了解并配置9800 WLC上的AAA缓存，以使用TLS

目录

简介

本文档介绍如何了解和配置Cisco Catalyst 9800无线LAN控制器(WLC)上的AAA缓存。

先决条件

要求

Cisco 建议您了解以下主题：

- AAA身份验证概念，包括RADIUS和EAP协议
- 无线局域网控制器(WLC)操作和配置工作流程
- 802.1X身份验证方法和证书管理
- 基本公钥基础设施(PKI)和证书签名流程

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Catalyst 9800系列无线LAN控制器
- 软件版本17.18.1或更高版本（此版本支持AAA缓存功能）
- 作为AAA/RADIUS服务器的思科身份服务引擎(ISE)
- 支持802.1X、EAP-TLS、EAP-PEAP、MAB和iPSK的网络访问设备

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

身份验证方法（如802.1X）依赖于与外部身份验证服务器（如RADIUS服务器）的通信。 当无线局域网控制器(WLC)无法访问服务器或服务器不可用时，无线客户端无法连接到SSID，导致服务中断。WLC会阻止客户端流量，直到身份验证成功。

从版本17.18.1开始，AAA缓存功能允许Catalyst 9800 WLC对无线客户端进行身份验证，即使AAA服务器因使用缓存的身份验证条目而变得不可用。这显着减少了AAA服务器中断期间的服务中断，并保持了无缝的客户端连接。

当接入点在本地模式或FlexConnect（中央身份验证）模式下运行时，支持AAA缓存机制。

Cisco Catalyst 9800 WLC上的AAA缓存功能：

- 初始身份验证（当可访问AAA服务器时）：WLC使用RADIUS将客户端身份验证请求转发到已配置的AAA服务器。一旦服务器返回Access-Accept，WLC会将客户端身份验证详细信息本地存储在其AAA缓存中。
- 客户端重新连接（当AAA服务器不可达时）：如果客户端在其缓存的条目到期之前重新连接，则WLC会查询其本地AAA缓存。如果存在有效的缓存数据，则在不联系AAA服务器的情况下授予网络访问权限。
- 故障切换支持：如果AAA服务器由于网络问题或故障而无法访问，WLC将继续使用缓存数据对客户端进行身份验证，确保之前经过身份验证的用户保持不间断访问。
- 缓存生存期和到期：AAA缓存中的条目是临时的且可配置。默认缓存持续时间为24小时；将计时器设置为0可使条目永不过期。如果客户端在其缓存条目过期后重新连接，则WLC尝试访问AAA服务器进行身份验证。

```
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
```

AAA缓存支持的身份验证类型包括：

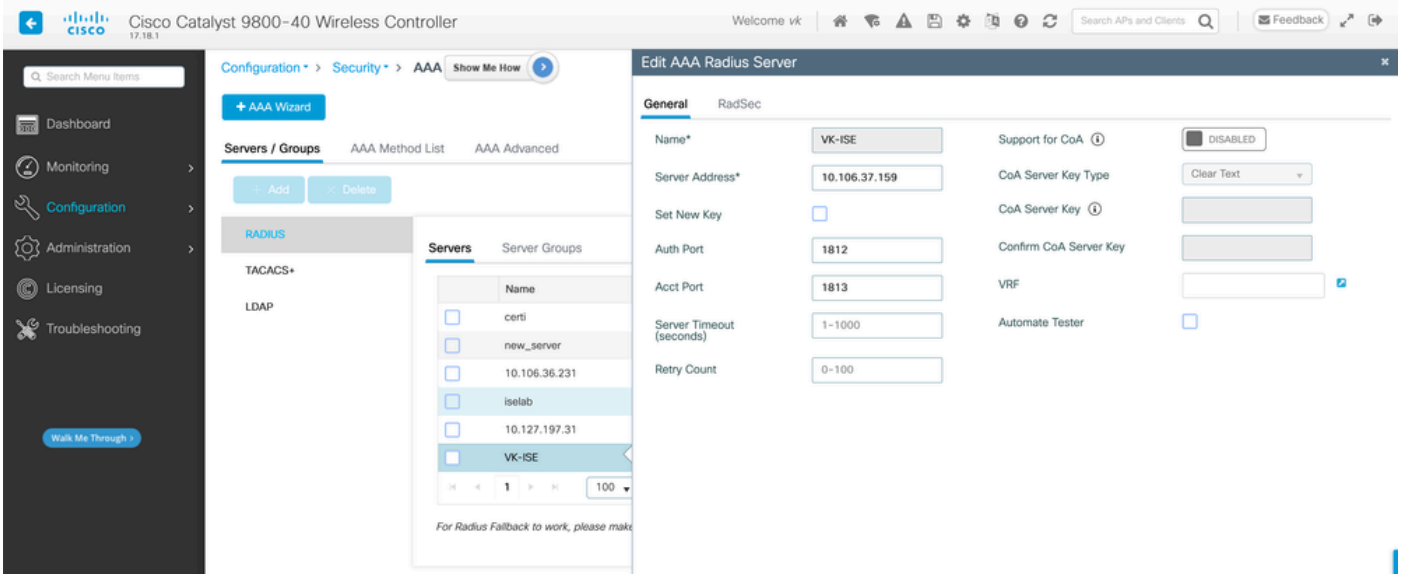
- EAP-TLS
- 采用MSCHAPv2的EAP-PEAP
- MAC身份验证绕行(MAB)、MAB+PSK和MAB+802.1x/iPSK

