瞭解和配置9800 WLC上的TLS AAA快取

目錄

簡介

本文說明如何瞭解和設定Cisco Catalyst 9800無線LAN控制器(WLC)上的AAA快取。

必要條件

需求

思科建議您瞭解以下主題：

- AAA驗證概念，包括RADIUS和EAP協定
- 無線區域網路控制器(WLC)作業和組態工作流程
- 802.1X身份驗證方法和證書管理
- 基本公開金鑰基礎架構(PKI)和憑證簽署程式

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Catalyst 9800系列無線LAN控制器
- 軟體版本17.18.1或更高版本（此版本支援AAA快取功能）
- 作為AAA/RADIUS伺服器的思科身分識別服務引擎(ISE)
- 支援802.1X、EAP-TLS、EAP-PEAP、MAB和iPSK的網路訪問裝置

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

身份驗證方法（如802.1X）取決於與外部身份驗證伺服器（如RADIUS伺服器）的通訊。 當無線LAN控制器(WLC)無法連線到伺服器或伺服器不可用時，無線使用者端無法連線到SSID，導致服務中斷。WLC會封鎖使用者端流量，直到驗證成功。

從版本17.18.1開始，AAA快取功能允許Catalyst 9800 WLC驗證無線客戶端，即使AAA伺服器通過使用快取的身份驗證條目變得不可用。這顯著減少了AAA伺服器停機期間的服務中斷，並保持了無縫的客戶端連線。

當接入點以本地模式或FlexConnect（中央身份驗證）模式運行時，支援AAA快取機制。

Cisco Catalyst 9800 WLC上的AAA快取功能：

- 初始身份驗證（當可訪問AAA伺服器時）：WLC使用RADIUS將使用者端驗證要求轉送到已設定的AAA伺服器。伺服器傳回Access-Accept後，WLC會將使用者端驗證詳細資訊儲存在其AAA快取中。
- 客戶端重新連線（無法訪問AAA伺服器時）：如果使用者端在其快取專案到期前重新連線，WLC會諮詢其本地AAA快取。如果存在有效的快取資料，則在不聯絡AAA伺服器的情況下授予網路訪問許可權。
- 故障轉移支援：如果AAA伺服器由於網路問題或失敗而無法連線，WLC會繼續使用快取資料驗證使用者端，確保先前驗證的使用者保持不間斷存取。
- 快取生存期和到期時間：AAA快取中的條目是臨時的，可以配置。預設快取持續時間為24小時；將計時器設定為0可使條目永不過期。如果使用者端在其快取專案過期後重新連線，WLC會嘗試連線至AAA伺服器進行驗證。

```
VK-WLC#show aaa cache group VK-SRV-GRP all
----------------------------------------------------------------------
 IOSD AAA Auth Cache entries:

 Entries in Profile dB VK-SRV-GRP for exact match:
No entries found in Profile dB
----------------------------------------------------------------------

  SMD AAA Auth Cache Entries:

 Total number of Cache entries is 0

 WNCD AAA Auth Cache entries:

MAC ADDR:                          C4E9.0A00.B1B0
Profile Name:                      VK-CACHE
User Name:                         vk@wireless.com
Timeout:                           28800
Created Timestamp :                09/18/25 15:28:54 UTC
Server IP Address:                 10.106.37.159
```

支援的AAA快取身份驗證型別包括：

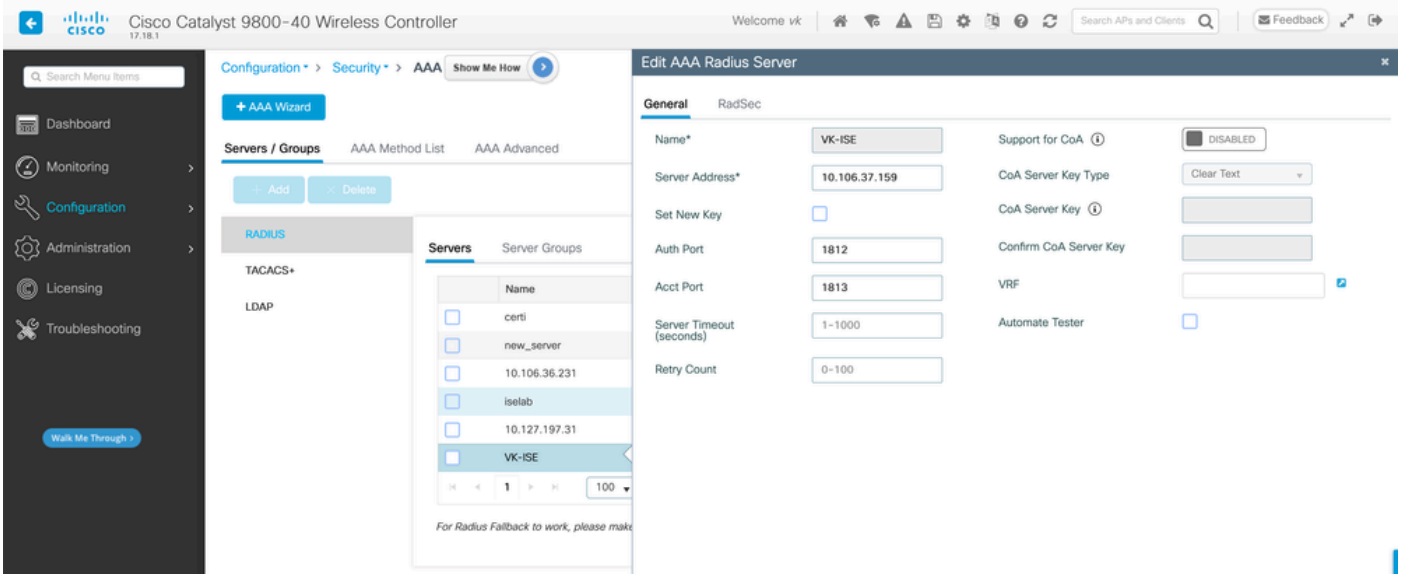
- EAP-TLS
- 採用MSCHAPv2的EAP-PEAP
- MAC Authentication Bypass(MAB)、MAB+PSK和MAB+802.1x/iPSK

