Comprendre et configurer le cache AAA pour TLS sur le WLC 9800

Table des matières

Introduction

Ce document décrit comment comprendre et configurer le cache AAA sur les contrôleurs LAN sans fil (WLC) Cisco Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Concepts d'authentification AAA, y compris les protocoles RADIUS et EAP
- Workflows d'exploitation et de configuration du contrôleur LAN sans fil (WLC)
- Méthodes d'authentification 802.1X et gestion des certificats
- Infrastructure à clé publique (PKI) de base et processus de signature de certificats

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur LAN sans fil Cisco Catalyst 9800
- Logiciel version 17.18.1 ou ultérieure (fonctionnalité de cache AAA prise en charge à partir de cette version)
- Cisco Identity Services Engine (ISE) en tant que serveur AAA/RADIUS
- Périphériques d'accès réseau prenant en charge 802.1X, EAP-TLS, EAP-PEAP, MAB et 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les méthodes d'authentification telles que 802.1X dépendent de la communication avec un serveur d'authentification externe (tel qu'un serveur RADIUS). Lorsque le contrôleur LAN sans fil (WLC) ne peut pas atteindre le serveur ou lorsque le serveur n'est pas disponible, les clients sans

fil ne peuvent pas se connecter au SSID, ce qui entraîne des interruptions de service. Le WLC bloque le trafic client jusqu'à ce que l'authentification réussisse.

À partir de la version 17.18.1, la fonctionnalité de cache AAA permet au WLC Catalyst 9800 d'authentifier les clients sans fil même si le serveur AAA devient indisponible à l'aide d'entrées d'authentification mises en cache. Cela réduit considérablement les interruptions de service pendant les pannes de serveur AAA et maintient une connectivité client transparente.

Le mécanisme de cache AAA est pris en charge lorsque les points d'accès fonctionnent en mode local ou en mode FlexConnect (authentification centrale).

Fonctionnalité de cache AAA sur le WLC Cisco Catalyst 9800 :

- Authentification initiale (lorsque le serveur AAA est accessible) : Le WLC transfère la demande d'authentification du client au serveur AAA configuré à l'aide de RADIUS. Une fois que le serveur retourne Access-Accept, le WLC stocke les détails d'authentification du client localement dans son cache AAA.
- Reconnexion du client (lorsque le serveur AAA est inaccessible) : Si un client se reconnecte avant l'expiration de son entrée mise en cache, le WLC consulte son cache AAA local. S'il existe des données en cache valides, l'accès au réseau est accordé sans contacter le serveur AAA.
- Prise en charge du basculement : Si le serveur AAA est inaccessible en raison de problèmes réseau ou d'une défaillance, le WLC continue d'authentifier les clients à l'aide des données mises en cache, en s'assurant que les utilisateurs précédemment authentifiés conservent un accès ininterrompu.
- Durée et expiration du cache : Les entrées du cache AAA sont temporaires et configurables. La durée du cache par défaut est de 24 heures ; en définissant le minuteur sur 0, faites en sorte que les entrées n'expirent jamais. Si un client se reconnecte après l'expiration de son entrée de cache, le WLC tente d'atteindre le serveur AAA pour l'authentification.

```
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
```

Les types d'authentification pris en charge pour le cache AAA incluent :

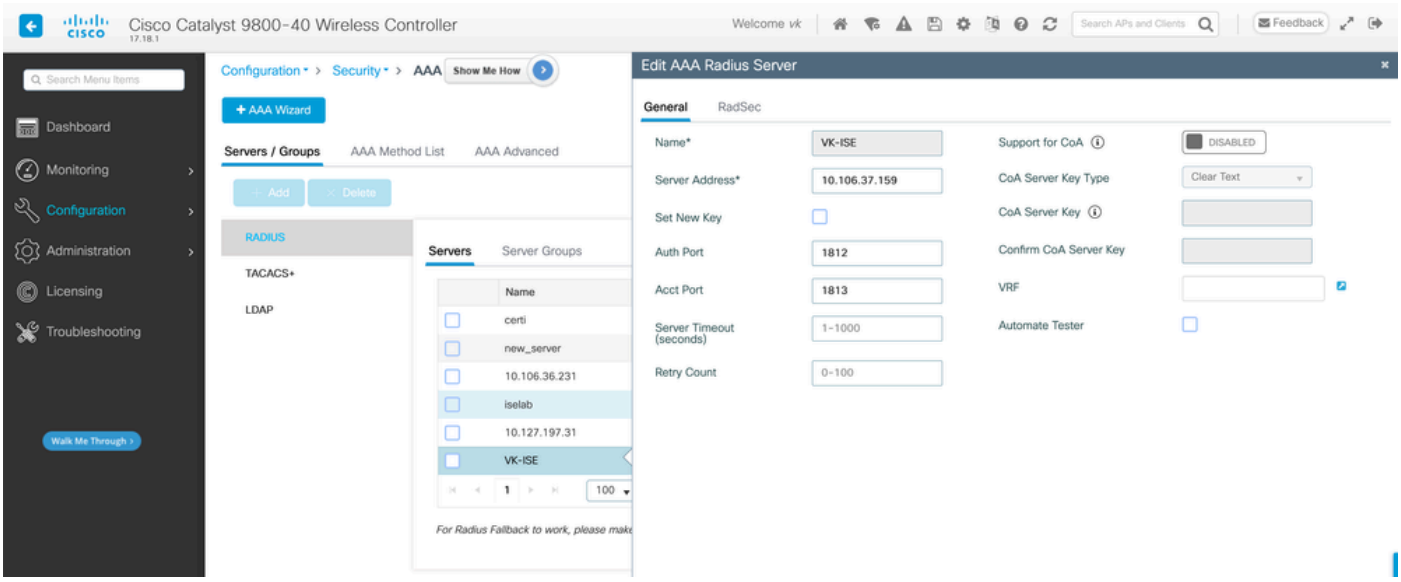
- EAP-TLS
- EAP-PEAP avec MSCHAPv2
- MAC Authentication Bypass (MAB), MAB+PSK et MAB+802.1x/iPSK

