AAA-Cache für TLS auf 9800 WLC verstehen und konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den AAA-Cache auf Cisco Catalyst 9800 Wireless LAN Controllern (WLC) konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- AAA-Authentifizierungskonzepte, einschließlich RADIUS- und EAP-Protokolle
- Wireless LAN Controller (WLC)-Betriebs- und Konfigurations-Workflows
- 802.1X-Authentifizierungsverfahren und Zertifikatsverwaltung
- PKI (Basic Public Key Infrastructure) und Zertifikatsignierungsprozesse

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst Wireless LAN Controller der Serie 9800
- Softwareversion 17.18.1 oder höher (AAA-Cache-Funktion wird von dieser Version unterstützt)
- Cisco Identity Services Engine (ISE) als AAA-/RADIUS-Server
- Netzwerkzugriffsgeräte mit Unterstützung von 802.1X, EAP-TLS, EAP-PEAP, MAB und iPSK

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Authentifizierungsmethoden wie 802.1X sind von der Kommunikation mit einem externen Authentifizierungsserver (z. B. einem RADIUS-Server) abhängig. Wenn der Wireless LAN

Controller (WLC) den Server nicht erreichen kann oder wenn der Server nicht verfügbar ist, können sich die Wireless-Clients nicht mit der SSID verbinden, was zu Serviceunterbrechungen führt. Der WLC blockiert den Client-Datenverkehr, bis die Authentifizierung erfolgreich ist.

Ab Version 17.18.1 ermöglicht die AAA-Cache-Funktion dem Catalyst 9800 WLC die Authentifizierung von Wireless-Clients, selbst wenn der AAA-Server nicht mehr verfügbar ist. Hierzu werden zwischengespeicherte Authentifizierungseinträge verwendet. Dadurch werden Serviceunterbrechungen bei AAA-Serverausfällen erheblich reduziert und die nahtlose Client-Verbindung aufrechterhalten.

Der AAA-Cache-Mechanismus wird unterstützt, wenn Access Points im lokalen Modus oder im FlexConnect-Modus (zentrale Authentifizierung) betrieben werden.

AAA-Cache-Funktionalität beim Cisco Catalyst 9800 WLC:

- Erstauthentifizierung (wenn AAA-Server erreichbar ist): Der WLC leitet die Client-Authentifizierungsanforderung mithilfe von RADIUS an den konfigurierten AAA-Server weiter. Sobald der Server Access-Accept zurückgibt, speichert der WLC die Details zur Client-Authentifizierung lokal in seinem AAA-Cache.
- Client-Neuverbindung (wenn AAA-Server nicht erreichbar ist): Wenn ein Client erneut eine Verbindung herstellt, bevor sein zwischengespeicherter Eintrag abläuft, ruft der WLC seinen lokalen AAA-Cache ab. Wenn gültige zwischengespeicherte Daten vorhanden sind, wird der Netzwerkzugriff gewährt, ohne den AAA-Server zu kontaktieren.
- Failover-Unterstützung: Wenn der AAA-Server aufgrund von Netzwerkproblemen oder -ausfällen nicht erreichbar ist, authentifiziert der WLC weiterhin Clients mithilfe von zwischengespeicherten Daten und stellt sicher, dass zuvor authentifizierte Benutzer einen unterbrechungsfreien Zugriff aufrechterhalten.
- Cache-Lebensdauer und -Ablauf: Die Einträge im AAA-Cache sind temporär und konfigurierbar. Die standardmäßige Cachedauer beträgt 24 Stunden. Wenn Sie den Timer auf 0 setzen, verfallen Einträge nie. Wenn ein Client nach Ablauf des Cache-Eintrags erneut eine Verbindung herstellt, versucht der WLC, den AAA-Server zur Authentifizierung zu erreichen.

```
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
```

Folgende Authentifizierungstypen werden für den AAA-Cache unterstützt:

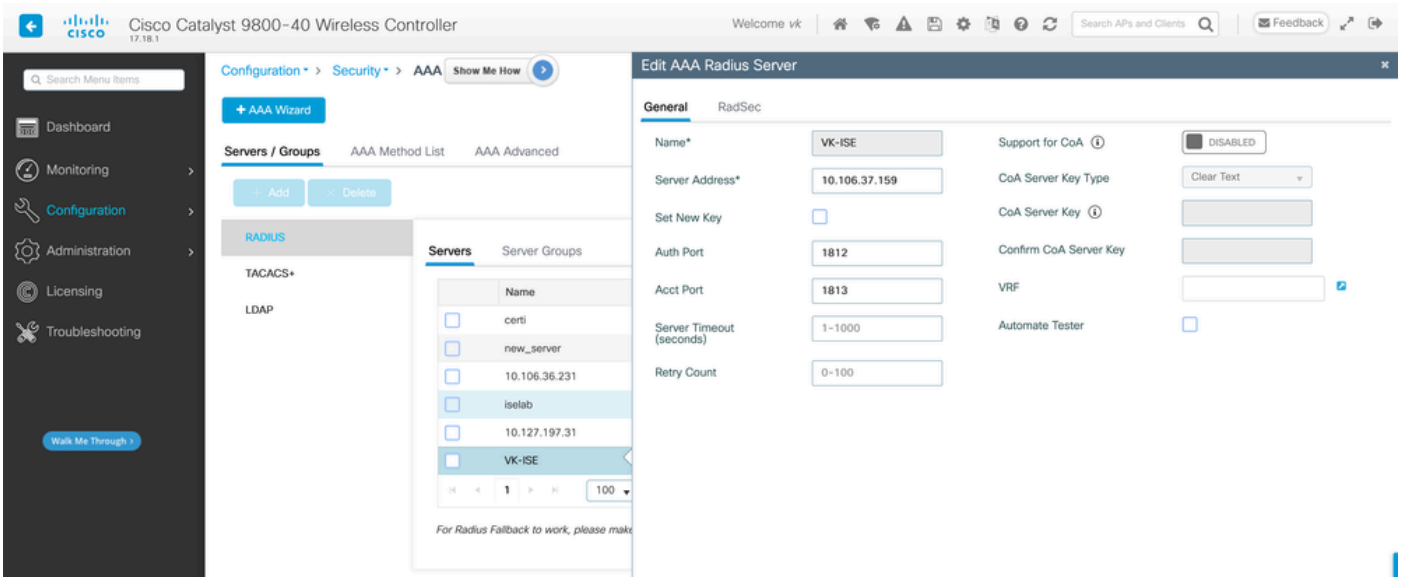
- EAP-TLS
- EAP-PEAP mit MSCHAPv2
- MAB (MAC Authentication Bypass), MAB+PSK und MAB+802.1x/iPSK

