# 思科 AnyConnect 安全移动客户端版本说明，版本 4.4

**首次发布日期:** 2016 年 12 月 13 日

**上次修改日期:** 2017 年 04 月 12 日

# AnyConnect 安全移动客户端版本 4.4 版本说明

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

注释

AnyConnect 版本 4.4.x 将成为所有 4.x 漏洞的维护路径。AnyConnect 4.0、4.1、4.2 和 4.3 客户必须升级到 AnyConnect 4.4.x，才能从未来的缺陷修复中受益。AnyConnect 4.0.x、4.1.x、4.2.x 和 4.3.x 中发现的任何缺陷都只能在 AnyConnect 4.4.x 维护版本中修复。

## 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。

### SUMMARY STEPS

1. 点击此链接前往 Cisco AnyConnect 安全移动客户端产品支持页面：
2. 登录 Cisco.com。
3. 点击**下载软件**。
4. 如果尚未选择最新版本，则展开**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：
   - 若要下载单一软件包，请查找要下载的软件包并点击**下载 (Download**）。
   - 若要下载多个软件包，请点击软件包行的**加入购物车 (Add to cart)**，然后点击“下载软件”(Download Software) 页面顶部的**下载购物车 (Download Cart**）。
6. 系统提示时，阅读并接受思科许可证协议。
7. 选择用于保存下载文件的本地目录并点击**保存 (Save)**。
8. 请参阅《Cisco AnyConnect 安全移动客户端版本 4.x 管理员指南》。

**DETAILED STEPS**

**步骤 1** 点击此链接前往 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 Cisco.com。

**步骤 3** 点击**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)** 文件夹并点击最新版本。

**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点击**下载 (Download**）。
- 若要下载多个软件包，请点击软件包行的**加入购物车 (Add to cart)**，然后点击“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点击**保存 (Save)**。

**步骤 8** 请参阅《Cisco AnyConnect 安全移动客户端版本 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 | anyconnect-win-*version*-webdeploy-k9.pkg |
| Mac OS X | anyconnect-macos-*version*-webdeploy-k9.pkg |
| Linux（64位） | anyconnect-linux64-*version*-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 | anyconnect-win-*version*-predeploy-k9.zip |
| Mac OS X | anyconnect-macos-*version*-predeploy-k9.dmg |
| Linux（64位） | anyconnect-linux64-*version*-predeploy-k9.tar.gz |

还可以下载其他文件，这些文件有助于您为 AnyConnect 添加其他功能。

## AnyConnect 4.4.02034 新增功能

AnyConnect 4.4.02034 是一个包括以下增强功能的维护版本，可以解决 AnyConnect 4.4.02034 ，第 27 页中所述的缺陷。

## AnyConnect 4.4.01054 新增功能

AnyConnect 4.4.02034 是一个包括以下增强功能的维护版本，可以解决 AnyConnect 4.4.01054 ，第 29 页中所述的缺陷。

- ISE 安全评估增强功能

注释 要利用这些 ISE 安全评估的功能，需要使用 ISE 2.2（或更高版本）。

有关ISE配置的更多详细信息，请参阅思科身份服务引擎管理员指南，版本2.2。

Stealth 代理安全评估 -（仅限 Windows 和 Mac）允许 ISE 安全评估在 AnyConnect Ul 中作为隐藏服务运行。例如，AnyConnect Stealth 安全评估代理可隐藏系统扫描块以及来自最终用户客户端的通知。

持续终端监控 - 监控已安装和正在运行的应用，确保检测终端上的动态变更。

下一代调配和发现 - 提供更多基于非 URL 重定向的选项，以便从 ISE 部署 AnyConnect 软件；加强 AnyConnect 与 ISE 通信的恢复能力，包括通过第三方网络基础架构支持合规流的能力。

