Cisco AnyConnect 安全移动客户端版本说明，版本 4.2

首次发布日期: 2015 年 05 月 05 日

上次修改日期: 2015 年 12 月 23 日

AnyConnect 安全移动客户端版本说明，版本 4.2

这些版本说明提供 Windows、Mac OS X 和 Linux 平台上 AnyConnect 安全移动的相关信息。

注释 AnyConnect 版本 4.2 x 将成为所有 4.x 漏洞的维护路径。AnyConnect 4.0 和 4.1 客户必须升级到 AnyConnect 4.2.x，才能受益于以后的缺陷修复。AnyConnect 4.0.x 和 4.1.x 中发现的所有缺陷将仅在 AnyConnect 4.2.x 维护版本中进行修复。但是，我们已经计划在此 4.2 版本之后不久便会发布一款最终的 4.1 维护版本。

请参阅以下版本说明，获取此版本 AnyConnect 所支持的移动设备相关信息。

- Cisco AnyConnect 安全移动客户端用户指南，版本 4.0 (Android)

下载最新版本的 AnyConnect

开始之前

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

SUMMARY STEPS

1. 点击此链接转至 Cisco AnyConnect 安全移动客户端产品支持页面：
2. 登录到 Cisco.com。
3. 点击**下载软件 (Download Software)**。
4. 如果尚未选择，请展开**最新版本 (Latest Releases)** 文件夹并点击最新版本。
5. 使用以下方法之一下载 AnyConnect 软件包。
   - 要下载单个软件包，请找到要下载的软件包并点击**下载 (Download)**。
   - 要下载多个软件包，请点击软件包行中的**添加至购物车 (Add to cart)**，然后点击在“下载软件”(Download Software) 页面顶部的**下载购物车 (Download Cart)**。
6. 系统提示时，请阅读并接受思科许可协议。
7. 选择一个本地目录保存下载项目并点击**保存 (Save)**。
8. 请参阅《Cisco AnyConnect 安全移动客户端管理员指南，版本 4.x》。

DETAILED STEPS

步骤 1 点击此链接转至 Cisco AnyConnect 安全移动客户端产品支持页面：http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html。

步骤 2 登录到 Cisco.com。

步骤 3 点击**下载软件 (Download Software)**。

步骤 4 如果尚未选择，请展开**最新版本 (Latest Releases)** 文件夹并点击最新版本。

步骤 5 使用以下方法之一下载 AnyConnect 软件包。

- 要下载单个软件包，请找到要下载的软件包并点击**下载 (Download)**。
- 要下载多个软件包，请点击软件包行中的**添加至购物车 (Add to cart)**，然后点击在“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，请阅读并接受思科许可协议。

步骤 7 选择一个本地目录保存下载项目并点击**保存 (Save)**。

步骤 8 请参阅《Cisco AnyConnect 安全移动客户端管理员指南，版本 4.x》。

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	anyconnect-win-*x.x.x*-k9.pkg
Mac OS X	anyconnect-macosx-i386-x.x.x-k9.pkg
Linux（64 位）	anyconnect-linux-64-*x.x.x*-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	anyconnect-win-<version>-pre-deploy-k9.iso
Mac OS X	anyconnect-macosx-i386-<version>-k9.dmg
Linux（64 位）	anyconnect-predeploy-linux-64-<*version*>-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 4.2.04018 中新增的功能

AnyConnect 4.2.04018 是维护版本，包括增强功能，可以解决AnyConnect 4.2.04018 ， 第 25 页中所述的缺陷。

AnyConnect 4.2.03013 中新增的功能

AnyConnect 4.2.03013 是维护版本，包括增强功能，可以解决AnyConnect 4.2.03013 ， 第 26 页中所述的缺陷。

AnyConnect 4.2.02075 中新增的功能

AnyConnect 4.2.02075 是维护版本，包括增强功能，可以解决AnyConnect 4.2.02075 ， 第 27 页中所述的缺陷。

AnyConnect 4.2.01035 中新增的功能

AnyConnect 4.2.01035 是维护版本，包括以下功能和增强功能，可以解决其中所述的缺陷 AnyConnect 4.2.01035 ， 第 29 页

AnyConnect 4.2.01022 中新增的功能

AnyConnect 4.2.01022 是维护版本，包括以下功能和增强功能，可以解决AnyConnect 4.2.01022 ， 第 31 页中所述的缺陷。

为应对非托管设备上日益增多的用户操作需求，您可以通过添加网络可视性模块 (NVM) 加强对 AnyConnect 的保护。它提供关于用户、应用、设备、位置和目标的流量和情景数据。借助 NVM，您可以选择是否将遥测设置为目标，这与总体基础设施部署完全不同。

AnyConnect 4.2.00096 中新增的功能

AnyConnect 4.2.00096 是主要版本，包括以下功能和增强功能，可以解决AnyConnect 4.2.00096 ， 第 31 页中所述的缺陷。

- 可靠访问强制网络门户中的企业资源，并且能够按需禁用这些资源
- 如果配置文件现在无效，最后一个连接条目在用户首选项中不再显示
- 能够基于参数过滤计算机证书并指定适当的计算机证书以便进行身份验证
- ISE 终端安全评估日志记录和补救改进
- Linux 桌面支持 IPv6 VPN 网络连接
- 提高值得信赖的网络检测 (TND) 的安全性和灵活性
- 预留差分服务代码点 (DSCP)，控制 Windows 或 OS X 平台上的 DSCP 仅用于 DTLS 连接。

重要互操作性注意事项

ISE 和 ASA 前端共存

- 如果您将 ISE 和 ASA 同时用于客户端终端安全评估，则在两个前端上配置文件必须匹配。
- 如果 NAC 代理用作终端，那么 AnyConnect 会忽略 ISE 1.3 服务器。
- 如果思科 NAC 代理和 AnyConnect ASA 终端安全评估模块均安装在客户端上，那么思科 NAC 代理必须至少是 4.9.4.3 版本或更高版本，才能防止终端安全评估冲突。
- 如果 AnyConnect 用作 ISE 中的终端，那么 NAC 代理忽略 ISE 1.3 服务器。

系统要求

本节确定对此版本的管理及终端要求。有关终端操作系统支持和每个功能的许可证要求，请参阅《AnyConnect 安全移动客户端功能、许可证和操作系统，版本 4.2》。

在所有支持的终端上安装的 AnyConnect 4.x 可与包括 IPSec 客户端在内的其他 VPN 客户端共存；但是，我们不支持运行 AnyConnect 的同时运行其他 VPN 客户端。

对 AnyConnect 配置文件编辑器的更改

安装配置文件编辑器前，必须先安装版本 6 或更高版本的 32 位 Java 版本。

AnyConnect 的 ISE 要求

ISE 版本要求

- ISE 1.3 为最低版本，能够将 AnyConnect 软件部署至终端并使用 AnyConnect 4.0 和更高版本的新的 ISE 终端安全评估模块对该终端进行终端安全评估。
- ISE 1.3 只能部署 AnyConnect 4.0 和更高版本。旧版本的 AnyConnect 必须从 ASA 进行网络部署、用 SMS 预部署或手动部署。

ISE 许可要求

要从 ISE 前端部署 AnyConnect 并使用 ISE 终端安全评估模块，在 ISE 管理节点上需要提供思科 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，版本 *2.0*》中的“思科 ISE 许可证”一章。

AnyConnect 的 ASA 要求

ASA 版本要求

- 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，您必须升级到 ASA 9.2 (1)：

  通过 VPN 进行的 ISE 终端安全评估

  AnyConnect 4.x 的 ISE 部署

  从版本开始支持更改 ASA 上的授权 (CoA)

- 如果要使用以下功能，您必须升级到 ASA 9.0：

  IPv6 支持

  思科下一代加密“Suite B”安全

  AnyConnect 客户端延迟升级

- 如果要执行以下功能，您必须使用 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、网络安全或遥测）。

