Dépanner les problèmes courants avec LWA sur les WLC 9800

Table des matières

Introduction

Ce document décrit les problèmes courants avec les clients se connectant à un WLAN avec l'authentification Web locale (LWA).

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances de base sur :

- Contrôleur LAN sans fil Cisco (WLC) 9800.
- Compréhension générale de l'authentification Web locale (LWA) et de sa configuration.

Composants utilisés

Les informations de ce document sont basées sur les versions logicielles et matérielles suivantes :

- WLC 9800-CL
- Point d'accès Cisco 9120AXI
- 9800 WLC Cisco IOS® XE version 17.9.3

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

LWA est un type d'authentification WLAN qui peut être configuré sur le WLC où le client final qui tente de se connecter, après avoir sélectionné le WLAN dans la liste, présente un portail à l'utilisateur. Dans ce portail, l'utilisateur peut entrer un nom d'utilisateur et un mot de passe (selon la configuration sélectionnée) pour terminer la connexion au WLAN.

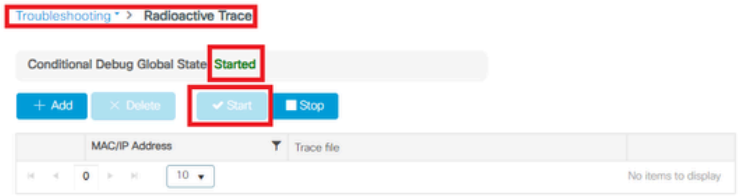
Référez-vous au guide de configuration Configure Local Web Authentication pour plus d'informations sur la façon de configurer LWA sur le WLC 9800.

Traces radioactives (RA) sur le WLC 9800

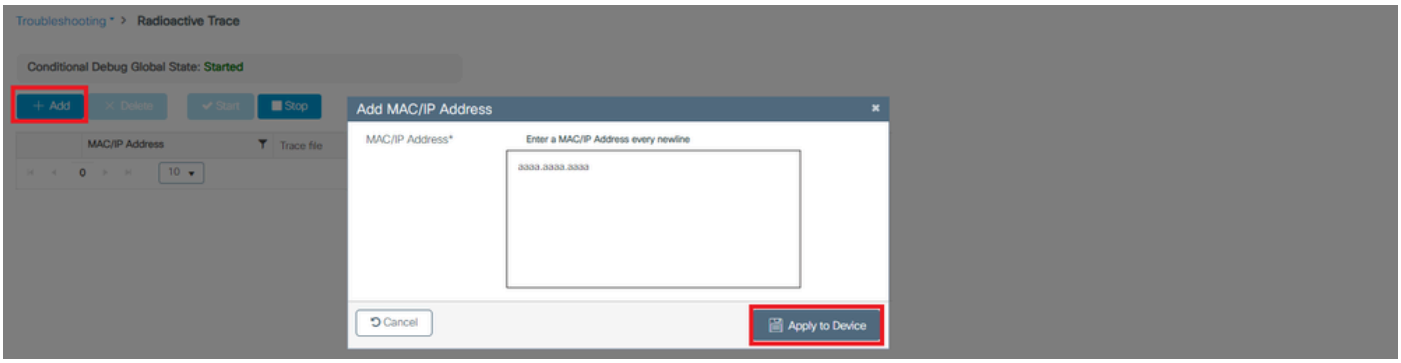
Les traces radioactives sont un excellent outil de dépannage qui peut être utilisé lors du dépannage de divers problèmes avec le WLC et la connectivité client. Pour collecter les traces d'annonce de routeur, procédez comme suit :

À partir de la GUI :

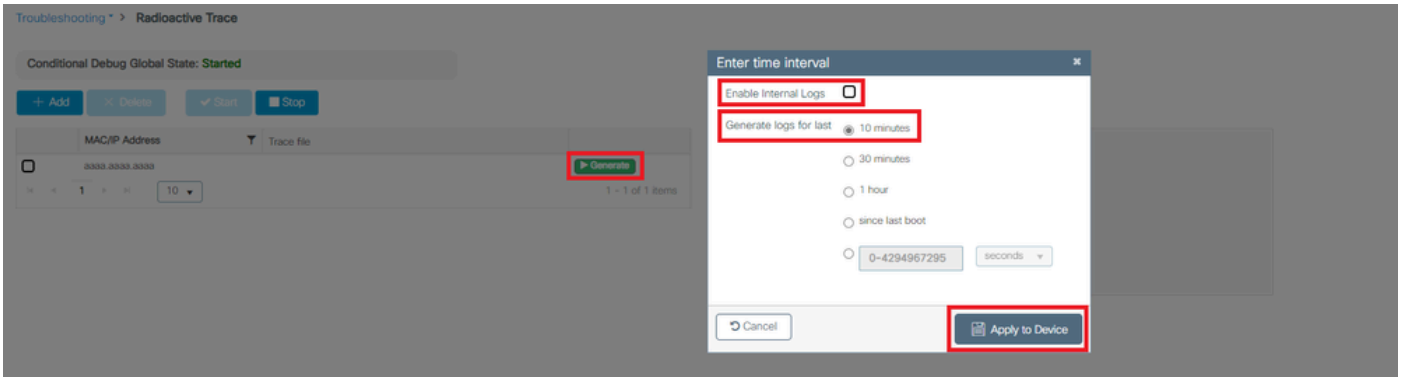
1. Accédez à Troubleshooting > Radioactive Trace.
2. Cliquez sur Démarrer pour activer l'état global du débogage conditionnel.
3. Cliquez sur + Ajouter. Une fenêtre contextuelle s'ouvre. Saisissez l'adresse MAC du client. Tout format d'adresse MAC est accepté (aabb.ccdd.eeff, AABB.CCDD.EEEE, aa:bb:cc:dd:ee:ff, ou AA:BB:CC:DD:EE:FF). Cliquez ensuite sur Apply to Device.
4. Demandez au client de reproduire le problème 3 ou 4 fois.
5. Une fois le problème reproduit, cliquez sur Generate (Générer).
6. Une nouvelle fenêtre contextuelle s'ouvre. Générez des journaux pendant les 10 dernières minutes. (Dans ce cas, il n'est pas nécessaire d'activer les journaux internes). Cliquez sur Apply to Device et attendez que le fichier soit traité.
7. Une fois le fichier généré, cliquez sur l'icône Download.



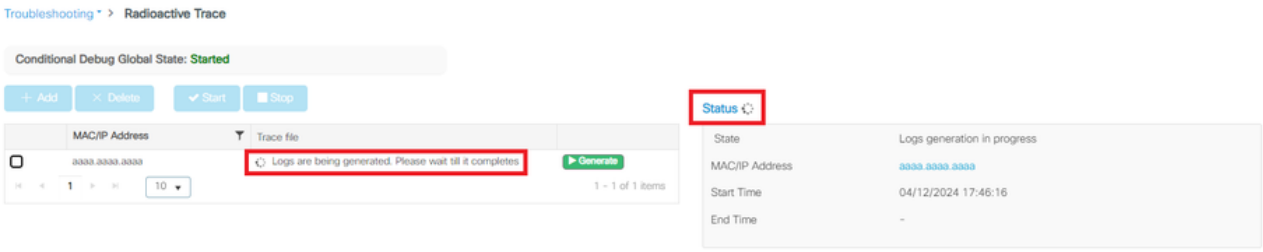
Activer le débogage conditionnel



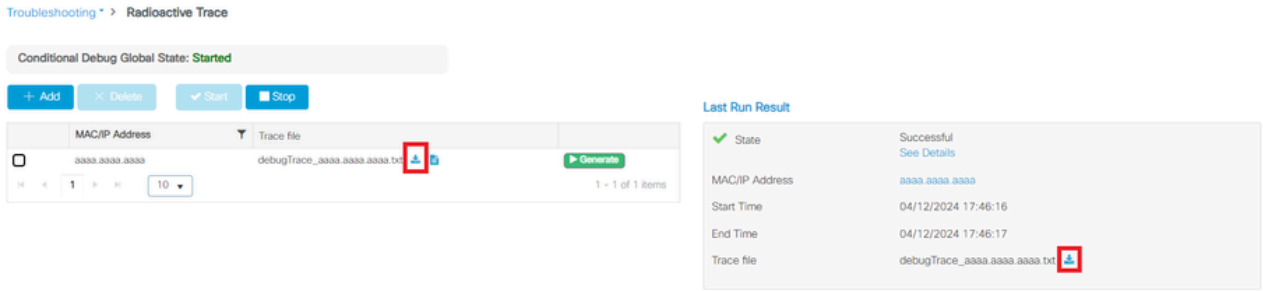
Ajouter une adresse MAC client



Générer des journaux pour les 10 dernières minutes



Attendez que le fichier soit



généréTéléchargez le fichier

À partir de la CLI :

<#root>

```
WLC# debug wireless mac
<mac-address>
 monitor-time 600
```

Un nouveau fichier dans le bootflash est généré appelé ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

