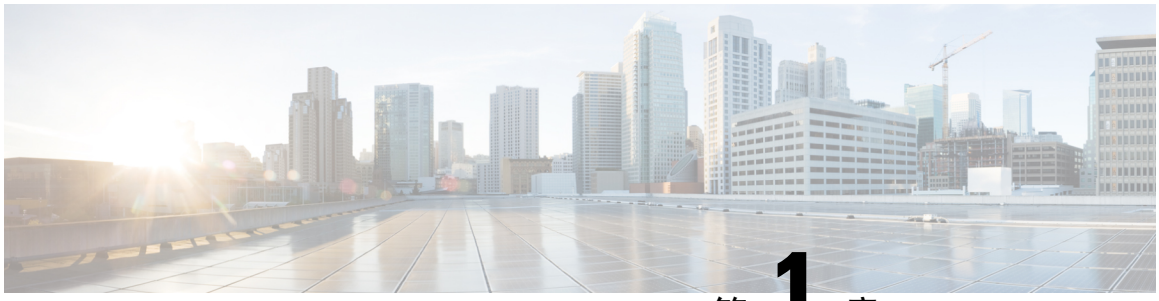
思科 **AnyConnect** 移动平台管理员指南，**4.7** 版

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录



第 1 章

移动设备上的 AnyConnect

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

移动设备上的 AnyConnect 操作和选项

关于 AnyConnect 移动 VPN 连接

此版本的 AnyConnect 安全移动客户端可用于以下移动平台：

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

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

AnyConnect VPN 连接可以通过以下方法之一建立：

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

移动设备上的 AnyConnect VPN 连接条目

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

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

- 用户手动配置。有关在移动设备上配置连接条目的过程，请参阅相应平台的用户指南。
- 由 Anyconnect VPN 客户端配置文件定义。

  AnyConnect VPN 客户端配置文件指定客户端行为并定义 VPN 连接条目。有关详细信息，请参阅在 AnyConnect VPN 配置文件中配置移动设备连接，第 8 页。

隧道型号

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

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

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

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

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

移动设备的安全网关身份验证

阻止不受信任的服务器

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

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

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

- **保持我的安全状态 (Keep Me Safe)** 以终止此连接，保持安全。

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

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

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

  如果用户正在查看的证书有效但不受信任，则用户可以：

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

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

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

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

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

注释 **严格证书信任**将覆盖此设置，请参阅以下说明。

移动设备上的客户端身份验证

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

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

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

- 由用户手动导入。有关向移动设备导入证书的过程，请参阅相关的用户指南。
- 使用 SCEP。有关详细信息，请参阅配置证书注册，第 77 页。

在移动设备上本地化

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

预包装的本地化

AnyConnect 和 Apple iOS 应用包括以下语言翻译：

- 加拿大法语 (fr-ca)
- 中文（台湾地区）(zh-tw)
- 捷克语 (cs-cz)
- 荷兰语 (nl-nl)
- 法语 (fr-fr)
- 德语 (de-de)
- 匈牙利语 (hu-hu)
- 意大利语 (it-it)
- 日语 (ja-jp)
- 韩语 (ko-kr)
- 拉丁美洲西班牙语 (es-co)
- 波兰语 (pl-pl)
- 葡萄牙语（巴西）(pt-br)
- 俄语 (ru-ru)
- 简体中文 (zh-cn)
- 西班牙语 (es-es)

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

下载的本地化

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

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

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

有关在 ASA 上配置本地化的说明，请参阅将转换表导入自适应安全设备，第 5 页。如果 ASA 不包含设备区域设置的本地化数据，将继续使用 AnyConnect 应用软件包中预装的本地化数据。

在移动设备上提供本地化的更多方式

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

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

将转换表导入自适应安全设备

过程

步骤 1 从 www.cisco.com 下载所需的转换表。

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

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

步骤 4 从下拉列表中选择适合的语言。

步骤 5 指定从何处导入转换表。

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

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

移动设备上的 FIPS 和套件 B 加密

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

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

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

其他移动准则和限制

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

在 ASA 安全网关上配置移动设备 VPN 连接

过程

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

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

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

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

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

示例：

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

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

在 AnyConnect VPN 配置文件中配置移动设备连接

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

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

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

过程

步骤 1 配置基本 VPN 访问。

请参阅配置 VPN 访问，第 39 页，了解桌面和移动终端通用的处理以下例外的程序：

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

步骤 2 配置移动特定属性：

a) 在 VPN 客户端配置文件中，选择导航窗格中的 **Server List**。
b) 选择 **Add** 将新服务器条目添加至列表，或从列表中选择服务器条目并按 **Edit** 打开 Server List Entry 对话框。
c) 配置特定于移动设备的参数（如AnyConnect 配置文件编辑器，移动设置，第 28 页中所述）。
d) 点击**确定**

步骤 3 使用以下方式之一来分发 VPN 客户端配置文件：

- 配置 ASA 以在建立 VPN 连接后将客户端配置文件上传到移动设备。

  请参阅AnyConnect 配置文件编辑器，第 11 页章节，了解关于如何将 VPN 客户端配置文件导入 ASA 并将其与组策略相关联的说明。

排除移动设备上的 AnyConnect 故障

开始之前

在移动设备上启用日志记录，并按照相应用户指南中的故障排除说明执行操作：

如果遵循这些说明未能解决问题，请尝试以下操作：

过程

步骤 1 确定在桌面客户端或其他移动操作系统上是否发生相同的问题。

步骤 2 确保在 ASA 中已安装适当的许可证。

步骤 3 如果证书身份验证失败，请检查以下项：

a) 确保选择了正确的证书。

b) 确保设备中的客户端证书将客户端身份验证作为扩展密钥使用。

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

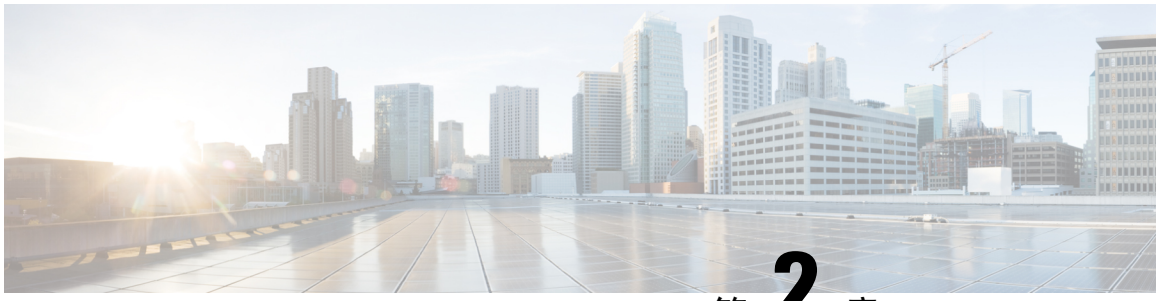
即便用户选择了证书，如果该证书不匹配配置文件中的过滤规则，也不会使用它进行身份验证。

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

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

下一步做什么

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



第 2 章

AnyConnect 配置文件编辑器

关于配置文件编辑器

思科 AnyConnect 安全移动客户端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** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Client Profile**。

步骤 2 单击 **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 Profile Location 字段中，单击 **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 **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 **OK**。

AnyConnect VPN 配置文件

AnyConnect 配置文件中启用了思科 AnyConnect 安全移动客户端功能。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 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“登录前启动”和/或“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 Logon** -（仅限 Windows）通过在 Windows 登录对话框出现之前启动 AnyConnect，强制用户在登录到 Windows 之前通过 VPN 连接而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。
- **Show Pre-connect Message** - 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** - 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。

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

- All（对于 Windows）- ASA 配置接受一台计算机和一个用户证书。
- User（对于 Windows）- ASA 配置接受两个用户证书。
- All（对于 macOS）- 使用所有可用 macOS 密钥链和文件存储区的证书。
- System（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（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。

- **Certificate Store Override** - 允许管理员指示 AnyConnect 在用户对其设备没有管理员权限时在 Windows 计算机证书存储库中搜索证书。证书存储区覆盖仅适用于 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。
- **Minimize On Connect** - 建立 VPN 连接后，AnyConnect GUI 最小化。
- **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。

- **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。

- **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。

  - **Auto Reconnect Behavior**
    - 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。

- **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 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 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拆分隧道。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。
  - 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。

- **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 Logon Enforcement** - 允许从 SSH 会话建立 VPN 会话。必须在组策略中配置拆分隧道。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。
  - 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 多个并行登录会被视为单个登录会话。如果用户同时具有本地和远程登录会话，则其会被视为本地用户。

- **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：
  - 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。

- **Clear SmartCard PIN**

- **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 IPv4 与 IPv6 协议之间的故障切换也可能发生在 VPN 会话期间。如果主 IP 协议丢失，在可能的情况下将通过副 IP 协议重新建立 VPN 会话。

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

- **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。

- **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

- **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，它不会在安全网关群集之间或群集内执行负载均衡。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。Automatic Selection 显示在客户端 GUI 的 Connection 选项卡中的 Connect To 下拉列表中。
  - **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。

- **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。

- **Automatic VPN Policy**（仅限 Windows 和 Mac）- 启用 Trusted Network Detection 可使 AnyConnect 根据 Trusted Network Policy 和 Untrusted Network Policy 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。
  - **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。
    - Disconnect（默认值）- 检测到受信任网络时断开 VPN 连接。
    - Connect - 检测到受信任网络时发起 VPN 连接。
    - Do Nothing - 在不受信任的网络中不执行任何操作。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 Do Nothing 会禁用 Trusted Network Detection。
    - 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。
  - **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。
    - 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。此选项禁用永不间断 VPN。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 Do Nothing 会禁用 Trusted Network Detection。
  - **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 (*)。

- **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。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。在单击 **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 **Set**。

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。如果未定义受信任的 DNS 域或受信任的 DNS 服务器，则会禁用此字段。

- **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不间断 VPN 参数来覆盖此设置。如果 AnyConnect 策略启用永不间断，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：需要使用永不间断的 VPN 连接

  - **Allow VPN Disconnect** - 确定 AnyConnect 是否为永不间断 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，永不间断 VPN 会话的用户可能想要单击 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 接入。

  - **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不间断和 Allow VPN Disconnect 时才适用。如果选择永不间断，则 fail-open 策略允许网络连接，fail-close 策略禁用网络连接。
    - 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 以外的互联网接入，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不间断 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

- **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 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。
  - Automatic - 启用 PPP 排除。AnyConnect 自动使用 PPP 服务器的 IP 地址。指示用户仅在自动检测无法获取 IP 地址时更改值。

- Disabled - 不应用 PPP 排除。
- Override - 也会启用 PPP 排除。当自动检测无法获取 PPP 服务器的 IP 地址且您将 PPP 排除配置为用户可控制时，选择此选项。

如果启用了 PPP Exclusion，则还要设置：

- **PPP Exclusion Server IP** - 用于 PPP 排除的安全网关的 IP 地址。

- **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。）
- **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。
  - **User Enforcement** - 指定当其他用户登录时是否结束 VPN 会话。此参数仅在“Retain VPN On Logoff”被选中且原始用户在 VPN 会话进行中注销 Windows 或 Mac OS X 时适用。
- **Authentication Timeout Values** - 默认情况下，AnyConnect 在终止连接尝试前，要等待长达 12 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 26 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 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，第 85 页

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。
- **Certificate Import Store** - 选择保存注册证书的 Windows 证书存储区。
- **Certificate Contents** - 指定要包含在 SCEP 注册请求中的证书内容：
  - Name (CN) - 证书中的通用名。
  - Department (OU) - 证书中指定的部门名称。
  - Company (O) - 证书中指定的公司名称。
  - State (ST) - 证书中指定的州标识符。
  - State (SP) - 另一个州标识符。
  - Country (C) - 证书中指定的国家/地区标识符。
  - Email (EA) - 邮件地址。以下示例中，Email (EA) 为 %USER%@cisco.com。%USER% 对应用户的 ASA 用户名登录凭证。
  - Domain (DC) - 域组件。在以下示例中，Domain (DC) 设置为 cisco.com。
  - SurName (SN) - 家族名或姓。
  - GivenName (GN) - 通常为名。
  - UnstructName (N) - 未定义的名称。
  - Initials (I) - 用户的首字母缩写。
  - Qualifier (GEN) - 用户的代限定符。例如，“Jr.”或“III.”
  - Qualifier (DN) - 整个 DN 的限定符。
  - City (L) - 城市标识符。
  - Title (T) - 人员的称谓。例如，女士、夫人、先生
  - CA Domain - 用于 SCEP 注册，一般为 CA 域。
  - Key size - 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，第 77 页

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，第 94 页了解最佳实践。

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 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。

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 Subject 和 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：

- Browse Local Files - 选择本地存在于计算机上的证书。
- Download file from a URL - 从任何文件托管服务器下载证书。
- 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。请参阅思科 *AnyConnect* 安全移动客户端管理员指南，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：

- Hostname - 用于指代主机、IP 地址或完全限定域名 (FQDN) 的别名。

- Host Address - 服务器的 IP 地址或 FQDN。
- User Group - 用于与主机地址一同组成基于组的 URL。
- Automatic SCEP Host - 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。
- Certificate Pins - 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 25 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，第 41 页

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 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组 URL 或组别名。
- **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 20 页中配置的备用服务器是所有连接条目的全局条目。将使用在此处为单个服务器列表条目输入的条目覆盖放入备用服务器位置中的任何条目。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群集，且启用了永不间断功能，则在此列表中指定群集的备用设备。否则，永不间断会阻止对负载均衡群集中备用设备的访问。

  - **Host Address** - 指定负载均衡群集中备用设备的 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、拆分隧道、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。

- **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 25 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 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，第 41 页

AnyConnect 配置文件编辑器，移动设置

Apple iOS/Android 设置

- **Certificate Authentication** - 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 证书存储区中搜索证书：
    - 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 Automatic。
    - 如果分配的证书因任何原因从 AnyConnect 证书存储区删除，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 Certificate Authentication 字段设置为 Disabled，此复选框将变暗。在该复选框变暗时，仍可配置和保存由 Match Domain or Host 以及 On Demand Action 字段定义的按需连接规则。

- **Match Domain or Host** - 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)。

- **On Demand Action** 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：

  - **Never connect** - 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。

  - **Connect if Needed** - 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。

- **Add or Delete** - 将 Match Domain or Host 和 On Demand Action 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。

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。但是，如果 TND 未在 NVM 配置文件中明确配置，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。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。有关 TND 参数设置的信息，请参阅 AnyConnect 配置文件编辑器，首选项（第 2 部分），第 16 页。

- **Desktop** 或 **Mobile** - 确定是在桌面还是移动设备上设置 NVM。**Desktop** 是默认值。未来将支持移动设备。
- **收集器配置**
  - **IP Address/FQDN** - 指定收集器的 IPv4 或 IPv6 IP 地址/FQDN。
  - **Port** - 指定收集器正在侦听哪个端口号。
- **缓存配置**
  - **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 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。
- **Periodic Flow Reporting**（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）。

- **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。
- **Collection Mode** - 通过选择 collection mode is off、trusted network only、untrusted network only 或 all networks，指定应从终端收集数据的时间。
- **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：
  - **Broadcast packets** 和 **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。
  - **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。
- **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 Add 时，系统显示 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 **Collection Mode** 设置为 **Trusted Network Only**，您无法为 **Untrusted Network Type** 创建 **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。
  - **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。
  - **Flow Filter Rule** - 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 Flow Filter Rules 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 **Add** 设置流过滤器规则的组成要素。
    - Name - 流过滤器规则的唯一名称。

- Type - 每个过滤器规则都有 Collect 或 Ignore 类型。确定满足过滤器规则时要执行的操作（Collect 或 Ignore）。如果收集，则在满足条件时允许流。如果忽略，则丢弃流。
- Conditions - 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。字段匹配区分大小写。

  Conditions - 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
  - **Type** - 确定要在数据收集策略中 **Include** 或 **Exclude** 的字段。默认值为 **Exclude**。会收集所有未选中的字段，而且未选中任何字段。
  - **Fields** - 确定将哪些字段作为数据收集策略的一部分。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。

    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（移动特定于移动设备）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 "范围" 下的 "**仅 Knox** " 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。
- **Acceptable Use Policy**（可选且特定于移动设备）- 单击 **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 **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。
- **受信任的网络检测** — 此功能可检测终端是否实际上位于公司网络中。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。点击**配置**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 配置值得信赖的网络检测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**）。

   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**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。

本地策略参数和值

以下参数是 VPN 本地策略编辑器和`AnyConnectLocalPolicy.xml`文件中的元素。XML 元素显示在尖括号中。

注释 如果您手动编辑此文件并忽略策略参数，则该功能采取默认行为。

- <acversion>

指定能够解释该文件中所有参数的最低版本的 AnyConnect 客户端。如果客户端运行比此版本更早的 AnyConnect 版本，则它读取文件时会发出事件日志警告。

格式是 acversion="<version number>"。

- **FIPS Mode** <FipsMode>

  为客户端启用 FIPS 型号。此设置强制客户端仅使用 FIPS 标准批准的算法和协议。

- **Bypass Downloader** <BypassDownloader>

  选择后，禁用 VPNDownloader.exe 模块启动，该模块负责检测本地版本动态内容的存在和更新。客户端不检查 ASA 上的动态内容，包括转换、定制、可选模块和核心软件更新。

  选中 Bypass Downloader 时，在客户端连接到 ASA 时将发生两种情况之一：

  - 如果 ASA 上的 VPN 客户端配置文件不同于客户端上的 VPN 客户端配置文件，则客户端将中止连接尝试。
  - 如果 ASA 上没有 VPN 客户端配置文件，则客户端会建立 VPN 连接，但它使用其硬编码的 VPN 客户端配置文件设置。

  注释 如果您在 ASA 上配置 VPN 客户端配置文件，则这些文件必须在客户端连接到 ASA 之前安装在客户端上（BypassDownloader 设置为 true）。因为配置文件可以包含管理员定义的策略，所以只在您不依赖于 ASA 来集中管理客户端配置文件时，才建议将 BypassDownloader 设置为 true。

- **Enable CRL Check** <EnableCRLCheck>

  仅对 *Windows* 桌面实施此功能。对于 SSL 和 IPsec VPN 连接，可以选择执行证书吊销列表 (CRL) 检查。启用此设置后，AnyConnect 检索链中所有证书的已更新 CRL。然后，AnyConnect 验证有关证书是否包含在不应再信任的这些已吊销证书中。如果发现该证书已被证书颁发机构 (CA) 吊销，则不进行连接。

