# 了解并配置WLC和ISE的EAP-TLS

## 目录

## 简介

本文档介绍如何使用802.1X和可扩展身份验证协议EAP-TLS设置无线局域网(WLAN)

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 802.1X身份验证过程
- 证书

### 使用的组件

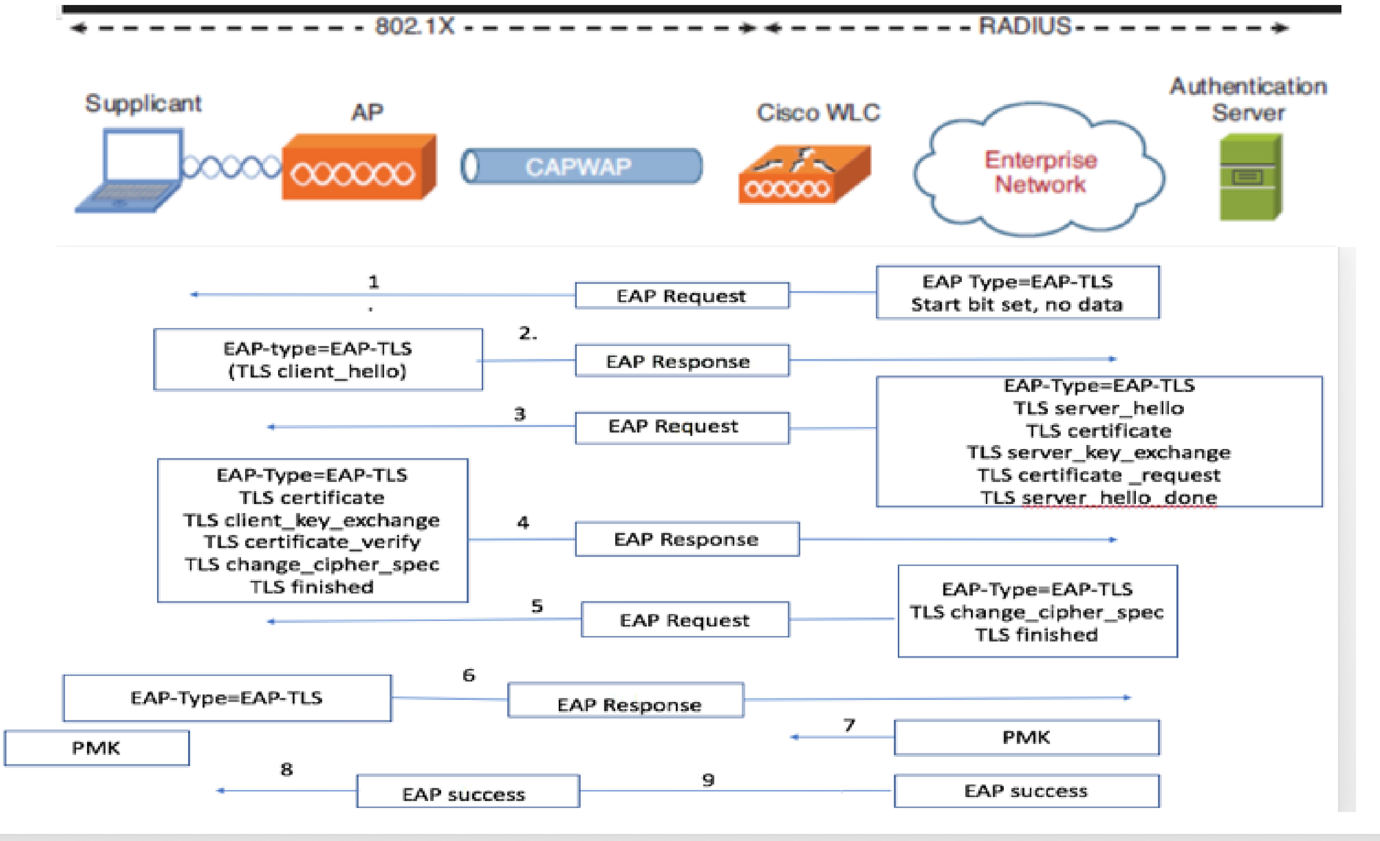
本文档中的信息基于以下软件和硬件版本：

- WLC 3504版本8.10
- 身份服务引擎(ISE)版本2.7

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流程中的步骤

1. 无线客户端与接入点(AP)关联。此时AP不允许客户端发送任何数据并发送身份验证请求。然后，请求方使用EAP-Response Identity进行响应。然后，WLC将用户ID信息传送到身份验证服务器。RADIUS服务器使用EAP-TLS启动数据包对客户端做出响应。EAP-TLS对话从此开始。
2. 对等体将EAP-Response发送回包含“client_hello”握手消息的身份验证服务器，该握手消息是设置为NULL的密码
3. 身份验证服务器使用包含下列内容的访问质询数据包进行响应：

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

4.客户端响应EAP-Response消息，其中包含：

```
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
```

5.在客户端成功进行身份验证后，RADIUS服务器会以包含“change_cipher_spec”和握手完成消息的Access-challenge进行响应。

6.收到此信息时，客户端验证哈希以便对radius服务器进行身份验证。

7.在TLS握手期间，从密钥动态派生新的加密密钥

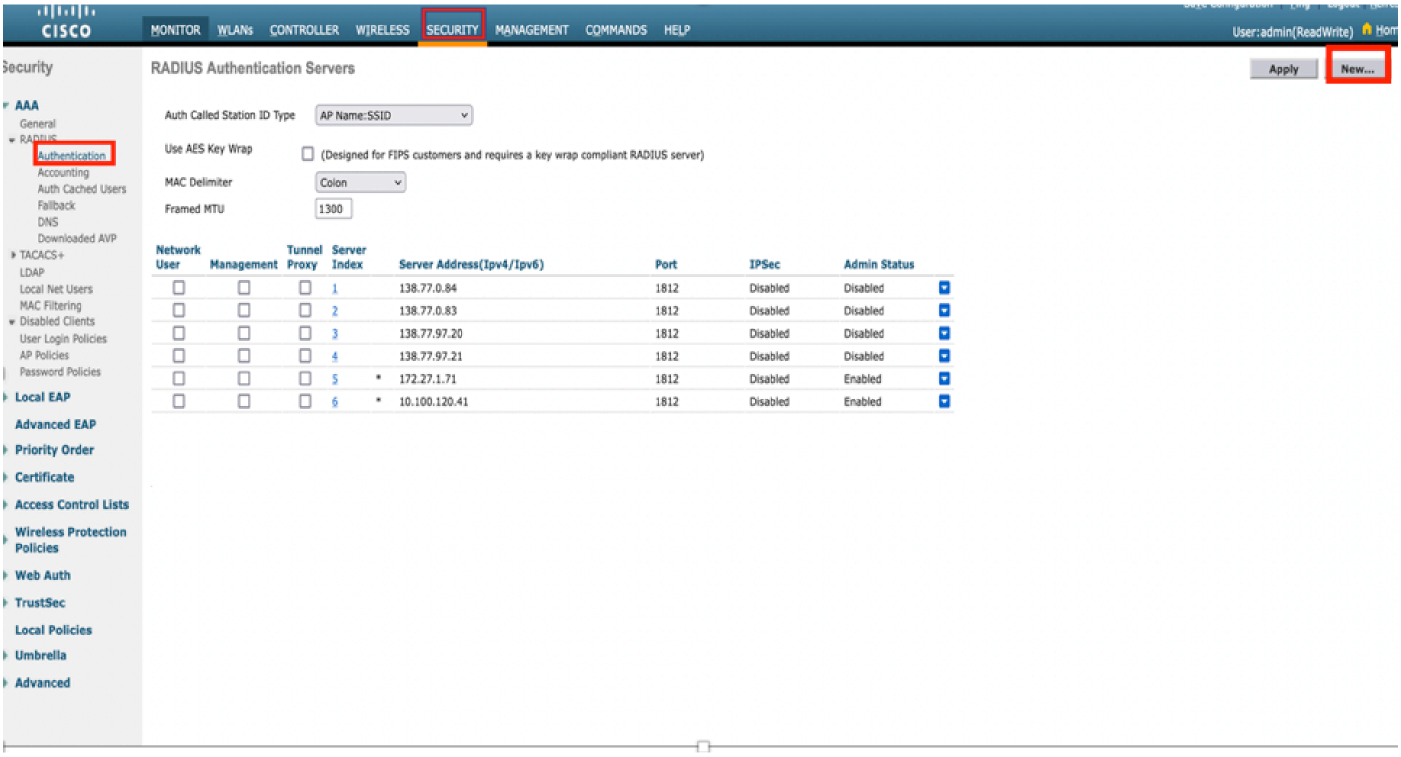
8/9.EAP — 成功最终从服务器发送到身份验证器，然后传递给请求方。

此时，启用EAP-TLS的无线客户端可以访问无线网络。

# 配置

## Cisco 无线 LAN 控制器

步骤1.第一步是在Cisco WLC上配置RADIUS服务器。要添加RADIUS服务器，请导航到**安全> RADIUS >身份验证**。单击**New**，如图所示。



RADIUS Authentication Servers

Auth Called Station ID Type: AP Name:SSID

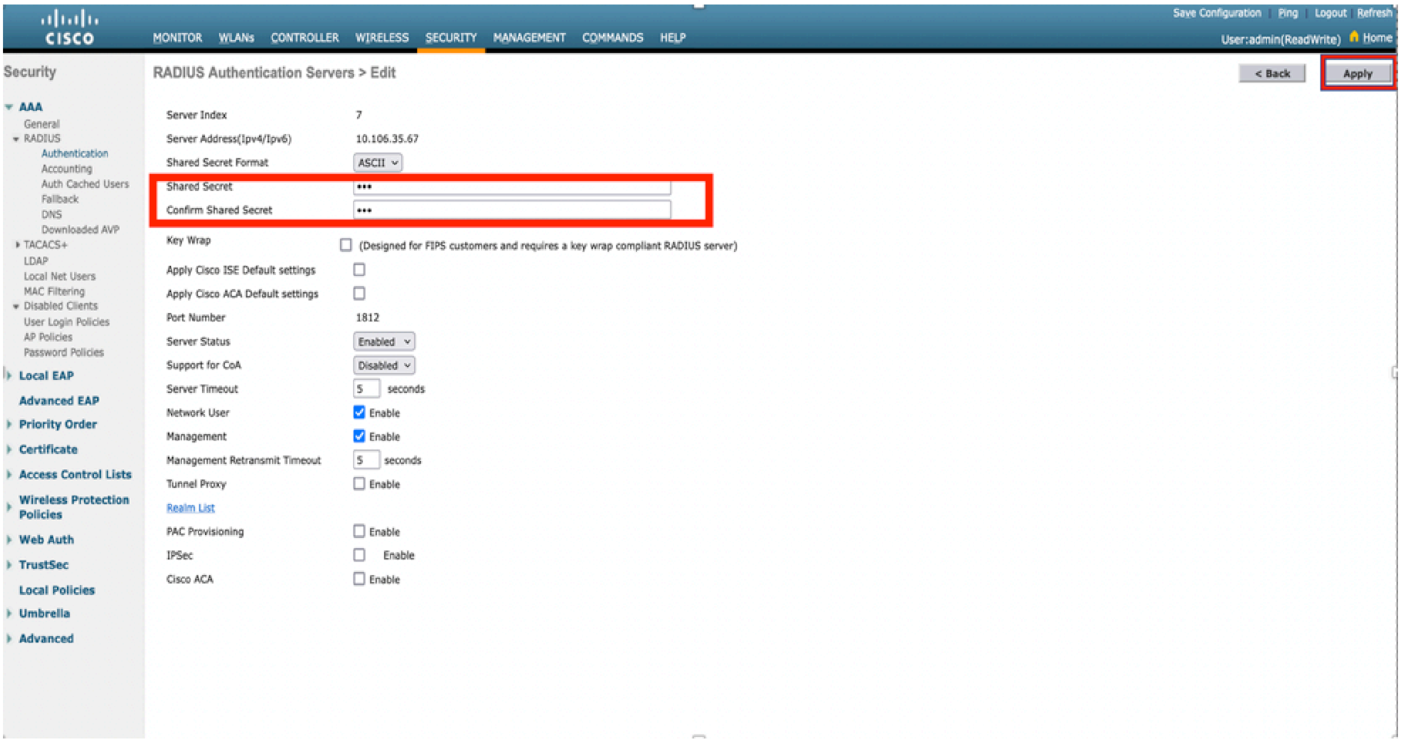
Use AES Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Colon

Framed MTU: 1300

| Network User | Management | Tunnel Proxy | Server Index | Server Address(Ipv4/Ipv6) | Port | IPSec | Admin Status |
|---|---|---|---|---|---|---|---|
| □ | □ | □ | 1 | 138.77.0.84 | 1812 | Disabled | Disabled |
| □ | □ | □ | 2 | 138.77.0.83 | 1812 | Disabled | Disabled |
| □ | □ | □ | 3 | 138.77.97.20 | 1812 | Disabled | Disabled |
| □ | □ | □ | 4 | 138.77.97.21 | 1812 | Disabled | Disabled |
| □ | □ | □ | 5 * | 172.27.1.71 | 1812 | Disabled | Enabled |
| □ | □ | □ | 6 * | 10.100.120.41 | 1812 | Disabled | Enabled |

步骤2.在此处，您需要输入用于验证ISE上的WLC的IP地址和共享密钥<password>。单击**Apply**以继续操作，如图所示。



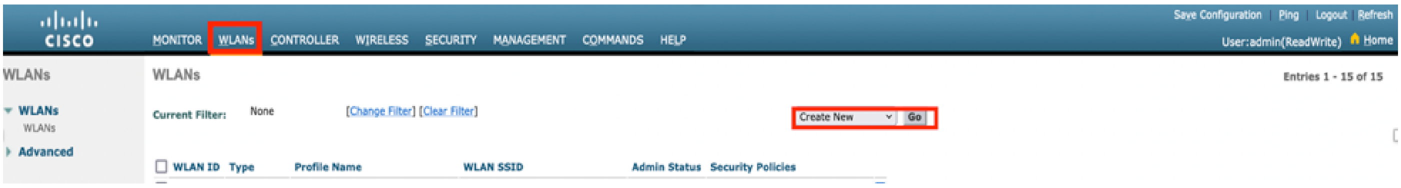
RADIUS Authentication Servers > Edit

| | |
|---|---|
| Server Index | 7 |
| Server Address(Ipv4/Ipv6) | 10.106.35.67 |
| Shared Secret Format | ASCII |
| Shared Secret | ••• |
| Confirm Shared Secret | ••• |
| Key Wrap | □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server) |
| Apply Cisco ISE Default settings | □ |
| Apply Cisco ACA Default settings | □ |
| Port Number | 1812 |
| Server Status | Enabled |
| Support for CoA | Disabled |
| Server Timeout | 5 seconds |
| Network User | ☑ Enable |
| Management | ☑ Enable |
| Management Retransmit Timeout | 5 seconds |
| Tunnel Proxy | □ Enable |
| Realm List | |
| PAC Provisioning | □ Enable |
| IPSec | □ Enable |
| Cisco ACA | □ Enable |

