AAA-cache voor TLS op 9800 WLC begrijpen en configureren

Inhoud

Inleiding

In dit document wordt beschreven hoe u AAA-cache kunt begrijpen en configureren op Cisco Catalyst 9800 Wireless LAN Controllers (WLC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- AAA-verificatieconcepten, waaronder RADIUS- en EAP-protocollen
- Werking- en configuratieworkflows van de Wireless LAN Controller (WLC)
- 802.1X-verificatiemethoden en certificaatbeheer
- Basisprocessen voor de ondertekening van Public Key Infrastructure (PKI) en certificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 9800-reeks draadloze LAN-controller
- Softwarerelease 17.18.1 of hoger (AAA-cachefunctie wordt ondersteund vanaf deze release)
- Cisco Identity Services Engine (ISE) als AAA/RADIUS-server
- Netwerktoegangsapparaten die 802.1X, EAP-TLS, EAP-PEAP, MAB en iPSK ondersteunen

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Authenticatiemethoden zoals 802.1X zijn afhankelijk van communicatie met een externe verificatieserver (zoals een RADIUS-server). Wanneer de draadloze LAN-controller (WLC) de server niet kan bereiken of wanneer de server niet beschikbaar is, kunnen draadloze clients geen verbinding maken met de SSID, waardoor de service wordt onderbroken. De WLC blokkeert clientverkeer totdat de verificatie succesvol is.

Vanaf versie 17.18.1 kan de Catalyst 9800 WLC met de AAA-cachefunctie draadloze clients verifiëren, zelfs als de AAA-server niet meer beschikbaar is met behulp van verificatiegegevens in de cache. Hierdoor wordt de onderbreking van de service tijdens uitval van de AAA-server aanzienlijk verminderd en blijft de clientconnectiviteit naadloos.

Het AAA-cachemechanisme wordt ondersteund wanneer toegangspunten in de lokale modus of in de FlexConnect-modus (centrale verificatie) werken.

AAA Cache Functionaliteit op Cisco Catalyst 9800 WLC:

- Initiële verificatie (wanneer AAA-server bereikbaar is): De WLC stuurt het clientverificatieverzoek door naar de geconfigureerde AAA-server met RADIUS. Zodra de server Access-Accept retourneert, slaat de WLC de clientverificatiegegevens lokaal op in de AAA-cache.
- Client Reconnection (Wanneer AAA-server onbereikbaar is): Als een client opnieuw verbinding maakt voordat de invoer in de cache verloopt, raadpleegt de WLC de lokale AAA-cache. Als er geldige gegevens in de cache aanwezig zijn, wordt netwerktoegang verleend zonder contact op te nemen met de AAA-server.
- Failover-ondersteuning: als de AAA-server onbereikbaar is vanwege netwerkproblemen of een storing, blijft de WLC clients verifiëren met behulp van gegevens in de cache, zodat eerder geverifieerde gebruikers ononderbroken toegang behouden.
- Levensduur en vervaldatum van cache: items in de AAA-cache zijn tijdelijk en configureerbaar. De standaardcacheduur is 24 uur; als u de timer instelt op 0, vervallen de vermeldingen nooit. Als een client opnieuw verbinding maakt nadat de cache-invoer is verlopen, probeert de WLC de AAA-server te bereiken voor verificatie.

```
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
```

Ondersteunde verificatietypen voor AAA-cache zijn onder meer:

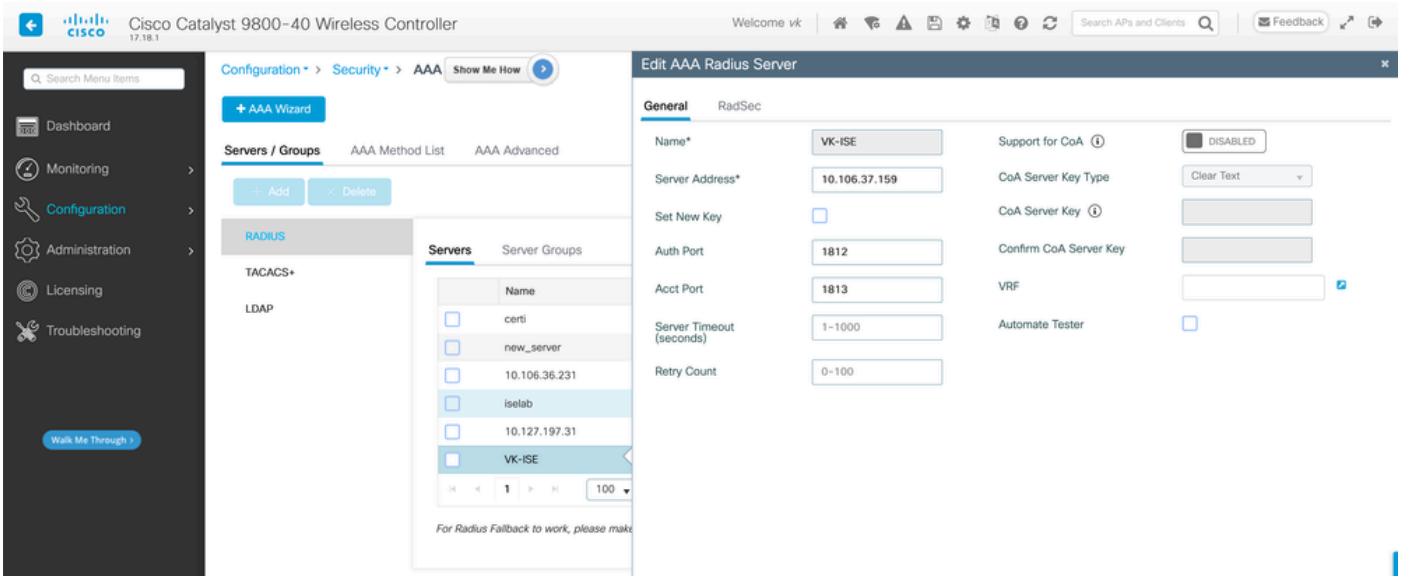
- EAP-TLS
- EAP-PEAP met MSCHAPv2
- MAC Authentication Bypass (MAB), MAB+PSK en MAB+802.1x/iPSK

