Apple iOS 版思科 AnyConnect 安全移动客户端用户指南，版本 4.0.x

Revised: October 21, 2017,

AnyConnect 用户指南

安装和启动 AnyConnect

AnyConnect 概述

Cisco AnyConnect 安全移动客户端 Apple iOS 版可提供安全无缝的企业网络远程访问。通过 AnyConnect，安装的应用可如同直接连接到企业网络一般进行通信。AnyConnect 是一款高级网络应用，可使您按照管理员的建议设置首选项、控制 AnyConnect 的操作，以及使用设备上的诊断工具和程序。

AnyConnect 可在您的企业中与移动设备管理软件配合使用。在这种情况下，请与管理员合作，确保遵守设备管理规则因为这些规则可能包括对一些已核准应用的 VPN 访问限制。您的组织可能会提供有关使用 AnyConnect Apple iOS 版的其他文档。

您的 Apple iOS 应用商店提供用于初始安装和所有升级的应用。思科自适应安全设备 (ASA) 是授权访问 VPN 的安全网关，但不支持 AnyConnect 适用于移动设备的更新。

显示帮助

如果帮助可用，AnyConnect 会在屏幕的右下角显示一个信息图标。轻触此图标可显示有关当前选项的帮助信息。

或者，轻触 **About**（关于）可显示用于访问本指南的链接。

开放式软件许可证说明

- 此产品包括 OpenSSL Project 开发的、可在 OpenSSL Toolkit 中使用的软件 (http://www.openssl.org/)。
- 此产品包括 Eric Young (eay@cryptsoft.com) 编写的加密软件。
- 此产品包括 Tim Hudson (tjh@cryptsoft.com) 编写的软件。

可用于 Apple iOS 的 AnyConnect 版本

Apple iOS 版思科 AnyConnect 目前有多个版本：

- 思科 ***AnyConnect***

  这是此新应用的初始版本。新思科 AnyConnect 是适用于 Apple iOS 的最新版本，建议使用此版本。（在试用版周期中，这个版本的 AnyConnect 命名为 *AnyConnect 2017*。）

  如果使用的是 Apple iOS 10.3 及更高版本，我们建议使用此版本。此版本使用 iOS 提供的新扩展框架来实施 VPN 及其所有功能。为了确保您已收到最新的 Apple iOS 漏洞修复，请使用最新版本。

现在 AnyConnect 4.0.07x 完全支持 Per App VPN 隧道功能。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。其编号为 4.0.07x。

- **思科旧版 *AnyConnect***

  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。

  旧版 AnyConnect 仅会更新严重的安全问题。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：

- 不能将 AnyConnect 应用从旧版 4.0.05x 或更早版本升级到新的 4.0.07x 版本。思科 AnyConnect 4.0.07x 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，发送到头端的设备 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。

支持的 Apple iOS 设备

思科 *AnyConnect 4.0.07x* 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，则仅可使用适用于运行 Apple iO 6.0 及更高版本的所有 iPhone、iPad 和 iPod Touch 设备的**旧版** ***AnyConnect 4.0.05x***。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。

安装 Apple iOS AnyConnect 应用

从 Apple 应用商店安装适用于 Apple iOS 的思科 AnyConnect 或旧版 AnyConnect 安全移动客户端。

开始之前

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。

过程

步骤 1 打开应用商店。

步骤 2 选择**搜索 (Search)**。

步骤 3 在搜索框中输入 anyconnect，然后依次轻触建议列表中的**思科 anyconnect** 或**旧版 anyconnect**。

步骤 4 轻触 **AnyConnect**。

步骤 5 轻触**免费 (Free)**，然后轻触**安装应用 (INSTALL APP)**。

步骤 6 选择**安装 (Install)**。

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，他们将按照此程序进行升级。

注释 不能将 AnyConnect 应用从旧版 4.0.05x 或更早版本升级到新的 4.0.07x 版本。思科 AnyConnect 4.0.07x 是单独的应用，使用不同的名称和图标进行安装。

在安装新版本 4.0.07xxx 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，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 点击**更新 (Update)**。

步骤 5 输入您的 **Apple ID 密码**。

步骤 6 点击 **OK**（**确定**）。
系统将开始执行 AnyConnect 升级。

启动 AnyConnect

过程

轻触 iPhone 或 iPad 主屏幕上的 AnyConnect 图标。
如果这是您在安装或升级后首次启动 AnyConnect，请选择**确认 (OK)** 启用 AnyConnect，以便此应用可以扩展您设备的虚拟专用网络 (VPN) 功能。

