# 移动设备上的 AnyConnect

移动设备上的 AnyConnect 类似于 Windows、Mac 和 Linux 平台上的 AnyConnect。本章介绍设备信息、配置信息、支持信息，以及适用于移动设备的 AnyConnect 特定的其他管理任务。



# 移动设备上的 AnyConnect 操作和选项

## 关于 AnyConnect 移动 VPN 连接

此版本的 AnyConnect 安全移动客户端可用于以下移动平台：

- Android
- Apple iOS
- Chromebook
- Windows Phone

每个受支持平台的应用商店都提供了思科 AnyConnect。它在 www.cisco.com 上不可用，或无法从安全网关进行分发。

AnyConnect 移动应用仅包含核心 VPN 客户端。它们不包括网络访问管理器、终端安全评估或网络安全等其他 AnyConnect 模块。在连接 VPN 的状态下，此应用使用 AnyConnect Identify Extensions (ACIDex) 向前端提供终端安全评估信息（称为“移动终端安全评估”）。

AnyConnect VPN 连接可以通过以下方法之一建立：

- 用户手动建立。
- 用户在单击管理员提供的自动连接操作时手动建立（仅适用于 Android 和 Apple iOS）。
- 通过按需连接功能自动建立（仅适用于 Apple iOS）。

# 移动设备上的 AnyConnect VPN 连接条目

连接条目通过安全网关的完全限定域名或 IP 地址（如有需要，包括隧道组 URL）识别安全网关地址。该连接条目还可以包括其他连接属性。

AnyConnect 支持在一个移动设备上拥有多个连接条目，以便寻址不同安全网关和/或 VPN 隧道组。如果配置了多个连接条目，则用户应了解使用哪个条目来发起VPN连接。通过以下方法之一来配置连接条目：

- 用户手动配置。有关在移动设备上配置连接条目的过程，请参阅相应平台的用户指南。
- 连接条目将在用户单击管理员提供的用于配置连接条目的链接后添加。

  请参阅生成 VPN 连接条目，第 32 页可向用户提供此类连接条目配置。
- 由 Anyconnect VPN 客户端配置文件定义。

  AnyConnect VPN 客户端配置文件指定客户端行为并定义 VPN 连接条目。有关详细信息，请参阅在 AnyConnect VPN 配置文件中配置移动设备连接，第 30 页。

# 隧道型号

AnyConnect 可以在托管或未托管的自带设备 (BYOD) 环境中运行。这些环境中的 VPN 隧道只在以下一种型号中运行：

- 系统隧道型号 - VPN 连接用于传送所有数据（全隧道），或仅传送流入/流出特定域或地址的数据（拆分隧道）。此型号可在所有移动平台上使用。
- Per App VPN 模式 - VPN 连接用于移动设备上的特定应用集（仅限 Android 和 Apple iOS）。

  AnyConnect 允许管理员在前端上定义一组应用。此列表使用 ASA 自定义属性机制来定义。此列表将发送给 AnyConnect 客户端，并在设备上实施。对于所有其他应用，在隧道之外或以明文形式发送数据。

  在 Apple iOS 上，需要有受管环境才能在此型号下运行。在 Android 上，受管和非受管环境均受支持。在这两个平台上的托管环境中，移动设备管理器还必须将设备配置为传送与 AnyConnect 配置传送相同的应用列表。

AnyConnect 的运行型号由从 ASA 前端收到的配置信息决定。特别是，与连接相关的组策略或动态访问策略 (DAP) 中是否存在 Per App VPN 列表。如果 Per App VPN 列表存在，AnyConnect 会在 Per App VPN 型号下运行；如果列表不存在，AnyConnect 会在系统隧道连接型号下运行。

# 移动设备的安全网关身份验证

### 阻止不受信任的服务器

建立 VPN 连接时，AnyConnect 将使用从安全网关接收的数字证书来验证服务器的身份。如果服务器证书无效（因过期或日期无效、密钥使用错误或名称不匹配导致证书错误），或证书不受信任（证书无法由证书颁发机构验证），抑或同时出现上述两种情况，则连接将被阻止。此时将显示一条阻止消息，用户必须选择如何处理。

**阻止不受信任的服务器 (Block Untrusted Servers)** 应用设置确定 AnyConnect 在无法识别安全网关时的响应方式。默认情况下开启此保护；用户可关闭此保护，但不建议这样做。

当**阻止不受信任的服务器 (Block Untrusted Servers)** 开启后，将向用户显示一条**不受信任的 VPN 服务器 (Untrusted VPN Server)** 阻止通知，告知此安全威胁。用户可选择：

- **保持我的安全状态 (Keep Me Safe)** 以终止此连接，保持安全。
- **更改设置 (Change Settings)** 以关闭“阻止不受信任的服务器”(Block Untrusted Servers) 应用首选项，但不建议这样做。用户禁用此安全保护功能后，必须重新初始化 VPN 连接。

当**阻止不受信任的服务器 (Block Untrusted Servers)** 关闭后，将向用户显示一条**不受信任的 VPN 服务器 (Untrusted VPN Server)** 取消阻止通知，告知此安全威胁。用户可选择：

- **取消 (Cancel)** 以取消连接并保持安全。
- **继续 (Continue)** 以继续连接，但不建议这样做。
- **查看详细信息 (View Details)** 以查看证书详细信息，更直观地判断证书的可接受性。

  如果用户正在查看的证书有效但不受信任，则用户可以：

  - 选择**导入并继续 (Import and Continue)** 将服务器证书导入 AnyConnect 证书存储区供以后使用，并继续连接。

    当此证书导入 AnyConnect 存储区后，使用此数字证书与服务器建立的后续连接将被自动接受。

  - 返回上一屏幕并选择**取消 (Cancel)** 或**继续 (Continue)**。

  如果证书因任何原因无效，用户只能返回上一屏幕并选择**取消 (Cancel)** 或**继续 (Continue)**。

最安全的网络 VPN 连接配置是：开启“阻止不受信任的服务器”(Block Untrusted Servers) 设置（默认设置），在安全网关上配置有效且受信任的服务器证书，并指示移动用户始终选择“保持我的安全状态”(Keep Me Safe)。

注释 **严格证书信任**将覆盖此设置，请参阅以下说明。

### OCSP 吊销

AnyConnect 客户端支持 OCSP（在线证书状态协议）。由此，使客户端可以实时查询各个证书的状态，具体方法为：向 OCSP 响应程序发送请求，并解析 OCSP 响应，即可获得证书状况。OCSP 用于验证整个证书链。对于每个证书，访问 OCSP 响应程序设有五秒的超时间隔。

用户可以在 Anyconnect 设置活动中启用或禁用 OCSP 验证，详细信息请参阅Cisco AnyConnect Secure Mobility Client 用户指南 (Android)，版本 4.6。此外，我们还在框架中添加了新 API 验证，MDM 管理员可使用其远程控制此功能。目前支持 Samsung 和 Google MDM。

### 严格证书信任

如果用户启用此项，在验证远程安全网关时，AnyConnect 将禁用任何无法验证的证书。客户端会连接安全网关失败，而不是提示用户接受这些证书。

注释 此设置将覆盖 **阻止不受信任的服务器**。

如果未选中，客户端将提示用户接受证书。这是默认行为。

我们强烈建议您为 AnyConnect 客户端启用“严格证书信任”，原因如下：

- 随着有针对性攻击的日益增多，在本地策略中启用 Strict Certificate Turst 有助于在用户从不受信任网络（例如公共访问网络）连接时，防止受到“中间人”攻击。
- 即使您使用完全可验证且受信任的证书，默认情况下 AnyConnect 客户端也允许最终用户接受不可验证的证书。如果最终用户受到中间人攻击，他们可能会被提示接受恶意证书。要从最终用户删除此决定，请启用 Strict Certificate Turst。

# 移动设备上的客户端身份验证

要完成VPN连接，用户必须提供用户名和密码、数字证书或这两种形式的凭证进行身份验证。管理员可以定义隧道组上的身份验证方法。为了保证在移动设备上提供最佳用户体验，思科建议根据身份验证配置情况使用多个 AnyConnect 连接配置文件。您必须确定平衡用户体验和安全的最佳方法。我们的建议如下：

- 对于移动设备的基于 AAA 的身份验证隧道组，组策略应有很长的空闲超时（例如 24 小时），以让客户端在无需用户重新进行身份验证的情况下即可保持重新连接状态。
- 要实现最透明的最终用户体验，请仅使用证书进行身份验证。使用数字证书时，无需用户交互即可建立 VPN 连接。

为了使用证书对连接安全网关的移动设备进行身份验证，最终用户必须在其设备上导入证书。之后，此证书可用于自动证书选择，也可以手动将其与特定连接条目关联。可使用以下方法导入证书：

- 由用户手动导入。有关向移动设备导入证书的过程，请参阅相关的用户指南。
- 使用 SCEP。有关详细信息，请参阅配置证书注册。
- 在用户单击管理员提供的链接以导入证书之后，便会添加。

  请参阅导入证书，第 38 页为您的用户提供这种证书部署。

# 使用 SAML 进行 VPN 身份验证

可以使用与 ASA 版本 9.7.1 集成的 SAML 2.0 进行初始会话身份验证。AnyConnect 4.6 引入了一个增强版的与嵌入浏览器的 SAML 集成，以替换以前版本中的本机（外部）浏览器集成。当连接到为 SAML 身份验证配置的隧道组时，AnyConnect 会打开一个嵌入式浏览器窗口以完成身份验证过程。每次SAML 尝试都使用新的浏览器会话，而浏览器会话特定于AnyConnect（会话状态不与任何其他浏览器共享）。尽管每次 SAML 身份验证尝试在开始时都没有会话状态，但尝试之间仍保持永久 cookie。

### 平台特定的要求

您必须满足以下系统要求，才能在嵌入式浏览器中使用 SAML：

- Windows - Windows 7（和更高版本）、Internet Explorer 11（和更高版本）
- macOS - macOS 10.10（或更高版本）（AnyConnect 正式支持 macOS 10.11 或更高版本）
- Linux - WebKitGTK+ 2.1 x（或更高版本）、Red Hat 7.4（或更高版本）官方软件包和 Ubuntu 16.04（或更高版本）

