别未超过必要的冗长程度。 • 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 （这些文件不太可能占用太多磁盘空间。）	通过 FTP 转至设备的 /data/pub 目录。 要配置通过 FTP 访问设备，请参阅 通过 FTP 访问设备
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 , on page 87。

Before you begin

- 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, on page 88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 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 磁盘管理 (Disk Management)**。

步骤 3 点击**编辑磁盘配额 (Edit Disk Quotas)**。

步骤 4 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 5 点击**提交 (Submit)**。

步骤 6 点击**确认 (Commit)** 确认更改。

管理数据存储时间

现在，您可以配置思科安全邮件和 Web 管理器，以便根据天数将邮件（数据）存储在“集中邮件跟踪”数据库中。

使用旧 Web 界面的“系统管理”(System Administration) > “磁盘管理”(Disk Management) > “编辑数据磁盘管理”(Edit Data Disk Management) 页面中的**应用数据存储时间 (Apply Data Storage Time)** 选项来配置数据存储时间。

“应用数据存储时间”(Apply Data Storage Time) 选项适用于以下任何一种情况：

- 如果达到配置的数据磁盘存储限制（例如 500 GB），系统会自动从数据库中删除消息，甚至是在达到配置的数据存储时间之前（例如“40 天”）。
- 如果配置的数据存储时间限制为 40 天，并且超过配置的数据存储时间限制的邮件（例如，邮件已存储“41 天”），则即使未达到配置的数据磁盘存储限制（例如，“500 GB”），系统也会自动删除相应邮件。

注释 您还可以使用 CLI 中的 `diskquotaconfig` > `edit` > `Centralized Email Tracking` 子命令中的 `Manage data based on the storage time` 语句，根据天数将邮件存储在“集中邮件跟踪”(Centralized Email Tracking) 数据库中。

重要信息：从思科安全邮件和 Web 管理器 13.6.2 版开始，Splunk 数据库不再用于邮件跟踪数据。所有新的邮件跟踪数据都将存储在 Lucene 数据库中。如果使用“应用数据存储时间”(Apply Data Storage Time) 选项，则包含邮件跟踪数据的 Splunk 数据库将自动删除。

操作：确保备份邮件跟踪数据（如果需要）。您可以在 CLI 中使用 `backupconfig` 命令来执行备份操作。有关详细信息，请参阅计划单次或经常性的备份，第 45 页。

注释 如果您的组织网络只有一个安全邮件和 Web 管理器，则需要在网络中部署新的虚拟机 (VM)。有关如何部署虚拟安全邮件和 Web 管理器的详细信息，请参阅《思科安全邮件和 Web 虚拟设备安装指南》。

开始之前

请确保您拥有集中邮件跟踪服务的有效功能密钥。

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

步骤 2 选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **磁盘管理 (Disk Management)**。

步骤 3 点击**编辑磁盘配额 (Edit Disk Quotas)**。

步骤 4 选择“集中邮件跟踪”(Centralized Email Tracking) 下的**应用数据存储时间 (Apply Data Storage Time)**，然后在给定字段中输入值，以便根据天数将邮件（数据）存储在“集中邮件跟踪”(Centralized Email Tracking) 数据库中。

步骤 5 点击**提交 (Submit)**。

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

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

步骤 2 点击**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **系统运行状况 (System Health)**。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 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 5 提交并确认更改。

使用 SAML 2.0 的 SSO

- 关于 SSO 和 SAML 2.0, on page 92
- SAML 2.0 SSO 工作流, on page 92
- SAML 2.0 的准则和限制, on page 93
- 如何为垃圾邮件隔离区配置 SSO, on page 100

• 如何在思科安全管理设备中配置 SSO, on page 93

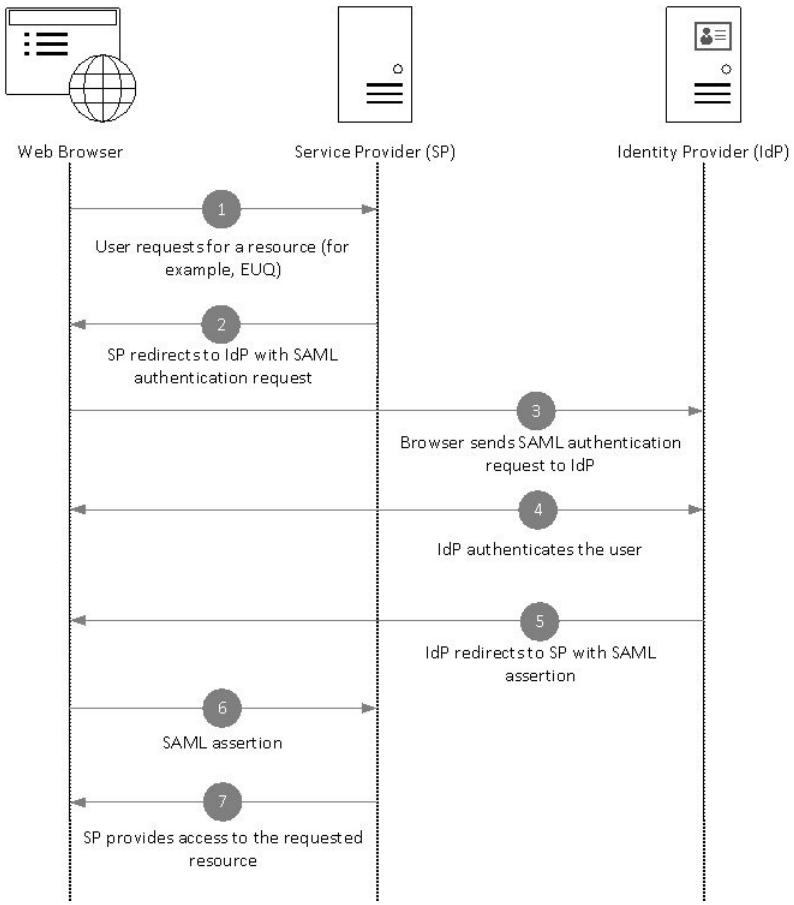
关于 SSO 和 SAML 2.0

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 SAML 2.0 SSO 的服务时使用的相同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：

***Figure 7: SAML 2.0 SSO* 工作流**



工作流程

1. 最终用户使用网络浏览器从运营商（您的设备）请求资源。例如，最终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. 身份提供程序对最终用户进行身份验证。身份提供程序会向最终用户显示登录页，然后最终用户登录。
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

注销

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。

概述

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。

如何在思科安全管理设备中配置 SSO

过程

	命令或操作	目的
步骤 1	查看前提条件。	前提条件， 第 94 页
步骤 2	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 95 页
步骤 3	[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管理设备通信， 第 96 页

	命令或操作	目的
步骤 4	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 99 页
步骤 5	在设备上使用 SAML 启用外部身份验证	启用 SAML 身份验证，第 99 页

