

Configurer FlexConnect EWA sur Catalyst 9800 WLC et ISE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifier](#)

[Exemple de suivi RA d'une tentative réussie](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer un FlexConnect EWA sur Catalyst 9800 WLC et ISE.

Conditions préalables

Exigences

Cisco recommande que vous connaissiez la configuration des contrôleurs LAN sans fil (WLC) 9800.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

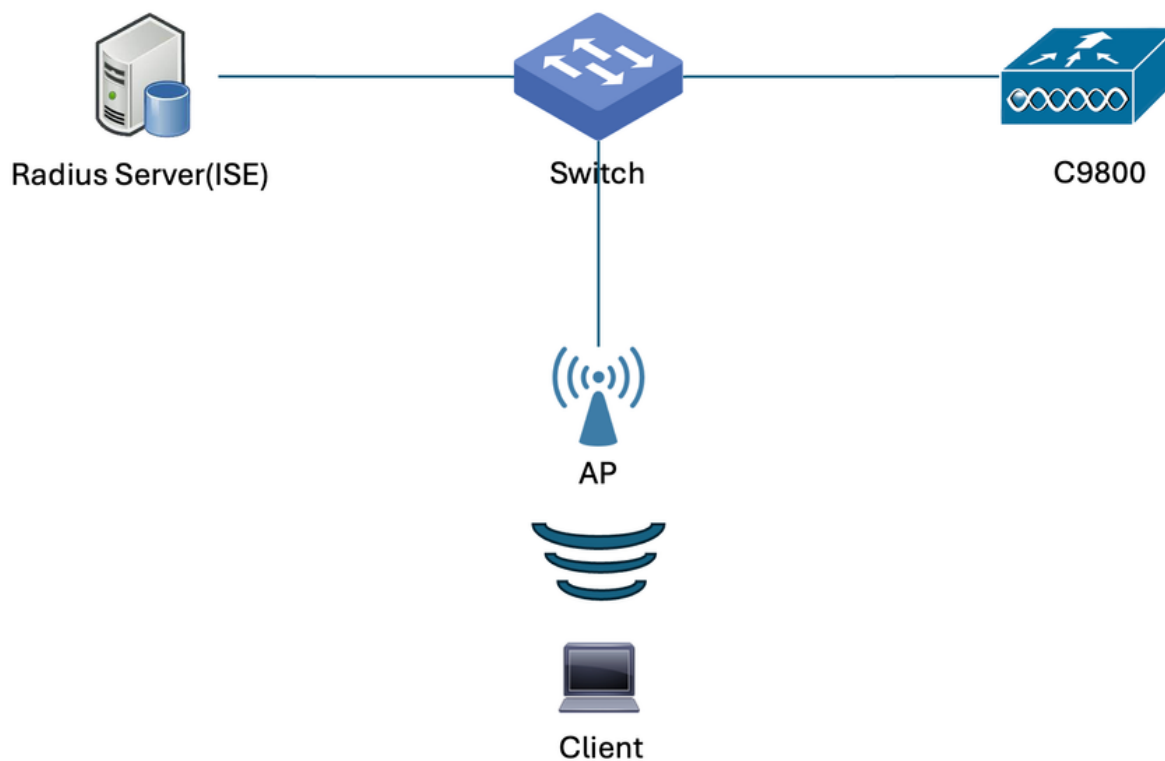
- Cisco Catalyst 9800 WLC Cisco IOS®XE Version 17.15.3
- Identity Service Engine (ISE) v3.4.0.608

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau

Le présent document se fonde sur la topologie suivante :

