

Externe webverificatie op de 9800 WLC configureren en problemen oplossen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Instellingen webparameter configureren](#)

[Samenvatting van CLI-configuratie:](#)

[AAA-instellingen configureren](#)

[Beleid en tags configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Altijd-aan-traceren](#)

[Voorwaardelijke debugging en radio actieve tracering](#)

[Ingesloten pakketvastlegging](#)

[Probleemoplossing aan cliëntzijde](#)

[Probleemoplossing voor HAR-browser](#)

[Packet Capture voor cliëntzijde](#)


[Voorbeeld van een succesvolle poging](#)

Inleiding

Dit document beschrijft hoe u externe webverificatie (EWA) kunt configureren en oplossen op een Catalyst 9800 draadloze LAN-controller (WLC).

Voorwaarden

Dit document veronderstelt dat de Webserver behoorlijk wordt gevormd om externe communicatie toe te staan en de Web-pagina wordt behoorlijk gevormd om alle noodzakelijke parameters voor WLC te verzenden om de gebruiker voor authenticatie te verklaren en cliëntzittingen te bewegen om staat in WERKING te stellen.

 **Opmerking:** Aangezien externe toegang tot bronnen door de WLC wordt beperkt via toegangslijsten, moeten alle scripts, lettertypen, afbeeldingen, enzovoort die worden gebruikt

 in de webpagina worden gedownload en lokaal blijven op de webserver.

De noodzakelijke parameters voor gebruikersverificatie zijn:

- **buttonClicked:** Deze parameter moet aan waarde "4" voor WLC worden geplaatst om de actie als authenticatiepoging te ontdekken.
- **redirectUrl:** De waarde in deze parameter wordt door de controller gebruikt om de client naar een specifieke website te leiden na succesvolle verificatie.
- **err_flag:** Deze parameter wordt gebruikt om te wijzen op een aantal fouten zoals onvolledige informatie of onjuiste referenties, op succesvolle authenticaties wordt deze ingesteld op "0".
- **gebruikersnaam:** Deze parameter wordt alleen gebruikt voor webauth parameterkaarten, als parameterkaart is ingesteld om toestemming te verlenen, dan kan deze worden genegeerd. Het moet worden ingevuld met de gebruikersnaam voor de draadloze client.
- **wachtwoord:** Deze parameter wordt alleen gebruikt voor webauth parameterkaarten, als parameterkaart is ingesteld om toestemming te verlenen, dan kan deze worden genegeerd. Het wachtwoord moet worden ingevuld met het wachtwoord van de draadloze client.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hyper Text Markup Language (HTML) webontwikkeling
- Cisco IOS®-XE draadloze functies
- Ontwikkelaarstools voor webbrowsers

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C980-CL WLC Cisco IOS®-XE versie 17.3.3
- Microsoft Windows Server 2012 met mogelijkheden voor Internet Information Services (IIS)
- 2802 en 9117 access points

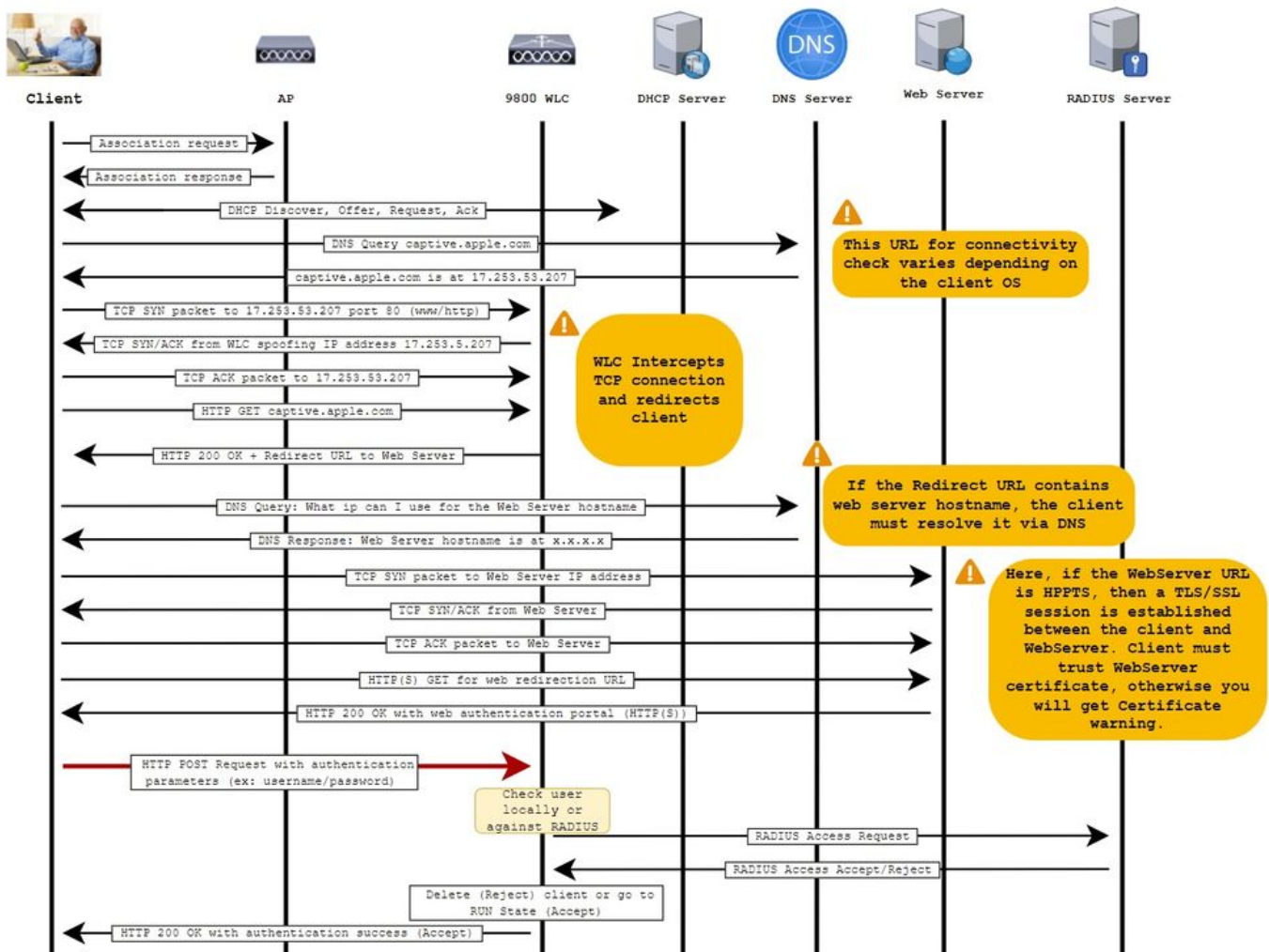
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Externe webverificatie maakt gebruik van een webportal dat buiten WLC wordt gehost op een speciale webserver of multifunctionele servers zoals Identity Services Engine (ISE) die granulaire toegang en beheer van webcomponenten mogelijk maken. De handdruk om met succes aan boord van een client naar een externe web authenticatie WLAN wordt weergegeven in de afbeelding. De afbeelding toont opeenvolgende interacties tussen de draadloze client, WLC, Domain Name System (DNS) server die Uniform Resource Location (URL) oplost en Webserver

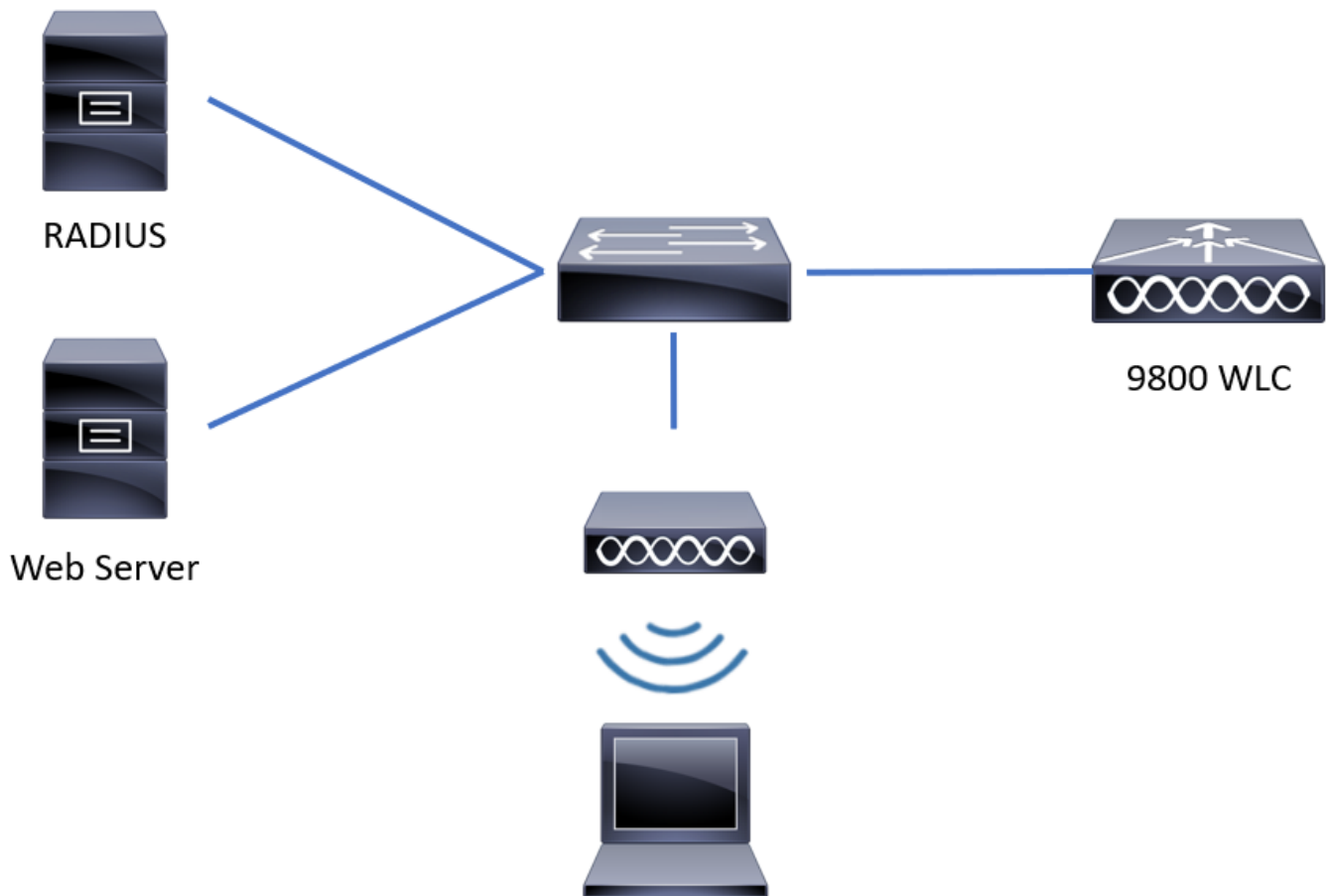
waar WLC gebruikersreferenties lokaal valideert. Deze workflow is handig om eventuele storingscondities op te lossen.

