

使用ISE内部CA在9800 WLC上配置EAP-TLS

目录

[简介](#)

[先决条件](#)

[使用的组件](#)

[背景信息](#)

[EAP-TLS身份验证流程](#)

[EAP-TLS流程中的步骤](#)

[配置](#)

[网络图](#)

[配置](#)

[ISE 配置](#)

[添加网络设备](#)

[验证内部CA](#)

[添加身份验证方法](#)

[指定证书模板](#)

[创建证书门户](#)

[添加内部用户](#)

[ISE证书调配门户和RADIUS策略配置](#)

[9800 WLC配置](#)

[将ISE服务器添加到9800 WLC](#)

[在9800 WLC上添加服务器组](#)

[在9800 WLC上配置AAA方法列表](#)

[在9800 WLC上配置授权方法列表](#)

[在9800 WLC上创建策略配置文件](#)

[在9800 WLC上创建WLAN](#)

[在9800 WLC上使用策略配置文件映射WLAN](#)

[将策略标记映射到9800 WLC上的接入点](#)

[安装完成后的WLC运行配置](#)

[为用户创建和下载证书](#)

[Windows 10计算机上的证书安装](#)

[验证](#)

[故障排除](#)

[参考](#)

简介

本文档介绍使用身份服务引擎的证书颁发机构对用户进行身份验证的EAP-TLS身份验证。

先决条件

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 无线控制器:运行17.09.04a的C9800-40-K9
- 思科ISE:运行版本3补丁4
- AP型号：C9130AXI-D
- 交换机：9200-L-24P

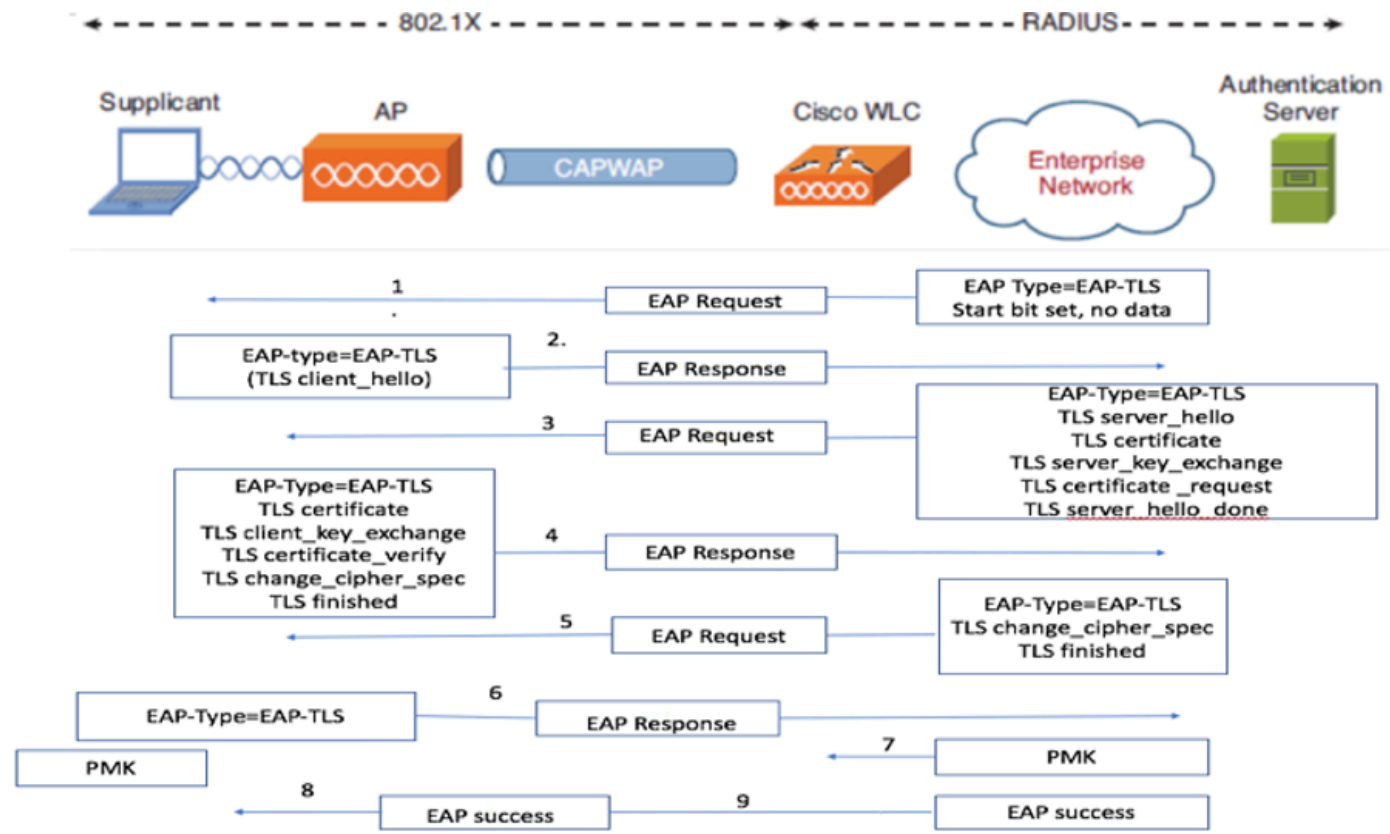
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

大多数组织都有自己的CA向最终用户颁发证书以进行EAP-TLS身份验证。ISE包括一个内置证书颁发机构，可用于生成用户在EAP-TLS身份验证中使用的证书。在无法使用完整CA的情况下，使用ISE CA进行用户身份验证会有优势。

本文档概述了有效使用ISE CA对无线用户进行身份验证所需的配置步骤。EAP-TLS身份验证流程

EAP-TLS身份验证流程



EAP-TLS身份验证流程

EAP-TLS流程中的步骤

1. 无线客户端与接入点(AP)关联。
2. 在此阶段，AP不允许数据传输并发送身份验证请求。
3. 客户端作为请求方，使用EAP-Response Identity进行响应。
4. 无线局域网控制器(WLC)将用户ID信息转发到身份验证服务器。
5. RADIUS服务器使用EAP-TLS启动数据包回复客户端。
6. EAP-TLS会话从此开始。
7. 客户端将EAP-Response发送回身份验证服务器，包括密码设置为NULL的client_hello握手消息。
8. 身份验证服务器使用访问质询数据包进行响应，该数据包包含：

```
TLS server_hello  
Handshake message  
Certificate  
Server_key_exchange  
Certificate request  
Server_hello_done
```

- 9.客户端回复的EAP-Response消息包括：

```
Certificate (for server validation)  
Client_key_exchange  
Certificate_verify (to verify server trust)  
Change_cipher_spec  
TLS finished
```

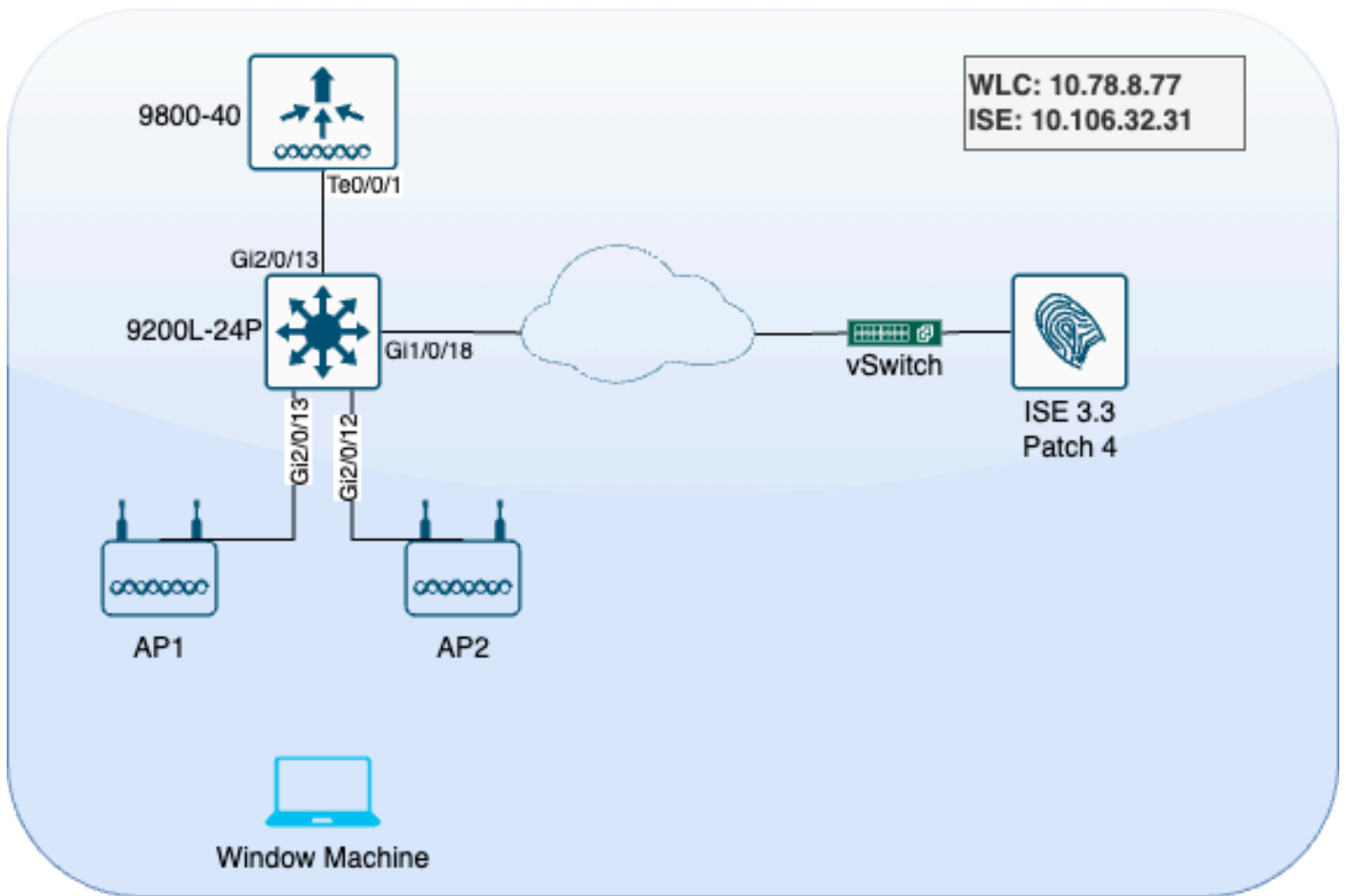
- 10.成功进行客户端身份验证后，RADIUS服务器将发送访问质询，内容包括：

```
Change_cipher_spec  
Handshake finished message
```

- 11.客户端验证哈希值以验证RADIUS服务器。
- 12.在TLS握手期间，从密钥动态派生新的加密密钥。
13. EAP-Success消息从服务器发送到身份验证器，然后发送到请求方。
- 14.启用EAP-TLS的无线客户端现在可以访问无线网络。

