Understand and Configure AAA Cache for TLS on 9800 WLC

Contents

Introduction

This document describes how to understand and configure AAA cache on Cisco Catalyst 9800 Wireless LAN Controllers (WLC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- AAA authentication concepts, including RADIUS and EAP protocols
- Wireless LAN Controller (WLC) operation and configuration workflows
- 802.1X authentication methods and certificate management
- Basic Public Key Infrastructure (PKI) and certificate signing processes

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Catalyst 9800 Series Wireless LAN Controller
- Software Release 17.18.1 or later (AAA cache feature supported from this release)
- Cisco Identity Services Engine (ISE) as AAA/RADIUS server
- Network Access Devices supporting 802.1X, EAP-TLS, EAP-PEAP, MAB, and iPSK

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Authentication methods such as 802.1X depend on communication with an external authentication server (such as a RADIUS server). When the Wireless LAN Controller (WLC) cannot reach the server or when the server is unavailable, wireless clients are not able to connect to the SSID, leading to service disruptions. The WLC blocks client traffic until authentication succeeds.

Starting from release 17.18.1, the AAA cache feature allows the Catalyst 9800 WLC to authenticate wireless clients even if the AAA server becomes unavailable by using cached authentication entries. This significantly reduces service disruption during AAA server outages and maintains seamless client connectivity.

The AAA cache mechanism is supported when Access Points are operating in local mode or FlexConnect

(central authentication) mode.

AAA Cache Functionality on Cisco Catalyst 9800 WLC:

- **Initial Authentication (When AAA Server is Reachable):** The WLC forwards the client authentication request to the configured AAA server using RADIUS. Once the server returns Access-Accept, the WLC stores the client authentication details locally in its AAA cache.
- **Client Reconnection (When AAA Server Unreachable):** If a client reconnects before its cached entry expires, the WLC consults its local AAA cache. If valid cached data exists, network access is granted without contacting the AAA server.
- **Failover Support:** If the AAA server is unreachable due to network issues or failure, the WLC continues to authenticate clients using cached data, ensuring that previously authenticated users maintain uninterrupted access.
- **Cache Lifetime and Expiry:** Entries in the AAA cache are temporary and configurable. The default cache duration is 24 hours; setting the timer to 0 make entries never expire. If a client reconnects after its cache entry has expired, the WLC attempts to reach the AAA server for authentication.

```
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
```

Supported authentication types for AAA cache include:

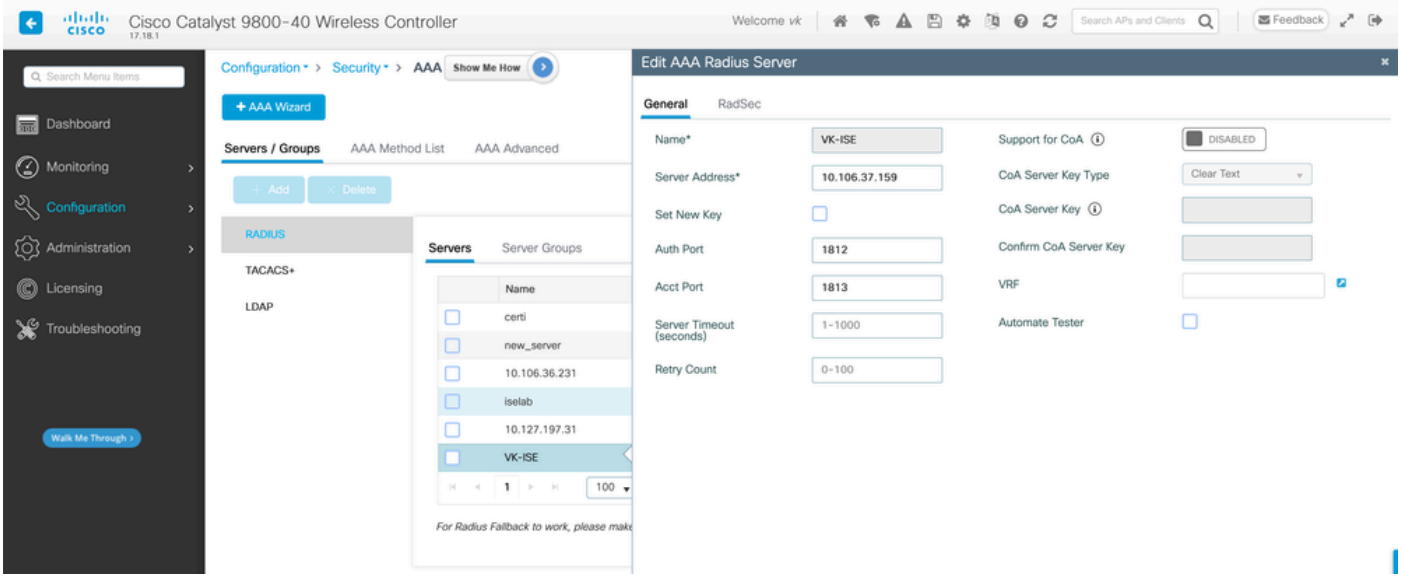
- EAP-TLS
- EAP-PEAP with MSCHAPv2
- MAC Authentication Bypass (MAB), MAB+PSK, and MAB+802.1x/iPSK

Configure

Step 1: Add AAA Server on WLC

Begin by adding your AAA (RADIUS) server to the Wireless LAN Controller. This can be done via the GUI or CLI.