应用攻击和卸载功能 - 可以针对特定应用采取策略操作或减少软件许可证的使用量。

终端环境可见性 - 添加唯一标识符 (UDID) 来标识特定终端，而不是仅依靠 MAC 地址。

更多环境检查 -（仅限 Windows 和 Mac）检查第三方和本机操作系统的防火墙状态以及自动补救能力

- 更改了与 OpenDNS Umbrella 相关的品牌名称。部分示例如下：

  OpenDNS Umbrella 现称为思科 Umbrella

  OpenDNS 全球网络现称为思科 Umbrella 全球网络

  Umbrella 虚拟设备现称为思科 Umbrella 虚拟设备

  OpenDNS Umbrella 漫游客户端现称为思科 Umbrella 漫游客户端

## AnyConnect 4.4.00243 新增功能

AnyConnect 4.4.00243 是主要版本，包括以下功能和增强功能，可以解决 AnyConnect 4.4.00243 ，第 30 页中所述的缺陷。

- SAML 2.0 SSO（已与 ASA 版本 9.7.1 相集成）- 通过 SAML 支持更广泛的基于 Web 的身份验证。您可以使用 SAML 执行初始单点登录 (SSO) 会话身份验证。在重新连接期间，AnyConnect 会有意不再执行 SAML 进程，因为这样会对无缝重新连接造成不利影响。此外，如果用户使用浏览器从 IdP 中注销，AnyConnect 会话仍会保持。您必须拥有 Apex 许可证，才能使用 SAML 功能。
- 多种证书身份验证（已与 ASA 版本 9.7.1 相集成）- Windows 为 AnyConnect 提供证书存储，以便用于 VPN 客户端配置文件。现在，您可以使用多种证书身份验证组合，并可通过配置安全网关来向客户端指示特定 VPN 连接可接受多种证书身份验证选项中的哪一种。
- 加强连接超时的安全性 - 使用 ASA 中的 vpn-session-timeout 和 vpn-session-timeout alert-interval 设置，AnyConnect 安全移动客户端的最终用户可在超出会话时间限制时收到会话到期通知。UI 会显示“您的连接即将超出会话时间限制。需要建立新的连接”(Your connection will soon exceed the session time limit. A new connection will be necessary) 消息，以便他们可以纠正这种情况，而不必从 VPN 注销。有关调整这些设置的更多信息，请参阅以下位置的**在组策略中指定最长 VPN 连接时间**部分：http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn-config/vpn-groups.html。

  **注释** 您可能需要将**显示连接通知 (Show Connection Notices)** 作为 AnyConnect 首选项启用，才能查看这些警报。

- DHCP 服务器路由控制 - 在 Windows 中，通过设置组策略自定义属性可以控制 DHCP 公共服务器路由的创建。为了避免在建立隧道时创建公共 DHCP 服务器路由，必须具有 no-dhcp-server-route 自定义属性并将其设置为 *true*。
- 进一步实施 IPv6 - 单堆栈或双堆栈网络中的 IPv6 连接非常稳定，用户可以控制用于连接的主 IP 协议和辅助 IP 协议。在 IPv6 至 IPv4（或反之）之间迁移时，重新连接是无缝的，如果隧道连接中断，应在两个协议之间进行回退。对于 IPv6，增加了 IKEv2 隧道支持。
- 网络可视性模块增强功能 -

  扩大数据收集范围，从而增加了匿名化散列处理，而不只是将其完全丢弃

  在 Windows、Windows 64 位和 Mac OS X 上支持将 Java 用作容器

  缓存配置，用于设置大小上限和持续时间

  定期流量报告，可按您所配置的间隔跟踪流量（例如服务器连接或下载）

- 适用于 Windows 的签名验证更新 - 只有思科提供的转换才可应用于 ASA 或 ISE。客户提供的转换（未经思科签名）无效。您可以通过带外方法应用自己的转换。

### 与 Umbrella 漫游安全插件相关的其他漏洞修复

- 如果注册失败，插件可能会在没有正确策略的情况下应用 DNS 保护。
- （仅限 Windows 10）网络适配器不会按正确的优先级顺序从系统返回。
- 支持云 API 可扩展性，以减少 Umbrella 后端云基础设施上 Umbrella 漫游插件的负载

注释 我们正在调查一种情况，即 Umbrella 漫游插件可能无法正确提取域搜索后缀，进而导致本地域解析问题。

**Mac OS X 修复**

- (CSCvb49067) IPv6 网络中应开启 Umbrella 保护状态
- 在 Umbrella 插件注册期间检索终端主机名时出错
- 支持云 API 可扩展性，以减少 Umbrella 后端云基础设施上 Umbrella 漫游插件的负载