配置

网络图



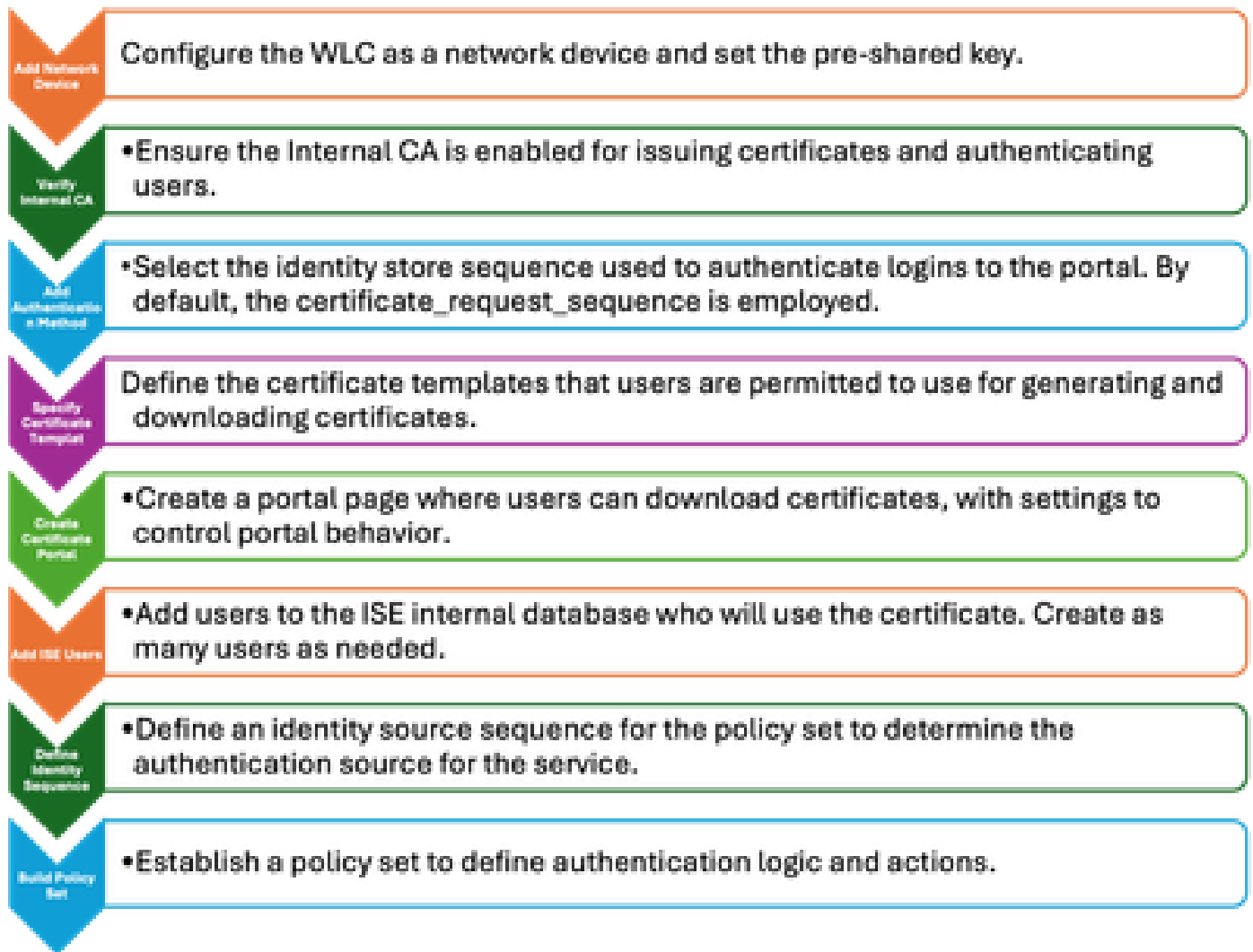
实验室拓扑结构

配置

在本节中，我们将配置两个组件：ISE和9800 WLC。

ISE 配置

以下是ISE服务器的配置步骤。每个步骤都附带此部分中的屏幕截图，以提供可视指导。

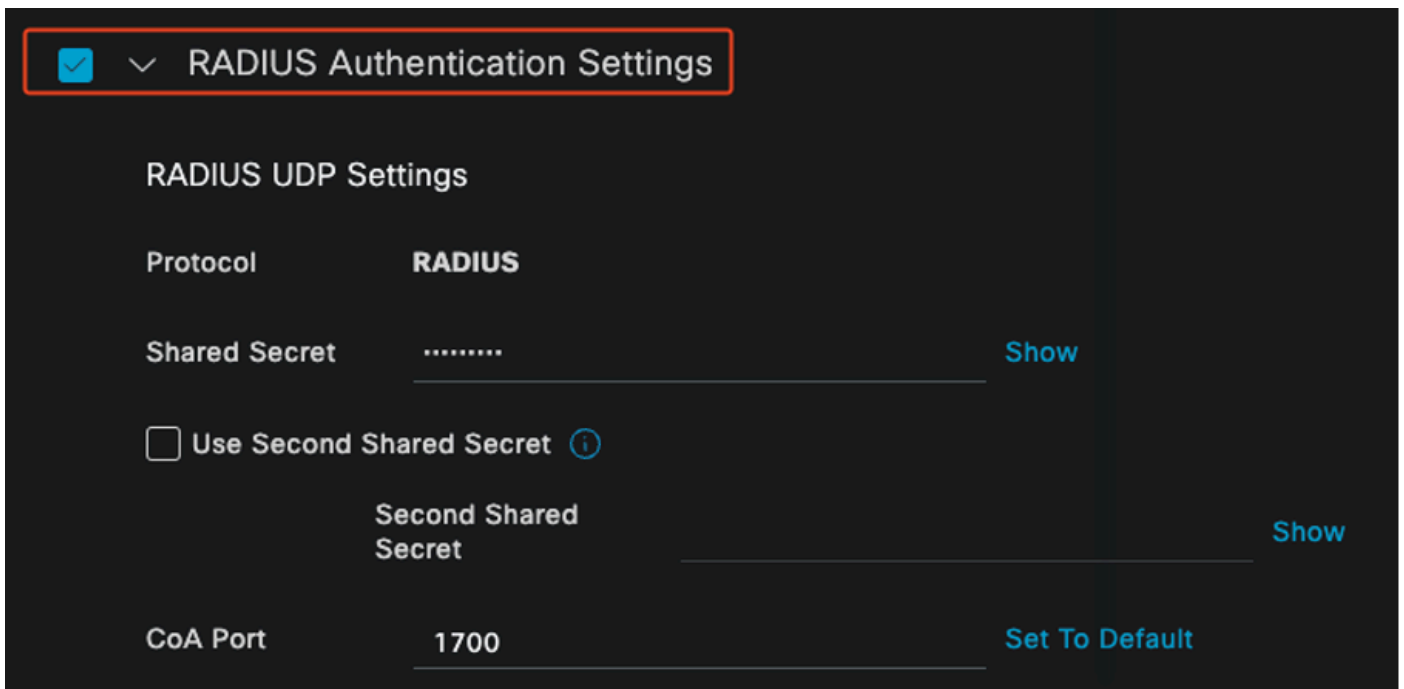


ISE服务器配置步骤

添加网络设备

要添加无线LAN控制器(WLC)作为网络设备，请使用以下说明：

1. 导航到Administration > Network Resources > Network Devices。
2. 单击+Add图标启动添加WLC的过程。
3. 确保预共享密钥与WLC和ISE服务器匹配，以实现正确的通信。
4. 正确输入所有详细信息后，点击左下角的Submit保存配置

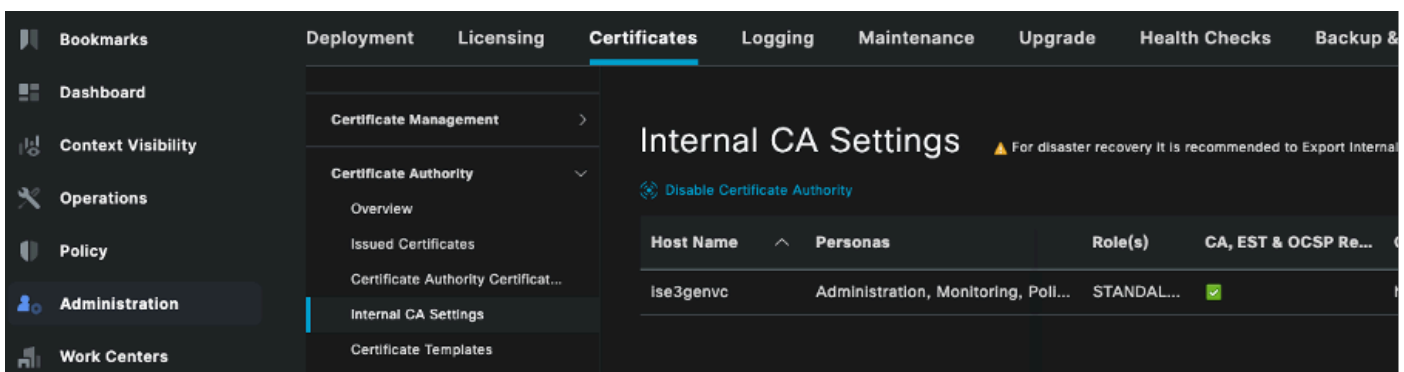


添加网络设备

验证内部CA

要验证内部证书颁发机构(CA)设置，请执行以下步骤：

1. 转至Administration > System > Certificates > Certificate Authority > Internal CA Settings。
2. 确保已启用CA列以确认内部CA处于活动状态。



验证内部CA

添加身份验证方法

导航到管理>身份管理>身份源序列。添加自定义身份序列以控制门户登录源。

Identities Groups External Identity Sources **Identity Source Sequences** Settings

[Identity Source Sequences List](#) > Allow_EMP_Cert

Identity Source Sequence

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	<input checked="" type="checkbox"/> Internal Users
Guest Users	<input type="checkbox"/>
All_AD_Join_Points	<input type="checkbox"/>

> < < >

认证方法

指定证书模板

要指定证书模板，请执行以下步骤：

步骤1. 导航到管理>System >证书>证书颁发机构>证书模板。

步骤2. 点击+Add图标以创建新的证书模板：

2.1 为模板提供ISE服务器的本地唯一名称。

2.2 确保公用名(CN)设置为\$UserName\$。

2.3检验主题备用名称(SAN)是否已映射到MAC地址。

2.4 将SCEP RA配置文件设置为ISE内部CA。

2.5在extended key usage部分，启用客户端身份验证。

Field	Value
* Name	EAP_Authentication_Certificate_Template
Description	This template will be used to issue certificates for EAP Authentication
Subject	\$UserName\$
Common Name (CN)	
Organizational Unit (OU)	Example unit
Organization (O)	Company name
City (L)	City
State (ST)	State
Country (C)	US
Subject Alternative Name (SAN)	MAC Address
Key Type	RSA
Key Size	2048
* SCEP RA Profile	ISE Internal CA
Valid Period	730 Day(s) (Valid Range 1 - 3652)
Extended Key Usage	<input checked="" type="checkbox"/> Client Authentication <input type="checkbox"/> Server Authentication

证书模板

创建证书门户

要创建用于生成客户端证书的证书门户，请执行以下步骤：

步骤1.导航到管理>设备门户管理>证书调配。

步骤2.单击创建，设置新的门户页面。

步骤3.为门户提供唯一名称，以便轻松识别它。

3.1.选择门户的端口号；将此设置为8443。

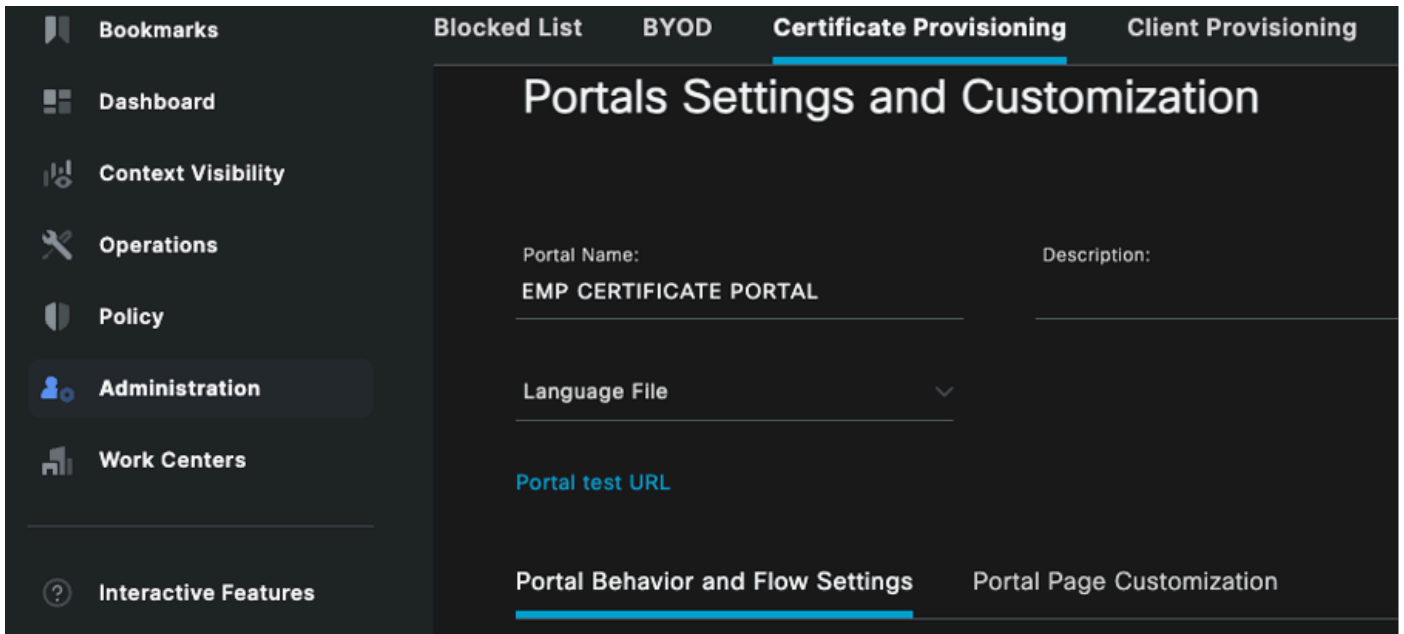
3.2.指定ISE侦听此门户的接口。

3.3.选择Certificate Group Tag作为默认门户证书组。

3.4.选择authentication method，指明用于验证登录此门户的身份库序列。

3.5.包括其成员可以访问门户的授权组。例如，如果您的用户属于此组，请选择Employee用户组。

3.6.定义在“证书调配”(Certificate Provisioning)设置下允许的证书模板。



Portal & Page Settings

Portal Settings

HTTPS port:*

1

8443

(8000 - 8999)

Allowed Interfaces:*

2

For PSNs Using Physical Interfaces

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3
- Gigabit Ethernet 4
- Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured

- Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
- Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
- Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: *

3

Default Portal Certificate Group

Configure certificates at:

[Administration > System > Certificates > System Certificates](#)

Authentication method: *

4

Certificate_Request_Sequence

Configure authentication methods at:

[Administration > Identity Management > Identity Source Sequences](#)

Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available

Q

- ALL_ACCOUNTS (default)
- GROUP_ACCOUNTS (default)
- OWN_ACCOUNTS (default)