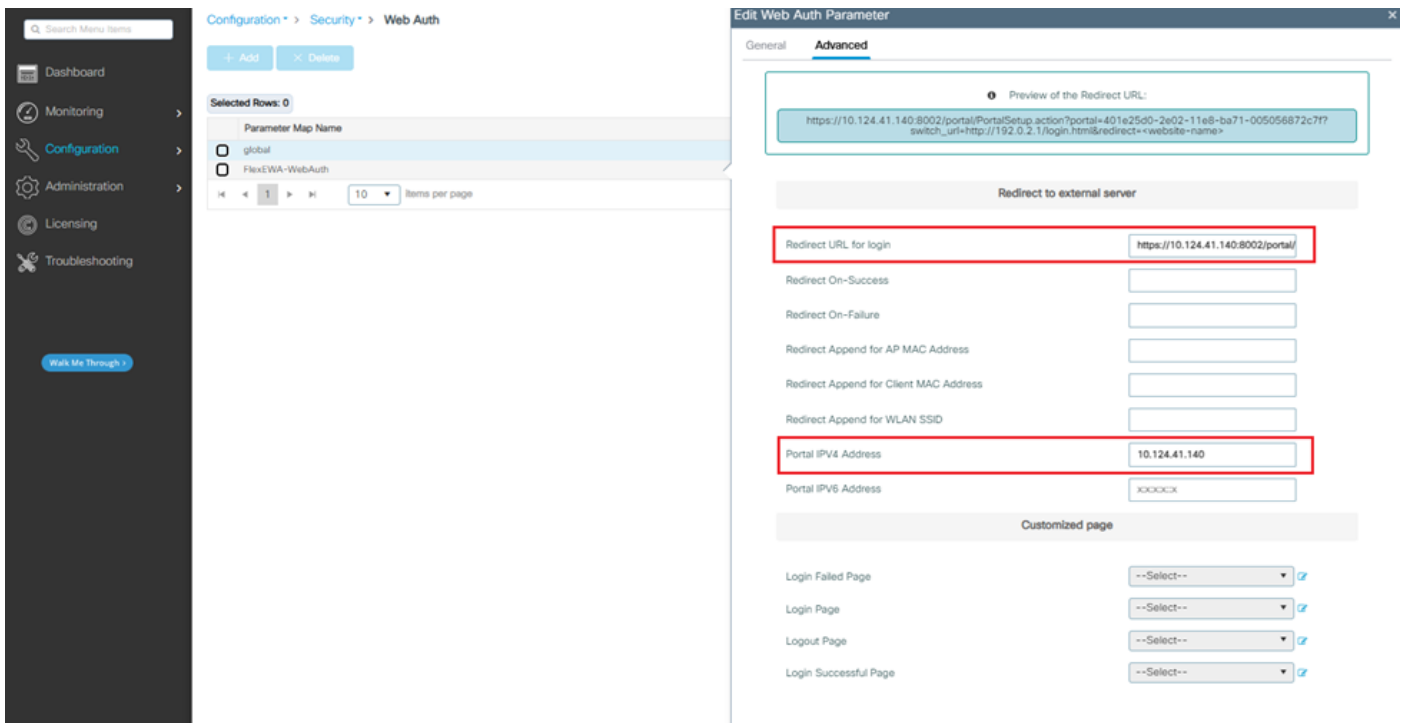


Configurations

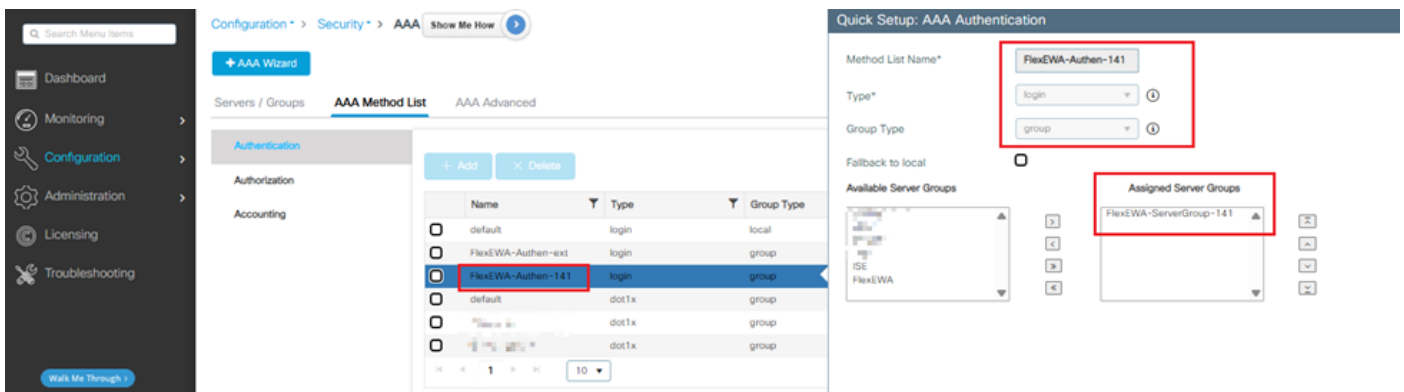
Étape 1. Accédez à Configuration > Security > Web Auth > +Add a Web Auth Parameter Map.

The screenshot shows the Cisco ISE configuration interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area displays the 'Configuration > Security > Web Auth' path. A table lists parameter maps: 'global', 'FlexEWA-WebAuth', and 'FlexEWA-WebAuth-141'. The 'FlexEWA-WebAuth-141' map is selected. On the right, the 'Edit Web Auth Parameter' dialog is open, showing the 'General' tab. The 'Parameter-map Name' is 'FlexEWA-WebAuth-141', 'Maximum HTTP connections' is 100, 'Init-State Timeout(secs)' is 120, and 'Type' is 'webauth'. The 'Banner Configuration' section shows 'Banner Title' and 'Banner Type' (set to 'None').

L'URL du portail est générée à partir d'ISE (étape 7).



Étape 2. Accédez à Configuration > Security > AAA > AAA Method List > Authentication > + Add an Authentication List.



Étape 3. Supposons que le port HTTPS soit 8002, reportez-vous à la liste de contrôle d'accès générée automatiquement WA-sec-10.124.41.140 pour ajouter une nouvelle liste de contrôle d'accès de préauthentification.

The screenshot shows the 'Edit ACL' configuration for 'FlexEWA141-sec-ACL'. The ACL Type is 'IPv4 Extended'. The Rules section shows a list of 10 rules, all with 'permit' action. The rules are summarized in the table below:

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

Étape 4 : vérification de la liste de contrôle d'accès générée automatiquement WA-v4-int 10.124.41.141

The screenshot shows the 'Edit ACL' configuration for 'WA-v4-int-10.124.41.141'. The ACL Type is 'IPv4 Extended'. The Rules section shows a list of 2 rules, both with 'deny' action. The rules are summarized in the table below:

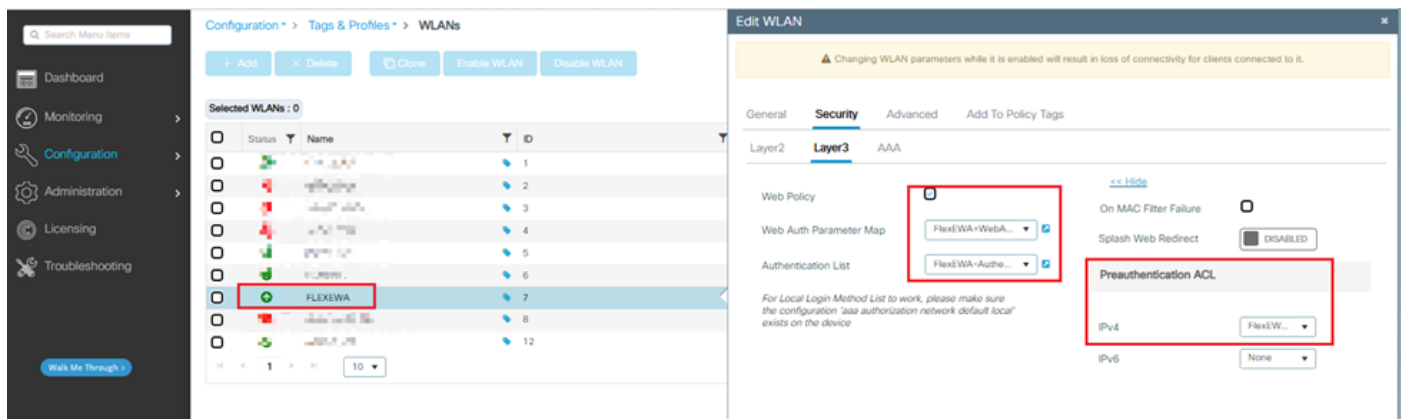
Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	deny	any		10.124.41.141		tcp	None	eq www	None	Disabled
20	deny	any		any		tcp	None	eq www	None	Disabled

Étape 5. Appliquer les deux ACL à Configuration > Tags&Profiles > Flex > Flex Profile > Policy ACL.

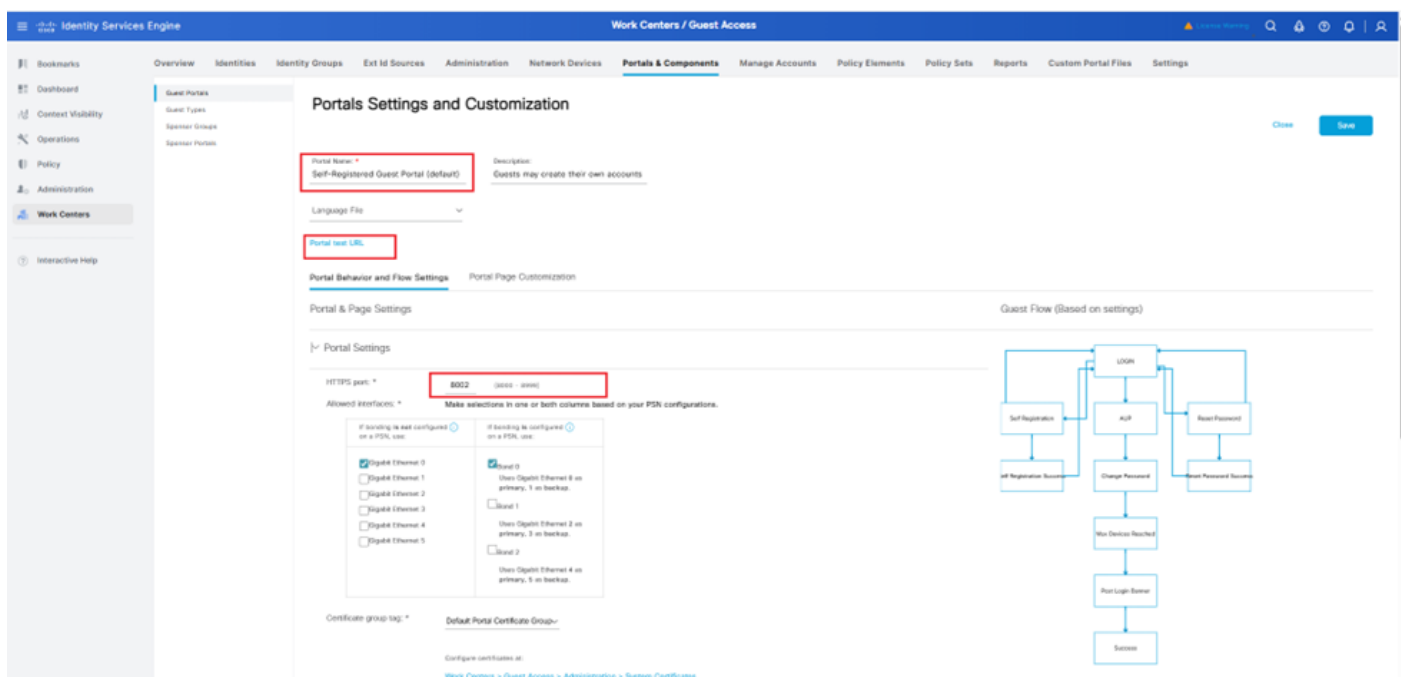
The screenshot shows the 'Edit Flex Profile' configuration for 'default-flex-profile'. The 'Policy ACL' tab is selected. The ACLs are listed in the table below:

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

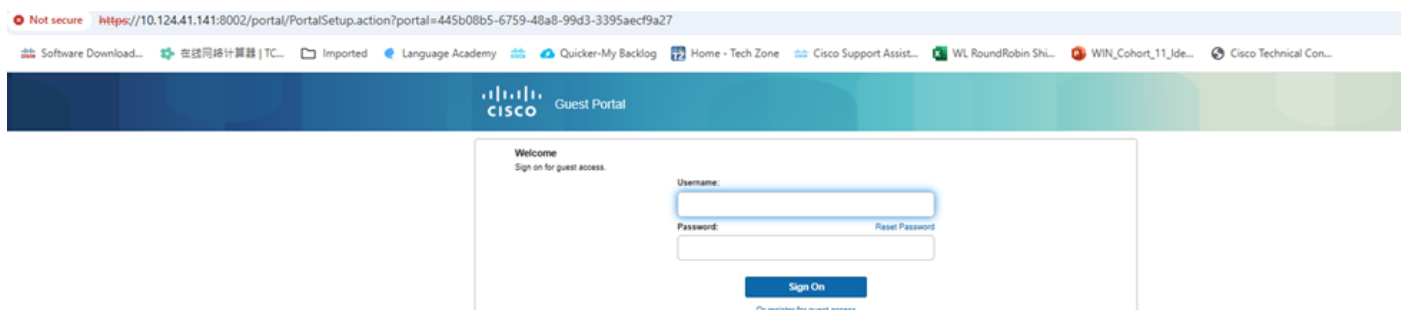
Étape 6. Application de la carte de paramètres d'authentification Web, de la liste d'authentification et de la liste de contrôle d'accès de préauthentification nouvellement créées au WLAN



Étape 7. Accédez à Work Centers > Portals & Components > Guest Portals > Portals Settings and Customization > Portal Name > Self-Registered Guest Portal (par défaut) pour générer l'URL du portail à partir d'ISE.

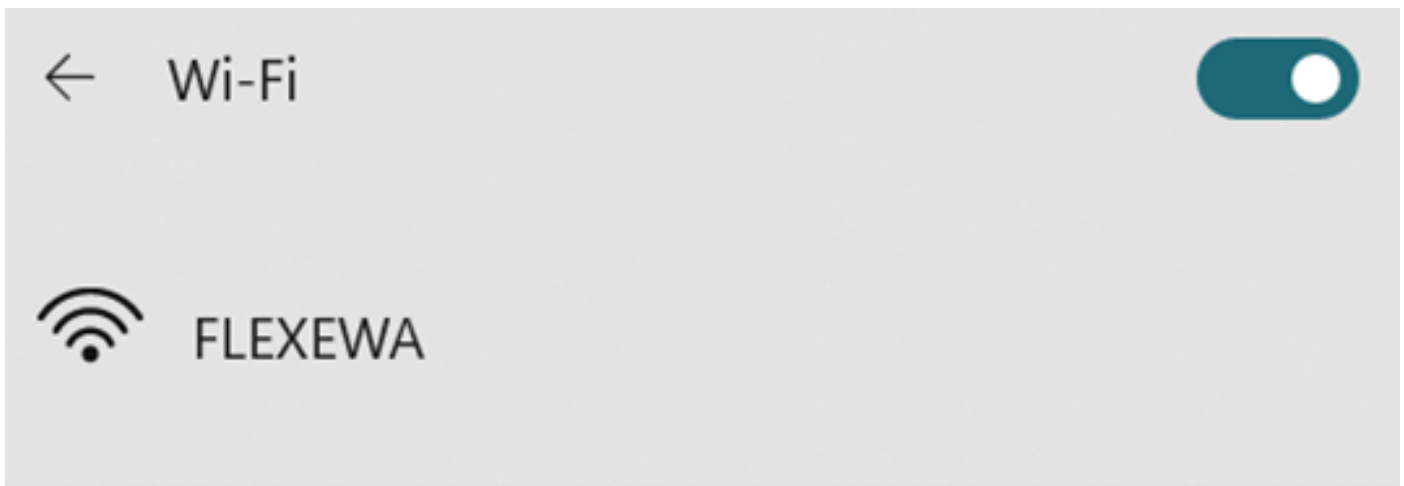


Ce portail Web répertorié apparaît après avoir cliqué sur URL de test du portail.

