

9800 WLC에서 TLS를 위한 AAA 캐시 이해 및 구성

목차

소개

이 문서에서는 Cisco Catalyst 9800 WLC(Wireless LAN Controller)에서 AAA 캐시를 이해하고 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RADIUS 및 EAP 프로토콜을 포함한 AAA 인증 개념
- WLC(Wireless LAN Controller) 운영 및 컨피그레이션 워크플로
- 802.1X 인증 방법 및 인증서 관리
- 기본 PKI(Public Key Infrastructure) 및 인증서 서명 프로세스

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Catalyst 9800 Series Wireless LAN Controller
- 소프트웨어 릴리스 17.18.1 이상(이 릴리스에서 AAA 캐시 기능 지원)
- AAA/RADIUS 서버로서의 Cisco ISE(Identity Services Engine)
- 802.1X, EAP-TLS, EAP-PEAP, MAB 및 iPSK를 지원하는 네트워크 액세스 디바이스

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

802.1X와 같은 인증 방법은 외부 인증 서버(예: RADIUS 서버)와의 통신에 따라 달라집니다. WLC(Wireless LAN Controller)가 서버에 연결할 수 없거나 서버를 사용할 수 없는 경우 무선 클라이언트가 SSID에 연결할 수 없으므로 서비스가 중단됩니다. WLC는 인증이 성공할 때까지 클라이언트 트래픽을 차단합니다.

17.18.1 릴리스부터 AAA 캐시 기능을 사용하면 캐시된 인증 항목을 사용하여 AAA 서버를 사용할

수 없게 되더라도 Catalyst 9800 WLC에서 무선 클라이언트를 인증할 수 있습니다. 이를 통해 AAA 서버 중단 시 서비스 중단을 크게 줄이고 원활한 클라이언트 연결을 유지할 수 있습니다.

AAA 캐시 메커니즘은 액세스 포인트가 로컬 모드 또는 FlexConnect(중앙 인증) 모드에서 작동할 때 지원됩니다.

Cisco Catalyst 9800 WLC의 AAA 캐시 기능:

- 초기 인증(AAA 서버에 연결할 수 있는 경우): WLC는 RADIUS를 사용하여 구성된 AAA 서버에 클라이언트 인증 요청을 전달합니다. 서버가 Access-Accept를 반환하면 WLC는 클라이언트 인증 세부사항을 AAA 캐시에 로컬로 저장합니다.
- 클라이언트 재연결(AAA 서버에 연결할 수 없는 경우): 클라이언트가 캐시된 항목이 만료되기 전에 다시 연결되면 WLC는 로컬 AAA 캐시를 참조합니다. 캐시된 유효한 데이터가 있는 경우 AAA 서버에 연결하지 않고도 네트워크 액세스가 허용됩니다.
- 장애 조치 지원: 네트워크 문제 또는 장애로 인해 AAA 서버에 연결할 수 없는 경우, WLC는 캐시된 데이터를 사용하여 클라이언트를 계속 인증하므로 이전에 인증된 사용자가 중단 없는 액세스를 유지할 수 있습니다.
- 캐시 수명 및 만료: AAA 캐시의 항목은 임시적이며 구성 가능합니다. 기본 캐시 기간은 24시간입니다. 타이머를 0으로 설정하면 엔트리가 만료되지 않습니다. 캐시 엔트리가 만료된 후 클라이언트가 다시 연결되면 WLC는 인증을 위해 AAA 서버에 연결하려고 시도합니다.

```
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 캐시에 대해 지원되는 인증 유형은 다음과 같습니다.

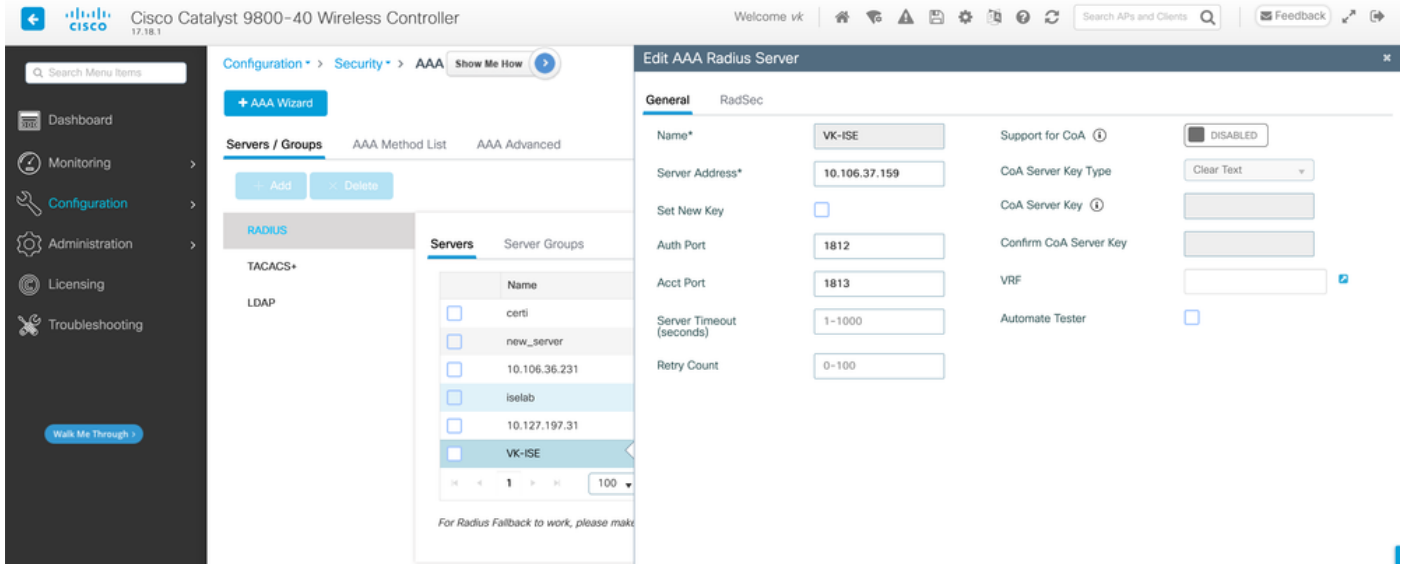
- EAP-TLS
- MSCHAPv2를 사용하는 EAP-PEAP
- MAB(MAC Authentication Bypass), MAB+PSK 및 MAB+802.1x/iPSK

구성

1단계: WLC에 AAA 서버 추가

먼저 AAA(RADIUS) 서버를 Wireless LAN Controller에 추가합니다. 이는 GUI 또는 CLI를 통해 수행할 수 있습니다.

GUI 방법: Configuration(컨피그레이션) > Security(보안) > AAA로 이동하여 서버를 추가합니다.



CLI 방법:

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

이 명령은 지정된 IP 주소, 인증 포트, 계정 관리 포트 및 공유 키를 사용하여 VK-ISE라는 RADIUS 서버 항목을 생성합니다.

2단계: AAA 캐시 프로파일 생성(CLI에만 해당)

캐시 동작을 정의하기 위한 AAA 캐시 프로파일을 생성합니다. 이 단계는 CLI 전용입니다.

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

이 명령은 VK-CACHE라는 캐시 프로파일을 만들고 지원되는 모든 인증 유형에 대해 캐싱을 활성화합니다.

3단계: 서버 그룹 생성 및 RADIUS 서버 및 캐시 프로파일 매핑(CLI에만 해당)

RADIUS 서버 그룹을 만들고, AAA 서버를 연결하고, 캐시 만료를 구성하고, 권한 부여/인증 프로파

일을 매핑합니다.

