Configuration de l'authentification EAP locale sur le WLC Catalyst 9800

Table des matières

Introduction

Ce document décrit la configuration de l'EAP local sur les WLC Catalyst 9800 (contrôleurs LAN sans fil).

Conditions préalables

Exigences

Ce document décrit la configuration de Local EAP (Extensible Authentication Protocol) sur les WLC Catalyst 9800 ; c'est-à-dire que le WLC fonctionne comme serveur d'authentification RADIUS pour les clients sans fil.

Ce document suppose que vous êtes familier avec la configuration de base d'un WLAN sur le WLC 9800 et se concentre uniquement sur le WLC fonctionnant comme serveur EAP local pour les clients sans fil.

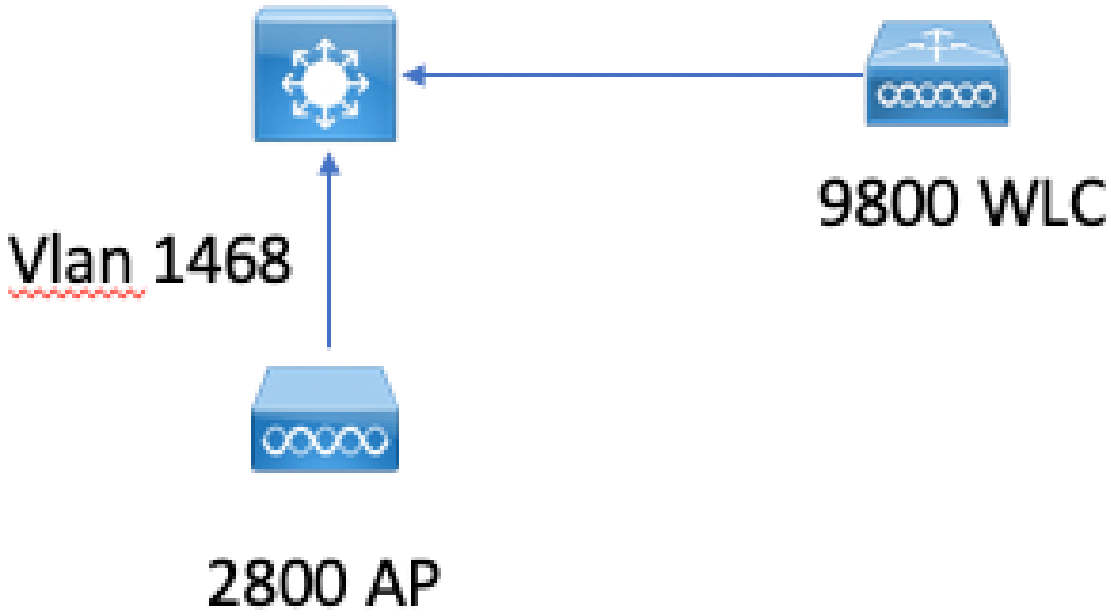
Composants utilisés

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.