# 重要互通性注意事项

**ISE 头端与 ASA 头端共存**

- 如果同时使用 ISE 和 ASA 执行客户端安全评估，则两个头端上的配置文件必须匹配。
- 如果为终端调配了 NAC 代理，AnyConnect 会忽略 ISE 1.3 服务器。
- 如果客户端上同时装有思科 NAC 代理和 VPN 安全评估 (HostScan) 模块，则思科 NAC 代理版本必须至少是 4.9.4.3 或更高版本才能防止安全评估冲突。
- 如果在 ISE 中为终端调配了 AnyConnect，NAC 代理会忽略 ISE 1.3 服务器。

# 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 或更高版本的 32 位版本。

## AnyConnect 的 ISE 要求

**ISE 版本要求**

- 至少需要 ISE 1.3 才能将 AnyConnect 软件部署到终端，以及使用 AnyConnect 4.0 和更高版本中的新 ISE 安全评估模块对该终端进行安全评估。
- ISE 1.3 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 头端部署 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《思科身份服务引擎版本 2.0 管理员指南》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，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

  AnyConnect 客户端延迟升级

- 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。

### 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加载到此型号。若要成功加载 AnyConnect，软件包的大小需要减少到适应可用闪存的大小，即减少操作系统数、没有 Host Scan 等。

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 互通性

通过 VPN 安全评估 (HostScan) 模块，思科 AnyConnect 安全移动客户端可以识别 ASA 主机中安装的操作系统、防病毒软件、反间谍软件和防火墙软件。

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、防病毒软件、反间谍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）。

AnyConnect 4.4.x 与 HostScan 4.3.05017 之前的 HostScan 版本不兼容。但是，AnyConnect 4.4.x 向后兼容 HostScan 4.3.05017，而您在 ASDM 中必须使用 HostScan 4.3.05017（或更高的 HostScan 4.3.x 版本）作为 HostScan 映像（“配置”[Configuration]>“远程访问 VPN”[Remote Access VPN]>“安全桌面管理器”[Secure Desktop Manager]>“Host Scan 映像”[Host Scan image]）。

Cisco.com 上提供防病毒软件、反间谍软件和防火墙应用列表。Firefox 浏览器是用于打开支持图表的最轻松方式。如果使用 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`。您可以使用 Microsoft Excel、Microsoft Excel Viewer 或 Open Office 打开该文件。

**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。

## ISE 安全评估合规性模块

ISE 安全评估合规性模块包含 ISE 安全评估支持的防病毒软件、反间谍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。当头端上的版本号（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。您可以用 Microsoft Excel、Microsoft Excel Viewer 或 OpenOffice 在以下位置查看图表：

## 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

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

思科 AnyConnect 安全移动客户端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 (PRT) | 客户体验反馈 | 网络可视性模块 | AMP 启用程序 | Umbrella 漫游安全 |
|---|---|---|---|---|---|---|---|---|---|---|
| Windows 7 SP1、8、8.1 和 10<br>x86（32 位）和 x64（64 位） | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|
| Mac OS X 10.10、10.11 和 10.12 | 是 | 否 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| Linux Red Hat 6、7 及 Ubuntu 12.04 (LTS) 和 14.04 (LTS)（仅限 64 位） | 是 | 否 | 否 | 是 | 否 | 是 | 是 | 否 | 否 | 否 |

注释 除以上所列的版本之外，其他版本也可能适用，不过思科没有全面测试以上所列版本之外的所有版本。

## 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 Cisco 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 的桌面模式下运行。
- 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，使用计算机密码的计算机身份验证在 Windows 8 或 10/Server 2012 上不起作用，除非对客户端桌面应用 Microsoft KB 2743127 (http://support.microsoft.com/kb/2743127) 中所述的注册表修复。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

- 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 2.0.0。
- gdk 2.0.0。
- libpango 1.0。
- iptables 1.2.7a 或更高版本。
- 随内核 2.4.21 或 2.6 提供的 tun 模块。

## Mac OS X 对 AnyConnect 的支持

### Mac OS X 要求

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

### 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 and identified developers（已签名的应用）。AnyConnect 是签名的应用，但并非以 Apple 证书进行签名。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** WebLaunch 或操作系统升级（例如 10.7 到 10.8）会按预期安装。只有预部署安装因为 Gatekeeper 的原因而需要额外的配置。