### 升级过程

具有本机（外部）浏览器的 SAML 2.0 在 AnyConnect 4.4 和 AnyConnect 4.5 以及 ASA 9.7.x、9.8.x 和 9.9.1 版中可用。具有嵌入式浏览器的全新增强版本要求升级到 AnyConnect 4.6 和 ASA 9.7.1.24（或更高版本）、9.8.2.28（或更高版本）或 9.9.2.1（或更高版本）。

在升级或部署具有嵌入式浏览器 SAML 集成的前端或客户端设备时，请注意以下情况：

- 如果您先部署 *AnyConnect 4.6*，则本机（外部）浏览器和嵌入式浏览器 SAML 集成将按预期进行，无需进一步操作。AnyConnect 4.6 支持现有的或已更新的 ASA 版本，即使首先部署 AnyConnect 也是如此。
- 如果您首先部署更新的 *ASA* 版本（具有嵌入式浏览器 *SAML* 集成），则必须依次升级 AnyConnect，因为默认情况下，更新的 ASA 版本与 AnyConnect 4.6 之前版本的本机（外部）浏览器 SAML 集成不向后兼容。任何现有 AnyConnect 4.4 或 4.5 客户端的升级都在身份验证之后进行，并且要求您在隧道组配置中启用 **saml external-browser** 命令。

在使用 SAML 时，请遵循以下指导原则：

- 如果在故障转移型号下使用永远在线 VPN，则不支持外部 SAML IdP（但是，使用内部 SAML IdP，ASA 会代理到 IdP 的所有流量并且受支持）
- 在嵌入式浏览器中不允许不受信任的服务器证书。

- CLI 或 SBL 型号中不支持嵌入式浏览器 SAML 集成。
- （仅移动设备）不支持单一注销。
- 在网络浏览器中建立的 SAML 身份验证不会与 AnyConnect 共享，反之亦然。
- 根据具体配置，在使用嵌入式浏览器连接到前端时，会使用各种不同的方法。例如，尽管 AnyConnect 相比于 IPv6 连接更喜欢 IPv4 连接，但嵌入式浏览器可能更喜欢 IPv6，或反之亦然。同样，在尝试代理和收到失败后，AnyConnect 可能会回退到没有代理状态，而嵌入式浏览器在尝试代理并收到失败后可能会停止导航。
- 为了使用 SAML 功能，必须使您的 ASA 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。
- ASDM 上的 VPN 向导目前不支持 SAML 配置。
- SAML IdP *NameID* 属性确定用户的用户名，并且用于授权、记帐和 VPN 会话数据库。
- 如果您希望用户每次通过 SAML 建立 VPN 会话时，都使用身份提供程序 (IdP) 重新进行身份验证，则应该在 AnyConnect 配置文件编辑器，首选项（第 1 部分）中将 Auto Reconnect 设置为 *ReconnectAfterResume*。
- 由于具有嵌入式浏览器的 AnyConnect 会针对每个 VPN 尝试使用新的浏览器会话，因此，如果 IdP 使用 HTTP 会话 cookie 来跟踪登录状态，则用户每次都必须重新进行身份验证。这种情况下，**配置 > 远程接入 VPN > 无客户端 SSL VPN 接入 > 高级 > 单点登录服务器** > 中的强制重新验证设置对 AnyConnect 启动的 SAML 身份验证没有任何影响。

有关其他配置详细信息，请参阅相应版本（9.7 或更高版本）的思科 ASA 系列 VPN 配置指南中的使用 *SAML 2.0* 的 *SSO* 部分。

# 在移动设备上本地化

适用于 Android 和 Apple iOS 的 AnyConnect 安全移动客户端支持本地化，可根据用户的区域设置调整 AnyConnect 用户界面和消息。

### 预包装的本地化

AnyConnect 和 Apple iOS 应用包括以下语言翻译：

- 加拿大法语 (fr-ca)
- 中文（台湾地区）(zh-tw)
- 捷克语 (cs-cz)
- 荷兰语 (nl-nl)
- 法语 (fr-fr)
- 德语 (de-de)
- 匈牙利语 (hu-hu)
- 意大利语 (it-it)

- 日语 (ja-jp)
- 韩语 (ko-kr)
- 拉丁美洲西班牙语 (es-co)
- 波兰语 (pl-pl)
- 葡萄牙语（巴西）(pt-br)
- 俄语 (ru-ru)
- 简体中文 (zh-cn)
- 西班牙语 (es-es)

安装 AnyConnect 时，这些语言的本地化数据会安装到移动设备上。移动设备上指定的本地化设置决定显示的语言。AnyConnect 会依次使用语言规范和地区规范来确定最佳匹配设置。例如，安装完成后，在法语-瑞士 (fr-ch) 区域设置下，最终的显示为法语-加拿大 (fr-ca)。AnyConnect 启动后，AnyConnect 用户界面和消息会被翻译为本地语言。

### 下载的本地化

对于不在 AnyConnect 软件包中的语言，管理员向 ASA 添加要通过 AnyConnect VPN 连接下载到设备的本地化数据。

思科在 Cisco.com 的产品下载中心提供 anyconnect.po 文件，其中包括所有可本地化的 AnyConnect 字符串。AnyConnect 管理员可下载 anyconnect.po 文件，提供可用字符串的翻译，然后将文件上传到 ASA。已将 anyconnect.po 文件安装到 ASA 上的 AnyConnect 管理员可下载此更新版本。

最初，AnyConnect 用户界面和消息以安装语言向用户显示。在设备用户建立了与 ASA 的第一个连接后，AnyConnect 将比较设备的首选语言与 ASA 上的可用本地化语言。如果 AnyConnect 找到匹配的本地化文件，则下载该本地化文件。下载完成后，AnyConnect 将使用已添加到 anyconnect.po 文件的翻译字符串显示用户界面和用户消息。如果字符串未翻译，AnyConnect 将显示默认的英语字符串。

有关在 ASA 上配置本地化的说明，请参阅将转换表导入自适应安全设备。如果 ASA 不包含设备区域设置的本地化数据，将继续使用 AnyConnect 应用软件包中预装的本地化数据。

### 在移动设备上提供本地化的更多方式

本地化 AnyConnect 用户界面和消息，第 38 页可为用户提供 URI 链接。

要求移动设备用户在自己的设备上管理本地化数据。有关执行以下本地化活动的程序，请参阅相应的用户指南：

- 从指定服务器导入本地化数据。用户选择导入本地化数据并指定安全网关的地址和区域设置。根据 ISO 639-1 指定区域设置，如适用，可添加国家代码（例如，en-US、fr-CA、ar-IQ 等等）。此本地化数据用来替代预先打包的已安装本地化数据。
- 恢复默认的本地化数据。此操作将恢复使用 AnyConnect 软件包中预装的本地化数据，并删除已导入的所有本地化数据。

## 将转换表导入自适应安全设备

过程

**步骤 1** 从 www.cisco.com 下载所需的转换表。

**步骤 2** 在 ASDM 中，转到 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Customization/Localization** > **GUI Text and Messages**。

**步骤 3** 单击 **Import**。系统会显示 Import Language Localization Entry 窗口。

**步骤 4** 从下拉列表中选择适合的语言。

**步骤 5** 指定从何处导入转换表。

**步骤 6** 单击 **Import Now**。即可将此转换表部署至 AnyConnect 客户端，并将其用作首选语言。本地化将在 AnyConnect 重新启动并连接后应用。

注释 对于在非移动设备上运行的 AnyConnect，即使没有使用思科安全桌面，也必须将思科安全桌面转换表导入自适应安全设备，这样 HostScan 消息才会进行本地化。

# 移动设备上的 FIPS 和套件 B 加密

用于移动设备的 AnyConnect 包含思科通用加密模块 (C3M)，该 Cisco SSL 实现包括 FIPS 140-2 兼容的加密模块和 NSA 套件 B 加密，是下一代加密 (NGE) 算法的一部分。套件 B 加密仅适用于 IPsec VPN；FIPS 兼容加密同时适用于 IPsec 和 SSL VPN。

连接时与前端协商加密算法的使用。协商取决于VPN连接两端的功能。因此，安全网关还必须支持 FIPS 兼容加密和套件 B 加密。

用户可将 AnyConnect 配置为仅在协商期间接受 NGE 算法，方法是在 AnyConnect 应用设置中启用 **FIPS 型号 (FIPS Mode)**。当“FIPS 型号”(FIPS Mode) 处于禁用状态时，AnyConnect 也接受 VPN 连接使用非 FIPS 加密算法。

### 其他移动准则和限制

- 套件 B 加密要求 Apple iOS 5.0 或更高版本；这是支持套件 B 中使用的 ECDSA 证书的 Apple iOS 最低版本。
- 套件 B 加密要求 Android 4.0 (Ice Cream Sandwich) 或更高版本；这是支持套件 B 中使用的 ECDSA 证书的 Android 最低版本。
- 在 FIPS 型号下运行的设备与按代理方法或传统方法使用 SCEP 为移动用户提供数字证书的方式不兼容。请相应计划您的部署。

# Android 设备上的 AnyConnect

有关该版本的功能和更新，请参阅适用于 Android 的 Cisco AnyConnect Secure Mobility Client 4.x 版发行说明。

有关此版本支持的功能和设备，请参阅 AnyConnect 移动平台和功能指南。

## Android 版 AnyConnect 的准则和限制

- ASA 不对 Android 版 AnyConnect 提供分发和更新。它们仅在 Google Play 中提供。
- Android 版 AnyConnect 仅支持网络可视性模块，不支持任何其他 AnyConnect 模块。
- Android 设备仅支持一个 AnyConnect 配置文件，即，从前端接收的最后一个配置文件。但是，一个配置文件可能包含多个连接条目。
- 如果用户尝试在不受支持的设备上安装 AnyConnect，将收到弹出消息安装错误：原因未知 -8 (Installation Error: Unknown reason -8)。此消息由 Android OS 生成。
- 如果用户在其主屏幕上安装 AnyConnect 构件，那么，无论是否选择了“在启动时启动”(Launch at startup) 首选项，AnyConnect 服务都将自动启动（但不连接）。
- 使用“从客户端证书预填充”功能时，Android 版 AnyConnect 需要对扩展的 ASCII 字符进行 UTF-8 字符编码。根据 KB-890772 和 KB-888180 中的说明，如果您想使用预填充，客户端证书必须采用 UTF-8 格式。
- AnyConnect 在通过 EDGE 连接发送或接收 VPN 流量时会阻止语音呼叫，这是 EDGE 和其他早期无线电技术的固有性质所决定的。
- 一些已知的文件压缩实用程序无法成功解压缩使用 AnyConnect“发送日志”(Send Log) 按钮打包的日志捆绑包。其解决方法是使用 Windows 和 Mac OS X 上的本地实用程序解压缩 AnyConnect 日志文件。
- **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。

