

Configuration et dépannage de l'authentification Web externe sur le WLC 9800

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration des paramètres Web](#)

[Résumé de la configuration CLL :](#)

[Configuration des paramètres AAA](#)

[Configurer les stratégies et les balises](#)

[Vérifier](#)

[Dépannage](#)

[Suivi permanent](#)

[Débogage conditionnel et traçage Radio Active](#)

[Captures de paquets intégrées](#)

[Dépannage côté client](#)

[Dépannage du navigateur HAR](#)

[Capture de paquets côté client](#)


[Exemple d'une tentative réussie](#)


Introduction

Ce document décrit comment configurer et dépanner l'authentification Web externe (EWA) sur un contrôleur LAN sans fil (WLC) Catalyst 9800.

Conditions préalables

Ce document suppose que le serveur Web est correctement configuré pour permettre la communication externe et la page Web est correctement configurée pour envoyer tous les paramètres nécessaires pour que le WLC authentifie l'utilisateur et déplace les sessions client à l'état d'exécution.

 Remarque : étant donné que l'accès aux ressources externes est limité par le WLC via des autorisations de liste d'accès, tous les scripts, polices, images, etc. qui sont utilisés dans la

 page Web doivent être téléchargés et restent locaux pour le serveur Web.

Les paramètres nécessaires à l'authentification des utilisateurs sont :

- `buttonClicked` : Ce paramètre doit être défini sur la valeur "4" pour que le WLC détecte l'action comme une tentative d'authentification.
- `redirectUrl` : la valeur de ce paramètre est utilisée par le contrôleur pour diriger le client vers un site Web spécifique lors d'une authentification réussie.
- `err_flag` : Ce paramètre est utilisé pour indiquer une erreur telle que des informations incomplètes ou des informations d'identification incorrectes, sur les authentifications réussies, il est défini sur "0".
- `username` : Ce paramètre est uniquement utilisé pour les mappages de paramètres `webauth`. Si la carte de paramètre est définie sur `consentement`, elle peut être ignorée. Il doit contenir le nom d'utilisateur du client sans fil.
- `password` : ce paramètre est uniquement utilisé pour les mappages de paramètres `webauth`. Si la carte de paramètres est définie sur `consentement`, elle peut être ignorée. Il doit contenir le mot de passe du client sans fil.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Développement Web en langage HTML (Hyper Text Markup Language)
- Fonctionnalités sans fil de Cisco IOS®-XE
- Outils de développement de navigateur Web

Composants utilisés

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

- C9800-CL WLC Cisco IOS®-XE Version 17.3.3
- Microsoft Windows Server 2012 avec fonctionnalités IIS (Internet Information Services)
- Points d'accès 2802 et 9117

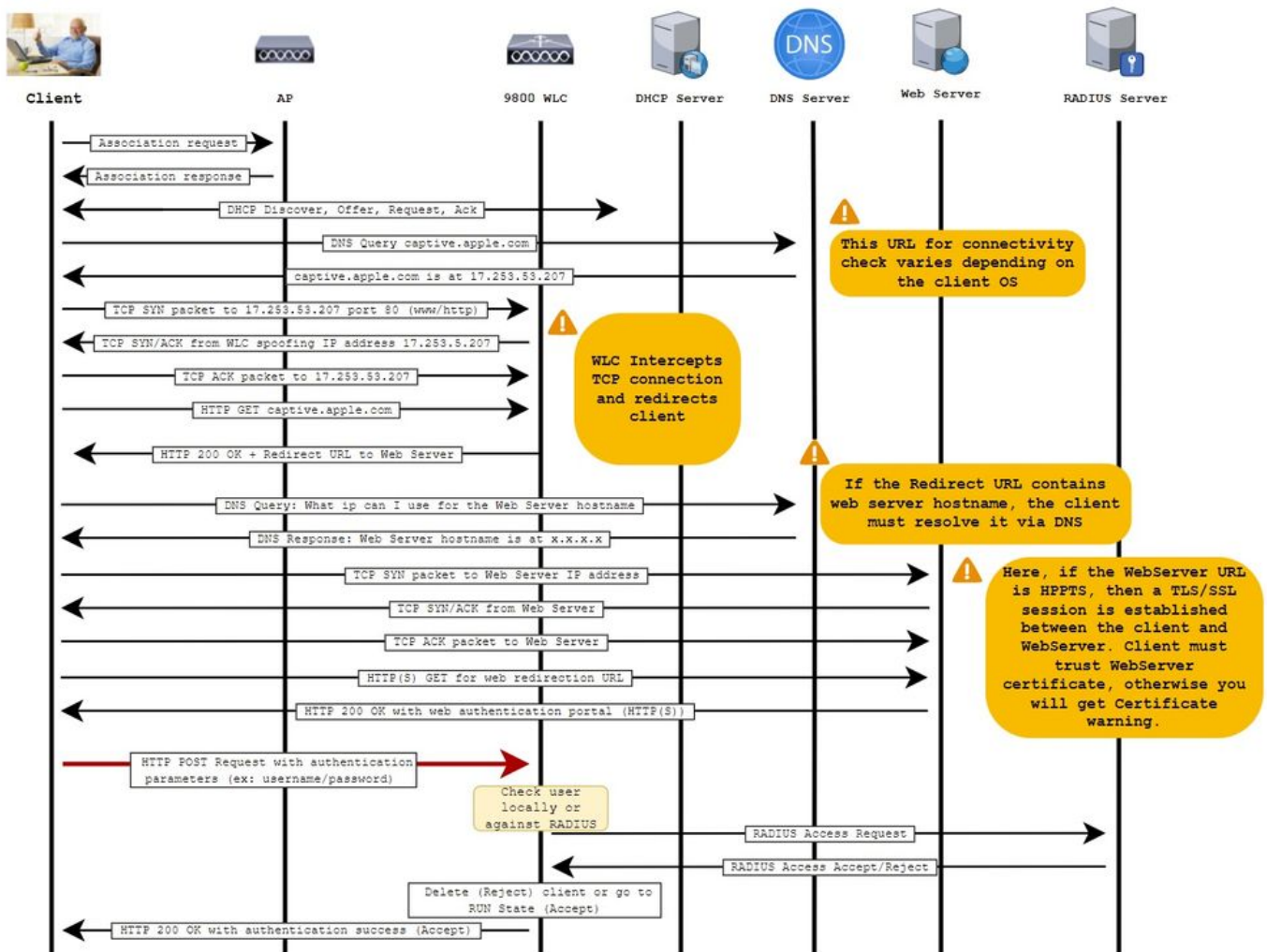
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'authentification Web externe exploite un portail Web hébergé en dehors du WLC sur un serveur Web dédié ou des serveurs polyvalents comme Identity Services Engine (ISE) qui permettent un accès et une gestion granulaires des composants Web. La connexion nécessaire à l'intégration réussie d'un client à un WLAN d'authentification Web externe est restituée dans l'image. L'image répertorie les interactions séquentielles entre le client sans fil, le WLC, le serveur DNS (Domain