从 AnyConnect **主**屏幕，您可以：

- 使用 **AnyConnect VPN** 开关，建立或终止 VPN 连接。
- 识别活动连接并导航至**连接(Connections)** 窗口，以查看或选择配置的其他连接条目。
- 查看当前 VPN 连接的状态和其他**详细信息**。
- 导航到**设置 (Settings)**、**诊断 (Diagnostics)** 和**关于 (About)** 窗口。

配置 VPN 连接

AnyConnect 需要以下信息以建立 VPN 连接：

- 用于访问您的网络的安全网关的地址。

此地址在连接条目中配置。连接条目列在 AnyConnect 主屏幕上。活动的连接条目会在 AnyConnect 主屏幕上或连接列表中标识出来。VPN 连接条目可在设备上手动配置，或由企业管理员自动配置。

- 用于成功完成连接的身份验证信息。

  该信息的形式为您必须牢记的用户名和密码，或者包含在已在您的设备上配置的数字证书中。某些 VPN 连接可能同时需要这两种身份验证方法。数字证书可在设备上手动配置，或由设备管理员自动配置。

请按照管理员的指示配置您的 AnyConnect 客户端。如果您没有获得明确的说明，请与管理员联系。

配置连接条目

连接条目指定安全网关，该安全网关提供您的专用网络的访问权限以及其他连接属性。

在 AnyConnect 主屏幕中选择**连接**，以查看您的设备上已配置的条目。此处可能会列出多个连接条目，部分位于 **Per-App VPN** 标题之下。连接条目可能具有以下状态：

- 已启用 - 此连接条目由移动设备管理器启用，可用于连接。
- 活动 - 此连接即当前处于活动状态的连接，会被标记或高亮显示。
- 已连接 - 此连接条目处于活动状态，当前已连接并正在运行。
- 已断开连接 - 此连接条目处于活动状态，但目前已断开连接，没有运行。

Per-App VPN 连接条目由企业移动设备管理器配置，可能包括一个应用列表，这些应用是允许访问企业专用网络的仅有应用。

过程

连接条目可在设备上手动配置，或按以下方式自动配置：

- 手动配置。

  您必须知道网络的安全网关的地址。该地址是安全网关的域名或 IP 地址，它还可以指定您所属的组。还可以配置其他连接属性。请参阅手动添加或修改连接条目，第 7 页。

- 通过点击管理员提供的链接自动配置。

  AnyConnect URI 链接可能包括在邮件中或发布在网页上。应用首选项 **External Control**（**外部控制**）必须设置为 **Prompt**（**提示**）或 **Enable**（**启用**），才能在您的设备上使用此功能。请参阅控制 AnyConnect 的外部使用，第 16 页

- 在连接到下载了包含连接条目的 AnyConnect 客户端配置文件的安全网关后进行自动配置。请参阅管理 VPN 配置文件，第 17 页。

- 通过您企业的移动设备管理软件进行配置。可在您的设备的 General Settings（常规设置）下找到设备管理配置文件。

手动添加或修改连接条目

开始之前

注释 您能够修改您创建的连接条目，但不能完全编辑已从 AnyConnect VPN 配置文件或 iPhone Configuration Utility mobileconfig 导入的连接。

过程

步骤 1 在 AnyConnect 主屏幕中，轻触 **Connections**（**连接**）。然后选择要修改的连接或选择 **Add VPN Connection**（**添加 VPN 连接**）。
将显示基本 VPN 连接参数。可随时轻触 **Cancel**（**取消**）取消配置过程或轻触 **Save**（**保存**）保存连接条目。

步骤 2 （可选） 轻触**说明**，指定连接条目的唯一名称。
此名称显示在 AnyConnect 主屏幕的连接列表中。建议名称长度不超过 24 个字符，以确保名称正常显示在连接列表中。使用键盘上的字母、空格、数字或符号。AnyConnect 会将字母保留为您指定的大写或小写格式。

例如：Example 1。

步骤 3 轻触 **Server Address**（**服务器地址**）以输入用于连接的思科自适应安全设备的域名、IP 地址或组 URL。
例如，vpn.example.com。

