

FlexConnect EWA configureren op Catalyst 9800 WLC en ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[RA Trace Voorbeeld van een succesvolle poging](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u een FlexConnect EWA configureert op Catalyst 9800 WLC en ISE.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de configuratie van de 9800 Wireless LAN Controllers (WLC).

Gebruikte componenten

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

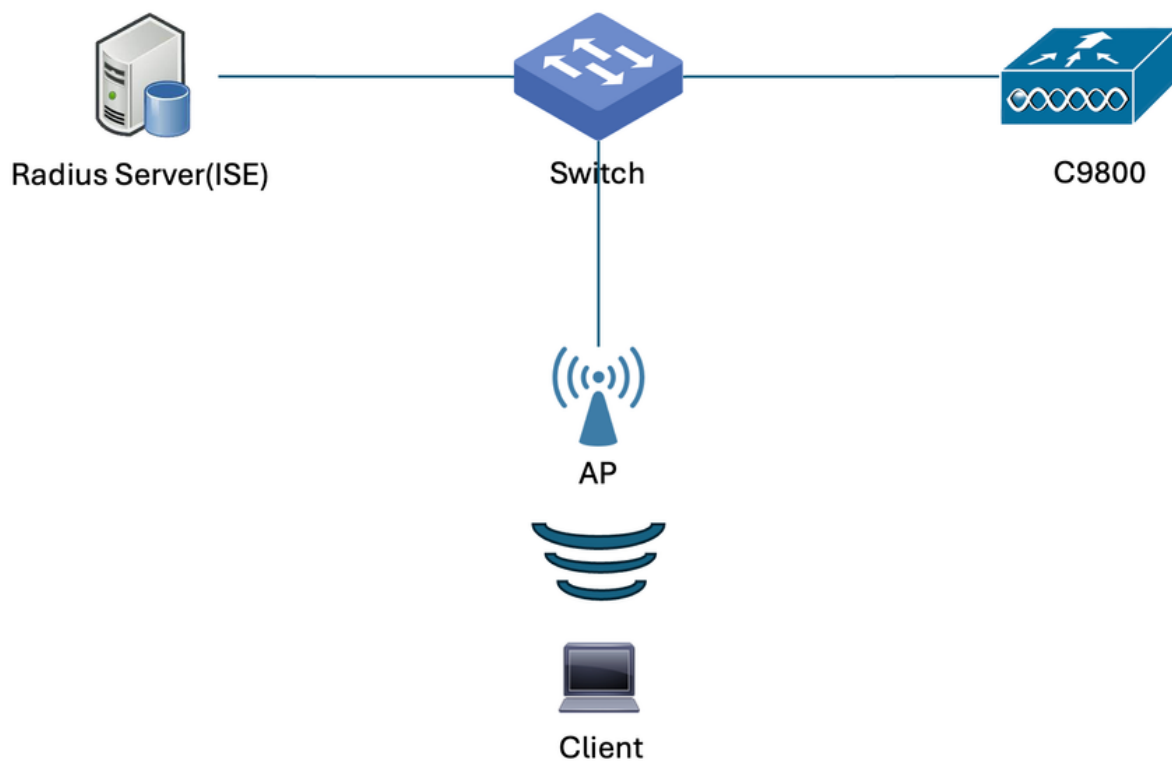
- Cisco Catalyst 9800 WLC Cisco IOS® XE versie 17.15.3
- Identity Service Engine (ISE) v3.4.0.608

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.

Configureren

Netwerkdigram

Dit document is gebaseerd op deze topologie:

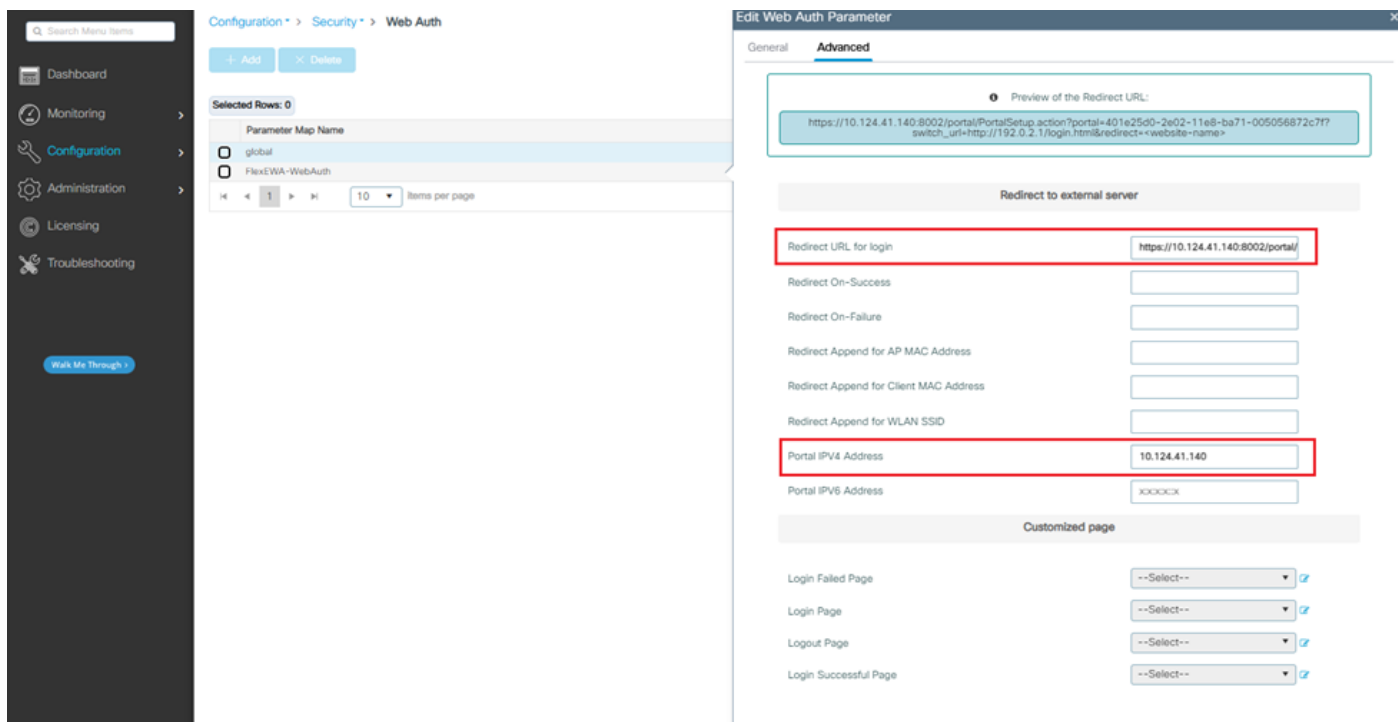


Configuraties

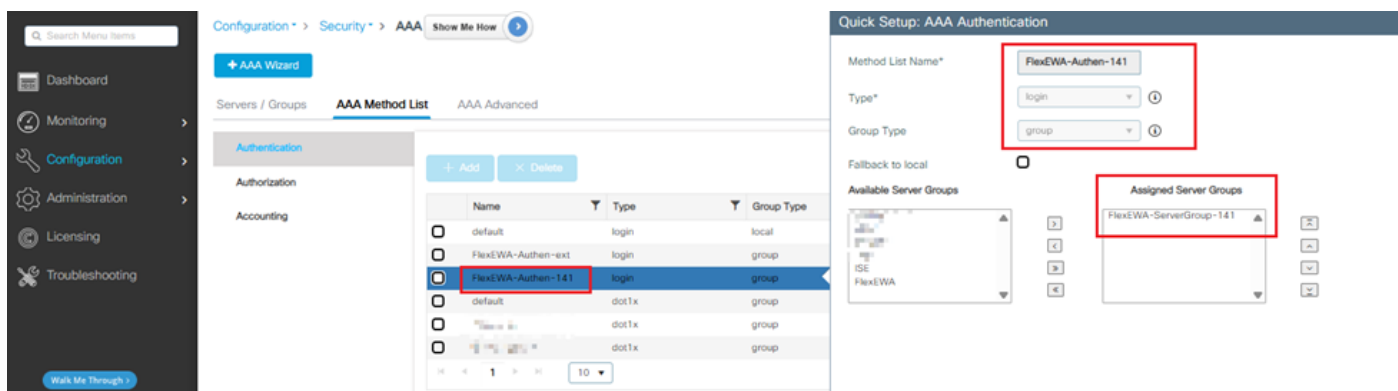
Stap 1. Navigeer naar Configuratie > Beveiliging > Web Auth > +Voeg een Web Auth Parameter Map toe.

The screenshot shows the Cisco ISE configuration interface. The left sidebar contains the navigation menu with 'Configuration' selected. The main area displays the 'Web Auth' configuration page. The 'Parameter Map Name' is set to 'FlexEWA-WebAuth-1'. The 'Type' is set to 'webauth'. The 'Banner Configuration' section is visible on the right.

De portal-URL wordt gegenereerd vanuit ISE (stap 7).



Stap 2. Navigeer naar Configuratie > Beveiliging > AAA > Methodenlijst > Authenticatie > + Voeg een verificatielijst toe.



Stap 3. Stel dat de HTTPS-poort 8002 is, raadpleeg dan de automatisch gegenereerde ACL WA-sec-10.124.41.140 om een nieuwe ACL voor preverificatie toe te voegen.

Configuration > Security > ACL

ACL Name: FlexEWA141-sec-ACL

ACL Type: IPv4 Extended

Rules:

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	permit	any		10.124.41.141		tcp	None	eq www	None	Disabled
15	permit	any		10.124.41.141		tcp	None	eq 8002	None	Disabled
20	permit	any		10.124.41.141		tcp	None	eq 443	None	Disabled
25	permit	10.124.41.141		any		tcp	eq 8002	None	None	Disabled
30	permit	10.124.41.141		any		tcp	eq www	None	None	Disabled
40	permit	10.124.41.141		any		tcp	eq 443	None	None	Disabled
50	permit	any		any		tcp	None	eq domain	None	Disabled
60	permit	any		any		udp	None	eq domain	None	Disabled
70	permit	any		any		udp	None	eq bootpc	None	Disabled
80	permit	any		any		udp	None	eq bootps	None	Disabled

Stap 4. Controleer de automatisch gegenereerde ACL WA-v4-int 10.124.41.141.

Configuration > Security > ACL

ACL Name: WA-v4-int-10.124.41.141

ACL Type: IPv4 Extended

Rules:

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	deny	any		10.124.41.141		tcp	None	eq www	None	Disabled
20	permit	any		any		tcp	None	eq www	None	Disabled

Stap 5. Pas de twee ACL's toe op Configuratie > Tags & Profielen > Flex > Flex-profiel > ACL-beleid.