```
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
```

이 명령 집합은 다음과 같습니다.

- VK-SRV-GRP라는 서버 그룹을 만듭니다.
- VK-ISE 서버를 연결합니다
- 캐시 만료를 8시간으로 설정
- 권한 부여 및 인증 프로파일을 모두 VK-CACHE에 매핑합니다.
- 연결할 수 없는 서버의 데드 타임을 5분으로 설정하고, 재시도 논리를 위한 데드 기준을 설정합니다.

4단계: 인증 및 권한 부여 방법 생성

서버 그룹 및 캐시의 사용을 지정하여 인증 및 권한 부여를 위한 방법 목록을 정의합니다.

```
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
```

이 명령은 802.1X 인증 및 네트워크 권한 부여를 위한 기본 방법 목록을 설정하여 캐시 및 서버 그룹의 우선순위를 지정합니다.

RADIUS 서버를 시도하기 전에 WLC가 먼저 캐시를 확인하도록 하려면(사용자가 이미 캐시되어 있는 경우 빠른 인증을 위해) 다음을 사용합니다.

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

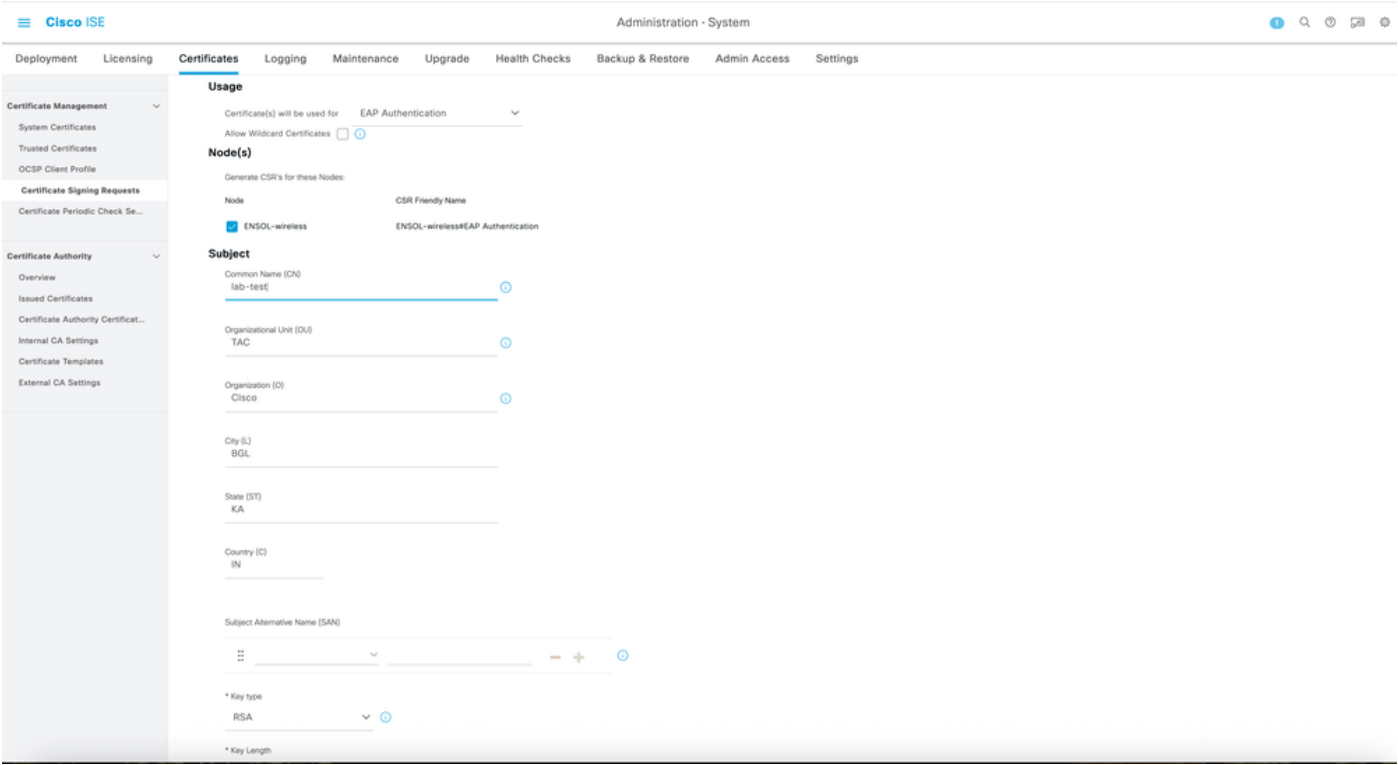