  使用 Cisco IronPort 网络安全设备所支持的服务。这些服务可以执行可接受的使用策略，通过批准或拒绝所有 HTTP 和 HTTPS 请求来保护终端免遭不安全的网站影响。

  部署防火墙规则。如果部署永远在线VPN，您可能要启用拆分隧道并配置防火墙规则以限制对本地打印和关联移动设备的网络访问。

  将动态访问策略或组策略配置为免除对符合条件的 VPN 用户进行永远在线 VPN 的部署。

  当 AnyConnect 会话处于隔离状态时，配置动态访问策略可在 AnyConnect GUI 上显示消息。

ASA 内存要求

注意 对于使用 AnyConnect 4.0 或更高版本的所有 ASA 5500 型号而言，建议采用的最小闪存为 512 MB。这样可以允许在 ASA.上托管多个终端操作系统，记录并调试以启用这些操作系统。

因为 ASA 5505 的闪存大小有限（最大为 128 MB），并非所有排列的 AnyConnect 软件包都可以加载到此模型。要成功加载 AnyConnect，您需要降低软件包大小（例如操作系统较少、无 Host Scan 等），直到软件包与可用闪存相匹配。

在进行 AnyConnect 安装或升级前，请检查可用空间。您可以使用以下方法之一执行此操作：

- 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 - 依次选择“工具”(Tools) >“文件管理”(File Management)。“文件管理”(File Management) 窗口将显示闪存空间。

如果 ASA 只有默认内部闪存大小或默认 DRAM 大小（适用于缓存内存），您在 ASA 上存储和加载多个 AnyConnect 客户端软件包时可能会遇到问题。即使您的闪存有足够空间承载软件包，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 内存要求和升级 ASA 内存的更多信息，请参阅思科 ASA 5500 系列的最新版本说明。

ASA 终端安全评估和 HostScan 的互操作性

AnyConnect 终端安全评估模块使 Cisco AnyConnect 安全移动客户端能够识别安装于 ASA 主机上的操作系统、杀毒软件、反间谍软件和防火墙软件。

ASA 终端安全评估模块需要 Cisco HostScan 来收集此信息。Cisco HostScan 作为其自带的软件包，可使用新的操作系统、杀毒软件、反间谍软件和防火墙软件信息定期更新。思科建议您始终升级到与 AnyConnect 兼容的最新 HostScan 可用版本。

AnyConnect 4.1.00028 与 Cisco HostScan 4.1.00028 (OPSWAT 3.6.10013.2) 或更高版本兼容。如果不能同时升级 AnyConnect 和 Host Scan，请先升级 Host Scan，再升级 AnyConnect。

AnyConnect 4.0.02052 与 Cisco HostScan 4.0.02052 (OPSWAT 3.6.10013.2) 或更高版本兼容。如果不能同时升级 AnyConnect 和 Host Scan，请先升级 Host Scan，再升级 AnyConnect。

防病毒、反间谍软件和防火墙应用列表可从 cisco.com 获得。支持图表使用 Firefox 浏览器最易打开。如果使用的是 Internet Explorer，请将文件下载到计算机并将文件扩展名从 `.zip` 更改为 `.xlsm`。您可以在 Microsoft Excel、Microsoft Excel Viewer 或 OpenOffice 中查看文件。

注释 如果采用不兼容的 HostScan 版本，则 AnyConnect 无法建立 VPN 连接。确保您运行的 HostScan 版本与 AnyConnect 运行的版本相同。此外，思科不建议组合使用 HostScan 和 ISE 终端安全评估模块。当两种不同的终端安全评估代理同时运行时，则会出现意外结果。

思科 Host Scan 软件包可预部署或安装在 ASA 8.4 版或更高版本上以便进行网络部署。

ISE 终端安全评估合规性模块

ISE 终端安全评估合规性模块包含用于 ISE 终端安全评估的受支持的杀毒软件、反间谍软件及防火墙列表。当 HostScan 列表按供应商组织的同时，ISE 终端安全评估列表按产品类型组织。当前端（ISE 或 ASA）的版本号高于终端版本时，OPSWAT 就会更新。这些升级是强制性的，且无需最终用户干预便会自动进行。

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。您可以使用 Microsoft Excel、Microsoft Excel Viewer 或以下位置的 OpenOffice 查看图表：http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html.

AnyConnect 的 IOS 支持

思科支持 AnyConnect VPN 访问作为安全网关的 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 VPN
- 连接故障策略
- 提供本地打印机和关联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

关于 IOS 对 AnyConnect VPN 提供支持的其他限制，请参阅思科 IOS SSL VPN 上不受支持的功能。

关于思科 IOS 功能支持的其他信息，请参阅 http://www.cisco.com/go/fn。

AnyConnect 4.0 4.1 4.2 支持的操作系统

Cisco AnyConnect 安全移动客户端版本 4.0 4.1 4.2 支持在其所含模块中使用以下操作系统：

支持的操作系统	VPN 客户端	网络访问管理器	云网络安全	ASA 终端安全评估	ISE 终端安全评估	DART	客户体验反馈
Windows 7、8、8.1 和 10 x 86 (32 位) 和 x 64 (64 位)	是	是	是	是	是	是	是
Mac OS X 10.8、10.9、10.10 或 10.11	是	否	是	是	是	是	是
Linux Red Hat 6、7 和 Ubuntu 12.04 (LTS)、14.04 (LTS) （仅 64 位）	是	否	否	是	否	是	是

AnyConnect 对 Microsoft Windows 的支持

Windows 要求

- 奔腾级处理器或更高版本。
- 100 MB 硬盘空间

- Microsoft 安装程序版本 3.1
- 从所有之前的 Windows 版本升级到 Windows 8.1，需要您在 Windows 升级完成后，先卸载 AnyConnect，然后再重新安装 AnyConnect。
- 从 Windows XP 升级到任何 Windows 更高版本都需要全新安装，因为在升级期间 Cisco AnyConnect 虚拟适配器未保留。手动卸载 AnyConnect，升级 Windows，然后手动或通过 WebLaunch 重新安装 AnyConnect。
- 要通过 WebLaunch 启动 AnyConnect，您必须使用 Firefox 3.0+ 的 32 位版本并启用 ActiveX 或安装 Sun JRE 1.4+。
- 当使用 Windows 8 或 8.1 时，需要 ASDM 版本 7.02 或更高版本。

Windows 限制

- Windows RT 不支持 AnyConnect。在操作系统中没有提供 API 来实现此功能。思科与微软就本主题已达成开放请求。需要此功能的用户应与微软联系，表达其兴趣。
- 如果其他第三方产品与 Windows 8 不兼容性，会阻止 AnyConnect 通过无线网络建立 VPN 连接。以下为该问题的两个示例：

  WinPcap 服务“远程数据包捕获协议 v.0（实验）”通过 Wireshark 进行分配但不支持 Windows 8。

  要解决此问题，请卸载 Wireshark 或禁用 WinPcap 服务，重新引导 Windows 8 计算机，然后尝试再次连接 AnyConnect。

  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。

  要解决此问题，请确保 Windows 8 计算机上已安装支持 Windows 8 的最新无线网卡或驱动程序。

- AnyConnect 不集成新的 UI 框架（称为城域设计语言），该语言部署在 Windows 8 上；但是，AnyConnect 确实能够以桌面模式在 Windows 8 上运行。
- 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，我们不会阻止在该操作系统中安装 AnyConnect。此外，Windows Server 2008 R2 需要可选的 SysWow64 组件
- 如果您在支持备用设备的系统中使用网络访问管理器，思科建议您使用默认的 Windows 8.x 关联计时器值（5 秒）。如果您发现 Windows 中的扫描列表小于预期，请增大关联计时器值，以便驱动程序可以完成网络扫描和填写扫描列表。

Windows 指南

- 验证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存在间歇性连接问题。
- 对于网络访问管理器，使用计算机密码进行计算机身份验证的功能在 Windows 8 或 10/Server 2012 上将不起作用，除非向客户端桌面应用注册表修复，此操作在 MicrosoftKB 2743127 (http:/