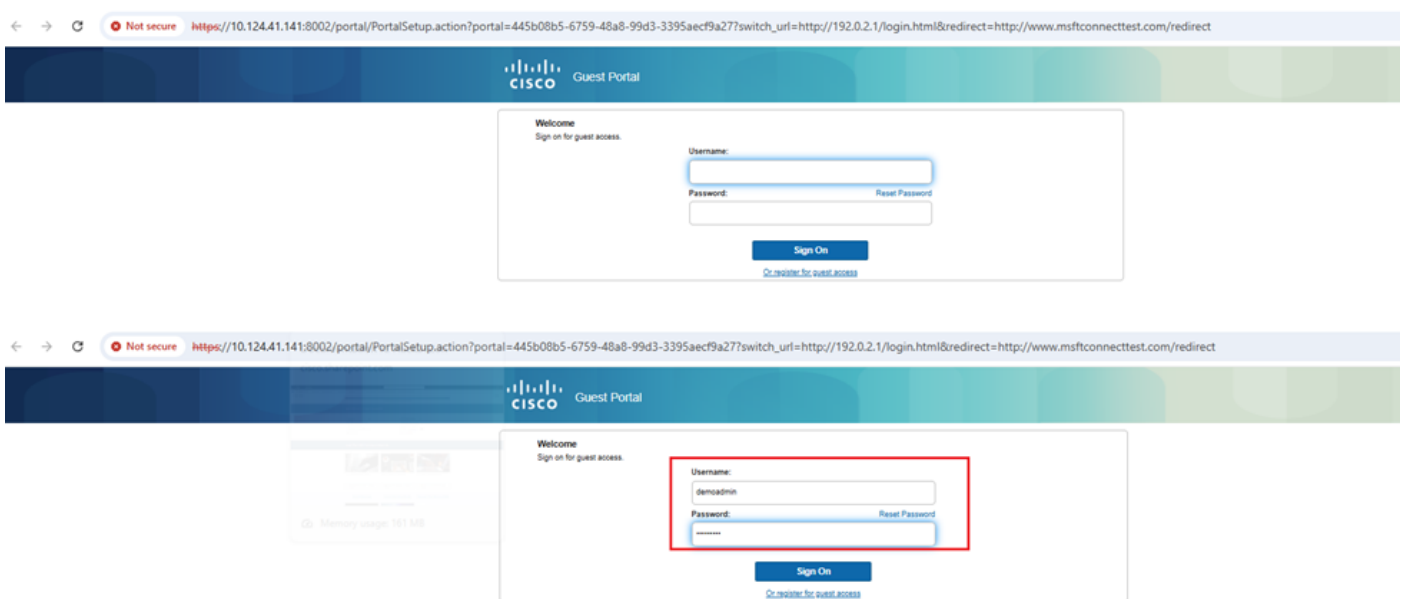


Vérifier

Étape 1. Connexion du SSID FLEXEWA



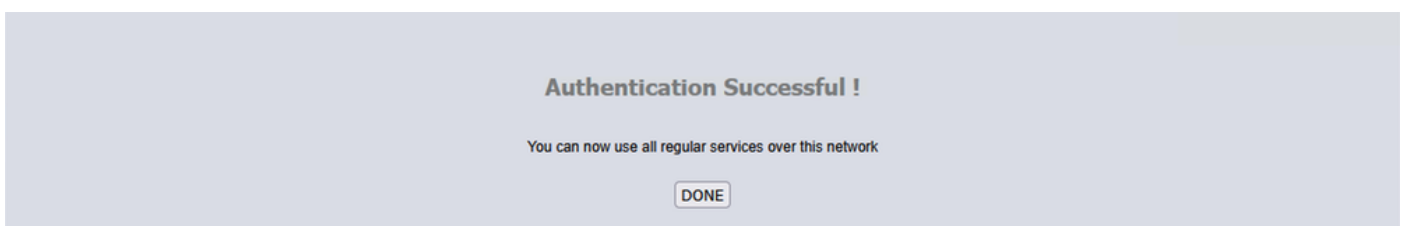
Étape 2. Redirection vers le portail et saisie du nom d'utilisateur et du mot de passe.



Étape 3. Le portail invité s'affiche :



Étape 4. Après avoir cliqué sur Continue, Authentication is Successful :



Exemple de suivi RA d'une tentative réussie

Il s'agit du résultat d'une tentative de connexion réussie du point de vue de la trace radio active.
Servez-vous de cette référence pour identifier les étapes de session client pour les clients qui se connectent à un SSID d'authentification Web de couche 3.

Client associé avec succès :

