

802.1x WLAN + VLAN覆盖(使用Mobility Express(ME)8.2和ISE 2.1)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[ME上的配置](#)

[在ISE上声明ME](#)

[在ISE上创建新用户](#)

[创建身份验证规则](#)

[创建授权规则](#)

[终端设备配置](#)

[验证](#)

[ME上的身份验证过程](#)

[ISE上的身份验证过程](#)

简介

本文档介绍如何使用Mobility Express控制器和外部远程身份验证拨入用户服务(RADIUS)服务器设置WLAN (无线局域网) ，并使用Wi-Fi保护访问2(WPA2)企业安全。身份服务引擎(ISE)用作外部RADIUS服务器的示例。

本指南中使用的可扩展身份验证协议(EAP)是受保护的可扩展身份验证协议(PEAP)。此外，客户端被分配到特定VLAN (默认情况下，除分配给WLAN的VLAN外) 。

先决条件

要求

Cisco 建议您了解以下主题：

- 802.1x
- PEAP
- 认证中心(CA)
- 证书

使用的组件

本文档中的信息基于以下软件和硬件版本：

ME v8.2

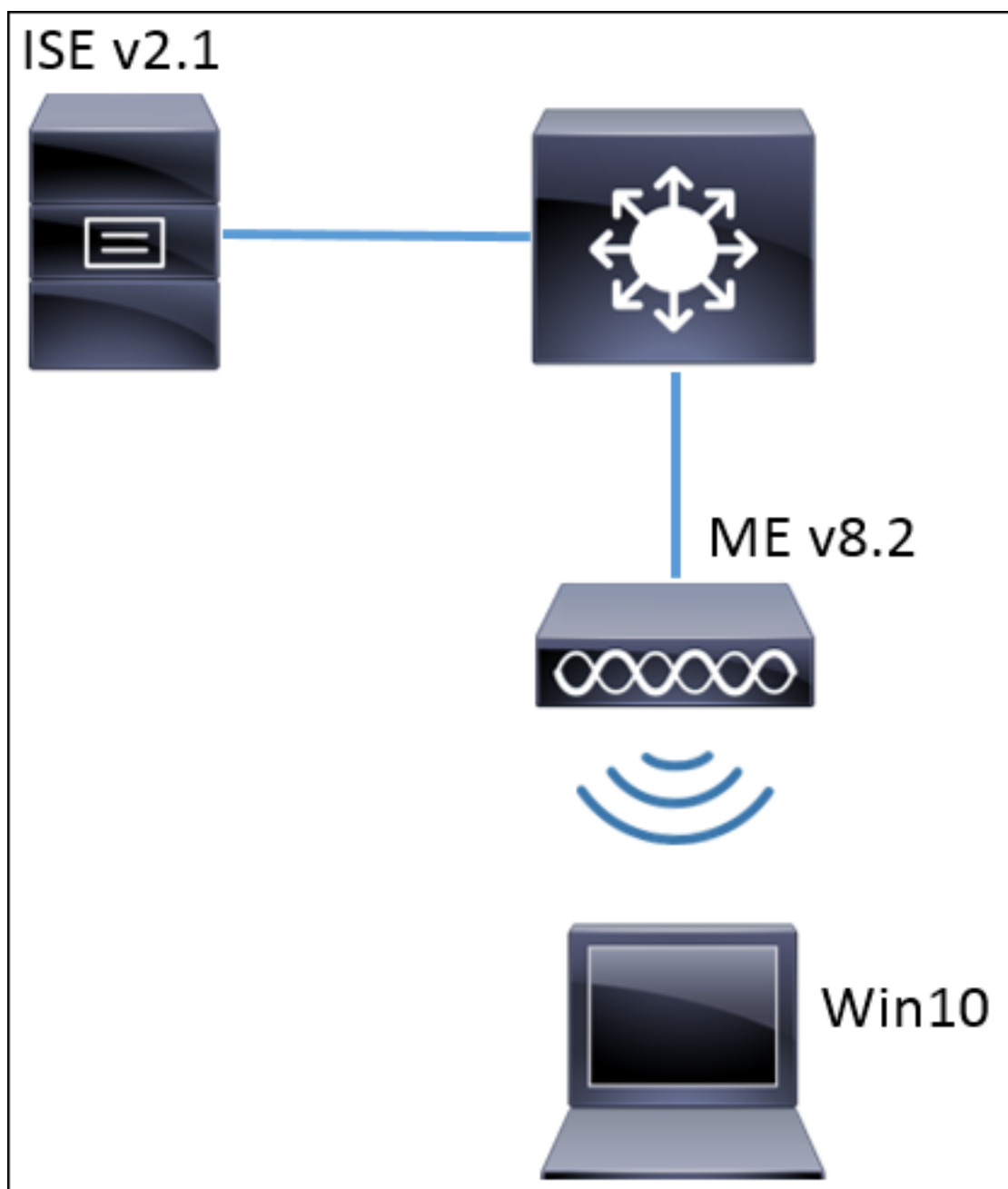
ISE v2.1

Windows 10笔记本电脑

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络图



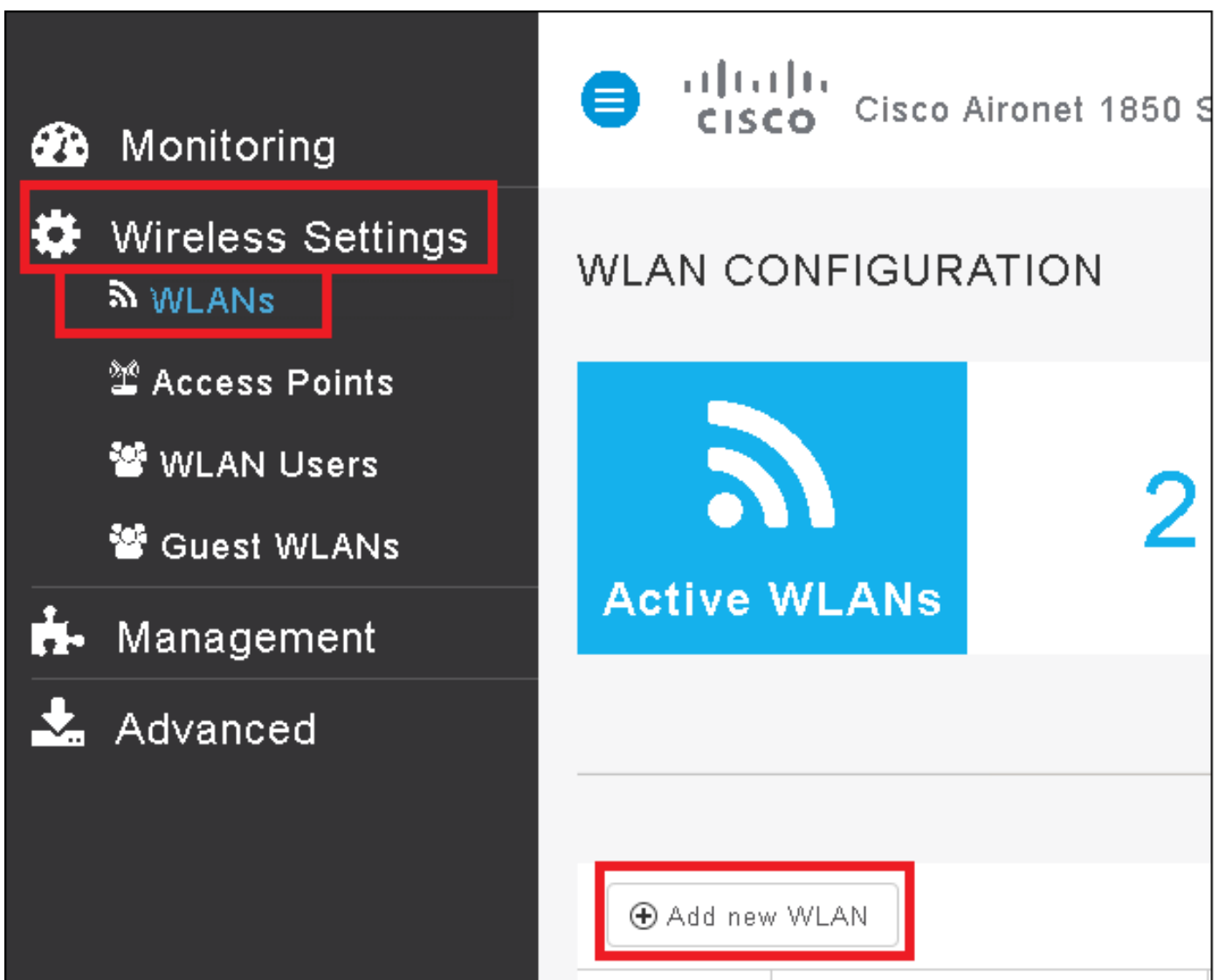
一般步骤为：

1. 在ME中创建服务集标识符(SSID)，并在ME上声明RADIUS服务器（本示例中为ISE）
2. 在RADIUS服务器(ISE)上声明ME
3. 在ISE上创建身份验证规则
4. 在ISE上创建授权规则
5. 配置终端

ME上的配置

为了允许RADIUS服务器与ME之间的通信，需要在ME上注册RADIUS服务器，反之亦然。此步骤显示如何在ME上注册RADIUS服务器。

步骤1.打开ME的GUI并导航至 **无线设置> WLANs >添加新WLAN**。



步骤2.为WLAN选择名称。

The screenshot shows a configuration window titled "Add New WLAN" with a close button (X) in the top right corner. Below the title bar are four tabs: "General", "WLAN Security", "VLAN & Firewall", and "QoS". The "General" tab is currently selected and underlined. The configuration fields are as follows:

WLAN Id	3
Profile Name *	me-ise
SSID *	me-ise
Admin State	Enabled
Radio Policy	ALL

At the bottom right of the window, there are two buttons: "Apply" (with a checkmark icon) and "Cancel" (with an X icon).

步骤3.在“WLAN安全”选项卡下指定安全配置。

选择**WPA2 Enterprise**，对于Authentication server，选择**External RADIUS**。单击编辑选项以添加RADIUS的IP地址并选择**共享密钥**密钥。



