Veelvoorkomende problemen met LWA op 9800 WLC's oplossen

Inhoud

Inleiding

Dit document beschrijft de gebruikelijke problemen met clients die verbinding maken met een WLAN met lokale webverificatie (LWA).

Voorwaarden

Vereisten

Cisco raadt u aan een basiskennis te hebben van:

- Cisco draadloze LAN-controller (WLC) 9800 Series.
- Algemeen begrip van Local Web Verification (LWA) en de configuratie ervan.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversies:

- Catalyst 9800-CL WLC
- Cisco access point 9120AXI
- 980 WLC Cisco IOS® XE versie 17.9.3

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

LWA is een type WLAN-verificatie dat op de WLC kan worden geconfigureerd, waar de eindclient die probeert verbinding te maken, nadat ze WLAN in de lijst hebben geselecteerd, een portal aan de gebruiker voorstelt. In dit portal kan de gebruiker een gebruikersnaam en wachtwoord invoeren (afhankelijk van de geselecteerde configuratie) om de verbinding met het WLAN te voltooien.

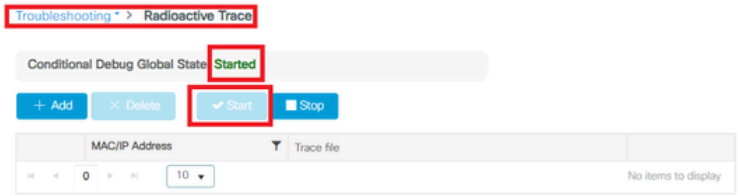
Raadpleeg de configuratiehandleiding voor lokale webverificatie configureren voor meer informatie over het configureren van de LWA op de 9800 WLC.

Radioactieve (RA) sporen op de 9800 WLC

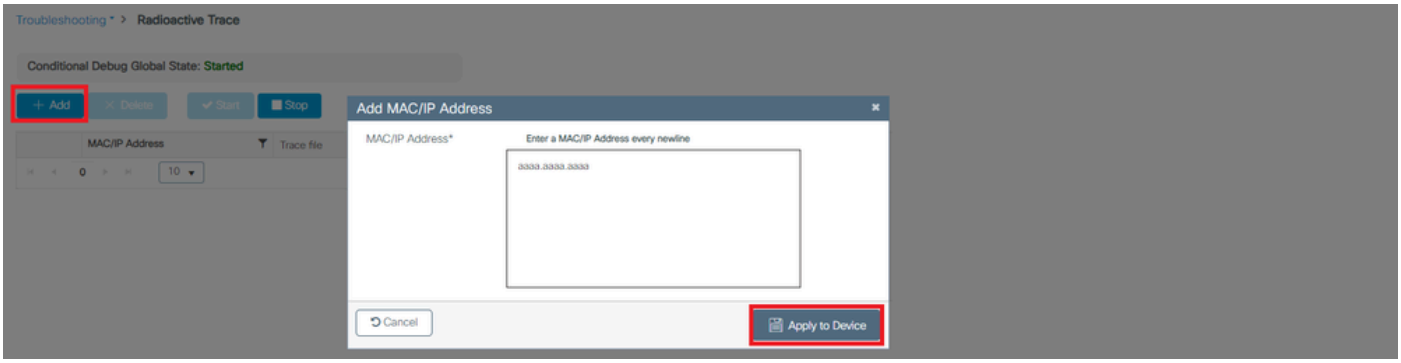
Radioactieve sporen zijn een geweldige tool voor probleemoplossing die kan worden gebruikt bij het oplossen van problemen met verschillende problemen met de WLC en client connectiviteit. Om RA-sporen te verzamelen, voert u de volgende stappen uit:

Via de GUI:

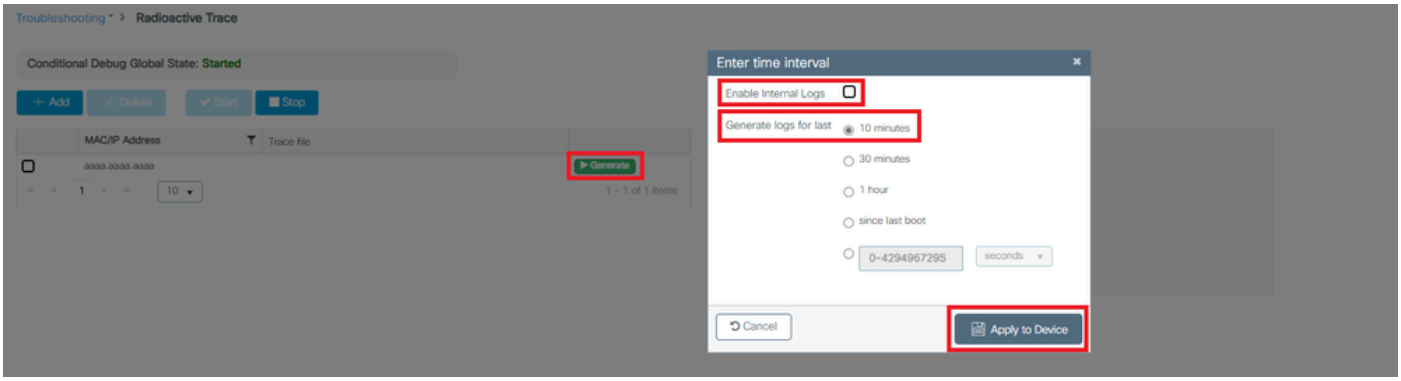
1. Ga naar Problemen oplossen > Radioactief spoor.
2. Klik op Start om voorwaardelijke debug wereldwijde status in te schakelen.
3. Klik op + Toevoegen. Er wordt een pop-upvenster geopend. Voer het MAC-adres van de client in. Elke MAC-adresindeling wordt geaccepteerd (abb.ccdd.eeff, AABB.cdd.EEEE, aa:bb:cc:dd:ee:ff, of AA:BB:CC:DD:EE:FF). Klik vervolgens op Toepassen op apparaat.
4. Laat de klant het probleem 3 of 4 keer reproduceren.
5. Klik nadat het probleem is gereproduceerd op Generate.
6. Er wordt een nieuw pop-upvenster geopend. Genereer logbestanden voor de laatste 10 minuten. (In dit geval is het niet nodig de interne logbestanden in te schakelen). Klik op Toepassen op apparaat en wacht tot het bestand verwerkt is.
7. Nadat het bestand is gegenereerd, klikt u op het pictogram Downloaden.



