使用無線LAN控制器和身份服務引擎的EAP-FAST身份驗證

目錄

簡介

本檔案將說明如何使用外部RADIUS伺服器設定無線LAN控制器(WLC)以進行可擴充驗證通訊協定(EAP) — 透過安全通道進行彈性驗證(FAST)驗證。此配置示例使用身份服務引擎(ISE)作為外部RADIUS伺服器來驗證無線客戶端。

本文檔重點介紹如何為無線客戶端配置匿名和身份驗證帶內（自動）保護訪問憑證(PAC)調配的ISE。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 輕量型存取點(LAP)和Cisco WLC組態的基本知識
- CAPWAP協定基礎知識
- 瞭解如何配置外部RADIUS伺服器，例如思科ISE
- 關於通用EAP框架的功能知識
- 安全協定（如MS-CHAPv2和EAP-GTC）的基本知識以及數位證書知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5520系列WLC（執行韌體版本8.8.111.0）Cisco 4800系列APAnyconnect NAM。思科安全ISE版本2.3.0.298執行15.2(4)E1版的Cisco 3560-CX系列交換器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

EAP-FAST協定是思科開發的一種可公開訪問的IEEE 802.1X EAP型別，用於支援無法實施強密碼策略並且希望部署不需要數位證書的802.1X EAP型別的客戶。

EAP-FAST協定是一種客戶端 — 伺服器安全體系結構，它使用傳輸級安全(TLS)隧道加密EAP事務。EAP-FAST隧道建立基於使用者獨有的強機密。這些強金鑰稱為PAC，ISE使用只為ISE所知的主金鑰生成這些金鑰。

EAP-FAST分為三個階段：

- **Phase zero（自動PAC調配階段）** - EAP-FAST階段0，可選階段是一種隧道安全方法，用於為請求網路訪問的使用者提供具有PAC的EAP-FAST終端使用者客戶端。**向終端使用者客戶端提供PAC是零階段的唯一目的。注意：**零階段是可選的，因為PAC也可以手動調配給客戶端，而不是使用零階段。有關詳細資訊，請參閱本文檔的PAC調配模式部分。
- **階段一** — 在第一階段，ISE和終端使用者客戶端基於使用者的PAC憑證建立TLS隧道。此階段要求為試圖獲得網路訪問許可權的使用者向終端使用者客戶端提供PAC，並且PAC基於尚未過期的主金鑰。EAP-FAST的第一階段未啟用任何網路服務。
- **階段2** — 在階段2，使用者身份驗證憑證使用EAP-FAST在TLS隧道內支援的內部EAP方法安全地傳遞到客戶端和RADIUS伺服器之間使用PAC建立的RADIUS。支援將EAP-GTC、TLS和MS-CHAP作為內部EAP方法。EAP-FAST不支援其他EAP型別。

有關詳細資訊，請參閱EAP-FAST的工作原理。

PAC

PAC是強大的共用金鑰，使ISE和EAP-FAST終端使用者客戶端能夠相互進行身份驗證，並建立TLS隧道用於EAP-FAST階段2。ISE通過使用主金鑰和使用者名稱生成PAC。

PAC包括：

- **PAC-Key** — 繫結到客戶端（和客戶端裝置）和伺服器標識的共用金鑰。
- **PAC Opaque** — 客戶端快取並傳遞到伺服器的不透明欄位。伺服器恢復PAC金鑰和客戶端身份以與客戶端相互進行身份驗證。
- **PAC-Info** — 至少包含伺服器標識，以使客戶端能夠快取不同的PAC。或者，它包含其他資訊，如PAC的過期時間。

PAC調配模式

如前所述，零階段是一個可選階段。

EAP-FAST提供兩個選項來調配具有PAC的客戶端：

- **自動PAC調配（EAP-FAST第0階段或帶內PAC調配）**
- **手動（帶外）PAC調配**

帶內/自動PAC調配通過安全網路連線將新的PAC傳送到終端使用者客戶端。自動PAC調配不需要網路使用者或ISE管理員的干預，只要您配置ISE和終端使用者客戶端以支援自動調配。

最新的EAP-FAST版本支援兩種不同的帶內PAC調配配置選項：

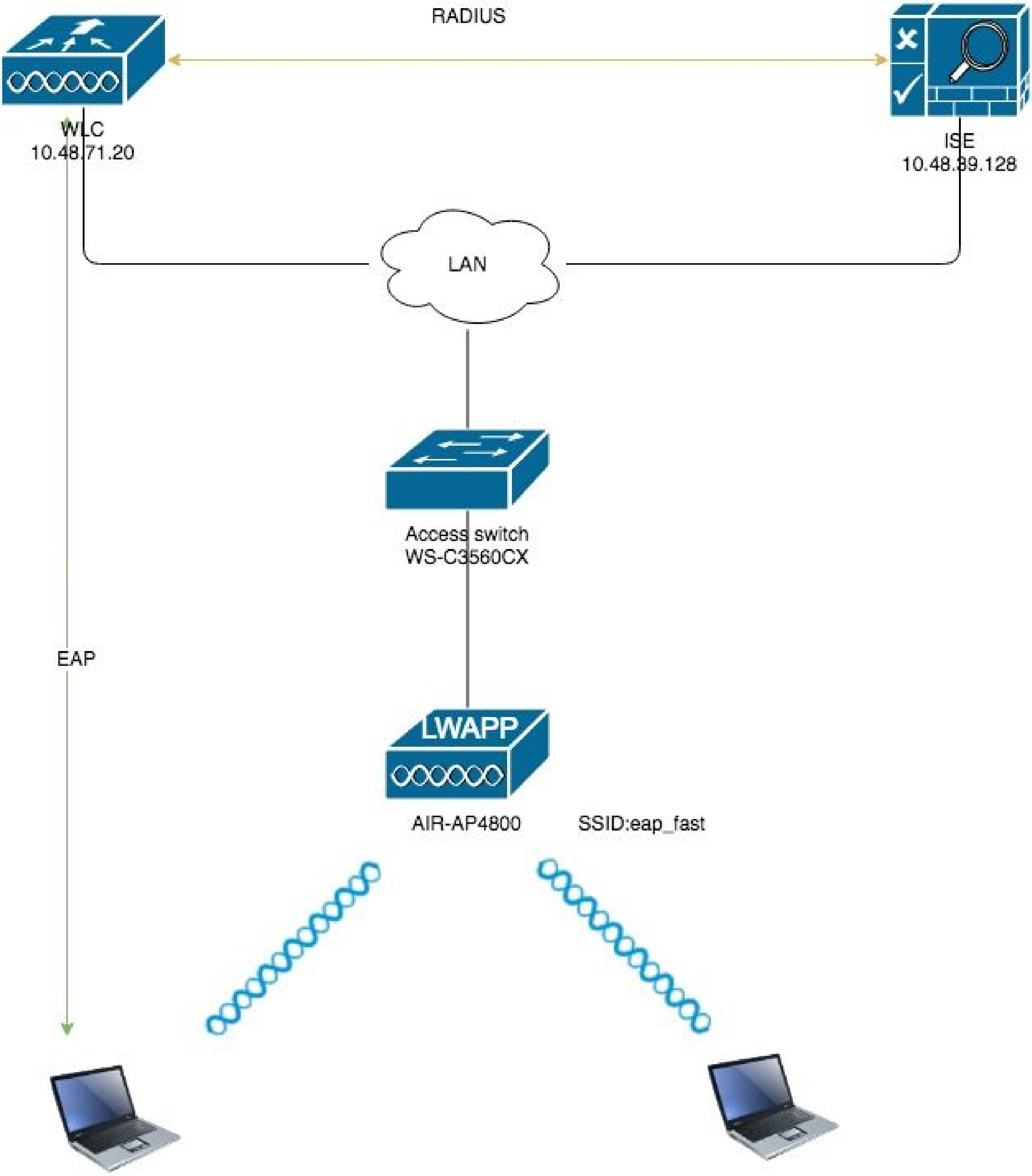
- **匿名帶內PAC調配**
- **經過身份驗證的帶內PAC調配**

注意：本文檔將討論這些帶內PAC調配方法以及如何配置它們。

帶外/手動PAC調配要求ISE管理員生成PAC文件，然後必須將其分發到適用的網路使用者。使用者必須使用其PAC檔案配置終端使用者客戶端。

設定

網路圖表



組態

配置WLC進行EAP-FAST身份驗證

執行以下步驟以配置WLC進行EAP-FAST身份驗證：

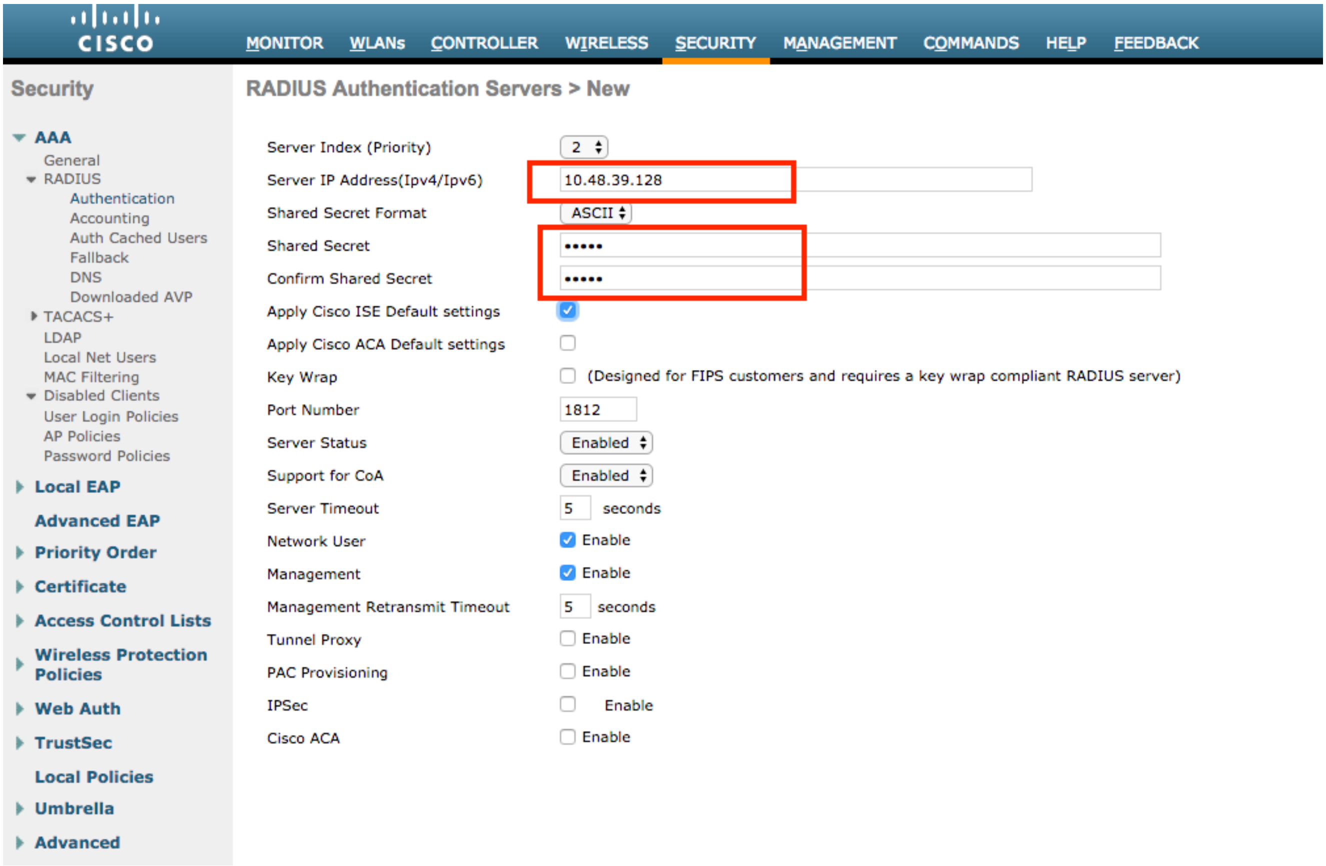
1. 設定WLC以透過外部RADIUS伺服器進行RADIUS驗證
2. 為EAP-FAST身份驗證配置WLAN

設定WLC以透過外部RADIUS伺服器進行RADIUS驗證

需要設定WLC，才能將使用者認證轉送到外部RADIUS伺服器。然後，外部RADIUS伺服器使用EAP-FAST驗證使用者憑證，並提供對無線客戶端的訪問。

完成以下步驟，設定外部RADIUS伺服器的WLC:

1. 從控制器GUI中選擇**Security**和**RADIUS Authentication**，以顯示「RADIUS Authentication Servers」頁面。接下來，按一下**New**以定義RADIUS伺服器。
2. 在**RADIUS Authentication Servers > New**頁面上定義RADIUS伺服器引數。這些引數包括：RADIUS伺服器IP位址共用金鑰連線埠號碼伺服器狀態本文檔使用IP地址為10.48.39.128的ISE伺服器。



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

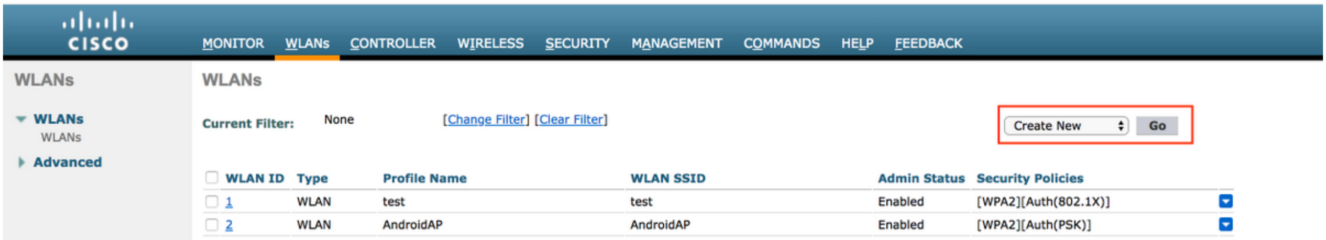
3. 按一下 **應用**.

