系统管理

本章包含以下部分：

注释 本部分介绍的一些功能或命令将会影响路由优先顺序或者会受路由优先顺序的影响。有关详细信息，请参阅附录 *B* “*IP* 地址接口和路由”。

• 接收和传送包含国际化域名 (IDN) 的邮件 ， 第 83 页

邮件网关的管理

以下任务可让您轻松管理邮件网关中的常用功能。

• 关闭或重新引导邮件网关 , on page 2
• 暂停邮件接收和传送 , on page 2
• 恢复暂停的邮件的接收和传送 , on page 3

关闭或重新引导邮件网关

在关闭或重新引导邮件网关后，可以稍后重新启动设备，而不会丢失传送队列中的任何邮件。

可以在 CLI 中使用 shutdown 或 reboot 命令，也可以使用 Web 界面：

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **关闭/暂停 (Shutdown/Suspend)**。

步骤 2 在**系统操作 (System Operations)** 部分，从**操作 (Operation)** 下拉列表中选择 **关闭 (Shutdown)** 或**重新引导 (Reboot)**。

步骤 3 输入等待的秒数，以允许打开的连接在被强制关闭之前完成。

默认延迟为三十 (30) 秒。

步骤 4 单击**确认 (Commit)**。

暂停邮件接收和传送

AsyncOS 允许您暂停邮件的接收和传送。您可以暂停：

- 接收某特定侦听程序或多个侦听程序上的邮件。
- 传送所有邮件或发送到某特定域或多个域的邮件。

使用 CLI 中的 suspend 命令或使用 Web 界面：

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **关闭/暂停 (Shutdown/Suspend)**。

步骤 2 暂停接收某特定侦听程序或多个侦听程序上的邮件。

在**邮件操作 (Mail Operations)** 部分，选择要暂停的功能和/或侦听程序。如果邮件网关有多个侦听程序，可以暂停各个侦听程序上的邮件接收。

步骤 3 暂停传送所有邮件或发送至某特定域或多个域的邮件。根据您的要求，执行以下操作之一：

a. 要暂停所有邮件的传送，请在**指定域/子域 (Specify Domain(s)/Subdomain(s))** 字段中，输入 All，然后按 **Enter**。

b. 要暂停传送至特定域或子域的邮件，请在**指定域/子域 (Specify Domain(s)/Subdomain(s))** 字段中，输入域或子域名称或 IP 地址，然后按 **Enter**。使用逗号分隔文本添加多个条目。

步骤 4 输入等待的秒数，以允许打开的连接在被强制关闭之前完成。

如果没有打开的连接，系统将立即变为离线状态。

默认延迟为 30 秒。

步骤 5 单击**确认 (Commit)**。

What to do next

当您准备恢复暂停的服务时，请参阅恢复暂停的邮件的接收和传送 , on page 3。

恢复暂停的邮件的接收和传送

使用“关闭/暂停”页面或 resume 命令恢复暂停的邮件的接收和传送。

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **关闭/暂停 (Shutdown/Suspend)**。

步骤 2 在**邮件操作 (Mail Operations)** 部分，选择要恢复的功能和/或侦听程序。

如果邮件网关有多个侦听程序，可以恢复各个侦听程序上的邮件接收。

步骤 3 恢复传送所有邮件或发送至某特定域或多个域的邮件。

在**指定域/子域 (Specify Domain(s)/Subdomain(s))** 字段中，单击目标条目上的关闭图标。

步骤 4 单击**确认 (Commit)**。

重置为出厂默认设置

Caution 如果您无法使用串行接口或管理接口上的默认设置通过默认的 Admin 用户账户重新连接到 Web 界面或 CLI，则请勿重置为出厂默认设置。

当对邮件网关进行物理传输时，您可能希望从出厂默认值开始。重置为出厂设置是极其具有破坏性的，仅当传输装备或最近重新进行了排序以解决配置问题时才重置为出厂设置。重置为出厂默认设

置会断开您与 Web 界面或 CLI 的连接，从而禁用您用来连接至邮件网关（FTP、SSH、HTTP、HTTPS）的服务，甚至会删除您已创建的其他用户账号。您可以通过如下方式重置为出厂默认设置：

- 在 Web 界面上，单击**系统管理 (System Administration) > 配置文件 (Configuration File)** 页面上的“重置”按钮，或单击**系统管理 (System Administration) > 系统设置向导 (System Setup Wizard)** 中的“重置配置”(Reset Configuration) 按钮。
- 在 CLI 上，使用 **resetconfig** 命令。

Note 仅当邮件网关处于离线状态时，**resetconfig** 命令才有效。重置为出厂设置后，邮件网关将恢复在线状态。

后续步骤

- 运行“系统设置向导”(System Setup Wizard)。有关详细信息，请参阅使用系统设置向导
- 打开邮件传送以恢复邮件传送。

显示 AsyncOS 的版本信息

要确定邮件网关上当前安装的 AsyncOS 版本，请使用 Web 界面上“监控”(Monitor) 菜单上的“系统概述”(System Overview) 页面（请参阅系统状态），或使用 CLI 中的 version 命令。

邮件网关许可

功能密钥

添加和管理功能密钥

对于物理邮件网关，功能密钥既特定于邮件网关的序列号，又特定于要启用的功能（您不能在一个系统上重用另一个系统的密钥）。

要在 CLI 中使用功能密钥，请使用 **featurekey** 命令。

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **功能密钥 (Feature Keys)**。

步骤 2 执行操作：

收件人	相应操作
查看活动功能密钥的状态	查看 **<序列号> 的功能密钥 (Feature Keys for <serial number>)** 部分。
查看已为邮件网关签发但又尚未激活的功能密钥	查看**待处理激活 (Pending Activation)** 部分。 如果您启用了自动下载和激活，则功能密钥不会出现在此列表中。
检查最近签发的功能密钥	单击“待处理激活”(Pending Activation) 部分的**检查新密钥 (Check for New Keys)** 按钮。 如果您尚未启用功能密钥的自动下载和激活，或者需要在下一次自动检查之前下载功能密钥，则此按钮很有用。
激活签发的功能密钥	在**待处理激活 (Pending Activation)** 列表中选择该密钥，并单击**激活选定的密钥 (Activate Selected Keys)**。
添加新功能密钥	使用**功能激活 (Feature Activation)** 部分。

What to do next

相关主题

- 自动执行功能密钥下载和激活 , on page 5
- “配置文件”(Configuration File) 页, on page 18

自动执行功能密钥下载和激活

您可以将邮件网关设置为自动检查、下载和激活为此邮件网关签发的功能密钥。

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **功能密钥设置 (Feature Keys Settings)**。

步骤 2 单击**编辑功能密钥设置 (Edit Feature Key Settings)**。

步骤 3 要查看新功能密钥的检查频率，请单击 (?) 帮助按键。

步骤 4 指定设置。

步骤 5 提交并确认更改。

What to do next

相关主题

- 添加和管理功能密钥 , on page 4

过期的功能密钥

如果功能密钥将要到期，邮件网关会在密钥到期之前的 90 天、60 天、30 天、15 天、5 天、1 天以及在密钥到期时发出警报。要接收这些警报，请确保您已订用系统警报。有关详细信息，请参阅警报, on page 39。

如果您尝试访问（通过 Web 界面）的功能的功能密钥已过期，请与您的思科代表或支持组织联系。

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邮件网关许可证。要激活智能软件许可，必须向思科智能软件管理器 (CSSM) 注册邮件网关。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。

注册邮件网关后，即可通过 CSSM 门户跟踪邮件网关许可证并监控许可证使用情况。邮件网关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。

请参阅https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html以了解思科智能软件管理器。

开始之前

- 请确保您的邮件网关具有互联网连接。
- 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。

- 邮件网关的系统时钟必须与 CSSM 的系统时钟同步。邮件网关系统时钟与 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**安全服务 (Security Services) -> 服务更新 (Service updates)** 为邮件网关配置的相同代理

注释 对于虚拟用户，每次收到新的 PAK 文件（新的或续约）时，生成许可证文件并将文件加载到邮件网关上。加载文件后，必须将 PAK 转换为智能许可。在智能许可模式下，加载文件时将忽略许可证文件中的功能密钥部分，并且只会使用证书信息。

注释 如果您已有思科 SecureX 帐户，请确保在邮件网关上启用智能许可模式之前先向思科 SecureX 注册您的邮件网关。

您必须执行以下程序，才能为邮件网关激活智能软件许可：

	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 8 页
第 2 步	向思科智能软件管理器注册邮件网关	向思科智能软件管理器注册邮件网关，第 8 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

过程

步骤 1 选择**系统管理 (System Administration) > 智能软件许可 (Smart Software Licensing)**。

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

要了解智能软件许可，单击“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，单击**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 注册邮件网关。

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 注册邮件网关。

注释 在传统许可模式下没有有效许可证的新虚拟邮件网关户没有评估期，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邮件网关用户才有评估期。如果新虚拟邮件网关用户希望评估智能许可功能，请联系思科销售团队，向智能帐户添加评估许可证。注册后，评估许可证可用于评估目的。

注释 在邮件网关上启用“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邮件网关

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

过程

步骤 1 选择**系统管理 (System Administration) > 智能软件许可 (Smart Software Licensing)**。

步骤 2 如果想要更改**传输设置 (Transport Settings)**，请单击**编辑 (Edit)**。可用选项包括：

- 直接：通过 HTTPS 直接将邮件网关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邮件网关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，然后单击“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”页面，然后访问“常规”选项卡，以生成新令牌。复制邮件网关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 3 切换回邮件网关，粘贴产品实例注册令牌。

步骤 4 单击**注册 (Register)**。

步骤 5 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，重新注册邮件网关。请参阅向智能思科软件管理器注册邮件网关 ，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”页面上查看注册状态。

注释 在启用了智能软件许可并向思科智能软件管理器注册邮件网关后，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。

申请许可证

成功完成注册过程后，必须按需申请邮件网关功能许可证。

过程

步骤 1 选择**系统管理 (System Administration) > 许可证 (Licenses)**。

步骤 2 单击**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 单击**提交 (Submit)**。

注释 默认情况下，已提供邮件处理和思科安全邮件网关退回验证的许可证。您不能激活、停用或发放这些许可证。

没有任何评估期或不合规状态的邮件处理和思科安全邮件网关退回验证的许可证。这不适用于虚拟邮件网关。

下一步做什么

当许可证过量使用或已到期时，它们将转为违规 (OOC) 模式，并且每个许可证可获得 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。

从思科智能软件管理器注销邮件网关

过程

步骤 1 选择**系统管理 (System Administration) > 智能软件许可 (Smart Software Licensing)**。

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

步骤 3 单击**提交 (Submit)**。

向智能思科软件管理器注册邮件网关

过程

步骤 1 选择**系统管理 (System Administration) > 智能软件许可 (Smart Software Licensing)**。

步骤 2 从**操作 (Action)** 下拉列表中选择**重新注册 (Reregister)**，然后单击**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邮件网关，第 8 页。

在不可避免的场景下，重置邮件网关配置后，您可以重新注册邮件网关。

更改传输设置

只能在向 CSSM 注册邮件网关之前更改传输设置。

注释 仅当已启用智能许可功能时，才可更改传输设置。如果已注册邮件网关，则必须取消注册邮件网关，才能更改传输设置。更改传输设置后，必须再次注册邮件网关。

请参阅向思科智能软件管理器注册邮件网关了解如何更改传输设置。

续约授权和证书

向思科智能软件管理器注册邮件网关后，您可以续订证书。

注释 只能在成功注册邮件网关后续约授权。

过程

步骤 1 选择**系统管理 (System Administration) > 智能软件许可 (Smart Software Licensing)**。

步骤 2 从**操作**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 单击**前往 (Go)**。

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

更新智能代理

要更新邮件网关上安装的智能代理版本，请执行以下步骤：

过程

步骤 1 选择**系统管理 (System Administration) > 智能软件许可 (Smart Software Licensing)**。

步骤 2 在**智能代理更新状态 (Smart Agent Update Status)** 部分，单击**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。

群集模式下的智能许可

在集群配置中，您可以启用智能软件许可，并使用思科智能软件管理器同时注册所有计算机。

操作过程：

1. 在已登录邮件网关上从集群模式切换到计算机模式。
2. 前往**系统管理 (System Administration) > 智能软件许可 (Smart Software Licensing)** 页面。
3. 单击**启用 (Enable)**。
4. 选中**在集群中的所有计算机上启用智能软件许可 (Enable Smart Software Licensing on all machines in the cluster)** 复选框。
5. 单击**确定 (OK)**。
6. 选中**在集群中的计算机之间注册智能软件许可 (Register Smart Software Licensing across machines in cluster)** 复选框。
7. 单击**注册 (Register)**。

注释 您可以在 CLI 中使用 `license_smart` 命令启用智能软件许可，并同时向思科智能软件管理器注册所有计算机。

注释 在集群配置中，您还可以启用智能软件许可，并向思科智能软件管理器单独注册所有计算机。在智能许可集群模式下，您可以登录任何邮件网关并配置智能许可功能。您可以登录邮件网关并逐个访问集群中的其他邮件网关，且配置智能许可功能，而无需从第一个邮件网关注销。

有关详细信息，请参阅使用集群进行集中管理。

虚拟邮件网关许可证

要设置和许可虚拟邮件网关，请参阅思科内容安全虚拟设备安装指南。本文档可从中指定的位置获得。

Note 安装虚拟邮件网关许可证之前，无法打开技术支持隧道或运行系统设置向导。

虚拟邮件网关许可证到期

虚拟邮件网关许可证到期之后，邮件网关将会继续传送邮件，但不会获得 180 天的安全服务。在此期间，不会进行安全服务更新。

许可证到期之前的 180 天、150 天、120 天、90 天、60 天、30 天、15 天、5 天、1 天和 0 秒将会发出警报，并且在宽限期结束之前会按照相同的间隔发出警报。这些警报属于“系统”(System)类型，严重性级别为“严重”(Critical)。要确保收到这些警报，请参阅添加警报收件人, on page 41。

这些警报也会记录在系统日志中。

各个功能密钥可能会先于虚拟邮件网关许可证到期。当这些密钥接近其到期日期时，您也会收到警报。

相关主题

- 在虚拟邮件网关上恢复 AsyncOS 可能会影响许可证 , on page 36

管理配置文件

邮件网关中的所有配置设置均可通过当个配置文件管理。该文件以 XML（可扩展标记语言）格式维护。

可以通过多种方式使用此文件：

- 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。如果您在配置邮件网关时出现错误，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，以快速查看邮件网关的所有配置。（许多较新的浏览器具有直接显示 XML 文件的功能。）这可以帮助你对当前配置中可能存在的小错误（如印刷错误）进行故障排除。
- 您可以下载现有配置文件，对其进行更改，并将其上传到同一邮件网关。这实际上是“绕过”CLI 和 Web 界面更改配置。
- 可以通过 FTP 访问上传整个配置文件，也可以将整个配置文件的一部分直接粘贴到 CLI 中。
- 由于文件是 XML 格式，所以还会提供描述配置文件中所有 XML 实体的相关 DTD（文档类型定义）。可以下载 DTD 先验证 XML 配置文件，再进行上传。（XML 验证工具可从 Internet 中获取。）

使用 XML 配置文件管理多个邮件网关

- 可以从一个邮件网关下载现有的配置文件，对其更改，再将其上传到另一个邮件网关。这样，您可以更轻松地管理多个邮件网关的安装。目前，您尚不能将配置文件从 C/X 系列邮件网关加载到 M 系列思科安全管理器邮件和网络网关。
- 您可以将从一个邮件网关下载的现有配置文件分成多个子部分。可以修改所有邮件网关间通用的部分（在多邮件网关环境中）并在更新子部分时将其加载到其他邮件网关。

