

# 了解并配置EAP-TLS与Mobility Express和ISE

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[EAP-TLS流](#)

[EAP-TLS流中的步骤](#)

[配置](#)

[Cisco Mobility Express](#)

[采用Cisco Mobility Express的ISE](#)

[EAP-TLS设置](#)

[ISE上的Mobility Express设置](#)

[ISE上的信任证书](#)

[EAP-TLS的客户端](#)

[在客户端 \( Windows桌面 \) 上下载用户证书](#)

[EAP-TLS的无线配置文件](#)

[验证](#)

[故障排除](#)

## 简介

本文档介绍如何在Mobility Express控制器中设置具有802.1x安全性的无线局域网(WLAN)。本文档还特别说明了可扩展身份验证协议(EAP) — 传输层安全(TLS)的使用。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Mobility Express初始设置
- 802.1x身份验证过程
- 证书

### 使用的组件

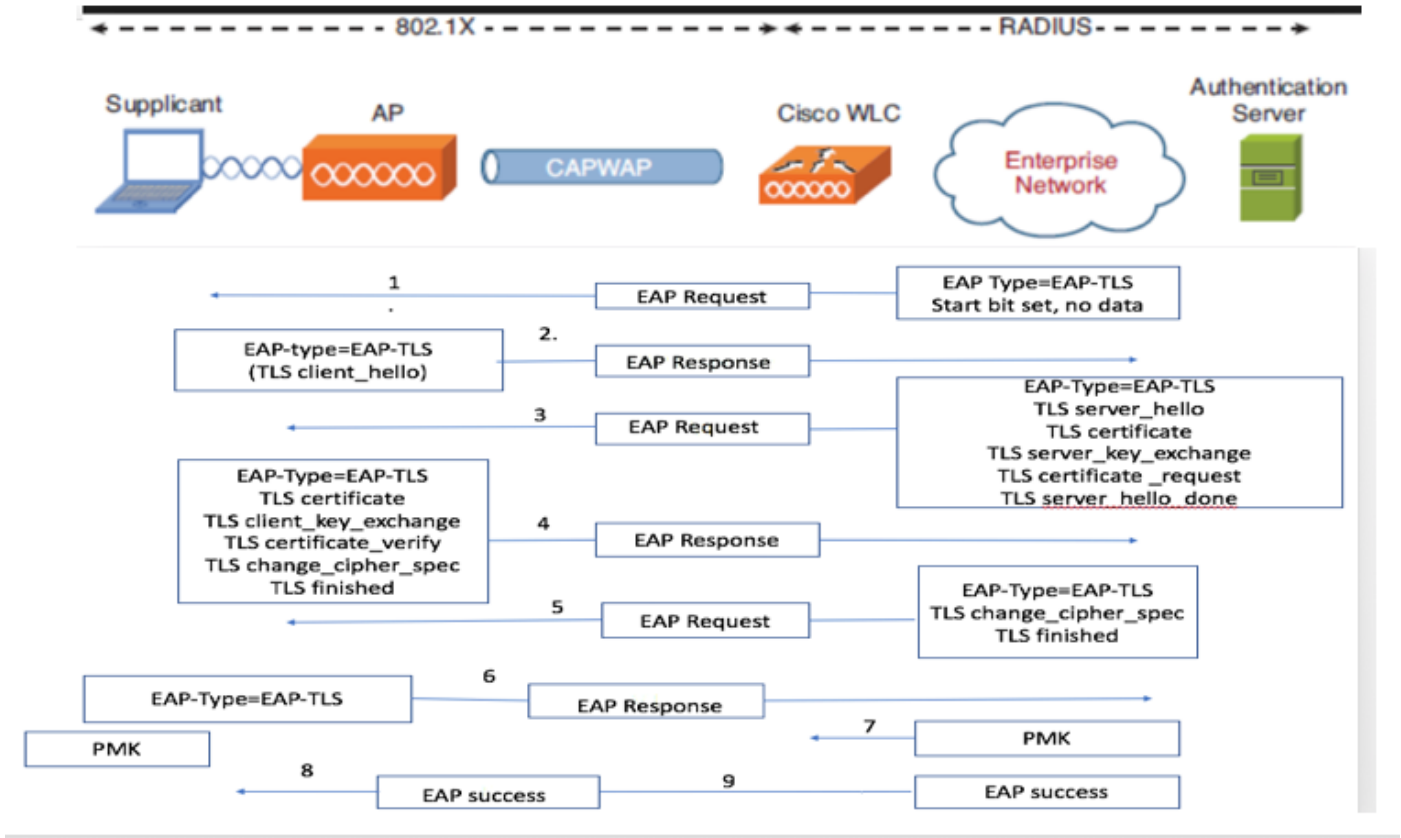
本文档中的信息基于以下软件和硬件版本：

- WLC 5508版本8.5
- 身份服务引擎(ISE)版本2.1

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

### EAP-TLS流



### EAP-TLS流中的步骤

1. 无线客户端与接入点(AP)关联。
2. AP不允许客户端此时发送任何数据并发送身份验证请求。
3. 请求方随后使用EAP响应身份进行响应。然后，WLC将用户ID信息传达给身份验证服务器。
4. RADIUS服务器使用EAP-TLS启动数据包响应客户端。EAP-TLS会话此时开始。
5. 对等体将EAP-Response发回包含“client\_hello”握手消息的身份验证服务器，该握手消息为NULL设置。
6. 身份验证服务器以包含以下内容的Access-challenge数据包作出响应：

```
TLS server_hello  
handshake message  
certificate  
server_key_exchange  
certificate request  
server_hello_done.
```

7. 客户端以EAP-Response消息响应，该消息包含：

Certificate → Server can validate to verify that it is trusted.

client\_key\_exchange

certificate\_verify → Verifies the server is trusted

change\_cipher\_spec

TLS finished

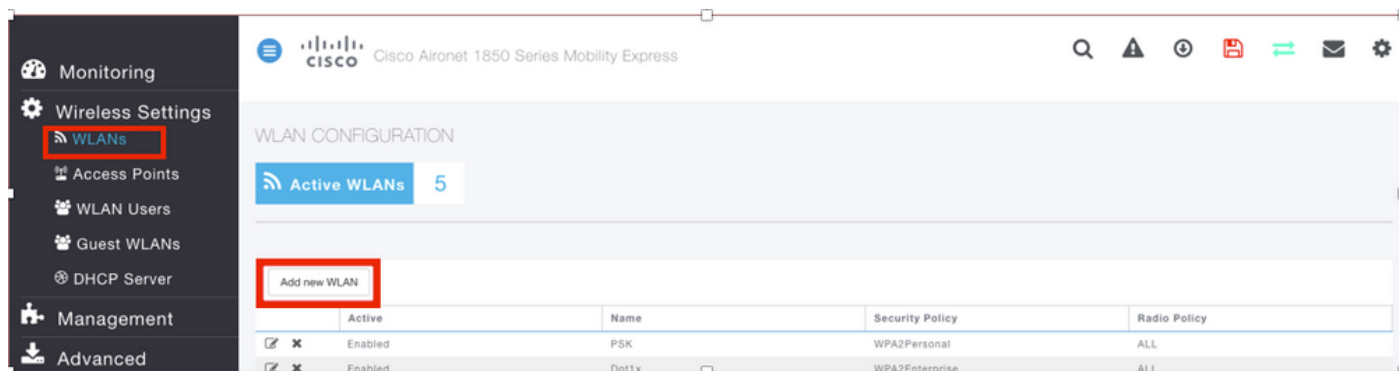
8. 在客户端成功进行身份验证后，RADIUS服务器以访问质询（包含“change\_cipher\_spec”和握手完成消息）作出响应。收到此消息后，客户端验证散列以验证RADIUS服务器。在TLS握手期间，新加密密钥会从密钥中动态派生。