Configurer

Étape 1 : Ajouter un serveur AAA sur WLC

Commencez par ajouter votre serveur AAA (RADIUS) au contrôleur LAN sans fil. Vous pouvez le faire via l'interface graphique ou l'interface de ligne de commande.

Méthode GUI : Accédez à Configuration > Security > AAA et ajoutez votre serveur.



Méthode CLI :

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

Cette commande crée une entrée de serveur RADIUS nommée VK-ISE avec l'adresse IP, le port d'authentification, le port de comptabilité et la clé partagée spécifiés.

Étape 2 : Créer un profil de cache AAA (CLI uniquement)

Créez un profil de cache AAA pour définir le comportement du cache. Cette étape est en mode CLI uniquement.

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

Cette commande crée un profil de cache nommé VK-CACHE et active la mise en cache pour tous les types d'authentification pris en charge.

Étape 3 : Créer un groupe de serveurs et mapper un serveur RADIUS et un profil de cache (CLI uniquement)

Créez un groupe de serveurs RADIUS, associez le serveur AAA, configurez l'expiration du cache et mappez les profils d'autorisation/d'authentification.

```
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
```

Cet ensemble de commandes :

- Crée un groupe de serveurs nommé VK-SRV-GRP
- Associe le serveur VK-ISE
- Définit l'expiration du cache à 8 heures
- Mappe les profils d'autorisation et d'authentification à VK-CACHE
- Définit le délai d'attente pour les serveurs inaccessibles à 5 minutes et les critères d'arrêt pour la logique de nouvelle tentative

