部署 AnyConnect

开始部署前

如果您正在部署 Umbrella 漫游安全模块，系统将自动检测并删除现已安装的所有 Umbrella 漫游客户端，以防止冲突。如果现已安装的 Umbrella 漫游客户端与某项 Umbrella 服务订用相关联，会将该项服务订用自动迁移至 Umbrella 漫游安全模块，除非 OrgInfo.json 文件与配置用于网络部署或预部署的 AnyConnect 安装程序处于 Umbrella 模块目录中的同一位置。您可能希望在部署 Umbrella 漫游安全模块之前手动卸载 Umbrella 漫游客户端。

此外，如果使用 Umbrella 漫游安全模块，您还必须完成以下前提条件：

- **获得 Umbrella 漫游帐户**。Umbrella 控制面板 http://dashboard.umbrella.com 是登录页，您可在此获得操作 AnyConnect Umbrella 漫游安全模块的必要信息。您还可以使用此站点来管理对漫游客户端活动的报告。

- **从控制面板下载 OrgInfo 文件**。要为部署 AnyConnect Umbrella 漫游安全模块做好准备，请从 Umbrella 控制面板获取 OrgInfo.json 文件。单击“身份 (Identities)”菜单结构中的**漫游计算机 (Roaming Computer)**，然后单击页面左上角的 + 符号。向下滚动到 AnyConnect Umbrella 漫游安全模块并单击**模块配置文件 (Module Profile)**。

  OrgInfo.json 文件包含关于您的 Umbrella 服务订用的具体信息，可让漫游安全模块了解向哪里报告，以及需要实施哪些策略。

AnyConnect 部署概述

部署 AnyConnect 是指安装、配置和升级 AnyConnect 客户端及其相关文件。

Cisco AnyConnect Secure Mobility Client 可通过以下方法部署到远程用户：

- 预部署 - 新安装和升级可以由最终用户执行，也可以由企业软件管理系统 (SMS) 执行。
- 网络部署 - 将 AnyConnect 软件包载入头端，即 ASA 或 FTD 防火墙或者 ISE 服务器。当用户连接到防火墙或 ISE 时，则会将 AnyConnect 部署到客户端。
  - 对于新安装，用户可连接到前端以下载 AnyConnect 客户端。客户端可手动或自动安装（通过网络启动）。
  - 更新由已安装 AnyConnect 的系统上运行的 AnyConnect 完成，或者通过将用户定向至 ASA 无客户端门户完成。
- 云更新 - 在部署 Umbrella 漫游安全模块后，可以使用上述方法之一以及云更新来更新任何 AnyConnect 模块。通过云更新，可自动从 Umbrella 云基础设施获得软件升级，且更新跟踪将取决于该软件升级，而非管理员的任何操作。默认情况下，将禁用通过云更新进行自动更新。

注释 需要考虑以下有关云更新的情况：

- 只会更新当前安装的软件模块。
- 不支持定制、本地化和任何其他部署类型。
- 更新仅在登录到桌面时才会进行，如果建立了 VPN，则不会进行更新。
- 当禁用更新时，最新软件功能和更新将不可用。
- 禁用云更新对其他更新机制或设置（例如网络部署、延迟更新等）没有影响。
- 云更新将忽略装有较新、未发布的版本（例如临时版本和修补版本）AnyConnect 的设备。

部署 AnyConnect 时，您可以启用额外功能的可选模块以及用于配置 VPN 和可选功能的客户端配置文件。

有关 ASA、IOS、Microsoft Windows、Linux 和 macOS 的系统、管理和终端要求，请参阅 AnyConnect 版本说明。

注释 有些第三方应用和操作系统可能会限制 ISE 终端安全评估代理和其他进程进行必要的文件访问和权限提升。确保 AnyConnect 安装目录（在 Windows 中目录是 C:\Program Files (x86)\Cisco，在 macOS 中目录是 /opt/cisco）受信任并/或位于终端防病毒、反恶意软件、反间谍软件、防数据丢失、权限管理器或组策略对象的允许/排除/信任列表中。

决定如何安装 AnyConnect

AnyConnect 可以由 ISE 2.0（或更高版本）和 ASA 头端进行网络部署，或者进行预部署。安装 AnyConnect 最初需要管理权限。

网络部署

要使用网络部署（从含下载程序的 ASA/ISE/Umbrella 云）升级 AnyConnect 或安装额外模块，您不需要管理权限。

- 从 ASA 或 FTD 设备进行网络部署 - 用户连接到头端设备上的 AnyConnect 无客户端网络门户，然后选择下载 AnyConnect。ASA 下载 AnyConnect 下载程序。AnyConnect 下载程序下载客户端，安装客户端，并启动 VPN 连接。
- 从 ISE 进行网络部署 - 用户连接到网络访问设备 (NAD)，例如 ASA、无线控制器或交换机。NAD 授权用户，并将用户重定向至 ISE 门户。将在客户端上安装 AnyConnect 下载程序，以管理软件包提取和安装，但不会启动 VPN 连接。

预部署

要使用预部署（手动或使用 SCCM 等进行带外部署）升级 AnyConnect 或安装额外模块，您需要管理权限。

- 使用企业软件管理系统 (SMS)。
- 手动分发 AnyConnect 文件存档，以及指导用户如何安装的说明。对于 Windows，文件存档格式是 zip；对于 Mac OS X，是 DMG；对于 Linux，是 gzip。

有关系统要求和许可依赖性，请参阅《AnyConnect 安全移动客户端功能、许可证和操作系统指南》。

注释 如果您使用 AnyConnect 终端安全评估 (HostScan) 在 Mac 或 Linux 平台上执行根权限活动，我们建议您预部署 AnyConnect 终端安全评估。

确定安装 AnyConnect 所需的资源

部署 AnyConnect 需要多种类型的文件：

- AnyConnect 核心客户端，包含在 AnyConnect 软件包中。
- 支持额外功能的模块，包含在 AnyConnect 软件包中。
- 配置 AnyConnect 和额外功能的客户端配置文件，您可以创建这些配置文件。

- 如果您要定制或本地化部署，还可以使用语言文件、图像、脚本和帮助文件。
- AnyConnect ISE 终端安全评估和合规性模块 (OPSWAT)。

为 AnyConnect 准备终端

结合使用 AnyConnect 和移动宽带卡

某些 3G 卡在使用 AnyConnect 前需要执行配置步骤。例如，VZAccess Manager 有三种设置：

- 调制解调器手动连接
- 调制解调器自动连接（漫游时除外）
- 局域网适配器自动连接

如果选择**局域网适配器自动连接**，请将首选项设置为 NDIS 模式。NDIS 是“永远在线”的连接，即使在 VZAccess 管理器关闭时，您仍可保持连接状态。当 VZAccess 管理器为 AnyConnect 安装准备就绪时，它将自动连接局域网适配器显示为设备连接首选项。当检测到 AnyConnect 接口时，3G 管理器将丢弃接口并允许 AnyConnect 连接。

当您进入更高优先级的连接时（有线网络的优先级最高，WiFi 次之，最后是移动宽带），AnyConnect 将在断开旧连接之前建立新连接。

在 Windows 上将 ASA 添加到 Internet Explorer 的受信任站点列表

Active Directory 管理员可以使用组策略将 ASA 添加到 Internet Explorer 中的受信任站点列表。此过程不同于本地用户在 Internet Explorer 中添加受信任站点的方式。

过程

步骤 1 在 Windows 域服务器上，以域管理员组成员的身份登录。

步骤 2 打开 Active Directory 用户和计算机 MMC 管理单元。

步骤 3 右键单击要在其中创建组策略对象的域或组织单元，然后单击 **Properties**。

步骤 4 选择 **Group Policy** 选项卡，然后单击 **New**。

步骤 5 为新的组策略对象键入名称，并按 **Enter** 键。

步骤 6 为阻止这一新策略应用于某些用户或组，请单击 **Properties**，选择 **Security** 选项卡，添加要禁止应用此策略的用户或组，然后在“允许”列中清除**读取**和**应用组策略**复选框。单击 **OK**。

步骤 7 单击**编辑**并选择**用户配置** > **Windows 设置** > **Internet Explorer 维护** > **安全性**。

步骤 8 在右侧窗格中，右键单击 **Security Zones and Content Ratings**，然后单击 **Properties**。

步骤 9 选择 **Import the current security zones and privacy settings**。出现提示时，单击 **Continue**。

步骤 10 单击 **Modify Settings**，选择 **Trusted Sites**，然后单击 **Sites**。

步骤 11 键入要添加到受信任站点列表的安全设备的 URL，然后单击 **Add**。格式可以包含主机名 (https://vpn.mycompany.com) 或 IP 地址 (https://192.168.1.100)。它可以是精确匹配 (https://vpn.mycompany.com) 或通配符 (https://*.mycompany.com)。

步骤 12 单击 **Close**，并连续单击 **OK**，直至所有对话框都关闭。

步骤 13 留足时间让策略传播到整个域或林。

步骤 14 在 Internet 选项窗口中单击 **OK**。

阻止 Internet Explorer 中的代理更改

某些情况下，AnyConnect 会隐藏（锁定）Internet Explorer 的 Tools > Internet Options > Connections 选项卡。显示此选项卡时，可让用户设置代理信息。隐藏此选项卡可防止用户有意或无意绕过隧道。断开连接后，该选项卡的锁定设置会撤消。选项卡锁定可被应用于该选项卡的任何管理员定义的策略覆盖。在以下情况下应用锁定：

- ASA 配置指定 Connections 选项卡锁定
- ASA 配置指定专用端代理
- Windows 组策略之前锁定了 Connections 选项卡（覆盖未锁定的 ASA 组策略设置）

对于 Windows 10 版本 1703（或更高版本），除了隐藏 Internet Explorer 中的“连接”选项卡外，AnyConnect 还会隐藏（锁定）“设置”应用中的“系统代理”选项卡，以防止用户故意或无意中绕过隧道。断开连接后，该锁定会撤消。

