Apple iOS 版 Cisco AnyConnect Secure Mobility Client 4.9.x 版本说明

Apple iOS 版 AnyConnect 版本说明

Apple iOS 移动设备版 AnyConnect

AnyConnect 安全移动客户端为远程用户提供与思科 ASA 5500 系列的安全 VPN 连接。通过该客户端，用户能够无缝、安全地远程访问企业网络，使安装的应用可如同直接连接到企业网络一般进行通信。AnyConnect 支持通过 IPv4 或 IPv6 隧道连接到 IPv4 和 IPv6 资源。

本文档适用于 AnyConnect 安全移动客户端和自适应安全设备 (ASA) 5500 的管理员，为 Apple iOS 设备上运行的 AnyConnect 提供版本特定信息。

AnyConnect 应用仅在 Apple ITunes 应用商店可获得。思科不分发 AnyConnect 移动版应用，您也不能从 ASA 部署该移动应用，但是，您可以从 ASA 为桌面设备部署其他版本的 AnyConnect，并同时支持此移动版本。

AnyConnect 移动版支持策略

思科支持应用商店当前提供的 AnyConnect 版本；但是，修复和增强功能仅在最新发行的版本中提供。

AnyConnect 许可

若要连接到 ASA 头端，需提供 AnyConnect 4.x Plus 或 Apex 许可证；试用许可证可用；请参阅 思科 AnyConnect 订购指南。

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 Cisco AnyConnect Secure Mobility Client 版本 4.x 中使用的开源软件（适用于移动设备）

使用 TestFlight 测试 Cisco AnyConnect Beta

AnyConnect 的试用版可用于 TestFlight 上预发行测试。单击此链接参与 TestFlight 测试：https://testflight.apple.com/join/N0QLSq2c。

稍后可使用此相同 TestFlight 链接退出。选择退出后，您需要卸载试用版并重新安装最新的非试用版 AnyConnect。

请及时报告在试用版测试过程中发现的问题，方式是发送邮件至思科邮箱 ac-mobile-feedback@cisco.com。思科技术支持中心 (TAC) 不会处理在 AnyConnect 的试用版中发现的问题。

可用于 Apple iOS 的 AnyConnect 版本

Apple iOS 版思科 AnyConnect 当前具有多个版本：

- **思科 *AnyConnect***

  Cisco AnyConnect 4.9 是适用于 Apple iOS 的最新版本，建议使用此版本。为确保您始终收到最新的 Apple iOS 漏洞修复，请升级至最新版本。

  我们建议对于 Apple iOS 10.3 及更高版本使用此版本。此版本使用 iOS 提供的新扩展框架来实施 VPN 及其所有功能。每个应用程序 VPN 隧道是完全受支持的功能，新扩展框架允许支持 TCP 和 UDP 应用。自此以后，此新思科 AnyConnect 版本将是唯一包含所有增强功能及漏洞修复的版本。

- **思科旧版 *AnyConnect***

  旧版 AnyConnect x 4.0.05x 在 iOS 11.x 上的版本不受支持。要与更高版本的 iOS 兼容，请安装应用商店中可用的最新 AnyConnect 应用。

  旧版 AnyConnect 支持目前在应用商店已推出一段时间的 Apple iOS 6.0 及更高版本。此版本将随时间推移而退出，但目前仍然可用，以便轻松过渡到建议的最新版本。

  旧版 AnyConnect 应用中的 Per App VPN 隧道功能不会获得 TAC 支持。客户若要使用 Per App VPN，应迁移到新版本。

  仅应针对严重的安全问题更新旧版 AnyConnect。此版本继续编号为 4.0.05x。

思科 AnyConnect 和旧版 AnyConnect 是不同的应用，其应用 ID 有所不同。因此：

- 在 AnyConnect 4.0.07x（及更高版本）中使用新扩展框架会导致来自传统 AnyConnect 4.0.05x 的行为发生以下更改：AnyConnect 认为隧道 DNS 服务器的流量是通过隧道传输的，即使它不在拆分 - 包含网络中。
- 不能将 AnyConnect 应用从旧版 4.0.05x 或更早版本升级到 AnyConnect 4.0.07x 或 4.6.x（或更高版本）。Cisco AnyConnect 4.0.07x（或 4.6.x 和更高版本）是单独的应用，使用不同的名称和图标进行安装。
- AnyConnect 的不同版本可以共存于移动设备之上，但思科不支持此操作。如果在安装了两个 AnyConnect 版本时尝试进行连接，行为可能与预期不同。请确保您的设备上只有一个 AnyConnect 应用，并且其版本适合您的设备和环境。
- 新 AnyConnect 应用版本 4.0.07072 或更高版本不能访问或使用以旧版 AnyConnect 版本 4.0.05069 及任何更早版本导入的证书。两个应用版本均可访问和使用 MDM 部署的证书。
- 如果要更新至新版本，应删除导入到旧版 AnyConnect 应用的应用数据，例如证书和配置文件。否则，它们将继续显示在系统 VPN 设置中。在卸载旧版 AnyConnect 应用之前删除应用数据。