9. 此时，启用EAP-TLS的无线客户端可以访问无线网络。

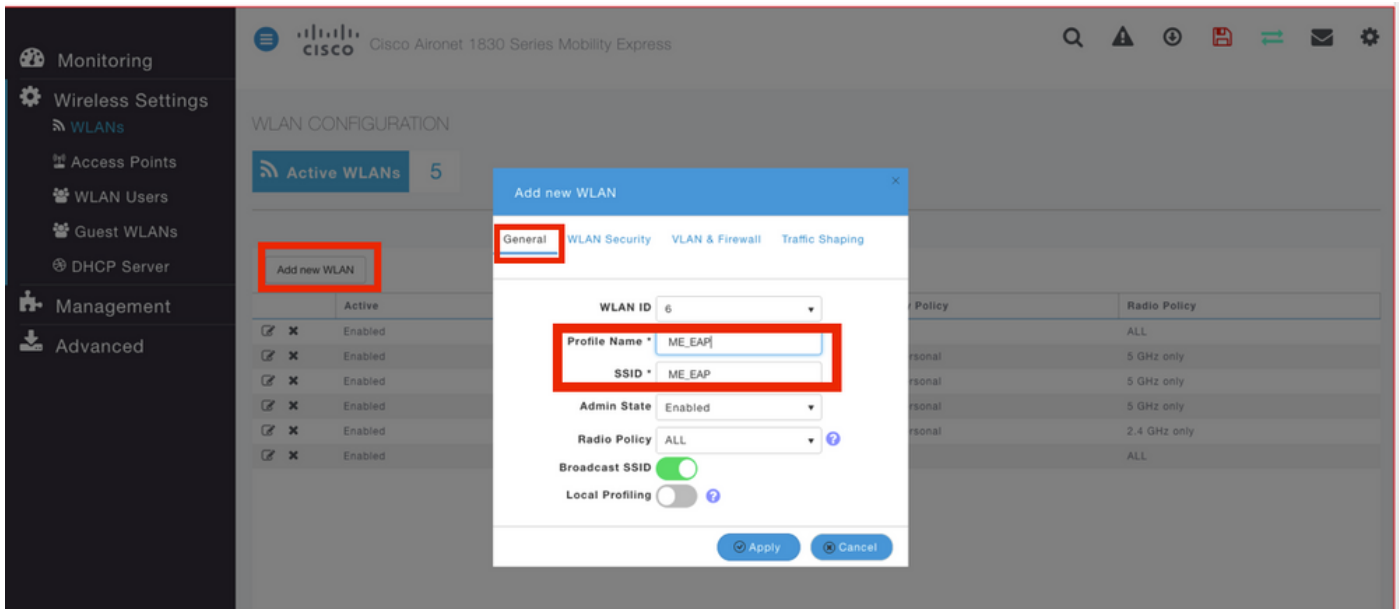
## 配置

### Cisco Mobility Express

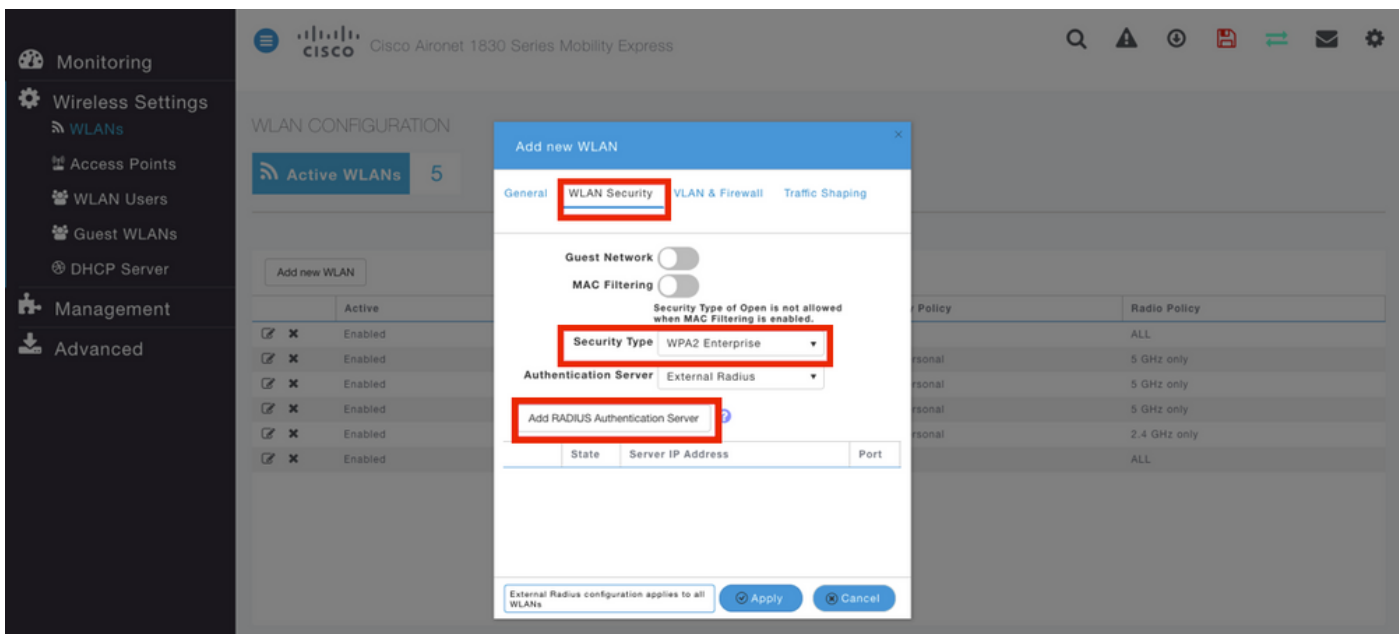
步骤1. 第一步是在Mobility Express上创建WLAN。要创建WLAN，请导航到WLAN > Add new WLAN(如图所示)。



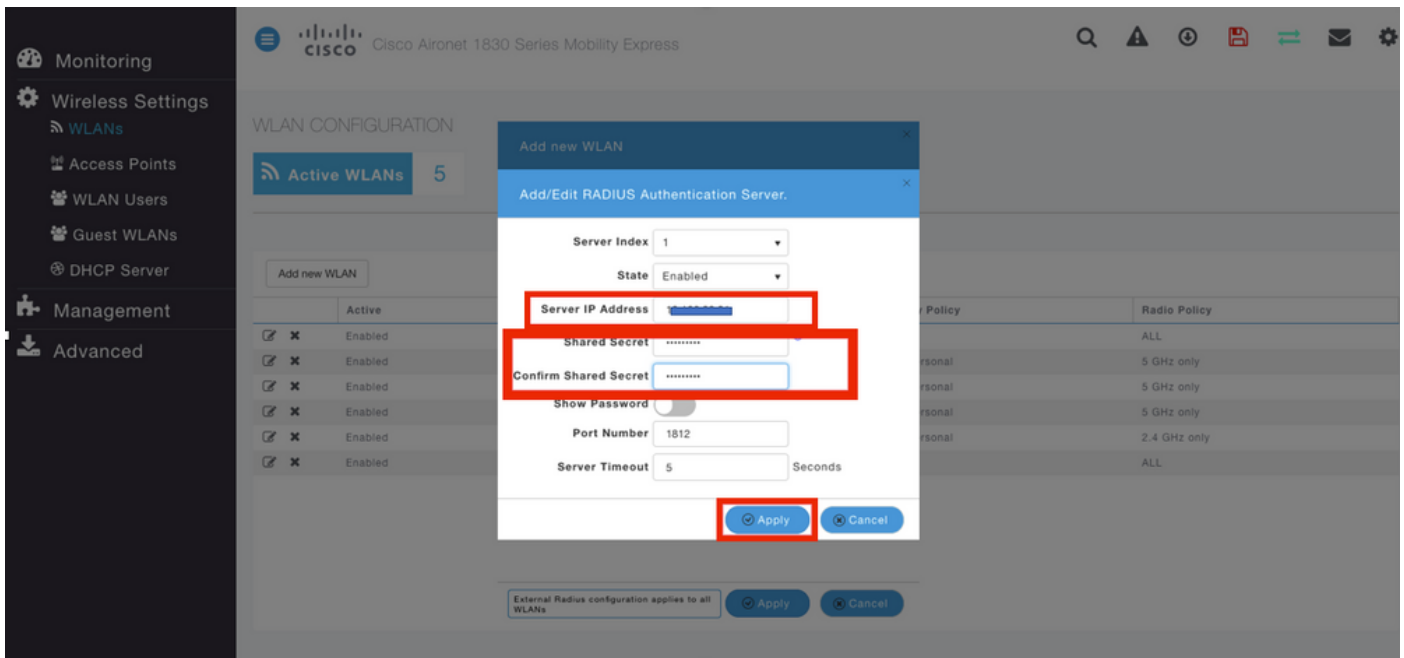
步骤2. 单击“添加新WLAN”后，将出现一个新弹出窗口。要创建配置文件名称，请导航至Add new WLAN > General(如图所示)。



