使用Windows和ISE 3.2为Dot1x配置安全客户端NAM

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 网络访问管理器

配置

- 网络图

配置

- 下载并安装安全客户端NAM（网络访问管理器）
- 下载并安装安全客户端NAM配置文件编辑器
- 常规默认配置
- 情形 1：为PEAP(MS-CHAPv2)用户身份验证配置安全客户端NAM请求方
- 方案 2：为EAP-FAST同步用户和机器身份验证配置安全客户端NAM请求方
- 情形 3：为EAP TLS用户证书身份验证配置安全客户端NAM请求方
- 配置ISR 1100和ISE以允许基于方案1 PEAP MSCHAPv2的身份验证
- 配置身份验证和授权策略
- 授权策略

验证

故障排除

- 问题 1：安全客户端未使用NAM配置文件
- 问题 2：必须收集日志以便进一步分析
- 重现问题
- 收集安全客户端DART套件

相关信息

简介

本文档介绍如何在Windows上配置安全客户端网络分析模块(NAM)。

先决条件

要求

Cisco 建议您了解以下主题：

- 对RADIUS请求方的基本了解
- Dot1x
- PEAP
- PKI

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Windows 10 Pro版本22H2,19045.3930
- ISE 3.2
- 思科C1117 Cisco IOS® XE软件版本17.12.02
- Active Directory 2016

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍如何在Windows上配置安全客户端NAM。使用预部署选项和配置文件编辑器执行dot1x身份验证。此外，还提供了如何实现此目标的一些示例。

在网络中，请求方是点对点LAN网段一端的实体，它寻求通过连接到链路另一端的身份验证器进行身份验证。

IEEE 802.1X标准使用术语Supplicant客户端来指代硬件或软件。实际上，请求方是安装在最终用户计算机上的软件应用程序。用户调用请求方并提交凭证以将计算机连接到安全网络。如果身份验证成功，则身份验证器通常允许计算机连接到网络。

网络访问管理器

网络接入管理器是客户端软件，根据策略提供安全的第2层网络。它会检测并选择最佳的第2层接入网络，并对有线和无线网络的接入执行设备身份验证。网络访问管理器管理用户和设备身份以及安全访问所需的网络访问协议。它可以智能地工作，防止最终用户进行违反管理员定义的策略的连接。

网络接入管理器设计为单宿主，一次只允许一个网络连接。此外，有线连接的优先级高于无线，因此，如果通过有线连接插入网络，无线适配器会因没有IP地址而被禁用。

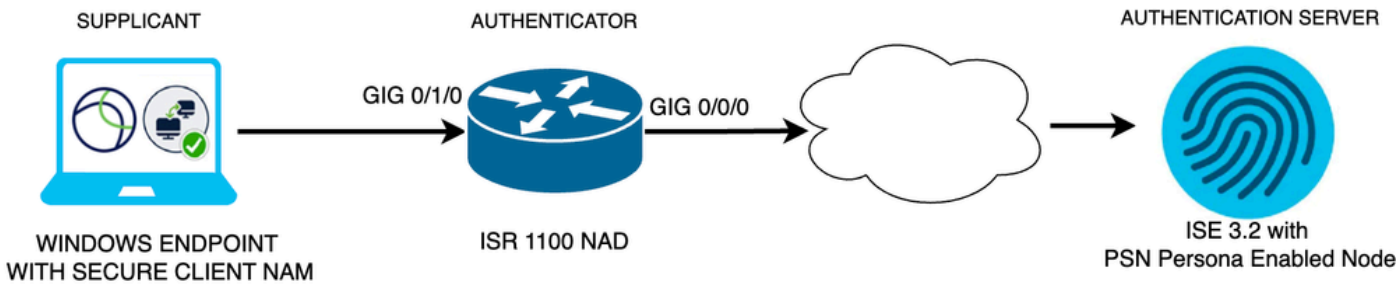
配置

网络图

理解dot1x身份验证需要三个部分：

1. 可以使用dot1x的请求方。
2. 身份验证器也称为NAS/NAD，用作封装RADIUS内dot1x流量的代理。
3. 和身份验证服务器。

在本示例中，请求方的安装和配置方式不同。稍后，显示网络设备配置和身份验证服务器的场景。



网络图

配置

1. 下载并安装安全客户端NAM（网络访问管理器）。
2. 下载并安装安全客户端NAM配置文件编辑器。
3. 常规默认配置。
4. 情形 1：为PEAP(MS-CHAPv2)用户身份验证配置安全客户端NAM请求方。
5. 方案 2：配置用户和机器身份验证时，同时为EAP-FAST配置安全客户端NAM请求方。
6. 场景3第1部分：为EAP-TLS配置安全客户端NAM请求方。
7. 场景3第2部分：配置需要和ISE演示。

下载并安装安全客户端NAM（网络访问管理器）

思科软件下载

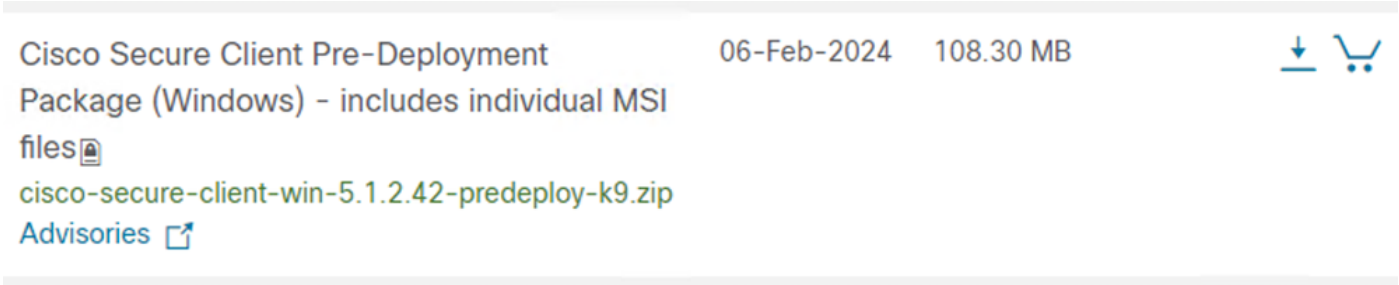
1.在产品名称搜索栏上，键入安全客户端5。

下载Home > Security > VPN and Endpoint Security Clients > Secure Client（包括AnyConnect）> Secure Client 5 > AnyConnect VPN Client Software。

2.在本配置示例中，使用版本5.1.2.42。

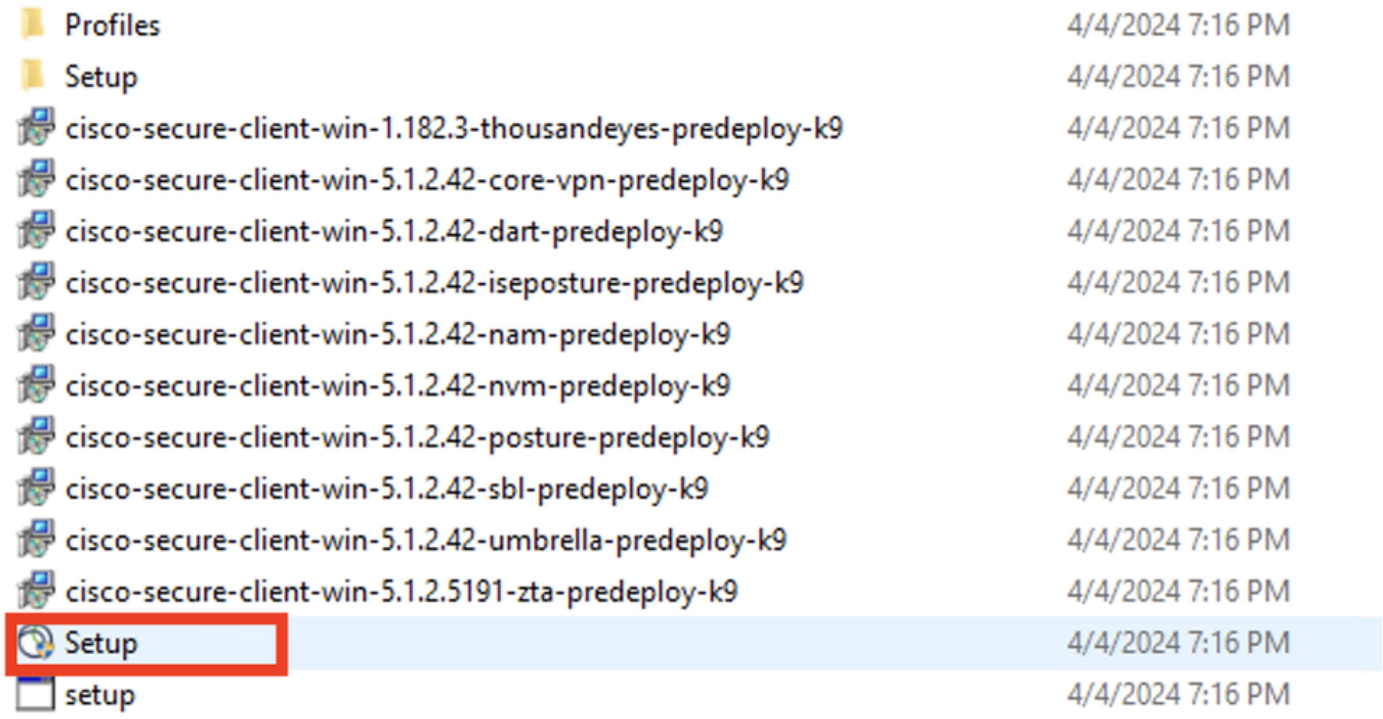
有多种方法可以将安全客户端部署到Windows设备；从SCCM、从身份服务引擎和VPN前端。但是，在本文中，使用的安装方法是预部署方法。

3.在此页面上，搜索文件Cisco Secure Client Headend Deployment Package(Windows)。



Msi zip文件

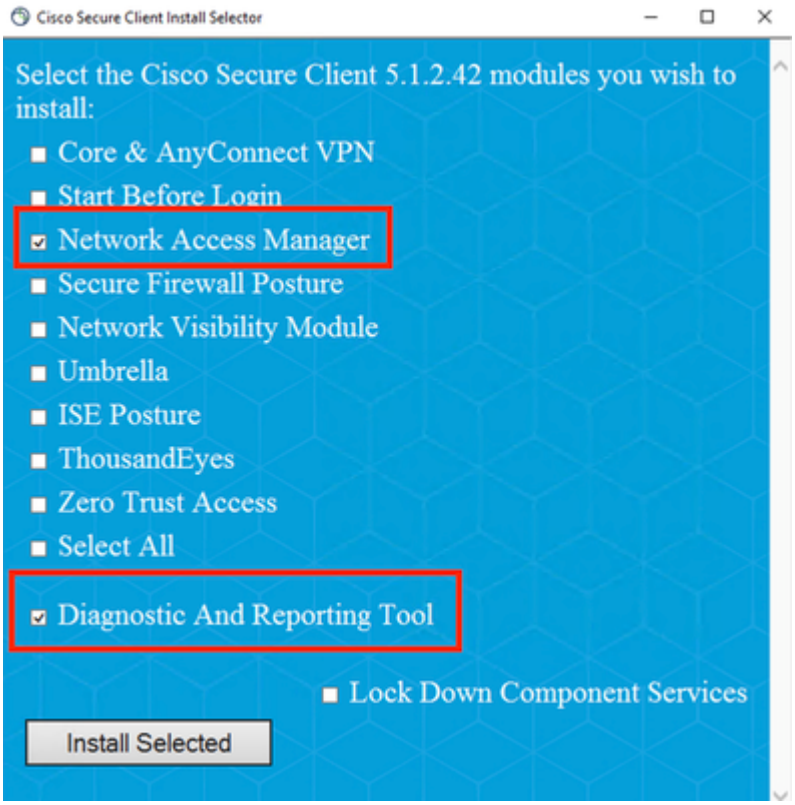
4.下载并解压后，单击Setup。



安全客户端文件

5.安装网络访问管理器和诊断和报告工具模块。

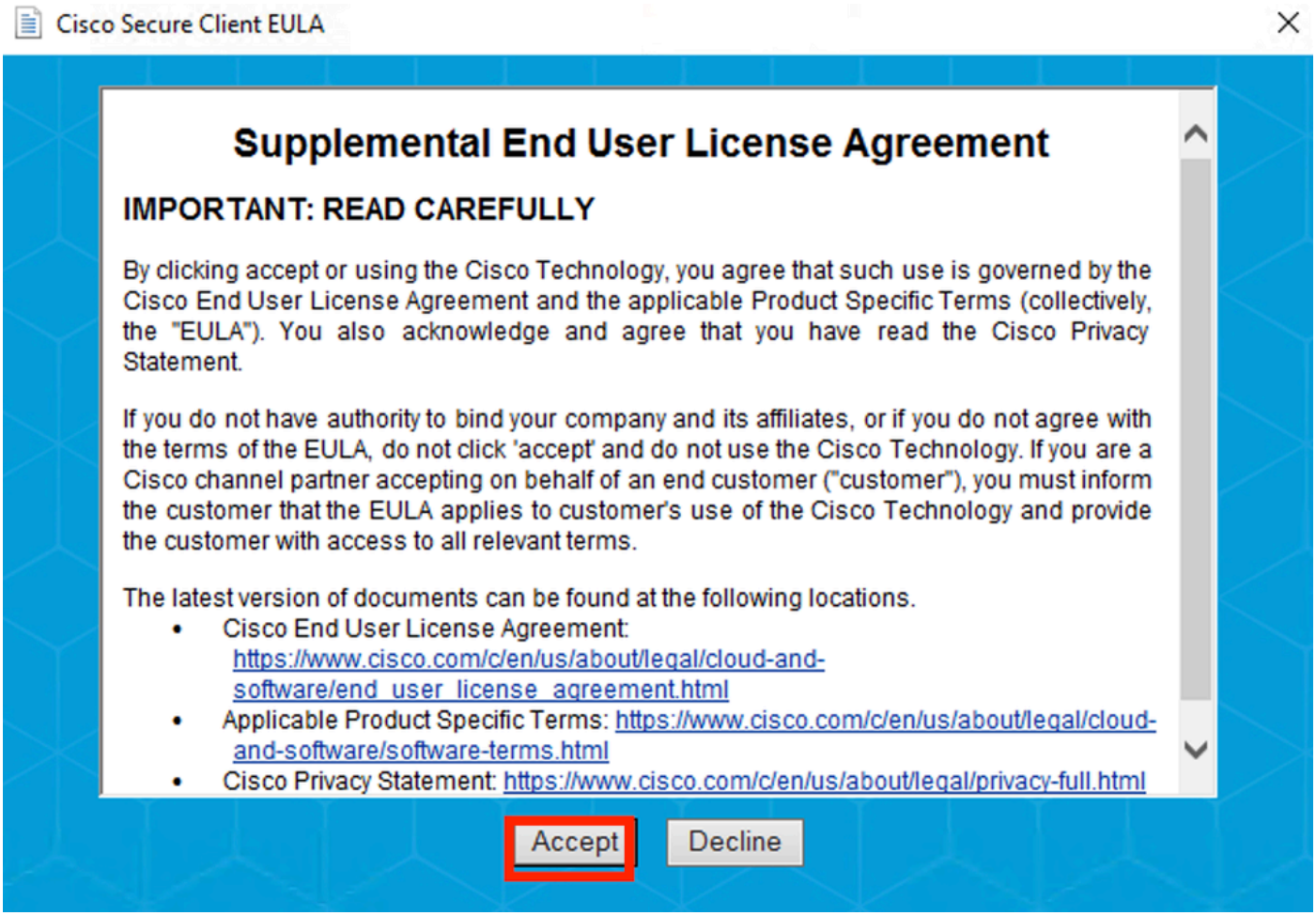
警告：如果使用Cisco Secure Client Wizard，VPN模块会自动安装，并在GUI中隐藏。如果未安装VPN模块，则NAM不起作用。如果使用单个MSI文件或不同的安装方法，请确保安装VPN模块。



安装选择器

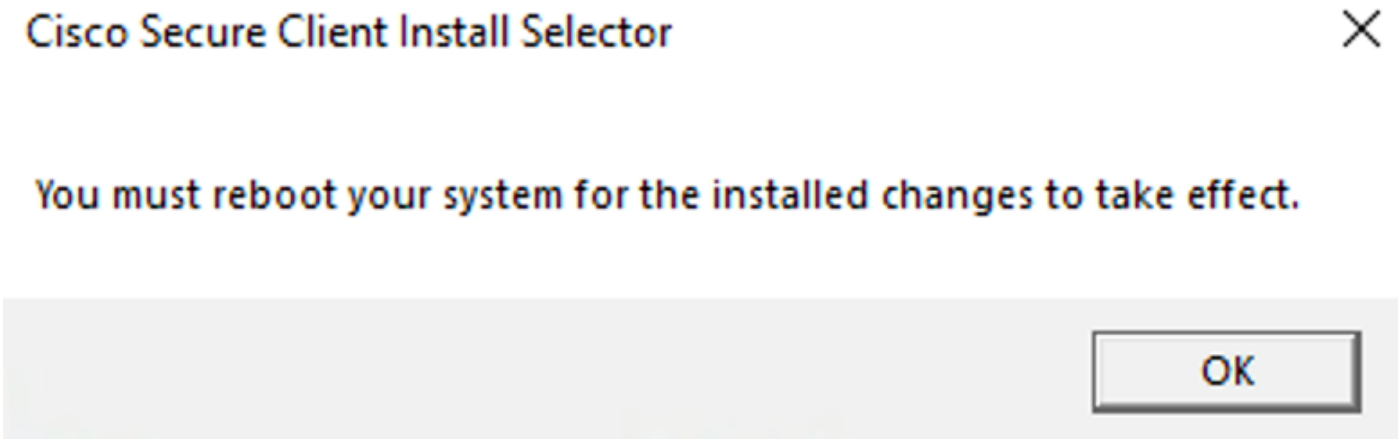
6.单击Install Selected。

7.接受EULA。



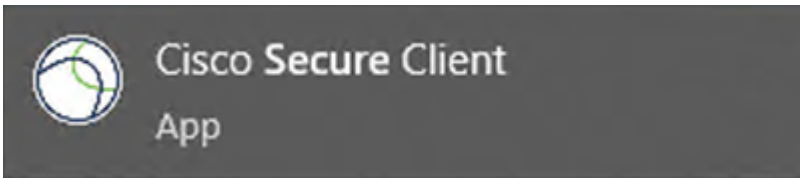
*EULA*窗口

8.安装NAM后需要重新启动。



重新启动要求窗口

9.安装后，可从Windows搜索栏找到并打开它。

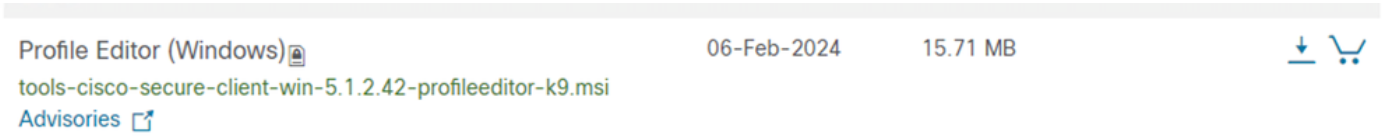


下载并安装安全客户端NAM配置文件编辑器

1.配置Dot1x首选项需要思科网络访问管理器配置文件编辑器。

2.从下载安全客户端的同一页上，找到Profile Editor选项。

3.本示例使用版本为5.1.2.42的选项。



配置文件编辑器

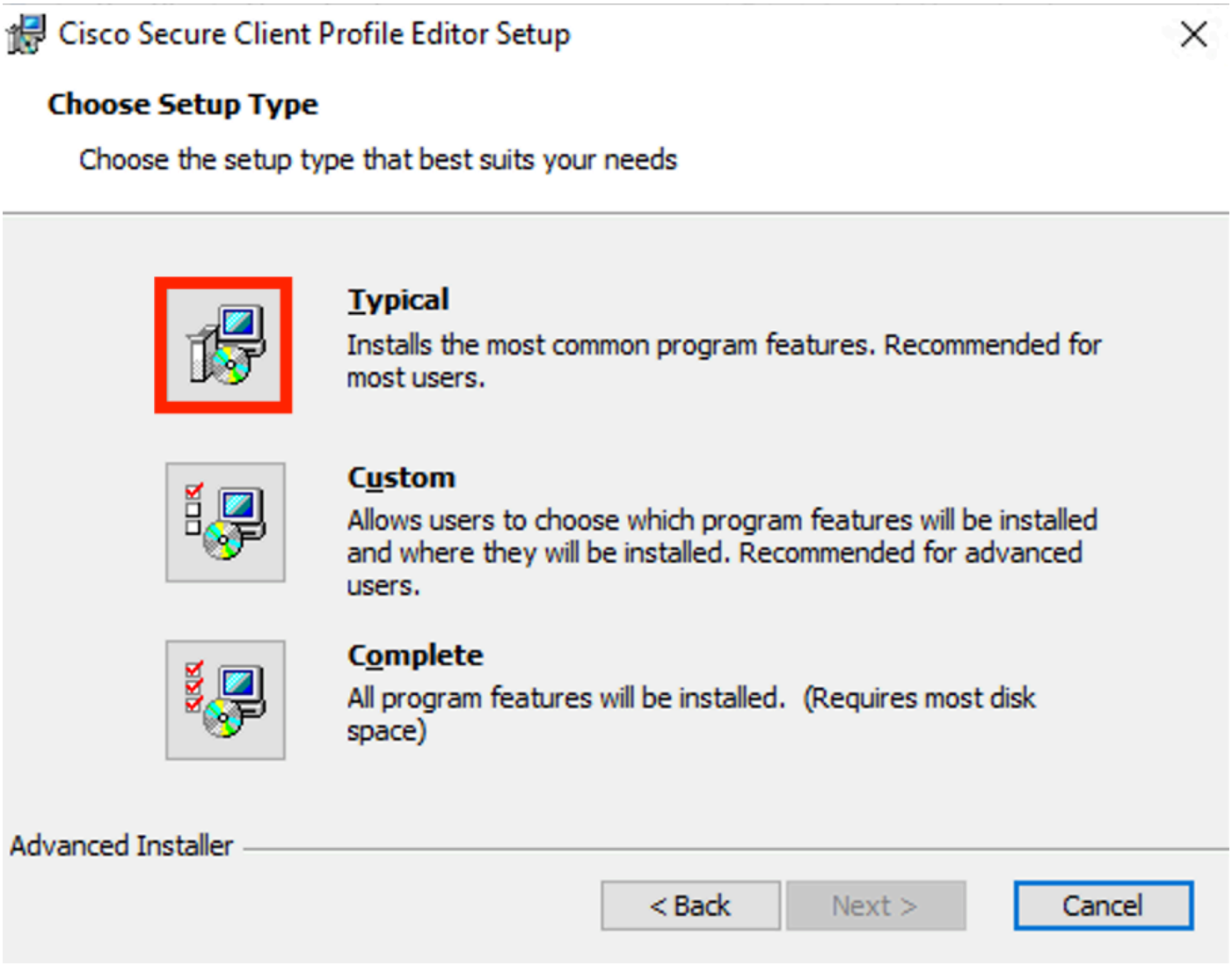
4.下载后，继续安装。

5.运行msi文件。

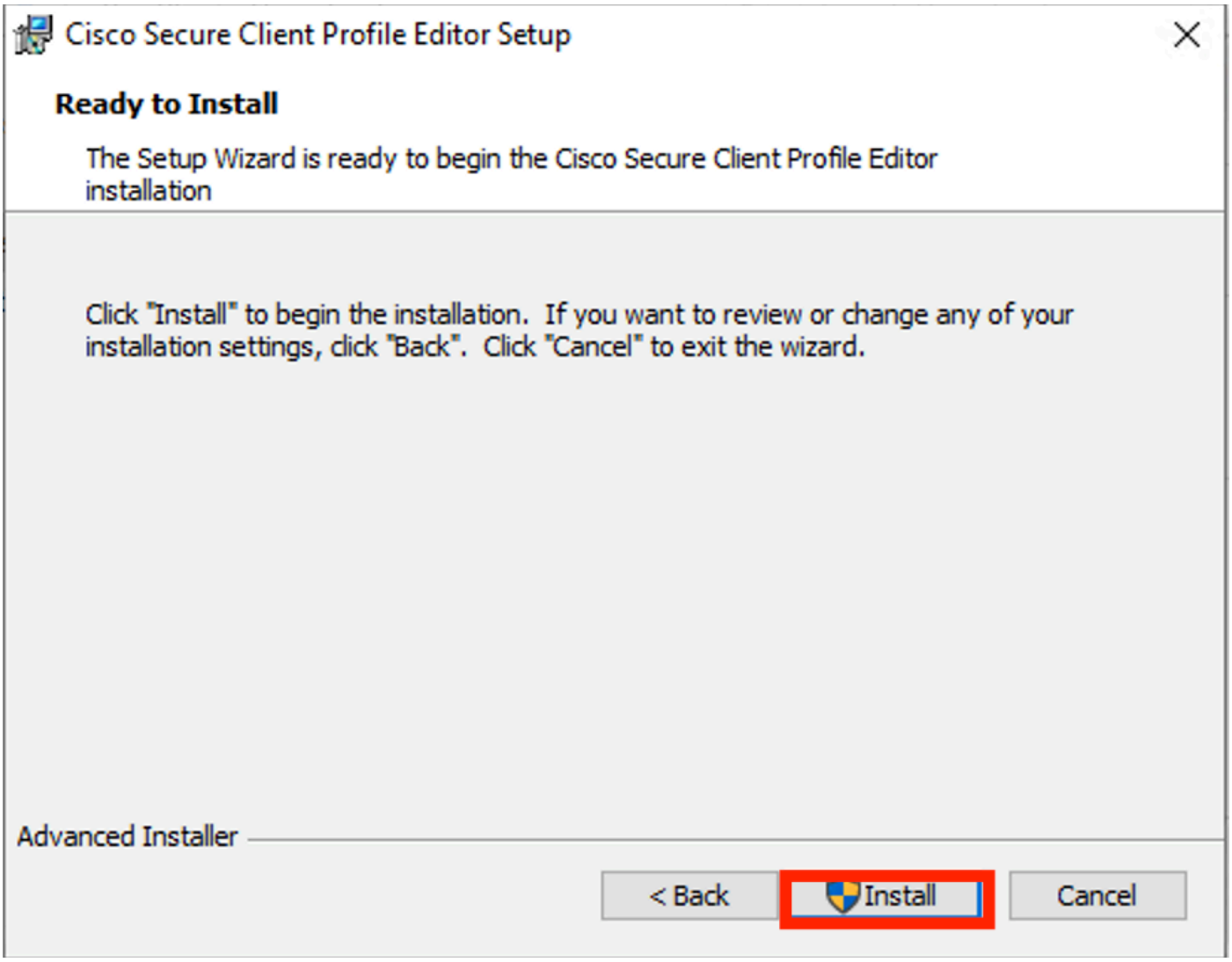


配置文件编辑器设置窗口

6.使用Typical设置选项。

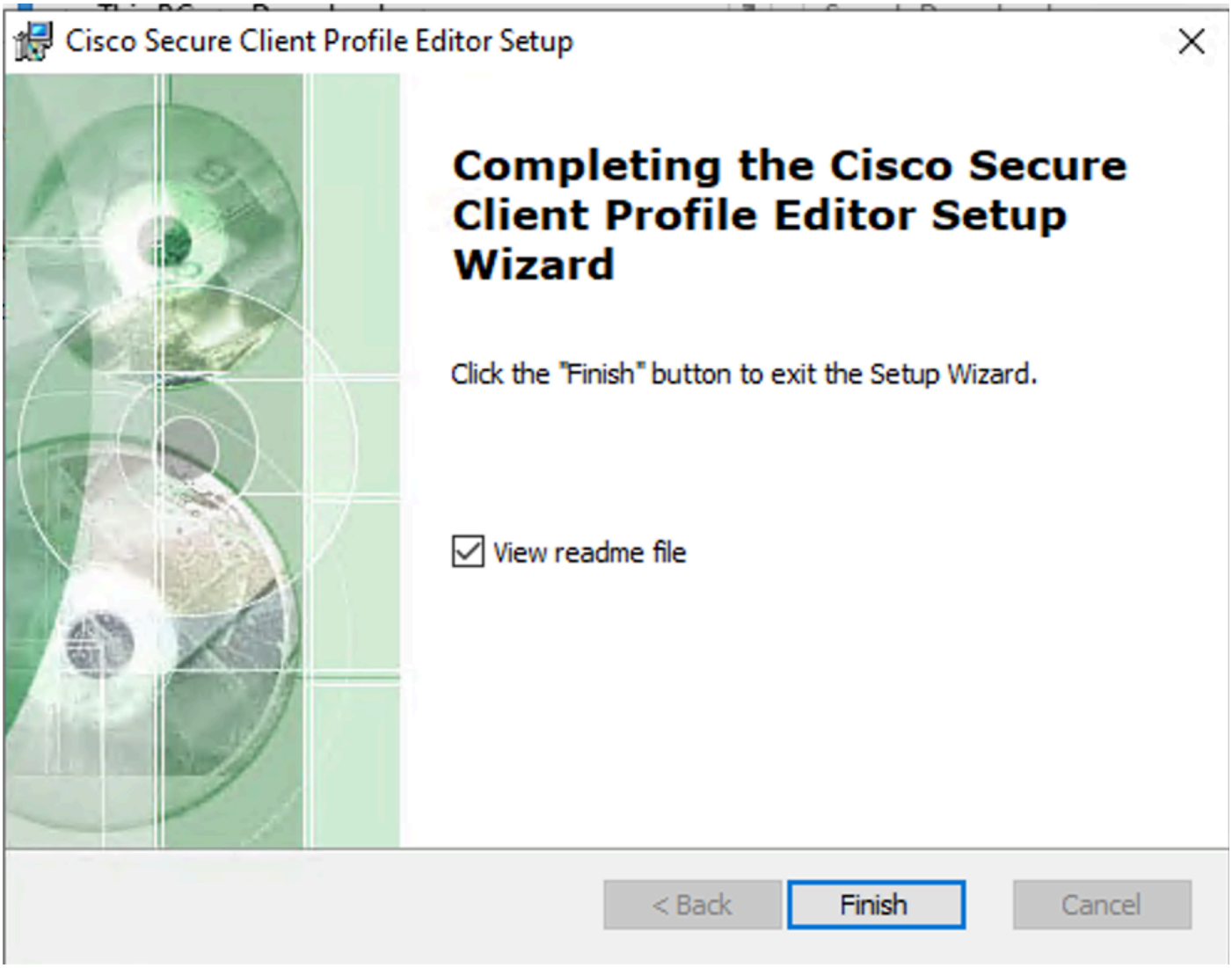

Cisco Secure Client Profile Editor Setup
Choose Setup Type
Choose the setup type that best suits your needs
Typical
Installs the most common program features. Recommended for most users.
Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.
Complete
All program features will be installed. (Requires most disk space)
Advanced Installer
< Back
Next >
Cancel