<#root>

```
WLC# more bootflash:
ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Copier le fichier sur un serveur externe pour analyse

<#root>

```
WLC# copy bootflash:
ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
 ftp://username:password@<ftp-server-ip>/path/RATRACE_FILENAME.txt
```

Pour plus d'informations sur le traçage radioactif, veuillez consulter ce lien.

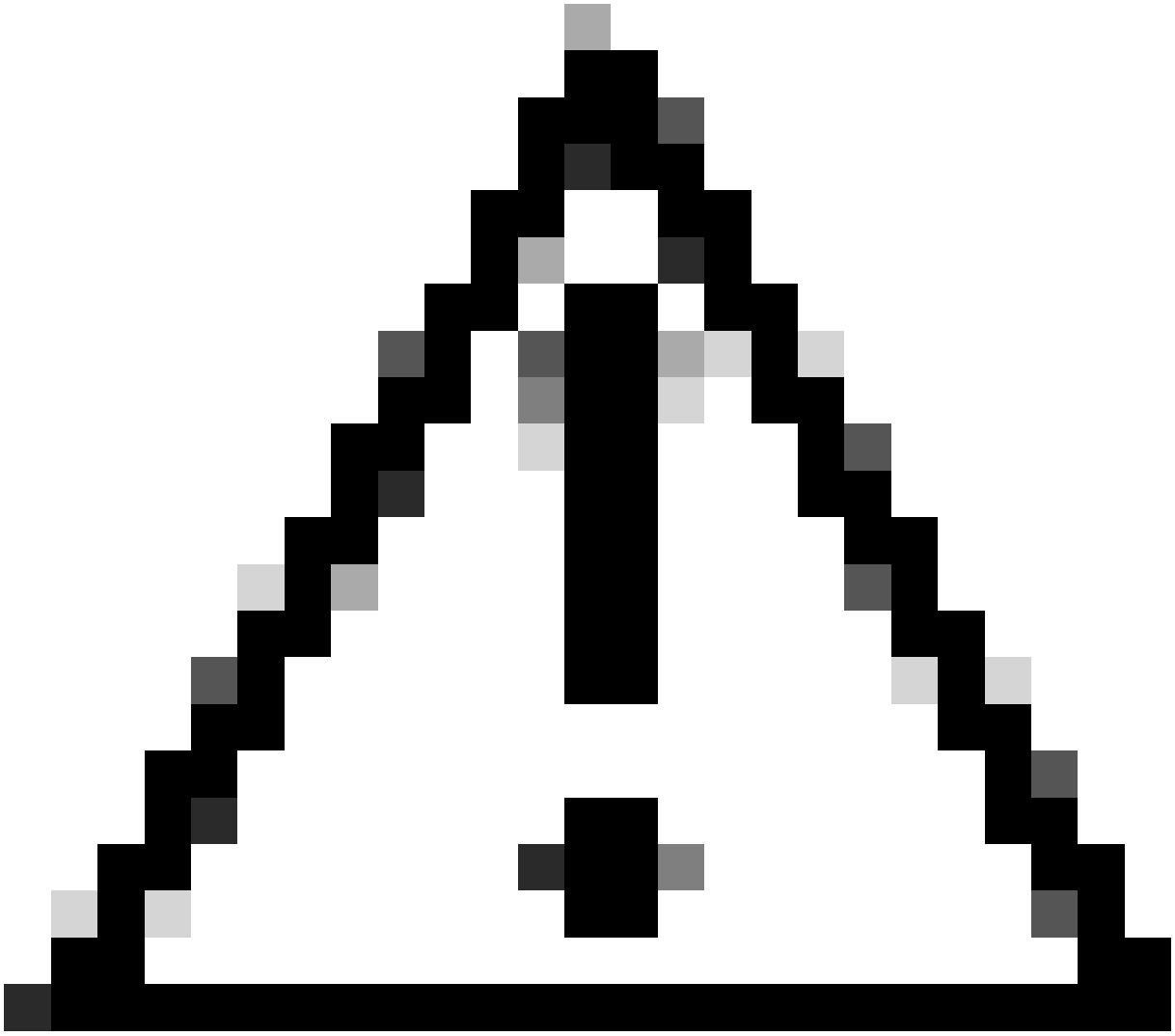
Flux attendu

Reportez-vous aux informations pour comprendre le scénario de travail pour LWA.

Étapes à suivre par le client du point de vue du client

1. Le client final s'associe au WLAN.
2. Le client obtient une adresse IP attribuée.
3. Le portail est présenté au client final.
4. Le client final saisit les informations de connexion.
5. Client final authentifié.
6. Le client final peut naviguer sur Internet.

Étapes à suivre par le client du point de vue du WLC



Attention : De nombreux journaux de la trace Radio Active (RA) ont été omis pour des raisons de simplicité.

Le client final s'associe au WLAN

<#root>

```
MAC: aaaa.bbbb.cccc

Association received

. BSSID d4e8.801a.3063, WLAN LWA-SSID, Slot 0 AP d4e8.801a.3060, APD4E8.8019.608C, old BSSID d4e8.801a.
MAC: aaaa.bbbb.cccc Received Dot11 association request. Processing started,SSID: LWA-SSID, Policy profi
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc Dot11 ie validate ext/supp rates. Validation Passed for Supported rates radio_type
MAC: aaaa.bbbb.cccc WiFi direct: Dot11 validate P2P IE. P2P IE not present.
MAC: aaaa.bbbb.cccc dot11 send association response. Framing association response with resp_status_code
MAC: aaaa.bbbb.cccc Dot11 Capability info byte1 1, byte2: 14
MAC: aaaa.bbbb.cccc WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled
MAC: aaaa.bbbb.cccc Clearing old call info.
```

```
MAC: aaaa.bbbb.cccc dot11 send association response. Sending assoc response of length: 161 with resp_st
MAC: aaaa.bbbb.cccc
```

Association success.

```
 AID 1, Roaming = True, WGB = False, 11r = False, 11w = False Fast roam = False
MAC: aaaa.bbbb.cccc DOT11 state transition: S_DOT11_ASSOCIATED -> S_DOT11_ASSOCIATED
```

Authentification L2

<#root>

```
MAC: aaaa.bbbb.cccc Starting L2 authentication. Bssid in state machine:d4e8.801a.3063 Bssid in request
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_L2_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc L2 Authentication initiated. method WEBAUTH, Policy VLAN 0, AAA override = 1
[aaaa.bbbb.cccc:capwap_90400002] -
```

authc_list: forwebauth

```
[aaaa.bbbb.cccc:capwap_90400002] - authz_list: Not present under wlan configuration
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT
MAC: aaaa.bbbb.cccc
```

L2 Authentication of station is successful.

```
, L3 Authentication : 1
```

Le client obtient une adresse IP attribuée

<#root>

```
MAC: aaaa.bbbb.cccc Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE
MAC: aaaa.bbbb.cccc
```

Received ip learn response. method: IPLEARN_METHOD_DHCP

Authentification L3

<#root>

```
MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc
```

L3 Authentication initiated. LWA

```
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT
```

Le client obtient une adresse IP

<#root>

```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
RX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
RX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE ->
```

S_IPLEARN_COMPLETE

Traitement du portail

<#root>

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

HTTP GET request

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

Parse GET, src [X.X.X.X] dst [Z.Z.Z.Z] url [http://connectivitycheck.gstatic.com/generate_204]

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 8
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

State GET_REDIRECT -> GET_REDIRECT

[...]

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

GET rcvd when in GET_REDIRECT state

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

HTTP GET request

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

Parse GET, src [X.X.X.X] dst [192.0.2.1] url [https://<virtual-ip-address>:443/login.html?redirect=http:

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 10

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

Param-map used: lwa-parameter_map

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

State GET_REDIRECT -> LOGIN

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

Sending Webauth login form

, len 8076
[...]
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

POST rcvd when in LOGIN state

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 get url: /login.html
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 4
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State LOGIN -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 45876/176 IO state READING -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

State AUTHENTICATING -> AUTHC_SUCCESS

Le WLC traite les informations à appliquer au client final de connexion

<#root>

[aaaa.bbbb.cccc:capwap_90400002]

Authc success from WebAuth, Auth event success

[aaaa.bbbb.cccc:capwap_90400002] Raised event

APPLY_USER_PROFILE

(14)
[aaaa.bbbb.cccc:capwap_90400002] Raised event RX_METHOD_AUTHC_SUCCESS (3)
[aaaa.bbbb.cccc:capwap_90400002] SM will not send event Template Deactivated to PRE for 0xAE000012
[aaaa.bbbb.cccc:capwap_90400002] SM will not send event Template Deactivated to PRE for 0xAE000012

Authentication Success.

Resolved Policy bitmap:4 for client aaaa.bbbb.cccc
Applying Attribute :

username 0 "cisco"

Applying Attribute : aaa-author-type 0 1 (0x1)
Applying Attribute : aaa-author-service 0 16 (0x10)
Applying Attribute : clid-mac-addr 0 3a e6 3b 9a fc 4a
Applying Attribute : addr 0 0xac104206
Applying Attribute : addrv6 0 "þ€"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : target-scope 0 0 [client]
Applying Attribute : audit-session-id 0 "1A4210AC0000001C5B12A51C"
Applying Attribute : aaa-unique-id 0 28 (0x1c)
Applying Attribute : client-iif-id 0 4261415483 (0xfe000a3b)