步骤 4 轻触 **Advanced**（**高级**）以配置高级 VPN 连接参数。

a) （可选） 为此连接配置 **Network Roaming**（**网络漫游**）。请参阅配置网络漫游。
b) （可选） 配置此连接使用的**证书**。请参阅配置证书的使用。
c) （可选） 查看**应用规则**。
如果您的设备由企业移动设备管理软件管理，您可能会在此处找到允许访问专用网络的应用列表。如果允许且安装了应用，此处将列出它们。所有其他应用的数据流都不会使用 VPN 连接，但会在 VPN 隧道外部不受阻碍地发送和接收数据。
d) （可选） 为此连接配置**按需连接**。请参阅配置按需连接。
e) （可选） 将此连接配置为 **Connect with IPsec**（**使用 IPsec 连接**）而不是使用 SSL 连接。请参阅配置 IPsec。
a) 轻触 **Add VPN Connection**（**添加 VPN 连接**）返回到初始配置窗口。

步骤 5 轻触 **Save**（**保存**）以保留连接值。

配置网络漫游

网络漫游配置 AnyConnect 在设备唤醒或更改连接类型（如 EDGE(2G)、1xRTT(2G)、3G 或 Wi-Fi）后重新连接所花费的时间量。可以开启或关闭网络漫游：

- ON（开启）-（默认值）此选项优化 VPN 访问。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 不限制其重新连接所花费的时间。

- OFF（关闭）- 此选项优化电池寿命。如果 AnyConnect 失去连接，它会在 20 秒内尝试建立新连接，然后停止尝试。如有必要，您必须建立新 VPN 连接。

开始之前

注释

- 网络漫游仅适用于低于 iOS 8 的版本。iOS 8 及更高版本始终如同已启用网络漫游一样运行，会尝试重新建立连接，直到成功。
- 此参数不影响数据漫游或使用多个移动服务提供商。
- iPhone Configuration Utility 生成的 VPN 配置不支持网络漫游。如果在 iOS 8 或更早版本上需要网络漫游，必须手动或通过 AnyConnect VPN 配置文件配置连接条目。

过程

在**高级**连接条目配置屏幕中，轻触**网络漫游**字段中的“开启”或“关闭”。

配置证书的使用

过程

步骤 1 在**高级**连接条目配置屏幕中，轻触**证书**以显示**选择证书**屏幕。

步骤 2 轻触以下选项之一：

- **Disabled**（**禁用**）-（默认）身份验证从不使用客户端证书。
- **Automatic**（**自动**）- AnyConnect 自动选择用于身份验证的客户端证书。在这种情况下，AnyConnect 将查看所有已安装的证书、忽略那些过期证书、应用VPN客户端配置文件中定义的证书匹配条件，然后使用与条件匹配的证书进行身份验证。每次建立 VPN 连接时，都会执行此操作。
- **Certificate Name**（**证书名称**）- 如果设备上已安装证书，则选择一个要与此 VPN 连接关联的证书。

步骤 3 轻触 **Advanced**（**高级**）返回到高级配置窗口。

配置按需连接

配置按需连接功能的方法是创建规则列表，当其他应用发起网络连接时将核对这些规则。如果匹配，这些规则将产生以下按需连接行为之一：

- **Never Connect**（**从不连接**）- 当匹配此列表中的规则时，iOS 从不尝试发起 VPN 连接。此列表中的规则优先于所有其他规则。

启用按需连接功能时，AnyConnect 会自动将服务器地址添加到此列表。这可以防止当您在 Web 浏览器上访问服务器的无客户端入口时自动建立 VPN 连接。如果您不希望发生此行为，请删除此规则。

- **Connect if Needed**（需要时连接）- 仅当系统无法使用 DNS 解析地址且匹配此列表中的规则时，iOS 才会尝试发起 VPN 连接。
- **Always Connect**（始终连接） - 在 Apple iOS 6 中，当匹配此列表中的规则时，iOS 将始终尝试发起 VPN 连接。在 iOS 7.x 中，不支持“Always Connect（始终连接）”，当匹配此列表中的规则时，行为与“Connect if Needed（需要时连接）”规则产生的行为相同。在更高版本中，不使用“Always Connect（始终连接）”，配置的规则将移动到“Connect if Needed（需要时连接）”列表中，并且行为与其相同。

这些规则包括主机名 (host.example.com)、域 (.example.com) 或部分域 (.internal.example.com) 的列表，但不能包括 IP 地址 (10.0.0.1)。AnyConnect 在每个列表条目的域名格式上很灵活，具体如下：

匹配	说明	示例条目	示例匹配	示例匹配失败
完全域名匹配。	输入前缀、点和域名。	email.example.com	email.example.com	www.example.com email.1example.com email.example1.com email.example.org
离散子域到顶级域的顺序完全匹配。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 anytext.1example.org 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	anytext.anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