設定

步驟 1:在WLC上新增AAA伺服器

首先將AAA(RADIUS)伺服器新增到無線LAN控制器。這可透過GUI或CLI完成。

GUI方法：導覽至Configuration > Security > AAA，然後新增您的伺服器。



CLI方法：

```
radius server VK-ISE
 address ipv4 10.106.37.159 auth-port 1812 acct-port 1813
 key Cisco123
```

此命令使用指定的IP地址、身份驗證埠、記帳埠和共用金鑰建立名為VK-ISE的RADIUS伺服器條目。

步驟 2:建立AAA快取配置檔案（僅限CLI）

建立AAA快取配置檔案以定義快取行為。此步驟僅適用於CLI。

```
aaa cache profile VK-CACHE all
```

此命令建立名為VK-CACHE的快取配置檔案，並啟用所有受支援的身份驗證型別的快取。

步驟 3:建立伺服器組並對映RADIUS伺服器和快取配置檔案（僅限CLI）

建立RADIUS伺服器組，關聯AAA伺服器，配置快取到期並對映授權/身份驗證配置檔案。

```
aaa group server radius VK-SRV-GRP
 server name VK-ISE
 cache expiry 8
 cache authorization profile VK-CACHE
 cache authentication profile VK-CACHE
 deadtime 5
radius-server dead-criteria time 5 tries 5
```

以下命令集：

- 建立名為VK-SRV-GRP的伺服器組
- 關聯VK-ISE服務器
- 將快取到期時間設定為8小時
- 將授權和身份驗證配置檔案映射到VK-CACHE
- 將不可達伺服器的死區時間設定為5分鐘，並將重試邏輯的死區條件設定為

步驟 4:建立身份驗證和授權方法

定義用於身份驗證和授權的方法清單，指定伺服器組和快取的使用。

```
aaa authentication dot1x default group VK-SRV-GRP cache VK-SRV-GRP
aaa authorization network default group VK-SRV-GRP cache VK-SRV-GRP
aaa local authentication default
authorization default
aaa authorization credential-download default cache VK-SRV-GRP
```

這些命令為802.1X身份驗證和網路授權設定預設方法清單，確定快取和伺服器組的優先順序。

如果您希望WLC在嘗試RADIUS伺服器之前先檢查快取（若要在使用者已快取的情況下進行更快的驗證），請使用：

```
aaa authentication dot1x default cache VK-SRV-GRP group VK-SRV-GRP
aaa authorization network default cache VK-SRV-GRP group VK-SRV-GRP
```

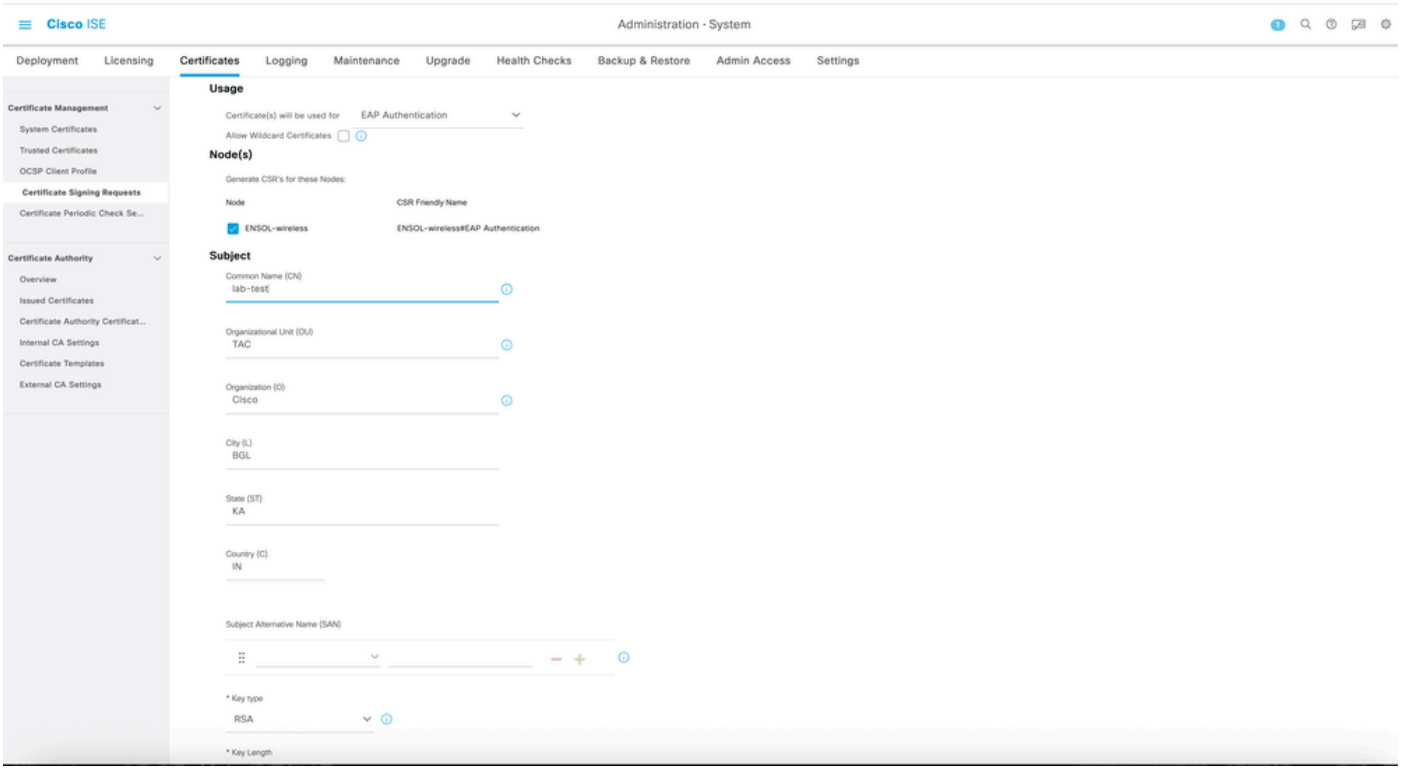
通過這些方法清單，WLC會首先查詢快取，只有在快取中找不到使用者時才會聯絡伺服器，從而加快對快取客戶端的身份驗證。