例如，可以在测试环境中使用邮件网关来测试“全局取消订用”(Global Unsubscribe) 命令。如果您认为已经正确配置了“全局取消订用”(Global Unsubscribe) 列表，则可以将“全局取消订用”(Global Unsubscribe) 配置部分从测试邮件网关加载到所有生产邮件网关。

管理配置文件

要在您的在邮件网关上管理配置文件，请依次单击“系统管理”(System Administration) > “配置文件”(Configuration File)。

“配置文件”(Configuration File) 页面包含以下部分：

- **当前配置 (Current Configuration)** - 用于保存和导出当前配置文件。
- **加载配置 (Load Configuration)** - 用于加载完整或部分配置文件。
- **最终用户安全列表/阻止列表数据库(垃圾邮件隔离区)** - 有关信息，请参阅使用安全列表和阻止列表基于发件人控制邮件发送和备份和恢复安全列表/阻止列表。
- **重置配置 (Reset Configuration)** - 用于将当前配置重置回出厂默认设置（应在重置配置之前先保存配置）。

Note 具有加密密码的配置文件以未加密的 PEM 格式随附私钥和证书。

相关主题

- 保存和导出当前的配置文件, on page 15
- 加载配置文件, on page 15

- 通过邮件发送配置文件, on page 15
- 重置当前的配置, on page 18

保存和导出当前的配置文件

使用**系统管理 (System Administration) > 配置文件 (Configuration File)** 页面的**当前配置 (Current Configuration)** 部分，可以将当前配置保存到您的本地计算机，或是保存到邮件网关上（位于FTP/SCP根目录下的 configuration 目录中），也可以通过邮件将其发送至指定的地址。

以下信息不随配置文件一起保存：

- 与 URL 过滤功能使用的服务进行安全通信所用的证书。
- “联系技术支持”(Contact Technical Support) 页面上保存的 CCO 用户 ID 和合同 ID。

可以通过选中**屏蔽配置文件中的密码**复选框来屏蔽用户的密码。屏蔽密码会使初始加密的密码在导出或保存的文件中替换为“*****”。但请注意，无法将包含屏蔽密码的配置文件重新加载到AsyncOS。

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
- DK/DKIM 签名密钥
- 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。

通过邮件发送配置文件

使用“系统管理”>“配置文件”中的“通过邮件将文件发送至”字段或使用 mailconfig 命令通过邮件将当前配置文件以附件形式发送给用户。

加载配置文件

使用**系统管理 (System Administration) > 配置文件 (Configuration File)** 页面的“加载配置”(Load Configuration) 部分将新配置信息加载到邮件网关中. 可以使用 `loadconfig` 命令在命令行界面中配置此参数。

可以使用以下三种方法之一加载信息：

- 将信息放在 configuration 目录，然后上传。
- 直接从本地计算机上传配置文件。
- 直接粘贴配置信息。

Note 无法加载包含屏蔽密码的配置文件。

在集群模式下，可以选择加载集群或邮件网关的配置。有关加载集群配置的说明，请参阅在集群邮件网关中加载配置。

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。对照邮件网关上 configuration 目录中的 DTD（文档类型定义）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先在邮件网关之外验证配置文件，再上传它们。

使用任何导入方法，均可导入整个配置文件（最高级别标记之间定义的信息：<config></config>）或配置文件的完整和唯一子部分，只要其中包含声明标记（如上），并括在<config></config>标记中即可。

“完整”表示 DTD 定义的特定小节的完整开始和结束标记都包括在内。例如，上传或粘贴如下内容：

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

<autosupport_enabled>0</autosu

</config>
```

将会在上传时引发验证错误。但使用如下内容：

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">
```

```
<config>
<autosupport_enabled>0</autosupport_enabled>
</config>
```

则不会出现此问题。

“唯一”表示要上传或粘贴的配置文件的子部分对于该配置非常明确。例如，系统可能只有一个主机名，所以允许上传以下代码（包括声明和 `<config></config>` 标记）：

```
<hostname>mail4.example.com</hostname>
```

。但是，系统可能定义了多个侦听程序，并为每个侦听程序定义了不同的收件人访问表，所以仅上传以下代码：

```
<rat>
       <rat_entry>
              <rat_address>ALL</rat_address>
         <access>RELAY</access>
     </rat_entry>
</rat>
```

会被视为不明确，所以不允许上传，即使是“完整”语法亦不例外。

Caution 上传或粘贴配置文件或配置文件的子部分时，可能会清除待处理的未确认更改。

如果配置文件分配的磁盘空间量小于邮件网关上当前存储的数据量，则时间最长的数据将被删除，以满足配置文件中指定的配额。

空标记与忽略的标记

上传或粘贴一部分配置文件时，请务必小心。如果不包含标记，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，上传如下内容：

```
<listeners></listeners>
```

将会从系统中移除所有侦听程序！

Caution 上传或粘贴配置文件的子部分时，可能会从 Web 界面或 CLI 断开自己并损坏大量配置数据。如果无法使用其他协议、串行接口或管理端口上的默认设置重新连接到邮件网关，请勿使用此命令禁用服务。此外，如果不确定 DTD 定义的确切配置语法，请勿使用此命令。务必先备份配置数据，再加载新的配置文件。

关于加载日志订用密码的注意事项

如果尝试加载的配置文件包含需要密码的日志订用（例如，将使用FTP推送的日志订用），loadconfig命令不会警告您缺少密码。FTP 推送失败，系统将生成警报，直到使用 logconfig 命令配置正确的密码。

关于字符集编码的注意事项

XML 配置文件的“编码”属性必须是“`ISO-8859-1`”，无论您使用哪种字符集离线操作文件。请注意，只要发出 `showconfig`、`saveconfig` 或 `mailconfig` 命令，都需要在文件中指定编码属性：

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

目前，只能加载此编码的配置文件。

相关主题

- 在集群邮件网关中加载配置

重置当前的配置

重置当前配置会使您的邮件网关恢复到原始出厂默认设置。在重置之前，请保存您的配置。集群环境中不支持通过 GUI 中的词按钮重置配置。

请参阅重置为出厂默认设置, on page 3。

查看配置文件

您只能使用 `showconfig` 命令查看配置文件详细信息。`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: IronPort 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.]
```

“配置文件”(Configuration File) 页

- 管理配置文件, on page 13
- 重置为出厂默认设置, on page 3

管理磁盘空间

（仅限虚拟邮件网关）增加可用磁盘空间

对于运行 ESXi 5.5 和 VMFS 5 的虚拟邮件网关，您可以分配 2TB 以上的磁盘空间。对于运行 ESXi 5.1 的邮件网关，限制为 2 TB。

要增加虚拟邮件网关实例的磁盘空间，请执行以下步骤：

Note 不支持减少磁盘空间。请参阅 VMWare 文档中的相关信息。

准备工作

仔细确定所需的磁盘空间。

Procedure

步骤 1 减少邮件网关实例。

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。发布时，可在以下位置获取 ESXi 5.5 的此信息：http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html。

步骤 3 依次转至**系统管理 (System Administration) > 磁盘管理 (Disk Management)**，并确认所做的更改是否已生效。

查看和分配磁盘空间使用情况

您可以通过在邮件网关上您的部署所用的功能之间分配磁盘空间来优化磁盘的使用。

收件人	相应操作
• 查看磁盘空间配额和每项服务的当前使用情况 • 您可以随时重新分配邮件网关上的磁盘空间	依次转至**系统管理 (System Administration) > 磁盘管理 (Disk Management)**。
管理数据卷	• 为了报告和跟踪服务和垃圾邮件隔离区，时间最长的数据将自动删除。 • 对于“策略”(Policy)、“病毒”(Virus) 和“爆发”(Outbreak) 隔离区，将执行在隔离区中配置的默认操作。请参阅自动处理的隔离邮件的默认操作。 • 对于“其他”(Miscellaneous) 配额，必须手动删除数据以将使用量将至您设置的新配额以下。请参阅管理“其他”配额的磁盘空间 , on page 20。

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	依次转至**系统管理 (System Administration) > 日志订用 (Log Subscriptions)**，并且： • 查看哪些日志目录使用的磁盘空间最多。 • 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 (Help and Support)**（屏幕右上侧附近）> **数据包捕获 (Packet Capture)**。
配置文件 （这些文件不太可能占用太多磁盘空间。）	通过 FTP 转至邮件网关的 /data/pub 目录。 要配置通过 FTP 访问邮件网关，请参阅FTP、SSH 和 SCP 访问
配额大小	依次转至**系统管理 (System Administration) > 磁盘管理 (Disk Management)**。

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，请参阅警报, on page 39。

磁盘空间和集中管理

磁盘空间管理只能在计算机模式下进行，不能在组或集群模式下进行。

托管安全服务

“服务概述”页面列出以下引擎的当前服务和规则版本：

- Graymail
- McAfee
- Sophos

您可以在“服务概述”页面执行以下任务：

- 手动更新引擎。有关详细信息，请参阅手动更新引擎，第 21 页
- 回滚到引擎的上一版本。有关详细信息，请参阅 回滚到以前版本的引擎，第 22 页

自动更新列显示特定引擎的自动更新的状态。如果要启用或禁用自动更新，请转到特定引擎的**全局设置**页面。

当为特定服务引擎禁用自动更新时，您将定期收到警报。如果要更改警报间隔，请使用“安全服务”(Security Services) > “服务更新”(Service Updates) 页面中的**禁用的自动引擎更新的警报间隔 (Alert Interval for Disabled Automatic Engine Updates)** 选项。

注释 对于应用了回滚的引擎，自动更新将被禁用。

相关主题

- 手动更新引擎，第 21 页
- 回滚到以前版本的引擎，第 22 页
- 查看日志，第 22 页
- 系统警告，第 48 页

手动更新引擎

过程

步骤 1 转到**安全服务 (Security Services)** > **服务概述 (Services Overview)** 页面。

步骤 2 单击**可用更新 (Available Updates)** 列中的**更新 (Update)**，以获取服务引擎的最新服务或规则版本。

注释 只有存在特定引擎的新更新时，**更新**选项才可用。

回滚到以前版本的引擎

过程

步骤 1 转到**安全服务 (Security Services)** > **服务概述 (Services Overview)**页。

步骤 2 单击**修改版本(Modify Versions)** 列中的**更改 (Change)**。

步骤 3 选择更新所需的规则和服务版本，然后单击**应用 (Apply)**。

邮件网关会将引擎回滚到上一个版本。

注释 服务更新以包的形式包含服务版本和规则版本。

单击**应用 (Apply)**后，将自动禁用特定引擎的自动更新。要启用自动更新，请转到特定引擎的“全局设置”页面。

查看日志

有关引擎回滚和禁用自动更新的信息将发布到以下日志：

- **更新程序日志**：包含关于引擎回滚和自动更新引擎的信息。大多数信息处于信息或调试级别。

  有关详细信息，请参阅更新程序日志示例。

服务更新

以下服务需要更新以获得最高效率：

- 功能密钥
- McAfeee 防病毒定义
- PXE 引擎
- Sophos 防病毒定义
- IronPort 反垃圾邮件规则
- 病毒爆发过滤器规则
- 时区规则
- URL 类别（用于 URL 过滤功能。有关详细信息，请参阅将来的 URL 类别集变更）
- 注册客户端（用于更新与用于URL过滤功能的基于云的服务进行通信所需的证书。有关信息，请参阅关于与Talos 情报服务的连接。）

- Graymail 规则

Note DLP 引擎和内容匹配分类器的设置在**安全服务 (Security Services) > 防数据丢失 (Data Loss Prevention)** 页面上处理。有关详细信息，请参阅关于更新 DLP 引擎和内容匹配分类器。

服务更新设置用于接收更新（（DLP 更新除外）的所有服务。不能为任何单个服务（DLP 更新除外）指定特有的设置。

要设置网络和邮件网关以获取这些重要更新，请参阅设置以获取升级和更新 , on page 23。

设置以获取升级和更新

分配升级和更新的选项

将 AsyncOS 升级和更新文件分配至您的邮件网关的方式有如下几种：

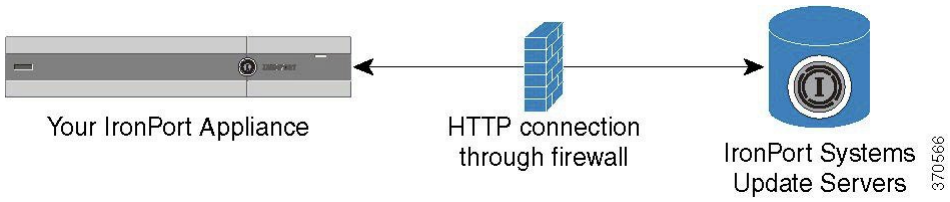
- 每台邮件网关都可直接从思科更新服务器下载文件。此为默认方法。
- 您可以从思科下载一次文件，然后从网络中的服务器将其分配到邮件网关。请参阅从本地服务器升级和更新, on page 24。

要选择和配置某种方法，请参阅配置服务器设置以下载升级和更新 , on page 27。

将您的网络配置为从思科服务器下载升级和更新

邮件网关直接连接到思科更新服务器，以查找并下载升级和更新：

Figure 1: 数据流更新方法



思科更新服务器使用动态 IP 地址。如果您有很强的防火墙策略，可能需要改为配置静态位置。有关详细信息，请参阅配置邮件网关以在严格的防火墙环境中获取升级和更新, on page 24。

创建一个防火墙规则以允许从端口 80 和 443 的思科更新服务器下载升级。

配置邮件网关以在严格的防火墙环境中获取升级和更新

思科 IronPort 升级和更新服务器使用动态 IP 地址。如果您有很强的防火墙策略，可能需要为更新和 AsyncOS 升级配置静态位置。

Procedure

步骤 1 请与思科客户支持联系，获取静态 URL 地址。

步骤 2 创建一个防火墙规则以允许从端口 80 的静态 IP 地址下载升级和更新。

步骤 3 依次选择**安全服务 (Security Services) > 服务更新 (Service Updates)**。

步骤 4 单击**编辑更新设置 (Edit Update Settings)**。

步骤 5 在“编辑更新设置”页面的“更新服务器(映像)”部分，选择“本地更新服务器”并在“基本URL”字段中输入在第 1 步中收到的静态 URL，以获取 AsyncOS 升级和 McAfee 防病毒定义。

步骤 6 确认已为“更新服务器(列表)”(Update Servers (list)) 部分选中“IronPort 更新服务器”(IronPort Update Servers)。

步骤 7 提交并确认更改。

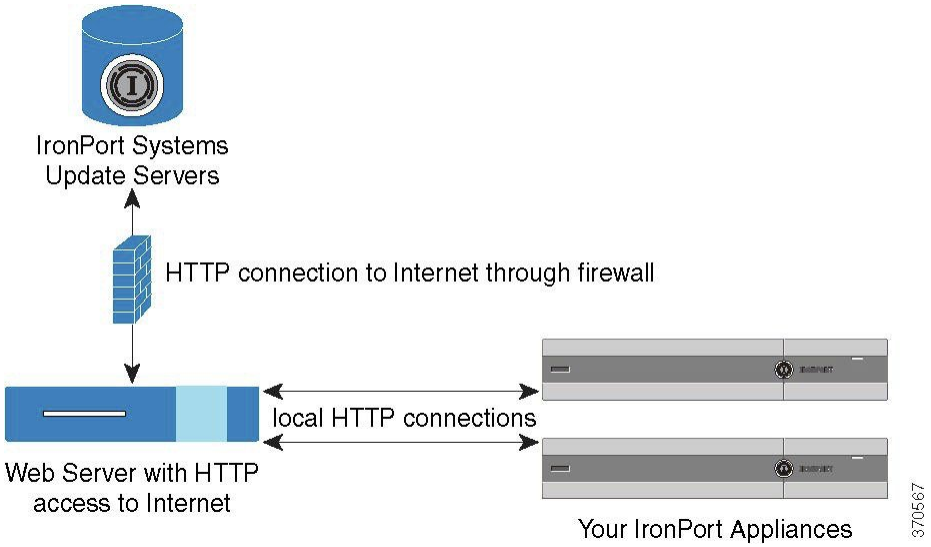
从本地服务器升级和更新

可以将 AsyncOS 升级映像下载到本地服务器并从您自己的网络内托管升级，无需直接从思科的更新服务器获得升级。使用此功能，升级映像将通过HTTP下载到网络中有权访问互联网的任何服务器。如果选择下载升级映像，即可配置内部 HTTP 服务器（“更新管理器”）将 AsyncOS 映像托管到您的设备。

如果您的邮件网关无权访问互联网，或是贵组织限制访问来镜像用于下载的站点，请使用本地服务器。将 AsyncOS 升级从本地服务器下载至每个邮件网关通常比从思科 IronPort 服务器下载速度要快。

Note 思科建议仅将本地服务器用于 AsyncOS 升级。如果为安全更新映像使用本地更新服务器，则本地服务器不会从思科 IronPort 自动接收安全更新，因此，您网络内的邮件网关无法始终拥有最新的安全服务。

Figure 2: 远程更新方法



Procedure

步骤 1 配置本地服务器，以检索和提供升级文件。

步骤 2 下载升级文件。

步骤 3 在 GUI 中使用**安全服务 (Security Services) > 服务更新 (Service Updates)**页或在 CLI 中使用 **updateconfig** 命令将设备配置为使用本地服务器。

步骤 4 使用**系统管理 (System Administration) > 系统升级 (System Upgrade)** 页面或在 CLI 中使用 upgrade 命令升级设备。

从本地服务器升级和更新的硬件和软件要求

要下载 AsyncOS 升级和更新文件，您的内部网络中必须有系统可满足以下条件：

- 对系统更新服务器的互联网访问权限。
- Web 浏览器（请参阅浏览器要求）。

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：

- Web 服务器（例如 Microsoft IIS (Internet Information Services) 或 Apache 开源服务器），该服务器应：
  - 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

在本地服务器上托管升级映像

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，请输入您的序列号（对于物理邮件网关）或 VLN（对于虚拟邮件网关设备）以及邮件网关的版本号。然后，系统将显示您可用的升级列表。单击要下载的升级版本，在本地服务器上解压根目录中的 ZIP 文件，但目录结构应保持完整。要使用升级映像，请在“编辑更新设置”页面中（或在 CLI 中使用 updateconfig）将邮件网关配置为使用本地服务器。

本地服务器还会托管 XML 文件，用于将网络中邮件网关的可用 AsyncOS 升级限制为下载的升级映像。此文件称为“清单”。证明文件位于升级映像 ZIP 文件的 asyncos 目录内。解压了本地服务器根目录中的 ZIP 文件后，在“编辑更新设置”页面中（或在 CLI 中使用 updateconfig）输入 XML 的完整 URL，包括文件名。

有关远程升级的详细信息，请参阅知识库或联系思科支持提供商。

通过代理服务器进行更新

默认情况下，邮件网关配置为直接连接到思科更新服务器接收更新。此连接通过 HTTP 在端口 80 上进行，并且内容已加密。如果不希望在防火墙中打开此端口，可以定义代理服务器以及邮件网关可以从其接收更新的规则的特定端口。

如果选择使用代理服务器，可以指定一个可选的身份验证和端口。

Note 如果定义了代理服务器，该代理服务器将自动用于配置为使用代理服务器的所有服务更新。无法为任何单个服务的更新关闭代理服务器。

配置服务器设置以下载升级和更新

指定将升级和更新下载至邮件网关所需的服务器和连接信息。

可以为 AsyncOS 升级和服务更新使用相同或不同的设置。

准备工作

确定邮件网关将直接从思科下载升级和更新，还是在网络的本地服务器中托管这些映像。然后，设置您的网络以支持所选的方式。查看设置以获取升级和更新 , on page 23下的所有主题。

Procedure

步骤 1 依次选择**安全服务 (Security Services) > 服务更新 (Service Updates)**。

步骤 2 单击**编辑更新设置 (Edit Update Settings)**。

步骤 3 输入选项：

设置	说明
更新服务器（图像）	选择要从思科 IronPort 更新服务器还是从网络的本地服务器下载思科 IronPort AsyncOS 升级映像和服务更新。默认设置为使用思科 IronPort 更新服务器下载升级和更新。 为为升级和更新使用相同设置，请在可见字段中输入信息。 如果选择本地更新服务器，请输入用于下载升级和更新的服务器的基本 URL 和端口号。如果服务器需身份验证，则也可以输入有效用户名和密码。 要单独为 AsyncOS 升级和 McAfee 防病毒定义输入单独的设置，请单击**单击以为 AsyncOS 使用不同设置 (Click to use different settings for AsyncOS)** 链接。 **Note** 智能多重扫描需要另一台本地服务器来为第三方反垃圾邮件规则下载更新。
更新服务器（列表）	为确保只有适合您的部署的升级和更新才可为每台邮件网关所用，思科 IronPort 会生成相关文件的证明列表。 选择从思科 IronPort 更新服务器还是本地网络服务器下载可用的升级和服务更新列表（证明 XML 文件）。 系统提供了独立的部分来为更新和 AsyncOS 升级指定服务器。升级和更新都默认选择从思科 IronPort 更新服务器下载。 如果选择本地更新服务器，请输入指向每个列表的证明 XML 文件的完整路径，包括文件名和服务器的 HTTP 端口号。如果将端口字段留空，AsyncOS 将使用端口 80。如果服务器需要身份验证，请输入有效的用户名和密码。

设置	说明
自动更新	为 Sophos 和 McAfee 防病毒定义、思科反垃圾邮件规则、思科智能多重扫描规则、PXE 引擎更新、病毒爆发过滤器规则和时区规则启用自动更新和升级间隔（邮件网关检查更新的频率）。 包括后缀 s、m 或 h，以表示秒、分钟或小时。输入 0（零）将禁用自动更新。 **Note** 只能使用**安全服务 (Security Services) > 防数据丢失 (Data Loss Prevention)**页面为 DLP 启用自动更新。但首先必须先为所有服务启用自动更新。有关详情，请参见关于更新 DLP 引擎和内容匹配分类器。
禁用的自动引擎更新的警报间隔	在针对特定引擎禁用“自动更新”功能时，输入要发送警报的特定频率。 包括后缀 m、h 或 d，表示月份、小时或天。默认值为 30 天。
接口	选择联系列出的安全组件更新的更新服务器时所用的网络接口。将显示可用的代理数据接口。默认情况下，邮件网关会选择一个接口使用。
HTTP 代理服务器	用于 GUI 中列出的服务的可选代理服务器。 如果指定代理服务器，则使用它来更新所有服务。
HTTPS 代理服务器	使用 HTTPS 的可选代理服务器。如果定义了 HTTPS 代理服务器，将使用它来更新 GUI 中列出的服务。

步骤 4 提交并确认更改。

配置自动更新

Procedure

步骤 1 依次导航至**安全服务 (Security Services) > 服务更新 (Service Updates)** 页面，然后单击**编辑更新设置 (Edit Update Settings)**。

步骤 2 选中该复选框以启用自动更新。

步骤 3 输入更新间隔（两次更新之间的等待时间）。为分钟添加后缀 **m**，为小时添加后缀 **h**。最大更新间隔为 1 小时。

配置邮件网关以验证更新程序服务器证书的有效性

每当邮件网关与更新程序服务器进行通信时，邮件网关均可检查思科更新程序服务器证书的有效性。如果配置了此选项并且验证失败，则不会下载更新，并在更新程序日志中记录详细信息。

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