只有以下所有条件均符合时，Apple IOS 才会为应用建立 VPN 连接：

- VPN 连接尚未建立。
- 某个应用通过其完全限定域名（而不是 IP 地址）指定目标。
- 连接条目配置为使用有效证书，并且按需连接功能已启用。
- AnyConnect 未能将域请求与 **Never Connect**（从不连接）列表中的字符串匹配。
- 符合以下两个条件之一：

  AnyConnect 将域请求与**始终连接**列表中的字符串匹配。

  DNS 查找失败，并且 AnyConnect 将域请求与 **Connect if Needed**（需要时连接）列表中的字符串匹配。

注释 当通过 iOS 的按需连接功能发起 VPN 连接时，如果隧道在特定时间间隔内处于非活动状态（没有流量通过隧道），iOS 会断开隧道。有关详细信息，请参阅 Apple 的https://support.apple.com/en-us/HT203743文档。

开始之前

- 连接条目必须配置为使用有效证书进行身份验证，有关详细信息，请参阅配置证书的使用，第 8 页。
- 该连接条目必须由用户创建。用户不能在从 ASA 下载的连接配置文件中配置按需连接。

过程

步骤 1 在 **Advanced**（**高级**）连接条目配置屏幕中，轻触 **Connect On Demand**（**按需连接**）旁边的 ON（开启）。

步骤 2 轻触 **Domain List**（**域列表**）。

步骤 3 要添加域，请执行以下操作之一：

- 轻触 Always Connect（始终连接）、Never Connect（从不连接）或 Connect if Needed（需要时连接）部分下的 **Add Domain**（**添加域**）以向该列表添加域字符串。Domains（域）屏幕会向该列表添加一行，并显示屏幕键盘以供您输入域字符串。
- 轻触屏幕顶部的 **Edit**（**编辑**）可添加、编辑或删除域字符串。

  要将域名从一个列表移动到另一个列表，请触摸域条目右侧的三条横线图标，然后将其拖到目标列表标题下方的区域。

  要删除域名，请轻触域名左侧的红色圆圈，然后轻触域右侧的 **Delete**（**删除**）。

步骤 4 点击 **Save**（**保存**）。

配置 IPsec

过程

步骤 1 在 **Advanced**（**高级**）连接条目配置屏幕中，轻触 **Connect with IPsec**（**使用 IPsec 连接**）以对此 VPN 连接使用 IPsec 而不是 SSL。
如果选择的 VPN 连接协议为 IPsec，则会显示身份验证参数。

步骤 2 （可选） 轻触 **Authentication**（**身份验证**）并选择该 IPsec 连接的身份验证方法：

- EAP-AnyConnect（默认）
- IKE-RSA

- EAP-GTC
- EAP-MD5
- EAP-MSCHAPv2

步骤 3 轻触 **Advanced**（**高级**）返回到高级配置窗口。

如果已指定使用 EAP-GTC、EAP-MD5 或 EAP-MSCHAPv3 进行身份验证，将显示 **IKE Identity**（**IKE 标识**）参数。

步骤 4 （可选） 轻触 **IKE Identity**（**IKE 标识**）以输入所需客户端标识。该标识由管理员提供。

删除连接条目

此过程可删除手动配置的 VPN 连接条目。删除从 VPN 安全网关导入的连接条目的唯一方法是删除下载的包含连接条目的 AnyConnect 配置文件。

过程

步骤 1 在 AnyConnect 主屏幕中，轻触 VPN 连接条目右侧的详细信息披露按钮。

步骤 2 依次轻触**删除 VPN 连接**。

配置证书

关于证书

证书用于对 VPN 连接的两端进行数字识别：安全网关或服务器，以及 AnyConnect 客户端或用户。服务器证书可标识 AnyConnect 的安全网关，用户证书可标识安全网关的 AnyConnect 用户。证书从证书颁发机构 (CA) 获取并由其验证。

当建立连接时，AnyConnect 始终预期从安全网关处获得服务器证书。安全网关仅预期从 AnyConnect 处获得证书（如果其已配置进行此操作）。验证 VPN 连接的另一种方式是，预期 AnyConnect 用户手动输入凭据。事实上，安全网关可配置为使用数字证书、手动输入的凭据或二者组合来验证 AnyConnect 用户。仅证书验证允许建立 VPN 连接，同时无需用户干涉。

由管理员将证书分发并用于安全网关和您的设备。按照管理员提供的说明导入、使用，并管理服务器和 AnyConnect VPN 的用户证书。本文档中提供的关于证书和证书管理的信息和流程供您了解和参考。