Configureren

Stap 1: AAA-server toevoegen aan WLC

Begin met het toevoegen van uw AAA-server (RADIUS) aan de draadloze LAN-controller. Dit kan worden gedaan via de GUI of CLI.

GUI-methode: Navigeer naar Configuratie > Beveiliging > AAA en voeg uw server toe.



CLI-methode:

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

Met deze opdracht wordt een RADIUS-serveritem gemaakt met de naam VK-ISE met het opgegeven IP-adres, de verificatiepoort, de accountpoort en de gedeelde sleutel.

Stap 2: AAA-cacheprofiel maken (alleen CLI)

Maak een AAA-cacheprofiel om het cachegedrag te definiëren. Deze stap is alleen CLI.

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

Met deze opdracht wordt een cacheprofiel met de naam VK-CACHE gemaakt en wordt caching voor alle ondersteunde verificatietypen mogelijk gemaakt.

Stap 3: Servergroep maken en RADIUS-server en cacheprofiel toewijzen (alleen CLI)

Maak een RADIUS-servergroep, koppel de AAA-server, configureer het verlopen van de cache en geef autorisatie-/verificatieprofielen voor toewijzingen op.

```
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
```

Deze set van opdrachten:

- Maakt een servergroep aan met de naam VK-SRV-GRP
- Associeert de VK-ISE-server
- Stel het cacheverloop in op 8 uur
- Koppelt zowel autorisatie- als authenticatieprofielen aan VK-CACHE
- Stelt de deadline voor onbereikbare servers in op 5 minuten en dode-criteria voor herhalingslogica