步骤3.为RADIUS身份验证创建WLAN。

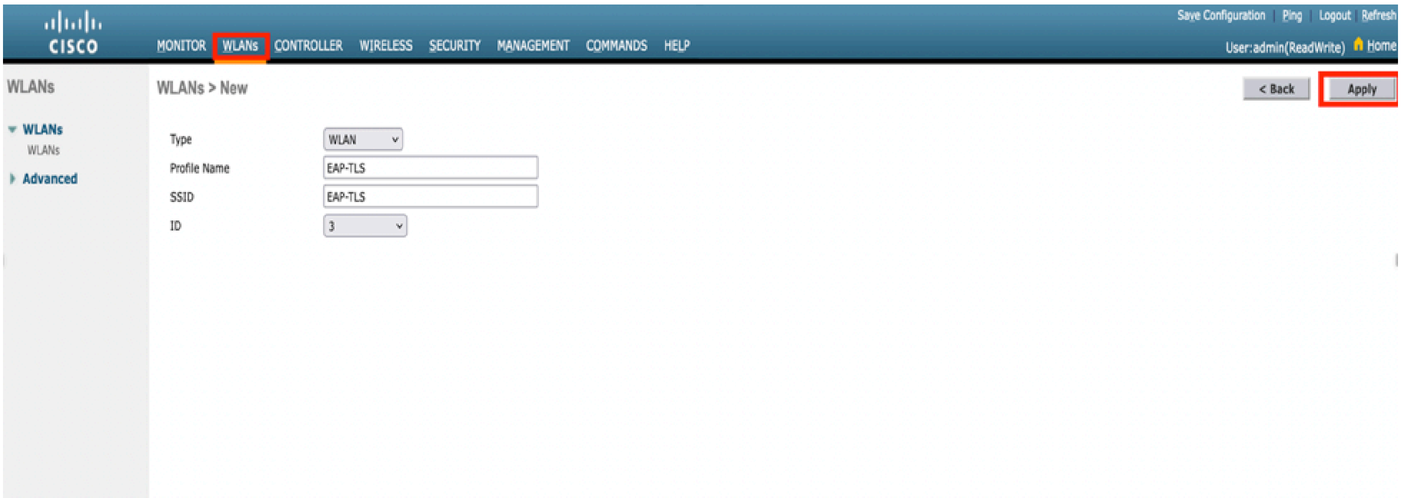
现在，您可以创建新的WLAN并将其配置为使用WPA-enterprise模式，以便使用RADIUS进行身份验证。

步骤4.从主菜单中选择**WLANs**，选择**Create New**，然后单击**Go**（如图所示）。


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Save Configuration | Ping | Logout | Refresh
User:admin(ReadWrite) Home
WLANs
WLANs
WLANs
Advanced
Entries 1 - 15 of 15
[Change Filter] [Clear Filter]
Create New
Go
WLAN ID
Type
Profile Name
WLAN SSID
Admin Status
Security Policies

Current Filter: None

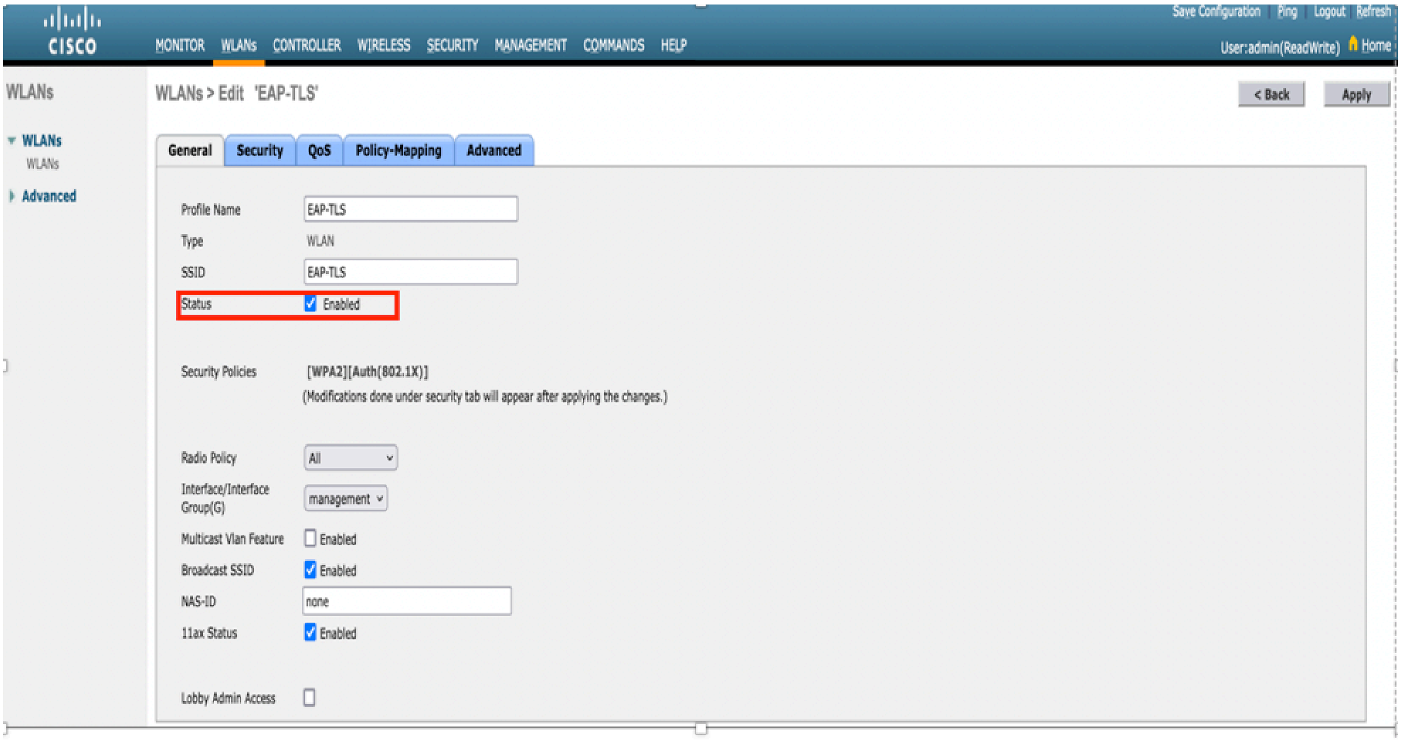
步骤5.将新的WLAN命名为**EAP-TLS**。单击**Apply**以继续操作，如图所示。


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Save Configuration | Ping | Logout | Refresh
User:admin(ReadWrite) Home
WLANs
WLANs
WLANs
Advanced
< Back
Apply

WLANs > New

| | |
|---|---|
| Type | WLAN |
| Profile Name | EAP-TLS |
| SSID | EAP-TLS |
| ID | 3 |

步骤6.单击**General**并确保状态为**Enabled**。默认安全策略是802.1X身份验证和WPA2，如图所示。


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
User:admin(ReadWrite) Home
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced

WLANs > Edit 'EAP-TLS'

Profile Name: EAP-TLS

Type: WLAN

SSID: EAP-TLS

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

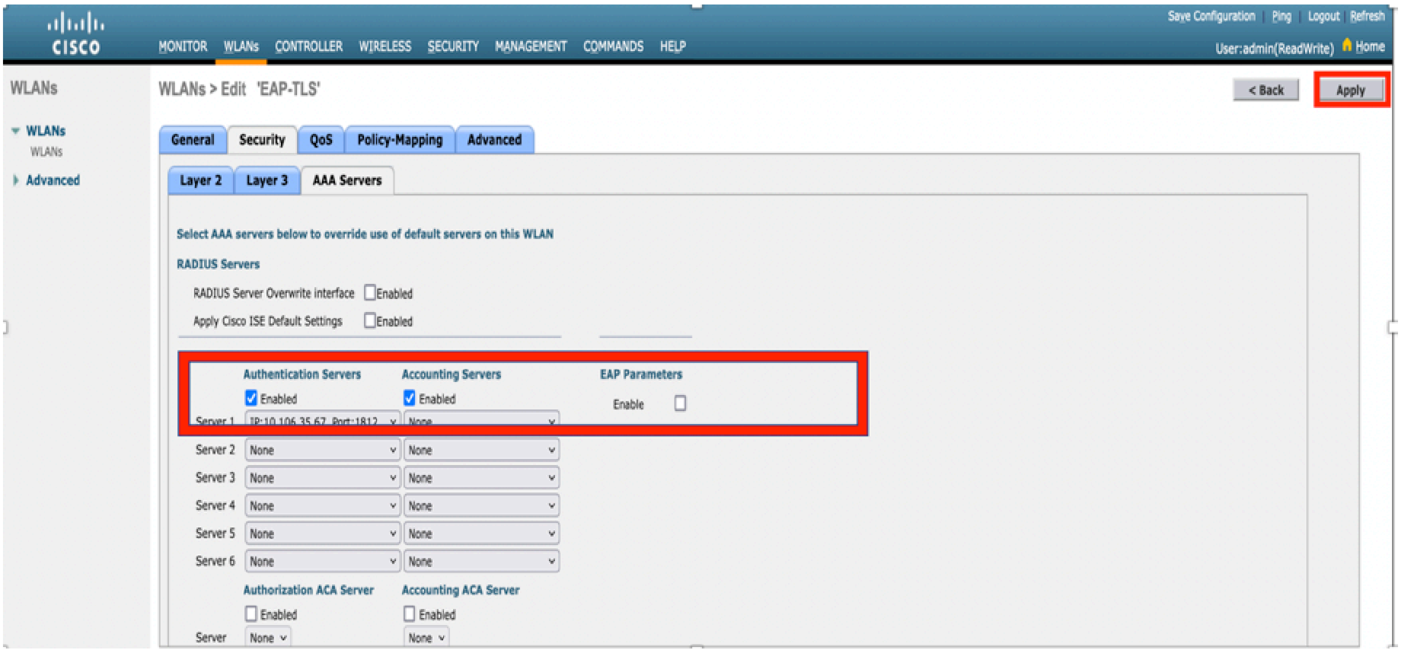
Broadcast SSID: ☑ Enabled

NAS-ID: none

11ax Status: ☑ Enabled

Lobby Admin Access: □

步骤7.现在，导航到**安全 > AAA服务器**选项卡，选择您刚才配置的RADIUS服务器，如图所示。


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
User:admin(ReadWrite) Home
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers

WLANs > Edit 'EAP-TLS'

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface □Enabled

Apply Cisco ISE Default Settings □Enabled

| | Authentication Servers | Accounting Servers | EAP Parameters |
|---|---|---|---|
| | ☑ Enabled | ☑ Enabled | Enable □ |
| Server 1 | IP:10.106.35.67, Port:1812 | None | |
| Server 2 | None | None | |
| Server 3 | None | None | |
| Server 4 | None | None | |
| Server 5 | None | None | |
| Server 6 | None | None | |
| | Authorization ACA Server | Accounting ACA Server | |
| | □ Enabled | □ Enabled | |
| Server | None | None | |