AnyConnect 将用户和服务器证书存于自身的证书存储区，以便用于身份验证。在**诊断 > 证书**屏幕可管理 AnyConnect 证书存储区。

用户证书管理

为了使用数字证书对安全网关进行身份验证，必须导入和配置用于 VPN 的用户证书。

按照管理员的指示，使用以下方法之一导入用户证书：

- 导入邮件中附加的证书，第 12 页
- 从超链接导入证书，第 13 页
- 手动导入证书，第 13 页
- 导入安全网关提供的证书，第 13 页

导入后，可以将证书与特定连接条目关联，或者在建立连接进行身份验证期间自动选择证书。请参阅配置证书的使用，第 8 页。

服务器证书管理

在建立连接时，从安全网关接收到的服务器证书将自动验证 AnyConnect 连接的服务器，前提是该服务器证书必须有效且受信任。其他:

- 有效但不受信任的服务器证书将经过审核、授权，并导入到AnyConnect证书存储区。当服务器证书导入到AnyConnect存储区后，后续的使用该数字证书建立的与服务器的连接会被自动接受。
- 无效证书无法导入到 AnyConnect 存储区中。只有证书被接受，才能完成当前连接。不推荐进行此操作。

如果不再用于身份验证，AnyConnect 存储区中的服务器证书可以删除。

导入邮件中附加的证书

开始之前

您的管理员必须通过邮件向您传送用于身份验证的证书。

过程

步骤 1 轻触附件证书的图标。
Apple iOS 可识别您刚打开了证书，并会打开安装向导。

步骤 2 轻触**安装 (Install)**。

步骤 3 按照安装向导中的提示操作。

步骤 4 如果系统提示您，请输入证书的身份验证代码。

步骤 5 轻触**下一步 (Next)**。
Apple iOS 将安装证书。

从超链接导入证书

开始之前

确保 AnyConnect 设置内的**外部控制**设置为**提示**或**启用**，以允许此活动。有关详细信息，请参阅控制 AnyConnect 的外部使用，第 16 页。

您的管理员必须向您提供指向要在 iOS 设备上安装的证书位置的超链接。

过程

步骤 1 轻触管理员提供的超链接。

步骤 2 如果看到提示，请提供证书的身份验证代码，并轻触**下一步**。

Apple iOS 随即会导入证书并显示证书注册消息。

手动导入证书

开始之前

您的管理员必须向您提供证书的 URL。

过程

步骤 1 在 AnyConnect 主屏幕中，依次轻触**诊断** > **证书**。

步骤 2 轻触 **User**（**用户**）选项卡。

步骤 3 轻触**导入证书**可手动导入证书。

步骤 4 输入管理员提供的 URL。

导入安全网关提供的证书

开始之前

您的管理员必须向您提供配置的连接条目名称，以便使用 SCEP 协议分发证书。

过程

步骤 1 在 AnyConnect 主屏幕的**选择连接**区域，轻触可以将证书下载到移动设备的连接的名称。

步骤 2 轻触 AnyConnect 的**打开 (On)** 按钮。

步骤 3 如果存在，轻触 **Get Certificate**（**获取证书**），或选择已配置为将证书下载到您的移动设备的组。

步骤 4 输入管理员提供的身份验证信息。

安全网关会将证书下载到您的设备，断开 VPN 会话，并且您会收到证书注册成功的消息。

步骤 5 点击 **OK**（**确定**）。

接下来的操作

AnyConnect 现在即可自动使用证书，您也可以将其分配给特定的连接条目。有关详细信息，请参阅配置证书的使用，第 8 页。

查看和删除证书

过程

步骤 1 在 AnyConnect 主屏幕中，依次轻触**诊断 > 证书**。

步骤 2 轻触**用户**选项卡查看 AnyConnect 证书存储区的用户证书。
轻触**编辑**删除单个证书，或轻触**删除所有用户证书**删除所有用户证书。

步骤 3 轻触**服务器**选项卡查看 AnyConnect 证书存储区的服务器证书。
轻触**编辑**删除单个证书，或轻触**删除所有服务器证书**删除所有服务器证书。

建立 VPN 连接

开始之前

- 您必须有活动的 Wi-Fi 连接或已经与服务提供商连接才能连接到 VPN。
- 要发起 VPN 连接，AnyConnect 主窗口的“选择连接”下必须至少列出一个连接条目。
- 要完成 VPN 连接，您必须有安全网关所需的身份验证信息。

