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

配置

- 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. 方案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：为EAP-FAST同步用户和计算机身份验证配置安全客户端NAM请求方
  - 6. 方案3：为EAP TLS用户证书身份验证配置安全客户端NAM请求方
  - 7. 配置ISR 1100和ISE以允许基于方案1 PEAP MSCHAPv2的身份验证

验证

故障排除

- 问题：安全客户端未使用NAM配置文件。
- 问题2：需要收集日志以进行进一步分析。
  - 1. 启用NAM扩展日志记录
  - 2. 重现问题。
  - 3. 收集安全客户端DART捆绑包。

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：

- 基本了解什么是RADIUS请求方
- 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，内置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，还举例说明了如何实现这一点。

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“请求方”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。

关于网络访问管理器

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。它可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。

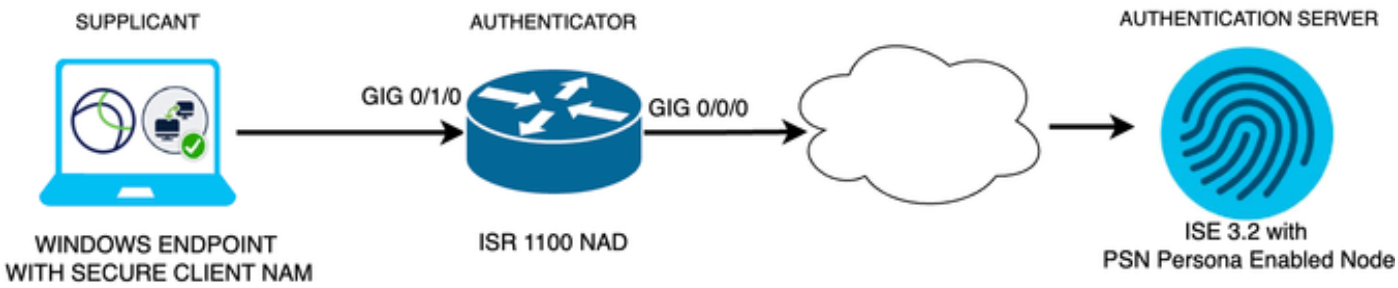
网络接入管理器设计为单宿主，一次只允许一个网络连接。此外，有线连接的优先级高于无线连接，因此，如果通过有线连接接入网络，无线适配器将因没有IP地址而被禁用。

配置

网络图

对于dot1x身份验证，需要三个部分；可以执行dot1x的请求方，身份验证器（也称为NAS/NAD，充当在RADIUS内封装dot1x流量的代理）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. 场景1：配置用于PEAP (MS-CHAPv2)用户身份验证的安全客户端NAM请求方。
5. 方案2：在配置用户和计算机身份验证时，为EAP-FAST同时配置安全客户端NAM请求方。
6. 方案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NAD和ISE演示。

1. 下载并安装安全客户端NAM（网络访问管理器）

思科软件下载

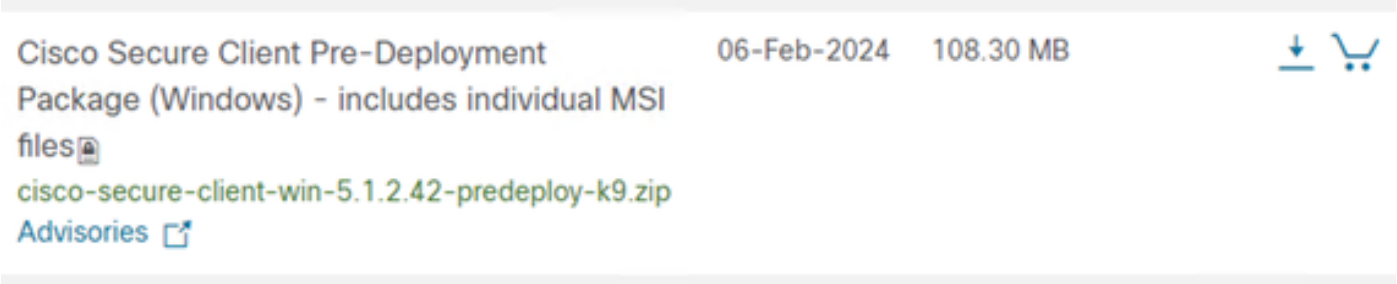
在产品名称搜索栏中，键入Secure Client 5。

依次下载主页(Home) >安全(Security) > VPN和终端安全客户端(VPN and Endpoint Security Clients) >安全客户端（包括AnyConnect） >安全客户端5 > AnyConnect VPN客户端软件(AnyConnect VPN Client Software)。

在此配置示例中，使用的是5.1.2.42版。

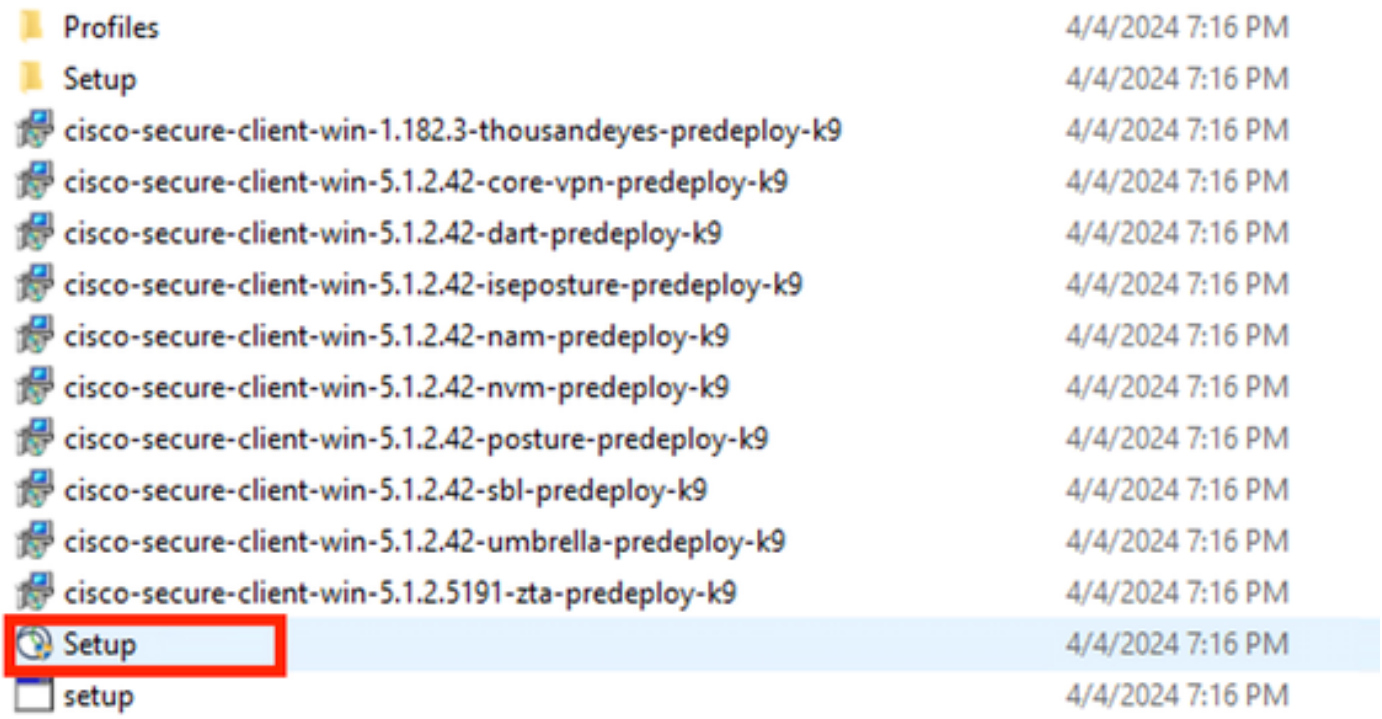
有多种方法可将安全客户端部署到Windows设备；从SCCM、从身份服务引擎和VPN前端。但是，本文采用的安装方法是预部署方法。

在页面上，搜索文件Cisco Secure Client Headend Deployment Package (Windows)。



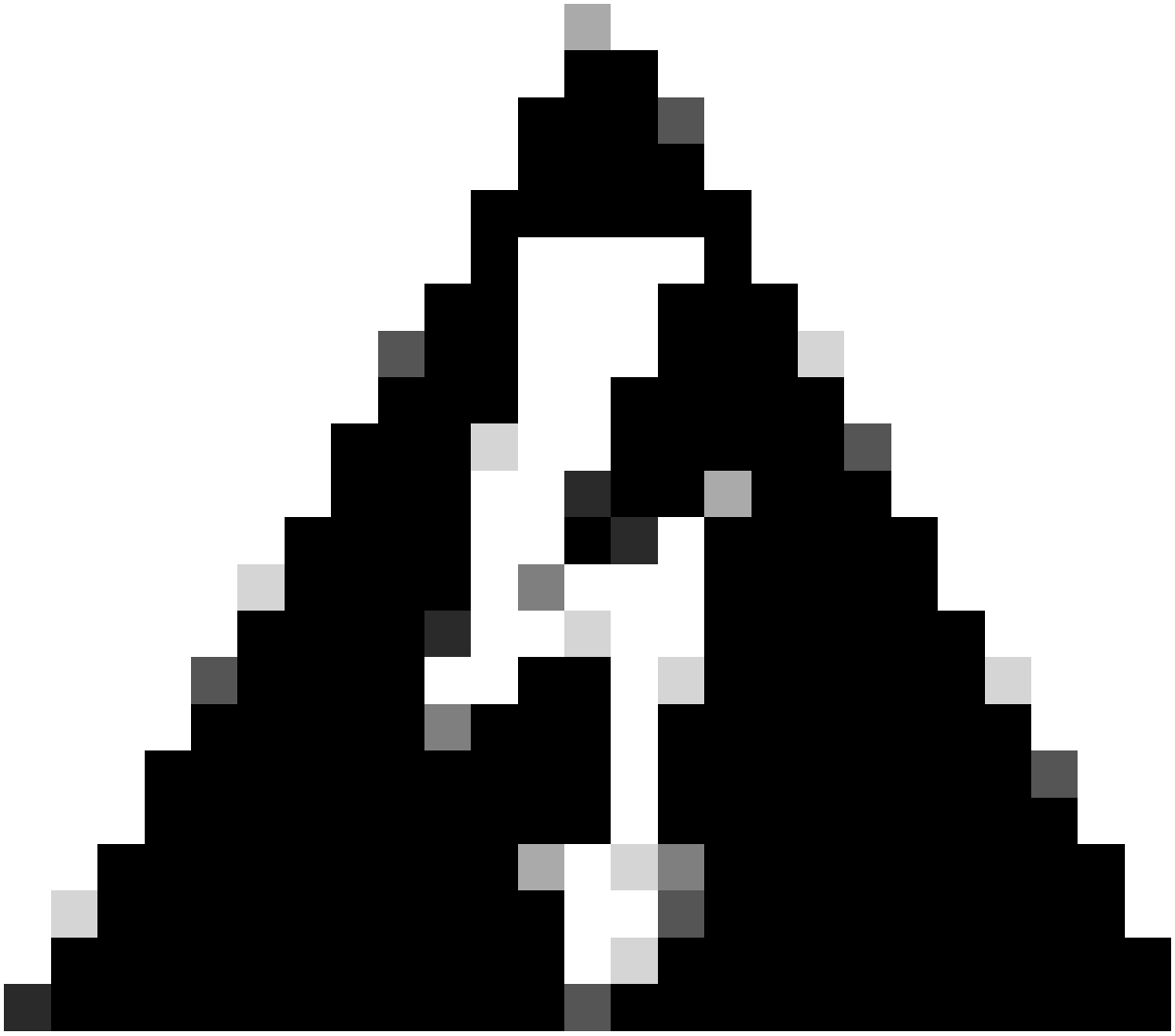
*Msi zip*文件

下载并解压后，单击Setup。

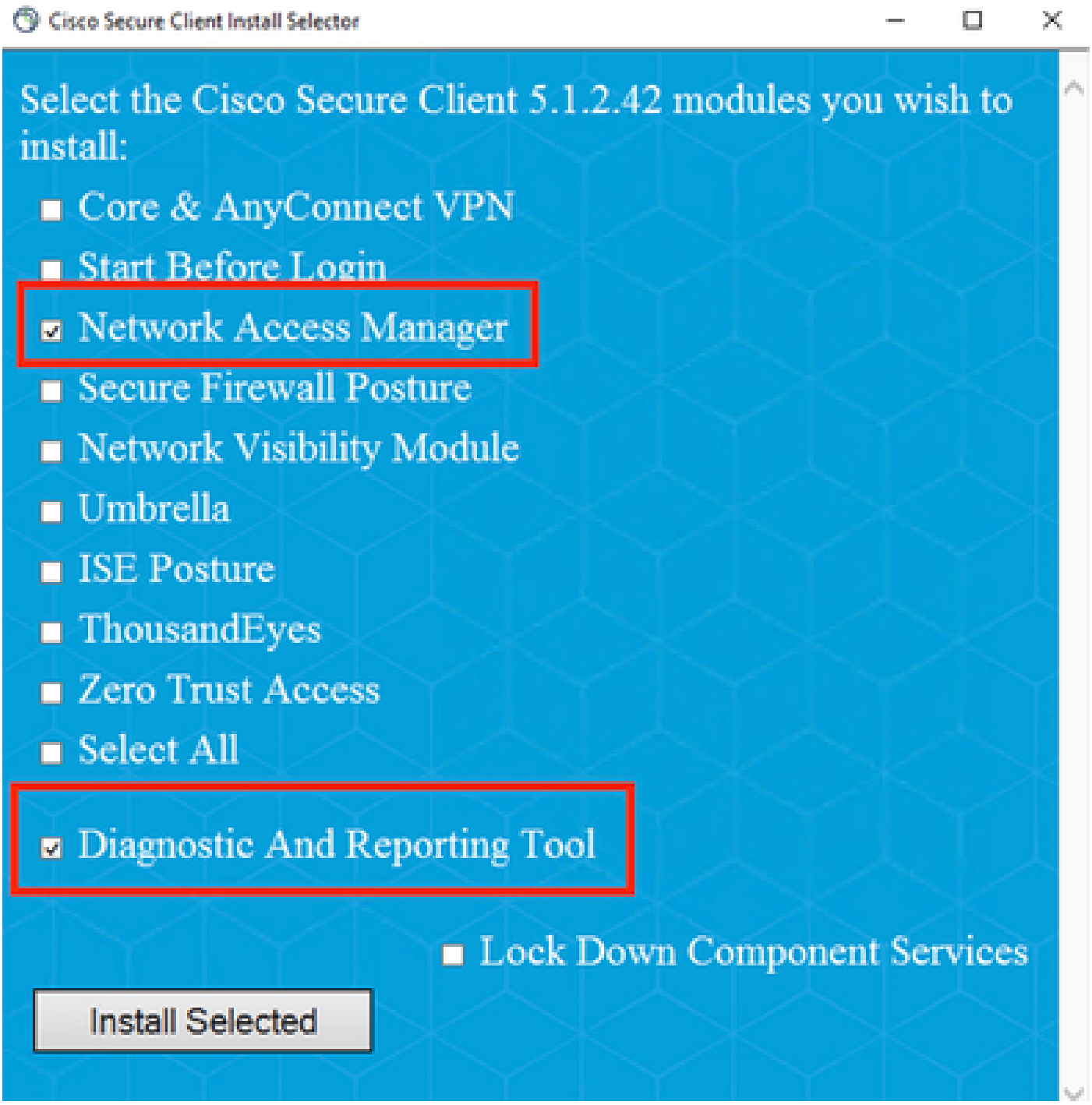


安全客户端文件

安装网络访问管理器和诊断和报告工具模块。



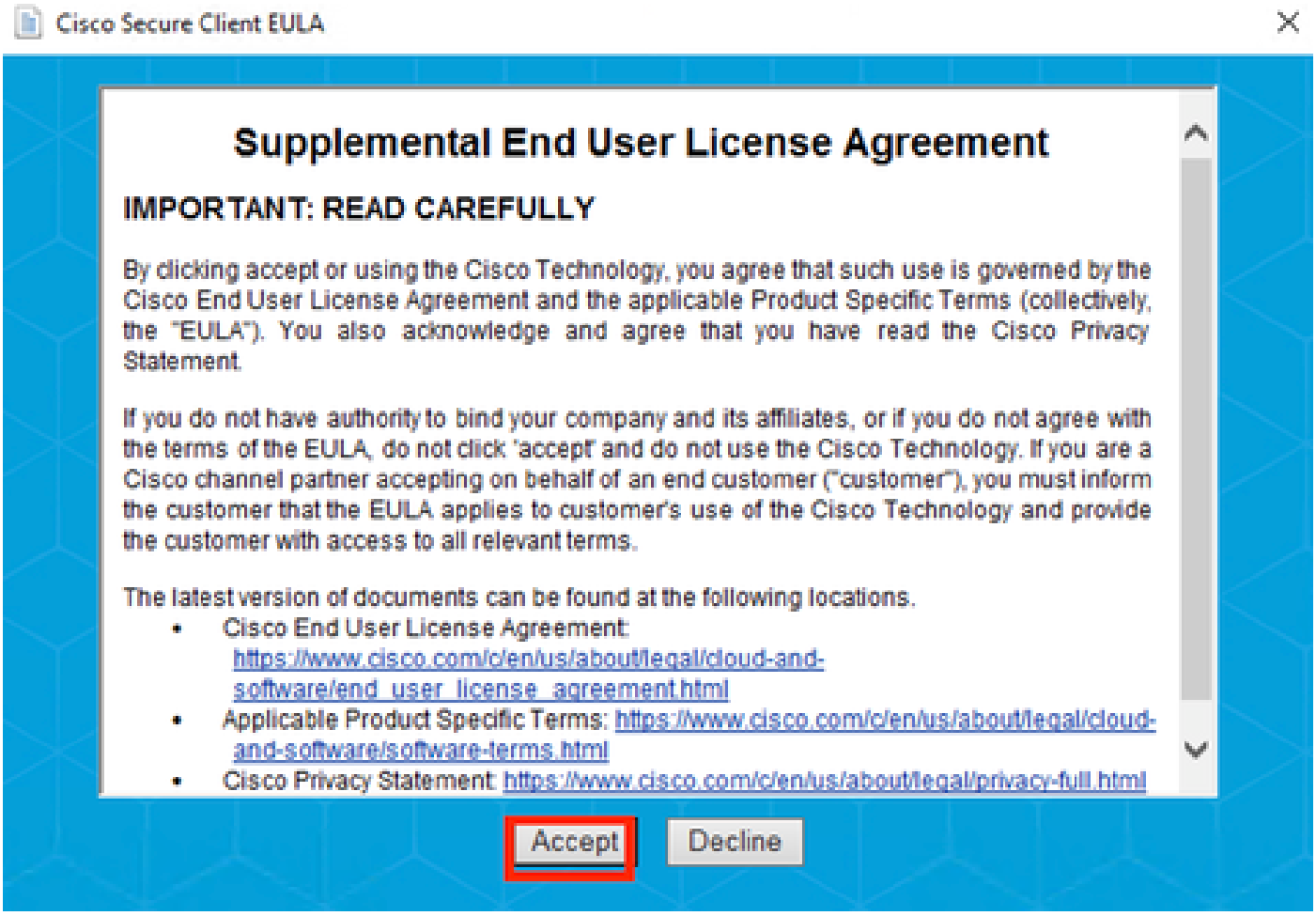
警告：如果使用Cisco Secure Client向导，VPN模块将自动安装并隐藏在GUI中。如果未安装VPN模块，则NAM不起作用。如果使用单个MSI文件或不同的安装方法，请确保安装VPN模块。