过程

步骤 1 在 ASDM 中，转到**配置 > 远程接入 VPN > 网络 (客户端) 接入 > 组策略**。

步骤 2 选择组策略，单击 **Edit** 或 **Add** 可编辑或新增组策略。

步骤 3 在导航窗格中，转到 **Advanced** > **Browser Proxy**。系统显示 Proxy Server Policy 窗格。

步骤 4 单击 **Proxy Lockdown** 以显示更多代理设置。

步骤 5 取消选中 **Inherit** 并选择以下两个选项之一：

- **Yes**，将启用代理锁定，并在 AnyConnect 会话期间隐藏 Internet Explorer 的 Connections 选项卡。
- **No**，将禁用代理锁定，并在 AnyConnect 会话期间显示 Internet Explorer 的 Connections 选项卡。

步骤 6 单击 **OK** 保存代理服务器策略更改。

步骤 7 单击 **Apply** 保存组策略更改。

配置 AnyConnect 如何处理 Windows RDP 会话

可以将 AnyConnect 配置为允许来自 Windows RDP 会话的 VPN 连接。默认情况下，由 RDP 连接到计算机的用户无法启动使用 Cisco AnyConnect Secure Mobility Client 的 VPN 连接。下表显示来自 RDP 会话的 VPN 连接的登录和注销选项。这些选项在 VPN 客户端配置文件中配置。

首选项名称	值	在 SBL 模式下是否可用？
Windows 登录强制	• Single Local Logon（默认值）- 在整个 VPN 连接期间只允许一个本地用户登录。此外，当一个或多个远程用户登录到客户端 PC 时，本地用户可以建立 VPN 连接。此设置对通过 VPN 连接从企业网络登录的远程用户没有影响。 注释 如果为全有或全无隧道配置了 VPN 连接，则修改 VPN 连接的客户端 PC 路由表会导致远程登录断开连接。如果 VPN 连接进行了拆分隧道配置，远程登录可能会也可能不会断开连接，这取决于 VPN 连接的路由配置。 • Single Logon - 在整个 VPN 连接期间只允许一个用户登录。如果通过本地或远程登录的用户不止一个，则在建立 VPN 连接时，将不允许该连接。如果 VPN 连接期间有第二个用户通过本地或远程登录，则 VPN 连接将终止。由于在 VPN 连接期间不允许进行其他登录，所以无法通过 VPN 连接进行远程登录。 注释 不支持多个用户同时登录。	支持
Windows VPN Establishment	• Local Users Only（默认值）- 阻止远程登录用户建立 VPN 连接。此功能与 AnyConnect 早期版本中的功能相同。 • Allow Remote Users - 允许远程用户建立 VPN 连接。但是，如果所配置的 VPN 连接路由导致远程用户断开连接，则 VPN 连接会终止，以允许远程用户重新获得对客户端 PC 的访问权限。如果远程用户想要断开其远程登录会话而不终止 VPN 连接，则必须在 VPN 建立后等待 90 秒钟。	不支持

有关其他 VPN 会话连接选项，请参阅 AnyConnect VPN 连接选项。

配置 AnyConnect 如何处理 Linux SSH 会话

可以将 AnyConnect 配置为允许来自 Linux SSH 会话的 VPN 连接。默认情况下，由 SSH 连接到计算机的用户无法启动使用 Cisco AnyConnect Secure Mobility Client 的 VPN 连接。下表显示来自 SSH 会话的 VPN 连接的登录和注销选项。这些选项在 VPN 客户端配置文件中配置。

Linux 登录实施 — 单点本地登录（默认值）：在整个 VPN 连接期间只允许一个本地用户登录。此外，当一个或多个远程用户登录到客户端 PC 时，本地用户可以建立 VPN 连接。此设置对通过 VPN 连接从企业网络登录的远程用户没有影响。

注释 如果为全有或全无隧道配置了 VPN 连接，则修改 VPN 连接的客户端 PC 路由表会导致远程登录断开连接。如果 VPN 连接进行了拆分隧道配置，远程登录可能会也可能不会断开连接，这取决于 VPN 连接的路由配置。

单点登录—在整个 VPN 连接期间仅允许一个用户登录。如果通过本地或远程登录的用户不止一个，则在建立 VPN 连接时，将不允许该连接。如果 VPN 连接期间有第二个用户通过本地或远程登录，则 VPN 连接将终止。由于在 VPN 连接期间不允许进行其他登录，所以无法通过 VPN 连接进行远程登录。

Linux VPN 建立 —

- Local Users Only（默认值）- 阻止远程登录用户建立 VPN 连接。
- Allow Remote Users - 允许远程用户建立 VPN 连接。

有关其他 VPN 会话连接选项，请参阅 AnyConnect VPN 连接选项。

Windows 上仅使用 DES 的 SSL 加密

默认情况下，Windows 不支持 DES SSL 加密。如果在 ASA 上配置仅使用 DES，AnyConnect 连接将失败。由于很难将这些操作系统配置为使用 DES，因此建议不要将 ASA 配置为仅使用 DES 的 SSL 加密。

在 Linux 上使用 NVM

在 Linux 上使用 NVM 之前，必须设置内核驱动程序框架 (KDF)。您可以选择预构建 AnyConnect 内核模块或基于目标构建驱动程序。如果您选择基于目标构建，则无需任何操作；在部署或重新引导期间会自动处理构建。

构建 AnyConnect 内核模块的前提条件

准备目标设备：

- 确保已安装 GNU Make Utility。
- 安装内核报头软件包：
  - 对于 RHEL，请安装软件包 **kernel-devel-$(uname -r)**，例如 kernel-devel-2.6.32-642.13.1.el6.x86_64。
  - 对于 Ubuntu，请安装软件包 **linux-headers-$(uname -r)**，例如 linux-headers-4.2.0-27-generic。

- 确保已安装 GCC 编译器。已安装 GCC 编译器的 *major.minor* 版本应与用来构建内核的 GCC 版本相匹配。您可在 /proc/version 文件中对其进行验证。

将 NVM 与预构建的 AnyConnect Linux 内核模块打包在一起

开始之前

完成构建 AnyConnect 内核模块的前提条件，第 7 页中的前提条件。

注释 在启用了安全访问的设备上不支持 NVM。

AnyConnect NVM 可以通过预构建的 AnyConnect Linux 内核模块进行打包，因此您不需要在每个目标设备上建立它，尤其是当目标设备具有相同的操作系统内核版本时。如果您决定不使用预构建选项，则可以在目标上使用，这在部署或重新引导期间自动发生，无需管理员输入。或者，如果您的部署在所有终端上没有内核先决条件，可以使用预构建选项。

注释 预构建的 AnyConnect Linux 内核模块不支持 Web 部署。

过程

步骤 1 提取 AnyConnect 预部署软件包：anyconnect-linux64-<版本>-predeploy-k9.tar.gz。

步骤 2 导航到 nvm 目录。

步骤 3 调用脚本 **$sudo ./build_and_package_ac_ko.sh**。

在运行脚本后，将创建 anyconnect-linux64-<版本>**-ac_kdf_ko-k9.tar.gz**，其包括 AnyConnect Linux 内核模块版本。在启用安全启动的系统上，使用安全启动所允许的专用密钥对模块进行签名。此文件仅可用于预部署。

下一步做什么

升级目标设备的操作系统内核时，必须通过更新的 Linux 内核模块重新部署 AnyConnect NVM。

预部署 AnyConnect

可使用 SMS 预部署 AnyConnect，方法是手动为最终用户分发要安装的文件或向用户提供 AnyConnect 文件存档以供连接。

当创建文件存档以安装 AnyConnect 时，存档的目录结构必须与客户端上安装的文件的目录结构一致，如以下章节所述：预部署 AnyConnect 配置文件的位置，第 11 页

开始之前

- 如果手动部署VPN配置文件，还必须将配置文件上传到头端。当客户端系统连接时，AnyConnect会验证客户端上的配置文件是否与头端上的配置文件匹配。如果已禁用配置文件更新，并且头端上的配置文件与客户端上的配置文件不同，则手动部署的配置文件将不起作用。
- 如果手动部署 AnyConnect ISE 终端安全评估配置文件，您还必须将该文件上传到 ISE。
- 如果您使用的是克隆虚拟机，请参考 克隆虚拟机配合使用 AnyConnect 指南（仅限 Windows），第 12 页。

过程

步骤 1 下载 AnyConnect 预部署软件包。

用于预部署的 AnyConnect 文件在 cisco.com 上提供。

操作系统	**AnyConnect 预部署软件包名称**
Windows 的 ISE 安全评估代理	anyconnect-win-版本-predeploy-k9.zip
macOS	anyconnect-macos-*version*-predeploy-k9.dmg
Linux（64位）	anyconnect-linux64-版本-predeploy-k9.tar.gz

Umbrella 漫游安全模块不可用于 Linux 操作系统。

步骤 2 创建客户端配置文件：某些模块和功能需要客户端配置文件。

以下模块需要客户端配置文件：

- AnyConnect VPN
- 思科 AnyConnect 网络访问管理器
- AnyConnect 网络安全
- AnyConnect ISE 终端安全评估
- AnyConnect AMP 启用程序
- 网络可视性模块
- Umbrella 漫游安全模块

以下模块不需要 AnyConnect 客户端配置文件：

- AnyConnect VPN 登录前开始
- AnyConnect 诊断和报告工具
- AnyConnect 终端安全评估

- AnyConnect 客户体验反馈

可在 ASDM 中创建客户端配置文件，并将这些文件复制到您的 PC。或者，您可以使用 Windows PC 上的独立配置文件编辑器。有关 Windows 独立编辑器的详细信息，请参阅关于配置文件编辑器。

步骤 3 或者定制和本地化 AnyConnect 客户端和安装程序。

步骤 4 准备分发的文件。这些文件的目录结构在预部署 AnyConnect 配置文件的位置中进行了描述。

步骤 5 创建 AnyConnect 安装所需的所有文件后，可将它们分发在一个存档文件中，或将这些文件复制到客户端。确保您计划连接到的头端（ASA 和 ISE）上也有相同的 AnyConnect 文件。

用于预部署和网络部署的 AnyConnect 模块可执行文件

下表列出了在将 Umbrella 漫游安全模块、网络访问管理器、AMP 启用程序、ISE 终端安全评估、网络安全及网络可视性模块客户端预部署或网络部署到 Windows 计算机时终端计算机上的文件名：

