

Configuración, verificación y solución de problemas de invitado con cables en controlador de LAN inalámbrica

Contenido

Introducción

Este documento describe cómo configurar, verificar y resolver problemas de acceso de invitado por cable en 9800 e IRCM con autenticación web externa.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

WLC 9800

WLC de AireOS

Túnel de movilidad

ISE

Se supone que se ha establecido un túnel de movilidad entre los dos WLC antes de configurar el acceso de invitado por cable.

Este aspecto está fuera del alcance de este ejemplo de configuración. Para obtener instrucciones detalladas, consulte el documento adjunto titulado [Configuración de topologías de movilidad en 9800](#)

Componentes Utilizados

9800 WLC versión 17.12.1

5520 WLC versión 8.10.185.0

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.

Configuración de invitado por cable en Catalyst 9800 anclado a otro Catalyst 9800

Diagrama de la red



Topología de red

Configuración en el WLC 9800 Externo

Configurar mapa de parámetro web

Paso 1: Vaya a Configuration > Security > Web Auth, seleccione Global, verifique la dirección IP virtual del controlador y la asignación de Trustpoint, y asegúrese de que el tipo esté configurado en webauth.

+ Add × Delete

Parameter Map Name

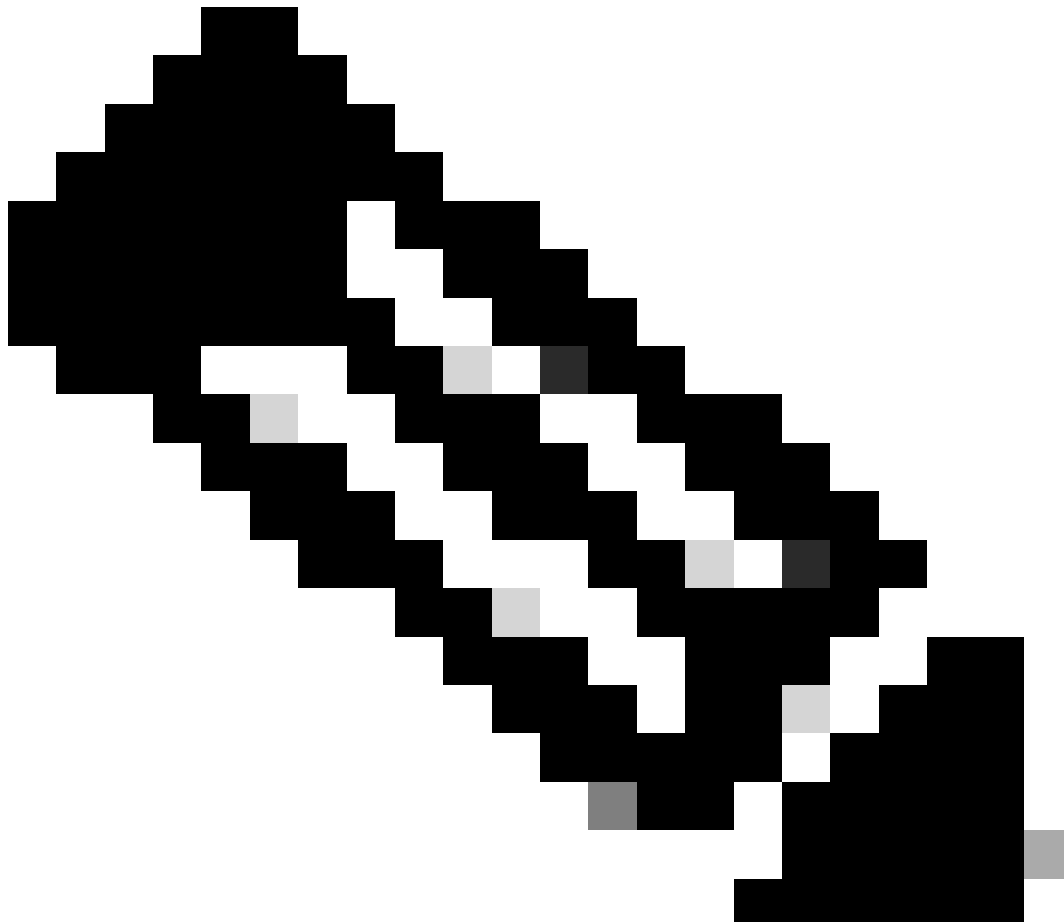
- global
- Web-Filter

1 10

General Advanced

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

Mapa de parámetro global



Nota: Web Auth intercept HTTPS es una configuración opcional. Si se requiere la redirección de HTTPS, la opción HTTPS de intercepción de Web Auth debe estar habilitada. Sin embargo, no se recomienda esta configuración ya que aumenta el uso de la CPU.

