使用无线LAN控制器和身份服务引擎的EAP-FAST身份验证

目录

简介

本文档说明如何使用外部RADIUS服务器配置无线局域网控制器(WLC)以进行可扩展身份验证协议(EAP) — 通过安全隧道进行灵活身份验证(FAST)身份验证。此配置示例使用身份服务引擎(ISE)作为外部RADIUS服务器对无线客户端进行身份验证。

本文档重点介绍如何为无线客户端配置匿名和经过身份验证的带内（自动）保护访问凭证(PAC)调配的ISE。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解轻量接入点 (LAP) 和 Cisco WLC 配置的基础知识
- CAPWAP协议的基本知识
- 了解如何配置外部RADIUS服务器，例如Cisco ISE
- 有关通用EAP框架的功能知识
- 有关安全协议（如MS-CHAPv2和EAP-GTC）的基本知识，以及有关数字证书的知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件 8.8.111.0 版本的 Cisco 5520 系列 WLC思科4800系列APAnyConnect NAM。思科安全ISE版本2.3.0.298运行版本15.2(4)E1的思科3560-CX系列交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

EAP-FAST协议是可公开访问的IEEE 802.1X EAP类型，思科开发此类型是为了支持无法实施强密码策略且希望部署不需要数字证书的802.1X EAP类型的客户。

EAP-FAST协议是使用传输级安全(TLS)隧道加密EAP事务的客户端 — 服务器安全架构。EAP-FAST隧道建立基于用户独有的强机密。这些强机密称为PAC，ISE使用仅知道ISE的主密钥生成PAC。

EAP-FAST分三个阶段进行：

- **阶段零（自动PAC调配阶段）** - EAP-FAST阶段零，可选阶段是隧道保护的方法，为请求网络访问的用户提供EAP-FAST最终用户客户端的PAC。**向最终用户客户端提供PAC是第零阶段的唯一目的。注意：**阶段零是可选的，因为PAC也可以手动调配到客户端，而不是使用阶段零。有关详细信息，请参阅本文档的PAC调配模式部分。
- **第1阶**段 — 在第1阶段，ISE和最终用户客户端根据用户的PAC凭证建立TLS隧道。此阶段要求最终用户客户端已为尝试获取网络访问权限的用户提供PAC，并且PAC基于尚未过期的主密钥。EAP-FAST的第一阶段未启用任何网络服务。
- **第2阶段** — 在第2阶段，使用TLS隧道内EAP-FAST支持的内部EAP方法将用户身份验证凭据安全地传递到使用客户端和RADIUS服务器之间的PAC创建的RADIUS。EAP-GTC、TLS和MS-CHAP作为内部EAP方法受支持。EAP-FAST不支持其他EAP类型。

有关详细信息，请参阅EAP-FAST的工作方式。

PAC

PAC是强共享密钥，使ISE和EAP-FAST最终用户客户端能够相互验证并建立TLS隧道以在EAP-FAST第2阶段使用。ISE使用活动主密钥和用户名生成PAC。

PAC包括：

- **PAC-Key** — 绑定到客户端（和客户端设备）和服务器标识的共享密钥。
- **PAC Opaque** — 客户端缓存并传递给服务器的不透明字段。服务器恢复PAC-Key和客户端身份，以与客户端相互进行身份验证。
- **PAC-Info** — 至少包括服务器的标识，以使客户端能够缓存不同的PAC。或者，它包括其他信息，如PAC的到期时间。

PAC调配模式

如前所述，零阶段是可选阶段。

EAP-FAST提供两个选项来为客户端调配PAC:

- **自动PAC调配（EAP-FAST阶段0或带内PAC调配）**
- **手动（带外）PAC调配**

带内/自动PAC调配通过安全网络连接向最终用户客户端发送新PAC。自动PAC调配无需网络用户或ISE管理员的干预，前提是您配置ISE和最终用户客户端以支持自动调配。

最新的EAP-FAST版本支持两个不同的带内PAC调配配置选项：

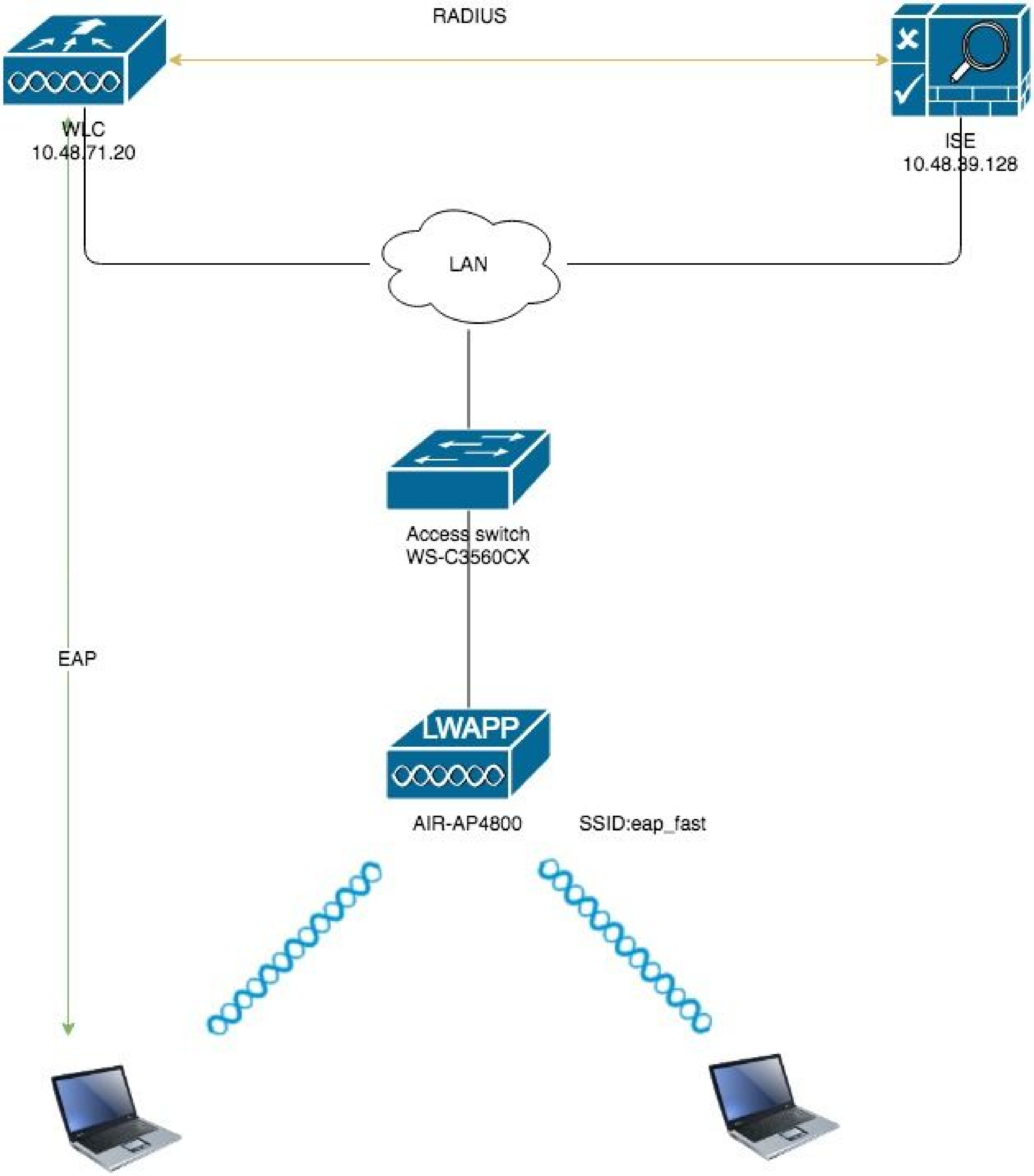
- **匿名带内PAC调配**
- **经过身份验证的带内PAC调配**

注意：本文档讨论这些带内PAC调配方法及其配置方法。

带外/手动PAC调配需要ISE管理员生成PAC文件，然后必须将其分发给适用的网络用户。用户必须使用其PAC文件配置最终用户客户端。

配置

网络图



配置

为EAP-FAST身份验证配置WLC

要配置WLC以进行EAP-FAST身份验证，请执行以下步骤：

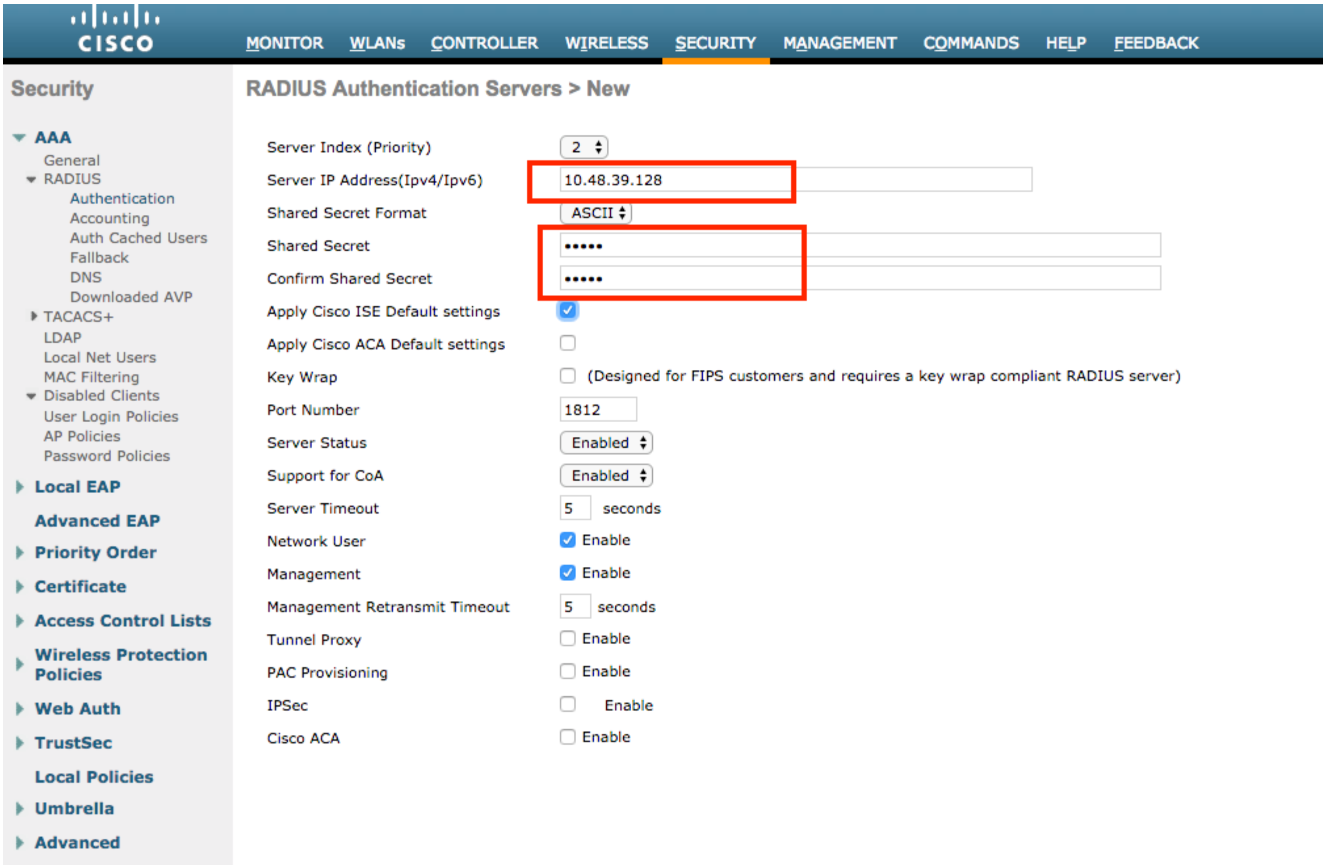
1. 配置 WLC 以便通过外部 RADIUS 服务器进行 RADIUS 身份验证
2. 为EAP-FAST身份验证配置WLAN

配置 WLC 以便通过外部 RADIUS 服务器进行 RADIUS 身份验证

需要配置 WLC 以便将用户凭证转发到外部 RADIUS 服务器。随后，外部 RADIUS 服务器使用 EAP-FAST 验证用户凭证，并提供对无线客户端的访问。

完成以下这些步骤，为外部 RADIUS 服务器配置 WLC：

1. 从控制器的 GUI 中选择**安全性和“RADIUS 身份验证”，以便显示“RADIUS 身份验证服务器”页。**然后，请点击**new来定义RADIUS服务器。**
2. 在 **RADIUS Authentication Servers > New 页上定义 RADIUS 服务器参数。**这些参数包括：RADIUS 服务器的 IP 地址共享密钥端口号服务器状态本文档使用IP地址为10.48.39.128的ISE服务器。



RADIUS Authentication Servers > New

Server Index (Priority) 2
Server IP Address(Ipv4/Ipv6) 10.48.39.128
Shared Secret Format ASCII
Shared Secret •••••
Confirm Shared Secret •••••
Apply Cisco ISE Default settings ☑
Apply Cisco ACA Default settings □
Key Wrap □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number 1812
Server Status Enabled
Support for CoA Enabled
Server Timeout 5 seconds
Network User ☑ Enable
Management ☑ Enable
Management Retransmit Timeout 5 seconds
Tunnel Proxy □ Enable
PAC Provisioning □ Enable
IPSec □ Enable
Cisco ACA □ Enable