Étape 4 : Créer des méthodes d'authentification et d'autorisation

Définissez les listes de méthodes d'authentification et d'autorisation, en spécifiant l'utilisation du groupe de serveurs et du 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
```

Ces commandes configurent des listes de méthodes par défaut pour l'authentification 802.1X et l'autorisation réseau, en donnant la priorité au cache et au groupe de serveurs.

Si vous voulez que le WLC vérifie d'abord le cache avant d'essayer le serveur RADIUS (pour une

authentification plus rapide si l'utilisateur est déjà mis en cache), utilisez :

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

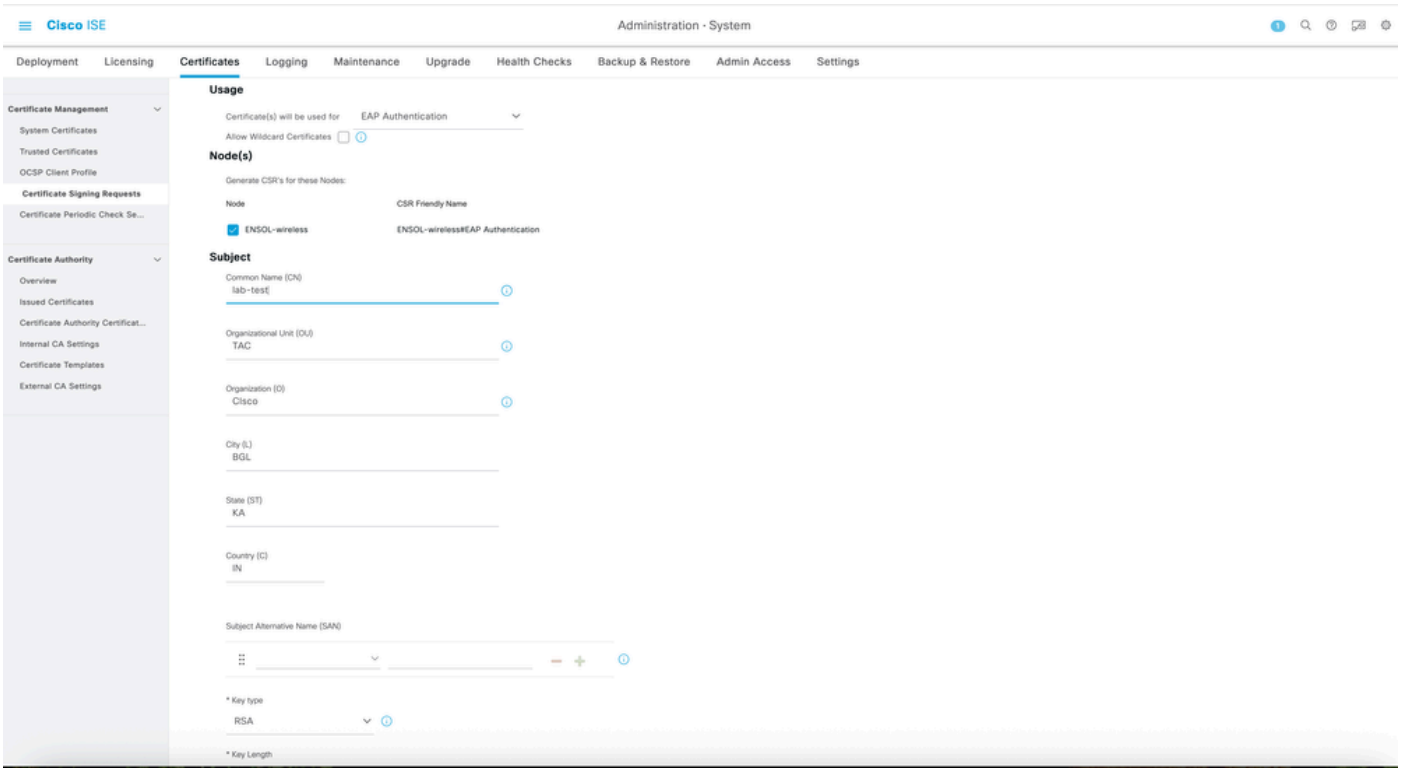