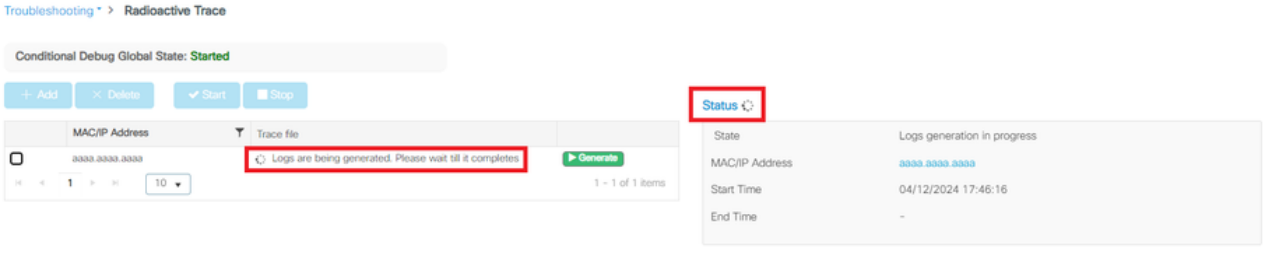
Voorwaardelijke debugging inschakelen



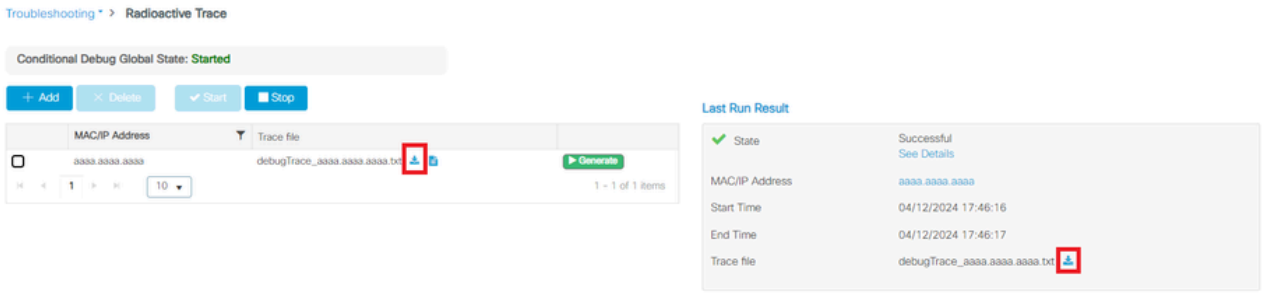
Voeg een client-MAC-adres toe



Logbestanden voor de laatste 10 minuten genereren



Wacht totdat het bestand is



gegenereerdDownload het bestand

Van de CLI:

<#root>

```
WLC# debug wireless mac
```

<mac-address>

```
 monitor-time 600
```

Er wordt een nieuw bestand in de bootflash gegenereerd met de naam ra_trace_MAC_<mac-address>_HMMSS.XXX_timezone_DayWeek_Month_Day_year.log

<#root>

```
WLC# more bootflash:
```

ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Kopieert het bestand naar een externe server voor 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
```

Raadpleeg voor meer informatie over Radioactive Tracing deze link.

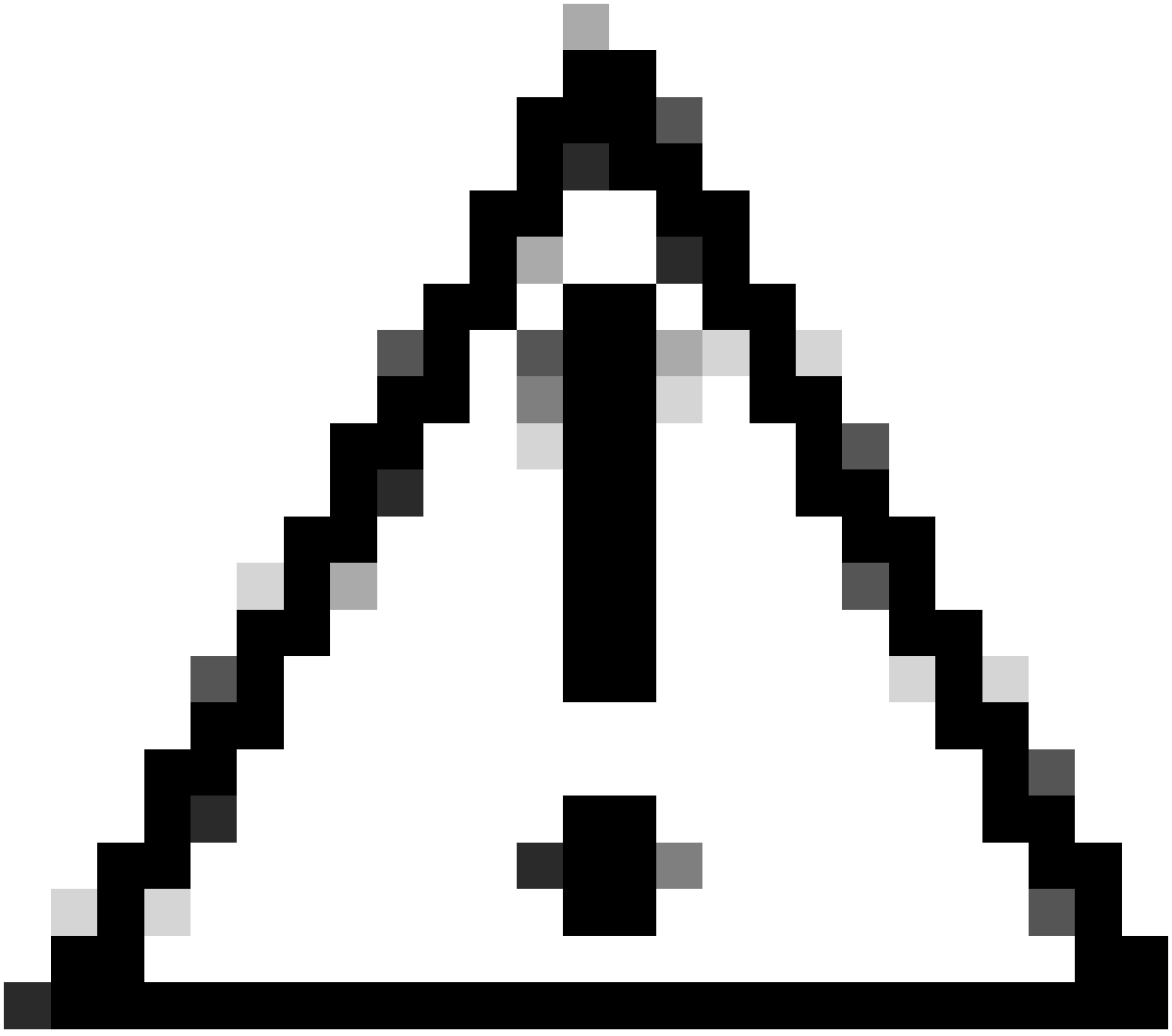
Verwachte doorloop

Verwijs naar de informatie om het werkende scenario voor LWA te begrijpen.

Stappen die de klant ondergaat vanuit het perspectief van de klant

1. End-client associaties met het WLAN.
2. De client krijgt een IP-adres toegewezen.
3. Portal wordt gepresenteerd aan de eindclient.
4. End-client voert aanmeldingsgegevens in.
5. End-client is geverifieerd.
6. De eindclient is in staat om te surfen op internet.

Stages de client ondergaat vanuit het WLC-perspectief



Waarschuwing: veel logs uit het spoor van Radio Active (RA) zijn weggelaten voor eenvoudigheids doeleinden.

End-client associaties met het 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

L2-verificatie

<#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

Cliënt krijgt een IP-adres toegewezen

<#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

L3-verificatie

<#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
```

Cliënt krijgt een IP-adres

<#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

Poortverwerking

<#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

WLC-procesinformatie die moet worden toegepast op de Connecting End-client

<#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 past gebruikersprofiel toe op de Connected End-client

<#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'
```

Web verificatie is voltooid

```
<#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
```

AAA-kenmerken toegepast op eindclient

```
<#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
" ]
```

End-client bereikt run state