## Android 特定注意事项

### Android 移动终端安全评估设备 ID 生成

现在，AnyConnect 会在全新安装时或用户清除应用数据后，生成基于 Android ID 的 256 字节唯一设备 ID。此 ID 取代基于早期版本中生成的 IMEI 和 MAC 地址的传统 40 字节设备 ID。

如果安装了早期版本的 AnyConnect，则已生成传统 ID。在升级到此版本的 AnyConnect 之后，此传统 ID 继续被报告为设备唯一 ID，直到用户清除应用数据或卸载 AnyConnect。

可通过以下三种方式查看生成的设备 ID：从 AnyConnect **诊断 (Diagnostics)** > **日志记录和系统信息 (Logging and System Information)** > **系统 (System)** > **设备标识符 (Device Identifiers)** 屏幕（在初始应用启动后），在 `device_identifiers.txt` 文件中的 AnyConnect 日志内，或者在**关于 (About)** 屏幕上。

**注释** 需要更新安全网关上的 DAP 策略，才能使用新设备 ID。

`Device-ID` 的确定方式如下：

```
Device-ID = bytesToHexString(SHA256(Android-ID))
```

其中 `Android-ID` 和 `bytesToHexString` 按如下方式定义：

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

```
String bytesToHexString(byte[] sha256rawbytes){
String hashHex = null;
if (sha256rawbytes != null){
  StringBuffer sb = new StringBuffer(sha256rawbytes.length * 2);
    for (int i = 0; i < sha256rawbytes.length; i++){
    String s = Integer.toHexString(0xFF & sha256rawbytes[i]).toUpperCase();
    if (s.length() < 2) {sb.append("0");}
    sb.append(s);
    }
  hashHex = sb.toString();
  }
return hashHex; }
```

## Android 设备权限

适用于 AnyConnect 操作的 Android 清单中声明了以下权限：

| 清单权限 | 说明 |
|---|---|
| uses-permission: android.permission.ACCESS_NETWORK_STATE | 允许应用访问网络的相关信息。 |
| uses-permission: android.permission.ACCESS_WIFI_STATE | 允许应用访问 Wi-Fi 网络的相关信息。 |
| uses-permission: android.permission.BROADCAST_STICKY | 允许应用广播粘性意图。这些广播在完成后，其数据由系统保留，以便客户端可以快速检索这些数据，而不必等待下一次广播。 |
| uses-permission: android.permission.INTERNET | 允许应用打开网络套接字。 |
| uses-permission: android.permission.READ_EXTERNAL_STORAGE | 允许应用从外部存储中读取。 |
| uses-permission: android.permission.READ_LOGS | 允许应用读取低层系统日志文件。 |
| uses-permission: android.permission.READ_PHONE_STATE | 允许只读访问电话状态，包括设备的电话号码、当前的蜂窝网络信息、正在进行的任何呼叫的状态，设备上注册的任何电话帐户列表。 |

| 清单权限 | 说明 |
| --- | --- |
| uses-permission: android.permission.RECEIVE_BOOT_COMPLETED | 允许应用在系统完成启动后接收广播。 |

# 在 Chromebook 上配置 Android 版 AnyConnect

Google 最近宣布弃用所有本地 Chromebook 应用。本文档旨在帮助您从本地 Chromebook 应用迁移，并帮助您在 Chromebooks 上配置 Android 版 AnyConnect。

有关其他信息，您可以访问此 Google 文档。

### 过程

**步骤 1** 使用管理员帐户登录 Google 管理员控制台。

**步骤 2** 在 Google 管理员控制台主页上，转到**设备 > Chrome**。

**步骤 3** 单击**应用和扩展程序 > 用户和浏览器**。

**步骤 4** 如果要将设置应用于所有人，请保留顶层组织单位的选中状态。否则，应用子组织单位。

**步骤 5** 单击**添加 > 从 Google Play 添加**。

**步骤 6** 选择 AnyConnect 作为要管理的应用。

**步骤 7** 唯一的托管配置是 JSON 文件，您可以通过单击上传图标将其粘贴或上传。

### 下一步做什么

密钥在 Android 的 .apk 软件包文件中定义。唯一的必填字段为 vpn_connection_host，但如果您在推送 AnyConnect VML 配置文件，则 JSON 密钥为 vpn_connection_profile。AnyConnect 支持下一节中列出的所有托管的配置密钥。

## AnyConnect 支持的托管配置密钥

托管限制（根）

- 密钥：vpn_connection_name
- 标题：连接名称
- 类型：string
- 说明：用户友好的名称（仅用于显示）。如果未设置，则默认为 host。
- 密钥：vpn_connection_host
- 标题：主机
- 类型：string
- 说明：指向前端的 URL。此栏必填。

- 密钥：vpn_connection_profile
- 标题：协议
- 类型：choice
- 可能的值：SSL | IPsec
- 说明：VPN 隧道协议（SSL 或 IPsec）。默认为 SSL
- 密钥：vpn_connection_ipsec_auth_mode
- 标题：IPsec 身份验证模式
- 类型：choice
- 说明：（可选）当隧道协议为 IPsec 时使用的身份验证模式。默认为 EAP-AnyConnect
- 密钥：vpn_connection_ipsec_ike_identity
- 标题：IKE 标识
- 类型：string
- 说明：（可选）仅当 IPsec 身份验证模式为 EAP_GTC、EAP-Md5 或 EAP-MSCHAPv2 时适用
- 密钥：vpn_connection_ipsec_ike_identity
- 标题：IKE 标识
- 类型：string
- 说明：（可选）仅当 IPsec 身份验证模式为 EAP_GTC、EAP-MD5 或 EAP-MSCHAPv2 时适用。
- 密钥：vpn_connection_keychain_cert_alias
- 标题：密钥链证书别名
- 类型：string
- 说明：（可选）要用于此 VPN 配置的客户端证书的密钥链别名
- 密钥：vpn_connection_perapp
- 标题：Per App VPN 允许的应用
- 类型：string
- 说明：（已弃用）请使用 vpn_connection_allowed_apps。
- 密钥：vpn_connection_allowed_apps
- 标题：Per App VPN 允许的应用
- 类型：string

- 说明：（可选）指定哪些应用（Android应用软件包名称的逗号分隔列表）应建立隧道，从而启用 Per App VPN。所有其他应用都不建立隧道。此设置要求在前端上启用 Per App VPN。
- 密钥：vpn_connection_disallowed_apps
- 标题：Per App VPN 禁止的应用
- 类型：string
- 说明：（可选）指定哪些应用（Android应用软件包名称的逗号分隔列表）不应建立隧道，从而启用 Per App VPN。所有其他应用都建立隧道。此设置要求在前端上启用 Per App VPN。
- 密钥：vpn_connection_allow_bypass
- 标题：允许应用绕过 VPN 隧道
- 类型：bool
- 说明：（可选）允许应用绕过此 VPN 连接。默认情况下，此项为禁用状态。
- 密钥：vpn_setting_replace_existing_profile
- 标题：替换现有的配置文件
- 类型：bool
- 说明：（可选）仅当设置 vpn_connection_profile 时适用。指定托管配置的配置文件是否应替换客户端上已安装的任何配置文件。为避免与ASA推送的配置文件冲突，可能需要禁用此项。默认情况下，此项为启用状态。
- 密钥：vpn_setting_apply_perapp_to_profile
- 标题：对配置文件导入的配置应用 Per App 规则
- 类型：bool
- 说明：（可选）指定是否将托管配置Per-App VPN规则（如果存在）应用于从AnyConnect配置文件 XML 导入的配置。默认情况下，此项为禁用状态。
- 密钥：vpn_connection_set_active
- 标题：设为活动
- 类型：bool
- 默认值：true
- 说明：（可选）将此设置为最后一个选择的 VPN 配置（如果没有任何配置）。
- 密钥：vpn_setting_fips_mode
- 标题：FIPS 模式
- 类型：bool

- 说明：（可选）是否为 AnyConnect 启用 FIPS 模式。
- 密钥：vpn_setting_uri_external_control
- 标题：URI 外部控制
- 类型：string
- 说明：（可选）配置 URI 处理（外部控制）。有效选项为“已提示”、“已启用”和“已禁用”。
- 密钥：vpn_setting_strict_mode
- 标题：严格模式
- 类型：bool
- 说明：（可选）是否为 AnyConnect 启用严格证书信任模式。
- 密钥：vpn_setting_certificate_revocation
- 标题：证书吊销
- 类型：bool
- 说明：（可选）是否为 AnyConnect 启用 OCSP 服务器证书检查。
- 密钥：vpn_connection_profile
- 标题：AnyConnect 配置文件
- 类型：string
- 说明：（可选）要导入的 AnyConnect 配置文件（XML 格式或 XML 的 Base64 编码）
- 密钥：vpn_connection_device_id
- 标题：设备标识符
- 类型：string
- 说明：（可选）报告给前端的设备标识符。如果未设置，AnyConnect 将生成随机的永久设备标识符。
- 密钥：vpn_connection_report_hardware_id
- 标题：报告硬件标识符（MAC 地址和 IMEI）以进行 VPN 身份验证
- 类型：bool
- 说明：（可选）AnyConnect 是否应尝试向前端报告硬件标识符。默认情况下，AnyConnect 会尝试报告硬件标识符（如果可访问）。
- 密钥：vpn_setting_allowed_saved_credentials

