思科邮件安全设备 AsyncOS 9.1 版本说明

发布日期：2015 年 3 月 30 日
修订日期：2016 年 7 月 6 日

目录

新增内容

特性	说明
FIPS 认证	思科邮件安全设备现已经过 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 认证编号 1643）。
文件分析隔离区增强功能	此版本可基于分析裁决，从内容安全管理设备的文件分析*集中*隔离区自动释放或删除邮件。 有关详细信息，请参阅思科内容安全设备 AsyncOS 9.1 的相关文档。

特性	说明
更新程序增强功能	思科邮件安全设备 AsyncOS 9.1 包含以下更新程序增强功能： • 邮件安全设备可在每次与思科更新程序服务器通信时，检查更新程序服务器证书的有效性。 • 如果您使用的是非透明代理服务器，则可以添加用于将代理证书签署到设备中的 CA 证书。这样，设备就会信任代理服务器通信。 有关详细信息，请参阅《*思科邮件安全设备 AsyncOS 用户指南*》。
禁用 SSLv3 以增强安全性的选项	为增强安全性，您可以对下列服务禁用 SSLv3： • 更新程序 • URL 筛选 • 最终用户隔离区 • LDAP 您可以在 CLI 中使用 `sslv3config` 命令对上述服务禁用 SSLv3。有关详细信息，请参阅《*思科邮件安全设备 AsyncOS 用户指南*》。

行为变化

为侦听程序配置全局设置时，现在可以根据主题大小指定接受还是拒绝邮件。如果指定此参数，则主题大小在指定限制内的邮件将被接受，而任何其他邮件则会被拒绝。有关详细信息，请参阅《*思科邮件安全设备 AsyncOS 用户指南*》。

升级路径

重要提示！

请在升级前参阅以下章节：

- **硬件设备**：只有某些型号支持此版本。请参阅此版本支持的硬件（第 3 页）。
- **虚拟设备**：要确保您获得此版本的所有优势，请参阅升级虚拟设备（第 3 页）。
- **集群配置（集中管理）**：请在升级集群之前完成此操作。请参阅利用集中管理升级部署（集群设备）（第 4 页）。
- **为确保成功升级**，必须在开始执行升级流程之前完成一些步骤。有关这些必备事项的详细信息，请参阅“安装和升级说明”一节，第 3 页。

您可以从以下版本升级到 **9.1.0-032** 版本：

- 8.0.1-023
- 8.0.2-066
- 8.5.5-280
- 8.5.6-074
- 8.5.6-092
- 8.5.6-106

- 8.5.6-116
- 9.0.0-500
- 9.1.0-024

安装和升级说明

阅读下文，并思考本节中列出的安装和升级影响。

当您从 Web 界面或命令行界面 (CLI) 升级思科邮件安全设备 AsyncOS 时，配置会保存到 /configuration/upgrade 目录下的文件中。您可以使用 FTP 客户端访问升级目录。每个配置文件名都附有版本号，而且配置文件中的密码是屏蔽的，因此无法人为识别。

您必须以管理员身份登录才能执行升级。此外，升级完成后必须重启设备。

此版本支持的硬件

- 所有虚拟设备型号。
- 以下硬件型号：
  - C380 或 C680
  - C170
  - 某些 C370、C370D、C670 或 X1070 设备

    要确定您的设备是否受支持，并解决设备当前不兼容的问题（如果有），请访问 http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html。

此版本不支持以下硬件：

C160、C360、C660 和 X1060

部署或升级虚拟设备

如果要部署或升级虚拟设备，请参阅《*思科内容安全虚拟设备安装指南*》（可从 http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html 获取）。

升级虚拟设备

如果拥有旧版本的邮件安全虚拟设备，并希望使用超过 2 TB 的磁盘空间，您不能只是简单地升级虚拟设备，而是应该为此版本部署一个新的虚拟机实例。您可以单独维护原有实例，也可以选择使用思科内容安全管理设备来同时管理新旧两个实例。