/support.microsoft.com/kb/2743127) 中进行描述。此修复包括将 DWORD 值 LsaAllowReturningUnencryptedSecrets 添加到 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa 注册表项并将该值设置为 1。此更改允许本地安全机构 (LSA) 向客户端（诸如思科网络访问管理器）提供计算机密码。此更改与 Windows 8 或 10/Server 2012 中增加的默认安全设置相关。使用计算机证书进行计算机身份验证不需要进行此更改，其工作方式将与使用预 Windows 8 操作系统的工作方式相同。

注释 计算机身份验证允许在用户登录之前，客户端桌面向网络进行身份验证。在此期间，管理员可以对此客户端计算机执行已计划的管理任务。实现 EAP 链接功能也需要进行计算机身份验证，RADIUS 服务器可以通过此功能对特定的客户端的用户和计算机均进行验证。结果就是确定公司资产和运用适当的访问策略。例如，如果这是个人资产（PC/笔记本电脑/平板电脑），并且使用公司凭证，终端将无法进行计算机身份验证，但是却在用户的网络连接中成功应用用户身份验证和适当的网络访问限制。

- 在 Windows 8 中，可以使用“首选项”(Preferences) > VPN >“统计信息”(Statistics) 选项卡中的“导出统计信息”(Export Stats) 按钮在桌面上保存文件。在 Windows 的其他版本中，会询问用户保存文件的位置。
- AnyConnect VPN 与 3 G 数据卡兼容，可以通过 WWAN 适配器接入 Windows 7 或更高版本的 Windows。

AnyConnect 对 Linux 的支持

Linux 要求

- 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。
- libstdc++ 用户必须具有 libstdc++ so.6 (GLIBCXX_3.4) 或更高版本，但需要低于版本 4。
- Android 5 (1.5) 或更高版本。网络安装适用的版本仅限于 Sun Java。您必须安装 Sun Java 并对浏览器进行配置才能使用该版本，而非使用其默认软件包。
- zlib - 支持 SSL deflate 压缩
- xterm - 如果您正从 ASA 无客户端门户上通过 Weblaunch 执行 AnyConnect 初始部署，才会需要该程序。
- gtk 2.0.0。
- gdk 2.0.0。

- libpango 1.0。
- iptables 1.2.7a 或更高版本。
- TUN 模块附带内核 2.4.21 或 2.6。

AnyConnect 对 Mac OS X 的支持

Mac OS X 要求

- AnyConnect 需要 50 MB 硬盘空间。
- 要正确操作 Mac OS X，AnyConnect 需要的最小显示分辨率为 1024 X 640 像素。

Mac OS X 指南

- Mac OS X 10.8 推出了一项称为 Gatekeeper 的新功能，该功能可限制允许在系统上运行的应用。您可选择允许从以下位置下载的应用：
  - Mac App Store
  - Mac App Store 和已确定的开发商
  - 任何地点

  默认设置为 Mac App Store 和已确定的开发商（已签名的应用）。AnyConnect 是已签名的应用，但并非以 Apple 证书签署。这意味着您必须选择“任何地点”(Anywhere) 设置或使用 Ctrl 键绕过选定的设置，以从预部署安装实现 AnyConnect 的安装和运行。进行网络部署或已安装 AnyConnect 的用户不受影响。有关详细信息，请参阅：http://www.apple.com/macosx/mountain-lion/security.html。

注释 可以根据需求进行 Web 启动或操作系统升级（例如从 10.7 升级到 10.8）安装。由于存在网守，仅预部署安装需要额外的配置。

AnyConnect 许可

有关最新版最终用户许可协议，请参阅《思科最终用户许可协议，AnyConnect 安全移动客户端，版本 4.x》。

有关开源许可确认，请参阅《AnyConnect 安全移动客户端上所用的开源软件，版本 4.2》。

要从 ISE 前端部署 AnyConnect 并使用 ISE 终端安全评估模块，在 ISE 管理节点上需要提供思科 ISE APEX 许可证。有关 ISE 许可证详细信息，请参阅《思科身份服务引擎管理员指南，版本 *2.0*》中的“思科 ISE 许可证”一章。

要从 ASA 前端部署 AnyConnect 并使用 VPN 和 ASA 终端安全评估模块，则需要提供 AnyConnect 4.X Plus 或 Apex 许可证，并且可以提供试用许可证。相关信息，请参阅《Cisco AnyConnect 订购指南》。

AnyConnect 4.X Plus 和 Apex 许可证概述以及功能使用哪个许可证的描述，请参阅《AnyConnect 安全移动客户端功能、许可证和操作系统，版本 4.2》。

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。Cisco AnyConnect 安全移动客户端可通过以下方法部署到远程用户：

- 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。

部署 AnyConnect 时，您可以包括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。请注意以下事项：

- 所有 AnyConnect 模块和配置文件都可进行预部署。预部署时，您必须特别注意模块安装顺序和其他细节。
- ASA 终端安全评估模块所用的客户体验反馈模块和 HostScan 软件包无法从 ISE 进行网络部署。
- 由 ISE 终端安全评估模块使用的合规性模块无法从 ASA 进行网络部署。

有关部署 AnyConnect 模块的详细信息，请参阅《Cisco AnyConnect 安全移动客户端管理员指南，版本 4.2》。

注释 无论何时您升级到新的 AnyConnect 软件包，都请确保从 CCO 将本地化 MST 文件更新至最新版本。

从 3.1 MR10 AnyConnect 客户端升级/不兼容问题

一旦 AnyConnect 3.1.10010 已自动部署到终端，您便无法连接到配置了 AnyConnect 版本 4.0、4.1、4.1 MR2 和 4.2（这些都不兼容）的安全网关。如果您尝试从 AnyConnect 3.1 MR10 版本升级到除 AnyConnect 4.1MR4（或更高版本）或高于 3.1.10010 的 3.1 版本外的任何版本，您将会收到不允许升级的通知。

有关详细信息，请参考 CSCuv12386。

从 AnyConnect 3.0 或更高版本升级

当您从 AnyConnect 安全移动客户端版本 3.0 或更高版本进行升级时，AnyConnect 将执行以下操作：

- 升级核心客户端的所有以前版本并保留所有 VPN 配置。
- 升级 AnyConnect 使用的所有 Host Scan 文件。

从 AnyConnect 2.5 及之前版本升级

当您从任意 AnyConnect 2.5.x 版本进行升级时，AnyConnect 安全移动客户端将会执行以下操作：

- 升级核心客户端的所有以前版本并保留所有 VPN 配置。
- 升级 AnyConnect 使用的所有 Host Scan 文件。
- 如果您安装网络访问管理器，AnyConnect 将保留所有 CSSC 5.x 配置，以便与网络访问管理器配合使用，然后删除 CSSC 5.x。
- 不升级或删除 Cisco IPsec VPN 客户端。但是，AnyConnect 客户端可与 IPsec VPN 客户端在计算机上共存。
- 不升级且不能与思科的 ScanSafe AnyWhere+ 共存。安装 AnyConnect 安全移动客户端之前必须先卸载 AnyWhere+。

注释 如果您从传统思科 VPN 客户端进行升级，物理适配器的 MTU 值则可能会降低到 1300。应将每台适配器的 MTU 恢复回默认值（通常为 1500），以便在使用 AnyConnect 时获得最佳性能。

不支持使用 ASA 或 Weblaunch 从 AnyConnect 2.2 进行升级。必须先卸载 AnyConnect 2.2，然后使用 SMS 或手动安装新版本。

基于 Web 的安装在 64 位 Windows 上可能会失败

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

当 Windows 注册表项 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth 设置为 0 时，Active X 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。

解决方案是：

- 运行 32 位版本的 Internet Explorer。
- 将注册表项编辑为非零值或从注册表中删除该值。

注释 在 Windows 8 中，从 Windows 启动屏幕启动 Internet Explorer 运行该 64 位版本。从桌面启动运行该 32 位版本。

AnyConnect 支持策略

思科支持 Cisco AnyConnect VPN 软件下载站点中可用的所有非试用版 AnyConnect 软件版本；但是，基于最新发布的版本，我们仅在维护或功能发布时提供修复和增强功能。