Catalyst 9800 sur la version 16.12.1s

Configurer

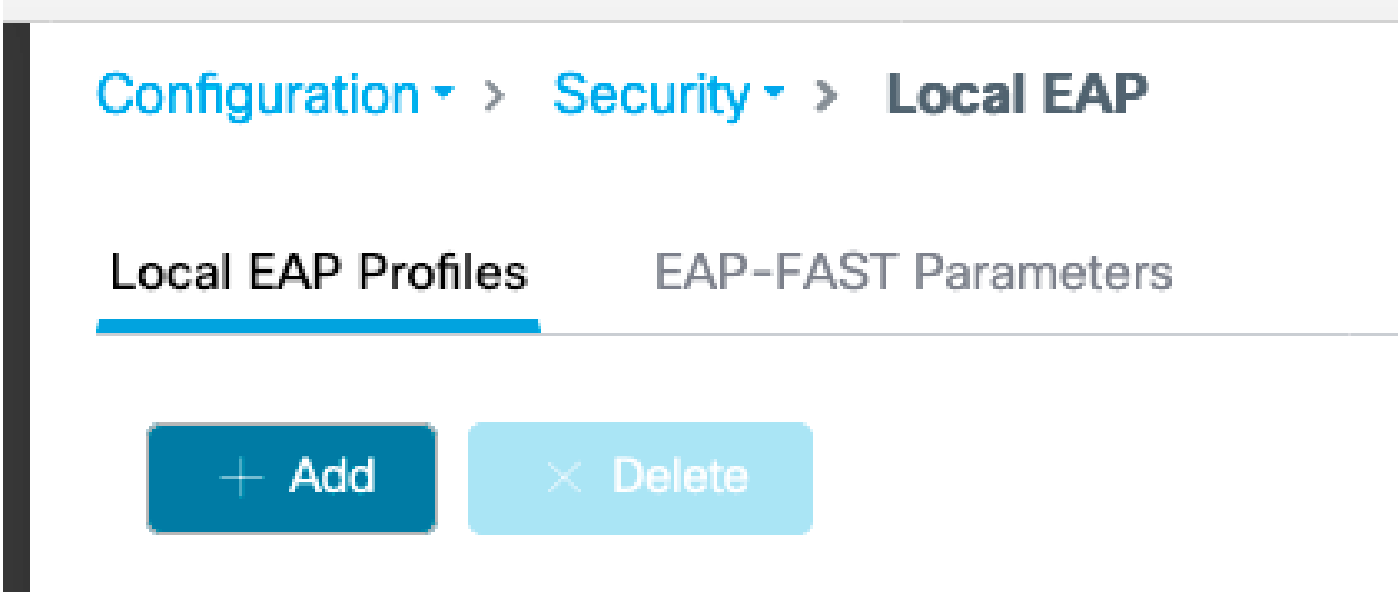
Diagramme du réseau



Configuration EAP locale principale

Étape 1. Profil EAP local

Accédez à Configuration > Security > Local EAP dans l'interface utilisateur Web du 9800.