如果您选择升级虚拟设备，则现有许可证保持不变。

从硬件设备迁移到虚拟设备

步骤 1 参阅部署或升级虚拟设备（第 3 页）中介绍的文档，使用此 AsyncOS 版本设置您的虚拟设备。

步骤 2 将您的硬件设备升级到此 AsyncOS 版本。

步骤 3 保存已升级硬件设备中的配置文件。

步骤 4 将硬件设备中的配置文件加载到虚拟设备上。

获取虚拟设备技术支持

有关获取虚拟设备技术支持的要求，请参阅《*思科内容安全虚拟设备的安装指南*》（可从 http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html 下载）。

从虚拟设备调配和激活思科注册信封服务管理员

有关调配虚拟设备所需的信息，请联系思科技术支持中心 (TAC)。

升级前的注意事项

在升级之前，请完成以下操作：

文件分析隔离区

- 如果您曾手动创建名为“文件分析”(File Analysis) 的策略隔离区，在从 AsyncOS 9.0 以前的版本进行升级之前，您必须删除此隔离区。

  为此，您可以使用其他名称创建一个新隔离区，并将邮件移动到该新隔离区，然后删除现有文件分析隔离区。有关在策略隔离区之间移动邮件的详细信息，请参阅用户指南或在线帮助。

  如果您不执行此操作，系统不会创建文件分析隔离区（用来自动处理发送以供分析的邮件）。
- 在完成升级，并且将系统配置为向系统创建的新文件分析隔离区发送邮件之后，您可能需要删除或禁用您的传入邮件策略，以及您之前为隔离区邮件（包含发送以供分析的文件）创建的任何内容过滤器。

利用集中管理升级部署（集群设备）

如果集群包含 C160、C360、C660 或 X1060 硬件设备，请在升级之前从集群中删除这些设备。

集群中的所有设备都必须运行同一 AsyncOS 版本，而 x60 硬件无法升级到此版本。因此如果需要，请为 x60 设备创建单独的集群。

从上一版本以外的版本进行升级

如果是从上一版本以外的主要 (AsyncOS X.0) 或次要 (AsyncOS X.x) 版本进行升级，应查看当前使用的版本和此版本之间所有主要和次要版本的版本说明。

维护版本 (AsyncOS X.x.x) 仅包含漏洞修复。

配置文件

对于主要版本，思科通常不支持配置文件向后兼容。但是对于次要版本，配置文件可向后兼容。旧版本中的配置文件可能与新版本兼容，但可能需要经过修改才能加载。如果对配置文件支持您有任何问题，请联系思科客户支持部门。

升级到此版本

准备工作

- 查看已知和已修复的问题（第 6 页）和安装和升级说明（第 3 页）。
- 如果要升级虚拟设备，请参阅升级虚拟设备（第 3 页）。

操作步骤

参照以下说明升级您的邮件安全设备。

步骤 1 将 XML 配置文件保存到设备外。

步骤 2 如果您使用安全列表/阻止列表功能，请将安全列表/阻止列表数据库导出到设备外部。

步骤 3 暂停所有侦听程序。

步骤 4 等待队列为空。

步骤 5 在“系统管理”(System Administration) 选项卡中，选择“系统升级”(System Upgrade) 页面。

步骤 6 点击**可用的升级 (Available Upgrades)** 按钮。页面会刷新，并显示可用的 AsyncOS 升级版本列表。

步骤 7 点击**开始升级 (Begin Upgrade)** 按钮，即可开始升级。回答出现的问题。

步骤 8 升级完成后，点击**立即重启 (Reboot Now)** 按钮重启设备。

步骤 9 恢复所有侦听程序。

升级后的注意事项

性能公告

RSA 邮件 DLP - 如果在一个对入站流量运行反垃圾邮件和防病毒扫描的设备上对出站流量启用 RSA 邮件 DLP，性能将降低不到 10%。但是对于仅运行出站邮件而不运行反垃圾邮件和防病毒扫描的设备，性能会显著降低。

SBNP - 在此版本中，SenderBase Network Participation 将使用情景自适应扫描引擎 (CASE) 收集数据，以支持 IronPort 信息服务。在某些配置下，客户可能会发现性能略有下降。