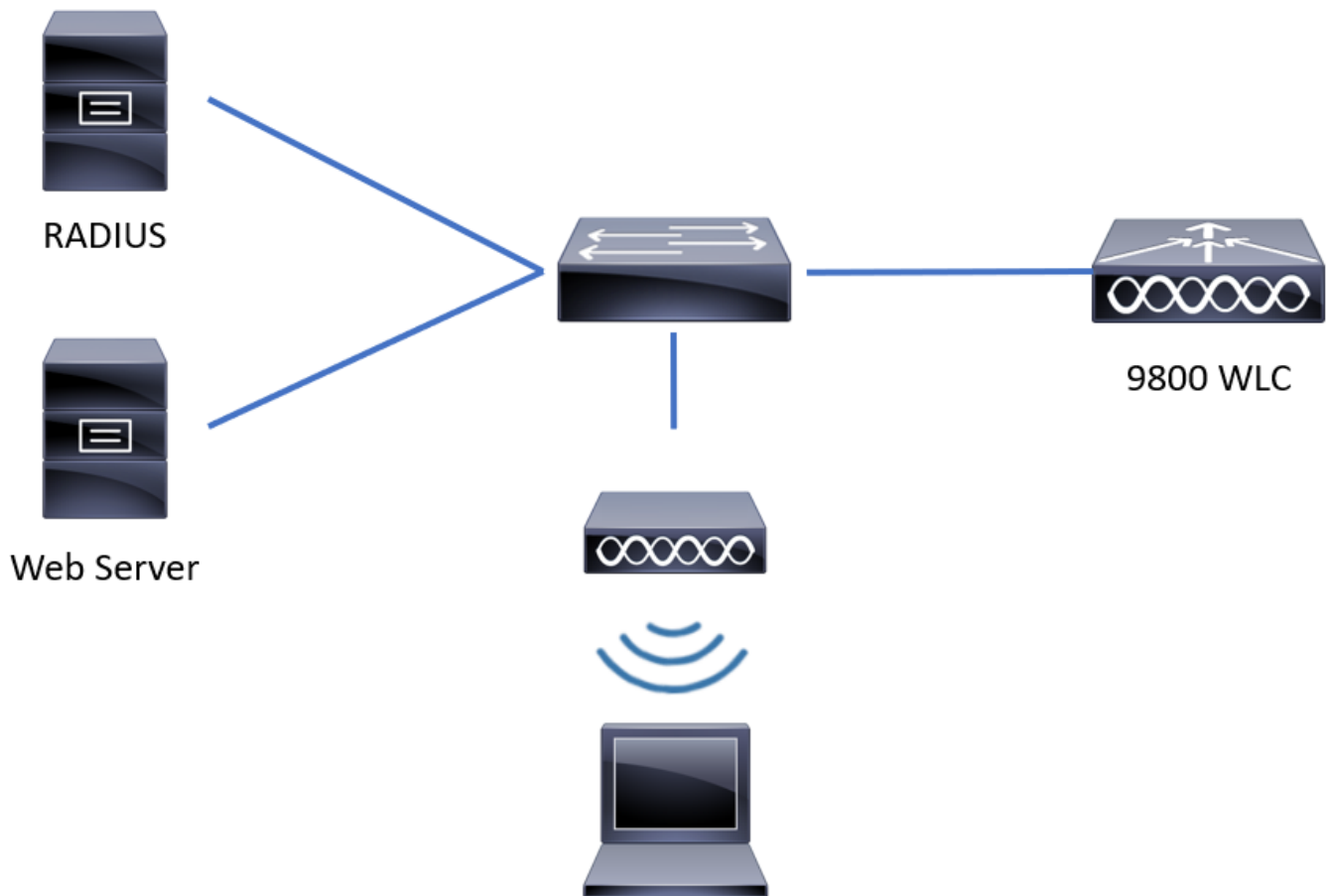
Name System) qui résout l'URL (Uniform Resource Location) et le serveur Web où le WLC valide localement les informations d'identification de l'utilisateur. Ce workflow est utile pour déboguer les conditions d'échec.

Remarque : avant l'appel HTTP POST du client au WLC, si l'authentification Web sécurisée est activée dans la carte-paramètre et si le WLC n'a pas de point de confiance signé par une autorité de certification de confiance, alors une alerte de sécurité est affichée dans le navigateur. Le client doit contourner cet avertissement et accepter le renvoi du formulaire afin que le contrôleur place les sessions client en état d'exécution.




Configurer

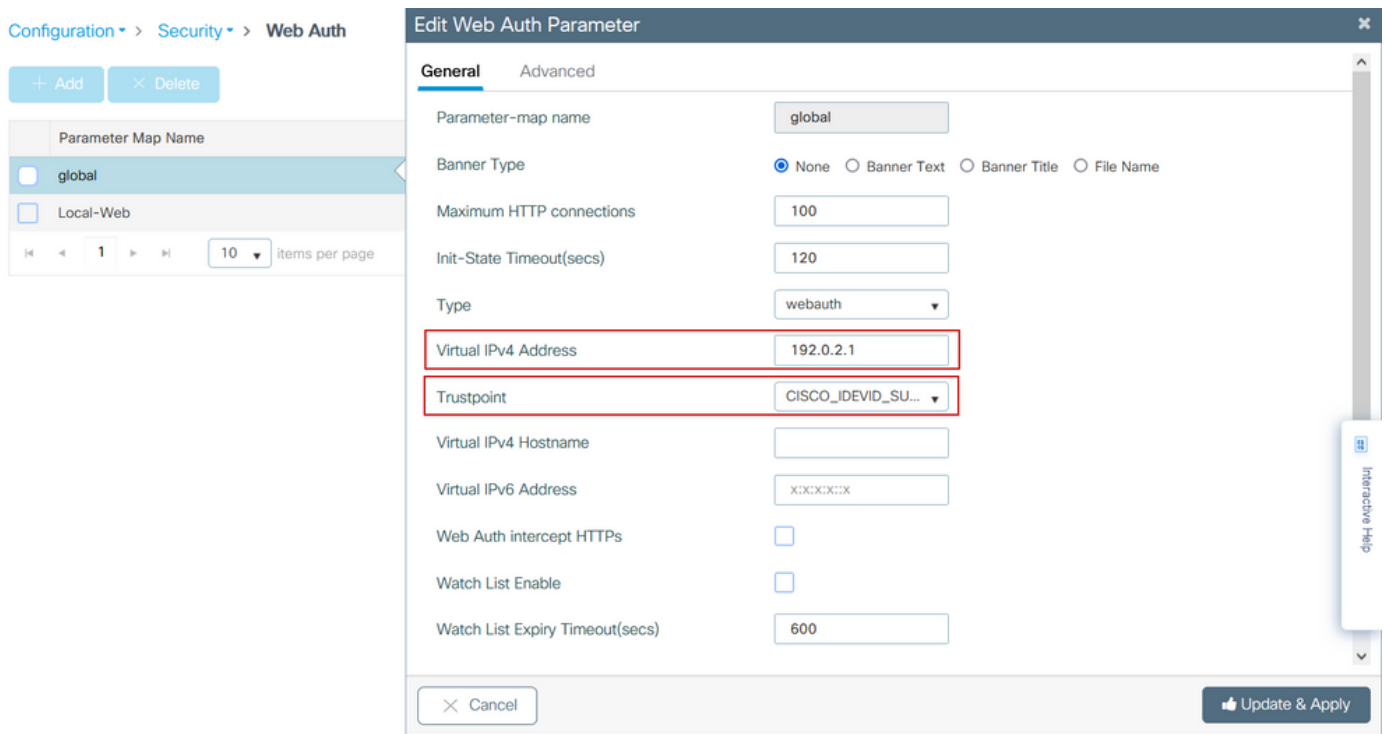
Diagramme du réseau



Configuration des paramètres Web

Étape 1. Accédez à Configuration > Security > Web Auth et choisissez la carte de paramètres globale. Vérifiez que l'adresse IPv4 virtuelle et le point de confiance sont configurés afin de fournir des fonctionnalités de redirection appropriées.