GUI Method: Navigate to **Configuration > Security > AAA** and add your server.



CLI Method:

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

This command creates a RADIUS server entry named **VK-ISE** with the specified IP address, authentication port, accounting port, and shared key.

Step 2: Create AAA Cache Profile (CLI Only)

Create an AAA cache profile to define cache behavior. This step is CLI-only.

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

This command creates a cache profile named **VK-CACHE** and enables caching for all supported authentication types.

Step 3: Create Server Group and Map RADIUS Server and Cache Profile (CLI Only)

Create a RADIUS server group, associate the AAA server, configure cache expiry, and map authorization/authentication profiles.

```
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
```

This set of commands:

- Creates a server group named **VK-SRV-GRP**
- Associates the **VK-ISE** server
- Sets cache expiry to 8 hours
- Maps both authorization and authentication profiles to **VK-CACHE**
- Sets deadtime for unreachable servers to 5 minutes, and dead-criteria for retry logic

Step 4: Create Authentication and Authorization Methods

Define method lists for authentication and authorization, specifying the use of the server group and cache.

```
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
```

These commands set up default method lists for 802.1X authentication and network authorization, prioritizing the cache and the server group.

If you want the WLC to check the cache first before attempting the RADIUS server (for faster authentication if the user is already cached), use:

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

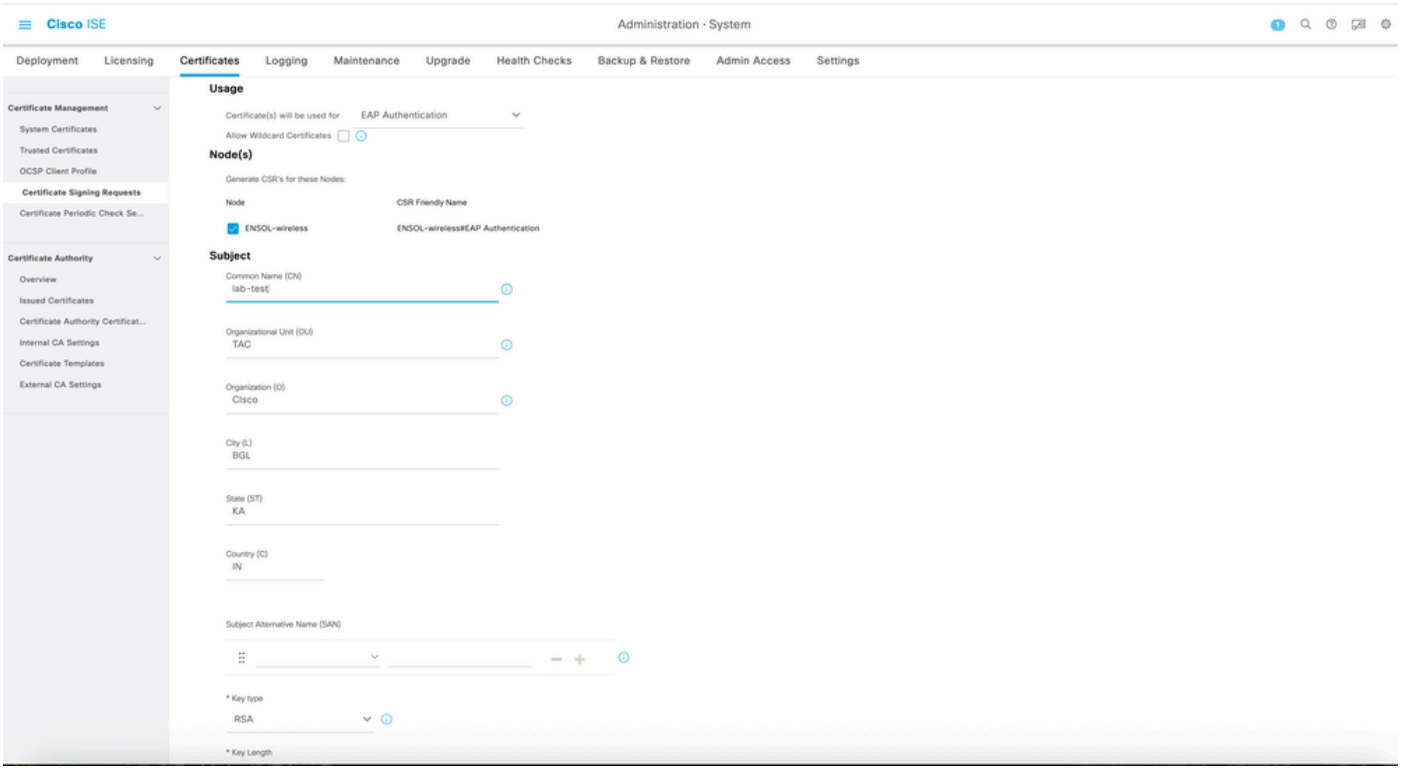
With these method lists, the WLC consults the cache first, only contacting the server if the user is not found in the cache, resulting in quicker authentication for cached clients.