配置

步骤 1：在WLC上添加AAA服务器

首先将您的AAA(RADIUS)服务器添加到无线LAN控制器。这可以通过GUI或CLI完成。

GUI方法：导航到Configuration > Security > AAA并添加服务器。



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、身份验证端口、记帐端口和共享密钥创建名为VK-ISE的RADIUS服务器条目。

步骤 2：创建AAA缓存配置文件（仅限CLI）

创建AAA缓存配置文件以定义缓存行为。此步骤仅适用于CLI。

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

此命令创建名为VK-CACHE的缓存配置文件，并启用所有受支持的身份验证类型的缓存。

步骤 3：创建服务器组并映射RADIUS服务器和缓存配置文件（仅限CLI）

创建RADIUS服务器组，关联AAA服务器，配置缓存到期和映射授权/身份验证配置文件。

```
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
```

这组命令：

- 创建名为VK-SRV-GRP的服务器组
- 关联VK-ISE服务器
- 将缓存到期时间设置为8小时
- 将授权和身份验证配置文件映射到VK-CACHE
- 将不可达服务器的死区时间设置为5分钟，并将重试逻辑的死区条件设置为

步骤 4：创建身份验证和授权方法

定义身份验证和授权的方法列表，指定服务器组和缓存的使用。

```
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
```

这些命令为802.1X身份验证和网络授权设置默认方法列表，确定缓存和服务器组的优先级。

如果希望WLC在尝试RADIUS服务器之前首先检查缓存（如果用户已缓存，则用于更快的身份验证），请使用：

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

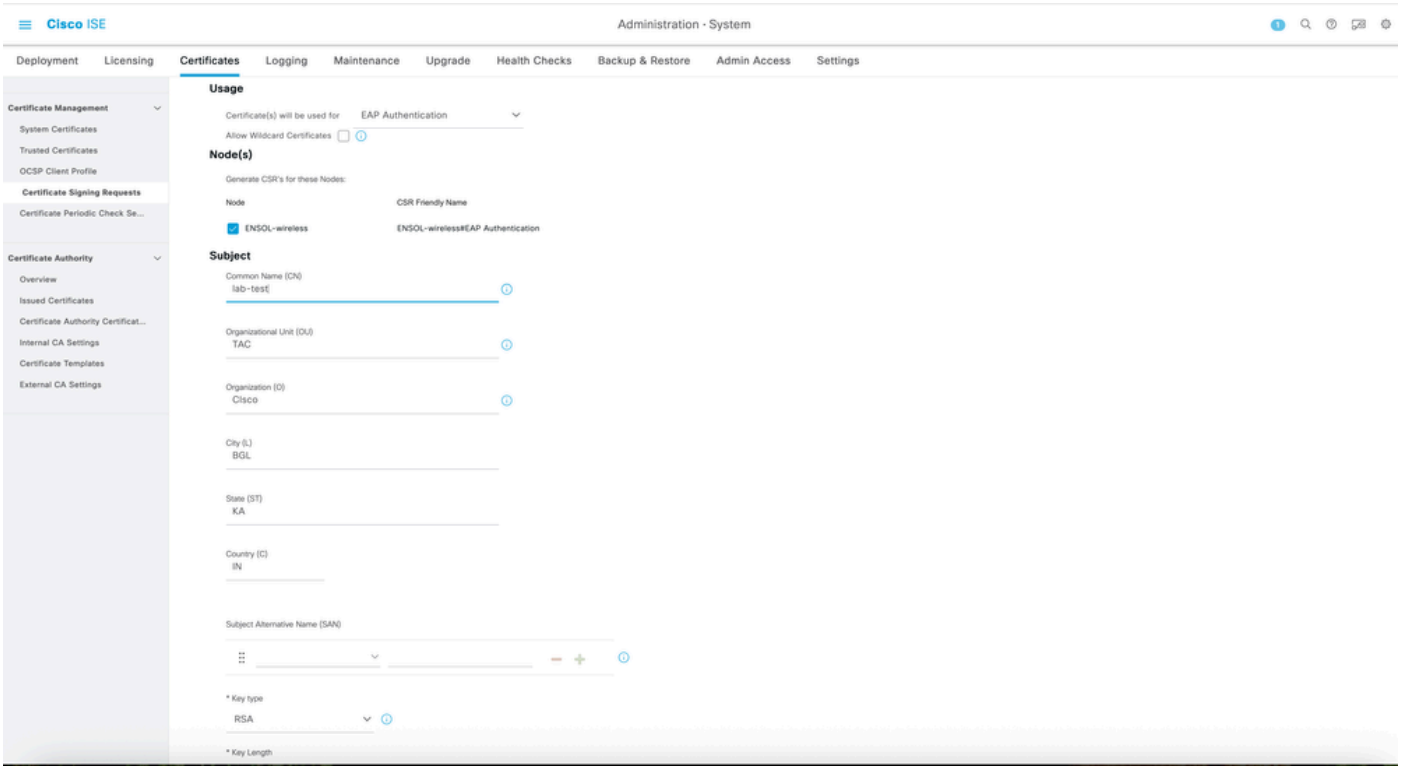
使用这些方法列表，WLC首先会查询缓存，只有在缓存中找不到用户时才会联系服务器，从而加快缓存客户端的身份验证。