Add New WLAN



General WLAN Security VLAN & Firewall QoS

Security WPA2 Enterprise ▼

Authentication Server External Radius ▼

	Radius IP ▲	Radius Port	Shared Secret	
		1812	*****	▲
		1812	*****	▼

External Radius configuration applies to all WLANs

Apply

Cancel

Add New WLAN

General WLAN Security VLAN & Firewall QoS

Security WPA2 Enterprise

Authentication Server External Radius

Radius IP ▲ Radius Port Shared Secret

a.b.c.d 1812

Please enter valid IPv4 address

External Radius configuration applies to all WLANs

Apply Cancel

<a.b.c.d>对应于RADIUS服务器。

步骤4.为SSID分配VLAN。

如果需要将SSID分配给AP的VLAN，可跳过此步骤。

要将此SSID的用户分配给特定VLAN（AP的VLAN除外），请启用**使用VLAN**标记并分配所需的VLAN ID。

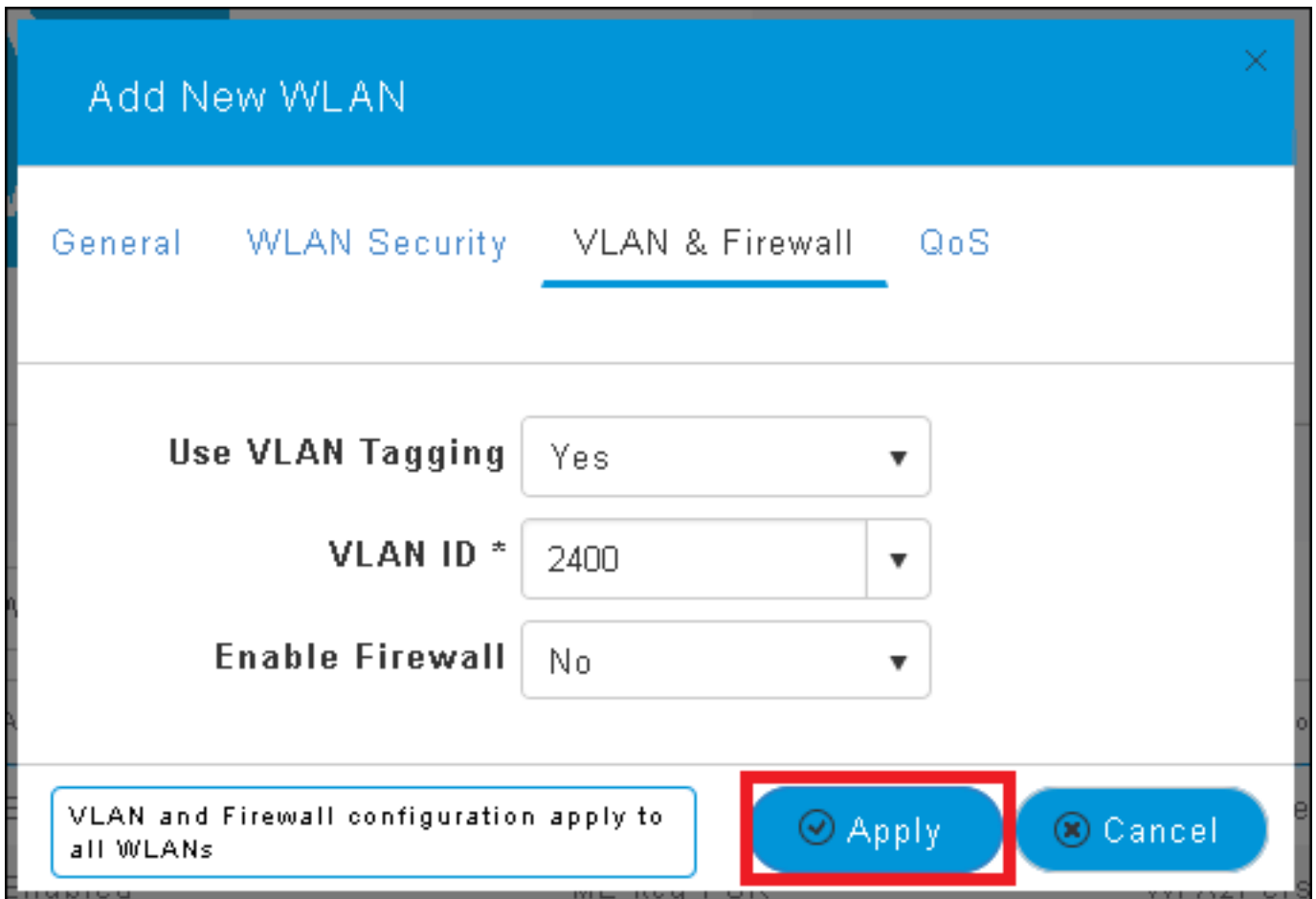
The screenshot shows a configuration window titled "Add New WLAN" with a close button (X) in the top right corner. Below the title bar are four tabs: "General", "WLAN Security", "VLAN & Firewall" (which is selected and underlined), and "QoS". The "VLAN & Firewall" tab contains three configuration items, each with a dropdown menu:

- Use VLAN Tagging**: Set to "Yes".
- VLAN ID ***: Set to "2400".
- Enable Firewall**: Set to "No".

At the bottom of the window, there is a blue box containing the text: "VLAN and Firewall configuration apply to all WLANs". To the right of this box are two buttons: "Apply" (with a checkmark icon) and "Cancel" (with an X icon).

