配置网络访问管理器

本章提供网络访问管理器的配置概述以及添加和配置用户策略和网络配置文件的说明。

关于网络访问管理器

网络访问管理器是依据其策略提供安全第 2 层网络的客户端软件。可检测并选择最佳第 2 层接入网络并对有线和无线网络的访问执行设备身份验证。网络访问管理器对安全访问所需的用户及设备身份和网络访问协议进行管理。智能化地工作可防止最终用户进行违反管理员定义的策略的连接。

网络访问管理器采用单宿主设计，一次只允许一个网络连接。此外，有线连接具有高于无线连接的优先级，因此，如果将您插入包含有线连接的网络，则无线适配器将变为禁用状态，并且没有 IP 地址。

如果您的有线或无线网络设置或特定 SSID 从组策略推送，它们可能会与网络访问管理器的正常运行冲突。在安装了网络访问管理器的情况下，不支持无线设置的组策略。

注释 网络访问管理器在 macOS 或 Linux 上不支持。

注释 如果在 Windows OS 上使用 ISE 终端安全评估，则必须在启动 AnyConnect ISE 终端安全评估之前安装网络访问管理器。

Cisco AnyConnect Secure Mobility Client的网络访问管理器组件支持以下主要功能：

- 传输层安全 (TLS) 协议版本 1.2
- 有线 (IEEE 802.3) 和无线 (IEEE 802.11) 网络适配器。

- 一些搭配 Windows 7 或更高版本的移动宽带 (3G) 网络适配器。（需要支持 Microsoft 移动宽带 API 的 WAN 适配器。）
- 使用 Windows 机器凭证的登录前身份验证。
- 使用 Windows 登录凭证的单点登录用户身份验证。
- 简化的 IEEE 802.1X 配置。
- IEEE MACsec 有线加密和企业策略控制。
- EAP 方法：
  - EAP-FAST、PEAP、EAP-TTLS、EAP-TLS 和 LEAP（EAP-MD5、EAP-GTC 和仅用于 IEEE 802.3 有线的 EAP-MSCHAPv2）。
- 内部 EAP 方法：
  - PEAP - EAP-GTC、EAP-MSCHAPv2 和 EAP-TLS。
  - EAP-TTLS - EAP-MD5 和 EAP-MSCHAPv2 和传统方法（PAP、CHAP、MSCHAP 和 MSCHAPv2）。
  - EAP-FAST - GTC、EAP-MSCHAPv2 和 EAP-TLS。
- 加密模式 - 静态 WEP（打开或共享）、动态 WEP、TKIP 和 AES。
- 密钥建立协议 - WPA、WPA2/802.11i。
- AnyConnect 在以下环境中支持提供智能卡的凭证：
  - Windows 中的 Microsoft CAPI 1.0 和 CAPI 2.0 (CNG)。
  - Windows 登录不支持 ECDSA 证书。因此，网络访问管理器单点登录 (SSO) 不支持 ECDSA 客户端证书。

注释 WPA3 目前不支持。

套件 B 和 FIPS

以下功能已在 Windows 7 或更高版本上经过 FIPS 认证，并且列出了所有例外情况：

- ACS 和 ISE 不支持 Suite B，但具有 OpenSSL 1.x 的 FreeRADIUS 2.x 支持 Suite B。Microsoft NPS 2008 部分支持 Suite B（NPS 证书仍必须是 RSA）。
- 802.1X/EAP 只支持过渡性 Suite B 配置文件（如 RFC 5430 中定义）。
- MACsec 符合 FIPS 规范。
- 支持 Elliptic Curve Diffie-Hellman (ECDH) 密钥交换。

- 支持 ECDSA 客户端证书。
- 支持操作系统存储区中的 ECDSA CA 证书。
- 支持网络配置文件中的 ECDSA CA 证书（PEM 编码）。
- 支持服务器的 ECDSA 证书链验证。

单点登录“单一用户”实施

Microsoft Windows 允许多名用户同时登录，但思科 AnyConnect 网络访问管理器将网络身份验证仅限于对单一用户执行。无论有多少用户登录，AnyConnect 网络访问管理器都在每个桌面或每台服务器上为一位用户保持活动状态。单用户登录实施意味着只有一位用户可以随时登录到系统，并且管理员无法强制当前登录的用户注销。

如果网络访问管理器客户端模块安装在 Windows 桌面上，系统的默认行为是实施单一用户登录。如果该模块安装在服务器上，默认行为是解除单一用户登录实施。但无论是哪种情况，您都可修改或添加注册表来更改默认行为。

限制

- Windows 管理员无法强制注销当前登录的用户。
- 对于同一用户，支持与所连接工作站的 RDP 会话。
- 凭证格式相同才会被视为同一用户。例如，user/example 与 user@example.com 就不相同。
- 智能卡用户也必须确保 PIN 相同才会被视为同一用户。

