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

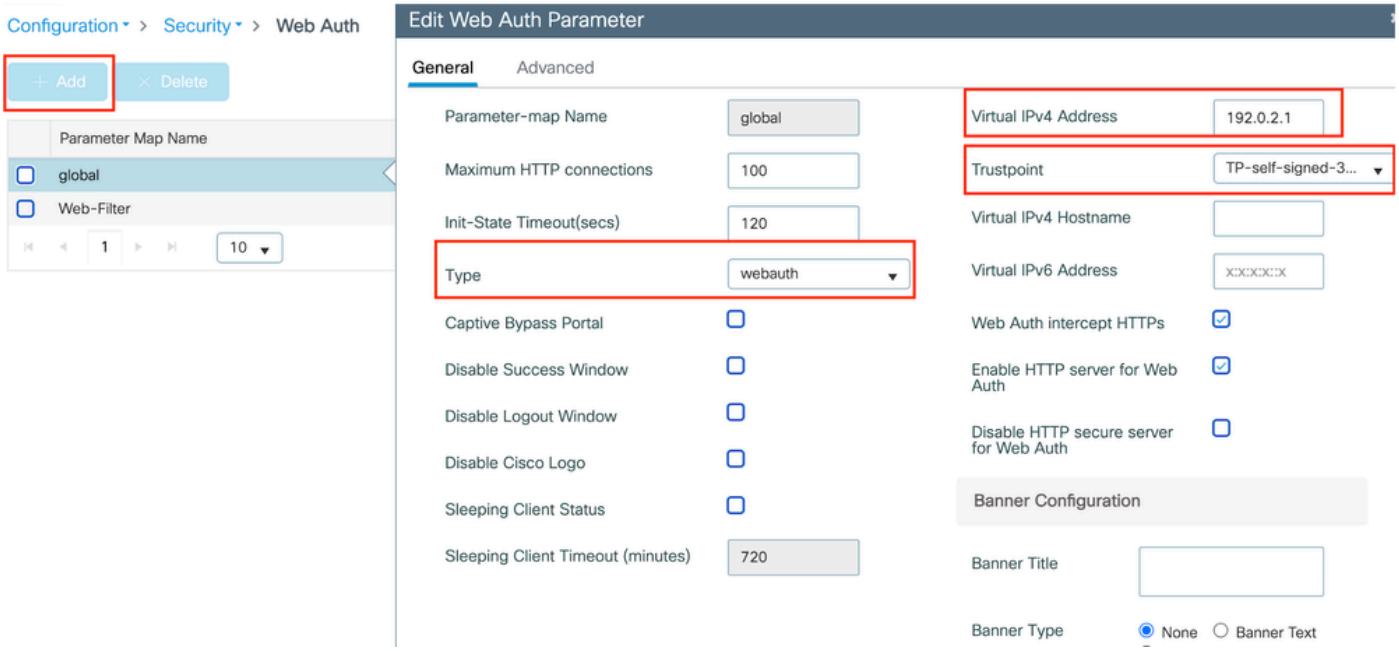
Diagramme du réseau

Topologie du réseau

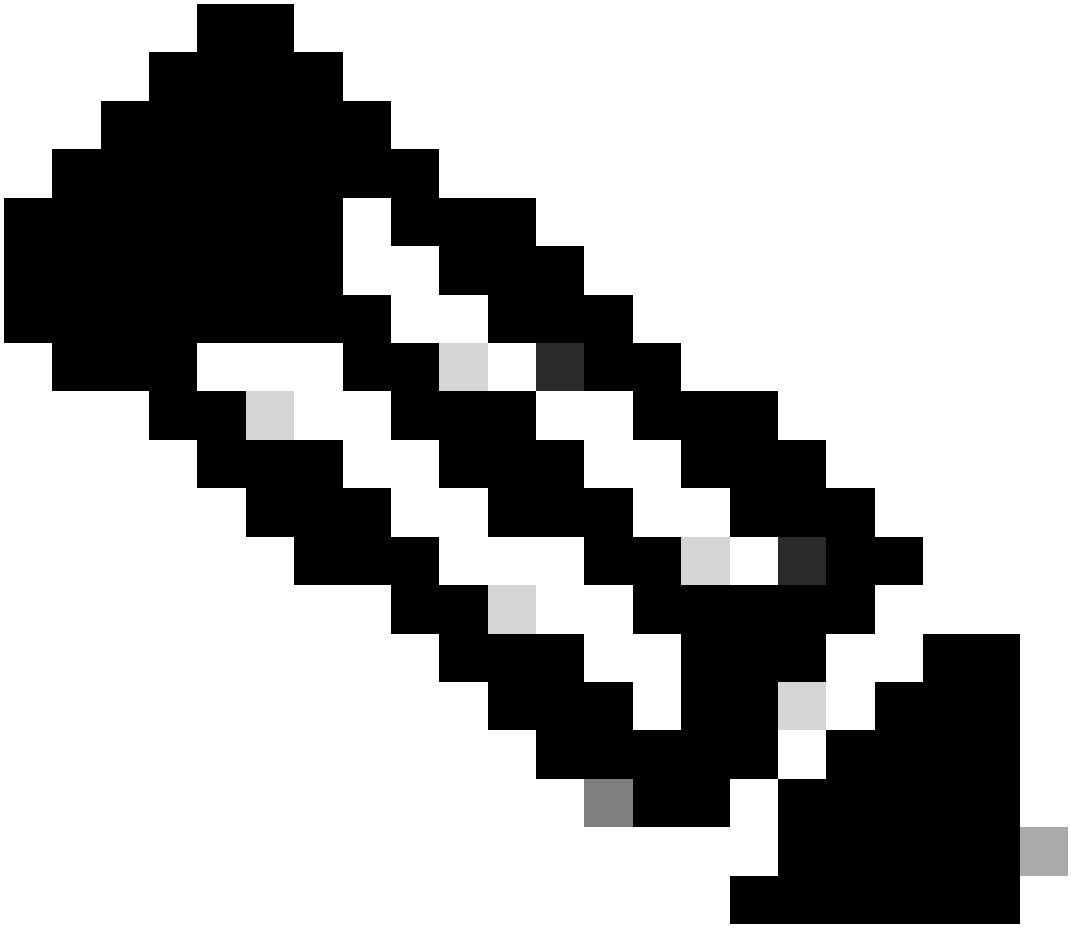
Configuration sur le WLC 9800 étranger

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.

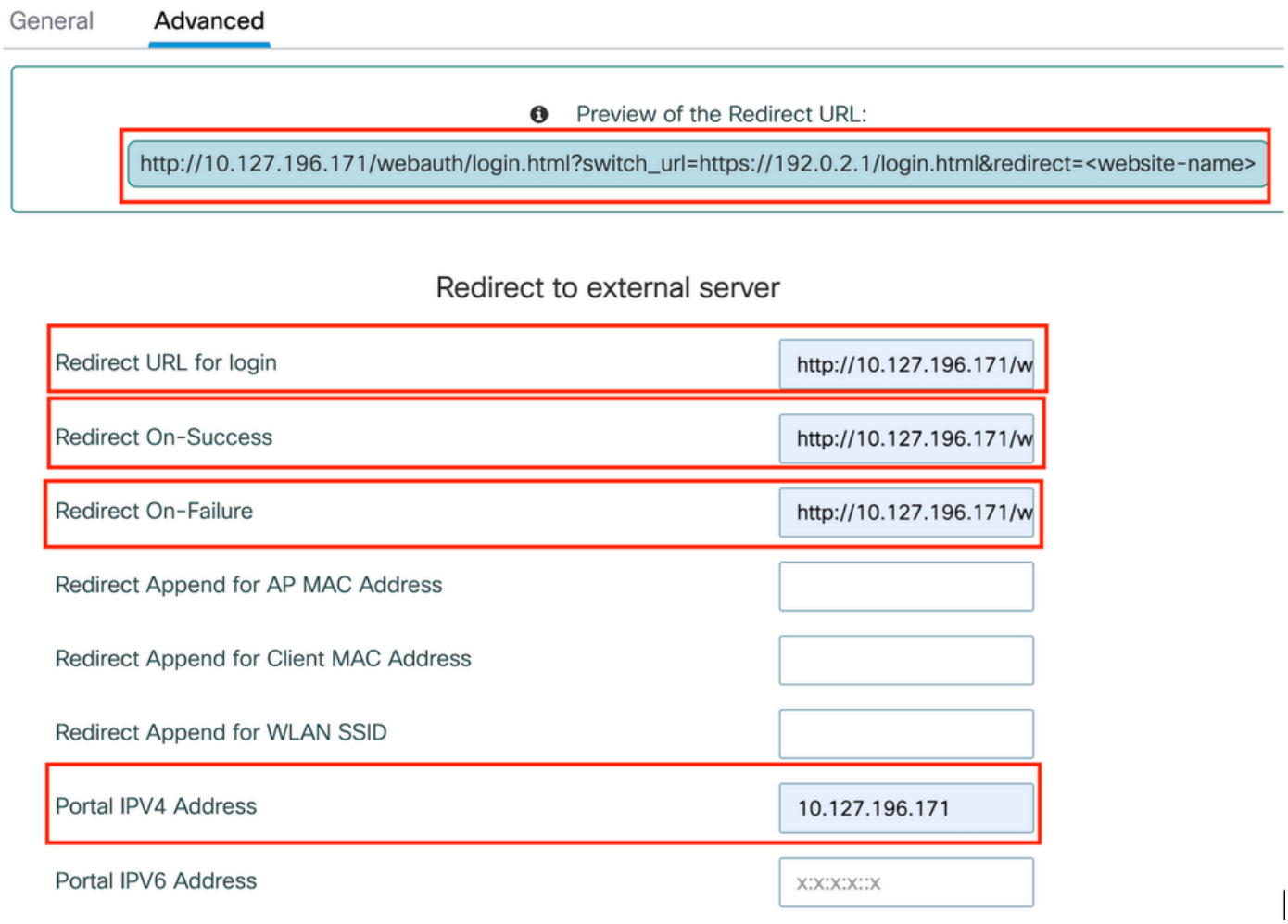


Mappage de paramètre global



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.



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
```

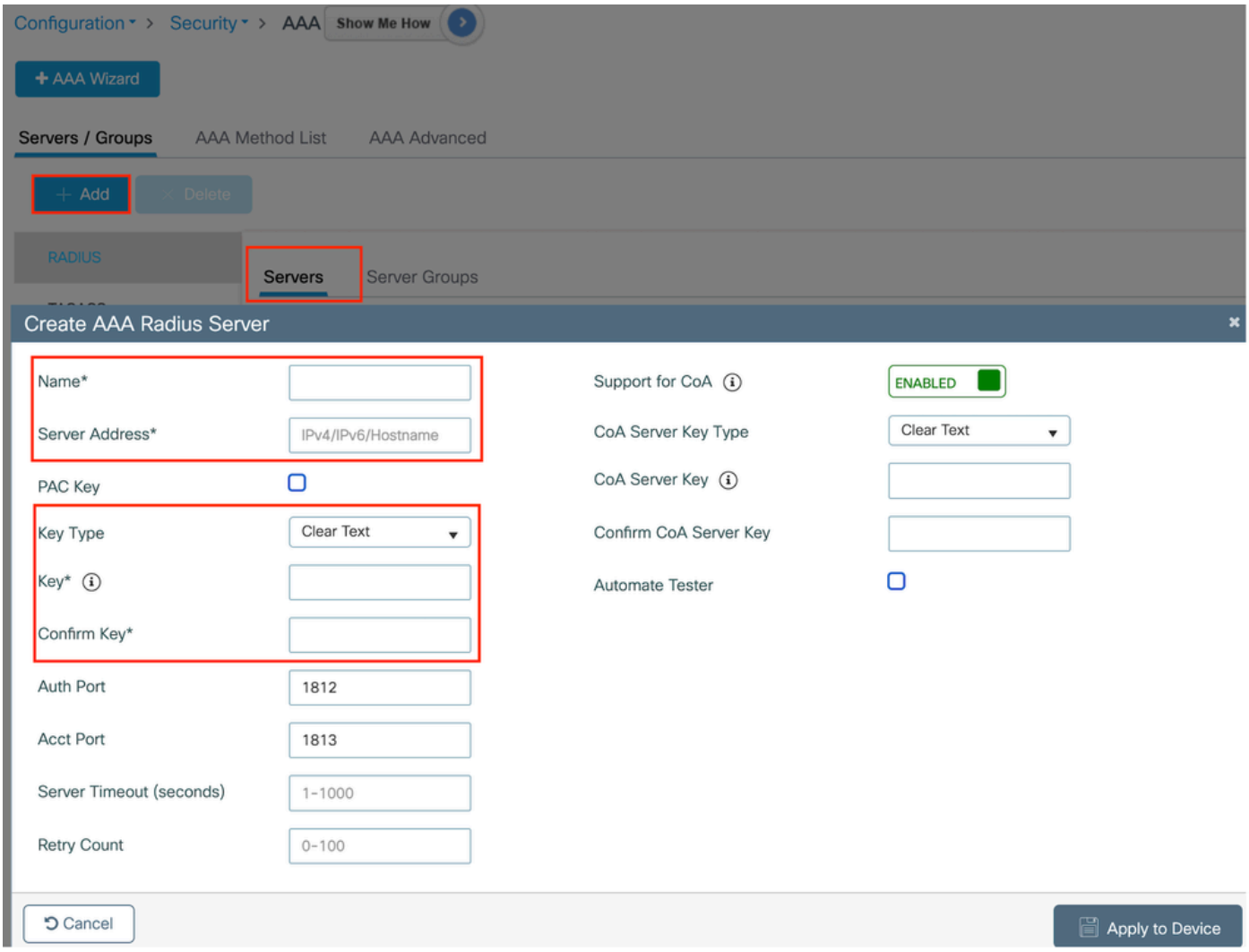
```
trustpoint TP-self-signed-3915430211
webauth-http-enable
```

> 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.

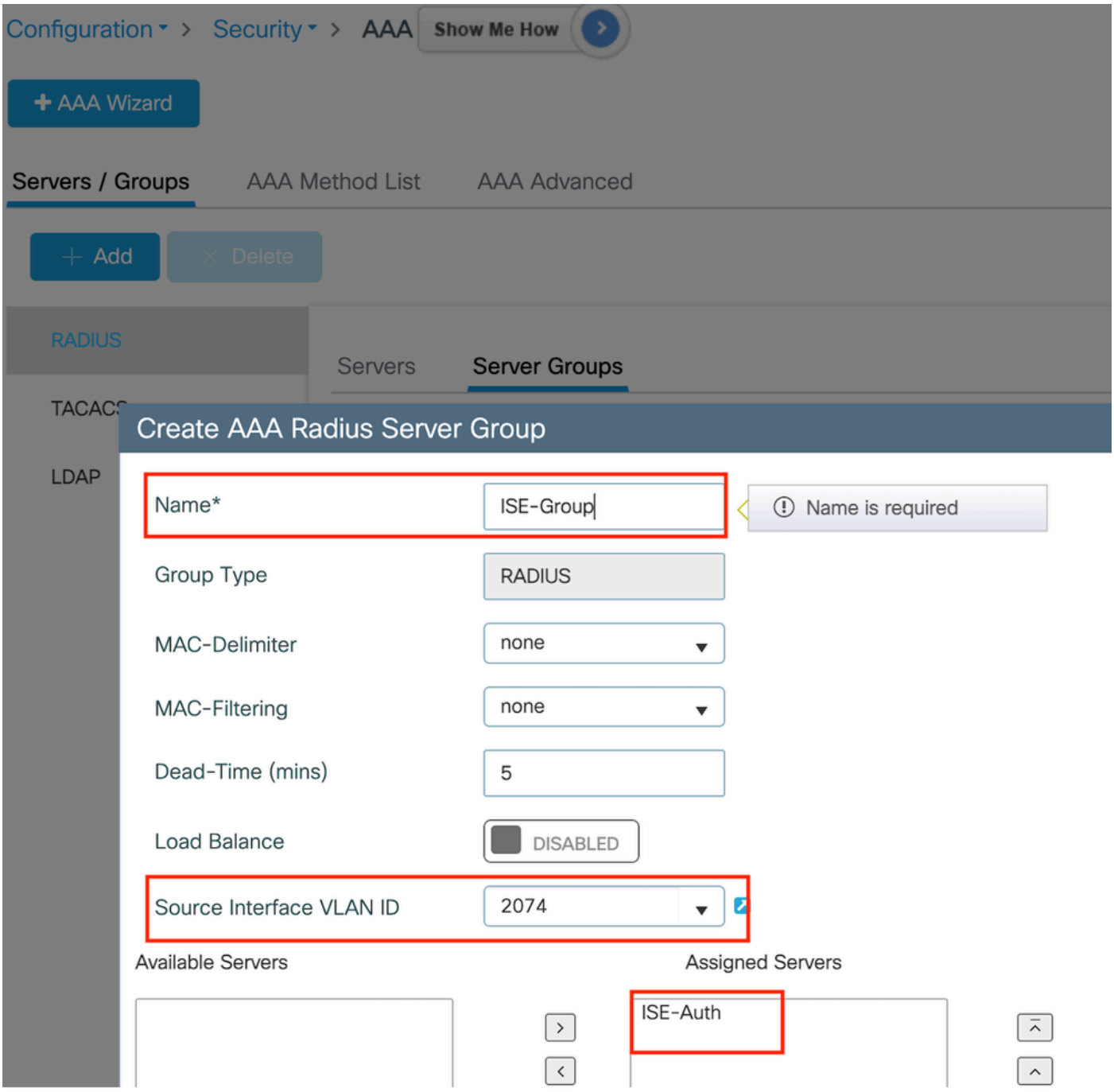


Configuration du serveur RADIUS

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.



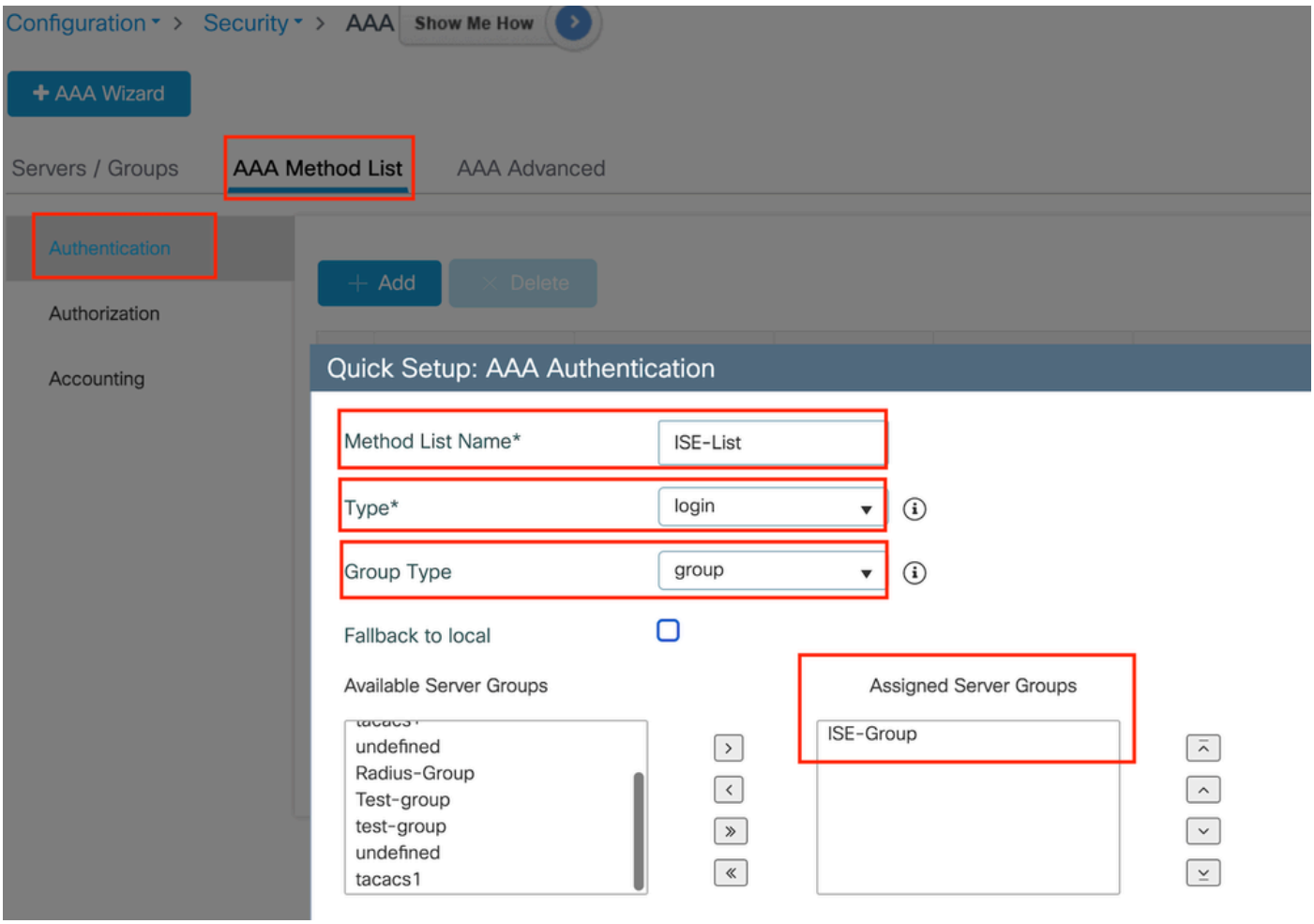
Groupe de serveurs Radius

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.



Liste des méthodes d'authentification

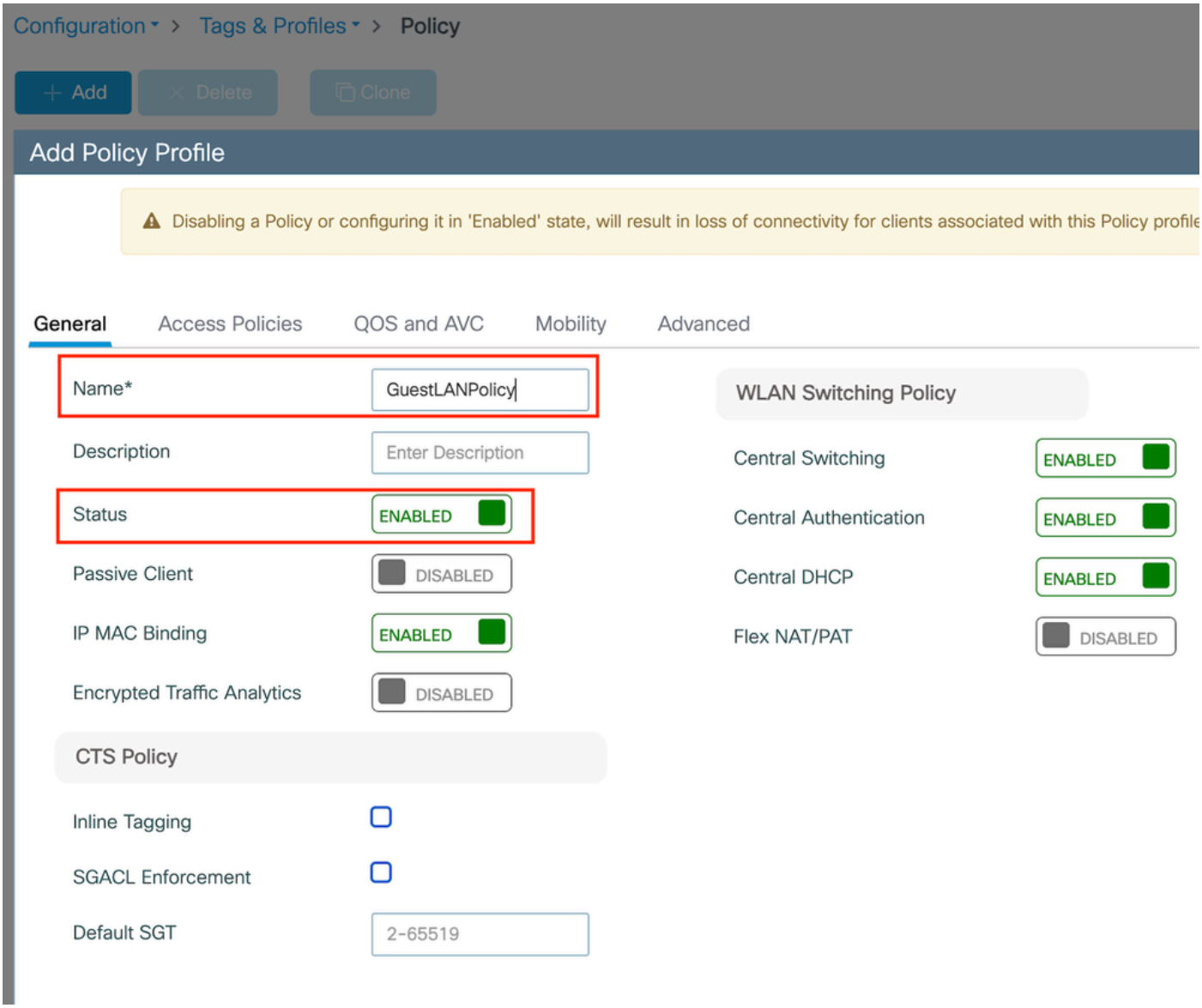
Configuration CLI

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

Configurer le profil de stratégie

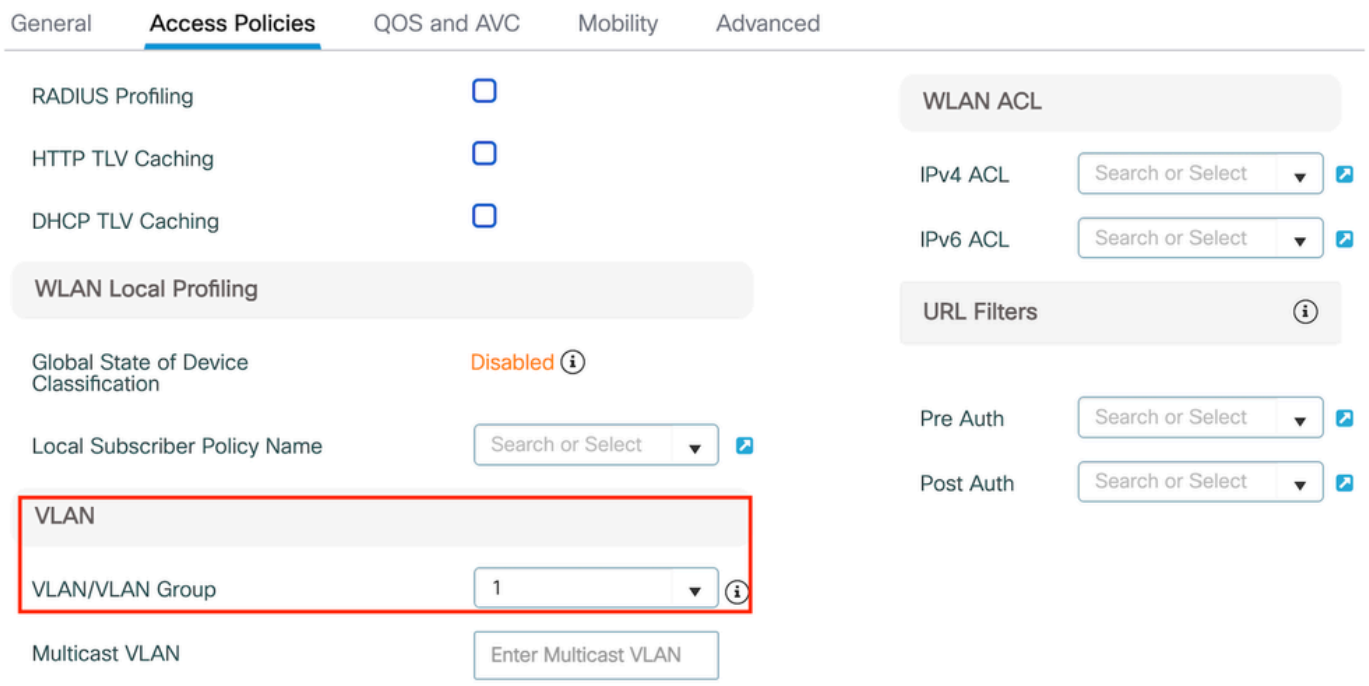
Étape 1 : Accédez à Configuration > Tags & Profiles > Policy, nommez votre nouveau profil dans

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



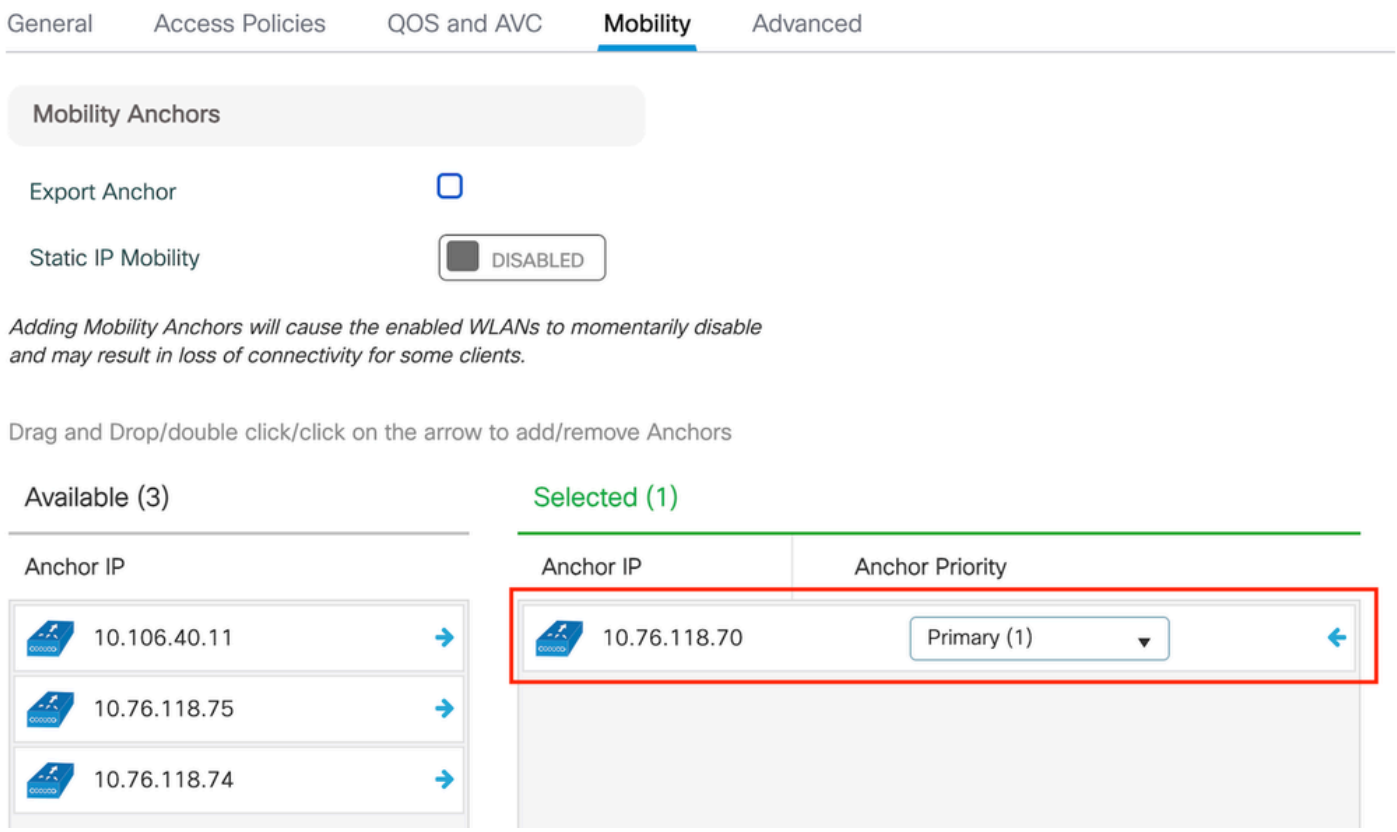
Profil de stratégie

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



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



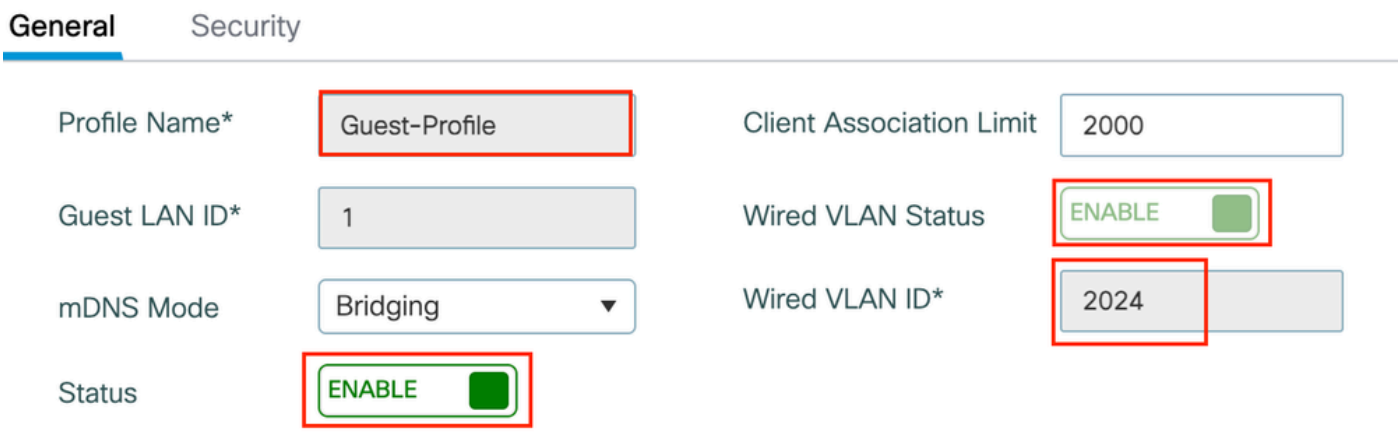
Carte de mobilité

Configuration CLI

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

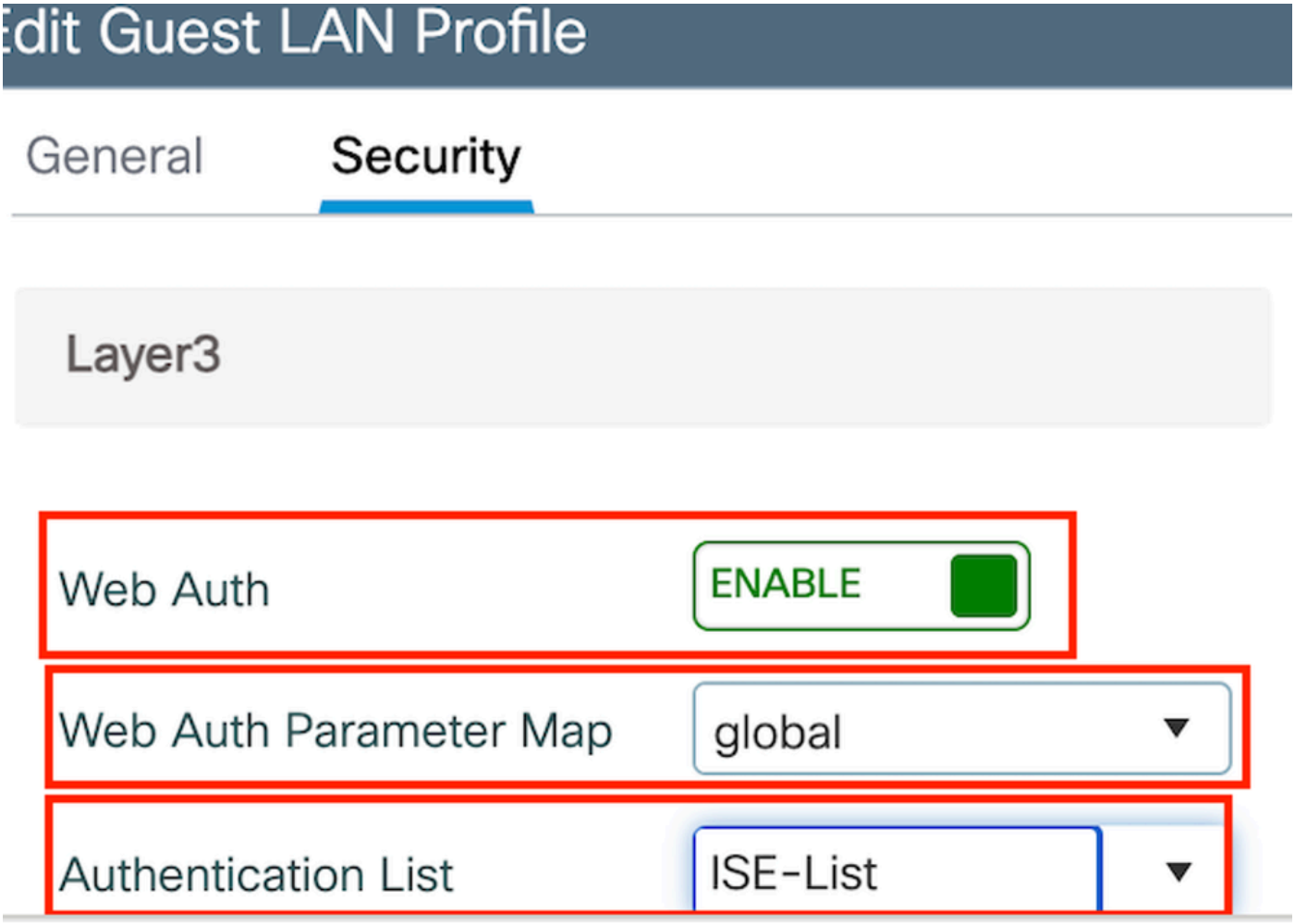
Configurer le profil de réseau local invité

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.



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.



Onglet Sécurité du réseau local invité

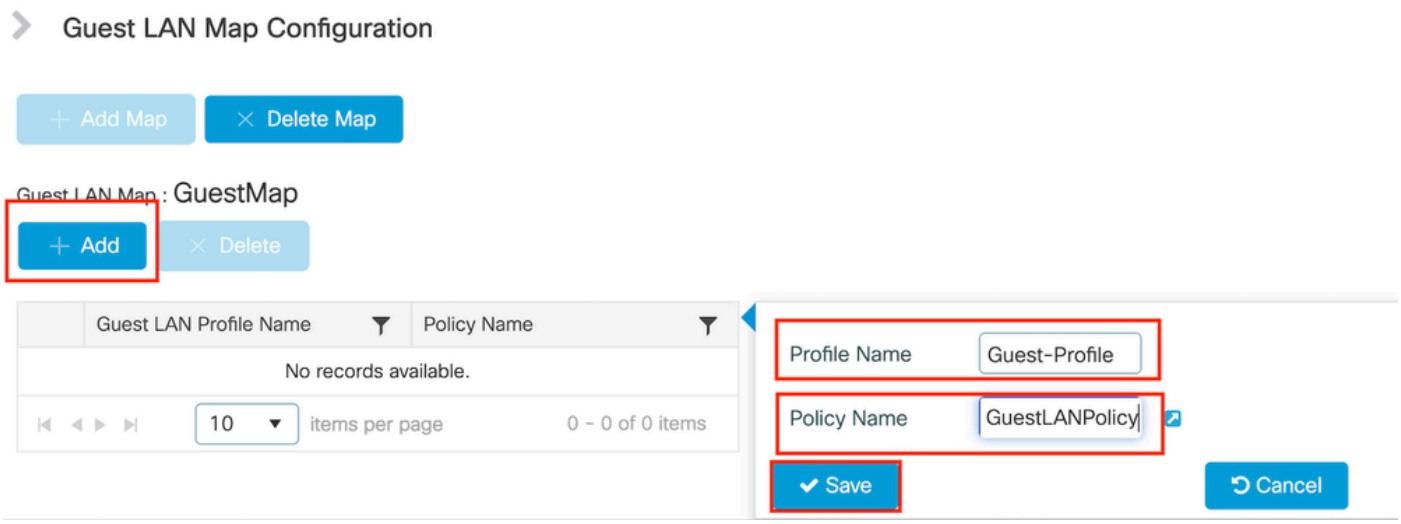
Configuration CLI