이러한 방법 목록을 사용하면 WLC는 먼저 캐시를 참조하고 사용자가 캐시에 없는 경우에만 서버에 연결하여 캐시된 클라이언트를 더 빠르게 인증합니다.

5단계: TLS 인증 구성(인증서 설정)

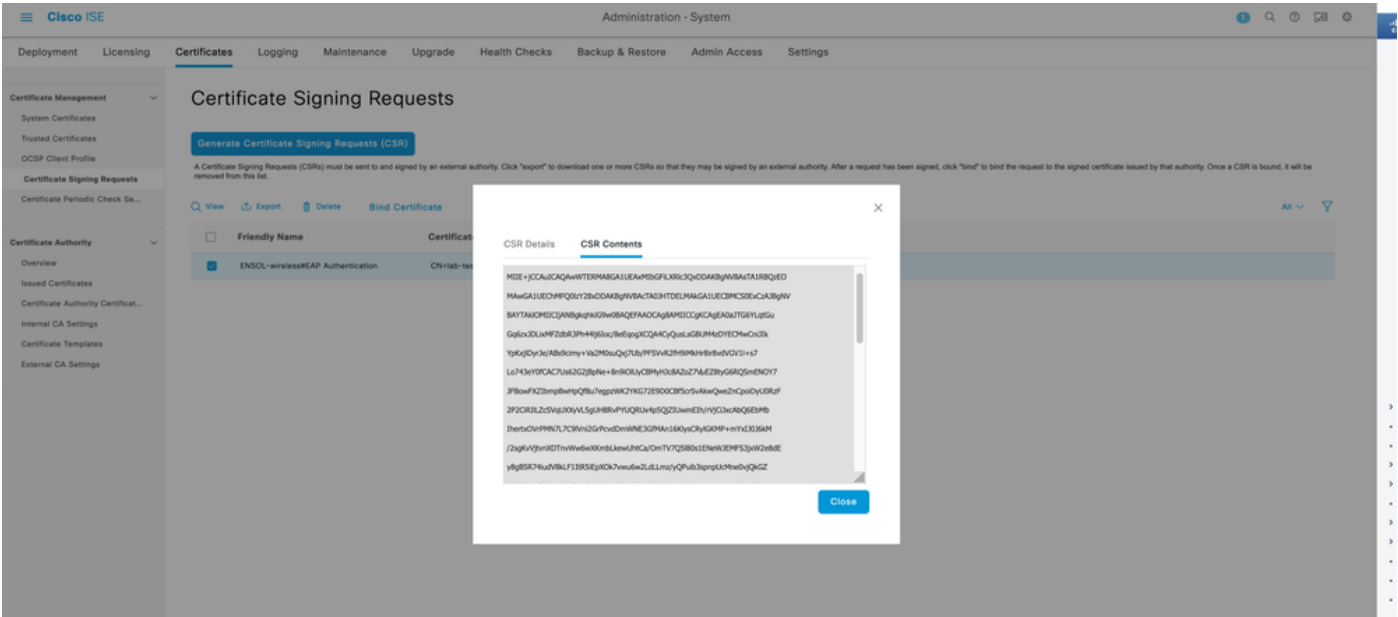
EAP-TLS 인증의 경우 WLC 및 AAA 서버 모두 CA(Certificate Authority)에서 서명한 서버 인증서가 필요합니다.

Cisco ISE(AAA 서버)에서 다음을 수행합니다.

- Certificates(인증서) > Certificate Management(인증서 관리) > Certificate Signing Requests(인증서 서명 요청)를 통해 CSR(Certificate Signing Request)을 생성합니다.



- CSR 콘텐츠를 복사하고 CA에서 서명 받기



- 서명된 인증서 다운로드(.cer 또는 .pem 형식)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded
certificate request
(CMC or
PKCS #10 or
PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
d20k11FgF0sFTXgBBu2H0G8KyHct ruKHCfvys8/4-
UR4s2AUMG1yATrFY0JH4zrcnAawdGydNtpmgva/W-