```
mail.example.com> updateconfig
Service (images):                                   Update URL:
-------------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort 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
[]> validate_certificates
Should server certificates from Cisco update servers be validated?
[Yes]>
Service (images):                                   Update URL:
-------------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort 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
[]>
```

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。

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

```
mail.example.com> updateconfig
...
...
...
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.
[]> 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-----
MMIICiDCCAfGgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCSU4x
DDAKBgNVBAgTA0tBUjENM.........................................
-----END CERTIFICATE-----
.
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.
[]>
```

升级 AsyncOS

Procedure

	Command or Action	Purpose
步骤 1	如果尚未执行此操作，请配置适用于所有更新和升级下载的设置，并构建网络以支持和（可选）分发这些下载。	设置以获取升级和更新 , on page 23
步骤 2	了解升级何时可用并确定是否安装。	可用升级通知, on page 31
步骤 3	每次升级之前都请执行必要以及建议的任务。	升级 AsyncOS 的准备工作, on page 32 升级集群中的计算机
步骤 4	执行升级。	下载和安装升级 , on page 32

关于升级集群系统

如果您要升级集群计算机，请参阅升级集群中的计算机。

有关升级过程的批量命令

《思科邮件安全设备 *AsyncOS CLI* 参考指南》中记录了升级操作程序的批处理命令，该指南位于以下网址：http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html。

可用升级通知

默认情况下，当邮件网关有 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。

在集群化的计算机上，操作仅适用于您登录的计算机。

收件人	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	单击通知中的向下箭头。
关闭当前通知。 邮件网关在新升级可用之前不会再显示其他通知。	单击向下箭头，然后选择**清除通知 (Clear the notification)**，然后单击**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)**。

可用升级通知

默认情况下，当邮件网关有 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。

在集群化的计算机上，操作仅适用于您登录的计算机。

收件人	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	单击通知中的向下箭头。
关闭当前通知。 邮件网关在新升级可用之前不会再显示其他通知。	单击向下箭头，然后选择**清除通知 (Clear the notification)**，然后单击**关闭 (Close)**。

收件人	相应操作
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 AsyncOS 的准备工作

作为一种最佳实践，思科建议按照如下步骤做好升级准备工作。

Before you begin

清除工作队列中的所有消息。如果不清除工作队列，您将无法执行升级。

Procedure

步骤 1 机下保存 XML 配置文件。如果出于任何原因需要恢复到升级之前的版本，将需要此文件。

步骤 2 如果要使用“安全列表/阻止列表”(Safelist/Blocklist) 功能，请机下导出该列表。

步骤 3 暂停所有侦听程序。如果从 CLI 执行升级，请使用 suspendlistener 命令。如果从 GUI 执行升级，则会自动暂停监听程序。

步骤 4 等待队列清空。可以使用 workqueue 命令查看工作队列中的邮件数，或使用 CLI 中的 rate 命令监控邮件网关上的邮件吞吐量。

Note 升级后重新启用侦听程序。

下载和安装升级

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 在一次操作中从本地服务器（而不是思科 IronPort 服务器）下载并升级 AsyncOS 时，升级将在下载时即时安装。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。

准备工作

- 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。然后配置邮件网关，以从您选择的资源获取升级。请参阅设置以获取升级和更新 , on page 23和配置服务器设置以下载升级和更新 , on page 27。
- 如果要立即安装升级，请遵循升级 AsyncOS 的准备工作, on page 32中的说明操作。
- 如果要在集群化系统中安装升级，请参阅升级集群中的计算机。

- 如果只下载升级，则在准备好要安装之前无前提条件。
- 升级后，您将无法在 FIPS 模式下使用 TLS v1.0 版本。但是如有必要，您可以在邮件网关上重新启用 TLS v1.0。

Procedure

步骤 1 依次选择**系统管理 (System Administration) > 系统升级 (System Upgrade)**。

步骤 2 单击**升级选项 (Upgrade Options)**。

步骤 3 单击**升级 (Upgrade)** 继续升级流程。

步骤 4 选择一个选项：

收件人	相应操作
通过单一操作下载并安装升级	单击**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	单击**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	单击**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) 请选择是否将当前配置保存到邮件网关上的 configuration 目录中。

b) 选择是否屏蔽配置文件中的密码。

Note 无法使用 GUI 中的“配置文件”页面或 CLI 中的 loadconfig 命令加载带屏蔽密码的配置文件。

c) 如果您想通过邮件发送配置文件的副本，请输入要将该文件发送到的邮件地址。使用逗号分隔多个邮件地址。

步骤 7 单击**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，单击**立即重启 (Reboot Now)**。

c) 大约 10 分钟后，请再次访问邮件网关并登录。

如果认为需要循环设置邮件网关电源，以解决升级问题，则请在您重启后经过至少 20 分钟再执行此操作。

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。

- 如果已安装升级：
  - 重新启用（恢复）侦听程序。
  - 为新系统保存配置文件。有关信息，请参阅管理配置文件, on page 13。
- 升级完成后，请重新启用侦听程序。

查看后台下载状态、取消或删除后台下载

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **系统升级 (System Upgrade)**。

步骤 2 单击**升级选项 (Upgrade Options)**。

步骤 3 选择一个选项：

收件人	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。
取消下载	单击页面中间的**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	单击页面中间的**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。

步骤 4 （可选）查看升级日志。

启用远程电源循环

只有在 80 - 和 90 - 系列硬件上，才能远程重置邮件网关机箱的电源。

如果您希望能够远程重置邮件网关电源，必须事先按照本节所述的过程启用和配置此功能。

准备工作

- 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《硬件安装指南》。
- 确保邮件网关可以远程访问；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。
- 要重启邮件网关，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》。

Procedure

步骤 1 使用 SSH 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：

a. 此功能的专用 IP 地址，加上网络掩码和网关。

b. 执行电源循环命令所需的用户名和密码。

这些证书与用于访问您的邮件网关的其他证书相互独立。

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邮件网关电源。

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

相关主题

- 远程重置邮件网关电源

恢复到之前版本的 AsyncOS

AsyncOS 提供将 AsyncOS 操作系统恢复到供应急之用的之前的合格内部版本。

恢复的影响

在邮件网关上使用 revert 命令是一项极具破坏性的操作。此命令会销毁所有配置日志和数据库。仅会保留管理接口上的网络信息保留，其余网络配置都将删除。此外，在重新配置邮件网关之前，恢复操作还会中断邮件处理。由于此命令会破坏网络配置，因此在您希望发出 revert 命令时，可能需要对邮件网关进行物理本地访问。

Caution 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。

在虚拟邮件网关上恢复 AsyncOS 可能会影响许可证

如果从适用于邮件的 AsyncOS 9.0 恢复到适用于邮件的 AsyncOS 8.5，则许可证不更改。

如果从适用于邮件的 AsyncOS 9.0 恢复到适用于邮件的 AsyncOS 8.0，则不会再有邮件网关不使用安全功能传送邮件的 180 天宽限期。

功能密钥到期日期在任何情况下都不会更改。

相关主题

- 虚拟邮件网关许可证到期 , on page 13

恢复 AsyncOS

Procedure

步骤 1 确保您拥有想要恢复到的版本的配置文件。配置文件不向后兼容。为此，可以通过邮件将该文件发送给自己或通过 FTP 发送文件。有关信息，请参阅通过邮件发送配置文件, on page 15。

步骤 2 在其他计算机上保存邮件网关当前配置的备份副本（不屏蔽密码）。

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 等待邮件队列清空。

步骤 5 登录到您要恢复的邮件网关的 CLI。

在运行 revert 命令时，系统将发出许多警告提示。接受这些警告提示之后，将会立即执行恢复操作。因此，在完成恢复前的步骤之前，请勿开始恢复过程。

步骤 6 从 CLI 中发出 **revert** 命令。

Note 恢复过程非常耗时。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邮件网关。

步骤 7 等待邮件网关重启两次。

步骤 8 计算机重启两次之后，请使用串行控制台并使用 **interfaceconfig** 命令配置具有可访问 IP 地址的接口。

步骤 9 在配置的某个接口上启用 FTP 或 HTTP。

步骤 10 以 FTP 传送您创建的 XML 配置文件，或将其粘贴到 GUI 界面。

步骤 11 加载您要恢复到的版本的 XML 配置文件。

步骤 12 如果使用“安全列表/阻止列表 (Safelist/Blocklist)”功能，请导入并恢复“安全列表/阻止列表 (Safelist/Blocklist)”数据库。

步骤 13 确认您的更改。

现在，应使用所选的 AsyncOS 版本运行恢复的邮件网关。

为邮件网关生成的邮件配置返回地址

在以下情况下，可以为 AsyncOS 生成的邮件配置信封发件人：

- 反病毒通知
- 退回
- DMARC 反馈
- 通知（notify() 和 notify-copy() 过滤器操作）
- 隔离去通知（以及隔离区管理中的“发送副本”[Send Copy]）
- 报告
- 其他所有邮件。

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。

可以在 GUI 中或是在 CLI 中使用 addressconfig 命令修改系统生成的邮件的返回地址.

Procedure

步骤 1 导航到“系统管理”(System Administration) >“返回地址”(Return Addresses) 页面。

步骤 2 单击**编辑设置 (Edit Settings)**。

步骤 3 对您要修改的一个或多个地址进行更改

步骤 4 提交并确认更改。

为系统运行状况参数配置阈值

根据贵组织的要求，您可以为邮件网关的各个运行状况参数（例如CPU使用、队列中的最大邮件数等）配置阈值。您还可以将邮件网关配置为在达到指定的阈值时发送警报。

Note 要使用 CLI 为系统运行状况参数配置阈值，请使用 healthconfig 命令。有关详细信息，请参阅 CLI 内联帮助或《适用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。

准备工作

请仔细确定阈值。

Procedure

步骤 1 依次单击**系统管理 (System Administration)** > **系统运行状况 (System Health)**。

步骤 2 单击**编辑设置 (Edit Settings)**。

步骤 3 配置以下选项：

- 为 CPU 使用指定阈值级别（以百分比形式）。

  此外，还要指定在当前的CPU使用达到配置的阈值时是否要接收警报。发送第一个警报之后，如果 CPU 使用在 15 分钟内达到了自 5% 触发第一个警报起的运行平均值，则会再发送一个警报。

  Note 这些警报的触发条件只有邮件处理过程中的 CPU 使用情况。

- 为内存页面交换指定阈值级别（以百分比形式）。

  此外，还要指定在整体内存交换使用率达到配置的阈值时是否要接收警报。发送第一个警报之后，如果内存页面交换达到了由 150% 或在 15 分钟警报间隔后触发第一个警报的值，则会再发送一个警报。例如，如果阈值设置为10，

  - 当内存交换使用率达到 10.1% 时，发送第一个警报。
  - 当内存交换使用率在 15 分钟内达到 15.1% 时，会发送另一个警报。

- 为队列中邮件的最大数指定阈值级别（以邮件数形式）。

  此外，还要指定在队列内的邮件数达到配置的阈值时是否要接收警报。发送第一个警报之后，如果队列内的邮件数在 15 分钟内达到了由 150% 触发第一个警报的值，则会再发送一个警报。例如，如果阈值设置为 1000，

  - 当队列内的邮件最大数达到 1002 时，发送第一个警报。
  - 当队列内的邮件最大数在 15 分钟内达到 1510 时，则会再发送一个警报。

Note 此功能的所有警报均属于“系统警报”(System Alert) 类别。

步骤 4 提交并确认更改。

What to do next

如果已为此功能配置了警报，请确保要订购系统警报。有关说明，请参阅添加警报收件人, on page 41。

检查邮件网关的运行状况

可以使用运行状况检查功能检查邮件网关的运行状况。执行运行状况检查时，系统将分析当前“状态日志”(Status Logs) 中的历史数据（最多三个月）以确定邮件网关的运行状况。

Note 对于要执行此分析的系统“状态日志”(Status Logs) 必须包含至少一个月的记录数据。

要执行运行状况检查，请

- 在 Web 界面上，依次转至**系统管理 (System Administration)** > **系统运行状况 (System Health)** 页面，然后单击**执行运行状况检查 (Run Health Check)**。
- 在 CLI 上，运行命令： **`healthcheck`**。

分析结果将指明系统在最近几个月内是否遇到了如下一个或多个问题：

- 资源节约模式
- 邮件处理延迟
- 高 CPU 使用
- 高内存使用
- 高内存页面交换

如果运行状况检查指明您的邮件网关遇到了上述一个或多个问题，请考虑查看和优化您的系统配置。有关详细信息，请参阅：
http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118881-technote-esa-00.html。

警报

警报邮件是自动生成的标准邮件，其中包含邮件网关上发生的事件的相关信息。这些事件的重要性（或严重性）级别可以从“微小”到“重要”不等，通常有关于邮件网关上的特定组件或功能。警报由邮件网关生成。您可以在更为精细的级别指定将哪些警报邮件发送给哪些用户以及为哪些严重性级别的事件发送警报。通过 GUI 中的“系统管理”>“警报”页面（或 CLI 中的 alertconfig 命令）管理警报。

警报严重性

可以针对以下严重性级别发送警报：

- 严重：需要立即注意。
- 警告 (Warning)：需要进一步监控并可能需要立即注意的问题或错误
- 信息：此设备的例行运行当中生成的信息。

自动支持

为了使思科能够更好地支持和设计未来的系统变更，可以将邮件网关配置为向思科系统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”，是允许我们的团队主动支持您的需求的有效方式。“自动支持”还发送每周报告，说明系统正常运行时间、**status**命令的输出和使用的AsyncOS版本。

默认情况下，设置为接收“参考”(Information)严重性级别的“系统”(System)警报类型的警报收件人，会收到发往思科的每封邮件的副本。如果您不希望内部每周发送警报邮件，可以禁用此功能。要启用或禁用此功能，请参阅配置警报设置, on page 42。

警报传送

从邮件网关发送到“警报收件人”(Alert Recipients)中指定地址的警报，遵循为这些目标定义的SMTP路由。

由于警报邮件可用来通知邮件网关中的问题，因此不使用 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。
- 警报邮件不通过工作队列传递，所以不对它们病毒扫描或垃圾邮件。另外，它们也不受邮件过滤器或内容过滤器约束。
- 警报邮件不通过传送队列传递，因此不受退回配置文件或目标控制限制的影响。

Note [可选 - 仅当使用 `alertconfig` CLI 命令启用了 TLS 支持并在 SSL 配置设置页面中启用了 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。

Note [可选 - 仅在使用 `alertconfig` CLI 命令启用了 TLS 支持并在 SSL 配置设置页面中启用了 X 509 验证时]：检查服务器证书的签名算法。

警报邮件示例