Opmerking: Voor HTTP POST-oproep van client naar WLC, als beveiligde web-authenticatie is ingeschakeld in de parameter-map en als de WLC geen trustpoint heeft dat is ondertekend door een vertrouwde certificeringsinstantie, wordt een security waarschuwing weergegeven in de browser. De client moet deze waarschuwing omzeilen en opnieuw indienen van het formulier accepteren, zodat de controller clientsessies in RUN-staat kan plaatsen.




Configureren

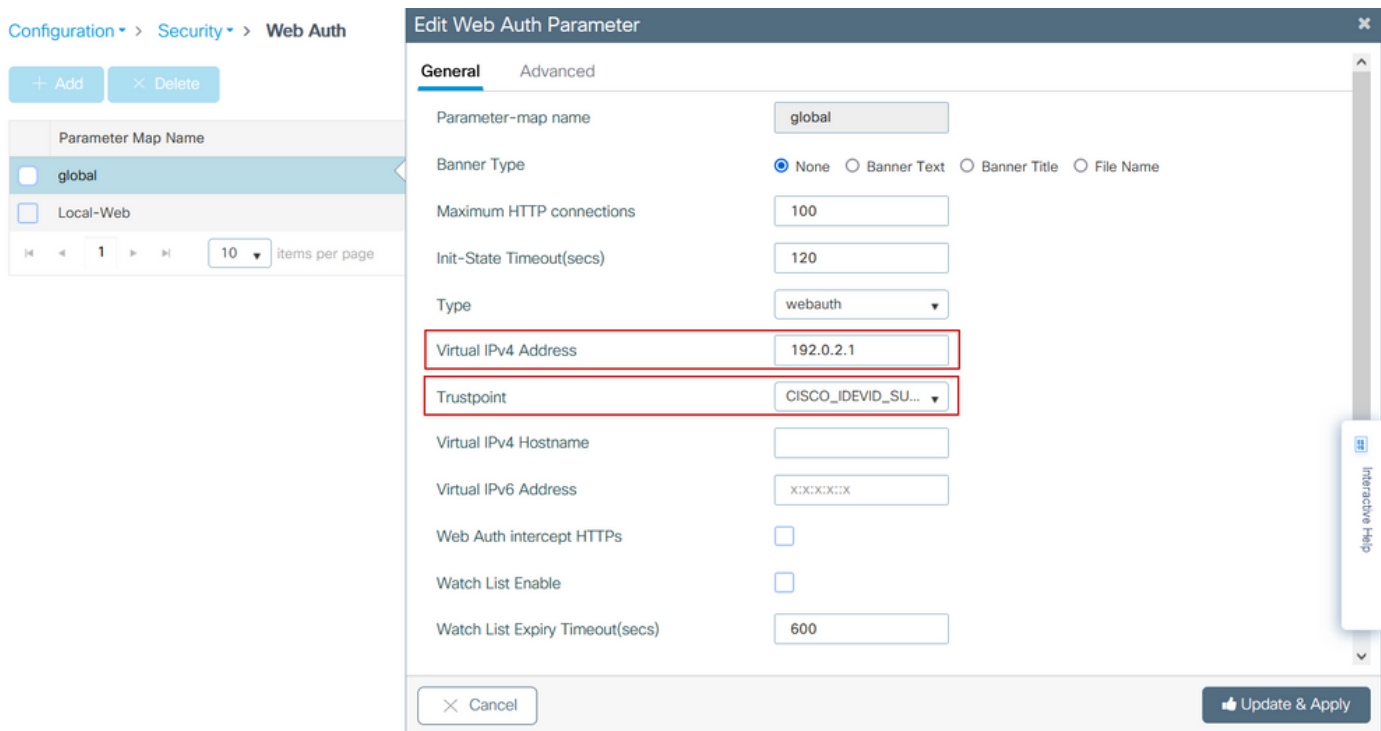
Netwerkdigram



Instellingen webparameter configureren

Stap 1. Navigeer naar Configuration > Security > Web Auth en kies de globale parameterkaart. Controleer of het virtuele IPv4-adres en het virtuele Trustpoint zijn geconfigureerd om de juiste omleidingsfuncties te bieden.

 **Opmerking:** Standaard gebruiken browsers een HTTP-website om een omleidingsproces te starten. Als er een HTTPS-omleiding nodig is, dan moet Web Auth Intercept HTTP worden gecontroleerd. Deze configuratie wordt echter niet aanbevolen, omdat het CPU-gebruik verhoogt.



CLI-configuratie:

```
<#root>
```

```
9800#
```

```
configure terminal
```

```
9800(config)#
```

```
parameter-map type webauth global
```

```
9800(config-params-parameter-map)#
```

```
virtual-ip ipv4 192.0.2.1
```

```
9800(config-params-parameter-map)#
```

```
trustpoint CISCO_IDEVID_SUDI
```

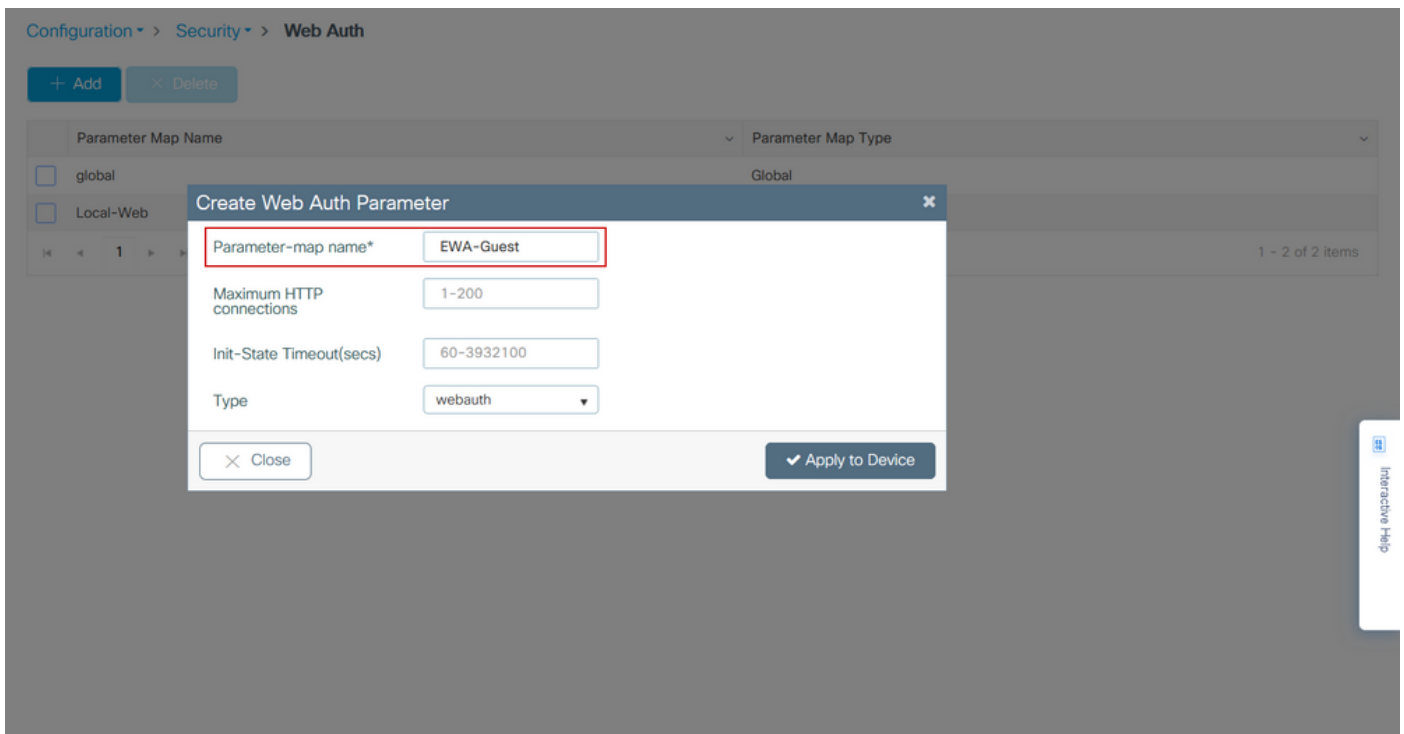
```
9800(config-params-parameter-map)#
```

```
secure-webauth-disable
```