安装选择器

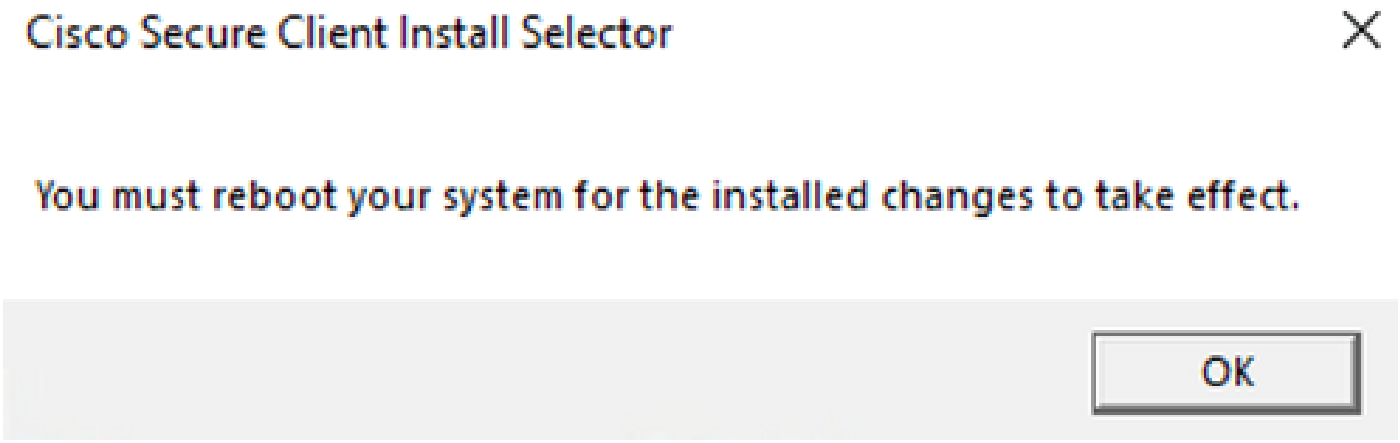
点击安装选定模块。

接受EULA。



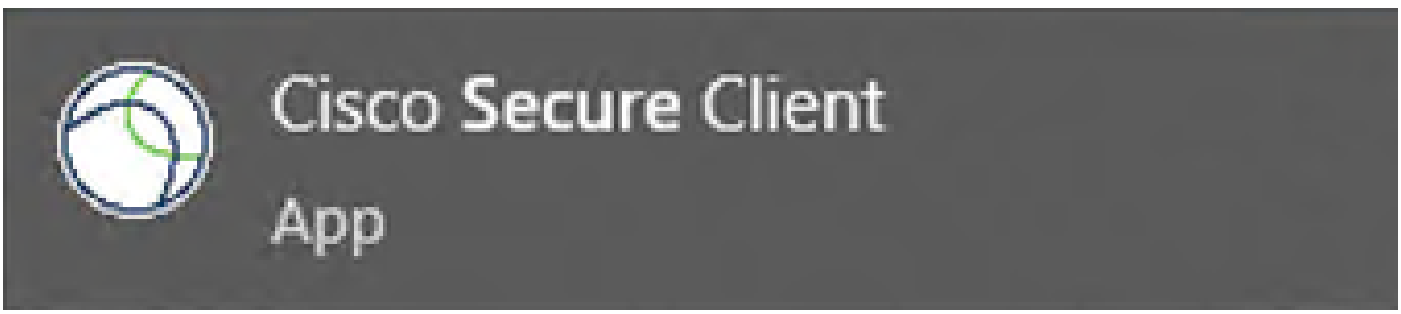
*EULA*窗口

安装NAM后需要重新启动。



重新启动要求窗口

安装后，可从Windows搜索栏找到并打开它。



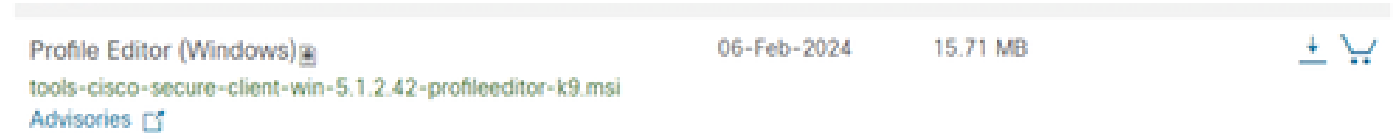
安全客户端程序

2. 下载并安装安全客户端NAM配置文件编辑器。

配置Dot1x首选项需要思科网络访问管理器配置文件编辑器。

在下载Secure Client的同一页面上，可以找到Profile Editor选项。

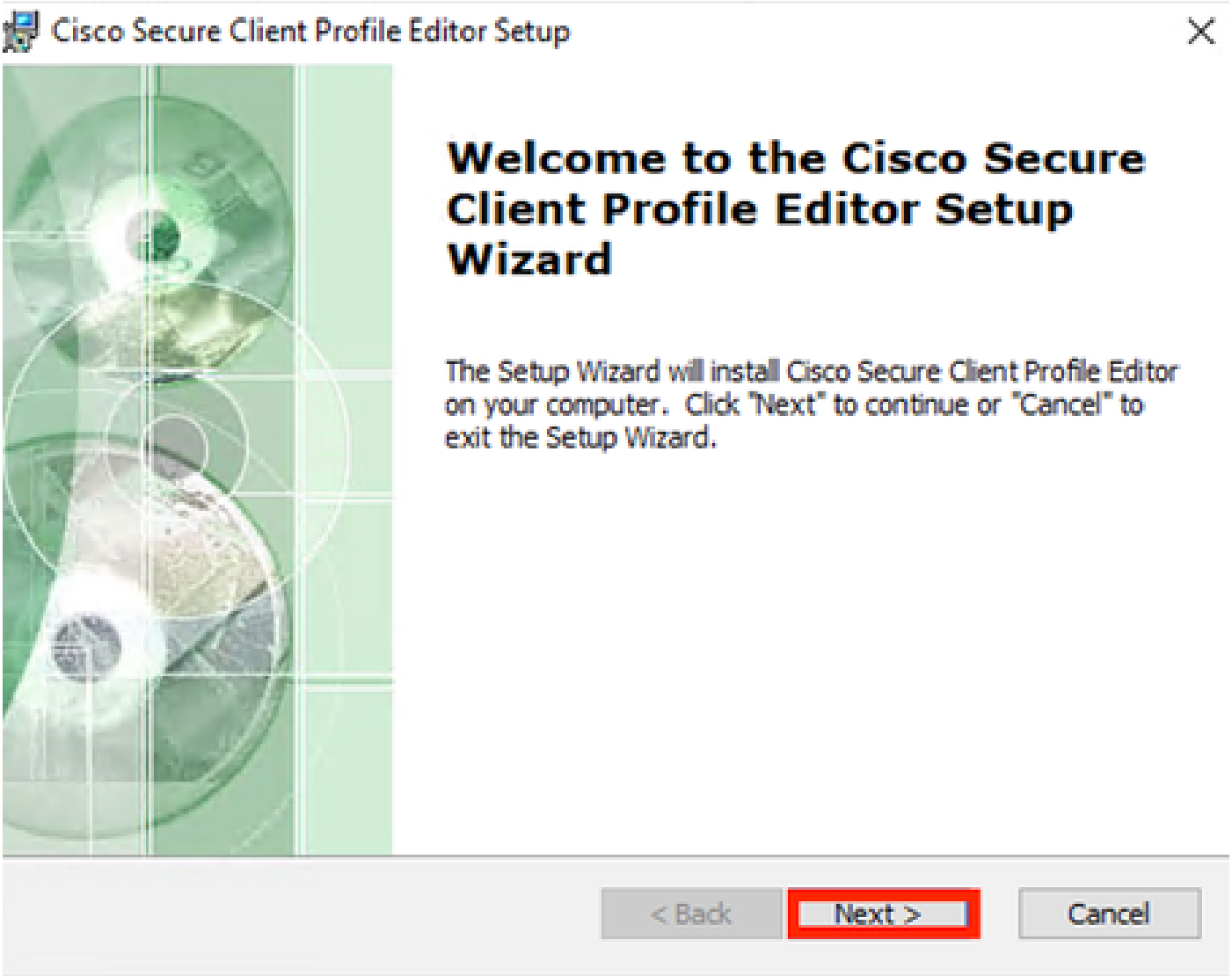
本示例使用版本5.1.2.42中的选项。



配置文件编辑器

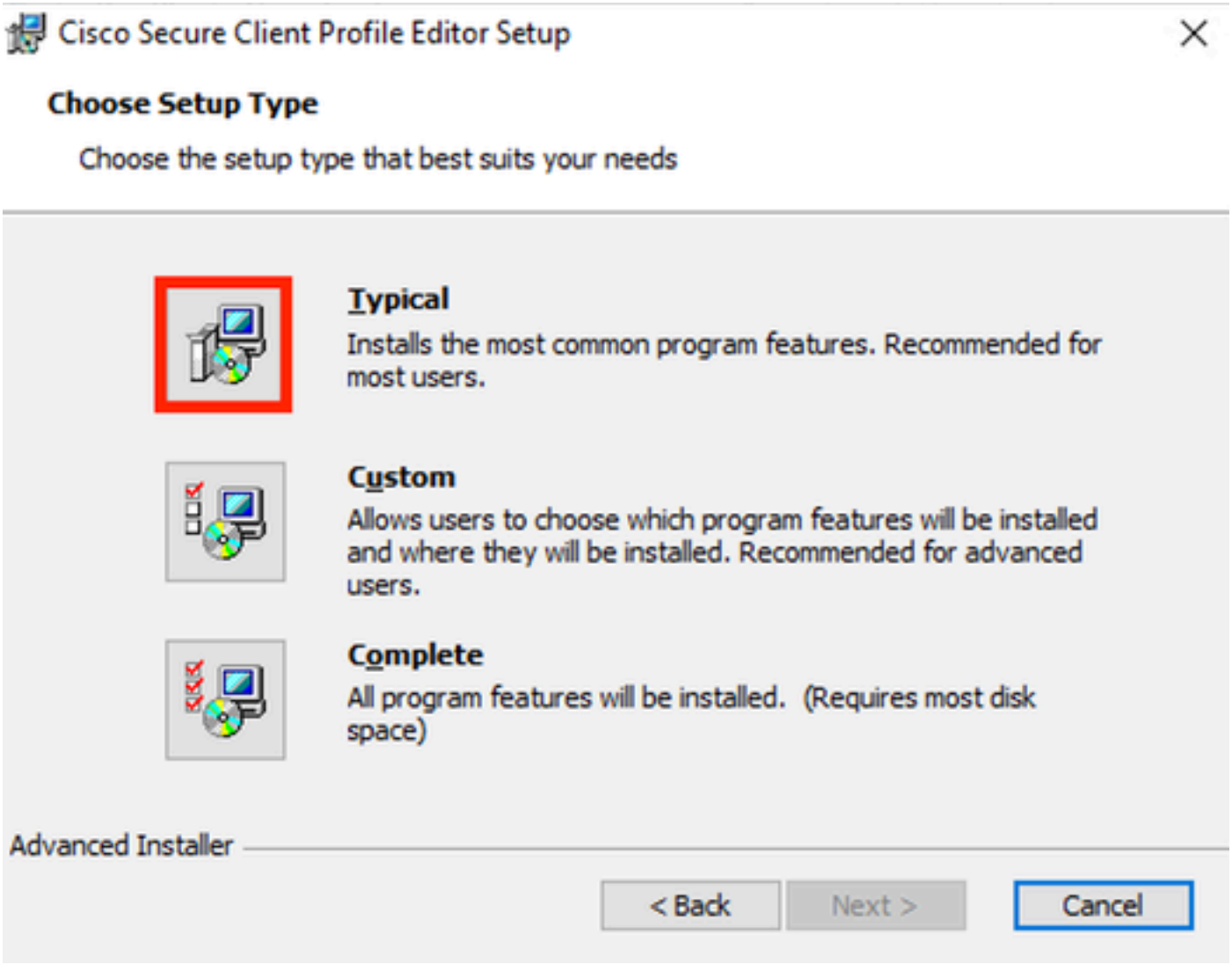
下载完成后，继续进行安装。

运行msi文件。

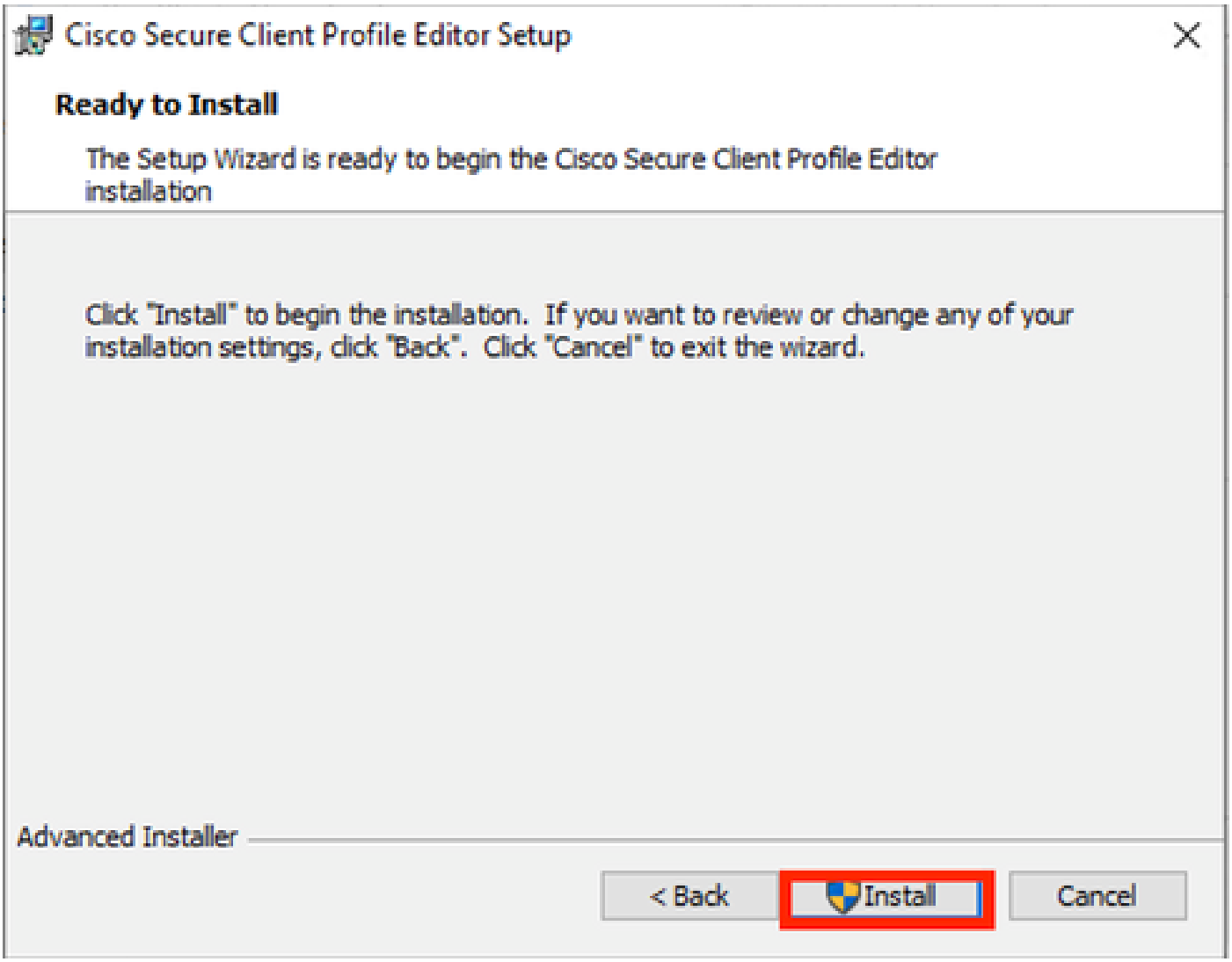


配置文件编辑器设置窗口

使用典型设置选项。

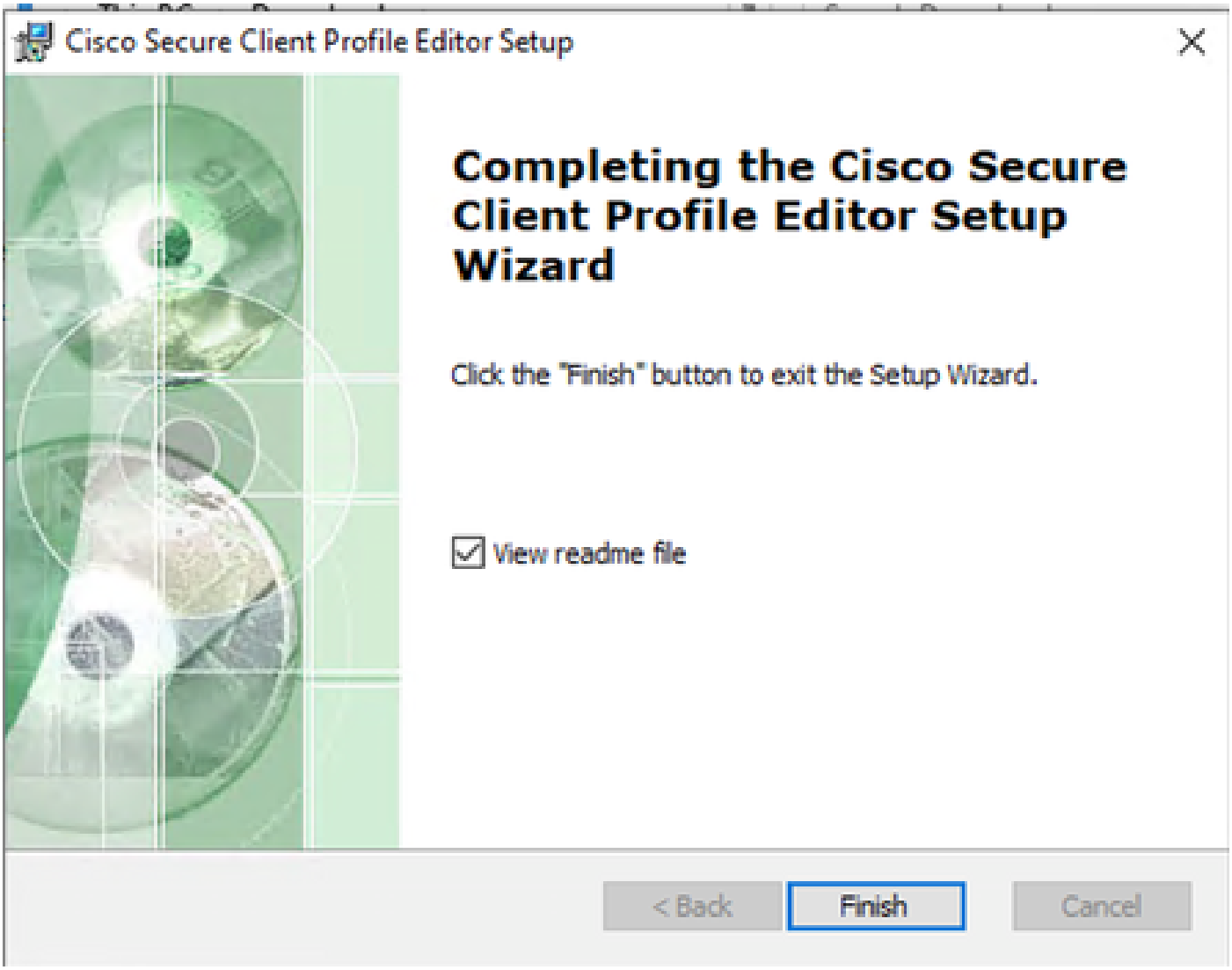


配置文件编辑器设置


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

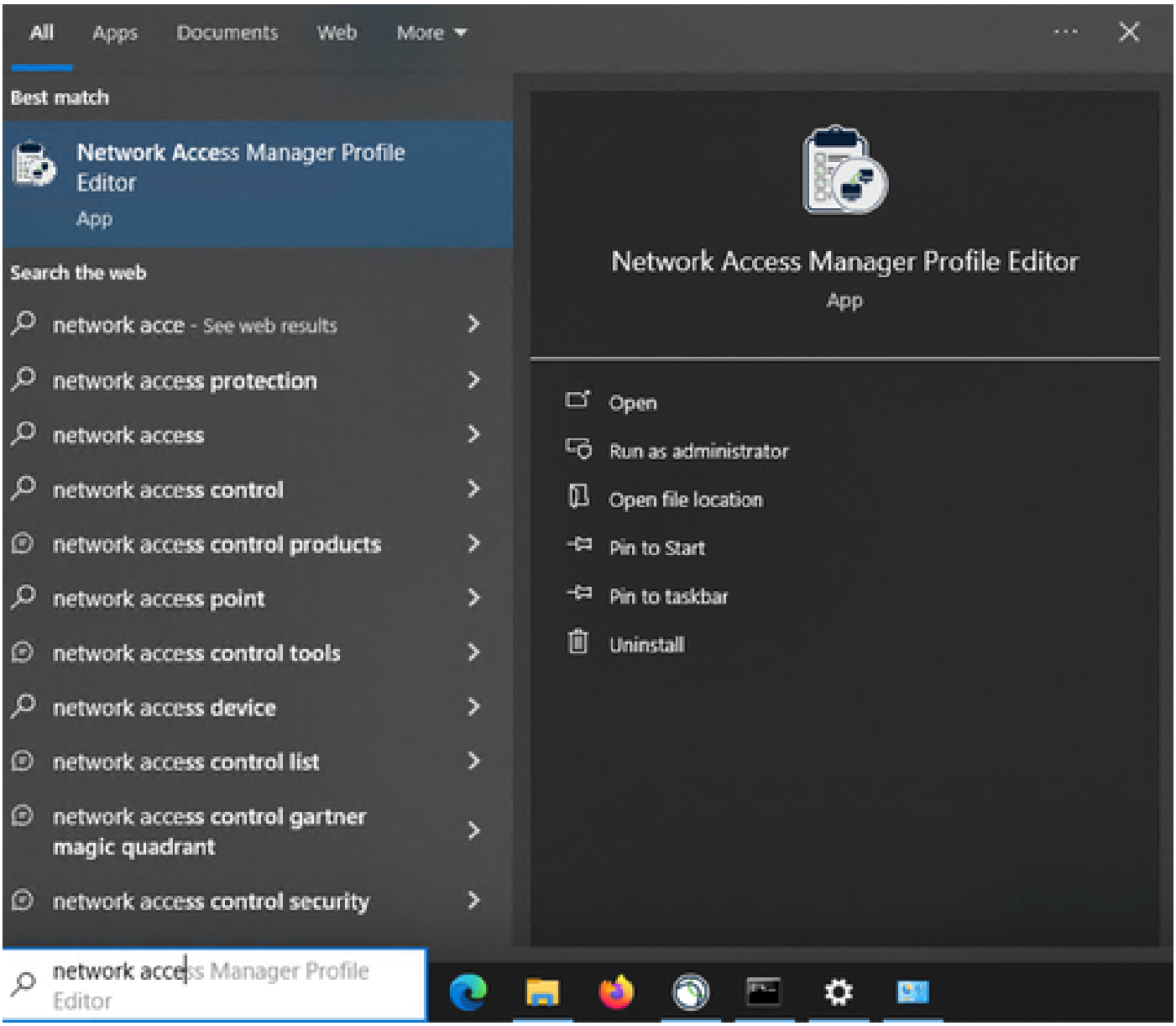
安装窗口

单击 完成。



配置文件编辑器设置结束

安装完成后，从搜索栏打开网络访问管理器配置文件编辑器。



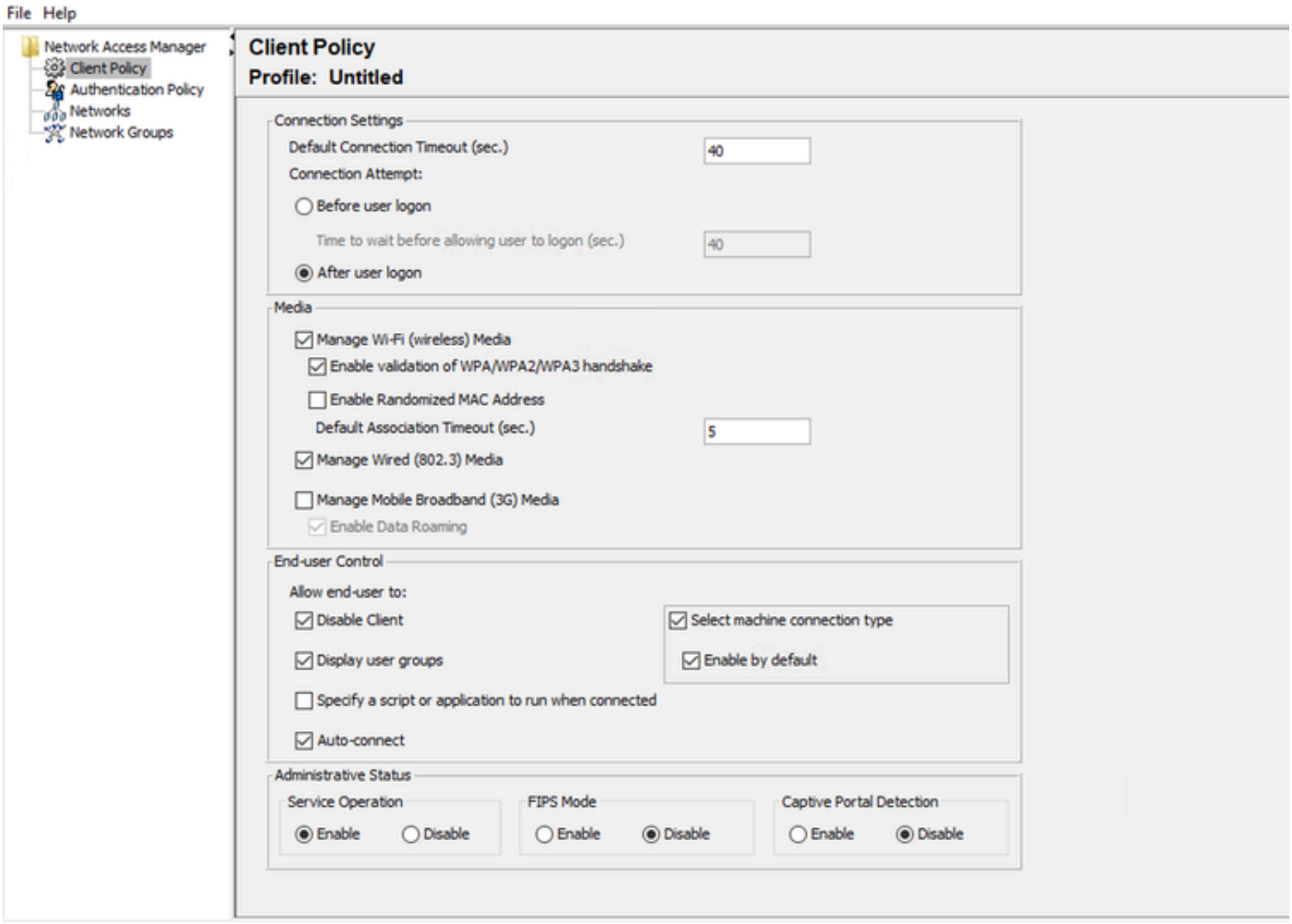
搜索栏上的NAM配置文件编辑器

网络访问管理器和配置文件编辑器的安装已完成。

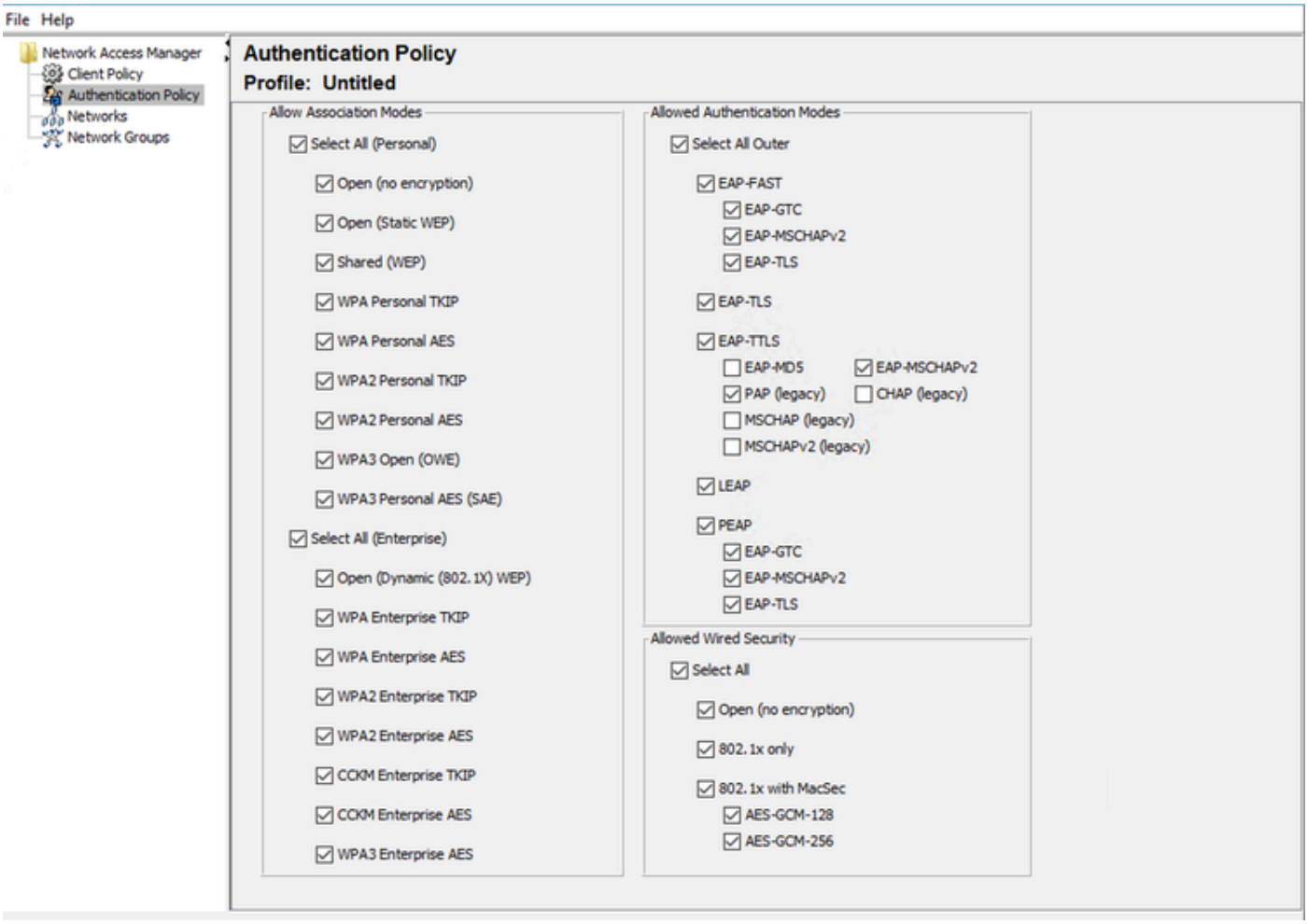
3. 常规默认配置

本文中介绍的所有场景都包含下列配置：

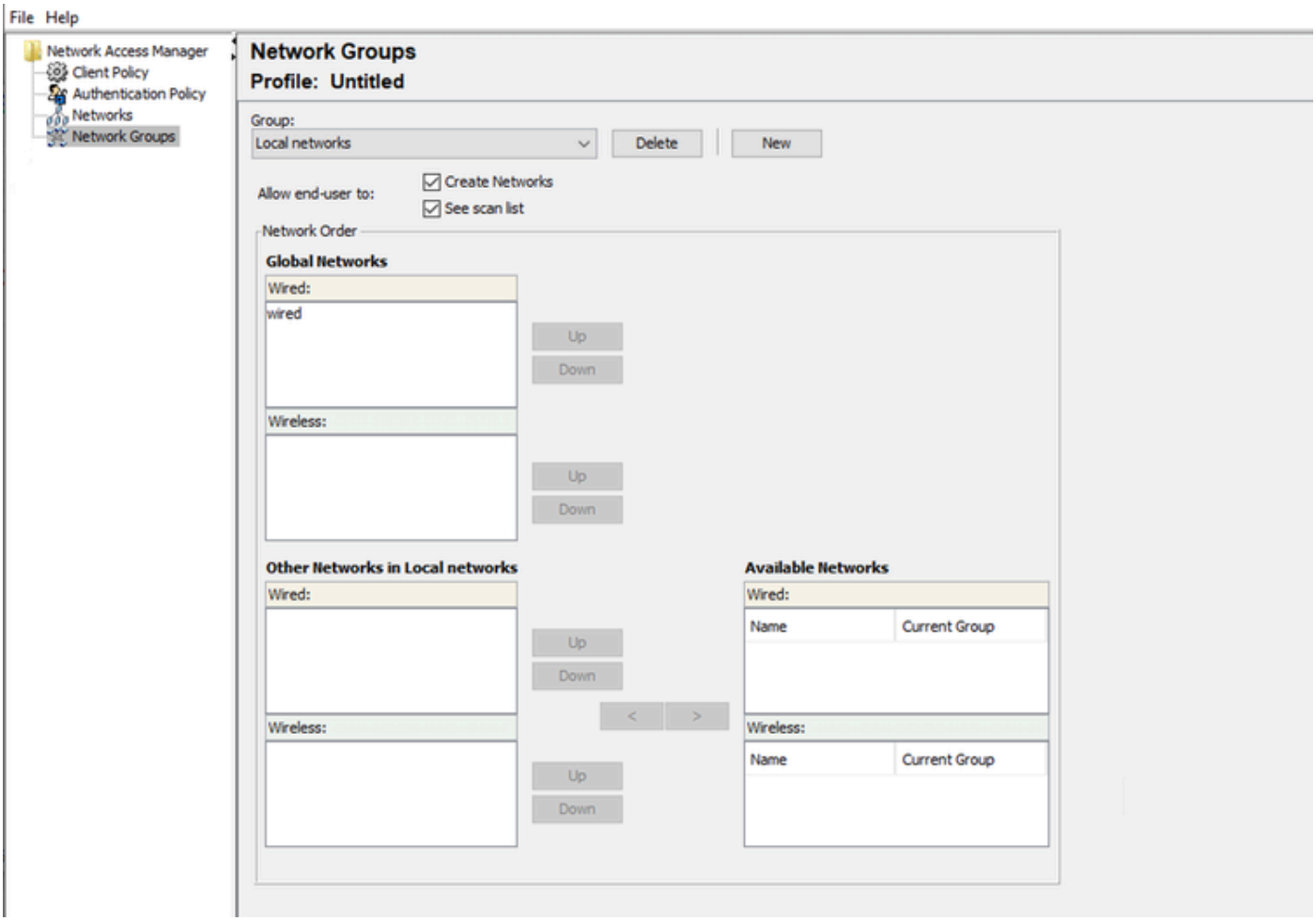
- 客户端策略
- 验证策略
- 网络组



*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



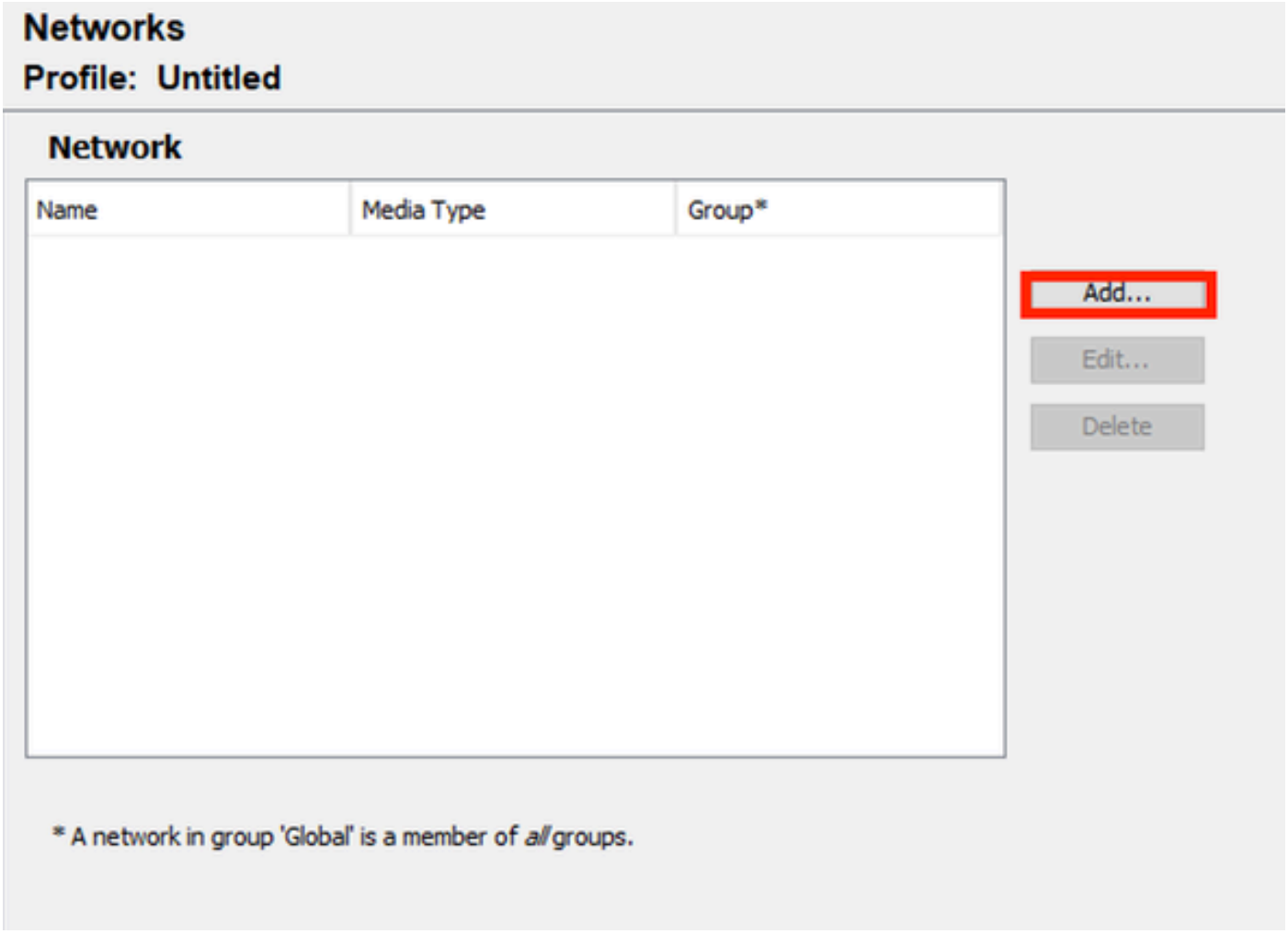
“网络组”选项卡

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

导航到网络部分。

可以删除默认的网络配置文件。

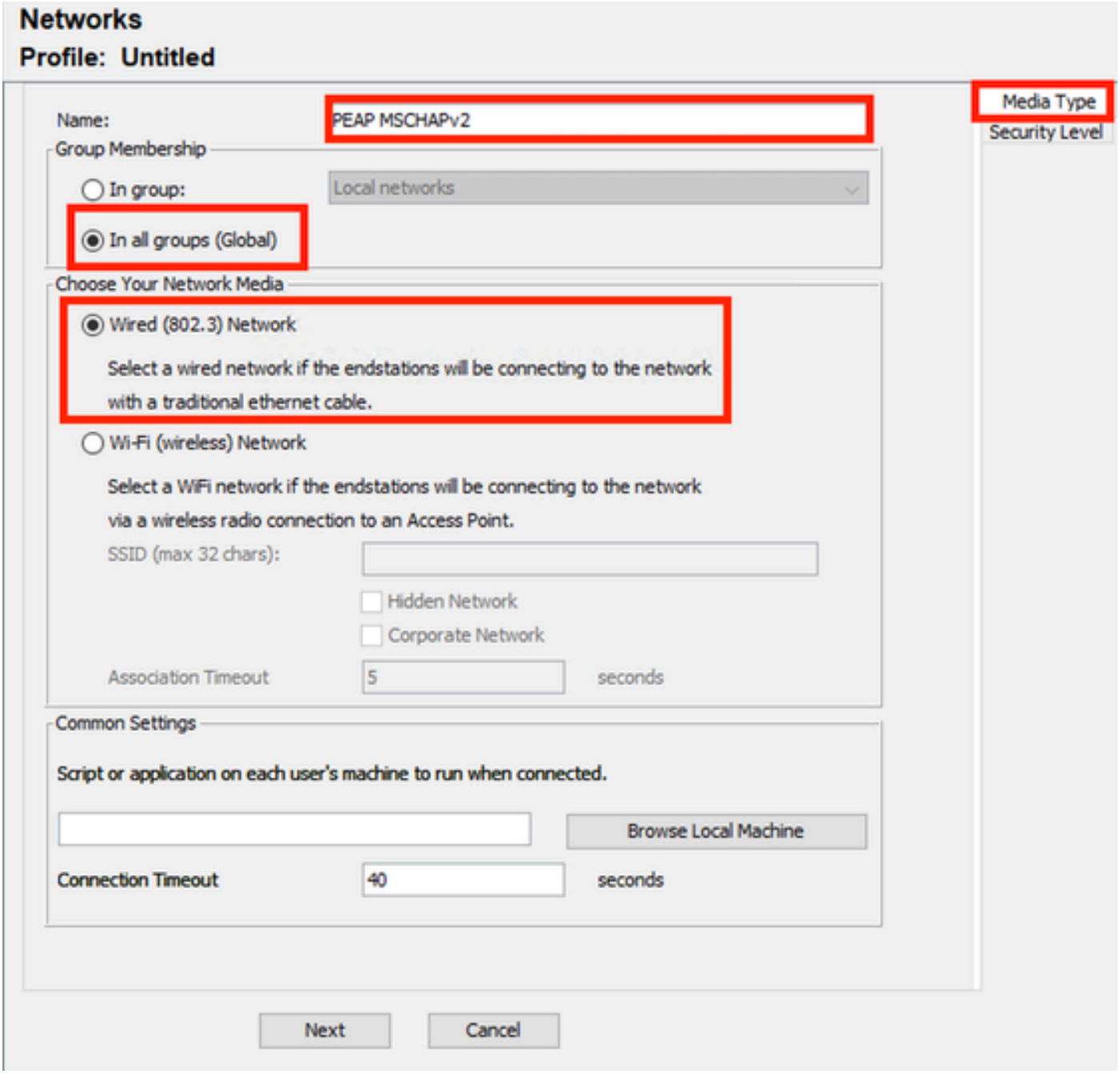
单击 Add。



网络配置文件创建

为Network配置文件命名。

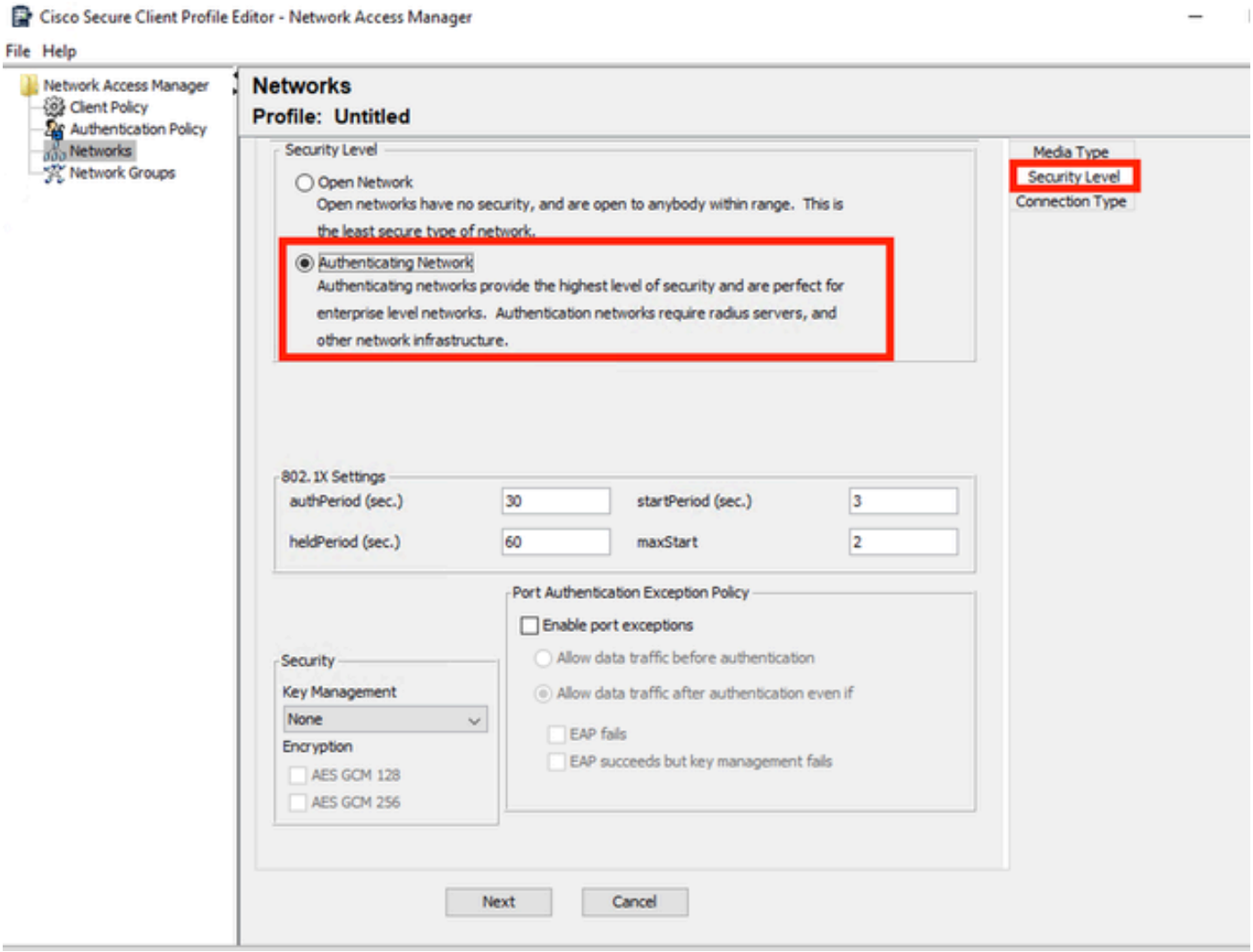
为Group Membership选择Global。选择有线网络介质。



网络配置文件媒体类型部分

