Configuration Vérification et dépannage de l'authentification Web sur Mac Filter Failure

Table des matières

Introduction

Ce document décrit comment configurer, dépanner et vérifier l'authentification Web locale sur la fonctionnalité « Mac Filter Failure » en utilisant ISE pour l'authentification externe.

Conditions préalables

Configurer ISE pour l'authentification MAC

Identifiants utilisateur valides configurés sur ISE/Active Directory

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

Compréhension de base de la navigation dans l'interface utilisateur Web du contrôleur

Configuration de la politique, du profil WLAN et des balises de politique

Configuration de la stratégie de service sur ISE

Composants utilisés

WLC 9800 version 17.12.2

AP AXI C9120

commutateur 9300

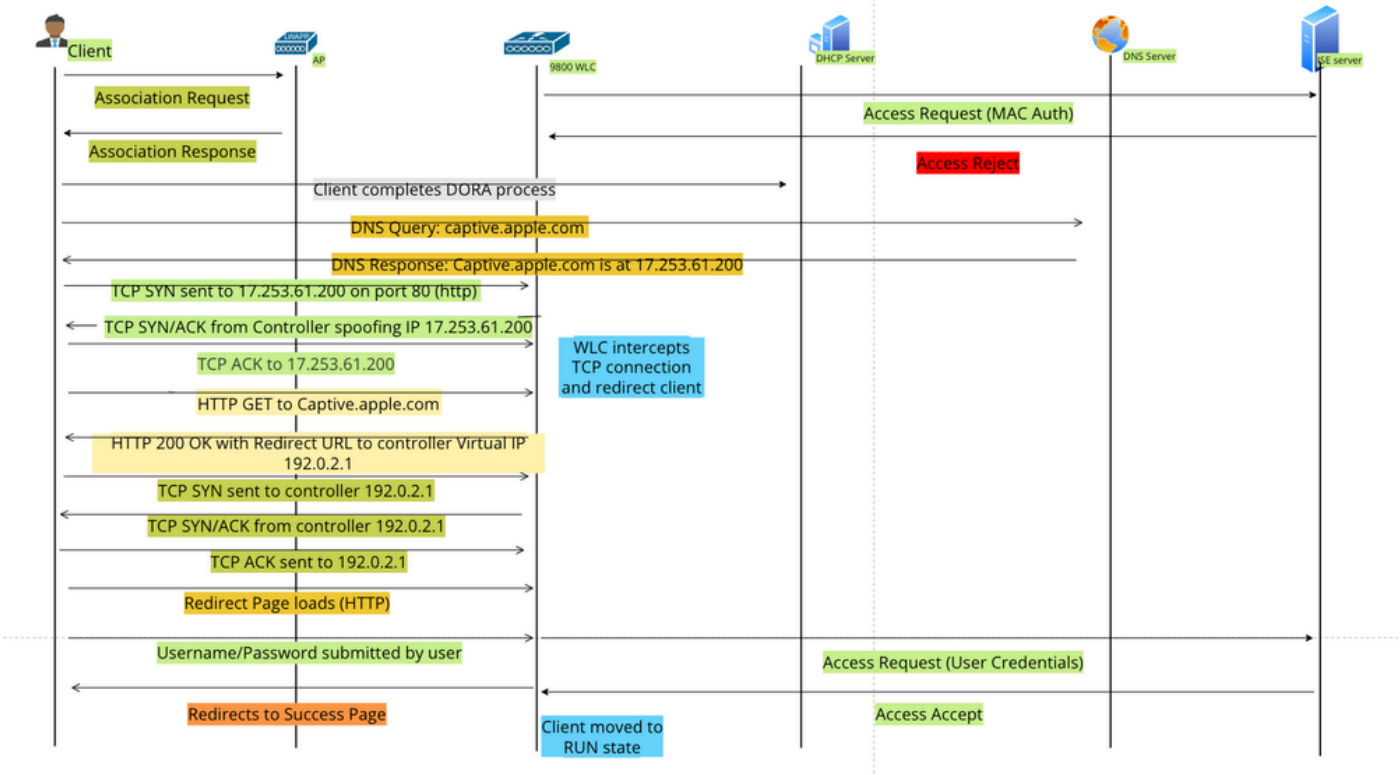
ISE version 3.1.0.518

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.

Informations générales

La fonctionnalité Web Auth « On Mac Failure Filter » sert de mécanisme de secours dans les environnements WLAN qui utilisent à la fois l'authentification MAC et l'authentification Web.

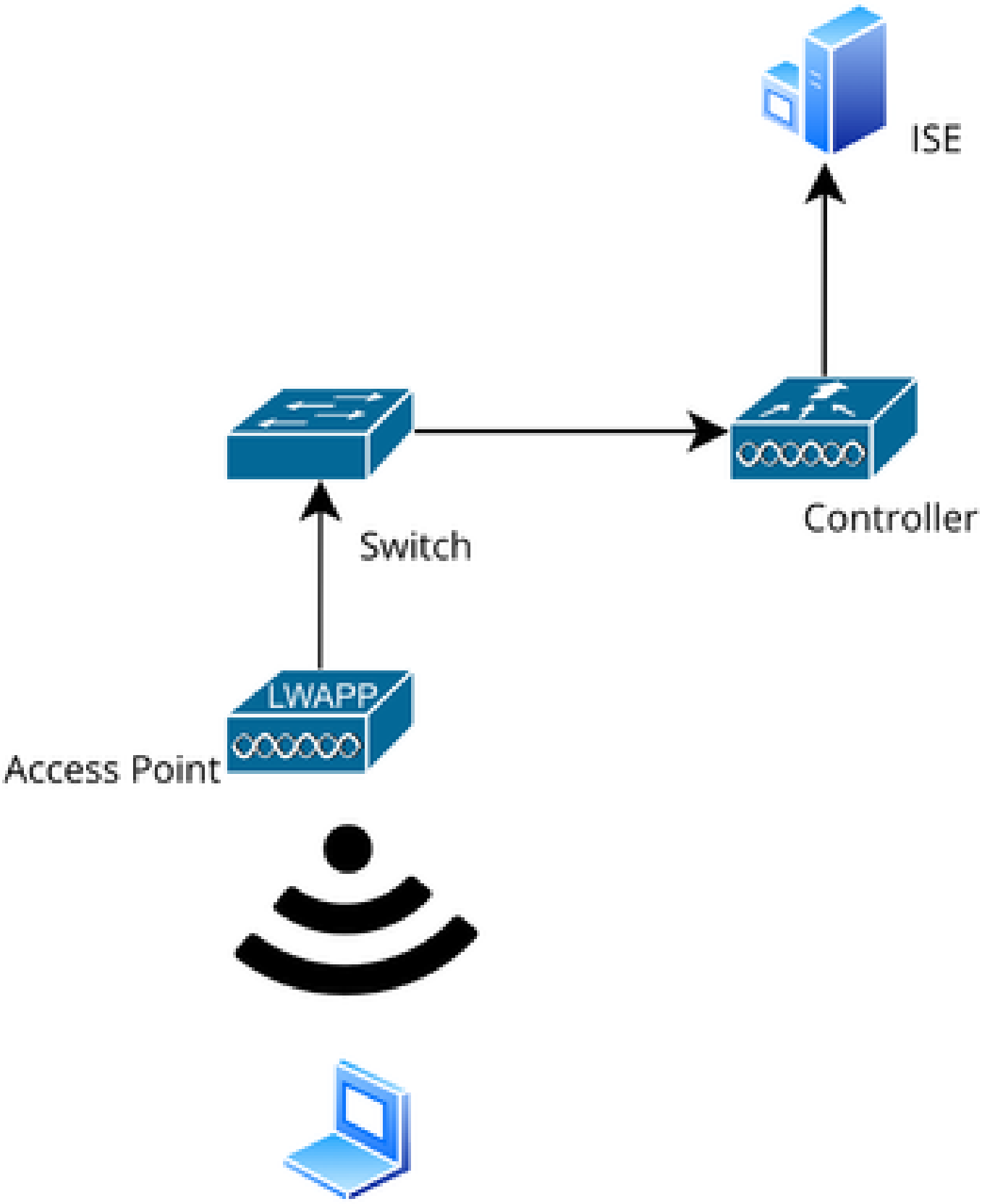
- Mécanisme de secours : lorsqu'un client tente de se connecter à un WLAN avec un filtre MAC sur un serveur RADIUS externe (ISE) ou un serveur local et qu'il échoue à s'authentifier, cette fonctionnalité lance automatiquement une authentification Web de couche 3.
- Authentification réussie : si un client réussit à s'authentifier via le filtre MAC, l'authentification Web est ignorée, ce qui permet au client de se connecter directement au WLAN.
- Éviter les désassociations : cette fonctionnalité permet d'empêcher les désassociations qui pourraient autrement se produire en raison d'échecs d'authentification du filtre MAC.



Flux d'authentification Web

Configurer

Diagramme du réseau



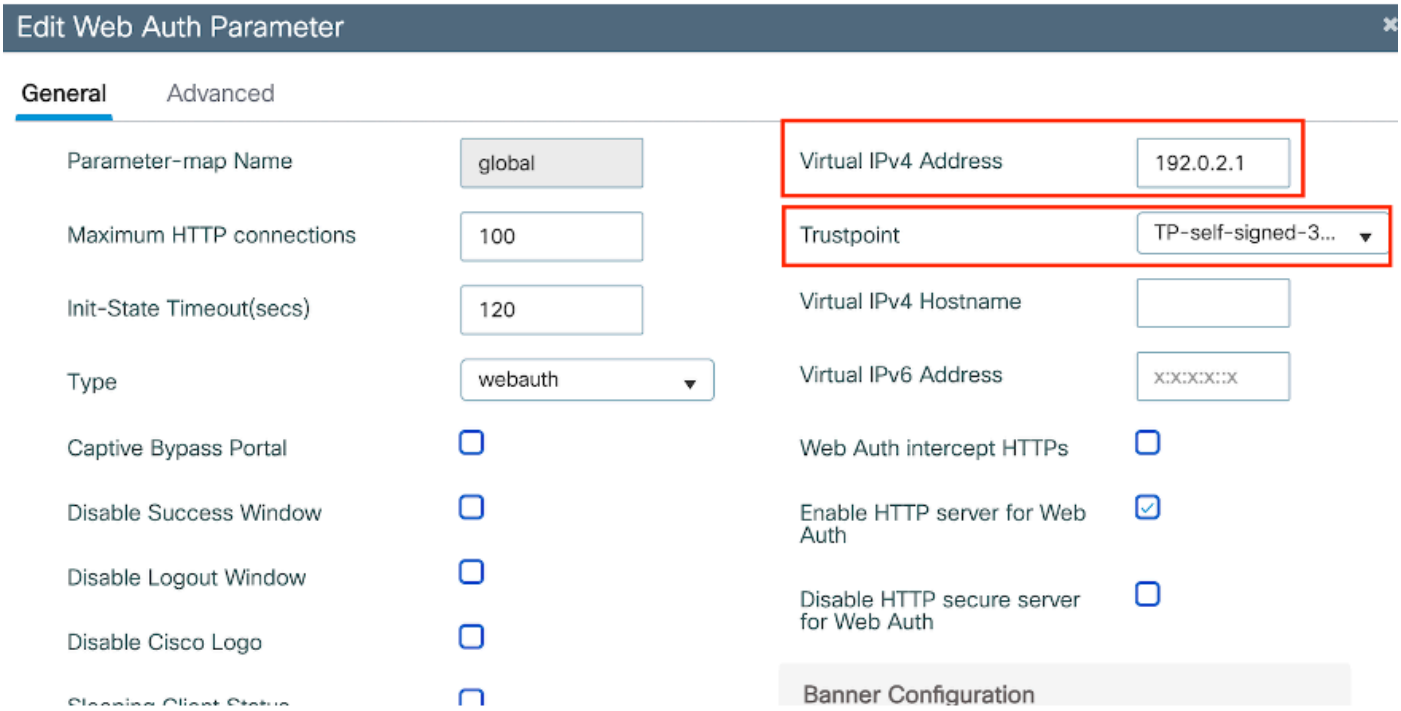
Topologie du réseau

Configurations

Configurer les paramètres Web

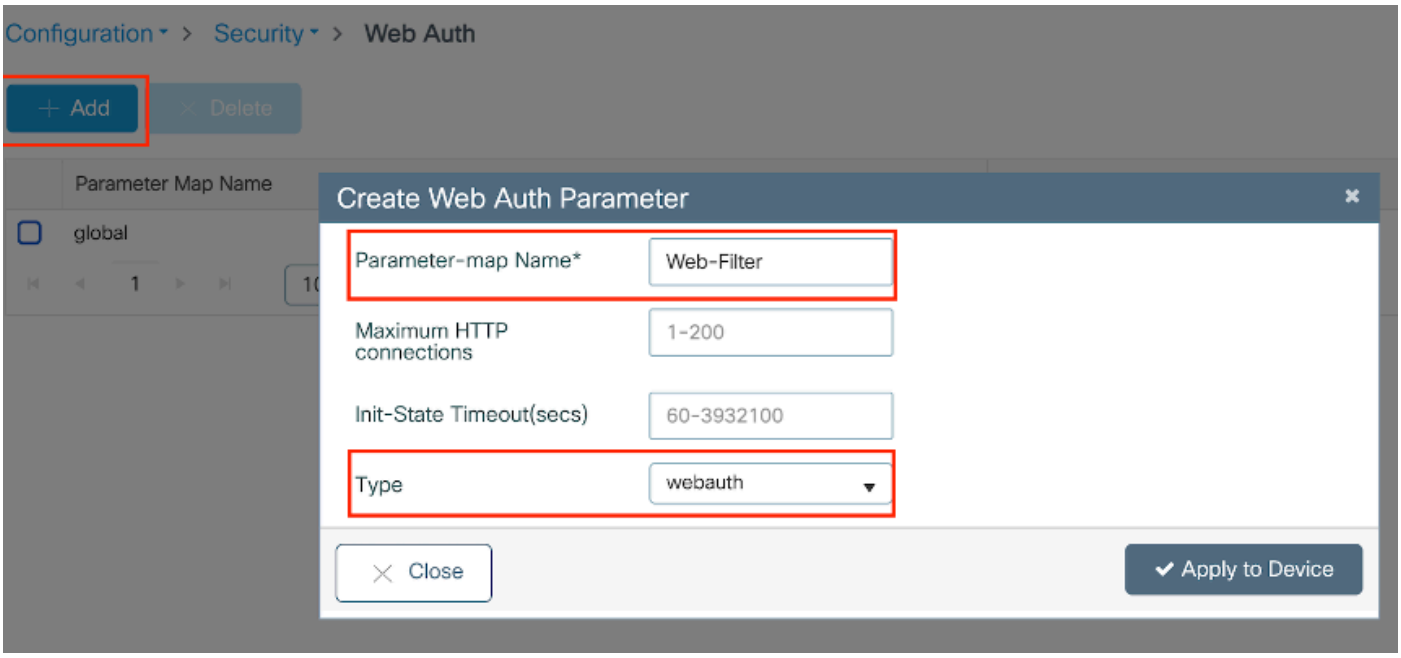
Accédez à Configuration > Security > Web Auth et sélectionnez le mappage de paramètre global

Vérifiez la configuration IP virtuelle et Trustpoint à partir de la carte de paramètres globale. Tous les profils de paramètres Web Auth personnalisés héritent de la configuration IP virtuelle et du point de confiance de la carte de paramètres globale.