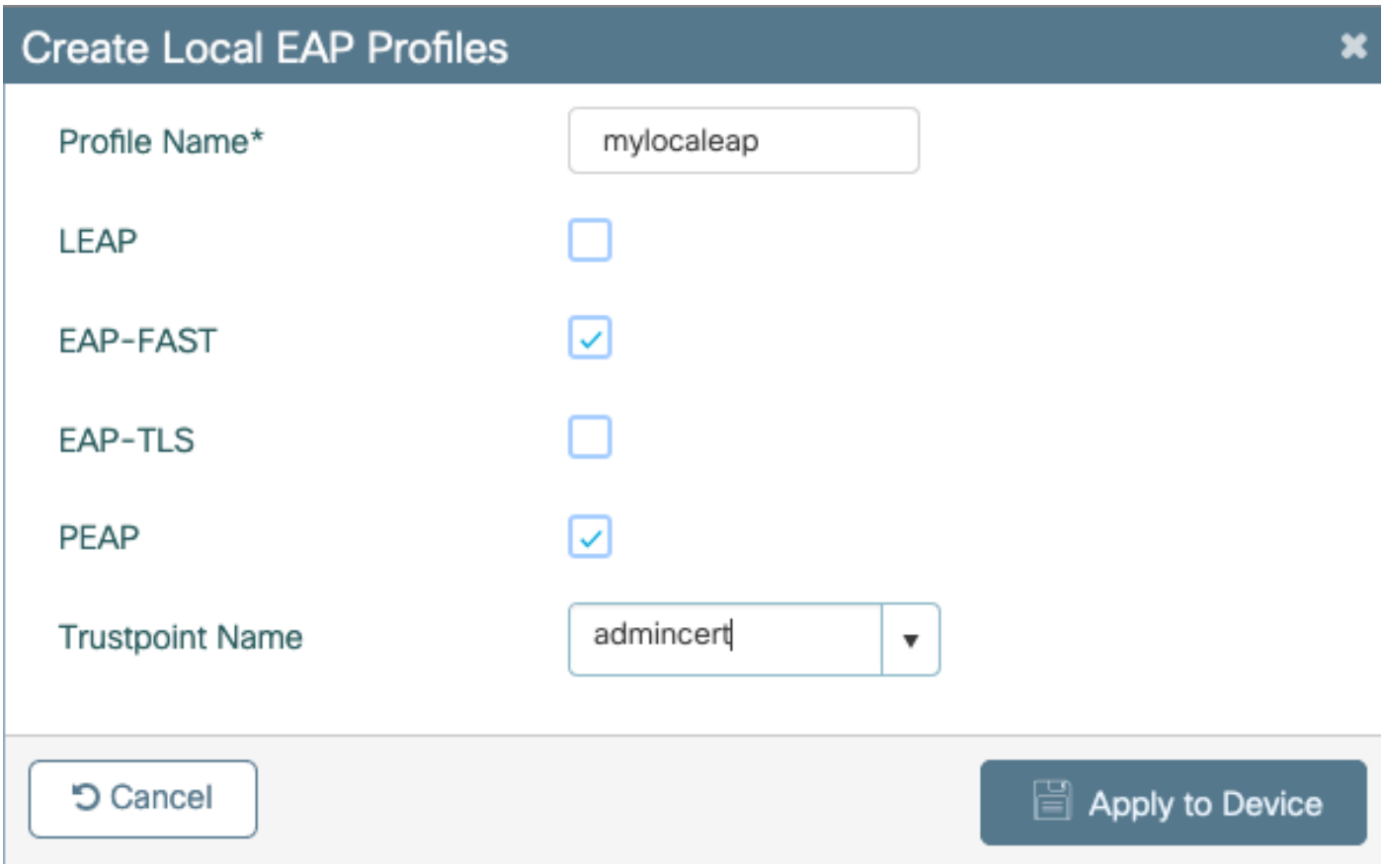


Sélectionnez Ajouter

Entrez un nom de profil.

Il n'est pas conseillé d'utiliser LEAP du tout en raison de sa faible sécurité. L'une des 3 autres méthodes EAP nécessite la configuration d'un point de confiance. En effet, le 9800, qui agit en tant qu'authentificateur, doit envoyer un certificat pour que le client l'approuve.

Les clients n'approuvent pas le certificat par défaut du WLC, vous devez donc désactiver la validation du certificat du serveur côté client (non conseillé) ou installer un point de confiance de certificat sur le WLC 9800 approuvé par le client (ou l'importer manuellement dans le magasin de confiance du client).



CLI :

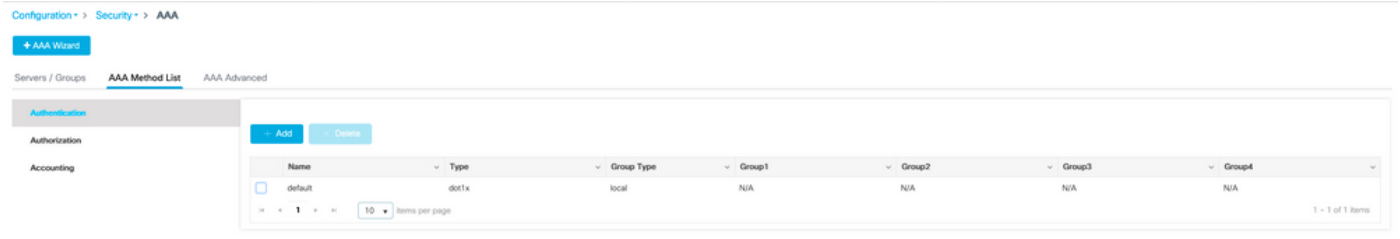
```
(config)#eap profile mylocapeap
(config-eap-profile)#method peap
(config-eap-profile)#pki-trustpoint admincert
```

Étape 2. méthode d'authentification AAA

Vous devez configurer une méthode AAA dot1x qui pointe localement aussi bien afin d'utiliser la base de données locale des utilisateurs (mais vous pourriez utiliser la recherche LDAP externe par exemple).

Accédez à Configuration > Security > AAA et accédez à l'onglet AAA method list pour Authentication. Sélectionnez Ajouter.

Choisissez le type « dot1x » et le type de groupe local.



Étape 3. Configurer une méthode d’autorisation AAA

Accédez au sous-onglet Autorisation et créez une nouvelle méthode pour le type credential-download et pointez-la vers local.

Procédez de même pour le type d'autorisation réseau

CLI :