Paso 2: en la pestaña Advanced, configure la URL de la página web externa para la redirección del cliente. Defina "Redirigir URL para inicio de sesión" y "Redirigir en caso de fallo"; "Redirigir en caso de éxito" es opcional. Una vez configurado, se muestra una vista previa de la URL de redirección en el perfil de autenticación Web.

General **Advanced**

Preview of the Redirect URL:

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

Redirect to external server

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

Ficha Opciones avanzadas

Configuración de 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

Nota: En este escenario, se utiliza el mapa de parámetro global. Según los requisitos, configure un mapa de parámetros web personalizado seleccionando Add (Agregar) y, en la ficha Advanced (Avanzado), establezca la URL de redirección. Los parámetros Trustpoint e IP virtual se heredan del perfil global.

Configuración AAA:

Paso 1: Crear un servidor Radius:

Navegue hasta Configuration > Security > AAA, haga clic en "Add" bajo la sección Server/Group y en la página "Create AAA Radius Server", ingrese el nombre del servidor, la dirección IP y el secreto compartido.

Configuration > Security > AAA Show Me How

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add - Delete

RADIUS Servers Server Groups

Create AAA Radius Server

Name*	<input type="text"/>	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	<input type="text" value="IPv4/IPv6/Hostname"/>	CoA Server Key Type	Clear Text ▼
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	<input type="text"/>
Key Type	Clear Text ▼	Confirm CoA Server Key	<input type="text"/>
Key* ⓘ	<input type="text"/>	Automate Tester	<input type="checkbox"/>
Confirm Key*	<input type="text"/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		

Cancel Apply to Device

Configuración del servidor de RADIUS

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: Creación de un Grupo de Servidores RADIUS:

Seleccione "Agregar" en la sección Grupos de servidores para definir un grupo de servidores y cambiar los servidores que se incluirán en la configuración del grupo.

Configuration > Security > AAA [Show Me How](#)

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add × Delete

RADIUS Servers **Server Groups**

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	<input type="checkbox"/> DISABLED	
Source Interface VLAN ID	2074	

Available Servers Assigned Servers

ISE-Auth

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:

Navegue hasta la pestaña Lista de métodos AAA, seleccione Agregar en Autenticación, defina un nombre de lista de métodos con Tipo como "login" y Tipo de grupo como "Grupo", y asigne el grupo de servidores de autenticación configurado en la sección Grupo de servidores asignado.

Configuration > Security > AAA Show Me How

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add - Delete

Quick Setup: AAA Authentication

Method List Name* ISE-List

Type* login

Group Type group

Fallback to local

Available Server Groups

Assigned Server Groups

ISE-Group

Lista de métodos de autenticación

Configuración de CLI

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

Configurar perfil de directiva

Paso 1: Navegue hasta Configuration > Tags & Profiles > Policy, asigne un nombre al nuevo perfil en la pestaña General y actívelo mediante el botón de estado.

Configuration > Tags & Profiles > Policy

+ Add × Delete Clone

Add Policy Profile

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

General Access Policies QOS and AVC Mobility Advanced

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

Perfil de política

Paso 2: en la pestaña Políticas de acceso, asigne una vlan aleatoria cuando se complete la asignación de vlan en el controlador de anclaje. En este ejemplo, vlan 1 está configurado

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Disabled** ⓘ

Local Subscriber Policy Name ⓘ

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL ⓘ

IPv6 ACL ⓘ

URL Filters ⓘ

Pre Auth ⓘ

Post Auth ⓘ

Ficha Política de acceso

Paso 3: En la pestaña Mobility, cambie el controlador de anclaje a Primary (1) y, opcionalmente, configure los túneles de movilidad secundarios y terciarios para los requisitos de redundancia