```
<#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
```

Gemeenschappelijke scenario's voor probleemoplossing

Verificatiefouten

Overwegingen

- Getoonde portal zegt "Verificatie mislukt" na het invoeren van juiste referenties.
- WLC toont client in status "Web Auth Pending".
- De spatpagina van het begin wordt opnieuw getoond aan de gebruiker.

WLC RA-sporen

<#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]

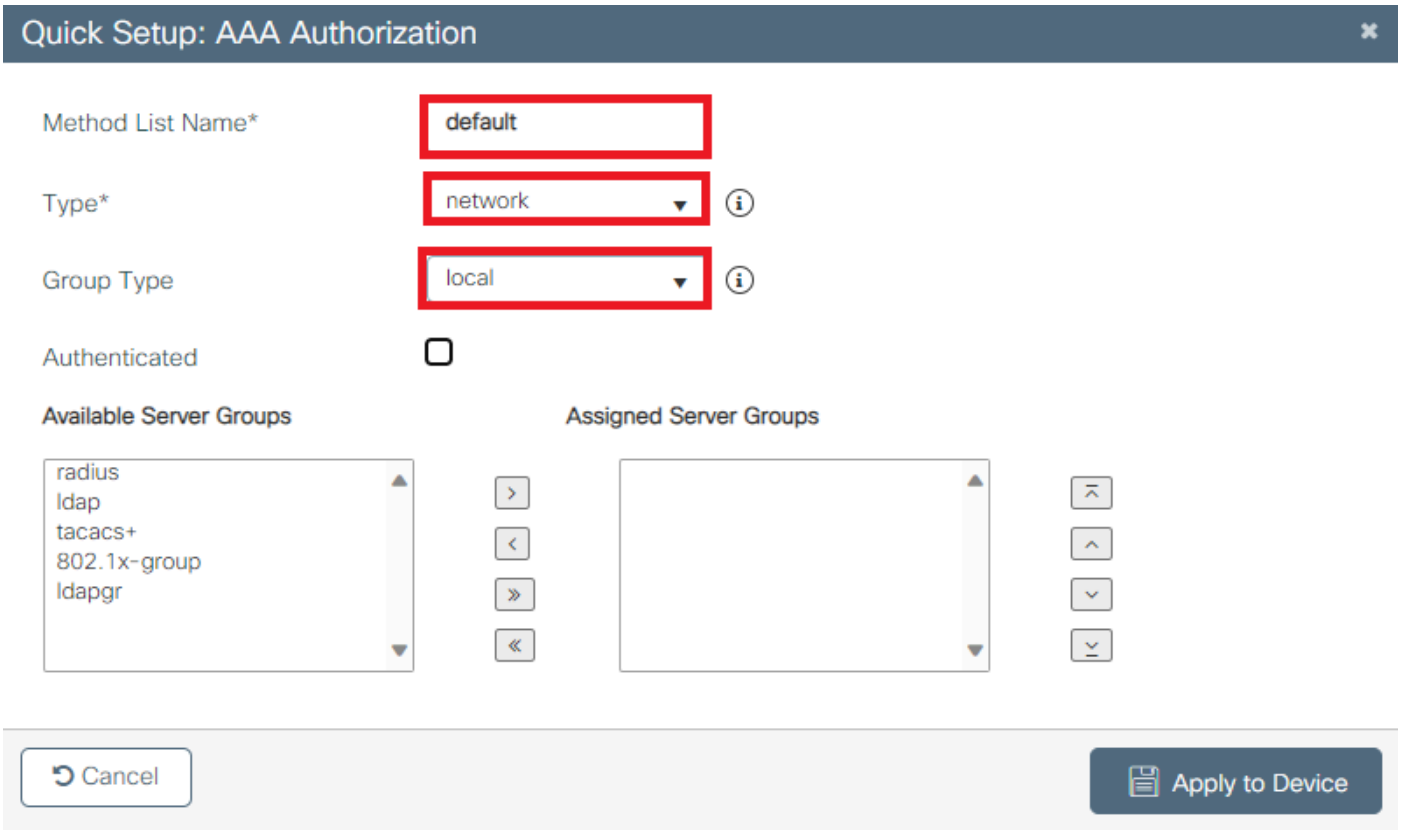
```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

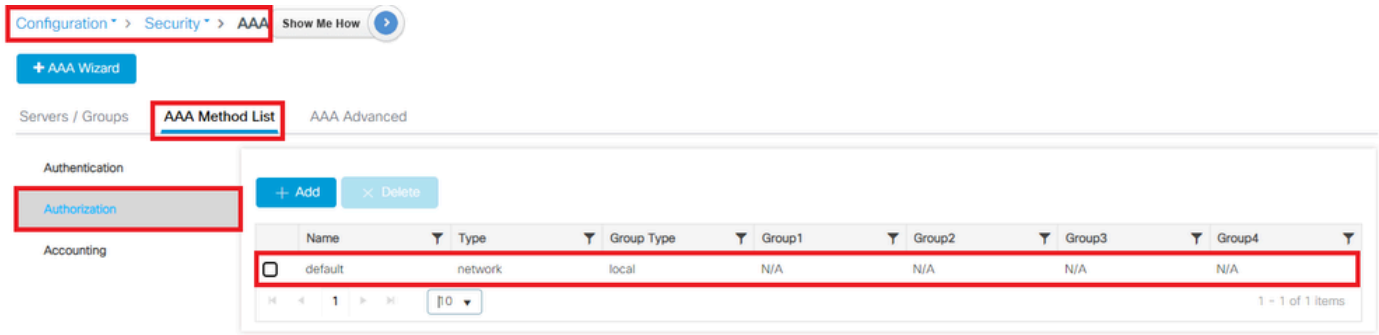
Aanbevolen oplossingen

Zorg ervoor dat de standaard AAA Method List voor netwerkautorisatie op de WLC-configuratie bestaat.

Via de GUI:

1. Ga naar Configuratie > Beveiliging > AAA > AAA-methodelijst > Autorisatie. Klik op + Toevoegen.
2. Configureer het als volgt:
    1. Naam methodelijst: standaard
    2. Type: netwerk
    3. Groepstype: lokaal
3. Klik op Toepassen op apparaat.





Van de CLI:

<#root>

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

Portal wordt niet getoond aan de gebruiker maar client verschijnt verbonden

Mogelijk gedrag ervaren van de end-client

- De eindcliënt ziet zijn apparaat als "Verbonden".
- De eindclient ziet de portal niet.

- De eindclient voert geen referenties in.
- De eindclient heeft een IP-adres toegewezen.
- WLC toont de client in "Run"-status.

WLC RA-sporen

De client krijgt een IP-adres toegewezen en wordt onmiddellijk verplaatst naar de status "Run" op de WLC. Gebruikerskenmerken tonen alleen het VLAN dat aan de eindclient is toegewezen.