步骤3.将身份验证类型配置为802.1x的WPA企业版，并在“添加新WLAN > WLAN安全”下配置RADIUS服务器，如图所示。



步骤4.单击Add RADIUS Authentication Server并提供RADIUS服务器的IP地址和Shared Secret，它必须与ISE上已配置的完全匹配，然后单击Apply，如图所示。



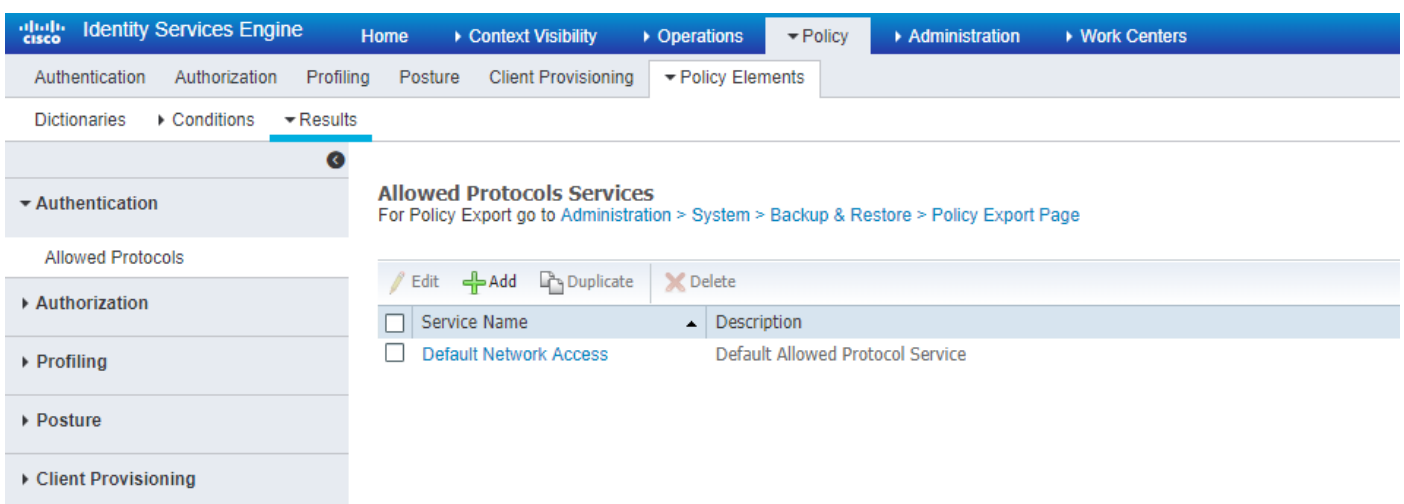
## 采用Cisco Mobility Express的ISE

### EAP-TLS设置

要构建策略，您需要创建允许的协议列表以在策略中使用。由于写入了dot1x策略，因此请根据策略的配置方式指定允许的EAP类型。

如果使用默认值，则允许大多数EAP类型进行身份验证，如果需要锁定对特定EAP类型的访问，则可能不是首选的。

步骤1. 导航至Policy > Policy Elements > Results > Authentication > Allowed Protocols，然后单击Add，如图所示。



步骤2. 在此允许的协议列表中，可以输入列表的名称。在这种情况下，Allow EAP-TLS（允许EAP-TLS）框被选中，其他框被取消选中，如图所示。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allowed Protocols Services List > New Allowed Protocols Service

**Allowed Protocols**

Name

Description

Allowed Protocols

**Authentication Bypass**

Process Host Lookup

**Authentication Protocols**

Allow PAP/ASCII

Allow CHAP

Allow MS-CHAPv1

Allow MS-CHAPv2

Allow EAP-MD5

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Enable Stateless Session Resume

Session ticket time to live

Proactive session ticket update will occur after  % of Time To Live has expired

Allow LEAP

Allow PEAP

**PEAP Inner Methods**

Allow EAP-MS-CHAPv2

Allow Password Change Retries  (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries  (Valid Range 0 to 3)

