思科邮件安全设备 AsyncOS 9.6 版本说明

发布日期：2015 年 7 月 20 日
修订日期：2016 年 7 月 6 日

目录

新增内容

思科邮件安全设备 AsyncOS 9.6 新增内容

特性	说明
使用 CLI 进行灰色邮件配置	邮件安全设备现在允许您配置灰色邮件检测，并使用 CLI 安全地取消订阅。使用以下命令： • `graymailconfig` - 使用此命令配置灰色邮件全局设置。 • `policyconfig` - 使用此命令配置灰色邮件策略设置。 有关详细信息，请参阅《*思科邮件安全设备 AsyncOS CLI 参考指南*》。
增强的信用卡号智能识别程序	信用卡号智能识别程序现在可以识别 JCB 卡号。
查看有关您所在组织所有设备的文件分析结果详细信息	现在您可以在云中查看通过您所在组织的任何内容安全设备上传的所有文件的详细文件分析结果。在 AsyncOS 9.5 中，您只能从上传该文件以待分析的设备中查看这些详细结果。 要配置此功能，请参阅用户指南（PDF）中的“文件信誉过滤和文件分析”一章。

思科邮件安全设备 AsyncOS 9.5 新增内容

特性	说明
灰色邮件检测和安全取消订阅	• 邮件安全设备使您能够： – 使用集成的灰色邮件引擎识别灰色邮件，并进行相应的策略控制。 – 为最终用户提供安全且简单的机制，使其能够使用基于云的取消订阅服务取消订阅不需要的灰色邮件。 • 您可以使用以下报告监控检测到的灰色邮件： – “概述”(Overview) 页面 >“传入邮件摘要”(Incoming Mail Summary) – “传入邮件”(Incoming Mail) 页面 >“按灰色邮件列出的发件人排行榜”(Top Senders by Graymail Messages) – “传入邮件”(Incoming Mail) 页面 >“传入邮件详细信息”(Incoming Mail Details) – “传入邮件”(Incoming Mail) 页面 >“传入邮件详细信息”(Incoming Mail Details) >“发件人配置文件”(Sender Profile)（深入分析视图） – “内部用户”(Internal Users) 页面 >“按灰色邮件列出的用户排行榜”(Top Users by Graymail) – “内部用户”(Internal Users) 页面 >“用户邮件流详细信息”(User Mail Flow Details) – “内部用户”(Internal Users) 页面 >“用户邮件流详细信息”(User Mail Flow Details) >“内部用户”(Internal User)（深入分析视图） • 如果启用了服务更新，思科更新服务器会自动检索灰色邮件管理解决方案的扫描规则。 请参阅用户指南中的“管理灰色邮件”一章。 **注** 在 AsyncOS 9.5 中，您无法配置灰色邮件检测，也无法使用 CLI 安全地取消订阅。
Web 互动跟踪	Web 互动跟踪功能提供有关点击重写的（策略或爆发过滤器）URL 的最终用户的信息，以及与每次用户点击相关的操作的信息。 启用此功能后，您可以使用 Web 互动跟踪报告查看很多信息，例如点击数最高的恶意 URL，点击恶意 URL 次数最多的用户，等等。 **注** Web 互动跟踪报告模块并非实时更新，而是每 30 分钟刷新一次。此外，在点击重写的 URL 后，Web 互动跟踪报告可能需要最多 2 个小时来报告此事件。 请参阅用户指南中的“防止恶意或不需要的 URL”一章。

特性	说明
系统运行状况监控增强功能	邮件安全设备包含以下系统运行状况监控增强功能： • **系统运行状况参数的可配置阈值**。根据您所在组织的要求，您可以为设备的多个运行状况参数配置阈值，例如整体 CPU 使用率、工作队列中的邮件数量，等等。还可以对设备进行配置，使其在超过指定阈值时自动发送警报。 请参阅用户指南中的“系统管理”一章。 • **改进的“系统容量”(System Capacity) 页面**。以下关于“系统容量”(System Capacity) 页面的报告现在显示已配置的系统运行状况参数阈值水平： – 工作队列 – 整体 CPU 使用率 – 内存页面交换 请参阅用户指南中的“使用邮件安全监控”一章。 • **升级指南**。使用 Web 界面或 CLI 执行升级时，系统会分析状态日志以确定设备是否已准备好升级。根据此分析的结果，系统将指导您是进行升级还是在升级之前执行其他任务。 请参阅用户指南中的“系统管理”一章。 • **按需运行状况检查**。您现在可以使用运行状况检查功能，随时在需要时检查设备的运行状况。系统会分析状态日志中的历史数据以确定设备的运行状况。您可以根据此分析采取补救措施。 请参阅用户指南中的“系统管理”一章。 • **资源节约活动图表。**此图显示设备进入资源节约模式的次数。您可以通过**监控 (Monitor) > 系统容量 (System Capacity) > 系统负载 (System Load)** 访问该图表。 请参阅用户指南中的“使用邮件安全监控”一章。
本地文件分析支持	如果您已在网络上部署 Cisco AMP Threat Grid 设备，则可以分析邮件附件是否含有恶意软件，而无需将其发送到云。 有关升级的信息，请参阅文件分析更改可能需要配置更改（第 11 页）。 要配置本地文件分析服务器，请参阅用户指南 PDF 中的“文件信誉过滤和文件分析”一章。
TLS v1.2 支持	思科邮件安全设备目前支持另一种 SSL 方法：TLS v1.2。请记住： • 如果您升级之前使用的是 TLS v1，也可以在升级之后协商使用 TLS v1.2。 • 如果您在升级之前没有使用 TLS v1，SSL 方法将不会在升级之后自动设置为 TLS v1.2。 您可以使用 Web 界面上的“SSL 配置”(SSL Configuration) 页面或运行 CLI 中的 `sslconfig` 命令，查看或修改现有的 SSL 配置。 **注** 在协商期间始终会选择客户端广告中最受支持的 TLS 或 SSL 方法。

