Cisco AnyConnect Secure Mobility Client 4.9 版本说明

AnyConnect Secure Mobility Client 4.9 版本说明

这些版本说明提供 Windows、macOS 和 Linux 平台上的 AnyConnect 安全移动的相关信息。始终开启的智能 VPN 可帮助 AnyConnect 客户端设备自动选择最佳网络接入点，并使其隧道协议适应最高效的方法。

注释 AnyConnect 版本 4.9.x 将成为所有 4.x 漏洞的维护路径。AnyConnect 4.0、4.1、4.2、4.3、4.4、4.5、4.6、4.7 和 4.8 客户必须升级到 AnyConnect 4.9.x 才能受益于未来的缺陷修复。AnyConnect 4.0.x、4.1.x、4.2.x、4.3.x、4.4.x、4.5.x、4.6.x、4.7.x 和 4.8.x 中发现的任何缺陷都只能在 AnyConnect 4.9.x 维护版本中修复。

具有 macOS 10.15 的 Cisco AnyConnect 用户可能无法建立 VPN 连接或可能会收到系统弹出消息-建议使用软件升级

思科 AnyConnect 和 HostScan 需要更新版本才能兼容即将推出的 macOS Catalina 版本 (10.15)。从 macOS Catalina 版本 (10.15) 开始，操作系统不再支持执行 32 位二进制文件。此外，必须对应用进行加密公证，才能由操作系统进行安装。Cisco AnyConnect 4.8.00175 是第一个正式支持在 macOS Catalina 上进行操作的版本，不包含 32 位代码。

下载 AnyConnect 的最新版本

开始之前

若要下载 AnyConnect 的最新版本，您必须是 Cisco.com 的注册用户。

过程

步骤 1 单击此链接前往Cisco AnyConnect Secure Mobility Client 产品支持页面：

http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html。

步骤 2 登录 Cisco.com。

步骤 3 单击**下载软件**。

步骤 4 如果尚未选择最新版本，则展开**最新版本 (Latest Releases)** 文件夹并单击最新版本。

步骤 5 使用以下方法之一下载 AnyConnect 软件包：

- 若要下载单一软件包，请查找要下载的软件包并单击**下载 (Download)**。
- 若要下载多个软件包，请单击软件包行的**加入购物车 (Add to cart)**，然后单击“下载软件”(Download Software) 页面顶部的**下载购物车 (Download Cart)**。

步骤 6 系统提示时，阅读并接受思科许可证协议。

步骤 7 选择用于保存下载文件的本地目录并单击**保存**。

步骤 8 请参阅《Cisco AnyConnect Secure Mobility Client 版本 4.x 管理员指南》。

用于网络部署的 AnyConnect 软件包文件名

操作系统	AnyConnect 网络部署软件包名称
Windows 的 ISE 安全评估代理	anyconnect-win-版本-webdeploy-k9.pkg
macOS	anyconnect-macos-版本-webdeploy-k9.pkg
Linux（64位）	anyconnect-linux64-版本-webdeploy-k9.pkg

用于预部署的 AnyConnect 软件包文件名

操作系统	AnyConnect 预部署软件包名称
Windows 的 ISE 安全评估代理	anyconnect-win-版本-predeploy-k9.zip
macOS	anyconnect-macos-*version*-predeploy-k9.dmg
Linux（64位）	anyconnect-linux64-版本-predeploy-k9.tar.gz

可另外下载的其他文件，它们有助于您向 AnyConnect 添加其他功能。

AnyConnect 4.9.02028 新功能

此 AnyConnect 4.9.02028 版本引入了以下增强，并解决了 AnyConnect 4.9.02028，第 30 页 中所述的缺陷：

AnyConnect 4.9.02028 是一个仅限 macOS 的版本，也可在 macOS 11 (Big Sur) 测试版 5（或公开测试版 2）或更高版本中运行。在 macOS 11 (Big Sur) 上进行新安装时，AnyConnect 使用系统扩展程序，而不是之前 AnyConnect 版本中使用的内核扩展程序。

之前的 AnyConnect 版本或许仍可以在 macOS 11 上运行，但仅限 MDM 管理的设备，原因是从 macOS 11 开始，必须获得基于 MDM 的 AnyConnect 内核扩展程序批准。

当 macOS Big Sur 正式发布后，AnyConnect 将加入对该操作系统的正式支持。欢迎客户现在进行测试，并且应该始终使用最新的 Big Sur 测试内部版本进行测试。

您可以将任何 Big Sur 兼容性问题发送到 **ask-anyconnect@cisco.com**。在 Big Sur OS 发布之前，您无法为兼容性问题开立 TAC 案件。

AnyConnect 4.9.01095 新功能

此 AnyConnect 4.9.01095 版本引入了以下增强和限制，并解决了 AnyConnect 4.9.01095，第 30 页 中所述的缺陷：

- Linux 用户在 VM 实例/Docker 容器上路由网络流量的能力。
- 升级到 AnyConnect 4.9.01095（仅限 Linux）后自动重新连接失败。有关详细信息，请参阅升级到 AnyConnect 4.9.01xxx（仅限 Linux）后客户端首次自动重新连接失败一节。

AnyConnect 4.9.00086 新功能

此版本是一个包括以下功能和支持更新的主要版本，可以解决 AnyConnect 4.9.00086，第 33 页 中所述的缺陷：

- NVM 扩展可以丰富流和端点数据，包括与 Splunk app 3.x 协调的新 NVM 收集器以及用于流信息的时间戳
- 对于 SSL VPN，AnyConnect 不再支持来自 TLS 和 DTLS 的以下密码套件：DHE-RSA-AES256-SHA 和 DES-CBC3-SHA
- 对于 IKEv2/IPsec，AnyConnect 不再支持以下算法：
  - 加密算法：DES 和 3DES
  - 伪随机函数 (PRF) 算法：MD5
  - 完整性算法：MD5
  - Diffie-hellman (DH) 组：2、5、14、24
- 更新后的 OpenSSL (Cisco SSL) 库

AnyConnect HostScan Engine Update 4.9.02028 新功能

AnyConnect HostScan 4.9.02028 支持 macOS 11 (Big Sur) 测试版 5（或公共测试版 2）或更高版本，并且包括对 Windows、macOS 和 Linux 版 MACOS 引擎的更新。

如果您对 HostScan 使用 macOS 11 测试版，则以前版本的 HostScan 将无法正常运行。因此，端点上的 AnyConnect HostScan 终端安全评估模块（如果之前已安装）和 ASA 上的 HostScan PKG 必须升级到 4.9.02028。

AnyConnect HostScan Engine Update 4.9.01095 新功能

AnyConnect HostScan 4.9.01095 包括对 HostScan 模块的这一更新，并解决了HostScan 4.9.01095 ， 第 36 页中所列的缺陷：

支持 Windows 10 端点的 Microsoft Defender 高级威胁防护 (ATP)。

AnyConnect HostScan Engine Update 4.9.00086 新功能

AnyConnect HostScan 4.9.00086 包括对 HostScan 模块的更新，并解决了HostScan 4.9.00086 ， 第 36 页中所列的缺陷。

系统要求

本节确定此版本的管理和终端要求。有关终端操作系统支持和每项功能的许可证要求，请参阅 AnyConnect 安全移动客户端功能、许可证和操作系统。

思科无法保证与其他 VPN 第三方客户端的兼容性。

对 AnyConnect 配置文件编辑器的更改

在安装配置文件编辑器前，必须安装 Java 版本 6 或更高版本。

AnyConnect 的 ISE 要求

- **警告!**

  不兼容警告：如果您是运行 2.0（或更高版本）的身份服务引擎 (ISE) 客户，则必须先阅读此信息，然后再继续！

  自版本 2.0 起，ISE RADIUS 支持 TLS 1.2；但是，在使用 TLS 1.2，由 CSCvm03681 跟踪时，EAP-FAST 的 ISE 实施中存在缺陷。此缺陷已在 ISE 的 2.4p5 版本中得到修复。此修复将在未来 ISE 的支持版本的热修补中提供。

  如果使用 EAP-FAST 对 NAM 4.7 进行身份验证，并且为上述版本以下的、支持 TLS 1.2 的任何 ISE 版本，则身份验证将失败，且终端将无法访问网络。

- 使用 AnyConnect 4.7 MR1（及更高版本）的 ISE 2.6（及更高版本）支持在有线和 VPN 流上的 IPv6 非重定向流（使用第 2 阶段发现）。
- AnyConnect 临时代理流在基于网络拓扑的 IPv6 网络上运行。ISE 在网络接口（例如，eth0/eth1）上支持多种 IPv6 配置方式。
- 与 ISE 终端安全评估流相关的 IPv6 网络具有以下限制：由于特定类型的网络适配器（例如，Microsoft Teredo 虚拟适配器），[IPv6] ISE 终端安全评估发现处于无限循环 (CSCvo36890)。

- 至少需要 ISE 2.0 才能将 AnyConnect 软件部署到终端，以及使用 AnyConnect 4.0 及更高版本中的新 ISE 安全评估模块对该终端进行安全评估。
- ISE 2.0 只能部署 AnyConnect 版本 4.0 及更高版本。更低版本的 AnyConnect 必须从 ASA 进行网络部署、使用 SMS 进行预部署或手动部署。

ISE 许可要求

若要从 ISE 前端部署 AnyConnect 并使用 ISE 安全评估模块，需要在 ISE 管理节点上安装思科 ISE Apex 许可证。有关 ISE 许可证的详细信息，请参阅《思科身份服务引擎管理员指南》的思科 *ISE* 许可证一章。

AnyConnect 的 ASA 要求

指定功能的最低 ASA/ASDM 版本要求

- 您必须升级到 ASA 9.10.1（或更高版本）和 ASDM 7.10.1（或更高版本）才能使用 DTLSv 1.2。

  注释 DTLSv 1.2 受除 5506-X、5508 和 5516-X 以外的所有 ASA 型号所支持，并且当 ASA 仅用作服务器而不充当客户端时适用。DTLS 1.2 支持其他密码，以及所有最新的 TLS/DTLS 密码和更大的 cookie。

- 您必须升级到 ASDM 7.10.1 才能使用管理 VPN 隧道。
- 必须升级到 ASDM 7.5.1 才能使用 NVM。
- 必须升级到 ASDM 7.4.2 才能使用 AMP 启用程序。
- 必须升级到 ASA 9.3(2) 才能使用 TLS 1.2。
- 如果要使用以下功能，必须升级到 ASA 9.2(1)：
  - 通过 VPN 执行 ISE 安全评估
  - AnyConnect 4.x 的 ISE 部署
  - 从此版本起支持 ASA 上的授权变更 (CoA)
- 如果要使用以下功能，必须升级到 ASA 9.0：
  - IPv6 支持
  - 思科下一代“Suite B”加密技术安全
  - 动态分割隧道（自定义属性）
  - AnyConnect 客户端延迟升级
  - 管理 VPN 隧道（自定义属性）