2025/09/09 15:21:48.617769958 {wncd_x_R0-0}{1} : [client-orch-sm] [17842] : (remarque) : MAC : f0b6.1e39.9ce8 Association reçue. BSSID c418.fc82.bb0b, WLAN FLEXEWA, Slot 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, BSSID MAC AP c418.fc82.bb0b
2025/09/09 15:21:48.617813534 {wncd_x_R0-0}{1} : [client-orch-sm] [17842] : (débogage) : MAC : f0b6.1e39.9ce8 A reçu une demande d'association Dot11. Traitement démarré,SSID : FLEXEWA, Profil de politique : default-policy-profile, Nom AP : 9178_1, Adresse Mac Ap : c418.fc82.bb00BSSID ID MAC0000.0000.0000wlan : 7RSSI : -30, NUJ : 67
2025/09/09 15:21:48.618002570 {wncd_x_R0-0}{1} : [client-orch-state] [17842] : (remarque) : MAC : f0b6.1e39.9ce8 Transition de l'état du client : 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 Impossible d'obtenir l'enregistrement dot11
2025/09/09 15:21:48.618301251 {wncd_x_R0-0}{1} : [dot11-validate] [17842] : (info) : MAC : f0b6.1e39.9ce8 Dot11 ie valider les taux ext/supp. Validation réussie pour les taux pris en charge radio_type 2
2025/09/09 15:21:48.618320304 {wncd_x_R0-0}{1} : [dot11-validate] [17842] : (débogage) : MAC : f0b6.1e39.9ce8 Dot11 ie valide rsnx, client n'utilisant pas sae, ignorer la vérification
2025/09/09 15:21:48.618339230 {wncd_x_R0-0}{1} : [dot11-validate] [17842] : (info) : MAC : f0b6.1e39.9ce8 WiFi direct : Dot11 valide l'IE P2P. IE P2P absent.
2025/09/09 15:21:48.618598747 {wncd_x_R0-0}{1} : [point11] [17842] : (débogage) : MAC : f0b6.1e39.9ce8 dot11 envoie une réponse d'association. Réponse d'association de tramage avec resp_status_code : 0
2025/09/09 15:21:48.618604733 {wncd_x_R0-0}{1} : [point11] [17842] : (débogage) : MAC : f0b6.1e39.9ce8 Dot11 Informations sur les capacités octet1 1, octet2 : 11
2025/09/09 15:21:48.618696034 {wncd_x_R0-0}{1} : [dot11-frame] [17842] : (info) : MAC : f0b6.1e39.9ce8 WiFi direct : ignorer la création d'un revendeur associé avec un IE P2P : Stratégie directe Wi-Fi désactivée
2025/09/09 15:21:48.618785409 {wncd_x_R0-0}{1} : [point11] [17842] : (info) : MAC : f0b6.1e39.9ce8 dot11 envoie une réponse d'association. Longueur de la réponse assoc d'envoi : 177 avec resp_status_code : 0, DOT11_STATUS : SUCCÈS_ÉTAT_POINT11
2025/09/09 15:21:48.618791096 {wncd_x_R0-0}{1} : [point11] [17842] : (remarque) : MAC : f0b6.1e39.9ce8 Association réussie. AID 33, Itinérance = Faux, WGB = Faux, 11r = Faux, 11w = Faux Itinérance rapide = Faux
2025/09/09 15:21:48.618806595 {wncd_x_R0-0}{1} : [point11] [17842] : (info) : MAC : f0b6.1e39.9ce8 DOT11 transition d'état : S_DOT11_INIT -> S_DOT11_ASSOCIATED
2025/09/09 15:21:48.618855282 {wncd_x_R0-0}{1} : [client-orch-sm] [17842] : (débogage) : MAC : L'association f0b6.1e39.9ce8 Station Dot11 a réussi.

Authentification de couche 2 ignorée :

2025/09/09 15:21:48.618992721 {wncd_x_R0-0}{1} : [client-orch-sm] [17842] : (débogage) : MAC :

f0b6.1e39.9ce8 Démarrage de l'authentification L2. Bssid dans l'ordinateur d'état :c418.fc82.bb0b
 Le Bssid dans la demande est :c418.fc82.bb0b
 2025/09/09 15:21:48.619006036 {wncd_x_R0-0}{1} : [client-orch-state] [17842] : (remarque) : MAC : f0b6.1e39.9ce8 Transition de l'état du client : S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
 2025/09/09 15:21:48.619093387 {wncd_x_R0-0}{1} : [auth-client] [17842] : (remarque) : MAC : f0b6.1e39.9ce8 L2 Authentication initié. méthode WEBAUTH, Policy VLAN 0, AAA override = 0 [...]
 2025/09/09 15:21:48.623839337 {wncd_x_R0-0}{1} : [auth-client] [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] Le type de périphérique de la session est détecté en tant que périphérique Intel et l'ancien nom de périphérique Intel de la session est détecté en tant que réseau INTEL CORPORATE et l'ancien réseau INTEL CORPORATE et l'ancien protocole map 1 et new est 1
 2025/09/09 15:21:48.623873529 {wncd_x_R0-0}{1} : [auth-mgr] [17842] : (info) : [f0b6.1e39.9ce8:capwap_90000008] une notification d'ajout/de modification d'attributs auth mgr est reçue pour attr dc-profile-name(1130)
 2025/09/09 15:21:48.623911035 {wncd_x_R0-0}{1} : [client-orch-sm] [17842] : (débogage) : MAC : f0b6.1e39.9ce8 L'authentification L2 de la station a réussi., Authentification L3 : 1

Plumb ACL :

2025/09/09 15:21:48.620896754 {wncd_x_R0-0}{1} : [webauth-sm] [17842] : (info) : [0.0.0.0]Démarrage de Webauth, mac [f0:b6:1e:39:9c:e8], IF 0, ID d'audit 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 utilisé : global
 2025/09/09 15:21:48.620935005 {wncd_x_R0-0}{1} : [webauth-state] [17842] : (info) : [f0b6.1e39.9ce8][0.0.0.0]État non valide -> 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]Créer une session, Ajouter une adresse 0.0.0.0
 2025/09/09 15:21:48.620946808 {wncd_x_R0-0}{1} : [auth-mgr-feat_wireless] [17842] : (info) : [0000.0000.0000:unknown] ID de zone 0x0 récupéré pour 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 utilisé : 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]State 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]Lance la session, transmet l'état à 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]Initialisation de session, sessions d'initialisation SM 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 utilisé : 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]State 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]Application d'une liste de contrôle d'accès d'interception IPv4 via SVM, nom : WA-v4-int-10.124.41.141-7, priorité : 50, IIF-ID : 0

2025/09/09 15:21:48.621032776 {wncd_x_R0-0}{1} : [svm] [17842] : (info) : SVM_INFO : Application du modèle de service WA-v4-int-10.124.41.141-7 (ML : AUCUN)

2025/09/09 15:21:48.621786262 {wncd_x_R0-0}{1} : [epm] [17842] : (info) : [f0b6.1e39.9ce8:capwap_90000008] La fonctionnalité (EPM URL PLUG-IN) a été démarrée (état Succès)