配置单点登录单一用户实施

要更改 Windows 工作站或服务器处理多位用户的方式，请更改注册表中 EnforceSingleLogon 的值。

在 Windows 中，该注册表项是 **EnforceSingleLogon** 且与 OverlayIcon 项在同一注册表位置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{B12744B8-5BB7-463a-B85E-BB7627E73002}
```

要配置一位或多位用户登录，请添加名为 EnforceSingleLogon 的 DWORD，并为其赋值 1 或 0。

对于 Windows：

- 1 表示仅限一个用户登录。
- 0 允许多位用户进行登录。

网络访问管理器部署

网络访问管理器作为 AnyConnect 的一部分进行部署。有关如何安装 AnyConnect 以及网络访问管理器和其他模块的信息，请参阅 AnyConnect 部署概述。

指南

- Windows 网络状态任务托盘图标引起的困扰 - 网络访问管理器将覆盖 Windows 网络管理。因此，在安装网络访问管理器后，无法使用网络状态图标连接到网络。

  建议操作：通过在 Windows 组策略中设置**删除网络图标**来删除任务托盘中的 Windows 网络图标。此设置仅影响托盘图标。用户仍可以使用控制面板创建本地无线网络。

- Windows 7 或更高版本的隐藏网络和网络选择 - 网络访问管理器尝试只连接在网络访问管理器网络扫描列表中配置的网络。

  在 Windows 7 或更高版本中，网络访问管理器会探测隐藏的 SSID。当发现第一个隐藏的 SSID 后，即停止查找。当配置了多个隐藏网络时，网络访问管理器按如下方式选择 SSID：

  - 第一个管理员定义的隐藏企业网络。
  - 管理员定义的隐藏网络。
  - 第一个用户定义的隐藏网络。由于网络访问管理器一次只能探测一个非广播 SSID，因此思科建议在您的站点只使用一个隐藏的企业网络。

- 网络连接短暂丢失或更长的连接时间 - 如果在安装网络访问管理器之前在 Windows 中定义了网络，Windows 连接管理器可能偶尔尝试与该网络建立连接。

  建议操作：当网络在范围内时，对所有 Windows 定义的网络关闭**自动连接 (Connect Automatically)** 或删除所有 Windows 定义的网络。

- 当网络访问管理器模块首次安装到客户端系统时，该模块可以配置为将一些现有 Windows 7 或更高版本无线配置文件转换为网络访问管理器配置文件格式。可以转换匹配以下条件的基础设施网络：

  - 开放
  - 静态 WEP
  - WPA/WPA2 个人
  - 只转换非 GPO 本地 Wi-Fi 用户网络配置文件。
  - 在配置文件转换期间，系统上必须运行 WLAN 服务。
  - 如果网络访问管理器 XML 配置文件已存在 (userConfiguration.xml)，则不会进行转换。

  要启用网络配置文件转换，请创建一个 MSI 转换将 PROFILE_CONVERSION 属性值设置为 1，然后将其应用到 MSI 包。或者在命令行中将 PROFILE_CONVERSION 属性更改为 1，然后安装 MSI 包。例如，**msiexec /i anyconnect-nam-win-3.1.xxxxx-k9.msi PROFILE_CONVERSION=1**。

- 必须先安装网络访问管理器，再启动 ISE 终端安全评估。ISE 终端安全评估使用网络访问管理器插件检测网络更改事件和 802.1x WiFi。

禁用 DHCP 连接性测试

当网络配置为使用动态 IP 地址时，Windows OS 服务尝试使用 DHCP 建立连接。然而，在通知网络访问管理器 DHCP 事务已完成之前，该操作系统的过程可能需要长达两分钟。除了 OS DHCP 事务外，网络访问管理器还触发了 DHCP 事务，以避免在通过操作系统建立连接时出现较大延迟并检验网络连接。

当您想要通过 NAM 禁用 DHCP 事务来进行连接测试，请添加以下注册表项为 DWORD，然后将数值进行如下设置：

- 64 位 Windows - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP 设置为 1
- 32 位 Windows - HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP 设置为 1

注释 我们强烈建议您不要禁用网络访问管理器 DHCP 连接性测试，因为它常常导致连接时间延长。

网络访问管理器配置文件

网络访问管理器配置文件在网络访问管理器配置文件编辑器中进行配置，后者在 ASDM 中提供，也可以作为独立的 Windows 应用。

“客户端策略”(Client Policy) 窗口

客户端策略 (Client Policy) 窗口可用于配置客户端策略选项。包括以下部分：

连接设置

可用于定义是在用户登录之前还是之后尝试建立网络连接。

- **默认连接超时 (Default Connection Timeout)** - 用作用户创建的网络的连接超时秒数。默认值是 40 秒。
- **用户登录前 (Before User Logon)** - 在用户登录之前连接网络。支持的用户登录类型包括用户帐户 (Kerberos) 身份验证，加载用户 GPO 和执行基于 GPO 的登录脚本。如果选择了“用户登录前”(Before User Logon)，您还可以设置允许用户登录前等待的时间 *(Time to Wait Before Allowing a User to Logon)*。

- **允许用户登录前等待的时间 (Time to wait before allowing user to Logon)** - 指定等待网络访问管理器建立完整网络连接的最大秒数（最坏情况）。如果无法在此时间内建立网络连接，则Windows登录进程继续进行用户登录。默认值为 5 秒。

  注释 如果网络访问管理器配置为管理无线连接，则必须将**允许用户登录前等待的时间 (Time to wait before allowing user to Logon)**设置为30秒或更长时间，因为可能还要额外花时间来建立无线连接。您还应该考虑到通过 DHCP 获取 IP 地址所需的时间。如果配置了两个或更多网络配置文件，您应该增大此值以涵盖两次或更多次连接尝试。

- **用户登录后 (After User Logon)** - 在用户登录到 Windows 之后连接网络。

媒体

指定哪些类型的媒体由网络访问管理器客户端控制。

- **管理 Wi-Fi（无线）媒体 (Manage Wi-Fi [wireless] Media)** - 启用 Wi-Fi 媒体的管理和 WPA/WPA2 握手的验证（可选）。

  IEEE 802.11i 无线网络标准指定请求方（在本例中是网络访问管理器）必须验证接入点的 RSN IE（即稳健的安全网络信息交换）。IE 是在密钥派生期间放在IEEE 801.X 协议数据包的 EAPOL 密钥数据中发送的，它应该与信标/探针响应帧中接入点的 RSN IE 匹配。

- **启用 WPA/WPA2 握手的验证 (Enable validation of WPA/WPA2 handshake)** - 验证 WPA/WPA2 握手。如果未选中，则跳过此可选验证步骤。

  注释 某些适配器并不一直提供接入点的RSN IE，因此身份验证尝试失败，客户端将无法连接。

- **默认关联超时 (Default Association Timeout)**（秒）- 如果启用 WPA/WPA2 握手，则必须指定默认关联超时。
- **管理有线 (IEEE 802.3) 媒体 (Manage Wired [IEEE 802.3] Media)** - 启用有线连接的管理。
- **管理移动宽带介质 (Manage Mobile Broadband Media)** - 启用 Windows Mobile 宽带适配器的管理。此功能默认为已禁用。

  注释 此功能处于试用版本状态。思科TAC对试用版本不提供支持。

- **启用数据漫游 (Enable Data Roaming)** - 确定是否允许数据漫游。

最终用户控制