配置文件编辑器设置


Cisco Secure Client Profile Editor Setup
Ready to Install
The Setup Wizard is ready to begin the Cisco Secure Client Profile Editor installation
Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.
Advanced Installer
< Back
Install
Cancel

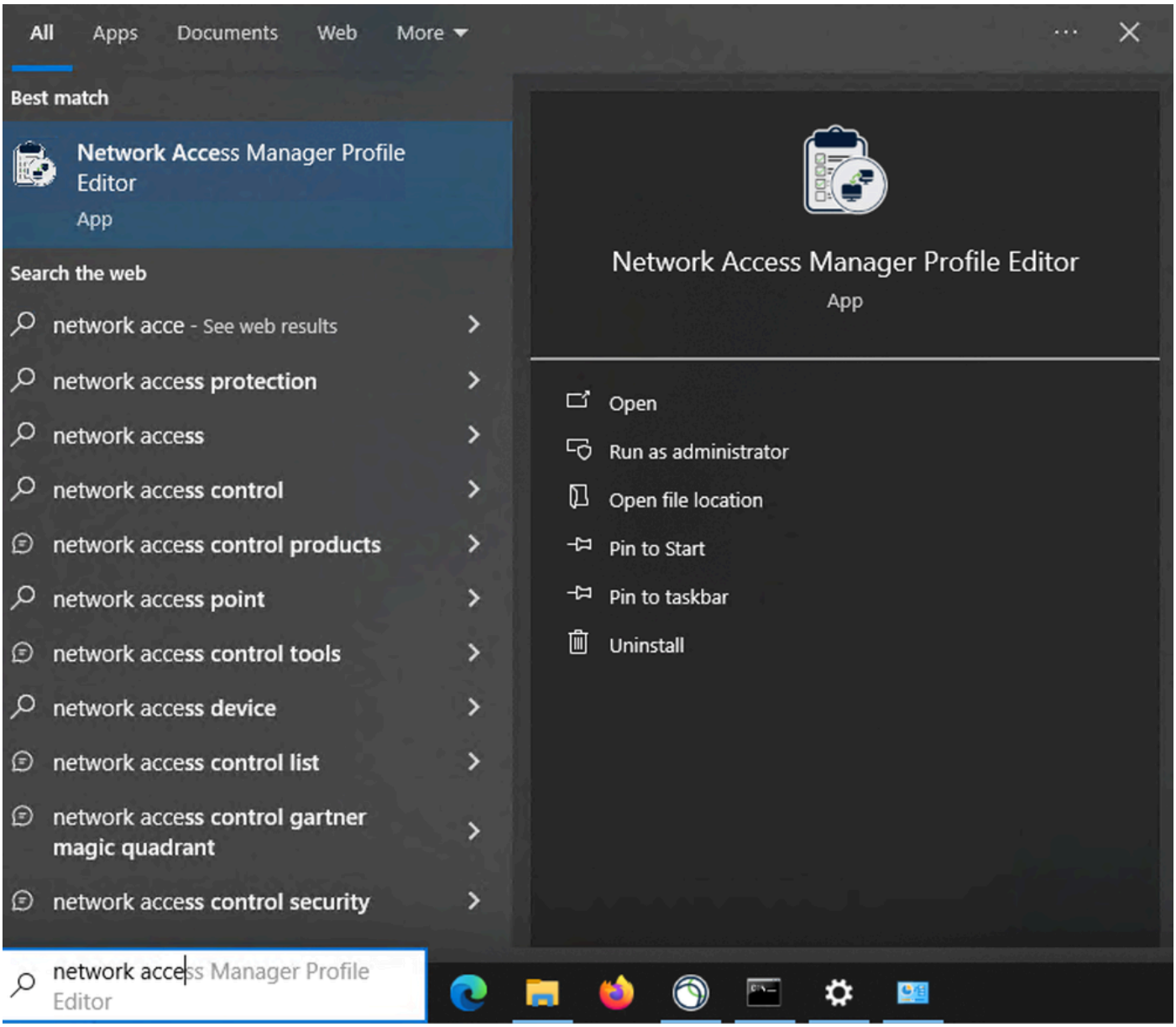
安装窗口

7.单击完成。



配置文件编辑器设置结束

8.安装后，从搜索栏打开网络访问管理器配置文件编辑器。



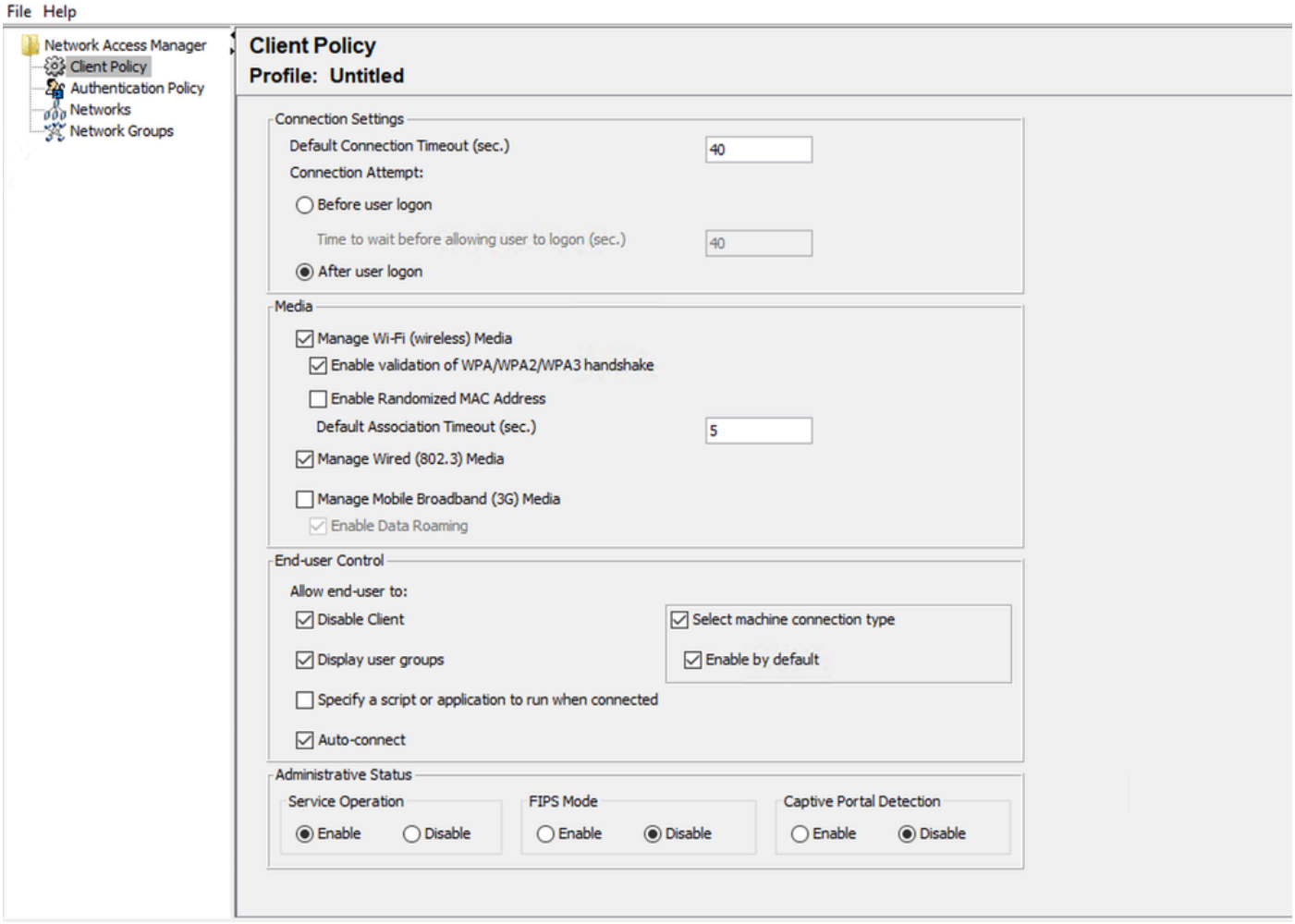
搜索栏上的NAM配置文件编辑器

9.网络访问管理器和配置文件编辑器的安装已完成。

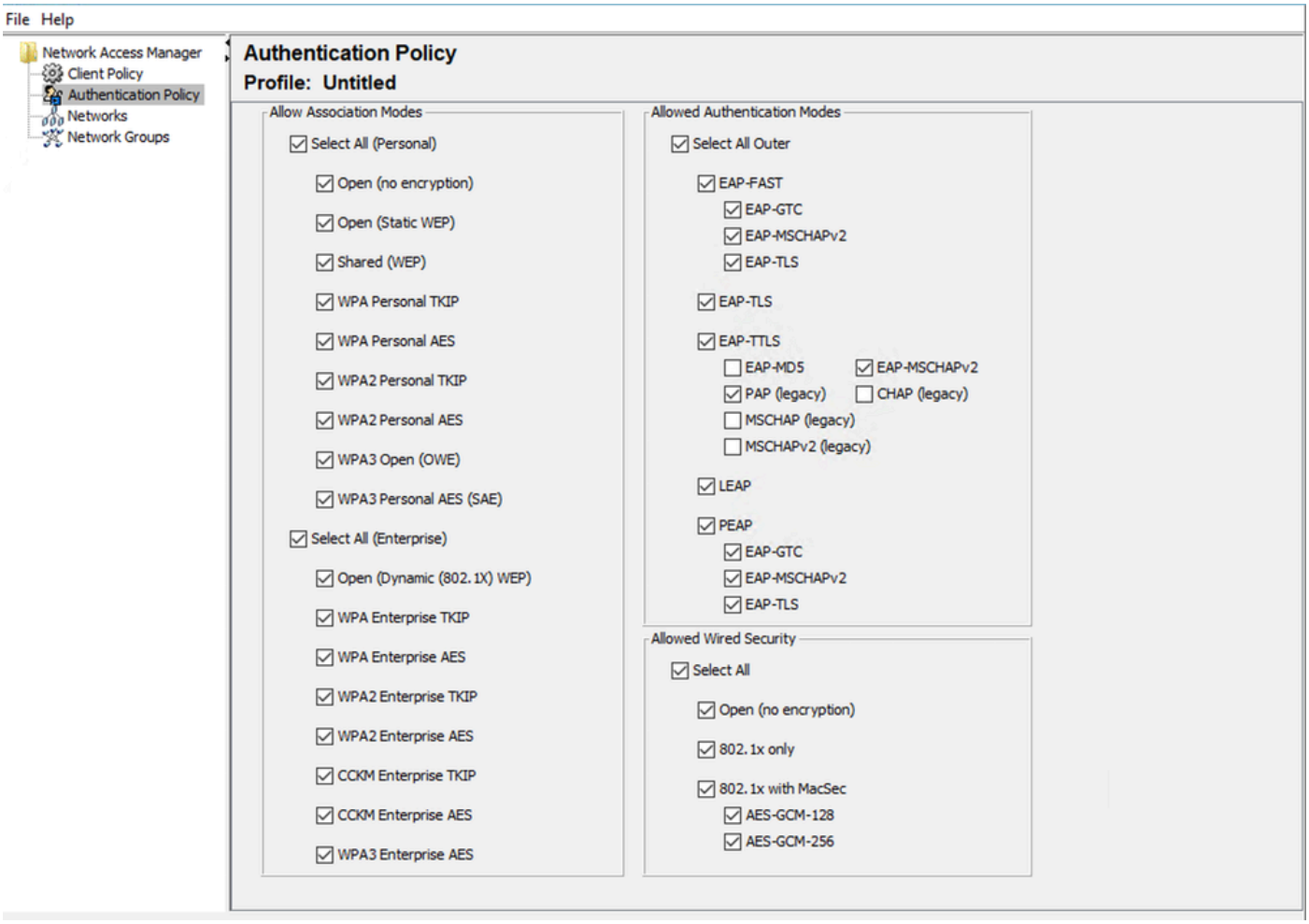
常规默认配置

1.本文中介绍的所有方案都包含以下配置：

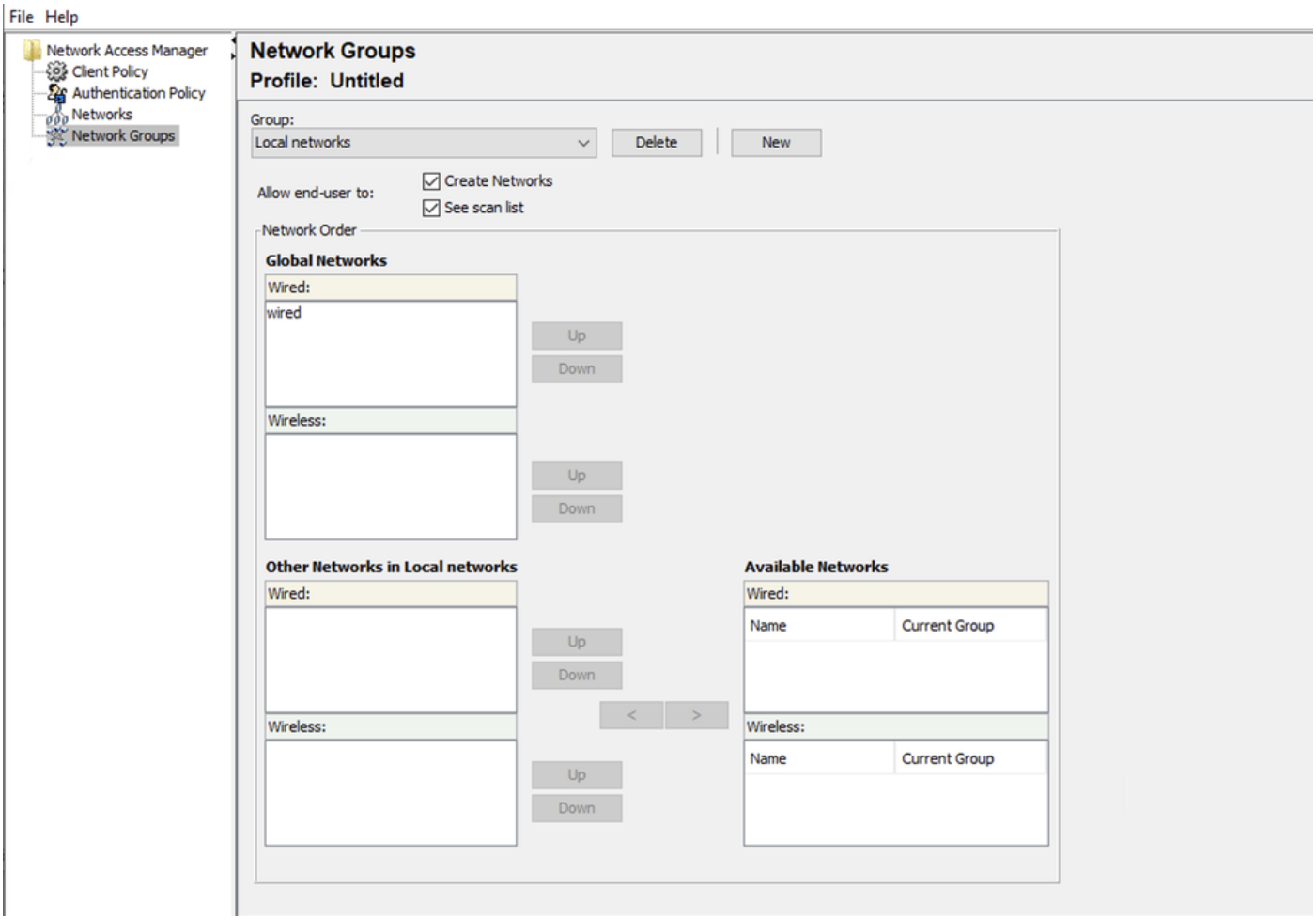
- 客户端策略
- 验证策略
- 网络组



*NAM*配置文件编辑器客户端策略



*NAM*配置文件编辑器身份验证策略



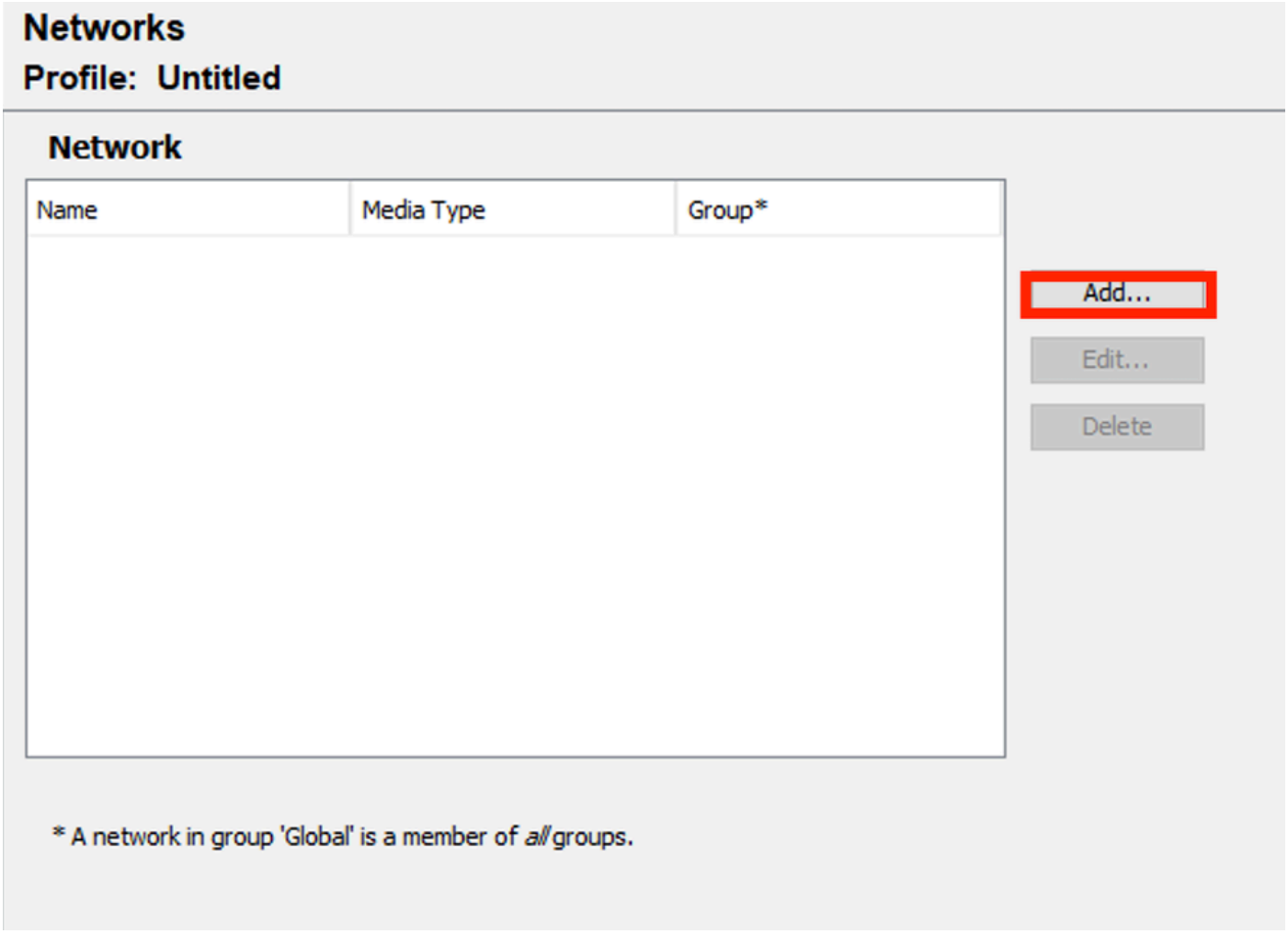
“网络组”选项卡

情形 1：为PEAP(MS-CHAPv2)用户身份验证配置安全客户端NAM请求方

1.定位至网络部分。

2.可以删除默认网络配置文件。

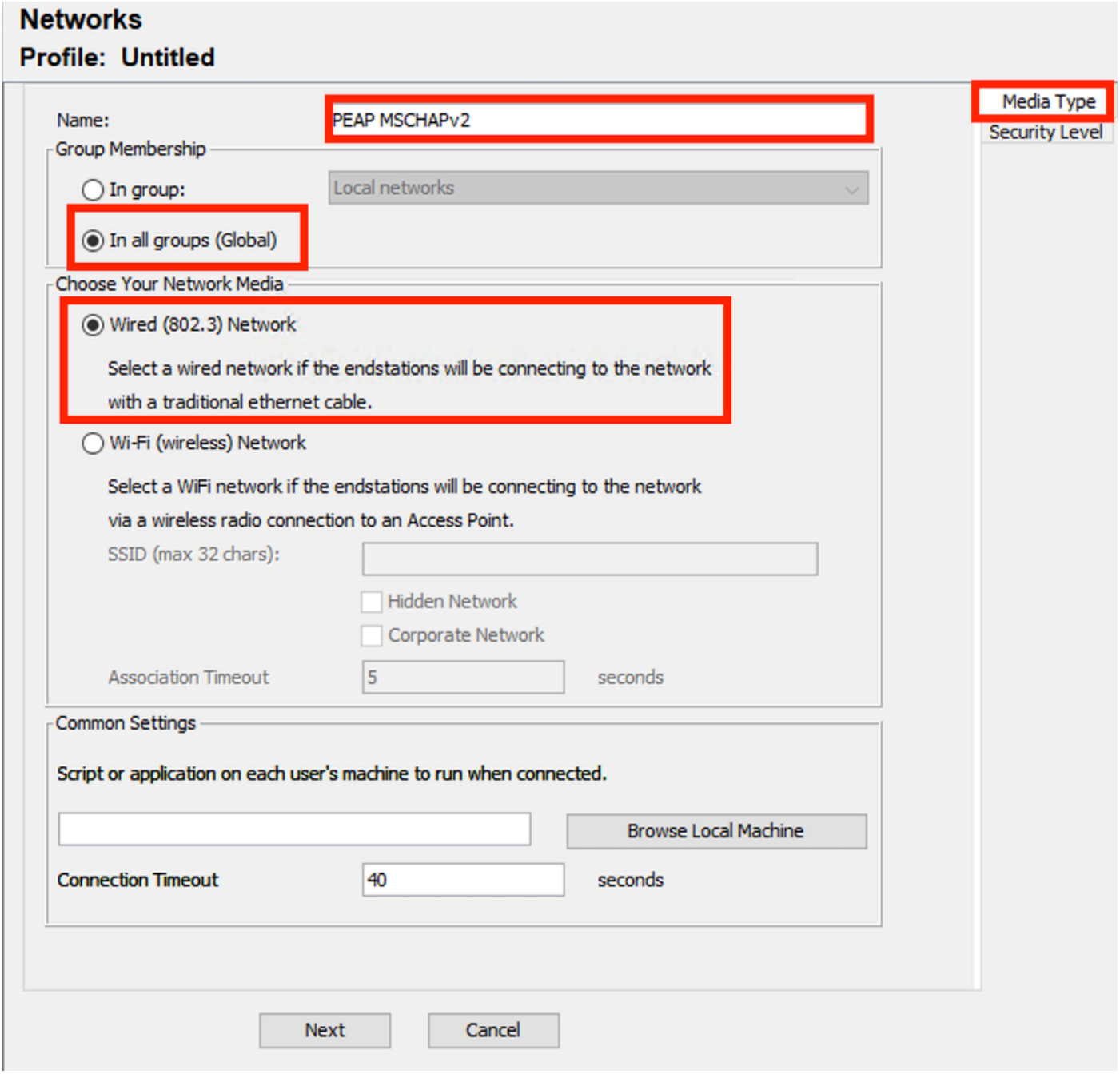
3.单击Add。



网络配置文件创建

4.命名网络配置文件。

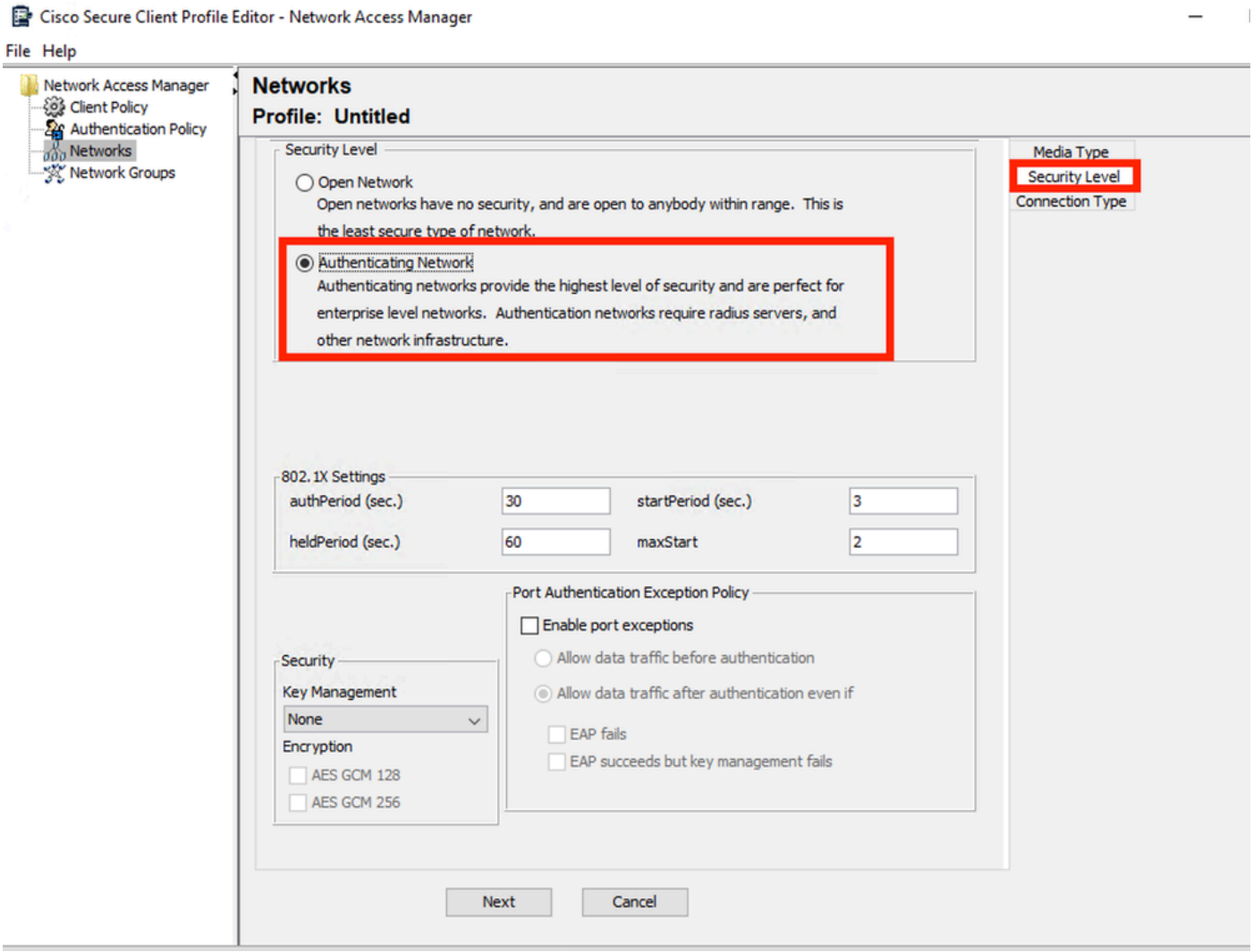
5.选择Global作为组成员资格。选择Wired Network介质。



Network Profile Media Type部分

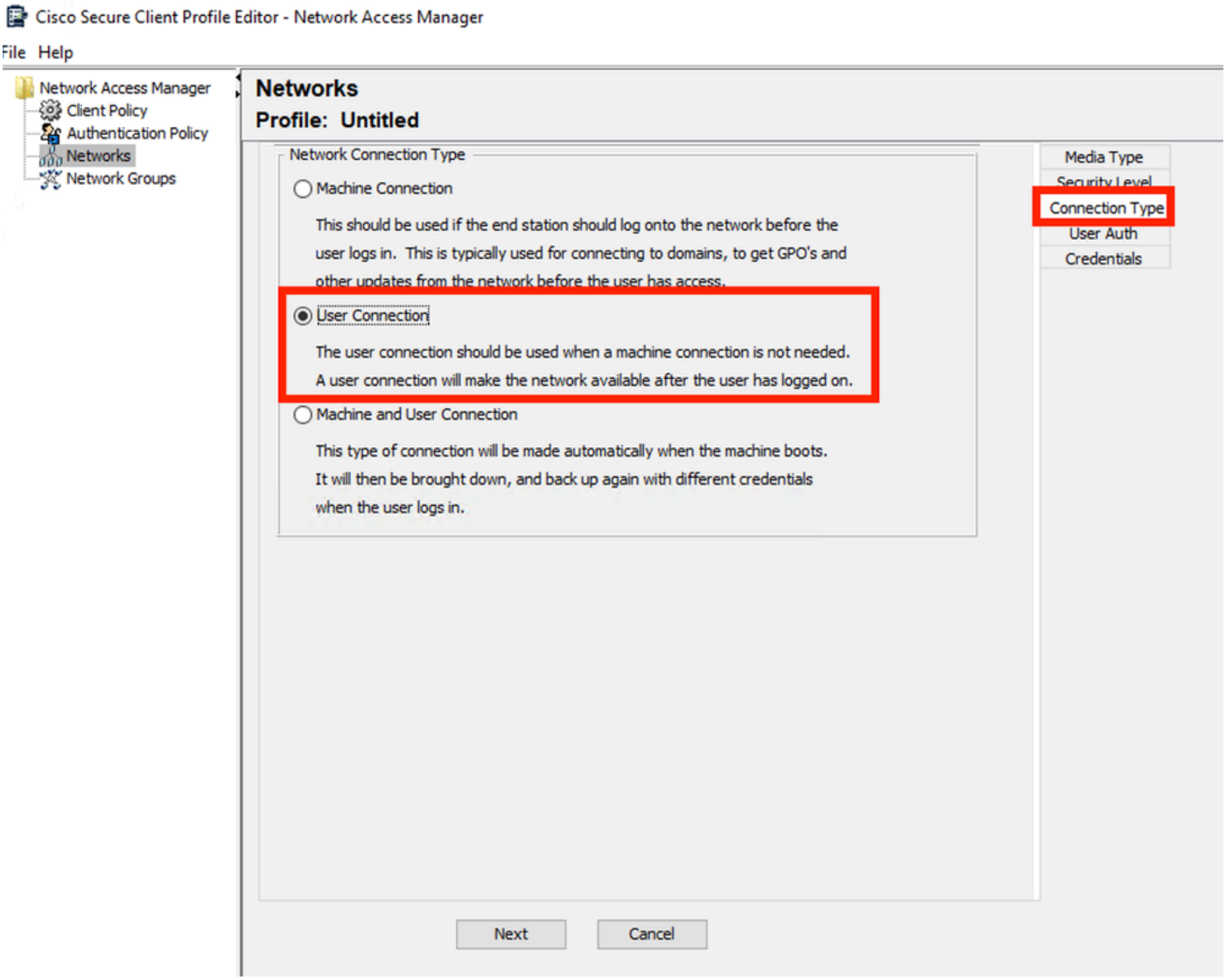
6.单击下一步。

7.选择Authenticating Network，并为Security Level部分中的其余选项使用默认值。



网络配置文件安全级别

8.单击下一步继续执行连接类型部分。

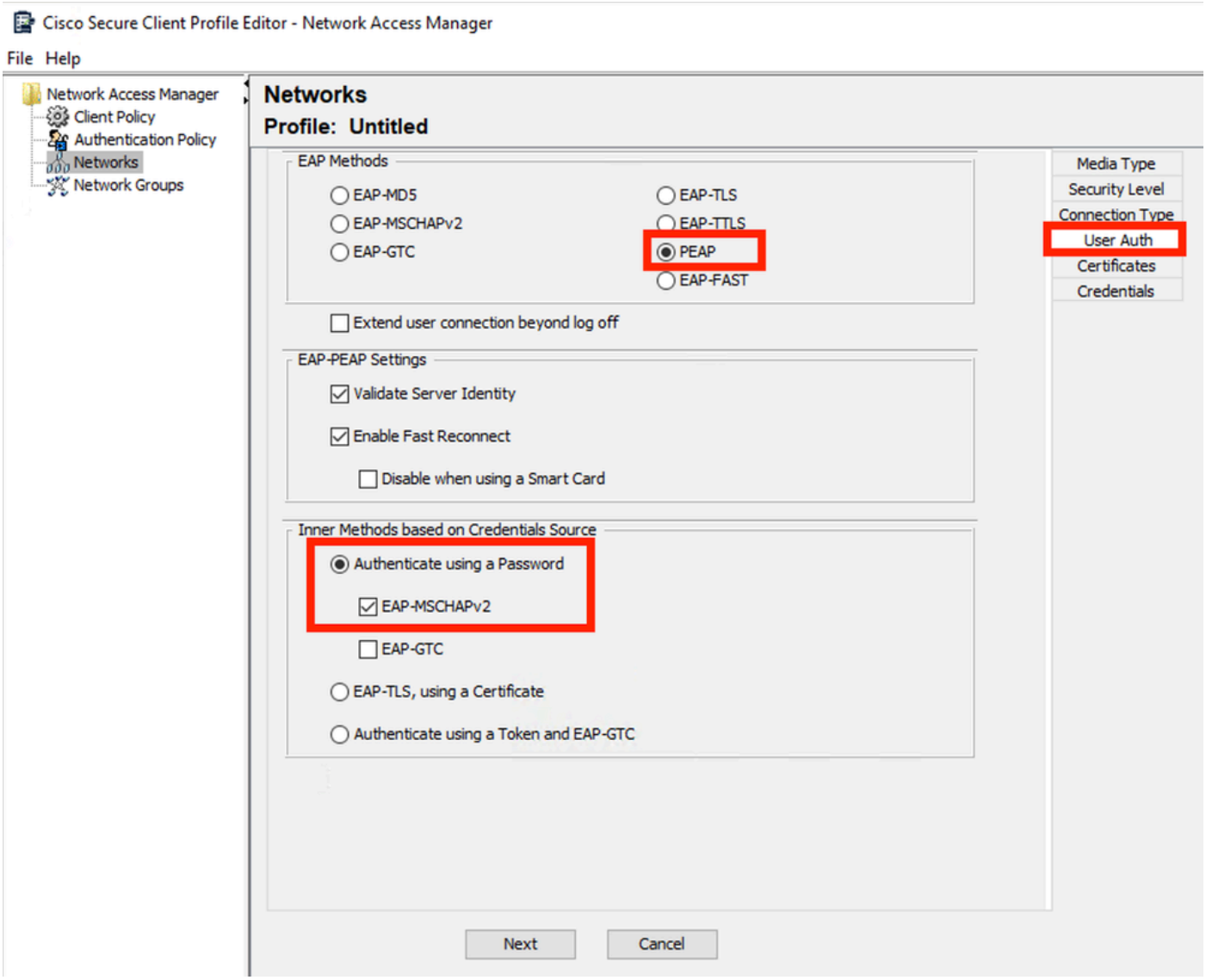


网络配置文件连接类型

9.选择User Connection(用户连接)连接类型。

10.单击下一步继续执行用户身份验证部分，此部分现在可用。

11.选择PEAP作为常规EAP方法。



网络配置文件用户身份验证

12.请勿更改EAP-PEAP设置中的默认值。

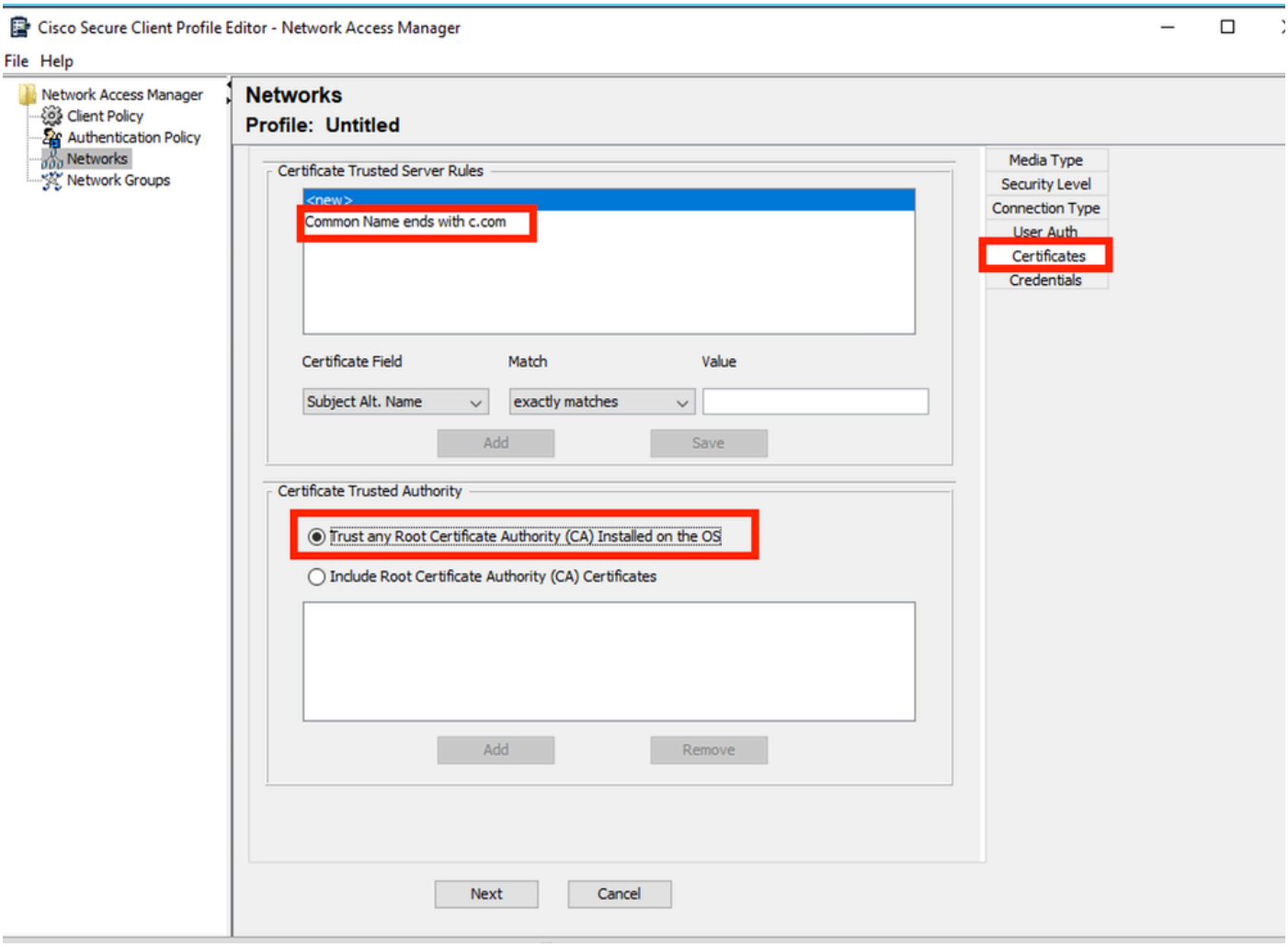
13.继续执行基于凭证源的内部方法部分。