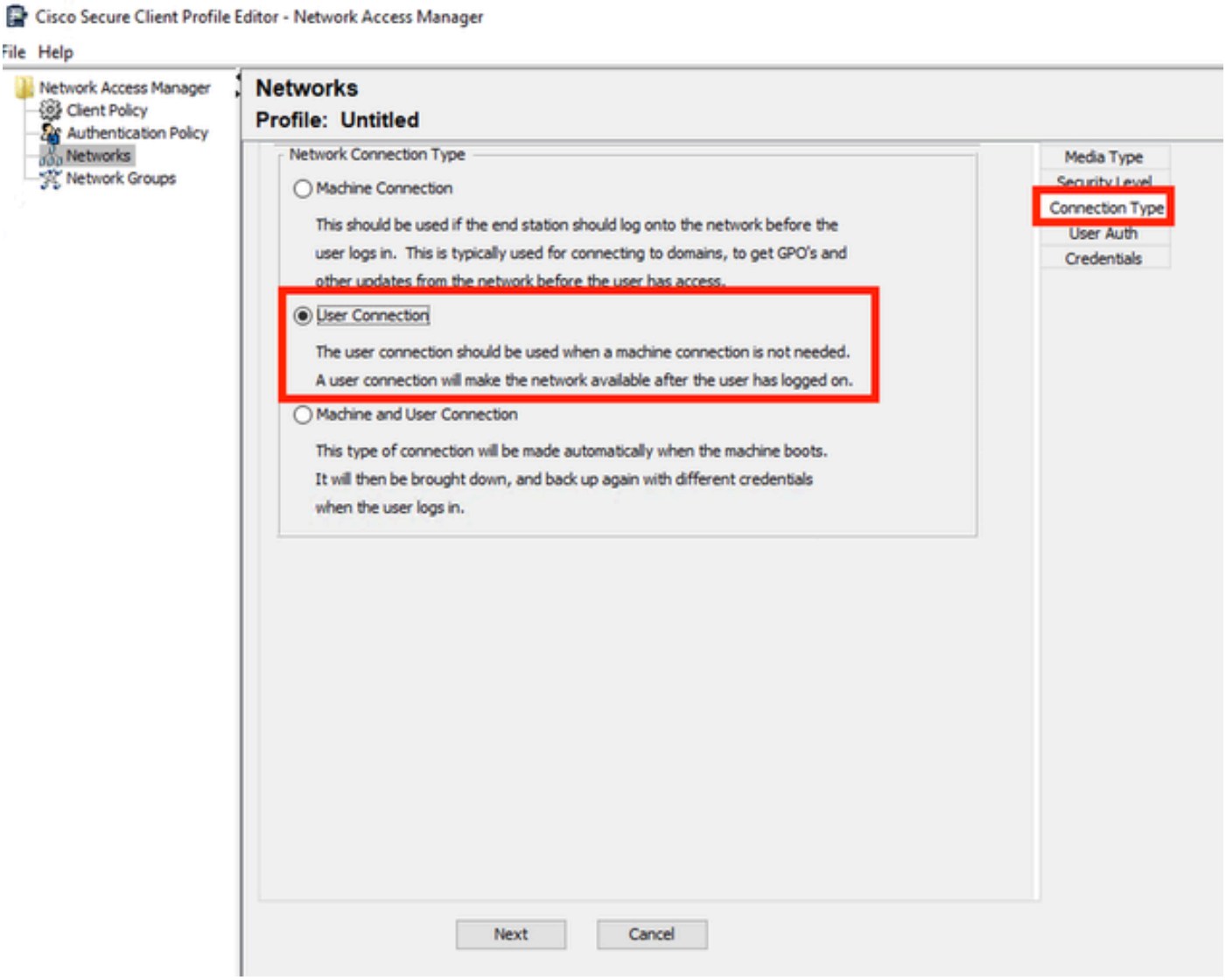
单击 Next。

选择Authenticating Network，并使用Security Level部分中其余选项的默认值。



网络配置文件安全级别

单击Next继续执行Connection Type部分。

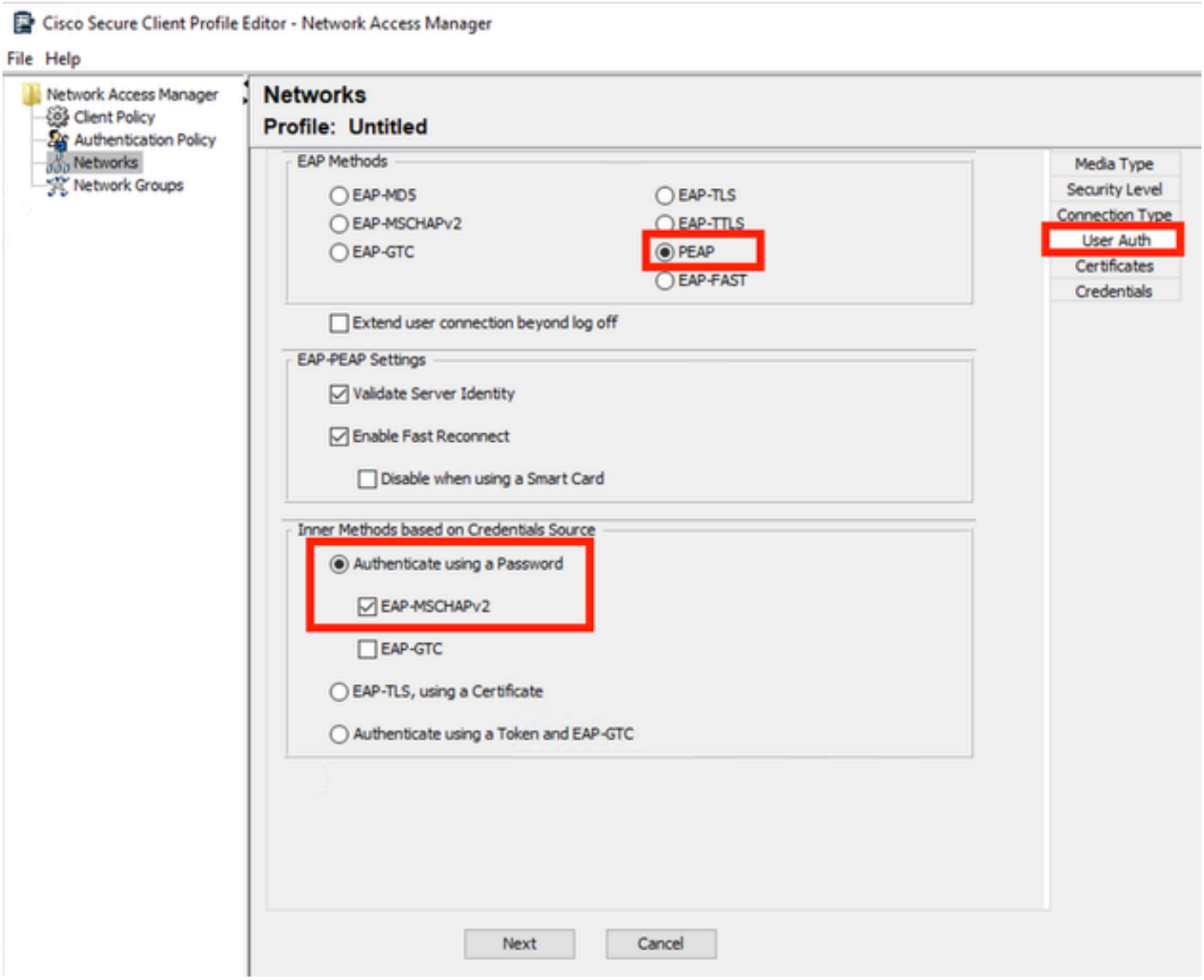


网络配置文件连接类型

选择User Connection连接类型。

点击下一步以继续参阅现在可用的用户身份验证部分。

选择PEAP作为常规EAP方法。



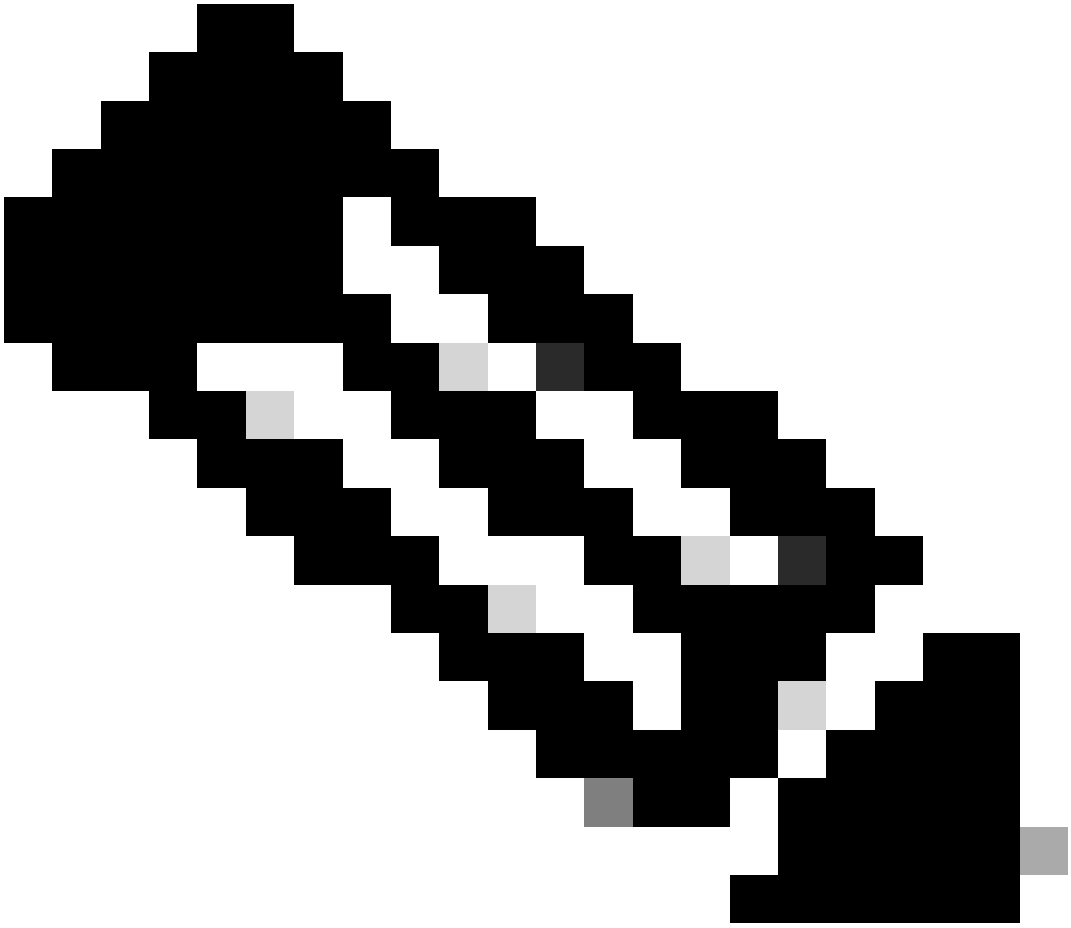
网络配置文件用户身份验证

请勿更改EAP-PEAP Settings中的默认值。

继续执行基于凭据源的内部方法部分。

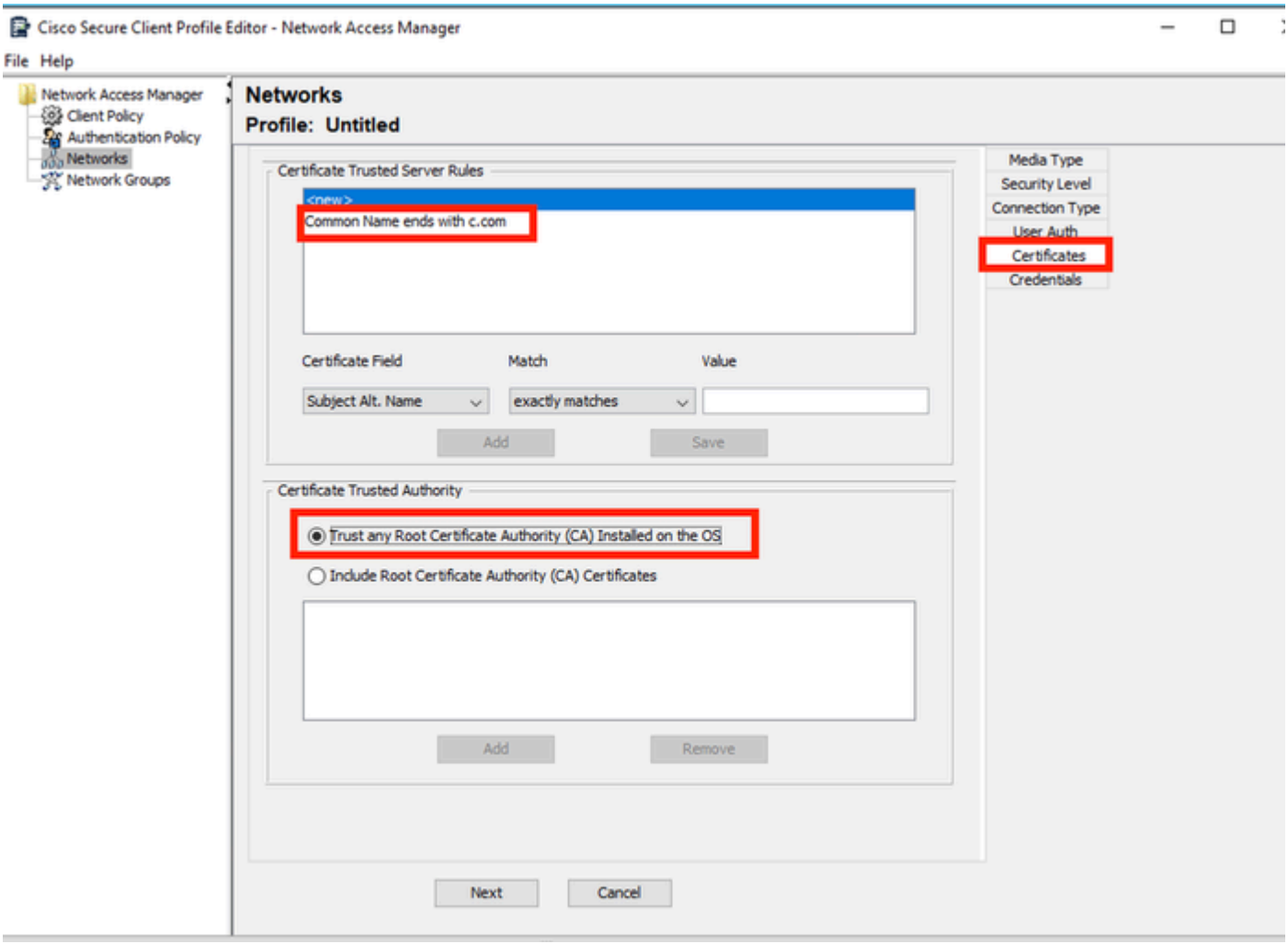
从EAP PEAP存在的多个内部方法中选择Authenticate using a Password，然后选择EAP-MSCHAPv2。

点击下一步以转到证书部分。



注意：由于选中了Validate Server Identity in EAP-PEAP Settings选项，因此将显示Certificate部分。对于EAP PEAP，它使用服务器证书进行封装。

在证书部分上，在证书受信任服务器规则中，使用规则公用名以c.com结尾。 此部分配置是指服务器在EAP PEAP流程期间使用的证书。如果在您的环境中使用身份服务引擎(ISE)，可以使用策略服务器节点EAP证书的公用名。

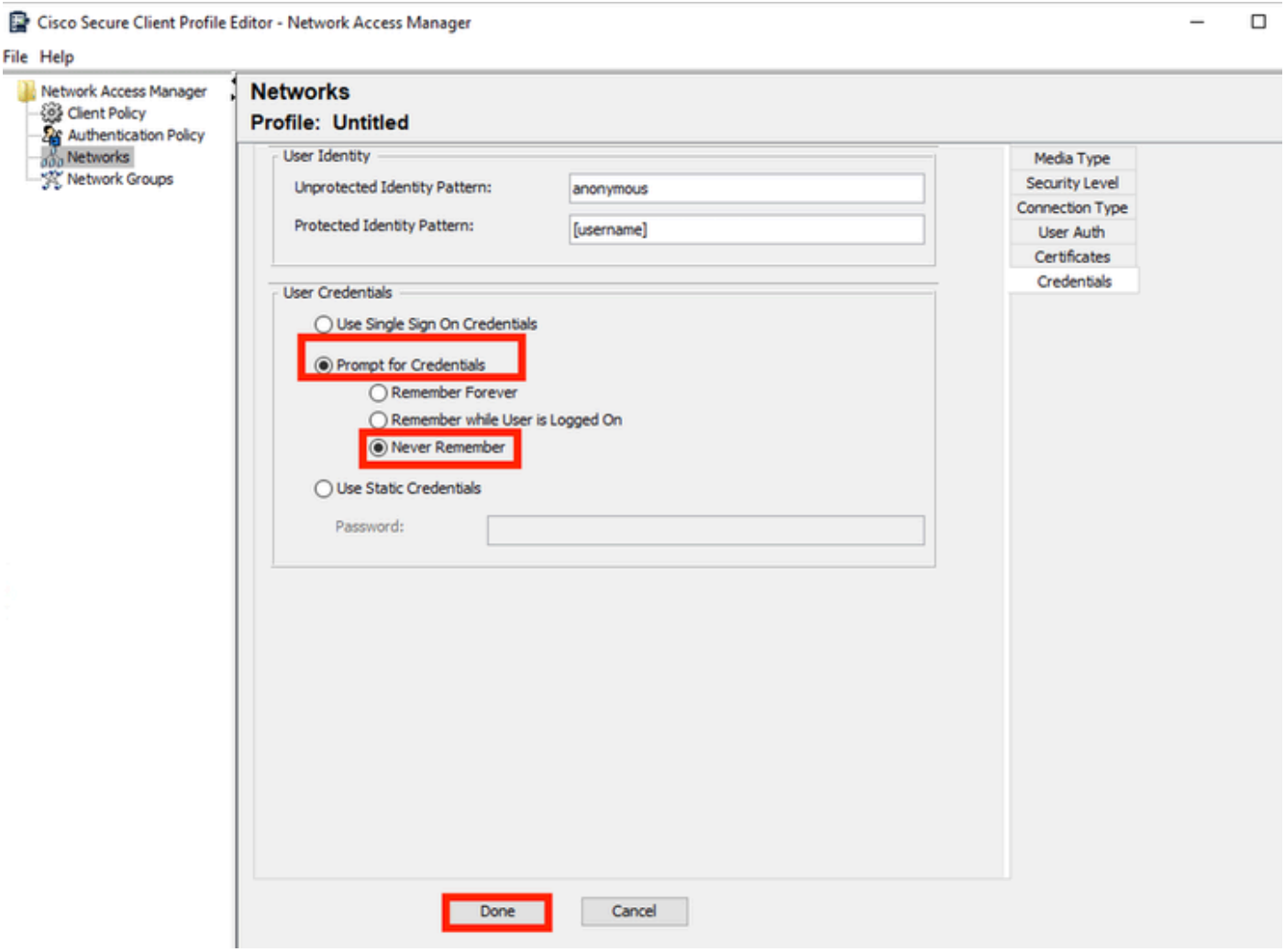


网络配置文件证书部分

可以在证书受信任颁发机构中选择两个选项。 对于此方案，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。

使用此选项，Windows设备将信任由“管理用户证书”程序“证书”— 当前用户>受信任的根证书颁发机构>证书中包含的证书签名的任何EAP证书。

单击 Next。



Network Profile Credentials部分

在凭据部分中，只有用户凭据部分被更改。

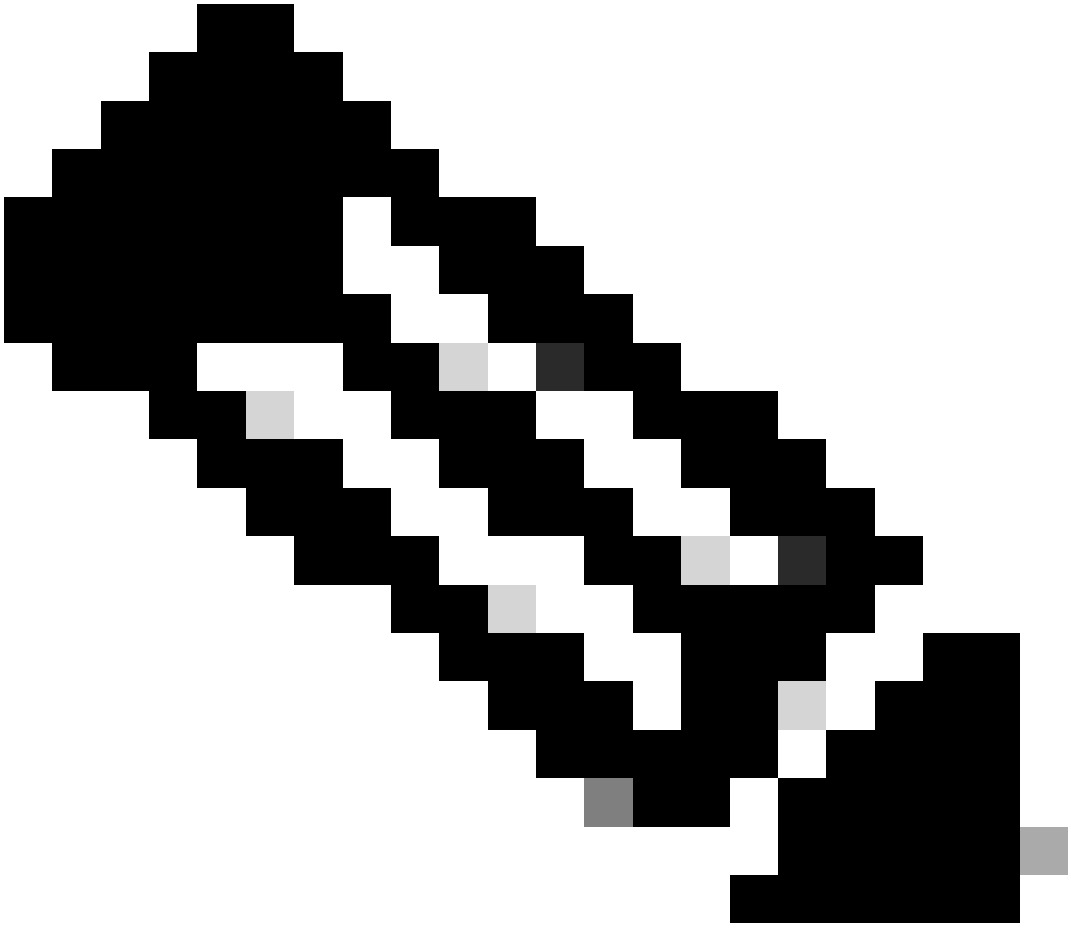
已选择选项Prompt for Credentials > Never Remember，因此在每个身份验证中，进行身份验证的用户必须输入其凭据。

单击完成。

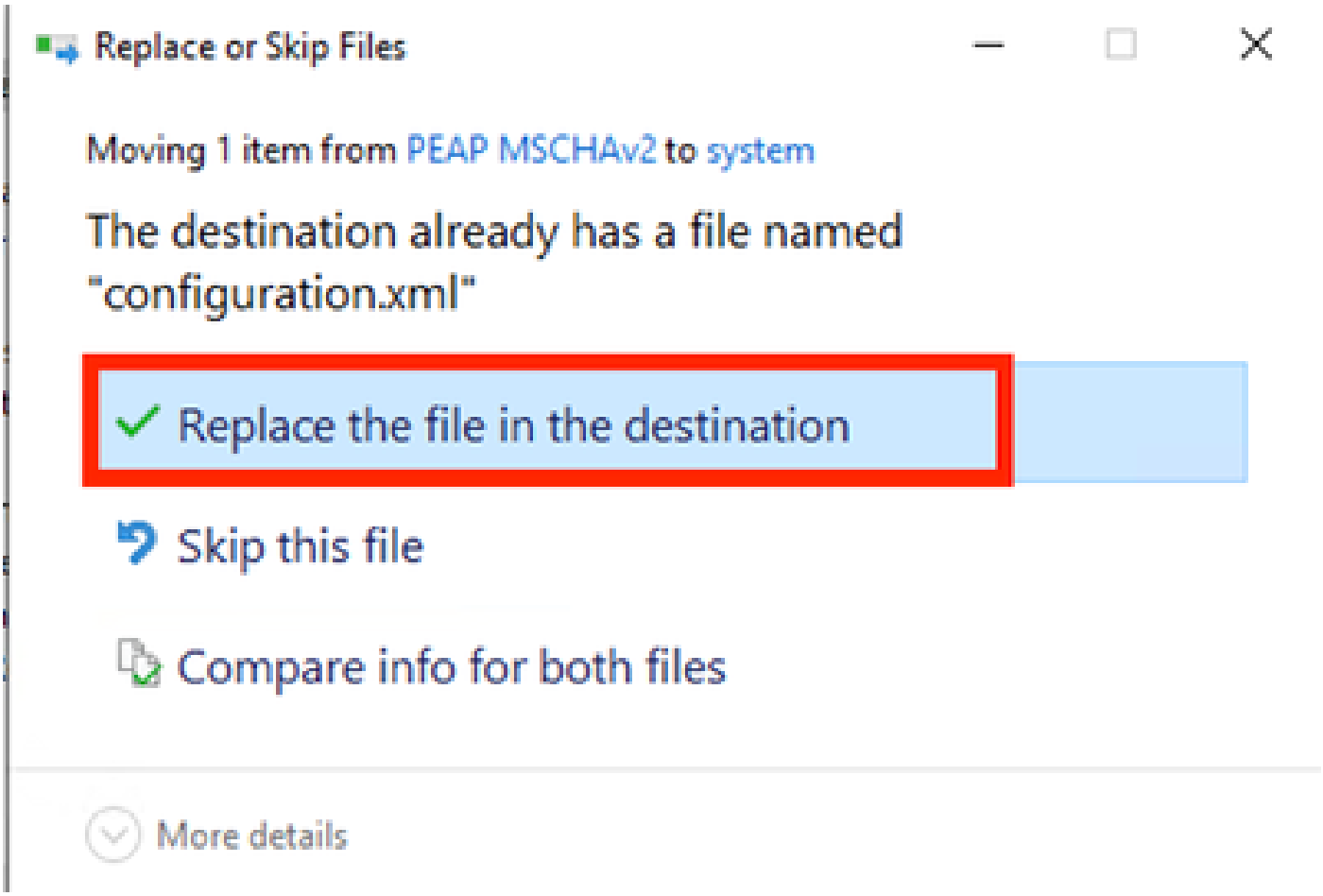
使用File > Save As选项将安全客户端网络访问管理器配置文件另存为configuration.xml。

要使Secure Client Network Access Manage使用刚创建的配置文件，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：该文件必须命名为configuration.xml，否则它将不起作用。