```
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



Plan du réseau local invité

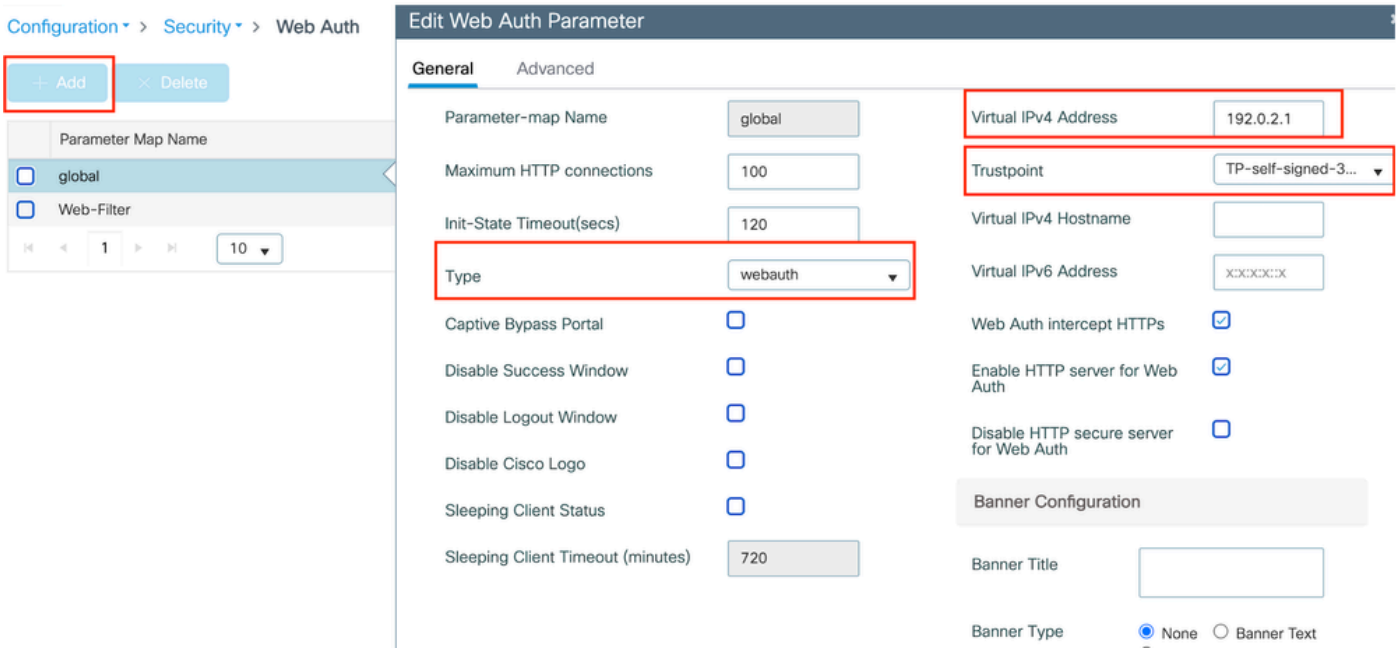
Configuration CLI

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

Configuration sur le WLC Anchor 9800

Configurer la carte de paramètres Web

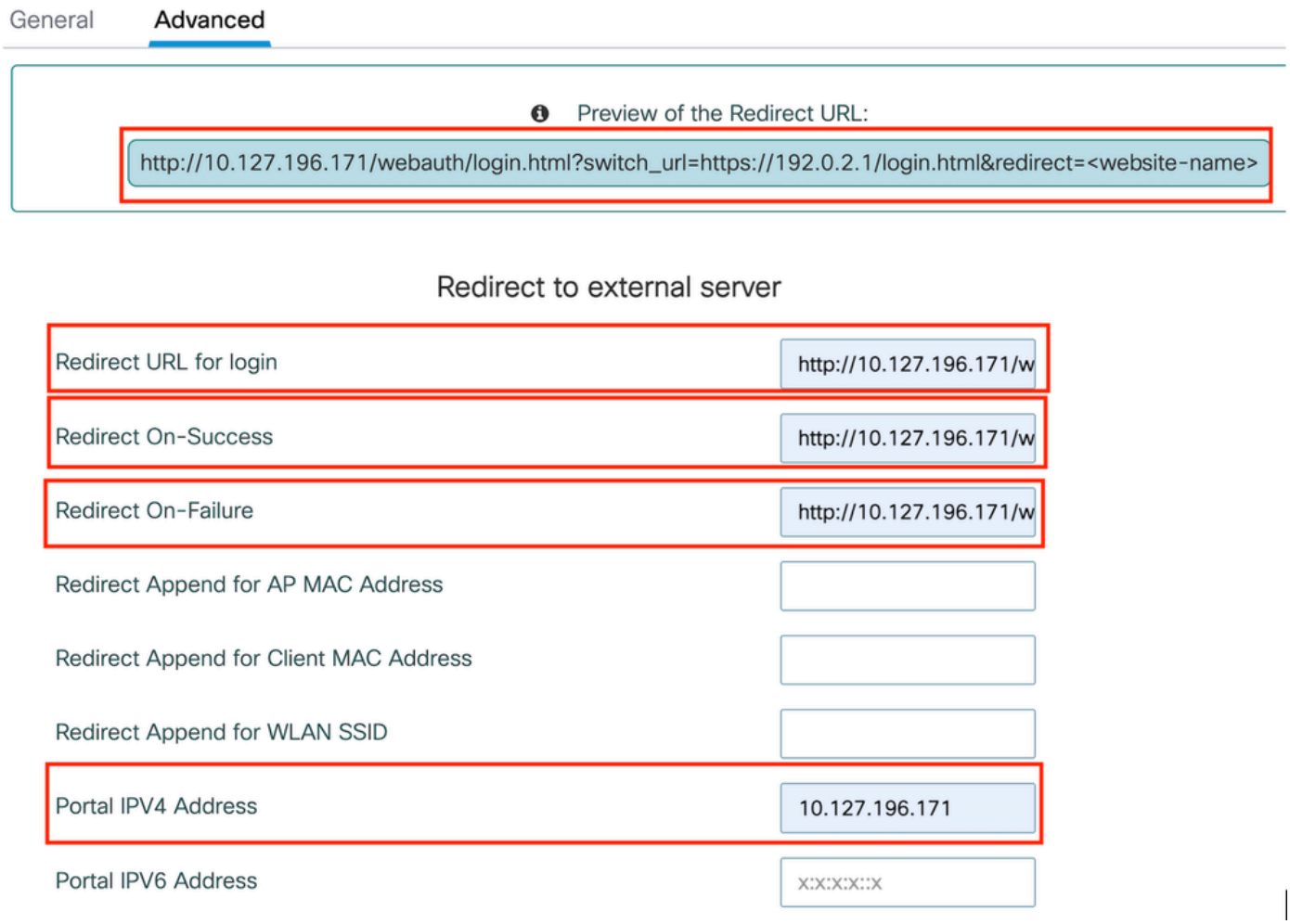
Étape 1 : Accédez à Configuration > Security > Web Auth, sélectionnez Global, vérifiez l'adresse IP virtuelle du contrôleur et le mappage Trustpoint, et assurez-vous que le type est défini sur webauth.



Mappage de paramètre global

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.