**注意：**在继续操作之前，最好检验是否可以从WLC访问RADIUS服务器。RADIUS使用UDP端口1812（用于身份验证），因此您需要确保此流量不会在网络的任何位置被阻止。

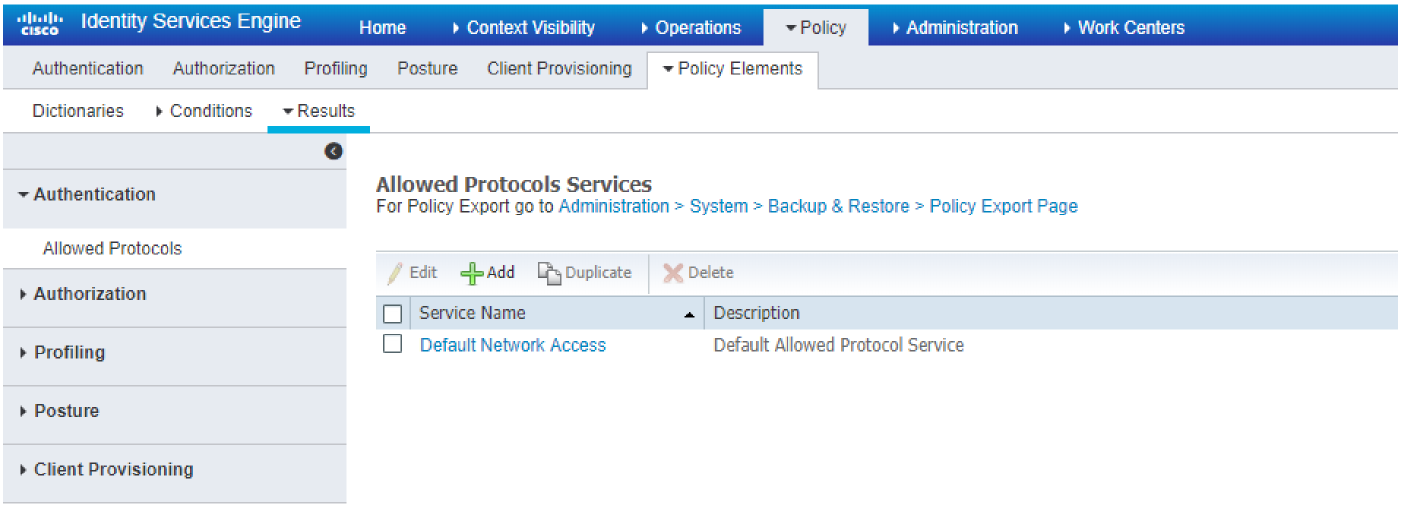
## 使用Cisco WLC的ISE

### EAP-TLS设置

为了构建策略，您需要创建允许在策略中使用的协议列表。由于写入了dot1x策略，请根据策略配置方式指定允许的EAP类型。

如果您使用默认值，则允许大多数EAP类型进行身份验证，如果您需要锁定对特定EAP类型的访问，则这些类型不是首选的。

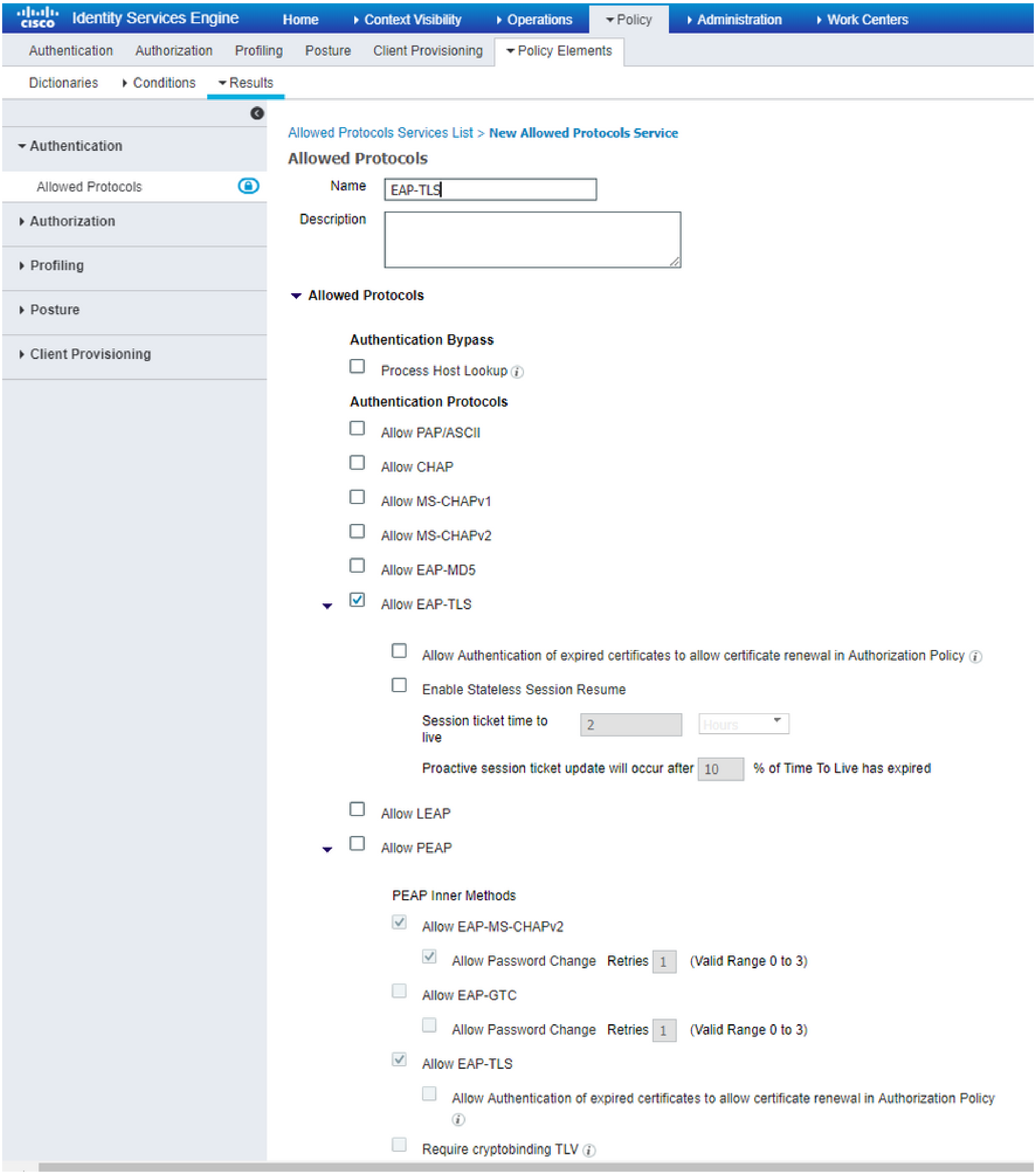
步骤1.导航到**策略>Policy元素>结果>身份验证>允许的协议**，然后单击**Add**，如图所示。



Allowed Protocols Services
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

| □ | Service Name | Description |
|---|---|---|
| □ | Default Network Access | Default Allowed Protocol Service |

步骤2.在此Allowed Protocol列表中，可以输入列表的名称。在这种情况下，**Allow EAP-TLS**框已选中，其他框未选中，如图所示。



Allowed Protocols Services List > **New Allowed Protocols Service**

**Allowed Protocols**

Name: EAP-TLS

Description:

**Allowed Protocols**

Authentication Bypass

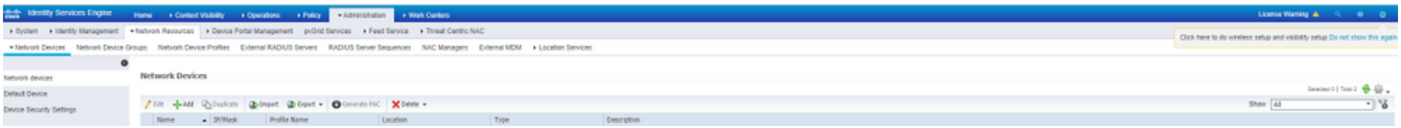
- □ Process Host Lookup

Authentication Protocols

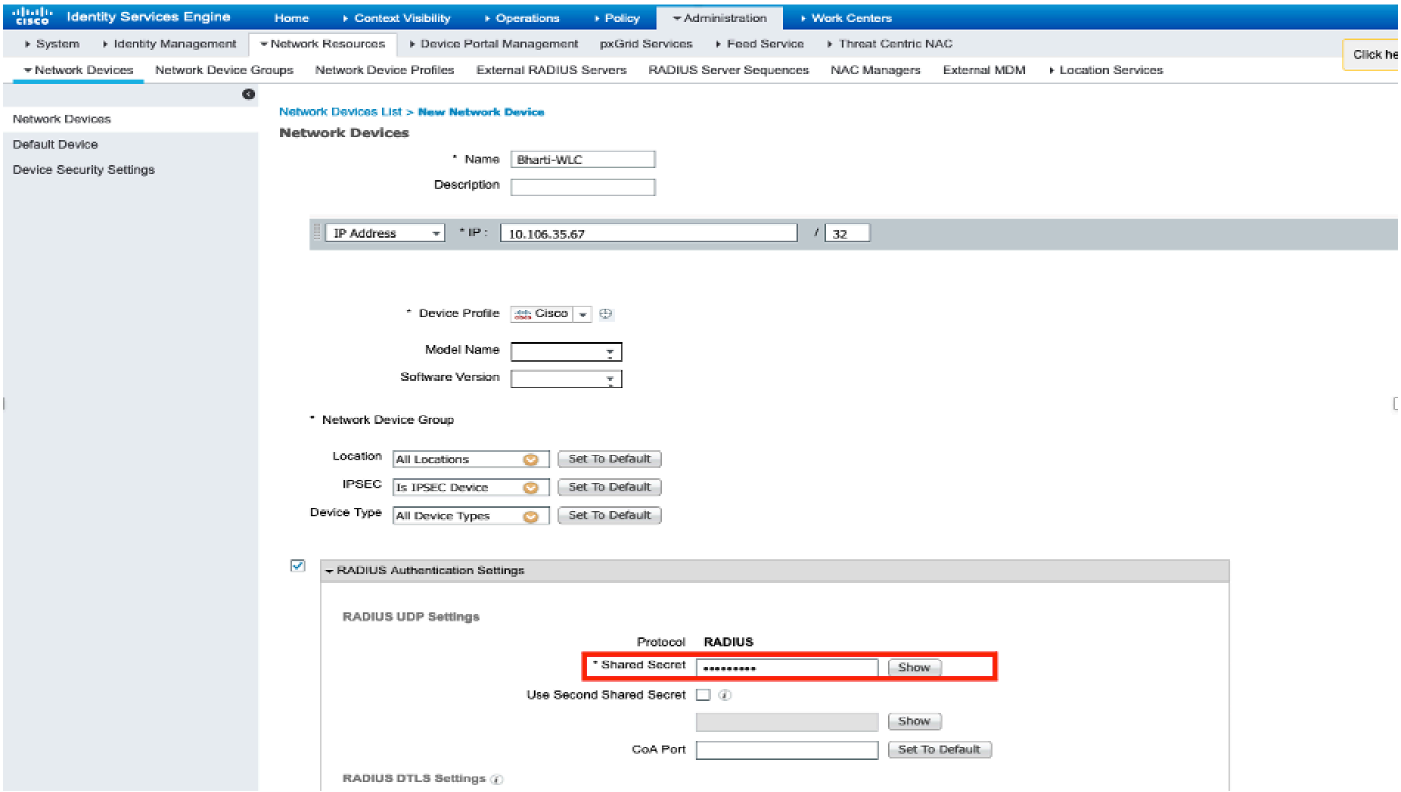
- □ Allow PAP/ASCII
- □ Allow CHAP
- □ Allow MS-CHAPv1
- □ Allow MS-CHAPv2
- □ Allow EAP-MD5
- ☑ Allow EAP-TLS
  - □ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
  - □ Enable Stateless Session Resume
  - Session ticket time to live: 2 Hours
  - Proactive session ticket update will occur after 10 % of Time To Live has expired
- □ Allow LEAP
- □ Allow PEAP
  - PEAP Inner Methods
  - ☑ Allow EAP-MS-CHAPv2
    - ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
  - □ Allow EAP-GTC
    - □ Allow Password Change Retries 1 (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WLC设置

第1步：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。



步骤2.输入如图所示的值。



Network Devices List > New Network Device

Network Devices

* Name: Bharti-WLC

Description:

IP Address * IP : 10.106.35.67 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations

IPSEC: Is IPSEC Device

Device Type: All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: ••••••••••

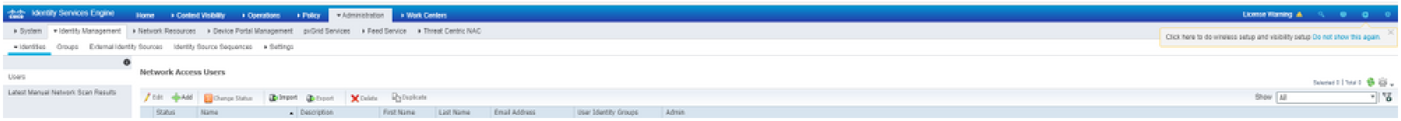
Use Second Shared Secret ☐

CoA Port:

RADIUS DTLS Settings

## 在 ISE 上创建新用户

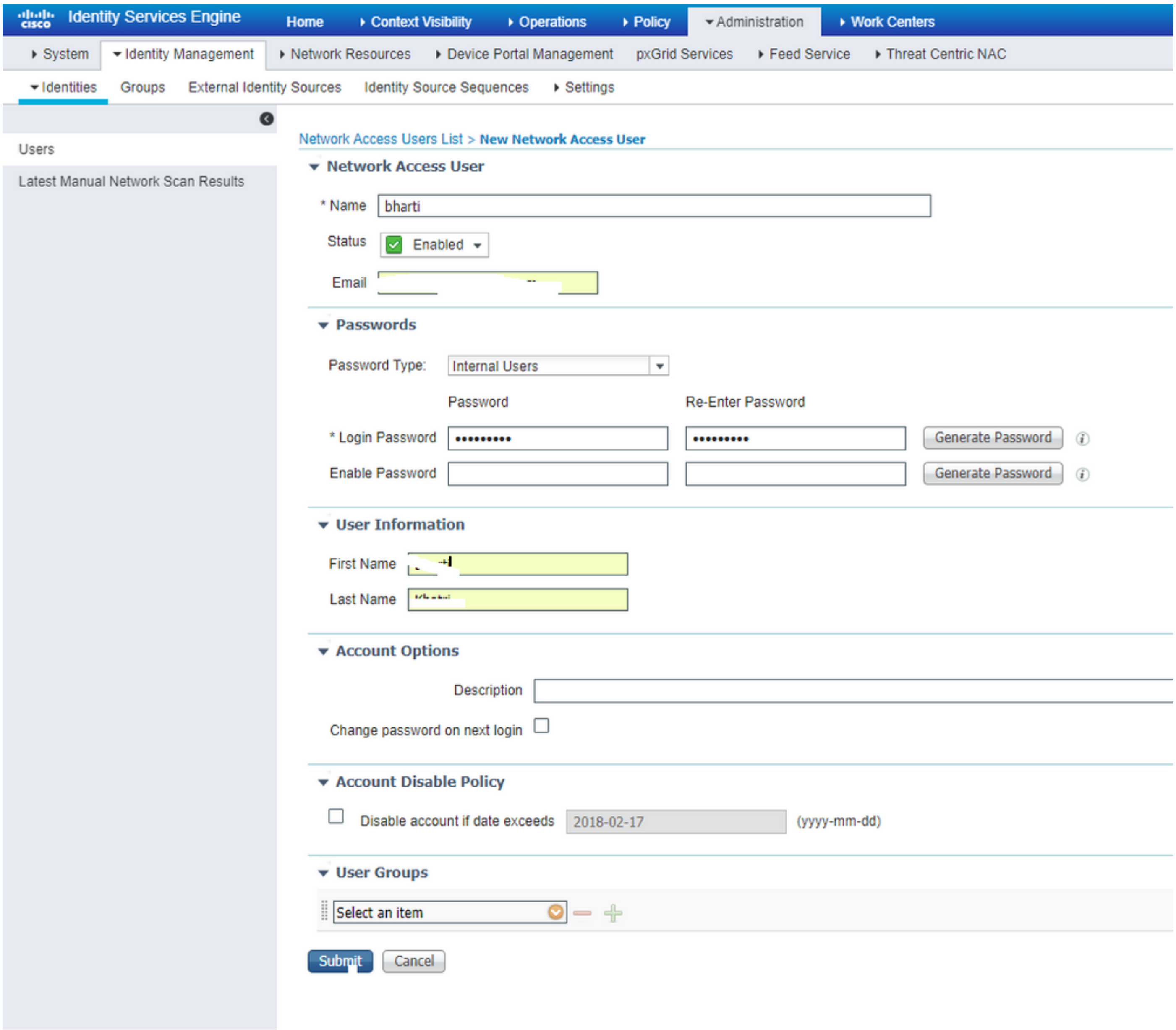
第 1 步： 导航至管理 > 身份管理 > 身份 > 用户 > 添加，如图所示。



Network Access Users

| Status | Name | Description | First Name | Last Name | Email Address | User Identity Groups | Admin |
|---|---|---|---|---|---|---|---|

步骤2.输入如图所示的信息。



Network Access Users List > **New Network Access User**

**Network Access User**

* Name: bharti

Status: ☑ Enabled

Email: [redacted]

**Passwords**

Password Type: Internal Users

| | Password | Re-Enter Password |
|---|---|---|
| * Login Password | ••••••••• | ••••••••• |
| Enable Password | | |

**User Information**

First Name: [redacted]

Last Name: [redacted]

**Account Options**

Description:

Change password on next login ☐

**Account Disable Policy**

☐ Disable account if date exceeds 2018-02-17 (yyyy-mm-dd)

**User Groups**

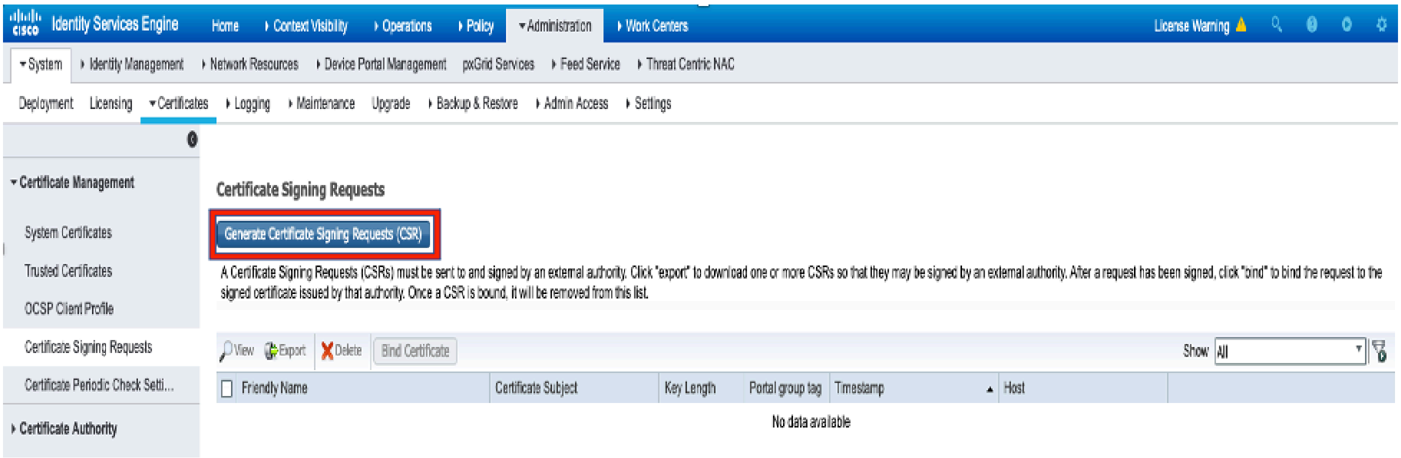
Select an item

## ISE上的信任证书

步骤1.导航到**管理>System >证书>证书管理>受信任证书**。

单击**Import**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的最重要部分，即信任ISE上的证书。为此，我们需要生成CSR。