Step 5: Configure TLS Authentication (Certificate Setup)

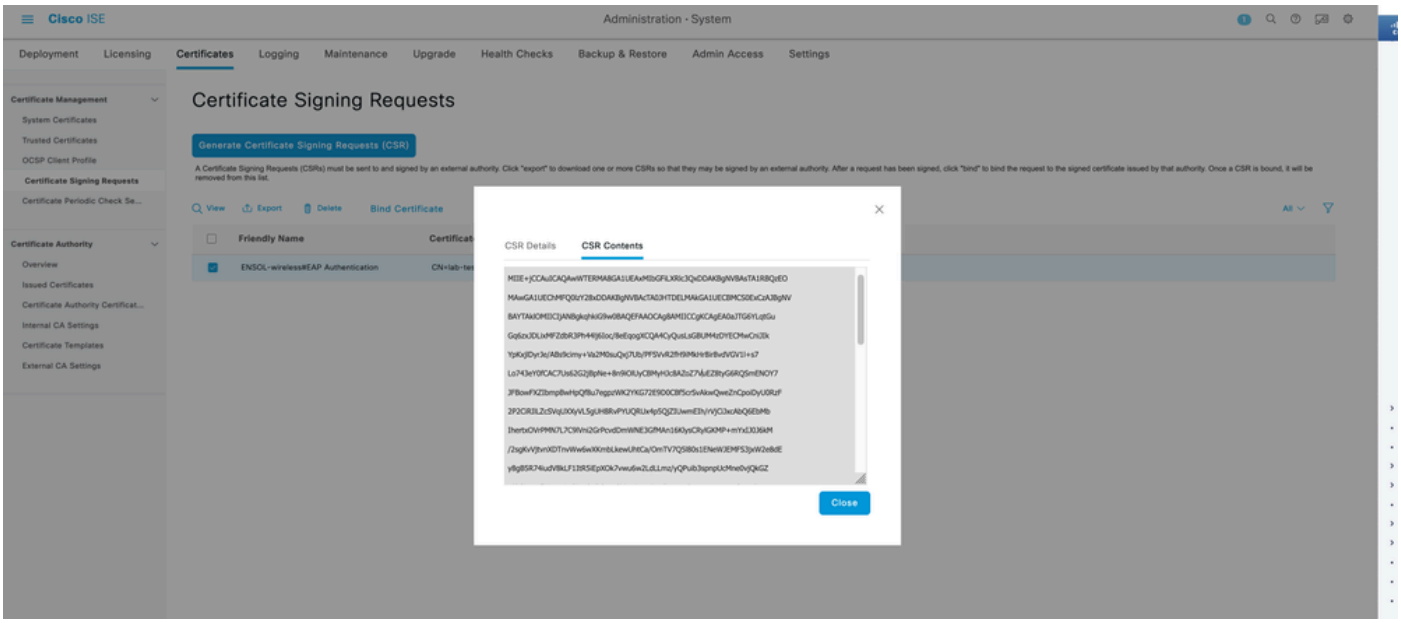
For EAP-TLS authentication, both the WLC and AAA server require server certificates signed by a Certificate Authority (CA).

On Cisco ISE (AAA Server):

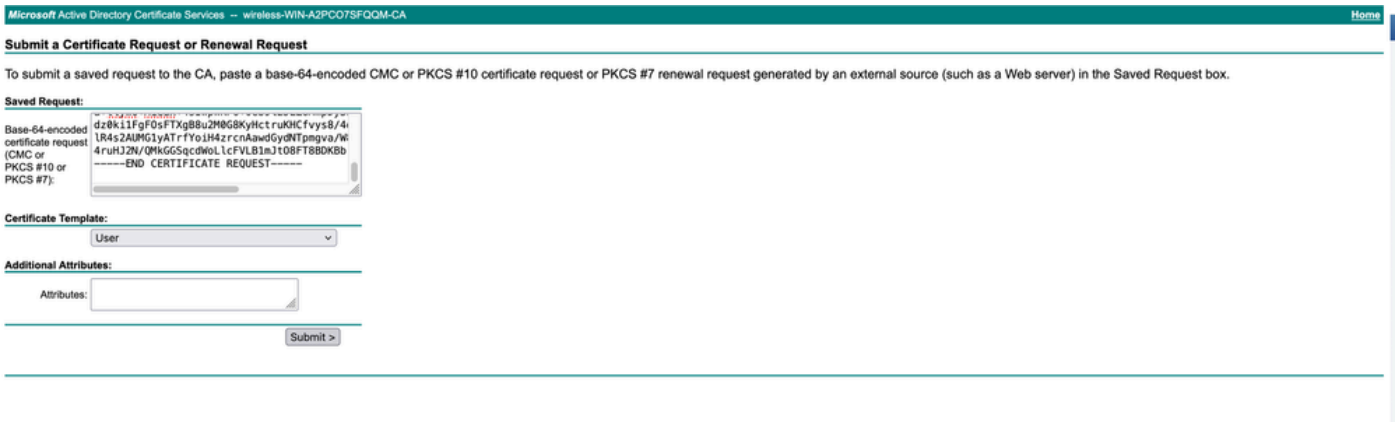
- Generate a Certificate Signing Request (CSR) via **Certificates > Certificate Management > Certificate Signing Requests**