Onglet Avancé

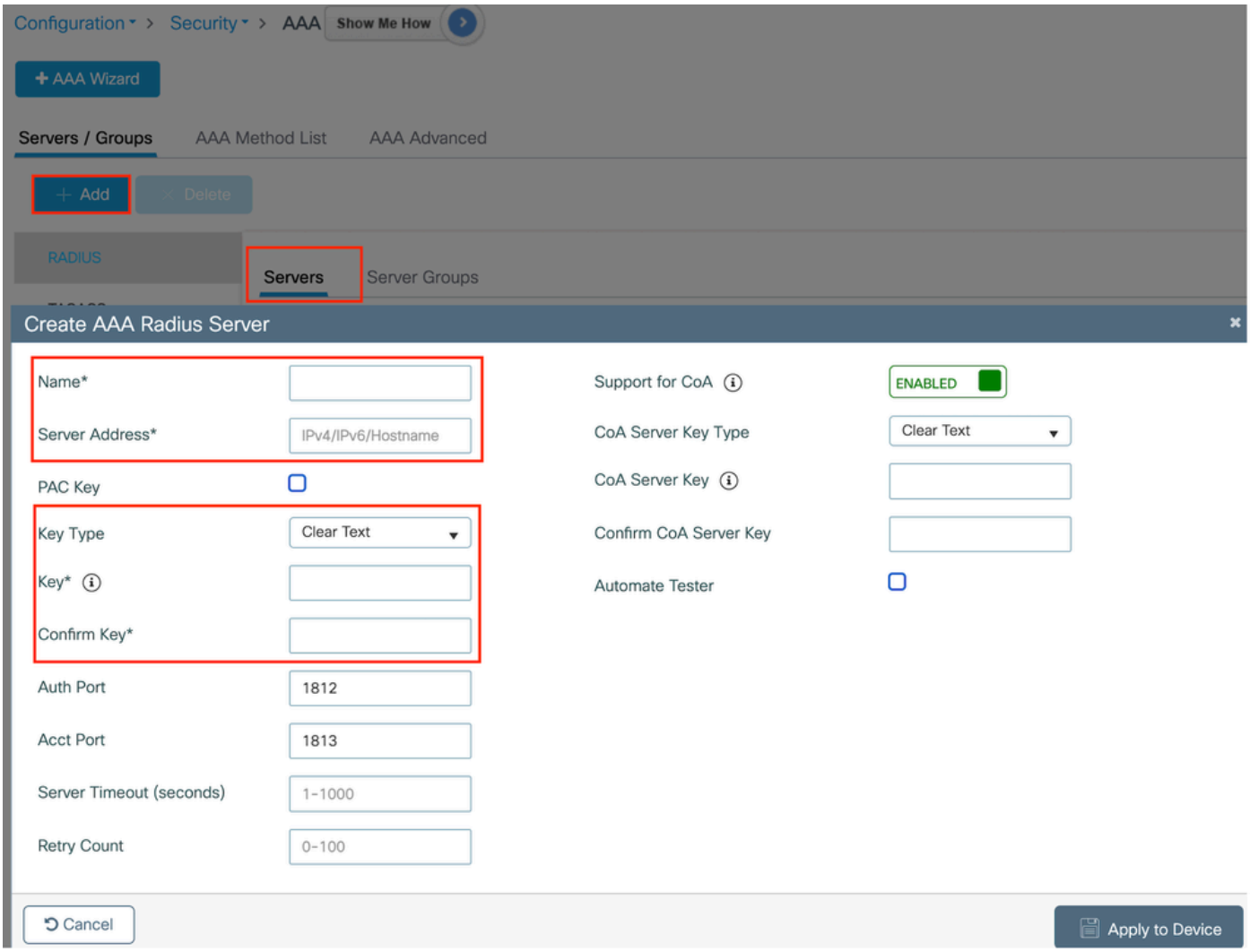
Configuration CLI

```
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.



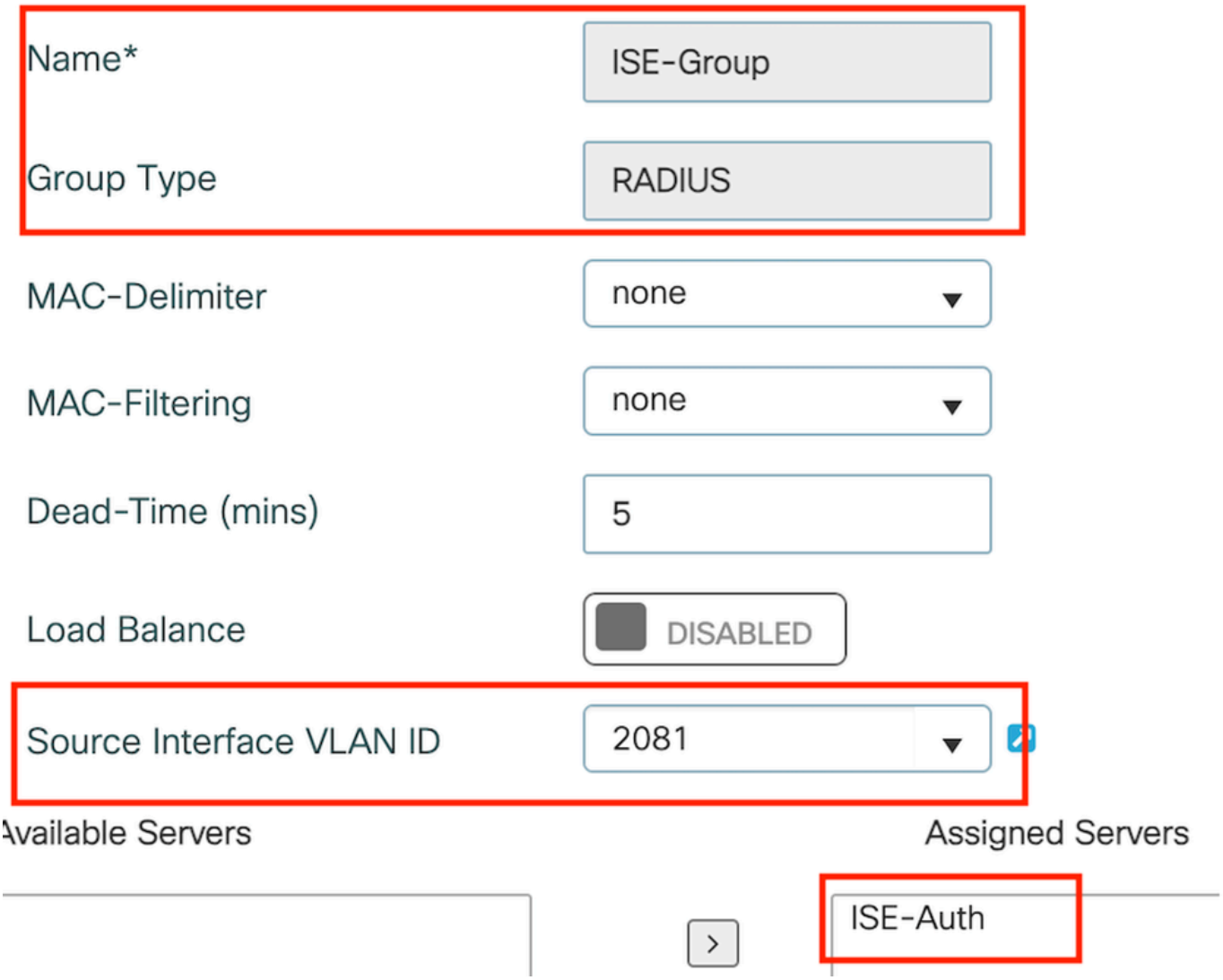
Configuration du serveur RADIUS

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.



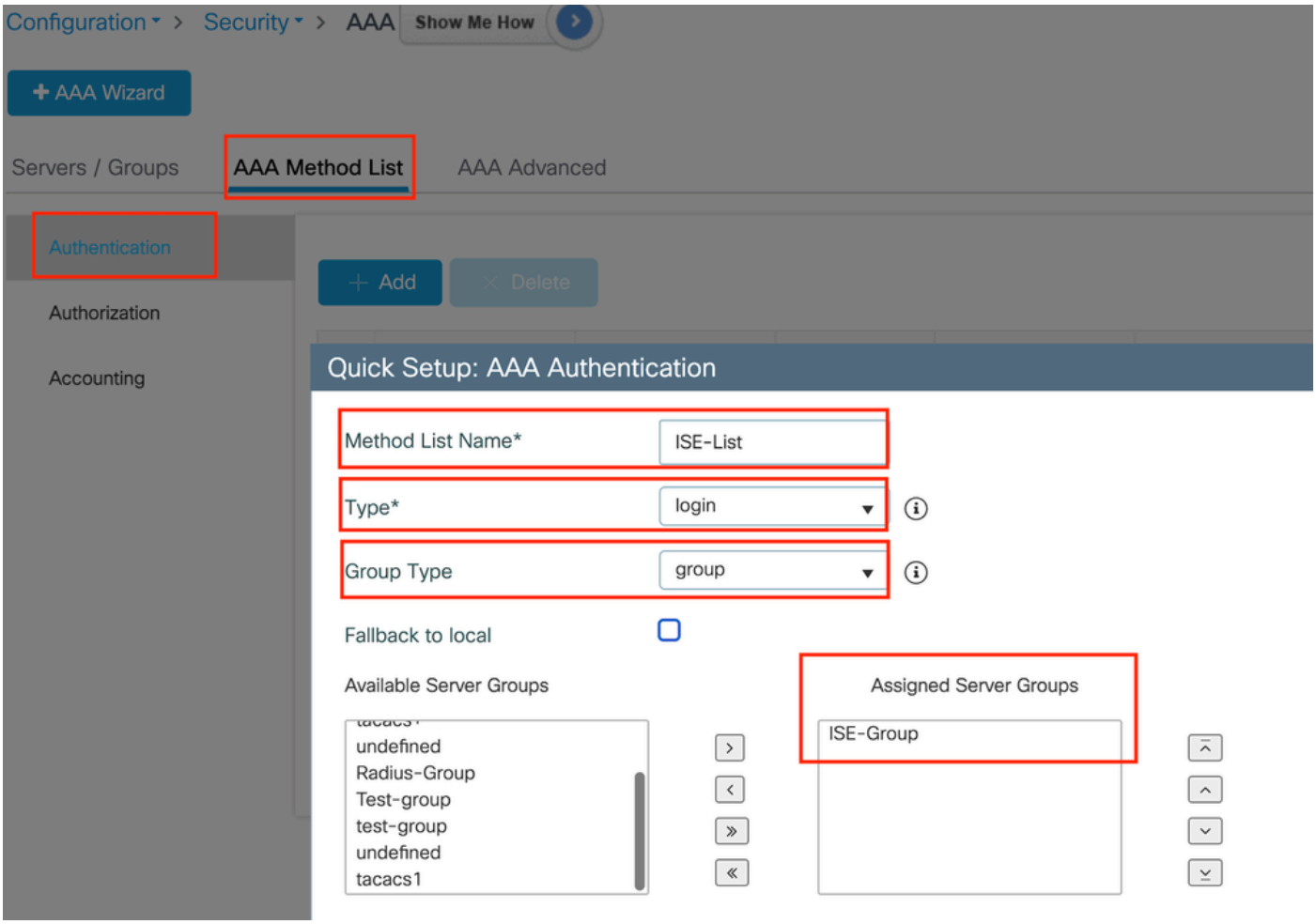
Groupe de rayons d'ancrage

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.



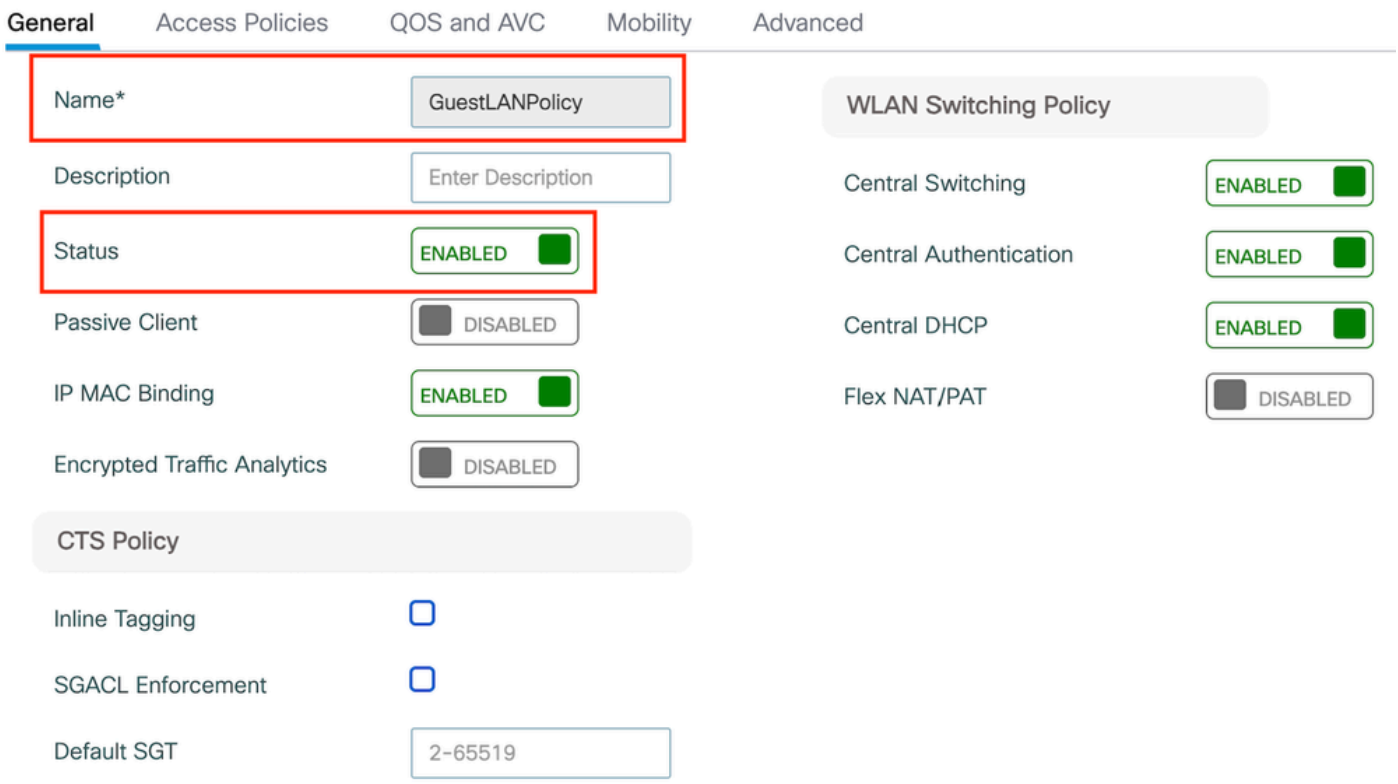
Liste des méthodes d'authentification

Configuration CLI

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

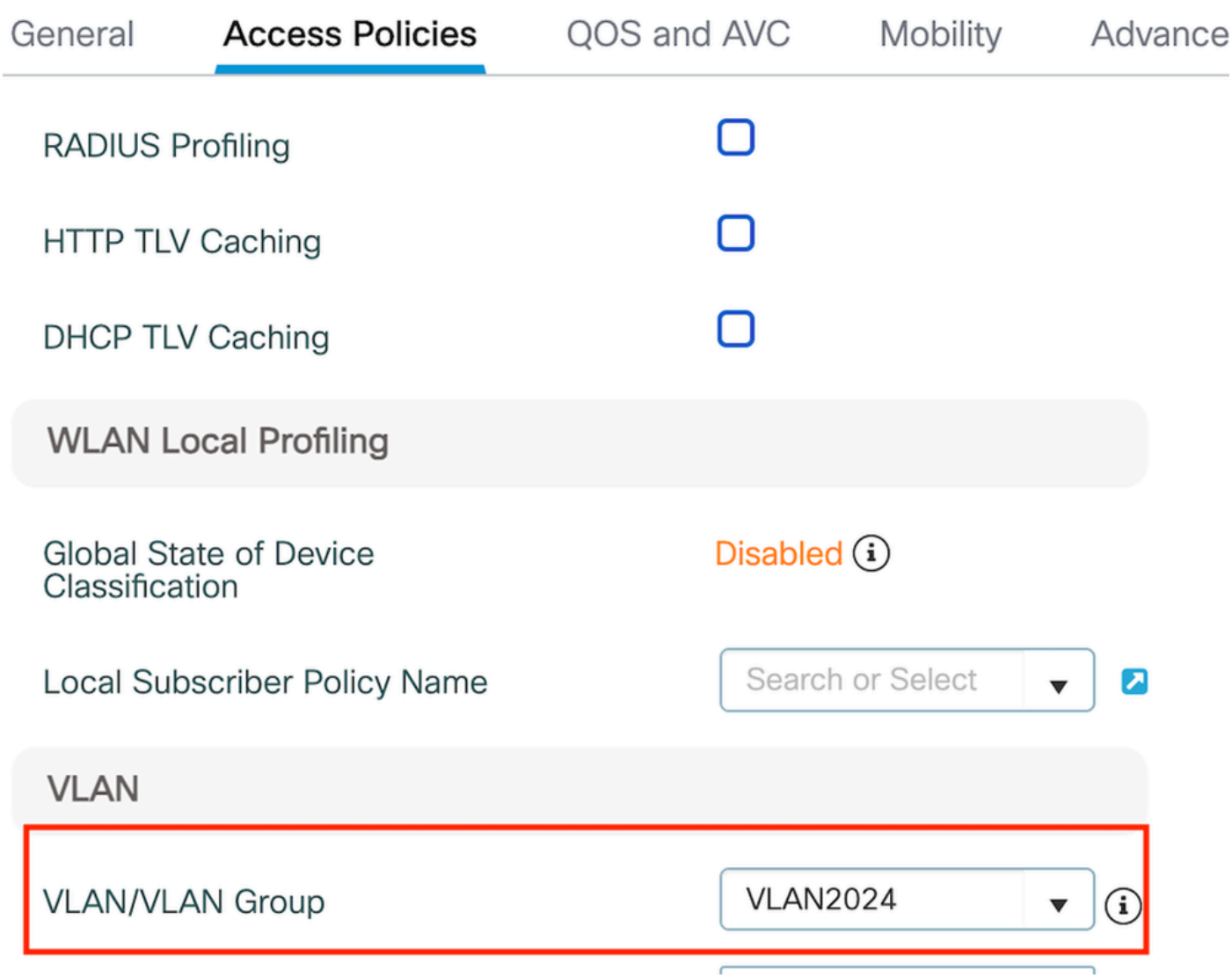
Configurer le profil de stratégie

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.

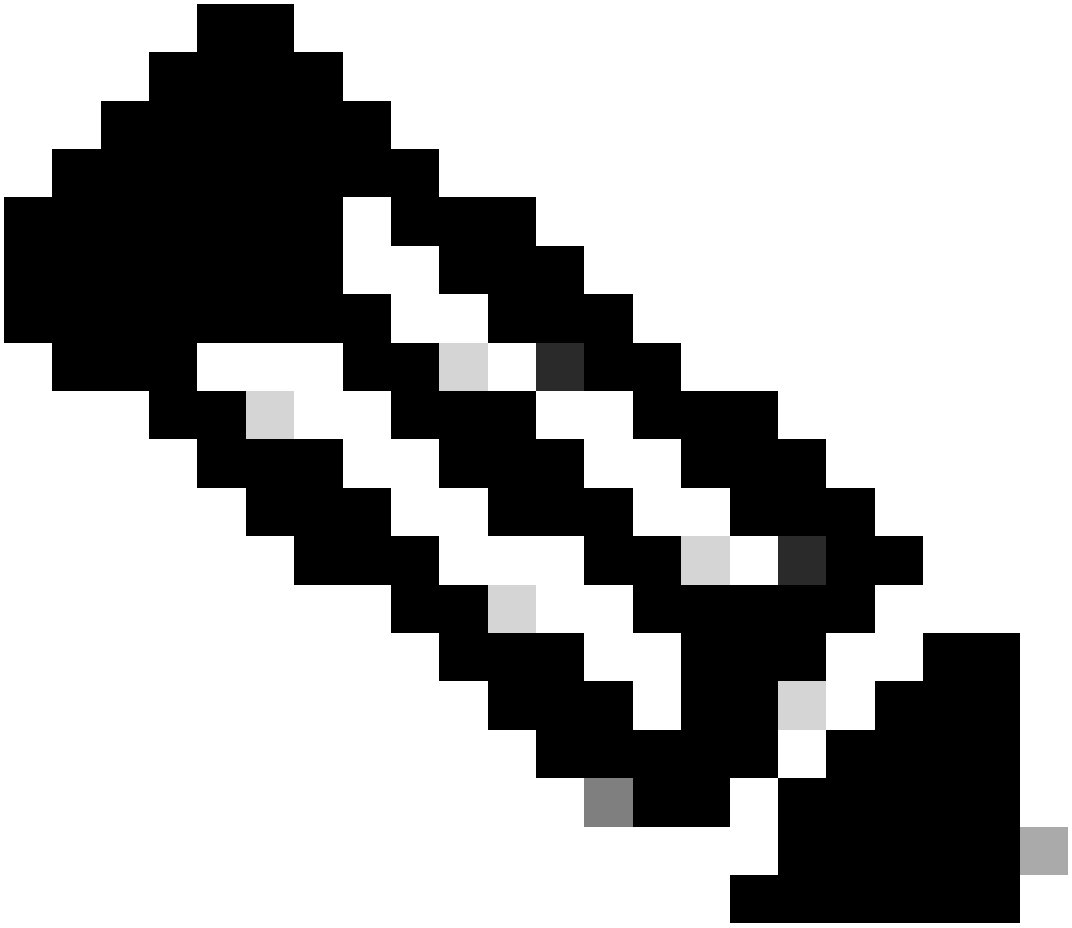


Profil de stratégie d'ancrage

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

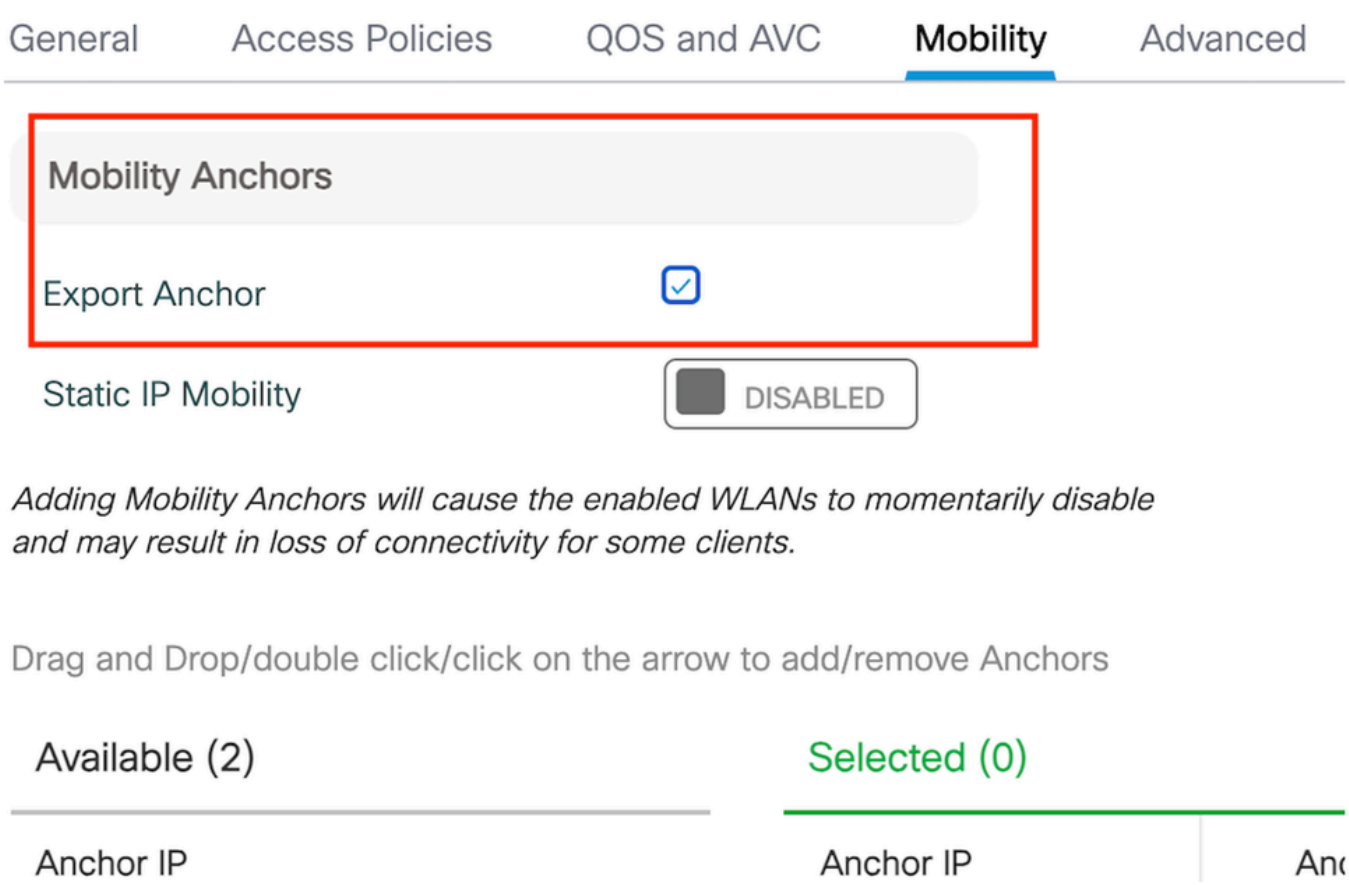


Onglet Access Policies

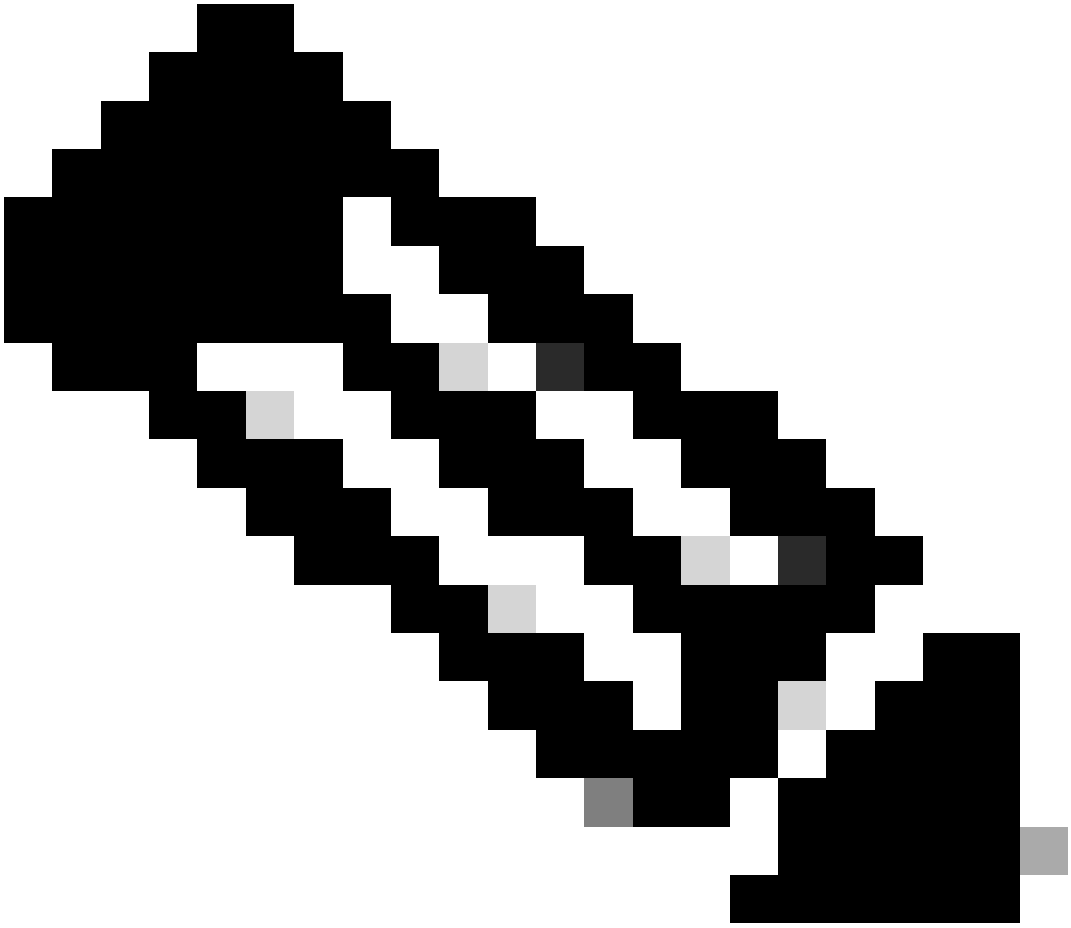


Remarque : la configuration du profil de stratégie doit correspondre sur les contrôleurs Foreign et Anchor, à l'exception du VLAN.

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



Exporter l'ancre



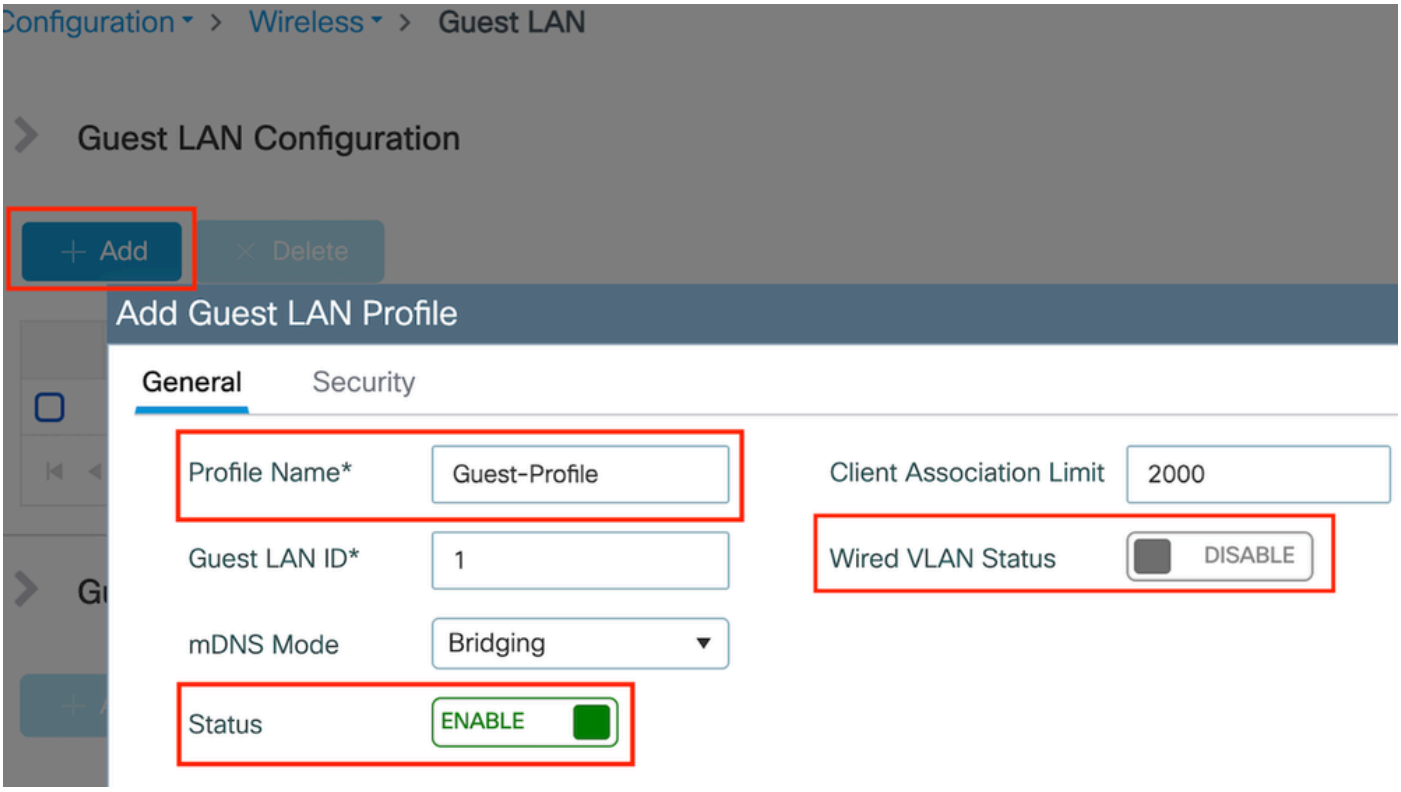
Remarque : cette configuration désigne le contrôleur de réseau local sans fil (WLC) 9800 comme WLC d'ancrage pour tout WLAN associé au profil de stratégie spécifié. Lorsqu'un WLC 9800 étranger redirige les clients vers le WLC d'ancrage, il fournit des détails sur le WLAN et le profil de stratégie attribué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

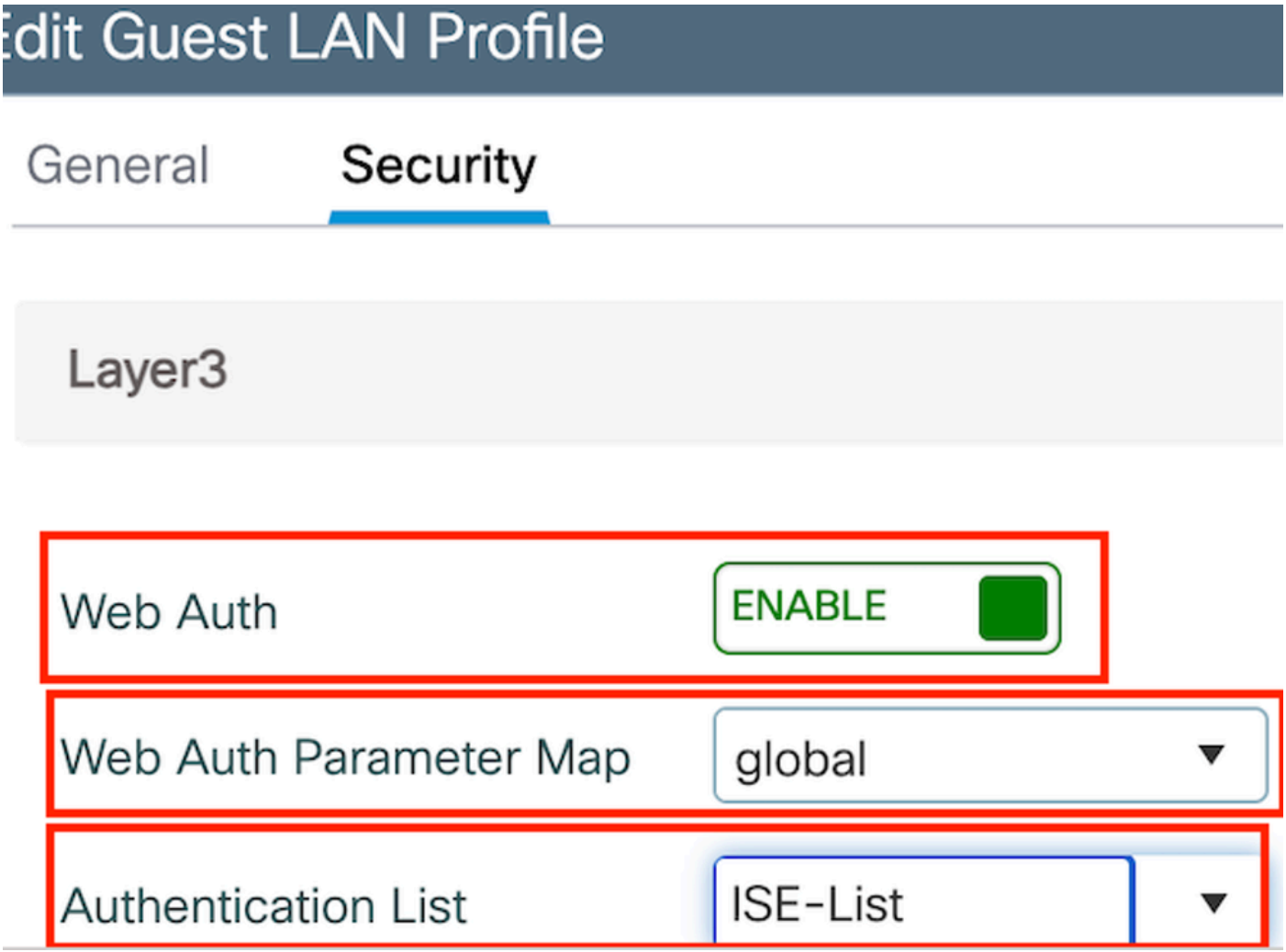
Configuration du profil de réseau local invité

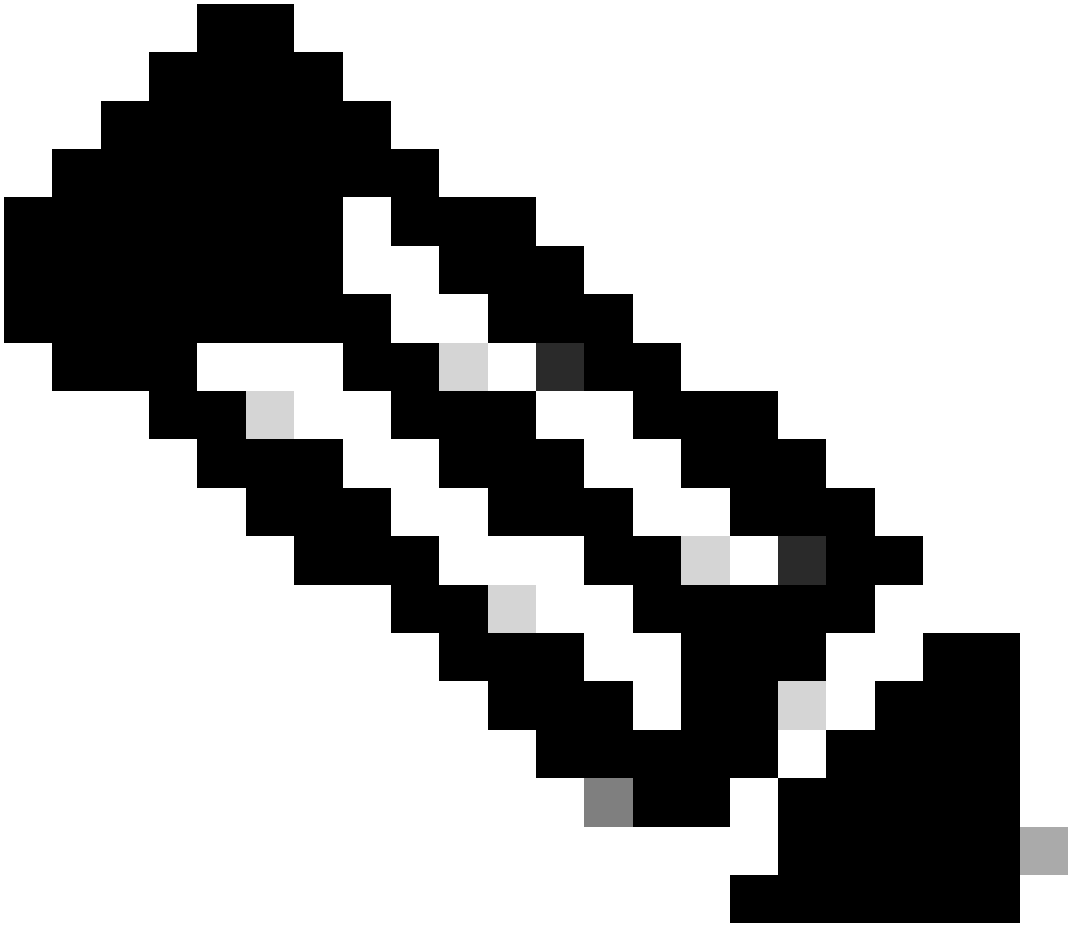
Étape 1 : Accédez à Configuration > Wireless > Guest LAN, puis sélectionnez Add pour créer et configurer le profil Guest LAN. Assurez-vous que le nom du profil correspond à celui du contrôleur étranger. Notez que le VLAN filaire doit être désactivé sur le contrôleur d'ancrage.



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



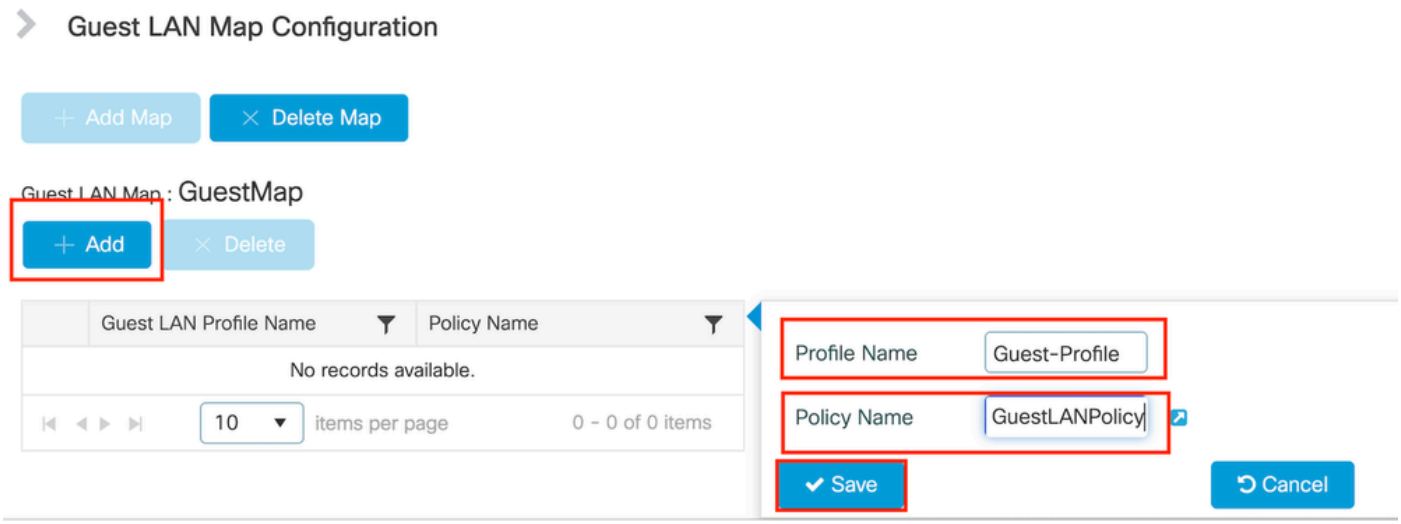
Remarque : la configuration du profil de réseau local invité doit être identique entre les contrôleurs Foreign et Anchor, à l'exception de l'état du réseau local virtuel câblé

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.



Plan du réseau local invité

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

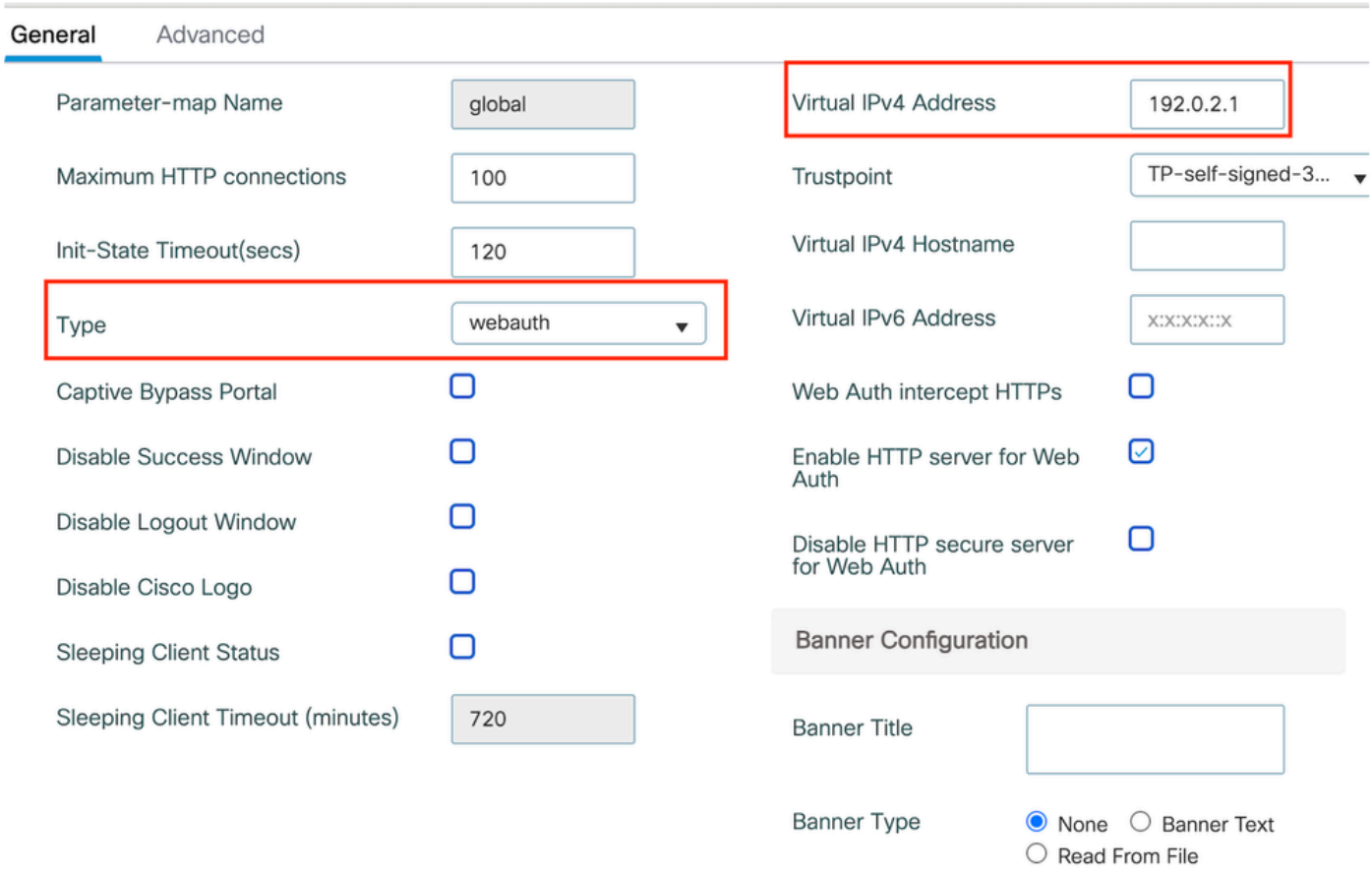
Configuration d'un invité filaire sur le catalyst 9800 ancré au contrôleur AireOS 5520

Topologie du réseau

Configuration sur le WLC 9800 étranger

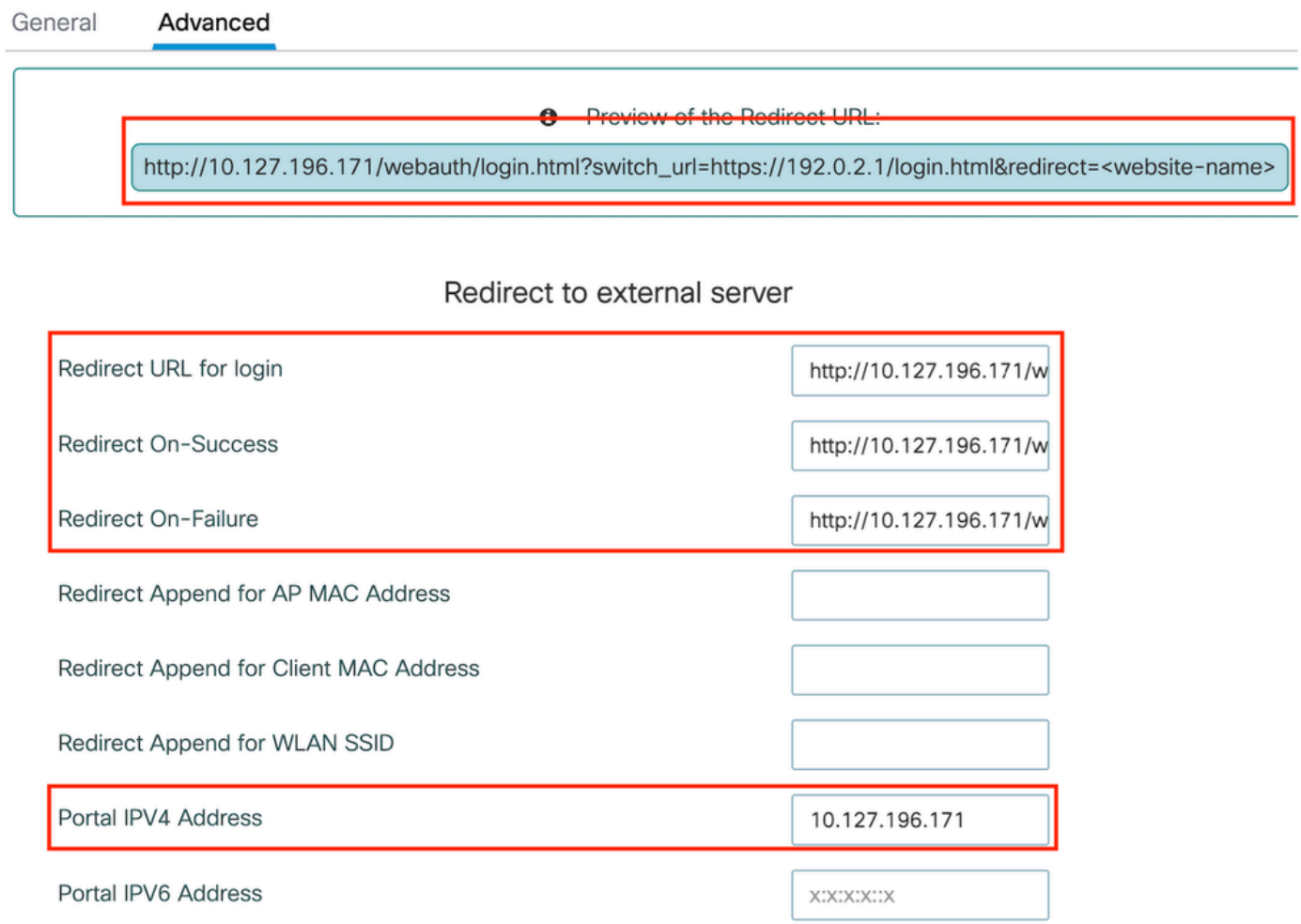
Configurer la carte de paramètres Web

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.



Carte de paramètre Web

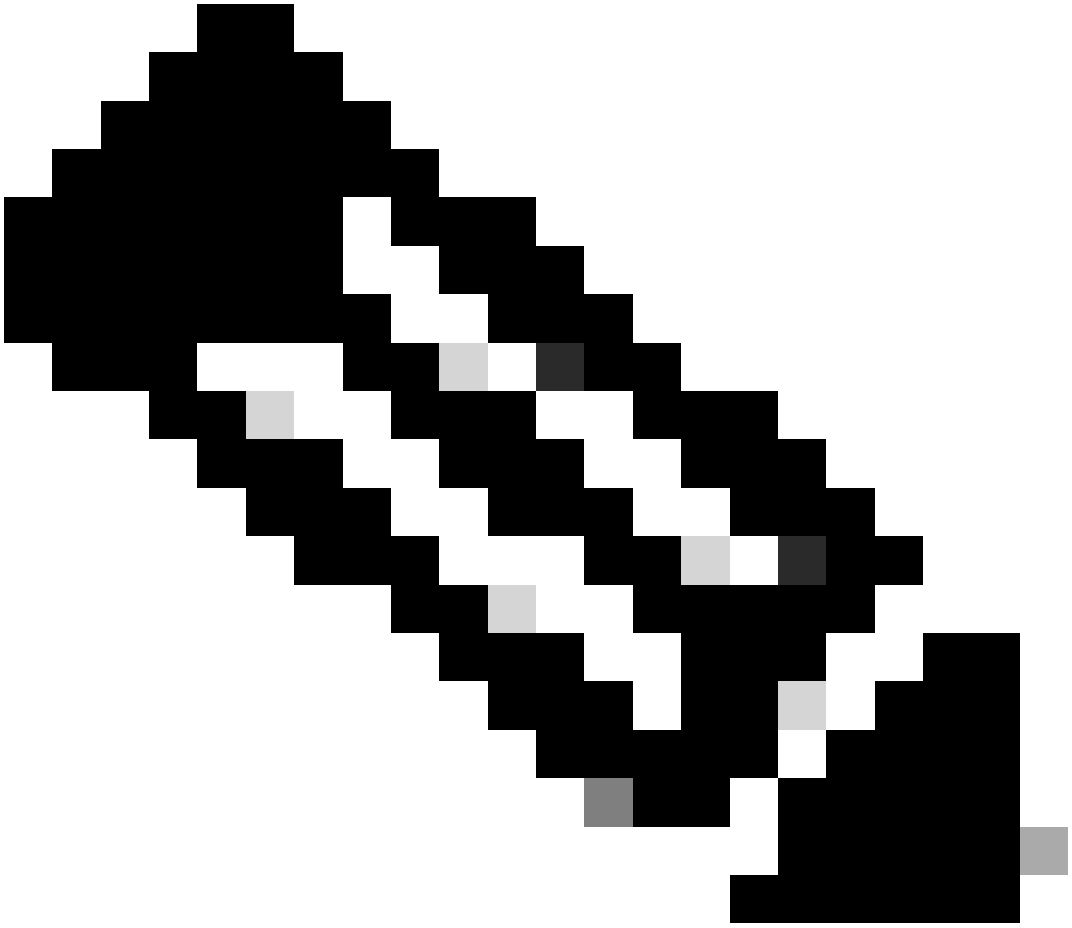
Étape 2 : Sous l'onglet Advanced, spécifiez l'URL de la page Web externe vers laquelle les clients doivent être redirigés. Configurez l'URL de redirection pour la connexion et la redirection en cas d'échec. Le paramètre Redirect On-Success est une configuration facultative.



Onglet Avancé

Configuration CLI

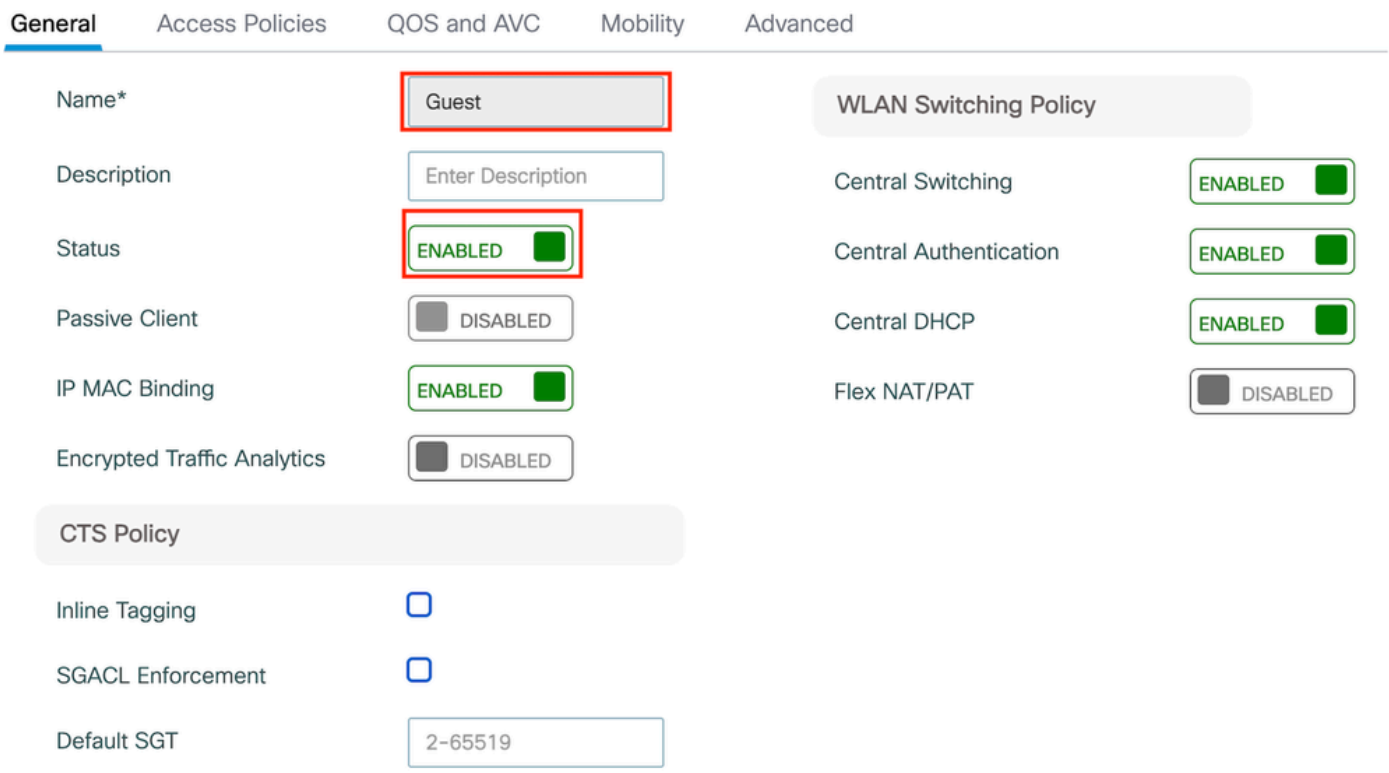
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171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

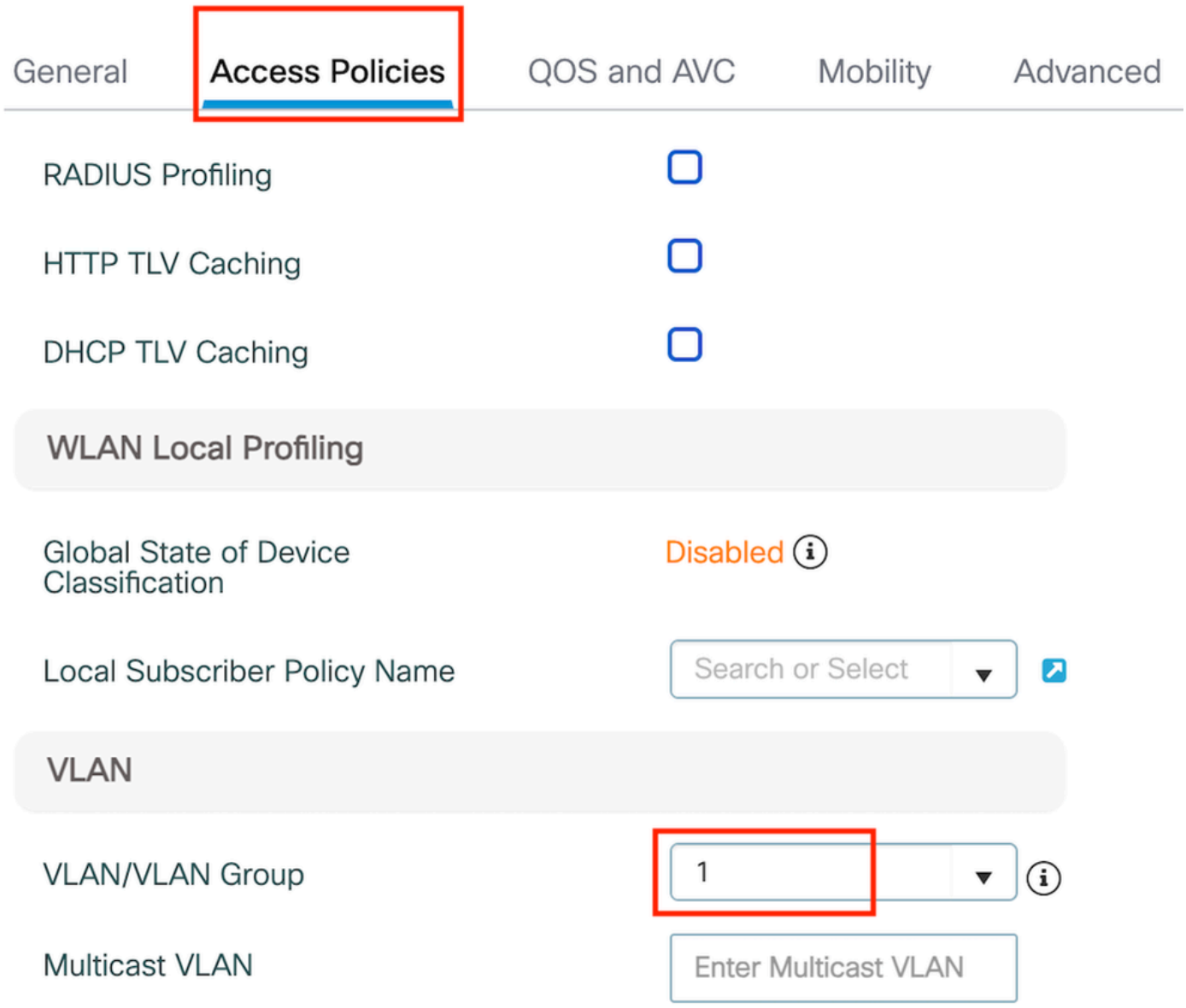
Configurer le profil de stratégie

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.



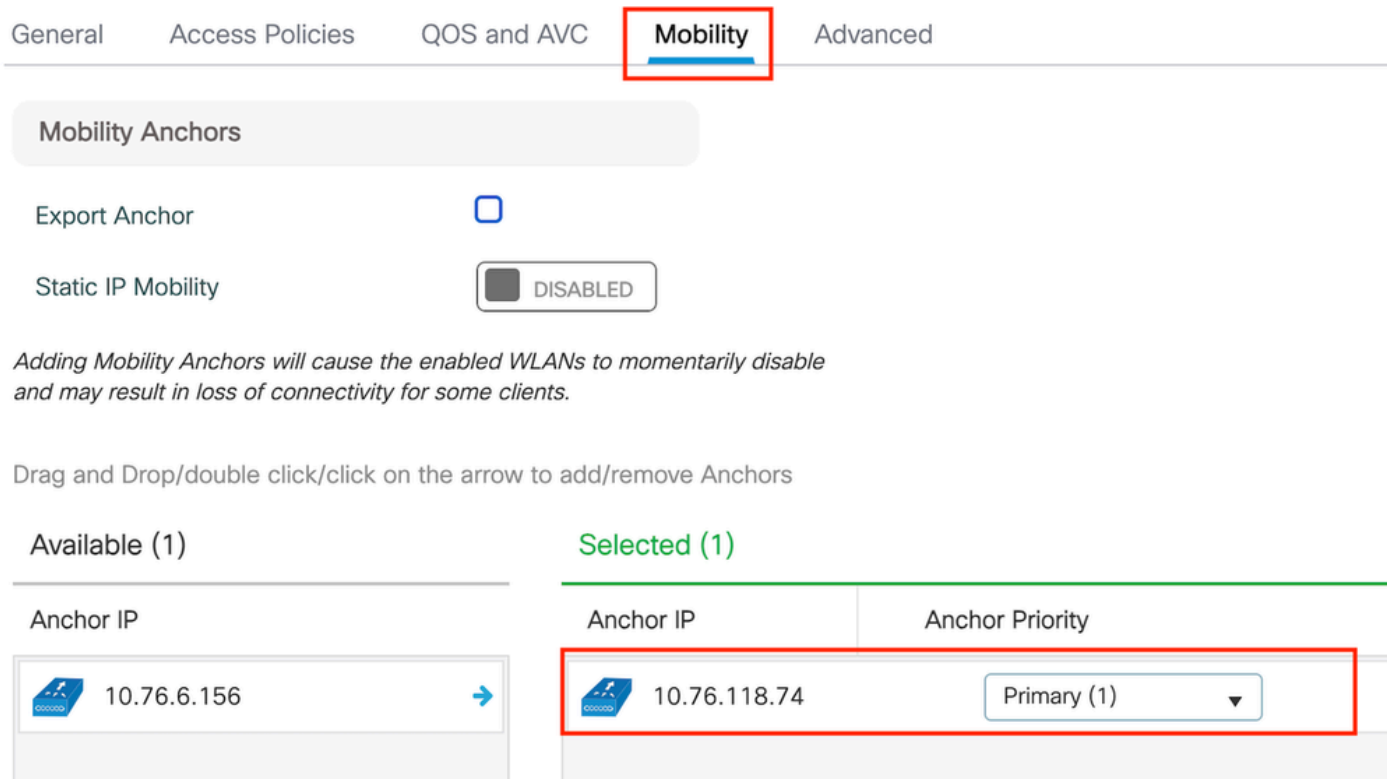
Profil de stratégie

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

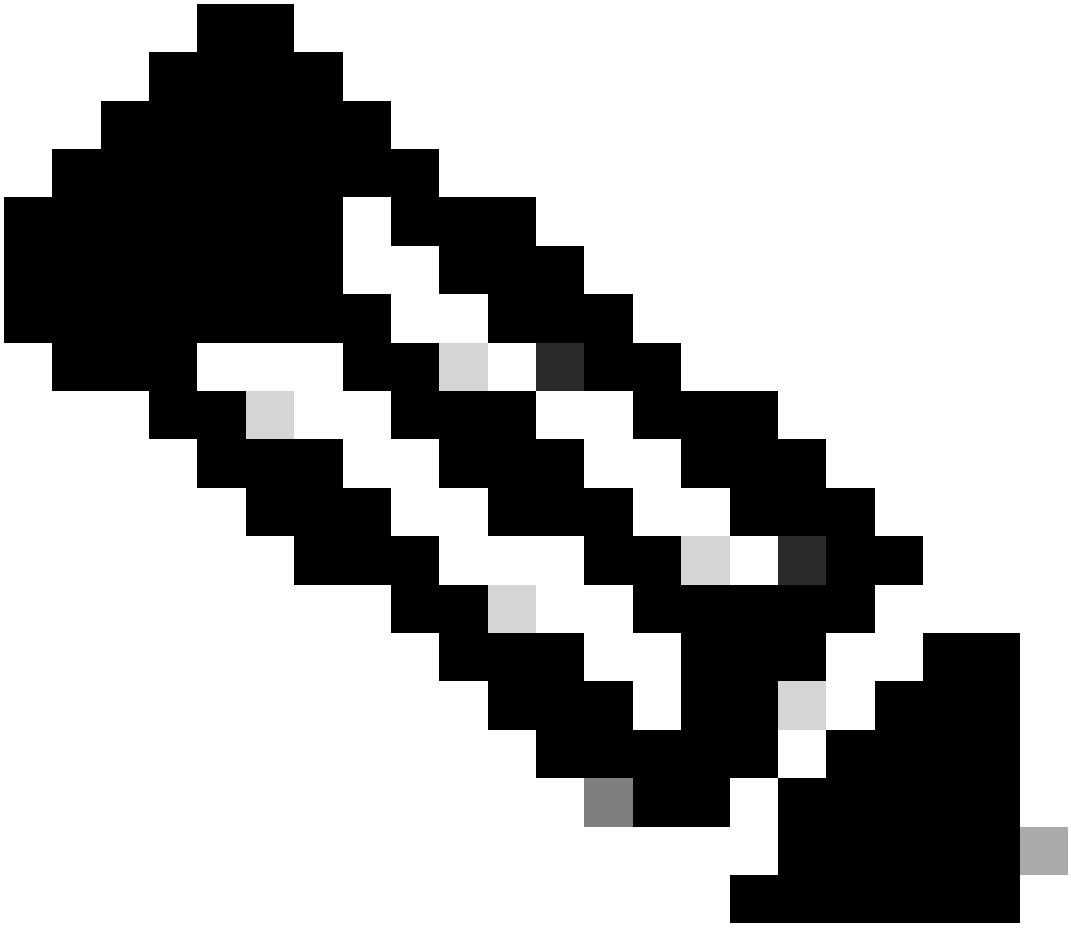


Politiques d'accès

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



Onglet Mobilité



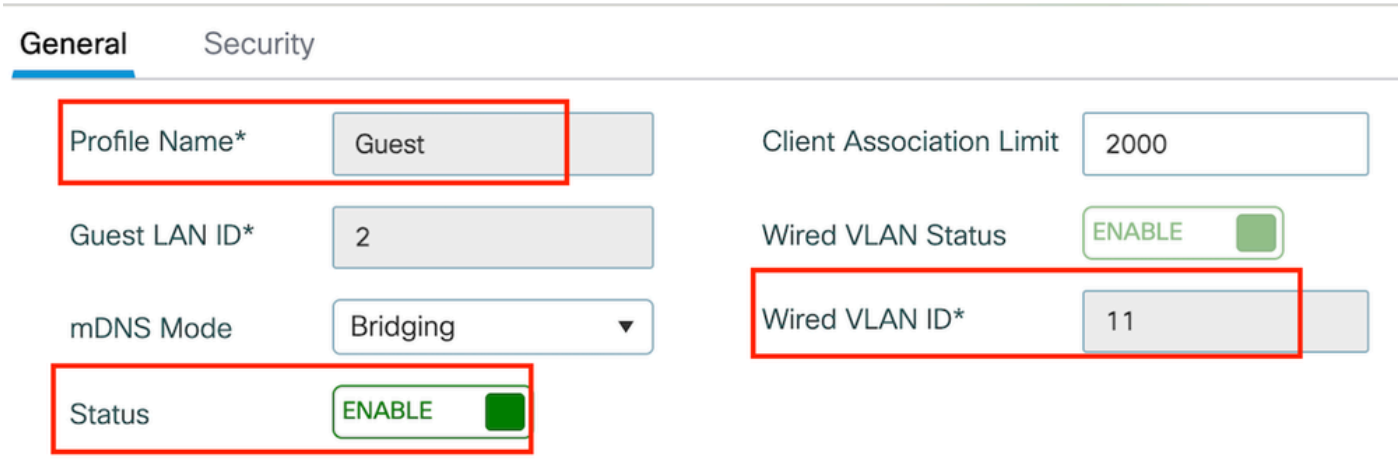
Remarque : le profil de stratégie du WLC étranger 9800 doit correspondre au profil de réseau local invité du WLC d'ancrage 5520, à l'exception de la configuration de réseau local virtuel

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
```