前提条件

- 支持的身份提供程序，第 94 页
- 用于安全通信的证书，第 94 页

支持的身份提供程序

验证您的组织使用的身份提供程序是否受思科邮件安全设备的支持。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 及更高版本
- Duo Access Gateway
- Azure AD

用于安全通信的证书

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。

转换证书

通常，从设备获取的证书采用 .pfx 格式，当您将设备配置为服务提供商时，必须将其转换为 pem 格式。

要将证书从 .pfx 格式转换为 pem 格式，请执行以下操作：

- 下载并安装 OpenSSL 工具，并导入从您设备中获取的证书文件 (.pfx)。
- 运行以下命令以 .pem 格式导出证书：`openssl pkcs12 -in <certname>.pfx -nokeys -out cert.pem`
- 运行以下命令以 .pem 格式导出私钥：`openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`
- 运行以下命令以从私钥中删除密码：`openssl rsa -in key.pem -out server.key`

将思科内容安全管理设备配置为服务提供程序

Before you begin

查看前提条件, on page 94。

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

步骤 2 选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > SAML**。

步骤 3 在“服务提供程序”(Service Provider) 部分下，点击**添加服务提供程序 (Add Service Provider)**。

步骤 4 输入下列详细信息：

字段	说明
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。
SP 证书	**Note** 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： **a.** 上传证书和相关的私钥。 **b.** 输入私钥密码。 **c.** 选择**签名请求 (Sign Request)**。 **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： **a.** 上传证书和相关的私钥。 **b.** 输入私钥密码。

字段	说明
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 (Sign Assertions)**。 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。请参阅将身份提供程序配置为与思科内容管理设备通信, on page 96。
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 5 点击**提交 (Submit)**。

步骤 6 记下“SSO 设置”(SSO Settings) 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”(Service Provider Settings) 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 (Export Metadata)** 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。

What to do next

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管理设备通信, on page 96。

将身份提供程序配置为与思科内容管理设备通信

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 95 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 95 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 配置为与思科安全管理设备进行通信，第 97 页。
- 将 Azure AD 配置为与思科安全管理设备进行通信，第 98 页。
- 将 Duo Access Gateway 配置为与思科安全管理设备进行通信，第 98 页。

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。请参阅将身份提供程序配置为与思科内容管理设备通信，第 96 页。

将 AD FS 配置为与思科安全管理设备进行通信

以下是将 AD FS（2.0 及更高版本）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“服务提供程序”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 格式的服务提供程序的（设备的）证书。
- 在“中继方信任”>“属性”>“高级”下将安全散列算法设置为 SHA-1。
- 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/format"] =