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Require cryptobinding TLV

## ISE上的Mobility Express设置

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

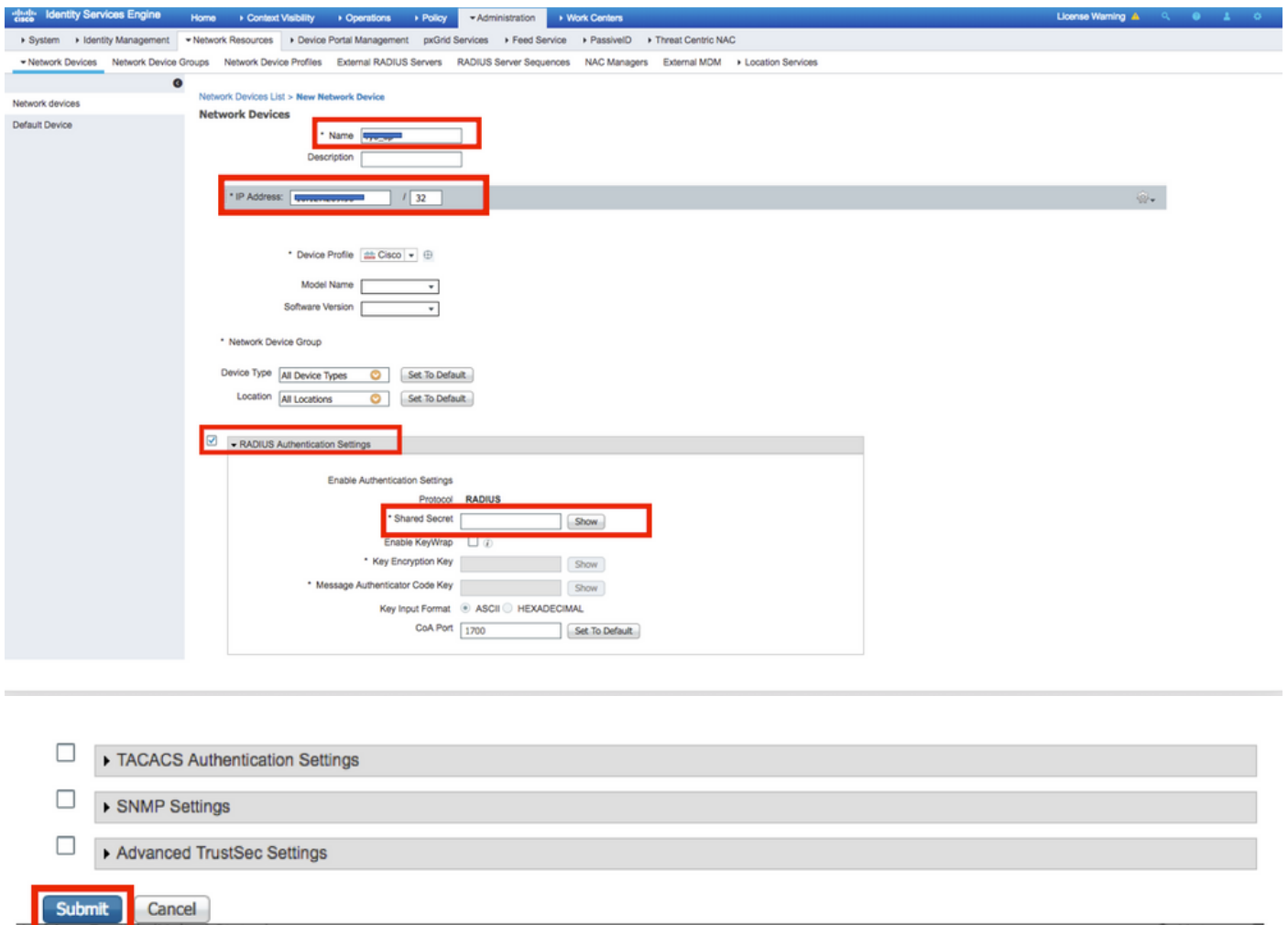
Network Devices

Selected 0 | Total 1

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
------	---------	--------------	----------	------	-------------

步骤2.输入图中所示的信息。

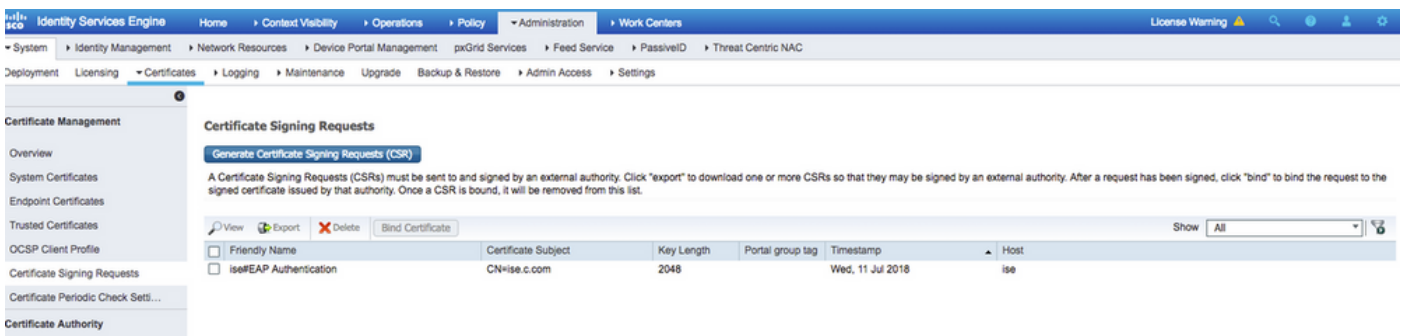


## ISE上的信任证书

步骤1.导航至Administration > System > Certificates > Certificate Management > Trusted certificates.

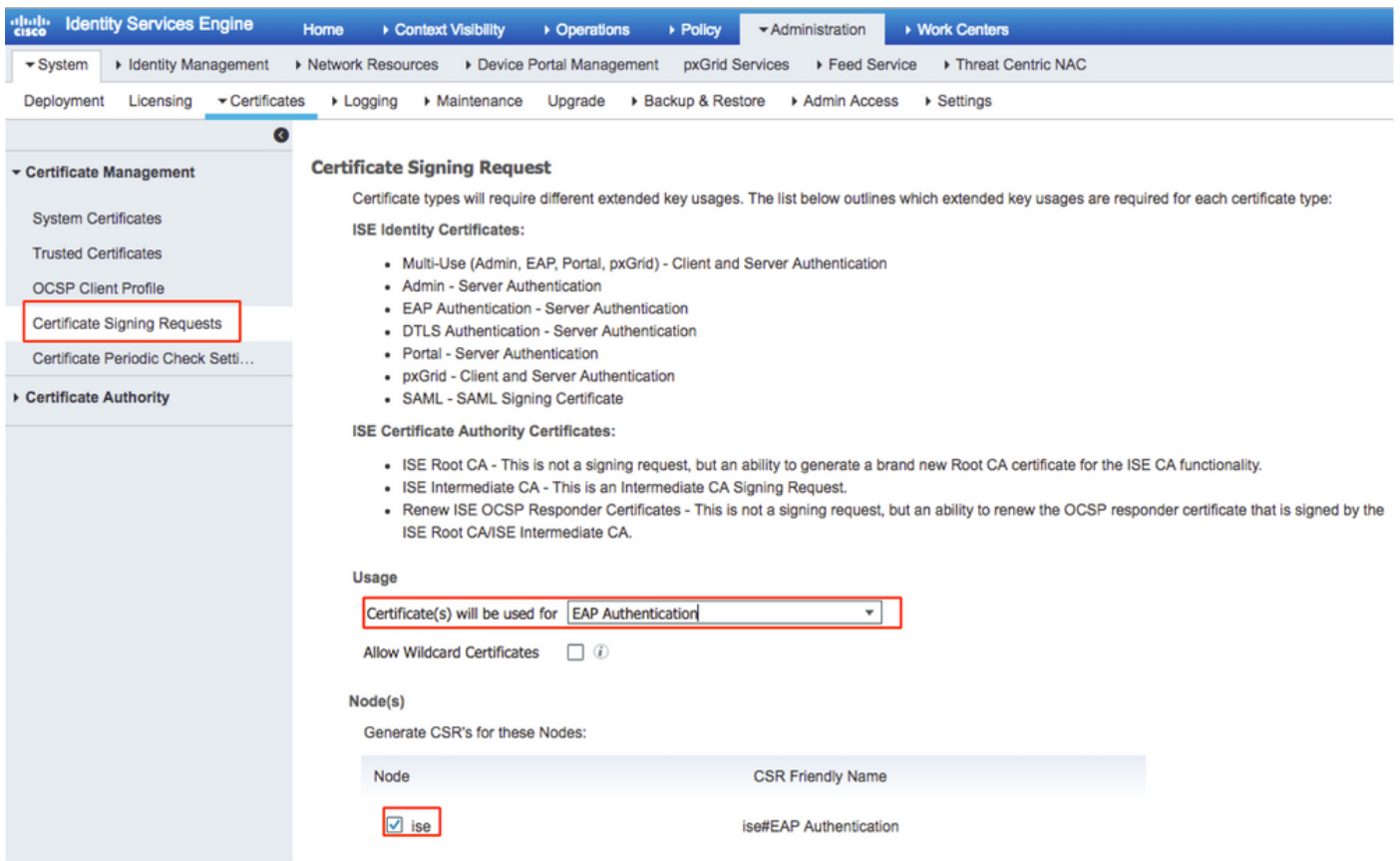
单击Import以将证书导入ISE。添加WLC并在ISE上创建用户后，您需要执行EAP-TLS中最重要的部分，即在ISE上信任证书。为此，您需要生成CSR。