关于“版本不再支持”的详细信息，请参阅 http://www.cisco.com/c/en/us/products/eos-eol-policy.html

指南和限制

Microsoft 不再支持 SHA-1

拥有 SHA-1 证书或 SHA-1 中间证书的安全网关直到 2017 年 1 月才被 Windows 终端视作有效。2017 年 1 月之后，Windows 终端便不再将拥有 SHA-1 证书的安全网关视作值得信赖。确保您的安全网关没有 SHA-1 身份证书，并且其任何中间证书均不是 SHA-1。

“代码签名证书：Windows 将不再受信任由 SHA-1 代码签名证书签名且时间戳在 2016 年 1 月 1 日以后的带有网络属性标记的文件。”请查看 Microsoft 文档，获得详细信息：此处

2016 年 1 月 1 日之前签名的文件有效期到 2017 年 1 月 1 日。

注释 由于代码签名的更改，当前 AnyConnect 用户**必须**升级到 3.1.13011，或未来的 4.2 MR 版本或 AnyConnect 4.3+ 版本，才能确保其 AnyConnect 在 2017 年 1 月 1 日之后可运行于 Windows 平台上。

不再支持 RC4 TLS 密码套件

由于已增强安全策略，AnyConnect 版本 4.2.01035 及以前版本不支持 RC4 TLS 密码套件。

OpenSSL 密码套件更改

由于 OpenSSL 标准开发团队已将一些密码套件标记为折中处理，我们在 AnyConnect 3.1.05187 以外不再对这些套件提供支持。不受支持的密码套件包括如下：DES-CBC-SHA、RC4-SHA 和 RC4-MD5。

同样，我们的加密工具包不再继续支持 RC4 密码；因此，我们将在 3.1.13011 和 4.2.01035 及更高版本中停止对上述密码的支持。

AnyConnect 支持 Mac OS X El Capitan 10.11

Cisco AnyConnect 安全移动客户端支持 Mac OS X El Capitan 10.11 操作系统。

在 ISE 终端安全评估中使用日志跟踪

在全新安装后，期望您会看到 ISE 终端安全评估日志跟踪消息。但是，如果您进入 ISE 终端安全评估配置文件编辑器，并将“启用代理日志跟踪文件”(Enable Agent Log Trace file) 更改为 0（禁用），则必须重启一次 AnyConnect 服务以便获得预期结果。

在 Mac 上与 ISE 终端安全评估的互操作性

如果您使用 Mac OS X 10.9 或更高版本并想要使用 ISE 终端安全评估，那么您可能需要执行以下操作以避免出现问题：

- 在终端安全评估期间，关闭证书验证可避免出现“无法与策略服务器联系”(failed to contact policy server" error) 的错误。
- 禁用强制网络门户应用；否则，发现探针被阻止，该应用仍旧保持在终端安全评估前的 ACL 状态。

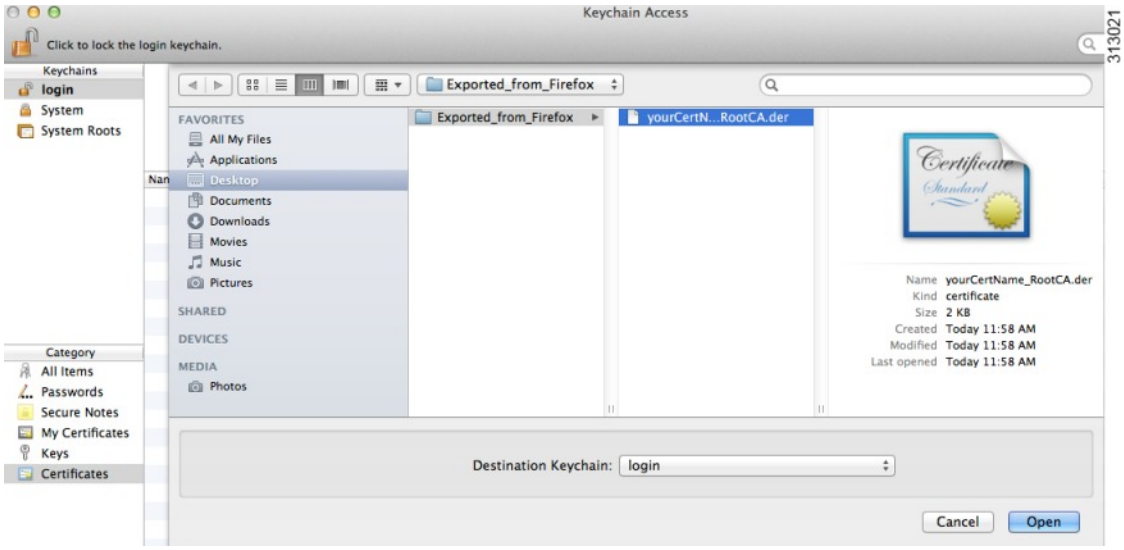
Mac OS X 上的 Firefox 证书存储区不受支持

Mac OS X 上的 Firefox 证书存储区存储权限如下：允许所有用户修改存储区内容，允许未授权用户或进程将非法 CA 添加至值得信赖的根存储区。Anyconnect 不再将 Firefox 存储区用于服务器验证或客户端证书。

如果需要，可指导用户如何从 Firefox 证书库导出 AnyConnect 证书，以及如何将这些证书导入 Mac OS X 密钥链。以下步骤是可以向 AnyConnect 用户进行讲解的示例。

1. 导航至 **Firefox > 首选项 (Preferences) > 高级 (Advanced)**，“证书”(Certificates) 选项卡，点击**查看证书 (View Certificates)**。
2. 选择用于 AnyConnect 的证书，然后点击**导出 (Export)**。

   AnyConnect 证书将最有可能位于“权限”(Authorities) 类别下。请与您的证书管理员确认，因为他们可能位于不同的类别下（“您的证书”(Your Certificates) 或“服务器”(Servers)）
3. 选择一个位置保存证书，例如您的桌面文件夹。
4. 在“格式”(Format) 下拉菜单中，选择 **X.509 证书 (DER) (X.509 Certificate [DER])**。如有必要，请向证书名称添加 .der 扩展名。

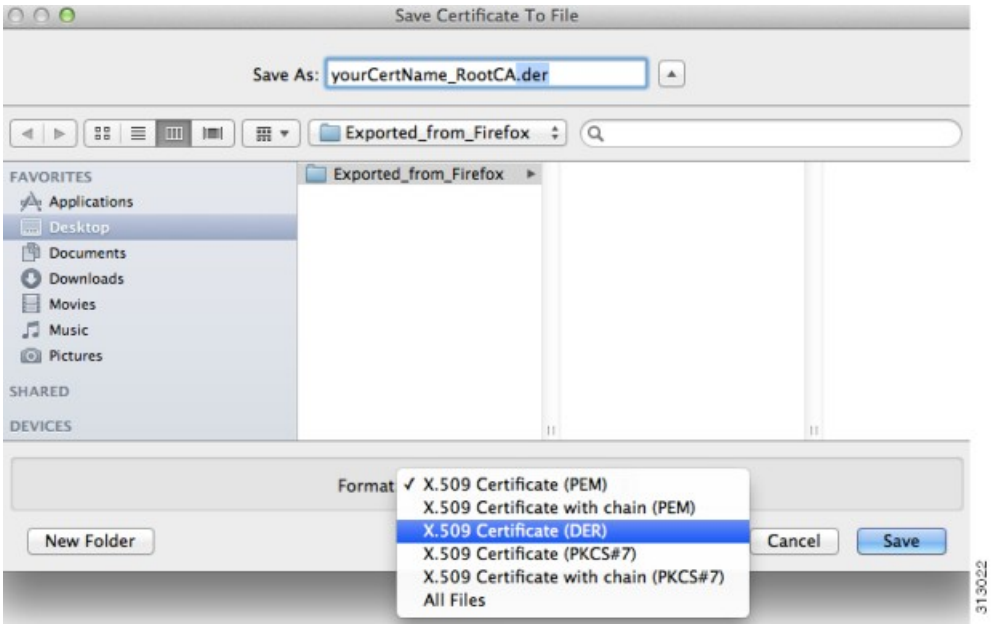


注释 注意：如果使用/需要多个 AnyConnect 证书和/或私钥，请为每个证书重复上述过程。

5 启动密钥链。导航至“文件”(File) - “导入项目”(Import Items)…，并选择您从 Firefox 导出的证书。

在“目标密钥链”(Destination Keychain) 中：选择所需的密钥链。本示例所使用的登录密钥链可能和您公司使用密钥链的不同。请与您的证书管理员确认并验证应导入您证书的密钥链。