步驟 5:配置TLS身份驗證（證書設定）

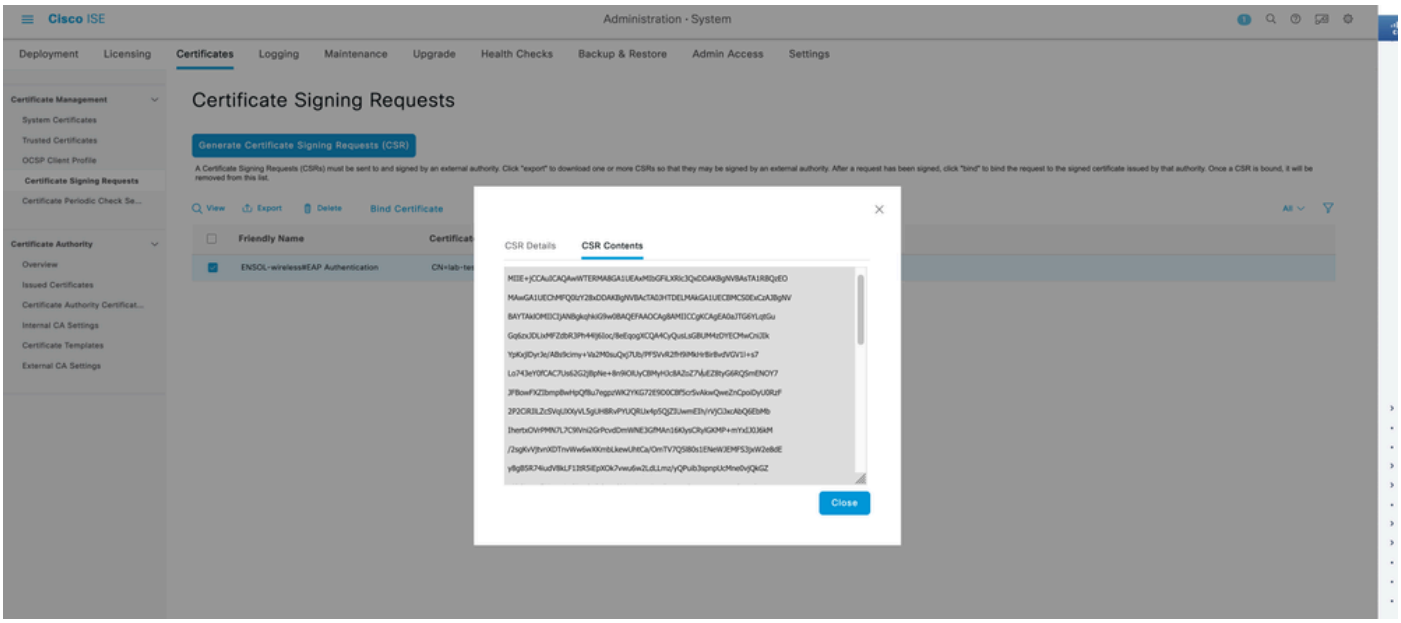
對於EAP-TLS身份驗證，WLC和AAA伺服器都需要由證書頒發機構(CA)簽名的伺服器證書。

在Cisco ISE（AAA伺服器）上：

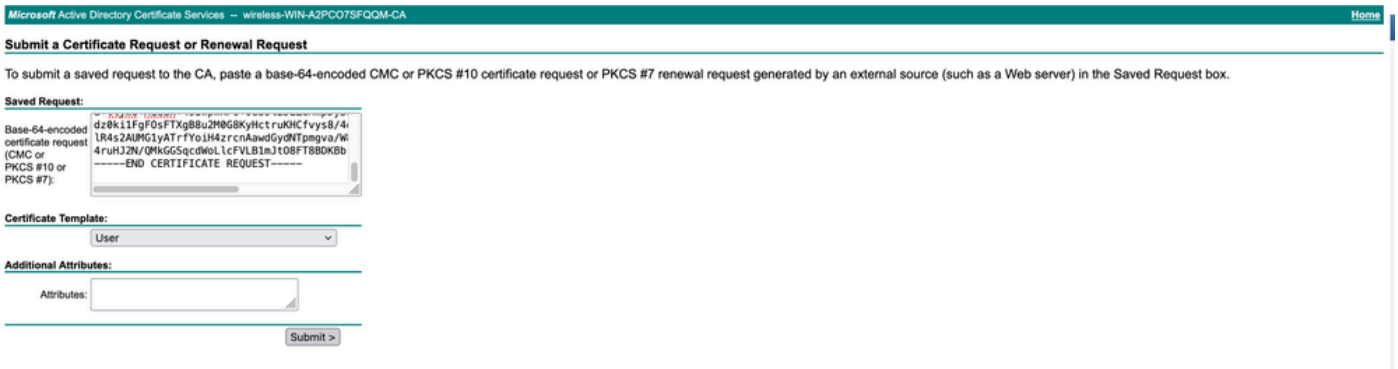
- 通過證書>證書管理>證書簽名請求生成證書簽名請求(CSR)