可以为用户配置以下控制：

- **禁用客户端 (Disable Client)** - 允许用户禁用和启用使用 AnyConnect UI 进行网络访问管理器的有线和无线媒体管理。
- **显示用户组 (Display user groups)** - 让用户创建的组（从 CSSC 5.x 创建）可见且能够连接，即使它们并不是管理员定义的组也是如此。
- **指定连接时运行的脚本或应用 (Specify a script or application to run when connected)** - 允许用户指定网络连接时运行的脚本或应用。

注释 脚本设置特定于一个用户配置的网络，并允许用户指定当该网络处于连接状态时运行的本地文件（.exe、.bat 或 .cmd）。为避免冲突，此脚本功能允许用户只为用户定义的网络（而不为管理员定义的网络）配置脚本或应用。此功能不允许用户就脚本运行而更改管理员网络。因此，管理员网络界面对用户不可用。此外，如果不允许用户配置正在运行的脚本，则此功能不会出现在网络访问管理器 GUI 中。

- **自动连接 (Auto-connect)** - 自动连接到一个网络，无需用户选择它。默认值为自动连接。

管理状态

- **服务操作 (Service Operation)** - 如果关闭服务，则使用此配置文件的客户端将无法连接以建立第二层连接。
- **FIPS 模式 (FIPS Mode)** - 如果启用 FIPS 模式，则网络访问管理器以符合政府要求的方式执行密码操作。

  联邦信息处理标准（FIPS 140-2 级别 1）是指定加密模块的安全要求的美国政府标准。根据软件和硬件的类型，FIPS 由面向 MACsec 或 Wi-Fi 的网络访问管理器支持。

表 *1:* 网络访问管理器的 *FIPS* 支持

媒体/操作系统	**Windows 7 或更高版本**
MACsec 有线网络	当使用支持 MACsec 的英特尔硬件 NIC 或任何非硬件 MACsec 时，都符合 FIPS。
Wi-Fi	不兼容的 FIPS

“身份验证策略”(Authentication Policy) 窗口

Authentication Policy 窗口可用于创建关联和身份验证网络过滤器，这些过滤器适用于所有网络连接。如果未选中任何关联或身份验证模式，则用户无法连接到身份验证 Wi-Fi 网络。如果选择了模式的

子集，则用户仅能连接到这些类型的网络。选择每个所需的关联或身份验证模式，或者选择**全选 (Select All)**。

内部方法也可以仅限于特定的身份验证协议。内部方法缩进显示在 Allowed Authentication Modes 窗格中外部方法（隧道）的下面。

选择身份验证协议的机制与当前客户端身份验证数据库集成在一起。安全无线局域网部署不要求为用户创建新的身份验证系统。

对内部隧道可用的 EAP 方法取决于内部方法凭证类型和外部隧道方法。在以下列表中，每个外部隧道方法都列出了针对每种凭证类型受支持的内部方法类型。

- PEAP
  - 密码凭证：EAP-MSCHAPv2 或 EAP-GTC
  - 令牌凭证：EAP-GTC
  - 证书凭证：EAP-TLS
- EAP-FAST
  - 密码凭证：EAP-MSCHAPv2 或 EAP-GTC
  - 令牌凭证：EAP-GTC
  - 证书凭证：EAP-TLS
- EAP-TTLS
  - 密码凭证：EAP-MSCHAPv2、EAP-MD5、PAP（传统）、CHAP（传统）、MSCHAP（传统）、MSCHAP-v2（传统）
  - 令牌凭证：PAP（传统）。网络访问管理器支持的默认令牌选项是 PAP，因为质询/响应方法并不是很适合基于令牌的身份验证。
  - 证书凭证：不适用

“网络”(Networks) 窗口

Networks 窗口可用于为企业用户配置预定义的网络。您可以配置对所有组可用的网络，或创建具有特定网络的组。“网络”(Networks) 窗口显示向导，可将窗格添加到现有窗口中，并且可让您通过单击**下一步 (Next)** 访问更多配置选项。

从根本上说，组是一套配置的连接（网络）。每个已配置的连接必须属于某个组，或者是所有组的成员。

注释 为向后兼容，使用思科安全服务客户端部署的由管理员创建的网络被视为隐藏的网络，不广播SSID。但是，用户网络被视为广播 SSID 的网络。

只有管理员可以创建新组。如果配置中未定义组，配置文件编辑器会创建一个自动生成的组。自动生成的组中包含未分配到任何管理员定义的组的网络。客户端尝试使用在活动组中定义的连接创建网络连接。根据“网络组”(Network Groups) 窗口中**创建网络 (Create Networks)** 选项的设置，最终用户可以将用户网络添加到活动组，或者从活动组删除用户网络。

定义的网络可用于列表顶部的所有组。因为您控制哪些网络位于全球网络中，所以您可以指定最终用户能够连接的网络，即使存在用户定义的网络也一样。最终用户无法修改或删除管理员配置的网络。

注释 最终用户可以将网络添加到组，但全球网络部分的网络除外，因为这些网络存在于所有组中，只能使用配置文件编辑器创建。

企业网络的典型最终用户不需要了解组即可使用此客户端。活动组是配置中的第一个组，但如果只有一个组可用，客户端不会知道活动组，也不会显示活动组。但是，如果存在多个组，用户界面会显示组的列表，并且指示活动组已选中。然后，用户可以从活动组中选择，重启后该设置也保持不变。根据“网络组”(Network Groups) 窗口中**创建网络 (Create Networks)** 选项的设置，最终用户无需使用组即可添加或删除自己的网络。

注释 组选择在重启和网络修复（右键单击托盘图标并选择**网络修复 (Network Repair)** 来完成）后保持不变。网络访问管理器在修复或重新启动时，会开始使用以前的活动组。

“网络”(Networks) 窗口的“媒体类型”(Media Type) 页面

您可以在 Networks 窗口的 Media Type 页面中创建或编辑有线或无线网络。设置随您的具体选择而不同。

第一个对话框中包括以下部分：

- Name - 输入将为该网络显示的名称。
- 组成员 (Group Membership) - 选择此配置文件应该对哪些网络组或组可用。
- 网络媒体 (Network Media) - 选择有线或 Wi-Fi（无线）。如果选择 Wi-Fi，您还可以配置以下参数：
  - SSID - 输入您的无线网络的 SSID（服务集标识符）。
  - Hidden Network - 允许连接到网络，即使它不广播其 SSID。
  - Corporate Network - 如果附近有企业网络，强制将网络连接首先配置为 Corporate。当企业网络使用非广播（隐藏）SSID 并且配置为隐藏时，网络访问管理器会主动寻找隐藏的 SSID，并且当有企业 SSID 在范围内时建立连接。
  - Association Timeout - 输入网络访问管理器在重新评估可用网络之前等待与特定无线网络相关联的时长。默认的关联超时为 5 秒。

- 常用设置
  - 脚本或应用程序 (Script or application) - 输入将在本地系统中运行的文件的路径和文件名，或者浏览文件夹并选择一个文件。以下规则适用于脚本和应用：
    - 您无法在登录前启动模式下运行脚本。
    - 接受扩展名为 .exe、.bat 或 .cmd 的文件。
    - 用户不得更改管理员创建的网络中定义的脚本或应用。
    - 您可以使用配置文件编辑器仅指定路径和脚本或应用的文件名。如果脚本或应用不存在于用户的机器上，将会显示一条错误消息。用户获通知，脚本或应用不存在于其机器上，并且需要联系系统管理员。
    - 您必须指定要运行的应用的完整路径，除非应用存在于用户的路径中。如果应用存在于用户的路径中，您可以仅指定应用或脚本的名称。
    - Connection Timeout - 输入网络访问管理器尝试连接到其他网络（当连接模式为自动时）或者使用另一个适配器之前等待建立网络连接的秒数。

注释 某些智能卡身份验证系统需要近 60 秒才能完成身份验证。使用智能卡时，您应增加 Connection Timeout 值，尤其是当智能卡可能必须尝试几个网络才能连接成功时。

