

# Configuration, vérification et dépannage d'un invité filaire dans un contrôleur LAN sans fil

## Table des matières

---

---

### Introduction

Ce document décrit comment configurer, vérifier et dépanner l'accès invité filaire dans le 9800 et l'IRCM avec l'authentification Web externe.

### Conditions préalables

#### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

9800 WLC

WLC AireOS

tunnel de mobilité

ISE

On suppose qu'un tunnel de mobilité entre les deux WLC a été établi avant de configurer l'accès invité filaire.

Cet aspect sort du cadre de cet exemple de configuration. Pour obtenir des instructions détaillées, reportez-vous au document joint intitulé [Configuration des topologies de mobilité sur le 9800](#)

#### Composants utilisés

WLC 9800 version 17.12.1

5520 WLC version 8.10.185.0

ISE version 3.1.0.518

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.

### Configuration d'un invité filaire sur le Catalyst 9800 ancré à un

## autre Catalyst 9800

### Diagramme du réseau



Topologie du réseau

## Configuration sur le WLC 9800 étranger

### Configurer la carte de paramètres Web

Étape 1 : Accédez à Configuration > Security > Web Auth, sélectionnez Global, vérifiez l'adresse IP virtuelle du contrôleur et le mappage Trustpoint, et assurez-vous que le type est défini sur webauth.

Parameter Map Name

- global
- Web-Filter

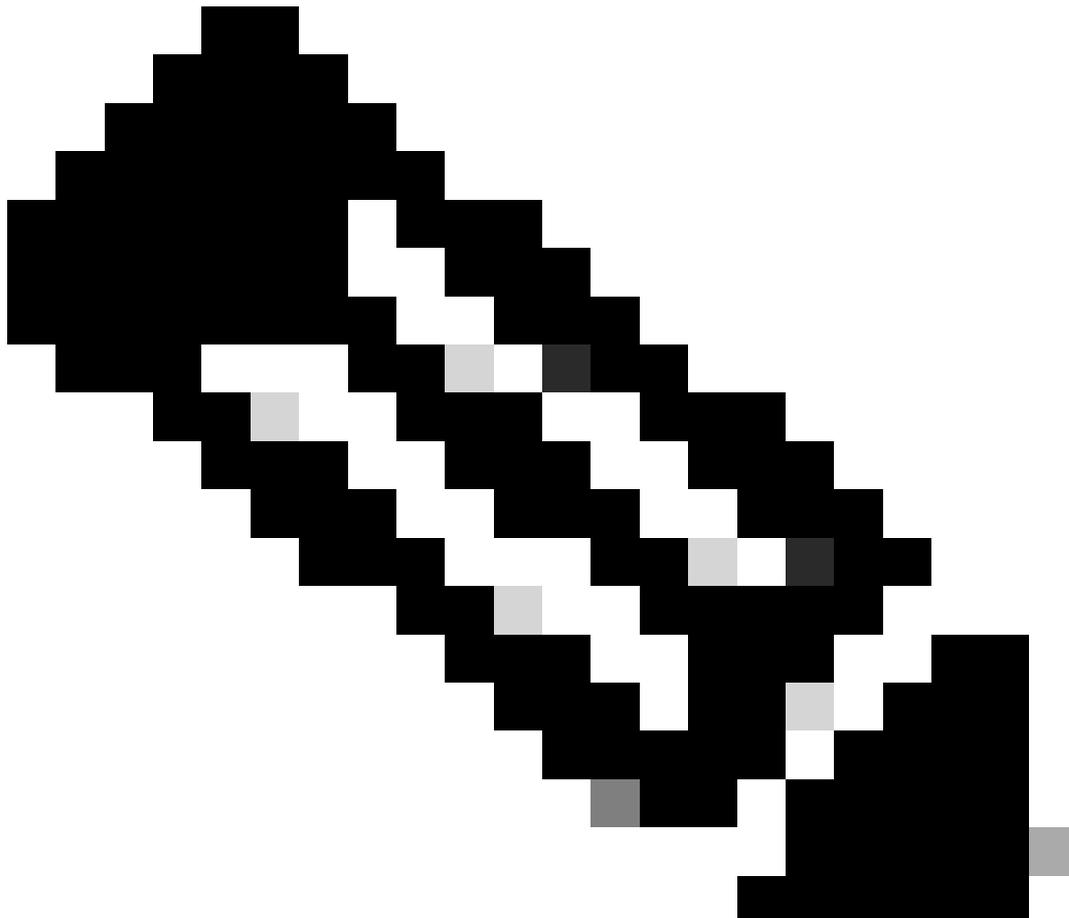
1 10

---

**General**    Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	XXXXXX:XX
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input checked="" type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	<b>Banner Configuration</b>	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text

Mappage de paramètre global



Remarque : l'interception HTTP par l'authentification Web est un paramètre facultatif. Si la redirection HTTPS est requise, l'option HTTPS d'interception d'authentification Web doit être activée. Cependant, cette configuration n'est pas recommandée car elle augmente l'utilisation du CPU.

Étape 2 : Sous l'onglet Advanced, configurez l'URL de la page Web externe pour la redirection du client. Définissez « Redirect URL for Login » et « Redirect On-Failure » ; « Redirect On-Success » est facultatif. Une fois configuré, un aperçu de l'URL de redirection s'affiche dans le profil d'authentification Web.

General **Advanced**

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

### Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	X:X:X:X

Onglet Avancé

## Configuration CLI

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
intercept-https-enable
```

trustpoint TP-self-signed-3915430211  
webauth-http-enable

Remarque : dans ce scénario, la carte de paramètre globale est utilisée. Selon les besoins, configurez une carte de paramètre Web personnalisée en sélectionnant Ajouter et, définissez l'URL de redirection sous l'onglet Avancé. Les paramètres Trustpoint et Virtual IP sont hérités du profil global.

## Paramètres AAA :

Étape 1 : Créez un serveur Radius :

Accédez à Configuration > Security > AAA, cliquez sur "Add" sous la section Server/Group, et sur la page "Create AAA Radius Server", entrez le nom du serveur, l'adresse IP et le secret partagé.

The screenshot shows the 'Create AAA Radius Server' configuration page. The 'Add' button and the 'Servers' tab are highlighted with red boxes. The form includes the following fields and options:

- Name\* (text input)
- Server Address\* (text input, placeholder: IPv4/IPv6/Hostname)
- PAC Key (checkbox, unchecked)
- Key Type (dropdown menu, value: Clear Text)
- Key\* (text input, with info icon)
- Confirm Key\* (text input)
- Auth Port (text input, value: 1812)
- Acct Port (text input, value: 1813)
- Server Timeout (seconds) (text input, value: 1-1000)
- Retry Count (text input, value: 0-100)
- Support for CoA (toggle, value: ENABLED)
- CoA Server Key Type (dropdown menu, value: Clear Text)
- CoA Server Key (text input)
- Confirm CoA Server Key (text input)
- Automate Tester (checkbox, unchecked)

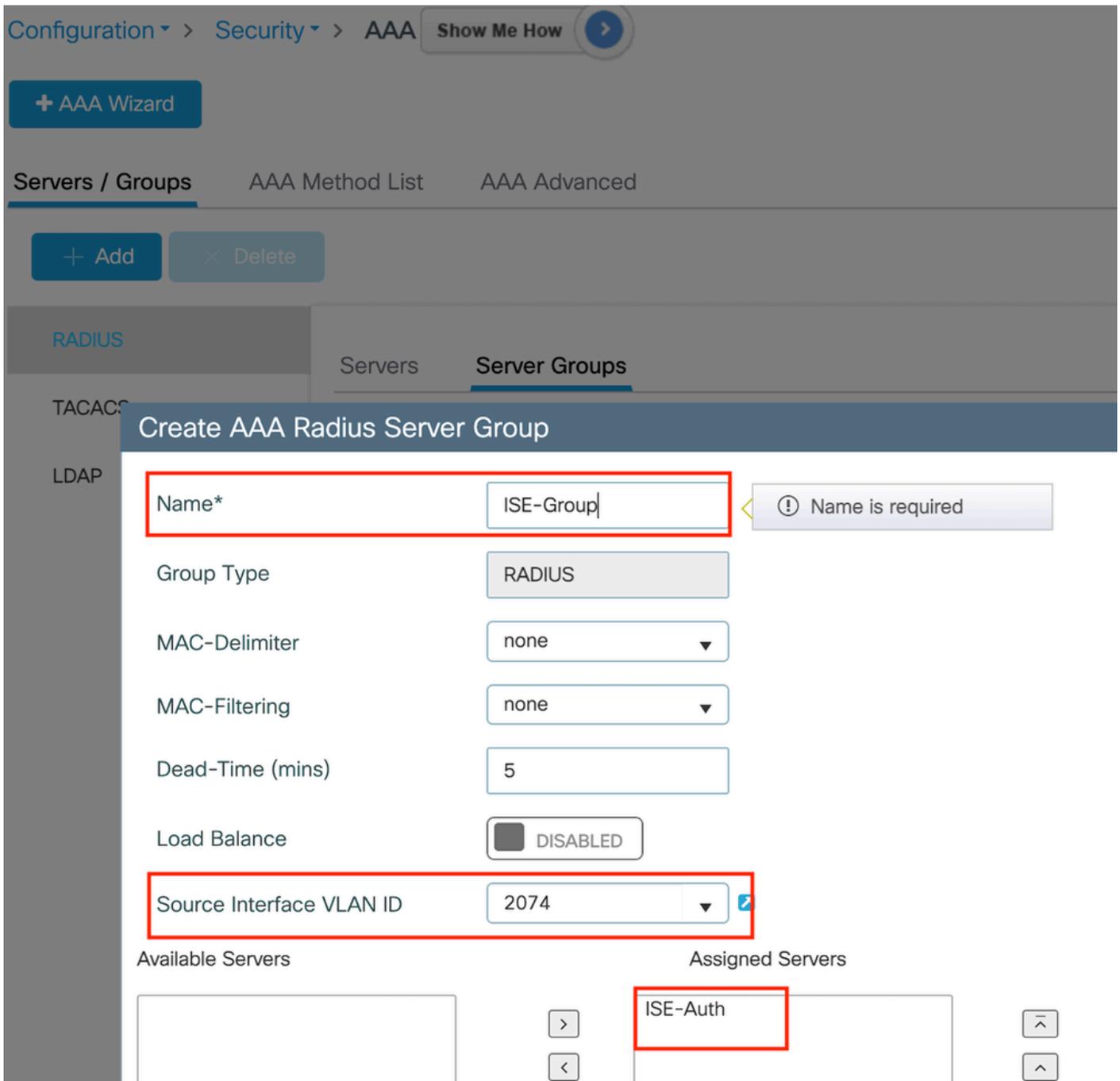
Buttons: Cancel, Apply to Device

Configuration du serveur RADIUS

Configuration CLI

```
radius server ISE-Auth
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
key *****
server name ISE-Auth
```

Étape 2 : créez un groupe de serveurs RADIUS :  
Sélectionnez Ajouter dans la section Groupes de serveurs pour définir un groupe de serveurs et basculer les serveurs à inclure dans la configuration du groupe.



Groupe de serveurs Radius

Configuration CLI

```
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2074
deadtime 5
```

Étape 3 : Configurez la liste de méthodes AAA :

Accédez à l'onglet Liste de méthodes AAA, sélectionnez Ajouter sous Authentification, définissez un nom de liste de méthodes avec le type « login » et le type de groupe « Group », et mappez le groupe de serveurs d'authentification configuré sous la section Groupe de serveurs affecté.

The screenshot shows the Cisco ISE configuration interface for AAA Method List. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is selected. Under the 'Authentication' section, the 'Add' button is highlighted. The 'Quick Setup: AAA Authentication' form is displayed with the following fields:

- Method List Name\*: ISE-List
- Type\*: login
- Group Type: group
- Fallback to local:
- Available Server Groups: tacacs, undefined, Radius-Group, Test-group, test-group, undefined, tacacs1
- Assigned Server Groups: ISE-Group

Liste des méthodes d'authentification

## Configuration CLI

```
aaa authentication login ISE-List group ISE-Group
```

## Configurer le profil de stratégie

Étape 1 : Accédez à Configuration > Tags & Profiles > Policy, nommez votre nouveau profil dans

l'onglet General, et activez-le à l'aide de la bascule d'état.

Configuration > Tags & Profiles > Policy

+ Add   × Delete   Clone

### 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*	<input type="text" value="GuestLANPolicy"/>	WLAN Switching Policy	
Description	<input type="text" value="Enter Description"/>	Central Switching	<input checked="" type="checkbox"/> ENABLED
Status	<input checked="" type="checkbox"/> ENABLED	Central Authentication	<input checked="" type="checkbox"/> ENABLED
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input checked="" type="checkbox"/> ENABLED
IP MAC Binding	<input checked="" type="checkbox"/> ENABLED	Flex NAT/PAT	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED		
CTS Policy			
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

Profil de stratégie

Étape 2 : Sous l'onglet Access Policies, attribuez un VLAN aléatoire lorsque le mappage de VLAN est terminé sur le contrôleur d'ancrage. Dans cet exemple, vlan 1 est configuré

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  ⓘ

**VLAN**

VLAN/VLAN Group  ⓘ

Multicast VLAN

**WLAN ACL**

IPv4 ACL  ⓘ

IPv6 ACL  ⓘ

**URL Filters** ⓘ

Pre Auth  ⓘ

Post Auth  ⓘ

Onglet Access Policy

Étape 3 : Sous l'onglet Mobility, basculez le contrôleur d'ancrage sur Primary (1) et configurez éventuellement des tunnels de mobilité Secondary et Tertiary pour les exigences de redondance

General Access Policies QOS and AVC **Mobility** Advanced

**Mobility Anchors**

Export Anchor

Static IP Mobility  DISABLED

*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

Anchor IP	Anchor Priority
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.106.40.11 <span style="float: right;">→</span> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.76.118.75 <span style="float: right;">→</span> </div> <div style="border: 1px solid #ccc; padding: 5px;">  10.76.118.74 <span style="float: right;">→</span> </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.76.118.70 <input type="text" value="Primary (1)"/> <span style="float: right;">←</span> </div>

Carte de mobilité

Configuration CLI

```
wireless profile policy GuestLANPolicy
mobility anchor 10.76.118.70 priority 1
no shutdown
```

## Configurer le profil de réseau local invité

Étape 1 : Accédez à Configuration > Wireless > Guest LAN, sélectionnez Add, configurez un nom de profil unique, activez Wired VLAN, entrez l'ID de VLAN pour les utilisateurs invités filaires et basculez l'état du profil sur Enabled.

General	Security
Profile Name*	Client Association Limit
<input type="text" value="Guest-Profile"/>	<input type="text" value="2000"/>
Guest LAN ID*	Wired VLAN Status
<input type="text" value="1"/>	<input checked="" type="checkbox" value="ENABLE"/>
mDNS Mode	Wired VLAN ID*
<input type="text" value="Bridging"/>	<input type="text" value="2024"/>
Status	
<input checked="" type="checkbox" value="ENABLE"/>	

Profil de réseau local invité

Étape 2 : Sous l'onglet Security, activez Web Auth, mappez la carte de paramètres Web Auth et sélectionnez le serveur Radius dans la liste déroulante Authentication.

# Edit Guest LAN Profile

General

**Security**

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List



Onglet Sécurité du réseau local invité

## Configuration CLI

```
guest-lan profile-name Guest-Profile 1 wired-vlan 2024
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## Plan du réseau local invité

Accédez à Configuration > Wireless > Guest LAN.