"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified");
```

- 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。此外，请确保添加颁发转换规则，以将组属性的 LDAP 属性作为传出声明类型（未指定的组）发送。

将 Azure AD 配置为与思科安全管理设备进行通信

以下是将Azure AD配置为与您的设备进行通信所需执行的高级任务。有关完整和详细的说明，请参阅 *Microsoft Azure AD* 文档。

- 将服务提供商（设备）的断言使用者URL添加为接收和处理SAML断言的服务提供商标识符。
- 在“企业应用 > 新建应用 > 非图库应用 > 单点登录 > 基本 SAML”配置下，在 Azure 门户中输入服务提供商（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。
- 如果您已将服务提供商（设备）配置为发送签名的 SAML 身份验证请求，请在“SAML 签名证书”部分（“企业应用 > 新建应用> 非图库应用 > 单点登录 > SAML 签名证书”）下上传服务提供商的证书（用于签署身份验证请求）。
- 在“用户属性和声明”部分（“企业应用 > 新建应用 > 非图库应用 > 单点登录 > 用户属性和声明”）下，配置组声明并添加组属性。
- 在“企业应用 > 新建应用 > 非图库应用 > 用户和组”下添加用户和组，以允许用户基于 SAML 断言或响应登录到应用。

将 Duo Access Gateway 配置为与思科安全管理设备进行通信

以下是将 Duo Access Gateway 配置为与设备进行通信所需执行的高级任务。有关完整的详细说明，请参阅 *Duo Security* 文档。

- 将服务提供商（设备）的断言使用者 URL 添加为接收和处理 SAML 断言的服务提供商终端。
- 在“Duo 管理面板 > 应用 > 保护应用 > SAML 服务提供商”下，输入服务提供商（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。
- 如果已将您的服务提供商（设备）配置为发送已签名的 SAML 身份验证请求，则在 Duo Access Gateway 上配置身份验证源时，请上传服务提供商的证书（用于签名身份验证请求），证书采用 .cer 格式。
- 如果计划将双核配置为发送加密的 SAML 断言，请在配置了双核接入网关上的身份验证源时，以 .cer 格式上传服务提供商（设备的）证书。
- 在“Duo 管理面板 > 应用 > 保护应用 > SAML 服务提供商”下，将“NameID" 格式为”选择为“未指定”。
- 在“Duo 管理面板 > 应用 > 保护应用 > SAML 服务提供商”下，将“安全散列算法”设置为 SHA-256。
- 在“Duo 管理面板”上，将“SAML 服务提供程序设置”另存为配置文件，并将配置文件作为 SAML 应用导入 Duo Access Gateway 中。

在思科内容安全管理设备上配置身份提供程序设置

Before you begin

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管理设备通信, on page 96。
- 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 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 2 选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **SAML**。

步骤 3 在“身份提供程序”(Identity Provider) 部分下，点击**添加身份提供程序 (Add Identity Provider)**。

步骤 4 输入下列详细信息：

字段	说明
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。
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 (Import Metadata)** 并选择元数据文件。

步骤 5 提交并确认更改。

What to do next

启用 SAML 身份验证, on page 99

启用 SAML 身份验证

您可以使用 SAML 来启用“单点登录”，以对用户进行身份验证，并将用户组分配给思科规则。

开始之前

请确保您已使用“服务提供商”和“身份提供程序”设置来配置 SAML 配置文件。请参阅如何在思科安全管理设备中配置 SSO，第 93 页。

步骤 1 导航至**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **用户 (Users)**。

步骤 2 向下滚动到**外部身份验证 (External Authentication)** 部分。

步骤 3 点击**启用 (Enable)**。

步骤 4 选中**启用外部身份验证 (Enable External Authentication)** 复选框。

步骤 5 从下拉列表中选择 **SAML** 作为身份验证类型。

步骤 6 （可选）在**外部身份验证属性名称映射**字段中，输入要从组映射中搜索的属性名称。

属性名称取决于为身份提供程序配置的属性。设备将搜索与**组映射**字段中的“属性名称”匹配的条目。这是可选项。如果不配置此项，设备将搜索“组映射”字段中的所有属性的匹配条目。

步骤 7 在**组映射**字段中，根据预定义或自定义用户角色，输入 SAML 目录中定义的组名称属性。您可以点击**添加行 (Add Row)** 以添加多个角色映射。

组映射必须包含组属性。您可以添加“未指定组”属性以对 SAML 断言或响应进行身份验证。

有关用户角色类型的详细信息，请参阅“用户”(User) 页面。

步骤 8 提交并确认更改。

下一步做什么

启用 SAML 外部身份验证后，您可以使用设备登录页面上的**使用单点登录**链接，并输入用户名以登录到设备。

如何为垃圾邮件隔离区配置 SSO

	相应操作	更多信息
第 1 步	查看前提条件。	前提条件, on page 101
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, on page 101
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 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, on page 104
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, on page 105

	相应操作	更多信息
第 6 步	将新的身份验证机制通知给最终用户。	

前提条件

- 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

Before you begin

查看前提条件, on page 101。

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

步骤 2 选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > SAML**。

步骤 3 在“服务提供程序”(Service Provider) 部分下，点击**添加服务提供程序 (Add Service Provider)**。

步骤 4 输入下列详细信息：

字段	说明
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。

字段	说明
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。
SP 证书	**Note** 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： **a.** 上传证书和相关的私钥。 **b.** 输入私钥密码。 **c.** 选择**签名请求 (Sign Request)**。 **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： **a.** 上传证书和相关的私钥。 **b.** 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 (Sign Assertions)**。 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。请参阅将身份提供程序配置为与思科内容安全管理设备通信, on page 103。
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 5 点击**提交 (Submit)**。

步骤 6 记下“SSO 设置”(SSO Settings) 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”(Service Provider Settings) 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 (Export Metadata)** 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。

What to do next

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, on page 103。

将身份提供程序配置为与思科内容安全管理设备通信

Before you begin

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, on page 101。
- 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, on page 101。

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, on page 103
- 将 PingFederate 7.2 配置为与思科内容安全管理设备通信, on page 104
- 《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。

What to do next

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, on page 104。

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“服务提供程序”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 格式的服务提供程序的（设备的）证书。
- 在“中继方信任”>“属性”>“高级”下将安全散列算法设置为 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

Before you begin

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, on page 103。
- 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 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **SAML**。

步骤 3 在“身份提供程序”(Identity Provider) 部分下，点击**添加身份提供程序 (Add Identity Provider)**。

步骤 4 输入下列详细信息：

字段	说明
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。
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 (Import Metadata)** 并选择元数据文件。

步骤 5 提交并确认更改。

What to do next

为垃圾邮件隔离区启用 SSO, on page 105

为垃圾邮件隔离区启用 SSO

Before you begin

确保您：

- 已配置**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **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。

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

步骤 2 依次选择**管理设备 (Management Appliance)** > **集中服务 (Centralized Services)** > **垃圾邮件隔离区 (Spam Quarantine)**。

步骤 3 点击**编辑设置 (Edit Settings)** 并向下滚动到“最终用户隔离区访问”(End-User Quarantine Access) 部分。

步骤 4 请确保已启用“最终用户隔离区访问”。

步骤 5 将最终用户身份验证方法设置为 **SAML2.0**。

步骤 6 （可选）指定在释放邮件前，是否显示邮件正文。

步骤 7 提交并确认更改。

What to do next

将新的身份验证机制通知给最终用户。

在 AsyncOS API 的思科内容安全管理上配置 OpenID Connect 1.0

概述

思科内容安全管理设备支持与使用身份提供程序 (IDP) 和 OpenID Connect 1.0 身份验证的应用或客户端集成，以便与设备中可用的 AsyncOS API 进行无缝连接。目前，您的设备仅使用 Microsoft AD FS 进行了 OpenID Connect 认证。

工作流程

在以下工作流程中，AD FS 会被用作身份提供程序，外部应用程序会被用作客户端，而设备会被用作资源提供程序。

步骤：

1. 在以下工作流程中，AD FS 会被用作身份提供程序，外部应用程序会被用作客户端，而设备会被用作资源提供程序，请参阅在设备上配置 OpenID Connect， 第 108 页。
2. [一次性活动] 设备根据步骤 1 中的配置获取 OpenID Connect 配置元数据和所需的密钥，以便验证访问令牌。
3. 在使用 AD FS 对外部应用进行身份验证后获取访问令牌。有关如何对访问令牌进行身份验证和接收的详细信息，请参阅身份验证提供程序或身份提供程序文档。
4. 将 API 请求与访问令牌一起发送到设备。
5. 设备会使用从第 2 步检索的密钥集来验证 API 请求中的访问令牌。

6. 设备对访问令牌中的所需的声明（签发者、受众）进行验证。
7. 设备使用角色声明值来授权和分配用户角色权限，以便访问 AsyncOS API。
8. 设备会为 AsyncOS API 请求提供适当的响应。

示例访问令牌

以下是示例访问令牌的格式：

标题

alg:RSA256

typ:JWT

[….]

负载

claim:aud: CiscoEmailAPICaller

claim:iss:http://adfsserver/adfs/services/trust

claim:iat: 1594712147

claim:exp: 1594712807

claim: CustomOrgIdentifier: MyCustomOrgId

claim: LastName: Fernandes

claim: FirstName: Erik

claim: Email: http://erik.fernandes@customorg.com

claim: Role: LogCollector

claim: Role: ReadOnly

[…..]

设备仅支持验证由以下算法签名的访问令牌：

- RSA256
- RSA384
- RSA512

前提条件

在使用 OpenID Connect 配置设备之前，请确保满足以下前提条件：

- 设备支持您的组织使用的身份验证提供程序。
- 应用可以使用身份验证提供程序进行身份验证并检索访问令牌。

- 设备可以通过 HTTP 连接到身份验证提供程序，以便获取 OpenID Connect 元数据配置。

在设备上配置 OpenID Connect

开始之前

确保您符合以下条件：

- 身份验证提供程序颁发的有效访问令牌（基于您的身份验证提供程序设置）。
- 访问令牌必须包含角色信息，以便允许设备执行所需的授权检查。

步骤 1 点击**系统管理 (System Administration)** > **OpenID Connect**。

步骤 2 点击**编辑设置 (Edit Settings)**

步骤 3 输入下表中描述的所需参数，以配置 OpenID Connect：

OpenID Connect 参数	说明
身份提供程序元数据 URL	输入用于获取 OpenID Connect 配置元数据的身份提供程序 URL。该元数据用于验证访问令牌。 以下是身份提供程序 URL 的示例 - https://example.com/adfs/.well-known/openid-configuration
签发者	输入访问令牌的签发者的值。 **注释** 在验证访问令牌时，该值必须与访问令牌的签发者声明值相匹配。 以下是颁发机构的示例 - http://example.com/adfs/services/trust
受众	输入必须与访问令牌的受众声明值匹配的受众值。 **注释** 如果要添加多个受众值，请点击**添加行 (Add Row)**。
声明名称	输入访问令牌中的声明名称，该令牌中包含了用户角色信息。声明名称用于从访问令牌检索角色信息。
身份提供程序到设备角色的映射	输入在身份提供程序服务器中定义的用户组角色，然后选择在设备中配置的对应本地用户角色，以便映射两个角色。 **注释** 如果要添加多个角色映射记录，请点击**添加行 (Add Row)**。

步骤 4 提交并确认更改。

下一步做什么

将访问令牌包含在 AsyncOS API 调用的授权承载报头中，并发送 API 请求。

以下是使用 API 的“授权承载”报头中的访问令牌调用 AsynOS API 的示例。

