简介

本章包含以下部分：

此版本中的新增功能

本部分介绍了此版本思科内容安全管理 AsyncOS 中的新增功能和增强功能。

表 *1: AsyncOS 14.1* 中的新增内容

功能	说明
新系统运行状况控制板	在 AsyncOS 14.0 中，您现在可以在页面中查看网络安全设备的当前状态和配置。您必须选择“监控”(Monitoring) > “系统运行状况”(System Health) 来监控网络安全设备的系统状态。 有关详细信息，请参阅 新 Web 界面中的系统运行状况控制面板。
导出跟踪数据	在 AsyncOS 14.1.0 中，导出跟踪已增强为： • 查看其他字段，使用“导出文件”(Export file) 选项以及邮件详细信息对相关邮件执行分析和调查。 • 执行导出时，您可以查看的最大行数现已被设为 50000。 有关详细信息，请参阅导出邮件服务。
隔离区自定义访问角色	管理员可以为隔离区邮件创建具有只读选项的自定义角色。只读选项可防止用户删除或释放邮件，并且仅对隔离区具有只读访问权限。

功能	说明
垃圾邮件隔离区阈值警报	当在指定持续时间内隔离一定数量的垃圾邮件时，AsyncOS 14.1.0 会发送警报。警报也会在生成的系统日志中输入。此外，思科安全邮件和 Web 管理器会在达到隔离阈值时触发警报。
单一平台	通过 AsyncOS 14.1.0，您可以节省更多时间，而无需在多个思科安全邮件和 Web 管理器中重复登录。您可以在主设备上查看各个思科安全邮件和 Web 管理器的报告、跟踪和隔离页面。要执行此操作，您可以从“跟踪、报告和隔离”(Tracking, Reporting, and Quarantine) 页面上列出的下拉列表中选择所需的思科安全邮件和 Web 管理器。 有关详细信息，请参阅 单一平台。
智能许可重新注册	您可以根据以下任一场景向思科云服务门户重新注册思科安全邮件和 Web 管理器： • 如果在自动向思科云服务门户注册邮件网关时无法查看或管理添加到思科云服务门户的设备。 • 如果在自动向思科云服务门户注册设备时，智能账户和思科云服务帐户尚未关联。 有关详细信息，请参阅 向思科云服务门户重新注册。
系统日志推送的新参数 - 日志检索方法	以下是在思科安全邮件和 Web 管理器中配置系统日志推送日志检索方法所需的新参数： • 远程系统日志服务器的端口号。 • 发送到远程系统日志服务器的日志消息的最大大小。 • [仅限 TCP 协议]：思科安全邮件和 Web 管理器与远程系统日志服务器之间的 TLS 连接。

表 *2: AsyncOS 14.0* 中的新增内容

功能	说明
增强的概述和传入邮件报告页面	以下是设备旧 Web 界面中的“传入邮件”(Incoming Mail) 报告页面的增强功能： 传入邮件 (Incoming Mail) 报告页面： 添加了新的列-“传入邮件详细信息”（Incoming Mail Details）部分中的“由域信誉过滤拦截”(Stopped by Domain Reputation Filtering)。 在“传入邮件详细信息”(Incoming Mail Details) 部分中，将“由信誉过滤拦截”(Stopped by Reputation Filtering) 列名更改为“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering)。 有关详细信息，请参阅使用集中邮件安全报告
新系统运行状况控制板	您现在可以在页面中查看网络安全设备的当前状态和配置。您必须选择**监控 (Monitoring)** > **系统运行状况 (System Health)** 来监控网络安全设备的系统状态。 有关详细信息，请参阅 新 Web 界面中的系统运行状况控制面板。
证书的使用	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 • 自定义列表 有关详细信息，请参阅常规管理任务

