

使用PEAP、ISE 2.1和WLC 8.3配置802.1X身份验证

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](#)

[在WLC上声明RADIUS服务器](#)

[创建 SSID](#)

[在ISE上声明WLC](#)

[在 ISE 上创建新用户](#)

[创建身份验证规则](#)

[创建授权配置文件](#)

[创建授权规则](#)

[终端设备配置](#)

[终端设备配置 — 安装ISE自签名证书](#)

[终端设备配置 — 创建WLAN配置文件](#)

[验证](#)

[WLC上的身份验证过程](#)

[ISE上的身份验证过程](#)

[故障排除](#)

简介

本文档介绍如何设置具有802.1x安全性和虚拟局域网(VLAN)覆盖的无线局域网(WLAN)。

先决条件

要求

Cisco 建议您了解以下主题：

- 802.1x
- 受保护的扩展身份验证协议 (PEAP)
- 证书颁发机构(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：

- WLC v8.3.102.0
- 身份服务引擎(ISE)v2.1
- Windows 10笔记本电脑

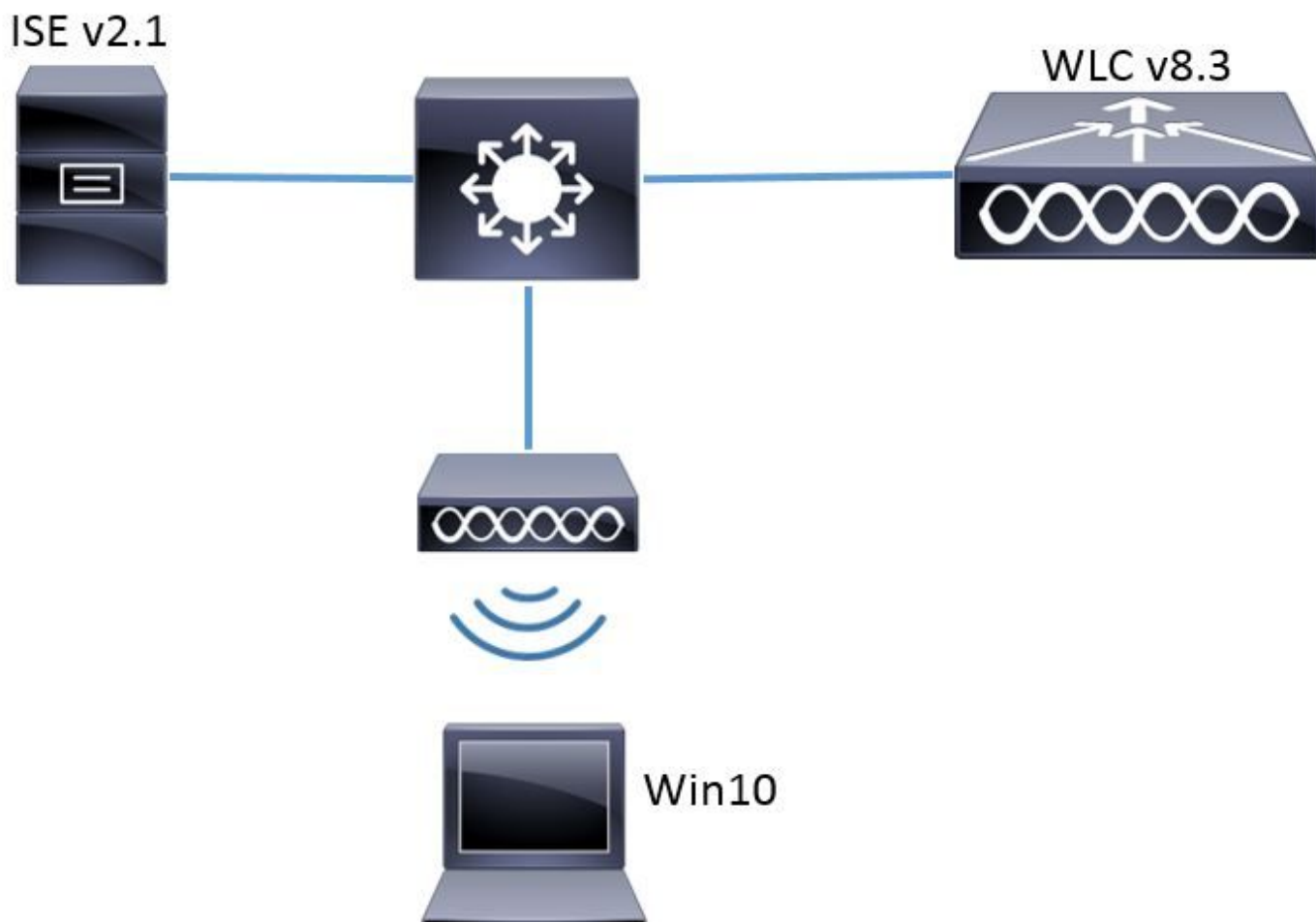
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

设置具有802.1x安全和VLAN的WLAN时，可以使用受保护的可扩展身份验证协议作为可扩展身份验证协议(EAP)进行覆盖。

配置

网络图



配置

一般步骤如下：

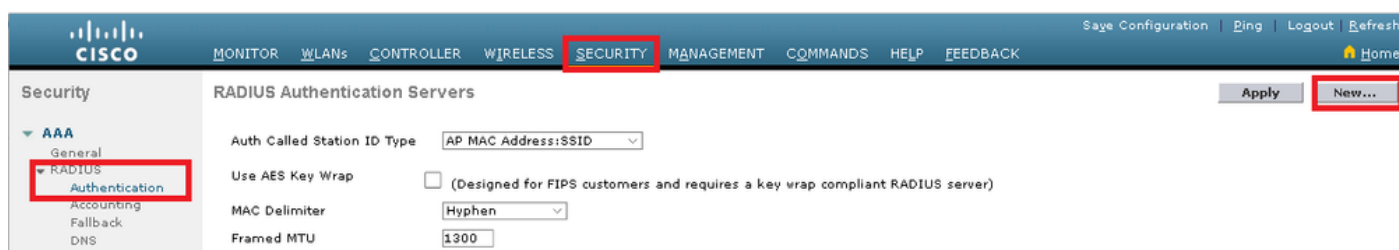
1. 在WLC上声明RADIUS服务器，反之亦然，以允许相互通信。
2. 在WLC中创建服务集标识符(SSID)。
3. 在ISE上创建身份验证规则。
4. 在ISE上创建授权配置文件。
5. 在ISE上创建授权规则。
6. 配置终端。