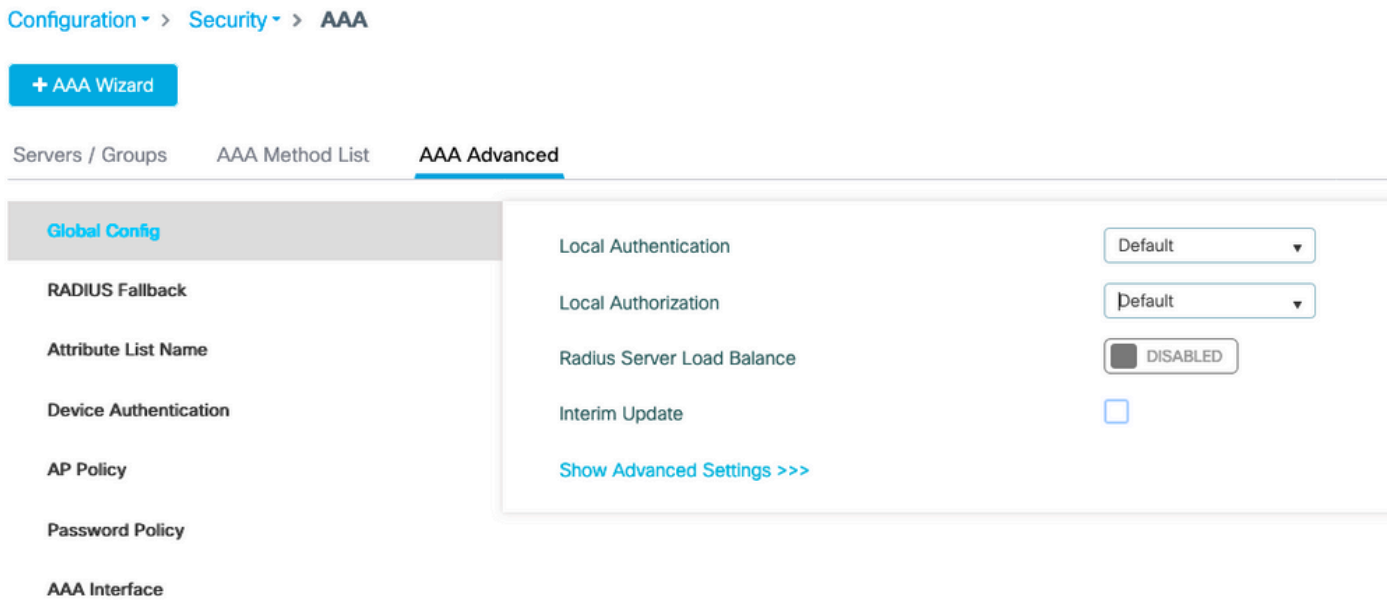
```
(config)#aaa new-model
(config)#aaa authentication dot1x default local
(config)#aaa authorization credential-download default local
(config)#aaa local authentication default authorization default
(config)#aaa authorization network default local
```

Étape 4. Configurer les méthodes avancées locales

Accédez à l'onglet AAA advanced.

Définissez la méthode d'authentification et d'autorisation locale. Comme cet exemple utilise la méthode « default » credential-download et « Default » dot1x, vous devez définir la valeur par défaut pour les zones déroulantes d'authentification locale et d'autorisation.

Si vous avez défini des méthodes nommées, choisissez "liste de méthodes" dans la liste déroulante et un autre champ vous permet d'entrer le nom de votre méthode.



CLI :

```
aaa local authentication default authorization default
```

Étape 5. Configurer un WLAN

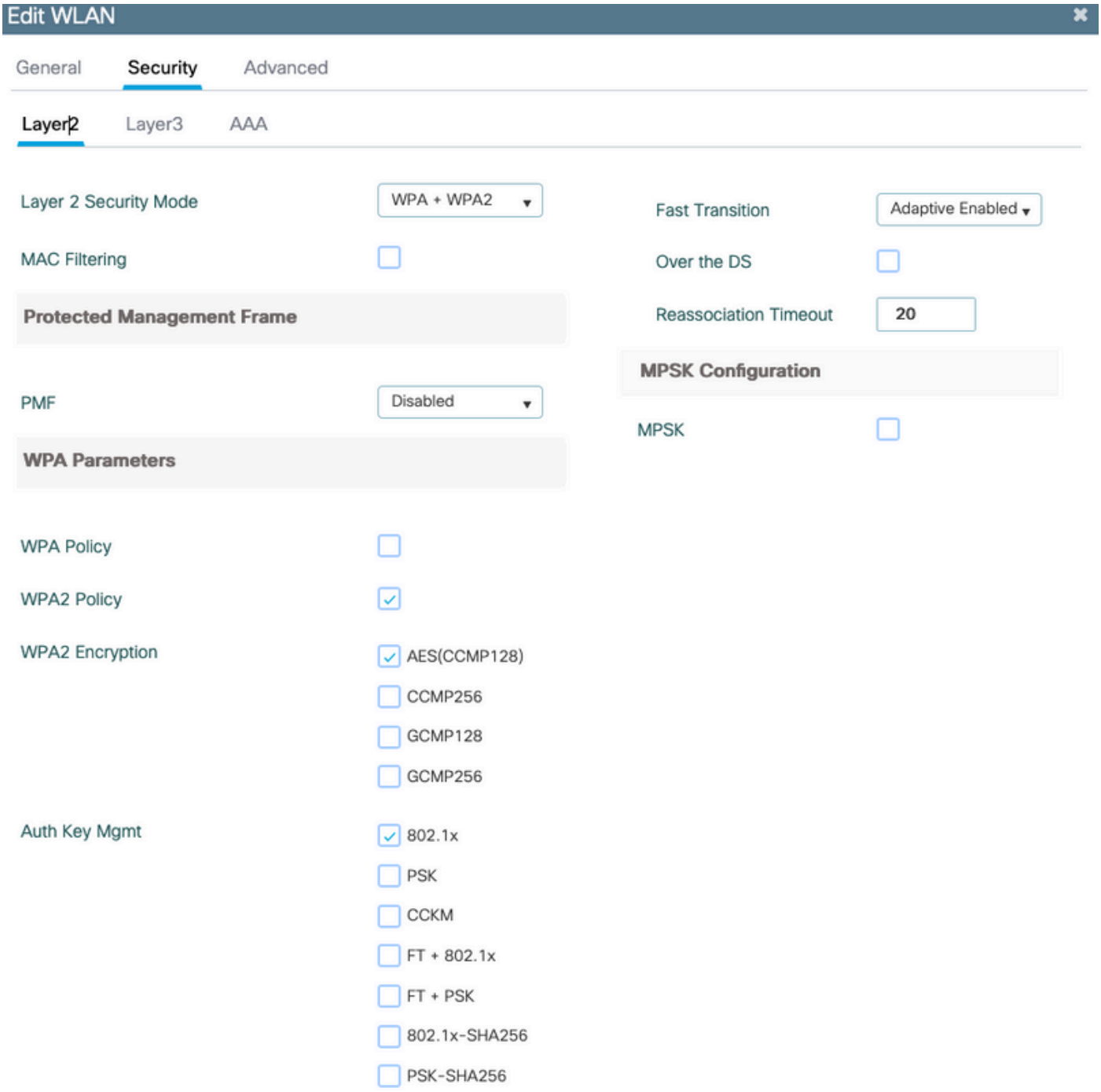
Vous pouvez ensuite configurer votre WLAN pour la sécurité 802.1x par rapport au profil EAP local et à la méthode d'authentification AAA définis à l'étape précédente.