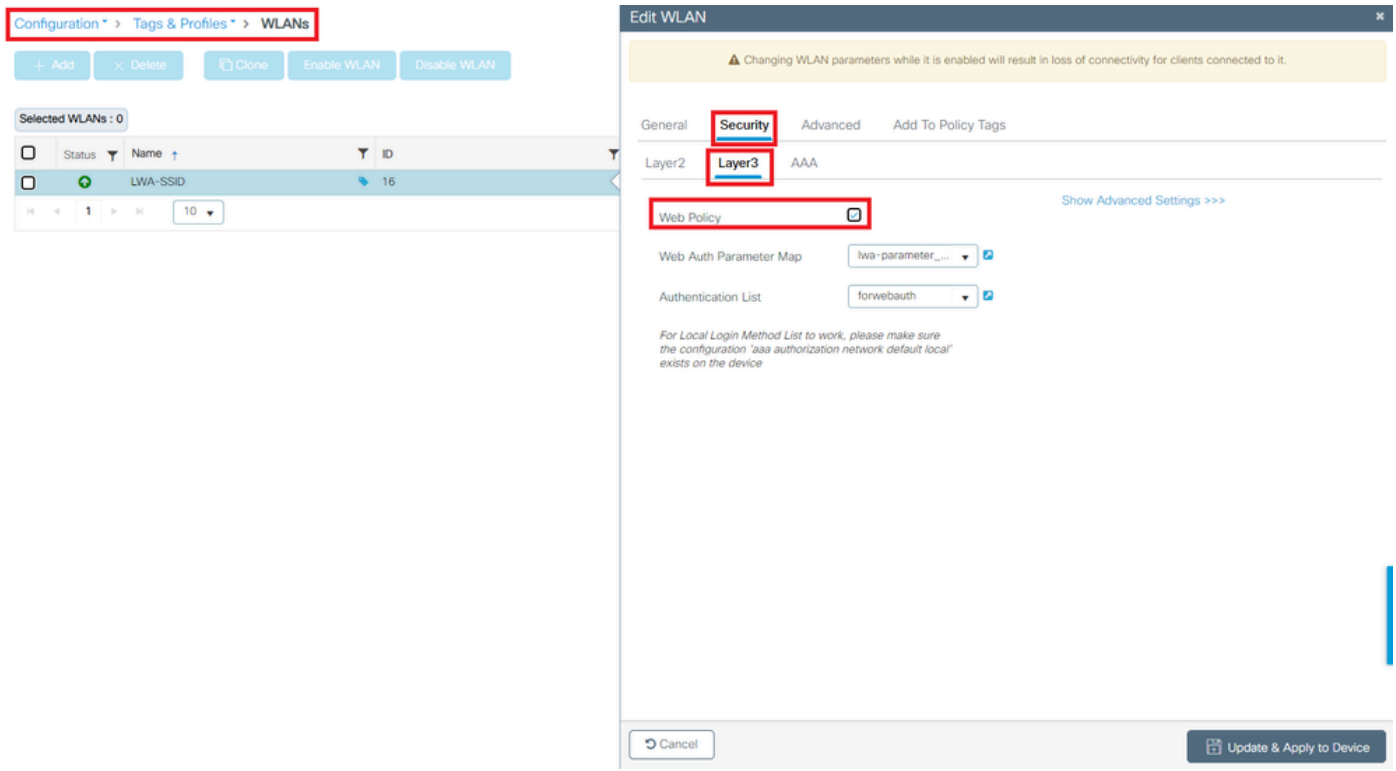
```
<#root>

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
```

Aanbevolen oplossingen

Zorg ervoor dat het webbeleid is ingeschakeld op het WLAN.

Via de GUI:

1. Ga naar Configuratie > Tags & profielen > WLAN’s.
2. Selecteer de WLAN’s.
3. Ga naar Security > Layer 3.
4. Zorg ervoor dat het selectievakje Web Policy is ingeschakeld.



Webbeleid moet worden ingeschakeld

Van de CLI:

<#root>

```
WLC# configure terminal


WLC(config)# wlan
```

<wlan>

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

Portal wordt niet getoond aan de gebruiker en client maakt geen verbinding

Mogelijk gedrag ervaren van de end-client

- End client ziet dat hun apparaat voortdurend probeert verbinding te maken.
- De eindclient ziet de portal niet.
- De eindclient heeft geen IP-adres toegewezen.
- WLC toont de client in "Webauth Pending" staat.

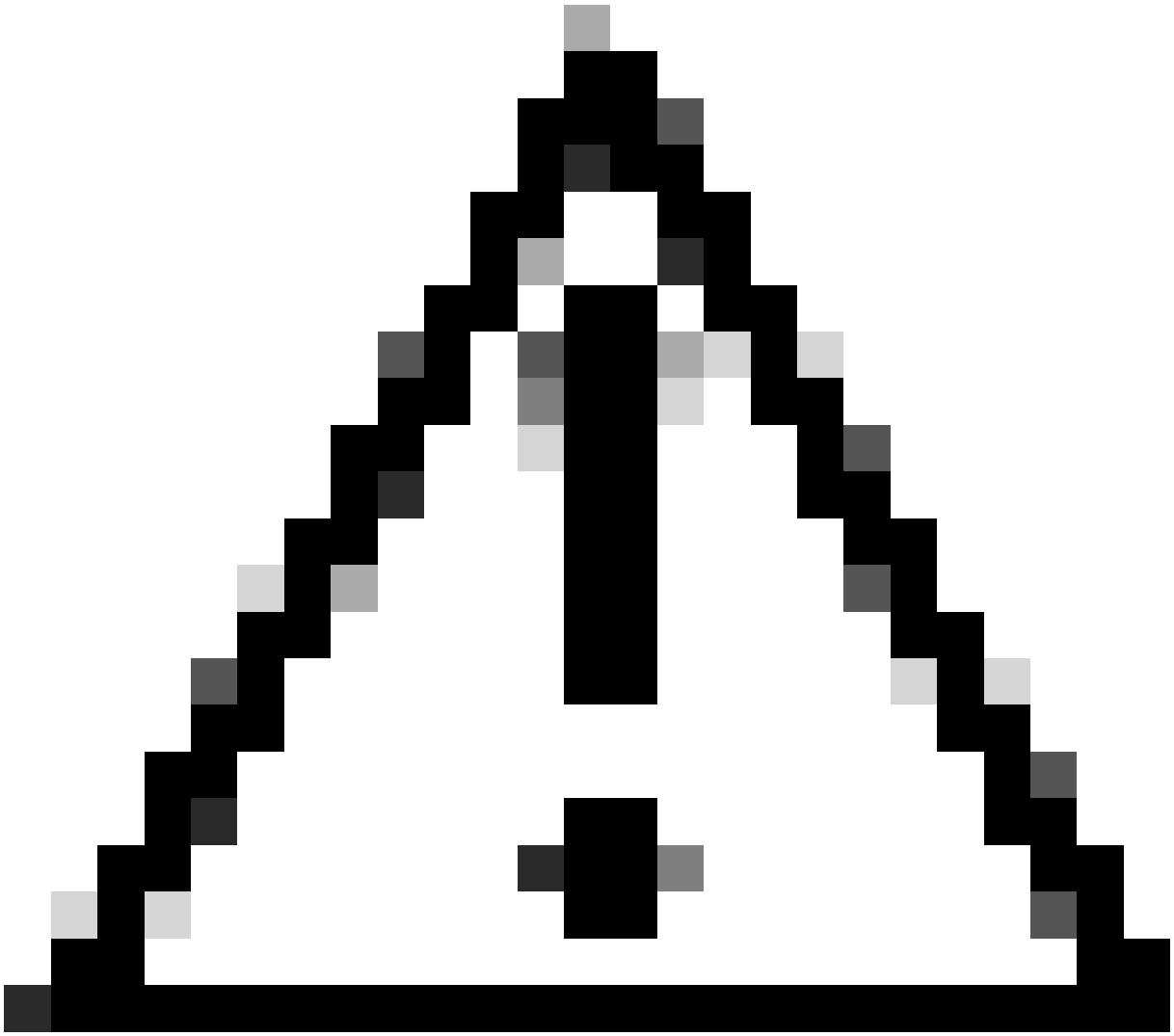
Aanbevolen oplossingen

Schakel de benodigde HTTP-/HTTPS-servers in. Het is nu mogelijk om meer controle te hebben

over welke HTTP/HTTPS-servers moeten worden ingeschakeld om zich volledig aan te passen aan de behoeften van het netwerk. Raadpleeg deze link voor meer informatie over het configureren van HTTP- en HTTPS-aanvragen voor webverificatie omdat er verschillende HTTP-combinaties worden ondersteund; HTTP kan bijvoorbeeld alleen worden gebruikt voor webadmin en HTTP kan worden gebruikt voor webauth.

