AnyConnect 配置文件编辑器

关于配置文件编辑器

Cisco AnyConnect Secure Mobility Client 软件包包含适用于所有操作系统的配置文件编辑器。在 ASA 上加载 AnyConnect 客户端映像时，ASDM 会激活配置文件编辑器。您可从本地或闪存上传客户端配置文件。

如果加载多个 AnyConnect 软件包，ASDM 会激活来自最新的 AnyConnect 软件包的客户端配置文件编辑器。此方法可确保编辑器显示所加载的最新 AnyConnect 以及早期版本客户端的功能。

还有在 Windows 上运行的独立配置文件编辑器。

从 ASDM 添加新配置文件

注释 在创建客户端配置文件之前，必须先上传客户端映像。

配置文件按照管理员定义的最终用户要求和终端上的身份验证策略部署为 AnyConnect 的一部分，使预配置的网络配置文件可供最终用户使用。使用配置文件编辑器创建并配置一个或多个配置文件。AnyConnect 将配置文件编辑器作为 ASDM 的一部分，并且作为独立的 Windows 程序。

要从 ASDM 向 ASA 添加新的客户端配置文件，请执行以下操作：

过程

步骤 1 打开 ASDM，并选择 **Configuration**（配置 ） > **Remote Access VPN**（远程访问 **VPN**） > **Network (Client) Access**（网络[客户端]访问） > **AnyConnect Client Profile**（**AnyConnect** 客户端配置文件）。

步骤 2 单击添加 **(Add)**。

步骤 3 输入配置文件名称。

步骤 4 从 Profile Usage 下拉列表中选择要为其创建配置文件的模块。

步骤 5 （可选）在“配置文件位置”(Profile Location) 字段中，单击**浏览闪存 (Browse Flash)**，并选择 ASA 上 XML 文件的设备文件路径。

步骤 6 （可选）如果使用独立编辑器创建了配置文件，请单击**上传 (Upload)** 以使用该配置文件定义。

步骤 7 （可选）从下拉列表中选择 AnyConnect 组策略。

步骤 8 单击**确定 (OK)**。

AnyConnect VPN 配置文件

AnyConnect 配置文件中启用了Cisco AnyConnect Secure Mobility Client功能。这些配置文件包含核心客户端 VPN 功能和可选客户端模块网络访问管理器、ISE 终端安全评估、客户体验反馈和网络安全的配置设置。在 AnyConnect 安装和更新过程中，ASA 将部署配置文件。用户无法管理或修改配置文件。

您可以配置 ASA 或 ISE，以向所有 AnyConnect 用户全局部署配置文件，或基于用户的组策略向用户部署。通常情况下，对于安装的每个 AnyConnect 模块，用户都有一个配置文件。在某些情况下，您可能希望为用户提供多个 VPN 配置文件。在多个位置工作的某些用户可能需要多个 VPN 配置文件。

某些配置文件设置本地存储在用户计算机的用户首选项文件或全局首选项文件中。用户文件包含 AnyConnect 客户端在客户端 GUI 的“首选项”(Preferences) 选项卡中显示用户可控设置所需的信息，以及有关上一次连接的信息，例如用户、组和主机。

全局文件包含有关用户可控设置的信息，因此您可以在登录之前应用这些设置（因为此时无用户）。例如，客户端需要了解登录前是否已启用“Start Before Login”（登录前启动）和/或“AutoConnect On Start”（启动时自动连接）功能。

AnyConnect 配置文件编辑器，首选项（第 1 部分）

- **Use Start Before Login**（**使用登录前启动**）-（仅限Windows）启用“Start Before Login”（登录前启动）以供客户端使用。启用“Start Before Login”（在登录前启动）后，AnyConnect 会在 Windows 登录对话框出现之前启动。用户会在登录 Windows 之前通过 VPN 连接到企业基础设施。进行身份验证之后，将会显示登录对话框，用户可以像平常一样登录。
- **显示预连接消息** - 支持管理员在用户首次尝试连接之前显示一条一次性消息。例如，此消息可以提醒用户将智能卡插入读卡器。此消息出现在 AnyConnect 消息目录中并已本地化。
- **Certificate Store**（**证书存储库**）- 控制 AnyConnect 使用哪个证书存储库来存储和读取证书。必须相应地配置安全网关，并命令客户端可以接受多个证书身份验证组合中的哪一个用于特定 VPN 连接。

  VPN 配置文件中的 CertificateStore 配置的值取决于安全网关可接受的证书类型：两个用户证书，或者一个计算机证书和一个用户证书。

若要允许证书存储库的访问由 AnyConnect 在 macOS 上进一步筛选，您可以配置从 Windows 或 macOS 下拉的证书存储库。MacOS 的新配置文件首选项是 CertificateStoreMac，支持以下添加的值：

- All（所有）（对于 Windows）- ASA 配置接受一台计算机和一个用户证书。
- User（用户）（对于 Windows）- ASA 配置接受两个用户证书。
- All（所有）（对于 macOS）- 使用所有可用 macOS 密钥链和文件存储区的证书。
- Syestem（系统）（对于 macOS）- 仅使用 macOS 系统密钥链和系统文件/PEM 存储区的证书。
- Login（登录）（对于 macOS）- 仅使用 macOS 登录和动态智能卡密钥链以及用户文件/PEM 存储区的证书。

- **证书存储库覆盖 (Certificate Store Override)** - 允许管理员指示 AnyConnect 在 Windows 计算机（本地系统）证书存储库中利用证书，以进行客户端证书身份验证。证书存储库覆盖仅适用于 SSL，默认情况下，UI 进程启动连接。使用 IPSec/IKEv2 时，AnyConnect 配置文件中的此功能不适用。

  注释 为了使用计算机证书与 Windows 连接，您必须具有预部署的配置文件并且启用了此选项。如果在连接之前 Windows 设备上不存在此配置文件，则在计算机存储库中无法访问证书，因而连接将失败。

  - **True** - AnyConnect 将在 Windows 计算机证书存储库中搜索证书。如果将 CertificateStore 设置为 *all*，则必须将 CertificateStoreOverride 设置为 *true*。
  - **False** - AnyConnect 不在 Windows 计算机证书存储库中搜索证书。

- **AutomaticCertSelection** - 当在安全网关上配置了多重证书身份验证时，您必须将此值设置为 **true**。
- **Auto Connect on Start** - 启动时，AnyConnect 自动与 AnyConnect 配置文件指定的安全网关建立 VPN 连接，或者连接到客户端连接到的最后一个网关。
- **连接时最小化 (Minimize On Connect)** - 建立 VPN 连接后，AnyConnect GUI 最小化。
- **本地 LAN 访问 (Local LAN Access)** - 允许用户在与 ASA 的 VPN 会话期间完成对连接到远程计算机的本地 LAN 的访问。

注释 若启用本地 LAN 访问，则用户计算机进入企业网络可能导致来自公共网络的安全漏洞。或者，您可以配置安全设备（版本 8.4 (1) 或更高版本）来部署一个 SSL 客户端防火墙，该防火墙使用默认组策略中包含的 AnyConnect 客户端本地打印防火墙规则。要启用此防火墙规则，您还必须在此编辑器的 Preferences（第 2 部分）中启用 Automatic VPN Policy、Always on 和 Allow VPN Disconnect。

- **禁用强制网络门户检测 (Disable Captive Portal Detection)** - 当 AnyConnect 客户端收到的证书的常用名与 ASA 名称不一致时，检测强制网络门户。此行为提示用户进行身份验证。使用自签名证书的某些用户可能要启用到 HTTP 强制网络门户后台的企业资源的连接，因此应选中 **Disable Captive Portal Detection** 复选框。管理员还可以确定他们是否希望该选项为用户可配置的选项，并相应地选中该复选框。如果选择用户可配置，则该复选框将出现在 AnyConnect 安全移动客户端 UI 的 Preferences 选项卡上。
- **自动重连 (Auto Reconnect)** - 连接丢失时，AnyConnect 尝试重新建立 VPN 连接（默认为启用）。如果禁用 Auto Reconnect，则无论连接出于何种原因断开连接，都不会尝试重新连接。