注释 为了缓解在特定智能卡中间件上发现的问题，AnyConnect 网络访问管理器通过对测试数据执行签名操作并验证该签名来验证智能卡 PIN。此测试签名针对位于智能卡上的每个证书进行，并且与证书的数量有关，因此可能显著增加智能卡身份验证的延迟。如果要禁用测试签名操作，可以在 HKEY_LOCAL_MACHINE/SOFTWARE/Cisco/Cisco AnyConnect Network Access Manager 中将 **DisableSmartcardPinVerifyBySigning** 作为一个 DWORD 添加到注册表项中并将其设置为 1。对启用此注册表项的任何更改都应使用所有智能卡和相关硬件进行全面测试，以确保操作正确。

“网络”(Networks) 窗口的“安全等级”(Security Level) 页面

在“网络”(Networks) 向导的“安全等级”(Security Level) 页面中，选择“开放式网络”(Open Network)、“身份验证网络”(Authentication Network) 或（仅为无线网络介质显示的）“共享密钥网络”(Shared Key Network)。每种网络类型的配置流程都不同，在以下各节进行说明。

- 配置身份验证网络 - 建议用于安全企业。
- 配置开放网络 - 不推荐，但是可用于通过强制网络门户环境提供访客接入。在强制网络门户状态下，网络访问管理器不支持自动启动浏览器。
- 配置共享密钥网络 - 建议用于小型办公室或家庭办公室等无线网络。

配置身份验证网络

如果您在“安全级别”(Security Level) 部分选择“身份验证网络”(Authenticating Network)，将显示额外的窗格，如下所述。在这些窗格中完成配置后，请单击**下一步 (Next)** 按钮，或选择**连接类型 (Connection Type)**选项卡打开“网络连接类型”(Network Connection Type) 对话框。

802.1X Settings 窗格

根据网络配置调整 IEEE 802.1X 设置：

注释 当 AnyConnect ISE 终端安全评估安装了网络访问管理器时，ISE 终端安全评估使用网络访问管理器插件检测到网络更改事件和 802.1X WiFi。

- authPeriod（秒）- 身份验证开始时，此设置将确定在身份验证消息超时之前请求方等待的时长，该时间过后需要验证方重新发起身份验证。
- heldPeriod（秒）- 身份验证失败时，此设置定义请求方等待多长时间后才能发出另一次身份验证尝试。
- startPeriod（秒）- 没有从验证方收到对 EAPOL-Start 消息的任何响应时，再次传输 EAPOL-Start 消息之间的时间间隔（秒）。
- maxStart - 请求方通过发送 IEEE 801.X 协议数据包、EAPOL 密钥数据或 EAPoL-Start，向验证方发起身份验证的次数，达到此次数后，请求方会假定没有验证方。此时，请求方允许数据流量。

提示 您可以仔细设置 startPeriod 和 maxStart，使发起身份验证所花的总时间小于网络连接计时器时间（startPeriod x maxStart < 网络连接计时器时间），配置单一身份验证有线连接以同时支持开放网络和身份验证网络。

请注意，在这种情况下，您应将网络连接计时器时间增加 (startPeriod x maxStart) 秒，让客户端有足够的时间获取 DHCP 地址和完成网络连接。

相反，若要仅在身份验证成功后才允许数据流量，您应该设置 startPeriod 和 maxStart，确保发起身份验证所花的总时间大于网络连接计时器时间（startPeriod x maxStart > 网络连接计时器时间）。

Security 窗格

仅为有线网络显示。

在“安全”(Security) 窗格中，选择以下参数的值：

- Key Management - 确定哪个密钥管理协议用于启用 MACsec 的有线网络。
  - None - 没有使用密钥管理协议，并且不执行有线加密。
  - MKA - 请求方尝试协商 MACsec 密钥管理协议策略和加密密钥。MACsec 是 MAC 层安全，在有线网络上提供 MAC 层加密。MACsec 协议采用加密手段来保护 MAC 层帧，依靠 MACsec 密钥协议 (MKA) 实体进行协商并分发加密密钥。
- 加密
  - None - 对数据流量执行完整性检查，但不加密。
  - MACsec: AES-GCM-128 - 仅当选择 MKA 进行密钥管理时，此选项才可用。它会使用 AES-GCM-128 对数据流量进行加密。
  - MACsec: AES-GCM-256 - 具有企业边缘 (eEdge) 集成的选定 IOS 版本支持此选项，仅当您选择 MKA 进行密钥管理时才可使用此选项。它必须与交换机端的设置匹配。通过启用 MACsec 256 加密标准，下行链路端口支持具有 MACsec 密钥协议 (MKA) 的 802.11 AE 加密，以便在具有 MACsec 功能的设备和主机设备之间进行加密。

有关详细信息，请参阅基于身份的网络服务：MAC 安全。

Port Authentication Exception Policy 窗格

此窗格仅为有线网络显示。

Port Authentication Exception Policy 窗格可让您在身份验证过程中定制 IEEE 802.1X 请求方的行为。如果端口异常未启用，请求方会继续其现有行为并仅在成功完成完整配置后（或如此部分之前所述，发起身份验证的 maxStarts 数量而没有验证器响应之后）才会打开端口。选择以下其中一个选项：

- 在身份验证前允许数据流量通过 - 在身份验证尝试之前允许数据流量通过。
- 在身份验证之后允许数据流量通过，即使：
  - EAP 失败 - 选择后，请求方尝试身份验证。如果身份验证失败，请求方在身份验证失败的情况下依然允许数据流量通过。
  - EAP 成功，但密钥管理失败 - 选择后，请求方尝试与密钥服务器就密钥进行协商，但在密钥协商因任何原因失败的情况下依然允许数据流量通过。此设置仅在已配置密钥管理的情况下有效。如果密钥管理设置为无，则复选框以灰色显示。

限制 MACsec 需要 ACS 版本 5.1 及更高版本和支持 MACsec 的交换机。请参阅《*Catalyst 3750-X* 和 *3560-X* 交换机软件配置指南》以了解 ACS 或交换机配置。

关联模式

该窗格仅对无线网络显示。

选择关联模式：

- WEP
- WAP Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA 2 Enterprise (TKIP)
- WPA 2 Enterprise (AES)
- CCKM (TKIP) -（需要思科 CB21AG 无线网卡）
- CCKM (AES) -（需要思科 CB21AG 无线网卡）

配置开放网络

开放网络不使用身份验证或加密。如果要创建开放（非安全）网络，请执行以下步骤。

步骤 1 从 Security Level 页面选择**开放式网络 (Open Network)**。此选择提供的网络安全性最低，建议用于访客接入无线网络。

步骤 2 单击**下一步 (Next)**。

步骤 3 确定连接类型。

配置共享密钥网络

Wi-Fi网络可使用共享密钥获得加密密钥，用于在终端之间和网络接入点之间对数据加密。配合WPA或 WPA2 Personal 使用共享密钥，可提供中等级别的安全性，适合于小型或家庭办公室。

注释 不建议对企业无线网络使用共享密钥安全性。

如果要将共享密钥网络作为您的安全级别，请执行以下步骤。

步骤 1 选择**共享密钥网络 (Shared Key Network)**。

步骤 2 在“安全级别”(Security Level) 窗口中单击**下一步 (Next)**。

步骤 3 指定 **User Connection** 或 **Machine Connection**。

步骤 4 单击**下一步 (Next)**。

步骤 5 Shared Key Type - 指定共享密钥关联模式，用于确定共享密钥类型。选项如下所示：

- WEP - 与静态 WEP 加密关联传统 IEEE 802.11 开放系统。
- Shared - 与静态 WEP 加密关联传统 IEEE 802.11 共享密钥。