爆发过滤器 - 爆发过滤器使用情景自适应扫描引擎来确定邮件的威胁级别，并基于自适应规则和爆发规则组合对邮件进行评分。在某些配置下，您可能会发现性能略有下降。

IronPort 垃圾邮件隔离区 - 如果对 C 系列或 X 系列设备启用机上 IronPort 垃圾邮件隔离区，则会最大程度减少额定负载设备上出现的系统吞吐量下降。对于在运行时接近或处于峰值吞吐量的设备，活动隔离区中的额外负载可能导致吞吐量降低 10-20%。如果您的系统已达到或接近饱和状态，并且您希望使用 IronPort 垃圾邮件隔离区，请考虑迁移到更大型的 C 系列设备或 M 系列设备。

如果将反垃圾邮件策略从减少垃圾邮件改为隔离垃圾邮件（无论是在机上还是机下），由于系统需要扫描更多垃圾邮件来防范病毒并确保内容安全，所以系统负载会有所增加。如需有关合理调整安装规模的帮助，请与授权支持提供商联系。

已知和已修复的问题

如需了解此版本中已知和已修复的问题，请使用思科漏洞搜索工具进行查找。

漏洞搜索工具的要求

如果您没有思科帐户，请注册思科帐户。访问 https://tools.cisco.com/RPF/register/register.do。

已知和已修复问题列表

已修复的问题	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.1.0&sb=fr&sts=fd&svr=4nH&srtBy=byRel&bt=custV
已知问题	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.1.0&sb=afr&sts=open&svr=3nH&srtBy=byRel&bt=custV

查找有关已知和已解决问题的信息

如需了解已知和已解决的缺陷的最新信息，请使用思科漏洞搜索工具进行查找。

准备工作

如果您没有思科帐户，请注册思科帐户。访问 https://tools.cisco.com/RPF/register/register.do。

操作步骤

步骤 1 转到 https://tools.cisco.com/bugsearch/。

步骤 2 使用思科帐户凭证登录。

步骤 3 依次点击**从列表中选择 (Select from list) > 安全 (Security) > 邮件安全 (Email Security) > 思科邮件安全设备 (Cisco Email Security Appliance)**，然后点击**确定 (OK)**。

步骤 4 在“版本”(Releases) 字段中，输入 **9.1.0**。

步骤 5 根据您的要求，执行以下操作之一：

- 要查看已解决问题的列表，请从“显示漏洞”(Show Bugs) 下拉列表中选择**这些版本中已修复的问题 (Fixed in these Releases)**。
- 要查看已知问题的列表，请从“显示漏洞”(Show Bugs) 下拉列表中选择**影响这些版本的问题 (Affecting these Releases)**，然后从“状态”(Status) 下拉列表中选择**未解决 (Open)**。

注 如果您有任何疑问或问题，请点击工具右上角的**帮助 (Help)** 或**反馈 (Feedback)** 链接。我们还提供了交互式导览，如需查看，请点击搜索字段上方的橙色信息栏中的链接。

文档更新

用户指南 PDF 的版本可能比在线帮助的版本更新。要获取用户指南 PDF 和其他有关此产品的文档，请在“在线帮助”(Online Help) 中点击**查看 PDF (View PDF)** 按钮，或访问相关文档（第 8 页）中显示的 URL。

有关其他资源的信息，包括知识库和思科支持社区，可在在线帮助和用户指南 PDF 的“其他资源”一章找到。

功能密钥

AsyncOS 设备以一分钟为间隔检查并应用功能密钥。因此，当您添加一个功能密钥时，查看更改可能最多需要一分钟。

哪些文件可进行信誉评估并送交分析？

评估文件信誉和文件送交分析的标准可能随时变更。标准仅适用于已注册的思科客户。具体请参阅《*思科内容安全产品高级恶意软件保护服务的文件条件*》（可在 http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html 获取）。

要访问该文档，您必须拥有思科客户帐户与支持合同。要进行注册，请访问 https://tools.cisco.com/RPF/register/register.do。

相关文档

思科内容安全产品文档	位置
硬件和虚拟设备	请参阅此表中的相应产品。
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
思科网络安全	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
思科邮件安全	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
思科内容安全设备 CLI 参考指南	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort 加密	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

服务与支持

可通过以下方法获得支持：

全球：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

支持站点：http://www.cisco.com/web/services/acquisitions/ironport.html

如果您是通过经销商或另一个供应商购买了支持，请直接联系该供应商咨询您的产品支持问题：

本文档需结合“相关文档”一节中列出的文档共同使用。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。