Konfigurieren

Schritt 1: AAA-Server auf WLC hinzufügen

Fügen Sie zunächst den AAA (RADIUS)-Server zum Wireless LAN Controller hinzu. Dies kann über die grafische Benutzeroberfläche oder die Kommandozeile erfolgen.

GUI-Methode: Navigieren Sie zu Configuration > Security > AAA, und fügen Sie Ihren Server hinzu.



CLI-Methode:

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

Mit diesem Befehl wird ein RADIUS-Servereintrag mit dem Namen VK-ISE mit der angegebenen IP-Adresse, dem Authentifizierungsport, dem Kontoführungsport und dem freigegebenen Schlüssel erstellt.

Phase 2: AAA-Cacheprofil erstellen (nur CLI)

Erstellen Sie ein AAA-Cacheprofil, um das Cacheverhalten zu definieren. Dieser Schritt ist nur auf die Kommandozeile beschränkt.

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

Mit diesem Befehl wird ein Cacheprofil mit dem Namen VK-CACHE erstellt und die Zwischenspeicherung für alle unterstützten Authentifizierungstypen aktiviert.

Schritt 3: Servergruppe erstellen und RADIUS-Server- und Cacheprofil zuordnen (nur CLI)

Erstellen Sie eine RADIUS-Servergruppe, ordnen Sie den AAA-Server zu, konfigurieren Sie das Ablaufdatum des Cache, und ordnen Sie Autorisierungs-/Authentifizierungsprofile zu.

```
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
```

Diese Befehlssätze:

- Erstellt eine Servergruppe mit dem Namen VK-SRV-GRP
- Verbindet den VK-ISE-Server
- Legt den Cache-Ablauf auf 8 Stunden fest
- Zuordnung von Autorisierungs- und Authentifizierungsprofilen zu VK-CACHE
- Legt die Totzeit für nicht erreichbare Server auf 5 Minuten und die Dead-Criteria für die Wiederholungslogik fest.

Schritt 4: Erstellen von Authentifizierungs- und Autorisierungsmethoden

Definieren Sie Methodenlisten für die Authentifizierung und Autorisierung, und geben Sie die Verwendung der Servergruppe und des Caches an.

```
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
```

Mit diesen Befehlen werden Standardmethodenlisten für die 802.1X-Authentifizierung und Netzwerkautorisierung eingerichtet, wobei der Cache und die Servergruppe priorisiert werden.

Wenn der WLC den Cache zuerst überprüfen soll, bevor er den RADIUS-Server startet (für eine schnellere Authentifizierung, wenn der Benutzer bereits zwischengespeichert ist), verwenden Sie Folgendes:

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

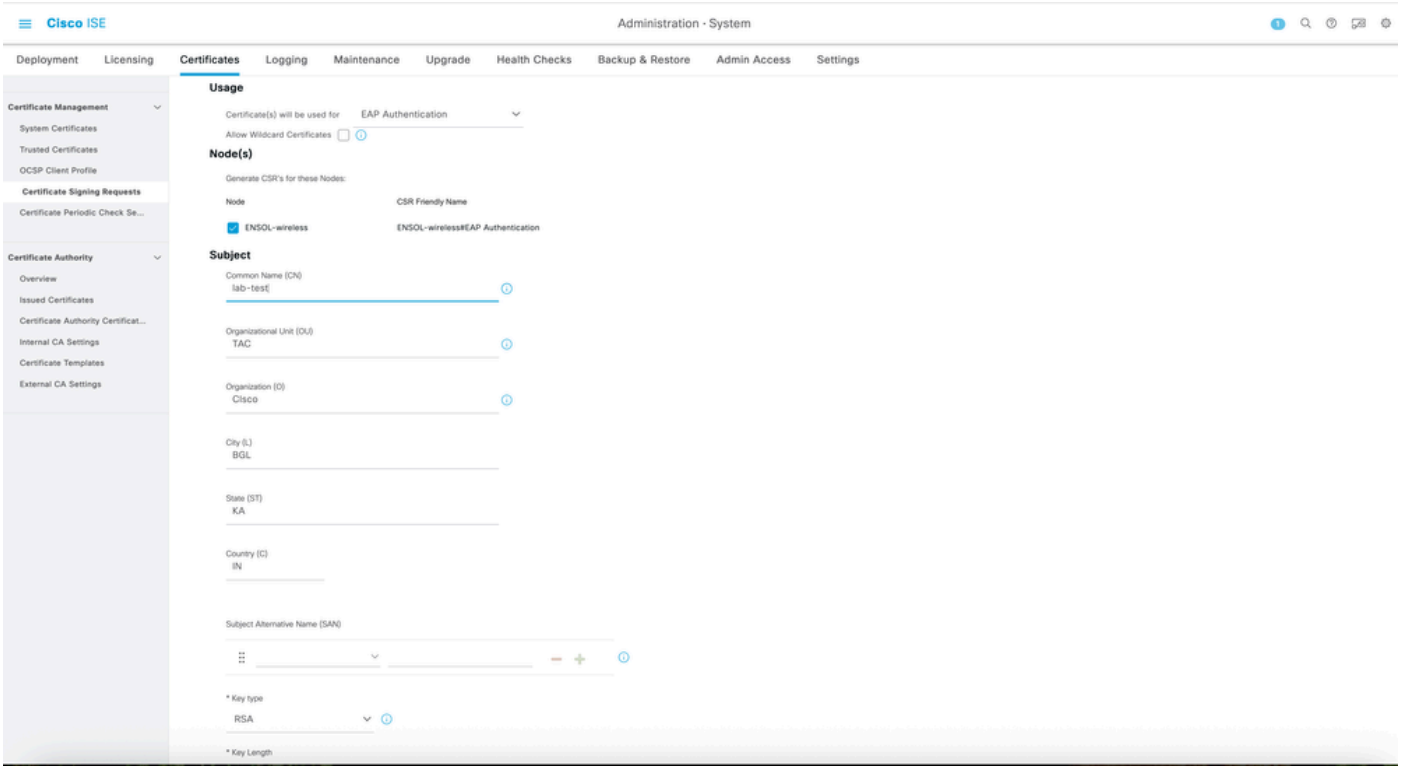
Bei diesen Methodenlisten fragt der WLC zuerst den Cache ab und kontaktiert nur dann den Server, wenn der Benutzer nicht im Cache gefunden wird. Dies führt zu einer schnelleren Authentifizierung für zwischengespeicherte Clients.

