

Configurer l'authentification Web locale avec l'authentification externe

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Authentification Web](#)

[Types d'authentification](#)

[Base de données pour authentification](#)

[Authentification Web locale](#)

[Authentification Web locale avec authentification externe](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurer l'authentification Web locale avec l'authentification externe sur l'interface CLI](#)

[Configurer le serveur AAA et le groupe de serveurs](#)

[Configurer l'authentification et l'autorisation locales](#)

[Configurer les mappages de paramètres](#)

[Configuration des paramètres de sécurité WLAN](#)

[Créer un profil de stratégie sans fil](#)

[Créer une balise de stratégie](#)

[Attribuer une balise de stratégie à un point d'accès](#)

[Configurer l'authentification Web locale avec l'authentification externe sur l'interface utilisateur Web](#)

[Configuration AAA sur un contrôleur WLC 9800](#)

[Configuration de WebAuth](#)

[Configuration d'un réseau local sans fil \(WLAN\)](#)

[Configuration du profil des politiques](#)

[Configuration des balises des politiques](#)

[Affectation des balises des politiques](#)

[Configuration ISE](#)

[Connecter le client invité](#)

[Vérifier](#)

[Show WLAN Summary](#)

[Afficher la configuration de mappage de paramètres](#)

[Afficher les informations AAA](#)

[Dépannage](#)

[Problèmes courants](#)

[Débogage conditionnel et suivi actif radio et capture de paquets intégrée](#)

Introduction

Ce document décrit comment configurer l'authentification Web locale avec l'authentification externe sur un WLC 9800 et ISE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration des contrôleurs LAN sans fil (WLC) du 9800
- Points d'accès légers (LAP)
- Comment configurer et configurer un serveur Web externe Identity Services Engine (ISE).
- Comment configurer et configurer les serveurs DHCP et DNS.

Composants utilisés

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

- 9800-40 WLC Cisco IOS® XE, version 17.18.4a avec APSP1 et APSP2
- Identity Services Engine (ISE), version 3.2.0.542
- Point d'accès Wi-Fi 7 sans fil Cisco® 9172I, version 17.18.4.202

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.

Authentification Web

L'authentification Web est une fonctionnalité de sécurité de couche 3 qui permet aux utilisateurs invités d'accéder au réseau.

Cette fonctionnalité est conçue pour fournir un accès invité facile et sécurisé aux SSID ouverts, sans avoir besoin de configurer un profil utilisateur, et elle peut également fonctionner avec des méthodes de sécurité de couche 2.

L'objectif de l'authentification Web est de permettre à des périphériques non approuvés (invités) d'accéder au réseau avec des privilèges d'accès au réseau limités, via un WLAN invité qui peut être configuré avec des mécanismes de sécurité, et la sécurité du réseau n'est pas compromise. Pour que les utilisateurs invités aient accès au réseau, ils doivent s'authentifier correctement, c'est-à-dire fournir les informations d'identification correctes ou accepter la stratégie d'utilisation acceptable (AUP) pour accéder au réseau.

L'authentification Web est un avantage pour les entreprises, car elle favorise la fidélité des utilisateurs, rend l'entreprise conforme à l'utilisation d'une clause de non-responsabilité que l'utilisateur invité doit accepter et permet à l'entreprise de communiquer avec les visiteurs.

Pour déployer l'authentification Web, il faut tenir compte de la manière dont le portail invité et l'authentification sont gérés. Il existe deux méthodes courantes :

- Authentification Web locale (LWA) : Méthode de redirection d'utilisateurs invités vers un portail directement à partir du WLC. La redirection et la liste de contrôle d'accès pré-WebAuth sont configurées localement sur le WLC.
- Authentification Web centralisée (CWA) : L'invention concerne un procédé de redirection d'utilisateurs invités dans lequel l'URL de redirection et la liste de contrôle d'accès de redirection sont configurées de manière centralisée sur un serveur externe (par exemple ISE) et communiquées au WLC via RADIUS. Dans l'authentification Web centrale, l'URL de redirection et la liste de contrôle d'accès de redirection sont situées de manière centrale sur un serveur externe (tel que RADIUS). Le serveur RADIUS est celui qui gère l'authentification, il envoie des instructions au WLC. Dans CWA, le WLC ne nécessite pas de certificat d'authentification Web local, un seul certificat est nécessaire sur le portail Web central et nécessite un serveur d'authentification central, tel qu'ISE. Pour lire CWA plus en détail, accédez à [Configurer l'authentification Web centrale \(CWA\) sur Catalyst 9800 WLC et ISE](#).

Dans l'authentification Web locale, le portail Web peut être présent sur le WLC ou sur un serveur externe. Dans LWA avec authentification externe, le portail Web est présent sur le WLC. Dans LWA avec un serveur Web externe, le portail Web est présent sur un serveur externe (tel que Cisco DNA Spaces). Un exemple de LWA avec un serveur Web externe est décrit en détail à l'adresse : [Configurez le portail captif DNA Spaces avec le WLC Catalyst 9800](#).

Schéma des différentes méthodes d'authentification Web :

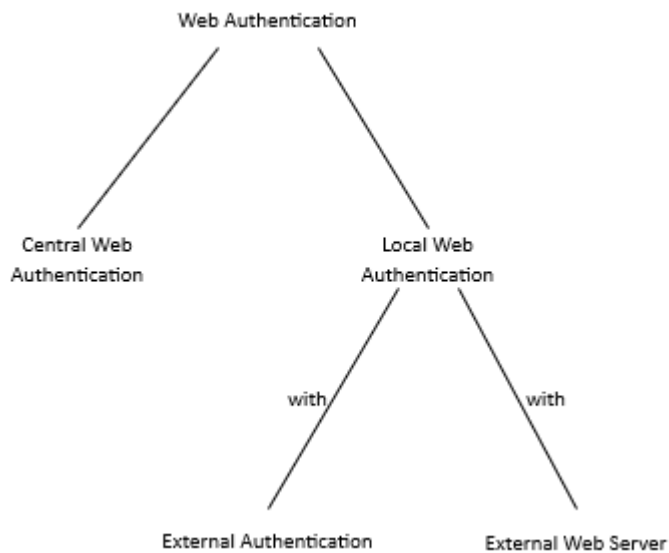


Schéma des différentes méthodes d'authentification Web



Remarque : Si vous déployez des points d'accès Wi-Fi 7 avec authentification Web sur un WLC 9800, assurez-vous que vous exécutez une version recommandée de Cisco IOS XE telle que 17.18.4a ou ultérieure.

Types d'authentification

Il existe quatre types d'authentification pour authentifier l'utilisateur invité :

- Webauth : Saisissez le nom d'utilisateur et le mot de passe.
- Consentement (Web-passthrough) : Acceptez AUP.
- Ignorer : Authentification basée sur l'adresse MAC du périphérique utilisateur invité.
- Web consent : Un mélange entre le nom d'utilisateur/mot de passe et accepter AUP.

webauth	authbypass	consent	webconsent
Username: Password: OK	Client connects to the SSID and gets an IP address, then the 9800 WLC checks if the MAC address is allowed to enter the network, if yes, it is moved to RUN state, if it is not it is not allowed to join. (It won't fall back to web authentication)	banner1 ☒ Accept ☐ Don't Accept OK	banner login ☒ Accept ☐ Don't Accept Username: Password: OK

Quatre types d'authentification pour authentifier l'utilisateur invité

Base de données pour authentification

Les informations d'identification pour l'authentification peuvent être stockées sur un serveur LDAP, localement sur le WLC ou sur le serveur RADIUS.

- Base de données locale : Les informations d'identification (nom d'utilisateur et mot de passe) sont stockées localement sur le WLC.
- Base de données LDAP : Les informations d'identification sont stockées dans la base de données principale LDAP. Le WLC interroge le serveur LDAP pour les informations d'identification d'un utilisateur particulier dans la base de données.
- Base de données RADIUS : Les informations d'identification sont stockées dans la base de données principale RADIUS. Le WLC interroge le serveur RADIUS pour les informations d'identification d'un utilisateur particulier dans la base de données.

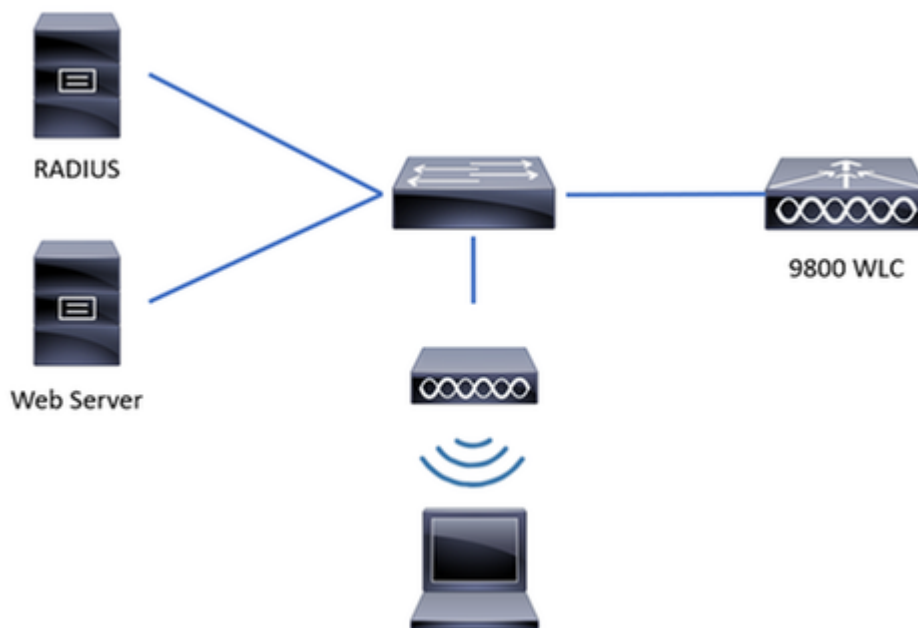
Authentification Web locale

Dans l'authentification Web locale, l'utilisateur invité est redirigé vers un portail Web directement à partir du WLC.