- 标题：允许用户保存凭证
- 类型：bool
- 默认值：false
- 说明：（可选）是否允许用户保存凭证（需要屏幕锁定）。默认情况下，不允许用户保存凭证。
- 密钥：vpn_configuration_list
- 标题：VPN 连接列表
- 类型：bundle_array
- 说明：（可选）使用此项配置多个连接条目。每个条目都是 vpn_configuration 捆绑包。
- 密钥：umbrella_org_id
- 标题：Umbrella 组织 ID
- 类型：string
- 说明：客户所属的组织 ID，显示在从 Cisco Umbrella 控制板下载的配置文件中。
- 密钥：umbrella_reg_token
- 标题：Umbrella 注册令牌
- 类型：string
- 说明：向组织颁发的唯一 regToken，值显示在从 Cisco Umbrella 控制板下载的配置文件中。
- 密钥：umbrella_va_fqdns
- 标题：Umbrella VA FQDN 列表
- 类型：string
- 说明：这是连接的网络中存在的 VA 的 FQDN 列表。
- 密钥：admin_email
- 标题：管理员电子邮件地址
- 类型：string
- 说明：（可选）设置发送日志的默认管理员电子邮件地址。
- 密钥：vpn_always_on_umbrella_only
- 标题：仅对 Umbrella 保护启用永远在线 VPN 模式
- 类型：bool
- 默认值：false

- 说明：（仅适用于使用Umbrella的情况下）如果设置为true，则永远在线VPN将仅应用Umbrella保护。如果设置为 false，则永远在线 VPN 将应用于 Umbrella 和远程访问。

vpn_configuration 捆绑包的托管限制

- 密钥：vpn_name
- 标题：显示名称
- 类型：string
- 说明：用户友好的名称（仅用于显示）。如果未设置，则默认为 host。
- 密钥：vpn_host
- 标题：主机
- 类型：string
- 说明：指向前端的 URL。此栏必填。
- 密钥：vpn_protocol
- 标题：协议
- 类型：choice
- 可能的值：SSL | IPsec
- 说明：VPN 隧道协议（SSL 或 IPsec）。默认为 SSL。
- 密钥：vpn_ipsec_auth_mode
- 标题：IPsec 身份验证模式
- 类型：choice
- 可能的值：EAP-AnyConnect | EAP-GTC | EAP-MD5 | EAP-MSCHAPv2 | IKE RSA
- 说明：（可选）当隧道协议为 IPsec 时使用的身份验证模式。默认为 EAP-Connect。
- 密钥：vpn_ipsec_ike_identity
- 标题：IKE 标识
- 类型：string
- 说明：（可选）仅当IPsec身份验证模式为EAP_GTC、EAP-MD5或EAP-MSCHAPv2时适用。
- 密钥：vpn_keychain_cert_alias
- 标题：密钥链证书别名
- 类型：string

- 说明：（可选）要用于此 VPN 配置的客户端证书的密钥链别名。
- 密钥：vpn_allowed_apps
- 标题：Per App VPN 允许的应用
- 类型：string
- 说明：（可选）指定哪些应用（Android 应用软件包名称的逗号分隔列表）应建立隧道，从而启用 Per App VPN。所有其他应用都不建立隧道。此设置要求在前端上启用 Per-App VPN。
- 密钥：vpn_disallowed_apps
- 标题：Per App VPN 禁止的应用
- 类型：string
- 说明：（可选）指定哪些应用（Android 应用软件包名称的逗号分隔列表）不应建立隧道，从而启用 Per-App VPN。所有其他应用都建立隧道。此设置要求在前端上启用 Per-App VPN。
- 密钥：vpn_allow_bypass
- 标题：允许应用绕过 VPN 隧道
- 类型：bool
- 说明：（可选）允许应用绕过此 VPN 连接。默认情况下，此项为禁用状态。
- 密钥：vpn_set_active
- 标题：设为活动
- 类型：bool
- 默认值：false
- 说明：（可选）将此设置为最后一个选择的 VPN 配置（如果没有任何配置）。

# Apple iOS 设备上的 AnyConnect

有关此版本支持的功能和设备，请参阅适用于 Apple iOS 的 Cisco AnyConnect Secure Mobility Client 4.x 版发行说明。

## Apple iOS 版 AnyConnect 准则和限制

Apple iOS 版 AnyConnect 仅支持与远程 VPN 接入相关的功能，例如：

- 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。

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：

- 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。

# Apple iOS 的特别注意事项

在 Apple iOS 设备上支持 AnyConnect 时，请注意：

- 本文档中的 SCEP 参考信息仅适用于 AnyConnect SCEP，不适用于 Apple iOS SCEP。
- 由于 Apple iOS 限制，通过 VPN 推送邮件通知不起作用。但是，当隧道策略从会话中排除外部可访问的 ActiveSync 连接时，AnyConnect 可以与这些连接并行工作。

### Apple iPhone 配置实用程序

Windows 或 Mac OS X 版本的 iPhone 配置实用程序 (IPCU) 用于对 Apple iOS 设备执行配置创建和部署过程，此程序可从 Apple 公司获取。此操作可代替在安全网关上配置 AnyConnect 客户端配置文件。

受 Apple 控制的现有 IPCU GUI 不了解 AnyConnect Ipsec 功能。在 IPCU 的现有 AnyConnect GUI 内配置 IPsec VPN 连接。按照“服务器”字段中的 RFC 2996 定义，使用以下 URI 语法。此“服务器”字段语法向后兼容记录的配置 SSL VPN 连接的用法。

[**ipsec**://][<**AUTHENTICATION**> [":" <**IKE-IDENTITY**> "@"]] <**HOST**> [":" <**PORT**>] ["/" <**GROUP-URL**>]

| 参数 | 说明 |
|---|---|
| ipsec | ：表示这是 IPsec 连接。如果省略，则假设是 SSL。 |

| 参数 | 说明 |
| --- | --- |
| AUTHENTICATION | 指定 IPsec 连接的身份验证方法。如果省略，则假设是 EAP-AnyConnect。有效值为：<br>• EAP-AnyConnect<br>• EAP-GTC<br>• EAP-MD5<br>• EAP-MSCHAPv2<br>• IKE-RSA |
| IKE-IDENTITY | 当 AUTHENTICATION 设置为 EAP-GTC、EAP-MD5 或 EAP-MSCHAPv2 时，指定 IKE 标识。用于其他身份验证设置时，此参数无效。 |
| HOST | 指定服务器地址。要使用的主机名或 IP 地址。 |
| PORT | 当前忽略，包括用于与 HTTP URI 方案保持一致。 |
| GROUP=URL | 附加到服务器名称的隧道组名称。 |

示例：

```
ipsec://EAP-AnyConnect@asa-gateway.example.com
ipsec://asa-gateway.example.com
```

要仅连接到符合标准的 Cisco IOS 路由器，请使用以下资源：

```
ipsec://eap-md5:<identity>@ios-gateway.example.com
```

### 按需连接的使用准则

Apple iOS 按需连接功能允许 Safari 等其他应用启动 VPN 连接。Apple iOS 根据为设备的活动连接条目配置的规则评估应用所请求的域。仅在符合以下所有条件时，Apple iOS 才代表应用建立 VPN 连接：

- VPN 连接尚未建立。
- 与 Apple iOS 按需连接兼容的应用请求域。
- 连接条目被配置为使用有效证书。
- 已在连接条目中启用 Connect On Demand。
- Apple iOS 无法将 Never Connect 列表中的字符串与域请求匹配。
- 满足以下任一条件：Apple iOS 匹配域请求“始终连接”列表中的字符串（仅限 Apple iOS 6）。或 DNS 查询失败，并且 Apple iOS 匹配域请求“按需连接”列表中的字符串。

使用按需连接功能时，请记住以下事项：

- 使用 iOS 的按需连接功能启动 VPN 连接后，如果隧道在特定时间间隔内处于不活动状态，iOS 将断开隧道连接。有关详细信息，请参阅 Apple 的 VPN 按需连接文档。
- 如果您配置规则，我们建议使用 Connect if Needed 选项。如果 DNS 查询内部主机失败，按需连接规则将启动 VPN 连接。它需要正确的 DNS 配置，以便企业中的主机名仅使用内部 DNS 服务器进行解析。
- 对于已配置按需连接的移动设备，基于证书的身份验证隧道组设有短暂（60 秒）的空闲超时 (vpn-idle-timeout)。如果您的 VPN 会话对于应用不是至关重要且无需始终保持连接，请设置短暂的空闲超时。苹果设备在不再需要 VPN 连接时（例如，设备进入休眠型号）会将其关闭。隧道组的默认空闲超时时间为 60 分钟。
- 始终连接的行为与版本有关：
  - 在 Apple iOS 6 上，iOS 在匹配此列表中的规则时始终会启动 VPN 连接。
  - 在 iOS 7.x 上，不支持“始终连接”。当此列表中的规则匹配时，其行为与 Connect If Needed 规则相同。
  - 在以后的版本中，不使用“始终连接”。配置的规则将跳转到 Connect if Needed 列表，并按照该规则操作。
- Apple 已针对按需连接功能推出了受信任的网络检测 (TND) 增强功能。此增强功能：
  - 通过确定设备用户是否位于受信任的网络中，扩展按需连接功能。
  - 仅适用于 Wi-Fi 连接。当通过其他类型的网络连接运行时，按需连接不使用 TND 来确定是否连接 VPN。
  - 不是独立功能，不能在按需连接功能之外配置或使用。

  请联系苹果公司，了解有关 iOS 6 中 Connect On Demand 值得信赖的网络检测的详细信息。
- 集成的 Apple iOS Ipsec 客户端和 AnyConnect 均使用相同的 Apple iOS VPN 按需连接框架。

### 利用拆分隧道拆分 DNS 解析行为

ASA 拆分隧道功能允许您指定哪种流量通过 VPN 隧道，哪种流量畅通无阻。一个称为拆分 DNS 的相关功能允许您指定哪种 DNS 流量适合通过 VPN 隧道进行 DNS 解析，哪种 DNS 流量由终端 DNS 解析器处理（畅通无阻）。拆分 DNS 在 Apple iOS 设备上与在其他设备（如果也配置了拆分隧道）上的工作方式不同。Apple iOS 版本的 AnyConnect 对此命令的响应如下：