```
Date: 23 Mar 2005 21:10:19 +0000

To: joe@example.com

From: IronPort C60 Alert [alert@example.com]

Subject: Critical-example.com: (Anti-Virus) update via http://newproxy.example.com
failed

The Critical message is:

update via http://newproxy.example.com failed

Version: 4.5.0-419

Serial Number: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2005

For more information about this error, please see
http://support.ironport.com

If you desire further information, please contact your support provider.
```

添加警报收件人

通过警报引擎，可以精细控制向哪些警报收件人发送哪些警报。例如，可以将系统配置为仅将特定警报发送给某警报收件人，将某警报收件人配置为仅在发送“系统”(System)（警报类型）的“严重”(Critical)（严重性）信息时接收通知。

Note 如果在系统设置期间启用了“自动支持”，则指定的邮件地址将默认接收所有严重性和类型的警报。可以随时更改此配置。

Procedure

步骤 1 依次选择**系统管理 (System Administration) > 警报 (Alerts)**。

步骤 2 单击**添加接收人 (Add Recipient)**。

步骤 3 输入收件人的邮件地址。可以输入多个地址，并以逗号分隔。

步骤 4 （可选）如果您要接收思科支持人员发来的软件版本和重要支持通知警报，请选中**版本和支持通知 (Release and Support Notifications)** 复选框。

步骤 5 选择此收件人将接收的警报类型和严重性。

步骤 6 提交并确认更改。

配置警报设置

以下设置适用于所有警报。

Note 使用 alertconfig CLI 命令定义要在邮件网关上保存的警报数量以供日后查看。

Procedure

步骤 1 单击“警报”(Alerts) 页面中的**编辑设置 (Edit Settings)**。

步骤 2 输入“信头源:”地址以在发送警报时使用，或选择“自动生成”(Automatically Generated) (“alert@<hostname>”)。

步骤 3 如果您要指定发送两次重复警报间隔的秒数，请选中该复选框。有关详细信息，请参阅发送重复警告, on page 42。

- 指定 AsyncOS 发送重复警报前等待的初始秒数。
- 指定 AsyncOS 发送重复警报前等待的最大秒数。

步骤 4 可以通过选中“IronPort 自动支持”(IronPort AutoSupport) 选项来启用“自动支持”。有关“自动支持”的详细信息，请参阅自动支持, on page 40。

- 如果启用了“自动支持”，则每周向设置为接收“参考”(Information) 级别系统警报的警报收件人发送“自动支持”报告。可以通过该复选框禁用此功能。

步骤 5 提交并确认更改。

警告设置

警告设置可控制警报的常规行为和配置，包括：

- 发送警告时的 RFC 2822 信头源:（输入地址或使用默认的“alert@<hostname>”）。也可以在 CLI 中使用 alertconfig -> from 命令设置此项。
- 发送重复警报前等待的初始秒数。
- 发送重复警报前等待的最大秒数。
- “自动支持”的状态（启用或禁用）。
- 每周向设置为接收“信息”(Information) 级别系统警报的警报收件人发送“自动支持”状态报告。

发送重复警告

可以指定 AsyncOS 发送重复警报前等待的初始秒数。如果将此值设置为 0，不会发送重复警报摘要，而是毫无任何延迟地发送所有重复警报（这样可能导致短时间内发送大量邮件）。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，如果等待 5 秒，警报发送时间将是 5 秒、15 秒、35 秒、75 秒、155 秒、315 秒，以此类推。

最终，间隔可能变得很大。您可以通过“发送重复警报前等待的最大秒数 (maximum number of seconds to wait before sending a duplicate alert)”字段，设置间隔之间等待的秒数限值。例如，如果将初始值设置为 5 秒，最大值为 60 秒，则在 5 秒、15 秒、35 秒、60 秒、120 秒时发送警报，以此类推。

查看最近的警报

邮件网关会保存最新的警报，因此如果丢失或删除了警报邮件，可以在 GUI 和 CLI 中进行查看。这些警报无法从邮件网关下载。

要查看最新警报的列表，请单击“警报”(Alerts) 页面上的**查看排名靠前的警报 (View Top Alerts)** 按钮或使用 CLI 中的 displayalerts 命令。可以在 GUI 中按日期、级别、文本和收件人排列警报。

默认情况下，邮件网关最多保存 50 条警报以显示在**排名靠前的警报 (Top Alerts)** 窗口中。使用 CLI 中的 alertconfig -> setup 命令编辑邮件网关保存的警报数。如果要禁用此功能，请将警报数更改为 0。

风险通告说明

下表按类别列出了警报，包括警报名称（使用的内部描述符）、警报的实际文本、说明、严重性（重要，参考或警告）以及邮件文本中所包含的参数（如果有）。参数值在警报的实际文本将被替换。例如，以下警报邮件可能会在邮件文本中提到“$ip”。生成警报时，“$ip”将替换为实际的 IP 地址。

- 反垃圾邮件警报, on page 43
- 防病毒警报, on page 44
- 目录搜集攻击预防 (DHAP) 警报, on page 45
- 硬件风险通告, on page 45
- 垃圾邮件隔离区警报, on page 46
- 安全列表/阻止列表警报, on page 47
- 系统警告, on page 48
- 更新程序警报, on page 58
- 病毒爆发过滤器警报, on page 58
- 将警报集群化, on page 59

反垃圾邮件警报

下表包含可通过 AsyncOS 生成的各种反垃圾邮件警报的列表，包括对警报和警报严重性的说明。

Table 1: 可能的反垃圾邮件警报列表

警报名称	邮件和描述	参数
AS.SERVER.ALERT	$engine anti-spam - $message $tb 严重。反垃圾邮件引擎失败时发送。	“**engine**”- 反垃圾邮件引擎的类型。 “**message**”- 日志邮件。 “**tb**”- 事件的回溯。
AS.TOOL.INFO_ALERT	更新 - $engine - $message 参考。反垃圾邮件引擎出现问题时发送。	“**engine**”- 反垃圾邮件引擎名称 “**message**”- 邮件
AS.TOOL.ALERT	更新 - $engine - $message 严重。当更新因用来管理反垃圾邮件引擎的某个工具出现问题而中止时发送。	“**engine**”- 反垃圾邮件引擎名称 “**message**”- 邮件

防病毒警报

下表包含可通过 AsyncOS 生成的各种防病毒警报的列表，包括对警报和警报严重性的说明：

Table 2: 可能的防病毒警报列表

警报名称	邮件和描述	参数
AV.SERVER.ALERT /AV.SERVER.CRITICAL	$engine antivirus - $message $tb 严重。防病毒扫描引擎出现严重问题时发送。	“**engine**”- 防病毒引擎的类型。 “**message**”- 日志邮件。 “**tb**”- 事件的回溯。
AV.SERVER.ALERT.INFO	$engine antivirus - $message $tb 信息。当防病毒扫描引擎出现参考事件时发送。	“**engine**”- 防病毒引擎的类型。 “**message**”- 日志邮件。 “**tb**”- 事件的回溯。
AV.SERVER.ALERT.WARN	$engine antivirus - $message $tb 警告。防病毒扫描引擎出现问题时发送。	“**engine**”- 防病毒引擎的类型。 “**message**”- 日志邮件。 “**tb**”- 事件的回溯。
MAIL.ANTIVIRUS.ERROR_MESSAGE	MID $mid antivirus $what error $tag 严重。如果防病毒扫描在扫描邮件时发生错误，则发送。	“**mid**”- MID “**what**”- 发生的错误。 “**tag**”- 病毒爆发名称（如果已设置）。

警报名称	邮件和描述	参数
MAIL.SCANNER. PROTOCOL_MAX_RETRY	MID $mid 已破坏，无法由 $engine 进行扫描。	“**mid**”- MID “**engine**”- 正在使用的引擎
	严重。因为邮件被破坏，所以扫描引擎尝试扫描邮件失败。当超出最大重试次数时，邮件将在不由引擎处理的情况下进行处理。	

目录搜集攻击预防 (DHAP) 警报

下表包含可通过 AsyncOS 生成的各种 DHAP 警报的列表，包括对警报和警报严重性的说明。

Table 3: 可能的目录搜集攻击预防警报列表

警报名称	邮件和描述	参数
LDAP.DHAP_ALERT	LDAP：检测到潜在的目录搜集攻击。有关此攻击的详细信息，请参阅系统邮件日志。	
	警告。检测到可能的目录搜集攻击时发送。	

硬件风险通告

下表包含可通过 AsyncOS 生成的各种硬件警报的列表，包括对警报和警报严重性的说明。

Table 4: 可能的硬件警报列表

警报名称	邮件和描述	参数
INTERFACE.ERRORS	端口 $port: 检测到 $in_err 输入错误、$out_err 输出错误、$col 冲突，请检查媒体设置。	“**port**”- 接口名称。 “**in_err**”- 自上一封邮件以来的输入错误数。 “**out_err**”- 自上一封邮件以来的输出错误数。 “**col**”- 自上一封邮件以来的数据包冲突数。
	警告。检测到接口错误时发送。	
MAIL.MEASUREMENTS_FILESYSTEM	$file 系统分区的处于 $capacity% 容量	“**file_system**”- 文件系统的名称 “**capacity**”- 文件系统满溢的程度（采用百分比形式）。
	警告。当磁盘分区接近容量 (75%) 时发送。	

警报名称	邮件和描述	参数
MAIL.MEASUREMENTS_FILESYSTEM.严重	$file 系统分区的处于 $capacity% 容量 严重。当磁盘分区达到90% 容量（以及 95%、96%、97% 等）时发送。	“**file_system**”- 文件系统的名称 “**capacity**”- 文件系统满溢的程度（采用百分比形式）。
SYSTEM.RAID_EVENT_ALERT	RAID 事件发生：$error 警告。发生严重 RAID 事件时发送。	“**error**”- RAID 错误的文本。
SYSTEM.RAID_EVENT_ALERT_INFO	RAID 事件发生：$error 参考。发生 RAID 事件时发送。	“**error**”- RAID 错误的文本。

垃圾邮件隔离区警报

下表包含可通过 AsyncOS 生成的各种垃圾邮件隔离区警报的列表，包括警报和警报严重性说明。

Table 5: 可能的垃圾邮件隔离区警报列表

警报名称	邮件和描述	参数
ISQ.CANNOT_CONNECT_OFF_BOX	ISQ：无法在 $host:$port 连接到机下隔离区 参考。当AsyncOS无法连接到（机下）IP地址时发送。	“**host**”- 机下隔离区的地址 “**port**”- 在机下隔离区连接到的端口
ISQ.CRITICAL	ISQ: $msg 严重。发生严重垃圾邮件隔离区错误时发送。	“**msg**”- 要显示的邮件
ISQ.DB_APPROACHING_FULL	ISQ：超过 $threshold% 的数据库为满 警告。垃圾邮件隔离区数据库接近满状态时发送。	“**threshold**”- 开始发送警报时达到的满状态阈值（以百分比形式）
ISQ.DB_FULL	ISQ：数据库已满 严重。垃圾邮件隔离区数据库已满时发送。	
ISQ.MSG_DEL_FAILED	ISQ：因以下原因未能删除 MID $mid（收件人为 $rcpt）：$reason 警告。未能成功从垃圾邮件隔离区删除邮件时发送。	“**mid**”- MID “**rcpt**”- 收件人或“全部” “**reason**”- 未删除邮件的原因

警报名称	邮件和描述	参数
ISQ.MSG_NOTIFICATION_FAILED	ISQ：未能发送通知邮件：$reason 警告。未成功发送通知邮件时发送。	“**reason**”- 未发送通知的原因
ISQ.MSG_QUAR_FAILED	警告。未成功隔离邮件时发送。	
ISQ.MSG_RLS_FAILED	ISQ：因以下原因未能将 MID $mid 发布到 $rcpt：$reason 警告。未成功发布邮件时发送。	“**mid**”- MID “**rcpt**”- 收件人或“全部” “**reason**”- 未发布邮件的原因
ISQ.MSG_RLS_FAILED_UNK_RCPTS	ISQ：因以下原因未能发布 MID $mid：$reason 警告。因收件人未知而未成功发布邮件时发送。	“**mid**”- MID “**reason**”- 未发布邮件的原因
ISQ.NO_EU_PROPS	ISQ：无法检索 $user 的属性。设置默认值 参考。当 AsyncOS 无法检索用户相关信息时发送。	“**user**”- 最终用户名称
ISQ.NO_OFF_BOX_HOST_SET	ISQ：在未设置主机的情况下设置机下 ISQ 参考。当 AsyncOS 配置为引用未定义的外部隔离区时发送。	

安全列表/阻止列表警报

下表包含可通过 AsyncOS 生成的各种安全列表/阻止列表警报的列表，包括对警报和警报严重性的说明

Table 6: 可能的安全列表/阻止列表警报列表

警报名称	邮件和描述	参数
SLBL.DB.RECOVERY_FAILED	SLBL：无法恢复最终用户安全列表/阻止列表数据库：“$error”。 严重。无法恢复安全列表/阻止列表数据库。	“**error**”- 错误原因
SLBL.DB.SPACE_LIMIT	SLBL：最终用户安全列表/阻止列表数据库超出了允许的磁盘空间：$current of $limit。 严重。安全列表/阻止列表数据库超出了允许的磁盘空间。	“**current**”- 已使用的空间量（以 MB 为单位） “**limit**”- 配置的限制（以 MB 为单位）

系统警告

下表包含可通过 AsyncOS 生成的各种系统警报的列表，包括对警报和警报严重性的说明。

Table 7: 可能的系统警报的列表

组件/警报名称	邮件和描述	参数
AMP.ENGINE.ALERT	请参阅确保接收有关高级恶意软件防护问题的警报	-
AsyncOS API Alerts	请参阅《使用思科安全邮件网关的 *AsyncOS API* - 入门指南》的“警报”部分。	-
Mailbox Auto Remediation Alerts	请参阅“警报”部分 补救邮箱中的邮件	-
COMMON.APP_FAILURE	应用故障发生：$error 警告。出现未知应用故障时发送。	“**error**”- 错误（通常为回溯）的文本。
COMMON.ENGINE_AUTO_UPDATE_ENABLED	<$level>: <$class> 信息：已为特定引擎 <$engine> 启用了自动更新。现在，您将收到此引擎的自动引擎更新。	“**$engine**”- 服务引擎的名称。值可以为： • Sophos • McAfee • Graymail
COMMON.ENGINE_AUTO_UPDATE_DISABLED	<$level>: <$class> 信息：已为特定引擎 <$engine> 禁用了自动更新。除非在特定引擎的“全局设置”页面中启用了自动更新，否则不会收到此引擎的任何自动更新。	“**$engine**”- 服务引擎的名称。值可以为： • Sophos • McAfee • Graymail
COMMON.KEY_EXPIRED_ALERT	您的“$feature”密钥已经到期。请联系您的授权思科销售代表。 警告。功能密钥过期时发送。	“**feature**”- 即将到期的功能的名称。
COMMON.KEY_EXPIRING_ALERT	您的“$feature”密钥将于 $days 天内到期。请联系您的授权思科销售代表。 警告。功能密钥即将到期时发送。	“**feature**”- 即将到期的功能的名称。 “**days**”- 功能将要到期的天数。

组件/警报名称	邮件和描述	参数
COMMON.KEY_FINAL_EXPIRING_ALERT	这是最终通知。您的“$feature”密钥将于 $days 天内到期。请联系您的授权思科销售代表。 警告。以功能密钥即将到期的最终通知形式发送。	“**feature**”- 即将到期的功能的名称。 “**days**”- 功能将要到期的天数。
KEYS.GRACE_EXPIRING_ALERT	邮件网关已经到期的所有安全服务许可证。邮件网关将在 $days 天内不使用安全服务继续传送邮件。 要续订安全服务许可证，请联系您的授权思科销售代表。 严重。从宽限期开始针对虚拟邮件网关许可证到期定期发送。	“**days**”- 发送警报时宽限期内所剩的天数。 有关宽限期的详细信息，请参阅虚拟邮件网关许可证到期 , on page 13。
KEYS.GRACE_FINAL_EXPIRING_ALERT	这是最终通知。邮件网关已经到期的所有安全服务许可证。邮件网关将在 1 天内不使用安全服务继续传送邮件。 要续订安全服务许可证，请联系您的授权思科销售代表。 严重。虚拟邮件网关许可证到期之前的一天发送。	有关宽限期的详细信息，请参阅虚拟邮件网关许可证到期 , on page 13。
KEYS.GRACE_EXPIRED_ALERT	您的宽限期已经到期。所有安全服务均已到期，因此您的邮件网关无法运行。采用新许可证之前，邮件网关不再传送邮件。 要续订安全服务许可证，请联系您的授权思科销售代表。 严重。当虚拟邮件网关的宽限期到期时发送。	有关宽限期的详细信息，请参阅虚拟邮件网关许可证到期 , on page 13。
DNS.BOOTSTRAP_FAILED	无法启动 DNS 解析器。无法联系根服务器。 警告。当邮件网关无法联系根 DNS 服务器时发送。	
COMMON.INVALID_FILTER	无效 class：$error 警告。当遇到无效过滤器时发送。	“**class**”-“Filter”、“SimpleFilter”等。 “**error**”- 其他有关为何过滤器无效的信息。

组件/警报名称	邮件和描述	参数