第2步：导航到**管理>证书>证书签名请求>生成证书签名请求(CSR)**，如图所示。



Certificate Signing Requests

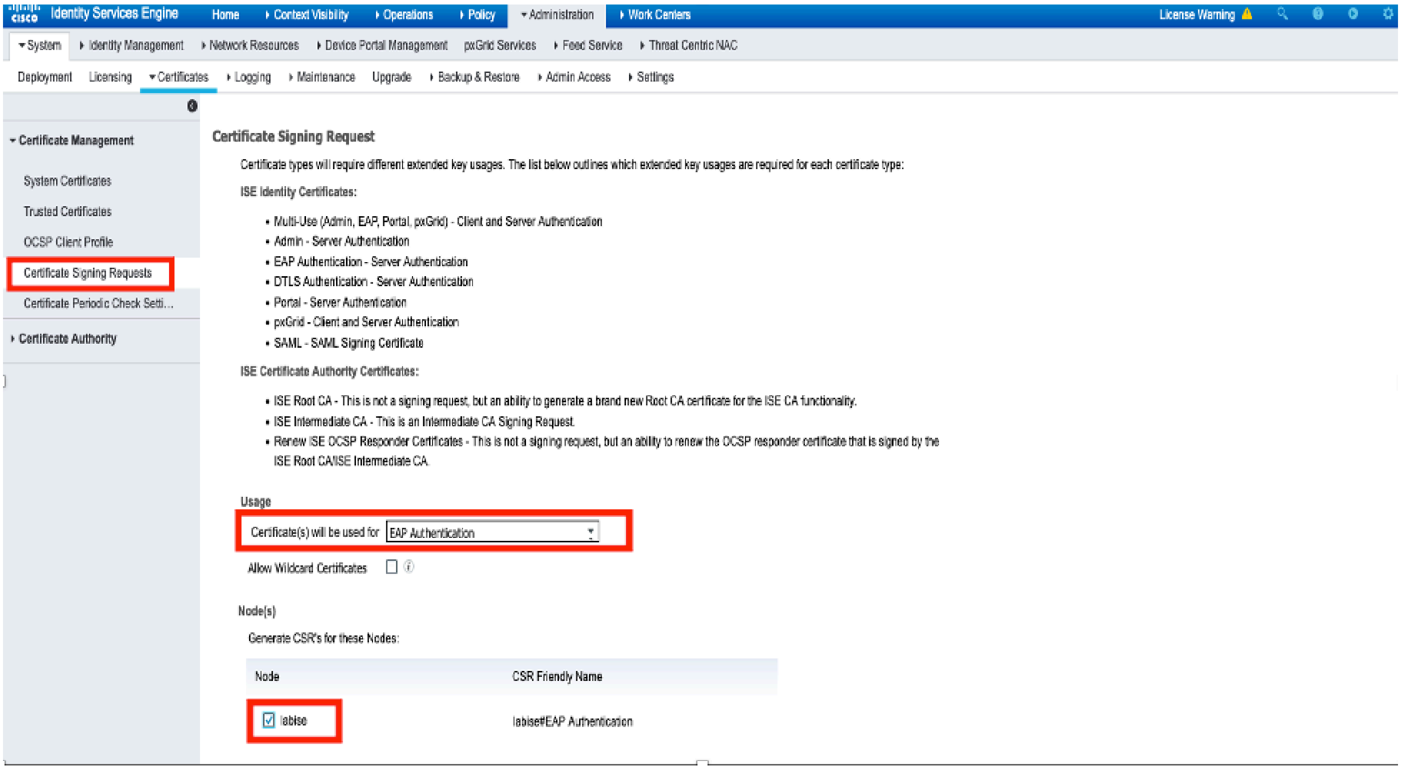
Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

| □ Friendly Name | Certificate Subject | Key Length | Portal group tag | Timestamp | Host |
|---|---|---|---|---|---|

No data available

第3步：要生成CSR，请导航到**Usage**，然后从**Certificate(s)is used**下拉选项中选择**EAP Authentication**，如图所示。



Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: EAP Authentication

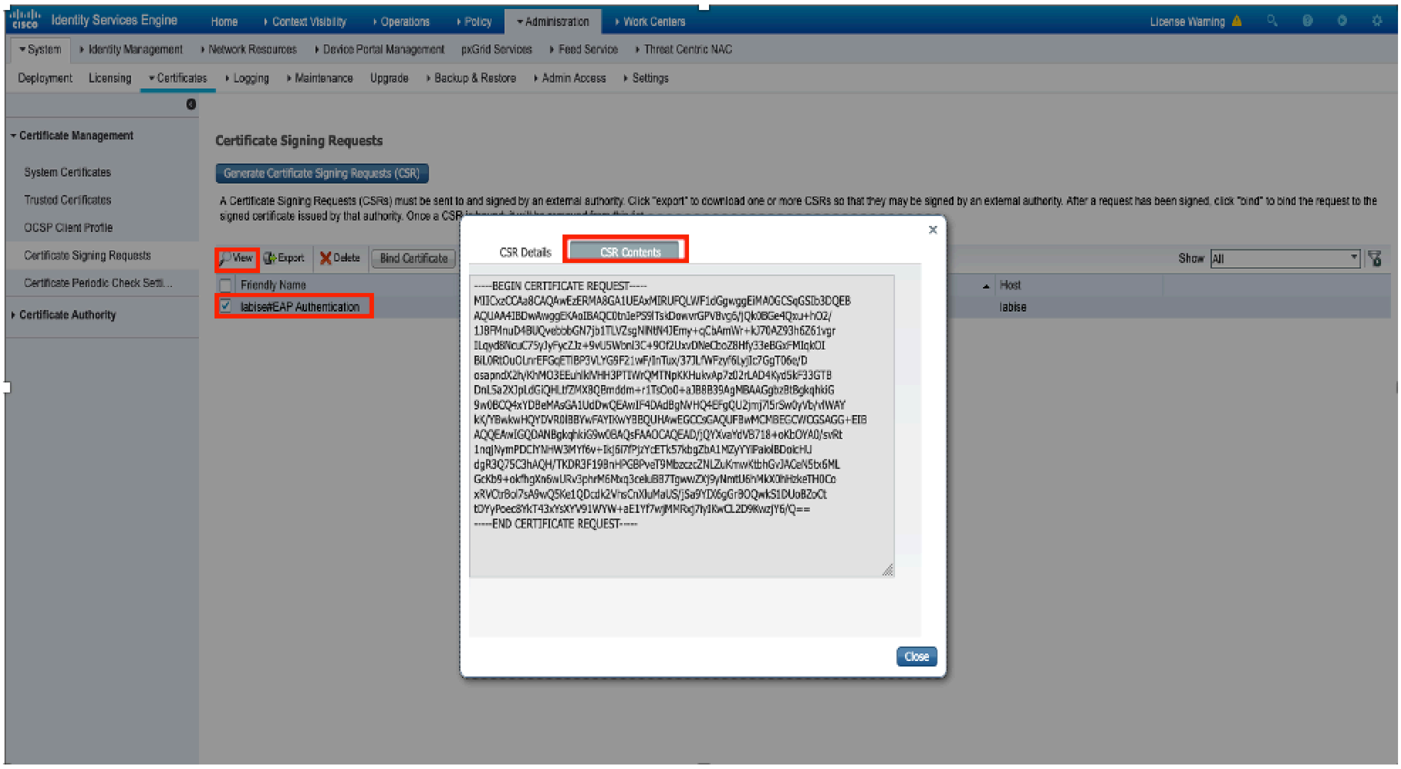
Allow Wildcard Certificates □

Node(s)

Generate CSR's for these Nodes:

| Node | CSR Friendly Name |
|---|---|
| ☑ labise | labise#EAP Authentication |

步骤4.可以查看ISE上生成的CSR。单击**View**，如图所示。



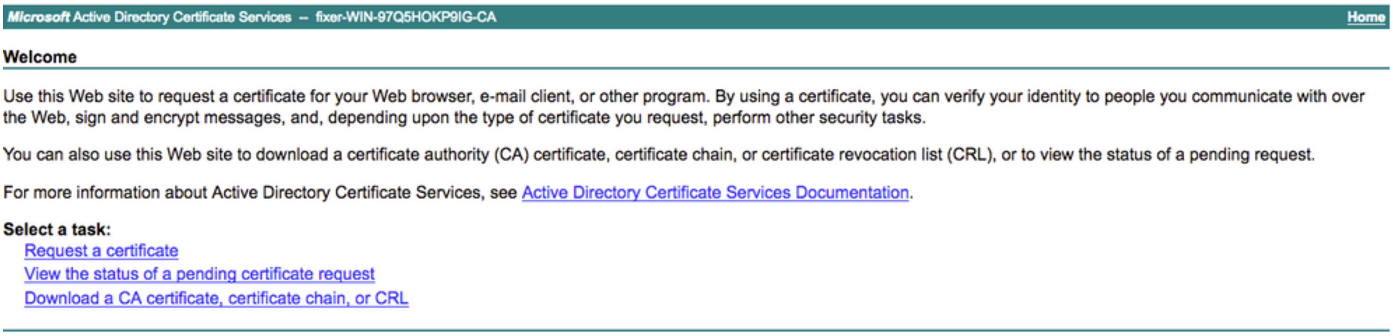
Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR

| | Friendly Name | Host |
|---|---|---|
| ☑ | labise#EAP Authentication | labise |

```
-----BEGIN CERTIFICATE REQUEST-----
MIICxzCCAa8CAQAwEzERMA8GA1UEAxMIRUFQLWF1dGgwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC0tn1ePS9lTskDowvrGPVBvg6/jQk0BGe4Qxu+hO2/
1J8FMnuD4BUQvebbbGN7jb1TLVZsgNlNtN4JEmy+qCbAmWr+kJ70AZ93h6Z61vgr
ILqyd8NcuC75yJyFycZJz+9vU5Wbnl3C+9Of2UxvDNeCboZ8Hfy33eBGxFMIqkOI
BiL0RtOuOLnrEFGqETIBP3VLYG9F21wF/InTux/37JL/WFzyf6LyjIc7GgT06e/D
osapndX2h/KhMO3EEuhlkNHH3PTIWrQMTNpKKHukvAp7z02rLAD4Kyd5kF33GTB
DnL5a2XJpLdGIQHLtfZMX8QBmddm+r1TsOo0+aJB8B39AgMBAAGgbzBtBgkqhkiG
9w0BCQ4xYDBeMAsGA1UdDwQEAwIF4DAdBgNVHQ4EFgQU2jmj7I5rSw0yVb/vlWAY
kK/YBwkwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBEGCWCGSAGG+EIB
AQQEAwIGQDANBgkqhkiG9w0BAQsFAAOCAQEAD/jQYXvaYdVB718+oKbOYA0/svRt
1nqjNymPDCIYNHW3MYf6v+Ikj6I7fPjzYcETk57kbgZbA1MZyYYIPaloIBDoicHJ
dgR3Q75C3hAQH/TKDR3F198nHPGBPvaT9MbzczcZNLZuKmwKtbhGvJACeN5tx6ML
GcKb9+okfhgXn6wURv3phrM6Mxq3celuBB7TgwwZXj9yNmtU6hMkX0hHzkeTH0Co
xRVCtrBol7sA9wQ5Ke1QDcdk2VnsCnXluMaUS/jSa9YDX6gGr8OQwkS1DUoBZoCt
tDYyPoec8YkT43xYsXYV91WYW+aE1Yf7wjMMRxj7ly1KwCL2D9KwzjY6/Q==
-----END CERTIFICATE REQUEST-----
```

步骤5.生成CSR后，浏览到CA服务器，然后单击**Request a certificate**，如图所示：



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

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

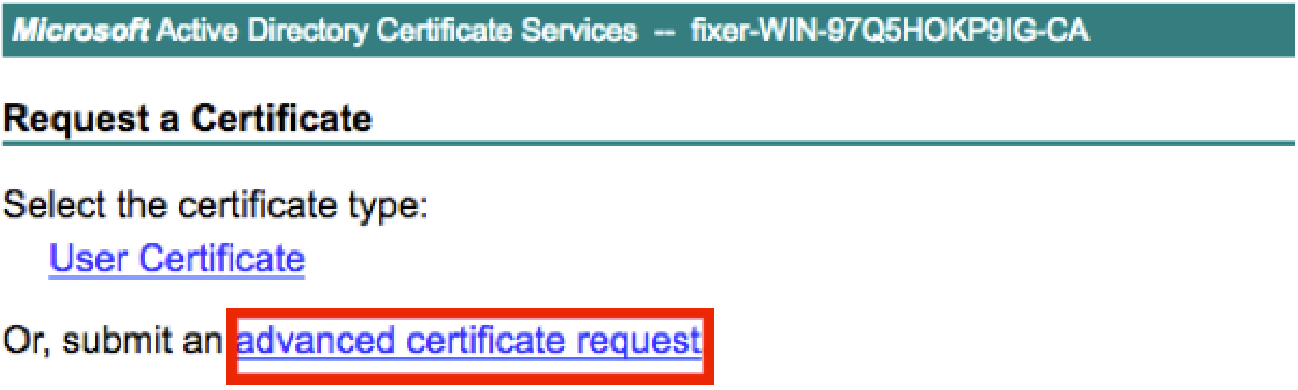
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

**Select a task:**

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

步骤6.请求证书后，您会获得**User Certificate**和**advanced certificate request**的选项，然后单击**advanced certificate request**，如图所示。