- 仅加密 split-dns 列表中所列域的 DNS 查询。

  AnyConnect 隧道仅允许对命令中指定域的 DNS 查询通过隧道。它会将所有其他 DNS 查询发送到本地 DNS 解析程序，以明文形式进行解析。例如，响应以下命令时，AnyConnect 仅通过隧道传输对 example1.com 和 example2.com 的 DNS 查询：

  ```
  hostname(config-group-policy)# split-dns value example1.com example2.com
  ```
- 仅加密 default-domain 命令中域的 DNS 查询。

如果 **split-dns none** 命令存在，且 **default-domain** 命令指定了一个域，则 AnyConnect 仅通过隧道传输该域的 DNS 查询，而将所有其他 DNS 查询畅通无阻地发送到本地 DNS 解析器进行解析。例如，响应以下命令时，AnyConnect 仅通过隧道传输 example1.com 的 DNS 查询：

```
hostname(config-group-policy)# split-dns none
hostname(config-group-policy)# default-domain value example1.com
```

- 畅通无阻地发送所有 DNS 查询。如果 **split-dns none** 和 **default-domain none** 命令存在于组策略中，或者虽然这些命令不存在于组策略中，但存在于默认组策略中，则 AnyConnect 将所有 DNS 查询畅通无阻地发送到本地 DNS 解析器进行解析。

**注释** 如果未指定 split-dns，则组策略继承存在于默认组策略中的拆分隧道域列表。要防止继承拆分隧道域列表，请使用 split-dns none 命令。

# Chrome OS 设备版 AnyConnect

有关此版本支持的功能和设备，请参阅适用于 Google Chrome 操作系统的 Cisco AnyConnect Secure Mobility Client 4.x 版发行说明。

## 在 Chrome 操作系统上使用 AnyConnect 的准则和限制

- 我们并未计划任何未来的 Chrome 操作系统版本。由于所有当前 ChromeBook 都支持 Android 应用，因此我们建议您改用 AnyConnect Android 应用。
- 当托管 Chromebook 设备（注册参加企业 Chrome 管理服务）时，AnyConnect 无法访问客户端证书：客户端证书身份验证不运行。
- 在低端 Chromebooks 上 VPN 性能受限（chromium 问题 #514341）。
- 51 或更高版本 Chrome 操作系统的 4.0.10113 或更高版 AnyConnect 支持自动重新连接（当网络接口断断续续时会重新连接 VPN 会话）。Chrome 51 及此 AC 版本发行之前，您如果丢失 Wi-Fi 连接或使设备休眠，AnyConnect 会无法自行重新连接。
- 除非使用 Chrome 操作系统 45 或更高版本，否则从安全网关收到的所有服务器证书，即使是完全受信任和有效的证书，也会被视为不可信。
- 在 Chrome 操作系统上安装或升级 AnyConnect 后，等到初始化完成后再配置 AnyConnect。AnyConnect 应用中会显示“正在初始化，请稍候…”（Initializing, please wait...）。这个过程会需要几分钟的时间。

# Windows Phone 设备上的 AnyConnect

有关此版本支持的功能和设备，请参阅适用于 Windows Phone 的 Cisco AnyConnect Secure Mobility Client 4.x 版发行说明。

## Windows 10 版和 Windows Phone 8.1 版 AnyConnect 的准则和限制

- 由于不支持 DTLS 和 IPsec/IKEv2 而导致性能受限。
- 不支持 VPN 漫游（在 WiFi 网络与 3/4G 网络之间转换）。
- AnyConnect 既不接收也不处理来自安全网关的 AnyConnect VPN 配置文件。
- 由用户断开的连接不会从前端完全断开。思科建议连接到提供短暂空闲超时的 ASA VPN 组，以便清除 ASA 上的孤立会话。
- 当移动设备用户连接到没有有效移动版许可证的ASA时，该用户将进入登录循环，即，输入凭证后，身份验证将重启，最后（经过 5 次尝试后）向用户发送一条通用错误消息：`VPN 连接失败，错误代码为 602 (The VPN connection has failed with error code 602)`。请与您的管理员联系，确保在安全网关上安装有效的移动版许可证

# 在 ASA 安全网关上配置移动设备 VPN 连接

过程

**步骤 1** 请参阅相应版本的 思科 ASA 5500-X 系列下一代防火墙配置指南，以了解桌面和移动终端的通用配置过程。对于移动设备，请注意以下方面：

| 属性 | ASDM 位置 | 例外 |
|---|---|---|
| 主页 URL | **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client > Customization** | AnyConnect 移动将忽略主页 URL 设置。身份验证成功后，您无法重定向移动客户端。 |
| AnyConnect 连接配置文件的名称和别名 | **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add / Edit** | 请勿在用于 AnyConnect 移动客户端连接的隧道组（连接配置文件）的 Name 或 Aliases 字段中使用特殊字符。使用特殊字符可能导致 AnyConnect 客户端显示错误消息：`Connect attempt has failed` after logging that it is `Unable to process response from Gateway`。 |

| 属性 | ASDM 位置 | 例外 |
| --- | --- | --- |
| Dead Peer Detection | 配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > 添加/编辑 > 高级 > AnyConnect 客户端 | 关闭服务器端的失效对等检测，因为它会阻止设备休眠。但是，客户端的失效对等项检测应保持开启，因为它使客户端可以确定隧道何时由于缺少网络连接而终止。 |
| SSL 保持连接消息 (SSL Keepalive Messages) | **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client** | 我们建议禁用这些保持连接消息，以保护移动设备的电池寿命，尤其是在启用客户端失效对等项检测的情况下。 |
| IPsec over NAT-T 保持连接消息 (IPsec over NAT-T Keepalive Messages) | 配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPsec > IKE 参数 | 必须选择**启用 IPsec over NAT-T (Enable IPsec over NAT-T)** 以使 AnyConnect IPsec 工作。启用时，默认情况下每 20 秒发送 NAT 保持连接消息，导致移动设备用电过度。<br>为了最大限度地降低对移动设备设备电量消耗的影响，我们建议您将 NAT-T Keepalive 设为最大值 3600，因为这些消息无法禁用。<br>使用 `crypto isakmp nat-traversal 3600` 命令在 ASA CLI 中指定此设置。 |

**步骤 2** 配置移动终端安全评估（也称为 AnyConnect 身份扩展，ACIDex），以根据需要接受、拒绝或限制移动连接。

请参阅思科 ASA 5500-X 系列下一代防火墙配置指南相应版本中的配置 *DAP* 中使用的终端属性程序。

**示例：**

当建立连接时，以下属性由 Apple iOS 上的 AnyConnect 发送到前端：

```
endpoint.anyconnect.clientversion="4.0.03004";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.devicetype="iPhone7,2";
endpoint.anyconnect.platformversion="9.0";
endpoint.anyconnect.deviceuniqueid="11025f84e99351e807f3583343bfec96351cb416";
```

**步骤 3** （可选） 配置 Per App VPN 隧道型号。

请参阅配置 Per App VPN，第 25 页。

如果未配置 Per App VPN 隧道型号，则 AnyConnect 应用在系统隧道型号下运行。

# 配置 Per App VPN

### 开始之前

AnyConnect Per App VPN 隧道需要：

- ASA 9.3.1 或更高版本以配置 Per App VPN 隧道。
- AnyConnect v4.0 Plus 或 Apex 许可证。

AnyConnect Per App VPN 支持以下移动平台：

- 运行 Android 5.0 (Lollipop) 或更高版本的 Android 设备。
- 运行 Apple iOS 8.3 或更高版本的 Apple iOS 设备，配置为在移动设备管理 (MDM) 解决方案中使用 Per App VPN。

### 过程

**步骤 1** 安装 Cisco AnyConnect 企业应用选择器工具，第 25 页。

**步骤 2** 确定隧道中允许的应用，第 26 页。

**步骤 3** 确定移动应用的应用 ID，第 27 页。

**步骤 4** 配置 Per App VPN，第 25 页。

**步骤 5** 使用应用程序选择器工具为您的平台指定 AnyConnect Per App VPN 策略：

- 为 Android 设备定义 Per-App VPN 策略，第 27 页
- 为 Apple iOS 设备定义 Per App VPN 策略，第 28 页

**步骤 6** 创建 Per App 定制属性，第 29 页（在 ASA 上）。

**步骤 7** 将定制属性分配到 ASA 上的策略，第 30 页。

# 安装 Cisco AnyConnect 企业应用选择器工具

应用选择器工具是一个独立应用，支持为 Android 和 Apple iOS 设备生成策略。

### 开始之前

Cisco AnyConnect 企业应用选择器需要 Java 7 或更高版本。

过程

**步骤 1** 从 Cisco.com AnyConnect 安全移动客户端 v4.x 软件中心 下载 Cisco AnyConnect 企业应用选择器工具。

**步骤 2** 如果您在策略中使用的是 Android 应用，则必须在系统中安装 Android SDK 和 Android SDK 构建工具。否则，请按如下方式安装它们。

a) 为您运行应用选择器工具所在的平台安装最新版本的 Android SDK 工具。

使用默认路径和设置为您的平台安装建议的**仅 SDK 工具**软件包，包括：安装 All Users（所有用户），以便按照所述访问软件包实体。

b) 使用 Android SDK 管理器，安装最新版本的 **Android SDK Build-tools**。

下一步做什么

**注释** 如果在应用选择器工具中收到提示，请配置对 Android 资产打包工具 **aapt** 的访问，方法是指定其安装位置 *Android SDK installation directory*\build-tools*build-tools version number*\。

# 确定隧道中允许的应用

当您支持移动设备（例如运行 Android 或 iOS 的手机）时，您可以使用移动设备管理器 (MDM) 应用微调 VPN 访问，以仅允许支持的应用使用 VPN 隧道。通过将远程访问 VPN 限制为批准的应用，您可以减少 VPN 前端的负载，也可以保护企业网络免受这些移动设备上安装的恶意应用的影响。

要使用基于每个应用的远程访问 VPN，您必须安装和配置第三方 MDM 应用。在 MDM 中，您要定义可通过 VPN 隧道使用的已批准应用的列表。说明如何配置和使用所选的第三方 MDM 不在本文档的讨论范围内。