Dans la section Guest LAN MAP configuration, sélectionnez Add and map the Policy profile and Guest LAN profile

## Guest LAN Map Configuration

+ Add Map    × Delete Map

Guest LAN Map : GuestMap

+ Add    × Delete

Guest LAN Profile Name	Policy Name
No records available.	
10 items per page    0 - 0 of 0 items	

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save    Cancel

Plan du réseau local invité

## Configuration CLI

```
wireless guest-lan map GuestMap  
guest-lan Guest-Profile policy GuestLANPolicy
```

## Configuration sur le WLC Anchor 9800

### Configurer la carte de paramètres Web

Étape 1 : Accédez à Configuration > Security > Web Auth, sélectionnez Global, vérifiez l'adresse IP virtuelle du contrôleur et le mappage Trustpoint, et assurez-vous que le type est défini sur webauth.

Configuration > Security > Web Auth

+ Add    × Delete

Parameter Map Name

- global
- Web-Filter

1    10

### Edit Web Auth Parameter

General    Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	XXXXXX:XX
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input checked="" type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text

Étape 2 : Sous l'onglet Advanced, configurez l'URL de la page Web externe pour la redirection du client. Définissez « Redirect URL for Login » et « Redirect On-Failure » ; « Redirect On-Success » est facultatif.

Une fois configuré, un aperçu de l'URL de redirection s'affiche dans le profil d'authentification Web.

General **Advanced**

**i** Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

### Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	x::x::x::x

Onglet Avancé

## Configuration CLI

```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 intercept-https-enable.
 trustpoint TP-self-signed-3915430211
 webauth-http-enable
```

## Paramètres AAA :

### Étape 1 : Créez un serveur Radius :

Accédez à Configuration > Security > AAA, cliquez sur Add sous la section Server/Group, et sur la page "Create AAA Radius Server", entrez le nom du serveur, l'adresse IP et le secret partagé.

The screenshot shows the 'Create AAA Radius Server' configuration page. The 'Name\*' field is highlighted with a red box. The 'Server Address\*' field is also highlighted with a red box. The 'Key Type' dropdown menu is highlighted with a red box. The 'Key\*' and 'Confirm Key\*' fields are highlighted with a red box. The 'Auth Port' field is set to 1812. The 'Acct Port' field is set to 1813. The 'Server Timeout (seconds)' field is set to 1-1000. The 'Retry Count' field is set to 0-100. The 'Support for CoA' toggle is set to 'ENABLED'. The 'CoA Server Key Type' dropdown menu is set to 'Clear Text'. The 'CoA Server Key' and 'Confirm CoA Server Key' fields are empty. The 'Automate Tester' checkbox is unchecked. The 'Apply to Device' button is visible at the bottom right.

Configuration du serveur RADIUS

### Configuration CLI

```
radius server ISE-Auth
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
key *****
server name ISE-Auth
```

### Étape 2 : créez un groupe de serveurs RADIUS :

Sélectionnez Add dans la section Server Groups pour définir un groupe de serveurs et basculer les serveurs à inclure dans la configuration du groupe.

Name*	ISE-Group
Group Type	RADIUS

MAC-Delimiter	none ▼
---------------	--------

MAC-Filtering	none ▼
---------------	--------

Dead-Time (mins)	5
------------------	---

Load Balance	<input type="checkbox"/> DISABLED
--------------	-----------------------------------

Source Interface VLAN ID	2081 ▼ 
--------------------------	--

Available Servers

Assigned Servers

--



ISE-Auth
----------

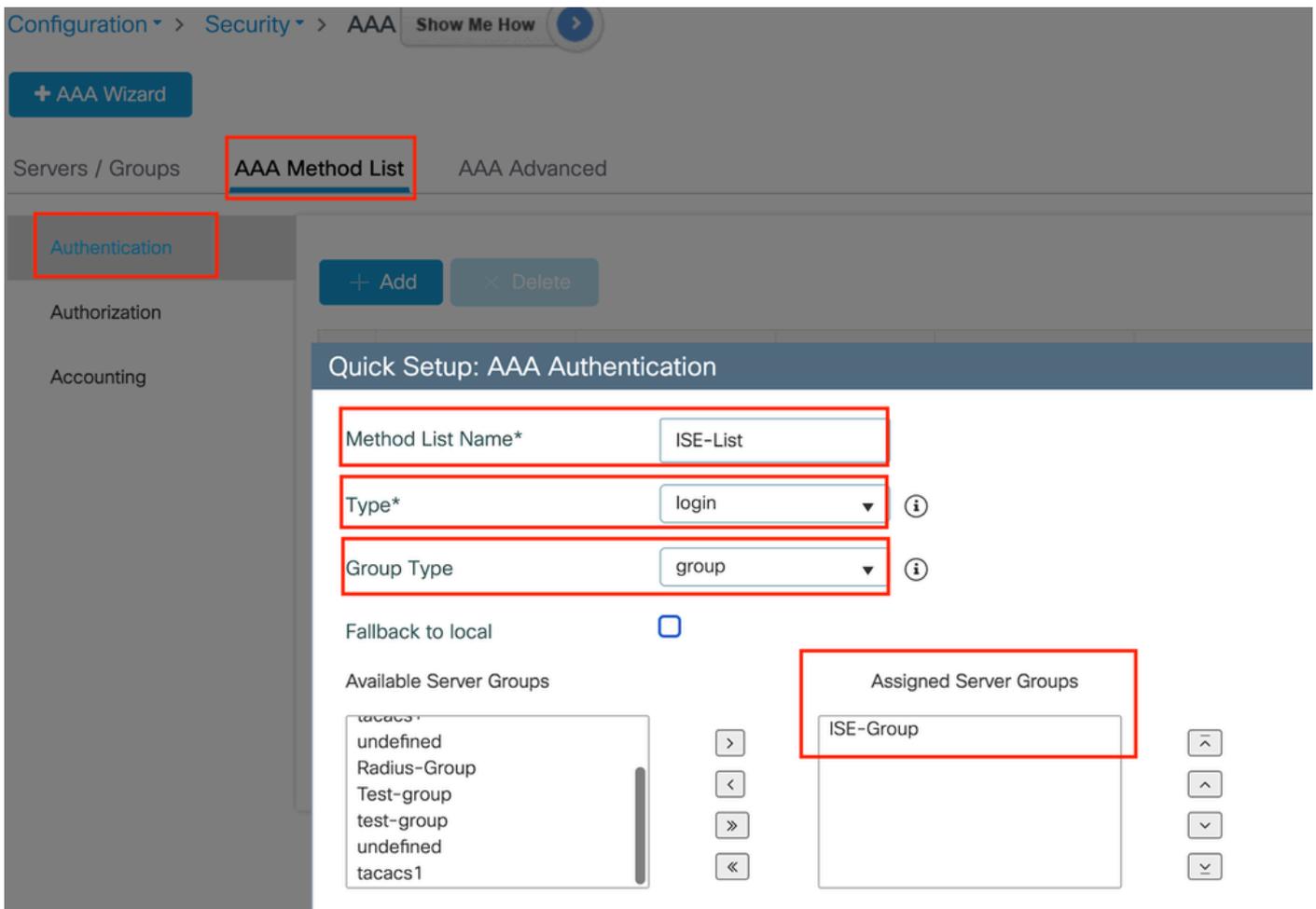
Groupe de rayons d'ancrage

### Configuration CLI

```
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2081
deadtime 5
```

Étape 3 : Configurez la liste de méthodes AAA :

Accédez à l'onglet AAA Method List, sélectionnez Add sous Authentication, définissez un nom de liste de méthodes avec le type « login » et le type de groupe « Group », et mappez le groupe de serveurs d'authentification configuré sous la section Assigned Server Group.



Liste des méthodes d'authentification

## Configuration CLI

```
aaa authentication login ISE-List group ISE-Group
```

## Configurer le profil de stratégie

Étape 1 : Accédez à Configuration > Tag & Profiles > Policy, configurez le profil de stratégie avec le même nom que sur le contrôleur étranger et activez le profil.

**General**

Access Policies

QOS and AVC

Mobility

Advanced

Name*	GuestLANPolicy
Description	Enter Description
Status	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED
IP MAC Binding	ENABLED <input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED
CTS Policy	
Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
Default SGT	2-65519

WLAN Switching Policy

Central Switching	ENABLED <input checked="" type="checkbox"/>
Central Authentication	ENABLED <input checked="" type="checkbox"/>
Central DHCP	ENABLED <input checked="" type="checkbox"/>
Flex NAT/PAT	<input type="checkbox"/> DISABLED

Profil de stratégie d'ancrage

Étape 2 : Sous Access Policies, mappez le VLAN client câblé à partir de la liste déroulante

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

### WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select

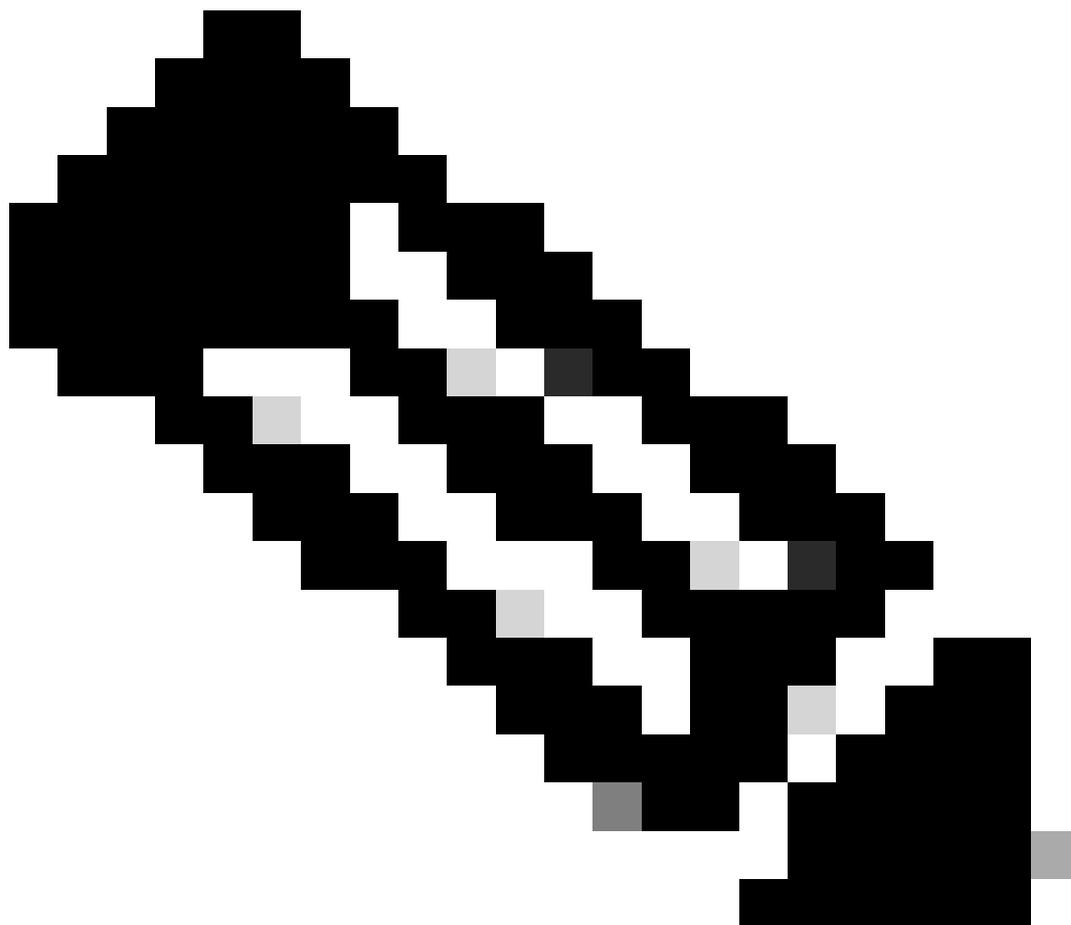


### VLAN

VLAN/VLAN Group

VLAN2024





Remarque : la configuration du profil de stratégie doit correspondre sur les contrôleurs Foreign et Anchor, à l'exception du VLAN.

---

Étape 3 : Sous l'onglet Mobility, cochez la case Export Anchor.

