部署 Cisco Secure Client

准备工作

以下项目符号列表突出显示与 AnyConnect 安全移动客户端 4.x 版本不同的关键支持、命名和功能更改。对于版本 5，AnyConnect 安全移动客户端已重命名为 Cisco Secure Client。

- 虽然网络访问管理器是 Cisco Secure Client 5.0 的一部分，但 SecureX 中的网络访问管理器配置文件编辑器将不适用于版本 5。
- AMP 启用程序仅适用于 Cisco Secure Client 5 中的 macOS，因为适用于 Windows 的 Cisco Secure Client 提供与 Cisco Secure Endpoint（原先的面向终端的高级恶意软件防护）的完全集成。
- 某些 AnyConnect 模块在 Cisco Secure Client 5 版本中也有新名称。HostScan（VPN 安全评估）将更改为 Cisco Secure Firewall 终端安全评估。在 ASDM UI 的 Remote Access VPN 窗口中，您将看到它被引用为终端安全评估（用于 Cisco Secure Firewall）。同样，从 Cisco.com 下载的 hostscan.pkg 将重命名为 secure-firewall-posture-版本-k9.pkg。
- 您会注意到文档和 ASDM UI 中对 AnyConnect 的引用。我们目前不打算将这些引用更改为新的 Cisco Secure Client名称，但完全支持 ASDM 来配置 Cisco Secure Client 5 配置文件。Cisco Secure Firewall ASA ASA 将是版本 9.18 及更高版本的新 ASA 名称。
- 第 5 版已移除 Umbrella 漫游安全模块为所有已安装 Umbrella 云基础设施的 AnyConnect 模块提供自动更新的功能。
- AnyConnect 的 Apex 和 Plus 许可证已更改为 Cisco Secure Client 的 Premier 和 Advantage 许可证。

Cisco Secure Client 部署概述

部署 Cisco Secure Client 是指安装、配置和升级 Cisco Secure Client 及其相关文件。

Cisco Secure 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。此部署选项不提供云管理。
- 网络部署 - 将 Cisco Secure Client 软件包载入头端，即 Cisco Secure Firewall ASA、Cisco Secure Firewall Threat Defense 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 Cisco Secure Client 部署到客户端。此部署选项不提供云管理。
  - 对于新安装，用户可连接到前端以下载 Cisco Secure Client。客户端可手动或自动安装（通过网络启动）。
  - 更新由已安装 Cisco Secure Client 的系统上运行的 Cisco Secure Client 完成，或者通过将用户定向至 Cisco Secure Firewall ASA 无客户端门户完成。
- SecureX 云管理部署 - 选择要启用的 Cisco Secure Client 选项后（例如“登录前启动”(Start Before Login)、“诊断和报告工具”(Diagnostics and Reporting Tool)、“Cisco Secure Firewall 终端安全评估”(Secure Firewall Posture)、“Network Visibility Module”、“安全 Umbrella”(Secure Umbrella)、“ISE 终端安全评估”(ISE Posture) 和“网络访问管理器”(Network Access Manager)），您可以点击 SecureX UI 的“部署管理”(Deployment Management) 页面上的**网络安装程序 (Network Installer)** 按钮。此操作会下载 csc-deployment.exe 文件，然后可以在命令提示符中执行该文件以安装云管理服务。云管理服务会自动下载您配置的模块并将您连接到 SecureX 云。然后，您可以选择在没有软件包或配置文件管理的情况下进行云注册，或者使用完整的云管理。Cisco Secure Client 可以与云管理一起使用，也可以不与云管理一起使用。
- 在 XDR 中，您可以导航至“客户端管理”(Client Management) > “部署”(Deployments) 以查看思科 XDR 组织中所有安全客户端部署的列表，并允许用户定义必须在特定部署中的所有计算机上安装的所有软件包和相关配置文件的列表一个组织。有关详细信息，请参阅 XDR 文档。

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

有关 Cisco Secure Firewall ASA、IOS、Microsoft Windows、Linux 和 macOS 的系统、管理和终端要求，请参阅 Cisco Secure Client 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 Cisco Secure Client 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。

此外，第三方安全应用程序 (AV/AS/AM/DLP) 可能会导致合规模块升级失败，这是因为交互会导致终端上缺少库。要避免这些问题，可在升级合规模块之前升级合规模块版本并将这些设为排除（在第三方安全应用程序中）：

```
-cisco-secure-client-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k0.pkg
-cisco-secure-client-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k9.exe
-cisco-secure-client-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k9.msi
-opswat.msi
```

合规性模块不是 SecureX 云管理部署的一部分。

决定如何安装 Cisco Secure Client

Cisco Secure Client 可以由 ISE 2.0（或更高版本）和 Cisco Secure Firewall ASA 头端进行网络部署，或者进行预部署。安装 Cisco Secure Client 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/Cisco Secure Firewall Threat Defense）升级 Cisco Secure Client 或安装额外模块，您不需要管理权限。

由于新的 Apple API 更改，当使用 webdeploy 从 macOS Cisco Secure Client 5.0.x（或更低版本）升级到 5.1.x（或更高版本）时，您必须具有管理员权限或通过 MDM 管理 macOS 设备才能预先批准应用扩展。此限制不适用于 Windows 或 Linux。

- 从 Cisco Secure Firewall ASA 或 Cisco Secure Firewall Threat Defense 设备进行网络部署 - 用户连接到头端设备上的 Cisco Secure Client 无客户端网络门户，然后选择下载 Cisco Secure Client。Cisco Secure Firewall ASA 将下载 Cisco Secure Client 下载程序。Cisco Secure Client 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 Cisco Secure Firewall 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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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 macOS，是 DMG；对于 Linux，是 gzip。

有关系统要求和许可依赖性，请参阅《Cisco Secure Client功能、许可证和操作系统指南》。

注释 如果您使用 Cisco Secure Firewall 终端安全评估 在 macOS 或 Linux 平台上执行根权限活动，我们建议您预部署 Cisco Secure Firewall 终端安全评估 终端安全评估。

确定安装 Cisco Secure Client 所需的资源

部署 Cisco Secure Client 需要多种类型的文件：

- AnyConnect VPN，它包含在 Cisco Secure Client 软件包中。
- 支持额外功能的模块，包含在 Cisco Secure Client 软件包中。
- 配置 Cisco Secure Client 和额外功能的客户端配置文件，您可以创建这些配置文件。
- 如果您要自定义或本地化部署，还可以使用语言文件、图像、脚本和帮助文件。
- ISE 终端安全评估和合规性模块 (OPSWAT)。