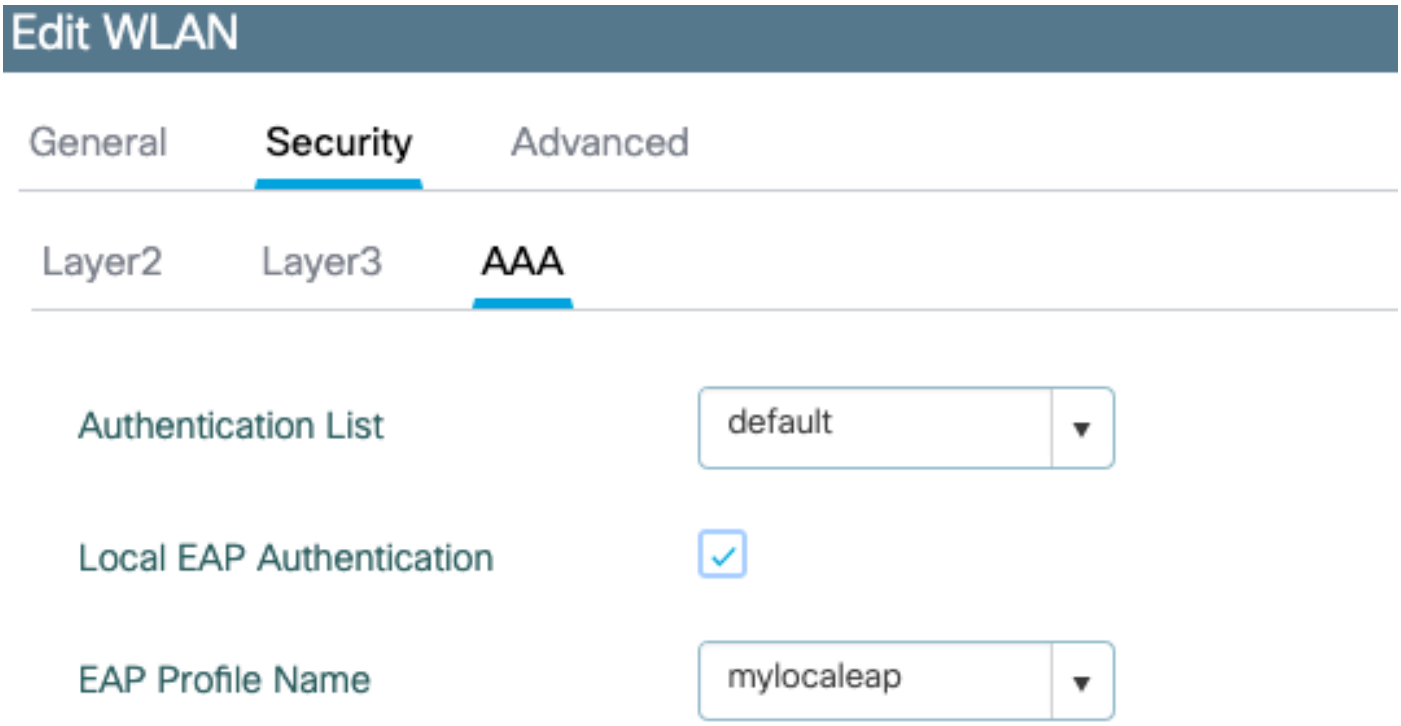
Accédez à Configuration > Tags and Profiles > WLANs > + Add >