為EAP-FAST身份驗證配置WLAN

接下來，配置客戶端用於連線到無線網路以進行EAP-FAST身份驗證的WLAN，並將其分配給動態介面。在此示例中配置的WLAN名稱為**eap fast**。此範例將此WLAN指派給管理介面。

完成以下步驟以設定**eap fast** WLAN及其相關引數：

1. 從控制器的GUI中按一下「**WLANs**」，以顯示「WLANs」頁面。此頁面列出控制器上存在的WLAN。
2. 按一下**New**以建立一個新的WLAN。

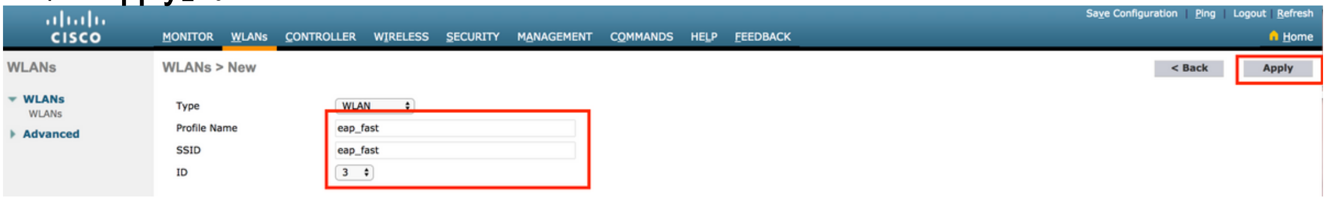


WLANs

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)]

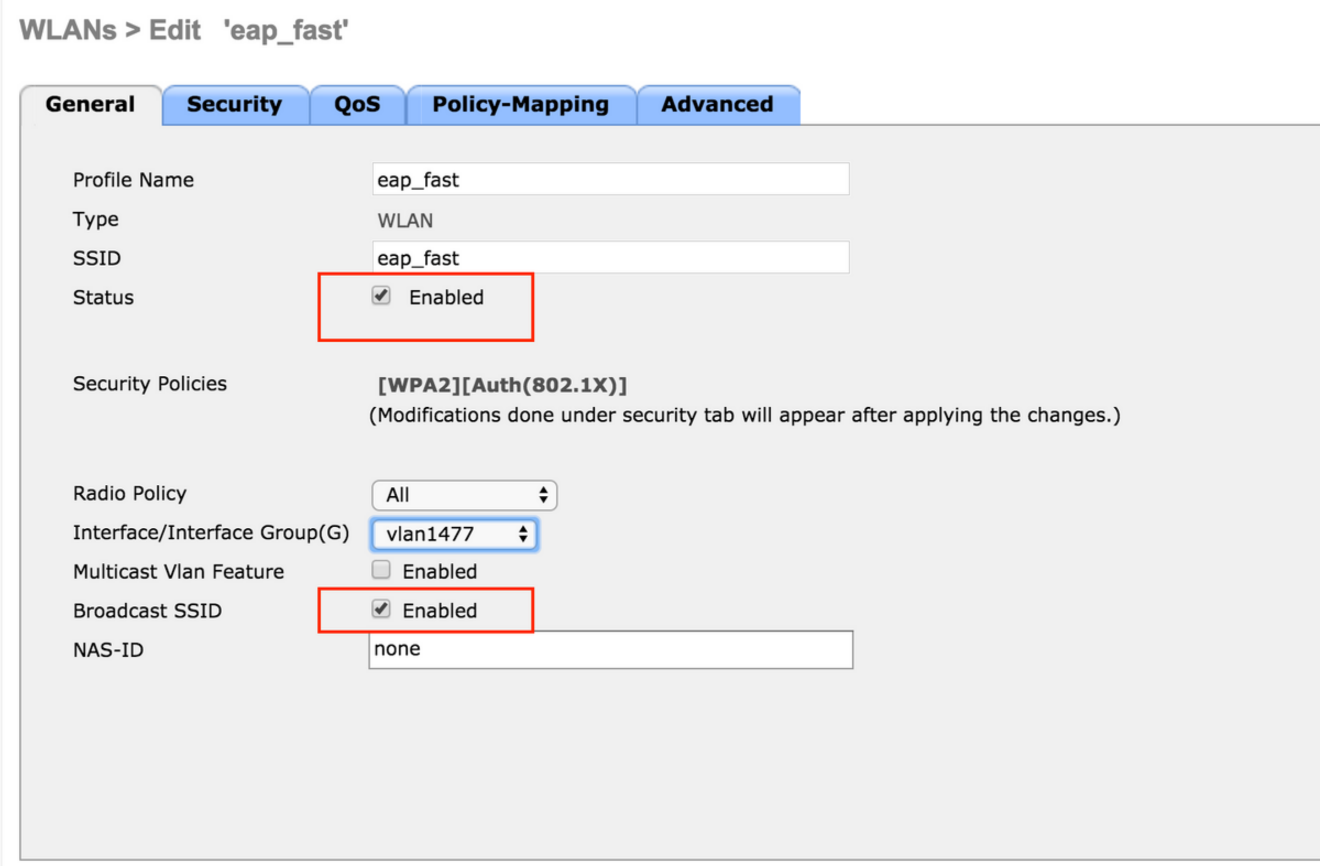
3. 在WLANs > New頁面上配置**eap_fast** WLAN SSID名稱、配置檔名稱和WLAN ID。然後，按一下「**Apply**」。



WLANs > New

Type	WLAN
Profile Name	eap_fast
SSID	eap_fast
ID	3

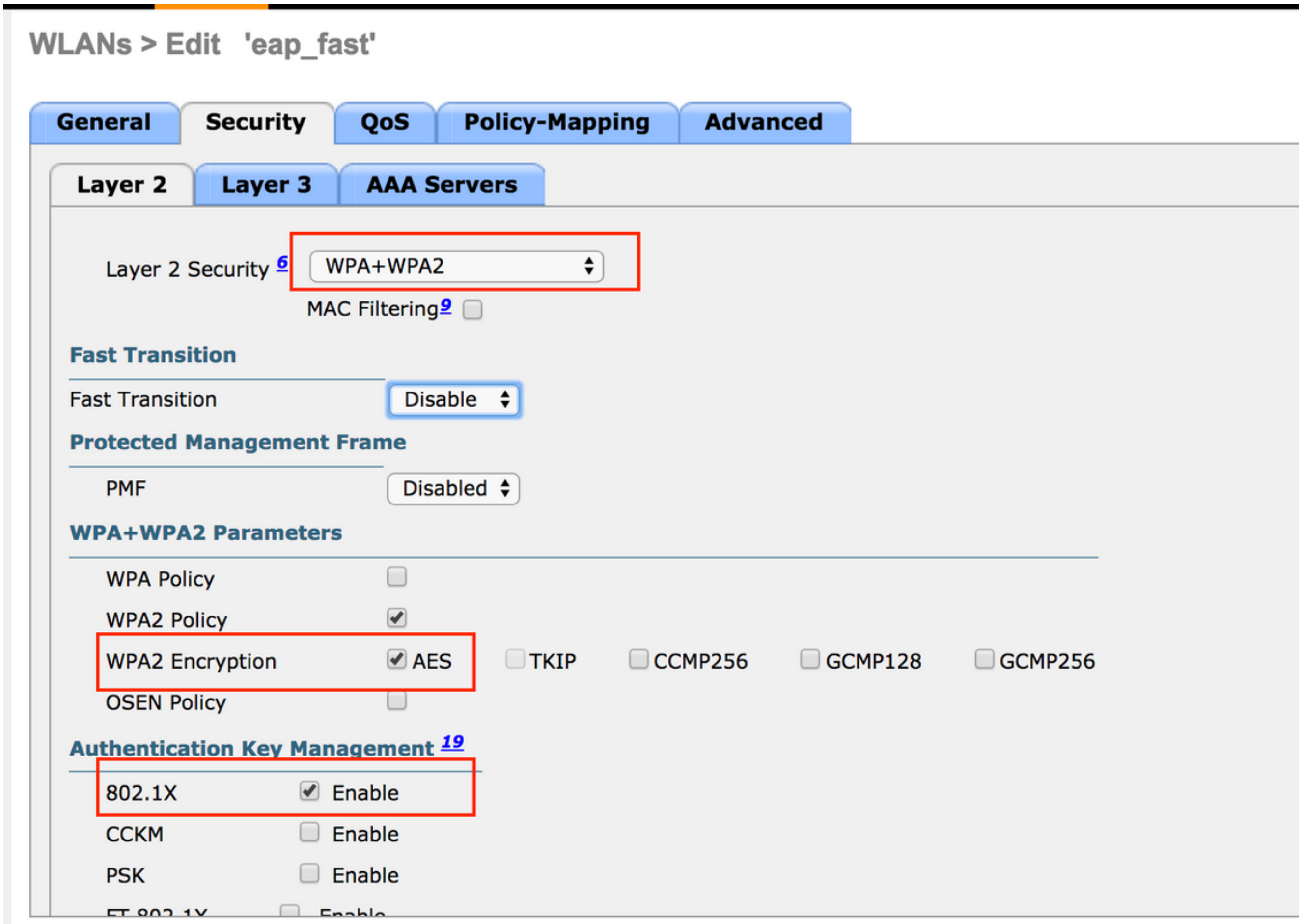
4. 建立新的WLAN後，系統會顯示新WLAN的**WLAN > Edit**頁面。在此頁面上，您可以定義此WLAN的特定各種引數。這包括常規策略、RADIUS伺服器、安全策略和802.1x引數。
5. 勾選**General Policies**索引標籤下的**Admin Status**覈取方塊以啟用WLAN。如果您希望AP在其信標幀中廣播SSID，請選中**Broadcast SSID**覈取方塊。



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 ->編輯 — >安全 — >第2層"** 頁籤選擇WPA/WPA2引數，並為AKM選擇dot1x。
   此範例為此WLAN使用WPA2/AES + dot1x作為第2層安全性。其它引數可以根據WLAN網路的要求進行修改。



WLANs > Edit 'eap_fast'

Layer 2 Security [6] WPA+WPA2

MAC Filtering[9] □

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]