  默认情况下会禁用 CRL 检查。仅当选中（或启用）Enable CRL Check 时，AnyConnect 才会执行 CRL 检查，因此，最终用户可能会观察到以下情况：

  - 如果通过 CRL 吊销证书，即使在 AnyConnect 本地策略文件中禁用 Strict Certificate Turst，与安全网关的连接也会无条件失败。
  - 如果无法检索 CRL（例如由于无法访问 CRL 分发点），并且在 AnyConnect 本地策略文件中启用 Strict Certificate Turst，与安全网关的连接也会无条件失败。否则，如果禁用 Strict Certificate Turst，则系统可能会提示该用户绕过此错误。

  注释 启用 Always On 时，AnyConnect 无法执行 CRL 检查。此外，如果 CRL 分发点不是公开可访问，则 AnyConnect 可能会遇到服务中断。

- **Restrict Web Launch** <RestrictWebLaunch>

  阻止用户使用不符合FIPS的浏览器来发起WebLaunch。其实现途径是阻止客户端获取用于发起AnyConnect 隧道的安全 Cookie。客户端向用户显示一条信息性消息。

- **Strict Certificate Trust** <StrictCertificateTrust>

  如果选中此项，则在对远程安全网关进行身份验证时，AnyConnect不允许它无法验证的任何证书。客户端并不提示用户接受这些证书，而是无法使用自签证书连接到安全网关并显示本地策略禁止接受不受信任的服务器证书。不会建立连接。。如果未选中，客户端将提示用户接受证书。这是默认行为。

  我们强烈建议您为 AnyConnect 客户端启用 Strict Certificate Trust，原因如下：

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

- **Restrict Preference Caching** <RestrictPreferenceCaching>

  根据设计，AnyConnect不将敏感信息缓存到磁盘。启用此参数会将本策略扩展到在AnyConnect首选项中存储的任何类型的用户信息。

  - Credentials - 不缓存用户名和辅助用户名。
  - Thumbprints - 不缓存客户端和服务器的证书拇指指纹。
  - CredentialsAndThumbprints - 不缓存证书拇指指纹和用户名。
  - All - 不缓存任何自动首选项。
  - false - 所有首选项都写入磁盘（默认值）。

- **Exclude Pem File Cert Store**（Linux 和 macOS）<ExcludePemFileCertStore>

  防止客户端使用 PEM 文件证书存储库来验证服务器证书和搜索客户端证书。

  存储库使用支持FIPS的OpenSSL，并具有关于在哪里可以获取客户端证书身份验证所需证书的信息。允许 PEM 文件证书存储库可确保远程用户使用符合 FIPS 的证书存储库。

- **Exclude Mac Native Cert Store**（仅限 macOS）<ExcludeMacNativeCertStore>

  防止客户端使用 Mac 本地 (keychain) 证书存储区验证服务器证书和搜索客户端证书。

- **Exclude Firefox NSS Cert Store**（Linux 和 macOS）<ExcludeFirefoxNSSCertStore>

  防止客户端使用 Firefox NSS 证书存储库来验证服务器证书和搜索客户端证书。

  存储库有关于在何处为客户端证书身份验证取得证书的信息。

- **Update Policy** <UpdatePolicy>

  控制客户端可以从哪些前端获取软件或配置文件更新。

- **Allow Software Updates From Any Server** <AllowSoftwareUpdatesFromAnyServer>

  允许或不允许VPN核心模块和其他可选模块的来自未授权服务器（未列在服务器名称列表中）的软件更新。

- **Allow VPN Profile Updates From Any Server** <AllowVPNProfileUpdatesFromAnyServer>

  允许或不允许来自未授权服务器（未列在服务器名称列表中）的 VPN 配置文件更新。

- **Allow Management VPN Profile Updates From Any Server**<AllowManagementVPNProfileUpdatesFromAnyServer>

  允许或不允许来自未授权服务器（未列在服务器名称列表中）的管理VPN配置文件更新。

- **Allow Service Profile Updates From Any Server** <AllowServiceProfileUpdatesFromAnyServer>

  允许或不允许来自未授权服务器（未列在服务器名称列表中）的其他服务模块配置文件更新。

- **Allow ISE Posture Profile Updates From Any Server** <AllowISEProfileUpdatesFromAnyServer>

  允许或不允许来自未授权服务器（未列在服务器名称列表中）的 ISE 终端安全评估配置文件更新。

- **Allow Compliance Module Updates From Any Server** <AllowComplianceModuleUpdatesFromAnyServer>

  允许或不允许来自未授权服务器（未列在服务器名称列表中）的合规性模块更新。

- **Server Name** <ServerName>

  在此列表中指定已授权服务器。允许这些前端在建立 VPN 连接后进行所有 AnyConnect 软件和配置文件的完全更新。服务器名称可以是 FQDN、IP 地址、域名或通配符加域名。

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，请参阅本地策略参数和值。

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。

通过“启用 FIPS”工具启用本地策略参数

对于所有操作系统，都可以使用思科的“启用 FIPS”工具创建启用了 FIPS 的 AnyConnect 本地策略文件。“启用 FIPS”工具是一个命令行工具，在 Windows 上使用管理员权限运行，或在 Linux 和 macOS 上以根用户身份运行。

有关在何处下载“启用 FIPS”工具的信息，请参阅收到的 FIPS 客户端许可信息。

在计算机的命令行中输入命令 EnableFIPS <参数> 运行“启用 FIPS”工具。以下使用说明适用于“启用 FIPS”工具：

- 如果未提供任何参数，该工具将启用 FIPS 并重新启动 vpnagent 服务 (Windows) 或 vpnagent 后台守护程序（macOS 和 Linux）。

- 使用空格分隔多个参数。

以下示例显示在 Windows 计算机上运行的“启用 FIPS”工具命令：

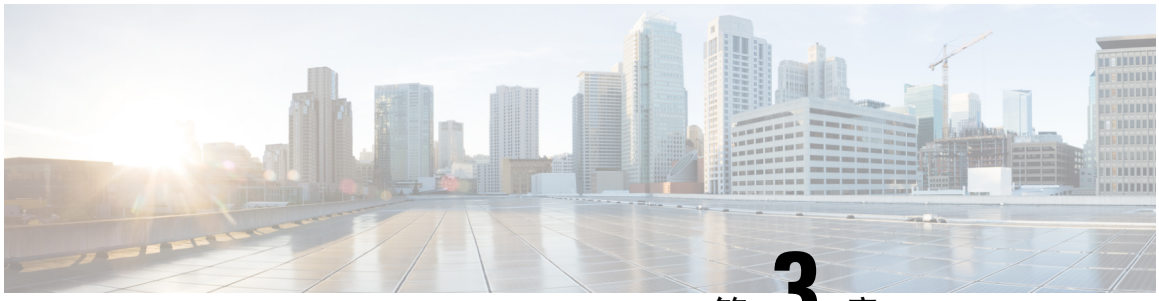
```
EnableFIPS rwl=false sct=true bd=true fm=false
```

下一个示例显示在 Linux 或 macOS 计算机上运行的命令：

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

下表显示可使用“启用 FIPS”工具配置的策略设置。参数与 AnyConnect 本地策略文件中的参数相匹配。

策略设置	参数和语法
FIPS 型号	fm=[true | false]
旁路下载程序	bd=[true | false]
限制 WebLaunch	rwl=[true | false]
严格证书信任	sct=[true | false]
限制首选项缓存	rpc=[Credentials | Thumbprints | CredentialsAndThumbprints | All | false]
排除 Firefox NSS 证书存储区 （Linux 和 macOS）	efn=[true | false]
排除 PEM 文件证书存储区（Linux 和 macOS）	epf=[true | false]
排除 Mac 本地证书存储区（仅 macOS）	emn=[true | false]



第 3 章

配置 VPN 访问

连接和断开 VPN

AnyConnect VPN 连接选项

AnyConnect 客户端为自动连接、自动重新连接或自动断开 VPN 会话提供多种选项。这些选项方便用户连接您的 VPN，它们还支持您的网络安全要求。

启动和重新启动 AnyConnect 连接

配置 VPN 连接服务器为您的用户所要手动连接的安全网关提供名称和地址。

选择以下 AnyConnect 功能，以提供方便的自动 VPN 连接：

- 登录前自动启动 Windows VPN 连接
- AnyConnect 启动时自动启动 VPN 连接
- 自动重新启动 VPN 连接

此外，还应考虑使用以下自动 VPN 策略选项实施增强的网络安全或将网络访问仅限于 VPN：

- 关于值得信赖的网络检测
- 需要使用永不间断的 VPN 连接
- 使用强制网络门户热点检测和补救

重新协商和维护 AnyConnect 连接

您可以限制 ASA 对用户保持 AnyConnect VPN 连接的时间长度（即便没有活动）。如果 VPN 会话进入空闲状态，您可以终止连接或重新协商连接。

- Keepalive - ASA 定期发送保持连接消息。这些消息会被 ASA 忽略，但对于维持客户端与 ASA 之间设备的连接很有用。

  有关通过 ASDM 或 CLI 配置保持连接的说明，请参阅思科 ASA 系列 VPN 配置指南中的启用保持连接部分。

- Dead Peer Detection - ASA 和 AnyConnect 客户端发送“R-U-There”消息。这些消息的发送频率低于 IPsec 的保持连接消息。您可以同时启用 ASA（网关）和 AnyConnect 客户端来发送 DPD 消息，并配置超时间隔。
  - 如果客户端未响应 ASA 的 DPD 消息，ASA 将再重试一次才将会话置于 Waiting to Resume 型号。此型号可使用户漫游网络，或进入睡眠型号，然后恢复连接。如果用户在空闲超时之前没有重新连接，ASA 将终止隧道。建议的网关 DPD 间隔是 300 秒。
  - 如果 ASA 不响应客户端的 DPD 消息，客户端将再尝试一次才终止隧道。建议的客户端 DPD 间隔是 30 秒。

    有关在 ASDM 中配置 DPD 的说明，请参阅相应版本的思科 ASA 系列 VPN 配置指南中的配置失效对等点检测。

- 最佳实践：
  - 将客户端 DPD 设置为 30 秒 (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection)。
  - 将服务器 DPD 设置为 300 秒 (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection)。
  - 将 SSL 和 IPsec 的密钥重新生成均设置为 1 小时 (Group Policy > Advanced > AnyConnect Client > Key Regeneration)。

终止 AnyConnect 连接

终止 AnyConnect 连接要求用户在安全网关上对其终端设备重新进行身份验证，并创建新的 VPN 连接。

以下连接参数基于超时终止 VPN 会话：

- Maximum Connect Time - 设置用户最长连接时间（以分钟为单位）。此时间结束时，系统会终止连接。您还可以允许无限连接时间（默认）。
- VPN Idle Timeout - 当会话处于非活动状态达到指定的时间时，终止任何用户会话。如果未配置 VPN 空闲超时，则使用默认空闲超时。
- Default Idle Timeout - 当会话处于非活动状态达到指定的时间时，终止任何用户会话。默认值为 30 分钟。默认值为 1800 秒。

请参阅相应版本的思科 ASA 系列 VPN 配置指南中的指定组策略的 *VPN* 会话空闲超时部分。

配置 VPN 连接服务器

AnyConnect VPN 服务器列表包含主机名和主机地址对，它们标识 VPN 用户将连接到的安全网关。主机名可以是别名、FQDN 或 IP 地址。

添加到服务器列表的主机显示在 AnyConnect GUI 的 Connect to 下拉列表中。然后，用户可以从下拉列表中进行选择以发起 VPN 连接。列表顶部的主机是默认服务器，在 GUI 下拉列表中首先出现。如果用户从列表中选择备用服务器，则所选服务器成为新的默认服务器。

一旦您将服务器添加到服务器列表，就可以查看其详细信息以及编辑或删除服务器条目。要将服务器添加到服务器列表，请遵循此过程。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Server List**。

步骤 2 单击 **Add**。

步骤 3 配置服务器的主机名和地址：

a) 输入 **Host Display Name**、用于指代主机的别名、FQDN 或 IP 地址。请勿在名称中使用“&”或“<”字符。如果您输入 FQDN 或 IP 地址，则无需在下一步骤中输入 **FQDN** 或 **IP Address**。

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。

b) （可选）输入主机的 **FQDN** 或 **IP Address**（如果在 Host Display Name 中没有输入）。

c) （可选）指定 **User Group**。

AnyConnect 使用 FQDN 或 IP 地址以及用户组来构成组 URL。

步骤 4 在 **Backup Server List** 中输入要回退到作为备用服务器的服务器。请勿在名称中使用“&”或“<”字符。

注释 相反，Server 菜单上的 Backup Server 选项卡是所有连接条目的全局条目。将使用在此处为单个服务器列表条目输入的条目覆盖放入备用服务器位置中的任何条目。此设置优先，并且是推荐做法。

步骤 5 （可选）将负载均衡服务器添加到 **Load Balancing Server List.**。请勿在名称中使用“&”或“<”字符。

如果此服务器列表条目的主机指定安全设备的负载均衡群集，且启用了永不间断功能，请将群集中的负载均衡设备添加到此列表中。否则，永不间断将阻止访问负载均衡群集中的设备。

步骤 6 为客户端指定 **Primary Protocol** 以用于此 ASA：

a) 选择 SSL（默认值）或 IPsec。

如果您指定 IPsec，则用户组必须是连接配置文件（隧道组）的准确名称。对于 SSL，用户组是连接配置文件的组 URL 或组别名。

b) 如果您指定 IPsec，请选择 **Standard Authentication Only** 以禁用默认身份验证方法（专有 AnyConnect EAP），然后从下拉列表中选择一种方法。

注释 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 配置会话超时、空闲超时、连接断开超时、分割隧道、分离 DNS、MSIE 代理配置及其他功能的能力。

步骤 7 （可选）为此服务器配置 SCEP：

a) 指定 SCEP CA 服务器的 URL。输入 FQDN 或 IP 地址。例如，http://ca01.cisco.com。

b) 选中 **Prompt For Challenge PW** 以让用户手动发出证书请求。当用户单击 **Get Certificate** 时，客户端将提示用户输入用户名和一次性密码。

c) 输入 CA 的证书拇指指纹。使用 SHA1 或 MD5 哈希值。您的 CA 服务器管理员可以提供 CA URL 和拇指指纹，且应该直接从服务器（而不是发布证书的 fingerprint 或 thumbprint 属性字段）检索拇指指纹。

步骤 8 单击 **OK**。

相关主题

AnyConnect 配置文件编辑器，服务器列表，第 25 页
AnyConnect 配置文件编辑器，添加/编辑服务器列表，第 26 页

登录前自动启动 Windows VPN 连接

关于“登录前启动”

“登录前启动”(SBL) 这一功能允许用户在登录 Windows 之前建立与企业基础设施的 VPN 连接。

在 SBL 安装并启用后，“网络连接”(Network Connection) 按钮用于启动 AnyConnect VPN 和网络接入管理器 UI。

SBL 还包括网络访问管理器图块，允许使用用户配置的家庭网络配置文件进行连接。SBL 型号中允许的网络配置文件包括使用非 802-1X 身份验证型号的所有媒体类型，例如开放 WEP、WPA/WPA2 个人和静态密钥 (WEP) 网络。

SBL 仅在 Windows 系统中可用，并使用取决于 Windows 版本的不同机制来实施：

- 在 Windows 中，登录前访问提供商 (PLAP) 用于实施 AnyConnect SBL。

  使用 PLAP 时，按 Ctrl+Alt+Del 组合键后打开一个窗口，在这个窗口中用户可以选择登录到系统或使用窗口右下角的 Network Connect 按钮激活“网络连接”（PLAP 组件）。

  PLAP 支持 Windows 的 32 位和 64 位版本。

您应该考虑为用户启用 SBL 的原因包括：

- 用户的计算机加入 Active Directory 基础设施。
- 用户拥有要求使用 Microsoft Active Directory 基础设施进行身份验证的网络映射驱动器。

- 用户无法在计算机上缓存凭证（组策略禁止缓存凭证）。在这种情况下，用户必须能够与公司网络中的域控制器通信，以便在获得计算机访问权限之前对其凭证进行验证。
- 用户必须运行从网络资源执行的登录脚本或需要访问网络资源。SBL 处于启用状态时，用户可访问本地基础设施和用户在办公室时通常会运行的登录脚本。这包括域登录脚本、组策略对象和用户登录其系统时通常发生的其他 Active Directory 功能。
- 存在可能需要连接到基础设施的网络组件（例如 MS NAP/CS NAC）。

“登录前启动”的限制

- AnyConnect 不与快速用户切换兼容。
- AnyConnect 无法由第三方登录前启动应用启动。

配置“登录前启动”

过程

步骤 1 安装 AnyConnect“登录前启动”模块。

步骤 2 在 AnyConnect 配置文件中启用 SBL。

安装 AnyConnect“登录前启动”模块

AnyConnect 安装程序会检测基础操作系统，并将来自 AnyConnect SBL 模块的适当 AnyConnect DLL 置于系统目录中。在 Windows 7 或 Windows 2008 服务器上，安装程序会确定正在使用的是 32 位还是 64 位版本的操作系统，并安装适当的 PLAP 组件，即 vpnplap.dll 或 vpnplap64.dll。

注释 如果在保留已安装的 VPNGINA 或 PLAP 组件的情况下卸载 AnyConnect，VPNGINA 或 PLAP 组件会禁用且远程用户看不见它们。

您可以预部署 SBL 模块或配置 ASA 以下载 SBL 模块。预部署 AnyConnect 时，“登录前启动”模块要求先安装核心客户端软件。如果使用 MSI 文件预部署 AnyConnect 核心和“登录前启动”组件，则必须按照正确的顺序进行操作。

过程

步骤 1 在 ASDM 中，转到 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**。

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 在左侧导航窗格中选择 **Advanced** > **AnyConnect Client**。

步骤 4 对 Optional Client Module for Download 设置取消选中 **Inherit**。

步骤 5 在下拉列表中选择 **AnyConnect SBL** 模块。

在 AnyConnect 配置文件中启用 SBL

开始之前

- 在调用 SBL 时需要存在网络连接。但在有些情况下，网络连接可能无法实现，因为无线连接可能依靠用户凭证才能连接到无线基础设施。由于 SBL 型号先于登录的凭证阶段存在，因此此情况下连接不可用。此时，无线连接需要配置为在登录过程中缓存凭证，或者需要配置其他无线身份验证，SBL 才可正常运行。
- 如果安装了网络访问管理器，您必须部署设备连接以确保适当的连接可用。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 1)**。

