Configuración de Verificación y Troubleshooting de Web Auth en Mac Filter Failure

Contenido

Introducción

Este documento describe cómo configurar, solucionar problemas y verificar la autenticación Web local en la función "Mac Filter Failure" usando ISE para la autenticación externa.

Prerequisites

Configuración de ISE para autenticación MAC

Credenciales de usuario válidas configuradas en ISE/Active Directory

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

Información básica para navegar por la interfaz de usuario web del controlador

Configuración de etiquetas de políticas, perfil WLAN y política

Configuración de políticas de servicio en ISE

Componentes Utilizados

9800 WLC versión 17.12.2

AP AXI C9120

9300 switch

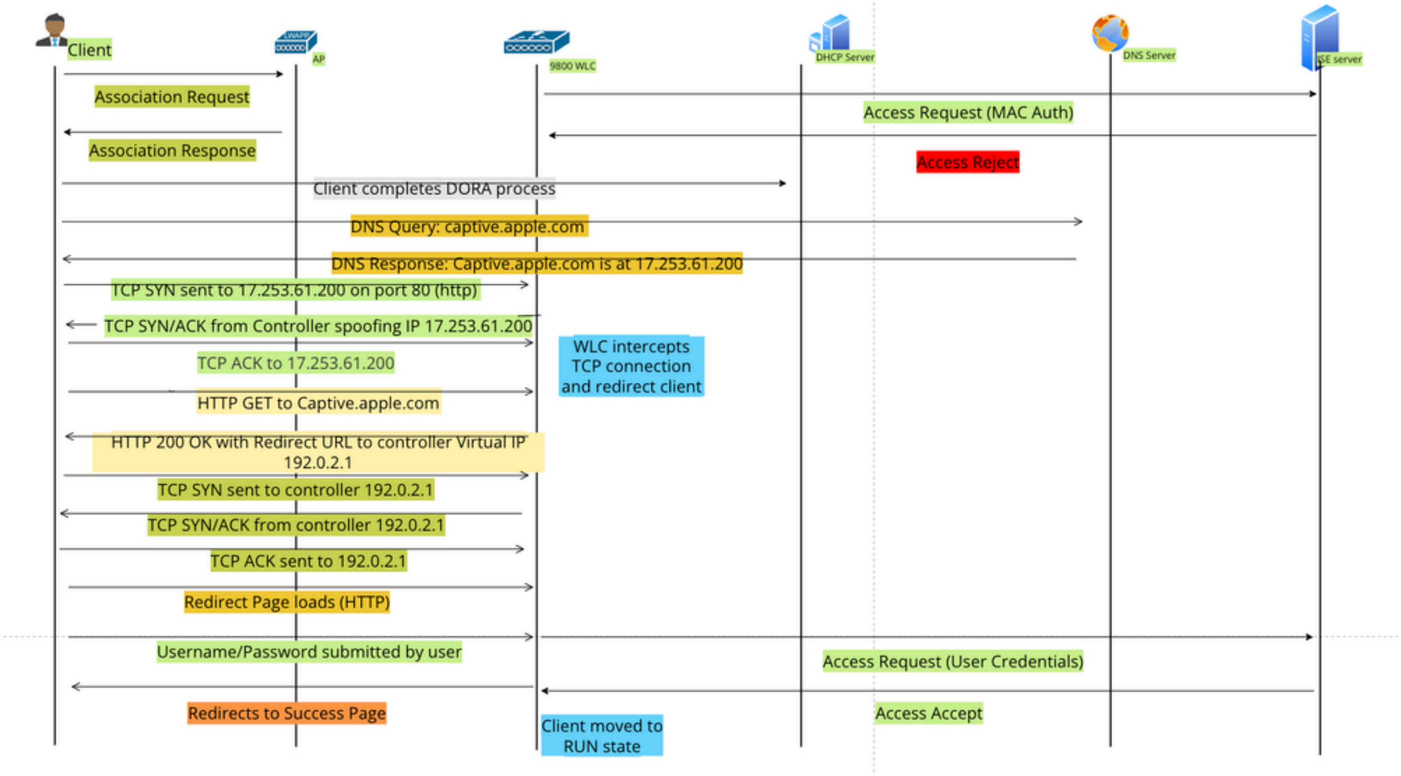
ISE versión 3.1.0.518

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La función Web Auth "On Mac Failure Filter" sirve como mecanismo de reserva en entornos WLAN que utilizan tanto la autenticación MAC como la autenticación Web.

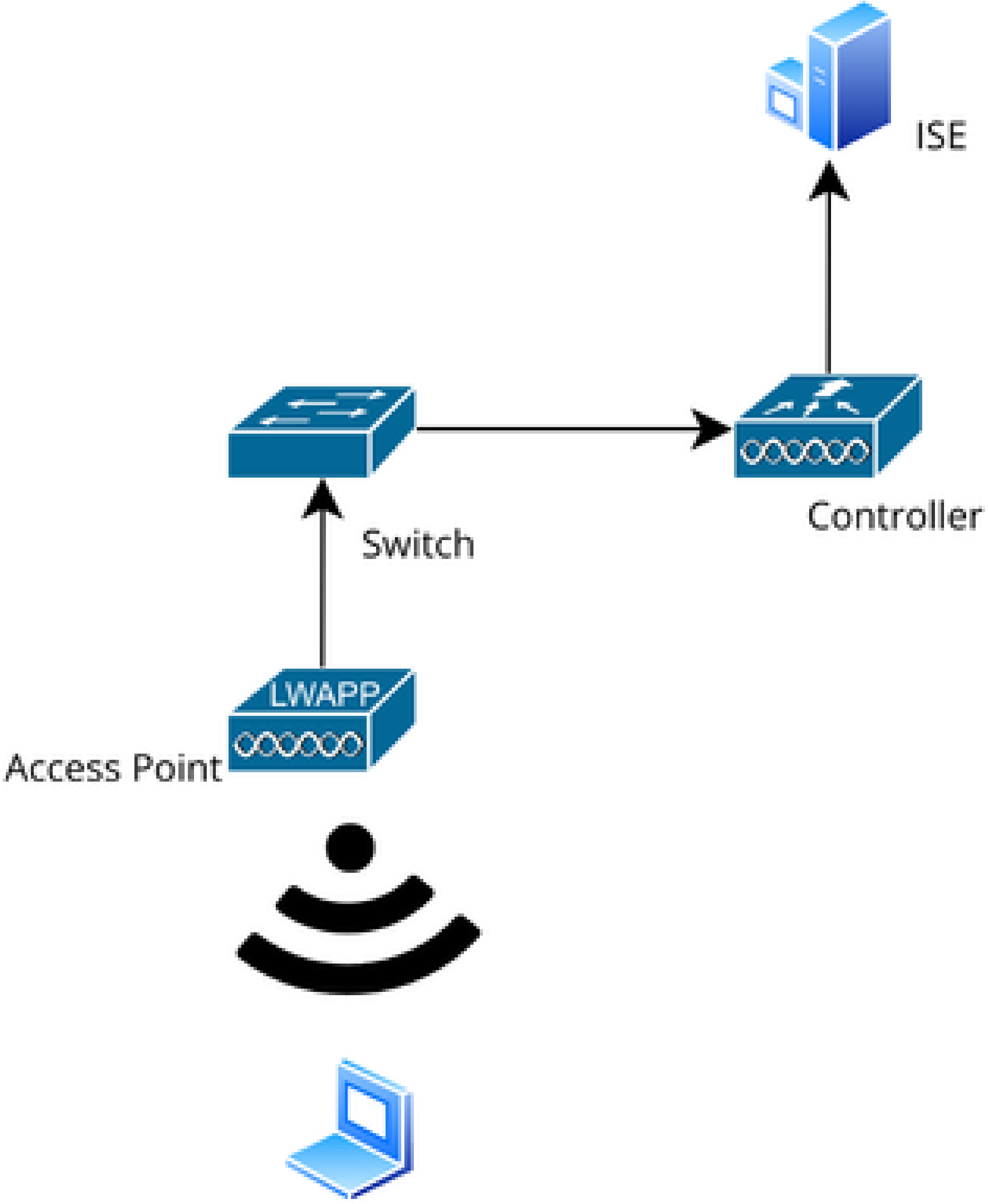
- Mecanismo de reserva: cuando un cliente intenta conectarse a una WLAN con filtro MAC en un servidor RADIUS externo (ISE) o un servidor local y no puede autenticarse, esta función inicia automáticamente una autenticación Web de capa 3.
- Autenticación satisfactoria: Si un cliente se autentica correctamente a través del filtro MAC, se omite la autenticación Web, lo que permite al cliente conectarse directamente a la WLAN.
- Cómo Evitar las Desasociaciones: Esta función ayuda a evitar las desasociaciones que, de lo contrario, podrían producirse debido a los fallos de autenticación del filtro MAC.


Client
AP
9800 WLC
DHCP Server
DNS Server
ISE server
Association Request
Access Request (MAC Auth)
Association Response
Access Reject
Client completes DORA process
DNS Query: captive.apple.com
DNS Response: Captive.apple.com is at 17.253.61.200
TCP SYN sent to 17.253.61.200 on port 80 (http)
TCP SYN/ACK from Controller spoofing IP 17.253.61.200
WLC intercepts TCP connection and redirect client
TCP ACK to 17.253.61.200
HTTP GET to Captive.apple.com
HTTP 200 OK with Redirect URL to controller Virtual IP 192.0.2.1
TCP SYN sent to controller 192.0.2.1
TCP SYN/ACK from controller 192.0.2.1
TCP ACK sent to 192.0.2.1
Redirect Page loads (HTTP)
Username/Password submitted by user
Access Request (User Credentials)
Redirects to Success Page
Access Accept
Client moved to RUN state

Flujo de autenticación web

Configurar

Diagrama de la red



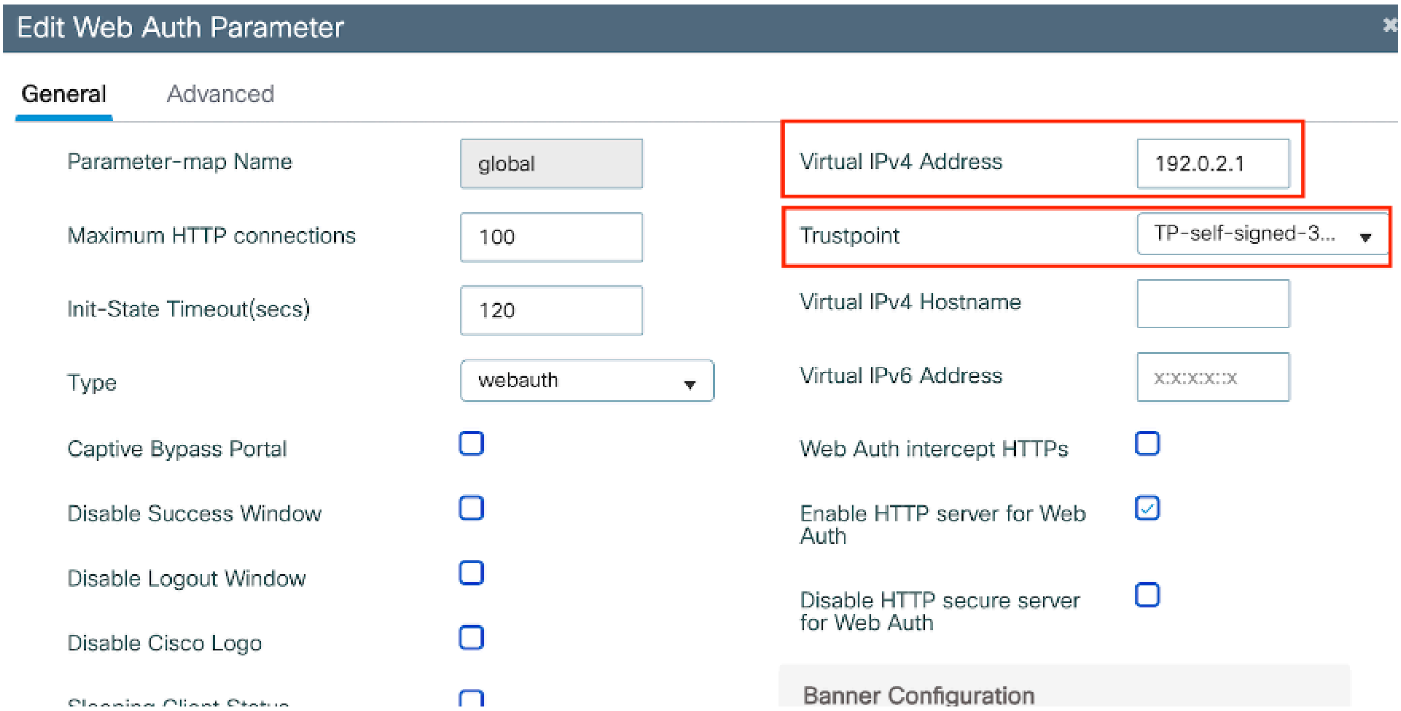
Topología de red

Configuraciones

Configurar parámetros web

Navegue hasta Configuration > Security > Web Auth y seleccione el mapa de parámetro Global

Verifique la configuración de IP virtual y Trustpoint desde el mapa de parámetro global. Todos los perfiles de parámetro de Web Auth personalizados heredan la configuración de IP virtual y Trustpoint del mapa de parámetro global.