Le portail Web peut se trouver dans le WLC ou dans un autre serveur. Ce qui rend local est le fait que l'URL de redirection et l'ACL qui correspond au trafic doivent être sur le WLC (et non l'emplacement du portail Web). Dans LWA, lorsqu'un utilisateur invité se connecte au WLAN invité, le WLC intercepte la connexion de l'utilisateur invité et les redirige vers l'URL du portail

Web, où l'utilisateur invité est invité à s'authentifier. Lorsque l'utilisateur invité entre des informations d'identification (nom d'utilisateur et mot de passe), le WLC capture les informations d'identification. Le WLC authentifie l'utilisateur invité avec un serveur LDAP, un serveur RADIUS ou une base de données locale (base de données présente localement sur le WLC). Dans le cas d'un serveur RADIUS (un serveur externe tel qu'ISE), il peut être utilisé non seulement pour stocker des informations d'identification, mais également pour fournir des options d'enregistrement de périphérique et d'auto-provisionnement. Dans le cas d'un serveur Web externe, tel que Cisco DNA Spaces, le portail Web est présent. Dans LWA, il y a un certificat sur le WLC et un autre sur le portail web.

L'image représente la topologie générique de LWA :



Topologie générique de LWA

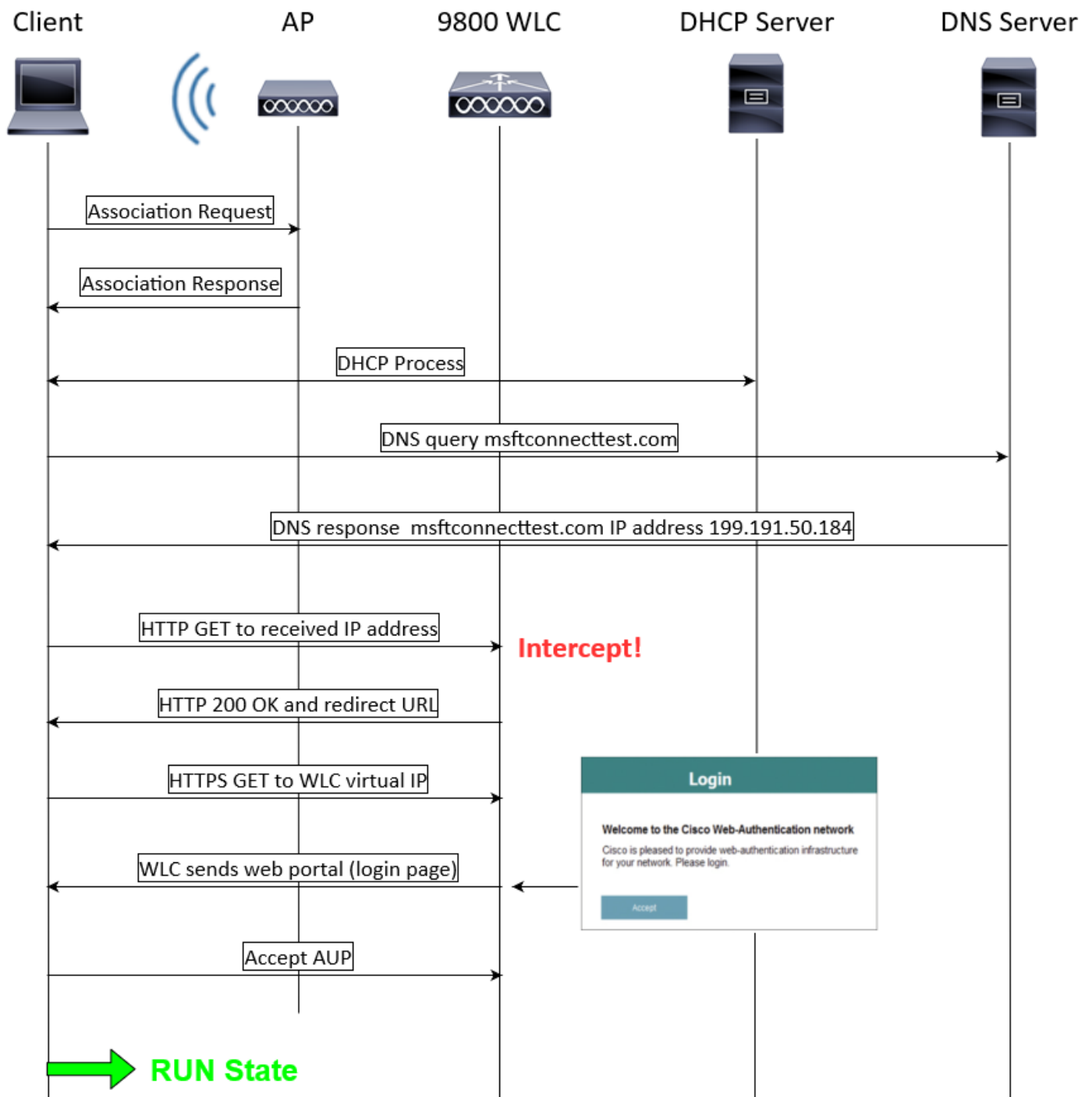
Périphériques de la topologie réseau de LWA :

- Client : Envoie des requêtes au serveur DHCP et DNS, demande l'accès au WLAN invité et répond aux requêtes du WLC.
- Point d'accès : Connecté à un commutateur, diffuse le WLAN invité et fournit une connexion sans fil aux périphériques des utilisateurs invités. Il autorise également les paquets DHCP et DNS avant l'authentification de l'utilisateur invité (avant d'entrer des informations d'identification valides).
- WLC : Gère les points d'accès et les clients. Le WLC héberge l'URL de redirection et la liste de contrôle d'accès qui correspond au trafic. Intercepte les requêtes HTTP des utilisateurs invités, les redirige vers un portail Web (page de connexion) où les utilisateurs invités doivent s'authentifier. Il capture les informations d'identification et authentifie les utilisateurs invités, et envoie des demandes d'accès à un serveur externe, un serveur LDAP ou une base de données locale pour confirmer la validité des informations d'identification.

- Serveur d'authentification : Répond aux demandes d'accès du WLC avec l'acceptation/le rejet d'accès. Le serveur d'authentification valide les informations d'identification de l'utilisateur invité et avertit le WLC si les informations d'identification sont valides ou non valides. Si les informations d'identification sont valides, l'utilisateur invité est autorisé à accéder au réseau (le serveur d'authentification fournit des options pour l'enregistrement des périphériques et l'auto-provisionnement). Si les informations d'identification ne sont pas valides, l'accès au réseau est refusé à l'utilisateur invité.

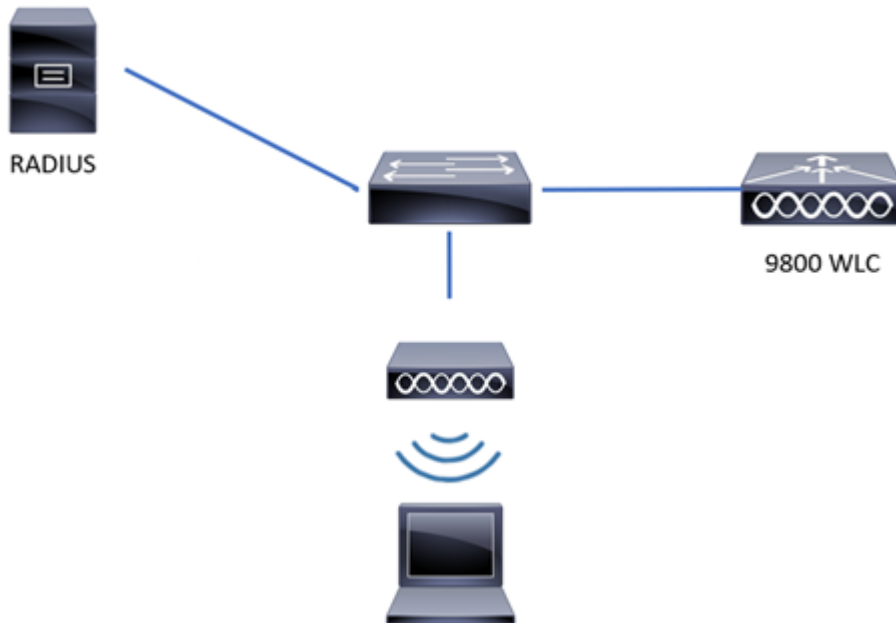
Flux LWA :

- L'utilisateur invité s'associe à un point d'accès qui diffuse le WLAN invité.
- L'utilisateur invité passe par le processus DHCP afin d'obtenir une adresse IP.
- L'utilisateur invité souhaite effectuer une vérification de la connectivité Internet au portail captif. S'il s'agit d'un appareil Apple, il tente le portail captif Apple ; s'il s'agit d'un appareil Android, il tente le portail captif Android ; s'il s'agit d'un périphérique Windows, il tente le portail de test de connexion Windows.
- L'utilisateur invité envoie une requête DNS pour demander l'adresse IP du portail captif. Le serveur DNS répond à la requête avec l'adresse IP correspondante.
- L'utilisateur invité envoie un message HTTP GET à l'adresse IP du portail captif.
- Le WLC intercepte ce message et répond à l'utilisateur invité avec HTTP 200 OK et l'URL de redirection.
- L'utilisateur invité envoie un message GET HTTPS à l'IP virtuelle du WLC et le WLC répond avec le portail Web.
- L'utilisateur invité est invité à saisir les informations d'authentification sur le portail Web.
- Le portail Web redirige l'utilisateur vers le WLC avec les informations d'identification fournies (si un portail Web externe est utilisé).
- Le WLC authentifie l'utilisateur invité via une base de données locale, ou il envoie une requête au serveur RADIUS ou LDAP, pour confirmer si les informations d'identification sont correctes (si le type d'authentification est webconsentement ou webauth).
- Si les informations d'identification sont correctes, le WLC authentifie l'utilisateur invité et passe à l'état d'exécution. Si les informations d'identification sont incorrectes, le WLC supprime l'utilisateur invité.
- Le WLC redirige le client vers l'URL d'origine qui a été entrée dans le navigateur Web.