```
curl --location --request
GET 'https://sma.com/sma/api/v2.0/config/logs/subscriptions?retrievalMethod=manual'
--header 'Authorization: Bearer <add access_token here>'
```

使用 CLI 在设备上配置 OpenID Connect

使用 **oidcconfig** 命令执行以下任务：

- 在 AsyncOS API 的邮件网关上配置 OpenID Connect。
- 删除邮件网关上的 OpenID Connect 配置设置。

自定义视图

使用收藏夹页面

（仅限通过本地身份验证的管理用户。）可以创建最常用的页面的快速访问列表。

要想	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”菜单中选择**将此页面添加到我的收藏夹**。 无需提交对“我的收藏夹”(My Favorites) 的更改。
对收藏内容进行重排序	依次选择**我的收藏夹 (My Favorites) > 查看我的所有收藏夹 (View All My Favorites)**，并按所需的顺序拖动收藏夹。
编辑收藏夹页面、名称或说明	依次选择**我的收藏夹 (My Favorites) > 查看我的所有收藏夹 (View All My Favorites)**，然后点击要编辑的收藏夹的名称。
删除收藏夹	依次选择**我的收藏夹 (My Favorites) > 查看所有收藏内容 (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。
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）
- 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。

Tip 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”(Options) 菜单中选择显示语言。

常规设置

- 改善网络界面显示 ， 第 111 页
- 监控 Web 使用情况分析 ， 第 110 页

监控 Web 使用情况分析

“使用情况分析”用于深入了解站点活动数据以分析统计信息。如果启用“使用情况分析”，设备将在新 Web 界面上收集设备的功能使用情况数据。使用情况统计数据可用于分析和提供有助于改善设备用户体验的见解。

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

步骤 2 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **常规设置 (General Settings)**。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 选中“使用情况分析”(Usage Analytics) 字段中的**启用 (Enable)** 复选框。

步骤 5 提交并确认更改。

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。

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

步骤 2 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **常规设置 (General Settings)**。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 选择“覆盖 IE 兼容模式”(Override IE Compatibility Mode) 字段中的**启用 (Enable)** 复选框。

步骤 5 提交并确认更改。

重启和查看设备上启用的服务的状态

可以使用 CLI 中的 `diagnostic > services` 子命令来：

- 重启设备上启用的服务，而不必重新启动设备。
- 查看设备上启用的服务的状态。

示例：查看报告服务的状态

在下面的示例中，`services` 命令用于查看设备上启用的报告服务的状态。

```
mail.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.


[]> services

Choose one of the following services:
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
- API_SERVER - API Server
[]> reporting

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
```

```
[]> status

Reporting has been up for 28d 20h 45m 35s.
```

示例：重启邮件跟踪服务

在下面的示例中，services 命令用于重新启动设备上启用的邮件跟踪服务。

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.

[]> services

Choose one of the following services:
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
- API_SERVER - API Server
[]> tracking

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> restart
```

管理证书颁发机构列表

设备会使用存储的受信任证书颁发机构来验证源自远程域的证书，以便建立域的凭证。您可以将安全管理设备配置为使用以下受信任证书颁发机构：

- 系统列表 - 设备具有受信任证书颁发机构的预装列表。此列表称为系统列表。
- 自定义列表 - 您可以自定义受信任证书颁发机构列表，然后将自定义列表导入设备。

注释 验证远程域的证书时，您可以使用系统列表或自定义列表，或同时使用两者。

可以在 GUI 中使用**网络 (Network) > 证书 (Certificates) > 编辑证书颁发机构 (Edit Certificate Authorities)** 页面，或在 CLI 中使用 **certconfig** > **certauthority** 命令。

在**网络 (Network) > 证书 (Certificates) > 编辑证书颁发机构 (Edit Certificate Authorities)** 页面，您可以执行以下任务：

- 选择是否使用系统列表。您可以启用或禁用系统列表。有关详细信息，请参阅禁用系统证书颁发机构列表，第 113 页。
- 选择是否使用自定义证书颁发机构列表。您可以启用设备使用自定义列表，然后从文本文件中导入列表。有关详细信息，请参阅导入自定义证书颁发机构列表，第 113 页。
- 导出证书颁发机构列表。您可以将证书颁发机构系统列表或自定义列表导出至本地驱动器上的某个位置。有关详细信息，请参阅 导出证书颁发机构列表，第 114 页。

在**网络 (Network) > 证书 (Certificates) > 管理受信任根证书 (Manage Trusted Root Certificates)** 页面，您可以执行以下任务：

- 查看证书的自定义和系统列表。有关详细信息，请参阅 显示信任根证书，第 114 页。
- 删除现有的证书。您可以删除已导入的自定义证书。有关详细信息，请参阅删除自定义证书，第 115 页

禁用系统证书颁发机构列表

预安装的系统证书颁发机构列表无法从设备上删除，但是，您可以启用或禁用此列表。您可以禁用它，从而只允许设备使用列表来验证远程主机的证书。

过程

	命令或操作	目的
步骤 1	导航到**网络 (Network) > 证书 (Certificates)** 页面。	
步骤 2	在“证书颁发机构”(Certificate Authorities) 部分，点击**编辑设置 (Edit Settings)**。	
步骤 3	对“系统列表”(System List) 点击**禁用 (Disable)** 选项。	
步骤 4	提交并确认更改。	

导入自定义证书颁发机构列表

您可以创建颁发证书颁发机构自定义列表，并将列表导入设备。此文件必须是PEM格式，且包括您希望设备信任的证书颁发机构的证书。

步骤 1 点击**网络 (Network) > 证书 (Certificates)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择**启用 (Enable)** 单选按钮。

步骤 4 在自定义列表中点击**选择文件 (Choose File)**。

步骤 5 浏览到证书所在的位置，然后点击**确定 (OK)**。

步骤 6 [可选]选中“FQDN验证”(FQDN Validation)复选框，以便允许邮件网关检查证书中存在的“公用名称”(Common Name)、“SAN：DNS 名称”(SAN: DNS Name) 字段或两者是否均为 FQDN 格式。