步骤 5：配置TLS身份验证（证书设置）

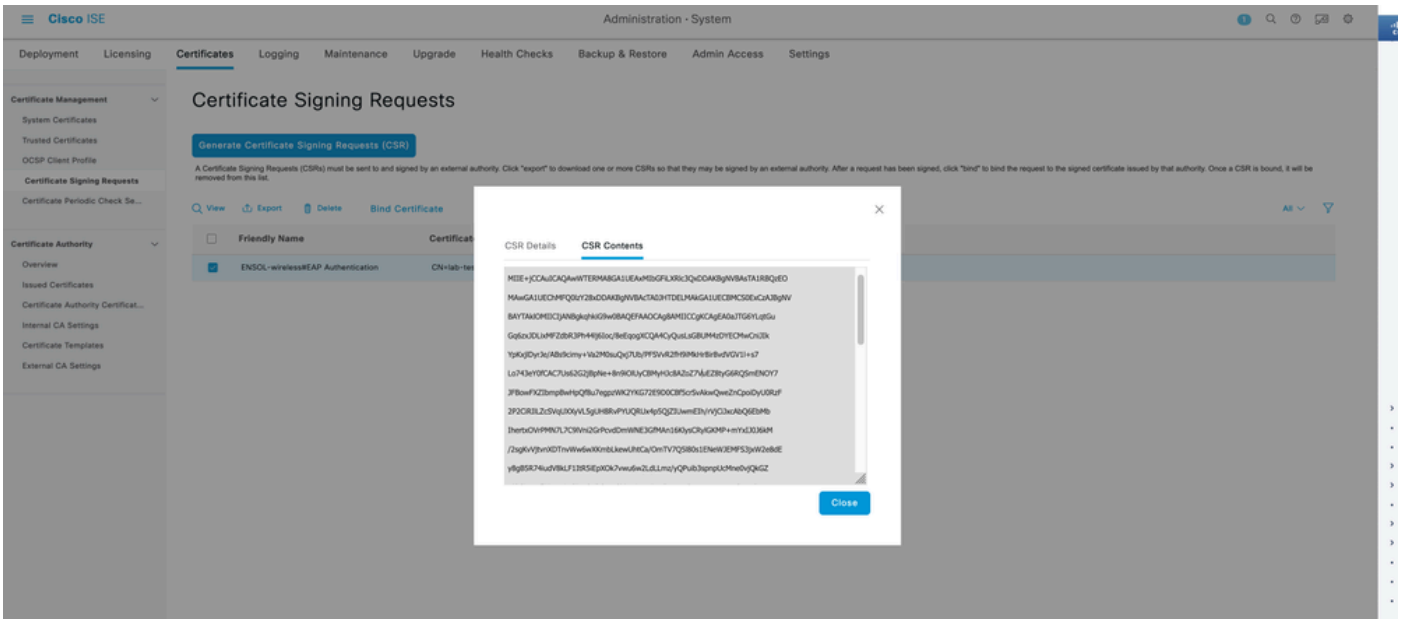
对于EAP-TLS身份验证，WLC和AAA服务器都需要由证书颁发机构(CA)签名的服务器证书。

在Cisco ISE（AAA服务器）上：

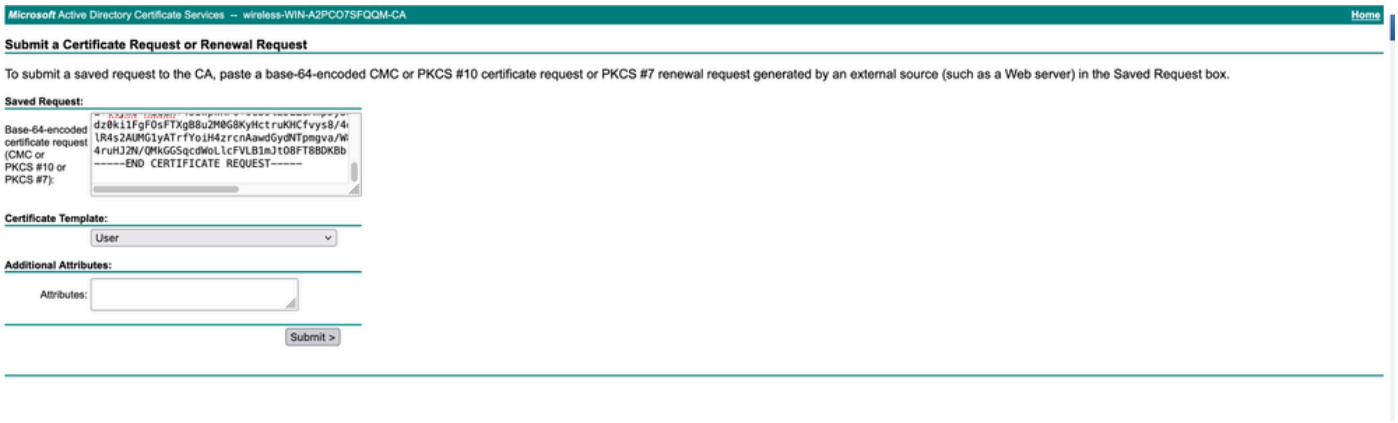
- 通过证书>证书管理>证书签名请求生成证书签名请求(CSR)