过程

步骤 1 在 AnyConnect 主屏幕上，轻触要使用的连接条目。

AnyConnect 将复位连接条目旁边的复选标记，并将断开当前所有 VPN 连接。

步骤 2 轻触 **AnyConnect VPN** 旁边的**开**。

步骤 3 如果需要，请使用系统管理员为您提供的凭据登录。

步骤 4 如果系统管理员指示您这样做，请轻触**获取证书 (Get Certificate)**。

步骤 5 如果需要，请轻触**连接 (Connect)**。
根据安全网关配置，AnyConnect 可能会检索连接条目并将它们添加到**连接** 列表。

VPN 图标显示在状态栏中，VPN 显示为 `Connected`。

注意 轻触 AnyConnect 主屏幕的另一个 VPN 连接即可断开当前 VPN 连接。

响应 AnyConnect 通知

响应不受信任的 VPN 服务器通知

所显示的**不受信任的 VPN 服务器**通知的类型取决于 **Block Untrusted VPN Server**（**阻止不受信任的 VPN 服务器**）应用首选项：

- 如果已启用，则显示阻止**不受信任的 VPN 服务器**！通知，请选择：
  - **Keep Me Safe**（**保证我的安全**）可保持此设置以及此阻止行为。
  - **Change Settings**（**更改设置**）可取消阻止。

    在更改 **Block Untrusted VPN Server**（**阻止不受信任的 VPN 服务器**）后，重新发起 VPN 连接。

- 如果未启用，则显示未阻止**不受信任的 VPN 服务器**！通知，请选择：

  Cancel（**取消**）可中止与不受信任服务器的 VPN 连接。

  Continue（**继续**）可与不受信任的服务器建立连接；不推荐使用此选项。

  View Details（**查看详细信息**）可查看证书详细信息并决定是否将服务器证书导入到 AnyConnect 证书存储区中以备将来接受，同时继续连接。

响应其他应用

为保护您的设备，当外部应用试图使用 AnyConnect 时，AnyConnect 将提醒您。当 AnyConnect 应用首选项 **External Control**（**外部控制**）设置为 **Prompt**（**提示**）时，会发生这种情况。

对于以下提示，请询问管理员是否轻触 **Yes**（**是**）来响应：

- Another application has requested that AnyConnect create a new connection to host.（其他应用请求 AnyConnect 创建到主机的新连接。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]
- Another application has requested that AnyConnect connect to host.（其他应用请求 AnyConnect 连接到主机。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]
- Another application has requested that AnyConnect disconnect the current connection.（其他应用请求 AnyConnect 断开当前连接。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]
- Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store.（其他应用请求 AnyConnect 将一个证书捆绑包导入到 AnyConnect 证书存储区。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]
- Another application has requested that AnyConnect import localization files.（其他应用请求 AnyConnect 导入本地化文件。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]
- Another application has requested that AnyConnect import profiles.（其他应用请求 AnyConnect 导入配置文件。）Do you want to allow this?（是否要允许此操作？）[Yes（是）|No（否）]

可选 AnyConnect 配置和管理

控制 AnyConnect 的外部使用

External Control（外部控制）应用设置指定 AnyConnect 应用如何响应外部 URI 请求。外部请求创建连接条目；连接或断开 VPN；导入客户端配置文件、证书或本地化文件。

外部请求通常由管理员通过电邮或在网页上提供。管理员将指示您使用以下值之一：

- Enabled（启用）- AnyConnect 应用自动允许所有 URI 命令。
- Disabled（禁用）- AnyConnect 应用自动禁止所有 URI 命令。
- Prompt（提示）- 每次在设备上访问 AnyConnect URI 时，AnyConnect 应用都会提示您。您可以允许或禁止 URI 请求。有关详细信息，请参阅 响应其他应用，第 15 页。