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

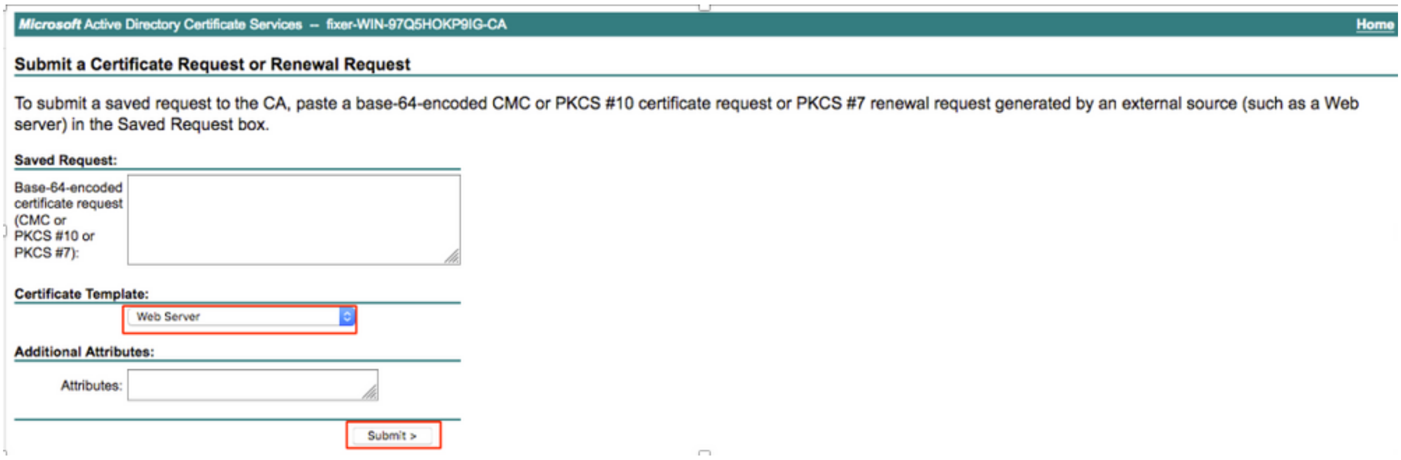
**Request a Certificate**

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，选择**Web Server**，然后单击**Submit**，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:

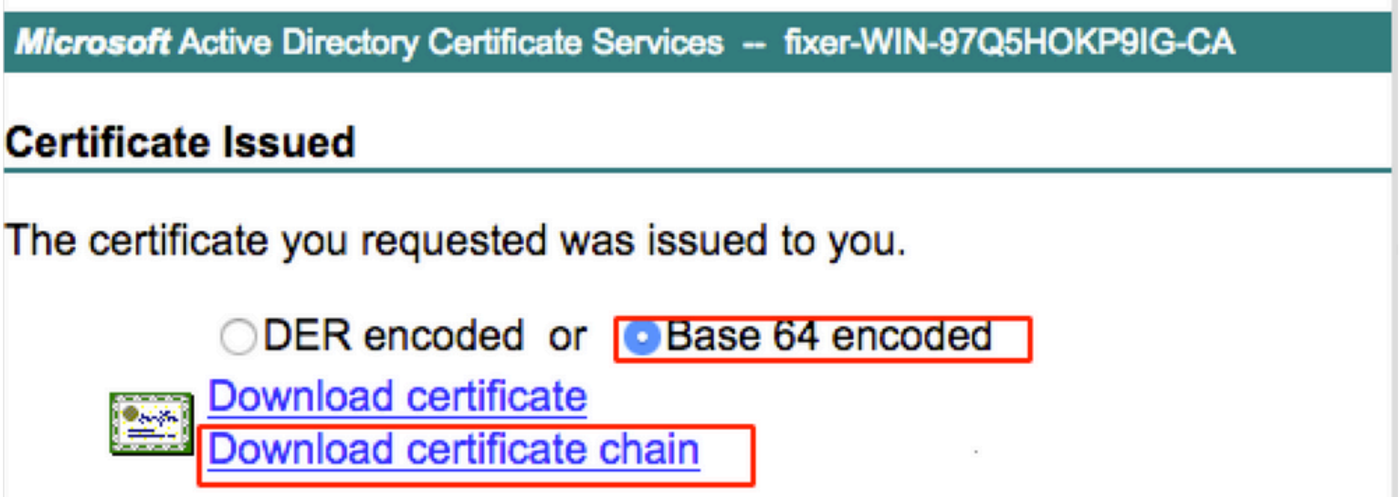
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template: Web Server

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 encoded**，然后单击**Download certificate chain**，如图所示。



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

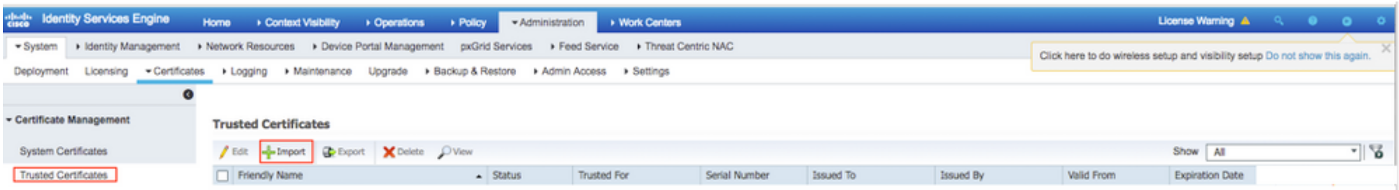
Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

步骤9.完成ISE服务器的证书下载。您可以提取证书，证书包含两个证书，一个根证书和其他中间证书。根证书可以在**管理>证书>受信任证书>导入**下导入，如图所示。

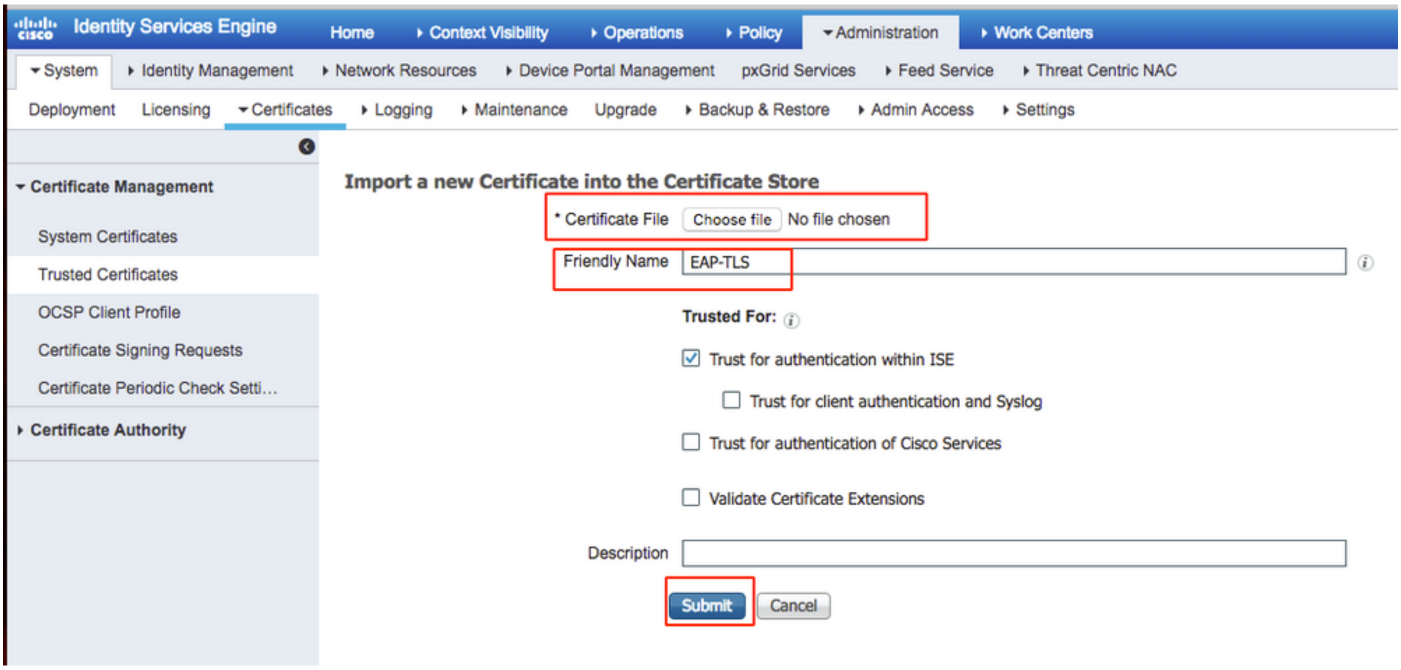


Click here to do wireless setup and visibility setup Do not show this again.

Trusted Certificates

Show: All

| □ | Friendly Name | Status | Trusted For | Serial Number | Issued To | Issued By | Valid From | Expiration Date |
|---|---|---|---|---|---|---|---|---|



Import a new Certificate into the Certificate Store

* Certificate File Choose file No file chosen

Friendly Name EAP-TLS

Trusted For:

☑ Trust for authentication within ISE

□ Trust for client authentication and Syslog

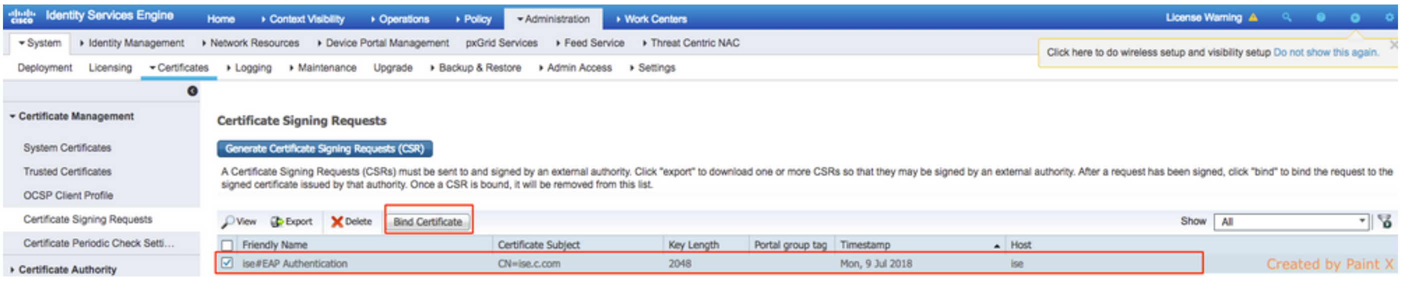
□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

Description

Submit Cancel

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



Certificate Signing Requests

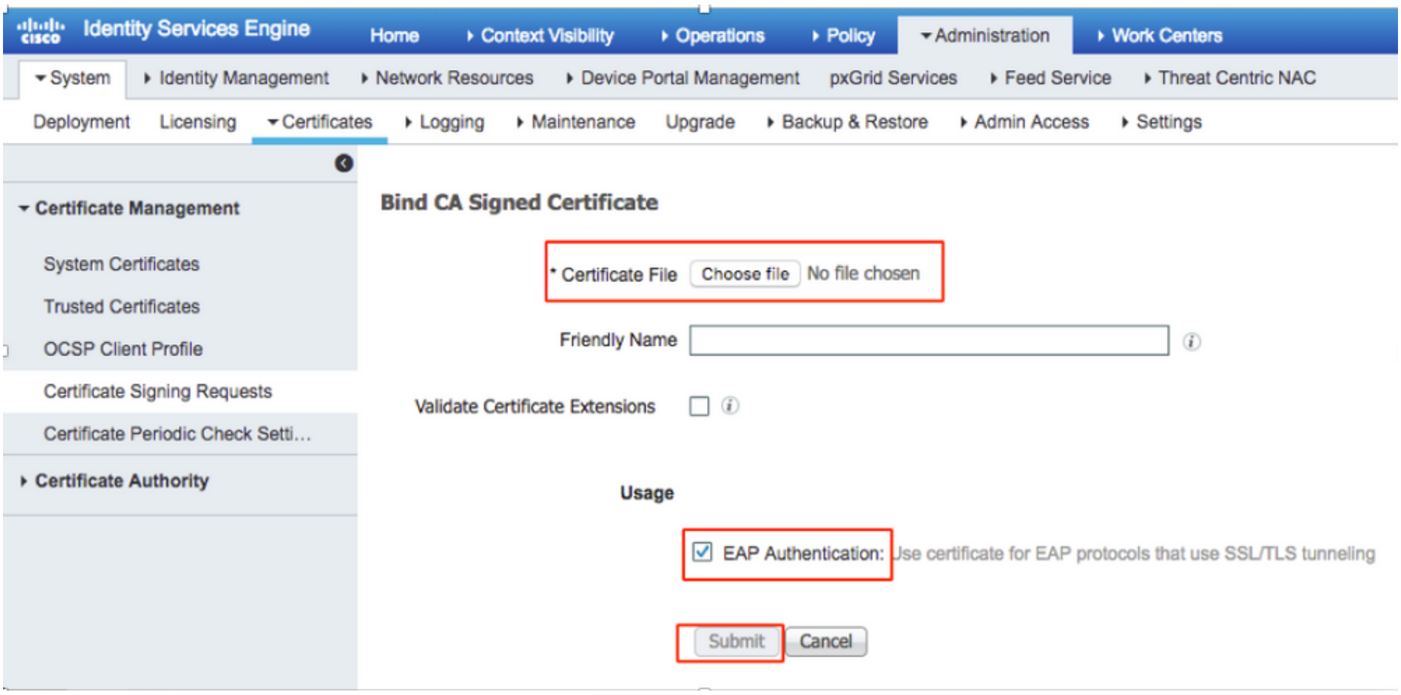
Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete Bind Certificate Show All

| □ | Friendly Name | Certificate Subject | Key Length | Portal group tag | Timestamp | Host |
|---|---|---|---|---|---|---|
| ☑ | ise#EAP Authentication | CN=ise.c.com | 2048 | | Mon, 9 Jul 2018 | ise |

步骤11.单击**Bind certificate**后，有一个选项可用于选择保存在桌面中的证书文件。浏览到中间证书，然后单击**Submit**，如图所示。



Bind CA Signed Certificate

* Certificate File Choose file No file chosen

Friendly Name

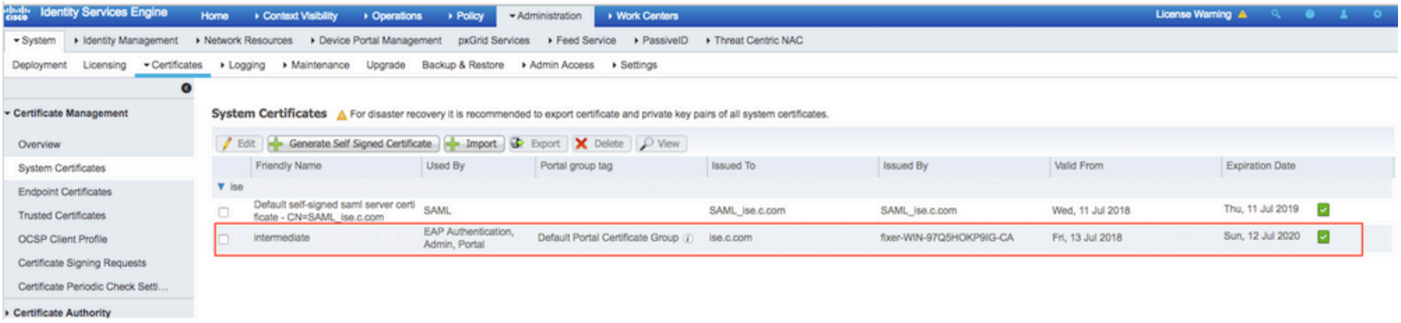
Validate Certificate Extensions □

Usage

☑ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

Submit Cancel

步骤12.要查看证书，请导航到**管理>证书>系统证书**，如图所示。



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

|  | Friendly Name | Used By | Portal group tag | Issued To | Issued By | Valid From | Expiration Date |  |
|---|---|---|---|---|---|---|---|---|
| ▼ ise |  |  |  |  |  |  |  |  |
| □ | Default self-signed saml server certificate - CN=SAML_ise.c.com | SAML |  | SAML_ise.c.com | SAML_ise.c.com | Wed, 11 Jul 2018 | Thu, 11 Jul 2019 | ✓ |
| □ | intermediate | EAP Authentication, Admin, Portal | Default Portal Certificate Group ⓘ | ise.c.com | fixer-WIN-97Q5HOKP9IG-CA | Fri, 13 Jul 2018 | Sun, 12 Jul 2020 | ✓ |