Avec ces listes de méthodes, le WLC consulte d'abord le cache, contactant seulement le serveur si l'utilisateur n'est pas trouvé dans le cache, ce qui entraîne une authentification plus rapide pour les clients mis en cache.

Étape 5 : Configurer l'authentification TLS (configuration du certificat)

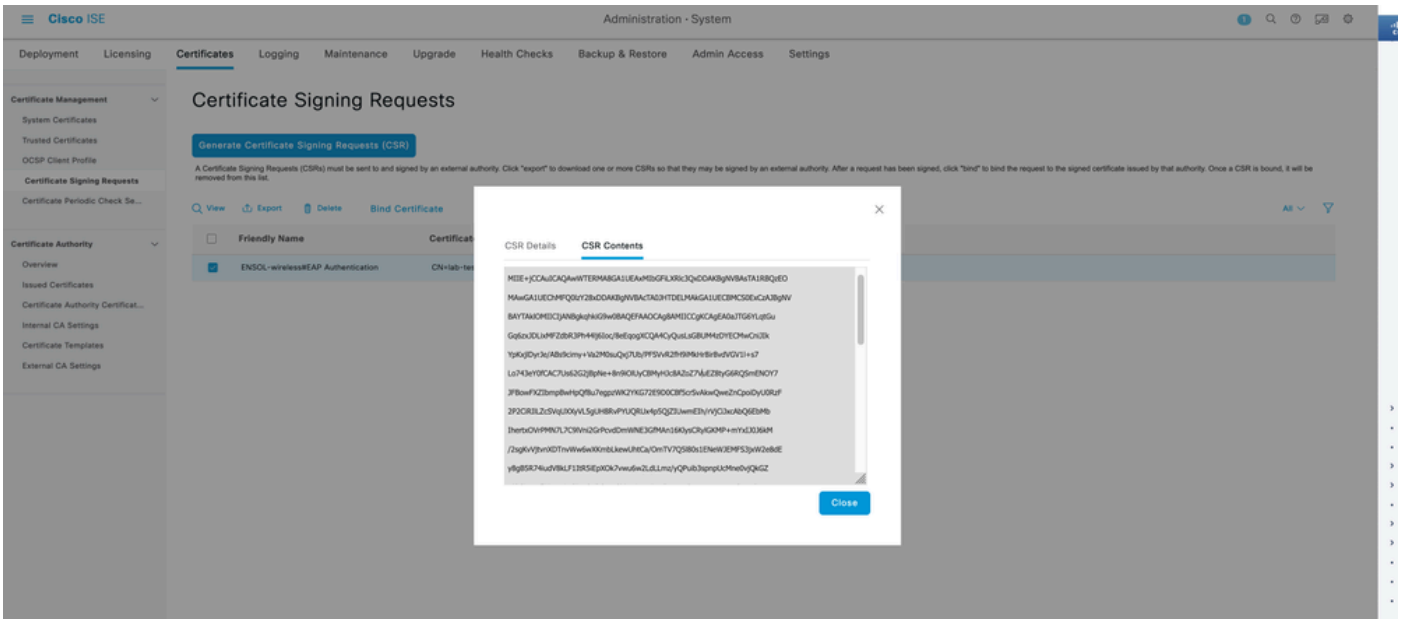
Pour l'authentification EAP-TLS, le WLC et le serveur AAA nécessitent tous deux des certificats de serveur signés par une autorité de certification (CA).

Sur Cisco ISE (serveur AAA) :

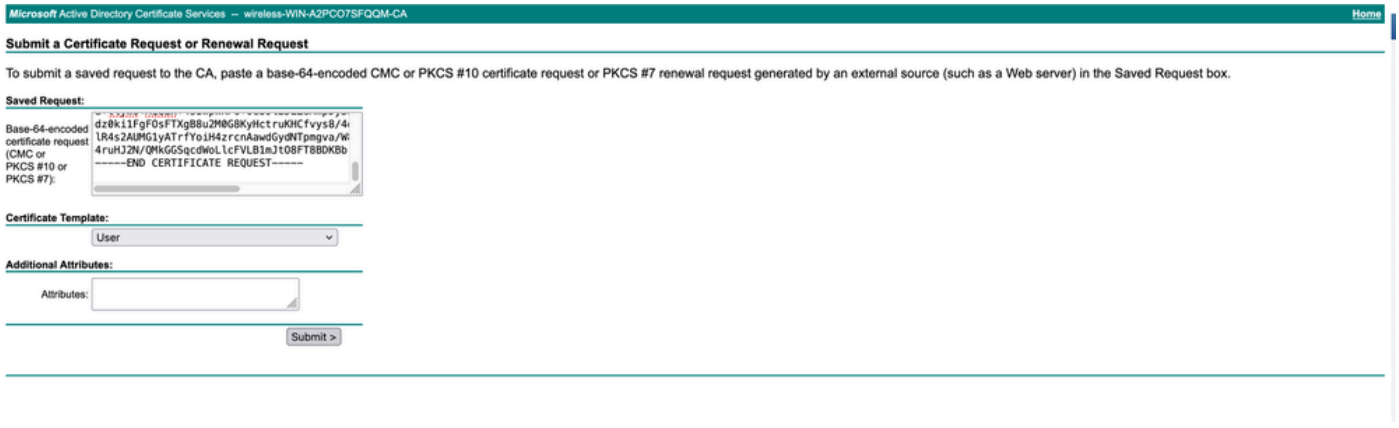
- Générer une demande de signature de certificat (CSR) via Certificats > Gestion des certificats > Demandes de signature de certificat