注释 在用户能够控制客户端行为的情形下，可以使用 Auto Reconnect。AlwaysOn 不支持此功能。

  - **自动重新连接行为**
    - DisconnectOnSuspend - AnyConnect 在系统暂停时释放分配给 VPN 会话的资源，并且在系统恢复后不尝试重新连接。
    - ReconnectAfterResume（默认值）- 连接丢失时，AnyConnect 尝试重新建立 VPN 连接。
- **自动更新 (Auto Update)** - 选中此选项时，将启用客户端的自动更新。如果选中 User Controllable，则用户可以在客户端覆盖此设置。
- **RSA 安全 ID 集成 (RSA Secure ID Integration)**（仅限 Windows）- 控制用户如何与 RSA 交互。默认情况下，AnyConnect 确定 RSA 交互的正确方法（自动设置：软件或硬件令牌均接受）。
- **Windows 登录强制 (Windows Logon Enforcement)** - 允许从远程桌面协议 (RDP) 会话建立 VPN 会话。必须在组策略中配置分割隧道。当建立 VPN 连接的用户注销时，AnyConnect 会断开 VPN 连接。如果连接由远程用户建立，则该远程用户注销时 VPN 连接会终止。
  - 单一本地登录 (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)** - 确定当远程登录到客户端 PC 的用户建立 VPN 连接时 AnyConnect 的行为。可能的值包括：
  - 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。

- **Linux 登录强制 (Linux Logon Enforcement)** - 允许从 SSH 会话建立 VPN 会话。必须在组策略中配置分割隧道。当建立 VPN 连接的用户注销时，AnyConnect 会断开 VPN 连接。如果连接由远程用户建立，则该远程用户注销时 VPN 连接会终止。
  - 单一本地登录 (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。

- **Linux VPN 建立 (Linux VPN Establishment)** - 确定当登录到客户端 PC 的用户使用 SSH 建立 VPN 连接时 AnyConnect 的行为。可能的值包括：
  - 仅限本地用户（默认值）- 阻止远程登录用户建立 VPN 连接。
  - 允许远程用户 - 允许远程用户建立 VPN 连接。
- **清除智能卡 PIN (Clear SmartCard PIN)**
- **支持的 IP 协议 (IP Protocol Supported)** - 若同时具有 IPv4 和 IPv6 地址的客户端尝试使用 AnyConnect 连接到 ASA，AnyConnect 需要决定使用哪种 IP 协议发起连接。默认情况下，AnyConnect 先使用 IPv4 尝试连接。如果这样不成功，AnyConnect 将尝试使用 IPv6 发起连接。

  此字段配置初始 IP 协议和回退顺序。
  - IPv4 - 仅可建立到 ASA 的 IPv4 连接。
  - IPv6 - 仅可建立到 ASA 的 IPv6 连接。
  - IPv4, IPv6 - 先尝试建立到 ASA 的 IPv4 连接。如果客户端无法使用 IPv4 建立连接，则尝试建立 IPv6 连接。
  - IPv6, IPv4 - 先尝试建立到 ASA 的 IPv6 连接。如果客户端无法使用 IPv6 进行连接，则尝试进行 IPv4 连接。

  注释 IP 协议的故障转移也可能发生在 VPN 会话期间。无论是在 VPN 会话之前还是在 VPN 会话期间执行，都会保持故障转移直到无法访问当前使用的安全网关 IP 地址。每当无法访问当前使用的 IP 地址时，客户端就会故障转移到与备用 IP 协议（如果可用）匹配的 IP 地址。

AnyConnect 配置文件编辑器，首选项（第 2 部分）

- **Disable Automatic Certificate Selection**（仅限 Windows）- 禁止客户端自动选择证书并提示用户选择身份验证证书。

  相关主题：配置证书选择

- **代理设置 (Proxy Settings)** - 在 AnyConnect 配置文件中指定一个策略来控制客户端对代理服务器的访问。当代理配置阻止用户从企业网络外部建立隧道时，使用此设置。
  - Native - 让客户端既使用以前由 AnyConnect 配置的代理设置，也使用在浏览器中配置的代理设置。在全局用户首选项中配置的代理设置优先于浏览器代理设置。
  - IgnoreProxy - 忽略用户计算机上的浏览器代理设置。
  - Override - 手动配置公共代理服务器的地址。公共代理是唯一一种支持 Linux 的代理类型。Windows 也支持公共代理。您可以将公共代理地址配置为 User Controllable。

- **允许本地代理连接 (Allow Local Proxy Connections)** - 默认情况下，AnyConnect 让 Windows 用户通过本地 PC 上的透明或不透明代理服务建立 VPN 会话。如果要禁用对本地代理连接的支持，请取消选中此参数。例如，某些无线数据卡提供的加速软件和某些防病毒软件上的网络组件都可提供透明代理服务

- **启用最佳网关选择 (Enable Optimal Gateway Selection)** (OGS)，（仅限 IPv4 客户端）- AnyConnect 根据往返时间 (RTT) 确定并选择哪个安全网关对于连接或重新连接是最佳选择，从而尽可能缩短互联网流量延迟，而且无需用户干预。OGS 不是安全功能，它不会在安全网关集群之间或集群内执行负载均衡。您控制 OGS 的激活和取消激活，并指定最终用户是否可以自己控制此功能。“自动选择”(Automatic Selection) 显示在客户端 GUI 的“连接”(Connection) 选项卡中的“连接到”(Connect To) 下拉列表中。
  - **暂停时间阈值 (Suspension Time Threshold)**（小时）- 输入在调用新网关选择计算之前 VPN 必须已暂停的最短时间（以小时为单位）。通过优化此值以及下一个可配置的参数 Performance Improvement Threshold，您可以在选择最佳网关和减少强制重新输入凭证次数之间找到适当的平衡。
  - **性能改进阈值 (Performance Improvement Threshold)** (%) - 在系统恢复后触发客户端重新连接到另一个安全网关的性能改进百分比。为特定网络调整这些值，可在选择最佳网关与减少次数之间找到合适的平衡，从而强制重新输入凭证。默认值为 20%。

  当 OGS 启用时，建议您也将此功能设置为用户可控制。

  OGS 存在以下限制：
  - 不能在设置为 Always On 的情况下运行
  - 它不支持自动代理检测
  - 它不支持代理自动配置 (PAC) 文件

- 如果使用 AAA，则在过渡到另外一个安全网关时，用户可能必须重新输入凭证。使用证书可消除此问题。

- **自动 VPN 策略 (Automatic VPN Policy)**（仅限 Windows 和 Mac）- 启用“受信任网络检测”可使 AnyConnect 根据“受信任网络策略”和“不受信任网络策略”自动管理何时启动或停止 VPN 连接。如果禁用，则 VPN 连接只能手动启动和停止。设置 Automatic VPN Policy 不会阻止用户手动控制 VPN 连接。
  - **受信任的网络策略 (Trusted Network Policy)** - 当用户处于企业网络（受信任网络）中时，AnyConnect 对 VPN 连接自动采取的操作。
    - 断开 (Disconnect)（默认值）- 检测到受信任网络时断开 VPN 连接。
    - 连接 (Connect) - 检测到受信任网络时发起 VPN 连接。
    - 不执行任何操作 - 在不受信任的网络中不执行任何操作。将“受信任的网络策略”(Trusted Network Policy) 和“不信任的网络策略”(Untusted Network Policy) 都设置为“不执行任何操作”(Do Nothing) 会禁用“值得信赖的网络检测”(Trusted Network Detection)。
    - 暂停 (Pause) - 如果用户在受信任网络外建立 VPN 会话之后进入被配置为受信任的网络，则 AnyConnect 会暂停此 VPN 会话而不是将其断开连接。当用户再次离开受信任网络时，AnyConnect 会恢复该会话。此功能是为了给用户提供方便，因为有了它，在用户离开受信任网络后不需要建立新的 VPN 会话。
  - **不受信任网络策略 (Untrusted Network Policy)** - 当用户处于企业网络外（不受信任的网络）时，AnyConnect 启动 VPN 连接。此功能可以在用户处于受信任网络外时发起 VPN 连接，从而鼓励提高安全意识。
    - 连接 (Connect)（默认值）- 在检测到不受信任网络时发起 VPN 连接。
    - Do Nothing - 在受信任网络中不执行任何操作。此选项禁用永远在线 VPN。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 Do Nothing 会禁用 Trusted Network Detection。
  - **受信任的 DNS 域 (Trusted DNS Domains)** - 客户端处于受信任网络中时，网络接口可能具有的 DNS 后缀（逗号分隔的字符串）。例如：*.cisco.com。DNS 后缀支持通配符 (*)。