IPBLOCKD.HOST_ADDED_TO_ALLOWED_LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED_LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED_LIST	由于 SSH DOS 攻击，位于 的主机已被添加到阻止列表。 位于 $ip 的主机已被永久添加到 SSH 运行列表。 位于 $ip 的主机已从阻止列表中删除。	“**ip**”- 尝试从其进行登录的 IP 地址。
	警告。 对于尝试通过 SSH 连接到邮件网关，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。 条目将于大约一天后自动从该阻止列表删除。	
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP：失败的组查询 $name，过滤器中的比较将评估为 false	“**name**”- 查询的名称。
	严重。当 LDAP 组查询失败时发送。	
LDAP.HARD_ERROR	LDAP：$name 内因 $why 原因发生工作队列处理错误	“**name**”- 查询的名称。 “**why**”- 错误发生的原因。
	严重。当LDAP查询完全失败时（尝试所有服务器之后）发送。	
LOG.ERROR.*	严重。各种日志记录错误。	
MAIL.FILTER.RULE_MATCH_ALERT	MID $mid 匹配 $rule_name 规则。\n 详细信息：$details	“**mid**”- 邮件的唯一识别号。 “**rule_name**”- 匹配的规则的名称。 “**details**”- 有关邮件或规则的详细信息。
	参考。每当信头请求规则被评价为 true 时发送。	
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	扫描各个收件人期间LDAP组查询失败，可能是 LDAP 错误配置或服务器不可访问所致。	
	严重。扫描各个收件人期间LDAP组查询失败时发送。	
MAIL.QUEUE.ERROR.*	严重。各种邮件队列硬错误。	

组件/警报名称	邮件和描述	参数
MAIL.OMH.DELIVERY_RETRY	主题 -“警报： $hostname 的邮件传送失败。一个或多个域的 DANE 验证失败。” 消息 - 由于 $hostname 中所有邮件交换 (MX) 主机的 DANE 验证失败，邮件传送失败。邮件网关将再次尝试邮件传送或退回邮件。	‘host’ - DANE 验证失败的主机。
MAIL.RES_CON_START_ ALERT. MEMORY	此系统（主机名：$hostname）已进入“资源节约”模式，以防止快速消耗重要系统资源。此系统的 RAM 利用率超出了 $memory_threshold_start% 的资源节约阈值。此系统允许的接收速率将随着 RAM 利用率越来越接近 $memory_threshold_halt% 而逐渐降低。 严重。当 RAM 使用率超过系统资源节约阈值时发送。	“**hostname**”- 主机的名称。 “**memory_threshold_start**”- 启动内存缓送技术时的百分比阈值。 “**memory_threshold_halt**”- 系统因内存过满而将中止时的百分比阈值。
MAIL.RES_CON_START_ ALERT. QUEUE_SLOW	此系统（主机名：$hostname）已进入“资源节约”模式，以防止快速消耗重要系统资源。队列出现过载，无法保持当前吞吐量。 严重。当邮件队列过载及企业系统资源节约时发送。	“**hostname**”- 主机的名称。
MAIL.RES_CON_START_ ALERT. QUEUE	此系统（主机名：$hostname）已进入“资源节约”模式，以防止快速消耗重要系统资源。此系统的队列利用率超出了 $queue_threshold_start% 的资源节约阈值。此系统允许的接收速率将随着队列利用率越来越接近 $queue_threshold_halt% 而逐渐降低。 严重。当队列利用率超过系统资源节约阈值时发送。	“**hostname**”- 主机的名称。 “**queue_threshold_start**”- 启动内存缓送技术时的百分比阈值。 “**queue_threshold_halt**”- 系统因队列过满而将中止时的百分比阈值。
MAIL.RES_CON_START_ ALERT. WORKQ	此系统（主机名：$hostname）已进入“资源节约”模式，以防止快速消耗重要系统资源。当前工作队列大小超出 $suspend_threshold 的阈值，因此侦听程序已挂起。工作队列大小下降到 $resume_threshold 时，侦听程序将会恢复。使用系统 CLI 上的“tarpit”命令可以改变这些阈值。 参考。由于工作队列过大暂停监听程序时发送。	“**hostname**”- 主机的名称。 “**suspend_threshold**”- 侦听程序挂起的工作队列大小下限。 “**resume_threshold**”- 侦听程序恢复的工作队列大小上限。

组件/警报名称	邮件和描述	参数
MAIL.RES_CON_START_ALERT	此系统（主机名：$hostname）已进入“资源节约”模式，以防止快速消耗重要系统资源。 严重。当邮件网关进入“资源保护”模式时发送。	“**hostname**”- 主机的名称。
MAIL.RES_CON_STOP_ALERT	由于资源利用率已下降到节约阈值以下，因此此系统（主机名：$hostname）已退出“资源节约”模式。 参考。当邮件网关退出“资源保护”模式时发送。	“**hostname**”- 主机的名称。
MAIL.URL_REP_CLIENT.CATEGORY_CHANGE	请参阅将来的 URL 类别集变更。	—
MAIL.BEAKER_CONNECTOR.CERTIFICATE_INVALID	请参阅URL 过滤故障排除。	
MAIL.BEAKER_CONNECTOR.ERROR_FETCHING_CERTIFICATE		
MAIL.WORK_QUEUE_PAUSED_NATURAL	工作队列已暂停，$num 个邮件，$reason 严重。当工作队列暂停时发送。	“**num**”- 工作队列中的邮件数。 “**reason**”- 工作队列暂停的原因。
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	工作队列已恢复，$num 个邮件 严重。当工作队列恢复时发送。	“**num**”- 工作队列中的邮件数。
NTP.NOT_ROOT	未以根用户身份运行，无法调整系统时间 警告。当邮件网关由于 NTP 未作为根运行而无法调整时间时发送。	
QUARANTINE.ADD_DB_ERROR	无法隔离 MID $mid - 隔离系统不可用 严重。无法将邮件发送至隔离区时发送。	“**mid**”- MID
QUARANTINE.DB_UPDATE_FAILED	无法更新隔离区数据库（当前版本：$version；目标版本：$target_version） 严重。无法更新隔离区数据库时发送。	“**version**”- 检测到的方案版本。 “**target_version**”- 目标方案版本。
QUARANTINE.DISK_SPACE_LOW	$file_system 分区空间不足导致隔离区系统不可用。 严重。当隔离区磁盘空间已满时发送。	“**file_system**”- 文件系统的名称

组件/警报名称	邮件和描述	参数
QUARANTINE.THRESHOLD_ALERT	隔离区“$quarantine”处于 $full% 满状态 警告。当隔离区达到容量的 5%、50% 或 75% 时发送。	“**quarantine**”- 隔离区的名称。 “**full**”- 隔离区满溢程度的百分比。
QUARANTINE.THRESHOLD_ALERT.SERIOUS	隔离区“$quarantine”处于 $full% 满状态 严重。当隔离区达到容量的 95% 时发送。	“**quarantine**”- 隔离区的名称。 “**full**”- 隔离区满溢程度的百分比。
REPORTD.DATABASE_OPEN_FAILED_ALERT	打开数据库时，报告系统遇到严重错误。为了防止其他服务中断，此计算机上的报告功能已禁用。请与客户支持联系以启用报告。错误消息如下：$err_msg 严重。当报告引擎无法打开数据库时发送。	“**err_msg**”- 出现的错误邮件
REPORTD.AGGREGATION_DISABLED_ALERT	“由于日志记录磁盘空间不足，对所收集报告数据的处理功能已禁用。磁盘使用量超过 $threshold 百分比。报告事件的记录很快将会受限，如果未释放磁盘空间（通过删除旧日志等方法），还可能会丢失报告数据。磁盘使用量下降到 $threshold 百分比以下时，报告数据的满状态处理将会自动重新启动。 警告。当系统磁盘空间不足时发送。当日志条目的磁盘使用量超过日志使用阈值时，报告禁用聚合并发送警报。	“**threshold**”- 阈值
REPORTING.CLIENT.UPDATE_FAILED_ALERT	报告客户端：报告系统在延长的一段时间 ($duration) 内无响应。 警告。当报告引擎无法保存报告数据时发送。	“**duration**”- 客户端一直在尝试联系报告后台守护程序的时长。此为一个采用人可读格式的字符串 (’1h 3m 27s’)。
REPORTING.CLIENT.JOURNAL.FULL	报告客户端：报告系统无法保持生成数据的速率。生成的所有新数据都将丢失。 严重。当报告引擎无法存储新数据时发送。	
REPORTING.CLIENT.JOURNAL.—	报告客户端：报告系统现在无法处理新数据。 参考。当报告引擎再次能够存储新数据时发送。	
PERIODIC_REPORTS.REPORT_TASK.BUILD_FAILURE	生成定期报告“$report_title”时出错。此订用已从调度程序删除。 严重。当报告引擎无法生成报告时发送。	“**report_title**”- 报告标题

组件/警报名称	邮件和描述	参数
PERIODIC_REPORTS.REPORT_TASK.EMAIL_FAILURE	以邮件发送定期报告“$report_title”时失败。此订用已从调度程序删除。 严重。当无法通过邮件发送报告时发送。	“**report_title**”- 报告标题
PERIODIC_REPORTS.REPORT_TASK.ARCHIVE_FAILURE	存档定期报告“$report_title”时失败。此订用已从调度程序删除。 严重。当报告无法存档时发送。	“**report_title**”- 报告标题
SENDERBASE.ERROR	处理对查询 $query 的响应时出错：响应为 $response 参考。处理 SenderBase 的响应出错时发送。	“**query**”- 查询地址。 “**response**”- 收到的响应的原始数据。
SMTPAUTH.FWD_SERVER_FAILED_ ALERT	SMTP 身份验证：无法到达转发服务器 $ip 时出错，原因为 $why 警告。无法访问 SMTP 身份验证转发服务器时发送。	“**ip**”- 远程服务器的 IP。 “**why**”- 错误发生的原因。
SMTPAUTH.LDAP_QUERY_FAILED	SMTP 身份验证：LDAP 查询失败，有关详细信息，请参阅 LDAP 调试日志。 警告。当 LDAP 查询失败时发送。	
SYSTEM.HERMES_SHUTDOWN_FAILURE. REBOOT	准备 ${what} 时，无法以温和的方式停止邮件服务器：${error}$what:=reboot 警告。关闭正在重启的系统出现问题时发送。	“**error**”- 发生的错误。
SYSTEM.HERMES_SHUTDOWN_FAILURE. SHUTDOWN	准备 ${what} 时，无法以温和的方式停止邮件服务器：${error}$what:=shut down 警告。关闭系统出现问题时发送。	“**error**”- 发生的错误。
SYSTEM.LOGIN_FAILURES_LOCK_ALERT	$Numlogins 次连续登录失败后，用户“$user”被锁定。上次从 $rhost 进行登录尝试 信息：当因失败登录尝试次数达到最大值而导致用户帐户被锁定时发送	“user”- 用户名称 “numlogins”- 配置的警报阈值 “rhost”- 远程主机的地址
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	更新收件人验证数据时出错：$why 严重。当收件人验证更新失败时发送。	“why”- 错误邮件。

组件/警报名称	邮件和描述	参数
SYSTEM.SERVICE_TUNNEL. 已禁用	技术支持：服务隧道已被禁用 参考。禁用为“思科支持服务”(Cisco Support Services) 创建的隧道时发送。	
SYSTEM.SERVICE_TUNNEL. ENABLED	技术支持：服务隧道已启用，端口 $port 参考。启用为“思科支持服务”(Cisco Support Services) 创建的隧道时发送。	“**port**”- 用于服务隧道的端口。
IPBLOCKD.HOST_ADDED_TO_ALLOWED_LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED_LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED_LIST	由于 SSH DOS 攻击，位于 的主机已被添加到阻止列表。 位于 $ip 的主机已被永久添加到 SSH 运行列表。 位于 $ip 的主机已从阻止列表中删除。 警告。 对于尝试通过 SSH 连接到邮件网关，但未提供有效凭证的 IP 地址，如果两分钟内失败尝试次数大于 10 次，则将其添加到 SSH 阻止列表。 当用户从相同 IP 地址登录成功时，该 IP 地址会被添加到允许列表中。 允许访问允许列表中的地址，即使它们也位于阻止列表中。 条目将于大约一天后自动从该阻止列表删除。	“**ip**”- 尝试从其进行登录的 IP 地址。
WATCHDOG_RESTART_ALERT_MSG	<$level>: <$class>, <$hostname>: $subject $text 警告。 邮件网关使用监控器服务监控以下引擎的运行状况： • 反垃圾邮件 • 防病毒 • 防恶意软件防护 • Graymail 如果上述任何一个引擎在某一持续时间内都没有响应监控器服务，则监控器服务将重启引擎，并向管理员发送警报。	“**subject**”- 特定于引擎的监控器警报主题 “**text**”- 特定于引擎的监控器警报文本

组件/警报名称	邮件和描述	参数
MAIL.IMH.GEODB_UPDATE_COUNTRIES'	警告。地理位置更新 - 受支持的国家/地区列表已更改。 增加的国家/地区 - <$added> 删除的国家/地区 - <$deleted> 相应地检查您的 HAT 发件人组、邮件过滤器和内容过滤器设置。	“added”- 添加了以下国家/地区：<iso_code1>:<country_name1>,<iso_code2>:<country_name2>, “deleted”- 删除了以下国家/地区：<iso_code1>:<country_name1>:<iso_code2>:<country_name2>,
MAIL.UPDATED_SHORT_URL_DOMAIN_LIST	信息。缩短的 URL 域列表已更新。 添加的域：<$added_domains> 删除的域：<$deleted_domains>	“added_domains”：添加了以下域：<domains_1>、<domain_2> “deleted_domains”：删除了以下域：<domain_3>、<domain_4>
MAIL.DOMAINS_NOT_REACHABLE	警告。邮件网关无法访问以下域以支持缩短的 URL：<$domains> 检查防火墙规则以允许邮件网关连接到这些域。	<$domains>：逗号分隔的域列表
MAIL.UPGRADE_CONFIG_CHANGE.ALERT	信息。在升级期间，当系统更改用户配置的值时发送。	**'text'** - 在升级过程中，智能多重扫描和灰色邮件全局配置设置已修改。请查看智能多重扫描和灰色邮件配置的全局设置。
CERTIFICATE.CERT_EXPIRING_ALERT	您的证书“$certificate”将在 $days 天后过期。 警报级别：WARNING	“**certificate**”，即将到期的证书的名称。 “**days**“，功能将要到期的天数。
CERTIFICATE.CERT_CRITICAL_EXPIRING_ALERT	您的证书“$certificate”将在 $days 小时后过期。 警报级别：CRITICAL；“CRITICAL”证书有效期少于 5 天。	“**certificate**”，即将到期的证书的名称。 “**days**”，天数及剩余时间 (HH:MM:SS)，例如 4 天 10:12:20 小时。
CERTIFICATE.CERT_EXPIRED_ALERT	您的证书“$certificate”已过期。 警报级别：CRITICAL	“**certificate**”，已过期的证书的名称。

组件/警报名称	邮件和描述	参数
MAIL.APP.NO_ACCESS_KEY	警报文本：“未能轮询思科高级钓鱼保护云服务的到期日期，添加 API AccessUID 和 API Access 秘钥 (Failed to poll for the Cisco Advanced Phishing Protection Cloud Service expiry date, add API AccessUID and API Access secret key)。 说明：当 APP 到期日期的查询因未输入 API 访问密钥和密钥而失败时，系统将发送警报。	不适用
MAIL.APP.INVALID_KEY	警报文本：“由于 API 访问密钥无效，无法轮询思科高级网络钓鱼保护云服务的到期日期。您需要重新配置 API 访问 UID 和密钥。 (Failed to poll for the Cisco Advanced Phishing Protection Cloud Service expiry date because the API Access Key is invalid. You need to re-configure the API Access UID and secret key.) 说明：当 APP 到期日期的查询因未输入 API 访问密钥和密钥而失败时，系统将发送警报。	不适用
MAIL.APP.EXPIRED	警报文本：思科高级网络钓鱼防护云服务已过期且已禁用。请联系您的思科客户经理续订服务并将其启用。(The Cisco Advanced Phishing Protection Cloud Service has expired and is disabled. Contact your Cisco Account Manager to renew the service and enable it.) 说明：思科高级网络钓鱼防护云服务已过期且已禁用。您需要更新应用程序许可证并启用 APP 服务。	不适用