# AnyConnect 许可

有关最新的最终用户许可协议，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。

若要从 ISE 头端部署 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《思科身份服务引擎版本 2.1 管理员指南》的思科 *ISE* 许可证一章。

若要从 ASA 头端部署 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 安全移动客户端：

- 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 软件包在头端（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，用户可连接到头端以下载 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，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。

有关部署 AnyConnect 模块的详细信息，请参阅《Cisco AnyConnect 安全移动客户端版本 4.4 管理员指南》。

**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。

## 从 3.1 MR10 AnyConnect 客户端升级/不兼容问题

将 AnyConnect 3.1.10010 自动部署到终端后，无法连接到使用不兼容的 AnyConnect 版本 4.0、4.1、4.1MR2、4.2 和 4.3 配置的安全网关。如果尝试从 AnyConnect 3.1 MR10 版本升级到 AnyConnect 4.1MR4（或更高版本）或高于 3.1.10010 的 3.1 版本以外的任何版本，将收到不允许升级的通知。

有关详细信息，请参阅 CSCuv12386。

## 从 AnyConnect 3.0 或更高版本升级

从 AnyConnect 安全移动客户端版本 3.0 或更高版本升级时，AnyConnect 会执行以下操作：

- 升级核心客户端的所有之前版本并保留所有 VPN 配置。
- 升级 AnyConnect 所使用的任何 Host Scan 文件。

### 从 AnyConnect 2.5 及更低版本升级

从 AnyConnect 的任何 2.5.x 版本升级时，AnyConnect 安全移动客户端会执行以下操作：

- 升级核心客户端的所有之前版本并保留所有 VPN 配置。
- 升级 AnyConnect 所使用的任何 Host Scan 文件。
- 如果安装网络访问管理器，AnyConnect 会保留所有 CSSC 5.x 配置，以供网络访问管理器使用，并随后删除 CSSC 5.x。
- 不会升级或删除 Cisco IPsec VPN 客户端。但是，AnyConnect 客户端可在计算机上与 IPsec VPN 客户端共存。
- 不会升级并无法与 Cisco ScanSafe AnyWhere+ 共存。必须在安装 AnyConnect 安全移动客户端前卸载 AnyWhere+。

**注释** 如果从传统 Cisco VPN 客户端升级，物理适配器的 MTU 值可能已降低到 1300。应针对每个适配器将 MTU 值还原为默认值（通常为 1500），以在使用 AnyConnect 时获得最优性能。

不支持使用 ASA 或 WebLaunch 从 AnyConnect 2.2 升级。必须先卸载 AnyConnect 2.2，然后手动或使用 SMS 安装新版本。

### 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

### 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。

### Win32 在连接待机方面的局限

由于 AnyConnect 是 Win32（非 Windows 商店）应用，所以在权限方面受到 Microsoft 的限制；因此，AnyConnect 无法实现对 Windows 8 及更高版本中“连接待机”(Connected Standby)（暂停和恢复事件）状态的访问。

### 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 (split-include) 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-包含 (split-include)（拒绝 0.0.0.0/32 或 ::/128）。

如果在拆分-包含 (split-include) 中配置了超网并且所需行为是要允许 LocalLan 访问，则需要对新行为进行以下配置：

- 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。

## 不再支持 RC4 TLS 密码套件

从 AnyConnect 版本 4.2.01035 开始，因安全策略增强功能而不再支持 RC4 TLS 密码套件。

## 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。

## 网络可视性模块与 LittleSnitch 防火墙不兼容

网络可视性模块与 Mac OS X 上的 LittleSnitch 防火墙不兼容。

### Mac OS X El Capitan 10.11 对 AnyConnect 的支持

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

### 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 Mac 上使用 ISE 安全评估的互通性

如果使用 Mac OS X 10.9 或更高版本并想要使用 ISE 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。