为 Cisco Secure Client 准备终端

结合使用 Cisco Secure Client 和移动宽带卡

某些 3G 卡在使用 Cisco Secure Client 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 (LAN adapter auto connect)**，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 Cisco Secure Client 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 Cisco Secure Client 接口时，3G 管理器将丢弃接口并允许 Cisco Secure Client 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），Cisco Secure Client 将在断开旧连接之前建立新连接。

阻止 Internet Explorer 中的代理更改

某些情况下，Cisco Secure Client 会隐藏（锁定）Internet Explorer 的“工具 > Internet 选项 > 连接”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：

- Cisco Secure Firewall ASA 配置指定“连接”(Connections) 选项卡锁定
- Cisco Secure Firewall ASA 配置指定私有端代理
- Windows 组策略之前锁定了“连接”选项卡（覆盖未锁定 Cisco Secure Firewall 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，Cisco Secure Client 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。

步骤 1 在 ASDM 中，转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **组策略 (Group Policies)**。

步骤 2 选择组策略，点击**编辑 (Edit)** 或**添加 (Add)** 可编辑或新增组策略。

步骤 3 在导航窗格中，转到**高级 (Advanced)** > **浏览器代理 (Browser Proxy)**。系统显示 Proxy Server Policy 窗格。

步骤 4 点击**代理锁定 (Proxy Lockdown)** 以显示更多代理设置。

步骤 5 取消选中**继承 (Inherit)** 并选择以下两个选项之一：

- **是**，将启用代理锁定，并在 Cisco Secure Client 会话期间隐藏 Internet Explorer 的“连接”选项卡。
- **否**，将禁用代理锁定，并在 Cisco Secure Client 会话期间显示 Internet Explorer 的“连接”选项卡。

步骤 6 点击**确定 (OK)** 保存代理服务器策略更改。

步骤 7 点击**应用 (Apply)** 保存组策略更改。

配置 Cisco Secure Client 如何处理 Windows RDP 会话

可以将 Cisco Secure Client 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 Secure 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。这些首选项在 VPN 客户端配置文件中配置：

Windows 登录实施 (Windows Logon Enforcement) - 在 SBL 模式下可用

- 单点本地登录 (Single Local Logon)（默认设置）-（本地：1，远程：无限制）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 连接进行了分割隧道配置，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。

- 单一登录 (Single Logon) -（本地 + 远程：1）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。

注释 不支持多个用户同时登录。

- 单一登录无远程 (Single Logon No Remote) -（本地：1，远程：0）在整个 VPN 连接期间只允许一个本地用户登录。不允许任何远程用户。如果在建立VPN连接后，有多个本地用户或任何远程用户登录，则将不允许此连接。如果VPN连接期间有第二个本地用户或任何远程用户登录，则此 VPN 连接将终止。

Windows VPN 建立 (Windows VPN Establishment) - 在 SBL 模式下不可用

- 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。

配置 Cisco Secure Client 如何处理 Linux SSH 会话

可以将 Cisco Secure Client 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 Secure 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 (Linux Login Enforcement) — 单点本地登录 (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连接进行了分割隧道配置，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 —

- 仅限本地用户（默认）- 阻止远程登录的用户建立 VPN 连接。
- Allow Remote Users - 允许远程用户建立 VPN 连接。

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 Cisco Secure Firewall ASA 上配置仅使用 DES，Cisco Secure Client 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 Cisco Secure Firewall ASA 配置为仅使用 DES 的 SSL 加密。

在 Linux 上使用 Network Visibility Module

在 Linux 上使用 Network Visibility Module 之前，必须设置内核驱动程序框架 (KDF)。您可以选择预构建 Cisco Secure Client 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 Cisco Secure Client 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。
  - 对于 Linux，安装所需的 libelf devel 软件包。
- 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 Cisco Secure Client Linux 内核模块打包在一起

开始之前

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

Cisco Secure Client Network Visibility Module 可以通过预构建的 Cisco Secure Client 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前提条件，可以使用预构建选项。

注释 预构建的 Cisco Secure Client Linux 内核模块不支持 Web 部署。

步骤 1 提取 Cisco Secure Client 预部署软件包：cisco-secure-client-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**。

下一步做什么

在运行脚本后，将创建 cisco-secure-client-linux64-<版本>-**ac_kdf_ko-k9.tar.gz**，其包括 Cisco Secure Client 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。

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 Cisco Secure Client Network Visibility Module。

预部署 Cisco Secure Client

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

当创建文件存档以安装 Cisco Secure Client 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，如预部署 Cisco Secure Client 配置文件的位置，第 11 页中所述：

开始之前

- 在 SecureX 中创建或部署配置文件时，请确保遵循以下两个要求：
  - 配置文件名称（适用于 VPN 或任何 Cisco Secure 模块配置文件）必须与在 ASA/FTD 头端和/或 ISE 中创建和配置的配置文件的名称完全匹配。
  - 要确保配置文件在所有终端和部署之间保持同步，还必须将在 SecureX 中创建的配置文件导入到 ASA/FTD 头端和/或 ISE 中。

    如果不符合上述要求，配置文件将不会在所有环境中保持同步，并且可能会禁用现有部署中当前配置的某些功能。例如，如果您在使用 VPN 时需要远程桌面功能，则必须 1) 在 SecureX 上的 VPN 配置文件中启用远程桌面功能，并且 2) 在 ASA/FTD 和/或 ISE 环境中配置的配置文件中启用该功能。

    如果要分发带外配置文件（使用 SCCM、MDM、SecureX 云管理等），而不在 Cisco Secure Firewall ASA 上配置 Cisco Secure Client 配置文件（以前称为 AnyConnect 配置文件），则可以使用 *UseLocalProfileAsAlternative* 自定义属性。在配置此自定义属性时，客户端会将本地（磁盘上）Cisco Secure Client 配置文件用于其设置和首选项（而不是通常的默认值）。仅当 1) 将 *UseLocalProfileAsAlternative* 设为已启用，并且 2) 未配置 ASA 组策略配置文件时，才会使用本地配置文件来建立会话。如果配置此自定义属性，并且未从 ASA 上的组策略配置中撤消或删除 Cisco Secure Client 配置文件，则在组策略上配置的 Cisco Secure Client 配置文件将保留并用于每个连接，其中自定义属性设置将被忽略。有关其他信息，请参阅

《*Cisco Secure Firewall ASA* 系列 *VPN ASDM* 配置指南》中的 在内部组策略中配置安全客户端自定义属性。

- 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，Cisco Secure Client 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 Cisco Secure Client 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 使用 Cisco Secure Client 克隆虚拟机的准则（仅限 Windows），第 14 页。