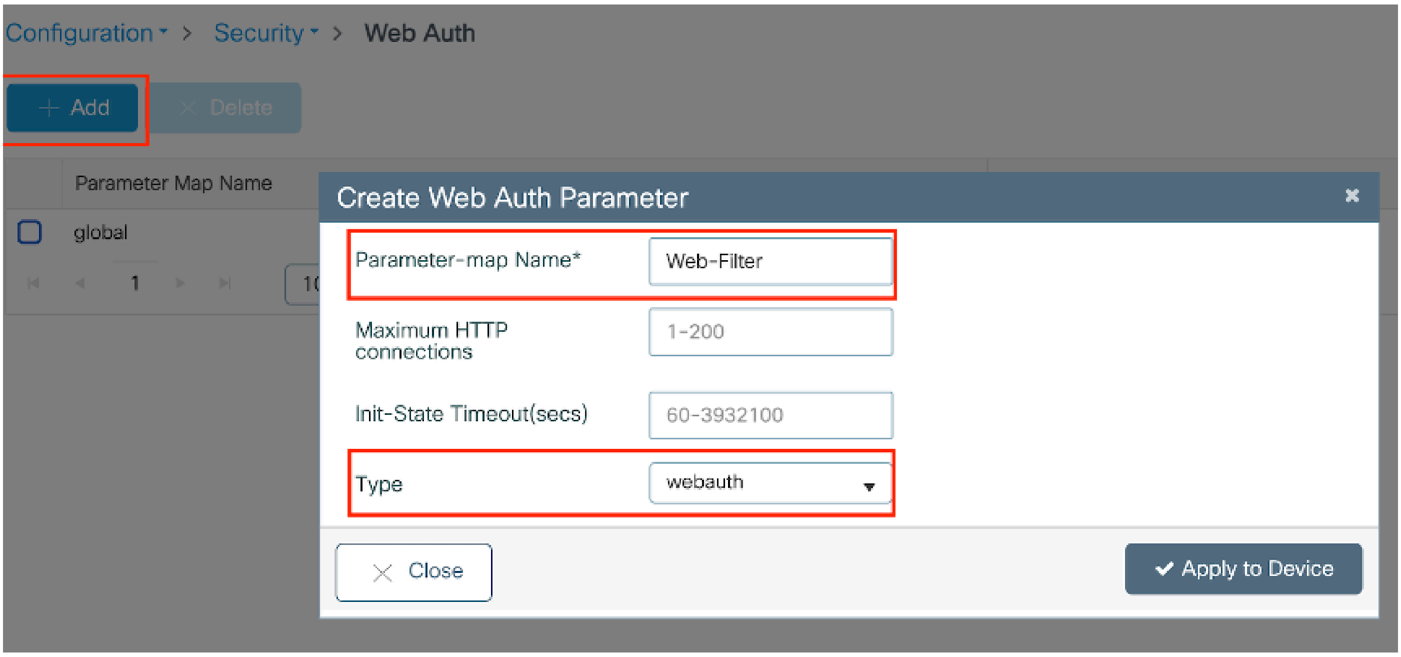


Edit Web Auth Parameter

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	X:X:X:X::X
Captive Bypass Portal	□	Web Auth intercept HTTPs	□
Disable Success Window	□	Enable HTTP server for Web Auth	☑
Disable Logout Window	□	Disable HTTP secure server for Web Auth	□
Disable Cisco Logo	□		

Perfil de parámetro de autenticación Web global

Paso 1: Seleccione "Agregar" para crear un mapa de parámetro de autenticación web personalizado. Ingrese el nombre del perfil y elija el tipo como "Webauth".



Create Web Auth Parameter

Parameter-map Name*	Web-Filter
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	webauth

Perfil de parámetro de autenticación web

Si los clientes también obtienen una dirección IPv6, también debe agregar una dirección IPv6 virtual en el mapa de parámetros. Utilice una dirección IP en el intervalo de documentación 2001:db8::/32

Si sus clientes obtuvieron una dirección IPv6, existe una buena posibilidad de que intenten obtener la redirección de autenticación web HTTP en V6 y no en V4, razón por la cual necesita que también se configure el IPv6 virtual.

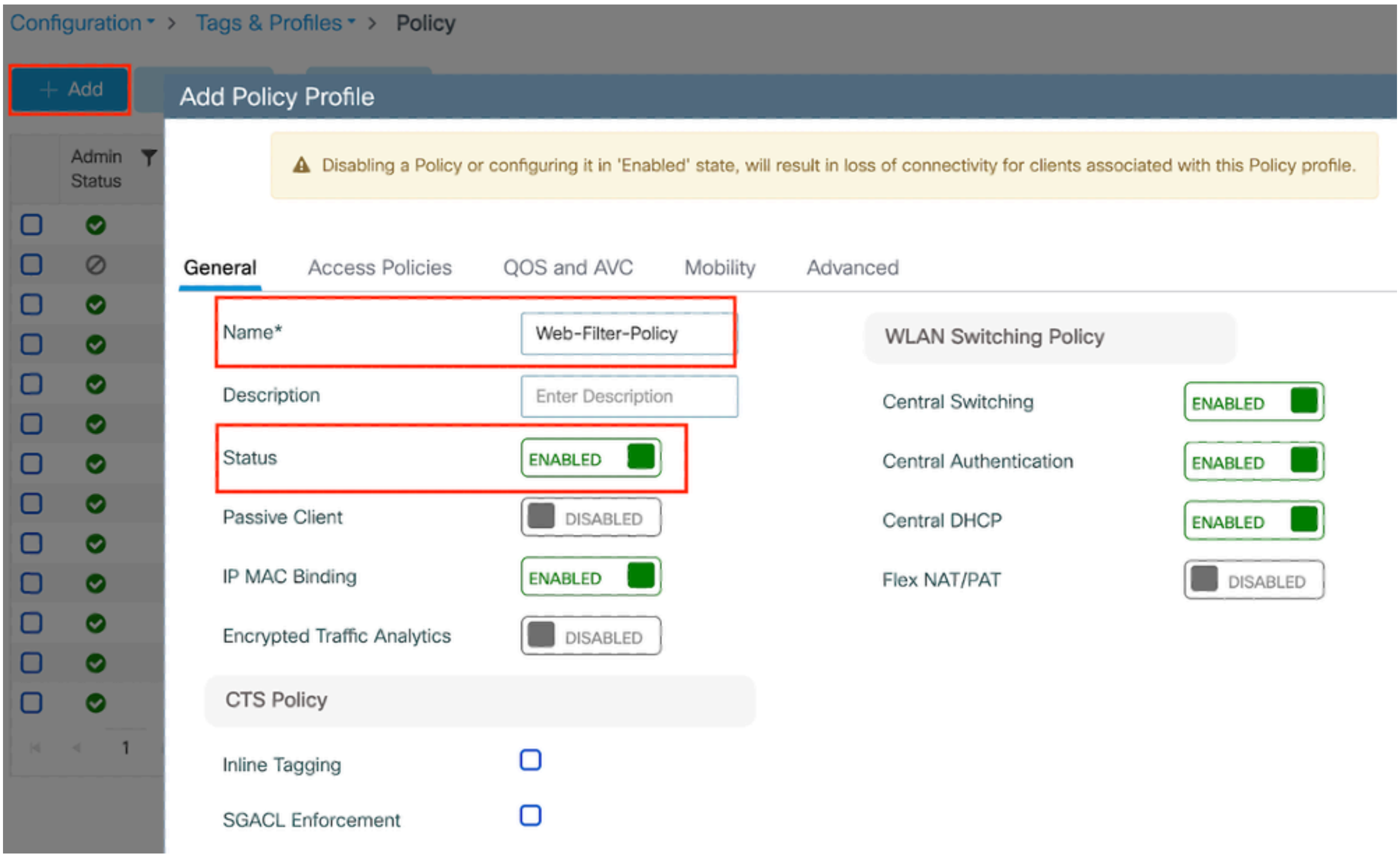
Configuración de CLI:

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

Configurar perfil de directiva

Paso 1: Crear un perfil de política

Vaya a Configuration > Tags & Profiles > Policy . Seleccione "Agregar". En la ficha General, especifique un nombre para el perfil y active la alternancia de estado.



Add Policy Profile

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

Name* Web-Filter-Policy

Description Enter Description

Status ENABLED

Passive Client DISABLED

IP MAC Binding ENABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging □

SGACL Enforcement □

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

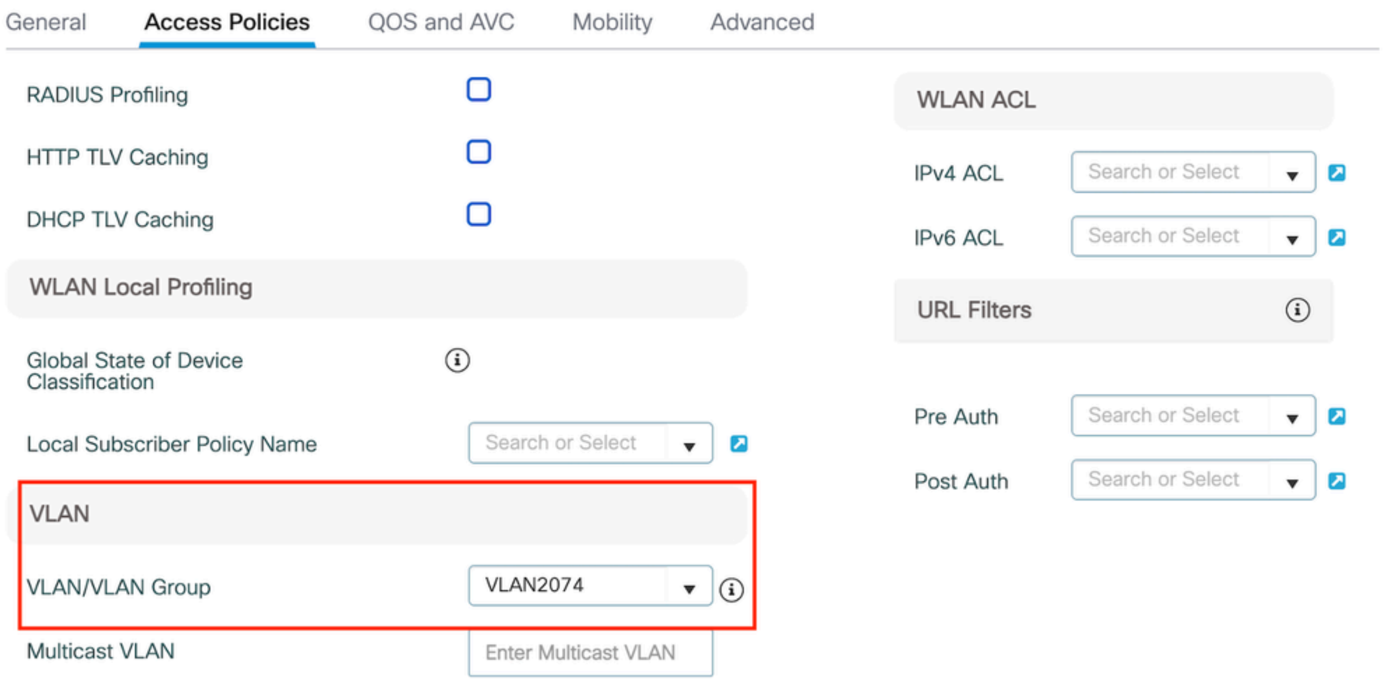
Central DHCP ENABLED

Flex NAT/PAT DISABLED

Perfil de política

Paso 2:

En la pestaña Políticas de acceso, elija la VLAN del cliente en la lista desplegable de la sección VLAN.



RADIUS Profiling □

HTTP TLV Caching □

DHCP TLV Caching □

WLAN Local Profiling

Global State of Device Classification

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: VLAN2074

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

URL Filters

Pre Auth: Search or Select

Post Auth: Search or Select

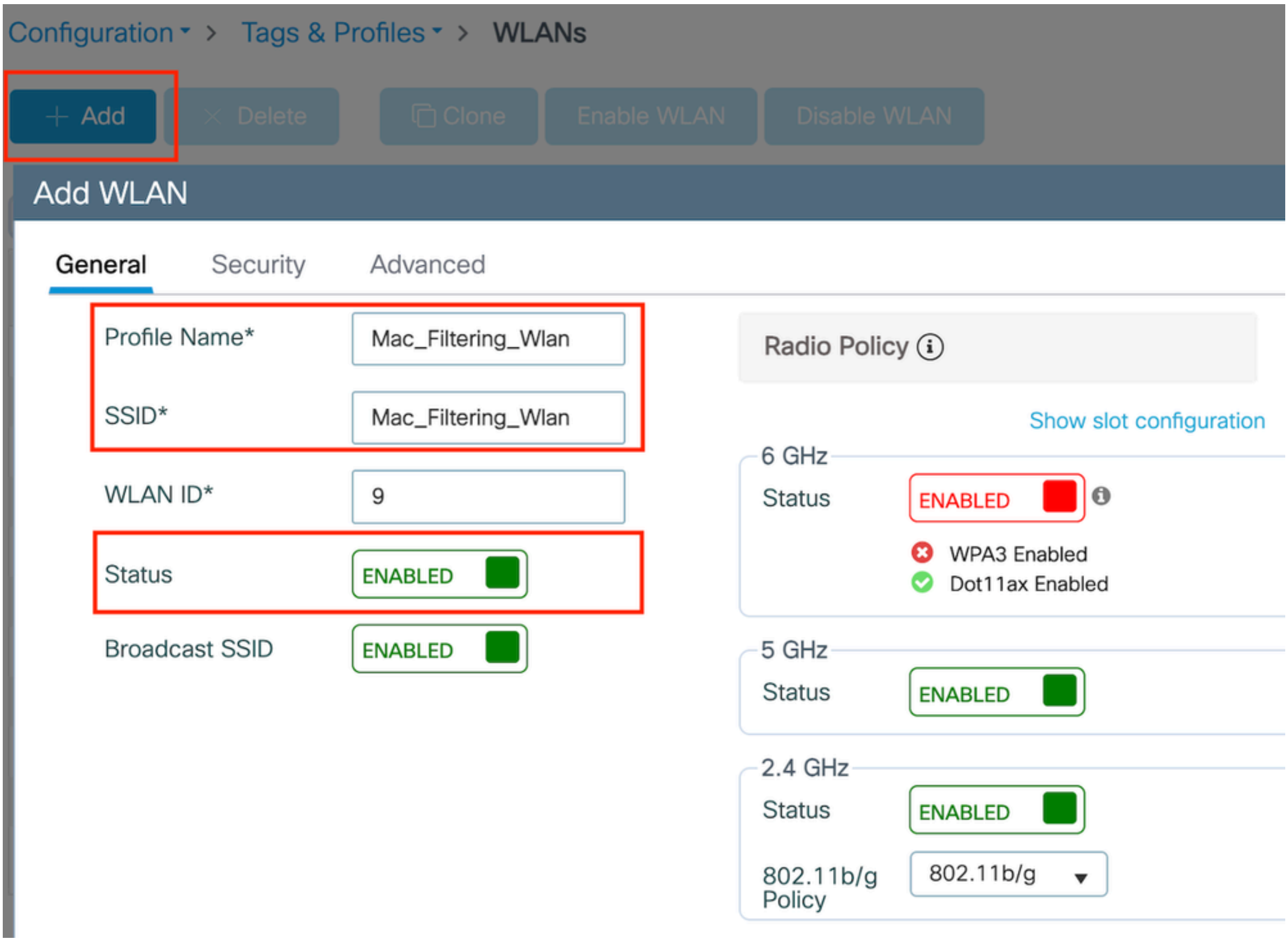
Ficha Política de acceso

Configuración de CLI:

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

Configuración del perfil WLAN

Paso 1: Vaya a Configuración > Etiquetas y perfiles > WLAN. Seleccione "Agregar" para crear un nuevo perfil. Defina un nombre de perfil y un nombre SSID, y habilite el campo de estado.