- 复制CSR内容，并由您的CA进行签名

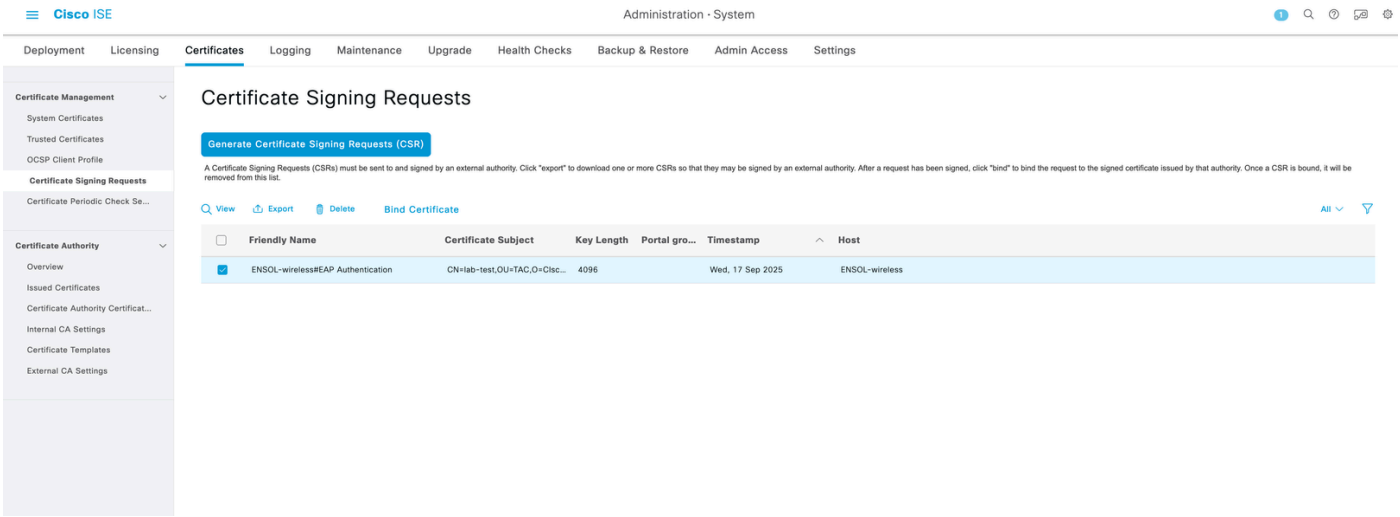


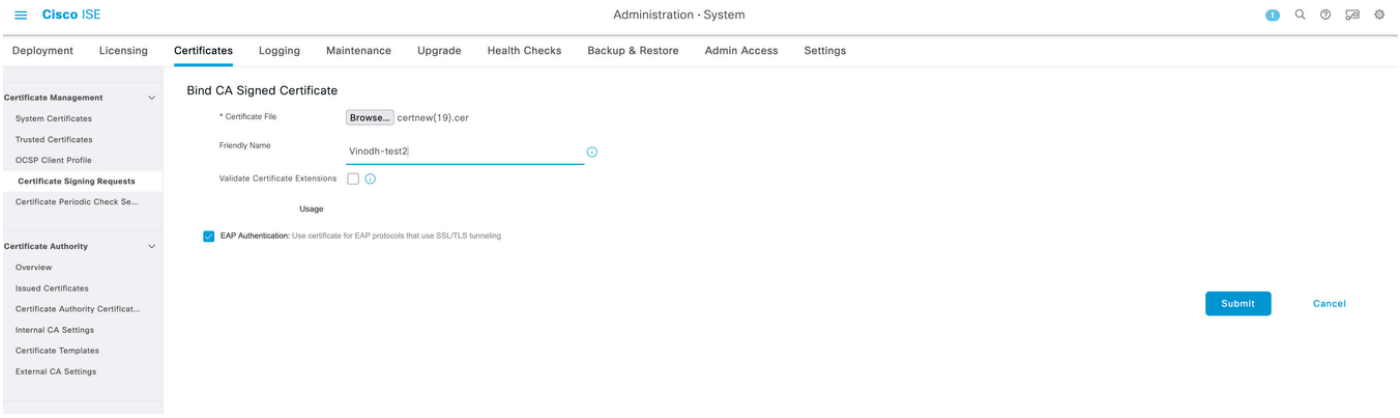
- 下载签名证书(.cer或.pem格式)