表 *1:* 网络部署或预部署的模块文件名

模块	网络部署安装程序（已下载）	预部署安装程序
网络访问管理器	anyconnect-win-版本-nam-webdeploy-k9.msi	anyconnect-win-版本-nam-predeploy-k9.msi
网络安全	anyconnect-win-版本 -websecurity-webdeploy-k9.exe	anyconnect-win-版本-websecurity-predeploy-k9.msi
ISE 终端安全评估	anyconnect-win-版本-iseposture-webdeploy-k9.msi	anyconnect-win-版本-iseposture-predeploy-k9.msi
AMP Enabler	anyconnect-win-版本-amp-webdeploy-k9.msi	anyconnect-win-版本-amp-predeploy-k9.exe
网络可视性模块	anyconnect-win-*version*-nvm-webdeploy-k9.exe	anyconnect-win-*version*-nvm-predeploy-k9.msi
Umbrella 漫游安全模块	anyconnect-win-*version*-umbrella-webdeploy-k9.exe	anyconnect-win-*version*-umbrella-predeploy-k9.msi

AnyConnect 4.3（及更高版本）已移至 Visual Studio (VS) 2015 版本环境，并且需要可再分发的 VS 文件以实现其网络访问管理器模块的功能。这些文件作为安装文件包的组成部分安装。您可以使用 .msi 文件将网络访问管理器模块升级到 4.3（或更高版本），但必须先升级 AnyConnect 安全移动客户端并运行版本 4.3（或更高版本）。

注释 如果有 Windows 服务器操作程序，在尝试安装 AnyConnect 网络访问管理器时，可能会发生安装错误。默认情况下，服务器操作系统上未安装 WLAN 服务，因此，您必须安装并重新启动 PC。网络访问管理器要在任何 Windows 操作系统上正常运行，必须具备 WLANAutoconfig 服务。

预部署 AnyConnect 配置文件的位置

如果要将文件复制到客户端系统，下表显示您必须将文件放置到的位置。

表 *2: AnyConnect* 核心文件

文件	描述
anyfilename.xml	AnyConnect 配置文件。此文件指定了为特定用户类型配置的功能和属性值。
AnyConnectProfile.xsd	定义 XML 架构格式。AnyConnect 使用此文件验证配置文件。

表 *3:* 所有操作系统的配置文件位置

操作系统	模块	位置
Windows	使用 VPN 的核心客户端	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	网络访问管理器	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigFiles
	网络安全	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
	客户体验反馈	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
	OPSWAT	%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\opswat
	ISE 终端安全评估	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture
	AMP Enabler	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\AMP Enabler
	网络可视性模块	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
	Umbrella 漫游安全模块	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella **注释** 要启用 Umbrella 漫游安全模块，必须从 Umbrella 控制面板中复制 OrgInfo.json 文件，并将其放置到此目标目录中，而不进行任何重命名。也可以将 OrgInfo.json 文件与 Umbrella 漫游安全模块安装程序放在同一位置，在安装前将该文件放置到 \Profiles\umbrella 中。

操作系统	模块	位置
macOS	所有其他模块	/opt/cisco/anyconnect/profile
	客户体验反馈	/opt/cisco/anyconnect/CustomerExperienceFeedback
	二进制文件	/opt/cisco/anyconnect/bin
	OPSWAT	/opt/cisco/anyconnect/lib/opswat
	库	/opt/cisco/anyconnect/lib
	用户界面资源	/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app/Contents/Resources/
	ISE 终端安全评估	/opt/cisco/anyconnect/iseposture/
	AMP Enabler	/opt/cisco/anyconnect/ampenabler/
	网络可视性模块	/opt/cisco/anyconnect/NVM/
	Umbrella 漫游安全模块	/opt/cisco/anyconnect/umbrella 注释 要启用 Umbrella 漫游安全模块，必须从 Umbrella 控制面板中复制 OrgInfo.json 文件，并将其放置到此目标目录中，而不进行任何重命名。也可以将 OrgInfo.json 文件与 Umbrella 漫游安全模块安装程序放在同一位置，在安装前将该文件放置到 \Profiles\umbrella 中。
Linux	NVM	/opt/cisco/anyconnect/NVM
	所有其他模块	/opt/cisco/anyconnect/profile

克隆虚拟机配合使用 AnyConnect 指南（仅限 Windows）

AnyConnect 终端由 AnyConnect 所有模块均使用的通用设备标识符 (UDID) 进行唯一标识。当对 Windows 虚拟机进行克隆时，源中所有克隆的 UDID 保持不变。要避免克隆虚拟机出现任何潜在问题，请在使用 AnyConnect 之前执行此操作：

1. 导航至 **C:\Program Files\Cisco\Cisco AnyConnect Secure MobilityClient**，并以管理员权限运行 dartcli.exe，如下所示：

   ```
   dartcli.exe -nu
   ```

   或

   ```
   dartcli.exe -newudid
   ```

2. 在执行此命令之前和之后打印 UDID，以确保 UDID 已通过此命令进行了更改：

   ```
   dartcli.exe -u
   ```

   或

```
dartcli.exe -udid
```

将 AnyConnect 模块预部署为独立应用

网络访问管理器、网络安全和 Umbrella 漫游安全模块可作为独立应用运行。安装 AnyConnect 核心客户端，但不使用 VPN 和 AnyConnect UI。

在 Windows 上使用 SMS 部署独立模块

过程

步骤 1 通过配置软件管理系统 (SMS) 来设置 MSI 属性 PRE_DEPLOY_DISABLE_VPN=1，从而禁用 VPN 功能。例如：

```
msiexec /package anyconnect-win-版本-predeploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx* <log_file_name>
```

MSI 将其中嵌入的 VPNDisable_ServiceProfile.xml 文件复制到为 VPN 功能的配置文件指定的目录。

步骤 2 安装模块。例如，以下 CLI 命令安装网络安全：

```
msiexec /package anyconnect-win-version-websecurity-predeploy-k9.msi /norestart /passive
/lvx* c:\test.log
```

步骤 3 （可选）安装 DART。

misexec /package annyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* c:\test.log

步骤 4 将经过模糊处理的客户端配置文件的副本保存到适当的 Windows 文件夹。

步骤 5 重新启动思科 AnyConnect 服务。

将 AnyConnect 模块部署为独立应用

您可以将 AnyConnect 网络访问管理器、网络安全和 Umbrella 漫游安全模块部署为用户计算机上的独立应用。DART 得到这些应用的支持。

独立 NVM有关其部署的优点和方法的详细信息，请参阅。

要求

VPNDisable_ServiceProfile.xml 文件还必须是在 VPN 客户端配置文件目录中的唯一 AnyConnect 配置文件。

独立模块的用户安装

您可以手动拆分各个安装程序并将它们分发给用户。

如果您决定向用户提供 zip 映像并要求他们安装，请务必向用户说明仅安装独立模块。

注释 如果计算机中此前未安装网络访问管理器，用户必须重启计算机才能完成网络访问管理器安装。此外，如果安装属于需要升级某些系统文件的升级安装，用户也必须重启计算机。

过程

步骤 1 指导用户选中 AnyConnect Network Access Manager、 AnyConnect Web Security Module 或 Umbrella Roaming Security Module。

步骤 2 指导用户取消选中 **Cisco AnyConnect VPN Module**。

这将禁用核心客户端的 VPN 功能，安装实用程序将网络访问管理器、网络安全或 Umbrella 漫游安全模块作为不含 VPN 功能的独立应用来安装。

步骤 3 （可选）选中 **Lock Down Component Services** 复选框。锁定组件服务将阻止用户关闭或停止 Windows 服务。

步骤 4 指导用户运行可选模块的安装程序，这些模块可在没有 VPN 服务的情况下使用 AnyConnect GUI。如果用户单击 Install Selected 按钮，将发生以下情况：

a) 弹出一个对话框，要求确认独立网络访问管理器、独立网络安全模块或 Umbrella 漫游安全模块的选择。
b) 如果用户单击 OK，安装实用程序将使用 PRE_DEPLOY_DISABLE_VPN=1 设置调用 AnyConnect 核心安装程序。
c) 安装实用程序将删除所有现有 VPN 配置文件，然后安装 VPNDisable_ServiceProfile.xml。
d) 安装实用程序将调用网络访问管理器、网络安全或 Umbrella 漫游安全安装程序。
e) 计算机将启用网络访问管理器、网络安全模块或 Umbrella 漫游安全模块，但不含 VPN 服务。

预部署到 Windows

使用 zip 文件分发 AnyConnect

zip 软件包文件包含安装实用程序（用于启动单个组件安装程序的选择器菜单程序）以及核心和可选 AnyConnect 模块的 MSI。将 zip 软件包文件提供给用户后，用户运行安装程序 (setup.exe)。该程序显示安装实用程序菜单，用户从中选择要安装的 AnyConnect 模块。您可能不希望用户选择要加载哪些模块。因此，如果您决定使用 zip 进行分发，请编辑 zip 以删除不想使用的模块，然后编辑 HTA 文件。

分发 ISO 的一种方法是使用虚拟 CD 挂载软件，如 SlySoft 或 PowerIS。

预部署 zip 修改

- 使用您在捆绑文件时创建的配置文件更新 zip 文件，并删除不希望分发的任何模块安装程序。

- 编辑 HTA 文件可对安装菜单进行个性化设置，并删除到不希望分发的任何模块安装程序的链接。

AnyConnect zip 文件内容

文件	目的
GUI.ico	AnyConnect 图标图像。
Setup.exe	启动安装实用程序。
anyconnect-win-版本-dart-predeploy-k9.msi	DART 模块的 MSI 安装程序文件。
anyconnect-win-版本-gina-predeploy-k9.msi	SBL 模块的 MSI 安装程序文件。
anyconnect-win-版本-iseposture-predeploy-k9.msi	ISE 终端安全评估模块的 MSI 安装程序。
anyconnect-win-版本-amp-predeploy-k9.exe	AMP 启用程序的 MSI 安装程序文件。
anyconnect-win-版本-nvm-predeploy-k9.msi	网络可视性模块的 MSI 安装程序文件。
anyconnect-win-版本-umbrella-predeploy-k9.msi	Umbrella 漫游安全模块的 MSI 安装程序文件。
anyconnect-win-版本-nam-predeploy-k9.msi	网络访问管理器模块的 MSI 安装程序文件。
anyconnect-win-版本-posture-predeploy-k9.msi	终端安全评估模块的 MSI 安装程序文件。
anyconnect-win-版本-websecurity-predeploy-k9.msi	网络安全模块的 MSI 安装程序文件。
anyconnect-win-版本-core-vpn-predeploy-k9.msi	AnyConnect 核心客户端的 MSI 安装程序文件。
autorun.inf	setup.exe 的信息文件。
eula.html	可接受使用策略。
setup.hta	安装实用程序 HTML 应用 (HTA)，您可以针对自己的站点进行定制。