Profil du paramètre d'authentification Web global

Étape 1 : Sélectionnez « Ajouter » pour créer une carte de paramètres d'authentification Web personnalisée. Entrez le nom du profil et choisissez le type « Webauth ».



Profil de paramètre Web Auth

Si vos clients obtiennent également une adresse IPv6, vous devez également ajouter une adresse IPv6 virtuelle dans le mappage de paramètres. Utilisez une adresse IP dans la plage de documentation 2001:db8::/32

Si vos clients ont obtenu une adresse IPv6, il y a de fortes chances qu'ils essaient d'obtenir la redirection d'authentification Web HTTP dans V6 et non dans V4, c'est pourquoi vous avez besoin que l'IPv6 virtuel soit également défini.

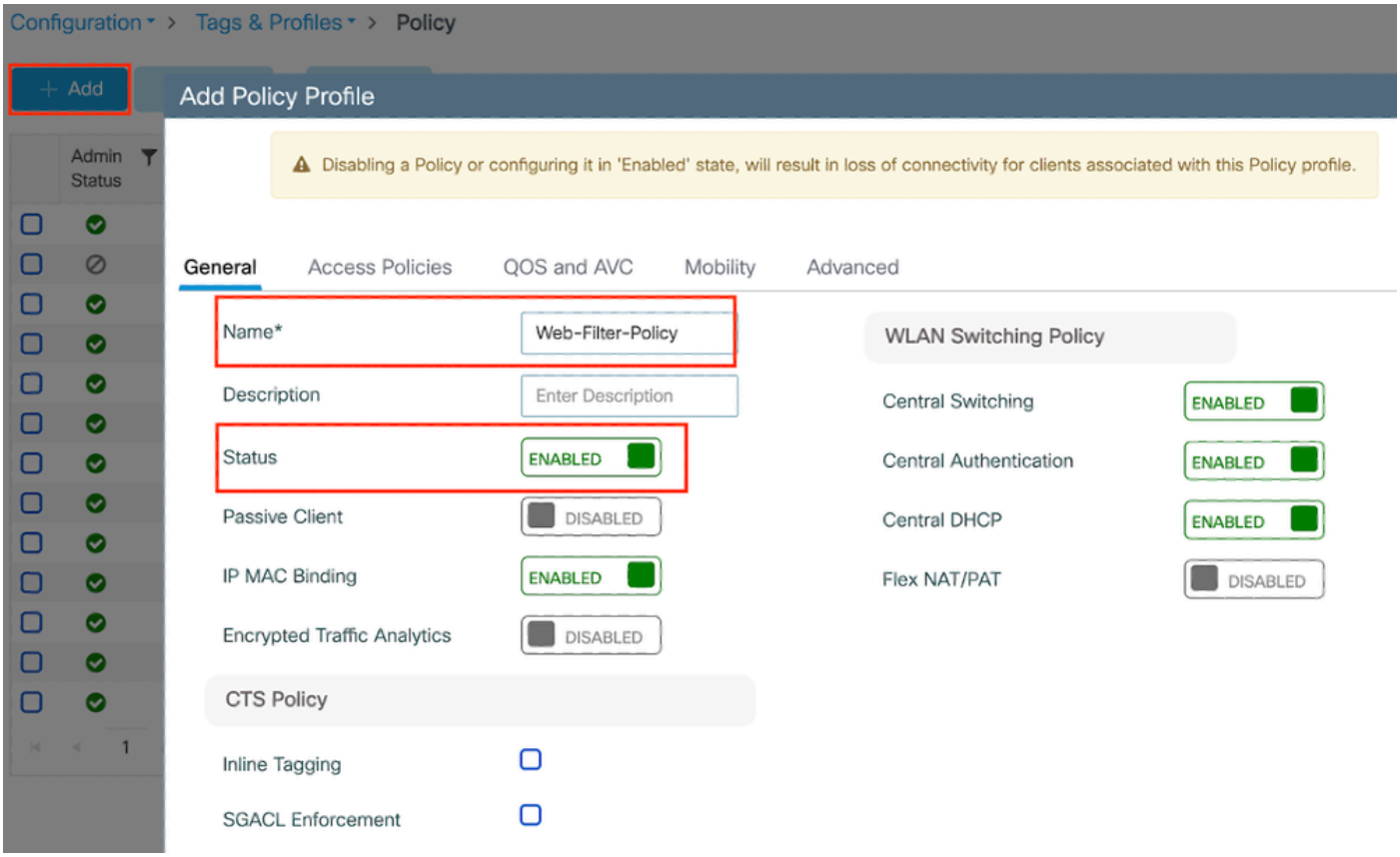
Configuration CLI :

```
parameter-map type webauth Web-Filter
 type webauth
```

Configurer le profil de stratégie

Étape 1 : Créez un profil de stratégie

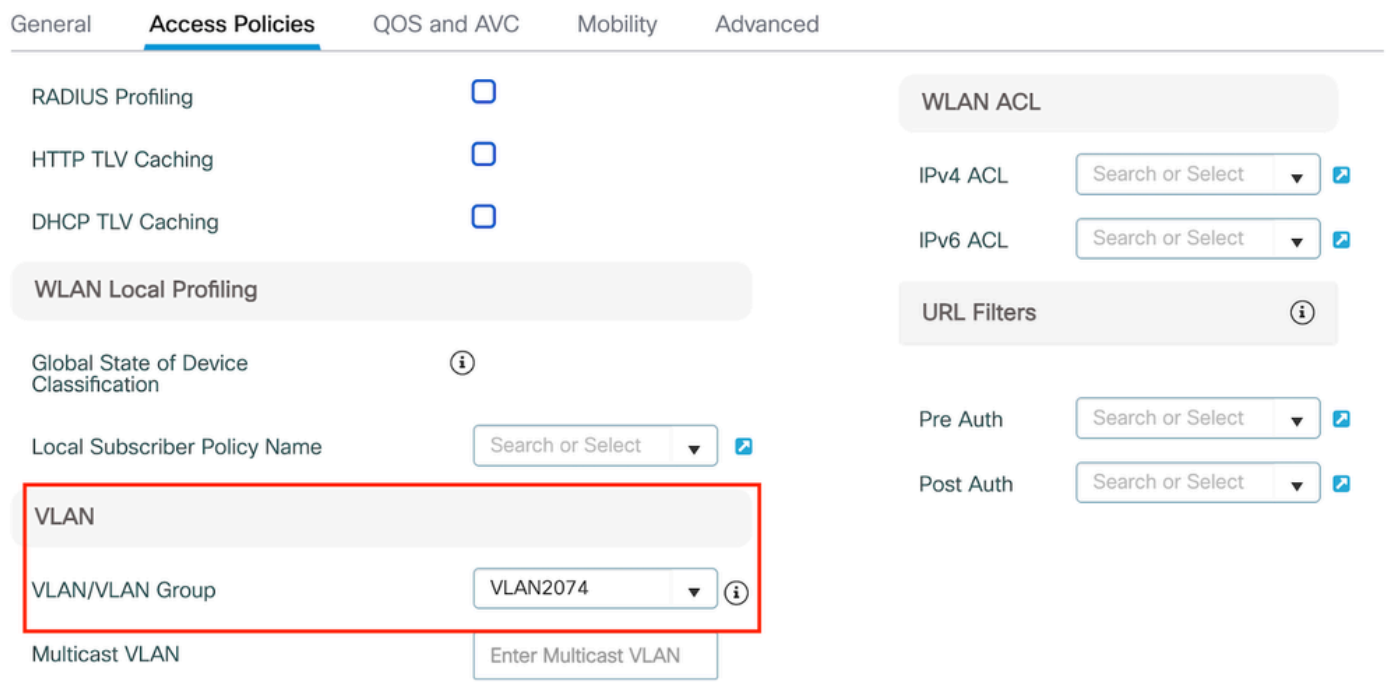
Accédez à Configuration > Tags & Profiles > Policy. Sélectionnez « Ajouter ». Dans l'onglet Général, spécifiez un nom pour le profil et activez le basculement d'état.



Profil de stratégie

Étape2:

Sous l'onglet Access Policies, sélectionnez le VLAN client dans la liste déroulante VLAN.



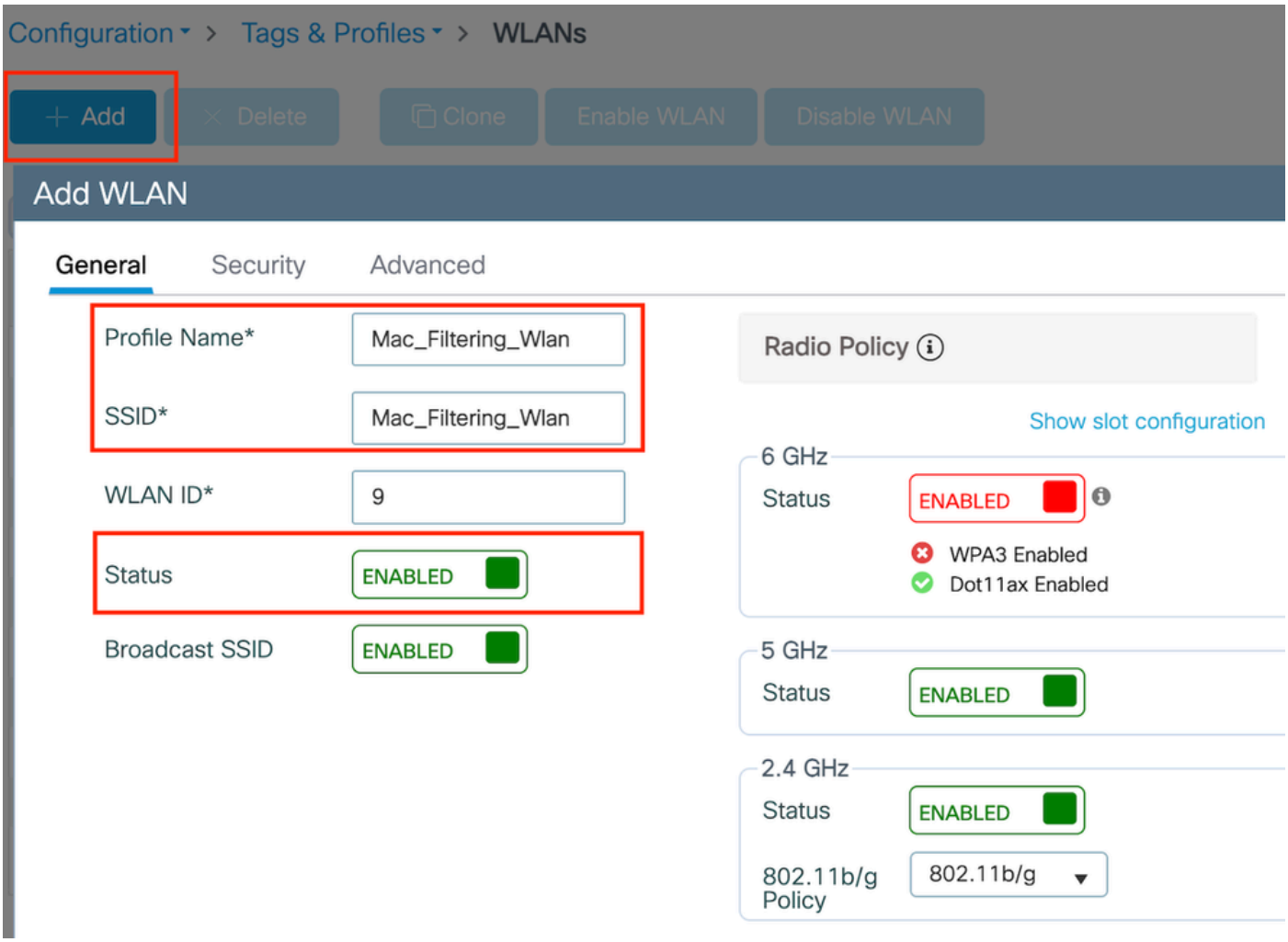
Onglet Access Policy

Configuration CLI :

```
wireless profile policy Web-Filter-Policy
 vlan VLAN2074
 no shutdown
```

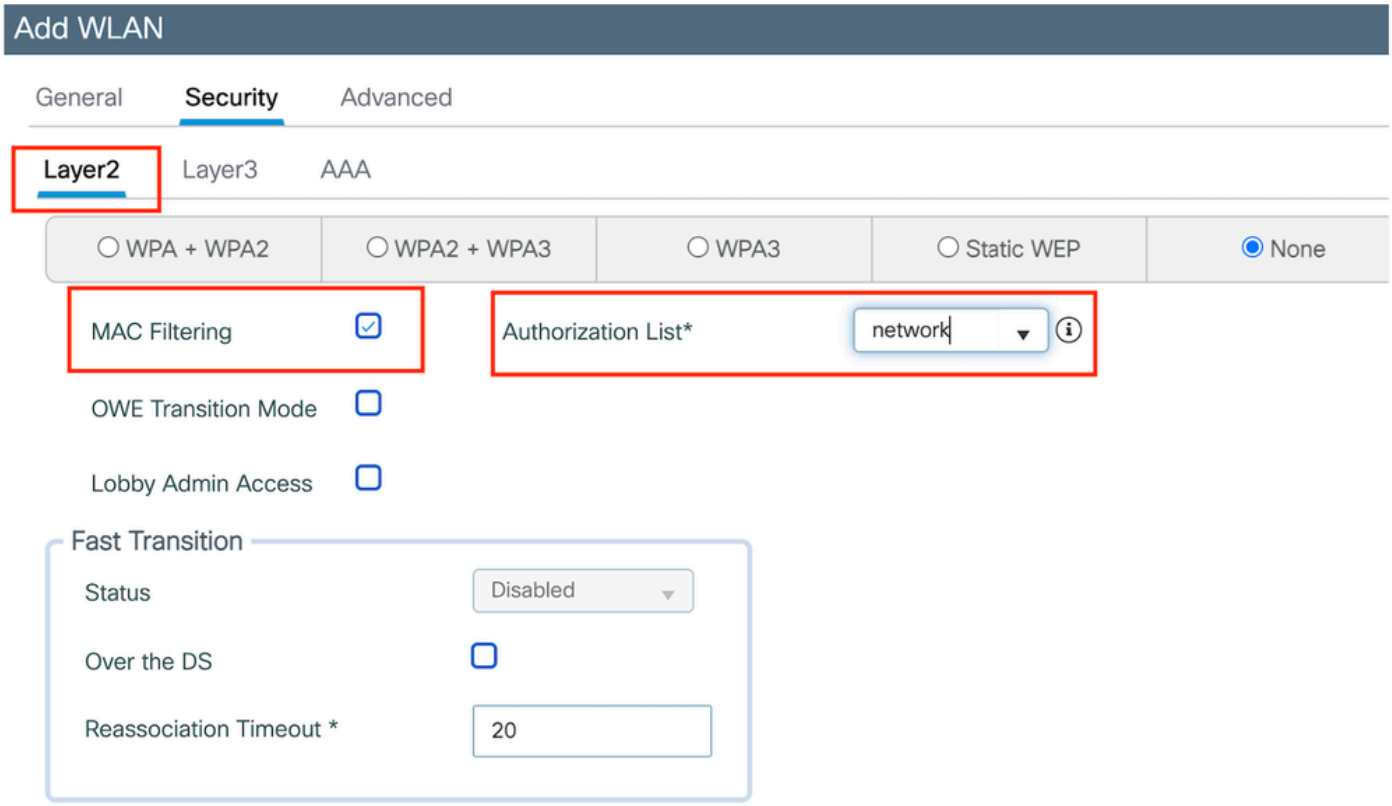
Configuration du profil WLAN

Étape 1 : Accédez à Configuration > Tags and Profiles > WLANs. Sélectionnez Ajouter pour créer un nouveau profil. Définissez un nom de profil et un nom SSID, puis activez le champ d'état.