Profile Name* Mac_Filtering_Wlan

SSID* Mac_Filtering_Wlan

WLAN ID* 9

Status ENABLED

Broadcast SSID ENABLED

Radio Policy

Show slot configuration

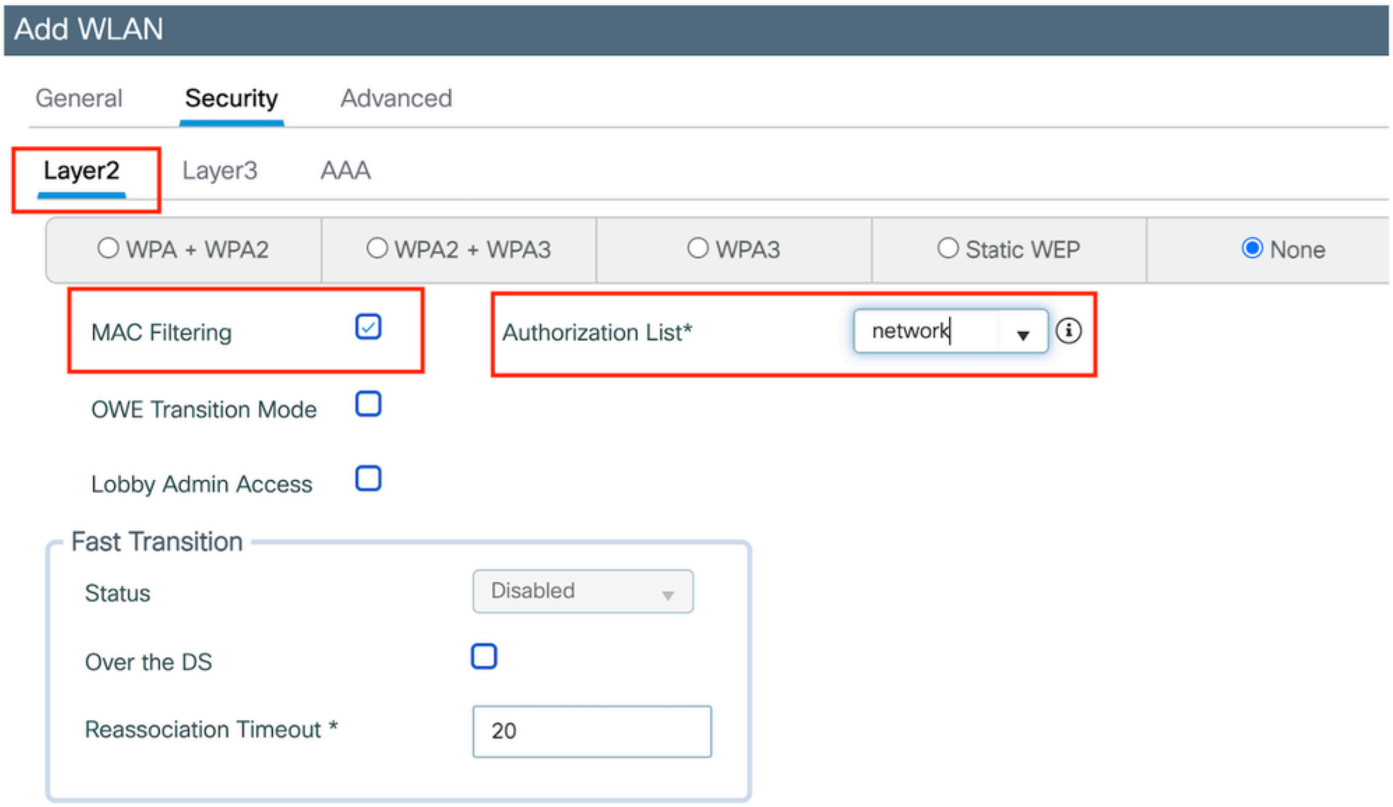
6 GHz
Status ENABLED
WPA3 Enabled
Dot11ax Enabled

5 GHz
Status ENABLED

2.4 GHz
Status ENABLED
802.11b/g Policy 802.11b/g

Perfil WLAN

Paso 2: en la ficha Security (Seguridad), active la casilla de verificación "Mac Filtering" (Filtrado de Mac) y configure el servidor RADIUS en la lista de autorización (ISE o servidor local). Esta configuración utiliza ISE tanto para la autenticación Mac como para la autenticación Web.



Add WLAN

General | **Security** | Advanced

Layer2 | Layer3 | AAA

○ WPA + WPA2 ○ WPA2 + WPA3 ○ WPA3 ○ Static WEP ● None

MAC Filtering ☑

Authorization List* network

OWE Transition Mode □

Lobby Admin Access □

Fast Transition

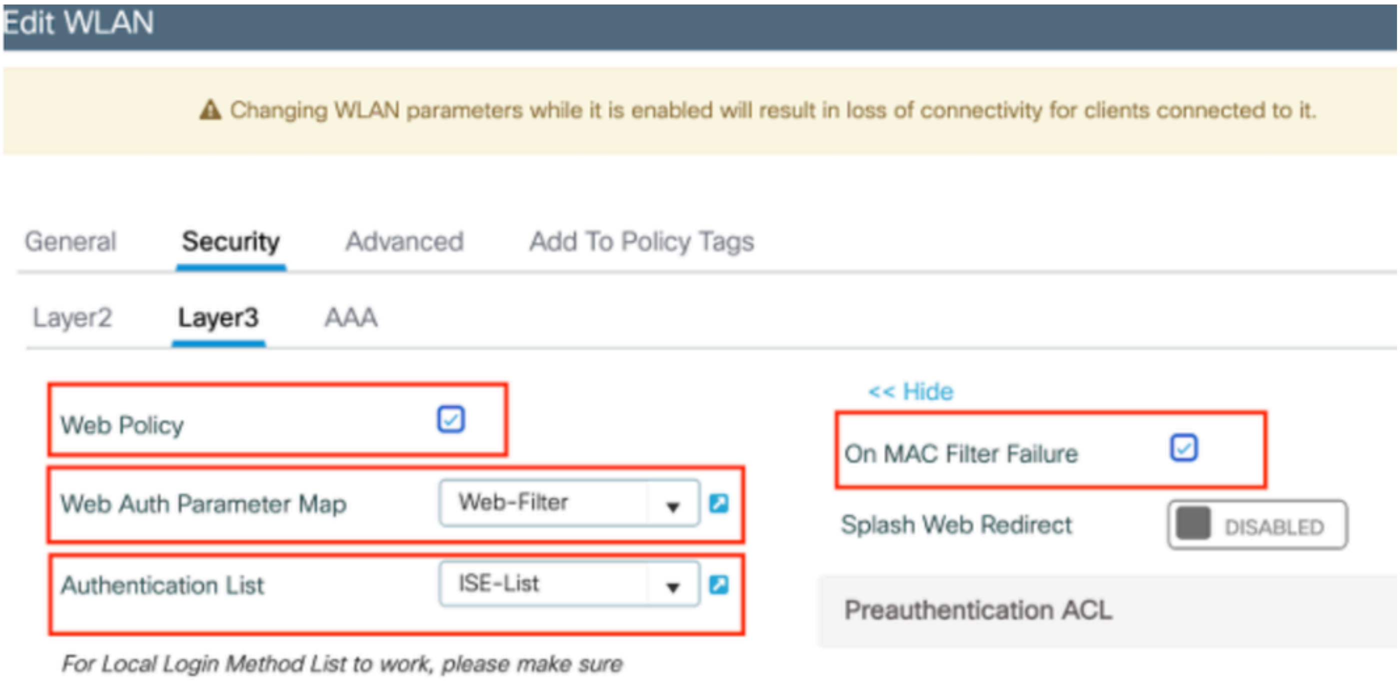
Status Disabled

Over the DS □

Reassociation Timeout * 20

Seguridad de capa 2 de WLAN

Paso 3: Vaya a Seguridad > Capa 3. Habilite la política web y asóciela con el perfil de mapa de parámetro de autenticación web. Marque la casilla de verificación "On Mac Filter Failure" y elija el servidor RADIUS en la lista desplegable Authentication (Autenticación).



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General | **Security** | Advanced | Add To Policy Tags