Indiquez le SSID et le nom du profil.

La sécurité Dot1x est sélectionnée par défaut sous la couche 2.

Sous AAA, sélectionnez Local EAP Authentication et choisissez Local EAP profile et AAA Authentication list dans la liste déroulante.


Edit WLAN
General
Security
Advanced
Layer2
Layer3
AAA
Layer 2 Security Mode
WPA + WPA2
MAC Filtering
Protected Management Frame
PMF
Disabled
WPA Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Auth Key Mgmt
802.1x
PSK
CCKM
FT + 802.1x
FT + PSK
802.1x-SHA256
PSK-SHA256
Fast Transition
Adaptive Enabled
Over the DS
Reassociation Timeout
20
MPSK Configuration
MPSK




```
(config)#wlan localpeapssid 1 localpeapssid
(config-wlan)#security dot1x authentication-list default
(config-wlan)#local-auth mylocaleap
```

Étape 6. Créer un ou plusieurs utilisateurs

Dans l'interface de ligne de commande, les utilisateurs doivent être de type network-user. Voici un exemple d'utilisateur créé dans l'interface de ligne de commande :

```
(config)#user-name 1xuser
 creation-time 1572730075
 description 1xuser
 password 0 Cisco123
 type network-user description 1xuser
```

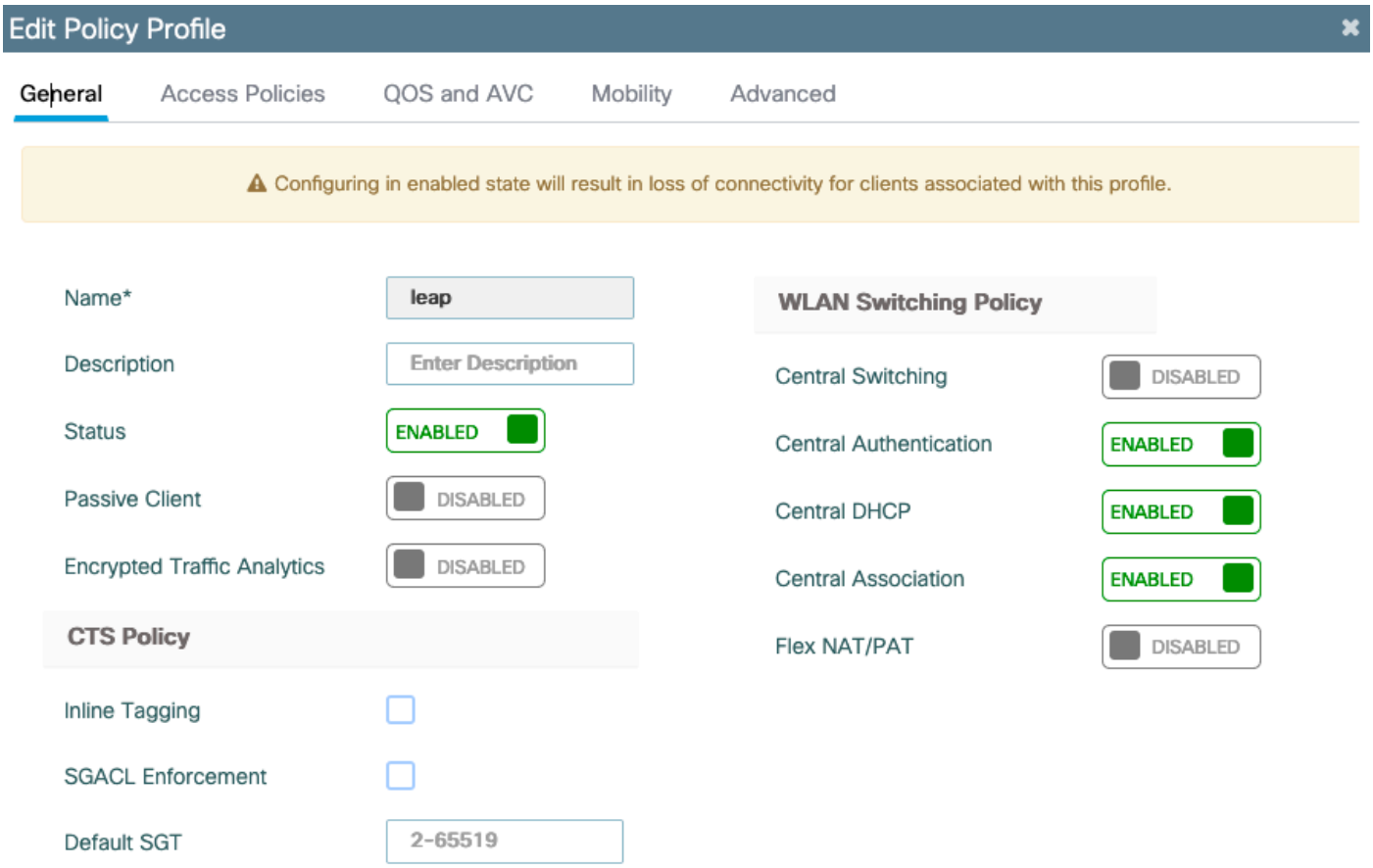
Une fois créé dans l'interface de ligne de commande, cet utilisateur est visible dans l'interface utilisateur Web, mais s'il est créé dans l'interface utilisateur Web, il n'existe aucune méthode pour en faire un utilisateur réseau à partir de la version 16.12