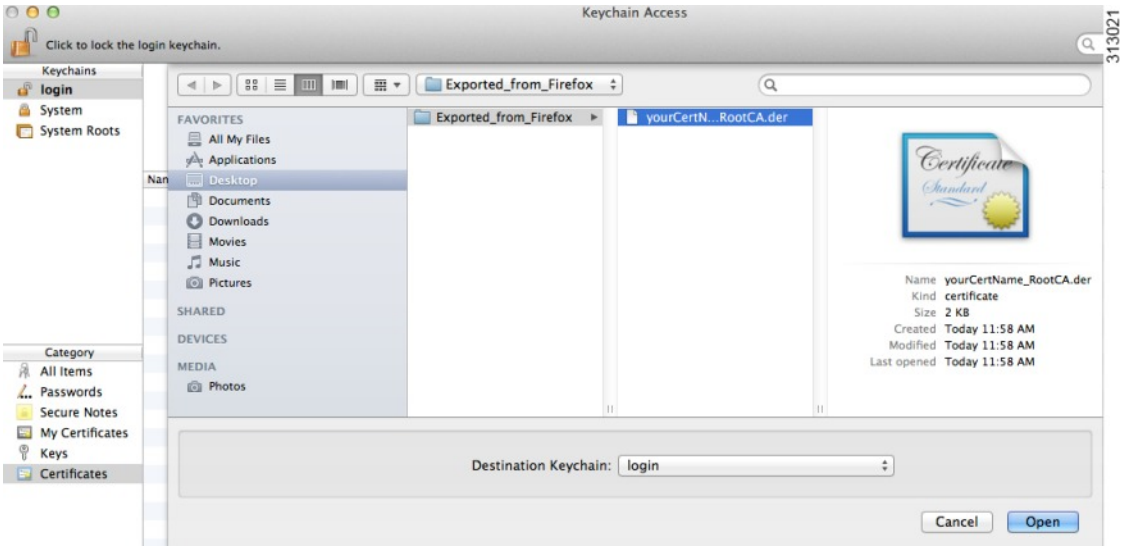
### 不支持 Mac OS X 上的 Firefox 证书存储

Mac OS X 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 Mac OS X 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 (Preferences) > 高级 (Advanced)** 的“证书”(Certificates) 选项卡，然后点击 **查看证书 (View Certificates)**。
2. 选择用于 AnyConnect 的证书，然后点击 **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。

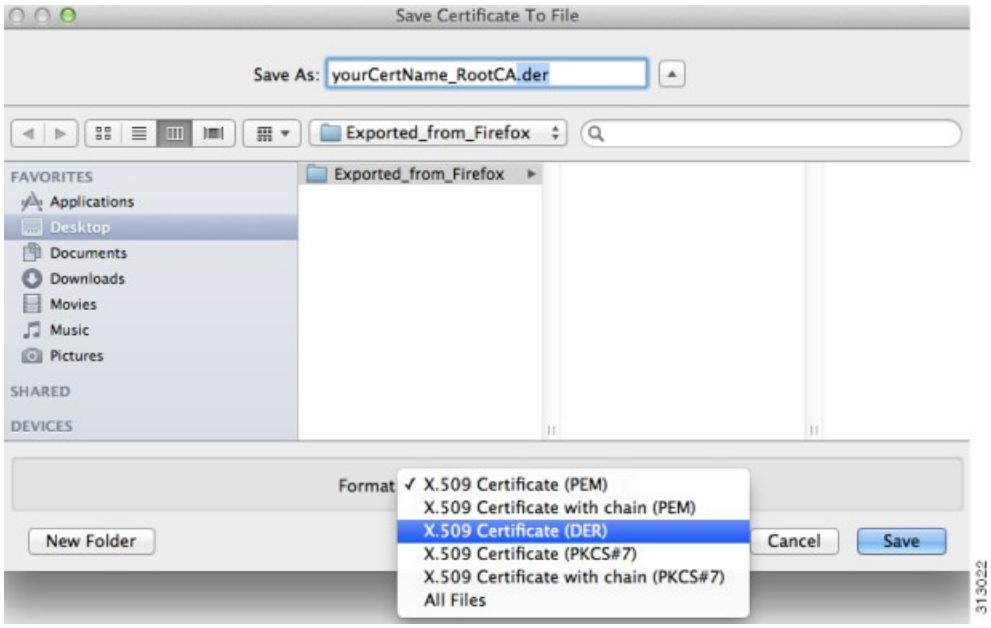



注释 如果使用/需要多个 AnyConnect 证书和/或私钥，请对每个证书重复上述流程）。

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。

## AnyConnect UI 因缺少依赖性 libpangox 出错

在许多较新的 Linux 分发版本中，AnyConnect 用户界面可能会无法启动，并出现以下错误：

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

缺失的库已过时且不再可用。这会影响其他应用，而不仅仅是影响 AnyConnect。

Pango 已发布 其他公司构建且可在线获得的兼容库的 源代码。要解决此问题，请查找并安装以下任一软件包 *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 正常工作

