



AsyncOS 8.7 版本说明适用于思科网络安全设备 (LD)

发布日期：2015 年 4 月 1 日

修订日期：2016 年 7 月 14 日

目录

- [新增内容（第 2 页）](#)
- [版本分类（第 4 页）](#)
- [此版本支持的硬件（第 4 页）](#)
- [升级路线（第 5 页）](#)
- [安装说明（第 5 页）](#)
- [已知和已解决的问题（第 7 页）](#)
- [相关文档（第 8 页）](#)
- [支持（第 8 页）](#)



新增内容

Cisco AsyncOS 8.7 新增内容

功能	说明
ISE 集成	AsyncOS 现在可以从同一网络中部署的身份服务引擎 (ISE) 1.3 版服务器访问其他用户身份信息。
SSL 配置	<p>为获得增强的安全性，可以对多个服务启用和禁用 SSLv3。在禁用 SSLv3 的情况下，服务会使用 TLSv1.0。</p> <p>您可以对设备管理 Web 用户界面、代理服务（包括安全客户端的 HTTPS 代理和凭证加密）、安全 LDAP 服务（包括身份验证、外部身份验证、SaaS SSO 和安全移动）以及更新服务启用或禁用 SSLv3。</p> <p>使用网络界面（“系统管理” (System Administration) > “SSL 配置” (SSL Configuration)）或 CLI (<code>sslconfig</code>)。</p>

AsyncOS 8.7 的要求和限制

请注意 AsyncOS 8.7 的以下要求和限制：

- AsyncOS 8.7 仅支持 1.3 版的身份服务引擎。
- AsyncOS 的此版本不支持连接器模式；但是，当在连接器模式下运行时，ISE 特定选项保持可视并以透明方式可用。再次重申，不支持连接器模式，如果系统是在该模式下运行，则不应升级到此版本。

Cisco AsyncOS 8.6 新增内容

功能	说明
虚拟设备增强功能	<ul style="list-style-type: none"> • 现在可在 KVM 虚拟机监控程序上部署虚拟设备在以下 Linux 平台上运行： <ul style="list-style-type: none"> - Red Hat Enterprise Linux Server 7.0 - Ubuntu Server 14.04.1 LTS • 支持磁盘存储的精简调配。 • 您可以将思科设备许可证和配置文件配置为在初始启动时自动加载在 VMWare ESXi 或 KVM 部署上。 <p>有关详细信息，请参阅以下位置的《思科内容安全虚拟设备安装指南》： http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html</p> <p>重要提示！ 请参阅运行于 KVM 上的虚拟设备重启时挂起（第 11 页）。</p>

Cisco AsyncOS 8.5 新增内容

功能	说明
高可用性	<p>此版本为设备通过代理在显式模式下运行的部署提供合适的内置高可用性选项。</p> <p>有关详细信息，请参阅《用户指南》中的“连接、安装和配置”一章。</p>
2048 位证书	由设备生成或处理的 SSL 证书的密钥长度现在是 2048 位。
LDAP 身份验证 (LDAP authentication)	LDAP 协议现在支持用于对设备的管理用户进行身份验证。
数量和时间配额	可以将时间和数量配额应用于访问策略和解密策略。配额允许个人用户继续访问互联网资源（或互联网资源类），直至其耗尽实施的数据量或时间限制为止。
网络安全虚拟设备增强功能	<ul style="list-style-type: none"> 支持 VMWare ESXi 5.5 在 ESXi 中支持精简调配 现在，在虚拟设备许可证到期后，有六个月的宽限期，在此期间，设备可以继续处理 Web 事务，但没有安全服务。 可以配置设备，以在接近许可证到期日期时发送警报。 现在可在虚拟设备上部署评估功能密钥
按计算机 ID 进行身份验证	对于使用 Active Directory 在连接器模式下进行的部署，此版本引入用于根据设备 ID 来授权访问的选项。
高级恶意软件保护增强功能	<ul style="list-style-type: none"> 高级恶意软件保护现在可以检测存档文件或压缩文件中的恶意软件。 您现在可以选择用于与 AMP 服务器进行通信的接口。 文件分析现在支持其他文件类型的分析。受支持的文件类型由云服务确定，并可随时更改。 <p>当配置文件分析功能时，可以选择要送交分析的文件类型，并且可以选择在选项更改时接收警报。</p> <p>有关详细信息，请参阅版本说明中的“哪些文件可以评估其信誉并送交分析”，并且参阅在线帮助或《用户指南》中的“文件信誉和文件分析”一章，以获取有关支持的文件类型和警报的信息。</p>
AAA 审核日志记录	AsyncOS 增强为跨多个日志标准化与 AAA 相关的日志记录，并且将其集中到中央日志订用中。这一新的日志订用将通过系统日志可导出。
密码安全增强功能	<p>已为本地定义的管理用户引入以下密码增强功能：</p> <ul style="list-style-type: none"> 向输入新密码的用户显示密码强度指示器。 按您指定的密码要求实施密码强度。 不允许在密码中使用某些单词。（请将禁止的单词的列表上传到设备。） 通过点击按钮生成密码的选项。 <p>有关详细信息，请参阅《用户指南》中的“设置管理用户的密码要求”和“添加本地用户帐户”部分。</p>