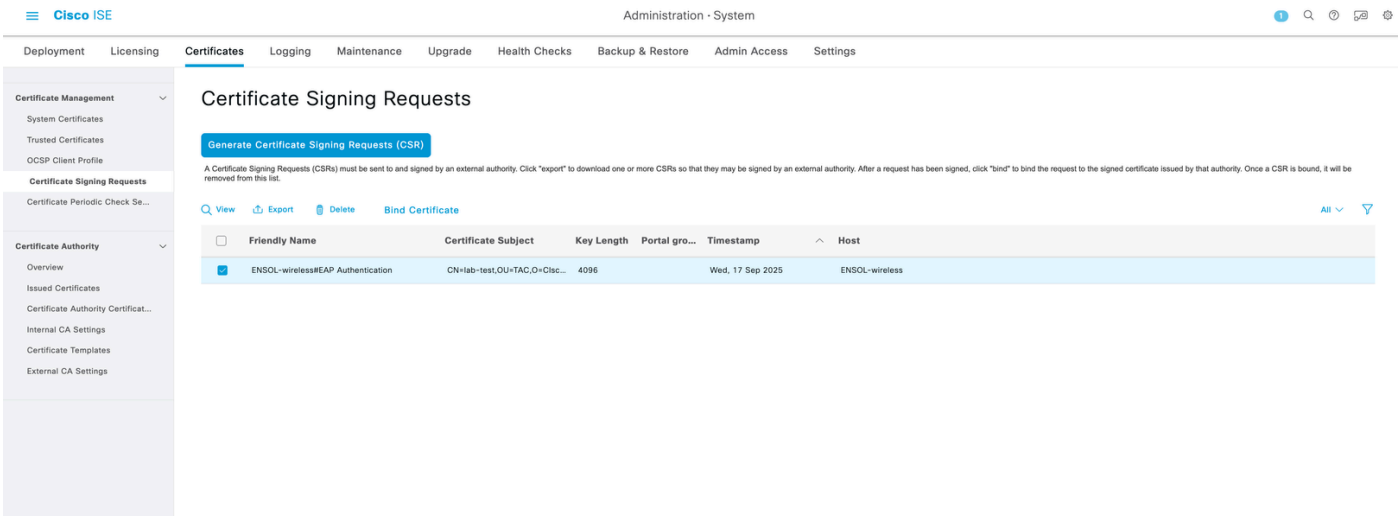
- Copiez le contenu CSR et faites-le signer par votre CA

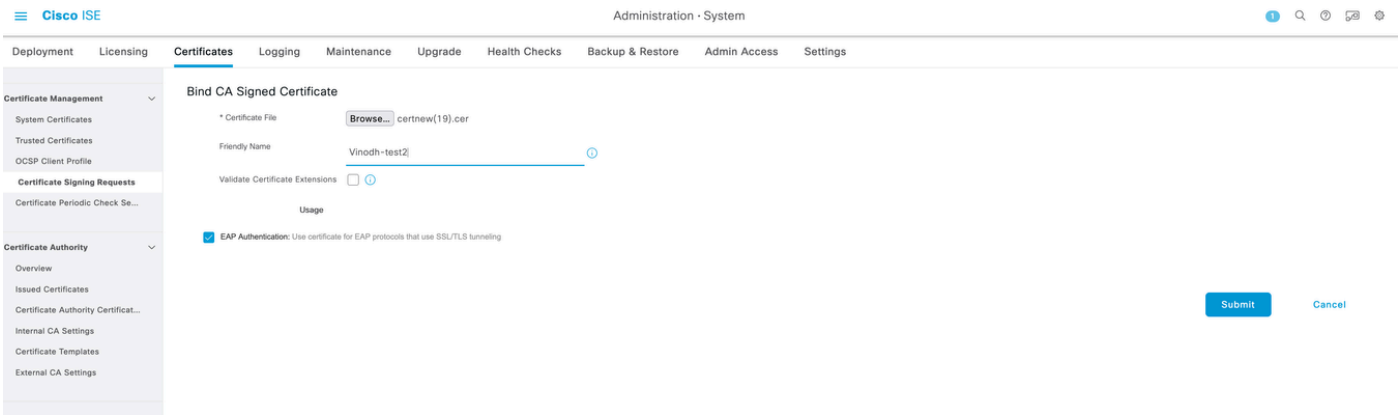


- Téléchargez le certificat signé (au format .cer ou .pem)

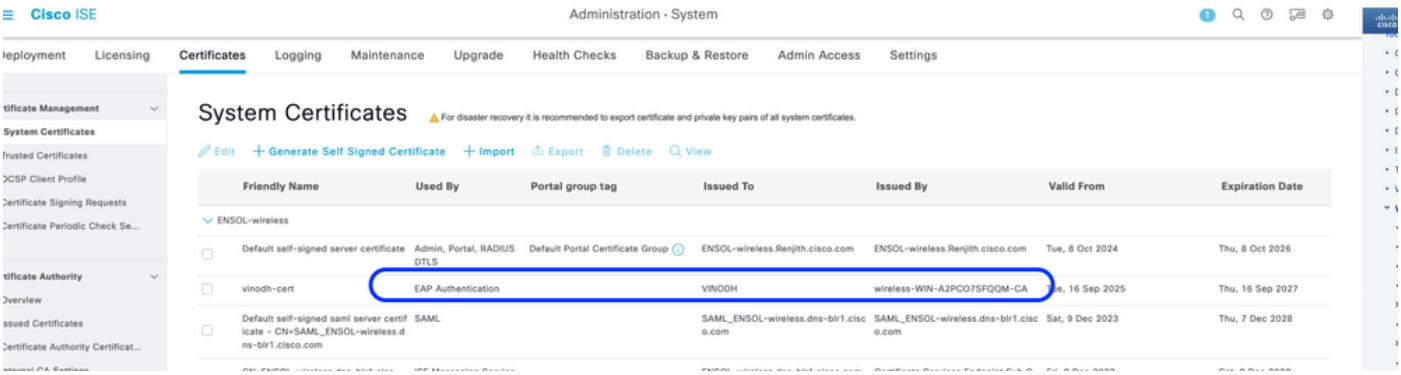


- Liez le certificat sur ISE en accédant au fichier de certificat signé et en cliquant sur « Envoyer »



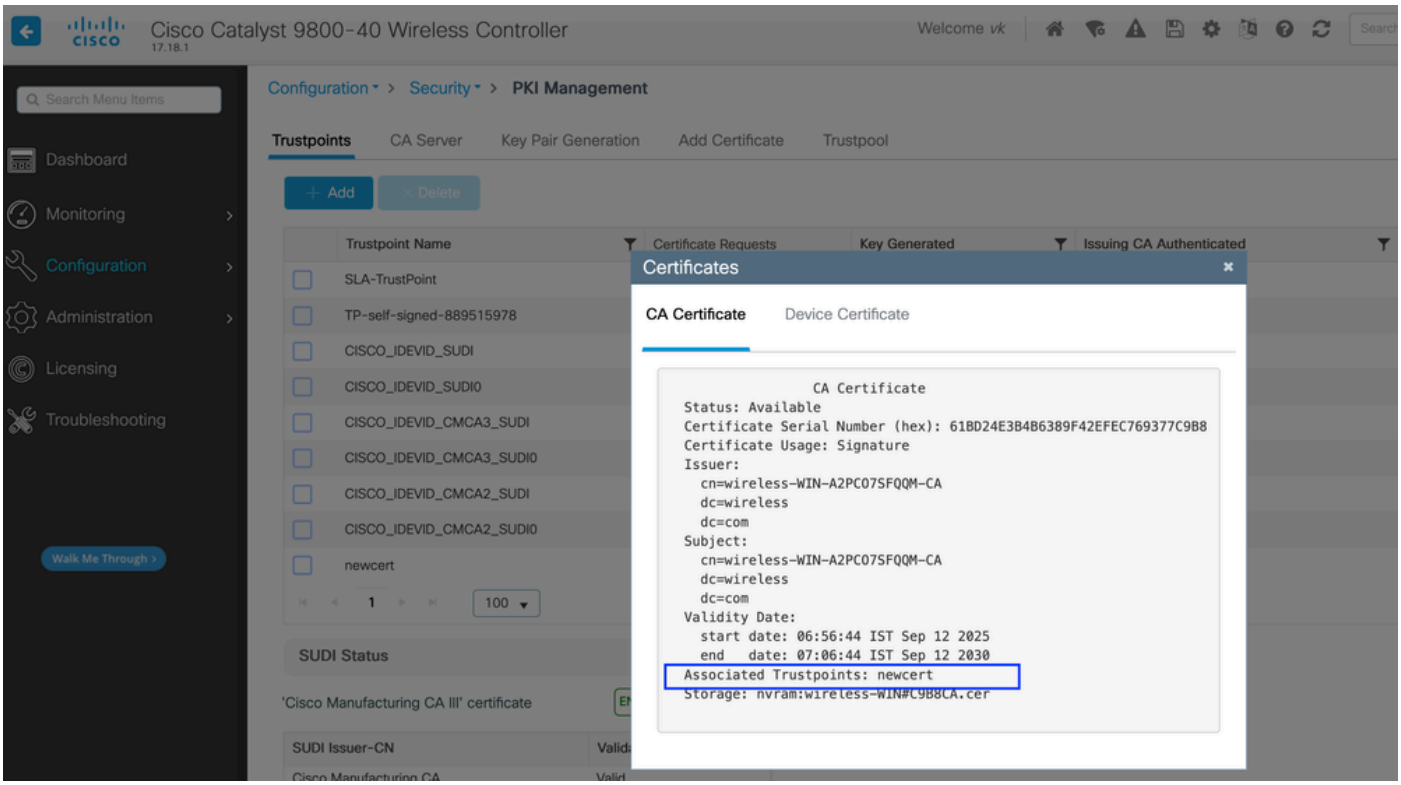


- Assurez-vous que le certificat signé est reflété sous le certificat système pour l'authentification EAP



Sur le WLC Cisco Catalyst 9800 :

- Générer un CSR sur le WLC
- Obtenez la signature CSR par la même CA que celle utilisée pour ISE
- Télécharger le certificat signé sur le WLC