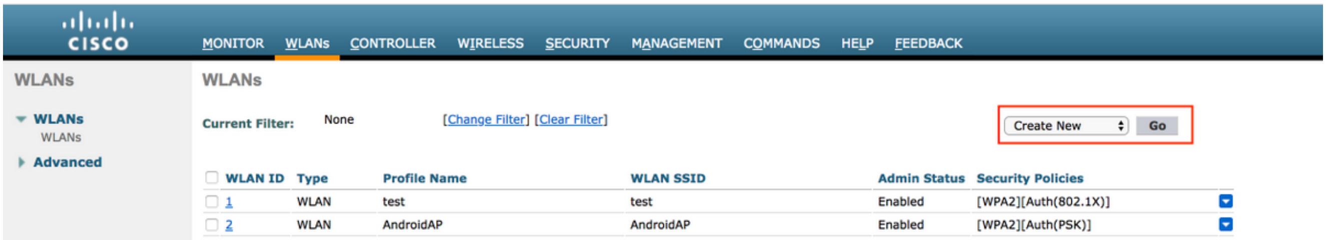
3. 单击 **应用**。

为EAP-FAST身份验证配置WLAN

接下来，配置客户端用于连接到无线网络的WLAN进行EAP-FAST身份验证并分配给动态接口。本示例中配置的WLAN名称是**eap fast**。本例将此 WLAN 分配到管理接口。

要配置eap快速WLAN及其相**关参**数，请完成以下步骤：

1. 从控制器的 GUI 中单击 **WLAN 以显示“WLAN”页。**此页列出了控制器上现有的 WLAN。
2. 单击 **New 以创建新的 WLAN。**

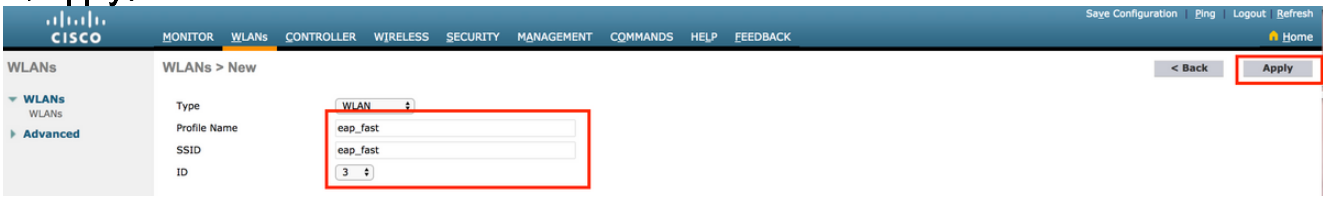


WLANs

Current Filter: None [Change Filter] [Clear Filter]

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 1	WLAN	test	test	Enabled	[WPA2][Auth(802.1X)]
□ 2	WLAN	AndroidAP	AndroidAP	Enabled	[WPA2][Auth(PSK)]

3. 在“WLAN”>“新建”页上配置eap_fast WLAN SSID名称、配置文件名称和WLAN ID。然后，单击 **Apply**。


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
WLANs
Advanced
< Back
Apply

WLANs > New

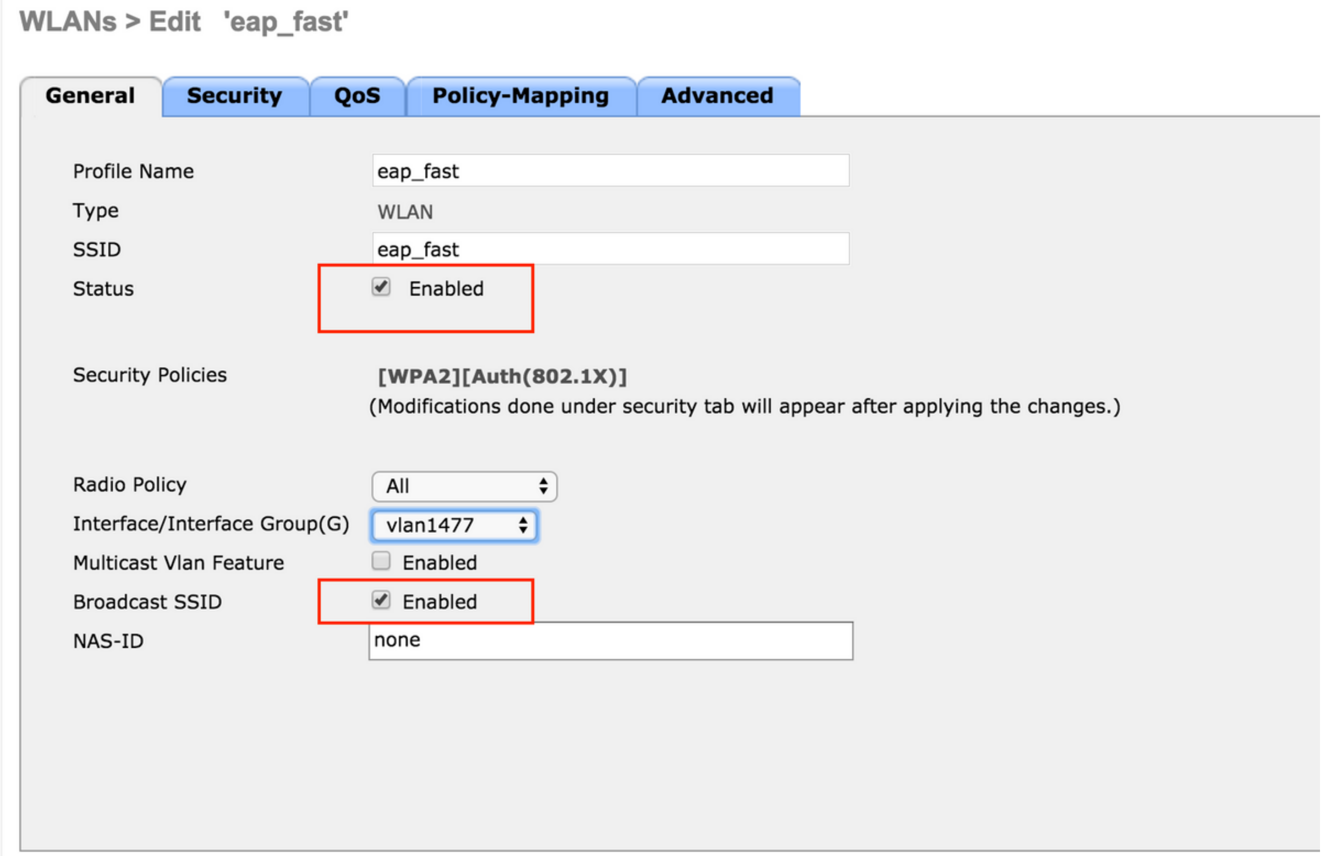
Type WLAN

Profile Name eap_fast

SSID eap_fast

ID 3

4. 创建新 WLAN 后，就会显示新 WLAN 的 **WLAN > Edit 页。**在此页上，可以定义特定于此 WLAN 的各种参数。这包括常规策略、RADIUS服务器、安全策略和802.1x参数。
5. 选中General Policies(**常规策**略)选项**卡下的Admin Status（管理状态）复选框以启用WLAN。**如果希望 AP 在其信标帧中广播 SSID，请选中 **Broadcast SSID 复选框。**



WLANs > Edit 'eap_fast'

Profile Name eap_fast

Type WLAN

SSID eap_fast

Status ☑ Enabled

Security Policies **[WPA2][Auth(802.1X)]**

(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

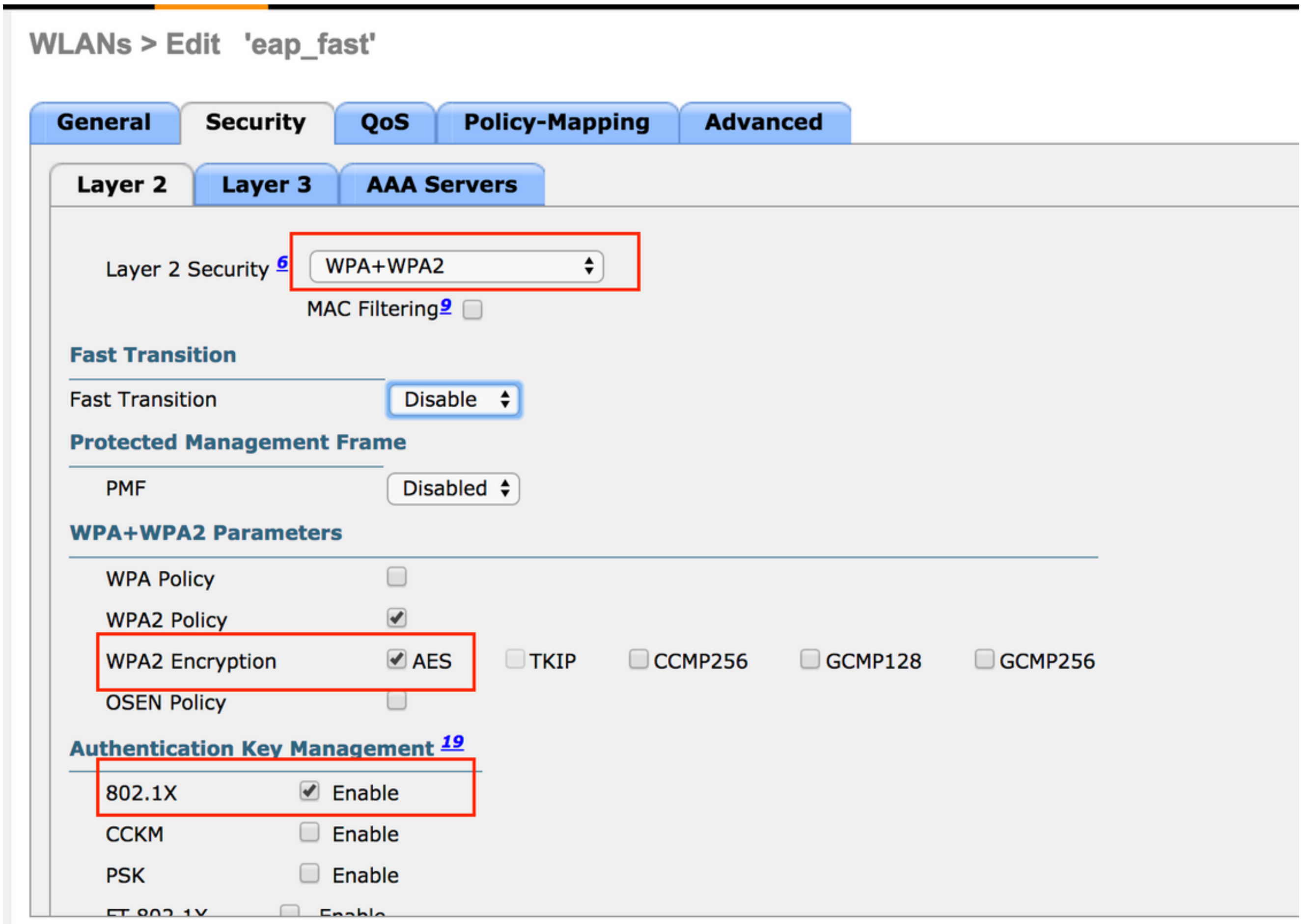
Interface/Interface Group(G) vlan1477

Multicast Vlan Feature □ Enabled

Broadcast SSID ☑ Enabled

NAS-ID none

6. 在“”下**WLAN ->编辑 — >安全 — >第2层"** 选项卡选择WPA/WPA2参数，并为AKM选择dot1x。本示例使用WPA2/AES + dot1x作为此WLAN的第2层安全。可以根据 WLAN 网络的需要修改其他参数。



WLANs > Edit 'eap_fast'

Layer 2 Security 6: WPA+WPA2

MAC Filtering9 □

Fast Transition

Fast Transition: Disable

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP □ CCMP256 □ GCMP128 □ GCMP256