Layer2 | **Layer3** | AAA

Web Policy ☑

Web Auth Parameter Map Web-Filter

Authentication List ISE-List

For Local Login Method List to work, please make sure

<< Hide

On MAC Filter Failure ☑

Splash Web Redirect DISABLED

Preauthentication ACL

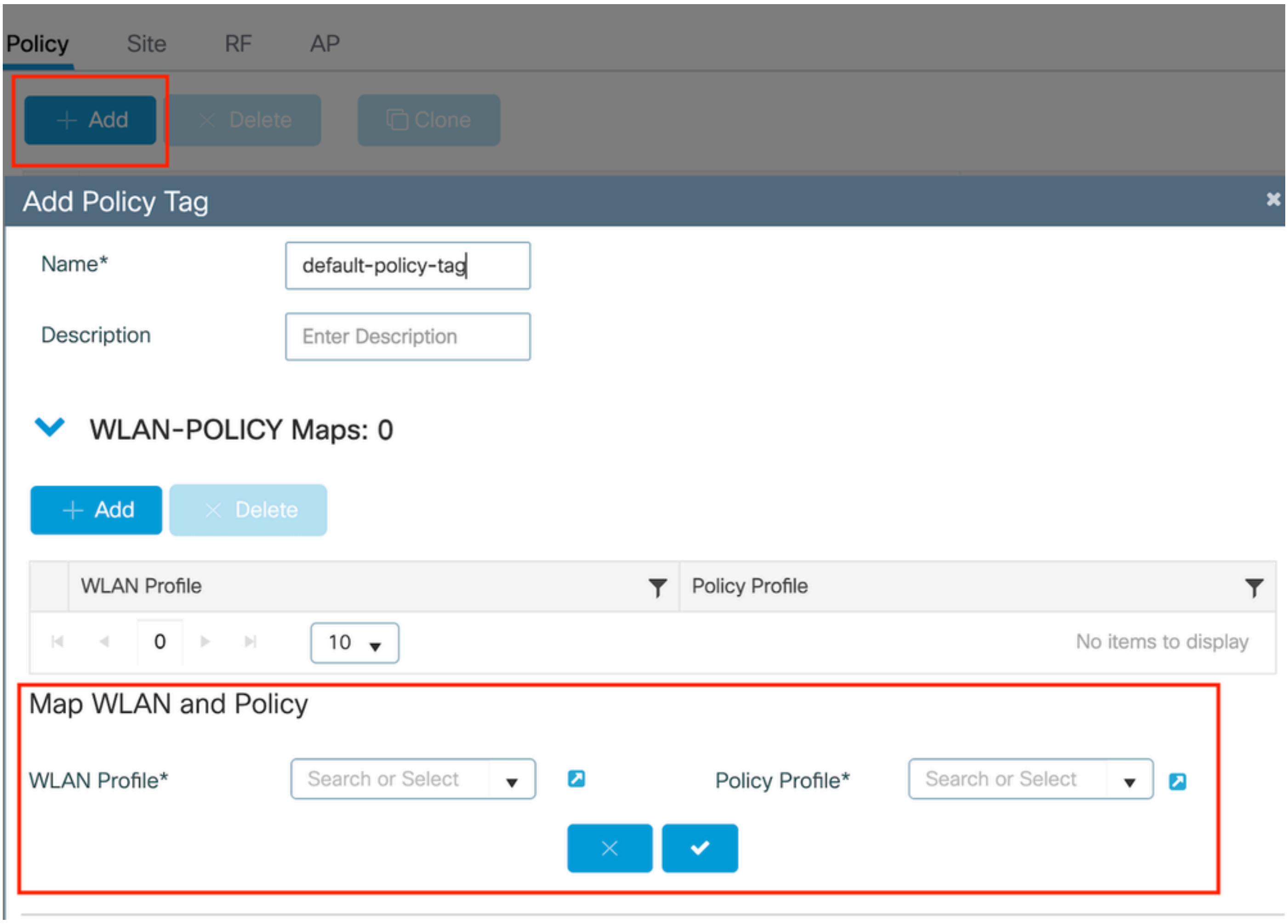
Ficha Seguridad de capa 3 de WLAN

Configuración de 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
```

Paso 4: Configuración de etiquetas de política, creación de perfil WLAN y asignación de perfil de política

Vaya a Configuration > Tags & Profiles > Tags > Policy. Haga clic en "Agregar" para definir un nombre para la etiqueta de directiva. En WLAN-Policy Maps, seleccione "Add" (Agregar) para asignar el perfil de política y WLAN creado anteriormente.



Add Policy Tag

Name* default-policy-tag

Description Enter Description

WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
0 · 10	No items to display

Map WLAN and Policy

WLAN Profile* Search or Select

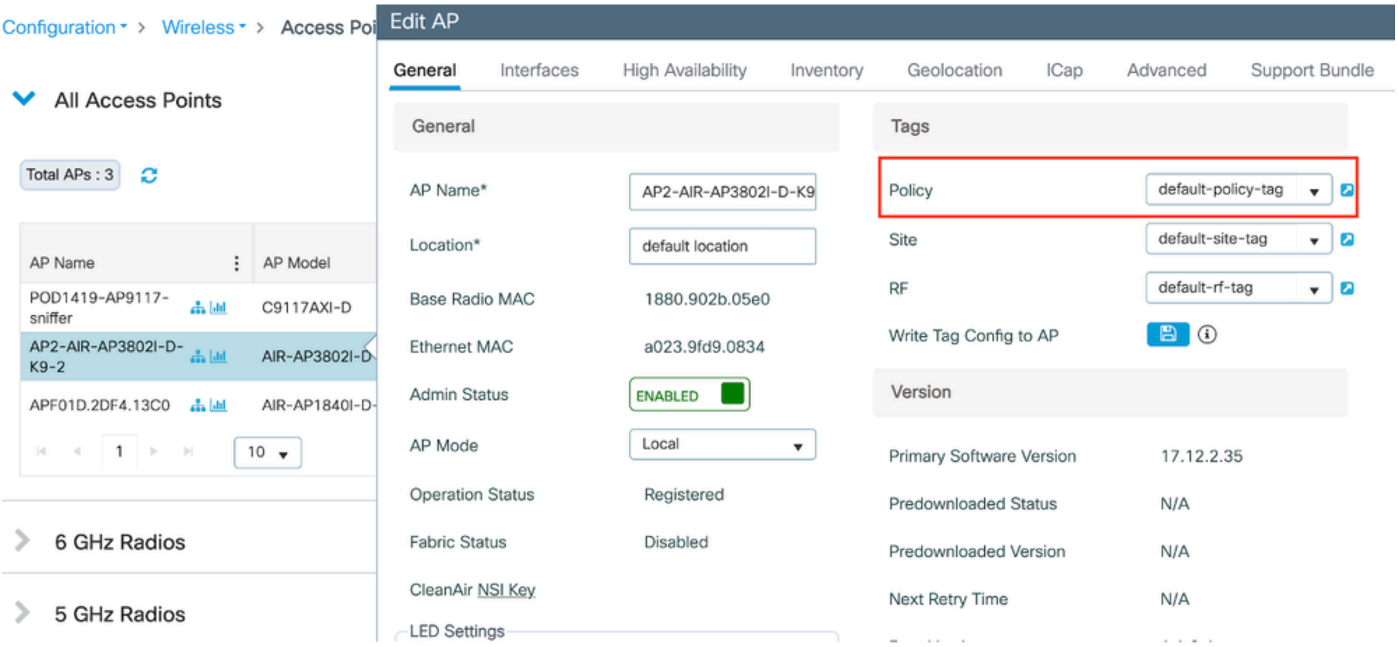
Policy Profile* Search or Select

Policy TAG map

Configuración de CLI:

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

Paso 5: Vaya a Configuración > Inalámbrico > Punto de acceso. Seleccione el punto de acceso responsable de difundir este SSID. En el menú Editar punto de acceso, asigne la etiqueta de directiva creada.



Configuration > Wireless > Access Poi

All Access Points

Total APs : 3

AP Name	AP Model
POD1419-AP9117-sniffer	C9117AXI-D
AP2-AIR-AP3802I-D-K9-2	AIR-AP3802I-D
APF01D.2DF4.13C0	AIR-AP1840I-D-

6 GHz Radios

5 GHz Radios

Edit AP

General | Interfaces | High Availability | Inventory | Geolocation | ICap | Advanced | Support Bundle

General

AP Name*	AP2-AIR-AP3802I-D-K9
Location*	default location
Base Radio MAC	1880.902b.05e0
Ethernet MAC	a023.9fd9.0834
Admin Status	ENABLED
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled
CleanAir NSI Key	

LED Settings

Tags

Policy	default-policy-tag
Site	default-site-tag
RF	default-rf-tag
Write Tag Config to AP	

Version

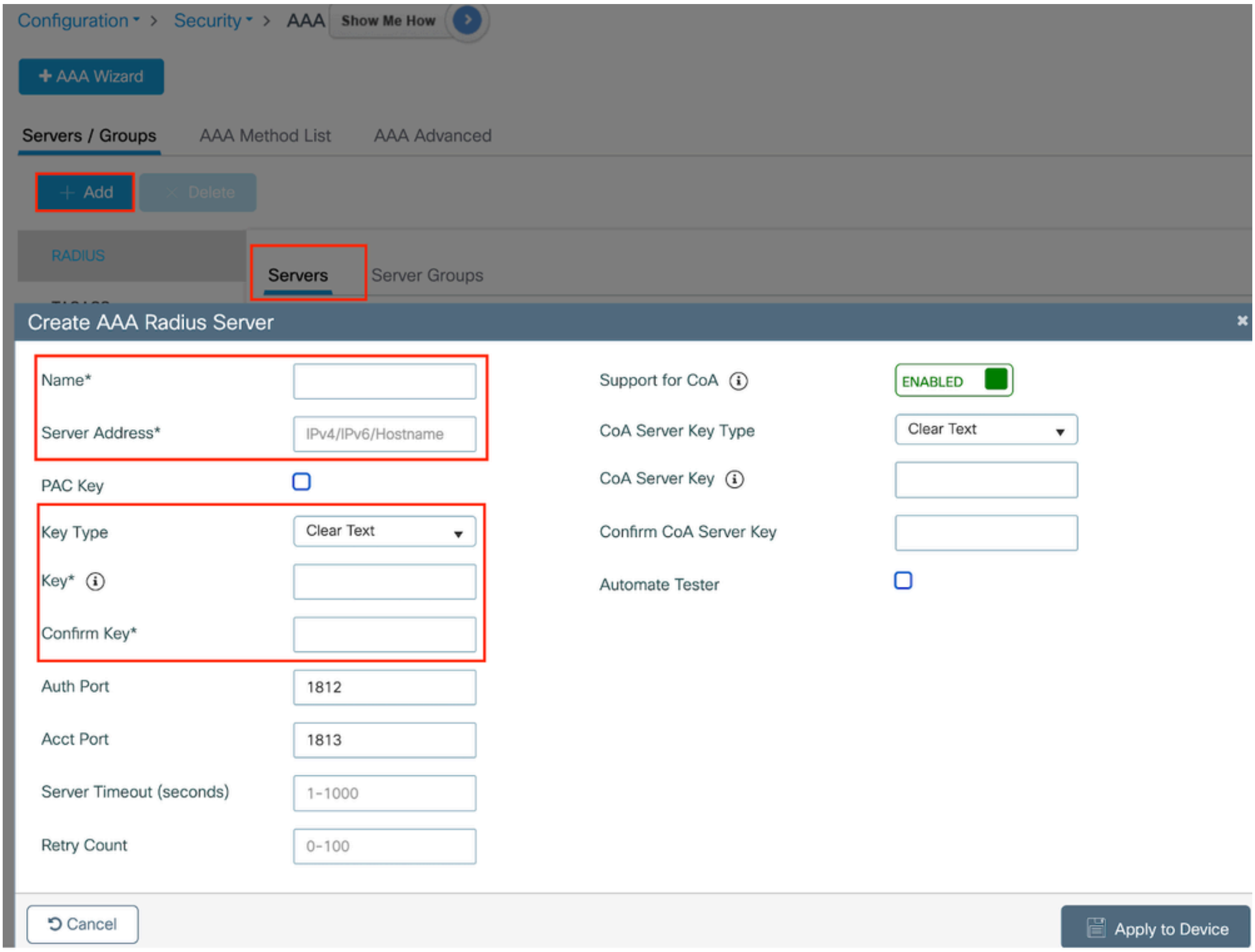
Primary Software Version	17.12.2.35
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A

Asignación de TAG de política a AP

Configuración de AAA:

Paso 1: Crear un servidor Radius:

Vaya a Configuration > Security > AAA. Haga clic en la opción "Agregar" en la sección Servidor/Grupo. En la página "Create AAA Radius Server" (Crear servidor RADIUS AAA), introduzca el nombre del servidor, la dirección IP y el secreto compartido.



Create AAA Radius Server

Name*	
Server Address*	IPv4/IPv6/Hostname
PAC Key	□
Key Type	Clear Text
Key*	
Confirm Key*	
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED
CoA Server Key Type	Clear Text
CoA Server Key	
Confirm CoA Server Key	
Automate Tester	□

Configuración del servidor

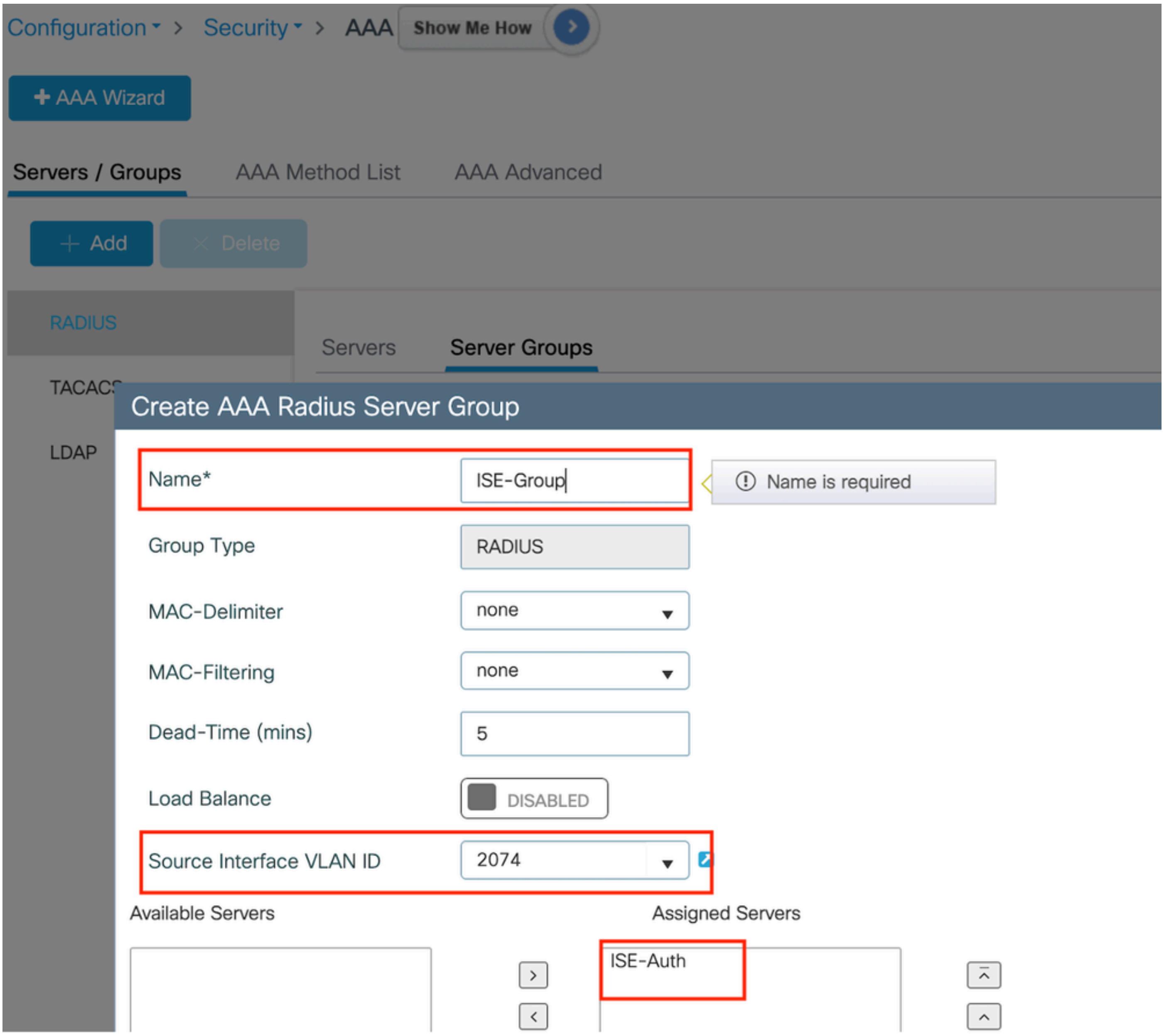
Configuración de CLI

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

Paso 2: Crear un grupo de servidores Radius:

Seleccione la opción "Agregar" en la sección Grupos de servidores para definir un grupo de servidores. Alternar los servidores que se incluirán en la misma configuración de grupo.

No es necesario establecer la interfaz de origen. De forma predeterminada, el 9800 utiliza su tabla de ruteo para averiguar la interfaz que se debe utilizar para alcanzar el servidor RADIUS y normalmente utiliza la gateway predeterminada.



Create AAA Radius Server Group

Name* ISE-Group

Name is required

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 5

Load Balance DISABLED

Source Interface VLAN ID 2074

ISE-Auth

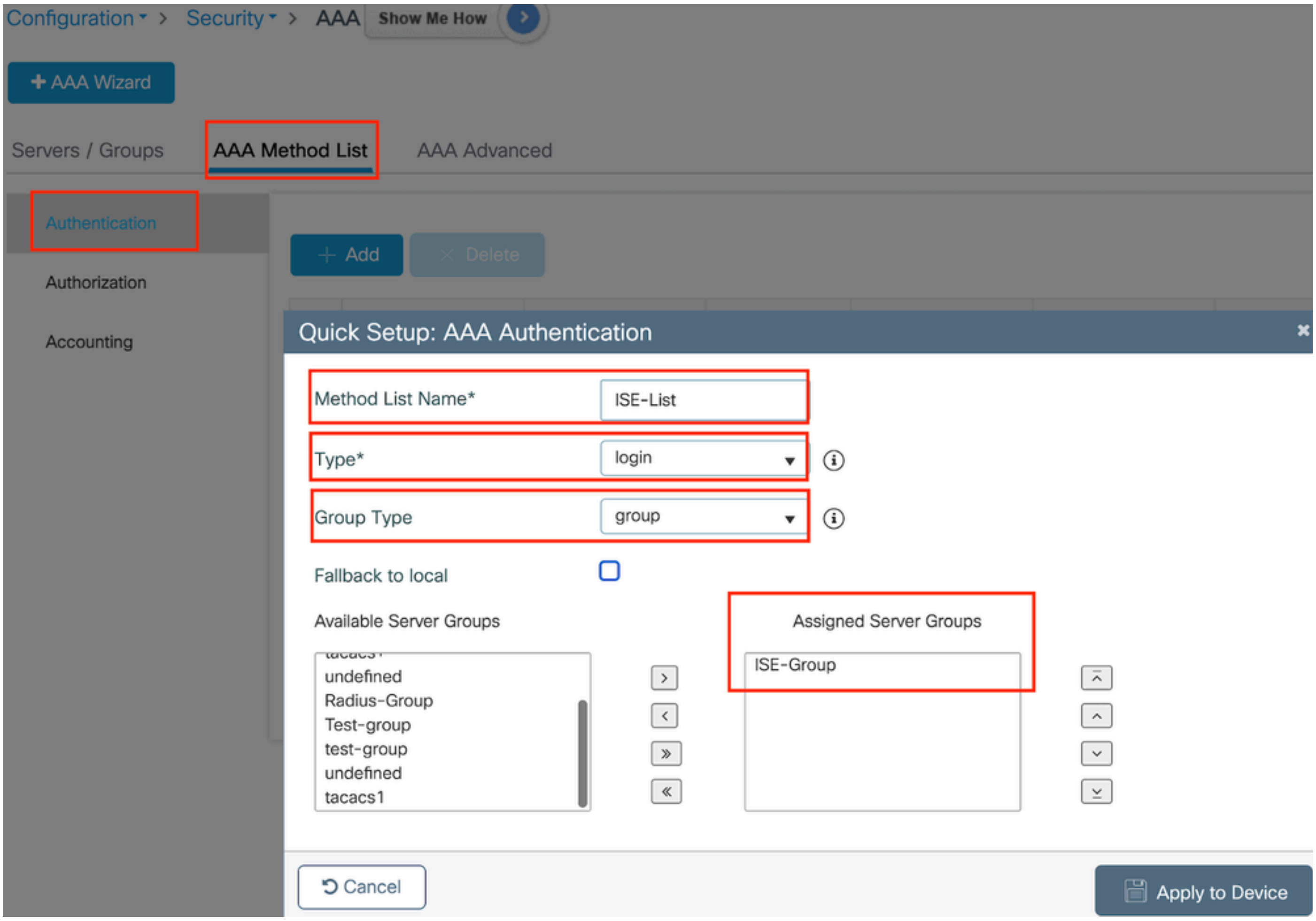
Grupo de servidores

Configuración de CLI

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

Paso 3: Configuración de la Lista de Métodos AAA:

Vaya a la pestaña Lista de métodos AAA. En Autenticación, haga clic en Agregar. Defina un nombre de lista de métodos con Tipo como "login" y Tipo de grupo como "Group". Asigne el grupo de servidores de autenticación configurado en la sección Grupo de servidores asignado.



Method List Name*: ISE-List

Type*: login

Group Type: group

Fallback to local: □

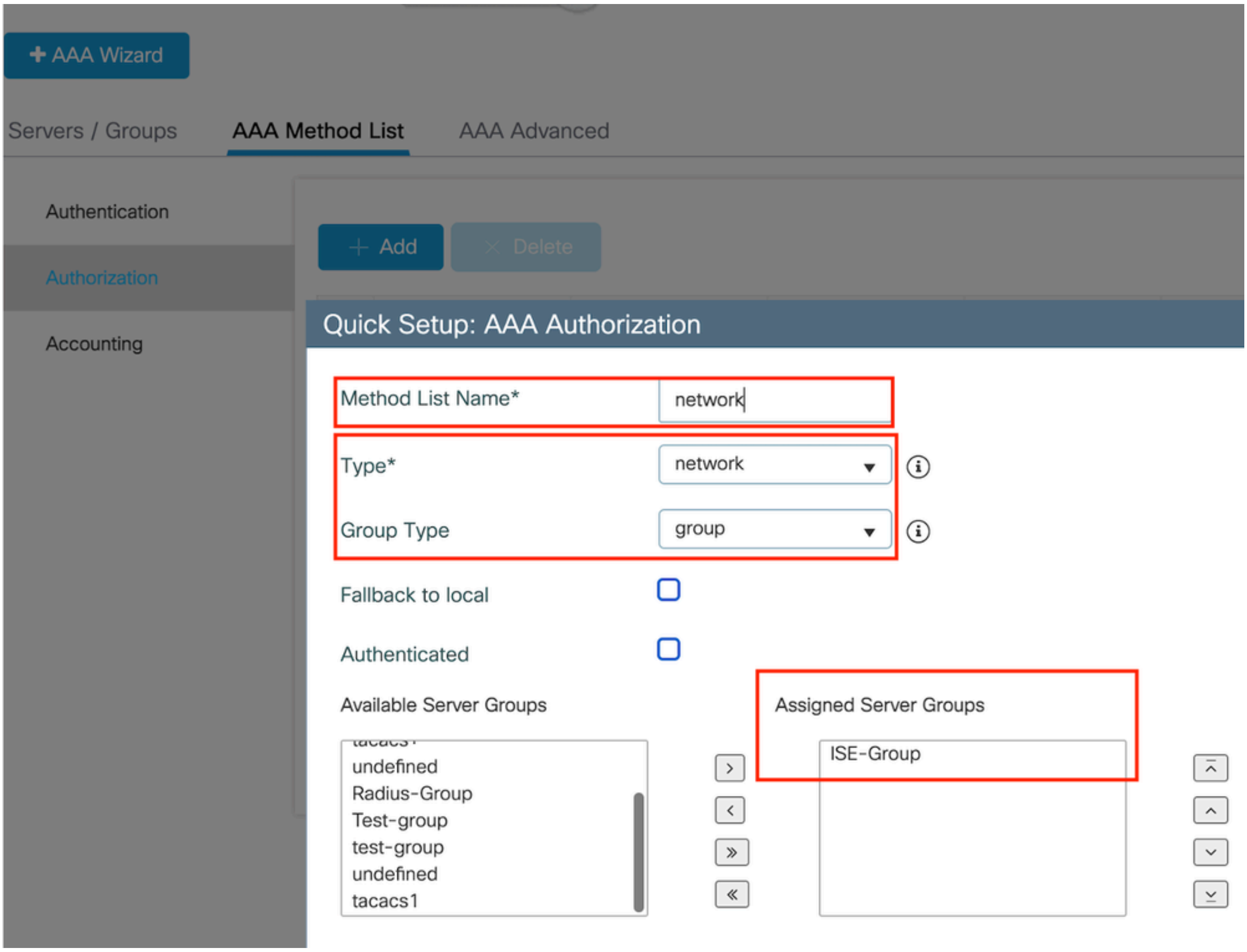
Assigned Server Groups: ISE-Group

Lista de métodos de autenticación

Configuración de CLI

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

Vaya a la sección Lista de métodos de autorización y haga clic en "Agregar". Defina un nombre de lista de métodos y establezca el tipo en "red" con Tipo de grupo como "Grupo". Cambie el servidor RADIUS configurado a la sección Grupos de Servidores Asignados.



Quick Setup: AAA Authorization

Method List Name* network

Type* network

Group Type group

Fallback to local □

Authenticated □

Available Server Groups: tacacs+, undefined, Radius-Group, Test-group, test-group, undefined, tacacs1

Assigned Server Groups: ISE-Group

Lista de métodos de autorización

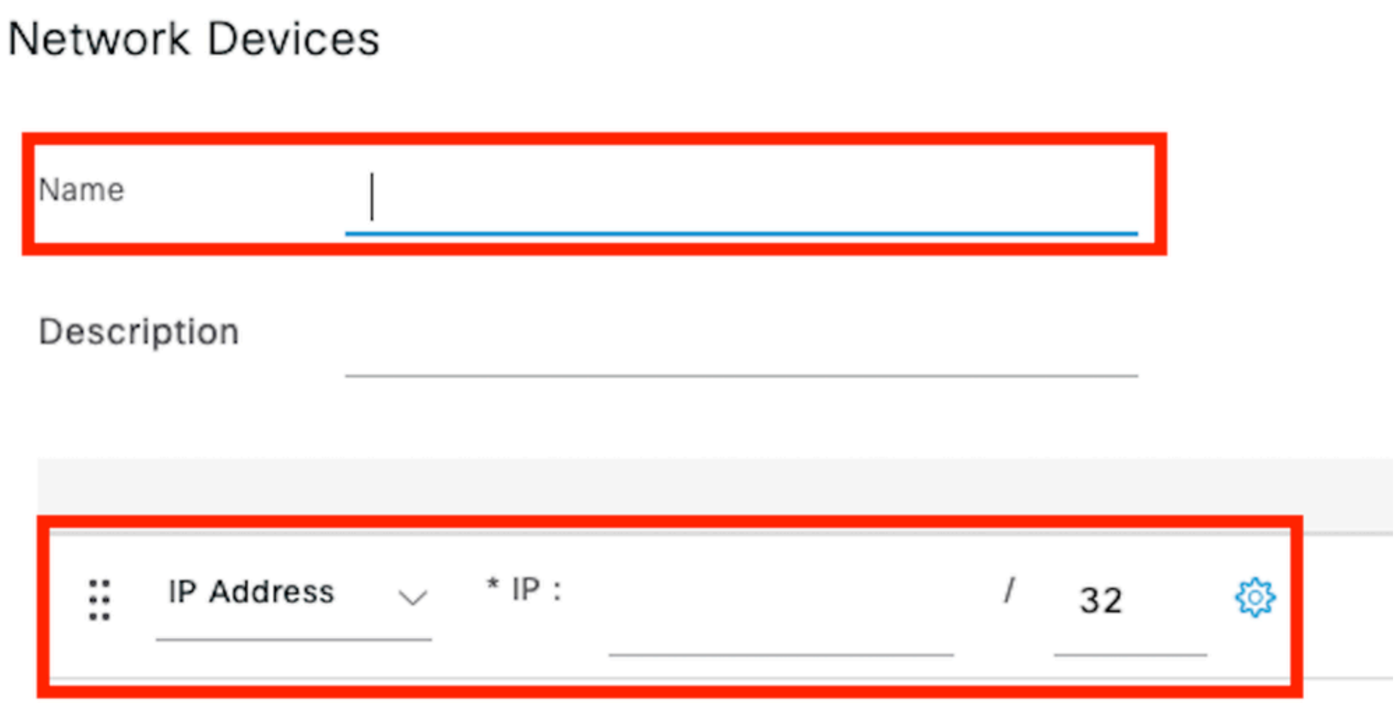
Configuración de CLI

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

Configuración de ISE:

Agregar WLC como dispositivo de red en ISE

Paso 1: Vaya a Administración > Dispositivos de red y haga clic en Agregar. Introduzca la dirección IP del controlador, el nombre de host y el secreto compartido en Configuración de autenticación de RADIUS



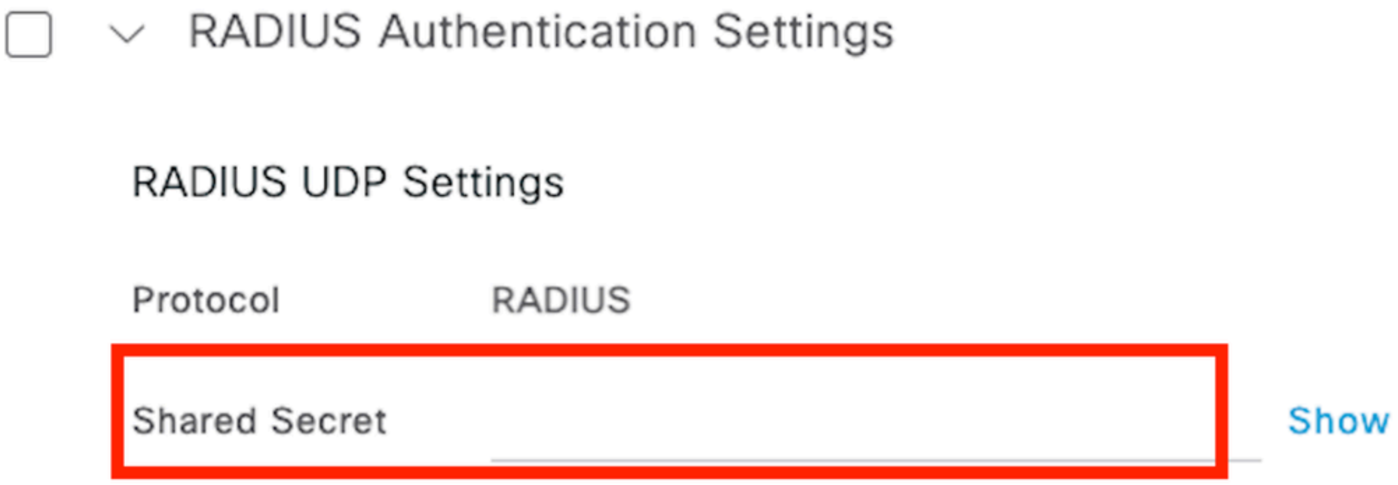
Network Devices

Name

Description

IP Address * IP : / 32

Agregar dispositivo de red



□ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

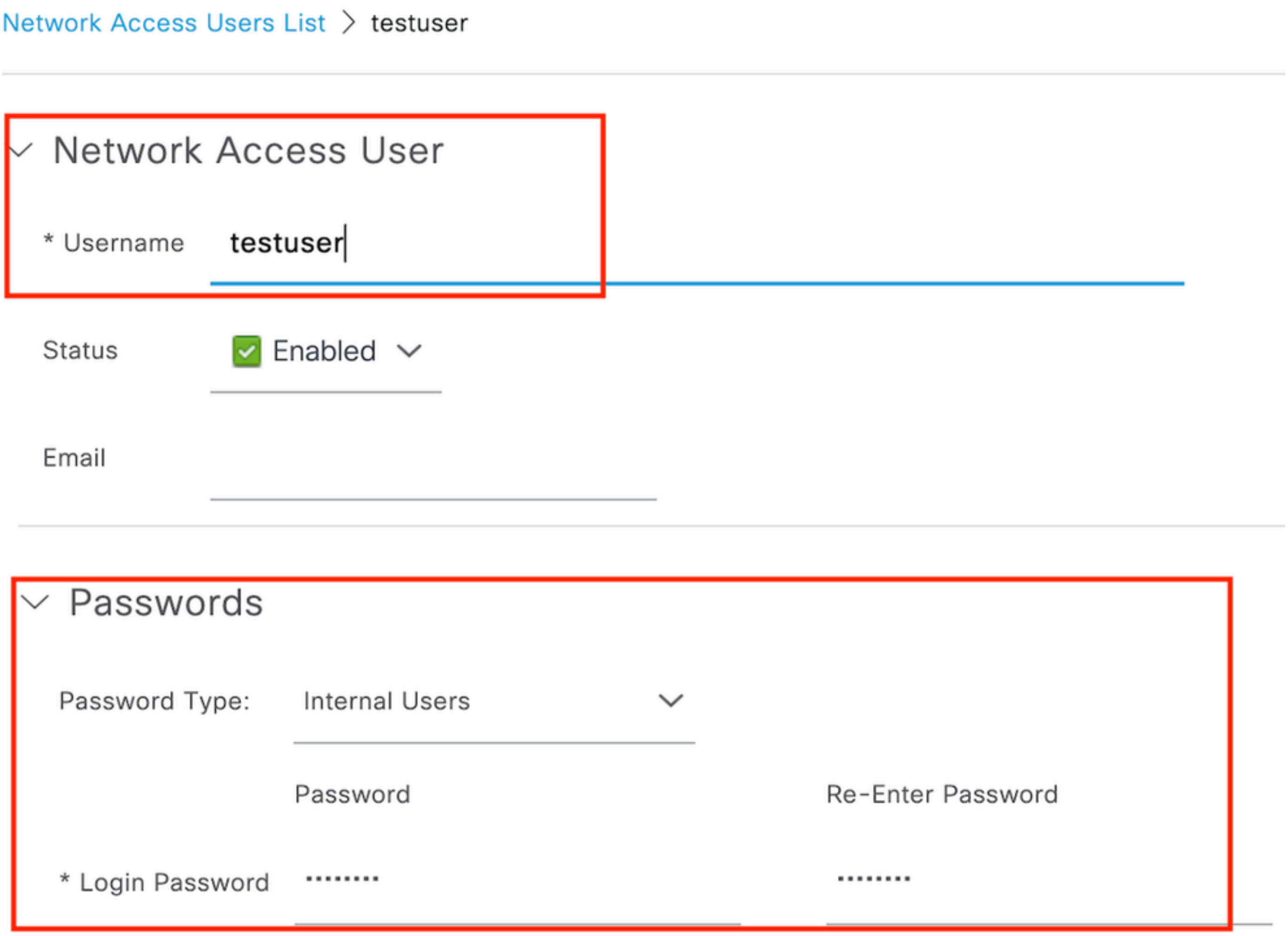
Shared Secret

secreto compartido

Paso 2: Crear entrada de usuario

En Identity Management > Identities (Administración de identidades > Identidades), seleccione la opción Add (Agregar).

Configure el nombre de usuario y la contraseña que el cliente debe utilizar para la autenticación Web



Network Access Users List > testuser

Network Access User

* Username testuser

Status ✓ Enabled

Email

Passwords

Password Type: Internal Users

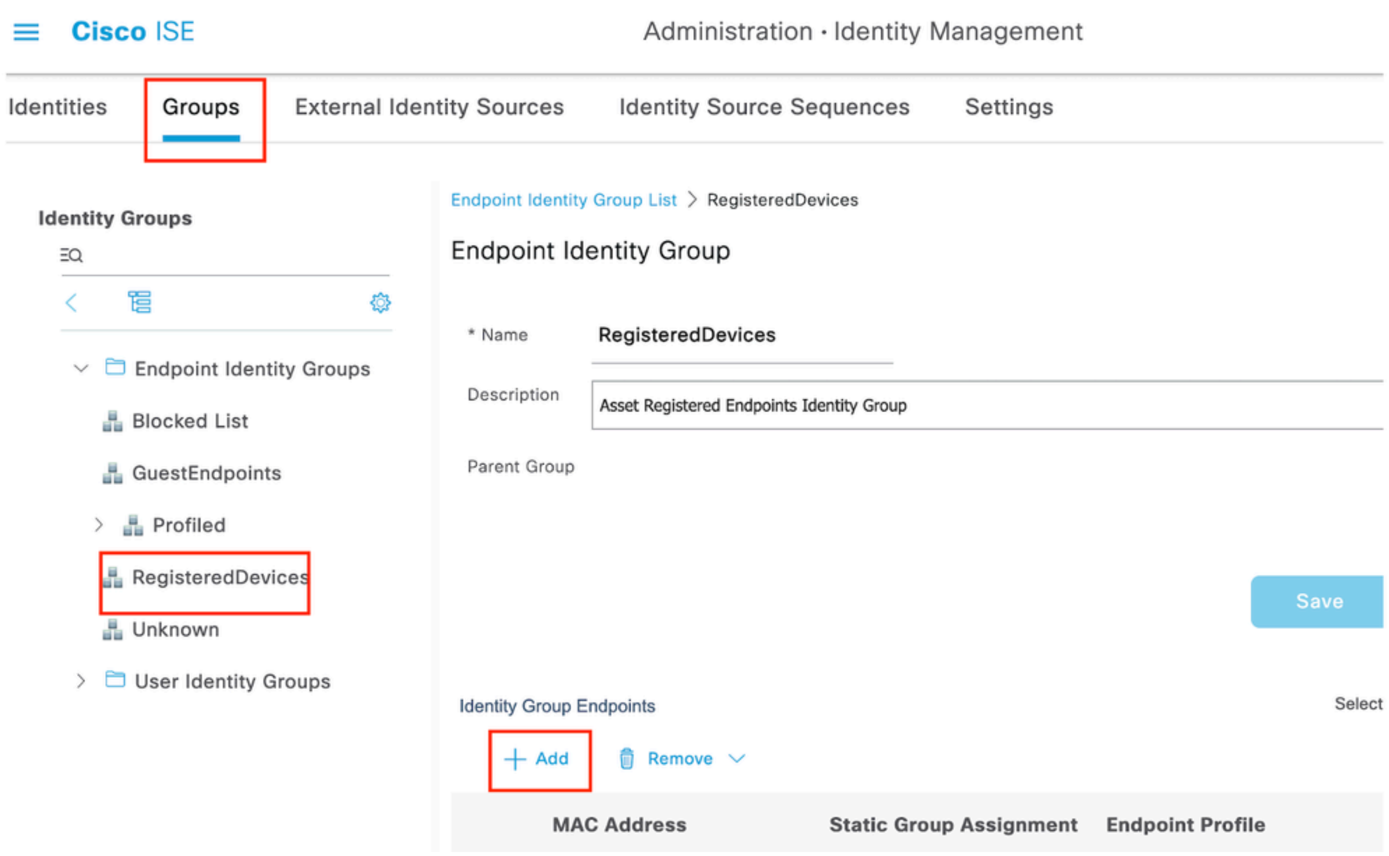
Password Re-Enter Password

* Login Password ········· ·········

Agregar credenciales de usuario

Paso 3: Vaya a Administration > Identity Management > Groups > Registered Devices y haga clic en Add.

Introduzca la dirección MAC del dispositivo para crear una entrada en el servidor.



Endpoint Identity Group

* Name: RegisteredDevices

Description: Asset Registered Endpoints Identity Group

Parent Group

Identity Group Endpoints

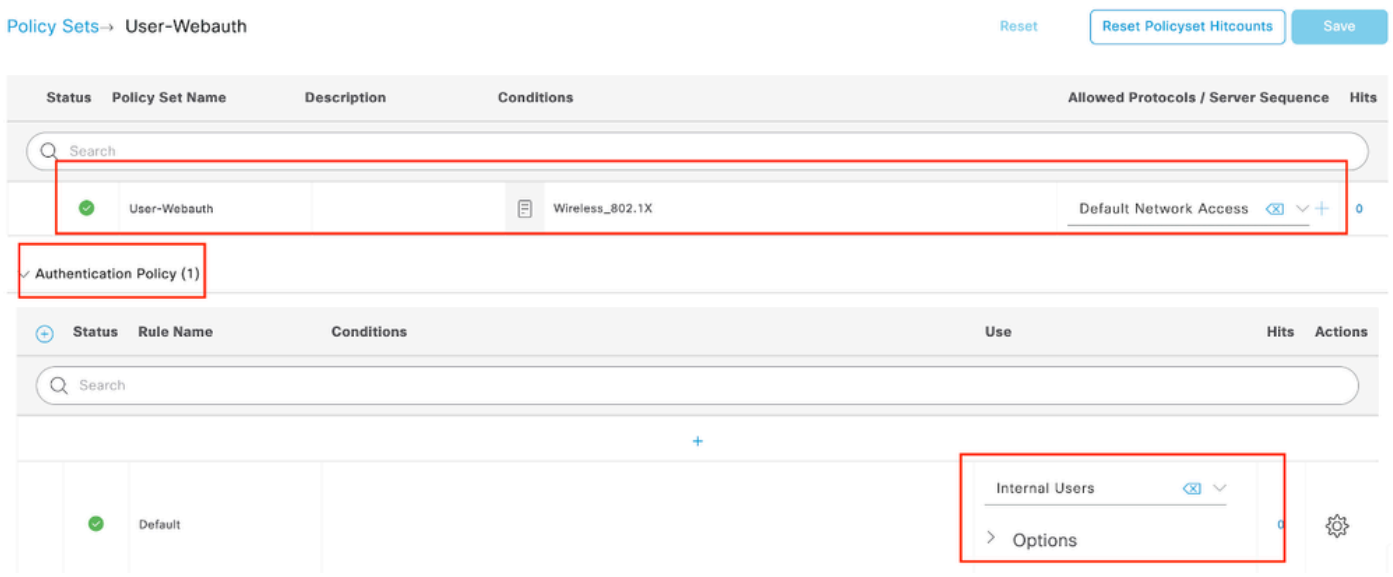
MAC Address	Static Group Assignment	Endpoint Profile

Agregar dirección MAC del dispositivo

Paso 4: Crear política de servicio

Vaya a Directiva > Conjuntos de directivas y seleccione el signo "+" para crear un nuevo conjunto de directivas

Este conjunto de políticas es para la autenticación Web de usuario, donde se crea un nombre de usuario y una contraseña para el cliente en Identity Management



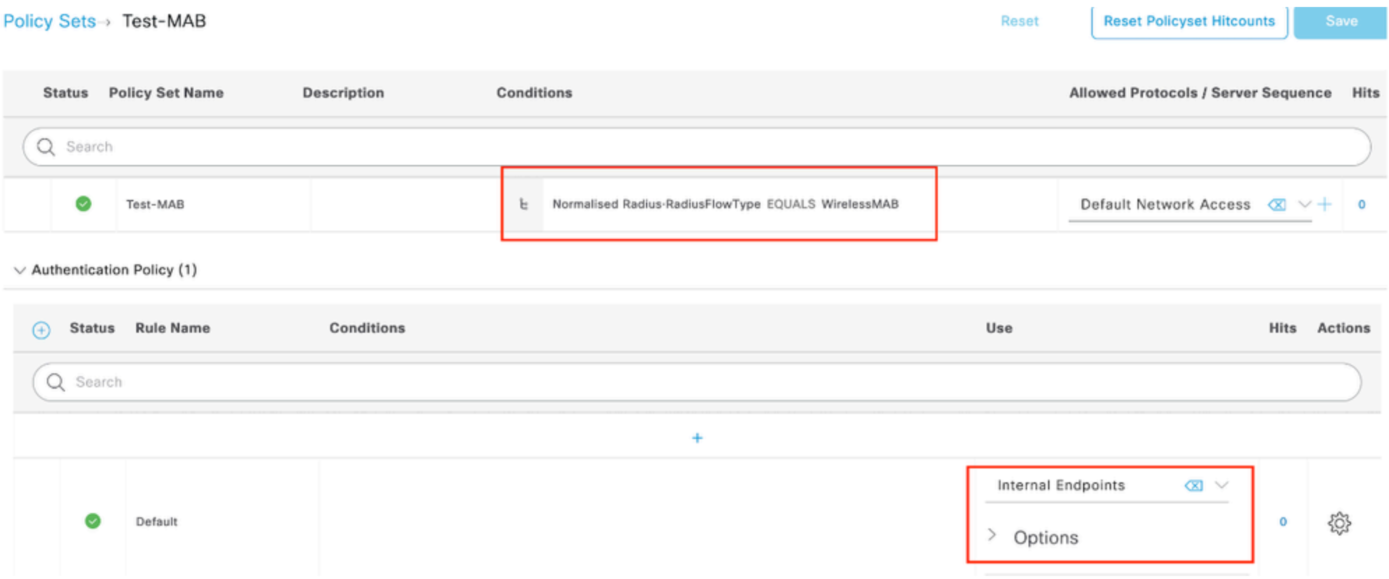
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	User-Webauth		Wireless_802.1X	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users	0	

Política del servicio de autenticación web

De manera similar, cree una política de servicio MAB y asigne los extremos internos en la política de autenticación.


Policy Sets → Test-MAB

Reset | Reset Policyset Hitcounts | Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Test-MAB		Normalised Radius·RadiusFlowType EQUALS WirelessMAB	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Endpoints Options	0	

Política del servicio de autenticación MAB

Verificación

Configuración del controlador

<#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

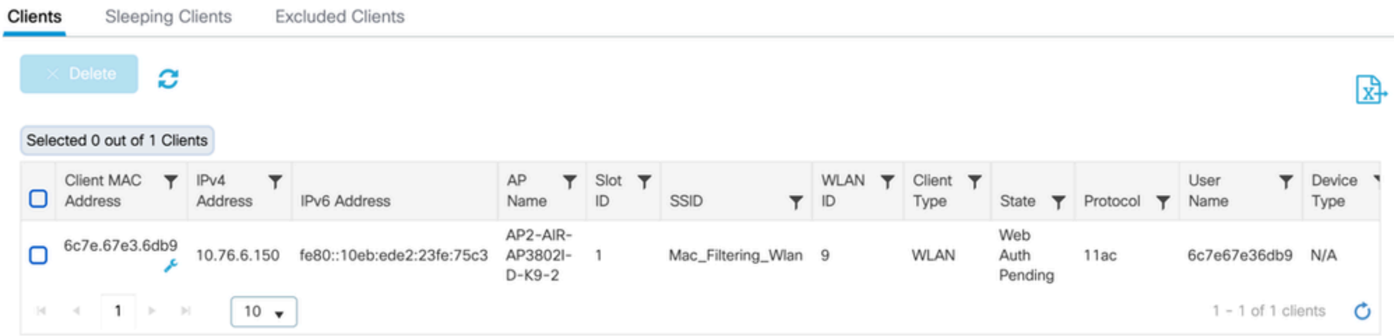
```
show ap name AP2-AIR-AP3802I-D-K9-2 tag detail
```