### Mobility Anchors

Export Anchor



Static IP Mobility



*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (2)

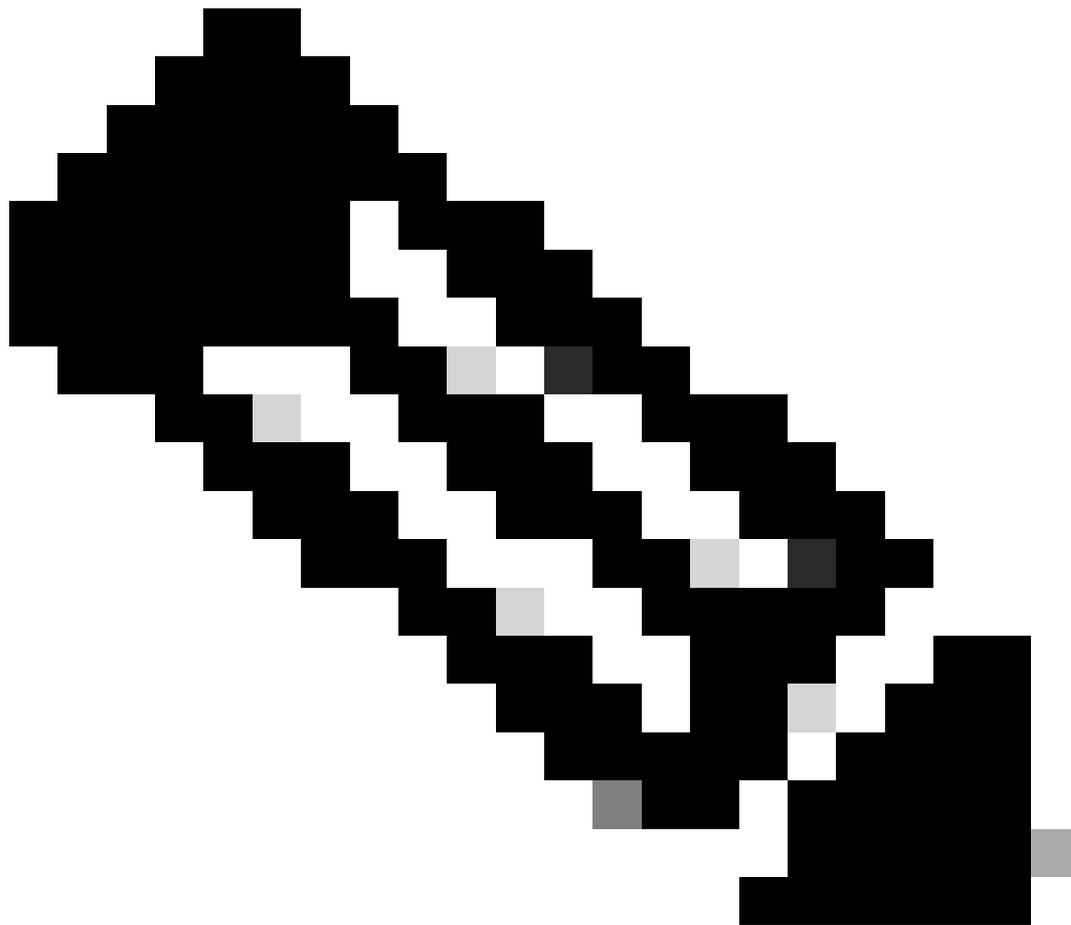
Selected (0)

Anchor IP

Anchor IP

Anchor IP

Exporter l'ancre



Remarque : cette configuration désigne le contrôleur de réseau local sans fil (WLC) 9800 comme WLC d'ancrage pour tout WLAN associé au profil de stratégie spécifié. Lorsqu'un WLC 9800 étranger redirige les clients vers le WLC d'ancrage, il fournit des détails sur le WLAN et le profil de stratégie attribué au client. Cela permet au WLC d'ancrage d'appliquer le profil de stratégie local approprié en fonction des informations reçues.

---

## Configuration CLI

```
wireless profile policy GuestLANPolicy
  mobility anchor
  vlan VLAN2024
  no shutdown
```

## Configuration du profil de réseau local invité

Étape 1 : Accédez à Configuration > Wireless > Guest LAN, puis sélectionnez Add pour créer et configurer le profil Guest LAN. Assurez-vous que le nom du profil correspond à celui du contrôleur étranger. Notez que le VLAN filaire doit être désactivé sur le contrôleur d'ancrage.

Configuration > Wireless > Guest LAN

> Guest LAN Configuration

+ Add × Delete

### Add Guest LAN Profile

**General** Security

Profile Name\*  Client Association Limit

Guest LAN ID\*  Wired VLAN Status  DISABLE

mDNS Mode

Status  ENABLE

Profil de réseau local invité

Étape 2 : Dans les paramètres de sécurité, activez Web Auth, puis configurez la carte de paramètres Web Auth et la liste d'authentification.

## Edit Guest LAN Profile

General

**Security**

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

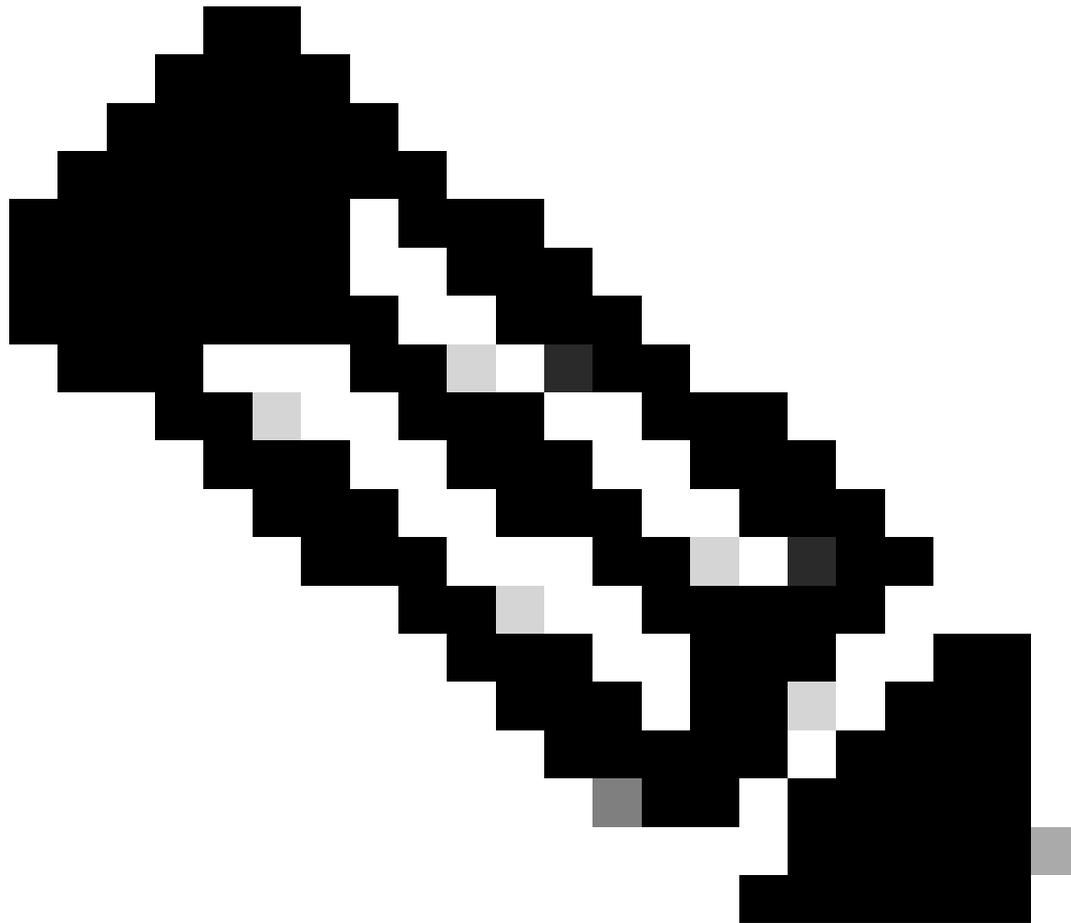
global



Authentication List

ISE-List





Remarque : la configuration du profil de réseau local invité doit être identique entre les contrôleurs Foreign et Anchor, à l'exception de l'état du réseau local virtuel câblé

---

## Configuration CLI

```
guest-lan profile-name Guest-Profile 1
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## Plan du réseau local invité

Étape 1 : Accédez à Configuration > Wireless > Guest LAN. Dans la section Configuration de la carte du réseau local invité, sélectionnez Add et mappez le profil de stratégie au profil du réseau local invité.

## > Guest LAN Map Configuration

+ Add Map   × Delete Map

Guest LAN Map : GuestMap

+ Add   × Delete

Guest LAN Profile Name	Policy Name
No records available.	
10 items per page   0 - 0 of 0 items	

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save   Cancel

Plan du réseau local invité

wireless guest-lan map GuestMap  
guest-lan Guest-Profile policy GuestLANPolicy

## Configuration d'un invité filaire sur le catalystr 9800 ancré au contrôleur AireOS 5520



Topologie du réseau

## Configuration sur le WLC 9800 étranger

## Configurer la carte de paramètres Web

Étape 1 : Accédez à Configuration > Security > Web Auth et sélectionnez Global. Vérifiez que l'adresse IP virtuelle du contrôleur et le point de confiance sont correctement mappés sur le profil, avec le type défini sur webauth.

General	Advanced		
Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3... ▼
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth ▼	Virtual IPv6 Address	x::x::x::x
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	<b>Banner Configuration</b>	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Read From File

Carte de paramètre Web

Étape 2 : Sous l'onglet Advanced, spécifiez l'URL de la page Web externe vers laquelle les clients doivent être redirigés. Configurez l'URL de redirection pour la connexion et la redirection en cas d'échec. Le paramètre Redirect On-Success est une configuration facultative.

Preview of the Redirect URL:

```
http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>
```

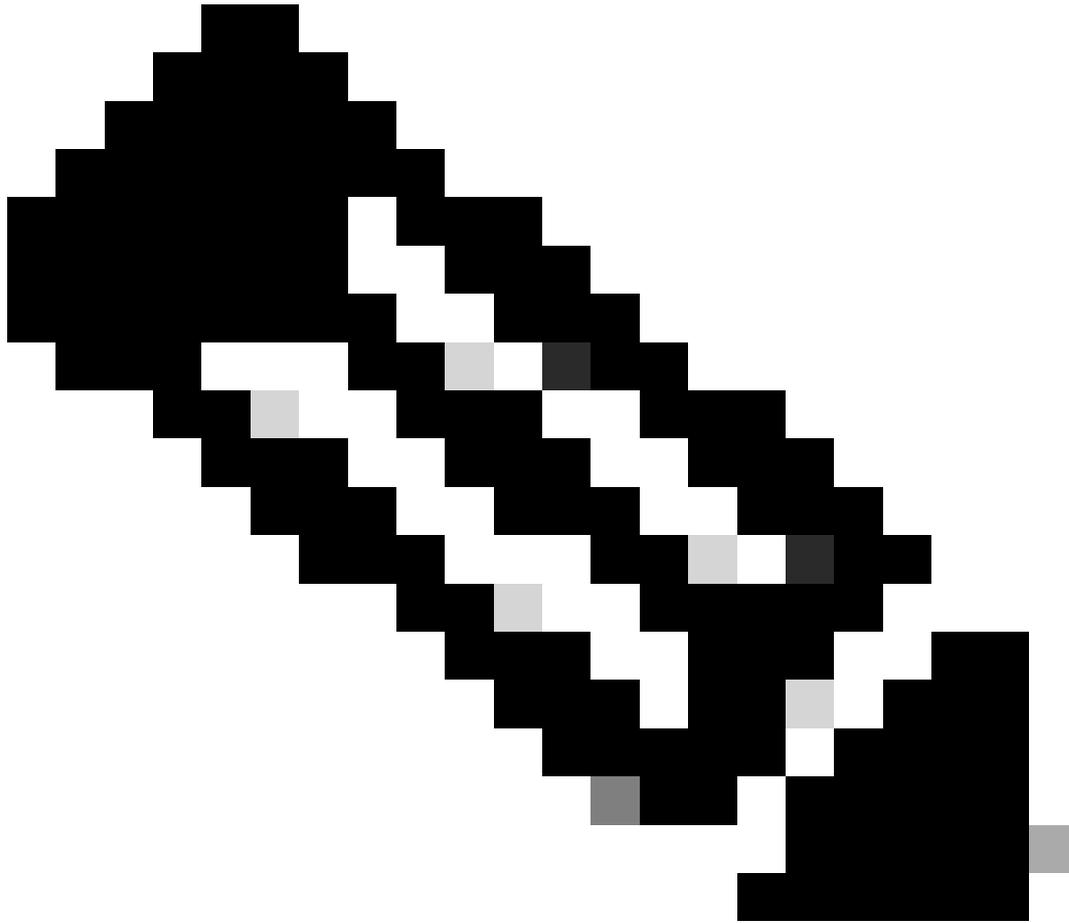
## Redirect to external server

Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X::X"/>

Onglet Avancé

## Configuration CLI

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



Remarque : pour la configuration AAA, veuillez vous reporter aux détails de configuration fournis dans la section "" pour le WLC 9800 étranger.

---

## Configurer le profil de stratégie

Étape 1 : Accédez à Configuration > Tags & Profiles > Policy. Sélectionnez Add, et dans l'onglet General, fournissez un nom pour le profil et activez le basculement d'état.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name\*

Guest

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

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

Flex NAT/PAT

DISABLED

Profil de stratégie

Étape 2 : dans l'onglet Access Policies, affectez un VLAN aléatoire.

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

1



Multicast VLAN

Enter Multicast VLAN

Politiques d'accès

Étape 3 : Dans l'onglet Mobility, activez le contrôleur d'ancrage et définissez sa priorité sur Primary (1)

### Mobility Anchors

Export Anchor



Static IP Mobility



*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

#### Available (1)

Anchor IP

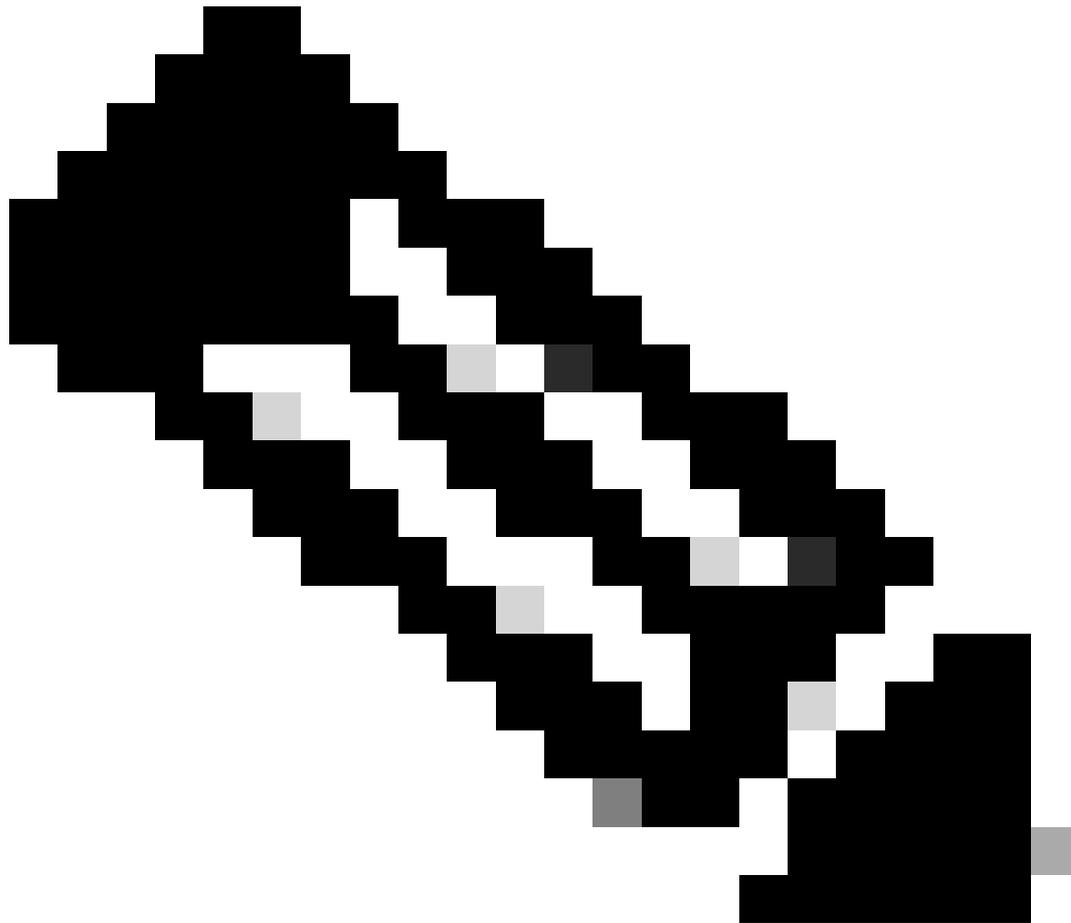
 10.76.6.156 
---

#### Selected (1)

Anchor IP

Anchor Priority

 10.76.118.74	Primary (1) 
--	---



Remarque : le profil de stratégie du WLC étranger 9800 doit correspondre au profil de réseau local invité du WLC d'ancrage 5520, à l'exception de la configuration de réseau local virtuel

---

## Configuration CLI