    注释 如果您使用的是 NVM，则不支持受信任的 DNS 域和服务器，因为 NVM 模块使用管理员定义的受信任服务器和证书散列来确定用户位于受信任还是不受信任的网络上。

  - **受信任 DNS 服务器 (Trusted DNS Servers)** - 客户端处于受信任网络中时，网络接口可能具有的 DNS 服务器地址（逗号分隔的字符串）。例如：192.168.1.2, 2001:DB8::1。IPv4 或 IPv6 DNS 服务器地址支持通配符 (*)。

- **Trusted Servers @ https://<server>[:<port>]** - 要添加为受信任的主机 URL。在单击**添加 (Add)** 后，将会添加 URL 并预填充证书哈希值。如果未找到哈希值，系统将显示一条错误消息，提示用户手动输入证书哈希值并单击**设置 (Set)**。

  可信 URL 要求必须存在一个安全 Web 服务器，且可通过可信任证书对其进行访问。安全 TND 尝试连接到列表中第一个已配置的服务器。如果无法联系到服务器，安全 TND 将尝试联系已配置列表中的下一台服务器。如果可以联系到服务器，但证书的哈希值不匹配，则网络将被标识为“不可信”。系统不会评估其他服务器。如果哈希值受信任，则满足“受信任”条件。

  注释 只有当一个或以上的受信任的 DNS 域或 DNS 服务器被定义时，您才可以配置该参数。如果受信任的 DNS 域或 DNS 服务器未被定义，则该字段将被禁用。

- **始终在线 (Always On)** - 确定当用户登录到运行受支持的 Windows 或 macOS 操作系统的计算机时，AnyConnect 是否自动连接到 VPN。您可以实施企业策略，以便在计算机不在受信任网络中时阻止计算机访问互联网资源，从而保护它免遭安全威胁。根据分配策略所用的匹配条件，您可以指定异常情况，从而在组策略和动态访问策略中设置永远在线 VPN 参数来覆盖此设置。如果 AnyConnect 策略启用永远在线，而动态访问策略或组策略禁用它，只要其条件匹配关于建立每个新会话的动态访问策略或组策略，客户端就为当前和将来的 VPN 会话保留此禁用设置。在启用后，您就可以配置其他参数。

  注释 AlwaysOn 用于连接建立和冗余运行而无需用户干预的情形；因此，在使用此功能时，您不需要配置或启用 Preferences 第 1 部分中的 Auto Reconnect。

  相关主题：需要使用永远在线的 VPN 连接

  - **允许 VPN 断开 (Allow VPN Disconnect)** - 确定 AnyConnect 是否为永远在线 VPN 会话显示 Disconnect 按钮。由于当前 VPN 会话存在性能问题或 VPN 会话中断后重新连接出现问题，永远在线 VPN 会话的用户可能想要单击“断开连接”(Disconnect) 以选择其他安全网关。

    Disconnect 会锁定所有接口，以防止数据泄漏并防止计算机在建立 VPN 会话外还以其他方式访问互联网。出于上述原因，禁用 Disconnect 按钮有时可能会阻碍或防止 VPN 访问。

  - **允许在 VPN 断开连接时访问以下主机 (Allow Access to the Following Hosts With VPN Disconnected)** - 当 VPN 在永远在线期间断开连接时，允许终端访问已配置的主机。值是主机的逗号分隔列表，可以是指定 IP 地址、IP 地址范围（CIDR 格式）或 FQDN。最多允许 500 个主机，并且不支持通配符。

    警告：对指定 FQDN 的访问取决于在不受信任网络中执行的名称解析。

- **连接失败策略 (Connect Failure Policy)** - 确定在 AnyConnect 无法建立 VPN 会话（例如，无法访问 ASA）时计算机是否可访问互联网。此参数只在启用了永远在线和 Allow VPN Disconnect 时才适用。如果选择永远在线，则 fail-open 策略允许网络连接，fail-close 策略禁用网络连接。
  - 已关闭 (Closed) - 当无法访问 VPN 时限制网络访问。此设置的目的是，当负责保护终端的专用网络中的资源不可用时，帮助保护企业资产免遭网络威胁。
  - Open - 当无法访问 VPN 时允许网络访问。

> **注意** 如果 AnyConnect 未能建立 VPN 会话，连接故障关闭策略会阻止网络访问。它主要用在网络访问的安全持久性比始终可用性更重要的企业中，以特别保证企业的安全。除本地资源（例如，分隔隧道允许和 ACL 限制的打印机和系留设备等）外，它会阻止所有网络访问。如果用户在安全网关不可用时需要 VPN 以外的互联网访问，它可能停止运行。AnyConnect 检测大多数强制网络门户。如果它不能检测到强制网络门户，连接故障关闭策略会阻止所有网络连接。
>
> 如果您部署关闭连接策略，我们强烈建议您采用分阶段方法。例如，首先利用连接失败打开策略部署永远在线 VPN，并调查用户 AnyConnect 无法无缝连接的频率。然后，在早期采用者用户中部署连接失败关闭策略的一个小型试点部署，并征求他们的反馈。逐步扩展试点计划，同时继续征求反馈，再考虑全面部署。部署连接失败关闭策略时，请确保向 VPN 用户告知网络访问限制以及连接失败关闭策略的优点。

相关主题：关于强制网络门户

如果 Connect Failure Policy 为 Closed，则您可以配置以下设置：

- **Allow Captive Portal Remediation** - 当客户端检测到强制网络门户（热点）时，让 AnyConnect 解除关闭连接失败策略所施加的网络访问限制。酒店和机场通常使用强制网络门户，它们要求用户打开浏览器并满足允许互联网访问所需的条件。默认情况下，此参数处于未选中状态可提供最高安全性。但是，如果您想要客户端连接到 VPN 而强制网络门户却阻止它这样做，则您必须启用此参数。
- **Remediation Timeout** - AnyConnect 解除网络访问限制的分钟数。此参数只在 Allow Captive Portal Remediation 参数被选中且客户端检测到强制网络门户时适用。指定满足一般强制网络门户要求所需的足够时间（例如，5 分钟）。
- **Apply Last VPN Local Resource Rules** - 如果 VPN 无法访问，则客户端应用其从 ASA 收到的最后一个客户端防火墙，此 ASA 可能包含允许访问本地 LAN 资源的 ACL。

相关主题：配置连接失败策略

- **强制网络门户补救浏览器故障转移 (Captive Portal Remediation Browser Failover)** - 允许最终用户使用外部浏览器（在关闭 AnyConnect 浏览器后）进行强制网络门户补救。

  请参阅使用强制网络门户热点检测和补救获得更多信息。

- **允许手动主机输入 (Allow Manual Host Input)** - 支持用户输入与 AnyConnect UI 的下拉框中所列内容不同的 VPN 地址。如果取消选中此复选框，VPN 连接将仅限于下拉框中的选项，并且用户只能输入新的 VPN 地址。