14.从EAP PEAP存在的多个内部方法中，选择使用密码进行身份验证，然后选择EAP-MSCHAPv2。

15.单击下一步继续转到证书部分。

注意：在EAP-PEAP Settings中选择了Validate Server Identity选项，此时将显示Certificate部分。对于EAP PEAP，它使用服务器证书进行封装。

16.在证书部分中，使用证书受信任服务器规则，规则公用名以c.com结尾。此部分配置是指服务器在EAP PEAP流期间使用的证书。如果您的环境中使用了身份服务引擎(ISE)，则可以使用策略服务器节点EAP证书的公用名。

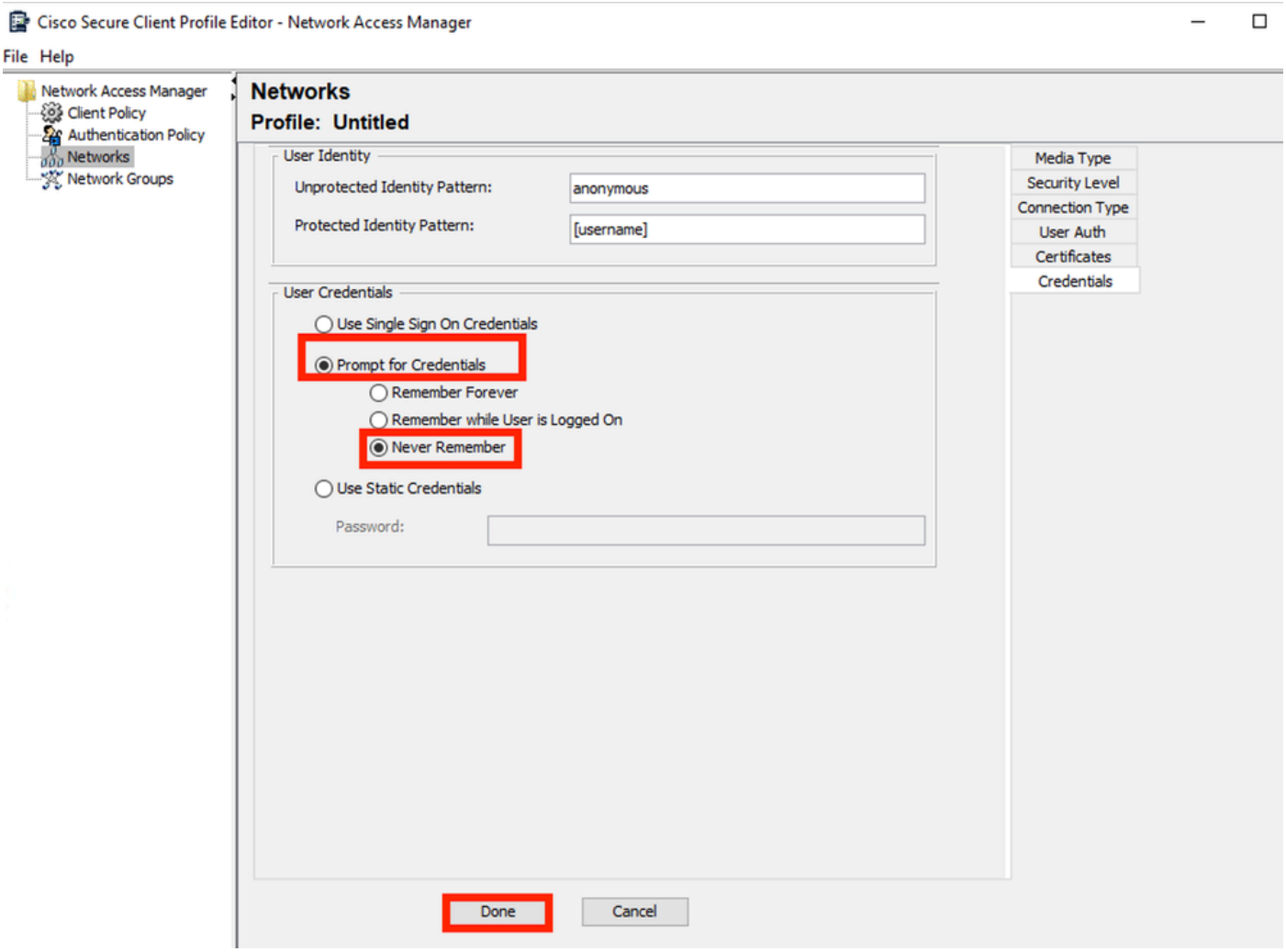


网络配置文件证书部分

17.可以在证书受信任颁发机构中选择两个选项。对于此方案，将使用操作系统上安装的Trust Any Root Certificate Authority(CA)选项，而不是添加签署RADIUS EAP证书的特定CA证书。

18.使用此选项，Windows设备信任由Manage User Certs程序Certificates — Current User > Trusted Root Certification Authorities > Certificates中包含的证书签名的任何EAP证书。

19.单击下一步。



Network Profile Credentials部分

20.在Credentials部分中，仅更改User Credentials部分。

21.选择提示输入凭证>从不记住选项，在每个身份验证中，选择身份验证的用户必须输入其凭证。

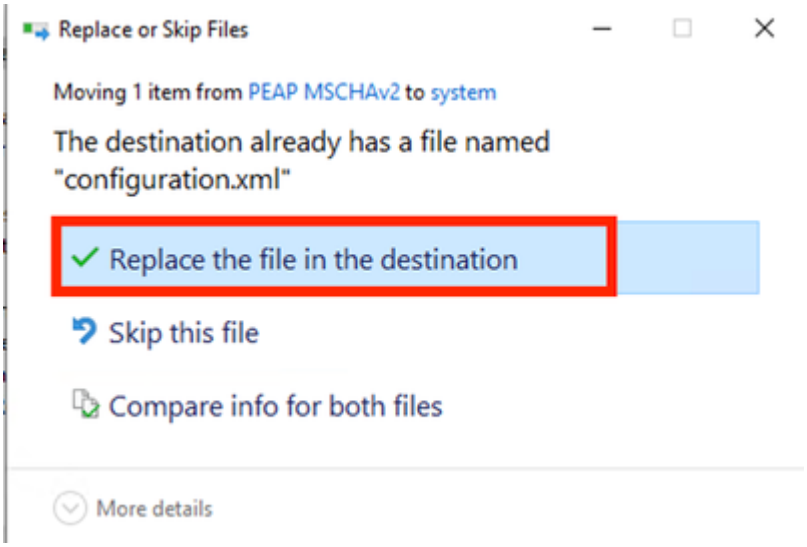
22.单击完成。

23.使用File > Save As选项将安全客户端网络访问管理器配置文件另存为configuration.xml。

24.为确保Secure Client Network Access Manage使用刚刚创建的配置文件，请将下一个目录中的configuration.xml文件替换为新文件：

C:\ProgramData\Cisco\Cisco安全客户端\网络访问管理器\system

注意：文件必须命名为configuration.xml，否则它不起作用。

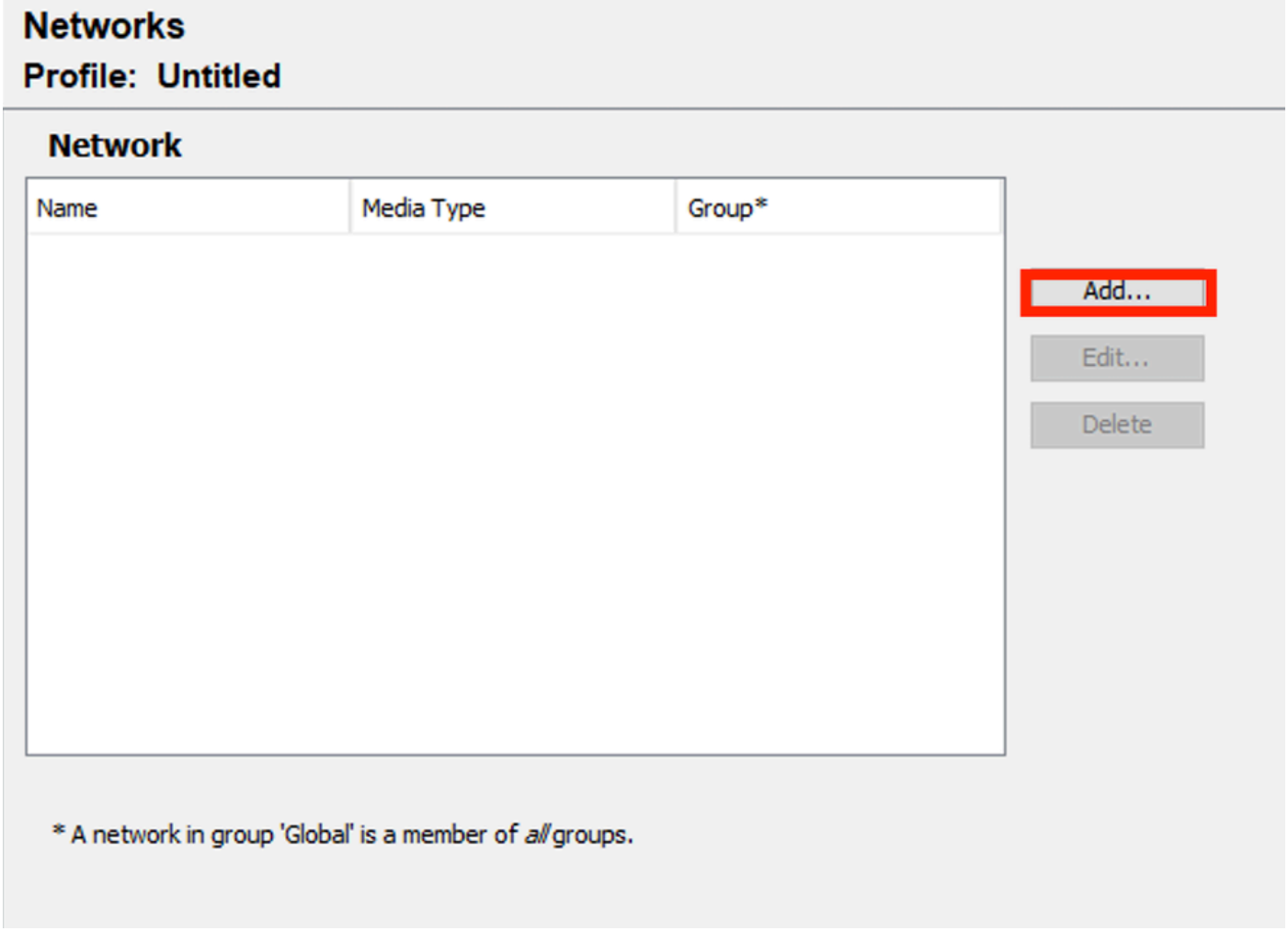


替换文件部分

方案 2：为EAP-FAST同步用户和机器身份验证配置安全客户端NAM请求方

1.打开NAM配置文件编辑器，然后导航至网络部分。

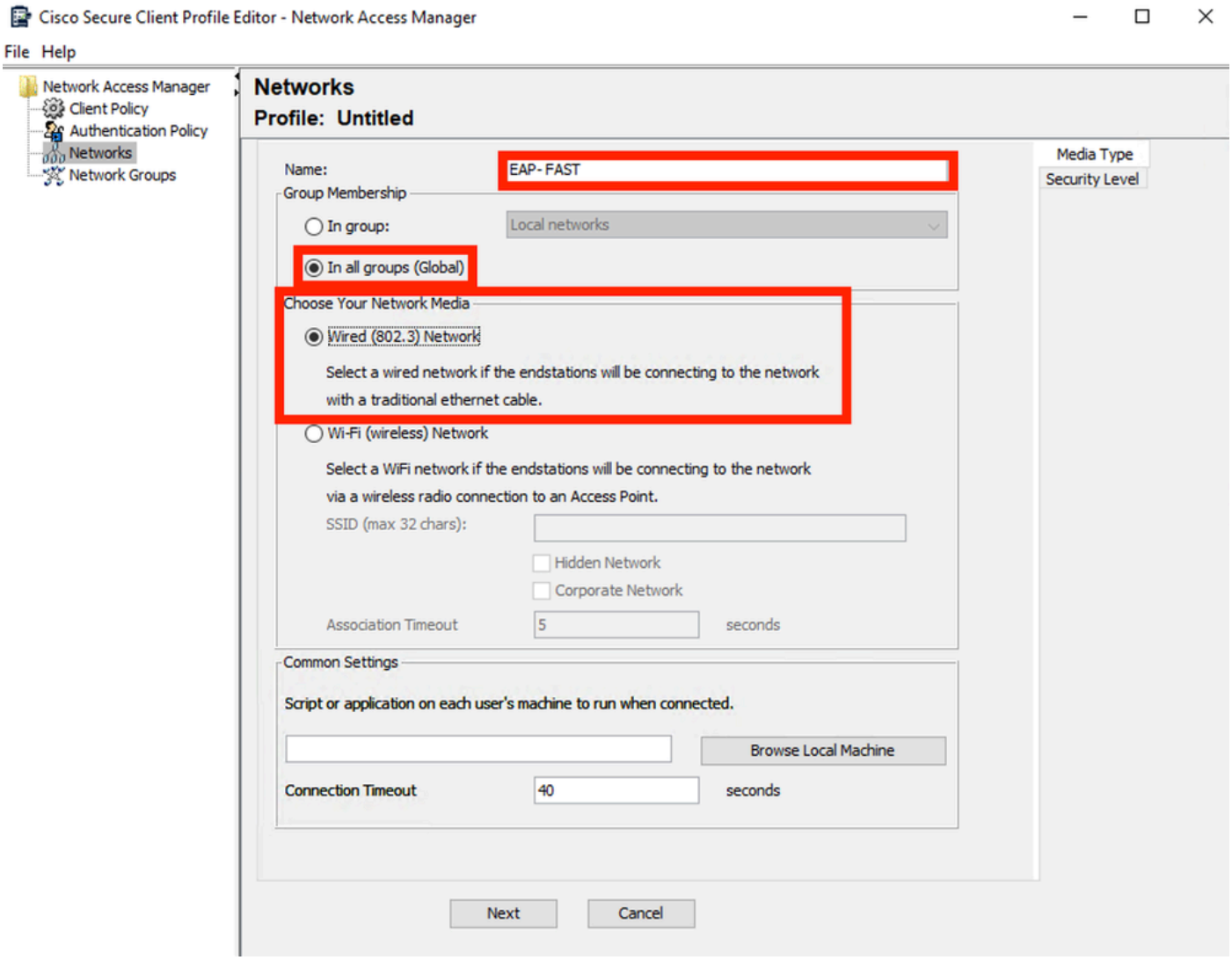
2.单击Add。



NAM配置文件编辑器网络选项卡

3.在网络配置文件中输入名称。

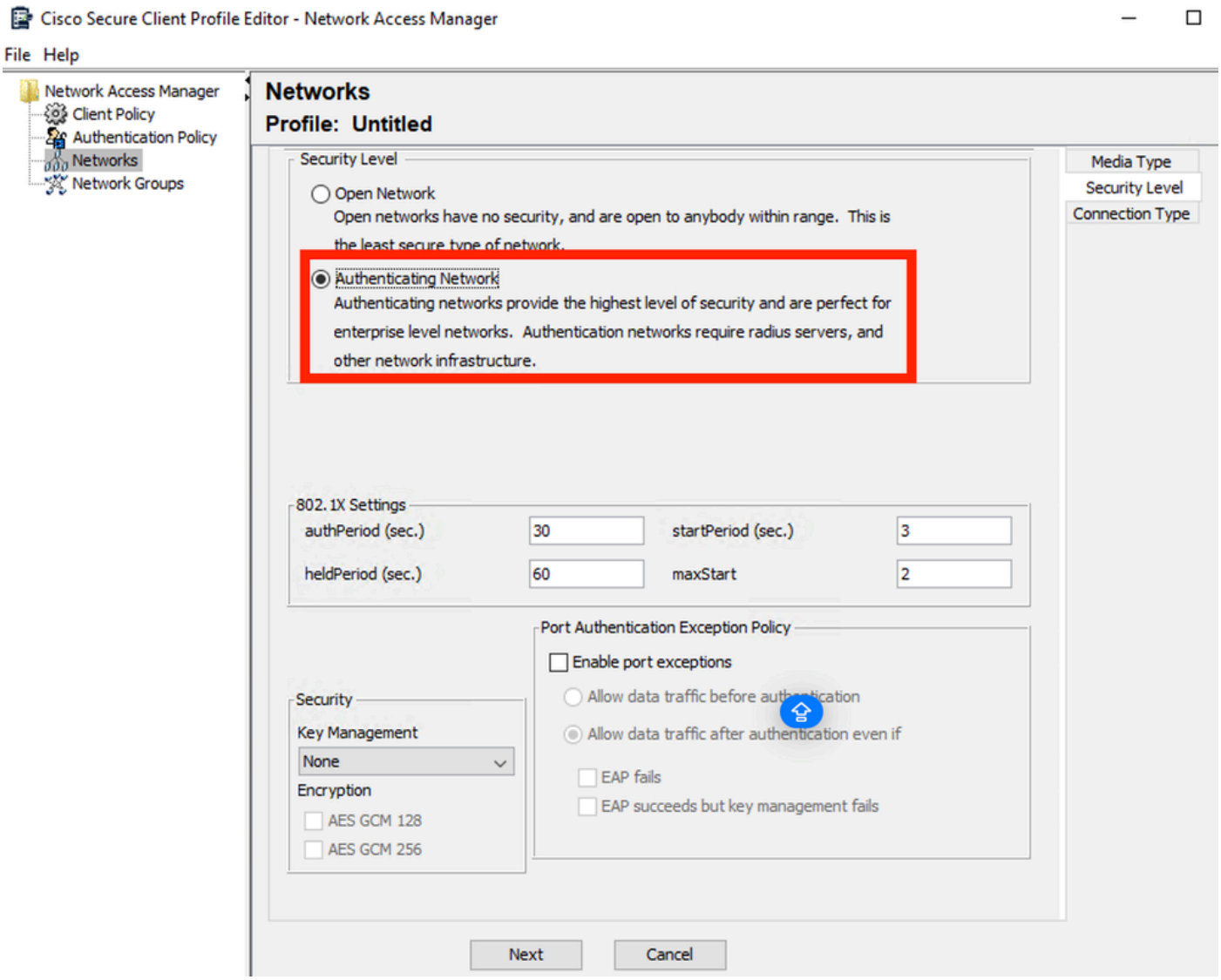
4.选择Global作为Group Membership。选择WiredNetwork Media。