MAIL.APP.EXPIRY_REMINDER	警报文本：思科高级网络钓鱼防护云服务于 $eaas_expiry_date 到期。您需要联系思科客户经理以续订服务 (Cisco Advanced Phishing Protection Cloud Service expires on $eaas_expiry_date. You need to contact your Cisco Account Manager to renew the service)。 说明：警报从到期日期前三天开始每天发送。	参数：eaas_expiry_date eaas_expiry_date - date，思科高级网络钓鱼防护云服务到期的日期
MAIL.APP.SERVICE_ UNAVAILABLE	警报文本：思科高级网络钓鱼防护云服务更新。无法建立与云服务的通信。(Cisco Advanced Phishing Protection Cloud Service update. Unable to establish communication with the cloud service.) 说明：APP 云服务不可用，因为连续十封邮件无法转发到 APP。	不适用

组件/警报名称	邮件和描述	参数
MAIL.APP.SERVICE_ AVAILABLE	警报文本：思科高级网络钓鱼防护云服务更新。已与云服务建立通信。(Alert text: Cisco Advanced Phishing Protection Cloud Service update. Communication with the cloud service has been established.) 描述：APP 云服务可用。	不适用

更新程序警报

下表包含可由 AsyncOS 生成的各种更新程序警报。

Table 8: 可能的更新程序警报列表

警报名称	邮件和描述	参数
UPDATER.APP.UPDATE_ ABANDONED	发布新版本后，$app 才会丢弃更新。$app 应用尝试并失败了 $attempts 次后才成功完成更新。这可能是由于网络配置问题或临时中断所致 警告。应用正在丢弃更新。	“**app**”- 应用名称。 “**attempts**”- 尝试次数。
UPDATER.UPDATERD. ANIFEST_FAILED_ALERT	更新程序已至少 $threshold 无法与更新程序服务器通信。 警告。未能获取服务器证明。	“**threshold**”- 人可读阈值字符串。
UPDATER.UPDATERD. RELEASE_NOTIFICATION	$mail_text 警告。发布通知。	“**mail_text**”- 通知文本。 “**notification_subject**”- 通知文本。
UPDATER.UPDATERD. UPDATE_FAILED	出现未知错误：$traceback 严重。未能运行更新。	“**traceback**”- 回溯。

病毒爆发过滤器警报

下表包含可通过 AsyncOS 生成的各种病毒爆发过滤器警报的列表，包括对警报和警报严重性的说明。请注意，爆发过滤器也可以在隔离区（具体是指爆发隔离区）的系统警报中引用。

Table 9: 可能的病毒爆发过滤器警报列表

警报名称	邮件和描述	参数
VOF.GTL_THRESHOLD_ALERT	病毒爆发过滤器规则更新警报：$text 上次在 $date $time 更新的所有规则。	“**text**”- 更新警报文本。 “**time**”- 上次更新时间。 “**date**”- 上次更新日期。
	参考。当病毒爆发过滤器阈值发生更改时发送。	
AS.UPDATE_FAILURE	$engine 更新不成功。这可能是由于瞬态网络或 DNS 问题、引起更新传输错误的 HTTP 代理配置或 downloads.ironport.com 不可用造成的。这种失败造成邮件网关上产生的特定错误是：$error	“**engine**”- 无法更新的引擎。 “**error**”- 发生的错误。
	警告。当反垃圾邮件引擎或 CASE 规则无法更新时发送。	

将警报集群化

下表包含可通过 AsyncOS 生成的各种系统警报的列表，包括对警报和警报严重性的说明：

Table 10: 可能的集群警报列表

警报名称	邮件和描述	参数
CLUSTER.CC_ERROR. AUTH_ERROR	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=计算机似乎不在集群中	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
	严重。发生身份验证错误时发送。如果计算机不是集群成员，可能会出现这种情况。	
CLUSTER.CC_ERROR.DROPPED	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=现有连接被丢弃	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
	警告。与集群的连接被丢弃时发送。	
CLUSTER.CC_ERROR.FAILED	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=连接失败	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
	警告。与集群的连接失败时发送。	
CLUSTER.CC_ERROR. FORWARD_FAILED	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=邮件转发失败，无上游连接	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
	严重。邮件网关无法将数据转发到集群中的计算机时发送。	

警报名称	邮件和描述	参数
CLUSTER.CC_ERROR.NOROUTE	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=未发现路由 严重。计算机无法获取到集群中另一计算机的路由时发送。	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR.SSH_KEY	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=主机密钥无效 严重。存在无效 SSH 主机密钥时发送。	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR.TIMEOUT	在 IP $ip 连接到集群计算机 $name 时出错 - $error - whyerror:=操作超时 警告。指定的操作超时时发送。	“**name**”- 计算机的主机名和/或序列号。 “**ip**”- 远程主机的 IP。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP	连接到集群计算机 $name 时出错 - $error - $why 严重。邮件网关为集群中的另一计算机获取有效 IP 地址时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP. AUTH_ERROR	连接到集群计算机 $name 时出错 - $error - whyerror:=计算机似乎不在集群中 严重。连接到集群中的计算机出现身份验证错误时发送。如果计算机不是集群成员，可能会出现这种情况。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP. DROPPED	连接到集群计算机 $name 时出错 - $error - whyerror:=现有连接被丢弃 警告。计算机无法为集群内的另一计算机获取有效 IP 地址并且与集群的连接丢弃时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP. FAILED	连接到集群计算机 $name 时出错 - $error - whyerror:=连接失败 警告。出现未知连接失败并且计算机无法为集群内的另一计算机获取有效 IP 地址时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。

警报名称	邮件和描述	参数
CLUSTER.CC_ERROR_NOIP.FORWARD_FAILED	连接到集群计算机 $name 时出错 - $error - whyerror:=邮件转发失败，无上游连接 严重。计算机无法为集群内的另一计算机获取有效IP地址并且邮件网关无法将设备转发至计算机时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP.NOROUTE	连接到集群计算机 $name 时出错 - $error - whyerror:=未发现路由 严重。计算机无法为集群内的另一计算机获取有效IP地址并且无法获取至计算机的路由时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP.SSH_KEY	连接到集群计算机 $name 时出错 - $error - whyerror:=主机密钥无效 严重。计算机无法为集群内的另一计算机获取有效 IP 地址并且无法获取有效 SSH 主机密钥时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.CC_ERROR_NOIP.TIMEOUT	连接到集群计算机 $name 时出错 - $error - whyerror:=操作超时 警告。计算机无法为集群内的另一计算机获取有效 IP 地址并且指定操作超时时发送。	“**name**”- 计算机的主机名和/或序列号。 “**why**”- 有关错误的详细文本信息。
CLUSTER.SYNC.PUSH_ALERT	覆盖计算机 $name 上的 $sections 严重。当配置数据不同步并且已发送到远程主机时发送。	“**name**”- 计算机的主机名和/或序列号。 “**sections**”- 正在发送的集群部分的列表。

更改网络设置

本节介绍用于配置邮件网关网络操作的功能。通过这些功能，可以直接访问在使用系统设置向导中使用系统设置向导（或 **systemsetup** 命令）配置的主机名、DNS 和路由设置。

本节讨论以下功能：

- **sethostname**
- DNS 配置（GUI 以及 **dnsconfig** 命令）
- 路由配置（GUI 以及通过 **routeconfig** 和 **setgateway** 命令）
- **dnsflush**
- 密码

- 网络接入
- 登录标识

更改系统主机名

主机名用于识别系统。您必须输入完全限定的主机名。要更改主机名，请执行以下操作：

- 在 Web 界面上，依次单击“网络”(Network) >“IP 接口”(IP Interfaces)，单击“管理”(Management)，然后在“主机名”(Hostname) 中更改主机名。
- 在 CLI 中，使用 sethostname 命令。

Note 确认更改后，新主机名才会生效。

配置域名系统 (DNS) 设置

可以通过 GUI 的“网络”菜单的“DNS”页面或 dnsconfig 命令为邮件网关配置 DNS 设置。

可以配置以下设置：

- 使用 Internet 的 DNS 服务器还是自己的服务器，以及具体使用的服务器
- 用于 DNS 通信的接口
- 反向 DNS 查找超时前等待的秒数
- 清除 DNS 缓存

指定 DNS 服务器

AsyncOS 可以使用 Internet 根 DNS 服务器、您自己的 DNS 服务器，或 Internet 根 DNS 服务器和您指定的授权 DNS 服务器。使用 Internet 根服务器时，可以指定用于特定域的备用服务器。由于备用 DNS 服务器适用于单个域，所有它必须对该域拥有授权（提供限定的 DNS 记录）。

不使用 Internet 的 DNS 服务器时，AsyncOS 支持“拆分”DNS 服务器。如果您要使用自己的内部服务器，还可以指定例外域及关联的 DNS 服务器。

设置“拆分 DNS”时，还应设置 in-addr.arpa (PTR) 条目。例如，如果要将“.eng”查询重定向到名称服务器 1.2.3.4，并且所有 .eng 条目均在 172.16 网络内，则应将“eng,16.172.in-addr.arpa”指定为拆分 DNS 配置中的域。

多个条目和优先级

对于输入的每个 DNS 服务器，都可以指定一个数字优先级。AsyncOS 将尝试使用优先级最接近 0 的 DNS 服务器。如果该 DNS 服务器没有响应，AsyncOS 将尝试使用下一个优先级的服务器。如果为相同优先级的 DNS 服务器指定了多个条目，则系统在每次执行查询时会随机列出该优先级的 DNS 服务器。然后，系统会等待简短时间让第一个查询到期或“超时”，然后会等待稍长一点的时间让第二个查询到期或“超时”，以此类推。所等待的时长取决于已配置的DNS服务器及优先级的确切总数。在任何特定优先级，所有 IP 地址的超时长度相同。第一个优先级的超时时间最短，后续每个

优先级的超时时间依次延长。而且，超时期限约为60秒。如果有一个优先级，则该优先级每台服务器的超时将为 60 秒。如果有两个优先级，则第一个优先级每台服务器的超时将为 15 秒；第二个优先级每台服务器的超时将为 45 秒。对于三个优先级，超时分别为 5 秒、10 秒、45 秒。

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

***Table 11: 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 将在优先级为 0 的两台服务器之间随机选择。如果一台优先级 0 的服务器关闭，则使用另一台。如果优先级为 0 的两台服务器均关闭，则使用优先级为 1 的服务器 (1.2.3.6)，最后是优先级为 2 (1.2.3.7) 的服务器。

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

邮件网关尝试对连接到侦听程序来收发邮件的所有远程主机执行“双重 DNS 查找”。[即：系统通过执行双向 DNS 查找，获取和验证远程主机 IP 地址的有效性。其中包括对连接主机的 IP 地址的反向 DNS (PTR) 查找，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 A 记录不存在，则系统将仅使用 IP 地址来匹配主机访问表 (HAT) 中的条目。此特定超时期限仅适用于此查找，与多个条目和优先级, on page 62中讨论的通用 GNS 超时无关。

每个 DNS 服务器的默认值为 20 秒。当 DNS 服务器有多个条目时，总超时值为（DNS 服务器数量乘以反向 DNS 查询超时值）秒数。例如，如果有 8 个 DNS 服务器，且反向 DNS 查询超时值为 20 秒，则总超时值为 (8 * 20) = 160 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。这样也可以防止在接收

主机的证书具有映射至主机 IP 查询的公共名称 (CN) 时邮件网关将邮件传送至需要 TLS 验证的连接的域。

DNS 警报

偶尔，系统会在邮件网关重启时生成消息为“未能引导 DNS 缓存”(Failed to bootstrap the DNS cache) 的警报。这些消息表示系统无法与其主 DNS 服务器通信，如果在建立网络连接前 DNS 子系统已上线，则可能在启动时出现这种情况。如果其他时候出现此消息，可能表示存在网络问题或DNS配置未指向有效的服务器。

清除 DNS 缓存

GUI 中的“清除缓存”按钮或 dnsflush 命令（有关 dnsflush 命令的详细信息，请参阅《适用于思科安全邮件网关的 AsyncOS 的 CLI 参考指南》）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

Procedure

步骤 1 依次选择**网络 (Network) > DNS**。

步骤 2 单击**编辑设置 (Edit Settings)**。

步骤 3 选择使用 Internet 的根 DNS 服务器还是自己的内部 DNS 服务器还是 Internet 的根 DNS 服务器，并指定备用 DNS 服务器。

步骤 4 如果您要使用自己的 DNS 服务器，请输入服务器 ID 并单击**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 62。

步骤 5 如果您要为某些域指定备用 DNS 服务器，请输入域名和备用 DNS 服务器 IP 地址。单击**添加行 (Add Row)** 添加其他域。

Note 可以为单个DNS服务器输入多个域名，只需使用逗号分隔域名即可。也可以输入多个DNS服务器，方法也是使用逗号分隔 IP 地址。

步骤 6 选择用于 DNS 通信的接口。

步骤 7 输入取消反向 DNS 查找之前等待的秒数。

步骤 8 也可以单击**清除缓存 (Clear Cache)** 清除 DNS 缓存。

步骤 9 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。

邮件网关可以使用互联网协议版本 4 (IPv4) 和互联网协议版本 6 (IPv6) 静态路由。

可以使用 CLI 中的 routeconfig 命令或使用以下过程管理静态路由。

Procedure

步骤 1 依次选择**网络 (Network) > 路由 (Routing)**。
步骤 2 针对要创建的静态路由类型（IPv4 或 IPv6）单击**添加路由 (Add Route)**。
步骤 3 输入路由名称。
步骤 4 输入目标 IP 地址。
步骤 5 输入网关 IP 地址。
步骤 6 提交并确认更改。

配置默认网关

可以使用 CLI 中的 setgateway 命令或使用以下过程配置默认网关。

Procedure

步骤 1 依次选择**网络 (Network) > 路由 (Routing)**。
步骤 2 针对要修改的互联网协议版本单击路由列表中的**默认路由 (Default Route)**。
步骤 3 更改网关 IP 地址。
步骤 4 提交并确认更改。

配置 SSL 设置

可以使用“SSL 配置设置”(SSL Configuration Settings) 页面或 sslconfig 命令为邮件网关配置 SSL 设置。

Procedure

步骤 1 依次单击**系统管理 (System Administration)** > **SSL 配置设置 (SSL Configuration Settings)**。
步骤 2 单击**编辑设置 (Edit Settings)**。

Important 如果您已从较低的 AsyncOS 版本（例如，12.0 或 12.1）升级，则 AsyncOS 14.x 及更高版本中的默认 SSL 密码将更改如下：

- 对于 **GUI HTTPS**-