在WLC上声明RADIUS服务器

为了允许RADIUS服务器和WLC之间的通信，您需要在WLC上注册RADIUS服务器，反之亦然。

GUI:

步骤1:打开WLC的GUI，导航到SECURITY > RADIUS > Authentication > New，如图所示。



第二步：输入RADIUS服务器信息，如图所示。

RADIUS Authentication Servers > New

Server Index (Priority)

Server IP Address(Ipv4/Ipv6)

Shared Secret Format

Shared Secret

Confirm Shared Secret

Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number

Server Status

Support for CoA

Server Timeout seconds

Network User Enable

Management Enable

Management Retransmit Timeout seconds

IPSec Enable

CLI :

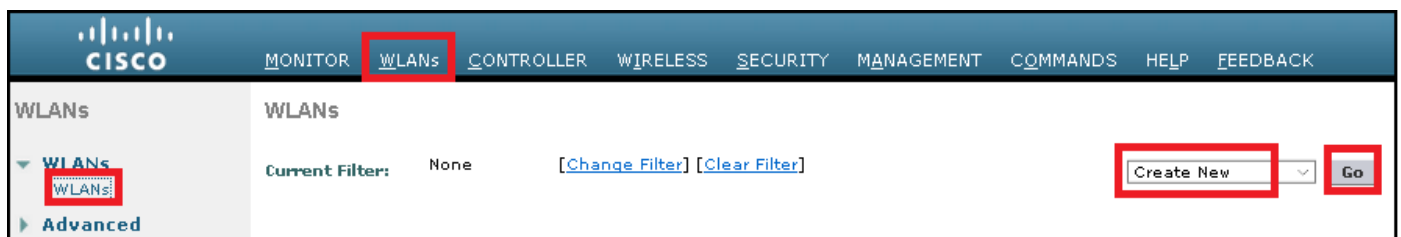
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

<a.b.c.d>对应于RADIUS服务器。

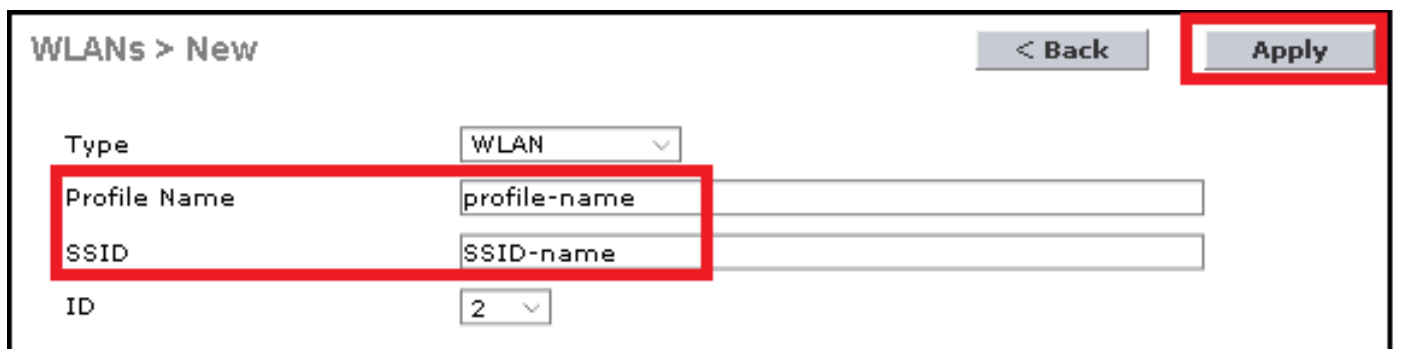
创建 SSID

GUI:

步骤1:打开WLC的GUI并导航至WLANs > Create New > Go，如图所示。



第二步：选择SSID和配置文件的名称，然后单击Apply，如图所示。



CLI :

```
> config wlan create <id> <profile-name> <ssid-name>
```

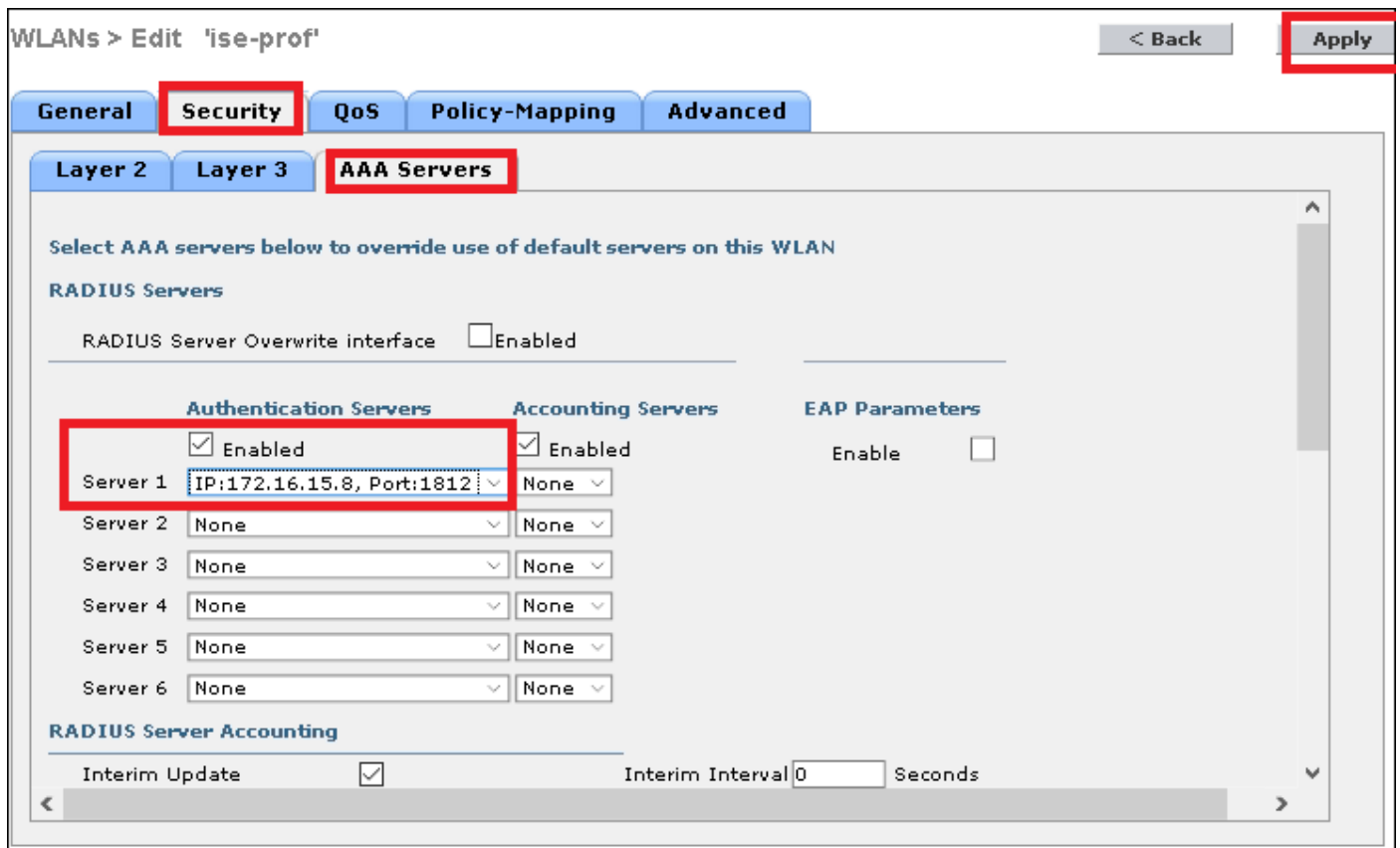
第三步：将RADIUS服务器分配给WLAN。

CLI :

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI:

导航到Security > AAA Servers并选择所需的RADIUS服务器，然后按图中所示的Apply。



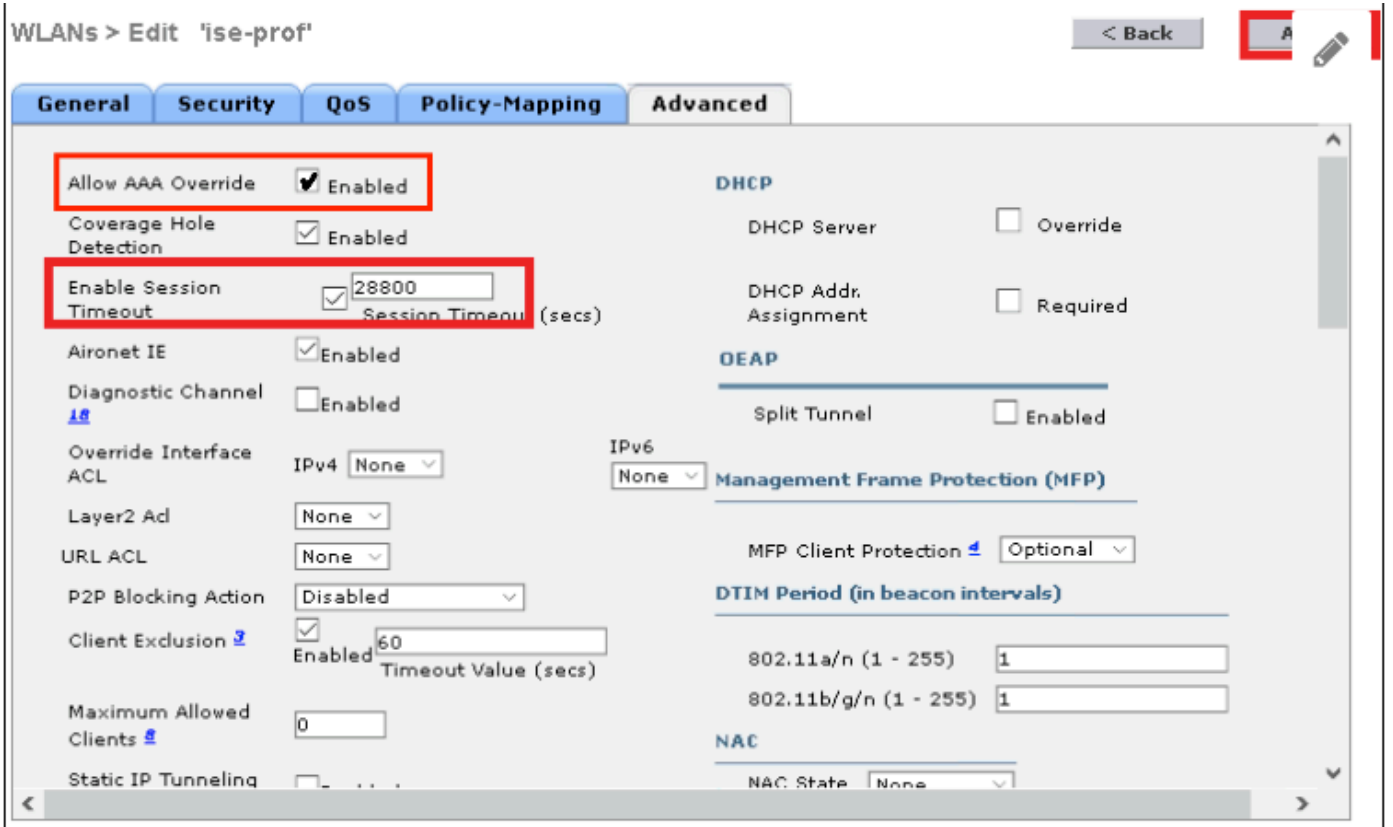
第四步：启用Allow AAA Override，并可选择增加会话超时

CLI：

```
> config wlan aaa-override enable <wlan-id>  
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

导航到WLANs > WLAN ID > Advanced并启用允许AAA覆盖。或者指定会话超时（如图所示）。



第五步：启用WLAN。

CLI：