Configuration > Tags & Profiles > Flex

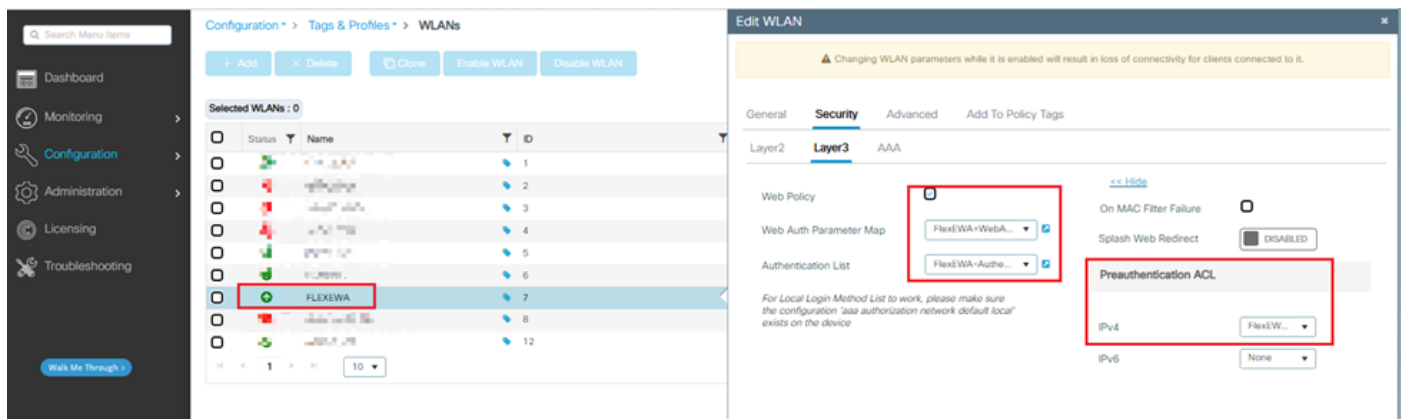
Selected Rows: 0

Flex Profile Name: default-flex-profile

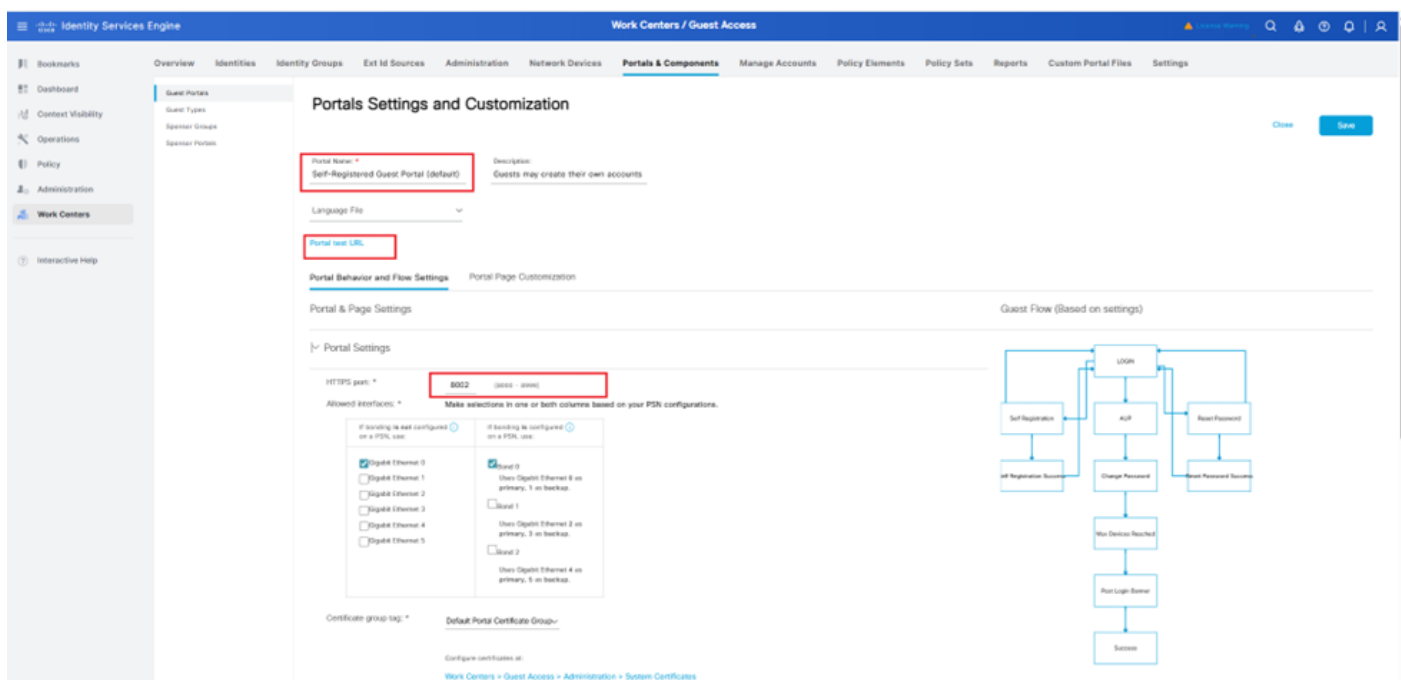
Policy ACL:

ACL Name	Central Web Auth	URL Filter
FlexEWA141-sec-ACL	Disabled	Disabled
WA-v4-int-10.124.41.141	Disabled	Disabled