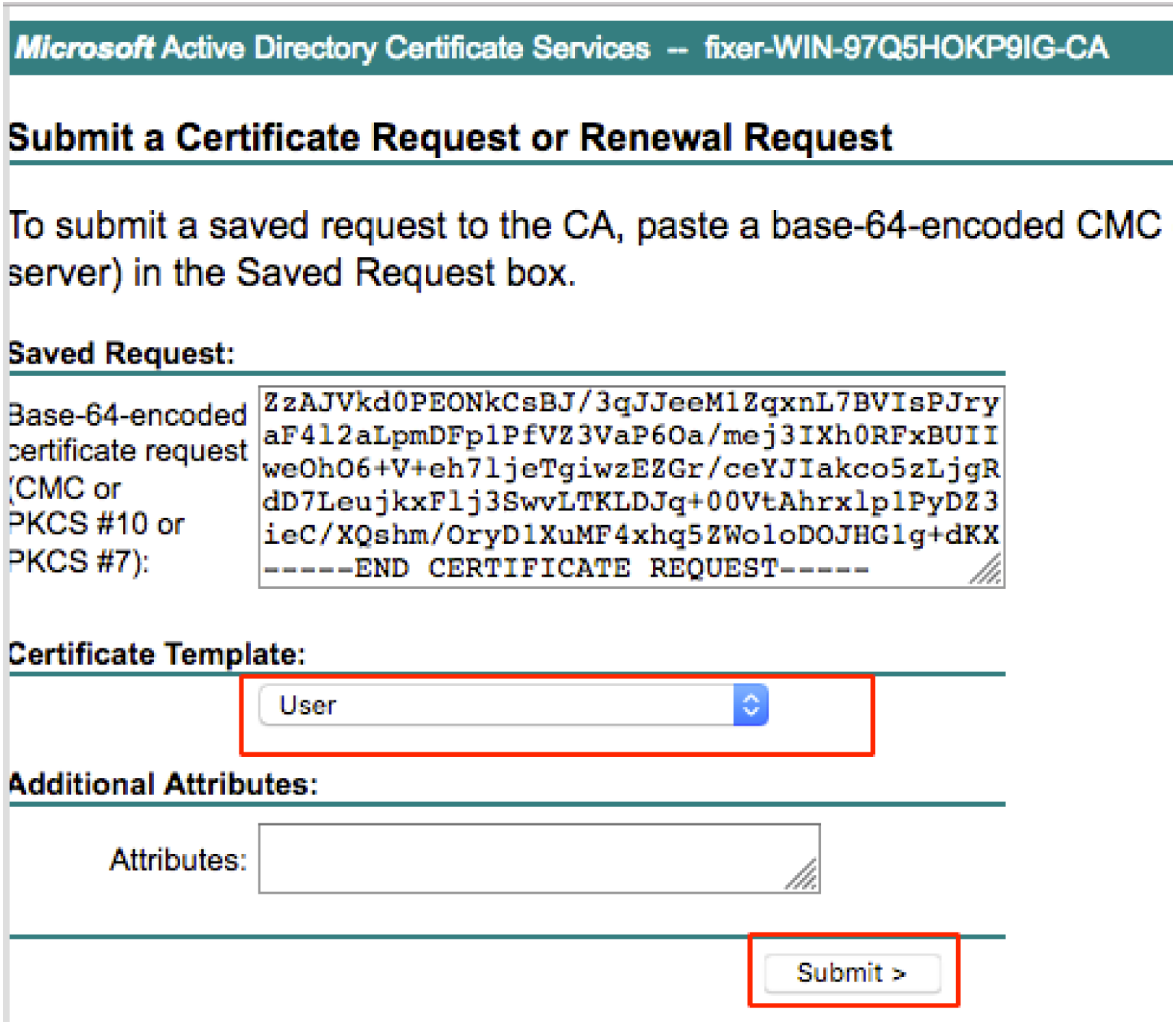
# EAP-TLS客户端

### 在客户端计算机上下载用户证书(Windows Desktop)

步骤1.要通过EAP-TLS对无线用户进行身份验证，您必须生成客户端证书。将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://sever ip addr/certsrv—

步骤2.请注意，CA必须与ISE的证书下载所用的相同。

为此，您需要浏览用于下载服务器证书的同一CA服务器。在同一个CA上，点击**Request a certificate**（请求证书），但这次您需要选择**User**作为证书模板，如图所示。