- Copy the CSR content and get it signed by your CA

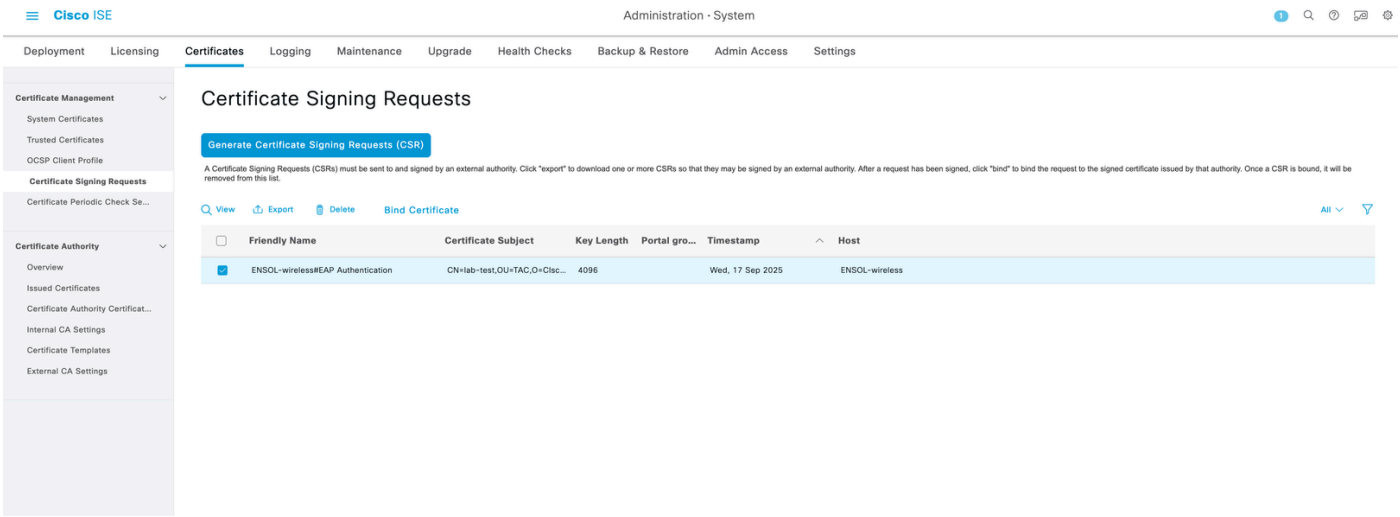


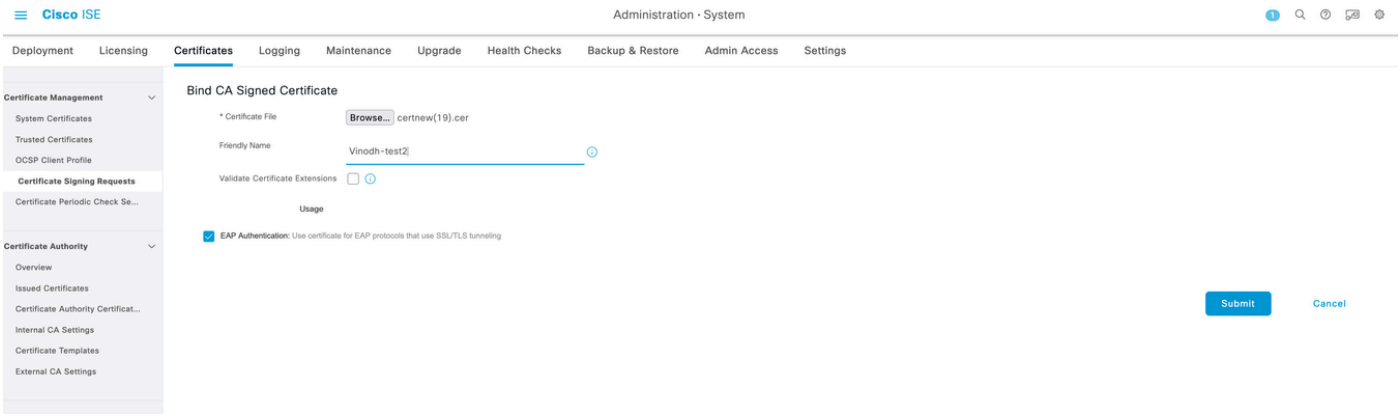
- Download the signed certificate (in **.cer** or **.pem** format)