Media Type部分

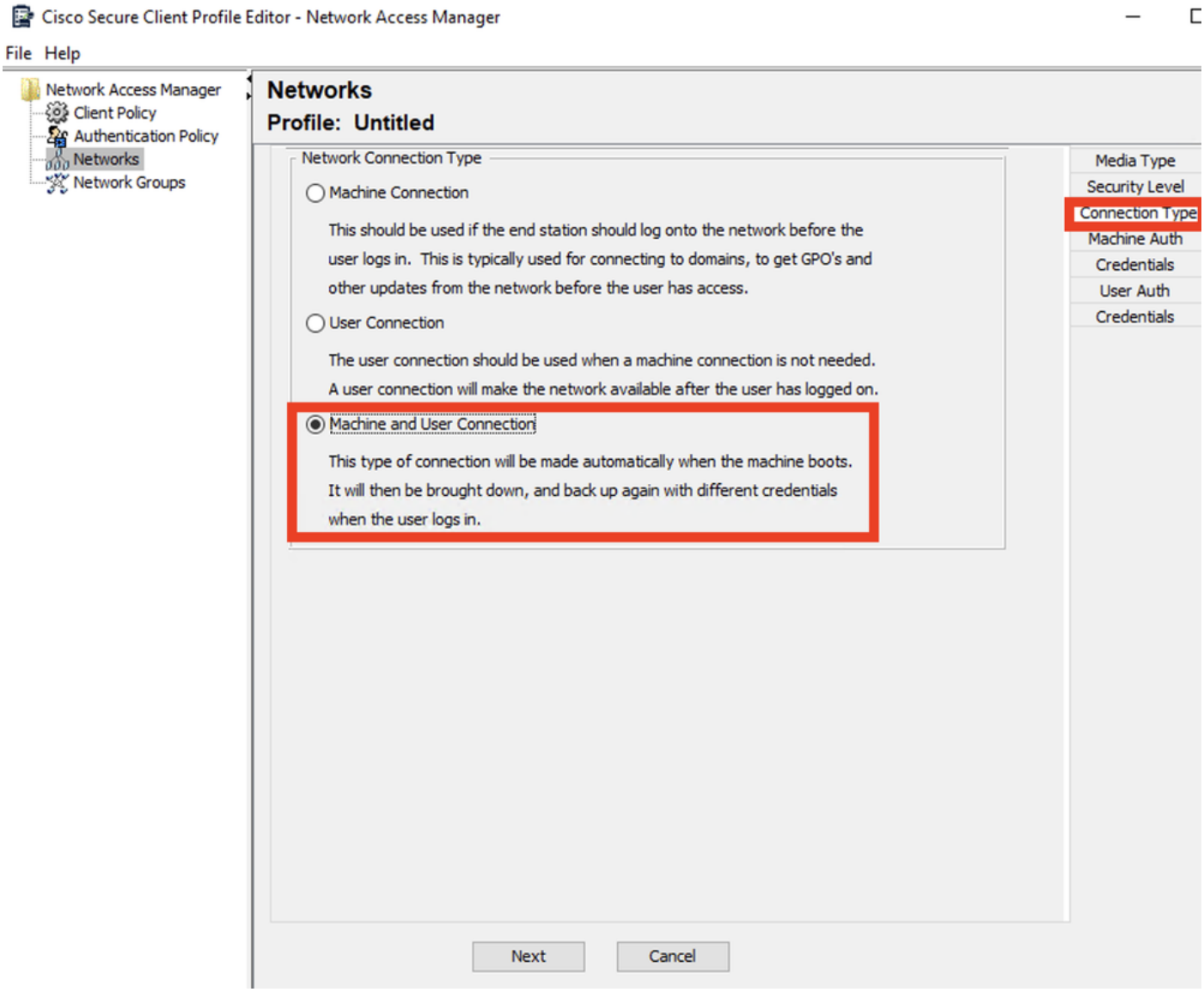
5.单击下一步。

6.选择Authenticating Network，不要更改本节中其余选项的默认值。



安全级别配置文件编辑器部分

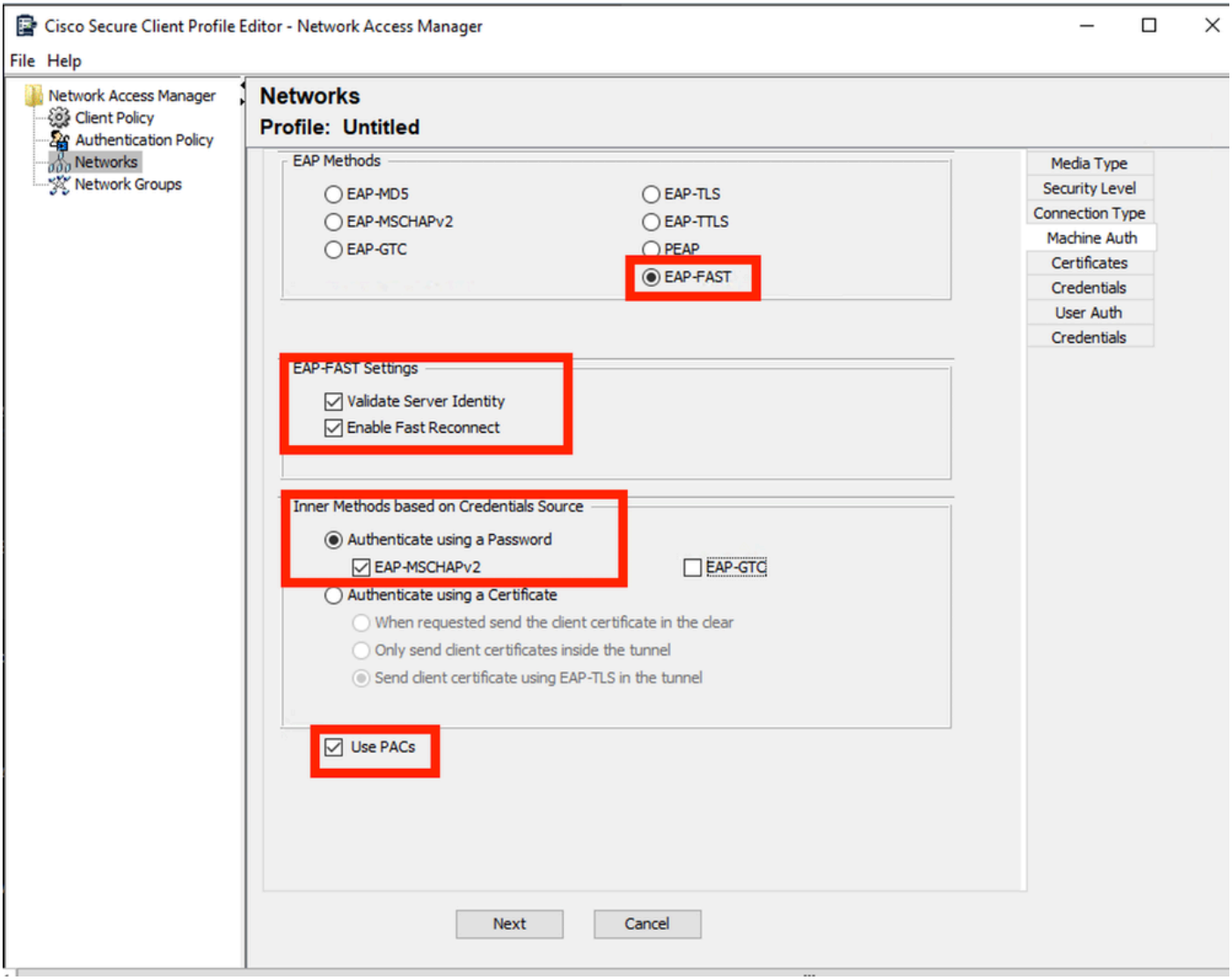
7.单击下一步继续执行连接类型部分。



Connection Type部分

8.通过选择第三个选项同时配置用户和计算机身份验证。

9.单击下一步。



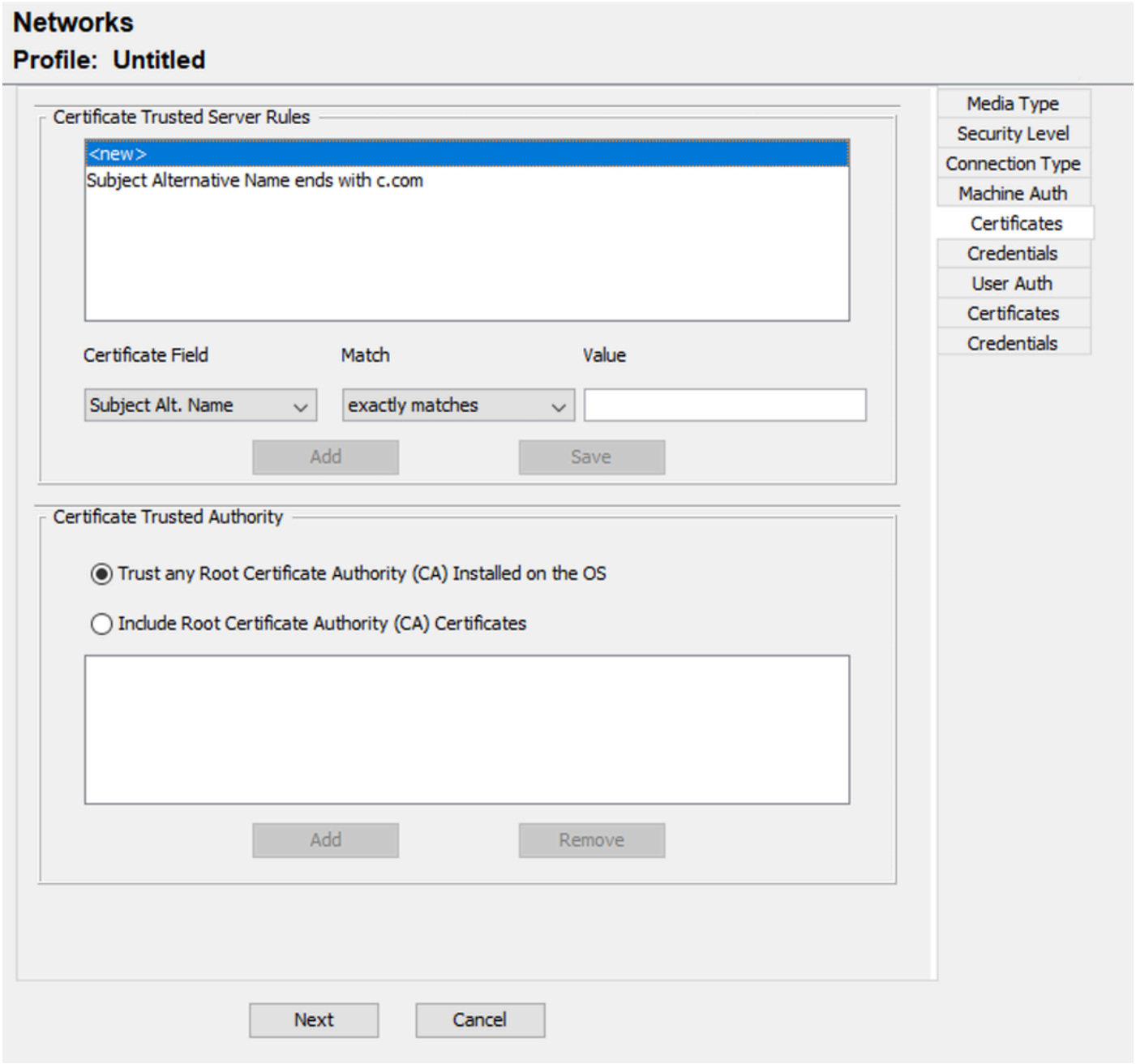
Machine Auth部分

10.在Machine Auth部分中，选择EAP-FAST作为EAP方法。请勿更改EAP FAST设置默认值。

11.对于Inner methods based on Credentials Source部分，选择Authenticate using a Password，然后选择EAP-MSCHAPv2作为方法。然后，选择使用PAC选项。

12.单击下一步。

13.在证书部分(证书受信任服务器规则)中，规则是以c.com结尾的公用名。此部分是指服务器在EAP PEAP流程期间使用的证书。如果您的环境中使用了身份服务引擎(ISE)，则可以使用策略服务器节点EAP证书的公用名称。

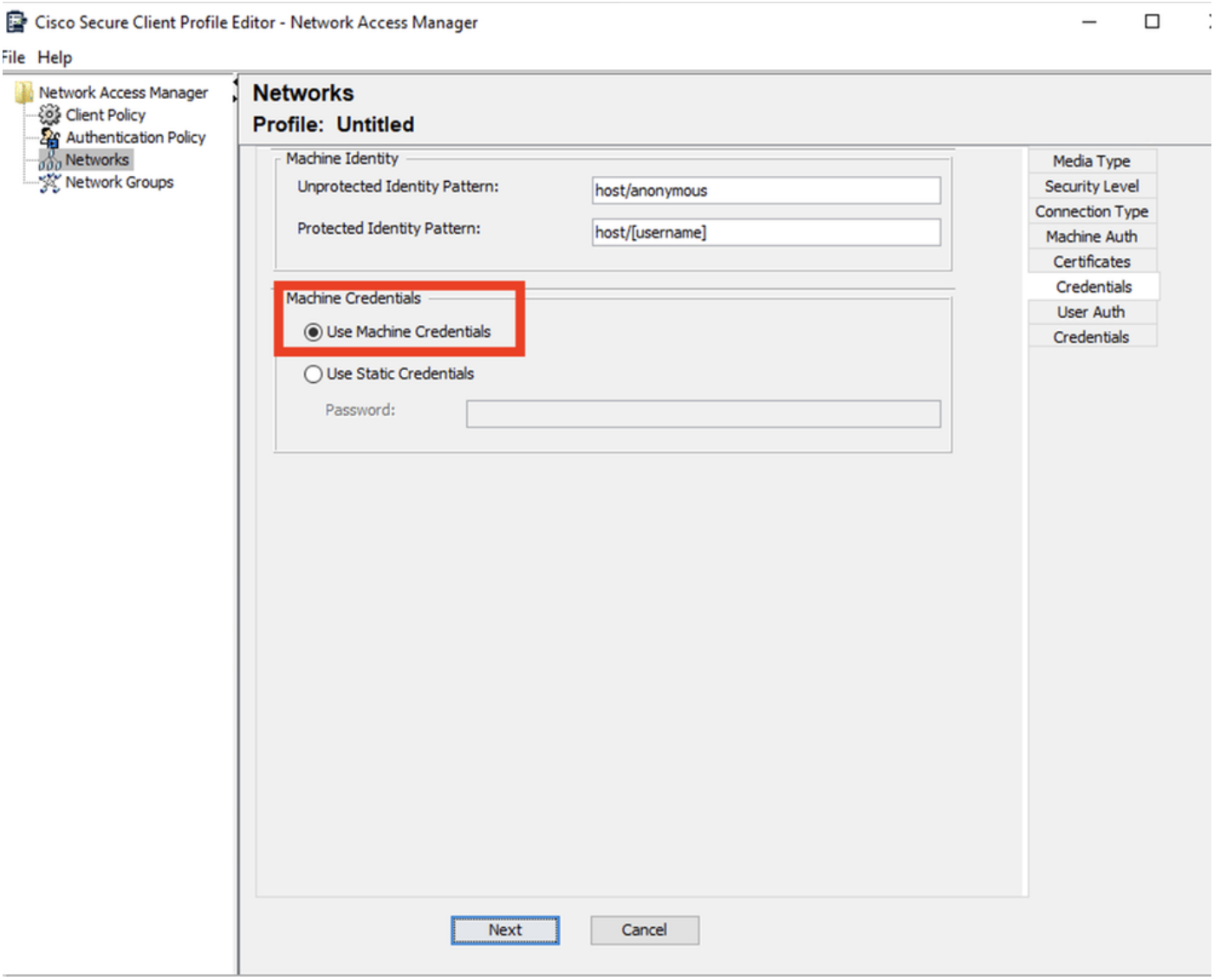


计算机身份验证服务器证书信任部分

14.可以在证书受信任颁发机构中选择两个选项。在此方案中，不是添加签署RADIUS EAP证书的特定CA证书，而是使用Trust Any Root Certificate Authority(CA)Installed on the OS选项。

15.使用此选项，Windows信任由Manage User Certs程序(Current User > Trusted Root Certification Authorities > Certificates)中包含的证书签名的任何EAP证书。

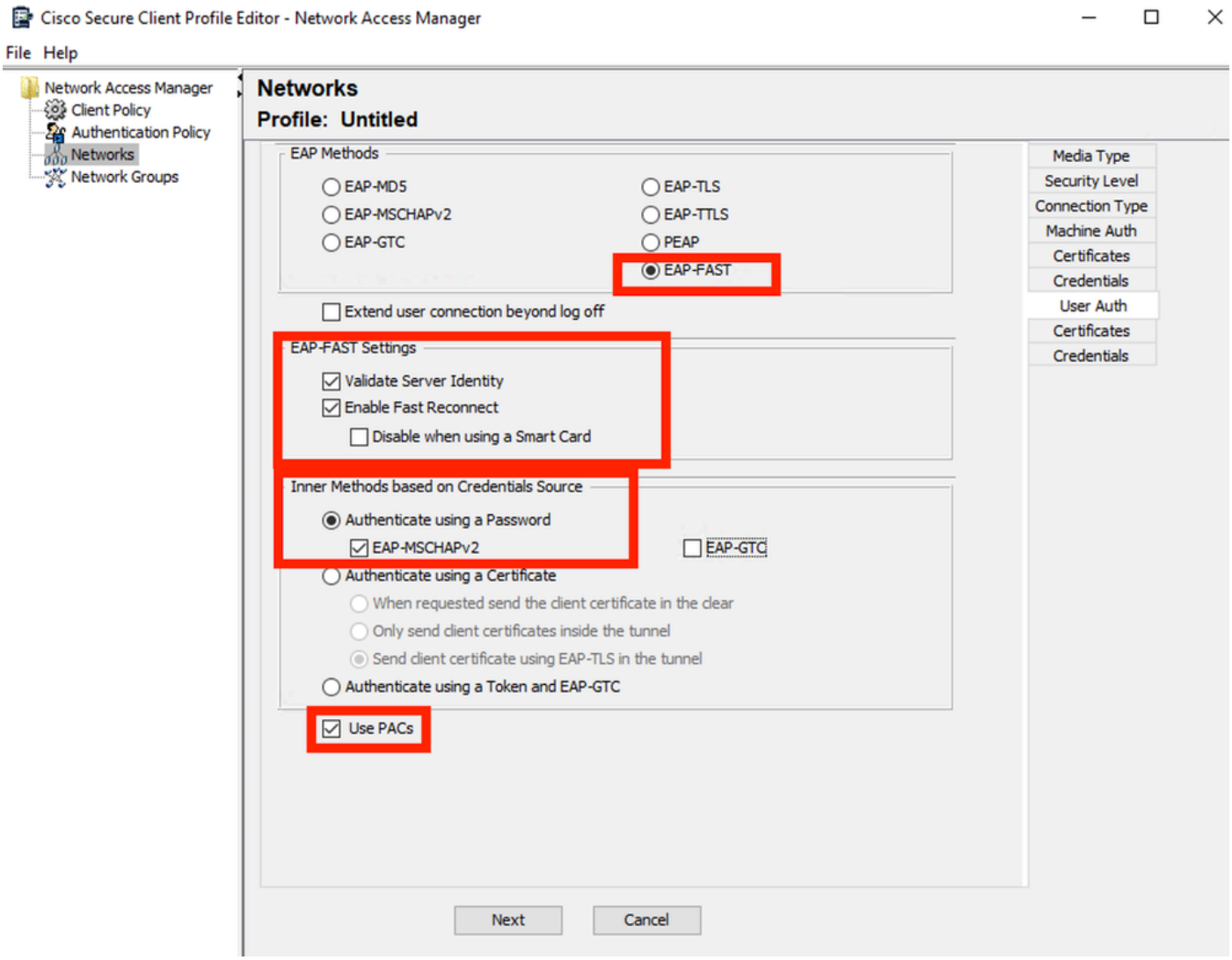
16.单击下一步。



Machine Auth Credentials部分

17.在计算机凭证部分中选择使用计算机凭证。

18.单击下一步。



User Authentication部分

19.对于User Auth，请选择EAP-FAST作为EAP方法。

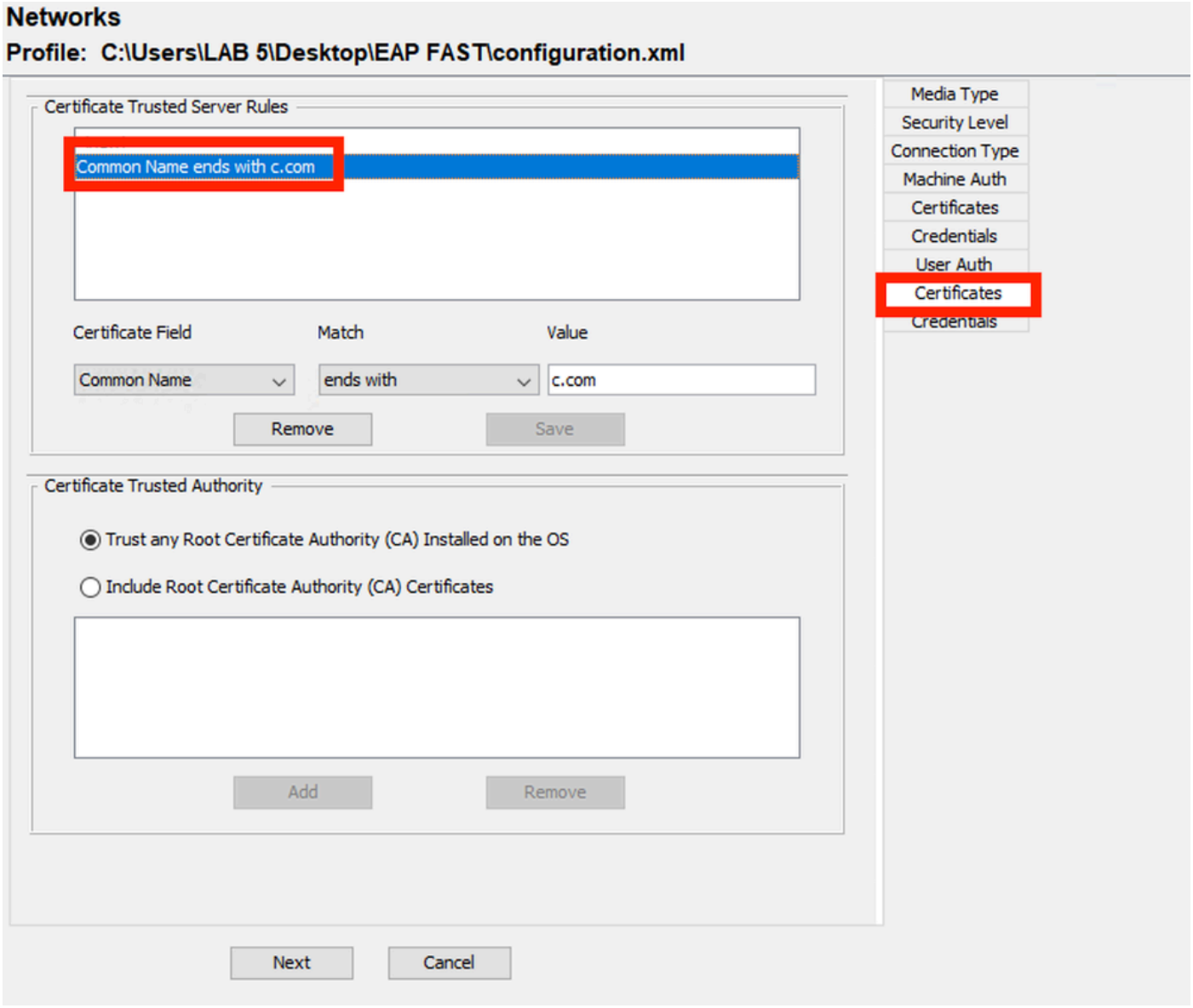
20.请勿更改EAP-FAST设置部分中的默认值。

21.对于“基于凭据的内部方法”来源部分，选择使用密码进行身份验证，然后选择EAP-MSCHAPv2作为方法。

22.选择使用PAC。

23.单击下一步。

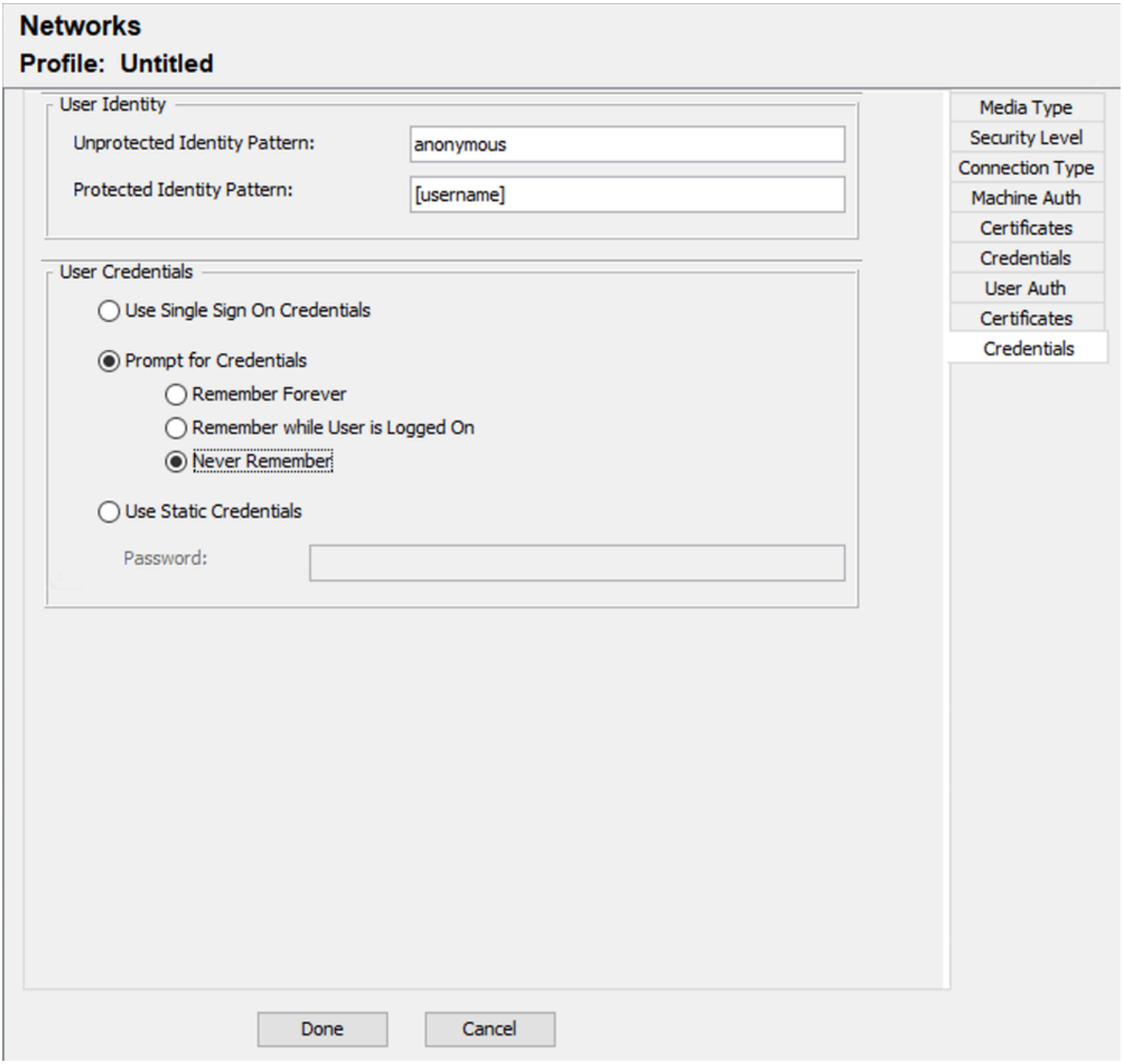
24.在证书部分的证书受信任服务器规则中，规则为公用名称，以c.com结尾。这些配置适用于服务器在EAP PEAP流程期间使用的证书。如果在您的环境中使用ISE，可以使用策略服务器节点EAP证书的公用名称。