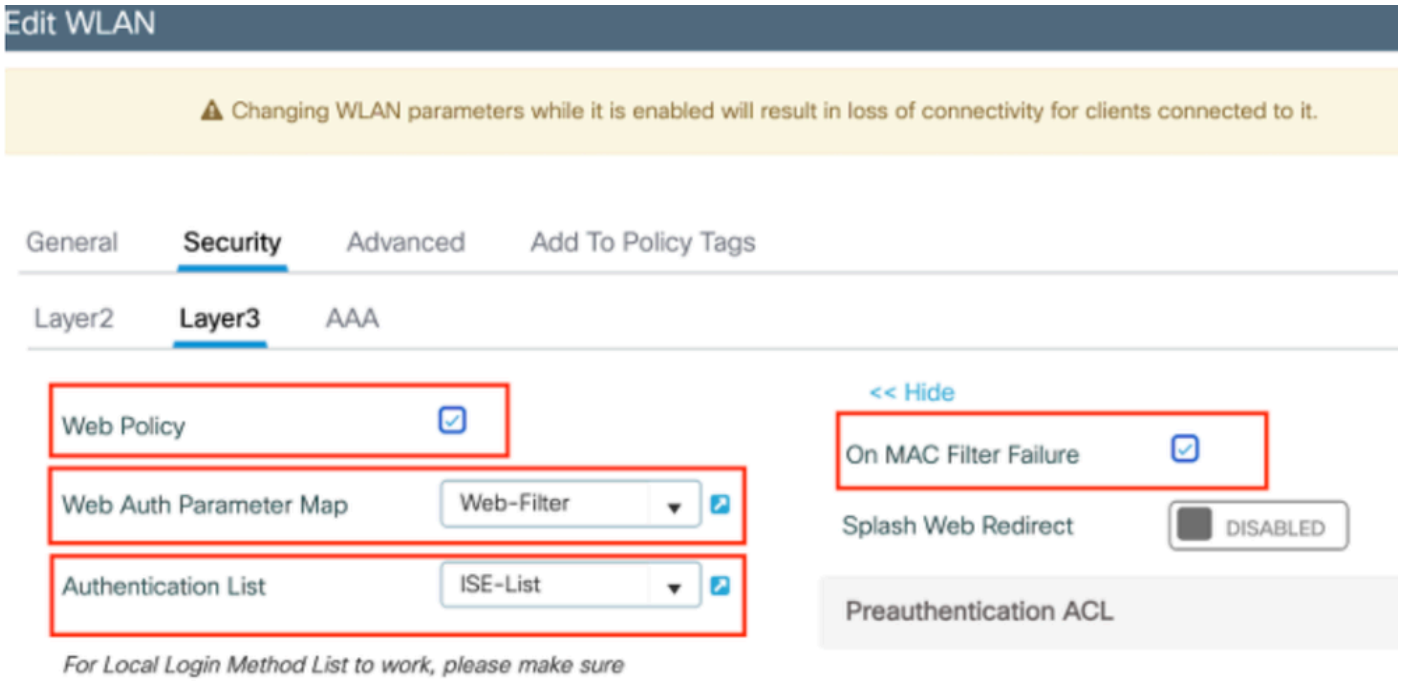
Profil WLAN

Étape 2 : Sous l'onglet Security, activez la case à cocher Mac Filtering et configurez le serveur RADIUS dans la liste Authorization List (ISE ou serveur local). Cette configuration utilise ISE pour l'authentification Mac et l'authentification Web.



Sécurité de la couche 2 WLAN

Étape 3 : accédez à Security > Layer3. Activez la stratégie Web et associez-la au profil de mappage des paramètres d'authentification Web. Cochez la case « On Mac Filter Failure » et choisissez le serveur RADIUS dans la liste déroulante Authentication.



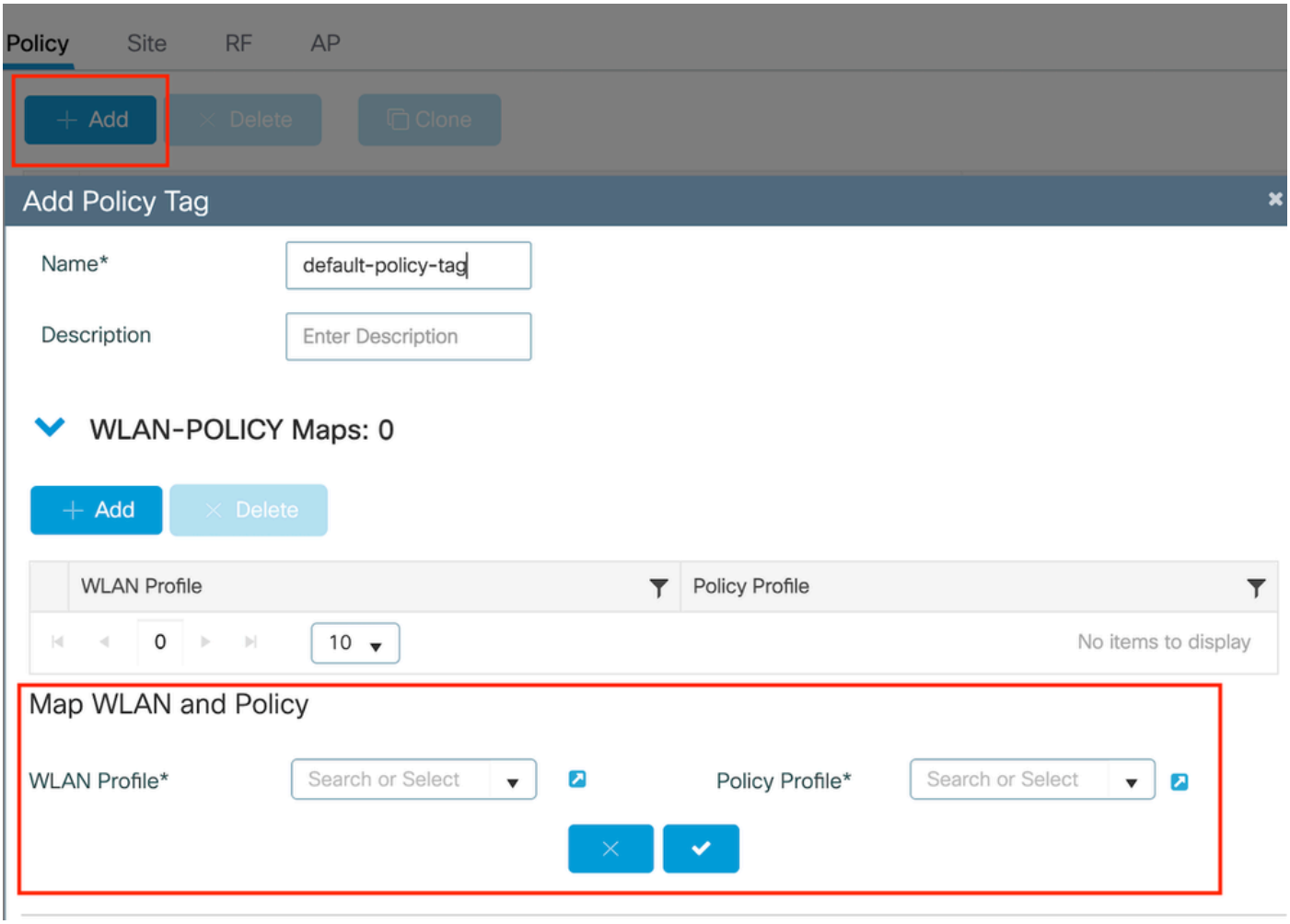
Onglet Sécurité de la couche 3 du WLAN

Configuration CLI

```
wlan Mac_Filtering_Wlan 9 Mac_Filtering_Wlan
 mac-filtering network
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 security web-auth
 security web-auth authentication-list ISE-List
 security web-auth on-macfilter-failure
 security web-auth parameter-map Web-Filter
 no shutdown
```

Étape 4 : configurez les balises de stratégie, créez le profil WLAN et le mappage du profil de stratégie

Accédez à Configuration > Tags & Profiles > Tags > Policy. Cliquez sur Ajouter pour définir un nom pour la balise de stratégie. Sous WLAN-Policy Maps, sélectionnez Add pour mapper le WLAN et le profil de stratégie précédemment créés.

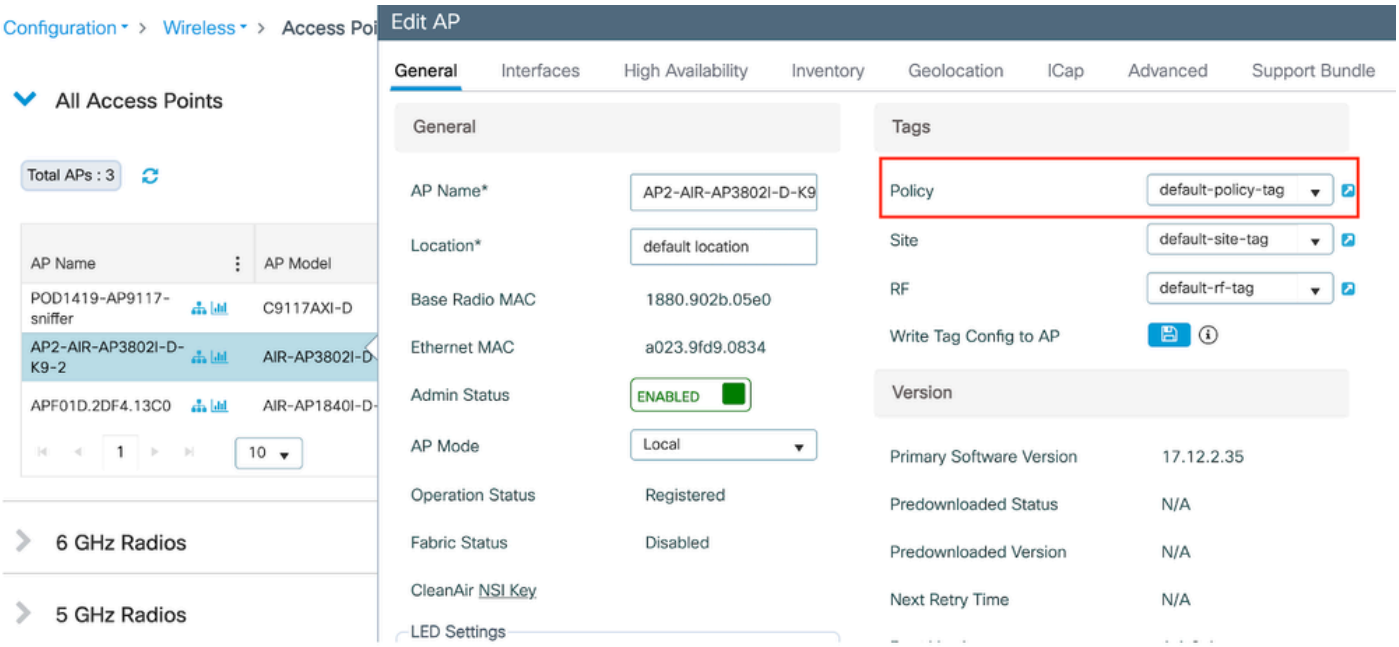


Mappage de balise de stratégie

Configuration CLI :

```
wireless tag policy default-policy-tag
 description "default policy-tag"
wlan Mac_Filtering_Wlan policy Web-Filter-Policy
```

Étape 5 : Accédez à Configuration > Wireless > Access Point. Sélectionnez le point d'accès chargé de diffuser ce SSID. Dans le menu Edit AP, affectez la balise de stratégie créée.