Stap 4: Authenticatie- en autorisatiemethoden maken

Methodenlijsten definiëren voor verificatie en autorisatie, met vermelding van het gebruik van de servergroep en 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
```

Met deze opdrachten worden standaardmethodenlijsten voor 802.1X-verificatie en netwerkautorisatie ingesteld, waarbij prioriteit wordt gegeven aan de cache en de servergroep.

Als u wilt dat de WLC eerst de cache controleert voordat de RADIUS-server wordt gebruikt (voor een snellere verificatie als de gebruiker al in de cache is geplaatst), gebruikt u:

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

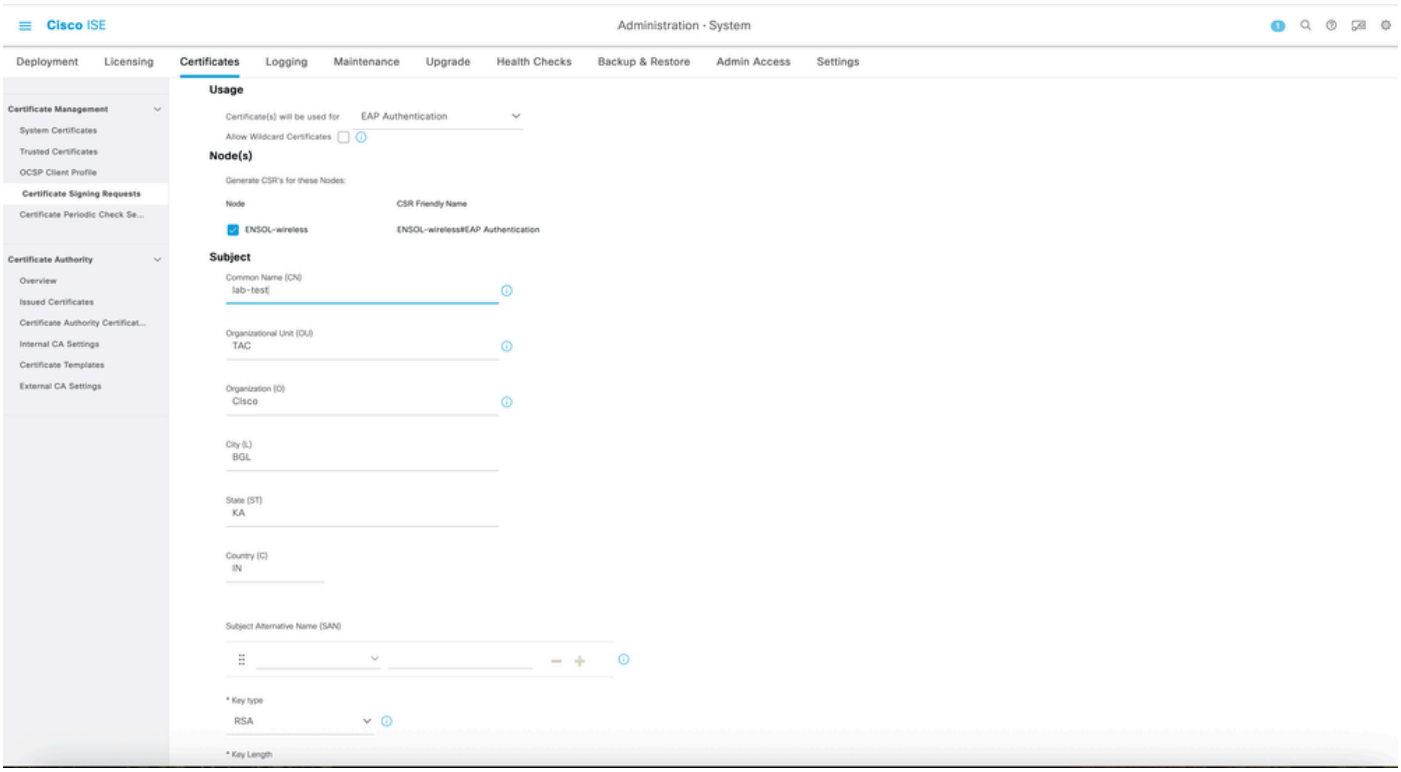