注意：如果使用VLAN标记，请确保接入点所连接的交换机端口配置为中继端口，而AP VLAN配置为本征端口。

步骤5.单击“应用”完成配置。



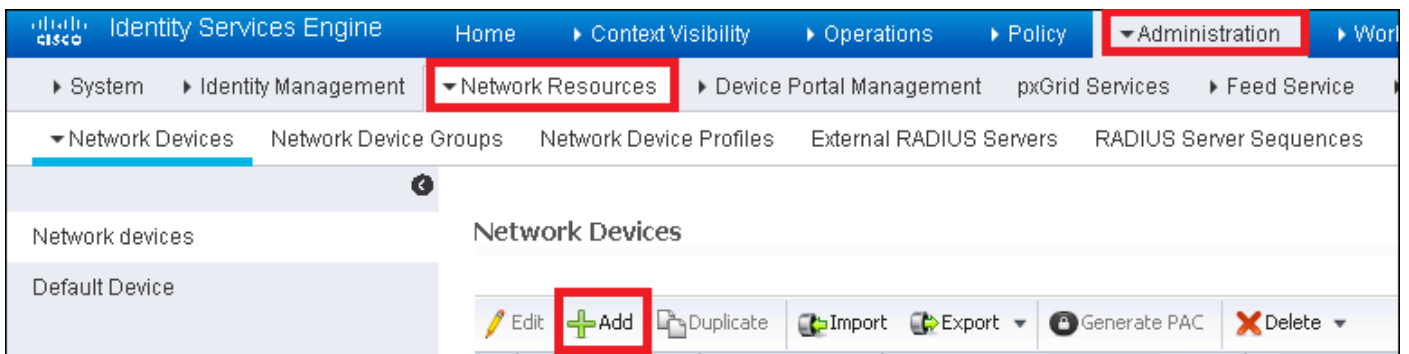
步骤6. 可选，将WLAN配置为接受VLAN覆盖。

在WLAN上启用AAA覆盖并添加所需的VLAN。为此，您需要打开到ME管理界面的CLI会话并发出以下命令：

```
>config wlan disable <wlan-id>  
>config wlan aaa-override enable <wlan-id>  
>config wlan enable <wlan-id>  
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

在ISE上声明ME

步骤1. 打开ISE控制台并导航至Administration > Network Resources > Network Devices > Add。



步骤2. 输入信息。

或者，可以根据设备类型、位置或WLC指定型号名称、软件版本、说明和分配网络设备组。

a.b.c.d对应于ME的IP地址。

Network Devices List > **New Network Device**

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

WLCs

RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

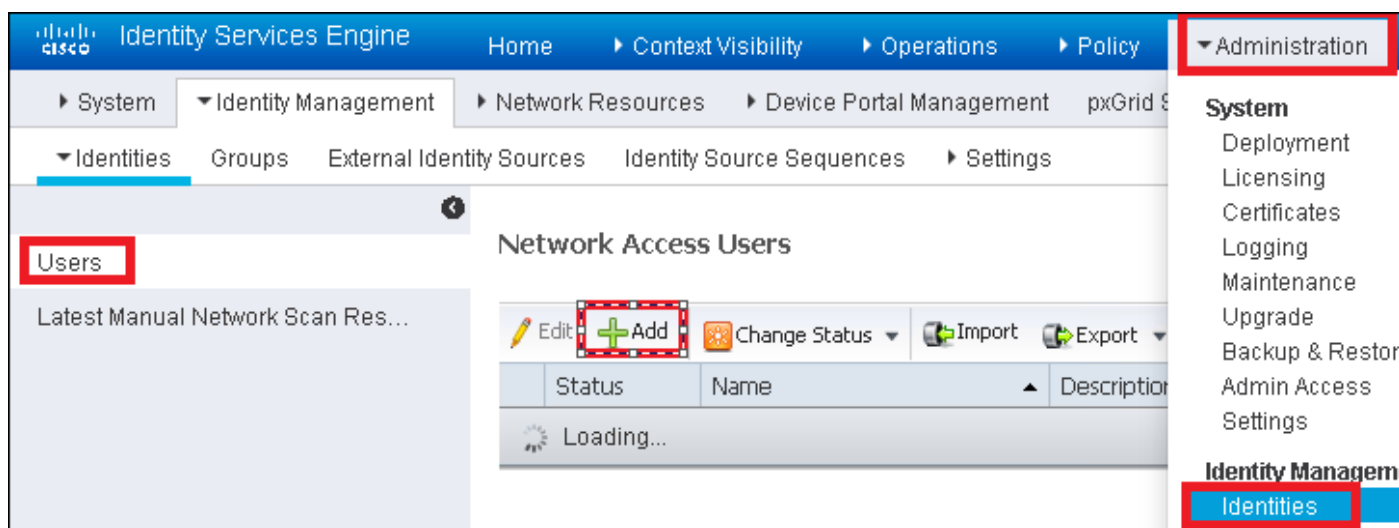
CoA Port

有关网络设备组的详细信息，请查看此链接：

[ISE — 网络设备组](#)

在ISE上创建新用户

步骤1. 导航至 **管理>身份管理>身份>用户>添加**。



步骤2. 输入信息。

在本示例中，此用户属于名为ALL_ACCOUNTS的组，但可以根据需要对其进行调整。

▼ Network Access User

* Name

Status Enabled ▼

Email

▼ Passwords

Password Type: ▼

Password

Re-Enter Passw

* Login Password

Enable Password

▼ User Information

First Name

Last Name

▼ Account Options