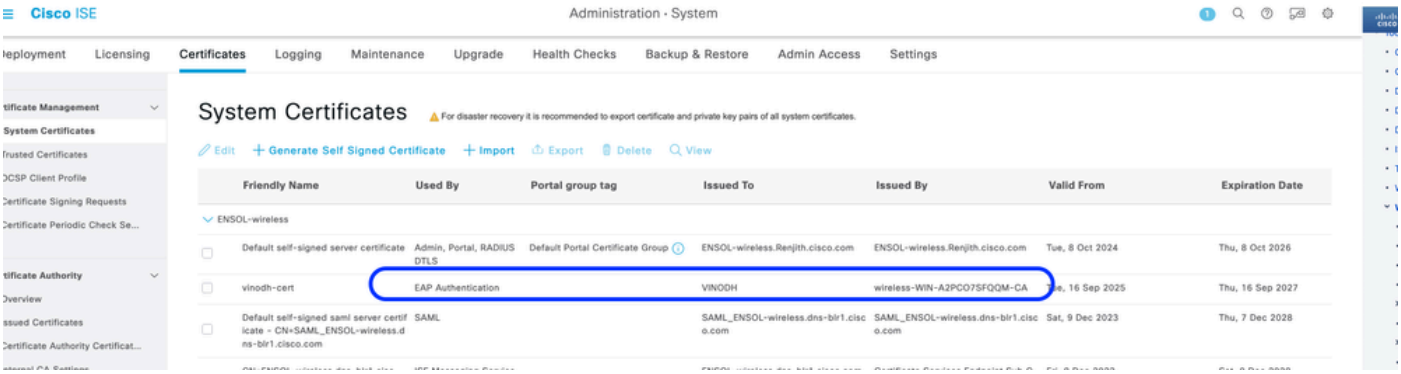


- 通过浏览到签名证书文件并点击“提交”在ISE上绑定证书



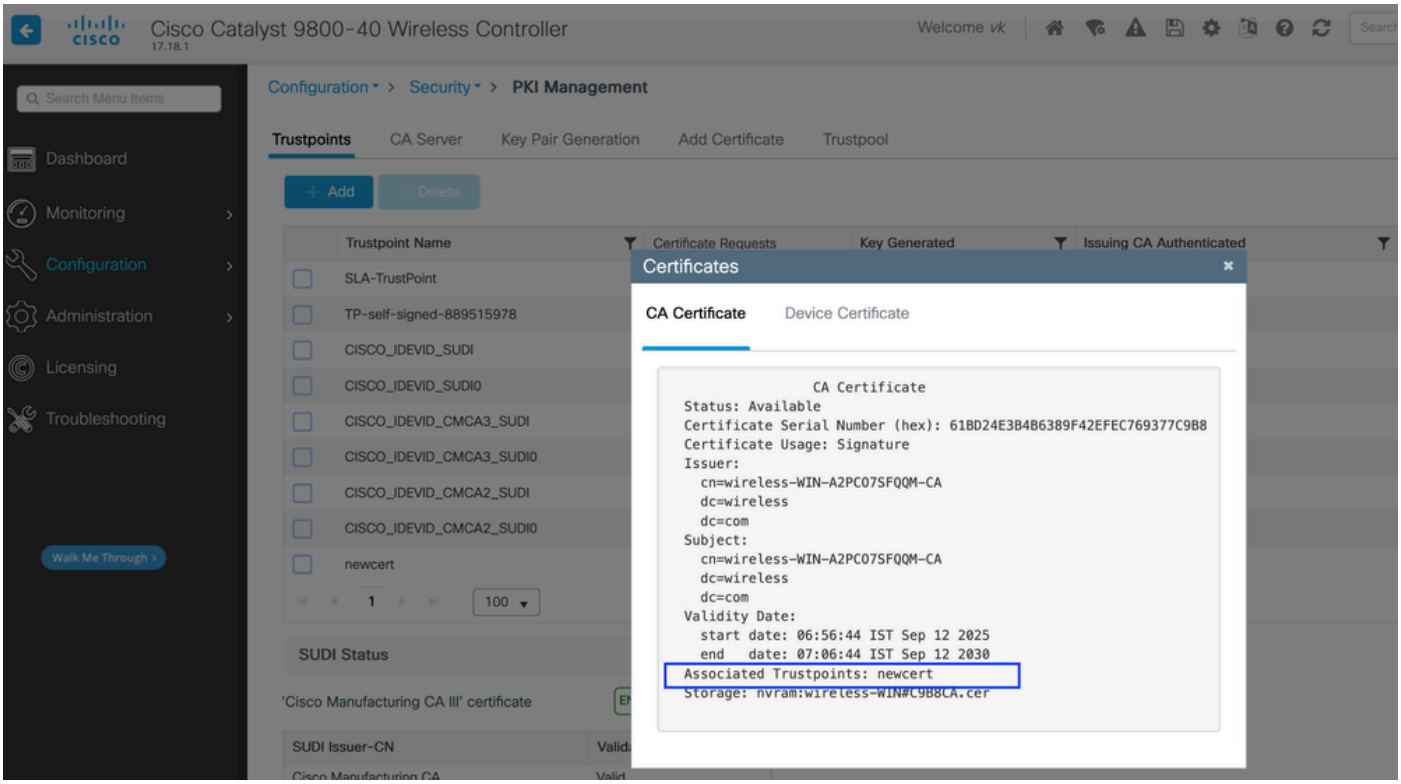


- 确保签名证书反映在EAP身份验证的系统证书下



在Cisco Catalyst 9800 WLC上：

- 在WLC上生成CSR
- 获取由用于ISE的同一CA签名的CSR
- 将签名证书上传到WLC



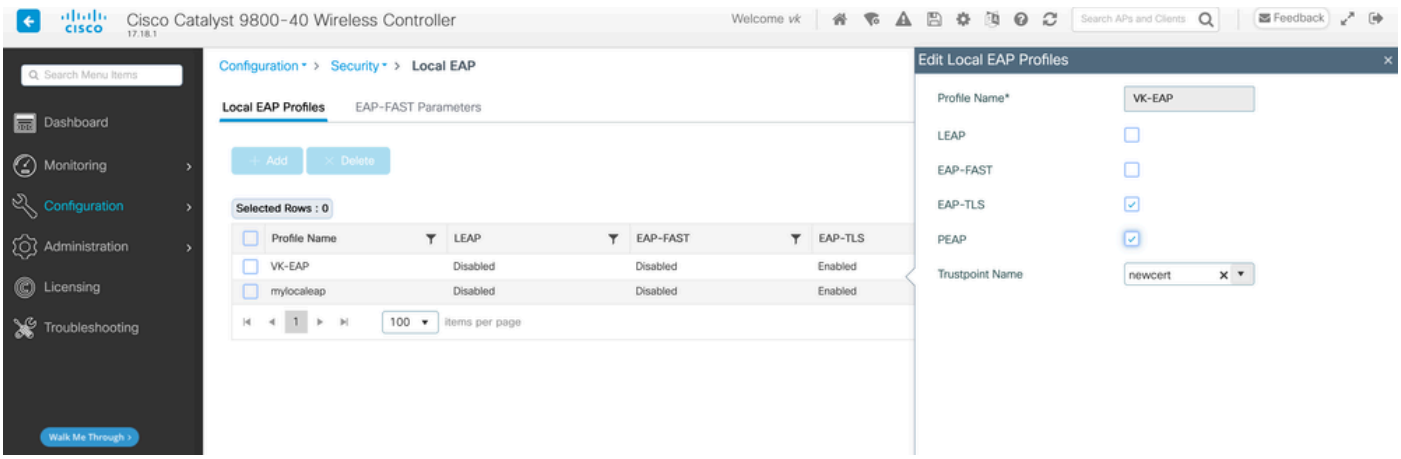
步骤 6：创建本地EAP配置文件和映射信任点

创建本地EAP配置文件并映射用于EAP-TLS身份验证的信任点。