Schritt 5: Konfigurieren der TLS-Authentifizierung (Zertifikateinrichtung)

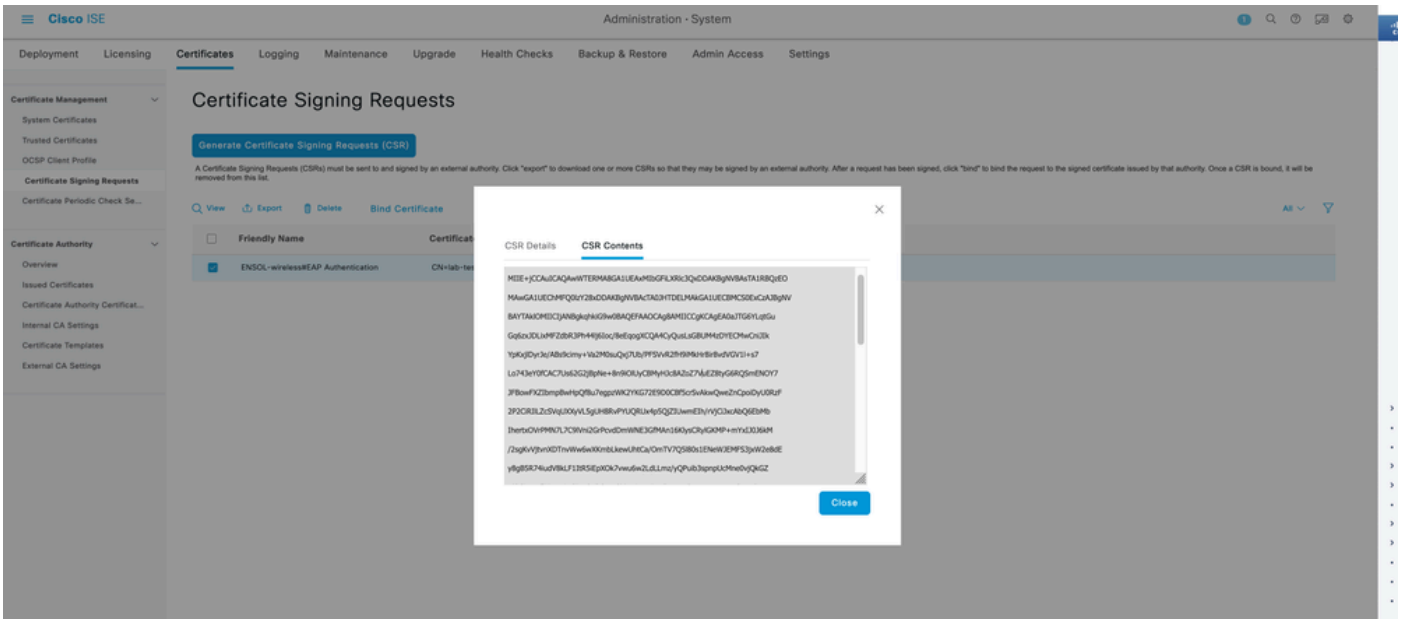
Für die EAP-TLS-Authentifizierung benötigen sowohl der WLC- als auch der AAA-Server Serverzertifikate, die von einer Zertifizierungsstelle (Certificate Authority, CA) signiert werden.

Auf der Cisco ISE (AAA-Server):

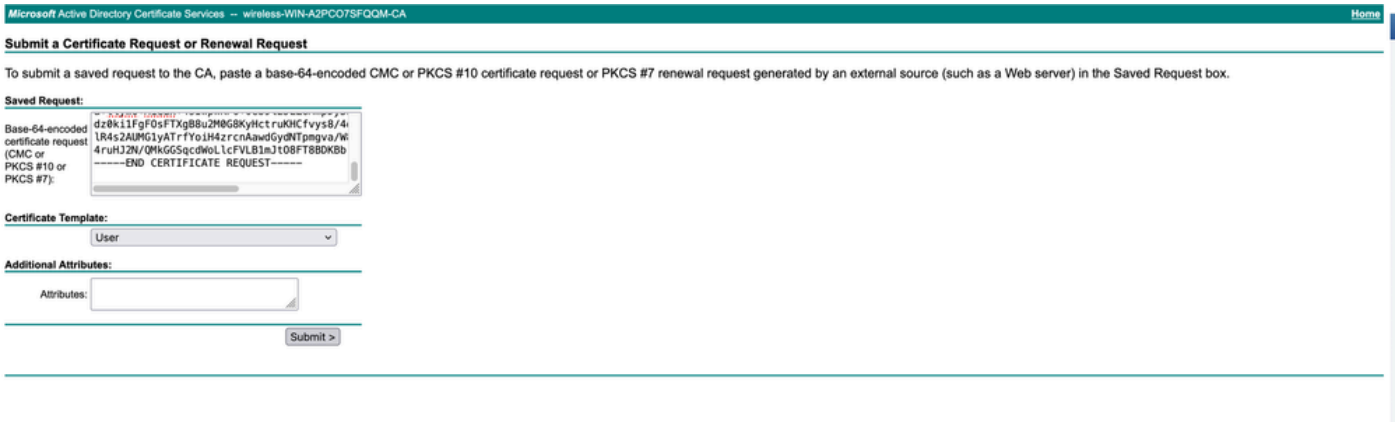
- Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR) über Zertifikate > Zertifikatsverwaltung > Zertifikatsanforderungen