步骤 2 选择 **Use Start Before Logon**。

步骤 3 （可选）要允许远程用户控制 SBL，请选择 **User Controllable**。

注释 在 SBL 生效之前，用户必须重新启动远程计算机。

“登录前启动”故障排除

过程

步骤 1 确保 AnyConnect 配置文件已加载到 ASA 上，随时可部署。

步骤 2 删除之前的配置文件（在硬盘驱动器上搜索这些文件以找到位置，*.xml）。

步骤 3 使用 Windows Add/Remove Programs 卸载 SBL 组件。重新启动计算机并重新测试。

步骤 4 在事件查看器中清除用户的 AnyConnect 日志并重新测试。

步骤 5 浏览回安全设备以再次安装 AnyConnect。

步骤 6 重新启动一次。下次重新启动时，您应看到 Start Before Logon 提示。

步骤 7 收集 DART 捆绑包并将其发送给 AnyConnect 管理员。

步骤 8 如果看到以下错误，请删除用户的 AnyConnect 配置文件：

```
Description: Unable to parse the profile C:\Documents and Settings\All Users\Application
Data
\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\VABaseProfile.xml. Host data not
available.
```

步骤 9 返回 .tmpl 文件，将副本另存为 .xml 文件，并将该 XML 文件用作默认配置文件。

AnyConnect 启动时自动启动 VPN 连接

此功能称为 Auto Connect On Start，它在 AnyConnect 启动时自动与 VPN 客户端配置文件指定的安全网关建立 VPN 连接。

Auto Connect On Start 默认禁用，需要用户指定或选择安全网关。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 1)**。

步骤 2 选择 **Auto Connect On Start**。

步骤 3 （可选）要让用户控制 Auto Connect On Start，请选择 **User Controllable**。

在 Windows 系统上配置登录前启动 (PLAP)

登录前启动 (SBL) 功能在用户登录到 Windows 之前启动一个 VPN 连接。这将确保用户在登录到计算机之前连接其公司基础设施。

SBL AnyConnect 功能称为登录前接入提供商 (PLAP)，它是一个可连接的凭证提供商。此功能可让编程网络管理员在登录前执行特定的任务，如收集凭证或连接到网络资源。PLAP 在所有受支持的 Windows 操作系统上提供 SBL 功能。PLAP 分别以 vpnplap.dll 和 vpnplap64.dll 支持 32 位和 64 位版本的操作系统。PLAP 功能支持 x86 和 x64。

安装 PLAP

vpnplap.dll 和 vpnplap64.dll 组件是现有安装的一部分，因此您可以在安全设备上加载一个附加 SBL 软件包，然后，该软件包将为目标平台安装适当的组件。PLAP 是一项可选功能。安装程序软件检测底层操作系统，并将适当的 DLL 放入系统目录中。在 Windows 7 或更高版本或者 Windows 2008 服务器中，安装程序会确定 32 位或 64 位版操作系统是否在使用中，以及是否安装了适当的 PLAP 组件。

注释 如果在保留已安装的 PLAP 组件的情况下卸载 AnyConnect，PLAP 组件会禁用且远程用户看不见该组件。

安装后，在您修改用户配置文件 <profile.xml> 以激活 SBL 之前，PLAP 处于不活动状态。请参阅在 AnyConnect 配置文件中启用 SBL，第 44 页。激活后，用户通过单击 Switch User 调用网络连接组件，然后，屏幕右下部分会显示 Network Connect 图标。

注释 如果用户误将用户界面最小化，用户可以通过按下 **Alt+Tab** 组合键还原界面。

使用 PLAP 登录至 Windows PC

过程

步骤 1 用户在 Windows 启动窗口按下 **Ctrl+Alt+Del** 组合键。

系统显示登录窗口，其中包含 Switch User 按钮。

步骤 2 用户单击 **Switch User**。系统显示 Network Connect 窗口。如果用户已通过 AnyConnect 连接建立其连接并单击了 **Switch User**，该 VPN 连接将保持。如果用户单击 **Network Connect**，原来的 VPN 连接将终止。如果用户单击 **Cancel**，VPN 连接将终止。

步骤 3 用户单击窗口右下角的 **Network Connect** 按钮可启动 AnyConnect。系统打开 AnyConnect 登录窗口。

步骤 4 用户可以使用此 GUI 照常登录。
此示例假设 AnyConnect 是唯一安装的连接提供商。如果安装了多个提供商，用户必须从此窗口中显示的项目中选择一个供应商进行使用。

步骤 5 当用户连接时，用户将看到一个类似于 Network Connect 窗口的屏幕，但该屏幕的右下角有一个 Microsoft Disconnect 按钮。连接成功只能由该按钮表示。

步骤 6 用户单击与其登录相关的图标。
建立连接后，即有几分钟时间可以进行登录。在经过大约两分钟的空闲超时后，用户登录会话将会超时，并向 AnyConnect PLAP 组件发出表明断开连接的消息，使 VPN 隧道断开连接。

使用 PLAP 从 AnyConnect 断开连接

成功建立 VPN 会话后，PLAP 组件会返回原窗口，此时窗口的右下角会显示一个 Disconnect 按钮。

当用户单击 **Disconnect** 时，VPN 隧道将断开连接。

除了在响应 **Disconnect** 按钮时显式断开连接外，隧道还在以下情况下断开连接：

- 当用户使用 PLAP 登录 PC 但接着按下 **Cancel** 时。
- 当 PC 在用户登录到系统之前关机时。
- 当 Windows 上的用户登录会话超时，系统返回到“Press CTRL + ALT + DEL to log on”屏幕时。

此行为是 Windows PLAP 架构的功能，而不是 AnyConnect 的功能。

自动重新启动 VPN 连接

启用 Auto Reconnect（默认值）时，AnyConnect 将从 VPN 会话中断中恢复并重新建立会话，而不管初始连接使用哪种介质。例如，它可以重新建立有线、无线或 3G 会话。启用“自动重新链接”后，

您还可以指定系统暂停或系统恢复时的重新连接行为。系统暂停是低功耗待机状态，如 Windows 的“休眠”或者 macOS 或 Linux 的“睡眠”。系统恢复是系统暂停后的恢复。

如果禁用 Auto Reconnect，无论连接出于何种原因断开，客户端都不会尝试重新连接。思科强烈建议对此功能使用默认设置（启用）。禁用此设置可能导致连接不稳定时 VPN 连接中断。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 1)**。

步骤 2 选择 **Auto Reconnect**。

步骤 3 选择 Auto Reconnect Behavior：

- Disconnect On Suspend -（默认值）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。
- Reconnect After Resume - 客户端在系统暂停期间保留分配给 VPN 会话的资源，并且在系统恢复后尝试重新连接。

使用值得信赖的网络检测来连接和断开连接

关于值得信赖的网络检测

值得信赖的网络检测 (TND) 可让您在用户处于公司网络（值得信赖的网络）内时让 AnyConnect 自动断开 VPN 连接，并在用户处于公司网络（不值得信赖的网络）之外时启动 VPN 连接。

TND 不会影响用户手动建立 VPN 连接的能力。它不会断开用户在值得信赖的网络中手动启动的 VPN 连接。如果用户先在不值得信赖的网络中，然后进入值得信赖的网络，TND 只断开 VPN 会话的连接。举例来说，如果用户在家建立 VPN 连接，然后移动到公司办公室，则 TND 会断开 VPN 会话的连接。

您可以在 AnyConnect VPN 客户端配置文件中配置 TND。不需要更改 ASA 配置。您需要指定 AnyConnect 识别出正在值得信赖的网络和不值得信赖的网络之间过渡时应采取的措施或策略，并确定值得信赖的网络和服务器。

值得信赖的网络检测指南

- 因为 TND 功能控制 AnyConnect GUI 并自动启动连接，所以 GUI 应该始终运行。如果用户退出 GUI，则 TND 不会自动启动 VPN 连接。
- 如果 AnyConnect 也在运行“登录前启动”，且用户进入受信任网络，则计算机上显示的 SBL 窗口将自动关闭。
- 无论是否配置了永不间断，在通过 IPv4 和 IPv6 网络到 ASA 的 IPv6 和 IPv4 VPN 连接上都支持值得信赖的网络检测。

- 如果 TND 配置不同，在用户计算机上的多个配置文件可能会出现问题。

  如果用户收到过已启用 TND 的配置文件，则系统重新启动时，AnyConnect 会尝试连接它最后一次连接到的安全设备，而这可能不是您希望的行为。要连接到其他安全设备，用户必须手动断开连接并重新连接到该前端。以下解决方法将帮助您避免发生此问题：

  - 在已加载到您企业网络中所有 ASA 上的客户端配置文件中启用 TND。
  - 创建一个配置文件（在其主机条目中列出所有 ASA），并将该配置文件加载到所有 ASA 上。
  - 如果用户不需要多个不同的配置文件，请为所有ASA上的配置文件使用相同的配置文件名称。每个 ASA 都会覆盖现有配置文件。

- 要在 Linux 上使用 TND，您必须在目标 (RHEL/Ubuntu) 设备上安装并正常运行网络管理器，且网络管理器必须维护网络接口。

配置值得信赖的网络检测

过程

步骤 1 打开 VPN 配置文件编辑器，并从导航窗格中选择 **Preferences (Part 2)**。

步骤 2 选择 **Automatic VPN Policy**。

步骤 3 在 **Trusted Network Policy** 中选择一个受信任网络策略。

这是用户处于公司网络（受信任网络）中时客户端执行的操作。选项有：

- Disconnect -（默认值）客户端终止受信任网络中的 VPN 连接。
- Connect - 客户端启动受信任网络中的 VPN 连接。
- Do Nothing - 客户端不在受信任网络中执行任何操作。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 Do Nothing 会禁用 Trusted Network Detection (TND)。
- 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。

步骤 4 在 **Untrusted Network Policy** 中选择一个不受信任的网络策略。

这是用户在公司网络之外时客户端执行的操作。选项有：

- Connect - 客户端在检测到不受信任网络后启动 VPN 连接。
- Do Nothing - 客户端在检测到不受信任网络后不执行任何操作。此选项禁用 永不间断 VPN。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 **Do Nothing** 会禁用 Trusted Network Detection。

步骤 5 指定 **Trusted DNS Domains**。

指定客户端在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）。如果您将多个 DNS 后缀添加到拆分 DNS 列表并在 ASA 上指定一个默认域，则可以分配多个 DNS 后缀。

AnyConnect 客户端按以下顺序构建 DNS 后缀列表：

- 前端传输的域。
- 前端传输的拆分 DNS 后缀列表。
- 公共接口的 DNS 后缀（如果已配置）。否则，是主后缀和连接特定后缀，以及主 DNS 后缀的父后缀（如果在 Advanced TCP/IP Settings 中选中了相应的复选框）。

要匹配此 **DNS** 后缀，请执行以下操作：	将此值用于 **TrustedDNSDomains**：
example.com（仅限）	*example.com
example.com AND anyconnect.example.com	*.example.com OR example.com, anyconnect.example.com
asa.example.com AND anyconnect.example.com	*.example.com OR asa.example.com, anyconnect.example.com

步骤 6 在 **Trusted DNS Servers** 中指定受信任的 DNS 服务器。

客户端在受信任网络中时网络接口可能具有的所有DNS服务器地址（逗号分隔的字符串）。例如：203.0.113.1,2001:DB8::1。IPv4 和 IPv6 DNS 服务器地址支持通配符 (*)。

您必须具有通过 DNS 可解析的前端服务器的 DNS 条目。如果按 IP 地址连接，则需要可以解析 mus.cisco.com 的 DNS 服务器。如果通过 DNS 无法解析 mus.cisco.com，则强制网络门户检测不会按预期工作。

注释 您可以配置 TrustedDNSDomains 和/或 TrustedDNSServers。如果配置 TrustedDNSServers，请确保输入所有 DNS 服务器，这样您的站点会成为受信任网络的一部分。

如果某个活动接口匹配 VPN 配置文件中的所有规则，则将其视为在受信任网络中。

步骤 7 指定一个您要添加为可信 URL 的主机 URL。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。在单击 **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 **Set**。

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。

需要使用永不间断的 VPN 连接

关于永不间断 VPN

除非VPN会话处于活动状态，否则计算机不在受信任网络中时，永不间断操作将阻止对互联网资源的访问。在此情况下，始终将 VPN 设置为开启可保护计算机免受安全威胁。

启用了永不间断时，它在用户登录并检测到不受信任网络后自动建立 VPN 会话。VPN 会话保持打开状态，直到用户从计算机中注销，或者会话计时器或空闲会话计时器（在ASA组策略中指定）到期为止。AnyConnect连续尝试重新建立连接以重新激活会话（如果它仍然打开）；否则，它连续尝试建立新 VPN 会话。

在 VPN 配置文件中启用了永不间断时，AnyConnect 可通过删除其他所有下载的 AnyConnect 配置文件并忽略配置为连接到 ASA 的所有公共代理来保护终端。

启用永不间断时，还需要考虑以下 AnyConnect 选项：

- 允许用户将永不间断 VPN 会话断开连接：AnyConnect 使用户可以将永不间断 VPN 会话断开连接。如果启用 **Allow VPN Disconnect**，则 AnyConnect 在 VPN 会话建立后显示 Disconnect 按钮。默认情况下，启用了永不间断 VPN 时，配置文件编辑器启用 Disconnect 按钮。

  按 Disconnect 按钮将锁定所有接口以防止数据泄漏以及保护计算机免受互联网访问（除非为了建立 VPN 会话）。永不间断 VPN 会话的用户可能希望单击 Disconnect，这样，在当前 VPN 会话出现性能问题或 VPN 会话中断后的重新连接问题时，他们可以选择备用安全网关。

- 设置连接失败策略：如果永不间断 VPN 已启用且 AnyConnect 无法建立 VPN 会话，则连接失败策略确定计算机是否可以访问互联网。请参阅为永远在线设置连接失败策略。

- 处理强制网络门户热点：请参阅使用强制网络门户热点检测和补救。

永不间断 VPN 的限制

- 如果启用了永不间断，但用户没有登录，则 AnyConnect 不建立 VPN 连接。AnyConnect 仅在登录后启动 VPN 连接。

- 永不间断 VPN 不支持通过代理进行连接。

永不间断 VPN 指引

为增强威胁防范，如果您配置了永不间断 VPN，我们建议采取以下额外保护措施：

- 我们强烈建议从证书颁发机构 (CA) 购买数字证书并在安全网关上注册。ASDM 在 **Configuration > Remote Access VPN > Certificate Management > Identity Certificates** 面板上提供一个 **Enroll ASA SSL VPN with Entrust** 按钮，以方便公共证书注册。

- 如果在故障转移型号下使用永远在线 VPN，则不支持外部 SAML IdP（但是，使用内部 SAML IdP，ASA 会代理到 IdP 的所有流量并且受支持）

- 向终端预部署一个配置有永不间断的配置文件，以限制只能连接到预定义的 ASA。预部署可以防止与欺诈服务器联系。

- 限制管理员权限，以便用户无法终止进程。具有管理权限的 PC 用户可以通过停止代理而忽略永不间断策略。如果想要确保永不间断绝对安全，您必须拒绝给用户分配本地管理权限。
- 限制对 Windows 计算机上思科子文件夹的访问，通常是 `C:\ProgramData`。
- 具有有限或标准权限的用户有时可能对其程序数据文件夹具有写访问权限。他们可以利用这种访问权限删除 AnyConnect 配置文件，从而避开永不间断功能。
- 为 Windows 用户预部署一个组策略对象 (GPO)，以防止具有有限权限的用户终止 GUI。为 macOS 用户预部署等效措施。

配置永不间断 VPN

过程

步骤 1 在 AnyConnect VPN 客户端配置文件中配置永不间断，第 51 页。

步骤 2 （可选）向服务器列表添加负载均衡备用群集成员。

步骤 3 （可选）从永远在线 VPN 排除用户。

在 AnyConnect VPN 客户端配置文件中配置永不间断

开始之前

永不间断 VPN 要求在 ASA 上配置有效、受信任的服务器证书；否则它将失败并记录表示证书无效的事件。此外，确保服务器证书能通过严格的证书信任型号可防止永不间断VPN配置文件的下载锁定与欺诈服务器的 VPN 连接。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。

步骤 2 选择 **Automatic VPN Policy**。

步骤 3 配置值得信赖的网络检测，第 48 页

步骤 4 选择 **Always On**。

步骤 5 （可选）选择或取消选择 **Allow VPN Disconnect**。

步骤 6 （可选）配置连接失败策略。

步骤 7 （可选）配置强制网络门户补救。

向服务器列表添加负载均衡备用群集成员

永不间断 VPN 会影响 AnyConnect VPN 会话的负载均衡。在永不间断 VPN 禁用后，当客户端连接到负载均衡群集中的主设备时，客户端遵守从主设备到任何备用群集成员的重定向。在永不间断 启

用后，除非在客户端配置文件的服务器列表中指定备用群集成员的地址，否则客户端不遵守从主设备的重定向。因此，请确保向服务器列表中添加任何备份群集成员。

要在客户端配置文件中指定备用群集成员的地址，请按以下步骤使用 ASDM 添加负载均衡备用服务器列表：

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Server List**。

步骤 2 选择作为负载均衡群集主设备的服务器，然后单击**编辑**。

步骤 3 输入任何负载均衡群集成员的 FQDN 或 IP 地址。

从永远在线 VPN 排除用户

可以配置豁免以覆盖永不间断策略。例如，您可能要让某些个人建立与其他公司的VPN会话，或者豁免用于非公司资产的永不间断策略。

在ASA的组策略和动态访问策略中设置的豁免可覆盖永不间断策略。根据用于分配策略的匹配条件指定例外情况。如果 AnyConnect 策略启用永不间断，而动态访问策略或组策略禁用它，则只要客户端的条件与建立每个新会话时的动态访问策略或组策略相符，客户端就会对当前和将来的VPN会话保留禁用设置。