- 当前的 MDM 配置文件不会触发新应用。EMM 供应商必须支持 VPNType (VPN)、VPNSubType (com.cisco.anyconnect) 和 ProviderType (packet-tunnel)。为了与 ISE 集成，它们必须能够将唯一标识符传递给 AnyConnect，因为 AnyConnect 在新框架中不能再访问此信息。有关如何设置此功能，请咨询您的 EMM 供应商，有些可能需要自定义 VPN 类型，另一些在发布时可能无可用的支持。

在 AnyConnect 4.0.07x 及更高版本中使用新扩展框架会导致旧版 AnyConnect 4.0.05x 中的行为发生以下变化：

- 在新版本中，发送到前端的设备 ID 不再是 UDID，而且重置为出厂设置后，设备 ID 将发生变化，除非您的设备从其进行的备份中执行恢复。
- 您可以使用 MDM 部署的证书和使用 AnyConnect 中可用的某种方法导入的证书：SCEP、通过 UI 手动导入或通过 URI 处理程序导入。新版 AnyConnect 不能再使用通过邮件或识别的这些方法之外的任何其他机制导入的证书。
- 在使用 UI 创建连接条目时，用户必须接受显示的 iOS 安全消息。
- 用户创建的条目若与从 AnyConnect VPN 配置文件中下载的主机条目名称相同，当它们处于活动状态时，在断开连接前不会对其重命名。另外，断开连接后，下载的主机连接条目将出现在 UI 中，保持连接时则不会显示在 UI 中。
- AnyConnect 认为隧道 DNS 服务器的流量将通过隧道传输，即使它不在拆分 - 包含网络中。

支持的 Apple iOS 设备

Cisco AnyConnect 4.9 作为最新的建议版本，可用于运行 Apple iOS 10.3 及更高版本的所有 iPhone、iPad 和 iPod Touch 设备。

如果设备不支持 Apple iOS 10.3 或更高版本，则只能使用**旧版 *AnyConnect 4.0.05x***，它可用于运行 Apple iOS 6.0 及更高版本的所有 iPhone、iPad 和 iPod Touch 设备。旧版 AnyConnect 中的 Per App 隧道需要 Apple iOS 8.3 或更高版本。

注释 AnyConnect 在 iPod Touch 上的显示和操作与在 iPhone 上相同。

在 Apple iOS 上升级 AnyConnect

AnyConnect 的升级是通过 Apple 应用商店进行管理的。在 Apple 应用商店通知用户思科 AnyConnect 或旧版 AnyConnect 升级可用后，他们可按照此程序进行升级。

注释 不能将 AnyConnect 应用从旧版 4.0.05x 或更早版本升级到 AnyConnect 4.0.07x 或 4.6.x 及更高版本。它们是独立的应用，安装有不同的名称和图标。

在安装新版本之前，请参阅 可用于 Apple iOS 的 AnyConnect 版本，第 2 页。思科建议您删除所有旧版 AnyConnect 应用数据，删除旧版 AnyConnect 应用，然后再安装新版本。

开始之前

在升级设备之前，必须断开 AnyConnect VPN 会话（若已建立）并关闭 AnyConnect 应用（若已打开）。如果不这样做，AnyConnect 会要求您重启设备，然后才能使用新版本的 AnyConnect。

注释 使用 Apple 按需连接功能时，只有运行早于 4.0.05032 的旧版 AnyConnect 版本或早于 9.3 的 Apple iOS 版本，此功能才适用于您的环境。在更新 AnyConnect 后，为了确保正确建立按需连接 VPN 隧道，用户必须手动启动 AnyConnect 应用并建立连接。如果不这样做，在下次 iOS 系统尝试建立 VPN 隧道时，系统会显示错误消息“VPN 连接需要启动应用”(The VPN Connection requires an application to start up)。