6 在“目标密钥链”(Destination Keychain) 中：选择所需的密钥链。本示例所使用的登录密钥链可能和您公司使用密钥链的不同。请与您的证书管理员确认并验证应导入您证书的密钥链。



7 对于用于 AnyConnect 或其所需的其他证书，请重复之前的步骤。

由于缺少依赖关系 libpangox，导致 AnyConnect UI 失败

在许多较新的 Linux 发行版本中，AnyConnect UI 可能无法以该错误开头：

```
error while loading shared libraries: libpangox-1.0.so.0: cannot open shared
object file: No such file or directory
```

缺少的库已过时且不再可用。这不仅会影响 AnyConnect，也会影响其他应用。

Pango 已发布兼容库的源代码，该兼容库可由其他人构建并在线提供。要解决此问题，请查找并安装以下软件包之一*pangox-compat-0.0.2-2.el7.x86_64.rpm* 或 `pangox-compat-0.0.2-3.fc20.x86_64.rpm`。

SSLv3 阻止 Host Scan 发挥作用

(CSCue04930) 当在 ASDM（“配置”(Configuration) > “远程访问 VPN”(Remote Access VPN) > “高级”(Advanced) > “SSL 设置”(SSL Settings) > 作为服务器进行协商的安全设备的 SSL 版本）中选择 SSLv3 选项“仅限 SSLv3”(SSLv3 only) 或“协商 SSL V3”(Negotiate SSL V3) 时，Host Scan 不起作用。在 ASDM 中显示警告消息以提醒管理员。

由修改的 sysctl 网络设置导致的问题

我们已看到 Apple 的宽带调谐器应用 (2005) 的实例用于 Mac OS X 10.9 上。该应用在 sysctl.conf 上更改网络设置，便可能导致连接问题。该应用为 Mac OS 的较早版本而设计。我们怀疑当前默认操作系统设置已把宽带网络考虑在内，因此大多数用户无须进行任何操作。

同时运行 AnyConnect 3.1.04074 和已修改的 sysctl 设置，可能生成以下信息：

```
The VPN client driver encountered an error..please restart
```

要验证

要验证 sysctl 网络设置是否是造成该问题的原因，请打开“终端”(Terminal) 窗口并键入：

```
sysctl -a | grep maxsockbuf
```

如果结果包含的数值远低于默认值 8388608，例如：

```
kern.ipc.maxsockbuf: 512000
```

则该值可能在 /etc/sysctl.conf 中已被 Apple 的宽带调谐器应用所覆盖

要修复

编辑 /etc/sysctl.conf，在设置 kern.ipc.maxsockbuf 的行中添加注释，并重新引导计算机。

或者

如果除了通过宽带调谐器应用进行的设置外，您未进行其他自定义设置，请重命名或删除 sysctl.conf。

Apple 已获知此问题，并已开通漏洞 ID：15542576

Safari 上的 Weblaunch 问题

Safari 上的 Weblaunch 存在一个问题。在随附于 OS X 10.9 (Mavericks) 的 Safari 版本中，默认安全设置阻止 AnyConnect Weblaunch 发挥作用。要将 Safari 配置为允许 Weblaunch，请按如下所述编辑 ASA 的 URL，使其处于不安全的模式。

1. 依次打开 **Safari** > **首选项 (Preferences)** > **安全 (Security)** > **管理网站设置 (Manage Website Settings)**。
2. 点击 ASA 并选择在不安全的模式下运行。

Active X 升级可以禁用 Weblaunch

只要无需对 ActiveX 控件进行更改，便可以使用有限用户帐户通过 Weblaunch 对 AnyConnect 软件进行自动升级。

偶尔，由于安全修复或添加新功能，会对控件进行更改。

如果控件调用自有限用户帐户时需要进行升级，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控件。

Java 7 问题

Java 7 可能导致 AnyConnect 安全移动客户端、HostScan、CSD 和无客户端 SSL VPN (WebVPN) 出现问题。问题和解决方法在故障排除技术说明《AnyConnect、CSD/Hostscan 及 WebVPN 的 Java 7 问题故障排除指南》（位于“安全”(Security) > Cisco HostScan 下的思科文档中）中进行介绍。

Internet Explorer、Java 7 和 AnyConnect 3.1.1 互操作性

当用户尝试连接到 ASA 时，当在终端安装 Java 7 时，当在 ASA 上安装和启用 Host Scan 时，以及在 ASA 上安装和启用 AnyConnect 3.1.1 时，Internet Explorer 的受支持版本停止工作。

当已安装 Active X 或之前版本的 Java 7 时，则不会发生此问题。要避免此问题，请在版本低于 Java 7 的终端应用上使用受支持的 Java 版本。

请参阅漏洞修复工具包和缺陷 CSCuc48299 进行验证。

当配置打开所有网络隧道时应用隐式 DHCP 过滤器

要在配置“打开所有网络隧道”(Tunnel All Networks) 时使本地 DHCP 流量畅通无阻，AnyConnect 在 AnyConnect 客户端连接时将特定路由添加到本地 DHCP 服务器。为防止此路由上出现数据泄漏，AnyConnect 在主机的 LAN 适配器上也采用隐式过滤器，屏蔽除 DHCP 流量外该路由的所有流量。

通过关联设备限定 AnyConnect VPN

思科仅允许通过蓝牙或 USB 关联的 Apple iPhone 设备限定 AnyConnect VPN 客户端。在部署 AnyConnect VPN 客户端前，其他关联设备提供的网络连接须通过该客户端验证。

AnyConnect 智能卡支持

AnyConnect 支持在以下环境中提供凭证的智能卡：

- Windows 7 和 Windows 8 中的 Microsoft CAPI 1.0 和 CAPI 2.0。
- Mac OS X 10.4 和更高版本上通过令牌实现的密钥链

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

AnyConnect 虚拟测试环境

思科借助这些虚拟机环境执行一部分 AnyConnect 客户端测试：

- VMware ESXi Hypervisor (vSphere) 4.0.1 及更高版本
- VMWare Fusion 2.x、3.x、和 4.x

我们虽然不支持在虚拟环境中运行 AnyConnect；但是希望 AnyConnect 可以在 VMWare 测试环境中正常运行。

如果您在虚拟环境中遇到与 AnyConnect 相关的任何问题，请进行报告。我们将竭诚为您解决问题。

AnyConnect 密码支持使用 UTF-8 字符

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

由于版本冲突，禁用自动更新可能导致连接受阻

当已经为运行 AnyConnect 的客户端禁用自动更新时，ASA 的版本必须与 AnyConnect 版本或之前已安装的版本相同，否则客户端将无法连接到 VPN。

要避免此问题，请在 ASA 上配置相同版本或之前版本的 AnyConnect 软件包，或启用自动更新以将客户端升级到新版本。

网络访问管理器和其他连接管理器之间的互操作性

当网络访问管理器运行时，会对网络适配器进行排斥控制，并且阻止其他软件尝试连接管理器（包括 Windows 本地连接管理器）尝试建立连接。因此，如果您希望 AnyConnect 用户使用其终端计算机上的其他连接管理器（例如 iPassConnect 移动管理器），则必须通过网络访问管理器 GUI 上的“禁用客户端”(Disable Client) 选项，或者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