```
wireless profile policy Guest
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor 10.76.118.74 priority 1
no shutdown
```

## Configurer le profil de réseau local invité

Étape 1 : Accédez à Configuration > Wireless > Guest LAN et sélectionnez Add. Configurez un nom de profil unique et activez le VLAN filaire, en spécifiant l'ID de VLAN dédié aux utilisateurs invités filaires. Enfin, basculez l'état du profil sur Activé.

**General**   Security

Profile Name*	Guest	Client Association Limit	2000
Guest LAN ID*	2	Wired VLAN Status	ENABLE <input checked="" type="checkbox"/>
mDNS Mode	Bridging ▼	Wired VLAN ID*	11
Status	ENABLE <input checked="" type="checkbox"/>		

Politique de réseau local invité

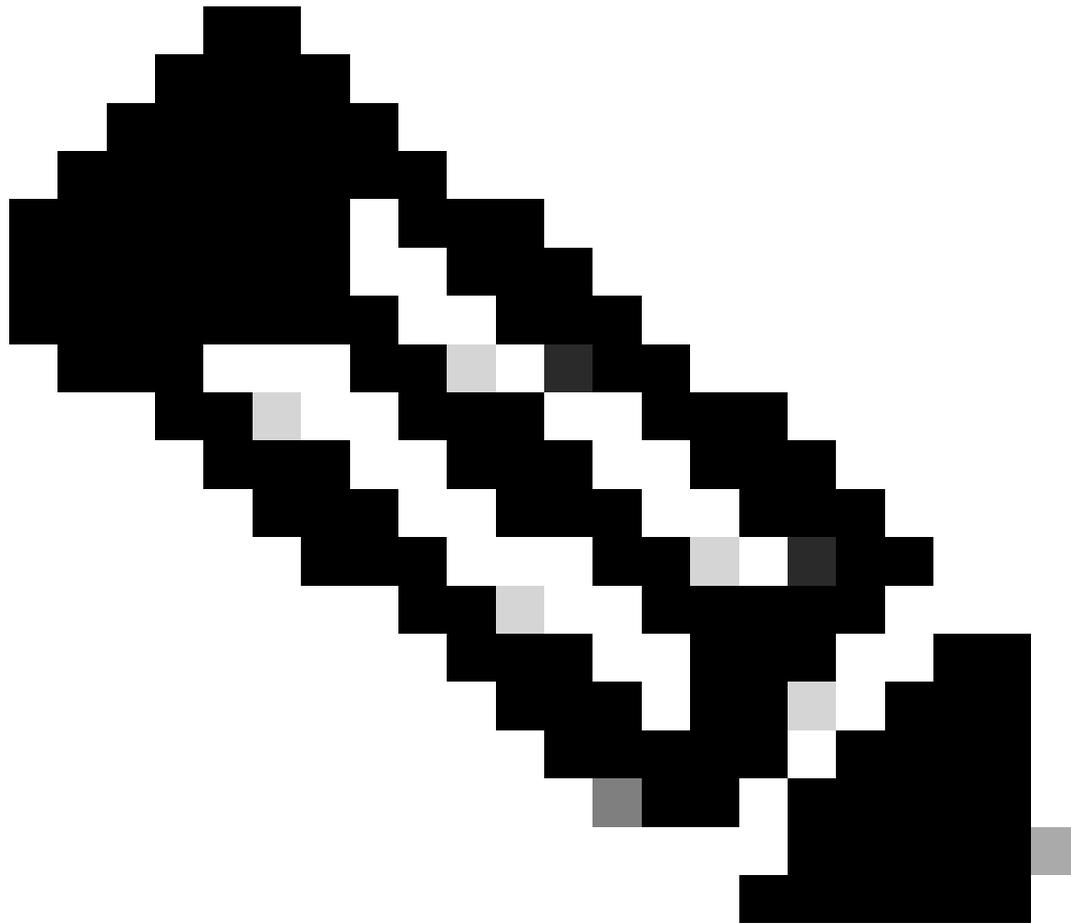
Étape 2 : Sous l'onglet Security, activez Web Auth, mappez la carte de paramètres Web Auth et sélectionnez le serveur RADIUS dans la liste déroulante Authentication.

**General**   **Security**

Layer3

Web Auth	ENABLE <input checked="" type="checkbox"/>
Web Auth Parameter Map	global ▼
Authentication List	ISE-List ▼

Onglet Sécurité



Remarque : le nom du profil de réseau local invité doit être identique pour le contrôleur d'ancrage 9800 étranger et 5520

---

## Configuration CLI

```
guest-lan profile-name Guest 2 wired-vlan 11
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## Plan du réseau local invité

Étape 1 : Accédez à Configuration > Wireless > Guest LAN. Dans la section de configuration Guest LAN MAP, sélectionnez Add et mappez le profil de stratégie au profil de réseau local invité.

## Guest LAN Map Configuration

+ Add Map    × Delete Map

Guest LAN Map : GuestMap

+ Add    × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page    0 - 0 of 0 items

Profile Name: Guest

Policy Name: Guest

Save    Cancel

Plan du réseau local invité

### Configuration CLI

```
wireless guest-lan map GuestMap  
guest-lan Guest policy Guest
```

## Configuration sur le WLC Anchor 5520

### Configurer l'authentification Web

Étape 1 : Accédez à Security > Web Auth > Web Login Page. Définissez le type d'authentification Web sur External (Redirect to external server) et configurez l'URL d'authentification Web externe. L'URL de redirection après la connexion est facultative et peut être configurée si les clients doivent être redirigés vers une page dédiée après une authentification réussie.

The screenshot shows the Cisco WLC configuration interface. The 'SECURITY' tab is selected in the top navigation bar. In the left sidebar, 'Web Auth' is expanded, and 'Web Login Page' is selected. The main configuration area shows the 'Web Login Page' settings. The 'Web Authentication Type' is set to 'External (Redirect to external server)'. The 'Redirect URL after login' is 'http://10.127.196.171/webauth/logout.html'. The 'Login Success Page Type' is 'None'. The 'External Webauth URL' is 'http://10.127.196.171/webauth/login.html'. There are 'Preview...' and 'Apply' buttons at the bottom right of the configuration area.

Paramètres d'authentification Web

## Paramètres AAA :

### Étape 1 : configurez le serveur RADIUS

Accédez à Security > Radius > Authentication > New.



### Serveur Radius

Étape 2 : Configurez l'adresse IP du serveur RADIUS et le secret partagé sur le contrôleur. Activez l'état du serveur sur Enabled et cochez la case Network User.

## RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Configuration du serveur

### Configurer la liste de contrôle d'accès

Étape 1 : Accédez à Sécurité > Liste de contrôle d'accès et sélectionnez Nouveau. Créez une liste

de contrôle d'accès de pré-authentification qui autorise le trafic vers DNS et le serveur Web externe.

The screenshot shows the Cisco ISE Security configuration page for 'Access Control Lists > Edit'. The 'SECURITY' tab is highlighted in the top navigation bar. The left sidebar shows the 'Access Control Lists' menu item highlighted. The main content area displays the 'General' configuration for the 'Pre-Auth\_ACL' list, showing 'Deny Counters' set to 0. Below this is a table of rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

Liste d'accès pour autoriser le trafic vers le serveur Web

## Configurer le profil de réseau local invité

Étape 1 : Accédez à WLANs > sélectionnez Create New .

Sélectionnez Type comme Guest LAN et configurez le même nom que le profil de stratégie du contrôleur étranger 9800.

The screenshot shows the Cisco ISE WLANs configuration page. The 'WLANs' tab is highlighted in the top navigation bar. The 'Create New' button is highlighted with a red box. Below the navigation bar, the 'Current Filter' is set to 'None'. The table below shows the columns for 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'.

Créer un réseau local invité

The screenshot shows the Cisco ISE 'WLANs > New' configuration page. The 'Type' dropdown is set to 'Guest LAN' and is highlighted with a red box. The 'Profile Name' is set to 'Guest' and the 'ID' is set to '2'. The 'Apply' button is highlighted with a red box.

Profil de réseau local invité

Étape 2 : mappez les interfaces d'entrée et de sortie sur le profil de réseau local invité.

Dans ce cas, l'interface d'entrée est none, car elle correspond au tunnel EoIP du contrôleur étranger.

L'interface de sortie est le VLAN auquel le client filaire se connecte physiquement .

**General** **Security** **QoS** **Advanced**

Profile Name: Guest

Type: Guest LAN

Status:  Enabled

Security Policies: **Web-Auth**  
(Modifications done under security tab will appear after applying the changes.)

Ingress Interface: None

Egress Interface: wired-vlan-11

NAS-ID: none

Profil de réseau local invité

Étape 3 : Sous l'onglet Security, sélectionnez Layer 3 security as Web Authentication et mappez la liste de contrôle d'accès de pré-authentification.