```
Applying Attribute :
vlan-id 0 100 (0xa63)

Applying Attribute : session-linksec-secured 0 False
Applying Attribute : nas-ip-address 0 0x0
Applying Attribute : nas-ipv6-Address 0 ""
Applying Attribute : interface 0 ""
Applying Attribute : port-type 0 19 [802.11 wireless]
Applying Attribute : nas-port 0 10014 (0x40eba)
Applying Attribute :
cisco-wlan-ssid 0 "LWA-SSID"

Applying Attribute :
wlan-profile-name 0 "LWA-SSID"

Applying Attribute : dnis 0 "d4-e8-80-1a-30-60:LWA-SSID"
Applying Attribute : formatted-clid 0 "3a-e6-3b-9a-fc-4a"
Applying Attribute : bsn-wlan-id 0 16 (0x10)
Applying Attribute : nas-identifier-wireless 0 "LWA-SSID"
Applying Attribute : timeout 0 86400 (0x15180)
Applying Attribute : priv-lvl 0 1 (0x1)
Applying Attribute : timeout 0 86400 (0x15180)
Applying Attribute :
 method 0 1 [webauth]

Applying Attribute : clid-mac-addr 0 3a e6 3b 9a fc 4a
Applying Attribute : intf-id 0 2420113410 (0x90400002)
[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr username(45
[aaaa.bbbb.cccc:capwap_90400002] SM Notified attribute
Add/Update username cisco

[aaaa.bbbb.cccc:capwap_90400002]
Received User-Name cisco for client aaaa.bbbb.cccc

[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr auth-domain
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Success'
[aaaa.bbbb.cccc:capwap_90400002] Context changing state from 'Running' to 'Authc Success'
[aaaa.bbbb.cccc:capwap_90400002]
Username cisco received

[aaaa.bbbb.cccc:capwap_90400002]
WLAN ID 16 received
```

WLC applique le profil utilisateur au client final connecté

```
<#root>
```

```
Applied User Profile: aaa-author-type 0 1 (0x1)
Applied User Profile: aaa-author-service 0 16 (0x10)
Applied User Profile: clid-mac-addr 0 3a e6 3b 9a fc 4a
Applied User Profile: target-scope 0 0 [client]
Applied User Profile: aaa-unique-id 0 28 (0x1c)
Applied User Profile: client-iif-id 0 4261415483 (0xfe000a3b)
Applied User Profile: vlan-id 0 100 (0xa63)
Applied User Profile:session-linksec-secured 0 False
Applied User Profile: nas-ip-address 0 0x0
Applied User Profile: nas-ipv6-Address 0 ""
Applied User Profile: interface 0 ""
Applied User Profile: port-type 0 19 [802.11 wireless]
Applied User Profile: nas-port 0 10014 (0x40eba)
Applied User Profile:

cisco-wlan-ssid 0 "LWA-SSID"


Applied User Profile:

 wlan-profile-name 0 "LWA-SSID"


Applied User Profile:nas-identifier-wireless 0 "LWA-SSID"
Applied User Profile: priv-lvl 0 1 (0x1)
Applied User Profile: method 0 1 [webauth]
Applied User Profile:

clid-mac-addr 0 3a e6 3b 9a fc 4a


Applied User Profile: intf-id 0 2420113410 (0x90400002)
Applied User Profile:

 username 0 "cisco"


Applied User Profile: bsn-wlan-id 0 16 (0x10)
Applied User Profile: timeout 0 86400 (0x15180)
Applied User Profile: timeout 0 86400 (0x15180)
MAC: aaaa.bbbb.cccc Link-local bridging not enabled for this client, not checking VLAN validity
[aaaa.bbbb.cccc:capwap_90400002]

User Profile applied successfully - REPLACE

[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr method(757)



[aaaa.bbbb.cccc:capwap_90400002]

Raised event AUTHZ_SUCCESS (11)

[aaaa.bbbb.cccc:capwap_90400002]

Context changing state from 'Authc Success' to 'Authz Success'
```

Authentification Web terminée

<#root>

```
MAC: aaaa.bbbb.cccc
```

```
L3 Authentication Successful.

 ACL:[]
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING ->

S_AUTHIF_WEBAUTH_DONE
```

Attributs AAA appliqués au client final

<#root>

```
[ Applied attribute : username 0 "

cisco

" ]
[ Applied attribute : bsn-wlan-id 0 16 (0x10) ]
[ Applied attribute : timeout 0 86400 (0x15180) ]
[ Applied attribute : timeout 0 86400 (0x15180) ]
[ Applied attribute :bsn-vlan-interface-name 0 "

myvlan

" ]
```

Le client final atteint l'état Exécuter

<#root>

```
Managed client RUN state notification: aaaa.bbbb.cccc
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS ->

S_CO_RUN
```

Scénarios de dépannage courants

Échecs d'authentification

Considérations

- Le portail affiché indique « Authentication Failed » après la saisie des informations d'identification correctes.
- Le WLC affiche le client à l'état « Authentification Web en attente ».
- La page d'accueil initiale s'affiche à nouveau pour l'utilisateur.

Traces WLC RA

<#root>

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State LOGIN -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 40828/176 IO state READING -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

Param-map used: lwa-parameter_map

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State AUTHENTICATING ->
```

AUTHC_FAIL [INVALID CREDENTIALS]

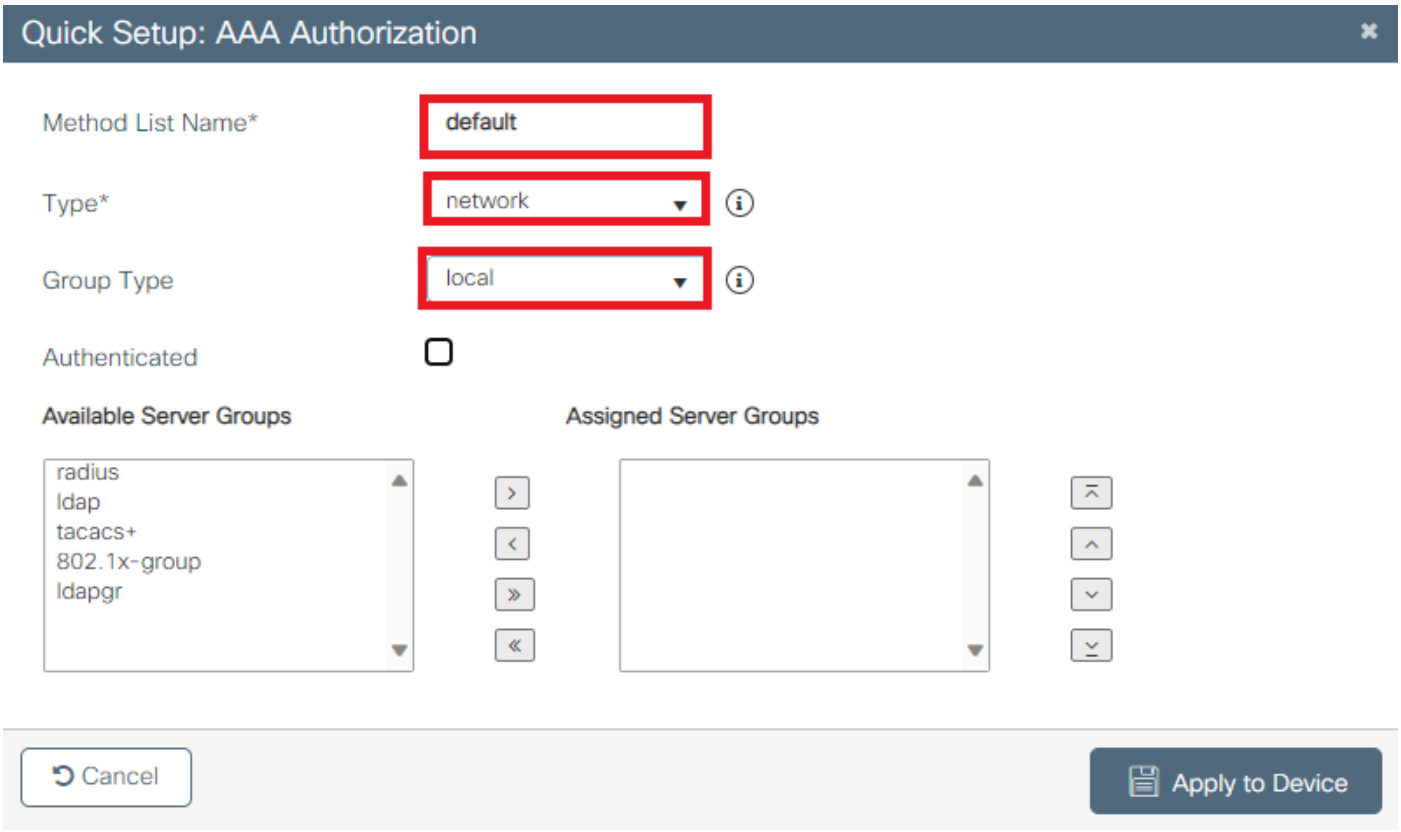
```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

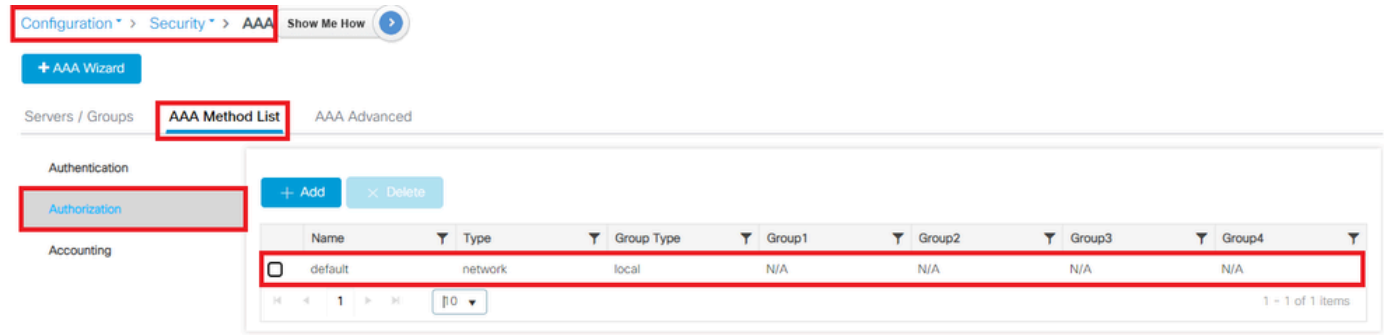
Solutions recommandées

Assurez-vous que la liste de méthodes AAA par défaut pour l'autorisation réseau existe sur la configuration WLC.

À partir de la GUI :

1. Accédez à Configuration > Security > AAA > AAA Method List > Authorization. Cliquez sur + Ajouter.
2. Configurez-le comme suit :
    1. Nom de la liste de méthodes : par défaut
    2. Type : réseau
    3. Type de groupe : local
3. Cliquez sur Apply to Device.





À partir de la CLI :

<#root>