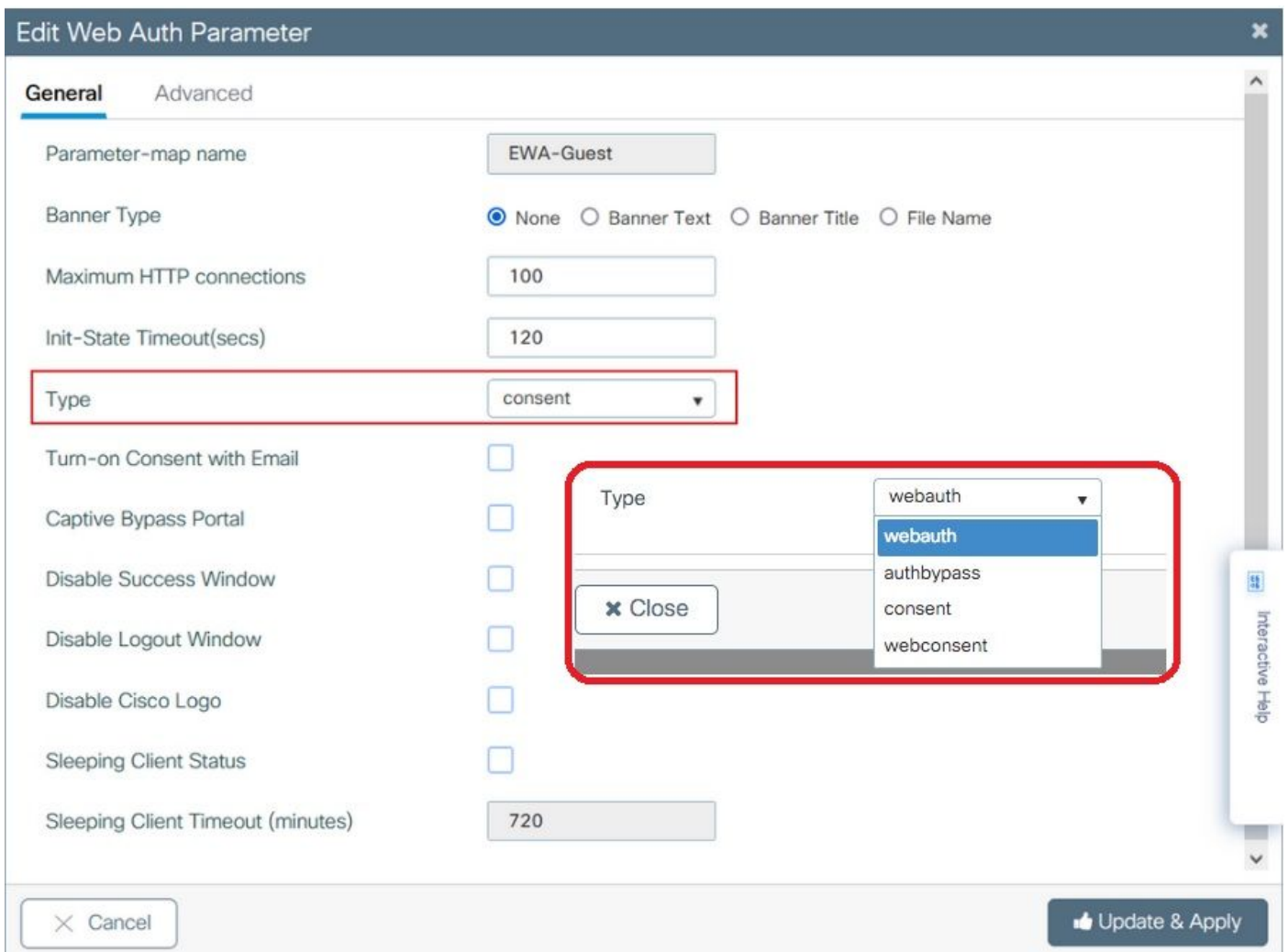
```
9800(config-params-parameter-map)#
```

```
webauth-http-enable
```

Stap 2. Selecteer + Add en vorm een naam voor de nieuwe parameterkaart die aan de externe server richt. U kunt desgewenst het maximale aantal HTTP-verificatiefouten configureren voordat de client wordt uitgesloten en de tijd (in seconden) die een client kan blijven gebruiken voor webverificatie.



Stap 3. Selecteer de nieuwe parameterkaart en configureer op het tabblad Algemeen het verificatietype uit de vervolgkeuzelijst Type.



- Parameter-map naam = Naam toegewezen aan de WebAuth Parameter kaart
- Maximum aantal HTTP-verbindingen = aantal verificatiefouten voordat client wordt uitgesloten
- Init-State Time-out (seconden) = seconden dat een client kan worden ingeschakeld voor webverificatie
- Type = Type webverificatie

webauth	overschrijven	toestemmen	webtoestemming
<p>Username: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="OK"/></p>	<p>De client maakt verbinding met de SSID en krijgt een IP-adres, dan de 9800 WLC controleert of het MAC-adres de lidstaat netwerk, zo ja, wordt het verplaatst om de staat uit te voeren, als dit niet het geval is niet toegestaan om toe te treden.</p> <p>(Het valt niet terug naar web authenticatie)</p>	<p>banner1</p> <p><input checked="" type="radio"/> Accept</p> <p><input type="radio"/> Don't Accept</p> <p><input type="button" value="OK"/></p>	<p>banner login</p> <p><input checked="" type="radio"/> Accept</p> <p><input type="radio"/> Don't Accept</p> <p>Username: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="OK"/></p>

Stap 4. Configureer vanuit het tabblad Advanced de Redirect voor aanmelding en het IPV4-adres van het portal met respectievelijk de specifieke URL van de serversite en het IP-adres.

Edit Web Auth Parameter ✕

General
Advanced

Redirect to external server

Redirect for log-in	http://172.16.80.8/w
Redirect On-Success	<input style="width: 100%;" type="text"/>
Redirect On-Failure	<input style="width: 100%;" type="text"/>
Redirect Append for AP MAC Address	<input style="width: 100%;" type="text" value="ap_mac"/>
Redirect Append for Client MAC Address	<input style="width: 100%;" type="text" value="client_mac"/>
Redirect Append for WLAN SSID	<input style="width: 100%;" type="text" value="ssid"/>
Portal IPv4 Address	<input style="width: 100%;" type="text" value="172.16.80.8"/>
Portal IPv6 Address	<input style="width: 100%;" type="text" value="X::X::X::X"/>
Express WiFi Key Type	<input style="width: 100%;" type="text" value="--- Select ---"/>

Customized page

Login Failed Page	<input style="width: 100%;" type="text"/>
-------------------	-------------------------------------------

✕ Cancel
👍 Update & Apply

? Interactive Help

CLI-configuratie voor stappen 2, 3 en 4:

```

<#root>
9800(config)#
parameter-map type webauth EWA-Guest
9800(config-params-parameter-map)#
type consent
9800(config-params-parameter-map)#
redirect for-login http://172.16.80.8/webauth/login.html
9800(config-params-parameter-map)#
redirect portal ipv4 172.16.80.8
  
```

Stap 5. (Optioneel) WLC kan de extra parameters verzenden via Query String. Dit is vaak nodig om 9800 compatibel te maken met externe portals van derden. In de velden "Redirect Append for AP MAC Address", "Redirect Append for Client MAC Address" en "Redirect Append for WLAN SSID" kunnen extra parameters worden toegevoegd aan de redirect ACL met een aangepaste

naam. Selecteer de nieuwe parameterkaart en navigeer naar het tabblad Geavanceerd, configureer de naam voor de benodigde parameters. De beschikbare parameters zijn:

- AP MAC-adres (in a:bb:cc:dd:ee:ff-indeling)
- MAC-adres client (in aa:bb:cc:dd:ee:ff-indeling)
- SSID-naam

Edit Web Auth Parameter

General **Advanced**

Redirect to external server

Redirect for log-in	<input type="text" value="http://172.16.80.8/we"/>
Redirect On-Success	<input type="text"/>
Redirect On-Failure	<input type="text"/>
Redirect Append for AP MAC Address	<input type="text" value="ap_mac"/>
Redirect Append for Client MAC Address	<input type="text" value="client_mac"/>
Redirect Append for WLAN SSID	<input type="text" value="ssid"/>
Portal IPV4 Address	<input type="text" value="172.16.80.8"/>
Portal IPV6 Address	<input type="text" value="x:x:x:x:x"/>
Express WiFi Key Type	<input type="text" value="--- Select ---"/>

Customized page

Login Failed Page	<input type="text"/>	
Login Page	<input type="text"/>	
Logout Page	<input type="text"/>	
Login Successful Page	<input type="text"/>	

Cancel Update & Apply

Interactive Help

CLI-configuratie:

```
<#root>
```

```
9800(config)#
```

```
parameter-map type webauth EWA-Guest
```

```
9800(config-params-parameter-map)#
```

```
redirect append ap-mac tag ap_mac
```

```
9800(config-params-parameter-map)#
```


```
redirect append wlan-ssid tag ssid
```


```
9800(config-params-parameter-map)#
```

```
redirect append client-mac tag client_mac
```

In dit voorbeeld resulteert de omleiding URL verzonden naar de client in:

```
http://172.16.80.8/webauth/consent.html?switch_url=http://192.0.2.1/login.html&ap_mac=&ssid=&client_mac=
```

 **Opmerking:** wanneer u de IPV4-adresgegevens van het portal toevoegt, wordt er automatisch een ACL toegevoegd die het HTTP- en HTTPS-verkeer van de draadloze clients naar de externe webverificatieserver mogelijk maakt, zodat u geen extra pre-auth ACL hoeft te configureren. Als u meerdere IP-adressen of URL's wilt toestaan, is de enige optie om een URL-filter te configureren zodat alle IP-overeenkomende URL's zijn toegestaan voordat de verificatie plaatsvindt. Het is niet mogelijk om meer dan één portaal IP-adres statisch toe te voegen, tenzij u URL-filters gebruikt.

 **Opmerking:** Global parameter map is de enige waar u virtuele IPv4 en IPv6 adres, Webauth onderscheppen HTTPs, captive bypass portal, watch list activeren en kijken naar lijst vervaltijd instellingen.

Samenvatting van CLI-configuratie:

Lokale webserver

```
parameter-map type webauth <web-parameter-map-name>  
type { webauth | authbypass | consent | webconsent }  
timeout init-state sec 300  
banner text ^Cbanner login^C
```

Externe webserver

```
parameter-map type webauth <web-parameter-map-name>
type webauth
timeout init-state sec 300
redirect for-login <URL-for-webauth>
redirect portal ipv4 <external-server's-IP>
max-http-conns 10
```

AAA-instellingen configureren

Deze configuratie sectie is alleen nodig voor parameters kaarten die zijn geconfigureerd voor ofwel webauth of webconsent authenticatie type.

Stap 1. Navigeer naar Configuration > Security > AAA en selecteer vervolgens AAA Method List. Configureer een nieuwe methodelijst, selecteer + Add en vul de lijstdetails in; zorg ervoor dat Type is ingesteld op "login" zoals in de afbeelding.