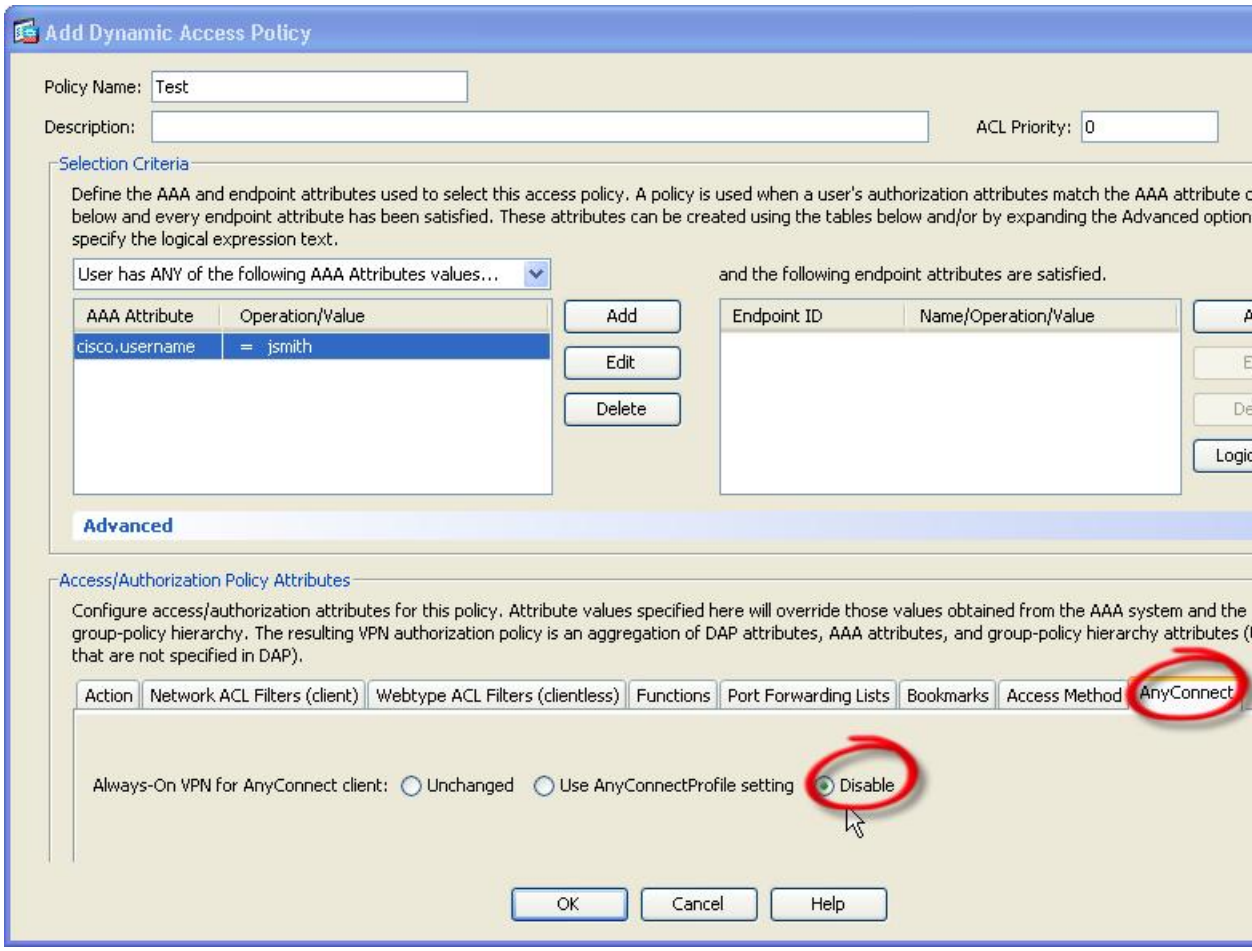
此过程配置使用 AAA 终端条件的动态访问策略以将会话匹配至非公司资产。

过程

步骤 1 选择 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add** 或 **Edit**。

步骤 2 配置条件以豁免来自永不间断 VPN 的用户。例如，使用 Selection Criteria 区域指定匹配用户登录 ID 的 AAA 属性。

步骤 3 单击 Add or Edit Dynamic Access Policy 窗口下半部分的 **AnyConnect** 选项卡。



步骤 4 单击 "永不间断 VPN for AnyConnect client" 旁边的 **Disable**。

为永远在线设置连接失败策略

关于连接失败策略

如果永不间断 VPN 已启用且 AnyConnect 无法建立 VPN 会话，连接失败策略会确定计算机是否可以访问互联网。当安全网关无法访问，或者 AnyConnect 无法检测到强制网络门户热点的存在时，就会出现这种情况。

开放策略允许完全网络访问，从而使用户可在需要访问互联网或其他本地网络资源时继续执行任务。

封闭策略在 VPN 会话建立前禁用所有网络连接。为此，AnyConnect 启用阻止来自终端（对于允许计算机连接的安全网关不受限制）的所有流量的数据包过滤器。

尽管采用了连接失败策略，AnyConnect 仍会继续尝试建立 VPN 连接。

设置连接失败策略指南

使用允许完全网络访问的开放策略时，请考虑以下内容：

- 直到建立 VPN 会话之后，安全和保护才可用。因此，终端设备可能会受到基于 Web 的恶意软件感染或者泄漏敏感数据。
- 如果启用了 Disconnect 按钮且用户单击 **Disconnect**，则打开连接失败策略不适用。

使用在建立 VPN 会话之前一直禁用所有网络连接的关闭策略时，请考虑以下内容：

- 如果用户需要 VPN 之外的互联网访问，则关闭策略会停止工作。
- 关闭策略旨在当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受网络威胁。终端始终受到保护以免遭基于 Web 的恶意软件攻击和防止敏感数据泄漏，因为除拆分隧道允许的本地资源（如打印机和外围设备）之外，所有网络访问都被阻止。
- 此选项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。
- 关闭策略会阻止强制网络门户补救，除非您专门启用它。
- 如果客户端配置文件中启用了 **Apply Last VPN Local Resources**，则您可以允许应用最新 VPN 会话实施的本地资源规则。例如，这些规则可以确定对活动同步和本地打印的访问权限。
- 若不顾关闭策略而启用了永不间断，则在 AnyConnect 软件升级期间，网络是畅通且开放的。
- 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不间断，并向用户调查 AnyConnect 不能无缝连接的频率。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。

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。实施连接故障关闭策略时要极度小心谨慎。

配置连接失败策略

仅在永不间断功能启用时才配置连接失败策略。默认情况下，连接失败策略是关闭的，以防止在无法访问 VPN 时访问互联网。要允许在此情况下访问互联网，必须将连接失败策略设置为开放。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。

步骤 2 将 **Connect Failure Policy** 参数设置为以下设置之一：

- Closed -（默认值）当无法连接到安全网关时限制网络访问。
- Open - 当客户端无法连接到安全网关时，允许通过浏览器和其他应用访问网络。

步骤 3 如果您指定了关闭策略，请执行以下操作：

a) 配置强制网络门户补救。

b) 如果要在禁用网络访问时保留最后一个 VPN 会话的本地设备规则，请选择 **Apply Last VPN Local Resources**。

使用强制网络门户热点检测和补救

关于强制网络门户

许多设施（例如，机场、咖啡店和酒店）提供 Wi-Fi 和有线访问，但可能要求用户在获得访问权之前先付款和/或同意遵守可接受的使用政策。这些设施使用称为强制网络门户的技术来防止应用连接，直到用户打开浏览器并接受访问条件为止。强制网络门户检测用于识别此限制，而强制网络门户补救是满足强制网络门户热点的要求以获取网络访问权限的过程。

在启动无需额外配置的 VPN 连接时，由 AnyConnect 自动检测强制网络门户。此外，AnyConnect 在强制网络门户检测期间不会修改任何浏览器配置设置，且不会自动补救强制网络门户。它依靠最终用户来执行补救。AnyConnect 根据当前配置对强制网络门户检测进行响应：

- 如果永不间断已禁用，或者永不间断已启用且连接失败策略处于打开状态，则在每个连接尝试时显示以下消息：

  ```
  The service provider in your current location is restricting access to the Internet.
  You need to log on with the service provider before you can establish a VPN session.
  You can try this by visiting any website with your browser.
  ```

  最终用户必须通过满足热点提供商的要求来执行强制网络门户补救。这些要求可以是付费接入网络、签署可接受使用策略、此两者或提供商规定的一些其他要求。

- 如果永不间断已启用并且连接失败策略关闭，需要明确启用强制网络门户补救。如果已启用，最终用户可以如上文所述执行补救。如果已禁用，则会在每次尝试连接时显示以下消息，且 VPN 无法连接。

  ```
  The service provider in your current location is restricting access to the Internet.
  The AnyConnect protection settings must be lowered for you to log on with the service
  provider. Your current enterprise security policy does not allow this.
  ```

配置强制网络门户补救

仅在永不间断功能启用且连接失败策略设置为关闭时，才配置强制网络门户补救。在这种情况下，可通过配置强制网络门户补救，在强制网络门户阻止 AnyConnect 连接到 VPN 时允许它连接到 VPN。

注释 强制网络门户补救的配置不适用于 Linux，因为此平台不支持无间断。因此，无论配置文件编辑器中的允许强制网络门户补救无间断如何设置，Linux 用户都可以补救强制网络门户。

如果连接失败策略设置为打开或永不间断未启用，则用户对网络的访问不会受到限制，而且用户无需在 AnyConnect VPN 客户端配置文件中进行任何特定配置，即可补救强制网络门户。

在支持无间断的平台（Windows 和 macOS）上，强制网络门户补救默认为禁用以提供最高安全性。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 1)**。

步骤 2 选择 **Allow Captive Portal Remediation.**

此设置可提升连接失败策略关闭导致的网络访问限制。

步骤 3 指定补救超时。

输入 AnyConnect 提升网络访问限制的分钟数。要满足强制网络门户要求，用户需要足够的时间。

增强的强制网络门户补救（仅限 Windows）

通过增强的强制网络门户补救功能，只要检测到强制网络门户具有受 AnyConnect 限制的网络访问（例如，由于无间断），就会在补救中使用 AnyConnect 嵌入式浏览器。在执行强制网络访问门户时，其他应用仍会受到阻止，同时 AnyConnect 浏览器处于挂起状态。用户可以关闭 AnyConnect 浏览器并故障转移到外部浏览器（如果已在配置文件中启用），这将导致 AnyConnect 复原到常规强制网络门户补救行为。执行此操作时，会显示以下消息：

```
Please retry logging on with the service provider to retain access to the Internet, by
visiting any website with your browser.
```

当检测到强制网络门户而网络访问受 AnyConnect 限制时，系统会自动启动 AnyConnect 浏览器，并显示以下消息提示用户进行补救：

```
The service provider in your current location is restricting access to the internet. You
need to log on with the service provider before you establish a VPN session, using the
AnyConnect browser.
```

配置强制网络门户补救浏览器故障转移

您可能希望将浏览器故障转移设置为每当启动用于强制网络门户补救的 AnyConnect 浏览器时应用。通过设置浏览器故障转移，用户可以在关闭 AnyConnect 浏览器后通过外部浏览器补救强制网络门户。

为强制网络门户补救启动的 AnyConnect 浏览器在服务器安全证书方面有着更严格的安全设置。在强制网络门户补救期间，不会接受不受信任的服务器证书。如果遇到不受信任的服务器证书，AnyConnect 浏览器不会加载相应的 HTTPS URL，这可能会阻止补救过程。如果不受信任的服务器证书在强制网络门户补救期间可接受，则应启用强制网络门户补救浏览器故障转移，以便允许用户对强制网络门户进行补救。启用后，用户可以关闭 AnyConnect 浏览器并继续使用外部浏览器进行补救，（因为 AnyConnect 会复原到常规强制网络门户补救行为）。

开始之前

仅在 Windows 上受支持。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 1)**。

步骤 2 如果您希望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，请选中强制网络**门户补救浏览器故障转移**。默认情况下，最终用户仅使用 AnyConnect 浏览器补救强制网络门户；也就是说，用户无法禁用增强的强制网络门户补救。

对强制网络门户检测和补救进行故障排除

AnyConnect 在以下情况下会错误地假设自己处于强制网络门户中。

- 如果 AnyConnect 尝试与包含不正确的服务器名称 (CN) 的证书的 ASA 通信，则 AnyConnect 客户端会认为它处于“强制网络门户”环境中。

  要避免此情况，请确保正确配置了 ASA 证书。证书中的 CN 值必须匹配 VPN 客户端配置文件中 ASA 服务器的名称。

- 如果在 ASA 之前，网络中有另一台设备，且该设备通过阻止对 ASA 的 HTTPS 访问来对客户端尝试联系 ASA 做出响应，则 AnyConnect 客户端会认为它处于“强制网络门户”环境中。当用户位于内部网络且通过防火墙连接 ASA 时，可能发生此情况。

  如果您需要从公司内部限制对 ASA 的访问，请配置防火墙以使至 ASA 地址的 HTTP 和 HTTPS 流量不会返回 HTTP 状态。应允许和完全阻止（也称为黑洞）对 ASA 的 HTTP/HTTPS 访问，从而确保发送至 ASA 的 HTTP/HTTPS 请求不会返回意外响应。

如果用户无法访问强制网络门户补救页面，请要求用户尝试以下操作：

- 终止任何使用 HTTP 的应用，如即时消息程序、邮件客户端、IP 电话客户端和除了一个执行补救的浏览器之外的一切应用。

  强制网络门户可能会通过忽略重复的连接尝试使它们在客户端超时，从而积极地抑制 DoS 攻击。若很多应用都尝试进行 HTTP 连接，会加剧此问题。

- 禁用并重新启用网络接口。此操作会触发强制网络门户检测重试。

- 重启计算机。

通过 L2TP 或 PPTP 配置 AnyConnect

某些国家/地区的 ISP 要求支持第 2 层隧道协议 (L2TP) 和点对点隧道协议 (PPTP)。

要通过点对点协议 (PPP) 连接将流量发送到安全网关，AnyConnect 使用外部隧道生成的点对点适配器。通过 PPP 连接建立 VPN 隧道时，客户端必须从要发送到 ASA 以外目标的隧道流量排除发送目标为 ASA 的流量。要指定是否排除路由及如何确定排除路由，请使用 AnyConnect 配置文件中的 PPP 排除设置。排除路由在 AnyConnect GUI 的 Route Details 中显示为非安全路由。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。

步骤 2 选择一种 **PPP Exclusion** 方法。此外，为此字段选中 **User Controllable**，让用户查看和更改此设置：

- Automatic - 启用 PPP 排除。AnyConnect 自动使用 PPP 服务器的 IP 地址。指示用户仅在自动检测无法获取 IP 地址时更改值。
- Override - 也会启用 PPP 排除。如果自动检测无法获取 PPP 服务器的 IP 地址，并且 PPP Exclusion UserControllable 值为 true，则指示用户按照下一节的说明使用此设置。
- Disabled - 不应用 PPP 排除。

步骤 3 在 **PPP Exclusion Server IP** 字段中，输入连接所用的 PPP 服务器的 IP 地址。为此字段选中 **User Controllable**，可让用户通过 preferences.xml 文件更改 PPP 服务器的此 IP 地址。

下一步做什么

有关更改 preferences.xml 文件的信息，请参阅“指示用户覆盖 *PPP* 排除”一节。

指示用户覆盖 PPP 排除

如果自动检测不起作用，并且您已将 PPP Exclusion 字段配置为用户可控制，则用户可以在本地计算机上通过编辑 AnyConnect 首选文件来覆盖设置。

过程

步骤 1 使用编辑器（如记事本）打开首选 XML 文件。

此文件位于用户计算机上的以下路径之一：

- Windows：%LOCAL_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml。例如，
- macOS：/Users/username/.anyconnect
- Linux：/home/username/.anyconnect

步骤 2 在 `<ControllablePreferences>` 下插入 PPPExclusion 详细信息，同时指定 Override 值和 PPP 服务器的 IP 地址。地址必须是格式正确的 IPv4 地址。例如：

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

步骤 3 保存文件。

步骤 4 退出并重新启动 AnyConnect。

使用管理 VPN 隧道

关于管理 VPN 隧道

管理 VPN 隧道可确保客户端系统在开启时连接到企业网络，这不仅限于最终用户建立了 VPN 连接的情况。您可以对办公室外的终端（尤其是用户很少通过VPN连接到办公网络的设备）执行补丁管理。需要企业网络连接的终端操作系统登录脚本也可以得益于此功能。

管理VPN隧道是为了向最终用户提供透明性；因此在默认情况下，用户应用发起的网络流量不会受到影响，而是会被定向到管理 VPN 隧道外部。

如果用户抱怨登录缓慢，可能表示管理隧道配置不当。配置管理 VPN 隧道 ， 第 61 页描述了启用该功能需要完成的配置步骤。如果症状表明，尽管遵循此配置，但仍然缺乏到公司网络的连接，请参阅管理 VPN 隧道连接问题故障排除。

管理 VPN 隧道的兼容性和要求

- 要求 ASA 9.0.1（或更高版本）和 ASDM 7.10.1（或更高版本）
- 在用户登录之前或之后，每当用户启动的 VPN 隧道断开连接时连接。

注释 当可信网络检测 (TND) 功能检测到可信网络或正在进行 AnyConnect 软件更新时，管理 VPN 隧道未建立。

- 在用户登录之前或之后，每当用户启动 VPN 隧道时，连接断开。
- 仅使用计算机存储证书验证。
- 默认情况下，需要分割包含隧道配置，以免影响用户发起的网络通信（因为管理VPN隧道对最终用户是透明的）。要覆盖此行为，请参阅配置自定义属性以支持全隧道配置 ， 第 62 页。
- 对服务器证书执行严格的证书检查。服务器证书根CA证书必须位于计算机证书存储区（Windows 上的计算机证书存储区或 macOS 上的系统密钥链或系统文件证书存储区）中。
- 使用备份服务器列表。
- 目前仅在 Windows 和 macOS 上可用。后续版本中会添加对于 Linux 的支持。

管理 VPN 隧道的不兼容性和限制

- 管理VPN配置文件不支持将代理设置的值设置为 *Native*。此限制仅适用于Windows客户端，因为管理VPN隧道可以在没有任何用户登录的情况下启动；因此，它不能依赖于用户特定的浏览器代理设置。