OSEN Policy □

Authentication Key Management 19

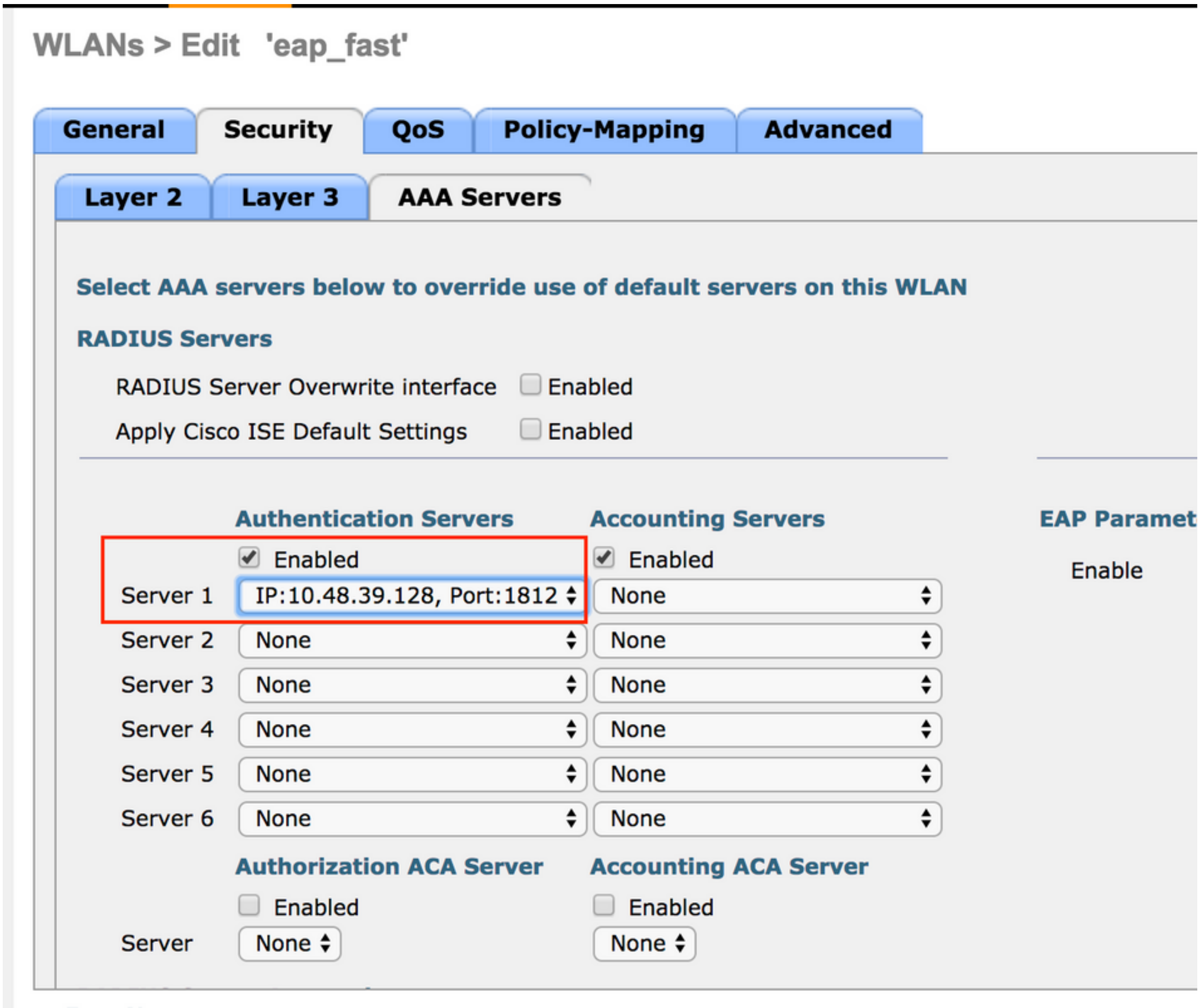
802.1X ☑ Enable

CCKM □ Enable

PSK □ Enable

FT 802.1X □ Enable

7. 在“WLAN -> Edit -> Security -> AAA Servers”选项卡下，从RADIUS Servers下的下拉菜单中选择适当的RADIUS服务器。



WLANs > Edit 'eap_fast'

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
	☑ Enabled	☑ Enabled
Server 1	IP:10.48.39.128, 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

EAP Paramet

Enable

8. 单击 **Apply**。**注意：**这是唯一需要在控制器上配置以进行EAP身份验证的EAP设置。所有其他特定于 EAP-FAST 的配置需要在 RADIUS 服务器和需要进行身份验证的客户端上完成。

为EAP-FAST身份验证配置RADIUS服务器

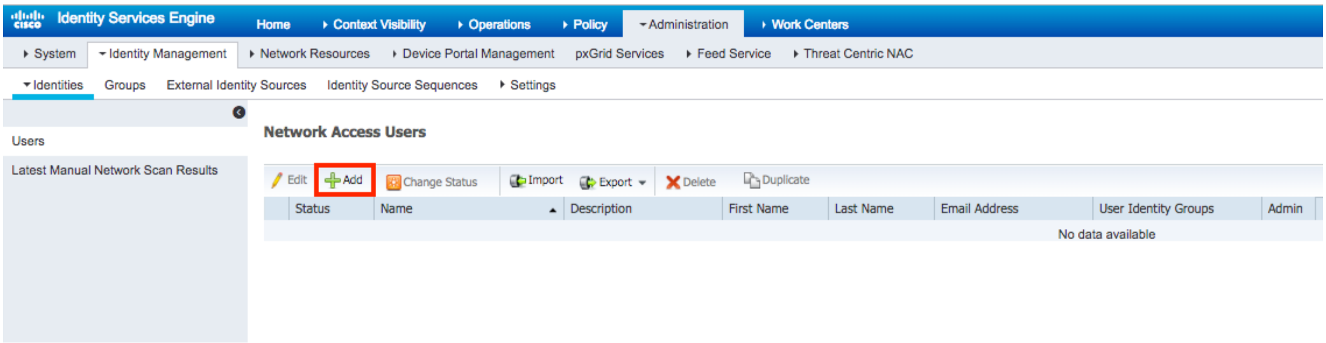
若要针对 EAP-FAST 身份验证配置 RADIUS 服务器，请执行下列步骤：

1. 创建一个用于对 EAP-FAST 客户端进行身份验证的用户数据库
2. 将 WLC 作为 AAA 客户端添加到 RADIUS 服务器
3. 使用匿名带内 PAC 配置为 RADIUS 服务器配置 EAP-FAST 身份验证
4. 在RADIUS服务器上配置带内PAC调配身份验证的EAP-FAST身份验证

创建一个用于对 EAP-FAST 客户端进行身份验证的用户数据库

此示例将EAP-FAST客户端的用户名和密码分别配置为<*eap_fast*>和<*EAP-fast1*>。

1. 在ISE Web管理UI中，在“Administration -> Identity Management **-> Users”下导航，**然后按**“Add”**图标。

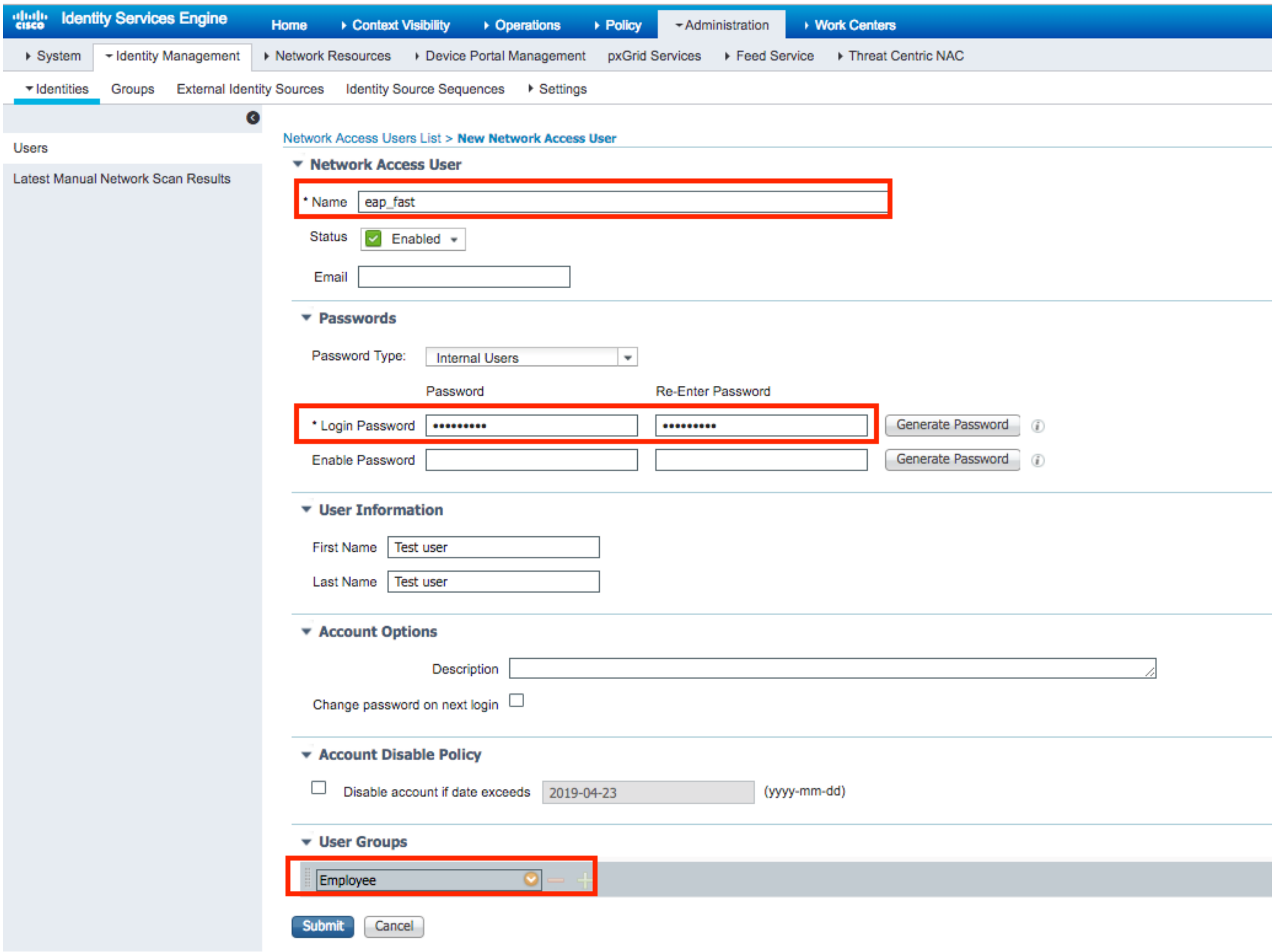


Network Access Users

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

No data available

2. 填写用户创建所需的表单 — “**Name**”和“**Login password**”，然后从下拉列表中选择“**User group**”;[可选地，您可以填写用户帐户的其他信息]
按“**Sumbit**”



Network Access Users List > New Network Access User

Network Access User

* Name: eap_fast

Status: ☑ Enabled

Email:

Passwords

Password Type: Internal Users

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

User Information

First Name: Test user

Last Name: Test user

Account Options

Description:

Change password on next login □

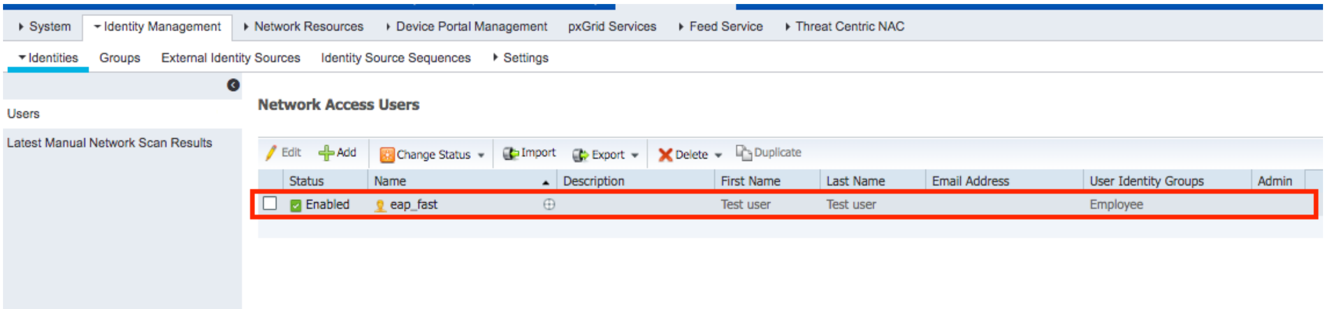
Account Disable Policy

□ Disable account if date exceeds 2019-04-23 (yyyy-mm-dd)

User Groups

Employee

3. 用户已创建。



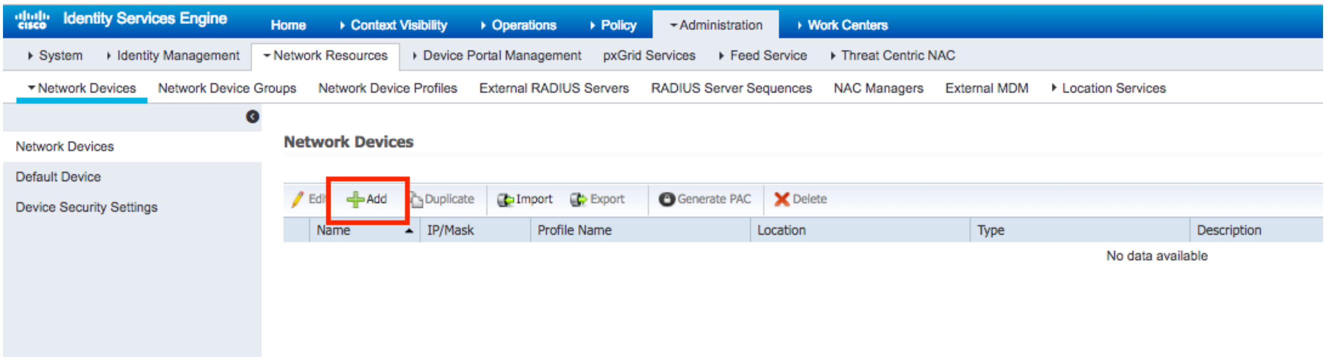
Network Access Users

	Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□	Enabled	eap_fast		Test user	Test user		Employee	