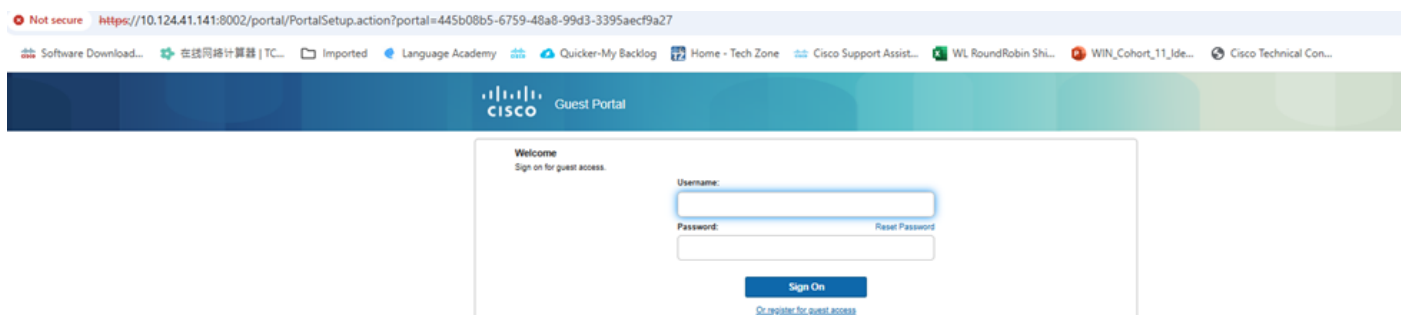
Stap 6. Pas de nieuw gemaakte Web Auth Parameter Map, Authentication List en PreAuthentication ACL toe op WLAN.



Stap 7. Navigeer naar Workcenters > Portals & Components > Guest Portals > Portals Settings and Customization > Portal Name > Self-Registered Guest Portal (standaard) om Portal URL van ISE te genereren.

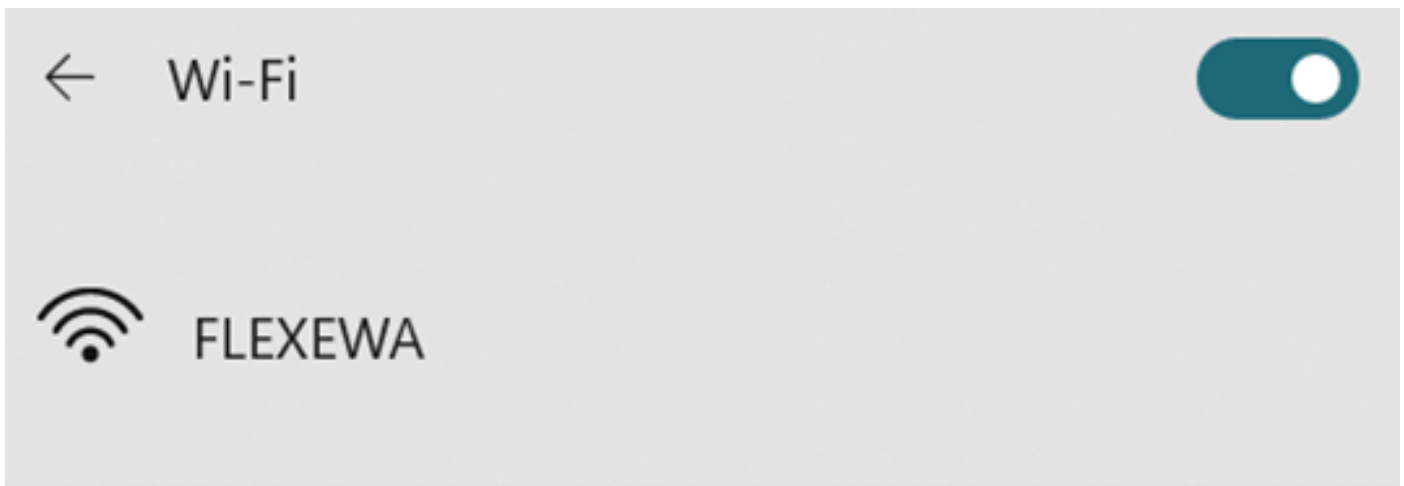


Dit weergegeven webportaal wordt weergegeven nadat u op URL voor portaaltest hebt geklikt.