 Remarque : par défaut, les navigateurs utilisent un site Web HTTP pour lancer le processus de redirection. Si la redirection HTTPS est nécessaire, l'interception des HTTP par l'authentification Web doit être vérifiée ; cette configuration n'est cependant pas recommandée, car elle augmente l'utilisation du CPU.



Configuration CLI :

```
<#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
```

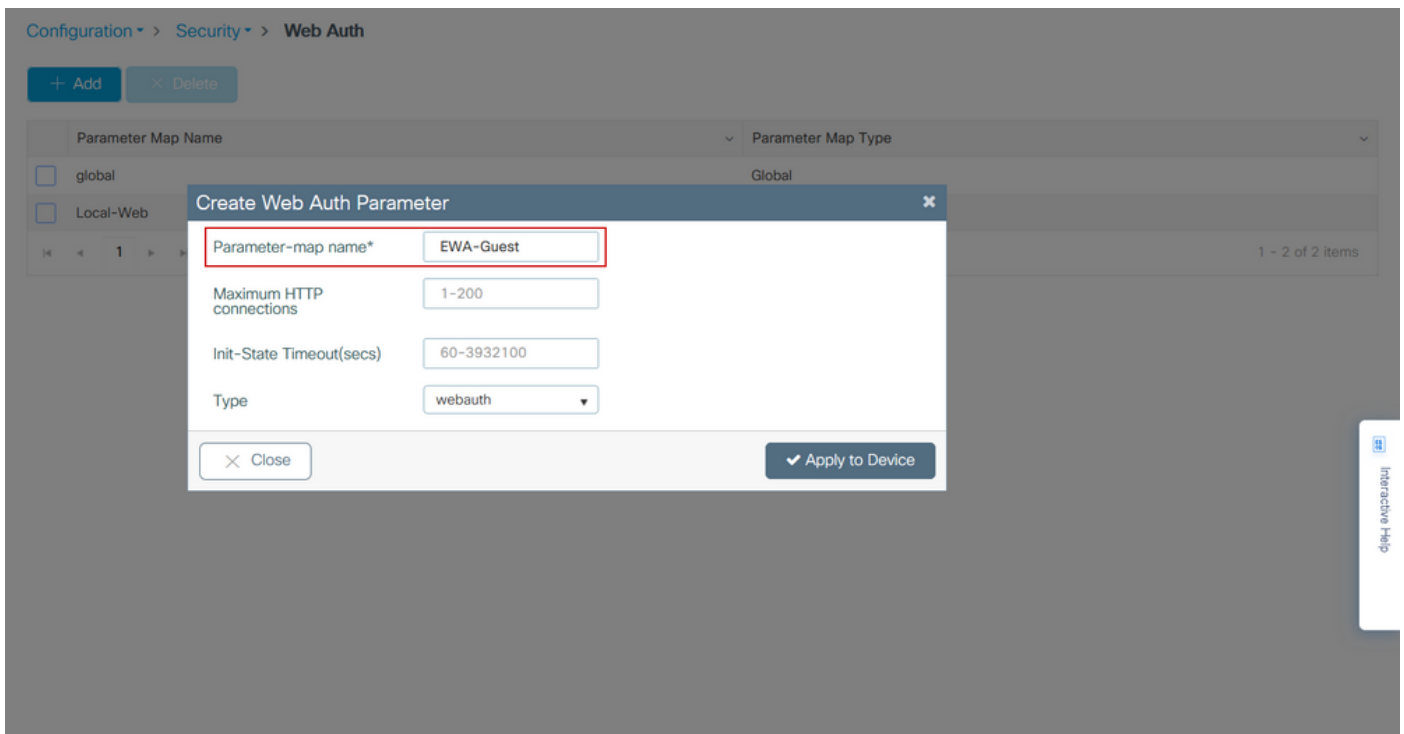
```
9800(config-params-parameter-map)#
```

```
secure-webauth-disable
```

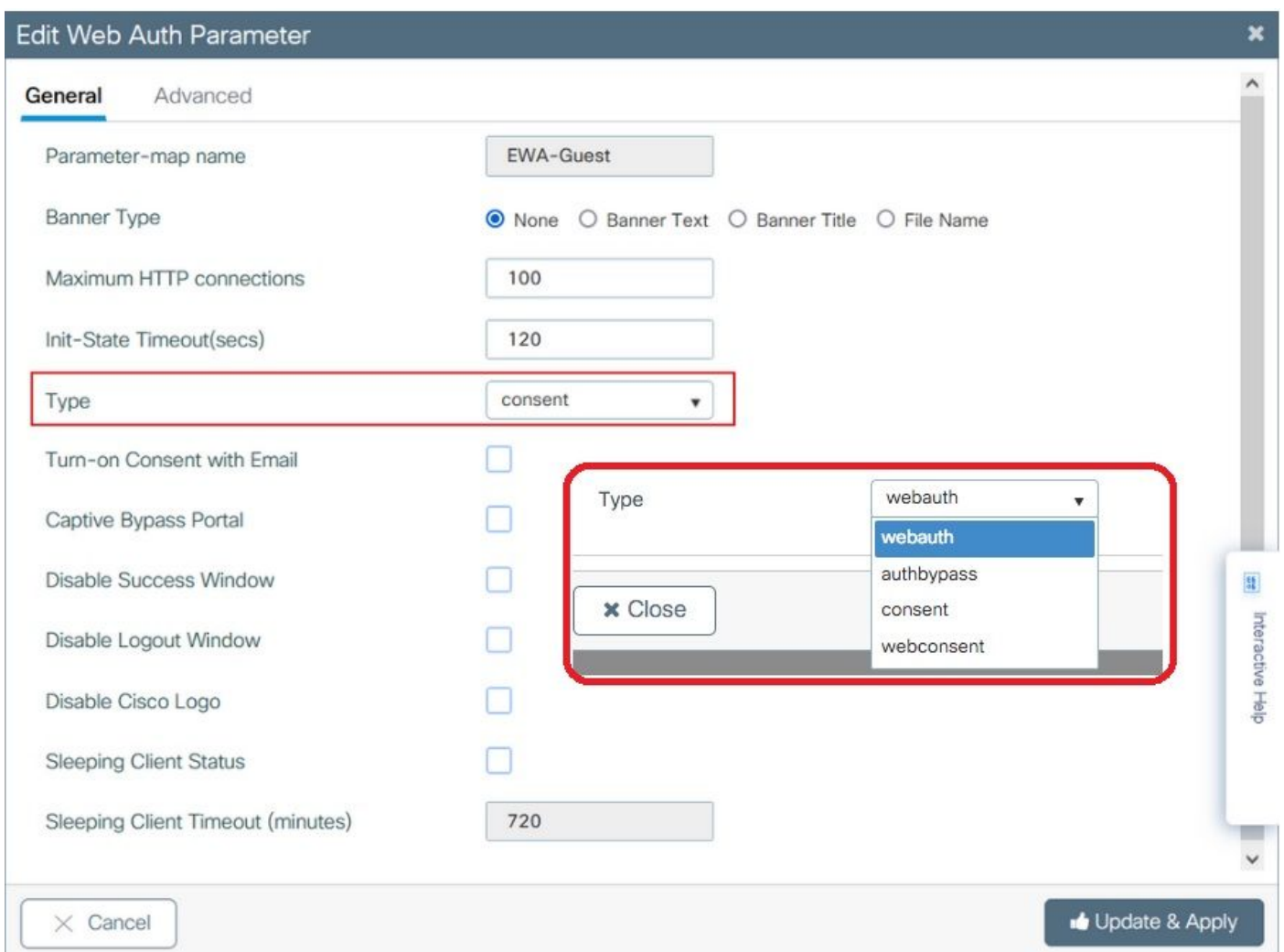
```
9800(config-params-parameter-map)#
```

```
webauth-http-enable
```

Étape 2. Sélectionnez + Ajouter et configurez un nom pour la nouvelle carte de paramètre qui pointe vers le serveur externe. Configurez éventuellement le nombre maximal d'échecs d'authentification HTTP avant que le client ne soit exclu et le temps (en secondes) qu'un client peut rester dans l'état d'authentification Web.