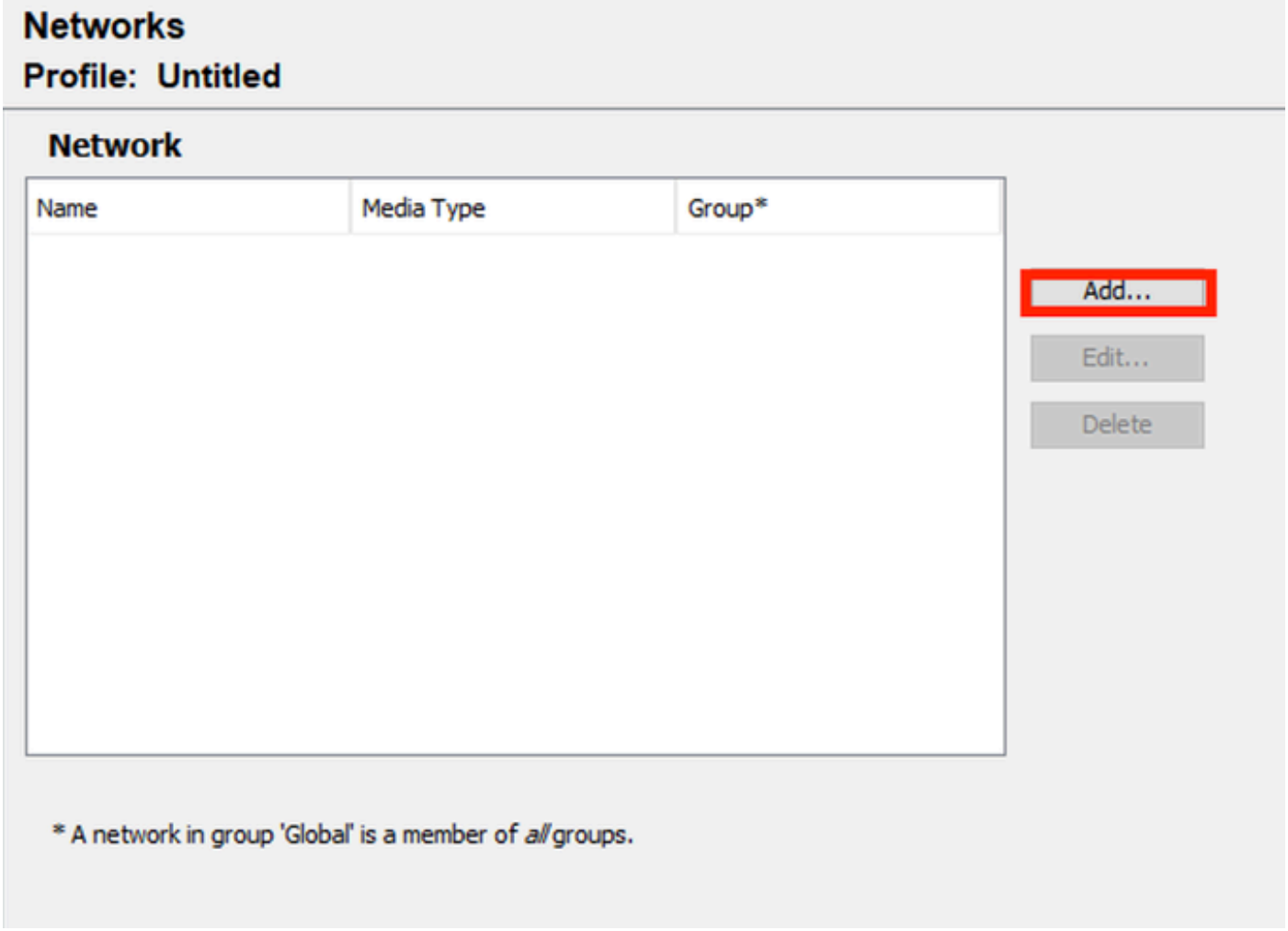


替换文件部分

5. 方案2：为EAP-FAST同步用户和计算机身份验证配置安全客户端NAM请求方

打开NAM配置文件编辑器并导航到网络部分。

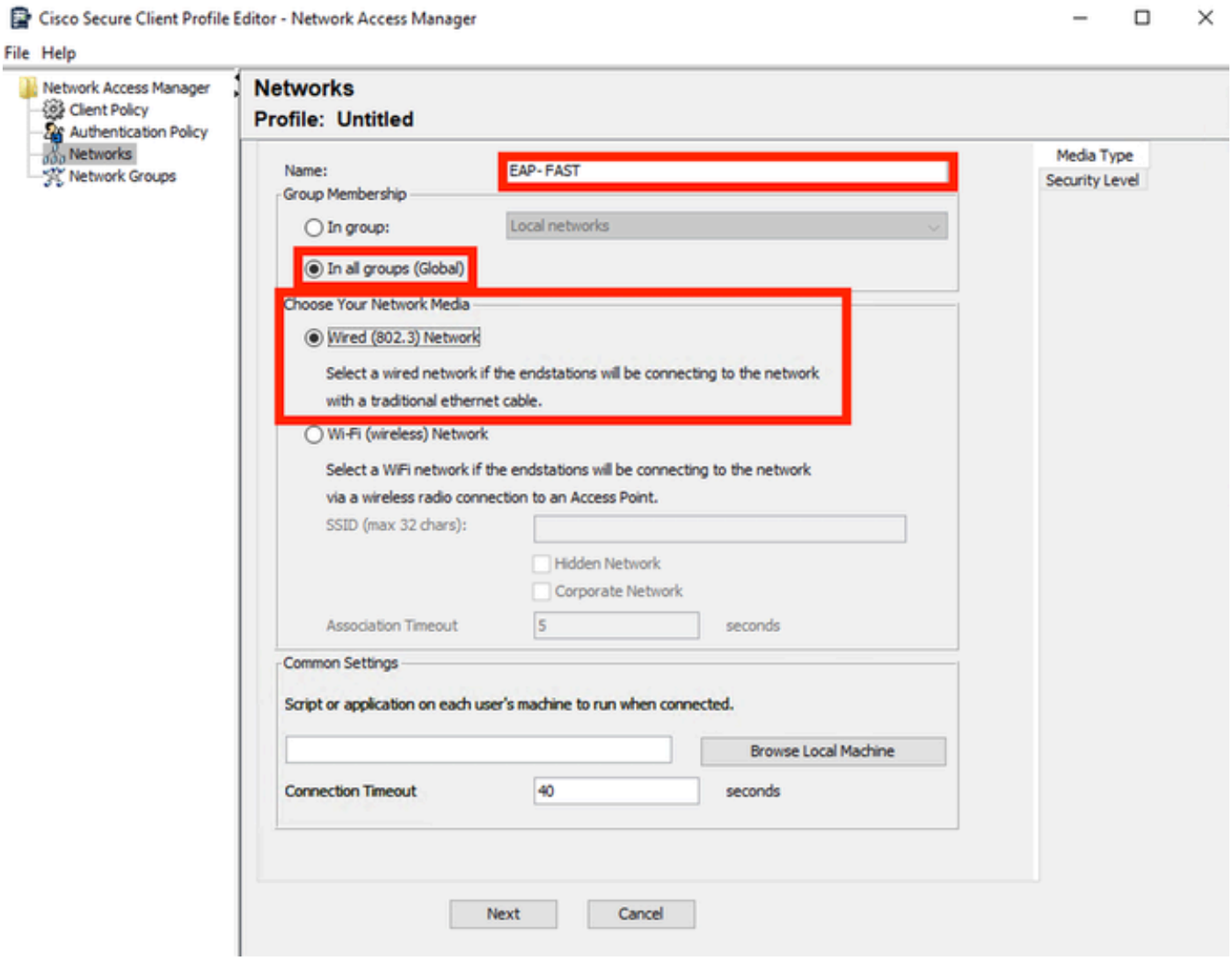
单击 Add。



NAM配置文件编辑器网络选项卡

在网络配置文件中输入名称。

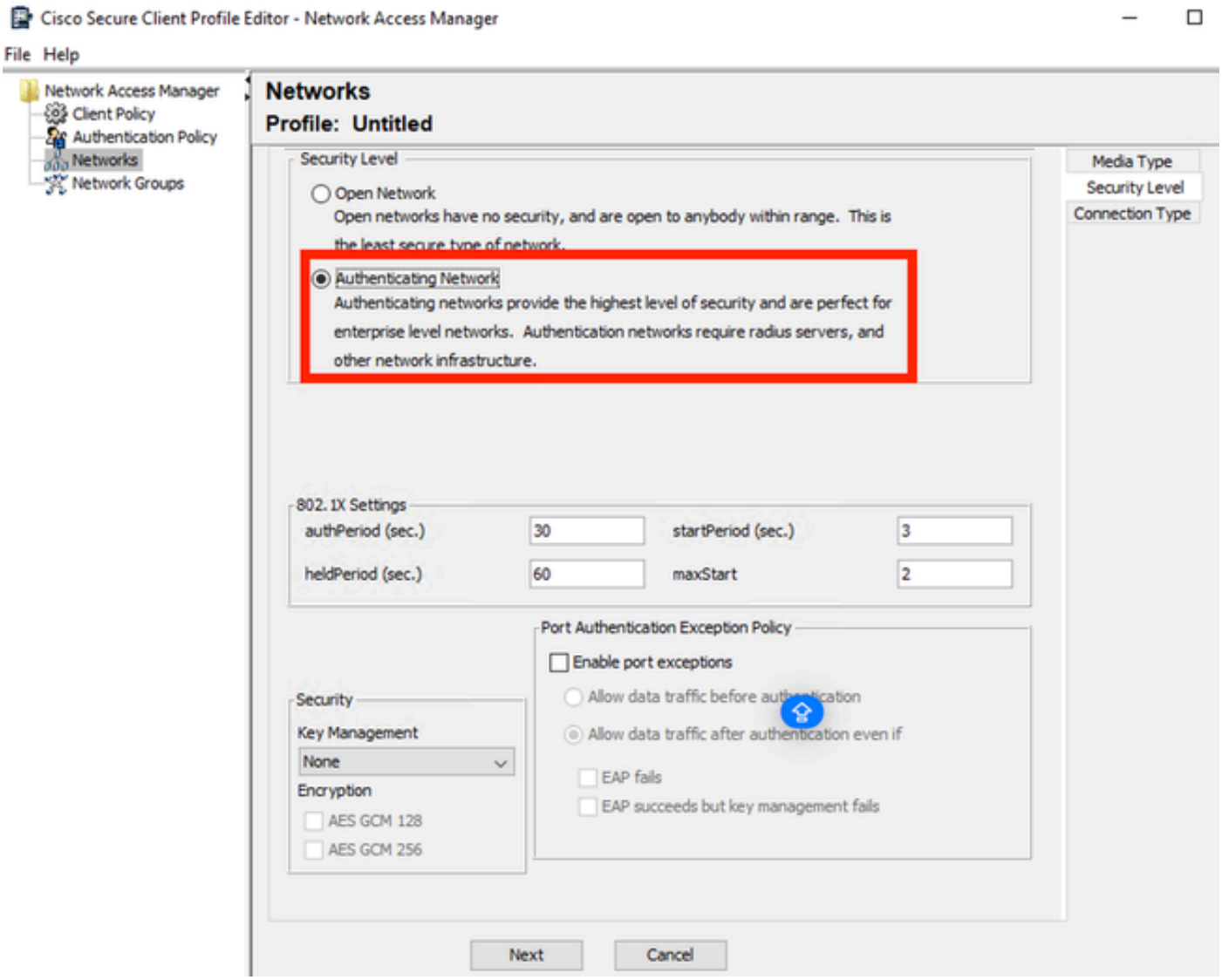
为Group Membership选择Global。选择有线网络介质。



Media Type部分

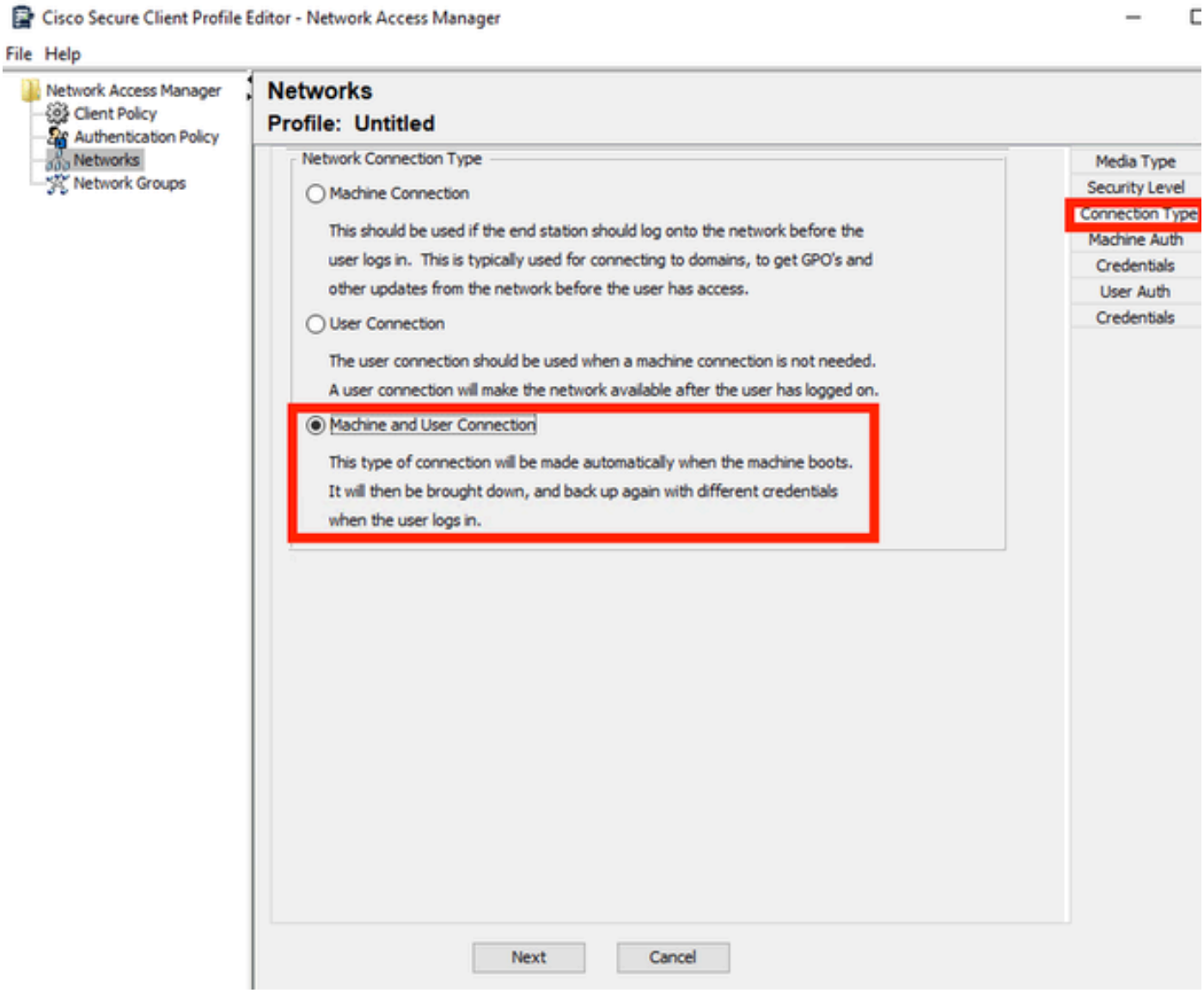
单击 Next。

选择Authenticating Network，且不更改此部分中其余选项的默认值。



Security Level Profile Editor部分

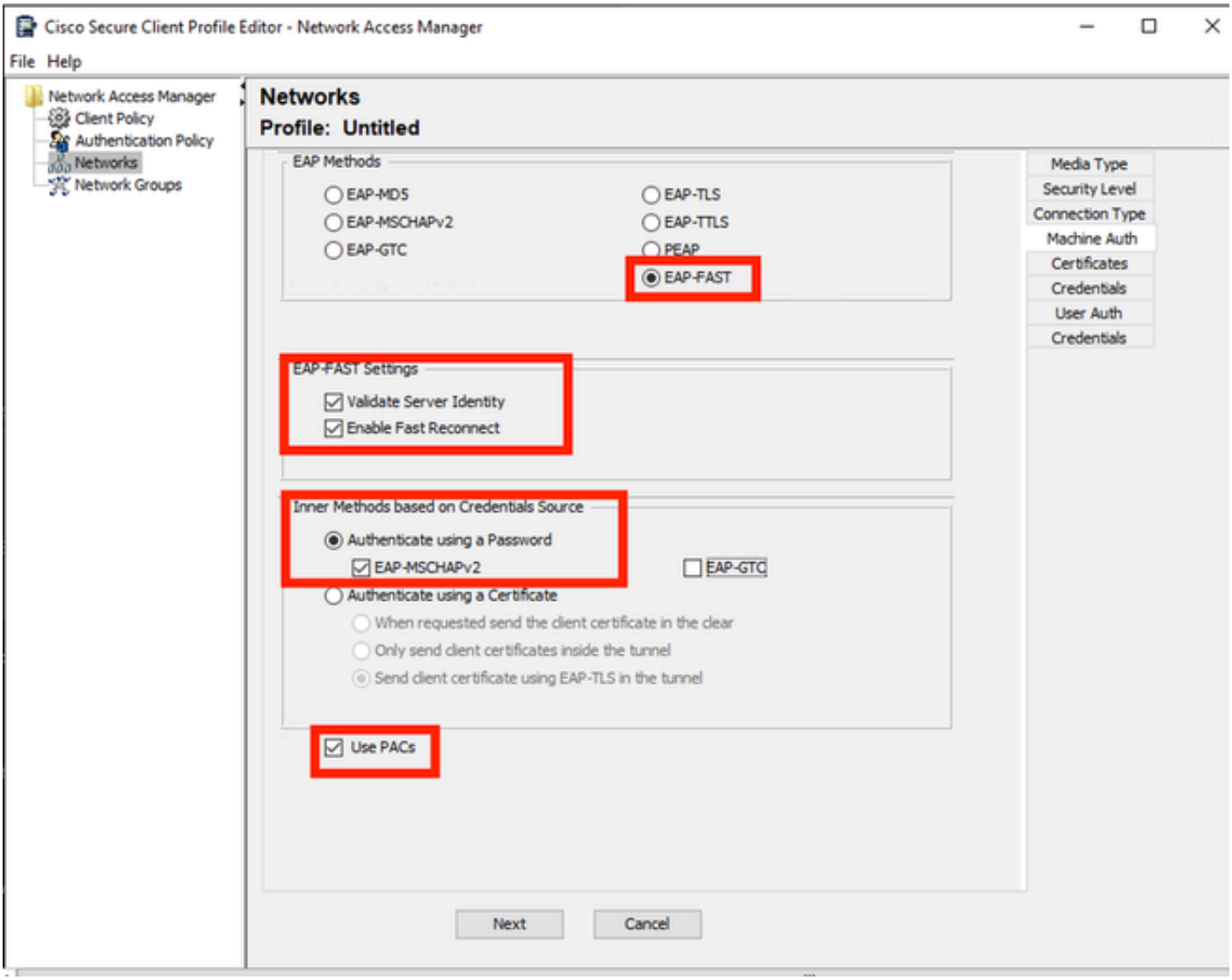
单击Next继续执行Connection Type部分。



Connection Type部分

通过选择第三个选项同时配置用户和计算机身份验证。

单击 Next。

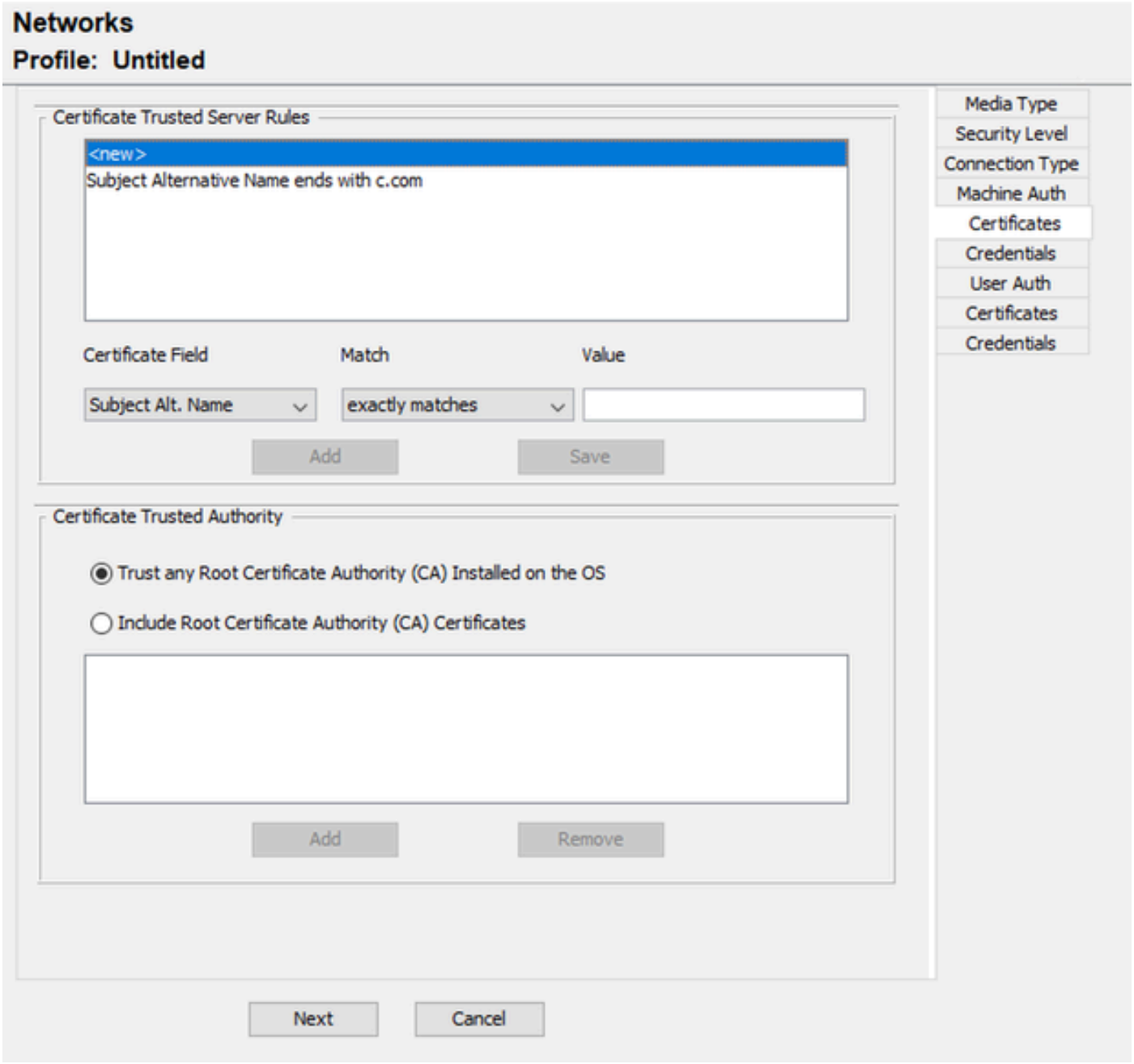


Machine Auth部分

在Machine Auth部分中，选择EAP-FAST作为EAP方法。请勿更改EAP FAST Settings默认值。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PACs选项。

单击 Next。

在证书部分上，在证书受信任服务器规则中，规则公用名以c.com结尾。此部分是指服务器在EAP PEAP流程期间使用的证书。如果在您的环境中使用身份服务引擎(ISE)，可以使用策略服务器节点EAP证书的公用名称。

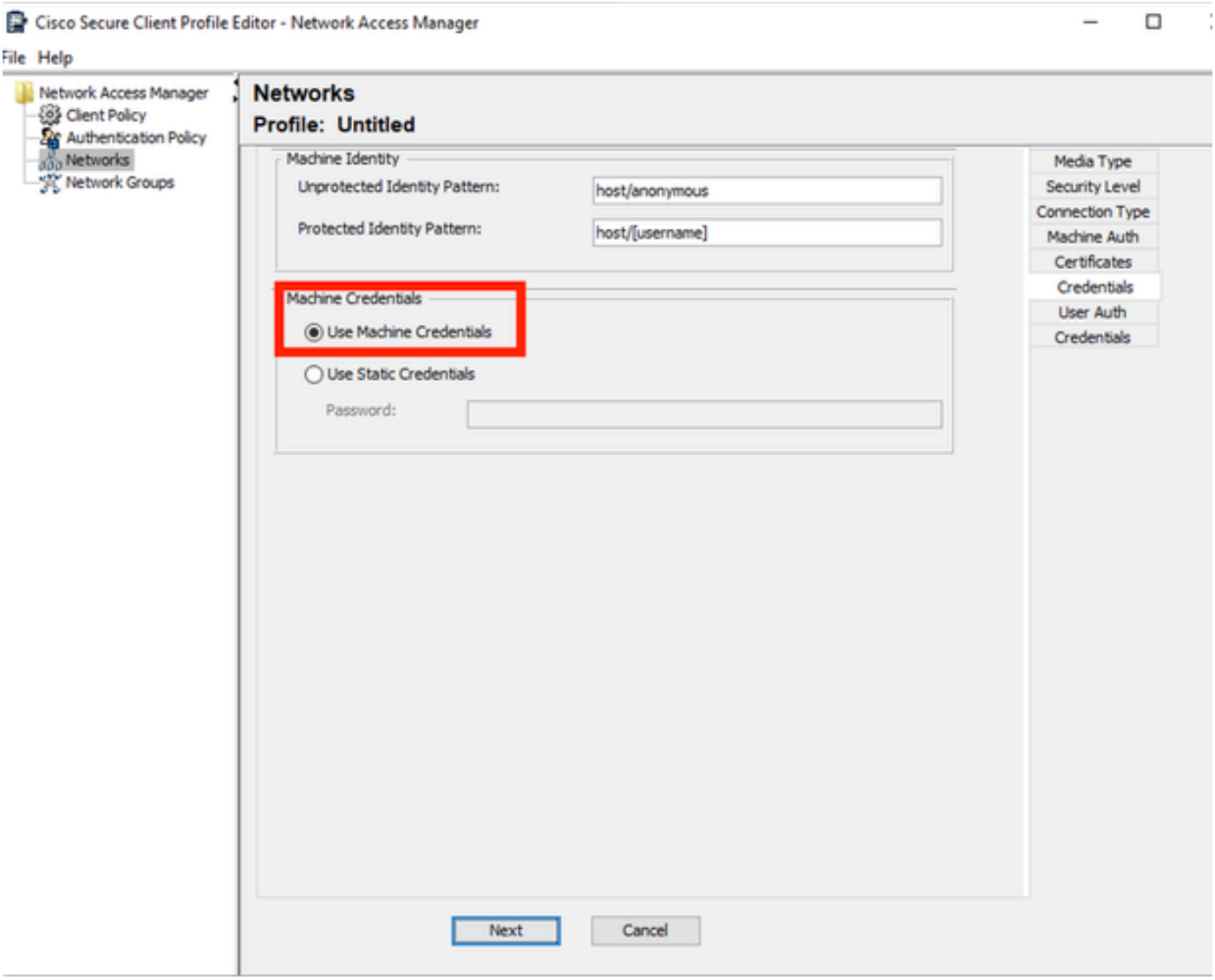


计算机身份验证服务器证书信任部分

可以在证书受信任颁发机构中选择两个选项。 对于此方案，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。

使用此选项，Windows将信任由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。

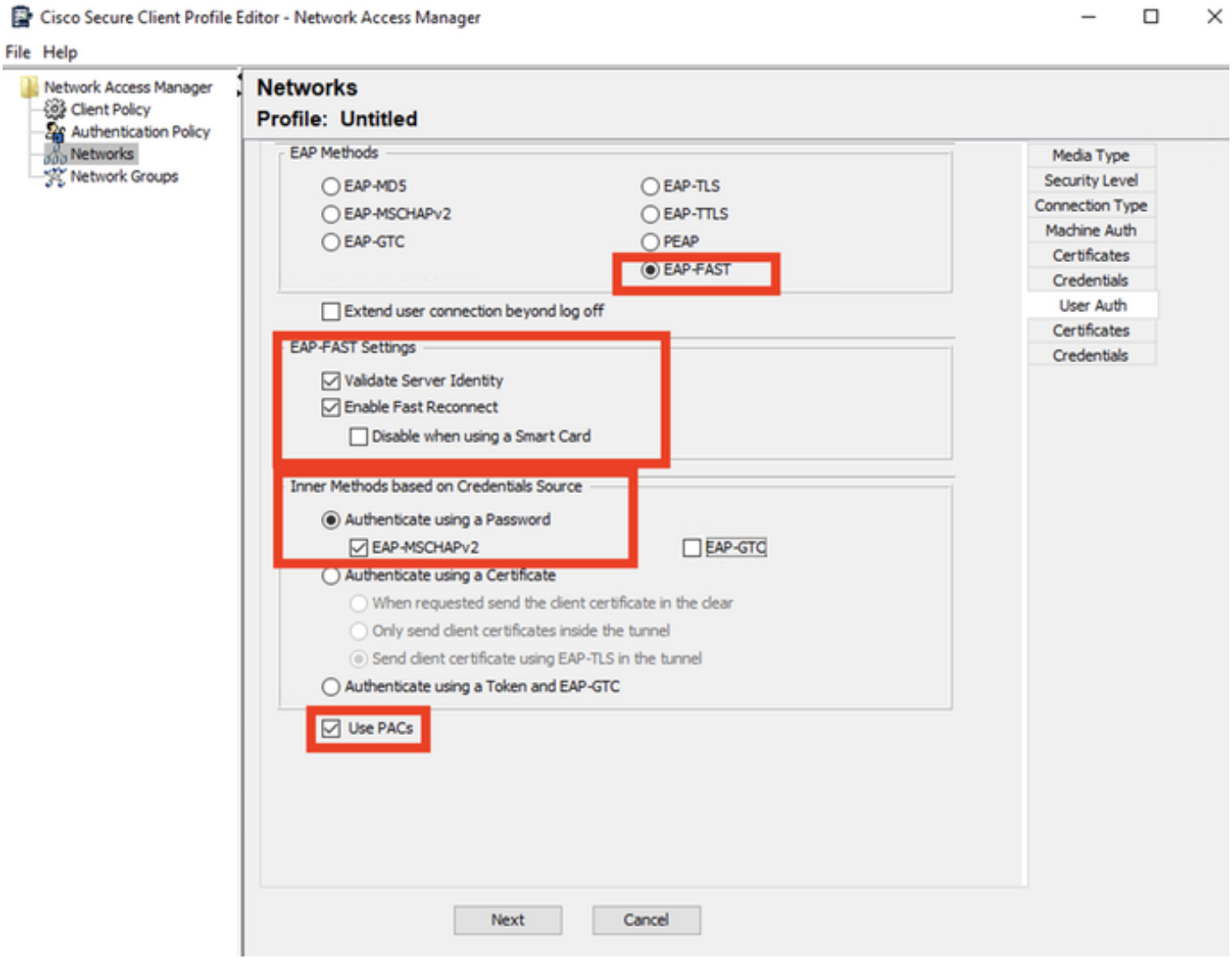
单击 Next。



Machine Auth Credentials部分

在计算机凭据部分中选择使用计算机凭据。

单击 Next。



User Authentication部分

对于User Auth，请选择EAP-FAST作为EAP方法。

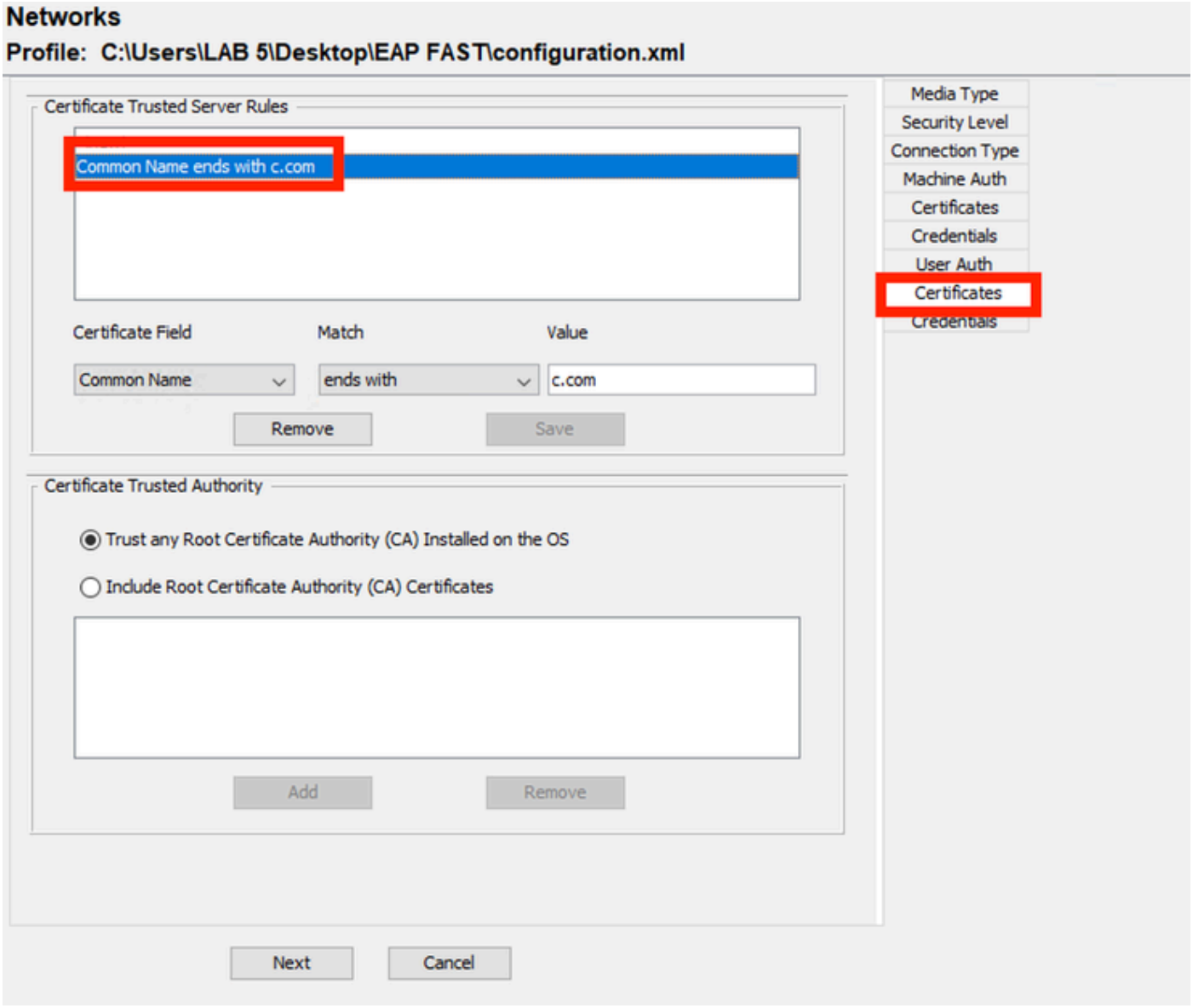
请勿更改EAP-FAST设置部分的默认值。

对于Inner Method based on credentials source部分，选择Authenticate using a Password和EAP-MSCHAPv2作为方法。

选择Use PACs。

单击 Next。

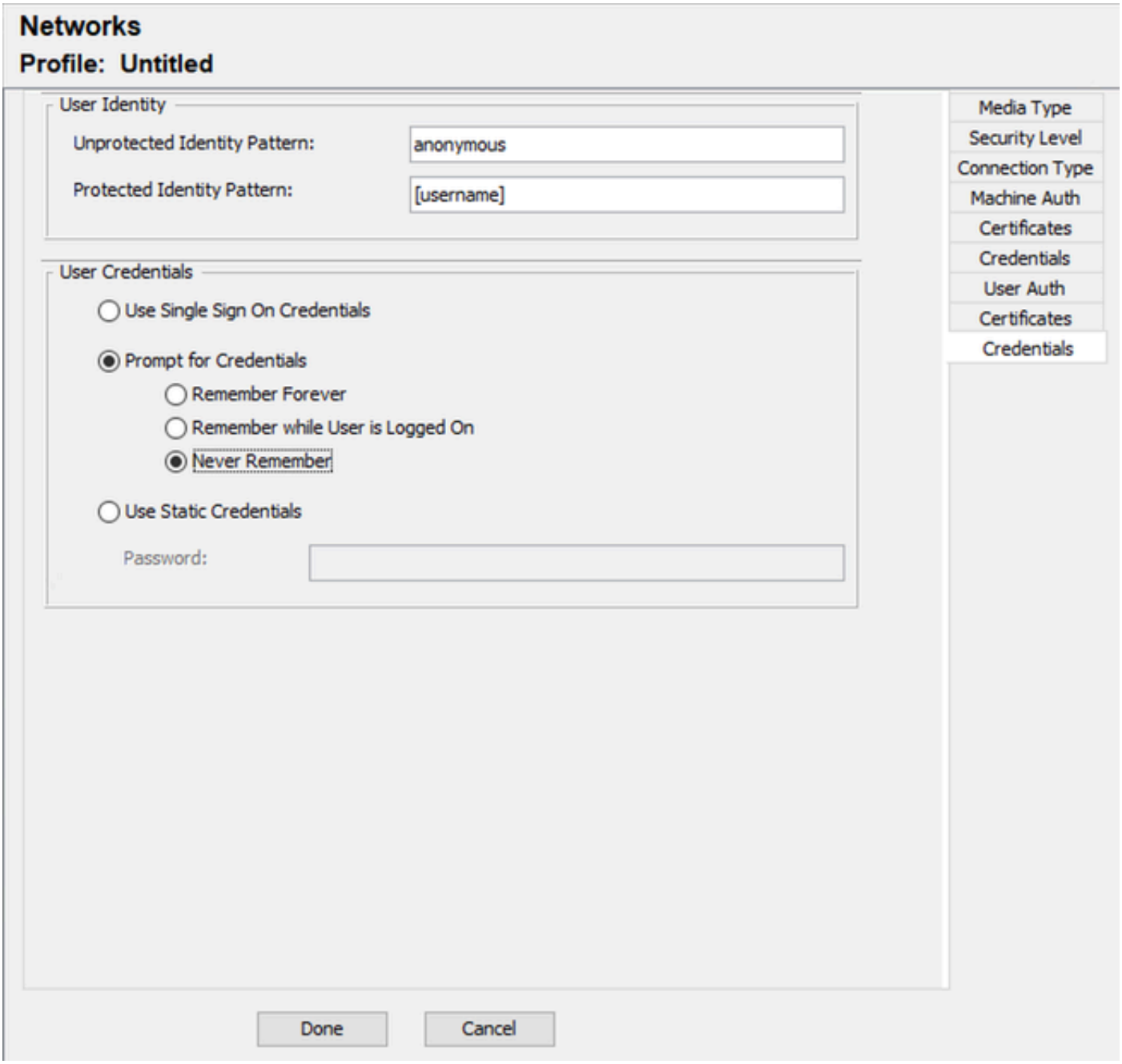
在证书部分的证书受信任服务器规则中，规则为公用名以c.com结束。这些配置适用于服务器在EAP PEAP流期间使用的证书。如果在您的环境中使用ISE，可以使用策略服务器节点EAP证书的公用名称。



用户身份验证服务器证书信任部分

可以在证书受信任颁发机构中选择两个选项。对于此方案，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。

单击 Next。



用户身份验证凭证

在“凭据”部分中，仅更改用户凭据部分。

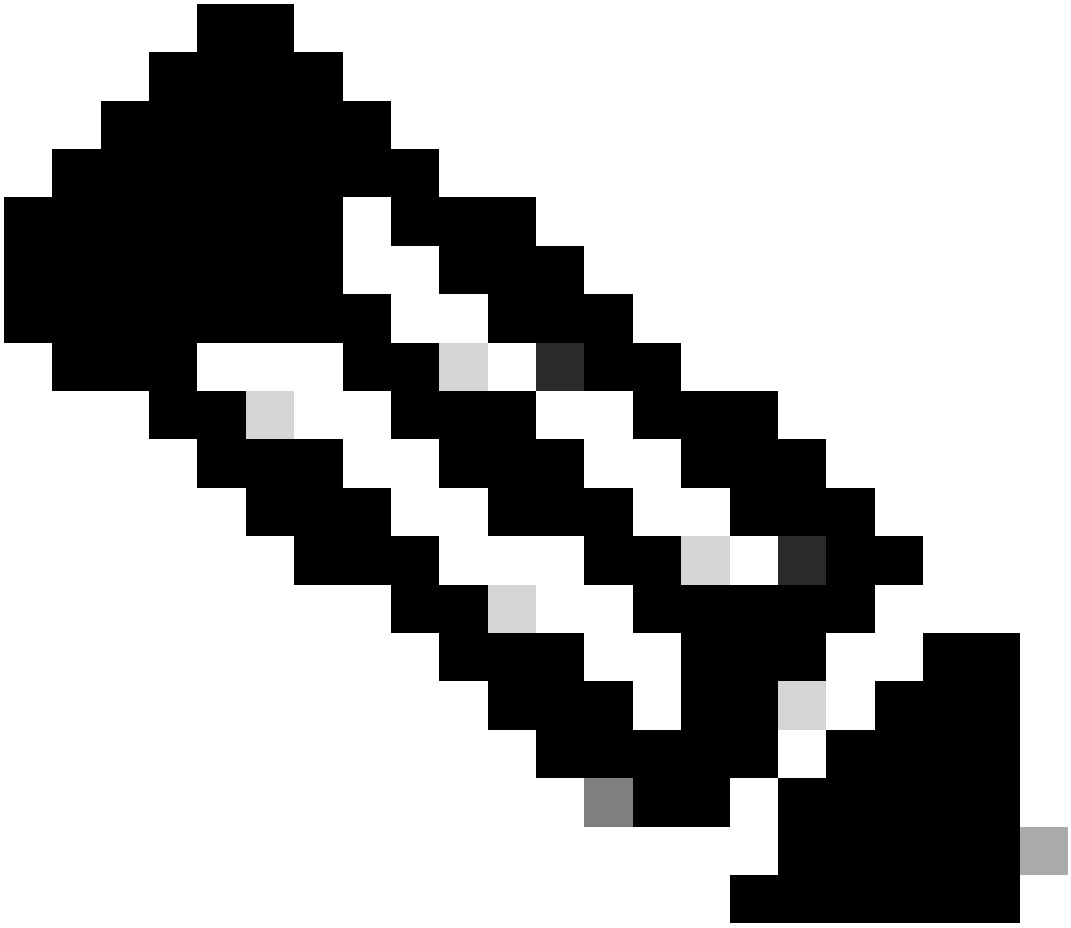
已选择选项Prompt for Credentials > Never Remember。因此，在每次身份验证中，进行身份验证的用户必须输入其凭证。

单击Done按钮。

选择File > Save as，然后将Secure Client Network Access Manager配置文件保存为configuration.xml。