Name	Type	Group Type	Group1	Group2	Group3	Group4
default	dot1x	group	radius	N/A	N/A	N/A
alzlab-rad-auth	dot1x	group	alzlab-rad	N/A	N/A	N/A

Method List Name* local-auth

Type* login

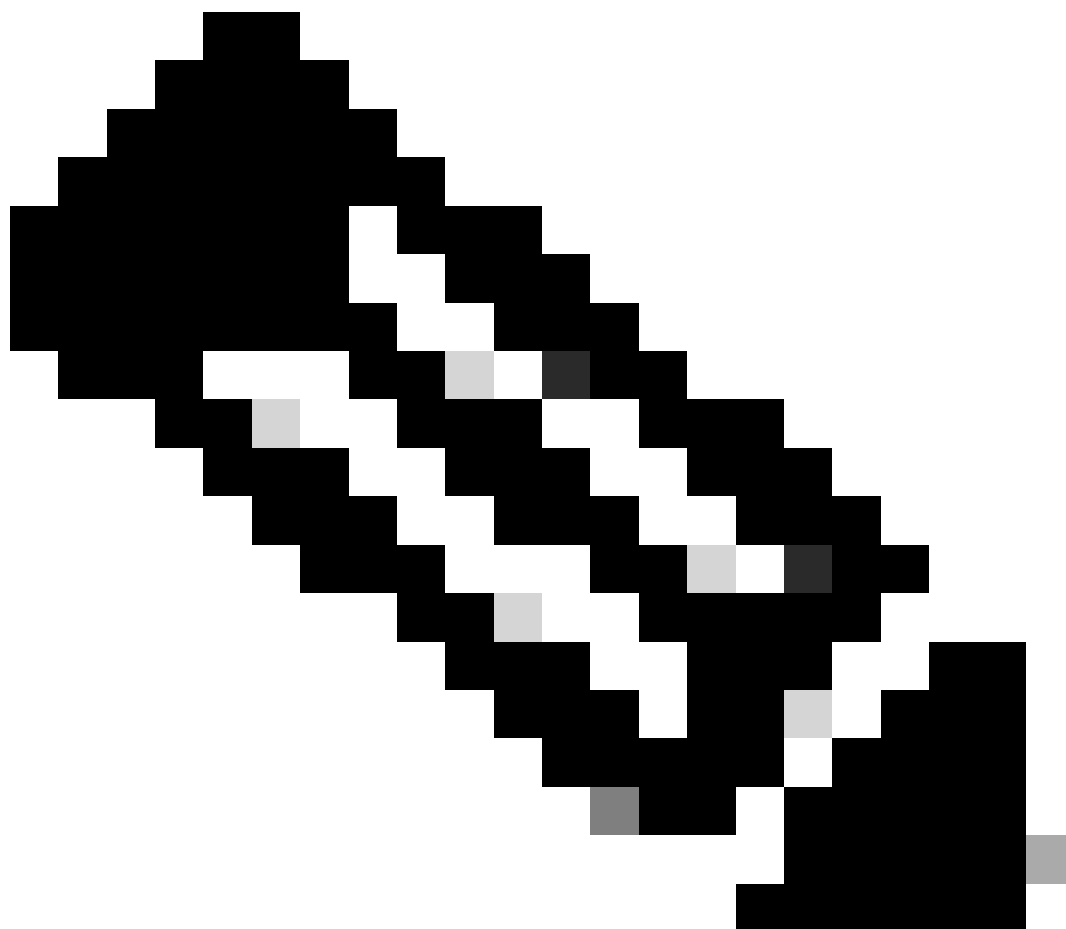
Group Type local

Available Server Groups: radius, ldap, tacacs+, alzlab-rad, fgalvezm-group

Assigned Server Groups: (empty)

Buttons: Cancel, Apply to Device

Stap 2. Selecteer Autorisatie en selecteer vervolgens + Add om een nieuwe methodelijst te maken. Geef het de standaardnaam met Type als netwerk zoals in de afbeelding.



Opmerking: aangezien het wordt geadverteerd door de controller tijdens de [WLAN Layer 3-beveiligingsconfiguratie](#): zorg ervoor dat de configuratie 'aaa autorisatienetwerk standaard lokaal' op het apparaat bestaat voor een lokale inlogmethodelijst om te werken. Dit betekent dat de lijst van de vergunningsmethode met standaard naam moet worden bepaald om lokale web-authenticatie behoorlijk te vormen. In deze sectie, wordt deze bepaalde lijst van de vergunningsmethode gevormd.

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add - Delete

Name	Type	Group Type	Group1	Group2	Group3	Group4
alzlab-rad-authz	network	group	alzlab-rad	N/A	N/A	N/A
wcm_loc_serv_cert	credential-download	local	N/A	N/A	N/A	N/A

10 items per page 1 - 2 of 2 items

Quick Setup: AAA Authorization

Method List Name*

Type* ⓘ

Group Type ⓘ

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+
- alzlab-rad
- fgalvezm-group

Assigned Server Groups

-

Cancel

Apply to Device

CLI-configuratie voor stappen 1 en 2:

```
<#root>
```

```
9800(config)#
```


```
aaa new-model
```

```
9800(config)#
```

```
aaa authentication login local-auth local
```

```
9800(config)#
```

```
aaa authorization network default local
```

 **Opmerking:** Als externe RADIUS-verificatie nodig is, leest u deze instructies met betrekking tot de RADIUS-serverconfiguratie op 9800 WLC's: [AAA Config op 9800 WLC](#). Zorg ervoor dat de lijst met verificatiemethoden is ingesteld op "login" als type in plaats van dot1x.

Stap 3. Ga naar Configuratie > Beveiliging > Gastgebruiker. Selecteer + Add en configureer de details van de gastgebruikersaccount.

Add Guest User ✕

General	Lifetime
User Name* <input type="text" value="guestuser"/>	Years* <input type="text" value="1"/>
Password* <input type="password" value="••••••••"/> <input type="checkbox"/> Generate password	Months* <input type="text" value="0"/>
Confirm Password* <input type="password" value="••••••••"/>	Days* <input type="text" value="0"/>
Description* <input type="text" value="WebAuth user"/>	Hours* <input type="text" value="0"/>
AAA Attribute list <input type="text" value="Enter/Select"/>	Mins* <input type="text" value="0"/>
No. of Simultaneous User Logins* <input type="text" value="0"/> <small>Enter 0 for unlimited users</small>	

CLI-configuratie:

```
<#root>
```

```
9800(config)#
```

```
user-name guestuser
```

```
9800(config-user-name)#
```

```
description "WebAuth user"
```

```
9800(config-user-name)#
```

```
password 0 <password>
```

```
9800(config-user-name)#
```

```
type network-user description "WebAuth user" guest-user lifetime year 1
```

If permanent users are needed then use this command:

```
9800(config)#
```

```
username guestuserperm privilege 0 secret 0 <password>
```

Stap 4. (optioneel) Bij de definitie van de parameterkaart worden automatisch een aantal toegangscontrolelijsten (ACL's) gemaakt. Deze ACL's worden gebruikt om te definiëren welk verkeer een omleiding naar webserver veroorzaakt en welk verkeer door mag gaan. Als er specifieke vereisten zijn, zoals meerdere IP-adressen van webserver of URL-filters, navigeer dan naar Configuration > Security > ACL selecteer + Add en definieer de benodigde regels; de vergunningen worden omgeleid terwijl de verklaringen verkeersspasses ontkennen.

Automatisch gemaakte ACL-regels zijn:

```
<#root>
```

```
alz-9800#
```

```
show ip access-list
```

```
Extended IP access list WA-sec-172.16.80.8
10 permit tcp any host 172.16.80.8 eq www
20 permit tcp any host 172.16.80.8 eq 443
30 permit tcp host 172.16.80.8 eq www any
40 permit tcp host 172.16.80.8 eq 443 any
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit udp any any eq bootpc
80 permit udp any any eq bootps
90 deny ip any any (1288 matches)
Extended IP access list WA-v4-int-172.16.80.8
10 deny tcp any host 172.16.80.8 eq www
20 deny tcp any host 172.16.80.8 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

Beleid en tags configureren

Stap 1. Navigeren naar Configuratie > Tags en profielen > WLAN's, selecteer + Add om een nieuw WLAN te maken. Definieer profiel en SSID naam, en Status in het tabblad Algemeen.

Add WLAN ✕

General Security Advanced

Profile Name*	EWA-Guest	Radio Policy	All ▼
SSID*	EWA-Guest	Broadcast SSID	ENABLED <input checked="" type="checkbox"/>
WLAN ID*	4		
Status	ENABLED <input checked="" type="checkbox"/>		

↶ Cancel Apply to Device

Stap 2. Selecteer het tabblad Beveiliging en stel Layer 2-verificatie in op Geen als u geen verificatie via het luchtcoderingsmechanisme nodig hebt. In Layer 3 selecteert u het veld Web Policy, selecteert u de parameterkaart in het vervolgkeuzemenu en kiest u de verificatielijst in het vervolgkeuzemenu. Als een aangepaste ACL eerder is gedefinieerd, selecteert u Geavanceerde instellingen tonen en selecteert u de juiste ACL in het vervolgkeuzemenu.

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

OWE Transition Mode

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

[Interactive Help](#)

Activate Windows

Go to System in Control Panel to activate Windows

Edit WLAN ✕

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy [Show Advanced Settings >>>](#)

Web Auth Parameter Map EWA-Guest ▼

Authentication List local-auth ▼ ⓘ

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

↶ Cancel Activate Windows Update & Apply to Device

[Interactive Help](#)

CLI-configuratie:

```
<#root>
```

```
9800(config)#
```

```
wlan EWA-Guest 4 EWA-Guest
```

```
9800(config-wlan)#
```

```
no security ft adaptive
```

```
9800(config-wlan)#
```

```
no security wpa
```

```
9800(config-wlan)#
```

```
no security wpa wpa2
```

```
9800(config-wlan)#
```

```
no security wpa wpa2 ciphers aes
```

```
9800(config-wlan)#
```

```
no security wpa akm dot1x
```

```
9800(config-wlan)#
```

```
security web-auth
```

```
9800(config-wlan)#
```

```
security web-auth authentication-list local-auth
```

```
9800(config-wlan)#
```

```
security web-auth parameter-map EWA-Guest
```

```
9800(config-wlan)#
```

```
no shutdown
```

Stap 3. Navigeer naar Configuration > Tags & profielen > Policy en selecteer + Add. Definieer de beleidsnaam en -status; zorg ervoor dat de centrale instellingen onder WLAN-switchingbeleid zijn ingeschakeld voor lokale toegangspunten. Selecteer in het tabblad Toegangsbeleid het juiste VLAN in het vervolgkeuzemenu VLAN/VLAN-groep zoals in de afbeelding.

Add Policy Profile



General

Access Policies

QOS and AVC

Mobility

Advanced

Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*

Guest-Policy

Description

Policy for guest access

Status

ENABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Central Association

ENABLED

Flex NAT/PAT

DISABLED

Cancel

Apply to Device

Add Policy Profile
✕

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name

VLAN

▼

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

↶ Cancel

📄 Apply to Device

CLI-configuratie:

```

<#root>
9800(config)#
wireless profile policy Guest-Policy

9800(config-wireless-policy)#
description "Policy for guest access"

9800(config-wireless-policy)#
vlan VLAN2621

9800(config-wireless-policy)#
no shutdown

```

Stap 4. Navigeren naar Configuratie > Tags & profielen > Tags, in het tabblad Beleid selecteert u + Toevoegen. Definieer een tagnaam en selecteer vervolgens onder WLAN-POLICY Maps + Add en voeg het eerder gemaakte WLAN- en beleidsprofiel toe.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ▶ 0 ▶▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile*
Policy Profile*

✕
✓

➤ RLAN-POLICY Maps: 0

↶ Cancel
📄 Apply to Device

CLI-configuratie:

```
<#root>
```

```
9800(config)#
```

```
wireless tag policy EWA-Tag
```

```
9800(config-policy-tag)#
```

```
wlan EWA-Guest policy Guest-Policy
```

Stap 5. Navigeer naar Configuration > Wireless > Access points en selecteer het toegangspunt dat wordt gebruikt om deze SSID uit te zenden. Selecteer in het menu AP bewerken de nieuwe tag in het vervolgkeuzemenu Beleid.

Edit AP
✕

AP Name*	C9117AXI-lobby	Primary Software Version	17.3.3.26
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	0cd0.f897.ae60	Predownloaded Version	N/A
Ethernet MAC	0cd0.f894.5c34	Next Retry Time	N/A
Admin Status	<input type="checkbox"/> DISABLED	Boot Version	1.1.2.4
AP Mode	Local ▼	IOS Version	17.3.3.26
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	ENABLED <input checked="" type="checkbox"/>	CAPWAP Preferred Mode	IPv4
LED Brightness Level	8 ▼	DHCP IPv4 Address	172.16.10.133
Tags		Static IP (IPv4/IPv6)	<input type="checkbox"/>
⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.			
Policy	EWA-Tag ▼	Time Statistics	
Site	default-site-tag ▼	Up Time	0 days 0 hrs 19 mins 13 secs
nr	default-rf-tag	Controller Association Latency	2 mins 7 secs

↶ Cancel
Activate Windows [Go to System in Control Panel to activate Windows](#)
Update & Apply to Device

Interactive Help

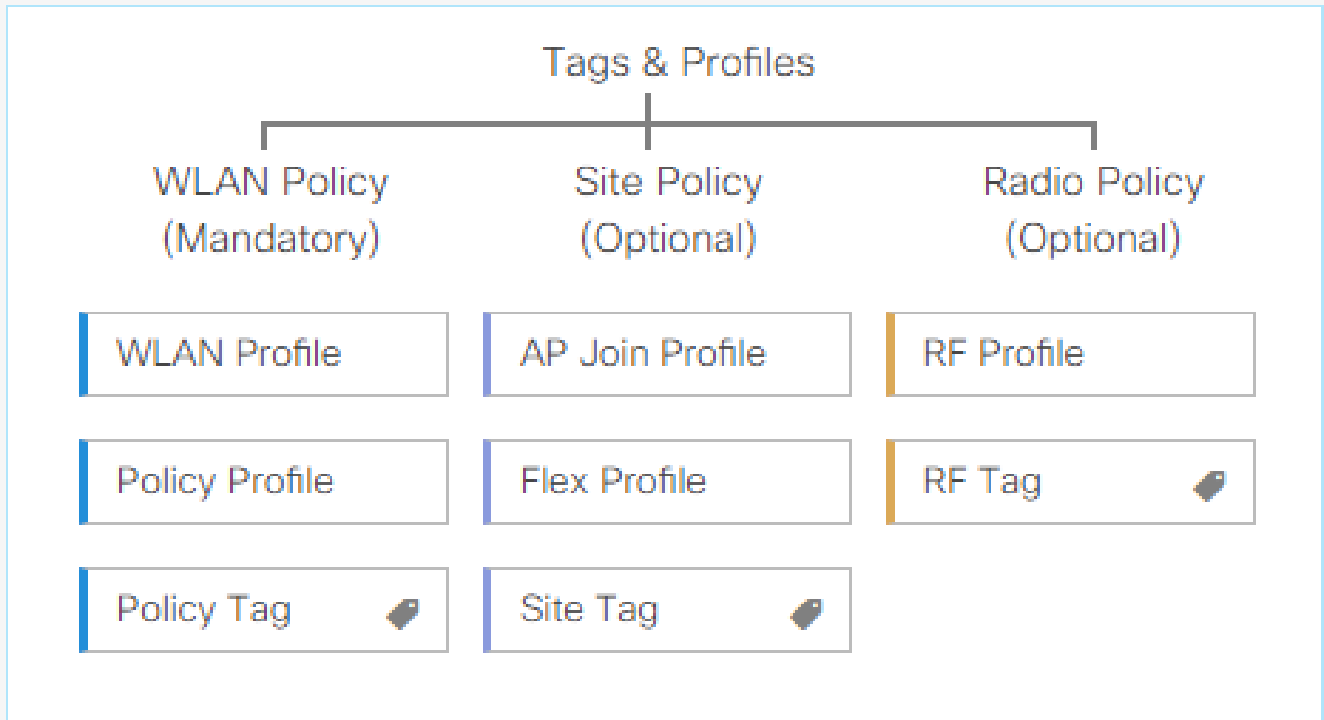
Als meerdere AP's tegelijkertijd getagd moeten worden, zijn er twee opties beschikbaar:

Optie A. Navigeer naar Configuratie > Draadloze Setup > Geavanceerd en selecteer Nu starten om de lijst van het configuratiemenu weer te geven. Selecteer het lijstpictogram naast Tag AP's, dit geeft de lijst weer van alle AP's in Join state, controleer de benodigde AP's en selecteer vervolgens + Tag AP's, selecteer de gemaakte Policy Tag in het uitrolmenu.

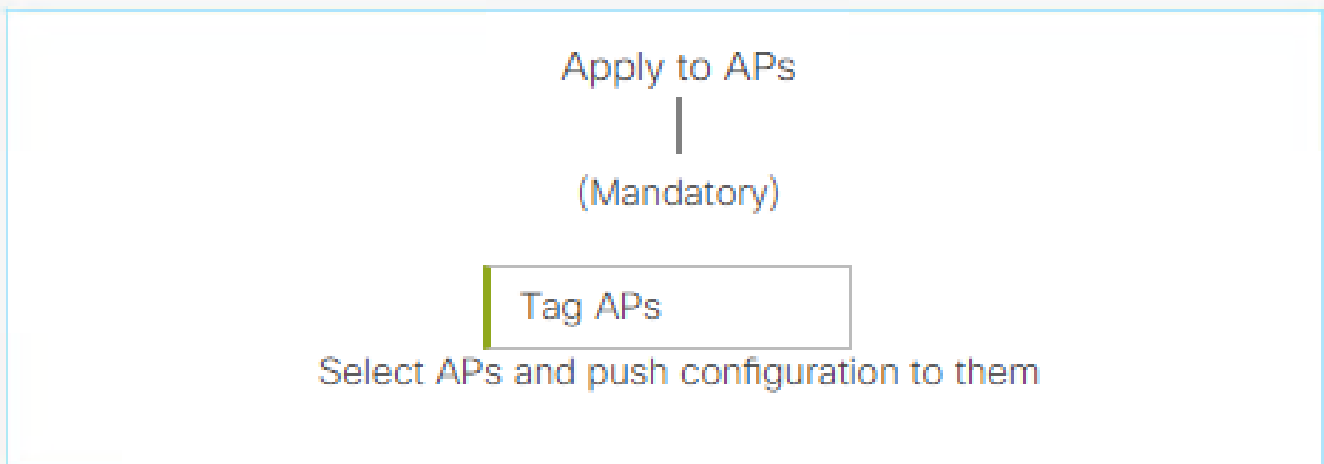
Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

DESIGN PHASE



DEPLOY PHASE



TERMINOLOGY

Tag

WLAN Policy, Policy Profile

Site Policy - AP Profile, Site Profile

Radio Policy - Radio Characteristics

ACTIONS



Go to List View



Create New

. Definieer regelnaam, AP-naam regex (met deze instelling kan de controller definiëren welke AP's zijn gelabeld), prioriteit (lagere getallen hebben een hogere prioriteit) en noodzakelijke tags.

Associate Tags to AP ✕

Rule Name*	<input type="text" value="Guest-APs"/>	Policy Tag Name	<input type="text" value="EWA-Tag"/>
AP name regex*	<input type="text" value="C9117-.*"/>	Site Tag Name	<input type="text" value="Search or Select"/>
Active	<input checked="" type="checkbox"/> YES	RF Tag Name	<input type="text" value="Search or Select"/>
Priority*	<input type="text" value="1"/>		

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt:

```
<#root>
```

```
9800#
```

```
show running-config wlan
```

```
9800#
```

```
show running-config aaa
```

```
9800#
```

```
show aaa servers
```

```
9800#
```

```
show ap tag summary
```

```
9800#
```

```
show ap name <ap-name> config general
```

```
9800#
```

```
show ap name <ap-name> tag detail
```

```
9800#
```

```
show wlan [summary | id | name | all]
```

```
9800#
```

```
show wireless tag policy detailed <policy-tag name>
```

9800#

show wireless profile policy detailed <policy-profile name>

Controleer de status en beschikbaarheid van de http server met de status van de ip http server:

<#root>

9800#

show ip http server status

HTTP server status: Enabled

HTTP server port: 80

HTTP server active supplementary listener ports: 21111

HTTP server authentication method: local

HTTP server auth-retry 0 time-window 0

HTTP server digest algorithm: md5

HTTP server access class: 0

HTTP server IPv4 access class: None

HTTP server IPv6 access class: None

[...]

HTTP server active session modules: ALL

HTTP secure server capability: Present

HTTP secure server status: Enabled

HTTP secure server port: 443

HTTP secure server ciphersuite: rsa-aes-cbc-sha2 rsa-aes-gcm-sha2

dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2

ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2

HTTP secure server TLS version: TLSv1.2 TLSv1.1

HTTP secure server client authentication: Disabled

HTTP secure server PIV authentication: Disabled

HTTP secure server PIV authorization only: Disabled

HTTP secure server trustpoint: CISCO_IDEVID_SUDI

HTTP secure server peer validation trustpoint:

HTTP secure server ECDHE curve: secp256r1

HTTP secure server active session modules: ALL

Verifieer ACL-plumb naar clientsessie met deze opdrachten:

<#root>

9800#

show platform software wireless-client chassis active R0 mac-address <Client mac in aaaa.bbbb.cccc forma

ID : 0xa0000002
MAC address : aaaa.bbbb.cccc
Type : Normal
Global WLAN ID : 4
SSID : EWA-Guest

Client index : 0
Mobility state : Local

Authentication state : L3 Authentication

VLAN ID : 2621
[...]
Disable IPv6 traffic : No

Dynamic policy template : 0x7b 0x73 0x0b 0x1e 0x46 0x2a 0xd7 0x8f 0x23 0xf3 0xfe 0x9e 0x5c 0xb0 0xeb 0xf

9800#

show platform software cgacl chassis active F0

Template ID
Group Index

Lookup ID Number of clients

0x7B 0x73 0x0B 0x1E 0x46 0x2A 0xD7 0x8F 0x23 0xF3 0xFE 0x9E 0x5C 0xB0 0xEB 0xF8 0x0000000a

0x0000001a 1

9800#

show platform software cgacl chassis active F0 group-idx <group index> acl

ACL ID ACL Name CGACL Type Protocol Direction Sequence

16 IP-Adm-V6-Int-ACL-global Punt IPv6 IN 1

25 WA-sec-172.16.80.8 Security IPv4 IN 2


26 WA-v4-int-172.16.80.8 Punt IPv4 IN 1

```
19 implicit_deny Security IPv4 IN 3
21 implicit_deny_v6 Security IPv6 IN 3
18 preauth_v6 Security IPv6 IN 2
```

Problemen oplossen

Altijd-aan-traceren

WLC 9800 biedt ALTIJD-ON traceermogelijkheden. Dit zorgt ervoor dat alle aan de client gerelateerde fouten, waarschuwingen en meldingen op het niveau constant worden vastgelegd en u kunt logbestanden bekijken voor een incident of storing nadat het is opgetreden.

 **Opmerking:** op basis van het volume van de gegenereerde logbestanden kunt u teruggaan van enkele uren tot enkele dagen.

Om de sporen te bekijken die 9800 WLC standaard heeft verzameld, kunt u via SSH/Telnet verbinding maken met de 9800 WLC en deze stappen lezen (zorg ervoor dat u de sessie aan een tekstbestand registreert).

Stap 1. Controleer de huidige controllertijd zodat u de logbestanden kunt volgen in de tijd terug naar toen het probleem zich voordeed.