Met deze methodenlijsten raadpleegt de WLC eerst de cache en neemt alleen contact op met de server als de gebruiker niet in de cache wordt gevonden, wat resulteert in een snellere verificatie voor clients in de cache.

Stap 5: TLS-verificatie configureren (certificaatinstelling)

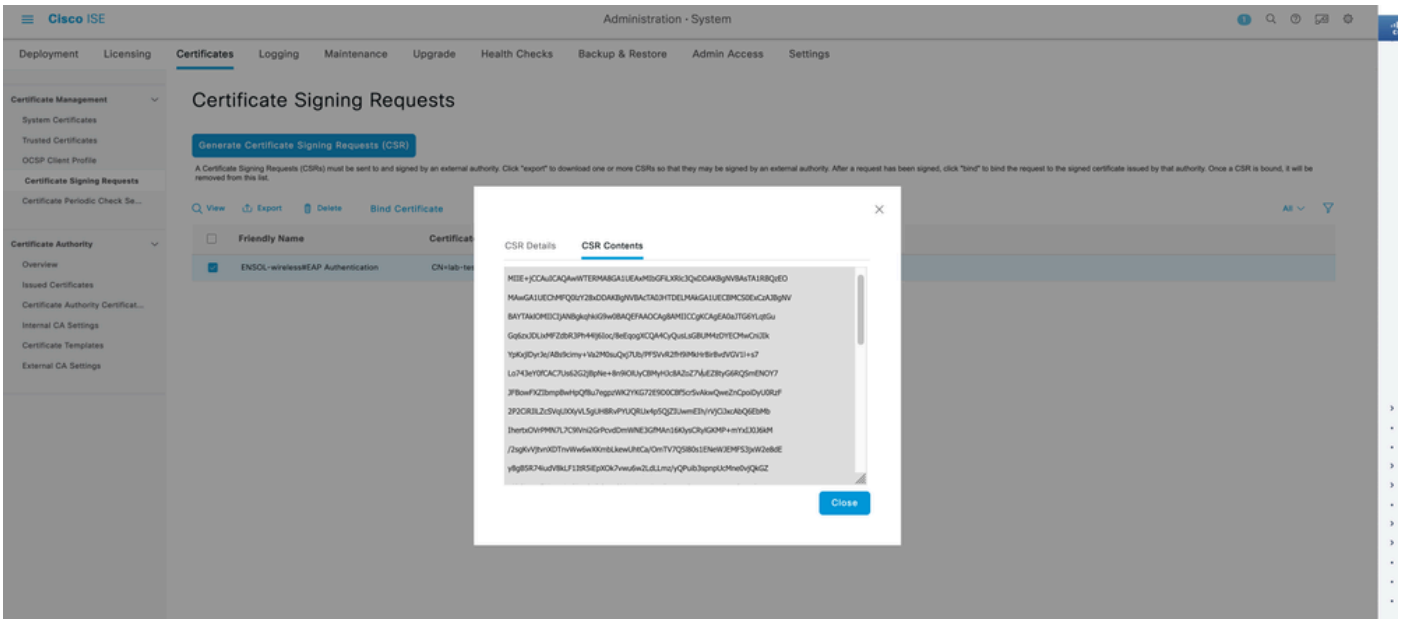
Voor EAP-TLS-verificatie hebben zowel de WLC- als de AAA-server servercertificaten nodig die zijn ondertekend door een certificeringsinstantie (CA).

Op Cisco ISE (AAA-server):

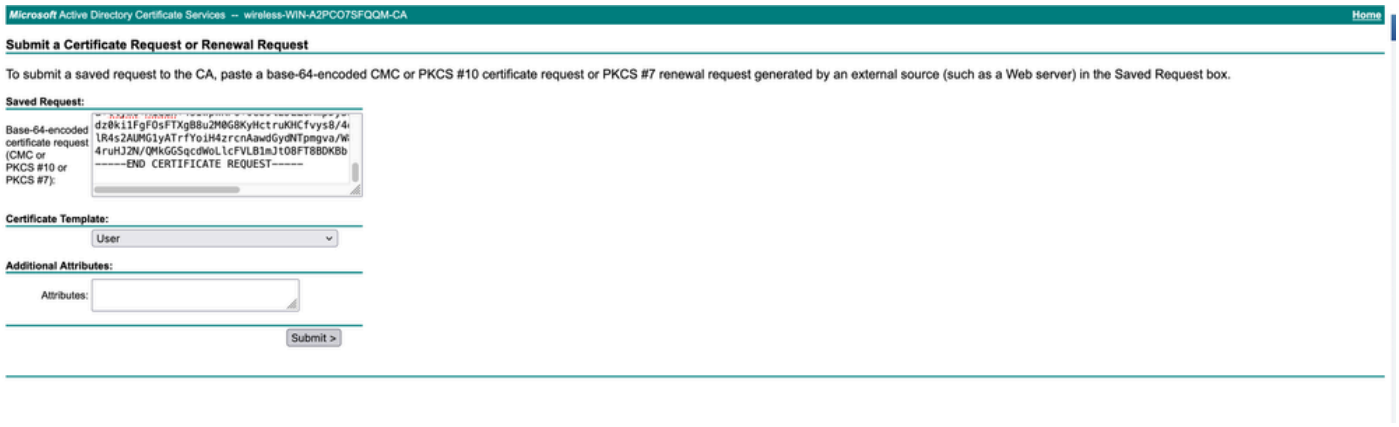
- Een aanvraag voor certificaatondertekening genereren via Certificaten > Certificaatbeheer > Certificaatondertekeningsverzoeken



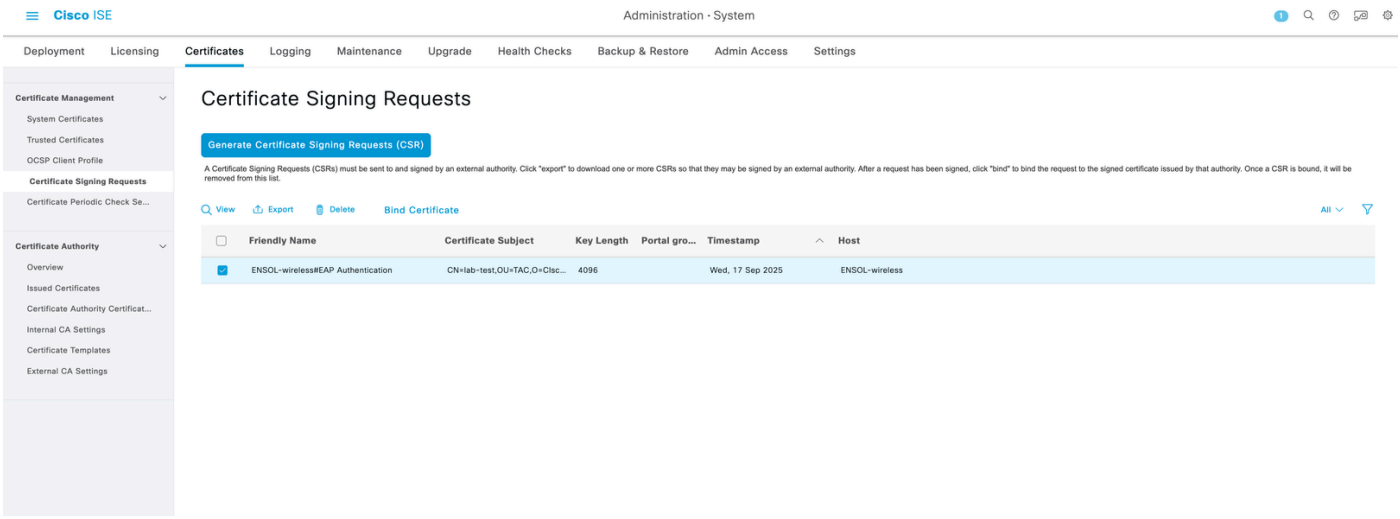