步骤 1 下载 Cisco Secure Client 预部署软件包。

用于预部署的 Cisco Secure Client 文件在 cisco.com 上提供。

操作系统	**Cisco Secure Client** 预部署软件包名称
Windows	cisco-secure-client-win-版本-predeploy-k9.zip
macOS	cisco-secure-client-macos-版本-predeploy-k9.dmg
Linux（64位）	（对于脚本安装程序）cisco-secure-client-linux64-版本-predeploy-k9.tar.gz （对于 RPM 安装程序）cisco-secure-client-linux64-版本-predeploy-rpm-k9.tar.gz （对于 DEB 安装程序）cisco-secure-client-linux64-版本-predeploy-deb-k9.tar.gz

Secure Umbrella 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。

以下模块需要创建 Cisco Secure Client 配置文件：

- AnyConnect VPN
- 网络访问管理器
- ISE 终端安全评估
- Cisco Secure Endpoint
- Network Visibility Module
- Umbrella 漫游安全模块

以下模块不需要创建 Cisco Secure Client 配置文件：

- 登录前开始

- 诊断和报告工具
- Cisco Secure Firewall 终端安全评估
- 客户体验反馈
- ThousandEyes Endpoint Agent 模块

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。

步骤 3 或者自定义和本地化 Cisco Secure Client 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 Cisco Secure Client 配置文件的位置中进行了描述。

步骤 5 创建 Cisco Secure Client 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（Cisco Secure Firewall ASA 和 ISE 等）上也有相同的 Cisco Secure Client 文件。

用于预部署和网络部署的 Cisco Secure Client 模块可执行文件

下表列出了在将 Zero Trust 访问模块、Umbrella 漫游安全模块、网络访问管理器、ISE 终端安全评估、Network Visibility Module 和 Thousand Eyes 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
Zero Trust 访问	cisco-secure-client-win-<版本>-zta-webdeploy-k9.msi	cisco-secure-client-win-<版本>-zta-predeploy-k9.msi
网络访问管理器	cisco-secure-client-win-版本-nam-webdeploy-k9.msi	cisco-secure-client-win-版本-nam-predeploy-k9.msi
ISE 终端安全评估	cisco-secure-client-win-版本 -iseposture-webdeploy-k9.msi	cisco-secure-client-win-版本 -iseposture-predeploy-k9.msi
Network Visibility Module	cisco-secure-client-win-版本-nam-webdeploy-k9.msi	cisco-secure-client-win-版本-nvm-predeploy-k9.msi
Umbrella 漫游安全模块	cisco-secure-client-win-版本 -umbrella-webdeploy-k9.msi	cisco-secure-client-win-版本 -umbrella-predeploy-k9.msi
ThousandEyes Endpoint Agent 模块	n/a	cisco-secure-client-win-版本 -thousandeyes-predeploy-k9.msi

注释 如果有 Windows 服务器操作程序，在尝试安装网络访问管理器时，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 Cisco Secure Client 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: Cisco Secure Client* 核心文件

文件	描述
anyfilename.xml	Cisco Secure Client 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。Cisco Secure Client 将使用此文件来验证配置文件。

表 *3:* 所有操作系统的配置文件位置

模块	位置
Windows 的 ISE 安全评估代理	
AnyConnect VPN 配置文件	%ProgramData%\Cisco\Cisco Secure Client\VPN\Profile
Zero Trust 访问	（二进制文件）C:\Program Files (x86)\Cisco\Cisco Secure Client\ZTA （配置和其他文件）C:\ProgramData\Cisco\Cisco Secure Client\ZTA
网络访问管理器	%ProgramData%\Cisco\ Cisco Secure Client\Network Access Manager\newConfigFiles
客户体验反馈	%ProgramData%\Cisco\ Cisco Secure Client\CustomerExperienceFeedback
ISE 终端安全评估	%ProgramData%\Cisco\Cisco Secure Client\ISE Posture
Cisco Secure Endpoint	%ProgramData%\Cisco\AMP
Network Visibility Module	%ProgramData%\Cisco\Cisco Secure Client\NVM

模块	位置
Umbrella 漫游安全模块	%ProgramData%\Cisco\Cisco Secure 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。
macOS	
ISE 终端安全评估	/opt/cisco/secureclient/iseposture/
AMP Enabler	/opt/cisco/secureclient/AMPEnabler/
Network Visibility Module	/opt/cisco/secureclient/NVM/
Umbrella 漫游安全模块	/opt/cisco/secureclient/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。
AnyConnect VPN 配置文件	/opt/cisco/secureclient/vpn/profile
Linux	
NVM	/opt/cisco/secureclient/NVM
AnyConnect VPN 配置文件	/opt/cisco/secureclient/vpn/profile

其他 Cisco Secure Client 文件位置

自定义和本地化 - Windows

- **L10N**
  - %ALLUSERSPROFILE%\Cisco\Cisco Secure Client\l10n
- 资源
  - %PROGRAMFILES%\Cisco\Cisco Secure Client\UI\res

自定义和本地化 - **macOS** 和 **Linux**

- **L10N**
  - /opt/cisco/secureclient/l10n
- 资源
  - /opt/cisco/secureclient/resources

macOS 二进制文件、库和 **UI** 资源

- 用户界面资源
  - /Applications/Cisco/Cisco Secure Client.app/Contents/Resources/
- 二进制文件
  - /opt/cisco/secureclient/bin
- 库
  - /opt/cisco/secureclient/lib

帮助

- **Windows** 的 **ISE** 安全评估代理
  - %ALLUSERSPROFILE%\Cisco\Cisco Secure Client\Help
- **macOS** 和 **Linux**
  - /opt/cisco/secureclient/help

OPSWAT 库

由 ISE 终端安全评估和 Cisco Secure Firewall 终端安全评估 使用

- **Windows** 的 **ISE** 安全评估代理
  - %PROGRAMFILES%\Cisco\Cisco Secure Client\OPSWAT
- **macOS**

  /opt/cisco/secureclient/lib/opswat

使用 Cisco Secure Client 克隆虚拟机的准则（仅限 Windows）

Cisco Secure Client 终端由 Cisco Secure Client 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 Cisco Secure Client 之前执行此操作：

1. 导航至 **%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART**，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 Cisco Secure Client 模块预部署为独立应用

某些模块（例如网络访问管理器、Umbrella 漫游安全模块或 ThousandEyes Endpoint Agent 模块）可以作为独立应用运行。已安装思科安全客户端，但未使用 VPN 和 Cisco Secure Client UI。

在 Windows 上使用 SMS 部署独立模块

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 cisco-secure-client-win-版本-core-vpn-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 Umbrella：

```
msiexec /package cisco-secure-client-win-版本-umbrella-predeploy-k9.msi /norestart /passive /lvx*
c:\test.log
```