```
<#root>
9800#
show clock
```

Stap 2. Verzamel syslogs van de controllerbuffer of externe syslog zoals die door de systeemconfiguratie wordt gedictieerd. Dit geeft een snel overzicht van de gezondheid van het systeem en eventuele fouten.

```
<#root>
9800#
show logging
```

Stap 3. Controleer of de debug-voorwaarden zijn ingeschakeld.


```
<#root>
9800#
```

```
show debugging
```

```
IOSXE Conditional Debug Configs:  
Conditional Debug Global State: Stop  
IOSXE Packet Tracing Configs:  
Packet Infra debugs:  
Ip Address
```

```
Port
```

```
-----|-----
```

 **Opmerking:** als u een van de vermelde voorwaarden ziet, betekent dit dat de sporen zijn aangemeld om het debug-niveau te bereiken voor alle processen die de ingeschakelde voorwaarden ervaren (mac-adres, IP-adres, enzovoort). Dit zou het volume van de boomstammen doen toenemen. Daarom wordt aanbevolen om alle voorwaarden te wissen wanneer niet actief debuggen.

Stap 4. Wi de aanname dat het geteste mac-adres niet als voorwaarde in Stap 3 vermeld stond. Verzamel de altijd-op berichtniveau sporen voor het specifieke mac adres.

```
<#root>
```

```
9800#
```

```
show logging profile wireless filter [mac | ip] [<aaaa.bbbb.cccc> | <a.b.c.d>] to-file always-on-<FILENAME>
```

U kunt de inhoud op de sessie weergeven of u kunt het bestand kopiëren naar een externe TFTP-server.

```
<#root>
```

```
9800#
```

```
more bootflash:always-on-<FILENAME.txt>
```

```
or
```

```
9800#
```

```
copy bootflash:always-on-<FILENAME.txt> tftp://<a.b.c.d>/<path>/always-on-<FILENAME.txt>
```

Voorwaardelijke debugging en radio actieve tracering

Als de altijd-on sporen u niet genoeg informatie geven om de trigger voor het probleem dat wordt onderzocht te bepalen, kunt u voorwaardelijke debugging inschakelen en Radio Active (RA)-spoor opnemen, dat debug level traces biedt voor alle processen die interacteren met de gespecificeerde voorwaarde (client mac-adres in dit geval). Lees deze stappen om voorwaardelijke debugging in te schakelen.

Stap 1. Zorg ervoor dat de debug-voorwaarden niet zijn ingeschakeld.


```
<#root>  
9800#  
clear platform condition all
```

Stap 2. Schakel de debug-voorwaarde in voor het draadloze client-MAC-adres dat u wilt controleren.

Met deze opdrachten wordt het opgegeven MAC-adres 30 minuten (1800 seconden) bewaakt. U kunt deze tijd optioneel tot 2085978494 seconden verlengen.

```
<#root>  
9800#  
debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

 Opmerking: als u meer dan één client tegelijk wilt controleren, voert u de opdracht debug Wireless mac uit per mac-adres.

 Opmerking: de activiteit van de draadloze client wordt niet weergegeven op de terminalsessie, aangezien alle logbestanden intern worden gebufferd om later te worden bekeken.

Stap 3. Reproduceer het probleem of gedrag dat u wilt controleren.

Stap 4. Stop de debugs als het probleem wordt gereproduceerd voordat de standaard of de ingestelde monitortijd is ingesteld.

```
<#root>  
9800#  
no debug wireless mac <aaaa.bbbb.cccc>
```

Zodra de monitor-tijd is verstreken of de debug-radio is gestopt, genereert de 9800 WLC een lokaal bestand met de naam:

```
ra_trace_MAC_aabbcccc_HMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Stap 5. Verzamel het bestand van de mac-adresactiviteit. U kunt het spoor .log naar een externe

server kopiëren of de uitvoer direct op het scherm weergeven.

Controleer de naam van het RA traces bestand.

```
<#root>
```

```
9800#
```

```
dir bootflash: | inc ra_trace
```

Kopieert het bestand naar een externe server:

```
<#root>
```

```
9800#
```

```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<a.b.c.d>
```

Geef de inhoud weer:

```
<#root>
```

```
9800#
```

```
more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Stap 6. Als de worteloorzaak nog niet duidelijk is, verzamel de interne logboeken die een meer breedsprakige mening van debug niveaulogboeken zijn. U hoeft de client niet opnieuw te debuggen, aangezien de opdracht debug-logbestanden biedt die al zijn verzameld en intern zijn opgeslagen.

```
<#root>
```

```
9800#
```

```
show logging profile wireless internal filter [mac | ip] [<aaaa.bbbb.cccc> | <a.b.c.d>] to-file ra-inter
```



Opmerking: deze opdrachtoutput geeft sporen voor alle registratieniveaus voor alle processen en is vrij omvangrijk. Neem contact op met Cisco TAC om te helpen bij het doorlopen van deze sporen.

```
<#root>
```

```
9800#
```

```
copy bootflash:ra-internal-<FILENAME>.txt tftp://<a.b.c.d>/ra-internal-<FILENAME>.txt
```

Geef de inhoud weer:

```
<#root>
```

```
9800#
```

```
more bootflash:ra-internal-<FILENAME>.txt
```

Stap 7. Verwijder de debug-voorwaarden.



Opmerking: Zorg ervoor dat u altijd de debug-voorwaarden verwijdert na een probleemoplossingssessie.

Ingesloten pakketvastlegging

9800 controllers kunnen pakketten native scannen; dit maakt probleemoplossing gemakkelijker als control plane pakketverwerking zichtbaarheid.

Stap 1. Bepaal ACL om verkeer van belang te filteren. Voor webverificatie wordt aanbevolen verkeer van en naar de webserver toe te staan, evenals verkeer van en naar een paar AP's waarop clients zijn aangesloten.

```
<#root>
```

```
9800(config)#
```

```
ip access-list extended EWA-pcap
```

```
9800(config-ext-nacl)#
```

```
permit ip any host <web server IP>
```

```
9800(config-ext-nacl)#
```

```
permit ip host <web server IP> any
```

```
9800(config-ext-nacl)#
```

```
permit ip any host <AP IP>
```

```
9800(config-ext-nacl)#
```

```
permit ip host <AP IP> any
```


Stap 2. Bepaal de parameters van de monitoropname. Zorg ervoor dat het verkeer van het controlevliegtuig in beide richtingen wordt toegelaten, verwijst de interface naar de fysieke opstraalverbinding van uw controlemechanisme.

```
<#root>
```

```
9800#
```

```
monitor capture EWA buffer size <buffer size in MB>
```

```
9800#
```

```
monitor capture EWA access-list EWA-pcap
```

```
9800#
```

```
monitor capture EWA control-plane both interface <uplink interface> both
```

```
<#root>
```

```
9800#
```

```
show monitor capture EWA
```

```
Status Information for Capture EWA
```

```
Target Type:
```

```
Interface: Control Plane, Direction: BOTH
```

```
Interface: TenGigabitEthernet0/1/0, Direction: BOTH
```

```
Status : Inactive
```

```
Filter Details:
```

```
Access-list: EWA-pcap
```

```
Inner Filter Details:
```

```
Buffer Details:
```

```
Buffer Type: LINEAR (default)
```

```
Buffer Size (in MB): 100
```

```
Limit Details:
```

```
Number of Packets to capture: 0 (no limit)
```

```
Packet Capture duration: 0 (no limit)
```

```
Packet Size to capture: 0 (no limit)
```

```
Packet sampling rate: 0 (no sampling)
```

Stap 3. Start de monitor om het probleem op te nemen en te reproduceren.

```
<#root>
```

9800#

```
monitor capture EWA start
```

```
Started capture point : EWA
```

Stap 4. Stop de monitor en voer deze uit.

```
<#root>
```

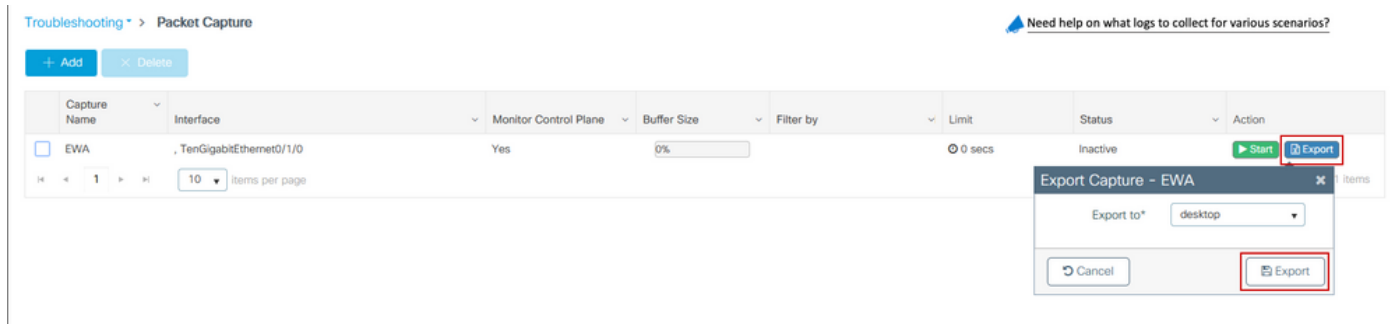
9800#

```
monitor capture EWA stop
```

```
Stopped capture point : EWA
```

```
9800#monitor capture EWA export tftp://<a.b.c.d>/EWA.pcap
```

Alternatief, kan de opname van GUI worden gedownload, naar Problemen oplossen > Packet Capture navigeren en Exporteren selecteren op de geconfigureerde opname. Selecteer desktop in het vervolgkeuzemenu om de opname via HTTP in de gewenste map te downloaden.