过程

步骤 1 在 AnyConnect 应用中，轻触**设置**。

步骤 2 轻触 **External Control**（**外部控制**）。

步骤 3 轻触 **Enabled**（**启用**）、**Disabled**（**禁用**）或 **Prompt**（**提示**）。

步骤 4 轻触 **Settings**（**设置**）返回到 Settings（设置）屏幕。

阻止不受信任的服务器

此应用设置确定当 AnyConnect 无法识别安全网关时是否阻止连接。默认情况下此保护处于打开状态；可以关闭此保护，但不推荐这样做。

AnyConnect 使用从服务器接收到的证书来验证其标识。如果存在由于过期或日期无效、密钥使用错误或名称不匹配而导致的证书错误，连接将被阻止。

当开启此设置时，阻止**不受信任的 VPN 服务器**！通知会提示您此安全威胁。

过程

步骤 1 在 AnyConnect 应用中，轻触**设置**。

步骤 2 轻触 **Block Untrusted Servers**（**阻止不受信任的服务器**）复选框以启用或禁用此首选项。

设置 FIPS 模式

在 FIPS 模式下，所有 VPN 连接均使用联邦信息处理标准 (FIPS) 加密算法。

开始之前

如果您需要在移动设备上启用 FIPS 模式才能连接到网络，管理员将通知您。

过程

步骤 1 在 AnyConnect 应用中，轻触**设置**。

步骤 2 轻触 **FIPS Mode**（**FIPS 模式**）以启用或禁用此首选项。

管理 VPN 配置文件

您应根据管理员提供的说明来管理设备上的 VPN 配置文件。

AnyConnect VPN 客户端配置文件为从安全网关下载的 XML 文件，它们指定客户端行为并标识 VPN 连接。VPN 客户端配置文件中的每个连接条目都指定了一个此终端设备可以接入的安全网关，以及其他连接属性、策略和限制。除设备上手动配置的 VPN 连接之外，初始化 VPN 连接时也可以选择这些连接条目。

注释 AnyConnect 一次仅在设备上保留一个 VPN 配置文件。

过程

步骤 1 在 AnyConnect 主页中，依次轻触**诊断** > **配置文件**。

步骤 2 选择:

- **导入配置文件** - 指定要导入的 VPN 配置文件的 URL。
- **删除配置文件** - 从设备中删除当前的 VPN 配置文件。

  注释 如果重新连接到同一 ASA 的域、IP 地址或组 URL，AnyConnect 将重新加载 VPN 配置文件并重新实施安全策略。
- **显示配置文件** - 在设备上显示或隐藏当前的 VPN 配置文件。

管理本地化

查看已安装的本地化数据

安装 AnyConnect 时，如果设备的指定区域设置与某个打包的语言翻译匹配，则您的移动设备将被本地化。AnyConnect 软件包中包括以下语言翻译：

- 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)

安装的语言取决于 **设置** > **通用** > **国际** > **语言**中指定的区域设置。AnyConnect 启动后，AnyConnect 用户界面和消息会立即翻译为本地语言。

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)。

过程

步骤 1 在 AnyConnect 应用中，依次轻触**诊断** > **本地化**。

步骤 2 查看您的移动设备上已安装的本地化文件列表。

指示的语言是 AnyConnect 当前正在使用的语言。

导入本地化数据

安装后，通过以下方式导入 AnyConnect 软件包不支持的语言的本地化数据：

- 点击管理员提供的已定义为导入本地化数据的超链接。

  管理员可以通过电邮或网页提供超链接，点击该超链接将导入本地化数据。此方法使用 AnyConnect URI 处理程序，这是为管理员提供的一个功能，用于简化 AnyConnect 配置和管理。

  注释 您必须在 AnyConnect 设置中将 External Control（外部控制）设置为 Prompt（提示）或 Enable（启用）以允许该 AnyConnect 活动。有关如何进行设置的信息，请参阅控制 AnyConnect 的外部使用，第 16 页。

