思科安全邮件网关使用入门

本章包含以下部分：

AsyncOS 14.2 中的新增功能

表 *1: AsyncOS 14.2* 中的新增功能

特性	说明
发件人成熟度	在此版本中，传统的发件人域信誉（SDR）域期限功能被替换为发件人成熟度。发件人成熟度是建立发件人信誉的重要功能。发件人成熟度是根据多个信息源自动生成的，用于垃圾邮件分类，可能不同于“基于 Whois 的域期间。” “发件人成熟度”表示思科 Talos 认为域作为邮件发件人的成熟度。调整成熟度值可以启用有关邮件的威胁检测，并且通常不会反映“基于 Whois 的域有效期”中表示的域有效期。 发件人成熟度被设为 30 天限制，如果超过该限制，域就会被视为邮件发件人的成熟地址，并且不会提供进一步的详细信息。 **注释** 从此版本开始，“SDR 域期限”配置的过滤器将自动更新为“SDR 发件人成熟度”过滤器。升级后，发件人成熟度值无效的过滤器将被标记为“非活动”。确保相应地查看和修改消息和内容过滤器。 发件人成熟度用于计算发件人信誉。未成熟域的信誉较低。思科 Talos 建议您仅依靠发件人信誉来确定策略操作。对于特定的非标准场景，发件人成熟度会用于优化过滤器。 **注释** 思科 Talos 不会手动调整域的成熟度，而是依靠自动化系统和传感器来确定最合适的值。 有关详细信息，请参阅发件人域信誉过滤。

特性	说明
新发件人域信誉判定	从此版本开始，将更新发件人域信誉判定，以准确反映预期含义和建议使用。 在升级期间，系统会自动更新发件人域信誉消息或内容过滤器配置，以反映新的判定。确保相应地查看和配置邮件或内容过滤器。 以下旧版 SDR 判定映射到新 SDR 判定： • “糟糕”到“不受信任” • “差”到“可疑” • “已污染”或“弱”至“中性” • 从“中立”到“优先” • “良好”到“可信” • “未知”到“未知” **注释** 已更新 SDR 报告和跟踪 AsyncOS API 以反映新的 SDR 威胁级别和类别结构。 **注释** SDR 邮件和跟踪日志已更新，以反映新的 SDR 威胁级别和发件人成熟度详细信息。 有关详细信息，请参阅发件人域信誉过滤。
发件人域信誉 (SDR) 过滤提升	在此版本中，SDR 服务的用户体验和整体质量通过性能改进，可用性提高和SDR部署得到增强。
文件分析报告的分组的提升	邮件网关现在使用智能账户 ID 对组织中的设备进行分组，并查看所有设备的文件分析结果。 在邮件网关上启用智能许可并配置设备组进行文件分析报告时，系统会自动将智能账户 ID 注册为设备组 ID。您可以随时更改设备组 ID，更改会立即生效，无需执行“提交”操作。 有关详细信息，请参阅（仅公共云文件分析服务）配置设备组。

特性	说明
智能软件许可增强功能	以下是智能软件许可功能的增强功能： • **许可证预留**：您可以为在邮件网关中启用的功能预留许可证，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邮件网关且不与互联网或外部设备通信的受保护用户。 有关详细信息，请参阅概述和预留功能许可证。 • **设备LED转换**：使用智能许可注册邮件网关后，所有现有的有效传统许可证将使用设备 LED 转换（DLC）过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。 有关详细信息，请参阅概述。
用于目标控制的 TLS 证书增强	您现在可以为特定域选择除“默认”目标控制条目中配置的证书以外的其他证书。 您可以通过以下方式之一选择不同证书： • 编辑相应的目标控制条目，并使用 Web 界面中的 TLS 证书选项选择其他证书。 • 在创建或编辑目标控制条目时，使用 CLI 中的 `destconfig` > 新建 或 编辑 子命令选择证书。 有关详细信息，请参阅控制 TLS。
修改经典许可 - Web 界面和 CLI 中的到期日期	从此版本开始，传统许可的 Web 界面和 CLI 中现有的“到期日期”列标题进行了如下修改：“到期日期（包括宽限期）”，以指示宽限期包含在到期日期中。 **注释** 修改所有警报消息和邮件日志以显示到期日期，包括功能密钥的宽限期。