步骤 3 （可选）安装 DART。

```
misexec /package cisco-secure-client-win-版本-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 Cisco Secure Client 服务。

将 Cisco Secure Client 模块部署为独立应用

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 Cisco Secure Client 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。

步骤 1 指示用户选中“安全客户端网络访问管理器”、“安全 Umbrella 模块”或“ThousandEyes Endpoint Agent 模块”。

步骤 2 指导用户取消选中**思科AnyConnect VPN 模块 (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、安全 Umbrella 模块或 ThousandEyes Endpoint Agent 模块作为不含 VPN 功能的独立应用来安装。

步骤 3 （可选）选中**锁定组件服务 (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 Cisco Secure Client GUI。如果用户点击“安装已选定”(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、Umbrella 漫游安全模块或 ThousandEyes Endpoint Agent 的选择。
b) 如果用户点击“确定”(OK)，安装实用程序将使用 PRE_DEPLOY_DISABLE_VPN=1 设置调用 Cisco Secure Client 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、安全 Umbrella 或 ThousandEyes Endpoint Agent 模块安装程序。
e) 计算机将启用网络访问管理器、安全 Umbrella 模块或 ThousandEyes Endpoint Agent，但不含 VPN 服务。

预部署到 Windows

使用 zip 文件分发 Cisco Secure Client

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 Cisco Secure Client 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 Cisco Secure Client 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。

Cisco Secure Client zip 文件内容

文件	目的
GUI.ico	Cisco Secure Client 图标图像。
Setup.exe	启动安装实用程序。
cisco-secure-client-win-版本-dart-predeploy-k9.msi	DART 模块的 MSI 安装程序文件。
cisco-secure-client-win-<版本>-zta-predeploy-k9.msi	Zero Trust 访问的 MSI 安装程序文件
cisco-secure-client-win-版本-SBL-predeploy-k9.msi	SBL 模块的 MSI 安装程序文件。
cisco-secure-client-win-版本-iseposture-predeploy-k9.msi	ISE 终端安全评估模块的 MSI 安装程序。
cisco-secure-client-win-版本-nvm-predeploy-k9.msi	Network Visibility Module 的 MSI 安装程序文件。
cisco-secure-client-win-版本-umbrella-predeploy-k9.msi	Umbrella 漫游安全模块的 MSI 安装程序文件。
cisco-secure-client-win-版本-nam-predeploy-k9.msi	网络访问管理器模块的 MSI 安装程序文件。
cisco-secure-client-win-版本-posture-predeploy-k9.msi	终端安全评估模块的 MSI 安装程序文件。
cisco-secure-client-win-版本-thousandeyes-predeploy-k9.msi	ThousandEyes Endpoint Agent 模块的 MSI 安装程序文件。
cisco-secure-client-win-版本-core-predeploy-k9.msi	AnyConnect VPN 模块的 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自定义。

使用 SMS 分发 Cisco Secure Client

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 Cisco Secure Client 时，必须禁用 AlwaysInstallElevated 或 Windows 用户帐户控制 (UAC) 组策略设置。否则，Cisco Secure Client 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 Cisco Secure Firewall 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。
- 下表提供了有关日志文件名的建议。通过遵循建议，您将获得可预测的位置，从而更轻松地在 DART 集合中查找所需的日志。同样，所提供的一些示例命令可能会提供您不需要的功能。例如，客户体验反馈命令会禁用反馈，默认情况下该反馈处于启用状态。

Windows 预部署 MSI 示例

已安装的模块	命令和日志文件
Cisco Secure 核心客户端：无 VPN 功能。 （在安装独立模块时使用。）	msiexec /package cisco-secure-client-win-版本-core-vpn-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* cisco-secure-client-win-版本-core-vpn-predeploy-k9-install-datetimestamp.log
有 VPN 功能的 Cisco Secure 核心客户端。 （除安装独立模块外，所有情况下均可使用。）	msiexec /package cisco-secure-client-win-版本-core-vpn-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-版本-core-vpn-predeploy-k9-install-datetimestamp.log
Zero Trust 访问	msiexec /package cisco-secure-client-win-版本-zta-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-<版本>-zta-predeploy-k9-install-datetimestamp.log

已安装的模块	命令和日志文件
客户体验反馈	msiexec /package cisco-secure-client-win-版本-core-vpn-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* cisco-secure-client-win-版本-core-vpn-predeploy-k9-install-datetimestamp.log
诊断和报告工具 (DART)	msiexec /package cisco-secure-client-win-版本-dart-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-版本-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package cisco-secure-client-win-版本-SBL-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-版本-SBL-predeploy-k9-install-datetimestamp.log
网络访问管理器	msiexec /package cisco-secure-client-win-版本-nam-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-版本-nam-predeploy-k9-install-datetimestamp.log
Cisco Secure Firewall 终端安全评估	msiexec /package cisco-secure-client-win-版本-posture-predeploy-k9.msi /norestart/passive /lvx* cisco-secure-client-win-版本-posture-predeploy-k9-install-datetimestamp.log
ISE 终端安全评估	msiexec /package cisco-secure-client-win-版本-iseposture-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-版本-iseposture-predeploy-k9-install-datetimestamp.log
Network Visibility Module	msiexec /package cisco-secure-client-win-版本-nvm-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-版本-nvm-predeploy-k9-install-datetimestamp.log
Umbrella 漫游安全	msiexec /package cisco-secure-client-win-版本-umbrella-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-版本-umbrella-predeploy-k9-install-datetimestamp.log
ThousandEyes Endpoint Agent 模块	msiexec /package cisco-secure-client-win-版本-thousandeyes-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-版本-thousandeyes-predeploy-k9-install-datetimestamp.log

Cisco Secure Client 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 Secure 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。启用锁定服务选项后，如果您具有管理员权限，还可以卸载所有 Cisco Secure Client模块。

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 (tools-cisco-secure-client-win-X.X.xxxx-transforms.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 Cisco Secure Client

您可以隐藏安装的 Cisco Secure Client 模块，这样用户从 Windows Add/Remove Program 列表中便看不到该模块。您无法启动或停止 Cisco Secure Client 服务。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 (tools-cisco-secure-client-win-X.X.xxxxx-transforms.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 Cisco Secure Client 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。

步骤 1 按以下顺序安装 Cisco Secure Client 模块：

a) 安装 Cisco Secure Client 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 Cisco Secure Client 卸载期间或安装升级过程中，此帐户会被删除。

b) 安装 Cisco Secure Client 诊断和报告工具 (DART) 模块，以提供有关 Cisco Secure Client安装的有用诊断信息。

c) 按任意顺序安装 Umbrella 漫游安全、Network Visibility Module、、SBL、网络访问管理器、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 Cisco Secure Client 模块：

a) 按任意顺序卸载 Umbrella 漫游安全、Network Visibility Module、、网络访问管理器、终端安全评估、ISE 合规性模块或 SBL。

b) 卸载 Cisco Secure Client 核心客户端模块。

c) 最后卸载 DART。

如果卸载过程失败，DART 信息会很有用。卸载安全客户端时，不会卸载ThousandEyes Endpoint Agent 模块。它需要自己卸载。

卸载 AnyConnect VPN 将卸载包括 Zero Trust 访问在内的所有模块，但 Duo Desktop 和ThousandEyes 除外。您还可以单独卸载 Zero Trust 访问。

注释 根据设计，卸载 Cisco Secure Client 后，某些 XML 文件仍然保留。

预部署到 macOS

在 macOS 上安装和卸载 Cisco Secure Client

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