```
WLC# configure terminal
WLC(config)# aaa authorization default network local
```

Le portail n'est pas affiché pour l'utilisateur mais le client semble connecté

Comportement possible du client final

- Le client final voit son périphérique comme « Connecté ».
- Le client final ne voit pas le portail.

- Le client final n'entre aucune information d'identification.
- Une adresse IP est attribuée au client final.
- Le WLC affiche le client à l'état « Exécuter ».

Traces WLC RA

Le client obtient une adresse IP attribuée et passe immédiatement à l'état « Exécuter » sur le WLC. Les attributs utilisateur affichent uniquement le VLAN attribué au client final.

<#root>

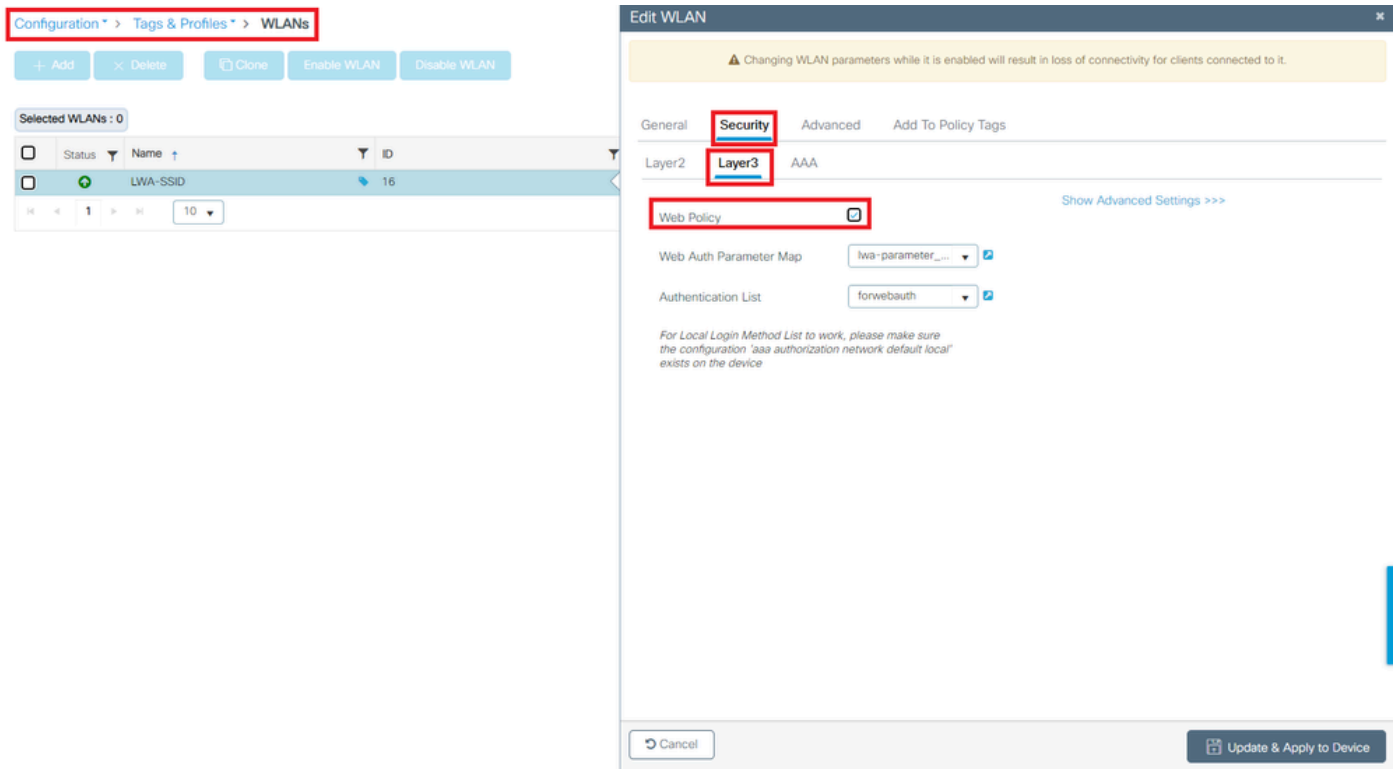
```
MAC: aaaa.bbbb.cccc

Client IP learn successful. Method: DHCP IP: X.X.X.X


[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr addr(8)
[aaaa.bbbb.cccc:capwap_90400002] SM Notified attribute Add/Update addr X.X.X.X
MAC: aaaa.bbbb.cccc IP-learn state transition:

 S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE


MAC: aaaa.bbbb.cccc Received ip learn response. method: IPLEARN_METHOD_DHCP
[ Applied attribute :bsn-vlan-interface-name 0 "

myvlan

" ]
[ Applied attribute : timeout 0 1800 (0x708) ]
MAC: aaaa.bbbb.cccc Client QoS run state handler
Managed client RUN state notification: aaaa.bbbb.cccc
MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
```

Solutions recommandées

Assurez-vous que la stratégie Web est activée sur le WLAN.

À partir de la GUI :

1. Accédez à Configuration > Tags & Profiles > WLANs.
2. Sélectionnez les WLAN LWA.
3. Accédez à Sécurité > Couche 3.
4. Assurez-vous que la case à cocher Stratégie Web est activée.



La stratégie Web doit être activée

À partir de la CLI :

<#root>