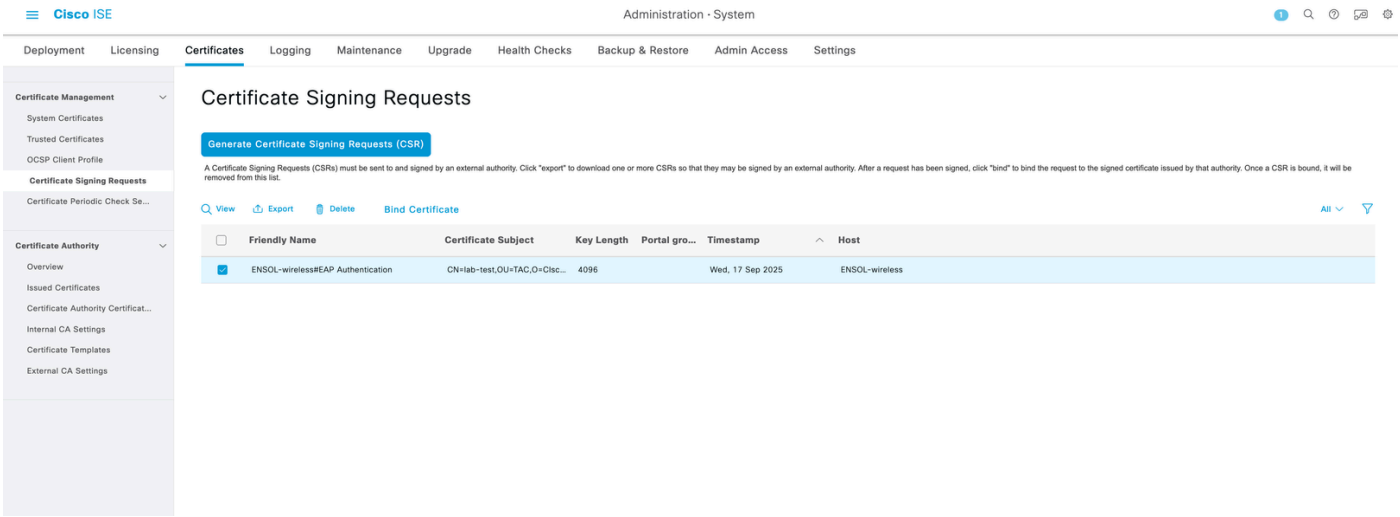
- 複製CSR內容並由您的CA簽署

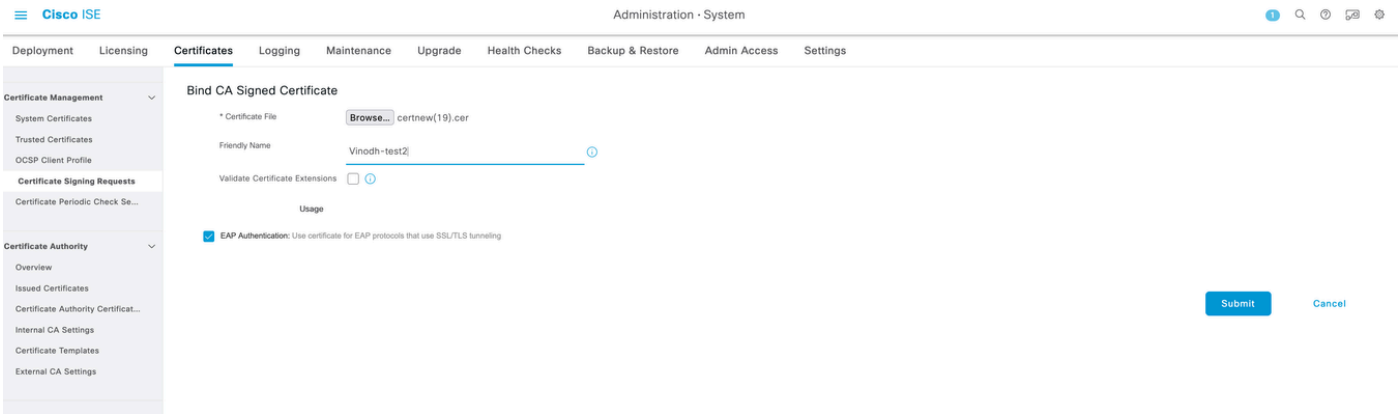


- 下載簽名的證書(.cer或.pem格式)