- 管理 VPN 配置文件不支持从 VPN 服务器推送的专用代理设置。由于管理 VPN 隧道对最终用户是透明的，因此用户特定或系统代理设置不会更改。
- 与“始终打开”功能不兼容，因为只要用户 VPN 隧道处于非活动状态，就会建立管理 VPN 隧道。但是，您可以为管理隧道连接配置组策略以隧道传输所有流量，从而确保在用户 VPN 隧道处于非活动状态时，物理接口不会泄漏任何流量。请参阅配置自定义属性以支持全隧道配置，第 62 页。
- 强制网络门户修复仅在 AnyConnect UI 正在运行且用户登录时执行，就像未启用管理 VPN 隧道功能一样。
- 管理 VPN 配置文件设置仅在管理 VPN 隧道处于活动状态时由 AnyConnect 实施。当管理 VPN 隧道断开连接时，仅实施用户 VPN 隧道配置文件设置。因此，管理 VPN 隧道根据用户 VPN 隧道配置文件中值得信赖的网络检测 (TND) 设置启动，即，当 TND 被禁用或检测到“不受信任的网络”时，无论配置的不受信任的网络策略为何。此外，管理 VPN 配置文件中的 TND 连接操作（仅在管理 VPN 隧道处于活动状态时实施）始终适用于用户 VPN 隧道，以确保管理 VPN 隧道对最终用户透明。为获得一致的用户体验，我们建议您在用户和管理 VPN 隧道配置文件中使用相同的 TND 设置。

管理 VPN 配置文件强制的必填首选项

在管理 VPN 隧道处于活动状态时，部分配置文件首选项为必填。为了帮助您配置有效的配置文件，AnyConnect 管理 VPN 配置文件编辑器通过禁用相应的 UI 控件来实施必填首选项。在管理隧道连接期间，以下首选项值会改写，主要是为了消除用户交互并最大限度地减少隧道中断：

- *AllowManualHostInput: false* - 与管理隧道无关（无头客户端）。
- *AlwaysOn: false* - 不相关，因为管理隧道断开连接时，会实施用户隧道配置文件首选项。
- *AutoConnectOnStart: false* - 仅适用于 UI 客户端，用于在启动时自动连接到先前连接的主机。
- *AutomaticCertSelection: true* - 避免证书选择弹出窗口。
- *AutoReconnect: true* - 避免网络更改时管理隧道终止。
- *AutoReconnectBehavior: ReconnectAfterResume* - 避免网络更改时管理隧道终止。
- *AutoUpdate: false* - 管理隧道连接期间不执行任何软件更新。
- *BlockUntrustedServers: true* - 避免不受信任的服务器证书提示。
- *CertificateStore: MachineStore* - 管理隧道验证在没有登录用户的情况下也应该成功。
- *CertificateStoreOverride: true* - Windows 上的计算机证书验证必需。
- *EnableAutomaticServerSelection: false* - 管理 VPN 配置文件中仅应有一个主机项。
- *EnableScripting: false* - 在管理隧道连接期间不会执行 AnyConnect 自定义脚本（在连接和/或断开连接时调用）。
- *MinimizeOnConnect:false* - 与管理隧道无关（无头客户端）。
- *RetainVPNOnLogoff:true* - 管理隧道应在用户注销时保持活动状态。

- *ShowPreConnect Message* - 与管理隧道无关（无头客户端）。
- *UserEnforcement: AnyUser* - 确保在某个用户登录时管理隧道不可能断开连接。
- *UseStartBeforeLogon:False* - 仅适用于用户隧道。
- *WindowsVPNEstablishment: AllowRemote Users* - 确保管理隧道不受任何类型的用户（本地/远程）登录影响。

此外，AnyConnect 在管理隧道连接期间不实施以下配置文件首选项：WindowsLogonEnforcement 和 SCEP 相关首选项。

配置管理 VPN 隧道

由于管理隧道连接可能在没有任何用户登录的情况下发生，因此仅支持计算机存储证书验证。因此，客户端主机的计算机证书存储区中至少需要有一个相关的客户端证书。

为管理 VPN 隧道创建配置文件

您只能将一个管理 VPN 配置文件部署到给定的客户端设备。管理 VPN 配置文件存储在专用目录（Windows 中是 %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun，macOS 中是 /opt/cisco/anyconnect/profile/mgmttun），有固定名称 (VpnMgmtTunProfile.xml)。管理 VPN 配置文件可以有零个或一个主机条目，指向按照#unique_91部分配置的隧道组。要自动禁用该功能（在隧道建立期间配置文件更新时），应在管理 VPN 配置文件中配置零个主机条目。

开始之前

完成#unique_91。

过程

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

步骤 2 单击 **Add**，Add AnyConnect Client Profiles 窗口即会打开。

步骤 3 选择 **AnyConnect Management VPN Profile** 作为要使用的配置文件。有关如何在 Add AnyConnect Client Profile 屏幕上填充字段的详细说明，请参阅《思科 ASA 系列 VPN ASDM 配置指南》中的“配置 AnyConnect 客户端配置文件”部分。

步骤 4 选择在#unique_91中创建的组策略。单击 **OK** 创建管理 VPN 配置文件，然后单击 **Edit** 以进行配置并完成后续更新。

（可选）上传已配置的管理 VPN 配置文件

您可能需要将使用独立 AnyConnect 管理 VPN 配置文件编辑器编辑或创建、从 AnyConnect 系统复制或者从其他 ASA 导出的已配置管理 VPN 配置文件上传到 ASA。

过程

步骤 1 在 ASDM 的 AnyConnect Client Profile 窗口中，依次单击 **Add** 和 **Upload...** 。
选择上传文件的目标位置时，请确保选择具有 *vpnm* 扩展名的配置文件。

步骤 2 提供配置文件名称，然后从 Profile Usage 下拉菜单中选择 **AnyConnect Management VPN Profile**。

步骤 3 选择在#unique_91中创建的组策略。单击 **OK** 以创建管理 VPN 配置文件。

将管理 VPN 配置文件关联到组策略

您必须将管理 VPN 配置文件添加到与用于管理隧道连接的隧道组关联的组策略。

注释 同样，也可以将管理VPN配置文件添加到映射至常规隧道组的组策略，用于用户隧道连接。当用户连接时，系统会下载管理 VPN 配置文件以及已映射到组策略的用户 VPN 配置文件，从而启用管理 VPN 隧道功能。

或者，您可以在带外部署管理 VPN 配置文件：确保将其命名为 VpnMgmtTunProfile.xml，将其复制到上文所述的管理 VPN 配置文件目录，然后重新启动思科 AnyConnect 安全移动代理服务（或重新引导）。

开始之前

完成#unique_91和为管理 VPN 隧道创建配置文件，第 61 页。

过程

步骤 1 在 ASDM 中导航到 **Group Policy** > **Advanced > AnyConnect Client**。

步骤 2 在要下载的客户端配置文件中，单击 **Add**，然后选择在为管理 VPN 隧道创建配置文件，第 61 页部分创建或更新的管理 VPN 配置文件。

配置自定义属性以支持全隧道配置

默认情况下，管理VPN隧道需要分割包含隧道配置，以免影响用户发起的网络通信（因为管理VPN隧道对最终用户是透明的）。您可以通过在管理隧道连接使用的组策略中配置以下自定义属性来改写此行为（在 Create Custom Attribute ASDM 窗口中：**Configuration** > **Remote Access VPN > Network (Client) Access > Group Policies > Edit > Advanced > AnyConnect Client > Custom Attributes > Add**）。

如果将属性名称和值都设置为 *true*，且配置为全隧道、分割包含、分割排除或绕过两种 IP 协议这几种配置之一，AnyConnect 会继续进行管理隧道连接。

限制管理 VPN 配置文件更新

您可以使用新的 AnyConnect 本地策略文件 (AnyConnectLocalPolicy.xml) 设置将管理 VPN 配置文件更新限制为某个受信任的服务器列表，并且仍允许来自任何服务器的用户 VPN 配置文件更新。选中 **Allow Management VPN Profile Updates From Any Server** 复选框，通过 本地策略参数和值 编辑此设置。

例如，如果仅允许从 VPN 服务器 TrustedServer 进行管理 VPN 配置文件更新，系统会取消选中该复选框，并将 TrustedServer 添加到受信任服务器列表中。（将 TrustedServer 替换为对应 VPN 配置文件服务器条目中的 FQDN 或 IP 地址。）

管理 VPN 隧道连接问题故障排除

如果客户端主机无法远程访问，则可能发生了各种情况，导致管理 VPN 隧道连接断开或未建立。在这些情况下，AnyConnect VPN GUI 和 CLI 会将管理连接状态反映为统计条目：

- Disconnected (disabled) - 功能禁用。
- Disconnected (trusted network) - TND 检测到受信任的网络，因此未建立管理隧道。
- Disconnected (user tunnel active) - 用户隧道当前处于挂起状态（管理隧道因而断开）。
- Disconnected (process launch failed) - 尝试管理隧道连接时遇到进程启动故障。
- Disconnected (connect failed) - 建立管理隧道时遇到连接故障。
- Disconnected (invalid VPN configuration) - 建立管理隧道时遇到无效的拆分隧道配置。请参阅配置自定义属性以支持全隧道配置 ， 第 62 页获得更多信息。
- Diconnected (software update pending) - AnyConnect 软件更新当前处于挂起状态（管理隧道因而断开）。
- Disconnected - 即将建立或由于其他原因无法建立管理隧道。

要排除管理 VPN 隧道上无连接的问题（预期在客户端主机上建立），请验证以下各项：

- 在 CLI 中的 AnyConnect UI Statistics 选项卡、Export Stats 输出或 Connection Information/Management Connection State 中，检查管理 VPN 连接的状态。如果管理连接状态意外地被列为“disconnected”并且提供的解释不足，请使用 DART 工具捕获 AnyConnect 日志，以便进一步排查故障。
- 如果在 UI 统计信息行中看到 *Management Connection State: Disconnected (disabled)*，请确保管理 VPN 配置文件配置了单个主机条目，指向通过证书身份验证设置的隧道组。关联的组策略必须配置有一个配置文件：管理 VPN 配置文件。

  注释 关联的组策略不应启用横幅。管理隧道连接期间不支持用户交互。

- 如果在 UI 统计信息行中看到 *Management Connection State: Disconnected (disabled)*，请确保在与用于常规用户隧道连接的隧道组关联的组策略中，配置了管理 VPN 配置文件。当用户连接到该隧道组时，系统会下载管理 VPN 配置文件，并启用该功能。

注释 或者，您也可以在带外部署管理 VPN 配置文件。

- 如果在 UI 统计信息行中看到 *Management Connection State: Disconnected (disabled)*，请注意，当需要用户交互时，管理隧道连接都会出现故障，如下所示：
  - 如果服务器证书不受信任。服务器证书的根 CA 证书必须位于计算机证书存储区中。
  - 如果与计算机存储证书相关的私人密钥受密码保护，则管理隧道连接无法使用对应的客户端证书。客户端证书无法使用，因为系统无法提示用户输入私钥密码。
  - 如果未将 macOS 系统密钥链私钥配置为允许访问而不提示 AnyConnect VPN 代理可执行文件 (vpnagentd)；管理隧道连接无法使用对应的客户端证书，因为系统无法提示用户输入访问私钥的凭证。
  - 如果组策略配置有横幅。

配置 AnyConnect 代理连接

关于 AnyConnect 代理连接

AnyConnect 通过本地、公共和私有代理来支持 VPN 会话：

- 本地代理连接：

  本地代理与 AnyConnect 在同一台计算机上运行，且有时用作透明代理。例如，一些无线数据卡提供的加速软件或一些防病毒软件（例如，Kaspersky）上的网络组件就是透明代理服务。

  本地代理的使用在 AnyConnect VPN 客户端配置文件中启用或禁用，请参阅允许本地代理连接。

- 公共代理连接：

  公共代理通常用于将网络流量匿名化。当 Windows 配置为使用公共代理时，AnyConnect 使用该连接。macOS 和 Linux 也支持使用公共代理作为本地和覆盖选项。

  配置公共代理连接，Windows中描述了如何配置公共代理。

- 私有代理连接：

  在企业网络上使用私有代理服务器来基于企业使用政策防止企业用户访问特定网站，例如色情、赌博或游戏站点。

  将组策略配置为在隧道建立后将私有代理设置下载到浏览器。在 VPN 会话结束后，设置恢复到其初始状态。请参阅配置专用代理连接，第 67 页。

注释 通过代理服务器的 AnyConnect SBL 连接取决于 Windows 操作系统版本和系统（机器）配置或其他第三方代理软件功能。因此，请参阅 Microsoft 或您使用的任何第三方代理应用提供的系统范围代理设置。

使用 VPN 客户端配置文件控制客户端代理

VPN 客户端配置文件可以阻止或重定向客户端系统的代理连接。对于 Windows 和 Linux，您可以配置（也可以允许用户配置）公共代理服务器的地址。

有关在 VPN 客户端配置文件中配置代理设置的详细信息，请参阅 AnyConnect 配置文件编辑器，首选项（第 2 部分）

生成代理自动配置文件以提供无客户端支持

某些版本的 ASA 需要 AnyConnect 配置才能支持在建立 AnyConnect 会话后通过代理服务器进行无客户端门户访问。为使此情况发生，AnyConnect 使用代理自动配置 (PAC) 文件修改客户端代理设置。仅在 ASA 没有指定私有端代理设置时，AnyConnect 才生成此文件。

AnyConnect 代理连接的要求

代理连接支持的操作系统视情况而定，如下所示：

代理连接类型	Windows	macOS	Linux
本地代理	是	是（覆盖和本地）	是
私有代理	是（在 Internet Explorer 上）	是（设定为系统代理设置）	否
公共代理	是（IE 和覆盖）	是（覆盖和本地）	是（覆盖和本地）

代理连接的限制

- IPv6 代理不支持进行任何类型的代理连接。
- 当已启用永不间断功能时，不支持通过代理进行连接。
- 要允许访问本地代理，需要一个 VPN 客户端配置文件。

允许本地代理连接

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。

步骤 2 选择（默认值）或取消选择 **Allow Local Proxy Connections**。默认情况下本地代理被禁用。

公共代理

公共代理在 Windows 和 Linux 平台上受支持。系统根据在客户端配置文件中设置的首选项选择代理服务器。在代理覆盖的情况下，AnyConnect 从配置文件抽取代理服务器。通过版本 4.1，我们在 Mac 上添加了代理支持，同时还在 Linux 和 macOS 上添加了本地代理配置。

在 Linux 上，在 AnyConnect 运行之前会导出本地代理设置。如果更改设置，则必须重新启动。

向代理服务器进行身份验证需要用户名和密码。当代理服务器配置为需要身份验证时，AnyConnect 支持基本和 NTLM 身份验证。AnyConnect 对话管理身份验证过程。成功向代理服务器进行身份验证后，AnyConnect 会提示输入 ASA 用户名和密码。

配置公共代理连接，Windows

请按照以下步骤在 Windows 上配置公共代理连接。

过程

步骤 1 从 Internet Explorer 或控制面板打开 **Internet Options**。

步骤 2 选择 **Connections** 选项卡，然后单击 **LAN Settings** 按钮。

步骤 3 配置局域网以使用代理服务器，并输入代理服务器的 IP 地址。

配置公共代理连接，macOS

过程

步骤 1 请转至系统首选项，然后选择您连接的相应接口。

步骤 2 单击 **Advanced**。

步骤 3 从新窗口中选择 **Proxies** 选项卡。

步骤 4 启用 HTTPS 代理。

步骤 5 在右面板的 Secure Proxy Server 字段中输入代理服务器地址。

配置公共代理连接，Linux

要在 Linux 中配置公共代理连接，您必须设置环境变量。

配置专用代理连接

过程

步骤 1 在 ASA 组策略中配置私有代理信息。请参阅思科 *ASA* 系列 *VPN* 配置指南中的为内部组策略配置浏览器代理部分。

注释 在 macOS 环境中，在打开终端并发出 **scutil --proxy** 之前，在浏览器中看不到从 ASA（在 VPN 连接时）向下推送的代理信息。

步骤 2 （可选）将客户端配置为忽略浏览器代理设置。

步骤 3 （可选）锁定 Internet Explorer 的 Connections 选项卡。

将客户端配置为忽略浏览器代理设置

您可以在 AnyConnect 配置文件中指定策略以绕过用户 PC 上的 Microsoft Internet Explorer 或 Safari 代理配置设置。这可防止用户在公司网络之外建立隧道，并防止 AnyConnect 通过不需要或非法的代理服务器进行连接。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。

步骤 2 在 Proxy Settings 下拉列表中，选择 **IgnoreProxy**。Ignore Proxy 会使客户端忽略所有的代理设置。不会针对从 ASA 下载的代理执行任何操作。

锁定 Internet Explorer 的 Connections 选项卡

在某些情况下，AnyConnect 会隐藏 Internet Explorer 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。在连接断开时会撤销选项卡锁定，并且被应用于该选项卡的所有管理员定义的策略所取代。此锁定发生的情况如下：

- ASA 配置指定 Connections 选项卡锁定。
- ASA 配置指定私有端代理。
- Windows 组策略之前锁定了 Connections 选项卡（覆盖未锁定 ASA 组策略设置）。

您可在组策略中将 ASA 配置为允许或不允许代理锁定。要使用 ASDM 执行此操作，请执行以下操作步骤：

过程

步骤 1 在 ASDM 中，转到 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**。

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 **Yes**，可启用代理锁定并在 AnyConnect 会话期间隐藏 Internet Explorer Connections 选项卡。或者，选择 **No** 可禁用代理锁定并在 AnyConnect 会话期间显示 Internet Explorer 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。

验证代理设置

- 对于 Windows：在注册表如下位置找到该代理设置：

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

- 对于 macOS：打开终端窗口，然后输入：

```
scutil --proxy
```

选择并排除 VPN 流量

将 IPv4 或 IPv6 流量配置为绕过 VPN

使用 Client Bypass Protocol 设置，您可以配置 AnyConnect 客户端在 ASA 只需要 IPv6 流量时如何管理 IPv4 流量，或者在 ASA 只需要 IPv4 流量时如何管理 IPv6 流量。

当 AnyConnect 客户端建立与 ASA 的 VPN 连接时，ASA 可以为客户端分配 IPv4 和/或 IPv6 地址。

如果为 IP 协议启用 Client Bypass Protocol，但未对该协议配置地址池（即，未通过 ASA 向客户端分配用于该协议的 IP 地址），则使用该协议的任何 IP 流量都不会通过 VPN 隧道发送，而会在隧道外部发送。

如果禁用 Client Bypass Protocol，且未对该协议配置地址池，则客户端将在 VPN 隧道建立后丢弃该 IP 协议的所有流量。

例如，假设 ASA 只将一个 IPv4 地址分配到 AnyConnect 连接，且终端为双协议栈。当终端尝试连接 IPv6 地址时，如果 Client Bypass Protocol 已禁用，IPv6 流量将被丢弃。如果 Client Bypass Protocol 已启用，IPv6 流量将以明文形式从客户端发送。