Probleemoplossing aan cliëntzijde

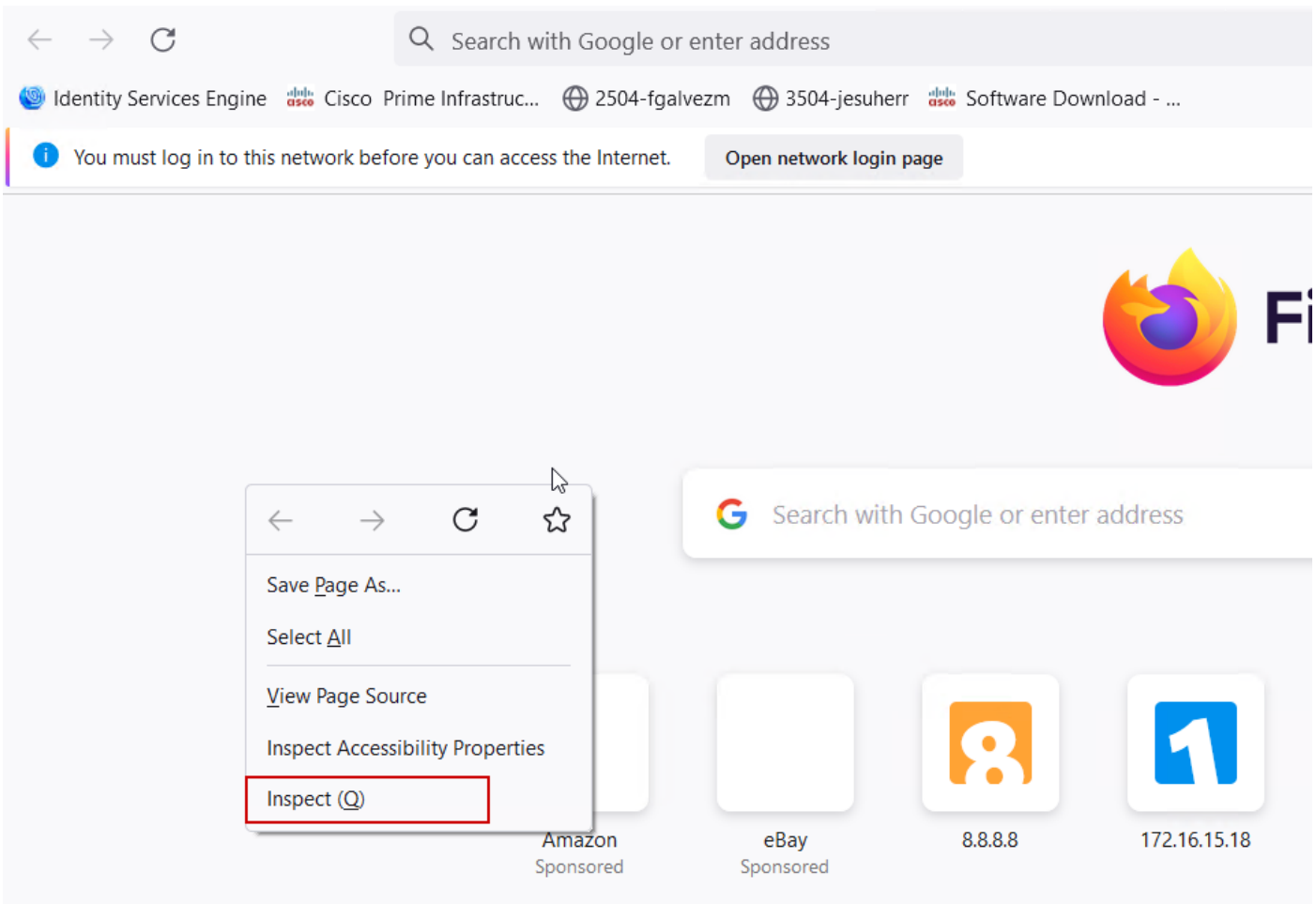
Web authenticatie WLAN's zijn afhankelijk van cliëntgedrag, op deze basis is kennis en informatie over gedrag aan de cliëntzijde essentieel om de basisoorzaak van web authenticatie fouten te identificeren.

Probleemoplossing voor HAR-browser

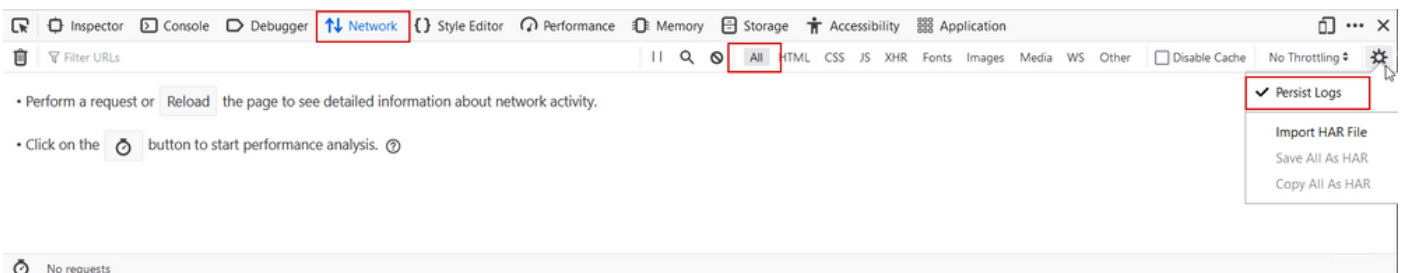
Veel moderne browsers, zoals Mozilla Firefox en Google Chrome, bieden tools voor consoleontwikkelaars om interacties met webapplicaties te debuggen. HAR-bestanden zijn records van client-server interacties en bieden een tijdlijn van HTTP-interacties, samen met aanvraag- en antwoordinformatie (headers, statuscode, parameters, enzovoort).

HAR-bestanden kunnen worden geëxporteerd vanuit de clientbrowser en geïmporteerd in een andere browser voor verdere analyse. Dit document beschrijft hoe u het HAR-bestand kunt verzamelen vanuit Mozilla Firefox.

Stap 1. Open Web Developer Tools met Ctrl + Shift + I, klik met de rechtermuisknop binnen de browser inhoud en selecteer Inspect.



Stap 2. Navigeer naar het netwerk en controleer of "All" is geselecteerd om alle verzoektypen op te nemen. Selecteer het versnellingspictogram en zorg ervoor dat Persiste Logs een pijl naast het heeft, anders wordt logboekaanvraag gewist wanneer een domeinwijziging wordt geactiveerd.



Stap 3. Reproduceer het probleem, zorg ervoor dat browser alle verzoeken registreert. Zodra het probleem is gereproduceerd, wordt de netwerklogboekregistratie gestopt, selecteer dan op het tandwielpictogram en selecteer Save All As HAR.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	172.16.80.2	/	document	html	756 B	503 B
	GET	172.16.80.2	favicon.ico	img	cached		
200	GET	172.16.80.8	consent.html?switch_url=http://192.0.2.1/login.html&ap_mac=0cd0f8:94:f8:0c	document	html	3.02 KB	2.78 KB
200	GET	172.16.80.8	aup.html	subdocument	html	cached	2.51 KB
404	GET	172.16.80.8	favicon.ico	FaviconLoader.jsm:191 (img)	html	cached	1.22 KB
200	POST	192.0.2.1	login.html	consent.html:37 (document)	html	2.33 KB	2.18 KB

Packet Capture voor cliëntzijde

Draadloze clients met OS zoals Windows of MacOS kunnen pakketten op hun draadloze kaartadapter detecteren. Hoewel geen directe vervanging van over-the-air pakketopnamen is, kunnen ze een overzicht geven van de algehele web-verificatiestroom.

DNS-verzoek:

11868	2021-09-28 06:44:07.364305	172.16.21.153	172.16.21.7	DNS	182	53	Standard query 0x8586 A prod.detectportal.prod.cloudops.mozgcp.net
11869	2021-09-28 06:44:07.375372	172.16.21.7	172.16.21.153	DNS	195	57857	Standard query response 0x8586 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.cloudops.mozgcp.net A 34.187.221.82
11870	2021-09-28 06:44:07.418773	172.16.21.7	172.16.21.153	DNS	118	51759	Standard query response 0x8586 A prod.detectportal.prod.cloudops.mozgcp.net A 34.187.221.82

De eerste TCP-handdruk en HTTP GET voor omleiding:

444	2021-09-27 21:53:46....	172.16.21.153	52.185.211.133	TCP	66	54623 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
445	2021-09-27 21:53:46....	172.16.21.153	96.7.93.42	HTTP	205	GET /files/vpn_ssid_notif.txt HTTP/1.1
446	2021-09-27 21:53:46....	96.7.93.42	172.16.21.153	HTTP	866	HTTP/1.1 200 OK (text/html)
447	2021-09-27 21:53:46....	172.16.21.153	96.7.93.42	TCP	54	65421 → 80 [ACK] Seq=303 Ack=1625 Win=131072 Len=0

TCP-handdruk met externe server:

11889	2021-09-28 06:44:07.872917	172.16.21.153	172.16.80.8	TCP	66	65209 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11890	2021-09-28 06:44:07.880494	172.16.80.8	172.16.21.153	TCP	66	80 → 65209 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1250 WS=256 SACK_PERM=1
11891	2021-09-28 06:44:07.888947	172.16.21.153	172.16.80.8	TCP	54	65209 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0

HTTP GET naar externe server (captive portal request):

11106	2021-09-28 06:44:08.524191	172.16.21.153	172.16.80.8	HTTP	563	GET /webauth/consent.html?switch_url=http://192.0.2.1/login.html&ap_mac=0cd0f8:94:f8:0c&client_mac=34:23:07:4c:6b:f7&ssid=844-Guest&redirect=http://www.ms
11107	2021-09-28 06:44:08.522258	172.16.80.8	172.16.21.153	TCP	54	80 → 65209 [ACK] Seq=1 Ack=510 Win=66048 Len=0
11112	2021-09-28 06:44:08.786215	172.16.80.8	172.16.21.153	TCP	1304	80 → 65209 [ACK] Seq=1 Ack=510 Win=66048 Len=1250 [TCP segment of a reassembled PDU]
11113	2021-09-28 06:44:08.787182	172.16.80.8	172.16.21.153	TCP	1304	80 → 65209 [ACK] Seq=1251 Ack=510 Win=66048 Len=1250 [TCP segment of a reassembled PDU]
11114	2021-09-28 06:44:08.787487	172.16.21.153	172.16.80.8	TCP	54	65209 → 80 [ACK] Seq=510 Ack=2501 Win=131072 Len=0
11115	2021-09-28 06:44:08.787653	172.16.80.8	172.16.21.153	HTTP	648	HTTP/1.1 200 OK (text/html)
11116	2021-09-28 06:44:08.834606	172.16.21.153	172.16.80.8	TCP	54	65209 → 80 [ACK] Seq=510 Ack=3095 Win=130560 Len=0