- 如果要执行以下操作，必须使用 ASA 8.4(1) 或更高版本：
  - 使用 IKEv2。
  - 使用 ASDM 编辑非 VPN 客户端配置文件（例如网络访问管理器、网络安全或遥感勘测）。
  - 使用思科 IronPort 网络安全设备支持的服务。这些服务让您能够通过授权或拒绝所有 HTTP 和 HTTPS 请求，强制实施可接受的使用策略并保护终端不受不安全网站的侵害。
  - 部署防火墙规则。如果部署永远在线 VPN，则可能需要启用分隔隧道，并配置防火墙规则，仅允许本地打印和连接移动设备访问网络。
  - 配置动态访问策略或组策略，让符合条件的 VPN 用户免于部署永远在线 VPN。
  - 当 AnyConnect 会话处于隔离状态时，请配置动态访问策略以在 AnyConnect GUI 中显示消息。
- 要执行从 4.3x 到 4.6.x 的 HostScan 迁移，需要 ASDM 7.9.2 或更高版本。

ASA 内存要求

⚠

注意 使用 AnyConnect 4.0 或更高版本的所有 ASA 5500 型号的建议最低闪存大小为 512 MB。此配置可托管多个终端操作系统并在 ASA 上启用日志记录和调试。

由于 ASA 5505 存在闪存大小限制（最大为 128 MB），并非所有 AnyConnect 软件包排列都将能够载入此型号。要成功加载 AnyConnect，您必须降低软件包的大小（即，减少操作系统数量、不使用 HostScan 等），直到能够容纳在可用闪存上。

在继续执行 AnyConnect 安装或升级前，检查可用空间大小。可以使用以下方法之一执行相关操作：

- CLI - 输入 **show memory** 命令。

```
asa3# show memory
Free memory:       304701712 bytes (57%)
Used memory:       232169200 bytes (43%)
-------------     ----------------
Total memory:      536870912 bytes (100%)
```

- ASDM - 选择“工具”(Tools)>“文件管理”(File Management)。“文件管理”(File Management) 窗口会显示闪存空间。

如果 ASA 只有默认内部闪存大小或默认 DRAM 大小（对于缓存内存），则可能无法在 ASA 上存储和加载多个 AnyConnect 客户端软件包。即使闪存有足够空间承载软件包文件，ASA 也可能会在解压缩和加载客户端映像时耗尽缓存内存。有关 ASA 内存要求以及升级 ASA 内存的其他信息，请参阅思科 ASA 5500 系列最新版本说明。

VPN 安全评估和 Hostscan 互操作性

通过 VPN 安全评估 (HostScan) 模块，Cisco AnyConnect Secure Mobility Client 可以识别 ASA 主机中安装的操作系统、反恶意软件和防火墙软件。

VPN 安全评估 (HostScan) 模块需要 Hostscan 来收集这些信息。Hostscan 作为单独的软件包提供，它会定期使用新操作系统、反恶意软件和防火墙软件信息进行更新。通常情况下，建议您运行最新版本的 HostScan（与 AnyConnect 的版本相同）。

在 HostScan 4.4 和更高版本中，防病毒软件、反间谍软件和防火墙的端点数据（端点属性）已更改。反间谍软件 *(endpoint.as)* 和防病毒 *(endpoint.av)* 均归类为反恶意软件 *(endpoint.am)*。防火墙 *(endpoint.pw)* 归类为防火墙 *(endpoint.pfw)*。有关此配置的具体信息，请参阅“AnyConnect HostScan 4.3.x 迁移到 4.6.x 及更高版本”文档。

HostScan 反恶意软件和防火墙支持图在 cisco.com 上提供。

注释 与不兼容的 HostScan 版本配合使用时，AnyConnect 将不会建立 VPN 连接。此外，思科不建议组合使用 HostScan 和 ISE 安全评估。否则，运行两种不同的安全评估代理时会出现意外结果。

提前通知 AnyConnect 4.3 HostScan 更新结束日期

AnyConnect 4.3 及更早版本的 HostScan 更新在 2018 年 12 月 31 日截止。HostScan 更新将由 HostScan 4.6（及更高版本）模块提供，与 AnyConnect 4.4.x（及更高版本）和 ASDM 7.9.2（及更高版本）兼容。本迁移指南详细介绍了 HostScan 迁移的信息。

ISE 安全评估合规性模块

ISE 安全评估合规性模块包含 ISE 安全评估支持的反恶意软件和防火墙的列表。HostScan 列表按供应商编组，ISE 安全评估列表则按产品类型编组。当前端上的版本号（ISE 或 ASA ）高于终端上的版本号时，OPSWAT 就会更新。这些升级是强制性的，无需最终用户干预即会自动进行。

库（zip 文件）中的各个文件由 OPSWAT 公司进行数字签名，而库本身被打包为单个自解压的可执行文件，由思科证书进行代码签名。有关详细信息，请参阅 ISE 合规型号。

IOS 对 AnyConnect 的支持

思科支持将 AnyConnect VPN 用作安全网关来访问 IOS 版本 15.1(2)T；但是，IOS 版本 15.1(2)T 当前不支持以下 AnyConnect 功能：

- 登录后永远在线的 VPN
- 连接失败策略
- 提供本地打印机和系留设备访问的客户端防火墙
- 最佳网关选择
- 隔离
- AnyConnect 配置文件编辑器
- DTLSv1.2

有关 IOS 对 AnyConnect VPN 的支持的其他限制，请参阅 Cisco IOS SSL VPN 不支持的功能。

有关其他 IOS 功能支持的信息，请参阅 http://www.cisco.com/go/fn。

AnyConnect 支持的操作系统

Cisco AnyConnect Secure Mobility Client 所包含的模块支持以下操作系统：

支持的操作系统	VPN 客户端	网络访问管理器	云网络安全	VPN 安全评估 (HostScan)	ISE 终端安全评估	议价授权请求工具 (DART)	客户体验反馈	网络可视性模块	AMP 启用程序	Umbrella 漫游安全
Microsoft 支持的 Windows 10 版本，适用于基于 ARM64 的 PC	支持	不支持	否	否	不支持	支持	支持	不支持	否	否
Windows 7、8、8.1 和当前 Microsoft 支持的 Windows 10 x86（32 位）和 x64（64 位）版本	支持	支持	支持	支持	支持	支持	支持	支持	支持	支持
macOS 10.13、10.14 和 10.15（从 10.15 和更高版本开始仅支持 64 位）	支持	不支持	支持	支持	支持	支持	支持	支持	支持	支持
Linux Red Hat 6、7、8.1 和 Ubuntu 16.04 (LTS)、18.04 (LTS) 和 20.04 (LTS)	支持	不支持	不支持	支持	不支持	支持	支持	支持	否	否

Microsoft Windows 对 AnyConnect 的支持

Windows 要求

- Pentium 级或更高级别的处理器。
- 100 MB 硬盘空间。
- Microsoft 安装程序版本 3.1。
- 如果是从以前的任意 Windows 版本升级到 Windows 8.1，需要卸载 AnyConnect，然后在 Windows 升级完成后重新安装 AnyConnect。

- 如果是从 Windows XP 升级到任意更高的 Windows 版本，需要执行全新安装，因为升级期间不会保留思科 AnyConnect 虚拟适配器。请手动卸载 AnyConnect，升级 Windows，然后以手动方式或通过 WebLaunch 重新安装 AnyConnect。
- 若要通过 WebLaunch 启动 AnyConnect，必须使用 Firefox 3.0+ 的 32 位版本，并启用 ActiveX 或安装 Sun JRE 1.4+。
- 使用 Windows 8 或 8.1 时，需要安装 ASDM 版本 7.02 或更高版本。

Windows 限制

- Windows RT 不支持 AnyConnect。该操作系统不提供用于执行此功能的 API。思科已就这一问题向 Microsoft 提出请求。需要此功能的用户应与 Microsoft 联系，表明对此很感兴趣。
- 其他第三方产品与 Windows 8 不兼容会导致 AnyConnect 无法通过无线网络建立 VPN 连接。下面就此问题提供两个示例：
  - 随 Wireshark 分发的 WinPcap 服务“远程数据包捕获协议 v.0（实验性）”不支持 Windows 8。

    若要解决此问题，请卸载 Wireshark 或禁用 WinPcap 服务，重新启动 Windows 8 计算机，然后重试 AnyConnect 连接。
  - 不支持 Windows 8 的过时无线网卡或无线网卡驱动程序阻止 AnyConnect 建立 VPN 连接。

    若要解决此问题，请确保在 Windows 8 计算机上安装支持 Windows 8 的最新无线网卡或驱动程序。
- AnyConnect 未与 Windows 8 上部署的新用户界面框架（称为 Metro 设计语言）集成，却在 Windows 8 的桌面型号下运行。
- HP 保护工具无法与 Windows 8.x 上的 AnyConnect 配合使用。
- 不支持 Windows 2008；但是，我们不会阻止在此操作系统上安装 AnyConnect。此外，Windows Server 2008 R2 需要可选的 SysWow64 组件
- 如果您在支持待机的系统上使用网络访问管理器，思科建议使用默认的 Windows 8.x 关联计时器值（5 秒）。如果您发现 Windows 中的扫描列表比预期短，请增加关联计时器值，让驱动程序可以完成网络扫描和填充扫描列表。

Windows 指南

- 确保客户端系统上的驱动程序受 Windows 7 或 8 支持。不受支持的驱动程序可能会出现间歇性连接问题。
- 对于网络访问管理器，在 Windows 8 或 10/Server 2012 上使用计算机密码进行计算机身份验证不起作用，除非已将 Microsoft KB 2743127 中所述的注册表修复应用于客户端桌面。此修复包括向 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa 注册表项添加 DWORD 值 LsaAllowReturningUnencryptedSecrets 并将此值设置为 1。此更改允许本地安全机构 (LSA) 向诸如思科网络访问管理器之类的客户端提供计算机密码。它与 Windows 8 或 10/Server 2012 中增

加的默认安全设置有关。使用计算机证书的计算机身份验证无需进行此更改，便可像在Windows 8 以前的操作系统上一样运行。

注释 计算机身份验证允许在用户登录之前，向网络验证客户端桌面的身份。在此期间，管理员可以执行此客户端计算机的计划管理任务。EAP链接功能也需要使用计算机身份验证，这样，RADIUS服务器便可以针对特定客户端同时验证用户和计算机的身份。在此过程中，将识别公司资产并应用适当的访问策略。例如，如果这是个人资产（PC/笔记本电脑/平板电脑），但使用的是公司凭证，终端将无法通过计算机身份验证，但可成功通过用户身份验证，并会向该用户的网络连接应用相应的网络访问限制。