Web 界面比较（新 Web 界面与旧 Web 界面）

下表显示了新 Web 界面与旧版界面的比较：

表 *2:* 新 *Web* 界面与旧版界面的比较

Web 界面页面或元素	新 Web 界面	旧 Web 界面
登录页面	登录到邮件网关后，系统将显示“邮件流摘要”(Mail Flow Summary) 页面。	登录到邮件网关后，系统将显示“我的控制板”(My Dashboard) 页面。

Web 界面页面或元素	新 Web 界面	旧 Web 界面
“报告”下拉列表	您可以从“报告”(Reports) 下拉列表中查看邮件网关的报告。	您可以从**监控 (Monitor)** 菜单查看邮件网关的报告。
“我的报告”页面	从“报告”下拉列表中选择**我的报告**。	您可以从**监控 (Monitor) > 我的控制面板 (My Dashboard)** 查看“我的报告”(My Reports) 页面。
“邮件流摘要”页面	**邮件流摘要**页面包括传入邮件和传出邮件的趋势图和摘要表。	**传入邮件**包括传入和传出邮件的图和摘要表。
“高级恶意软件保护”报告页面	以下各部分在“报告”菜单的**高级恶意软件保护**报告页面上可用： • 摘要 • AMP 文件信誉 • 文件分析 • 文件追溯 • 邮箱自动补救	邮件网关的**监控 (Monitor)** 菜单下具有以下**高级恶意软件保护 (Advanced Malware Protection)** 报告页面： • 高级恶意软件防护 • AMP 文件分析 • AMP 判定更新 • 邮箱自动补救
“爆发过滤器”页面	“过去一年病毒爆发”和“过去一年病毒爆发摘要”在新 Web 界面的**爆发过滤 (Outbreak Filtering)** 报告页面中不可用。	**监控 (Monitor) > 病毒爆发过滤器 (Outbreak Filters)** 页面显示“过去一年病毒爆发”(Past Year Virus Outbreaks) 和“过去一年病毒爆发摘要”(Past Year Virus Outbreak Summary)。
垃圾邮件隔离区（管理和最终用户）	在新 Web 界面中单击**隔离区 (Quarantine) > 垃圾邮件隔离区 (Spam Quarantine) > 搜索 (Search)**。 最终用户可以使用以下 URL 访问垃圾邮件隔离区： https://example.com:<https-api-port>/euq-login 其中，`example.com` 是设备主机名，`<https-api-port>` 是防火墙上打开的 AsyncOS API HTTPS 端口。	您可以从**监控 (Monitor) > 垃圾邮件隔离区 (Spam Quarantine)** 菜单查看垃圾邮件隔离区。

Web 界面页面或元素	新 Web 界面	旧 Web 界面
策略、病毒和爆发隔离区	在新 Web 界面中单击**隔离区 (Quarantine) > 其他隔离区 (Other Quarantine)**。 在新 Web 界面中，您只能查看“策略”、“病毒”和“病毒爆发隔离区”。	在邮件网关上，您可以使用**监控 (Monitor) > 策略、病毒和病毒爆发隔离区 (Policy, Virus and Outbreak Quarantines)** 来查看、配置和修改策略、病毒和病毒爆发隔离区。
为隔离区中的邮件选择所有操作	您可以选择多个（或所有）邮件并执行邮件操作，例如删除、延迟、发布、移动等。	您不能选择多个邮件来执行邮件操作。
附件的最大下载限制	已隔离邮件的附件下载最大限制为 25 MB。	-
受拒连接数	要搜索已拒绝连接，请单击上的**跟踪 (Tracking) > 搜索 (Search) > 已拒绝连接 (Rejected Connection)** 选项卡。	-
查询设置	邮件跟踪功能的查询设置字段在上不可用。	您可以在“邮件跟踪”功能的“查询设置”字段中设置查询超时。
邮件跟踪数据可用性	单击 Web 界面页面右上方的齿轮图标，以访问“邮件跟踪数据可用性”(Message Tracking Data Availability) 页面。	您可以查看邮件网关缺少数据的时间间隔。
显示邮件的更多详细信息	您可以查看邮件的更多详细信息，例如判定图表、上次状态、发件人组、发件人 IP、IP 信誉得分和策略匹配详细信息。	-
判定图表和上次状态判定	判定图表显示由邮件网关中的每个引擎触发的各种可能判定的信息。 邮件的“上次状态”决定了在引擎的所有可能判定之后触发的最终判定。	邮件的判定图表和上次状态判定不可用。
邮件详细信息中的邮件附件和主机名	在邮件网关上邮件的“邮件详细信息”部分，不显示邮件附件和主机名。	邮件附件和主机名显示在邮件的“邮件详细信息”部分。