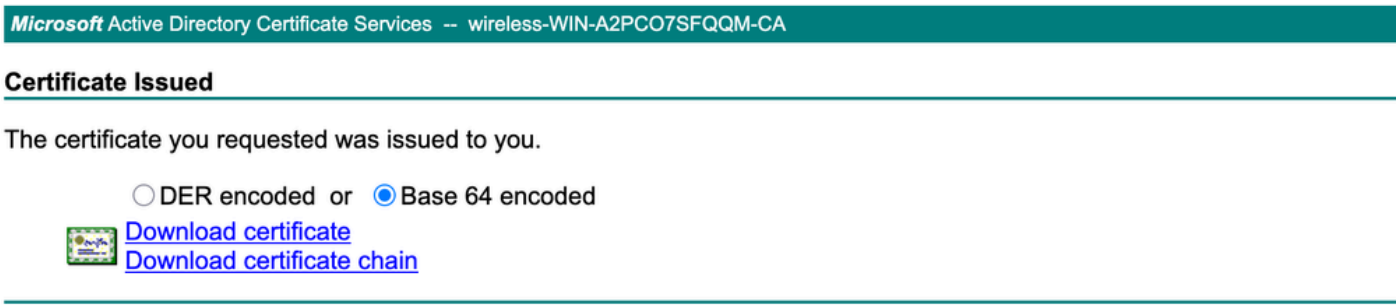


- CSR-Inhalt kopieren und von Ihrer Zertifizierungsstelle signieren lassen

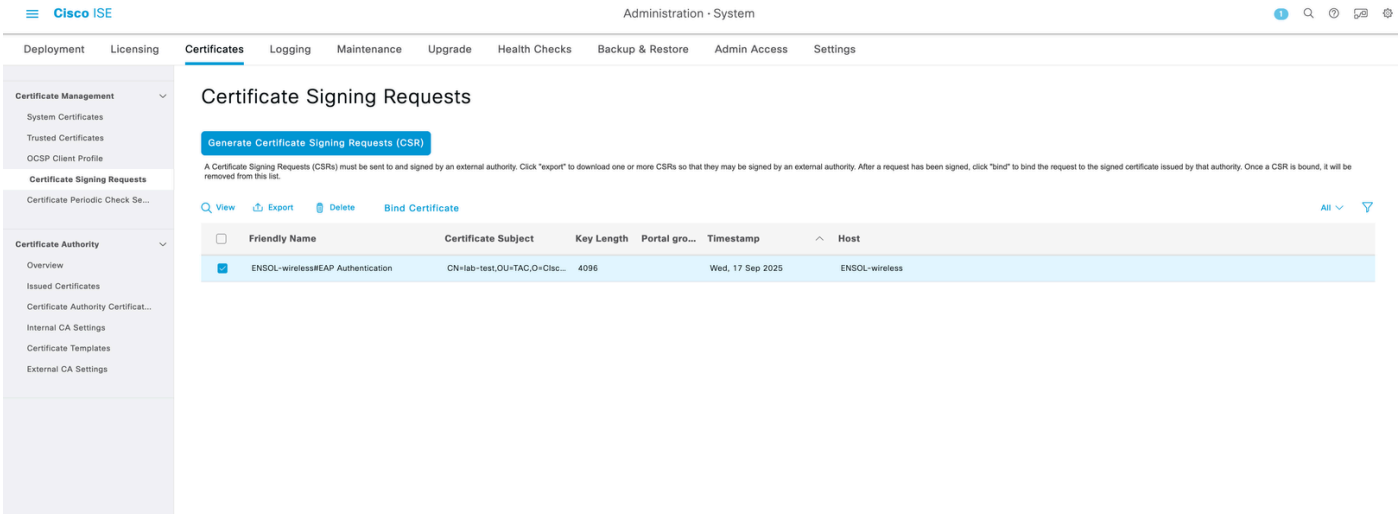


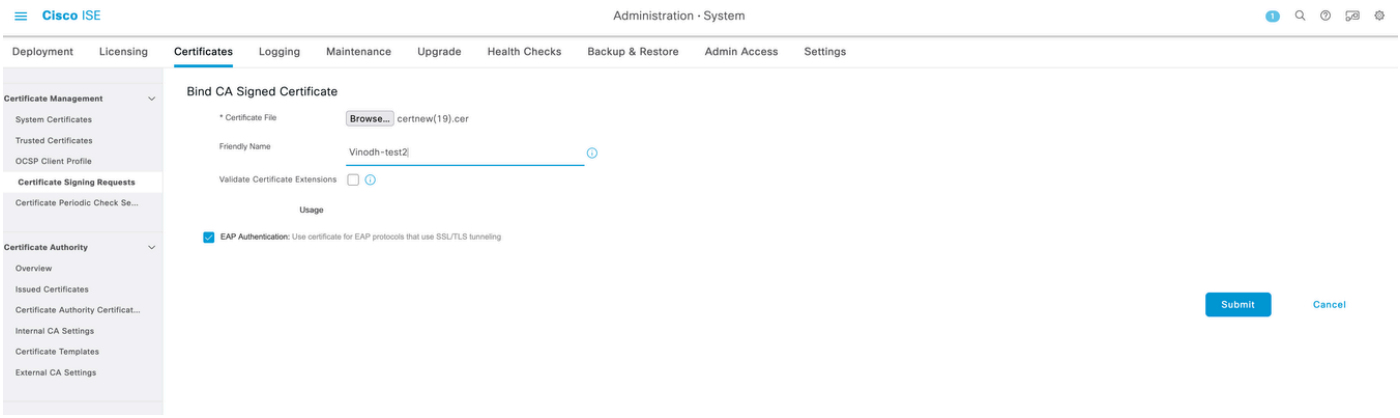
- Signiertes Zertifikat herunterladen (im Format .cer oder .pem)