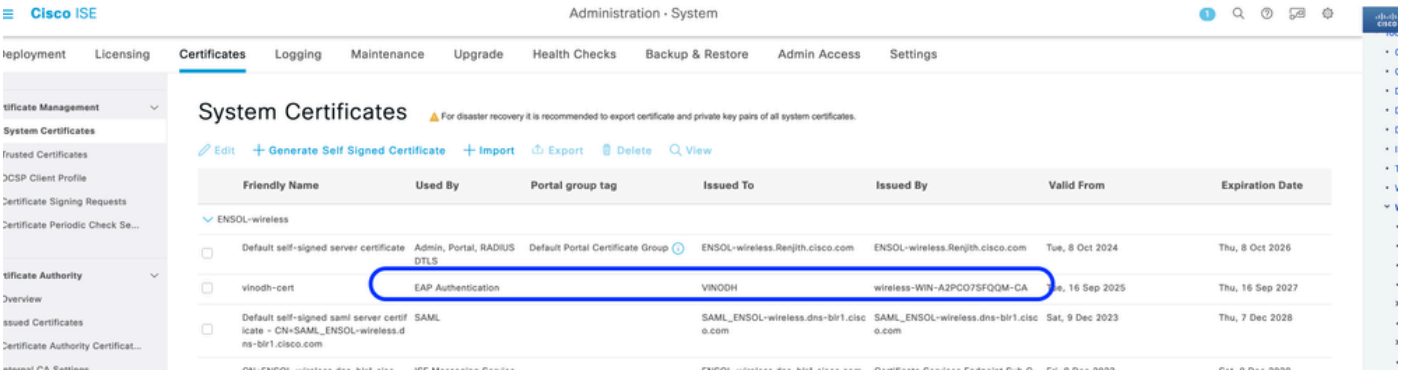


- Bind the certificate on ISE by browsing to the signed certificate file and clicking "Submit"



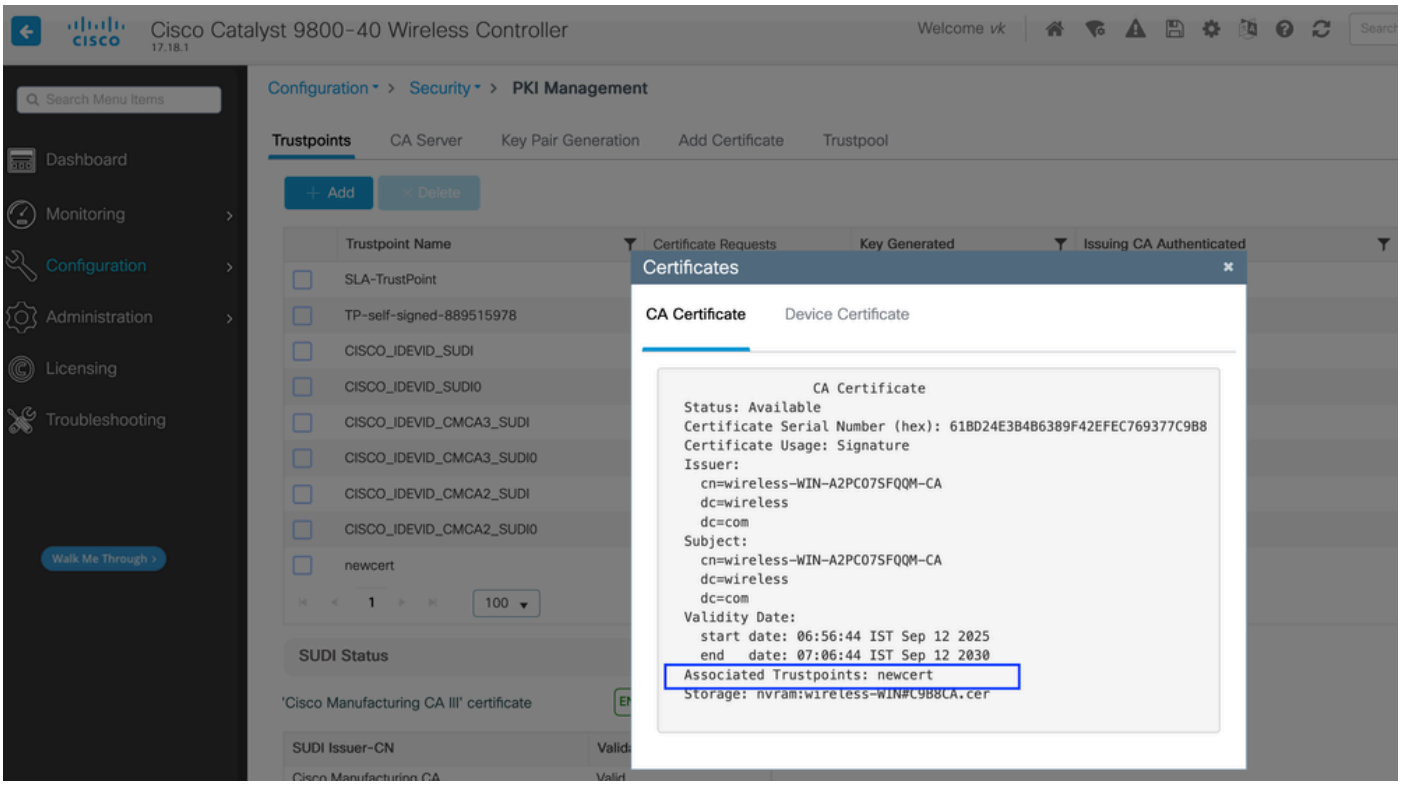


- Ensure the signed certificate is reflected under system certificate for EAP authentication



On Cisco Catalyst 9800 WLC:

- Generate a CSR on the WLC
- Get the CSR signed by the same CA used for ISE
- Upload the signed certificate to the WLC