- Kopieer de CSR-inhoud en laat deze ondertekenen door uw CA

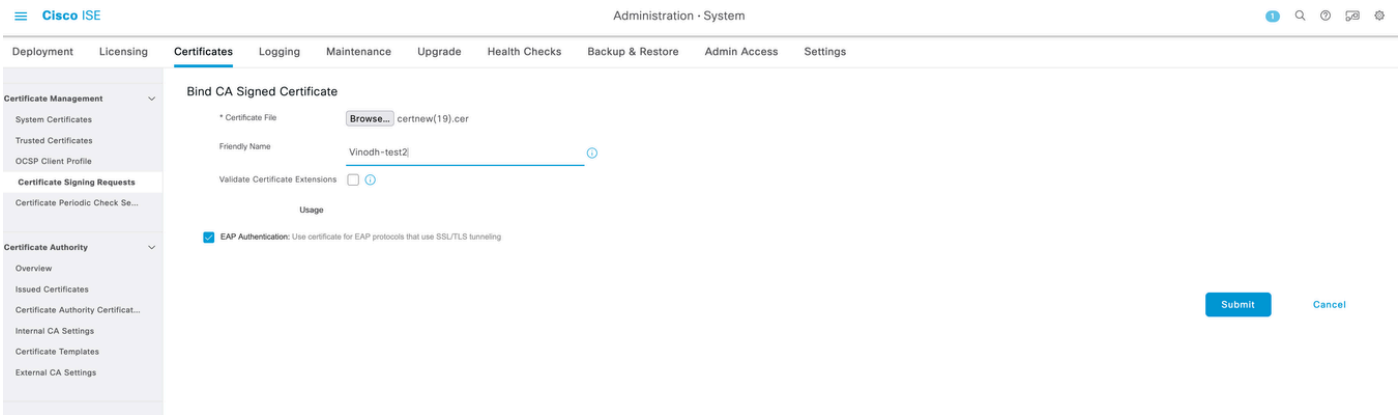


- Download het ondertekende certificaat (in .cer of .pem formaat)

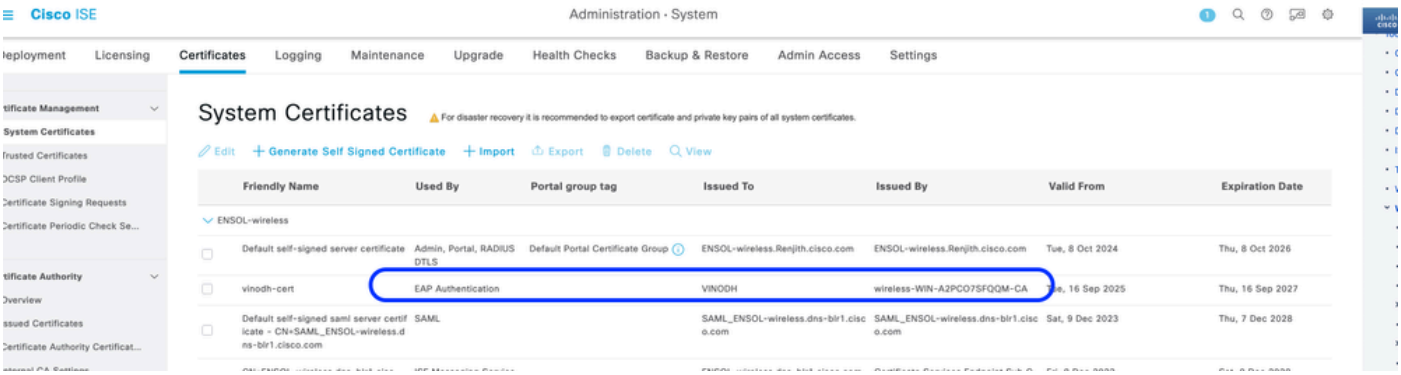


- Bind het certificaat op ISE door naar het ondertekende certificaatbestand te bladeren en op "Verzenden" te klikken



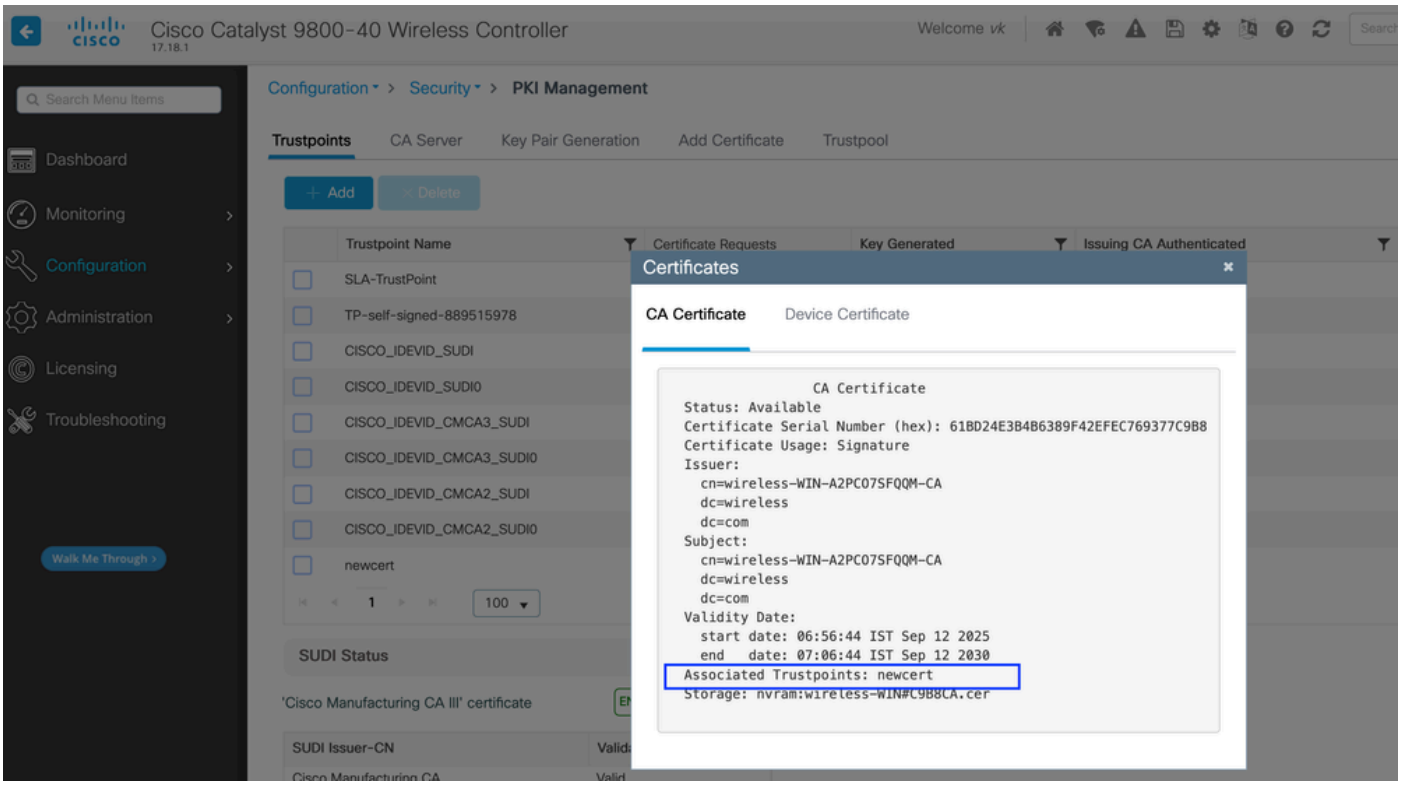


- Ervoor zorgen dat het ondertekende certificaat wordt weergegeven in het systeemcertificaat voor EAP-verificatie



Op Cisco Catalyst 9800 WLC:

- Genereer een CSR op de WLC
- Laat de CSR ondertekenen door dezelfde CA die voor ISE wordt gebruikt
- Upload het ondertekende certificaat naar de WLC