要使安全客户端网络访问管理器使用刚才创建的配置文件，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

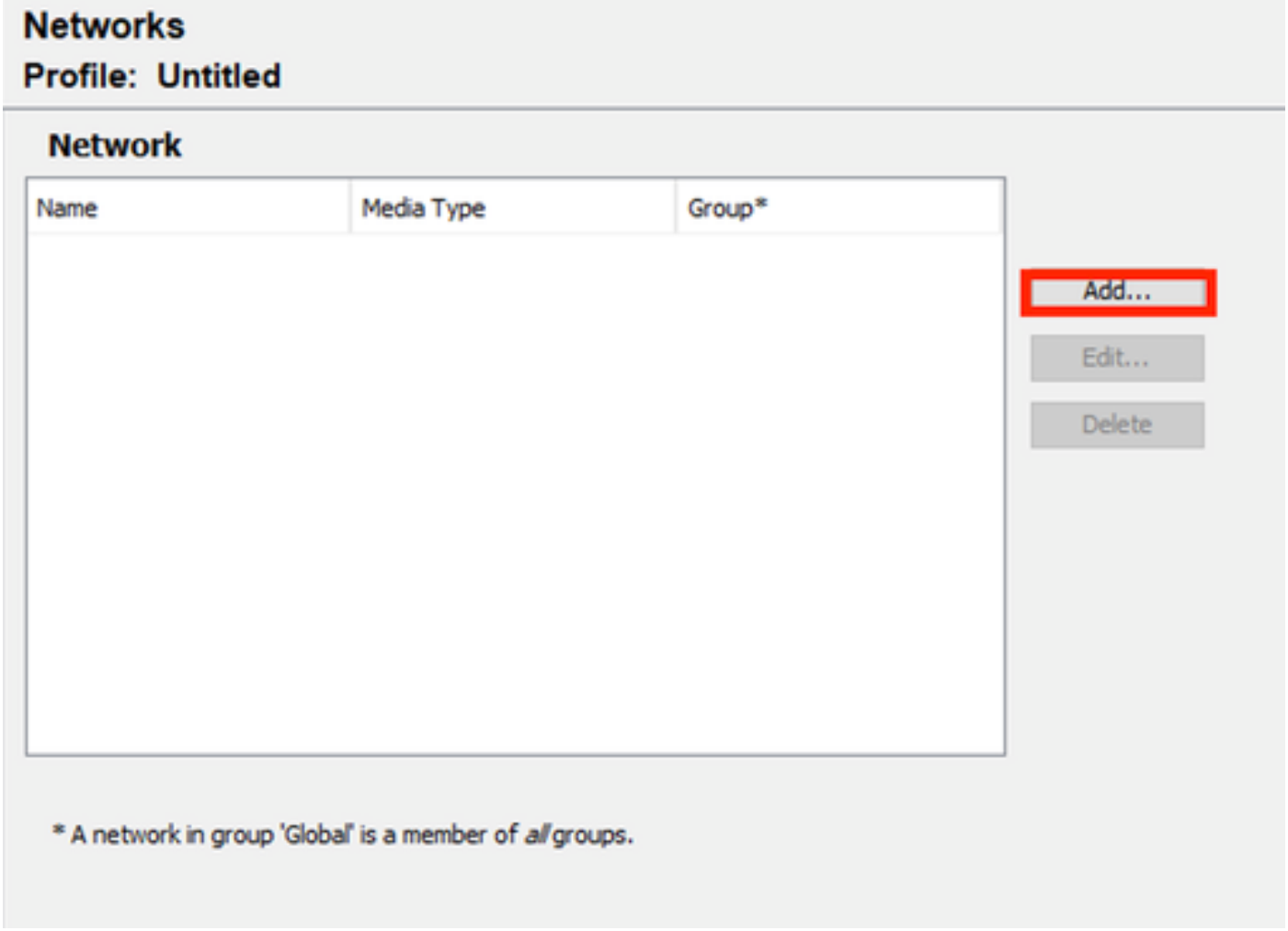


注意：该文件必须命名为configuration.xml，否则它将不起作用。

6. 方案3：为EAP TLS用户证书身份验证配置安全客户端NAM请求方

打开NAM配置文件编辑器，然后导航到网络部分。

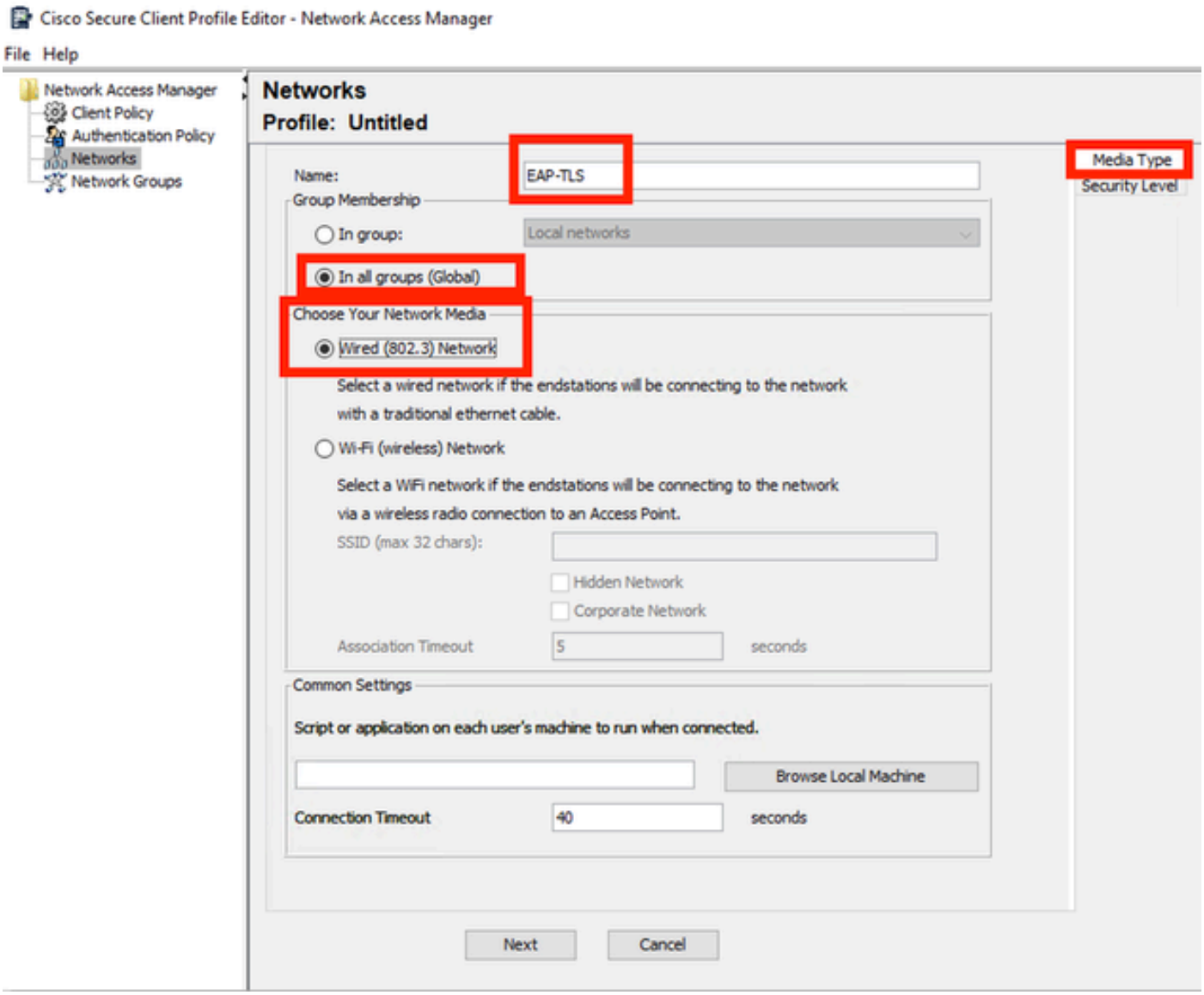
单击 Add。



Network Creation部分

为网络配置文件命名，在本例中，使用用于此方案的EAP协议命名。

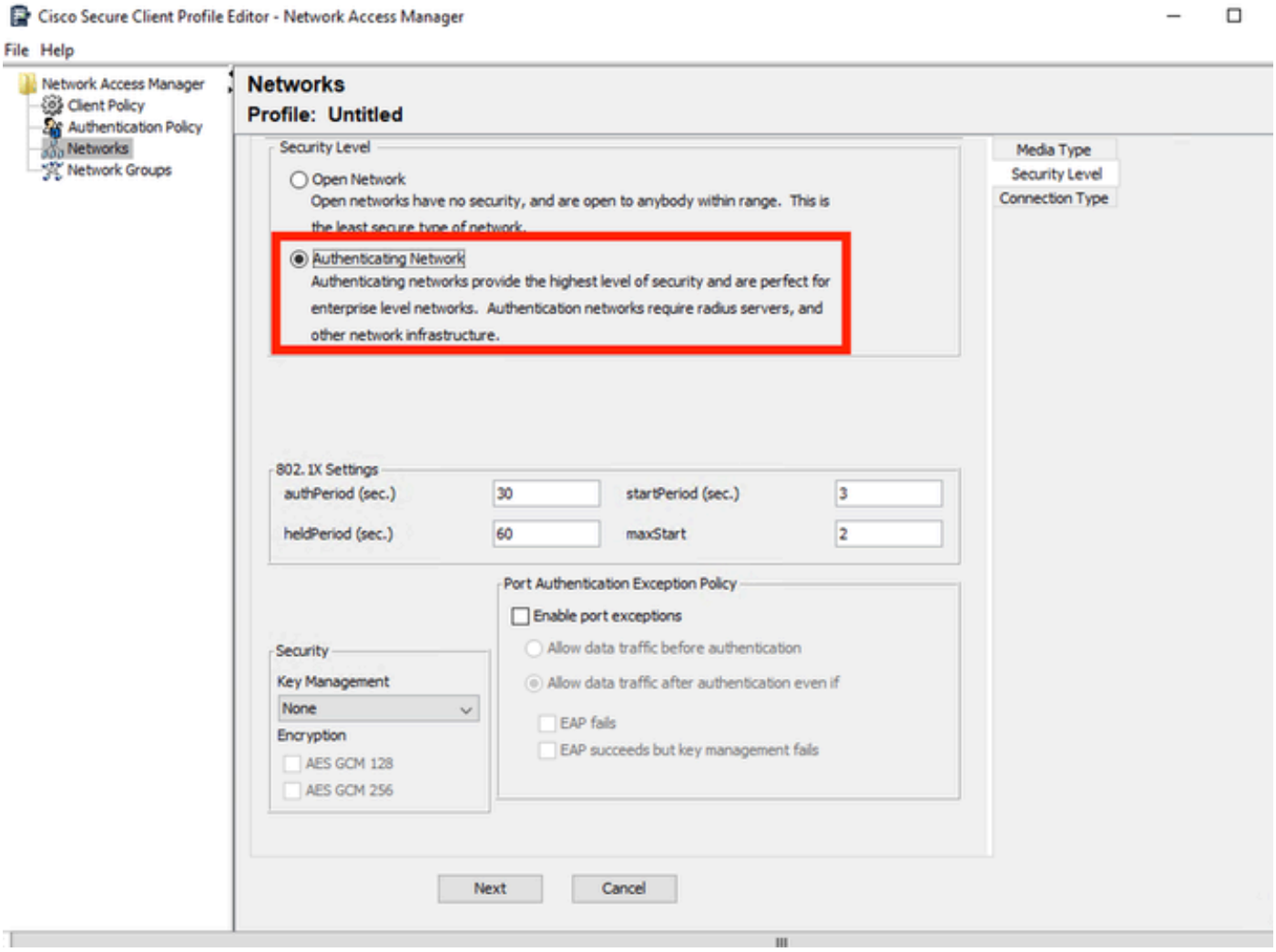
为Group Membership选择Global。和有线网络介质。



Media Type部分

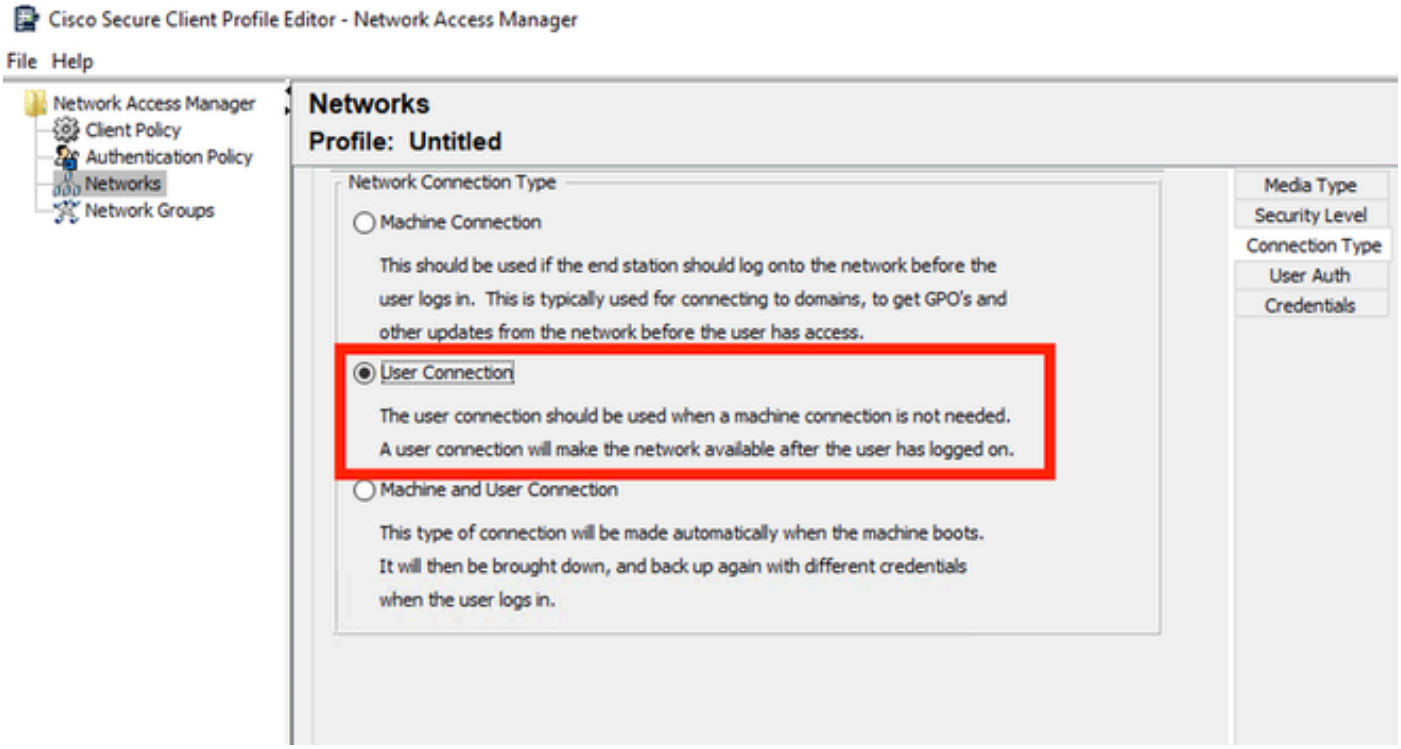
单击 Next。

选择Authenticating Network，且不更改Security Level部分中其余选项的默认值。



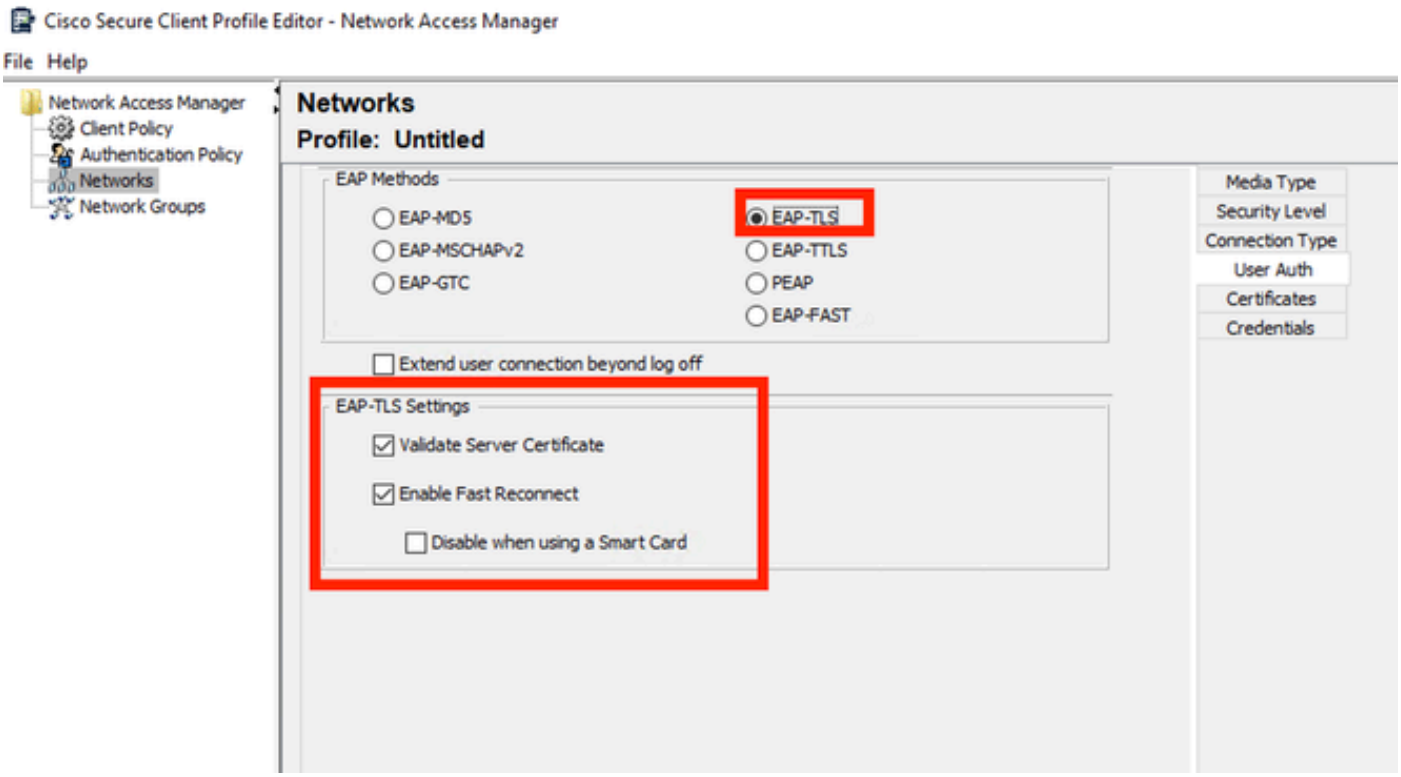
安全级别

此场景适用于使用证书的用户身份验证。因此，使用了选项User Connection。



连接类型

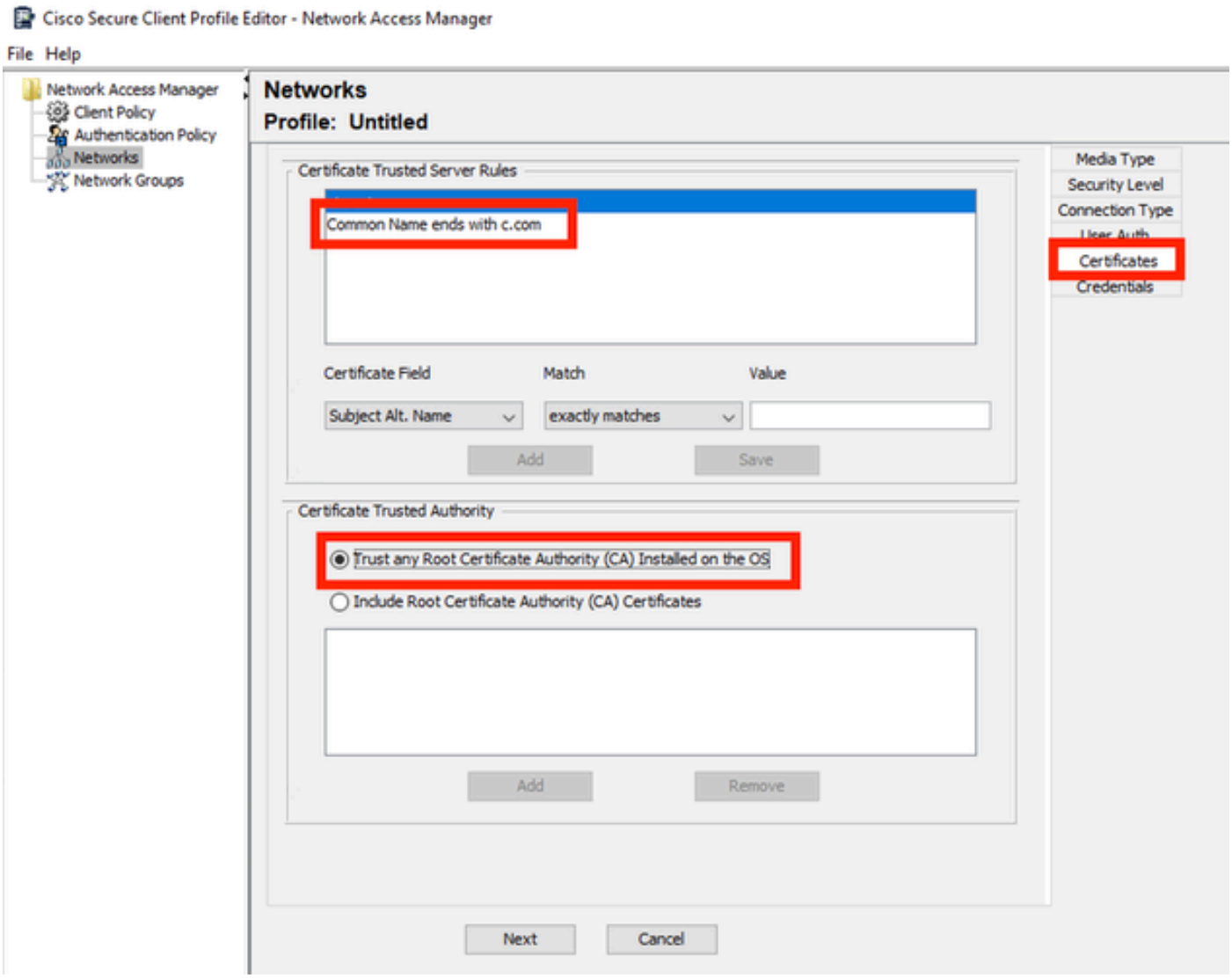
将EAP-TLS配置为EAP方法。请勿更改EAP-TLS设置部分中的默认值。



User Auth部分

在Certificates部分，创建与AAA EAP-TLS证书匹配的规则。如果您使用的是ISE，请在管理>系统>证书部分查找此规则。

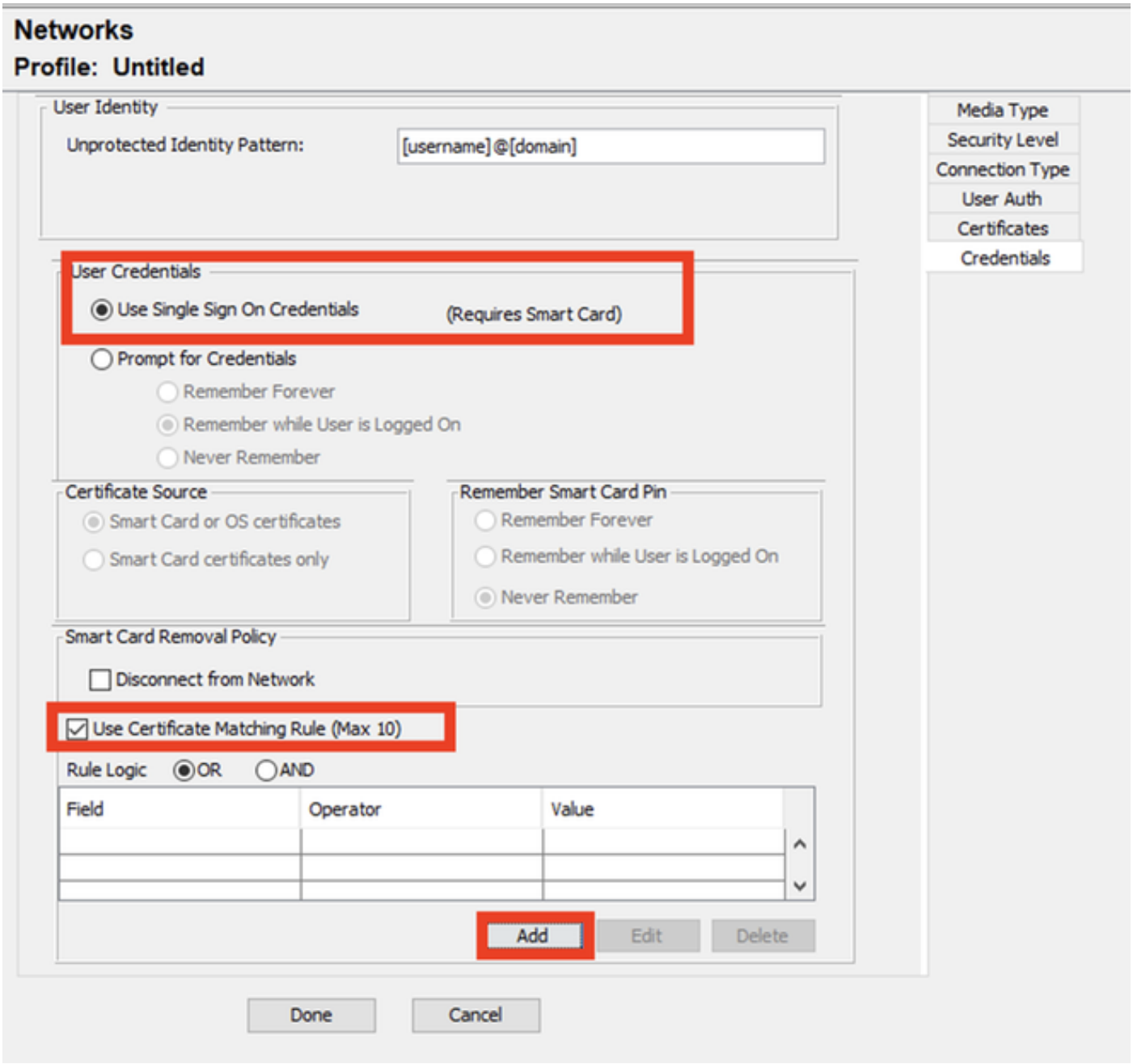
对于Certificate Trusted Authority部分，选择Trust any Root Certificate Authority (CA) installed on the OS。



用户身份验证服务器证书信任设置

单击 Next。

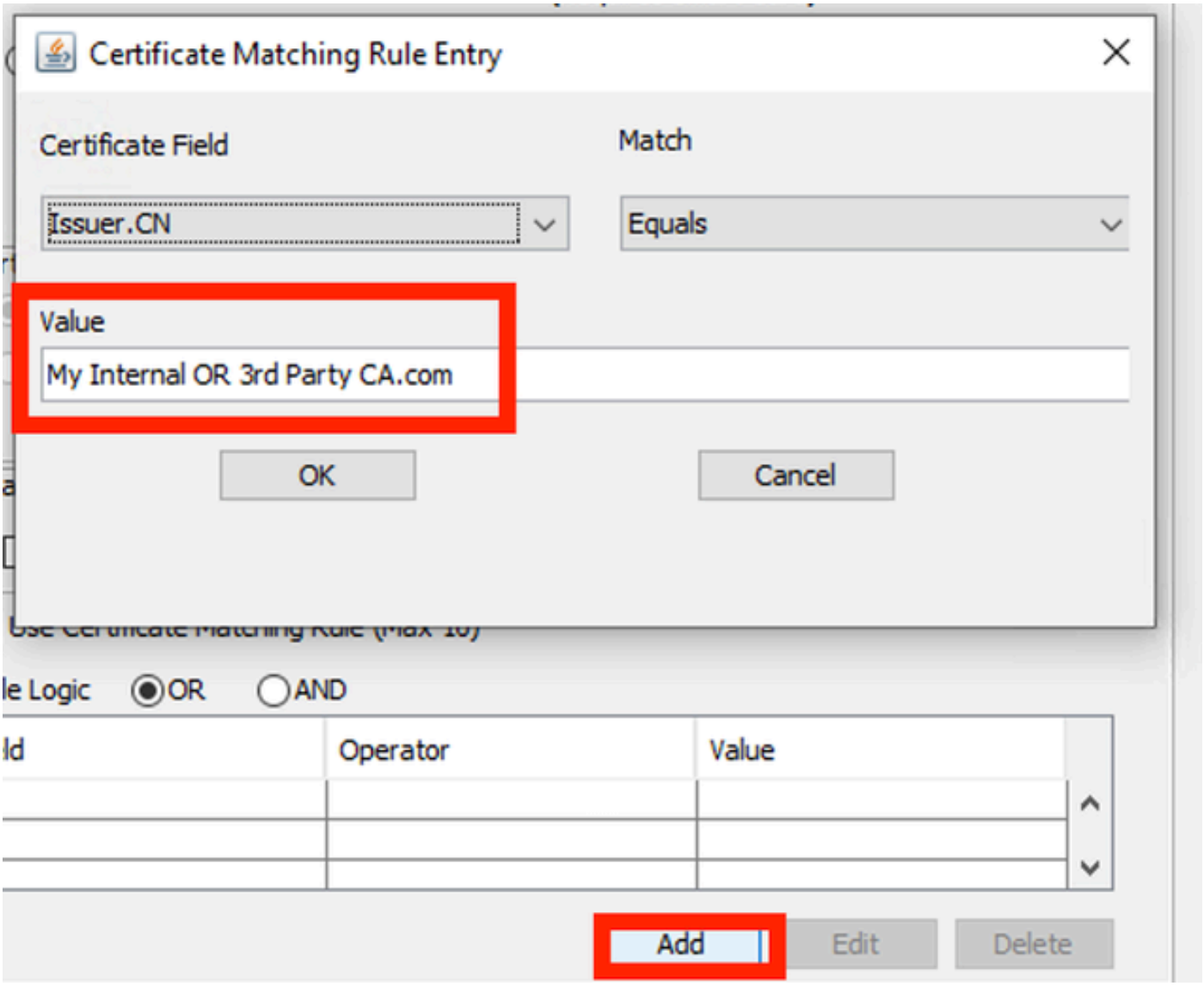
对于User Credentials部分，不要更改第一部分中的默认值。



*User Auth Credentials*部分

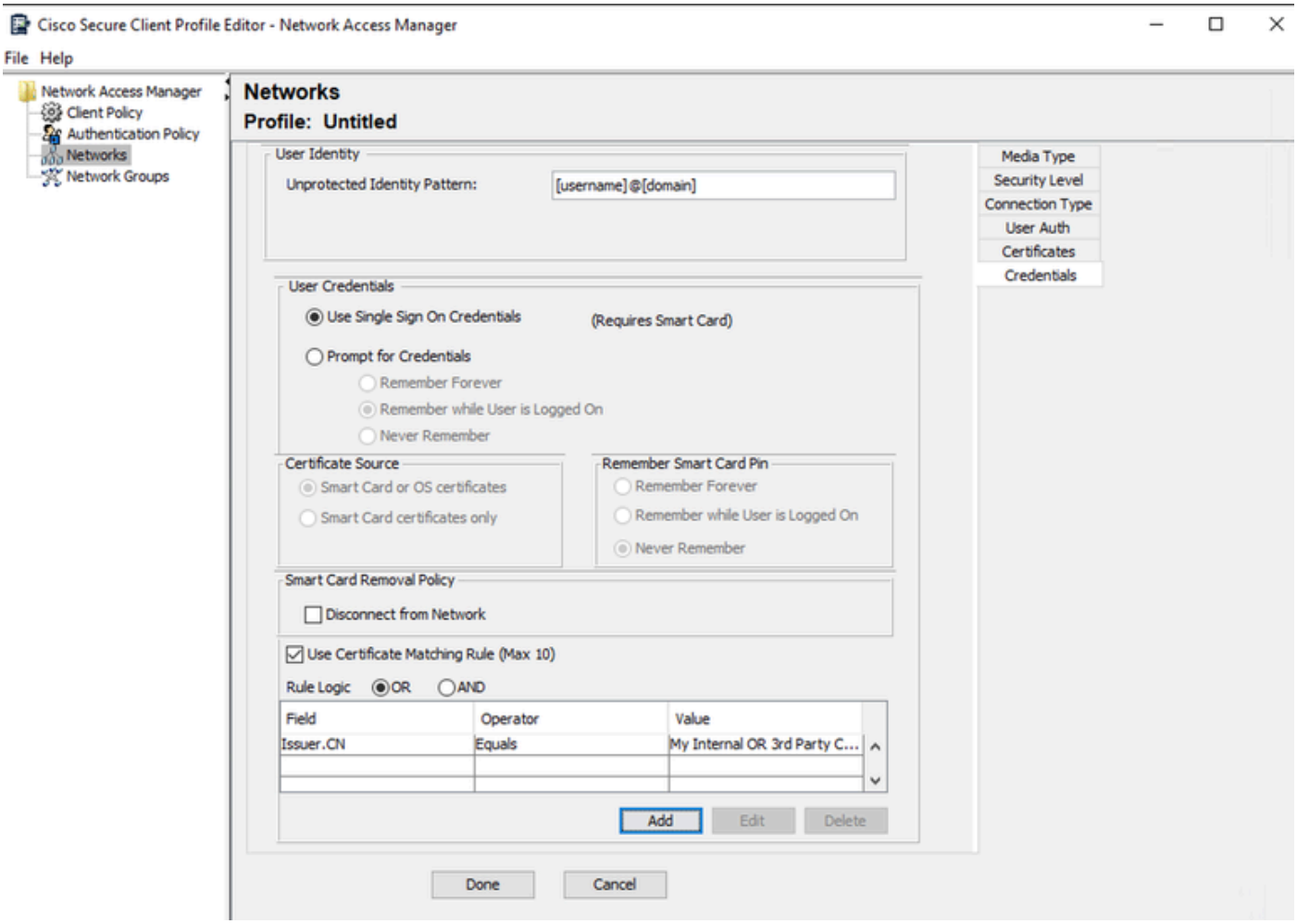
必须配置与用户在EAP TLS过程中发送的身份证书匹配的规则。要执行此操作，请点击Use Certificate Machining Rule (Max 10)旁边的复选框。