Zero Trust 访问模块不是 macOS 的 webdeploy 软件包的一部分。

Cisco Secure Client 5 支持所有 Apple 支持的 macOS 11（及更高版本）版本。

要从您的发行版中删除任何 Cisco Secure Client 模块，请在访达中运行 Cisco Secure Client 卸载程序，导航至“应用”>Cisco，然后双击**卸载**。或者在 /opt/cisco/secure client/bin 中运行 VPN vpn_uninstall.sh 脚本。

卸载 AnyConnect VPN 将删除 Zero Trust 访问。此外，您可以使用 sudo 运行此外壳脚本，以仅删除 Zero Trust访问：/opt/cisco/secureclient/bin/zta_uninstall.sh

获取为 macOS 预部署配置文件的写入权限

以下过程说明了如何自定义模块、创建配置文件并将该配置文件添加到 DMG 包。在将任何文件复制到嵌入式配置文件文件夹之前，必须为安装程序映像设置写入权限。它还将 Cisco Secure Client 用户界面设置为在启动时自动启动，这使 Cisco Secure Client 可以为相应模块提供必要的用户和组信息。

步骤 1 从 Cisco.com 下载 Cisco Secure Client DMG 软件包（例如用于 Network Visibility Module 的 cisco-secure-client-macos-<版本>-*nvm*-standalone.dmg）。

步骤 2 在安装过程中，批准出现的系统扩展弹出窗口。
安装完成后，独立应用程序将安装在终端上，支持文件将放置在相应模块的 /opt/cisco/secureclient 目录下。例如，对于 Network Visibility Module，文件会被放在 /opt/cisco/secureclient/nvm 中。

步骤 3 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 4 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 5 在运行 Windows 操作系统的计算机上安装独立配置文件编辑器。必须选择所需的 Cisco Secure Client 模块作为自定义安装的一部分或进行完整安装。默认情况下不会安装这些模块。

步骤 6 启动配置文件编辑器并创建包含所需配置的配置文件。

步骤 7 以 Network Visibility Module 为例，以下步骤说明了如何正确保存配置文件。按照这些步骤，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（例如用于 Network Visibility Module 的 NVM_ServiceProfile.wso），并将其保存到与您保存该文件（如 NVM_ServiceProfile.xml）相同的位置。

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 Cisco Secure Client x.x.x/Profiles/NVM。或者，使用终端应用，如下所示的 Network Visibility Module 实例：`cp <wso 的路径> \Volumes\"Cisco Secure Client <版本>"\Profiles\nvm\`

b) 在 macOS 安装程序中，转到 Cisco Secure Client 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 功能：
`<ACTransforms><DisableVPN>true</DisableVPN></ACTransforms>`

c) Cisco Secure Client 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）。

Cisco Secure Client 的当前版本使用 Apple 颁发的证书进行签名，并由 Apple 进行认证。如果 Gatekeeper 是为 Mac 应用商店（仅）配置的，则必须选择**应用商店和确定的开发者**设置，或按住 Control 键绕过所选设置，从预先部署的安装中安装和运行 Cisco Secure Client。有关更多信息，请参阅：在 Mac 上安全打开应用

macOS 11（及更高版本）上的其他 Duo Desktop 要求

Zero Trust 访问模块包括 Duo Desktop 安装，在 macOS 11（及更高版本）上通过 MDM 部署 Zero Trust 访问时，有自己的其他设置要求。

有关这些额外的 Duo 设置要求，请参阅《适用于 macOS 11+ 用户的 Duo 设备运行状况应用证书部署指南》。

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。

步骤 1 安装 Cisco Secure Client 核心 VPN 模块，此过程会安装 GUI 和 VPN 功能（SSL 和 IPsec）。

步骤 2 安装 DART 模块，该模块提供有关 Cisco Secure Client 核心 VPN 和其他已安装模块的诊断信息。

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 Network Visibility Module。

使用 RPM 或 DEB 安装程序进行升级

使用 RPM/DEB 安装程序从脚本安装的版本升级时，存在以下限制：

- 不支持从前端自动更新客户端。您必须使用系统软件包管理器执行带外更新。
- RPM 和 DEB 安装程序支持的唯一 Cisco Secure Client 模块是 VPN 和 DART。
- 在切换到使用 RPM 或 DEB 安装程序之前，您必须卸载当前现有的 Cisco Secure Client（包括所有模块）。
- 不能使用脚本安装程序更新现有的 RPM 或 DEB 安装。

卸载用于 Linux 的模块

用户卸载 Cisco Secure Client 的顺序非常重要。

如果卸载过程失败，DART 信息将非常有价值。

步骤 1 卸载 Network Visibility Module。

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 Cisco Secure Client 核心 VPN 模块。

步骤 4 卸载 DART。

在 Linux 设备上手动安装/卸载 NVM

步骤 1 提取 Cisco Secure Client 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/secureclient/bin/nvm_uninstall.sh 卸载 Network Visibility Module。

用于服务器证书验证的证书存储库

默认情况下，Cisco Secure Client 使用 PEM 文件证书存储库，包括系统 CA 证书位置 (/etc/ssl/certs)，以便验证服务器证书。NSS 证书库也可用于 Cisco Secure Client 验证服务器证书。

激活 NSS 证书存储库

您可以按照以下选项之一操作：

- 创建文件夹：~/.cisco/certificates/nssdb。Cisco Secure Client 会使用此路径来存储 NSS 证书数据库。您可以使用 OnConnect 脚本来创建此文件夹。
- 让 Cisco Secure Client 在当前用户的 Firefox 默认配置文件中搜索并使用 NSS 证书数据库。不支持通过 Snap 或Flatpak 安装的 Firefox。

如果您从未启动已安装的 Firefox 浏览器，则必须先启动它，以便 Firefox 生成默认配置文件。

如果不使用 NSS 证书存储库

您必须将本地策略配置为排除 Firefox NSS 证书存储库，并且必须保持启用 PEM 文件证书存储库。

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。

此操作可用于 VPN 安装程序、网络访问管理器、Network Visibility Module 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 Cisco Secure Endpoint。

在 Linux 设备上手动安装 DART

1. 将 ciscosecureclient-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 您只能使用 **/opt/cisco/ciscosecureclient/dart/dart_uninstall.sh** 来卸载 DART。

Web部署 Cisco Secure Client

网络部署是指客户端系统上的 Cisco Secure Client 下载程序从头端获取 Cisco Secure Client 软件，或使用头端上的门户安装或更新 Cisco Secure Client。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) 仅适用于使用 Internet Explorer 浏览器的 Windows 操作系统。

通过 Cisco Secure Firewall ASA 进行网络部署

Cisco Secure Firewall ASA 上的无客户端门户执行 Cisco Secure Client 网络部署。

用户打开浏览器并连接到 Cisco Secure Firewall ASA 的无客户端门户。在门户上，用户点击**启动 AnyConnect 客户端 (Start AnyConnect Client)** 按钮。然后，他们可以手动下载 Cisco Secure Client 软件包。

如果您使用不同的软件更新方法或不需要与 ASDM 集成配置文件编辑器，则无需在 Cisco Secure Firewall ASA 上配置 Cisco Secure Client Web 部署软件包。

Cisco Secure Firewall ASA 网络部署限制

- 不支持将同一操作系统的多个 Cisco Secure Client 软件包载入 Cisco Secure Firewall ASA。
- Web 部署时，Cisco Secure Firewall 终端安全评估模块中不含 OPSWAT 定义。您必须手动部署 Cisco Secure Firewall 终端安全评估 模块或将其载入 ASA 上，以向客户端提供 OPSWAT 定义。
- 如果 Cisco Secure Firewall ASA 只有默认内部闪存大小，您在 ASA 上存储和加载多个 Cisco Secure Client 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，Cisco Secure Firewall 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 Cisco Secure Client 以及升级 Cisco Secure Firewall 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 Cisco Secure Firewall ASA，但不支持链路本地安全网关地址。
- 对于 Windows 用户，我们建议您在安装和首次使用之前安装 Microsoft .NET framework 4.6.2（及更高版本）。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 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 模块。

通过 ISE 进行网络部署

ISE 上的策略确定 Cisco Secure Client 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 Cisco Secure Client门户。该 ISE 门户将帮助用户下载和安装 Cisco Secure Client。门户将下载网络设置助理，该工具会帮助用户安装 Cisco Secure Client。

ISE 部署限制

- 如果 ISE 和 Cisco Secure Firewall ASA 均执行 Cisco Secure Client 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 Cisco Secure Client 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“代理配置”(Agent Configuration) > “策略”(Policy) > “客户端调配”(Client Provisioning) 下配置 NAC 代理或 Cisco Secure Client ISE 终端安全评估模块。

在 ASA 上配置网络部署

下载 Cisco Secure Client 软件包。

从思科软件下载网页下载最新的 Cisco Secure 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	cisco-secure-client-win-版本-webdeploy-k9.pkg
macOS	cisco-secure-client-macos-版本-webdeploy-k9.pkg
Linux（64位）	cisco-secure-client-linux64-版本-webdeploy-k9.pkg

注释 您不应具有 Cisco Secure Firewall ASA 上同一操作系统的不同版本。

在 Cisco Secure Firewall ASA 上加载 Cisco Secure Client 软件包

步骤 1 导航到 **Configuration**（配置）> **Remote Access**（远程访问）> **VPN** > **Network (Client) Access**（网络[客户端]访问）> **AnyConnect Client Software**（**AnyConnect** 客户端软件）。Cisco Secure Client 面板显示 Cisco Secure Firewall ASA 上当前加载的 Cisco Secure Client 映像。映像出现的顺序是 Cisco Secure Firewall ASA 将其下载到远程计算机的顺序。