用户身份验证服务器证书信任部分

25.可以在证书受信任颁发机构中选择两个选项。在此场景中，使用选项Trust Any Root Certificate Authority(CA)Installed on the OS，而不是添加签署RADIUS EAP证书的特定CA证书。

26.单击下一步。



用户身份验证凭证

27.在“凭证”部分中，仅更改用户凭证部分。

28.选择提示输入凭证>永不记忆选项。因此，在每个身份验证中，进行身份验证的用户必须输入其凭证。

29.单击完成按钮。

30.选择文件>另存为，并将安全客户端网络访问管理器配置文件另存为configuration.xml。

31.要创建安全客户端网络访问管理器，请使用刚创建的配置文件，并将下一个目录中的configuration.xml文件替换为新文件：

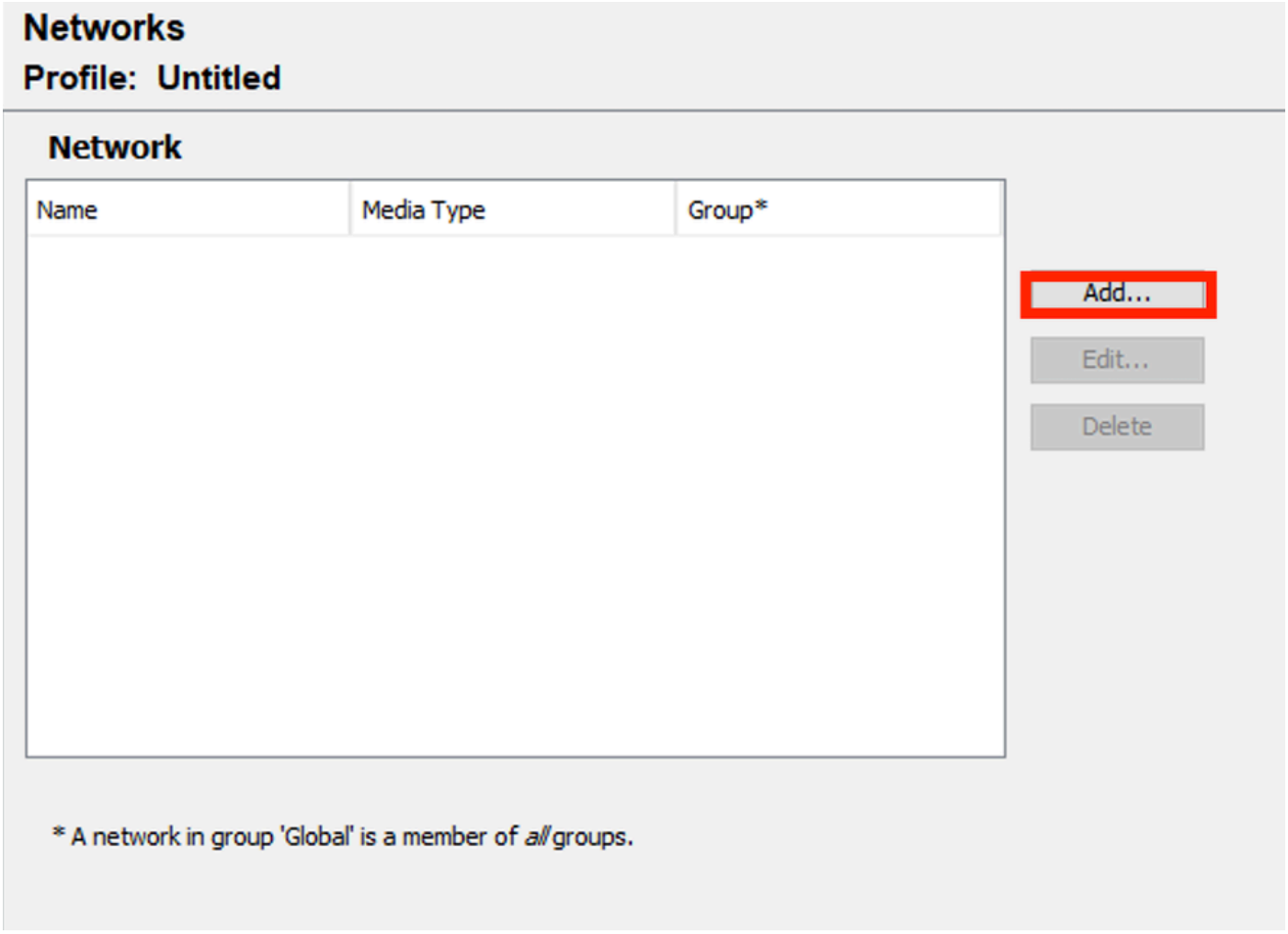
C:\ProgramData\Cisco\Cisco安全客户端\网络访问管理器\system

注意：文件必须命名为configuration.xml，否则它不起作用。

情形 3：为EAP TLS用户证书身份验证配置安全客户端NAM请求方

1.打开NAM配置文件编辑器，然后导航至网络部分。

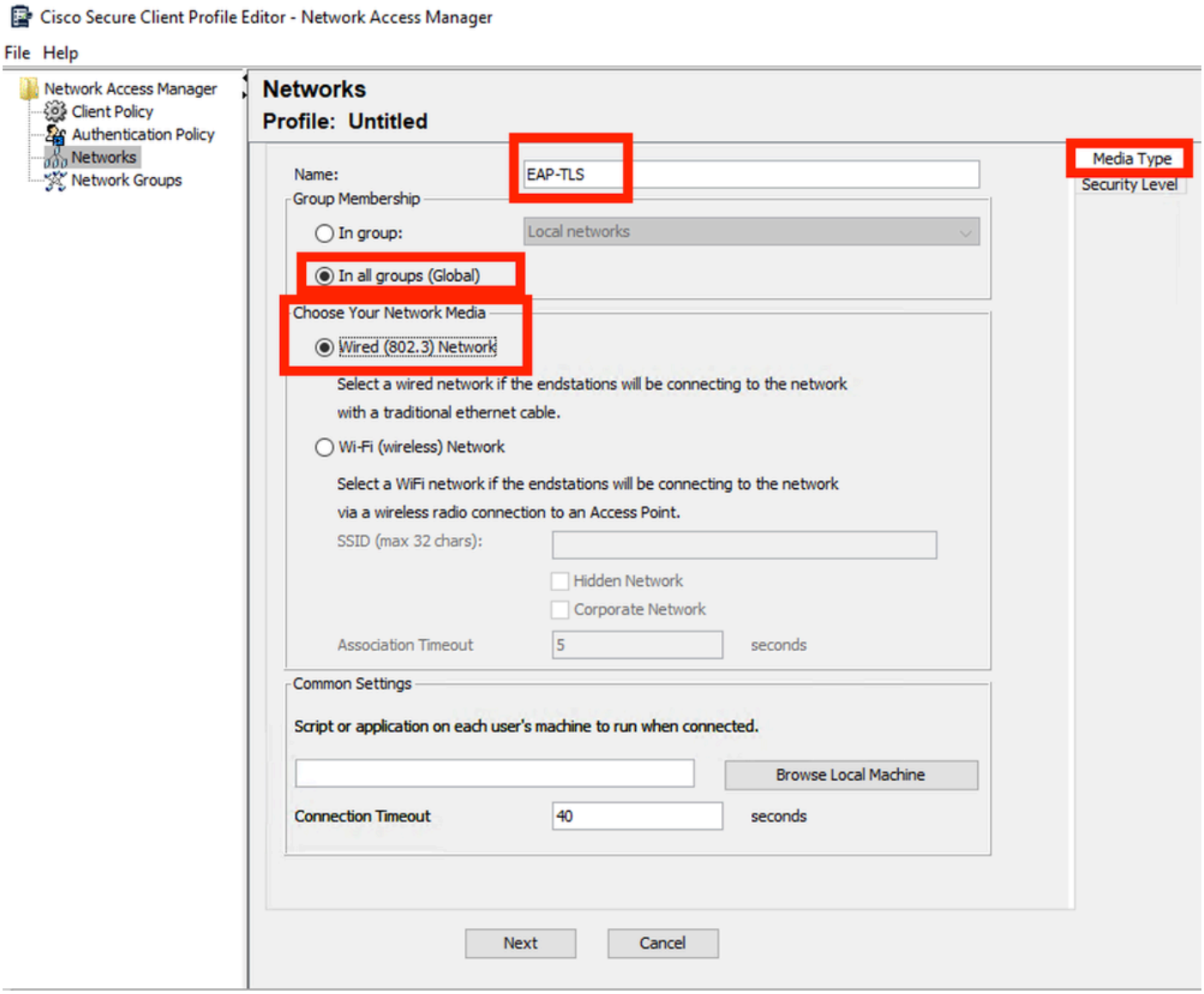
2.单击Add。



Network Creation部分

3.命名网络配置文件，在本例中，名称为EAP协议。

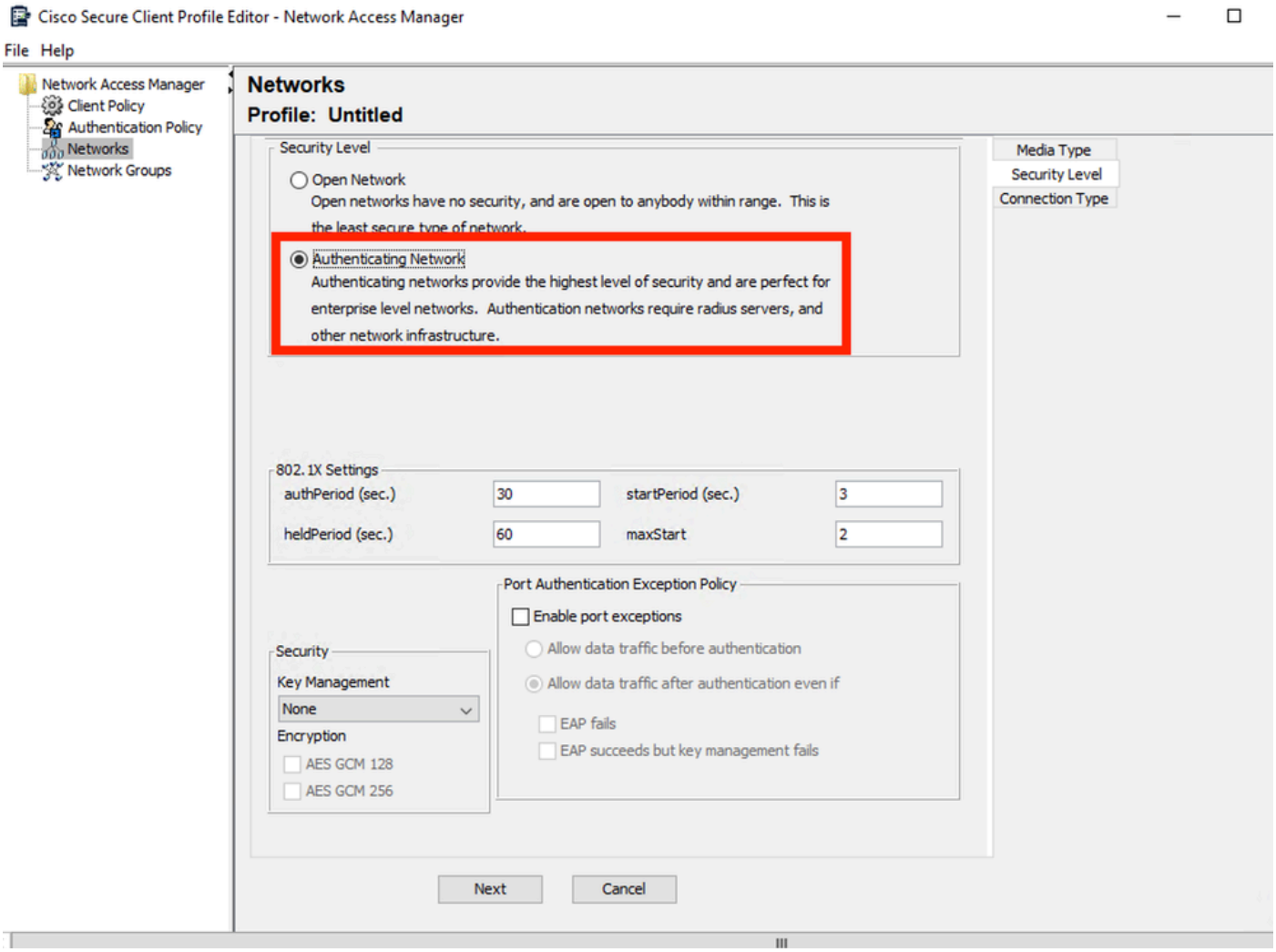
4.选择Global作为Group Membership。和有线网络介质。



Media Type部分

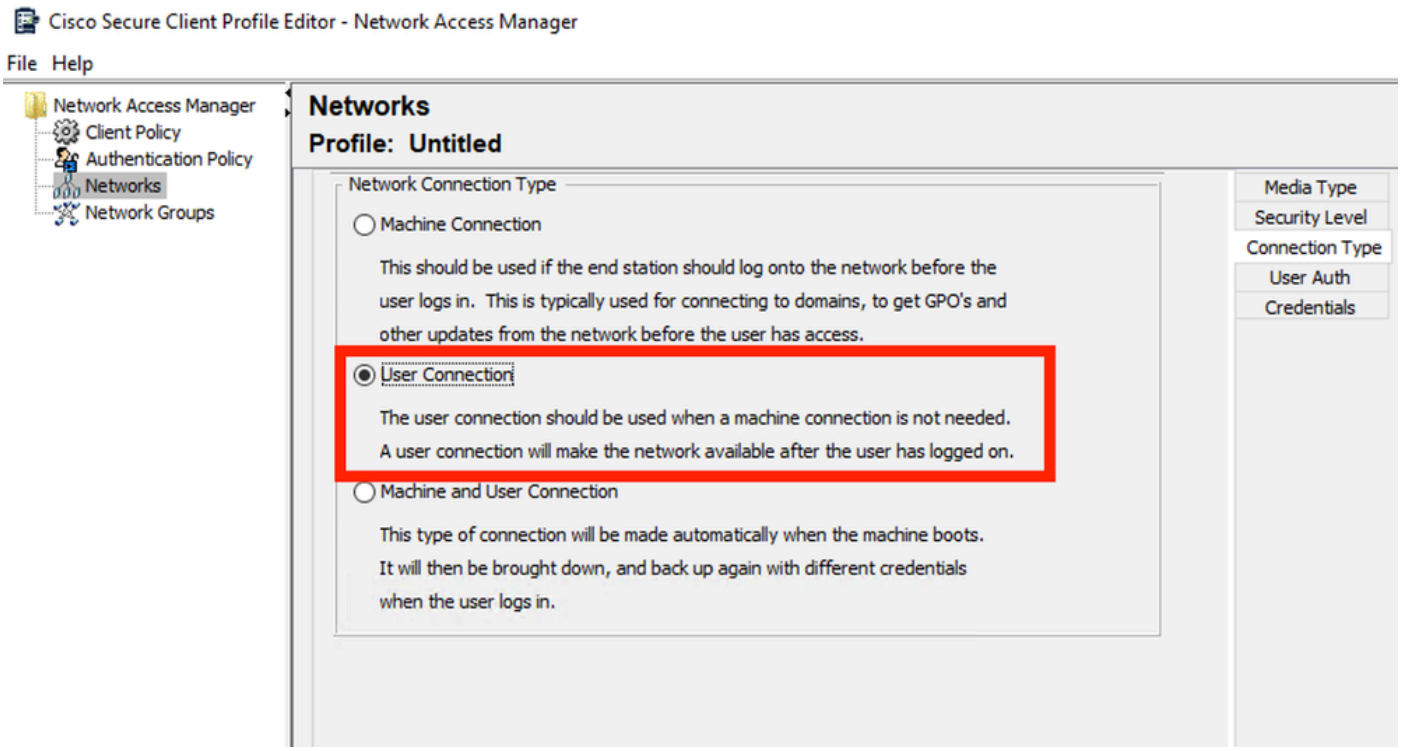
5.单击下一步。

6.选择Authenticating Network，不要更改Security Level部分中其余选项的默认值。



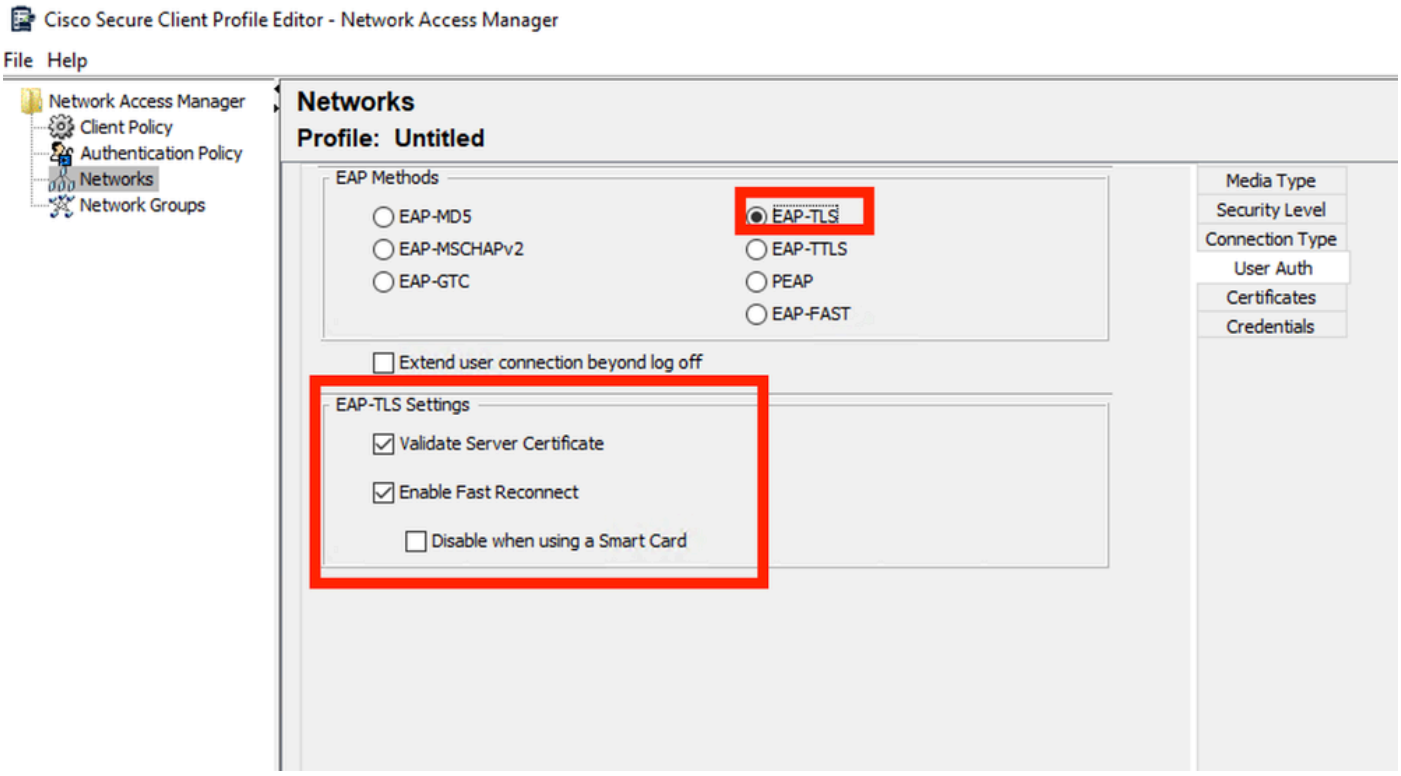
安全级别

7.此场景用于使用证书进行用户身份验证。因此，使用User Connection选项。



连接类型

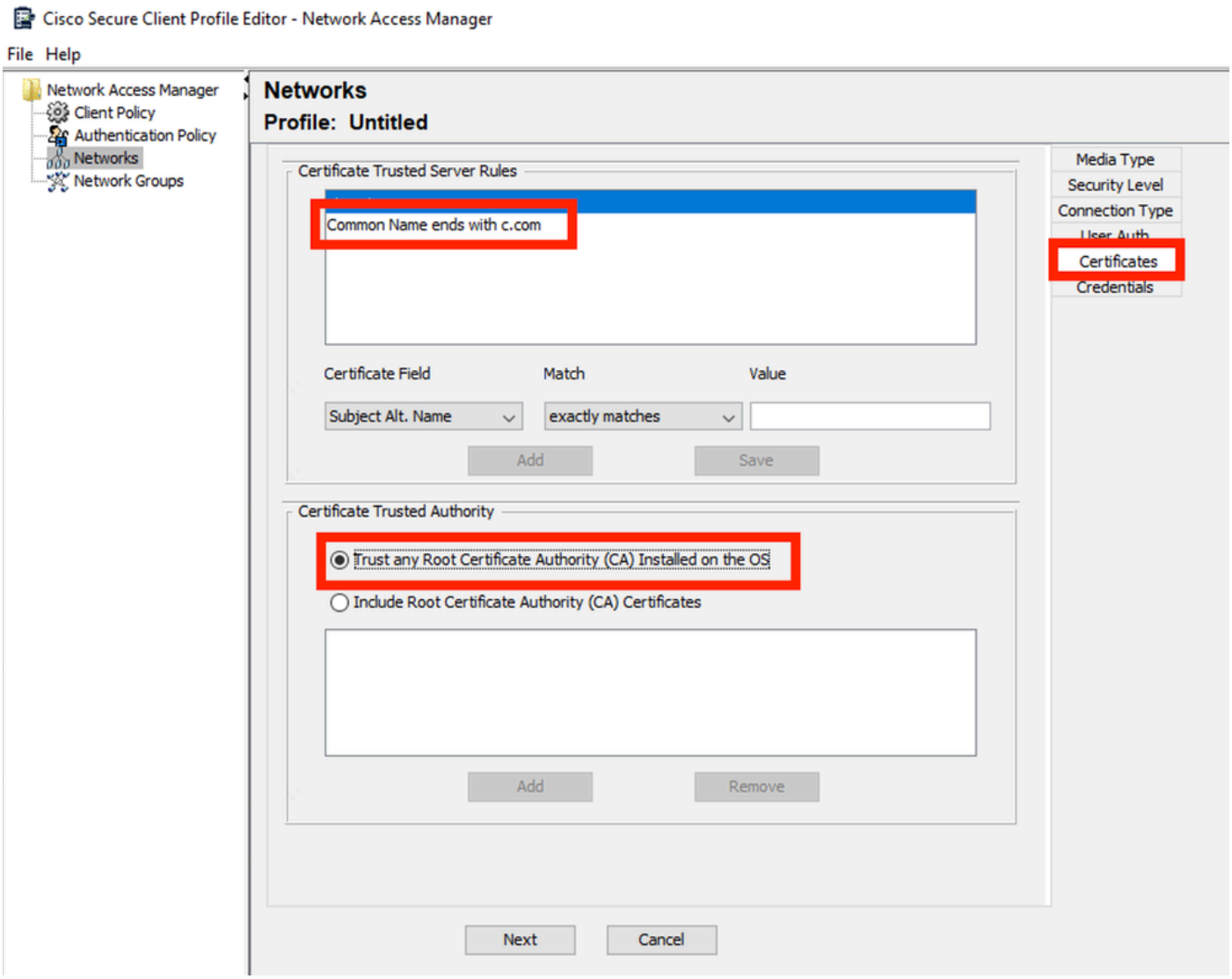
8.将EAP-TLS配置为EAP方法，并且不要更改EAP-TLS设置部分中的默认值。



User Auth部分

9.对于“证书”部分，创建匹配AAA EAP-TLS证书的规则。如果您使用的是ISE，请在Administration > System > Certificates部分中查找此规则。

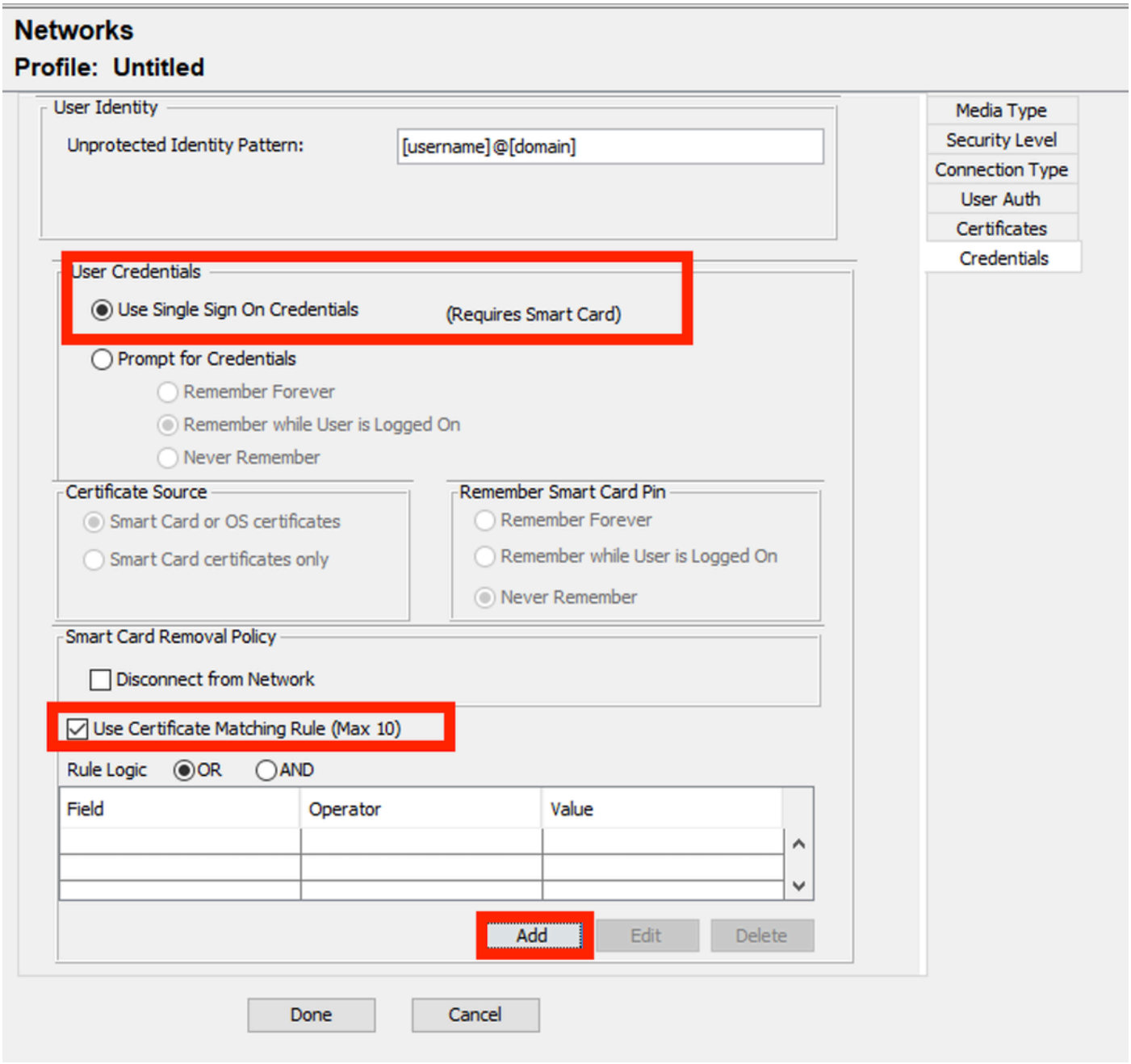
10.对于Certificate Trusted Authority部分，选择Trust any Root Certificate Authority(CA)installed on the OS。