(CSCue04930) 在 ASDM 中选择 SSLv3 “仅限 SSLv3”(SSLv3 only) 或“协商 SSLv3”(Negotiate SSLv3) 选项时，Host Scan 不会正常工作（“配置”[Configuration] > “远程访问 VPN”[Remote Access VPN] > “高级”[Advanced] > “SSL 设置”[SSL Settings] > 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。

## 修改 sysctl 网络设置导致的问题

我们发现存在 Apple Broadband Tuner 应用（从 2005 年起）与 Mac OS X 10.9 配合使用的实例。该应用更改 sysctl.conf 中的网络设置，这可能导致连接问题。该应用设计适用于更低版本的 Mac OS。我们怀疑当前默认操作系统设置将宽带网络纳入考虑范围，因此大多数用户将无需采取任何措施。

和 AnyConnect 3.1.04074 一起运行经过修改的 sysctl 设置可能会生成以下消息：

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

### 验证

若要验证问题原因是否为 sysctl 网络设置，请打开终端窗口并输入：

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

如果结果包含远低于默认值 8388608 的值，例如：

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

则此值可能已被 Apple Broadband Tuner 应用在 /etc/sysctl.conf 中覆盖

### 修复

编辑 /etc/sysctl.conf，对设置 kern.ipc.maxsockbuf 的行添加注释，然后重新启动计算机。

或

如果除 Broadband Tuner 应用设置的自定义值外没有其他自定义值，则重命名或删除 sysctl.conf。

Apple 已知晓此问题，并已提交漏洞 ID 15542576。

### 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 编辑为不安全模式。

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

### 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。

### Internet Explorer、Java 7 和 AnyConnect 3.1.1 互通性

Internet Explorer 的受支持版本在以下情况下停止运行：当用户尝试连接到 ASA 时、当终端上安装了 Java 7 时，当 ASA 上安装并启用了 Host Scan 时、当 ASA 上安装并启用了 AnyConnect 3.1.1 时。

如果安装的是 ActiveX 或更低版本的 Java 7，此情况不会发生。若要避免此问题，请在终端上使用 Java 的受支持版本，即低于 Java 7 的版本。

请参阅 Bug Toolkit 和缺陷 CSCuc48299 进行验证。

### 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。
- Mac OS X 10.4 及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

思科使用以下虚拟机环境执行部分 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。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 Host Scan 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 Host Scan 软件包的行为错误解释为恶意。在安装安全评估模块或 Host Scan 软件包之前，将防病毒软件配置到“白名单”或将以下 Host Scan 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。

## 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 (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，请将该终端配置为永不成为主要或备用浏览器。

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 点击 **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。