Étape 3. Sélectionnez le mappage de paramètres nouvellement créé, dans l'onglet General et configurez le type d'authentification dans la liste déroulante Type.



- Nom du mappage de paramètre = Nom attribué au mappage de paramètre WebAuth
- Nombre maximal de connexions HTTP = nombre d'échecs d'authentification avant exclusion du client
- Délai d'attente d'état d'initialisation (secondes) = secondes pendant lesquelles un client peut être à l'état d'authentification Web
- Type = Type d'authentification Web

webauth	authbypass	consentement	consentement Internet
<p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p><input type="button" value="OK"/></p>	<p>Le client se connecte au SSID et obtient une adresse IP, puis le WLC 9800 vérifie si l'adresse MAC est autorisé à entrer dans le réseau, si oui, il est déplacé à l'état EXÉCUTER, si ce n'est pas le cas non autorisé à rejoindre.</p> <p>(Il ne revient pas à l'authentification Web)</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="text"/></p> <p><input type="button" value="OK"/></p>

Étape 4. Dans l'onglet Advanced, configurez la redirection pour la connexion et l'adresse IPV4 du portail avec l'URL du site serveur et l'adresse IP spécifiques respectivement.

Edit Web Auth Parameter ✕

General
Advanced

Redirect to external server

Redirect for log-in	<input style="width: 60%;" type="text" value="http://172.16.80.8/w"/>
Redirect On-Success	<input style="width: 60%;" type="text"/>
Redirect On-Failure	<input style="width: 60%;" type="text"/>
Redirect Append for AP MAC Address	<input style="width: 60%;" type="text" value="ap_mac"/>
Redirect Append for Client MAC Address	<input style="width: 60%;" type="text" value="client_mac"/>
Redirect Append for WLAN SSID	<input style="width: 60%;" type="text" value="ssid"/>
Portal IPv4 Address	<input style="width: 60%;" type="text" value="172.16.80.8"/>
Portal IPv6 Address	<input style="width: 60%;" type="text" value="X::X::X::X"/>
Express WiFi Key Type	<input style="width: 60%;" type="text" value="--- Select ---"/>

Customized page

Login Failed Page	<input style="width: 60%;" type="text"/>
-------------------	--

✕ Cancel
👍 Update & Apply

? Interactive Help

Configuration CLI pour les étapes 2, 3 et 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
  
```

Étape 5. (Facultatif) WLC peut envoyer les paramètres supplémentaires via Query String. Cela est souvent nécessaire pour rendre le 9800 compatible avec les portails externes tiers. Les champs "Redirect Append for AP MAC Address", "Redirect Append for Client MAC Address" et "Redirect Append for WLAN SSID" permettent d'ajouter des paramètres supplémentaires à la liste de

contrôle d'accès de redirection avec un nom personnalisé. Sélectionnez la carte de paramètres nouvellement créée et accédez à l'onglet Avancé, configurez le nom pour les paramètres nécessaires. Les paramètres disponibles sont les suivants :

- Adresse MAC du point d'accès (au format aa:bb:cc:dd:ee:ff)
- Adresse MAC du client (au format aa:bb:cc:dd:ee:ff)
- Nom SSID

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

Configuration CLI :

```
<#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
```

Pour cet exemple, l'URL de redirection envoyée au client se traduit par :

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

 Remarque : lorsque vous ajoutez les informations d'adresse IPv4 du portail, il ajoute automatiquement une liste de contrôle d'accès qui autorise le trafic HTTP et HTTPS des clients sans fil vers le serveur d'authentification Web externe, de sorte que vous n'avez pas à configurer une liste de contrôle d'accès de pré-auth supplémentaire. Si vous souhaitez autoriser plusieurs adresses IP ou URL, la seule option est de configurer un filtre d'URL de sorte que toutes les adresses IP correspondant à des URL données soient autorisées avant que l'authentification ait lieu. Il n'est pas possible d'ajouter de manière statique plusieurs adresses IP de portail, sauf si vous utilisez des filtres d'URL.

 Remarque : la carte de paramètre globale est la seule où vous pouvez définir les adresses IPv4 et IPv6 virtuelles, les HTTP d'interception Webauth, le portail de contournement captif, l'activation de la liste de contrôle et les paramètres de délai d'expiration de la liste de contrôle.

Résumé de la configuration CLI :

Serveur Web local

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

Serveur Web externe