- 在 Windows 8 中，“首选项”(Preferences) >“VPN”>“统计信息”(Statistics) 选项卡上的“导出统计信息”(Export Stats) 按钮会将文件保存在桌面。而在其他 Windows 版本中，系统会询问用户要将文件保存在什么位置。
- AnyConnect VPN 与 3G 数据卡兼容，这种数据卡可通过 WWAN 适配器与 Windows 7 或更高版本建立连接。

Linux 对 AnyConnect 的支持

Linux 要求

- 不支持使用没有 GUI 会话的 VPN CLI（例如 SSH）。
- Linux 上的 AnyConnect 不支持 Firefox 的 Snap 版本。Mozilla 的 Firefox 是 Linux 上受官方支持的浏览器。
- x86 指令集。
- 64 位处理器。
- 32 MB RAM。
- 20 MB 硬盘空间。
- 安装需要具备超级用户权限。
- network-manager
- libnm （libnm.so 或 libnm-glib.so）
- libstdc++ 用户必须拥有 libstdc++.so.6(GLIBCXX_3.4) 或更高版本，但必须低于版本 4。
- Java 5 (1.5) 或更高版本。唯一适用于网络安装的版本为 Sun Java。必须安装 Sun Java 并将浏览器配置为使用 Sun Java 而不是默认软件包。
- zlib - 用于支持 SSL deflate 压缩
- xterm - 仅在通过 WebLaunch 从 ASA 无客户端门户对 AnyConnect 进行初始部署时需要。

- gtk 2.24
- webkitgtk+ 2.10 或更高版本，仅当您使用 AnyConnect 嵌入式浏览器应用时才需要
- iptables 1.2.7a 或更高版本。
- 随内核 2.4.21 或 2.6 提供的 tun 模块。

AnyConnect 对 macOS 的支持

macOS 要求

- AnyConnect 需要 50 MB 的硬盘空间。
- 要正确操作 macOS，AnyConnect 的显示分辨率至少需要为 1024 x 640 像素。

macOS 指南

macOS 的 AnyConnect 4.8 已经过认证，并且正式推出安装程序磁盘映像 (dmg)。

AnyConnect 许可

有关最新的最终用户许可协议，请参阅《Cisco 最终用户许可协议，AnyConnect Secure Mobility Client 版本 4.x》。

有关我们的开源许可确认，请参阅《AnyConnect 安全移动客户端中使用的开源软件》。
http://www.cisco.com/content/en/us/support/security/anyconnect-secure-mobility-client/products-licensing-information-listing.html.

若要从 ISE 前端部署 AnyConnect 并使用 ISE 安全评估模块，需要在 ISE 管理节点上安装思科 ISE Apex 许可证。有关 ISE 许可证的详细信息，请参阅思科身份服务引擎的思科 *ISE* 许可证一章。

若要从 ASA 前端部署 AnyConnect 并使用 VPN 和 VPN 安全评估 (HostScan) 模块，需要使用 AnyConnect 4.X Plus 或 Apex 许可证、提供试用版许可证，请参阅思科 AnyConnect 订购指南。

有关 AnyConnect 4.X Plus 和 Apex 许可证的概述及各种功能所需的许可证说明，请参阅 AnyConnect 安全移动客户端功能、许可证和操作系统。

AnyConnect 安装概述

部署 AnyConnect 指安装、配置和升级 AnyConnect 客户端及其相关文件。可通过以下方法为远程用户部署Cisco AnyConnect Secure Mobility Client：

- 预部署 - 新安装和升级可以由最终用户执行，也可以由企业软件管理系统 (SMS) 执行。
- 网络部署 — AnyConnect 软件包在前端（ASA 或 ISE 服务器）加载。当用户连接到 ASA 或 ISE 时，AnyConnect 会部署到客户端。

- 对于新安装，用户可连接到前端以下载 AnyConnect 客户端。客户端可手动或自动安装（通过网络启动）。
- 更新由已安装 AnyConnect 的系统上运行的 AnyConnect 完成，或者通过将用户定向至 ASA 无客户端门户完成。

- 云更新 - 在部署 Umbrella 漫游安全模块后，可以使用上述方法之一以及云更新来更新任何 AnyConnect 模块。通过云更新，可自动从 Umbrella 云基础设施获得软件升级，且更新跟踪将取决于该软件升级，而非管理员的任何操作。默认情况下，将禁用通过云更新进行自动更新。

部署 AnyConnect 时，可以将用于启用额外功能的可选模块以及用于配置 VPN 和其他功能的客户端配置文件包含在内。请注意以下事项：

- 可以预部署所有 AnyConnect 模块和配置文件。预部署时，必须特别注意模块安装顺序和其他细节。
- 客户体验反馈模块和 VPN 安全评估模块使用的 Hostscan 软件包不能从 ISE 进行网络部署。
- ISE 安全评估模块所使用的合规性模块不能从 ASA 进行网络部署。

注释 只要升级到新的 AnyConnect 软件包，请务必使用 CCO 提供的最新版本更新本地化 MST 文件。

在 64 位 Windows 上进行基于 Web 的安装可能会失败

此问题适用于 Windows 7 和 8 上的 Internet Explorer 10 和 11。

当 Windows 注册表项 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth 设置为 0 时，ActiveX 在 AnyConnect 网络部署期间会出现问题。

有关详细信息，请参阅 http://support.microsoft.com/kb/2716529。

解决方案为：

- 运行 Internet Explorer 的 32 位版本。
- 将注册表项编辑为非零值，或从注册表删除该值。

注释 在 Windows 8 上，如果运行 64 位版本，从 Windows 开始屏幕启动 Internet Explorer。如果运行 32 位版本，则从桌面启动。

AnyConnect 支持策略

思科仅根据最近发布的 4.x 版本提供修复补丁和增强功能。签订了 AnyConnect 4.x 条款/合同、条款/合同有效且正在运行已发布 AnyConnect 4.x 版本的任何客户均可获得 TAC 支持。如果使用过时的软件版本遇到问题，系统可能会要求您验证当前的维护版本是否可解决问题。

只有已安装最新修复补丁的 AnyConnect 4.x 版本才能访问软件中心。我们建议您下载适合您部署的所有映像，因为我们无法保证您想要部署的版本将来是否仍可供下载。

规定和限制

升级到 AnyConnect 4.9.01xxx（仅限 Linux）后客户端首次自动重新连接失败

由于 CSCvu65566 修复及其设备 ID 计算变化，Linux 的某些部署（尤其是使用 LVM 的部署）在从前端更新为 4.9.01xxx 或更高版本后会立即遇到一次性连接尝试错误。运行 AnyConnect 4.8 并连接前端以执行自动更新（Web 部署）的 Linux 用户可能会收到以下错误：“安全网关已拒绝连接尝试。需要新尝试连接同一或其他安全网关，这需要重新身份验证。”要成功连接，您可以在 AnyConnect 升级后手动启动另一个 VPN 连接。初始升级到 4.9.01xxx 或更高版本后，您将不再遇到此问题。

从 AnyConnect 4.7MR4 升级后连接无线网络时可能出现问题

网络访问管理器做出了修订，以便将无线 LAN 配置文件写入到磁盘，而不是使用内存中的临时配置文件。Microsoft 为解决一个 OS 错误而提出了这一更改请求，但结果导致“无线 LAN 数据使用”窗口崩溃，最终间歇性出现无线连接问题。为防止这些问题，我们将网络访问管理器恢复为使用内存中的原始临时 WLAN 配置文件。升级到 4.8MR2 或更高版本时，网络访问管理器将删除磁盘上的大多数无线 LAN 配置文件。在定向时，操作系统 WLAN 服务无法删除某些硬配置文件，但如果有任何剩余，都会妨碍网络访问管理器连接无线网络的能力。从 4.7MR4 升级到 4.8MR2 后，如果在连接无线网络时遇到问题，请执行以下步骤：

1. 停止 Cisco AnyConnect 网络访问管理器服务。
2. 在管理员命令提示符下，输入

```
netsh wlan delete profile name=*(AC)
```

这将删除之前版本（AnyConnect 4.7MR4 到 4.8MR2）遗留的配置文件。或者，您可以查找名称中附带 **AC** 的配置文件，然后将其从本机请求方删除。

Nslookup 命令需要 macOS 修复才能按预期工作

正等待 macOS 修复来纠正 AnyConnect 版本 4.8.03036（及更高版本）中与 nslookup 命令相关的问题，即 nslookup 不通过采用拆分包含隧道配置的 VPN 隧道发送 DNS 查询。此问题最初出现在 AnyConnect 4.8.03036 中，当时该版本加入了对 CSCvo18938 缺陷的修复。Apple 建议的 CSCvo18938 更改最终揭露了另一个操作系统问题，导致 nslookup 出现有问题的行为。

Apple 已请求客户将底层操作系统问题直接上报给他们。当上报给 Apple 时，请引用 macOS 缺陷 FB7670484。作为一种临时解决办法，您可以将 VPN DNS 服务器作为参数传递到 nslookup：**nslookup [名称] [ip_dnsServer_vpn]**。

服务器证书验证错误

(CSCvu71024) 如果 ASA 前端或 SAML 提供程序使用由 AddTrust 根（或中介之一）签署的证书，则由于它们已在 2020 年 5 月到期，因此 AnyConnect 身份验证可能会失败。已到期的证书会导致 AnyConnect 失败并显示为服务器证书验证错误，直到操作系统进行所需的更新以适用 2020 年 5 月到期问题为止。

Windows DNS 客户端优化警告

当启用拆分 DNS 后，Windows 8 及更高版本中存在的 Windows DNS 客户端优化可能会导致无法解析某些域名。临时应对方法是通过更新以下注册表项禁用此类优化：