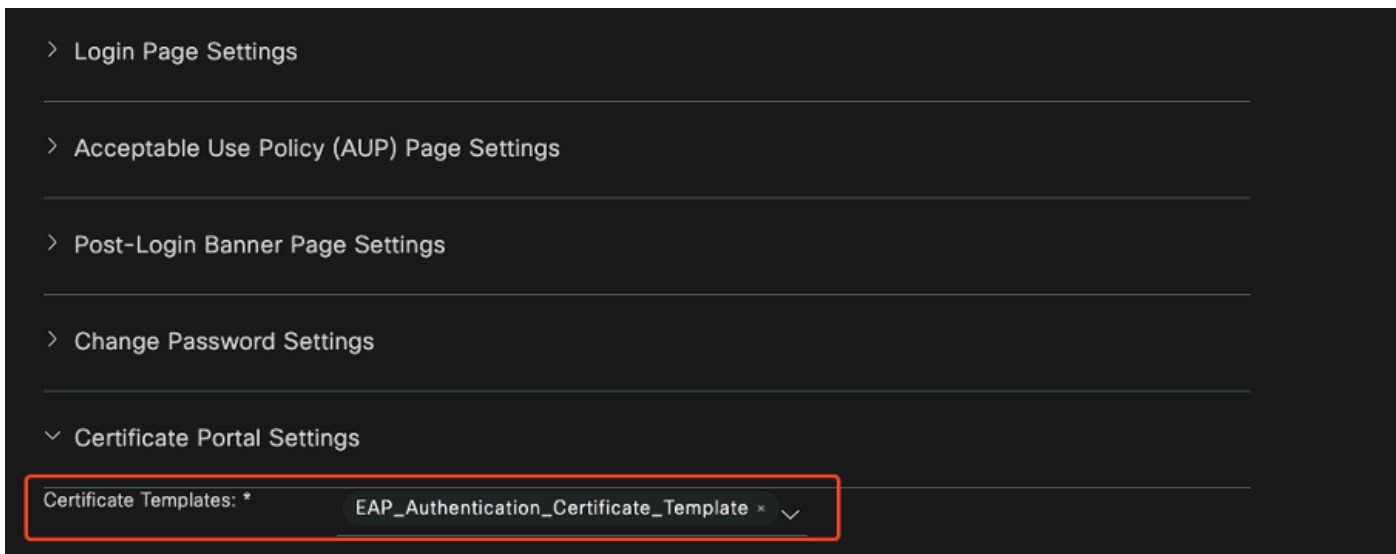
Chosen

Employee

Choose all

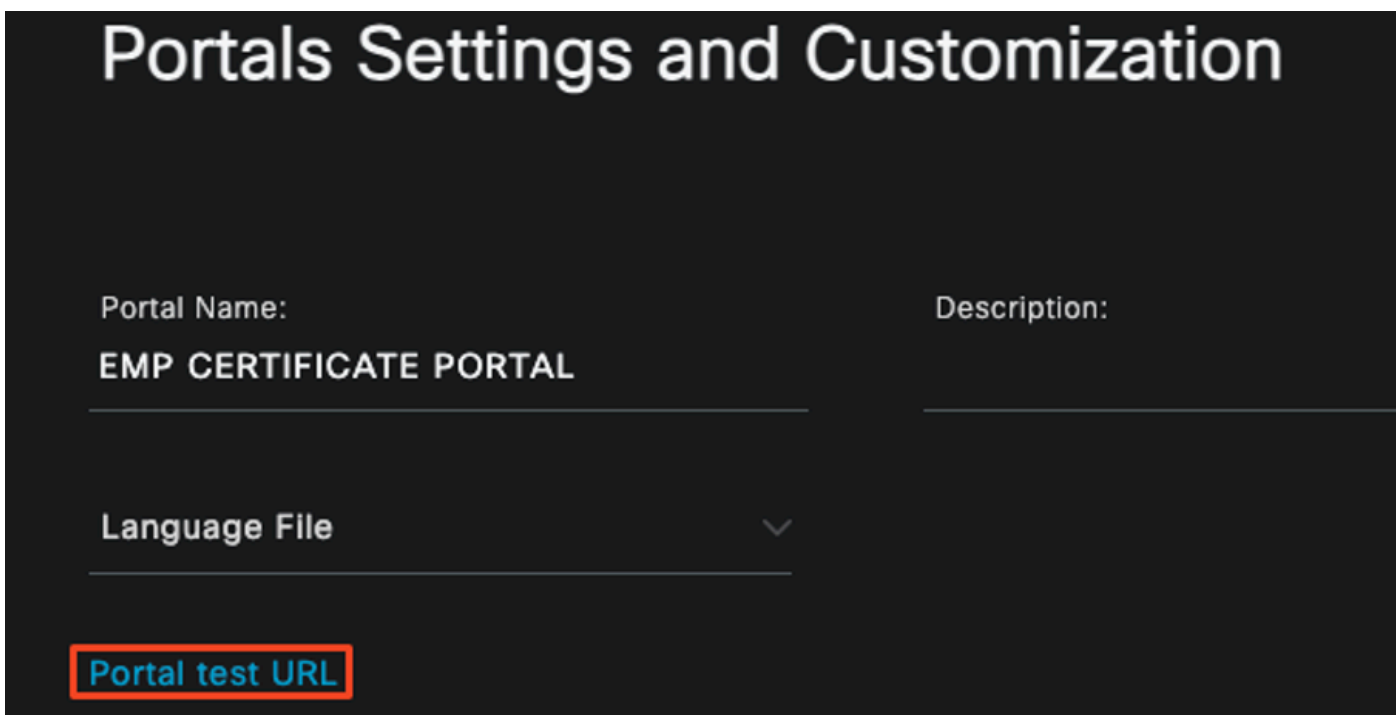
Clear all

Fully qualified domain name (FQDN):

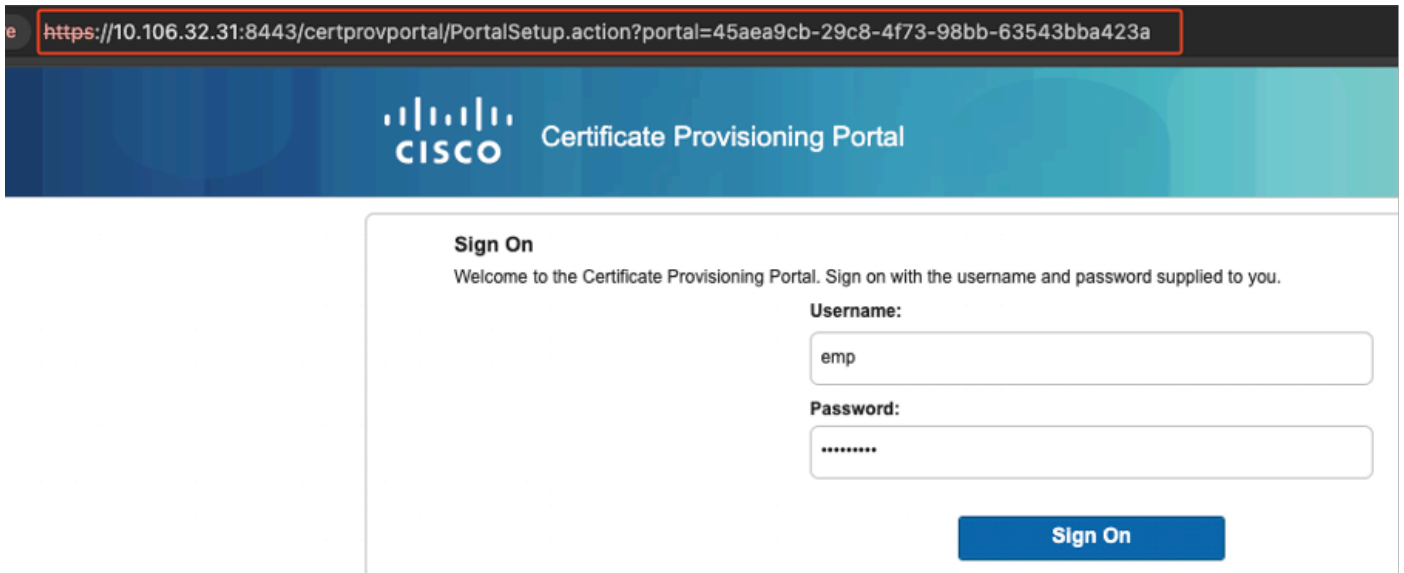


证书门户配置

完成此设置后，您可以通过点击门户测试URL来测试门户。此操作将打开门户页面。



测试门户页面URL

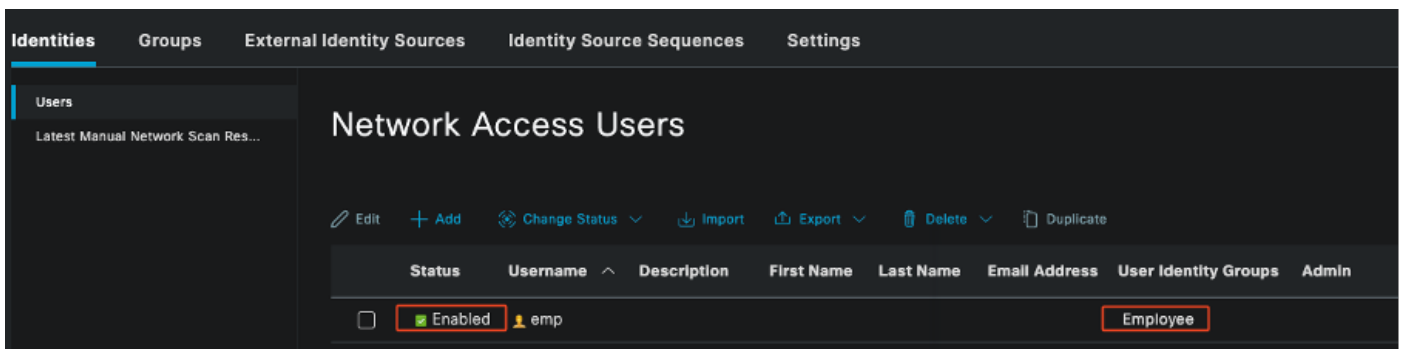


门户页

添加内部用户

要创建通过证书门户进行身份验证的用户，请执行以下步骤：

1. 转至Administration > Identity Management > Identities > Users。
2. 单击选项将用户添加到系统。
3. 选择用户所属的User Identity Groups。在本例中，将用户分配到Employee组。



添加内部用户

ISE证书调配门户和RADIUS策略配置

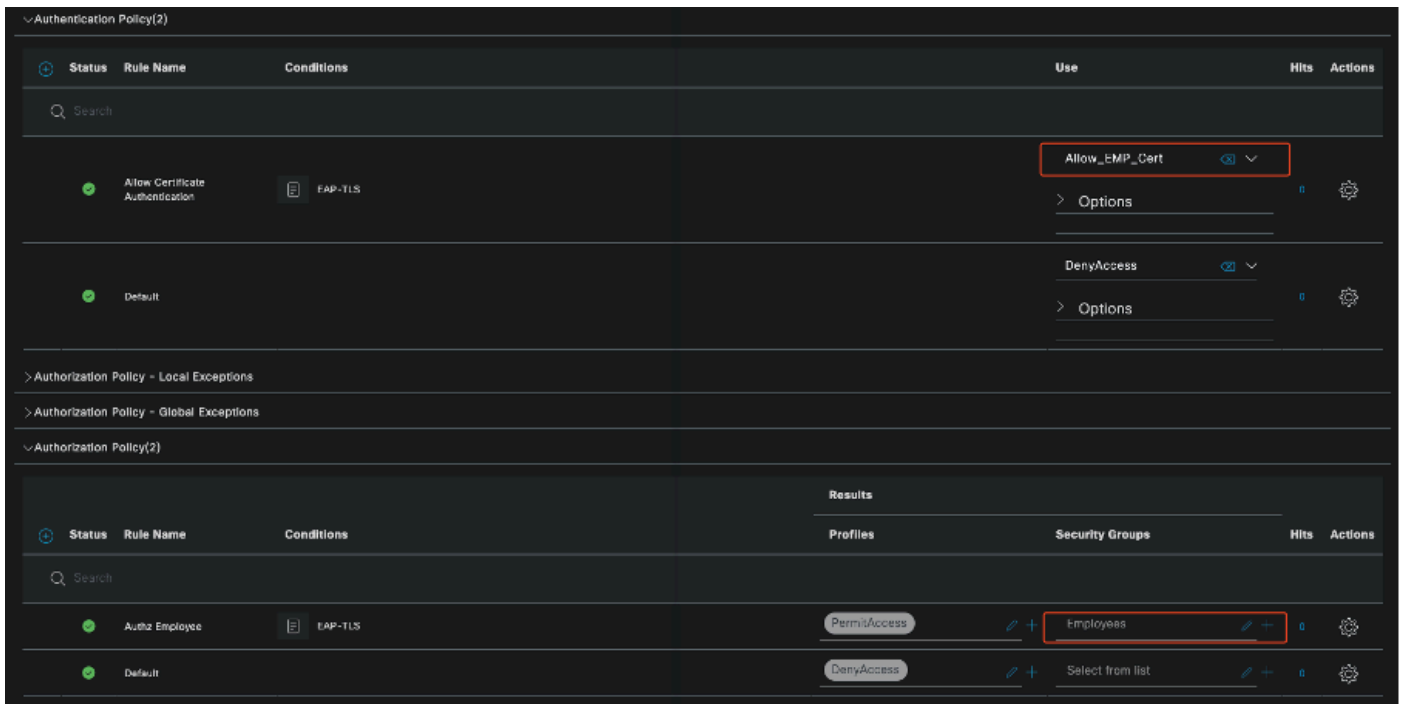
上一节介绍ISE证书调配门户的设置。现在，我们将ISE RADIUS策略集配置为允许用户身份验证。