更改的行为

思科邮件安全设备 AsyncOS 9.6 中更改的行为

内容字典更改	为实现高效处理，以下内容字典条目将被视为单词： • 只包含字母数字字符的条目 • 包含以下字符的邮件地址：0-9、A-Z、a-z、点、下划线、连字符和 at 符号 • 包含以下字符的域名：0-9、A-Z、a-z、点、下划线、连字符和 at 符号 如果您想要设备将这些单词处理为正则表达式，请将单词放在括号内，例如 `(user@example.com)`。
文件分析	文件分析更改可能需要您执行操作。请参阅文件分析更改可能需要配置更改（第 11 页）。

思科邮件安全设备 AsyncOS 9.5 中更改的行为

营销邮件设置	如果您在升级到 AsyncOS 9.5 或更高版本后，在某个邮件策略的反垃圾邮件设置下启用了反垃圾邮件扫描并配置了营销邮件设置： • 灰色邮件将默认全局启用。 • 反垃圾邮件设置下的营销邮件设置将移动到同一策略的灰色邮件设置下。 • 使用灰色邮件相关的报告时，请记住： – 营销邮件的数量是在升级前后检测到的营销邮件之和。 – 灰色邮件总数不包括在升级前检测到的营销邮件数量。 – 尝试的邮件总数还包括在升级前检测到的营销邮件数量。

升级路径

升级到思科邮件安全设备 AsyncOS 9.6.0-051（维护部署）

您可以从以下版本升级到 9-6-0-051 版本：

- 8-5-6-106
- 9.1.0-032
- 9.5.0-201
- 9.6.0-042
- 9.6.0-047

升级到思科邮件安全设备 AsyncOS 9.6.0-047（一般部署）

您可以从以下版本升级到 9-6-0-047 版本：

- 8-5-6-106
- 9-6-0-042

升级到思科邮件安全设备 AsyncOS 9.6.0-042（一般部署）

您可以从以下版本升级到 9-6-0-042 版本：

- 8-5-6-106
- 8-5-7-042
- 9-1-0-032
- 9-5-0-201

升级到思科邮件安全设备 AsyncOS 9.5（有限部署）

您可以从以下版本升级到 9.5.0-201 版本：

- 8.5.6-106
- 9.1.0-032
- 9.5.0-144

安装和升级说明

阅读并考虑本部分中列出的安装和升级影响。

当您通过 Web 界面或命令行界面 (CLI) 升级 AsyncOS 时，相应配置会保存到 /configuration/upgrade 目录中的文件。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。

URL 信誉功能服务器中的更改

重要提示！ URL 信誉功能服务器使用的服务器池已经更改。因此，启用 URL 过滤功能时，您可能会发现以下某种症状：

- 设备上的工作队列进行备份
- web_client 日志中有大量的“请求已过期”条目
- 出现警报，指示您的设备无法连接到思科网络安全服务

要解决此问题，您必须减少同时发送以进行验证的 URL 的数量。

程序

步骤 1 使用 SSH 访问命令行界面。

步骤 2 输入 `websecurityadvancedconfig`。

步骤 3 将**输入未完成请求的阈值 (Enter the threshold value for outstanding requests)** 的对应值从默认值改为 5。

注 请务必确保不更改任何其他设置。

步骤 4 提交更改。

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

如需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*》，可通过以下网址获取：http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html。

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 8 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。

请务必选择与网络设置相关的相应选项。

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

请在升级之前查看以下内容：

- 文件分析隔离区（第 9 页）
- FIPS 合规性（第 9 页）
- 利用集中管理升级部署（集群设备）（第 9 页）
- 从上一版本以外的版本进行升级（第 9 页）
- 配置文件（第 9 页）