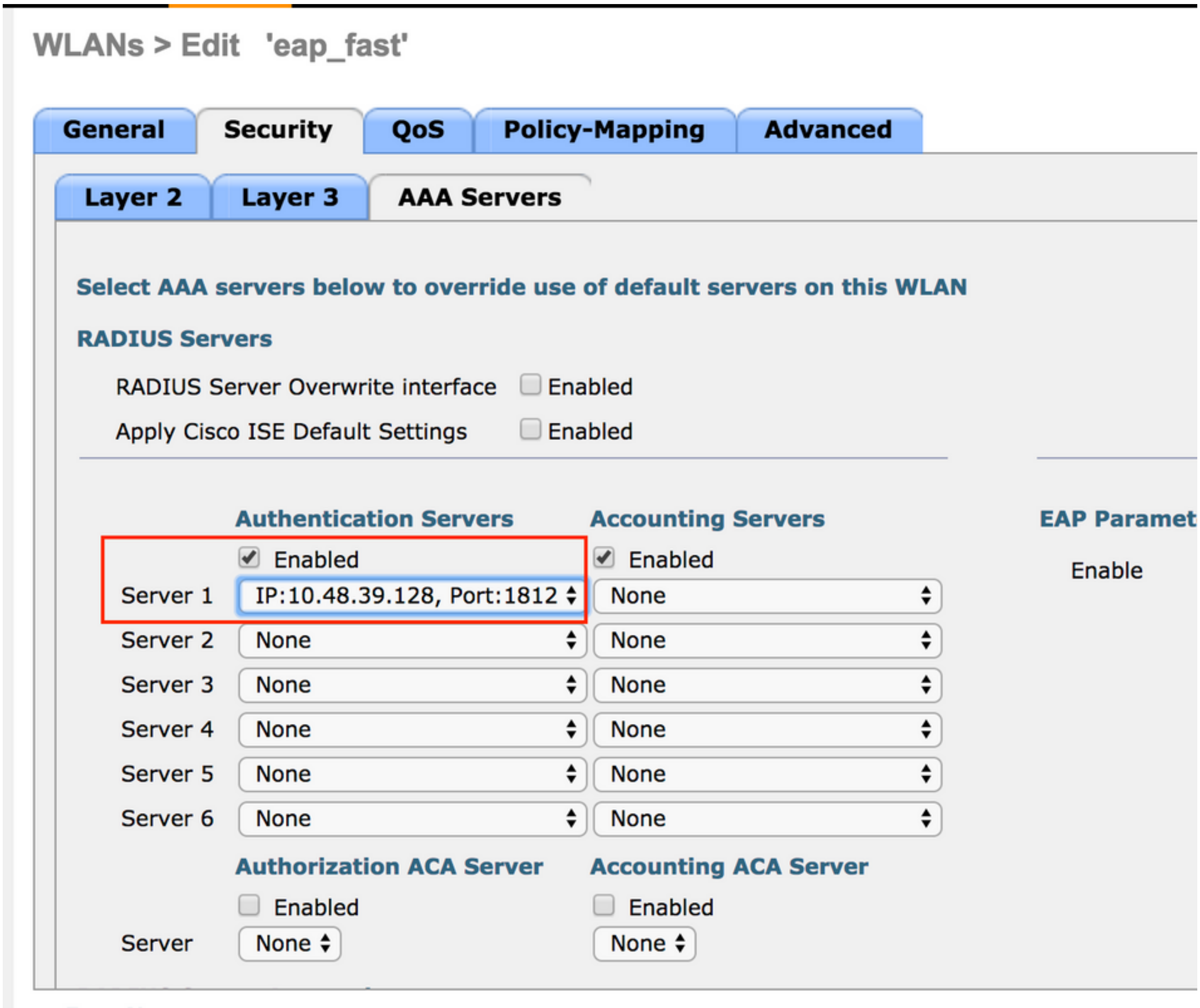
802.1X ☑ Enable

CCKM □ Enable

PSK □ Enable

FT 802.1X □ Enable

7. 在「WLAN -> Edit -> Security -> AAA Servers」頁籤下，從RADIUS Servers下的下拉選單中選擇適當的RADIUS伺服器。



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

EAP Paramet

Enable

	Authorization ACA Server	Accounting ACA Server
	□ Enabled	□ Enabled
Server	None	None

8. 按一下「**Apply**」。**注意：**這是需要在控制器上為EAP身份驗證配置的唯一EAP設定。EAP-FAST的所有其他配置需要在RADIUS伺服器和需要身份驗證的客戶端上完成。

為EAP-FAST身份驗證配置RADIUS伺服器

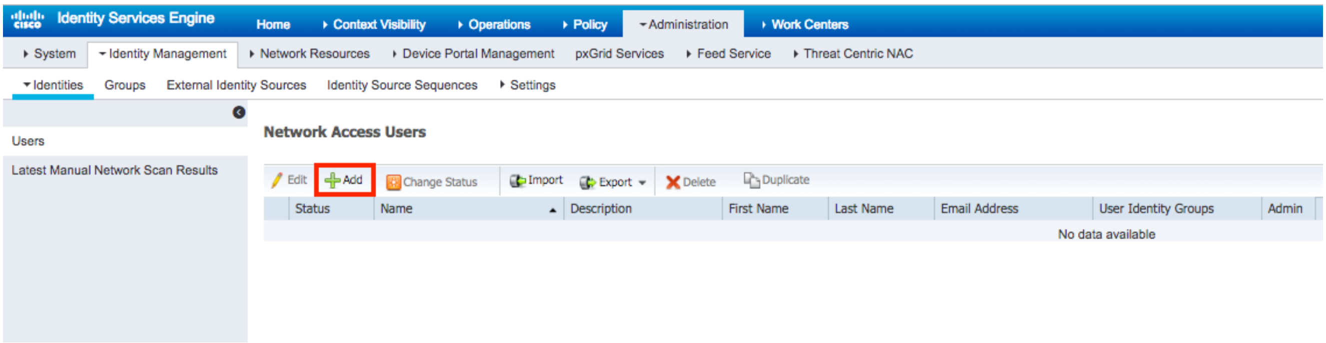
執行以下步驟以配置RADIUS伺服器進行EAP-FAST身份驗證：

1. 建立使用者資料庫以驗證EAP-FAST客戶端
2. 將WLC作為AAA使用者端新增到RADIUS伺服器
3. 使用匿名帶內PAC調配在RADIUS伺服器上配置EAP-FAST身份驗證
4. 使用經過身份驗證的帶內PAC調配在RADIUS伺服器上配置EAP-FAST身份驗證

建立使用者資料庫以驗證EAP-FAST客戶端

此示例將EAP-FAST客戶端的使用者名稱和密碼分別配置為<*eap_fast*>和<*EAP-fast1*>。

1. 在ISE Web管理員UI中，在「**管理**」 **—>**「**身份管理**」 **—>**「**使用者**」下導航，**然後按「新增**」圖示。

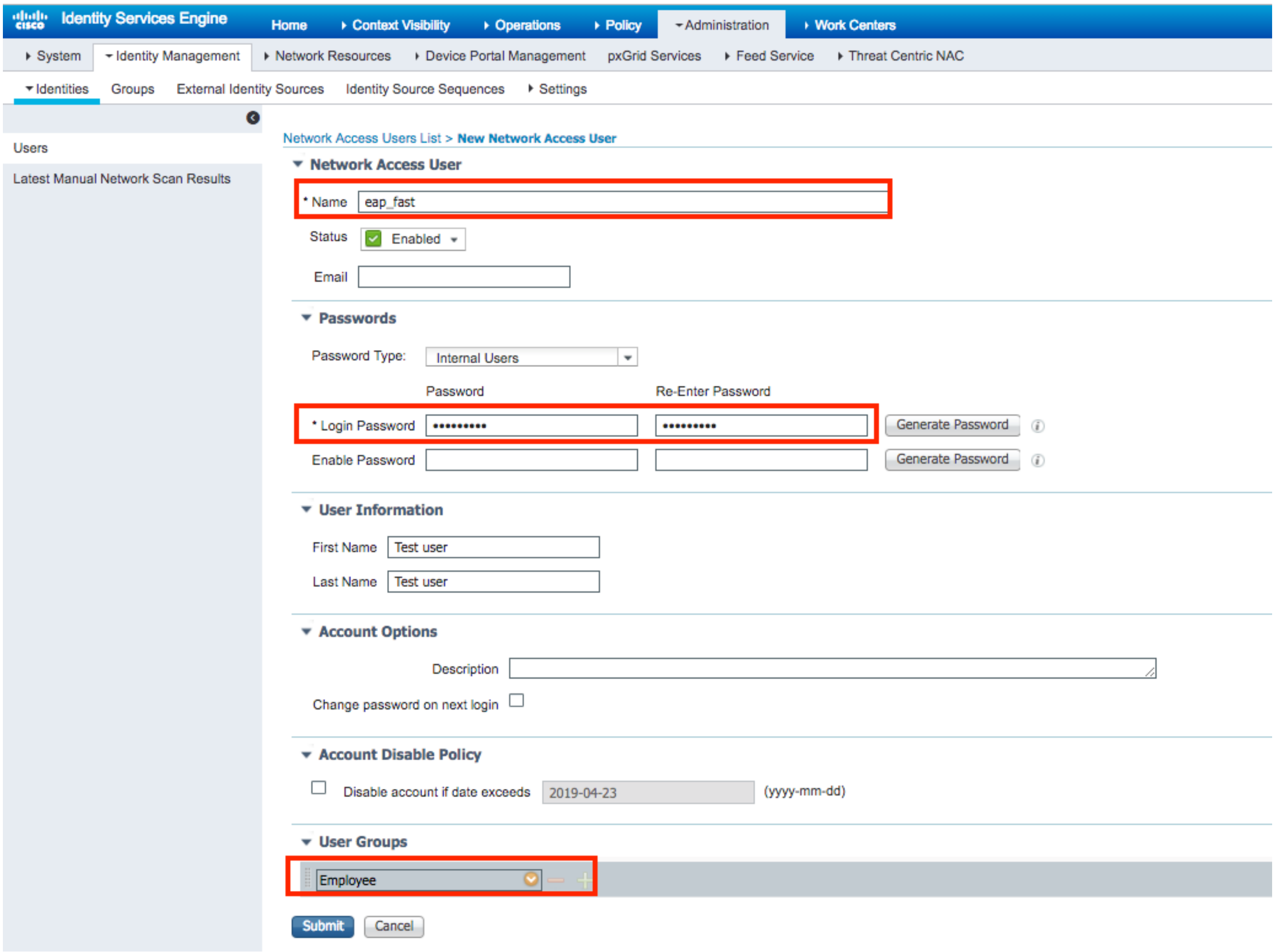


Network Access Users

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

No data available

2. 填寫要建立使用者所需的表單 — 「Name」和「Login password」 ，然後從下拉選單中選擇「User group」 ;[可選，您可以填寫使用者帳戶的其他資訊]
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 □