```
WLC# configure terminal
```

```
WLC(config)# wlan
```

<wlan>

```
WLC(config-wlan)# shutdown
WLC(config-wlan)# security webauth
WLC(config-wlan)# no shutdown
```

Le portail ne s'affiche pas à l'utilisateur et le client ne se connecte pas

Comportement possible du client final

- Le client final constate que son périphérique tente continuellement de se connecter.
- Le client final ne voit pas le portail.
- Aucune adresse IP n'est attribuée au client final.
- WLC affiche le client à l'état « Webauth Pending ».

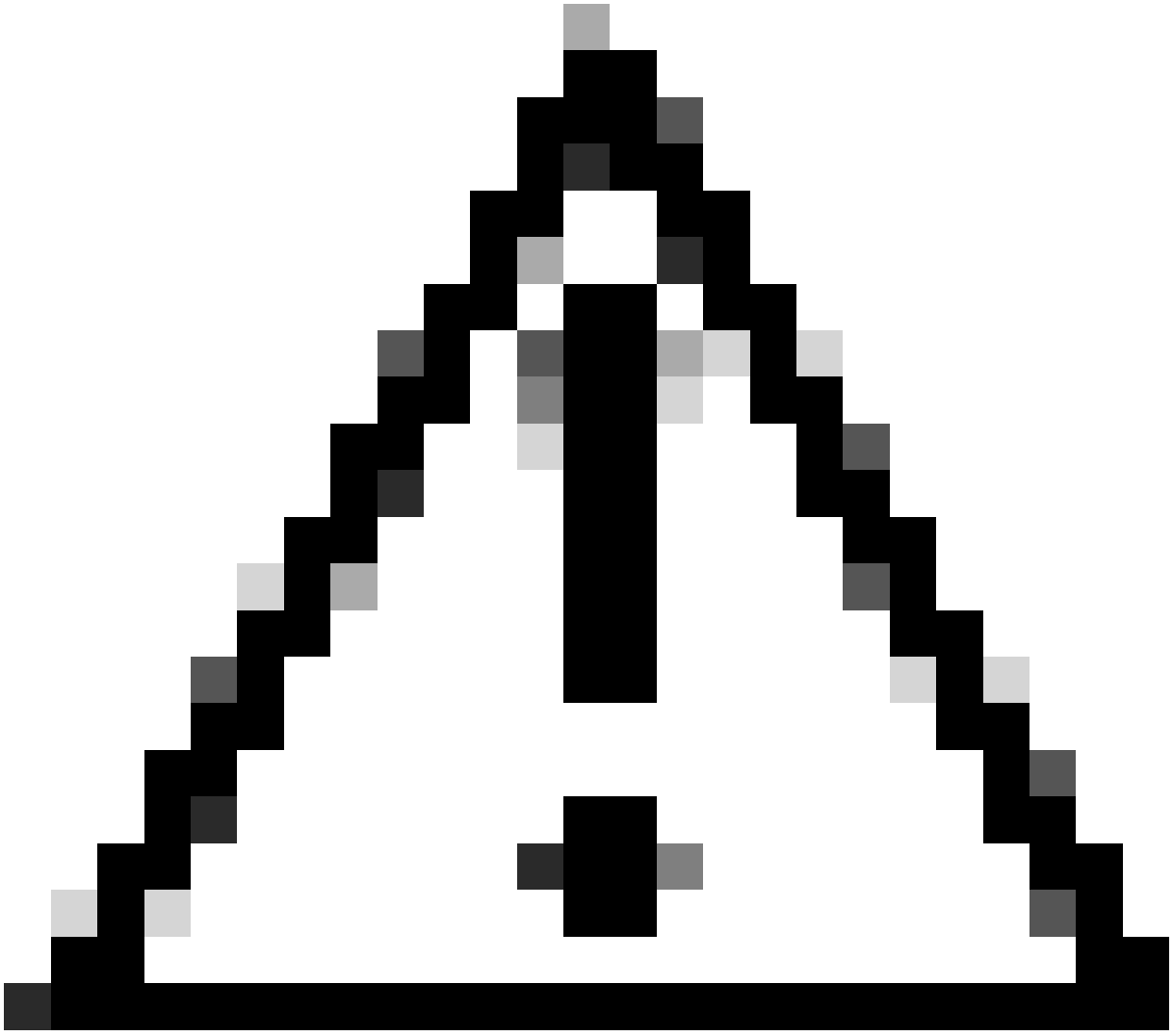
Solutions recommandées

Activez les serveurs HTTP/HTTPS nécessaires. Il est désormais possible de mieux contrôler les

serveurs HTTP/HTTPS devant être activés pour s'adapter pleinement aux besoins du réseau. Reportez-vous à ce lien pour plus d'informations sur la configuration des requêtes HTTP et HTTPS pour l'authentification Web, car plusieurs combinaisons HTTP sont prises en charge ; par exemple, les HTTP peuvent être utilisés pour webadmin uniquement et HTTP pour webauth.

Pour permettre la gestion des périphériques administratifs et l'authentification Web avec un accès HTTP et HTTPS, à partir de l'interface de ligne de commande :

```
WLC# configure terminal
WLC(config)# ip http server
WLC(config)# ip http secure-server
```



Attention : si ces deux serveurs sont désactivés, il n'y a pas d'accès à l'interface graphique utilisateur (GUI) du WLC.

Les clients finaux n'obtiennent pas d'adresse IP

Comportement possible du client final

- Les clients finaux constatent que leur périphérique tente constamment d'obtenir une adresse IP.
- WLC affiche le client à l'état « Apprentissage IP ».

Traces WLC RA

Demandes de découverte sans offre en retour.

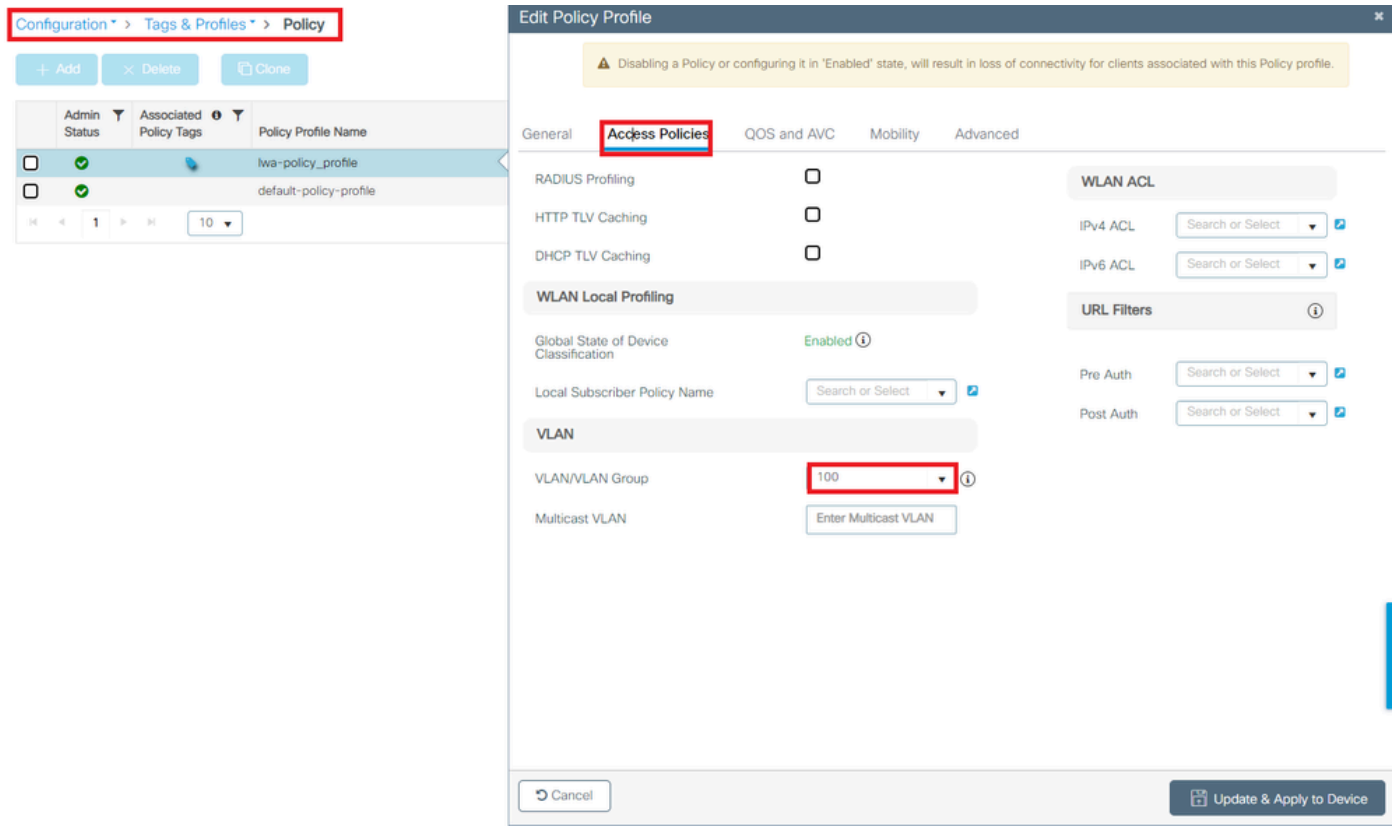
```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
```

Solutions recommandées

Tout d'abord : vérifiez que le VLAN correct est affecté au profil de stratégie.

À partir de la GUI :

1. Accédez à Configuration > Tags & Profiles > Policy.
2. Sélectionnez le profil de stratégie utilisé.
3. Accédez à Stratégies d'accès.
4. Sélectionnez le VLAN approprié.



À partir de la CLI :

<#root>

```
WLC# show wireless profile policy detailed
```

<policy-profile>

```
Policy Profile Name :
```

<policy-profile>

```
Description :
```

<policy-profile>

```
Status : ENABLED
VLAN :
```

VLAN-selected

```
[...]