步骤2.导航至Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests(CSR)，如图所示。

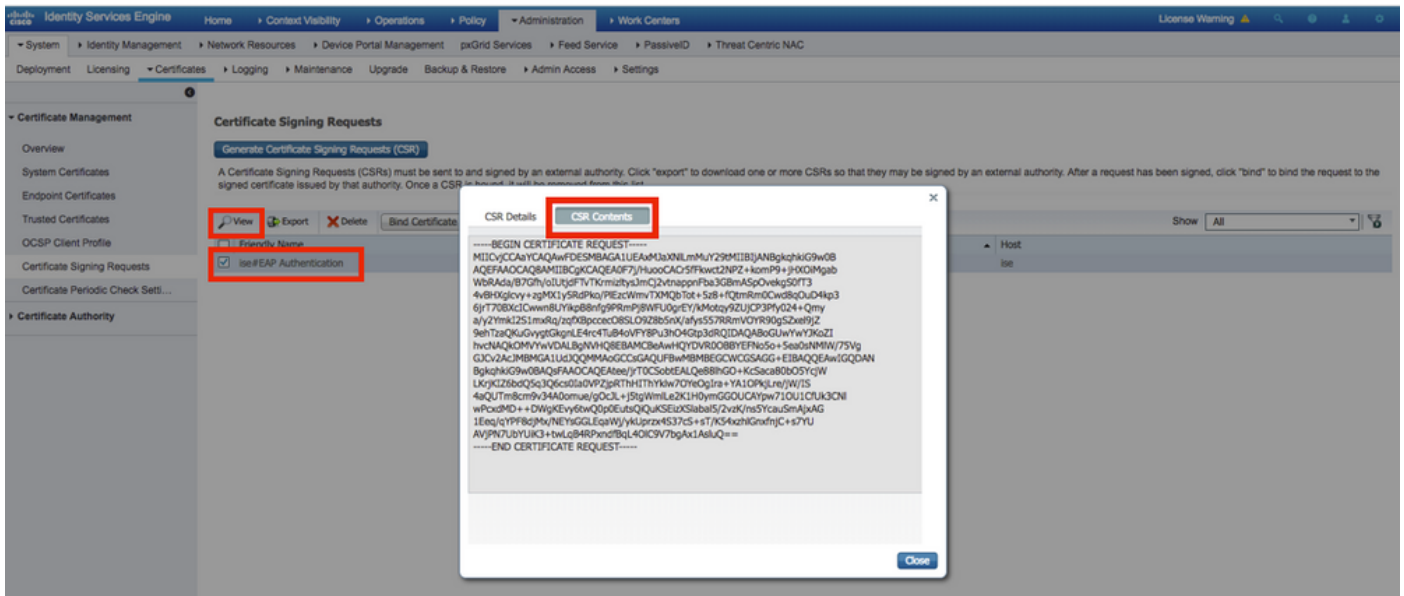


步骤3.要生成CSR，请导航至Usage，并从Certificate(s)will be used for下拉选项中选择EAP Authentication，如图所示。

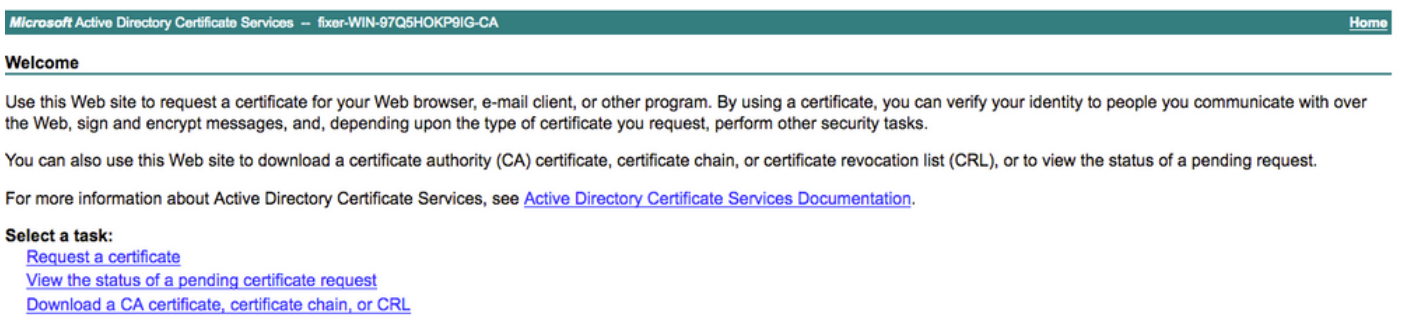




步骤4. 可以查看在ISE上生成的CSR。单击View，如图所示。



步骤5. 生成CSR后，浏览CA服务器，然后单击“请求证书”，如图所示：





步骤6. 申请证书后，您将获得用户证书和高级证书请求的选项，单击高级证书请求，如图所示。

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

## Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#)

步骤7. 粘贴在Base-64编码的证书请求中生成的CSR。从“证书模板：”下拉选项中，选择Web服务器并单击提交，如图所示。

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA Home

---

**Submit a Certificate Request or Renewal Request**

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

**Certificate Template:**

**Additional Attributes:**

Attributes:

步骤8. 单击Submit后，您将获得选择证书类型的选项，选择Base-64编码，然后单击Download certificate chain，如图所示。

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

## Certificate Issued

The certificate you requested was issued to you.

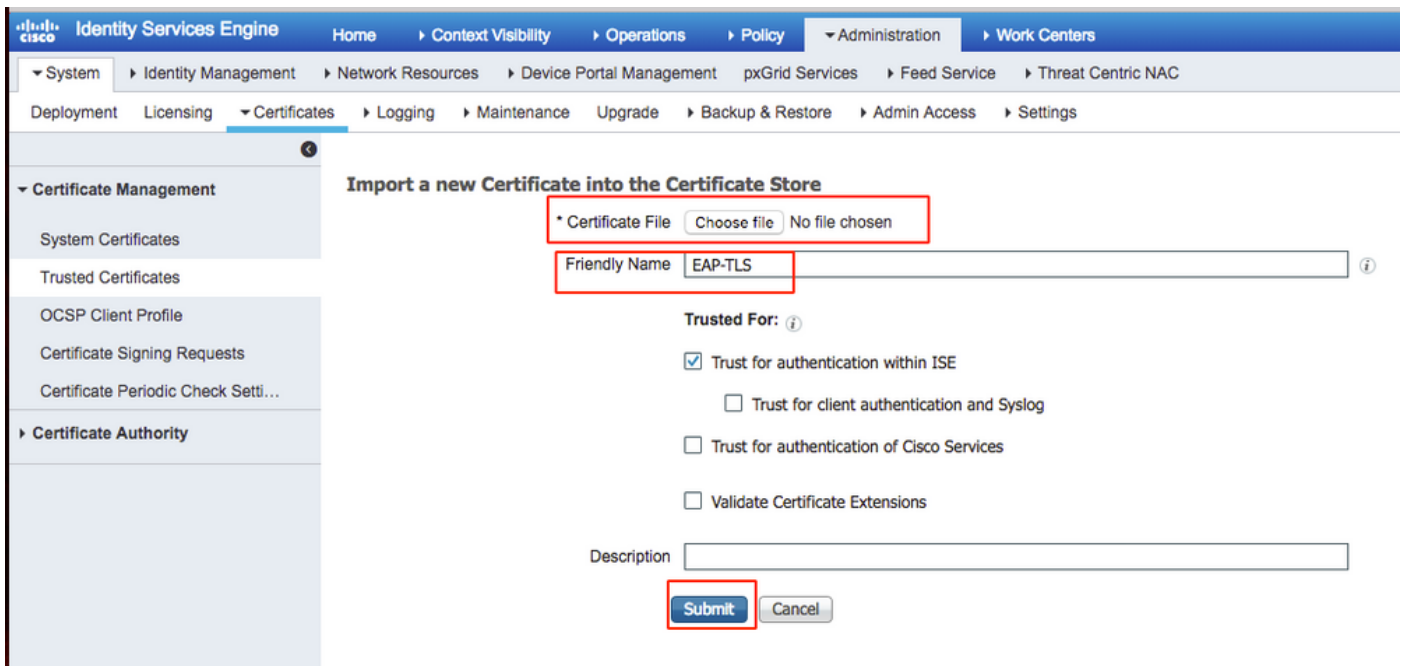
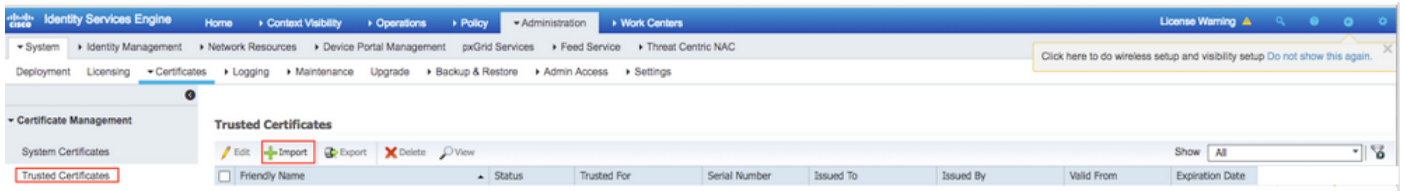
DER encoded or  Base 64 encoded