Étape 7. Créer un profil de stratégie. Créer une balise de stratégie pour mapper ce profil WLAN au profil de stratégie

Accédez à Configuration > Tags and profiles > Policy

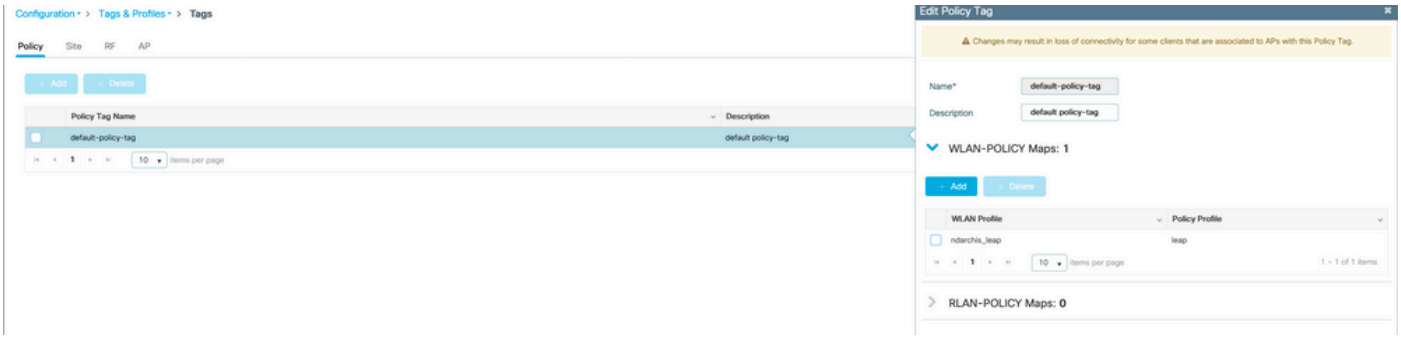
Créez un profil de stratégie pour votre WLAN.

Cet exemple montre un scénario de commutation locale flexconnect mais d'authentification centrale sur le VLAN 1468, mais cela dépend de votre réseau.



Accédez à Configuration > Tags and profiles > Tags

Attribuez votre WLAN à un profil de stratégie dans votre balise.



Étape 8. Déployez la balise de stratégie sur les points d'accès.

Dans ce cas, pour un seul AP, vous pouvez assigner les balises directement sur l'AP.

Accédez à Configuration > Wireless > Access points et sélectionnez le point d'accès que vous souhaitez configurer.

Assurez-vous que les balises attribuées sont celles que vous avez configurées.