版本 12.4.4.5 的 Intel 无线网络接口卡驱动程序与网络访问管理器不兼容。如果此驱动程序和网络访问管理器安装在相同的终端上，则此驱动程序可能导致网络连接不连贯且 Windows 操作系统会突然关闭。

避免 SHA 2 证书验证失败 (CSCtn59317)

AnyConnect 客户端依靠证书的 Windows 加密服务提供商 (CSP) 对 IPsec/IKEv2 VPN 连接的 IKEv2 身份验证阶段所需数据进行哈希和签名。如果 CSP 不支持 SHA 2 算法，并且面向伪随机功能 (PRF) SHA256、SHA384 或 SHA512 配置 ASA，同时面向证书或证书和 AAA 身份验证配置连接配置文件（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。

要避免此问题，您可以将 ASA 上 IKEv2 策略中的 PRF 配置为 md5 或 sha (SHA 1)。或者，可以将证书 CSP 值修改为发挥作用的本地 CSP（例如 Microsoft Enhanced RSA 和 AES 加密提供商。）请勿将此解决方法应用于智能卡证书。您不能更改 CSP 名称。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区中的证书及其当前的 CSP 值：certutil -store -user My

   以下示例显示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. 识别证书中的 <CN> 属性。在示例中，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 或更高版本中，使用以下命令：certutil -csp “Microsoft Enhanced RSA and AES Cryptographic Provider“ -f -repairstore -user My <CN> carol smith

5 重复第 2 步并验证是否为证书显示新的 CSP 值。

为 Host Scan 配置防病毒应用

防病毒应用可以将包含在终端安全评估模块及 Host Scan 软件包内的某些应用的行为误解释为恶意。安装终端安全评估模块或 Host Scan 软件包之前，将您的杀毒软件配置到“白名单”或将以下 HostScan 应用归为安全例外项：

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

IKEv2 不支持 Microsoft Internet Explorer 代理

IKEv2 不支持公共侧 Microsoft Internet Explorer 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。

对于 IKEv2，可能需要在组策略上进行 MTU 调整

AnyConnect 有时从某些路由器接收并丢弃数据包分段，导致某些网络流量未能通过。

要避免此问题，请降低 MTU 值。建议值为 1200。以下示例显示使用 CLI 执行此操作的方法：

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

要使用 ASDM 设置 MTU，请转至“配置”(Configuration)>“网络（客户端）访问”(Network [Client] Access)>“组策略”(Group Policies)>“添加”(Add) 或“编辑”(Edit)>“高级”(Advanced)>“SSL VPN 客户端”(SSL VPN Client)。

使用 DTLS 时 MTU 会自动调整

如果为 DTLS 启用“失效对等项检测”(DPD)，则客户端自动确定路径 MTU。如果您之前已使用 ASA 降低 MTU 值，则应将该设置恢复为默认值 (1406)。建立隧道期间，客户端使用特殊 DPD 数据包自动调整 MTU。如果您仍有问题，请如前所述使用 ASA 上的 MTU 配置对 MTU 进行限制。

网络访问管理器和组策略

Windows Active Directory 无线组策略可以管理在特定 Active Directory 域的 PC 上的无线设置及其部署的所有无线网络。当安装网络访问管理器时，管理员必须意识到某些无线组策略对象 (GPOs) 可能影响网络访问管理器的行为。管理员应该在执行完整的 GPO 部署之前，通过网络访问管理器测试 GPO 策略设置。以下 GPO 条件可能阻碍网络访问管理器按预期运行：

- 当使用 Windows 7 或更高版本时，使用**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。

FreeRADIUS 配置为与网络访问管理器配合使用

要使用网络访问管理器，您可能需要调整 FreeRADIUS 配置。默认情况下，所有 ECDH 相关的密码都被禁用以避免漏洞。在 /etc/raddb/eap.conf 中，更改 cipher_list 值。

实现接入点之间漫游需要完整身份验证

当客户端在同一网络中的接入点之间漫游时，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，而不是利用更快速的 PMKID 实现重新关联。因此，在某些情况下，如果活动配置文件需要，AnyConnect 会提示用户在每次完整身份验证时输入凭证。

IPv6 网络流量下思科云网络安全行为用户指南

除非已指定 IPv6 地址、域名、地址范围或通配符，IPv6 网络流量将被发送至扫描代理，由扫描代理执行 DNS 查找，以查看是否存在与用户尝试连接的 URL 对应的 IPv4 地址。如果扫描代理找到了 IPv4 地址，它会使用该地址进行连接。如果未找到 IPv4 地址，将放弃连接。

如果希望所有 IPv6 流量绕过扫描代理，您可以为所有 IPv6 流量添加此静态例外：/0。执行此操作将使所有 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。

防止 LAN 上的其他设备显示主机名

当某人使用 AnyConnect 与远程 LAN 上的 Windows 7 或更高版本建立 VPN 会话后，用户 LAN 中其他设备上的网络浏览器在受保护的远程网络中显示主机名称。但是，其他设备无法访问这些主机。

要确保 AnyConnect 主机在子网间防止泄露主机名（包括 AnyConnect 终端主机名），请配置该终端，不将其作为主浏览器或备用浏览器。

1. 在“搜索程序和文件”(Search Programs and Files) 文本框中输入 **regedit**。
2. 导航至 **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\Parameters**
3. 双击**维护服务器列表 (MaintainServerList)**。

系统将打开“编辑字符串”(Edit String) 窗口。

1. 输入**否 (No)**。
2. 点击**确定 (OK)**。

3 关闭“注册表编辑器”(Registry Editor) 窗口。

吊销消息

如果 AnyConnect 尝试验证指定 LDAP 证书吊销列表 (CRL) 的分发点的服务器证书，且分发点仅供内部访问，那么在身份验证后 AnyConnect 证书吊销警告弹出窗口会打开。

如果要避免显示此弹出窗口，请执行以下任一操作：

- 没有任何私有 CRL 要求即可获取证书。
- 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造成严重安全分歧结果。

本地化文件中的消息可以跨多行显示

如果您尝试在本地化文件中搜索消息，这些消息可跨多行显示，如下例所示：

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

在某些路由器后，适用于 Mac OS X 性能的 AnyConnect

当适用于 Mac OS X 的 AnyConnect 客户端尝试创建一个到网关（运行 IOS）的 SSL 连接时，或者当 AnyConnect 客户端尝试从某些类型的路由器（例如思科虚拟办公室 (CVO) 路由器）后创建到 ASA 的 IPsec 连接时，某些网络流量可能通过连接，而其他流量可能丢弃。AnyConnect 可能无法正确计算 MTU。

要解决此问题，可以使用 Mac OS X 命令行中的以下命令将 AnyConnect 适配器的 MTU 手动设置为较低值：

sudo ifconfig utun0 mtu 1200（适用于 Mac OS X 10.7 或更高版本）

防止 Windows 用户规避永远在线

在 Windows 电脑上，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访问权限。他们可以利用这种权限删除 AnyConnect 配置文件，进而规避永远在线功能。为避免这种情况，请将计算机配置为限制对 `C:\ProgramData` 文件夹的访问或至少限制对思科子文件夹的访问。

避免无线承载网络

使用 Windows 7 或更高版本的无线承载网络功能可导致 AnyConnect 不稳定。使用 AnyConnect 时，我们不建议启用此功能或运行可启用此功能的前端应用（如 Connectify 或虚拟路由器）。

AnyConnect 要求将 ASA 配置为接受 TLSv1 流量

AnyConnect 要求 ASA 接受 TLSv1 流量，但不接受 SSLv3 流量。SSLv3 密钥派生算法采用可以减弱密钥派生的方式使用 MD5 和 SHA-1。TLSv1 作为 SSLv3 的接替者，解决该问题以及存在于 SSLv3 的其他安全问题。