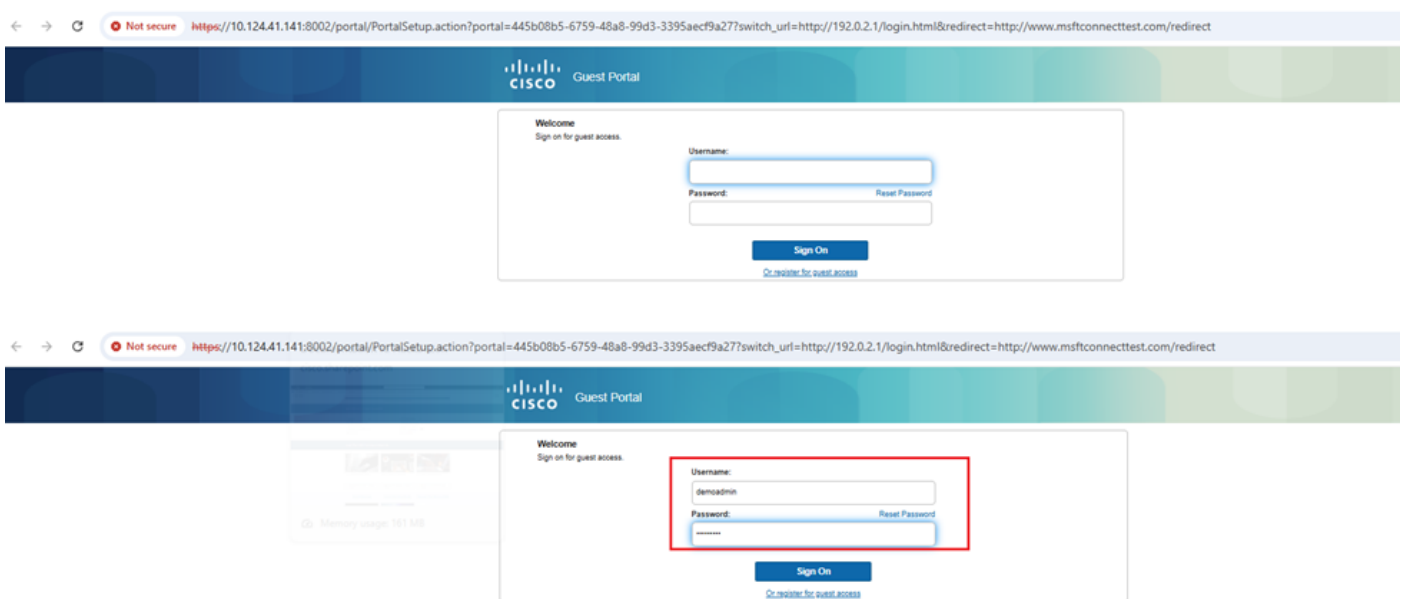


Verifiëren

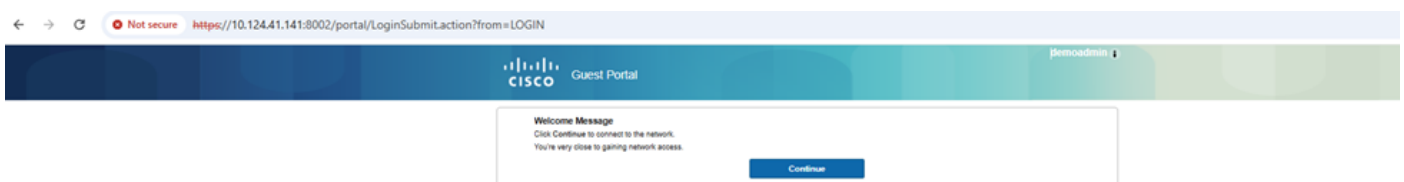
Stap 1. FLEXEWA-SSID aansluiten.



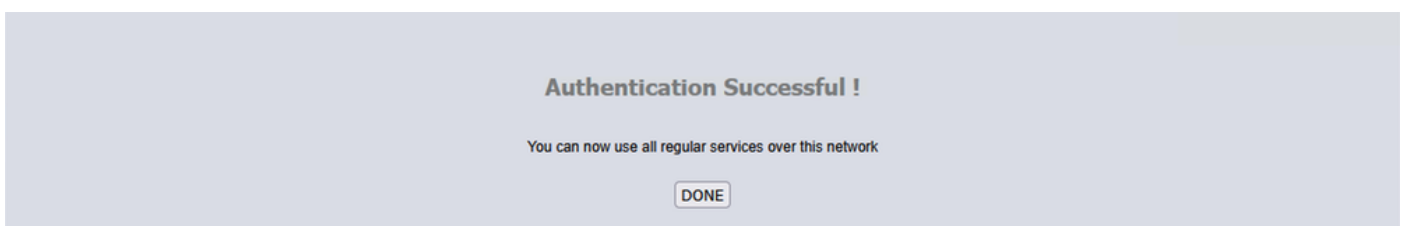
Stap 2. Doorverwijzen naar portal en gebruikersnaam en wachtwoord invoeren.



Stap 3. Het gastenportaal verschijnt:



Stap 4. Nadat u op Doorgaan hebt geklikt, is de verificatie voltooid:



RA Trace Voorbeeld van een succesvolle poging

Dit is de uitvoer van een geslaagde verbindingspoging vanuit het perspectief van Radio Active trace. Gebruik dit als referentie om cliensessiefasen te identificeren voor clients die verbinding maken met een Layer 3-webverificatie-SSID.

Client gekoppeld:

2025/09/09 15:21:48.617769958 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (opmerking): MAC: f0b6.1e39.9ce8 Association ontvangen. BSSID c418.fc82.bb0b, WLAN FLEXEWA, Sleuf 1 AP c418.fc82.bb00, 9178_1, Site tag HK, Policy tag default-policy-tag, Policy profile default-policy-profile, Switching Central, Socket delay 0ms, AP BSSID MAC c418.fc82.bb0b

2025/09/09 15:21:48.617813534 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug): MAC: f0b6.1e39.9ce8 Ontvangen Dot11-associatieverzoek. Verwerking gestart, SSID: FLEXEWA, beleidsprofiel: standaardbeleidsprofiel, AP-naam: 9178_1, AP Mac-adres: c418.fc82.bb00BSSID MAC0000.0000.0000wlan-ID: 7RSSI: -30, SNR: 67

2025/09/09 15:21:48.618002570 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (opmerking): MAC: f0b6.1e39.9ce8 overgang clientstatus: S_CO_INIT -> S_CO_ASSOCIATING

2025/09/09 15:21:48.618017149 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (ERR): MAC: f0b6.1e39.9ce8 dot11-record is niet opgehaald

2025/09/09 15:21:48.618301251 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (info): MAC: f0b6.1e39.9ce8 Dot11 ie valideert ext/supp rates. Validatie geslaagd voor ondersteunde tarieven radio_type 2

2025/09/09 15:21:48.618320304 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (debug): MAC: f0b6.1e39.9ce8 Dot11 ie validate rsnx, client not using sae, skip check

2025/09/09 15:21:48.618339230 {wncd_x_R0-0}{1}: [dot11-valideren] [17842]: (info): MAC: f0b6.1e39.9ce8 WiFi direct: Dot11 valideren P2P IE. P2P IE niet aanwezig.