## WLANs > Edit 'Guest'

**General** **Security** **QoS** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Layer 3 Security: Web Authentication

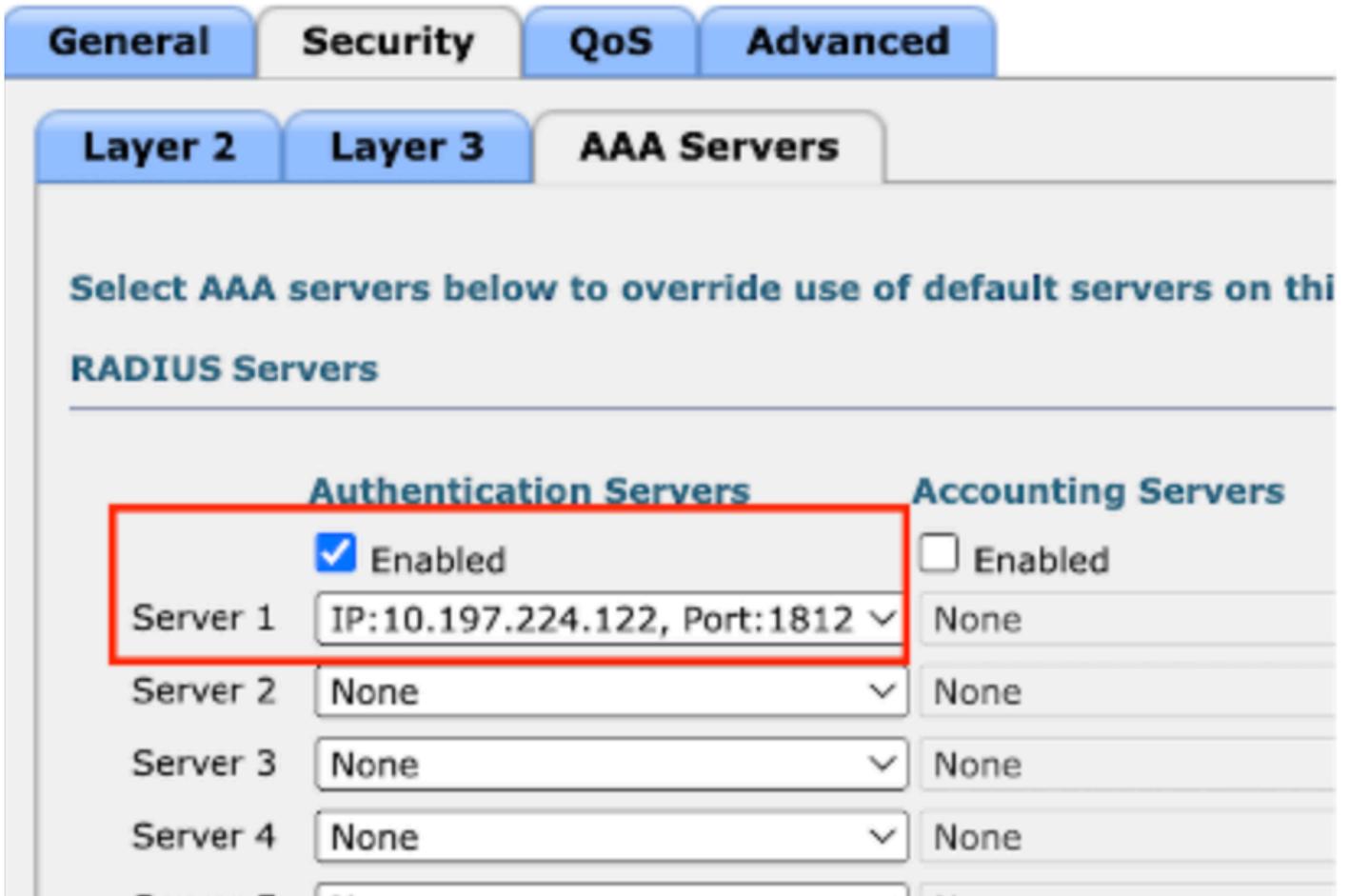
Preauthentication ACL: IPv4 Pre-Auth\_ACL IPv6 None

Override Global Config<sup>20</sup>:  Enable

Onglet Sécurité du réseau local invité

Étape 4 : Accédez à Security > AAA Server.

Sélectionnez la liste déroulante et mappez le serveur RADIUS au profil de réseau local invité.



Mappage du serveur RADIUS au profil LAN invité

Étape 5 : Accédez à WLAN. Passez le curseur sur l'icône déroulante du profil de réseau local invité et sélectionnez Ancres de mobilité.



Étape 6 : Sélectionnez Mobility Anchor Create pour configurer le contrôleur en tant qu'ancrage d'exportation pour ce profil de réseau local invité.



Création d'ancrage de mobilité

Configuration d'un invité filaire sur AireOS 5520 ancré à catalystr 9800



Topologie du réseau

## Configuration sur le WLC étranger 5520

### Configuration d'interface contrôleur

Étape 1 : Accédez à Controller > Interfaces > New. Configurez un nom d'interface, un ID de VLAN et activez le réseau local invité.

Un invité filaire nécessite deux interfaces dynamiques.

Commencez par créer une interface dynamique de couche 2 et désignez-la comme réseau local invité. Cette interface sert d'interface d'entrée pour le réseau local invité, où les clients filaires se connectent physiquement.

The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANA'. The left sidebar lists various configuration categories, with 'Interfaces' highlighted in red. The main content area is titled 'Interfaces > Edit' and is divided into several sections:

- General Information:** Interface Name is 'wired-guest' (highlighted in red), and MAC Address is 'a0:e0:af:32:d9:ba'.
- Configuration:** 'Guest Lan' is checked (highlighted in red), and NAS-ID is 'none'.
- Physical Information:** Port Number is '1', Backup Port is '0', and Active Port is '1'.
- Interface Address:** VLAN Identifier is '2020' (highlighted in red), DHCP Proxy Mode is 'Global', and 'Enable DHCP Option 82' is unchecked.

Interface d'entrée

Étape 2 : Accédez à Controller > Interfaces > New. Configurez un nom d'interface, ID de VLAN.

La deuxième interface dynamique doit être une interface de couche 3 sur le contrôleur, les clients filaires reçoivent l'adresse IP de ce sous-réseau VLAN. Cette interface sert d'interface de sortie pour le profil de réseau local invité.

**Controller**

**Interfaces > Edit**

**General Information**

Interface Name	vlan2024
MAC Address	a0:e0:af:32:d9:ba

**Configuration**

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0
NAS-ID	none

**Physical Information**

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input type="checkbox"/>

**Interface Address**

VLAN Identifier	2024
IP Address	10.105.211.85
Netmask	255.255.255.128
Gateway	10.105.211.1

Interface de sortie

## Configuration du port de commutateur

Les utilisateurs invités filaires se connectent au commutateur de couche d'accès, ces ports désignés doivent être configurés avec le VLAN dans lequel le LAN invité est activé sur le contrôleur

Configuration du port du commutateur de couche accès

interface GigabitEthernet <x/x/x>

description Accès invité filaire

switchport access vlan 2020

switchport mode access

tranche

Configuration du port de liaison ascendante du contrôleur étranger

interface TenGigabitEthernet<x/x/x>

description Port agrégé vers le WLC étranger

switchport mode trunk

switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2020

tranche

Configuration du port de liaison ascendante du contrôleur d'ancrage

interface TenGigabitEthernet<x/x/x>

description Port trunk vers le WLC d'ancrage

switchport mode trunk

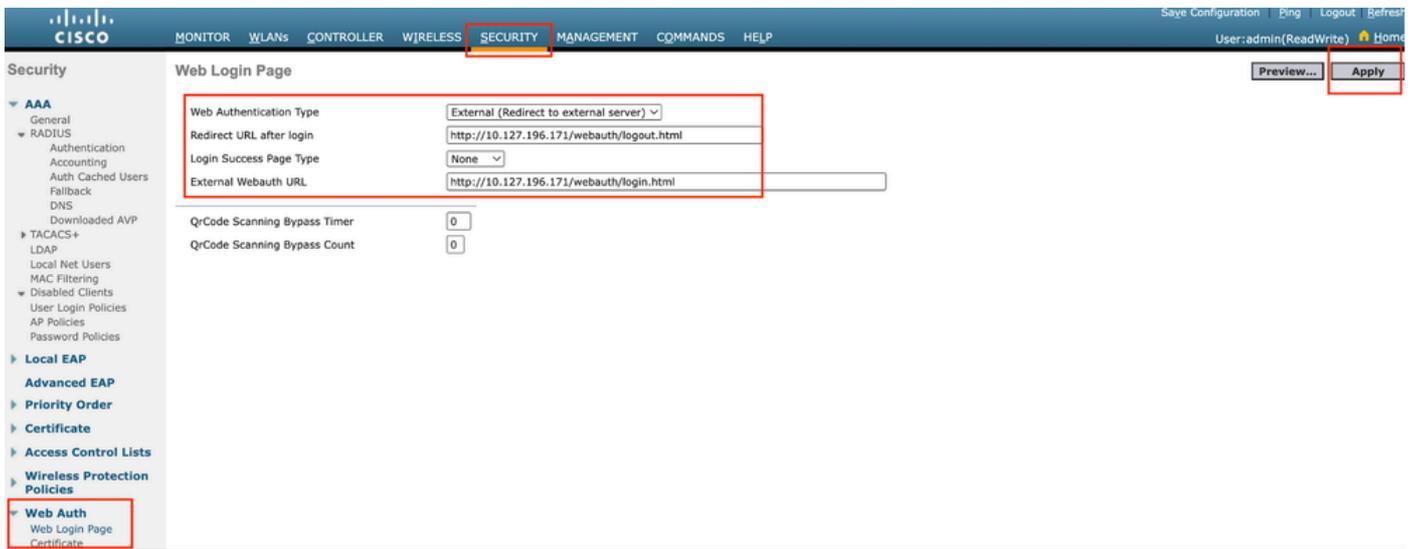
switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2024

tranche

## Configurer l'authentification Web

Étape 1 : Accédez à Security > Web Auth > Web Login Page. Définissez le type d'authentification Web sur External (Redirect to external server) et configurez l'URL d'authentification Web externe. L'URL de redirection après la connexion est facultative et peut être configurée si les clients doivent être redirigés vers une page dédiée après une authentification réussie.



Paramètres d'authentification Web

## Paramètres AAA :

Étape 1 : configurez le serveur RADIUS

Accédez à Security > Radius > Authentication > New.



Serveur Radius

Étape 2 : Configurez l'adresse IP du serveur RADIUS et le secret partagé sur le contrôleur. Activez l'état du serveur sur Enabled et cochez la case Network User.

## RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Configuration du serveur

### Configurer la liste de contrôle d'accès

Étape 1 : Accédez à Sécurité > Liste de contrôle d'accès et sélectionnez Nouveau. Créez une liste

de contrôle d'accès de pré-authentification qui autorise le trafic vers DNS et le serveur Web externe.

The screenshot shows the Cisco Security configuration interface. The 'SECURITY' tab is highlighted in the top navigation bar. On the left sidebar, 'Access Control Lists' is selected. The main content area is titled 'Access Control Lists > Edit' and shows the 'General' tab for an ACL named 'Pre-Auth\_ACL'. The 'Deny Counters' are set to 0. Below this is a table of ACL entries:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

Liste d'accès pour autoriser le trafic vers le serveur Web

## Configurer le profil de réseau local invité

Étape 1 : Accédez à WLAN > Create New > Go.

The screenshot shows the Cisco WLAN configuration interface. The 'WLANs' tab is highlighted in the top navigation bar. Below the navigation bar, there is a 'Current Filter: None' section with links for '[Change Filter]' and '[Clear Filter]'. To the right, there is a 'Create New' dropdown menu and a 'Go' button. Below this is a table header for WLANs:

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
--------------------------	---------	------	--------------	-----------	--------------	-------------------

Profil de réseau local invité

Sélectionnez Type en tant que réseau local invité et configurez un nom de profil. Le même nom doit être configuré sur le profil de stratégie et le profil de réseau local invité du contrôleur d'ancrage 9800.

## WLANs > New

Type

Guest LAN

Profile Name

Guest-Profile

ID

3

Profil de réseau local invité

Étape 2 : sous l'onglet Général, mappez l'interface d'entrée et de sortie sur le profil de réseau local invité.

L'interface d'entrée est le VLAN auquel les clients câblés se connectent physiquement.

L'interface de sortie est le sous-réseau VLAN que les clients demandent pour l'adresse IP.

General	Security	QoS	Advanced
Profile Name	Guest-Profile		
Type	Guest LAN		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	<b>Web-Auth</b> (Modifications done under security tab will appear after applying th		
Ingress Interface	wired-guest		
Egress Interface	vlan2024		
NAS-ID	none		

Profil de réseau local invité

Étape 3 : Accédez à Security > Layer 3.

Sélectionnez Layer 3 Security comme Web Authentication et mappez la liste de contrôle d'accès

de pré-authentification.

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security

Preauthentication ACL IPv4 Pre-Auth\_ACL IPv6 None

Override Global Config<sup>20</sup>  Enable

Web Authentication

Onglet Sécurité de couche 3

Étape 4 :

Sous l'onglet AAA servers, mappez le serveur Radius et cochez la case Enabled.

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on the

**RADIUS Servers**

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.197.224.122, Port:1812	<input type="checkbox"/> Enabled None
Server 2	None	None
Server 3	None	None
Server 4	None	None

Mappage des serveurs RADIUS sur le profil de réseau local invité

Étape 5 : Accédez à la page WLAN et passez le curseur sur l'icône descendante du profil Guest LAN et sélectionnez Mobility Anchors.

<input type="checkbox"/>	30	WLAN	guest-1665	guest-1665	Disabled	[WPA + WPA2][Auth(PSK)]	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1	Guest LAN	Guest-Profile	---	Enabled	Web-Auth	<input type="button" value="Remove"/> <input type="button" value="Mobility Anchors"/>
<input type="checkbox"/>	2	Guest LAN	Guest	---	Disabled	Web-Auth	

Ancres de mobilité

Étape 6 : Mappez l'ancre de mobilité de la liste déroulante au profil de réseau local invité.

### Mobility Anchors

WLAN SSID Guest-Profile

Switch IP Address (Anchor) Data Path Co

local  
 10.106.39.41  
 10.76.6.156  
 10.76.118.70

Switch IP Address (Anchor)

**Foot Notes**

Mappage de l'ancre de mobilité au LAN invité

## Configuration sur le WLC Anchor 9800

### Configurer la carte de paramètres Web

Étape 1 : Accédez à Configuration > Security > Web Auth et sélectionnez Global. Vérifiez que l'adresse IP virtuelle du contrôleur et le point de confiance sont correctement mappés sur le profil, avec le type défini sur webauth.

**General**

## Advanced

Parameter-map Name	<input type="text" value="global"/>
Maximum HTTP connections	<input type="text" value="100"/>
Init-State Timeout(secs)	<input type="text" value="120"/>
Type	<input type="text" value="webauth"/>
Captive Bypass Portal	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>
Sleeping Client Status	<input type="checkbox"/>
Sleeping Client Timeout (minutes)	<input type="text" value="720"/>

Virtual IPv4 Address	<input type="text" value="192.0.2.1"/>
Trustpoint	<input type="text" value="TP-self-signed-3..."/>
Virtual IPv4 Hostname	<input type="text"/>
Virtual IPv6 Address	<input type="text" value=":::~::~"/>
Web Auth intercept HTTPs	<input type="checkbox"/>
Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable HTTP secure server for Web Auth	<input type="checkbox"/>

**Banner Configuration**

Banner Title	<input type="text"/>
Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Read From File

Carte de paramètre Web

Étape 2 : Sous l'onglet Advanced, spécifiez l'URL de la page Web externe vers laquelle les clients doivent être redirigés. Configurez l'URL de redirection pour la connexion et la redirection en cas d'échec. Le paramètre Redirect On-Success est une configuration facultative.