步骤 2 要添加 Cisco Secure Client 映像，请点击**添加 (Add)** 并选择以下选项之一：

- 点击**浏览闪存 (Browse Flash)** 可选择已上传到 Cisco Secure Firewall ASA 的 Cisco Secure Client 映像。
- 点击**上传 (Upload)** 浏览至您存储于本地计算机上的 Cisco Secure Client 映像。

步骤 3 点击**确定 (OK)** 或**上传 (Upload)**。

步骤 4 单击**应用 (Apply)**。

启用其他 Cisco Secure Client 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，Cisco Secure Client 必须将这些模块下载到 VPN 终端。

注释 如果您选择“登录前开始”(Start Before Login)，还必须在 AnyConnect VPN 配置文件中启用此功能。

步骤 1 在 ASDM 中，转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **组策略 (Group Policies)**。

步骤 2 选择组策略，点击**编辑 (Edit)** 或**添加 (Add)** 可编辑或新增组策略。

步骤 3 在导航窗格中，选择**VPN 策略 (VPN Policy)** > **AnyConnect 客户端 (AnyConnect Client)**。在**要下载的客户端模块 (Client Modules to Download)** 中，点击**添加 (Add)**，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 Cisco Secure Firewall ASA 的模块。

步骤 4 点击**应用 (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 Cisco Secure Client 网络部署软件包添加到 Cisco Secure Firewall ASA，然后才能在 Cisco Secure Firewall ASA 上创建客户端配置文件。

步骤 1 导航到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

步骤 2 选择要与组关联的客户端配置文件，然后点击**更改组策略 (Change Group Policy)**。

步骤 3 在“更改配置文件策略”(Change Policy for Profile) 策略名称窗口中，从“可用组策略”(Available Group Policies) 字段中选择组策略，然后点击右箭头，将其移到 Policies 字段。

步骤 4 点击**确定 (OK)**。

步骤 5 在 Cisco Secure Client配置文件页面上，点击**应用 (Apply)**。

步骤 6 点击**保存 (Save)**。

步骤 7 完成配置时，点击**确定 (OK)**。

在 ISE 上配置网络部署

ISE 可配置和部署 Cisco Secure Client 核心 VPN 模块、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 Cisco Secure Firewall ASA 时可使用的所有 Cisco Secure Client 模块和资源。当用户浏览到 ISE 控制的资源时：

- 如果 ISE 在 Cisco Secure Firewall ASA 之后，则用户连接 ASA，下载 Cisco Secure Client，然后建立 VPN 连接。如果 Cisco Secure Client ISE 终端安全评估并非由 Cisco Secure Firewall ASA 安装，则用户将重定向到 Cisco Secure Client门户来安装 ISE 终端安全评估。
- 如果 ISE 不在 Cisco Secure Firewall ASA 后面，则用户会连接到 Cisco Secure Client 门户，而该门户会引导用户在 ISE 上安装 Cisco Secure Client 配置中定义的 Cisco Secure Client 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 Cisco Secure Client 客户端调配门户。
- 当用户在 ISE 中被定向到 Cisco Secure Client 调配门户时：

- 如果浏览器是 Internet Explorer，则 ISE 将下载 Cisco Secure Client 下载程序，然后该下载程序会加载 Cisco Secure Client。
- 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 Cisco Secure Client 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 Cisco Secure Client 配置文件
- 将 Cisco Secure Client 资源从本地设备添加到 ISE
- 从远程站点添加 Cisco Secure Client 调配资源
- 部署 Cisco Secure Client 和资源

注释 由于 Cisco Secure Client 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 Cisco Secure Client 资源：

- Cisco Secure Client 核心 VPN 和其他模块，包括 ISE 终端安全评估模块
- 配置文件：Network Visibility Module、Cisco Secure Endpoint、VPN、网络访问管理器、客户反馈和 ISE 终端安全评估
- 自定义文件
  - 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 Cisco Secure Client gettext 转换
  - Windows Installer 转换

准备 Cisco Secure Client 文件进行 ISE 上传

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

注释 对于 Cisco Secure Firewall ASA，安装将使用 VPN 下载程序进行。在下载后，将通过 Cisco Secure Firewall 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 Cisco Secure Firewall 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 Cisco Secure Client 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 列表的 ISE 终端安全评估配置文件。

- 将自定义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：
  - Cisco Secure Client 用户界面资源
  - VPN 连接脚本
  - 帮助文件
  - 安装程序转换

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

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

配置 ISE 以部署 Cisco Secure Client

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

注释 在 ISE 中配置 Cisco Secure Client 配置对象时，取消选中 Cisco Secure Client 模块选择下的 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 (Policy)** > **策略元素 (Policy Elements)** > **结果 (results)** > 。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 Cisco Secure Client 软件包文件。为您计划部署的任何其他 Cisco Secure Client 资源重复添加本地磁盘代理资源。

3. 选择添加 **(Add)** > **AnyConnect 配置 (AnyConnect Configuration)** > 。此 Cisco Secure Client 配置用于对模块、配置文件、自定义/语言包和 OPSWAT 软件包进行配置，如下表所述。

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

   表 *4: ISE* 中的 *Cisco Secure Client* 资源

提示符	ISE 资源类型和说明
Cisco Secure Client 数据包	CiscoSecureClientDesktopWindows CiscoSecureClientDesktopOSX CiscoSecureClientDesktopLinux CiscoTemporalAgentWindows CiscoTemporalAgentOSX
合规性模块	CiscoSecureClientComplianceModuleWindows CiscoSecureClientComplianceModuleOSX CiscoSecureClientComplianceModuleLinux
Cisco Secure Client 配置文件	代理配置文件 (Profile) ISE 为上传的 Cisco Secure Client 软件包所提供的每个配置文件显示一个复选框。
自定义捆绑包	代理CustomizationBundle
本地化捆绑包	代理LocalizationBundle

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 Cisco Secure Client 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 Cisco Secure Client 代理，要么是传统 NAC/MAC 代理。配置 Cisco Secure Client 代理时，请选择一个在步骤 2 创建的 Cisco Secure Client 配置。

在 Cisco Secure Firewall Threat Defense 上配 Web 部署

Cisco Secure Firewall Threat Defense 设备是提供类似于 Cisco Secure Firewall ASA 的安全网关功能的下一代防火墙 (NGFW)。Cisco Secure Firewall Threat Defense 设备仅支持使用 Cisco Secure Client 的远程接入 VPN (RA VPN)，不支持其他客户端或无客户端 VPN 访问。隧道建立和连接通过 IPsec IKEv2 或 SSL 完成。连接到 Cisco Secure Firewall Threat Defense 设备时不支持 IKEv1。

在 Cisco Secure Firewall Threat Defense 头端上配置 Windows、macOS 和 Linux Cisco Secure Client，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，Cisco Secure Firewall Threat Defense 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 Cisco Secure Client。Cisco Secure Firewall Threat Defense 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 Cisco Secure Client 应用程序。它们需要满足最低配置要求，以便与 Cisco Secure Firewall Threat Defense 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 Cisco Secure Client 软件。

目前，在 Cisco Secure Firewall Threat Defense 上只能配置 Cisco Secure Client 核心 VPN 和 Cisco Secure Client VPN 配置文件并将它们分发到终端。Cisco Secure Firewall Management Center 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。

Cisco Secure Client 和 Cisco Secure Firewall Threat Defense 的准则和限制

- 唯一支持的 VPN 客户端是 Cisco Secure 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 Cisco Secure Client。
- 将 Cisco Secure Client 与 Cisco Secure Firewall Threat Defense] 配合使用需要 4.0 或更高版本的 Cisco Secure Client，以及 6.2.1 或更高版本的 Cisco Secure Firewall Management Center。
- Cisco Secure Firewall Management Center 内在不支持 Cisco Secure Client 配置文件编辑器，您必须单独配置 VPN 配置文件。在 Cisco Secure Firewall Management Center 中作为文件对象添加 VPN 配置文件和 Cisco Secure Client 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 Cisco Secure Client 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（Cisco Secure Firewall 终端安全评估、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。