将 WLC 作为 AAA 客户端添加到 RADIUS 服务器

若要将控制器定义为 ACS 服务器上的 AAA 客户端，请完成下列步骤：

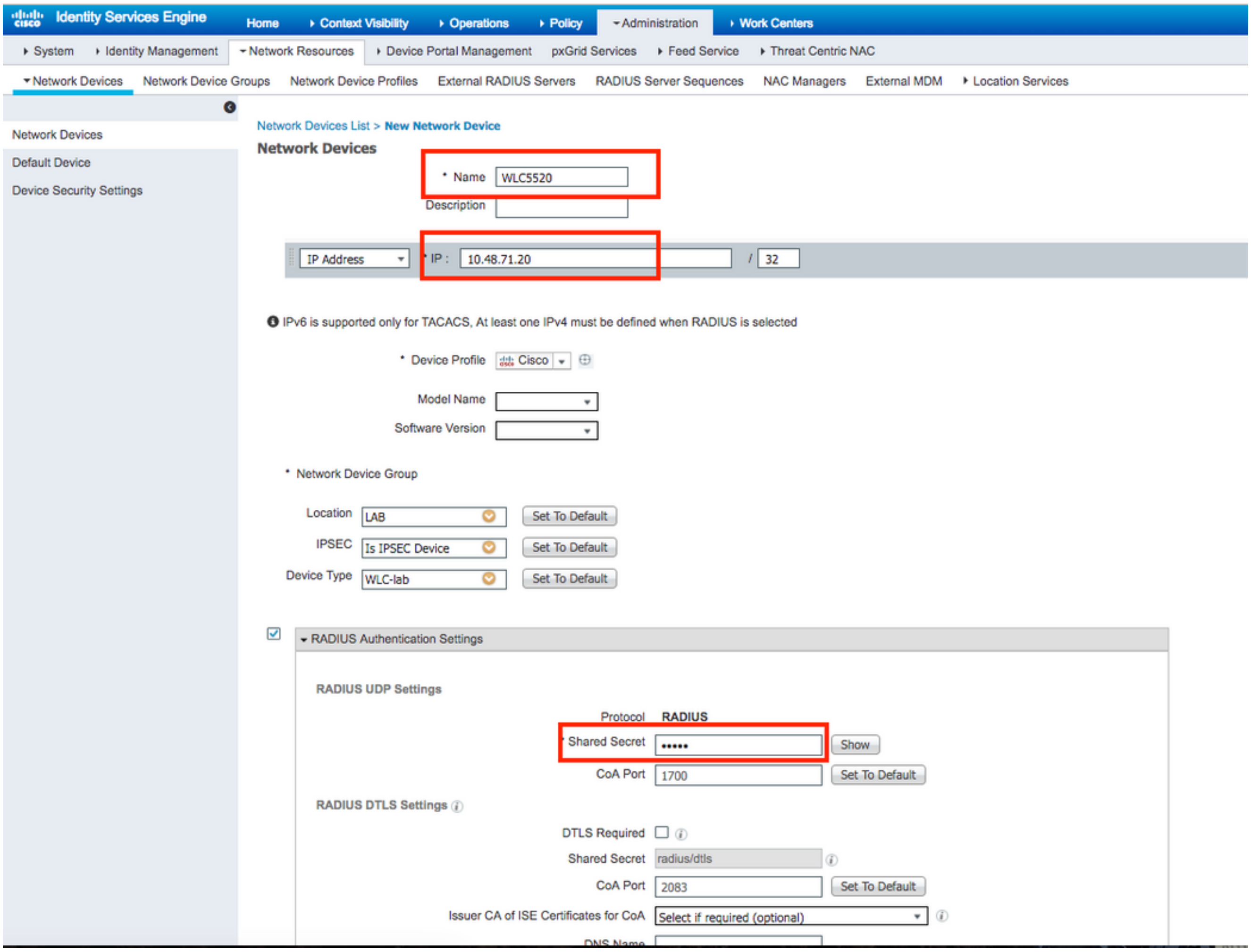
1. 在ISE Web admin UI中，在“Administration -> Network Resources -> **Network Devices”下导航，然后按“Add”**图标。



Name	IP/Mask	Profile Name	Location	Type	Description

No data available

2. 填写要添加的设备所需的表单 — **“Name”**、**“IP”**，并在“**Shared Secret**”表单中配置与前面部分在WLC上配置的相同的共享密钥密码[可选地，您可以填写设备的其他信息，如位置、组等]。按“**Sumbit**”



Network Devices List > New Network Device

Network Devices

* Name WLC5520

Description

IP Address * IP : 10.48.71.20 / 32

IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Location LAB

IPSEC Is IPSEC Device

Device Type WLC-lab

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret •••••

CoA Port 1700

RADIUS DTLS Settings

DTLS Required □

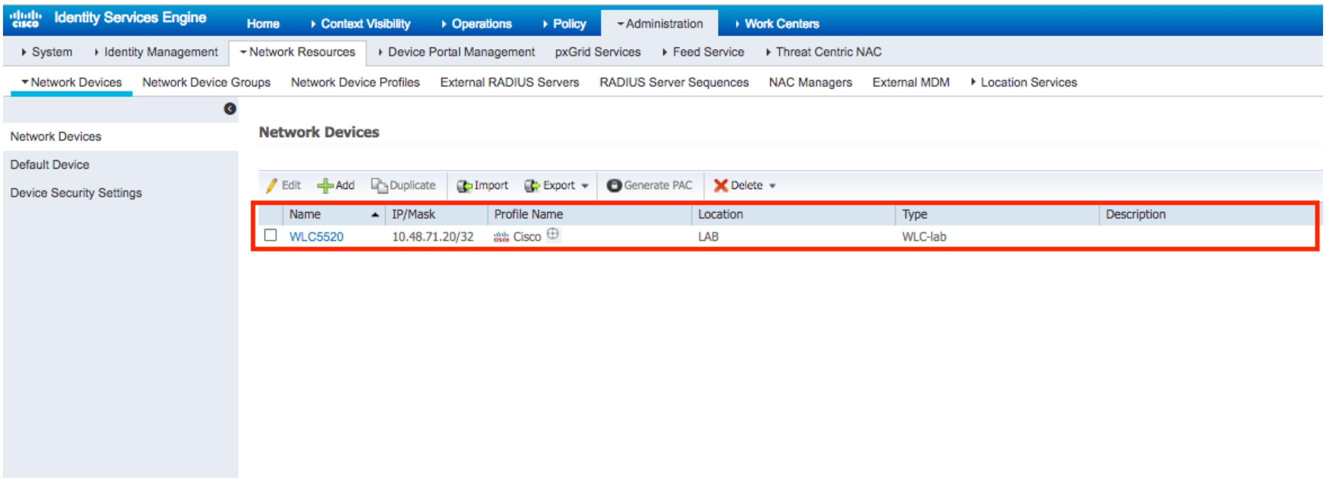
Shared Secret radius/dtls

CoA Port 2083

Issuer CA of ISE Certificates for CoA Select if required (optional)

DNS Name

3. 设备已添加到ISE网络访问设备列表。（需要）



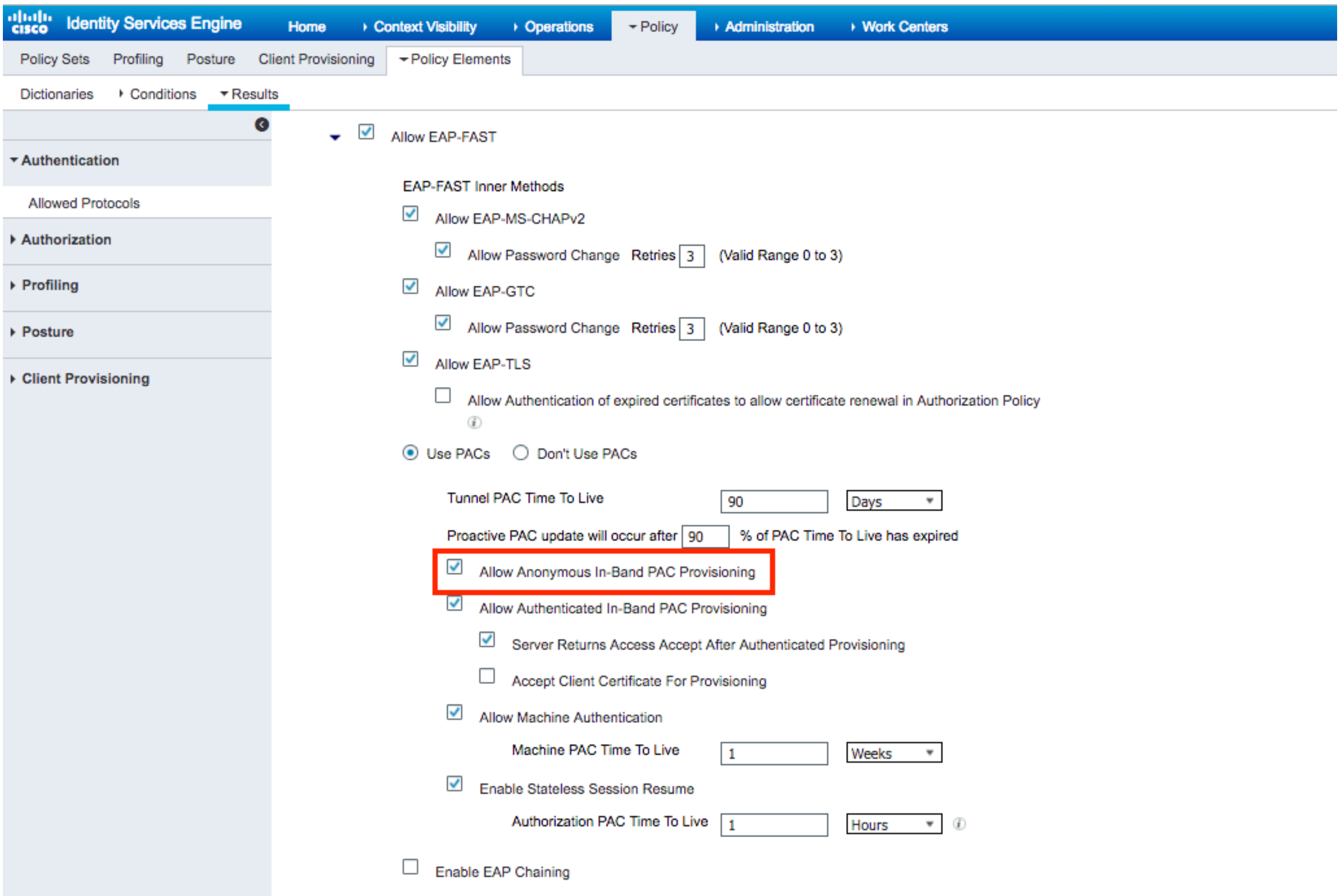
	Name	IP/Mask	Profile Name	Location	Type	Description
□	WLC5520	10.48.71.20/32	Cisco	LAB	WLC-lab	

使用匿名带内 PAC 配置为 RADIUS 服务器配置 EAP-FAST 身份验证

通常，如果部署中没有PKI基础设施，则希望使用这种方法。

在对等体对ISE服务器进行身份验证之前，此方法在经过身份验证的Diffie-HellmanKey协议(ADHP)隧道内运行。

要支持此方法，我们需要在ISE的“**允许匿名带内PAC调配**”**下**启用“允许身份验证**协议**”：



☑ Allow EAP-FAST

EAP-FAST Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 3 (Valid Range 0 to 3)

☑ Allow EAP-GTC

☑ Allow Password Change Retries 3 (Valid Range 0 to 3)