Description

Change password on next login

▼ Account Disable Policy

Disable account if date exceeds

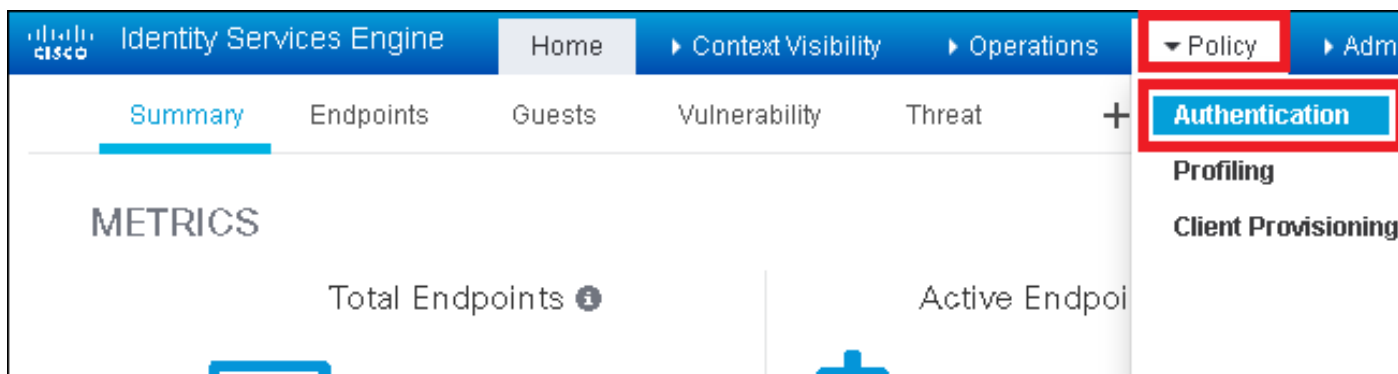
▼ User Groups

+

创建身份验证规则

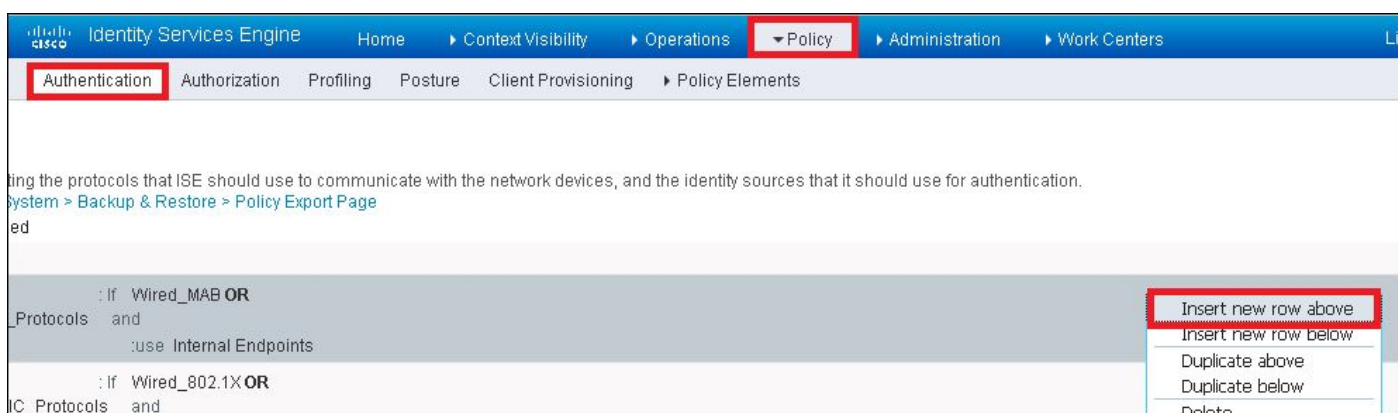
身份验证规则用于验证用户的凭证是否正确（验证用户是否真正是其所说的用户），并限制允许其使用的身份验证方法。

步骤1: 导航 到策略>身份验证。



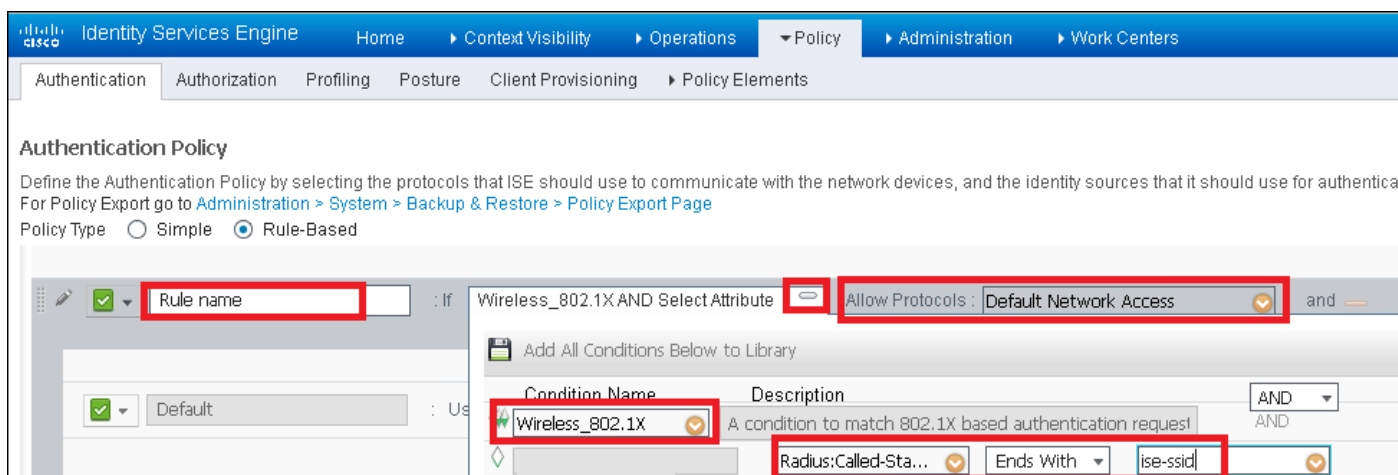
步骤2.插入新的身份验证规则。

要执行此操作，请导航至Policy > Authentication > Insert new row above/below。

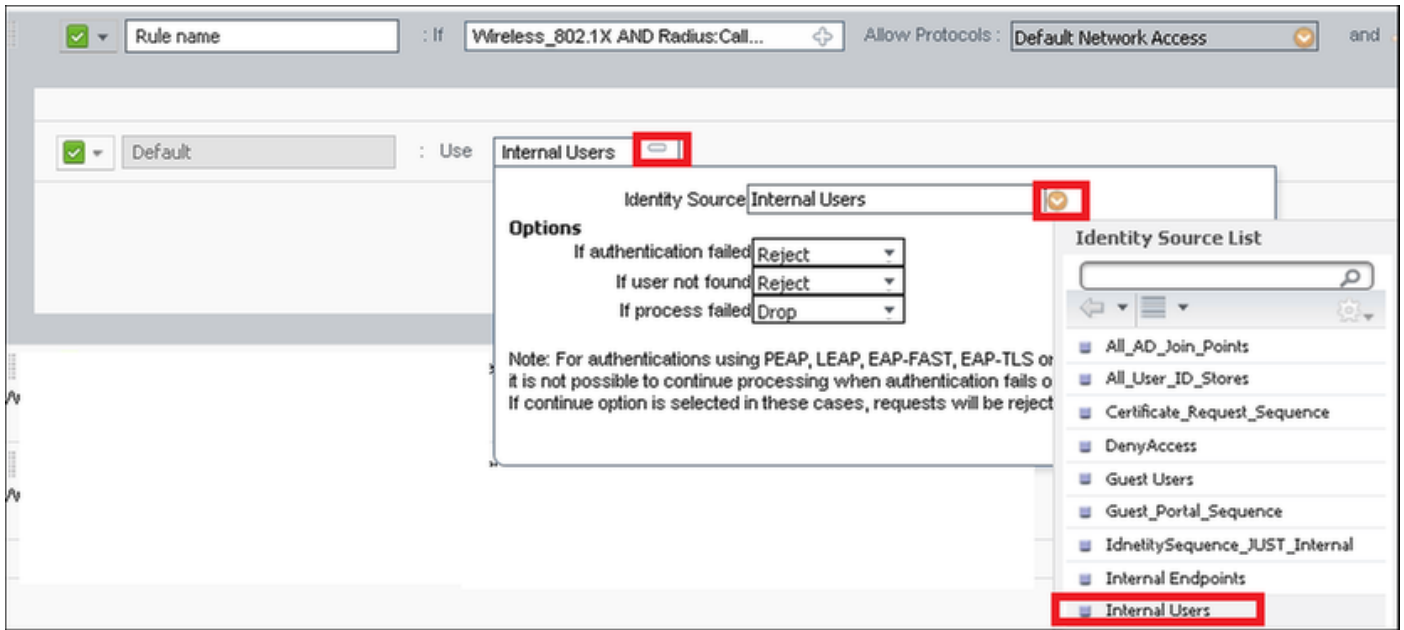


步骤3.输入所需信息

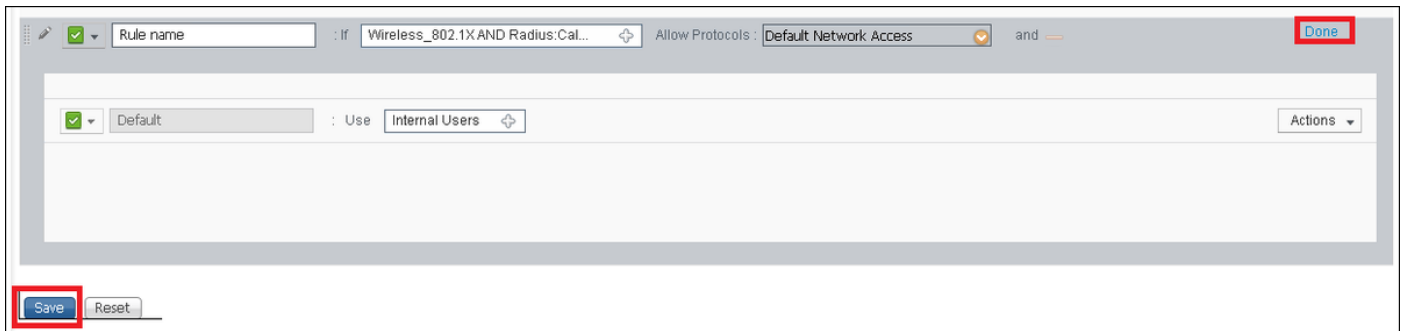
此身份验证规则示例允许在默认网络访问列表下列出的所有协议，这适用于无线802.1x客户端的身份验证请求和被叫站ID，并以ise-ssid结尾。



此外，为匹配此身份验证规则的客户端选择身份源(在本例中为内部用户)



完成后，单击“完成并保存”。



有关允许协议策略的详细信息，请参阅以下链接：

[允许的协议服务](#)

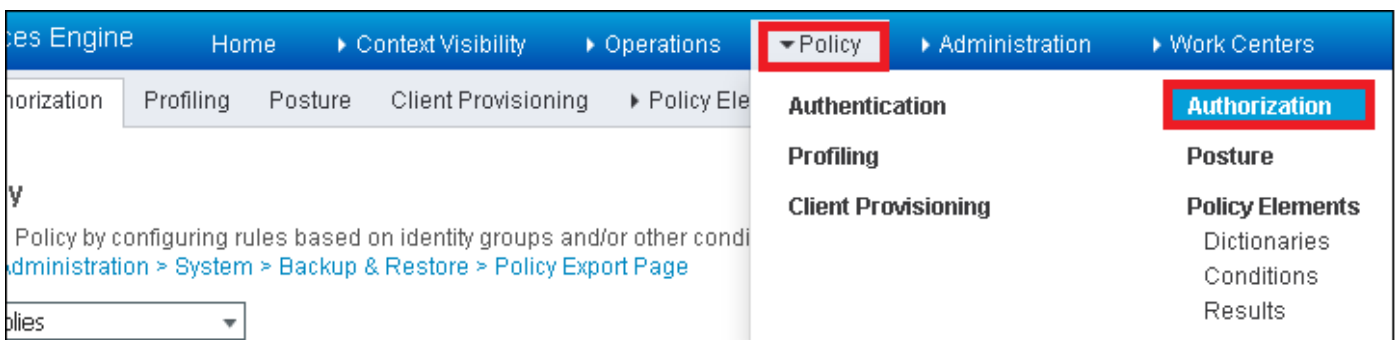
有关身份源的详细信息，请参阅以下链接：

[创建用户身份组](#)

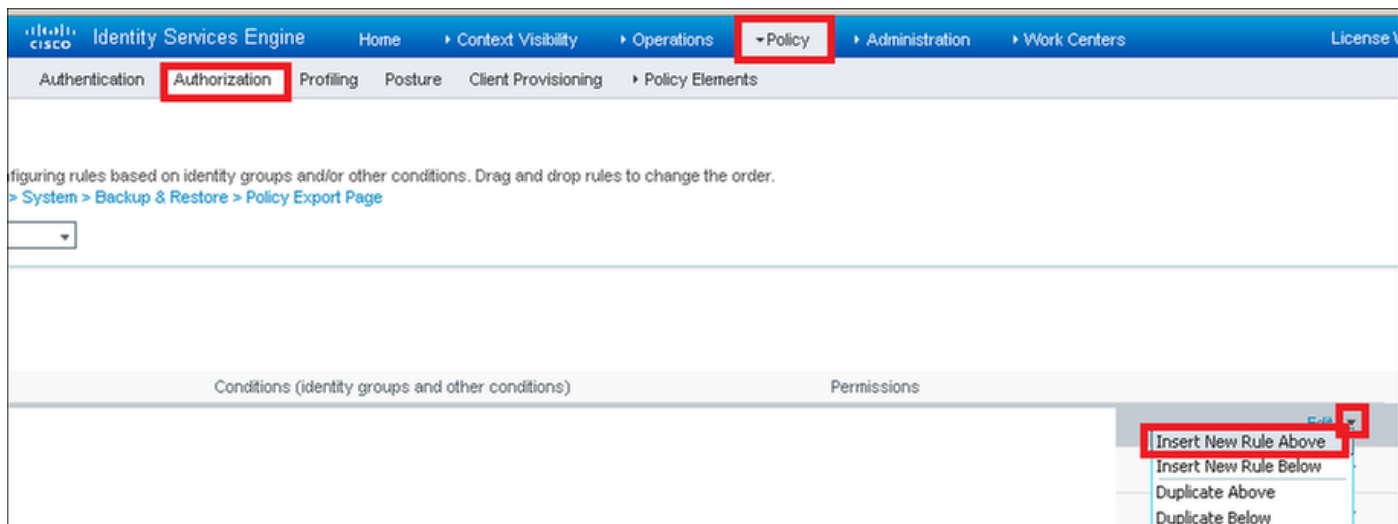
创建授权规则

授权规则是确定是否允许客户端加入网络的负责规则

步骤1.导航至Policy > Authorization。

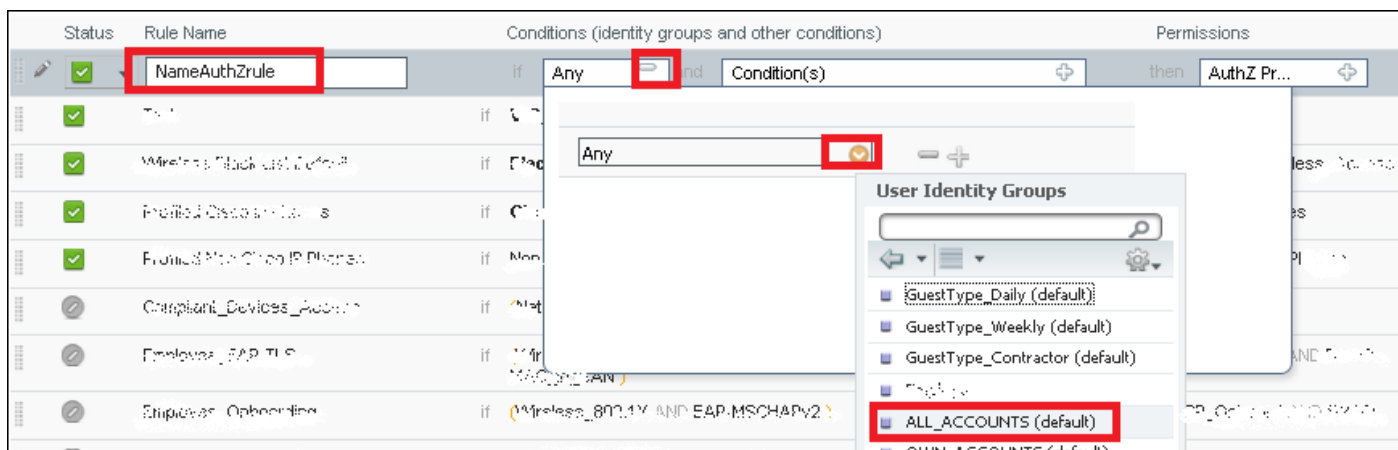


步骤2.插入新规则。导航至Policy > Authorization > Insert New Rule Above/Below。

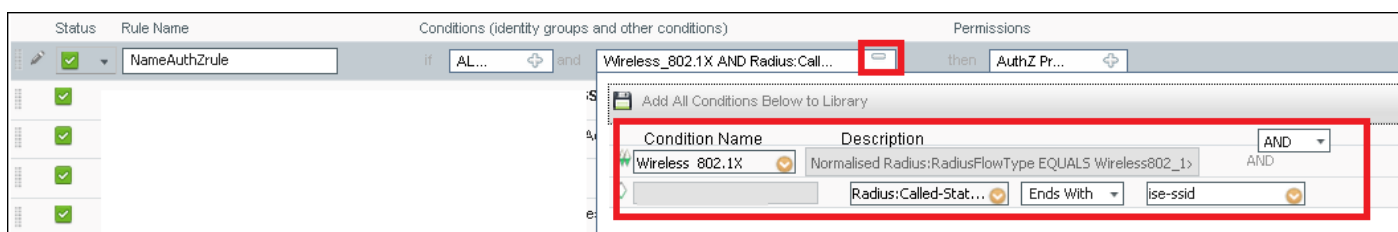


步骤3.输入信息。

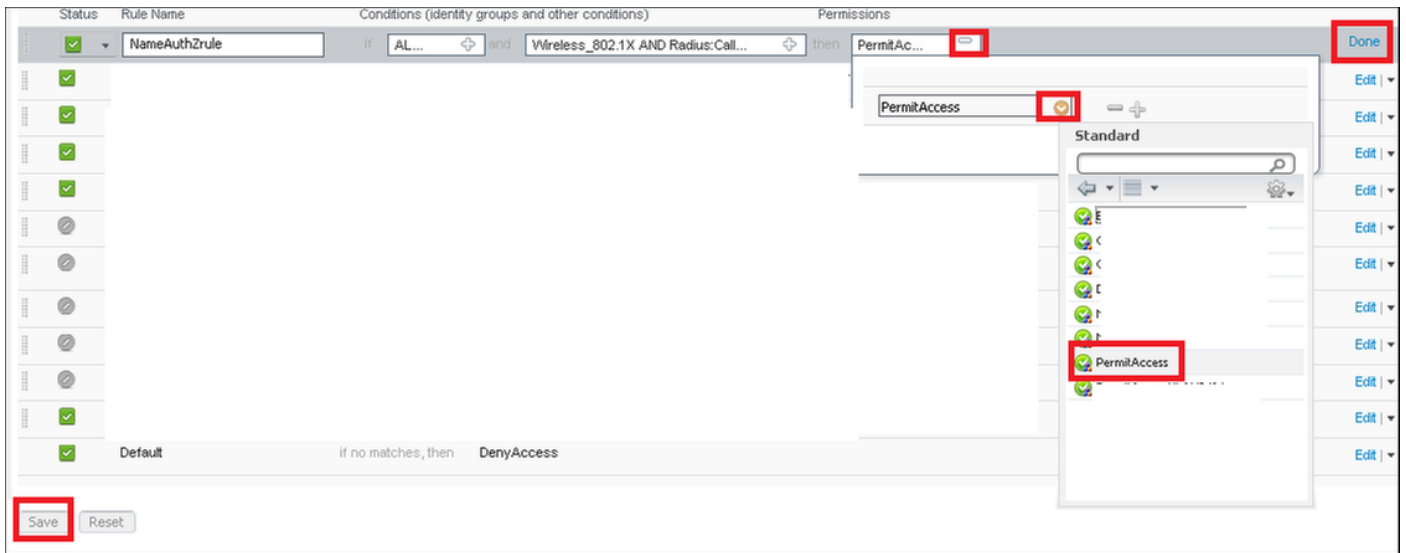
首先为规则和存储用户的身份组选择一个名称。在本示例中，用户存储在组ALL_ACCOUNTS中。