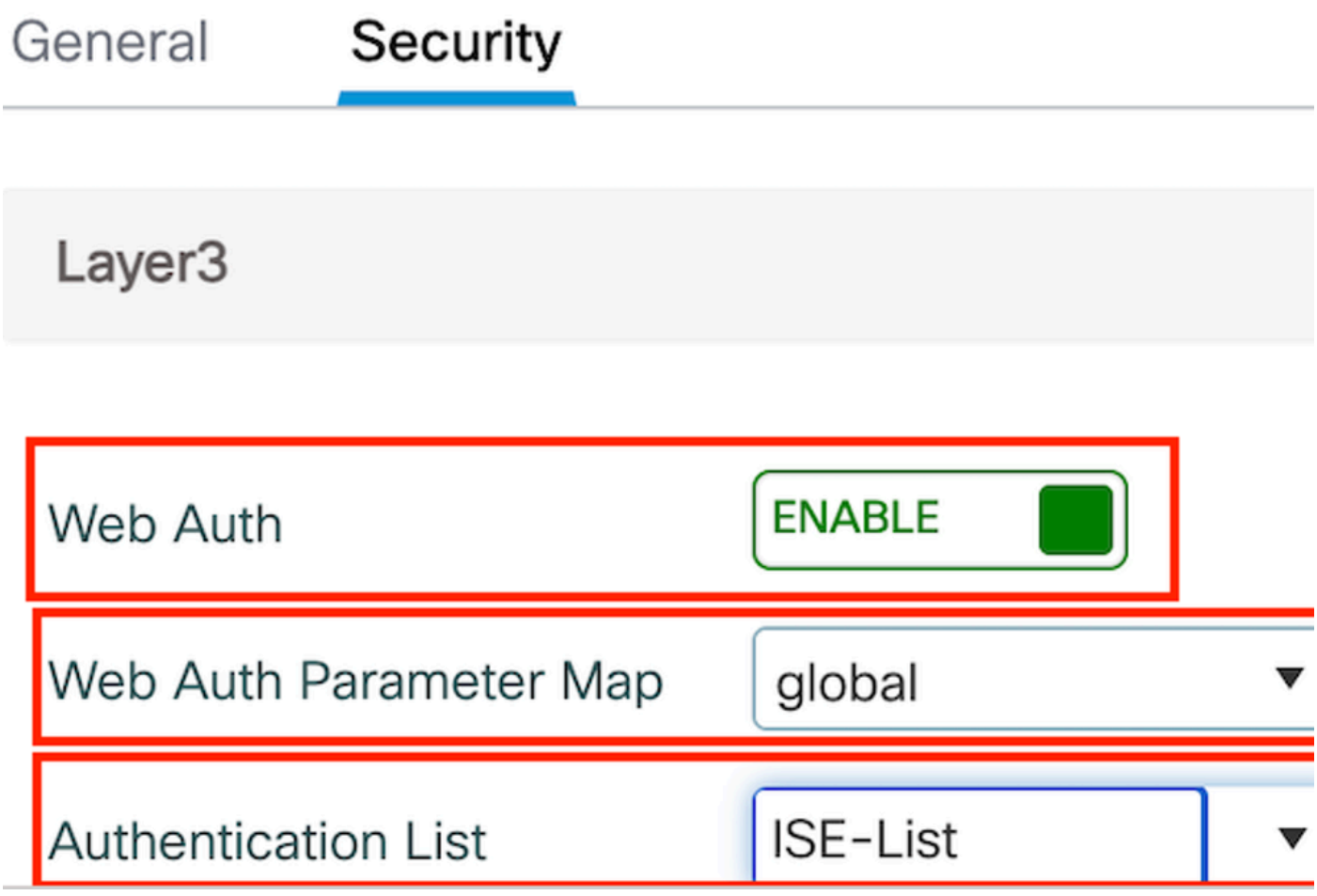
Configurer le profil de réseau local invité

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.