☑ Allow EAP-TLS

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

● Use PACs ○ Don't Use PACs

Tunnel PAC Time To Live 90 Days

Proactive PAC update will occur after 90 % of PAC Time To Live has expired

☑ Allow Anonymous In-Band PAC Provisioning

☑ Allow Authenticated In-Band PAC Provisioning

☑ Server Returns Access Accept After Authenticated Provisioning

□ Accept Client Certificate For Provisioning

☑ Allow Machine Authentication

Machine PAC Time To Live 1 Weeks

☑ Enable Stateless Session Resume

Authorization PAC Time To Live 1 Hours

□ Enable EAP Chaining

注：确保您具有允许的密码类型验证，例如EAP-MS-CHAPv2 for EAP-FAST内部方法，因为显然，使用匿名带内调配时，我们不能使用任何证书。

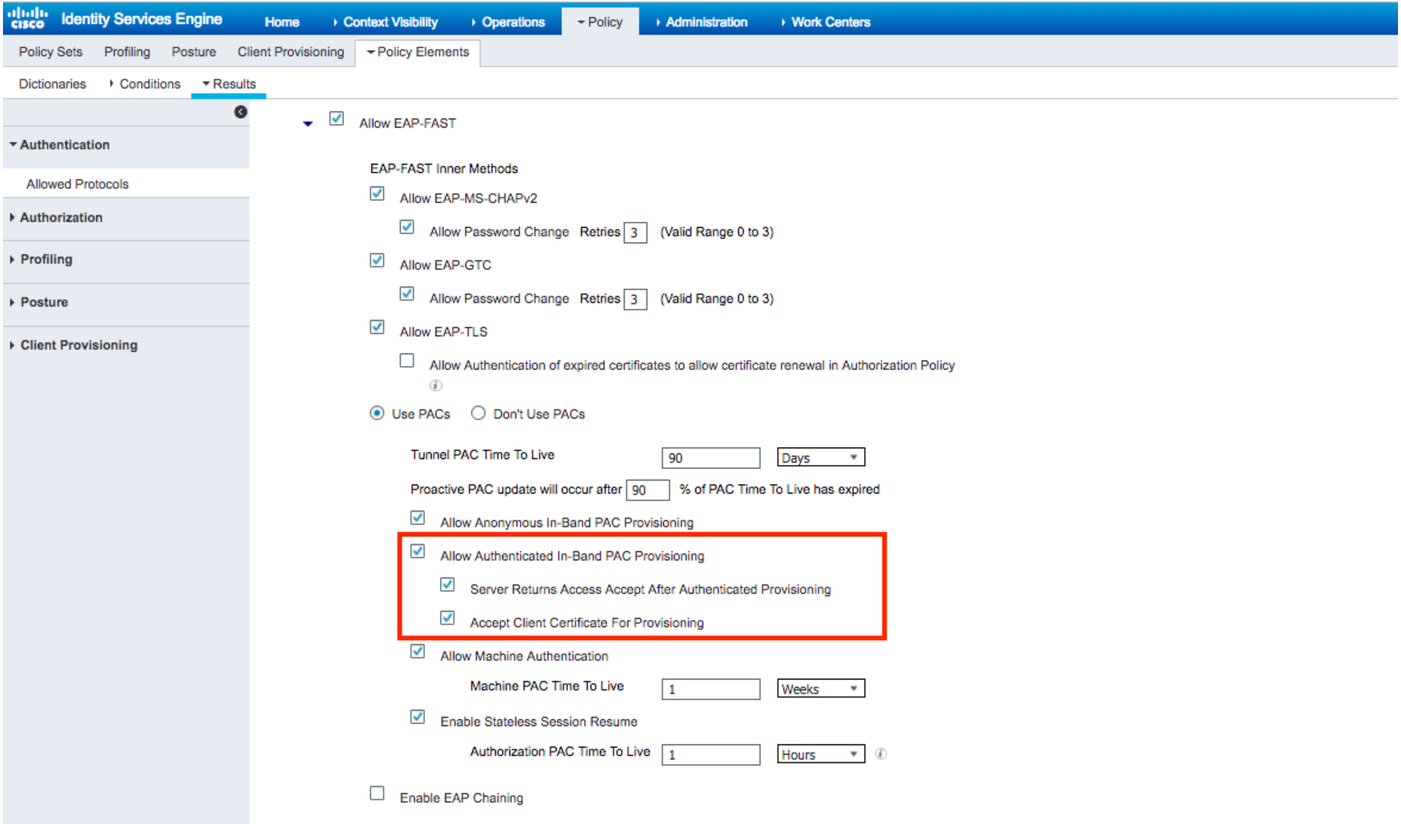
在RADIUS服务器上配置带内PAC调配身份验证的EAP-FAST身份验证

这是最安全和推荐的选项。TLS隧道基于服务器证书构建，服务器证书由请求方验证，客户端证书由ISE验证（默认）。

该选项需要为客户端和服务器提供PKI基础设施，但可能只限于服务器端，或在两端跳过。

在ISE上，身份验证带内调配还有两个其他选项：

1. "Server Returns Access Accept After Authenticated Provisioning" — 通常，在PAC调配后，应发送Access-Reject，强制请求方使用PAC重新进行身份验证。但是，由于PAC调配是在经过身份验证的TLS隧道中完成的，因此我们可以立即使用Access-Accept响应，以最大限度地缩短身份验证时间。（在这种情况下，请确保您在客户端和服务器端有受信任证书）。
2. **"Accept Client Certificate For Provisioning" — 如果不想为客户端设备提供PKI基础设施，并且仅在ISE上具有受信任证书，则启用该选项，允许跳过服务器端的客户端证书验证。**



☑ Allow EAP-FAST

EAP-FAST Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 3 (Valid Range 0 to 3)

☑ Allow EAP-GTC

☑ Allow Password Change Retries 3 (Valid Range 0 to 3)

☑ Allow EAP-TLS

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

● Use PACs ○ Don't Use PACs

Tunnel PAC Time To Live 90 Days

Proactive PAC update will occur after 90 % of PAC Time To Live has expired

☑ Allow Anonymous In-Band PAC Provisioning

☑ Allow Authenticated In-Band PAC Provisioning

☑ Server Returns Access Accept After Authenticated Provisioning

☑ Accept Client Certificate For Provisioning

☑ Allow Machine Authentication

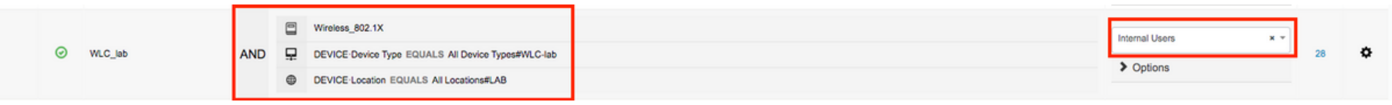
Machine PAC Time To Live 1 Weeks

☑ Enable Stateless Session Resume

Authorization PAC Time To Live 1 Hours

□ Enable EAP Chaining

在ISE上，我们还为无线用户定义简单身份验证策略集，以下示例使用作为条件参数的设备类型以及位置和身份验证类型，匹配该条件的身份验证流将根据内部用户数据库进行验证。



WLC_lab

AND
- Wireless_802.1X
- DEVICE·Device Type EQUALS All Device Types#WLC-lab
- DEVICE·Location EQUALS All Locations#LAB

Internal Users

Options

28

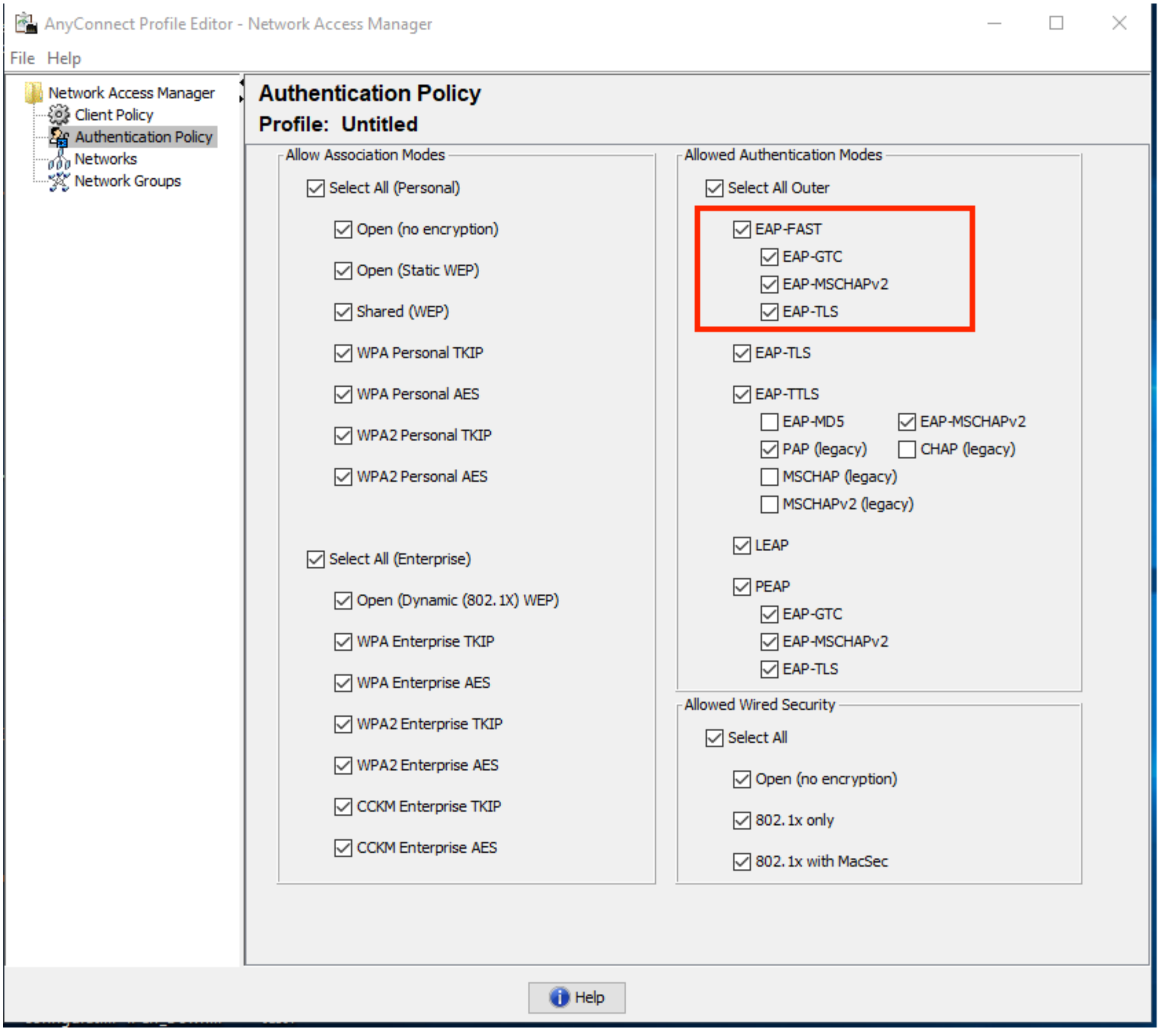
验证

本示例将显示经过身份验证的带内PAC调配流和网络访问管理器(NAM)配置设置以及各自的WLC调试。

NAM配置文件配置

要配置Anyconnect NAM配置文件以使用EAP-FAST根据ISE对用户会话进行身份验证，需要执行以下步骤：

1. 打开网络访问管理器配置文件编辑器并加载当前配置文件。
2. 确保在“允**许的身**份验证模式”**下启用“EAP-FAST”**



Authentication Policy

Profile: Untitled

Allow Association Modes

☑ Select All (Personal)

- ☑ Open (no encryption)
- ☑ Open (Static WEP)
- ☑ Shared (WEP)
- ☑ WPA Personal TKIP
- ☑ WPA Personal AES
- ☑ WPA2 Personal TKIP
- ☑ WPA2 Personal AES

☑ Select All (Enterprise)

- ☑ Open (Dynamic (802.1X) WEP)
- ☑ WPA Enterprise TKIP
- ☑ WPA Enterprise AES
- ☑ WPA2 Enterprise TKIP
- ☑ WPA2 Enterprise AES
- ☑ CCKM Enterprise TKIP
- ☑ CCKM Enterprise AES

Allowed Authentication Modes

☑ Select All Outer

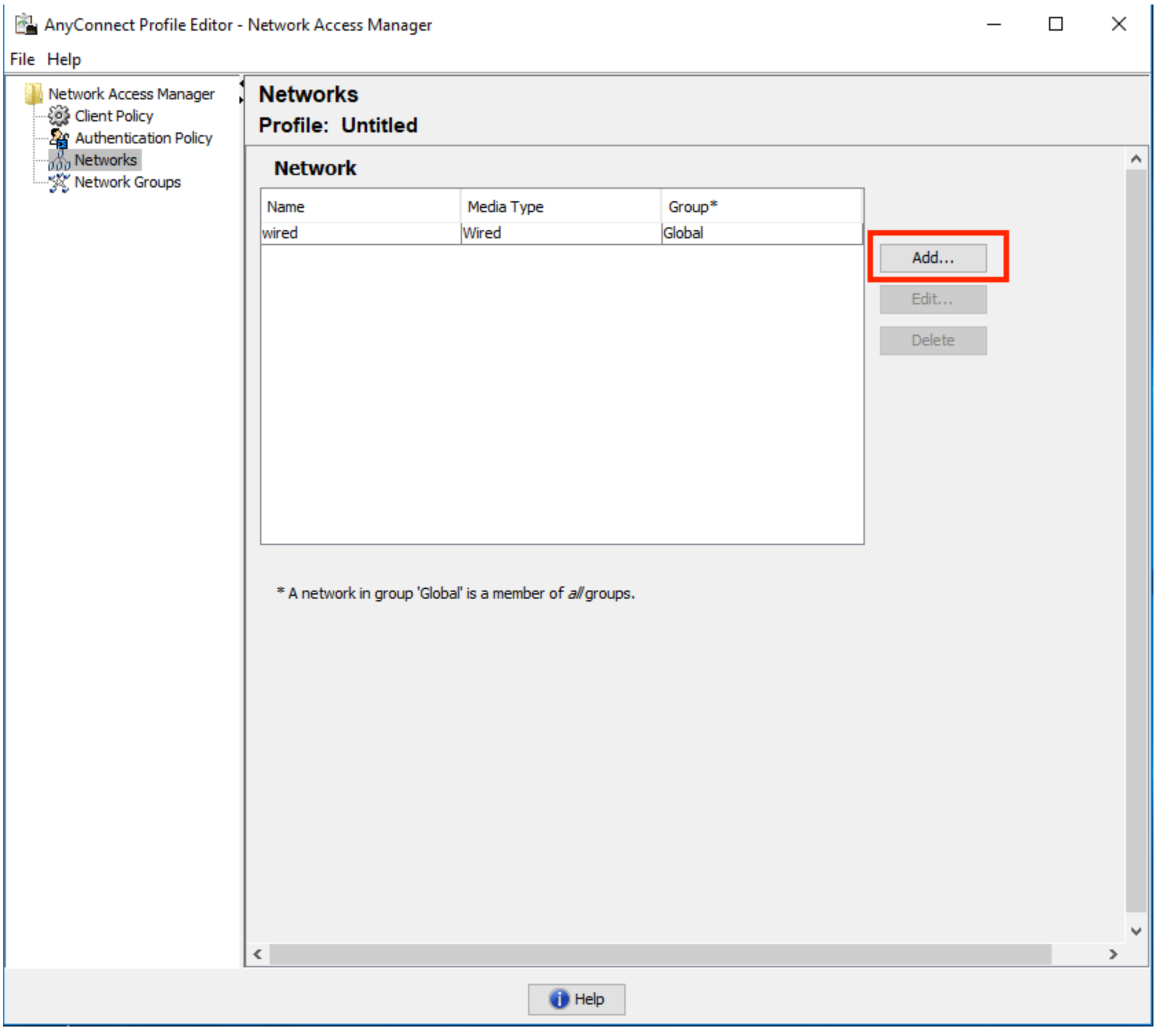
- ☑ EAP-FAST
  - ☑ EAP-GTC
  - ☑ EAP-MSCHAPv2
  - ☑ EAP-TLS
- ☑ EAP-TLS
- ☑ EAP-TTLS
  - □ EAP-MD5
  - ☑ EAP-MSCHAPv2
  - ☑ PAP (legacy)
  - □ CHAP (legacy)
  - □ MSCHAP (legacy)
  - □ MSCHAPv2 (legacy)
- ☑ LEAP
- ☑ PEAP
  - ☑ EAP-GTC
  - ☑ EAP-MSCHAPv2
  - ☑ EAP-TLS