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

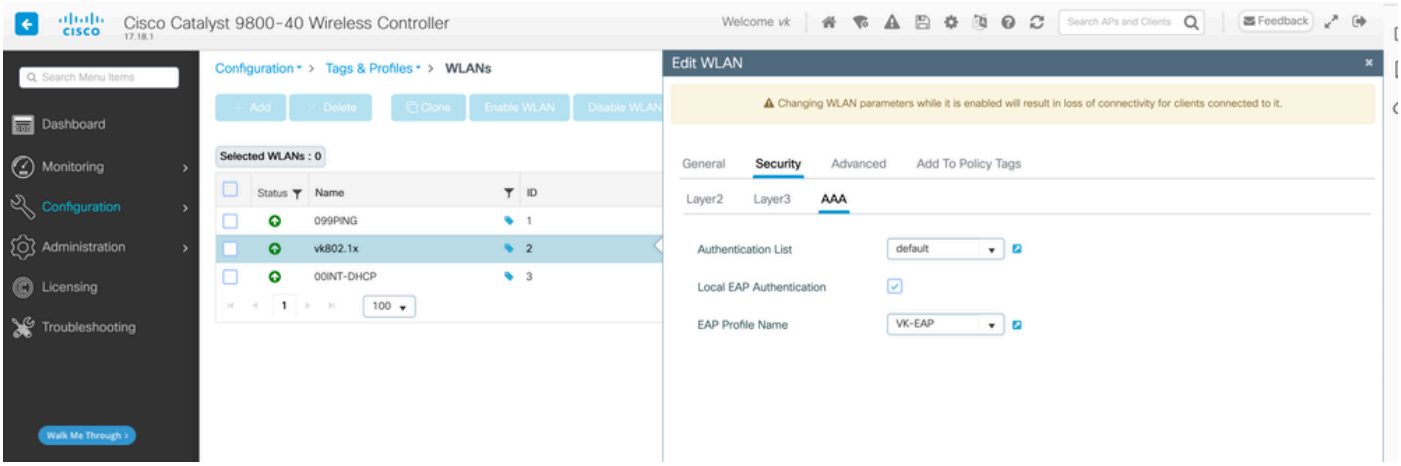
此命令使用EAP-TLS创建名为VK-EAP的EAP配置文件，并将信任点映射到名为newcert的证书。

GUI方法：导航到Configuration > Security > Local EAP并创建EAP配置文件。



步骤 7：将方法列表和EAP配置文件应用于SSID

配置您的SSID以使用创建的身份验证和EAP配置文件。




```
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
```