```
> config wlan enable <wlan-id>
```

GUI:

导航到WLANs > WLAN ID > General，然后启用如图所示的SSID。

WLANs > Edit 'ise-prof' < Back Apply

General Security QoS Policy-Mapping Advanced

Profile Name: ise-prof

Type: WLAN

SSID: ise-ssid

Status: Enabled

Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): management

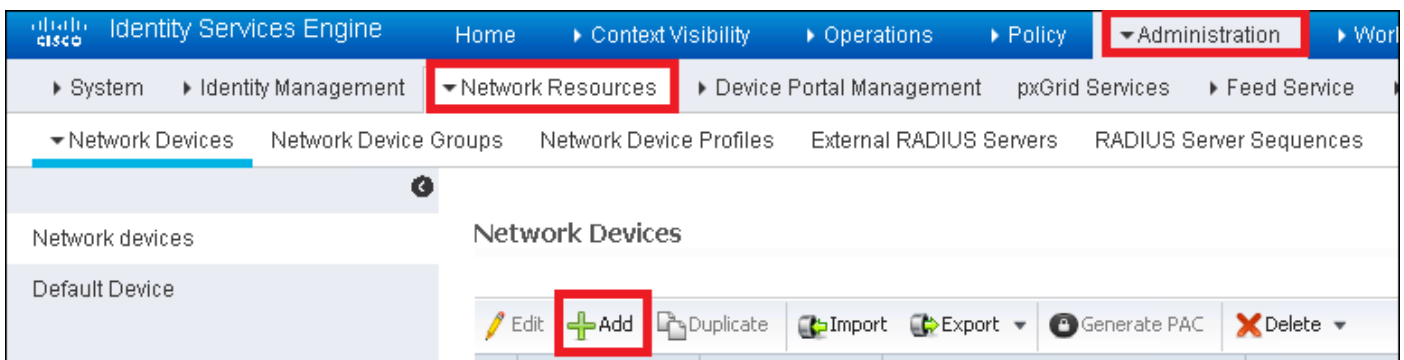
Multicast Vlan Feature: Enabled

Broadcast SSID: Enabled

NAS-ID: none

在ISE上声明WLC

步骤1:打开ISE控制台并导航到管理>网络资源>网络设备>添加，如图所示。



第二步：输入值。

或者，它可以是指定的型号名称、软件版本、说明，并根据设备类型、位置或WLC分配网络设备组。

a.b.c.d对应发送请求的身份验证的WLC接口。默认情况下，它是管理接口，如图所示。

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

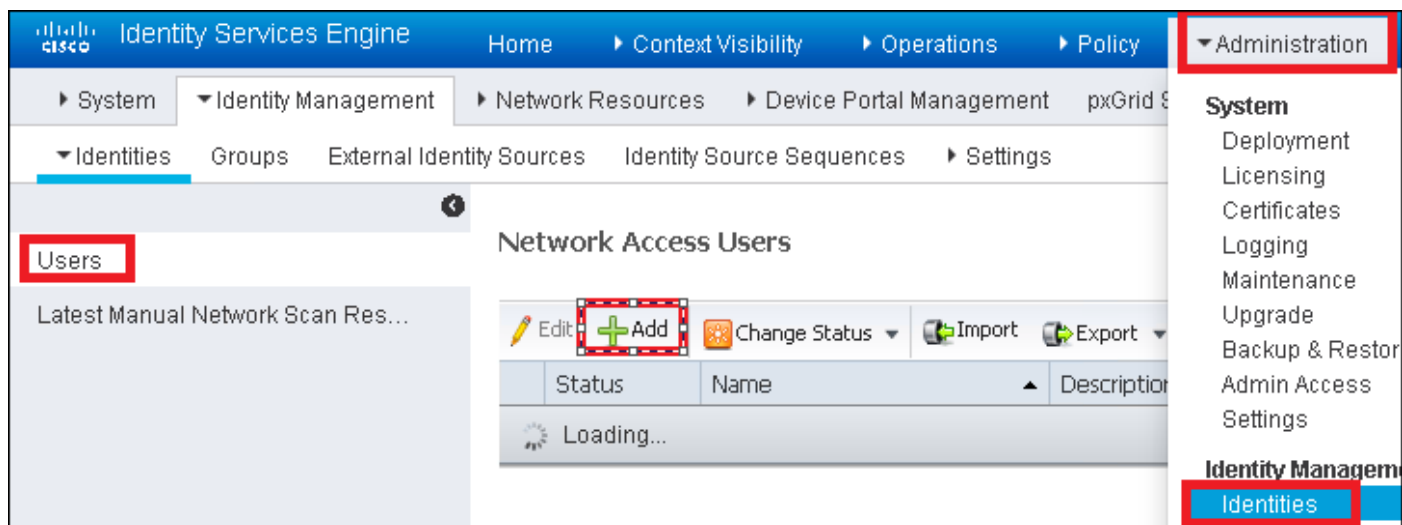
CoA Port

有关网络设备组的详细信息：

[ISE - 网络设备组](#)

在 ISE 上创建新用户

步骤1:导航到管理>身份管理>身份>用户>添加，如图所示。



第二步：输入相关信息。