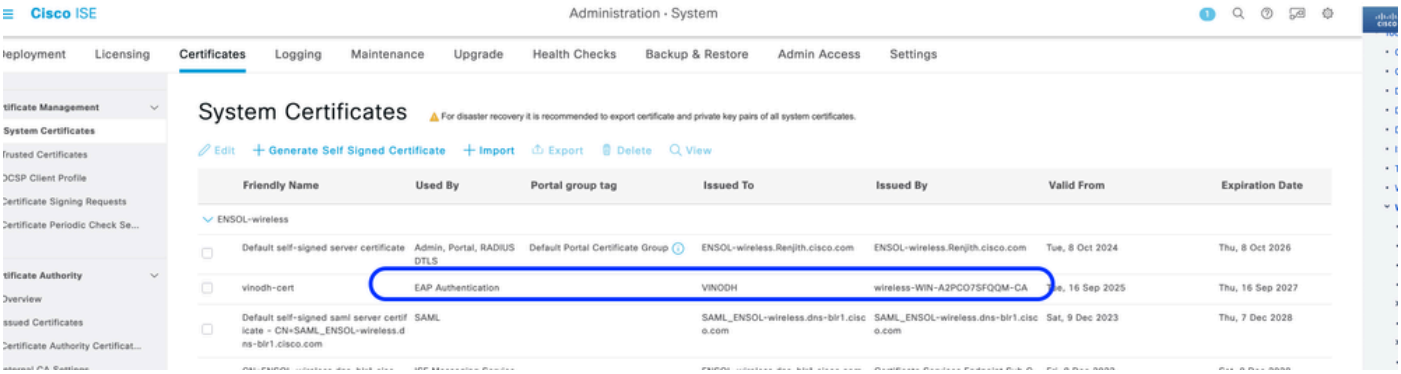


- 通過瀏覽到簽名證書檔案並按一下「提交」在ISE上繫結證書



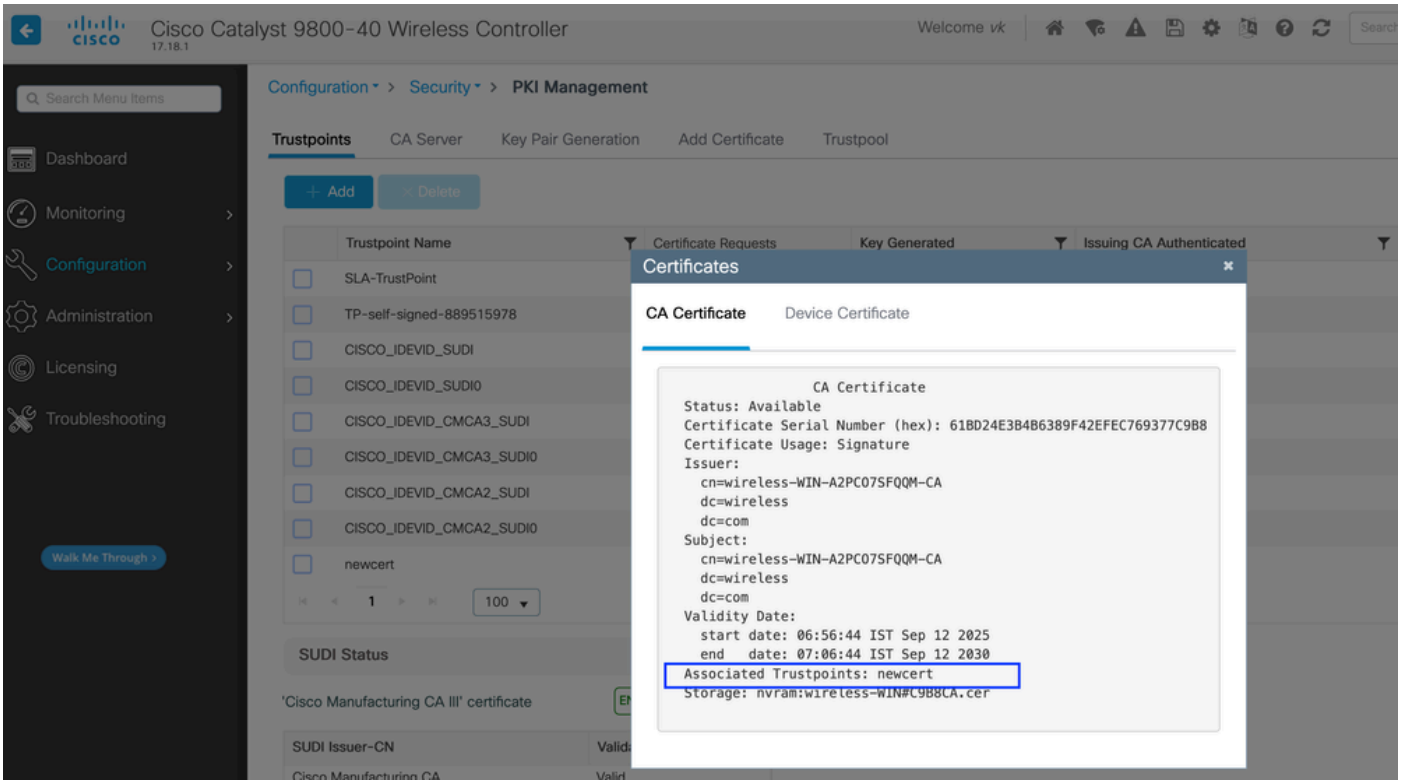


- 確保已簽名的證書反映在EAP身份驗證的系統證書下



在Cisco Catalyst 9800 WLC上：

- 在WLC上產生CSR
- 獲取由用於ISE的同一CA簽名的CSR
- 將簽名的憑證上傳到WLC



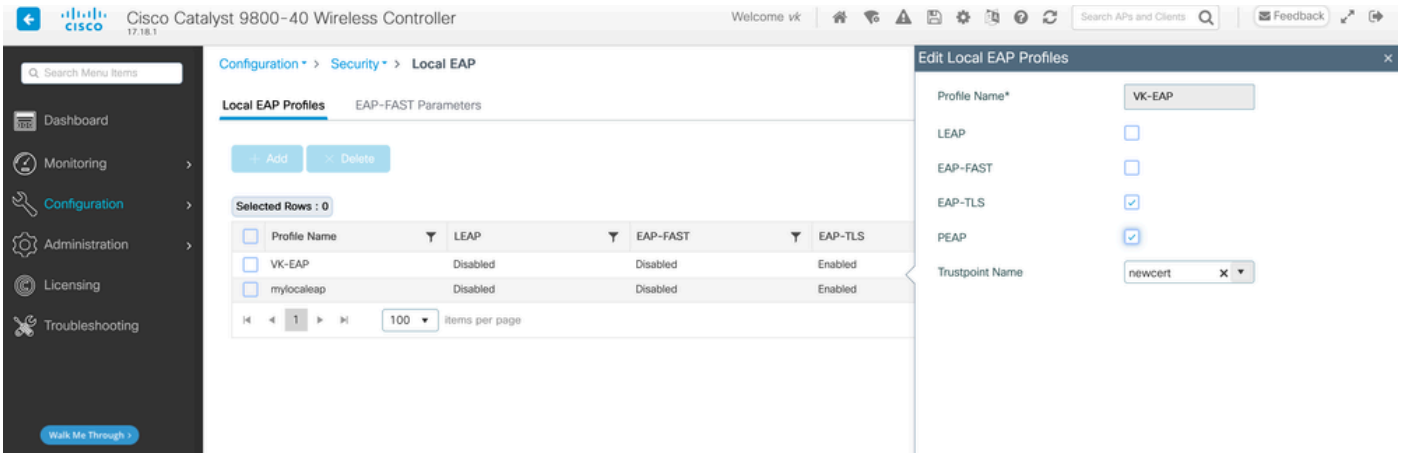
步驟 6:建立本地EAP配置檔案和對映信任點

建立本地EAP配置檔案並對映用於EAP-TLS身份驗證的信任點。

```
eap profile VK-EAP
 method tls
 pki-trustpoint newcert
```