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

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/3qJJeeMlZqxnL7BVIsPJry
aF412aLpmDFplPfVZ3VaP6Oa/mej3IXh0RFxBUII
weOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR
dD7LeujkxFlj3SwvLTKLDJq+00VtAhrxlplPyDZ3
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHGlg+dKX
-----END CERTIFICATE REQUEST-----
```

Certificate Template: User

Additional Attributes:

Attributes:

步骤3.然后，按照之前对服务器执行的操作单击**download certificate chain**。

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)访问它。

1. 要打开MMC，请导航到**开始>运行> MMC**。
2. 导航到**文件>添加/删除管理单元**
3. 双击**证书**。
4. **选择计算机帐**户。
5. 选择**Local Computer** > **Finish**
6. 单击**OK**以退出“管理单元”窗口。
7. 点击**证书>个人>证书**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**。

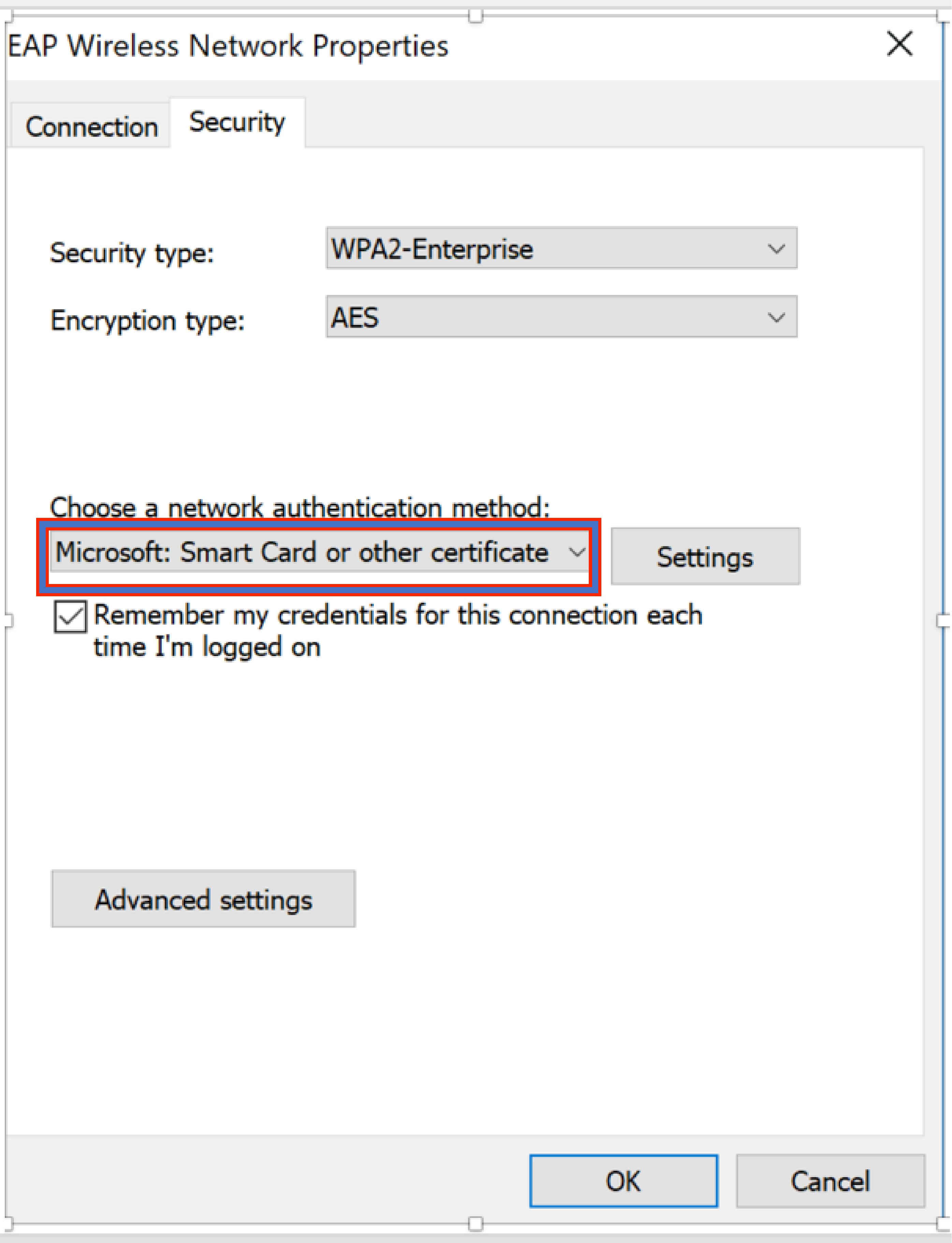
14. 选择**Automatically select the certificate store based on the type of certificate**。
15. 单击**完成并确定**

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

## EAP-TLS的无线配置文件

步骤1.更改之前为受保护的可扩展身份验证协议(PEAP)创建的无线配置文件，以便改用EAP-TLS。单击**EAP wireless profile**。

步骤2.选择**Microsoft:智能卡或其他证**书，然后点**击图**像中显示的OK。



EAP Wireless Network Properties

Security type: WPA2-Enterprise

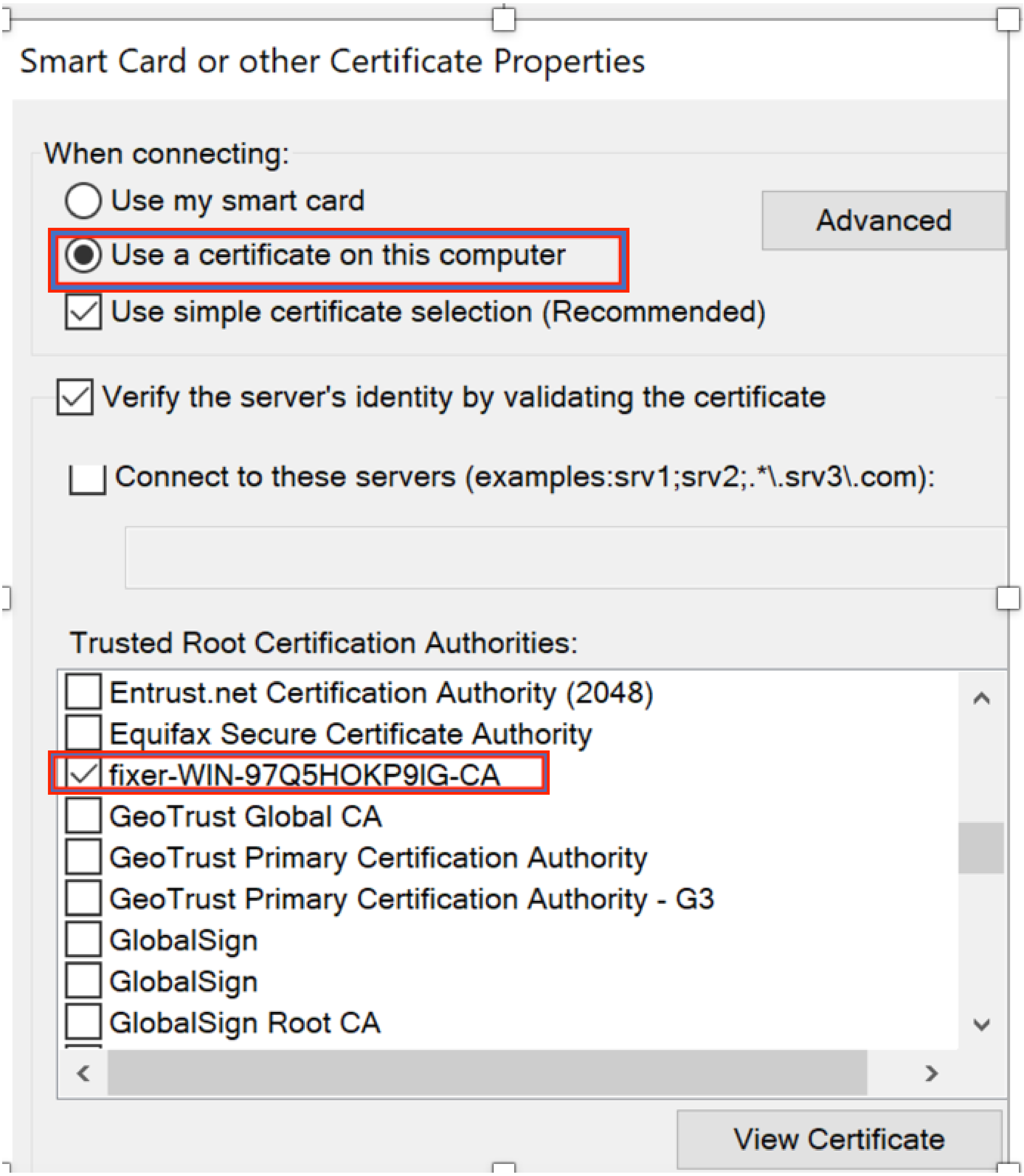
Encryption type: AES

Choose a network authentication method:

Microsoft: Smart Card or other certificate

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

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

☑ Use simple certificate selection (Recommended)

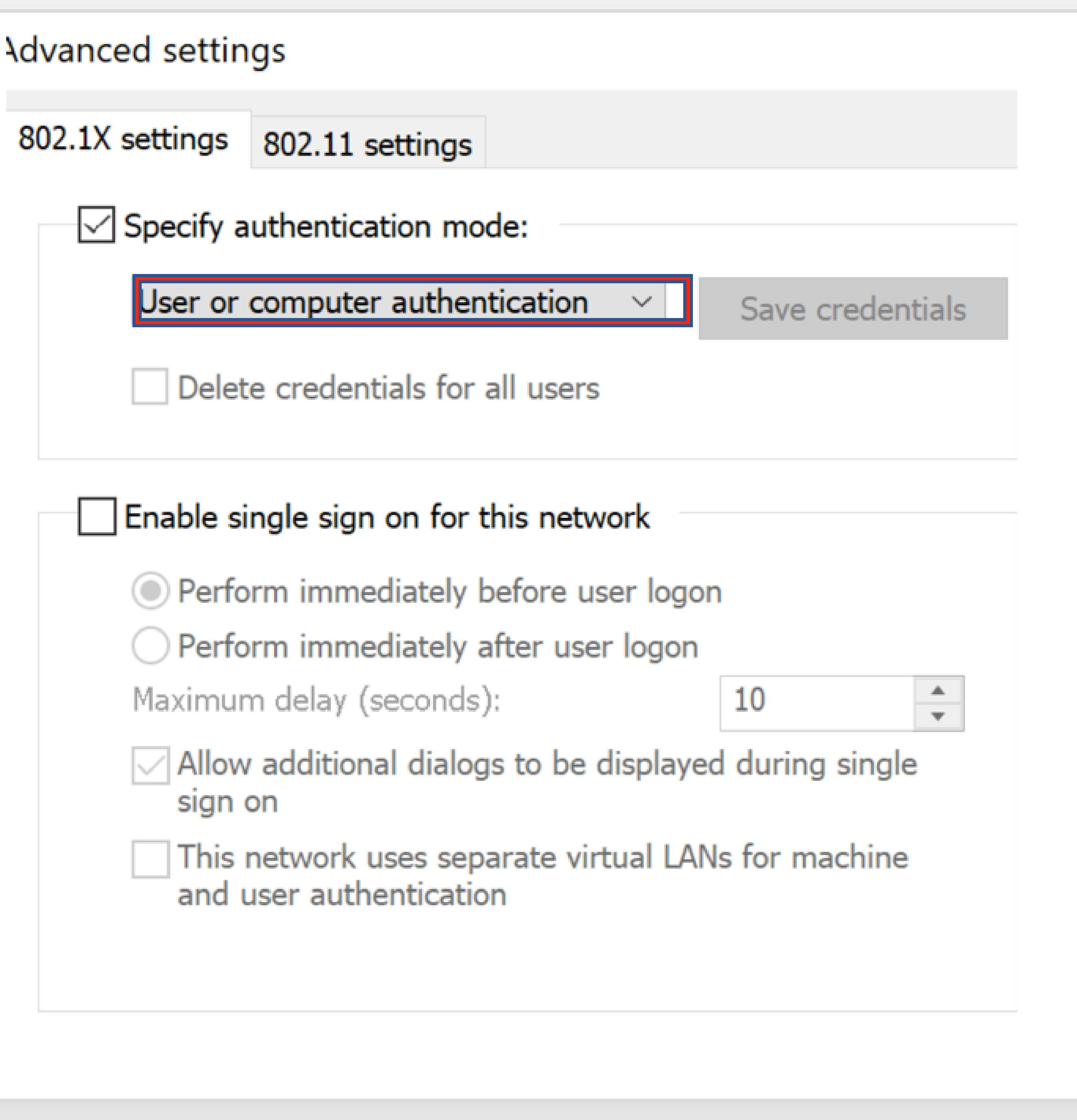
☑ Verify the server's identity by validating the certificate

□ 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

步骤4.单击**Advanced Settings**，然后从802.1x settings选项卡中选择**User or computer authentication**，如图所示。



\dvanced 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

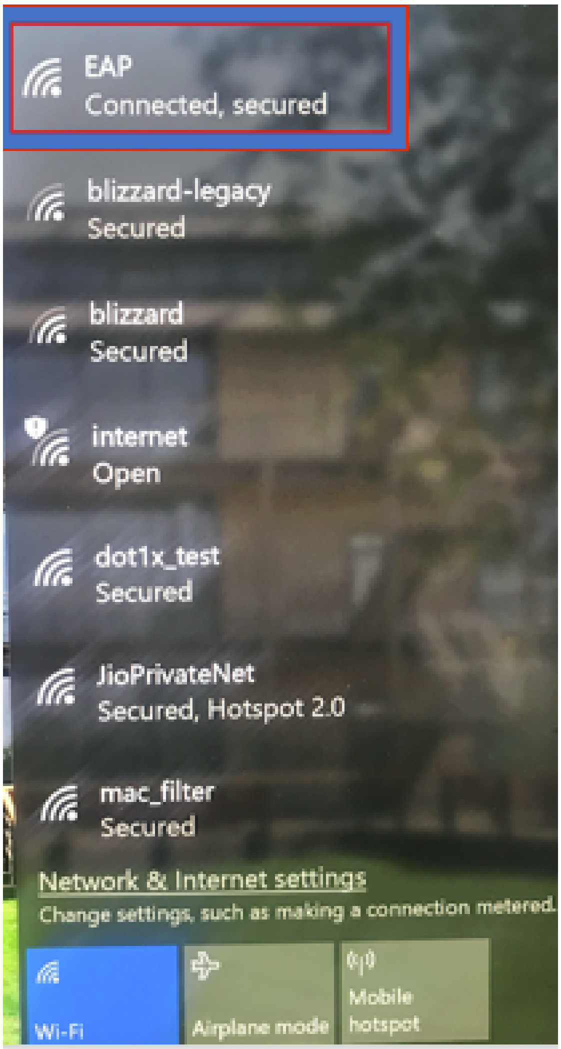
○ Perform immediately after user logon

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

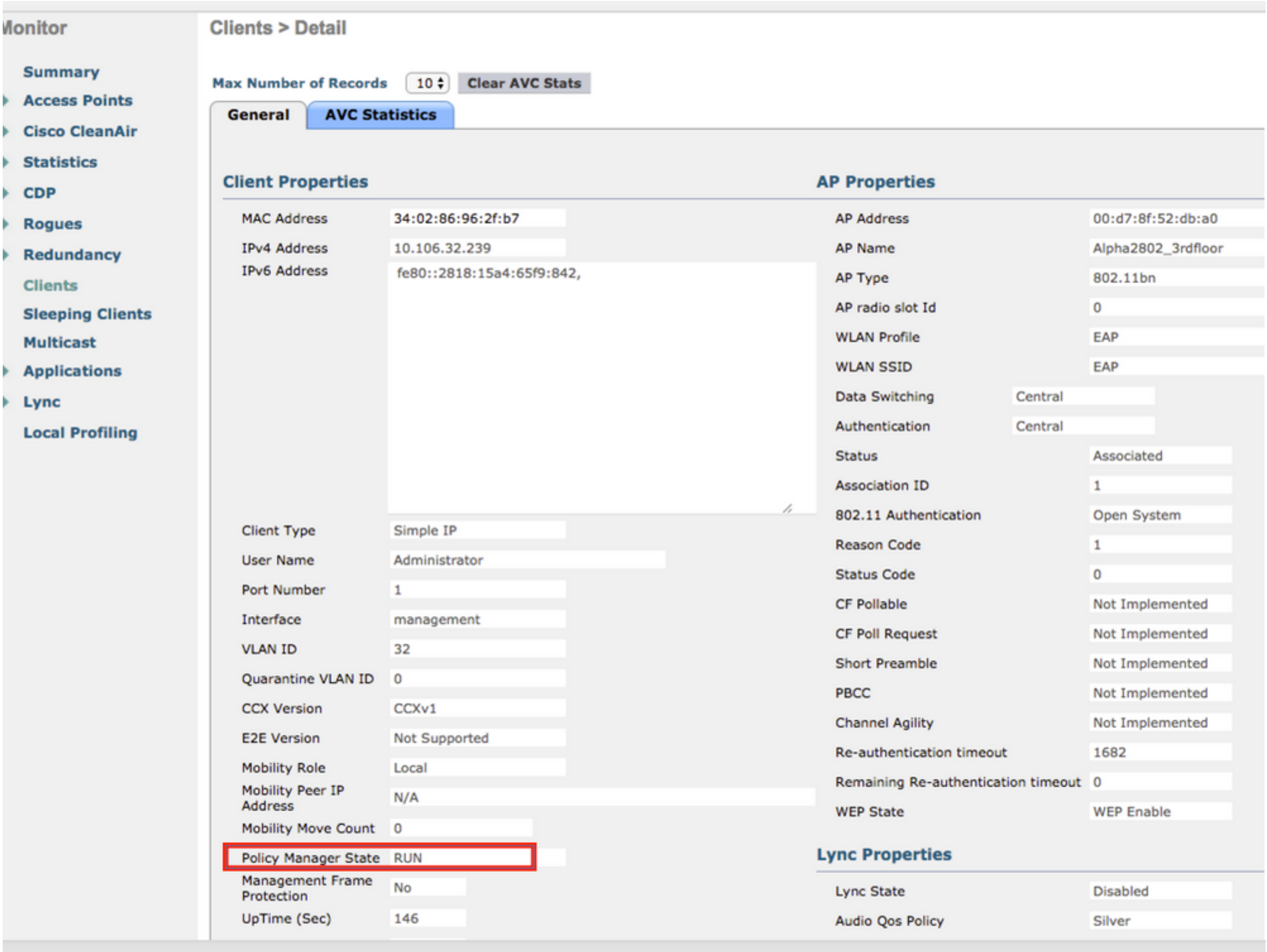
步骤5.现在，再次尝试连接到无线网络，选择正确的配置文件（本示例中的EAP）和**Connect**。如图所示，您已连接到无线网络。



# 验证

使用本部分可确认配置能否正常运行。

步骤1.客户端策略管理器状态必须显示为RUN。这意味着客户端已完成身份验证、获取的IP地址并准备传递如图所示的流量。



Clients > Detail

Max Number of Records 10

Client Properties

| | |
|---|---|
| MAC Address | 34:02:86:96:2f:b7 |
| IPv4 Address | 10.106.32.239 |
| IPv6 Address | fe80::2818:15a4:65f9:842, |
| Client Type | Simple IP |
| User Name | Administrator |
| Port Number | 1 |
| Interface | management |
| VLAN ID | 32 |
| Quarantine VLAN ID | 0 |
| CCX Version | CCXv1 |
| E2E Version | Not Supported |
| Mobility Role | Local |
| Mobility Peer IP Address | N/A |
| Mobility Move Count | 0 |
| Policy Manager State | RUN |
| Management Frame Protection | No |
| UpTime (Sec) | 146 |

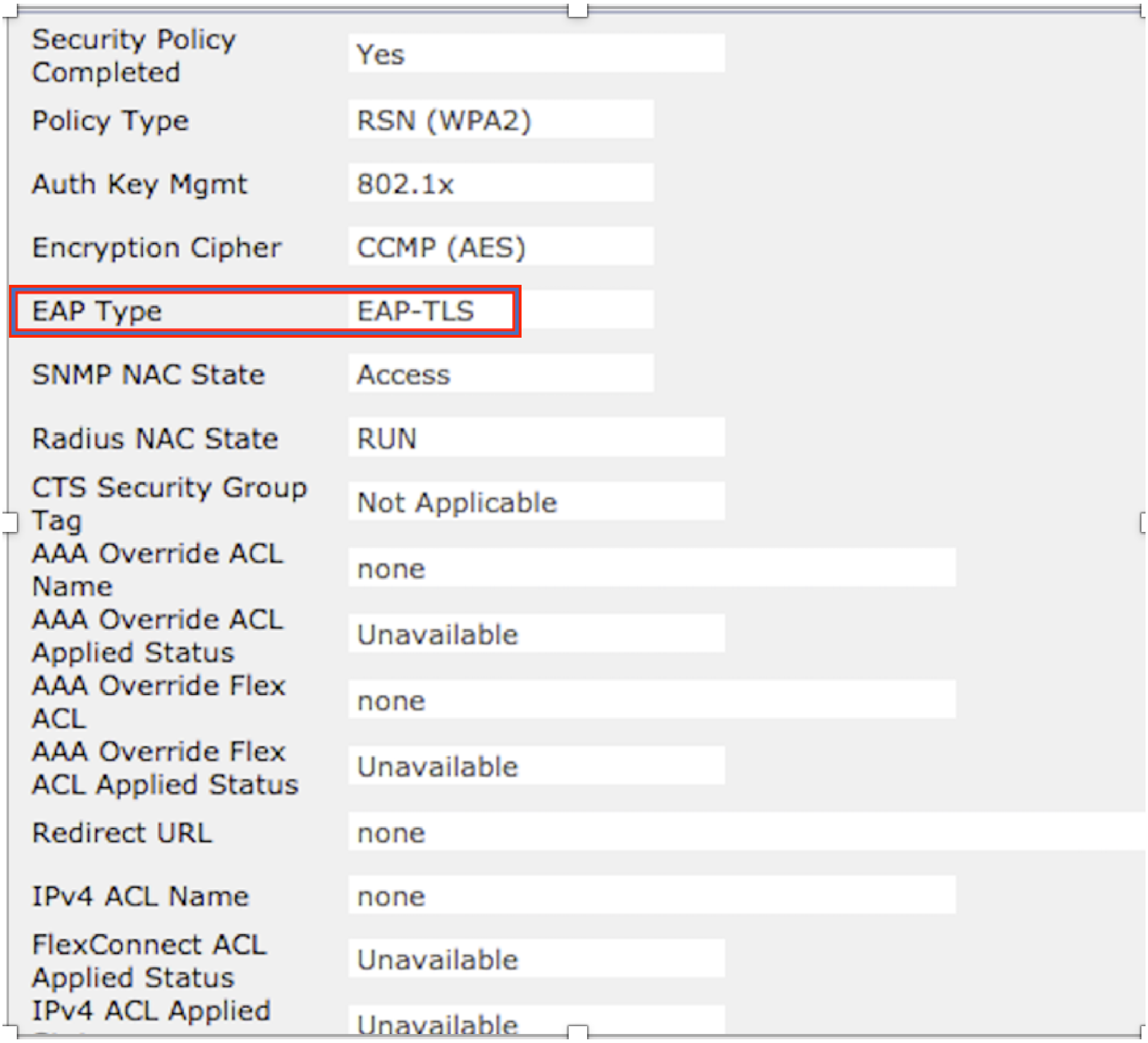
AP Properties

| | |
|---|---|
| AP Address | 00:d7:8f:52:db:a0 |
| AP Name | Alpha2802_3rdfloor |
| AP Type | 802.11bn |
| AP radio slot Id | 0 |
| WLAN Profile | EAP |
| WLAN SSID | EAP |
| Data Switching | Central |
| Authentication | Central |
| Status | Associated |
| Association ID | 1 |
| 802.11 Authentication | Open System |
| Reason Code | 1 |
| Status Code | 0 |
| CF Pollable | Not Implemented |
| CF Poll Request | Not Implemented |
| Short Preamble | Not Implemented |
| PBCC | Not Implemented |
| Channel Agility | Not Implemented |
| Re-authentication timeout | 1682 |
| Remaining Re-authentication timeout | 0 |
| WEP State | WEP Enable |

Lync Properties

| | |
|---|---|
| Lync State | Disabled |
| Audio Qos Policy | Silver |

步骤2.在客户端详细信息页面中验证WLC上正确的EAP方法，如图所示。



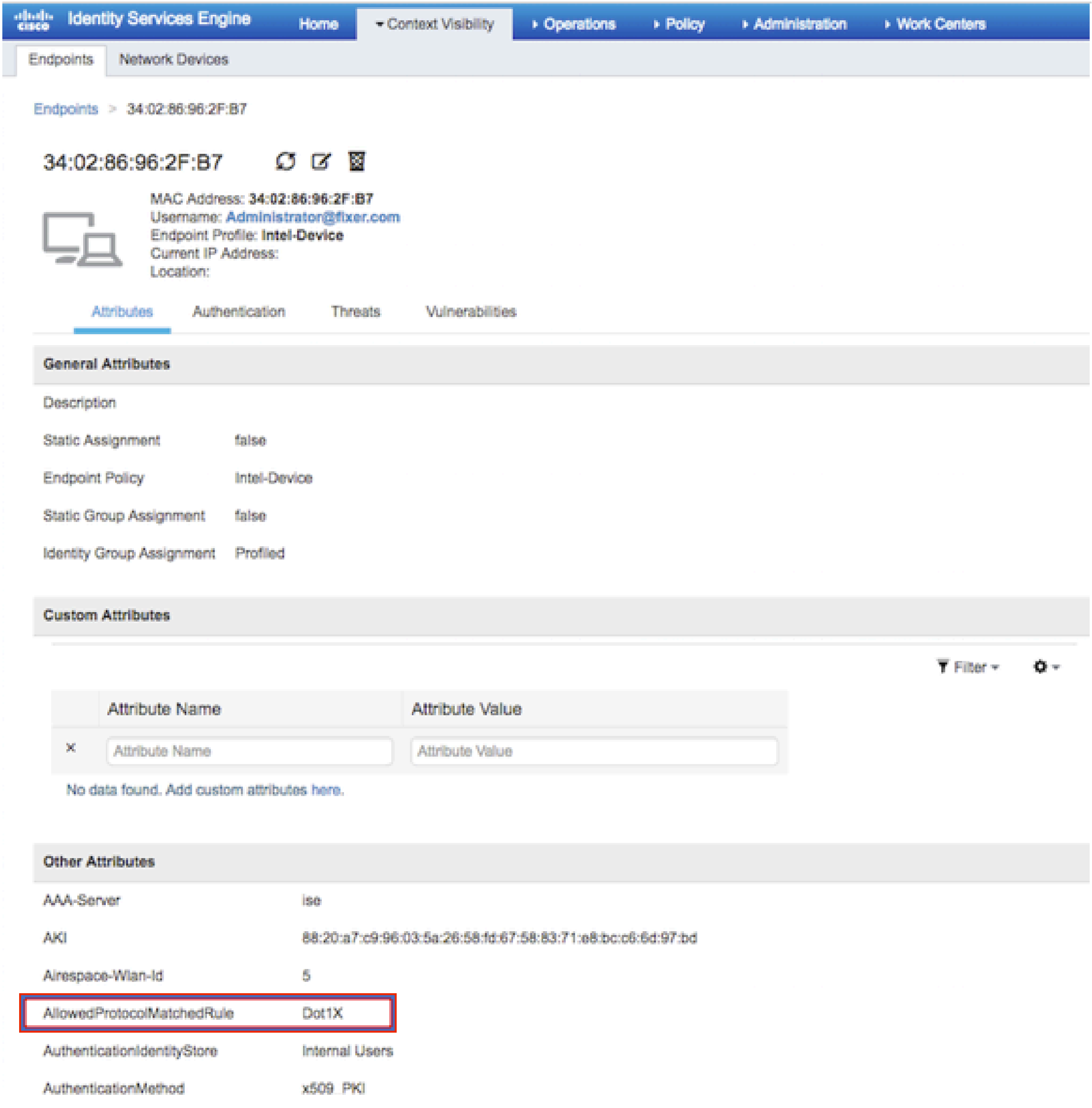
| | |
|---|---|
| Security Policy Completed | Yes |
| Policy Type | RSN (WPA2) |
| Auth Key Mgmt | 802.1x |
| Encryption Cipher | CCMP (AES) |
| EAP Type | EAP-TLS |
| SNMP NAC State | Access |
| Radius NAC State | RUN |
| CTS Security Group Tag | Not Applicable |
| AAA Override ACL Name | none |
| AAA Override ACL Applied Status | Unavailable |
| AAA Override Flex ACL | none |
| AAA Override Flex ACL Applied Status | Unavailable |
| Redirect URL | none |
| IPv4 ACL Name | none |
| FlexConnect ACL Applied Status | Unavailable |
| IPv4 ACL Applied | Unavailable |

步骤3.以下是来自控制器CLI的客户端详细信息（剪切的输出）：