使用 SMS 分发 AnyConnect

从 zip 映像提取要部署的模块的安装程序 (*.msi) 后，可以手动分发这些安装程序。

要求

- 在 Windows 上安装 AnyConnect 时，必须禁用 AlwaysInstallElevated 或 Windows 用户帐户控制 (UAC) 组策略设置。否则，AnyConnect 安装程序可能无法访问安装所需的某些目录。
- Microsoft Internet Explorer (MSIE) 用户应将头端添加到受信任站点列表或安装 Java。添加到受信任站点列表会启用 ActiveX 控件进行安装，此时用户交互最少。

配置文件部署过程

- 如果使用 MSI 安装程序，MSI 将选择已放置在 Profiles 文件夹中的任何配置文件并在安装过程中将其放置在相应的文件夹中。在CCO上可用的预部署MSI文件中会提供适当的文件夹路径。
- 如果在安装后手动预部署配置文件，请手动复制配置文件或使用 SMS（如 Altiris）将配置文件部署到相应的文件夹。
- 确保放到头端上的客户端配置文件与预部署到客户端的客户端配置文件相同。还必须将此配置文件绑定到ASA上使用的组策略。如果该客户端配置文件与头端上的客户端配置文件不匹配，或者如果没有将其绑定到组策略，则您可能获得不一致的行为，包括访问被拒绝。

Windows 预部署 MSI 示例

已安装的模块	命令和日志文件
无 VPN 功能的 AnyConnect 核心客户端。 安装独立网络访问管理器或网络安全模块时使用。	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
有 VPN 功能的 AnyConnect 核心客户端。	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
客户体验反馈	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
诊断和报告工具 (DART)	msiexec /package anyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-win-*version*-gina-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-gina-predeploy-k9-install-datetimestamp.log
网络访问管理器	msiexec /package anyconnect-win-*version*-nam-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-nam-predeploy-k9-install-datetimestamp.log
网络安全	msiexec /package anyconnect-win-*version*-websecurity-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-websecurity-predeploy-k9-install-datetimestamp.log
VPN 终端安全评估 (HostScan)	msiexec /package anyconnect-win-*version*-posture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-posture-predeploy-k9-install-datetimestamp.log
ISE 终端安全评估	msiexec /package anyconnect-win-*version*-iseposture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-iseposture-predeploy-k9-install-datetimestamp.log

已安装的模块	命令和日志文件
AMP Enabler	msiexec /package anyconnect-win-*version*-amp-predeploy-k9.msi / norestart/passive /lvx* anyconnect-win-*version*-amp-predeploy-k9-install-datetimestamp.log
网络可视性模块	msiexec /package anyconnect-win-*version*-nvm-predeploy-k9.msi / norestart/passive /lvx* anyconnect-win-*version*-nvm-predeploy-k9-install-datetimestamp.log
Umbrella 漫游安全	msiexec /package anyconnect-win-*version*-umbrella-predeploy-k9.msi / norestart/passive /lvx* anyconnect-*version*-umbrella-predeploy-k9-install-datetimestamp.log

AnyConnect 示例 Windows 转换

思科提供示例 Windows 转换以及介绍如何使用转换的文档，以下划线字符 (_) 开头的转换是一般 Windows 转换，它允许您仅将某些转换应用于某些模块安装程序。以字母字符开头的转换是 VPN 转换。每个转换都有使用说明文档，转换下载说明文档是 sampleTransforms-*x.x.x*.zip。

Windows 预部署安全选项

思科建议授予最终用户对托管Cisco AnyConnect Secure Mobility Client 的设备的有限权限。如果最终用户确保其他权利，则安装程序可提供锁定功能，防止用户和本地管理员关闭或停止终端上建立为锁定的 Windows 服务。在网络安全模块中，您可以使用服务密码将客户端设置为绕过模式。您还可以阻止用户卸载 AnyConnect。

Windows 锁定属性

每个 MSI 安装程序都支持通用属性 (LOCKDOWN)，当该属性设置为非零值时，可防止与安装程序相关的 Windows 服务被终端设备上的用户或本地管理员控制。我们建议您使用安装时提供的示例转换 (anyconnect-vpn-transforms-X.X.xxxxx.zip) 来设置该属性，并将转换应用至您想锁定的每个 MSI 安装程序。锁定选项同样是 ISO 安装实用程序中的一个复选框。

从添加/删除程序列表中隐藏 AnyConnect

您可以隐藏安装的 AnyConnect 模块，这样用户从 Windows Add/Remove Program 列表中便看不到该模块。即使您使用 ARPSYSTEMCOMPONENT=1 启动任何安装程序，该模块都不会显示在 Windows Add/Remove Program 列表中。

我们建议您使用我们提供的示例转换 (anyconnect-vpn-transforms-X.X.xxxxx.zip) 来设置此属性。将该转换应用于您希望隐藏的每个模块的每个 MSI 安装程序。

Windows 上的 AnyConnect 模块安装和删除顺序

模块安装程序在开始安装之前会确认其版本与核心客户端相同。如果版本不匹配，该模块不会安装，并且安装程序通知用户存在版本不匹配。如果您使用安装实用程序，则会构建软件包中的模块并将其封装在一起，且版本始终匹配。

过程

步骤 1 按以下顺序安装 AnyConnect 模块：

a) 安装 AnyConnect 核心客户端模块，此过程会安装 GUI 和 VPN 功能（SSL 和 IPsec）。

在 Windows 和 macOS 中，已创建受限制的用户帐户 (ciscoacvpnuser)，以便仅在检测到启用了管理隧道功能时才实施最小特权原则。在 AnyConnect 卸载期间或安装升级过程中，此帐户会被删除。

b) 安装 AnyConnect 诊断和报告工具 (DART) 模块，以提供有关 AnyConnect 核心客户端安装的有用诊断信息。

c) 按任意顺序安装 Umbrella 漫游安全模块、网络可视性模块、AMP 启用程序、SBL、网络访问管理器、网络安全、终端安全评估模块或 ISE 合规性模块。

步骤 2 按以下顺序卸载 AnyConnect 模块：

a) 按任意顺序卸载 Umbrella 漫游安全模块、网络可视性模块、AMP 启用程序、网络访问管理器、网络安全、终端安全评估、ISE 合规性模块或 SBL。

b) 卸载 AnyConnect 核心客户端。

c) 最后卸载 DART。

如果卸载过程失败，DART 信息会很有用。

注释 根据设计，卸载 AnyConnect 后，某些 XML 文件仍然保留。

预部署到 macOS

在 macOS 上安装和卸载 AnyConnect

用于 macOS 的 AnyConnect 以 DMG 文件形式分发，其中包括所有 AnyConnect 模块。当用户打开 DMG 文件，然后运行 AnyConnect.pkg 文件时，系统会启动安装对话框，引导用户完成安装。在 Installation Type 屏幕上，用户可以选择要安装的软件包（模块）。

要从您的分发中删除任何 AnyConnect 模块，可使用 Apple pkgutil 工具，并在修改后签署软件包。也可以使用 ACTransforms.xml 修改安装程序。您可以定制语言和外观，以及更改一些其他安装操作，如“定制”章节中的使用 ACTransform.xml 在 macOS 上自定义安装程序行为所述。

在 Mac OS 上安装 AnyConnect 模块作为独立应用

可以只安装网络安全、网络可视性模块或 Umbrella 漫游安全模块，而不含 VPN。不使用 VPN 和 AnyConnect UI。

以下过程通过安装独立配置文件编辑器、创建配置文件和将该配置文件添加到 DMG 软件包中，来说明如何定制这些模块。它还将 AnyConnect 用户界面设置为在启动时自动启动，这使 AnyConnect 可以为相应模块提供必要的用户和组信息。

过程

步骤 1 从 Cisco.com 下载 Cisco AnyConnect Secure Mobility Client DMG 软件包。

步骤 2 打开文件访问安装程序。请注意，下载的映像是只读文件。

步骤 3 通过运行磁盘实用程序或使用终端应用以使安装程序映像可写入，如下所示：

```
hdiutil convert <source dmg> -format UDRW -o <output dmg>
```

步骤 4 在运行 Windows 操作系统的计算机上安装独立配置文件编辑器。作为定制安装或完全安装的组成部分，必须选择所需的 AnyConnect 模块。默认情况下不会安装这些模块。

步骤 5 启动配置文件编辑器并创建配置文件。

步骤 6 将配置文件适当保存为 `WebSecurity_ServiceProfile.xml` 或 `OrgInfo.json`（从您控制面板上获得的名称），放在安全位置。

对于这些模块，配置文件编辑器将为该配置文件创建另一个模糊处理的版本（例如对于网络安全，将创建 `WebSecurity_ServiceProfile.wso`），并将其保存到与您保存该配置文件相同的位置（例如对于网络安全，将保存到 `WebSecurity_ServiceProfile.xml`）。按照以下步骤操作，以完成模糊处理：

a) 将指定的 .wso 文件从 Windows 设备复制到 macOS 相应文件夹路径下的安装程序数据包中（例如对于网络安全，路径为 `AnyConnect x.x.x/Profiles/websecurity`）。或者对于网络安全实例，使用如下所示的终端应用：

```
cp <path to the wso> \Volumes\"AnyConnect <VERSION>"\Profiles\websecurity\
```

b) 在 macOS 安装程序中，转到 `AnyConnect x.x.x/Profiles` 目录并在 TextEdit 中打开 `ACTransforms.xml` 文件进行编辑。设定 `<DisableVPN>` 元素为 **true** 以确保不安装 VPN 的功能：

```
<ACTransforms>
<DisableVPN>true</DisableVPN>
</ACTransforms>
```

c) AnyConnect DMG 数据包现在已准备就绪，可分配给您的用户。

步骤 7 将配置文件适当保存为 `WebSecurity_ServiceProfile.xml`、`NVM_ServiceProfile.xml` 或 `OrgInfo.json`（您从控制面板上获得的名称），放在安全位置。