```
Policy tag mapping
```

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

Estado de la política del cliente en el controlador

Vaya a la sección Panel > Clientes para confirmar el estado de los clientes conectados. El cliente se encuentra actualmente en estado pendiente de autenticación Web



□	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type
□	6c7e.67e3.6db9	10.76.6.150	fe80::10eb:ede2:23fe:75c3	AP2-AIR-AP3802I-D-K9-2	1	Mac_Filtering_Wlan	9	WLAN	Web Auth Pending	11ac	6c7e67e36db9	N/A

Detalles del cliente

```
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
```

Después de la autenticación Web correcta, el estado del administrador de directivas de cliente pasa a RUN

<#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
```

Troubleshoot

La funcionalidad de la función Web Auth on MAC Failure se basa en la capacidad del controlador para activar la autenticación web en caso de fallo del MAB. Nuestro objetivo principal es recopilar los rastros de RA de manera eficiente desde el controlador para la resolución de problemas y el análisis.

Recopilación de trazas radiactivas

Active Radio Active Tracing para generar seguimientos de depuración de cliente para la dirección MAC especificada en la CLI.

Pasos para habilitar el seguimiento radiactivo:

Asegúrese de que todas las depuraciones condicionales estén inhabilitadas

```
clear platform condition all
```

Habilitar depuración para la dirección MAC especificada

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

Después de reproducir el problema, deshabilite la depuración para detener la recopilación de seguimiento de RA.

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

Una vez que se detiene el seguimiento de RA, el archivo de depuración se genera en la memoria de inicialización del controlador.

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

Copie el archivo en un servidor externo.