- Cisco Secure Firewall Threat Defense设备不会配置或部署自定义或本地化 Cisco Secure Client 所必需的文件。
- Cisco Secure Firewall Threat Defense 上不支持需要 Cisco Secure Client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 Cisco Secure Firewall Threat Defense 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 Cisco Secure Firewall Threat Defense 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 Cisco Secure Firewall Threat Defense 上配置和部署 Cisco Secure Client 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 Cisco Secure Client 软件和配置文件

Cisco Secure Client 可通过多种方式更新。

- Cisco Secure Client - 当 Cisco Secure Client 连接到 Cisco Secure Firewall ASA 时，Cisco Secure Client 下载程序将检查 Cisco Secure Firewall 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。
- ASA 或 FTD 网络门户 - 您指示用户连接到 Cisco Secure Firewall 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 Cisco Secure Client 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 Cisco Secure Client 下载程序，以管理软件包提取和安装。您必须将部署软件包上传到 Cisco Secure Firewall ASA 前端，并确保 Cisco Secure Client 客户端的版本与 Cisco Secure Firewall 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 Cisco Secure Client 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 Cisco Secure Client 更新
  - 在 Cisco Secure Firewall ASA 和 ISE 上配置相同版本的 Cisco Secure Client

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

前提条件

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 Cisco Secure Firewall 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 Cisco Secure Client 客户端调配门户。
- ISE 位于 Cisco Secure Firewall ASA 之后。

Cisco Secure Client 已安装在客户端上

1. 用户启动 Cisco Secure Client，提供凭证，并点击“连接”(Connect)。
2. Cisco Secure Firewall 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. Cisco Secure Client 启动 Cisco Secure Client 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 Cisco Secure Firewall 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 Cisco Secure Client 客户端调配门户。
2. 通过使用浏览器，用户下载并执行网络设置助理 (NSA)，该工具会下载并启动 Cisco Secure Client 下载程序。
3. Cisco Secure Client 下载程序执行在 ISE 上配置的所有 Cisco Secure Client 升级，其中现在包括 Cisco Secure Client 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。

Cisco Secure Client 未安装

1. 用户浏览到站点，启动到 Cisco Secure Firewall ASA 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. Cisco Secure Client 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. Cisco Secure Client 下载程序执行在 Cisco Secure Firewall ASA 上配置的升级，然后启动 VPN 隧道。下载程序完成。

如果 Cisco Secure Firewall 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 Cisco Secure Client 客户端调配门户。
2. Cisco Secure Client 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 Cisco Secure Client ISE 终端安全评估模块。
3. ISE 终端安全评估代理启动终端安全评估。

禁用 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Firewall 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 Cisco Secure Client

您可以将 Cisco Secure Firewall 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 Cisco Secure Client 或转到无客户端入口页面。

提示用户下载 Cisco Secure Client 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。

步骤 1 在 ASDM 中，转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **组策略 (Group Policies)**。

步骤 2 选择组策略，点击**编辑 (Edit)** 或**添加 (Add)** 可编辑或新增组策略。

步骤 3 在导航窗格中，选择**高级 (Advanced)** > **AnyConnect 客户端 (AnyConnect Client)** > **登录设置 (Login Settings)**。如果需要，取消选中**继承 (Inherit)** 复选框，然后选择“登录后”(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“默认登录后选择”(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 点击**确定 (OK)** 并确保将更改应用到组策略中，然后点击**保存 (Save)**。

允许用户延期升级

您可以强制用户通过禁用 AutoUpdate 接受 Cisco Secure Client 更新，如禁用 Cisco Secure Client 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，Cisco Secure Client 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 macOS 都支持延期更新。

在 Cisco Secure Firewall ASA 上配置延迟更新

在 Cisco Secure Firewall ASA 上，通过添加自定义属性，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 配置添加自定义属性的过程取决于所运行的 Cisco Secure Firewall ASA/ASDM 版本。请根据您部署的 ASA/ASDM 版本，请参阅《Cisco ASA 系列 VPN CLI 或 ASDM 配置指南》，了解自定义属性配置过程。

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 Cisco Secure Client 版本。 最低版本检查适用于头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

步骤 1 遵循以下步骤进行导航：

a) 选择**策略 (Policy)** > **结果 (Results)**。

b) 展开 **Client Provisioning**。

c) 选择**资源 (Resources)**，然后点击**添加 (Add)** > **来自本地磁盘的代理资源 (Agent resources from local disk)**。

d) 上传 Cisco Secure Client pkg 文件，然后选择**提交 (Submit)**。

步骤 2 上载您创建的任何其他 Cisco Secure Client 资源。

步骤 3 在**资源 (Resources)** 上，使用您上传的 Cisco Secure Client 软件包添加 **AnyConnect 配置**。Cisco Secure Client 配置具有用于配置延期更新的字段。

设置更新策略

更新策略概述

如果 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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**允许任何服务器的 ISE 终端安全评估配置文件更新 (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。
  - **使用允许来自任何服务器的合规性模块更新 (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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Firewall 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。

更新策略准则

- 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。
- 软件更新包括下载自定义、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。

- 下载启用永远在线的 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	永远在线
登录前开始	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

- 在 Windows 中，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 Cisco Secure Firewall 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：

  `%ALLUSERESPROFILE%\Cisco\Cisco Secure Client\Logs` 目录。

- 您必须重新启动 Cisco Secure Client 服务才能选择本地策略文件中的任何更改。

更新策略示例

此示例显示了客户端上的 Cisco Secure Client 版本不同于各 Cisco Secure Firewall 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>false</AllowSoftwareUpdatesFromAnyServer>
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowManagementVPNProfileUpdatesFromAnyServer>true</AllowManagementVPNProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>false</AllowServiceProfileUpdatesFromAnyServer>
<AllowScriptUpdatesFromAnyServer>true</AllowScriptUpdatesFromAnyServer>
<AllowHelpUpdatesFromAnyServer>true</AllowHelpUpdatesFromAnyServer>
<AllowResourceUpdatesFromAnyServer>true</AllowResourceUpdatesFromAnyServer>
```

```
<AllowLocalizationUpdatesFromAnyServer>true</AllowLocalizationUpdatesFromAnyServer>
<AuthorizedServerList>
<ServerName>seattle.example.com</ServerName>
<ServerName>newyork.example.com</ServerName>
</AuthorizedServerList>
</UpdatePolicy>
</AnyConnectLocalPolicy>
```