4ruHJ2N/QMKGGSgcw0L1cFVLB1mJ108FT8B0Kbb
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

User

Additional Attributes:

Attributes:

Submit >

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

- 서명된 인증서 파일을 찾아 "Submit(제출)"을 클릭하여 ISE에서 인증서를 바인딩합니다.

Certificate Signing Requests

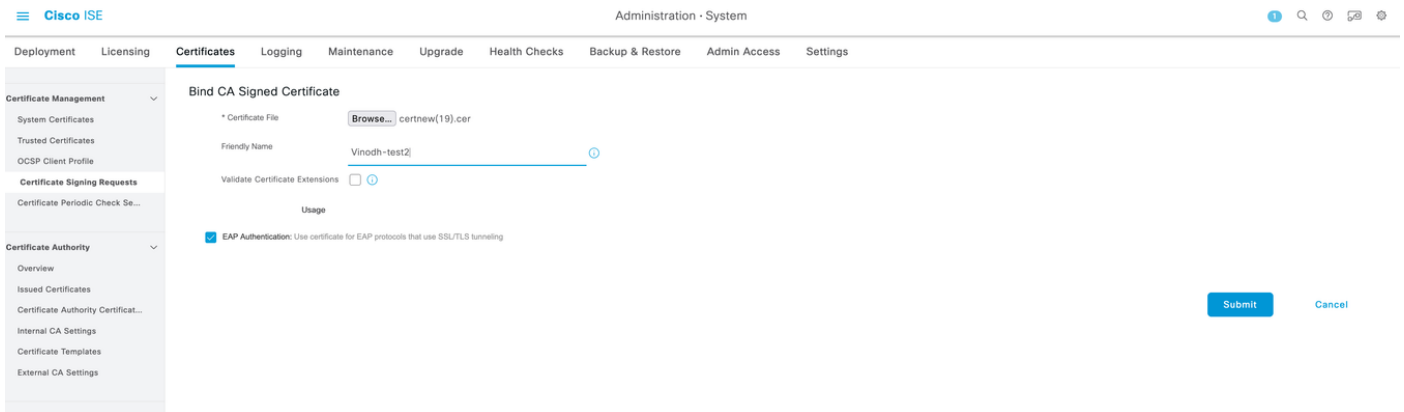
Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

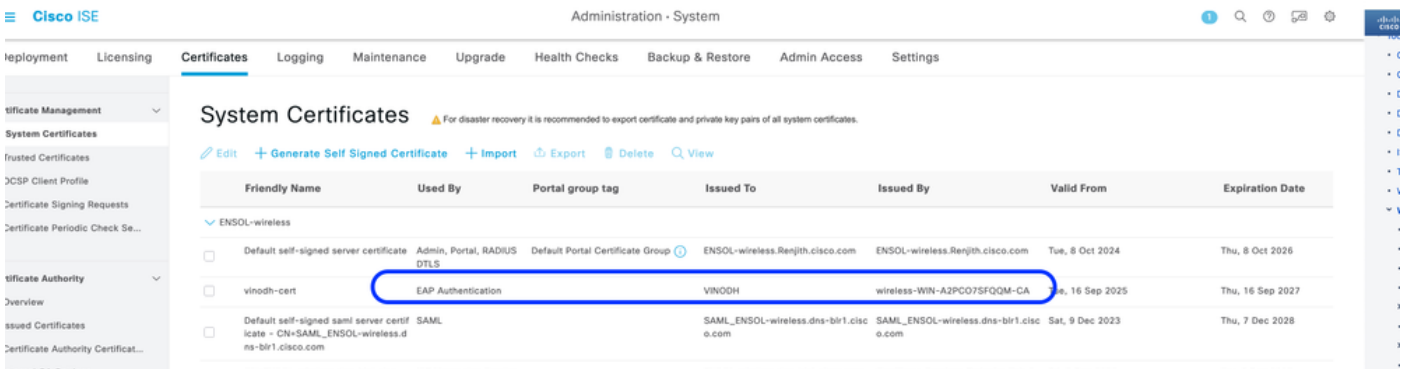
[View](#) [Export](#) [Delete](#) [Bind Certificate](#)

All

☐	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
☒	ENSOL-wirelessREAP Authentication	CN=lab-test,OU=TAC,O=Clisc...	4096		Wed, 17 Sep 2025	ENSOL-wireless