用户身份验证服务器证书信任设置

11.单击下一步。

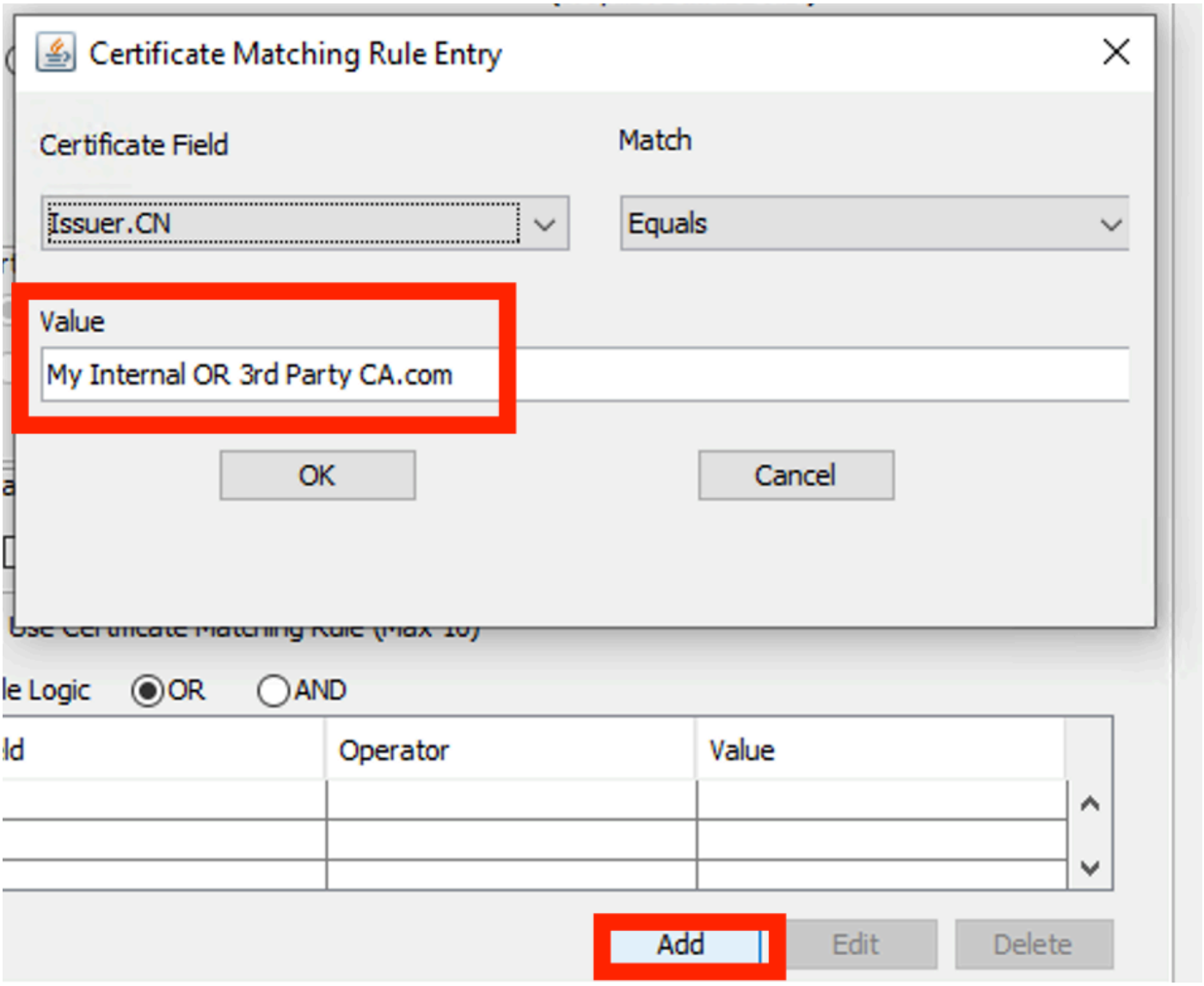
12，对于User Credentials部分，不要更改第一部分中的默认值。



User Auth Credentials部分

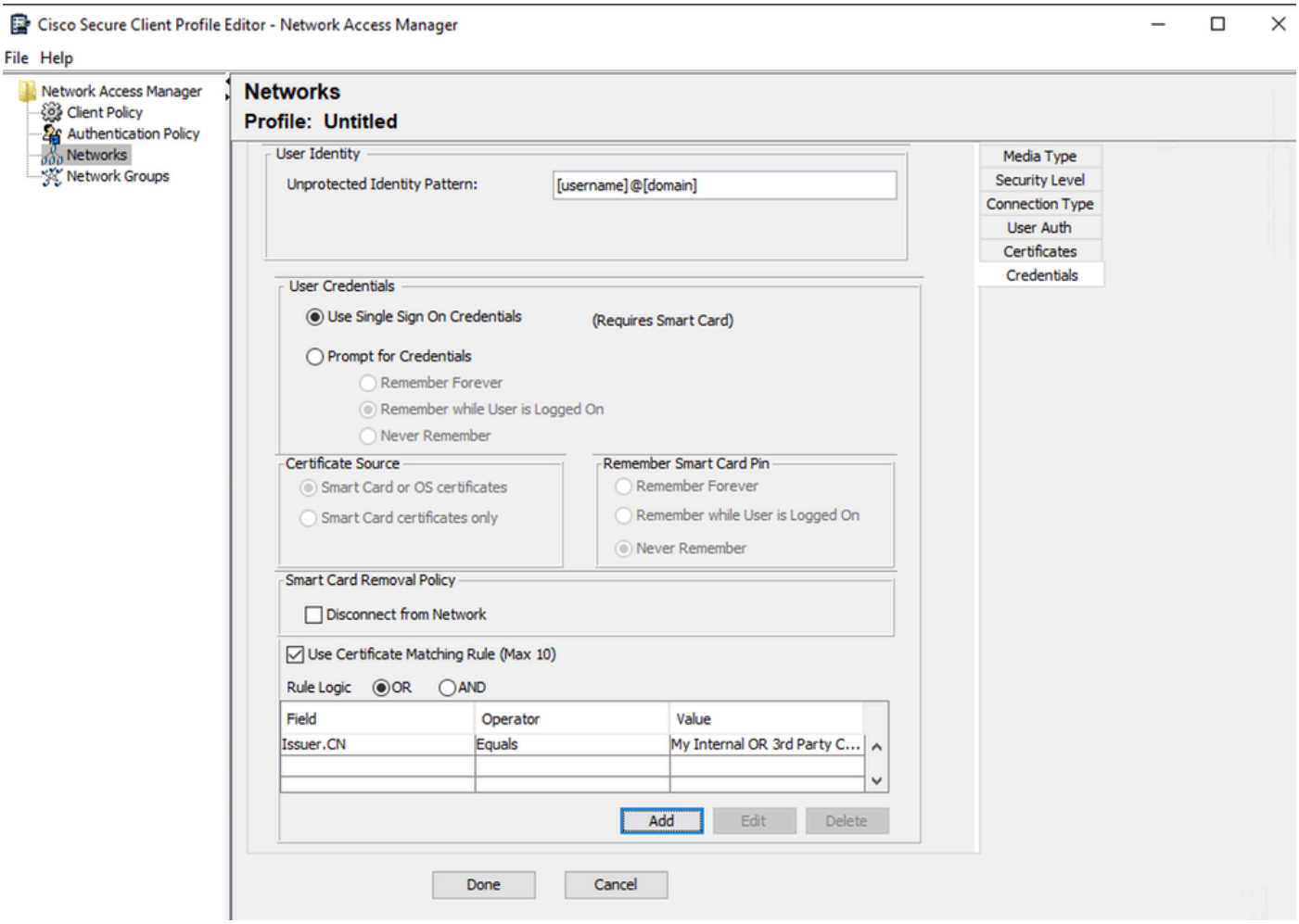
13.配置与用户在EAP TLS过程中发送的身份证书匹配的规则非常重要。要执行此操作，请点击使用证书匹配规则（最多10）旁边的复选框。