有以下 Cisco Secure Firewall 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
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 Cisco Secure Client VPN 核心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 Cisco Secure Client 来配置的授权服务器。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 Cisco Secure Client 来配置的授权 Cisco Secure Firewall ASA。VPN 和网络访问管理器模块会进行升级。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 Cisco Secure Firewall ASA。即使需要进行软件更新并且也有软件更新可用，但由于策略决定了不允许版本升级，因此无法进行更新。连接终止。

本地计算机上用户首选项文件的位置

Cisco Secure Client 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。Cisco Secure Client 使用本地文件配置客户端 GUI 上“首选项”(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。

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

下表列出了放置在 Cisco Secure Client 的 VPN 子目录下的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	%USERPROFILE%\AppData\Local\Cisco\ Cisco Secure Client\VPN\preferences.xml
	全局	%ALLUSERSPROFILE%\Cisco\Cisco Secure Client\VPN\preferences_global.xml

操作系统	类型	文件和路径
macOS	用户	$HOME/.vpn/.anyconnect
	全局	/opt/cisco/secureclient/vpn/.anyconnect_global
Linux	用户	$HOME/.vpn/.anyconnect
	全局	/opt/cisco/secureclient/.vpn/.anyconnect_global

Cisco Secure Client 使用的端口

下表列出了每个协议的 Cisco Secure Client 使用的端口。

协议 (Protocol)	Cisco Secure Client 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

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。