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





Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

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

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

Available (3)	Selected (1)
Anchor IP	Anchor IP Anchor Priority
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.106.40.11 → </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.76.118.75 → </div> <div style="border: 1px solid #ccc; padding: 5px;">  10.76.118.74 → </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.76.118.70 <input type="text" value="Primary (1)"/> ← </div>

Mapa de movilidad

Configuración de CLI

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

Configurar perfil de LAN de invitado

Paso 1: Vaya a Configuration > Wireless > Guest LAN, seleccione Add, configure un nombre de perfil único, habilite Wired VLAN, ingrese el ID de VLAN para usuarios invitados por cable y cambie el estado del perfil a Enabled.

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

Perfil de LAN de invitado

Paso 2: en la ficha Security (Seguridad), habilite Web Auth (Autenticación web), asigne el mapa de parámetros de autenticación web y seleccione el servidor Radius en la lista desplegable Authentication (Autenticación).

Edit Guest LAN Profile

General

Security

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List



Ficha Seguridad de LAN para invitados

Configuración de CLI

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

MAPA LAN de invitado

Vaya a Configuration > Wireless > Guest LAN.

En la sección de configuración Guest LAN MAP, seleccione Add y asigne el perfil Policy y el perfil de Guest LAN

Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map: GuestMap

+ Add × Delete

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

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save Cancel

MAPA LAN de invitado

Configuración de CLI

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

Configuración en Anchor 9800 WLC

Configurar mapa de parámetro web

Paso 1: Vaya a Configuration > Security > Web Auth, seleccione Global, verifique la dirección IP virtual del controlador y la asignación de Trustpoint, y asegúrese de que el tipo esté configurado en webauth.

Configuration > Security > Web Auth

+ Add × Delete

Parameter Map Name

- global
- Web-Filter

1 10

Edit Web Auth Parameter

General Advanced

Parameter-map Name: global

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth

Captive Bypass Portal:

Disable Success Window:

Disable Logout Window:

Disable Cisco Logo:

Sleeping Client Status:

Sleeping Client Timeout (minutes): 720

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-3...

Virtual IPv4 Hostname:

Virtual IPv6 Address: x::x::x::x

Web Auth intercept HTTPs:

Enable HTTP server for Web Auth:

Disable HTTP secure server for Web Auth:

Banner Configuration

Banner Title:

Banner Type: None Banner Text

Paso 2: en la pestaña Advanced, configure la URL de la página web externa para la redirección del cliente. Defina "Redirigir URL para inicio de sesión" y "Redirigir en caso de fallo"; "Redirigir en caso de éxito" es opcional.

Una vez configurado, se muestra una vista previa de la URL de redirección en el perfil de autenticación Web.

General **Advanced**

i Preview of the Redirect URL:

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

Redirect to external server

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

Ficha Opciones avanzadas

Configuración de 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
```

Configuración AAA:

Paso 1: Crear un servidor Radius:

Navegue hasta Configuration > Security > AAA, haga clic en Add bajo la sección Server/Group y en la página "Create AAA Radius Server", ingrese el nombre del servidor, la dirección IP y el secreto compartido.

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

Configuración del servidor de RADIUS

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: Creación de un Grupo de Servidores RADIUS:

Seleccione Agregar en la sección Grupos de Servidores para definir un grupo de servidores y alternar los servidores que se incluirán en la configuración del grupo.

Name* ISE-Group

Group Type RADIUS

MAC-Delimiter none ▼

MAC-Filtering none ▼

Dead-Time (mins) 5

Load Balance DISABLED

Source Interface VLAN ID 2081 ▼

Available Servers

Assigned Servers



ISE-Auth

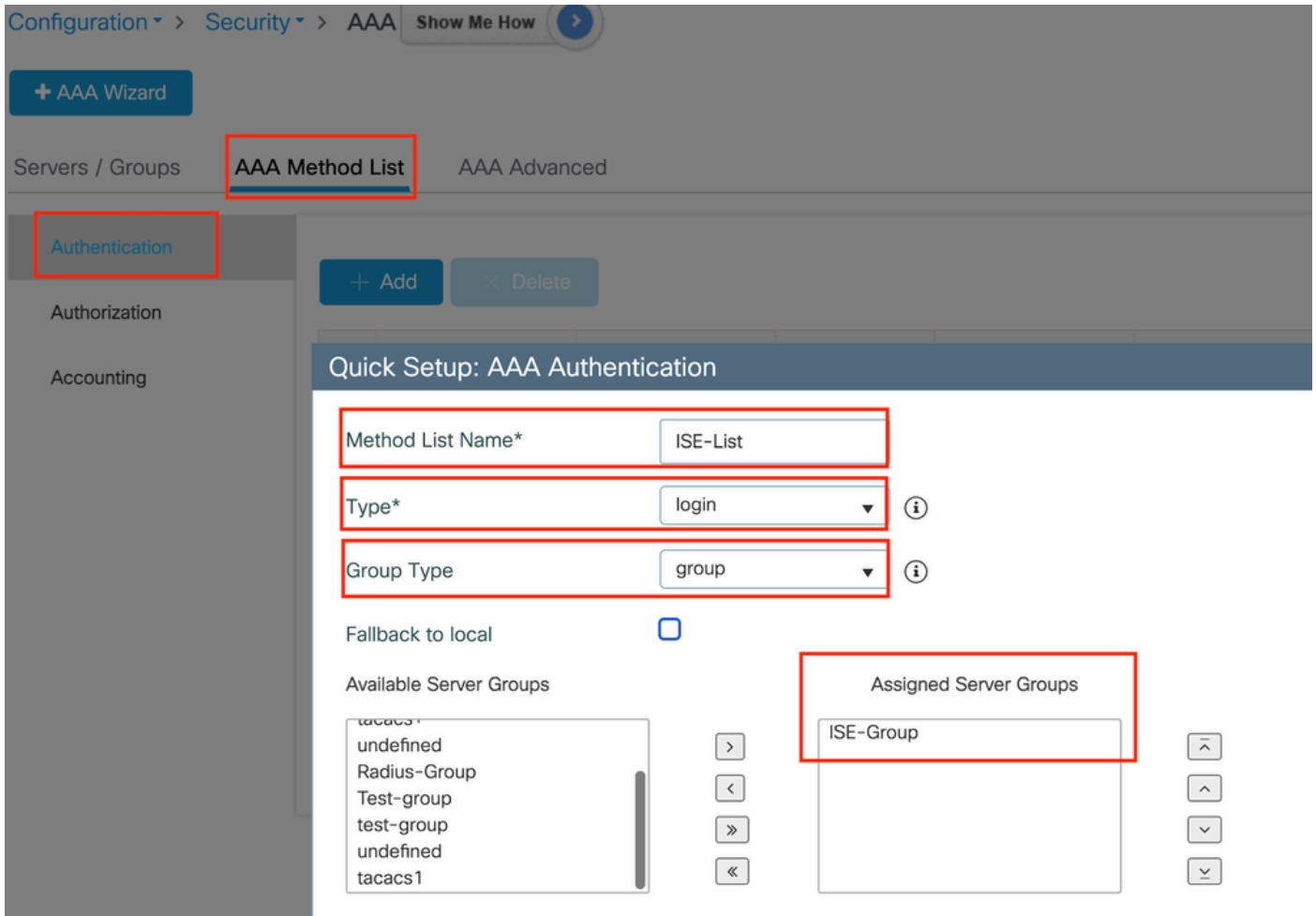
Grupo de radio de anclaje

Configuración de CLI

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

Paso 3: Configuración de la Lista de Métodos AAA:

Navigate hasta la pestaña AAA Method List, seleccione Add en Authentication, defina un nombre de lista de métodos con Type como "login" y Group como "Group", y asigne el grupo de servidores de autenticación configurado en la sección Assigned Server Group .



Lista de métodos de autenticación

Configuración de CLI

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

Configurar perfil de directiva

Paso 1: Vaya a Configuration > Tag & Profiles > Policy, configure el perfil de política con el mismo nombre que en el controlador externo y habilite el perfil.

General

Access Policies

QOS and AVC