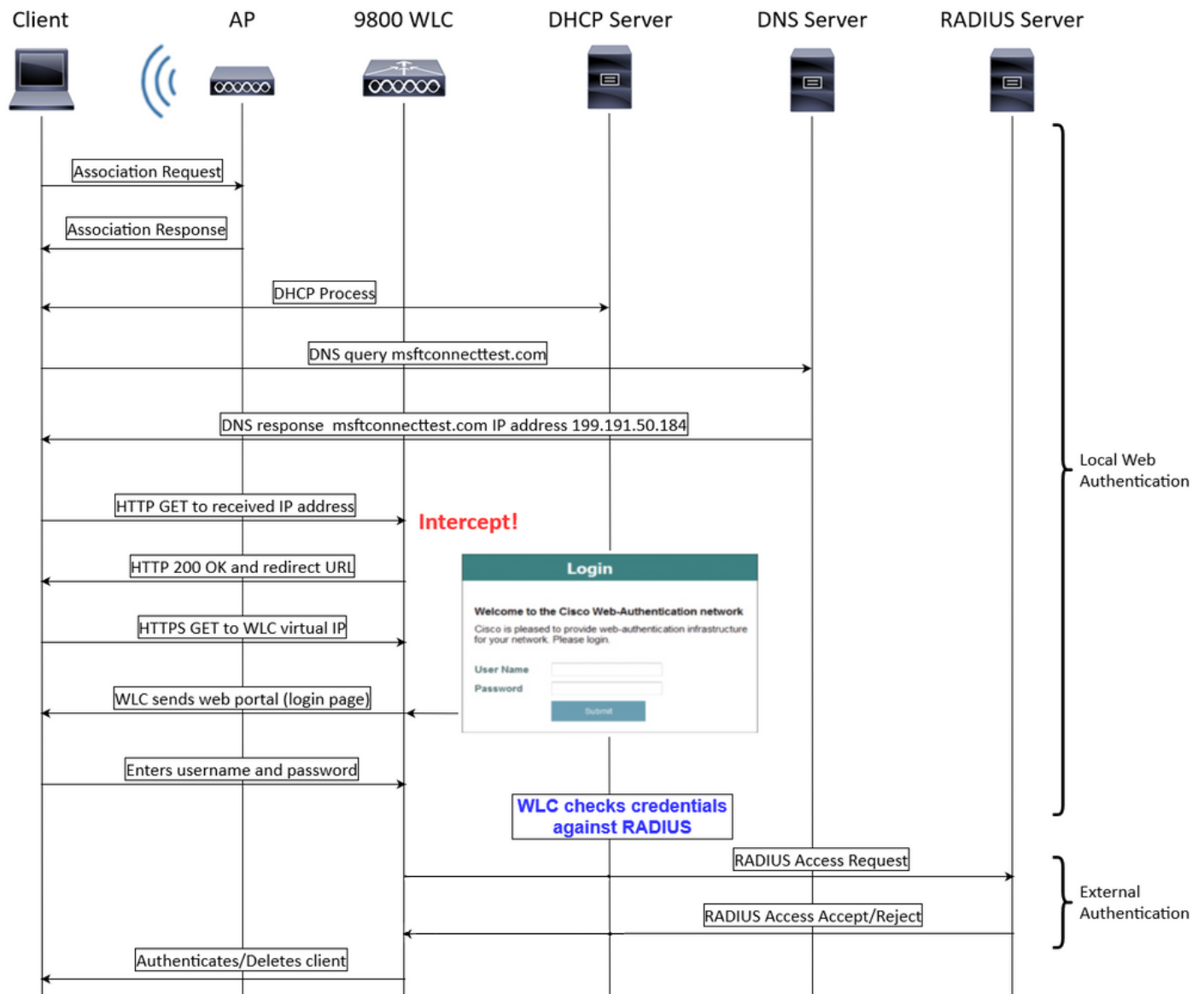
Flux LWA

Authentification Web locale avec authentification externe



Topologie générique de LWA-EA

LWA-EA est une méthode de LWA où le portail Web et l'URL de redirection sont situés sur le WLC et les informations d'identification sont stockées sur un serveur externe, tel qu'ISE. Le WLC capture les informations d'identification et authentifie le client via un serveur RADIUS externe. Lorsque l'utilisateur invité entre des informations d'identification, le WLC vérifie les informations d'identification par rapport à RADIUS, il envoie une demande d'accès RADIUS et reçoit un message d'acceptation/de refus d'accès RADIUS du serveur RADIUS. Ensuite, si les informations d'identification sont correctes, l'utilisateur invité passe à l'état EXÉCUTÉ. Si les informations d'identification sont incorrectes, l'utilisateur invité est supprimé par le WLC.



Flux LWA-EA

Configurer

Diagramme du réseau

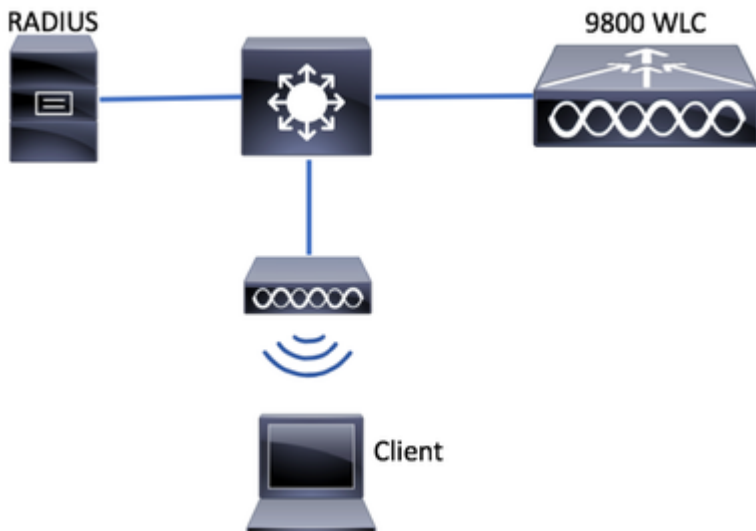


Diagramme du réseau



Remarque : Cet exemple de configuration ne couvre que la commutation/l'authentification centrale. La configuration de la commutation locale flexible présente des exigences légèrement différentes pour la configuration de l'authentification Web.

Configurer l'authentification Web locale avec l'authentification externe sur l'interface CLI

Configurer le serveur AAA et le groupe de serveurs

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4 <ip address> auth-port 1812 acct-port 1813
9800WLC(config-radius-server)#key cisco
9800WLC(config-radius-server)#exit
9800WLC(config)#aaa group server radius RADIUSGROUP
9800WLC(config-sg-radius)#server name RADIUS
9800WLC(config-sg-radius)#end
```

Configurer l'authentification et l'autorisation locales

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
```

```
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

Configure Parameter Maps

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)# parameter-map type webauth global
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint <trustpoint name>
9800WLC(config-params-parameter-map)#end
```

Configuration des paramètres de sécurité WLAN

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Créer un profil de stratégie sans fil

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan <vlan name>
9800WLC(config-wireless-policy)#no shutdown
9800WLC(config-wireless-policy)#end
```

Créer une balise de stratégie

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless tag policy POLICY_TAG
```

```
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

Attribuer une balise de stratégie à un point d'accès

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap <MAC address>
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
9800WLC(config-ap-tag)#end
```

Pour terminer la configuration côté ISE, accédez à la section Configuration ISE.

Configurer l'authentification Web locale avec l'authentification externe sur l'interface utilisateur Web

Configuration AAA sur un contrôleur WLC 9800

Étape 1 : ajout du serveur ISE à la configuration du WLC 9800

Accédez à Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add et entrez les informations du serveur RADIUS comme indiqué dans l'image :

Create AAA Radius Server

General

RadSec

Show Me How >

Name*	RADIUS	Support for CoA ⓘ	ENABLED ☒
Server Address*	192.0.2.30	CoA Server Key Type	Clear Text ▼
PAC Key	☐	CoA Server Key ⓘ	
Key Type	Clear Text ▼	Confirm CoA Server Key	
Key* ⓘ		VRF	
Confirm Key*		Automate Tester	☐
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

Cancel

Apply to Device

Configuration AAA sur un contrôleur WLC 9800

Étape 2 : ajout du groupe de serveurs RADIUS

Accédez à Configuration > Security > AAA > Servers/Groups > RADIUS > Servers Group > + Add et entrez les informations du groupe de serveurs RADIUS :

Create AAA Radius Server Group

Name*

RADIUSGROUP

Group Type

RADIUS

Show Me How >

MAC-Delimiter

none

MAC-Filtering

none

Dead-Time (mins)

5

Load Balance

☐ DISABLED

IPv4 Source Interface

Search or Select

i

IPv4 VRF

Search or Select

IPv6 Source Interface

Search or Select

i

IPv6 VRF

Search or Select

Available Servers

Assigned Servers

>

<

>>

<<

RADIUS

Cancel

Apply to Device

Ajouter le groupe de serveurs RADIUS

Étape 3 : création d'une liste de méthodes d'authentification

Accédez à Configuration > Security > AAA > AAA Method List > Authentication > + Add:

Quick Setup: AAA Authentication

Method List Name*

LWA_AUTHENTICATION

Type*

login

Group Type

group

Fallback to local

☐

Available Server Groups

radius
ldap
tacacs+

Assigned Server Groups

RADIUSGROUP

Cancel

Apply to Device

Créer une liste de méthodes d'authentification

Étape 4. Créez une liste de méthodes d'autorisation.

Accédez à Configuration > Security > AAA > AAA Method List > Authorization > + Add:

Quick Setup: AAA Authorization

Method List Name*

LWA_AUTHORIZATION

Type*

network

Group Type

group

Fallback to local

☐

Authenticated

☐

Available Server Groups

radius
ldap
tacacs+

Assigned Server Groups

RADIUSGROUP

Cancel

Apply to Device

Créez une liste de méthodes d'autorisation

Configuration de WebAuth

Créez ou modifiez une correspondance de paramètres. Sélectionnez le type webauth, l'adresse IPv4 virtuelle doit être une adresse non utilisée sur le réseau pour éviter les conflits d'adresses IP, et ajoutez un point de confiance.

Accédez à Configuration > Security > Web Auth > + Add ou sélectionnez une carte de paramètre :

Configuration > Security > Web Auth

+ Add - Delete

Parameter Map Name

global

1 10

Edit Web Auth Parameter

General Advanced

Parameter-map Name: global

Banner Title:

Banner Type: ☒ None ☐ Banner Text ☐ File Name

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth

Captive Bypass Portal: ☐

Disable Success Window: ☐

Disable Logout Window: ☐

Disable Cisco Logo: ☐

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-94747...

Virtual IPv4 Hostname:

Virtual IPv6 Address: :::::XX

Web Auth intercept HTTPs: ☐

Enable HTTP server for Web Auth: ☐

Disable HTTP secure server for Web Auth: ☐

Cancel Update & Apply

Configuration de WebAuth

Configuration d'un réseau local sans fil (WLAN)

Étape 1 : création du WLAN

Allez à Configuration > Tags & Profiles > WLANs > +Add (configuration > balises et profils > WLAN > +ajouter) et configurez le réseau selon vos besoins.