在本示例中，此用户属于名为ALL_ACCOUNTS的组，但可以根据需要进行调整，如图所示。

▼ Network Access User

* Name

Status Enabled ▼

Email

▼ Passwords

Password Type: ▼

Password

Re-Enter Password

* Login Password

Enable Password

▼ User Information

First Name

Last Name

▼ Account Options

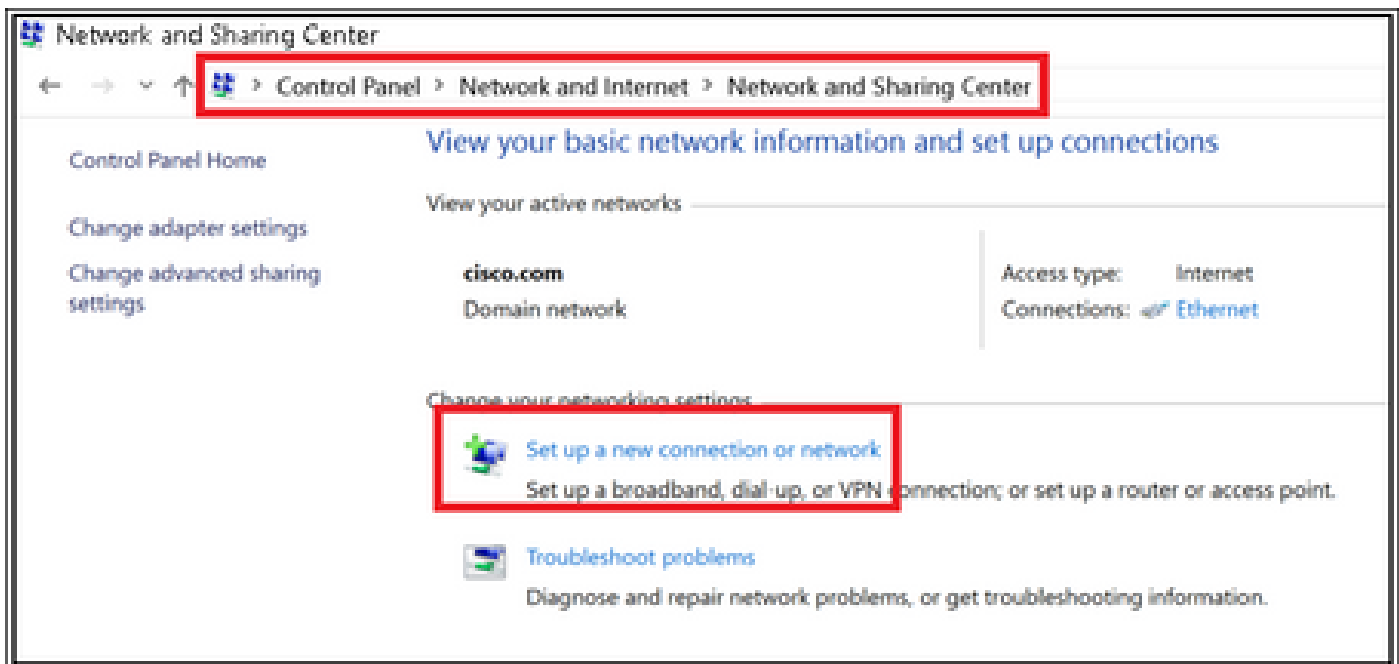
Description

Change password on next login

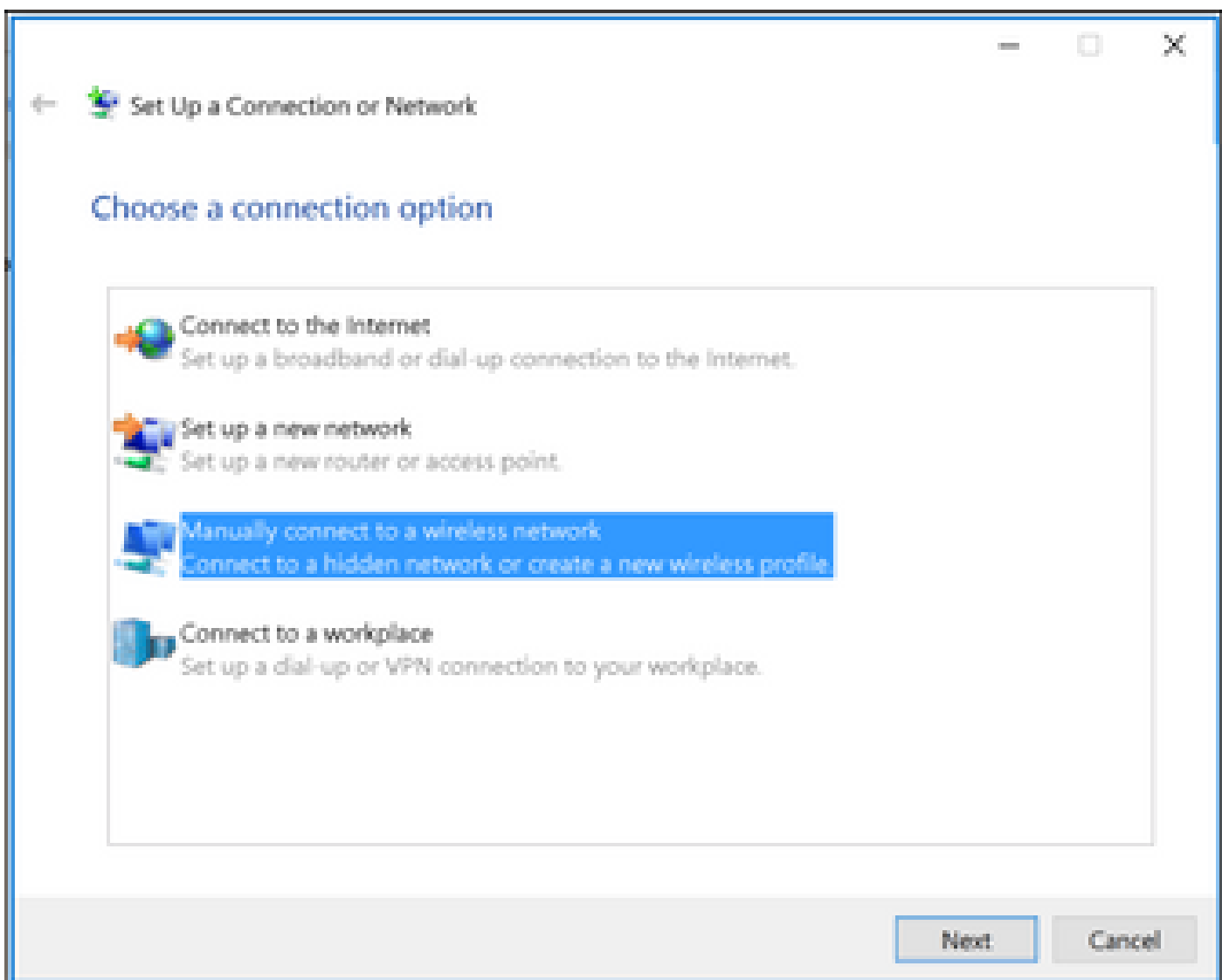
▼ Account Disable Policy

Disable account if date exceeds

▼ User Groups



第三步：选择Manually connect to a wireless network，然后单击Next，如图所示。



第四步：输入SSID名称和安全类型WPA2-Enterprise的信息，然后单击Next，如图所示。

← Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

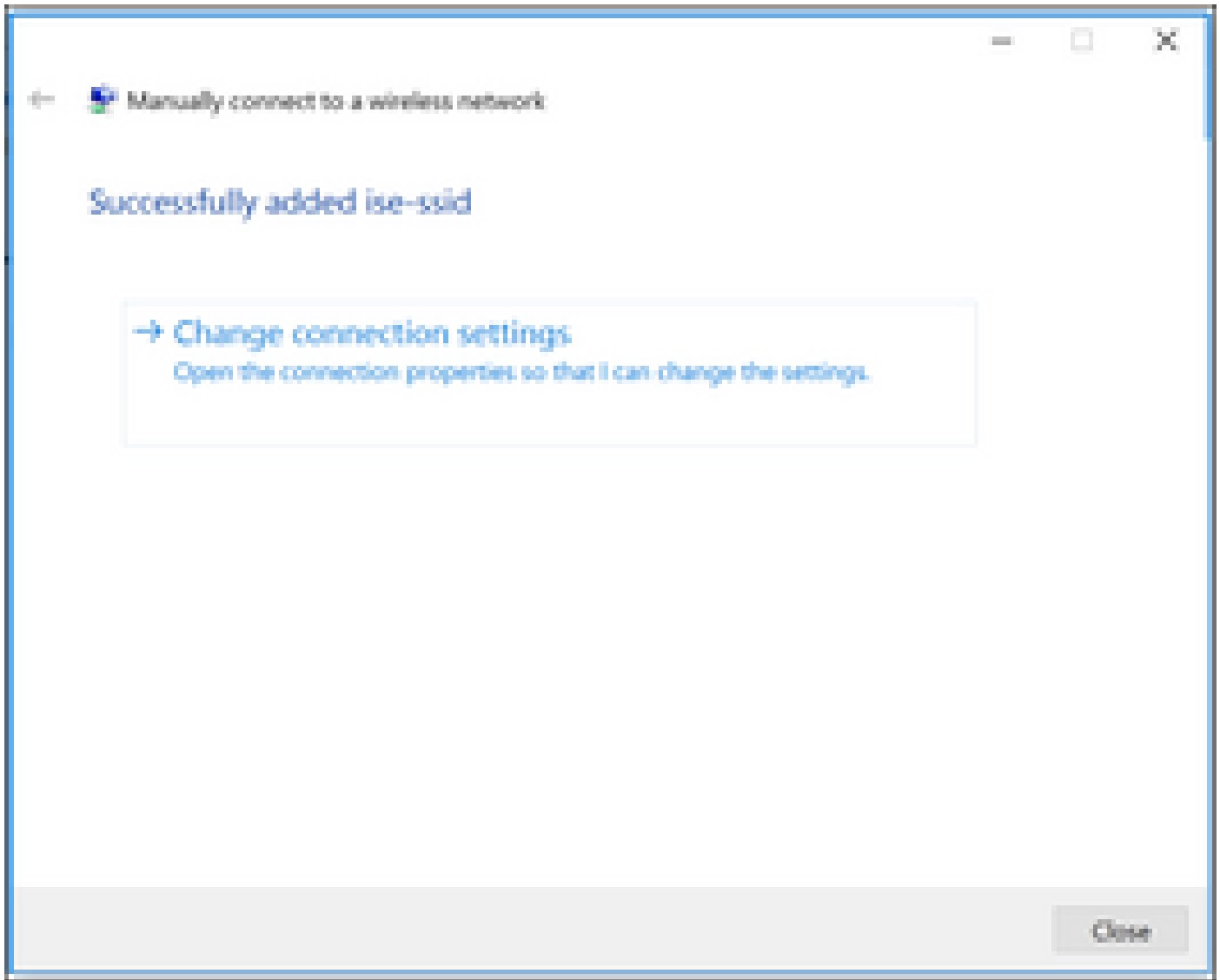
Security Key: Hide characters

Start this connection automatically

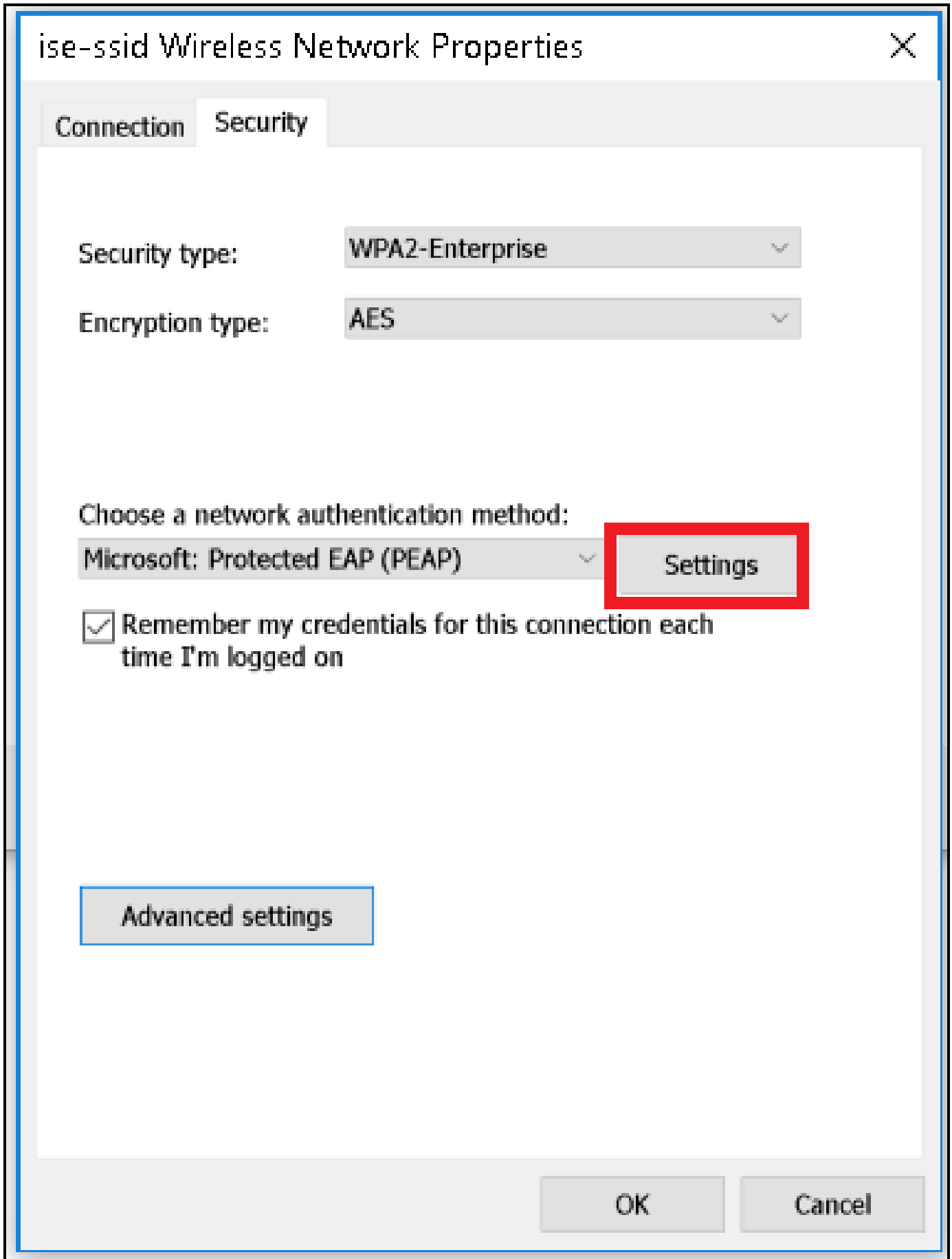
Connect even if the network is not broadcasting