```
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
```

Configuration des paramètres AAA

Cette section de configuration n'est nécessaire que pour les mappages de paramètres configurés pour le type d'authentification webauth ou webconsentement.

Étape 1. Accédez à Configuration > Security > AAA, puis sélectionnez AAA Method List. Configurez une nouvelle liste de méthodes, sélectionnez + Ajouter et remplissez les détails de la liste ; assurez-vous que Type est défini sur "login" comme indiqué dans l'image.

Configuration > Security > AAA Show Me How >

+ AAA Wizard

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

Authentication

Authorization

Accounting

+ Add × Delete

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

10 items per page 1 - 2 of 2 items

Quick Setup: AAA Authentication ✕

Method List Name*

Type* ⓘ

Group Type ⓘ

Available Server Groups

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

Assigned Server Groups

Cancel Apply to Device

Étape 2. Sélectionnez Autorisation, puis + Ajouter pour créer une nouvelle liste de méthodes. Attribuez-lui le nom par défaut « Type » comme réseau, comme illustré dans l'image.



Remarque : étant donné qu'elle est annoncée par le contrôleur lors de la [configuration de sécurité de couche 3 du WLAN](#) : pour que la liste de méthodes de connexion locale fonctionne, assurez-vous que la configuration « aaa authorization network default local » existe sur le périphérique. Cela signifie que la liste de méthodes d'autorisation avec le nom default doit être définie afin de configurer correctement l'authentification Web locale. Dans cette section, cette liste de méthodes d'autorisation particulière est configurée.

Configuration > Security > AAA Show Me How >

[+ 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](#)

Configuration CLI pour les étapes 1 et 2 :

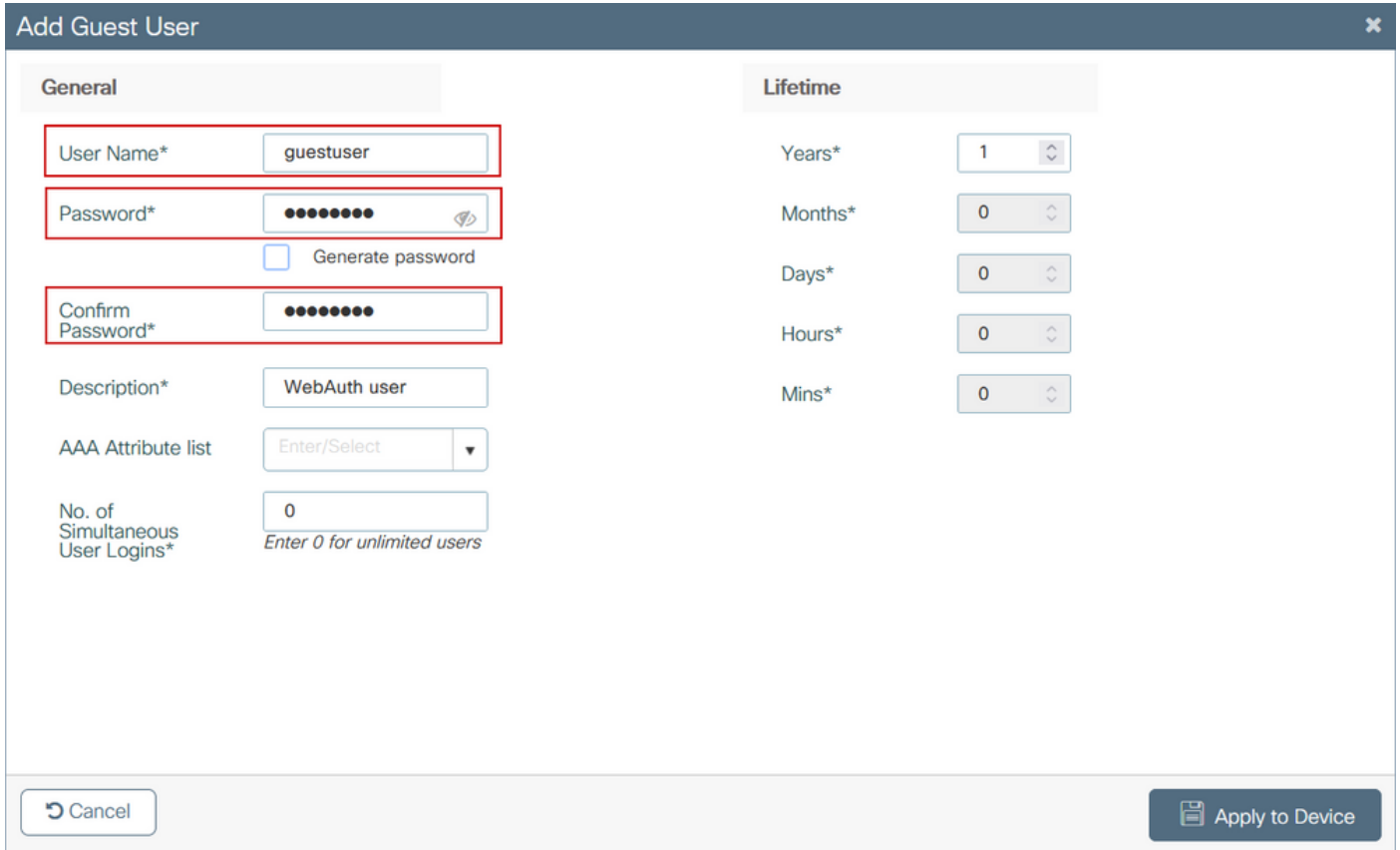
```
<#root>
9800(config)#
aaa new-model

9800(config)#
aaa authentication login local-auth local

9800(config)#
aaa authorization network default local
```

 Remarque : si une authentification RADIUS externe est nécessaire, lisez ces instructions relatives à la configuration du serveur RADIUS sur les WLC 9800 : [Configuration AAA sur le WLC 9800](#). Assurez-vous que le type « login » est défini dans la liste des méthodes d'authentification au lieu de dot1x.

Étape 3. Accédez à Configuration > Security > Guest User. Sélectionnez + Ajouter et configurer les détails du compte d'utilisateur invité.



Add Guest User

General

User Name*

Password* Generate password

Confirm Password*

Description*

AAA Attribute list

No. of Simultaneous User Logins*
Enter 0 for unlimited users

Lifetime

Years*

Months*

Days*

Hours*

Mins*

Configuration CLI :

```
<#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>
```

Étape 4. (Facultatif) Lors de la définition d'une carte de paramètres, deux listes de contrôle d'accès (ACL) sont automatiquement créées. Ces listes de contrôle d'accès sont utilisées pour définir le trafic qui déclenche une redirection vers le serveur Web et le trafic autorisé à transiter. Si des exigences spécifiques, telles que plusieurs adresses IP de serveur Web ou des filtres d'URL, existent, alors naviguez vers Configuration > Security > ACL select + Add et définissez les règles nécessaires ; les instructions permit sont redirigées tandis que les instructions deny définissent les passages de trafic.

Les règles des listes de contrôle d'accès créées automatiquement sont :

```
<#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
```

Configurer les stratégies et les balises

Étape 1. Accédez à Configuration > Tags & Profiles > WLANs, sélectionnez + Add pour créer un nouveau WLAN. Définissez le profil et le nom SSID, ainsi que l'état dans l'onglet General.

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

Étape 2. Sélectionnez l'onglet Security et définissez l'authentification de couche 2 sur None si vous n'avez pas besoin d'un mécanisme de cryptage par liaison radio. Dans l'onglet Layer 3, cochez la case Web Policy, sélectionnez la carte de paramètre dans le menu déroulant et choisissez la liste d'authentification dans le menu déroulant. Si une liste de contrôle d'accès personnalisée a été définie précédemment, sélectionnez Show Advanced Settings et sélectionnez la liste de contrôle d'accès appropriée dans le menu déroulant.

⚠ 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

Cancel

Activate Windows

Go to System in Control Panel to activate Windows



Update & Apply to Device

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

[Show Advanced Settings >>>](#)

Web Policy

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

[Interactive Help](#)

↶ Cancel Activate Windows Update & Apply to Device

Configurations CLI :

```
<#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
```

Étape 3. Accédez à Configuration > Tags & Profiles > Policy et sélectionnez + Add. Définissez le nom et l'état de la stratégie ; assurez-vous que les paramètres Central sous Stratégie de commutation WLAN sont activés pour les points d'accès en mode local. Dans l'onglet Access Policies, sélectionnez le VLAN correct dans le menu déroulant VLAN/VLAN Group, comme illustré dans l'image.

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

Configuration CLI :

```

<#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

```

Étape 4. Accédez à Configuration > Tags & Profiles > Tags, dans l'onglet Policy, sélectionnez + Add. Définissez un nom de balise, puis sous WLAN-POLICY Maps, sélectionnez + Add et ajoutez le WLAN et le profil de stratégie précédemment créés.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

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

Map WLAN and Policy

WLAN Profile*	<input type="text" value="EWA-Guest"/>	Policy Profile*	<input type="text" value="Guest-Policy"/>
---------------	--	-----------------	---

➤ RLAN-POLICY Maps: 0

Configuration CLI :