- **PPP 排除 (PPP Exclusion)** - 对于通过 PPP 连接的 VPN 隧道，指定是否以及如何确定排除路由。客户端可以将去往此安全网关的流量从去往安全网关外目标的隧道流量中排除。排除路由在 AnyConnect GUI 的 Route Details 中显示为非安全路由。如果将此功能设置为用户可控制，则用户能够读取和更改 PPP 排除设置。

  - 自动 (Automatic) - 启用 PPP 排除。AnyConnect 自动确定 PPP 服务器的 IP 地址。
  - 覆盖 (Override) - 使用 *PPP Exclusion Server IP*（*PPP* 排除服务器 *IP*）字段中指定的预定义服务器 IP 地址来启用 PPP 排除。*PPP Exclusion Server IP*（*PPP* 排除服务器 *IP*）字段仅适用于此覆盖方法，并且仅在“Automatic”（自动）选项无法检测 PPP 服务器的 IP 地址时使用。

    为“PPP Exclusion Server IP”（PPP 排除服务器 IP）选中 **User Controllable**（用户可控制）字段可允许最终用户通过 preferences.xml 文件手动更新 IP 地址。请参阅 指示用户覆盖 PPP 排除 一节。

  - Disabled - 不应用 PPP 排除。

- **Enable Scripting** - 如果安全设备闪存上存在 OnConnect 和 OnDisconnect 脚本，则启动它们。

  - **Terminate Script On Next Event** - 发生向另一个可编写脚本事件的过渡时终止正在运行的脚本进程。例如，如果 VPN 会话结束，则 AnyConnect 终止正在运行的 OnConnect 脚本。如果客户端启动新的 VPN 会话，则终止正在运行的 OnDisconnect 脚本。在 Microsoft Windows 上，客户端还会终止 OnConnect 或 OnDisconnect 脚本启动的任何脚本以及它们的所有脚本子代。在 macOS 和 Linux 上，客户端只会终止 OnConnect 或 OnDisconnect 脚本，它不会终止子脚本。

  - **Enable Post SBL On Connect Script** - 启动 OnConnect 脚本（如果存在），然后 SBL 建立 VPN 会话。（仅当 VPN 终端运行 Microsoft Windows 时才受支持。）

- **注销时保留 VPN (Retain VPN On Logoff)** - 确定是否在用户注销 Windows 或 Mac 操作系统时保留 VPN 会话。

  - **用户强制 (User Enforcement)** - 指定当其他用户登录时是否结束 VPN 会话。此参数仅在“注销时保留 VPN”(Retain VPN On Logoff) 被选中且原始用户在 VPN 会话进行中注销 Windows 或 macOS 时适用。

- **身份验证超时值 (Authentication Timeout Values)** - 默认情况下，AnyConnect 在终止连接尝试前，要等待长达 30 秒才能从安全网关获得身份验证。然后，AnyConnect 显示一条消息，指示身份验证已超时。输入介于 10 - 120 之间的秒数。

AnyConnect 配置文件编辑器，备用服务器

您可以配置一个备用服务器列表，以便客户端在用户选择的服务器发生故障时使用。如果用户选择的服务器发生故障，客户端会尝试连接到在列表顶端的最佳服务器备用。如果该尝试失败了，客户端会按其选择结果依次尝试最佳网关选择列表中剩余的每个服务器。

注释 仅当未在 AnyConnect 配置文件编辑器，添加/编辑服务器列表，第 18 页中定义备用服务器时，才会尝试使用您在此处配置的任何备用服务器。在 Server List 中配置的服务器优先，而此处列出的备用服务器将被覆盖。

Host Address - 指定一个 IP 地址或完全限定域名 (FQDN) 以包含在备用服务器列表中。

- **Add** - 将主机地址添加到备用服务器列表。
- **Move Up** - 将选定的备用服务器在列表中向上移动。如果用户选择的服务器发生故障，则客户端首先尝试连接到此列表顶端的备用服务器，必要时再沿着列表从上到下逐个尝试。
- **Move Down** - 将选定的备用服务器在列表中向下移动。
- **Delete** - 从服务器列表中删除备用服务器。

AnyConnect 配置文件编辑器，证书匹配

启用可用于优化此窗格中自动客户端证书选择的各属性的定义。

如果未指定证书匹配条件，则 AnyConnect 应用以下证书匹配规则：

- Key Usage：Digital_Signature
- Extended Key Usage：Client Auth

如果配置文件中指定了任何条件匹配规范，则不应用这些匹配规则，除非配置文件中具体列出了这些规则。

- **Key Usage** - 在选择可接受的客户端证书时，使用以下证书密钥属性：
  - Decipher_Only - 解密数据，且未设置其他位（Key_Agreement 除外）。
  - Encipher_Only - 加密数据，且未设置其他位（Key_Agreement 除外）。
  - CRL_Sign - 验证 CRL 上的 CA 签名。
  - Key_Cert_Sign - 验证证书上的 CA 签名。
  - Key_Agreement - 密钥协议。

- Data_Encipherment - 加密除 Key_Encipherment 以外的数据。
- Key_Encipherment - 加密密钥。
- Non_Repudiation - 验证数字签名保护，以免错误拒绝某些操作（Key_Cert_sign 或 CRL_Sign 除外）。
- Digital_Signature - 验证数字签名（Non_Repudiation、Key_Cert_Sign 或 CRL_Sign 除外）。

- **Extended Key Usage** - 使用以下 Extended Key Usage 设置。OID 括在括号内：
  - ServerAuth (1.3.6.1.5.5.7.3.1)
  - ClientAuth (1.3.6.1.5.5.7.3.2)
  - CodeSign (1.3.6.1.5.5.7.3.3)
  - EmailProtect (1.3.6.1.5.5.7.3.4)
  - IPSecEndSystem (1.3.6.1.5.5.7.3.5)
  - IPSecTunnel (1.3.6.1.5.5.7.3.6)
  - IPSecUser (1.3.6.1.5.5.7.3.7)
  - TimeStamp (1.3.6.1.5.5.7.3.8)
  - OCSPSign (1.3.6.1.5.5.7.3.9)
  - DVCS (1.3.6.1.5.5.7.3.10)
  - IKE Intermediate

- **Custom Extended Match Key**（最多 10 个）- 指定定制扩展匹配密钥（如果有，最多 10 个）。证书必须与您输入的所有指定密钥匹配。以 OID 格式（例如 1.3.6.1.5.5.7.3.11）输入密钥。

注释 如果创建的一个定制扩展匹配密钥的 OID 大小超过 30 个字符，则您单击“确定”(OK) 按钮时，该密钥不会被接受。OID 的最大字符数限制是 30。

- **只与支持密钥用法扩展 (EKU) 的证书匹配** - 先前的做法是：如果设置了证书可分辨名称 (DN) 匹配规则，客户端会与带特定 EKU OID 和所有不带 EKU 的证书匹配。为了在保持一致性的同时提升清晰度，您可以禁止与不带 EKU 证书进行匹配。默认设置为保留客户所期待的这一传统行为。您必须通过单击复选框来启用新行为以及禁止该匹配。

- **Distinguished Name**（最多 10 个）- 指定在选择可接受的客户端证书时用于完全匹配条件的可分辨名称 (DN)。
  - **Name** - 用于匹配的可分辨名称 (DN)：
    - CN - 主题通用名