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
Value:DisableParallelAandAAAA
Data: 1
Key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient
Value: DisableSmartNameResolution
Data: 1
```

macOS 10.15 用户准备

MacOS 10.15 操作系统不支持32位二进制文件。此外，Apple 验证安装在10.15 上的所有软件是否已通过数字签名进行加密公证。为了获得最佳的用户体验，我们建议升级到 AnyConnect 4.8，因为它是在 macOS 10.15 上正式支持操作的第一个版本，不包含32位代码。

否则，请注意以下限制：

- 4.7.03052 之前的 AnyConnect 版本可能需要使用活动的互联网连接才能进行升级。
- 在 macOS 10.15 上，4.8. x 之前的 AnyConnect HostScan 版本将不起作用。请参阅 HostScan 未升级时无法与 macOS 10.15 一起运行 (CSCvq11813)，第 14 页。
- MacOS 10.15 上的 AnyConnect HostScan 和 SystemScan 用户将在初始启动期间遇到权限弹出窗口。请参阅 初始 AnyConnect HostScan 或系统扫描启动（CSCvq64942）时的权限弹出窗口，第 15 页。

HostScan 未升级时无法与 macOS 10.15 一起运行 (CSCvq11813)

4.8. x 之前的 AnyConnect HostScan 软件包无法与 macOS Catalina (10.15) 一起运行。运行 HostScan 软件包早于 4.8.x 的最终用户尝试从 macOS Catalina 连接到 ASA 前端时，无法成功完成 VPN 连接，收到终端安全评估失败的消息。

要为 HostScan 用户启用成功的 VPN 连接，所有 DAP 和 HostScan 策略均必须与 HostScan 4.8.00175（或更高版本）兼容。有关与从 HostScan 4.3. x 到 4.8. x 的策略迁移相关的其他信息，请参阅 AnyConnect HostScan 迁移 4.3. x 到 4.6. x 及更高版本。

作为恢复 VPN 连接的一种解决方法，在其 ASA 前端上具有 HostScan 软件包的系统管理员可能会禁用 HostScan。如果禁用，则所有 HostScan 终端安全评估功能以及依赖终端信息的 DAP 策略均不可用。

相关字段通知可以在此处找到： https://www.cisco.com/c/en/us/support/docs/field-notices/704/fn70445.html。

初始 AnyConnect HostScan 或系统扫描启动（CSCvq64942）时的权限弹出窗口

macOS 10.15（及更高版本）要求应用获取用户访问桌面、文档、下载和网络卷文件夹的权限。要授予此访问权限，您可以在初始启动 HostScan、系统扫描（在网络上启用 ISE 终端 安全评估时）或 DART（在执行 ISE 终端安全评估或安装 HostScan 时）时，查看弹出窗口。ISE 终端安全评估和 HostScan 均使用 OPSWAT 对终端进行终端安全评估，且终端安全评估检查根据配置的产品和策略访问这些文件夹。

在这些弹出窗口中，您必须单击**确定**以访问这些文件夹，并继续执行终端安全评估流程。如果单击**不允许**，终端可能不会保持合规，并且终端安全评估和补救可能会失败而不能访问这些文件夹。

要更正不允许选择

要再次查看这些弹出窗口并授予对文件夹的访问权限，请编辑缓存设置：

1. 打开**系统首选项**。
2. 导航至**安全和隐私** > **隐私** > **文件和文件夹** > 。
3. 在Cisco AnyConnect Secure Mobility Client 文件夹中，删除文件夹访问相关的缓存详细信息。

权限弹出窗口将再次出现，并显示后续终端安全评估的开始，用户可以单击**确定**以授予访问权限。

目前不支持在 macOS 上进行 GUI 自定义

目前不支持在 macOS 上进行 GUI 资源自定义。在 4.8 的后续版本中，我们正在努力增强 GUI 资源自定义功能。

与 SentinelOne 不兼容

AnyConnect 伞模块与 SentinelOne 终端安全软件不兼容。

升级到 4.8 后 macOS 管理隧道断开连接

如果您遇到以下任何一种情况，则涉及改进安全性以遵守 Apple 公证：

- 您与 AnyConnect 4.7 的管理隧道连接，但 AnyConnect 4.8 版本在同一环境中失败。
- VPN 统计信息窗口显示 “断开连接(连接失败)” 作为管理隧道状态。
- 控制台日志指示“证书验证失败”，表示管理隧道断开连接。

如果配置为允许访问（不提示）到 AnyConnect 应用或可执行文件，则在升级到 AnyConnect 4.8 后，必须重新添加该应用或可执行文件，然后才能重新配置 ACL。您必须更改密钥链访问系统存储库中的私钥访问权限，才能包括来自4.8 的 vpnagentd 进程：

1. 导航至**系统密钥链** > **系统** > **我的证书** > **私钥**。
2. 从“访问控制”选项卡中删除 vpnagentd 进程。
3. 将当前 vpnagentd 添加到/opt/cisco/anyconnect/bin 文件夹中。
4. 出现提示时，输入密码。
5. 退出 Keychain Access 并停止 VPN 服务。
6. 重新启动。

在 ISE 终端安全评估中未检测到默认补丁管理 (CSCvq64901)

在使用 macOS 10.15 时，ISE 终端安全评估无法检测默认补丁管理。需要进行 OPSWAT 修复才能解决这种情况。

网络访问管理器不支持基于 PMK 的漫游

在 Windows 上，不能在网络访问管理器中使用基于 PMK 的漫游。

DART 需要管理员权限

由于系统安全限制，DART 现在需要 macOS、Ubuntu 18.04 和 Red Hat 7 的管理员权限才能收集日志。

在 FIPS Mode 型号下进行已恢复 IPsec 连接 (CSCvm87884)

使用版本 4.6.2 和 4.6.3 的 AnyConnect 客户遇到了 IPsec 连接问题。在 AnyConnect 版本 4.7（及更高版本）中恢复 IPsec 连接 (CSCvm87884) 后，将不再支持 FIPS 型号下的 Diffie-hellman 组 2 和 5。因此，在 FIPS 型号下 AnyConnect 无法再连接到 9.6 以下版本的 ASA，也无法使用配置控制 DH 组 2 或 5。

Firefox58 上证书存储数据库的更改（NSS 库更新）

（仅影响使用 *58* 之前的 *Firefox* 的用户）由于 NSS 证书存储区数据库格式更改从 Firefox 58 开始，AnyConnect 也会进行更改以使用新的证书数据库。如果使用 58 之前的 Firefox 版本，请将 NSS_DEFAULT_DB_TYPE="sql" 环境变量设置为 58，以确保 Firefox 和 AnyConnect 访问相同的数据库文件。

网络访问管理器和组策略冲突

如果您的有线或无线网络设置或特定 SSID 从 Windows 组策略推送，它们可能会与网络访问管理器的正常运行冲突。在安装了网络访问管理器的情况下，不支持无线设置的组策略。

使用 Windows 10 版本 1703 (CSCvg04014) 的网络访问没有隐藏扫描列表

Windows 10 版本 1703 更改了其 WLAN 行为，这会导致网络访问管理器扫描无线网络 SSID 时出现中断。由于 Microsoft 正在检查的 Windows 代码存在漏洞，因此网络访问管理器尝试访问隐藏网络的行为会受到影响。为了提供最佳户体验，我们已在网络访问管理器安装期间对两个注册表项进行设置，禁用了 Microsoft 的新功能，然后在卸载过程中将其此设置删除。

AnyConnect macOS 10.13 (High Sierra) 的兼容性

推荐用于 macOS 10.13 (High Sierra) 的 AnyConnect 版本为 AnyConnect 4.5.02XXX 及更高版本。

AnyConnect 4.5.02XXX 和更高版本包含附加功能和警告，可以通过在其 macOS“Preferences”（首选项）->“Security & Privacy”（安全和隐私）窗格中启用 AnyConnect 软件扩展，指导用户完成利用 AnyConnect 全部功能所需的步骤。需要手动启用软件扩展是 macOS 10.13 (High Sierra) 中的一项新操作系统要求。此外，如果在将用户系统升级到 macOS 10.13 和更高版本之前，先将 AnyConnect 升级到 4.5.02XXX 及更高版本，则用户将自动启用 AnyConnect 软件扩展。

运行 macOS 10.13（及更高版本）的用户，如果其 AnyConnect 版本低于 4.5.02XXX，则必须在其 macOS“首选项 -> 安全和隐私”窗格中启用 AnyConnect 软件扩展。虽然 AnyConnect 4.4.04030 和 4.5.01044 经过测试可与 macOS 10.13（及更高版本）一起使用，这些用户将没有添加到 AnyConnect 4.5.02XXX 的附加功能和警告指导。对于低于 AnyConnect 4.5.02xxx 的版本，在启用扩展后，您可能需要手动重新引导。

如 https://support.apple.com/en-gb/HT208019 中所述，macOS 系统管理员可能有其他功能来禁用“用户批准的内核扩展加载”，这对任何目前受支持的 AnyConnect 版本都有效。

发生电源事件或网络中断时对安全评估的影响

如果发生网络变化或电源事件，则被中断的安全评估过程将不会自动完成。网络或电源变化会导致 AnyConnect 下载错误，用户必须确认此错误，然后才能继续进行此过程。

网络访问管理器无法自动回退到 WWAN/3G/4G

所有通向 WWAN/3G/4G 的连接必须由用户手动触发。如果没有任何有线或无线连接可用，网络访问管理器则不会自动连接到这些网络。

由于签名/文件完整性验证错误，NAM 网络部署、DART、ISE 安全评估和/或安全评估失败

此“时间戳签名和/或证书无法验证或格式错误”仅在从 ASA 或 ISE AnyConnect 4.4 M R 2（或更高版本）的网络部署期间在 Windows 上发生。仅作为 MSI 文件部署的 NAM、DART、ISE 安全评估和安全评估模块会受到影响。由于使用的是 SHA-2 时间戳证书服务，因此需要最新的受信任根证书才能正确验证时间戳证书链。对于预部署或已配置为自动更新根证书的开箱即用的 Windows 系统，不会出现此问题。但是，如果已禁用“自动根证书更新”设置（不是默认设置），请参考 https://technet.microsoft.com/en-us/library/dn265983(v=ws.11).aspx 或手动安装我们使用的时间戳根证书。您还可以使用签名工具验证问题是否为 AnyConnect 以外的问题，方法是运行