Add WLAN

General Security Advanced

Profile Name*: LWA_EA

SSID*: LWA_EA

WLAN ID*: 1

Status: ENABLED

Broadcast SSID: ENABLED

Wi-Fi 6E Compatibility: 1/2 requirements met

Wi-Fi 7 Compatibility: 0/3 requirements met 0/3 bands enabled

Radio Policy ⓘ

Show slot configuration

6 GHz Status: ENABLED ⓘ

5 GHz Status: ENABLED

2.4 GHz Status: ENABLED

802.11b/g Policy: 802.11b/g

Créez le WLAN.

Étape 2. Accédez à Security > Layer2 et, sur Layer 2 Security Mode, sélectionnez None.

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

☐ WPA + WPA2 ☐ WPA2 + WPA3 ☐ WPA3 ☐ Static WEP ☒ None

MAC Filtering ☐

OWE Transition Mode ☐

Lobby Admin Access ☐

Création de la sécurité WLAN

Étape 3. Accédez à Security > Layer3 et sur Web Policy cochez la case, sur Web Auth Parameter Map sélectionnez le nom du paramètre, et sur Authentication List sélectionnez la liste d'authentification créée précédemment.

Add WLAN

General **Security** Advanced

Layer2 **Layer3** AAA

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

Web Auth Parameter Map

Authentication List

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

Cancel

Créer la liste d'authentification WLAN

Le WLAN est affiché dans la liste WLAN :

Configuration > Tags & Profiles > WLANs

+ Add × Delete Clone Enable WLAN Disable WLAN WLAN Wizard

Selected WLANs : 0

☐	Status	Name	ID	SSID	2.4/5 GHz Security	6 GHz Security
☐		LWA_EA	1	LWA_EA	[open],[Web Auth]	

1 - 1 of 1 items

WLAN créé

Configuration du profil des politiques

Dans un profil de stratégie, vous pouvez sélectionner le VLAN qui attribue les clients, entre autres paramètres.

Vous pouvez soit utiliser votre profil de politique par défaut, soit en créer un nouveau.

Étape 1. Créer un nouveau profil de stratégie.

Accédez à Configuration > Tags & Profiles > Policy et configurez votre profil de stratégie par défaut ou créez-en un nouveau.

Assurez-vous que le profil est activé.

Add Policy Profile



⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

POLICY_PROFILE

Description

Enter Description

Status

ENABLED ☒

Passive Client

☐ DISABLED

IP MAC Binding

ENABLED ☒

Encrypted Traffic Analytics

☐ DISABLED

WLAN Switching Policy

Central Switching

ENABLED ☒

Central Authentication

ENABLED ☒

Central DHCP

ENABLED ☒

Flex NAT/PAT

☐ DISABLED

Créer un nouveau profil de stratégie

Étape 2 : sélection du VLAN

Rendez-vous à l'onglet Access Policies (politiques d'accès) et sélectionnez le nom du réseau VLAN dans la liste déroulante ou entrez manuellement son ID.

Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this 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
Disabled ⓘ

Local Subscriber Policy Name
Search or Select

VLAN

VLAN/VLAN Group
VLAN1432 x ⓘ

Multicast VLAN
Enter Multicast VLAN

WLAN ACL

IPv4 ACL
Search or Select

IPv6 ACL
Search or Select

URL Filters ⓘ

Pre Auth
Search or Select

Post Auth
Search or Select

Cancel
Apply to Device

Sélectionner le réseau VLAN

Configuration des balises des politiques

Vous pouvez associer votre SSID à votre profil de politiques dans la balise de politiques. Vous pouvez soit créer une nouvelle balise de politiques, soit utiliser la balise de politique par défaut.

Allez à Configuration > Tags & Profiles > Tags > Policy (configuration > balises et profils > balises > politiques) et ajoutez-en une nouvelle si nécessaire, comme illustré dans l'image.

Sélectionner + Ajouter :

Add Policy Tag

Name*
POLICY_TAG

Description
Enter Description

WLAN-POLICY Maps : 0

+ Add
X Delete

WLAN Profile	Policy Profile
No records available.	

10 items per page
0 - 0 of 0 items

Configuration des balises des politiques

Liez votre profil de réseau WLAN au profil de politiques souhaité:

Add Policy Tag

+ Add
X Delete

WLAN Profile	Policy Profile
No records available.	

10 items per page
0 - 0 of 0 items

Map WLAN and Policy

WLAN Profile*
LWA_EA
Policy Profile*
POLICY_PRO...

X
✓

> RLAN-POLICY Maps : 0

Cancel
Apply to Device

Configuration des balises des politiques

Affectation des balises des politiques

Affectez la balise de politiques aux points d'accès nécessaires.

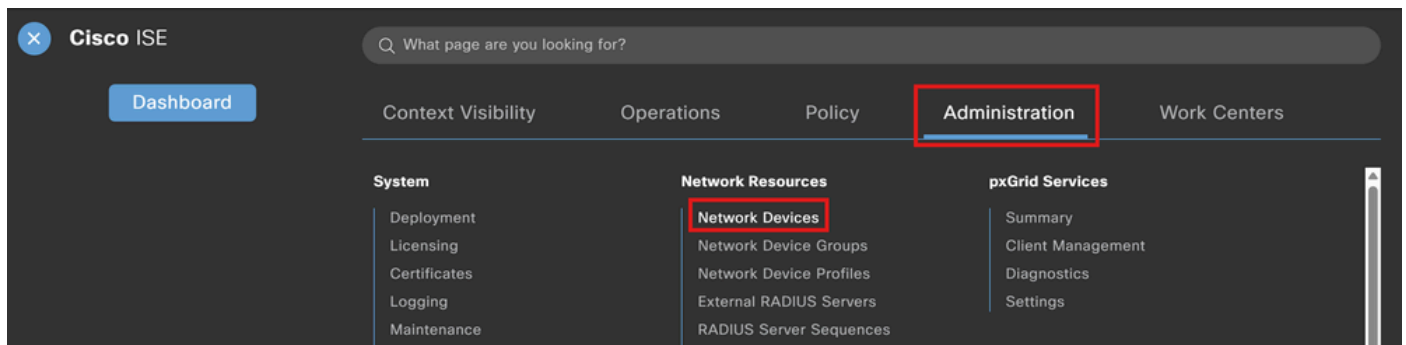
Pour attribuer la balise à un point d'accès, allez à Configuration > Wireless > Access Points > AP Name > General Tags (configuration > sans fil > points d'accès > nom des points d'accès > balises générales), effectuez l'affectation nécessaire, puis cliquez sur Update & Apply to Device (mettre à jour et appliquer à l'appareil).

Affectation des balises des politiques

Configuration ISE

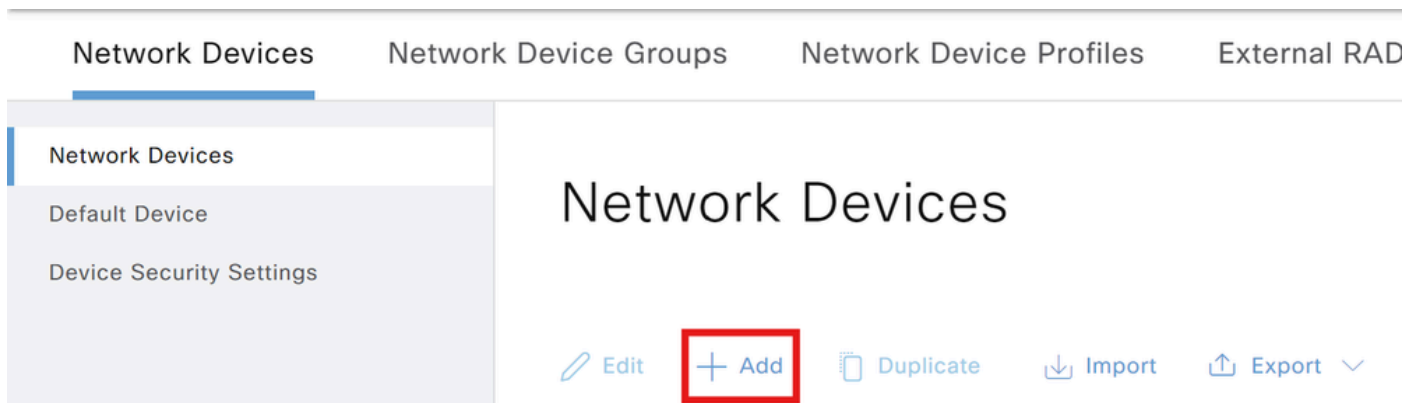
Ajouter un contrôleur WLC 9800 à ISE

Étape 1. Accédez à Administration > Network Resources > Network Devices comme indiqué dans l'image.



Ajouter un contrôleur WLC 9800 à ISE

Étape 2. Cliquez sur + Ajouter.



Ajouter des périphériques réseau

Il peut s'agir d'un nom de modèle, d'une version logicielle, d'une description et d'une affectation de groupes d'appareils réseau en fonction des types d'appareils, de l'emplacement ou des contrôleurs WLC.

Étape 3. Entrez les paramètres du WLC 9800 comme indiqué dans l'image. Entrez la même clé RADIUS définie lors de la création du serveur côté WLC. Cliquez ensuite sur Envoyer.

Network Devices

Name

9800-WLC

Description



IP Address



* IP :

192.0.2.20

/

32



Device Profile



Cisco



Model Name



Software Version



Network Device Group

Location

All Locations



[Set To Default](#)

IPSEC

Is IPSEC Device



[Set To Default](#)

Device Type

All Device Types



[Set To Default](#)



✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

.....

[Show](#)

Paramètres WLC du 9800

Étape 4. Accédez à Administration > Network Resources > Network Devices, vous pouvez voir la

liste des périphériques réseau.