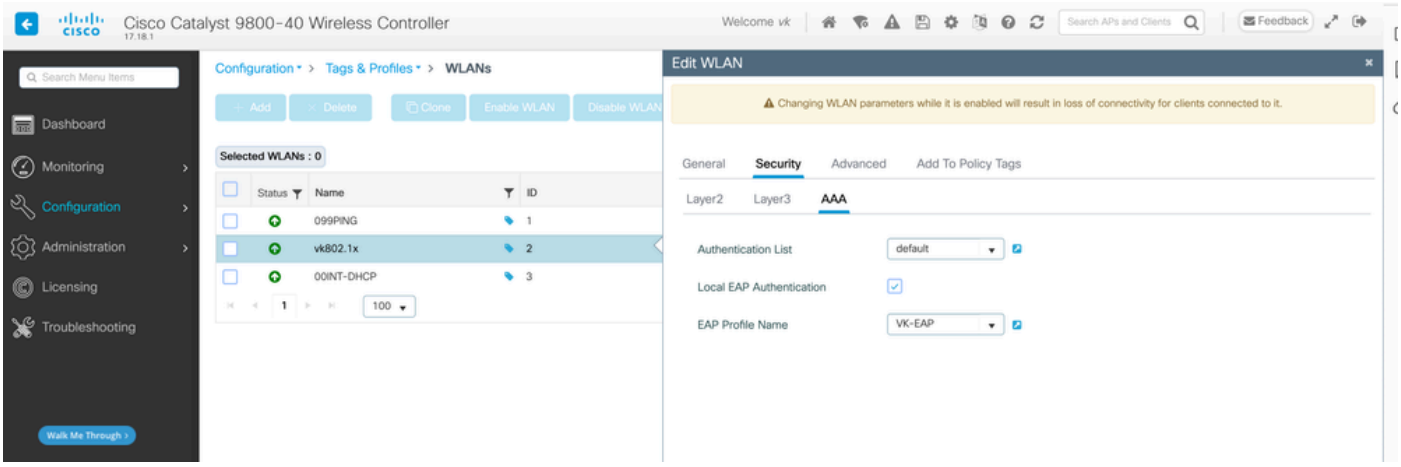
此命令使用EAP-TLS建立名為VK-EAP的EAP配置檔案，並將信任點對映到名為newcert的證書。

GUI方法：導航到Configuration > Security > Local EAP，然後建立EAP配置檔案。



步驟 7:將方法清單和EAP配置檔案應用到SSID

將您的SSID配置為使用建立的身份驗證和EAP配置檔案。




```
wlan vk802.1x 2 vk802.1x
 local-auth VK-EAP
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 security dot1x authentication-list default
```