```
(Cisco Controller-Standby) >show client detail 34:02:86:96:2f:b7
Client MAC Address............................... 34:02:86:96:2f:b7
Client Username ................................. Administrator
AP MAC Address................................... 00:d7:8f:52:db:a0
AP Name.......................................... Alpha2802_3rdfloor
AP radio slot Id................................. 0
Client State..................................... Associated
Wireless LAN Id.................................. 5
Wireless LAN Network Name (SSID)................. EAP
Wireless LAN Profile Name........................ EAP
Hotspot (802.11u)................................ Not Supported
BSSID............................................ 00:d7:8f:52:db:a4
Connected For ................................... 48 secs
Channel.......................................... 1
IP Address....................................... 10.106.32.239
Gateway Address.................................. 10.106.32.1
Netmask.......................................... 255.255.255.0
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
```

第4步：在ISE上，导航到**情景可视性>端点>属性**，如图所示。



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:

**General Attributes**

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

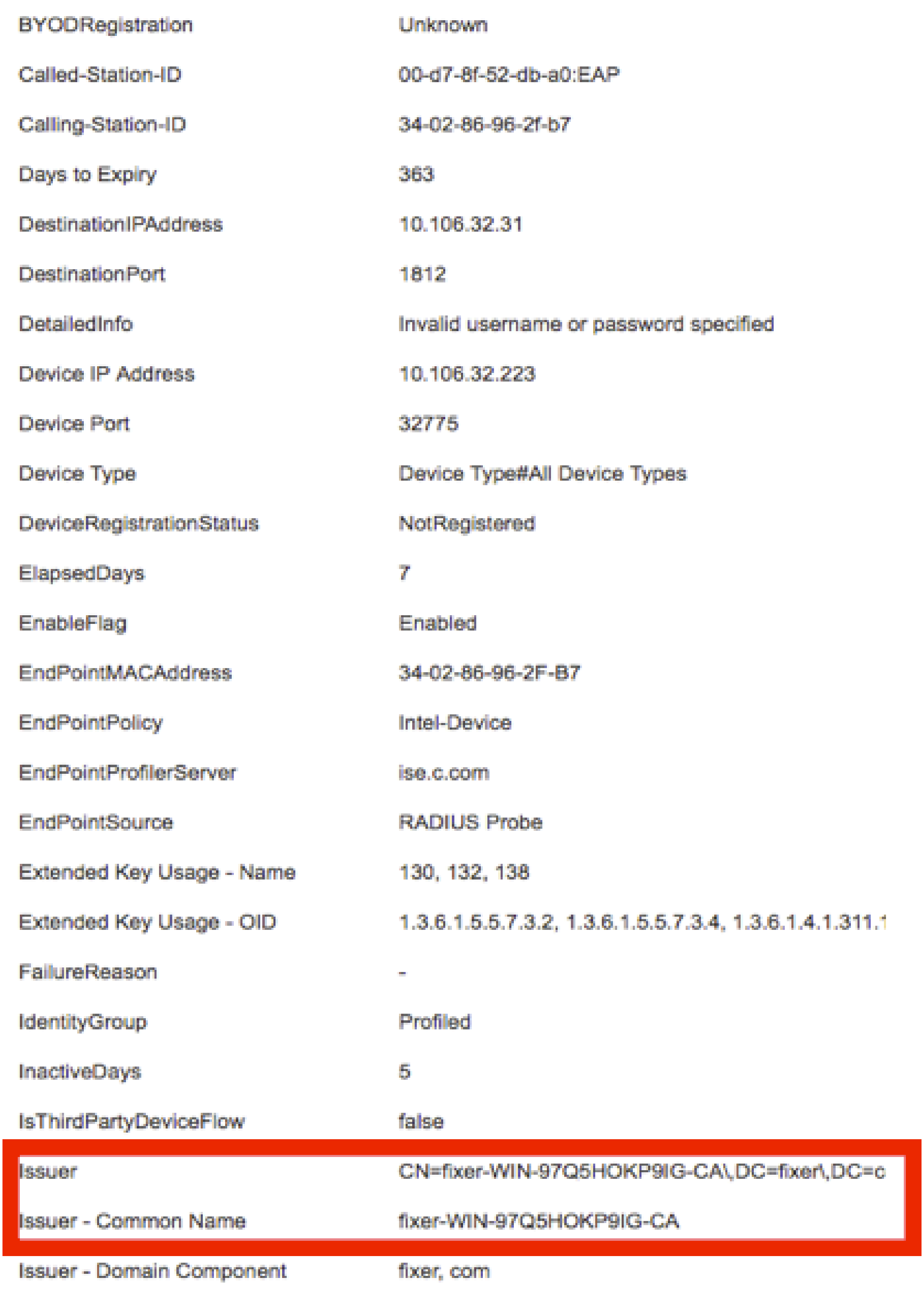
**Custom Attributes**

| Attribute Name | Attribute Value |
|---|---|
| Attribute Name | Attribute Value |

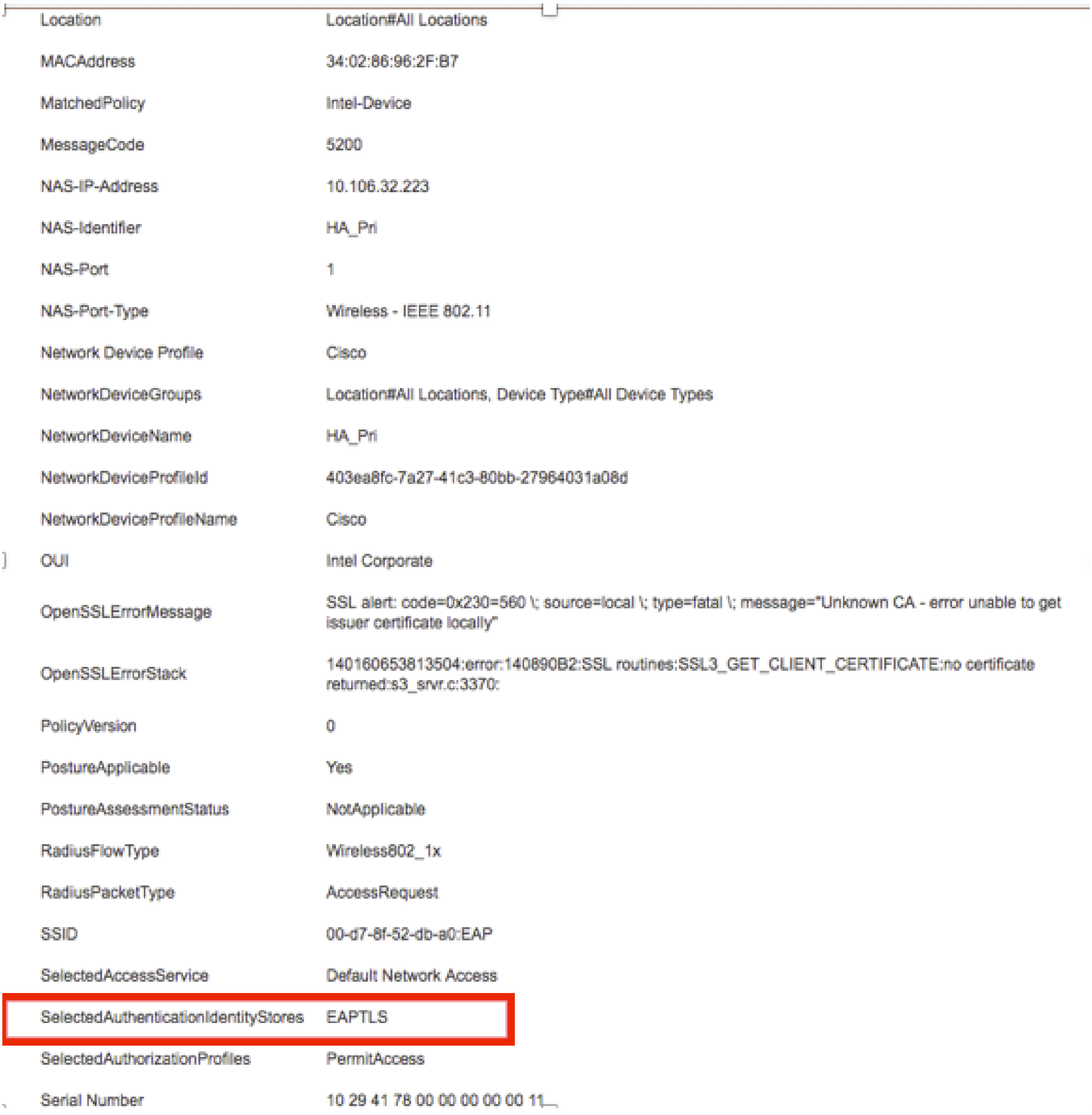
No data found. Add custom attributes here.

**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 | 5 |
| AllowedProtocolMatchedRule | Dot1X |
| AuthenticationIdentityStore | Internal Users |
| AuthenticationMethod | x509_PKI |



| | |
|---|---|
| BYODRegistration | Unknown |
| Called-Station-ID | 00-d7-8f-52-db-a0:EAP |
| Calling-Station-ID | 34-02-86-96-2f-b7 |
| Days to Expiry | 363 |
| DestinationIPAddress | 10.106.32.31 |
| DestinationPort | 1812 |
| DetailedInfo | Invalid username or password specified |
| Device IP Address | 10.106.32.223 |
| Device Port | 32775 |
| Device Type | Device Type#All Device Types |
| DeviceRegistrationStatus | NotRegistered |
| ElapsedDays | 7 |
| 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, 1.3.6.1.4.1.311.1 |
| FailureReason | - |
| IdentityGroup | Profiled |
| InactiveDays | 5 |
| IsThirdPartyDeviceFlow | false |
| Issuer | CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=c |
| Issuer - Common Name | fixer-WIN-97Q5HOKP9IG-CA |
| Issuer - Domain Component | fixer, com |



| | |
|---|---|
| Location | Location#All Locations |
| MACAddress | 34:02:86:96:2F:B7 |
| MatchedPolicy | Intel-Device |
| MessageCode | 5200 |
| NAS-IP-Address | 10.106.32.223 |
| NAS-Identifier | HA_Pri |
| NAS-Port | 1 |
| NAS-Port-Type | Wireless - IEEE 802.11 |
| Network Device Profile | Cisco |
| NetworkDeviceGroups | Location#All Locations, Device Type#All Device Types |
| NetworkDeviceName | HA_Pri |
| 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" |
| OpenSSLErrorStack | 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 | AccessRequest |
| SSID | 00-d7-8f-52-db-a0:EAP |
| SelectedAccessService | Default Network Access |
| SelectedAuthenticationIdentityStores | EAPTLS |
| SelectedAuthorizationProfiles | PermitAccess |
| Serial Number | 10 29 41 78 00 00 00 00 00 11 |

# 故障排除

当前没有可用于对此配置进行故障排除的特定信息。