如果建立 IPsec 隧道（而不是 SSL 连接），则不会通知 ASA 是否在客户端上启用了 IPv6，因此 ASA 始终推送客户端旁路协议设置。

请在 ASA 的组策略中配置 Client Bypass Protocol。

过程

步骤 1 在 ASDM 中，转到 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies**。

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 选择 **Advanced** > **AnyConnect**。

步骤 4 如果该组策略不是默认组策略，请取消选中 **Client Bypass Protocol** 旁边的 **Inherit**。

步骤 5 选择以下选项之一：

- 单击 **Disable** 以丢弃 ASA 未向其分配地址的 IP 流量。
- 单击 **Enable** 以明文形式发送该 IP 流量。

步骤 6 单击 **OK**。

步骤 7 单击 **Apply**。

配置支持本地打印机和关联设备的客户端防火墙

请参阅思科 *ASA* 系列配置指南中的支持本地打印机和关联设备的客户端防火墙部分。

配置拆分隧道

分割隧道在网络（客户端）访问组策略中配置。请参阅思科 ASA 系列 VPN 配置指南中的为 *AnyConnect* 流量配置拆分隧道部分。

在 ASDM 中更改组策略后，在 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy** 中确保组策略与连接配置文件关联。

关于动态拆分隧道

动态拆分隧道旨在增强当前拆分隧道选项，这些选项通过 ASDM 组策略配置中的“Exclude Network List Below”或“Tunnel Network List Below”选项配置。除了通常用于定义拆分隧道的静态包含或排除方法外，您还可以使用动态拆分隧道包含或排除方法在 VPN 隧道中包含或排除有关特定服务的流量。您可以为每个 IP 协议配置一个不同的拆分隧道设置。例如，可以为 IPv4 启用动态拆分包含隧道（如 IPv4 拆分包含和动态拆分包含域），并且可以为 IPv6 启用动态拆分排除隧道（如 IPv6 全隧道和动态拆分排除域）。此外，AnyConnect 4.6 版本还添加了增强的动态拆分隧道，其中指定了动态拆分排除和动态拆分包含域以增强域名匹配。

动态拆分排除隧道 - 多个基于云的服务可能托管在同一 IP 池中，并且可能基于用户位置或基于云托管计算资源的负载而解析为不同的 IP 地址。若管理员只想从 VPN 隧道排除单个此类服务，使用静态排除方法定义此类策略就会有些困难（如果还需要考虑 ISP NAT、6to4、4to6 和其他网络转换型号，则更是如此）。通过动态拆分排除隧道，您可以在建立隧道后基于主机DNS域名动态调配拆分排除隧道。例如，VPN 管理员可以将 example.com 配置为在运行时从 VPN 隧道中排除。当 VPN 隧道在正常运行且某个应用尝试连接到 mail.example.com 时，VPN 客户端会自动更改系统路由表和过滤器，以允许隧道之外的连接。

增强的动态拆分排除隧道 - 为动态拆分排除隧道配置了动态拆分排除和动态拆分包含域时，从 VPN 隧道动态排除的流量必须至少与一个动态拆分排除域相匹配，但不匹配任何动态拆分包含域。例如，如果 VPN 管理员配置了动态拆分排除域 example.com 和动态拆分包含域 mail.example.com，则除 mail.example.com 以外的所有 example.com 流量都将从隧道中排除。

动态拆分包含隧道 - 通过动态拆分包含隧道，您可以在建立隧道后基于主机 DNS 域名动态调配拆分包含隧道。例如，VPN 管理员可以将 domain.com 配置为在运行时包含在 VPN 隧道中。当 VPN 隧道在正常运行且某个应用尝试连接到 www.domain.com 时，VPN 客户端会自动更改系统路由表和过滤器，以允许 VPN 隧道内的连接。

增强的动态拆分包含隧道 - 为动态拆分包含隧道配置了动态拆分包含和动态拆分排除域时，动态包含在VPN隧道中的流量必须至少与一个动态拆分包含域相匹配，但不匹配任何动态拆分排除域。例如，如果 VPN 管理员将 domain.com 配置为拆分包含域并将 www.domain.com 配置为拆分排除域，则除 www.domain.com 以外的所有 domain.com 流量都通过隧道传输。

注释 动态拆分隧道在 Linux 中不受支持。

静态拆分隧道与动态拆分隧道之间的互操作性

静态和动态排除可以共存。静态拆分隧道在建立隧道后应用，而动态拆分隧道在已连接隧道期间出现传送到域的流量时应用。

动态拆分排除隧道

动态拆分排除隧道应用到“隧道全部”、“拆分包含”和“拆分排除”隧道：

- Tunnel All Networks - VPN 隧道中的所有排除都是动态的。
- Exclude Specific Networks - 动态排除会添加到预配置的静态排除。
- Include Specific Networks - 仅当已排除主机名至少有一个 IP 地址与拆分包含网络重叠时，动态排除才相关。否则，流量已从 VPN 隧道排除，且不执行任何动态排除。

增强的动态拆分排除隧道适用于“隧道全部”和“拆分排除”隧道。如果配置了动态拆分排除和动态拆分包含域，以及拆分包含隧道，则生成的配置为增强的动态拆分包含隧道。

动态拆分包含隧道

动态拆分包含隧道仅适用于拆分包含配置。

增强的动态拆分包含隧道仅适用于拆分包含配置。

注释 启用静态或动态拆分隧道后，Umbrella 漫游安全保护处于活动状态。您可能必须在 VPN 隧道中静态包含或排除 Umbrella 云解析器，除非它们可访问且可由 VPN 隧道探测。

具有拆分隧道配置的重叠方案的结果

动态包含或排除仅涵盖尚未包含或排除的 IP 地址。应用了静态和某种形式的动态隧道，且需要强制实施新的动态包含或排除时，可能出现与已应用的包含或排除的冲突。当实施动态排除（包含与已排除的域名匹配且作为 DNS 响应一部分的所有 IP 地址）时，仅考虑排除尚未排除的地址。同样，当强制实施动态包含（包括与已包含的域名匹配且作为 DNS 响应一部分的所有 IP 地址）时，仅考虑包含尚未包含的地址。

静态公共路由（例如安全网关路由等拆分排除和关键路由）优先于动态拆分包括路由。因此，如果动态包含的至少一个 IP 地址与静态公共路由匹配，则不强制实施动态包含。

同样，静态拆分-包含路由优先于动态拆分排除路由。因此，如果动态排除的至少一个 IP 地址与静态拆分（包含路由）匹配，则不强制实施动态排除。

动态拆分隧道使用通知

在连接 VPN 隧道后，可以通过以下几种方式查看为动态拆分隧道设置的内容：

- Statistics 选项卡 - 显示动态隧道排除和动态隧道包含，其中包括从 VPN 隧道中排除或包含在其中的域名，如 ASA 组策略中所配置的那样。
- Export Stats - 生成一个文件，其中包括从 VPN 隧道中排除或包含在其中的域名，以及用于 IPv4 和 IPv6 的隧道型号。动态路由也包含在导出的统计信息中。
- Route Details 选项卡 - 显示 IPv4 和 IPv6 动态拆分排除和包含路由，其中包括与每个排除或包含的 IP 地址对应的主机名。

  注释 AnyConnect UI 针对每种 IP 协议，最多仅显示 200 条由 AnyConnect VPN 实施的安全或非安全路由。超过 200 条路由时，将会出现截断，并且您可以运行 **route print**（在 Windows 上）或 **netstat-rn** （在 Linux 或 macOS 上）查看所有路由。

- VPN configuration log message - 显示从 VPN 隧道中排除或包含在其中的域数。

拆分 DNS

在网络（客户端）访问策略中配置拆分 DNS 时，AnyConnect 将通过隧道向特定 DNS 服务器传送指定 DNS 查询（同时也在组策略内配置）。所有其他 DNS 查询将以明文形式进入客户端操作系统中的 DNS 解析程序来进行 DNS 解析。如果未配置拆分 DNS，AnyConnect 将通过隧道传送所有 DNS 查询。

拆分 DNS 的要求

拆分 DNS 支持标准和更新查询（包括 A、AAAA、NS、TXT、MX、SOA、ANY、SRV、PTR 和 CNAME）。允许与任何隧道网络匹配的 PRT 查询通过隧道。

Windows 和 macOS 平台均支持 AnyConnect 拆分 DNS。

对于 macOS，仅当满足以下条件之一时，AnyConnect 才能对特定 IP 协议使用真拆分 DNS：

- 为组策略中的一种 IP 协议（例如 IPv4）配置分割 DNS 并为另一种 IP 协议（例如 IPv6）配置客户端绕行协议（对后一种 IP 协议不配置地址池）。
- 为两个 IP 协议都配置分离 DNS。

配置拆分 DNS

要在组策略中配置拆分 DNS，请执行以下操作：

过程

步骤 1 配置至少一个 DNS 服务器。

请参阅思科 ASA 系列 VPN 配置指南中的为内部组策略配置服务器属性部分。

确保指定的专用 DNS 服务器与客户端平台配置的 DNS 服务器不重叠。如果重叠，域名解析不会正常运转，且查询可能会终止。

步骤 2 配置拆分 - 包含隧道：

在 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling** 窗格中，选择 **Tunnel Network List Below** 策略，然后指定要隧道化的地址的 **Network List**。

拆分 DNS 不支持 Exclude Network List Below 拆分隧道策略。您必须使用 Tunnel Network List Below 拆分隧道策略来配置拆分 DNS。

步骤 3 配置拆分 DNS：

在 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling** 窗格中，取消选中 **Send All DNS lookups through tunnel**，然后在 **DNS Names** 中指定其查询需要隧道化的域的名称。

下一步做什么

在 ASDM 中更改组策略后，在 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy** 中确保组策略与连接配置文件关联。

使用 AnyConnect 日志验证拆分 DNS

要验证是否启用了拆分 DNS，请搜索 AnyConnect 日志中包含“Received VPN Session Configuration Settings”的条目。该条目指示已启用拆分 DNS。IPv4 拆分 DNS 和 IPv6 拆分 DNS 有各自的日志条目。

检查哪些域使用拆分 DNS

您可以使用依赖于操作系统 DNS 解析程序的任何工具或应用来解析域名。例如，您可以使用 ping 或网络浏览器来测试拆分 DNS 解析。其他工具（如 nslookup 或 dig）会规避操作系统 DNS 解析程序。

要使用客户端检查哪些域用于拆分 DNS，请按照以下步骤操作：

过程

步骤 1 运行 **ipconfig/all** 并记录 DNS 后缀搜索列表旁边列出的域。

步骤 2 建立 VPN 连接，并再次检查 DNS 后缀搜索列表旁边列出的域。

在建立隧道后添加的这些额外域是用于拆分 DNS 的域。

注释 此过程假定从 ASA 推送的域不会与已在客户端主机上配置的域重叠。

管理 VPN 身份验证

重要安全注意事项

- 我们不建议在安全网关上使用自签证书，因为用户有可能无意中将浏览器配置为信任欺诈服务器上的证书，并且用户在连接到安全网关时必须响应安全警告，这会带来不便。
- 我们强烈建议您为 AnyConnect 客户端启用 Strict Certificate Trust，原因如下：

  要配置 **Strict Certificate Trust** ，请参阅本地策略参数和值，第 33 页中的本地策略参数和值部分。

配置服务器证书处理

服务器证书验证

- （仅限 Windows）对于 SSL 和 IPsec VPN 连接，可以选择执行证书吊销列表 (CRL) 检查。在配置文件编辑器中启用此设置后，AnyConnect将检索链中所有证书的已更新CRL。随后它将验证

有关证书是否包含在不应再受信任的这些已吊销证书中；如果发现该证书已被证书颁发机构 (CA) 吊销，则不进行连接。有关详细信息，请参阅本地策略参数和值，第 33 页。

- 当用户连接到使用服务器证书配置的ASA时，系统仍将显示表示信任并导入该证书的复选框，即便信任链（根证书、中间证书等）存在问题也是如此。如果存在其他证书问题，则不显示该复选框。
- 如果使用 FQDN 的初始验证失败，则通过 FQDN 执行的 SSL 连接不会进行第二次服务器证书验证（包括使用 FQDN 的解析 IP 地址进行名称验证）。
- 如果服务器证书包含密钥使用，则 IPsec 和 SSL 连接将要求属性必须不仅包含 DigitalSignature，还包含 KeyAgreement 或 KeyEncipherment。如果服务器证书包含 EKU，则属性必须包含 serverAuth（用于 SSL 和 IPsec）或 ikeIntermediate（仅用于 IPsec）。请注意，接受 KU 或 EKU 不需要服务器证书。
- IPsec 和 SSL 连接将对服务器证书执行名称验证。以下规则适用于 IPsec 和 SSL 名称验证：
  - 如果存在具有相关属性的主题备选名称扩展，则仅对主题备选名称执行名称验证。相关属性包括针对所有证书的 DNS 名称属性，此外，如果针对某一 IP 地址执行连接，则还包括 IP 地址属性。
  - 如果不存在主题备选名称扩展，或存在主题备选名称扩展但不包含相关属性，则对证书主题中找到的任何公用名称属性执行名称验证。
  - 如果证书出于名称验证目的而使用了通配符，则通配符只能位于第一个（最左）子域，且必须是子域中的最后一个（最右）字符。出于名称验证的目的而将忽略任何不合规的通配符条目。
- 对于 OSX，过期的证书仅在密钥链访问配置为 Show Expired Certificates 时显示。默认情况下，过期的证书将隐藏，这可能会给用户造成困扰。

无效的服务器证书处理

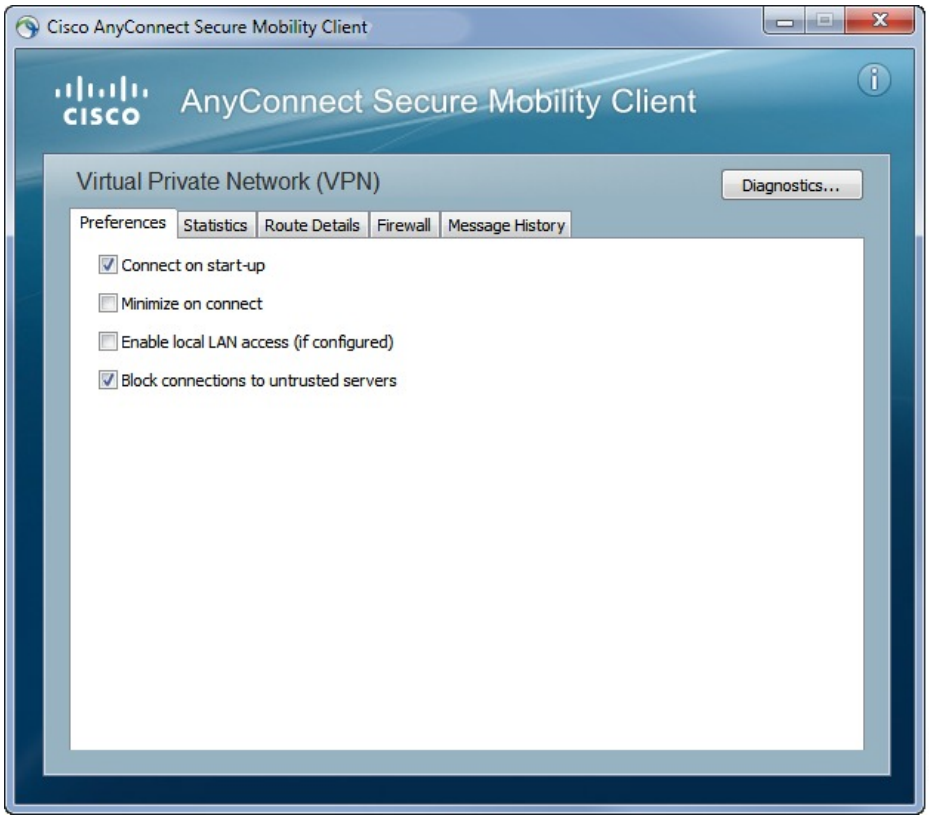
为了应对不断增加的针对不受信任网络上移动用户的定向攻击，我们改进了客户端的安全保护，以帮助阻止严重的安全漏洞。默认的客户端行为已更改，以提供一层额外防御来阻挡中间人攻击。

用户交互

当用户尝试连接到安全网关，并且存在证书错误（由于过期、日期无效、密钥使用错误或 CN 不匹配）时，用户会看到一个红色对话框，其中含有 Change Settings 和 Keep Me Safe 按钮。

注释 Linux 下的对话框可能看起来与本文档所示的对话框不同。

- 单击 **Keep Me Safe** 将取消连接。
- 单击 **Change Settings** 将打开 AnyConnect 的 Advanced > VPN >Preferences 对话框，用户可在其中启用与不受信任服务器的连接。当前连接尝试将被取消。



如果用户取消选中 **Block connections to untrusted servers**，并且唯一的证书问题是 CA 不受信任，则用户下次尝试连接到此安全网关时，将看不到 Certificate Blocked Error Dialog 对话框；他们只会看到以下对话框：

如果用户选中 **Always trust this VPN server and import the certificate** 选项，则未来与此安全网关的连接不会提示用户继续。

注释 如果用户在 **AnyConnect Advanced > VPN > Preferences** 中选中 **Block connections to untrusted servers**，或者用户的配置满足准则和限制部分下描述的型号列表中的条件之一，则 AnyConnect 将拒绝无效服务器证书。

改进的安全行为

当客户端接受无效的服务器证书时，该证书保存在客户端的证书存储库中。以前，仅保存证书的拇指指纹验证。请注意，仅当用户选择始终信任并导入无效服务器证书时，才保存无效证书。

不会出现管理权限改写而自动导致最终用户安全性降低的情况。要完全删除最终用户先前的安全决策，请在用户的本地策略文件中启用 **Strict Certificate Trust**。启用 Strict Certificate Trust 后，用户将看到一条错误消息，并且连接失败；没有用户提示。

有关在本地策略文件中启用 Strict Certificate Trust 的信息，请参阅本地策略参数和值，第 33 页中的 *AnyConnect* 本地策略参数和值部分。

指南和限制

在以下情况下将拒绝无效服务器证书：

- AnyConnect VPN 客户端配置文件启用了 Always on，并且应用的组策略或 DAP 未将其关闭。
- 客户端的本地策略启用了 Strict Certificate Trust。
- AnyConnect 配置为在登录前启动。
- 使用机器证书存储库中的客户端证书进行身份验证。