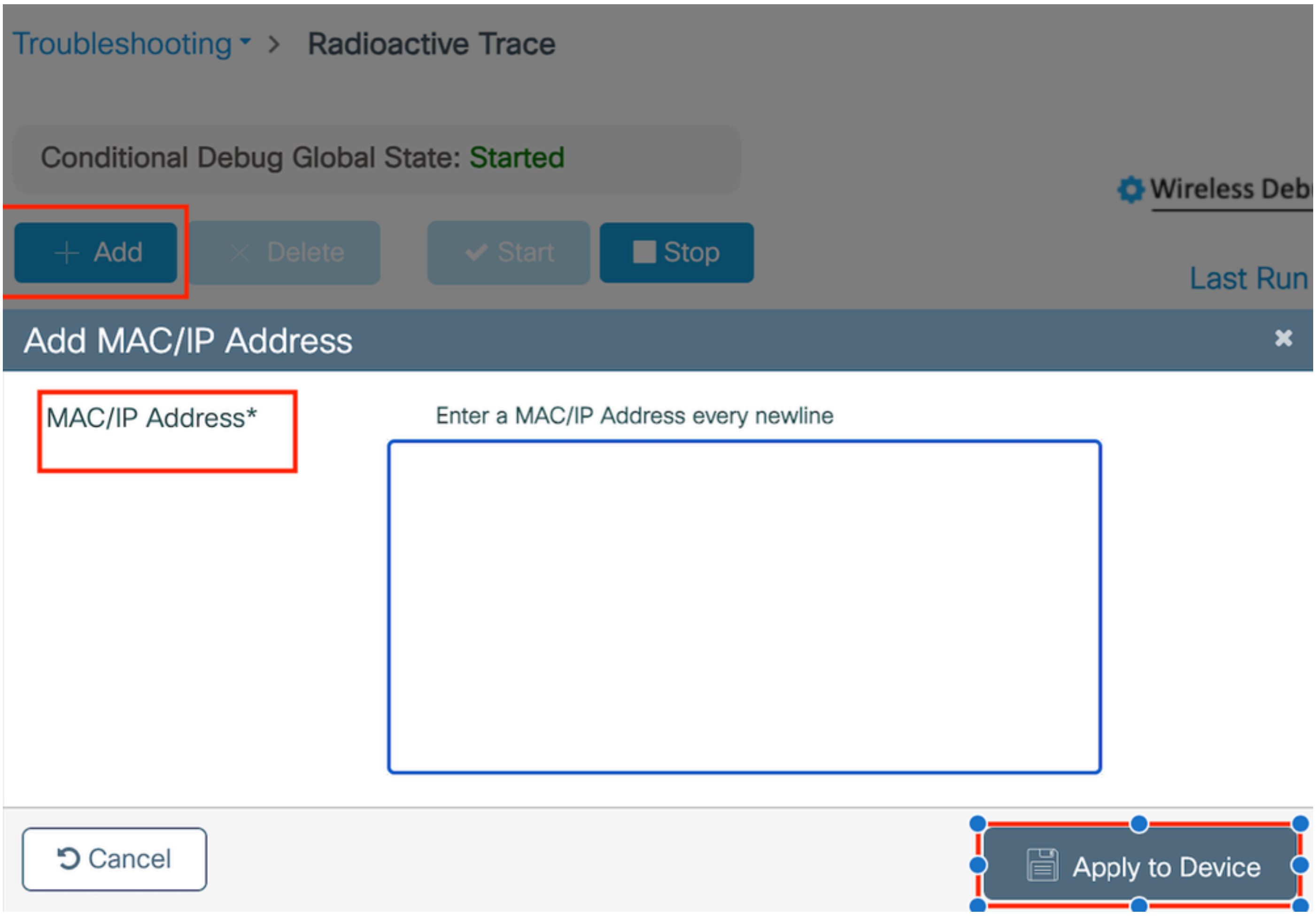
```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP addre
```

Mostrar el registro de depuración:

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

Activar el seguimiento de RA en la GUI,

Paso 1: Vaya a Troubleshooting > Radioactive Trace. Seleccione la opción para agregar una nueva entrada y, a continuación, introduzca la dirección MAC del cliente en la ficha Add MAC/IP Address (Agregar dirección MAC/IP).

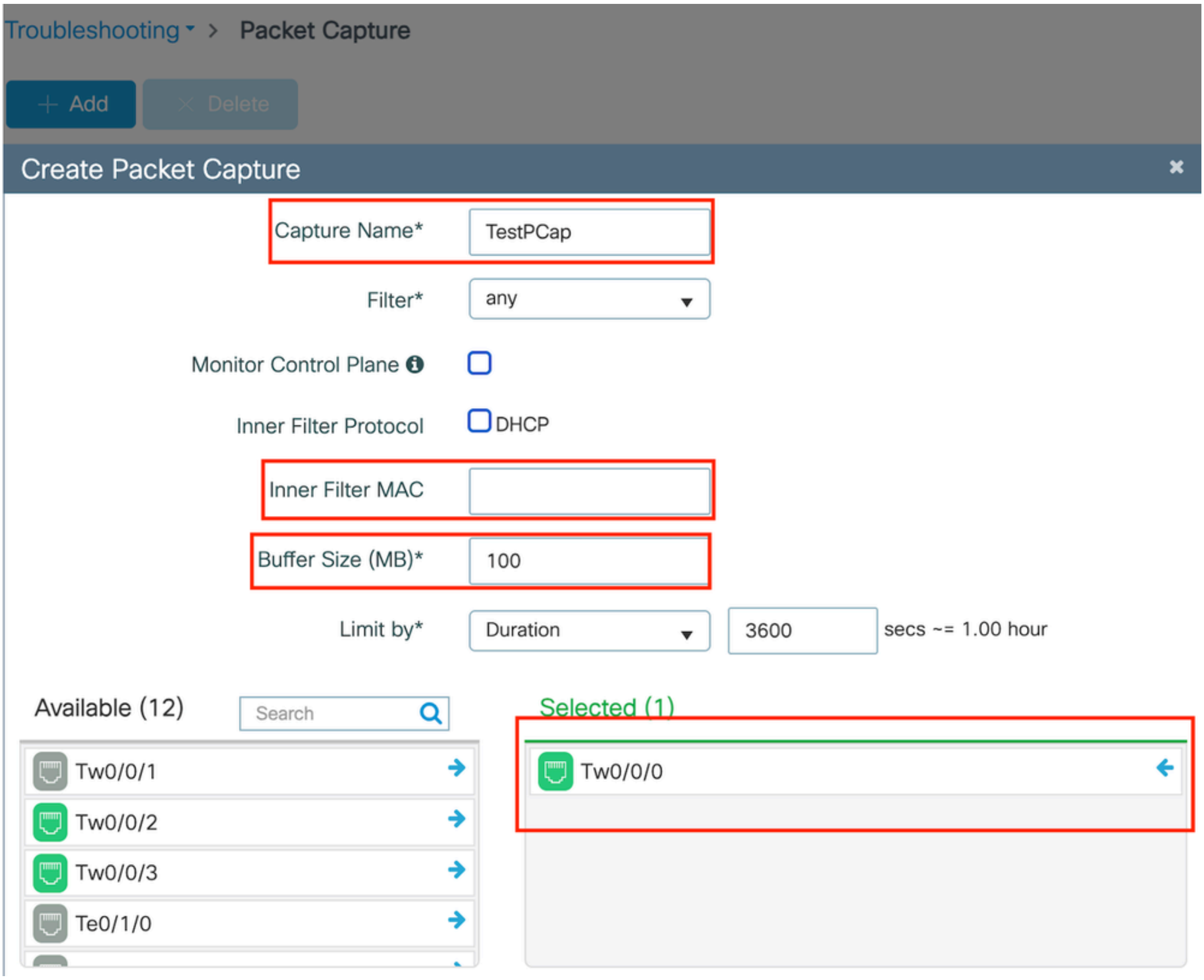


Troubleshooting > Radioactive Trace
Conditional Debug Global State: Started
+ Add
× Delete
✔ Start
Stop
Wireless Deb
Last Run
Add MAC/IP Address
MAC/IP Address*
Enter a MAC/IP Address every newline
Cancel
Apply to Device

seguimiento activo por radio

Capturas de paquetes integradas:

Vaya a Resolución de problemas > Captura de paquetes. Introduzca el nombre de la captura y especifique la dirección MAC del cliente como MAC del filtro interno. Establezca el tamaño del búfer en 100 y elija la interfaz de enlace ascendente para supervisar los paquetes entrantes y salientes.



Create Packet Capture

Capture Name*: TestPCap

Filter*: any

Monitor Control Plane: □

Inner Filter Protocol: □ DHCP

Inner Filter MAC:

Buffer Size (MB)*: 100

Limit by*: Duration 3600 secs ~= 1.00 hour

Available (12)

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

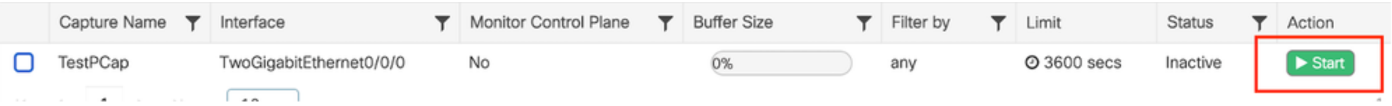
Selected (1)

Tw0/0/0

Captura de paquetes integrada

Nota: Seleccione la opción "Supervisar tráfico de control" para ver el tráfico redirigido a la CPU del sistema y reinyectado en el plano de datos.

Seleccione Iniciar para capturar paquetes



	Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
□	TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	▶ Start

Iniciar captura

Configuración de CLI

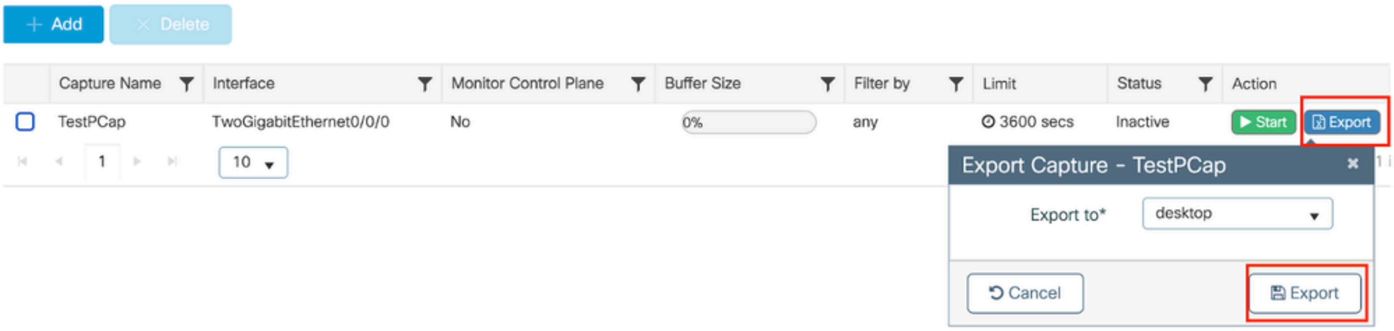
```
monitor capture TestPCap inner mac <H.H.H>
monitor capture TestPCap buffer size 100
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
monitor capture TestPCap start
```

```
<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)
```

Exportar captura de paquetes al servidor TFTP externo

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



	Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
□	TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	▶ Start Export

Export to* desktop

Exportar captura de paquetes

Ejemplo: durante una autenticación MAC correcta, un dispositivo cliente se conecta a la red, su dirección MAC es validada por el servidor RADIUS a través de políticas configuradas y, tras la verificación, el acceso lo concede el dispositivo de acceso a la red, lo que permite la conectividad de red.

Una vez que el cliente se asocia, el controlador envía una solicitud de acceso al servidor ISE.

El nombre de usuario es la dirección MAC del cliente, ya que se trata de la autenticación 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 envía la aceptación de acceso porque tenemos una entrada de usuario válida

```
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]
```

Estado de política del cliente transicionado a autenticación Mac completada

```
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
```

El cliente se encuentra en el estado de aprendizaje de IP después de una autenticación MAB satisfactoria

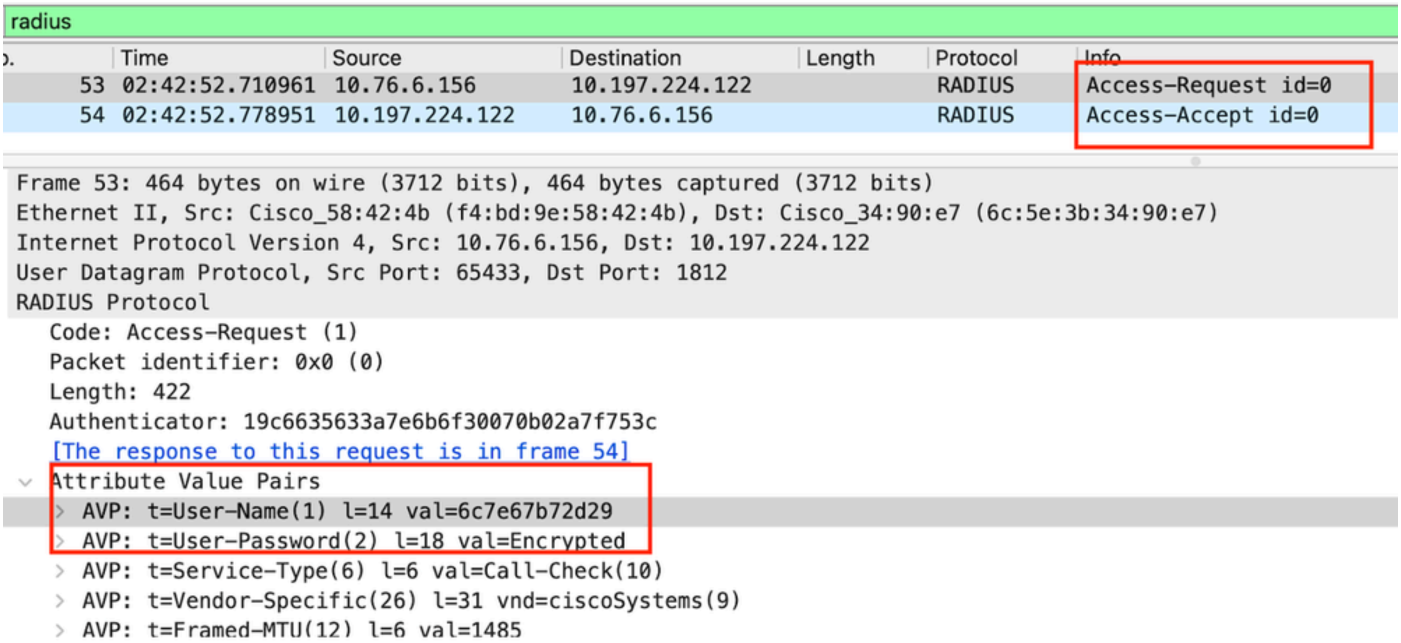
```
2024/07/16 21:12:55.791404789 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67b7.2d2
2024/07/16 21:12:55.791739386 {wncd_x_R0-0}{1}: [client-iplearn] [17765]: (info): MAC: 6c7e.67b7.2d29
```

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

Estado del administrador de directivas de cliente actualizado a RUN, se omite la autenticación Web para el cliente que completa la autenticación MAB

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

Verificación mediante captura de paquetes integrada



```
radius
o.        Time              Source           Destination      Length   Protocol  Info
     53   02:42:52.710961   10.76.6.156      10.197.224.122            RADIUS    Access-Request id=0
     54   02:42:52.778951   10.197.224.122   10.76.6.156               RADIUS    Access-Accept id=0

Frame 53: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 422
    Authenticator: 19c6635633a7e6b6f30070b02a7f753c
    [The response to this request is in frame 54]
  ⌄ Attribute Value Pairs
    > AVP: t=User-Name(1) l=14 val=6c7e67b72d29
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=Service-Type(6) l=6 val=Call-Check(10)
    > AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
    > AVP: t=Framed-MTU(12) l=6 val=1485
```

Paquete Radius

Ejemplo de fallo de autenticación MAC para un dispositivo cliente

Autenticación Mac iniciada para un cliente después de una asociación exitosa

```
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 enviaría Rechazo de acceso, ya que esta entrada de dispositivo no está presente en 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
```

Se inició Web-Auth para el dispositivo del cliente debido a un error de MAB

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

Una vez que el cliente inicia una solicitud GET HTTP, la URL de redirección se envía al dispositivo cliente, ya que el controlador falsifica la sesión TCP correspondiente.

```
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
```

El cliente inicia un HTTP Get a la URL de redireccionamiento y una vez que la página se carga, se envían las credenciales de inicio de sesión.