Beheer van beheerapparaten en webverificatie met zowel HTTP- als HTTPS-toegang via de CLI mogelijk maken:

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



Waarschuwing: als beide servers zijn uitgeschakeld, is er geen toegang tot de grafische gebruikersinterface (GUI) van de WLC.

Eindclients krijgen geen IP-adres

Mogelijk gedrag ervaren van de end-client

- De cliënten van het eind zien hun apparaat voortdurend probeert om een IP adres te krijgen.
- WLC toont de client in de staat "IP Learning".

WLC RA-sporen

Verzoeken tot ontdekking zonder aanbod terug.

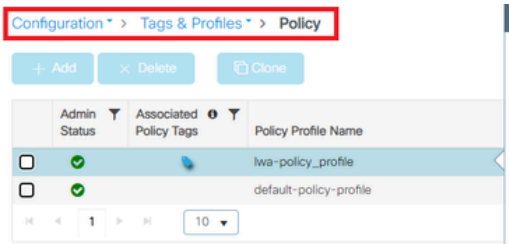
```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
```

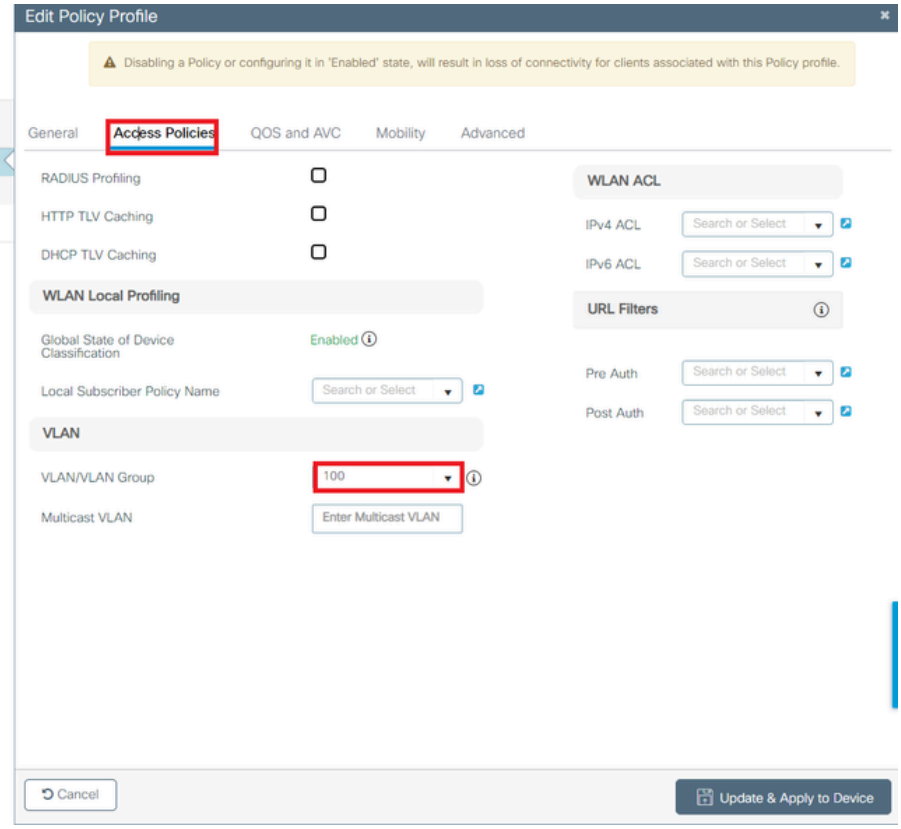
Aanbevolen oplossingen

Eerst: Zorg ervoor dat aan het beleidsprofiel het juiste VLAN is toegewezen.

Via de GUI:

1. Ga naar Configuratie > Tags & profielen > Beleid.
2. Selecteer het gebruikte beleidsprofiel.
3. Ga naar Toegangsbeleid.
4. Selecteer het juiste VLAN.





Van de 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>

Ten tweede: Zorg ervoor dat er een DHCP-pool beschikbaar is voor de gebruiker ergens. Controleer de configuratie en de bereikbaarheid. RA-sporen tonen aan onder welke VLAN DHCP DORA-proces doorgaat. Zorg ervoor dat dit VLAN het juiste VLAN is.

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

Aangepaste portal wordt niet getoond aan de end-client

Mogelijk gedrag ervaren van de end-client

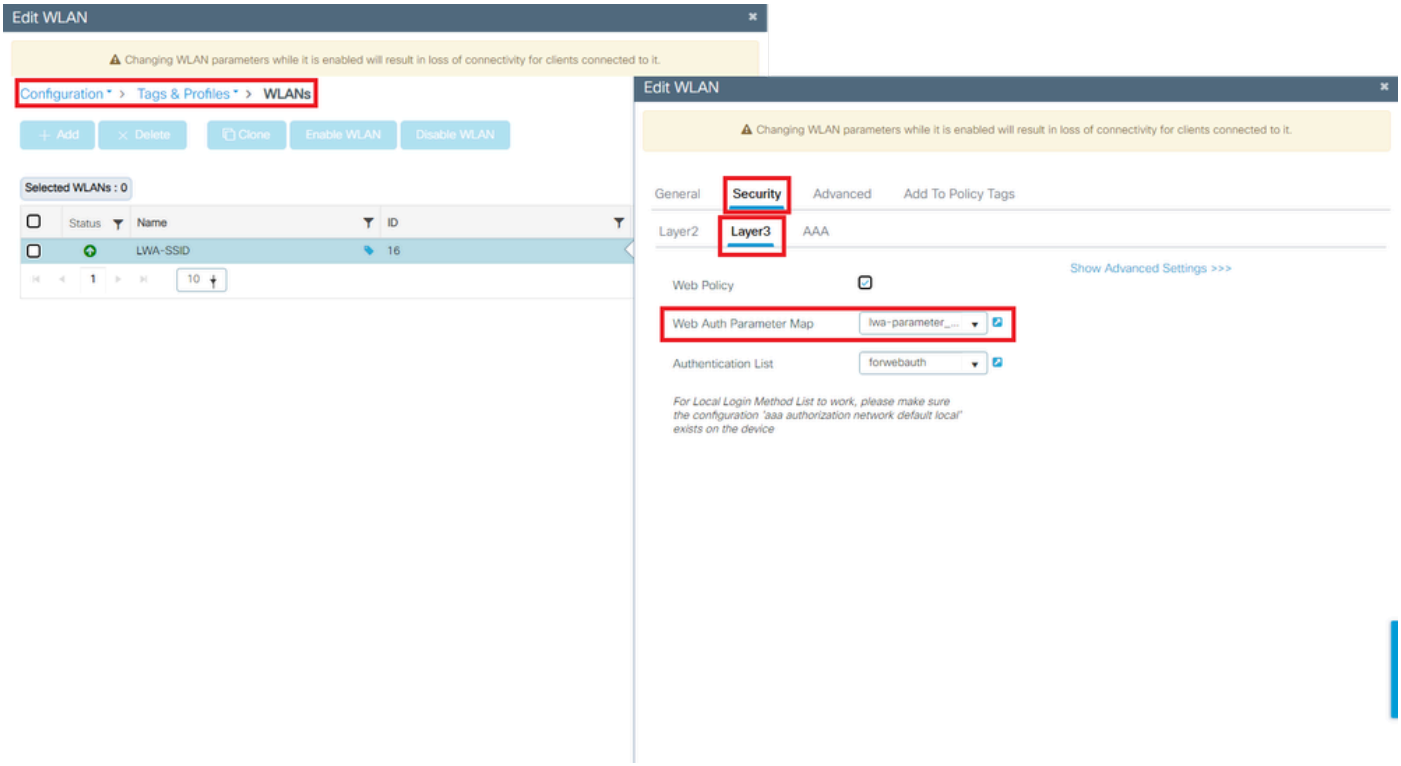
- Het defaultportaal van de WLC wordt gezien.