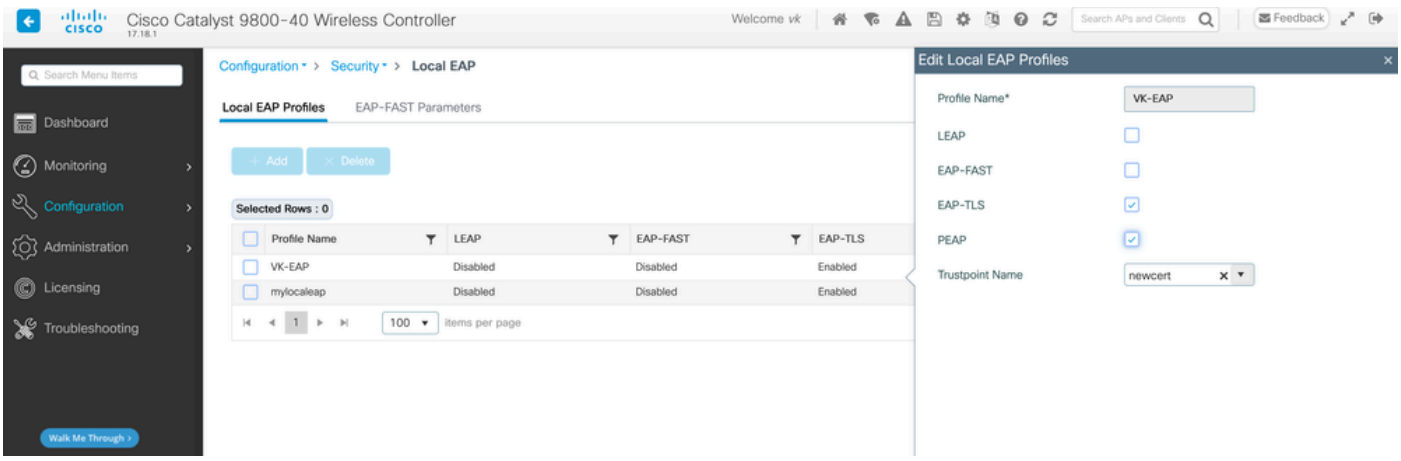
Étape 6 : Créer un profil EAP local et mapper le point de confiance

Créez un profil EAP local et mappez le point de confiance pour l'authentification EAP-TLS.

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

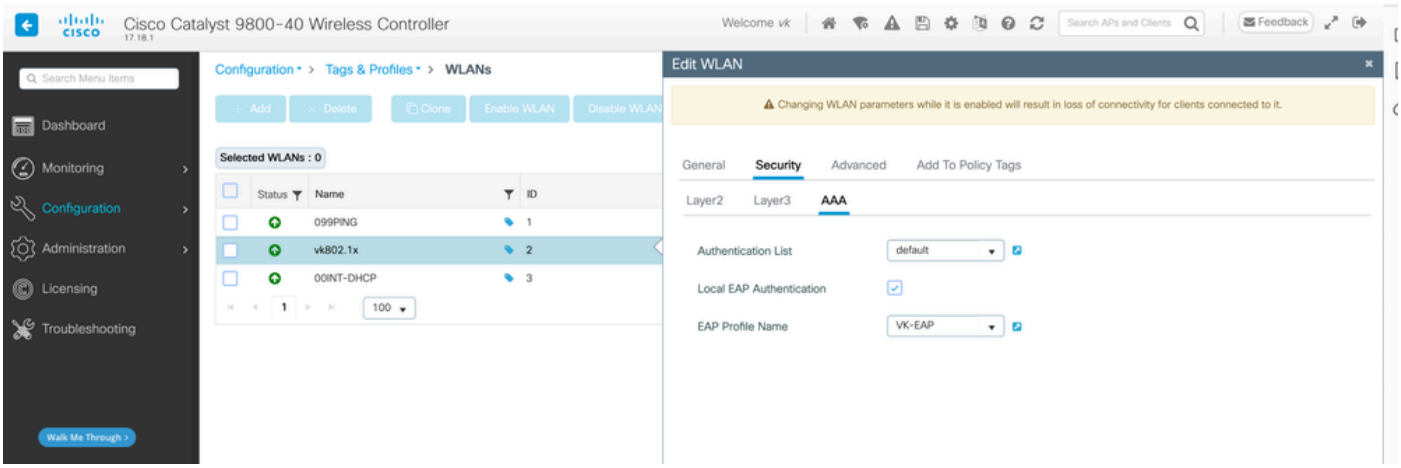
Cette commande crée un profil EAP nommé VK-EAP en utilisant EAP-TLS et mappe le point de confiance au certificat nommé newcert.

Méthode GUI : Accédez à Configuration > Security > Local EAP et créez le profil EAP.



Étape 7 : Appliquer la liste de méthodes et le profil EAP au SSID

Configurez votre SSID pour utiliser l'authentification et le profil EAP créés.



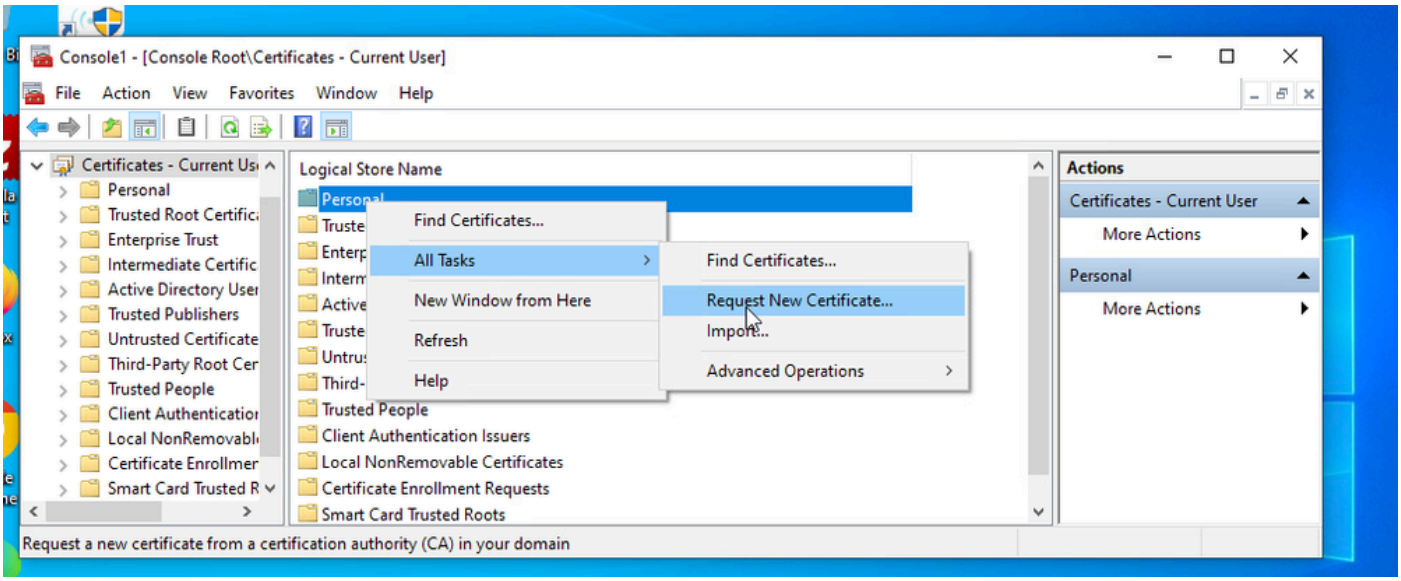