- C - 主题国家/地区
- DC - 域组件
- DNQ - 主题 DN 限定符
- EA - 主题邮件地址
- GENQ - 主题代际限定符
- GN - 主题给定名称
- I - 主题首字母缩写
- L - 主题城市
- N - 主题未定义的名称
- O - 主题公司
- OU - 主题部门
- SN - 主题姓氏
- SP - 主题省/自治区
- ST - 主题州
- T - 主题称谓
- ISSUER-CN - 颁发者通用名
- ISSUER-DC - 颁发者组件
- ISSUER-SN - 颁发者姓氏
- ISSUER-GN - 颁发者给定名称
- ISSUER-N - 颁发者未定义的名称
- ISSUER-I - 颁发者首字母缩写
- ISSUER-GENQ - 颁发者代际限定符
- ISSUER-DNQ - 颁发者 DN 限定符
- ISSUER-C - 颁发者国家/地区
- ISSUER-L - 颁发者城市
- ISSUER-SP - 颁发者所在省/自治区
- ISSUER-ST - 颁发者所在州
- ISSUER-O - 颁发者所在公司
- ISSUER-OU - 颁发者所在部门

- ISSUER-T - 颁发者称谓
- ISSUER-EA - 颁发者邮件地址

- **Pattern** - 指定要匹配的字符串。要匹配的型号应仅包括要匹配的字符串部分。不需要包括型号匹配或正则表达式语法。如果输入了语法，此语法将被视为待搜索字符串的一部分。

  例如，如果示例字符串是 abc.cisco.com，且为了与 cisco.com 匹配，则输入的型号应该是 cisco.com。

- **Operator** - 为此 DN 执行匹配时使用的运算符。
  - Equal - 与 == 等效
  - Not Equal - 与 != 等效
- **Wildcard** - 启用后将包含通配符型号匹配。在通配符启用的情况下，该型号可以位于字符串的任何位置。
- **Match Case** - 选中可启用区分大小写的型号匹配。

相关主题

配置证书匹配

AnyConnect 配置文件编辑器，证书注册

证书注册使 AnyConnect 能够使用简单证书注册协议 (SCEP) 调配和续订用于客户端身份验证的证书。

- **Certificate Expiration Threshold** - 在证书过期日前，AnyConnect 提醒用户其证书即将过期的天数（RADIUS 密码管理不支持该功能）。默认值为零（不显示警告）。值范围为 0 到 180 天。
- **macOS**
- 注册证书只能被导入到用户登录密钥链中。
- **移动平台**
- 注册证书只能被导入到应用程序沙盒。
- **Certificate Import Store**（**证书导入存储库**） — 选择保存注册证书的 Windows 证书存储库。
- **Certificate Contents** - 指定要包含在 SCEP 注册请求中的证书内容：
  - 名称 (CN) - 证书中的通用名。
  - 部门 (OU) - 证书中指定的部门名称。
  - 公司 (O) - 证书中指定的公司名称。
  - 州 (ST) - 证书中指定的州标识符。
  - 州 (SP) - 另一个州标识符。

- 国家/地区 (C) - 证书中指定的国家/地区标识符。
- 邮件 (EA) - 邮件地址。以下示例中，邮件地址 (EA) 为 %USER%@cisco.com。%USER% 对应用户的 ASA 用户名登录凭证。
- 域 (DC) - 域组件。在以下示例中，域 (DC) 设置为 cisco.com。
- 姓氏 (SN) - 家族名或姓。
- 给定名称 (GN) - 通常为名。
- UnstructName (N) - 未定义的名称。
- 首字母缩写 (I) - 用户的首字母缩写。
- 限定符 (GEN) - 用户的代限定符。例如，“Jr.”或“III.”
- 限定符 (DN) - 整个 DN 的限定符。
- 城市 (L) - 城市标识符。
- 称谓 (T) - 人员的称谓。例如，女士、夫人、先生
- CA 域 - 用于 SCEP 注册，一般为 CA 域。
- 密钥大小 - 为待注册证书所生成的 RSA 密钥的大小。

- **Display Get Certificate Button** - 启用 AnyConnect GUI 可在下列条件下显示 Get Certificate 按钮：
  - 证书设置为在证书过期阈值定义的时间段后过期（RADIUS 不支持）。
  - 证书已过期。
  - 证书不存在。
  - 证书无法匹配。

相关主题

配置证书注册

AnyConnect 配置文件编辑器，证书锁定

必备条件

开始证书锁定之前，请参阅关于证书锁定了解最佳实践。

使用VPN配置文件编辑器启用首选项，并配置全局证书锁定和按主机证书锁定。如果在“全局锁定(Global Pins)”部分中启用了首选项，则只能在服务器列表部分中按主机锁定证书。启用该首选项后，可以配置一个全局锁定列表，供客户端进行证书锁定验证使用。在服务器列表部分中添加按主机锁定与添加全局锁定类似。您可以锁定证书链中的任何证书，这些证书会被导入配置文件编辑器以计算锁定所需的信息。

添加锁定 (Add Pin) - 启动证书锁定向导，该向导会指导您将证书导入配置文件编辑器并锁定它们。

该窗口的证书详细信息部分允许您直观地验证“主题 (Subject)”和“颁发者 (Issuer)”列。

证书锁定向导

您可以将服务器证书链的任何证书导入到配置文件编辑器中，以指定锁定所需的信息。配置文件编辑器支持三个证书导入选项：

- 浏览本地文件 (Browse Local Files) - 选择本地存在于计算机上的证书。
- 从 URL 下载文件 (Download file from a URL) - 从任何文件托管服务器下载证书。
- 粘贴 PEM 格式的信息 (Paste information in PEM format) - 以 PEM 格式插入信息，包括证书开始报头和结束报头。

注释 您仅可导入 DER、PEM 和 PKCS7 数据格式的证书。

AnyConnect 配置文件编辑器，移动策略

AnyConnect 3.0 版及更高版本不支持 Windows Mobile 设备。请参阅 *Cisco AnyConnect Secure Mobility Client* 管理员指南，版本 *2.5*，了解 Windows Mobile 设备的相关信息。

AnyConnect 配置文件编辑器，服务器列表

您可以配置在客户端GUI中显示的服务器列表。用户可以在该列表中选择服务器以建立VPN连接。

服务器列表表列：

- 主机名 - 用于指代主机、IP 地址或完全限定域名 (FQDN) 的别名。
- 主机地址 - 服务器的 IP 地址或 FQDN。
- 用户组 - 用于与主机地址一同组成基于组的 URL。
- 自动 SCEP 主机 - 为调配和续订进行客户端身份验证的证书而指定的简单证书注册协议。
- CA URL - 此服务器用于连接到证书颁发机构 (CA) 的 URL。
- 证书锁定 - 在锁定验证期间，由客户端使用的按主机锁定。请参阅 AnyConnect 配置文件编辑器，证书锁定，第 16 页。

注释 客户端在锁定验证期间使用全局锁定和对应的按主机锁定。按主机锁定的配置方式类似于使用证书锁定向导配置全局锁定的方式。

Add/Edit - 启动 Server List Entry 对话框，您可在此指定上述服务器参数。

Delete - 从服务器列表中删除服务器。

Details - 显示有关备用服务器或服务器 CA URL 的更多详细信息。

相关主题

配置 VPN 连接服务器

AnyConnect 配置文件编辑器，添加/编辑服务器列表

- **Host Display Name** - 输入用于指代主机的别名、IP 地址或完全限定域名 (FQDN)。
- **FQDN or IP Address** - 指定服务器的 IP 地址或 FQDN。
  - 如果在“主机地址”(Host Address) 字段中指定了 IP 地址或 FQDN，则 Host Name 字段中的条目会变成 AnyConnect 客户端弹出式托盘的连接下拉列表中的服务器标签。
  - 如果仅在 Hostname 字段中指定了 FQDN，而未在 Host Address 字段中指定 IP 地址，则 Hostname 字段中的 FQDN 将由 DNS 服务器进行解析。
  - 如果输入 IP 地址，请使用安全网关的公共 IPv4 地址或全局 IPv6 地址。不支持使用链路本地安全网关地址。
- **User Group** - 指定一个用户组。

  用户组用于与主机地址一起形成一个基于组的URL。如果指定主要协议为 IPsec，则用户组必须是连接配置文件（隧道组）的确切名称。对于 SSL，用户组是连接配置文件的 group-url。