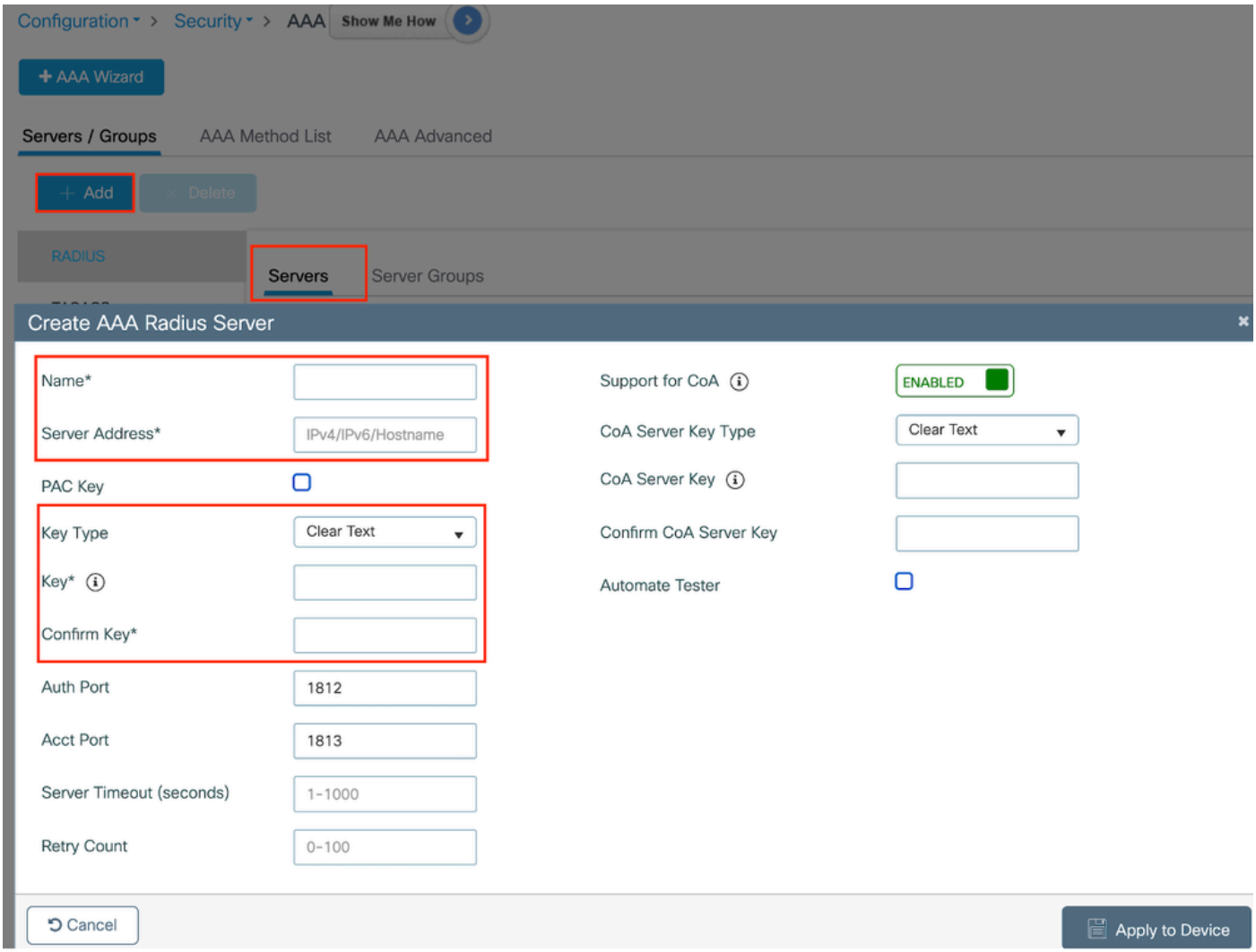


Mappage de la politique TAG vers AP

Configurez les paramètres AAA :

Étape 1 : Créez un serveur Radius :

Accédez à Configuration > Security > AAA. Cliquez sur l'option Ajouter sous la section Serveur/Groupe. Sur la page « Create AAA Radius Server », saisissez le nom du serveur, l'adresse IP et le secret partagé.



Configuration du serveur

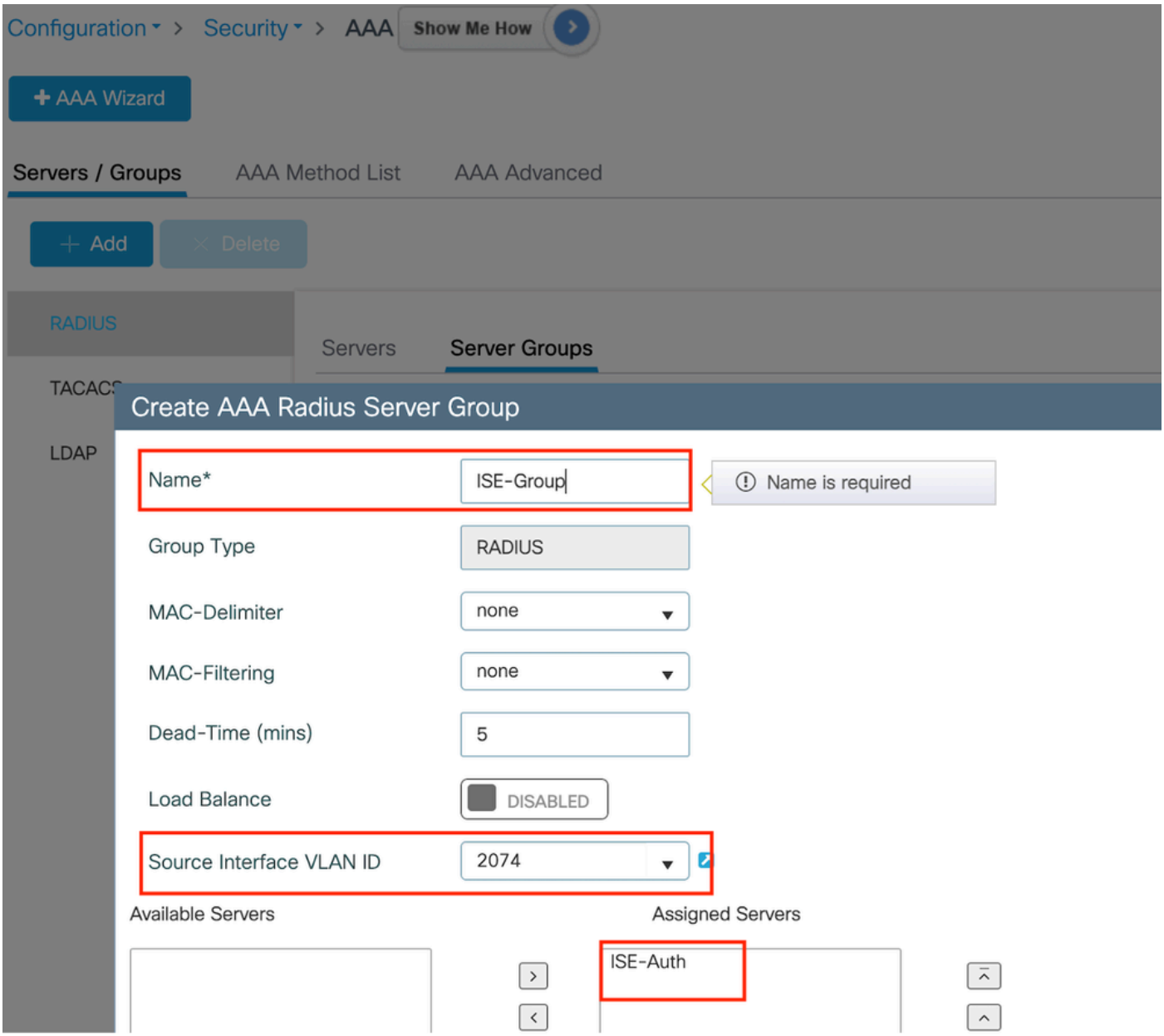
Configuration CLI

```
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 l'option Ajouter dans la section Groupes de serveurs pour définir un groupe de serveurs. Basculez les serveurs à inclure dans la même configuration de groupe.

Il n'est pas nécessaire de définir l'interface source. Par défaut, le routeur 9800 utilise sa table de routage pour déterminer l'interface à utiliser pour atteindre le serveur RADIUS et utilise généralement la passerelle par défaut.



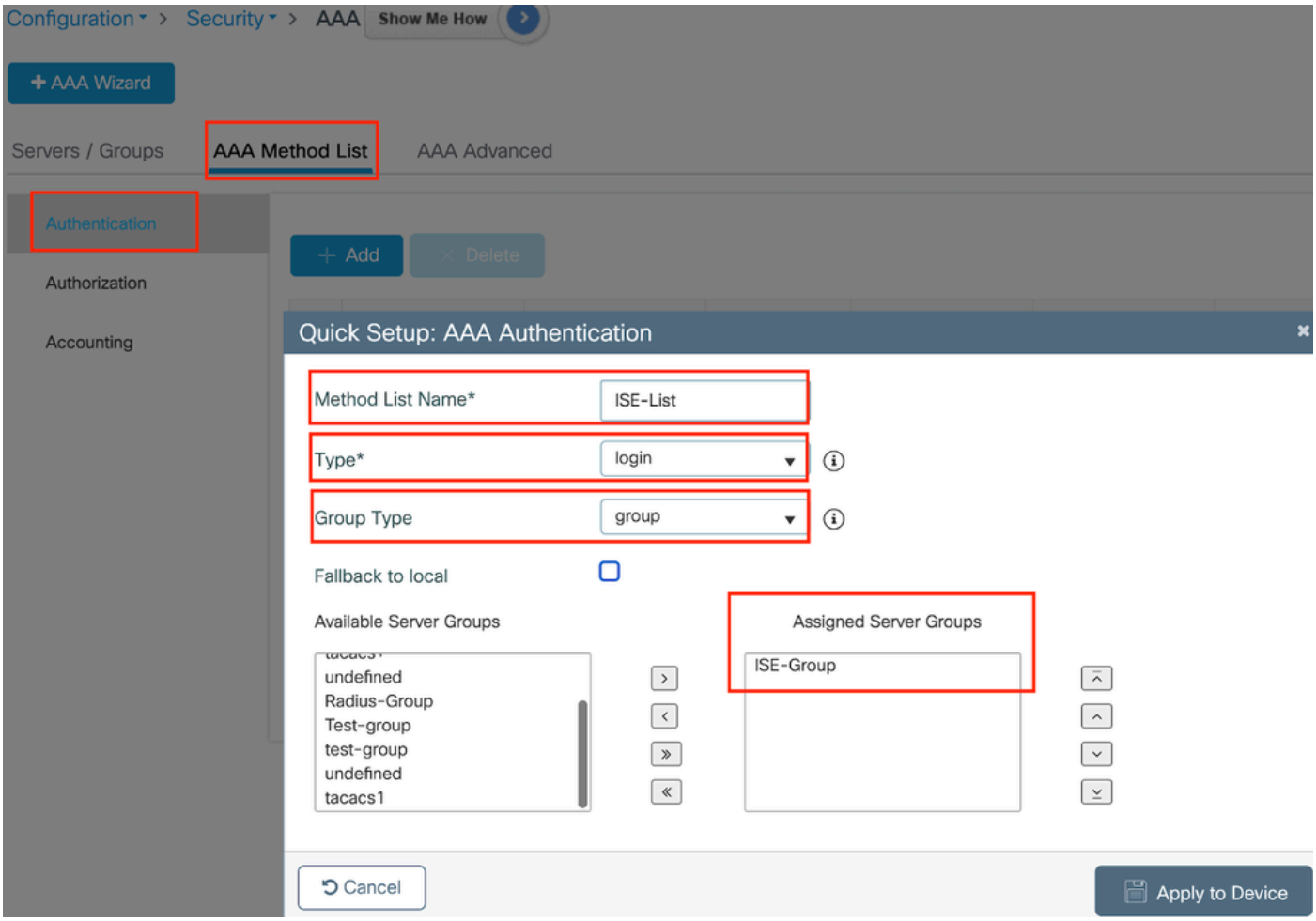
Groupe de serveurs

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. Sous Authentication, cliquez sur Add. Définissez un nom de liste de méthodes avec le type « login » et le type de groupe « Group ». Mappez le groupe de serveurs d'authentification configuré sous la section Groupe de serveurs assigné.

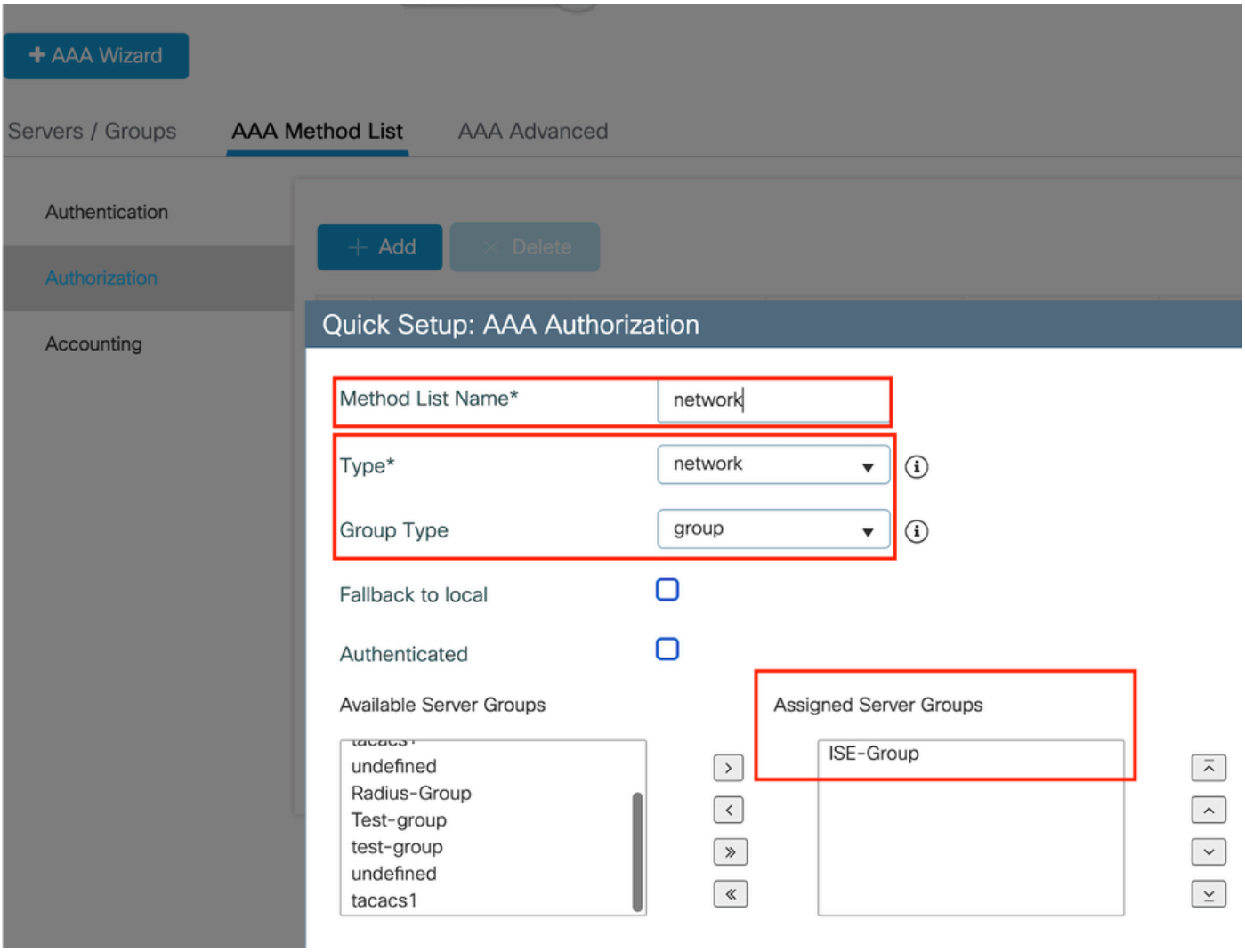


Liste des méthodes d'authentification

Configuration CLI

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

Accédez à la section Liste des méthodes d'autorisation et cliquez sur Ajouter. Définissez un nom de liste de méthodes et définissez le type sur « réseau » avec le type de groupe « Groupe ». Basculez le serveur RADIUS configuré vers la section Assigned Server Groups.



Liste des méthodes d'autorisation

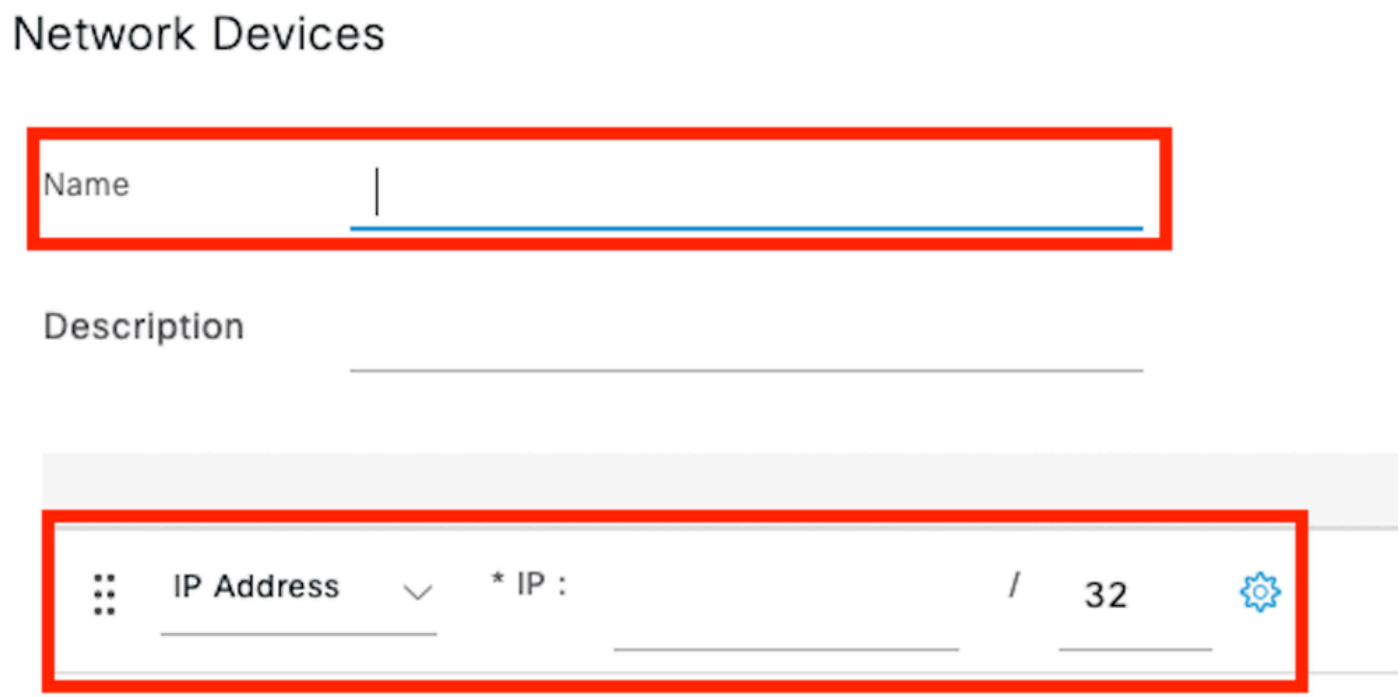
Configuration CLI