如果要避免显示此弹出窗口，请执行以下任一操作：

- 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. "
```

## Mac OS X 版 AnyConnect 部署于特定类型路由器之后时的性能

当 Mac OS X 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 Mac OS X 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 Mac OS X 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 要求 ASA 配置为接受 TLSv1 流量

AnyConnect 要求 ASA 接受 TLSv1 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。

### Host Scan 报告内容

受支持的防病毒软件、反间谍软件和防火墙产品都不报告上次扫描时间信息。Host Scan 报告以下信息：

- 对于防病毒软件和反间谍软件

  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头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。

### 在 Java 安装程序失败时使用 Mac OS X 上的手动安装选项

如果用户在 Mac 上从 ASA 头端使用 WebLaunch 来启动 AnyConnect，且 Java 安装程序失败，将出现显示**手动安装 (Manual Install)** 链接的对话框。此时，用户应执行以下操作：

1. 点击**手动安装 (Manual Install)**。将出现对话框，显示保存包含 OS X 安装程序的 `.dmg` 文件的选项。
2. 打开文件并使用查找器浏览到安装卷来安装磁盘映像 (`.dmg`) 文件。
3. 打开终端窗口并使用 CD 命令导航到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，选择**应用 (Applications)** > **Cisco** > **Cisco AnyConnect 安全移动客户端 (Cisco AnyConnect Secure Mobility Client)** 来启动 AnyConnect 会话，或使用启动板。

### 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 Cisco 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 4.4.02034

若要查找有关此版本中已解决警告的最新信息，请参阅思科漏洞搜索工具。

表 *1*：已解决

| 标识符 | 组件 | 标题 |
|---|---|---|
| CSCvd10396 | download_install | 从 4.1 升级到 4.4 期间，几台计算机中的 AnyConnect 出现故障 |
| CSCux42801 | gui | 当点击 Enter 重新连接时，AnyConnect 会启动高级屏幕 |
| CSCvd23056 | gui | 启用缩放的情况下，高分辨率显示的 AnyConnect 平铺窗口不正确 |
| CSCux95776 | nam | 使用 NAM 首次登录 win 时，使用错误的凭据无法执行 n/w 访问 |
| CSCvb875955 | nam | AnyConnect NAM 有时不显示 SSID |
| CSCvd06041 | nam | 锁定后，Windows Surface Pro 中的 AnyConnect 连接丢失 |
| CSCvd28999 | nam | 当 Windows 10 从低功率状态下恢复时，有时不会建立 NAM WiFi 连接 |
| CSCvd510910 | nam | 当用户验证失败时，NAM 会切换到延伸超出注销的用户验证模式 |
| CSCvd51118 | posture-asa | 当 Windows 10 从低功率状态下恢复时，有时不会建立 NAM WiFi 连接<br>Cscan 崩溃 - HostScan v4.3.05019 |
| CSCvc99583 | posture-ise | 在某些情景下，在 Mac ISE 10.12 中检测不到 ISE |
| CSCvd24513 | vpn | 客户端防火墙：Windows 中基于当前本地化的行为不可靠 |
| CSCvd33217 | vpn | 当不存在 DNS 服务器导致重新连接环路失败时，缓存的 SG IP 被清除 |
| CSCvd53608 | vpn | 解析 slowDNS 时，等待 VPN 代理响应的下载程序更新超时 |
| CSCvd73624 | vpn | MacOS：在桌面登录期间，独立的 Umbrella 模块（VPN 已禁用）不会启动 AnyConnect UI |

表 *2*：开放

| 标识符 | 组件 | 标题 |
|---|---|---|
| CSCvd90969 | fireamp | 由于验证代码标志，无法在 Windows 上安装 Fireamp 连接器 |

若要查找有关此版本中已解决警告的最新信息，请参阅思科漏洞搜索工具。

## AnyConnect 4.4.01054

若要查找有关此版本中已解决警告的最新信息，请参阅思科漏洞搜索工具。

**表 *3*：已解决**

| 标识符 | 组件 | 标题 |
|---|---|---|
| CSCvc87398 | api | 接收回调 VpnStateNotification 时出现问题 |
| CSCva28598 | 核心层 | AnyConnect 和 Verizon Jetpack (Netgear) 导致 Windows 10 出现 BSOD 问题 |
| CSCvc09700 | 核心层 | 升级至 Windows 10 版本 1511 后添加了持久路由 - 导致 AnyConnect 中断 |
| CSCvc54120 | 核心层 | 不管 LocalUsersOnly 设置如何，AnyConnect 4.3 都允许 RDP 用户进行连接 |