单击 Add。



证书匹配规则窗口

用用户证书的CN替换值My Internal或第三方CA.com。



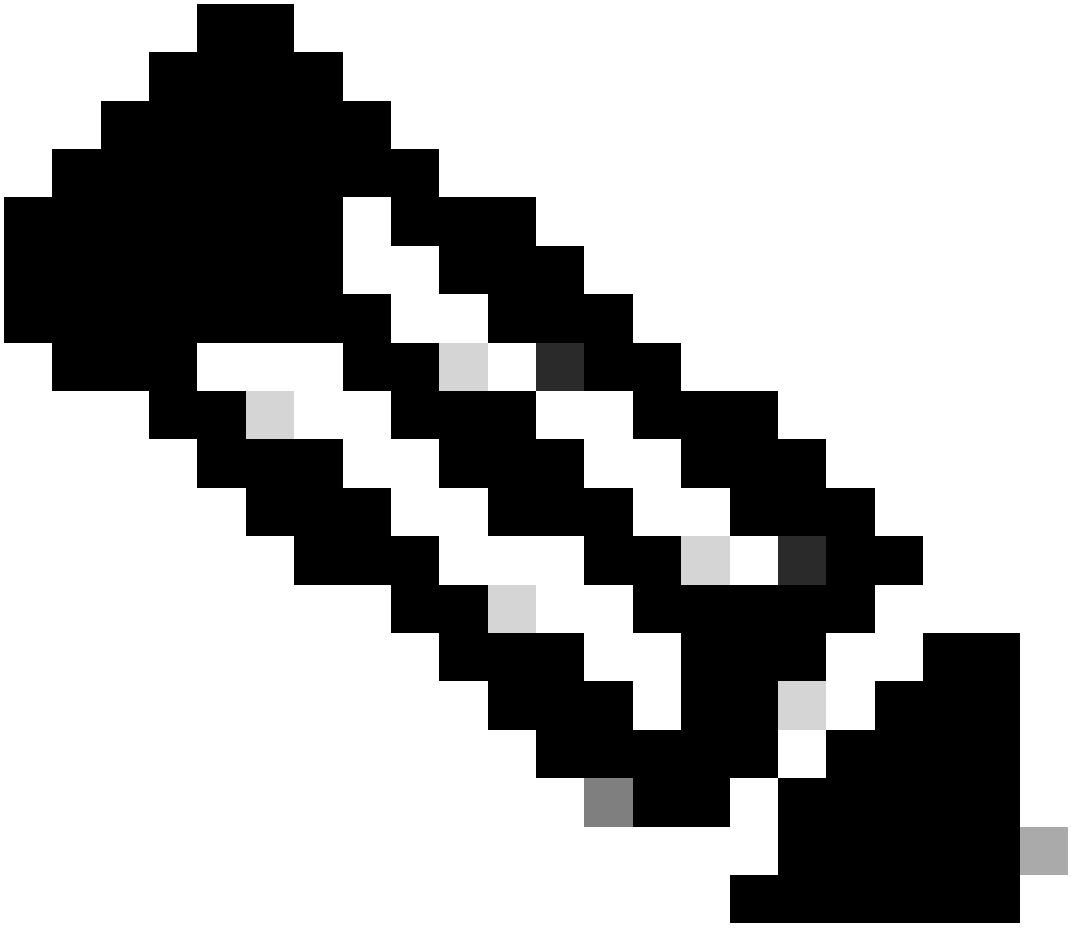
用户身份验证证书凭证部分

单击Done完成配置。

选择File > Save as以将Secure Client Network Access Manager配置文件另存为configuration.xml。

要使安全客户端网络访问管理器使用刚才创建的配置文件，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

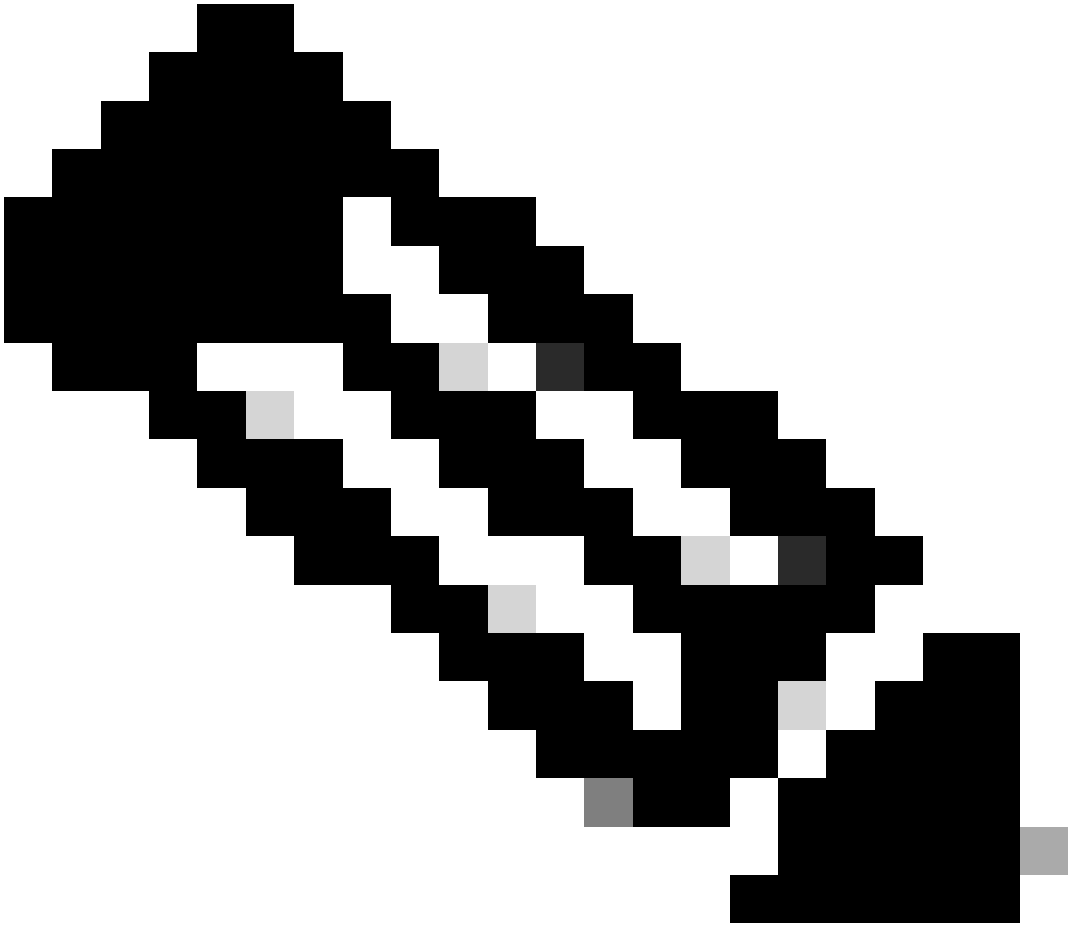


注意：该文件必须命名为configuration.xml，否则它将不起作用。

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

配置ISR 1100路由器。

本部分介绍需要使dot1x正常运行的基本配置。



注：对于多节点ISE部署，指向启用了策略服务器节点角色的任何节点。在Administration > System > Deployment选项卡中导航到ISE可对此进行检查。

```
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>
!
!
```