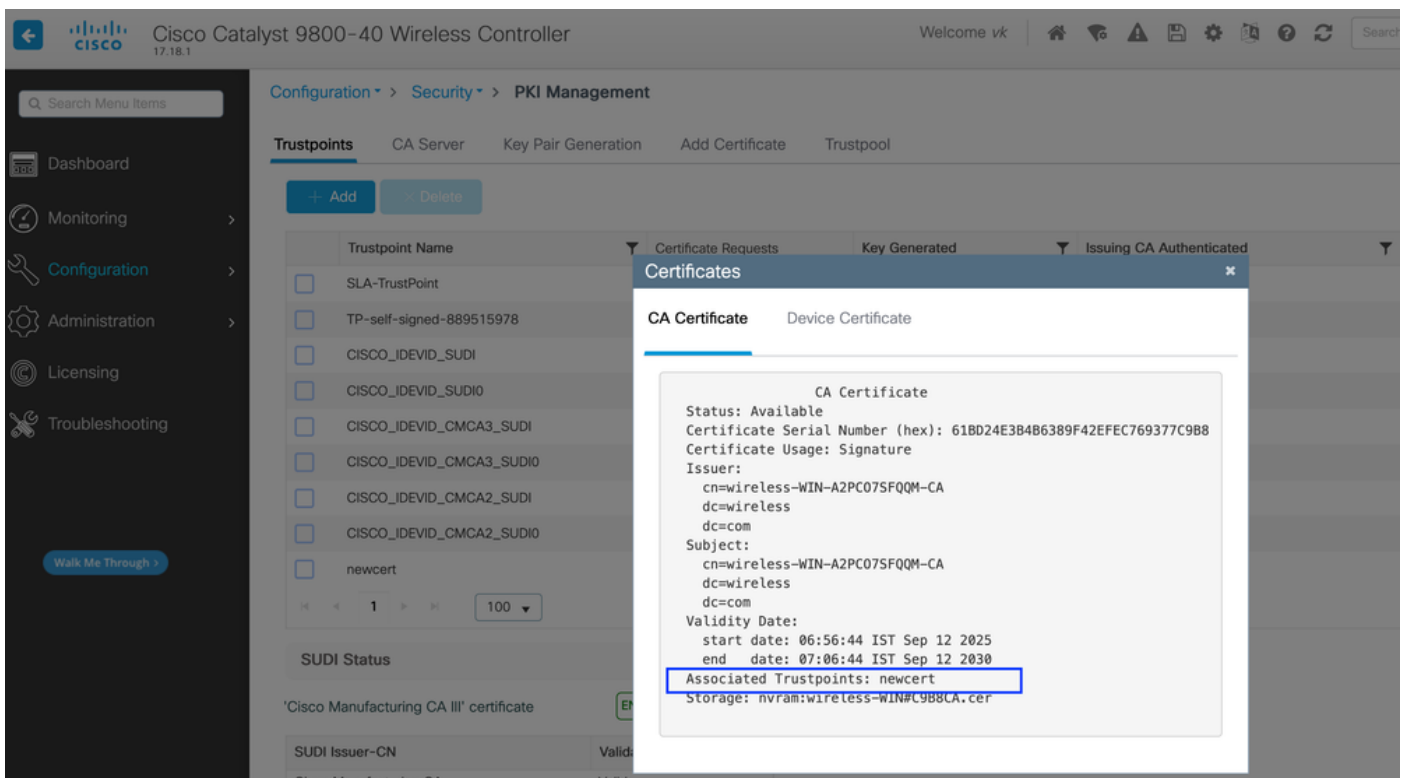


- 서명된 인증서가 EAP 인증을 위해 시스템 인증서에 반영되는지 확인합니다



Cisco Catalyst 9800 WLC의 경우:

- WLC에서 CSR 생성
- ISE에 사용된 것과 동일한 CA에서 서명한 CSR 가져오기
- 서명된 인증서를 WLC에 업로드합니다



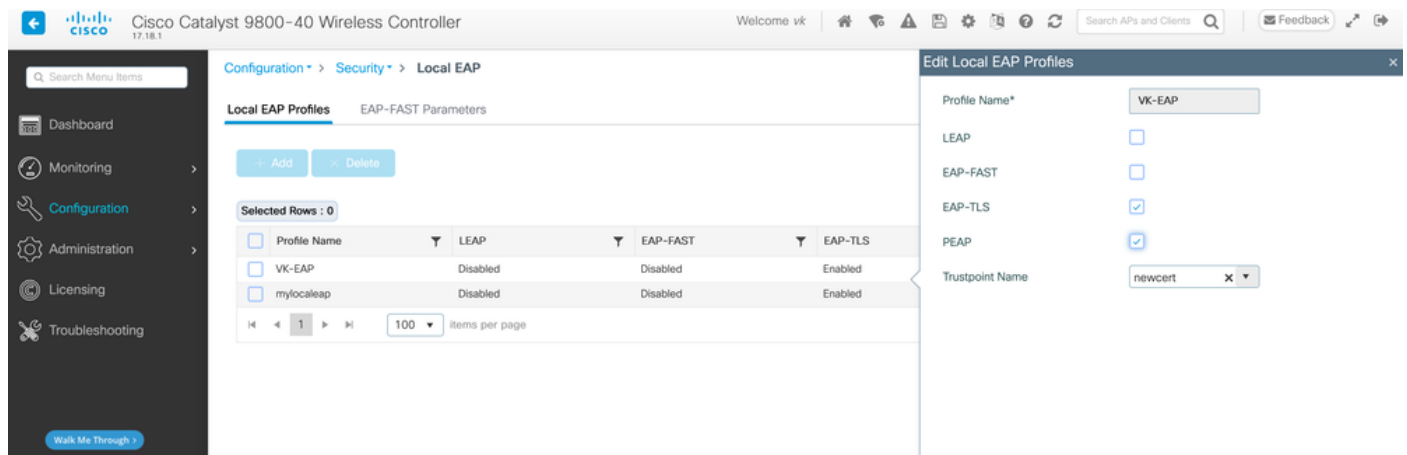
6단계: 로컬 EAP 프로파일 생성 및 신뢰 지점 매핑

로컬 EAP 프로파일을 생성하고 EAP-TLS 인증을 위한 신뢰 지점을 매핑합니다.

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

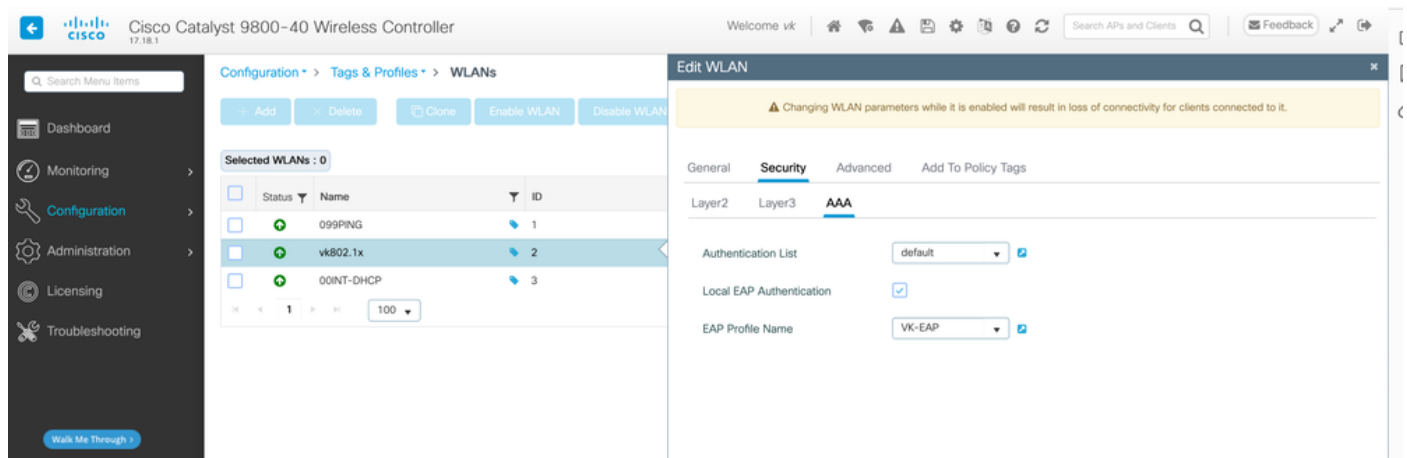
이 명령은 EAP-TLS를 사용하여 VK-EAP라는 EAP 프로파일을 생성하고 신뢰 지점을 newcert라는 인증서에 매핑합니다.

GUI 방법: Configuration(컨피그레이션) > Security(보안) > Local EAP(로컬 EAP)로 이동하고 EAP 프로파일을 생성합니다.



7단계: SSID에 방법 목록 및 EAP 프로파일 적용

생성된 인증 및 EAP 프로파일을 사용하도록 SSID를 구성합니다.