过程

步骤 1 轻触 iOS 主页上的**应用商店**图标。

步骤 2 轻触 **AnyConnect 升级通知**。

步骤 3 阅读新功能。

步骤 4 单击**更新 (Update)**。

步骤 5 输入您的 **Apple ID 密码**。

步骤 6 单击 **OK**（**确定**）。

系统将开始执行 AnyConnect 升级。

新增功能

Apple iOS 移动设备版 AnyConnect 4.9.00518 的新功能

此版本的 AnyConnect 提供以下功能和支持更新，并解决了 Apple iOS 版 AnyConnect 4.9.00518 中已解决的问题，第 11 页 中所述的缺陷：

- 支持多个隧道 - 必须在 MDM VPN 配置文件中进行配置才能启用。有关其他信息，请参阅《Cisco AnyConnect Secure Mobility Client 管理员指南版本 4.9》中的**移动设备上的 AnyConnect** 章节。
- 在 AnyConnect 4.9 版本中，删除了某些较不安全的密码套件：
  - 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

Apple iOS 版 AnyConnect 功能表

AnyConnect 在 Apple iOS 设备上支持以下功能：

类别：功能	Apple iOS
部署和配置：	
从应用存储区安装或升级。	支持
Cisco VPN 配置文件支持（手动导入）	支持
Cisco VPN 配置文件支持（连接时导入）	支持
MDM 配置的连接条目	支持
用户配置的连接条目	支持
隧道连接：	
TLS	支持
数据报 TLS (DTLS)	支持
IPsec IKEv2 NAT-T	支持
IKEv2 - 原始 ESP	否
Suite-B（仅 IPsec）	支持
TLS 压缩	是，仅限 32 位设备
失效对等项检测	支持
隧道保持有效	支持
多个活动网络接口	否
Per App 隧道连接	是，需要 Cisco AnyConnect 4.0.09xxx 及 iOS 10.3 或更高版本。
完全隧道（OS 对于某些流量可能生成异常，例如传至应用商店的流量）。	支持
拆分隧道（拆分包括）。	支持
本地 LAN（拆分排除）。*	是
拆分 DNS	支持
自动重新连接/网络漫游	是
按需 VPN（由目标触发）	是，与 Apple iOS 按需连接兼容。

类别：功能	Apple iOS
按需 VPN（由应用触发）	是，仅当在 Per App VPN 模式下运行时。
重新生成密钥	支持
IPv4 公共传输	支持
IPv6 公共传输	支持
通过 IPv4 隧道的 IPv4	支持
通过 IPv4 隧道的 IPv6	支持
通过 IPv4 隧道的 IPv6	支持
IPv6 over IPv6 隧道	支持
默认域	支持
DNS 服务器配置	支持
私人代理支持	是
代理例外	是，但不支持通配符规范
公共代理支持	否
登录前横幅	支持
登录后横幅	支持
DSCP 保留	否
连接和断开	
VPN 负载均衡	支持
备用服务器列表	支持
最佳网关选择	否
身份验证：	
SAML 2.0	支持
客户端证书身份验证	支持
在线证书状态协议 (OCSP)	否
手动用户证书管理	支持
手动服务器证书管理	支持
SCEP 传统注册	否
SCEP 代理注册	是
自动选择证书	支持

类别：功能	Apple iOS
手动选择证书	支持
智能卡支持	否
用户名和密码	支持
令牌/质询	支持
双重身份验证	支持
组 URL（在服务器地址中指定）	支持
组选择（下拉选项）	支持
从用户证书预填充凭证	支持
保存密码	否
用户界面：	
独立 GUI	支持
本地 OS GUI	是，功能受限制
API/URI 处理程序（请参阅下文）	支持
UI 定制	否
UI 本地化	是，应用包含预先打包的语言。
用户首选项	支持
支持一键式 VPN 访问的主屏幕构件	否
AnyConnect 特定状态图标	否
移动安全评估：（AnyConnect 标识扩展，ACIDex）	
序列号或唯一 ID 检查	支持
与头端共用操作系统和 AnyConnect 版本	支持
AnyConnect NVM 支持	否
URI 处理：	
添加连接项	支持
连接到 VPN	支持
连接时预填充凭证	支持
断开 VPN	支持
导入证书	支持
导入本地化数据	支持

类别：功能	**Apple iOS**
导入 XML 客户端配置文件	支持
URI 命令的外部（用户）控件	支持
报告和故障排除：	
统计信息	支持
记录/诊断信息 (DART)	支持
认证：	
FIPS 140-2 第 1 层	支持