对于这些模块，配置文件编辑器将为该配置文件创建另一个模糊处理的版本（例如对于网络安全，将创建 `WebSecurity_ServiceProfile.wso`），并将其保存到与您保存该配置文件相同的位置（例如对于网络安全，将保存到 `WebSecurity_ServiceProfile.xml`）。按照以下步骤操作，以完成模糊处理：

a) 将指定的 .wso 文件从 Windows 设备复制到 macOS 相应文件夹路径下的安装程序数据包中（例如对于网络安全，路径为 `AnyConnect x.x.x/Profiles/websecurity`）。或者对于网络安全实例，使用如下所示的终端应用：

```
cp <path to the wso> \Volumes\"AnyConnect <VERSION>"\Profiles\websecurity\
```

b) 在 macOS 安装程序中，转到 `AnyConnect x.x.x/Profiles` 目录并在 TextEdit 中打开 `ACTransforms.xml` 文件进行编辑。设定 `<DisableVPN>` 元素为 **true** 以确保不安装 VPN 的功能：

```
<ACTransforms>
<DisableVPN>true</DisableVPN>
</ACTransforms>
```

c) AnyConnect DMG 数据包现在已准备就绪，可分配给您的用户。

在 macOS 上限制应用

Gatekeeper 可以限制允许哪些应用在系统上运行。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 应用商店和已确定的开发商”(Mac App Store and identified developers)（已签名的应用）。

AnyConnect 当前版本是使用 Apple 证书的已签名应用。如果（仅）面向 Mac App Store 配置 Gatekeeper，则您必须选择“任何地点”(Anywhere) 设置或按住 Ctrl 键单击，以绕过选定的设置，进而通过预部署的安装方式安装和运行 AnyConnect。有关详细信息，请参阅：http://www.apple.com/macosx/mountain-lion/security.html。

预部署到 Linux

安装用于 Linux 的模块

您可以打开用于 Linux 的单个安装程序并手动分配它们。预部署安装包中的各个安装程序均可以单独运行。使用压缩文件实用程序查看和提取 tar.gz 文件中的文件。

过程

步骤 1 安装 AnyConnect 核心客户端模块，此过程会安装 GUI 和 VPN 功能（SSL 和 IPsec）。

步骤 2 安装 DART 模块，该模块提供关于 AnyConnect 核心客户端安装的有用诊断信息。

步骤 3 安装终端安全评估模块或 ISE 合规性模块。

步骤 4 安装 NVM。

卸载用于 Linux 的模块

用户卸载 AnyConnect 的顺序非常重要。

如果卸载过程失败，DART 信息将非常有价值。

过程

步骤 1 卸载 NVM。

步骤 2 卸载终端安全评估模块或 ISE 合规性模块。

步骤 3 卸载 AnyConnect 核心客户端。

步骤 4 卸载 DART。

在 Linux 设备上手动安装/卸载 NVM

过程

步骤 1 提取 AnyConnect 预部署软件包。

步骤 2 导航到 nvm 目录。

步骤 3 调用脚本 **$sudo ./nvm_install.sh**。

您可以使用 /opt/cisco/anyconnect/bin/nvm_uninstall.sh 卸载 NVM。

使用 Firefox 初始化的服务器证书验证

如果要将服务器证书与 AnyConnect 配合使用，必须使 AnyConnect 可访问证书存储库，并将证书验证为受信任。默认情况下，AnyConnect 使用 Firefox 证书存储库。

激活 Firefox 证书存储库

在 Linux 设备上安装 AnyConnect 后，请在首次尝试连接 AnyConnect 前打开 Firefox 浏览器。打开 Firefox 后，会创建一个包含证书存储库的配置文件。

如果不使用 Firefox 证书存储库

如果选择不使用 Firefox，则必须将本地策略配置为排除 Firefox 证书存储库，并且必须配置 PEM 存储库。

多模块要求

如果部署核心客户端以及一个或多个可选模块，则必须对每个安装程序应用锁定属性。Windows 预部署 MSI 示例，第 16 页介绍了锁定。

此操作可用于 VPN 安装程序、网络访问管理器、网络安全、网络可视性模块和 Umbrella 漫游安全模块。

注释 如果选择激活对 VPN 安装程序的锁定，将因此也会锁定 AMP 启用程序。

在 Linux 设备上手动安装 DART

1. 将 anyconnect-dart-linux-(ver)-k9.tar.gz 存储在本地。
2. 从终端使用 **tar -zxvf** <含文件名的 *tar.gz* 文件路径命令提取 tar.gz 文件。
3. 从终端导航到提取的文件夹，并使用 **sudo ./dart_install.sh** 命令运行 dart_install.sh。
4. 接受许可协议，并等待安装完成。

注释 您仅可使用 **/opt/cisco/anyconnect/dart/dart_uninstall.sh** 卸载 DART。

网络部署 AnyConnect

网络部署是指客户端系统上的 AnyConnect 下载程序从头端获取 AnyConnect 软件，或使用头端上的门户安装或更新 AnyConnect。传统网络启动过于依赖浏览器支持（以及 Java 和 ActiveX 要求），作为一种替代方案，我们改进了自动网络部署的流程，该流程在初始下载以及从无客户端页面启动时会显示。自动调配 (Weblaunch) 适用于支持 NPAPI（Netscape 插件应用编程接口）的所有浏览器以及支持 ActiveX 的浏览器。

通过 ASA 进行网络部署

ASA 上的无客户端门户执行 AnyConnect 网络部署。流程如下：

用户打开浏览器并连接到 ASA 的无客户端门户。在门户上，用户单击**启动 AnyConnect 客户端**按钮。然后，他们可以手动下载 AnyConnect 软件包。如果他们运行的浏览器支持 NPAPI（Netscape 插件应用编程接口）插件，则还可以使用该选项卡通过 weblaunch（ActiveX 或 Java）来启动自动网络调配。

ASA 网络部署限制

- 不支持将同一 O/S 的多个 AnyConnect 软件包载入 ASA。
- 网络部署时，VPN 终端安全评估 (HostScan) 模块中不含 OPSWAT 定义。您必须手动部署 HostScan 模块或将其载入 ASA 上，以向客户端提供 OPSWAT 定义。

- 如果 ASA 只有默认内部闪存大小，您在 ASA 上存储和加载多个 AnyConnect 客户端软件包时可能会遇到问题。即使您的闪存有足够空间承载软件包，ASA 也可能会在解压缩和加载客户端映像时耗尽缓存内存。有关部署 AnyConnect 以及升级 ASA 内存时 ASA 内存要求的详细信息，请参阅最新的 VPN 设备版本说明。
- 用户可使用 IP 地址或 DNS 连接到 ASA，但不支持链路本地安全网关地址。
- 您必须将支持网络启动的安全设备的 URL 添加到 Internet Explorer 的受信任站点列表中。可使用组策略完成此操作，如在 Windows 上将 ASA 添加到 Internet Explorer 的受信任站点列表所述。
- 对于 Windows 7 SP1 用户，我们建议您在安装和首次使用之前安装 Microsoft .NET framework 4.0。在启动时，Umbrella 服务将检查是否已安装了 .NET framework 4.0（或更高版本）。如果未检测到，则不会激活 Umbrella 漫游安全模块，并将显示一条消息。下载然后安装 .NET Framework，必须重新启动才能激活 Umbrella 漫游安全模块。

通过 ISE 进行网络部署

ISE 上的策略确定 AnyConnect 客户端的部署时间。用户打开浏览器并连接到 ISE 控制的资源，然后重定向到 AnyConnect 客户端门户。该 ISE 门户将帮助用户下载和安装 AnyConnect。在 Internet Explorer 中，ActiveX 控件将指导用户进行安装。在其他浏览器中，门户将下载网络设置助理，该工具会帮助用户安装 AnyConnect。

ISE 部署限制

- 如果 ISE 和 ASA 均执行 AnyConnect 网络部署，则两个前端上的配置必须匹配。
- 如果在 ISE Client Provisioning Policy 中配置了 AnyConnect ISE 终端安全评估代理，则 ISE 服务器只能由该代理发现。ISE 管理员可在 Agent Configuration > Policy > Client Provisioning 下配置 NAC 代理或 AnyConnect ISE 终端安全评估模块。

在 ASA 上配置网络部署

WebLaunch 的浏览器限制

表 *4:* 按操作系统划分的针对 *Weblaunch* 的 *AnyConnect* 浏览器支持

操作系统	浏览器
Microsoft 当前支持的 Windows 10 x86（32 位）和 x64（64位）版本	Internet Explorer 11
Windows 8.x x86（32 位）和 x64（64 位）	Internet Explorer 11
Windows 7 SP1 x86（32 位）和 x64（64位）	Internet Explorer 11
macOS 10.13、10.14（64 位）和 10.15（64 位）	Safari 11

注释 由于 EDGE 浏览器不支持 ActiveX，因此我们的调配页面隐藏了自动调配选项。

注释 网络启动适用于支持 NPAPI（网景插件应用编程接口）插件的所有浏览器。

此外，由于添加了 AnyConnect Umbrella 漫游安全模块，因此需要 Microsoft .NET 4.0。

下载 AnyConnect 软件包

从思科 AnyConnect 软件下载网页下载最新的 Cisco AnyConnect Secure Mobility Client 软件包。

操作系统	AnyConnect 网络部署软件包名称
Windows 的 ISE 安全评估代理	anyconnect-win-版本-webdeploy-k9.pkg
macOS	anyconnect-macos-版本-webdeploy-k9.pkg
Linux（64位）	anyconnect-linux64-版本-webdeploy-k9.pkg

注释 您不应具有 ASA 上同一操作系统的不同版本。

在 ASA 上加载 AnyConnect 软件包

过程

步骤 1 导航到配置 > 远程接入 > VPN > 网络 (客户端) 接入 > AnyConnect 客户端软件。AnyConnect 客户端映像面板会显示当前在 ASA 上加载的 AnyConnect 映像。映像出现的顺序是 ASA 将其下载到远程计算机的顺序。