1. 配置ISE RADIUS策略集
2. 导航到Policy > Policy Sets。
3. 点击加号(+)创建新的策略集。

在本示例中，设置一个简单的策略集，用于使用用户证书对用户进行身份验证。



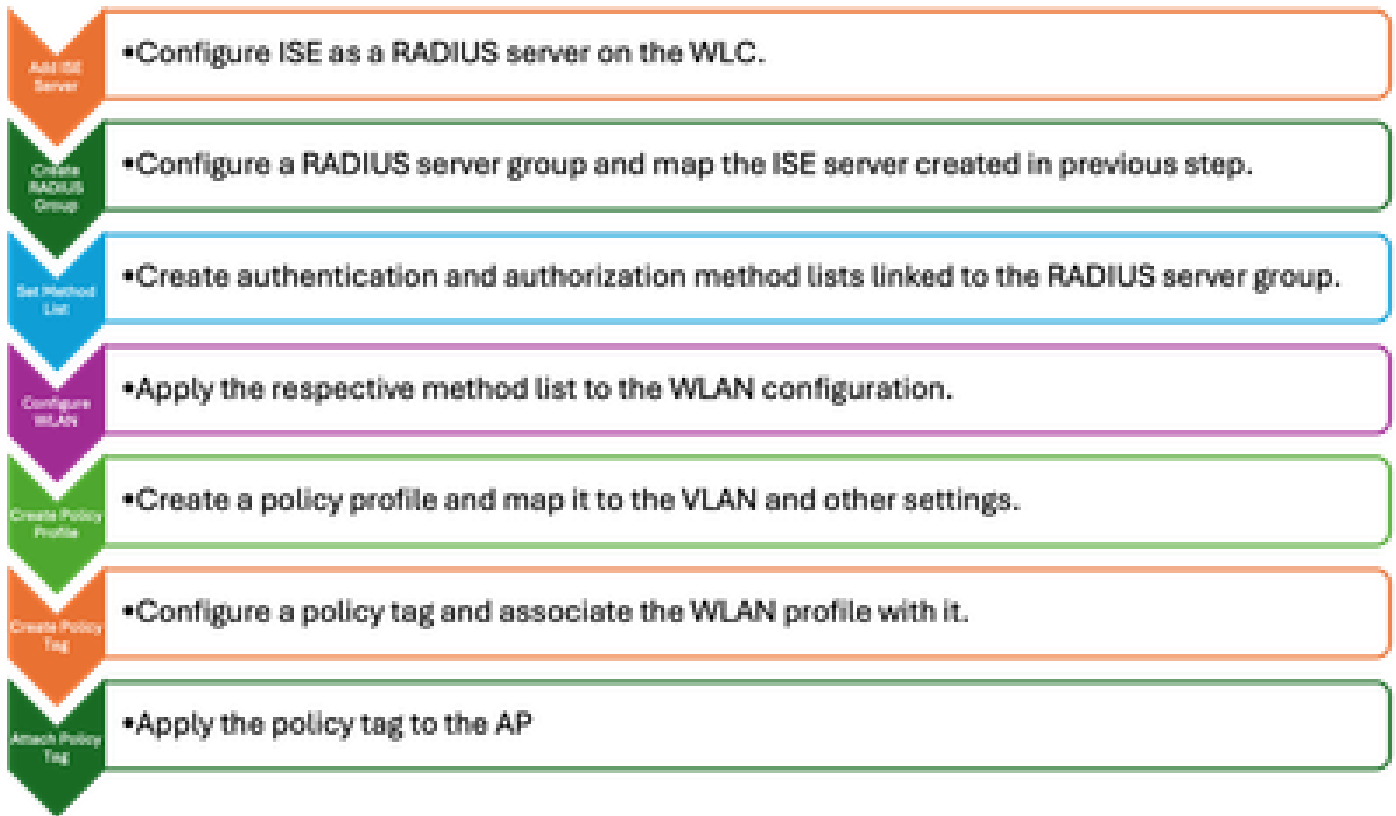
策略集



显示身份验证和授权策略的策略集

9800 WLC配置

以下是9800 WLC的配置步骤。每个步骤都附带此部分中的屏幕截图，以提供可视指导。



WLC配置步骤

将ISE服务器添加到9800 WLC

1. 要将ISE服务器与9800无线局域网控制器(WLC)集成，请执行以下步骤：
2. 转至Configuration > Security > AAA。
3. 单击Add按钮以在WLC配置中包含ISE服务器。

Configuration > Security > AAA Show Me How

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add Delete

RADIUS

TACACS+

LDAP

Create AAA Radius Server

Name* ISE3

Server Address* 10.106.32.31

PAC Key

Key Type Clear Text

Key*

Confirm Key*

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ENABLED

CoA Server Key Type Clear Text

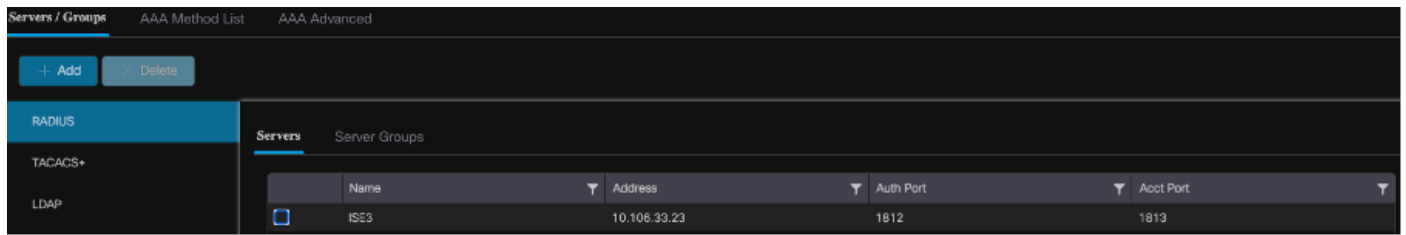
CoA Server Key

Confirm CoA Server Key

Automate Tester

在WLC中添加ISE服务器

添加服务器后，它将显示在服务器列表中。

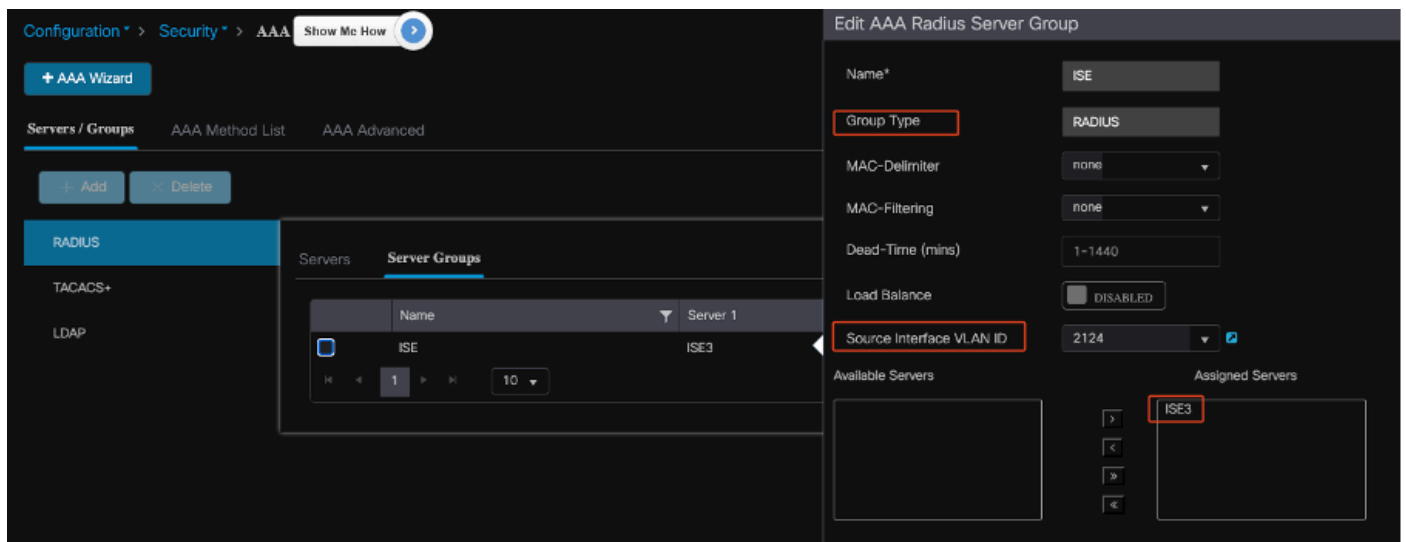


显示Radius服务器

在9800 WLC上添加服务器组

要在9800无线LAN控制器上添加服务器组，请完成以下步骤：

1. 导航到Configuration > Security > AAA。
2. 单击Server Group选项卡，然后单击Add以创建新的服务器组。

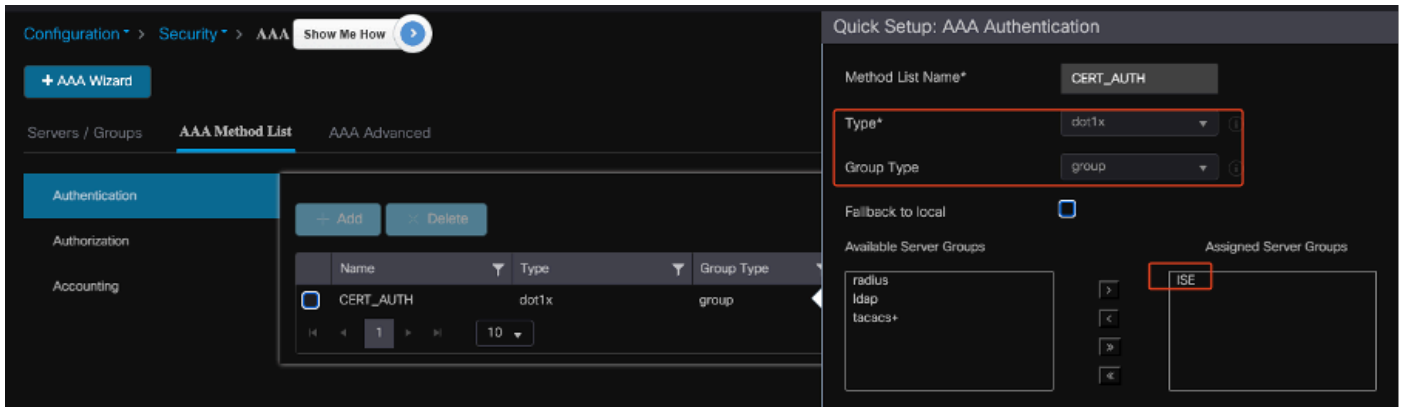


将ISE服务器映射到Radius服务器组

在9800 WLC上配置AAA方法列表

创建服务器组后，按照以下步骤配置身份验证方法列表：

1. 导航到Configuration > Security > AAA > AAA Method List。
2. 在Authentication选项卡中，添加新的身份验证方法列表。
3. 将类型设置为dot1x。
4. 选择group作为组类型。
5. 包括您之前创建的ISE服务器组作为服务器组。

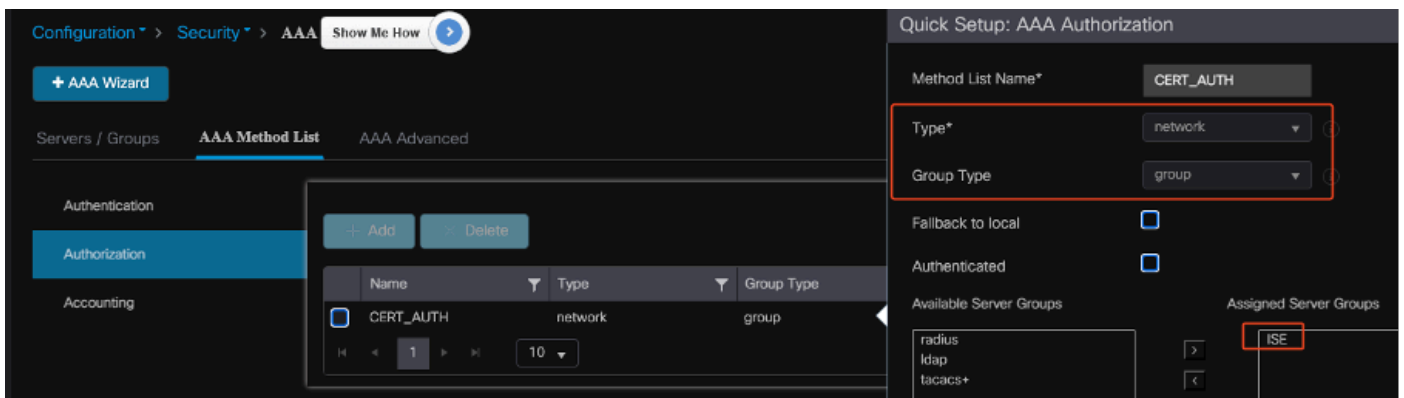


创建身份验证方法列表

在9800 WLC上配置授权方法列表

要设置授权方法列表，请执行以下步骤：

1. 导航到AAA Method List部分中的Authorization选项卡。
2. 单击Add创建新的授权方法列表。
3. 选择network作为类型。
4. 选择group作为组类型。
5. 包括ISE服务器组作为服务器组。