* 对于 iOS 设备，无论由于操作系统的实施情况如何配置 ASA，都会启用本地 LAN 访问。

自适应安全设备要求

以下功能对 ASA 有最低版本要求：

注释 请参阅您的平台的功能表，以确认这些功能在当前 AnyConnect 移动版本中的可用性。

- 您必须升级到 ASA 9.7.1.24、9.8.2.28、9.9.2.1 或更高版本，才能使用 SAML 身份验证功能。请确保客户端和服务器版本都是最新的。
- 必须升级到 ASA 9.3.2 或更高版本才能使用 TLS 1.2。
- 必须升级到 ASA 9.3.2 或更高版本才能使用 Per App VPN 隧道连接模式。
- 必须升级到 ASA 9.0 才能使用以下移动功能：
  - IPsec IKEv2 VPN
  - Suite B 加密
  - SCEP 代理
  - 移动状况
- ASA 版本 8.0(3) 和自适应安全设备管理器 (ASDM) 6.1(3) 是支持移动设备版 AnyConnect 的最低版本。

其他思科头端支持

思科 IOS 15.3(3)M+/15.2(4)M+ 支持 AnyConnect SSL 连接。

思科 ISR g2 15.2(4)M+ 支持 AnyConnect IKEv2 连接

Cisco Firepower 威胁防御版本 6.2.1 及更高版本中支持 AnyConnect SSL 和 IKEv2。

Apple iOS 版 AnyConnect 准则和限制

- CSCvs82209 - 在访问通过 SCEP 导入并需要生物特征进行访问的客户端证书时，iOS 13.3.1 和更高版本上发生“找不到有效证书”错误。iOS 13.3.1 移除了 AnyConnect Network Extension 使用 SCEP 导入证书的能力，这些证书具有要求生物特征（TouchID/FaceID/密码）才能访问的安全特性。在重新设计客户端以适应此更改之前，请使用无生物特征选项的 SCEP 部署证书。
- AnyConnect 可由用户手动配置、通过 iPhone 配置实用程序 (http://www.apple.com/support/iphone/enterprise/) 生成的 AnyConnect VPN 客户端配置文件配置或使用企业移动设备管理器配置。
- Apple iOS 设备仅支持一个 AnyConnect VPN 客户端配置文件。生成的配置内容始终与最近的配置文件匹配。例如，如果您连接到 vpn.example1.com，然后连接到 vpn.example2.com，则从 vpn.example2.com 导入的 AnyConnect VPN 客户端配置文件将替换从 vpn.example1.com 导入的配置文件。
- 此版本支持隧道保持连接功能；但是，它会降低设备电池的寿命。增加更新间隔值可以缓解此问题。
- **不兼容 DHE**

  在 AnyConnect 版本4.6 中引入 DHE 密码支持后，会导致 ASA 9.2 之前的 ASA 版本出现不兼容问题。如果您使用 ASA 9.2 之前的版本的 DHE 密码，则必须在这些 ASA 版本上禁用 DHE 密码。

Apple iOS 按需连接注意事项：

- 当设备休眠时，由于 iOS 按需逻辑而自动连接的 VPN 会话及已配置“暂停时断开连接”的 VPN 会话会断开连接。唤醒设备后，按需逻辑将根据需要重新连接 CPN 会话。
- 启动用户界面和 VPN 连接后，AnyConnect 会收集设备信息。因此，如果用户在一开始或在设备信息（例如操作系统版本）变更后，依赖于 iOS 的按需连接功能来启动连接，AnyConnect 有时候可能误报移动安全评估信息。
- 使用 Apple 按需连接功能时，只有运行早于 4.0.05032 的旧版 AnyConnect 版本或早于 9.3 的 Apple iOS 版本，此功能才适用于您的环境。在更新 AnyConnect 后，为了确保正确建立按需连接 VPN 隧道，用户必须手动启动 AnyConnect 应用并建立连接。如果不这样做，在下次 iOS 系统尝试建立 VPN 隧道时，系统会显示错误消息“VPN 连接需要启动应用”(The VPN Connection requires an application to start up)。

思科 AnyConnect 和旧版 AnyConnect 是不同的应用，其应用 ID 有所不同。因此：

- 不能将 AnyConnect 应用从旧版 4.0.05x 或更早版本升级到新版本。较新的版本是单独的应用，安装有不同的名称和图标。
- AnyConnect 的不同版本可以共存于移动设备之上，但思科不支持此操作。如果在安装了两个 AnyConnect 版本时尝试进行连接，行为可能与预期不同。请确保您的设备上只有一个 AnyConnect 应用，并且其版本适合您的设备和环境。
- 新 AnyConnect 应用版本 4.0.07072 或更高版本不能访问或使用以旧版 AnyConnect 版本 4.0.05069 及任何更早版本导入的证书。两个应用版本均可访问和使用 MDM 部署的证书。