步骤 7 点击**提交 (Submit)**。

注释 下面将对 CA 导入执行以下检查：

- 到期时间
- 重复
- 存在 CA 标记并已设为“True”
- 如果导入了中间证书颁发机构，则会存在根证书颁发机构。

导出证书颁发机构列表

如果您只想在系统中使用部分受信任证书颁发机构，或者要编辑现有的自定义列表。

注释 您可以将自定义列表导出为一个 .txt 文件，并可编辑添加或删除证书颁发机构，然后将该文件作为自定义列表重新导入设备。

步骤 1 点击**网络 (Network) > 证书 (Certificates)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

“编辑设置”(Edit Settings) 将列出自定义证书和思科受信任根证书。

步骤 3 点击证书名称。

步骤 4 点击**导出 (Export)** 以导出证书。

显示信任根证书

步骤 1 点击**网络 (Network) > 证书 (Certificates)**。

步骤 2 点击**管理受信任根证书 (Manage Trusted Root Certificates)**。

“管理受信任根证书”(Manage Trusted Root Certificates) 会列出自定义和思科受信任的根证书。

步骤 3 选中**覆盖信任 (Override Trust)** 复选框以覆盖信任。

步骤 4 点击**提交 (Submit)**。

在“管理受信任根证书”(Manage Trusted Root Certificates) 页面中，您可以点击“下载证书”(Download Certificate) 以下载证书并将其存储到本地计算机。

删除自定义证书

步骤 1 点击**网络 (Network)** > **证书 (Certificates)**。

步骤 2 点击**管理受信任根证书 (Manage Trusted Root Certificates)**。

“管理受信任根证书”(Manage Trusted Root Certificates) 会列出自定义证书。

步骤 3 点击**删除 (Delete)** 以删除自定义受信任根证书。

步骤 4 点击**提交 (Submit)**。

配置 CRL 源

在证书验证过程中，思科安全邮件和 Web 管理器会检查名为证书撤销列表 (CRL) 的已撤销证书列表，以确保用户的证书未被撤销。您需要在服务器上保留此列表的最新版本，思科安全邮件和 Web 管理器将按您创建的计划下载该列表。您也可以手动更新列表。

相关主题

- 使用 GUI 来配置 CRL 源， 第 115 页
- 配置 CRL 源的全局设置， 第 116 页
- 使用 CLI 来配置 CRL 源， 第 117 页

使用 GUI 来配置 CRL 源

您可以将 CRL 源配置为启用或禁用检查已撤销证书的列表。您可以添加、更新和删除 CRL 源。

要配置 CRL 源，请执行以下步骤：

步骤 1 点击**网络 (Network)** > **CRL 源 (CRL Sources)**。

步骤 2 点击**添加 CRL 源 (Add CRL Source)** 以添加新的 CRL 源。

系统将显示**添加 CRL（证书吊销列表）源 (Add CRL [Certificate Revocation Lists] Source)** 窗口。

步骤 3 输入下表中描述的所需参数，在思科安全邮件和 Web 管理器上添加 CRL 源。

参数	说明
CRL 文件名	输入 CRL 源文件的名称。

参数	说明
CRL 文件类型	输入 CRL 源文件的类型。您可以选择 ASN.1（抽象语法表示法 1）或 PEM（隐私增强邮件）CRL 文件类型。
从中下载 CRL 文件的主源 URL	输入 URL 作为文件的主要源，包括文件名。 例如 https://crl.example.com/certs.crl
当主源不可用时使用的辅助源 URL（可选）	输入 URL 作为文件的辅助源，包括文件名。此字段为选填字段。
启用计划的 CRL 文件自动更新	输入下载 CRL 源文件的计划。 选择**启用 CRL 文件的计划自动更新 (Enable Scheduled auto update of CRL file)** 以启用计划的自动更新。您可以选择“每日”(Daily)、“每周”(Weekly) 或“每月”(Monthly) 选项，并指定必须进行下载的时间（24 小时制）。
测试源	点击**测试 CRL 源 (Test CRL Source)** 以测试 CRL 源文件是否更新成功。 **注释** 未在数据库中下载 CRL 源文件。点击此按钮时，它会测试 CRL 源文件是否已成功更新。

步骤 4 提交并确认更改。

下一步做什么

您可以更新和删除 CRL 源。

- 选择 CRL 源，然后点击**更新 (Update)** 以手动更新 CRL 源。
- 选择CRL 源，然后点击**删除图标**以删除 CRL 源。点击**清除所有 CRL 源 (Clear All CRL Sources)** 以删除所有 CRL 源。

配置 CRL 源的全局设置

您可以为 CRL 源配置全局设置，从而启用或禁用以下连接的 CRL 检查：

- 入站 SMTP TLS
- 出站 SMT TLS
- 网络界面

要为 CRL 源配置全局设置，请执行以下步骤：

步骤 1 点击**网络 (Network)** > **CRL 源 (CRL Sources)**。

步骤 2 在**CRL 源 (CRL Sources)** 窗口的 **CRL 源的全局设置 (Global Settings for CRL Sources)** 部分中点击**编辑设置 (Edit Settings)**。

步骤 3 选中或取消选中以下复选框以启用或禁用提供的选项：

- **对入站 SMTP TLS 进行 CRL 检查**
- **对出站 SMTP TLS 进行 CRL 检查**
- **对 Web 界面进行 CRL 检查**

选中**全局设置 (Global Settings)** 复选框以启用所有选项。

步骤 4 提交并确认更改。

使用 CLI 来配置 CRL 源

您可以使用 `certconfig > CRL` 子命令通过使用 CLI 来配置 CRL 源。

在执行命令时，您可以执行下表中提到的操作：

子命令	目的
新	添加新的 CRL 源。
EDIT	修改现有 CRL 源。
DELETE	删除 CRL 源。
PRINT	显示所有 CRL 源。
更新	手动更新 CRL 源。
SETUP	配置CRL源的全局设置。您可以为以下连接启用或禁用 CRL 检查： • 入站 SMTP TLS • 出站 SMT TLS • 网络界面

示例 1：

您可以使用 `SETUP` 子命令来为 Web 界面启用 CRL 检查，如下例所示：

```
 mail3.example.com> certconfig

Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> CRL
```

```
Certificate Revocation List Summary
Inbound SMTP TLS: Disabled
Outbound SMTP TLS: Disabled
Web Interface: Disabled

There are currently 1 CRL sources configured.

Choose the operation you want to perform:
- NEW - Create a new CRL source
- EDIT - Modify a CRL source
- DELETE - Remove a CRL source
- PRINT - Display all CRL sources
- UPDATE - Manually update a CRL file
- SETUP - Change global settings
[]> setup

Do you want to enable CRL check for inbound SMTP TLS? [N]> n

Do you want to enable CRL check for outbound SMTP TLS? [N]> n

Do you want to enable CRL check for Web Interface? [N]> y

Certificate Revocation List Summary
Inbound SMTP TLS: Disabled
Outbound SMTP TLS: Disabled
Web Interface: Enabled

There are currently 1 CRL sources configured.
```