```
wlan vk802.1x 2 vk802.1x
 local-auth VK-EAP
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 security dot1x authentication-list default
 no shutdown
```

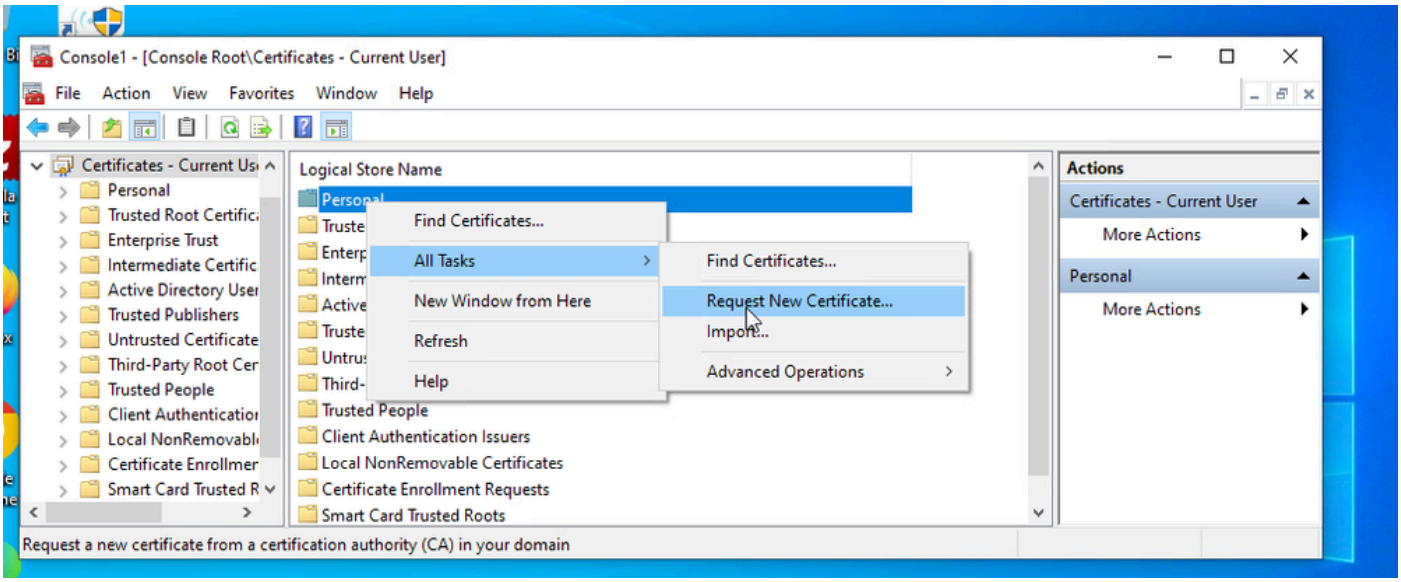
Cette configuration :

- Crée le SSID vk802.1x avec l'ID WLAN 2
- Active l'authentification locale avec le profil VK-EAP
- Applique les politiques radio pour les bandes 2,4 GHz et 5 GHz
- Applique l'authentification 802.1X en utilisant la liste de méthodes par défaut
- Active le SSID (sans arrêt)

Étape 8 : Déploiement de certificats utilisateur sur des clients sans fil

Assurez-vous que les clients sans fil disposent du certificat utilisateur nécessaire pour l'authentification. Dans les environnements de travaux pratiques, un périphérique joint à un domaine Active Directory (AD) peut recevoir le certificat via MMC (Microsoft Management Console). Il existe d'autres méthodes pour distribuer des certificats en fonction de votre environnement.





Vérifier

Vous pouvez vérifier les entrées de cache AAA sur le WLC 9800 à l'aide des commandes CLI. Notez que pour les WLC Catalyst 9800, les entrées de cache sont répertoriées sous "WNCD AAA Auth Cache entries", et non "SMD AAA Auth Cache entries".

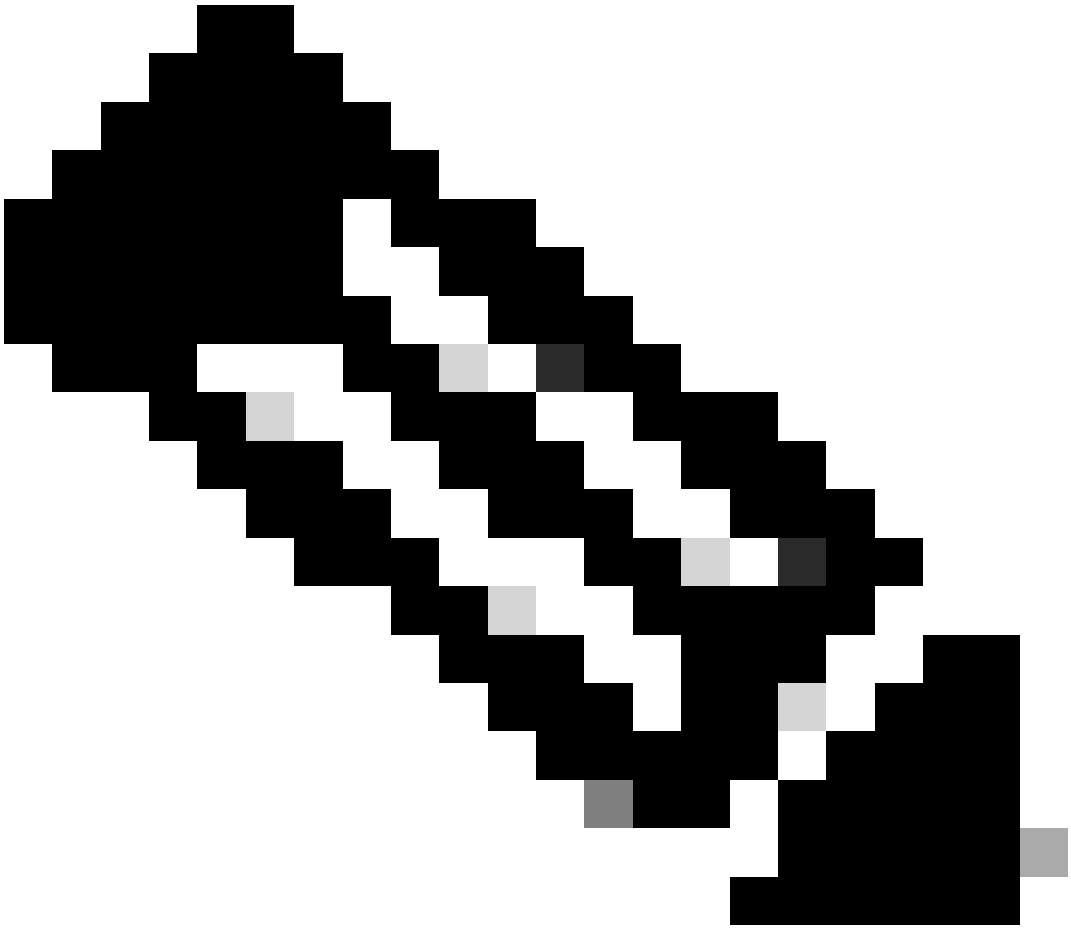
```
show aaa cache group <Server Group> all
```

Cette commande affiche les entrées de cache AAA actuelles stockées sur le WLC. Exemple de rapport :