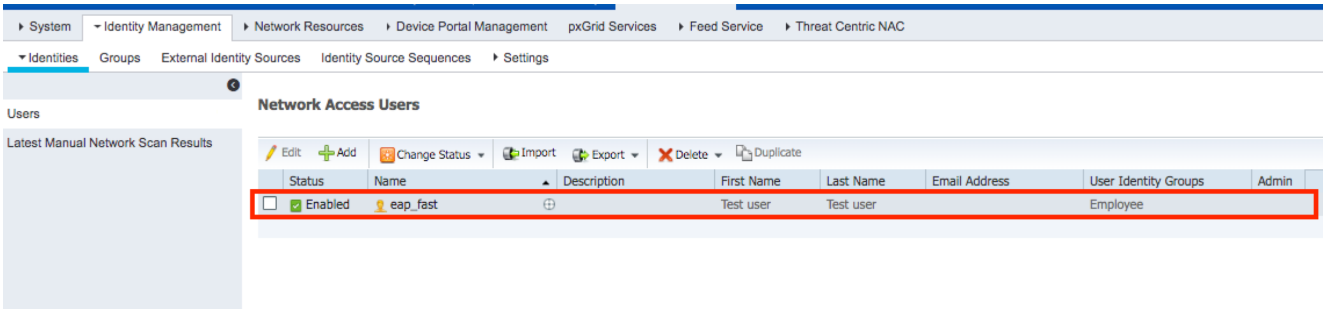
Account Disable Policy

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

User Groups

Employee

3. 已建立使用者。



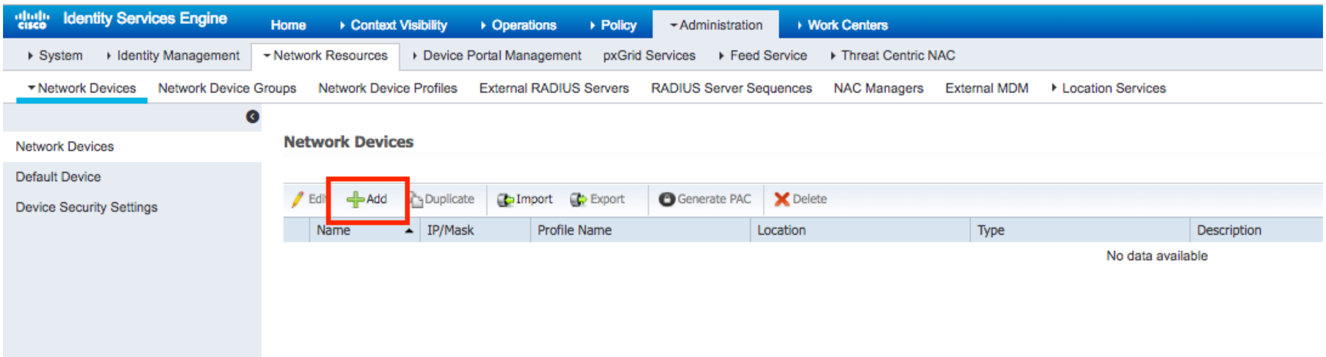
Network Access Users

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

將WLC作為AAA使用者端新增到RADIUS伺服器

完成以下步驟，將控制器定義為ACS伺服器上的AAA使用者端：

1. 在ISE Web管理UI中，在**「管理」 —>「網路資源」 —>「網路裝置」**下導航，**然後按「新增」**圖示。

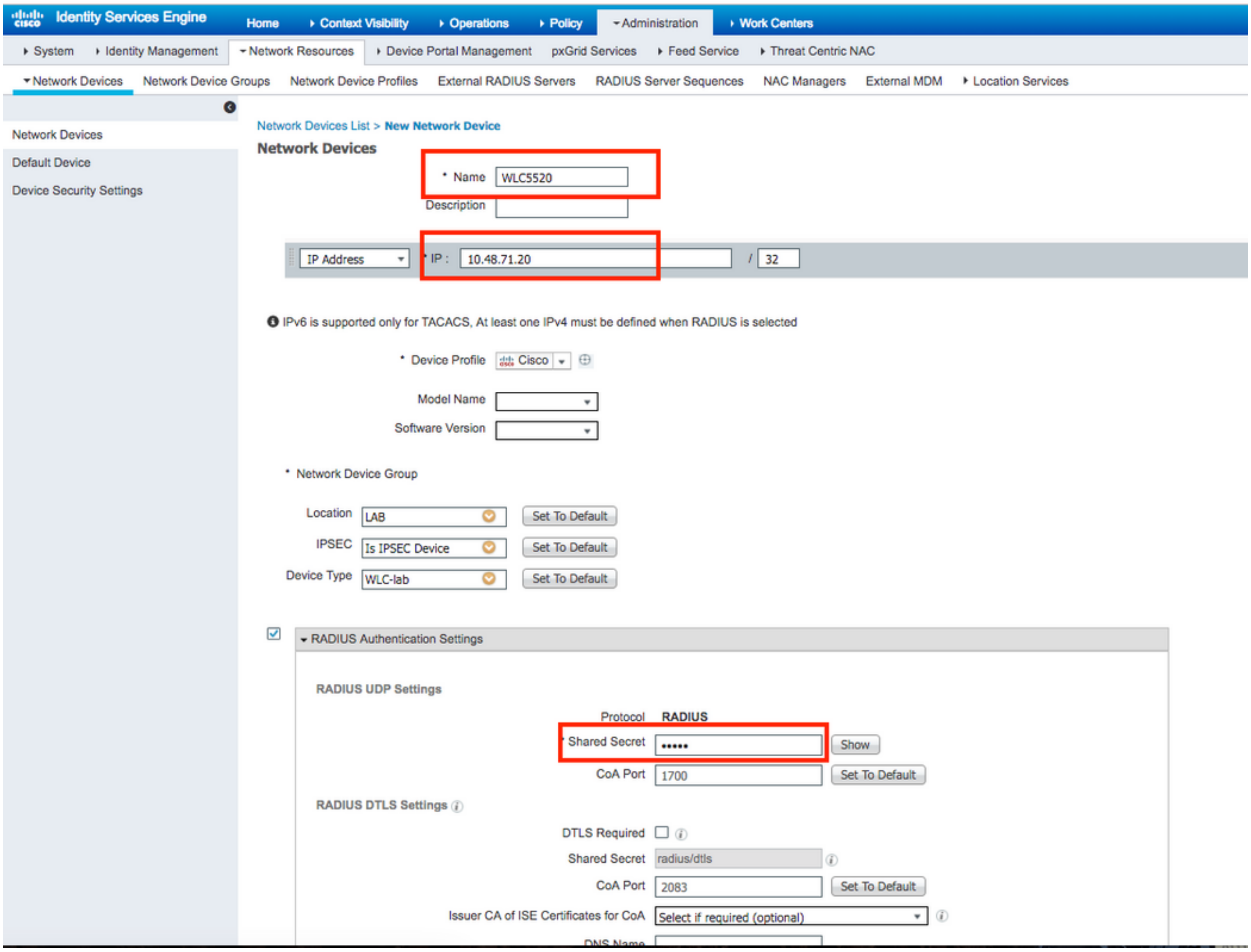


Network Devices

Name	IP/Mask	Profile Name	Location	Type	Description

No data available

2. 填寫要新增的裝置的所需表單 — 「**Name**」、「**IP**」並配置相同的共用金鑰密碼（如我們在前面的章節中在WLC上配置的一樣），在「**Shared Secret**」表單中[您可以選擇填寫裝置的其它資訊，如位置、組等]。
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: □

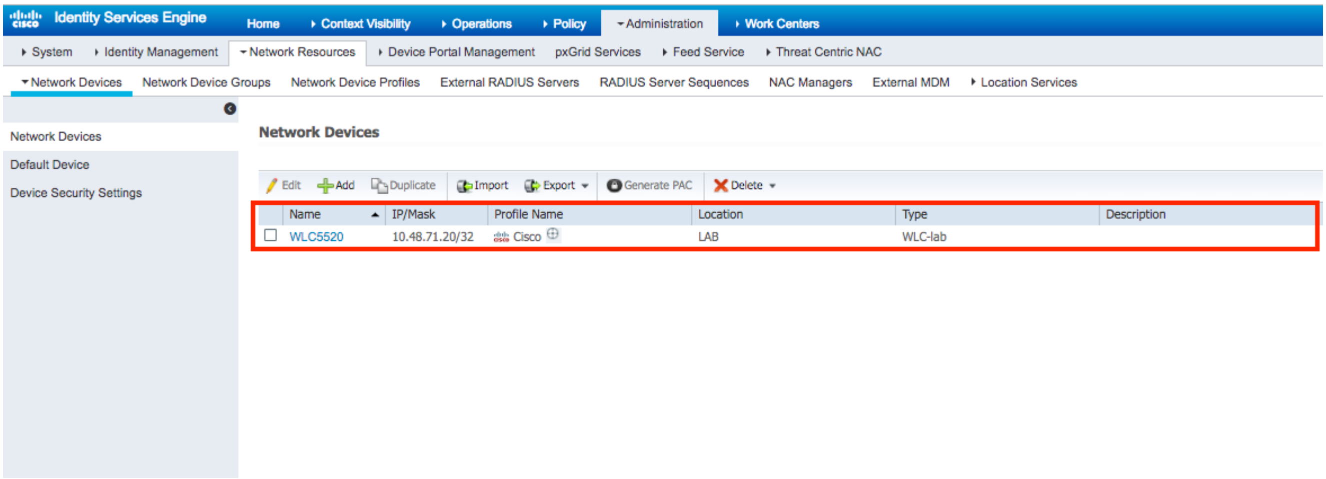
Shared Secret: radius/dtls

CoA Port: 2083

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

DNS Name

3. 裝置已新增到ISE網路訪問裝置清單。(NAD)



Network Devices

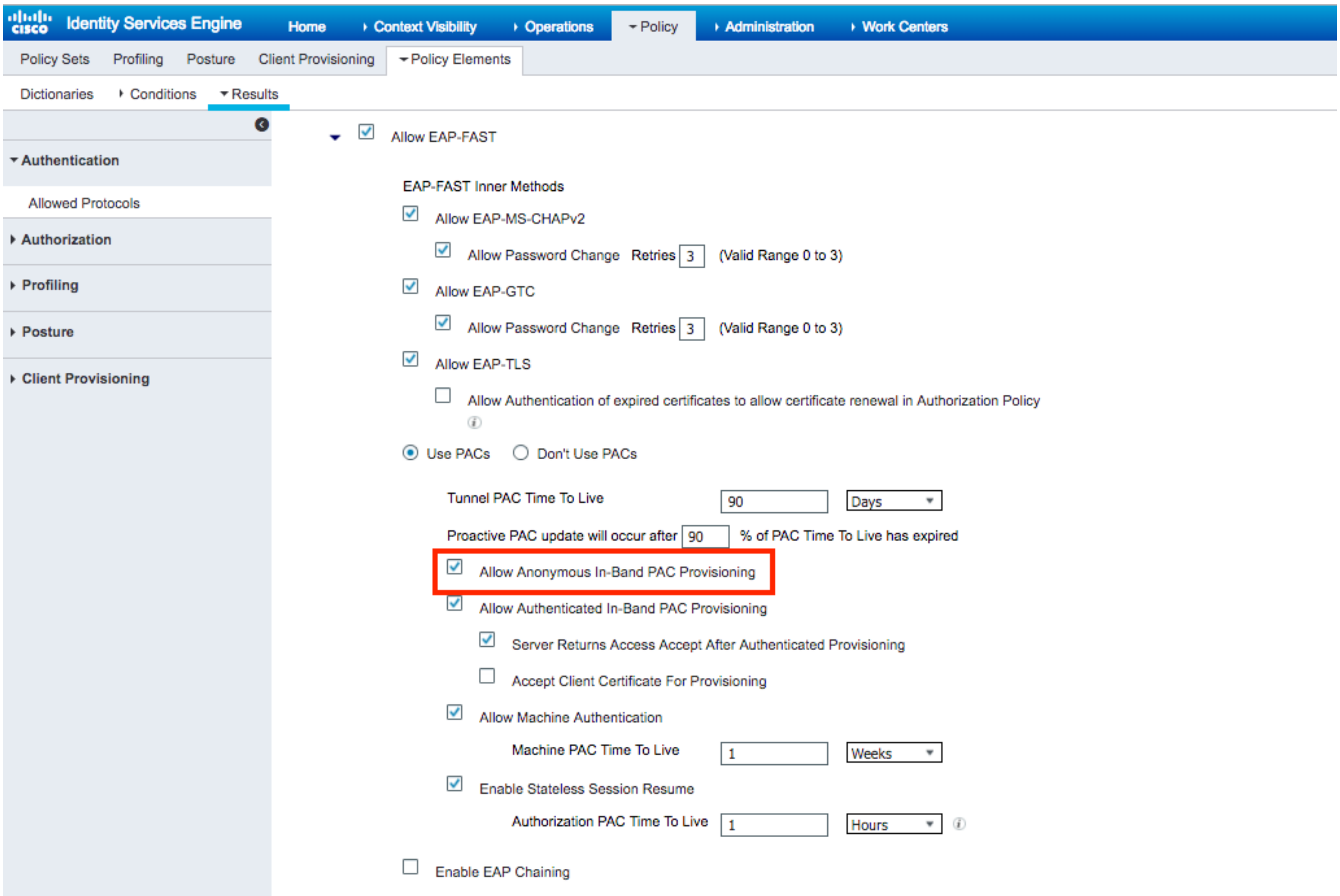
	Name	IP/Mask	Profile Name	Location	Type	Description
□	WLC5520	10.48.71.20/32	Cisco	LAB	WLC-lab	

使用匿名帶內PAC調配在RADIUS伺服器上配置EAP-FAST身份驗證

通常，如果部署中沒有PKI基礎設施，則希望使用此類方法。

在對等體驗證ISE伺服器之前，此方法運行在已驗證Diffie-Hellman金鑰協定協定(ADHP)隧道中。

要支援此方法，我們需要在ISE的「身份驗證允許的協定」(**Authentication Allowed Protocols)下啟用「Allow Anonymous In-band PAC Provisioning**」：