Preview of the Redirect URL:

```
http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>
```

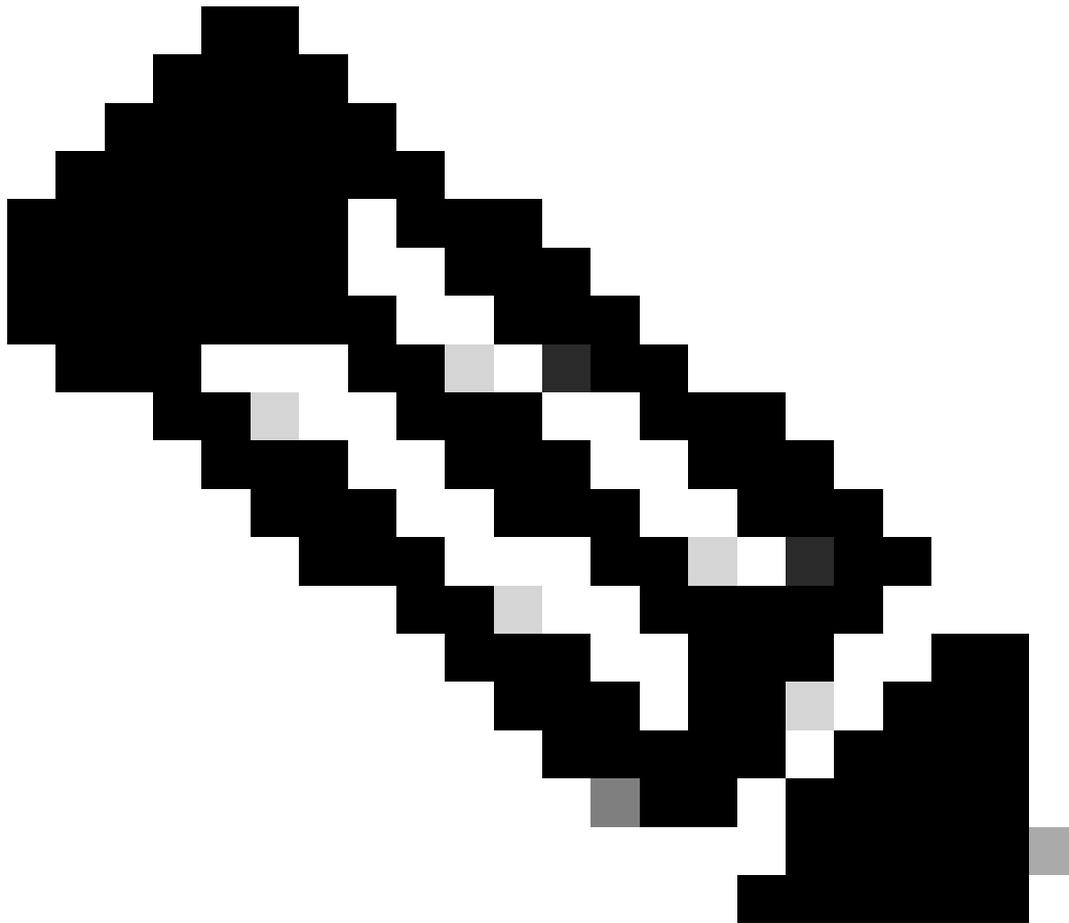
## Redirect to external server

Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X::X"/>

Onglet Avancé

## Configuration CLI

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



Remarque : pour la configuration AAA, reportez-vous aux détails de configuration fournis dans la section « Configurer un invité filaire sur un catalyst 9800 ancré à un autre catalyst 9800 » pour le WLC 9800 étranger.

---

## Configurer le profil de stratégie

Étape 1 : Accédez à Configuration > Tags & Profiles > Policy. Configurez le profil de stratégie avec le même nom que celui utilisé pour le profil de réseau local invité du contrôleur étranger.

**General**

Access Policies

QOS and AVC

Mobility

Advanced

Name\*

Description

Status  ENABLED

Passive Client  DISABLED

IP MAC Binding  ENABLED

Encrypted Traffic Analytics  DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching  ENABLED

Central Authentication  ENABLED

Central DHCP  ENABLED

Flex NAT/PAT  DISABLED

Profil de stratégie

Étape 2 : Sous l'onglet Access Policies, mappez le VLAN client filaire dans la liste déroulante

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

VLAN2024



Multicast VLAN

Enter Multicast VLAN

Politiques d'accès

Étape 3 : Sous l'onglet Mobility, cochez la case Export Anchor.

**Mobility Anchors**

Export Anchor



Static IP Mobility



*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

Onglet Mobilité

### Configuration CLI

```
wireless profile policy Guest-Profile
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor
vlan VLAN2024
no shutdown
```

### Configurer le profil de réseau local invité

Étape 1 : Accédez à Configuration > Wireless > Guest LAN et sélectionnez Add pour configurer le profil Guest LAN et désactiver l'état du VLAN filaire.

Le nom du profil de réseau local invité sur l'ancre doit être identique au profil de réseau local invité sur le WLC étranger.

Profile Name*	Guest-Profile	Client Association Limit	2000
Guest LAN ID*	1	Wired VLAN Status	<input type="checkbox"/> DISABLE
mDNS Mode	Bridging		
Status	ENABLE <input checked="" type="checkbox"/>		

Profil de réseau local invité

Étape 2 : Sous l'onglet Security, activez Web Auth. Sélectionnez la carte de paramètres Web Auth et la liste d'authentification dans la liste déroulante

## Edit Guest LAN Profile

### Layer3

Web Auth	ENABLE <input checked="" type="checkbox"/>
Web Auth Parameter Map	global
Authentication List	ISE-List

Onglet Sécurité LAN invité

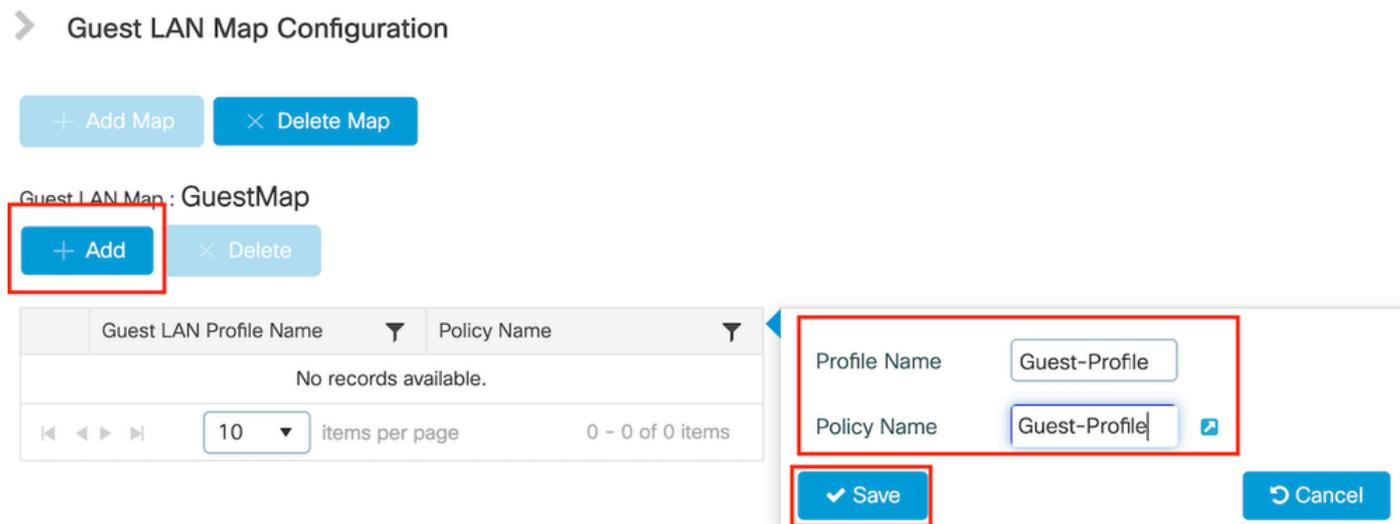
### Configuration CLI

```
guest-lan profile-name Guest-Profile 1
```

```
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## Plan du réseau local invité

Étape 1 : Accédez à Configuration > Wireless > Guest LAN. Dans la section de configuration Guest LAN MAP, sélectionnez Add et mappez le profil de stratégie au profil de réseau local invité.



Plan du réseau local invité

## Vérifier

Valider la configuration du contrôleur

```
#show résumé guest-lan
```

GLAN	GLAN Profile Name	Status
1	Guest-Profile	UP
2	Guest	UP

```
#show guest-lan id 1
```

```
<#root>
```

```
Guest-LAN Profile Name      : Guest
=====
Guest-LAN ID                : 2
Wired-Vlan                  :
11
Status                      :
```

**Enabled**

Number of Active Clients : 0  
Max Associated Clients : 2000  
Security  
    WebAuth :

**Enabled**

    Webauth Parameter Map : global  
    Webauth Authentication List :

**ISE-List**

    Webauth Authorization List : Not configured  
mDNS Gateway Status : Bridge

#show parameter-map type webauth global

<#root>

Parameter Map Name : global  
Type :

**webauth**

Redirect:  
    For Login :

http://10.127.196.171/webauth/login.html

    On Success :

http://10.127.196.171/webauth/logout.html

    On Failure :

http://10.127.196.171/webauth/failed.html

    Portal ipv4 :

10.127.196.171

        Virtual-ipv4 :

192.0.2.1

#show parameter-map type webauth name <profile name> (Si le profil de paramètre Web personnalisé est utilisé)

Récapitulatif de #show wireless guest-lan-map

GLAN Profile Name	Policy Name
-----	-----
Guest	Guest

## Résumé de la mobilité sans fil #show

IP	Public Ip	MAC Address
10.76.118.70	10.76.118.70	f4bd.9e59.314b

### #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 secure server capability: Present  
HTTP secure server status: Enabled  
HTTP secure server port: 443  
HTTP secure server trustpoint: TP-self-signed-3010594951

### >show guest-lan summary

Number of Guest LANs..... 1

GLAN ID	GLAN Profile Name	Status	Interface Name
2	Guest	Enabled	wired-vlan-11

### >show guest-lan 2

Guest LAN Identifier..... 2  
Profile Name..... Guest  
Status..... Enabled  
Interface..... wired-vlan-11

Radius Servers  
  Authentication..... 10.197.224.122 1812 \*  
  Web Based Authentication..... Enabled  
  Web Authentication Timeout..... 300  
  IPv4 ACL..... Pre-Auth\_ACL

    Mobility Anchor List

GLAN ID	IP Address	Status
2	10.76.118.74	Up

>show custom-web all

```
Radius Authentication Method..... PAP
Cisco Logo..... Enabled
CustomLogo..... None
Custom Title..... None
Custom Message..... None
Custom Redirect URL..... http://10.127.196.171/webauth/logout.html
Web Authentication Login Success Page Mode..... None
Web Authentication Type..... External
Logout-popup..... Enabled
External Web Authentication URL..... http://10.127.196.171/webauth/login.html
QR Code Scanning Bypass Timer..... 0
QR Code Scanning Bypass Count..... 0
```

>show custom-web guest-lan 2

```
Guest LAN Status..... Enabled
Web Security Policy..... Web Based Authentication
WebAuth Type..... External
Global Status..... Enabled
```

Valider l'état de stratégie client

Sur Étranger,

Récapitulatif du client sans fil #show

L'état du gestionnaire de stratégies client sur le contrôleur étranger est EXÉCUTÉ une fois que le client s'est associé avec succès.

<#root>

MAC Address	AP Name	Type ID	State	Protocol Meth
a0ce.c8c3.a9b5	N/A			

GLAN 1

Run

802.3

Web Auth

Export Foreign

>show client detail a0ce.c8c3.a9b5

<#root>

```

Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username ..... N/A
Client Webauth Username ..... N/A
Client State..... Associated
User Authenticated by ..... None
Client User Group.....
Client NAC OOB State..... Access
guest-lan..... 1
Wireless LAN Profile Name..... Guest-Profile
Mobility State.....

```

**Export Foreign**

```

Mobility Anchor IP Address.....
10.76.118.70

```

Security Policy Completed.....

**Yes**

Policy Manager State.....

**RUN**

```

Pre-auth IPv4 ACL Name..... Pre-Auth_ACL
EAP Type..... Unknown
Interface.....

```

**wired-guest-egress**