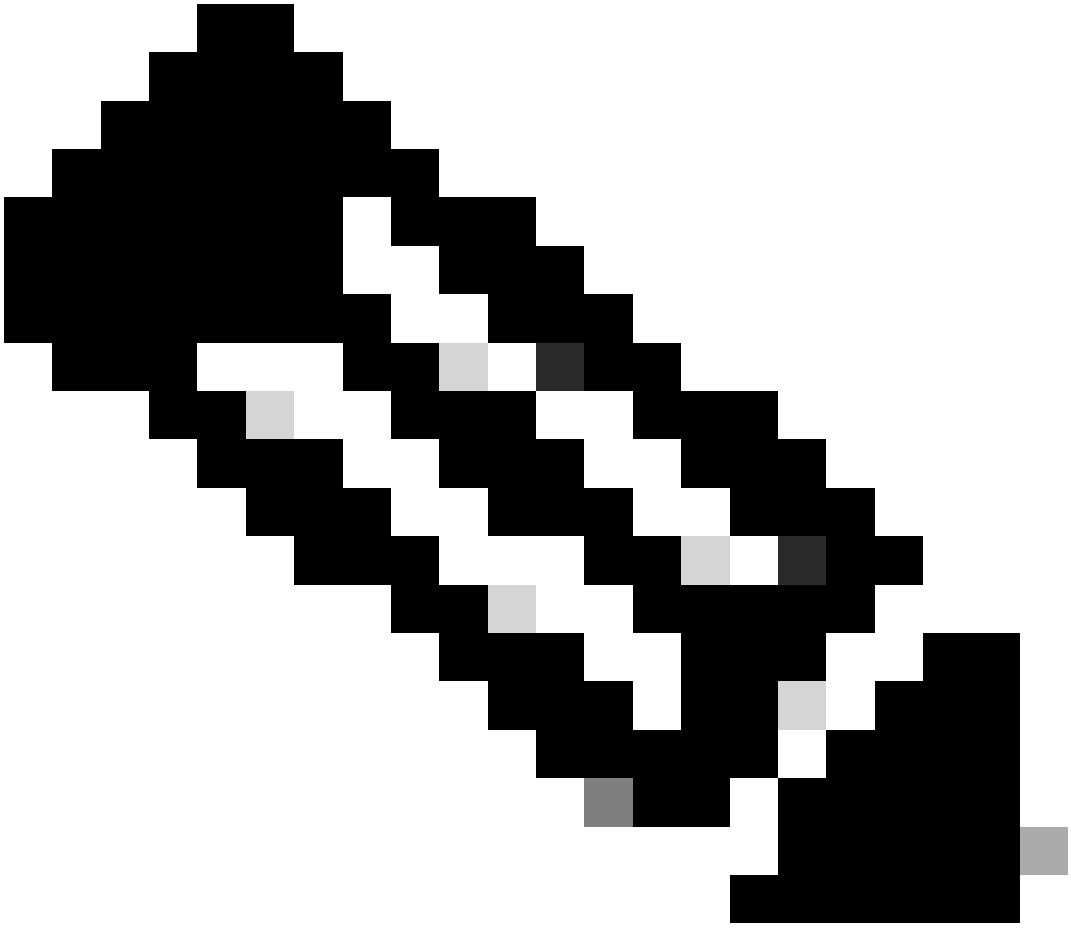


Politique de réseau local invité

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.



Onglet Sécurité



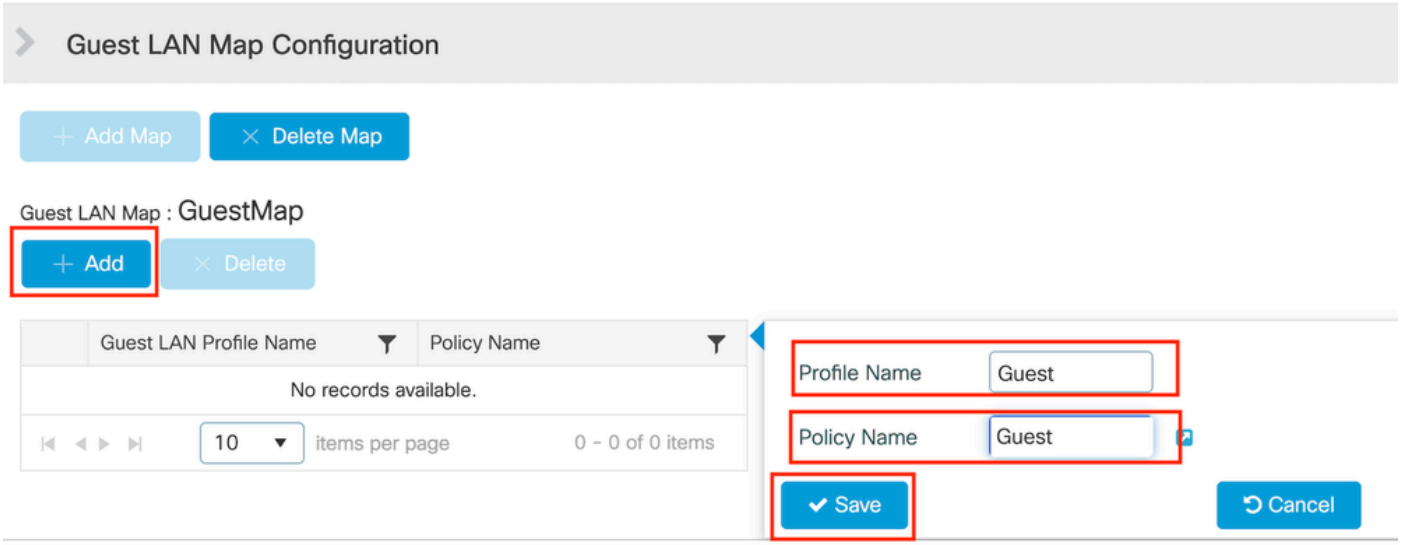
Remarque : le nom du profil de réseau local invité doit être identique pour le contrôleur d'ancrage 9800 étranger et 5520

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.