当您使用 AnyConnect 从移动设备建立 VPN 连接时，所有流量（包括来自个人应用的流量）都通过 VPN 路由。如果您想只通过 VPN 路由公司应用，以便从 VPN 中排除非公司流量，可以使用 Per-App VPN 选择哪些应用通过 VPN 进行隧道连接。

配置 Per-App VPN 具有以下主要优点：

- 性能 - 它将 VPN 中的流量限制为需要进入企业网络的流量。因此，您可以释放 RA VPN 前端的资源。
- 保护 - 由于只允许来自批准的应用的流量，因此可保护公司隧道免受用户可能无意间在移动设备上安装的未批准恶意应用的影响。由于这些应用不包括在隧道中，因此来自这些应用的流量永远不会发送到前端。

移动终端上运行的移动设备管理器 (MDM) 在应用上强制实施 Per-App VPN 策略。

# 确定移动应用的应用 ID

我们强烈建议您在选择在用户移动设备上提供服务的移动设备管理器 (MDM) 中配置 Per-App 策略。这样可以极大简化前端配置。

如果您决定还要在前端配置允许的应用列表，则需要确定每种类型的终端上每个应用的应用 ID。

应用 ID（在 iOS 中称为捆绑包 ID）是反向 DNS 名称。您可以使用星号作为通配符。例如，*.* 表示所有应用，com.cisco.* 表示所有 Cisco 应用。

- Android - 在网络浏览器中转至 Google Play，然后选择“应用”类别。单击要允许的应用（或悬停在该应用上），然后查看 URL。应用 ID 位于 URL 中的 **id=** 参数上。例如，Facebook Messenger 的 URL 如下，因此应用 ID 是 com.facebook.orca：

  ```
  https://play.google.com/store/apps/details?id=com.facebook.orca
  ```

对于通过 Google Play 无法获得的应用（例如您自己的应用），下载一个程序包名称查看器应用以提取该应用 ID。Cisco 不为任何可用的应用背书，但这些应用之一应能够满足您的需求。

- iOS - 查找捆绑包 ID 的方式之一：

  1. 使用桌面浏览器（例如 Chrome）搜索应用名称。
  2. 在搜索结果中，查找从 Apple App Store 下载该应用的链接。例如，Facebook Messanger 的下载链接类似于 https://apps.apple.com/us/app/messenger/id454638411。
  3. 复制 **id** 字符串后面的数字。在本例中，即 **454638411**。
  4. 打开一个新的浏览器窗口，然后将该数字添加到以下 URL 的末尾：

     ```
     https://itunes.apple.com/lookup?id=
     ```

     在本例中，即为 https://itunes.apple.com/lookup?id=454638411
  5. 系统将提示您下载文本文件，该文件通常命名为 1.txt。下载文件。
  6. 在文本编辑器（例如写字板）中打开文件，然后搜索 bundleId。例如："bundleId":"com.facebook.Messenger"。在本例中，捆绑包 ID 为 com.facebook.Messenger。以此作为应用 ID。

拥有应用 ID 列表后，您可以配置策略。

# 为 Android 设备定义 Per-App VPN 策略

Per-app VPN 策略包含一组规则，其中每条规则标识数据在隧道中流动的应用。指定规则选项以在移动设备环境中更严格地标识允许的应用及其使用。您需要在 ASA 上配置某种 Per-app 策略（自定义属性），以便 Per-app 正常运行，即使已为 Per-app 配置了 MDM。Application Selector 工具使用来自应用的软件包文件 `*.apk` 的信息可设置规则选项。有关 Android 软件包的清单信息，请参阅 http://developer.android.com/guide/topics/manifest/manifest-element.html。

### 开始之前

Cisco AnyConnect 企业应用选择器需要 Java 7 或更高版本。

### 过程

**步骤 1** 启动应用选择器，并选择 **Android** 移动设备平台。

**步骤 2** 设置所需的**应用 ID (App ID)** 字段。

- 选择**从磁盘导入**，以便从本地系统存储的应用中获取特定于应用的软件包信息。

  “APP ID”字段（反式 DNS 格式的字符串）会自动填入。例如，如果选择适用于 Apple iOS 策略的 Chrome 应用，“APP ID”字段将设置为 **`com.google.chrome.ios`**。对于 Android 上的 Chrome，它将设置为 **`com.android.chrome`**。

- 或者，您也可以直接输入此特定于应用的信息。

- 使用通配符指定反向 DNS 格式，例如，指定 com.cisco.* 以通过隧道传送所有思科应用，而不是在各自的规则中列出每个应用。通配符必须是“应用 ID”(APP ID) 条目中的最后一个字符。

  在托管环境中配置 Per-app VPN 时，请确保 ASA 策略与 MDM 策略允许相同的应用通过隧道。我们建议指定 *.* 为应用 ID，以允许所有应用通过隧道，并确保 MDM 策略是隧道应用的唯一仲裁者。非 *.* 策略不受支持。

**步骤 3** （可选） 选择列出的应用，并根据需要配置更多参数。

- 最低版本 - 软件包清单属性 *android: versionCode* 中指定的所选应用的最低版本。
- 匹配证书 ID - 签署证书的应用摘要。
- Allow Shared UID - 默认值为 true。如果设置为 false，具有软件包清单中指定的 *android: sharedUserId* 属性的应用将不匹配此规则，并会被阻止访问隧道。

**步骤 4** 单击**文件 > 保存**以保存此 Per-app VPN 策略。

**步骤 5** 选择 **Policy > View Policy** 查看已定义策略的表示。

复制此字符串。此字符串将成为 ASA 上自定义属性 *perapp* 的值。

# 为 Apple iOS 设备定义 Per App VPN 策略

Apple iOS 设备上的 Per App VPN 策略完全由 MDM 设施控制。因此，AnyConnect 必须允许所有应用，而 MDM 必须配置 per app 策略来指定可通过隧道的特定应用。

### 开始之前

Cisco AnyConnect 企业应用选择器需要 Java 7 或更高版本。

过程

**步骤 1** 启动应用选择器，并选择 **Apple iOS** 移动设备平台。

**步骤 2** 将所需的 **App ID** 字段设置为 ***.***。

此设置允许所有应用通过 AnyConnect 隧道，并可确保 MDM per app 策略是隧道应用的唯一仲裁者。

**步骤 3** 单击**文件 > 保存**以保存此 Per App VPN 策略。

**步骤 4** 选择 **Policy > View Policy** 查看已定义策略的表示。

复制此字符串。此字符串将成为 ASA 上自定义属性 *perapp* 的值。

# 创建 Per App 定制属性

过程

**步骤 1** 在 ASDM 中，导航到 **Configuration > Remote Access VPN > Network (Client) Access> Advanced > AnyConnect Custom Attributes** 以配置定制属性类型。

**步骤 2** 选择 **Add** 或 **Edit** 并在 **Create / Edit Custom Attribute Type** 窗格中设置以下项：

a) 将 *perapp* 输入为类型。

类型必须是 *perapp*，因为这是 AnyConnect 客户端唯一可识别的 Per App VPN 属性类型。将此属性添加到远程访问 VPN 组配置文件会自动将隧道限制到明确标识的平台。来自所有其他应用的流量将自动从隧道中排除。

b) 输入您选择的描述。

**步骤 3** 单击 **OK** 关闭此窗格。

**步骤 4** 导航到 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names** 以配置定制属性。

**步骤 5** 选择 **Add** 或 **Edit** 并在 **Create / Edit Custom Attribute Name** 窗格中设置以下项：

a) 选择 *perapp* 属性 **Type**。

b) 输入 **Name**。此名称用于向策略分配此属性。

c) 选择 **Add**，可通过从策略工具复制 BASE64 格式并将其粘贴在此处来一个或多个值。

每个值不得超过 420 个字符。如果值超过此长度，请为其他值内容添加多个值。配置的值在发送到 AnyConnect 客户端之前会合并。

# 将定制属性分配到 ASA 上的策略

perapp 定制属性可以分配到组策略或动态访问策略。

过程

**步骤 1** 打开 ASA 上的策略：

- 对于组策略，导航到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client > Custom Attributes**。
- 对于动态访问策略，导航到 **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies Add / Edit**。在 **Access/Authorization Policy Attributes** 部分中，选择 **AnyConnect Custom Attributes** 选项卡。

**步骤 2** 单击 **Add** 或 **Edit** 添加或编辑现有属性，从而打开 **Create / Edit Custom Attribute** 窗格。

**步骤 3** 从下拉列表中选择预定义的 *perapp* 属性类型。

**步骤 4** 选择 **Select Value**，然后从下拉列表中选择预定义的值。

**步骤 5** 单击 **OK** 关闭打开的配置窗格。

# 在 AnyConnect VPN 配置文件中配置移动设备连接

AnyConnect VPN 客户端配置文件是指定客户端行为并定义 VPN 连接条目的 XML 文件。每个连接条目指定一个可访问终端设备及其他连接属性、策略和条件的安全网关。使用 AnyConnect 配置文件编辑器来创建 VPN 客户端配置文件，其中包括移动设备的主机连接条目。

用户无法修改或删除从 ASA 传输到移动设备的 VPN 配置文件中定义的连接条目。用户只能修改和删除其手动创建的连接条目。

在任一时刻，AnyConnect 在移动设备上只保留一个当前 VPN 客户端配置文件。在启动自动或手动 VPN 连接后，新的 VPN 配置文件完全取代当前配置文件。如果用户手动删除当前配置文件，则会删除此配置文件，同时删除此配置文件中定义的所有连接条目。

过程

**步骤 1** 配置基本 VPN 访问。

请参阅配置 VPN 访问，了解桌面和移动终端通用的处理以下例外的程序：

| 配置文件属性 | 例外 |
| --- | --- |
| Auto Reconnect | 对于 Apple iOS 之外的所有平台，无论自动连接如何规定，AnyConnect 移动版始终会尝试 ReconnectAfterResume。<br><br>仅 Apple iOS 支持暂停时断开连接 (Disconnect on Suspend)。当选择“暂停时断开连接”(Disconnect on Suspend) 时，AnyConnect 将断开连接并释放分配到 VPN 会话的资源。只有用户手动连接或配置了按需连接，它才会作出响应而重新连接。 |
| 本地局域网接入 | AnyConnect 移动版将忽略本地 LAN 接入设置，始终允许本地 LAN 接入，无论客户端配置文件中的设置如何。 |