Mobility

Advanced

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

WLAN Switching Policy

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

Perfil de política de anclaje

Paso 2: en Access Policies, asigne la vlan del cliente cableado de la lista desplegable

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

VLAN2024





Nota: La configuración del perfil de política debe coincidir en ambos controladores, el externo y el de anclaje, excepto para la VLAN.

Paso 3: En la pestaña Mobility, marque la casilla Export Anchor.

Mobility Anchors

Export Anchor



Static IP Mobility



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

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

Available (2)

Selected (0)

Anchor IP

Anchor IP

Anchor IP

Exportar delimitador



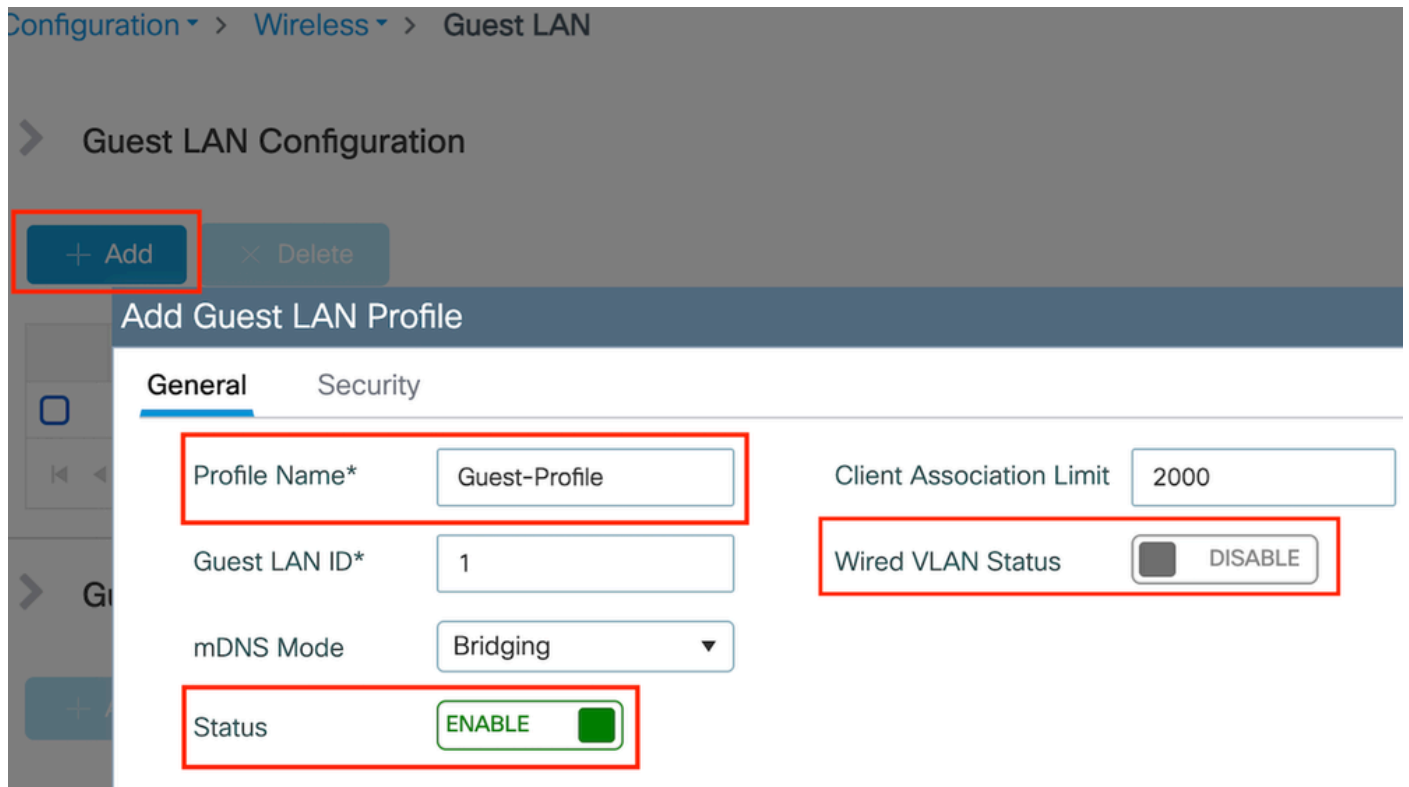
Nota: Esta configuración designa el controlador de LAN inalámbrica (WLC) 9800 como el WLC de anclaje para cualquier WLAN asociada con el perfil de política especificado. Cuando un WLC 9800 externo redirige a los clientes al WLC de anclaje, proporciona detalles sobre el WLAN y el perfil de política asignado al cliente. Esto permite que el WLC de anclaje aplique el perfil de política local apropiado basado en la información recibida.

Configuración de CLI

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

Configurar perfil de LAN de invitado

Paso 1: Vaya a Configuration > Wireless > Guest LAN, luego seleccione Add para crear y configurar el perfil de Guest LAN. Asegúrese de que el nombre del perfil coincida con el del controlador externo. Tenga en cuenta que la VLAN cableada debe estar inhabilitada en el controlador de anclaje.



Perfil de LAN de invitado

Paso 2: en la configuración de seguridad, habilite Web Auth y luego configure el mapa de parámetro de Web Auth y la lista de autenticación.