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

第五步：选择Change connection settings以自定义WLAN配置文件的配置，如图所示。



第六步：导航到Security选项卡，然后单击Settings，如图所示。



步骤 7. 选择是否验证了RADIUS服务器。

如果是，请启用Verify the server identity by validating the certificate，并从Trusted Root Certification Authorities:列表中选择ISE的自签名证书。

之后，选择Configure并禁用Automatically use my Windows logon name and password...，然后单击OK，如图所示。

Protected EAP Properties



When connecting:

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1; srv2; *.*\, srv3\, com):

Trusted Root Certification Authorities:

- English Global Root...
- English Global Root...
- English Global Root...
- EAP-SelfSignedCertificate
- English Global Root...
- English Global Root...
- English Global Root...
- English Global Root...

Notifications before connecting:

Tell user if the server name or root certificate isn't specified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

Configure...

Enable Fast Reconnect

Disconnect if server does not present cryptobinding TLV

Enable Identity Privacy

OK

Cancel

返回Security选项卡后，选择Advanced settings，将身份验证模式指定为User authentication，并保存ISE上配置的凭证，以便对用户进行身份验证，如映像所示。

ise-ssid Wireless Network Properties



Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) Settings

Remember my credentials for this connection each time I'm logged on

Advanced settings

OK

Cancel

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):

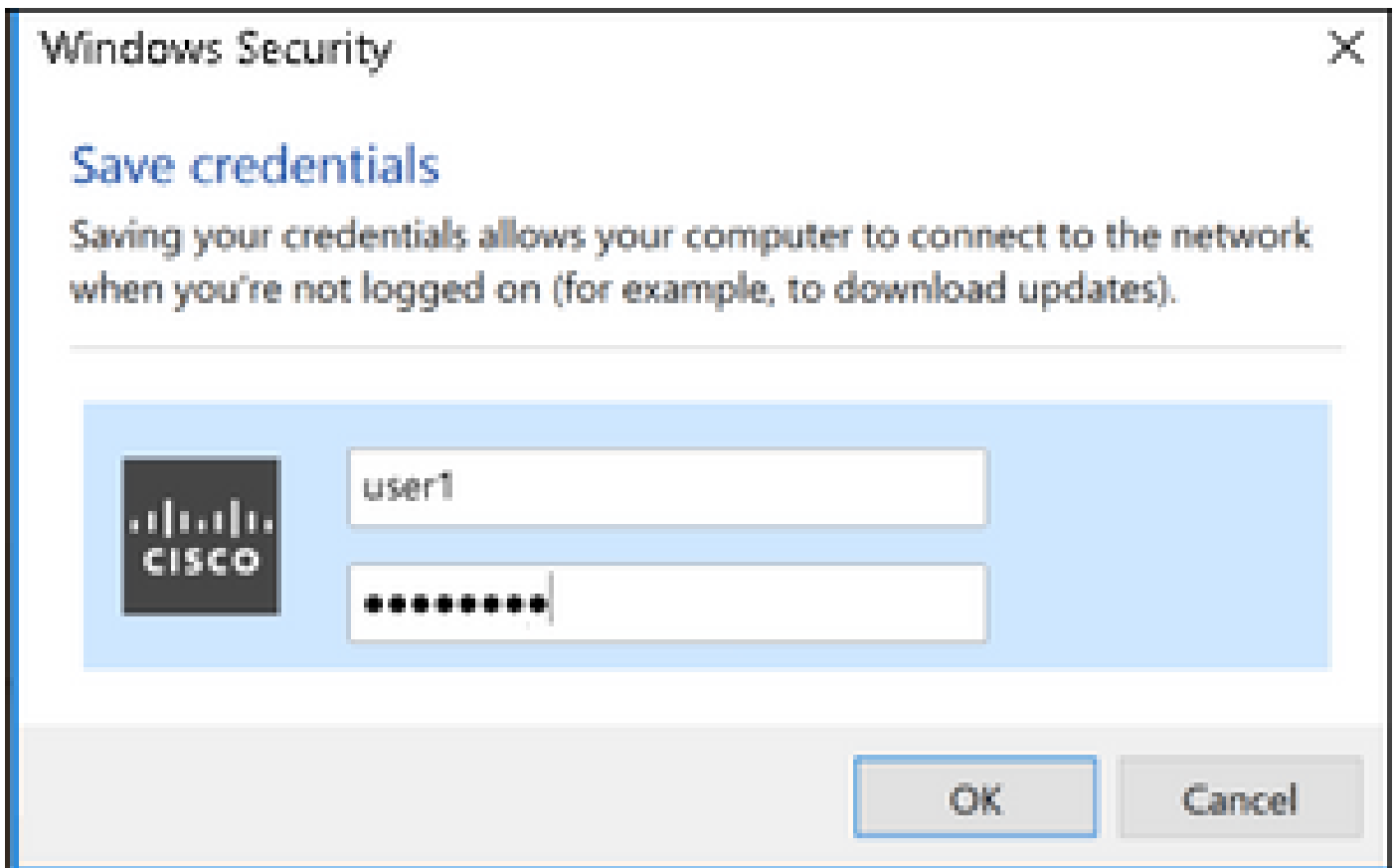
10

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

使用本部分可确认配置能否正常运行。

身份验证流程可以从WLC或ISE角度进行验证。

WLC上的身份验证过程

运行以下命令以监控特定用户的身份验证过程：