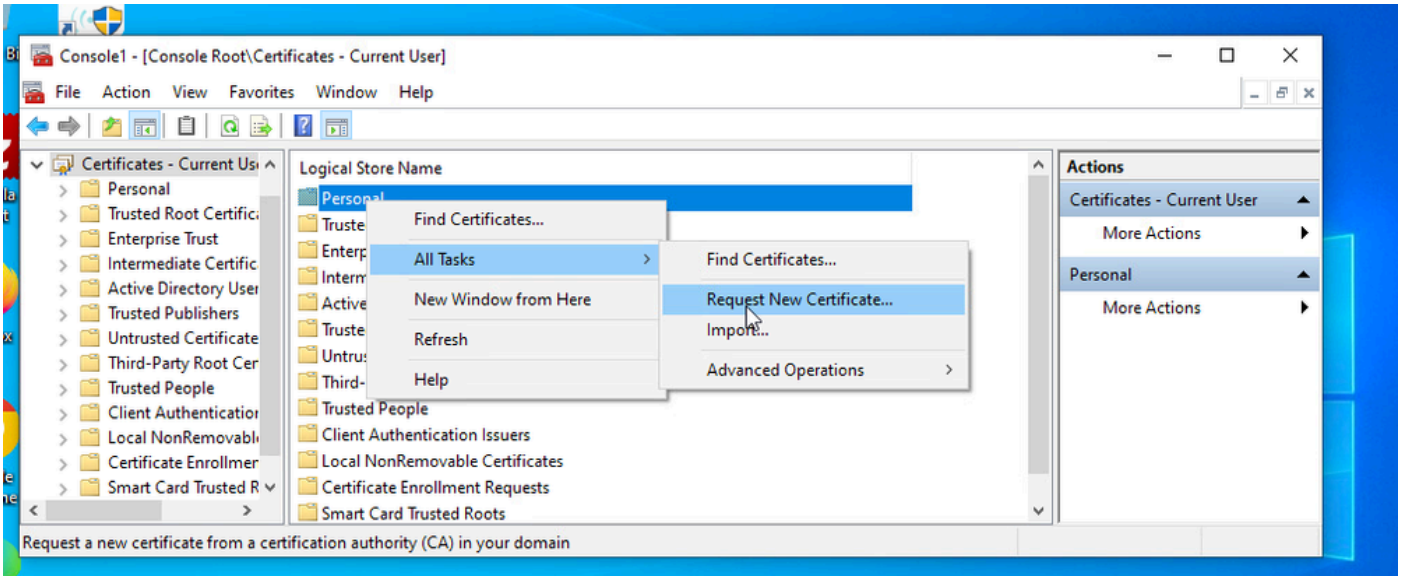
```
no shutdown
```

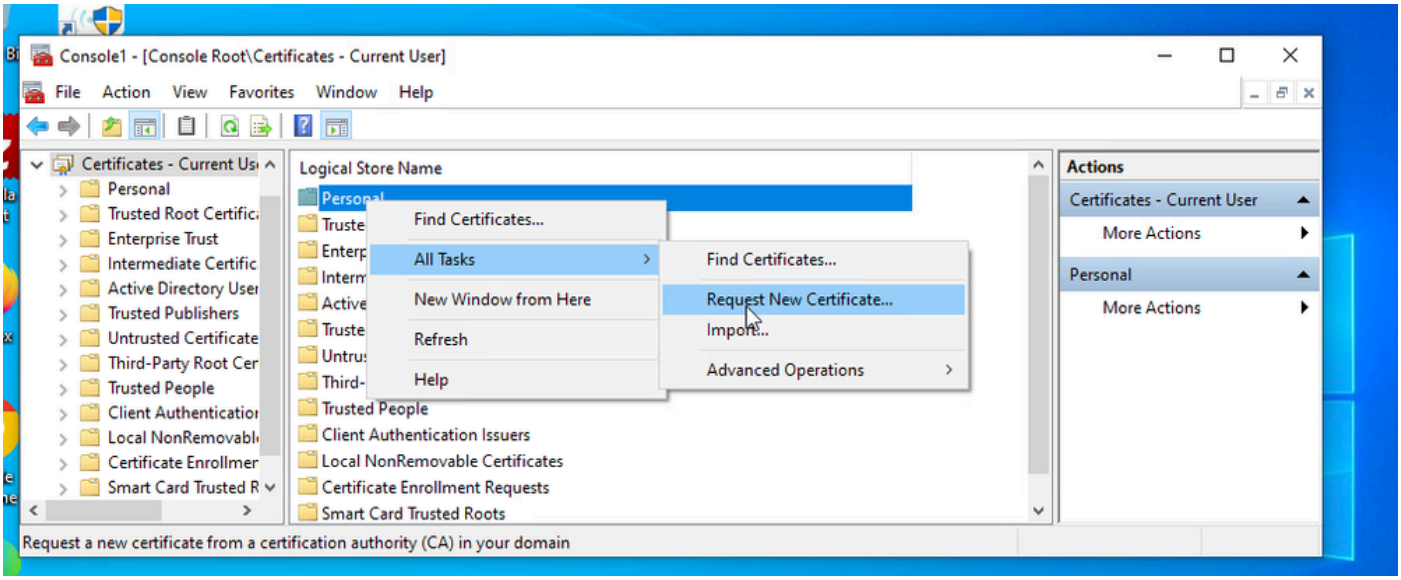
此配置：

- 建立帶WLAN ID 2的SSID vk802.1x
- 使用VK-EAP配置檔案啟用本地身份驗證
- 對2.4GHz和5GHz頻段應用無線電策略
- 使用預設方法清單實施802.1X身份驗證
- 啟動SSID（無關閉）

步驟 8:無線客戶端上的使用者證書部署

確保無線客戶端具有進行身份驗證所需的使用者證書。對於實驗室環境，加入Active Directory(AD)域的裝置可以通過MMC（Microsoft管理控制檯）接收證書。 根據您的環境，還有其他一些分發證書的方法。





驗證

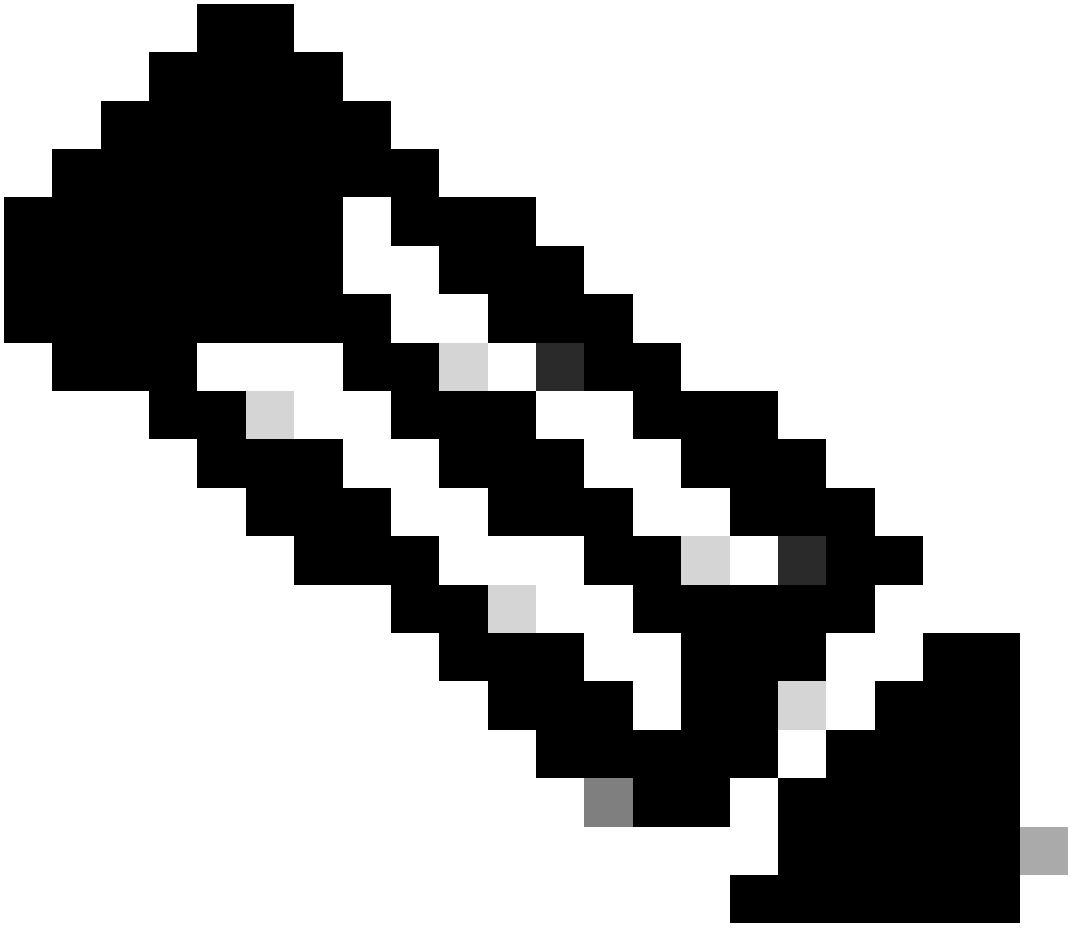
您可以使用CLI指令檢查9800 WLC上的AAA快取專案。請注意，對於Catalyst 9800 WLC，快取專案列在「WNCD AAA Auth Cache entries」下，而不是「SMD AAA Auth Cache entries」下。

```
show aaa cache group <Server Group> all
```