```

VLAN..... 2024
Quarantine VLAN..... 0

```

Sur l'ancre,

La transition d'état du client doit être surveillée sur le contrôleur d'ancrage.

L'état du gestionnaire de stratégie client est en attente d'authentification Web .

<#root>

MAC Address	AP Name	Type ID	State	Protocol Meth
a0ce.c8c3.a9b5	10.76.6.156			

**GLAN 1**

Webauth Pending

802.3

Web Auth

**Export Anchor**

Une fois le client authentifié, l'état du gestionnaire de stratégies passe à l'état EXÉCUTÉ.

MAC Address	AP Name	Type ID	State	Protocol	Method
a0ce.c8c3.a9b5	10.76.6.156	GLAN 1	Run	802.3	Web

#show adresse MAC du client sans fil a0ce.c8c3.a9b5 detail

<#root>

Client MAC Address : a0ce.c8c3.a9b5  
Client MAC Type : Universally Administered Address  
Client DUID: NA  
Client IPv4 Address :

10.105.211.69

Client State : Associated  
Policy Profile : Guest-Profile  
Flex Profile : N/A  
Guest Lan:  
GLAN Id: 1  
GLAN Name: Guest-Profile

Mobility:

Foreign IP Address :

10.76.118.74

Point of Attachment : 0xA0000003  
Point of Presence : 0  
Move Count : 1  
Mobility Role :

Export Anchor

Mobility Roam Type :

L3 Requested

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 35 seconds

VLAN : VLAN2024

Session Manager:

Point of Attachment : mobility\_a0000003  
IIF ID : 0xA0000003  
Authorized : FALSE  
Session timeout : 28800  
Common Session ID: 4a764c0a0000008ea0285466

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State :

Login

Webauth Method :

Webauth

Server Policies:

Resultant Policies:

URL Redirect ACL :

WA-v4-int-10.127.196.171

Preauth ACL :

WA-sec-10.127.196.171

VLAN Name : VLAN2024

VLAN :

2024

Absolute-Timer : 28800

Le client passe à l'état EXÉCUTÉ après une authentification Web réussie.

show wireless client mac-address a0ce.c8c3.a9b5 detail

<#root>

Client MAC Address : a0ce.c8c3.a9b5

Client MAC Type : Universally Administered Address

Client DUID: NA

Client IPv4 Address :

10.105.211.69

Client Username :

testuser

Client State : Associated

Policy Profile : Guest-Profile

Flex Profile : N/A

Guest Lan:

GLAN Id: 1

GLAN Name: Guest-Profile

Wireless LAN Network Name (SSID) : N/A

BSSID : N/A

Connected For : 81 seconds

Protocol : 802.3

Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 81 seconds

VLAN : VLAN2024

Last Tried Aaa Server Details:

Server IP :

10.197.224.122

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Resultant Policies:

URL Redirect ACL :

IP-Adm-V4-LOGOUT-ACL

VLAN Name : VLAN2024

VLAN :

2024

Absolute-Timer : 28800

>show client detail a0:ce:c8:c3:a9:b5

<#root>

Client MAC Address..... a0:ce:c8:c3:a9:b5  
Client Username ..... N/A  
Client Webauth Username ..... N/A  
Client State..... Associated  
Wireless LAN Profile Name..... Guest  
WLAN Profile check for roaming..... Disabled  
Hotspot (802.11u)..... Not Supported  
Connected For ..... 90 secs  
IP Address..... 10.105.211.75  
Gateway Address..... 10.105.211.1  
Netmask..... 255.255.255.128  
Mobility State.....

Export Anchor

Mobility Foreign IP Address.....

10.76.118.70

Security Policy Completed..... No

Policy Manager State.....

WEBAUTH\_REQD

Pre-auth IPv4 ACL Name.....

Pre-Auth\_ACLPre-auth

IPv4 ACL Applied Status..... Yes  
Pre-auth IPv4 ACL Applied Status.....

Yes

Après l'authentification, le client passe à l'état EXÉCUTÉ.

<#root>

show client detail a0:ce:c8:c3:a9:b5  
Client MAC Address..... a0:ce:c8:c3:a9:b5  
Client Username .....

testuser

Client Webauth Username .....

testuser

Client State.....

Associated

User Authenticated by .....

RADIUS Server

Client User Group..... testuser  
Client NAC OOB State..... Access  
Connected For ..... 37 secs  
IP Address.....

10.105.211.75

Gateway Address..... 10.105.211.1  
Netmask..... 255.255.255.128  
Mobility State.....

Export Anchor

Mobility Foreign IP Address..... 10.76.118.70  
Security Policy Completed..... Yes  
Policy Manager State.....

RUN

Pre-auth IPv4 ACL Name..... Pre-Auth\_ACL  
Pre-auth IPv4 ACL Applied Status..... Yes  
EAP Type..... Unknown  
Interface.....

wired-vlan-11

VLAN.....

11

Quarantine VLAN..... 0

# Dépannage

## Débogage du contrôleur AireOS

Activer le débogage client

```
>debug client <H.H.H>
```

Pour vérifier si le débogage est activé

```
>show debugging
```

Pour désactiver le débogage

```
debug disable-all
```

## 9800 Trace radioactive

Activez Radio Active Tracing pour générer des traces de débogage client pour l'adresse MAC spécifiée dans l'interface de ligne de commande.

Étapes pour activer le suivi radioactif :

Vérifiez que tous les débogages conditionnels sont désactivés.

```
clear platform condition all
```

Activer le débogage pour l'adresse MAC spécifiée.

```
debug wireless mac <H.H.H> monitor-time <Time in seconds>
```

Après avoir reproduit le problème, désactivez le débogage pour arrêter la collection de traces RA.

```
no debug wireless mac <H.H.H>
```

Une fois la trace RA arrêtée, le fichier de débogage est généré dans le bootflash du contrôleur.

```
show bootflash: | include ra_trace  
2728          179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Da
```

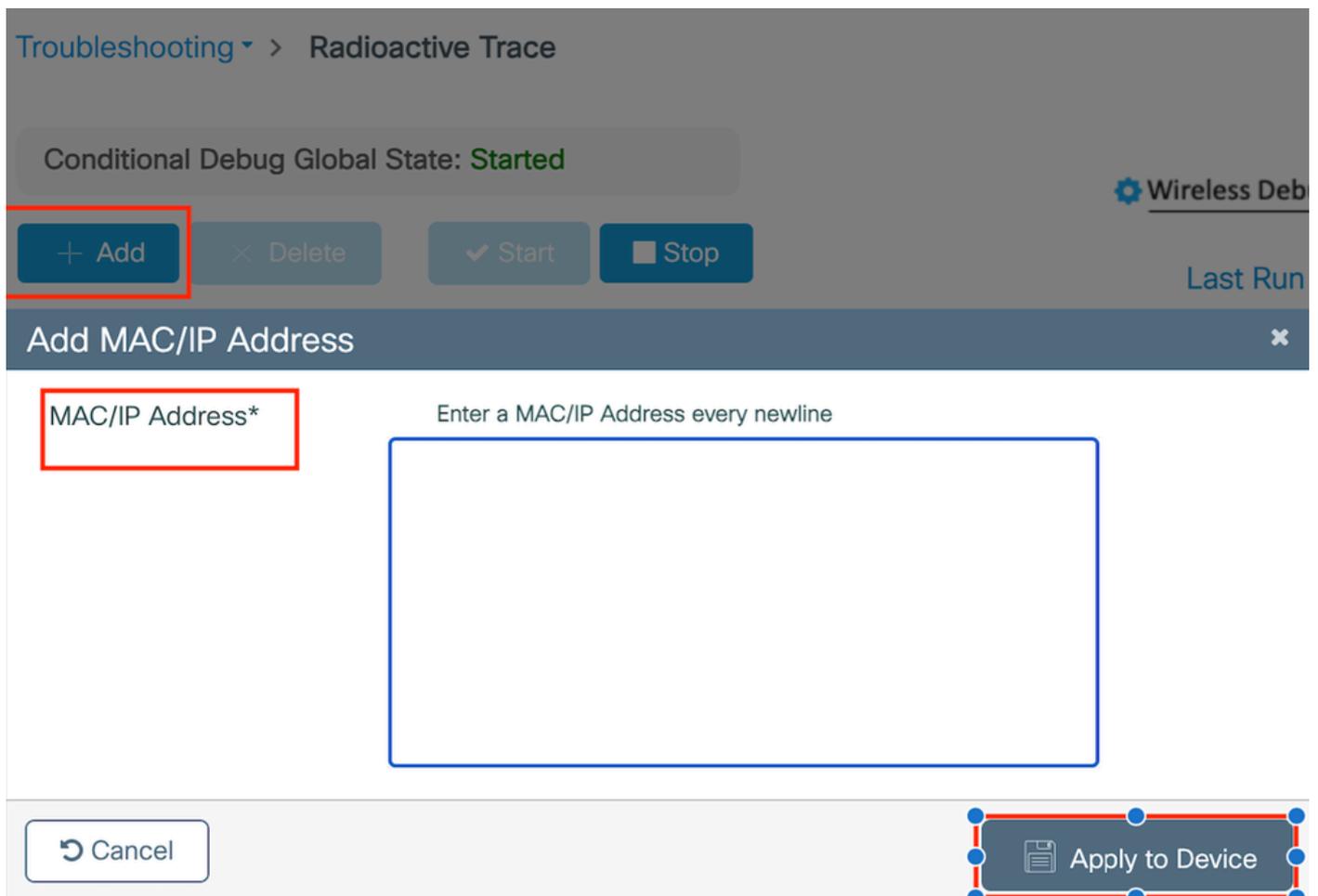
Copiez le fichier sur un serveur externe .

```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP address>
```

Affichez le journal de débogage :

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

Activer le suivi RA dans l'interface utilisateur graphique,



Activer le suivi RA sur WebUI

Capture de paquets intégrée

Accédez à Troubleshooting > Packet Capture. Entrez le nom de capture et spécifiez l'adresse MAC du client comme adresse MAC de filtre interne. Définissez la taille de la mémoire tampon sur 100 et choisissez l'interface de liaison ascendante pour surveiller les paquets entrants et sortants.

+ Add    × Delete

### Create Packet Capture

Capture Name\*    TestPCap

Filter\*    any

Monitor Control Plane

Inner Filter Protocol  DHCP

Inner Filter MAC

Buffer Size (MB)\*    100

Limit by\*    Duration    3600    secs ≈ 1.00 hour

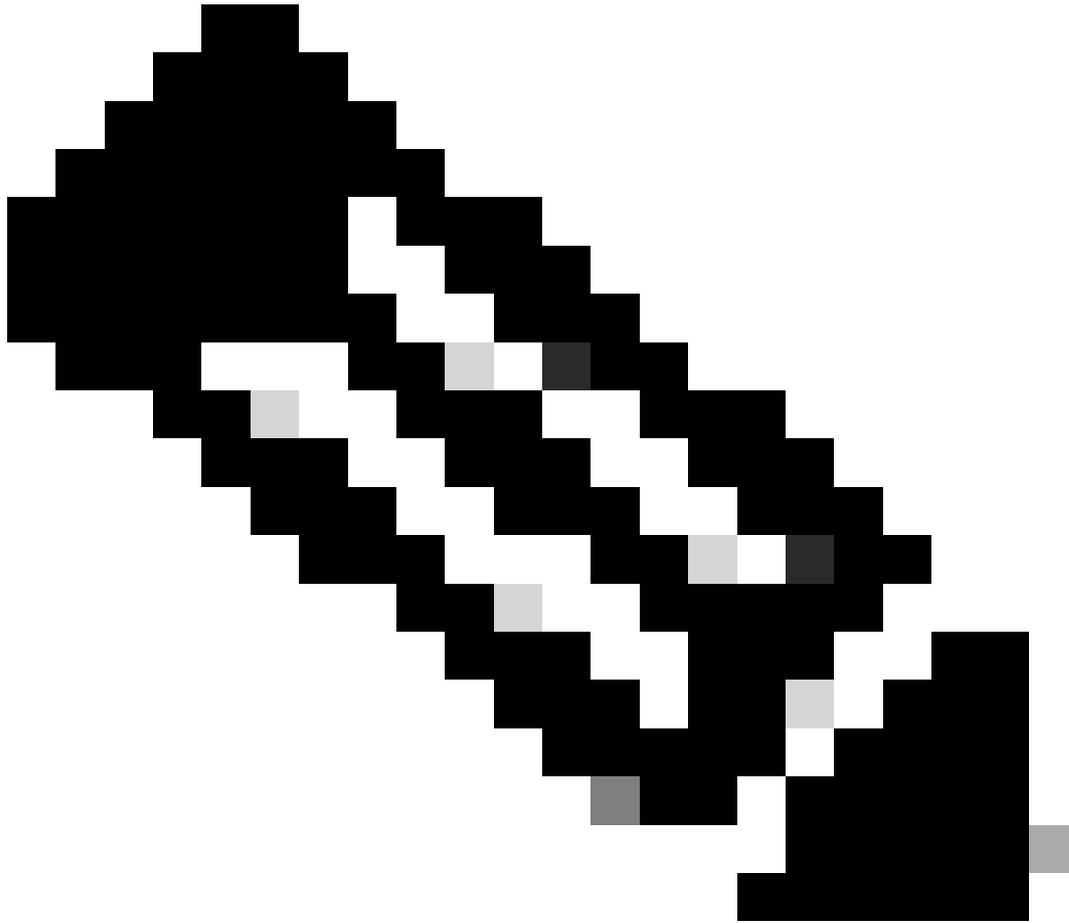
Available (12)    Search

- Tw0/0/1
- Tw0/0/2
- Tw0/0/3
- Te0/1/0

Selected (1)

- Tw0/0/0

Capture de paquets intégrée



Remarque : sélectionnez l'option « Surveiller le trafic de contrôle » pour afficher le trafic redirigé vers le processeur système et réinjecté dans le plan de données.

Accédez à Troubleshooting > Packet Capture et sélectionnez Start pour capturer des paquets.

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	<input type="button" value="Start"/>

Démarrer la capture de paquets

## Configuration CLI

```
monitor capture TestPCap inner mac <H.H.H>
monitor capture TestPCap buffer size 100
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
monitor capture TestPCap start
```

<Reproduce the issue>

```
monitor capture TestPCap stop
```

```
show monitor capture TestPCap
```

Status Information for Capture TestPCap

Target Type:

Interface: TwoGigabitEthernet0/0/0, Direction: BOTH

Status : Inactive

Filter Details:

Capture all packets

Inner Filter Details:

Mac: 6c7e.67e3.6db9

Continuous capture: disabled

Buffer Details:

Buffer Type: LINEAR (default)

Buffer Size (in MB): 100

Limit Details:

Number of Packets to capture: 0 (no limit)

Packet Capture duration: 3600

Packet Size to capture: 0 (no limit)

Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

Exportez la capture de paquets vers un serveur TFTP externe.