因此，AnyConnect 客户端无法和以下“ssl server-version”的 ASA 设置建立连接。

ssl server-version sslv3

ssl server-version sslv3-only

安装时出现 Trend Micro 冲突

如果您的设备具有 Trend Micro，由于驱动程序冲突，则不会安装网络访问管理器。可以卸载 Trend Micro 或取消选中 **trend micro 普通防火墙驱动程序 (trend micro common firewall driver)** 绕过该问题。

Host Scan 将会报告什么

受支持的杀毒软件、反间谍软件和防火墙产品均不报告最后一次扫描时间信息。Host scan 报告以下信息：

- 用于防病毒和反间谍软件

  产品说明

  产品版本

  文件系统保护状态（活动扫描）

  数据文件时间（最后更新和时间戳）

- 用于防火墙

  产品说明

  产品版本

  防火墙是否已启用

长时间重新连接 (CSCtx35606)

如果您启用 IPv6，或者在 Internet Explorer 中启用自动发现代理设置，或者当前的网络环境中不支持自动发现代理设置，则您可能会遇到在 Windows 中长时间重新连接的情况。作为解决方法，如果当前网络环境不支持代理自动发现，您就可以断开未用于 VPN 连接的所有物理网络适配器或在 IE 中禁用代理自动发现。如果采用版本 3.1.03103，具有多宿主系统的设备也可能存在长时间重新连接问题。

具有有限权限的用户无法升级 ActiveX

在 Windows 7 或更高版本中，具有有限权限的用户帐户无法升级 ActiveX 控件，因此也不能使用网络部署方法升级 AnyConnect 客户端。出于最大限度安全性考虑，思科建议用户连接至前端并从应用内部进行客户端升级。

注释　如果之前使用管理帐户在客户端已安装 ActiveX 控件，则用户可以升级 ActiveX 控件。

如果 Java 安装程序失败，请使用 Mac OS X 上的手动安装选项

如果用户在 Mac 上使用 WebLaunch 从 ASA 前端启动 AnyConnect 且 Java 安装程序失败，则对话框中会出现**手动安装 (Manual Install)** 链接。出现此类情况时，用户应执行以下操作：

1. 点击**手动安装 (Manual Install)**。对话框中显示此选项可保存 `.dmg` 文件（包含 OS X 安装程序）。
2. 打开磁盘映像文件 (`.dmg`) 后进行装载，并使用查找器浏览至已装载的卷。
3. 打开“终端”(Terminal) 窗口并使用 CD 命令导航至包含已保存文件的目录。打开 `.dmg` 文件并运行安装程序。
4. 在安装后，依次选择**应用 (Applications)** > **Cisco** > **Cisco AnyConnect 安全移动客户端 (Cisco AnyConnect Secure Mobility Client)** 启动 AnyConnect 会话，或使用 Launchpad。

无主动密钥缓存 (PKC) 或 CCKM 支持

网络访问管理器不支持 PKC 或 CCKM 缓存。在 Windows 7 中，不能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)，可供用户编写自己的自定义客户端程序。

API 软件包包含文档、源文件和库文件，可为 Cisco AnyConnect VPN 客户端提供 C++ 界面支持。您可以使用库和示例程序，用于构建在 Windows、Linux 和 Mac OS X 平台。Windows 平台上的生成文件（或项目文件）也包括在内。对于其他平台，它包括平台特定脚本，显示编译示例代码的方法。网络管理员可将其应用（GUI、CLI 或嵌入式应用）链接到此类文件和库。

您可以从 Cisco.com 下载这些 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 警告

警告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 https://tools.cisco.com/bugsearch/ 在此版本中介绍以下未解决或已解决警告的详细信息。需要通过思科帐户访问漏洞搜索工具。如果您尚无思科帐户，请在此处注册https://tools.cisco.com/RPF/register/register.do。

AnyConnect 4.2.04018

已解决和未解决的警告

要查找此版本已解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

表 *1*：已解决

标识符	组件	标题
certificate	CSCuy12161	AnyConnect 不再需要服务器证书上的密钥协议
core	CSCuy88042	当 HostScan 终端安全评估通过慢速网络链路操作失败时，请通知用户
core	CSCuz01066	AnyConnect 正将公用接口设置为 VA 地址
gui	CSCuy75474	GUI 在下拉控制列表中不显示连接的条目
posture-asa	CSCuy19255	HostScan 在 Mac 上不为 Microsoft AV 检测“activescan”
posture-asa	CSCuy43073	HostScan 无法检测到 ESET 终端安全活动状态扫描
posture-asa	CSCuy45662	为 Linux 版 McAfee VirusScan 2.x 添加 HostScan 支持
posture-asa	CSCuz01661	HostScan 无法检测到 ESET 智能安全 7 活动状态扫描
posture-ise	CSCuy96879	非管理员用户的 ISE 终端安全评估代理 SCCM 补救操作失败
profile editor	CSCuu34998	无法在计算机上使用 JRE 1.8 安装独立配置文件编辑器
vpn	CSCut09823	AnyConnect：ICMP6 防火墙规则未正确处理

vpn	CSCuy78946	AnyConnect 不与 Linux 上的 PEM 存储区连接

要查找此版本未解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

未解决

身份	组件	标题
CSCuz342222	posture-asa	Linux：启用 HostScan 导致无法从 4.2.3013 版升级到 4.2.4018 版

AnyConnect 4.2.03013

已解决和未解决的警告

要查找此版本已解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

表 *2*：已解决

标识符	组件	标题
CSCuy34417	core	AnyConnect 客户端配置文件列表不按字母顺序显示
CSCuw74246	dart	将 Windows 10 错误报告为 Windows 8
CSCux95450	gui	JAWS 不会将终端安全评估状态报告为合规
CSCuy43409	gui	将 IKEv2 和“始终开启”(Always On) 以及 TND 配合使用时，会弹出“多个 AnyConnect”(AnyConnect-Multiple) 窗口
CSCux40858	nam	WWAN APN 间歇性丢失
CSCuy13416	nvm	NVM 无法获取流信息
CSCuw67168	posture-asa	ENH：HostScan：添加对 Mac 版 Bitdefender 病毒扫描程序的支持

标识符	组件	标题
CSCux40109	posture-asa	没有检测到 TrendMicro OfficeScan 到版本 11 的更新
CSCux98114	posture-asa	HostScan 无法在 Mac OS X 上获取 UTF 8 字符串编码的证书字段
CSCuy27569	posture-asa	HostScan 无法从证书的主题名称中获取序列号
CSCuy43901	posture-asa	Linux：ciscod.service 无法加载
CSCux94204	posture-ise	ISE 2.0 P2 终端安全评估 - 磁盘加密不起作用
CSCuy57519	posture-ise	已为事件 ID 259 生成太多日志
CSCuy51590	profile editor	3.1 以上版本的 websec 配置文件编辑器保存 xml 配置文件中的信标配置
CSCut12260	vpn	AnyConnect MacOSX 客户端的 VPN url 崩溃
CSCux04097	vpn	主机文件的安全机制无法实现
CSCuy45271	vpn	涉及 dashost.exe 的 Windows 8 和 10 BSOD
CSCuy51155	web security	Mac 重新引导问题：许可证验证失败
CSCuy51534	web security	AnyConnect web sec 4.2 提示验证可信任网络

要查找此版本未解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

AnyConnect 4.2.02075

已解决和未解决的警告

要查找此版本已解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

表 3：已解决

标识符	组件	标题
CSCux86654	download_install	VPN：ISE 终端安全评估配置文件未由下载程序进行安装
CSCuw92067	gui	菜单选项在列出的选项旁边标有 % 标记
CSCur85411	nam	在登录至 PC 之前，请允许连接到用户创建的网络
CSCus21060	posture-asa	CScan 每分钟都会生成“指纹不匹配”(Fingerprints do not match) 的 Windows 日志
CSCuw80272	posture-asa	HostScan 支持适用于 Mac OS10.11 的 Mac OS X 内置防火墙
CSCuw96489	posture-asa	HostScan“activescan”返回“internalerror”进行 ESET 防病毒操作
CSCux07750	posture-asa	HostScan Mac OS X 10 Sophos 9.2 - lastupdate 值未填充
CSCux52516	posture-asa	无法使用高级终端评估启用 Win 8.1 防火墙
CSCux53899	posture-asa	Linux：启用 HostScan 可造成在断开交流电源后无法连接平台
CSCuw91192	posture-ise	无法检测 AVG 2016
CSCus37509	vpn	Linux：AC 3.1 Debian Jessie - vpnagentd.service 无法加载
CSCus79211	vpn	AnyConnect 首选项解析问题
CSCuw16498	vpn	处于禁用状态的 vpndownloader 上，AnyConnect SBL 缺少“断开连接”(Disconnect) 按钮