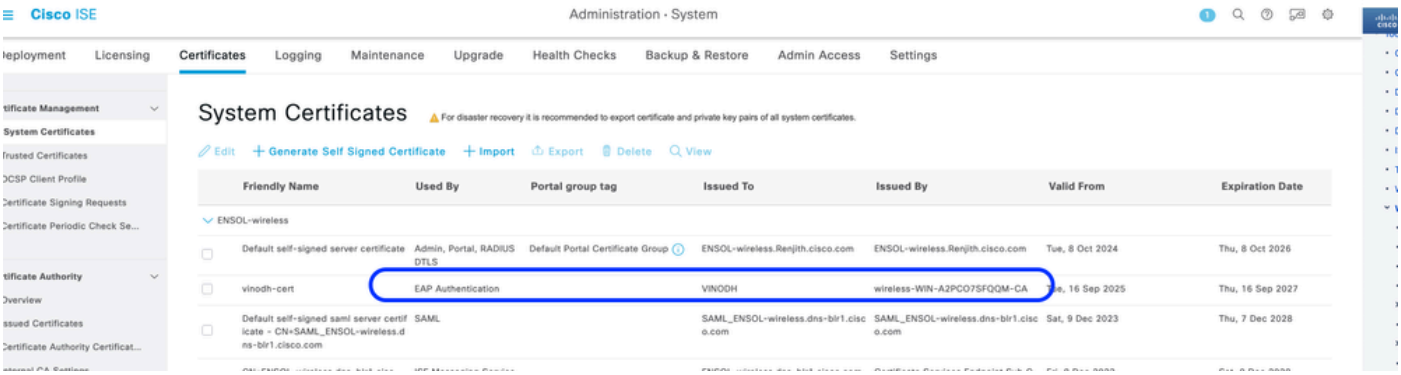


- Binden des Zertifikats an die ISE durch Navigieren zur signierten Zertifikatsdatei und Klicken auf "Senden"



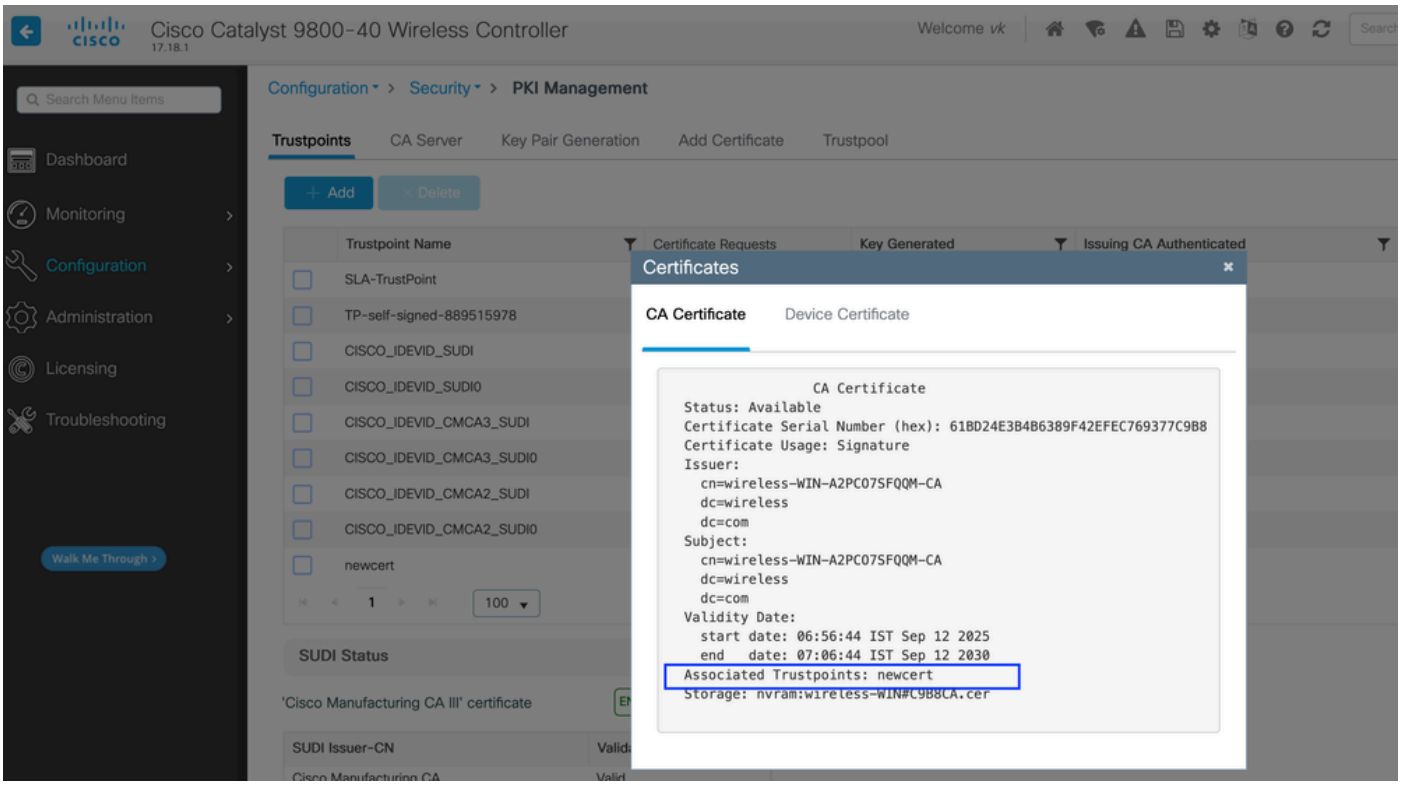


- Stellen Sie sicher, dass das signierte Zertifikat unter dem Systemzertifikat für die EAP-Authentifizierung aufgeführt ist.