```
signtool.exe verify /v /all/debug/pa<file to verify>
```

Microsoft 提供的 Windows SDK 命令。

身份验证期间的 macOS 密钥链提示

在 macOS 上，启动 VPN 连接后可能会出现密钥链身份验证提示。只有在从安全网关发出客户端证书请求后，需要访问客户端证书私钥时，才会出现提示。即使隧道组未配置证书身份验证，也可以在ASA上配置证书映射，这会导致当客户端证书私钥的访问控制设置配置为允许访问之前确认时，出现密钥链提示。

配置 AnyConnect VPN 配置文件以将 AnyConnect 访问严格限制为从登录密钥链访问客户端证书（在 ASDM 配置文件编辑的“首选项（第 1 部分）- 证书存储 - macOS”下选择“登录”。您可以使用以下操作之一来停止密钥链身份验证提示：

- 在客户端配置文件中配置证书来匹配条件，以排除已知的系统密钥链证书。
- 在系统密钥链中配置客户端证书私钥的访问控制设置，以允许访问 AnyConnect。

Umbrella 漫游安全插件更改

https://dashboard.umbrella.com 现已提供控制面板，可用于检索 `OrgInfo.json` 文件。从此处，您可以导航到**身份 > 漫游计算机**，单击左上角的 +（“添加”图标），然后从 AnyConnect Umbrella 漫游安全模块部分单击**模块配置文件**。

当安装了网络访问管理器时，Microsoft 无意中阻止了 Windows 10 的更新

当安装了网络访问管理器时，Microsoft 旨在阻止对较早版本 Windows 的更新，但无意中也阻止了 Windows 10 和 Creators Edition (RS2)。由于发生错误 (Microsoft Sysdev 11911272)，您必须首先卸载网络访问管理器模块，才能升级到 Creators Editor (RS2)。然后，可以在升级后重新安装该模块。Microsoft 计划于 2017 年 6 月推出针对此错误的修复。

Windows 10 Defender 误报 - 思科 AnyConnect 适配器问题

当升级到 Windows 10 Creator Update（2017 年 4 月）时，您可能会收到 Windows Defender 消息，说 AnyConnect 适配器出现问题。Windows Defender 指示您在“设备性能和运行状况”(Device Performance and Health) 部分下启用适配器。实际上，不使用该适配器时应将其禁用，不应采取手动操作。这种误报错误会以 Sysdev # 11295710 代码报告给 Microsoft。

AnyConnect 4.4MR1（或更高版本）和 4.3MR5 与 Windows 10 Creators 版本 (RS2) 兼容。

与 Microsoft Windows 10 的 AnyConnect 兼容性

AnyConnect 4.1MR4(4.1.04011) 及更高版本与 Windows 10 正式版兼容。技术支持中心 (TAC) 支持从 2015 年 7 月 29 日开始提供。

为获得最佳效果，我们建议在 Windows 10 系统上执行 AnyConnect 的全新安装，而不要从 Windows 7/8/8.1 升级。如果计划从已预安装 AnyConnect 的 Windows 7/8/8.1 升级，请确保先升级 AnyConnect，然后再升级操作系统。在升级到 Windows 10 之前，**必须**卸载网络访问管理器模块。在系统升级完成

后，可以在系统上重新安装网络访问管理器。还可以选择完全卸载 AnyConnect，然后在升级到 Windows 10 后，重新安装一个受支持的版本。

新拆分包含隧道行为 (CSCum90946)

过去，如果拆分-包含 (split-include) 网络是本地子网的超网，则不会通过隧道传输本地子网流量，除非配置的拆分-包含 (split-include) 网络与本地子网完全匹配。随着对 CSCum90946 的解析，当拆分-包含网络是本地子网的超网时，本地子网流量可通过隧道传输，除非在访问列表 (ACE/ACL) 中还配置了拆分排除（拒绝 0.0.0.0/32 或 ::/128）。

如果在拆分-包含中配置了超网并且所需行为是要允许 LocalLan 访问，则需要对这一引入 AnyConnect 版本 4.2MR1 的行为进行以下配置：

- 访问列表 (ACE/ACL) 必须同时包含针对超网的许可操作以及针对 0.0.0.0/32 或 ::/128 的拒绝操作。
- 在 AnyConnect 配置文件中启用“本地 LAN 访问”(Local LAN Access)（在配置文件编辑器的“首选项第 1 部分”[Preferences Part 1] 菜单中）。（另外，您还可以使用该选项将其设为用户可控制。)

Microsoft 正在逐步淘汰 SHA-1 支持

2017 年 2 月 14 日后，Windows Internet Explorer 11/Edge 浏览器或 Windows AnyConnect 终端使用 SHA-1 证书的安全网关或以 SHA-1 为中间证书的证书可能不再被视为有效。2017 年 2 月 14 日后，Windows 终端可能认为使用 SHA-1 证书的安全网关或中间证书不再可信。我们强烈建议您的安全网关不要使用 SHA-1 身份证书，也不要再使用 SHA-1 作为任何中间证书。

Microsoft 已对其原有的记录和计时计划进行修改。他们发布了有关如何测试 2017 年 2 月的变更是否会影响您的环境的详细信息。对于使用 SHA-1 安全网关或中间证书或运行旧版 AnyConnect 的客户，思科无法对 AnyConnect 的正常运行做出任何保证。

思科强烈建议客户密切关注 AnyConnect 的最新维护版本，以确保随时获取所有可用的修复补丁。签有有效 AnyConnect Plus、Apex 和仅 VPN 条款/合同的客户，可通过 Cisco.com 软件中心获取最新版本 AnyConnect 4.x 及更高版本。不再对 AnyConnect 版本 3.x 实施主动维护，亦不应再使用它们进行任何部署。

注释 在 Microsoft 逐步淘汰 SHA-1 的同时，思科已确认 AnyConnect 4.3 和 4.4（及更高版本） 可以继续正常运行。长期来看，Microsoft 计划在所有环境下的 Windows 中都不再信任 SHA-1，但他们当前的公告尚未就此提供任何细节或时间信息。根据淘汰的确切日期，许多较早版本的 AnyConnect 随时可能无法再正常运行。有关更多信息，请参阅 Microsoft 公告。

使用 SHA512 证书进行身份验证时，身份验证失败

（对于 Windows 7、8 和 8.1 用户），当客户端使用 SHA512 证书进行身份验证时，身份验证失败，即使客户端日志显示该证书处于使用状态，亦不例外。ASA 日志可正确显示 AnyConnect 未发送任何证书。Windows 的这些版本要求您在 TLS 1.2 中启用对 SHA512 证书的支持，系统默认情况下不

支持该证书。要了解如何对这些 SHA512 证书提供支持，请参阅 https://support.microsoft.com/en-us/kb/2973337。

OpenSSL 密码套件更改

由于 OpenSSL 标准开发团队将部分密码套件标记为已被泄露，在 AnyConnect 3.1.05187 以外，我们不再对这些密码套件提供支持。不受支持的密码套件如下：DES-CBC-SHA、RC4-SHA 和 RC4-MD5。

同样，我们的加密工具包已中断对 RC4 密码的支持；因此，我们对其的相应支持也将随版本 3.1.13011 和 4.2.01035 等终止。

在 ISE 安全评估中使用日志跟踪

在全新安装后，您会按预期看到 ISE 安全评估日志跟踪消息。但是，如果进入 ISE 安全评估配置文件编辑器并将“启用代理日志跟踪”(Enable Agent Log Trace) 文件更改为 0（禁用），则必须执行 AnyConnect 服务重新启动来获得预期结果。

在 macOS 上使用 ISE 终端安全评估的互操作性

如果使用 macOS 10.9 或更高版本并想要使用 ISE 终端安全评估，可能需要执行以下操作来避免出现问题：

- 在安全评估期间，关闭证书验证以避免出现“无法联系策略服务器”(failed to contact policy server") 错误。
- 禁用强制网络门户应用；否则，发现探测会被阻止，且应用仍会处于安全评估前的 ACL 状态。

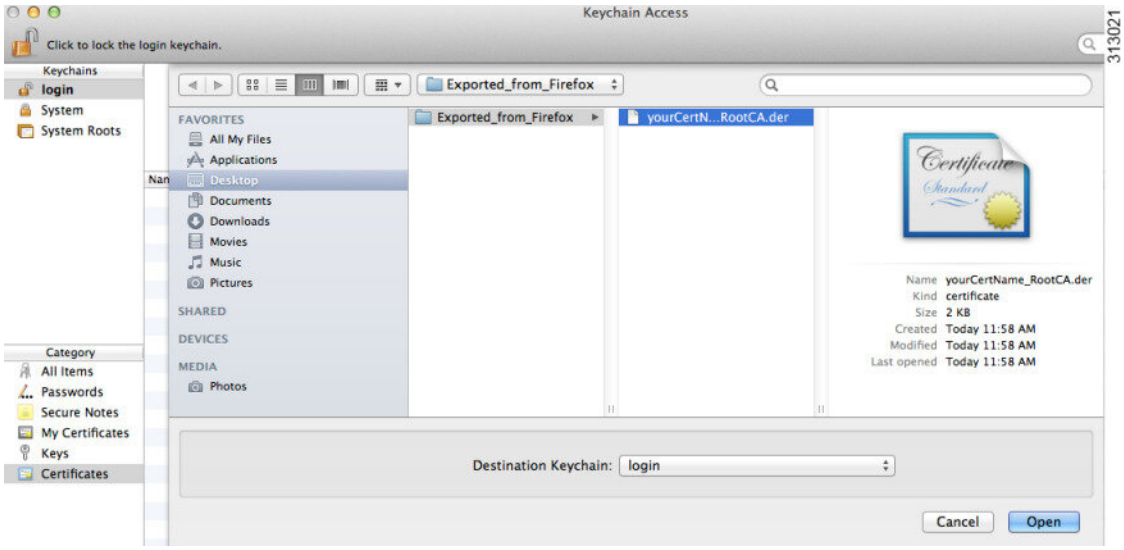
不支持在 macOS 上使用 Firefox 证书存储

macOS 上的 Firefox 证书存储在存储时提供允许所有用户修改存储内容的权限，这让未授权用户或进程能够将非法 CA 添加到受信任的根存储中。AnyConnect 不再将 Firefox 存储用于服务器验证或客户端证书。

如有必要，请向您的用户说明如何从 Firefox 证书存储库中导出 AnyConnect 证书，以及如何将它们导入到 macOS 密钥链。以下步骤是可能需要告知 AnyConnect 用户的内容示例。

1. 导航到 **Firefox > 首选项 > 隐私和安全 > 高级**的“证书”选项卡，然后单击**查看证书**。
2. 选择用于 AnyConnect 的证书，然后单击 **导出 (Export**）。

   您的 AnyConnect 证书很可能在“颁发机构”(Authorities) 类别下。请与您的证书管理员核实，因为这些证书可能在其他类别（“您的证书”[Your Certificates] 或“服务器”[Servers]）之下。
3. 选择一个位置用于保存证书，例如，位于桌面的文件夹。
4. 在“格式”(Format) 下拉菜单中，选择 **X.509 证书 (DER) (X.509 Certificate [DER])**。如果需要，将 .der 扩展名添加到证书名称。

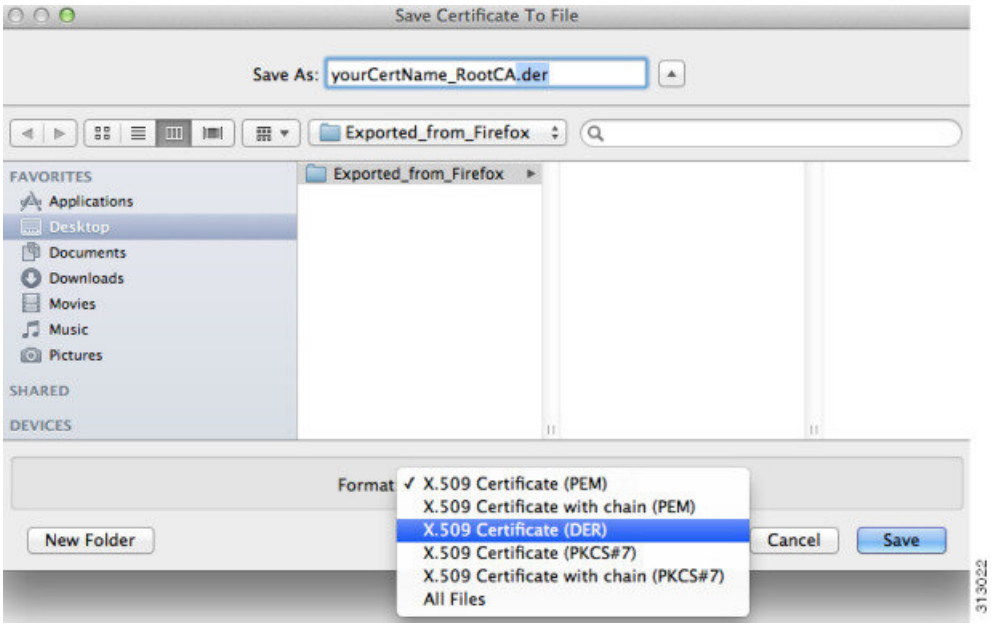


注释 如果使用/需要多个 AnyConnect 证书和/或私钥，请对每个证书重复上述流程）。

5. 启动秘钥链。导航到“文件”(File)、“导入项目...”(Import Items...)，然后选择从 Firefox 导出的证书。

   在“目标密钥链：”(Destination Keychain:) 中，选择所需的密钥链。您公司使用的登录密钥链可能与本例中所用的登录密钥链不同。请咨询证书管理员，了解应将您的证书导入哪个密钥链。

6. 在“目标密钥链：”(Destination Keychain:) 中，选择所需的密钥链。您公司使用的登录密钥链可能与本例中所用的登录密钥链不同。请咨询证书管理员，了解应将您的证书导入哪个密钥链。



7. 对 AnyConnect 使用或需要的其他证书重复前述步骤。

SSLv3 阻止 HostScan 正常工作

(CSCue04930) 在 ASDM 中选择 SSLv3 “仅限 SSLv3”或“协商 SSLv3”选项时，HostScan 不会正常工作（配置 > 远程访问 VPN > 高级 > SSL 设置 > 要作为服务器协商的安全设备的 SSL 版本）。ASDM 中会显示警告消息，用于提醒管理员。

Safari 的 WebLaunch 问题

Safari 的 WebLaunch 存在问题。OS X 10.9 (Mavericks) 随附的 Safari 版本中的默认安全设置阻止 AnyConnect WebLaunch 正常工作。若要配置 Safari 允许使用 WebLaunch，请如下所述，将 ASA 的 URL 编辑为不安全型号。

Safari 9（及更早版本）

1. 打开 Safari **首选项**。
2. 选择**安全**首选项。
3. 单击**管理网站设置 ...** 按钮。
4. 从左侧列出的选项中选择 **Java** 。
5. 对于您尝试连接的网站 "Hostname_or_IP_address"，将该选项从**屏蔽**更改为**无间断**。
6. 单击**完成**。

Safari 10（及更高版本）

1. 打开 Safari **首选项**。
2. 选择**安全**首选项。
3. 将**互联网插件:** 选项选中为**允许插件**。
4. 选择**插件设置**按钮。
5. 从左侧列出的选项中选择 **Java** 。
6. 突出显示您尝试连接的 "Hostname_or_IP_address"。
7. 按住 **Alt**（或**选项**），然后单击下拉菜单。确保选中**打开**，且取消选中**在安全型号下运行**。
8. 单击**完成**。

ActiveX 升级可能会禁用 WebLaunch

可使用受限用户帐户通过 WebLaunch 自动升级 AnyConnect 软件，但前提是不需要对 ActiveX 控件进行更改。

有时，由于安全修复或新增功能等原因，该控件将更改。

如果通过受限用户帐户调用时，该控件要求升级，那么管理员必须使用 AnyConnect 预安装程序、SMS、GPO 或其他管理部署方法部署该控件。

Java 7 问题

Java 7 可能会导致 AnyConnect 安全移动客户端、HostScan、CSD 和无客户端 SSL VPN (WebVPN) 出现问题。有关问题和解决方法的说明，请参阅故障排除技术说明与 AnyConnect，CSD / Hostscan 和 WebVPN 相关的 Java 7 问题 - 故障排除指南。详细信息请查阅“安全”(Security) > “思科 Hostscan”(Cisco Hostscan) 下的思科文档。

配置“所有网络通过隧道”(Tunnel All Networks) 时应用隐式 DHCP 过滤器

在配置“所有网络通过隧道”(Tunnel All Networks) 的情况下，为了让本地 DHCP 流量能够不受阻碍地传输，AnyConnect 在 AnyConnect 客户端连接时将向本地 DHCP 服务器添加特定路由。为了防止此路由出现数据泄露，AnyConnect 还对主机计算机的局域网适配器应用隐式过滤器，在该路由中阻止除 DHCP 流量外的所有流量。

系留设备上的 AnyConnect VPN

思科仅在通过蓝牙或 USB 连接的 Apple iPhone 上通过 AnyConnect VPN 客户端资格审查。对于其他连接设备提供的网络连接，应在部署前面向 AnyConnect VPN 客户端进行验证。

AnyConnect 智能卡支持

AnyConnect 在以下环境中支持智能卡提供的凭证：

- Windows7、Windows 8 和 Windows 10 中的 Microsoft CAPI 1.0 和 CAPI 2.0。
- macOS 上的密钥链，以及 macOS 10.12 及更高版本上的 CryptoTokenKit。

注释 AnyConnect 不支持 Linux 或 PKCS #11 设备上的智能卡。

AnyConnect 虚拟测试环境

思科使用以下虚拟机环境执行部分 AnyConnect 客户端测试：

- VM Fusion 7.5.x、10.x、11.5.x
- ESXi Hypervisor 6.0.0、6.5.0 和 6.7.x
- VMware Workstation 15.x

我们不支持在虚拟环境中运行 AnyConnect；但是，我们预期 AnyConnect 会在我们执行测试的 VMWare 环境中正常运行。

如果您在虚拟环境中遇到任何 AnyConnect 问题，请报告给我们。我们将尽力解决这些问题。

UTF-8 字符对 AnyConnect 密码的支持

与 ASA 8.4(1) 或更高版本配合使用的 AnyConnect 3.0 或更高版本在使用 RADIUS/MSCHAP 和 LDAP 协议发送的密码中支持 UTF-8 字符。

禁用自动更新可能会因版本冲突而阻止连接

如果对运行 AnyConnect 的客户端禁用自动更新，ASA 必须安装相同的 AnyConnect 版本或更低版本，否则客户端无法连接到 VPN。

若要避免此问题，请在 ASA 上配置相同版本或更低版本的 AnyConnect 软件包，或通过启用自动更新将客户端升级到新版本。

网络访问管理器与其他连接管理器之间的互通性

当网络访问管理器运行时，它会对网络适配器进行独占控制，并会阻止其他软件连接管理器（包括 Windows 本地连接管理器）尝试建立连接。因此，如果希望 AnyConnect 用户使用终端计算机上的其他连接管理器（例如 iPassConnect Mobility Manager），则必须通过网络访问管理器 GUI 上的“禁用客户端”(Disable Client) 选项，或通过停止网络访问管理器服务，来禁用网络访问管理器。

网络接口卡驱动程序与网络访问管理器不兼容

Intel 无线网络接口卡驱动程序版本 12.4.4.5 与网络访问管理器不兼容。如果此驱动程序与网络访问管理器安装在同一终端上，可能会导致不一致的网络连接和 Windows 操作系统突然关闭。

避免 SHA 2 证书验证失败 (CSCtn59317)

AnyConnect 客户端利用证书的 Windows 密码运营商 (CSP) 对 IPsec/IKEv2 VPN 连接的 IKEv2 身份验证阶段所需数据进行哈希计算和签名。如果 CSP 不支持 SHA 2 算法，且为伪随机功能 (PRF) SHA256、SHA384 或 SHA512 配置了 ASA，并同时为证书或证书和 AAA 身份验证配置了连接配置文件（隧道组），则证书身份验证失败。用户收到“证书验证失败”(Certificate Validation Failure) 消息。

对于属于不支持 SHA 2 类算法的 CSP 的证书，此验证失败仅发生在 Windows 上。其他支持的操作系统不存在此问题。

若要避免此问题，可以将 ASA 上 IKEv2 策略的 PRF 配置为 md5 或 sha (SHA 1)。或者，可以将证书 CSP 值修改为有效的本地 CSP，例如 Microsoft 增强 RSA 和 AES 加密提供程序。请勿将此变通方法应用于智能卡证书。不能更改 CSP 名称。而应联系智能卡提供商，获取支持 SHA 2 算法的更新 CSP。

⚠

注意 如果未能正确执行下述变通操作，则可能会损坏用户证书。指定证书更改时，请格外谨慎。

您可以使用 Microsoft Certutil.exe 实用程序修改证书 CSP 值。Certutil 是管理 Windows CA 的命令行实用程序，在 Microsoft Windows Server 2003 管理工具包中提供。您可以从以下 URL 下载工具包：

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&displaylang=en

按以下步骤运行 Certutil.exe 和更改证书 CSP 值：

1. 打开终端计算机上的命令窗口。
2. 使用以下命令，查看用户存储中的证书及其当前的 CSP 值：**certutil -store -user My**

   以下示例显示了通过此命令显示的证书内容：