示例 2：

您可以使用 `PRINT` 子命令来显示所有 CRL 源，如下例所示：

```
mail3.example.com> certconfig

Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> CRL

Certificate Revocation List Summary
Inbound SMTP TLS: Disabled
Outbound SMTP TLS: Disabled
Web Interface: Disabled
There are currently 1 CRL sources configured.

Choose the operation you want to perform:
- NEW - Create a new CRL source
- EDIT - Modify a CRL source
- DELETE - Remove a CRL source
- PRINT - Display all CRL sources
- UPDATE - Manually update a CRL file
- SETUP - Change global settings

[]> PRINT
Currently configured CRL sources (disabled sources are marked with *):
1. crl16:  http://crl.example.com/certs.crl.pem
Certificate Revocation List Summary
Inbound SMTP TLS: Disabled
Outbound SMTP TLS: Disabled
Web Interface: Disabled
There are currently 1 CRL sources configured.
Choose the operation you want to perform:
```

```
- NEW - Create a new CRL source
- EDIT - Modify a CRL source
- DELETE - Remove a CRL source
- PRINT - Display all CRL sources
- UPDATE - Manually update a CRL file
- SETUP - Change global settings
```

接收和传送包含国际化域名 (IDN) 的邮件

思科安全邮件和 Web 管理器可以接收和传送邮件地址包含 IDN 域的邮件。

目前，您的邮件网关仅支持以下语言的 IDN 域：

印度语区域语言：印地语、泰米尔语、泰卢固语、卡纳达语、马拉提语、旁遮普语、马拉雅拉姆语、班加利语、古吉拉特语、乌尔都语、阿萨姆语、尼泊尔语、班加拉语、博多语、道格里语、克什米利语、孔卡尼语、迈提利语、马尼普利语、奥里亚语、梵语、圣达里语、信德语和图鲁语。

欧洲和亚洲语言：法语、俄语、日语、德语、乌克兰语、韩语、西班牙语、意大利语、中文、荷兰语、泰语、阿拉伯语和哈萨克语。

相关主题

- 前提条件 IDN，第 119 页
- 可在思科安全电子邮件和 Web 管理器中使用 IDN 域进行配置的功能，第 119 页

前提条件 IDN

在使用国际化域名 (IDN) 功能之前，请确保满足以下前提条件：

- 所有传入邮件都必须使用 UTF-8 编码的 IDN。

  例如：向邮件网关发送邮件的 MTA 必须支持 IDN，并要确保邮件中的域采用 UTF-8 格式。

- 所有传出邮件都必须使用 UTF-8 编码的 IDN，并且目标服务器必须相应地接受和支持 IDN。

  例如：接受来自邮件网关的邮件的 MTA 必须支持以 UTF-8 格式编码的 IDN 和域。

- 在所有适用的 DNS 记录中，必须使用 Punycode 格式来配置 IDN

  例如：在为 IDN 配置 MX 记录时，DNS 记录中的域必须采用 Punycode 格式。

可在思科安全电子邮件和 Web 管理器中使用 IDN 域进行配置的功能

对于此版本，您只能在思科安全邮件和 Web 管理器中使用 IDN 域来配置以下功能：

- **SMTP 路由配置设置：**
  - 添加或编辑 IDN 域。
  - 使用 IDN 域导出或导入 SMTP 路由。

- **DNS 配置设置**：使用 IDN 域添加或编辑 DNS 服务器。
- **报告配置设置**：查看报告中的 IDN 数据（用户名、邮件地址和域）。
- **邮件跟踪配置设置**：查看邮件跟踪中的 IDN 数据（用户名、邮件地址和域）。
- **策略、病毒和爆发隔离区配置设置**：
  - 查看可能正在传输恶意软件（由防病毒引擎确定）且包含 IDN 域的邮件。
  - 查看可能作为垃圾邮件或恶意软件由爆发过滤器捕获到且包含 IDN 域的邮件。
  - 查看被邮件过滤器、内容过滤器和 DLP 邮件操作拦截且包含 IDN 域的邮件。
- **垃圾邮件隔离区配置设置**：
  - 查看被检测为垃圾邮件或可疑垃圾邮件且包含 IDN 域的邮件。
  - 将包含 IDN 域的邮件地址添加到安全列表和阻止列表类别。
- **最终用户隔离** - 身份验证模式为 NONE 时支持 IDN。此阶段不支持其他身份验证模式。

FQDN

完全限定域名 (FQDN) 是互联网上特定计算机或主机的完整域名。对于 X.509 证书，FQDN 验证会验证该证书的主题可分辨名称的公共名称字段 (CN) 以及类型为 dNSName (SAN:dNSName) 的 subjectAltName 扩展名。AsyncOS 会在其字段中验证域名以及公共名称和 SAN:dNSName 的证书。最好使用 SAN:dNSName 名称。有效 FQDN 的示例包括 example.com, *.example.com。

FQDN 合规标准包括：

- 证书中应存在 CN 或 SAN:dNSName，并且 AsyncOS 要求任何一个证书都要符合 FQDN。
- CN 和 SAN:dNSName 都存在于证书，并且 AsyncOS 要求两者都应符合FQDN。

变体包括：

- 对等证书验证，第 121 页
- 自定义 CA 验证，第 121 页
- 设备证书验证，第 122 页

在执行添加或导入设备证书时，思科安全邮件和 Web 管理器会在启用 FQDN 验证的情况下以及在服务器的对等证书验证期间对证书执行 FQDN 验证。所有详细的日志记录都会在思科安全邮件和 Web 管理器 system.current 或 gui.current 日志文件中进行跟踪。但是；思科安全邮件和 Web 管理器不允许导入没有通用名称 (CN) 且具有不带关键扩展名的备用主题名称的证书。

对等证书验证

AsyncOS 提供通用配置来控制 SSL 配置下的所有服务（例如 TLS）的 FQDN 验证。但 FQDN 服务必须手动启用。

- 使用 GUI 验证对等证书，第 121 页
- 使用 CLI 验证对等证书，第 121 页

使用 GUI 验证对等证书

步骤 1 前往**系统管理 (System Administration) > SSL 配置 (SSL Configuration)** 页面。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中随对等证书 FQDN 验证列出的**启用 (Enable)** 复选框。

步骤 4 点击**提交 (Submit)**。

使用 CLI 验证对等证书

您必须输入 sslconfig 命令才能对对等证书执行验证。

开始之前

prompt> sslconfig

```
Disabling SSLv3 is recommended for best security.
Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential.
 So to avoid communications errors, always select a contiguous set
of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.
Choose the operation you want to perform:
- VERSIONS - Enable or disable SSL/TLS versions
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, updater and LDAP.
```