```
aaa authorization network network group ISE-Group
```

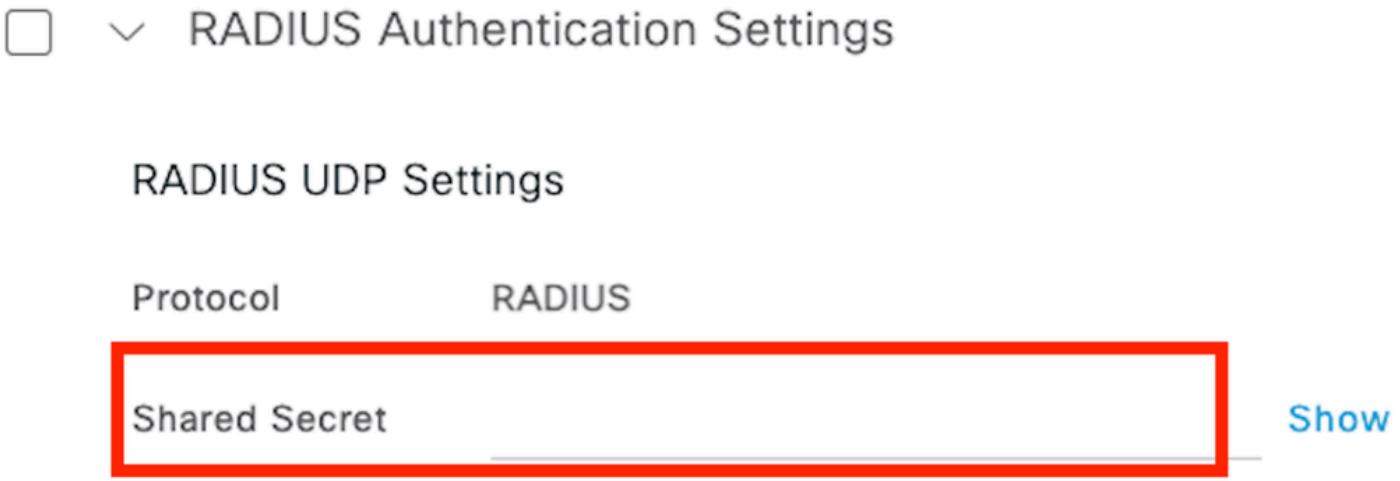
Configuration ISE:

Ajouter WLC en tant que périphérique réseau sur ISE

Étape 1 : Accédez à Administration > Network Devices et cliquez sur Add. Saisissez l'adresse IP, le nom d'hôte et le secret partagé du contrôleur dans les paramètres d'authentification Radius



Ajouter un périphérique réseau

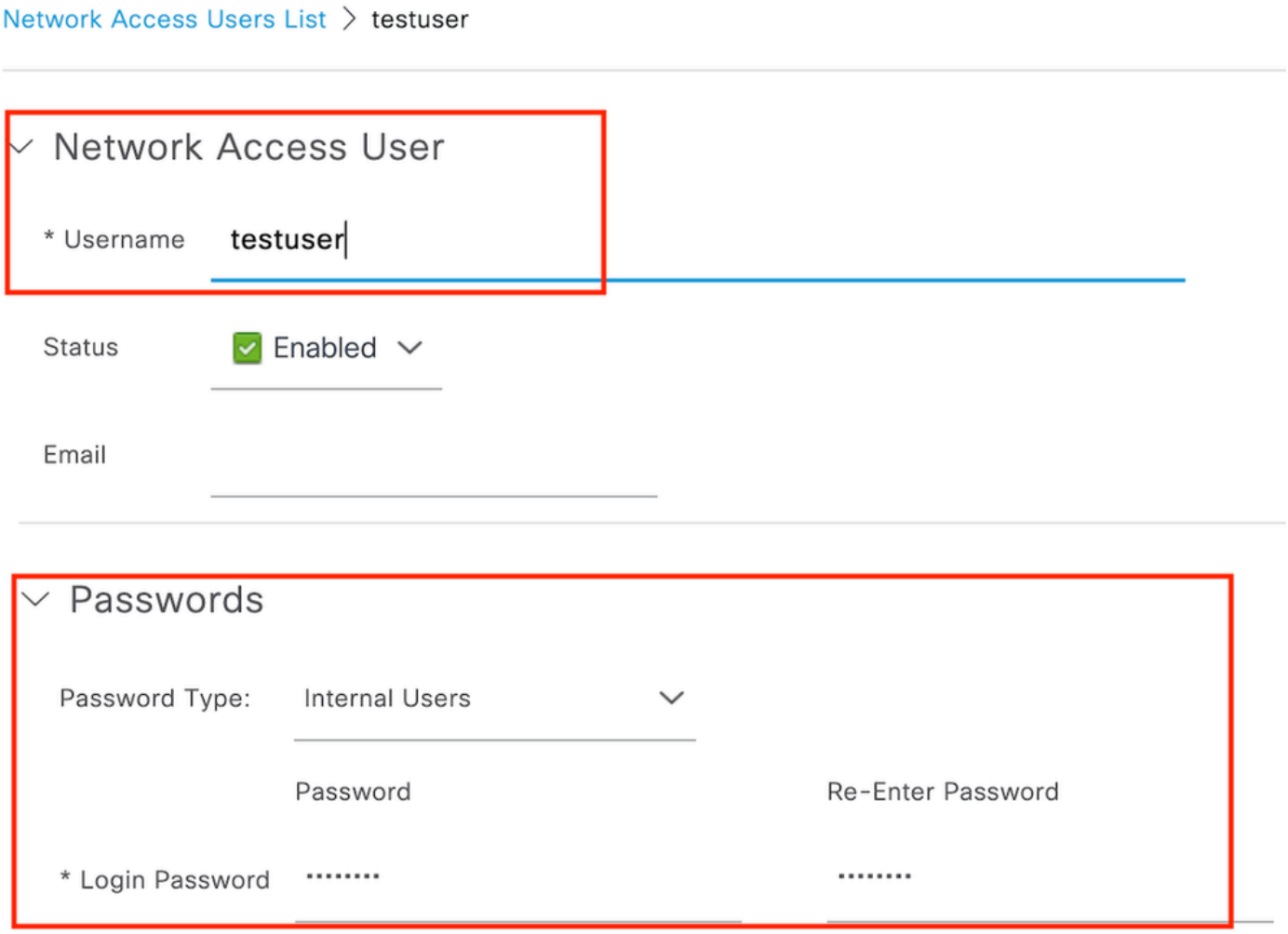


Secret partagé

Étape 2 : Créer une entrée utilisateur

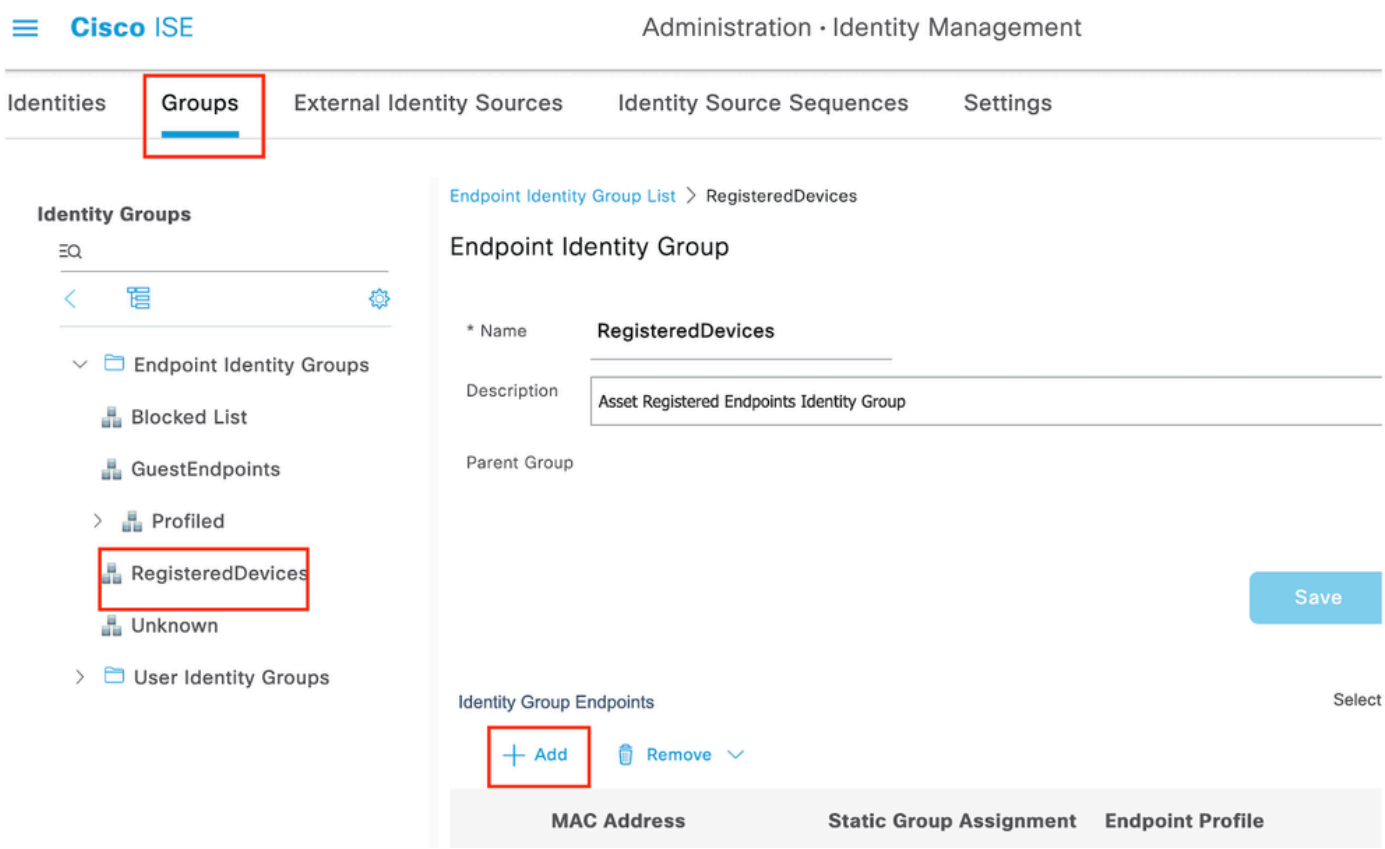
Sous Gestion des identités > Identités, sélectionnez l'option Ajouter.

Configurez le nom d'utilisateur et le mot de passe que le client doit utiliser pour l'authentification Web



Étape 3 : Accédez à Administration > Identity Management > Groups > Registered Devices et cliquez sur Add.

Entrez l'adresse MAC du périphérique pour créer une entrée sur le serveur.

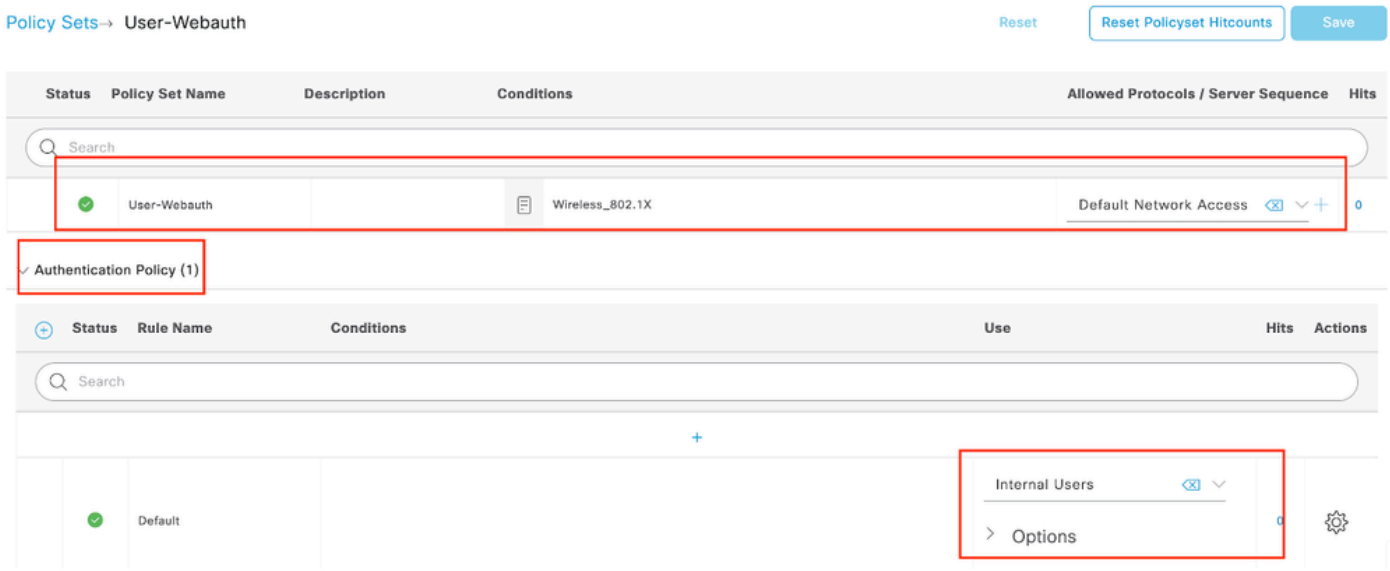


Ajouter une adresse MAC de périphérique

Étape 4 : Créez une stratégie de service

Accédez à Policy > Policy sets et sélectionnez le signe « + » pour créer un nouveau jeu de stratégies

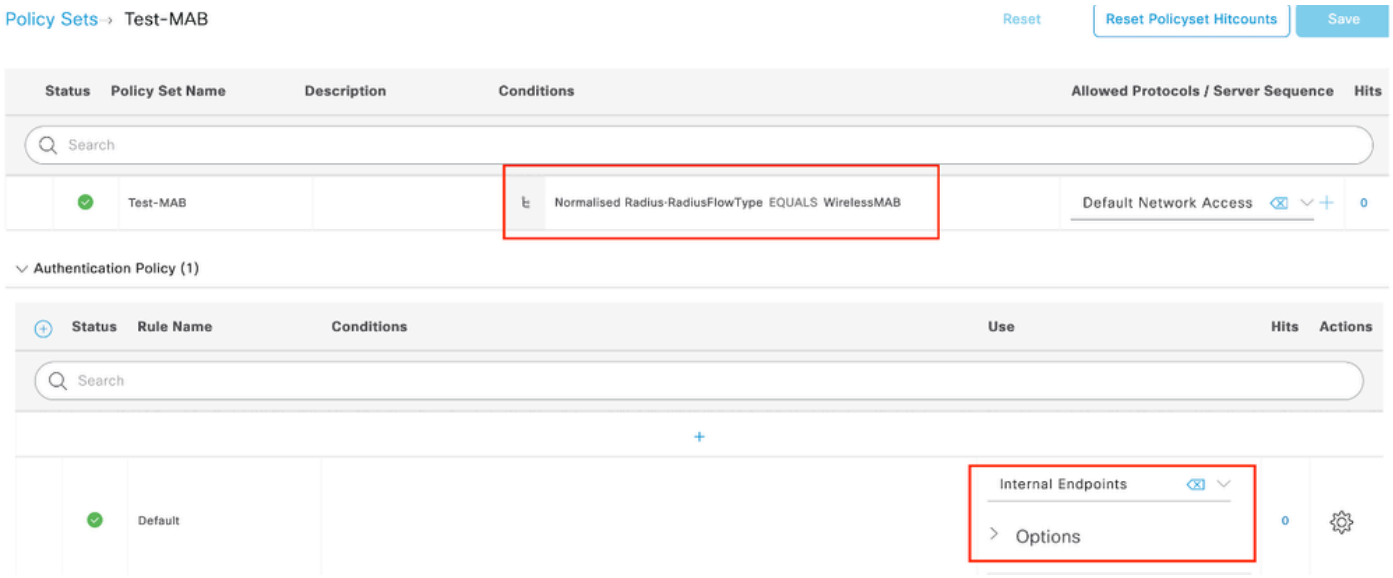
Ce jeu de stratégies est destiné à l'authentification Web des utilisateurs, où un nom d'utilisateur et un mot de passe pour le client sont créés dans la Gestion des identités



Stratégie du service d'authentification Web

De même, créez une stratégie de service MAB et mappez les terminaux internes sous la stratégie

d'authentification.



Stratégie de service d'authentification MAB

Vérifier

Configuration du contrôleur

<#root>