```
<#root>
```

```
9800(config)#
```

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

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

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

Étape 5. Accédez à Configuration > Wireless > Access Points et sélectionnez l'AP qui est utilisé pour diffuser ce SSID. Dans le menu Edit AP, sélectionnez la balise nouvellement créée dans le menu déroulant Policy.

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
...	default-site-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

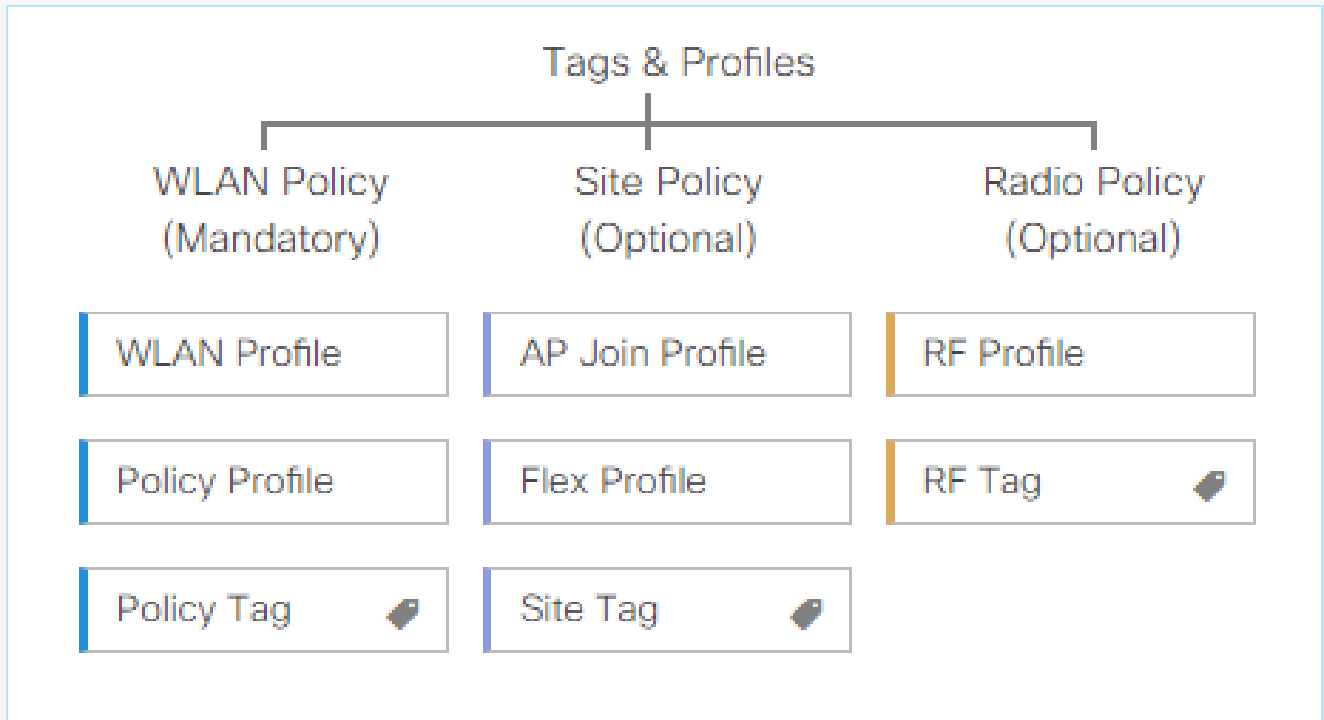
Si plusieurs points d'accès doivent être balisés en même temps, deux options sont disponibles :

Option A. Accédez à Configuration > Wireless Setup > Advanced, puis sélectionnez Start Now pour afficher la liste du menu de configuration. Sélectionnez l'icône de liste en regard de Tag APs, cela affiche la liste de tous les AP dans l'état Join, vérifiez les AP nécessaires, puis sélectionnez + Tag APs, sélectionnez la balise de stratégie créée dans le menu déroulant.

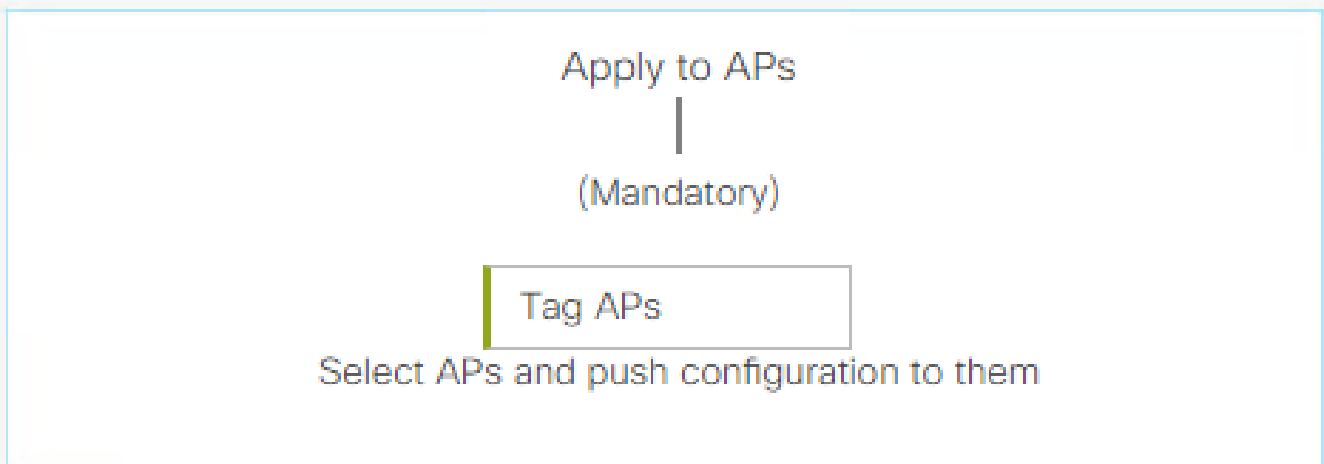
Wireless Setup Flow Overview

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

. Définissez le nom de la règle, l'expression régulière du nom de l'AP (ce paramètre permet au contrôleur de définir quels AP sont balisés), la priorité (les numéros inférieurs ont une priorité plus élevée) et les balises nécessaires.

Associate Tags to AP ✕

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

↶ Cancel 📄 Apply to Device

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement:

```
<#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>
```

Vérifiez l'état et la disponibilité du serveur http avec show ip http server status :

```
<#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
```

Vérifiez l'accès à la session client avec ces commandes :

<#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
```

Dépannage

Suivi permanent

Le WLC 9800 offre des fonctionnalités de suivi ALWAYS-ON. Cela garantit que tous les messages d'erreur, d'avertissement et de niveau de notification liés à la connectivité du client sont constamment consignés et que vous pouvez afficher les journaux d'un incident ou d'une défaillance après qu'il se soit produit.

 Remarque : en fonction du volume de journaux générés, vous pouvez revenir de quelques heures à plusieurs jours.

Afin d'afficher les traces que le WLC 9800 a collectées par défaut, vous pouvez vous connecter via SSH/Telnet au WLC 9800 et lire ces étapes (assurez-vous que vous consignez la session dans un fichier texte).

Étape 1. Vérifiez l'heure actuelle du contrôleur de sorte que vous puissiez suivre les journaux dans l'heure jusqu'à quand le problème s'est produit.

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

Étape 2. Collectez les syslogs à partir de la mémoire tampon du contrôleur ou du syslog externe, comme dicté par la configuration système. Cela permet d'obtenir un aperçu rapide de l'état du système et des erreurs éventuelles.

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

Étape 3. Vérifiez si les conditions de débogage sont activées.

```
<#root>
```

```
9800#
```

```
show debugging
```


```
IOSXE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

```
IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address _____ Port  
-----|-----
```

 Remarque : si une condition est répertoriée, cela signifie que les traces sont consignées au niveau de débogage pour tous les processus qui rencontrent les conditions activées (adresse MAC, adresse IP, etc.). Cela augmenterait le volume de journaux. Par conséquent, il est recommandé d'effacer toutes les conditions lorsque vous ne procédez pas activement au débogage.

Étape 4. En supposant que l'adresse MAC testée n'était pas répertoriée comme condition à l'étape 3. Collectez les traces de niveau de notification toujours actives pour l'adresse MAC spécifique.

```
<#root>
```

```
9800#
```

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

Vous pouvez soit afficher le contenu de la session, soit copier le fichier sur un serveur TFTP externe.