配置仅证书身份验证

您可以指定想要用户使用 AAA 通过用户名和密码进行身份验证，还是使用数字证书验证（或同时使用两种方式）。配置仅证书身份验证时，用户可以使用数字证书进行连接，不需要提供用户 ID 和密码。

为了在使用多个组的环境中支持仅通过证书身份验证，您可以配置多个组 URL。每个组 URL 包含一个不同的客户端配置文件，其中包含一些定制数据，以允许创建特定于组的证书映射。例如，可在 ASA 上调配工程部的 Department_OU 值，以便在此过程中的证书显示给 ASA 时将用户放入此组。

注释 用于向安全网关验证客户端身份的证书必须有效且受信任（由 CA 签署）。不接受自签客户端证书。

过程

步骤 1 转到 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles**。选择一个连接配置文件，然后单击 Edit。系统将打开 Edit AnyConnect Connection Profile 窗口。

步骤 2 单击窗口左侧窗格中导航树的 **Basic** 节点（如果尚未单击）。在窗口右窗格的 **Authentication** 区域中，启用 **Certificate** 方法。

步骤 3 单击 **OK** 应用更改。

配置证书注册

思科 AnyConnect 安全移动客户端使用简单证书注册协议 (SCEP) 在客户端身份验证过程中调配和续订证书。采用以下方式通过 AnyConnect IPsec 和 SSL VPN 连接到 ASA 来支持使用 SCEP 的证书注册：

- SCEP 代理：ASA 作为客户端与证书颁发机构 (CA) 之间 SCEP 请求和响应的代理。
  - CA 必须能够接入 ASA，而不是 AnyConnect 客户端，因为客户端不会直接访问 CA。
  - 注册始终会由客户端自动发起。无需用户参与。

相关主题

AnyConnect 配置文件编辑器，证书注册，第 24 页

SCEP 代理注册和操作

以下步骤说明如何获取证书，以及在为 SCEP 代理配置 AnyConnect 和 ASA 时如何建立基于证书的连接。

1. 用户使用为证书和 AAA 身份验证配置的连接配置文件连接到 ASA 前端。ASA 向客户端请求证书和 AAA 凭证进行身份验证。

2. 用户输入其 AAA 凭证，但有效证书不可用。此情形将在使用输入的 AAA 凭证建立隧道之后触发客户端发送一个自动 SCEP 注册请求。
3. ASA 将注册请求转发到 CA，并将 CA 的响应返回客户端。
4. 如果 SCEP 注册成功，则客户端向用户显示一条（可配置的）消息，并断开当前会话连接。现在，用户即可使用证书身份验证连接到 ASA 隧道组。

   如果SCEP注册失败，客户端会向用户显示一条（可配置）消息并断开当前会话连接。用户应与其管理员联系。

其他 SCEP 代理操作注意事项：

- 如果进行了相应的配置，则客户端将在证书过期之前自动续订，无需用户干预。
- SCEP 代理注册使用 SSL 进行 SSL 和 IPsec 隧道证书身份验证。

证书颁发机构要求

- 支持所有符合 SCEP 的 CA，包括 IOS CS、Windows Server 2003 CA 和 Windows Server 2008 CA。
- CA 必须处于自动授予型号。不支持证书轮询。
- 您可以将某些CA配置为将注册密码用邮件发送给用户，以增加一层安全保护。CA密码是发送到证书颁发机构来识别用户的质询密码或令牌。然后，密码被配置在AnyConnect客户端配置文件中，此配置文件成为授予证书之前 CA 验证的 SCEP 请求的一部分。

证书注册指南

- 对 ASA 的无客户端（基于浏览器的）VPN 访问不支持 SCEP 代理，但 WebLaunch（无客户端发起的 AnyConnect）支持 SCEP 代理。
- ASA 负载均衡支持通过 SCEP 注册。
- ASA 并不指出注册失败的原因，尽管它记录从客户端收到的请求。必须在 CA 或客户端上调试连接问题。
- ASA 上的仅通过证书身份验证和证书映射：

  为了在使用多个组的环境中支持仅通过证书身份验证，您可以配置多个组 URL。每个组 URL 包含一个不同的客户端配置文件，其中包含一些定制数据，以允许创建特定于组的证书映射。例如，会在 ASA 上配置 Engineering 的 Department_OU 值，以便当来自此进程的证书呈现给 ASA 时将用户放入此隧道组中。
- 识别注册连接应用策略。

  在 ASA 上，aaa.cisco.sceprequired 属性可用于捕获注册连接和在选择的 DAP 记录中应用适当的策略。
- Windows 证书警告：

Windows 客户端在首次尝试从证书颁发机构获得证书时可能收到一条警告。出现提示时，用户必须单击 Yes。这会允许他们导入根证书。它不影响他们使用客户端证书进行连接。

配置 SCEP 代理证书注册

为 SCEP 代理注册配置 VPN 客户端配置文件

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Certificate Enrollment**。

步骤 2 选择 **Certificate Enrollment**。

步骤 3 配置在注册证书中要请求的 **Certificate Contents**。有关证书字段的定义，请参阅 AnyConnect 配置文件编辑器，证书注册。

注释
- 如果您使用 %machineid%，则必须为桌面客户端加载 HostScan/Posture。
- 对于移动客户端，必须指定至少一个证书字段。

配置 ASA 以支持 SCEP 代理注册

对于 SCEP 代理，一个 ASA 连接配置文件支持证书注册和证书的授权 VPN 连接。

过程

步骤 1 创建组策略，例如，cert_group。设置以下字段：

- 在 General 中的 **SCEP Forwarding URL** 内输入 CA 的 URL。
- 在 Advanced > AnyConnect Client 窗格中，取消选中要下载的客户端配置文件的 **Inherit**，并指定为 SCEP 代理配置的客户端配置文件。例如，指定 ac_vpn_scep_proxy 客户端配置文件。

步骤 2 为证书注册和证书授权连接创建连接配置文件，例如 cert_tunnel。

- 身份验证：两者（AAA 和证书）。
- 默认组策略：cert_group。
- 在 Advanced > General 中，选中 **Enable SCEP Enrollment for this Connction Profile**。
- 在 Advanced > GroupAlias/Group URL 中，创建包含此连接配置文件的组 (cert_group) 的组 URL。

为 SCEP 设置 Windows 2008 服务器证书颁发机构

如果证书颁发机构软件在 Windows 2008 服务器上运行，您可能需要对服务器做出以下配置更改之一，以支持 SCEP 与 AnyConnect 一起使用。

在证书颁发机构上禁用 SCEP 密码

以下步骤说明如何禁用 SCEP 质询密码，以便客户端无需在 SCEP 注册之前提供带外密码。

过程

步骤 1 在认证中心服务器上，启动注册编辑器。您可以通过依次选择 **Start** > **Run**，键入 **regedit** 并单击 **OK** 来执行此操作。

步骤 2 导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword。

如果 EnforcePassword 密钥不存在，请将其创建为新密钥。

步骤 3 编辑 EnforcePassword，并将其设置为“0”。如果不存在，请将其创建为 REG-DWORD。

步骤 4 退出 regedit，然后重新引导证书颁发机构服务器。

在证书颁发机构上设置 SCEP 模板

以下步骤说明如何创建证书模板，并将其指定为默认的 SCEP 模板。

过程

步骤 1 启动 Server Manager。可通过选择 Start > Admin Tools > Server Manager 执行此操作。

步骤 2 展开 Roles > Certificate Services（或 AD Certificate Services）。

步骤 3 导航到 CA Name > Certificate Templates。

步骤 4 右键单击 **Certificate Templates > Manage**。

步骤 5 从 Cert Templates Console 中，右键单击用户模板并选择 **Duplicate**

步骤 6 为新模板选择 **Windows Server 2008 version** ，然后单击 **OK**。

步骤 7 将模板显示名更改为描述性名称，如 NDES-IPSec-SSL。

步骤 8 调整站点的有效期。大多数站点选择三年或更长有效期以避免证书过期。

步骤 9 在 Cryptography 选项卡中，为部署设置最小密钥长度。

步骤 10 在 Subject Name 选项卡中，选择 **Supply in Request**。

步骤 11 在 Extensions 选项卡中，将 Application Policies 设置为至少包括：

- 客户端身份验证
- IP 安全端系统
- IP 安全 IKE intermediate

- IP 安全隧道终止
- IP 安全用户

这些值对于 SSL 或 IPsec 有效。

步骤 12 单击 **Apply**，然后单击 **OK** 保存新模板。

步骤 13 从 Server manager > Certificate Services-CA Name，右键单击 Certificate Templates。选择 New > Certificate Template to Issue，然后选择您创建的新模板（在本示例中为 NDES-IPSec-SSL）并单击 **OK**。

步骤 14 编辑注册表。您可以通过选择 Start > Run、regedit 并单击 **OK** 执行此操作。

步骤 15 导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP。

步骤 16 将以下三个关键字的值设置为 **NDES-IPSec-SSL**。

- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

步骤 17 单击 **Save**，并重新启动证书颁发机构服务器。

配置证书到期通知

配置 AnyConnect 以提醒用户其身份验证证书即将到期。**Certificate Expiration Threshold** 设置指定 AnyConnect 在证书到期之前多少天提醒用户其证书即将到期。AnyConnect 在每次连接时都会提醒用户，直到证书实际到期或已获取新证书。

注释 证书到期阈值功能不能与 RADIUS 一起使用。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Certificate Enrollment**。

步骤 2 选择 **Certificate Enrollment**。

步骤 3 指定 **Certificate Expiration Threshold**。

这是 AnyConnect 在证书到期前提醒用户其证书即将到期的天数。

默认值为 0（不显示警告）。范围为 0 至 180 天。

步骤 4 单击 **OK**。

配置证书选择

以下步骤显示 AnyConnect 配置文件中可以配置证书搜索方式的所有位置，以及在客户端系统中选择证书的方式。这些都不是必须执行的步骤，如果您未指定任何条件，AnyConnect 将使用默认密钥匹配。

AnyConnect 读取 Windows 上的浏览器证书存储区。对于 Linux，必须创建隐私增强邮件 (PEM) 格式的文件存储。对于 macOS，可以使用隐私增强邮件 (PEM) 格式的文件存储或密钥链。

过程

步骤 1 Windows 和 macOS：配置要使用的证书存储区，第 82 页

在 VPN 客户端配置文件中指定 AnyConnect 使用的证书存储库。

步骤 2 仅限 Windows：提示 Windows 用户选择身份验证证书，第 84 页

配置 AnyConnect，为用户显示有效的证书列表，让他们选择证书以对会话进行身份验证。

步骤 3 对于 macOS 和 Linux 环境：为 macOS 和 Linux 创建 PEM 证书存储区，第 85 页

步骤 4 对于 macOS 和 Linux 环境：在 VPN 本地策略配置文件中选择要排除的证书存储库。

步骤 5 配置证书匹配，第 85 页

配置 AnyConnect 在存储库中搜索证书时尝试匹配的密钥。您可以指定密钥、扩展密钥，并添加定制扩展密钥。还可以使用可分辨名称指定 AnyConnect 匹配的运算符值型号。

配置要使用的证书存储区

对于 Windows 和 macOS，系统会为 VPN 客户端配置文件中使用的 AnyConnect 提供单独的证书存储区。您可以有一种或多种证书身份验证组合并可配置安全网关，以指令客户端对于特定的 VPN 连接，可以接受多种证书身份验证选项中的哪一种。例如，如果您在本地策略文件中将 ExcludeMacNativeCertStore 设置为 *true*（以强制 AnyConnect 仅使用文件证书存储区，例如用户和系统文件证书存储区），并将基于配置文件的证书存储区设置为 Login（以强制 AnyConnect 仅使用证书存储区，例如登录和动态智能卡密钥链，以及用户文件存储区），则 AnyConnect 中的组合过滤结果将严格使用用户文件证书存储区。

拥有计算机管理权限的用户有权访问两个证书存储库。没有管理权限的用户只能访问用户证书存储库。通常，Windows 用户不具备管理权限。选择 **Certificate Store Override** 将允许 AnyConnect 访问计算机存储库，即使在用户没有管理权限时也是如此。

注释 计算机存储库的访问控制会因 Windows 版本和安全设置而异。因此，即使用户具备管理权限，也可能无法使用计算机存储库中的证书。在此情况下，选择 **Certificate Store Override** 可允许访问计算机存储库。

下表介绍 AnyConnect 如何根据搜索的 **Certificate Store** 和 **Certificate Store Override** 是否被选中来搜索客户端中的证书。

Certificate Store 设置	Certificate Store Override 设置	AnyConnect 搜索策略
所有（对于 Windows）	已清除	AnyConnect 搜索所有的证书存储库。当用户不具备管理权限时，不允许 AnyConnect 访问计算机存储库。 该设置为默认设置。此设置适合大多数情况。请勿更改此设置，除非有特定原因或场景要求这样做。
所有（对于 Windows）	已选中	AnyConnect 搜索所有的证书存储库。当用户不具备管理权限时，允许 AnyConnect 访问计算机存储库。
所有（对于 macOS）	已选中	AnyConnect 使用所有可用 macOS 密钥链和文件存储区的证书。
用户（对于 Windows）	不适用	AnyConnect 只在用户证书存储库中进行搜索。证书存储库覆盖不适用，原因是没有管理权限的用户可以访问此证书存储库。
系统（对于 macOS）	已选中	AnyConnect 仅使用 macOS 系统密钥链和系统文件/PEM 存储区的证书。仅使用 macOS 系统密钥链和系统文件/PEM 存储区的证书。
登录（对于 macOS）	已选中	AnyConnect 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。

使用多重证书身份验证

开始之前

- 仅在桌面平台（Windows、OS X 和 Linux）上受支持。
- 您必须已在 VPN 配置文件中启用了 *AutomaticCertSelection*。
- 您在该 VPN 配置文件中设置的证书匹配配置将限制可用于多重证书身份验证的证书。

注释 不支持 SCEP。

过程

步骤 1 设置 **Certificate Store**：

- 对于一个计算机证书和一个用户证书，请在 VPN 配置文件中将 CertificateStore 设置为 **All**，并按步骤 2 中所述启用 *CertficateStoreOverride*。
- 对于两个用户证书，请在 VPN 配置文件中将 CertificateStore 设置为 **All** 或 **User**，但按步骤 2 中所述保留 *CertificateStoreOverride*。

步骤 2 如果要在用户不具备管理权限时允许 AnyConnect 搜索计算机证书存储区，请选择 **Certificate Store Override**。

使用基本证书身份验证

过程

步骤 1 设置 **Certificate Store**。

- All - 指示 AnyConnect 客户端使用所有证书存储库来定位证书。
- Machine - 指示 AnyConnect 客户端仅在 Windows 本地计算机证书存储库中查找证书。
- User - 指示 AnyConnect 客户端仅在本地用户证书存储库中查找证书。

步骤 2 如果要在用户不具备管理权限时允许 AnyConnect 搜索计算机证书存储区，请选择 **Certificate Store Override**。

提示 Windows 用户选择身份验证证书

您可以将 AnyConnect 配置为向用户显示有效证书列表并让他们选择证书以对会话进行身份验证。已到期的证书未必会视作无效。例如，如果使用的是 SCEP，则服务器可能会向客户端颁发新证书。消除已到期的证书可能会完全阻止客户端进行连接，因此需要手动干预和频带外证书分发。AnyConnect 仅限制基于与安全相关的属性（例如密钥用途、密钥类型和强度等）的客户端证书，具体取决于配置的证书匹配规则。此配置仅对 Windows 可用。默认情况下，用户证书选择被禁用。

过程

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。

步骤 2 要启用证书选择，请取消选中 **Disable Certificate Selection**。

步骤 3 取消选中 **User Controllable**，除非您要用户能够在 **Advanced** > **VPN** > **Preferences** 窗格中打开和关闭自动证书选择。

为 macOS 和 Linux 创建 PEM 证书存储区

AnyConnect 支持从隐私增强型邮件 (PEM) 格式化文件存储区中检索证书。AnyConnect 从远程计算机上的文件系统读取 PEM 格式化的证书文件，对其进行验证和签署。

开始之前

为了使客户端在任何情况下都能获得适当的证书，请确保您的文件满足以下要求：

- 所有证书文件必须以扩展名 .pem 结尾。
- 所有的私钥文件都必须以扩展名 .key 结尾。
- 客户端证书及其对应的私有密钥必须具有相同的文件名。例如：client.pem 和 client.key。

提示 可以使用指向 PEM 文件的软链接，而不是保留 PEM 文件的副本。

要创建PEM文件证书存储区，请创建如下列出的路径和文件夹。将相应的证书置于这些文件夹中：

PEM 文件证书存储区文件夹	所存储证书的类型
~/.cisco/certificates/ca **注释** .cisco/ 位于主目录中。	受信任 CA 和根证书
~/.cisco/certificates/client	客户端证书
~/.cisco/certificates/client/private	私有密钥

计算机证书与 PEM 文件证书相同（除了根目录）。对于计算机证书，用 /opt/.cisco 替代 ~/.cisco。否则，将应用列出的证书的路径、文件夹和类型。

配置证书匹配

AnyConnect 可将其证书搜索限于匹配一组特定密钥的证书。证书匹配是在 AnyConnect VPN 客户端配置文件的 **Certificate Matching** 窗格中设置的全局条件。条件包括：

- 密钥使用
- 扩展密钥使用
- 可分辨名称

相关主题

AnyConnect 配置文件编辑器，证书匹配，第 21 页

配置密钥使用

选择 **Key Usage** 密钥会将 AnyConnect 可用的证书限于至少有一个所选密钥的证书。支持的密钥列在 VPN 客户端配置文件的 **Key Usage** 列表中，其中包括：

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

如果指定一个或多个条件，证书必须匹配至少一个条件才被视为匹配的证书。

配置扩展密钥使用

选择 **Extended Key Usage** 密钥会将 AnyConnect 可用的证书限于具有这些密钥的证书。下表列出一组已知的限制条件及其对应的对象标识符 (OID)。

限制条件	OID
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	1.3.6.1.5.5.8.2.2

配置自定义扩展匹配密钥

所有其他 OID（例如本文档的一些示例中所使用的 1.3.6.1.5.5.7.3.11）被视为“自定义”。作为管理员，如果您所需的 OID 未包含在众所周知的集合中，则可以添加自己的 OID。