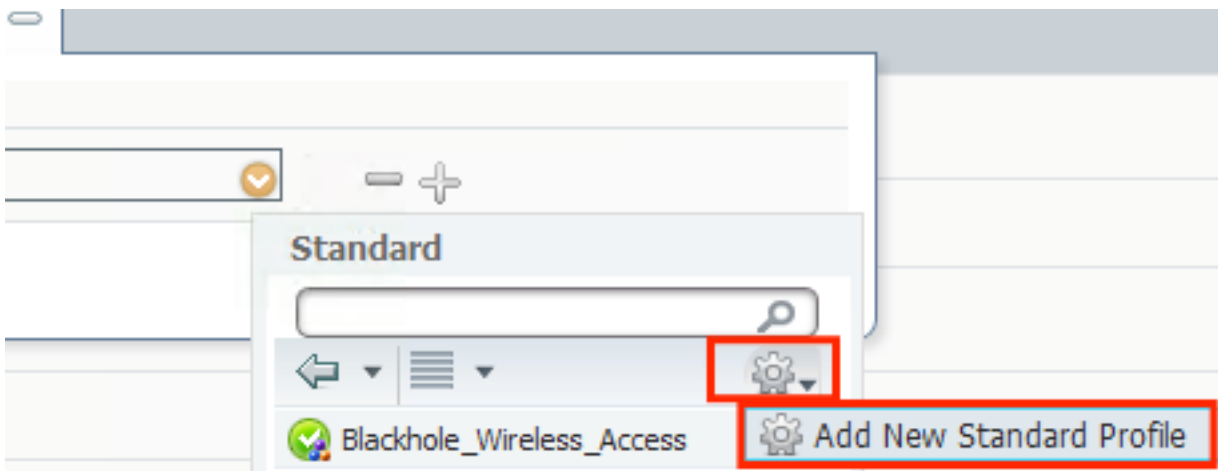
之后，选择使授权过程符合此规则的其他条件。在本示例中，如果授权进程使用802.1x无线，并且称为站ID以ise-ssid结尾，则授权进程会符合此规则。



最后，选择允许客户端加入网络的授权配置文件，单击完成并保存。



或者，创建新的授权配置文件，将无线客户端分配到不同的VLAN:



输入相关信息:

Add New Standard Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DAACL Name

ACL (Filter-ID)

VLAN Tag ID IDName

Voice Domain Permission

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:vlan-id
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

终端设备配置

配置Windows 10笔记本电脑，使其使用PEAP/MS-CHAPv2(质询握手身份验证协议第2版的Microsoft版本)连接到具有802.1x身份验证的SSID。

在此配置示例中，ISE使用其自签名证书执行身份验证。

要在Windows计算机上创建WLAN配置文件，有两个选项：

1. 在计算机上安装自签名证书以验证和信任ISE服务器以完成身份验证
2. 绕过RADIUS服务器的验证并信任用于执行身份验证的任何RADIUS服务器（不推荐，因为它可能会成为安全问题）

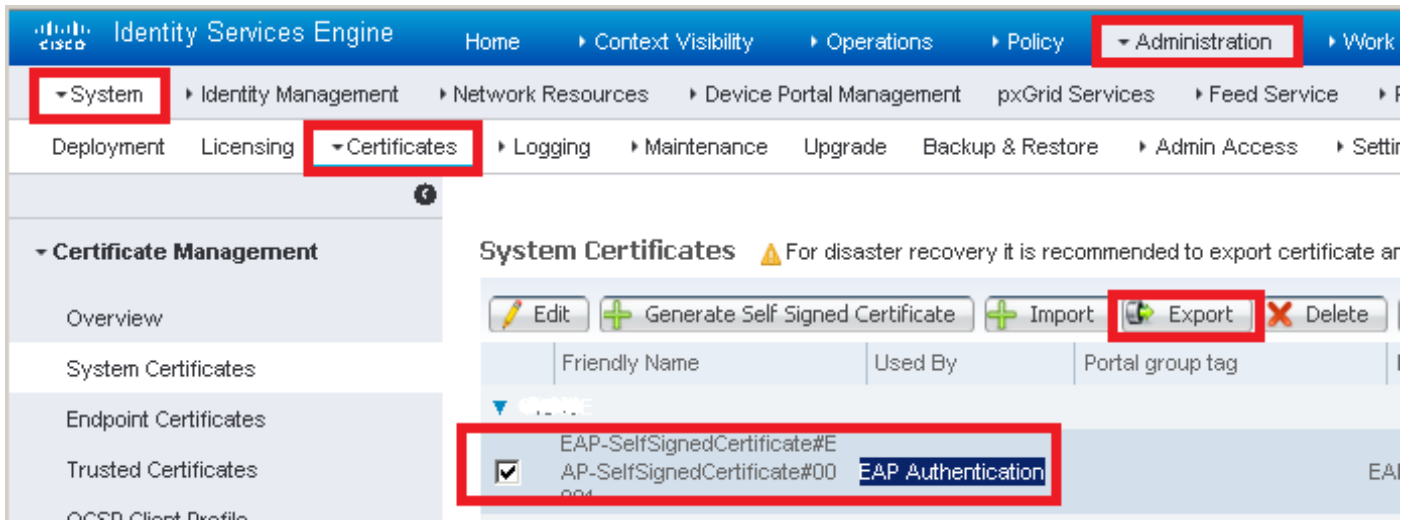
这些选项的配置在“终端设备配置 [— 创建WLAN配置文件 — 步骤7](#)”中进行了说明。

终端设备配置 — 安装ISE自签名证书

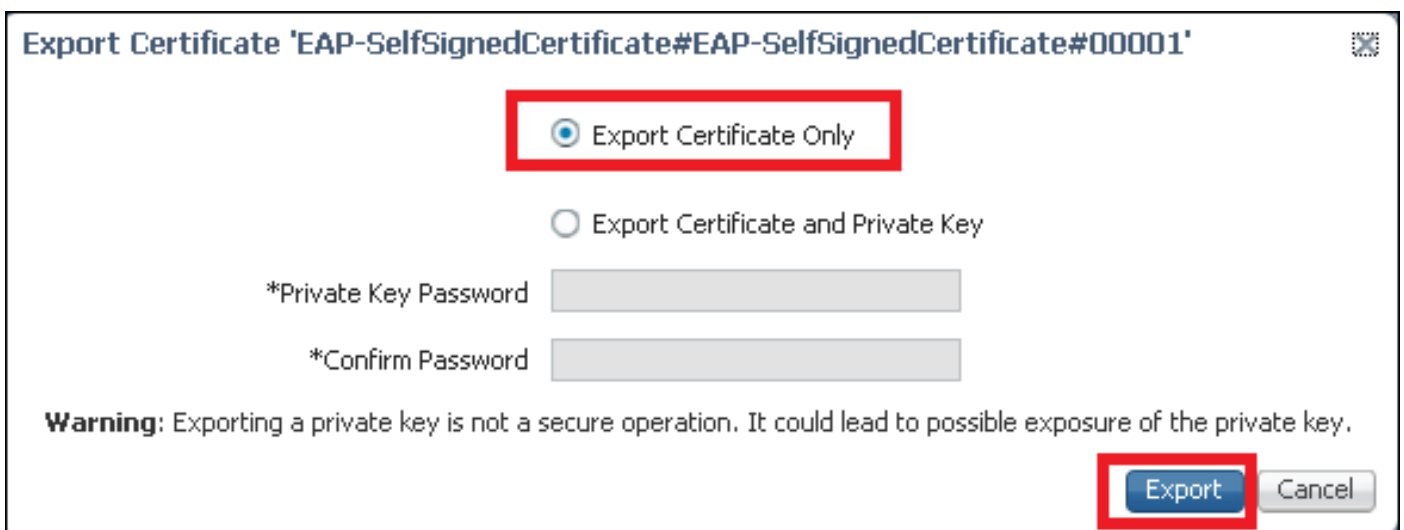
步骤1.从ISE导出自签名证书。

登录到ISE并导航至Administration > System > Certificates > System Certificates。

然后选择用于EAP身份验证的证书，然后单击导出。



将证书保存到所需位置。此证书安装在Windows计算机上。

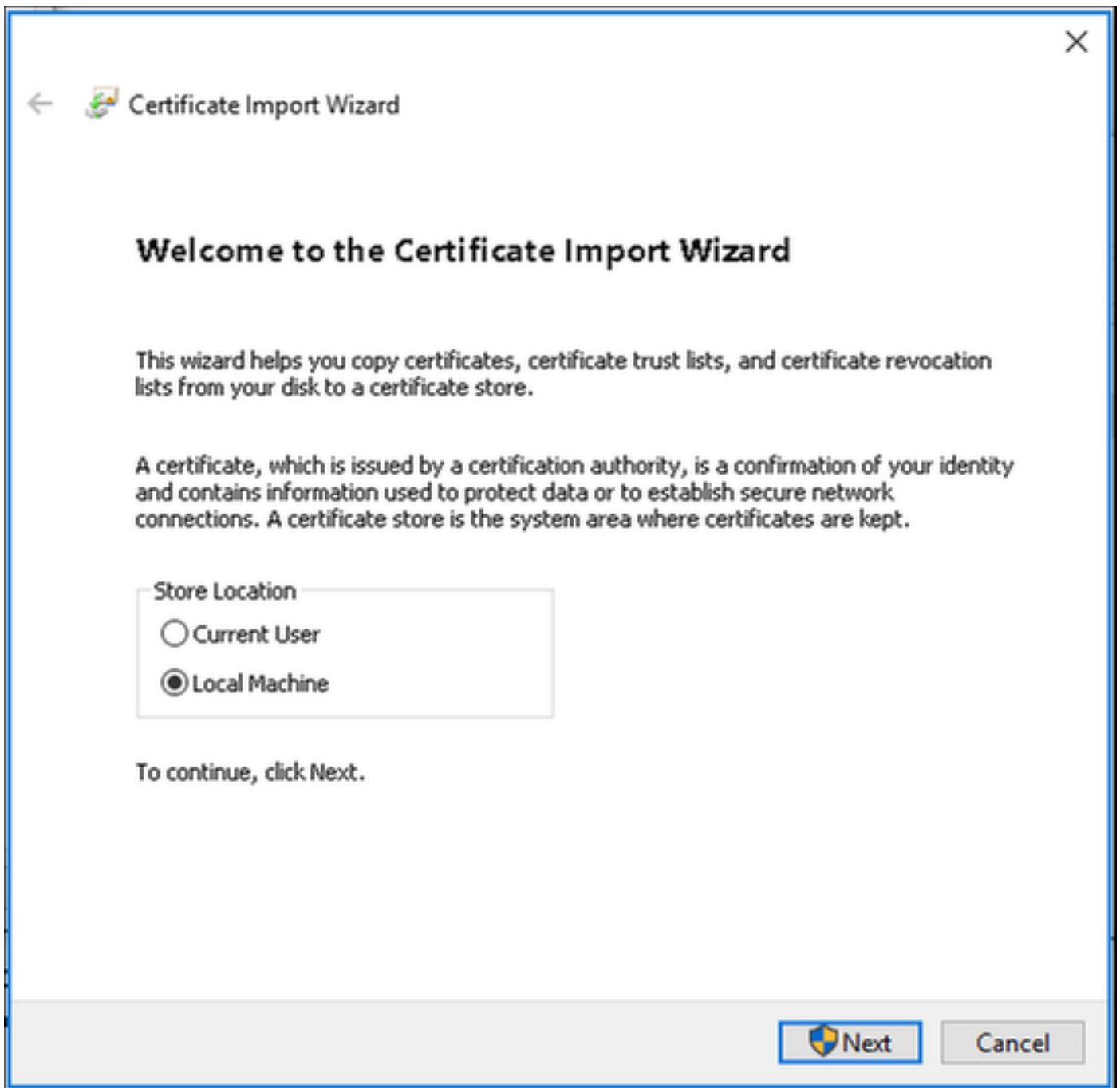


步骤2.在Windows计算机中安装证书。

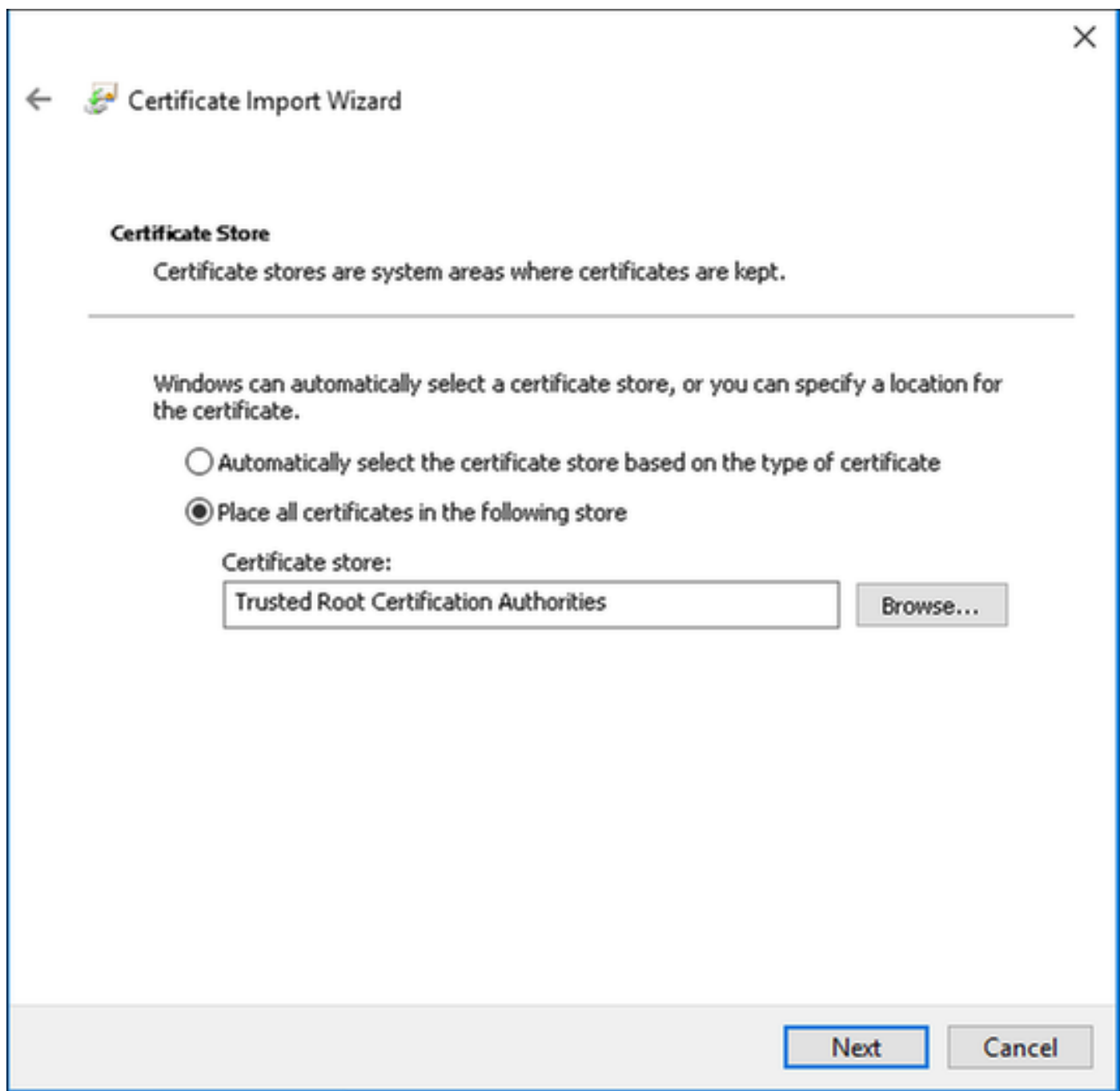