```
<#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>
```

Débogage conditionnel et traçage Radio Active

Si les traces toujours actives ne vous donnent pas assez d'informations pour déterminer le déclencheur du problème en cours d'investigation, vous pouvez activer le débogage conditionnel et capturer la trace Radio Active (RA), qui fournit des traces de niveau de débogage pour tous les processus qui interagissent avec la condition spécifiée (adresse MAC du client dans ce cas). Afin

d'activer le débogage conditionnel, lisez ces étapes.


Étape 1. Assurez-vous qu'aucune condition de débogage n'est activée.


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

Étape 2. Activez la condition de débogage pour l'adresse MAC du client sans fil que vous souhaitez surveiller.

Ces commandes commencent à surveiller l'adresse MAC fournie pendant 30 minutes (1 800 secondes). Vous pouvez aussi augmenter ce délai pour qu'il atteigne jusqu'à 2085978494 secondes.

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

 Remarque : pour surveiller plusieurs clients à la fois, exécutez la commande debug wireless mac par adresse mac.

 Remarque : l'activité du client sans fil n'est pas affichée sur la session du terminal car tous les journaux sont mis en mémoire tampon en interne afin d'être affichés ultérieurement.

Étape 3. Reproduisez le problème ou le comportement que vous souhaitez surveiller.

Étape 4. Arrêtez le débogage si le problème est reproduit avant la fin du temps de surveillance par défaut ou configuré.

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

Une fois que le temps de surveillance s'est écoulé ou que le débogage sans fil a été arrêté, le contrôleur WLC 9800 génère un fichier local du nom de :

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Étape 5. Recueillir le fichier de l'activité de l'adresse MAC. Il est possible de copier le fichier de suivi RA .log sur un serveur externe ou d'afficher le résultat directement à l'écran.

Vérifiez le nom du fichier de suivi RA.

```
<#root>
```

```
9800#
```

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

Copiez le fichier sur un serveur externe :

```
<#root>
```

```
9800#
```

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

Affichez-en le contenu :

```
<#root>
```

```
9800#
```


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

Étape 6. Si vous ne trouvez toujours pas la cause première, collectez les journaux internes, qui peuvent vous offrir une vue plus détaillée des journaux de niveau de débogage. Vous n'avez pas besoin de déboguer à nouveau le client car la commande fournit des journaux de débogage qui ont déjà été collectés et stockés en interne.

```
<#root>
```

```
9800#
```

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

 Remarque : cette sortie de commande retourne des traces pour tous les niveaux de journalisation pour tous les processus et est assez volumineuse. Veuillez contacter le TAC Cisco afin de vous aider à analyser ces traces.

```
<#root>
```



```
9800#
```

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

Affichez-en le contenu :

```
<#root>
```

```
9800#
```

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

Étape 7. Supprimez les conditions de débogage.



Remarque : assurez-vous de toujours supprimer les conditions de débogage après une session de dépannage.

Captures de paquets intégrées

Les contrôleurs 9800 peuvent détecter les paquets en mode natif, ce qui facilite le dépannage grâce à la visibilité du traitement des paquets du plan de contrôle.

Étape 1. Définissez une liste de contrôle d'accès pour filtrer le trafic concerné. Pour l'authentification Web, il est recommandé d'autoriser le trafic en provenance et à destination du serveur Web, ainsi que le trafic en provenance et à destination de quelques points d'accès où les clients sont connectés.

```
<#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
```

Étape 2. Définissez les paramètres de capture du moniteur. Assurez-vous que le trafic du plan de contrôle est activé dans les deux directions, l'interface fait référence à la liaison ascendante physique de votre contrôleur.

```
<#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)
```

Étape 3. Démarrez la capture du moniteur et reproduisez le problème.

```
<#root>
```

9800#

```
monitor capture EWA start
```

Started capture point : EWA

Étape 4. Arrêtez la capture du moniteur et exportez-la.

<#root>

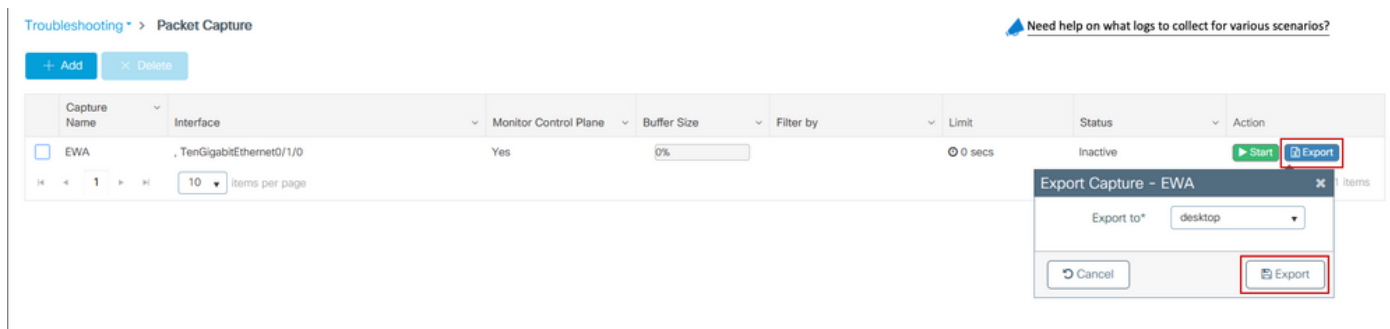
9800#