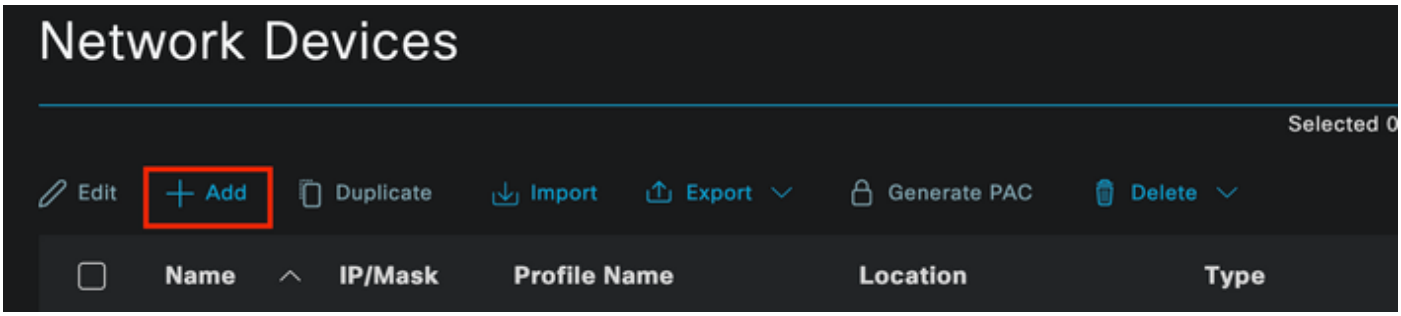
```
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

配置身份服务引擎3.2。

配置网络设备。

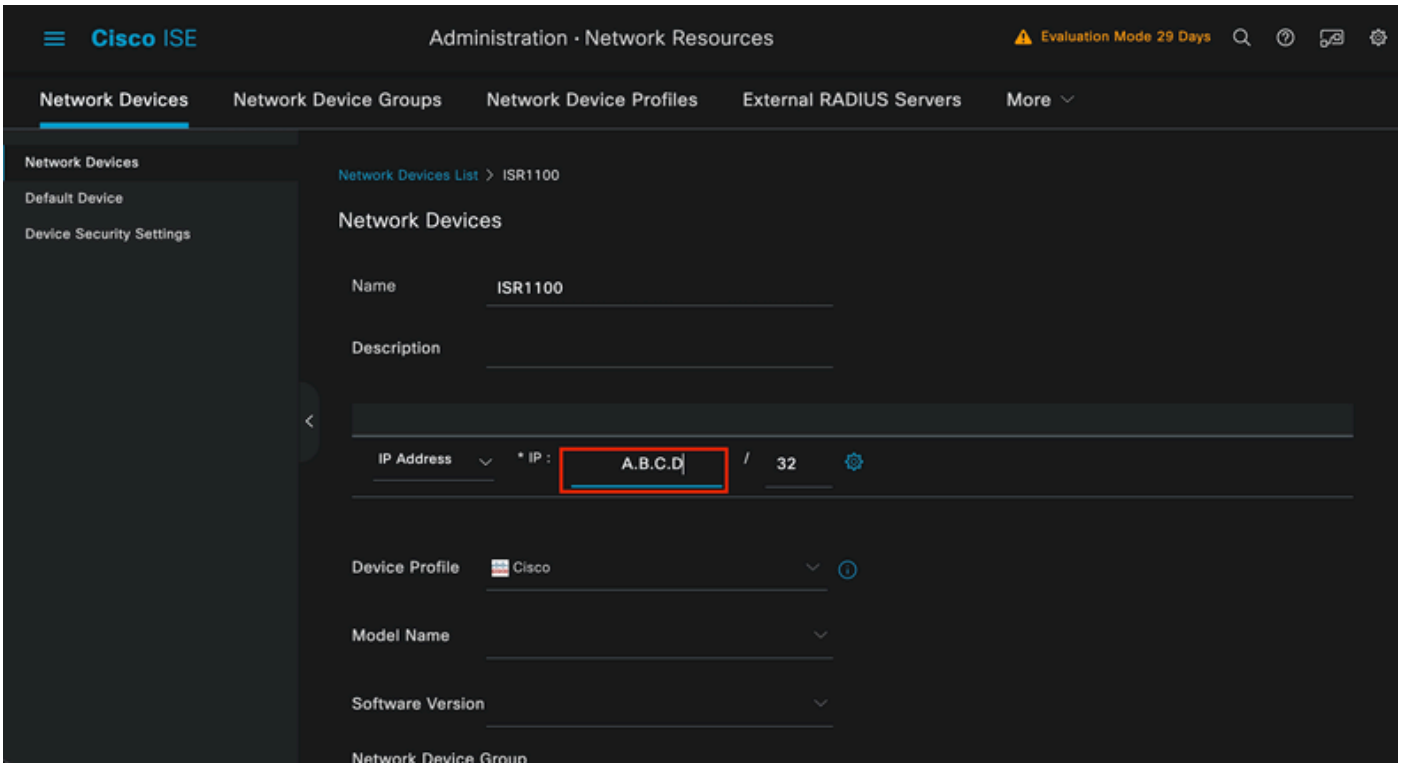
将ISR NAD添加到ISE Administration > Network Resources > Network Devices。

单击 Add。



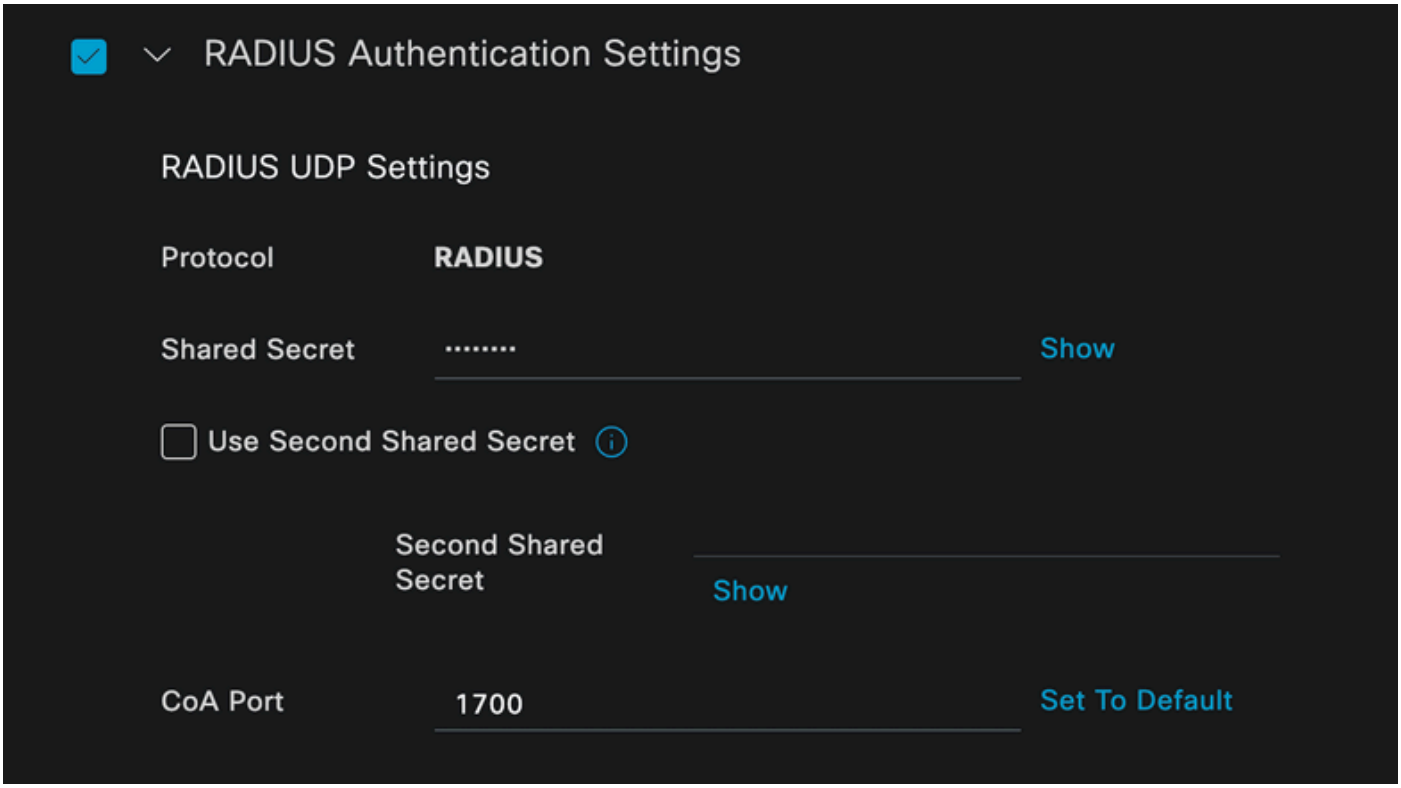
Network Device部分

为您正在创建的NAD指定名称。添加网络设备IP。



网络设备创建

在同一页的底部，添加与网络设备配置中使用的共享密钥相同。



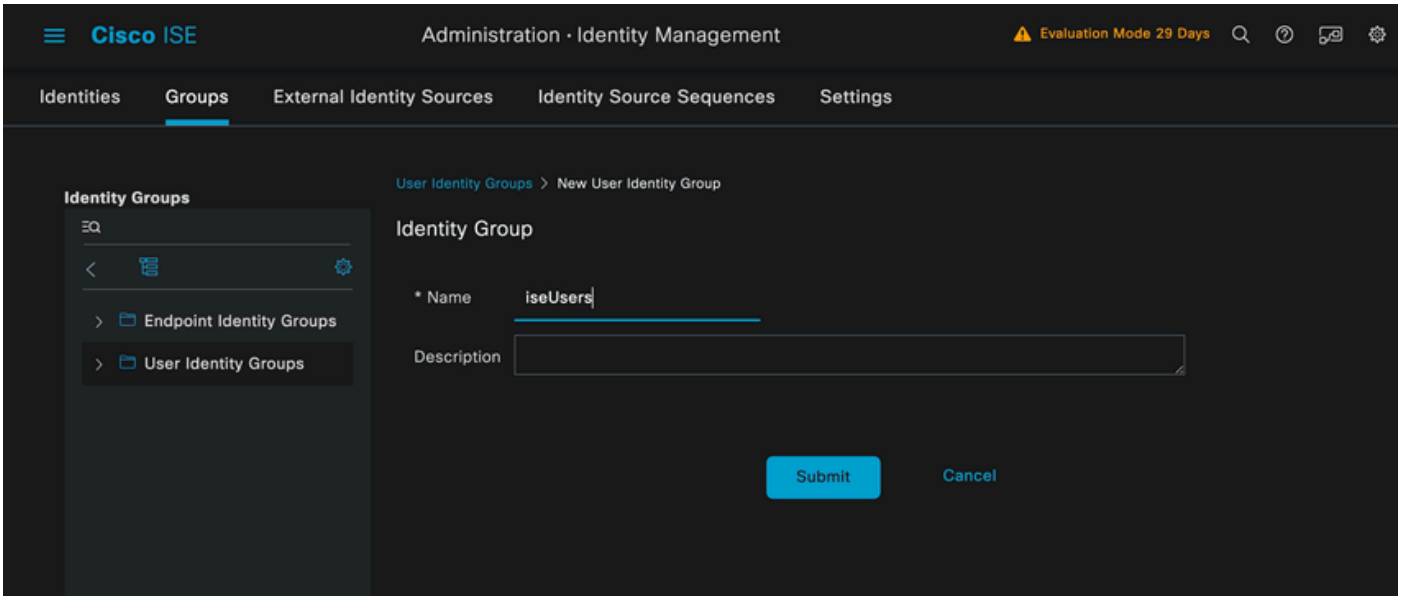
网络设备*Radius*设置

保存更改。

配置用于对终端进行身份验证的身份。

使用ISE本地身份验证。本文未解释外部ISE身份验证。

导航到Administration > Identity Management > Groups选项卡，然后创建用户所在的组。为此演示创建的身份组是iseUsers。

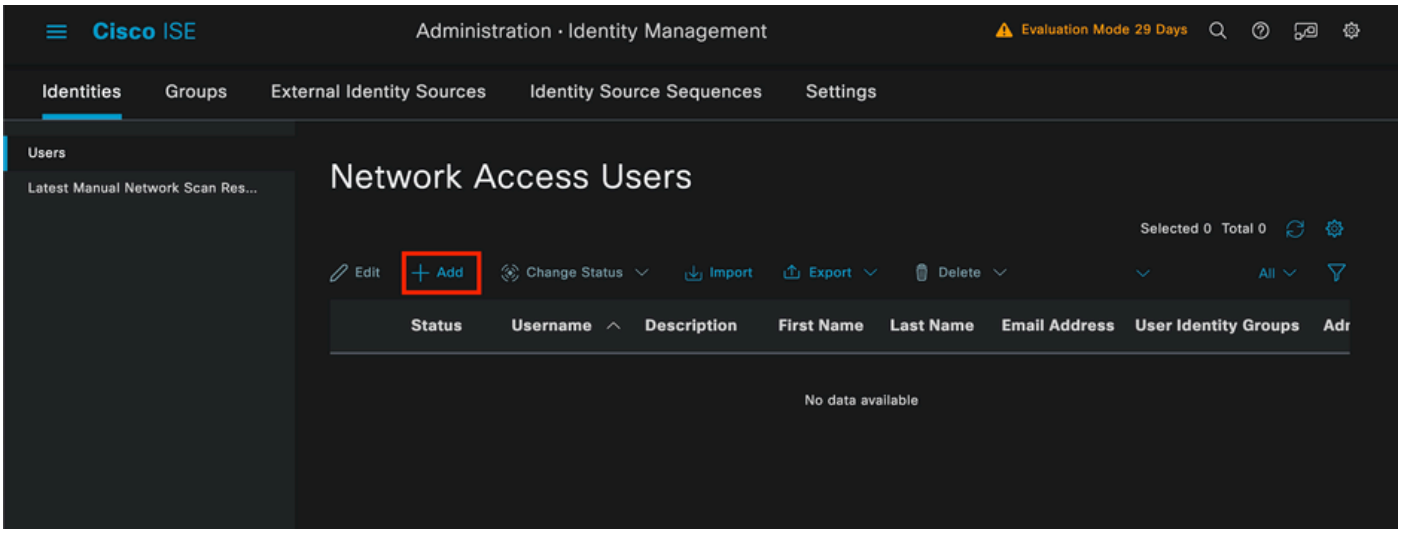


身份组创建

单击“Submit”。

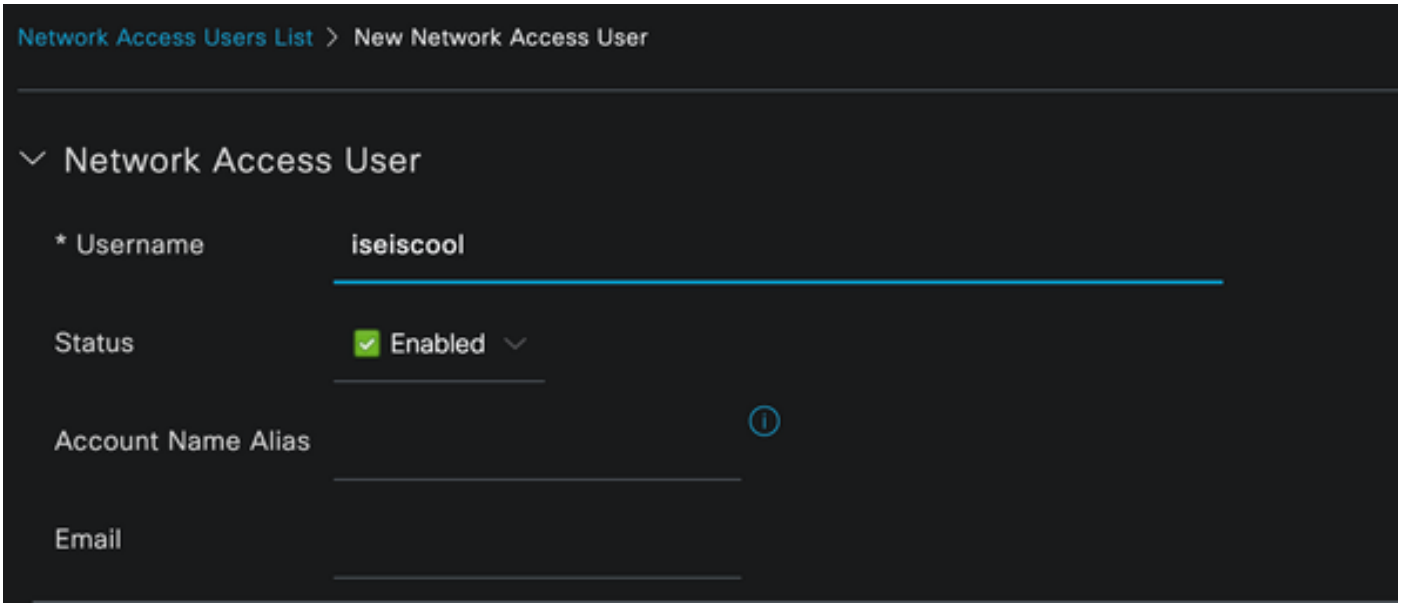
导航到管理>身份管理>身份选项卡。

单击 Add。



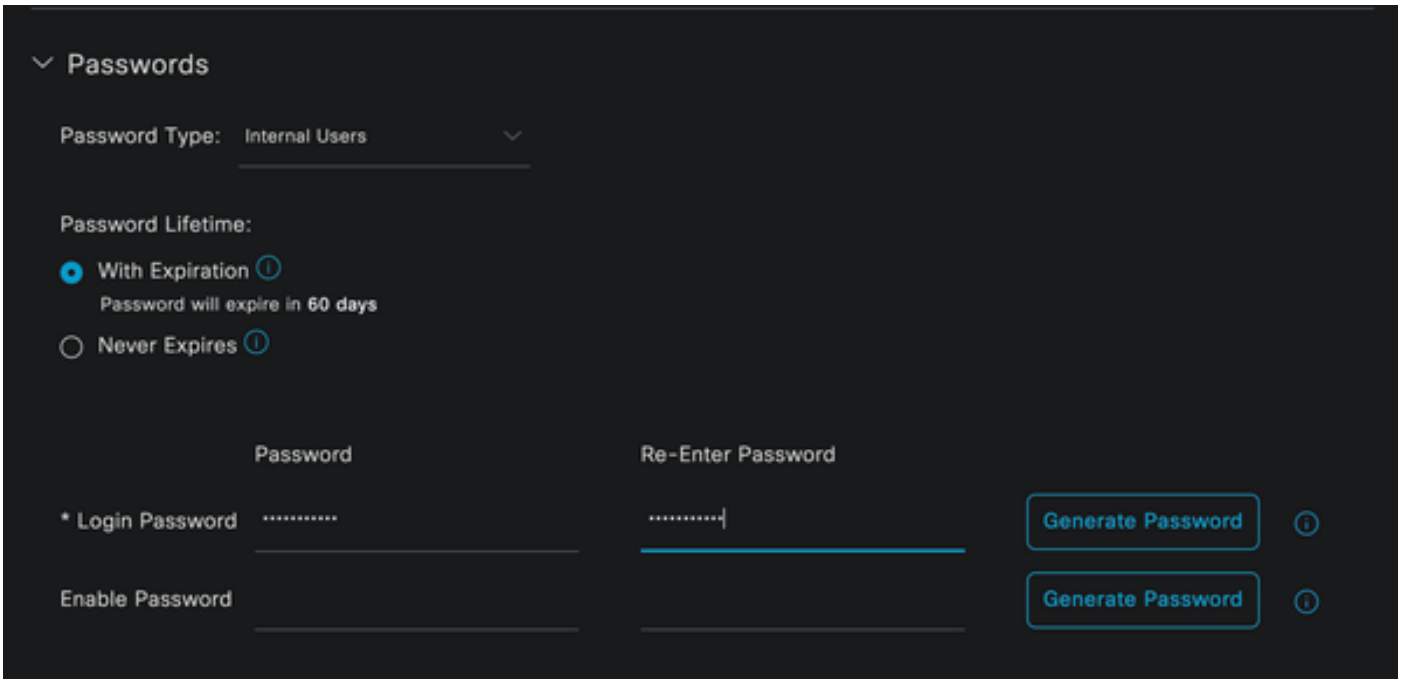
网络访问用户部分

作为必填字段的一部分，以用户的名称开头。此示例中使用用户名iseiscool。



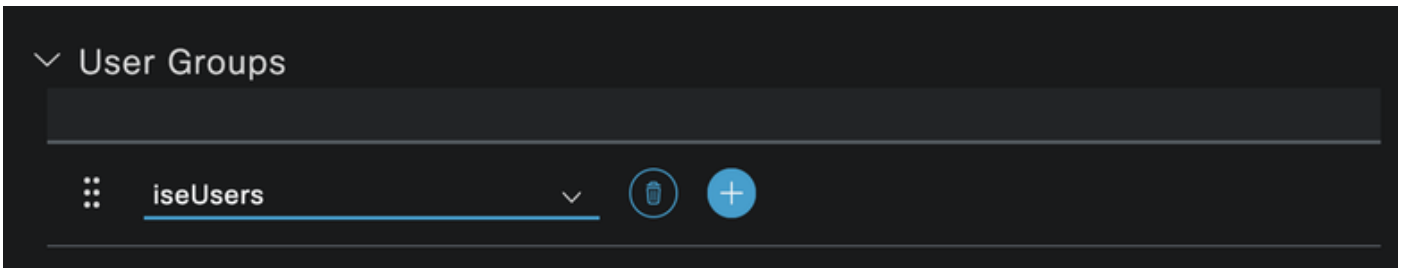
网络访问用户创建

为用户指定密码。 使用VainillaISE97。



User Creation Password部分

将用户分配到iseUsers组。

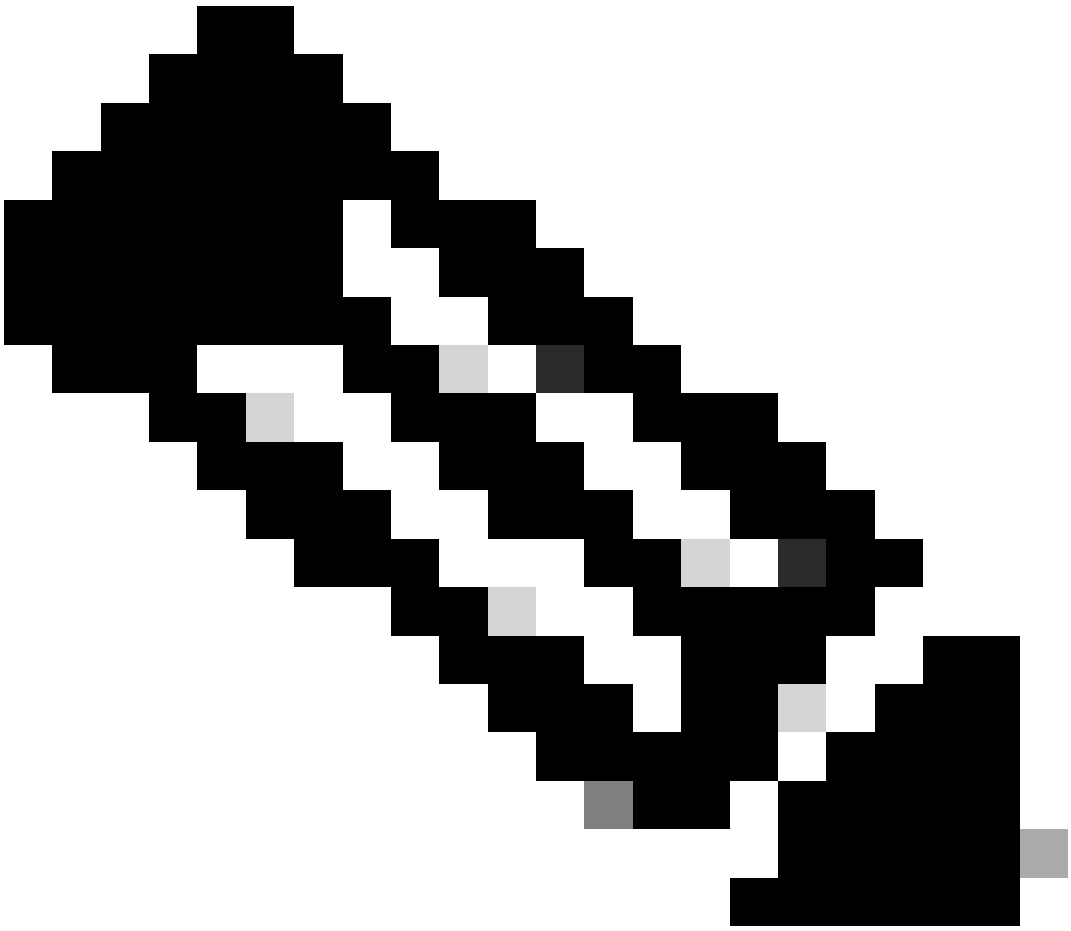


用户组分配

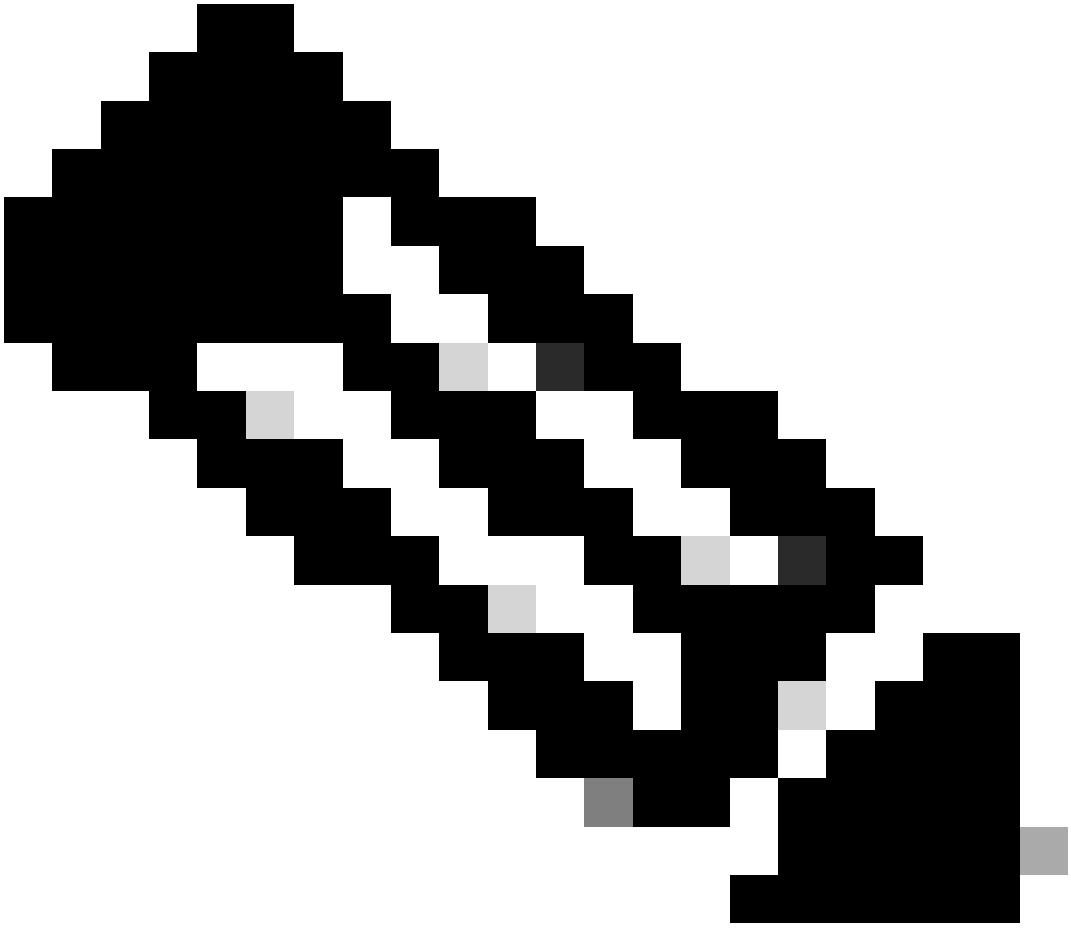
配置策略集。

导航到ISE菜单>策略>策略集。

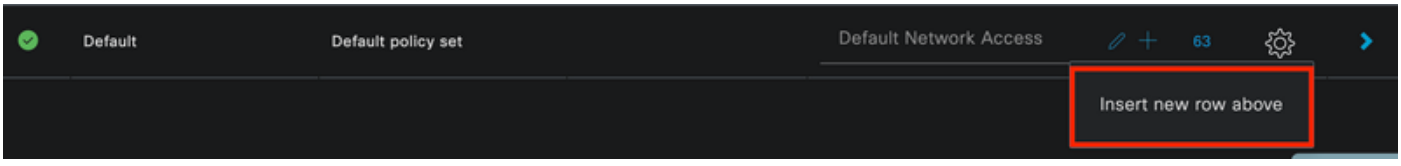
可以使用默认策略集。但是，本示例创建了一个名为Wired的示例。



注意：对策略集进行分类和差异化有助于排除故障，

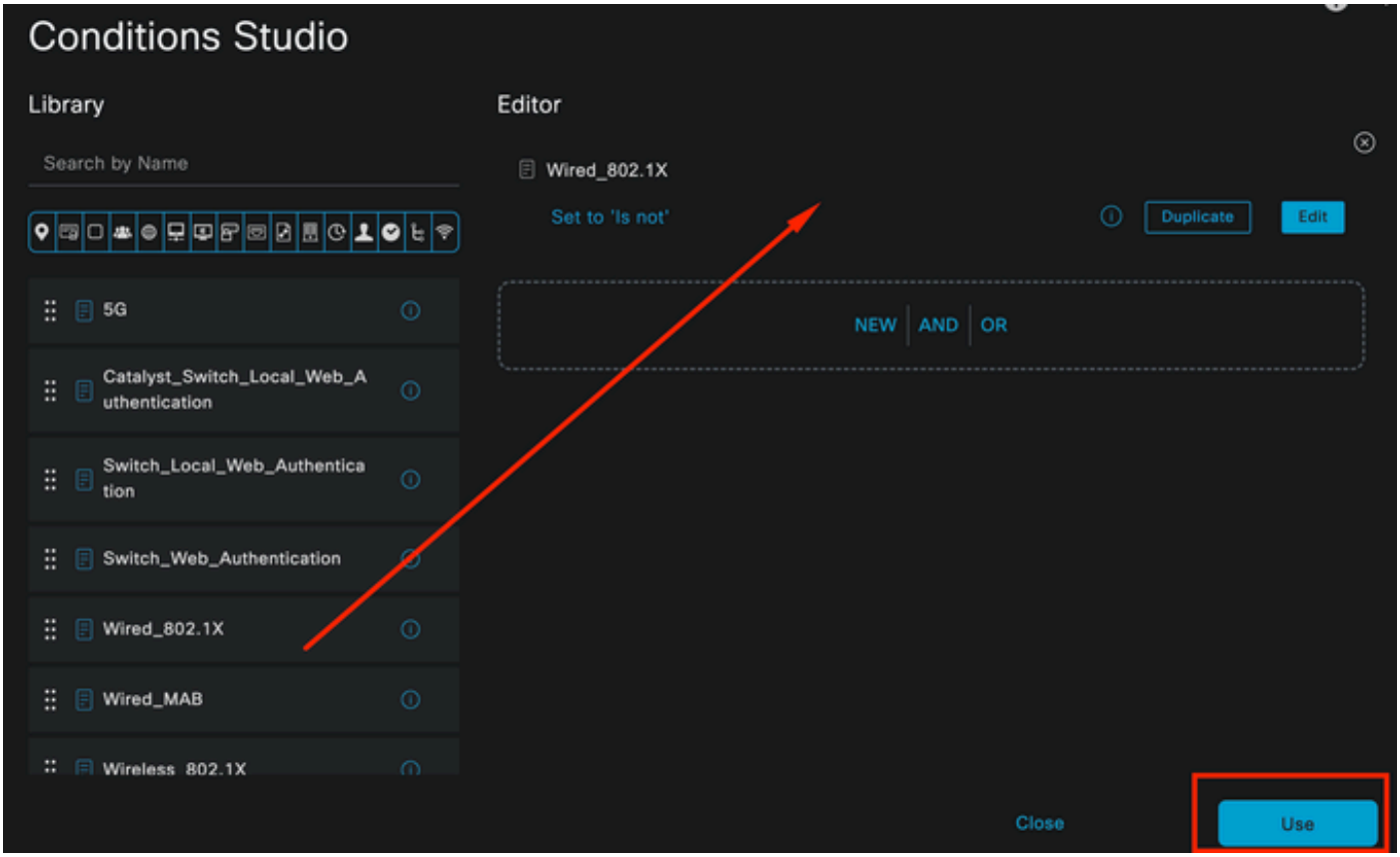


注意：如果看不到添加或加号图标，可以点击任何策略集的齿轮图标，然后选择在上方插入新行。



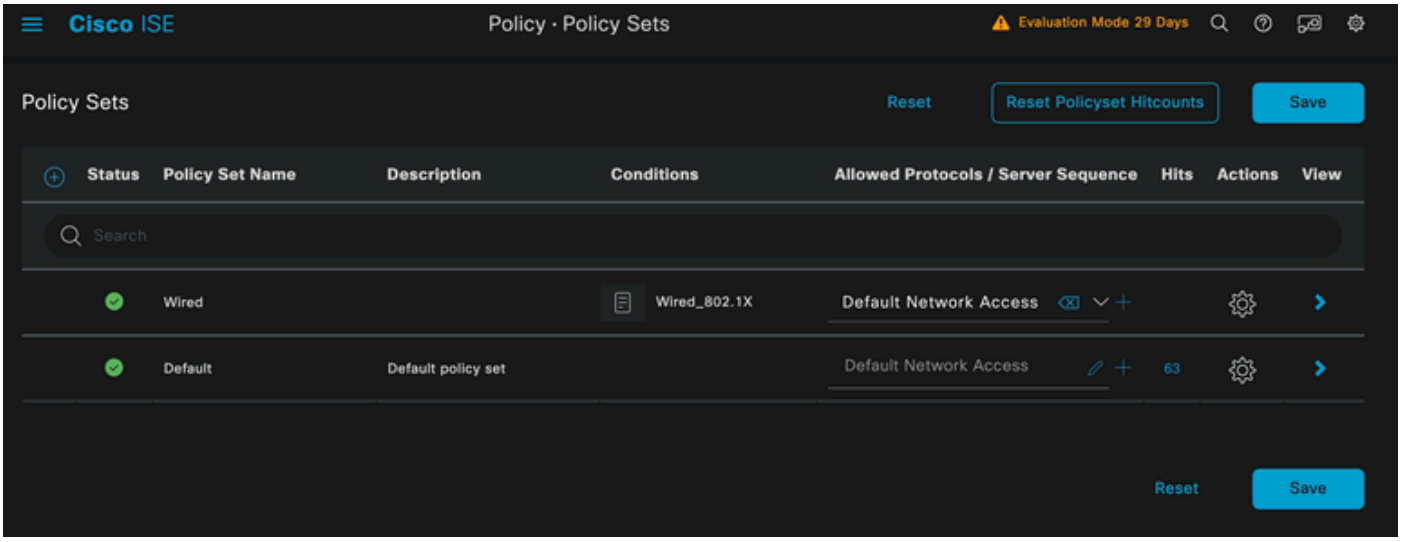
齿轮图标选项

使用的条件是有线8021x。拖动它，然后单击使用。



身份验证策略条件工作室

在允许的协议部分中选择默认网络访问。

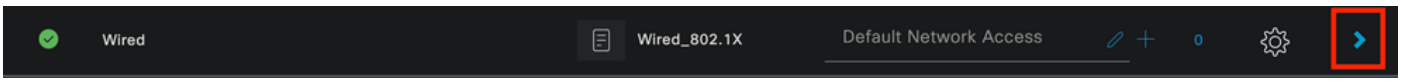


策略集一般视图

Click Save.

2.d.配置身份验证和授权策略。

单击>图标。



有线策略集

展开Authentication Policy部分。

点击+图标。

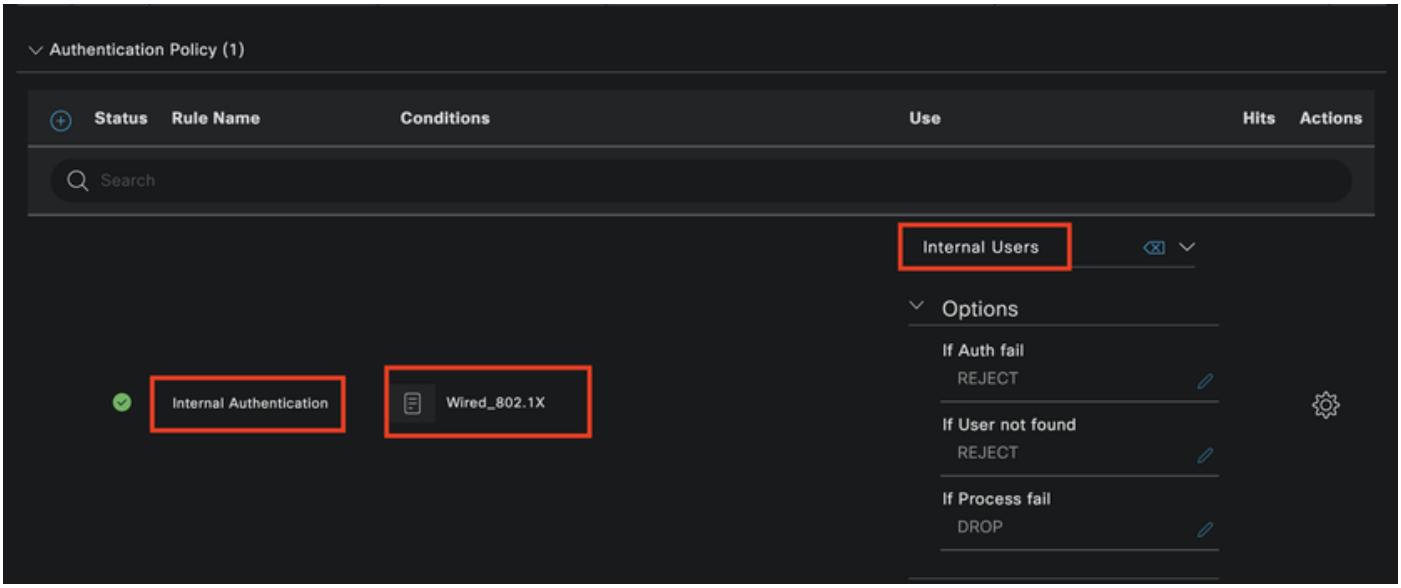
验证策略

为身份验证策略指定名称。 此示例中使用内部身份验证。

点击此新身份验证策略的条件列上的+图标。

使用的是预配置条件Wired Dot1x。

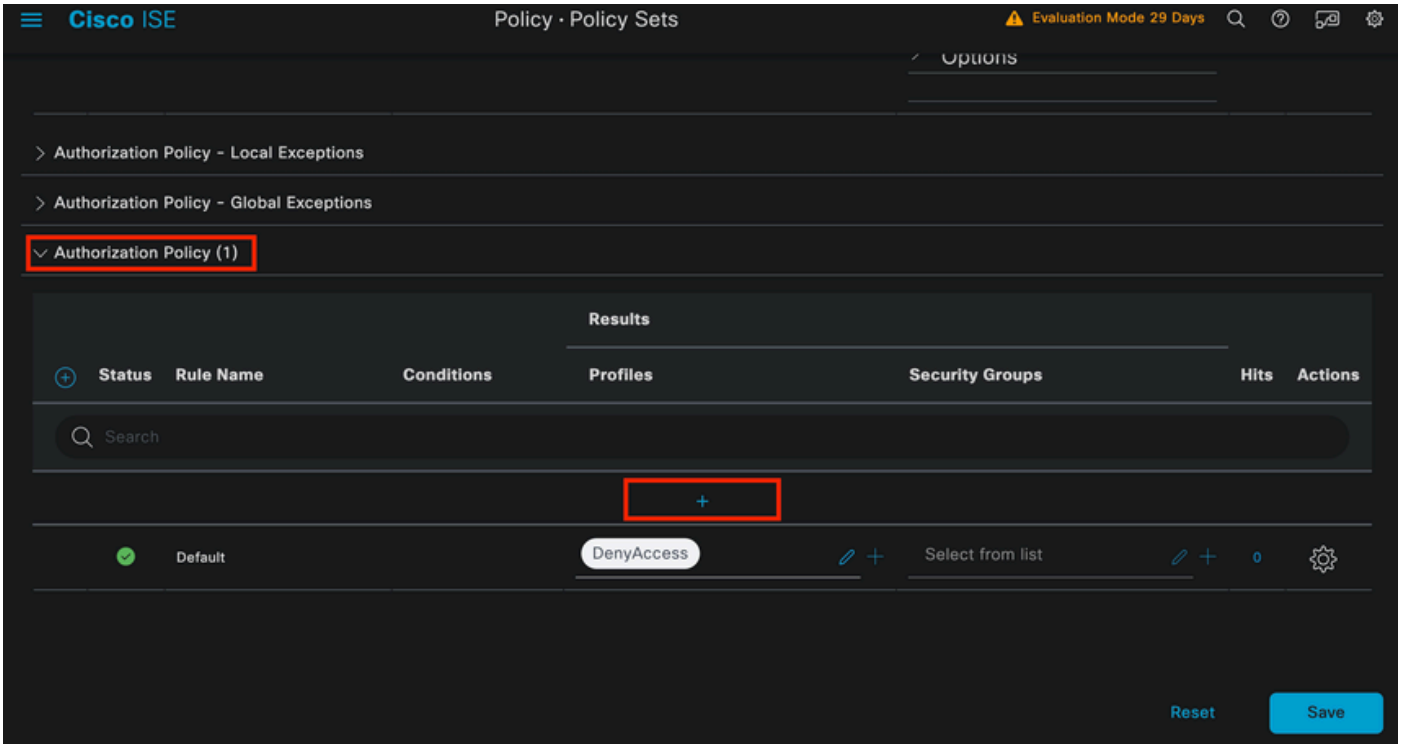
最后，在使用列中选择内部用户。



验证策略

授权策略.

授权策略部分位于页面底部。展开并单击+图标。



授权策略

命名最近创建的授权策略。 在此配置示例中，使用了名称Internal ISE Users。

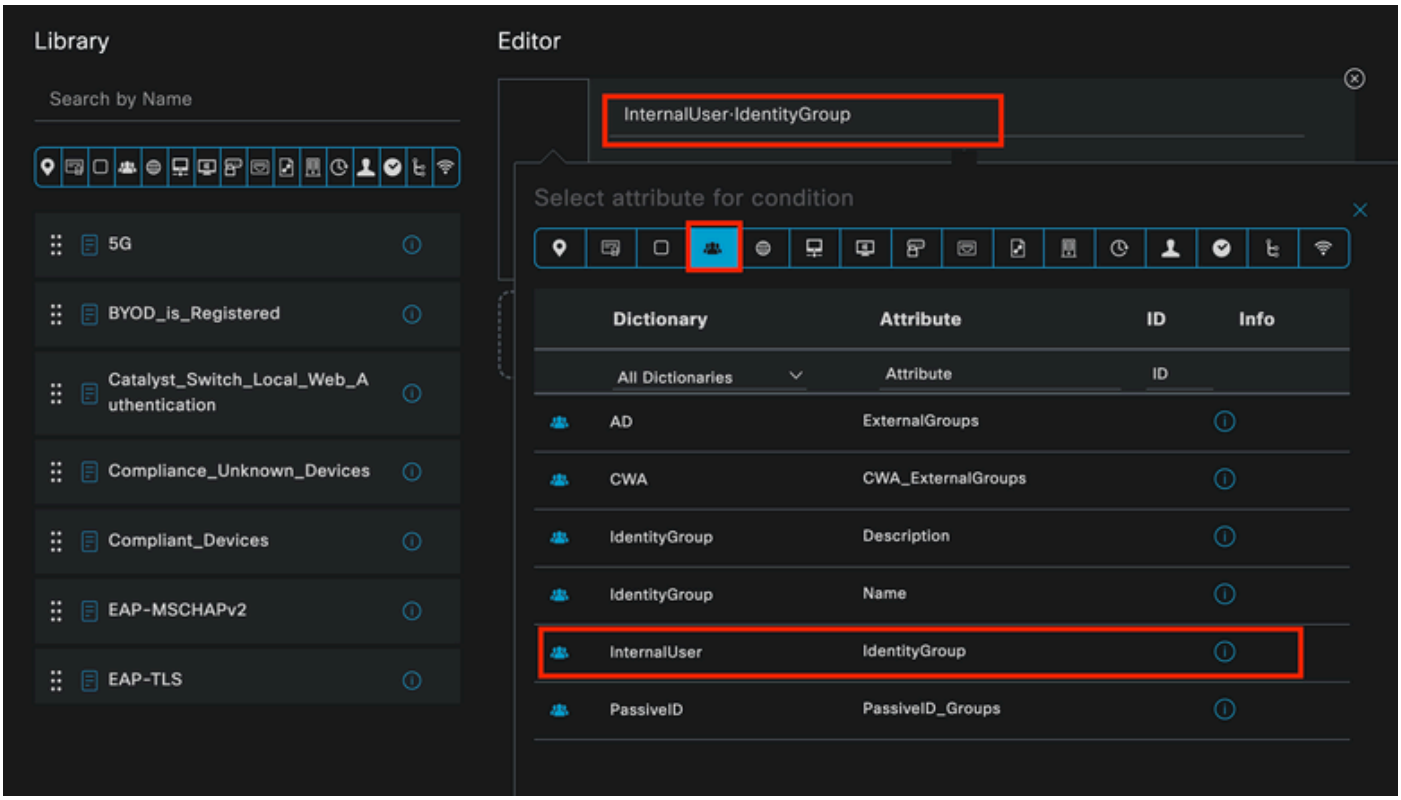
要为此授权策略创建条件，请在条件列中点击+图标。

使用组IseUsers。

单击属性部分。

选择IdentityGroup图标。

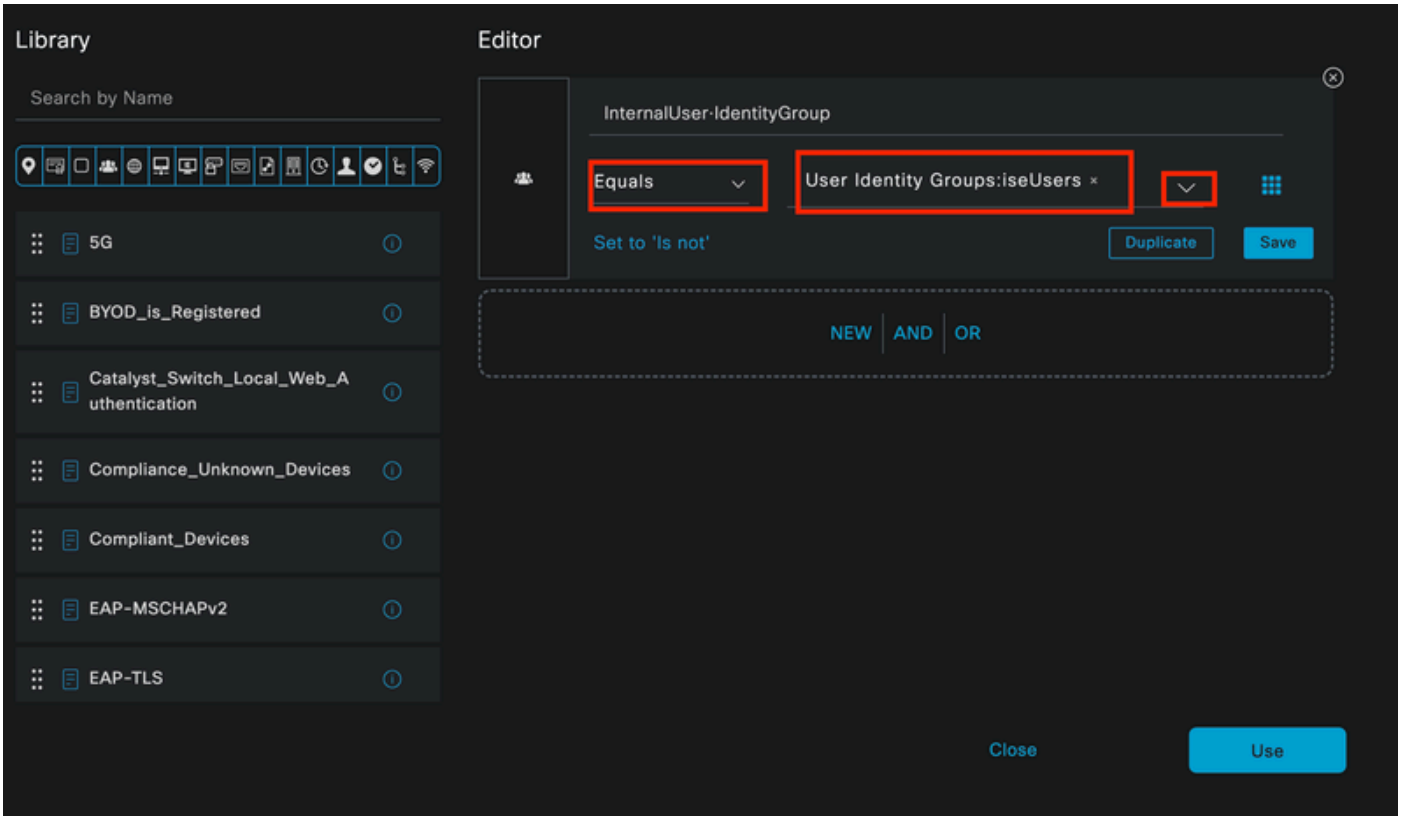
从字典中选择带有IdentityGroup属性的InternalUser字典。



条件创建

选择Equals运算符。

从用户身份组中，选择组IseUsers。