Aanbevolen oplossingen

Ten eerste: Zorg ervoor dat het WLAN de aangepaste Web Auth Parameter Map gebruikt.

Via de GUI:

1. Ga naar Configuratie > Tags & profielen > WLAN's.
2. Selecteer het WLAN in de lijst.
3. Ga naar Security > Layer 3.
4. Selecteer de aangepaste kaart voor webautorisatieparameters.



Aangepaste parameter map geselecteerd

Van de 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>

Ten tweede: het is belangrijk om op te merken dat de aangepaste download van het webportaal Cisco.com niet werkt met een zeer robuuste en gecompliceerde programmeringsinterface. Het wordt over het algemeen aanbevolen om wijzigingen alleen op CSS-niveau aan te brengen en mogelijk afbeeldingen toe te voegen of te verwijderen. Applets, PHP, modificeer variabelen, React.js, etc. worden niet ondersteund. Als een aangepast portaal niet aan de client wordt getoond, probeer dan de standaard WLC-pagina's te gebruiken en kijk of het probleem kan worden gerepliceerd. Als het portaal met succes wordt gezien, dan is er iets dat niet wordt ondersteund op de aangepaste pagina's die worden verondersteld te worden gebruikt.

Ten derde: Bij gebruik van een EWC (Embedded Wireless Controller) wordt voorgesteld om de CLI te gebruiken om de aangepaste pagina's toe te voegen om ervoor te zorgen dat ze correct worden weergegeven:

<#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
```

Aangepaste portal wordt niet correct weergegeven aan de end client

Mogelijk gedrag ervaren van de end-client

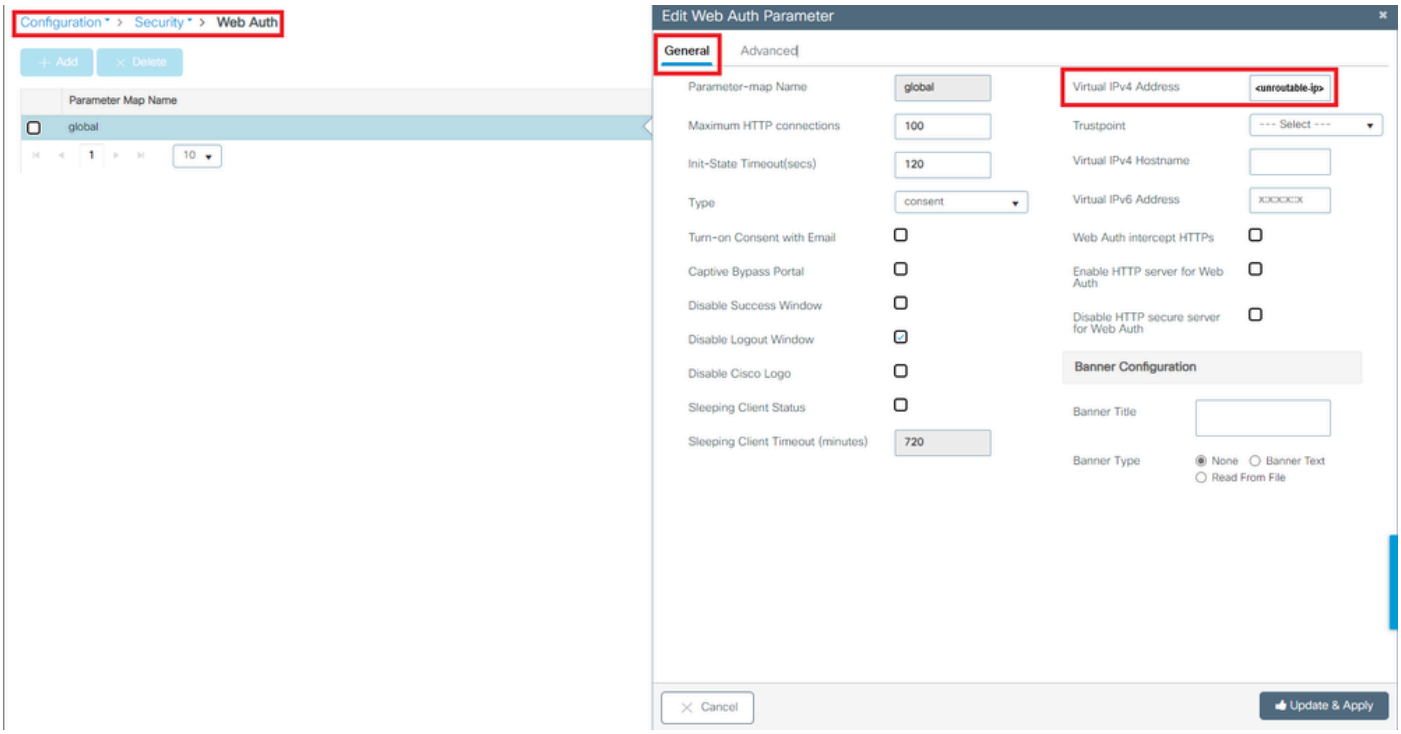
- Het aangepaste portaal wordt niet correct weergegeven (dat wil zeggen dat er geen afbeeldingen worden weergegeven).

Aanbevolen oplossingen

Zorg ervoor dat aan de globale parameterkaart een virtueel IP-adres wordt toegewezen.

Via de GUI:

1. Ga naar Configuratie > Beveiliging > Webautorisatie.
2. Selecteer de globale parameterkaart van de lijst.
3. Voeg een niet-routeerbaar virtueel IP-adres toe.



Virtueel IP-adres op wereldwijde parameterkaart ingesteld op een onrouteerbaar IP-adres

Van de CLI:

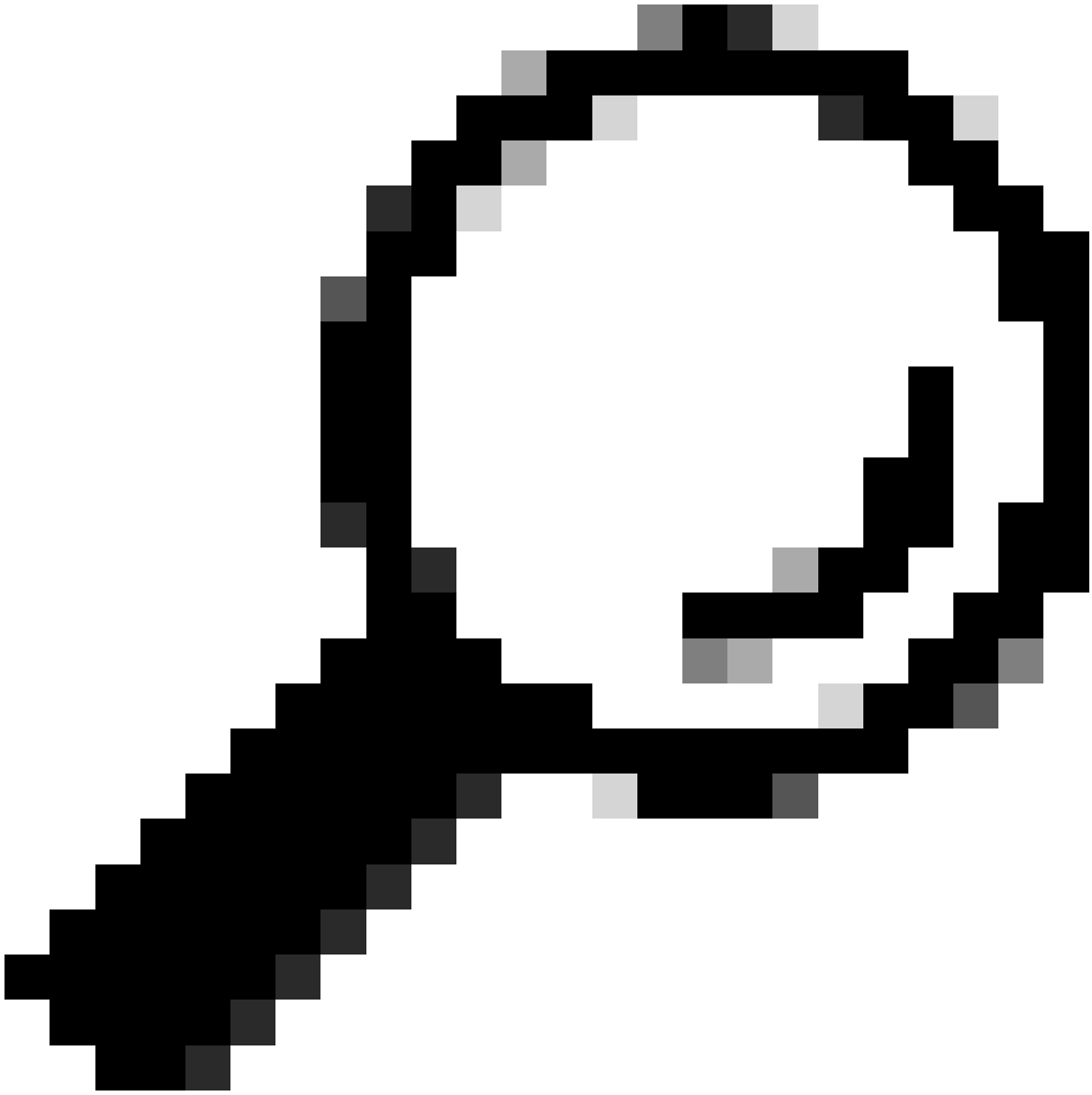
<#root>