Network Devices

Selected 0 Total 6

EditAddDuplicateImportExportGenerate PACDelete

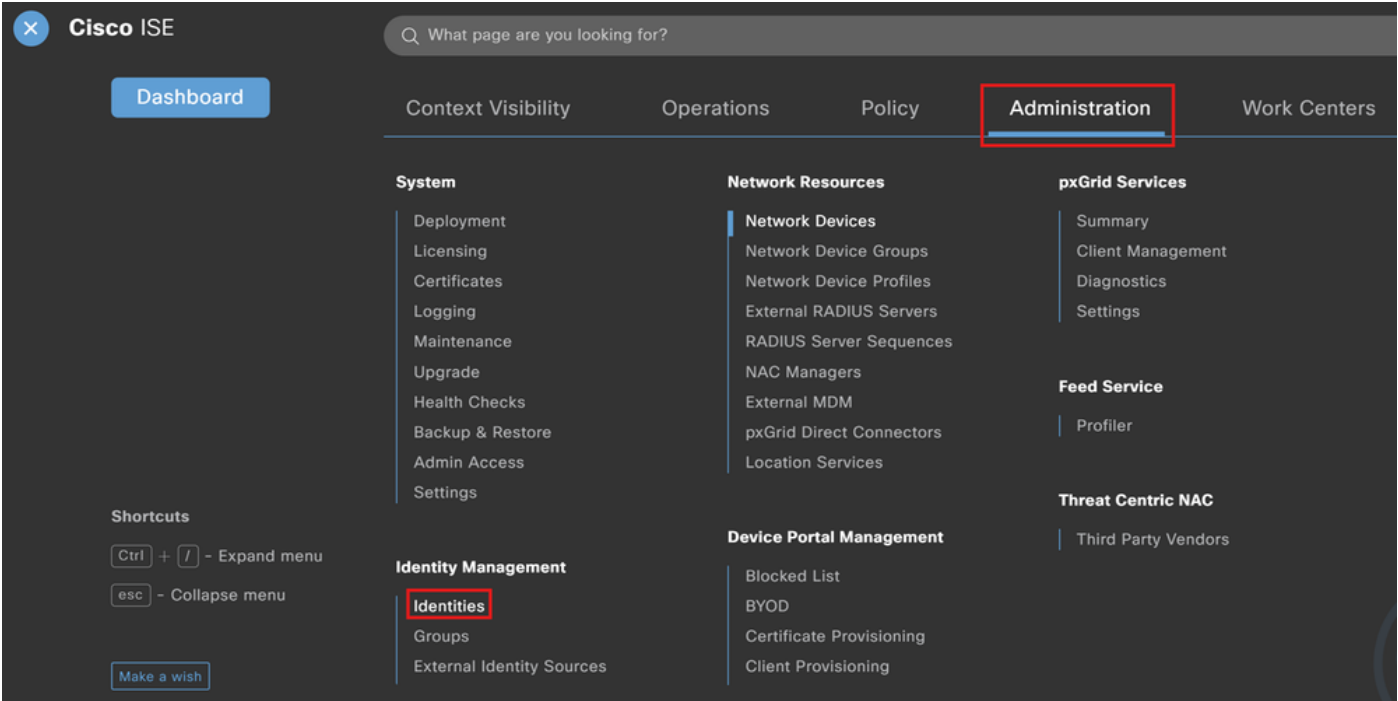
Quick Filter

	Name	IP/Mask	Profile Name	Location	Type
☐	9800		Cisco	All Locations	All Device Types
☐	9800-2		Cisco	All Locations	All Device Types
☐	9800-40		Cisco	All Locations	All Device Types
☐	9800-WLC	192.0.2.20/32	Cisco	All Locations	All Device Types

Liste des périphériques réseau

Créer un nouvel utilisateur sur ISE

Étape 1. Accédez à Administration > Identity Management > Identities :



Administration ISE - Identités

Étape 2. Accédez à Utilisateurs, cliquez sur +Ajouter.

Users

Latest Manual Network Scan Res...

Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#) [Delete](#)

Status

Username ^

Description

First Name

Last Name

Em:

Ajouter un utilisateur

Étape 3. Entrez le nom d'utilisateur et le mot de passe de l'utilisateur invité, puis cliquez sur Submit.

[Network Access Users List](#) > [New Network Access User](#)

Network Access User

* Username

guest

Status

☒ Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

☒ With Expiration

Password will expire in 60 days

☐ Never Expires

Password

Re-Enter Password

* Login Password

Generate Password

i

Enable Password

Generate Password

i

Créer un nouvel utilisateur sur ISE

Étape 4. Accédez à Administration > Identity Management > Identities > Users, vous pouvez voir la liste des utilisateurs.

Network Access Users

Edit

+ Add

Change Status

Import

Export

Delete

Duplicate

Status

Username

Descripti...

First Name

Last Name

Email Address

User Identity Groups

Admin

Enabled

guest

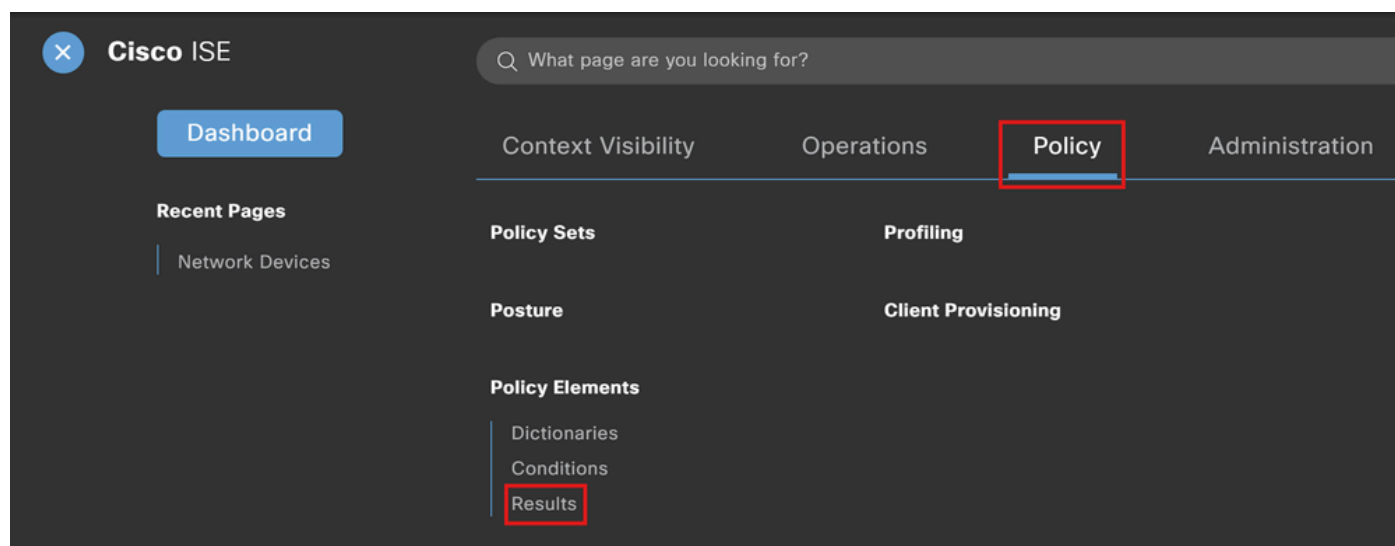
Liste des utilisateurs d'accès réseau

Créer un profil d'autorisation

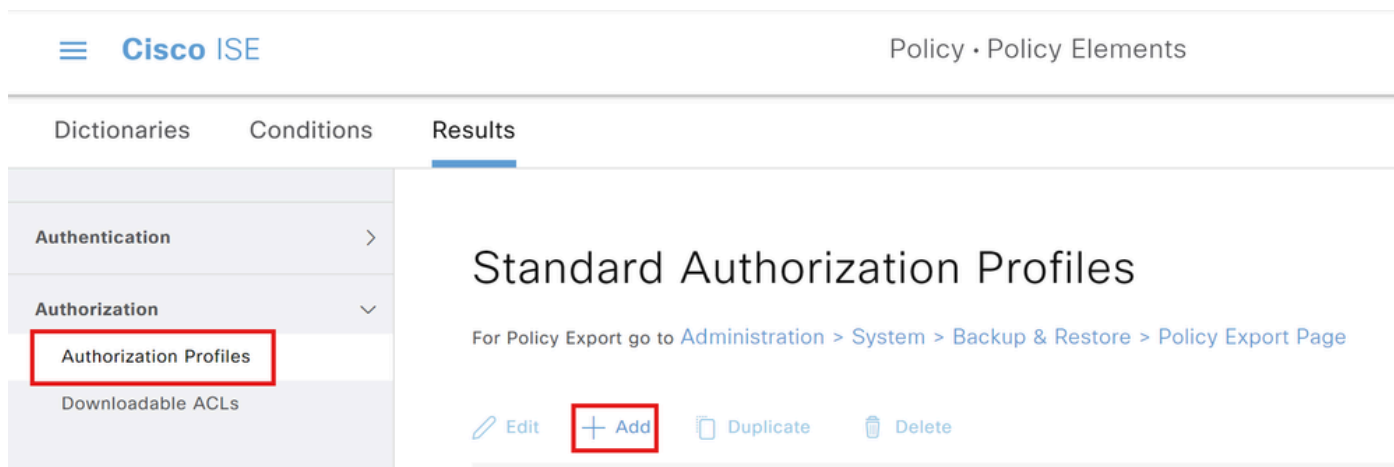
Le profil de politiques est le résultat attribué à un client selon ses paramètres (comme son adresse MAC, ses informations d'authentification, le réseau WLAN utilisé, etc.). Il est possible de lui affecter des paramètres précis comme un réseau local virtuel (VLAN), des listes de contrôle d'accès (ACL), des redirections d'URL (Uniform Resource Locator), etc.

Ces étapes montrent comment créer le profil d'autorisation nécessaire pour rediriger le client vers le portail d'authentification. Notez que dans les versions récentes d'ISE, un résultat d'autorisation Cisco_Webauth existe déjà. Ici, vous pouvez le modifier pour modifier le nom de la liste de contrôle d'accès de redirection afin qu'il corresponde à ce que vous avez configuré sur le contrôleur WLC.

Étape 1. Accédez à Policy > Policy Elements > Results.



Étape 2. Accédez à Authorization > Authorization Profiles. Cliquez sur +Add afin de créer un profil d'autorisation.



The screenshot shows the Cisco ISE web interface. The top navigation bar includes the Cisco ISE logo and the text 'Policy • Policy Elements'. Below this, there are tabs for 'Dictionaries', 'Conditions', and 'Results'. The 'Results' tab is active. On the left sidebar, under the 'Authorization' section, 'Authorization Profiles' is highlighted with a red box. The main content area is titled 'Standard Authorization Profiles' and includes a link for 'Policy Export'. At the bottom of the main content area, there are buttons for 'Edit', '+ Add' (highlighted with a red box), 'Duplicate', and 'Delete'.

Ajouter un profil d'autorisation

Étape 3 : création du profil d'autorisation LWA_EA_AUTHORIZATION. Les détails des attributs doivent être Access Type=ACCESS_ACCEPT. Cliquez sur Submit.