- 连接到已被管理员配置为通过 VPN 连接提供可下载的本地化数据的安全网关。

  如果要使用此方法，管理员会通过 XML 配置文件提供相应的 VPN 连接信息或预定义的连接条目。本地化数据可通过 VPN 连接下载到您的设备并立即生效。

- 使用“AnyConnect 本地化管理活动”屏幕上的**导入本地化**选项可手动导入，如以下所述。

过程

步骤 1 在 AnyConnect 应用中，依次轻触**诊断** > **本地化**。

步骤 2 轻触 **Import Localization**（**导入本地化**）。

步骤 3 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的本地化数据。

恢复本地化数据

过程

步骤 1 在 AnyConnect 应用中，依次轻触**诊断** > **本地化**。

步骤 2 轻触 **Restore Localization**（**恢复本地化**）。

恢复使用 AnyConnect 软件包中预装的本地化数据并删除所有已导入的本地化数据。

系统将根据**设置** > **通用** > **国际** > **语言**中指定的设备区域设置选择恢复的语言。

删除 AnyConnect

过程

步骤 1 在 AnyConnect 主页中，依次轻触**诊断** > **配置文件** > **删除配置文件**。

步骤 2 （可选） 在 AnyConnect 主页中，依次轻触**诊断** > **证书** > **删除证书**。

步骤 3 返回设备主屏幕。

步骤 4 如果您将 AnyConnect 置于文件夹中，则打开该文件夹。

步骤 5 轻触并按住 AnyConnect 图标，直到其上方出现删除 (X) 图标。

步骤 6 轻触删除图标。

对 AnyConnect 进行监控和故障排除

显示 AnyConnect 版本和许可证

过程

在 AnyConnect 主屏幕中，轻触 **About**（**关于**）。

接下来的操作

轻触 **About**（关于）窗口中的链接可打开本指南的最新版本。

查看 AnyConnect 统计数据

当存在 VPN 连接时，AnyConnect 会记录统计数据。

过程

在 AnyConnect 主屏幕中，轻触 **Details**（详细信息）> **Statistics**（统计数据）。

详细统计数据包括以下值：

- 安全路由 - 目标为 0.0.0.0 和子网掩码为 0.0.0.0 的条目表示所有 VPN 流量均加密，并通过 VPN 连接发送或接收。
- 不安全路由 - 仅当 SecureRoutes.Traffic 目标下存在 0.0.0.0/0.0.0.0（由 VPN 安全网关确定，从加密连接中排除）时才显示。

查看系统信息

过程

在 AnyConnect 主屏幕中，依次轻触**诊断** > **系统信息**。

查看和管理日志消息

为了防止为设备资源增加不必要的负载，AnyConnect 默认不记录消息。仅为了故障排除目的启用日志记录。

过程

步骤 1 在 AnyConnect 主屏幕中，轻触**诊断**。

步骤 2 打开 **VPN 调试日志**以启用日志记录。

步骤 3 轻触**日志**。

步骤 4 选择：

- **消息** - 显示日志消息。滚动以查看其他消息。
- **服务** - 显示服务调试日志消息。滚动以查看其他消息。
- **应用** - 显示应用调试日志消息。滚动以查看其他消息。
- **清除日志** - 删除所有日志消息。

- **诊断** - 返回“诊断”屏幕。

发送日志消息

开始之前

您的设备上必须已配置邮件帐户，并且 **VPN 调试日志**必须设置为“打开”。

过程

步骤 1 在 AnyConnect 主屏幕中，依次轻触**诊断** > **邮件日志**。

步骤 2 描述问题和重现问题的步骤，然后轻触**发送** 。

步骤 3 选择将日志发送给**管理员**或**思科**，并使用邮件应用程序进行发送。

常见 Apple iOS 问题

本主题介绍常见问题的解决方案。如果在尝试这些解决方案后仍然存在问题，请联系您所在组织的 IT 支持部门。

我无法编辑/删除一些连接配置文件。

您的系统管理员设置的策略会影响将主机条目导入您的 AnyConnect 连接配置文件。要删除这些配置文件，请依次轻触**诊断** > 配置文件 > **清除配置文件数据**。

尝试保存或编辑配置时出错。

错误原因是一个已知的操作系统问题。Apple 正在努力解决它。作为临时解决方法，请尝试重新启动应用。

连接超时和主机无法解析。

网络连接问题、低格信号水平以及网络拥塞通常会导致超时和主机无法解析错误。如果附近有 LAN，请尝试使用您的设备设置应用首先建立与 LAN 的连接。对于超时错误，重复多次尝试通常可解决问题。

当设备从睡眠状态被唤醒时，无法重新建立 VPN 连接。

启用 VPN 连接条目中的网络漫游。如果启用网络漫游不能解决问题，请检查您的 EDGE(2G)、1xRTT(2G)、3G 或 Wi-Fi 连接。

注释 此问题预期会遇到，取决于您的组织如何配置 VPN。

基于证书的身份验证不起作用。

如果之前曾成功验证，则检查证书的有效性和到期日。请咨询您的系统管理员，确保您使用相应的证书进行连接。

Apple iOS 按需连接功能不起作用或意外连接。

确保连接与“从不连接”(Never Connect) 列表不存在规则冲突。如果该连接使用“视需要连接”(Connect If Needed) 规则，则尝试使用“始终连接”(Always Connect) 规则替代。

AnyConnect 无法建立连接，但是未显示错误消息。

仅当 AnyConnect 应用打开时才会显示消息。

存在名为 Cisco AnyConnect 的配置文件，且无法删除。

请尝试重启应用。

当我删除 AnyConnect 应用时，VPN 配置仍然出现在 Apple iOS VPN 设置中。

要删除这些配置文件，请重新安装 AnyConnect，依次轻触**诊断** > 配置文件 > **清除配置文件数据**。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此网址：http://www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

© 2015-2017 Cisco Systems, Inc. All rights reserved.

美洲总部
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

亚太区总部
Cisco Systems (USA) Pte. Ltd.
Singapore

欧洲总部
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco 在全球拥有 200 多个办事处。相关地址、电话和传真号码可见于
Cisco 位于 www.cisco.com/go/offices 上的网站。