Edit Guest LAN Profile

General

Security

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List





Nota: La configuración del perfil de LAN de invitado debe ser idéntica entre los controladores externos y de anclaje, excepto para el estado de VLAN con cable

Configuración de CLI

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

MAPA LAN de invitado

Paso 1: Vaya a Configuration > Wireless > Guest LAN. En la sección de configuración de Guest LAN MAP, seleccione Add y asigne el perfil de política al perfil de Guest LAN.

Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map : GuestMap

+ Add × Delete

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

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save Cancel

MAPA LAN de invitado

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

Configuración de invitado por cable en Catalyst 9800 anclado al controlador AireOS 5520



Topología de red

Configuración en el WLC 9800 Externo

Configurar mapa de parámetro web

Paso 1: Vaya a Configuration > Security > Web Auth y seleccione Global. Verifique que la dirección IP virtual del controlador y el Trustpoint estén correctamente asignados en el perfil, con el tipo establecido en webauth.

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

Mapa de parámetro web

Paso 2: en la pestaña Advanced, especifique la URL de la página web externa a la que se deben redirigir los clientes. Configure la URL de redireccionamiento para el inicio de sesión y redireccione en caso de fallo. El parámetro Redirigir cuando se realiza correctamente es una configuración opcional.

Preview of the Redirect URL:

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

Redirect to external server

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

Ficha Opciones avanzadas

Configuración de 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
```