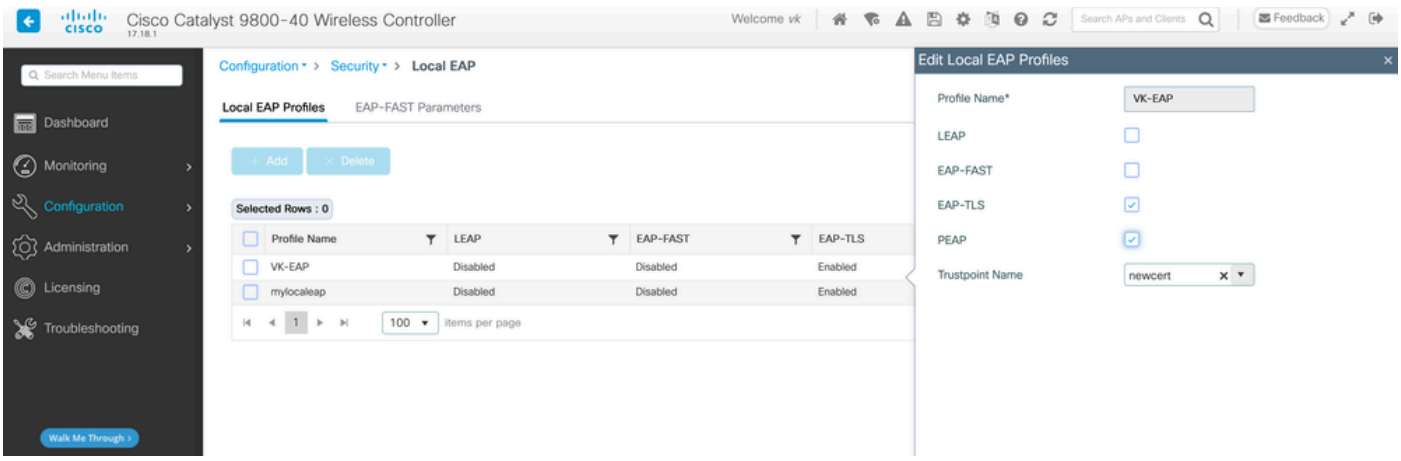
Stap 6: Maak een lokaal EAP-profiel en maak een Trustpoint-kaart

Maak een lokaal EAP-profiel en wijs het vertrouwenspunt voor EAP-TLS-verificatie toe.

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

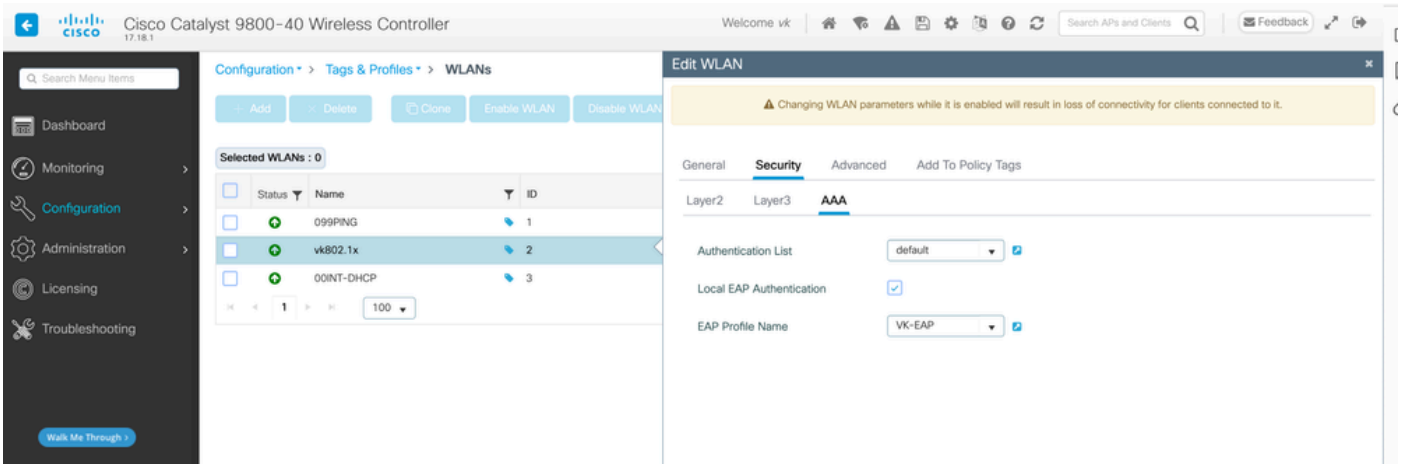
Deze opdracht maakt een EAP-profiel met de naam VK-EAP met behulp van EAP-TLS en koppelt het trustpoint aan het certificaat met de naam newcert.

GUI-methode: Navigeer naar Configuratie > Beveiliging > Lokale EAP en maak het EAP-profiel.



Stap 7: Methodenlijst en EAP-profiel toepassen op SSID

Configureer uw SSID om de gemaakte verificatie en het EAP-profiel te gebruiken.



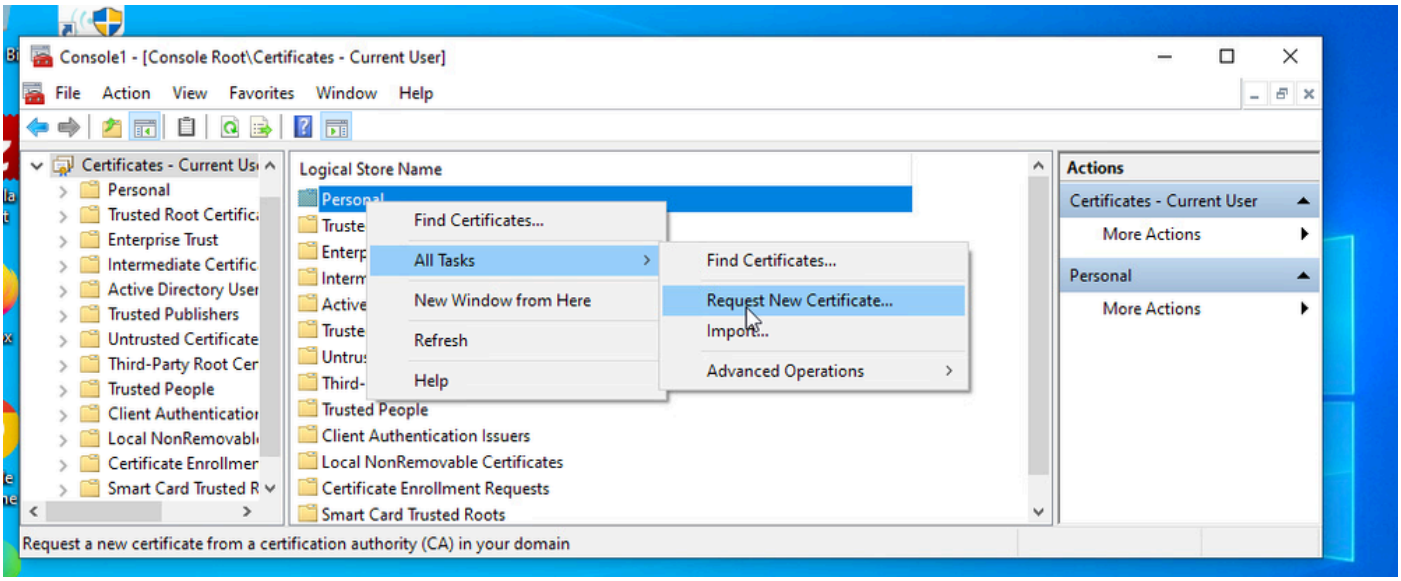