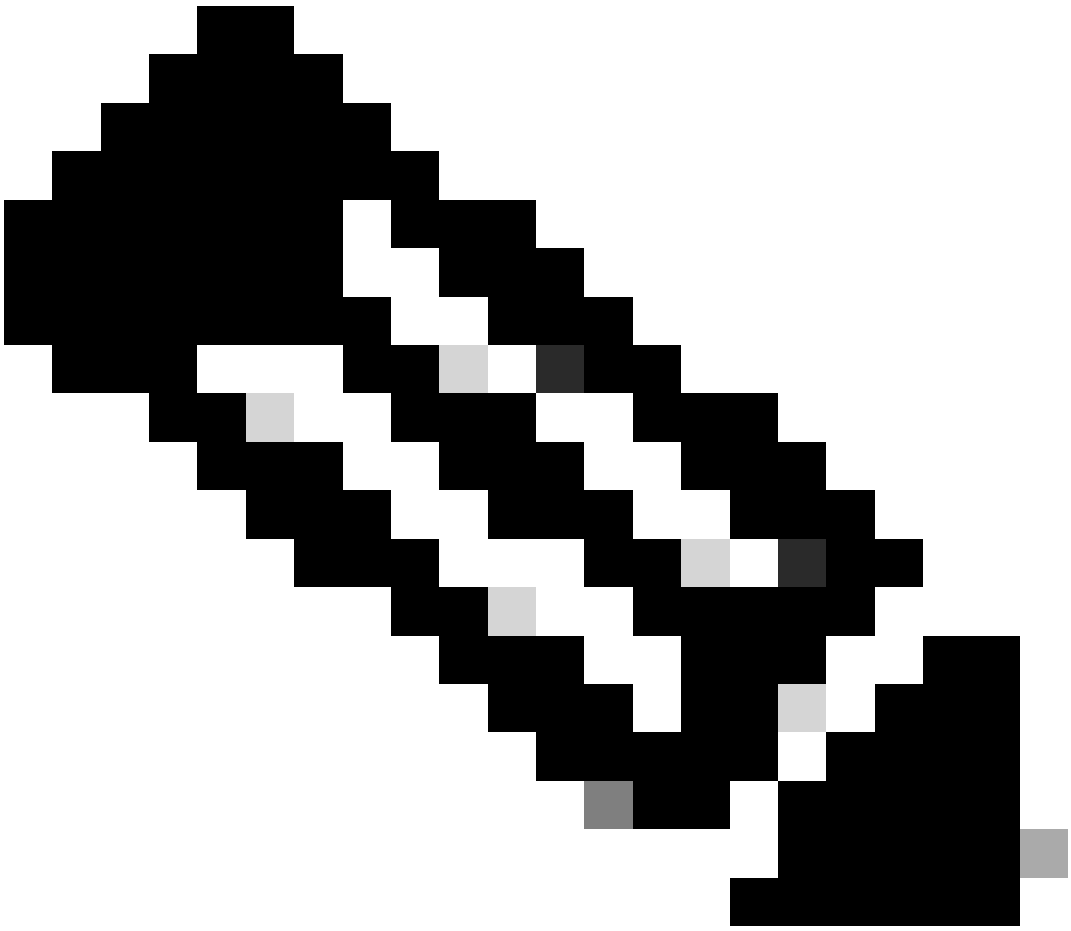


条件创建

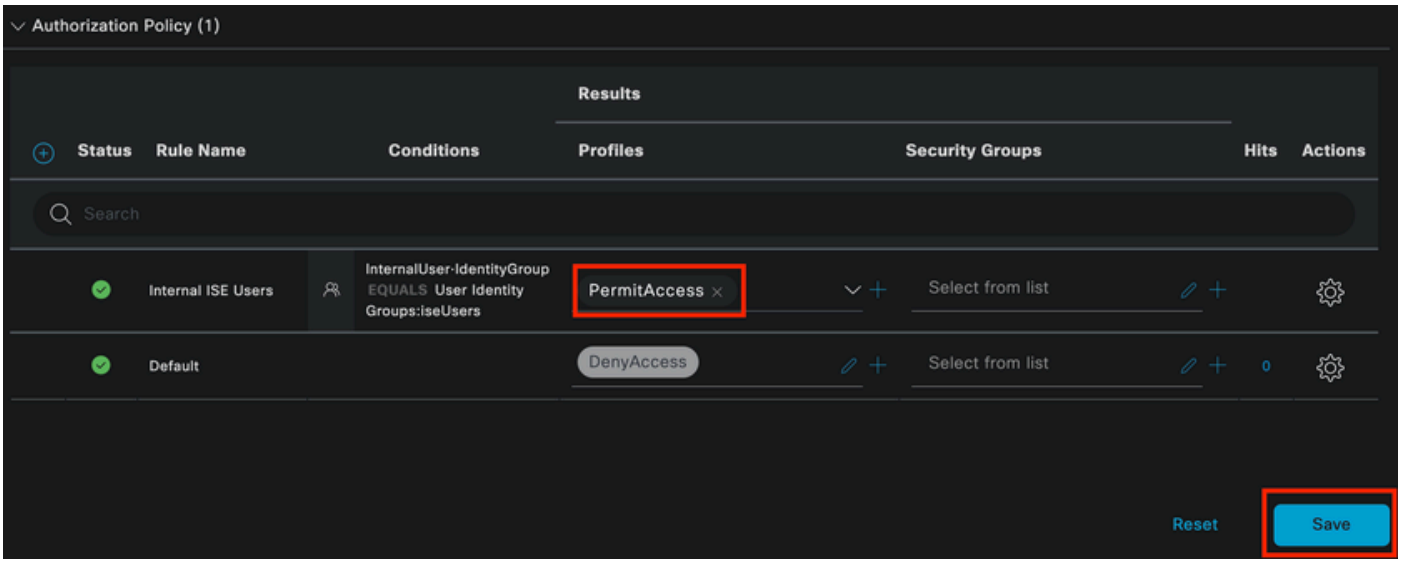
单击Use。

添加结果授权配置文件。

使用预配置的配置文件Permit Access。



注意：请注意，到达此有线Dot1x策略集（不属于用户身份组ISEUsers的一部分）的ISE的身份验证命中默认授权策略，其结果为DenyAccess。



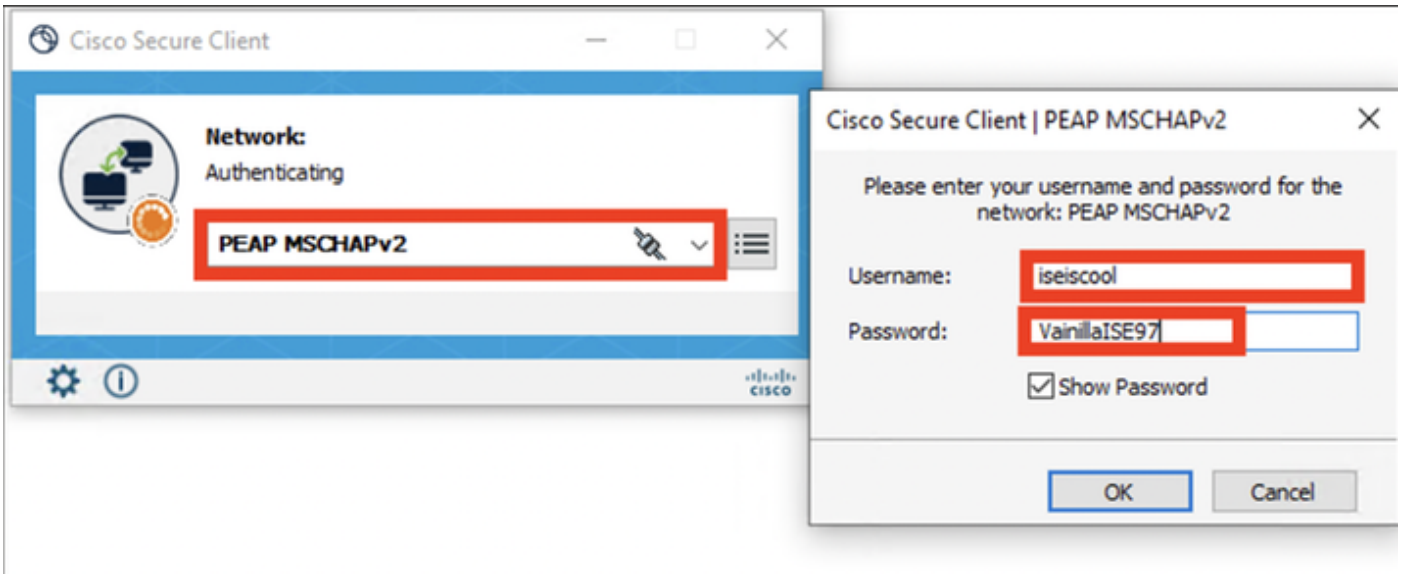
授权策略

Click Save.

验证

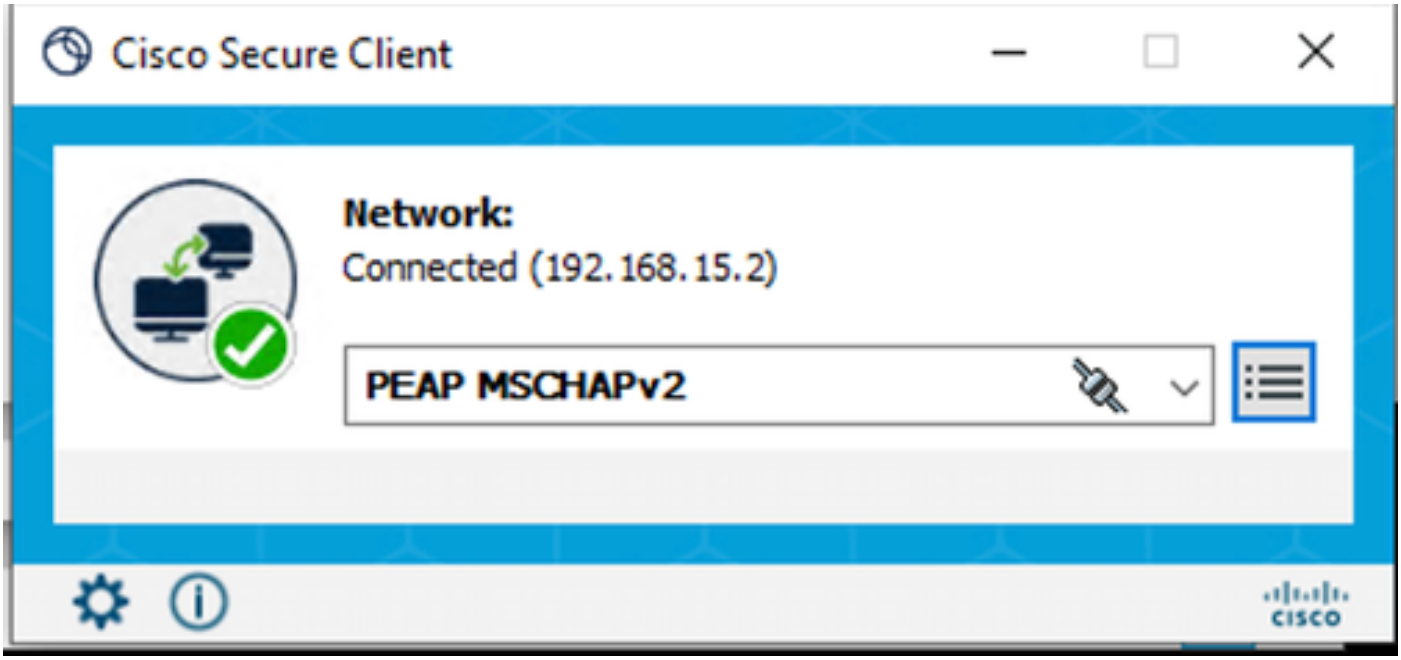
配置完成后，安全客户端将提示输入凭证，并指定PEAP MSCHAPv2配置文件的用法。

输入先前创建的凭证。



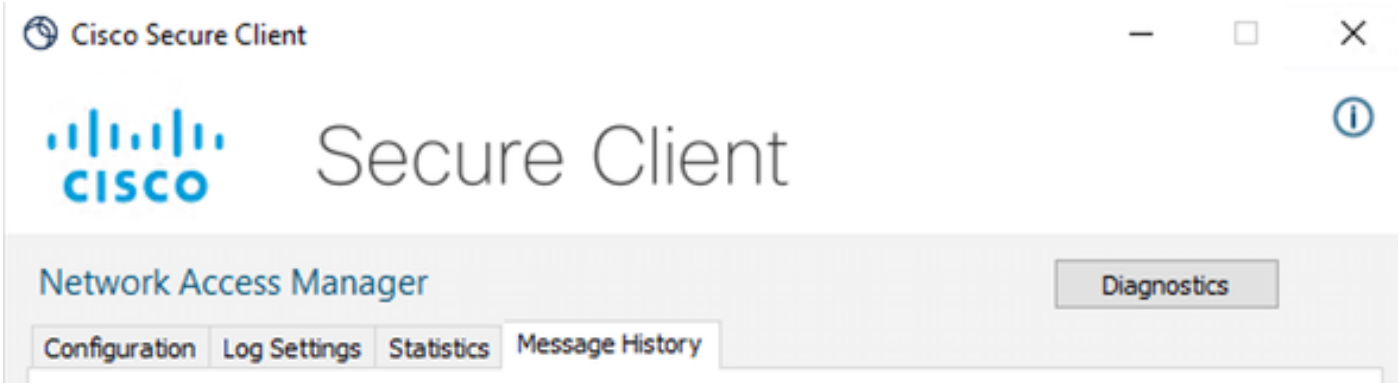
安全客户端*NAM*

如果终端身份验证正确，。 NAM显示其已连接。

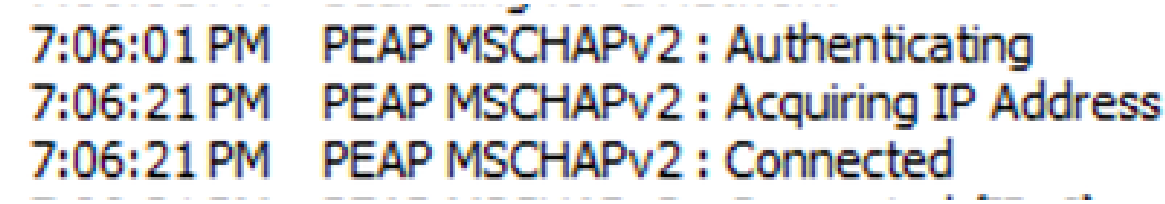


安全客户端*NAM*

通过点击信息图标并导航到消息历史记录部分，可显示NAM执行的每个步骤的详细信息。



安全客户端消息历史记录



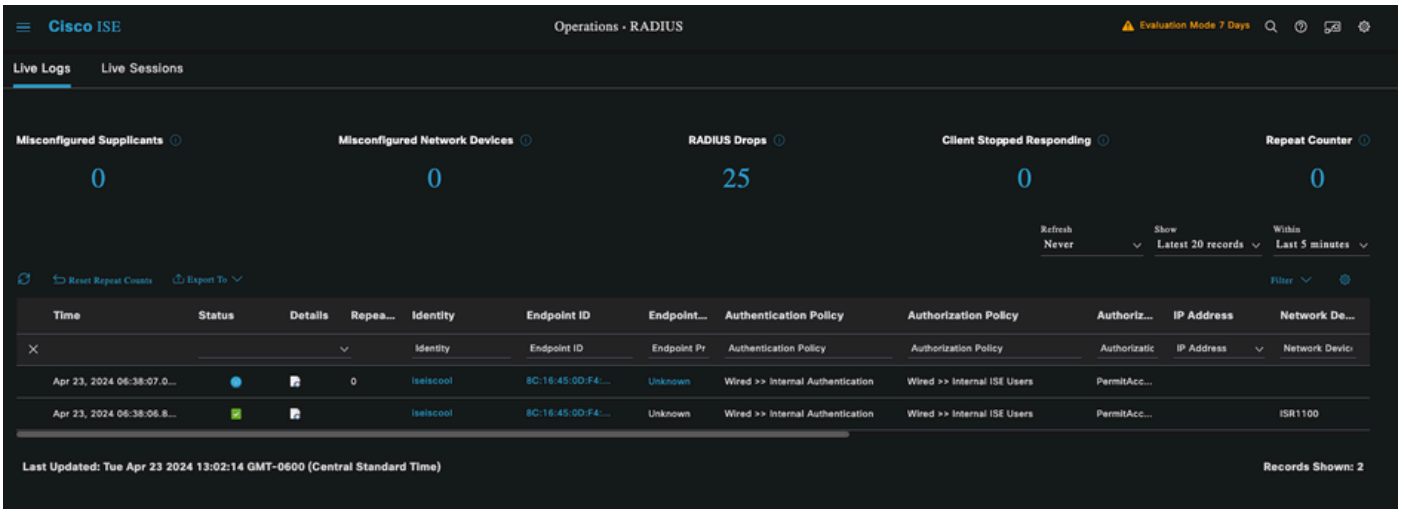
安全客户端消息历史记录

从ISE导航到操作> Radius LiveLogs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，例如：

- 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

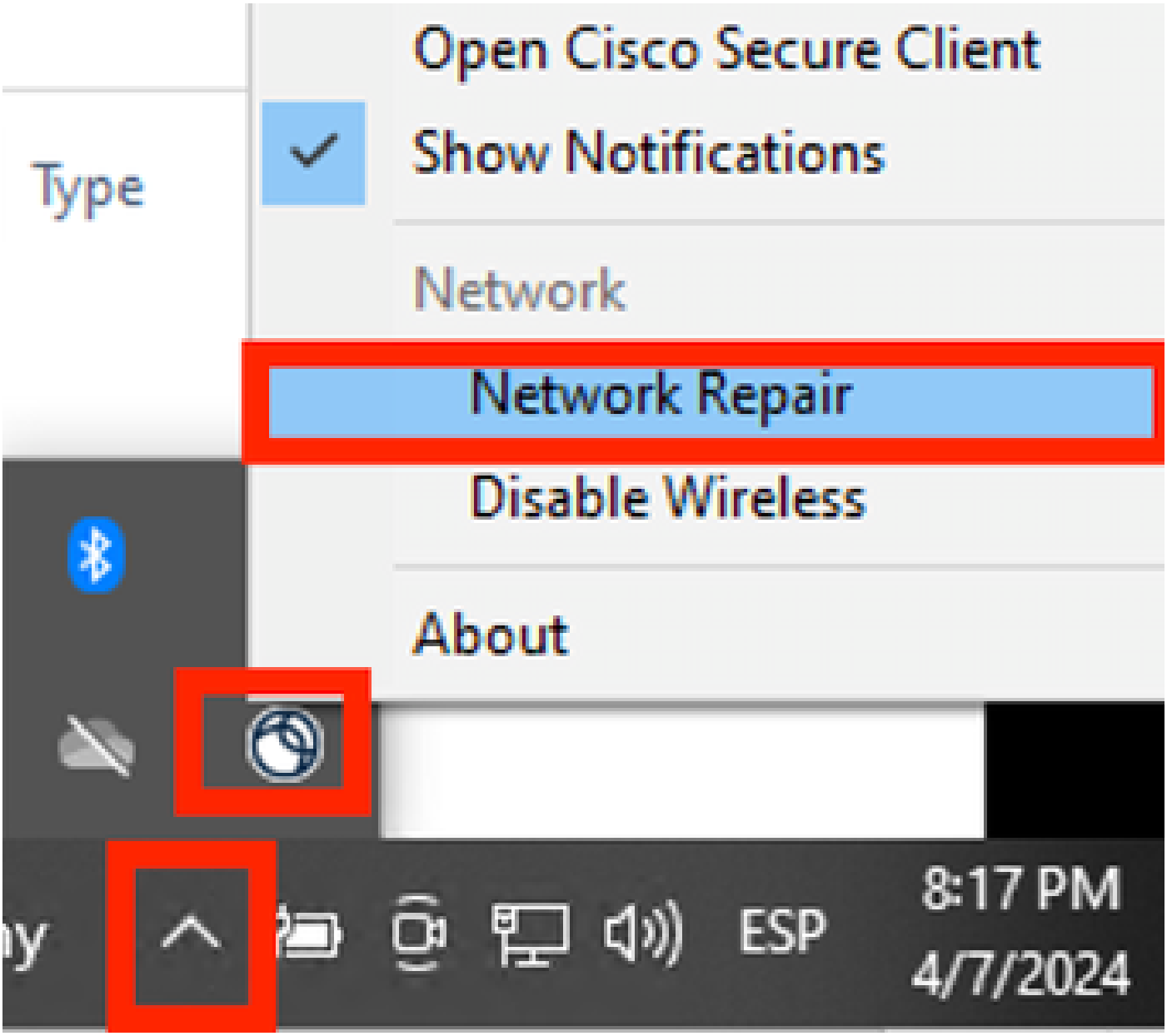
由于您可以看到它符合正确的策略，并且结果为成功的身份验证状态，因此可以断定配置是正确的。

故障排除

问题：安全客户端未使用NAM配置文件。

如果NAM未使用在配置文件编辑器中创建的新配置文件，请为安全客户端使用网络修复选项。

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。



Network Repair部分

问题2：需要收集日志以进行进一步分析。

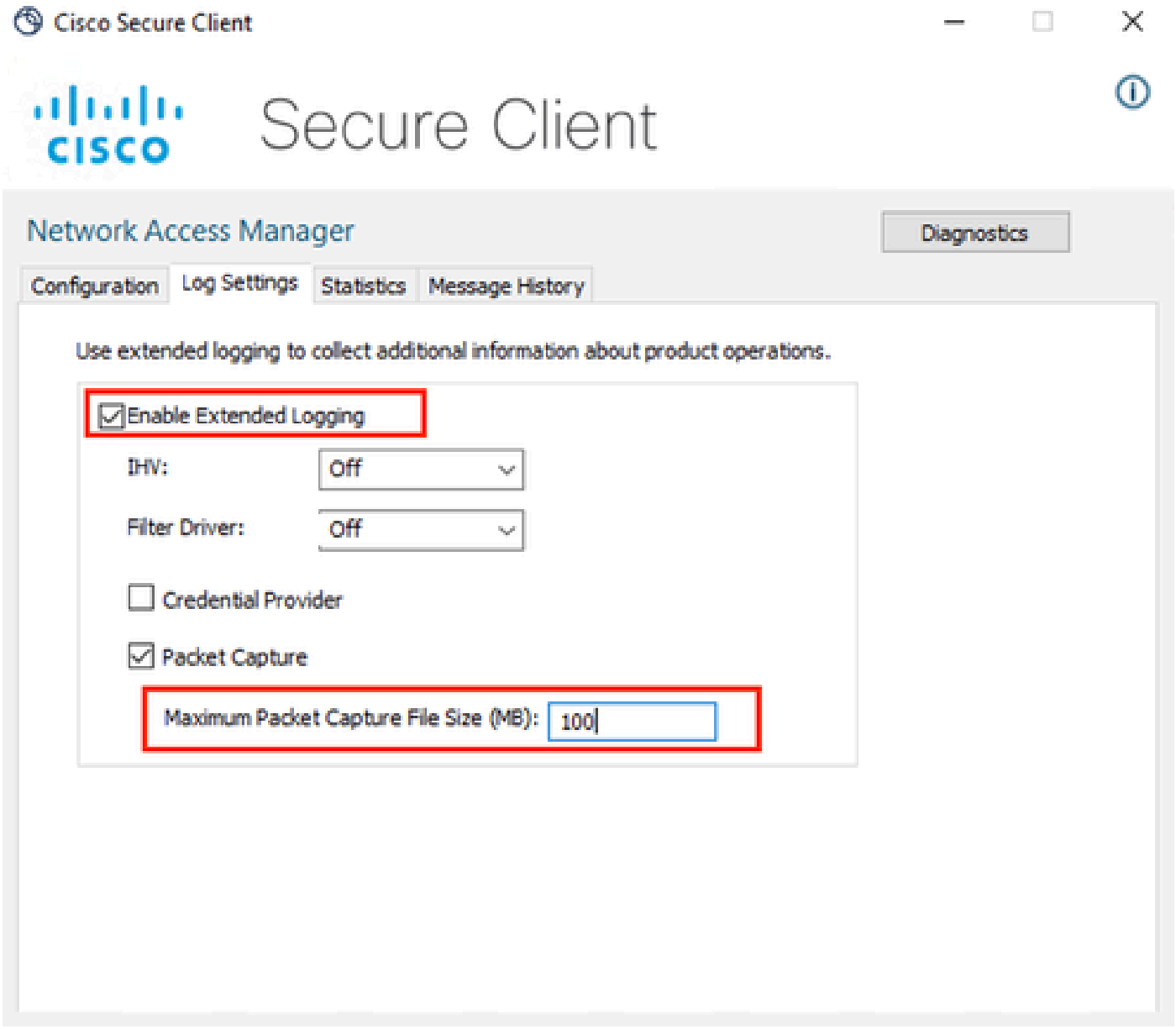
1. 启用NAM扩展日志记录

打开NAM，然后点击齿轮图标。

NAM接口

导航到日志设置选项卡。选中Enable Extended Logging复选框。

将数据包捕获文件大小设置为100 MB。



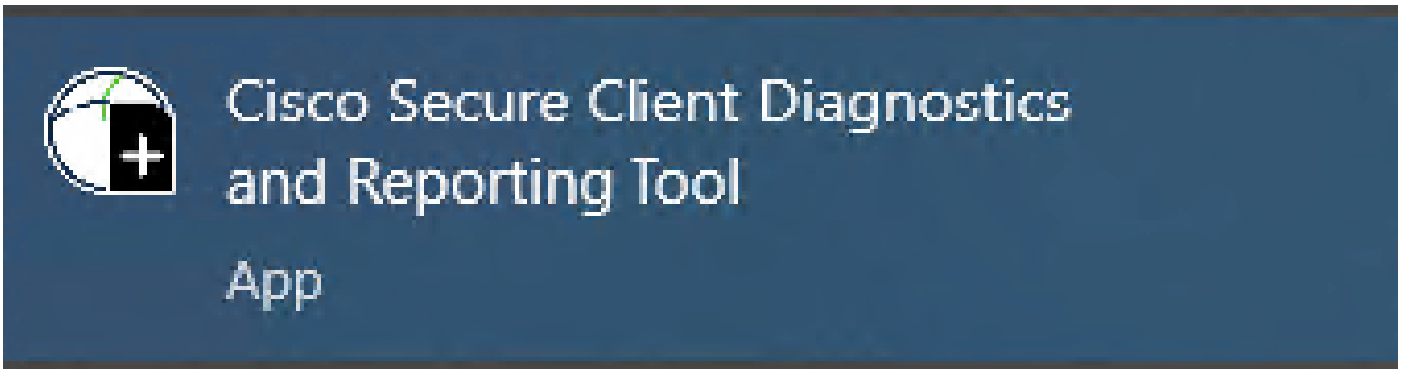
安全客户端NAM日志设置

2. 重现问题。

启用扩展日志记录后，系统会多次重现该问题，以确保生成日志并捕获流量。

3. 收集安全客户端DART捆绑包。

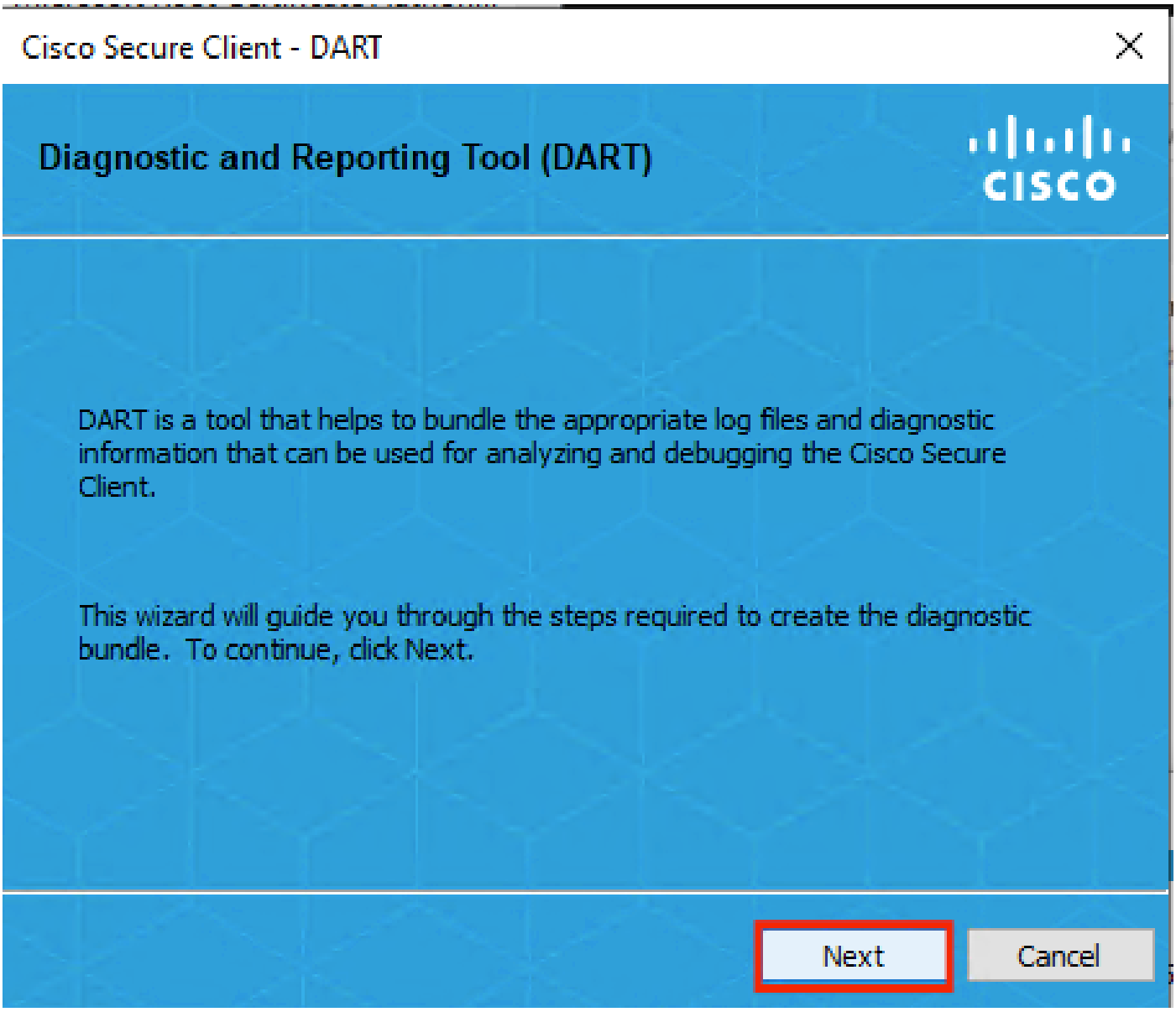
在Windows中，导航到搜索栏并键入Cisco Secure Client Diagnostics and Reporting Tool。



DART模块

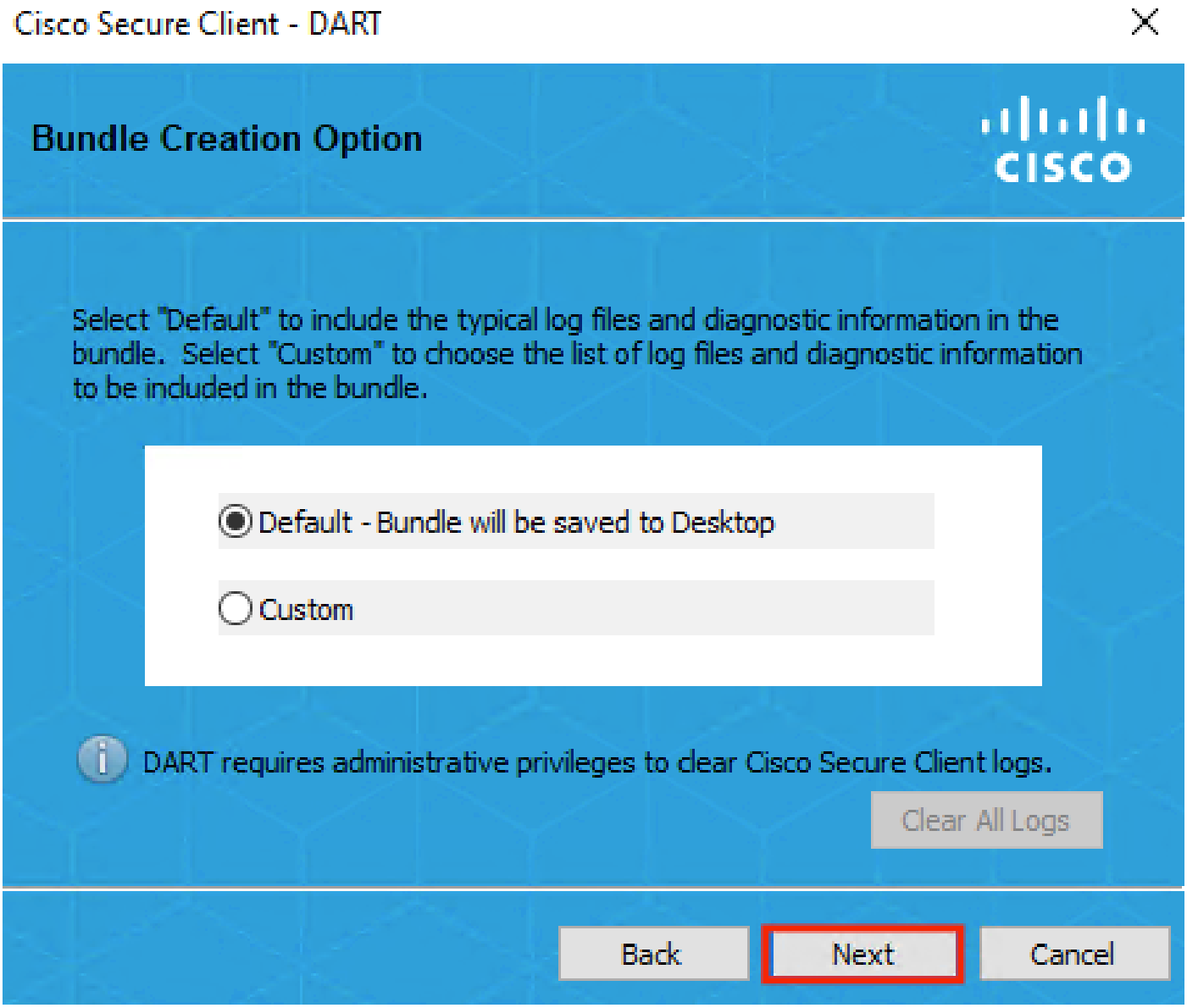
在安装过程中，您还安装了此模块。该工具通过收集日志和相关dot1x会话信息，在故障排除过程中提供帮助。

在第一个窗口中单击Next。



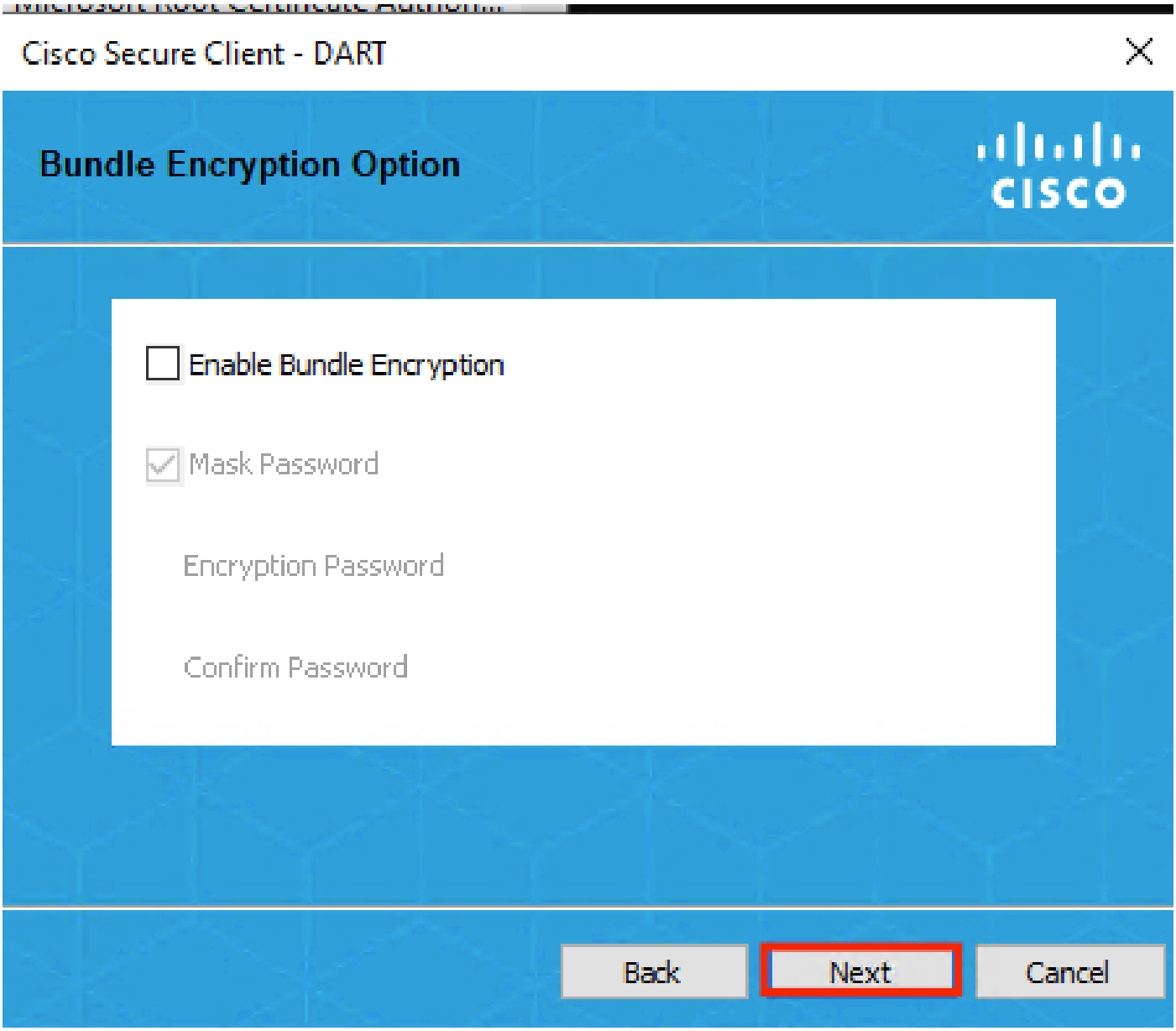
DART模块

再次单击Next，以便将日志捆绑包保存在桌面上。



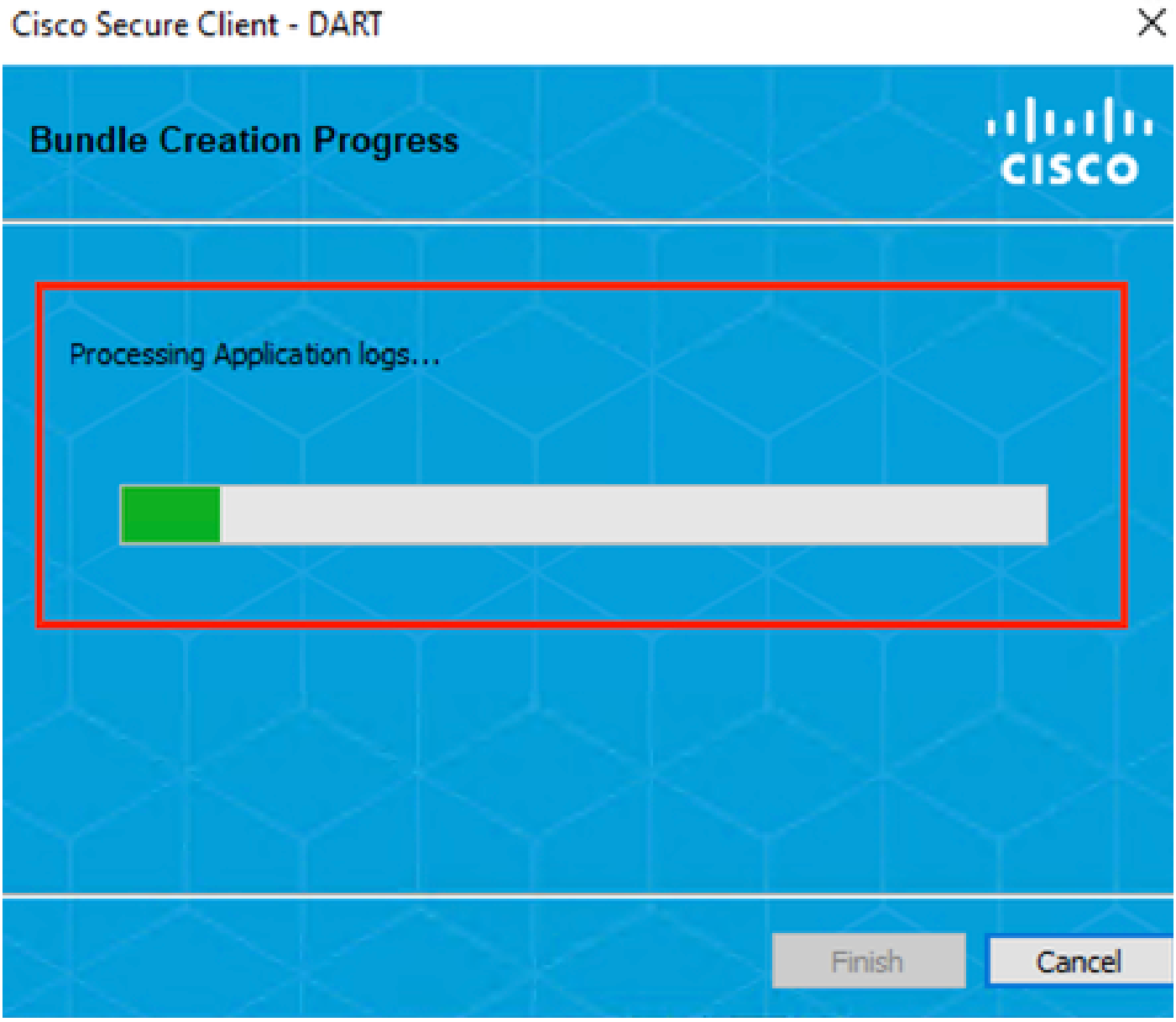
DART模块

如果需要，请选中Enable Bundle Encryption复选框。



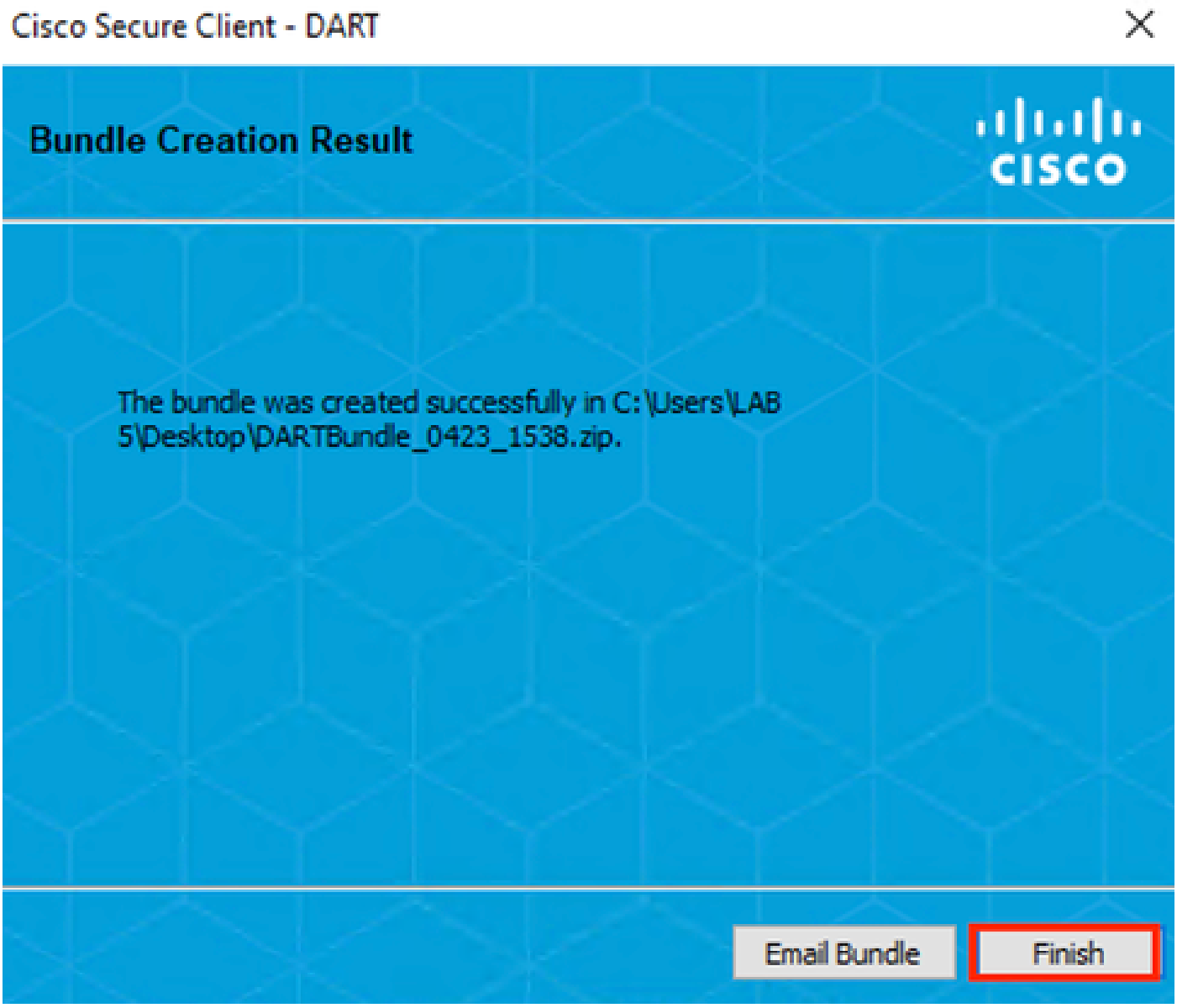
DART模块

DART日志收集开始。



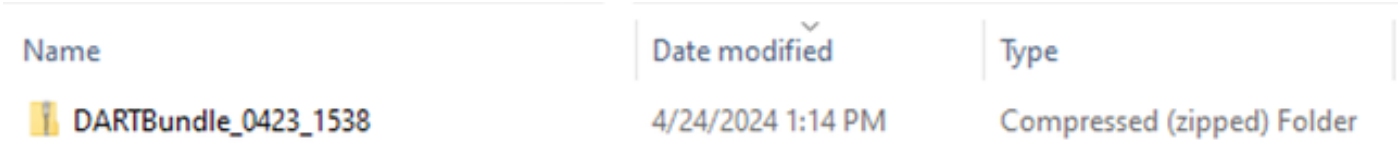
DART日志收集

完成此过程可能需要10分钟或更长时间。



DART捆绑包创建结果

在桌面目录中可找到DART结果文件。



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）。

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）。