```
wlan vk802.1x 2 vk802.1x
local-auth VK-EAP
radio policy dot11 24ghz
```

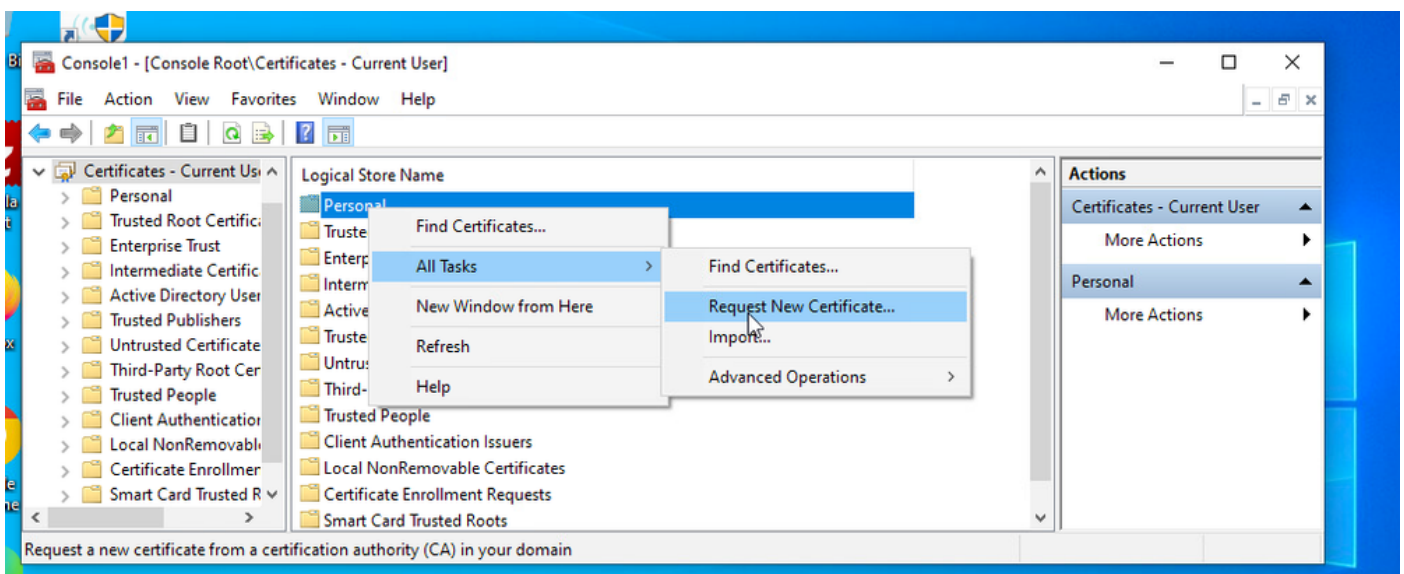
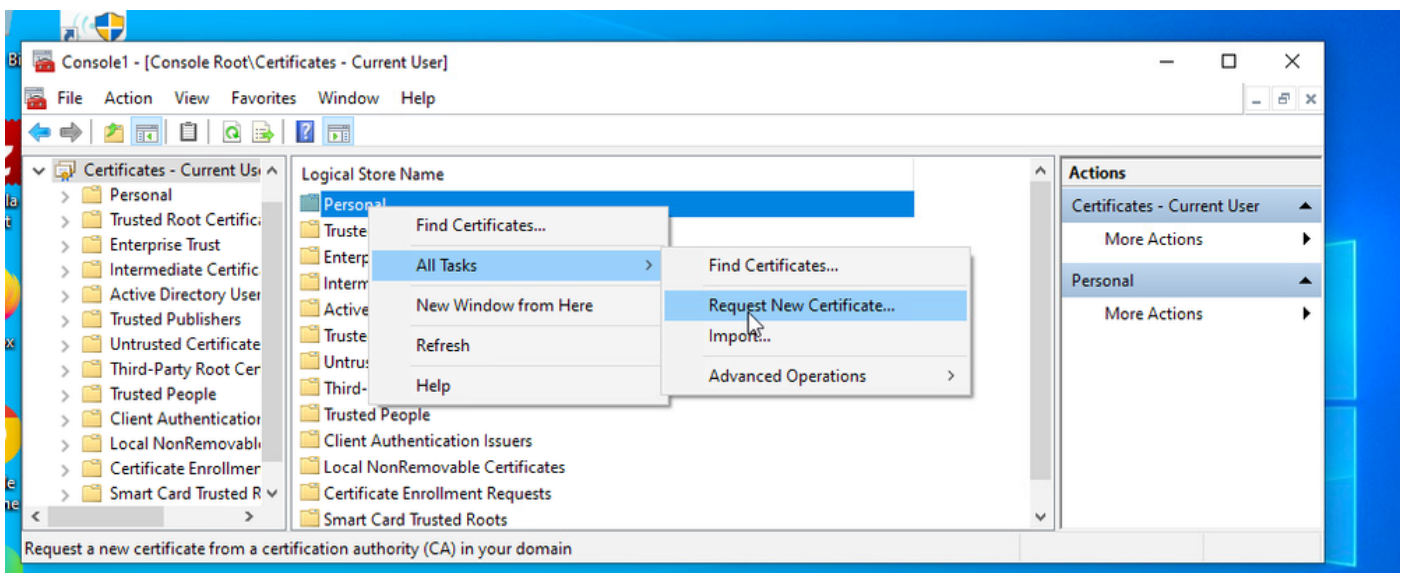
```
radio policy dot11 5ghz
no security ft adaptive
security dot1x authentication-list default
no shutdown
```

이 컨피그레이션:

- WLAN ID 2로 SSID vk802.1x를 생성합니다.
- VK-EAP 프로파일을 사용하여 로컬 인증을 활성화합니다.
- 2.4GHz 및 5GHz 대역 모두에 무선 정책 적용
- 기본 방법 목록을 사용하여 802.1X 인증을 적용합니다.
- SSID를 표시합니다(종료 없음).

8단계: 무선 클라이언트의 사용자 인증서 배포