```
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
...
```

Vérifiez que les clients peuvent se reconnecter et sont authentifiés via le cache AAA lorsque le serveur AAA n'est pas disponible.



Remarque : Pour l'authentification PEAP , la conception actuelle nécessite le renvoi de paires AV Cisco contenant le nom d'utilisateur et le hachage des informations d'identification pour chaque utilisateur pendant l'authentification par le serveur Radius.

cisco-av-pair = AS-Username=testuser

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

Chaque utilisateur doit être configuré avec les attributs de paire AV sur RADIUS.

Le mot de passe ou AS-Credential-Hash doit être au format NT-hash (https://codebeautify.org/ntlm-hash-generator).

Dépannage

Le dépannage du cache AAA et des problèmes d'authentification implique plusieurs étapes :

Étape 1 : Vérifier les entrées du cache AAA

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

Assurez-vous que les entrées client attendues sont présentes dans le cache.

Étape 2 : Valider l'installation de certificats et les points de confiance

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

Assurez-vous que les certificats sont correctement installés et mappés aux points de confiance appropriés pour l'authentification EAP-TLS.

Étape 3 : Confirmer les listes de méthodes d'authentification

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

Vérifiez que les listes de méthodes référencent le groupe de serveurs et les profils de cache corrects.

Étape 5 : Vérifier le suivi interne 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
```

Références:

[17.18 Guide de configuration du logiciel]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.