Allowed Wired Security

☑ Select All

- ☑ Open (no encryption)
- ☑ 802.1x only
- ☑ 802.1x with MacSec

3. “添**加”新**网络配置文件：



Networks

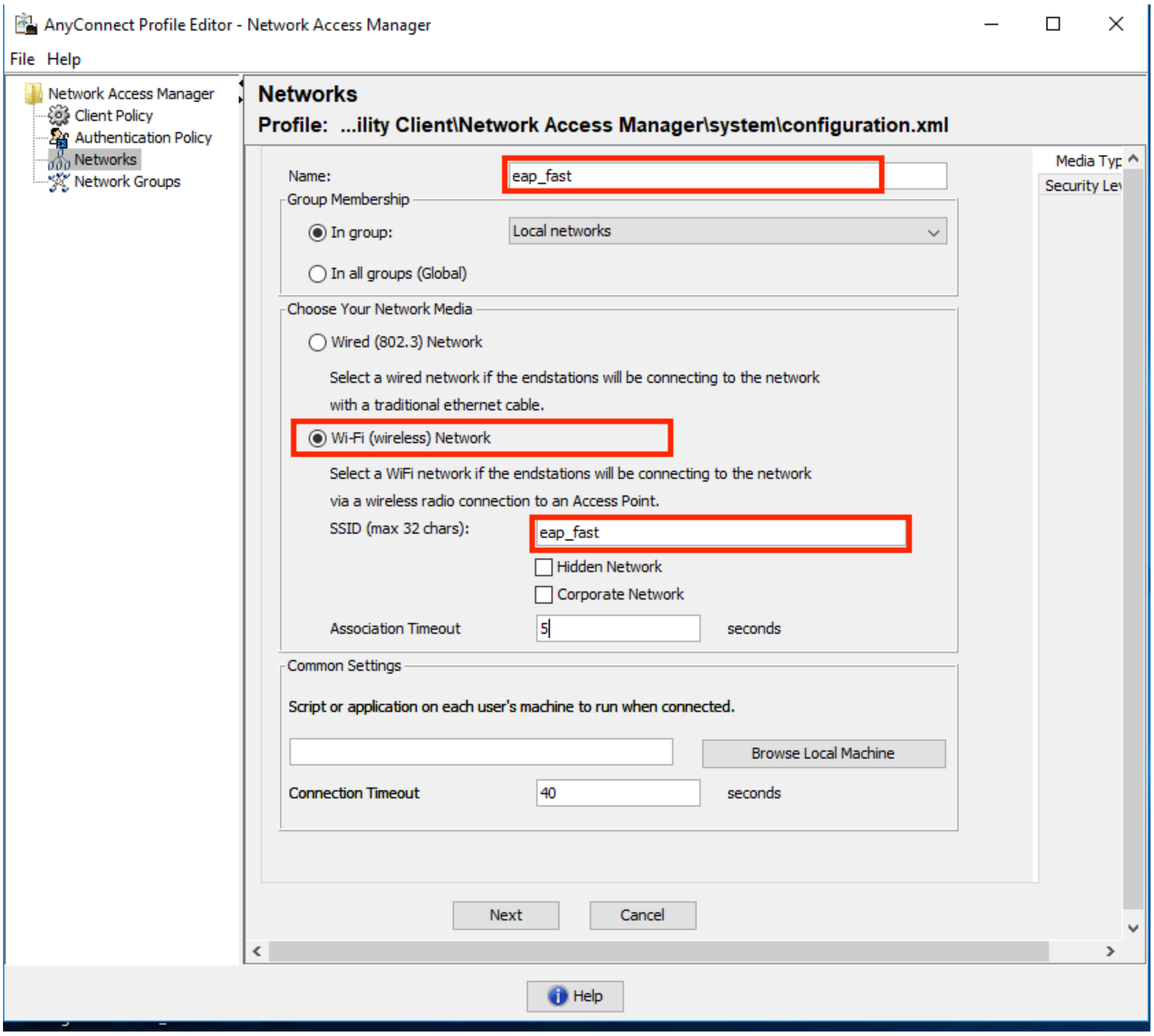
Profile: Untitled

Network

Name	Media Type	Group*
wired	Wired	Global

* A network in group 'Global' is a member of *all* groups.

4. 在“介**质类型”**配置部分下，定义配置文件“**名称**”，无线作为介质网络类型并指定SSID名称。



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Name: eap_fast

Group Membership

● In group: Local networks

○ In all groups (Global)

Choose Your Network Media

○ Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

● Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars): eap_fast

□ Hidden Network

□ Corporate Network

Association Timeout 5 seconds

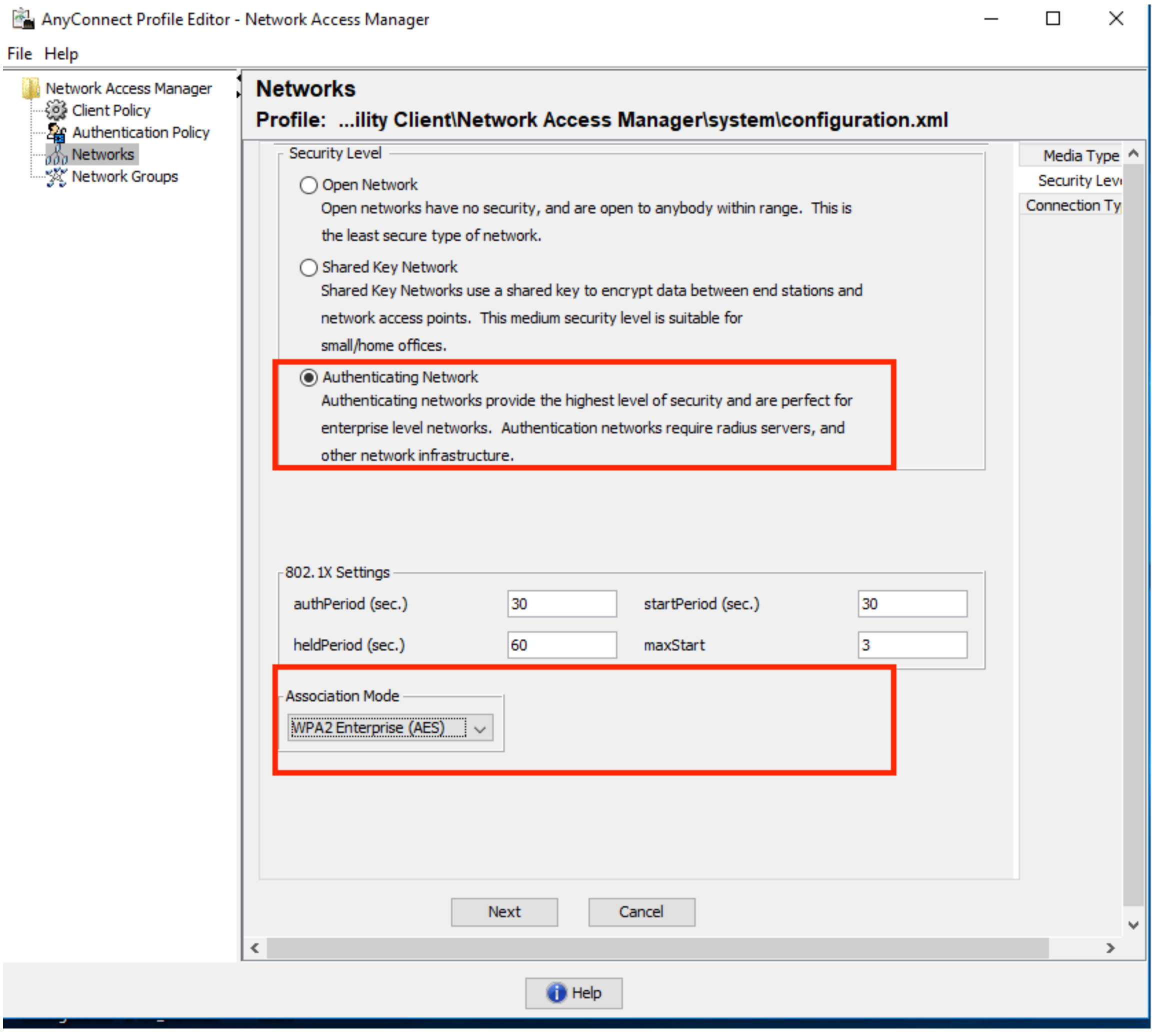
Common Settings

Script or application on each user's machine to run when connected.

Browse Local Machine

Connection Timeout 40 seconds

5. 在“安**全级别”配**置选项卡下，选择“身份验证网络”并将关联模式指定为WPA2企业(AES)



AnyConnect Profile Editor - Network Access Manager

Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Security Level

○ Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

○ Shared Key Network
Shared Key Networks use a shared key to encrypt data between end stations and network access points. This medium security level is suitable for small/home offices.

● Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

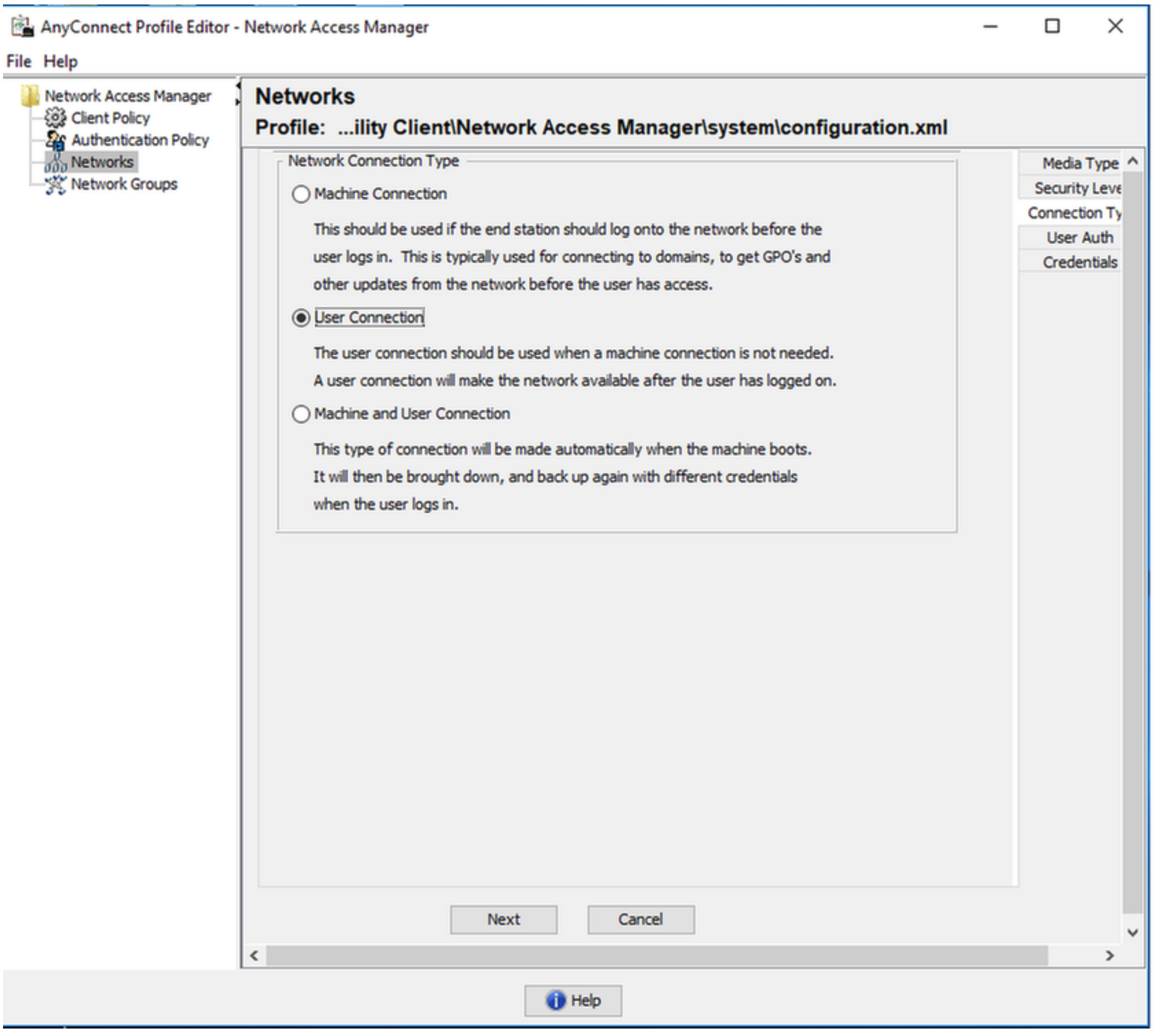
802.1X Settings

authPeriod (sec.) 30
startPeriod (sec.) 30
heldPeriod (sec.) 60
maxStart 3

Association Mode

WPA2 Enterprise (AES)

6. 在本示例中，我们使用用户类型身份验证，因此在下一个选项卡“连接类型”下选择“用户连接”