**步骤 2** 配置移动特定属性：

a) 在 VPN 客户端配置文件中，选择导航窗格中的 **Server List**。
b) 选择 **Add** 将新服务器条目添加至列表，或从列表中选择服务器条目并按 **Edit** 打开 Server List Entry 对话框。
c) 配置特定于移动设备的参数（如AnyConnect 配置文件编辑器，移动设置中所述）。
d) 单击**确定**

**步骤 3** 使用以下方式之一来分发 VPN 客户端配置文件：

- 配置 ASA 以在建立 VPN 连接后将客户端配置文件上传到移动设备。

  请参阅AnyConnect 配置文件编辑器章节，了解关于如何将 VPN 客户端配置文件导入 ASA 并将其与组策略相关联的说明。

- 向用户提供 AnyConnect URI 链接以导入客户端配置文件。（仅限 Android 和 Apple iOS）

  请参阅导入 VPN 客户端配置文件，第 38 页，为您的用户提供这种部署过程。

- 让用户使用移动设备上的 **Profile Management** 来导入 AnyConnect 配置文件。（仅限 Android 和 Apple iOS）

  有关特定于设备的程序，请参阅相应的移动设备用户指南。

# 使用 URI 处理程序自动执行 AnyConnect 操作

AnyConnect 中的 URI 处理程序可让其他应用以通用资源标识符 (URI) 的形式向 AnyConnect 传递操作请求。为简化 AnyConnect 用户设置过程，请将 URI 嵌入网页或电邮消息上的链接，并且向用户提供访问说明。

### 开始之前

- AnyConnect 中的 URI 处理程序可让其他应用以通用资源标识符 (URI) 的形式向 AnyConnect 传递操作请求。

**在托管环境中：**

外部控制在启用后允许所有 URI 命令，而无需用户交互。设置提示后，用户会收到 URI 活动的通知，然后可在请求时选择允许或不允许该活动。如果您使用提示，则应该告知用户如何响应与 URI 处理相关的提示。用于在 MDM 上配置设置的密钥和 vales 包括：

密钥 - *UriExternalControl*

值 - 已启用、提示或已禁用

**注释** 在 MDM 中完成配置设置并向下推送到用户设备后，不允许用户对此设置进行更改。

**在非托管环境中：**

AnyConnect 应用中的 URI 处理默认禁用。移动设备用户通过将 **External Control** 应用设置设为 Enable 或 Prompt 来允许此功能。外部控制在启用后允许所有 URI 命令，而无需用户交互。设置提示后，用户会收到 URI 活动的通知，然后可在请求时选择允许或不允许该活动。

- 输入 URI 处理程序参数值时，必须使用 URL 编码。使用工具（例如此链接中的工具）对操作请求编码。此外，请参阅下面提供的示例。
- 在 URI 中，`%20` 代表空格、`%3A` 代表冒号 (:)、`%2F` 代表正斜线 (/)、`%40` 代表 @ 符号。
- URI 中的斜线是可选的。

向用户提供以下任何操作的说明。

# 生成 VPN 连接条目

使用此 AnyConnect URI 处理程序可简化用户生成 AnyConnect 连接条目。

**anyconnect:**[//]**create**[/]**?name=***Description***&host=***ServerAddress*[**&Parameter1=***Value***&Parameter2=***Value* ...]

**准则**

- *host* 参数是必需的。所有其他参数均可选择。在设备上执行操作时，AnyConnect 会保存您输入到与 *name* 和 *host* 相关联的连接条目的所有参数值。
- 对要添加到设备的每个连接条目使用单独的链接。不支持在单个链路中指定多个创建连接条目操作。

**参数**

- **name**- AnyConnect 主屏幕的连接列表和 AnyConnect 连接条目的 Description 字段中显示的连接条目的唯一名称。AnyConnect 仅在名称唯一时才响应。建议名称不超过 24 个字符，以确保能正常显示在连接列表中。在字段中输入文本时，使用设备上显示的键盘上的字母、数字或符号。字母区分大小写。

- **host**- 输入要连接的 ASA 的域名、IP 地址或组 URL。AnyConnect 会将此参数的值插入 AnyConnect 连接条目的“服务器地址”(Server Address) 字段中。

```
anyconnect://create/?name=SimpleExample&host=vpn.example.com
anyconnect:create?name=SimpleExample&host=vpn.example.com
```

- **protocol** protocol（可选，如果未指定，则默认为 SSL）- 用于此连接的 VPN 协议。有效值为：
  - SSL
  - IPSec

```
anyconnect:create?name=ExampleIPsec&host=vpn.company.com&protocol=IPsec
```

- **authentication** （可选，仅当协议指定为 IPsec 时适用，默认为 EAP-AnyConnect）- 用于 IPsec VPN 连接的身份验证方法。有效值为：
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA

- **ike-identity** （身份验证设置为 EAP-GTC、EAP-MD5 或 EAP-MSCAPv2 时需要）- 在 AUTHENTICATION 设置为 EAP-GTC、EAP-MD5 或 EAP-MSCHAPv2 时的 IKE 身份。用于其他身份验证设置时，此参数无效。

```
anyconnect:create?name=Description&host=vpn.company.com&protocol=IPsec
&authentication=eap-md5&ike-identity=012A4F8B29A9BCD
```

- **netroam** （可选，仅适用于 Apple iOS）- 确定是否限制在设备唤醒后或连接类型（例如 EDGE、3G 或 Wi-Fi）更改后重新连接所需的时间。此参数不影响数据漫游或使用多个移动服务运营商。有效值为：
  - true -（默认值）此选项可优化 VPN 访问。AnyConnect 在 AnyConnect 连接条目的 Network Roaming 字段中插入值 ON。如果 AnyConnect 失去连接，它将尝试建立新连接，直到成功为止。此设置让应用依赖于与 VPN 的持续连接。AnyConnect 不限制重新连接所需的时间。
  - false - 此选项可延长电池寿命。AnyConnect 将此值与 AnyConnect 连接条目的 Network Roaming 字段中的 OFF 值关联。如果 AnyConnect 失去连接，它在 20 秒内会一直尝试建立新连接，之后停止尝试。如有必要，用户或应用必须启动新的 VPN 连接。

```
anyconnect:create?name=Example%201&host=vpn.example.com&netroam=true
```

- **keychainalias** （可选） - 从系统证书存储区导入证书到 AnyConnect 证书存储区。此选项仅适用于 Android 移动平台。

  如果指定的证书不在系统存储区，系统会首先提示用户选择并安装该证书，再提示用户允许或拒绝将其复制到 AnyConnect 存储区。在移动设备上必须启用外部控制。

以下示例将创建一个名为 *SimpleExample* 的新连接条目，该条目的 IP 地址设置为 *vpn.example.com*，并分配有名为 *client* 的证书用于身份验证。

```
anyconnect://create/?name=SimpleExample&host=vpn.example.com&keychainalias=client
```

- **usecert**（可选）- 确定在建立与主机的 VPN 连接时是否使用设备上安装的数字证书。有效值为：
  - true（默认设置）- 允许建立与主机的 VPN 连接时自动选择证书。将 usecert 改为 true 而不指定 certcommonname 值，会将 Certificates 字段设为 Automatic，导致在连接时从 AnyConnect 证书存储区中选择证书。
  - false - 禁用自动选择证书。

```
anyconnect:create?name=Example%201&host=vpn.example.com&usecert=true
```

- **certcommonname**（可选，但需要 usecert 参数）- 与设备上预装的有效证书的公用名称匹配。AnyConnect 将该值插入 AnyConnect 连接条目的 Certificate 字段中。

  要查看设备上安装的此证书，请单击 **Diagnostics** > **Certificates**。您可能需要滚动才能看到主机需要的证书。单击详细信息披露按钮可查看从证书读取的 Common Name 参数及其他值。

- **useondemand**（可选，仅适用于 Apple iOS，并且要求 usecert、certcommonname 参数和以下域规范）- 确定应用（如 Safari）是否可以启动 VPN 连接。有效值为：
  - false（默认值）- 阻止应用启动 VPN 连接。使用此选项是阻止发出 DNS 请求的应用潜在触发 VPN 连接的唯一方式。AnyConnect 将此选项与 AnyConnect 连接条目的 Connect on Demand 字段中的 OFF 值相关联。
  - true - 允许应用使用 Apple iOS 启动 VPN 连接。如果将 useondemand 参数设置为 true，AnyConnect 将在 AnyConnect 连接条目的 Connect on Demand 字段中插入 ON 值。（如果 useondemand = true，则需要 domainlistalways 或 domainlistifneeded 参数）

```
anyconnect:create?name=Example%20with%20certificate&host=vpn.example.com
&netroam=true&usecert=true&certcommonname=example-ID&useondemand=true
&domainlistalways=email.example.com,pay.examplecloud.com
&domainlistnever=www.example.com&domainlistifneeded=intranet.example.com
```

- **domainlistnever**（可选，要求 useondemand = true）- 列出域以评估是否符合取消使用 Connect on Demand 功能的条件。此列表是 AnyConnect 用于评估域请求是否匹配的第一个列表。如果域请求匹配，AnyConnect 将忽略该域请求。AnyConnect 将此列表插入 AnyConnect 连接条目的 Never Connect 字段中。此列表可让您排除特定资源。例如，您可能不想通过面向公众的 Web 服务器自动进行 VPN 连接。示例值为 `www.example.com`。
- **domainlistalways**（如果 useondemand=true，则需要 domainlistalways 或 domainlistifneeded 参数）- 列出域以评估是否匹配 Connect on Demand 功能。此列表是 AnyConnect 用于评估域请求是否匹配的第二个列表。如果应用请求访问此参数指定的域之一，并且尚未进行 VPN 连接，则 Apple iOS 会尝试建立 VPN 连接。AnyConnect 会将此列表插入 AnyConnect 连接条目的 Always Connect 字段中。示例值列表是 `email.example.com,pay.examplecloud.com`。
- **domainlistifneeded**（如果 useondemand=true，则需要 domainlistalways 或 domainlistifneeded 参数）- 如果发生 DNS 错误，AnyConnect 将根据此列表评估域请求是否匹配。如果此列表中有字符串和域匹配，Apple iOS 会尝试建立 VPN 连接。AnyConnect 会将此列表插入 AnyConnect 连