2025/09/09 15:21:48.618598747 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug): MAC: f0b6.1e39.9ce8 dot11 verstuur associatierespons. Framing associatie reactie met resp_status_code: 0

2025/09/09 15:21:48.618604733 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug): MAC: f0b6.1e39.9ce8 Dot11 Capability info byte1 1, byte2: 11

2025/09/09 15:21:48.618696034 {wncd_x_R0-0}{1}: [dot11-frame] [17842]: (info): MAC: f0b6.1e39.9ce8 WiFi direct: assoc bouwen met P2P overslaan IE: WiFi direct-beleid uitgeschakeld

2025/09/09 15:21:48.618785409 {wncd_x_R0-0}{1}: [dot11] [17842]: (info): MAC: f0b6.1e39.9ce8 dot11 verstuur associatierespons. Het verzenden van een assoc respons van lengte: 177 met resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS

2025/09/09 15:21:48.618791096 {wncd_x_R0-0}{1}: [dot11] [17842]: (Noot): MAC: f0b6.1e39.9ce8 Associatiesucces. AID 33, Zwerven = Vals, WGB = Vals, 11r = Vals, 11w = Vals Snel zwerven = Vals

2025/09/09 15:21:48.618806595 {wncd_x_R0-0}{1}: [dot11] [17842]: (info): MAC: f0b6.1e39.9ce8 DOT11 statusovergang: S_DOT11_INIT -> S_DOT11_ASSOCIATED

2025/09/09 15:21:48.618855282 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug): MAC: f0b6.1e39.9ce8 Station Dot11 associatie is succesvol.

Layer 2-verificatie overgeslagen:

2025/09/09 15:21:48.618992721 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug): MAC: f0b6.1e39.9ce8 Start L2-verificatie. Bssid in staatsmachine: c418.fc82.bb0b Bssid in aanvraag is:

c418.fc82.bb0b

2025/09/09 15:21:48.619006036 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (opmerking): MAC: f0b6.1e39.9ce8 overgang clientstatus: S_CO_ASSOCIATING ->

S_CO_L2_AUTH_IN_PROGRESS

2025/09/09 15:21:48.619093387 {wncd_x_R0-0}{1}: [client-auth] [17842]: (opmerking): MAC: f0b6.1e39.9ce8 L2-verificatie gestart. methode WEBAUTH, Policy VLAN 0, AAA-overschrijving = 0 [...]

2025/09/09 15:21:48.623839337 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC: f0b6.1e39.9ce8 Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_PENDING -> S_AUTHIF_L2_WEBAUTH_DONE

2025/09/09 15:21:48.623863687 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] Apparaattype voor de sessie wordt gedetecteerd als Intel-Apparaat en oude Intel-Apparaat & Apparaatnaam voor de sessie wordt gedetecteerd als INTEL CORPORATE en oude INTEL CORPORATE & Old protocolkaart 1 en nieuw 1

2025/09/09 15:21:48.623873529 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] auth mgr attr add/change notification is ontvangen voor attr dc-profile-name(1130)

2025/09/09 15:21:48.623911035 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug): MAC: f0b6.1e39.9ce8 L2 Authenticatie van station is succesvol., L3 Authenticatie: 1

ACL-load:

2025/09/09 15:21:48.620896754 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (info): [0.0.0.0]Starten van Webauth, mac [f0:b6:1e:39:9c:e8], IIF 0, audit-ID D1257C0A000000CA2D54F867

2025/09/09 15:21:48.620927053 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): [f0b6.1e39.9ce8][0.0.0.0]Param-map gebruikt: global

2025/09/09 15:21:48.620935005 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): [f0b6.1e39.9ce8][0.0.0.0]Ongeldige status -> INIT

2025/09/09 15:21:48.620942683 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Sessie maken, adres 0.0.0.0 toevoegen

2025/09/09 15:21:48.620946808 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17842]: (info): [0000.0000.0000:unknown] ID van opgehaalde zone 0x0 voor bssid 12364632846638254486

2025/09/09 15:21:48.620958619 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Param-map gebruikt: FlexEWA=WebAuth-141

2025/09/09 15:21:48.620962048 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Staat INIT -> INIT

2025/09/09 15:21:48.620978097 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Sessie starten, status doorsturen naar 0 IF 0x90000008 mac [F0B6.1E39.9CE8]

2025/09/09 15:21:48.620981018 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Initiële sessie, SM init sessies 5

2025/09/09 15:21:48.620988217 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Param-map gebruikt: FlexEWA=WebAuth-141

2025/09/09 15:21:48.620991618 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Staat INIT -> INIT