步骤 2 要添加 AnyConnect 映像，单击 **Add**。

- 单击 **Browse Flash** 可选择已上传到 ASA 的 AnyConnect 映像。
- 单击 **Upload** 浏览至您存储于本地计算机上的 AnyConnect 图像。

步骤 3 单击 **OK** 或 **Upload**。

步骤 4 单击应用。

启用其他 AnyConnect 模块

要启用其他功能，请在组策略或本地用户配置中指定新模块名称。注意启用附加模块将影响下载时间。启用功能时，AnyConnect 必须将这些模块下载到 VPN 终端。

注释 如果您选择 Start Before Logon，还必须在 AnyConnect 客户端配置文件中启用此功能。

过程

步骤 1 在 ASDM 中，转到**配置 > 远程接入 VPN > 网络 (客户端) 接入 > 组策略**。

步骤 2 选择组策略，单击 **Edit** 或 **Add** 可编辑或新增组策略。

步骤 3 在导航窗格中，选择**VPN 策略 > AnyConnect 客户端**。在**要下载的客户端模块**中，单击**添加**，然后选择要添加到此组策略的每个模块。可用的模块是您添加或上传到 ASA 的模块。

步骤 4 单击 **Apply** 并保存对组策略的更改。

在 ASDM 中创建客户端配置文件

必须将 AnyConnect 网络部署软件包添加到 ASA，然后才能在 ASA 上创建客户端配置文件。

过程

步骤 1 导航到 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。

步骤 2 选择要与组关联的客户端配置文件，然后单击 **Change Group Policy**。

步骤 3 在 Change Policy for Profile 策略名称窗口中，从 Available Group Policies 字段中选择组策略，然后单击右箭头，将其移到 Policies 字段。

步骤 4 单击 **OK**。

步骤 5 在 AnyConnect Client Profile 页面上，单击 **Apply**。

步骤 6 单击 **Save**。

步骤 7 完成配置时，单击 **OK**。

在 ISE 上配置网络部署

ISE 可配置和部署 AnyConnect 核心、ISE 终端安全评估模块和 OPSWAT（合规性模块）以支持 ISE 的终端安全评估。ISE 还可以部署在连接到 ASA 时可使用的所有 AnyConnect 模块和资源。当用户浏览到 ISE 控制的资源时：

- 如果 ISE 在 ASA 之后，则用户连接 ASA，下载 AnyConnect，然后建立 VPN 连接。如果 AnyConnect ISE 终端安全评估并非由 ASA 安装，则用户将重定向到 AnyConnect 客户端门户来安装 ISE 终端安全评估。
- 如果 ISE 不在 ASA 之后，则用户连接到 AnyConnect 客户端门户，该门户会引导用户在 ISE 上安装 AnyConnect 配置中定义的 AnyConnect 资源。如果 ISE 终端安全评估状态未知，常见配置是将浏览器重定向到 AnyConnect 客户端调配门户。
- 当用户在 ISE 中被定向到 AnyConnect 客户端调配门户时：
  - 如果浏览器是 Internet Explorer，则 ISE 将下载 AnyConnect 下载程序，然后该下载程序会加载 AnyConnect。
  - 对于所有其他浏览器，ISE 将打开客户端调配重定向门户，该门户会显示下载网络设置助理 (NSA) 工具的链接。用户运行 NSA，该工具可查找 ISE 服务器并下载 AnyConnect 下载程序。

    NSA 在 Windows 上运行完毕后会自行删除。在 macOS 上运行完毕后，必须手动将其删除。

ISE 文档介绍了如何执行以下操作：

- 在 ISE 中创建 AnyConnect 配置文件
- 将 AnyConnect 资源从本地设备添加到 ISE
- 从远程站点添加 AnyConnect 调配资源
- 部署 AnyConnect 客户端和资源

注释 由于 AnyConnect ISE 终端安全评估模块在发现中不支持基于 Web 代理的重定向，思科建议您使用基于非重定向的发现。您可以在《思科身份服务引擎管理员指南》的“无需对不同网络进行 URL 重定向的客户端调配”部分中找到更多信息。

ISE 可配置和部署以下 AnyConnect 资源：

- AnyConnect 核心和模块，包括 ISE 终端安全评估模块
- 配置文件：网络可视性模块、AMP 启用程序、VPN、网络访问管理器、网络安全、客户反馈和 AnyConnect ISE 终端安全评估
- 定制文件
  - 用户界面资源
  - 二进制文件、连接脚本文件和帮助文件
- 本地化文件
  - 用于消息本地化的 AnyConnect gettext 转换
  - Windows Installer 转换

准备 AnyConnect 文件进行 ISE 上传

- 下载适用于操作系统的 AnyConnect 软件包，以及您希望在本地 PC 上部署的其他 AnyConnect 资源。

  注释 对于 ASA，安装将使用 VPN 下载程序进行。在下载后，将通过 ASA 推送 ISE 终端安全评估配置文件，并在 ISE 终端安全评估模块联系 ISE 之前提供随后调配该配置文件所需的发现主机。而对于 ISE，ISE 终端安全评估模块只会在发现 ISE 后获取该配置文件，这有可能导致错误。因此，在连接到 VPN 时，建议使用 ASA 推送 ISE 终端安全评估模块。

- 为您计划部署的模块创建配置文件。至少创建一个 AnyConnect ISE 终端安全评估配置文件 (ISEPostureCFG.xml)。

  注释 如果使用了基于非重定向的发现，则预部署 ISE 终端安全评估模块时必须使用包含 Call Home List 的 ISE 终端安全评估配置文件。

- 将定制和本地化资源合并成一个 ZIP 存档，该存档在 ISE 中称为捆绑包。捆绑包可包含：
  - AnyConnect UI 资源
  - VPN 连接脚本
  - 帮助文件
  - 安装程序转换

  AnyConnect 本地化捆绑包可包含：
  - 二进制格式的 AnyConnect Gettext 转换
  - 安装程序转换

按照《准备 AnyConnect 定制和本地化进行 ISE 部署》中所述的步骤创建 ISE 捆绑包。

配置 ISE 以部署 AnyConnect

必须先将 AnyConnect 软件包上传到 ISE，然后再上传和创建其他 AnyConnect 资源。

注释 在 ISE 中配置 AnyConnect 配置对象时，取消选中“AnyConnect 模块选择”(AnyConnect Module Selection) 下的 VPN 模块不会禁用已部署/已调配客户端上的 VPN。

1. 在 ISE 中，选择**策略** > **策略元素** > **结果** > 。展开**客户端调配 (Client Provisioning)** 显示**资源 (Resources)**，然后选择**资源 (Resources)**。

2. 选择**添加 (Add)** > **本地磁盘代理资源 (Agent resources from local disk)**，然后上传 AnyConnect 软件包文件。为您计划部署的任何其他 AnyConnect 资源重复添加本地磁盘代理资源。
3. 选择**添加** > **AnyConnect 配置** > 。此 AnyConnect 配置用于对模块、配置文件、定制/语言包和 OPSWAT 软件包进行配置，如下表所述。

   可在 ISE、ASA 或 Windows AnyConnect 配置文件编辑器中创建和编辑 AnyConnect ISE 终端安全评估配置文件。下表显示 ISE 中每个 AnyConnect 资源的名称以及资源类型的名称。

   表 *5: ISE* 中的 *AnyConnect* 资源

提示符	ISE 资源类型和说明
AnyConnect 软件包	AnyConnectDesktopWindows AnyConnectDesktopOSX AnyConnectWebAgentWindows AnyConnectWebAgentOSX
合规性模块	AnyConnectComplianceModuleWindows AnyConnectComplianceModuleOSX
AnyConnect 配置文件	AnyConnectProfile ISE 为上传的 AnyConnect 软件包所提供的每个配置文件显示一个复选框。
定制捆绑包	AnyConnectCustomizationBundle
本地化捆绑包	AnyConnectLocalizationBundle

4. 创建基于角色或基于操作系统的客户端调配策略。对于客户端调配终端安全评估代理，可选择 AnyConnect 和 ISE 传统 NAC/MAC 代理。每个客户端调配策略只能调配一个代理，要么是 AnyConnect 代理，要么是传统 NAC/MAC 代理。配置 AnyConnect 代理时，请选择一个在步骤 2 创建的 AnyConnect 配置。

在 FTD 上置网络部署

Firepower 威胁防御 (FTD) 设备是下一代防火墙 (NGFW)，提供类似于 ASA 的安全网关功能。FTD 设备仅支持使用 AnyConnect 安全移动客户端的远程接入 VPN (RA VPN)，不支持任何其他客户端或无客户端 VPN 接入。隧道建立和连接通过 IPsec IKEv2 或 SSL 完成。连接到 FTD 设备时不支持 IKEv1。

在 FTD 头端上配置 Windows、Mac 和 Linux AnyConnect 客户端，并在连接后进行部署，使远程用户能够访问 SSL 或 IKEv2 IPsec VPN 客户端，而无需安装和配置客户端软件。如果以前安装了客户端，当用户验证时，FTD 头端会检查客户端的版本，并根据需要升级客户端。

如果没有以前安装的客户端，远程用户需输入配置的接口 IP 地址，以下载和安装 AnyConnect 客户端。FTD 头端将下载和安装与远程计算机的操作系统匹配的客户端，并建立安全连接。

从平台应用程序商店可安装适用于 Apple iOS 和 Android 设备的 AnyConnect 应用程序。它们需要满足最低配置要求，以便与 FTD 头端建立连接。对于其他头端设备和环境，也可以使用本章介绍的另一种部署方法来分发 AnyConnect 软件。

目前，在 FTD 上只能配置核心 AnyConnect VPN 模块和 AnyConnect VPN 配置文件并将它们分发到终端。Firepower 管理中心 (FMC) 中的远程接入 VPN 策略向导可快速而轻松地设置这些基本 VPN 功能。