- WPA/WPA2-Personal - 一种 Wi-Fi 安全协议，用于从密码预共享密钥 (PSK) 获得加密密钥。

步骤 6 如果选择了传统 IEEE 802.11 WEP 或共享密钥，请选择 40 位、64 位、104 位或 128 位。40 位或 64 位 WEP 密钥必须是 5 个 ASCII 字符或 10 个十六进制数字。104 位或 128 位 WEP 密钥必须是 13 个 ASCII 字符或 26 个十六进制数字。

步骤 7 如果选择了 WPA 或“WPA2 个人”(WPA2 Personal)，请选择要使用的加密类型 (TKIP/AES)，然后输入共享密钥。输入的密钥必须为 8 到 63 个 ASCII 字符或正好 64 个十六进制数字。如果共享密钥由 ASCII 字符组成，请选择 **ASCII**。如果共享密钥包含 64 个十六进制数字，请选择**十六进制 (Hexadecimal)**。

步骤 8 单击**完成 (Done)**。然后单击**确定 (OK)**。

Networks，Network Connection Type 窗格

本节介绍 Networks 窗口的网络连接类型窗格，该窗格遵循网络访问管理器配置文件编辑器中的安全级别。选择以下连接类型之一：

- Machine Connection - 存储在 Windows Active Directory 中的设备名称用来进行授权。计算机连接通常用于无需用户凭证进行连接的情况。即使用户已注销且用户凭证不可用，如果终端站应登录到网络，也请选择此选项。此选项通常用于在用户获得访问权限之前连接域并从网络获得 GPO 和其他更新。

  注释 如果没有可用的已知网络，VPN 登录前启动 (SBL) 会失败。SBL 模式中允许的网络配置文件包括使用非 802-1X 身份验证模式的所有媒体类型，例如开放 WEP、WPA/WPA2 个人和静态密钥 (WEP) 网络。如果为 Before User Logon 和计算机连接授权配置网络访问管理器，网络访问管理器将要求用户提供网络信息，并且 VPN SBL 成功启动。

- User Connection - 用户凭证用于进行授权。

  如果在“客户端策略”(Client Policy) 窗格中选择了“用户登录前”(Before User Logon)，则用户在 Windows 开始屏幕中输入登录凭证后，网络访问管理器会收集用户的凭证。在 Windows 启动用户的 Windows 会话时，网络访问管理器会建立网络连接。

  如果在“客户端策略”(Client Policy) 窗格中选择了“用户登录后”(After User Logon)，则用户登录到 Windows 后，网络访问管理器才启动连接。

  用户注销后，当前用户网络连接即终止。如果计算机网络配置文件可用，NAM 会重新连接到计算机网络。

- Machine and User Connection - 仅在配置网络身份验证时可用，如在 Security Level 窗格中所选。计算机 ID 和用户凭证均使用，但仅当用户未登录到设备时，计算机部分才有效。这两部分的配置是相同的，但是，计算机连接的身份验证类型和凭证可能与用户连接的身份验证类型和凭证不同。

当用户未登录时，选择此选项可始终通过计算机连接将 PC 连接到网络。当用户已登录时，选择此选项可始终通过用户连接将 PC 连接到网络。

在 EAP-FAST 配置为 EAP 方法（在下一个窗格中）时，支持 EAP 链接。这意味着网络访问管理器会确认计算机和用户为已知实体并且由公司管理。

当您选择网络连接类型时，“网络”(Networks) 对话框中会显示其他选项卡。使用这些选项卡，可为所选网络连接类型设置 EAP 方法和凭证。

Networks、User 或 Machine Authentication 页面

在选择网络连接类型后，选择这些连接类型的身份验证方法。在选择身份验证方法后，显示屏幕会更新为选择的方法，并要求您提供其他信息。

注释 如果您已启用 MACsec，请确保选择支持 MSK 密钥派生的 EAP 方法，例如 PEAP、EAP-TLS 或 EAP-FAST。此外，即使没有启用 MACsec，使用网络访问管理器也可将 MTU 从 1500 降低至 1468 以支持 MACsec。

EAP 概述

EAP 是一种 IETF RFC，可满足身份验证协议与承载它的传输协议进行分离的要求。此分离允许传输协议（如 IEEE 802.1X、UDP 或 RADIUS）承载 EAP 协议，而无需更改身份验证协议。

基本 EAP 协议包括四种数据包类型：

- EAP 请求 - 身份验证器向请求方发送请求数据包。每个请求都有一个类型字段，用于指示请求内容，如请求方身份和要使用的 EAP 类型。顺序号允许身份验证器和对等项将 EAP 响应与各个 EAP 请求进行匹配。
- EAP 响应 - 请求方向身份验证器发送响应数据包并使用顺序号与启动的 EAP 请求进行匹配。EAP 响应的类型通常匹配 EAP 请求，除非响应为负 (NAK)。
- EAP 成功 - 身份验证成功后，身份验证器向请求方发送成功数据包。
- EAP 失败 - 如果身份验证失败，身份验证器向请求方发送失败数据包。

在 IEEE 802.11X 系统中使用 EAP 时，接入点在 EAP 穿透模式下工作。在此模式下，接入点检查代码、标识符和长度字段，然后将从请求方收到的 EAP 数据包转发至 AAA 服务器。从 AAA 服务器身份验证器接收的数据包将转发到请求方。

EAP-GTC

EAP-GTC 是基于简单用户名和密码身份验证的 EAP 身份验证方法。不使用质询响应方法，用户名和密码均以明文传递。建议在隧道 EAP 方法内部（请参阅下面的隧道 EAP 方法）或针对一次性密码 (OTP) 使用此方法。

EAP-GTC 不提供相互身份验证。它只对客户端进行身份验证，因此欺诈服务器可能会获取用户的凭证。如果需要相互身份验证，则在隧道 EAP 方法内部使用 EAP-GTC，这样可提供服务器身份验证。

EAP-GTC 未提供密钥材料。因此，不能对 MACsec 使用此方法。如果进一步的流量加密需要密钥材料，则在隧道 EAP 方法内使用 EAP-GTC，这样可提供密钥材料（如有必要，还提供内部和外部 EAP 方法加密绑定）。

有两个密码源选项：

- 使用密码进行身份验证 - 只适用于有良好保护的有线环境
- 使用令牌进行身份验证 - 更安全，因为令牌代码或 OTP 的生命期较短（通常约为 10 秒）

注释 网络访问管理器、身份验证器和 EAP-GTC 协议均无法区分密码和令牌代码。这些选项只影响网络访问管理器中凭证的生命期。虽然可在注销前或更长时间内记住密码，但不能记住令牌代码（因为每次身份验证时都提示用户输入令牌代码）。

如果使用密码进行身份验证，可以使用此协议对照包含哈希值密码的数据库进行身份验证，因为密码以明文传递到身份验证器。如果存在数据库泄露的可能，建议使用此方法。

EAP-TLS

EAP 传输层安全 (EAP-TLS) 是基于 TLS 协议 (RFC 2246) 的 IEEE 802.1X EAP 身份验证算法。TLS 使用基于 X.509 数字证书的相互身份验证。EAP-TLS 消息交换提供相互身份验证、加密套件协商、密钥交换、客户端与身份验证服务器之间的身份验证以及可用于流量加密的密钥材料。

下面的列表提供了 EAP-TLS 客户端证书可为有线和无线连接提供强身份验证的主要原因：

- 身份验证自动进行，通常无需用户干预。
- 不存在对用户密码的依赖性。
- 数字证书提供强身份验证保护。
- 使用公共密钥加密保护消息交换。
- 证书不易受字典攻击。
- 身份验证过程会为数据加密和签名生成相互确定的密钥。

EAP-TLS 包含两个选项：

- “验证服务器证书”(Validate Server Certificate) - 启用服务器证书验证。
- “启用快速重新连接”(Enable Fast Reconnect) - 启用 TLS 会话恢复，只要 TLS 会话数据同时保存在客户端和服务器上，就允许使用简短的 TLS 握手进行快得多的重新身份验证。

注释 对于计算机连接身份验证，“使用智能卡时禁用”(Disable When Using a Smart Card) 选项不可用。

EAP-TTLS