Plan du réseau local invité

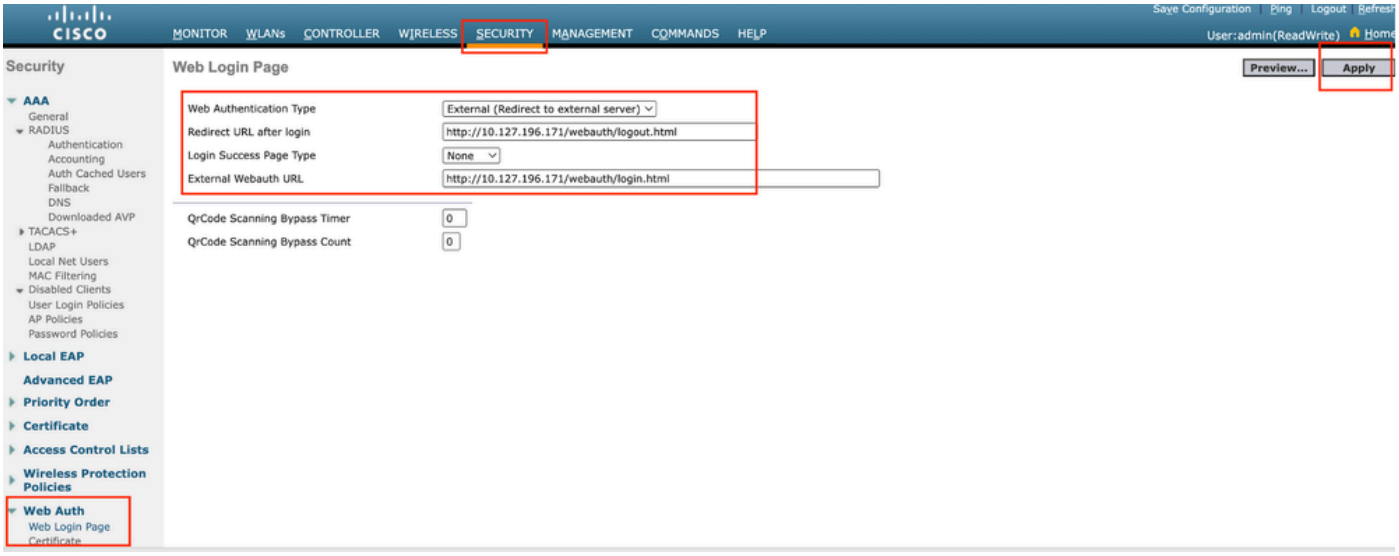
Configuration CLI

```
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.

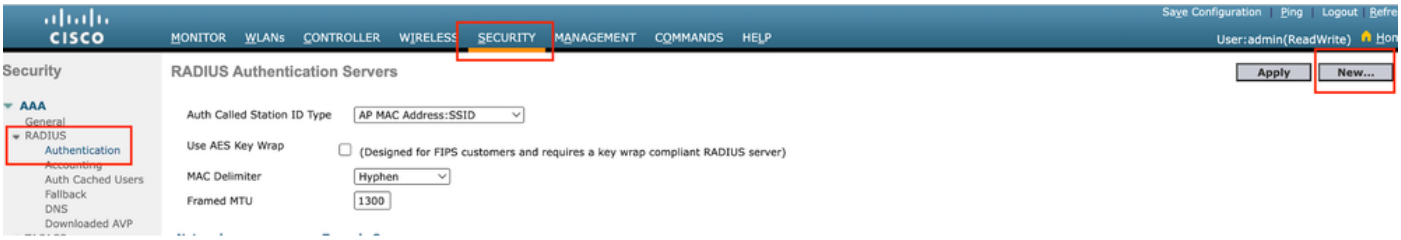


Paramètres d'authentification Web

Paramètres AAA :

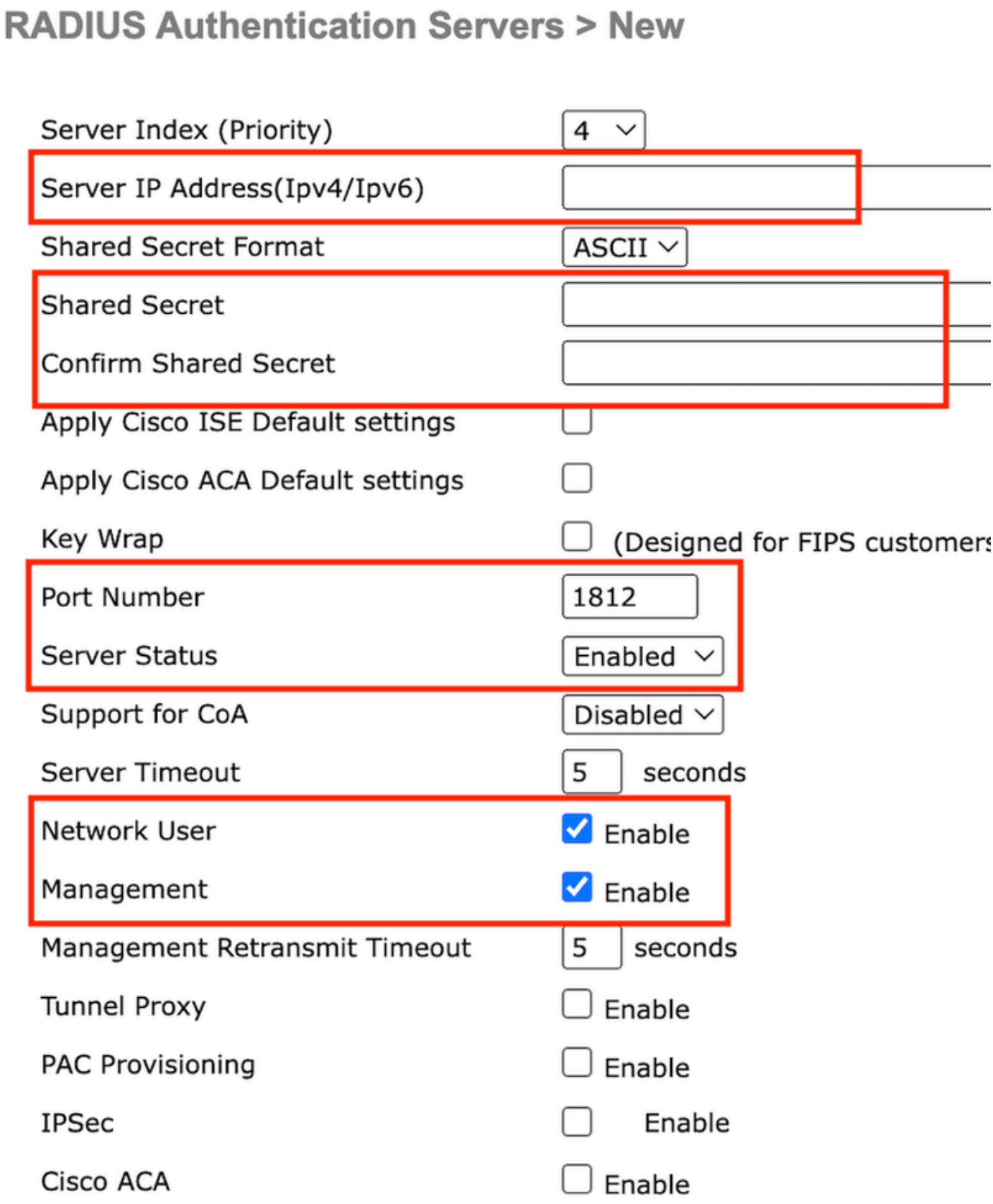
Étape 1 : configurez le serveur RADIUS

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.

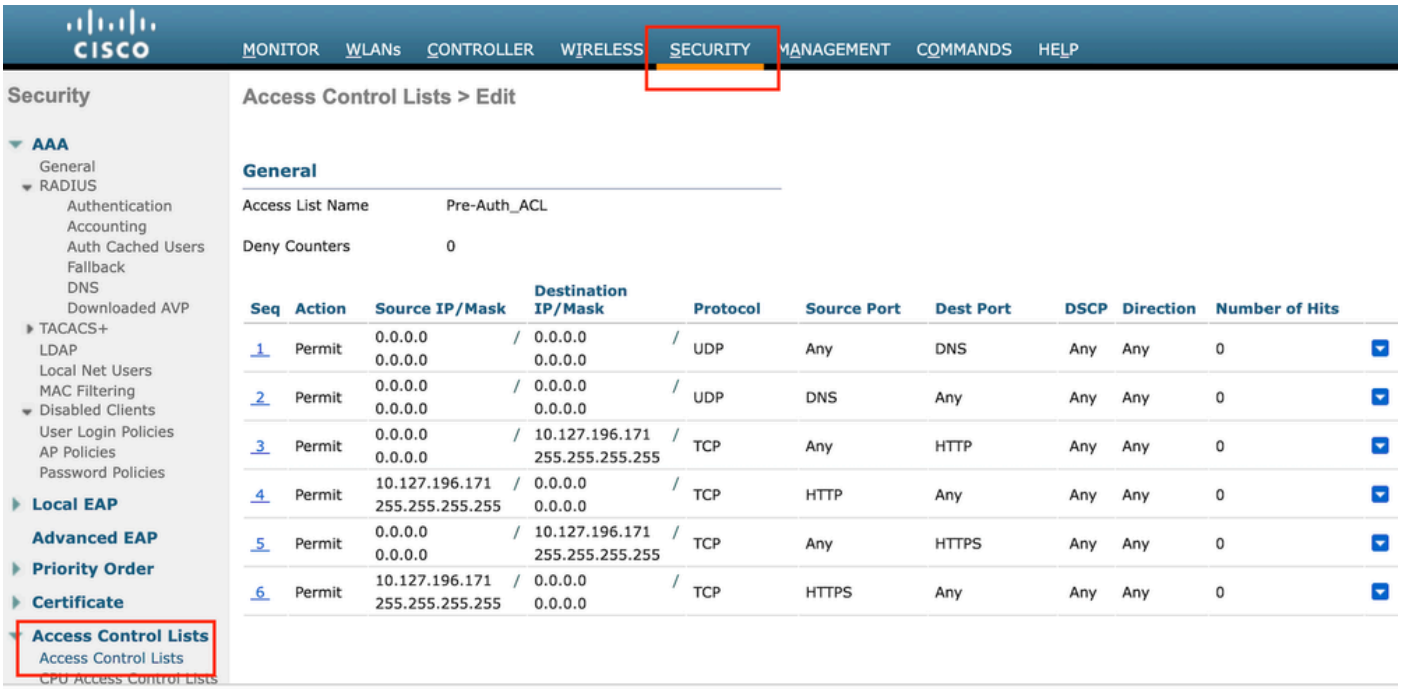


Configuration du serveur

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.



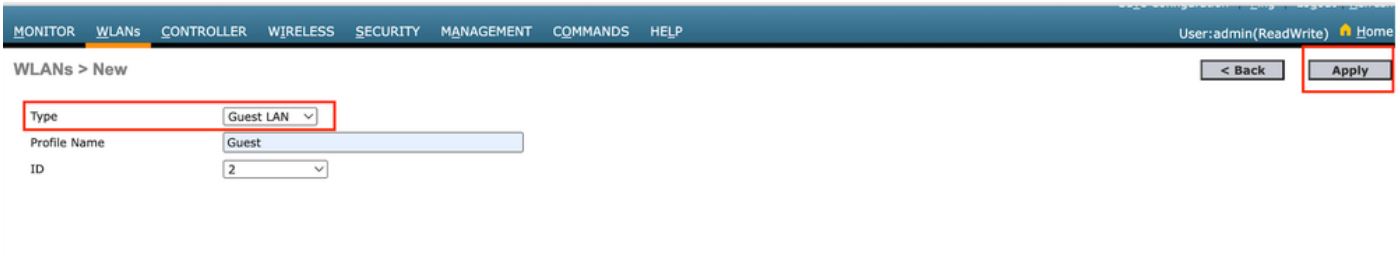
Liste d'accès pour autoriser le trafic vers le serveur Web

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.

Créer un réseau local invité

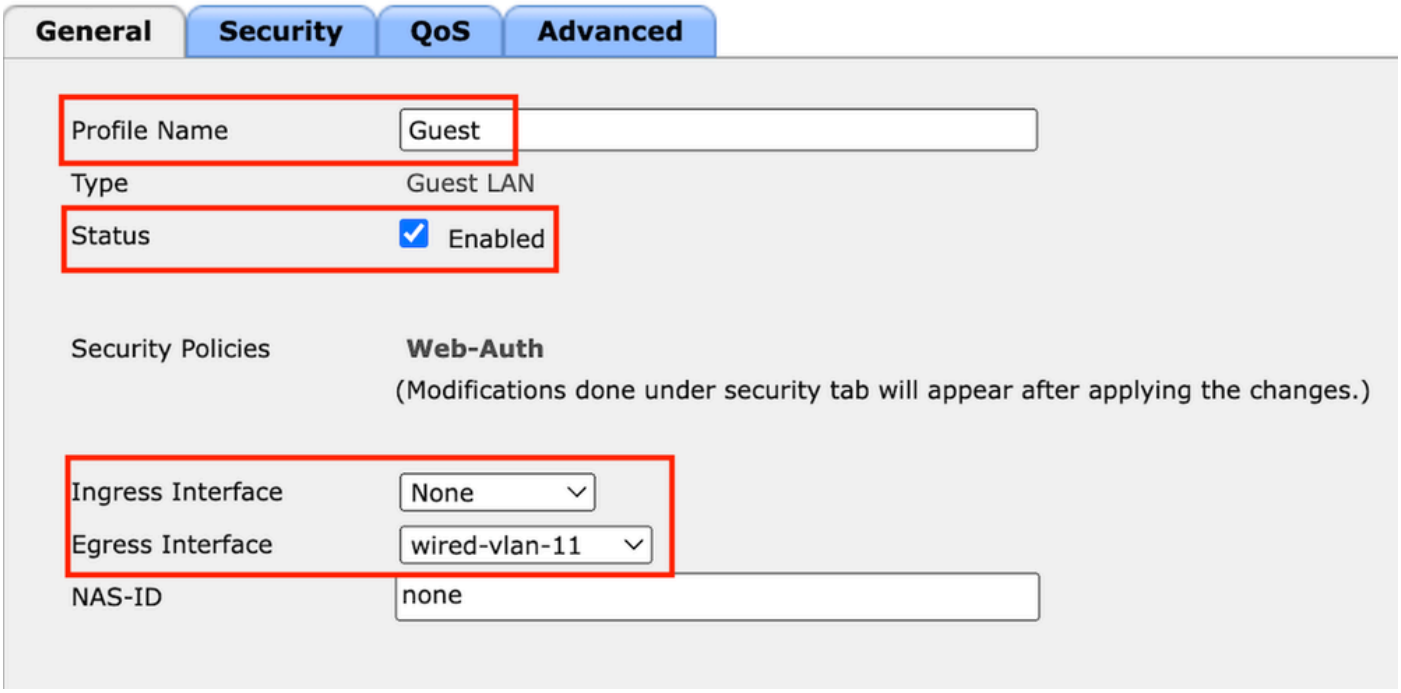


Profil de réseau local invité

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

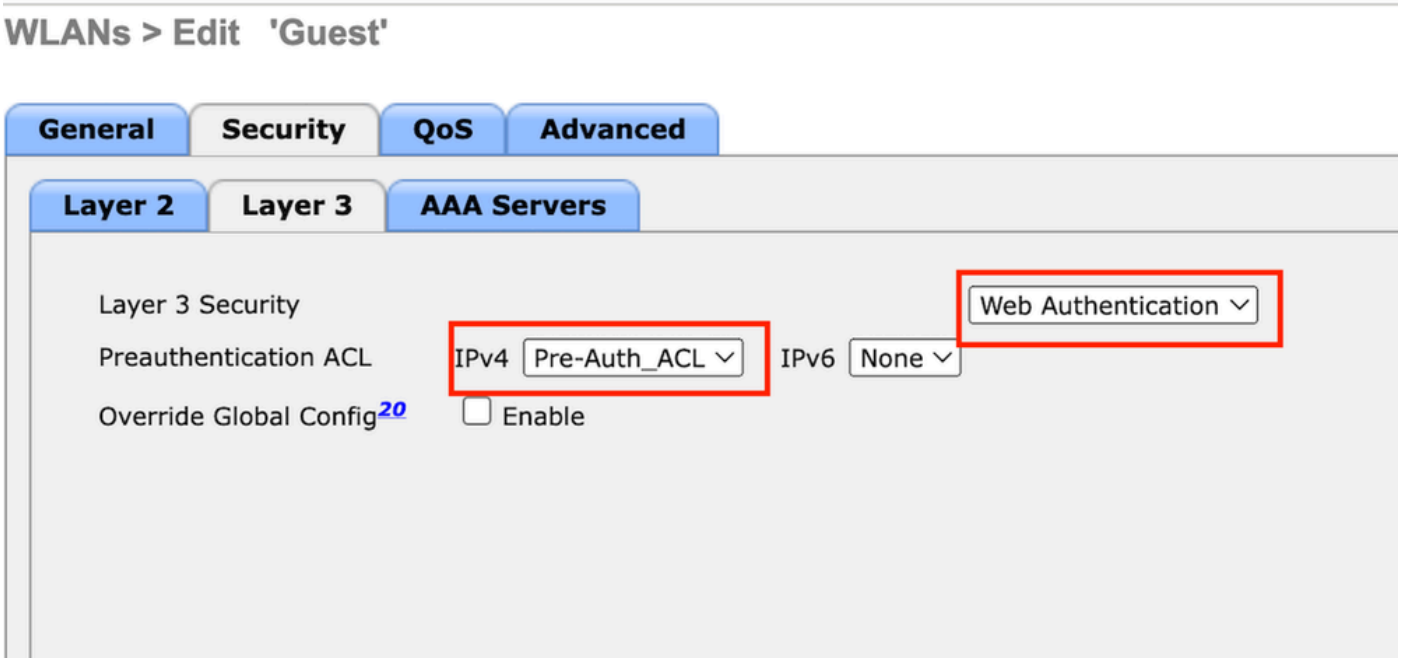
Dans ce cas, l'interface d'entrée est none, car elle correspond au tunnel EoIP du contrôleur étranger.

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



Profil de réseau local invité

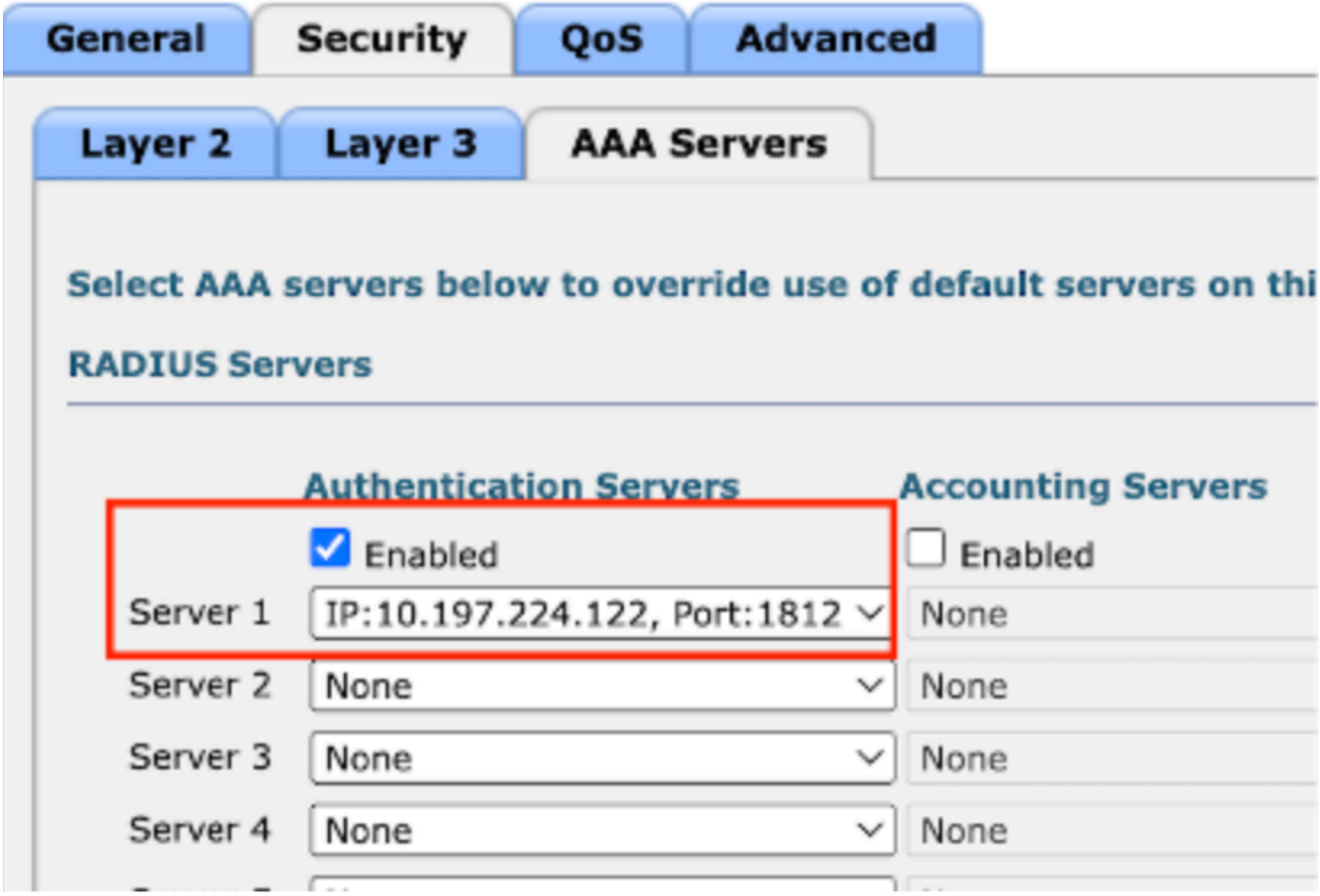
Étape 3 : Sous l'onglet Security, sélectionnez Layer 3 security as Web Authentication et mappez la liste de contrôle d'accès de pré-authentification.



Onglet Sécurité du réseau local invité

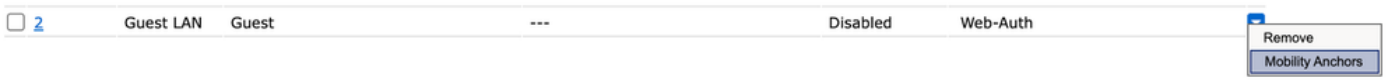
Étape 4 : Accédez à Security > AAA Server.

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'ancre de mobilité

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

Topologie du réseau

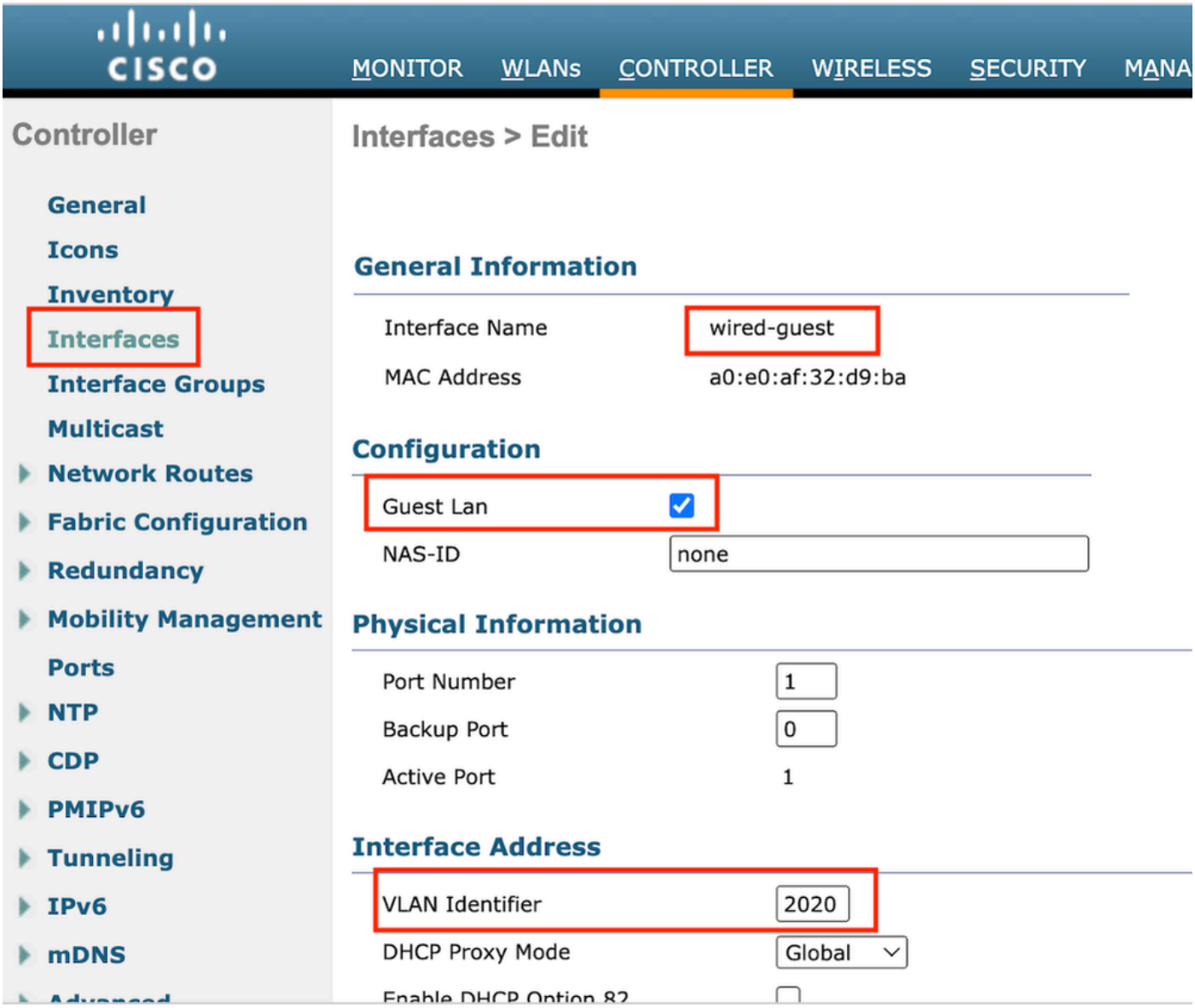
Configuration sur le WLC étranger 5520

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.

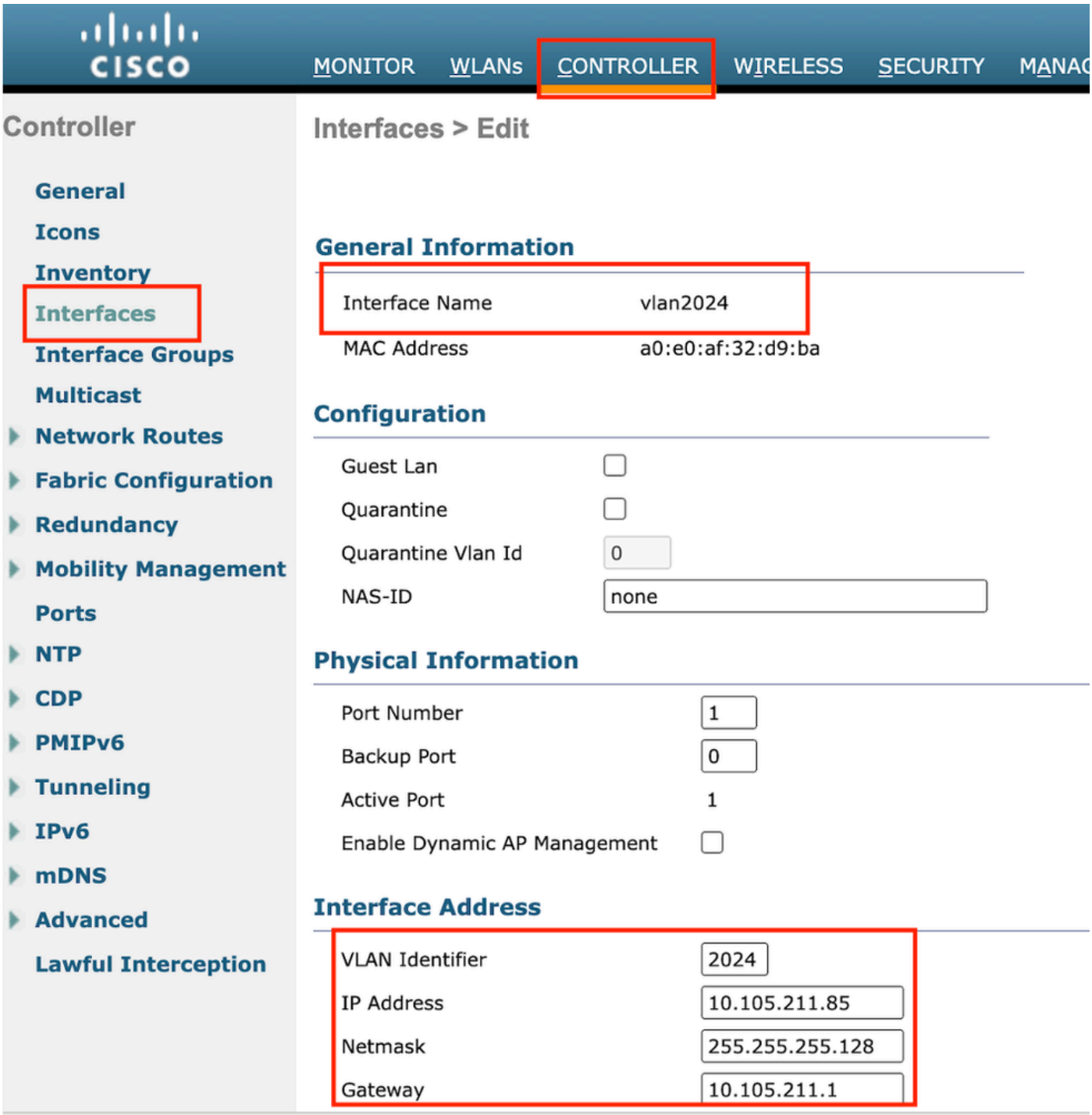
Commencez par créer une interface dynamique de couche 2 et désignez-la comme réseau local invité. Cette interface sert d'interface d'entrée pour le réseau local invité, où les clients filaires se connectent physiquement.



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.



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

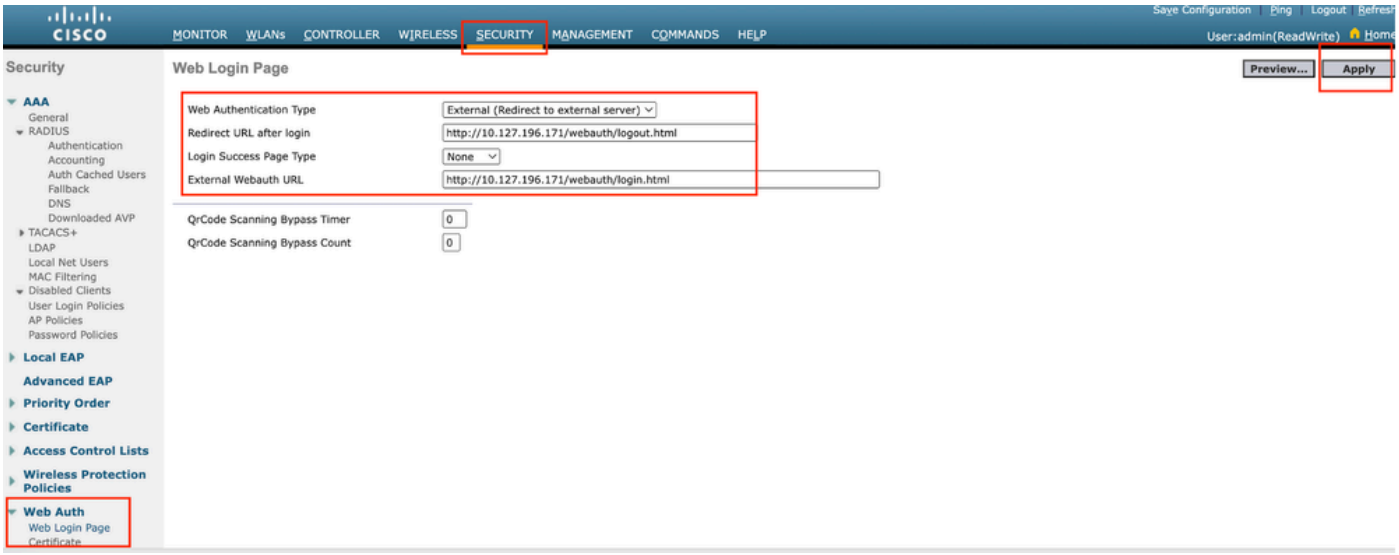
switchport trunk native vlan 2081

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.

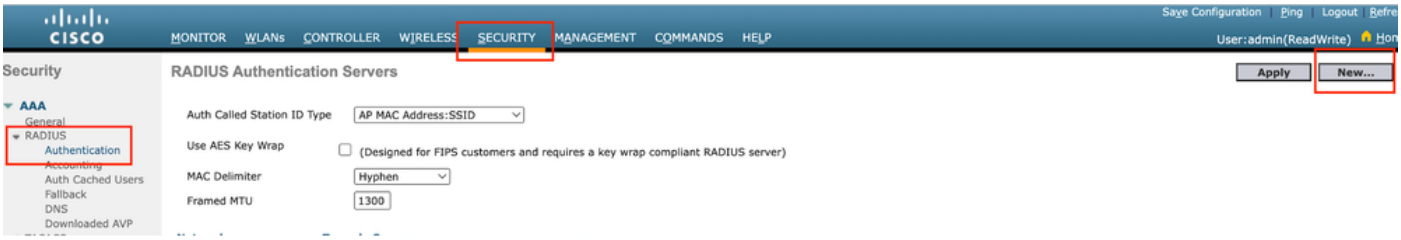


Paramètres d'authentification Web

Paramètres AAA :

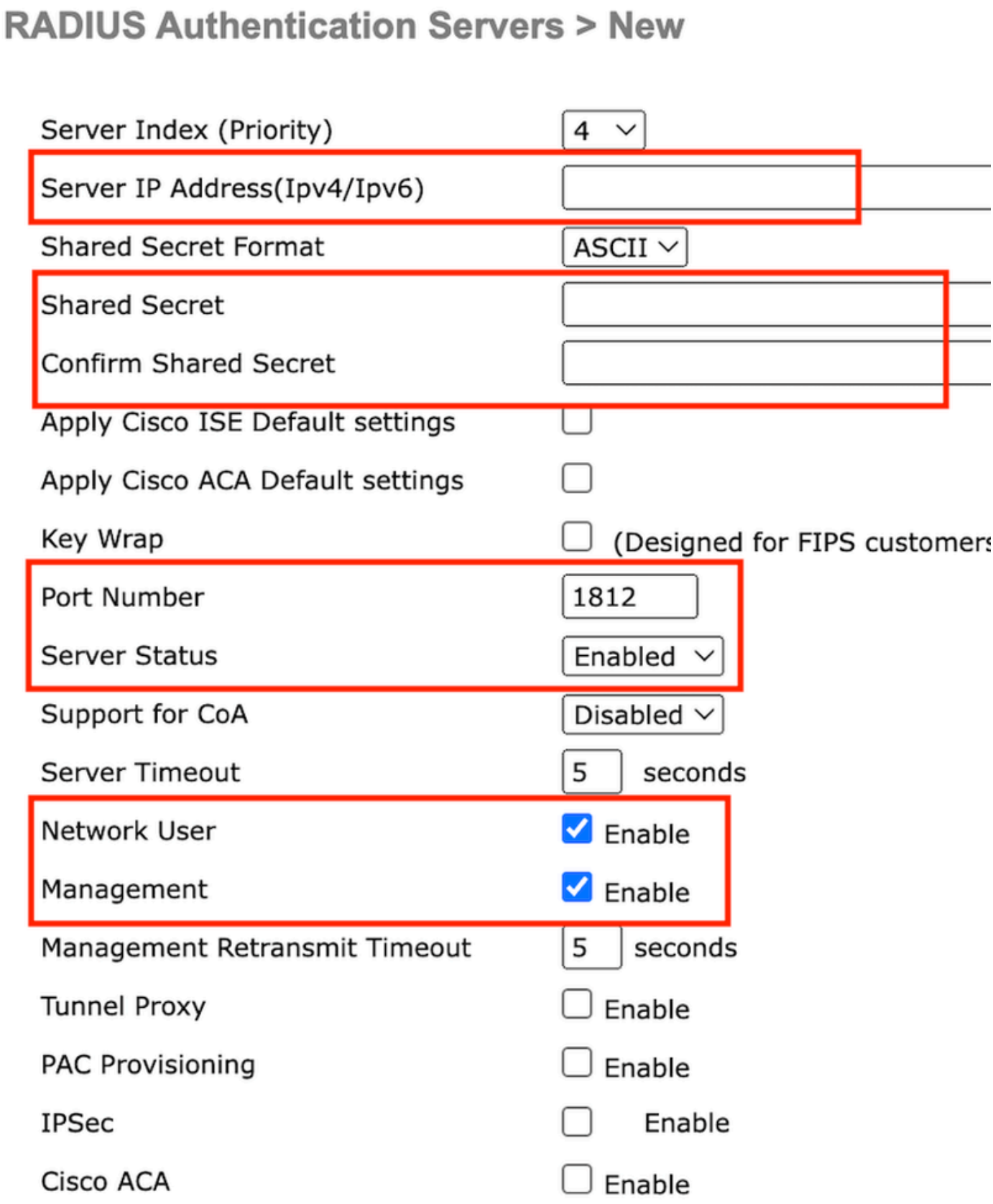
Étape 1 : configurez le serveur RADIUS

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.

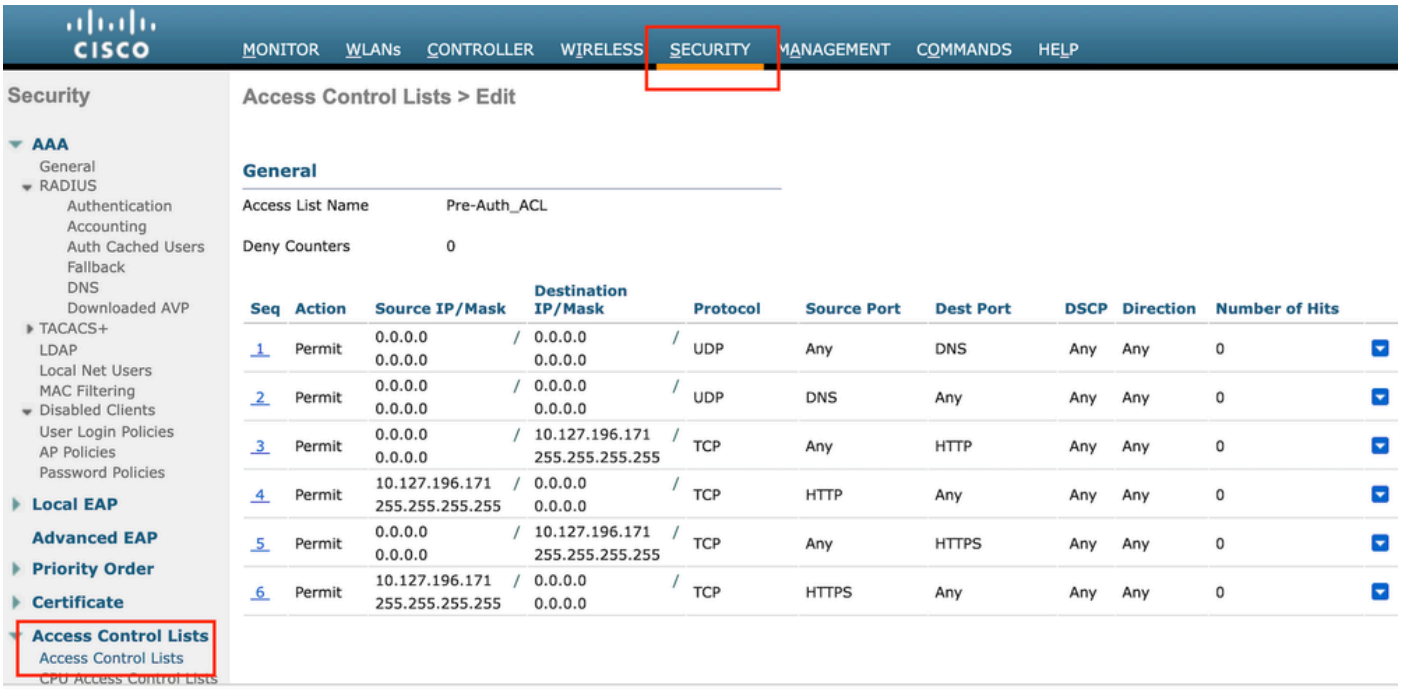


Configuration du serveur

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.



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.

Profil de réseau local invité

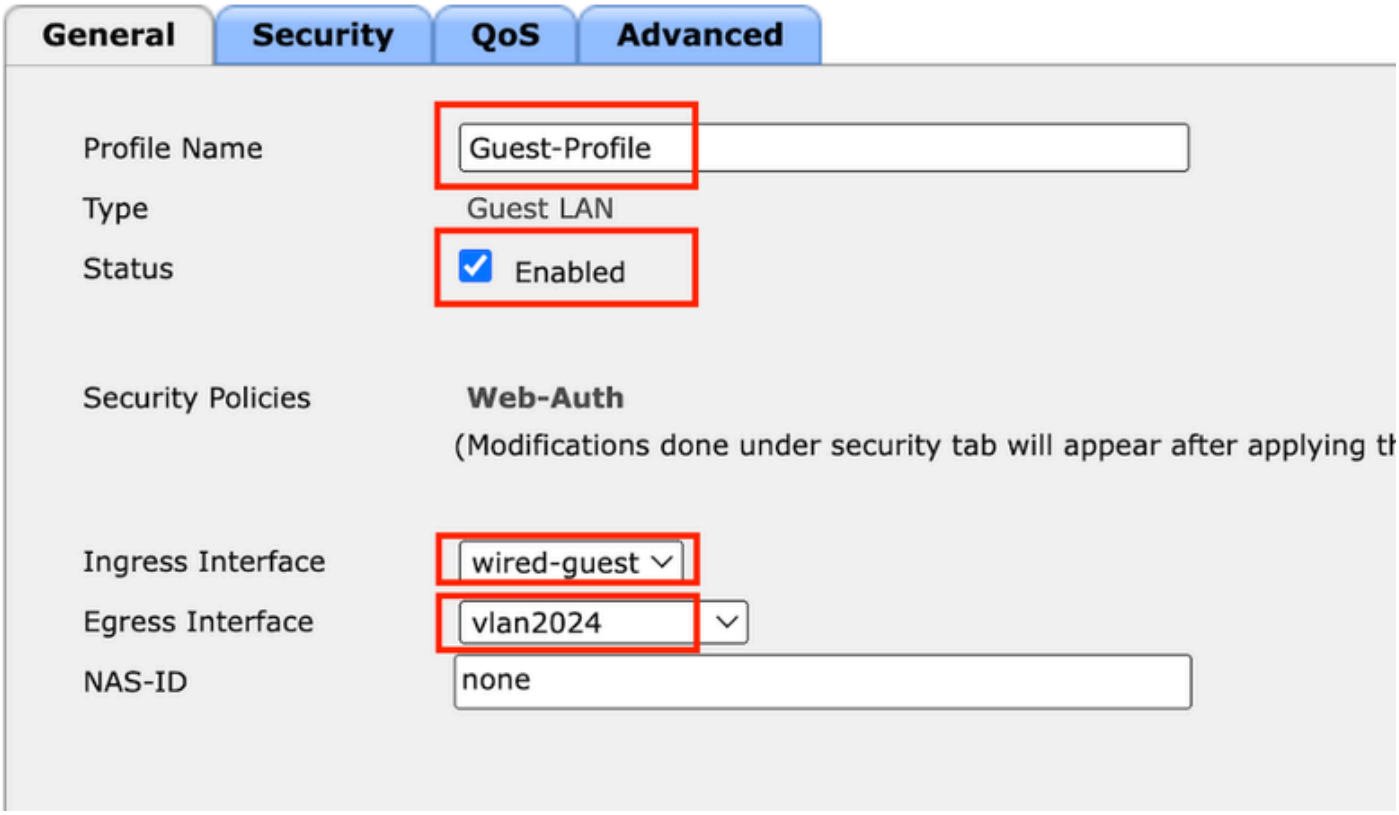
Sélectionnez Type en tant que réseau local invité et configurez un nom de profil. Le même nom doit être configuré sur le profil de stratégie et le profil de réseau local invité du contrôleur d'ancrage 9800.

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.

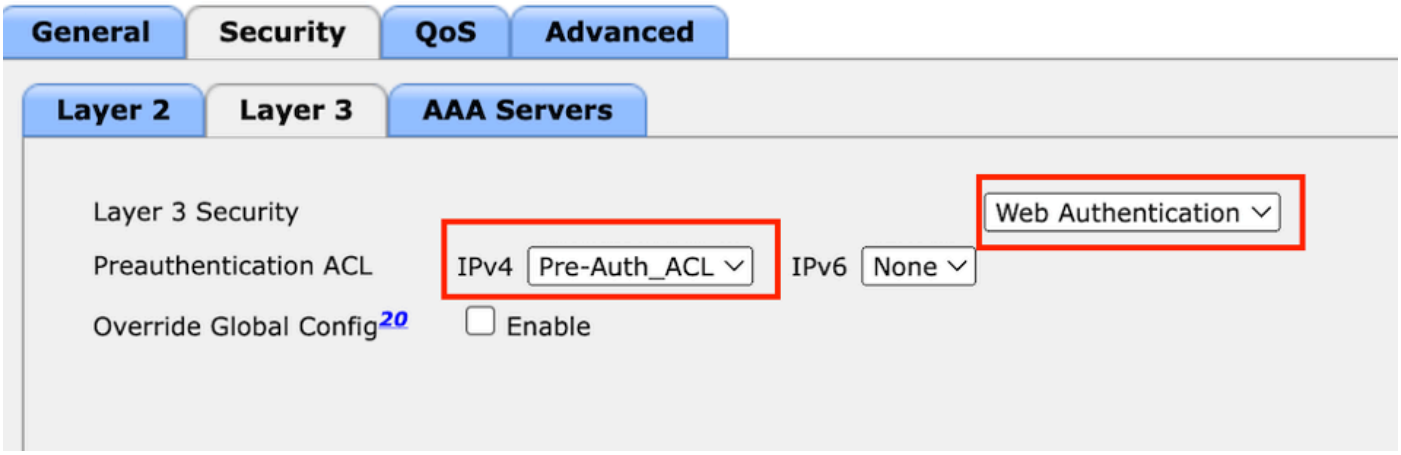


Profil de réseau local invité

Étape 3 : Accédez à Security > Layer 3.

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

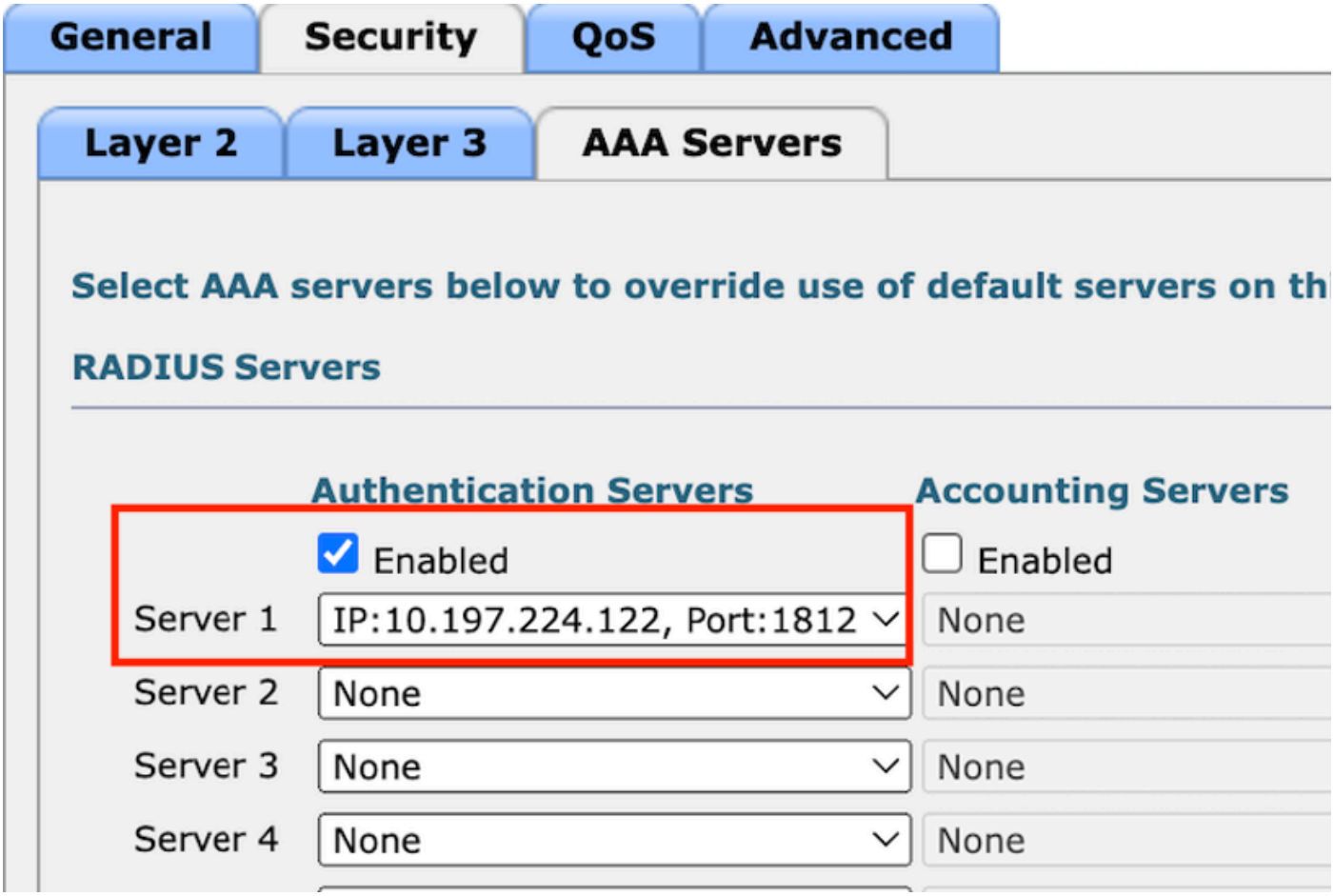
de pré-authentification.



Onglet Sécurité de couche 3

Étape 4 :

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



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.

Ancres de mobilité

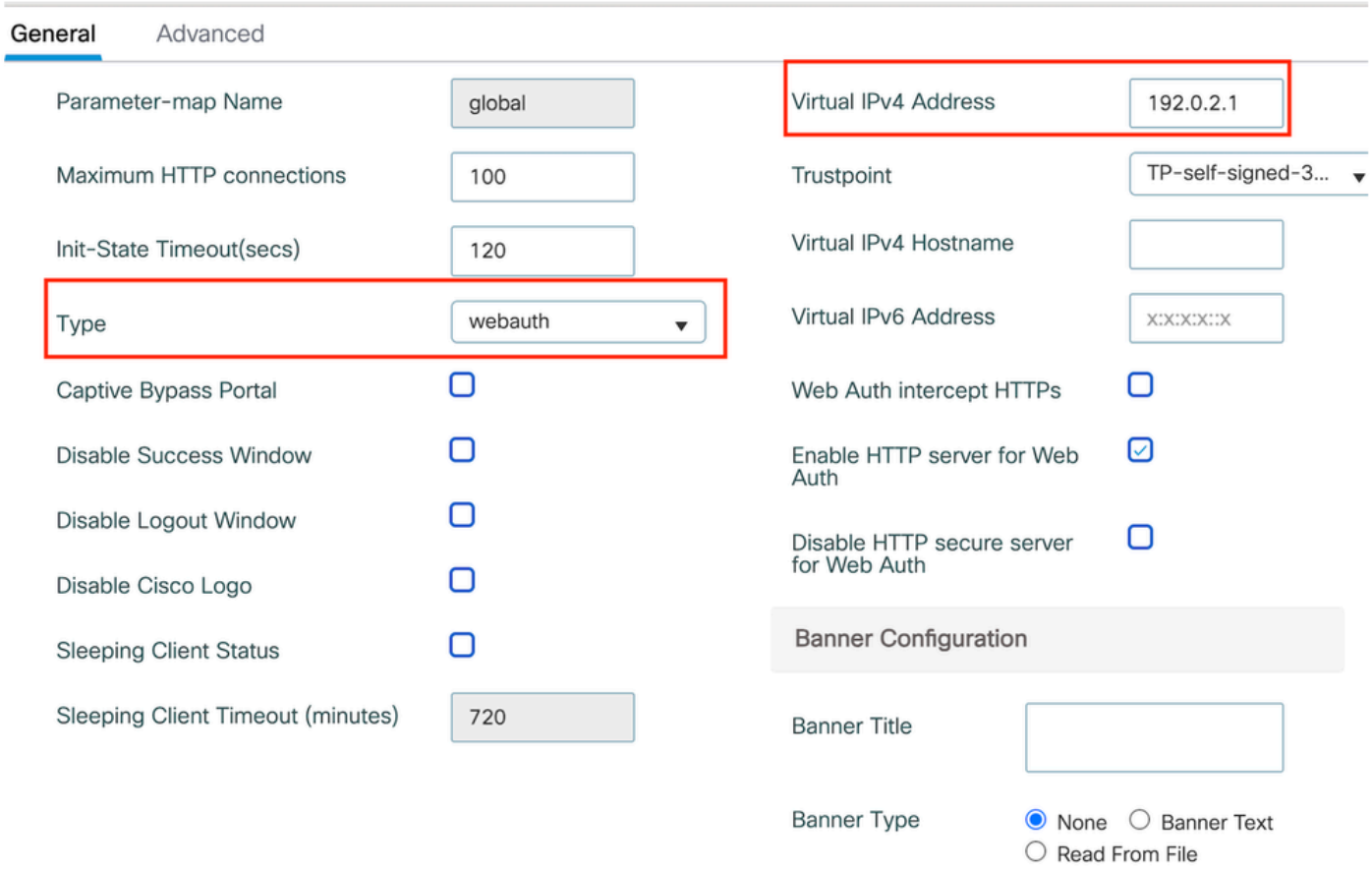
Étape 6 : Mappez l'ancre de mobilité de la liste déroulante au profil de réseau local invité.

Mappage de l'ancre de mobilité au LAN invité

Configuration sur le WLC Anchor 9800

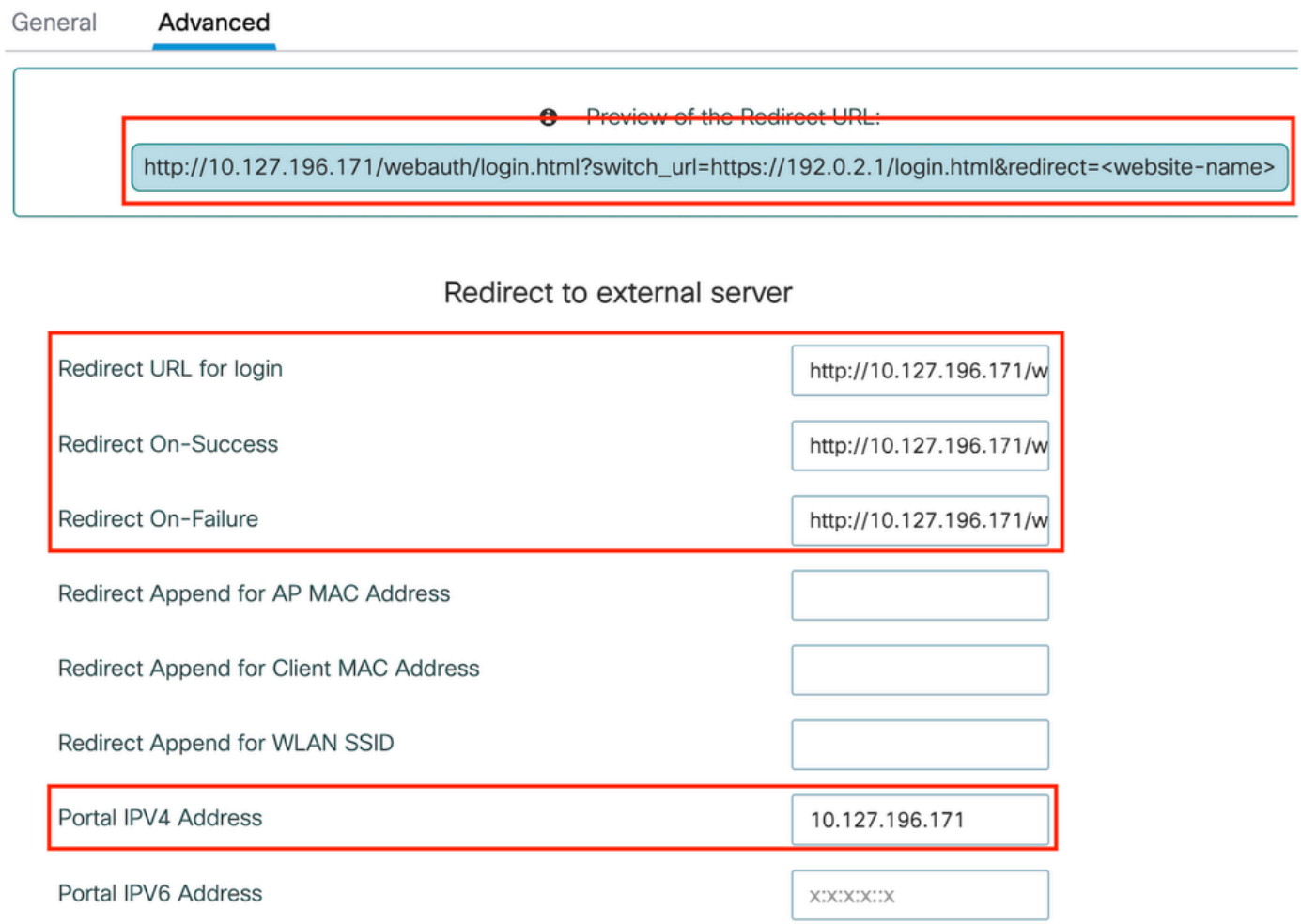
Configurer la carte de paramètres Web

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.



Carte de paramètre Web

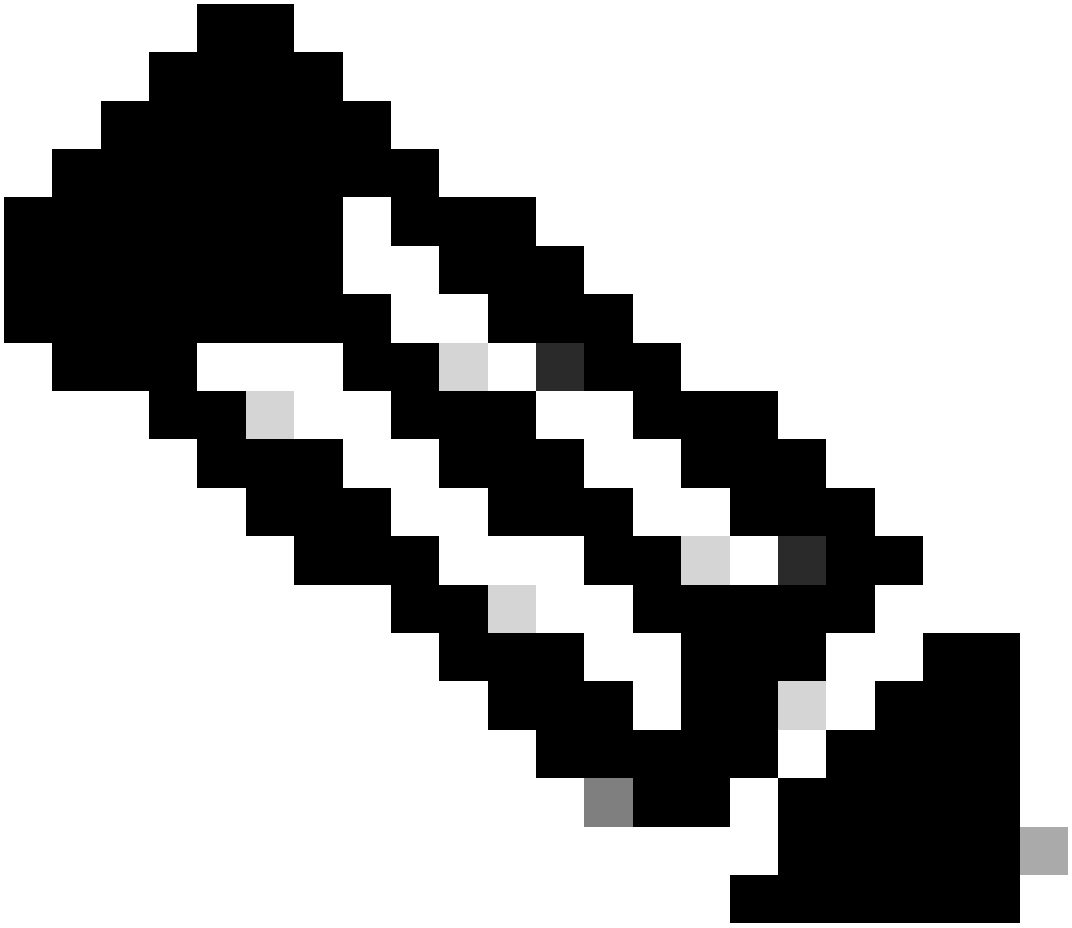
Étape 2 : Sous l'onglet Advanced, spécifiez l'URL de la page Web externe vers laquelle les clients doivent être redirigés. Configurez l'URL de redirection pour la connexion et la redirection en cas d'échec. Le paramètre Redirect On-Success est une configuration facultative.



Onglet Avancé

Configuration CLI

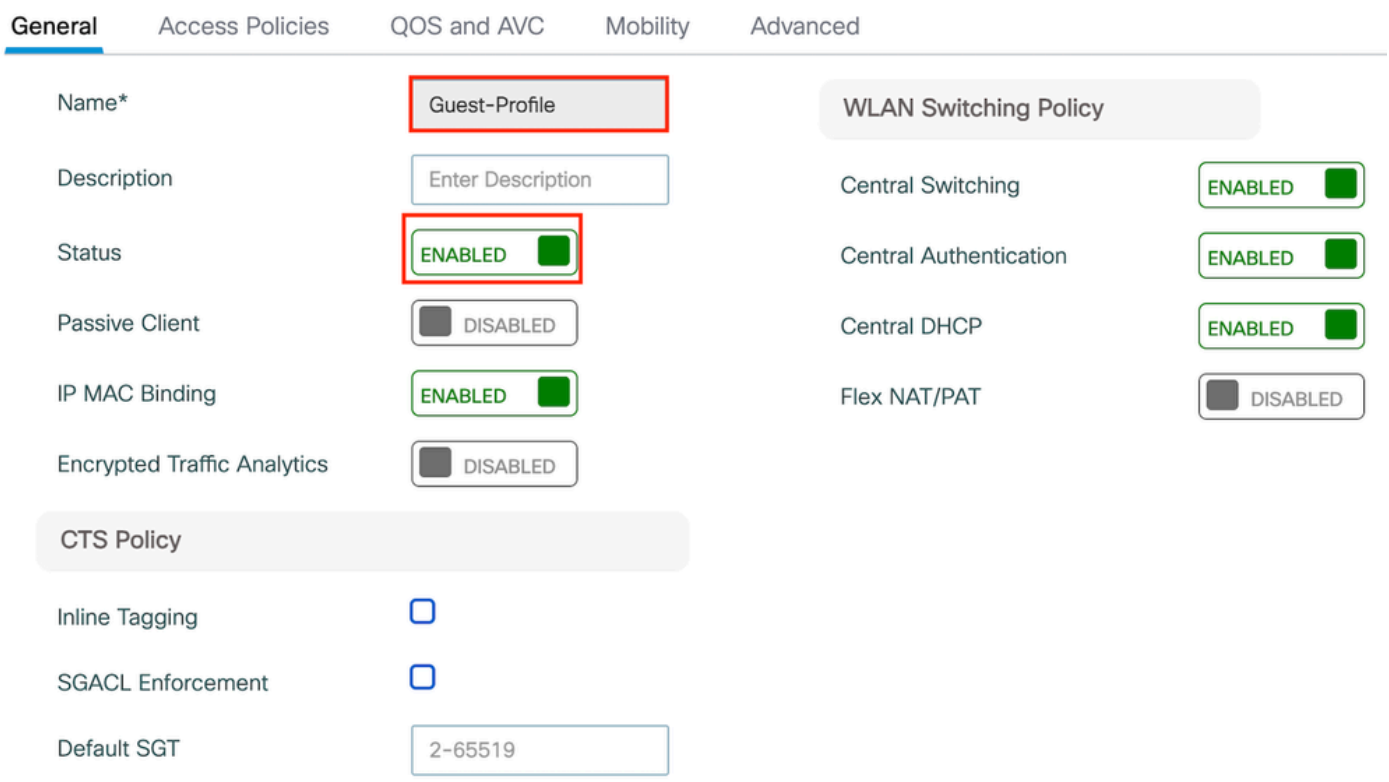
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171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

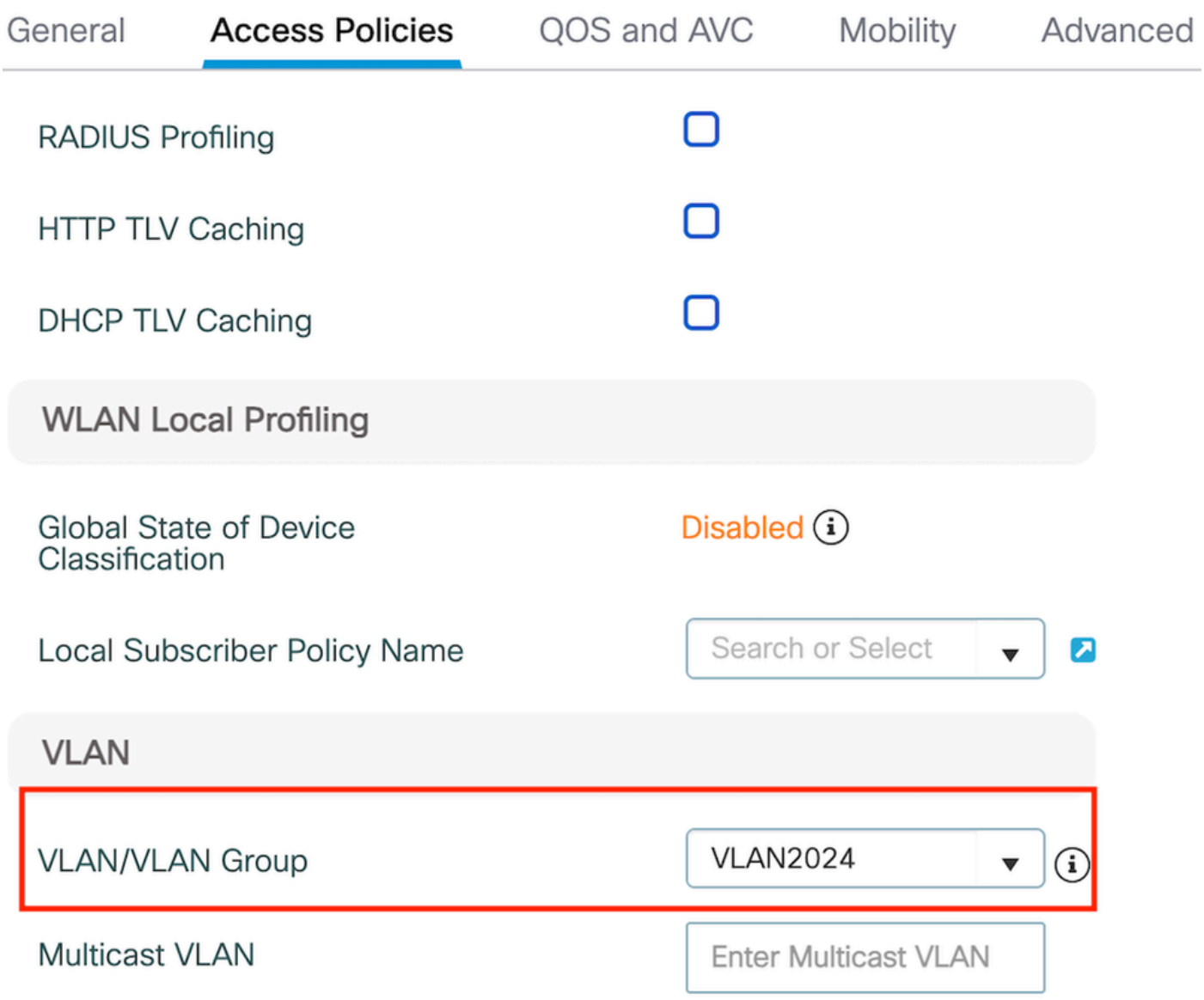
Configurer le profil de stratégie

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.



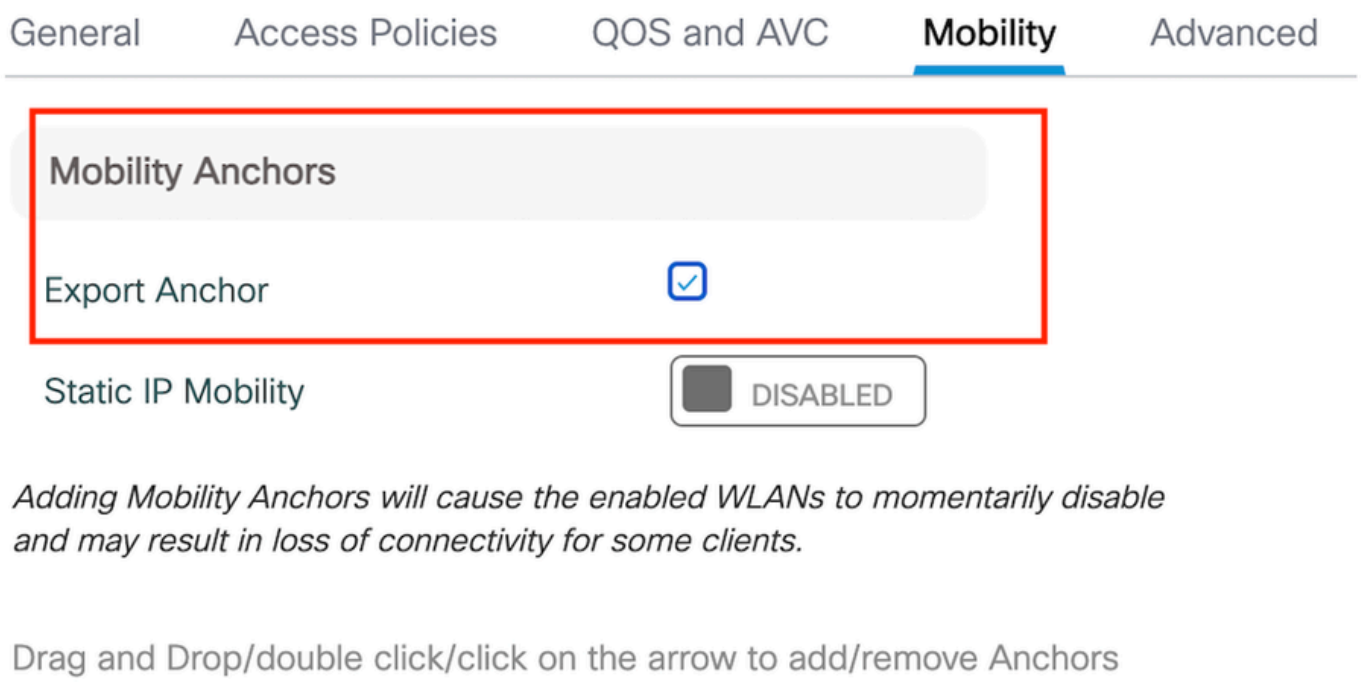
Profil de stratégie

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



Politiques d'accès

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



Onglet Mobilité

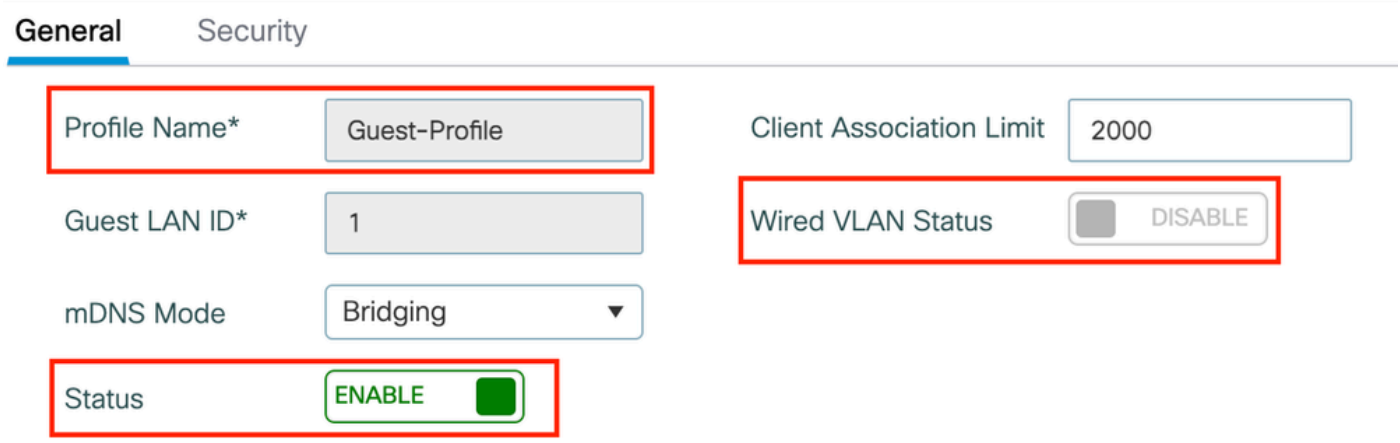
Configuration CLI