무선 클라이언트에 인증에 필요한 사용자 인증서가 있는지 확인합니다. 랩 환경의 경우 AD(Active Directory) 도메인에 가입한 디바이스는 MMC(Microsoft Management Console)를 통해 인증서를 받을 수 있습니다. 환경에 따라 인증서를 배포하는 다른 방법이 있습니다.



다음을 확인합니다.

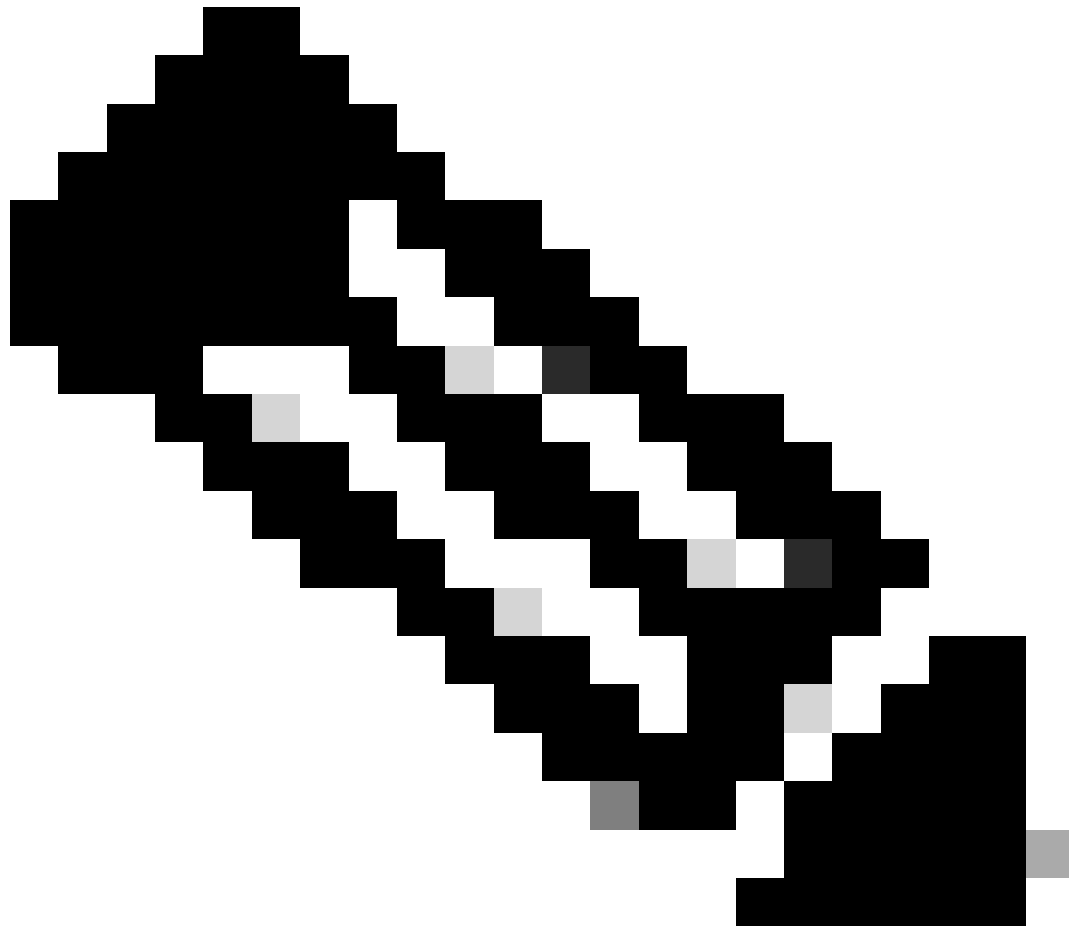
CLI 명령을 사용하여 9800 WLC에서 AAA 캐시 항목을 확인할 수 있습니다. Catalyst 9800 WLC의 경우 캐시 항목은 "SMD AAA Auth Cache entries"가 아니라 "WNCD AAA Auth Cache entries" 아래에 나열됩니다.

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

이 명령은 WLC에 저장된 현재 AAA 캐시 항목을 표시합니다. 출력 예:

```
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
...
```

AAA 서버를 사용할 수 없을 때 클라이언트가 다시 연결하고 AAA 캐시를 통해 인증될 수 있는지 확인합니다.



참고: PEAP 인증의 경우, 현재 설계에서는 Radius 서버에 의한 인증 중에 각 사용자에게 대한 사용자 이름 및 자격 증명 해시가 포함된 Cisco AV 쌍을 반환해야 합니다.

cisco av 쌍 = AS 사용자 이름 = testuser

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

모든 사용자는 RADIUS에서 AV 쌍 특성으로 구성해야 합니다.

비밀번호 또는 AS-Credential-Hash는 NT-hash 형식(<https://codebeautify.org/ntlm-hash-generator>)이어야 합니다.

문제 해결

AAA 캐시 및 인증 문제를 트러블슈팅하려면 여러 단계를 수행해야 합니다.

1단계: AAA 캐시 항목 확인

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

필요한 클라이언트 항목이 캐시에 있는지 확인합니다.

2단계: 인증서 설치 및 신뢰 지점 검증

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

인증서가 올바르게 설치되고 EAP-TLS 인증을 위한 적절한 신뢰 지점에 매핑되어 있는지 확인합니다.

3단계: 인증 방법 목록 확인

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

메서드 목록이 올바른 서버 그룹 및 캐시 프로ファイルを 참조하는지 확인합니다.

5단계: RA 내부 추적 확인

<#root>

```
2025/09/18 13:02:37.069850424 {wncd_x_R0-0}{2}: [radius] [16292]: (ERR): RADIUS/DECODE: No response from
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 wrap
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 requ
```

```
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 l
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_EVENTS
```

```
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(00000000)
```

this indicates 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 l
```

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

참조:

[17.18 소프트웨어 컨피그레이션 가이드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.