简介

本章包含以下部分：

- 此版本中的新增功能 ， 第 1 页
- 思科 思科安全邮件和 Web 管理器概述, on page 5

此版本中的新增功能

本部分介绍了此版本思科 安全邮件和 Web 管理器的 AsyncOS 中的新增功能和增强功能。

表 *1: AsyncOS 15.0* 中的新增功能

特性	说明
[仅限本地] FIPS 认证	思科安全邮件和 Web 管理器已经通过 FIPS 认证，并已集成以下 FIPS 140-2 认可的加密模块：思科通用加密模块（FIPS 140-2 认证#4036）。 **注释** 思科安全邮件和 Web 管理器 FIPS 认证仅适用于邮件网关集成，而不适用于安全 Web 设备集成。 **注释** 如果安全邮件和 Web 管理器处于 FIPS 模式下，则不支持 TLS v1.0 方法。 有关详细信息，请参阅FIPS 管理。
单日志行 (SLL)	SLL 功能可创建、索引邮件跟踪数据并将其存储为单个日志行或展平模型。因此，您可以执行查询并快速获得响应。此功能通过快速响应、低内存和 CPU 使用率来提高跟踪查询或搜索性能。 此功能仅适用于升级后的邮件跟踪数据。

特性	说明
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。 您可以使用以下方式配置 CRL 源： • 在旧 Web 界面中导航至**网络 (Network)** >**CRL 源 (CRL Sources)** > **添加 CRL 源 (Add CRL Source)** > **添加 CRL**（**证书撤销列表**）**源 (Add CRL [Certificate Revocation Lists] Source)** 窗口。 • 在 CLI 中使用 `Certconfig` > `CRL` 子命令。 有关配置 CRL 源的详细信息，请参阅配置 CRL 源。

特性	说明
删除旧的 Splunk 数据	当您升级到思科安全邮件和 Web 管理器 15.0 及更高版本时，如果邮件跟踪数据包含在Splunk数据库中，那么倘若继续升级，系统将删除 Splunk 数据库和二进制文件。 **注释** 从思科安全邮件和Web管理器13.6.2版开始，Splunk数据库不再用于存储邮件跟踪数据。所有新的邮件跟踪数据都将存储在 Lucene 数据库中。在升级到思科安全邮件和网络管理器 15.0 后，升级到思科安全邮件和网络管理器13.6.2之前的所有跟踪数据都将被删除，并且无法恢复。 在升级到思科安全邮件和Web管理器15.0及更高版本的过程中，CLI 或安全邮件和 Web 管理器的 Web 界面上会显示一条警告消息，指示系统将删除 Splunk 数据库。 **警告消息示例** 从思科安全邮件和网络管理器 *13.6.2* 版本开始，我们已将邮件跟踪数据移至较新的存储系统。通常，旧数据会自动替换为新存储系统中的新数据。但是，在某些情况下（例如，延迟升级、低邮件流量和跟踪数据等），旧存储系统中可能仍会存在不再支持的旧数据的痕迹。 您的情况是 *19 MB*，最后一次更新是在 *2022* 年 *8* 月 *11* 日。 您可以备份邮件跟踪数据（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，请参阅用户手册的“常见管理任务”一章中的“计划单次备份或定期备份”部分。 如果您继续执行此升级过程，那么您的 *Splunk* 邮件跟踪数据将被删除。 您可以选择继续升级或中止升级。 您同意继续进行此升级吗*? [Y]"* **注释** 警告消息仅对本地管理员用户显示。 **注释** 用于收集 Splunk 数据库调试信息的 **debug** 子菜单将从 CLI 中的`Diagnostic > Tracking` 子命令中删除。

特性	说明
重置对初始制造商值的网络配置	现在，您可以使用 `Diagnostic > Reload` 子命令将网络配置重置为初始制造商值。 `Diagnostic > Reload` 子命令可恢复出厂配置并清除用户配置。此子命令会完全擦除现有的用户和配置数据。因此，您可以对这些设备使用与新设备相同的安装和配置方法。 显示最后一个 Reload 子命令的执行状态的新子命令 Reload Status 已被添加到 Diagnostic 命令中。 有关这些子命令的详细信息，请参阅 Diagnostic - Reload 子命令 和 Diagnostic - Reload Status 命令。
在 TLS 通信期间为对等证书执行 X.509 验证	您可以将安全邮件和 Web 管理器配置为对对等证书执行 X.509 验证。X.509 验证适用于以下服务： • 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 • SSE 连接器 • SSE 服务器 有关详细信息，请参阅 X.509 证书。
思科安全邮件和 Web 管理器虚拟设备型号的新 RAM 值	从 AsyncOS 15.0 版本开始，通过 KVM 或 VMWare ESXi 部署的 M600v 安全邮件和 Web 管理器虚拟设备模型会有一个新的 RAM 值。 有关适用于虚拟设备型号的新 RAM 值的详细信息，请参阅《思科内容安全虚拟设备安装指南》，网址为：https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html

特性	说明
[仅限本地] Azure 平台的第 2 代部署支持	从 AsyncOS 15.0 版本开始，安全邮件和 Web 管理器支持 Azure 的第 2 代部署。 **注释** Azure 第 2 代部署支持的型号仅限 **M600V**。 **注释** 在 Azure 平台上部署后，第 2 代映像无法启动。部署第 2 代映像后，您必须重新启动虚拟机。 有关 Azure 平台上的第 2 代部署的详细信息，请参阅思科安全邮件虚拟网关和 Azure 上的思科安全邮件和 Web 管理器虚拟部署指南，网址为：https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html。
[仅限本地] Microsoft Hyper-V Server 2019 支持	思科安全邮件和 Web 管理器 15.0 支持 Microsoft Hyper-V Server 2019。
[仅限本地] Hyper-V 的第 2 代部署支持	从 AsyncOS 15.0 版本开始，思科安全邮件和 Web 管理器仅支持 Hyper-V 的第 2 代部署。 **注释** Hyper-V 第 2 代部署支持的型号仅限 **M600V**。 有关详细信息，请参阅《思科内容安全虚拟设备安装指南》，网址为：https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html。
[仅限本地] 支持的 AWS 部署模式	从 AsyncOS 15.0 版本开始，支持 AWS 部署的型号仅限 **M600V**。 有关更多信息，请参阅《Amazon Web 服务指南》中的“在亚马逊弹性计算云上部署思科安全邮件网关、安全 Web 以及 安全邮件和 Web 管理器虚拟设备”，网址为：https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html。

思科 思科安全邮件和 Web 管理器概述

面向思科 安全邮件和 Web 管理器的 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 邮件网关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思科安全邮件和 Web 管理器设备上也可用。
- **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 思科安全邮件和 Web 管理器设备不涉及集中邮件管理或 邮件网关“集群”。

- **集中化升级管理**：您可以使用单个 思科安全邮件和 Web 管理器设备 (SMA) 同时升级多个网络安全设备 (WSA)。
- **数据备份**：在思科安全邮件和 Web 管理器设备中备份数据，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。

您可以从单个思科安全邮件和 Web 管理器设备中协调安全操作，也可以在多个设备之间分布负载。

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。