```
================ Certificate 0 ================
Serial Number: 3b3be91200020000854b
Issuer: CN=cert-issuer, OU=Boston Sales, O=Example Company, L=San Jose,
S=CA, C=US, E=csmith@example.com
NotBefore: 2/16/2011 10:18 AM
NotAfter: 5/20/2024 8:34 AM
Subject: CN=Carol Smith, OU=Sales Department, O=Example Company, L=San Jose, S=C
A, C=US, E=csmith@example.com
Non-root Certificate
Template:
Cert Hash(sha1): 86 27 37 1b e6 77 5f aa 8e ad e6 20 a3 14 73 b4 ee 7f 89 26
  Key Container = {F62E9BE8-B32F-4700-9199-67CCC86455FB}
  Unique container name: 46ab1403b52c6305cb226edd5276360f_c50140b9-ffef-4600-ada
6-d09eb97a30f1
  Provider = Microsoft Enhanced RSA and AES Cryptographic Provider
Signature test passed
```

3. 识别证书的 <CN> 属性。在此示例中，CN 是 Carol Smith。您会在下一步中需要此信息。
4. 使用以下命令修改证书CSP。以下示例使用主题<CN>值选择要修改的证书。您也可以使用其他属性。

   在 Windows 7 或更高版本上，使用此命令：**certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider" -f -repairstore -user My <CN> carol smith**

5. 重复第 2 步并验证证书出现的新 CSP 值。

为 AnyConnect 配置防病毒应用

防病毒软件、反恶意软件和入侵防御系统 (IPS) 等应用可以将 思科 AnyConnect 应用的行为误判为恶意行为。您可以配置例外以避免此类误判。安装 AnyConnect 模块或软件包后，请配置您的防病毒软件以允许 Cisco AnyConnect 安装文件夹，或将 Cisco AnyConnect 应用程序归为安全例外。

下面列出了要排除的通用目录，但列表可能不完整：

- C:\Users\<user>\AppData\Local\Cisco
- C:\ProgramData\Cisco
- C:\Program Files x86)\Cisco

为 HostScan 配置防病毒应用

防病毒应用可能会将安全评估模块包括的部分应用以及 HostScan 软件包的行为误判为恶意行为。在安装安全评估模块或 HostScan 软件包之前，请配置防病毒软件以便允许运行以下 HostScan 应用程序或将其归为安全例外项：

- cscan.exe
- ciscod.exe
- cstub.exe

IKEv2 不支持公共代理

IKEv2 不支持公共侧代理。如果您需要支持该功能，请使用 SSL。根据安全网关发送的配置指令，IKEv2 和 SSL 均支持专用侧代理。IKEv2 应用从网关发送的代理配置，随后的 HTTP 流量应遵循该代理配置。

IKEv2 可能要求对组策略进行 MTU 调整

AnyConnect 有时会接收并丢弃某些路由器的数据包片段，这会导致某些网络流量无法通过。

若要避免此问题，请降低 MTU 值。我们建议使用 1200。以下示例展示如何使用 CLI 执行此操作：