```
AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:
!aNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA
```

- 对于入站 **SMTP** -

```
AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:
!aNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA
```

- 对于出站 **SMTP** -

```
ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:AES256:!SRP:
!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:!eNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT
:-IDEA:!DHE-RSA-AES256-SHA
```

步骤 3 根据您的要求，执行以下操作：

- 设置 GUI HTTPS SSL 设置。在 GUI HTTPS 下，指定要使用的 SSL 方法和密码。
- 设置入站 SMTP SSL 设置。在入站 SMTP 下，指定要使用的 SSL 方法和密码。
- 设置出站 SMTP SSL 设置。在出站 SMTP 下，指定要使用的 SSL 方法和密码。
- 设置其他 TLS 客户端服务。在“其他 TLS 客户端服务”(Other TLS Client Services) 下，如果您的邮件网关处于非 FIPS 模式，则会默认禁用 TLS v1.0 方法。您可以在邮件网关上为 TLS 客户端服务“LDAP”和“Updater”启用 TLS v1.0 方法。

请记住：

- [在非 FIPS 模式下]您不能同时启用 TLS v1.0 和 v1.1 方法。但是，可以结合 TLS v1.2 方法启用这些方法。
- 如果计划在启用了 TLS v1.0 的非 FIPS 模式下从较低的 AsyncOS 版本（例如 12.x 或 13.0）升级到 AsyncOS 13.5.1 及更高版本，则会默认禁用 TLS v1.0。您需要在升级后在邮件网关上启用 TLS v1.0 方法。
- 从 AsyncOS 13.5.1 及更高版本开始，不再支持 SSLv2 和 SSL v3 方法。
- 如果邮件网关处于 FIPS 模式下，则不支持 TLS v1.0 方法。
- 如果邮件网关处于非 FIPS 模式下，则会默认禁用 TLS v1.0 方法。

步骤 4 [可选]选中**启用 (Enable)** 复选框，以允许邮件网关对“TLS 警报”、“出站 SMTP”、“更新程序”和“LDAP”服务器服务的对等证书执行 FQDN 验证。

步骤 5 [可选]选中**启用 (Enable)** 复选框，以允许邮件网关对“TLS 警报”、“出站 SMTP”、“更新程序”和“LDAP”服务器服务的对等证书执行 X.509 验证。

步骤 6 单击**提交 (Submit)**。

步骤 7 单击**确认更改 (Commit Changes)**。

使用 SAML 2.0 的单点登录 (SSO)

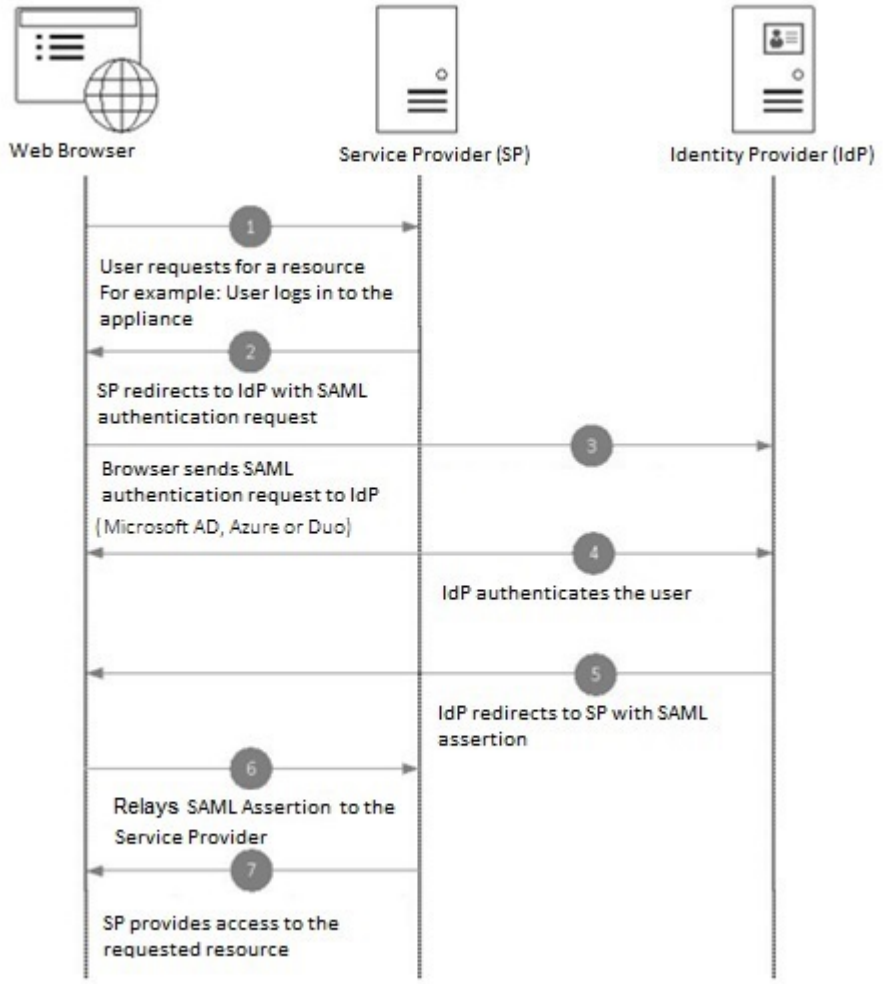
关于单点登录 (SSO) 和 SAML 2.0

邮件网关现在支持 SAML 2.0 SSO，以便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登录邮件网关设备的 Web 界面。例如，如果您启用 Duo、Microsoft AD FS 或 Azure 作为 SAML 身份提供程序 (IdP)，则可以将邮件网关配置为服务提供商 (SP) 以支持 SAML 2.0 SSO。用户可以一次登录，并访问所有 SAML 2.0 SSO 启用的服务。

SAML 2.0 SSO 工作流

SAML 2.0 SSO 工作流显示在下图中：

图 *3: SAML* 工作流



SAML 2.0 的准则和限制

总则

您只能在图形用户界面 (GUI) 上使用“使用 SAML 的单点登录”(Single Sign-On using SAML)。您可以使用 GUI 和命令行界面 (CLI) 来配置 SAML 配置文件。

您只能在邮件网关上配置服务提供商和身份提供程序的一个实例。

注销

当用户从邮件网关中注销时，他们不会从其他 SAML 2.0 SSO 启用的应用中注销。

限制

不能在群集级别配置 SAML 配置文件。所有 SAML 配置都限于计算机级别。

如何在邮件网关上配置 SSO

过程

	命令或操作	目的
步骤 1	查看先决条件。	前提条件，第 69 页
步骤 2	将邮件网关配置为服务提供程序。	将邮件网关配置为服务提供商，第 70 页
步骤 3	[在 IDP 上] 配置身份提供程序以便与您的邮件网关配合使用。	配置要与邮件网关通信的身份提供程序，第 72 页
步骤 4	配置邮件网关上的身份提供程序设置。	配置邮件网关上的身份提供程序设置，第 74 页
步骤 5	在邮件网关上使用SAML启用外部身份验证。	启用 SAML 身份验证

前提条件

- 支持的身份提供程序，第 69 页
- 用于安全通信的证书，第 69 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邮件网关的支持。以下是初步合格的身份提供程序：

- 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

注释 您可以使用任何标准 SAML 2.0 身份提供程序在邮件网关上通过使用 SAML 来配置 SSO。

用于安全通信的证书

获取保护邮件网关与身份提供程序之间通信所需的下列证书：

- 如果希望邮件网关对 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，然后将相同的证书导入邮件网关。您的邮件网关将使用此证书来验证已签名的 SAML 断言。

转换证书

要从邮件网关创建和导出证书，请参阅证书的使用。通常，从邮件网关获取的证书采用 .pfx 格式，当您将 邮件网关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，并导入从您邮件网关中获取的证书文件 (.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`

将邮件网关配置为服务提供商

注释 身份提供程序上的服务提供商设置是根据邮件网关上的服务提供商配置进行配置的。

开始之前

请确保查看前提条件，第 69 页。

过程

步骤 1 使用 Web 界面登录到您的邮件网关。

步骤 2 导航至**系统管理 (System Administration) > SAML**。

步骤 3 单击**添加服务提供商 (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（在本例中为您的邮件网关）。服务提供程序实体 ID 的格式通常为一个 URI。

字段	说明
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。在身份提供程序上配置服务提供商设置时，需要这些详细信息。
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。 断言使用者 URL 是用于访问您邮件网关的 URL。在身份提供程序上配置服务提供商设置时，需要这些详细信息。
SP 证书	您可以选择通过以下方式之一导入服务提供商证书： • 从下拉列表中选择邮件网关上可用的签名证书。 • 导入证书和相关的私钥。证书必须是 (.cert) 格式，而私钥必须是 (.key) 格式。 • 导入 PKCS #12 文件格式的证书。PKCS #12 格式的证书必须使用密码。 （可选）**签名身份验证请求** 如果希望设备对 SAML 身份验证请求进行签名，请执行以下操作： **1.** 上传从邮件网关和相关私钥中获取的证书。 您必须以 **(cert)** 格式上传证书。有关详细信息，请参阅用于安全通信的证书，第 69 页。 **2.** 输入私钥密码。 **3.** 选择**签名请求**。 （可选）**解密已加密的断言** 如果计划将身份提供程序配置为加密 SAML 断言： **1.** 上传从邮件网关和相关私钥中获取的证书。 **2.** 输入私钥密码。 **注释** 私钥必须采用 **.key** 格式。有关证书使用情况的信息，请参阅用于安全通信的证书，第 69 页。
签名断言	如果希望身份提供程序对 SAML 断言进行签名，请选择**签名断言**。 如果选择此选项，则必须将身份提供程序的证书添加到邮件网关中。请参阅配置邮件网关上的身份提供程序设置，第 74 页。
组织详细信息	输入组织的详细信息。身份提供程序将在错误日志中使用此信息。

字段	说明
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 单击**提交 (Submit)** 并确认更改。

步骤 6 记下“SSO 设置”页面上显示的服务提供商元数据（实体 ID 和断言客户 URL）以及在“服务提供商”页面上显示的名称 ID 格式。在身份提供程序上配置服务提供程序设置时，需要这些详细信息。

可以选择将元数据作为文件导出。配置设置之后，单击**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。

下一步做什么

配置要与您的邮件网关通信的身份提供程序。请参阅配置要与邮件网关通信的身份提供程序，第 72 页。

配置要与邮件网关通信的身份提供程序

开始之前

确保您：

- 已将邮件网关配置为服务提供程序。请参阅将邮件网关配置为服务提供商，第 70 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。请参阅将邮件网关配置为服务提供商，第 70 页。

过程

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（您的邮件网关）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。

如果已将邮件网关配置为对 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：

- 配置要与邮件网关通信的 AD FS，第 73 页。
- 配置要与邮件网关通信的 Duo Access Gateway，第 73 页。
- 配置要与邮件网关通信的 Azure AD，第 74 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

配置邮件网关上的身份提供程序设置。请参阅配置邮件网关上的身份提供程序设置，第 74 页。

配置要与邮件网关通信的 AD FS

以下是将 AD FS（2.0 及更高版本）配置为与您的邮件网关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（邮件网关的）断言消费者 URL 添加为中继方。
- 在“中继方信任”(Relaying Party Trusts) > “属性”(Properties) > “标识符”(Identifiers) > “中继方标识符”(Relaying Party Identifier) 下输入服务提供程序的（邮件网关的）的实体 ID。请确保此值与邮件网关上“运营商”(Service Provider) 设置中的“实体 ID”(Entity 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”(Relaying Party Trusts) >“属性”(Properties)>“加密”(Encryption) 下上传 .cer 格式的服务提供程序的（邮件网关的）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。

配置要与邮件网关通信的 Duo Access Gateway

以下是将 Duo Access Gateway 配置为与邮件网关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（邮件网关）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”(Duo Admin Panel) > “应用”(Applications) > “保护应用”(Protect an Application) > “SAML 服务提供商”(SAML Service Provider)”下，输入服务提供商（邮件网关）的实体 ID。请确保此值与邮件网关上“运营商”设置中的“实体 ID”值相同。
- 如果已将您的服务提供商（邮件网关）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（邮件网关的）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。

配置要与邮件网关通信的 Azure AD

以下是将 Azure AD 配置为与您的邮件网关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（邮件网关）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（邮件网关的）实体 ID。请确保此值与邮件网关上“运营商”设置中的“实体 ID”值相同。
- 如果您已将服务提供商（邮件网关）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。
- 在为“SAML > 用户和组”创建的 Azure 应用，下添加用户和/或组，以控制可以登录到此 Azure SAML 应用的用户。

配置邮件网关上的身份提供程序设置

开始之前

确保您：

- 已配置要与您的邮件网关通信的身份提供程序。请参阅配置要与邮件网关通信的身份提供程序，第 72 页。

- 已复制身份提供程序元数据详细信息，或已将身份提供程序元数据文件导出为文件。

过程

步骤 1 在 Web 界面上登录您的邮件网关。

步骤 2 导航至**系统管理 (System Administration) > SAML**。

步骤 3 单击**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	单击**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。

下一步做什么

启用 SAML 身份验证。

在 AsyncOS API 的邮件网关上配置 OpenID Connect 1.0

概述

思科安全邮件网关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，以便与邮件网关中可用的 AsyncOS API 进行无缝连接。目前，您的邮件网关仅使用 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，而邮件网关会被用作资源提供程序。

步骤：

1. [一次性活动] 配置邮件网关以验证访问令牌。有关详细信息，请参阅 在邮件网关上配置 OpenID Connect，第 77 页。
2. [一次性活动] 邮件网关根据步骤 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邮件网关。
5. 邮件网关会使用从第 2 步检索的密钥集来验证 API 请求中的访问令牌。
6. 邮件网关对访问令牌中的所需的声明（签发者、受众）进行验证。
7. 邮件网关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. 邮件网关会为 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：