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Network Connection Type

○ Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

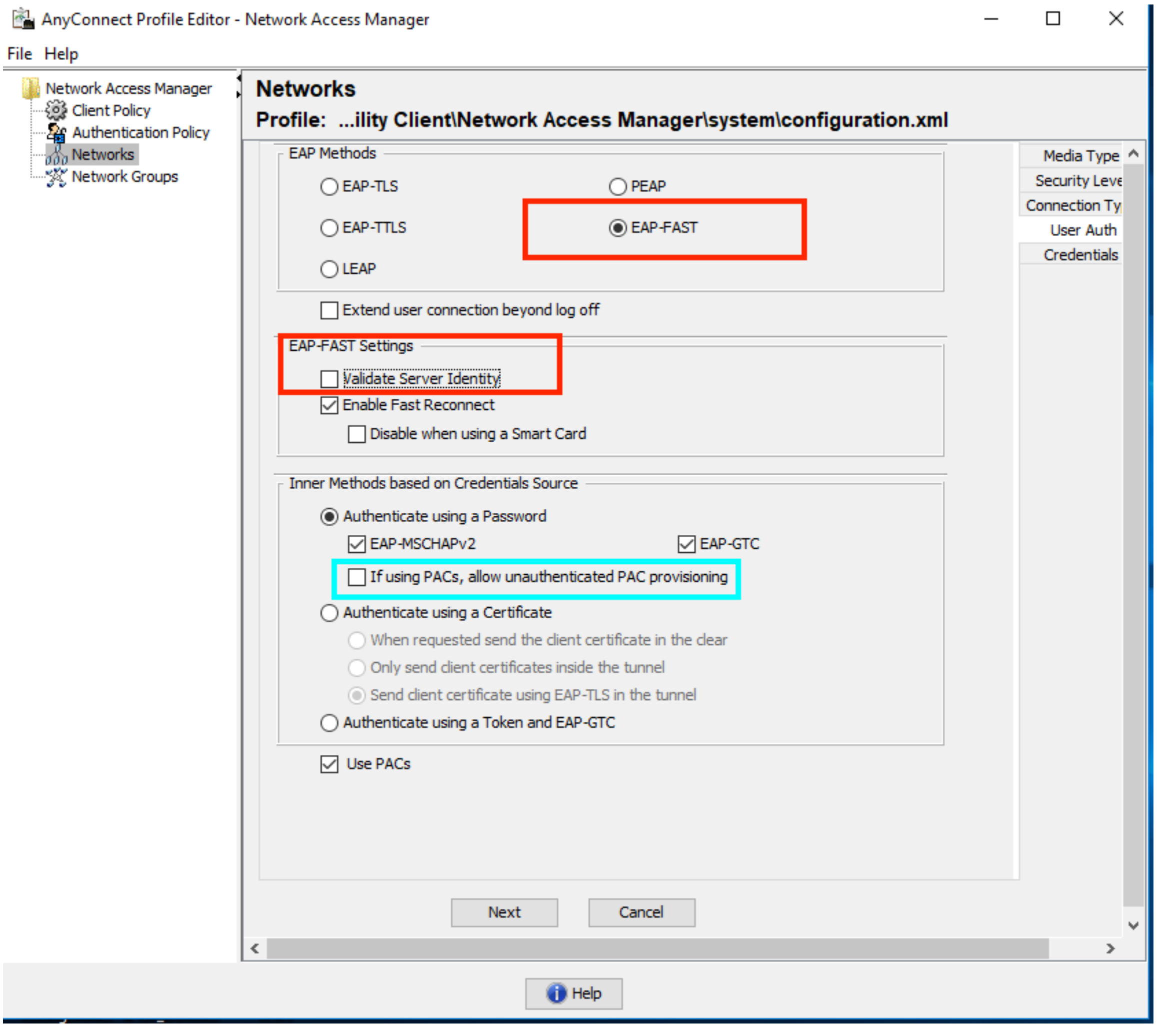
● User Connection

The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.

○ Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

7. 在“**User Auth**”选项卡下，指定EAP-FAST作为允许的身份验证方法并禁用服务器证书验证，因为在本示例中我们不使用受信任证书。



AnyConnect Profile Editor - Network Access Manager

File Help

- Network Access Manager
  - Client Policy
  - Authentication Policy
  - Networks
  - Network Groups

Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

EAP Methods

○ EAP-TLS ○ PEAP

○ EAP-TTLS ● EAP-FAST

○ LEAP

□ Extend user connection beyond log off

EAP-FAST Settings

□ Validate Server Identity

☑ Enable Fast Reconnect

□ Disable when using a Smart Card

Inner Methods based on Credentials Source

● Authenticate using a Password

☑ EAP-MSCHAPv2 ☑ EAP-GTC

□ If using PACs, allow unauthenticated PAC provisioning

○ Authenticate using a Certificate

○ When requested send the client certificate in the clear

○ Only send client certificates inside the tunnel

● Send client certificate using EAP-TLS in the tunnel

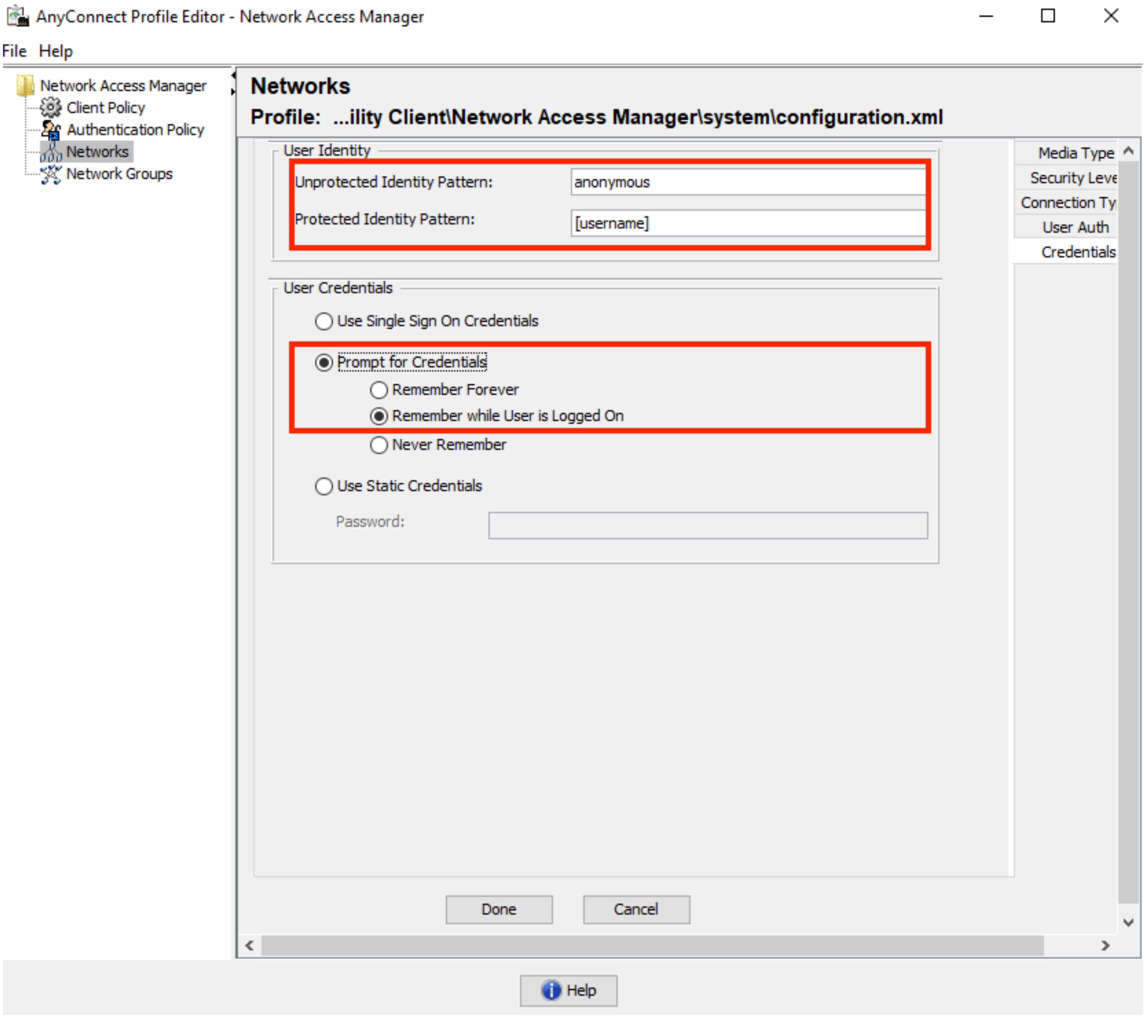
○ Authenticate using a Token and EAP-GTC

☑ Use PACs

注意：在实际生产环境中，请确保在ISE上安装了受信任证书，并在NAM设置中启用服务器证书验证选项。

注意：选项"如果使用PAC，则仅在匿名带内PAC调配的情况下才必须选择允许未经身份验证的PAC调配"。

8. 定义用户凭据，如果您愿意使用与登录使用相同的凭据，则使用SSO；如果希望在连接到网络时要求用户提供凭据，则选择"提示提供凭据"；或者为该访问类型定义静态凭据。在本示例中，我们提示用户在尝试连接网络时输入凭证。



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

User Identity

Unprotected Identity Pattern: anonymous

Protected Identity Pattern: [username]

User Credentials

○ Use Single Sign On Credentials

● Prompt for Credentials

○ Remember Forever

● Remember while User is Logged On

○ Never Remember

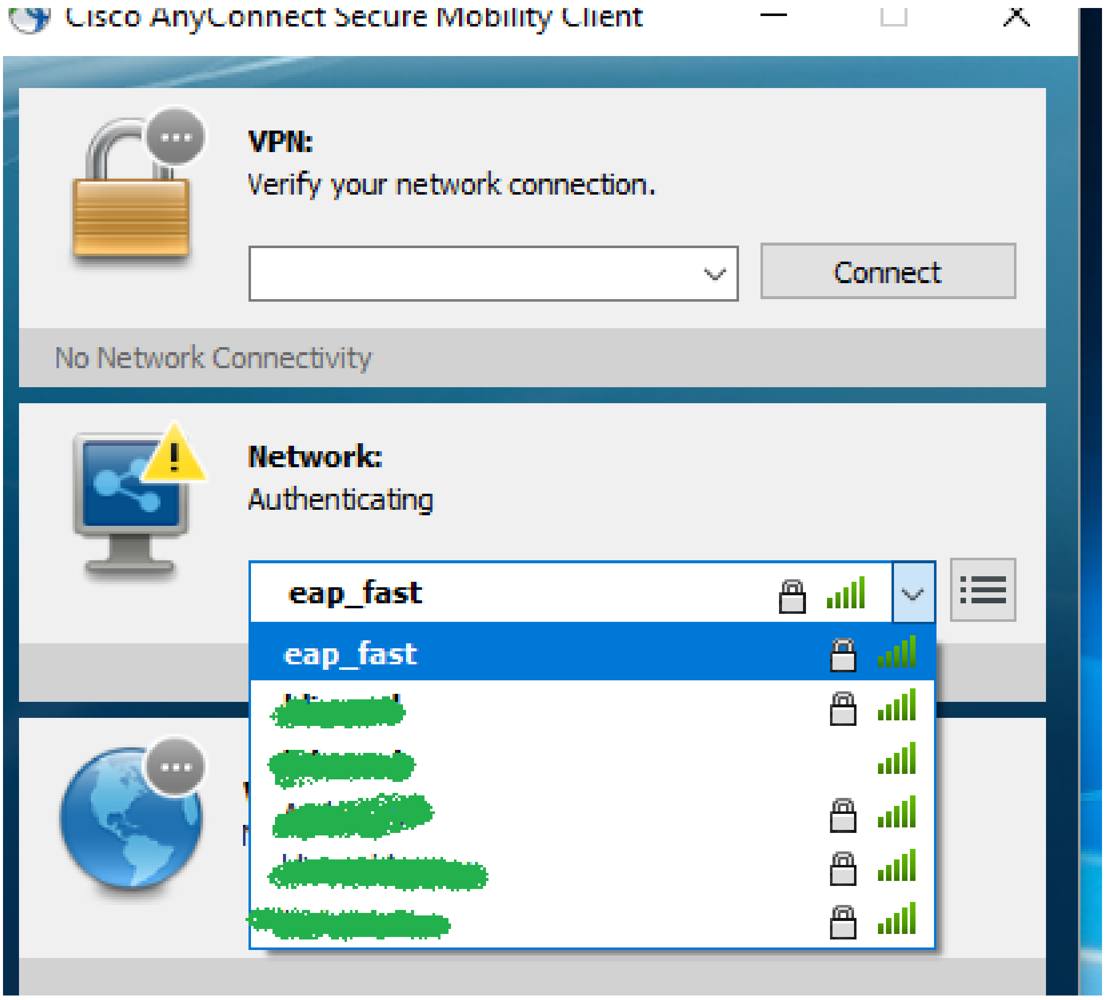
○ Use Static Credentials

Password:

9. 将配置的配置文件保存到相应的NAM文件夹下。

使用EAP-FAST身份验证测试与SSID的连接。

1. 从Anyconnect网络列表中选择相应的配置文件



Cisco AnyConnect Secure Mobility Client

VPN:
Verify your network connection.

No Network Connectivity

Network:
Authenticating

eap_fast

eap_fast

[redacted]

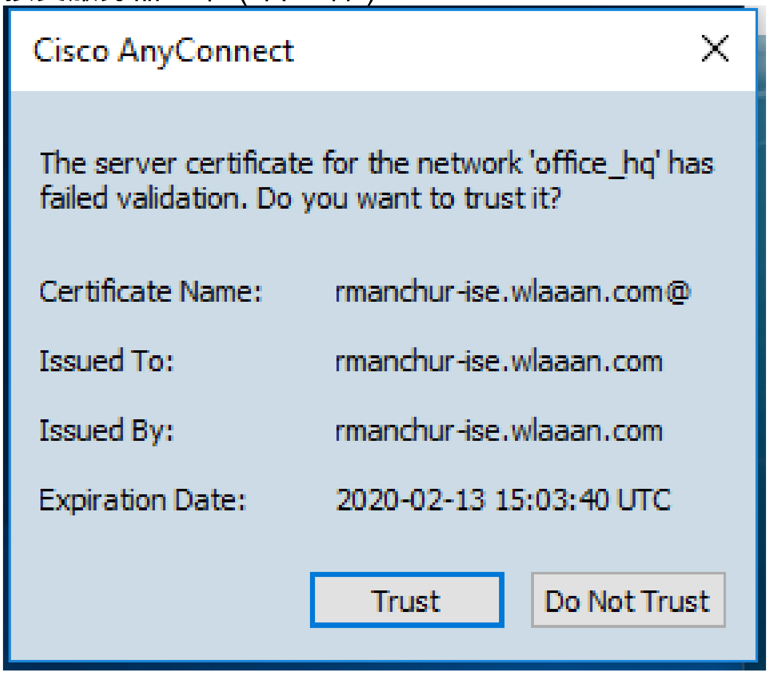
[redacted]

[redacted]

[redacted]

[redacted]

2. 输入身份验证所需的用户名和密码
3. 接受服务器证书（自签名）



Cisco AnyConnect

The server certificate for the network 'office_hq' has failed validation. Do you want to trust it?