```
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

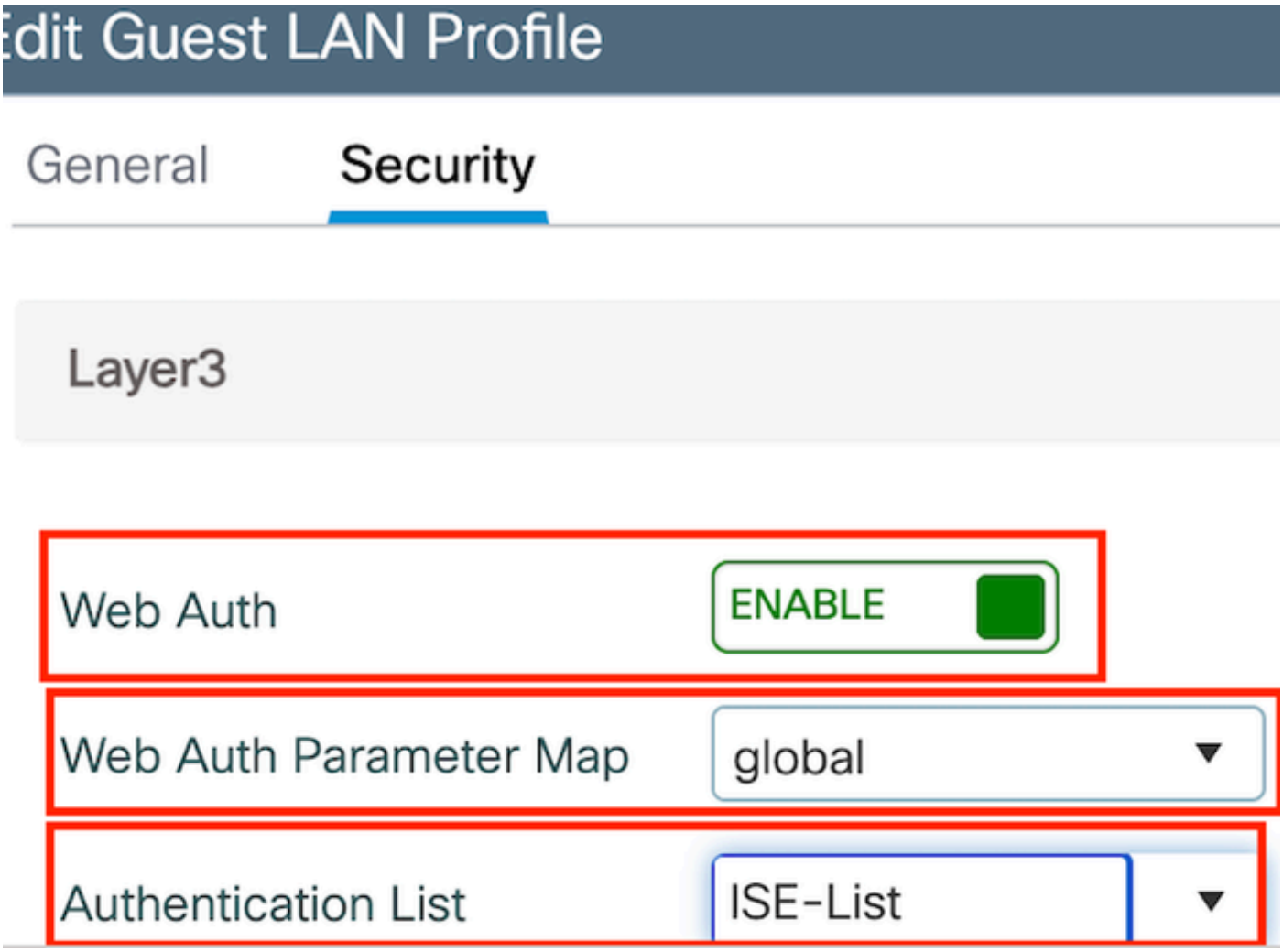
Étape 1 : Accédez à Configuration > Wireless > Guest LAN et sélectionnez Add pour configurer le profil Guest LAN et désactiver l'état du VLAN filaire.