功能	说明
网络跟踪增强功能	在按“恶意软件威胁”(Malware Threat) 过滤网络跟踪结果时，有一个新的“所有恶意软件”(All Malware) 选项。
思科内容安全管理虚拟设备	您现在可以使用与物理硬件设备具有相同功能的虚拟内容安全管理设备来管理多个网络安全设备。
受信任根证书管理	受信任根证书管理从“安全服务”(Security Services) > “HTTPS 代理”(HTTPS Proxy) 移至“网络”(Network) > “证书管理”(Certificate Management)。
DNS 服务器故障切换	如果主 DNS 服务器对于用户指定的数量的查询没有响应，则将其视为发生故障，并会将查询自动重定向到辅助服务器。

版本分类

每个版本通过版本类型（ED - 早期部署，GD - 通用部署等）进行识别。有关这些术语的说明，请参阅 <http://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/content-security-release-terminology.pdf>。

此版本支持的硬件

- 所有虚拟设备型号。
- 以下硬件型号：
 - S170
 - S370
 - S670
 - S680
 - S380

对于部分硬件型号，需要进行内存升级才能安装或升级到此 AsyncOS 版本。有关详细信息，请参阅 <http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html>

升级路线

在开始升级之前，请参阅[安装说明（第 5 页）](#)。

对于思科网络安全设备，您可以从以下版本升级至 AsyncOS 版本 8.7.0-172:

- | | | | |
|-------------|-------------|-------------|-------------|
| • 7-7-0-500 | • 7.7.5-190 | • 8-0-0-408 | • 8-1-0-235 |
| • 7-7-0-608 | • 7.7.5-194 | • 8-0-0-503 | • 8-1-0-245 |
| • 7-7-0-706 | • 7.7.5-195 | • 8-0-5-075 | |
| • 7-7-0-710 | • 7.7.5-302 | • 8-0-5-079 | • 8-5-0-389 |
| • 7-7-0-725 | • 7.7.5-311 | • 8-0-5-082 | • 8-5-0-390 |
| • 7-7-0-736 | | • 8-0-6-053 | • 8-5-0-476 |
| • 7-7-0-744 | | • 8-0-6-078 | • 8-5-0-518 |
| • 7-7-0-753 | | • 8-0-6-101 | • 8-5-1-019 |
| • 7-7-0-757 | | • 8-0-6-119 | • 8-5-1-021 |
| • 7-7-0-760 | | • 8-0-7-142 | • 8-6-0-025 |
| • 7-7-0-761 | | | • 8-7-0-141 |

安装说明

- [从非 ISE 版本和带“ISE 预览”的 AsyncOS 8.5 升级](#)
- [兼容性详细信息](#)
- [部署虚拟设备](#)
- [配置文件](#)

从非 ISE 版本和带“ISE 预览”的 AsyncOS 8.5 升级

不包括 ISE 支持的所有 AsyncOS 版本（即 8.5.0-497 之前的所有版本）和可用性有限的 AsyncOS 8.5 “ISE 预览”版本，不需要管理员和 pxGrid 证书，在所有包含 ISE 支持的 Cisco AsyncOS 版本中需要这些证书。因此，当您从非 ISE 版本或启用 ISE 的 ISE 预览安装版进行升级时，在提供两个额外的证书（进入[网络 \(Network\)](#) > [身份服务引擎 \(Identity Services Engine\)](#))后，ISE 功能才能正确运行。

兼容性详细信息

- [与思科安全管理 AsyncOS 的兼容性](#)
- [IPv6 和 Kerberos 在云连接器模式下不可用](#)
- [IPv6 地址的功能支持](#)
- [Kerberos 身份验证对于操作系统和浏览器的可用性](#)

与思科安全管理 AsyncOS 的兼容性

有关此版本和思科内容安全管理 AsyncOS 版本之间的兼容性情况，请参阅兼容性表格：
<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>。

IPv6 和 Kerberos 在云连接器模式下不可用

当在云连接器模式下进行设备配置时，IPv6 地址和 Kerberos 身份验证的不可用选项会在 Web 界面的页面上显示。虽然这些选项看似可用，但它们在云连接器模式下不受支持。在云连接器模式下，请勿尝试配置设备使用 IPv6 地址或 Kerberos 身份验证。