将之前导出的证书复制到Windows计算机，将文件的扩展名从.pem更改为.crt，然后双击该文件并选择“安装证书……”。



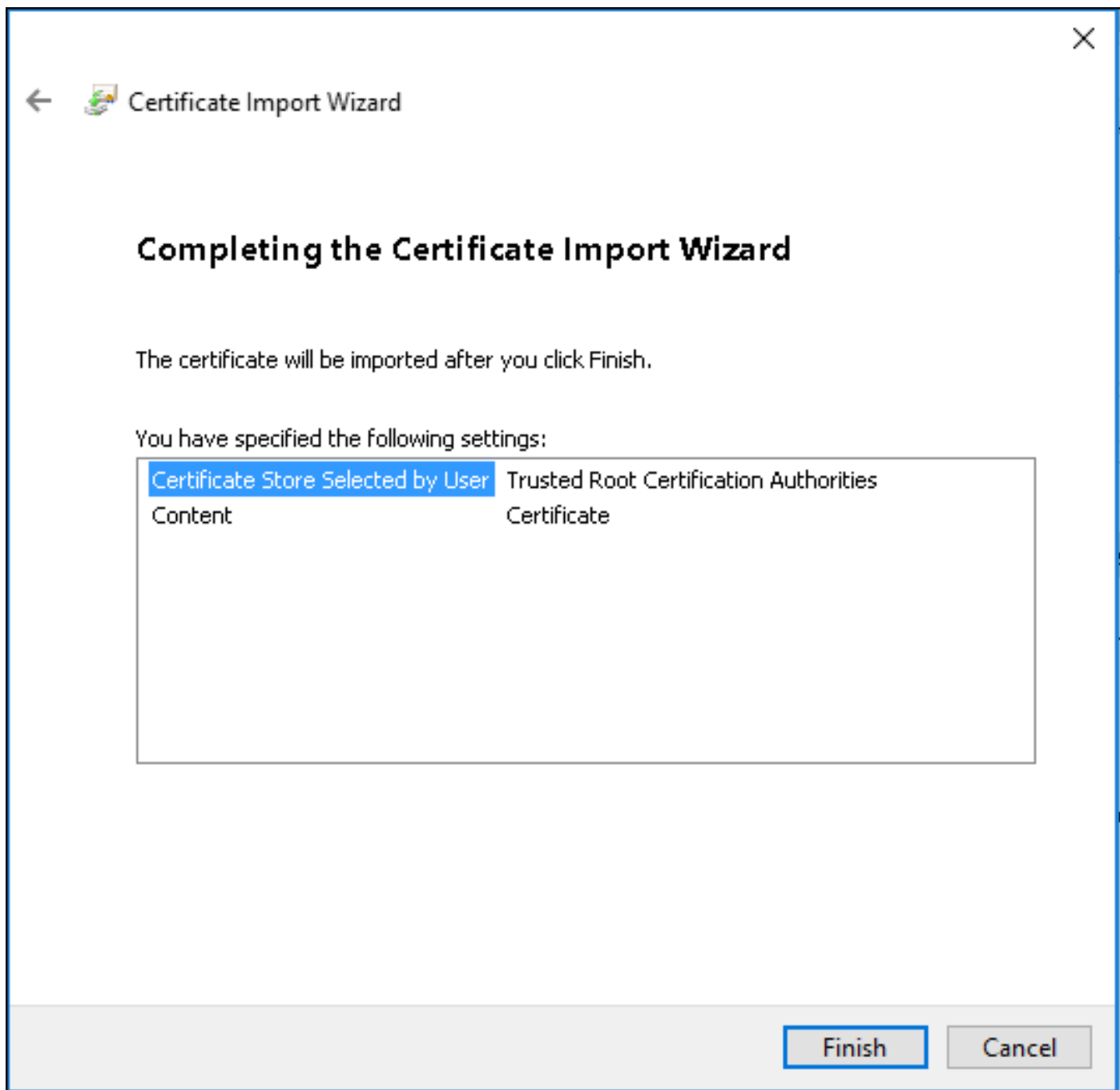
选择在本地计算机中安装它，然后单击下一步。



选择Place all certificates in the following store，然后浏览并选择Trusted Root Certification Authorities(受信任的根证书颁发机构)。然后单击“下一步”。



然后单击 Finish。



最后单击“**Yes (是)**”确认证书的安装。

Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): 011A193D 7007713D 0204E3D0 4759215D
4294213C

Warning:

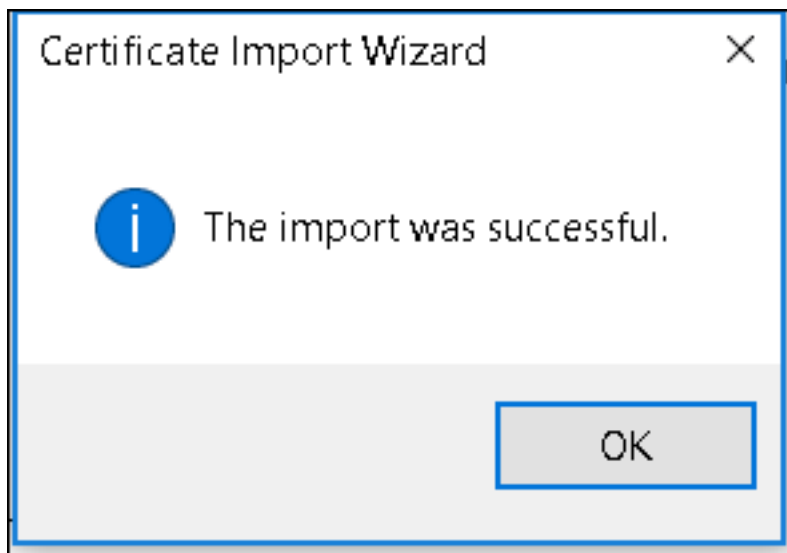
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes

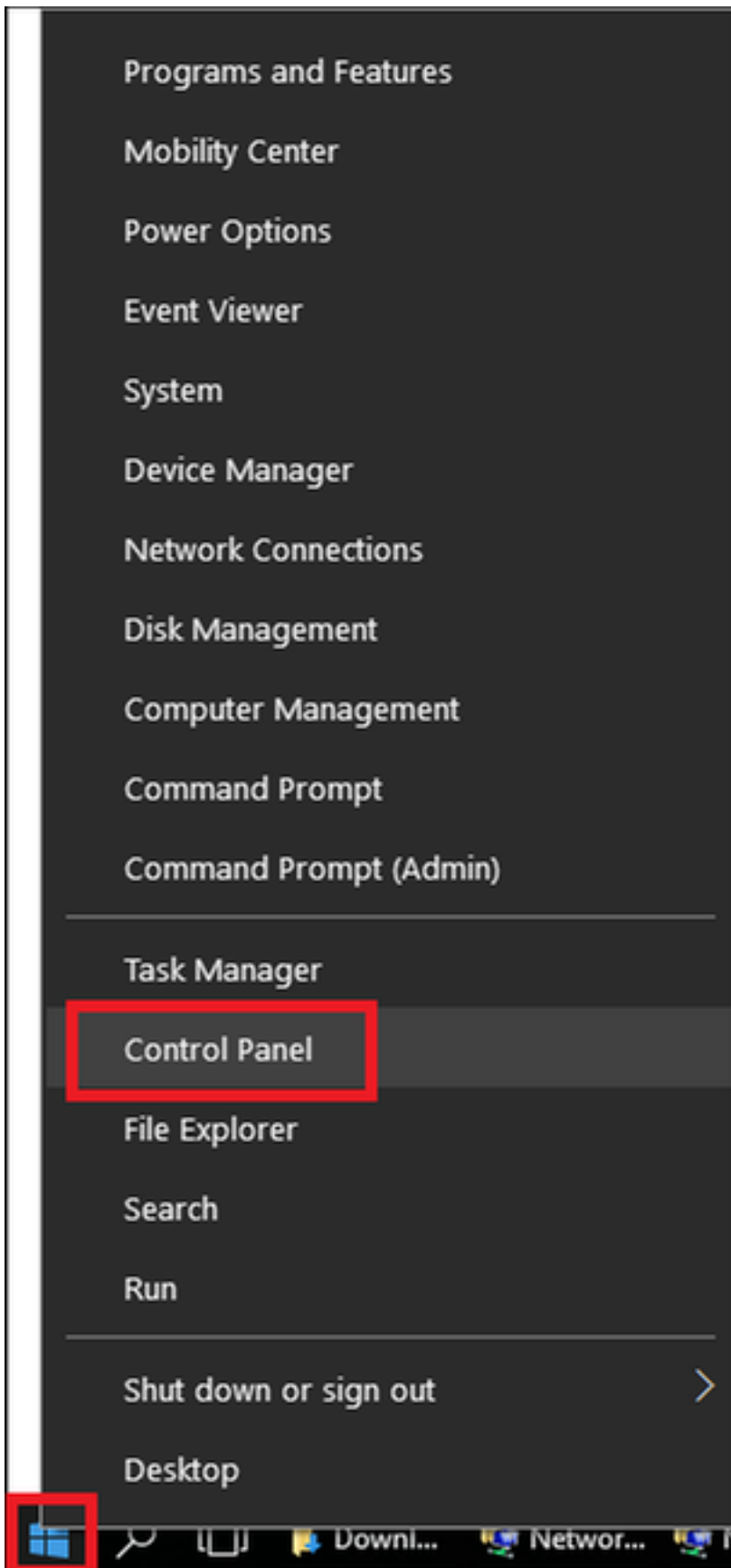
No

最后单击OK。

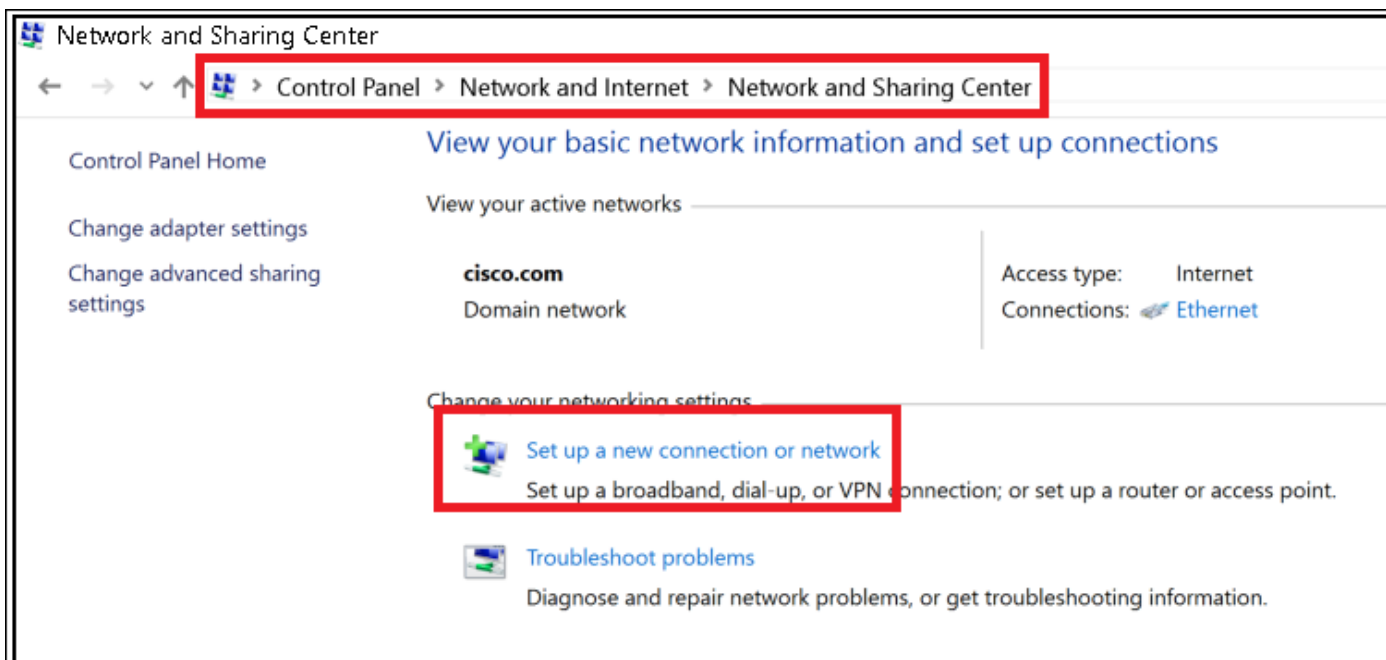


终端设备配置 — 创建WLAN配置文件

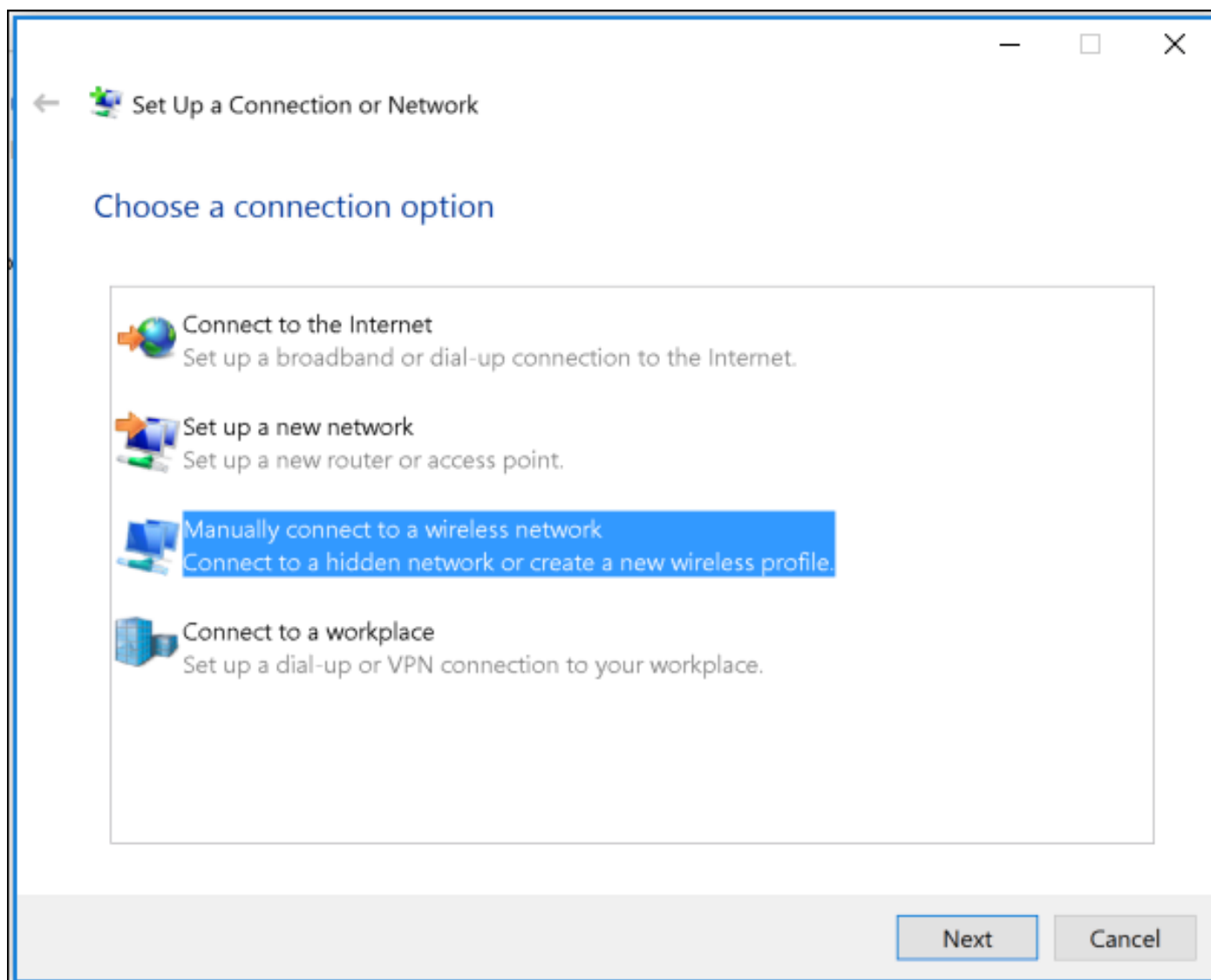
步骤1. 右键单击“开始”图标并选择“控制面板”。



步骤2.导航到Network and Internet(网络和Internet)，然后导航到Network and Sharing Center(网络和共享中心),然后单击Set up a new connection or network (设置新连接或网络)。



步骤3.选择“手动连接到无线网络”，然后单击“下一步”。



步骤4.输入名称为SSID的信息，并输入安全类型WPA2-Enterprise，然后单击Next。

← Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

Security Key: Hide characters

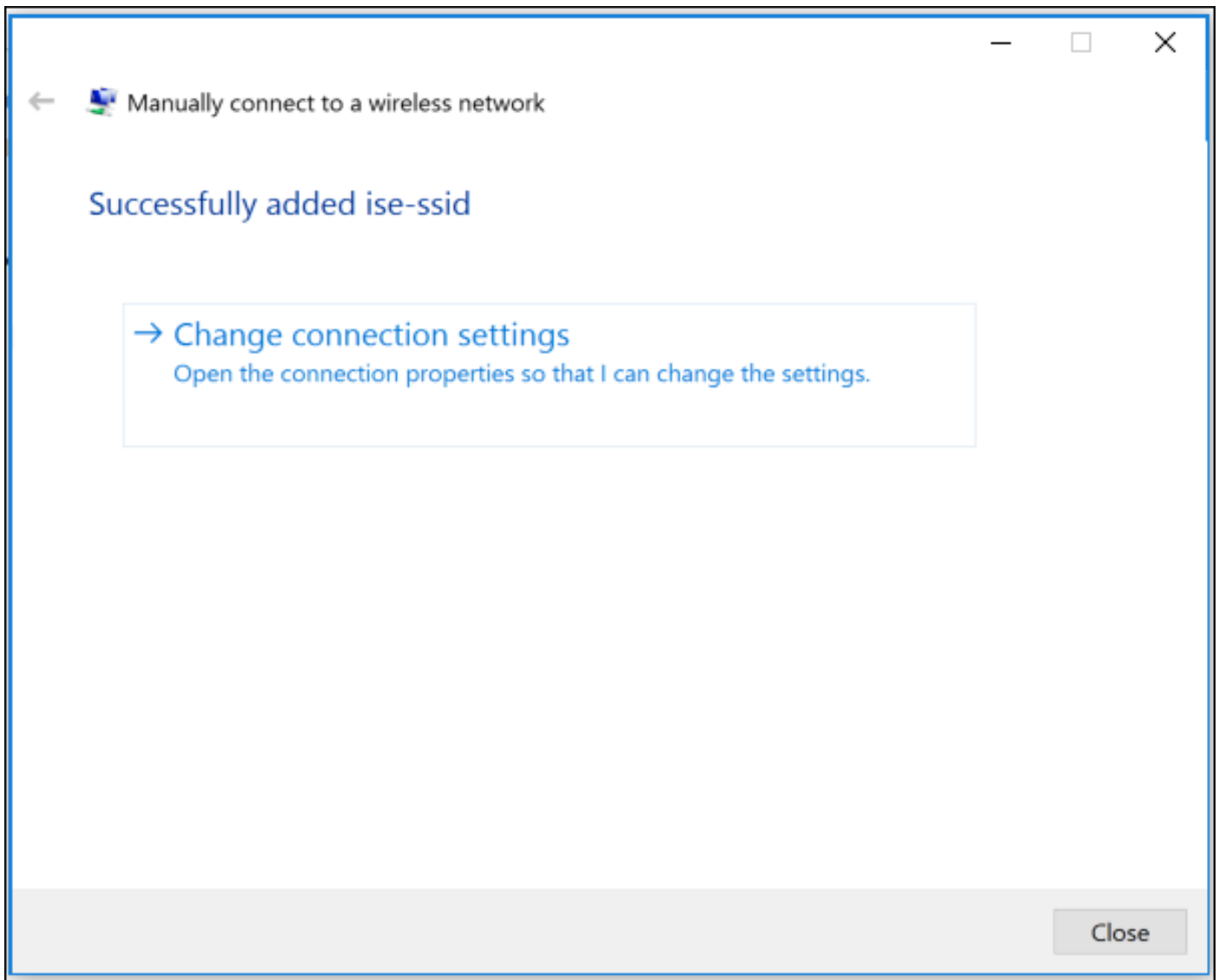
Start this connection automatically