14.单击Add。



证书匹配规则窗口

15.将My Internal or 3rd Party CA.com字符串的值替换为用户证书的CN。



User Auth Certificate Credentials部分

16.单击完成完成配置。

17.选择文件>另存为，将安全客户端网络访问管理器配置文件另存为configuration.xml。

18.要添加安全客户端网络访问管理器，请使用刚创建的配置文件，并将下一个目录中的configuration.xml文件替换为新文件：

C:\ProgramData\Cisco\Cisco安全客户端\网络访问管理器\system

注意：文件必须命名为configuration.xml，否则它不起作用。

配置ISR 1100和ISE以允许基于方案1 PEAP MSCHAPv2的身份验证

1.配置ISR 1100路由器。

2.本节介绍NAD必须具备的基本配置，以确保dot1x按预期运行。



注意：对于多模ISE部署，指向启用了策略服务器节点角色的任何节点。这可以通过导航到管理>系统>部署选项卡中的ISE来检查。

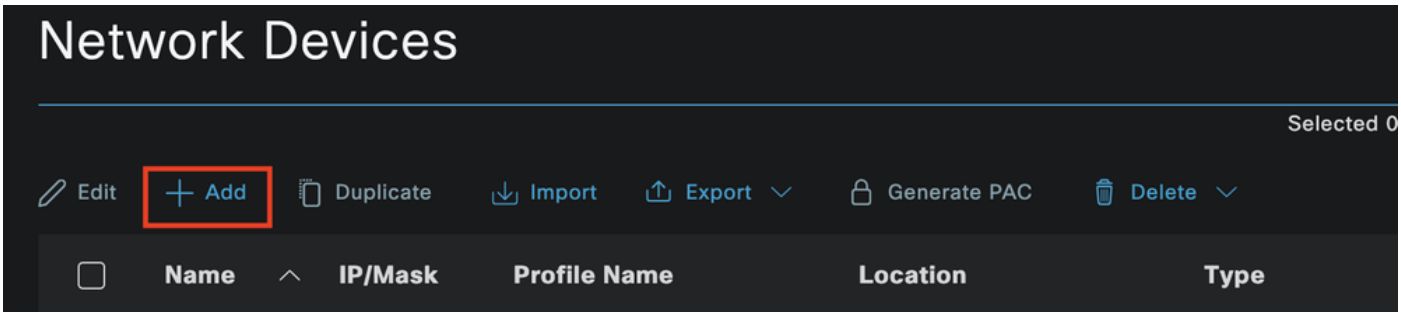
```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
 client A.B.C.D server-key  <Your shared secret>
!
!
radius server  ISE-PSN-1
 address ipv4 A.B.C.D auth-port 1645 acct-port 1646
 timeout 15
 key <Your shared secret>
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

3.配置身份服务引擎3.2。

4.配置网络设备。

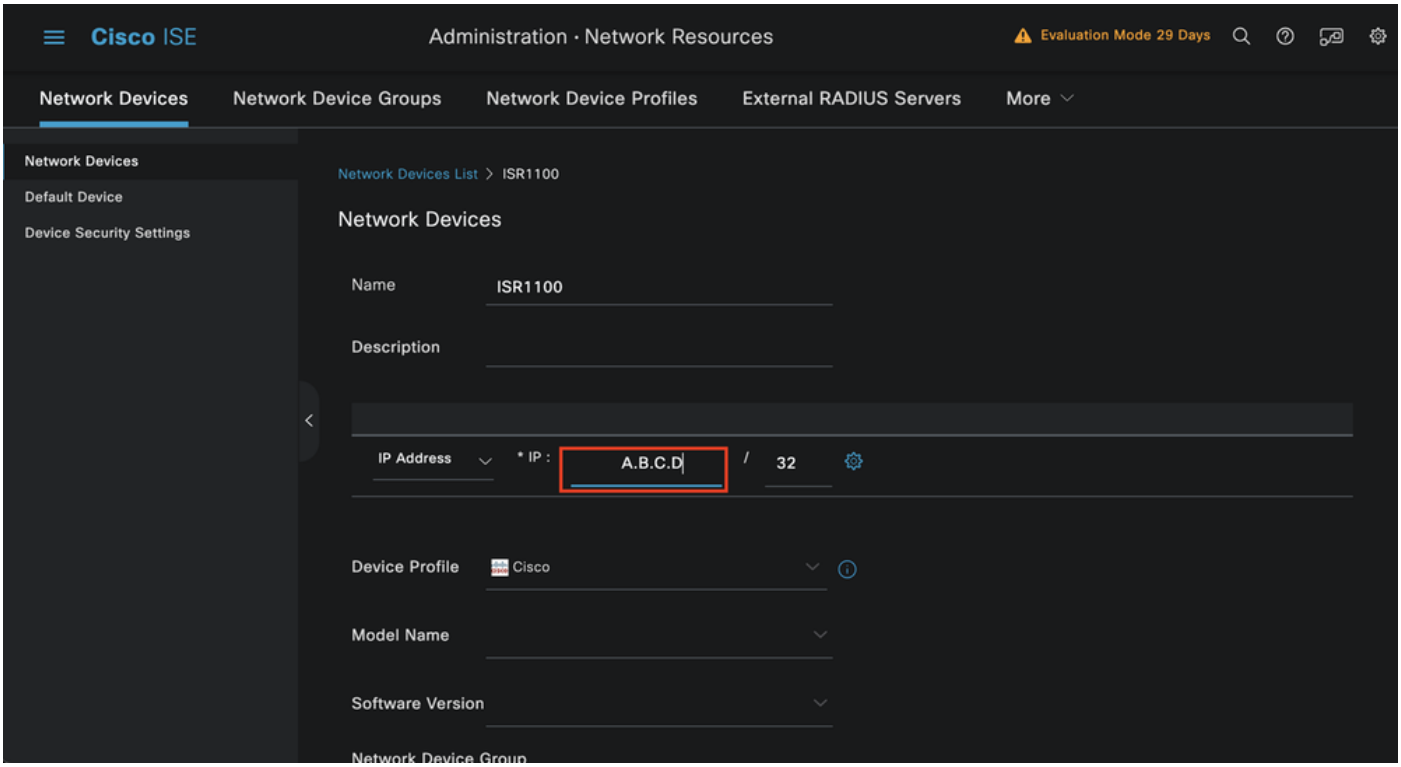
5.将ISR NAD添加到ISE Administration > Network Resources > Network Devices。

6.单击Add。



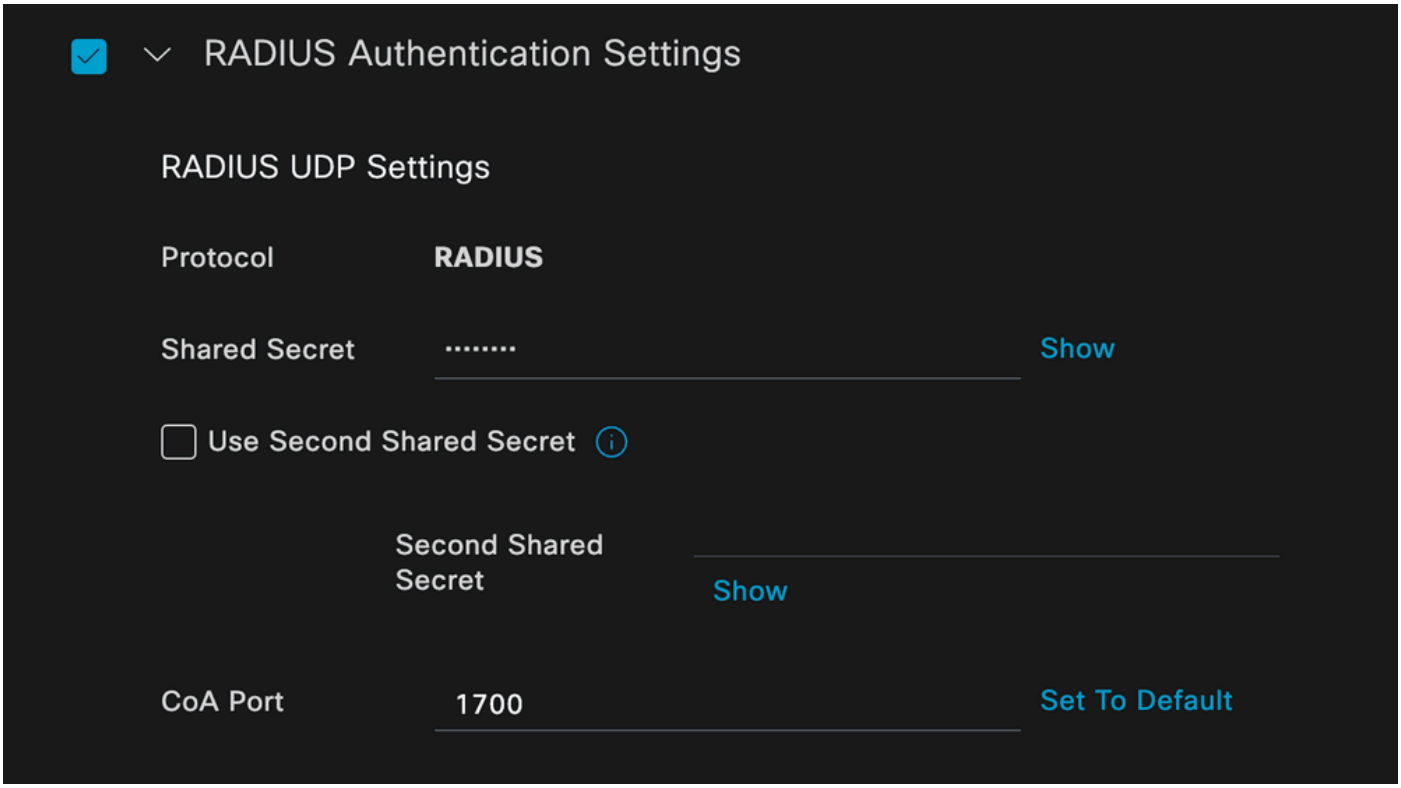
Network Device部分

7.为正在创建的NAD指定名称。添加网络设备IP。



网络设备创建

8.在同一页的底部，添加网络设备配置中使用的共享密钥。



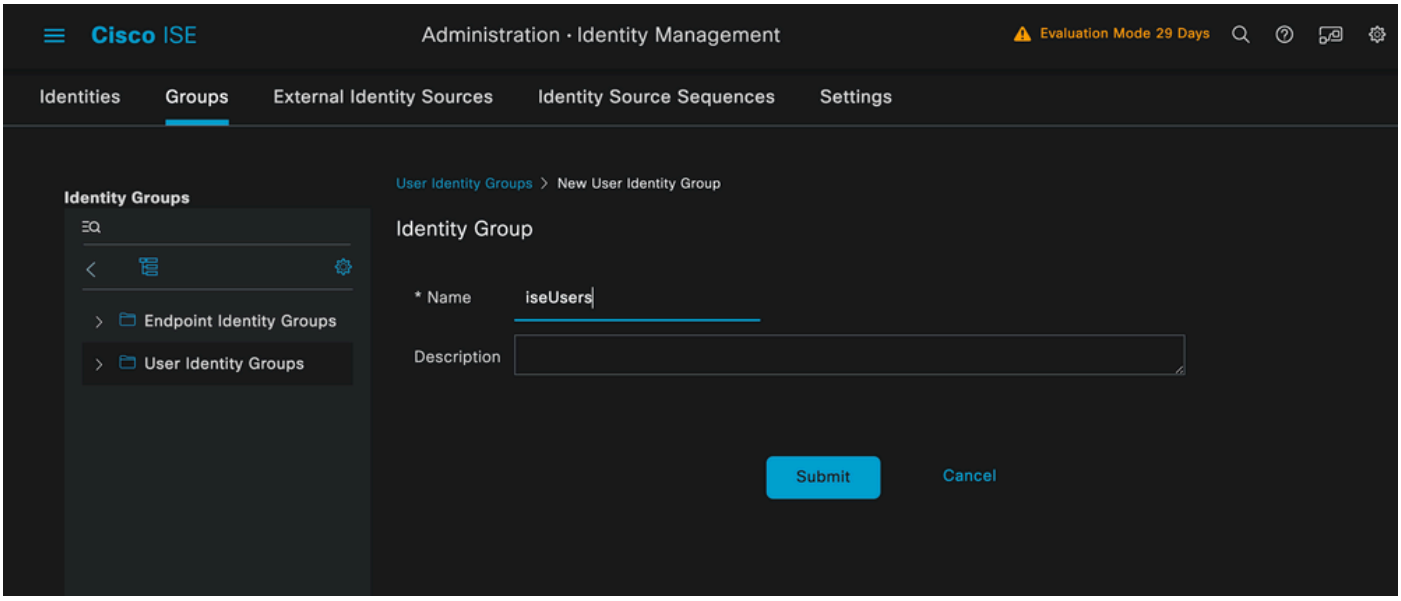
网络设备*Radius*设置

8.保存更改。

9.配置用于对终端进行身份验证的身份。

10.使用ISE本地身份验证，本文未解释外部ISE身份验证。

11.定位至管理>身份管理>组标签，然后创建用户所属的组。为此示例创建的身份组是iseUsers。

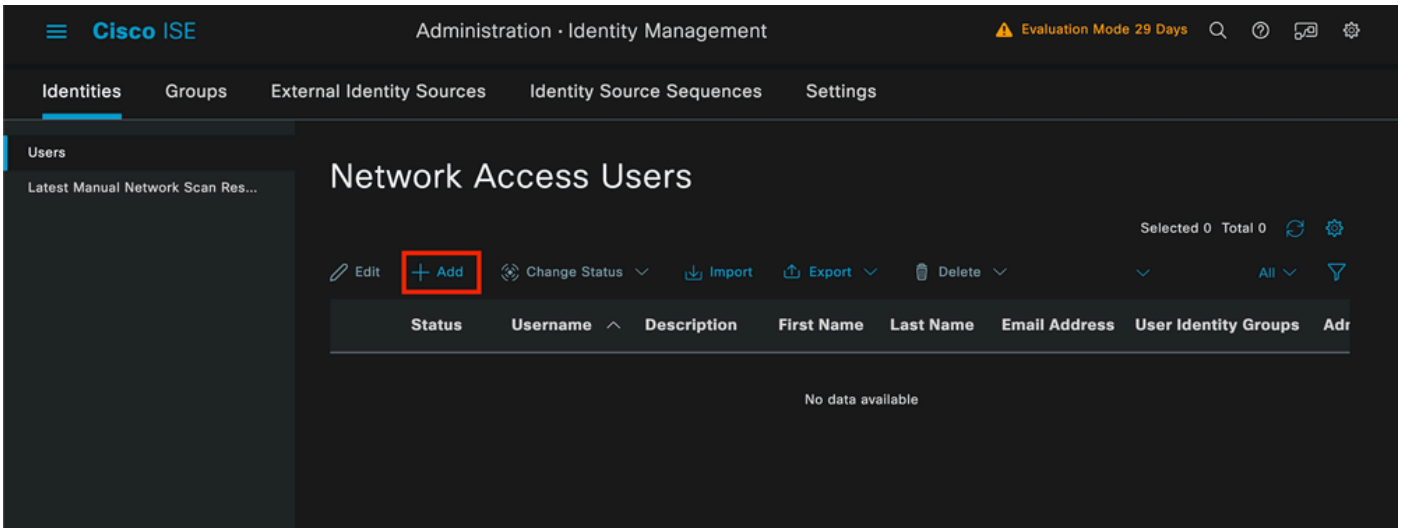


身份组创建

12.单击Submit。

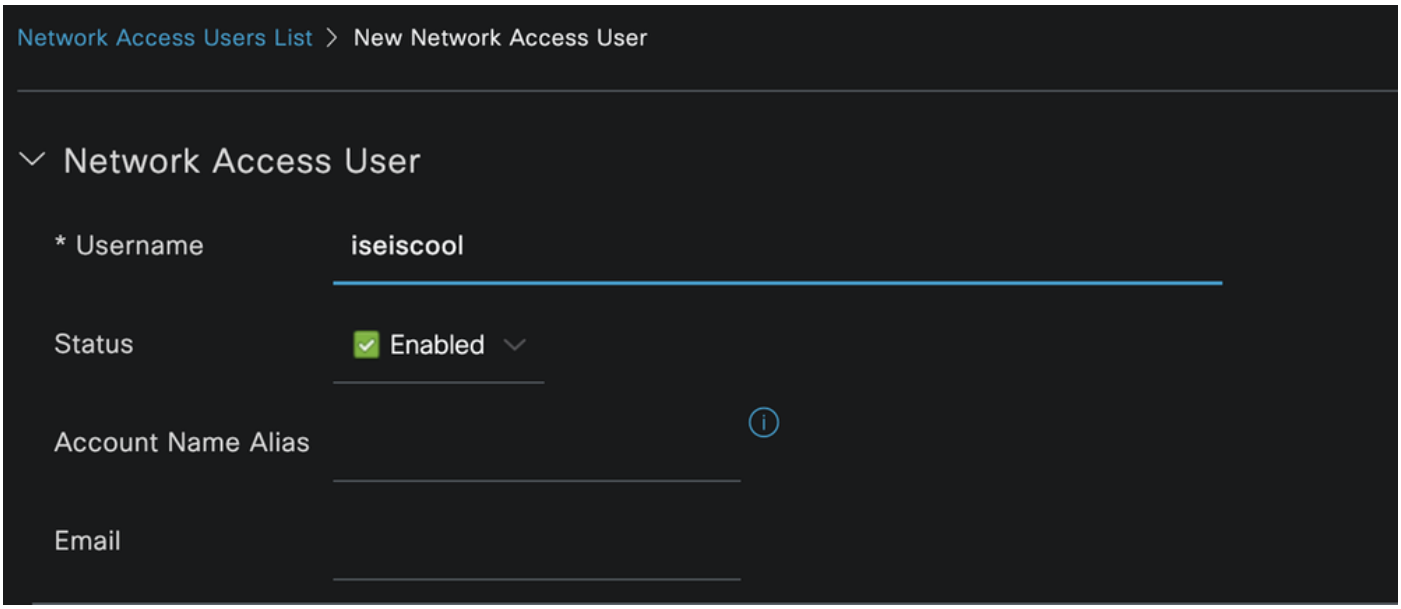
13.导航到管理>身份管理>身份选项卡。

14.单击Add。



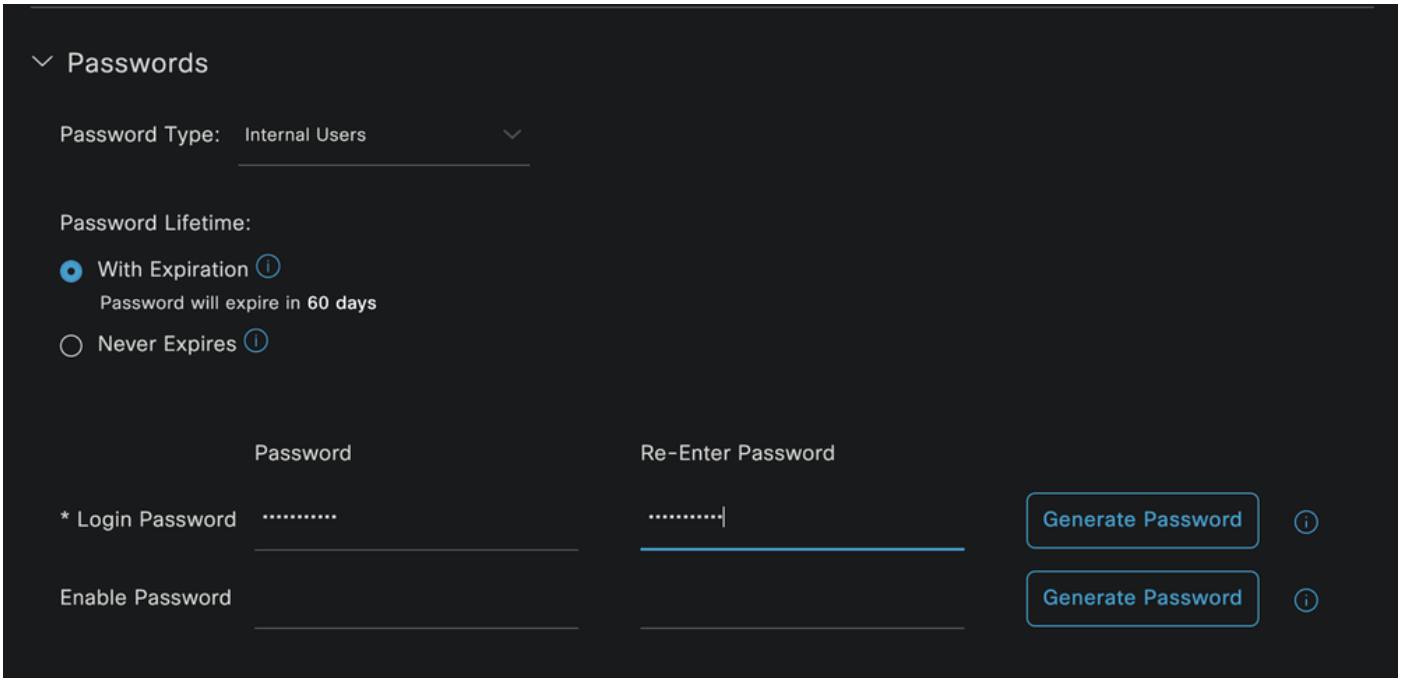
Network Access Users部分

15.作为必填字段的一部分。以用户的名称开头。本示例中使用的是用户名iseiscool。



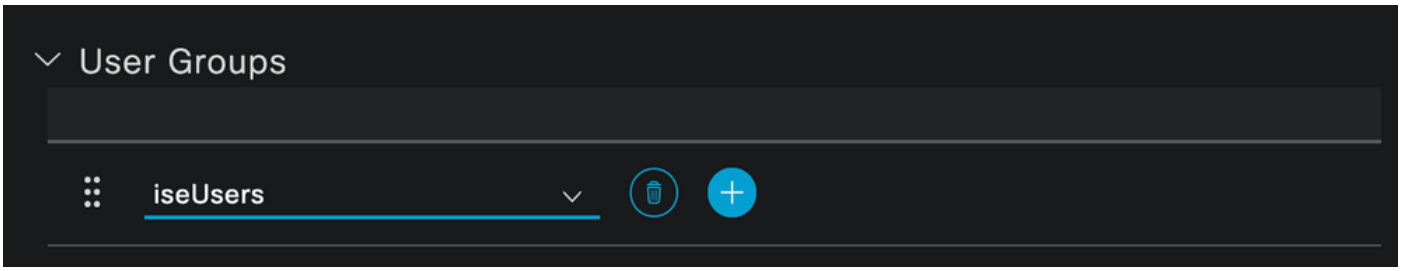
网络访问用户创建

16.为用户分配密码，在本示例中，使用VainillaISE97。



User Creation Password部分

17.将用户分配到iseUsers组。



用户组分配

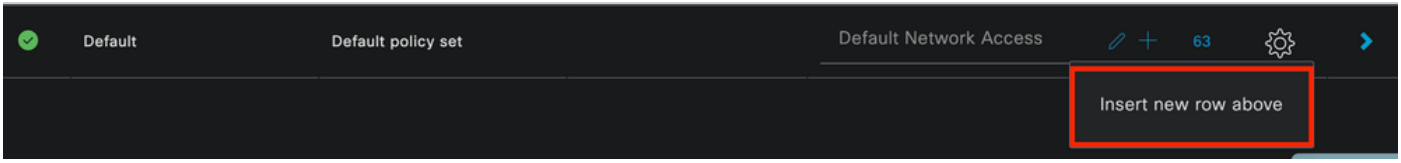
18.配置策略集。

19.导航到ISE菜单>策略>策略集。

20.可以使用默认策略集。但是，此示例创建了一个名为Wired的示例。

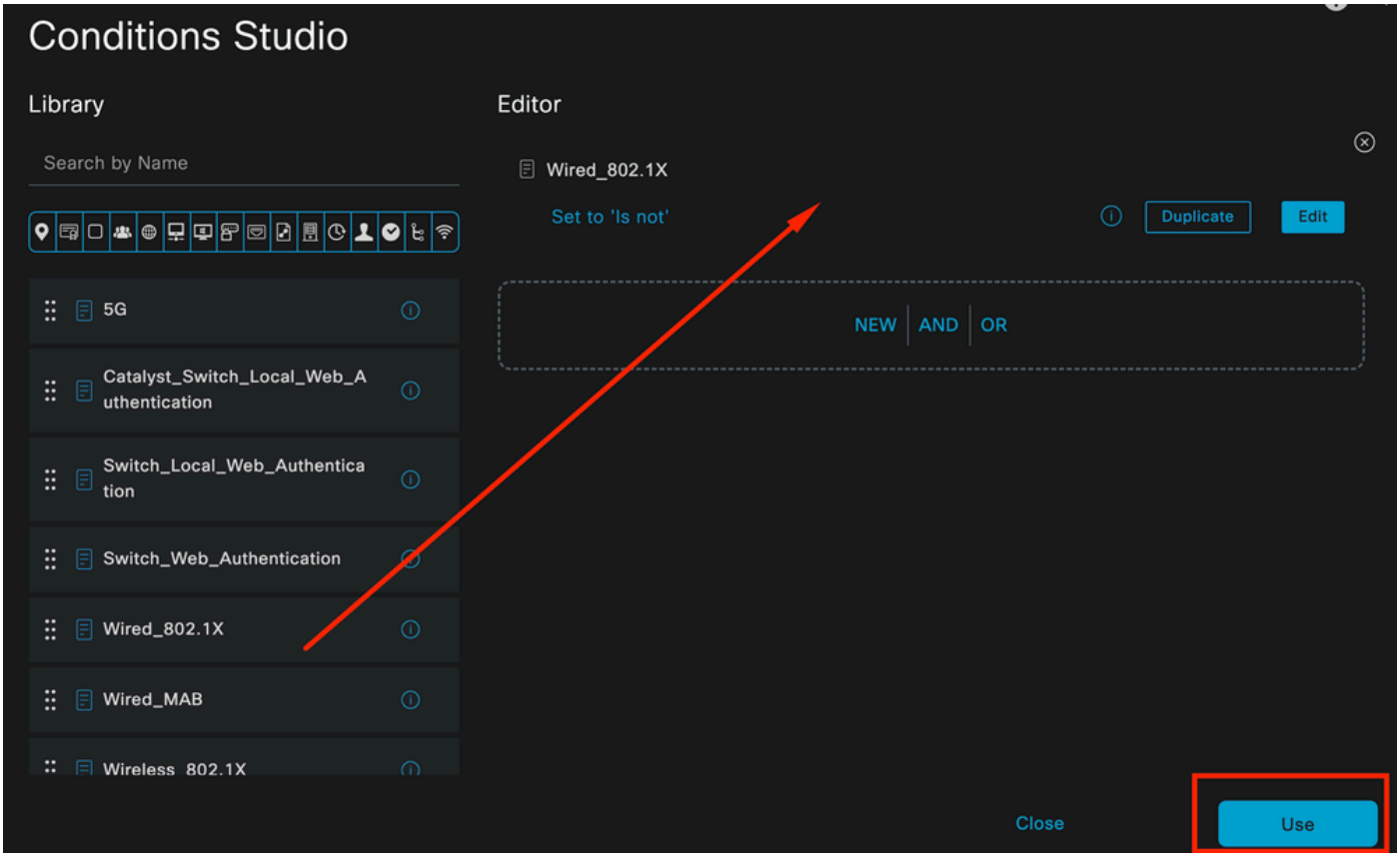
注意：对策略集进行分类和差异化有助于进行故障排除，

如果添加或加号图标“+”不可见，则可以单击任何策略集的齿轮图标，然后选择Insert new row above。



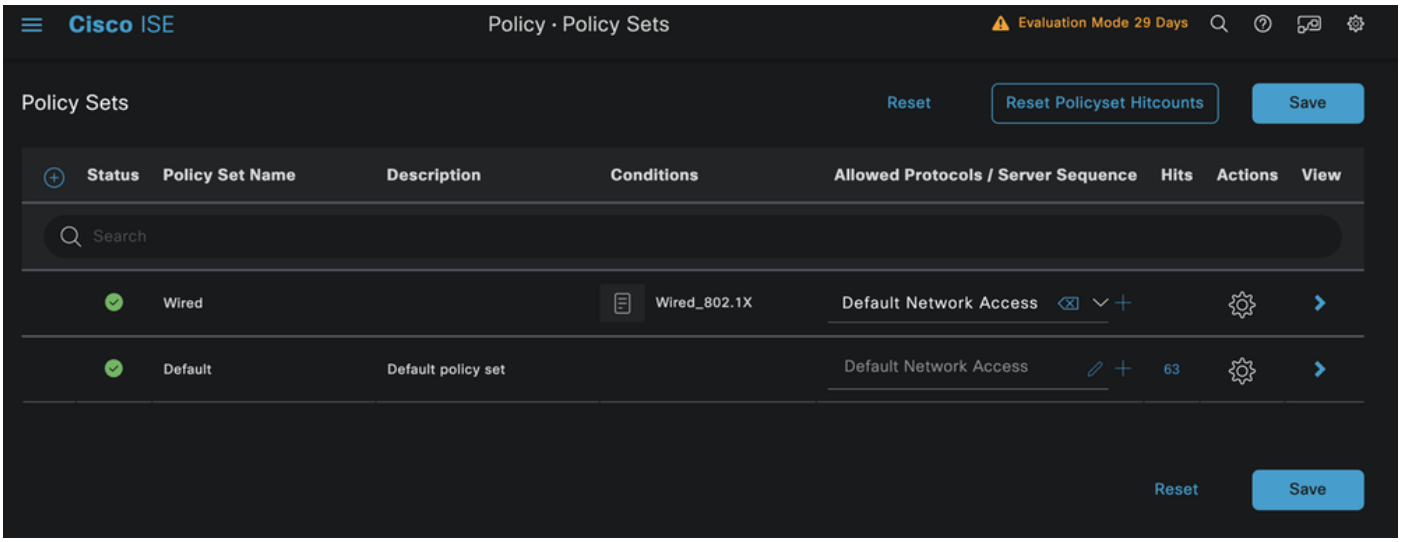
齿轮图标选项

21.使用的条件是有线8021x，请将其拖动。然后单击Use。



身份验证策略条件工作室

22.在允许的协议部分中选择默认网络访问。

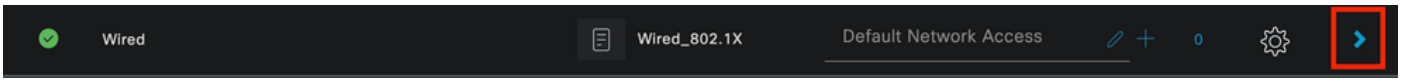


策略集常规视图

23.单击保存。

配置身份验证和授权策略

1.单击>图标。



有线策略集

2.展开Authentication Policy部分。

3.单击“+”图标。



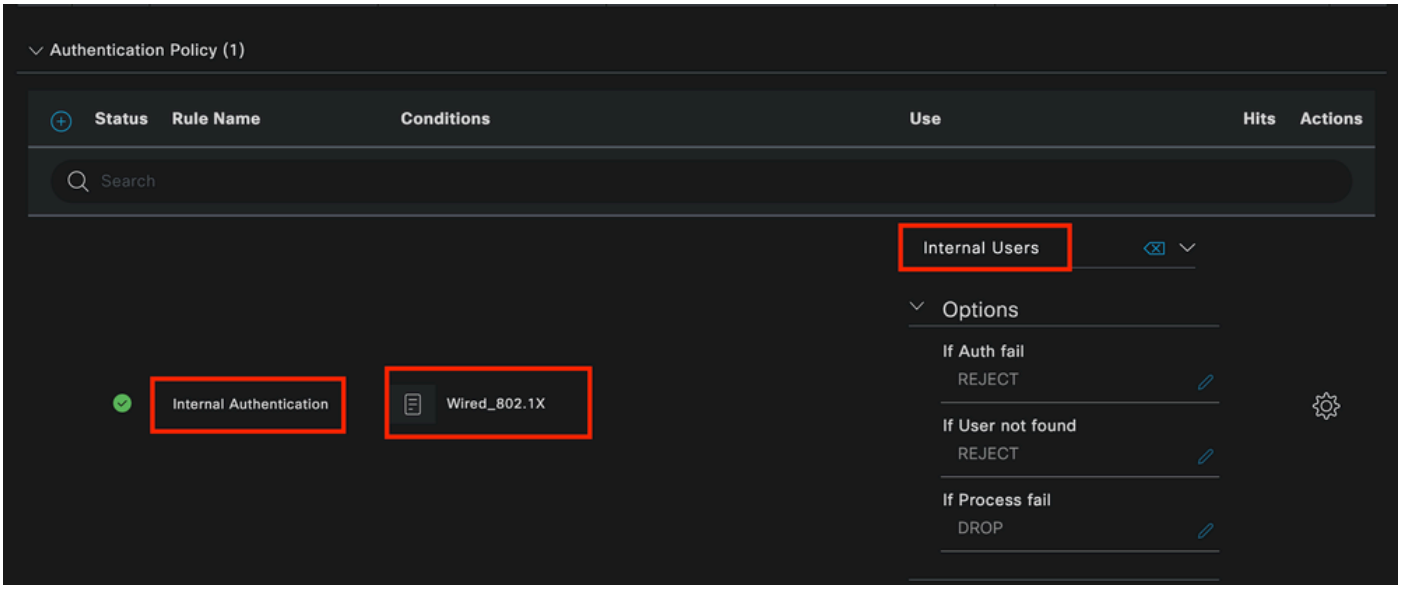
验证策略

4.为身份验证策略分配名称；本示例使用内部身份验证。

5.点击此新身份验证策略条件列上的“+”图标。

6.使用预配置条件Wired Dot1x。

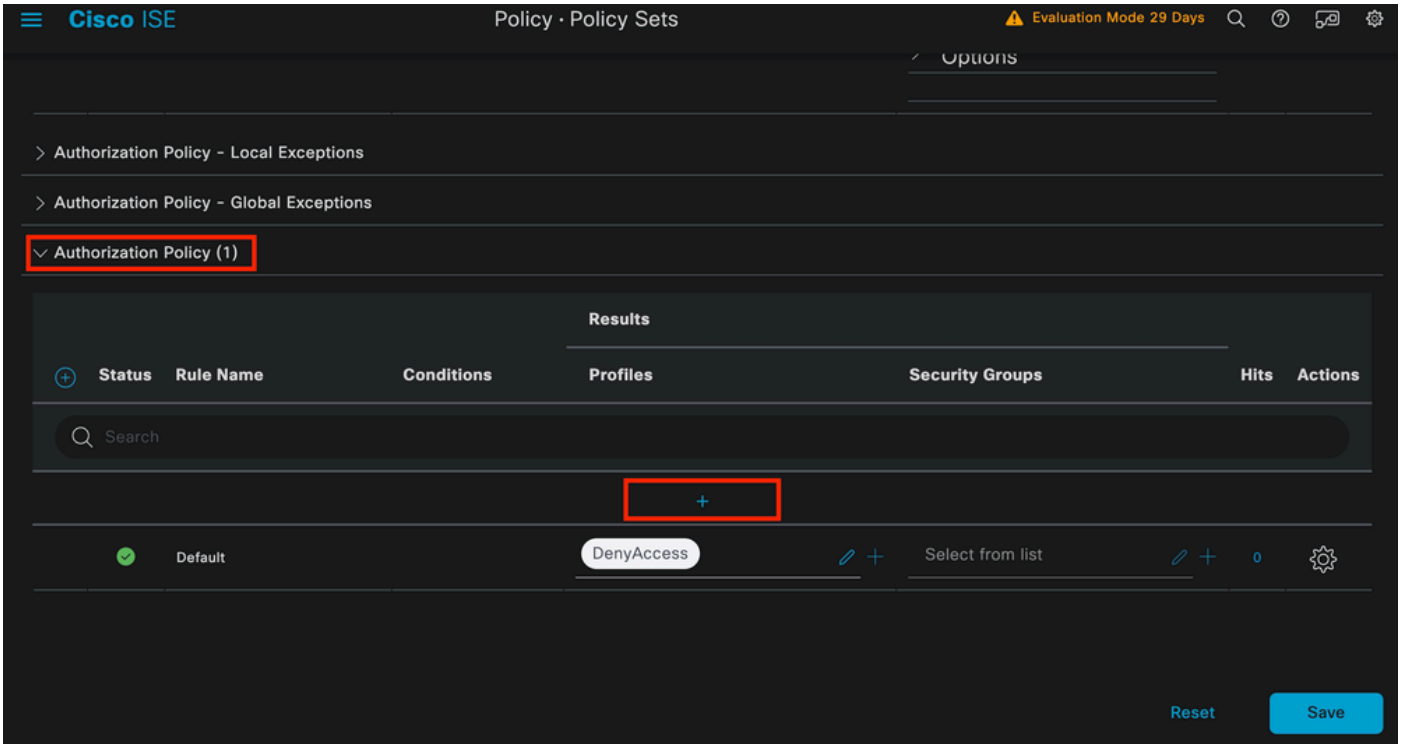