IPv6 地址的功能支持

支持 IPv6 地址的特性和功能：

- 命令行和 Web 界面。您可使用 [http://\[2001:2:2::8\]:8080](http://[2001:2:2::8]:8080) 或 [https://\[2001:2:2::8\]:8443](https://[2001:2:2::8]:8443) 访问 WSA
- 对 IPv6 数据流量 (HTTP/HTTPS/SOCKS/FTP) 执行代理操作
- IPv6 DNS 服务器
- WCCP 2.01 (Cat6k 交换机) 和第 4 层透明重定向
- 上游代理
- 身份验证服务
 - Active Directory (NTLMSSP、Basic 和 Kerberos)
 - LDAP
 - SaaS SSO
 - 通过 CDA (WSA 和 CDA 之间仅支持通过 IPv4 协议进行通信) 的透明用户标识
 - 凭据加密
- Web 报告和 Web 跟踪
- 外部 DLP 服务器 (WSA 和 DLP 服务器之间仅支持通过 IPv4 协议进行通信)
- PAC 文件托管

需要 Ipv4 地址的特性和功能

- 内部 SMTP 中继 (Internal SMTP Relay)
- 外部身份验证
- 日志订阅推送方法：FTP、SCP 和系统日志
- NTP 服务器
- 本地更新服务器，包括用于更新的代理服务器
- 身份验证服务
- AnyConnect 安全移动
- Novell eDirectory 身份验证服务器
- 最终用户通知页面的自定义徽标
- 网络安全设备和安全管理设备之间的通信
- 版本 2.01 之前的 WCCP 版本
- SNMP

Kerberos 身份验证对于操作系统和浏览器的可用性

您可以在以下操作系统和浏览器中使用 Kerberos 身份验证功能：

- Windows Server 2003、2008、2008R2 和 2012
- Mac (OSX 10.5+ 版本) 的 Safari 和 Firefox 浏览器的最新版本
- Windows 7 和 XP 的 IE (7+ 版本) 和 Firefox 与 Chrome 浏览器的最新版本

Kerberos 身份验证对于以下操作系统和浏览器不适用：

- 前面未提到的 Windows 系统
- 前面未提到的浏览器
- iOS 和 Android

部署虚拟设备

要部署虚拟设备，请参阅 *思科内容安全虚拟设备安装指南*，其可从 <http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html> 获取。

从硬件设备迁移到虚拟设备

无法从硬件设备迁移至该版本。

配置文件

通常，旧版本 AsyncOS 的配置文件与新版本 AsyncOS 不兼容，反之亦然。

已知和已解决的问题

使用思科缺陷搜索工具查找有关已知和已修复缺陷的信息。

缺陷搜索工具的要求

如果您没有思科帐户，请注册一个帐户。访问 <https://tools.cisco.com/RPF/register/register.do>。

已知和已修复问题的列表

已知问题	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.7.0&sb=af&sts=open&svr=3nH&srtBy=byRel&bt=custV
已修复的问题	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=8.7.0-172&sb=fr&svr=3nH&srtBy=byRel&bt=custV

查找其他缺陷

- 步骤 1 转到 <https://tools.cisco.com/bugsearch/>。
- 步骤 2 使用思科帐户凭据登录。
- 步骤 3 输入搜索条件。
- 步骤 4 如果您有任何问题或疑问，请点击工具右上角的**帮助 (Help)** 或**反馈 (Feedback)** 链接。

相关文档

此产品的文档可从 <http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html> 获取。

思科内容安全管理设备的文档可从 <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html> 获取。

支持

知识库

您可以通过以下 URL 访问思科客户支持网站上的思科知识库：

<http://www.cisco.com/web/ironport/knowledgebase.html>



注意

您需要 Cisco.com 用户 ID 才能访问网站。如果您没有 Cisco.com 用户 ID，您可以点击以下链接进行注册：<https://tools.cisco.com/RPF/register/register.do>

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。它提供了一个场所，供相关人员讨论常规的网络安全问题以及有关思科具体产品的技术信息。您可以在论坛中发布主题，以咨询问题并与其他思科用户分享信息。

通过以下 URL 访问思科支持社区以了解网络安全和关联管理：

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

客户支持

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

支持网站：访问 http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

对于普通问题，您还可以访问设备中的客户支持。如需相关指导，请参阅《用户指南》或联机帮助。

本文档需结合“[相关文档](#)”一节中列出的文档共同使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请转至此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

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。

© 2015 年思科系统公司。版权所有。