文件分析隔离区

- 如果您使用名称“文件分析”手动创建了策略隔离区，则从早于 AsyncOS 9.0 的版本进行升级之前必须删除此隔离区。

  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。

FIPS 合规性

AsyncOS 9.5 和 9.6 版本不符合 FIPS。如果在设备上启用了 FIPS 模式，必须在升级到 AsyncOS 9.5 或 9.6 之前禁用该模式。

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。

集群中的所有机器都必须运行同一 AsyncOS 版本，而 x60 硬件无法升级到此版本。因此，必要时，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 12 页）和安装和升级说明（第 7 页）。
- 如果要升级虚拟设备，请参阅升级虚拟设备（第 8 页）。

程序

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。

后续操作

查看性能公告（第 11 页）。

升级后的注意事项

虚拟设备：重要提示！SSH 安全漏洞修复所需的更改

本节中提到的要求适用于 AsyncOS 9.6。

如果您的设备有以下安全漏洞，则升级期间会得到修复：
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport。

如果您没有在升级前修复此问题，则升级期间会看到一则表示问题已修复的消息。如果您看到此消息，需要采取以下操作以使设备在升级后回到完全正常的工作状态：

- 从 SSH 实用程序中的已知主机列表中删除设备的现有条目。然后对设备使用 SSH 并用新密钥接受连接。
- 如果您使用 SCP 推送将日志转移到远程服务器（包括 Splunk）：从远程服务器中清除设备的旧 SSH 主机密钥。
- 对于集群配置（邮件安全设备）：
  - 使用 `logconfig > hostkeyconfig > delete` 命令删除所有虚拟邮件安全设备的主机密钥（主机密钥在升级后修改）。
  - 使用 `logconfig > hostkeyconfig > scan` 命令将每个虚拟邮件安全设备的新密钥添加到集群中的所有机器。使用集群中每个虚拟邮件安全设备的 IP 地址。

    例如，如果一个集群中有两台虚拟邮件安全设备，则更新这两台机器的主机密钥。

然后，在集群中的这两台设备上运行以下命令：
`logconfig > hostkeyconfig > scan > <IP address of vESA1>`
和
`logconfig > hostkeyconfig > scan > <IP address of vESA2>`。

- 使用 `clusterconfig` 命令，将机器重新连接到集群。
- 使用 `clusterconfig > connstatus` 命令验证机器是否已正确重新连接，以此检查重新连接状态。

- 如果您的部署包括思科内容安全管理设备，请参阅版本说明中有关该设备的重要说明。

替换旧的演示证书

升级到 AsyncOS 9.6 或更高版本后，您可以不再使用以下 IronPort 设备演示证书：delivery_cer、https_cer、ldaps_cer 和 receiving_cer。这些证书是使用较旧密码创建的，并且不与设备的 TLS 版本相兼容。因此，使用这些证书的服务与特定域之间的通信可能会失败。升级后，请使用新的演示证书替换这些证书。有关详细信息，请参阅 https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200025-9-5-and-newer-AsyncOS-for-Email-Security.html。

文件分析更改可能需要配置更改

在云中查看文件分析结果详细信息

AsyncOS 9.6 中引入了以下更改，这些更改还适用于从 AsyncOS 8.5.5 到 AsyncOS 9.5 的升级。

如果您部署了多个内容安全设备（邮件、Web 和/或管理），并且想要在云中查看通过您所在组织的任何设备上传的所有文件的详细文件分析结果，您必须在升级后对每个设备上的设备组进行配置。

有关详细信息，请参阅用户指南 PDF 的“文件信誉过滤和文件分析”一章中有关分组设备的信息。

验证已分析的文件类型未被更改

先从 AsyncOS 9.5 开始：

文件分析云服务器 URL 已更改，因此可分析的文件类型在升级后可能已更改。如果有更改，您应该会收到警报。要验证进行分析的所选文件类型，请选择**安全服务 (Security Services) > 文件信誉和分析 (File Reputation and Analysis)**。

性能公告

RSA 邮件 DLP

- 如果在一个对入站邮件运行反垃圾邮件和防病毒扫描的设备上对出站邮件启用 RSA 邮件 DLP，性能将降低不到 10%。
- 相对于上一场景而言，在仅运行出站邮件而未运行反垃圾邮件和防病毒扫描的设备上启用 RSA 邮件 DLP，可能导致性能进一步降低。

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，会最大程度降低名义上高负载的设备遭受的系统吞吐量下降。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（第 12 页）
- 已知和已修复问题列表（第 12 页）
- 查找有关已知和已解决问题的信息（第 12 页）

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	AsyncOS 9.6	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.6.0&sb=anfr&sts=fd&srtBy=byRel&bt=custV
	AsyncOS 9.5	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.5.0&sb=fr&srtBy=byRel&bt=custV
已知问题	AsyncOS 9.6	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.6.0&sb=anfr&sts=open&srtBy=byRel&bt=custV
	AsyncOS 9.5	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.5.0&sb=afr&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。

程序

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，输入版本号，例如 9.6。

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 的版本可能要比在线帮助的版本新。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 14 页）中显示的 URL。

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。

在云中查看文件分析详细信息

有关配置此功能的最新说明，请参阅用户指南 PDF，可通过 http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html 获得。

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
思科 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”部分中列出的文档共同使用。