☑ 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

注意：請確保您已允許密碼型別身份驗證，如用於EAP-FAST內部方法的EAP-MS-CHAPv2，因為顯然使用匿名帶內調配時，我們無法使用任何證書。

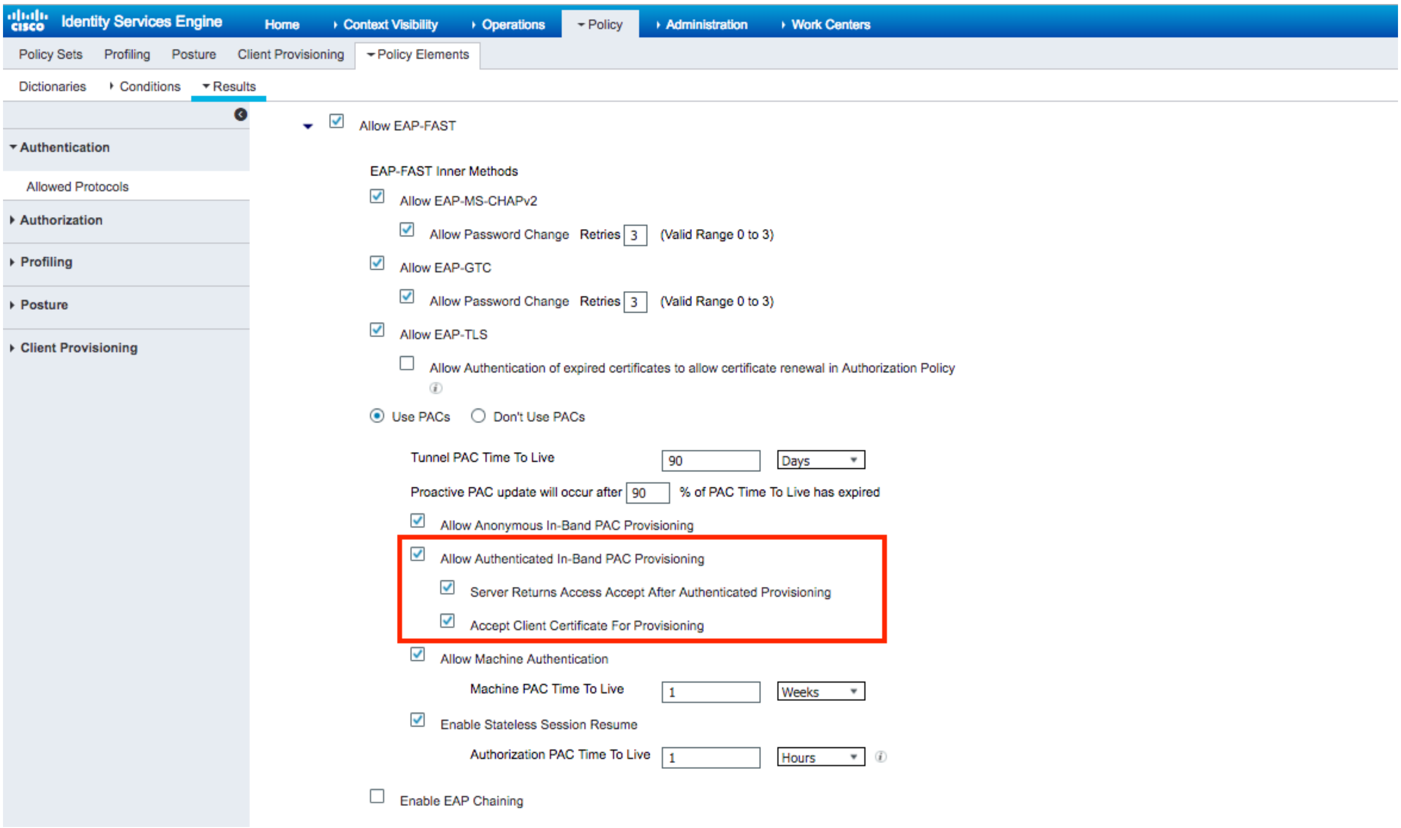
使用經過身份驗證的帶內PAC調配在RADIUS伺服器上配置EAP-FAST身份驗證

這是最安全和推薦的選項。TLS隧道基於由請求方驗證的伺服器證書構建，客戶端證書由ISE驗證（預設）。

該選項要求客戶端和伺服器具有PKI基礎架構，儘管它可能僅限於伺服器端或在兩端被跳過。

在ISE上，還有兩個用於身份驗證帶內調配的額外選項：

1. 「**Server Returns Access Accept After Authenticated Provisioning**」 - 通常，在PAC調配後，應傳送Access-Reject，強制請求方使用PAC重新進行身份驗證。但是，由於PAC設定是在經過驗證的TLS隧道中完成的，因此我們可以立即使用Access-Accept進行響應，以最小化身份驗證時間。（在這種情況下，請確保客戶端和伺服器端有受信任證書）。
2. **「Accept Client Certificate For Provisioning」 — 如果不想向客戶端裝置提供PKI基礎設施，並且僅在ISE上具有受信任證書，則啟用該選項，該選項允許跳過伺服器端客戶端證書驗證。**



☑ 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

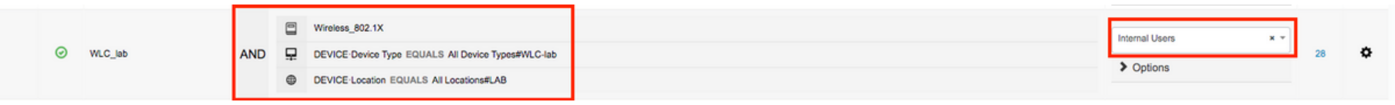
Machine PAC Time To Live 1 Weeks

☑ Enable Stateless Session Resume

Authorization PAC Time To Live 1 Hours

□ Enable EAP Chaining

在ISE上，我們還為無線使用者定義簡單身份驗證策略集，以下示例使用裝置型別和位置以及身份驗證型別作為條件引數，匹配該條件的身份驗證流將根據內部使用者資料庫進行驗證。