WLC# configure terminal
WLC(config)# wireless profile policy
```

<policy-profile>

```
WLC(config-wireless-policy)#
```

vlan <correct-vlan>

Deuxièmement : assurez-vous qu'un pool DHCP est disponible pour l'utilisateur quelque part. Vérifiez sa configuration et son accessibilité. Les traces RA indiquent sous quel VLAN le processus DHCP DORA est en cours. Assurez-vous que ce VLAN est le bon VLAN.

```
DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff src_ip
DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y.Y,
DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff src_ip
DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y.Y,
```

Le portail personnalisé n'apparaît pas au client final

Comportement possible du client final

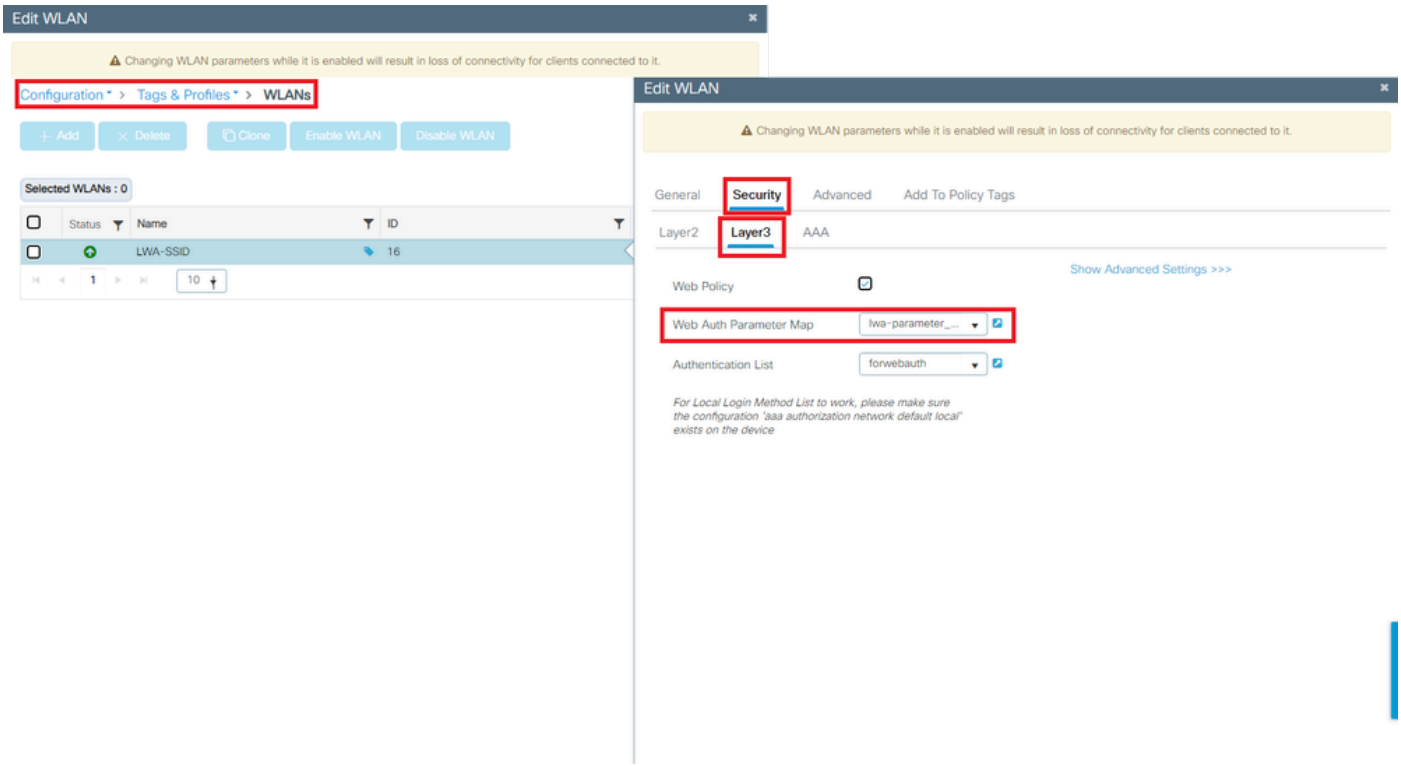
- Le portail par défaut du WLC est visible.

Solutions recommandées

Tout d'abord : assurez-vous que le WLAN utilise la carte de paramètres d'authentification Web personnalisée.

À partir de la GUI :

1. Accédez à Configuration > Tags & Profiles > WLANs.
2. Sélectionnez le WLAN dans la liste.
3. Accédez à Sécurité > Couche 3.
4. Sélectionnez la carte de paramètres d'authentification Web personnalisée.



Mappage de paramètres personnalisés sélectionné

À partir de la CLI :

<#root>

```
WLC# show wlan name LWA-SSID
WLAN Profile Name : LWA-SSID
================================================
[...]
Security:
     Webauth Parameter Map :
```

<parameter-map>

```
WLC# configure terminal
WLC(config)# wlan
```

<wlan>

```
WLC(config-wlan)# security web-auth parameter-map
```

<parameter-map>

Deuxièmement : il est important de noter que l'interface de programmation personnalisée téléchargée depuis le portail Web Cisco.com ne fonctionne pas avec une interface de programmation très robuste et complexe. Il est généralement recommandé d'effectuer des modifications uniquement au niveau CSS et d'ajouter ou de supprimer des images. Les applets, PHP, les variables de modification, React.js, etc. ne sont pas supportés. Si un portail personnalisé n'est pas affiché au client, essayez d'utiliser les pages WLC par défaut et voyez si le problème

peut être répliqué. Si le portail s'affiche correctement, cela signifie que les pages personnalisées qui sont censées être utilisées ne prennent pas en charge certains éléments.

Troisièmement : si vous utilisez un EWC (contrôleur sans fil intégré), il est conseillé d'utiliser l'interface de ligne de commande pour ajouter les pages personnalisées afin de s'assurer qu'elles sont correctement affichées :

<#root>