2025/09/09 15:21:48.621023019 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]IPv4-interceptie van ACL via SVM toepassen, naam:
WA-v4-int-10.124.41.141-7, prioriteit: 50, IIF-ID: 0
2025/09/09 15:21:48.621032776 {wncd_x_R0-0}{1}: [svm] [17842]: (info): SVM_INFO: Solliciteer
Svc Tempel WA-v4-int-10.124.41.141-7 (ML:GEEN)
2025/09/09 15:21:48.621786262 {wncd_x_R0-0}{1}: [epm] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] De functie (EPM URL PLUG-IN) is gestart (successtatus)
2025/09/09 15:21:48.621804034 {wncd_x_R0-0}{1}: [epm-acl] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Filter-ID: FlexEWA141-sec-ACL ontvangen
2025/09/09 15:21:48.622151544 {wncd_x_R0-0}{1}: [epm] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Functie (EPM ACL PLUG-IN) is gestart (successtatus)
2025/09/09 15:21:48.622187815 {wncd_x_R0-0}{1}: [svm] [17842]: (info): SVM_INFO: Response
of epm is SYNC with return code Success
2025/09/09 15:21:48.62226011 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Verhogen van de teksjabloon geactiveerd (9) op deze sessie,
client (onbekend) (0)
2025/09/09 15:21:48.622265240 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Het toepassen van IPv6 onderschept ACL via SVM,
naam: IP-Adm-V6-Int-ACL-global-7, prioriteit: 52, IIF-ID: 0
2025/09/09 15:21:48.622270327 {wncd_x_R0-0}{1}: [svm] [17842]: (info): SVM_INFO: Application
Svc Templ IP-Adm-V6-Int-ACL-global-7 (ML:NONE)
2025/09/09 15:21:48.622898831 {wncd_x_R0-0}{1}: [epm] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] De functie (EPM URL PLUG-IN) is gestart (status Succes)
2025/09/09 15:21:48.622932973 {wncd_x_R0-0}{1}: [svm] [17842]: (info): SVM_INFO: Response
of epm is SYNC with return code Success
2025/09/09 15:21:48.622957784 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Verhogen van de teksjabloon geactiveerd (9) op deze sessie,
client (onbekend) (0)
2025/09/09 15:21:48.623119047 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug): MAC:
f0b6.1e39.9ce8 Dot11 SAE vindt ipsk-voortgang als 0, niet in wachtende staat
2025/09/09 15:21:48.623126095 {wncd_x_R0-0}{1}: [lbridge-main] [17842]: (debug): MAC:
f0b6.1e39.9ce8 Link-local bridging niet ingeschakeld voor deze client, VLAN-validiteit wordt niet
gecontroleerd
2025/09/09 15:21:48.623205421 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Context wijzigen van 'Idle' naar 'Running'
2025/09/09 15:21:48.623209350 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Methode webauth wijzigen staat van 'Niet uitvoeren' naar
'Uitvoeren'
2025/09/09 15:21:48.623572855 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] SM kan gebeurtenissjabloon niet naar PRE verzenden voor
0x8D000C0
2025/09/09 15:21:48.623680228 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC:
f0b6.1e39.9ce8 Client auth-interface state transition:
S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP -> S_AUTH_IF_L2_WEBAUTH_PENDING

IP Learn-proces:

2025/09/09 15:21:51.628124695 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (opmerking): MAC: f0b6.1e39.9ce8 overgang clientstatus: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

2025/09/09 15:21:51.628463813 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: (info): MAC: f0b6.1e39.9ce8 IP-learn-statusovergang: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

2025/09/09 15:21:51.632284534 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC: f0b6.1e39.9ce8 Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE

2025/09/09 15:21:51.676501288 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (info): RX: IPv6 DHCP van intf capwap_9000008 op vlan 174 Src MAC: f0b6.1e39.9ce8 Dst MAC: 3333.0001.0002 Ipv6 SRC: fe80:3f83:2848:d30:7aea, Ipv6 DST: ff02:1:2, type: msg type: DHCPV6_MSG_SOLICIT xid: 14443573

2025/09/09 15:21:51.676541447 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (info): TX: IPv6 DHCP van intf capwap_9000008 op vlan 174 Src MAC: f0b6.1e39.9ce8 Dst MAC: 3333.0001.0002 Ipv6 SRC: fe80:3f83:2848:d30:7aea, Ipv6 DST: ff02:1:2, type: msg type: DHCPV6_MSG_SOLICIT xid: 14443573

2025/09/09 15:21:51.706187097 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (info): RX: ARP van interface capwap_90000008 op vlan 174 Bron: MAC: f0b6.1e39.9ce8 Dest MAC: ffff.ffff.ffff ARP REQUEST, ARP sender MAC: f0b6.1e39.9ce8 ARP doel MAC: 0000.0000.0000 ARP afzender IP: 169.254.137.222, ARP doel IP: 169.254.137.222, [...]

2025/09/09 15:21:52.686190945 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: (opmerking): MAC: f0b6.1e39.9ce8 Client IP learning geslaagd. Methode: DHCP IP: 10.124.37.251

2025/09/09 15:21:52.686244192 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] auth mgr attr add/change notification is ontvangen voor attr(8)

2025/09/09 15:21:52.686285422 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Wijzig notif CB, Adres toevoegen 10.124.37.251 [F0B6.1E39.9CE8]

2025/09/09 15:21:52.686289265 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17842]: (info): [0000.0000.0000:unknown] ID van opgehaalde zone 0x0 voor bssid 12364632846638254486

2025/09/09 15:21:52.686291647 {wncd_x_R0-0}{1}: [WebAuth-sess] [17842]: (info): WebAuth-sessie toevoegen aan ipv4-hashtabel voor vrf id 0, ipv4 vrf-tabel id 0

2025/09/09 15:21:52.686430038 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] SM Notified attribuut Toevoegen/Bijwerken addr 10.124.37.251