Vérifier

Les lignes de configuration principales sont les suivantes :

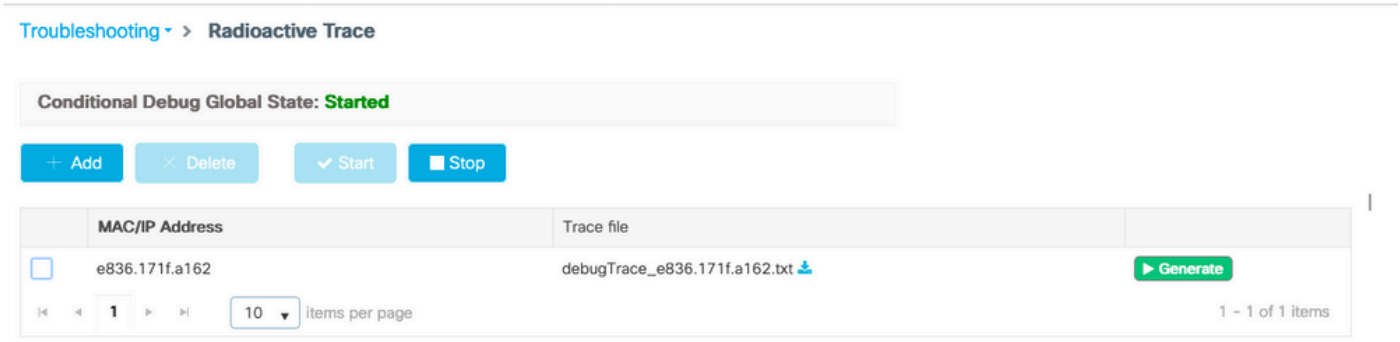
```
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download default local
aaa local authentication default authorization default
eap profile mylocaleap
method peap
pki-trustpoint admincert
user-name 1xuser
creation-time 1572730075 description 1xuser
password 0 Cisco123
type network-user description 1xuser
wlan ndarchis_leap 1 ndarchis_leap
local-auth mylocaleap
security dot1x authentication-list default
no shutdown
```

Dépannage

Notez que Cisco IOS® XE 16.12 et les versions antérieures ne prennent en charge que TLS 1.0 pour l'authentification EAP locale, ce qui peut entraîner des problèmes si votre client ne prend en charge que TLS 1.2, comme c'est de plus en plus la norme. Cisco IOS® XE 17.1 et versions ultérieures prennent en charge TLS 1.2 et TLS 1.0.

Afin de dépanner un client spécifique qui a du mal à se connecter, utilisez RadioActive Tracing. Accédez à Troubleshooting > RadioActive Trace et ajoutez l'adresse MAC du client.

Sélectionnez Start pour activer le suivi pour ce client.



Une fois le problème reproduit, vous pouvez sélectionner le bouton Generate afin de produire un

fichier qui contient la sortie de débogage.

Exemple d'un client qui ne parvient pas à se connecter en raison d'un mot de passe incorrect

```
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.785 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [eap] [23294]: (info): FAST:EAP_FAIL from inner method MSCHAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [eap-auth] [23294]: (info): FAIL for EAP method name: EAP-FAS
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rai
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [errmsg] [23294]: (note): %DOT1X-5-FAIL: Authentication faile
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [auth-mgr] [23294]: (info): [e836.171f.a162:capwap_90000004] A
```

Suivi en cas d'échec

Il est possible de vérifier la liste des événements d'échec pour une adresse MAC donnée avec la commande trace-on-failure, même si aucun débogage n'est activé.

Dans l'exemple suivant, la méthode AAA était absente au début (événement d'arrêt du serveur AAA), puis le client a utilisé des informations d'identification incorrectes quelques minutes plus tard.

La commande est show logging trace-on-failure summary dans la version 16.12 et antérieure et est show logging profile wireless (filter mac <mac>) trace-on-failure dans Cisco IOS® XE 17.1 et

versions ultérieures. Il n'y a pas de différence technique à part que 17.1 et les versions ultérieures vous permettent de filtrer pour l'adresse MAC du client.

```
Nico9800#show logging profile wireless filter mac e836.171f.a162 trace-on-failure
Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis 2 ...
sending cmd to chassis 1 ...
Collecting files on current[1] chassis.
# of files collected = 30
Collecting files on current[2] chassis.
# of files collected = 30
Collecting files from chassis 1.
Time                          UUID                 Log

-----------------------------------------------------------------------------------------------------


2019/10/30 14:51:04.438     0x0      SANET_AUTHC_FAILURE - AAA Server Down username , audit session id
2019/10/30 14:58:04.424     0x0      e836.171f.a162 CLIENT_STAGE_TIMEOUT State = AUTHENTICATING, WLAN p
```

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.