  注释 在 IKEv2/IPsec 连接中，当无法访问主服务器时，为主服务器输入的 **User Group**（用户组）信息会转发到备份服务器。要使 SSL 具有相同的行为，还必须将用户组信息作为 URL（例如，https://example.com/usergroup）而不只是 FQDN 提供给备份服务器。
- **Additional mobile-only settings** - 选择此项可配置 Apple iOS 和 Android 移动设备。
- **Backup Server List**

  我们建议您配置一个备用服务器列表，以便客户端在用户选择的服务器发生故障时使用。如果服务器发生故障，则客户端首先尝试连接到此列表顶端的服务器，必要时再沿着列表从上到下逐个尝试。

注释 相反，在 AnyConnect 配置文件编辑器，备用服务器，第 12 页 中配置的备用服务器是所有连接条目的全局条目。在配置文件编辑器的备份服务器中输入的任何条目都会被这里的备份服务器列表中的单个服务器列表条目所覆盖。此设置优先，并且是推荐做法。

- **Host Address** - 指定一个 IP 地址或 FQDN 以包含在备用服务器列表中。如果客户端无法连接到主机，则它将尝试连接到备用服务器。
- **Add** - 将主机地址添加到备用服务器列表。
- **Move Up** - 将选定的备用服务器在列表中向上移动。如果用户选择的服务器发生故障，则客户端首先尝试连接到此列表顶端的备用服务器，必要时再沿着列表从上到下逐个尝试。
- **Move Down** - 将选定的备用服务器在列表中向下移动。
- **Delete** - 从服务器列表中删除备用服务器。

- **Load Balancing Server List**

  如果此服务器列表条目的主机是安全设备的负载均衡集群，且启用了永远在线功能，则在此列表中指定集群的备用设备。否则，永远在线会阻止对负载均衡集群中备用设备的访问。

  - **Host Address** - 指定负载均衡集群中备用设备的 IP 地址或 FQDN。
  - **Add** - 将地址添加到负载均衡备用服务器列表中。
  - **Delete** - 从列表中删除负载均衡备用服务器。

- **Primary Protocol** - 指定连接到此服务器所用的协议，即 SSL 或 IPsec（与 IKEv2 结合使用）。默认协议是 SSL。
  - **Standard Authentication Only (IOS Gateways)** - 当选择 IPsec 作为协议时，您可以选择此选项，将连接的身份验证方法限制为 IOS 服务器。

    注释 如果此服务器是 ASA，则将身份验证方法从专有的 AnyConnect EAP 更改为基于标准的方法会禁用 ASA 的以下功能：配置会话超时、空闲超时、断开连接超时、分割隧道、拆分 DNS、MSIE 代理配置及其他功能。

  - **Auth Method During IKE Negotiation** - 选择一种基于标准的身份验证方法。
    - **IKE Identity** - 如果选择基于标准的 EAP 身份验证方法，您可以在此字段中输入一个组或域作为客户端标识。客户端将字符串以 ID_GROUP 型 IDi 负载的形式发送。默认情况下，此字符串是 *$AnyConnectClient$*。

- **CA URL** - 指定 SCEP CA 服务器的 URL。输入 FQDN 或 IP 地址。例如，http://ca01.cisco.com。
- **证书锁定 (Certificate Pins)** - 锁定验证期间由客户端使用的按主机锁定。请参阅AnyConnect 配置文件编辑器，证书锁定 ，第 16 页。
- **Prompt For Challenge PW** - 启用此项可让用户手动发出证书请求。当用户单击“获取证书”(Get Certificate) 时，客户端将提示用户输入用户名和一次性密码。
- **CA Thumbprint** - CA 的证书拇指指纹。使用 SHA1 或 MD5 哈希值。

注释 CA 服务器管理员可以提供 CA URL 和拇指指纹。拇指指纹应直接从服务器获取，而不是从它发布的证书的 fingerprint 或 thumbprint 属性字段中获取。

相关主题

配置 VPN 连接服务器

AnyConnect 配置文件编辑器，移动设置

Apple iOS/Android 设置

- **证书身份验证** - 与连接条目相关的证书身份验证策略属性指定如何处理此连接的证书。有效值为：
  - **Automatic** - AnyConnect 自动选择连接时进行身份验证所使用的客户端证书。在这种情况下，AnyConnect 将查看所有已安装的证书、忽略那些过期证书、应用 VPN 客户端配置文件中定义的证书匹配条件，然后使用与条件匹配的证书进行身份验证。每次设备用户尝试建立 VPN 连接时都会出现这种情况。
  - **Manual** - AnyConnect 将在下载配置文件并执行以下任一操作时，从 Android 设备上的 AnyConnect 证书存储库中搜索证书：
    - 如果 AnyConnect 基于 VPN 客户端配置文件中定义的证书匹配条件找到一个证书，则它将该证书分配给连接条目并在建立连接时使用该证书。
    - 如果找不到匹配的证书，证书身份验证策略将设置为“自动”。
    - 如果分配的证书因任何原因从 AnyConnect 证书存储库删除，则 AnyConnect 将证书身份验证策略重置为 Automatic。
  - **Disabled** - 客户端证书不用于身份验证。
- **Make this Server List Entry active when profile is imported** - 当 VPN 配置文件下载到设备时，将服务器列表条目定义为默认连接。只有一个服务器列表条目可以具有此名称。默认值为禁用。

仅适用于 Apple iOS 的设置

- **Reconnect when roaming between 3G/Wifi networks** - 该设置启用时（默认值），AnyConnect 在丢失连接、设备唤醒或连接类型发生更改（例如 EDGE(2G)、1xRTT(2G)、3G 或 Wi-Fi）后不限制用于尝试重新连接的时间。此功能提供了实现跨网络的持续安全连接的无缝移动性。此功能对于需要与企业连接的应用非常有用，但也会消耗更多的电池电量。

  如果网络漫游被禁用，且 AnyConnect 丢失连接，它在必要时尝试重新建立连接的时间最长可达 20 秒。如果无法建立连接，设备用户或应用必须启动一个新 VPN 连接（如果需要）。

  注释 网络漫游不影响数据漫游或使用多个移动服务提供商。

- **Connect on Demand**（需要证书颁发机构）- 此字段可让您配置由 Apple iOS 提供的按需连接功能。您可以创建规则列表，每当其他应用启动使用域名系统 (DNS) 解析的网络连接时都进行检查。

  按需连接仅可在 Certificate Authentication 字段设置为 Manual 或 Automatic 时使用。如果“证书身份验证”字段设置为“已禁用”，此复选框将变暗。在该复选框变暗时，仍可配置和保存由“匹配域或主机”以及“按需操作”字段定义的按需连接规则。

- **匹配域或主机** - 输入您希望为其创建按需连接规则的主机 (host.example.com)、域名 (.example.com) 或部分域 (.internal.example.com)。请勿在此字段中输入 IP 地址 (10.125.84.1)。

- **按需操作**指定设备用户尝试连接上一步中定义的域或主机时执行的下列操作之一：

  - **从不连接** - iOS 在匹配此列表中的规则时从不启动 VPN 连接。此列表中的规则优先于所有其他列表。

    注释 当 Connect on Demand 启用时，应用会将服务器地址自动添加到此列表中。这将防止您在尝试使用网络浏览器访问服务器的无客户端门户时自动建立 VPN 连接。如果您不希望发生此行为，请删除此规则。

  - **按需连接** - iOS 仅在系统因无法使用 DNS 解析地址而匹配此列表中的规则时启动 VPN 连接。

  - **Always Connect** - 始终连接行为与版本有关：

    - 在 Apple iOS 6 上，iOS 在匹配此列表中的规则时始终启动 VPN 连接。
    - iOS 7.x 上不支持 Always Connect，当此列表中的规则匹配时，其行为与 Connect If Needed 规则相同。
    - 更高版本中不使用 Always Connect，配置的规则将跳转到 Connect if Needed 列表，并按照该规则操作。