7.在使用列中，选择内部用户。



验证策略

授权策略

1. Authorization Policy部分位于页面底部。展开它并点击+图标。



授权策略

2.命名最近创建的授权策略。在此配置示例中，使用内部ISE用户的名称。

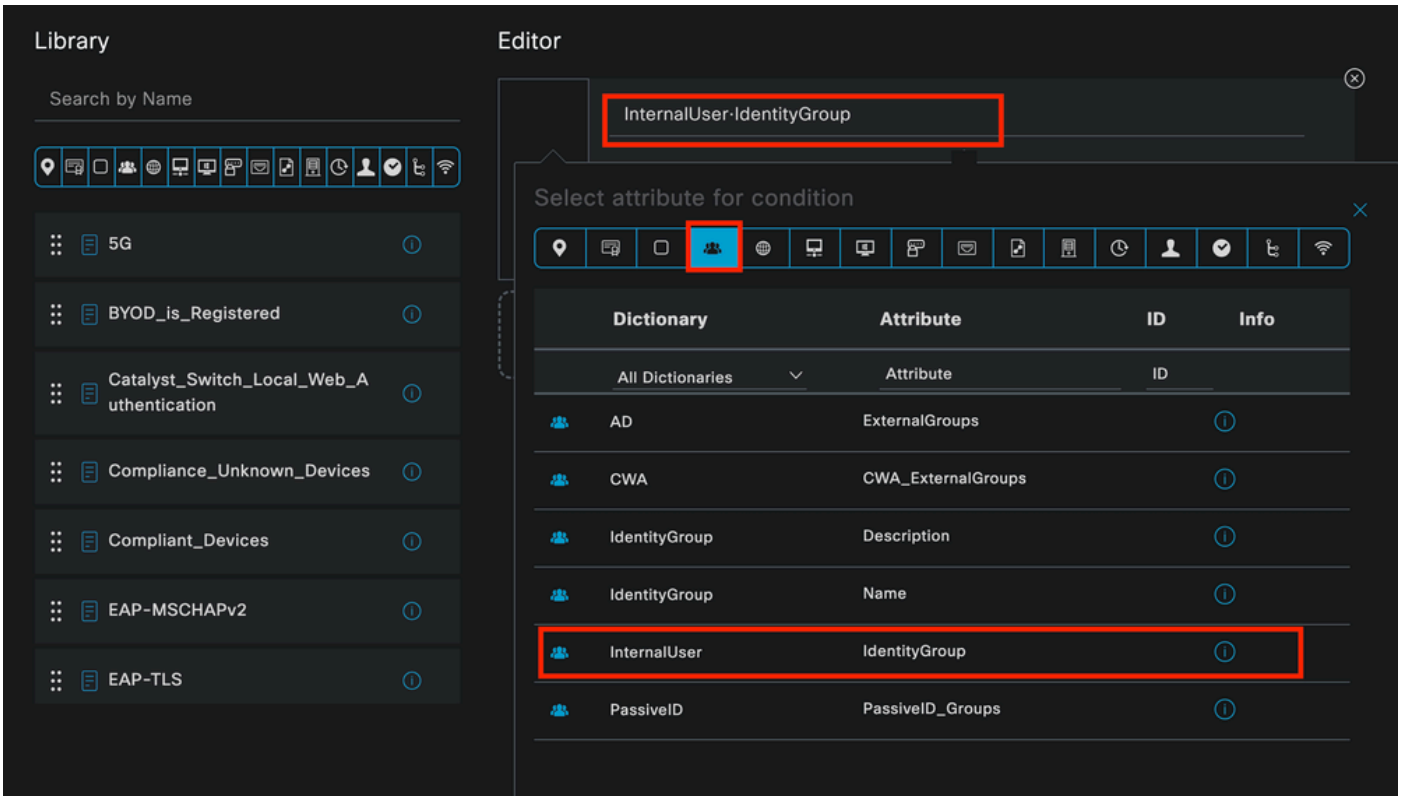
3.要为此授权策略创建条件，请点击“条件”列中的“+”图标。

4.使用IseUsers组。

5.单击属性部分。

6.选择IdentityGroup图标。

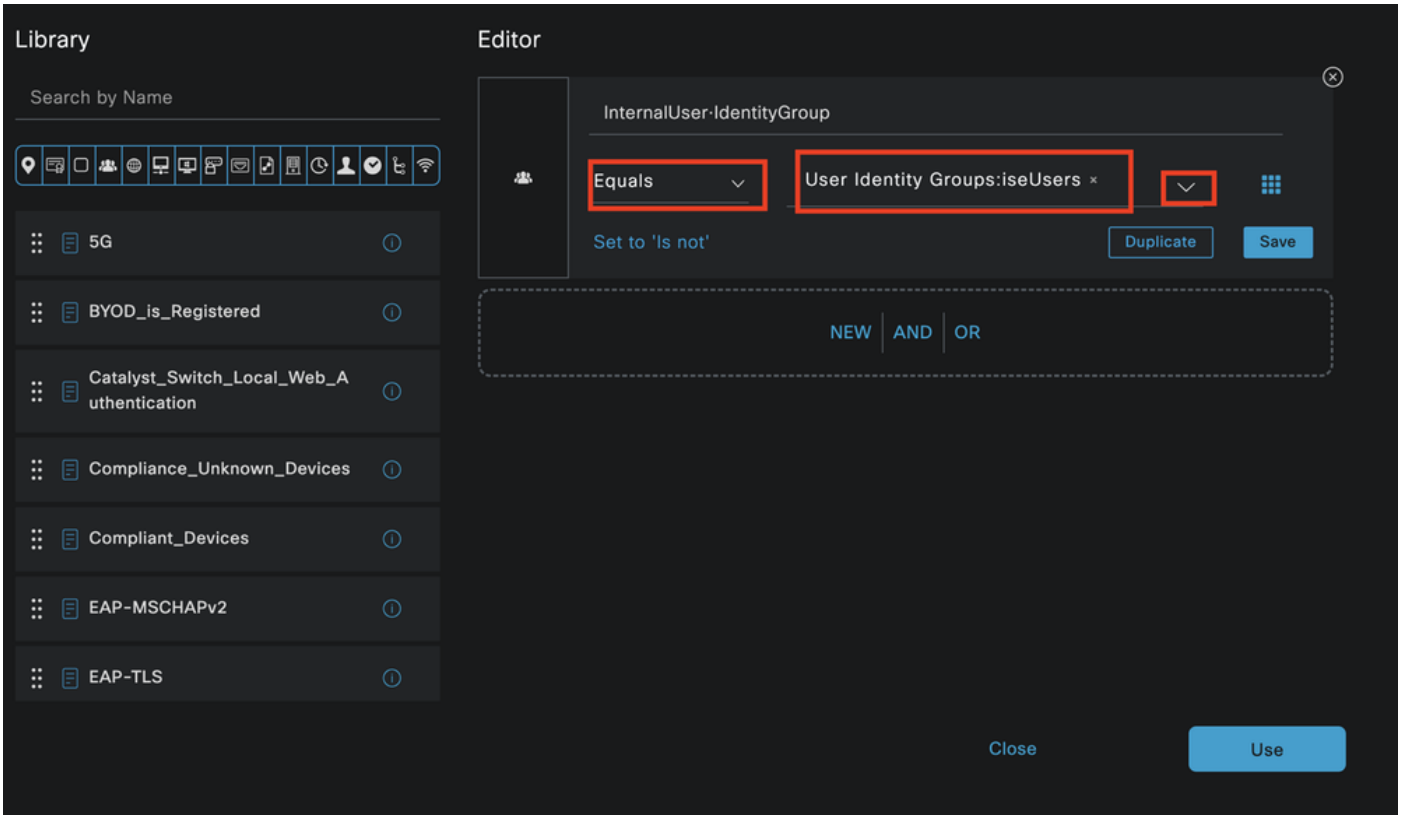
7.从词典中，选择随IdentityGroup属性提供的InternalUser词典。



条件创建

8.从下拉菜单中，选择Equals运算符。

9.从User Identity Groups下拉菜单中，选择IseUsers组。



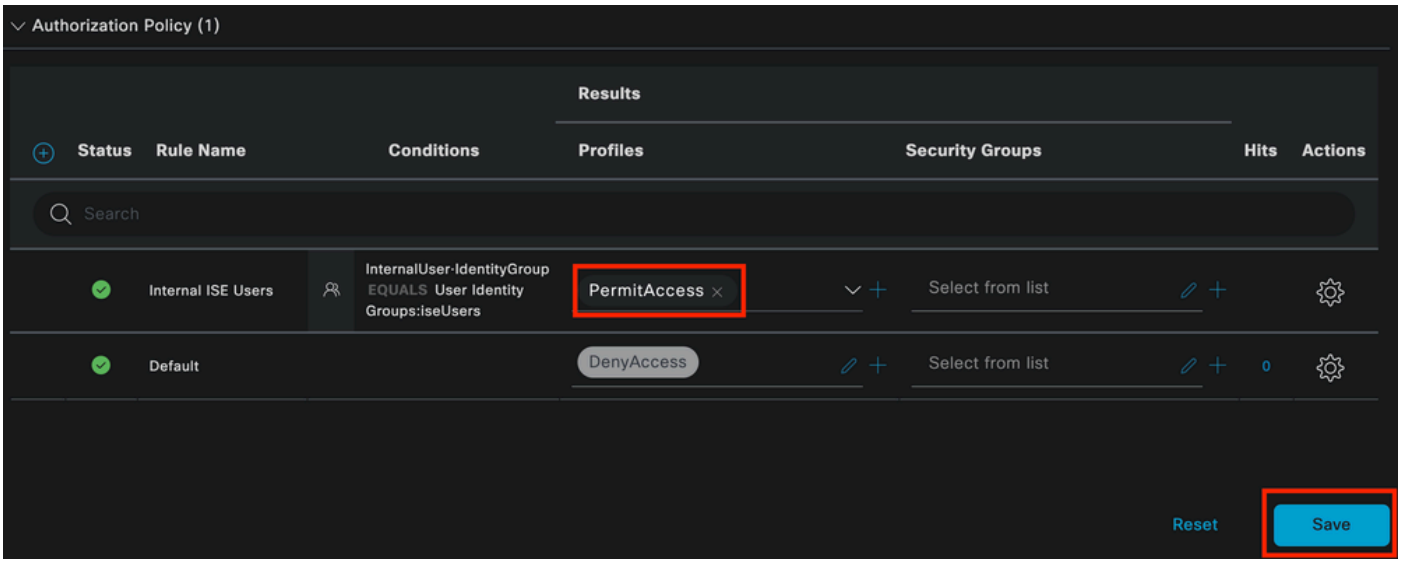
条件创建

10.单击Use。

11.添加Result Authorization Profile。

12.使用预配置的配置文件Permit Access。

注意：进入有线Dot1x策略集的ISE的身份验证不属于用户身份组ISEUsers。点击默认授权策略，这会导致DenyAccess。



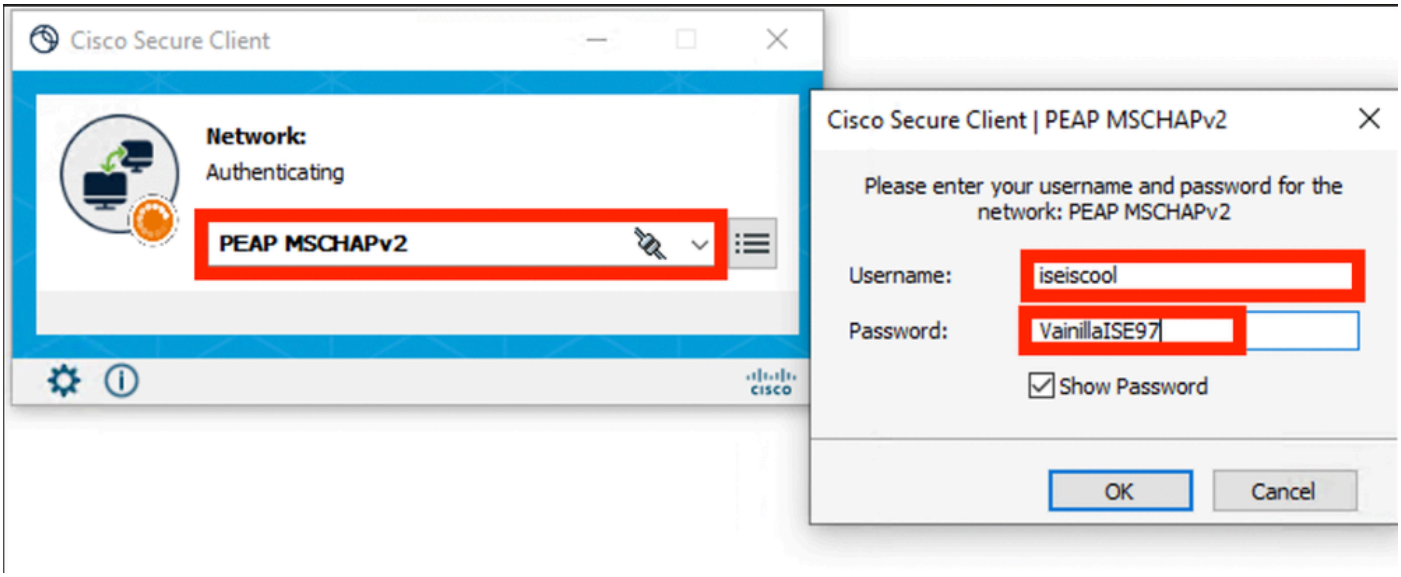
授权策略

13.单击Save。

验证

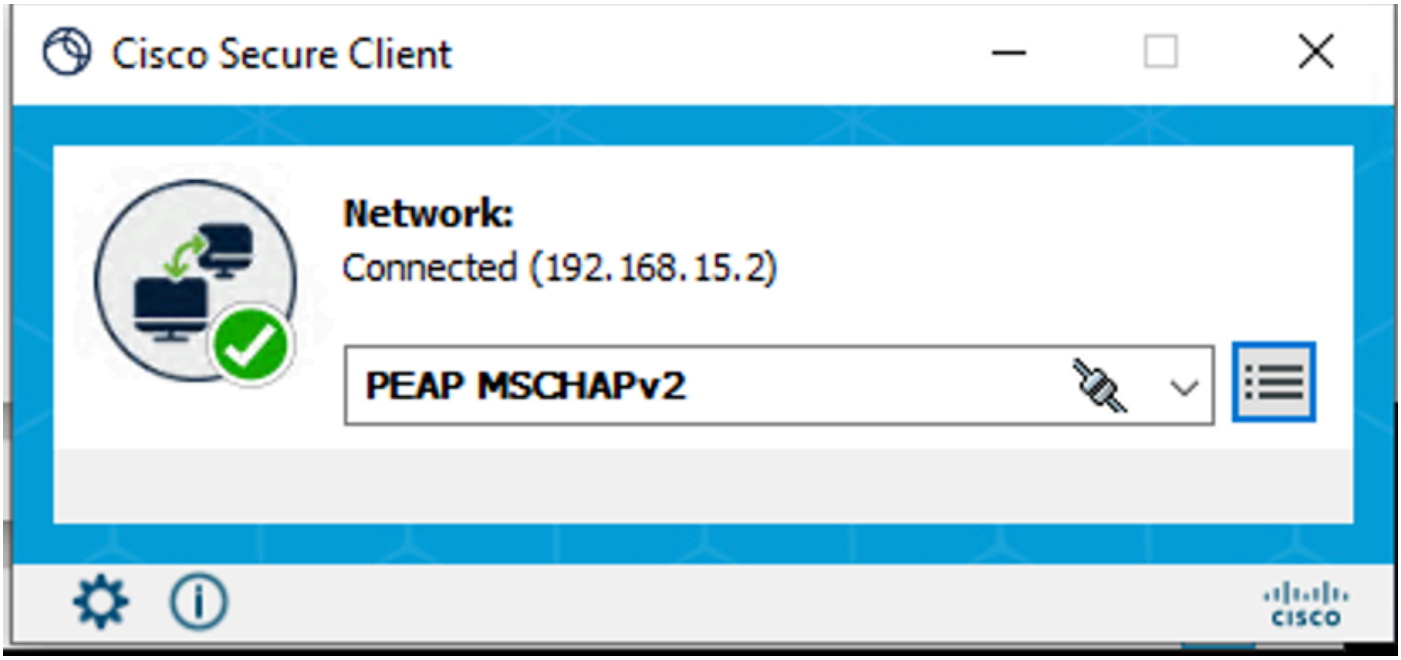
1.配置完成后，安全客户端会提示输入凭证，并指定PEAP MSCHAPv2配置文件的用法。

2.输入以前创建的身份证明。



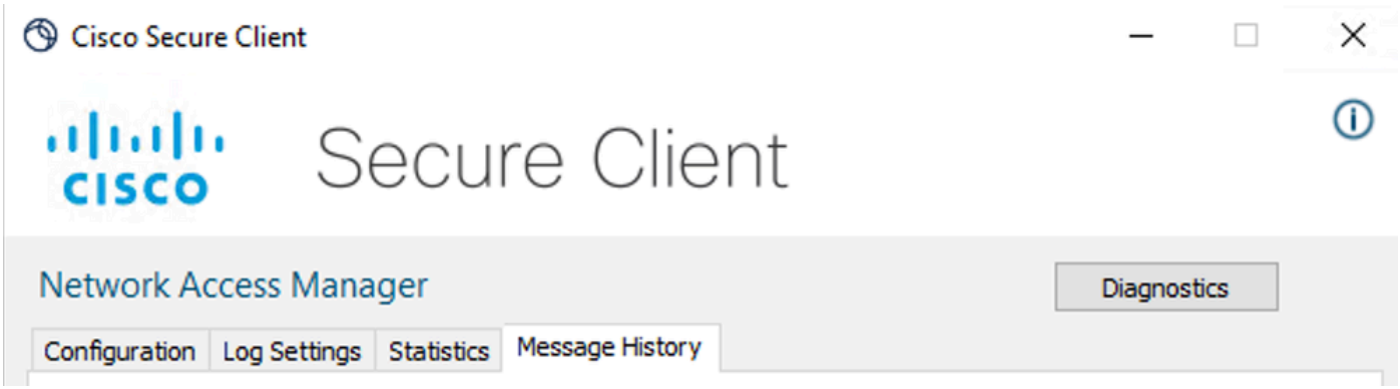
安全客户端*NAM*

3.如果终端身份验证正确，NAM将显示其已连接。

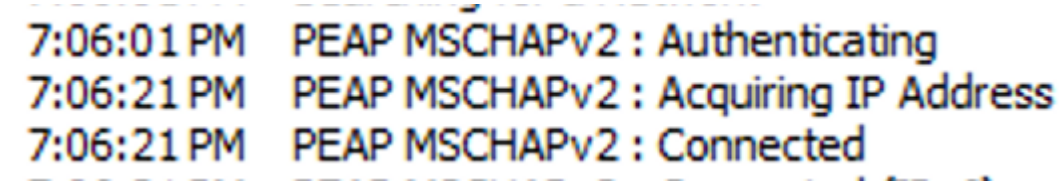


安全客户端*NAM*

4.通过单击信息图标并导航到消息历史记录部分，系统将显示所完成的每个步骤的详细信息。



安全客户端消息历史记录



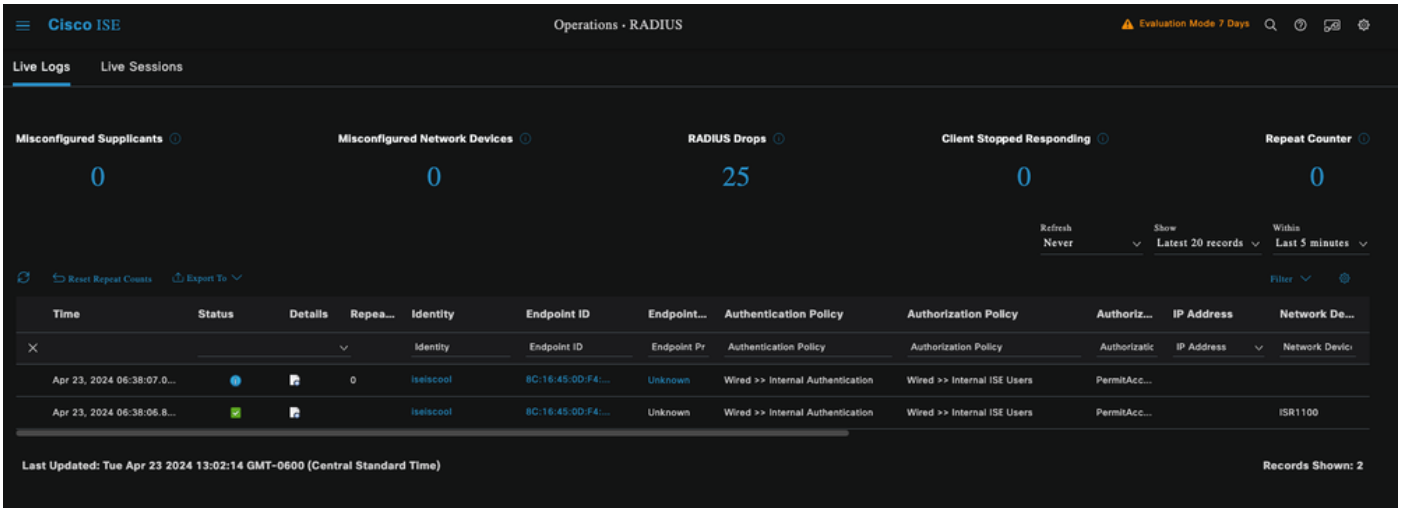
安全客户端消息历史记录

5.从ISE导航到操作> Radius LiveLogs以查看身份验证的详细信息。如下图所示，显示了使用的用户名。

其他详细信息如下：

- 时间戳
- Mac 地址

- 使用的策略集
- 验证策略
- 授权策略
- 其他有关资料



*ISE RADIUS*实时日志

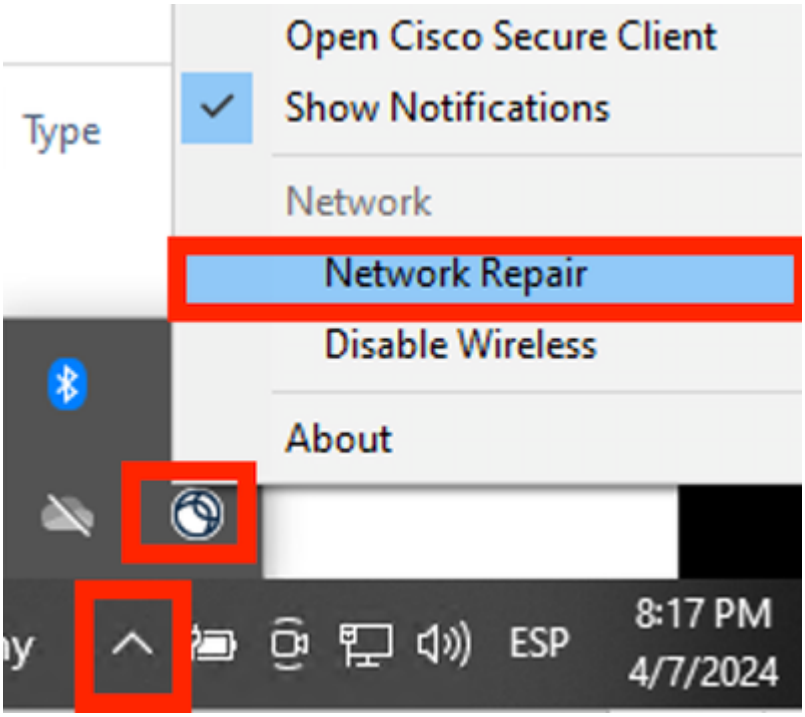
6.在此视图中，显示所有正确的策略，结果是身份验证状态成功。此命令可以确定配置是否正确。

故障排除

问题 1：安全客户端未使用NAM配置文件

1.如果新配置文件是在配置文件编辑器中创建的，而NAM未使用它，请对Secure Client使用Network Repair选项。

2.通过导航到Windows栏>单击扬抑图标>右键单击安全客户端图标>单击网络修复，可以找到此选项。



网络修复部分

问题 2：必须收集日志以便进一步分析

1.启用NAM扩展日志

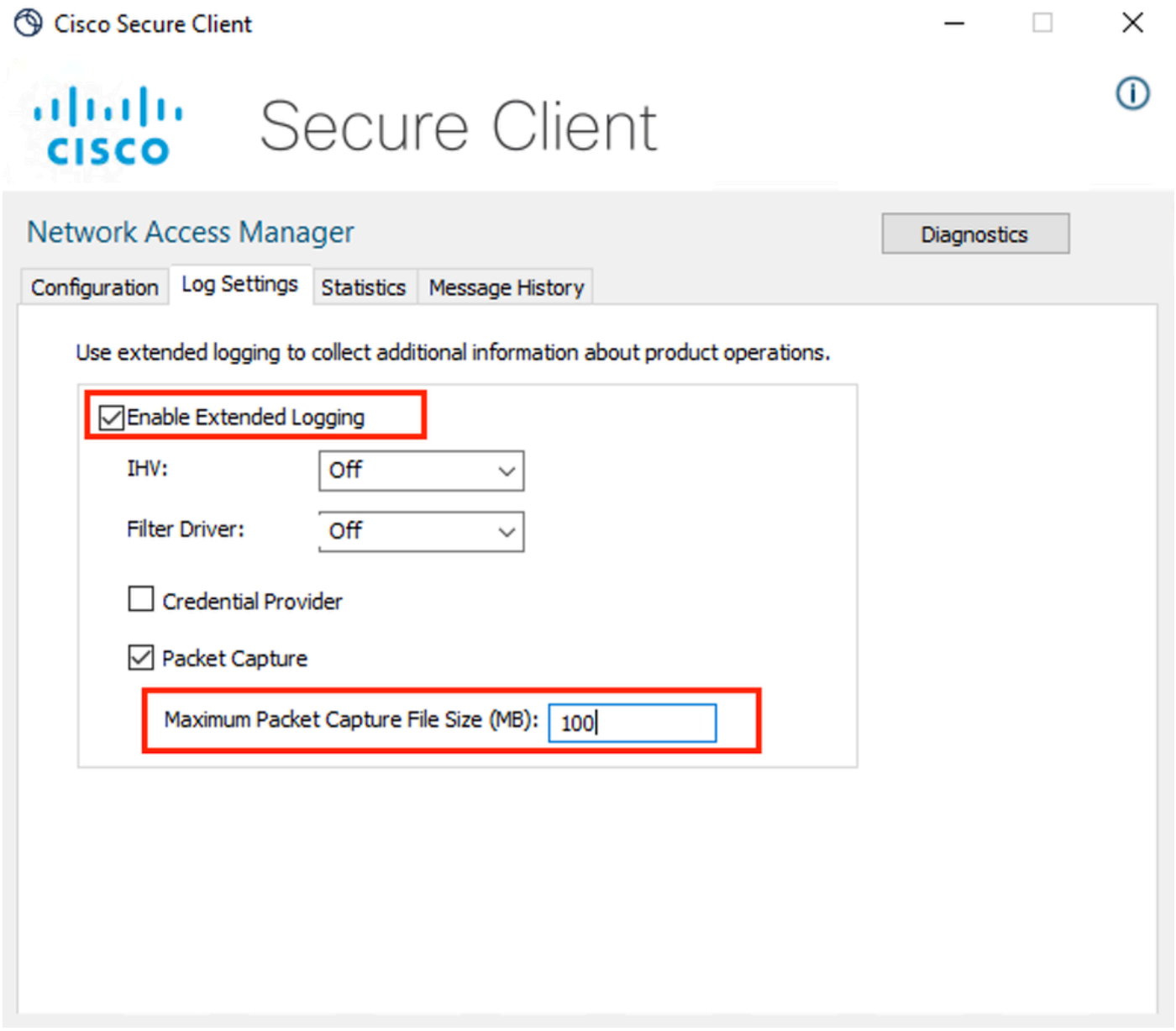
2.打开NAM，然后单击齿轮图标。



NAM接口

3.定位至日志设置标签。选中Enable Extended Logging复选框。

4.将Packet Capture File Size设置为100 MB。



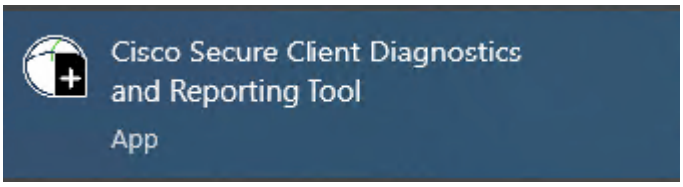
安全客户端NAM日志设置

重现问题

5.启用扩展日志记录后，多次重现该问题，以确保生成日志并捕获流量。

收集安全客户端DART套件

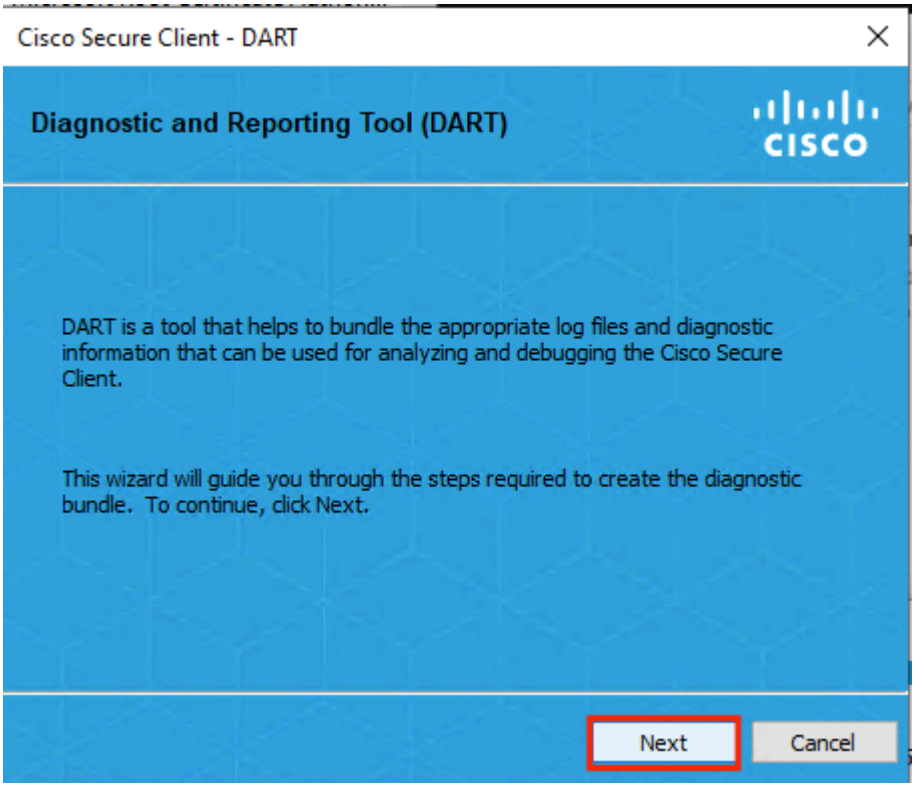
6.从Windows导航到搜索栏并键入：Cisco Secure Client Diagnostics and Reporting Tool。



DART模块

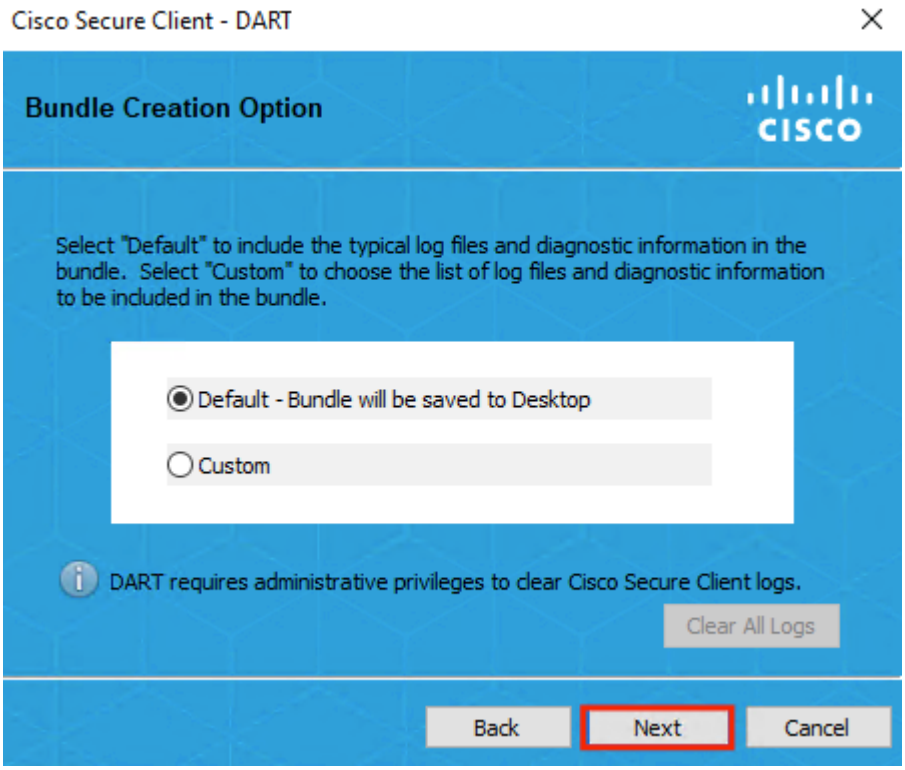
7.在安装过程中，您还安装了此模块。该工具通过收集日志和相关dot1x会话信息在故障排除过程中提供帮助。

8.单击第一个窗口中的下一步。



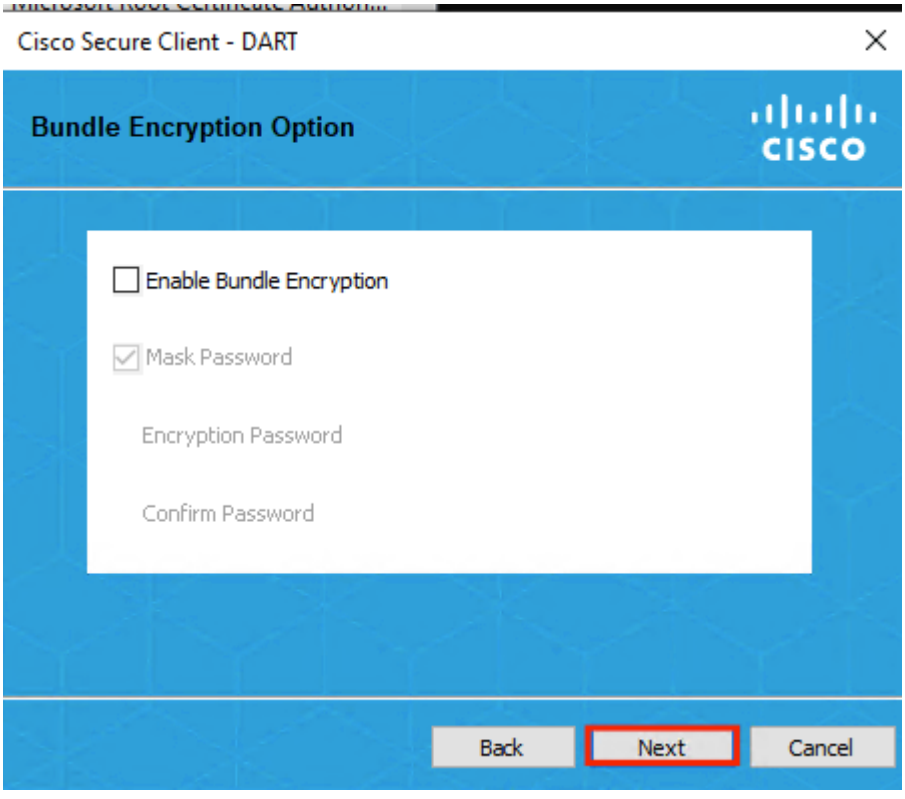
DART模块

9.单击Next，这样日志捆绑包可以保存在桌面上。



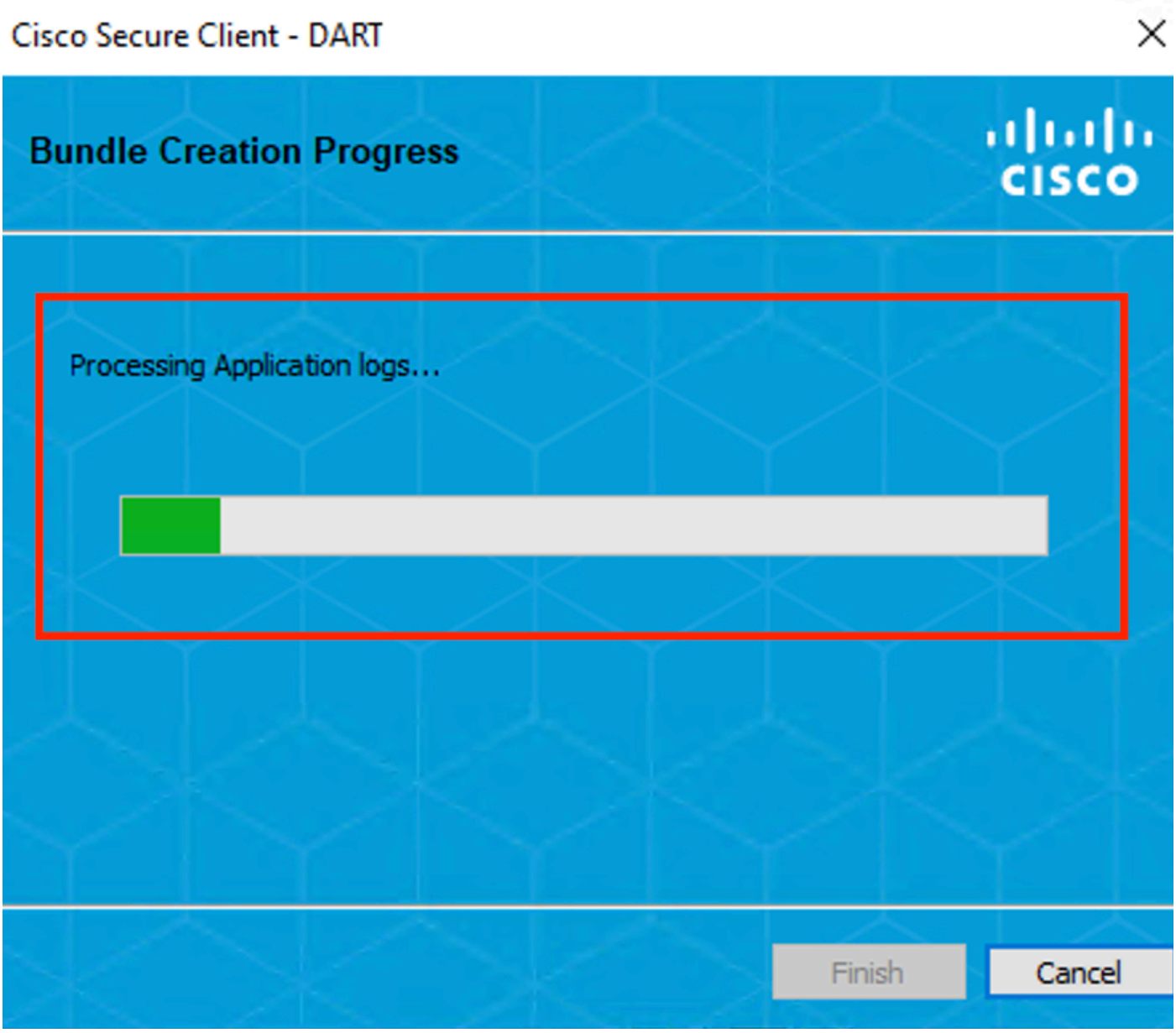
DART模块

10.如有必要，请点击启用捆绑加密复选框。



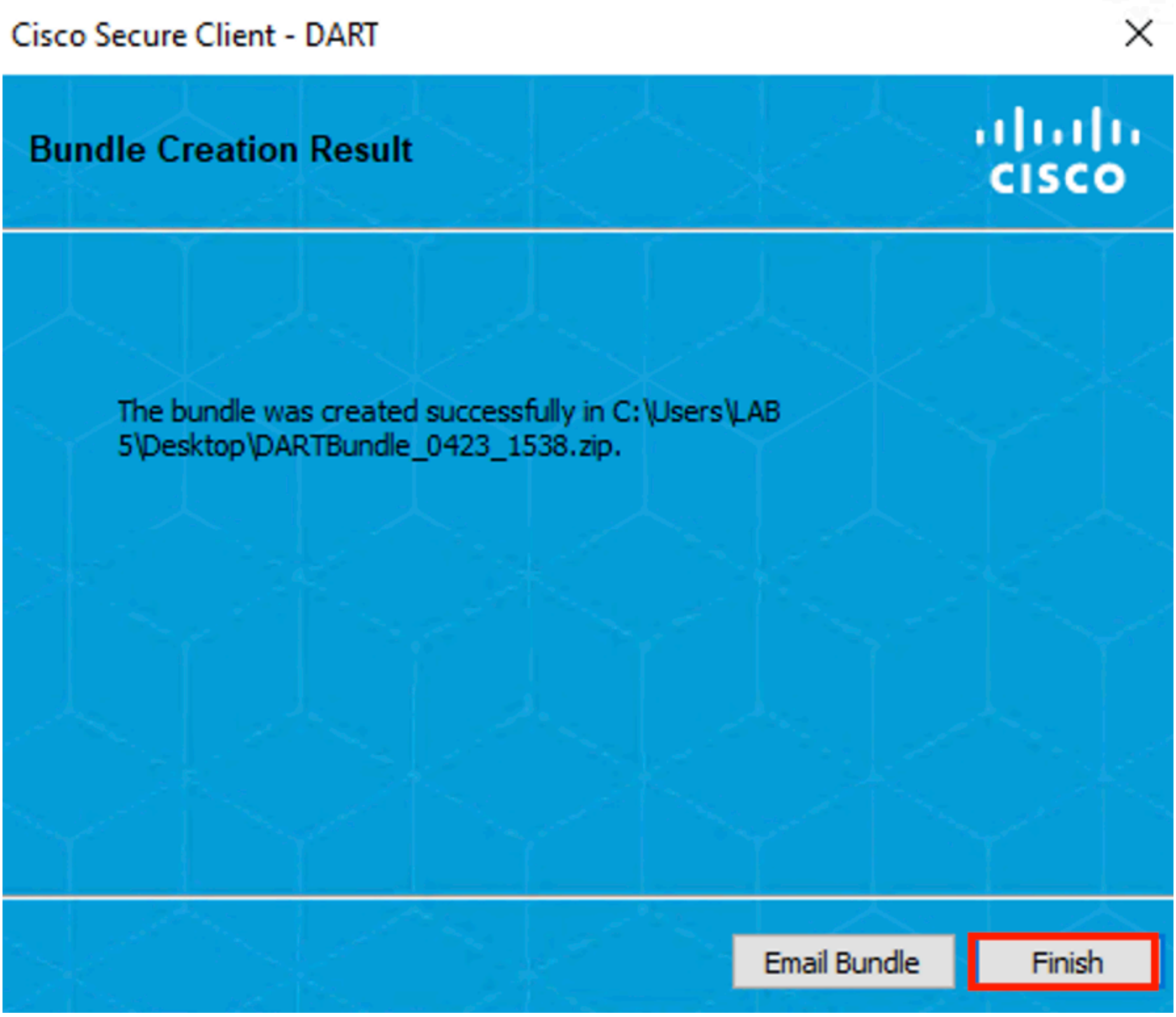
DART模块

11. DART日志收集开始。



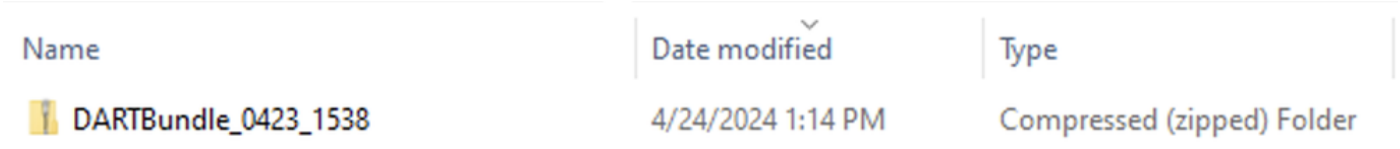
DART日志集合

12.整个过程可能需要10分钟左右才能完成。



DART捆绑包创建结果

13.DART结果文件可在桌面目录中找到。



DART结果文件

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。