| CSCvc12767 | download_install | 对于 Mac，卸载“ISE 客户端调配”(ISE Client Provisioning) 下的 NAC 代理不会卸载 NAC |
| CSCvc43976 | gui | Windows SBL 版思科 AnyConnect 安全移动客户端权限升级漏洞 |
| CSCvc73780 | gui | 4.4.01022：在隐身模式不应显示“首选项”(Preference) 窗口 |
| CSCvd02715 | gui | 4.4.0.1048：当客户端从隐身切换为标准模式时，系统扫描 UI 不正确 |
| CSCuz57473 | nam | 对于使用 SSO 的新用户，NAM 与错误消息不一致 |
| CSCvc56754 | nam | NAM 安装程序不应再提供 DIFxAPI DLL |
| CSCvc86615 | nam | AnyConnect UI 在打开与 NAM 相关的 UI 时崩溃 |
| CSCvc62819 | opswat-asa | 使用 hostscan_4.3.05017 启用 DAP 时，Windows 7 AnyConnect 用户无法进行连接 |
| CSCvb99491 | opswat-ise | 请求在适用于 ISE 的 Mac 10.12 中支持 Filevault 10.12.x |
| CSCvc16571 | opswat-ise | ISE 合规性模块不支持 Symantec Endpoint Protection 14.x |
| CSCvc56097 | opswat-ise | AVC 无法在 Windows 上显示应用数据 |

| 标识符 | 组件 | 标题 |
|---|---|---|
| CSCvb49663 | posture-ise | 不管强制性要求状态如何，系统都会针对可选要求弹出补救提示 |
| CSCvc14638 | posture-ise | 访问网络驱动器时显示“IT 策略禁止使用 USB 存储设备”(IT policy prohibits the use of USB storage devices) |
| CSCvc47785 | posture-ise | OS X 10.9 上的安全评估失败 |
| CSCvc62236 | posture-ise | ZipException 导致 ISE 2.1 AnyConnectComplianceModuleOSX 3.6.10910.2 下载失败 |
| CSCux13191 | vpn | 如果不存在 hal-get-property，CLI 无法进行连接 |
| CSCvb63859 | vpn | 适用于 Linux 的思科 AC 将敏感信息保留在内存中 |
| CSCvc00828 | vpn | AnyConnect 备份服务器连接会绕过代理 |
| CSCvc89318 | vpn | AnyConnect 4.3 无法区分 RDP 登录和本地登录，AllowRemoteUsers 不起作用 |
| CSCvc67700 | Web 安全 | 在服务启动期间，网络安全代理崩溃 |

若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。

## AnyConnect 4.4.00243

若要了解本版本中已解决警告的最新相关信息，请参阅思科漏洞搜索工具。

**表 *4*：已解决**

| 标识符 | 组件 | 标题 |
|---|---|---|
| CSCuz92464 | download_install | 思科 AnyConnect 本地权限升级漏洞 |
| CSCvc12767 | download_install | 对于 Mac，卸载“ISE 客户端调配”(ISE Client Provisioning) 下的 NAC 代理不会卸载 NAC |
| CSCuw79769 | posture-asa | HostScan 会忽略 ASA 头端设置的日志记录级别 |
| CSCva40592 | posture-asa | 在安装有 Java 8 的 Mac 上，HostScan/CSD 冻结 ASDM |
| CSCuz55943 | posture-ise | AnyConnect 4.x 在关闭 PRA 计时器后，代理不会发送 PRA 更新 |
| CSCva03590 | posture-ise | AnyConnect 安全评估模块会间歇性发生崩溃 |

| 标识符 | 组件 | 标题 |
|---|---|---|
| CSCuv65460 | vpn | 在 Mac OS X 中自动重新连接后会删除系统代理设置 |
| CSCva35797 | vpn | AnyConnect 对 CVE-2016-2177、CVE-2016-2178 的评估 |
| CSCvb41365 | vpn | AnyConnect 无法通过 Windows 10 (1607) 版本的代理进行连接 |
| CSCvb48665 | vpn | 2016 年 9 月 AnyConnect 对 OpenSSL 的评估 |
| CSCvb62962 | vpn | OS X：Deflate 压缩不起作用（无法传输某些数据） |
| CSCvc04354 | vpn | 主页 URL 不能搭配 AnyConnect 4.3 使用 |
| CSCvc05423 | vpn | Mac OS 10.12 (Sierra) IPv6 地址隐私功能导致网络不稳定 |

若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。

# 相关文档

### 其他 AnyConnect 文档

- 思科 AnyConnect 安全移动客户端版本说明，版本 4.4
- 思科 AnyConnect 安全移动客户端管理员指南，版本 4.4
- AnyConnect 安全移动客户端功能、许可证和操作系统，版本 4.4
- *AnyConnect* 安全移动客户端版本 *4.4* 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 ASA 系列文档一览
- 思科 ASA 5500-X 系列下一代防火墙配置指南
- 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 2.2
- 思科身份服务引擎管理员指南，版本 2.2