```
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>



Tip: Het virtuele IP-adres dient als het omleidingsadres voor de inlogpagina voor webverificatie. Geen ander apparaat op het netwerk moet hetzelfde IP hebben, het mag niet worden toegewezen aan een fysieke poort en het mag niet voorkomen op een routeringstabel. Daarom wordt aanbevolen om het virtuele IP te configureren als een niet-routeerbaar IP-adres, alleen de IP-adressen die zich op de RFC5737 bevinden kunnen worden gebruikt.

Portal zegt dat "Uw verbinding is niet veilig/verifieer handtekening mislukt"

Mogelijk gedrag ervaren van de end-client

- Bij het openen van het portaal ziet de client een fout die zegt dat de verbinding niet veilig is.
- Verwacht wordt dat het portaal een certificaat gebruikt.

Wat te weten

Als het portaal naar verwachting wordt weergegeven onder HTTPS, betekent dit dat het een SSL (Secure Socket Layer) certificaat moet gebruiken. Dit certificaat moet worden afgegeven door een certificeringsinstantie van een derde partij (CA) om te valideren dat het domein echt is; vertrouwen geven aan eindklanten bij het invoeren van hun referenties en/of het bekijken van de portal. Raadpleeg dit document voor het uploaden van een certificaat naar de WLC.

Aanbevolen oplossingen

Ten eerste: herstart de gewenste HTTP/HTTPS-services. Het is nu mogelijk om meer controle te hebben over welke HTTP/HTTPS-servers moeten worden ingeschakeld om zich volledig aan te passen aan de behoeften van het netwerk. Raadpleeg deze link voor meer informatie over het configureren van HTTP- en HTTPS-aanvragen voor webverificatie.

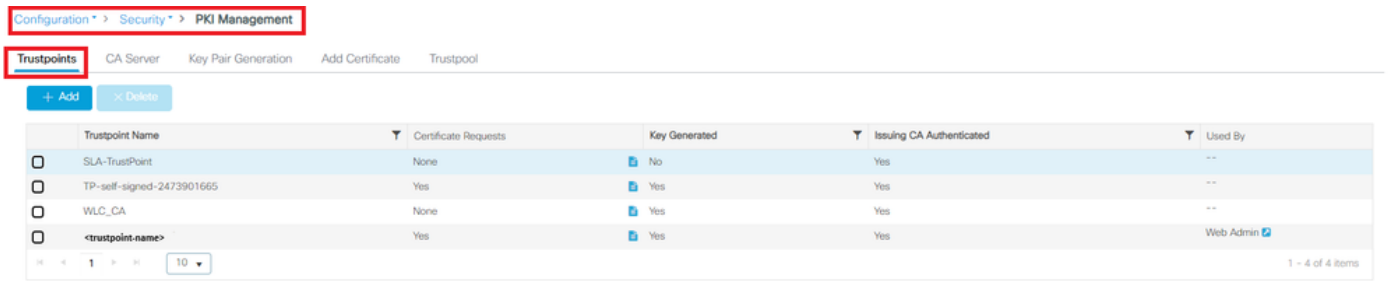
Van de CLI:

```
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
```