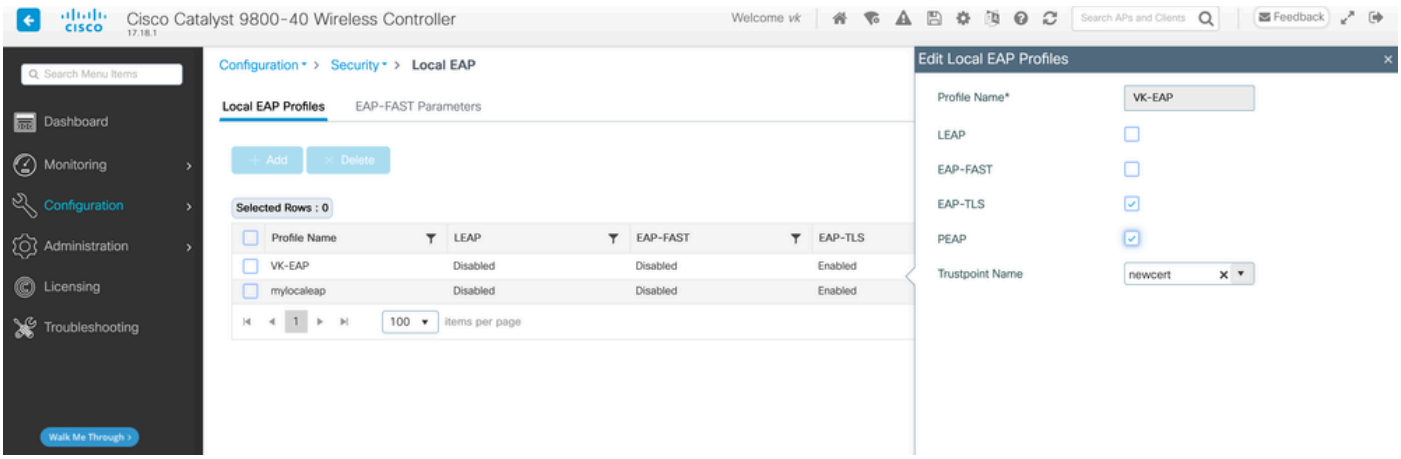
Step 6: Create Local EAP Profile and Map Trustpoint

Create a local EAP profile and map the trustpoint for EAP-TLS authentication.

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

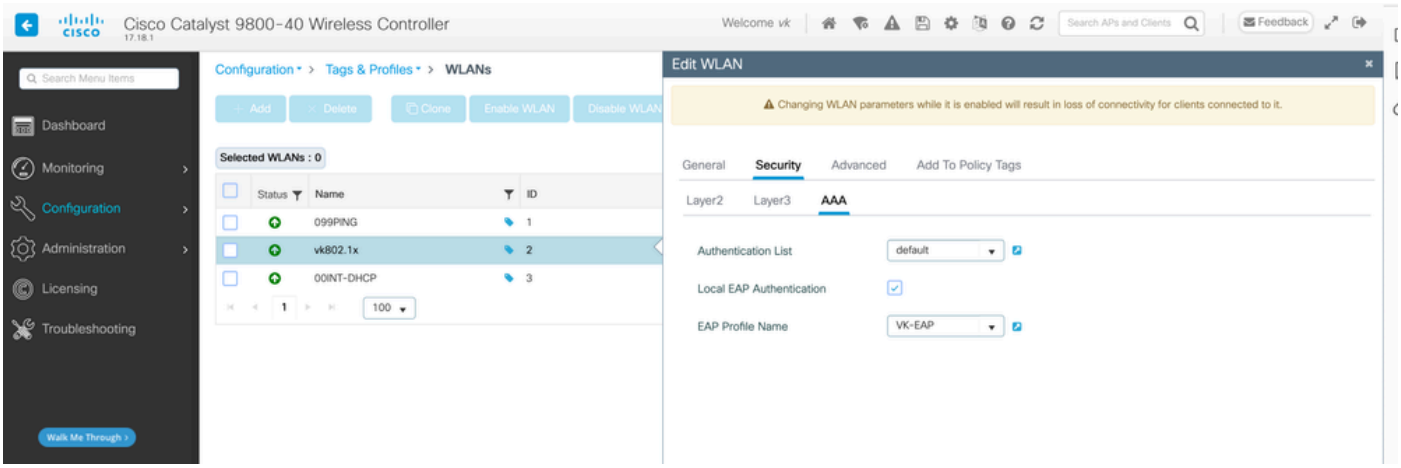
This command creates an EAP profile named **VK-EAP** using EAP-TLS and maps the trustpoint to the certificate named **newcert**.

GUI Method: Navigate to **Configuration > Security > Local EAP** and create the EAP profile.