WLC_lab AND Wireless_802.1X

DEVICE·Device Type EQUALS All Device Types#WLC-lab

DEVICE·Location EQUALS All Locations#LAB

Internal Users

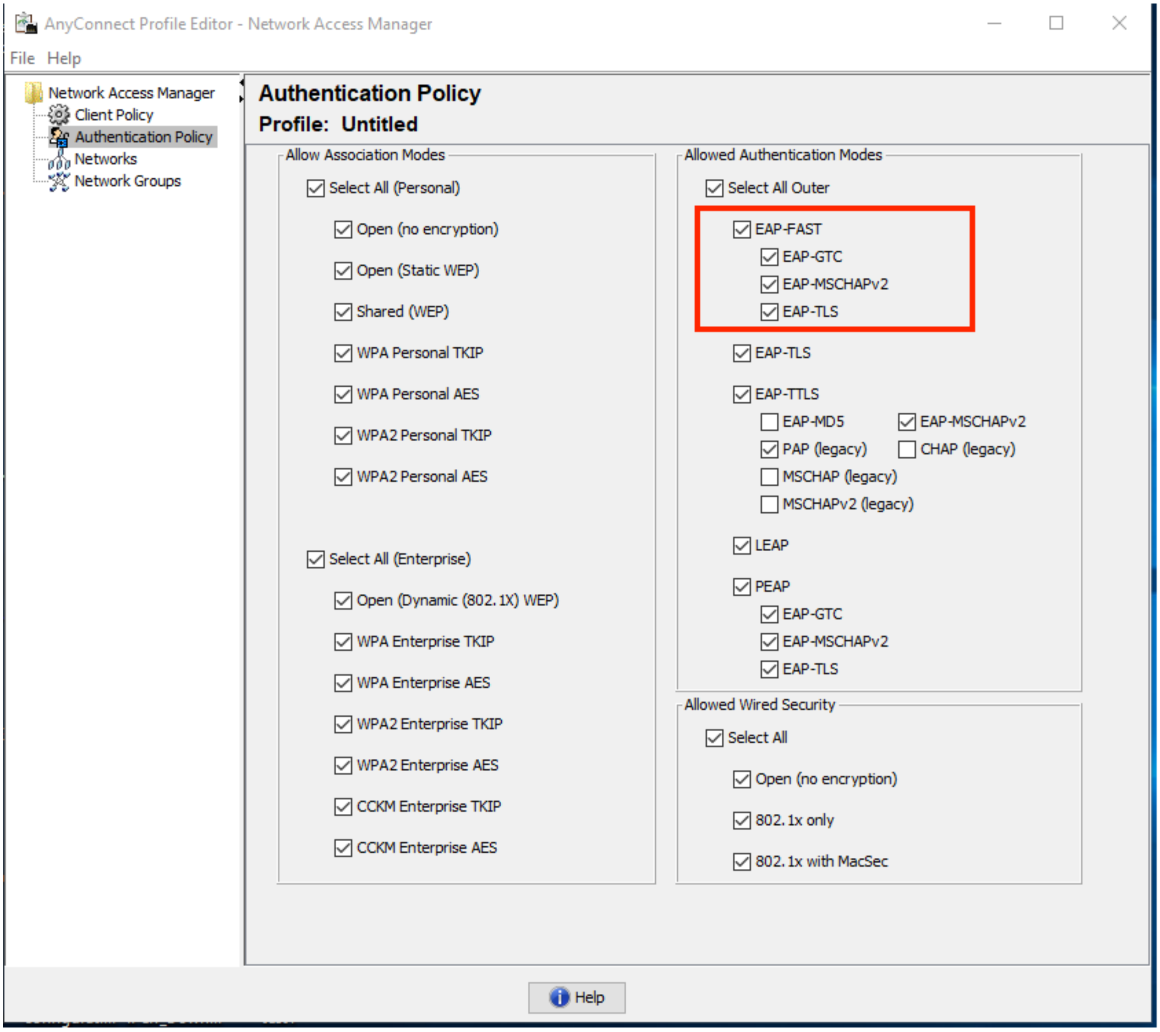
驗證

此範例將顯示經過驗證的帶內PAC布建流程和網路存取管理員(NAM)組態設定以及各自的WLC偵錯。

NAM配置檔案配置

要配置Anyconnect NAM配置檔案以使用EAP-FAST對ISE驗證使用者會話，需要執行以下步驟：

1. 開啟網路訪問管理器配置檔案編輯器並載入當前配置檔案。
2. 確保在「允許**的驗證模**式」下啟用**「EAP-FAST」**



AnyConnect Profile Editor - Network Access Manager

File Help

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

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

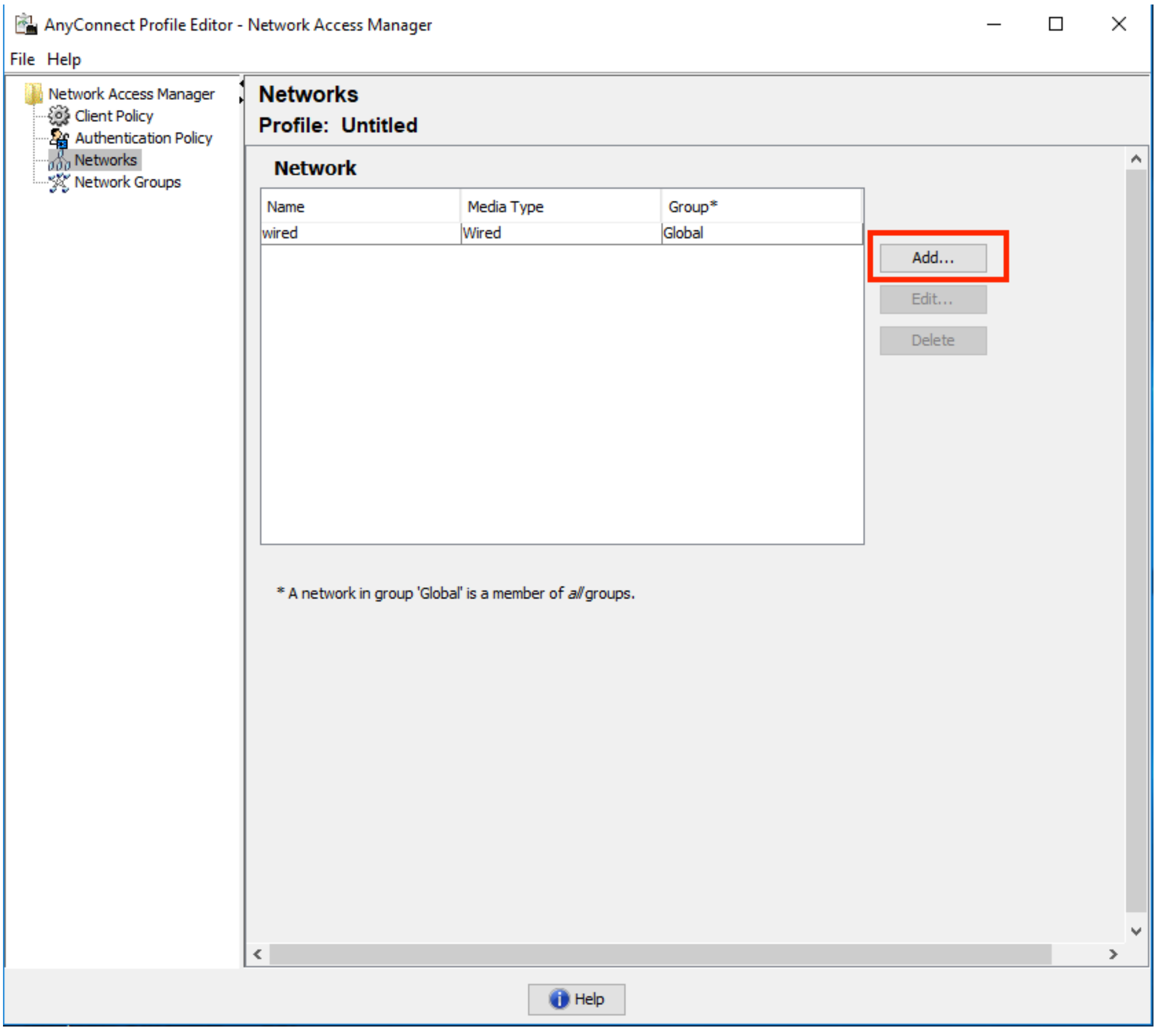
Allowed Authentication Modes

☑ 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. "**Add**"一個新網路設定檔：



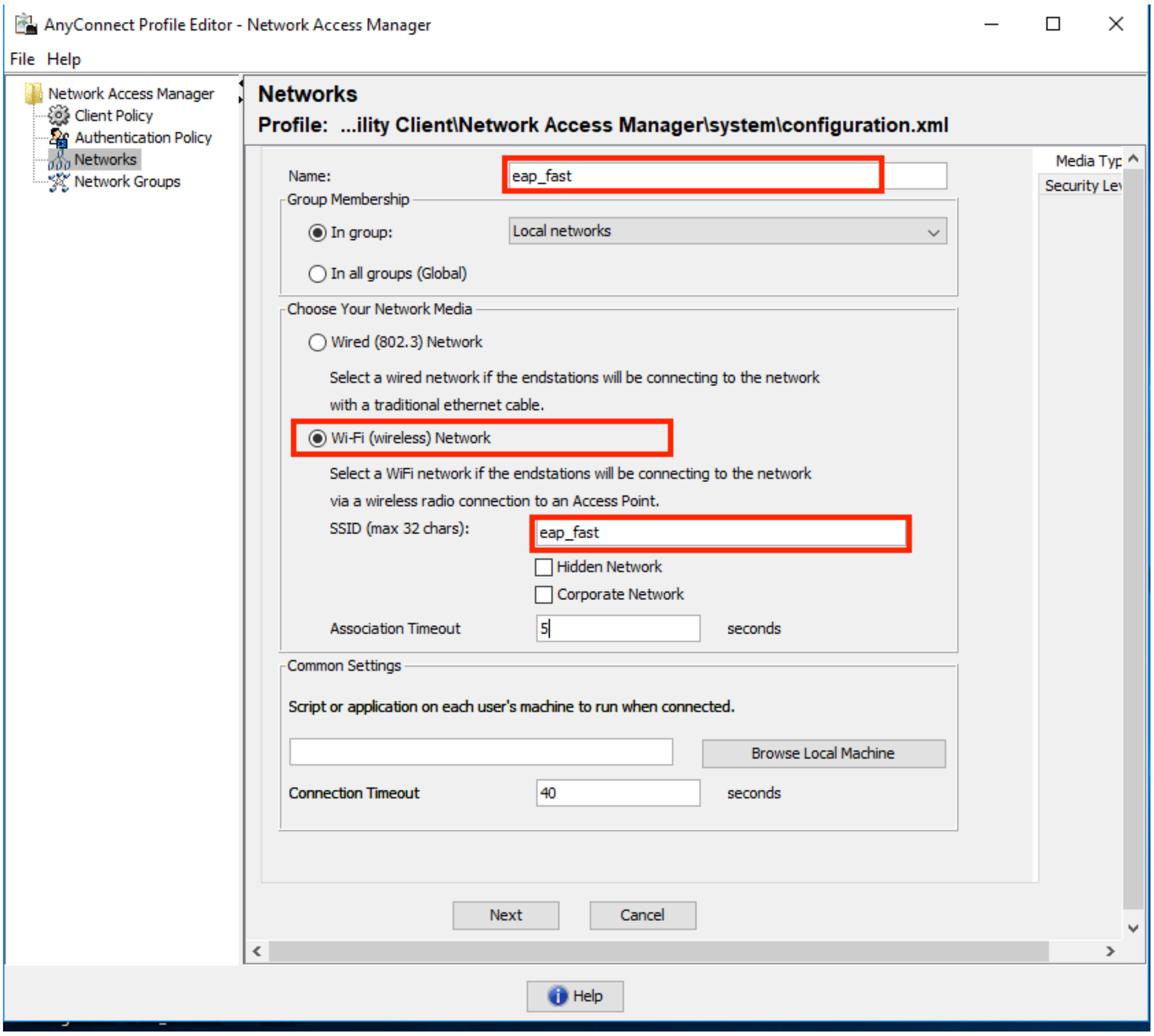
Networks
Profile: Untitled

Network

Name	Media Type	Group*
wired	Wired	Global

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

4. 在「**Media type**」配置部分下定義配置檔案「**Name**」，wireless作為您的媒體網路型別，並指定SSID名稱。



AnyConnect Profile Editor - Network Access Manager

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

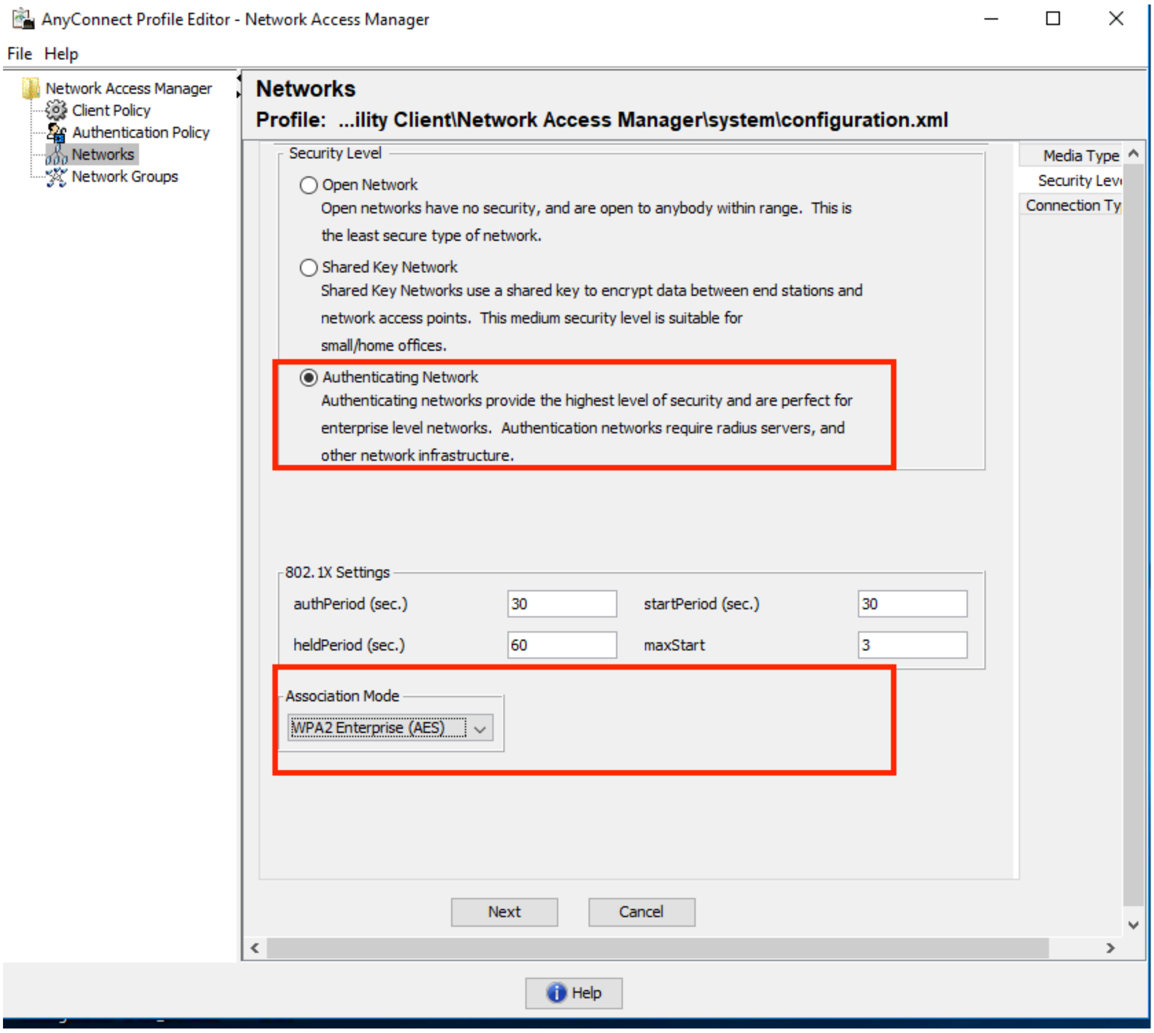
Common Settings

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

Browse Local Machine

Connection Timeout 40 seconds

5. 在「安**全級別」配置**頁籤下，選擇「驗證網路」，並將關聯模式指定為WPA2企業(AES)



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.

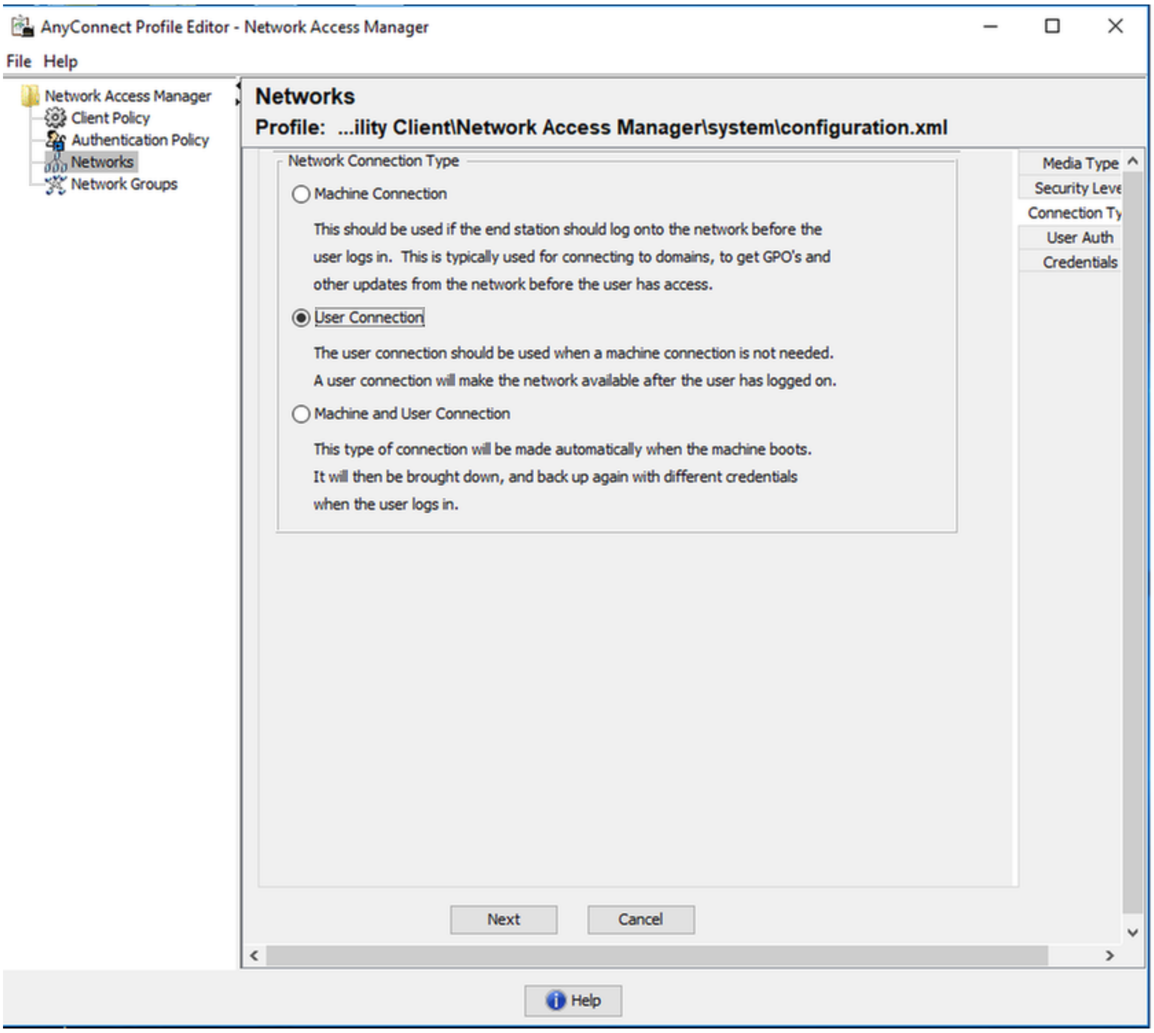
● Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

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

Association Mode: WPA2 Enterprise (AES)

6. 在本例中，我們使用使用者型別身份驗證，因此，在下一個頁籤「Connection type」下選擇「User Connection」



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.