EAP 隧道传输层安全 (EAP-TTLS) 是扩展 EAP-TLS 功能的两阶段协议。第 1 阶段执行完整 TLS 会话，并生成用于在第 2 阶段安全地在服务器与客户端之间隧道化属性的会话密钥。您可以使用在第 2 阶段隧道化的属性通过多种不同机制执行其他身份验证。

网络访问管理器不支持在 EAP-TTLS 身份验证期间使用的内部和外部方法加密绑定。如果需要加密绑定，则必须使用 EAP-FAST。加密绑定可防御特殊类别的中间人攻击，在这类攻击中，攻击者无需知道凭证就可以劫持用户的连接。

可以在第 2 阶段使用的身份验证机制包括以下协议：

- PAP（密码验证协议）- 使用双向握手为对等项提供证明其身份的简单方法。对等项向身份验证器重复发送 ID/密码对，直至身份验证确认或失败。如果需要相互身份验证，必须将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。

  由于密码传递到身份验证器，您可以使用此协议对照包含哈希值密码的数据库进行身份验证。如果存在数据库泄露的可能，建议使用此方法。

  注释 可以使用 EAP-TTLS PAP 进行基于令牌和基于 OTP 的身份验证。

- CHAP（质询握手身份验证协议）- 使用三次握手验证对等项的身份。如果需要相互身份验证，应将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。使用此质询响应方法，需要在身份验证器的数据库中存储明文密码。
- MS-CHAP (Microsoft CHAP) - 使用三次握手验证对等项的身份。如果需要相互身份验证，应将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。使用这个基于密码的 NT 哈希值的质询响应方法，需要在身份验证器的数据库中存储明文密码或至少存储密码的 NT 哈希值。
- MS-CHAPv2 - 通过在响应数据包中包含对等项质询以及在成功数据包中包含身份验证器响应来提供对等项之间的相互身份验证。先对客户端、再对服务器进行身份验证。如果服务器需要先于客户端进行身份验证（以防御字典攻击），应该将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。使用这个基于密码的 NT 哈希值的质询响应方法，需要在身份验证器的数据库中存储明文密码或至少存储密码的 NT 哈希值。

配置 EAP-TTLS

- EAP - 允许使用以下 EAP 方法之一：
  - EAP-MD5 (EAP Message Digest 5) - 使用三向握手来验证对等体的身份（类似于 CHAP）。使用这种质询-响应方法，需要在验证方的数据库中存储明文密码。

- EAP-MSCHAPv2 - 使用三次握手验证对等体的身份。先对客户端、再对服务器进行身份验证。如果对服务器的身份验证需要先于客户端（例如为防止字典攻击），则应配置EAP-TTLS以在第 1 阶段验证服务器的证书。对 NT 哈希值形式的密码使用这种质询-响应方法时，需要在验证方的数据库中存储明文密码或至少 NT 哈希值形式的密码。

- EAP-TTLS 设置
  - Validate Server Identity - 启用服务器证书验证。

    注释 如果启用此选项，请确保在 RADIUS 服务器上安装的服务器证书中包含服务器身份验证的扩展密钥用法 (EKU)。当 RADIUS 服务器在身份验证期间将其配置的证书发送到客户端时，必须对网络访问和身份验证使用此服务器身份验证设置。

  - Enable Fast Reconnect - 只启用外部 TLS 会话恢复，而不管内部身份验证是跳过还是由验证方控制。

    注释 Disable When Using a Smart Card 不适用于机器连接身份验证。

- Inner Methods - 指定在 TLS 隧道创建后使用的内部方法。仅适用于 Wi-Fi 媒体类型。

PEAP 选项

受保护的 EAP (PEAP) 是基于隧道 TLS 的 EAP 方法。它在客户端身份验证之前使用 TLS 进行服务器身份验证，以加密内部身份验证方法。内部身份验证在受信任加密保护的隧道内进行，支持多种不同的内部身份验证方法，包括证书、令牌和密码。网络访问管理器不支持在 PEAP 身份验证期间使用的内部和外部方法加密绑定。如果需要加密绑定，则必须使用 EAP-FAST。加密绑定可防御特殊类别的中间人攻击，在这类攻击中，攻击者无需知道凭证就可以劫持用户的连接。

PEAP 通过提供以下服务保护 EAP 方法：

- 为 EAP 数据包创建 TLS 隧道
- 消息身份验证
- 消息加密
- 服务器到客户端的身份验证

可以使用以下身份验证方法：

- 使用密码进行身份验证

- EAP-MSCHAPv2 - 使用三次握手验证对等体的身份。先对客户端、再对服务器进行身份验证。如果服务器需要先于客户端进行身份验证（如为了防御字典攻击），则必须配置PEAP以验证服务器的证书。使用基于密码的 NT 哈希值的质询响应方法，需要在身份验证器数据库中存储明文密码或至少存储密码的 NT 哈希值。
- EAP-GTC（EAP 通用令牌卡）- 定义 EAP 信封以承载用户名和密码。如果需要相互身份验证，则必须配置 PEAP 以验证服务器的证书。由于密码以明文传递到身份验证器，可以使用此协议对照包含哈希值密码的数据库进行身份验证。如果存在数据库泄露的可能，建议使用此方法。

- EAP-TLS，使用证书
  - EAP-TLS - 定义 EAP 信封以承载用户证书。为避免中间人攻击（劫持有效用户的连接），建议不要将 PEAP (EAP-TLS) 和 EAP-TLS 配置文件混合在一起向同一身份验证器进行身份验证。应相应地配置身份验证器（不同时启用普通和隧道 EAP-TLS）。

配置 PEAP

- PEAP-EAP 设置
  - Validate Server Identity - 启用服务器证书验证。

    注释 如果启用此选项，请确保在 RADIUS 服务器上安装的服务器证书中包含服务器身份验证的扩展密钥用法 (EKU)。当 RADIUS 服务器在身份验证期间将其配置的证书发送到客户端时，必须对网络访问和身份验证使用此服务器身份验证设置。

  - Enable Fast Reconnect - 仅启用外部 TLS 会话恢复。验证器控制是否跳过内部身份验证。
  - Disable when using a smart card - 在使用智能卡进行身份验证时，请勿使用“快速重新连接”。智能卡仅适用于用户连接。
  - Authenticate using a token and EAP GTC - 对计算机身份验证不可用。

- 基于凭证源的内部方法
  - 使用 EAP-MSCHAPv2 和/或 EAP-GTC 的密码进行身份验证。
  - EAP-TLS，使用证书进行身份验证。
  - 使用令牌和 EAP-GTC 进行身份验证 - 对计算机身份验证不可用。

    注释 在用户登录之前，智能卡支持在 Windows 上不可用。

EAP-FAST 设置

EAP-FAST 是 IEEE 802.1X 身份验证类型，可提供简单灵活的部署和管理。它支持多种用户和密码数据库类型、服务器发起的密码过期和更改以及数字证书（可选）。

EAP-FAST 针对想要部署 IEEE 802.1X EAP 类型的客户而开发，该类型不使用证书但可防御字典攻击。

自 AnyConnect 3.1 起，配置计算机和用户连接时均支持 EAP 链。这意味着网络访问管理器将验证计算机和用户是否为已知实体且由公司管理，这对于控制用户拥有的连接到企业网络的资产来说非常有用。有关 EAP 链的详细信息，请参阅 RFC 3748。

EAP-FAST 将 TLS 消息封装在 EAP 内，包括三个协议阶段：

1. 调配阶段 - 使用经过身份验证的 Diffie-Hellman 协议 (ADHP) 调配具有名为保护访问凭证 (PAC) 的共享加密凭证的客户端。
2. 隧道建立阶段 - 使用 PAC 建立隧道。
3. 身份验证阶段 - 身份验证服务器对用户凭证（令牌、用户名/密码或数字证书）进行身份验证。

与其他隧道 EAP 方法不同，EAP-FAST 提供内部和外部方法之间的加密绑定，可防御特殊类别的中间人攻击，在这类攻击中，攻击者可劫持有效用户的连接。

配置 EAP-FAST

- EAP-FAST 设置