```
hostname# config t
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

若要使用 ASDM 设置 MTU，请转到**配置** > **网络（客户端）访问** > **组策略** > **添加** 或**编辑** > **高级** > **SSL VPN 客户端**。

使用 DTLS 时会自动调整 MTU

如果 DTLS 启用失效对等项检测 (DPD)，客户端会自动确定路径 MTU。如果之前使用 ASA 降低了 MTU，则应将该设置还原为默认值 (1406)。在建立隧道连接期间，客户端使用特殊 DPD 数据包自动调整 MTU。如果仍有问题，请如之前那样，使用 ASA 中的 MTU 配置来限制 MTU。

网络访问管理器和组策略

Windows Active Directory 无线组策略管理部署到特定 Active Directory 域中的 PC 上的无线设置和所有无线网络。安装网络访问管理器时，管理员必须了解可能影响网络访问管理器行为的特定无线组策略对象 (GPO)。管理员应在执行完整 GPO 部署前针对网络访问管理器测试 GPO 策略设置。以下 GPO 条件可能会阻止网络访问管理器按预期运行：

- 使用 Windows 7 或更高版本时，**仅对允许的网络使用组策略配置文件 (Only use Group Policy profiles for allowed networks)** 选项。

与网络访问管理器配合使用的 FreeRADIUS 配置

若要使用网络访问管理器，可能需要调整 FreeRADIUS 配置。默认禁用所有与 ECDH 相关的密码，以防出现漏洞。在 /etc/raddb/eap.conf 中，更改 cipher_list 值。

在无线接入点之间漫游时需要进行完整身份验证

当客户端在同一网络的无线接入点之间漫游时，运行 Windows 7 或更高版本的移动终端必须执行完整的 EAP 身份验证，而不能利用更加快速的 PMKID 重新关联。因此，在某些情况下，如果有效配置文件需要，AnyConnect 会提示用户为每次完整身份验证输入凭证。

IPv6 网络流量的思科云网络安全行为用户准则

除非已指定 IPv6 地址、域名、地址范围或通配符，否则 IPv6 网络流量会被发送至扫描代理并由扫描代理执行 DNS 查找，以确定是否存在与用户尝试连接的 URL 对应的 IPv4 地址。如果扫描代理找到 IPv4 地址，它会使用该地址进行连接。如果未找到 IPv4 地址，则会终止连接。

如果希望所有 IPv6 流量绕过扫描代理，可以为所有 IPv6 流量添加此静态例外 ::/0。执行此操作会使所有 IPv6 流量绕过所有扫描代理。这意味着 IPv6 流量不受思科云网络安全的保护。

阻止局域网中的其他设备显示主机名

在用户使用 AnyConnect 在远程局域网上与 Windows 7 或更高版本建立 VPN 会话后，用户局域网中其他设备上的网络浏览器会显示受保护远程网络上的主机的名称。但是，其他设备无法访问这些主机。

若要确保 AnyConnect 主机阻止主机名（包括 AnyConnect 终端主机的名称）在子网间泄露，请将该端点配置为永不成为主要或备用浏览器。

1. 在“搜索程序和文件”文本框中输入 **regedit**。
2. 导航到 **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\Parameters**
3. 双击 **MaintainServerList**。

“编辑字符串”(Edit String) 窗口将打开。

1. 输入 **No**。
2. 单击 **OK**。
3. 关闭“注册表编辑器”(Registry Editor) 窗口。

证书吊销消息

在分发点仅内部可访问的情况下，如果 AnyConnect 尝试验证指定 LDAP 证书吊销列表 (CRL) 分发点的服务器证书，系统会在身份验证后显示 AnyConnect 证书吊销警告弹出窗口。

若要避免显示此弹出窗口，请执行以下操作之一：

- 在没有任何隐私 CRL 要求的情况下获取证书。
- 在 Internet Explorer 中禁用服务器证书吊销检查。

注意 在 Internet Explorer 中禁用服务器证书吊销检查可能会对操作系统的其他用途产生严重安全影响。

本地化文件中的消息可以长达多行

如果尝试在本地化文件中搜索消息，这些消息可以长达多行，如以下示例所示：

```
msgid ""
"The service provider in your current location is restricting access to the "
"Secure Gateway. "
```

macOS 版 AnyConnect 部署于特定类型路由器之后的性能

当 macOS 版 AnyConnect 客户端尝试与运行 IOS 的网关建立 SSL 连接时，或者当该 AnyConnect 客户端尝试使用特定类型的路由器（例如思科虚拟办公室 [CVO] 路由器）与 ASA 建立 IPsec 连接时，某些网络流量可以通过该连接，而其他流量则无法通过。AnyConnect 可能会错误地计算 MTU。

若要解决此问题，请从 macOS 命令行使用以下命令，将 AnyConnect 适配器的 MTU 手动设置为较低的值：

`sudo ifconfig utun0 mtu 1200`（适用于 macOS v10.7 及更高版本）

防止 Windows 用户规避永远在线功能

在 Windows 计算机上，具有有限或标准权限的用户有时可能对其程序数据文件夹具有写入访问权限。这让他们能够删除 AnyConnect 配置文件，由此规避永远在线功能。若要避免这种情况，请将计算机配置为限制对 `C:\ProgramData` 文件夹的访问，或至少配置为限制对 Cisco 子文件夹的访问。

避免使用无线承载网络

使用 Windows 7 或更高版本的无线承载网络功能会让 AnyConnect 变得不稳定。使用 AnyConnect 时，不建议启用此功能或运行启用此功能的前端应用（例如 Connectify 或虚拟路由器）。

AnyConnect 不需要将 ASA 配置为需要 TLSv3 流量

AnyConnect 要求 ASA 接受 TLSv1 或 TLSv1.2 流量，而不是 SSLv3 流量。SSLv3 密钥派生算法在使用 MD5 和 SHA-1 时会弱化密钥派生。SSLv3 的后续协议 TLSv1 解决了 SSLv3 中存在的这一问题及其他安全问题。

因此，AnyConnect 客户端无法使用“ssl server-version”的以下 ASA 设置建立连接：

ssl server-version sslv3

ssl server-version sslv3-only

在安装时与 Trend Micro 发生冲突

如果设备上有 Trend Micro，网络访问管理器将因驱动程序冲突而不会安装。可卸载 Trend Micro 或取消选中 **trend micro common firewall driver** 来绕过该问题。

HostScan 报告内容

受支持的反恶意软件和防火墙产品均不会报告上次扫描时间信息。HostScan 会报告以下内容：

- 对于反恶意软件
  - 产品描述
  - 产品版本
  - 文件系统保护状态（主动扫描）
  - 数据文件时间（上次更新时间和时间戳）
- 对于防火墙
  - 产品描述
  - 产品版本
  - 是否已启用防火墙

长时间重新连接 (CSCtx35606)

如果启用 IPv6，且 Internet Explorer 中启用了代理设置的自动发现或当前网络环境不支持代理设置的自动发现，那么可能在 Windows 中体验到长时间重新连接。解决方法是，在当前网络环境不支持代理自动发现的情况下，断开 VPN 连接未使用的所有物理网络适配器或在 IE 中禁用代理自动发现。在版本 3.1.03103 中，具有多宿主系统的用户也可能会体验到长时间重新连接。

具有有限权限的用户无法升级 ActiveX

在 Windows 7 或更高版本上，具有有限权限的用户帐户无法升级 ActiveX 控件，并因此无法使用网络部署方法升级 AnyConnect 客户端。作为最安全的选项，思科建议用户通过连接到前端并升级来从应用内部升级客户端。

注释 如果之前使用了管理员帐户在客户端上安装 ActiveX 控件，则用户可以升级 ActiveX 控件。

没有主动密钥缓存 (PKC) 或 CCKM 支持

网络访问管理器不支持 PKC 或 CCKM 缓存。在 Windows 7 上，无法使用非思科无线网卡进行快速漫游。

AnyConnect 安全移动客户端的应用编程接口

AnyConnect 安全移动客户端包括应用编程接口 (API)，可供想要编写自己的客户端程序的用户使用。

API 软件包包含文档、源文件和库文件，可支持思科 AnyConnect VPN 客户端的 C++ 接口。可以使用库和示例程序在 Windows、Linux 和 MAC 平台上构建。Windows 平台的生成文件（或项目文件）也包括在内。对于其他平台，它包括展示如何编译示例代码的平台特定脚本。网络管理员可以将应用（GUI、CLI 或嵌入式应用）链接到此类文件和库。