接条目的 Connect If Needed 字段中。此列表最常用于对通过企业局域网无法访问的内部资源获取短时间访问权限。示例值为 `intranet.example.com`。

使用以逗号分隔的列表指定多个域。按需连接规则仅支持域名，而不支持 IP 地址。但 AnyConnect 灵活支持每个列表条目的域名格式，如下所示：

| 匹配 | 说明 | 示例条目 | 示例匹配 | 示例匹配失败 |
|---|---|---|---|---|
| 仅限准确的前缀和域名。 | 输入前缀、点和域名。 | email.example.com | email.example.com | www.example.com<br>email.1example.com<br>email.example1.com<br>email.example.org |
| 任何具有准确域名的前缀。前导点可阻止连接到以 * example.com（例如 notexample.com）结尾的主机。 | 输入一个点，后面紧跟要匹配的域名。 | .example.org | anytext.example.org | anytext.example.com<br>anytext.1example.org<br>anytext.example1.org |
| 以您指定的文本结尾的任何域名。 | 输入要匹配的域名的末尾部分。 | example.net<br>anytext. | anytext-example.net<br>anytext.example.net | anytext.example1.net<br>anytext.example.com |

# 建立 VPN 连接

使用此 AnyConnect URI 处理程序可连接到 VPN，以便用户轻松建立 VPN 连接。您还可以在 URI 中嵌入附加信息以执行以下任务：

- 预填用户名和密码
- 预填用于双重身份验证的用户名和密码
- 预填用户名和密码，并指定连接配置文件别名

此操作需要 name 或 host 参数，但允许同时使用以下语法之一：

**anyconnect:**[//]**connect**[/]**?**[**name=***Description*|**host=***ServerAddress*]
[**&Parameter1**=*Value***&Parameter2**=*value* ...]

或

**anyconnect:**[//]**connect**[/]**?name=***Description***&host=***ServerAddress*
[**&Parameter1**=*value***&Parameter2**=*value* ...]

### 指南

- 如果语句中的所有参数值与设备上 AnyConnect 连接条目中的参数值都匹配，则 AnyConnect 将使用其余参数建立连接。
- 如果 AnyConnect 无法使语句中的所有参数与连接条目中的参数匹配，并且 name 参数是唯一的参数，则它会生成一个新连接条目，然后尝试 VPN 连接。
- 仅在使用一次性密码 (OTP) 基础设施时，才应该在使用 URI 建立 VPN 连接时指定密码。

### 参数

- **name**- 连接条目的名称与在 AnyConnect 主窗口的连接列表中显示的名称相同。AnyConnect 根据 AnyConnect 连接条目的 Description 字段评估此值，如果使用前述说明在设备上创建了连接条目，则也曾调用 name。此值区分大小写。
- **host**- 输入域名、IP 地址或 ASA 的组 URL 以匹配 AnyConnect 连接条目的 Server Address 字段，如果使用前述说明在设备上生成了连接条目，则也曾调用 host。

  在 ASDM 中配置组 URL 的方法是选择 **“配置”(Configuration) >“远程访问 VPN”(Remote Access VPN) >“网络 (客户端) 访问”(Network (Client) Access) >“AnyConnect 连接配置文件”(AnyConnect Connection Profiles) >“高级”(Advanced) >“组别名/组 URL”(Group Alias/Group URL) >“组 URL”(Group-URL)**。
- **onsuccess**- 在连接成功时执行此操作。平台特定的行为：
  - 对于 Apple iOS 设备，指定在此连接转换到已连接状态时要打开的 URL，或使用 anyconnect:close 命令关闭 AnyConnect GUI。
  - 对于 Android 设备，指定在此连接转换为已连接状态或已处于已连接状态时要打开的 URL。可指定多个 onsuccess 操作。AnyConnect 始终在 Android 设备上连接成功后关闭 GUI。
- **onerror**- 连接失败时执行此操作。平台特定的行为：
  - 对于 Apple iOS 设备，指定在此连接失败时要打开的 URL，或使用 anyconnect:close 命令关闭 AnyConnect GUI。
  - 对于 Android 设备，指定在此连接失败时要打开的 URL。可指定多个 onerror 操作。AnyConnect 始终在 Android 设备上连接失败后关闭 GUI。
- **prefill_username**- 提供连接 URI 中的用户名并将其预填到连接提示中。
- **prefill_password**- 提供连接 URI 中的密码并且将其预填到连接提示中。此字段应仅用于为一次性密码配置的连接配置文件。
- **prefill_secondary_username**- 在配置为需要双重身份验证的环境中，此参数提供连接 URI 中的辅助用户名，并且将其预填到连接提示中。
- **prefill_secondary_password**- 在配置为需要双重身份验证的环境中，此参数提供连接 URI 中辅助用户名的密码，并且将其预填到连接提示中。

- **prefill_group_list**— 选择 **配置 > 远程访问 VPN > 网络 (客户端) 访问 > AnyConnect 连接配置文件 > 高级 > 组别名/组 URL > 连接别名** 可在 ASDM 中定义的连接别名。

示例

- 在组 URI 中提供连接名称和主机名或组 URL：

```
anyconnect://connect/?name=Example
```

```
anyconnect:connect?host=hr.example.com
```

```
anyconnect:connect?name=Example&host=hr.example.com
```

```
anyconnect://connect/?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 提供针对成功或失败的操作

  使用 onsuccess 或 onerror 参数可根据连接操作的结果开始打开指定的 URL：

```
anyconnect://connect?host=vpn.company.com
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

  在 Android 上可以指定多个 onsuccess 操作：

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
&onsuccess=tel:9781111111
```

  在 Apple iOS 设备上，anyconnect://close 命令可在 onsuccess 或 onerror 参数中用来关闭 AnyConnect GUI：

```
anyconnect://connect?host=vpn.company.com
&onsuccess=anyconnect%3A%2F%2Fclose
```

- 提供连接信息并在 URI 中预填用户名和密码：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
```

```
anyconnect:connect?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 为双重身份验证提供连接信息并预填用户名和密码：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_secondary_username=user2&prefill_secondary_password=password2
```

- 提供连接信息、预填用户名和密码，并指定连接配置文件别名：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_group_list=10.%20Single%20Authentication
```

# 断开 VPN 连接

使用此 AnyConnect URI 处理程序可将用户从 VPN 断开。

**anyconnect:**[//]**disconnect**[/]**&onsuccess=**URL

### 参数

onsuccess 参数仅适用于 Android 设备。指定 URL 在此连接断开或已处于断开状态时打开。

### 示例

```
anyconnect:disconnect
```

# 导入证书

使用此 URI 处理程序命令可将 PKCS12 编码的证书捆绑包导入到终端。AnyConnect 客户端使用终端上已安装的 PKCS12 编码的证书向 ASA 验证自身。仅支持 pkcs12 证书类型。

**anyconnect:**[//]**import**[/]**?type=pkcs12&uri=***http%3A%2F%2Fexample.com%2Fcertificatename.p12*

### 参数

- **type**- 仅支持 pkcs12 证书类型。
- **uri**- 在其中找到证书的 URL 编码的标识符。

### 示例

```
anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12
```

# 导入 VPN 客户端配置文件

使用此 URI 处理程序方法将客户端配置文件分发到 AnyConnect 客户端。

**anyconnect:**[//]**import**[/]**?type=profile&uri=***filename.xml*

### 示例

```
anyconnect:import?type=profile&uri=file%3A%2F%2Fsdcard%2Fprofile.xml
```

# 本地化 AnyConnect 用户界面和消息

使用此 URI 处理程序方法本地化 AnyConnect 客户端。

**anyconnect:**[//]**import**[/]**?type=localization&lang=***LanguageCode***&host=***ServerAddress*

### 参数

导入操作需要所有参数。

- **type**- 导入类型，本例中为本地化。
- **lang**- 长度为两个字符或四个字符的语言标记，表示 anyconnect.po 文件中提供的语言。例如，语言标记可能采用简化形式，fr 表示“法语”，fr-ca 表示“加拿大法语”。
- **host**- 输入 ASA 的域名或 IP 地址以匹配 AnyConnect 连接条目的 Server Address 字段。

### 示例

```
anyconnect:import?type=localization&lang=fr&host=asa.example.com
```

# 排除移动设备上的 AnyConnect 故障

### 开始之前

在移动设备上启用日志记录，并按照相应用户指南中的故障排除说明执行操作：

- Cisco AnyConnect Secure Mobility Client 用户指南 (Android)，版本 4.6
- Cisco AnyConnect Secure Mobility Client 用户指南 (Apple iOS)，版本 4.6.x
- Cisco AnyConnect Secure Mobility Client 用户指南，版本 4.1.x (Windows Phone)

如果遵循这些说明未能解决问题，请尝试以下操作：

### 过程

**步骤 1** 确定在桌面客户端或其他移动操作系统上是否发生相同的问题。

**步骤 2** 确保在 ASA 中已安装适当的许可证。

**步骤 3** 如果证书身份验证失败，请检查以下项：

a) 确保选择了正确的证书。

b) 确保设备中的客户端证书将客户端身份验证作为扩展密钥使用。

c) 确保 AnyConnect 配置文件中的证书匹配规则不会过滤掉用户选择的证书。

即便用户选择了证书，如果该证书不匹配配置文件中的过滤规则，也不会使用它进行身份验证。

d) 如果身份验证机制使用与 ASA 关联的任何记账策略，请验证用户是否能够成功进行身份验证。

e) 如果您在期望使用仅证书身份验证时看到身份验证屏幕，请配置该连接以使用组 URL 并确保没有为隧道组配置辅助身份验证。

**步骤 4** 在 Apple iOS 设备上，请检查以下事项。

a) 如果在设备唤醒后 VPN 连接未恢复，请确保网络漫游已启用。

b) 如果使用按需连接，请验证已配置仅证书身份验证和组 URL。

### 下一步做什么

如果问题仍然存在，请在客户端上启用日志记录并在ASA中启用调试日志记录。有关详细信息，请参阅合适版本的 思科 ASA 5500-X 系列下一代防火墙配置指南。