Web 界面页面或元素	新 Web 界面	旧 Web 界面
邮件详细信息中的发件人组、发件人 IP、IP 信誉得分和策略匹配	邮件的发件人组、发件人 IP、IP 信誉得分和策略匹配的详细信息显示在邮件网关的“邮件详细信息”(Message Details) 部分中。	邮件的发件人组、发件人 IP、IP 信誉得分和策略匹配在邮件的“邮件详细信息”部分不可用。
邮件方向（传入或传出）	邮件网关的“邮件跟踪结果”页面显示邮件方向（传入或传出）。	“邮件跟踪结果”页面不显示邮件方向（传入或传出）。

哪里可以获得详细信息

思科提供以下资源用于了解有关邮件网关的更多信息：

- 文档 , on page 7
- 培训, on page 8
- 思科通知服务 , on page 8
- 知识库, on page 8
- 思科支持社区, on page 9
- 思科客户支持, on page 9
- 第三方贡献者, on page 9
- 思科欢迎您发表意见, on page 9
- 注册思科账户 , on page 10

文档

可通过单击右上角的“帮助和支持”(Help and Support)，直接从设备 GUI 访问联机帮助版本的用户手册。

思科安全邮件网关的文档集包括以下文档和手册：

- 版本说明
- 思科邮件安全设备模型快速入门指南
- 所用型号或系列的硬件安装或硬件安装与维护指南
- 思科内容安全虚拟设备安装指南
- 适用于思科安全邮件网关思科邮件安全设备的 *AsyncOS* 用户指南（本手册）
- 《适用于思科安全邮件网关的 *AsyncOS CLI* 参考指南》
- 《使用思科安全邮件网关的 AsyncOS API - 入门指南》

所有思科内容安全产品的文档均可从以下位置获取：

思科内容安全产品的文档	位置
硬件和虚拟设备	请参阅此表中适用的产品。

思科内容安全产品的文档	位置
思科邮件安全	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd- products-support-series-home.html
思科网络安全	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products- support-series-home.html
思科内容安全管理	http://www.cisco.com/c/en/us/support/security/content-security-management- appliance/tsd-products-support-series-home.html
适用于思科内容安全设备的 CLI 参考指南	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
思科 IronPort 加密	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html

培训

有关培训的详细信息可从以下网址获得：

- http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html
- http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

思科通知服务

注册以接收与思科内容安全设备相关的通知，如安全建议、现场通知、销售终止或支持终止声明，以及有关软件更新和已知问题的信息。

您可以指定通知接收频率和要接收的信息类型等选项。您必须为您所用的每种产品单独注册。

要进行注册，请访问 http://www.cisco.com/cisco/support/notifications.html

需要 Cisco.com 账户才能注册。如果没有，请参阅注册思科账户 , on page 10。

知识库

Procedure

步骤 1 转到主产品页面 (http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html)

步骤 2 查找名称中包含 **TechNotes** 的链接。

思科支持社区

思科支持社区是一个面向思科客户、合作伙伴和员工的在线论坛。它提供了一个讨论常规邮件和网络安全问题以及有关具体思科产品的技术信息的场合。您可以在论坛中发布主题，以咨询问题并与其他用户分享信息。

请通过以下 URL 访问客户支持门户上的思科支持社区：

- 针对邮件安全和相关管理：

  https://supportforums.cisco.com/community/5756/email-security

- 针对网络安全和相关管理：

  https://supportforums.cisco.com/community/5786/web-security

思科客户支持

Cisco TAC：http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

旧版 IronPort 的支持站点：http://www.cisco.com/c/en/us/services/acquisitions/ironport.html

对于普通问题，您还可以从邮件网关上访问客户支持。有关说明，请参阅用户指南或在线帮助。

第三方贡献者

有关与您的版本对应的开源代码授权信息，请访问以下页面：
http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-release-notes-list.html。

Cisco AsyncOS 的某些软件根据 FreeBSD, Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives, Inc. 及其他第三方贡献者的软件许可协议条款、通知和条件分发，所有此类条款和条件均包含在思科许可协议当中。