[Authorization Profiles](#) > New Authorization Profile

Authorization Profile

* Name	LWA_EA_AUTHORIZATION
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	☐
Track Movement	☐
Agentless Posture	☐
Passive Identity Tracking	☐

Créer un profil d'autorisation

Étape 4. Accédez à Politique > Eléments de politique > Résultats > Autorisation > Profils d'autorisation, vous pouvez voir les profils d'autorisation.

Dictionaries

Conditions

Results

Authentication >

Authorization ▾

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit

+ Add

Duplicate

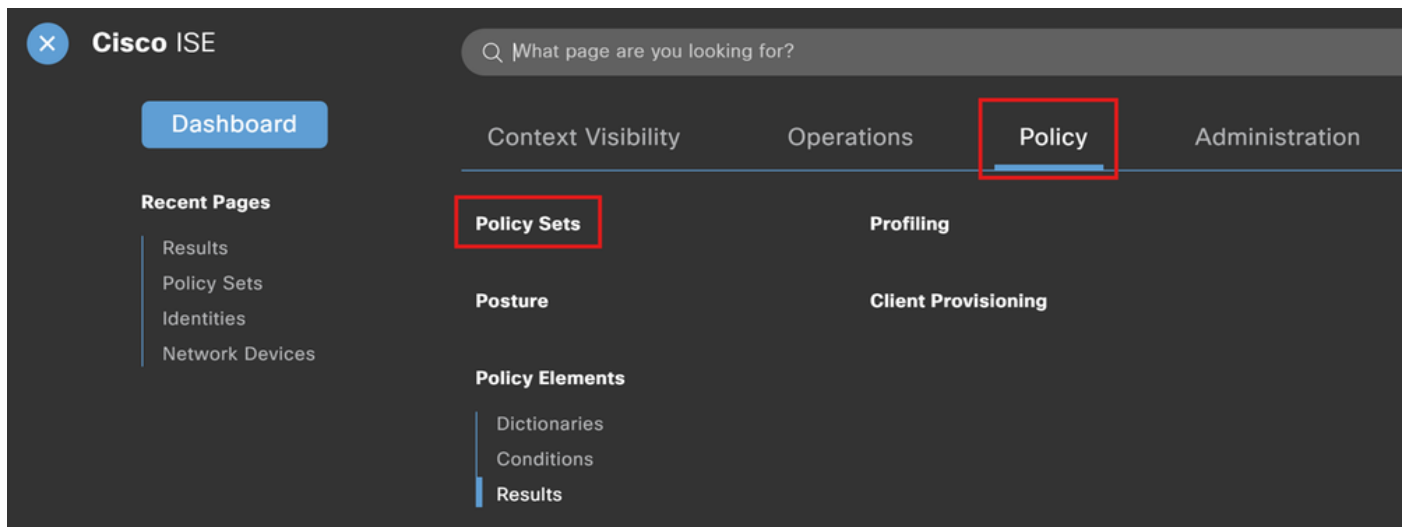
Delete

☐	Name	Profile
☐	9800-admin-priv	 Cisco 
☐	9800-helpdeskuser-priv	 Cisco 
☐	AuthZ-Guest	 Cisco 
☐	AuthZ_Guest-Redirect	 Cisco 
☐	AuthZ_Mobile	 Cisco 
☐	Block_Wireless_Access	 Cisco 
☐	Cisco_IP_Phones	 Cisco 
☐	Cisco_Temporal_Onboard	 Cisco 
☐	Cisco_WebAuth	 Cisco 
☐	LWA_EA_AUTHORIZATION	 Cisco 

Liste des profils d'autorisation

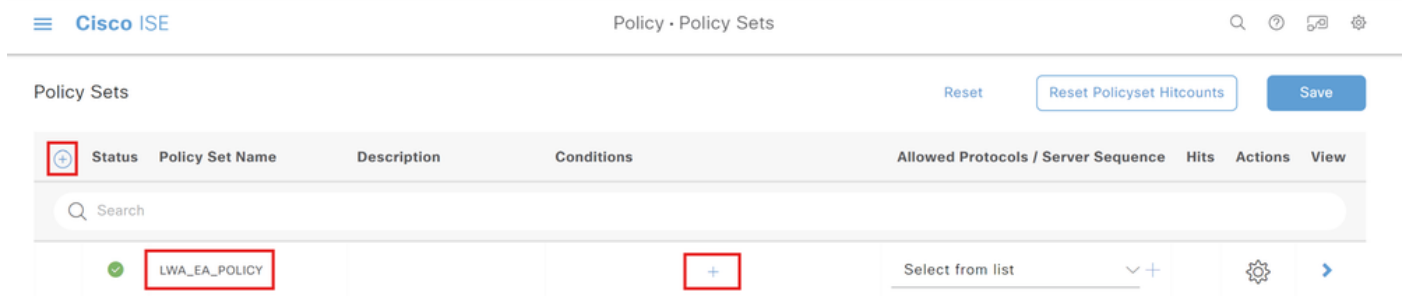
Configurer une règle d'authentification

Étape 1. Accédez à Policy > Policy Sets.



Stratégie ISE - Ensembles de stratégies

Étape 2. Sélectionnez le signe + et tapez le nom du jeu de stratégies LWA_EA_POLICY. Cliquez sur la colonne Conditions.



Configurer une règle d'authentification

Étape 3. Dans Dictionnaire, sélectionnez Accès réseau. Dans Attribut, sélectionnez Nom d'utilisateur.

Conditions Studio

Library

Search by Name



5G	
Catalyst_Switch_Local_Web_Authentication	
Switch_Local_Web_Authentication	
Switch_Web_Authentication	
Wired_802.1X	
Wired_MAB	
Wireless_802.1X	

Editor

Network Access-UserName

Select attribute for condition

Dictionary

Attribute

ID

Info

Network Access	Attribute	ID	
Network Access	Device IP Address		
Network Access	ISE Host Name		
Network Access	NetworkDeviceName		
Network Access	Protocol		
Network Access	UserName		
Network Access	VN		

Accès réseau dictionnaire

Étape 4. Définissez Equals et tapez guest dans la zone de texte (le nom d'utilisateur défini sur Administration > Identity Management > Identities > Users). Cliquez sur Save afin d'enregistrer les modifications.

Search by Name



5G	
Catalyst_Switch_Local_Web_Authentication	
Switch_Local_Web_Authentication	
Switch_Web_Authentication	
Wired_802.1X	
Wired_MAB	
Wireless_802.1X	
Wireless_Access	
Wireless_MAB	

Network Access-UserName

Equals

guest

Set to 'Is not'

Duplicate

Save

NEW AND OR

Close

Use

Nom d'utilisateur Invité

Étape 5. Accédez à Policy > Policy Sets. Dans l'ensemble de stratégies que vous avez créé, dans la colonne Protocoles autorisés/Séquence de serveur, sélectionnez Accès réseau par défaut.

The screenshot shows the Cisco ISE Policy Sets interface. At the top, there are buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save'. Below is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The 'Allowed Protocols / Server Sequence' column is highlighted with a red box. A dropdown menu is open for the 'LWA_EA_POLICY' row, showing 'Default Network Access' selected and highlighted with a red box.

Ensembles de stratégies

Étape 6. Cliquez sur Save afin d'enregistrer les modifications.

Configurer les règles d'autorisation

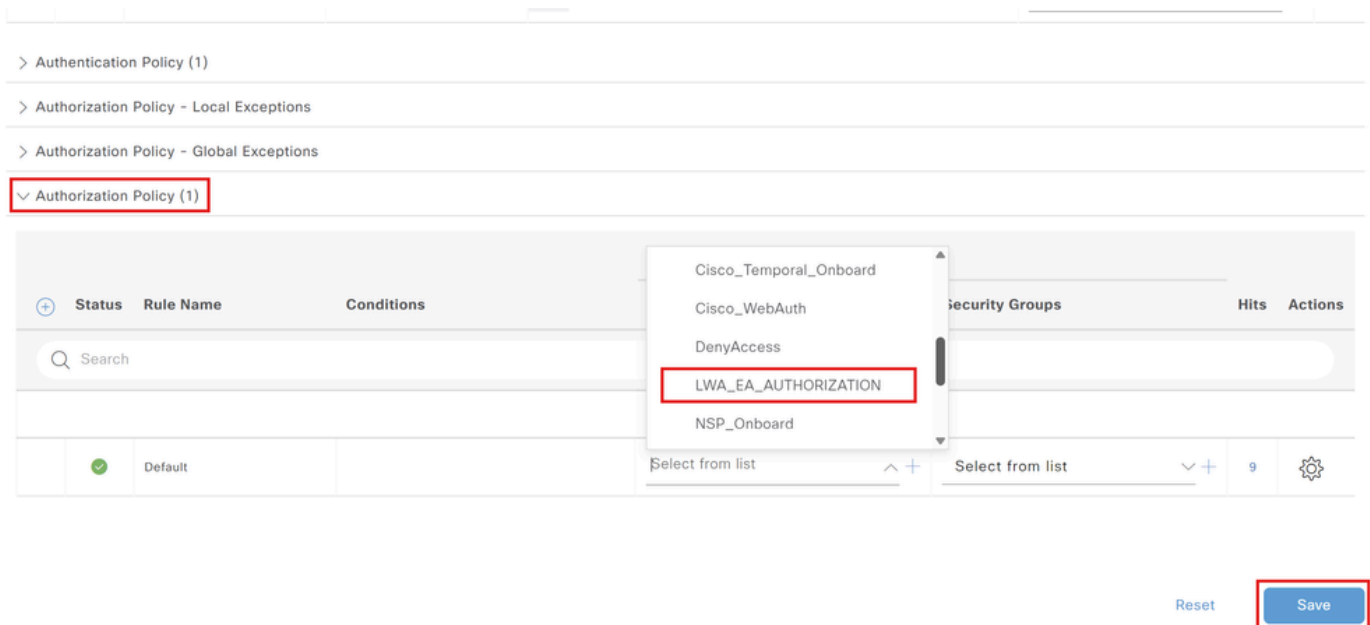
La règle d'autorisation est celle qui détermine quelles autorisations (quel profil d'autorisation) s'appliquent au client.

Étape 1. Accédez à Policy > Policy Sets. Cliquez sur l'icône en forme de flèche du jeu de stratégies que vous avez créé.

The screenshot shows the Cisco ISE Policy Sets interface. The 'Default Network Access' button in the 'Allowed Protocols / Server Sequence' column is highlighted with a red box.