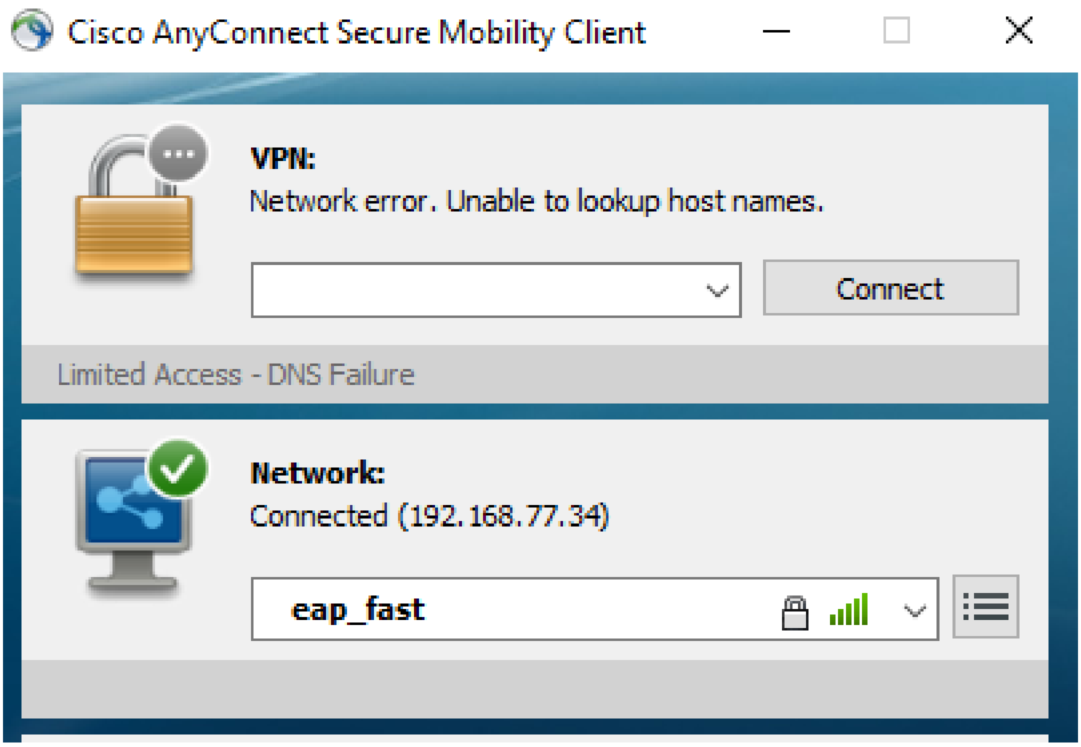
Certificate Name: rmanchur-ise.wlaaan.com@

Issued To: rmanchur-ise.wlaaan.com

Issued By: rmanchur-ise.wlaaan.com

Expiration Date: 2020-02-13 15:03:40 UTC

4. done



Cisco AnyConnect Secure Mobility Client

VPN:

Network error. Unable to lookup host names.

Limited Access - DNS Failure

Network:

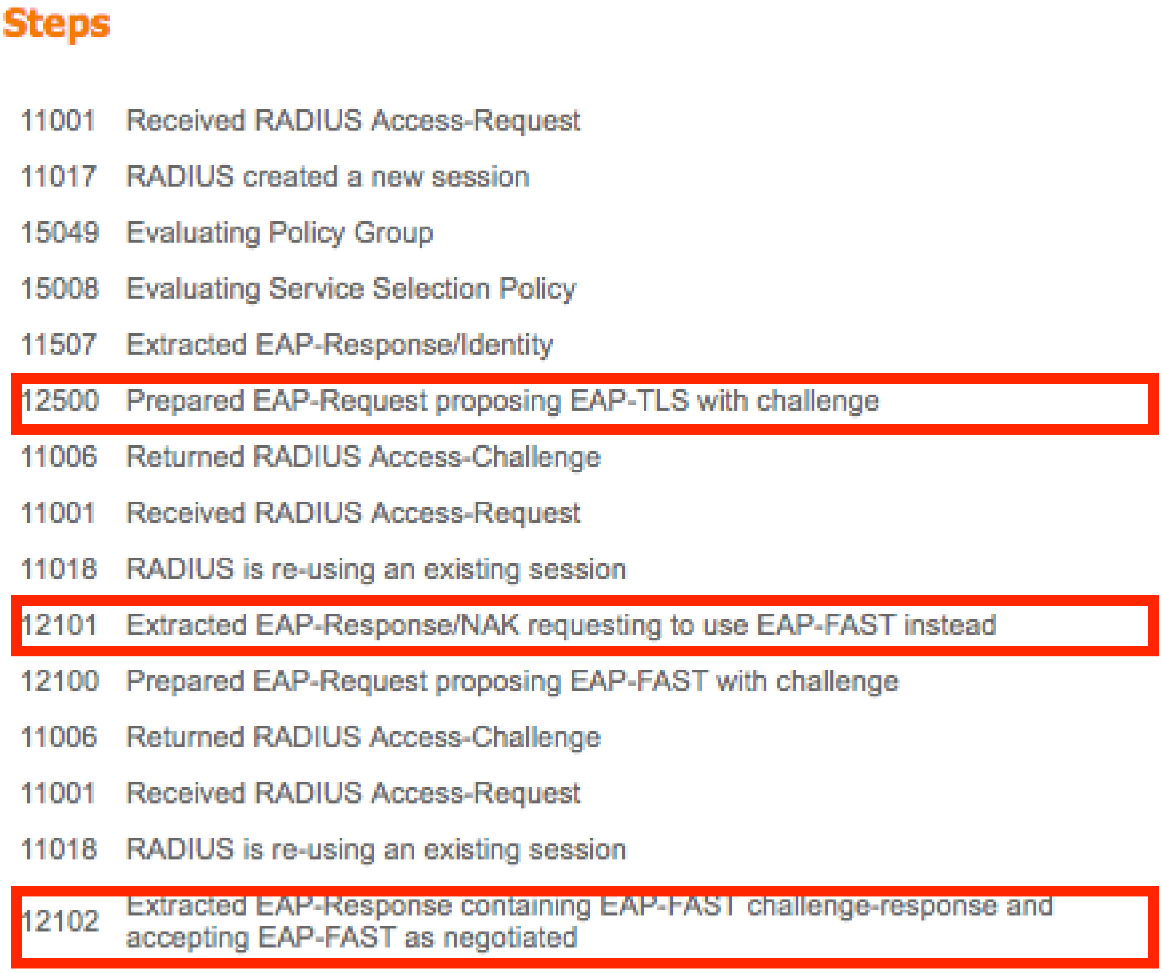
Connected (192.168.77.34)

eap_fast

ISE身份验证日志

显示EAP-FAST和PAC调配流的ISE身份验证日志可在“**操作 — > RADIUS ->实时日志**”下查看，并可使用“缩放”图标查看更多详**细信**息：

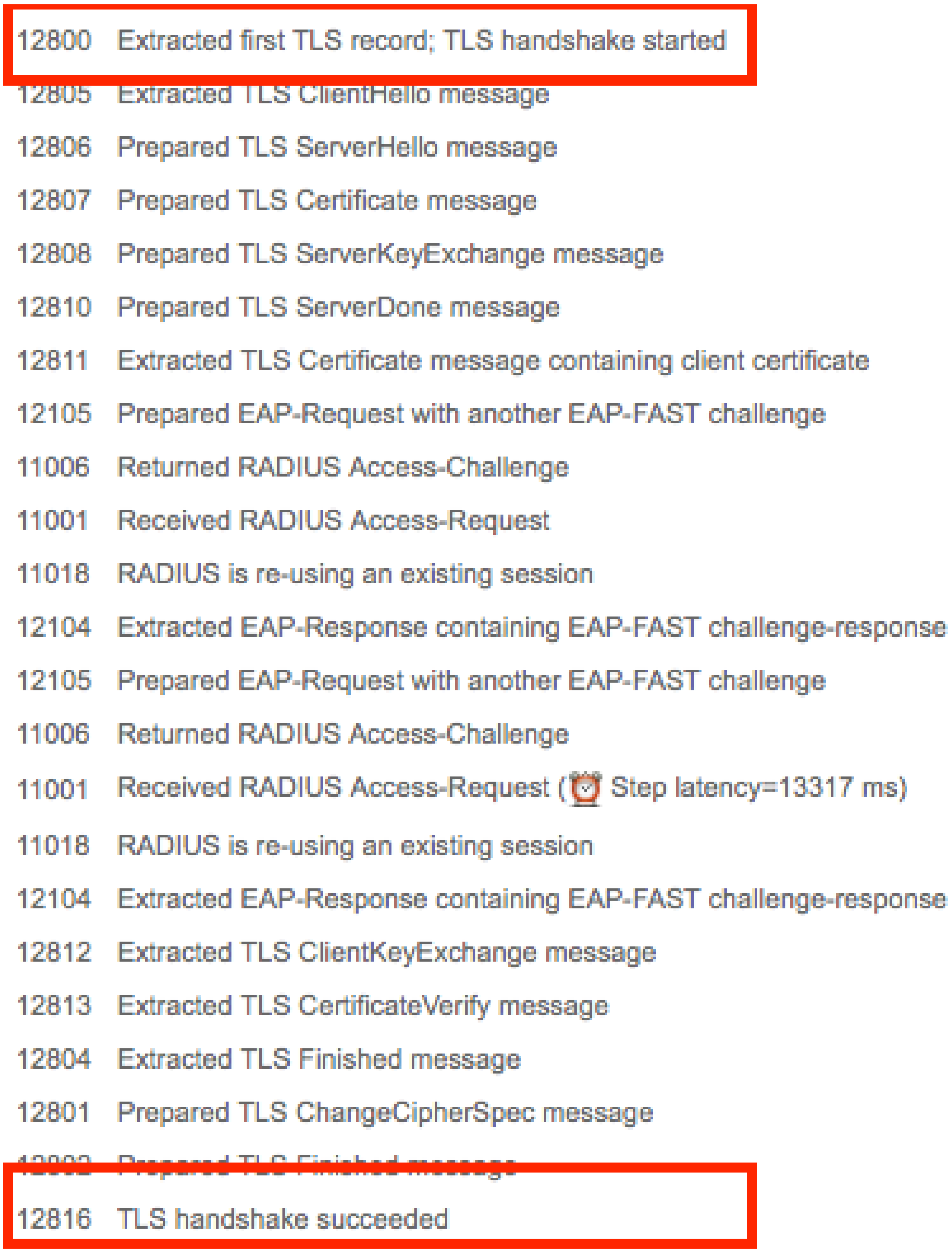
1. 客户端已开始身份验证，ISE建议将EAP-TLS作为身份验证方法，但客户端拒绝并建议EAP-FAST，这是客户端和ISE都同意的方法。



```
Steps

11001   Received RADIUS Access-Request
11017   RADIUS created a new session
15049   Evaluating Policy Group
15008   Evaluating Service Selection Policy
11507   Extracted EAP-Response/Identity
12500   Prepared EAP-Request proposing EAP-TLS with challenge
11006   Returned RADIUS Access-Challenge
11001   Received RADIUS Access-Request
11018   RADIUS is re-using an existing session
12101   Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100   Prepared EAP-Request proposing EAP-FAST with challenge
11006   Returned RADIUS Access-Challenge
11001   Received RADIUS Access-Request
11018   RADIUS is re-using an existing session
12102   Extracted EAP-Response containing EAP-FAST challenge-response and
        accepting EAP-FAST as negotiated
```

2. 客户端和服务器之间的TLS握手已启动，已为PAC交换提供受保护环境，并已成功完成。



```
12800   Extracted first TLS record; TLS handshake started
12805   Extracted TLS ClientHello message
12806   Prepared TLS ServerHello message
12807   Prepared TLS Certificate message
12808   Prepared TLS ServerKeyExchange message
12810   Prepared TLS ServerDone message
12811   Extracted TLS Certificate message containing client certificate
12105   Prepared EAP-Request with another EAP-FAST challenge
11006   Returned RADIUS Access-Challenge
11001   Received RADIUS Access-Request
11018   RADIUS is re-using an existing session
12104   Extracted EAP-Response containing EAP-FAST challenge-response
12105   Prepared EAP-Request with another EAP-FAST challenge
11006   Returned RADIUS Access-Challenge
11001   Received RADIUS Access-Request (⏰ Step latency=13317 ms)
11018   RADIUS is re-using an existing session
12104   Extracted EAP-Response containing EAP-FAST challenge-response
12812   Extracted TLS ClientKeyExchange message
12813   Extracted TLS CertificateVerify message
12804   Extracted TLS Finished message
12801   Prepared TLS ChangeCipherSpec message
12802   Prepared TLS Finished message
12816   TLS handshake succeeded
```

3. 内部身份验证已启动，且ISE已使用MS-CHAPv2（基于用户名/密码的身份验证）成功验证用户凭证