El controlador envía una solicitud de acceso a ISE

Se trata de una autenticación web ya que se observa un nombre de usuario válido en el paquete de aceptación de acceso

```
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
```

Access-Accept recibido desde 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
```

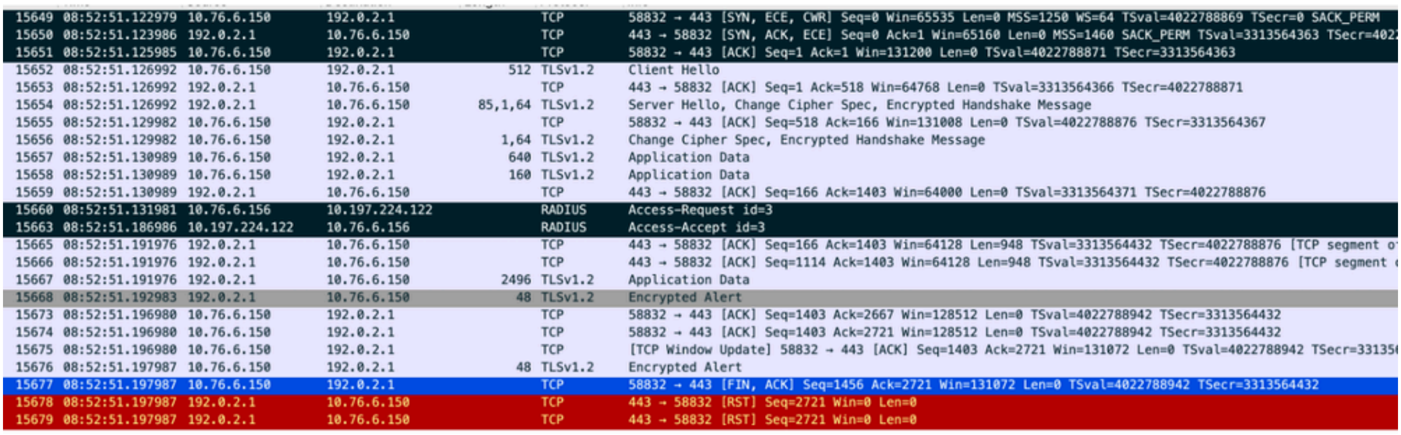
La autenticación web se realiza correctamente y la transición del estado del cliente al estado RUN

```
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
```

Verificación mediante capturas EPC

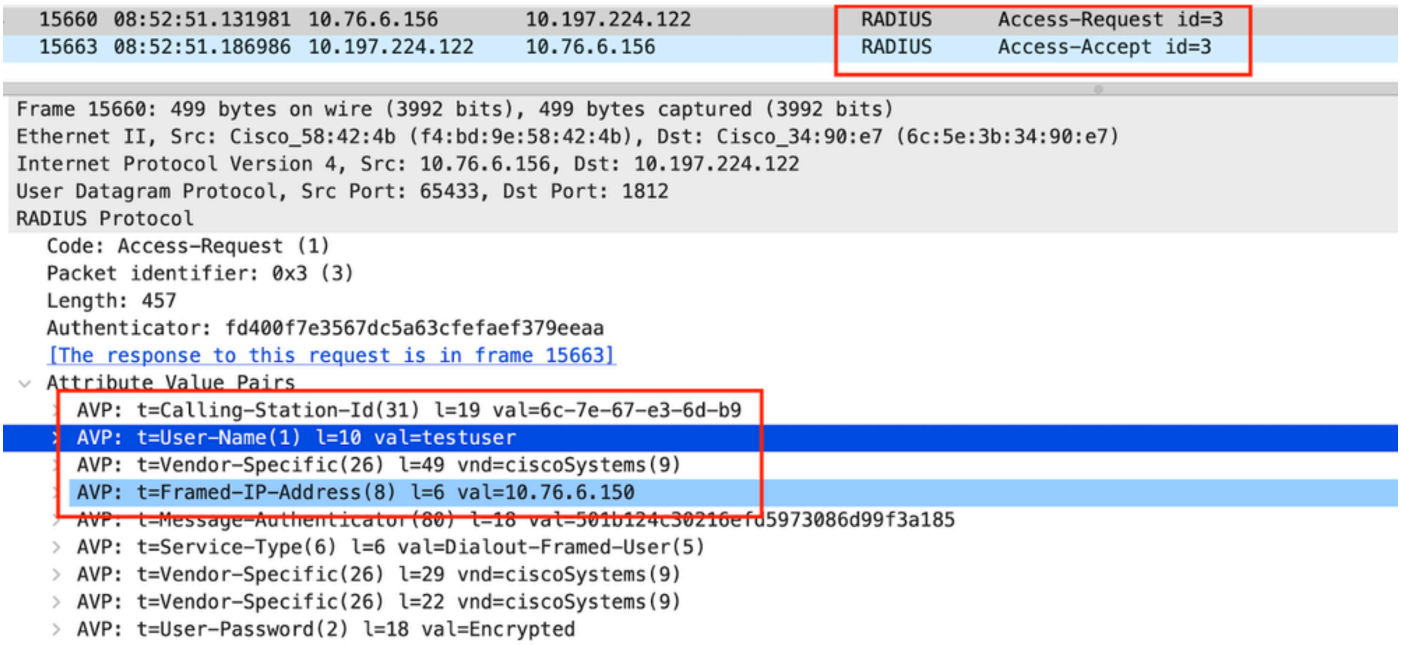
El cliente completa el protocolo de enlace TCP con la dirección IP virtual del controlador y el cliente carga la página del portal de redirección. Una vez que el usuario envía el nombre de usuario y la contraseña, podemos observar una solicitud de acceso radius desde la dirección IP de administración del controlador.

Después de una autenticación exitosa, la sesión TCP del cliente se cierra y en el controlador el cliente pasa al estado RUN.



```
15649 08:52:51.122979 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1250 WS=64 TSval=4022788869 TSecr=0 SACK_PERM
15650 08:52:51.123986 192.0.2.1       10.76.6.150                TCP      443 → 58832 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3313564363 TSecr=402
15651 08:52:51.125985 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=4022788871 TSecr=3313564363
15652 08:52:51.126992 10.76.6.150     192.0.2.1             512  TLSv1.2  Client Hello
15653 08:52:51.126992 192.0.2.1       10.76.6.150                TCP      443 → 58832 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313564366 TSecr=4022788871
15654 08:52:51.126992 192.0.2.1       10.76.6.150       85,1,64  TLSv1.2  Server Hello, Change Cipher Spec, Encrypted Handshake Message
15655 08:52:51.129982 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [ACK] Seq=518 Ack=166 Win=131008 Len=0 TSval=4022788876 TSecr=3313564367
15656 08:52:51.129982 10.76.6.150     192.0.2.1            1,64  TLSv1.2  Change Cipher Spec, Encrypted Handshake Message
15657 08:52:51.130989 10.76.6.150     192.0.2.1             640  TLSv1.2  Application Data
15658 08:52:51.130989 10.76.6.150     192.0.2.1             160  TLSv1.2  Application Data
15659 08:52:51.130989 192.0.2.1       10.76.6.150                TCP      443 → 58832 [ACK] Seq=166 Ack=1403 Win=64000 Len=0 TSval=3313564371 TSecr=4022788876
15660 08:52:51.131981 10.76.6.156     10.197.224.122             RADIUS   Access-Request id=3
15663 08:52:51.186986 10.197.224.122  10.76.6.156                RADIUS   Access-Accept id=3
15665 08:52:51.191976 192.0.2.1       10.76.6.150                TCP      443 → 58832 [ACK] Seq=166 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment o
15666 08:52:51.191976 192.0.2.1       10.76.6.150                TCP      443 → 58832 [ACK] Seq=1114 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment
15667 08:52:51.191976 192.0.2.1       10.76.6.150          2496  TLSv1.2  Application Data
15668 08:52:51.192983 192.0.2.1       10.76.6.150            48  TLSv1.2  Encrypted Alert
15673 08:52:51.196980 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [ACK] Seq=1403 Ack=2667 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15674 08:52:51.196980 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [ACK] Seq=1403 Ack=2721 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15675 08:52:51.196980 10.76.6.150     192.0.2.1                  TCP      [TCP Window Update] 58832 → 443 [ACK] Seq=1403 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=33135
15676 08:52:51.197987 10.76.6.150     192.0.2.1              48  TLSv1.2  Encrypted Alert
15677 08:52:51.197987 10.76.6.150     192.0.2.1                  TCP      58832 → 443 [FIN, ACK] Seq=1456 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15678 08:52:51.197987 192.0.2.1       10.76.6.150                TCP      443 → 58832 [RST] Seq=2721 Win=0 Len=0
15679 08:52:51.197987 192.0.2.1       10.76.6.150                TCP      443 → 58832 [RST] Seq=2721 Win=0 Len=0
```

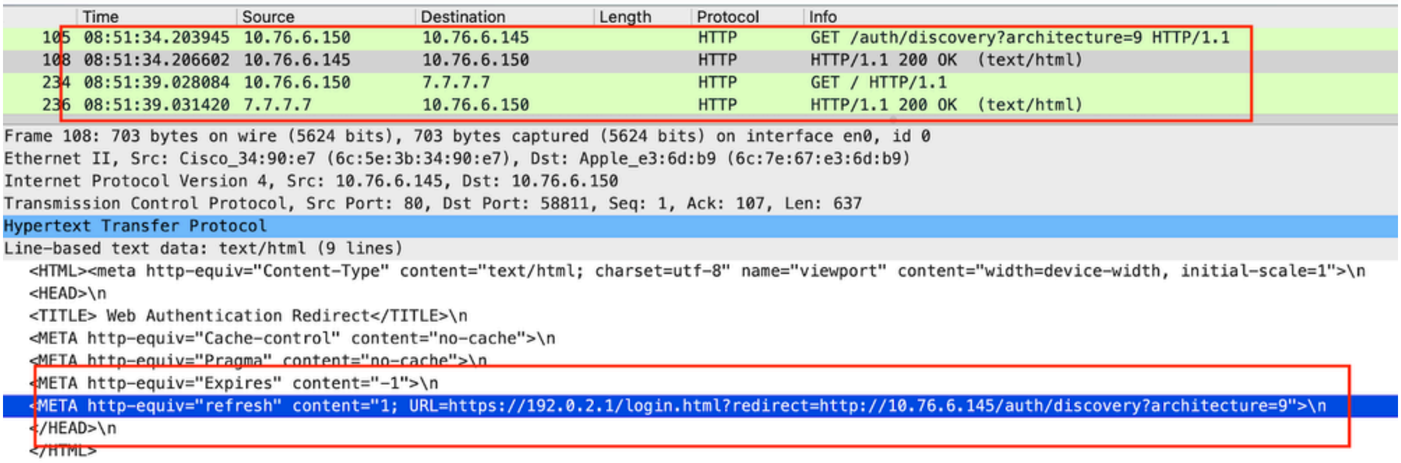
Flujo TCP con paquete RADIUS



```
  15660  08:52:51.131981  10.76.6.156        10.197.224.122        RADIUS      Access-Request  id=3
  15663  08:52:51.186986  10.197.224.122     10.76.6.156           RADIUS      Access-Accept  id=3

 Frame 15660: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits)
 Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
 Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
 User Datagram Protocol, Src Port: 65433, Dst Port: 1812
 RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x3 (3)
    Length: 457
    Authenticator: fd400f7e3567dc5a63cfefaef379eeaa
    [The response to this request is in frame 15663]
  ⌄ Attribute Value Pairs
    › AVP: t=Calling-Station-Id(31) l=19 val=6c-7e-67-e3-6d-b9
    › 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=10.76.6.150
    › AVP: t=Message-Authenticator(80) l=18 val=501b124c30216efd5973086d99f3a185
    › 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
```

Paquete RADIUS enviado a ISE con credenciales de usuario

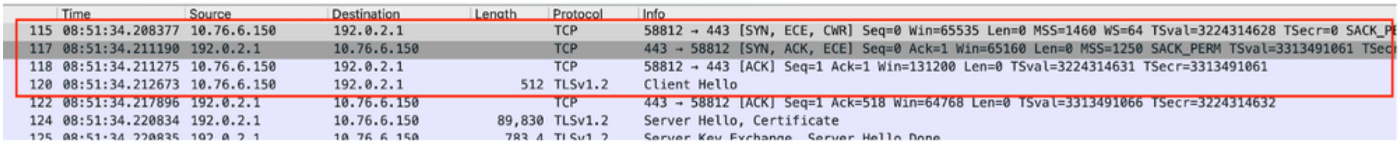
La captura de Wireshark del lado del cliente para validar que el tráfico del cliente se está redirigiendo a la página del portal y validar el intercambio de señales TCP con el controlador de la dirección IP virtual/servidor web



```
      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>
```

Captura del lado del cliente para validar la URL de redirección

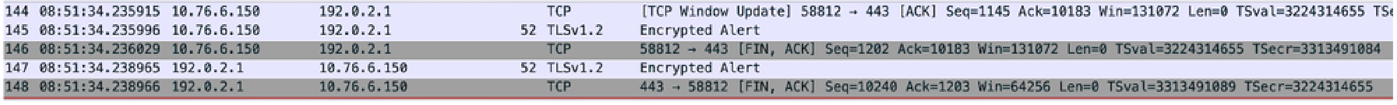
El cliente establece el protocolo de enlace TCP a la dirección IP virtual del controlador



```
      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 TSec
  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
```

Protocolo de enlace TCP entre el cliente y el servidor web

La sesión se cierra tras una autenticación web correcta.



```
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
```

Sesión TCP cerrada después de que el cliente complete la autenticación Web

Artículo relacionado

[Comprensión de las Depuraciones Inalámbricas y la Recopilación de Registros en los Controladores de LAN Inalámbrica Catalyst 9800]()

[Autenticación basada en Web en 9800]()

[Configuración de la autenticación Web local en 9800]()