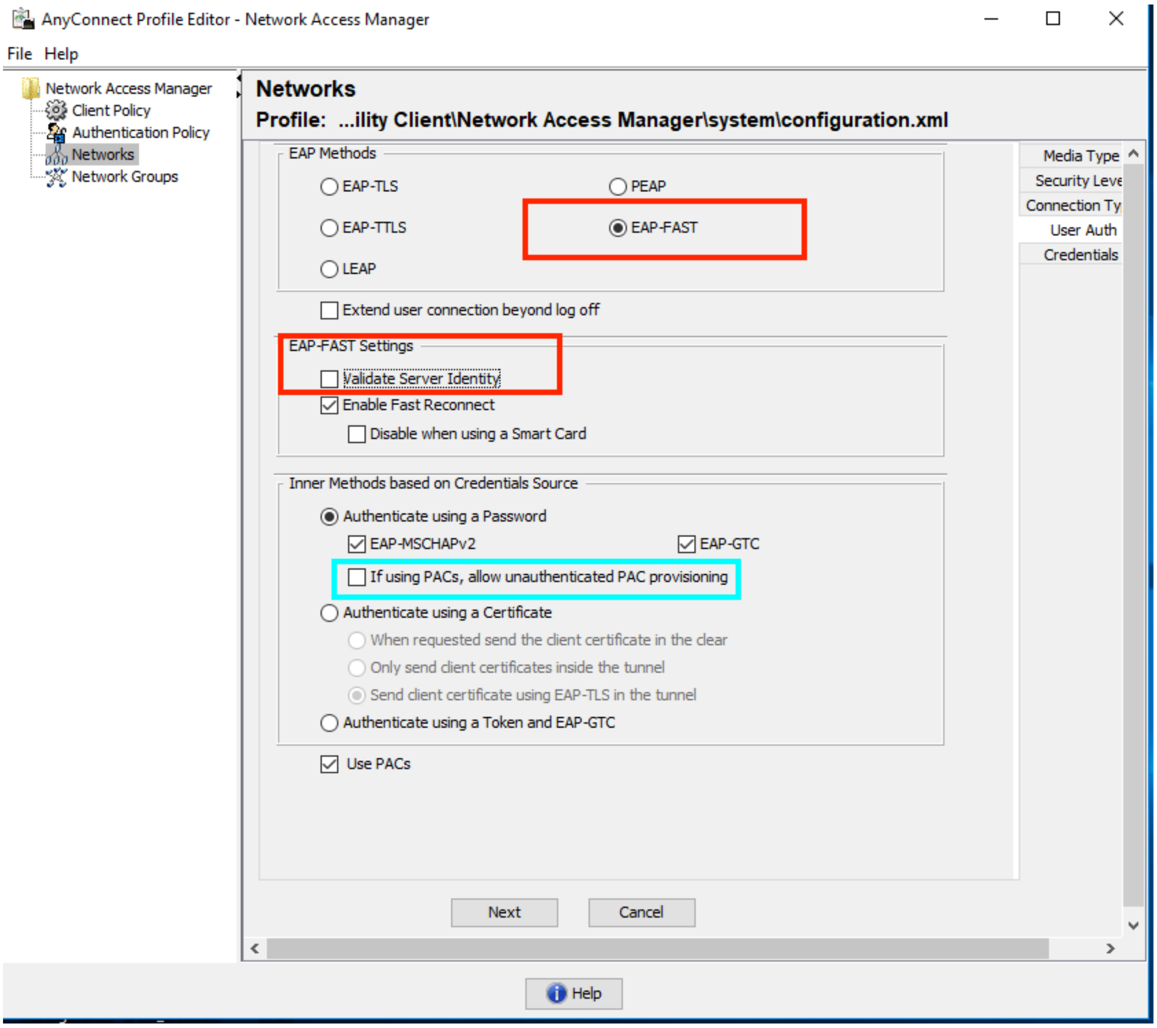
● User Connection

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**」頁籤下，將EAP-FAST指定為允許的身份驗證方法，並禁用伺服器證書驗證，因為在本示例中，我們沒有使用受信任的證書。



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

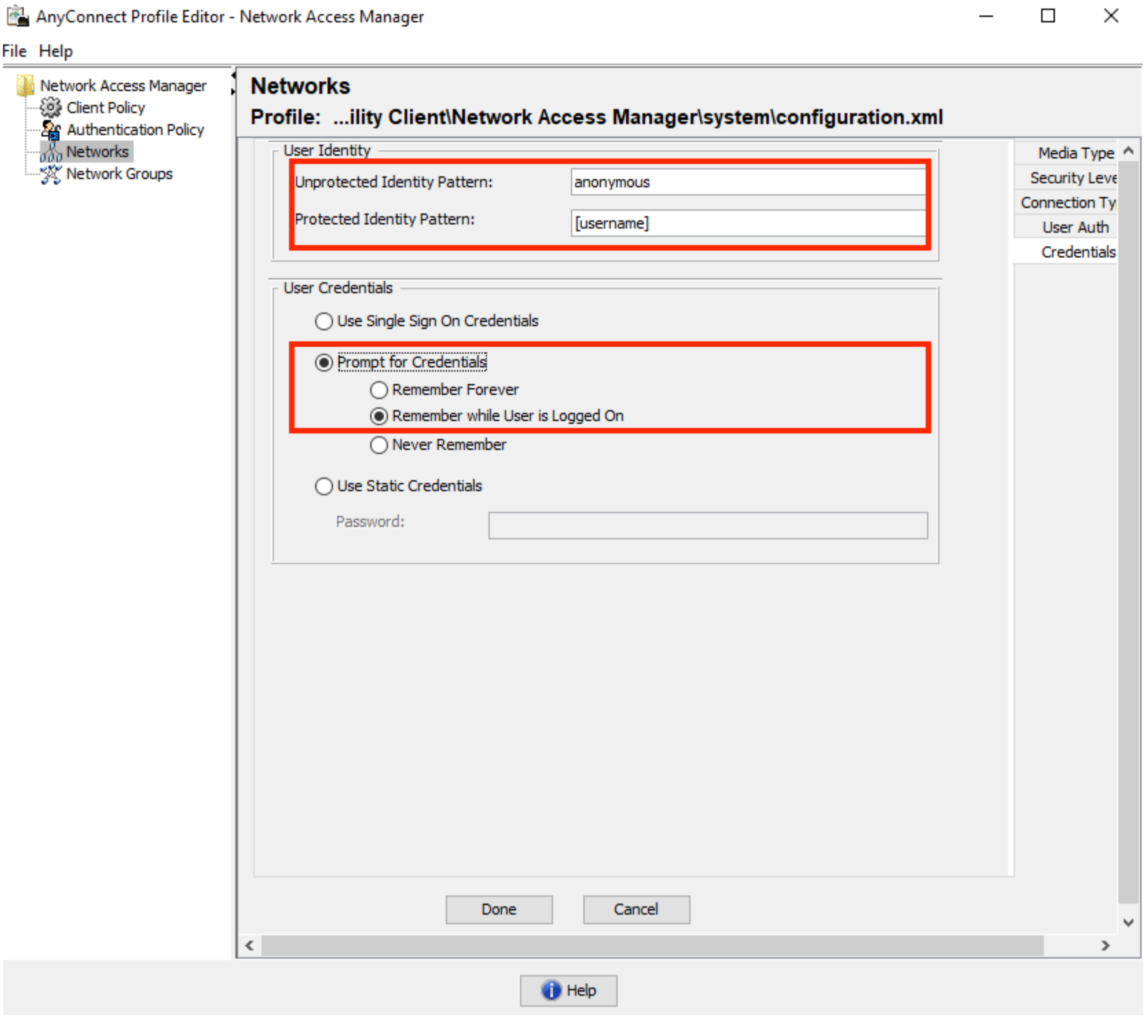
○ Authenticate using a Token and EAP-GTC

☑ Use PACs

注意：在實際生產環境中，請確保在ISE上安裝受信任證書並在NAM設定中啟用伺服器證書驗證選項。

附註：僅當出現匿名帶內PAC調配時，才必須選擇「如果使用PAC，允許未經身份驗證的PAC調配」選項。

8. 定義使用者憑證，如果您願意使用與用於登入的相同憑證，可以定義為SSO；如果您希望使用者在連線到網路時需要提供憑證，請選擇「提示輸入憑證」；或者定義該訪問型別的靜態憑證。在本示例中，我們提示使用者在嘗試連線到網路時輸入憑據。



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

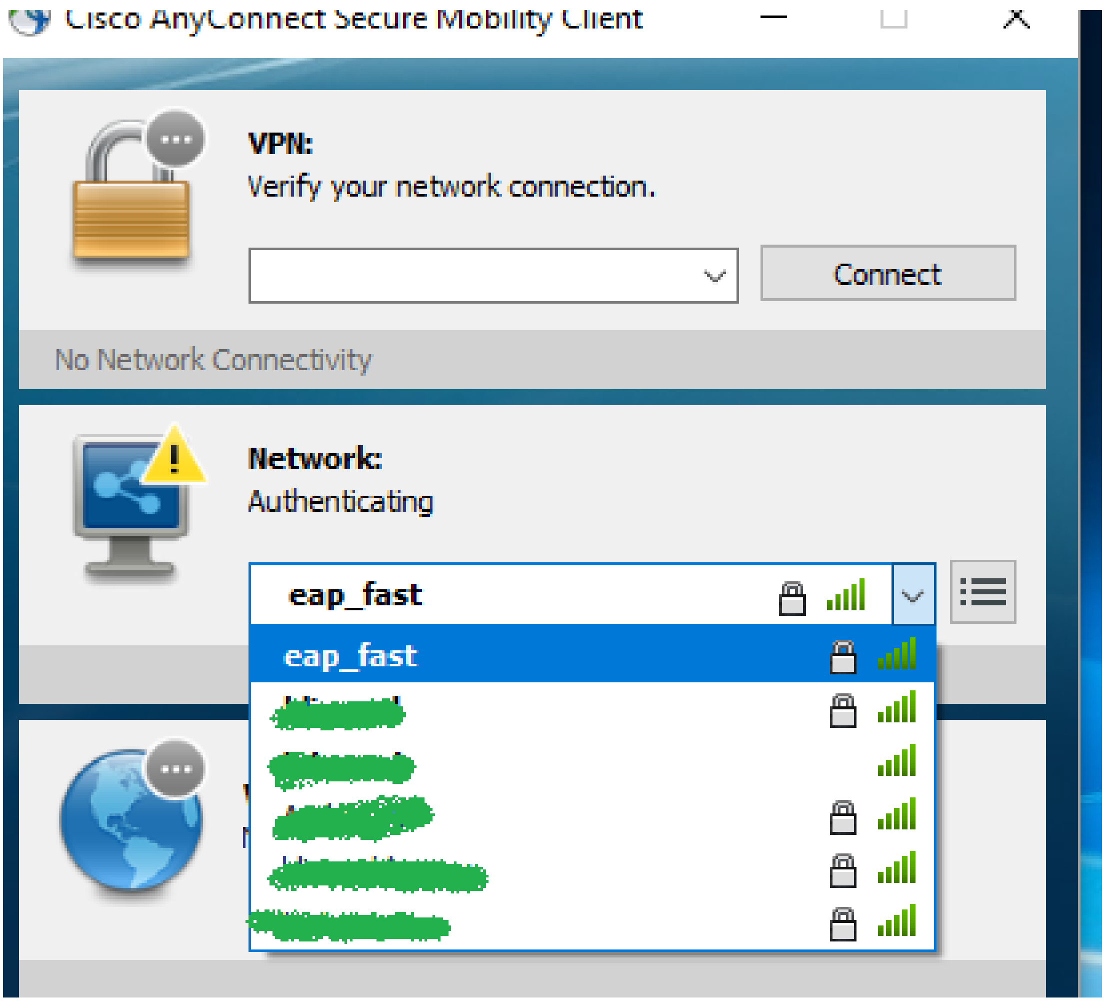
○ Use Static Credentials

Password:

9. 將配置的配置檔案儲存到各自的NAM資料夾中。

使用EAP-FAST身份驗證測試與SSID的連線。

1. 從Anyconnect網路清單中選擇相應的配置檔案



Cisco AnyConnect Secure Mobility Client

VPN:
Verify your network connection.