```
monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap
```

Accédez à Troubleshooting > Packet Capture et sélectionnez Export pour télécharger le fichier de capture sur l'ordinateur local.

The screenshot shows a configuration table for packet captures. The table has columns for Capture Name, Interface, Monitor Control Plane, Buffer Size, Filter by, Limit, Status, and Action. The 'TestPCap' entry is selected. The 'Export' button in the Action column is highlighted with a red box. A dialog box titled 'Export Capture - TestPCap' is open, showing 'Export to\*' set to 'desktop' and the 'Export' button also highlighted with a red box.

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	<input type="button" value="Start"/> <input type="button" value="Export"/>

Export Capture - TestPCap

Export to\* desktop

Télécharger EPC

Extraits de journal de travail

Journal de débogage du client AireOS Foreign Controller

## Paquet filaire reçu du client filaire

\*apfReceiveTask: May 27 12:00:55.127: a0:ce:c8:c3:a9:b5 Wired Guest packet from 10.105.211.69 on mobil

## Demande d'ancrage d'exportation de bâtiment de contrôleur étranger

\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Attempting anchor export for mobile a0:ce:c8:c3:  
\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 mmAnchorExportSend: Building ExportForeignLradM  
\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 SGT Payload built in Export Anchor Req 0

Le contrôleur étranger envoie une requête d'exportation d'ancrage au contrôleur d'ancrage.

\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Export Anchor request sent to 10.76.118.70

Le contrôleur d'ancrage envoie un accusé de réception pour la requête d'ancrage du client

\*Dot1x\_NW\_MsgTask\_5: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Recvd Exp Anchor Ack for mobile a0:ce:c8:c3:

Le rôle de mobilité pour les clients sur le contrôleur étranger est mis à jour pour exporter des éléments étrangers.

\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP\_REQD (7) mobility role update requ  
Peer = 10.76.118.70, Old Anchor = 10.76.118.70, New Anchor = 10.76.118.70

Le client est passé à l'état EXÉCUTÉ.

\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP\_REQD (7) State Update from Mobilit  
\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Stopping deletion of Mobile Station: (callerId:  
\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Moving client to run state

## 9800 Contrôleur étranger trace radioactive

Le client s'associe au contrôleur.

2024/07/15 04:10:29.087608331 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

La détection de mobilité est en cours après l'association.

2024/07/15 04:10:29.091585813 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

2024/07/15 04:10:29.091605761 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

Une fois la détection de mobilité traitée, le type d'itinérance client est mis à jour vers L3 demandé.

2024/07/15 04:10:29.091664605 {wncd\_x\_R0-0}{1}: [mm-transition] [17765]: (info): MAC: a0ce.c8c3.a9b5 MM

2024/07/15 04:10:29.091693445 {wncd\_x\_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Roam t

Le contrôleur étranger envoie la demande d'ancrage d'exportation au WLC d'ancrage.

2024/07/15 04:10:32.093245394 {mobilityd\_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex

2024/07/15 04:10:32.093253788 {mobilityd\_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Fo

2024/07/15 04:10:32.093274405 {mobilityd\_R0-0}{1}: [mm-client] [18316]: (info): MAC: a0ce.c8c3.a9b5 For

La réponse Export Anchor est reçue du contrôleur Anchor et le VLAN est appliqué à partir du profil utilisateur.

2024/07/15 04:10:32.106775213 {mobilityd\_R0-0}{1}: [mm-transition] [18316]: (info): MAC: a0ce.c8c3.a9b5

2024/07/15 04:10:32.106811183 {mobilityd\_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex

2024/07/15 04:10:32.107183692 {wncd\_x\_R0-0}{1}: [epm-misc] [17765]: (info): [a0ce.c8c3.a9b5:Tw0/0/0] An

2024/07/15 04:10:32.107247304 {wncd\_x\_R0-0}{1}: [svm] [17765]: (info): [a0ce.c8c3.a9b5] Applied User Pr

2024/07/15 04:10:32.107250258 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [17765]: (info): Applied User Profile:

Une fois la demande Export Anchor traitée, le rôle de mobilité du client est mis à jour vers Export Foreign.

2024/07/15 04:10:32.107490972 {wncd\_x\_R0-0}{1}: [mm-client] [17765]: (debug): MAC: a0ce.c8c3.a9b5 Proce

2024/07/15 04:10:32.107502336 {wncd\_x\_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Mobili

2024/07/15 04:10:32.107533732 {wncd\_x\_R0-0}{1}: [sanet-shim-translate] [17765]: (info): Anchor Vlan: 20

2024/07/15 04:10:32.107592251 {wncd\_x\_R0-0}{1}: [mm-client] [17765]: (note): MAC: a0ce.c8c3.a9b5 Mobili

Le client passe à l'état d'apprentissage IP.

```
2024/07/15 04:10:32.108210365 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 04:10:32.108293096 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: a0ce.c8c3.a9b5
```

Après l'apprentissage IP, le client passe à l'état RUN sur le WLC étranger.

```
2024/07/15 04:10:32.108521618 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5
```

Journal de débogage du client du contrôleur AireOS Anchor

Requête d'ancrage d'exportation reçue du contrôleur étranger.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Anchor Export Request Recvd for mobile a0:c
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv: Extracting mmPayloadExpo
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv Ssid=Guest useProfileNa
```

Le VLAN de pontage local est appliqué au client.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Updated local bridging VLAN to 11 while app
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Applying Interface(wired-vlan-11) policy on
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 After applying Interface(wired-vlan-11) pol
```

Le rôle Mobilité est mis à jour pour Exporter l'ancre et l'état du client Transmis Associé.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 0.0.0.0 START (0) mobility role update requ
Peer = 10.76.118.70, Old Anchor = 0.0.0.0, New Anchor = 10.76.118.74
Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5
add client MAC a0:ce:c8:c3:a9:b5 IP 10.76.1
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5
Sent message to add a0:ce:c8:c3:a9:b5 on me
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv (mm_listen.c:7933) Changi
```

La mobilité est terminée, l'état du client est associé et le rôle de mobilité est Exporter l'ancrage.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mob
```

L'adresse IP du client est apprise sur le contrôleur et l'état est transmis du DHCP requis à l'authentification Web requise.

```
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 Static IP client associated to interface wired-vlan
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 dtlArpSetType: Changing ARP Type from 0 ---> 1 for
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 10.105.211.75 DHCP_REQD (7) Change state to WEBAUTH
```

L'URL Webauth est formulée en ajoutant l'URL de redirection externe et l'adresse IP virtuelle du contrôleur.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Preparing redirect URL according to configure
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Web-auth type External, using URL:http://10.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added switch_url, redirect URL is now http://
```

Ajout de l'adresse MAC du client et du WLAN à l'URL.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added client_mac , redirect URL is now http://
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now http://10.127
```

URL finale après avoir parcouru le GET HTTP pour l'hôte 10.105.211.1

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser host is 10.105.211.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser path is /auth/discovery
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-added redirect=, URL is now http://10.127.196.
```

L'URL de redirection est envoyée au client dans le paquet de réponse 200 OK.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- 200 send_data =HTTP/1.1 200 OK
Location:http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&client_mac=a0
```

Le client établit une connexion TCP avec l'hôte d'URL de redirection. Une fois que les clients ont envoyé le nom d'utilisateur et le mot de passe de connexion sur le portail, une requête radius est envoyée par le contrôleur au serveur radius.

Une fois que le contrôleur reçoit un Access-Accept, le client ferme la session TCP et passe à l'état

RUN.

```
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Sending the packet to v4 host 10.197.224.122:18
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Successful transmission of Authentication Packe
*aaaQueueReader: May 28 10:46:59:077: AVP[01] User-Name.....testuser
*aaaQueueReader: May 28 10:46:59:077: AVP[03] Calling-Station-Id.....a0-ce-c8
*aaaQueueReader: May 28 10:46:59:077: AVP[04] Nas-Port.....0x000000
*aaaQueueReader: May 28 10:46:59:077: AVP[05] Nas-Ip-Address.....0x0a4c76
*aaaQueueReader: May 28 10:46:59:077: AVP[06] NAS-Identifier.....POD1586-
*aaaQueueReader: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 radiusServerFallbackPassiveStateUpdate: RADIUS
*radiusTransportThread: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Access-Accept received from RADIUS serv
*Dot1x_NW_MsgTask_5: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Processing Access-Accept for mobile a0:ce:c
*apfReceiveTask: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Moving client to run state
```

## 9800 Contrôleur d'ancrage radioactif trace

Message d'annonce de mobilité pour le client provenant du contrôleur étranger.

```
2024/07/15 15:10:20.614677358 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Ex
```

Requête d'ancrage d'exportation reçue du contrôleur étranger lorsque le client s'associe pour laquelle la réponse d'ancrage d'exportation est envoyée par le contrôleur d'ancrage qui peut être vérifiée sur la trace RA du contrôleur étranger.

```
2024/07/15 15:10:22.615246594 {mobilityd_R0-0}{1}: [mm-transition] [15259]: (info): MAC: a0ce.c8c3.a9b5
```

Le client passe à l'état d'association et le rôle de mobilité passe à Export Anchor.

```
2024/07/15 15:10:22.616156811 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b5
```

```
2024/07/15 15:10:22.627358367 {wncd_x_R0-0}{1}: [mm-client] [14709]: (note): MAC: a0ce.c8c3.a9b5 Mobili
```

```
2024/07/15 15:10:22.627462963 {wncd_x_R0-0}{1}: [dot11] [14709]: (note): MAC: a0ce.c8c3.a9b5 Client da
```

```
2024/07/15 15:10:22.627490485 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Ex
```

```
2024/07/15 15:10:22.627494963 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Fo
```

IP learn est terminé, IP du client a appris via ARP .

```
2024/07/15 15:10:22.628124206 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:23.627064171 {wncd_x_R0-0}{1}: [sisf-packet] [14709]: (info): RX: ARP from interface m
2024/07/15 15:10:24.469704913 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470527056 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470587596 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470613094 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
```

L'état de la stratégie client est en attente d'authentification Web.

```
2024/07/15 15:10:24.470748350 {wncd_x_R0-0}{1}: [client-auth] [14709]: (info): MAC: a0ce.c8c3.a9b5 Cli
```

La connexion TCP est usurpée par le contrôleur. Lorsque le client envoie une requête HTTP GET, une trame de réponse 200 OK est envoyée, qui contient l'URL de redirection.

Le client doit établir une connexion TCP avec l'URL de redirection et charger la page.

```
2024/07/15 15:11:37.579177010 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579190912 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579226658 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579230650 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123072893 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123082753 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
```

Lorsque le client envoie les informations d'identification de connexion sur la page du portail Web, un paquet de demande d'accès est envoyé au serveur RADIUS pour authentification.

```
2024/07/15 15:12:04.281076844 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Send Access-Request t
2024/07/15 15:12:04.281087672 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator e3 01
2024/07/15 15:12:04.281093278 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Calling-Station-Id
2024/07/15 15:12:04.281097034 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
2024/07/15 15:12:04.281148298 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Cisco AVpair
```

Access-Accept est reçu du serveur radius, webauth est réussi.

```
2024/07/15 15:12:04.683597101 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Received from id 1812
2024/07/15 15:12:04.683607762 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator 52 3e
2024/07/15 15:12:04.683614780 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
```

L'authentification est réussie et l'état de la stratégie client est en cours d'exécution.

```
2024/07/15 15:12:04.683901842 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:12:04.690643388 {wncd_x_R0-0}{1}: [errmsg] [14709]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/15 15:12:04.690726966 {wncd_x_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied attribute :bs
2024/07/15 15:12:04.691064276 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
```

## Analyse de capture de paquets intégrée

No.	Time	Source	Destination	Length	Protocol	Info
804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)

> Frame 806: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits)

> Ethernet II, Src: Cisco\_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco\_34:90:cb (6c:5e:3b:34:90:cb)

> Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.76.6.156

> User Datagram Protocol, Src Port: 16667, Dst Port: 16667

> Control And Provisioning of Wireless Access Points - Data

> Ethernet II, Src: Cisco\_34:90:d4 (6c:5e:3b:34:90:d4), Dst: CeLink\_c3:a9:b5 (a0:ce:c8:c3:a9:b5)

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4095

> Internet Protocol Version 4, Src: 10.105.211.1, Dst: 10.105.211.69

> Transmission Control Protocol, Src Port: 80, Dst Port: 54351, Seq: 1, Ack: 108, Len: 743

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Location: http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=http://10.105.211.1/auth/discovery?architecture=9\r\n

Content-Type: text/html\r\n

> Content-Length: 527\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.000000000 seconds]

[Request in frame: 804]

[Request URI: http://10.105.211.1/auth/discovery?architecture=9]

File Data: 527 bytes

Le client est redirigé vers la page du portail

La session est fermée après réception de l'URL de redirection.

804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
805	15:10:24.826953	10.105.211.1	10.105.211.69		TCP	80 → 54351 [ACK] Seq=1 Ack=108 Win=65152 Len=0 TSval=2124108437 TSecr=2231352500
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)
807	15:10:24.826953	10.105.211.69	10.105.211.1		TCP	54351 → 80 [ACK] Seq=108 Ack=744 Win=131008 Len=0 TSval=2231352500 TSecr=2124108437
812	15:10:24.835955	10.105.211.69	10.105.211.1		TCP	54351 → 80 [FIN, ACK] Seq=108 Ack=744 Win=131072 Len=0 TSval=2231352510 TSecr=2124108437
813	15:10:24.836947	10.105.211.1	10.105.211.69		TCP	80 → 54351 [FIN, ACK] Seq=744 Ack=109 Win=65152 Len=0 TSval=2124108447 TSecr=2231352510
814	15:10:24.836947	10.105.211.69	10.105.211.1		TCP	54351 → 80 [ACK] Seq=109 Ack=745 Win=131072 Len=0 TSval=2231352510 TSecr=2124108447

La session TCP est fermée après réception de l'URL de redirection

Le client initie une connexion TCP en trois étapes vers l'hôte d'URL de redirection et envoie une requête HTTP GET.

Une fois la page chargée, les identifiants de connexion sont soumis sur le portail, le contrôleur envoie une demande d'accès au serveur RADIUS pour authentifier le client.

Une fois l'authentification réussie, la session TCP vers le serveur Web est fermée et sur le contrôleur, l'état du gestionnaire de stratégies client passe à EXÉCUTER.



## Article connexe

[Configuration de la fonction WLAN Anchor Mobility sur Catalyst 9800](#)

[Exemple de configuration d'un accès invité câblé avec des contrôleurs AireOS](#)

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.