您可以从 Cisco.com 下载 API。

有关 AnyConnect API 的支持问题，请发送邮件到以下地址：anyconnect-api-support@cisco.com。

AnyConnect 4.9.02028

警告用于描述思科软件版本中的意外行为或缺陷。

思科漏洞搜索工具包含此版本中有关未解决和已解决的警告的详细信息。需要使用思科帐户才能访问该漏洞搜索工具。如果没有，请在 https://tools.cisco.com/RPF/register/register.do 中注册。

已解决

标识符	组件	标题
CSCvu57985	核心层	ENH：支持 AnyConnect 上的 NetworkExtension

AnyConnect 4.9.01095

思科漏洞搜索工具包含此版本中有关未解决和已解决的警告的详细信息。需要使用思科帐户才能访问该漏洞搜索工具。如果没有，请在 https://tools.cisco.com/RPF/register/register.do 中注册。

已解决

标识符	组件	标题
CSCvp53403	核心层	在通过 SBL 连接后，GUI 中显示非预期（错误）的 <主机名>
CSCvt08780	核心层	Linux 上的 VM 实例/Docker 容器无法路由网络流量
CSCvu03376	核心层	使用“自动检测代理”（组代理上设置的专用代理）导致间歇性浏览故障
CSCvu19710	核心层	使用 WiFi 呼叫（FaceTime 呼叫）时无法修改 IP 转发表错误

标识符	组件	标题
CSCvu82615	核心层	VPN 客户端代理的 DNS 组件遇到意外错误（动态拆分隧道）
CSCvv15092	核心层	macOS 上的 AnyConnect 4.9.00086 上报告内存利用率过高
CSCvu65566	dart	即使非克隆操作系统，Linux DART 也会生成相同的 UDID
CSCvu22557	download_install	从 4.8.3052 升级到 4.9.64 AnyConnect 后无法通过 IPsec 建立 VPN 连接
CSCvu03997	gui	macOS 嵌入式 SAML 浏览器不下载 .dmg 文件
CSCvs78379	nam	登录使用 SBL GUI 创建的 WiFi 网络时，不会保持连接状态
CSCvs86736	nam	NAM 应允许使用大于 1024 字节的 PAC 文件
CSCvt06237	nam	添加供用户创建的网络在计算机时间内连接的选项，以便支持 VPN 管理隧道
CSCvt74330	nam	当管理员配置的隐藏网络不可用时，NAM 客户端无法切换到用户定义的网络
CSCvu24358	nam	在使用 NAM 的 PC 上关闭 RDP 会话后无法在本地登录
CSCvu26262	nam	NAM 凭据提供程序不加载 Imprivata OneSign Agent 凭据提供程序 DLL
CSCvq97328	opswat-ise	ENH：合规性模块支持 macOS 版 Kaspersky Internet Security 20.x
CSCvu83305	opswat-ise	Cortex 7.x 的 AnyConnect AM 条件
CSCvc89249	posture-ise	支持 TrendMicro WorryFree 6.x 以用于终端安全评估

标识符	组件	标题
CSCvm56656	posture-ise	AC 合规性模块 4.3.x 支持 ESET Endpoint Security 7.x
CSCvo46838	posture-ise	Kaspersky Endpoint Security 11.x 在终端安全评估修复时不存在于磁盘加密中
CSCvp27316	posture-ise	ENH：合规性模块支持 Trend Micro Apex One 14.x
CSCvq20688	posture-ise	对 macOS 的终端安全评估 KES11 支持
CSCvu06725	swg	SWG 客户端崩溃/冻结
CSCvu63661	umbrella	在发送带有大响应的多个 TCP DNS 请求后，DNS 解析全局挂起
CSCvu68957	umbrella	macOS 上的 Umbrella 同步和状态更改延迟
CSCvu73467	umbrella	在 NIC 上启用动态 IPv6 配置后（使用 IPv6 DNS 服务器），Umbrella DNS 保护被禁用
CSCvf65224	vpn	ENH：允许 AnyConnect 在 Linux 计算机上的 /etc/ssl/certs 目录中搜索 CA 证书
CSCvt35162	vpn	由于 Windows 的自动重新启动登录 (ARSO) 功能，导致 AnyConnect SBL 图标缺失
CSCvt49314	vpn	AnyConnect 在活动 DTLS 会话恢复为 TLS 后多次重新连接
CSCvt63861	vpn	采用 Weblaunch 的 Linux 平台 AnyConnect 安装说明显示错误的 OS 映像
CSCvt64638	vpn	仅限 Windows：AnyConnect 不支持接口名称中使用 Unicode 字符

标识符	组件	标题
CSCvt85695	vpn	AnyConnect 在初始 IKE_SA_INIT 中提供 Diffie-hellman 组 1 或 2
CSCvu95344	vpn	删除智能卡后，AnyConnect 无法断开 VPN
CSCvv19684	vpn	从 4.9 FCS 到 4.9 MR1 的云升级不启动

AnyConnect 4.9.00086

思科漏洞搜索工具包含此版本中有关未解决和已解决的警告的详细信息。需要使用思科帐户才能访问该漏洞搜索工具。如果没有，请在 https://tools.cisco.com/RPF/register/register.do 中注册。

已解决

标识符	组件	标题
CSCvs60391	核心层	OpenSSL 1.0.2q 中的多个漏洞
CSCvs60397	核心层	libxml2 2.9.8 中的多个漏洞
CSCvt31657	核心层	Umbrella/SWG 客户端不遵守 O365 旁路
CSCvt74385	核心层	添加动态拆分排除项时 macOS/pfctl 中的延迟
CSCvt92079	核心层	macOS - 间歇性 OS 内存分配故障导致 IPv6 路由表处于不一致状态
CSCvu46279	核心层	macOS - 由于 vpnagent 被阻止而导致传递网络流量时出现延迟
CSCvu22557	download_install	从 4.8.3052 升级到 4.9.64 AnyConnect 后无法通过 IPsec 建立 VPN 连接
CSCvt82526	gui	适用于 Windows VPN SAML 浏览器的 AnyConnect 有时会生成重复的 JavaScript 键值事件
CSCvu03997	gui	macOS 嵌入式 SAML 浏览器不下载 dmg 文件

标识符	组件	标题
CSCvm85974	nam	在为使用 PSK 的 SSID 输入错误的密码时，AnyConnect NAM 不重新提示输入密码
CSCvt99342	nam	不再支持未经身份验证的 PAC 调配（4.9 和更高版本）
CSCvu13185	nam	NAM PE：添加配置策略选项，允许用户创建的网络在计算机时间内进行连接
CSCvu06461	nvm	当路径和参数较大时会丢弃 CFlows
CSCvt12850	nvm	Android-NVM：当 NVM TND 配置为不可信时不立即发送 Cashed 流
CSCvu01704	nvm	NVM 收集器不预加载 nvzFlowV4 模板
CSCvu21676	nvm	Linux：提取进程参数时 NVMAgent 崩溃
CSCvr21787	opswat-ise	ENH：支持 Trend Micro OfficeScan Client 版本 14.x
CSCvc89249	posture-ise	支持 TrendMicro WorryFree 6.x 以用于终端安全评估
CSCvm56656	posture-ise	AnyConnect 合规性模块 4.3.x 支持 ESET Endpoint Security 7.x
CSCvo46838	posture-ise	Kaspersky Endpoint Security 11.x 在终端安全评估修复时不存在于磁盘加密中
CSCvp27316	posture-ise	ENH：合规性模块支持 Trend Micro Apex One 14.x
CSCvq20688	posture-ise	对 macOS 的终端安全评估 KES11 支持
CSCvt72492	umbrella	在 Windows 上不会始终应用 Umbrella 云更新参数更改
CSCvf32537	vpn	ENH：AnyConnect 的 VPN 高带宽/吞吐量性能改进

标识符	组件	标题
CSCvq74726	vpn	ENH：AnyConnect 动态拆分隧道应支持具有低 TTL 的情况
CSCvs78426	vpn	通过 VPN 隧道错误地发送 DHCP 流量
CSCvt49314	vpn	AnyConnect 在活动 DTLS 会话恢复为 TLS 后多次重新连接
CSCvt75904	vpn	macOS：Umbrella 在 macOS 上停滞在保留状态
CSCvt81585	vpn	AnyConnect VPN 无法连接并显示错误 HTTP/1.1 401 未经授权 X-原因：其他错误
CSCvt85695	vpn	AnyConnect 不应在初始 IKE_SA_INIT 中提供 Diffie-hellman 组 1 或 2
CSCvt88461	vpn	升级后 AnyConnect VPN 无法连接并显示 HTTP/1.1 401 未经授权 X-原因：其他错误
CSCvt90659	vpn	AC 4.8.3036 macOS：短名称 DNS 查询不起作用 - macOS 解析器不附加默认域
CSCvt95013	vpn	AnyConnect VPN 负载均衡 IKEv2 在 AC 4.8 上失败
CSCvu03917	vpn	启用自动证书选择的情况下 AnyConnect 连接失败
CSCvu10868	vpn	如果静态拆分排除是动态排除的超网，则动态拆分排除会中断连接
CSCvt65103	vpn-wer	ENH：AnyConnect 支持非 RDP 远程桌面类型

开放

要查找有关此版本中解决缺陷的最新信息，请参阅思科漏洞搜索工具：

标识符	组件	标题
CSCvo32995	nam	ENH：为单独配置的无线网络添加“自动连接”功能支持
CSCvu51439	nvm	每次在 ASDM 上编辑 NVM 配置文件时，都会复制 TND 配置并推送到端点

HostScan 4.9.01095

警告用于描述思科软件版本中的意外行为或缺陷。

思科漏洞搜索工具包含此版本中有关未解决和已解决的警告的详细信息。需要使用思科帐户才能访问该漏洞搜索工具。如果没有，请在 https://tools.cisco.com/RPF/register/register.do 中注册。

已解决

标识符	组件	标题
CSCvr90986	opswat-asa	ENH：HostScan 支持 Win 10 端点的 Microsoft Defender 高级威胁防护 (ATP)
CSCvu14696	opswat-asa	HostScan Ciscod 守护程序创建多个 codesign/pkgutil 进程
CSCvu20458	opswat-asa	HostScan 错误地报告高于 4.18.1902.5 的 Windows Defender 版本
CSCvt12241	posture-asa	AnyConnect 4.9.x HostScan 在 Linux 上的终端安全评估启动阶段停滞

HostScan 4.9.00086

警告用于描述思科软件版本中的意外行为或缺陷。

思科漏洞搜索工具包含此版本中有关未解决和已解决的警告的详细信息。需要使用思科帐户才能访问该漏洞搜索工具。如果没有，请在 https://tools.cisco.com/RPF/register/register.do 中注册。

已解决

标识符	组件	标题
CSCvt12241	posture-asa	AC 98.136.00022 (4.9) HostScan 在 Linux 上的终端安全评估启动阶段停滞