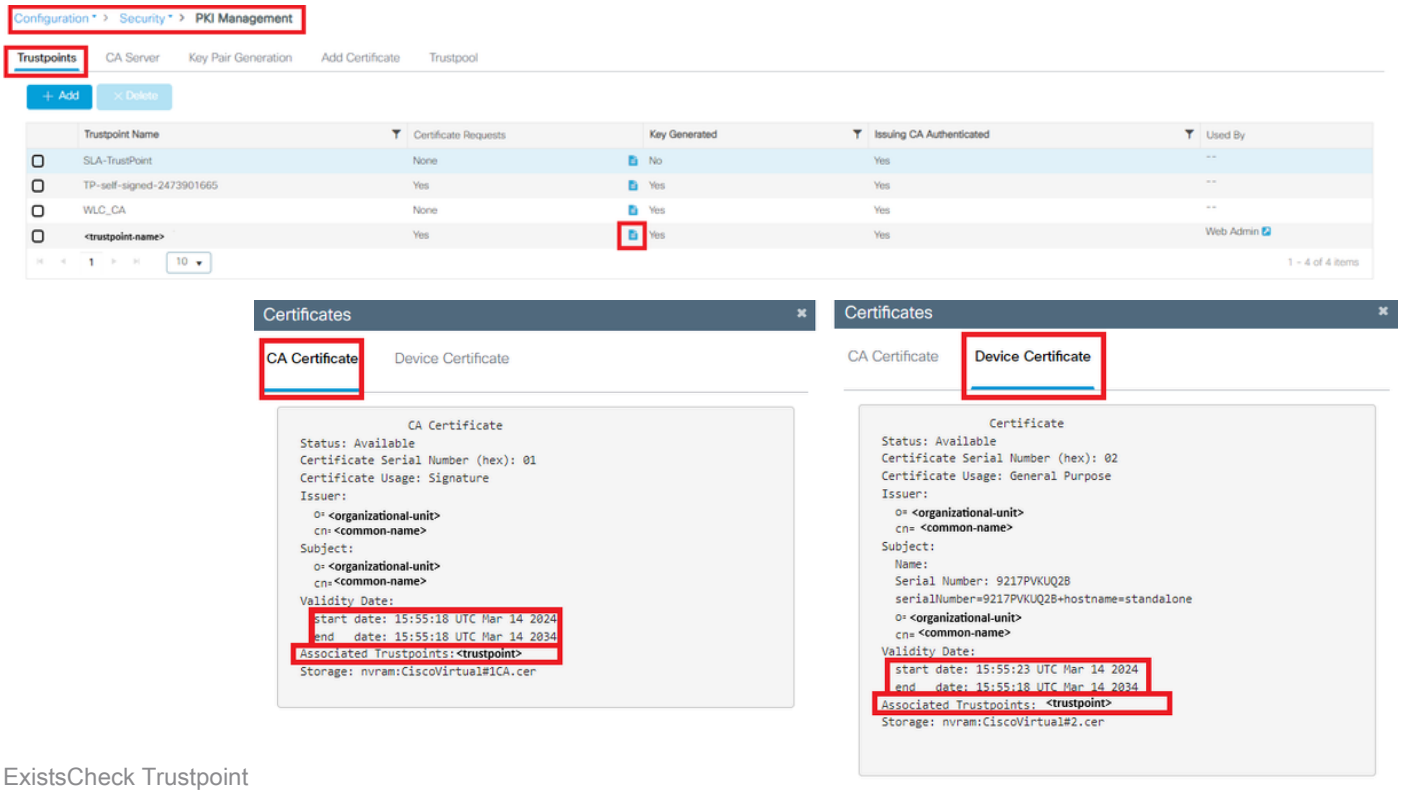
Ten tweede: Zorg ervoor dat het certificaat correct geüpload is naar de WLC en dat de geldigheidsdatum correct is.

Via de GUI:

1. Ga naar Configuratie > Beveiliging > PKI-beheer
2. Zoek naar het Trustpoint op de lijst
3. Controleer de details



Controleer de Trustpoint



ExistsCheck Trustpoint
DetailsCheckTrustpoint validiteit

Van de 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>

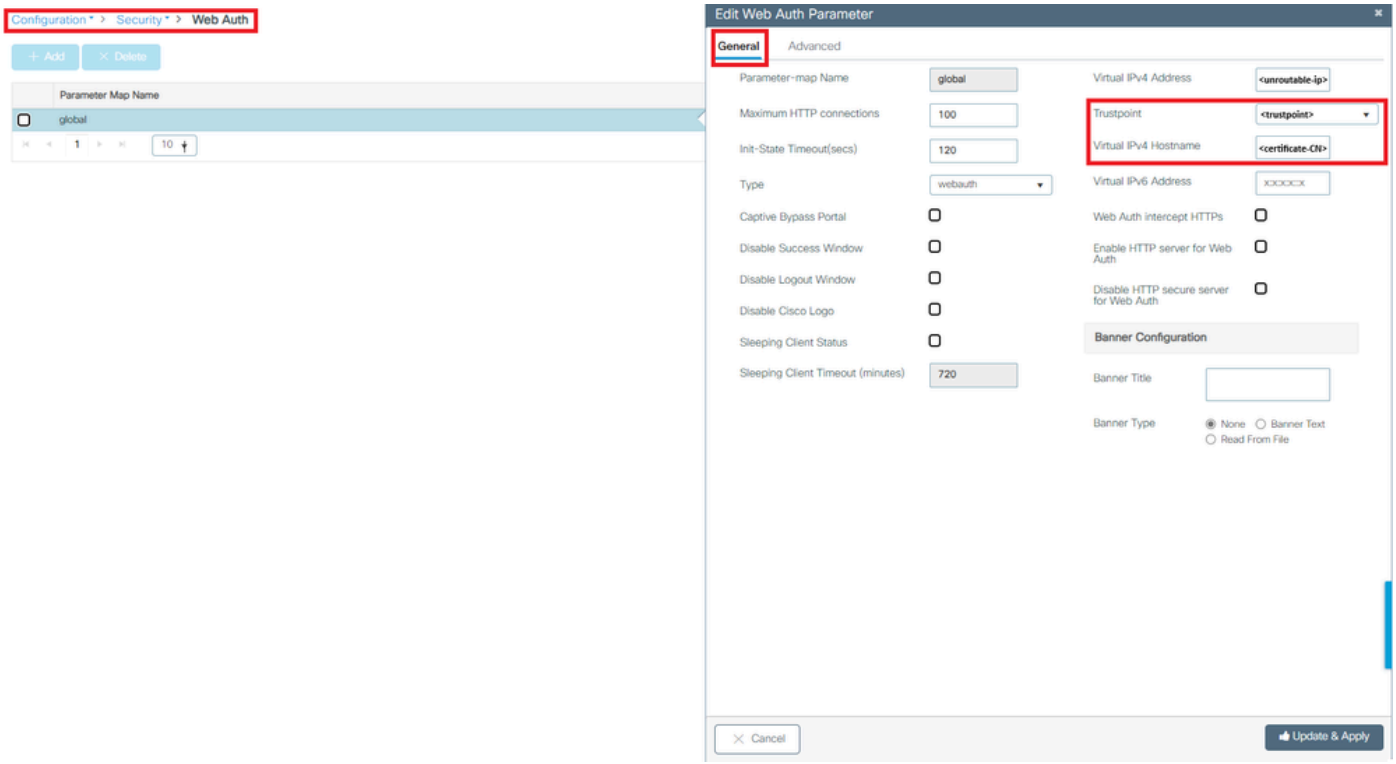
end date: <end-date>

Associated Trustpoints: <trustpoint>

Ten derde: Zorg ervoor dat het juiste certificaat geselecteerd is voor gebruik op de WebAuth parameterkaart en dat de virtuele IPv4 Hostname overeenkomt met de algemene naam (CN) in het certificaat.

Via de GUI:

1. Ga naar Configuratie > Beveiliging > Webautorisatie.
2. Selecteer de gebruikte parameterkaart in de lijst.
3. Controleer of het trustpoint en de virtuele IPv4 Hostname correct zijn.



Controleer Trustpoint en cirkelvormige IPv4-hostnaam

Van de 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>

Gerelateerde informatie

- Lokale webverificatie configureren
- Webgebaseerde verificatie (EWC)
- Pas de webverificatieportal op Catalyst 9800 WLC aan
- CSR-certificaten genereren en downloaden op Catalyst 9800 WLC's
- Virtuele interfaces configureren

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.