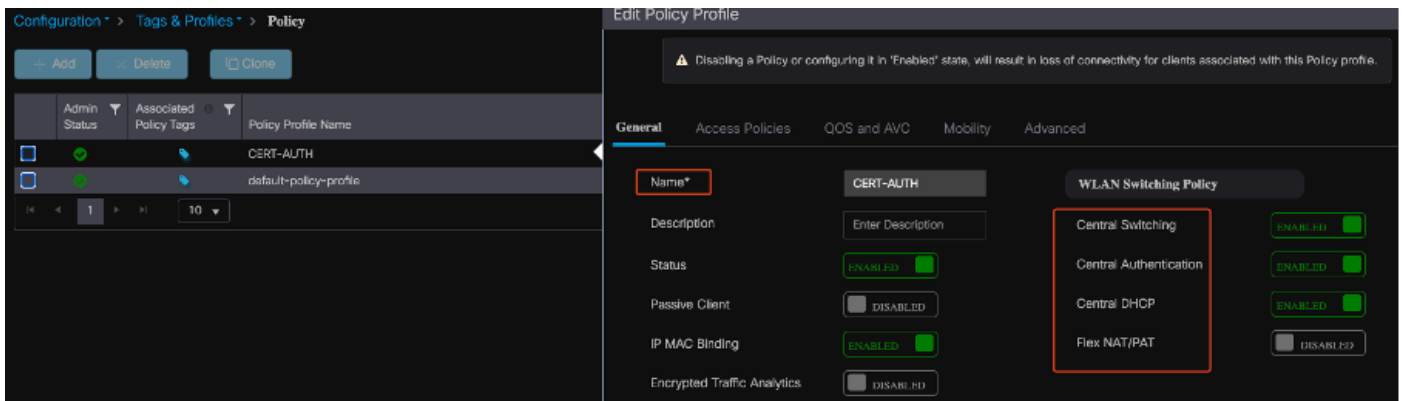


添加授权方法列表

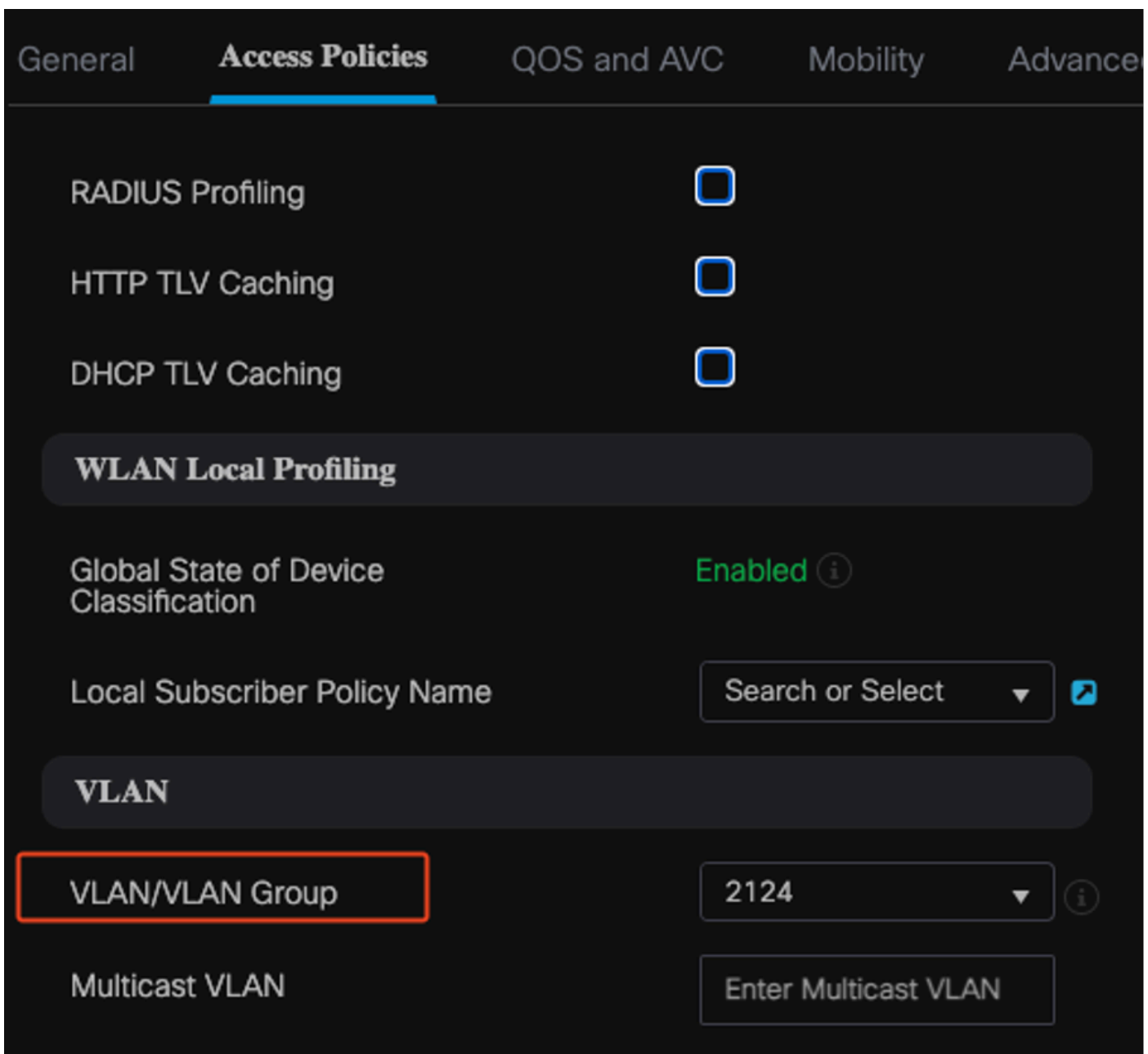
在9800 WLC上创建策略配置文件

完成RADIUS组配置后，继续创建策略配置文件：

1. 导航至配置 > 标签和配置文件 > 策略。
2. 单击Add创建新的策略配置文件。
3. 为策略配置文件选择适当的参数。在本例中，所有设备都处于中心状态，并且实验VLAN用作客户端VLAN。

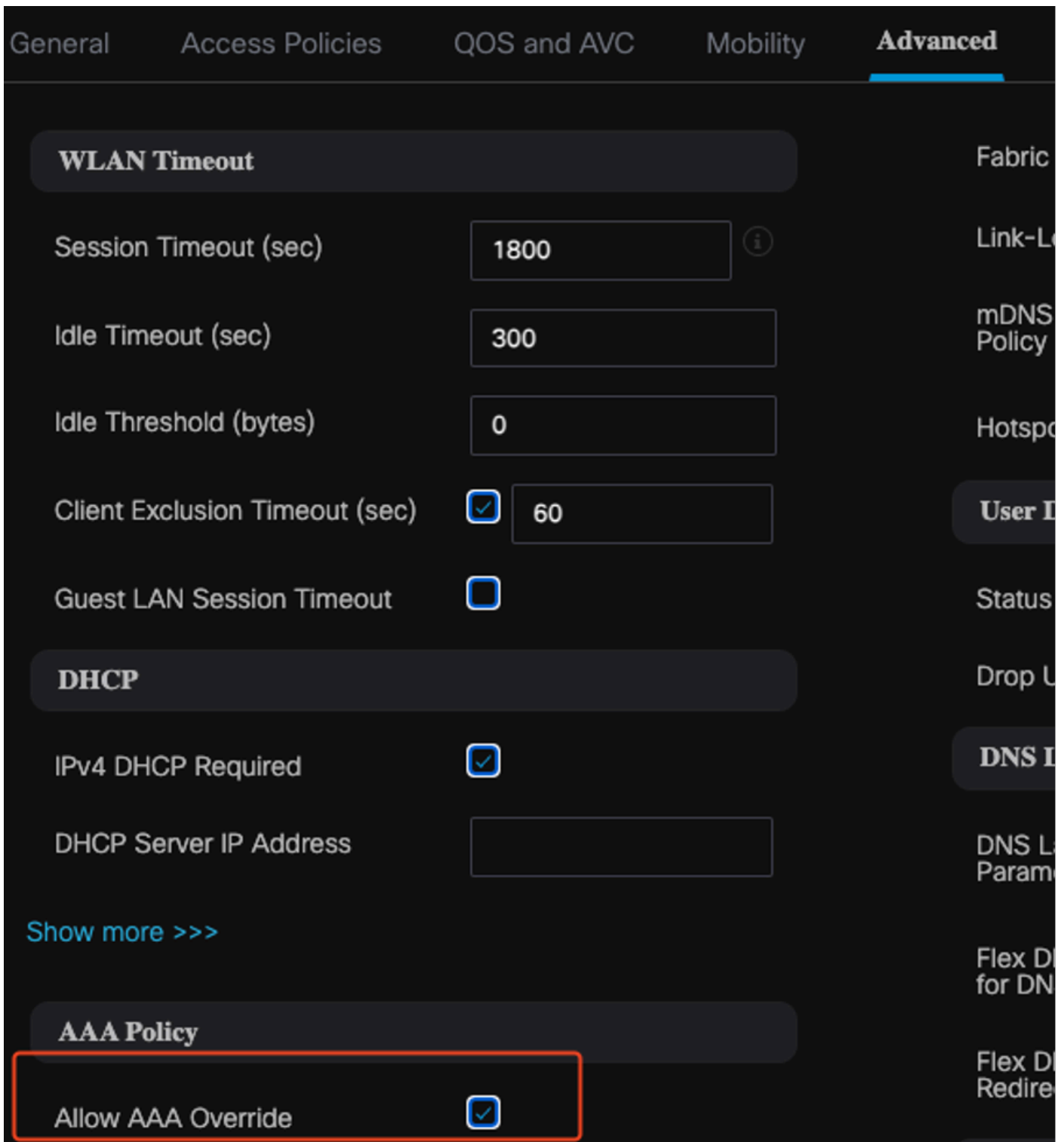


配置策略配置文件



VLAN到策略的映射

配置RADIUS授权时，请确保在策略配置文件设置的高级选项卡中启用AAA Override选项。此设置允许无线局域网控制器将基于RADIUS的授权策略应用于用户和设备。