```
Header
alg:RSA256
typ:JWT
[...]
Payload
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: erik.fernandes@customorg.com
claim: Role: LogCollector
claim: Role: ReadOnly
[...]
```

邮件网关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 配置邮件网关之前，请确保满足以下前提条件：

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

在邮件网关上配置 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，以便允许邮件网关执行所需的授权检查。

过程

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

步骤 2 单击**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 (Description)**
身份提供程序元数据 URL	输入用于获取 Open ID 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。 以下是签发者的示例 - http://example.com/adfs/services/trust。

OpenID Connect 参数	说明 (Description)
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，请单击**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，然后选择在邮件网关中配置的相应本地用户角色，以便映射这两个角色。 注释 如果要添加多个角色映射记录，请单击**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://esa.com/esa/api/v2.0/config/logs/subscriptions?retrievalMethod=manual'

--header 'Authorization: Bearer <add access_token here>’
```

系统时间

要在邮件网关上设置系统时间，请设置使用的时区，或者选择一个 NTP 服务器和查询接口，然后使用 GUI 中“系统管理”菜单中的“时区”或“时间设置”页面或使用 CLI 中的以下命令：ntpconfig、settime 和 settz。

也可以在**系统管理 (System Administration) > 时间设置 (Time Settings)** 页面上或使用 tzupdate CLI 命令验证 AsyncOS 使用的时区文件。

选择时区

“时区”(Time Zone) 页面（可通过 GUI 中的“系统管理”(System Administration) 菜单访问）显示了您邮件网关的时区。可以选择特定的时区或 GMT 偏移。

Procedure

步骤 1 在**系统管理 (System Administration) > 时区 (Time Zone)** 页面中单击**编辑设置 (Edit Settings)**。

步骤 2 从下拉菜单中选择区域、国家/地区和时区。

步骤 3 提交并确认更改。

选择 GMT 偏移

Procedure

步骤 1 在**系统管理 (System Administration) > 时区 (Time Zone)** 页面中单击**编辑设置 (Edit Settings)**。

步骤 2 从区域列表中选择“GMT 偏移时间 (GMT Offset)”。

步骤 3 在“时区”(Time Zone) 列表中选择偏移。偏移是指为了达到 GMT（本初子午线）所必须增加/减去的小时数。小时前缀减号（“-”）表示本初本初子午线以东。加号（“+”）表示本初子午线以西。

步骤 4 提交并确认更改。

编辑时间设置

可以使用以下方法之一编辑邮件网关的时间设置：

- （推荐）使用网络时间协议 (NTP) 设置邮件网关系统时间, on page 79
- 手动设置邮件网关系统时间 , on page 80

（推荐）使用网络时间协议 (NTP) 设置邮件网关系统时间

这是建议的时间保留方法，特别是您的邮件网关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。

Procedure

步骤 1 导航到“系统管理”(System Administration) >“时间设置”(Time Settings) 页面。

步骤 2 单击**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，然后单击**添加行 (Add Row)**。可以添加多个 NTP 服务器。

步骤 5 要从列表中删除 NTP 服务器，请单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 提交并确认更改。

手动设置邮件网关系统时间

通常不建议使用此时间保留方法。而是使用网络时间协议服务器。

Procedure

步骤 1 导航到“系统管理”(System Administration) >“时间设置”(Time Settings) 页面。
步骤 2 单击**编辑设置 (Edit Settings)**。
步骤 3 在“时间保留方法”(Time Keeping Method) 部分，选择“手动设置时间”(Set Time Manually)。
步骤 4 输入月、日、年、小时、分钟和秒数。
步骤 5 选择上午或下午
步骤 6 提交并确认更改。

自定义视图

- 使用收藏夹页面 , on page 80
- 设置用户首选项, on page 81

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。

收件人	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”(My Favorites) 菜单选择**将此页面添加到我的收藏夹 (Add This Page To My Favorites)**。 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。
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。
查看或构建自定义报告页面	请参阅“我的控制面板”页面。

设置用户首选项

本地用户可以定义每个账户特定的首选项设置，如语言。当用户首次登录邮件网关时，默认应用这些设置。存储每个用户的首选项设置，无论用户从哪个客户机登录到邮件网关，首选项设置都相同。

如果用户更改了这些设置，但未确认这些更改，那么当用户重新登录时，这些设置将恢复为默认值。

Note 外部验证的用户不能使用此功能。这些用户可以直接从“选项”(Options) 菜单中选择语言。

Procedure

步骤 1 使用想要定义其首选项设置的用户账户登录到设备。

步骤 2 依次选择**选项 (Options) > 首选项 (Preferences)**。“选项”(Options) 菜单位于窗口的右上角。

步骤 3 单击**编辑首选项 (Edit Preferences)**。

步骤 4 配置设置：

首选项设置	说明
语言显示 (Language Display)	AsyncOS for Web 在 Web 界面和 CLI 中使用的语言。
登录页 (Landing Page)	用户登录到邮件网关后显示的页面。
显示的报告时间范围（默认值）(Reporting Time Range Displayed [default])	报告选项卡上显示的默认报告时间范围。
显示的报告行数 (Number of Reporting Rows Displayed)	默认情况下，系统显示的每个报告的数据行数。

步骤 5 提交并确认更改。

步骤 6 单击页面底部的**返回上一页 (Return to previous page)** 链接。

常规设置

您可以编辑邮件网关的以下常规设置：

- 覆盖 Internet Explorer 兼容模式, on page 81
- 在新 Web 界面上收集邮件网关的使用情况统计信息 , on page 82

覆盖 Internet Explorer 兼容模式

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。

Procedure

步骤 1 依次单击**系统管理 (System Administration)** > **常规设置 (General Settings)**。

步骤 2 选择**覆盖 IE 兼容模式 (Override IE Compatibility Mode)** 复选框。

步骤 3 提交并确认更改。

在新 Web 界面上收集邮件网关的使用情况统计信息

“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”，邮件网关将在新 Web 界面上收集邮件网关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邮件网关用户体验的见解。

默认情况下，邮件网关上启用了“使用情况分析”。如果要禁用“使用情况分析”，请执行以下操作：

Procedure

步骤 1 依次单击**系统管理 (System Administration)** > **常规设置 (General Settings)**。

步骤 2 清除**使用情况分析**复选框。

步骤 3 提交并确认更改。

配置 HTTP 信头长度的最大值

现在，可以使用 CLI 中的 `adminaccessconfig > maxhttpheaderfieldsize` 命令来配置发送到邮件网关的 HTTP 请求的 HTTP 信头长度最大值。

HTTP 信头字段大小的默认值为 4096 (4 KB)，最大值为 33554432 (32 MB)。

重启和查看服务引擎的状态

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

- 重启邮件网关上启用的服务引擎，而不必重新启动邮件网关。
- 查看邮件网关上启用的服务引擎的状态。

有关详细信息，请参阅《适用于思科安全邮件网关的 CLI 参考指南》。

接收和传送包含国际化域名 (IDN) 的邮件

邮件网关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，第 83 页
- 可使用邮件网关中的 IDN 域配置的功能，第 83 页

前提条件

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。

可使用邮件网关中的 IDN 域配置的功能

对于此版本，您**只能**在邮件网关中使用 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。
- **侦听程序配置设置**：

- 为入站或出站侦听程序中的默认域添加或编辑 IDN 域。
- 在 HAT 或 RAT 表中添加或编辑 IDN 域。
- 使用 IDN 域导出或导入 HAT 或 RAT 表。

- **邮件策略配置设置**
  - 在“传入邮件策略”(Incoming Mail Policies) 中使用 IDN 域添加或编辑发件人（“以下发件人”(Following Senders) 或“非以下发件人”(Following Senders are Not) 选项）和收件人（“以下收件人”(Following Recipients) 或“非以下收件人”(Following Recipients are Not) 选项）的域。
  - 在“传出邮件策略”(Outgoing Mail Policies) 中使用 IDN 域添加或编辑发件人（“以下发件人”(Following Senders) 或“非以下发件人”(Following Senders are Not) 选项）和收件人（“以下收件人”(Following Recipients) 或“非以下收件人”(Following Recipients are Not) 选项）的域。
  - 在传入或传出邮件策略中使用 IDN 域查找的发件人或收件人。
  - 使用 IDN 域定义发件人验证例外表。
  - 使用 IDN 域创建地址列表。
  - 使用 IDN 域添加或编辑目标域以进行目标控制。

- **退回配置文件配置设置**：使用 IDN 域添加或编辑备用邮件地址。
- **发件人域信誉配置设置**：定义 IDN 域的发件人域信誉得分。
- **IP 信誉配置设置**：定义 IDN 域的 IP 信誉得分。
- **LDAP 配置设置**：使用 IDN 域为传入和传出邮件创建 LDAP 组查询、接受查询、路由查询和伪装查询。
- **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病毒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。

注释 目前，只有在“垃圾邮件隔离区”(Spam Quarantine) 设置页面的“最终用户隔离区访问”(End-User Quarantine Access) 部分中将最终用户身份验证方式设置为“无”(None) 时，包含 IDN 域的收件人才能访问最终用户隔离区。

- **SPF 配置设置**：使用 IDN 域对邮件执行 SPF 验证。
- **DKIM 配置设置**：使用 IDN 域对邮件执行 DKIM 签名和验证
- **DMARC 配置设置**：使用 IDN 域对邮件执行 DMARC 验证。