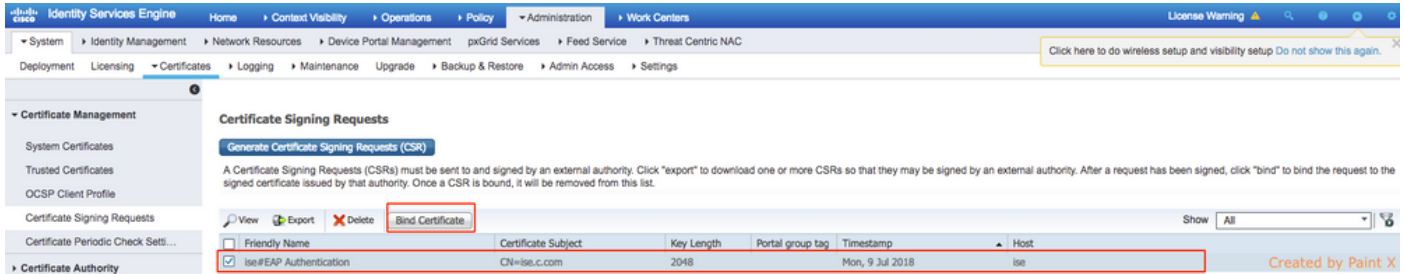
[Download certificate](#)

[Download certificate chain](#)

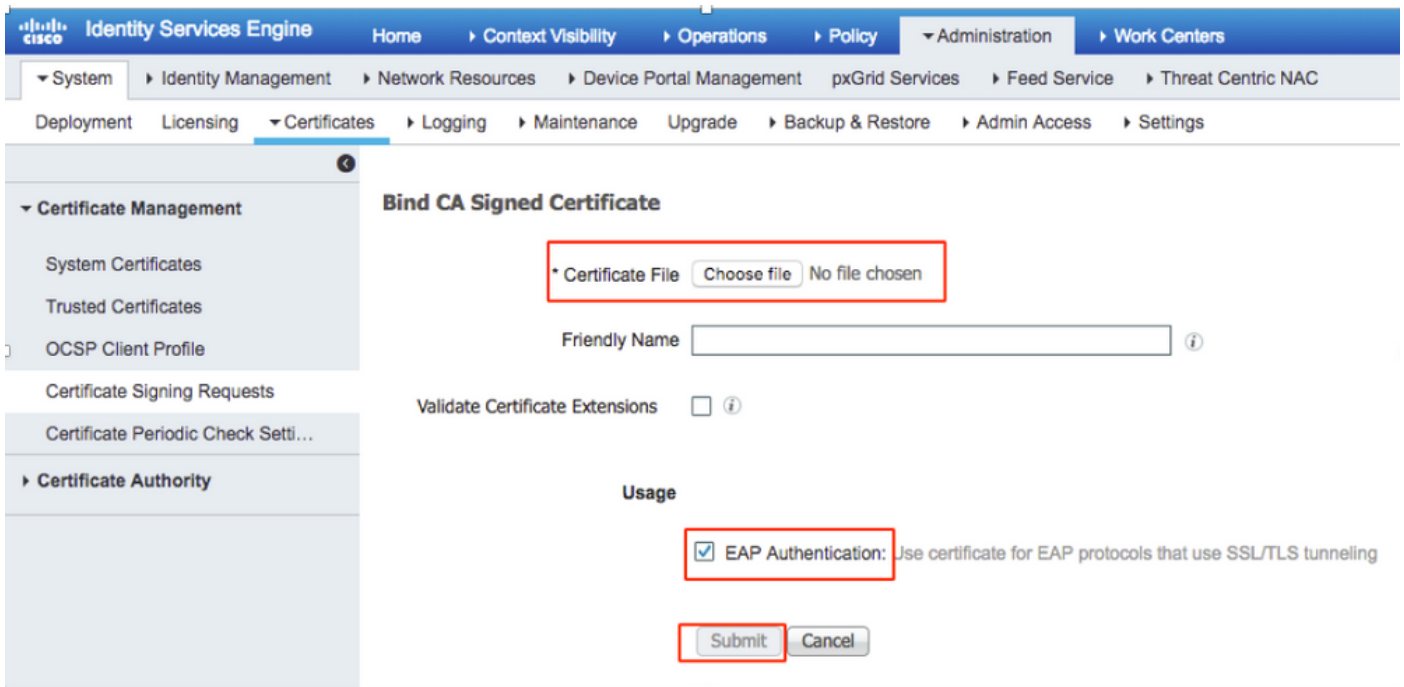
步骤9. ISE服务器的证书下载已完成。您可以提取证书，证书将包含两个证书，一个根证书和其他中间证书。根证书可以在Administration > Certificates > Trusted certificates > Import下导入，如图所示。



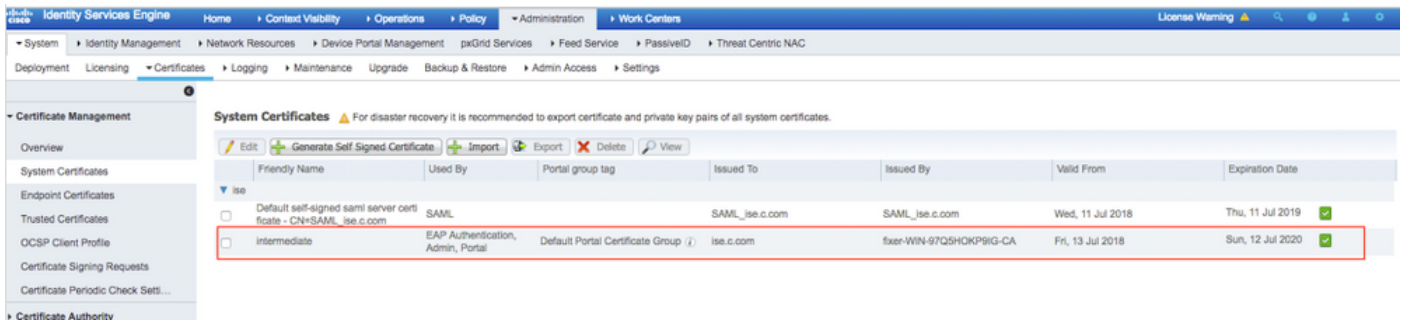
步骤10.单击**Submit**后，证书将添加到受信任证书列表。此外，需要中间证书才能与CSR绑定，如图所示。



步骤11.单击“绑定证书”后，便可以选择保存在桌面上的证书文件。浏览到中间证书，然后单击**Submit**，如图所示。



步骤12.要查看证书，请导航至Administration > Certificates > System Certificates，如图所示。



## EAP-TLS的客户端

### 在客户端 ( Windows桌面 ) 上下载用户证书

步骤1.要通过EAP-TLS对无线用户进行身份验证，必须生成客户端证书。将您的Windows计算机连接到网络，以便访问服务器。打开Web浏览器并输入以下地址：<https://server ip addr/certsrv>—

步骤2.请注意，CA必须与为ISE下载证书的CA相同。

为此，您需要浏览用于下载服务器证书的另一CA服务器。在同一CA上，单击**Request a certificate(请求证书)**，但是，这次您需要选择**User (用户)**作为Certificate Template (证书模板)，如图所示。

## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.

### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIspJry  
aF4l2aLpmDFp1PfvZ3VaP6Oa/mej3IXh0RFxBUII  
weOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR  
dD7LeujkxFlj3SwvLTKLDJq+00VtAhrxlp1PyDZ3  
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX  
-----END CERTIFICATE REQUEST-----
```

### Certificate Template:

User

### Additional Attributes:

Attributes:

Submit >

步骤3.然后，按以前对服务器执行的步骤单击下载证书链。

获得证书后，请按照以下步骤在Windows笔记本电脑上导入证书。

步骤4.要导入证书，您需要从Microsoft管理控制台(MMC)访问该证书。

1. 要打开MMC，请导航至“开始”>“运行”>“MMC”。
2. 导航至“文件”>“添加/删除管理单元”
3. 双击Certificates。
4. 选择计算机帐户。
5. 选择“本地计算机”>“完成”
6. 单击确定以退出“管理单元”窗口。
7. 单击Certificates > Personal > Certificates旁边的[+]。
8. 右键单击“证书”，然后选择“所有任务”>“导入”。
9. 单击 Next。
10. 单击浏览。
11. 选择要导入的.cer、.crt或.pfx。
12. 单击 Open (打开)。
13. 单击 Next。

14. 选择**Automatically select the certificate store based on the type of certificate**。

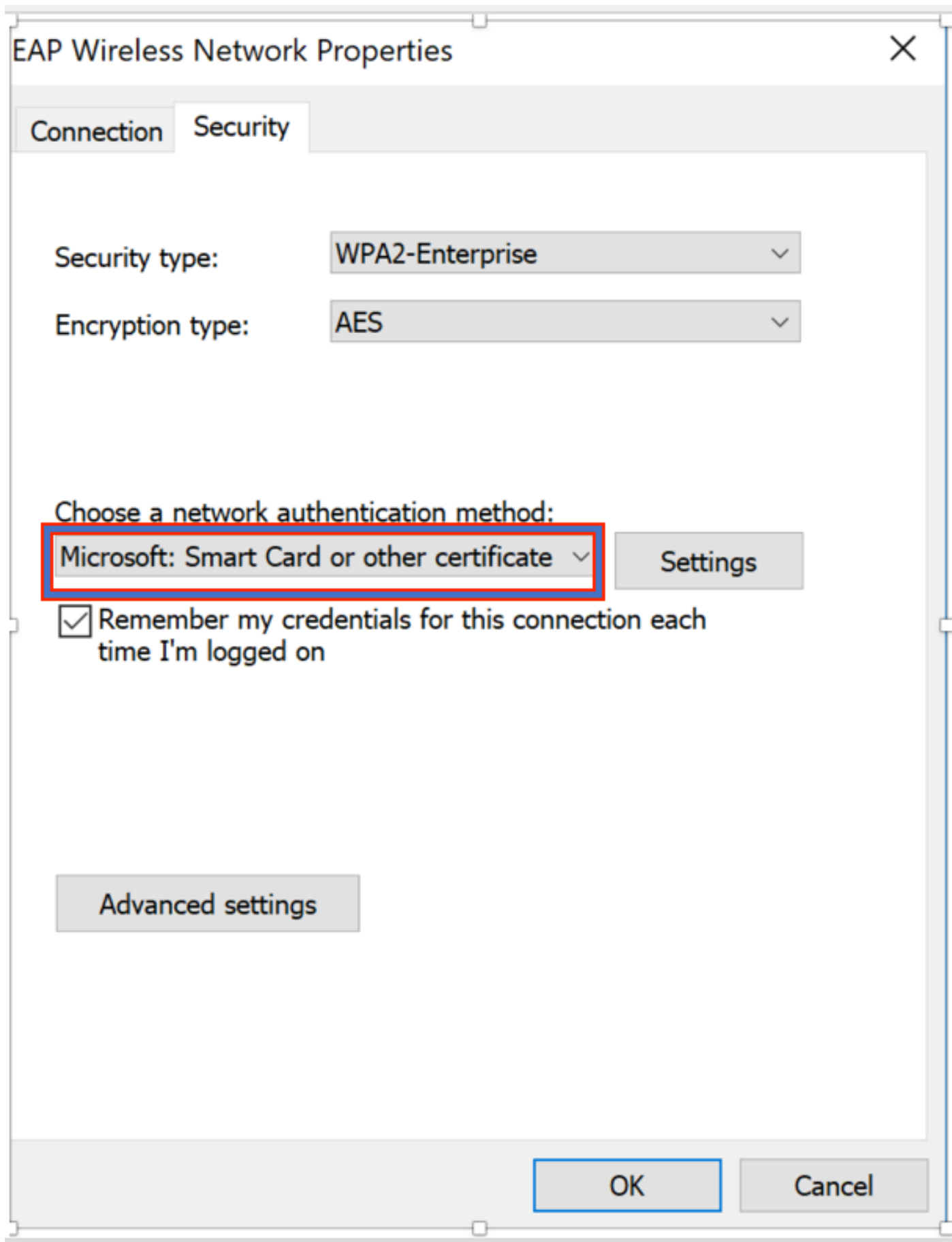
15. 单击**“完成”和“确定”**

完成证书导入后，您需要为EAP-TLS配置无线客户端（本例中为windows桌面）。

## **EAP-TLS的无线配置文件**

步骤1.更改之前为受保护可扩展身份验证协议(PEAP)创建的无线配置文件，以改用EAP-TLS。单击**EAP Wireless Profile**。

步骤2.选择**Microsoft:智能卡或其他证书**，然后单击**OK（确定）**，如图所示。



步骤3.单击**Settings**，然后选择从CA服务器颁发的根证书，如图所示。

## Smart Card or other Certificate Properties

When connecting:

Use my smart card

Use a certificate on this computer

Advanced

Use simple certificate selection (Recommended)

Verify the server's identity by validating the certificate

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

Trusted Root Certification Authorities:

Entrust.net Certification Authority (2048)

Equifax Secure Certificate Authority

fixer-WIN-97Q5HOKP9IG-CA

GeoTrust Global CA

GeoTrust Primary Certification Authority

GeoTrust Primary Certification Authority - G3

GlobalSign

GlobalSign

GlobalSign Root CA



View Certificate

步骤4.单击“高级设置”，然后从802.1x设置选项卡中选择用户或计算机身份验证，如图所示。



## Advanced settings

802.1X settings

802.11 settings

Specify authentication mode:

User or computer 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

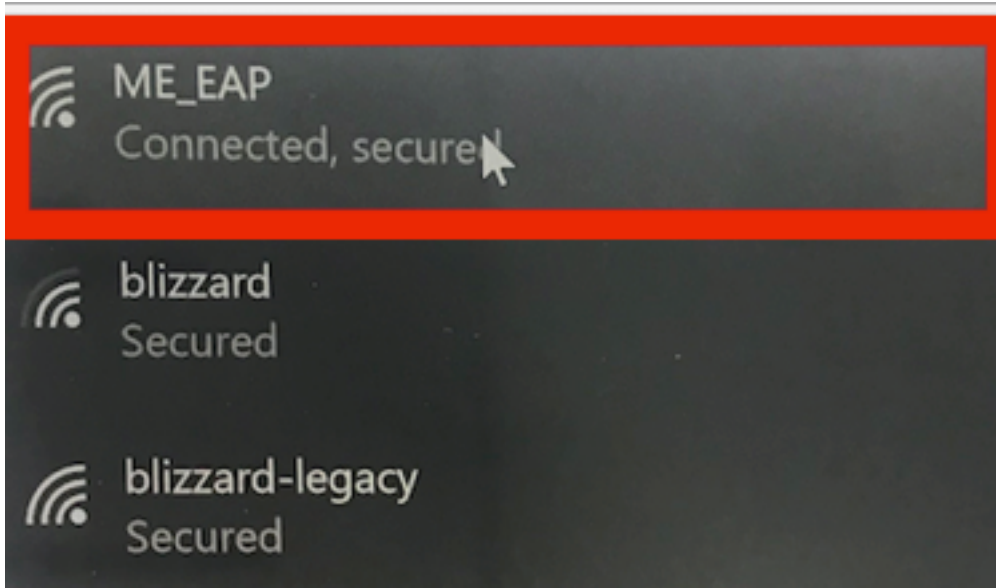
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

步骤5.现在，请尝试再次连接到无线网络，选择正确的配置文件（本例中为EAP）并连接。您已连接到无线网络，如图所示。

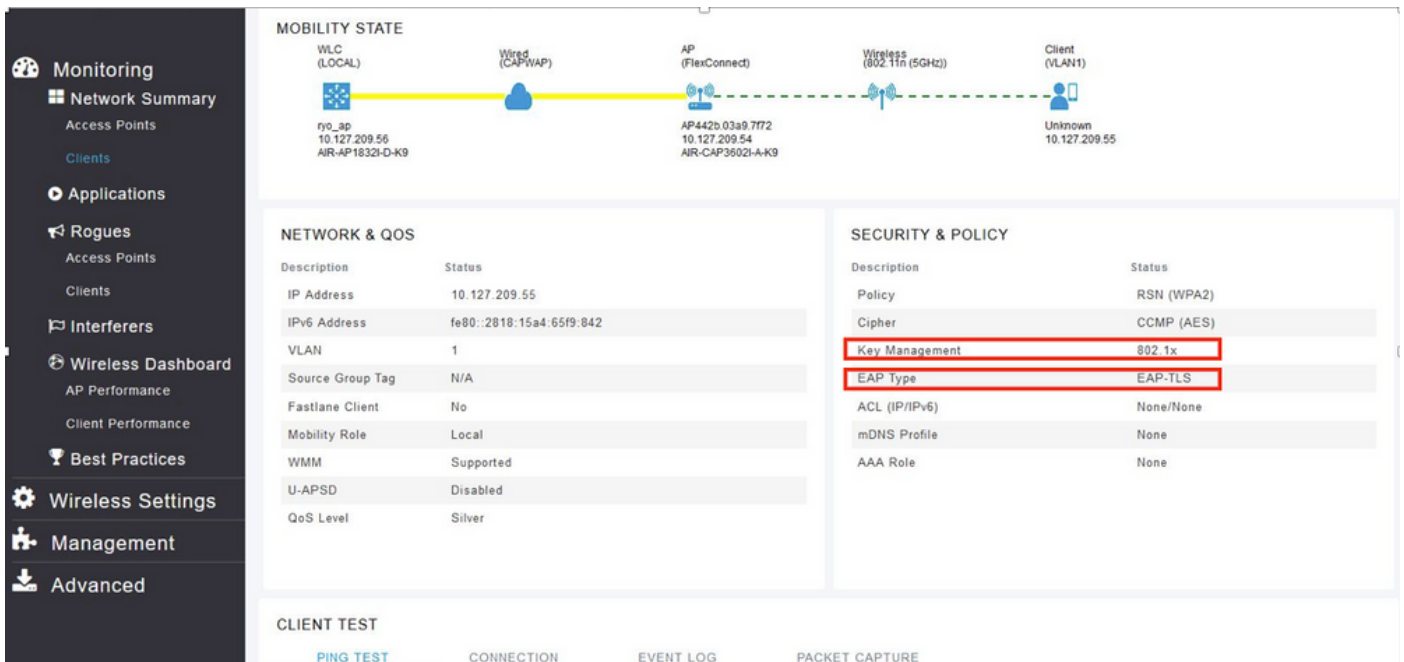


## 验证

使用本部分可确认配置能否正常运行。

步骤1. 客户端EAP类型必须是EAP-TLS。这意味着客户端已使用EAP-TLS完成身份验证，已获取IP地址，并且已准备好如图所示传递流量。

The screenshot shows a network management interface with a sidebar on the left and a main content area. The sidebar includes sections for Monitoring, Applications, Rogues, Interferers, Wireless Dashboard, Best Practices, Wireless Settings, Management, and Advanced. The main content area is titled 'CLIENT VIEW' and displays details for a client named 'ME\_EAP'. The 'GENERAL' section shows the client's User Name as 'Administrator', Host Name as 'Unknown', MAC Address as '34:02:86:96:2f:b7', Uptime as 'Associated since 37 Seconds', and SSID as 'ME\_EAP' (highlighted with a red box). The AP Name is 'AP442b.03a9.7f72 (Ch 56)'. The 'CONNECTIVITY' section shows a progress bar with five steps: Start, Association, Authentication, DHCP, and Online, all of which are completed. The 'TOP APPLICATIONS' section shows 'No Data Available!'. The 'MOBILITY STATE' section shows a diagram of the network topology, including WLC (LOCAL), Wired (CAPWAP), AP (FlexConnect), Wireless (802.11n (5GHz)), and Client (VLAN1).






步骤2. 以下是来自控制器CLI的客户端详细信息（输出已修剪）：