这些协议的全文可通过以下网站查看：

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html。

经 Tobi Oetiker 明确书面同意，Cisco AsyncOS 的部分软件基于 RRDtool。

本文档中部分相关内容的复制已取得 Dell Computer Corporation 的许可。本文档中部分相关内容的复制已取得 McAfee, Inc. 的许可。本文档中部分相关内容的复制已取得 Sophos Plc 的许可。

思科欢迎您发表意见

思科技术出版物团队乐于将努力提高产品文档的质量。我们时刻欢迎您的评论和建议。您可以将评论发送至以下邮件地址：

contentsecuritydocs@cisco.com

请在邮件主题中提供产品名称、版本号和文档发布日期。

注册思科账户

要访问 Cisco.com 上的许多资源，都需要有思科账户。

如果您没有 Cisco.com 用户 ID，可以在此注册一个账户： https://idreg.cloudapps.cisco.com/idreg/register.do

相关主题

- 思科通知服务 , on page 8
- 知识库, on page 8

思科安全邮件网关概述

AsyncOS™ 操作系统包括以下功能：

- 网关处的**反垃圾邮件**，通过 SenderBase 信誉过滤器和思科反垃圾邮件集成的独特多层方法。
- 网关处的**防病毒**，使用 Sophos 和 McAfee 防病毒扫描引擎。
- **病毒爆发过滤器™**，思科针对新病毒、诈骗和网络钓鱼爆发提供的独特预防保护，可以隔离危险邮件，直到应用新的更新，从而缩短新邮件威胁的漏洞窗口。
- **策略、病毒和病毒爆发隔离区**提供一个安全的位置来存储可疑邮件供管理员评估。
- 内部或外部的**垃圾邮件隔离区**，使最终用户可以访问隔离的垃圾邮件和疑似垃圾邮件。
- **邮件身份验证**。Cisco AsyncOS 支持各种不同形式的邮件身份验证，包括传入邮件的发件人策略框架 (SPF)、发件人 ID 框架 (SIDF) 和 DomainKeys 确定的邮件 (DKIM) 验证，以及传出邮件的 DomainKeys 和 DKIM 签名。
- 思科**邮件加密**。可以加密传出邮件以满足 HIPAA、GLBA 或类似的管理需求。为此，需要在邮件网关上配置加密策略并使用本地密钥服务器或托管密钥服务来加密邮件。
- **邮件安全管理器**，一个综合控制面板，用于管理邮件网关中的所有邮件安全服务和应用。邮件安全管理器可以基于用户组实施邮件安全，以便通过不同的入站和出站策略管理思科信誉过滤器、病毒爆发过滤器、反垃圾邮件、防病毒和邮件内容策略。
- **机上邮件跟踪**。AsyncOS for Email 包含机上邮件跟踪功能，可帮助轻松获取邮件网关所处理邮件的状态。
- 针对所有入站和出站邮件的**邮件流监控**，用于全面了解企业的所有邮件流量。
- 基于发件人的 IP 地址、IP 地址范围或域，针对入站发件人的**访问控制**。
- 广泛的**邮件和内容过滤**技术，用于实施公司策略并在特定邮件进入或离开公司基础设施时执行相应操作。过滤器规则根据邮件或附件内容、有关网络的信息、邮件信封、邮件信头或邮件正文识别邮件。过滤器操作允许删除、退回、存档、密件复制或更改邮件，或者生成通知。
- **通过传输层安全使用安全 SMTP 进行邮件加密**可确保加密在公司基础设施与其他可信主机之间传输的邮件。
- **Virtual Gateway™** 技术允许邮件网关在单个服务器中用作多个邮件网关，以便划分不同来源或活动中的邮件以通过单独的 IP 地址发送。这样可以确保影响一个 IP 地址的可传送性问题不会影响其他 IP 地址。
- **防止恶意附件和链接**（在邮件中），由多个服务提供。
- 使用**防数据丢失**控制和监控从组织传出的信息。

AsyncOS 支持符合 RFC 2821 标准的简单邮件传输协议 (SMTP)，以接受并传输邮件。

大多数报告、监控和配置命令都可通过基于 Web 的 GUI 和 HTTP 或 HTTPS 使用。此外，还为系统提供了从 Secure Shell (SSH) 或直接串行连接访问的交互式命令行界面 (CLI)。

您还可以设置思科安全邮件和 Web 管理器，以统一管理多个邮件网关的报告、跟踪和隔离管理。

相关主题

- 支持的语言, on page 11

支持的语言

AsyncOS 可使用以下任何语言显示其 GUI 和 CLI：

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

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。