配置证书可分辨名称

Distinguished Name 表包含证书标识符，用于将客户端可以使用的证书限于符合指定条件的证书。单击 **Add** 按钮以在列表中添加条件，并且设置值或通配符以与添加了条件的内容匹配。

标识符	描述
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier

标识符	描述
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

Distinguished Name 可以包含零个或多个匹配条件。证书必须匹配所有指定的条件才被视为匹配的证书。**Distinguished Name** 匹配指定证书必须或不能具有指定的字符串，并且指定是否允许对字符串使用通配符。

使用 SAML 进行 VPN 身份验证

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

平台特定的要求

您必须满足以下系统要求，才能在嵌入式浏览器中使用 SAML：

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

升级过程

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

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

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

在使用 SAML 时，请遵循以下指导原则：

- 如果在故障转移型号下使用永远在线 VPN，则不支持外部 SAML IdP（但是，使用内部 SAML IdP，ASA 会代理到 IdP 的所有流量并且受支持）
- 在嵌入式浏览器中不允许不受信任的服务器证书。
- CLI 或 SBL 型号中不支持嵌入式浏览器 SAML 集成。
- （仅移动设备）不支持单一注销。
- 在 Web 浏览器中建立的 SAML 身份验证不会与 AnyConnect 共享，反之亦然。
- 根据具体配置，在使用嵌入式浏览器连接到前端时，会使用各种不同的方法。例如，尽管 AnyConnect 相比于 IPv6 连接更喜欢 IPv4 连接，但嵌入式浏览器可能更喜欢 IPv6，或反之亦然。同样，在尝试代理和收到失败后，AnyConnect 可能会回退到没有代理状态，而嵌入式浏览器在尝试代理并收到失败后可能会停止导航。
- 为了使用 SAML 功能，必须使您的 ASA 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。
- ASDM 上的 VPN 向导目前不支持 SAML 配置。
- SAML IdP *NameID* 属性确定用户的用户名，并且用于授权、记帐和 VPN 会话数据库。
- 如果您希望用户每次通过 SAML 建立 VPN 会话时，都使用身份提供程序 (IdP) 重新进行身份验证，则应该在 AnyConnect 配置文件编辑器，首选项（第 1 部分），第 12 页中将 Auto Reconnect 设置为 *ReconnectAfterResume*。
- 由于具有嵌入式浏览器的 AnyConnect 会针对每个 VPN 尝试使用新的浏览器会话，因此，如果 IdP 使用 HTTP 会话 cookie 来跟踪登录状态，则用户每次都必须重新进行身份验证。这种情况下，**Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** > 中的 *Force Re-Authentication* 设置对 AnyConnect 启动的 SAML 身份验证没有任何影响。

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

使用 SDI 令牌 (SoftID) 集成进行 VPN 身份验证

AnyConnect 支持在 Windows 7 x86（32 位）和 x64（64 位）上运行 RSA SecurID 客户端软件 1.1 版和更高版本。

RSA SecurID 软件验证器可减少用户为确保企业资产访问安全而需要管理的项目数量。远程设备上的 RSA SecurID 软件令牌将生成一个随机的一次性验证码，该验证码每 60 秒变更一次。术语 SDI 的全称是 Security Dynamics, Inc. 技术，指代这一项使用硬件和软件令牌的一次性密码生成技术。

通常情况下，用户通过单击工具托盘中的 AnyConnect 图标、选择希望连接的连接配置文件，然后在身份验证对话框中输入适当的凭证来建立 AnyConnect 连接。登录（质询）对话框将匹配为用户所属的隧道组配置的身份验证类型。登录对话框中的输入字段可明确表明身份验证需要哪类输入。

对于 SDI 身份验证，远程用户需要在 AnyConnect 软件界面中输入 PIN（个人识别码）并接收 RSA SecurID 验证码。用户在安全应用中输入验证码后，RSA 身份验证管理器将验证该验证码并准许用户获得访问权限。

使用 RSA SecurID 硬件或软件令牌的用户将看到输入字段，这些字段指示用户应输入验证码或 PIN，PIN 或验证码以及对话框底部的状态行可提供更多要求信息。用户直接向 AnyConnect 用户界面输入软件令牌 PIN 或密码。

初始登录对话框的外观取决于安全网关设置：用户可通过主登录页面、主索引 URL、隧道组登录页面或隧道组 URL（URL/隧道组）访问安全网关。要通过主登录页面访问安全网关，则必须在“Network (Client) Access AnyConnect Connection Profiles”页面上选中“Allow user to select connection”复选框。在任何一种情况中，安全网关都会向客户端发送登录页面。主登录页面具有可供用户选择隧道组的下拉列表。由于在 URL 中指定隧道组，隧道组登录页面不含下拉列表。

在主登录页面（具有连接配置文件或隧道组的下拉列表）上，默认隧道组的身份验证类型将确定密码输入字段标签的初始设置。例如，如果默认隧道组使用 SDI 身份验证，则字段标签为“Passcode”，但如果默认隧道组使用 NTLM 身份验证，字段标签为“Password”。在 2.1 版及更高版本中，字段标签不会因用户选择不同的隧道组而动态更新。对于隧道组登录页面，字段标签将与隧道组要求匹配。

客户端支持在密码输入字段中输入 RSA SecurID 软件令牌 PIN。如果安装 RSA SecurID 软件令牌软件，并且隧道组身份验证类型为 SDI，则字段标签为“Passcode”，并且状态栏会声明“Enter a username and passcode or software token PIN”。如果使用 PIN，则针对同一隧道组和用户名的后续连续登录都将包含“PIN”字段标签。客户端使用输入的 PIN 从 RSA SecurID 软件令牌 DLL 检索验证码。每次身份验证成功后，客户端均会保存隧道组、用户名以及身份验证类型，保存的隧道组将成为新的默认隧道组。

AnyConnect 接受针对任意 SDI 身份验证的验证码。即使密码输入标签为“PIN”，用户仍可按照状态栏的指示输入验证码。客户端将按照原样向安全网关发送验证码。如果使用验证码，则针对同一隧道组和用户名的后续连续登录都将包含“Passcode”字段标签。

RSASecureIDIntegration 配置文件设置有三个可能的值：

- Automatic - 客户端首先尝试一种方法，如果失败，则尝试另一种方法。默认将用户输入视为令牌验证码 (HardwareToken)，如果失败，则将其视为软件令牌 PIN (SoftwareToken)。如果身份验证成功，该成功方法将设置为新 SDI 令牌类型，并缓存在用户首选项文件中。对于下一次身份验证尝试，SDI 令牌类型将定义首先尝试的方法。通常，用于当前身份验证尝试的令牌与上次成功身份验证尝试中使用的令牌相同。然而，当用户名或组选择更改时，它将恢复为首先尝试默认方法，如输入字段标签所示。

注释 SDI 令牌类型仅在自动设置中有意义。当身份验证型号不是自动型号时，可以忽略 SKI 令牌类型的日志。HardwareToken 作为默认选项可避免触发下一个令牌型号。

- SoftwareToken - 客户端始终将用户输入视为软件令牌 PIN，输入字段标签为“PIN:”。
- HardwareToken - 客户端始终将用户输入视为令牌验证码，输入字段标签为“Passcode:”。

注释 AnyConnect 不支持将多个令牌的令牌选择导入 RSA 软件令牌客户端软件。相反，客户端使用通过 RSA SecurID 软件令牌 GUI 选择的默认选项。

SDI 身份验证交换的类别

所有 SDI 身份验证交换均属于以下类别之一：

- 普通 SDI 身份验证登录
- 新用户型号
- 新 PIN 型号
- 清除 PIN 型号
- 下一个令牌码型号

普通 SDI 身份验证登录

普通登录质询始终用作第一个质询。SDI 身份验证用户必须分别在用户名和验证码或 PIN 字段中提供用户名和令牌验证码（或者在使用软件令牌时提供 PIN）。客户端将信息返回到安全网关（中心站点设备），然后安全网关使用身份验证服务器（SDI 或通过 RADIUS 代理的 SDI）对身份验证进行验证。

如果身份验证服务器接受身份验证请求，则安全网关会将成功页面发送回客户端，身份验证交换完成。

如果验证码不被接受，则身份验证失败，安全网关会发送一个新的登录质询页面以及一条错误消息。如果达到 SDI 服务器上的验证码失败次数阈值，则 SDI 服务器会将令牌放入下一个令牌码型号中。

新用户型号、清除 PIN 型号和新 PIN 型号

PIN 只能在 SDI 服务器上由网络管理员清除。

在新用户型号、清除 PIN 型号和新 PIN 型号中，AnyConnect 缓存用户创建的 PIN 或系统分配的 PIN，供以后在“下一个验证码”登录质询中使用。

从远程用户的角度来看，清除 PIN 型号和新用户型号是相同的，而且安全网关对两者同等对待。在这两种情况下，远程用户要么必须输入新 PIN，要么由 SDI 服务器分配一个新 PIN。唯一的区别在于对初始质询的用户响应。

对于新 PIN 型号，现有 PIN 用于生成验证码，就像在任何普通质询中一样。对于清除 PIN 型号，硬件令牌根本不会使用 PIN，用户只需输入令牌码。连续八个零 (00000000) 的 PIN 用于为 RSA 软件令牌生成验证码。无论哪种情况，SDI 服务器管理员都必须通知用户使用什么 PIN 值（如果有的话）。

将新用户添加到 SDI 服务器与清除现有用户的 PIN 这两种操作会得到相同的结果。在这两种情况下，用户必须提供新 PIN 或者由 SDI 服务器分配一个新 PIN。在这些型号中，对于硬件令牌，用户只需从 RSA 设备输入一个令牌码。无论哪种情况，SDI 服务器管理员都必须通知用户使用什么 PIN 值（如果有的话）。

创建新 PIN

如果没有当前 PIN，则 SDI 服务器要求满足以下条件之一（具体取决于系统的配置）：

- 系统必须给用户分配一个新 PIN（默认值）
- 用户必须创建一个新 PIN
- 用户可以选择创建 PIN 或由系统分配 PIN

如果 SDI 服务器配置为允许远程用户选择是创建 PIN 还是由系统分配 PIN，则登录屏幕会显示一个包含这些选项的下拉列表。状态行提供提示消息。

对于系统分配的 PIN，如果 SDI 服务器接受用户在登录页面上输入的验证码，则安全网关会向客户端发送系统分配的 PIN。客户端向安全网关发送回响应，表示用户看到了新 PIN，系统继续“下一个验证码”质询。

如果用户选择创建新 PIN，则 AnyConnect 会显示一个对话框以便输入该 PIN。PIN 必须是一个 4 到 8 位的数字。由于 PIN 是一种类型的密码，用户在这些输入字段中输入的任何内容都显示为星号。

使用 RADIUS 代理时，PIN 确认是继原始对话框之后的一个单独质询。客户端将新 PIN 发送到安全网关，安全网关继续“下一个验证码”质询。

“下一个验证码”和“下一个令牌代码”质询

对于“下一个验证码”质询，客户端使用在创建或分配新 PIN 过程中缓存的 PIN 值从 RSA SecurID 软件令牌 DLL 检索下一个验证码并将其返回给安全网关，而不会提示用户。同样，对于软件令牌的“下一个令牌代码”质询，客户端从 RSA SecurID 软件令牌 DLL 检索下一个令牌代码。

比较本地 SDI 与 RADIUS SDI

网络管理员可以配置安全网关，以允许通过以下型号之一进行 SDI 身份验证：

- 本地 SDI 指安全网关中与 SDI 服务器直接通信以便处理 SDI 身份验证的本地能力。
- RADIUS SDI 指安全网关使用 RADIUS SDI 代理（与 SDI 服务器通信）执行 SDI 身份验证的过程。

对于远程用户而言，本地 SDI 和 RADIUS SDI 看起来是相同的。由于 SDI 消息在 SDI 服务器上可配置，ASA 上的消息文本必须与 SDI 服务器上的消息文本匹配。否则，向远程客户端用户显示的提示可能不适合身份验证过程中所需的操作。AnyConnect 可能无法响应，并且身份验证可能失败。

RADIUS SDI 质询基本上反映本地 SDI 交换，仅有极少例外情况。因为两者最终都与 SDI 服务器进行通信，需从客户端获取的信息和索取信息的顺序相同。

在身份验证过程中，RADIUS 服务器向 ASA 显示访问质询消息。这些质询消息中有包含来自 SDI 服务器的文本的应答消息。ASA 直接与某 SDI 服务器通信时的消息文本与通过 RADIUS 代理通信时的消息文本不同。因此，为了向 AnyConnect 显示为本地 SDI 服务器，ASA 必须解析来自 RADIUS 服务器的消息。

此外，由于 SDI 消息在 SDI 服务器上可配置，ASA 的消息文本必须与 SDI 服务器的消息文本（全部或部分）匹配。否则，向远程客户端用户显示的提示可能不适用于身份验证期间所需的操作。AnyConnect 可能无法响应，并且身份验证可能失败。

配置 ASA 以支持 RADIUS/SDI 消息

要配置 ASA 以解释特定于 SDI 的 RADIUS 回复消息并提示 AnyConnect 用户执行相应的操作，您必须配置连接配置文件（隧道组），以模拟与 SDI 服务器直接通信的方式转发 RADIUS 回复消息。用户对 SDI 服务器进行身份验证时，必须通过此连接配置文件进行连接。

过程

步骤 1 转到 **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles**。

步骤 2 选择要配置来解释特定于 SDI 的 RADIUS 回复消息的连接配置文件，然后单击 **Edit**。

步骤 3 在 **Edit AnyConnect Connection Profile** 窗口中，展开左侧导航窗格中的 Advanced 节点，然后选择 **Group Alias / Group URL**。

步骤 4 选中 **Enable the display of SecurID messages on the login screen**。

步骤 5 单击 **OK**。

步骤 6 依次选择 **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **AAA Server Groups**。

步骤 7 单击 **Add** 以添加 AAA 服务器组。

步骤 8 在 Edit AAA Server Group 对话框中配置 AAA 服务器组，然后单击 **OK**。

步骤 9 在 **AAA Server Groups** 区域，选择您刚刚创建的 AAA 服务器组，然后单击 **Servers in the Selected Group** 区域中的 **Add**。

步骤 10 在 SDI 消息区域中，展开 **Message Table** 区域。双击消息文本字段以编辑消息。在 ASA 上配置 RADIUS 回复消息文本以匹配（全部或部分）RADIUS 服务器发送的消息文本。

下表显示消息代码、默认 RADIUS 回复消息文本和每个消息的功能：

注释 ASA 使用的默认消息文本是思科安全访问控制服务器 (ACS) 使用的默认消息文本。如果您使用思科安全 ACS，且它使用默认消息文本，则您无需在 ASA 上配置消息文本。

由于安全设备按字符串在表中显示的顺序搜索字符串，因此您必须确保用于消息文本的字符串不是另一字符串的子集。例如，对于 new-pin-sup 和 next-ccode-and-reauth，“new PIN”均是默认消息文本的一部分。如果您将 new-pin-sup 配置为“new PIN”，则当安全设备从 RADIUS 服务器收到“new PIN with the next card code”时，它将此文本与 new-pin-sup 代码（而不是 next-ccode-and-reauth 代码）匹配。

消息代码	默认 **RADIUS** 应答消息文本	功能
next-code	Enter Next PASSCODE	表示用户必须输入不含 PIN 的 NEXT 令牌代码。
new-pin-sup	Please remember your new PIN	表示已提供新的系统 PIN 并向用户显示该 PIN。
new-pin-meth	Do you want to enter your own pin	来自用户的请求，表明要使用哪种新的 PIN 方法创建新的 PIN。
new-pin-req	Enter your new Alpha-Numerical PIN	表示用户生成的 PIN 并请求用户输入此 PIN。
new-pin-reenter	Reenter PIN:	在内部由 ASA 用于确认用户提供的 PIN。客户端确认 PIN 而不提示用户。
new-pin-sys-ok	New PIN Accepted	表示已接受用户提供的 PIN。
next-ccode-and-reauth	new PIN with the next card code	遵循 PIN 操作，表示用户必须等待下一个令牌代码并输入新 PIN 和下一个令牌代码才能进行身份验证。
ready-for-sys- pin	ACCEPT A SYSTEM GENERATED PIN	在内部由 ASA 用于表示用户已为系统生成的 PIN 做好准备。

步骤 11 单击 **OK**，然后单击 **Apply**，再单击 **Save**。

关于证书锁定

AnyConnect 证书锁定有助于检测服务器证书链是否确实来自连接服务器。此功能根据 VPN 配置文件设置运行，是 AnyConnect 服务器证书验证策略的附加功能。AnyConnect 本地策略文件中的严格证书信任设置不会对证书锁定检查产生任何影响。您可以在VPN配置文件中全局配置锁定，或按主机配置锁定。针对主要主机配置的锁定也将对服务器列表中的备用主机有效。用户无法更改证书锁定检查的首选项。锁定验证失败会导致 VPN 连接终止。

注释 只有在已启用首选项且 VPN 配置文件中包含与连接服务器相关的锁定设置时，AnyConnect 才会执行锁定验证。

在 VPN 配置文件编辑器 AnyConnect 配置文件编辑器，证书锁定，第 25 页中，您可以启用首选项并配置全局证书锁定和按主机的证书锁定。

在配置和维护证书锁定时，必须保持谨慎。当设置首选项时，请考虑以下建议：

- 锁定根证书和/或中间证书，因为这些证书在操作系统中得到了 CA 供应商的良好维护
- 锁定多个来自不同 CA 的根证书和/或中间证书，以便在任何 CA 受到影响时作为备用证书
- 锁定多个根证书和/或中间证书，以简化 CA 过渡
- 如果锁定某个枝叶证书，请使用相同的证书签名请求在证书续期时保留公共密钥
- 锁定服务器列表中的所有连接主机

全局和每主机锁定

您可以全局或按主机配置证书锁定。对于大多数连接主机有效的锁定会配置为全局锁定。我们建议您在VPN配置文件中的全局锁定下配置根、中间证书颁发机构和通配符叶证书。仅对连接主机有效的锁定被视为按主机锁定。我们建议在 VPN 配置文件中的按主机锁定下配置自签名叶证书。

注释 AnyConnect 会在锁定验证过程中检查对应的连接服务器的全局锁定和按主机锁定。

注释 多个 VPN 配置文件中的全局锁定不会合并。用于 VPN 连接的文件连接服务器会严格审视锁定。

注释 仅当在全局锁定部分中启用了证书锁定首选项时，才可锁定按主机证书。