```
show wireless tag policy detailed
```

default-policy-tag

```
Policy Tag Name : default-policy-tag
Description     : default policy-tag
Number of WLAN-POLICY maps: 1
WLAN Profile Name                Policy Name
------------------------------------------------------------------------
```

Mac_Filtering_Wlan

Web-Filter-Policy

<#root>

```
show wireless profile policy detailed
```

Web-Filter-Policy

```
Policy Profile Name                :
```

Web-Filter-Policy

```
Description                          :
Status                               :
```

ENABLED

```
VLAN                                 :
```

2074

```
Multicast VLAN                       : 0
```

<#root>

```
show wlan name
```

Mac_Filtering_Wlan

```
WLAN Profile Name     :
```

Mac_Filtering_Wlan

```
================================================
Identifier                                 : 9
Description                                :
Network Name (SSID)                        :
```

Mac_Filtering_Wlan

```
Status                                     :
```

Enabled

```
Broadcast SSID                             :
```

Enabled

```
Mac Filter Authorization list name         :
```

network

```
Webauth On-mac-filter Failure              :
```

Enabled

```
    Webauth Authentication List Name       :
```

ISE-List

```
    Webauth Authorization List Name        : Disabled
    Webauth Parameter Map                  :
```

Web-Filter

<#root>

```
show parameter-map type webauth name Web-Filter
Parameter Map Name               :
```

Web-Filter

```
  Type                           :
```

webauth

```
  Auth-proxy Init State time     : 120 sec
  Webauth max-http connection    : 100
  Webauth logout-window          :
```

Enabled

```
  Webauth success-window         :
```

Enabled

```
  Consent Email                  : Disabled
  Activation Mode                : Replace
  Sleeping-Client                : Disabled
  Webauth login-auth-bypass:
```

<#root>

```
show ip http server status

HTTP server status:
```

Enabled

```
HTTP server port:
```

80

```
HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local
HTTP server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server IPv4 access class: None
HTTP server IPv6 access class: None
HTTP server base path:
HTTP File Upload status: Disabled
HTTP server upload path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 300
Maximum number of secondary server connections allowed: 50
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 600 seconds
Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status:
```

Enabled

```
HTTP secure server port:
```

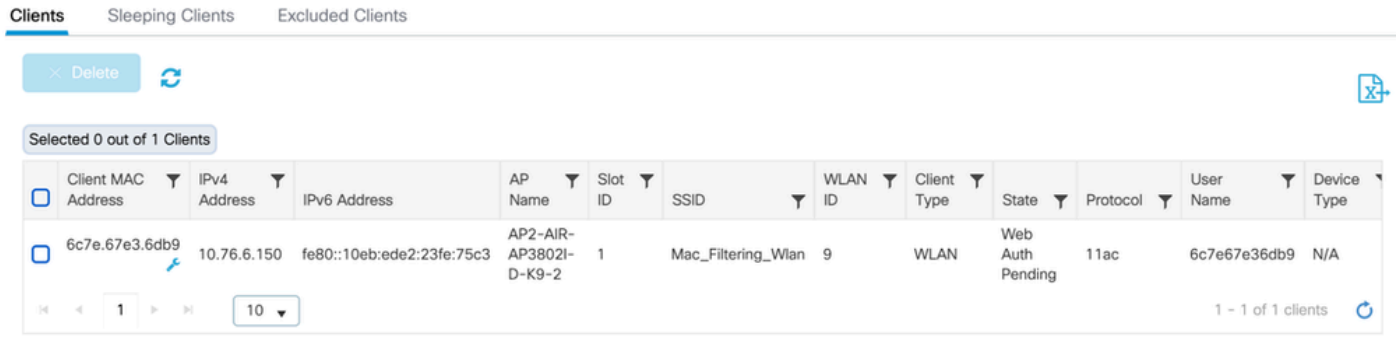
443

```
show ap name AP2-AIR-AP3802I-D-K9-2 tag detail

Policy tag mapping
```

```
------------------
WLAN Profile Name                Policy Name                      VLAN                              Flex
-------------------------------------------------------------------------------------------------------
Mac_Filtering_Wlan               Web-Filter-Policy                2074                              ENAB
```

État de la stratégie client sur le contrôleur

Accédez à la section Tableau de bord > Clients pour confirmer l'état des clients connectés.
Le client est actuellement en attente d'authentification Web



Détail du client

```
show wireless client summary
Number of Clients: 1
MAC Address    AP Name                                          Type ID   State             Protocol Meth
-------------------------------------------------------------------------------------------------------
6c7e.67e3.6db9 AP2-AIR-AP3802I-D-K9-2                           WLAN 9    Webauth Pending   11ac     Web
```

<#root>

```
show wireless client mac-address 6c7e.67e3.6db9 detail
Client MAC Address :
```

6c7e.67e3.6db9

```
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
```

10.76.6.150

```
Client IPv6 Addresses : fe80::10eb:ede2:23fe:75c3
Client Username :
```

6c7e67e36db9

```
AP MAC Address : 1880.902b.05e0
AP Name: AP2-AIR-AP3802I-D-K9-2
AP slot : 1
Client State : Associated
Policy Profile :
```

Web-Filter-Policy

```
Flex Profile : N/A
Wireless LAN Id: 9
WLAN Profile Name:
```

Mac_Filtering_Wlan

```
Wireless LAN Network Name (SSID): Mac_Filtering_Wlan
BSSID : 1880.902b.05eb

Client ACLs : None
Mac authentication :
```

Failed

```
Policy Manager State:
```

Webauth Pending

```
Last Policy Manager State :
```

IP Learn Complete

```
Client Entry Create Time : 88 seconds
Policy Type : N/A
Encryption Cipher : None

Auth Method Status List
        Method : Web Auth
                Webauth State    :
```

Get Redirect

```
                Webauth Method   :
```

Webauth

Une fois l'authentification Web réussie, le gestionnaire de stratégies client passe à l'état EXÉCUTER

<#root>