  - Validate Server Identity - 启用服务器证书验证。启用此选项会在管理实用程序中引入两个额外的对话框，并且在网络访问管理器配置文件编辑器任务列表中添加额外的证书窗格。

    注释 如果启用此选项，请确保在 RADIUS 服务器上安装的服务器证书中包含服务器身份验证的扩展密钥用法 (EKU)。当 RADIUS 服务器在身份验证期间将其配置的证书发送到客户端时，必须对网络访问和身份验证使用此服务器身份验证设置。

  - Enable Fast Reconnect - 启用会话恢复。用来在 EAP-FAST 中恢复身份验证会话的两种机制是用户授权 PAC（用于代替内部身份验证）和 TLS 会话恢复（用于允许简化的外部 TLS 握手）。此 Enable Fast Reconnect 参数可启用或禁用这两种机制。验证方决定具体使用哪一种机制。

    注释 计算机 PAC 提供简化的 TLS 握手，无需内部身份验证。此控制通过启用/禁用 PAC 参数来处理。

注释 “使用智能卡时禁用”(Disable When Using a Smart Card) 选项仅适用于用户连接授权。

- Inner methods based on Credentials Source - 可让您使用密码或证书进行身份验证。
  - 使用 EAP-MSCHAPv2 或 EAP-GTC 的密码进行身份验证。EAP-MSCHAPv2 提供相互身份验证，但它先对客户端、再对服务器进行身份验证。如果要在相互身份验证中先对服务器进行身份验证，请配置 EAP-FAST 只用于经过身份验证的调配，并且验证服务器的证书。EAP-MSCHAPv2 使用基于密码的 NT 哈希值的质询-响应方法，它要求您在验证方的数据库中存储明文密码或至少 NT 哈希值形式的密码。由于密码在 EAP-GTC 中以明文形式传递给验证方，因此您可以使用此协议根据数据库进行身份验证。
  - Authenticate using a certificate - 决定使用证书进行身份验证的以下条件：收到请求时，以明文形式发送客户端证书，仅在隧道内发送客户端证书，或者使用 EAP-TLS 在隧道中发送客户端证书。
  - 使用令牌和 EAP-GTC 进行身份验证。
- Use PACs - 可以指定使用 PAC 进行 EAP-FAST 身份验证。PAC 是分发给客户端以优化网络身份验证的凭证。

注释 通常使用 PAC 选项，因为大多数身份验证服务器对 EAP-FAST 使用 PAC。在删除此选项之前，请验证身份验证服务器不对 EAP-FAST 使用 PAC。否则，客户端的身份验证尝试不会成功。

LEAP 设置

LEAP（轻量级 EAP）支持无线网络。它基于可扩展身份验证协议 (EAP) 框架，由思科开发，旨在创建比 WEP 更安全的协议。

注释 LEAP 容易受到字典攻击，除非实施强密码并定期使密码过期。思科建议使用 EAP-FAST、PEAP 或 EAP-TLS，它们的身份验证方法不易受字典攻击。

只能用于用户身份验证的 LEAP 设置：

- 注销后延长用户连接 - 用户注销后保持连接打开状态。如果同一用户再次登录，网络连接仍处于活动状态。

请参阅对 Cisco LEAP 漏洞的字典攻击以了解详细信息。

定义网络凭证

在 Networks > Credentials 窗格中，指定是否使用用户和/或机器凭证，并且配置受信任服务器验证规则。

配置用户凭证

EAP 对话可能涉及多种 EAP 身份验证方法，其中每种身份验证要求的身份可能不同（例如先是计算机身份验证，然后是用户身份验证）。例如，对等项最初可能声称身份为 nouser@cisco.com 以将身份验证请求发送到 cisco.com EAP 服务器。但是，一旦已协商 TLS 会话，对等项可能声称身份为 johndoe@cisco.com。因此，即使通过用户的身份提供保护，目标领域也不一定匹配，除非对话在本地身份验证服务器上终止。

对于用户连接，当使用了 [username] 和 [domain] 占位符模式时，适用以下条件：

- 如果客户端证书用于身份验证 - 从各 X509 证书属性获取 [username] 和 [password] 的占位符值。根据首次匹配按下述顺序分析属性。例如，如果对于用户身份验证，身份是 userA@example.com（其中 username=userA 且 domain=example.com），对于计算机身份验证，身份是 hostA.example.com（其中 username=hostA 且 domain=example.com），将分析以下属性：
- 如果是基于用户证书的身份验证：
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@eample.com
  - Subject = .../CN=userA/DC=example/DC=com/...
  - Subject = userA (no domain)
- 如果是基于计算机证书的身份验证：
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- 如果凭证源是最终用户 - 从用户输入的信息获取占位符的值。
- 如果从操作系统获取证书 - 从登录信息获取占位符的值。
- 如果凭证是静态的 - 没有使用占位符。

在 Credentials 窗格中，您可以指定用于对关联网络进行身份验证所需的凭证。

步骤 1 定义受保护身份模式的用户身份。网络访问管理器支持以下身份占位符模式：

- [username] - 指定用户名。如果用户输入 username@domain 或 domain\username，则域部分会被剥离。

- [raw] - 完全按照用户的输入指定用户名。
- [domain] - 指定用户设备的域。

步骤 2 指定典型的未受保护的身份模式。

尚未协商的会话遇到身份请求，并以明文响应，而无需完整性保护或身份验证。这些会话可能遭到监听和数据包修改。

- anonymous@[domain] - 常常用在隧道方法中，用于在以明文发送值时隐藏用户身份。在内部方法中，将真实用户身份提供为受保护的身份。
- [username]@[domain] - 用于非隧道化方法。

  注释 以明文发送未受保护的身份信息。如果初始明文身份请求或响应被篡改，服务器可能会发现一旦建立了 TLS 会话就无法验证身份。例如，用户 ID 可能无效或不在 EAP 服务器处理的领域内。

步骤 3 指定保护身份模式。

为防止用户 ID 被监听，明文身份只能提供足以让身份验证请求路由到正确领域的信息。

- [username]@[domain]
- 用作用户身份的实际字符串（无占位符）

步骤 4 提供更多用户凭证信息：

- Use Single Sign On Credentials - 从操作系统的登录信息中获取凭证。如果登录凭证失败，网络访问管理器暂时（直到下次登录）开启并提示用户通过 GUI 提供凭证。

  注释 您不能将 Windows 登录凭证与网络访问管理器和 SSO 一起自动使用。将 SSO 与网络访问管理器一起使用需要拦截登录凭证；因此，系统将在安装或注销后提示您重新启动。

- Use Static Credentials - 从该配置文件编辑器提供的网络配置文件获取用户凭证。如果静态凭证失败，网络访问管理器在加载新配置之后才会再次使用凭证。

  注释 在此字段中，& 符号是无效字符。

- Prompt for Credentials - 通过 AnyConnect GUI 获取来自最终用户的凭证，正如下文所指定：
  - Remember Forever - 永久记住凭证。如果记住的凭证失败，则再次提示用户输入凭证。凭证保留在文件中，并使用本地计算机密码进行加密。
  - Remember While User Is Logged On - 记住凭证，直到用户注销为止。如果记住的凭证失败，则再次提示用户输入凭证。
  - Never Remember - 从不记住凭证。网络访问管理器每次需要凭证信息以进行身份验证时都会提示用户。

步骤 5 在需要证书时确定哪个证书源用于进行身份验证：

- 智能卡或操作系统证书 - 网络访问管理器使用在操作系统证书存储库或智能卡中找到的证书。

- 仅限智能卡证书 - 网络访问管理器仅使用智能卡中找到的证书。