Flèche Jeu de stratégies

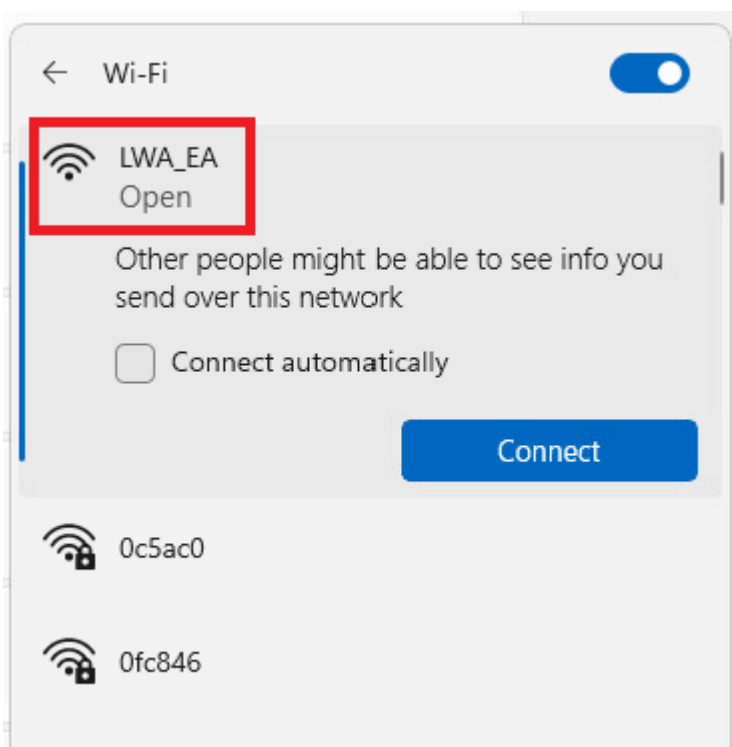
Étape 2. Sur la même page Policy set, développez Authorization Policy comme indiqué dans l'image. Dans la colonne Profiles, supprimez DenyAccess et ajoutez LWA_EA_AUTHORIZATION. Cliquez sur Save afin d'enregistrer les modifications.



Politique d'autorisation

Connecter le client invité

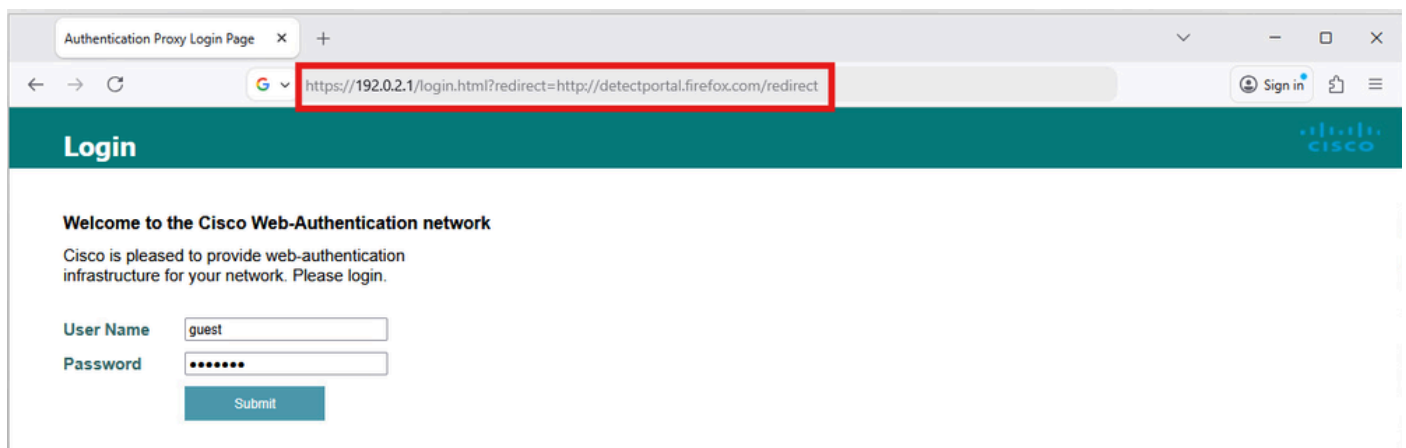
Étape 1. Sur votre ordinateur/téléphone, accédez aux réseaux Wi-Fi, recherchez le SSID LWA_EA et sélectionnez Connect.



Connecter le client invité

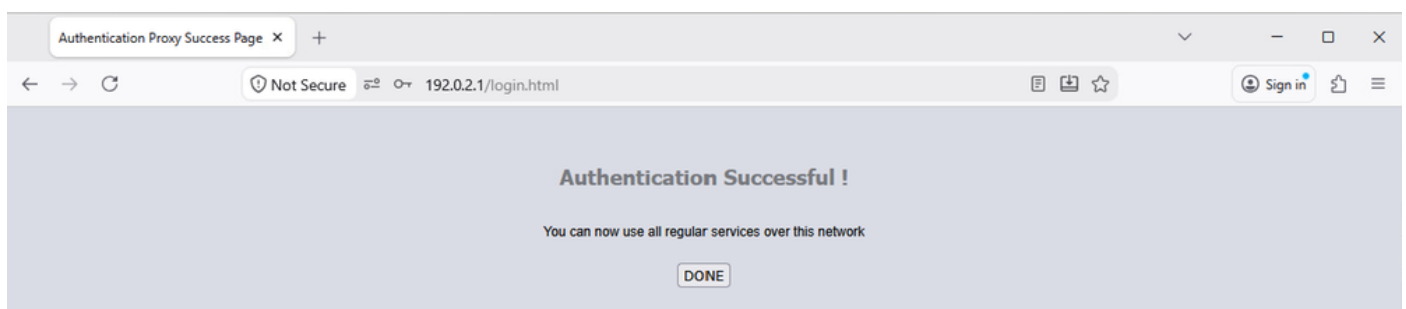
Étape 2. Une fenêtre de navigateur s'affiche avec la page de connexion. L'URL de redirection se

trouve dans la zone URL, et vous devez taper le nom d'utilisateur et le mot de passe pour accéder au réseau. Sélectionnez ensuite Envoyer.



Page de connexion avec URL de redirection

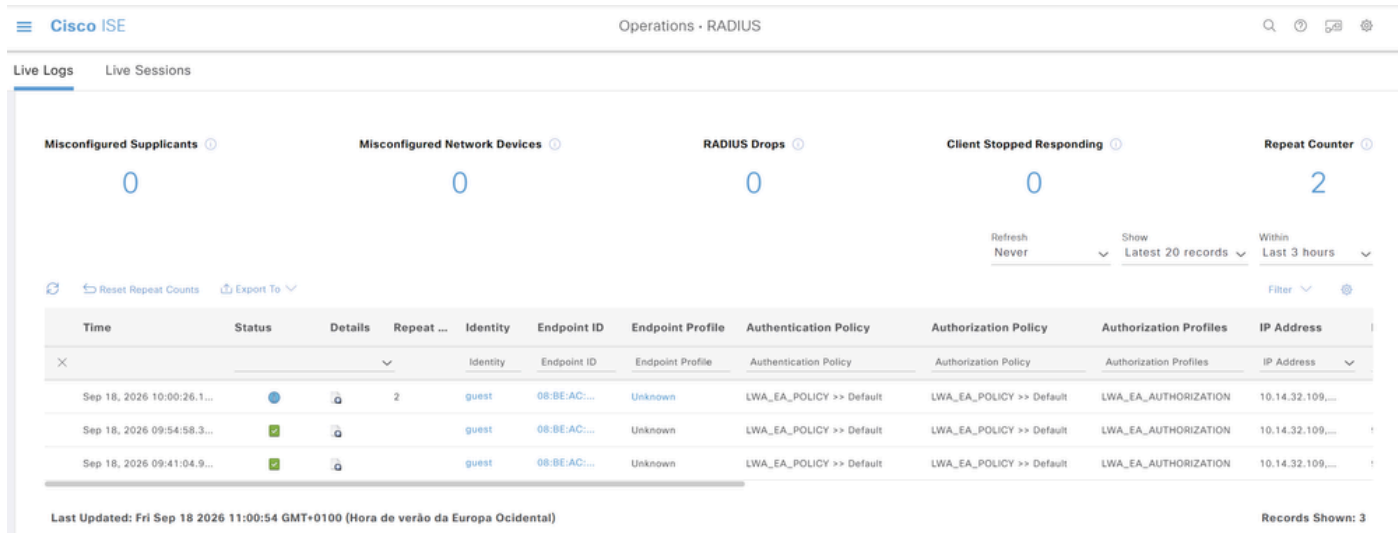
Si les informations d'identification sont correctes, une page d'authentification réussie s'affiche :



Page Authentification - Connexion réussie

 Remarque : L'URL présentée a été fournie par le WLC. Il contient l'IP virtuelle du WLC et la redirection pour l'URL de test de connexion Windows.

Étape 3. Accédez à Operations > RADIUS > Live Logs. Vous pouvez voir le périphérique client authentifié, ainsi que ses stratégies d'authentification et d'autorisation.



Journaux Radius Live

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Show WLAN Summary

<#root>

```
9800WLC#show wlan summary
```

```
Number of WLANs: 1
ID Profile Name SSID Status 2.4GHz/5GHz Security
-----
```

```
1 LWA_EA LWA_EA UP [open],[Web Auth]
```

```
9800WLC#
```

```
show wlan name LWA_EA
```

```
WLAN Profile Name : LWA_EA
=====
Identifier : 1
Description :
Network Name (SSID) : LWA_EA
Status : Enabled
Broadcast SSID : Enabled
Advertise-Apname : Disabled
Universal AP Admin : Disabled
(...)
Accounting list name :
```

802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security

Web Based Authentication : Enabled

OWE Transition Mode : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled

Webauth Authentication List Name : LWA_AUTHENTICATION

Webauth Authorization List Name : Disabled

Webauth Parameter Map : global

(...)
Security-2.4GHz/5GHz

802.11 Authentication : Open System

Static WEP Keys : Disabled

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

OSEN : Disabled
PMF Support : Disabled
(...)
Band Select : Disabled
Load Balancing : Disabled
(...)