CSCuw35003	vpn	在 vpncli 非交互模式下，AnyConnect 处于重新连接状态	
CSCux27277	vpn	AnyConnect 重新连接失败，显示“MTU 值太小”(MTU too small) 的错误	
CSCuy01698	vpn	Windows 8.1 和 Windows 10 上的 BSOD	
CSCux63081	web security	Websec 证书管理：如果已删除或重命名 p7b 文件，则不会下载该文件	

要查找此版本未解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

AnyConnect 4.2.01035

已解决和未解决的警告

要查找此版本已解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

表 4：已解决

标识符	组件	标题
CSCum90946	core	当 split-include 是本地子网的超网时，可路由本地 LAN 子网。
CSCuv04516	core	AnyConnect 删除主机文件最后一个条目
CSCuw47430	core	在 OS X 中未显示质询/响应（质询消息）
CSCuv48563	download install	AnyConnect 安全移动客户端任意文件移动漏洞
CSCux64964	download install	无法从 ASA 安装已更新的 VPN 配置文件
CSCut27870	gui	AnyConnect 将在成功连接时显示感叹号

CSCux26329	gui	AnyConnect 4.x：如果用户主文件夹中有空间，则不启动 GUI
CSCux41420	mobile	AnyConnect 评估 OpenSSL 2015 年 12 月期间的漏洞
CSCuu83807	nam	需要使用一种方法来在 NAM 中手动配置 DHCP 功能
CSCuv93588	phone home	Mac OS X 10.10 3 到 10.10 5 下的 AnyConnect 4.1 每个隔几分钟便会出现崩溃
CSCuv79716	posture-asa	如果通过 msi 软件包已预部署从 ASA 升级 HostScan，则该升级会失败
CSCuw23596	posture-ise	AnyConnect 终端安全评估模块报告错误的操作系统版本
CSCuw81938	posture-ise	AnyConnect 终端安全评估模块将在终端安全评估 XML 报告中发送非法字符
CSCux01500	posture-ise	PM 补救失败，显示错误的错误消息
CSCur31786	vpn	在 AnyConnect 客户端连接上删除 DNS 后缀列表
CSCuv74296	vpn	SBL 在 Windows 10 上不起作用
CSCuw12132	vpn	AnyConnect：ClearSmartcardPin XML 标记不起作用
CSCuw43845	vpn	证书匹配应覆盖 EKU 的所有默认过滤规则
CSCux13036	vpn	AnyConnect 4.2 忽略 preferences.xml 文件
CSCuw99991	web security	由于 MS 可再分发软件包不兼容，导致客户端崩溃

CSCux24537	web security	客户端发出 gprefresh 导致出现 cpu 峰值	

要查找此版本未解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

AnyConnect 4.2.01022

已解决和未解决的警告

要查找此版本已解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

表 *5*：已解决

标识符	组件	标题
CSCuv56788	web security	Websec 客户端无法检测到 TND 服务器

要查找此版本未解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

表 *6*：未解决

标识符	组件	标题
CSCux20705	download_install	Win 10：从 4.2.96 > 4.2.1022 间歇性地升级失败
CSCuv87103	nvm	Mac 上流记录的源 IP 地址为 0.0.0.0
CSCux03932	nvm	NVM 错误报告从交流 DNS 缓存服务请求的 DNS 流量

AnyConnect 4.2.00096

已解决和未解决的警告

要查找此版本已解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

表 *7*：已解决

标识符	组件	标题	

CSCut83093	build_system	未根据 AnyConnect Mac OS X 上的 CiscoSSL 链接可执行文件
CSCum90946	core	当 split-include 是本地子网的超网时，可路由本地 LAN 子网。
CSCur78318	core	AnyConnect 3.1 vpnagent 和 vpncommon 模块同时崩溃
CSCur82067	core	如果 IPv6 DNS 服务器配置在 PHY 接口上，则看不到 DNS 查询
CSCuv01279	download_install	Windows 权限提升漏洞的 AnyConnect 客户端
CSCuv11947	download_install	Linux 或 OS/X 权限提升漏洞的 AnyConnect 客户端
CSCum86682	mobile	AnyConnect 不应丢弃不合格主机的 DNS 请求
CSCuu53359	mobile-android	Android：修复有效的分段问题
CSCuv08412	nam	AnyConnect 4.x 登录不一致的 GUI
CSCuw02322	phone home	将 Windows 10 错误报告为 Windows 8
CSCut12524	posture-asa	ASDM：HostScan 无法在升级到 3.1.06073 版本后进行配置
CSCuu87817	posture-asa	当 Kaspersky 2015 进行实时扫描时，HostScan 失败
CSCuv24279	posture-asa	HostScan 无法找到 AVG 2015 的“lastupdate”值
CSCuv82622	posture-asa	HostScan 3.1.10010 无法识别 Windows 10
CSCut93871	posture-ise	AnyConnect ISE 终端安全评估模块在内存中保持的时间要长于必要时间
CSCuu04245	posture-ise	远程可触发空指针在 ISE 中解引用

CSCuu88169	posture-ise	Microsoft System Center 终端 4.x 病毒定义检查失败	
CSCuf07885	vpn	通过隧道的DNS流量使用全隧道配置 (Windows) 进行限制。	
CSCuu91515	vpn	DTLS 在 SSL 密钥重新生成后中断，同时启动交流电源 3.1MR7/4.0MR2	
CSCuu94601	vpn	如果 IPProtocolSupport 仅为 IPv6，则 AnyConnect 无法连接 [IKEv2]	
CSCuv14020	vpn	当禁用 VpnDownloader 时，SBL 会造成 10 到 15 分钟延迟	
CSCuv58340	vpn	允许 ManualHostInput XML 标记不起作用	
CSCuw13589	vpn	电缆重新连接后，AnyConnect 将无法自动重新连接	
CSCuv35713	web security	抑制 GetHashSHA256 错误消息	
CSCuv42179	web security	未安装许可密钥的网络安全截获浏览器流量	

要查找此版本未解决缺陷相关的最新信息，请参阅思科漏洞搜索工具。

表 *8*：未解决

标识符		标题	
CSCuv46351		在 OS X Yosemite 上的交流 VPN 包括 Apple 无线直接链路 MAC 地址	
CSCuw28341		显示在 VPN 磁贴上的误导性消息	

相关文档

其他 AnyConnect 文档

- Cisco AnyConnect 安全移动客户端版本说明，版本 4.2
- Cisco AnyConnect 安全移动客户端管理员指南，版本 4.2
- AnyConnect 安全移动客户端功能、许可证和操作系统，版本 4.2
- AnyConnect 安全移动客户端版本 4.2 中使用的开源软件
- 思科最终用户许可协议，AnyConnect 安全移动客户端，版本 4.x

ASA 相关文档

- 思科 ASA 系列版本说明
- 思科 ASDM 版本说明
- 导航思科 ASA 系列文档
- 思科 ASA 系列 VPN CLI 配置指南，版本 9.2
- 思科 ASA 系列 VPN ASDM 配置指南
- 支持的 VPN 平台，思科 ASA 5500 系列
- Host Scan 支持图表

ISE 相关文档

- 思科身份服务引擎版本说明，版本 2.0
- 思科身份服务引擎管理员指南，版本 2.0》