AnyConnect 和 FTD 的准则和局限性

- 唯一支持的 VPN 客户端是 Cisco AnyConnect Secure Mobility Client。不支持任何其他客户端或本机 VPN。不支持使用无客户端 VPN 作为自己的实体；无客户端 VPN 仅用于部署 AnyConnect 客户端。
- 在 FTD 上使用 AnyConnect 需要版本 4.0 或更高版本的 AnyConnect，以及版本 6.2.1 或更高版本的 FMC。
- FMC 内在不支持 AnyConnect 配置文件编辑器，您必须单独配置 VPN 配置文件。在 FMC 中作为文件对象添加 VPN 配置文件和 AnyConnect VPN 软件包，它们将成为 RA VPN 配置的一部分。
- 目前不支持核心 VPN 功能之外的安全移动、网络访问管理和所有其他 AnyConnect 模块以及它们的配置文件。
- 不支持 VPN 负载均衡。
- 不支持浏览器代理。
- 不支持所有终端安全评估变体（HostScan、终端安全评估和 ISE）和基于客户端安全评估的动态访问策略。
- Firepower 威胁防御设备不会配置或部署自定义或本地化 AnyConnect 所必需的文件。
- FTD 上不支持需要 AnyConnect 客户端上自定义属性的功能，例如：桌面客户端上的延迟升级和移动客户端上的 Per-App VPN。
- 不能在 FTD 头端执行本地身份验证，因此，配置的用户不可用于远程连接，并且 FTD 不能作为证书颁发机构。此外，不支持以下身份验证功能：
  - 辅助或双重身份验证
  - 使用 SAML 2.0 的单一登录
  - TACACS、Kerberos（KCD 身份验证）和 RSA SDI
  - LDAP 授权（LDAP 属性映射）
  - RADIUS CoA

有关在 FTD 上配置和部署 AnyConnect 的详细信息，请参阅相应版本的《Firepower 管理中心配置指南（版本 6.2.1 或更高版本）》中的 *Firepower* 威胁防御远程接入 *VPN* 一章。

更新 AnyConnect 软件和配置文件

AnyConnect 可通过多种方式更新。

- AnyConnect 客户端 - 当 AnyConnect 连接到 ASA 时，AnyConnect 下载程序将检查 ASA 上是否加载了任何新软件或配置文件。AnyConnect 下载程序将这些更新下载到客户端，并将建立 VPN 隧道。
- 云更新 - Umbrella 漫游安全模块可从 Umbrella 云基础设施为所有已安装的 AnyConnect 模块提供自动更新。通过云更新，可自动从 Umbrella 云基础设施获得软件升级，且更新跟踪将取决于该软件升级，而非管理员的任何操作。默认情况下，将禁用通过云更新进行自动更新。
- ASA 或 FTD 网络门户 - 您指示用户连接到 ASA 的无客户端网络门户进行更新。FTD 仅可下载核心 VPN 模块。
- ISE - 当用户连接到 ISE 时，ISE 将使用其 AnyConnect 配置判断是否有更新的组件或新的终端安全评估要求。在授权后，网络访问设备 (NAD) 会将用户重定向到 ISE 门户，将在客户端上安装 AnyConnect 下载程序，以管理软件包提取和安装。我们建议您将部署软件包上传到 ASA 前端，并确保 AnyConnect 客户端的版本与 ASA 和 ISE 部署软件包版本相匹配。

  接收到 "在建立 VPN 隧道时，必须执行自动软件更新，但无法执行" 的消息表示配置的 ISE 策略需要更新。当本地设备上的 AnyConnect 版本比 ISE 上配置的版本更旧时，您可以选择以下选项，因为在 VPN 处于活动状态时不允许客户端更新：

  - 在带外部署 AnyConnect 更新
  - 在 ASA 和 ISE 上配置相同版本的 AnyConnect

可以允许最终用户延迟更新，并且即便您将更新载入头端，也可阻止客户端更新。

升级示例流程

必备条件

以下示例假定：

- 您已在 ISE 中创建动态授权控制列表 (DACL)，且列表已推送到 ASA。该列表使用客户端的终端安全评估状态确定何时将客户端重定向到 ISE 上的 AnyConnect 客户端调配门户。
- ISE 在 ASA 之后。

AnyConnect 已安装在客户端上

1. 用户启动 AnyConnect，提供凭证，并单击“连接”(Connect)。
2. ASA 建立与客户端的 SSL 连接，将身份验证凭证传递到 ISE，ISE 验证凭证。
3. AnyConnect 启动 AnyConnect 下载程序，该下载程序执行所有升级操作，并启动 VPN 隧道。

如果 ASA 未安装 ISE 终端安全评估，则

1. 用户浏览到任何站点时，DACL 将其重定向到 ISE 上的 AnyConnect 客户端调配门户。

2. 如果使用 Internet Explorer 浏览器，ActiveX 控件将启动 AnyConnect 下载程序。在其他浏览器中，用户下载并执行网络设置助理 (NSA)，该工具会下载并启动 AnyConnect 下载程序。
3. AnyConnect 下载程序执行在 ISE 上配置的所有 AnyConnect 升级，其中现在包括 AnyConnect ISE 终端安全评估模块。
4. 客户端上的 ISE 终端安全评估代理将启动终端安全评估。

未安装 AnyConnect

1. 用户浏览到站点，启动到 ASA 无客户端门户的连接。
2. 用户提供身份验证凭证，该凭证将传输到 ISE 并进行验证。
3. AnyConnect 下载程序由 Internet Explorer 中的 ActiveX 控件和其他浏览器中的 Java 小应用启动。
4. AnyConnect 下载程序执行在 ASA 上配置的升级，然后启动 VPN 隧道。下载程序完成。

如果 ASA 未安装 ISE 终端安全评估，则

1. 用户再次浏览到站点，然后重定向到 ISE 上的 AnyConnect 客户端调配门户。
2. 在 Internet Explorer 中，ActiveX 控件启动 AnyConnect 下载程序。在其他浏览器中，用户下载并执行网络设置助理，该工具将下载并启动 AnyConnect 下载程序。
3. AnyConnect 下载程序通过现有 VPN 隧道执行 ISE 上配置的所有升级，其中包括添加 AnyConnect ISE 终端安全评估模块。
4. ISE 终端安全评估代理启动终端安全评估。

禁用 AnyConnect 自动更新

可以通过配置和分发客户端配置文件来禁用或限制 AnyConnect 自动更新。

- 在 VPN 客户端配置文件中：
  - Auto Update 将禁用自动更新。您可以将此配置文件包括在 AnyConnect 网络部署安装中，或添加到现有的客户端安装中。您也可以允许用户切换此设置。
- 在 VPN 本地策略配置文件中：
  - 绕过下载程序阻止将 ASA 上的任何更新内容下载到客户端。
  - Update Policy 在连接到不同头端时提供对软件和配置文件更新的精细控制。

在 WebLaunch 期间提示用户下载 AnyConnect

您可以将ASA配置为提示远程用户启动网络部署，并配置一个时间段，在这个时间段内他们可以选择下载 AnyConnect 或转到无客户端入口页面。

提示用户下载 AnyConnect 在组策略或用户帐户中进行配置。以下步骤显示如何在组策略中启用此功能。

过程

步骤 1 在 ASDM 中，转到**配置** > **远程接入 VPN** > **网络 (客户端) 接入** > **组策略**。

步骤 2 选择组策略，单击 **Edit** 或 **Add** 可编辑或新增组策略。

步骤 3 在导航窗格中，选择**高级** > **AnyConnect 客户端** > **登录设置**。如果需要，取消选中 **Inherit** 复选框，然后选择 Post Login 设置。

如果您选择提示用户，请指定超时时间段并选择在 Default Post Login Selection 区域中该时间段过期后要采取的默认操作。

步骤 4 单击 **OK** 并确保将更改应用到组策略中，然后单击 **Save**。

允许用户延期升级

您可以强制用户通过禁用 AutoUpdate 接受 AnyConnect 更新，如禁用 AnyConnect 自动更新中所述。默认情况下，AutoUpdate 为启用状态。

也可以允许用户延迟客户端更新，直到以后设置“延期更新”(Deferred Update)。如果配置了“延期更新”(Deferred Update)，当客户端更新可用时，AnyConnect 会打开一个对话框，询问用户是希望立即更新，还是希望延迟更新。所有 Windows、Linux 和 OS X 都支持 Deferred Upgrade（延期更新）。

在 ASA 上配置延迟更新

在 ASA 上，通过添加定制属性，然后在组策略中引用和配置这些属性，可以启用延迟更新。必须创建并配置**所有**自定义属性以使用延迟升级。

向 ASA 配置添加定制属性的过程取决于所运行的 ASA/ASDM 版本。请根据您部署的 ASA/ASDM 版本，参阅 *Cisco ASA* 系列 *VPN ASDM* 配置指南或 *Cisco ASA* 系列 *VPN CLI* 配置指南，了解定制属性配置过程。

以下属性和值用于在 ASDM 中配置延迟更新：

定制属性 *	有效值	默认值	备注
DeferredUpdateAllowed	true false	False	True 可以启用延迟更新。如果延迟更新被禁用 (false)，以下设置会被忽略。

定制属性 *	有效值	默认值	备注
DeferredUpdateMinimumVersion	*x.x.x*	0.0.0	实现更新可延迟所必须要安装的最低 AnyConnect 版本。 此最低版本检查适用于在前端上启用的所有模块。如果启用的任意模块（包括 VPN）未安装或不符合最低版本要求，则连接不符合延迟更新条件。 如果未指定此属性，无论在终端上安装的版本如何，系统都会显示（或自动关闭）延迟提示。
DeferredUpdateDismissTimeout	0-300 （秒）	150 秒	延迟升级提示在自动关闭之前显示的秒数。仅当显示延迟更新提示时才应用此属性（先评估最低版本属性）。 如果此属性缺失，则禁用自动关闭功能，对话框会一直显示（如需要），直到用户作出响应。 将此属性设置为零，则允许根据以下条件强制进行自动延迟或升级： • 已安装的版本和 DeferredUpdateMinimumVersion 的值。 • DeferredUpdateDismissResponse 的值。
DeferredUpdateDismissResponse	延迟更新	更新	发生 DeferredUpdateDismissTimeout 时采取的操作。

* 定制属性值区分大小写。

在 ISE 中配置延期更新

过程

步骤 1 遵循以下步骤进行导航：

a) 选择 **Policy** > **Results**。
b) 展开 **Client Provisioning**。
c) 选择 **Resources**，然后单击 **Add** > **Agent Resources from Local Disk**。
d) 上传 AnyConnect pkg 文件，然后选择 **Submit**。