自定义 CA 验证

在将自定义证书颁发机构导入设备时，您可以通过 AsyncOS 执行 FQDN 验证。您必须手动启用验证。

步骤 1 输入命令 CERTCONFIG > CERTAUTHORITY > CUSTOM > IMPORT

```
Enter in the command-line interface the CERTCONFIG > CERTAUTHORITY > CUSTOM > IMPORT command
```

步骤 2 输入要导入的文件的文件名。

```
Enter the name of the file on machine "appliance" to import:
[]> filename.pem
```

步骤 3 确认是否要检查 FQDN。

```
Do you want to check if Common Name is in Fully Qualified Domain Name(FQDN) format ? [N]> y
```

设备证书验证

在将设备证书导入设备时，您可以通过 AsyncOS 执行 FQDN 验证。您必须手动启用验证。

步骤 1 输入 CERTCONFIG > CERTIFICATE > SETUP 命令。

```
Prompt>  CERTCONFIG > CERTIFICATE > SETUP >
```

步骤 2 如果想要中间证书，则输入。

```
Do you want to add an intermediate certificate? [N]>
```

步骤 3 如果要检查 FQDN，则输入。

```
Do you want to check if Common Name is in Fully Qualified Domain Name(FQDN) format ? [N]> y
```

X.509 证书

X.509 是定义公钥证书格式的国际电信联盟 (ITU) 标准。X.509 证书使用数字签名将身份绑定到公钥。

X.509 合规性的标准是对等证书不得包含安全性较低的签名算法或椭圆曲线 (EC)。

在添加或导入证书时，安全邮件和 Web 管理器会对证书执行 X.509 验证。如果在服务器的对等证书验证期间启用了 X.509 验证，则安全邮件和 Web 管理器会执行对等证书的 X.509 验证。详细的日志记录会在思科安全邮件和 Web 管理器 system.current 日志文件中进行跟踪。

相关主题

- 对等证书验证，第 122 页
- 自定义 CA 证书验证，第 124 页
- 设备证书验证，第 124 页

对等证书验证

AsyncOS 提供了一种通用配置，用于在 TLS 通信期间控制 SSL 配置下的以下服务的对等证书的 X.509 验证：

- 出站 SMTP

- LDAP
- 更新程序
- TLS 警报
- 系统日志服务器
- 智能许可服务器
- 安全服务交换连接器
- 安全服务交换服务器

但是，您必须为出站 SMTP、LDAP、更新程序和基于 TLS 的警报手动启用对等证书的 X.509 验证。默认情况下，将对系统日志服务器、智能许可服务器、安全服务交换连接器和安全服务交换服务器的对等证书执行 X.509 验证。

您可以使用 Web 界面或 CLI 来配置对等证书的 X.509 验证。

相关主题

- 使用 GUI 验证对等证书，第 123 页
- 使用 CLI 验证对等证书，第 123 页

使用 GUI 验证对等证书

步骤 1 导航至**系统管理 (System Administration)** > **SSL 配置 (SSL Configuration)**。

系统将显示“SSL 配置”(SSL Configuration) 页面。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选中随**对等证书 X509 验证 (Peer Certificate X509 Validation)** 列出的**启用 (Enable)** 复选框。

步骤 4 点击**提交 (Submit)** 并确认更改。

使用 CLI 验证对等证书

您可以使用 `sslconfig` 命令来验证对等证书。

```
mail.example.com> sslconfig

Disabling SSLv3 is recommended for best security.

Note that the SSL/TLS service on remote servers may require that the selected TLS versions
 be sequential. So to avoid
communications errors, always select a contiguous set of versions for each service. For
example, do not enable TLS 1.0
and 1.2, while leaving TLS 1.1 disabled.

Choose the operation you want to perform:
- VERSIONS - Enable or disable SSL/TLS versions
```

```
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, updater
and LDAP.
- PEER_CERT_X509 - Validate peer certificate X509 compliance for Alert Over TLS, updater
and LDAP.
```

自定义 CA 证书验证

在将自定义 CA 证书导入安全邮件和 Web 管理器时，AsyncOS 不会执行 X.509 验证。

步骤 1 在 CLI 中输入 `CERTCONFIG > CERTAUTHORITY > CUSTOM > IMPORT` 命令。

```
mail.example.com> CERTCONFIG > CERTAUTHORITY > CUSTOM > IMPORT
```

步骤 2 输入要导入的文件的名称。

```
mail.example.com> Enter the name of the file on machine "appliance" to import:
[]> filename.pem
```

导入文件时不进行任何验证。

设备证书验证

在将设备证书导入思科安全邮件和 Web 管理器时，AsyncOS 会执行 X.509 验证。您必须手动启用验证。

步骤 1 在 CLI 中输入 `CERTCONFIG > CERTIFICATE > SETUP` 命令。

```
mail.example.com> CERTCONFIG > CERTIFICATE > SETUP
```

步骤 2 如果要使用证书或密钥来进行接收、传送、HTTPS 管理访问和 LDAP，请输入 **Y**。

```
Do you want to use one certificate/key for receiving, delivery, HTTPS management access, and LDAPS?
```

AsyncOS 会对导入的设备证书执行 X.509 验证。

单一平台

通过单一平台 (SPoG) 功能，您可以访问单个思科安全邮件和 Web 管理器上的思科安全邮件和 Web 管理器详细信息。您必须确保将多台思科安全邮件和 Web 管理器设备连接到主思科安全邮件和 Web 管理器设备。您可以查看主设备上的辅助思科安全邮件和 Web 管理器设备的监控、跟踪、隔离等信息。但是，要执行此操作，您必须使用主思科安全邮件和 Web 管理器的命令行界面来启用配置。

准备工作

确保所有思科安全邮件和 Web 管理器设备版本相同。

要在主要思科安全邮件和Web管理器设备中启用下拉列表并收集信息，您必须使用**smaapplianceconfig**命令。

一旦启用了配置，您就可以在主设备中查看辅助思科安全邮件和 Web 管理器的详细信息，请参阅SPoG 查看主要思科安全电子邮件和 Web 管理器的详细信息，第 130 页

注释 在启用或禁用 SPoG 时，同时登录到 NGUI 的所有用户的会话将变得无效，服务器会收到新的请求将其注销。用户必须重新登录。

此外，如果将思科安全邮件和 Web 管理器添加到 SPoG 或从 SPoG 中删除，而您当前正登录到同一思科安全邮件和 Web 管理器的 NGUI，则您将会由于 JWT 验证的变化而被注销。

注释 在所有连接的 SPoG 设置中，用户或与身份验证相关的设置都应相同。

例如，假设您尝试以外部身份验证用户的身份登录在思科安全邮件和 Web 管理器；在辅助思科安全邮件和 Web 管理器上也应进行相同的外部身份验证设置，以便从主思科安全邮件和 Web 管理器访问辅助思科安全邮件和 Web 管理器。