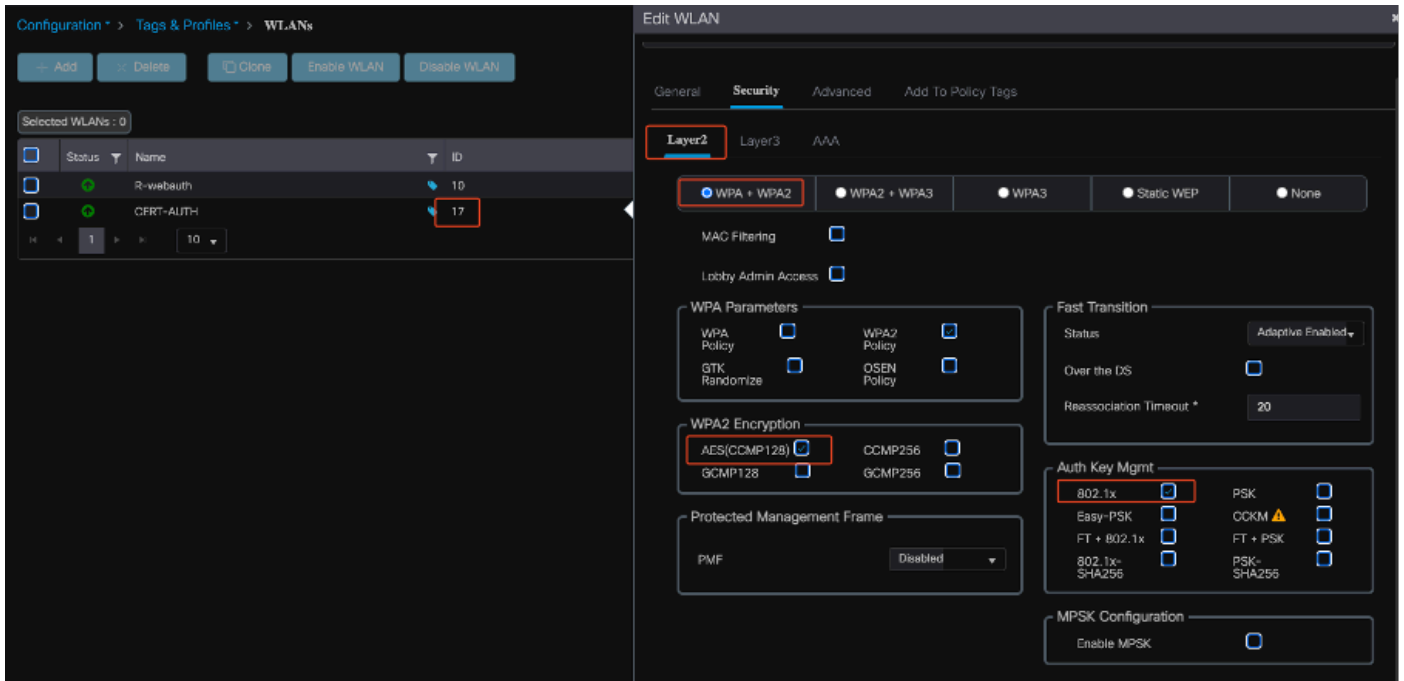


AAA覆盖

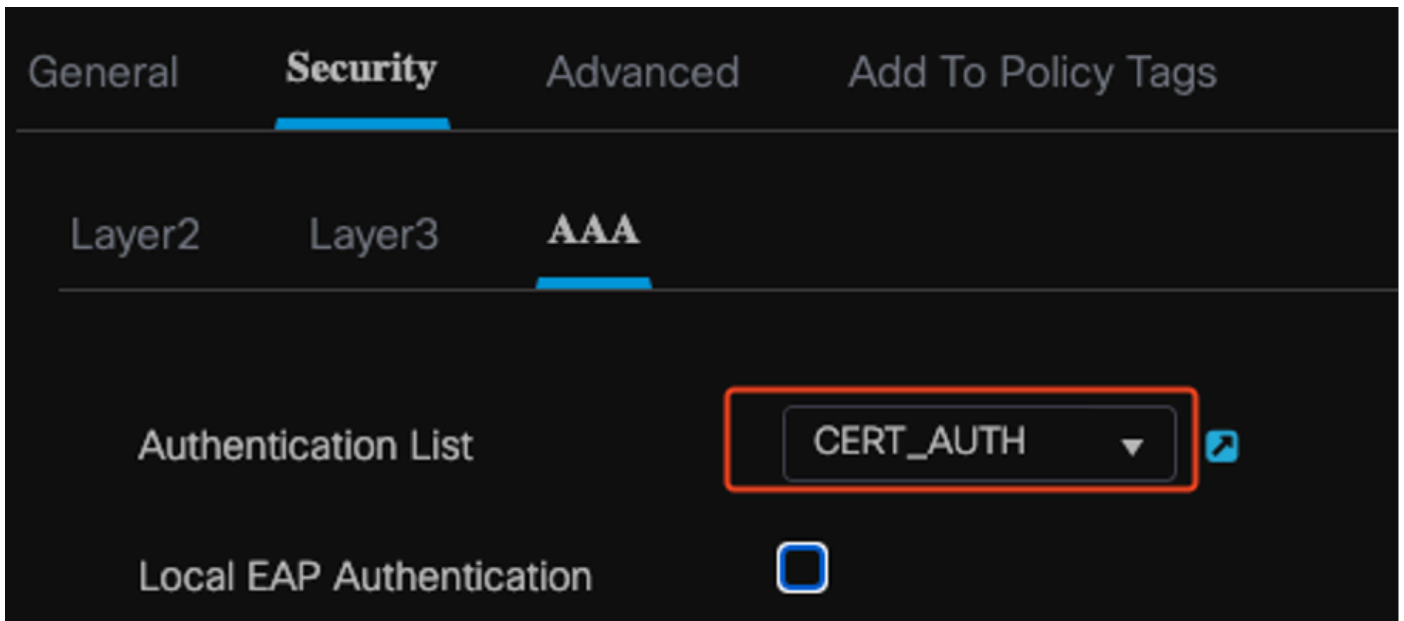
在9800 WLC上创建WLAN

要设置具有802.1x身份验证的新WLAN，请执行以下步骤：

1. 导航到配置>标签和配置文件> WLAN。
2. 单击Add以创建新的WLAN。
3. 选择第2层身份验证设置并启用802.1x身份验证。



WLAN配置文件配置

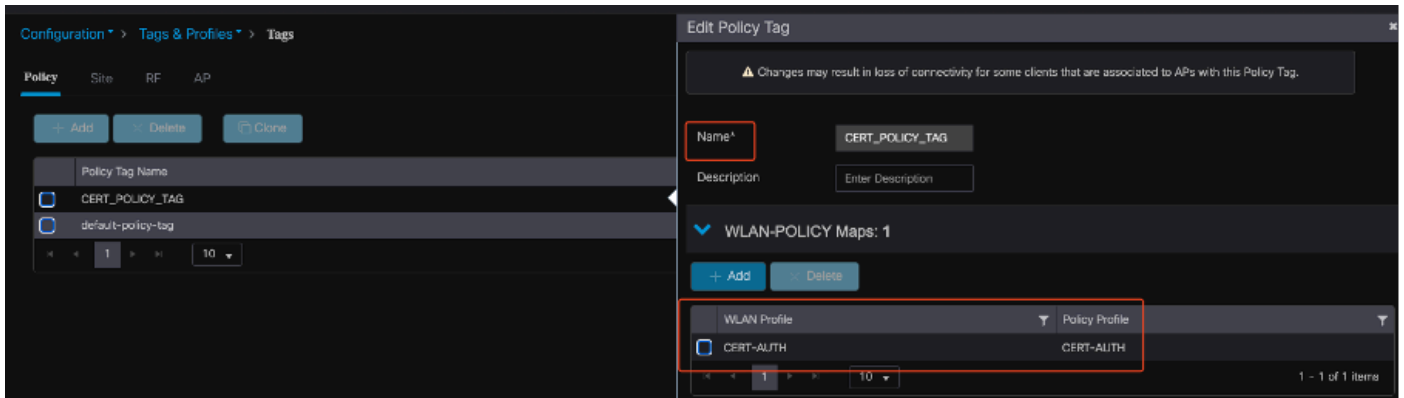


WLAN配置文件到方法列表映射

在9800 WLC上使用策略配置文件映射WLAN

要将WLAN与策略配置文件关联，请执行以下步骤：

1. 导航到配置>标签和配置文件>标签。
2. 单击Add添加新标记。
3. 在WLAN-POLICY部分，将新创建的WLAN映射到相应的策略配置文件。

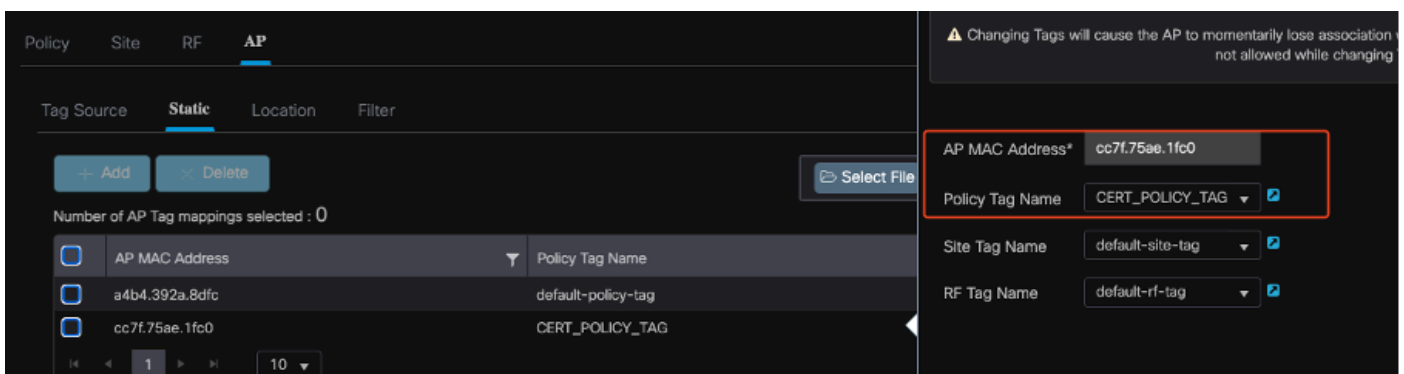


策略标签配置

将策略标记映射到9800 WLC上的接入点

要将策略标记分配给接入点(AP)，请完成以下步骤：

1. 导航到配置>标签和配置文件>标签> AP。
2. 转到AP配置中的Static (静态) 部分。
3. 点击要配置的特定AP。
4. 将您创建的策略标记分配到所选AP。



AP标记分配

安装完成后的WLC运行配置

```

aaa group server radius ISE
  server name ISE3
  ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
  client 10.106.32.31 server-key Cisco!123
!
```

```

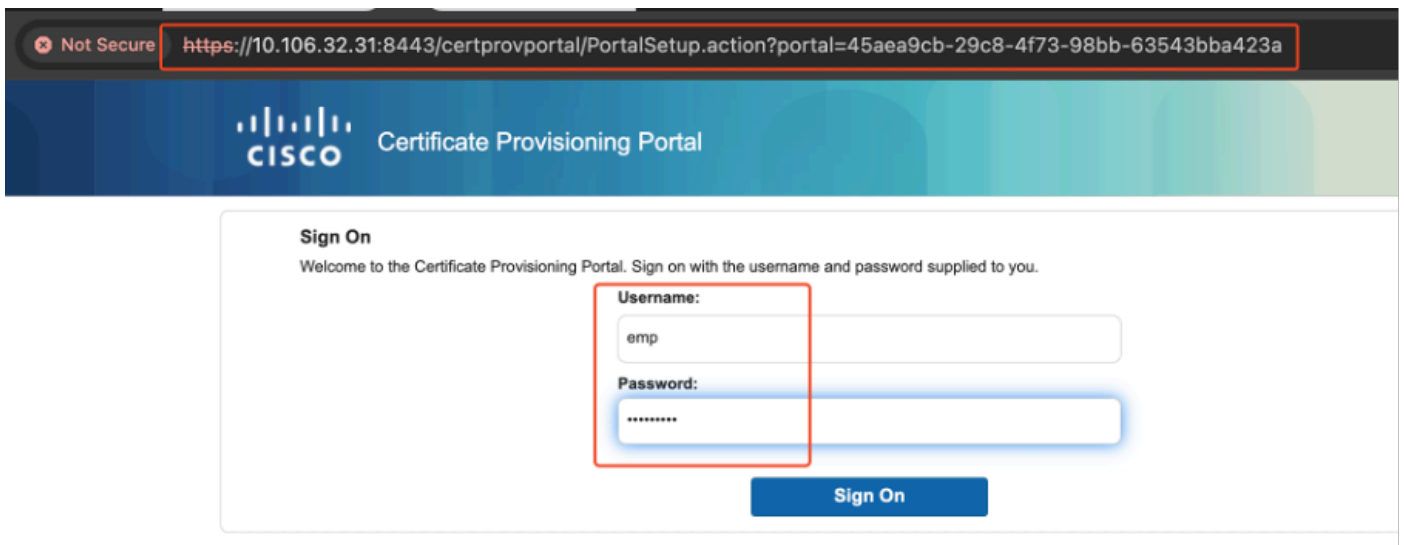
wireless profile policy CERT-AUTH
aaa-override
  ipv4 dhcp required
  vlan 2124
  no shutdown
wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
```

```
security dot1x authentication-list CERT_AUTH
no shutdown
!
wireless tag policy CERT_POLICY_TAG
wlan CERT-AUTH policy CERT-AUTH
```

为用户创建和下载证书

要为用户创建和下载证书，请执行以下步骤：

1. 让用户登录之前设置的证书门户。



访问证书门户

2. 接受可接受的使用政策(AUP)。然后，ISE显示用于生成证书的页面。

3. 选择Generate a single certificate(without a certificate signing request)。

Certificate Provisioning

I want to: *

Generate a single certificate (without a certificate...) 1

Common Name (CN): *

emp 2

MAC Address: *

242f.d0da.a563 3

Choose Certificate Template: *

EAP_Authentication_Certificate_Template 4

Description:

Certificate Download Format: *

PKCS12 format, including certificate chain (...) 5

Certificate Password: *

Enter password to download and view/install the certificate

Confirm Password: *

Generate

Reset

生成证书

要通过证书调配门户生成证书，请确保填写以下必填字段：

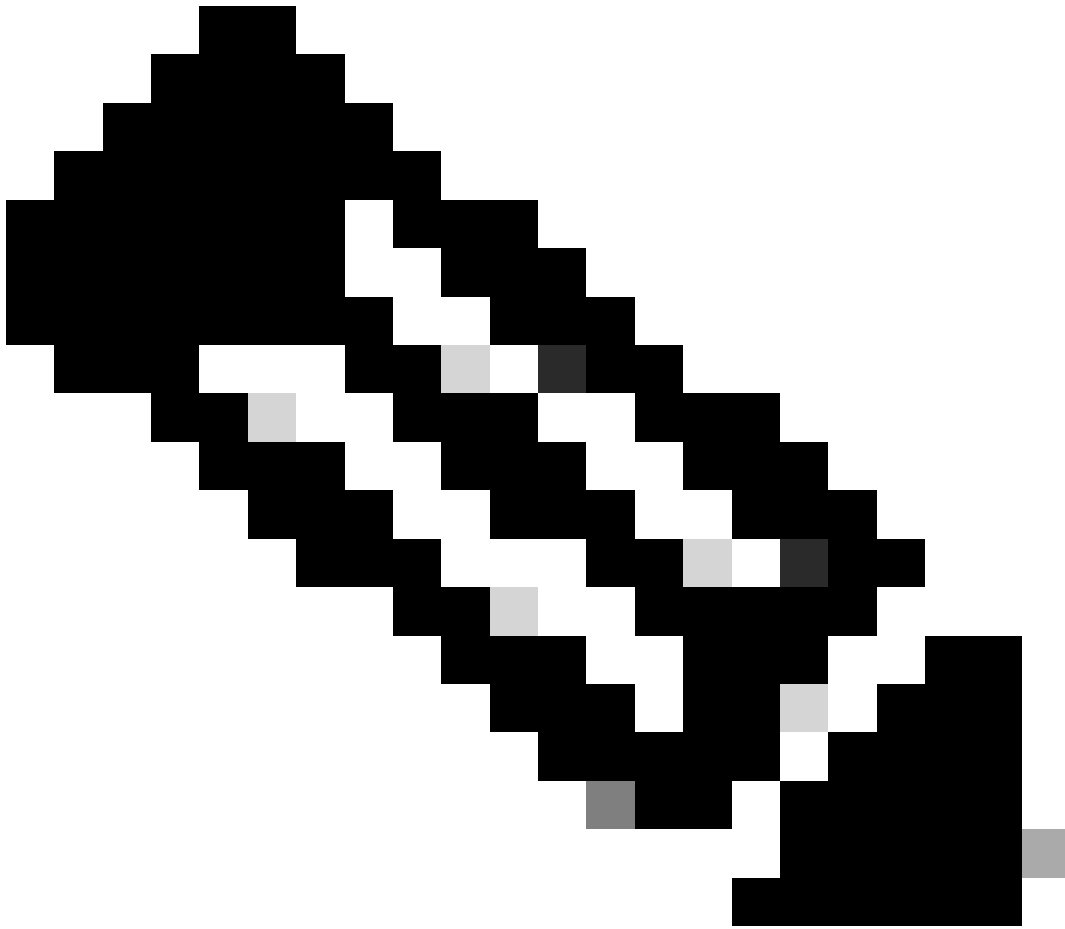
- CN:身份验证服务器使用客户端证书中Common Name字段中显示的值对用户进行身份验证。在Common Name字段中，输入用户名（用于登录证书调配门户）。
- MAC 地址：主题备用名称(SAN)是X.509扩展，允许将各种值与安全证书关联。思科ISE版本2.0仅支持MAC地址。因此，在SAN/MAC地址字段中。
 - 证书模板:证书模板定义CA在验证请求和颁发证书时使用的字段集。公用名(CN)等字段用于验证请求（CN必须与用户名匹配）。CA在颁发证书时使用其他字段。
- 证书密码:您需要证书密码来保护您的证书。必须提供证书密码才能查看证书的内容并在设备上导入证书。
- 您的密码必须符合以下规则：
- 密码必须至少包含1个大写字母、1个小写字母和1个数字