```
wlan vk802.1x 2 vk802.1x
 local-auth VK-EAP
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 security dot1x authentication-list default
 no shutdown
```

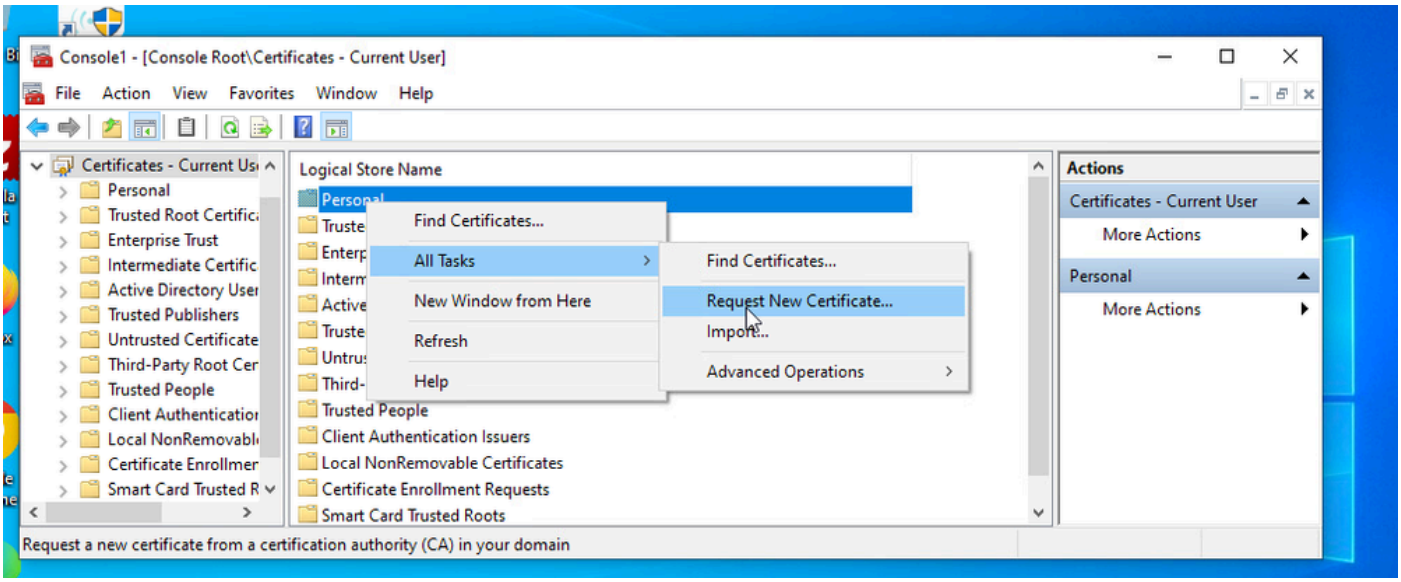
Deze configuratie:

- Hiermee maakt u SSID vk802.1x met WLAN-ID 2
- Hiermee wordt lokale verificatie met het VK-EAP-profiel ingeschakeld
- Past radiobeleid toe voor zowel 2,4 GHz- als 5 GHz-banden
- 802.1X-verificatie afdwingen met de standaardmethodenlijst
- Brengt de SSID omhoog (niet afsluiten)

Stap 8: Implementatie van gebruikerscertificaten op draadloze clients

Zorg ervoor dat draadloze clients beschikken over het benodigde gebruikerscertificaat voor verificatie. Voor laboratoriumomgevingen kan een apparaat dat is gekoppeld aan een Active Directory (AD)-domein het certificaat ontvangen via MMC (Microsoft Management Console). Er zijn andere methoden om certificaten te distribueren, afhankelijk van uw omgeving.





Verifiëren

U kunt de AAA-cachegegevens op de 9800 WLC controleren met CLI-opdrachten. Merk op dat voor Catalyst 9800 WLC's cachevermeldingen worden vermeld onder "WNCD AAA Auth Cache-vermeldingen", niet "SMD AAA Auth Cache-vermeldingen".

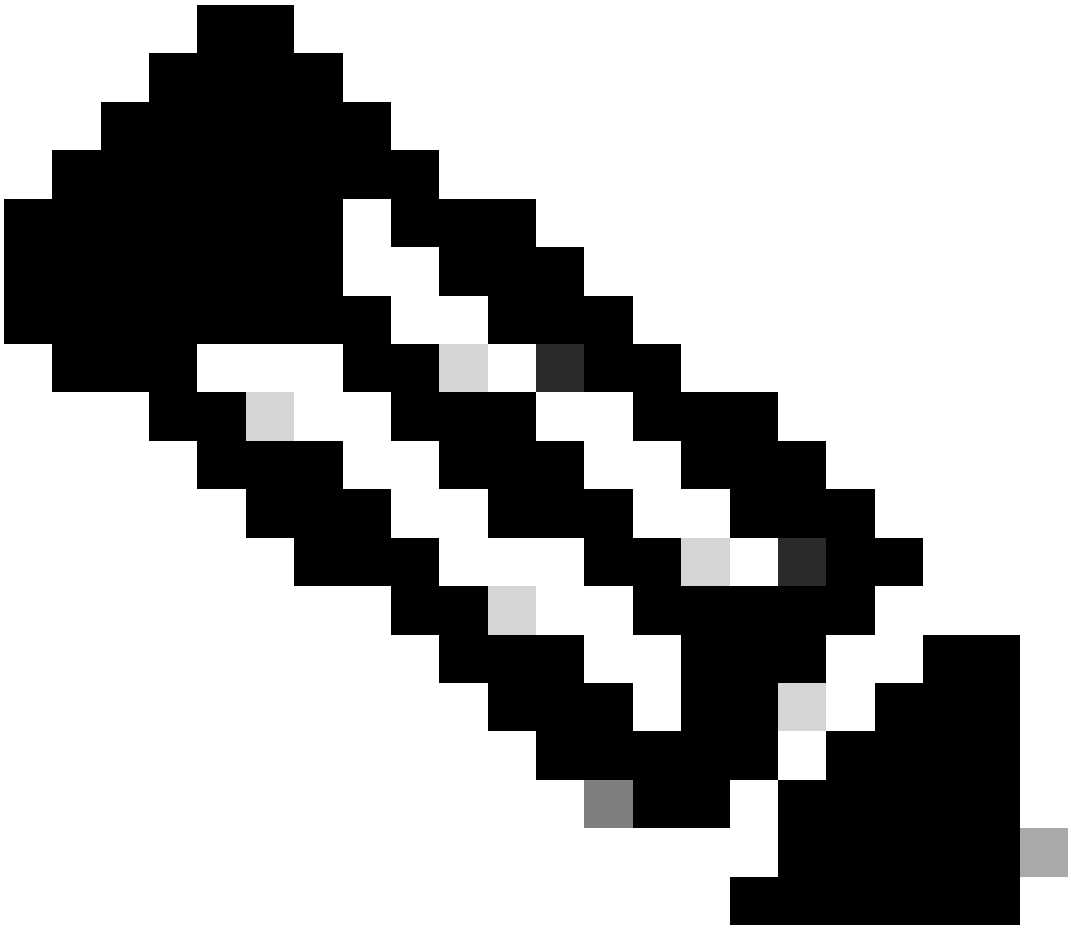
```
show aaa cache group <Server Group> all
```

Met deze opdracht worden de huidige AAA-cachegegevens weergegeven die zijn opgeslagen op de WLC. Voorbeeld van uitvoer:

```
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
...
```

Controleer of clients opnieuw verbinding kunnen maken en worden geverifieerd via de AAA-cache wanneer de AAA-server niet beschikbaar is.



Opmerking: voor PEAP-verificatie vereist het huidige ontwerp terugkerende Cisco AV-paren met de gebruikersnaam en de hash voor de referenties voor elke gebruiker tijdens de verificatie door de Radius-server.

cisco-av-pair = AS-Username=testuser

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

Elke gebruiker moet worden geconfigureerd met de AV-pair-attributen op RADIUS.

Het wachtwoord of AS-Credential-Hash moet in het NT-hash-formaat (https://codebeautify.org/ntlm-hash-generator) zijn.

Problemen oplossen

Problemen met AAA-cache en -verificatie kunnen in verschillende stappen worden opgelost:

Stap 1: Controleer AAA-cachegegevens

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

Zorg ervoor dat de verwachte clientgegevens in de cache aanwezig zijn.

Stap 2: Certificaatinstallatie en Trustpoints valideren

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

Zorg ervoor dat de certificaten correct zijn geïnstalleerd en toegewezen aan de juiste betrouwbare punten voor EAP-TLS-verificatie.

Stap 3: Verificatiemethodenlijsten bevestigen

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

Valideren dat de referentielijst van de juiste servergroep en cacheprofielen bestaat.

Stap 5: Controleer het interne spoor van RA

<#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

Referenties:

[17.18 Gids voor softwareconfiguratie]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.