No Network Connectivity

Network:
Authenticating

eap_fast

eap_fast

[redacted]

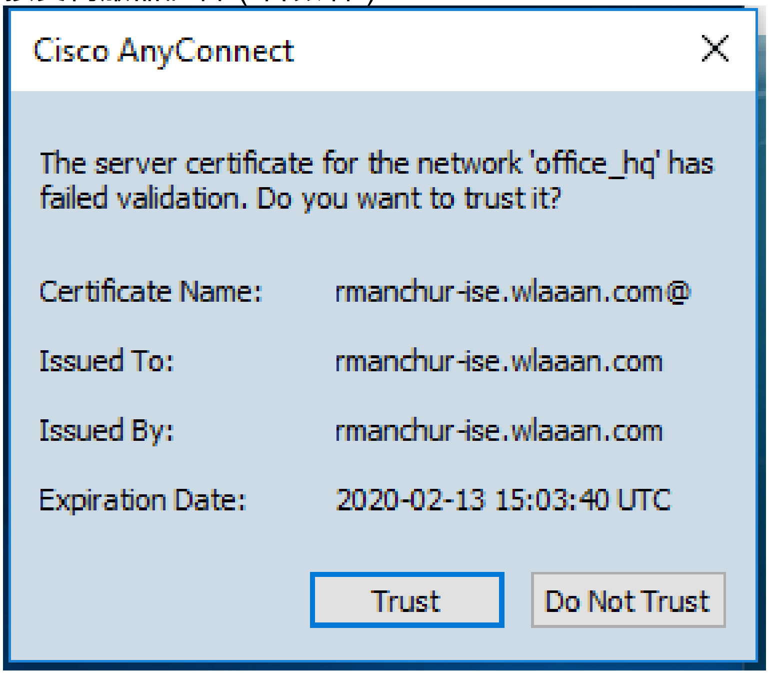
[redacted]

[redacted]

[redacted]

[redacted]

2. 輸入身份驗證所需的使用者名稱和密碼
3. 接受伺服器證書（自簽名）



Cisco AnyConnect

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

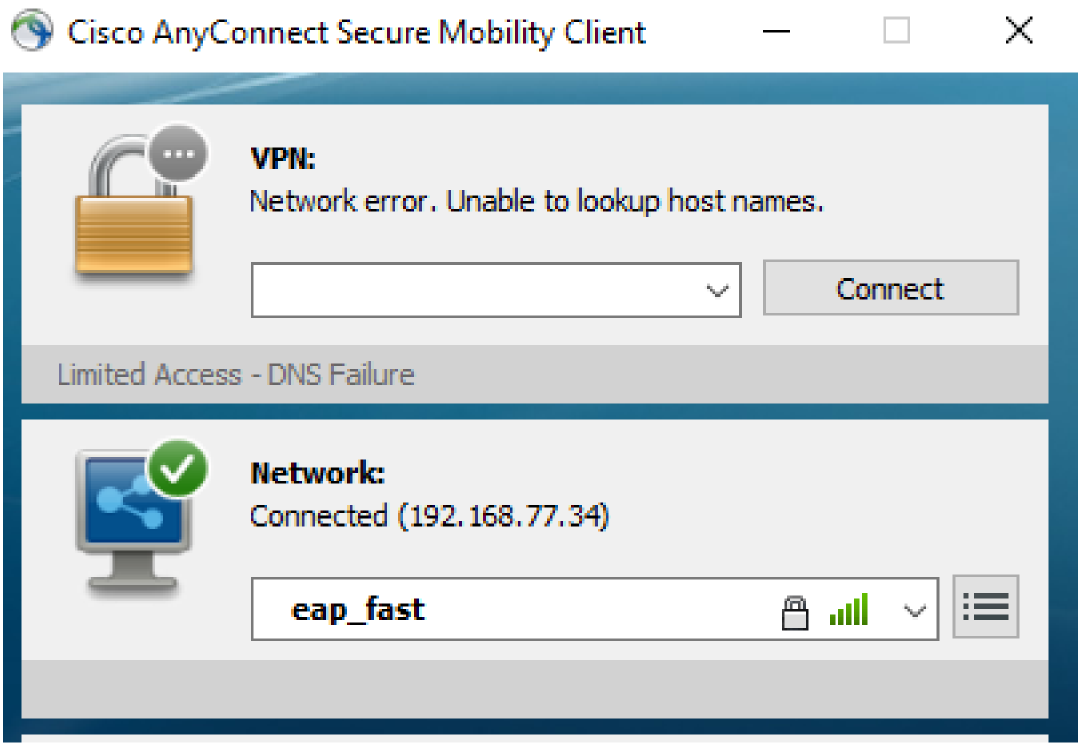
Certificate Name: rmanchur-ise.wlaaan.com@

Issued To: rmanchur-ise.wlaaan.com

Issued By: rmanchur-ise.wlaaan.com

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

4. 完成



Cisco AnyConnect Secure Mobility Client

VPN:
Network error. Unable to lookup host names.

Limited Access - DNS Failure

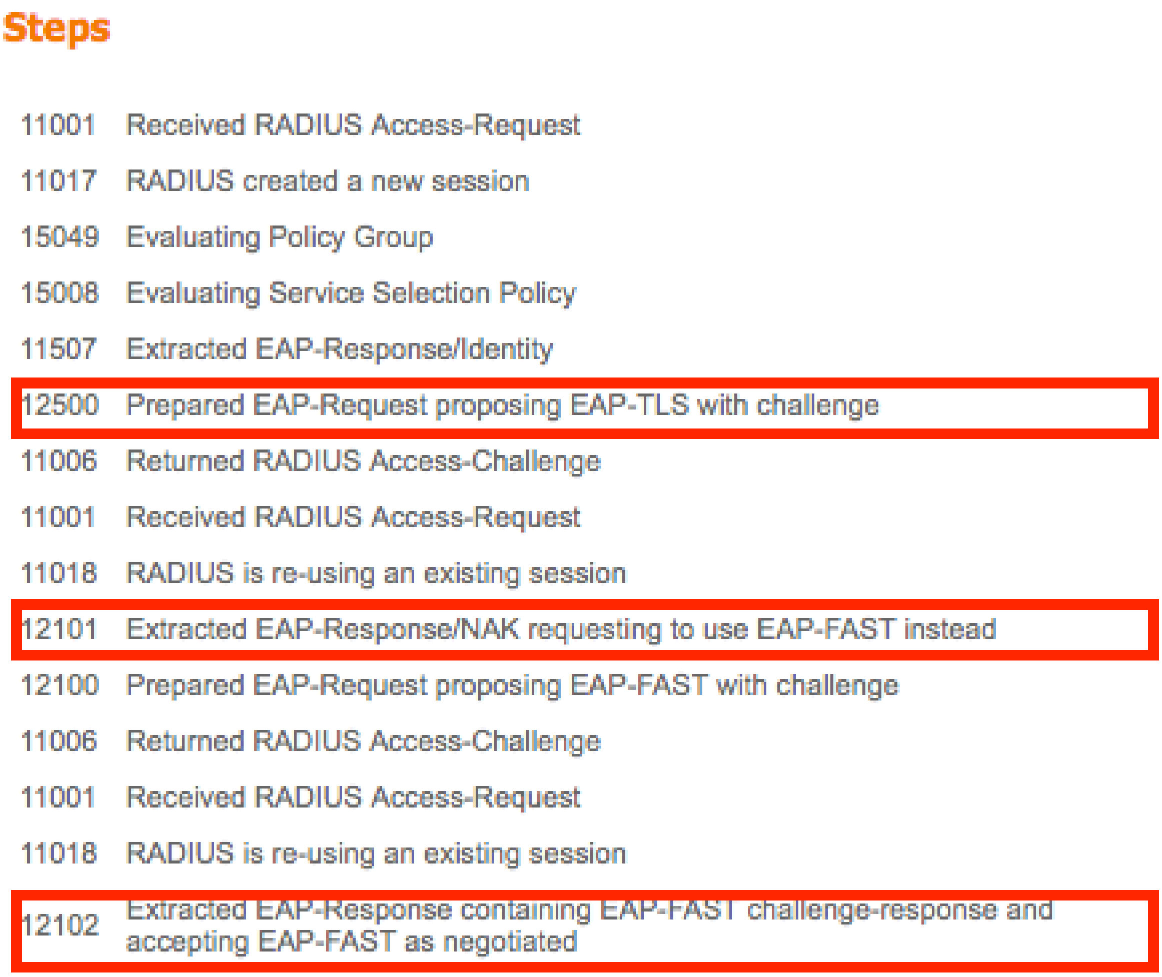
Network:
Connected (192.168.77.34)

eap_fast

ISE身份驗證日誌

顯示EAP-FAST和PAC調配流的ISE身份驗證日誌可在「**Operations -> RADIUS -> Live Logs**」下檢視，並可使用「**Zoom」圖示檢視更多詳**細資訊：

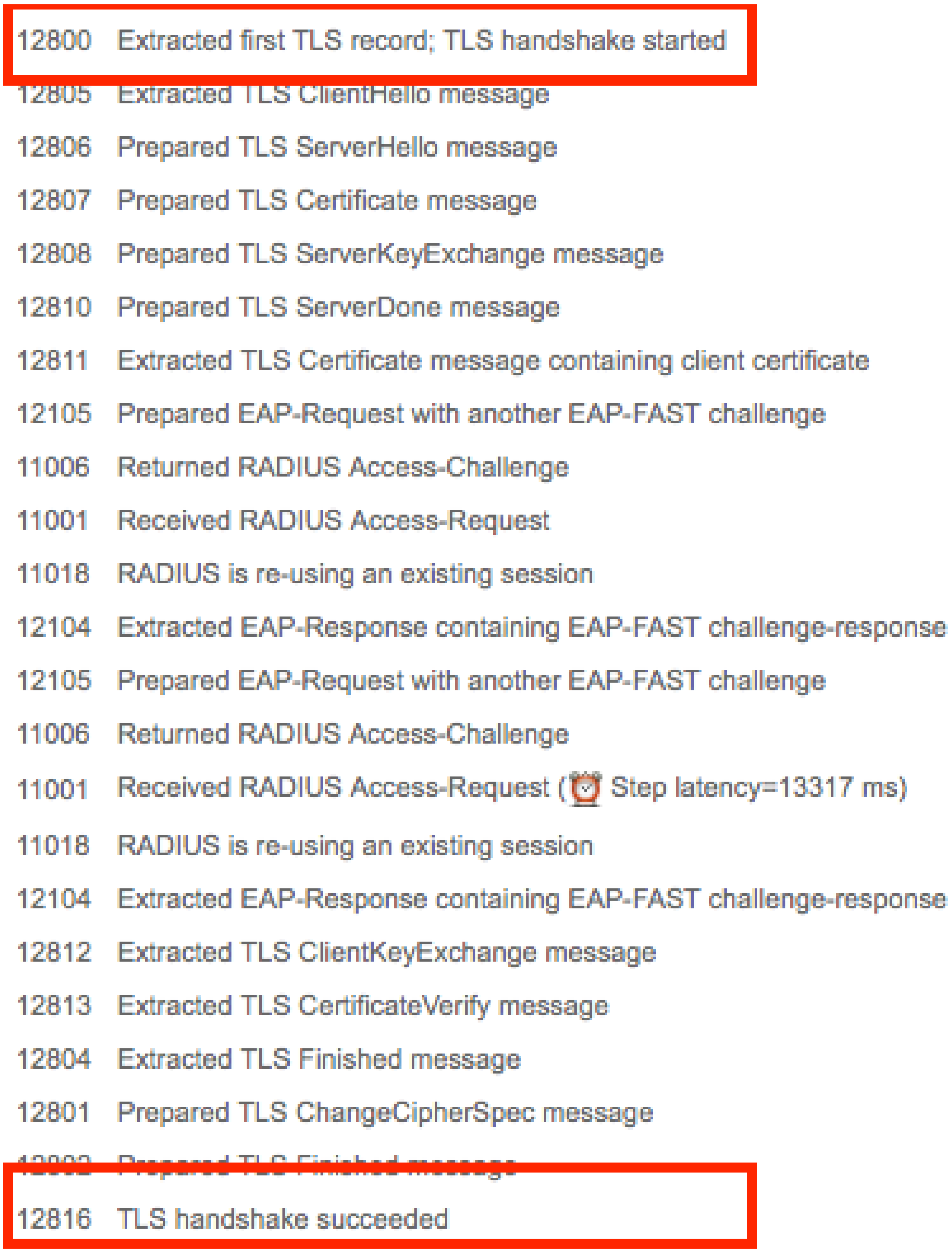
1. 客戶端已啟動身份驗證，而ISE提議將EAP-TLS作為身份驗證方法，但客戶端拒絕並提議了EAP-FAST，這是客戶端和ISE同意的方法。



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. 客戶端與伺服器之間開始了TLS握手，為PAC交換提供了受保護的環境，並成功完成。



```
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. 內部身份驗證已啟動，使用者憑據已使用MS-CHAPv2（基於使用者名稱/密碼的身份驗證）由ISE成功驗證