Für den Cisco Catalyst 9800 WLC:

- Erstellen einer CSR-Anfrage auf dem WLC
- CSR von derselben Zertifizierungsstelle signieren lassen, die auch für die ISE verwendet wird
- Signiertes Zertifikat in den WLC hochladen



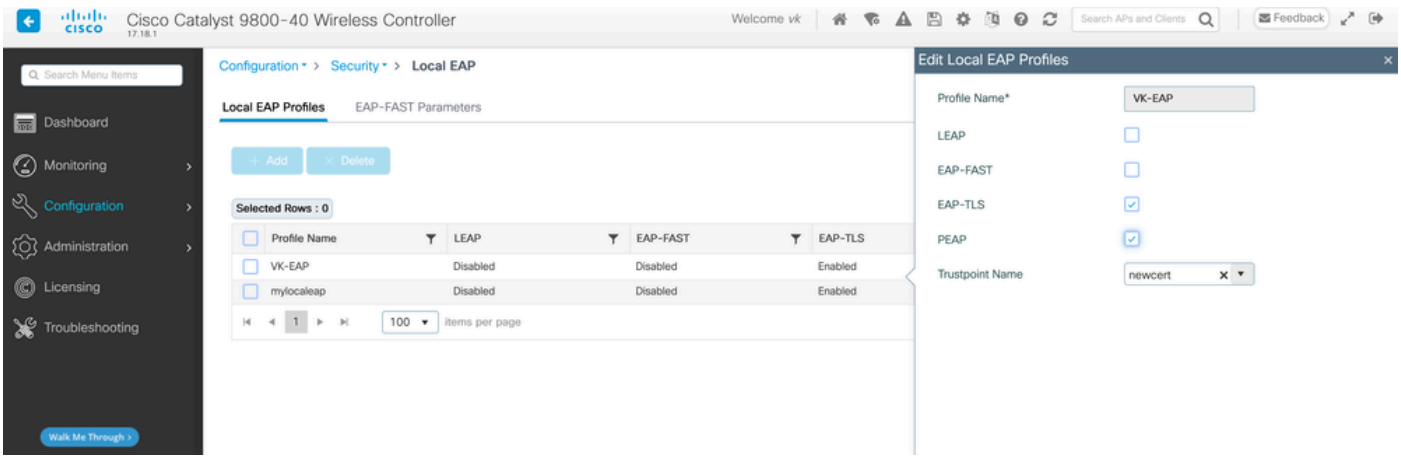
Schritt 6: Lokales EAP-Profil erstellen und Vertrauenspunkt zuordnen

Erstellen Sie ein lokales EAP-Profil, und ordnen Sie den Vertrauenspunkt für die EAP-TLS-Authentifizierung zu.

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

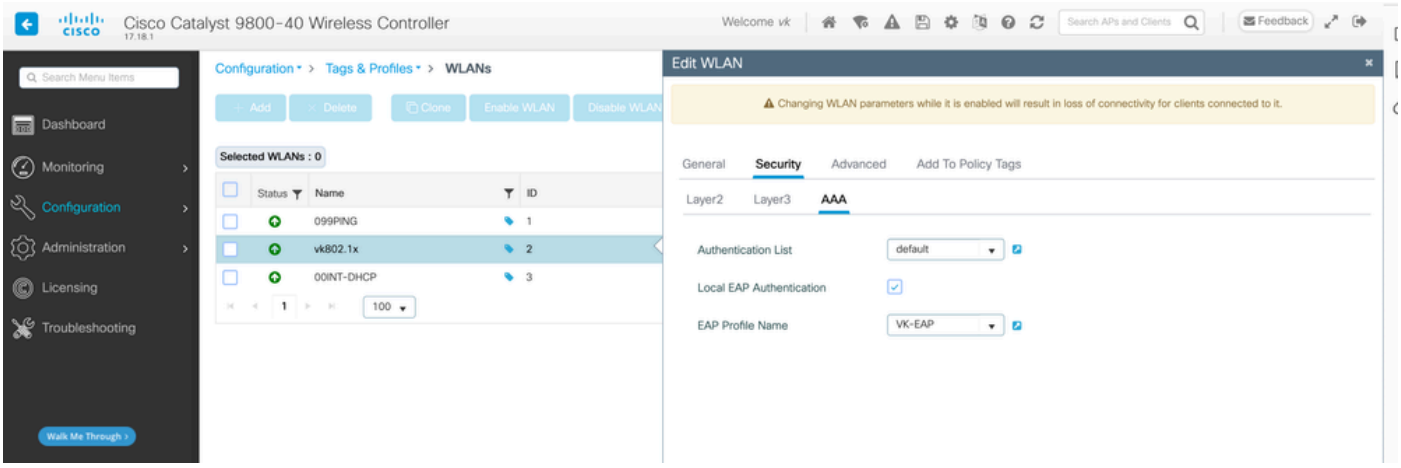
Mit diesem Befehl wird ein EAP-Profil mit dem Namen VK-EAP unter Verwendung von EAP-TLS erstellt, und der Vertrauenspunkt wird dem Zertifikat mit dem Namen newcert zugeordnet.

GUI-Methode: Navigieren Sie zu Configuration > Security > Local EAP, und erstellen Sie das EAP-Profil.



Schritt 7: Methodenliste und EAP-Profil auf SSID anwenden

Konfigurieren Sie Ihre SSID so, dass sie das erstellte Authentifizierungs- und EAP-Profil verwendet.