Connect even if the network is not broadcasting

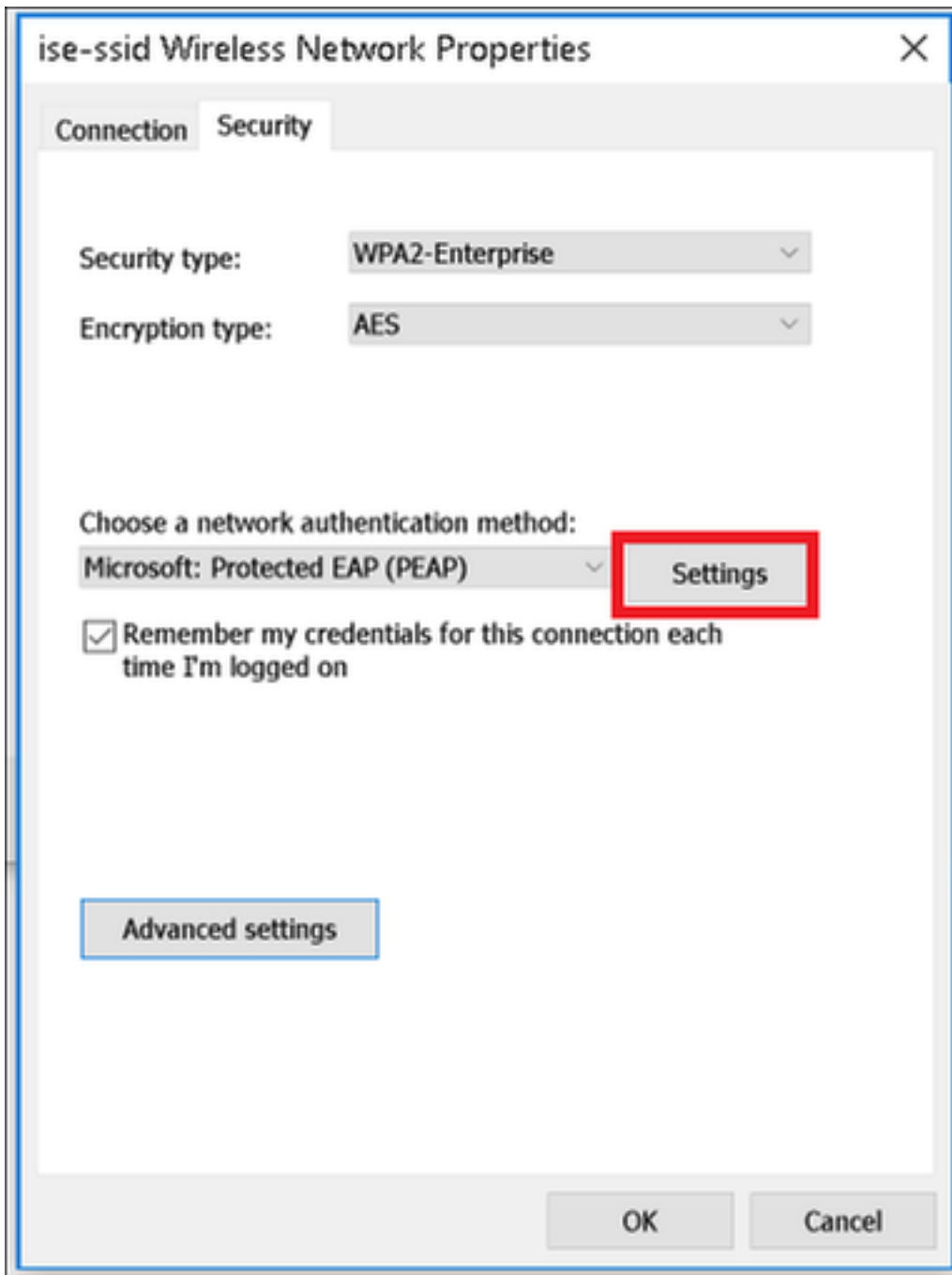
Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

步骤5.选择“更改连接设置”以自定义WLAN配置文件的配置。



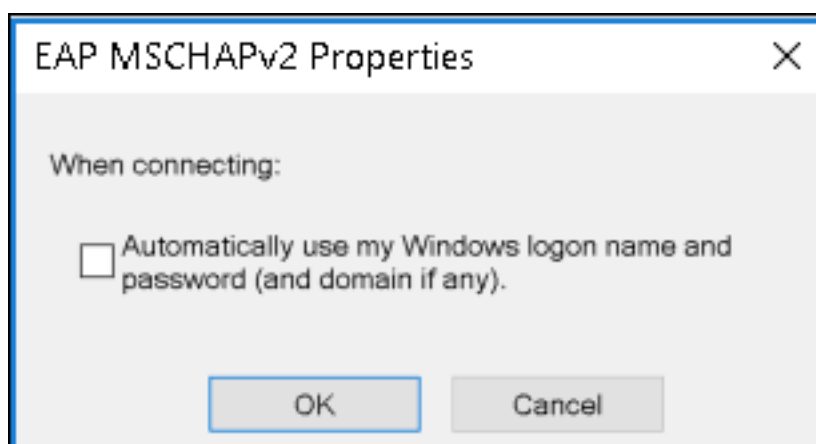
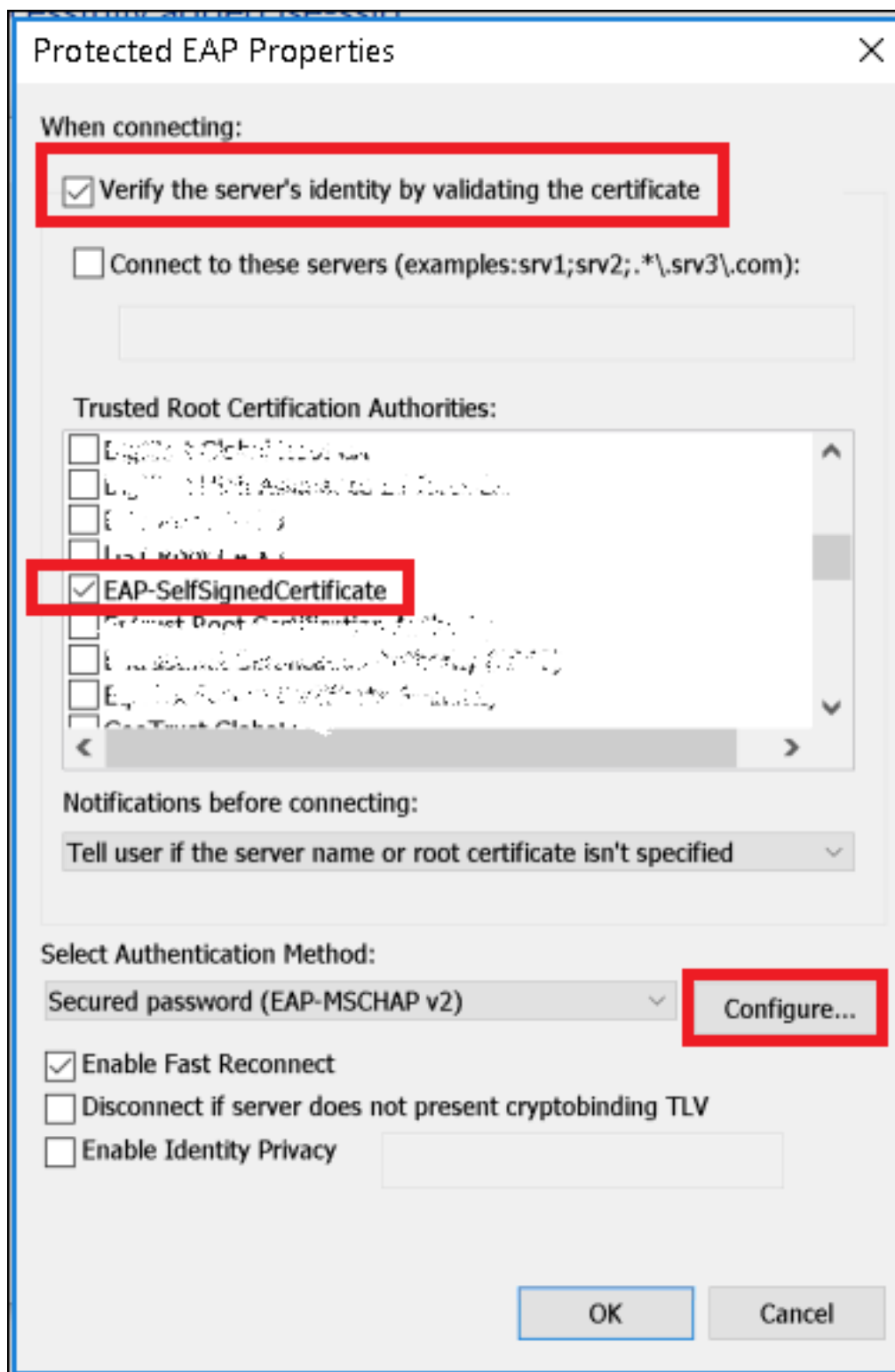
步骤6. 导航至“安全”选项卡并单击“设置”。



步骤7.选择是否验证RADIUS服务器。

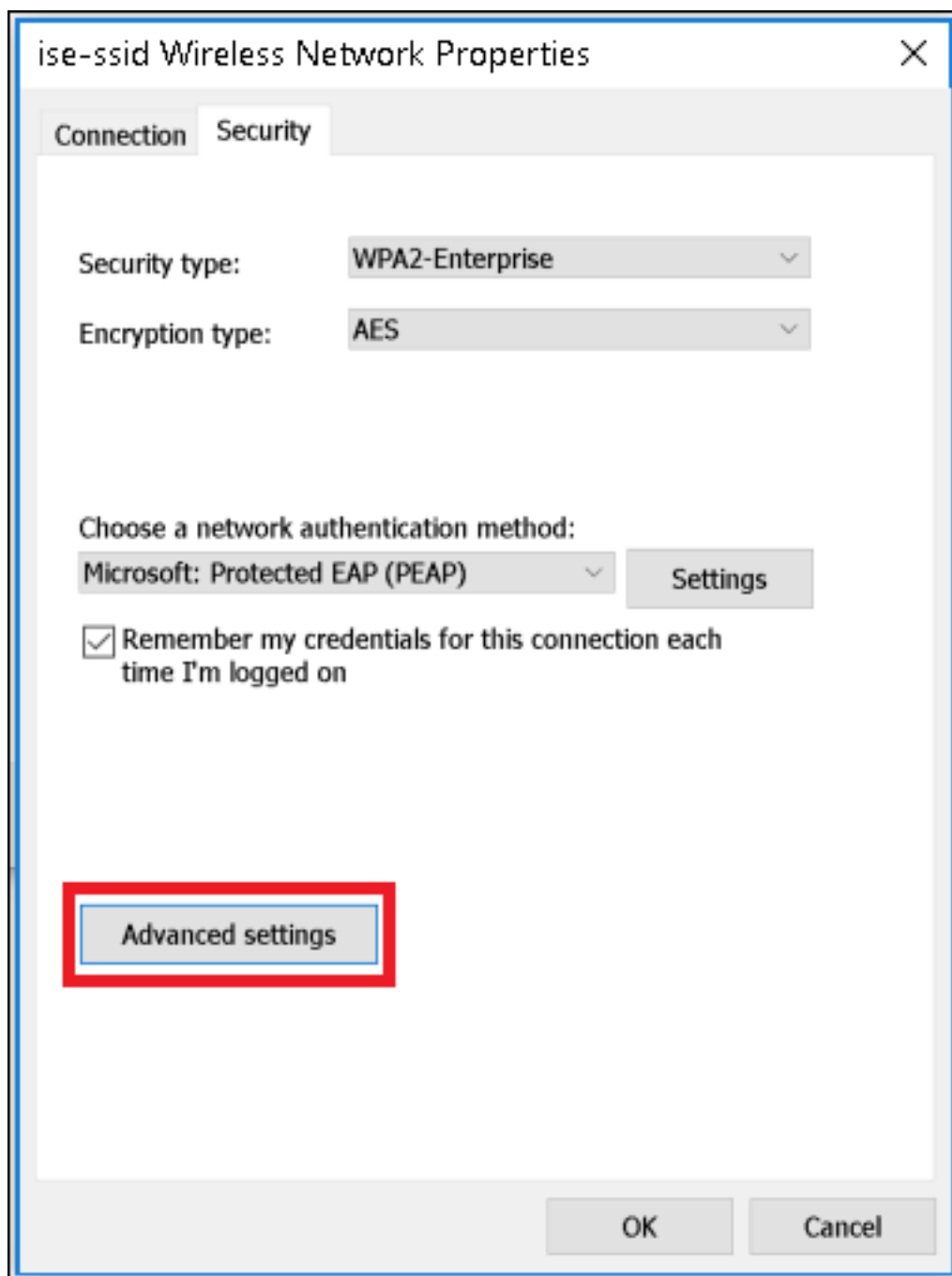
如果是，请启用Verify the server identity by validating the certificate and from Trusted Root Certification Authorities: list select the self-signed certificate of ISE。

之后，选择配置并禁用自动使用我的Windows登录名和密码.....，然后单击确定



步骤8.配置用户凭证

返回安全选项卡后，选择**高级设置**，将身份验证模式指定为**用户身份验证**并保存在ISE上配置的凭证以对用户进行身份验证。



Advanced settings



802.1X settings

802.11 settings

Specify authentication mode:

User authentication

Save credentials

Delete credentials for all users

Enable single sign on for this network

Perform immediately before user logon

Perform immediately after user logon

Maximum delay (seconds):

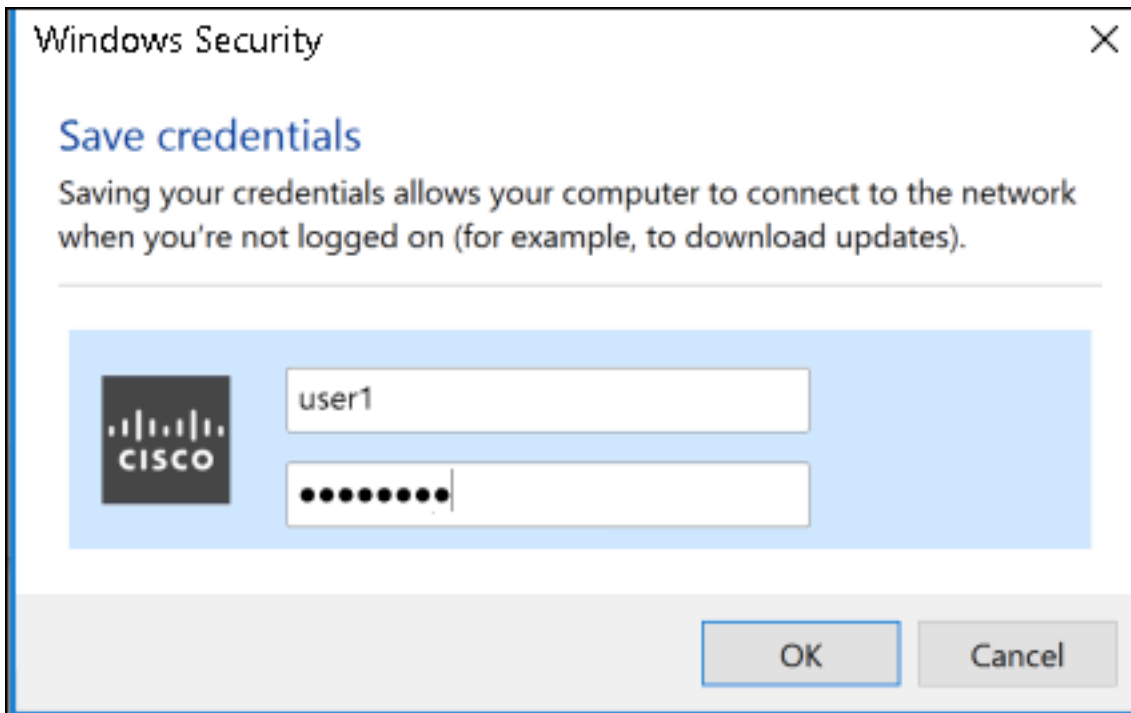
10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

OK

Cancel



验证

身份验证流可以从WLC或ISE角度进行验证。

ME上的身份验证过程

运行此命令以监控特定用户的身份验证过程：