HTTP POST naar virtuele IP voor verificatie:

12331	2021-09-28 06:44:50.644118	172.16.21.153	192.0.2.1	TCP	66	52359 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
12332	2021-09-28 06:44:50.648080	192.0.2.1	172.16.21.153	TCP	66	80 → 52359 [SYN, ACK] Seq=0 Ack=1 Win=84240 Len=0 MSS=1250 SACK_PERM=1 WS=120
12333	2021-09-28 06:44:50.649166	172.16.21.153	192.0.2.1	TCP	54	52359 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
12334	2021-09-28 06:44:50.667759	172.16.21.153	192.0.2.1	HTTP	609	POST /login.html HTTP/1.1 (application/x-www-form-urlencoded)
12335	2021-09-28 06:44:50.672372	192.0.2.1	172.16.21.153	TCP	54	80 → 52359 [ACK] Seq=1 Ack=556 Win=64128 Len=0
12337	2021-09-28 06:44:50.680599	192.0.2.1	172.16.21.153	TCP	1014	80 → 52359 [ACK] Seq=1 Ack=556 Win=64128 Len=960 [TCP segment of a reassembled PDU]
12338	2021-09-28 06:44:50.680996	192.0.2.1	172.16.21.153	TCP	1014	80 → 52359 [ACK] Seq=961 Ack=556 Win=64128 Len=960 [TCP segment of a reassembled PDU]
12339	2021-09-28 06:44:50.681125	172.16.21.153	192.0.2.1	TCP	54	52359 → 80 [ACK] Seq=556 Ack=1921 Win=131072 Len=0
12340	2021-09-28 06:44:50.681261	192.0.2.1	172.16.21.153	HTTP	544	HTTP/1.0 200 OK (text/html)
12341	2021-09-28 06:44:50.681423	192.0.2.1	172.16.21.153	TCP	54	80 → 52359 [FIN, ACK] Seq=2411 Ack=556 Win=64128 Len=0
12342	2021-09-28 06:44:50.681591	172.16.21.153	192.0.2.1	TCP	54	52359 → 80 [ACK] Seq=556 Ack=2411 Win=130560 Len=0
12353	2021-09-28 06:44:50.749948	172.16.21.153	192.0.2.1	TCP	54	52359 → 80 [ACK] Seq=556 Ack=2412 Win=130560 Len=0

Voorbeeld van een succesvolle poging

Dit is de uitvoer van een succesvolle verbindingspoging vanuit het perspectief van het Radio Actieve spoor, gebruik dit als verwijzing om de stadia van de cliëntzitting voor cliënten te identificeren die met een Laag 3 Web authenticatie SSID verbinden.

802.11 Verificatie en koppeling:

<#root>

2021/09/28 12:59:51.781967 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (note): MAC: 3423.874c.6bf7 Assoc
2021/09/28 12:59:51.782009 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7

Received Dot11 association request.

Processing started,

SSID: EWA-Guest, Policy profile: Guest-Policy

, AP Name: C9117AXI-lobby, Ap Mac Address: 0cd0.f897.ae60 BSSID MAC0000.0000.0000 wlan ID: 4RSSI: -39,
2021/09/28 12:59:51.782152 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C
2021/09/28 12:59:51.782357 {wncd_x_R0-0}{1}: [dot11-validate] [26328]: (info): MAC: 3423.874c.6bf7 Wi-Fi
2021/09/28 12:59:51.782480 {wncd_x_R0-0}{1}: [dot11] [26328]: (debug): MAC: 3423.874c.6bf7 dot11 send a

Sending association response with resp_status_code: 0

2021/09/28 12:59:51.782483 {wncd_x_R0-0}{1}: [dot11] [26328]: (debug): MAC: 3423.874c.6bf7 Dot11 Capabi
2021/09/28 12:59:51.782509 {wncd_x_R0-0}{1}: [dot11-frame] [26328]: (info): MAC: 3423.874c.6bf7 Wi-Fi di
2021/09/28 12:59:51.782519 {wncd_x_R0-0}{1}: [dot11] [26328]: (info): MAC: 3423.874c.6bf7 dot11 send as
2021/09/28 12:59:51.782611 {wncd_x_R0-0}{1}: [dot11] [26328]: (note): MAC: 3423.874c.6bf7

Association success. AID 1

, Roaming = False, WGB = False, 11r = False, 11w = False
2021/09/28 12:59:51.782626 {wncd_x_R0-0}{1}: [dot11] [26328]: (info): MAC: 3423.874c.6bf7 DOT11 state t
2021/09/28 12:59:51.782676 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7

Station Dot11 association is successful.

Layer 2-verificatie overgeslagen:

<#root>

2021/09/28 12:59:51.782727 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7 Sta
2021/09/28 12:59:51.782745 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C
2021/09/28 12:59:51.782785 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7

L2 Authentication initiated. method WEBAUTH

, Policy VLAN 2621,AAA override = 0
2021/09/28 12:59:51.782803 {wncd_x_R0-0}{1}: [sanet-shim-translate] [26328]: (ERR): 3423.874c.6bf7 wlan
[...]
2021/09/28 12:59:51.787912 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:51.787953 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:51.787966 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7

L2 Authentication of station is successful., L3 Authentication : 1

Standaard ACL-waarde:

<#root>

2021/09/28 12:59:51.785227 {wncd_x_R0-0}{1}: [webauth-sm] [26328]: (info): [0.0.0.0]Starting Webauth, m
2021/09/28 12:59:51.785307 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [26328]: (info): [0000.0000.0000:
2021/09/28 12:59:51.785378 {wncd_x_R0-0}{1}: [webauth-ac1] [26328]: (info): capwap_9000000b[3423.874c.6

Applying IPv4 intercept ACL via SVM, name: WA-v4-int-172.16.80.8

, priority: 50, IIF-ID: 0
2021/09/28 12:59:51.785738 {wncd_x_R0-0}{1}: [epm-redirect] [26328]: (info): [0000.0000.0000:unknown]
URL-Redirect-ACL = WA-v4-int-172.16.80.8

2021/09/28 12:59:51.786324 {wncd_x_R0-0}{1}: [webauth-ac1] [26328]: (info): capwap_9000000b[3423.874c.6
Applying IPv6 intercept ACL via SVM, name: IP-Adm-V6-Int-ACL-global, priority: 52

, IIF-ID: 0
2021/09/28 12:59:51.786598 {wncd_x_R0-0}{1}: [epm-redirect] [26328]: (info): [0000.0000.0000:unknown]
URL-Redirect-ACL = IP-Adm-V6-Int-ACL-global

2021/09/28 12:59:51.787904 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client

IP-leerproces:

<#root>

2021/09/28 12:59:51.799515 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C
2021/09/28 12:59:51.799716 {wncd_x_R0-0}{1}: [client-iplearn] [26328]: (info): MAC: 3423.874c.6bf7
IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

2021/09/28 12:59:51.802213 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:51.916777 {wncd_x_R0-0}{1}: [sisf-packet] [26328]: (debug): RX: ARP from interface cap
[...]
2021/09/28 12:59:52.810136 {wncd_x_R0-0}{1}: [client-iplearn] [26328]: (note): MAC: 3423.874c.6bf7
Client IP learn successful. Method: ARP IP: 172.16.21.153

2021/09/28 12:59:52.810185 {wncd_x_R0-0}{1}: [epm] [26328]: (info): [0000.0000.0000:unknown] HDL = 0x0
2021/09/28 12:59:52.810404 {wncd_x_R0-0}{1}: [auth-mgr] [26328]: (info): [3423.874c.6bf7:capwap_9000000
2021/09/28 12:59:52.810794 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [26328]: (info): [0000.0000.0000:
2021/09/28 12:59:52.810863 {wncd_x_R0-0}{1}: [client-iplearn] [26328]: (info): MAC: 3423.874c.6bf7
IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

Layer 3-verificatie- en omleidingsproces:

<#root>

2021/09/28 12:59:52.811141 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7
L3 Authentication initiated. LWA

2021/09/28 12:59:52.811154 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:55.324550 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c
2021/09/28 12:59:55.324565 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c
HTTP GET request

2021/09/28 12:59:55.324588 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_900000b[3423.874c.6bf7] [...]

2021/09/28 13:01:29.859434 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_900000b[3423.874c.6bf7]

POST rcvd when in LOGIN state

2021/09/28 13:01:29.859636 {wncd_x_R0-0}{1}: [webauth-ac1] [26328]: (info): capwap_900000b[3423.874c.6bf7]

2021/09/28 13:01:29.860335 {wncd_x_R0-0}{1}: [webauth-ac1] [26328]: (info): capwap_900000b[3423.874c.6bf7]

2021/09/28 13:01:29.861092 {wncd_x_R0-0}{1}: [auth-mgr] [26328]: (info): [3423.874c.6bf7:capwap_900000b[3423.874c.6bf7]]

Authc success from WebAuth, Auth event success

2021/09/28 13:01:29.861151 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [26328]: (note): Authentication Success.

2021/09/28 13:01:29.862867 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7

L3 Authentication Successful.

ACL:[]

2021/09/28 13:01:29.862871 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7

Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE

Overgang naar RUN-status:

<#root>

2021/09/28 13:01:29.863176 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7 ADD MOB

2021/09/28 13:01:29.863272 {wncd_x_R0-0}{1}: [errmsg] [26328]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_

Username entry (3423.874C.6BF7) joined with ssid (EWA-Guest) for device with MAC: 3423.874c.6bf7

2021/09/28 13:01:29.863334 {wncd_x_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [Applied attribute :bsn-v

2021/09/28 13:01:29.863336 {wncd_x_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [Applied attribute : time

2021/09/28 13:01:29.863343 {wncd_x_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [Applied attribute : url-

2021/09/28 13:01:29.863387 {wncd_x_R0-0}{1}: [ewlc-qos-client] [26328]: (info): MAC: 3423.874c.6bf7 Cli

2021/09/28 13:01:29.863409 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [26328]: (debug):

Managed client RUN state notification

: 3423.874c.6bf7

2021/09/28 13:01:29.863451 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7

Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

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.