步骤 2 上载您创建的任何其他 AnyConnect 资源。

步骤 3 在 **Resources** 上，使用您上传的 AnyConnect 软件包添加 **AnyConnect Configuration**。AnyConnect Configuration 具有用于配置延期更新的字段。

延期更新 GUI

下图显示当有更新可用且配置了延迟更新时用户看到的用户界面。图的右边部分显示当配置了 **DeferredUpdateDismissTimeout** 时的用户界面。

设置更新策略

更新策略概述

如果 AnyConnect 软件和配置文件更新可用且客户端允许更新，则可在连接到前端时进行更新。为 AnyConnect 更新配置前端，以便可以进行更新。VPN 本地策略文件中的更新策略设置决定了是否允许更新。

更新策略有时被称之为软件锁定。如果配置了多个前端，更新策略也称之为多域策略。

默认情况下，更新策略设置允许来自任何前端的软件和配置文件更新。请按如下方式设置更新策略参数以限制此操作：

- 通过在 **Server Name** 列表中指定头端，允许或授权特定头端更新所有 AnyConnect 软件和配置文件。

  前端服务器名可以是 FQDN 或 IP 地址。同时也可以是通配符，例如：*.example.com。

  有关更新发生方式的完整说明，请参阅以下已授权服务器更新策略行为。

- 对于所有其他未指定或未授权的前端：
  - 使用 **Allow Software Updates From Any Server** 选项，允许或拒绝 VPN 核心模块和其他可选模块的软件更新。
  - 使用 **Allow VPN Profile Updates From Any Server** 选项，允许或拒绝 VPN 配置文件更新。
  - 使用 **Allow Service Profile Updates From Any Server** 选项，允许或拒绝其他服务模块配置文件更新。
  - 使用 **Allow ISE Posture Profile Updates From Any Server** 选项，允许或拒绝 ISE 终端安全评估配置文件更新。
  - 使用 **Allow Compliance Module Updates From Any Server** 选项，允许或拒绝合规性模块更新。

有关更新发生方式的完整说明，请参阅以下未授权的服务器更新策略行为。

已授权服务器更新策略行为

当连接到 **Server Name** 列表中的已授权头端时，其他更新策略参数不适用并且会出现以下情况：

- 比较前端上 AnyConnect 软件包的版本与客户端版本，以确定软件是否应该更新。
  - 如果 AnyConnect 软件包的版本比客户端上的版本旧，则不进行软件更新。
  - 如果 AnyConnect 软件包的版本与客户端上的版本相同，则只下载和安装在前端上配置以供下载并且在客户端上不存在的软件模块。
  - 如果 AnyConnect 软件包的版本比客户端的版本新，则下载和安装前端上为下载配置的软件模块以及客户端上已安装的软件模块。
- 前端上的 VPN 配置文件、ISE 终端安全评估配置文件和每个服务配置文件都将与客户端上的配置文件进行比较以确定是否应更新：
  - 如果前端的配置文件与客户端的配置文件相同，则不会进行更新。
  - 如果前端的配置文件与客户端的配置文件不同，则会进行下载。

未授权的服务器更新策略行为

连接到未授权的头端时，系统将通过 **Allow ... Updates From Any Server** 选项确定 AnyConnect 的更新方式，如下所述：

- **Allow Software Updates From Any Server:**
  - 如果选中此选项，则允许对此未授权的 ASA 进行软件更新。根据对上述授权前端的版本比较进行更新。
  - 如果未选中此选项，则不会进行软件更新。此外，如果基于版本比较发生更新，系统将终止 VPN 连接尝试。
- **Allow VPN Profile Updates From Any Server:**
  - 如果选中此选项，则当前端的 VPN 配置文件与客户端的配置文件不同时，对 VPN 配置文件进行更新。
  - 如果未选中此选项，则不会更新 VPN 配置文件。此外，如果基于差异发生 VPN 配置文件更新，系统将终止 VPN 连接尝试。
- **Allow Service Profile Updates From Any Server:**
  - 如果选中此选项，则当前端的配置文件与客户端的配置文件不同时，对每个服务配置文件进行更新。
  - 如果未选中此选项，则不会更新服务配置文件。

- **Allow ISE Posture Profile Updates From Any Server:**
  - 如果选中此选项，则在前端 ISE 终端安全评估配置文件不同于客户端 ISE 终端安全评估配置文件时，更新 ISE 终端安全评估配置文件。
  - 如果未选中此选项，则不会更新 ISE 终端安全评估配置文件。ISE 终端安全评估代理需要具备 ISE 终端安全评估配置文件才能运行。
- **Allow Compliance Module Updates From Any Server:**
  - 如果选中此选项，则在前端合规性模块不同于客户端合规性模块时更新合规性模块。
  - 如果未选中此选项，则不更新合规性模块。ISE 终端安全评估代理需要具备合规性模块才能运行。

更新策略指南

- 通过在授权的 **Server Name** 列表中列出服务器的 IP 地址，远程用户可以使用该 IP 地址连接到头端。如果用户尝试使用 IP 地址连接，但前端被列为 FQDN，那么该尝试将被视为连接到未授权的域。
- 软件更新包括下载定制、本地化、脚本和转换。在禁止软件更新时，将不会下载这些项目。如果某些客户端不允许脚本更新，请不要依赖脚本来实施策略。
- 下载启用永不间断的 VPN 配置文件将删除客户端上的所有其他 VPN 配置文件。在决定允许或拒绝从未授权前端或非企业前端更新 VPN 配置文件时，请注意这一点。
- 如果因安装和更新策略而未能将 VPN 配置文件下载到客户端，则以下功能将不可用：

服务禁用	不受信任网络策略
证书存储区覆盖	受信任的 DNS 域
显示预连接消息	受信任 DNS 服务器
本地局域网接入	永不间断
在登录前启动	强制网络门户补救
本地代理连接	脚本编写
PPP 排除	注销时保持 VPN
自动 VPN 策略	需要设备锁定
受信任的网络策略	自动服务器选择

- 下载程序将创建一个单独的文本日志 (UpdateHistory.log) 来记录下载历史信息。此日志包含更新时间、更新客户端的 ASA、更新的模块以及升级前后安装的版本。此日志文件存储于：

  `%AllUsers%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Logs` 目录。

更新策略示例

此示例显示了客户端上的 AnyConnect 版本不同于各 ASA 前端时客户端的更新行为。

假定 VPN 本地策略 XML 文件中的更新策略如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
xmlns=http://schemas.xmlsoap.org/encoding/
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
<FipsMode>false</FipsMode>
<BypassDownloader>false</BypassDownloader><RestrictWebLaunch>false</RestrictWebLaunch>
<StrictCertificateTrust>false</StrictCertificateTrust>
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>
<RestrictTunnelProtocols>false</RestrictTunnelProtocols>
<UpdatePolicy>
<AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>false</AllowISEProfileUpdatesFromAnyServer>
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AuthorizedServerList>
    <ServerName>seattle.example.com</ServerName>
    <ServerName>newyork.example.com</ServerName>
    </AuthorizedServerList>
</UpdatePolicy>
</AnyConnectLocalPolicy>
```

有以下 ASA 前端配置：

ASA 前端	加载的 **AnyConnect** 软件包	要下载的模块
seattle.example.com	版本 4.7.01076	VPN、网络访问管理器、网络安全
newyork.example.com	版本 4.7.03052	VPN、网络访问管理器
raleigh.example.com	版本 4.7.04056	VPN、终端安全评估

当客户端当前运行 AnyConnect VPN 和网络访问管理器模块时，可能出现以下更新序列：

- 客户端连接到 seattle.example.com，这是一个采用相同版本的 AnyConnect 来配置的授权服务器。下载并安装了网络安全软件模块和网络安全配置文件（如果可用）。如果 VPN 和网络访问管理器配置文件可供下载，且不同于客户端上的 VPN 和配置文件，则也会被下载。
- 客户端随后连接到 newyork.example.com，这是一个采用较新版本的 AnyConnect 来配置的授权 ASA。下载并安装了 VPN、网络访问管理器和网络安全模块。若配置文件可供下载且不同于客户端上的配置文件，则也会被下载。
- 客户端随后连接到 raleigh.example.com，这是一个未授权的 ASA。因为允许软件更新，所以 VPN、网络访问管理器、网络安全和终端安全评估模块均会升级。由于不允许更新 VPN 配置文件和服务配置文件，因此无法下载这些配置文件。如果认为 VPN 配置文件已更新（基于差异），则连接将终止。

AnyConnect 参考信息

本地计算机上用户首选项文件的位置

AnyConnect 将某些配置文件设置存储在用户计算机上的用户首选项文件和全局首选项文件中。AnyConnect 使用本地文件配置客户端 GUI 上 Preferences 选项卡中用户可控制的设置并显示有关最新连接的信息，如用户、组和主机。

AnyConnect 使用全局文件来配置登录之前发生的操作，例如 Start Before Logon 和 AutoConnect On Start。

下表显示客户端计算机上首选项文件的文件名和安装路径：

操作系统	类型	文件和路径
Windows	用户	C:\Users\username\AppData\Local\Cisco\ Cisco AnyConnect VPN Client \ preferences.xml
	全局	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\ preferences_global.xml
macOS	用户	/Users/username/.anyconnect
	全局	/opt/cisco/anyconnect/.anyconnect_global
Linux	用户	/home/username/.anyconnect
	全局	/opt/cisco/anyconnect/.anyconnect_global

AnyConnect 和传统 VPN 客户端使用的端口

下表列出了传统思科 VPN 客户端使用的端口和每个协议的 Cisco AnyConnect Secure Mobility Client 。

协议	思科 AnyConnect 客户端端口
TLS (SSL)	TCP 443
SSL 重定向	TCP 80（可选）
DTLS	UDP 443（可选，但强烈推荐）
IPsec/IKEv2	UDP 500、UDP 4500

协议	思科 VPN 客户端 (IPsec) 端口
IPsec/NATT	UDP 500、UDP 4500
IPsec/NATT	UDP 500、UDP 4500
IPsec/TCP	TCP（可配置）

协议	思科 VPN 客户端 (IPsec) 端口
IPsec/UDP	UDP 500、UDP X（可配置）