Step 7: Apply Method List and EAP Profile to SSID

Configure your SSID to use the created authentication and EAP profile.




```
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
```

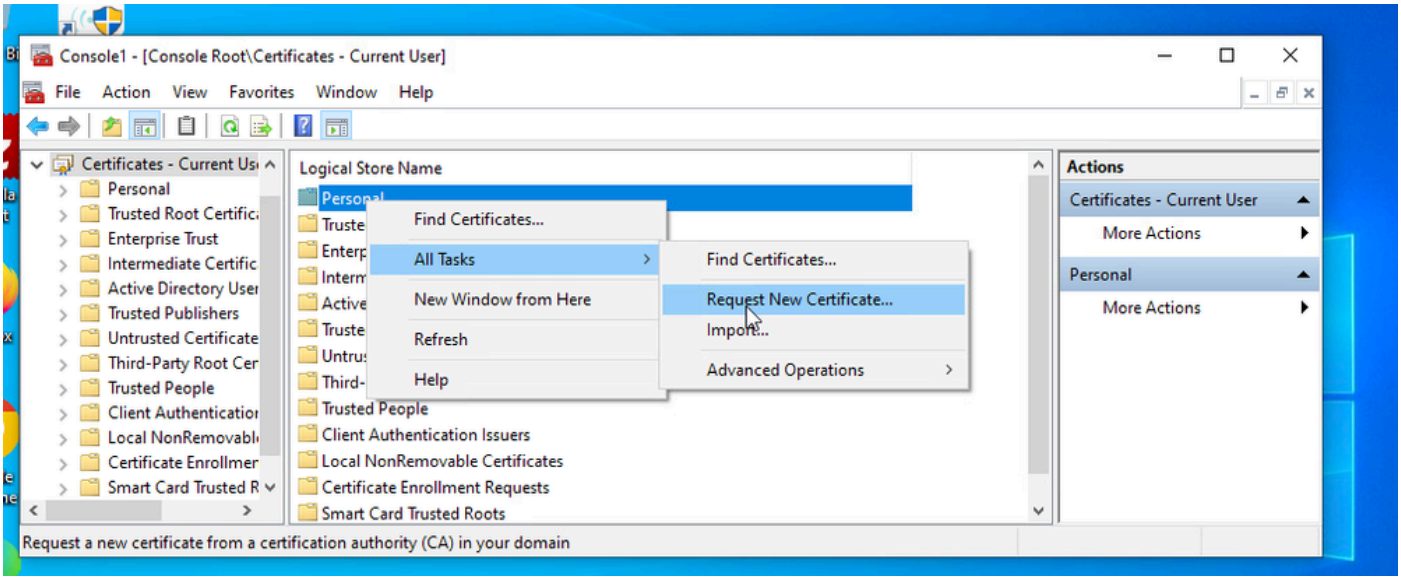
```
 no shutdown
```

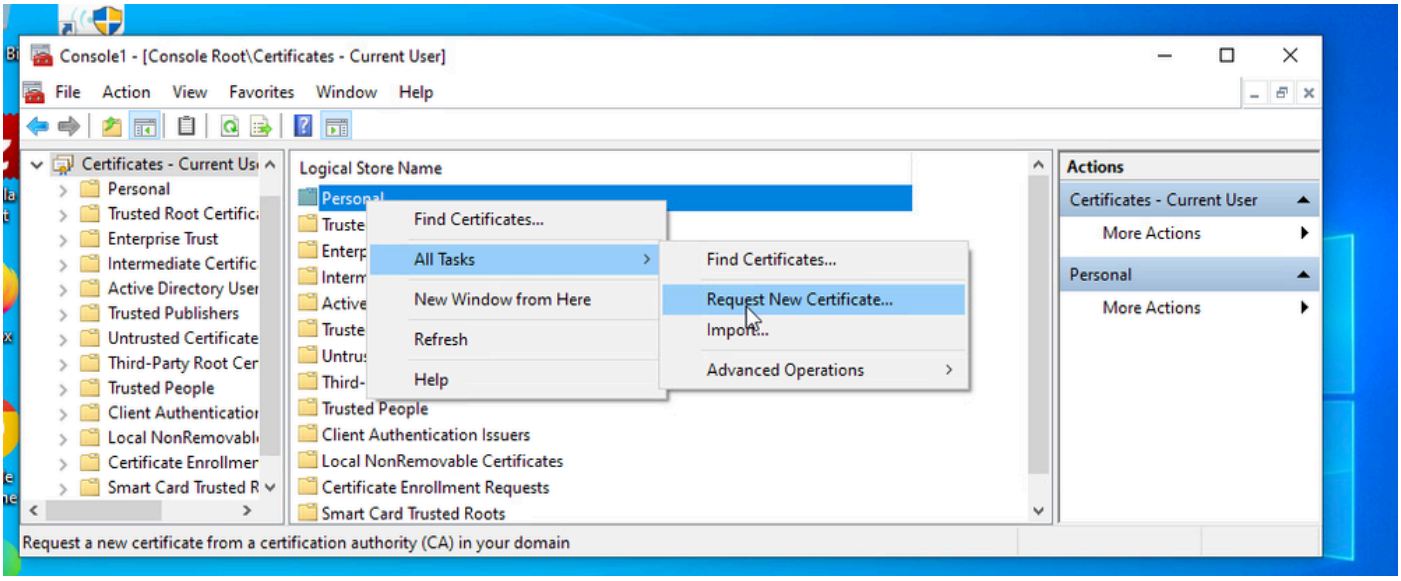
This configuration:

- Creates SSID **vk802.1x** with WLAN ID 2
- Enables local authentication with the **VK-EAP** profile
- Applies radio policies for both 2.4GHz and 5GHz bands
- Enforces 802.1X authentication using the default method list
- Brings up the SSID (no shutdown)

Step 8: User Certificate Deployment on Wireless Clients

Ensure that wireless clients have the necessary user certificate for authentication. For lab environments, a device joined to an Active Directory (AD) domain can receive the certificate via MMC (Microsoft Management Console). There are other methods to distribute certificates depending on your environment.