```
show wireless client mac-address 6c7e.67e3.6db9 detail

Client ACLs : None
Mac authentication : Failed
Policy Manager State:
```

Run

```
Last Policy Manager State :
```

Webauth Pending

```
Client Entry Create Time : 131 seconds
Policy Type : N/A
```

Dépannage

La fonctionnalité d'authentification Web sur échec MAC repose sur la capacité du contrôleur à déclencher l'authentification Web en cas d'échec MAB. Notre objectif principal est de collecter efficacement les traces d'annonce de routeur à partir du contrôleur pour le dépannage et l'analyse.

Collecte des traces radioactives

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 .

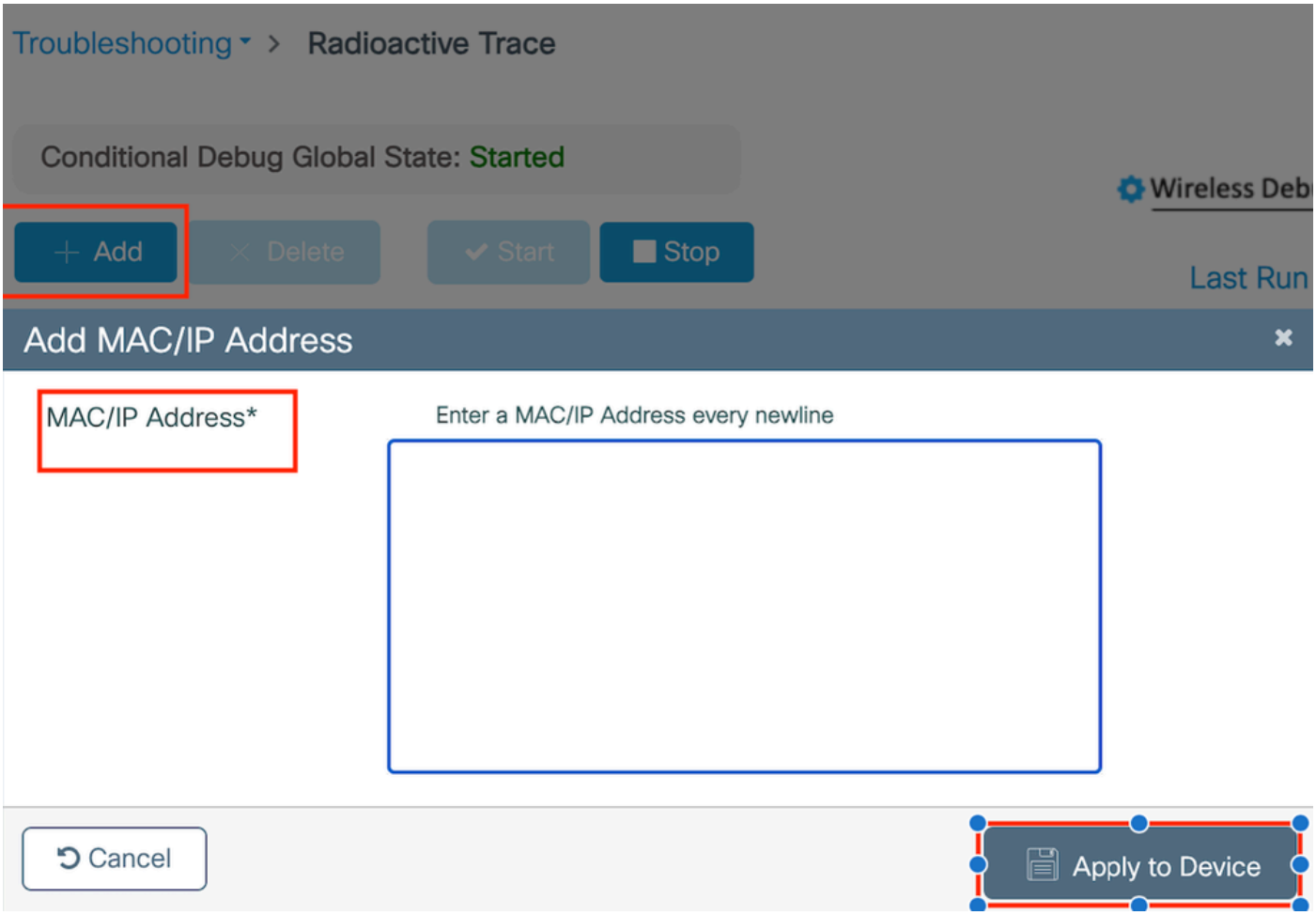
```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP addr
```

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,

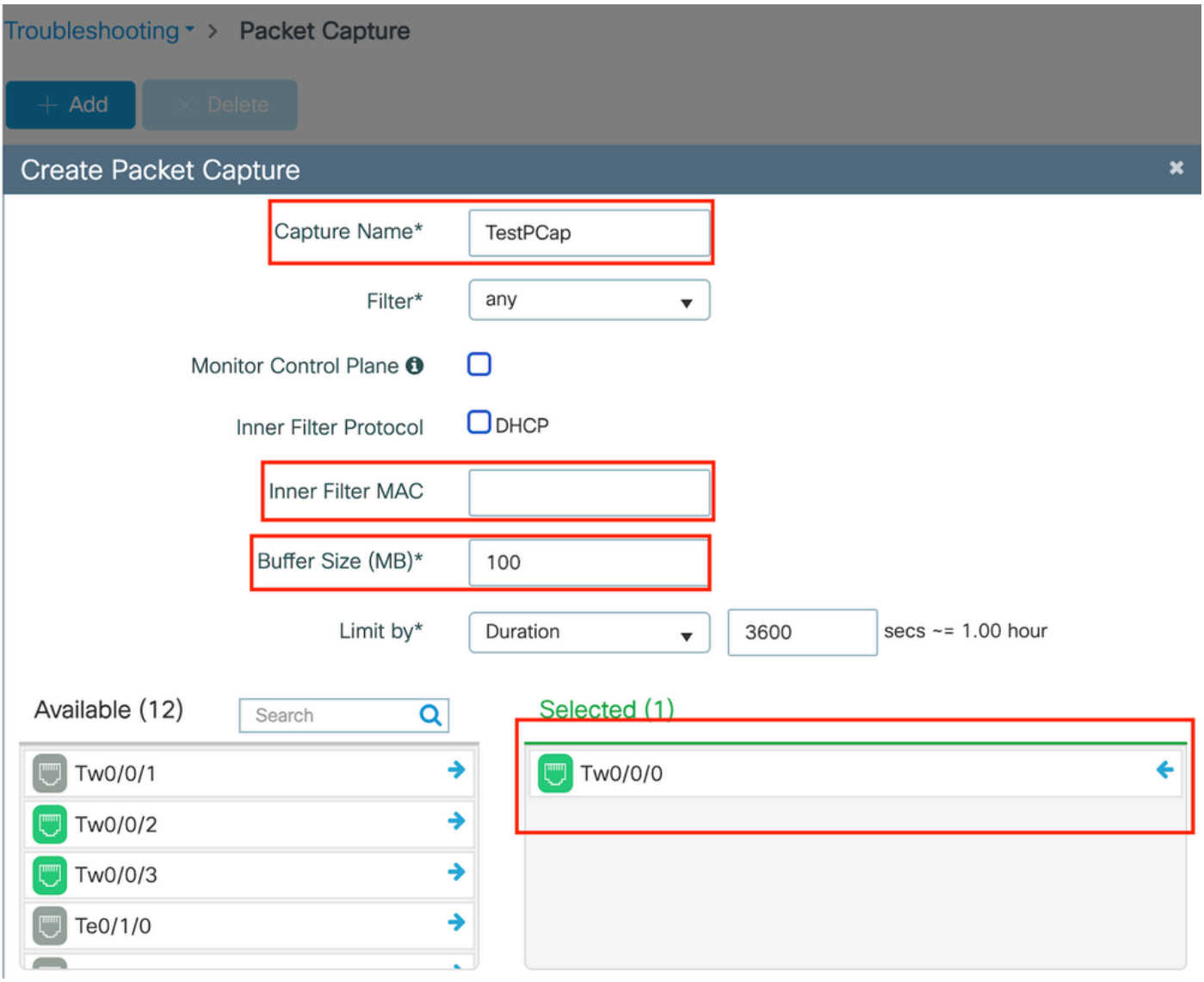
Étape 1 : Accédez à Troubleshooting > Radioactive Trace. Sélectionnez l'option permettant d'ajouter une nouvelle entrée, puis saisissez l'adresse MAC du client dans l'onglet Add MAC/IP Address (Ajouter une adresse MAC/IP).



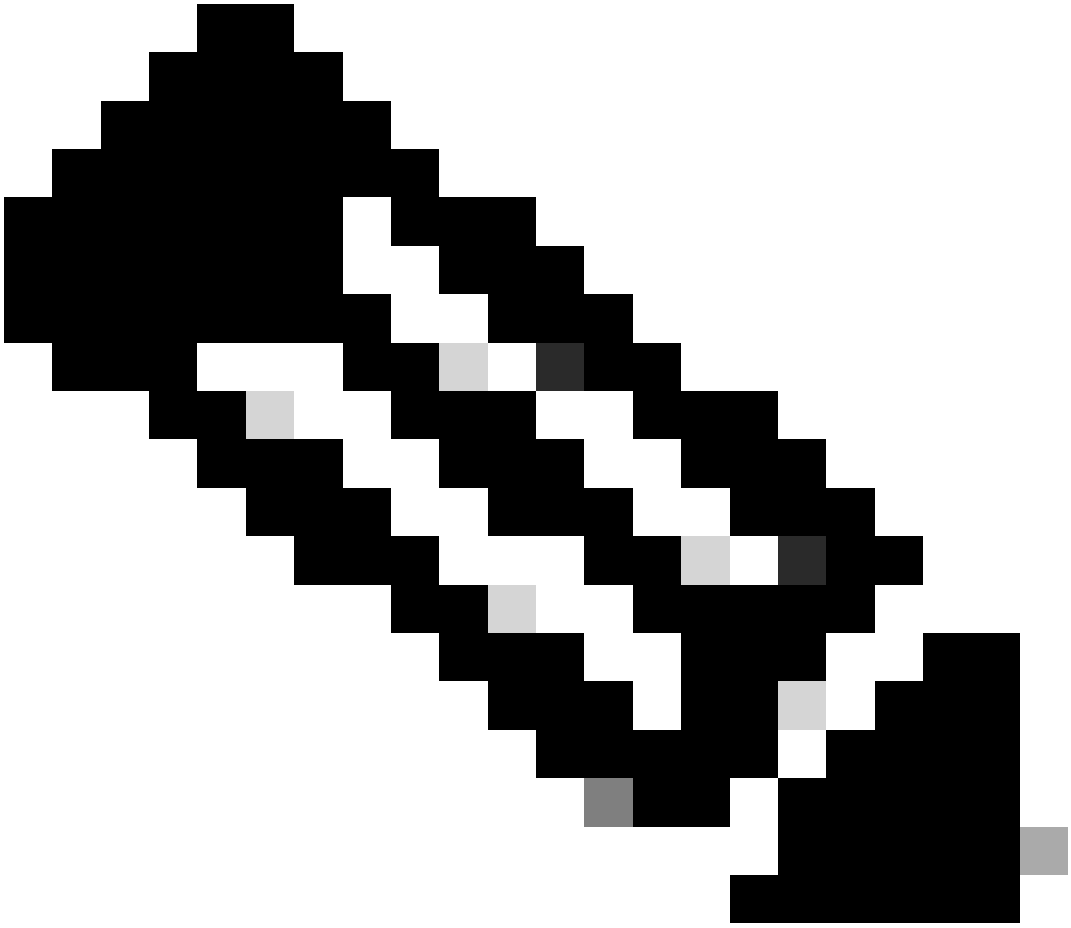
Suivi RA

Captures de paquets intégrées :

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.

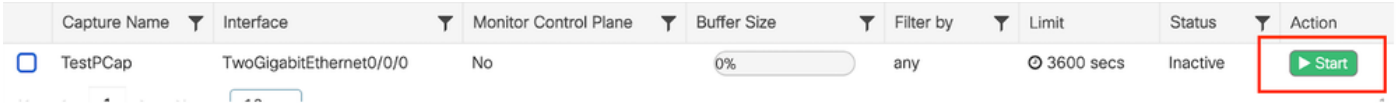


Capture de paquets intégrée



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.

Sélectionnez Start pour capturer les paquets



Commencer la capture

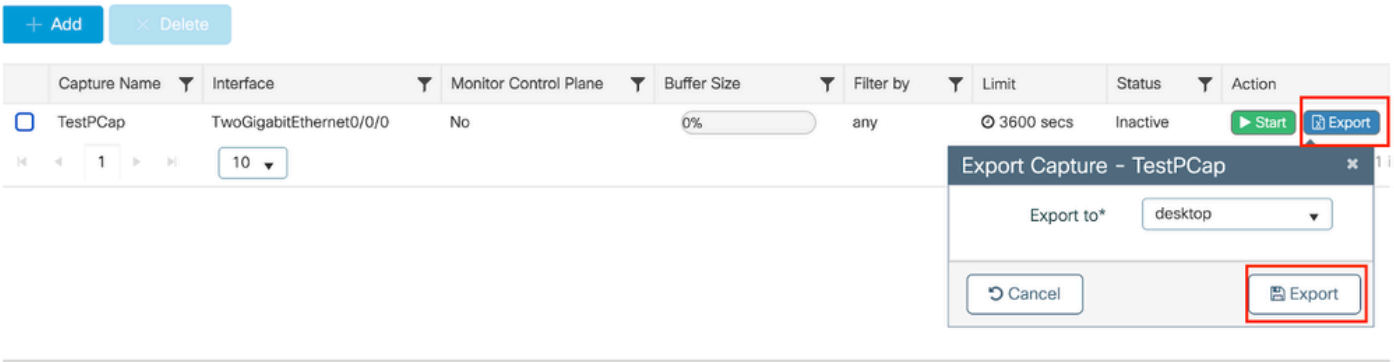
Configuration CLI

```
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)
```

Exporter la capture de paquets vers un serveur TFTP externe

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



Exporter la capture de paquets

Exemple de scénario au cours d'une authentification MAC réussie, un périphérique client se connecte au réseau, son adresse MAC est validée par le serveur RADIUS par le biais de stratégies configurées et, après vérification, l'accès est accordé par le périphérique d'accès réseau, ce qui permet la connectivité réseau.

Une fois le client associé, le contrôleur envoie une requête d'accès au serveur ISE,

Le nom d'utilisateur est l'adresse MAC du client car il s'agit de l'authentification MAB

```
2024/07/16 21:12:52.711298748 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/16 21:12:52.711310730 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator 19 c6
2024/07/16 21:12:52.711326401 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/16 21:12:52.711329615 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Password
2024/07/16 21:12:52.711337331 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Service-Type
2024/07/16 21:12:52.711340443 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
2024/07/16 21:12:52.711344513 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:   Cisco AVpair
2024/07/16 21:12:52.711349087 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Framed-MTU
2024/07/16 21:12:52.711351935 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
2024/07/16 21:12:52.711377387 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  EAP-Key-Name
2024/07/16 21:12:52.711382613 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
2024/07/16 21:12:52.711385989 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:   Cisco AVpair
```

ISE envoie Access-Accept car nous avons une entrée utilisateur valide

```
2024/07/16 21:12:52.779147404 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/16 21:12:52.779156117 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator 5d dc
2024/07/16 21:12:52.779161793 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/16 21:12:52.779165183 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Class
2024/07/16 21:12:52.779219803 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
```

```
2024/07/16 21:12:52.779417578 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
2024/07/16 21:12:52.779436247 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
```

État de la stratégie client passé à Mac Auth terminé

```
2024/07/16 21:12:52.780181486 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67b7.2d29  Cli
2024/07/16 21:12:52.780238297 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: 6c7e.67b7.2d29
```

Le client est en état d'apprentissage IP après une authentification MAB réussie

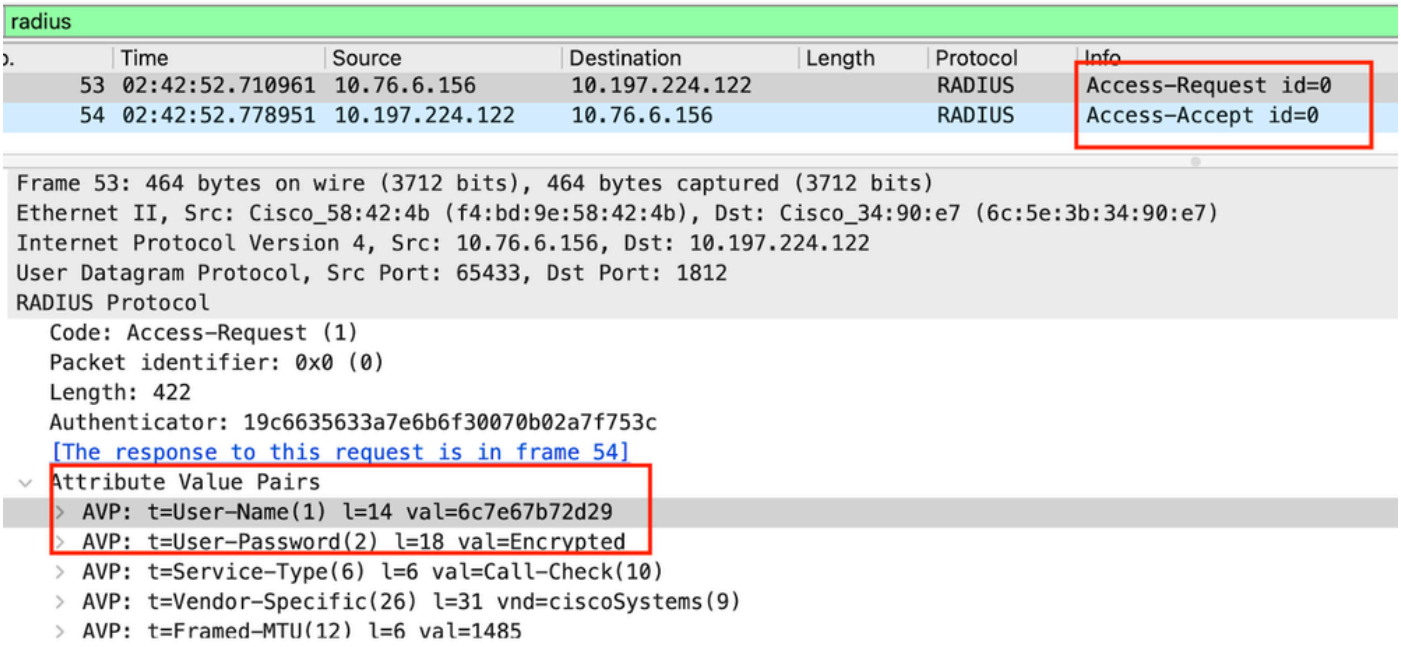
```
2024/07/16 21:12:55.791404789 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67b7.2d2
2024/07/16 21:12:55.791739386 {wncd_x_R0-0}{1}: [client-iplearn] [17765]: (info): MAC: 6c7e.67b7.2d29
```

```
2024/07/16 21:12:55.794130301 {iosrp_R0-0}{1}: [buginf] [4440]: (debug): AUTH-FEAT-SISF-EVENT: IP updat
```

L'état du gestionnaire de stratégie client est mis à jour en RUN, l'authentification Web est ignorée pour le client qui termine l'authentification MAB

```
2024/07/16 21:13:11.210786952 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
```

Vérification via la capture de paquets intégrée



Paquet Radius

Exemple d'échec d'authentification MAC pour un périphérique client

Authentification Mac lancée pour un client après une association réussie

```
2024/07/17 03:20:59.842211775 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842280253 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17765]: (note): Authentication Succes
2024/07/17 03:20:59.842284313 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9  Cli
2024/07/17 03:20:59.842320572 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
```

ISE enverrait Access-Reject car cette entrée de périphérique n'est pas présente dans ISE

```
2024/07/17 03:20:59.842678322 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842877636 {wncd_x_R0-0}{1}: [auth-mgr] [17765]: (info): [6c7e.67e3.6db9:capwap_9000
```

L'authentification Web a été lancée pour le périphérique client car MAB a échoué

```
2024/07/17 03:20:59.843728206 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9  Cli
```

Une fois que le client lance une requête HTTP GET, l'URL de redirection est envoyée au périphérique client lorsque la session TCP correspondante est usurpée par le contrôleur.