```
EWC# configure terminal
EWC(config)# parameter-map type
```

<parameter-map>

```
EWC(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
EWC(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
EWC(config-params-parameter-map)# custom-page failure device flash:loginfail.html
EWC(config-params-parameter-map)# custom-page success device flash:loginsucess.html
EWC(config-params-parameter-map)# end
```

Le portail personnalisé n'apparaît pas correctement au client final

Comportement possible du client final

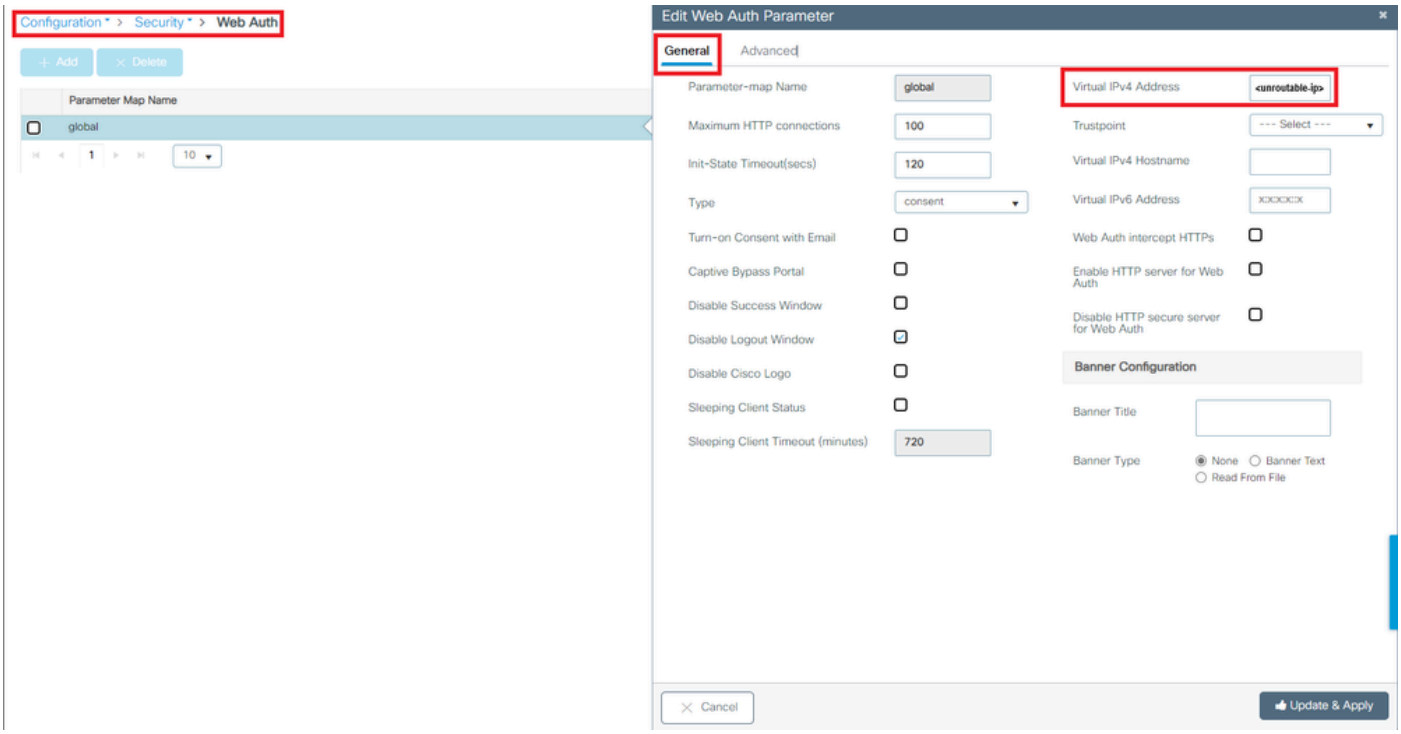
- Le portail personnalisé n'est pas affiché correctement (c'est-à-dire que les images ne sont pas affichées).

Solutions recommandées

Assurez-vous qu'une adresse IP virtuelle est attribuée à la carte de paramètre globale.

À partir de la GUI :

1. Accédez à Configuration > Security > Web Auth.
2. Sélectionnez la carte de paramètre globale dans la liste.
3. Ajoutez une adresse IP virtuelle non routable.



Adresse IP virtuelle sur mappage de paramètres global défini sur une adresse IP non routable

À partir de la CLI :

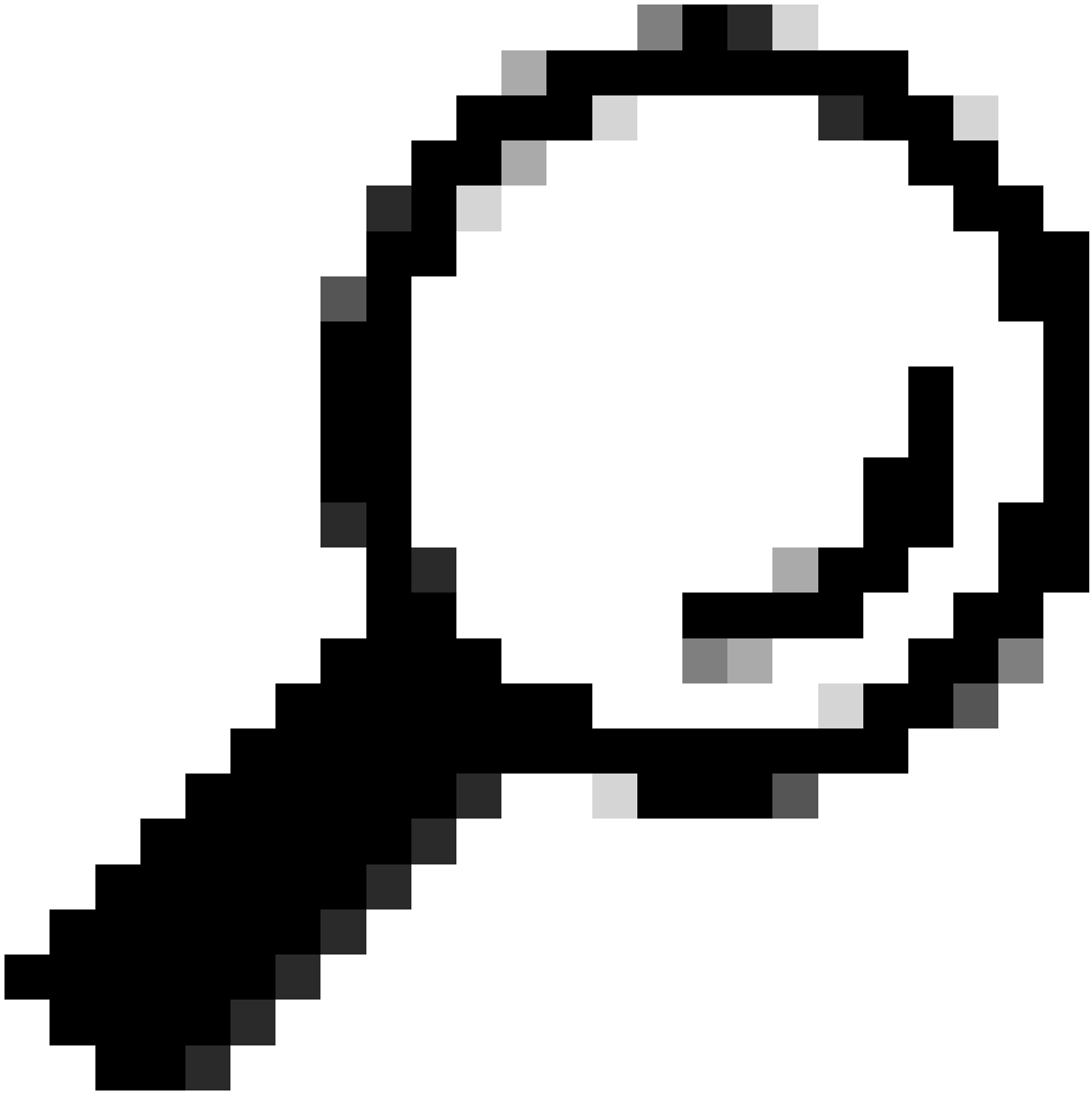
<#root>

```
WLC# show parameter-map type webauth global
Parameter Map Name : global
[...]
Virtual-ipv4 :
```

<unroutable-ip>

```
[...]

WLC# configure terminal
WLC(config)# parameter-map type webauth global
WLC(config-params-parameter-map)# virtual-ip ipv4
```

<unroutable-ip>



Conseil : l'adresse IP virtuelle sert d'adresse de redirection pour la page de connexion de l'authentification Web. Aucun autre périphérique sur le réseau ne doit avoir la même adresse IP, il ne doit pas être mappé à un port physique, ni exister sur une table de routage. Par conséquent, il est recommandé de configurer l'adresse IP virtuelle en tant qu'adresse IP non routable, seules celles qui sont sur le RFC5737 peuvent être utilisées.

Portal indique que « Votre connexion n'est pas sécurisée/la vérification de la signature a échoué »

Comportement possible du client final

- Lors de l'ouverture du portail, le client voit une erreur indiquant que la connexion n'est pas sécurisée.

- Le portail doit utiliser un certificat.

Choses à savoir

Si le portail doit être affiché sous HTTPS, cela signifie qu'il doit utiliser un certificat SSL (Secure Socket Layer). Ce certificat doit être émis par une autorité de certification tierce afin de valider que le domaine est bien réel. Les clients finaux doivent faire confiance à cette autorité lorsqu'ils entrent leurs informations d'identification et/ou consultent le portail. Afin de télécharger un certificat vers le WLC, veuillez vous référer à ce document.

Solutions recommandées

Commencez par redémarrer les services HTTP/HTTPS souhaités. Il est désormais possible de mieux contrôler les serveurs HTTP/HTTPS devant être activés pour s'adapter pleinement aux besoins du réseau. Reportez-vous à ce lien pour plus d'informations sur la configuration des requêtes HTTP et HTTPS pour l'authentification Web.

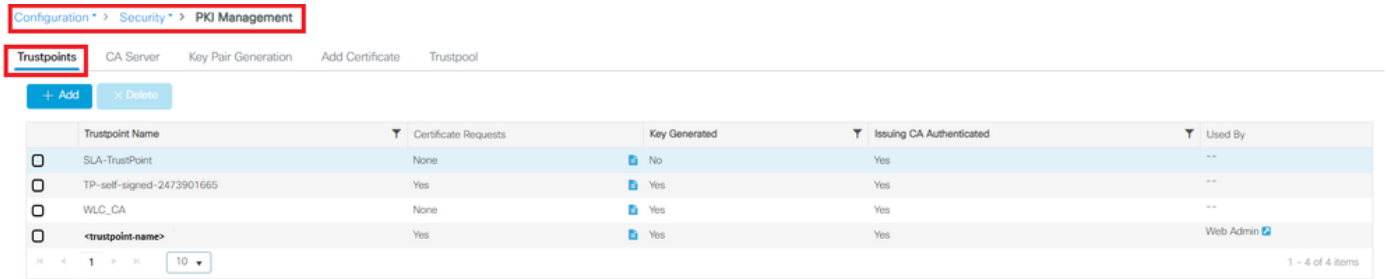
À partir de la CLI :