Show Parameter Map Configuration

9800WLC#show running-config | section parameter-map type webauth global

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
```

trustpoint TP-self-signed-123456

Show AAA Information

<#root>

9800WLC#show aaa method-lists authentication

authen queue=AAA_ML_AUTHEN_LOGIN

name=LWA_AUTHENTICATION valid=TRUE id=BD000005 :state=ALIVE : SERVER_GROUP RADIUSGROUP

authen queue=AAA_ML_AUTHEN_ENABLE

authen queue=AAA_ML_AUTHEN_PPP

authen queue=AAA_ML_AUTHEN_SGBP

(...)

9800WLC#show aaa method-lists authorization

author queue=AAA_ML_AUTHOR_SHELL

author queue=AAA_ML_AUTHOR_NET

name=LWA_AUTHORIZATION valid=TRUE id=90000006 :state=ALIVE : SERVER_GROUP RADIUSGROUP

author queue=AAA_ML_AUTHOR_CONN

author queue=AAA_ML_AUTHOR_IPMOBILE

author queue=AAA_ML_AUTHOR_RM

(...)

9800WLC#show aaa servers

RADIUS: id 2, priority 1, host 192.0.2.30, auth-port 1812, acct-port 1813, hostname RADIUS

State: current UP, duration 8421s, previous duration 0s

Dead: total time 0s, count 0

Platform State from SMD: current UP, duration 8421s, previous duration 0s

SMD Platform Dead: total time 0s, count 0

Platform State from WNCD (0) : current UP

(...)

Dépannage

Problèmes courants

Voici plusieurs guides sur la façon de résoudre les problèmes d'authentification Web, tels que :

- Les utilisateurs ne peuvent pas authentifier.
- Problèmes de certificat.
- L'URL de redirection ne fonctionne pas.
- Les utilisateurs invités ne peuvent pas se connecter au WLAN invité.
- Les utilisateurs n'obtiennent pas d'adresse IP.
- La redirection vers la page de connexion d'authentification Web échoue.
- Une fois l'authentification réussie, les utilisateurs invités ne parviennent pas à accéder à Internet.

Ces guides décrivent en détail les étapes de dépannage :

- [Dépannage des problèmes courants d'authentification Web](#)
- [Autres situations à dépanner](#)

Débogage conditionnel et suivi actif radio et capture de paquets intégrée

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 (l'adresse MAC du client dans ce cas). Afin d'activer le débogage conditionnel, utilisez les étapes dans le guide, [Débogage conditionnel et RadioActive trace](#).

Vous pouvez également collecter des données EPC (Embedded Packet capture). EPC est une fonction de capture de paquets qui permet de visualiser les paquets destinés aux WLC Catalyst 9800, provenant de ceux-ci et transitant par ceux-ci, à savoir les paquets DHCP, DNS et HTTP GET dans LWA. Ces captures peuvent être exportées pour une analyse hors ligne avec Wireshark. Pour des étapes détaillées sur la façon de faire ceci, référez-vous à [Capture de paquets incorporée](#).

Exemple d'une tentative réussie

Il s'agit de la sortie de RA_traces pour une tentative réussie d'identifier chacune des phases lors du processus d'association/authentification, tout en étant connecté à un SSID invité avec un serveur RADIUS.

Association/authentification 802.11 :

[client-orch-sm] [17062] : (remarque) : MAC : 08be.ac3f Association reçue. BSSID cc70.edcf.552f, WLAN LWA_EA, AP logement 1 2ce3.8eb4, CW9172I-LAB

[client-orch-sm] [17062] : (débogage) : MAC : 08be.ac3f A reçu une demande d'association Dot11. Traitement démarré, SSID : LWA_EA, Profil de stratégie : POLICY_PROFILE, Nom du point d'accès : CW9172I-LAB, adresse MAC d'application : 2ce3.8eb4 BSSID ID MAC0000.0000.0000 wlan : 1 RSSI : -49, NUJ : 46

[client-orch-state] [17062] : (remarque) : MAC : 08be.ac3f Transition d'état du client : S_CO_INIT -> S_CO_ASSOCIATING

[dot11-validate] [17062] : (info) : MAC : 08be.ac3f Dot11 ie valider les taux ext/supp. Validation réussie

pour les taux pris en charge radio_type 2

[dot11-validate] [17062] : (info) : MAC : 08be.ac3f WiFi direct : Dot11 valide l'IE P2P. IE P2P absent.

[point11] [17062] : (débogage) : MAC : 08be.ac3f dot11 send association response. Réponse d'association de tramage avec resp_status_code : 0

[point11] [17062] : (débogage) : MAC : 08be.ac3f Dot11 Informations de capacité octet1 1, octet2 : 11

[dot11-frame] [17062] : (info) : MAC : 08be.ac3f WiFi direct : ignorer la création d'un revendeur associé avec un IE P2P : Stratégie directe Wi-Fi désactivée

[point11] [17062] : (info) : MAC : 08be.ac3f dot11 send association response. Longueur de la réponse assoc d'envoi : 130 avec resp_status_code : 0, DOT11_STATUS : SUCCÈS_ÉTAT_POINT11

[point11] [17062] : (remarque) : MAC : 08be.ac3f Réussite de l'association. AID 1, Itinérance = Faux, WGB = Faux, 11r = Faux, 11w = Faux Itinérance rapide = Faux

[point11] [17062] : (info) : MAC : 08be.ac3f transition d'état DOT11 : S_DOT11_INIT -> S_DOT11_ASSOCIATED

[client-orch-sm] [17062] : (débogage) : MAC : L'association 08be.ac3f Station Dot11 a réussi.

Processus d'apprentissage IP :

[client-orch-state] [17062] : (remarque) : MAC : 08be.ac3f Transition d'état du client : S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

[client-iplearn] [17062] : (info) : MAC : 08be.ac3f IP-learn state transition : S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

[auth-client] [17062] : (info) : MAC : 08be.ac3f Transition d'état de l'interface d'authentification du client : S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE

[client-iplearn] [17062] : (remarque) : MAC : 08be.ac3f Apprentissage des adresses IP du client réussi. Méthode : IP DHCP : 10.14.32.109

[client-iplearn] [17062] : (info) : MAC : 08be.ac3f IP-learn state transition : S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

[client-orch-sm] [17062] : (débogage) : MAC : 08be.ac3f Réception de la réponse d'apprentissage ip. méthode : IPLEARN_METHOD_DHCP

Authentification de couche 3 :

[client-orch-sm] [17062] : (débogage) : MAC : 08be.ac3f Authentification C3 déclenchée. état = 0x0, Réussite

[client-orch-state] [17062] : (remarque) : MAC : 08be.ac3f Transition d'état du client : S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS

[auth-client] [17062] : (remarque) : MAC : 08be.ac3f Lancement de l'authentification C3. LOI

[auth-client] [17062] : (info) : MAC : 08be.ac3f Transition d'état de l'interface d'authentification du client : S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[webauth-httpd] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]GET rcvd en état LOGIN

[webauth-httpd] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]Requête HTTP GET

[webauth-httpd] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]Parse GET, src [10.14.32.109] dst [10.107.221.82] url [<http://firefox.detect.portal/>]

[webauth-httpd] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]Lecture terminée : parse_request_return 8

[webauth-io] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]56538/219 LECTURE DE L'ÉTAT DES E/S -> ÉCRITURE

[webauth-io] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]56538/219 État des E/S ÉCRITURE -> LECTURE

[webauth-io] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]56539/218 État des E/S NOUVEAU -> LECTURE

[webauth-io] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Lire l'événement, Message prêt

[webauth-httpd] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]POST rcvd en état LOGIN

Authentification de couche 3 réussie, déplacez le client à l'état d'exécution :

[auth-mgr] [17062] : (info) : [08be.ac3f : capwap_90000004] Invité de nom d'utilisateur reçu pour le client 08be.ac3f

[auth-mgr] [17062] : (info) : [08be.ac3f : capwap_90000004] une notification d'ajout/de modification d'attribut auth mgr est reçue pour attr auth-domain(954)

[auth-mgr] [17062] : (info) : [08be.ac3f : capwap_90000004] L'état de la méthode webauth passe de 'En cours d'exécution' à 'Réussite authentique'

[auth-mgr] [17062] : (info) : [08be.ac3f : capwap_90000004] Changement de l'état du contexte de 'En cours d'exécution' à 'Authentique réussite'

[auth-mgr] [17062] : (info) : [08be.ac3f : capwap_90000004] une notification d'ajout/de modification d'attribut auth mgr est reçue pour la méthode attr(757)

[auth-mgr] [17062] : (info) : [08be.ac3f : capwap_90000004] Événement déclenché AUTHZ_SUCCESS (11)

[auth-mgr] [17062] : (info) : [08be.ac3f : capwap_90000004] Le contexte change l'état de 'Authc Success' en 'Authz Success'

[webauth-acl] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]Application de la liste de contrôle d'accès de déconnexion IPv4 via SVM, nom : IP-Adm-V4-LOGOUT-ACL, priorité : 51, IIF-ID : 0

[webauth-sess] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]Param-map utilisé : global

[webauth-state] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]Param-map utilisé : global

[webauth-state] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]State AUTHC_SUCCESS - > AUTHZ

[page-webauth] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]Page de réussite de l'envoi de Webauth

[webauth-io] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]56539/218 AUTHENTIFICATION DE L'ÉTAT DES E/S -> ÉCRITURE

[webauth-io] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]56539/218 ÉTAT DES E/S ÉCRITURE -> FIN

[webauth-httpd] [17062] : (info) : capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Supprimez l'E/S ctx et fermez le socket, id [99000029]

[auth-client] [17062] : (remarque) : MAC : Authentification L3 08be.ac3f réussie. ACL :[]

[auth-client] [17062] : (info) : MAC : 08be.ac3f Transition d'état de l'interface d'authentification du client : S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE

[webauth-httpd] [17062] : (info) : capwap_90000004[08be.ac3f][10.48.39.243]56538/219 Supprimer l'E/S ctx et fermer le socket, id [D7000028]

[errmsg] [17062] : (info) : %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE : R0/0: wncd : Entrée de nom d'utilisateur (invité) jointe à ssid (LWA_EA) pour le périphérique avec MAC : 08be.ac3f

[aaa-attr-inf] [17062] : (info) : [Attribut appliqué : bsn-vlan-interface-name 0 "VLAN0039"]

[aaa-attr-inf] [17062] : (info) : [Attribut appliqué : timeout 0 1800 (0x708)]

[aaa-attr-inf] [17062] : (info) : [Attribut appliqué : url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]

[ewlc-qos-client] [17062] : (info) : MAC : 08be.ac3f Gestionnaire d'état d'exécution QoS client

[rog-proxy-capwap] [17062] : (débogage) : Notification d'état d'exécution du client géré : 08be.ac3f

[client-orch-state] [17062] : (remarque) : MAC : 08be.ac3f Transition d'état du client : S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)

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.