- 。 密码的长度必须介于8到15个字符之间
- 。 允许的字符包括A-Z、a-z、0-9、_、#

填写所有字段后，选择Generate以创建和下载证书。

Windows 10计算机上的证书安装

要在Windows 10计算机上安装证书，请按以下步骤打开Microsoft管理控制台(MMC):

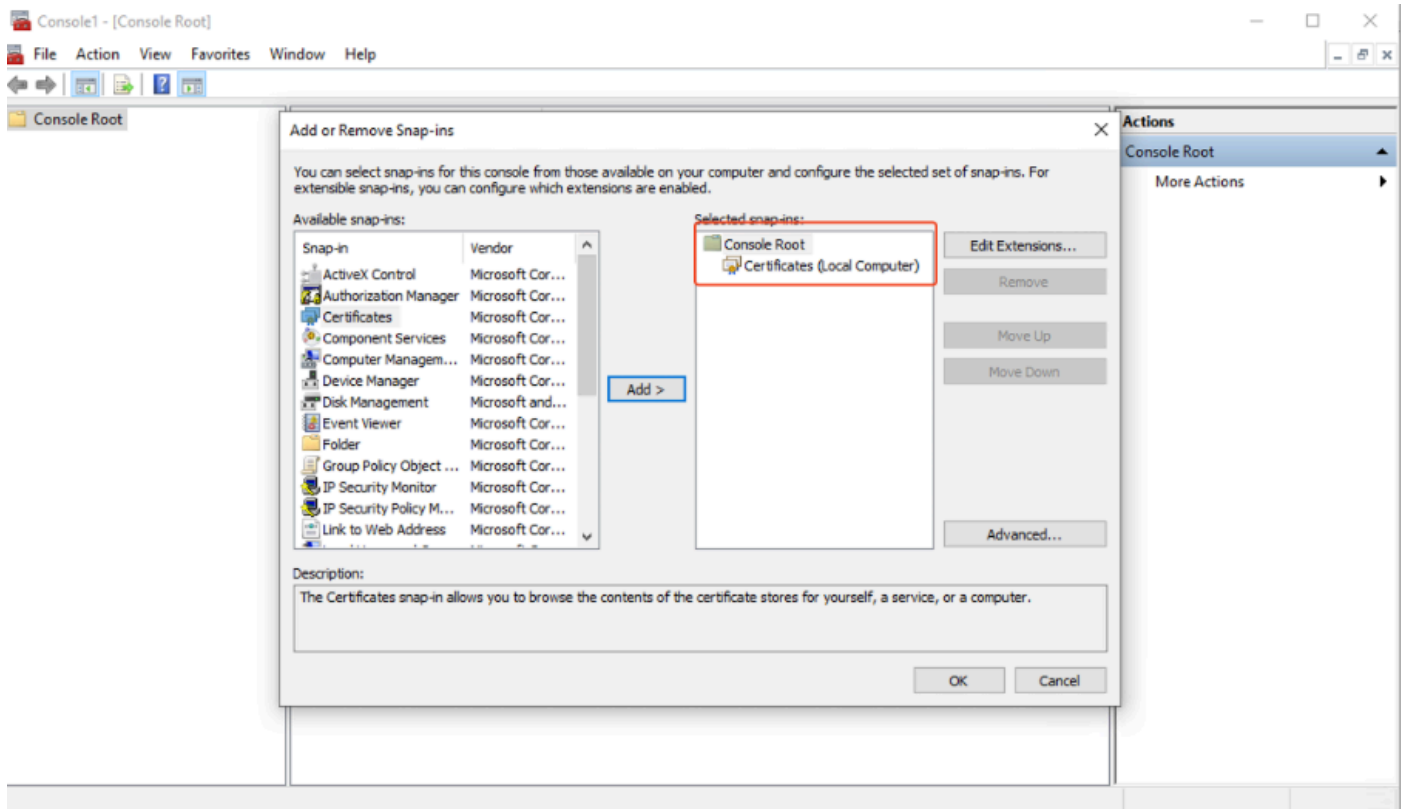


注意：这些说明可能因您的Windows设置而异，因此建议参阅Microsoft文档以了解具体的详细信息。

-
1. 单击Start，然后单击Run。
 2. 在“Run（运行）”框中键入mmc，然后按Enter。Microsoft管理控制台打开。
 3. 添加证书管理单元：
 4. 转到文件>添加/删除管理单元。
 5. 选择Add，然后选择Certificates，然后单击Add。

6. 选择Computer Account，然后选择Local Computer，然后单击Finish。

这些步骤允许您管理本地计算机上的证书。




Windows MMC控制台

步骤1.导入证书：

- 1.1.单击菜单中的Action。
- 1.2.转到所有任务，然后选择导入。
- 1.3.按照提示查找并选择计算机上存储的证书文件。



←  Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\admin\Desktop\emp-2025-01-06_08-30-59\emp_C4-E9-0

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX, .P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

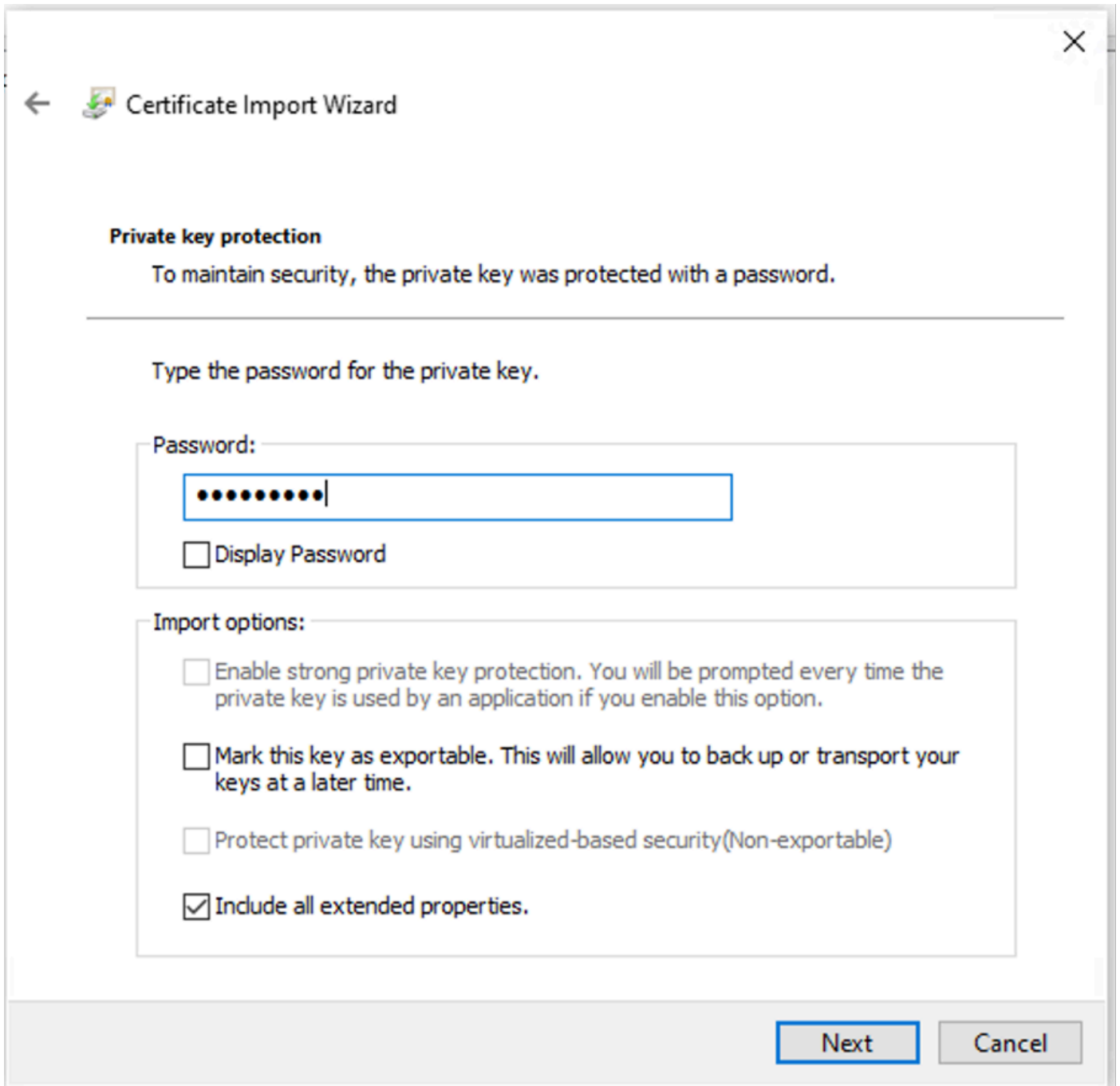
Microsoft Serialized Certificate Store (.SST)

Next

Cancel

导入证书

在证书导入过程中，系统会提示您输入在门户上生成证书时创建的密码。请确保准确输入此密码以成功导入证书并将其安装在计算机上。

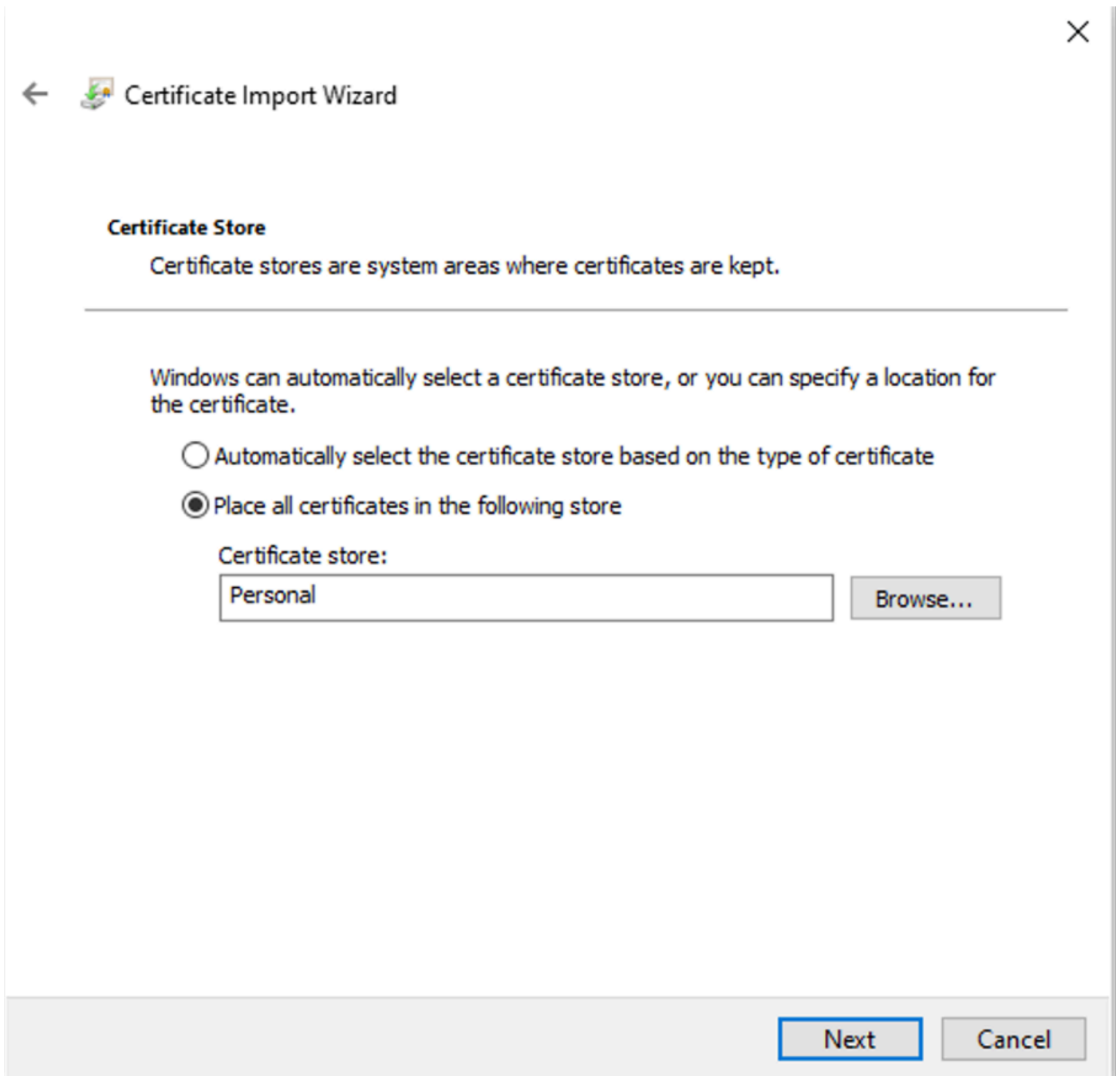


输入证书密码

步骤2.将证书移动到适当的文件夹：

- 2.1.打开Microsoft Management Console(MMC)，然后导航到Certificates(Local Computer)> Personal文件夹。
- 2.2.检查证书并确定其类型（例如，根CA、中间CA或个人）。
- 2.3.将每个证书移动到相应的存储区：
- 2.4.根CA证书：转到受信任的根证书颁发机构。
- 2.5.中间CA证书：转到中级证书颁发机构。

2.6.个人证明：离开Personal文件夹。



在个人文件夹中存储证书

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
Certificate Services Endpoint Sub CA - ise3genvc	Certificate Services Node CA - ise3genvc	1/3/2035	<All>	EndpointSubCA	
Certificate Services Node CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<All>	certificate_nodeCA	
Certificate Services Root CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<All>	certificate	
emp	Certificate Services Endpoint Sub CA - ise3genvc	1/6/2027	Client Authentication	emp_C4-E9-0A-00-...	
ise3genvc.lab.local	ise3genvc.lab.local	1/3/2027	Server Authentication, Client Authentication	Self-Signed	