- **添加或删除** - 将“匹配域或主机”和“按需操作”字段中指定的规则添加到规则表中，或从规则表中删除所选的规则。

NVM 配置文件编辑器

在配置文件编辑器中，配置收集服务器的 IP 地址或 FQDN。您还可以自定义数据收集策略，用于选择要发送哪些类型数据，以及确定数据是否匿名。

网络可视性模块可以使用包含 IPv4 地址的单个堆栈 IPv4、包含 IPv6 地址的单个堆栈 IPv6 或双堆栈 IPv4/IPv6，建立与操作系统首选的 IP地址的连接。

移动网络可视性模块仅可以使用 IPv4 建立连接。不支持 IPv6 连接。

注释 当网络可视性模块在受信任网络中时，该模块发送流量信息。默认情况下，不收集任何数据。仅在配置文件中进行了相应配置时才会收集数据，且连接终端后，会继续收集数据。如果在一个不可信网络上进行收集，则会缓存数据，并在终端处于受信任的网络中时发送数据。如果您将收集数据发送到 Stealthwatch 7.3.1 及更低版本（或 Splunk 及类似 SIEM 工具之外的工具），则缓存数据会在受信任网络上发送一次，但不会进行处理。对于 Stealthwatch 应用程序，请参阅 Stealthwatch 企业终端许可证和 NVM 配置指南。

如果已在 NVM 配置文件中配置了 TND，则受信任的网络检测由 NVM 完成，并且不依赖于 VPN 来确定终端是否位于受信任的网络中。此外，如果 VPN 为已连接状态，则会将终端视作处于受信任网络中，并会发送流信息。NVM 特定的系统日志会显示 TND 使用情况。

直接在 NVM 配置文件中配置 TND 时，管理员定义的受信任服务器和证书散列将确定用户位于受信任还是不受信任的网络上。管理员为核心 VPN 配置文件配置 TND 会在核心 VPN 配置文件中另外配置受信任 DNS 域和受信任 DNS 服务器：AnyConnect 配置文件编辑器，首选项（第 2 部分），第 7 页。

- **桌面 (Desktop)** 或**移动 (Mobile)** - 确定是在桌面还是移动设备上设置 NVM。**桌面 (Desktop)** 是默认值。 未来将支持移动设备。
- **收集器配置**
  - **IP 地址/FQDN (IP Address/FQDN)** - 指定收集器的 IPv4 或 IPv6 IP 地址/FQDN。
  - **端口 (Port)** - 指定收集器正在侦听哪个端口号。
  - **安全 (Secure)** - 确定是否希望 NVM 通过 DTLS 安全地将数据发送到收集器。选中此复选框后，NVM 将使用 DTLS 进行传输。DTLS 连接要求终端信任 DTLS 服务器（收集器）证书。系统将以静默方式拒绝任何不受信任的证书。

    DTLS 支持需要收集器作为 CESA Splunk 应用 v3.1.0 的一部分，DTLS 1.2 是支持的最低版本。
- **缓存配置**

- **最大大小 (Max Size)** - 指定该数据库可以达到的最大大小。以前对缓存大小有预设的限制，但您现在可在配置文件中配置它。缓存中的数据以加密格式存储，因此只有拥有根权限的进程可以解密数据。

  一旦达到大小限制，将从空间中丢弃最旧数据，将空间留给新数据。

- **最大持续时间 (Max Duration)** - 指定您希望将数据存储多少天。如果您还设置了最大大小，则首先达到的限制优先。

  一旦达到天数限制，将从空间中丢弃日期最早的数据，将空间留给日期最近的数据。如果仅配置了“最大持续时间 (Max Duration)”，则没有大小上限；如果二者都被禁用，则大小上限为 50 MB。

- **定期模板**- 指定从终端发出模板的时间间隔。默认值为 1440 分钟
- **定期流量报告**（可选，仅应用于桌面）- 单击以启用定期流量报告。默认情况下，NVM 发送连接结束时的流量相关信息 （当禁用此选项时）。如果需要定期的流量相关信息（甚至在这些流量被关闭之前），请在此处设置间隔（以秒为单位）。值为 0 表示在每个流量开始和结束时发送流量信息。如果值为 *n*，则将在每个流量开始时、每隔 *n* 秒时和结束时发送流量信息。使用此设置跟踪长期运行的连接（甚至在这些连接被关闭之前）。
- **聚合时间间隔** - 指定从端点导出数据流的时间间隔。使用 5 秒默认值时，一个数据包中将捕获不止一个数据流。如果时间间隔值为 0 秒，则每个数据包都有一个数据流。有效范围为 0 到 600 秒。
- **限制速率 (Throttle Rate)** - 限制控制以什么速率将数据从缓存发送到收集器，以便尽量减小对最终用户的影响。您可以对实时和缓存数据应用限制（只要存在缓存的数据）。以 Kbps 为单位，输入限制速率。默认值为 500 Kbps。

  在该固定时段后，缓存数据将被导出。输入 0 将禁用该功能。
- **收集模式 (Collection Mode)** - 通过选择收集模式关闭 (collection mode is off)、仅受信任网络 (trusted network only)、仅不受信任网络 (untrusted network only) 或所有网络 (all networks)，指定应从终端收集数据的时间。
- **收集标准 (Collection Criteria)** - 您可以在数据收集时减少不必要的广播，以便仅分析相关数据。通过以下选项控制数据搜集：

  - **广播数据包 (Broadcast packets)** 和**组播数据包 (Multicast packets)**（仅适用于桌面）- 默认情况下，为了提高效率，会关闭广播和组播数据包收集，以便缩短在后端资源上花费的时间。单击该复选框可启用对广播和组播数据包的收集并过滤数据。
  - **仅限 KNOX (KNOX only)**（可选且特定于移动设备）- 选中后，将仅从 KNOX 工作空间收集数据。默认情况下，未选中此字段，将会从工作空间内部和外部收集数据。

- **数据收集策略 (Data Collection Policy)** - 您可以添加数据收集策略，并将它们与网络类型或连接情形相关联。您可以将一种策略应用于 VPN，而将另一种策略应用于非 VPN 流量，因为多个接口可以同时处于活跃状态。

  在单击“添加”(Add) 时，系统显示“数据收集策略”(Data Collection Policy) 窗口。在创建策略时，请记住以下指导原则：

- 默认情况下，如果未创建策略或未与网络类型相关联，则将报告和收集所有字段。
- 每种数据收集策略必须与至少一种网络类型相关联，但您不能将两种策略与同一种网络类型相关联。
- 具有更具体的网络类型的策略优先。例如，因为 VPN 是受信任网络的一部分，所以包含 VPN 网络类型的策略的优先级高于采用受信任网络为指定网络的策略。
- 您只能基于所选的收集型号，为网络创建适用的数据收集策略。例如，如果**收集模式 (Collection Mode)** 设置为 **仅受信任网络 (Trusted Network Only)**，您无法为**不受信任网络类型 (Untrusted Network Type)** 创建**数据收集策略 (Data Collection Policy)**。
- 如果从较新版本的 AnyConnect 打开来自较早版本 AnyConnect 的配置文件，它会自动将该配置文件转换为较新的版本。转换过程中会为所有网络添加数据收集策略，用于排除先前匿名的字段。
- **名称 (Name)** - 为您要创建的策略指定名称。
- **Network Type** - 通过选择 VPN、受信任或不受信任，来确定收集型号，或者应用数据收集策略的网络。如果您选择受信任网络，则策略也适用于 VPN 案例。
- **流过滤器规则** - 定义一组条件和一个操作，可以在满足所有条件时收集或忽略流。您最多可以配置 25 条规则，每条规则最多可以定义 25 个条件。使用“流过滤器规则”列表右侧的向上和向下按钮调整规则的优先级，并对后续规则给予更高的考虑。单击**添加 (Add)** 设置流过滤器规则的组成要素。
  - 名称 - 流过滤器规则的唯一名称。
  - 类型 - 每个过滤器规则都有“收集”或“忽略”类型。确定满足过滤器规则时要执行的操作（“收集”或“忽略”）。如果收集，则在满足条件时允许流。如果忽略，则丢弃流。
  - 条件 - 为要匹配的每个字段添加一个条目以及一个运算，以确定字段值对匹配项是否应相等或不相等。每个运算都有一个字段标识符和该字段的对应值。该字段区分大小写，除非您在设置过滤器引擎规则时对规则集应用了不区分大小写操作 (EqualsIgnoreCase)。启用后，规则中设置的 Value 字段中的输入不区分大小写。
- **包括/排除**
  - **类型 (Type)** - 确定要在数据收集策略中**包含 (Include)** 或**排除 (Exclude)** 的字段。默认值为**排除 (Exclude)**。所有未选中的字段都收集起来。未选中任何字段时，将收集所有字段。
  - **字段** - 确定要从终端接收哪些信息以及收集哪些字段的数据以满足策略要求。根据网络类型和包含或排除的字段，NVM 将在终端上收集相应数据。