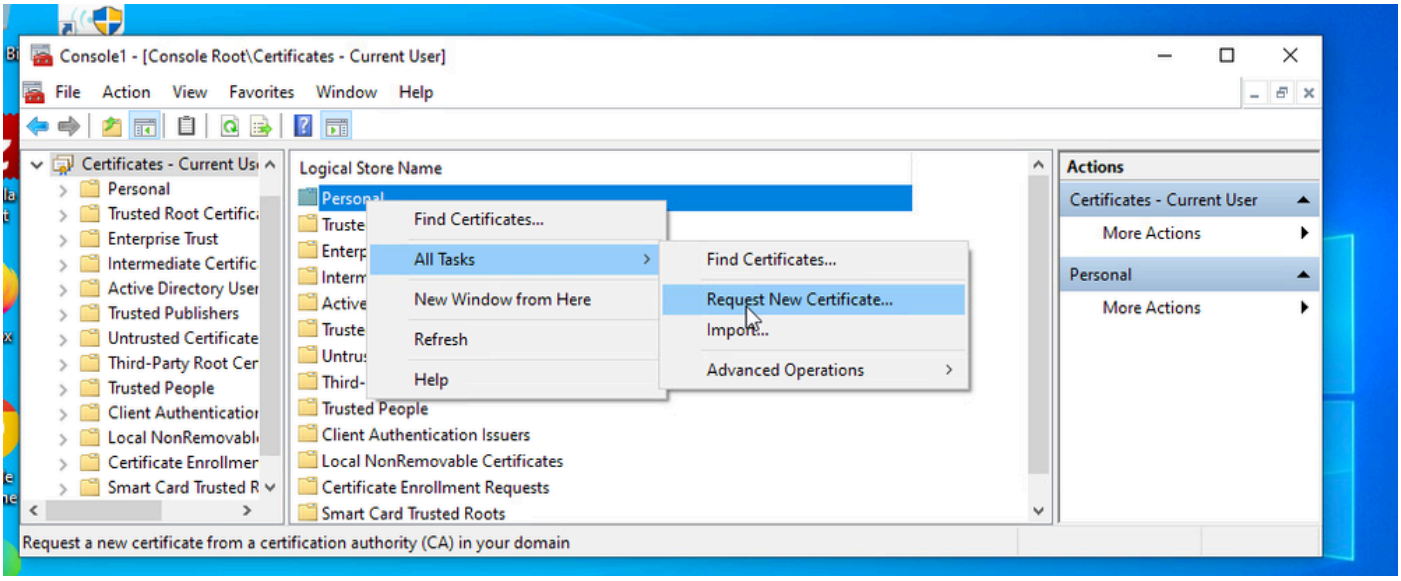
```
no shutdown
```

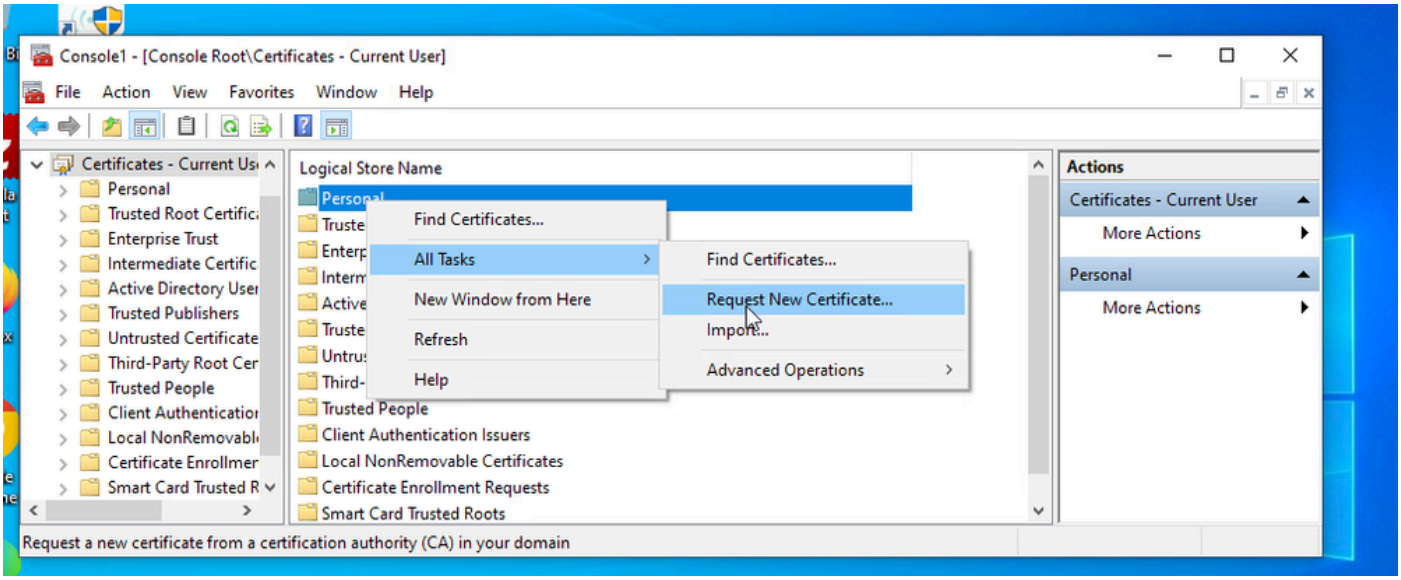
此配置：

- 创建SSID vk802.1x,WLAN ID为2
- 使用VK-EAP配置文件启用本地身份验证
- 为2.4GHz和5GHz频段应用无线电策略
- 使用默认方法列表实施802.1X身份验证
- 启动SSID(no shutdown)