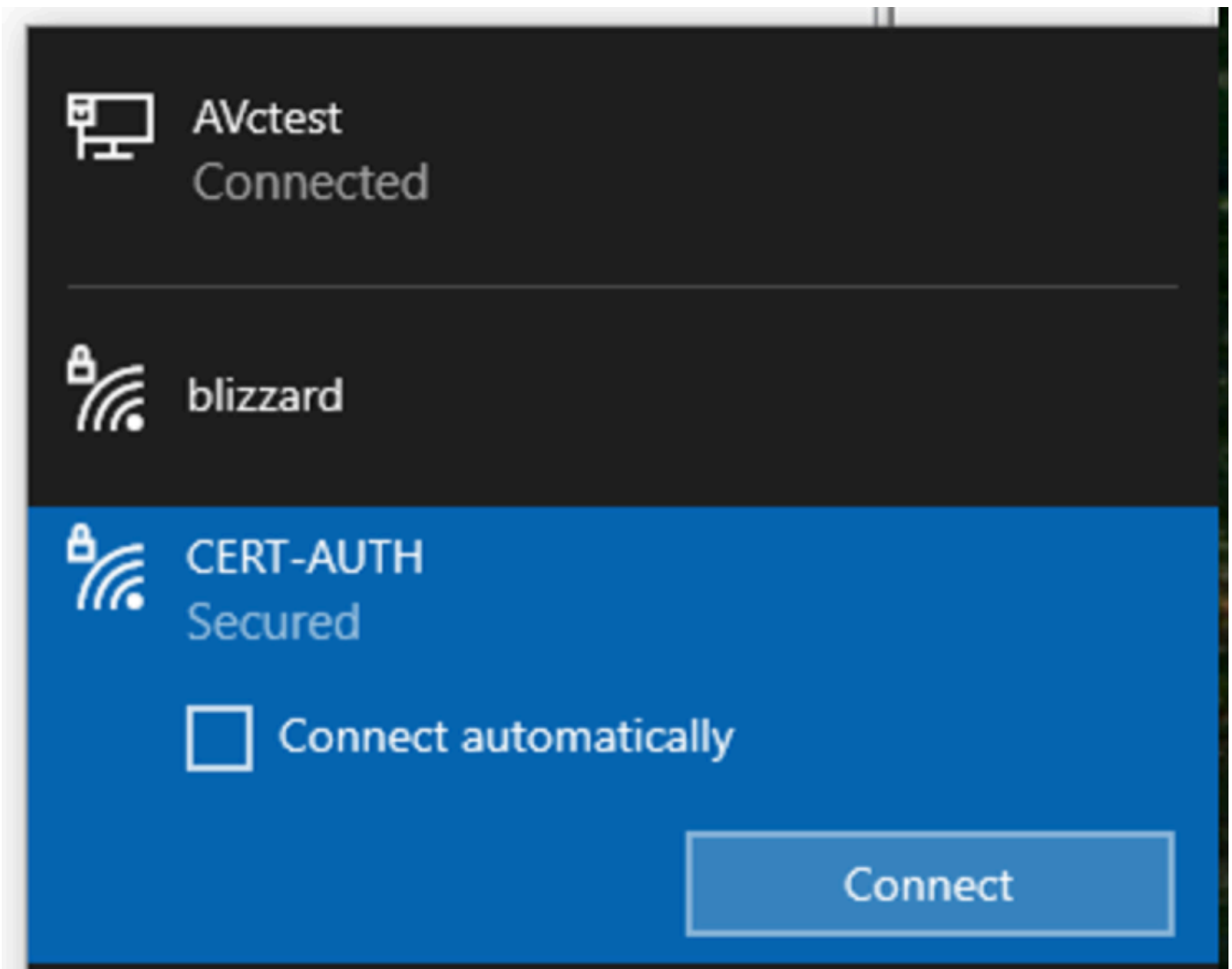
在其存储中移动证书

连接Windows计算机

将证书移动到正确的存储区后，请使用以下步骤连接到WLAN:

1. 单击系统托盘中的network图标查看可用的无线网络。

2. 查找并单击要连接的WLAN的名称。
3. 单击Connect并继续执行任何其他提示，以使用证书进行身份验证来完成连接过程。



连接到无线网络

在与WLAN的连接过程中出现提示时，选择Connect using a certificate(使用证书进行连接)选项。



CERT-AUTH
Secured

Enter your user name and password

Connect using a certificate

OK

Cancel

使用证书作为凭证

这使您能够使用证书成功连接到无线网络。

```
C:\>netsh wlan show interface
```

```
There is 1 interface on the system:
```

```
Name : Wi-Fi 3
Description : TP-Link Wireless USB Adapter
GUID : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
Physical address : 24:2f:d0:da:a5:63
State : connected
SSID : CERT-AUTH
BSSID : a4:88:73:9e:8d:af
Network type : Infrastructure
Radio type : 802.11ac
Authentication : WPA2-Enterprise
Cipher : CCMP
Connection mode : Profile
Channel : 36
Receive rate (Mbps) : 360
Transmit rate (Mbps) : 360
Signal : 100%
Profile : CERT-AUTH
```

```
Hosted network status : Not available
```

```
C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
```

```
EAP type : Microsoft: Smart Card or other certificate
```

验证无线配置文件

验证

验证WLC是否正在广播WLAN:

```
<#root>
```

```
POD6_9800#show wlan summ
```

```
Number of WLANs: 2
```

```
ID Profile Name SSID Status Security
```

```
-----
```

```
17
```

```
CERT-AUTH
```

```
CERT-AUTH
```

```
UP [WPA2][802.1x][AES]
```

验证WLC上的AP是否打开 :

```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-----
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

确保AP正在广播WLAN:

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
-----
17 a488.739e.8da0
```

```
POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
-----
17
a488.739e.8daf
```

使用EAP-TLS连接的客户端 :

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----
242f.d0da.a563 AP1 WLAN

17
IP Learn 11ac

Dot1x
Local

POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
Wireless LAN Network Name (SSID): CERT-AUTH

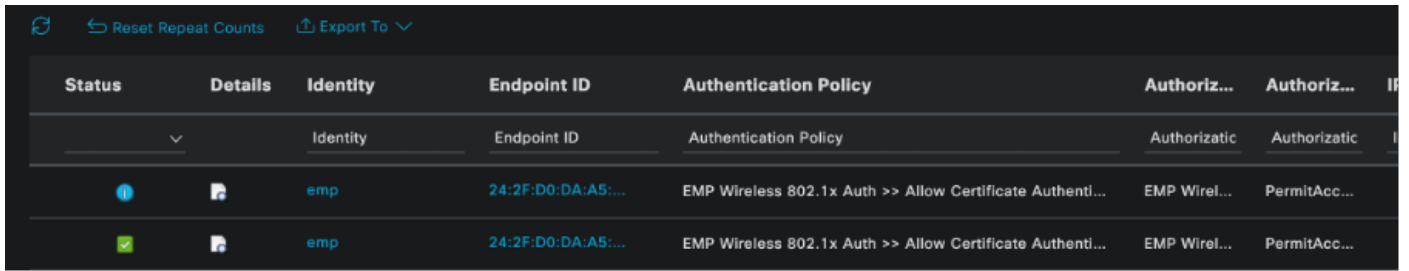
BSSID : a488.739e.8daf

EAP Type : EAP-TLS

VLAN : 2124
Multicast VLAN : 0
```

VLAN : 2124

Cisco Radius ISE实时日志 :



The screenshot displays a table of Cisco ISE Radius logs. The table has columns for Status, Details, Identity, Endpoint ID, Authentication Policy, and Authorization. Two entries are visible, both for the identity 'emp' and endpoint ID '24:2F:D0:DA:A5:...'. The first entry has a status of 'i' (info) and the second has a status of '✓' (success). Both entries show the authentication policy 'EMP Wireless 802.1x Auth >> Allow Certificate Authenti...' and authorization 'EMP Wire...' and 'PermitAcc...'.

Status	Details	Identity	Endpoint ID	Authentication Policy	Authoriz...	Authoriz...
i		emp	24:2F:D0:DA:A5:...	EMP Wireless 802.1x Auth >> Allow Certificate Authenti...	EMP Wire...	PermitAcc...
✓		emp	24:2F:D0:DA:A5:...	EMP Wireless 802.1x Auth >> Allow Certificate Authenti...	EMP Wire...	PermitAcc...

ISE Radius实时日志

详细身份验证类型 :

Authentication Details

Source Timestamp	2025-01-08 11:58:21.055
Received Timestamp	2025-01-08 11:58:21.055
Policy Server	ise3genvc
Event	5200 Authentication succeeded
Username	emp
Endpoint Id	24:2F:D0:DA:A5:63
Calling Station Id	24-2f-d0-da-a5-63
Endpoint Profile	TP-LINK-Device
Identity Group	User Identity Groups:Employee,Profiled
Audit Session Id	4D084E0A0000007E46F0C6F7
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	lab-9800
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.78.8.77
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccess
Security Group	Employees

ISE详细日志

显示EAP-TLS数据包的WLC EPC捕获：

No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLV1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLV1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLV1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLV1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

显示EAP事务的WLC捕获

- 数据包编号87对应于文档开头所述的EAP-TLS流中的步骤8。
- 数据包编号115对应于文档开头所述的EAP-TLS流中的步骤9。
- 数据包编号118对应于文档开头所述的EAP-TLS流中的步骤10。

显示客户端连接的无线活动(RA)跟踪：此RA跟踪经过过滤，可显示身份验证事务的一些相关行。

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655] (调试) 发送加密DTLS消息。目的IP 10.78.8.78[5256]，长499

2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (信息) RADIUS发送访问请求到10.106.33.23 1812 id 0/25,len 390

2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655] (信息) 从id 1812/25 10.106.33.23 0、Access-Challenges、len 123接收的RADIUS

2025/01/08 11 58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP，负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]收到的EAPOL数据包 — 版本1,EAPOL类型EAP，负载长度204,EAP类型= EAP-TLS

2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (信息) RADIUS发送访问请求到10.106.33.23 1812 id 0/26,len 663

2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655] (信息) 从id 1812/26 10.106.33.23 0、Access-Challenges、len 1135接收的RADIUS

2025/01/08 11 58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP，负载长度1012,EAP类型= EAP-TLS

2025/01/08 11 58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]已收到EAPOL数据包 — 版本1,EAPOL类型EAP，负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (信息) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/27, len 465

2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655] (信息) 从id 1812/27 10.106.33.23 0、Access-Challenges、len 1131接收的RADIUS

2025/01/08 11 58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP，负载长度1008,EAP类型= EAP-TLS

2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]已收到EAPOL数据包 — 版本1,EAPOL类型EAP , 负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (信息) RADIUS发送访问请求到10.106.33.23 1812 id 0/28,len 465

2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655] (信息) 从id 1812/28 10.106.33.23 0、Access-Challens、len 275接收的RADIUS

2025/01/08 11 58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP , 负载长度158,EAP类型= EAP-TLS

2025/01/08 11 58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]已收到EAPOL数据包 — 版本1,EAPOL类型EAP , 负载长度1492,EAP类型= EAP-TLS

2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (信息) RADIUS发送访问请求到10.106.33.23 1812 id 0/29,len 1961

2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655] (信息) 从id 1812/29 10.106.33.23 0、Access-Challens、len 123接收的RADIUS

2025/01/08 11 58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP , 负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]已收到EAPOL数据包 — 版本1,EAPOL类型EAP , 负载长度1492,EAP类型= EAP-TLS

2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (信息) RADIUS发送访问请求到10.106.33.23 1812 id 0/30,len 1961

2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655] (信息) 从id 1812/30 10.106.33.23 0、Access-Challens、len 123接收的RADIUS

2025/01/08 11 58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP , 负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]已收到EAPOL数据包 — 版本1,EAPOL类型EAP , 负载长度1492,EAP类型= EAP-TLS

2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (信息) RADIUS发送访问请求到10.106.33.23 1812 id 0/31,len 1961

2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655] (信息) 从id 1812/31 10.106.33.23 0、Access-Challens、len 123接收的RADIUS

2025/01/08 11 58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP , 负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]收到的EAPOL数据包 — 版本1,EAPOL类型EAP , 负载长度247,EAP类型= EAP-TLS

2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (信息) RADIUS发送访问请求到10.106.33.23 1812 id 0/32,len 706

2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655] (信息) 从id 1812/32

10.106.33.23 0、Access-Challenges、len 174接收的RADIUS

2025/01/08 11 58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]发送的EAPOL数据包 — 版本3,EAPOL类型EAP , 负载长度57,EAP类型= EAP-TLS

2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]收到的EAPOL数据包 — 版本1,EAPOL类型EAP , 负载长度6,EAP类型= EAP-TLS

2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (信息) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/33, len 465

2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (信息) 从id 1812/33 10.106.33.23 0、Access-Accept、len 324接收的RADIUS

2025/01/08 11 58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (信息) [242f.d0da.a563 capwap_90800005]已引发eap方法EAP-TLS的身份更新事件

故障排除

除典型的无线802.1x故障排除步骤外，没有针对此问题的具体故障排除步骤：

1. 执行客户端RA跟踪调试以检查身份验证过程。
2. 执行WLC EPC捕获以检查客户端、WLC和RADIUS服务器之间的数据包。
3. 检查ISE实时日志以验证请求是否与正确的策略匹配。
4. 在Windows终端上验证证书安装正确且存在整个信任链。

参考

- [证书调配门户常见问题解答，版本3.2](#)
- [了解ISE内部证书颁发机构服务](#)
- [了解并配置WLC和ISE的EAP-TLS](#)

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）。