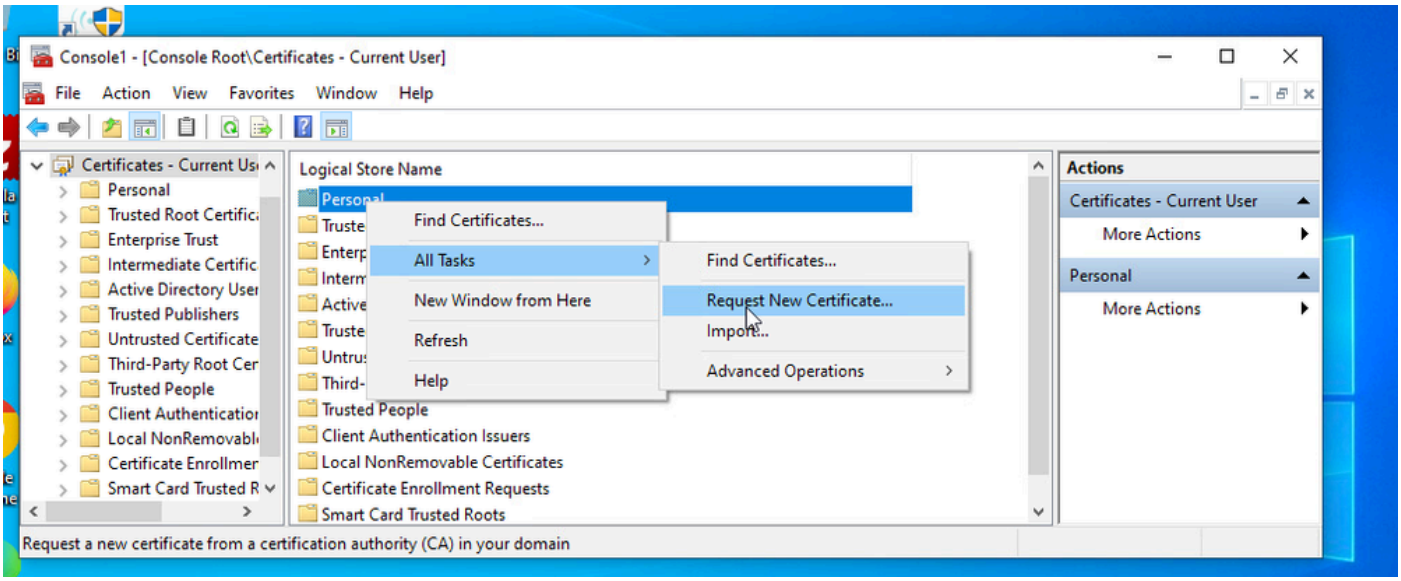

```
wlan vk802.1x 2 vk802.1x
 local-auth VK-EAP
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 security dot1x authentication-list default
 no shutdown
```

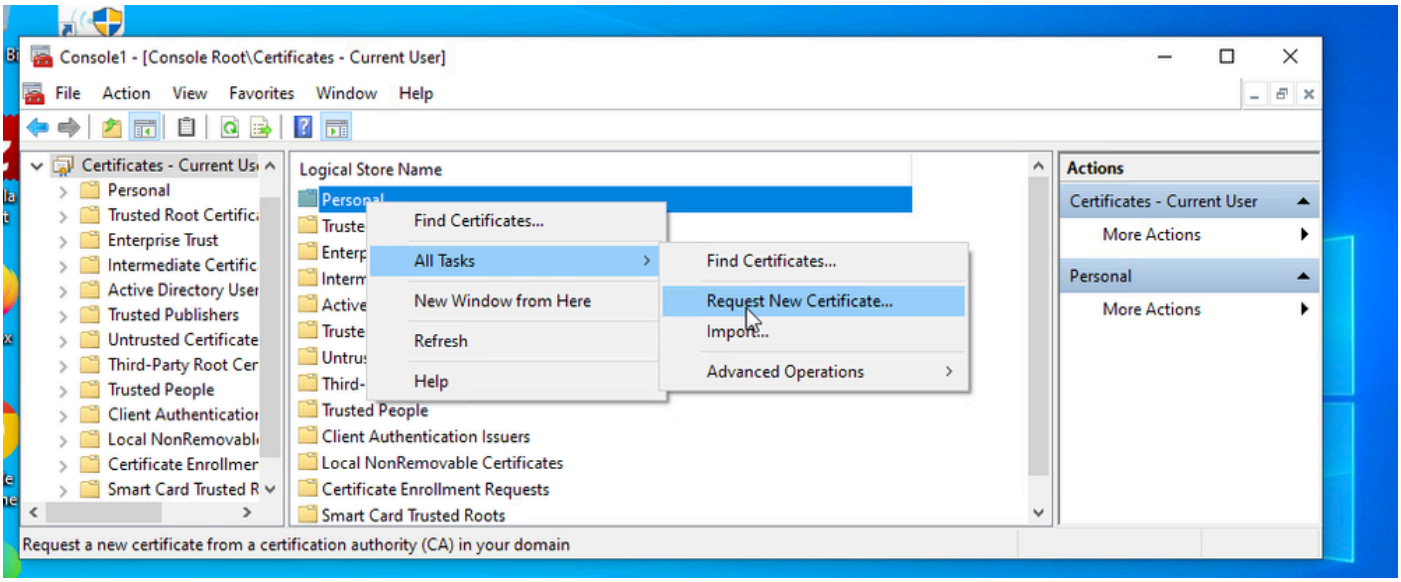
Diese Konfiguration:

- Erstellt SSID vk802.1x mit WLAN-ID 2
- Aktiviert die lokale Authentifizierung mithilfe des VK-EAP-Profils
- Anwendung von Funkrichtlinien für 2,4-GHz- und 5-GHz-Frequenzbänder
- Erzwingt 802.1X-Authentifizierung mithilfe der Standardmethodenliste
- SSID aktivieren (kein Herunterfahren)

Schritt 8: Bereitstellung von Benutzerzertifikaten auf Wireless-Clients

Stellen Sie sicher, dass Wireless-Clients über das für die Authentifizierung erforderliche Benutzerzertifikat verfügen. In Laborumgebungen kann ein Gerät, das einer Active Directory (AD)-Domäne angehört, das Zertifikat über MMC (Microsoft Management Console) empfangen. Je nach Ihrer Umgebung gibt es auch andere Methoden zur Verteilung von Zertifikaten.