此命令顯示WLC上儲存的當前AAA快取條目。輸出示例：

```
WNCD AAA Auth Cache entries
---------------------------
Client MAC: 00:11:22:33:44:55
SSID: vk802.1x
User: user@domain.com
Cache Expiry: 8h
Auth Method: EAP-TLS
...
```

驗證當AAA伺服器不可用時，客戶端是否可以重新連線並通過AAA快取進行身份驗證。



附註：對於PEAP身份驗證，當前設計要求返回Cisco AV對，其中包含由Radius伺服器進行身份驗證期間每個使用者的使用者名稱和憑據雜湊。

cisco-av-pair = AS-Username=testuser

cisco-av-pair = AS-Credential-Hash=F2E787D376CBF6D6DD3600132E9C215D

每個使用者都必須在RADIUS上設定AV配對屬性。

Password或AS-Credential-Hash必須採用NT雜湊格式(https://codebeautify.org/ntlm-hash-generator)。

疑難排解

排除AAA快取和身份驗證問題涉及幾個步驟：

步驟 1:檢查AAA快取條目

```
show aaa cache group <Server Group> all
```

確保快取中存在預期的客戶端條目。

步驟 2:驗證證書安裝和信任點

```
show crypto pki trustpoints
show crypto pki certificates
```

確保正確安裝證書並將其對映到EAP-TLS身份驗證的正確信任點。

步驟 3:確認身份驗證方法清單

```
show running-config | include aaa authentication
show running-config | include aaa authorization
```

驗證該方法清單是否引用了正確的伺服器組和快取配置檔案。

步驟 5:檢查RA內部跟蹤

<#root>

```
2025/09/18 13:02:37.069850424 {wncd_x_R0-0}{2}: [radius] [16292]: (ERR): RADIUS/DECODE: No response fro
2025/09/18 13:02:37.069850966 {wncd_x_R0-0}{2}: [radius] [16292]: (ERR): RADIUS/DECODE: Case error(no r
2025/09/18 13:02:37.069853220 {wncd_x_R0-0}{2}: [aaa-sg-ref] [16292]: (debug): AAA/SG: Server group wra
2025/09/18 13:02:37.069853836 {wncd_x_R0-0}{2}: [aaa-sg-ref] [16292]: (debug): AAA/SG: Server group ref
2025/09/18 13:02:37.069855784 {wncd_x_R0-0}{2}: [aaa-sg-cache] [16292]: (debug): AAA/AUTHEN/CACHE: Don'
2025/09/18 13:02:37.069856826 {wncd_x_R0-0}{2}: [aaa-svr] [16292]: (debug): AAA SRV(00000000): protocol
2025/09/18 13:02:37.069860954 {wncd_x_R0-0}{2}: [aaa-authen] [16292]: (debug): MAC address in AAA reque

2025/09/18 13:02:37.069864992 {wncd_x_R0-0}{2}: [aaa-svr] [16292]: (debug): AAA SRV(00000000): Authen me


2025/09/18 13:02:37.069868198 {wncd_x_R0-0}{2}: [ewlc-infra-evmgr] [16292]: (debug): Add message event
2025/09/18 13:02:37.069875634 {wncd_x_R0-0}{2}: [ewlc-infra-evmgr] [16292]: (debug): Evmgr message even
2025/09/18 13:02:37.069876688 {wncd_x_R0-0}{2}: [wncd_0] [16292]: (debug): Sanet eventQ: AAA_CACHE_EVEN

2025/09/18 13:02:37.069887794 {wncd_x_R0-0}{2}: [aaa-prof] [16292]: (debug): AAA/PROFILE/DB: Find - Four
2025/09/18 13:02:37.069955264 {wncd_x_R0-0}{2}: [aaa-sg-cache] [16292]: (debug): AAA/AUTHEN/CACHE(00000

this indiates that cache/local auth is being used


2025/09/18 13:02:37.070019998 {wncd_x_R0-0}{2}: [wncd_0] [16292]: (debug): AAA Local EAP(1419) Sending
2025/09/18 13:02:37.070022944 {wncd_x_R0-0}{2}: [ewlc-infra-evmgr] [16292]: (debug): Add message event
```

```
2025/09/18 13:02:37.070025886 {wncd_x_R0-0}{2}: [aaa-sg-cache] [16292]: (debug): AAA/AUTHEN/CACHE(000000
2025/09/18 13:02:37.070028162 {wncd_x_R0-0}{2}: [ewlc-infra-evmgr] [16292]: (debug): Evmgr message even
```

參考資料:

[17.18軟體配置指南]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。