通过使用 **smaapplianceconfig** 命令，您可以：

- SPoG 添加思科安全邮件和 Web 管理器，第 125 页
- SPoG 编辑思科安全邮件和 Web 管理器，第 126 页
- SPoG 删除思科安全邮件和 Web 管理器，第 128 页
- 思科安全电子邮件和 Web 管理器上的 SPoG 启用服务，第 129 页
- SPoG 查看主要思科安全电子邮件和 Web 管理器的详细信息，第 130 页

SPoG 添加思科安全邮件和 Web 管理器

以下示例显示了如何添加思科安全邮件和 Web 管理器。

```
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ====== ============= ========= ======== ===========
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> ADD
Enter the IP address or hostname of an appliance to transfer data with.
(A hostname may be entered in this field, however it will be immediately
resolved to an IP address when the form is submitted.)
```

```
[]> vm21sma0062.cs21
Enter a name to identify this appliance
[]> SMA0062
File transfer access via SSH is required to transfer reporting data, message logs, and
quarantine safelist/blocklist data from appliances
Would you like to configure file transfer access for this appliance? [Y]>
Would you like to use a custom ssh port to connect to this appliance? [N]>
Enter the login credentials for an administrator or an operator account on the appliance.
This will be used to obtain an SSH key for file transfers.
Username:
[]> admin
Passphrase:
[]>
Appliance 10.10.3.62 added.
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ======= ============= ========= ======== ===========
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
3 10.10.3.62 SMA0062 Yes Disabled Disabled Disabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> added vm21sma0062.cs21
Changes committed: Tue Apr 27 10:28:01 2021 GMT
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ======= ============= ========= ======== ===========
1 10.10.3.62 SMA0062 Yes Disabled Disabled Disabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
```

SPoG 编辑思科安全邮件和 Web 管理器

以下示例显示了如何编辑辅助思科安全邮件和 Web 管理器连接参数。

```
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ======= ============= ========= ======== ===========
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
3 10.10.3.62 SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> EDIT
Enter the name or number of the appliance you wish to edit.
```

```
[]> 3
Enter the IP address or hostname of an appliance to transfer data with.
(A hostname may be entered in this field, however it will be immediately
resolved to an IP address when the form is submitted.)
[10.10.3.62]>
Enter a name to identify this appliance
[SMA0062]> Tracking_SMA0062
File transfer access via SSH is required to transfer reporting data, message logs, and
quarantine safelist/blocklist data from appliances
Would you like to configure file transfer access for this appliance? [Y]>
Would you like to use a custom ssh port to connect to this appliance? [N]>
Appliance 10.10.3.62 was edited
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ================ ============= ========= ======== ===========
1 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.62 Tracking_SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> SERVICES
Enter the name or number of the appliance you wish to configure.
[]> 1
Services for appliance "SMA63" at address 10.10.3.63:
------------------------------------------------------------------------
Email Reporting service: Disabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Would you like Email Reporting to be enabled on this appliance? [N]>
Would you like Email Tracking to be enabled on this appliance? [Y]>
Would you like Spam Quarantines to be enabled on this appliance? [Y]>
Services for appliance "SMA63" at address 10.10.3.63:
------------------------------------------------------------------------
Email Reporting service: Disabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Enter the name or number of the appliance you wish to configure.
[]>
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ================ ============= ========= ======== ===========
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
3 10.10.3.62 Tracking_SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> services
Enter the name or number of the appliance you wish to configure.
[]> 3
Services for appliance "Tracking_SMA0062" at address 10.10.3.62:
------------------------------------------------------------------------
Email Reporting service: Enabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
```

```
Would you like Email Reporting to be enabled on this appliance? [Y]> N
Would you like Email Tracking to be enabled on this appliance? [Y]>
Would you like Spam Quarantines to be enabled on this appliance? [Y]> N
Services for appliance "Tracking_SMA0062" at address 10.10.3.62:
------------------------------------------------------------------------
Email Reporting service: Disabled
Email Tracking service: Enabled
Spam Quarantines service: Disabled
Enter the name or number of the appliance you wish to configure.
[]>
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= ========== ================ ============= ========= ======== ===========
1 10.10.3.62 Tracking_SMA0062 Yes Disabled Enabled Disabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> use vm21sma0062.cs21 for tracking
Changes committed: Tue Apr 27 10:32:32 2021 GMT
```

SPoG 删除思科安全邮件和 Web 管理器

以下示例显示了如何删除思科安全邮件和 Web 管理器。

```
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= ========== ================ ============= ========= ======== ===========
1 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.62 Tracking_SMA0062 Yes Disabled Enabled Disabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> DELETE
Enter the name or number of the appliance you wish to delete.
[]> 3
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= ========== ====== ============= ========= ======== ===========
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
```

```
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> deleting Tracking_SMA0062
Changes committed: Tue Apr 27 10:37:12 2021 GMT
vm21sma0061.cs21>
```

思科安全电子邮件和 Web 管理器上的 SPoG 启用服务

以下示例显示了如何在思科安全邮件和 Web 管理器上启用服务。

```
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ======= ============= ========= ======== ===========
1 10.10.3.62 SMA0062 Yes Disabled Disabled Disabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> SERVICES
Enter the name or number of the appliance you wish to configure.
[]> 1
Services for appliance "SMA0062" at address 10.10.3.62:
-------------------------------------------------------------------------
Email Reporting service: Disabled
Email Tracking service: Disabled
Spam Quarantines service: Disabled
Would you like Email Reporting to be enabled on this appliance? [N]> Y
Would you like Email Tracking to be enabled on this appliance? [N]> Y
Would you like Spam Quarantines to be enabled on this appliance? [N]> Y
Services for appliance "SMA0062" at address 10.10.3.62:
-------------------------------------------------------------------------
Email Reporting service: Enabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Enter the name or number of the appliance you wish to configure.
[]>
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =========== ======= ============= ========= ======== ===========
1 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.62 SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> anabled services on vm21sma0062.cs21
Changes committed: Tue Apr 27 10:29:17 2021 GMT
vm21sma0061.cs21>
```

SPoG 查看主要思科安全电子邮件和 Web 管理器的详细信息

要查看辅助设备的详细信息，则必须：

- 导航至主要思科安全邮件和 Web 管理器设备的隔离区页面。
- 从**查看 SMA (View SMA)** 下拉列表中选择辅助思科安全邮件和 Web 管理器。

现在，您可以在主设备上查看与所选辅助思科安全邮件和 Web 管理器对应的数据。

在使用 **smaapplianceconfig** 命令中的 **services** 子命令启用后，您也可以在“跟踪”(Tracking) 和“监控”(Monitoring) 页面中查看相同内容。

当地语言翻译版本说明

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