```
WLC# configure terminal
WLC(config)# no ip http server
WLC(config)# no ip http secure-server
WLC(config)# ip http server
WLC(config)# ip http secure-server
```

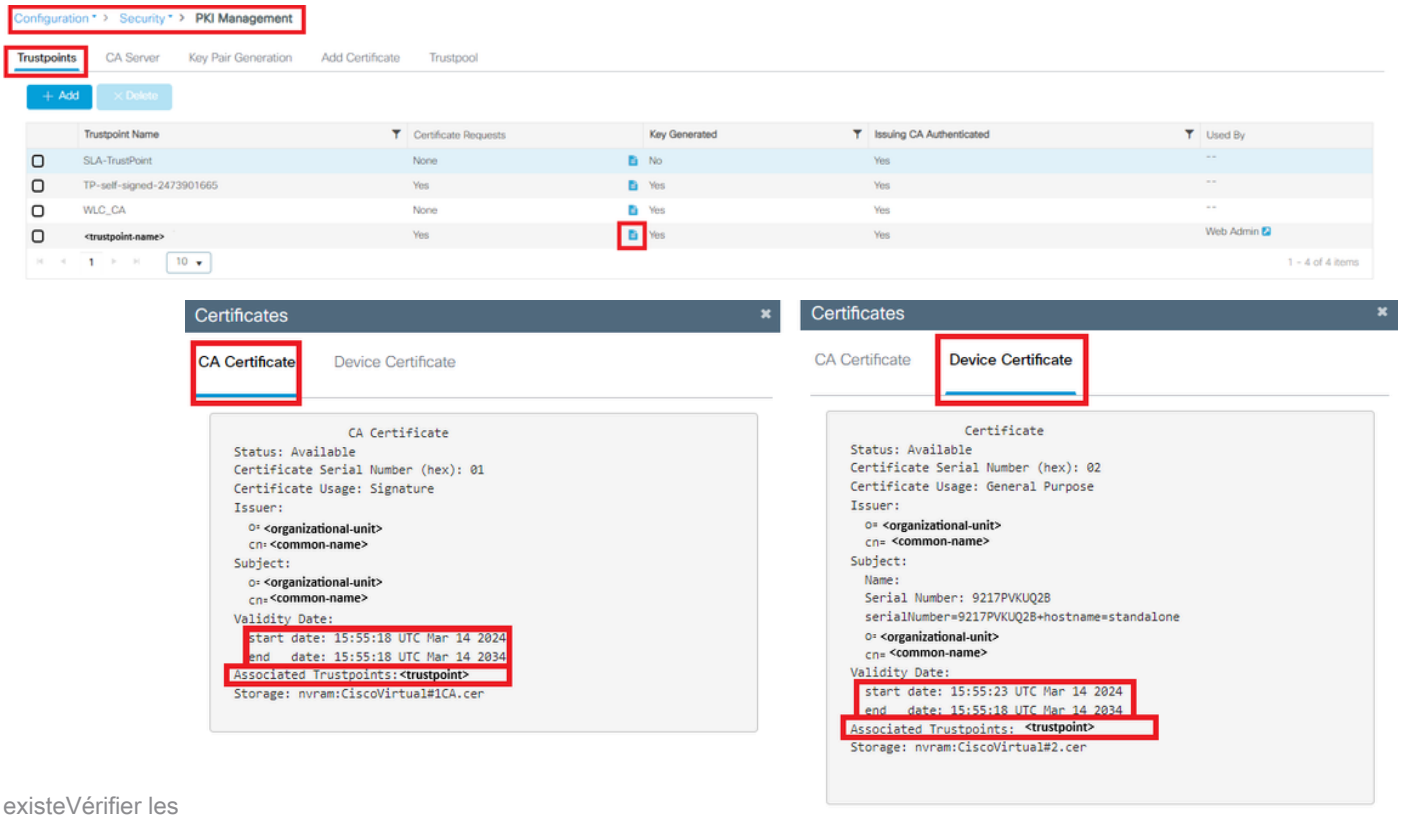
Deuxièmement : assurez-vous que le certificat est correctement téléchargé sur le WLC et que sa date de validité est correcte.

À partir de la GUI :

1. Accédez à Configuration > Security > PKI Management
2. Rechercher le point de confiance dans la liste
3. Vérifiez ses détails



Vérifier que le point de confiance



existeVérifier les
détails du point de confianceVérifier la validité du point de confiance

À partir de la CLI :

<#root>

```
WLC# show crypto pki certificate
```

[<certificate>]

```
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=<Common Name>
    o=<Organizational Unit>
  Subject:
    cn=<Common Name>
    o=<Organizational Unit>
  Validity Date:
```

start date: <start-date>

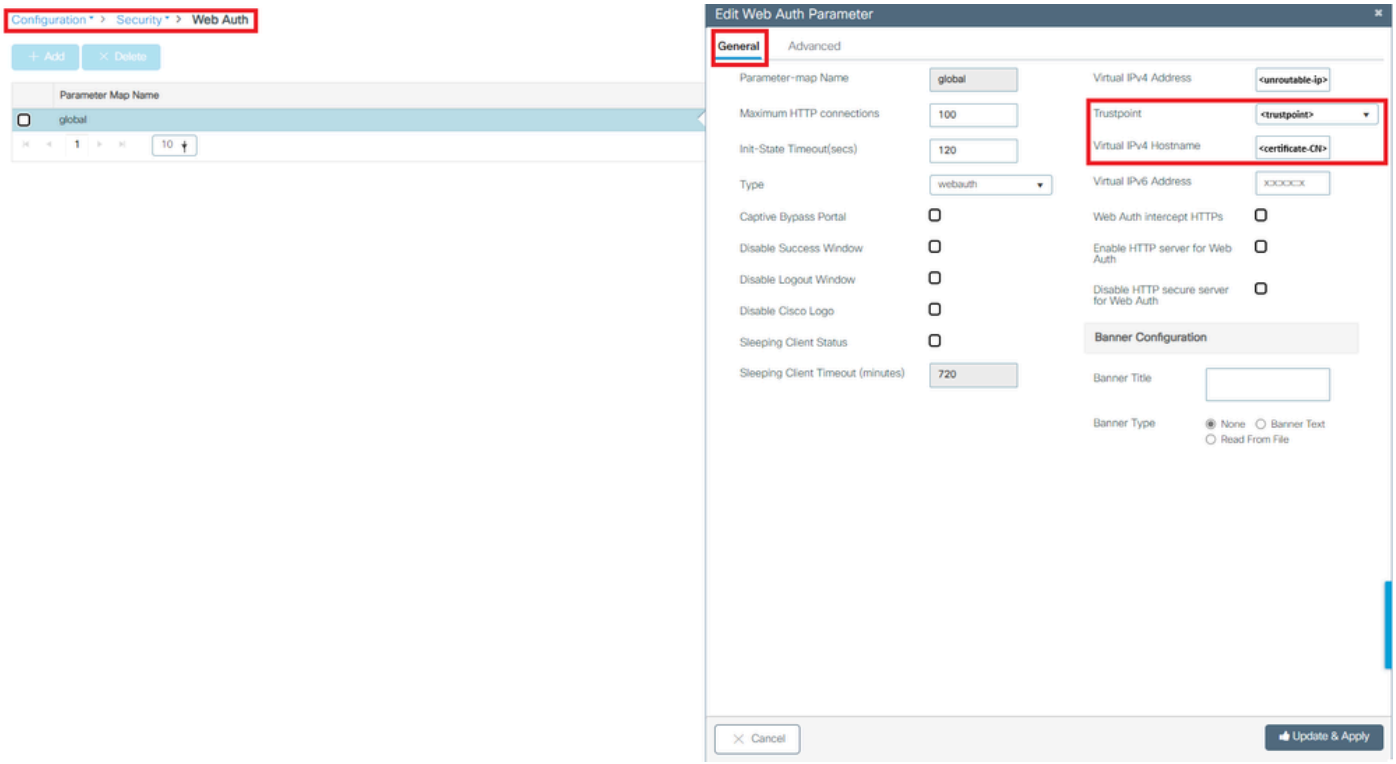
end date: <end-date>

Associated Trustpoints: <trustpoint>

Troisièmement : assurez-vous que le certificat correct sélectionné pour une utilisation sur la carte de paramètre WebAuth et que le nom d'hôte IPv4 virtuel correspond au nom commun (CN) dans le certificat.

À partir de la GUI :

1. Accédez à Configuration > Security > Web Auth.
2. Sélectionnez le mappage de paramètre utilisé dans la liste.
3. Vérifiez que le point de confiance et le nom d'hôte IPv4 virtuel sont corrects.



Vérifier le point de confiance et le nom d'hôte IPv4 virtuel

À partir de la CLI :

<#root>

```
WLC# show run | section paramter-map type
```

<type> <name>

```
parameter-map type
```

<type> <name>

```
[...]
virtual-ip ipv4
```

<unroutable-ip> <certificate-common-name>

```
trustpoint
```

<trustpoint>

Informations connexes

- Configurer l'authentification Web locale
- Authentification Web (EWC)
- Personnalisation du portail d'authentification Web sur le WLC Catalyst 9800
- Générer et télécharger des certificats CSR sur les WLC Catalyst 9800
- Configuration des interfaces virtuelles

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.