Überprüfung

Sie können die AAA-Cacheeinträge des 9800 WLC mithilfe von CLI-Befehlen überprüfen. Beachten Sie, dass bei Catalyst 9800 WLCs die Cache-Einträge unter "WNCD AAA Auth Cache-Einträge" und nicht unter "SMD AAA Auth Cache-Einträge" aufgeführt sind.

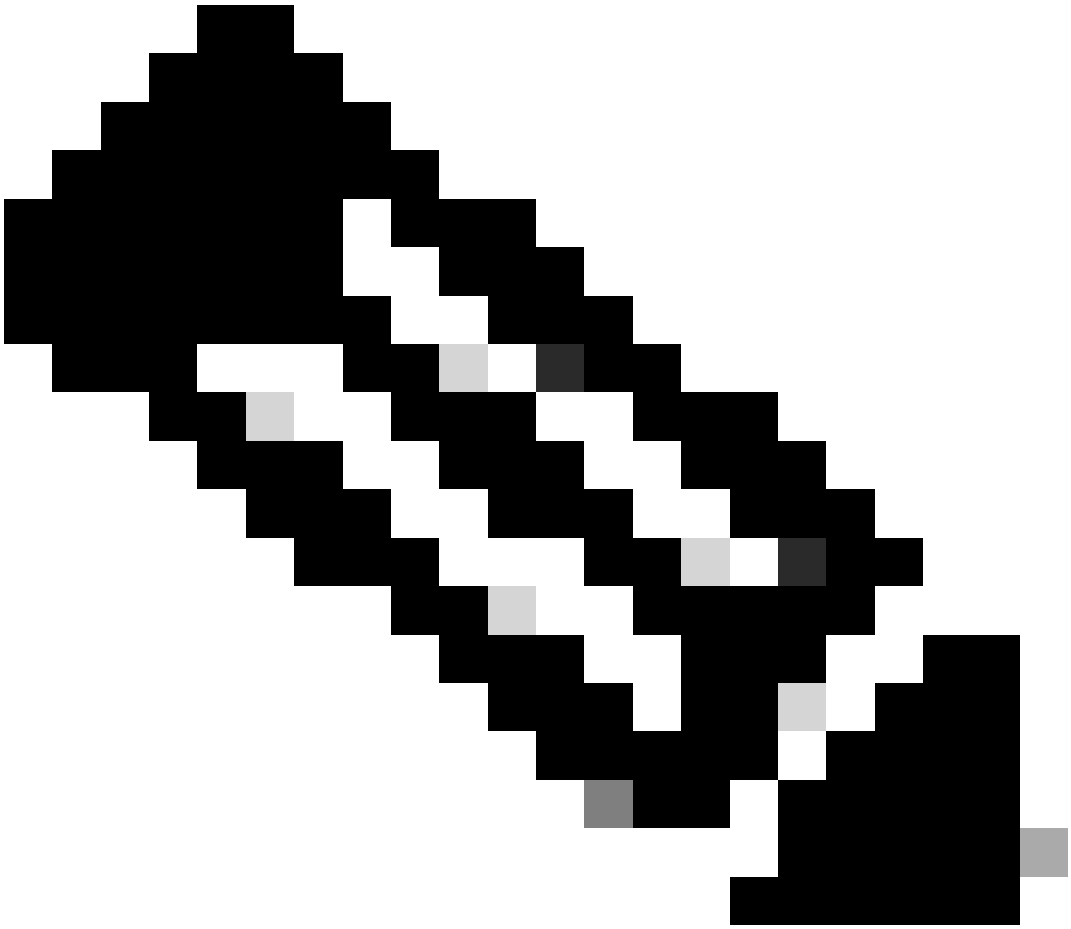
```
show aaa cache group <Server Group> all
```

Mit diesem Befehl werden die aktuellen AAA-Cacheeinträge angezeigt, die auf dem WLC gespeichert sind. Beispiel:

```
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
...
```

Stellen Sie sicher, dass Clients erneut eine Verbindung herstellen können und über den AAA-Cache authentifiziert werden, wenn der AAA-Server nicht verfügbar ist.



Anmerkung: Für die PEAP-Authentifizierung erfordert das vorliegende Design die Rückgabe von Cisco AV-Paaren, die den Benutzernamen und den Credential Hash für jeden Benutzer während der Authentifizierung durch den Radius-Server enthalten.

cisco-av-pair = AS-Username=testuser

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

Jeder Benutzer muss mit den AV-pair-Attributen auf RADIUS konfiguriert werden.

Das Kennwort oder der AS-Credential-Hash muss das NT-Hash-Format haben (https://codebeautify.org/ntlm-hash-generator).

Fehlerbehebung

Die Fehlerbehebung bei AAA-Cache- und Authentifizierungsproblemen umfasst mehrere Schritte:

Schritt 1: AAA-Cacheeinträge überprüfen

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

Stellen Sie sicher, dass die erwarteten Clienteinträge im Cache vorhanden sind.

Phase 2: Überprüfen der Zertifikatinstallation und der Vertrauenspunkte

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

Stellen Sie sicher, dass die Zertifikate richtig installiert und den richtigen Vertrauenspunkten für die EAP-TLS-Authentifizierung zugeordnet sind.

Schritt 3: Authentifizierungsmethodenlisten bestätigen

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

Überprüfen Sie, ob diese Methodenlisten auf die richtige Servergruppe und die richtigen Cacheprofile verweisen.

Schritt 5: Interne RA-Ablaufverfolgung überprüfen

<#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
```

Referenzen:

[17.18 Software-Konfigurationsleitfaden]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.