- 如果要更新至新版本，应删除导入到旧版 AnyConnect 应用的应用数据，例如证书和配置文件。否则，它们将继续显示在系统 VPN 设置中。在卸载旧版 AnyConnect 应用之前删除应用数据。
- 当前的 MDM 配置文件不会触发新应用。EMM 供应商必须支持 VPNType (VPN)、VPNSubType (com.cisco.anyconnect) 和 ProviderType (packet-tunnel)。为了与 ISE 集成，它们必须能够将唯一标识符传递给 AnyConnect，因为 AnyConnect 在新框架中不能再访问此信息。有关如何设置此功能，请咨询您的 EMM 供应商，有些可能需要自定义 VPN 类型，另一些在发布时可能无可用的支持。

在 AnyConnect 4.6.x 及更高版本中使用新扩展框架会导致旧版 AnyConnect 4.0.05x 中的行为发生以下变化：

- 在新版本中，发送到前端的设备 ID 不再是 UDID，而且重置为出厂设置后，设备 ID 将发生变化，除非您的设备从其进行的备份中执行恢复。
- 您可以使用 MDM 部署的证书和使用 AnyConnect 中可用的某种方法导入的证书：SCEP、通过 UI 手动导入或通过 URI 处理程序导入。新版 AnyConnect 不能再使用通过邮件或识别的这些方法之外的任何其他机制导入的证书。
- 在使用 UI 创建连接条目时，用户必须接受显示的 iOS 安全消息。
- 用户创建的条目若与从 AnyConnect VPN 配置文件中下载的主机条目名称相同，当它们处于活动状态时，在断开连接前不会对其重命名。另外，断开连接后，下载的主机连接条目将出现在 UI 中，保持连接时则不会显示在 UI 中。

已知兼容性问题

在 AnyConnect 4.7. xxxxx 及更高版本中

- 当拆分排除配置中仅包含隧道 IPv6（未分配 IPv4 地址）时，连接到 ASA 的拆分隧道不起作用。

  除排除列表条目之外，所有流量均会通过隧道传输，然而拆分排除列表不被认可，所以所有 IPv6 流量都将被排除。请参阅 CSCvb80768：IPv6 拆分排除和 IPv4 全部丢弃将从隧道中排除所有 v6 流量。(RADAR 29623849)。

- 如果 AnyConnect UI 保持打开状态，并且 iOS 错误地断开了 UI 与内部 AnyConnect 扩展之间的进程间通信 (IPC)，则所有 UI 活动都会失败或响应错误。

  要解决此故障，必须关闭并重启 AnyConnect UI，由此重新建立 IPC。如果在 UI 关闭时 IPC 意外断开，则下次打开 UI 时，它会重新建立连接。请参阅 CSCvb95722：未能达到已暂停状态 (RADAR 29313229)。

- 对于按需连接，若已通过 ASA 将更新的 VPN 连接配置文件推送到客户端，则必须打开 AnyConnect UI。如果 UI 未打开，更新的配置文件将不会同步，因此不会使用所作的更改。

  遗憾的是，系统中没有标志指示用户打开 UI 来同步新配置文件（如同旧版 AnyConnect），所以更新的连接可能从未使用。目前没有解决此问题的方法。请参阅 CSCvc35923：使用按需 AC 不会通知用户必须打开 AC 来同步更新的连接配置文件 (RADAR 30173053)。

- 在受管 Per App 配置中，为 Per App 配置的应用流量在不当情况下通过用户创建（非受管）的 VPN 连接传输。

  请参阅 CSCvc36024：PerApp - 应用可通过非 PAV 完全隧道传输流量 (RADAR 29513803)。

未解决和已解决的 AnyConnect 问题

思科漏洞搜索工具 (https://tools.cisco.com/bugsearch/) 包含此版本中有关未解决和已解决的问题的详细信息。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。

Apple iOS 版 AnyConnect 4.9.00518 中已解决的问题

列出的已解决错误只是特别应用于 iOS 的错误。请注意，在桌面版本说明 (https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect49/release/notes/release-notes-anyconnect-4-9.html) 中定义的某些跨平台缺陷可能适用于移动版本。当错误被报告为已修复时，它将在具有较高AnyConnect 版本号的所有操作系统平台（包括移动操作系统）上可用。跨平台适用的 VPN、核心、NVM 和类似组件的错误将不会在后续移动版本中重复。例如，在桌面版本 4.9.00086 中解决的 VPN 组件错误不会再次列在 iOS 版本 4.9.00512 中，因为该 iOS 版本高于报告已修复错误的版本。