步骤 6 在 Remember Smart Card Pin 参数中，确定网络访问管理器记住用于从智能卡检索证书的 PIN 的时间长度。请参阅步骤 2 以了解可用的选项。

注释 PIN 保留时间绝不能超过证书本身的保留时间。

某些智能卡连接所需时间可能比其他智能卡更长，这取决于智能卡芯片和驱动程序（也称为加密服务提供程序 (CSP) 和密钥存储提供程序 (KSP)）。增加连接超时可能给网络足够时间来执行基于智能卡的身份验证。

配置计算机凭证

EAP 对话可能涉及多种 EAP 身份验证方法，其中每种身份验证要求的身份可能不同（例如先是计算机身份验证，然后是用户身份验证）。例如，对等成员最初可能要求 nouser@example.com 的身份来将身份验证请求路由到 cisco.com EAP 服务器。但是，一旦 TLS 会话经过协商，对等成员就可能要求 johndoe@example.com 的身份。因此，即使通过用户的身份提供保护，目标领域也不一定匹配，除非对话在本地身份验证服务器上终止。

对于计算机连接，只要使用 [username] 和 [domain] 占位符，以下条件即适用：

- 如果客户端证书用于身份验证 - 从各 X509 证书属性获取 [username] 和 [password] 的占位符值。根据首次匹配按下述顺序分析属性。例如，如果对于用户身份验证来说身份是 userA@cisco.com（其中 username=userA，domain=cisco.com），对于计算机身份验证来说是 hostA.cisco.com（其中 username=hostA，domain=cisco.com），则分析以下属性：
- 如果是基于用户证书的身份验证：
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@example.com
  - Subject = .../CN=userA/DC=example.com/...
  - Subject = userA (no domain)
- 如果是基于计算机证书的身份验证：
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- 如果客户端证书不用于身份验证 - 从操作系统获取凭证，[username] 占位符代表分配的计算机名称。

使用凭证面板，可以指定所需的计算机凭证。

步骤 1 为受保护的身份模式定义计算机身份。网络访问管理器支持以下身份占位符模式：

- [username] - 指定用户名。如果用户输入 username@domain 或 domain\username，则会删除域部分。
- [raw] - 完全按照用户的输入指定用户名。
- [domain] - 指定用户 PC 的域。

步骤 2 定义典型的未受保护的计算机身份模式。

尚未协商的会话遇到身份请求，并以明文响应，而无需完整性保护或身份验证。这些会话可能遭到监听和数据包修改。

- host/anonymous@[domain]
- 作为计算机身份发送的实际字符串（无占位符）

步骤 3 定义受保护的计算机身份模式。

为防止用户 ID 被监听，明文身份只能提供足以让身份验证请求路由到正确领域的信息。典型的受保护的计算机身份模式如下所示：

- host/[username]@[domain]
- 作为计算机身份使用的实际字符串（无占位符）

步骤 4 提供更多计算机凭证信息。

- 使用机器凭证 - 从操作系统获取凭证。
- 使用静态凭证 - 指定要在部署文件中发送的实际静态密码。静态凭证不适用于基于证书的身份验证。

设置网络访问管理器以选择正确的证书

在客户端身份验证时，如果有两个证书，则网络访问管理器将根据证书属性自动选择最佳证书。由于首选证书的条件因客户而已，所以您必须配置以下字段来确定证书选择，并提供需要的规则来覆盖证书选择。

如果多个证书与同一个规则匹配或者没有证书与规则匹配，则ACE引擎将根据算法对证书优先级进行排序，并根据特定条件（例如，是否有私钥，是否来自设备存储库等）选择一个证书。如果多个证书具有相同的优先级，ACE 引擎将选择在该优先级中找到的第一个证书。

步骤 1 从 AnyConnect 配置文件编辑器中，选择“**网络**”**(Networks)** 选项卡。

步骤 2 选择要编辑的网络。

步骤 3 选择**计算机凭证 (Machine Credentials)** 选项卡。

步骤 4 在页面底部，选择**使用证书匹配规则 (Use Certificate Matching Rule)**。

步骤 5 从“证书字段”(Certificate Field) 下拉菜单中，选择您要的搜索条件。

步骤 6 从“匹配”(Match) 下拉菜单中，确定搜索是否包含字段完全匹配（等于）或字段部分匹配（包括）。

步骤 7 在“数值”(Value) 字段中，输入证书搜索条件。

配置受信任服务器验证规则

为 EAP 方法配置了“验证服务器身份”(Validate Server Identity) 选项时，“证书”(Certificate) 面板允许您配置证书服务器或授权的验证规则。验证的结果将确定证书服务器或授权是否得到信任。

要定义证书服务器验证规则，请执行以下步骤：

步骤 1 显示**证书字段 (Certificate Field)** 和**匹配 (Match)** 列的可选设置时，单击下拉箭头并选择所需的设置。

步骤 2 在 Value 字段中输入值。

步骤 3 在“规则”(Rule) 下，单击**添加 (Add)**。

步骤 4 在“受信任证书颁发机构”(Certificate Trusted Authority) 窗格中，选择以下选项之一：

- 信任安装在操作系统上的所有根证书颁发机构 (CA) (Trust Any Root Certificate Authority [CA] Installed on the OS) - 如果选择此选项，仅将本地计算机或证书存储区视为服务器的证书链验证。
- 包括根证书颁发机构 (CA) 证书。

  注释 如果选择“包括根证书颁发机构 (CA) 证书”(Include Root Certificate Authority [CA] Certificates)，则必须单击**添加 (Add)** 将 CA 证书导入到配置。如果使用的证书正在从 Windows 证书库中导出，请使用“Base 64 encoded X.509 (.cer)”选项。

Network Groups 窗口

在 Network Groups 窗口中，可向特定的组分配网络连接。对连接分组提供多项优势：

- 当用户尝试连接时，可改善用户体验。当配置了多个隐藏网络时，客户端可以按照定义的顺序遍历隐藏网络列表，直到成功建立连接。在这些情况下，分组可大幅减少建立连接所需的时间。
- 简化所配置连接的管理。使您可以根据需要将管理员网络与用户网络分隔，并允许公司的多角色用户（或经常访问同一区域的用户）在组中定制网络，以提高可选网络列表的可管理性。

作为分发包的一部分而定义的网络将锁定，从而防止用户编辑配置设置或删除网络配置文件。

您可以将网络定义为全局网络。执行此操作时，网络将显示在全局网络部分中。该部分划分为有线和无线网络类型。在这种类型的网络中只能执行排序编辑。

所有非全局网络必须存在于一个组中。默认情况下，会创建一个组，如果所有网络都是全局网络，用户可以删除该组。

步骤 1 从下拉列表选择一个组。

步骤 2 选择**创建网络 (Create networks)** 可允许最终用户在该组中创建网络。部署后，如果您取消选中此项，网络访问管理器会从该组中删除用户创建的任何网络，这会强制用户在另一个组中重新输入网络配置。

步骤 3 选择**查看扫描列表 (See scan list)**，以在使用 AnyConnect GUI 将该组选择为活动组时允许最终用户查看扫描列表。或者，清除复选框以限制用户查看扫描列表。例如，如果您要阻止用户意外连接到相邻设备，应限制扫描列表访问。

注释 这些设置应用基于组。

步骤 4 使用右箭头和左箭头从在“组”(Group) 下拉列表中选择的组中插入和删除网络。如果某网络已移出当前组，则它会放置到默认组中。当默认组正在编辑时，您无法从其中移动网络（使用 > 按钮）。

注释 在给定网络中，每个网络的显示名称必须唯一。因此，任何一组不能包含两个或更多具有相同显示名称的网络。

步骤 5 使用上箭头和下箭头更改组中网络的优先级顺序。