2025/09/09 15:21:48.621804034 {wncd_x_R0-0}{1} : [epm-acl] [17842] : (info) : [f0b6.1e39.9ce8:capwap_90000008] ID de filtre : FlexEWA141-sec-ACL reçue

2025/09/09 15:21:48.622151544 {wncd_x_R0-0}{1} : [epm] [17842] : (info) : [f0b6.1e39.9ce8:capwap_90000008] La fonctionnalité (EPM ACL PLUG-IN) a été démarrée (état Succès)

2025/09/09 15:21:48.622187815 {wncd_x_R0-0}{1} : [svm] [17842] : (info) : SVM_INFO : La réponse de epm est SYNC avec le code de retour Success

2025/09/09 15:21:48.622226011 {wncd_x_R0-0}{1} : [auth-mgr] [17842] : (info) : [f0b6.1e39.9ce8:capwap_90000008] Déclenchement du modèle d'événement suivant activé (9) sur cette session, client (inconnu) (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]Application d'une liste de contrôle d'accès d'interception IPv6 via SVM, nom : IP-Adm-V6-Int-ACL-global-7, priorité : 52, IIF-ID : 0

2025/09/09 15:21:48.622270327 {wncd_x_R0-0}{1} : [svm] [17842] : (info) : SVM_INFO : Application du modèle de service 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] La fonctionnalité (EPM URL PLUG-IN) a été démarrée (état Succès)

2025/09/09 15:21:48.622932973 {wncd_x_R0-0}{1} : [svm] [17842] : (info) : SVM_INFO : La réponse de epm est SYNC avec le code de retour Success

2025/09/09 15:21:48.622957784 {wncd_x_R0-0}{1} : [auth-mgr] [17842] : (info) : [f0b6.1e39.9ce8:capwap_90000008] Déclenchement du modèle d'événement suivant activé (9) sur cette session, client (inconnu) (0)

2025/09/09 15:21:48.623119047 {wncd_x_R0-0}{1} : [point11] [17842] : (débogage) : MAC : f0b6.1e39.9ce8 Dot11 SAE détecte ipsk progress comme 0, pas dans l'état en attente

2025/09/09 15:21:48.623126095 {wncd_x_R0-0}{1} : [llbridge-main] [17842] : (débogage) : MAC : f0b6.1e39.9ce8 Le pontage link-local n'est pas activé pour ce client et ne vérifie pas la validité du VLAN

2025/09/09 15:21:48.623205421 {wncd_x_R0-0}{1} : [auth-mgr] [17842] : (info) : [f0b6.1e39.9ce8:capwap_90000008] Modification de l'état du contexte de 'Inactif' à 'En cours d'exécution'

2025/09/09 15:21:48.623209350 {wncd_x_R0-0}{1} : [auth-mgr] [17842] : (info) : [f0b6.1e39.9ce8:capwap_90000008] La méthode webauth passe de l'état « Not run » à « Running »

2025/09/09 15:21:48.623572855 {wncd_x_R0-0}{1} : [auth-mgr] [17842] : (info) : [f0b6.1e39.9ce8:capwap_90000008] SM ne peut pas envoyer le modèle d'événement activé au

PRE pour 0x8D0000C0

2025/09/09 15:21:48.623680228 {wncd_x_R0-0}{1} : [auth-client] [17842] : (info) : MAC : f0b6.1e39.9ce8 Client auth-interface state transition :

S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP -> S_AUTHIF_L2_WEBAUTH_PENDING

Processus d'apprentissage IP :

2025/09/09 15:21:51.628124695 {wncd_x_R0-0}{1} : [client-orch-state] [17842] : (remarque) : MAC : f0b6.1e39.9ce8 Transition de l'état du client : 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 Transition de l'état IP-learn : S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

2025/09/09 15:21:51.632284534 {wncd_x_R0-0}{1} : [auth-client] [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: DHCP IPv6

à partir de intf capwap_90000008 sur vlan 174 Src MAC : f0b6.1e39.9ce8 Dst MAC :

3333.0001.0002 Ipv6 SRC : fe80::3f83:2848:d30:7aea, heure d'été IPv6 : ff02::1:2, type : type de message : DHCPV6_MSG_SOLICIT xid : 14443573

2025/09/09 15:21:51.676541447 {wncd_x_R0-0}{1} : [sisf-packet] [17842] : (info) : TX: DHCP IPv6

à partir de intf capwap_90000008 sur vlan 174 Src MAC : f0b6.1e39.9ce8 Dst MAC :

3333.0001.0002 Ipv6 SRC : fe80::3f83:2848:d30:7aea, heure d'été IPv6 : ff02::1:2, type : type de message : DHCPV6_MSG_SOLICIT xid : 14443573

2025/09/09 15:21:51.706187097 {wncd_x_R0-0}{1} : [sisf-packet] [17842] : (info) : RX: ARP de l'interface capwap_90000008 sur le VLAN 174 Adresse MAC source : f0b6.1e39.9ce8 MAC dest. :

ffff.ffff.ffff REQUÊTE ARP, adresse MAC de l'expéditeur ARP : MAC cible ARP f0b6.1e39.9ce8 :

0000.0000.0000 ARP expéditeur IP : 169.254.137.222, IP cible ARP : 169.254.137.222,

[...]