注释 升级期间，如果存在以下情况之一，默认从流信息的报告中排除 ProcessPath、ParentProcessPath、ProcessArgs 和 ParentProcessArgs：

- 如果较旧版本NVM中的配置文件没有数据收集策略或有包含数据收集策略。
- 如果较旧版本 NVM 中的配置文件有排除数据收集策略，并且该配置文件已使用更新的4.9版本配置文件编辑器打开并保存。如果较旧版本NVM中的配置文件有排除数据收集策略，但该配置文件未使用更新的4.9版本配置文件编辑器打开和保存，则包含这四个字段。

如果 NVM 无法计算父进程 ID，则值默认为 4294967295。

FlowStartMsec 和 FlowStopMsec 确定流的纪元时间戳（以毫秒为单位）。

对于 AnyConnect 版本4.4（和更高版本），您现在可以选择接口状态和 SSID，这将指定接口的网络状态为受信任还是不受信任。

- **Optional Anonymization Fields** - 如果要关联同一终端上的记录，同时保留隐私，请选择所需的字段进行匿名化，它们将作为值的哈希而不是实际值进行发送。字段的子集可用于匿名化。

  标记为包含或排除的字段不可用于匿名；同样，标记为匿名的字段不可用于包含或排除。

- **用于 Knox 的数据收集策略 (Data Collection Policy for Knox)**（**特定于移动设备**）- 该选项用于在选择移动配置文件时指定数据收集策略。要为Knox容器创建数据收集策略，请选择Scope下的 **Knox-Only** 复选框。除非指定单独的 Knox 容器数据收集策略，否则应用于 Knox 容器流量的设备范围内的数据收集策略也适用于 Knox 容器流量。要添加或删除数据收集策略，请参阅上面的数据收集策略说明。您可以为移动配置文件设置最多 6 个不同的数据收集策略：3 个用于设备，3 个用于 Knox。

- **可接受的使用策略 (Acceptable Use Policy)**（可选且特定于移动设备）- 单击**编辑 (Edit)**，在对话框中为移动设备定义可接受的使用策略。完成后，单击**确定 (OK)**。最多允许 4000 个字符。

  配置NVM后，此消息会显示给用户。远程用户无法选择拒绝NVM活动。网络管理员使用MDM工具控制 NVM。

- **Export on Mobile Network**（**可选且特定于移动设备**）- 指定在设备使用移动网络时，是否允许导出 NVM 流。如果启用（默认值），当显示或后续通过 **设置** > **NVM-设置** > > **将移动数据用于** AnyConnect Android 应用中的 NVM" 复选框来启动 “可接受的用户策略” 窗口时，最终用户可以覆盖管理员 。如果取消选中"在移动网络上导出"复选框，当设备使用移动网络时，不会导出 NVM 流，最终用户无法对其进行更改。

- **受信任的网络检测** — 此功能可检测终端是否实际上位于企业网络中。NVM 使用网络状态来确定何时导出 NVM 数据并应用相应的数据收集策略。单击**配置 (Configure)** 以设置受信任的网络检测的配置。SSL 探测会发送到已配置的受信任前端，如果可访问，则前端会使用证书响应。然后，系统将根据配置文件编辑器中的散列设置提取指纹（SHA-256 散列）并将其与之匹配。成功匹配表明终端位于受信任的网络中；但是，如果前端无法访问，或者如果证书散列不匹配，则系统会将终端视为位于不受信任的网络中。

  注释 从内部网络的外部进行操作时，TND 会执行 DNS 请求并尝试与已配置服务器建立 SSL 连接。思科强烈建议使用别名，以确保在内部网络以外使用的机器不会通过这些请求泄露您组织的名称和内部结构。

  如果 TND 未在 NVM 配置文件中配置或如果已安装了 VPN 模块，NVM 会使用 VPN 的 TND 功能来确定终端是否位于受信任的网络中。NVM 配置文件编辑器中的 TND 配置包括以下内容：

  1. **https://** — 输入每个受信任服务器的 URL （IP 地址、FQDN 或端口地址），然后单击**添加 (Add)**）。

     注释 代理后的受信任服务器不受支持。

  2. **证书散列 (SHA-256)** — 如果与受信任服务器的 SSL 连接成功，则系统会自动填充此字段。否则，您可以通过输入服务器证书的 SHA-256 散列并单击**设置 (Set)** 来手动对其进行设置。
  3. **受信任服务器列表** — 通过此过程可以定义多个受信任服务器。（至多 10 个。）由于服务器会按已配置的顺序尝试受信任的网络检测，因此您可以使用**上移**和**移动 |向下**按钮来调整该顺序。如果终端无法连接到第一台服务器，它会尝试连接第二台服务器，依此类推。在对列表中的所有服务器进行尝试后，终端等待 10 秒后会再进行最后一次尝试。当服务器进行身份验证时，系统会视为终端在受信任的网络中。

将配置文件另存为 `NVM_ServiceProfile.xml`。您必须将配置文件准确保存为此名称，否则 NVM 将无法收集和发送数据。

AnyConnect 本地策略

AnyConnectLocalPolicy.xml 是包含安全设置的客户端上的 XML 文件。ASA 不部署该文件。您必须使用企业软件部署系统手动安装该文件或将其部署到用户计算机中。如果您对用户系统中的现有本地策略文件进行了更改，则系统将重启。

本地策略首选项

您可以在 VPN 本地策略编辑器中指定要包含在 `AnyConnectLocalPolicy.xml` 文件中的以下首选项。

手动更改本地策略参数

过程

步骤 1 从客户端安装检索 AnyConnect 本地策略文件 (AnyConnectLocalPolicy.xml) 的副本。

表 *1:* 操作系统和 *AnyConnect* 本地策略文件安装路径

操作系统	安装路径
Windows	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Linux	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect

步骤 2 编辑参数设置。您可以手动编辑 AnyConnectLocalPolicy 文件，或使用随 AnyConnect 配置文件编辑器安装程序分发的 VPN 本地策略编辑器。

步骤 3 将该文件另存为 `AnyConnectLocalPolicy.xml`，并使用公司软件部署系统将文件部署到远程计算机。

步骤 4 重启远程计算机，以便使对本地策略文件的更改生效。

在 MST 文件中启用本地策略参数

有关说明和可以设置的值，请参阅本地策略首选项。

创建 MST 文件以更改本地策略参数。MST 参数名称对应于 AnyConnect 本地策略文件 (AnyConnectLocalPolicy.xml) 中的参数：

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

注释 AnyConnect 安装不会自动覆盖用户计算机上的现有本地策略文件。必须先删除用户计算机上的现有策略文件，以便客户端安装程序可以创建新的策略文件。

注释 对本地策略文件的任何更改都需要重新启动系统。