步骤 8::无线客户端上的用户证书部署

确保无线客户端具有身份验证所需的用户证书。对于实验室环境，加入Active Directory(AD)域的设备可以通过MMC（Microsoft管理控制台）接收证书。 根据您的环境，还有其他方法可以分发证书。





验证

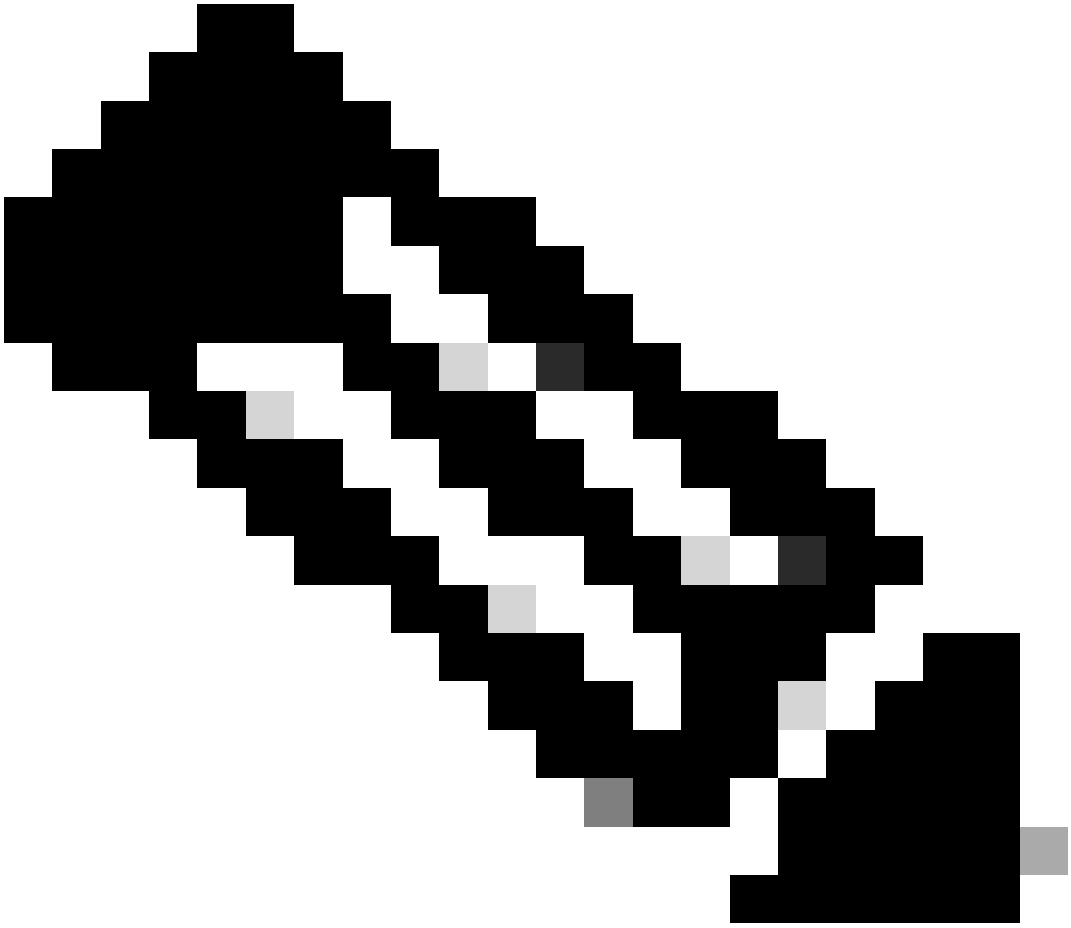
您可以使用CLI命令检查9800 WLC上的AAA缓存条目。请注意，对于Catalyst 9800 WLC，缓存条目列在“WNCD AAA Auth Cache entries”下，而不是“SMD AAA Auth Cache entries”下。

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

此命令显示WLC上存储的当前AAA缓存条目。示例输出：

```
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
...
```

当AAA服务器不可用时，验证客户端是否可以重新连接并通过AAA缓存进行身份验证。



注意：对于PEAP身份验证，当前设计要求返回包含Radius服务器身份验证期间每个用户的用户名和凭证哈希的Cisco AV对。

cisco-av-pair = AS-Username=testuser

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

必须在RADIUS上为每个用户配置AV对属性。

Password或AS-Credential-Hash必须采用NT哈希格式(https://codebeautify.org/ntlm-hash-generator)。

故障排除

排除AAA缓存和身份验证问题涉及几个步骤：

步骤 1：检查AAA缓存条目

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

确保缓存中存在预期的客户端条目。

步骤 2：验证证书安装和信任点

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

确保正确安装证书并将其映射到EAP-TLS身份验证的正确信任点。

步骤 3：确认身份验证方法列表

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

验证该方法列表是否引用了正确的服务器组和缓存配置文件。

步骤 5：检查RA内部跟踪

<#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(00000

2025/09/18 13:02:37.070028162 {wncd_x_R0-0}{2}: [ewlc-infra-evmgr] [16292]: (debug): Evmgr message even

参考资料:

[17.18软件配置指南]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。