2025/09/09 15:21:52.686190945 {wncd_x_R0-0}{1} : [client-iplearn] [17842] : (remarque) : MAC :

f0b6.1e39.9ce8 Client IP learn successful. Méthode : IP DHCP : 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] une notification d'ajout/de modification d'attribut auth mgr est reçue pour attr addr(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]Notification de modification CB, Ajouter l'adresse

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 de zone 0x0 récupéré pour bssid 12364632846638254486

2025/09/09 15:21:52.686291647 {wncd_x_R0-0}{1} : [webauth-sess] [17842] : (info) : ajout d'une

session webauth à la table de hachage ipv4 pour vrf id 0, ipv4 vrf table 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 attribute Add/Update 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 nombre d'échecs du VLAN 174 0 compteur_sale 0 is_sale 0

2025/09/09 15:21:52.686710209 {wncd_x_R0-0}{1} : [client-iplearn] [17842] : (info) : MAC :

f0b6.1e39.9ce8 Transition de l'état IP-learn : S_IPLEARN_IN_PROGRESS ->
S_IPLEARN_COMPLETE

Processus d'authentification et de redirection de couche 3 :

2025/09/09 15:21:52.687395906 {wncd_x_R0-0}{1} : [auth-client] [17842] : (remarque) : MAC : f0b6.1e39.9ce8 Lancement de l'authentification L3. LOI

2025/09/09 15:21:52.687472722 {wncd_x_R0-0}{1} : [auth-client] [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 à partir de l'interface Po1 sur le VLAN 174 Src MAC : 4006.d589.4e78 Dst MAC : ffff.ffff.ffff ip_source : 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 à partir de l'interface Po1 sur le 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] : (explicite) : 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 État des E/S NOUVEAU -> LECTURE

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 Lire l'événement, Message prêt

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 en état INIT

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]Requête HTTP GET

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 reçu en état LOGIN

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]Annuler l'application de la liste de contrôle d'accès IPv4 interceptée via SVM, nom « WA-v4-int-10.124.41.141-7 », pri 50, IF 0

2025/09/09 15:22:32.376230716 {wncd_x_R0-0}{1} : [auth-mgr] [17842] : (info) : [f0b6.1e39.9ce8:capwap_90000008] Déclenchement du modèle d'événement suivant désactivé (11) sur cette session, client (inconnu) (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]Annuler l'application de la liste de contrôle

d'accès IPv6 interceptée via SVM, nom « IP-Adm-V6-Int-ACL-global », pri 52, IF 0
2025/09/09 15:22:32.376734374 {wncd_x_R0-0}{1} : [auth-mgr] [17842] : (info) :
[f0b6.1e39.9ce8:capwap_90000008] Déclenchement du modèle d'événement suivant désactivé
(11) sur cette session, client (inconnu) (0)
2025/09/09 15:22:32.376865998 {wncd_x_R0-0}{1} : [point11] [17842] : (débogage) : MAC :
f0b6.1e39.9ce8 Dot11 SAE détecte ipsk progress comme 0, pas dans l'état en attente
2025/09/09 15:22:32.376870611 {wncd_x_R0-0}{1} : [llbridge-main] [17842] : (débogage) : MAC :
f0b6.1e39.9ce8 Le pontage link-local n'est pas activé pour ce client et ne vérifie pas la validité du
VLAN
2025/09/09 15:22:32.376949875 {wncd_x_R0-0}{1} : [auth-mgr] [17842] : (info) :
[f0b6.1e39.9ce8:capwap_90000008] Authc success from WebAuth, Auth event success

Transition vers l'état EXÉCUTÉ :

2025/09/09 15:22:32.379351256 {wncd_x_R0-0}{1} : [auth-client] [17842] : (remarque) : MAC :
f0b6.1e39.9ce8 ADD MOBILE envoyé. Indicateurs d'état du client : BSSID 0x38 : MAC : IFID
c418.fc82.bb0b capwap : 0x90000008, Ajouter les mobiles envoyés : 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 : Entrée de nom
d'utilisateur (demoadmin) associée à ssid (FLEXEWA) pour le périphérique avec MAC :
f0b6.1e39.9ce8 sur le canal (100)
2025/09/09 15:22:32.379671775 {wncd_x_R0-0}{1} : [aaa-attr-inf] [17842] : (info) : [Attribut
appliqué : bsn-vlan-interface-name 0 "wlc-management"]
2025/09/09 15:22:32.379673695 {wncd_x_R0-0}{1} : [aaa-attr-inf] [17842] : (info) : [Attribut
appliqué : timeout 0 28800 (0x7080)]
2025/09/09 15:22:32.379683417 {wncd_x_R0-0}{1} : [aaa-attr-inf] [17842] : (info) : [Attribut
appliqué : 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 Gestionnaire d'état d'exécution QoS du client
2025/09/09 15:22:32.379756610 {wncd_x_R0-0}{1} : [rog-proxy-capwap] [17842] : (débogage) :
Notification d'état d'exécution du client géré : f0b6.1e39.9ce8
2025/09/09 15:22:32.379810670 {wncd_x_R0-0}{1} : [client-orch-state] [17842] : (remarque) : MAC
: f0b6.1e39.9ce8 Transition de l'état du client : S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Informations connexes

- [Configuration et dépannage de l'authentification Web externe sur le WLC 9800](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.