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



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



Onglet Sécurité LAN invité

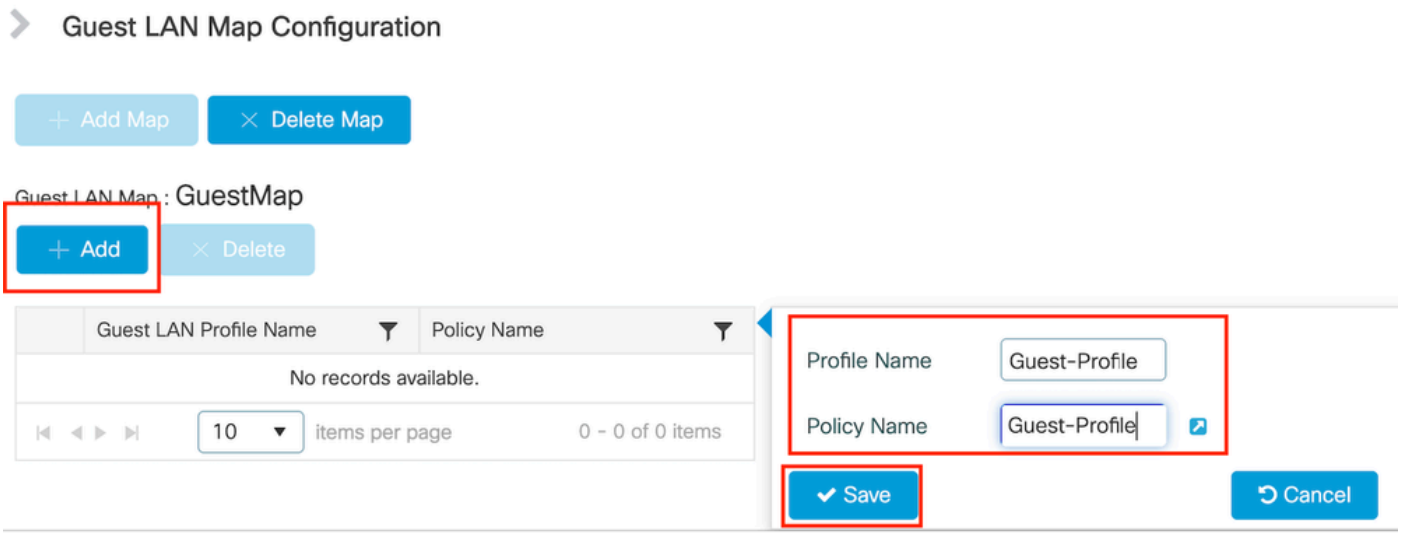
Configuration CLI

```
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 Meth
-------------------------------------------------------------------------------------------------------------
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 is 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
```

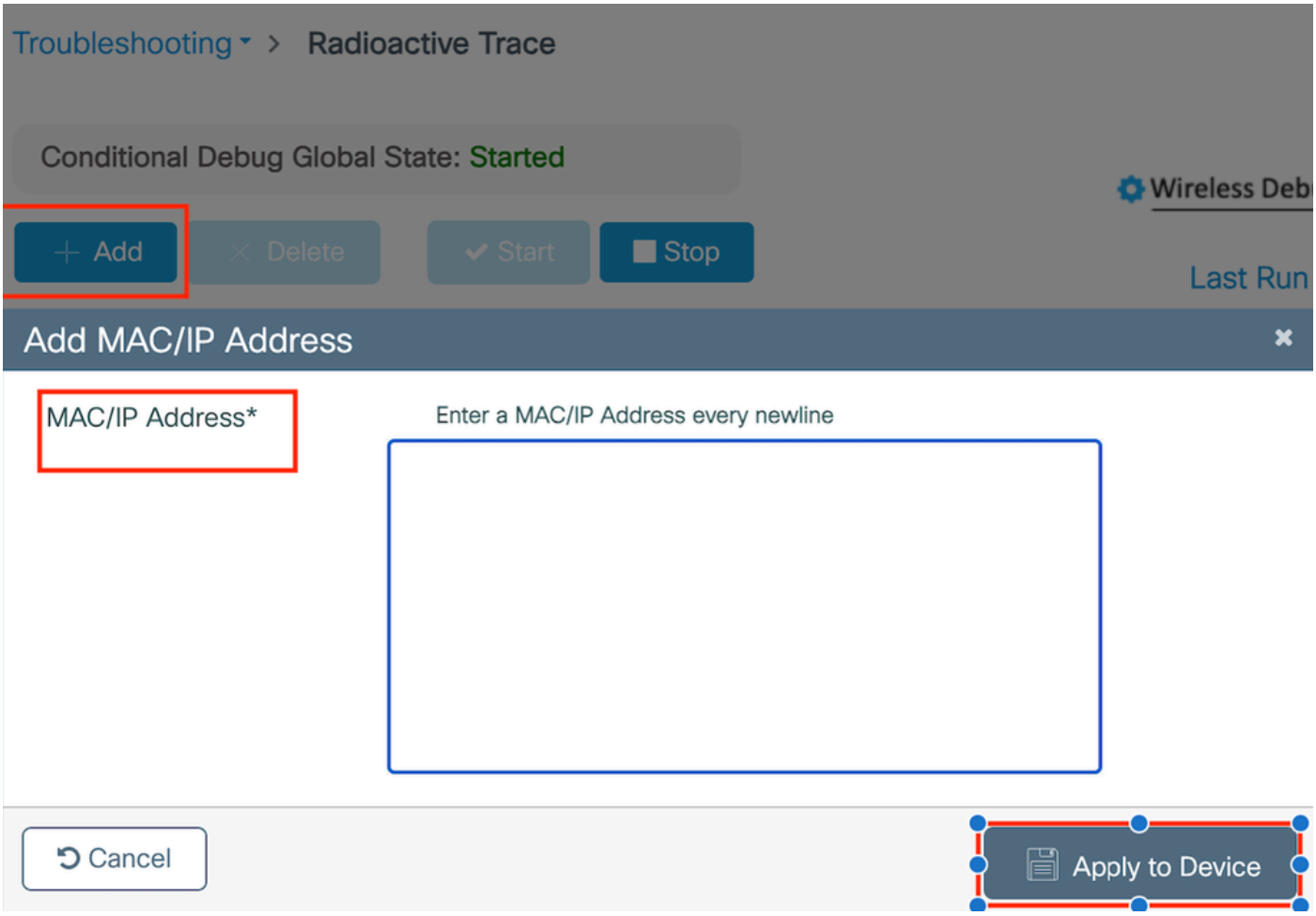
Copiez le fichier sur un serveur externe .

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

Affichez le journal de débogage :

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

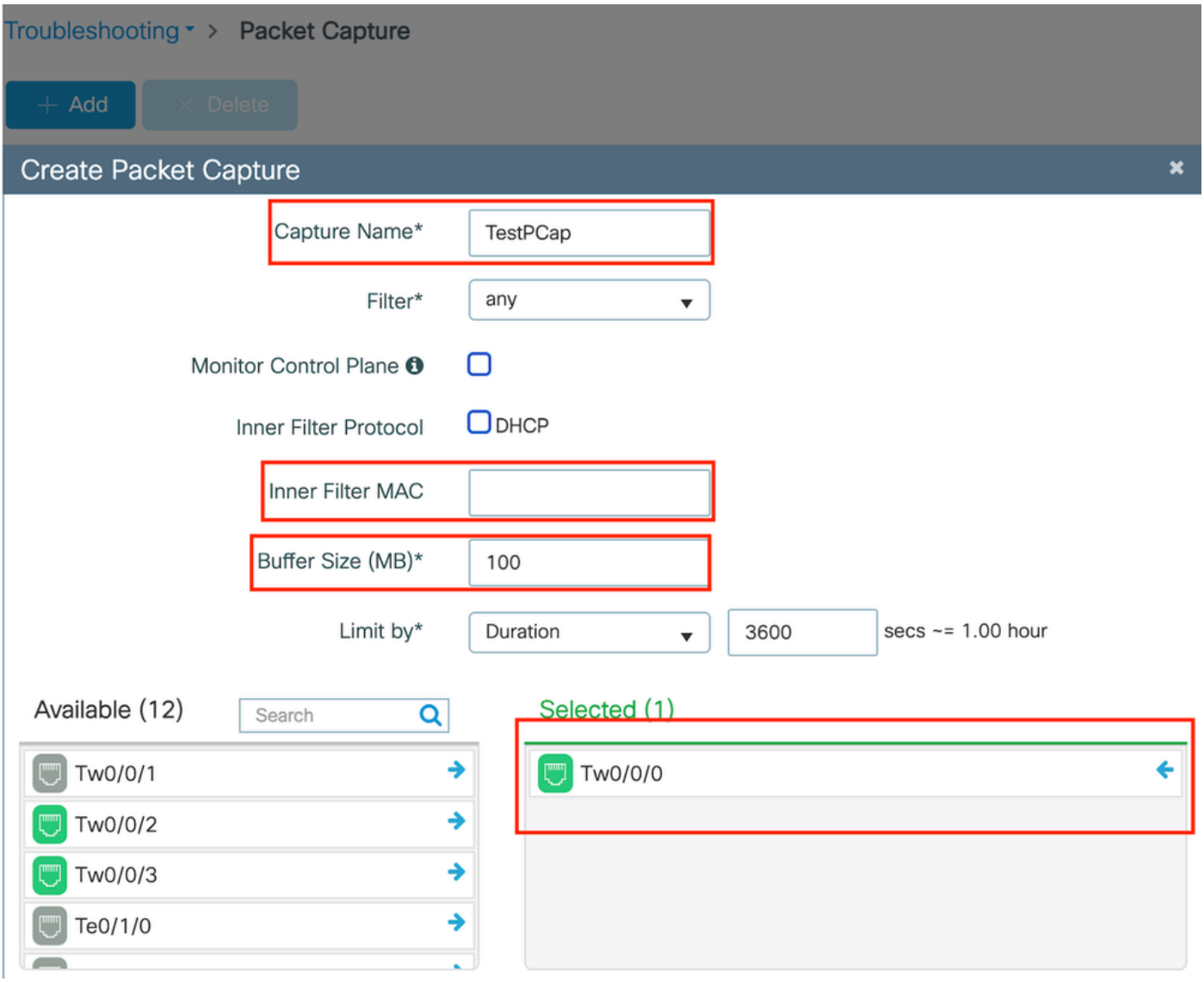
Activer le suivi RA dans l'interface utilisateur graphique,



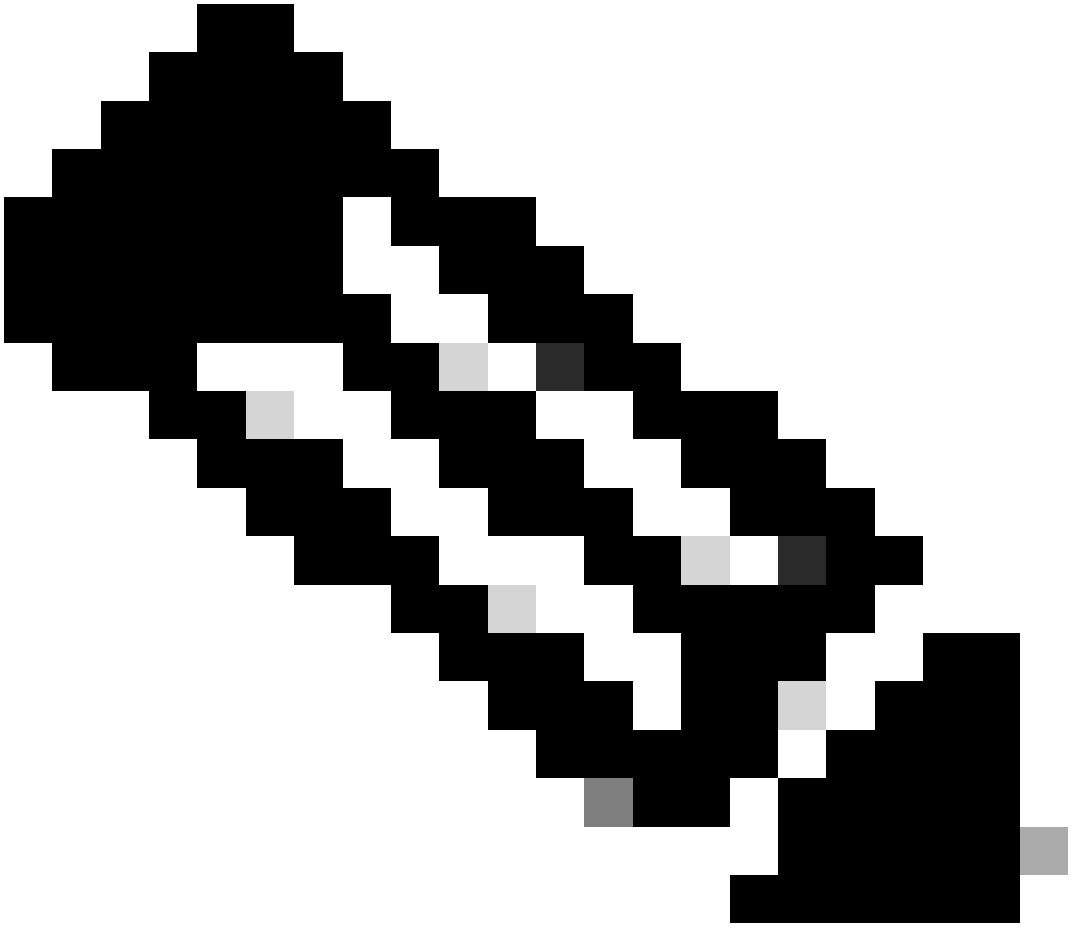
Activer le suivi RA sur WebUI

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.

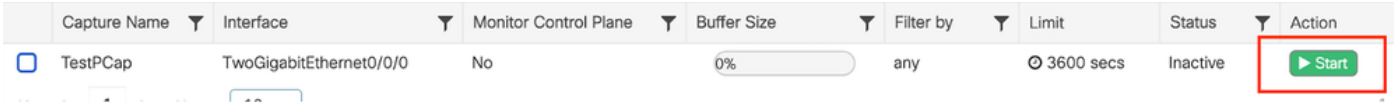


Capture de paquets intégrée



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.



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
```

```
<Reporduce the issue>

monitor capture TestPCap stop
```

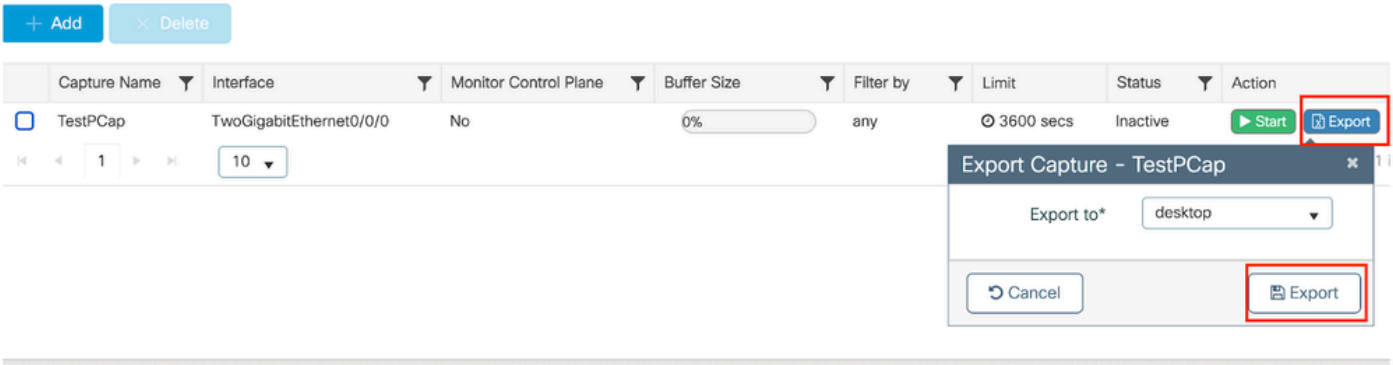
```
show monitor capture TestPCap

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.



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:c
```

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.a9b
```

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.a9b
2024/07/15 04:10:29.091605761 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
```

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.a9b
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.a9b
```

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 parqué 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 Re
```

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.a9b
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 {wnc2024/07/15 15:12:04.280574375 {wncd_x_R0-0}{1}: [webauth-httpd] [1470
```

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
```

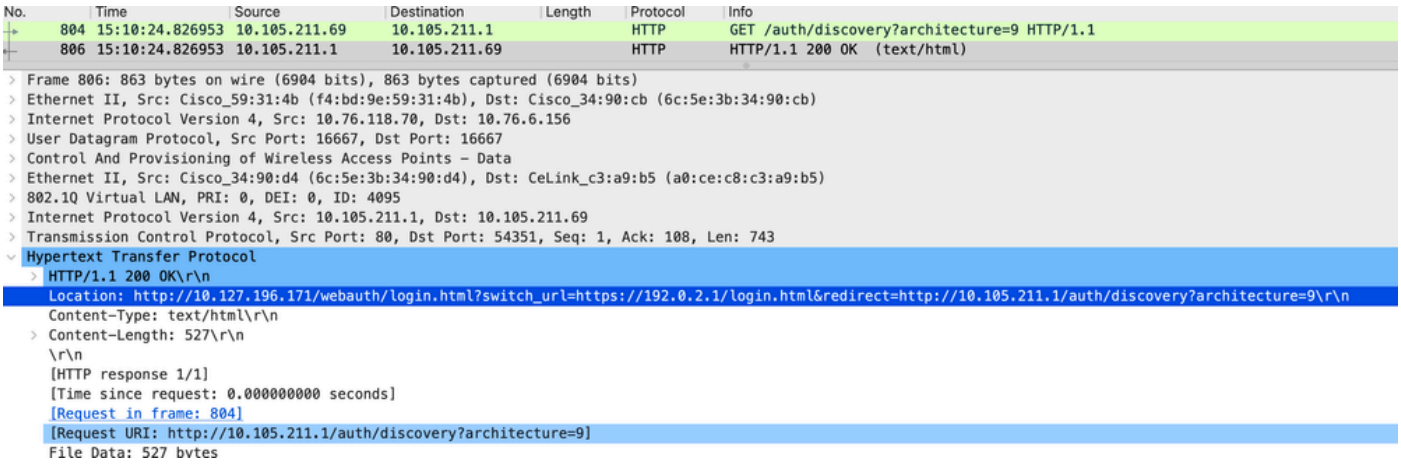
Access-Accept est reçu du serveur radius, webauth est réussi.

```
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.

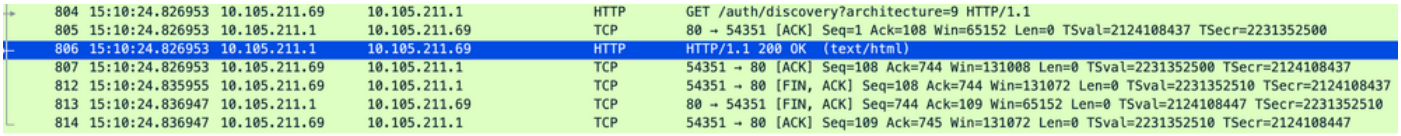
```
2024/07/15 15:12:04.683901842 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:12:04.690643388 {wncd_x_R0-0}{1}: [errmsg] [14709]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/15 15:12:04.690726966 {wncd_x_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied 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



Le client est redirigé vers la page du portail

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

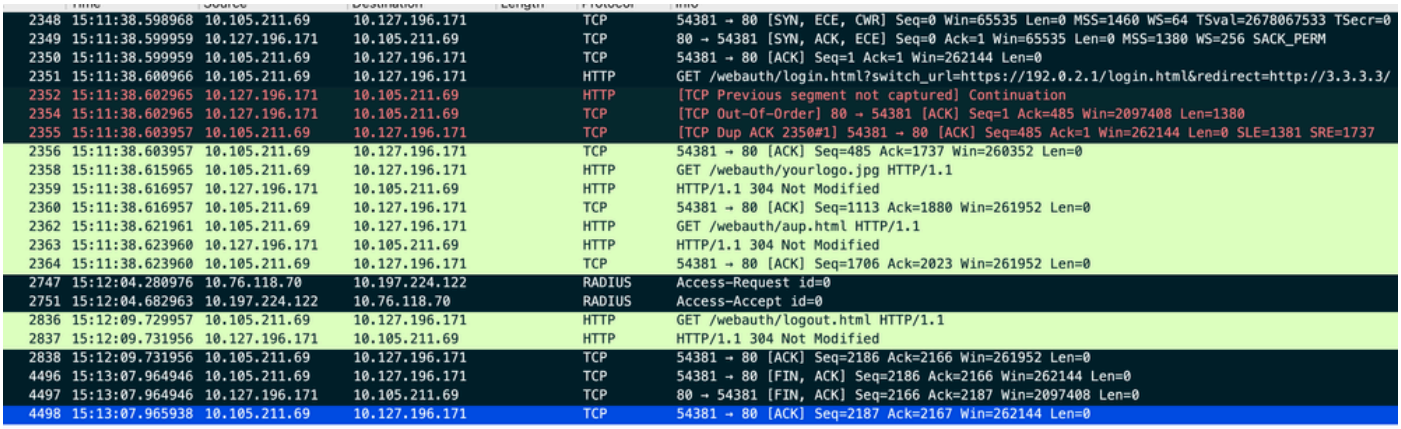


La session TCP est fermée après réception de l'URL de redirection

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.

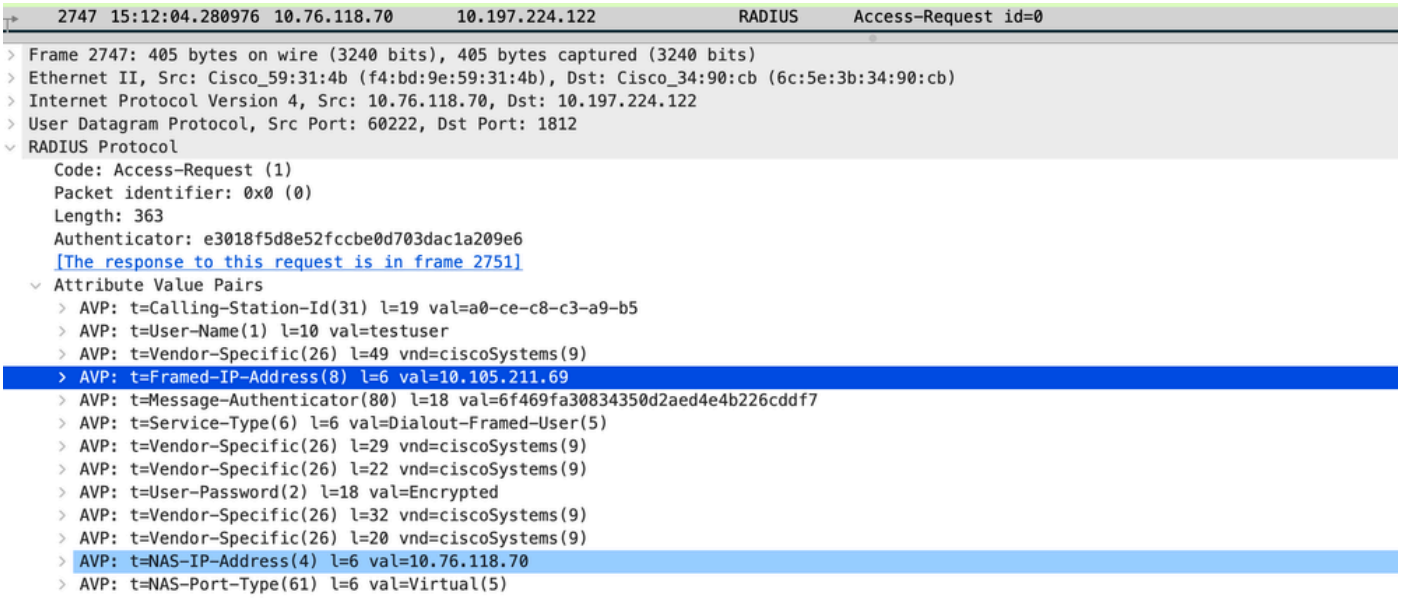
Une fois l'authentification réussie, la session TCP vers le serveur Web est fermée et sur le contrôleur, l'état du gestionnaire de stratégies client passe à EXÉCUTER.



2348	15:11:38.598968	10.105.211.69	10.127.196.171	TCP	54381 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2678067533 TSecr=0
2349	15:11:38.599959	10.127.196.171	10.105.211.69	TCP	80 → 54381 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
2350	15:11:38.599959	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2351	15:11:38.600966	10.105.211.69	10.127.196.171	HTTP	GET /webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://3.3.3.3/
2352	15:11:38.602965	10.127.196.171	10.105.211.69	HTTP	[TCP Previous segment not captured] Continuation
2354	15:11:38.602965	10.127.196.171	10.105.211.69	TCP	[TCP Out-Of-Order] 80 → 54381 [ACK] Seq=1 Ack=485 Win=2097408 Len=1380
2355	15:11:38.603957	10.105.211.69	10.127.196.171	TCP	[TCP Dup ACK 2350#1] 54381 → 80 [ACK] Seq=485 Ack=1 Win=262144 Len=0 SLE=1381 SRE=1737
2356	15:11:38.603957	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=485 Ack=1737 Win=260352 Len=0
2358	15:11:38.615965	10.105.211.69	10.127.196.171	HTTP	GET /webauth/yourlogo.jpg HTTP/1.1
2359	15:11:38.616957	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2360	15:11:38.616957	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1113 Ack=1880 Win=261952 Len=0
2362	15:11:38.621961	10.105.211.69	10.127.196.171	HTTP	GET /webauth/aup.html HTTP/1.1
2363	15:11:38.623960	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2364	15:11:38.623960	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1706 Ack=2023 Win=261952 Len=0
2747	15:12:04.280976	10.76.118.70	10.197.224.122	RADIUS	Access-Request id=0
2751	15:12:04.682963	10.197.224.122	10.76.118.70	RADIUS	Access-Accept id=0
2836	15:12:09.729957	10.105.211.69	10.127.196.171	HTTP	GET /webauth/logout.html HTTP/1.1
2837	15:12:09.731956	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2838	15:12:09.731956	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=2186 Ack=2166 Win=261952 Len=0
4496	15:13:07.964946	10.105.211.69	10.127.196.171	TCP	54381 → 80 [FIN, ACK] Seq=2186 Ack=2166 Win=262144 Len=0
4497	15:13:07.964946	10.127.196.171	10.105.211.69	TCP	80 → 54381 [FIN, ACK] Seq=2166 Ack=2187 Win=2097408 Len=0
4498	15:13:07.965938	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=2187 Ack=2167 Win=262144 Len=0

Le client envoie une requête HTTP GET à la page du portail et termine l'authentification avec succès

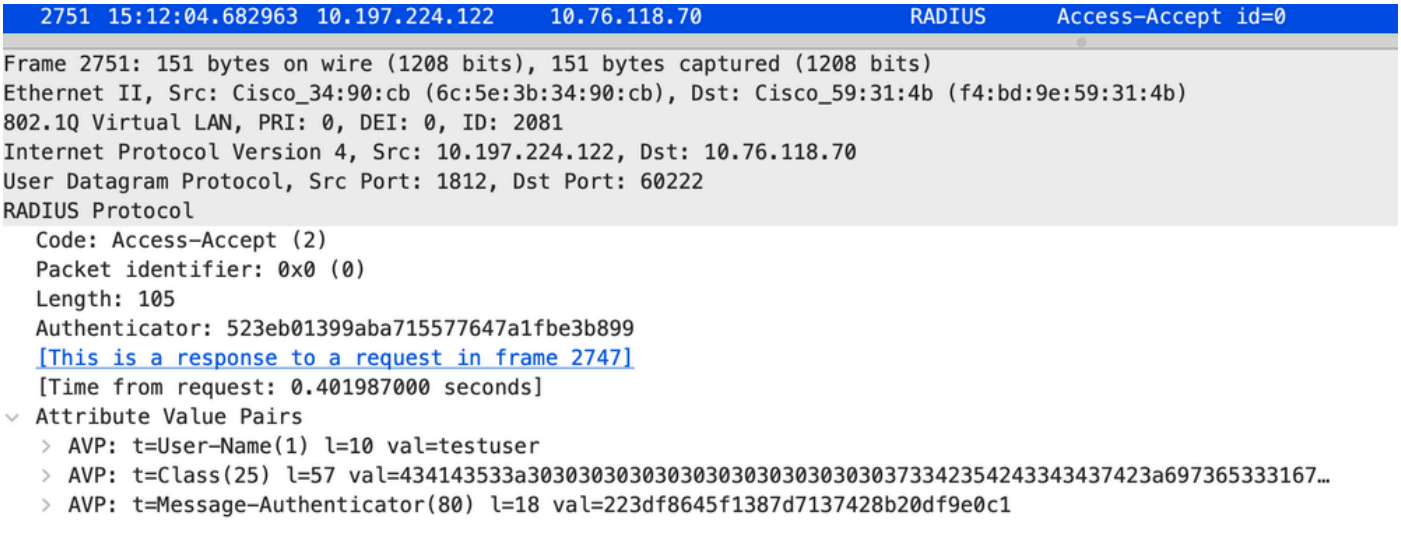
Paquet de demande d'accès Radius



```
2747 15:12:04.280976 10.76.118.70 10.197.224.122 RADIUS Access-Request id=0
> Frame 2747: 405 bytes on wire (3240 bits), 405 bytes captured (3240 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: 10.197.224.122
> User Datagram Protocol, Src Port: 60222, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 363
    Authenticator: e3018f5d8e52fccbe0d703dac1a209e6
    [The response to this request is in frame 2751]
  v Attribute Value Pairs
    > AVP: t=Calling-Station-Id(31) l=19 val=a0-ce-c8-c3-a9-b5
    > AVP: t=User-Name(1) l=10 val=testuser
    > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    > AVP: t=Framed-IP-Address(8) l=6 val=10.105.211.69
    > AVP: t=Message-Authenticator(80) l=18 val=6f469fa30834350d2aed4e4b226cddf7
    > AVP: t=Service-Type(6) l=6 val=Dialout-Framed-User(5)
    > AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
    > AVP: t=NAS-IP-Address(4) l=6 val=10.76.118.70
    > AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5)
```

Paquet de demande d'accès

Paquet d'acceptation d'accès Radius



```
2751 15:12:04.682963 10.197.224.122 10.76.118.70 RADIUS Access-Accept id=0
Frame 2751: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
Ethernet II, Src: Cisco_34:90:cb (6c:5e:3b:34:90:cb), Dst: Cisco_59:31:4b (f4:bd:9e:59:31:4b)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2081
Internet Protocol Version 4, Src: 10.197.224.122, Dst: 10.76.118.70
User Datagram Protocol, Src Port: 1812, Dst Port: 60222
RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0x0 (0)
  Length: 105
  Authenticator: 523eb01399aba715577647a1fbe3b899
  [This is a response to a request in frame 2747]
  [Time from request: 0.401987000 seconds]
v Attribute Value Pairs
  > AVP: t=User-Name(1) l=10 val=testuser
  > AVP: t=Class(25) l=57 val=434143533a3030303030303030303030303733423542433434374237a697365333167…
  > AVP: t=Message-Authenticator(80) l=18 val=223df8645f1387d7137428b20df9e0c1
```

Paquet Access Accept

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.