```
(Cisco Controller) >show client detail 34:02:86:96:2f:b7
Client MAC Address..... 34:02:86:96:2f:b7
Client Username ..... Administrator
AP MAC Address..... c8:f9:f9:83:47:b0
AP Name..... AP442b.03a9.7f72
AP radio slot Id..... 1
Client State..... Associated
Client User Group..... Administrator
Client NAC OOB State..... Access
Wireless LAN Id..... 6
Wireless LAN Network Name (SSID)..... ME_EAP
Wireless LAN Profile Name..... ME_EAP
Hotspot (802.11u)..... Not Supported
BSSID..... c8:f9:f9:83:47:ba
Connected For ..... 18 secs
Channel..... 56
IP Address..... 10.127.209.55
Gateway Address..... 10.127.209.49
Netmask..... 255.255.255.240
IPv6 Address..... fe80::2818:15a4:65f9:842
--More-- or (q)uit
Security Policy Completed..... Yes
Policy Manager State..... RUN
Policy Type..... WPA2
Authentication Key Management..... 802.1x
Encryption Cipher..... CCMP-128 (AES)
Protected Management Frame ..... No
Management Frame Protection..... No
EAP Type..... EAP-TLS
```

步骤3. 在ISE上，导航至Context Visibility > End Points > Attributes，如图所示。

Endpoints > 34:02:86:96:2F:B7

34:02:86:96:2F:B7   



MAC Address: 34:02:86:96:2F:B7  
 Username: Administrator@fixer.com  
 Endpoint Profile: Intel-Device  
 Current IP Address:  
 Location:

Attributes Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment	false
Endpoint Policy	Intel-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

Custom Attributes

Filter 

Attribute Name	Attribute Value
<input type="text" value="Attribute Name"/>	<input type="text" value="Attribute Value"/>

No data found. Add custom attributes here.

Other Attributes

AAA-Server	ise
AKI	88:20:a7:c9:96:03:5a:26:58:fd:67:58:83:71:e8:bc:c6:6d:97:bd
Airespace-Wlan-Id	6
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509_PKI
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access

BYODRegistration	Unknown
Called-Station-ID	c8-f9-f9-83-47-b0:ME_EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	344
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.127.209.56
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	21
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.11
FailureReason	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9\G-CA,DC=fixer,DC=cc
Issuer - Common Name	fixer-WIN-97Q5HOKP9\G-CA
Issuer - Domain Component	fixer, com
Key Usage	0, 2
Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7

MatchedPolicy	Intel-Device
MessageCode	5411
NAS-IP-Address	10.127.209.56
NAS-Identifier	ryo_ap
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	ryo_ap
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
NetworkDeviceProfileName	Cisco
OUI	Intel Corporate
OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
PolicyVersion	0
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	Wireless802_1x
RadiusPacketType	Drop
SSID	c8-f9-f9-83-47-b0:ME_EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

## 故障排除

目前没有针对此配置的故障排除信息。