```
monitor capture EWA stop
```

Stopped capture point : EWA

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

Vous pouvez également télécharger la capture à partir de l'interface graphique utilisateur, naviguer vers Troubleshooting > Packet Capture et sélectionner Export sur la capture configurée. Sélectionnez Desktop (Bureau) dans le menu déroulant pour télécharger la capture via HTTP dans le dossier souhaité.



Dépannage côté client

Les WLAN d'authentification Web dépendent du comportement du client. Sur cette base, la connaissance et l'information du comportement côté client sont essentielles pour identifier la cause première des erreurs d'authentification Web.

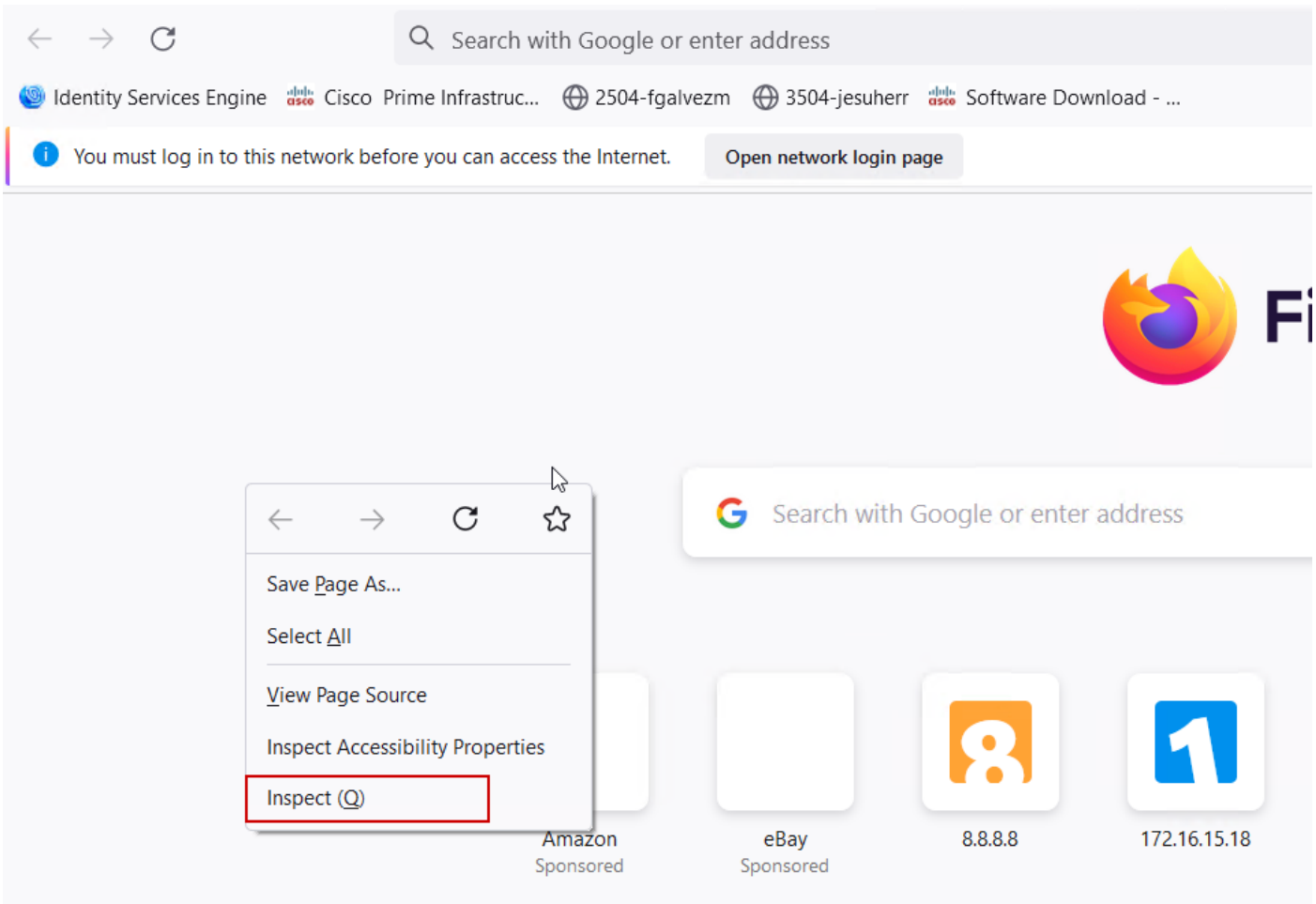
Dépannage du navigateur HAR

De nombreux navigateurs modernes, tels que Mozilla Firefox et Google Chrome, fournissent des outils de développement de console pour déboguer les interactions d'applications Web. Les fichiers HAR sont des enregistrements des interactions client-serveur et fournissent une chronologie des interactions HTTP ainsi que des informations sur les requêtes et les réponses (en-têtes, code d'état, paramètres, etc.).

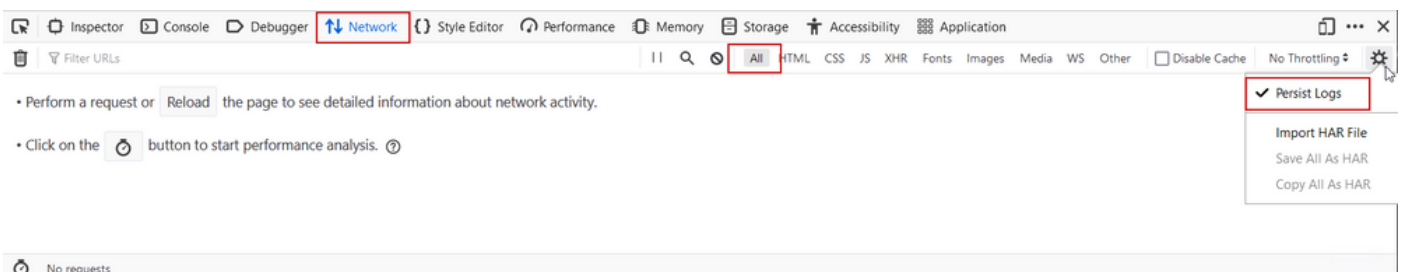
Les fichiers HAR peuvent être exportés à partir du navigateur client et importés dans un autre

navigateur pour une analyse plus approfondie. Ce document décrit comment collecter le fichier HAR de Mozilla Firefox.

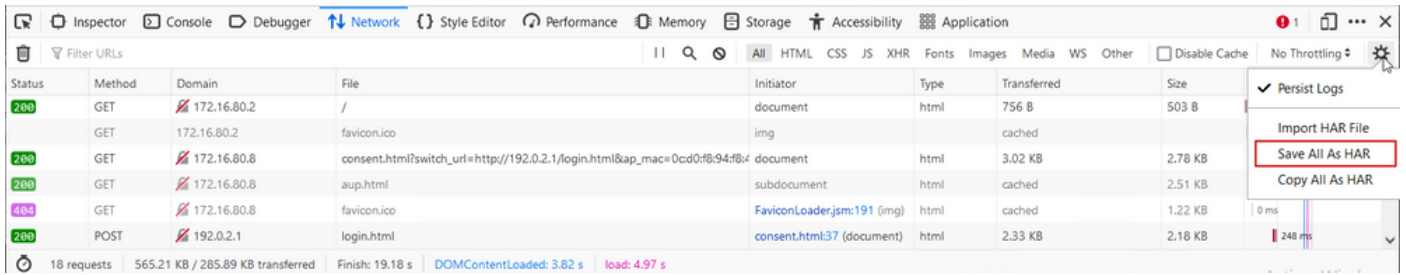
Étape 1. Ouvrez Web Developer Tools avec Ctrl + Maj + I, ou cliquez avec le bouton droit dans le contenu du navigateur et sélectionnez Inspect.



Étape 2. Accédez à Réseau, assurez-vous que « Tout » est sélectionné pour capturer tous les types de demande. Sélectionnez l'icône de l'engrenage et assurez-vous que Persist Logs a une flèche à côté d'elle, sinon les demandes de journaux sont effacées chaque fois qu'un changement de domaine est déclenché.



Étape 3. Reproduisez le problème, assurez-vous que le navigateur consigne toutes les requêtes. Une fois, le problème est reproduit arrêter la journalisation du réseau, puis sélectionnez sur l'icône d'engrenage et sélectionnez Enregistrer tout comme HAR.



Capture de paquets côté client

Les clients sans fil équipés d'un système d'exploitation tel que Windows ou MacOS peuvent détecter des paquets sur leur carte sans fil. Bien qu'ils ne remplacent pas directement les captures de paquets en direct, ils peuvent fournir un aperçu du flux global d'authentification Web.

Requête DNS :

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 34.187.221.8
11870	2021-09-28 06:44:07.410773	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

Connexion TCP initiale et HTTP GET pour la redirection :

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

Connexion TCP avec le serveur externe :

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 vers le serveur externe (requête de portail captif) :

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=0c:d0:f8:97:ae:60&client_mac=34:23:87:4c:6b:f7&ssid=Edu-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 06:44:08.706215	172.16.21.153	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 vers IP virtuelle pour authentification :

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 06:44:50.749940	172.16.21.153	192.0.2.1	TCP	54	52359 → 80 [ACK] Seq=556 Ack=2412 Win=130560 Len=0

Exemple d'une tentative réussie

Il s'agit du résultat d'une tentative de connexion réussie du point de vue de la trace radio active.

Utilisez-le comme référence pour identifier les étapes de session client pour les clients qui se connectent à un SSID d'authentification Web de couche 3.

authentification et association 802.11 :

<#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.

Authentification de couche 2 ignorée :

<#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

Plumb ACL :

<#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

Processus d'apprentissage IP :

<#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

Processus d'authentification et de redirection de couche 3 :

<#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

Transition vers l'état EXÉCUTÉ :

<#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

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.