功能	说明
智能许可	在启用和注册智能许可时，将启用云服务并自动注册设备。 • 为了启用或禁用思科 SecureX和思科威胁响应，generalconfig 命令下引入了该选项。 • 命令 Threstresponseconfig 将显示警告消息“输入通用配置命令以启用/禁用思科 SecureX/威胁响应功能”(Enter general config command to Enable/Disable of Cisco SecureX/ Threat Response feature)。 • 引入命令 smartaccountinfo 来获取智能帐户信息。 • 在启用 CloudServices 时，思科 SecureX 将自动启用，而在禁用 CloudServices 时也将禁用思科 Securex。 有关详细信息，请参阅与思科 SecureX 或思科威胁响应集成。
在内容安全网关上启用思科 SecureX 或威胁响应	您必须使用常规配置设置在内容安全网关上启用思科 SecureX 或威胁响应。 有关详细信息，请参阅与思科 SecureX 或思科威胁响应集成。
邮件策略详细信息的新报告	新报告 – 在设备的新 Web 界面中添加了邮件策略详细信息。使用此报告可查看与已配置的邮件策略匹配的邮件数量。 有关详细信息，请参阅使用集中邮件安全报告
对思科威胁响应中的邮件执行补救操作	在思科威胁响应中，您现在便可对设备处理的邮件进行调查并采取以下补救操作： • 删除 • 转发 • 转发并删除 有关详细信息，请参阅与思科 SecureX 或思科威胁响应集成。

功能	说明
支持国际化域名 (IDN)	AsyncOS 14.0 现在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。 有关详细信息，请参阅简介，第 1 页
垃圾邮件通知	包含了一个新字段“自定义徽标位置”(Custom Logo Position)，您可以将相同的徽标添加到垃圾邮件通知邮件的指定位置。
对产品及相关文档进行品牌更名	我们将产品和相关文档从“思科内容安全管理”更名为“思科安全邮件和 Web 管理器”。
密码	您的邮件和网络管理器中添加了新的密码规则，用于定义您的登录密码： 有关详细信息，请参阅常规管理任务
FQDN	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 有关详细信息，请参阅常规管理任务

思科内容安全管理概述

思科内容安全管理 AsyncOS 包含以下功能：

- **外部垃圾邮件隔离区**：为最终用户保存垃圾邮件和可疑垃圾邮件，并且使最终用户和管理员可以在做出最终决定之前审核被标为垃圾邮件的邮件。

- **集中策略、病毒和病毒爆发隔离区**：提供单一界面来管理多个邮件安全设备的隔离区和其中隔离的邮件。允许将隔离的邮件存储在防火墙后。
- **集中报告**：从多个邮件和网络安全设备运行有关汇聚数据的报告。各个设备上可用的相同报告功能在安全管理设备上也可用。
- **集中跟踪**：使用单个界面跟踪由多个邮件和网络安全设备处理的邮件和网络事务。
- **网络安全设备的集中配置管理**：为保持简单性和一致性，集中管理多个网络安全设备的策略定义和策略部署。

Note 安全管理设备不涉及集中邮件管理或邮件安全设备“集群”。

- **集中化升级管理**：您可以使用单个安全管理设备 (SMA) 同时升级多个网络安全设备 (WSA)。
- **数据备份**：在安全管理设备中备份数据，包括报告和跟踪数据、隔离的邮件及安全和阻止的发件人列表。
- **支持国际化域名 (IDN)**：AsyncOS 14.0 现在可以接收和传送包含 IDN 域的邮件地址的邮件。目前，您的内容安全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。

对于此版本，您只能在内容安全网关中使用 IDN 域来配置很少的功能。

- SMTP 路由配置设置 - 添加或编辑 IDN 域，使用 IDN 域来导出或导入 SMTP 路由。
- 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、病毒和病毒爆发隔离区配置设置：查看由防病毒引擎确定的包含可能正在传输恶意软件的 IDN 域的邮件，查看由病毒爆发过滤器作为潜在垃圾邮件或恶意软件捕获的包含 IDN 域的邮件，查看由邮件过滤器、内容过滤器和 DLP 邮件操作捕获的包含 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的包含 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。

可以从单个安全管理设备中协调安全操作，也可以在多个设备之间分布负载。