```
> debug client <mac-add-client>
> debug dot1x event enable
> debug dot1x aaa enable
```

身份验证成功的示例（省略了某些输出）：

```
<#root>
```

```
*apfMsConnTask_1: Nov 24 04:30:44.317:
```

```
e4:b3:18:7c:30:58 Processing assoc-req station:e4:b3:18:7c:30:58 AP:00:c8:8b:26:2c:d0-00
```

```
thread:1a5cc288
```

```
*apfMsConnTask_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 Reassociation received from mobile on BSSID 00
```

```
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mobil
```

*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying site-specific Local Bridging override
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Local Bridging Interface Policy for s
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 RSN Capabilities: 60
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Marking Mobile as non-

e4:b3:18:7c:30:58 Received 802.11i 802.1X key management suite, enabling dot1x Authentication

11w Capable

*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Received RSN IE with 1 PMKIDs from mobile e4:b
*apfMsConnTask_1: Nov 24 04:30:44.319: Received PMKID: (16)
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Searching for PMKID in MSCB PMKID cache for mo
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache f
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Initializing policy
*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP ru
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfMsAssoStateInc
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2 (apf_policy.c:437) Changing sta
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout forstation e4:b
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Stopping deletion of Mobile Station: (callerId
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Func: apfPemAddUser2, Ms Timeout = 0, Session
*apfMsConnTask_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00:
*spamApTask2: Nov 24 04:30:44.323: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58 Received ADD_MOBILE ack - Initiating 1x to STA e4:
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58

Sent dot1x auth initiate message for mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 reauth_sm state transition 0 ---> 1 for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 EAP-PARAM Debug - eap-params for Wlan-Id :2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x rea
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326:

e4:b3:18:7c:30:58 Sending EAP-Request/Identity to mobile e4:b3:18:7c:30:58 (EAP Id 1)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from m
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Resetting reauth count 1 to 0 for mobile e4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 EAP State update from Connecting to Authent
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=215) fo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 WARNING: updated EAP-Identifier 1 ==> 215
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Resetting reauth count 0 to 0 for mobile e4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) fo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Processing Access-Accept for mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 ac1 from 255 to 255

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 Flex ac1 from 65535 to 6

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Username entry (user1) created for mobile, length = 253

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name received: vlan2404

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 override for default ap group, marking intg

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mo

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Re-applying interface policy for client

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 apfApplyWlanPolicy: Apply WLAN Policy over

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:

e4:b3:18:7c:30:58 Inserting AAA Override struct for mobile

MAC: e4:b3:18:7c:30:58, source 4

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying override policy from source Overri

*Dot1x_NW_MsgTask_0: Nov 24

04:30:44.531: e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name receive

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying Interface(vlan2404) policy on Mobi

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Re-applying interface policy for client

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Setting re-auth timeout to 0 seconds, got f

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x rea

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for stati

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for stati

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding BSSID 00:c8:8b:26:2c:d1 to PMKID cac

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: New PMKID: (16)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 unsetting PmkIdValidatedByAp

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Updating AAA Overrides from local for stati

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding Audit session ID payload in Mobility

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can ta

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Sending EAP-Success to mobile e4:b3:18:7c:3

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AAACB from Dot1xCB as AAA auth is d

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 key Desc Version FT - 0

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Found an cache entry for BSSID 00:c8:8b:26:

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: Including PMKID in M1 (16)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: M1 - Key Data: (22)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: [0000] dd 14 00 0f ac 04 cc 3a 3d 26 80 17 8b f1 2d c5

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: [0016] cd fd a0 8a c4 39

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Starting key exchange to mobile e4:b3:18:7c:30:58, data packets will be dropped

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for r

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Entering Backend Auth Success state (id=223

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authentication
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547:

e4:b3:18:7c:30:58 Received EAPOL-key in PTK_START state (message 2) from mobile

e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for EAP Pkt for mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:

e4:b3:18:7c:30:58 Received EAPOL-key in PTKINITNEGOTIATING state (message 4)

from mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Freeing EAP Retransmit Buffer for mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMs1xStateInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:

e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Client Vlan Ip: 172.16.0.134, Vlan mask
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Virtual Ip: 10.10.10.10
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile L2AUTHCOMPLETE (4)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556:

e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6677
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
type = Airespace AP - Learn IP address
on AP 00:c8:8b:26:2c:d0, slot 0, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile L2AUTHCOMPLETE (4)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keys for mobile e4:b3:18:7c:30:58
*spamApTask2: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 00:c8:8b:26:2c:d0
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update request received
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.3
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) State Update from Mobility

```

*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Ad
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
  IPv4 ACL ID = 255,
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobi
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Sent an XID frame
*dtlArpTask: Nov 24 04:30:47.932: e4:b3:18:7c:30:58 Static IP client associated to interface vlan2404 w
*dtlArpTask: Nov 24 04:30:47.933: e4:b3:18:7c:30:58 apfMsRunStateInc
*dtlArpTask: Nov 24 04:30:47.933:

e4:b3:18:7c:30:58 172.16.0.151 DHCP_REQD (7) Change state to RUN (20)

last state DHCP_REQD (7)

```

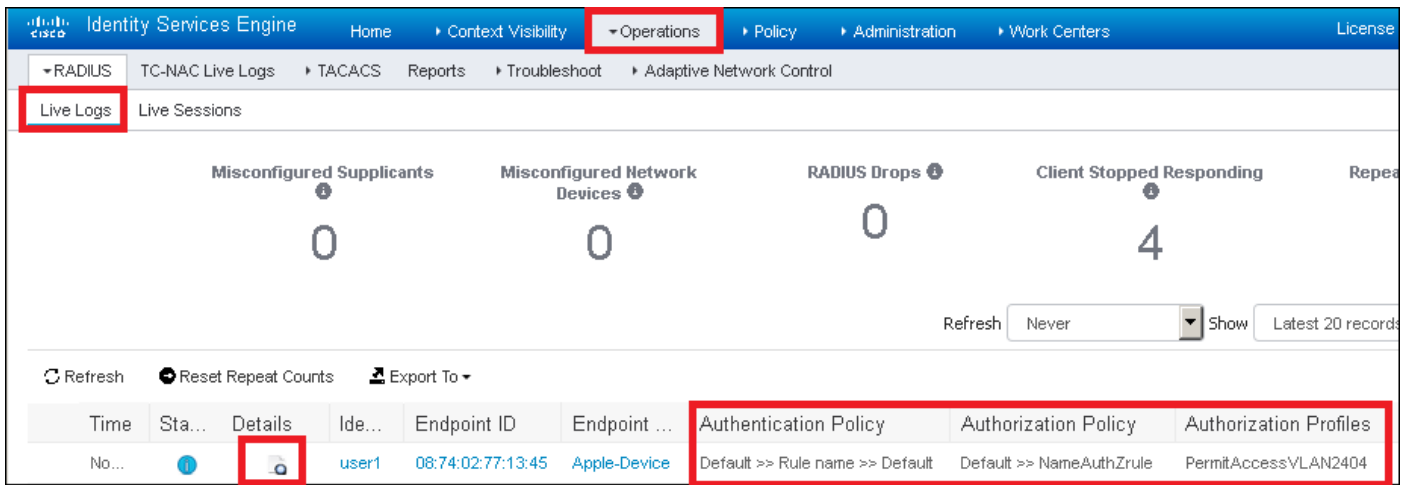
要轻松读取调试客户端输出，请使用无线调试分析器工具：

[Wireless Debug Analyzer](#)

ISE上的身份验证过程

导航到操作(Operations)> RADIUS >实时日志(Live Logs)，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。

有关详细信息，请单击Details以查看更详细的身份验证过程，如图所示。



故障排除

当前没有故障排除此配置的特定可用资料。

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）。