```
> debug client <mac-add-client>
```

身份验证成功的示例（省略部分输出）：

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on
BSSID 38:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state START (0)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state AUTHCHECK (2)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on
```


AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48)

*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0

*apfMsConnTask_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3**

*apfMsConnTask_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1**

*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x_reauth_sm.c:47

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3 is disabled - applying Global eap timers and retries

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Connecting state

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: **08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1)**

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45**

*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45**

.

.

.

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45**

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253**

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cache at index 0 for station 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: New PMKID: (16)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility handoff

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can take care of same.

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: M1 - Key Data: (22)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: **08:74:02:77:13:45 Starting key exchange to mobile**

08:74:02:77:13:45, data packets will be dropped

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile

08:74:02:77:13:45

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Authenticated state

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-key in PTK_START state (message 2) from mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!!

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!!!!!!

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0.....

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45

state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Received EAPOL-key in

PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 255.255.255.224

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name:

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7)

pemAdvanceState2 6623, Adding TMP rule

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule

type = Airespace AP - Learn IP address

```

on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role
update request from Unassociated to Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
6261, Adding TMP rule
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast
Path rule
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug:
regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller
apf_ms.c:3593)
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state
to RUN (20) last state DHCP_REQD (7)

```

要方便地读取调试客户端输出，请使用无线调试分析器工具：

[无线调试分析器](#)

ISE上的身份验证过程

导航至操作> RADIUS >实时日志，以查看分配给用户的身份验证策略、授权策略和授权配置文件。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The 'Operations' menu is expanded, and 'RADIUS' is selected. Under 'RADIUS', 'Live Logs' is highlighted. The main content area displays several metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), and Client Stopped Responding (4). Below these metrics is a table of log entries. The table has columns for Time, Status, Details, Idle Time, Endpoint ID, Endpoint Name, Authentication Policy, Authorization Policy, and Authorization Profiles. A red box highlights the 'Details' column for a log entry with ID 1, showing a user named 'user1' with endpoint ID '08:74:02:77:13:45' and endpoint name 'Apple-Device'. The authentication policy is 'Default', the authorization policy is 'NameAuthZrule', and the authorization profile is 'PermitAccess'.

Time	Sta...	Details	Idle...	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles
No...	1		user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccess

有关详细信息，请单击Details查看更详细的身份验证过程。