Verify

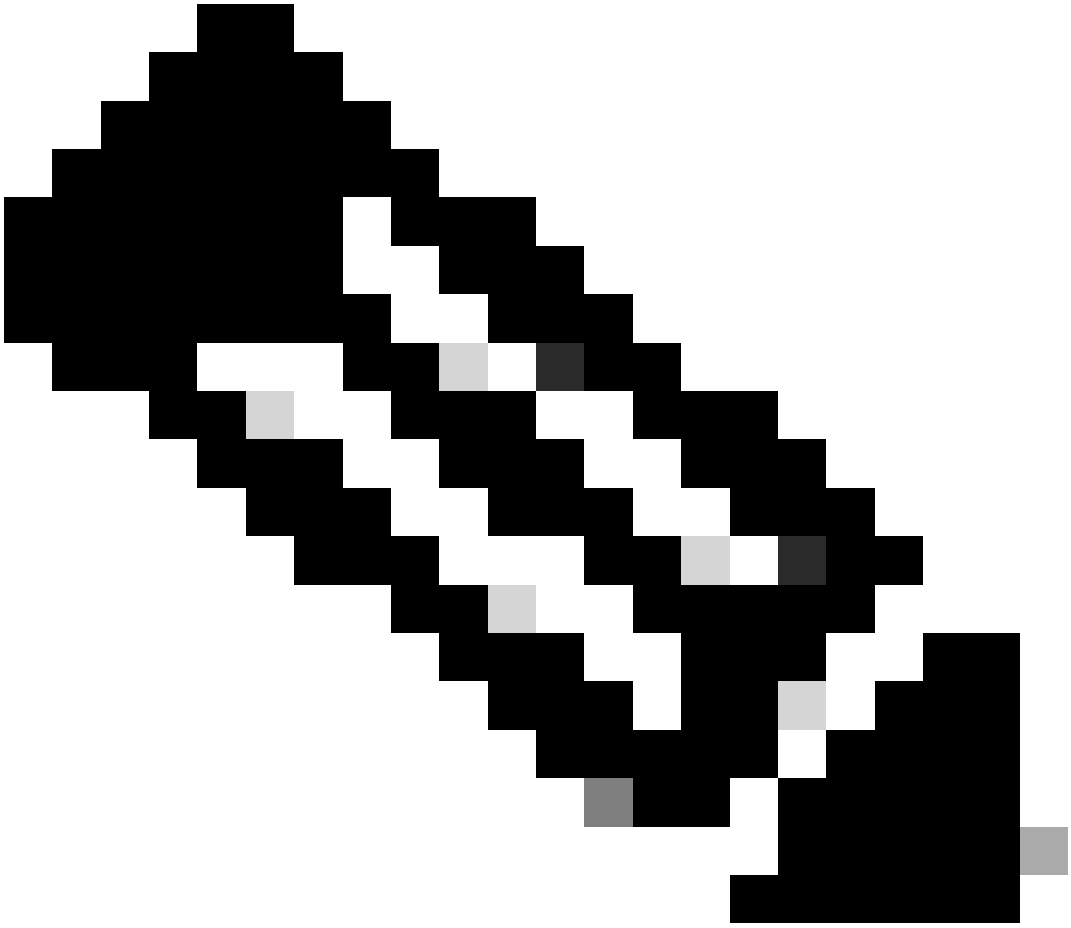
You can check the AAA cache entries on the 9800 WLC using CLI commands. Note that for Catalyst 9800 WLCs, cache entries are listed under "WNCD AAA Auth Cache entries", not "SMD AAA Auth Cache entries".

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

This command displays the current AAA cache entries stored on the WLC. Example output:

```
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
...
```

Verify that clients can reconnect and are authenticated via the AAA cache when the AAA server is unavailable.



Note: For PEAP authentication , the current design requires returning Cisco AV pairs containing the username and credential hash for each user during authentication by Radius server.

cisco-av-pair = AS-Username=testuser

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

Every user must be configured with the AV-pair attributes on RADIUS.

The Password or AS-Credential-Hash must be in the NT-hash format (https://codebeautify.org/ntlm-hash-generator).

Troubleshoot

Troubleshooting AAA cache and authentication issues involves several steps:

Step 1: Check AAA Cache Entries

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

Ensure that the expected client entries are present in the cache.

Step 2: Validate Certificate Installation and Trustpoints

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

Ensure that the certificates are correctly installed and mapped to the proper trustpoints for EAP-TLS authentication.

Step 3: Confirm Authentication Method Lists

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

Validate that method lists reference the correct server group and cache profiles.

Step 5: Check RA internal trace

<#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
```

References:

[17.18 Software Configuration Guide]