```
2024/07/17 03:21:37.817434046 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (info): capwap_90000005[6c7e.6
2024/07/17 03:21:37.817459639 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817466483 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817482231 {wncd_x_R0-0}{1}: [webauth-state] [17765]: (info): capwap_90000005[6c7e.6
```

Le client lance une requête HTTP Get vers l'URL de redirection et une fois la page chargée, les informations d'identification de connexion sont envoyées.

Le contrôleur envoie une demande d'accès à ISE

Il s'agit d'une authentification Web car un nom d'utilisateur valide est observé dans le paquet d'acceptation d'accès

```
2024/07/17 03:22:51.132347799 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/17 03:22:51.132362949 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator fd 40
2024/07/17 03:22:51.132368737 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Calling-Station-Id
2024/07/17 03:22:51.132372791 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/17 03:22:51.132376569 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
```

Acceptation d'accès reçue d'ISE

```
2024/07/17 03:22:51.187040709 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/17 03:22:51.187050061 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator d3 ac
2024/07/17 03:22:51.187055731 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/17 03:22:51.187059053 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Class
2024/07/17 03:22:51.187102553 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
```

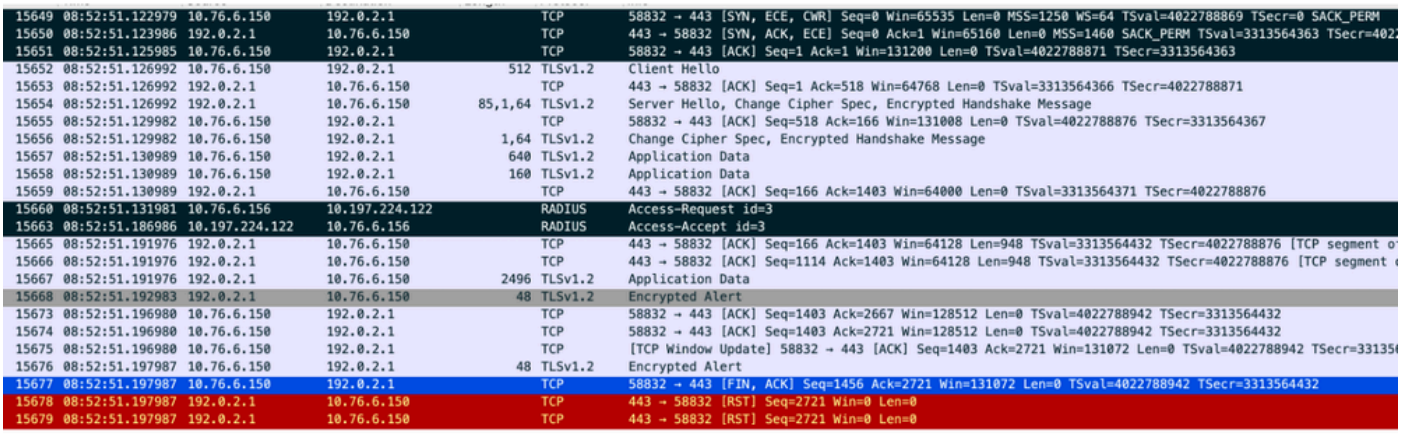
Authentification Web réussie et passage de l'état client à l'état EXÉCUTÉ

```
2024/07/17 03:22:51.193775717 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/17 03:22:51.194009423 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67e3.6db
```

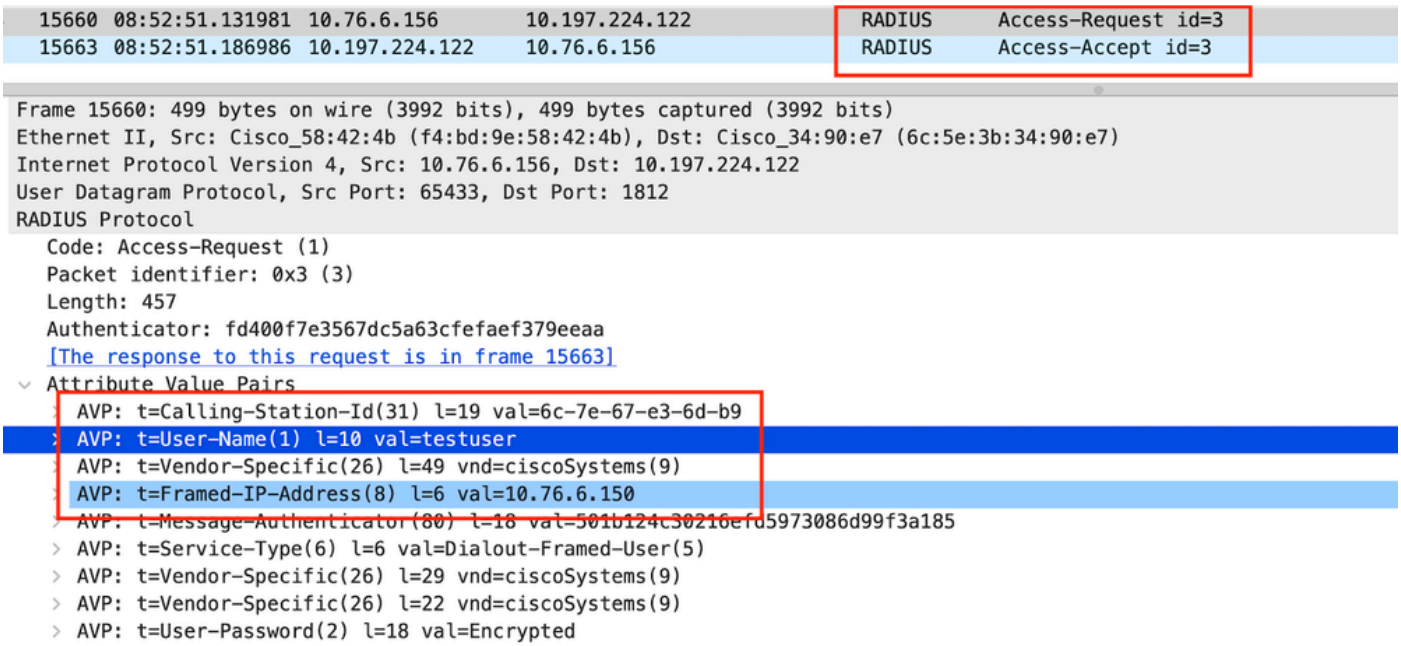
Vérification via des captures EPC

Le client termine la connexion TCP avec l'adresse IP virtuelle du contrôleur et charge la page du portail de redirection. Une fois que l'utilisateur a envoyé le nom d'utilisateur et le mot de passe, nous pouvons observer une requête d'accès radius à partir de l'adresse IP de gestion du contrôleur.

Une fois l'authentification réussie, la session TCP du client est fermée et le client passe à l'état RUN sur le contrôleur.

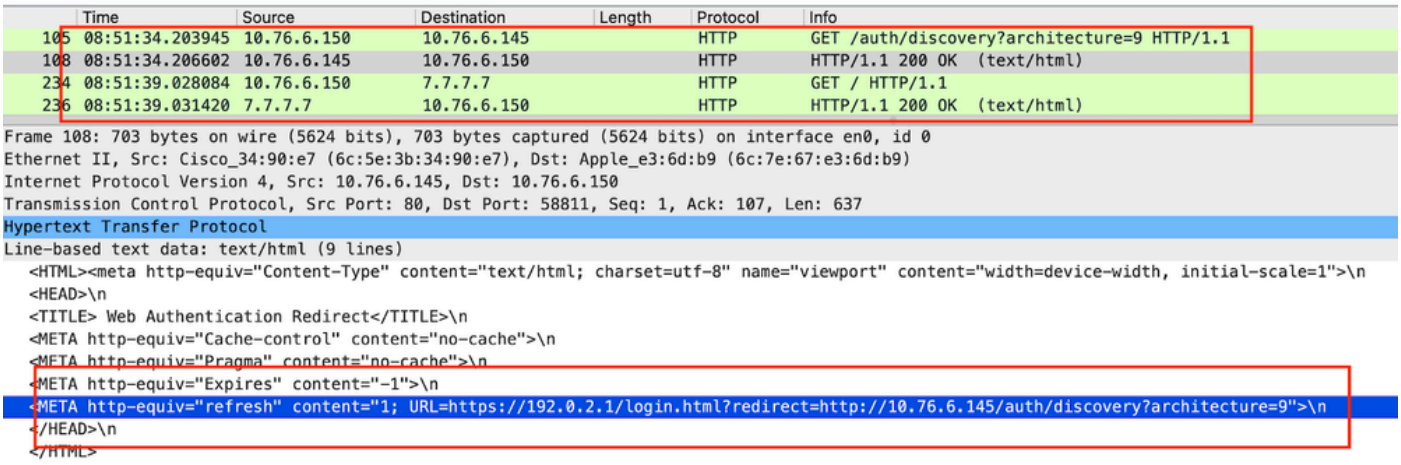


Flux TCP avec paquet radius



Paquet Radius envoyé à ISE avec informations d'identification utilisateur

Capture Wireshark côté client pour valider que le trafic client est redirigé vers la page du portail et valider la connexion TCP au contrôleur adresse IP virtuelle/serveur Web

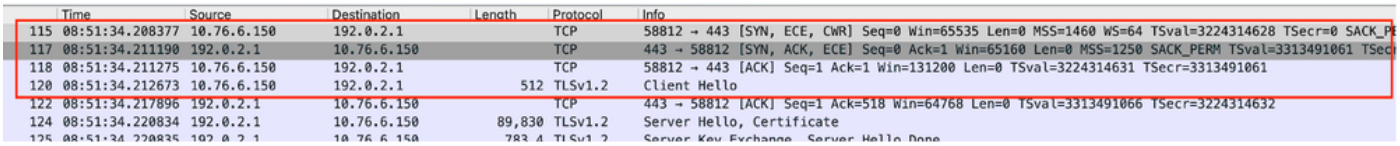


	Time	Source	Destination	Length	Protocol	Info
105	08:51:34.203945	10.76.6.150	10.76.6.145		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
108	08:51:34.206602	10.76.6.145	10.76.6.150		HTTP	HTTP/1.1 200 OK (text/html)
234	08:51:39.028084	10.76.6.150	7.7.7.7		HTTP	GET / HTTP/1.1
236	08:51:39.031420	7.7.7.7	10.76.6.150		HTTP	HTTP/1.1 200 OK (text/html)

```
Frame 108: 703 bytes on wire (5624 bits), 703 bytes captured (5624 bits) on interface en0, id 0
Ethernet II, Src: Cisco_34:90:e7 (6c:5e:3b:34:90:e7), Dst: Apple_e3:6d:b9 (6c:7e:67:e3:6d:b9)
Internet Protocol Version 4, Src: 10.76.6.145, Dst: 10.76.6.150
Transmission Control Protocol, Src Port: 80, Dst Port: 58811, Seq: 1, Ack: 107, Len: 637
Hypertext Transfer Protocol
Line-based text data: text/html (9 lines)
  <HTML><meta http-equiv="Content-Type" content="text/html; charset=utf-8" name="viewport" content="width=device-width, initial-scale=1">\n
  <HEAD>\n
  <TITLE> Web Authentication Redirect</TITLE>\n
  <META http-equiv="Cache-control" content="no-cache">\n
  <META http-equiv="Pragma" content="no-cache">\n
  <META http-equiv="Expires" content="-1">\n
  <META http-equiv="refresh" content="1; URL=https://192.0.2.1/login.html?redirect=http://10.76.6.145/auth/discovery?architecture=9">\n
  </HEAD>\n
  </HTML>
```

Capture côté client pour valider l'URL de redirection

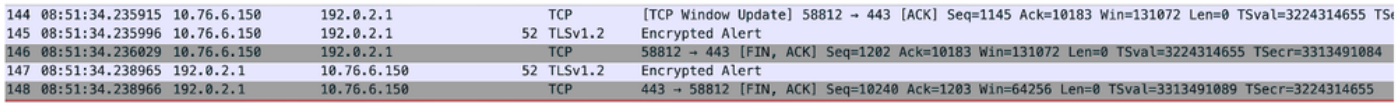
Le client établit une connexion TCP à l'adresse IP virtuelle du contrôleur



	Time	Source	Destination	Length	Protocol	Info
115	08:51:34.208377	10.76.6.150	192.0.2.1		TCP	58812 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3224314628 TSecr=0 SACK_PE
117	08:51:34.211190	192.0.2.1	10.76.6.150		TCP	443 → 58812 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1250 SACK_PERM TSval=3313491061 TSecr
118	08:51:34.211275	10.76.6.150	192.0.2.1		TCP	58812 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=3224314631 TSecr=3313491061
120	08:51:34.212673	10.76.6.150	192.0.2.1	512	TLSv1.2	Client Hello
122	08:51:34.217896	192.0.2.1	10.76.6.150		TCP	443 → 58812 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313491066 TSecr=3224314632
124	08:51:34.220834	192.0.2.1	10.76.6.150	89,830	TLSv1.2	Server Hello, Certificate
125	08:51:34.220835	192.0.2.1	10.76.6.150	783.4	TLSv1.2	Server Key Exchange, Server Hello Done

Connexion TCP entre le client et le serveur Web

La session est fermée après une authentification Web réussie.



144	08:51:34.235915	10.76.6.150	192.0.2.1		TCP	[TCP Window Update] 58812 → 443 [ACK] Seq=1145 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSe
145	08:51:34.235996	10.76.6.150	192.0.2.1	52	TLSv1.2	Encrypted Alert
146	08:51:34.236029	10.76.6.150	192.0.2.1		TCP	58812 → 443 [FIN, ACK] Seq=1202 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491084
147	08:51:34.238965	192.0.2.1	10.76.6.150	52	TLSv1.2	Encrypted Alert
148	08:51:34.238966	192.0.2.1	10.76.6.150		TCP	443 → 58812 [FIN, ACK] Seq=10240 Ack=1203 Win=64256 Len=0 TSval=3313491089 TSecr=3224314655

Session TCP fermée après l'authentification Web du client

Article connexe

[Comprendre les débogages sans fil et la collecte de journaux sur les contrôleurs LAN sans fil Catalyst 9800]

[Authentification Web sur le 9800]

[Configurer l'authentification Web locale sur le 9800]

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

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