2025/09/09 15:21:52.686456653 {wncd_x_R0-0}{1}: [epm] [17842]: (info): [0000.0000.0000:unknown] HDL = 0x0 vlan 174 fail count 0 dirty_counter 0 is_dirty 0

2025/09/09 15:21:52.686710209 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: (info): MAC: f0b6.1e39.9ce8 IP-learn-statusovergang: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

Layer 3-verificatie en omleidingsproces:

2025/09/09 15:21:52.687395906 {wncd_x_R0-0}{1}: [client-auth] [17842]: (opmerking): MAC: f0b6.1e39.9ce8 L3-verificatie gestart. LWA

2025/09/09 15:21:52.687472722 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC:

f0b6.1e39.9ce8 Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

2025/09/09 15:21:52.687723489 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (info): RX: DHCPv4 vanaf interface Po1 op vlan 174 SRC MAC: 4006.d589.4e78 Dst MAC: ffff.ffff.ffff src_ip: 10.124.37.242, dst_ip: 255.255.255.255, BOOTPREPLY, SISF_DHCPACK, giaddr: 0.0.0.0, yiaddr: 10.124.37.251, CMAC: f0b6.1e39.9ce8

2025/09/09 15:21:52.687992316 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (info): TX: DHCPv4 vanaf interface Po1 op vlan 174 SRC MAC: 4006.d589.4e78 Dst MAC: f0b6.1e39.9ce8 src_ip: 10.124.37.242, dst_ip: 255.255.255.255, BOOTPREPLY, SISF_DHCPACK, giaddr: 0.0.0.0, yiaddr: 10.124.37.251, CMAC: f0b6.1e39.9ce8

2025/09/09 15:21:52.688020475 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17842]: (breedsprakig): Type: EWLC_CAPWAP_HDR_AP, Id:23277

[...]

2025/09/09 15:21:55.663715832 {wncd_x_R0-0}{1}: [webauth-io] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197 IO staat NIEUW>

2025/09/09 15:21:55.664060604 {wncd_x_R0-0}{1}: [webauth-io] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197 Lees evenement, Bericht gereed

2025/09/09 15:21:55.664071121 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]GET rcvd wanneer in INIT-toestand

2025/09/09 15:21:55.664077798 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]HTTP GET-verzoek

2025/09/09 15:21:55.664094019 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Parse GET, src [10 124 37 251] DST [23 5 165 82] URL [<http://www.msftconnecttest.com/connecttest.txt>]

[...]

2025/09/09 15:22:16.420792303 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]POST rcvd bij aanmelding

2025/09/09 15:22:32.375197748 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]IPv4-intecept ACL niet toepassen via SVM, naam "WA-v4-int-10.124.41.141-7", pri 50, IIF 0

2025/09/09 15:22:32.376230716 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] Verhogen van de teksjabloon gedeactiveerd (11) op deze sessie, client (onbekend) (0)

2025/09/09 15:22:32.376262689 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]IPv6-intecept ACL niet toepassen via SVM, naam "IP-Adm-V6-Int-ACL-global", pri 52, IIF 0

2025/09/09 15:22:32.376734374 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_90000008] Verhogen van de teksjabloon gedeactiveerd (11) op deze sessie, client (onbekend) (0)

2025/09/09 15:22:32.376865998 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug): MAC: f0b6.1e39.9ce8 Dot11 SAE vindt ipsk-voortgang als 0, niet in wachtende staat

2025/09/09 15:22:32.376870611 {wncd_x_R0-0}{1}: [lbridge-main] [17842]: (debug): MAC: f0b6.1e39.9ce8 Link-local bridging niet ingeschakeld voor deze client, VLAN-validiteit wordt niet gecontroleerd

2025/09/09 15:22:32.376949875 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Authc succes van WebAuth, succes van het Auth-evenement

Overgang naar de status RUN:

2025/09/09 15:22:32.379351256 {wncd_x_R0-0}{1}: [client-auth] [17842]: (opmerking): MAC:
f0b6.1e39.9ce8 ADD MOBILE verzonden. Clientstatusvlaggen: 0x38 BSSID: MAC:

c418.fc82.bb0b capwap IFID: 0x90000008, Mobiele telefoons toevoegen verzonden: 1

2025/09/09 15:22:32.379583842 {wncd_x_R0-0}{1}: [errmsg] [17842]: (info):

%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: vermelding van
gebruikersnaam (demoadmin) gekoppeld aan SSID (FLEXEWA) voor apparaat met MAC:
f0b6.1e39.9ce8 op kanaal (100)

2025/09/09 15:22:32.379671775 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (info): [Toegepast
kenmerk :bsn-vlan-interface-naam 0 "wlc-management"]

2025/09/09 15:22:32.379673695 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (info): [Toegepast
kenmerk: timeout 0 28800 (0x7080)]

2025/09/09 15:22:32.379683417 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (info): [Toegepast
kenmerk: url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]

2025/09/09 15:22:32.379727993 {wncd_x_R0-0}{1}: [ewlc-qos-client] [17842]: (info): MAC:
f0b6.1e39.9ce8 Client QoS run state handler

2025/09/09 15:22:32.379756610 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [17842]: (debug):
Managed client RUN-statusmelding: f0b6.1e39.9ce8

2025/09/09 15:22:32.379810670 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (opmerking): MAC:
f0b6.1e39.9ce8 overgang clientstatus: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Gerelateerde informatie

- [Externe webverificatie configureren en oplossen op 9800 WLC](#)

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.