Nota: Para la configuración AAA, consulte los detalles de configuración proporcionados en la sección "" para el WLC 9800 Externo.

Configurar perfil de directiva

Paso 1: Vaya a Configuración > Etiquetas y perfiles > Política. Seleccione Add y, en la ficha General, proporcione un nombre para el perfil y habilite la alternancia de estado.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Guest

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Perfil de políticas

Paso 2: en la pestaña Políticas de acceso, asigne una VLAN aleatoria.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

1



Multicast VLAN

Enter Multicast VLAN

Políticas de acceso

Paso 3: En la pestaña Movilidad, alterne el controlador de anclaje y establezca su prioridad en Primario (1)

Mobility Anchors

Export Anchor



Static IP Mobility




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

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

Available (1)



Anchor IP

 10.76.6.156 

Selected (1)

Anchor IP

Anchor Priority

 10.76.118.74	Primary (1) 
--	---



Nota: El perfil de política del WLC externo 9800 debe coincidir con el perfil de LAN de invitado del WLC de anclaje 5520, excepto para la configuración de vlan

Configuración de 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
```

Configurar perfil de LAN de invitado

Paso 1: Vaya a Configuration > Wireless > Guest LAN y seleccione Add. Configure un nombre de

perfil único y habilite VLAN cableada, especificando el ID de VLAN dedicado para usuarios invitados con cable. Por último, cambie el estado del perfil a Activado.

General

Security

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

Política de LAN de invitado

Paso 2: en la pestaña Security, habilite Web Auth, asigne el mapa de parámetro de Web Auth y seleccione el servidor RADIUS de la lista desplegable Authentication.

General

Security

Layer3

Web Auth

ENABLE

Web Auth Parameter Map

global

Authentication List

ISE-List

Ficha Seguridad



Nota: El nombre del perfil de la LAN de invitado debe ser el mismo para el controlador de anclaje 9800 externo y 5520

Configuración de CLI

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

MAPA LAN de invitado

Paso 1: Vaya a Configuration > Wireless > Guest LAN. En la sección de configuración Guest LAN MAP, seleccione Add y asigne el perfil de política al perfil de LAN de invitado.

> Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map : GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page 0 - 0 of 0 items

Profile Name: Guest

Policy Name: Guest

Save Cancel

MAPA LAN de invitado

Configuración de CLI

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

Configuración en Anchor 5520 WLC

Configurar autenticación web

Paso 1: Navegue hasta Seguridad > Autenticación Web > Página de Login Web. Establezca el tipo de autenticación Web en Externa (Redirigir a servidor externo) y configure la URL de autenticación Web externa. El URL de redireccionamiento después del login es opcional y se puede configurar si los clientes necesitan ser redirigidos a una página dedicada después de una autenticación exitosa.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

User: admin(ReadWrite) Home

Security

Web Login Page

Web Authentication Type: External (Redirect to external server)

Redirect URL after login: http://10.127.196.171/webauth/logout.html

Login Success Page Type: None

External Webauth URL: http://10.127.196.171/webauth/login.html

QrCode Scanning Bypass Timer: 0

QrCode Scanning Bypass Count: 0

Preview... Apply

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Auth Cached Users
 - Failback
 - DNS
 - Downloaded AVP
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
 - Web Login Page
 - Certificate

Configuración AAA:

Paso 1: Configuración del servidor RADIUS

Vaya a Seguridad > Radio > Autenticación > Nuevo.



Servidor Radius

Paso 2: Configure la IP del servidor RADIUS y el secreto compartido en el controlador. Cambie el estado del servidor a Habilitado y marque la casilla de verificación Usuario de red.

RADIUS Authentication Servers > New

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

Configuración del servidor

Configurar lista de control de acceso

Paso 1: Navegue hasta Seguridad > Lista de control de acceso y seleccione Nuevo. Cree una

ACL de autenticación previa que permita el tráfico a DNS y al servidor web externo.

The screenshot shows the Cisco ISE Security page. The 'SECURITY' tab is highlighted. The left sidebar shows the navigation menu with 'Access Control Lists' selected. The main content area is titled 'Access Control Lists > Edit' and shows the 'General' tab for an ACL named 'Pre-Auth_ACL'. The 'Deny Counters' are set to 0. A table lists six permit rules:

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

Lista de acceso para permitir el tráfico al servidor web

Configurar perfil de LAN de invitado

Paso 1: Vaya a WLANs > seleccione Create New .

Seleccione Type as Guest LAN y configure el mismo nombre que el perfil de política del controlador externo 9800.

The screenshot shows the Cisco ISE WLANs page. The 'WLANs' tab is highlighted. The 'Current Filter' is set to 'None'. A 'Create New' button is visible, along with a 'Go' button. Below the buttons, there is a table header with columns: 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'.

Crear LAN de invitado

The screenshot shows the Cisco ISE 'WLANs > New' page. The 'Type' dropdown is set to 'Guest LAN'. The 'Profile Name' field contains 'Guest'. The 'ID' dropdown is set to '2'. There are 'Back' and 'Apply' buttons at the bottom right.

Perfil de LAN de invitado

Paso 2: asigne las interfaces de entrada y salida en el perfil de LAN de invitado.

La interfaz de ingreso en este caso es ninguna porque la interfaz de ingreso es el túnel EoIP del

controlador externo.

La interfaz de egreso es la VLAN donde el cliente cableado se conecta físicamente .

The screenshot shows the 'Security' tab of a configuration interface. The 'Profile Name' is 'Guest'. The 'Type' is 'Guest LAN'. The 'Status' is 'Enabled'. Under 'Security Policies', 'Web-Auth' is selected. The 'Ingress Interface' is 'None' and the 'Egress Interface' is 'wired-vlan-11'. The 'NAS-ID' is 'none'.

Profile Name	Guest
Type	Guest LAN
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	Web-Auth (Modifications done under security tab will appear after applying the changes.)
Ingress Interface	None
Egress Interface	wired-vlan-11
NAS-ID	none

Perfil de LAN de invitado

Paso 3: en la pestaña Security, seleccione Layer 3 security as Web Authentication y asigne la ACL de autenticación previa.

WLANs > Edit 'Guest'

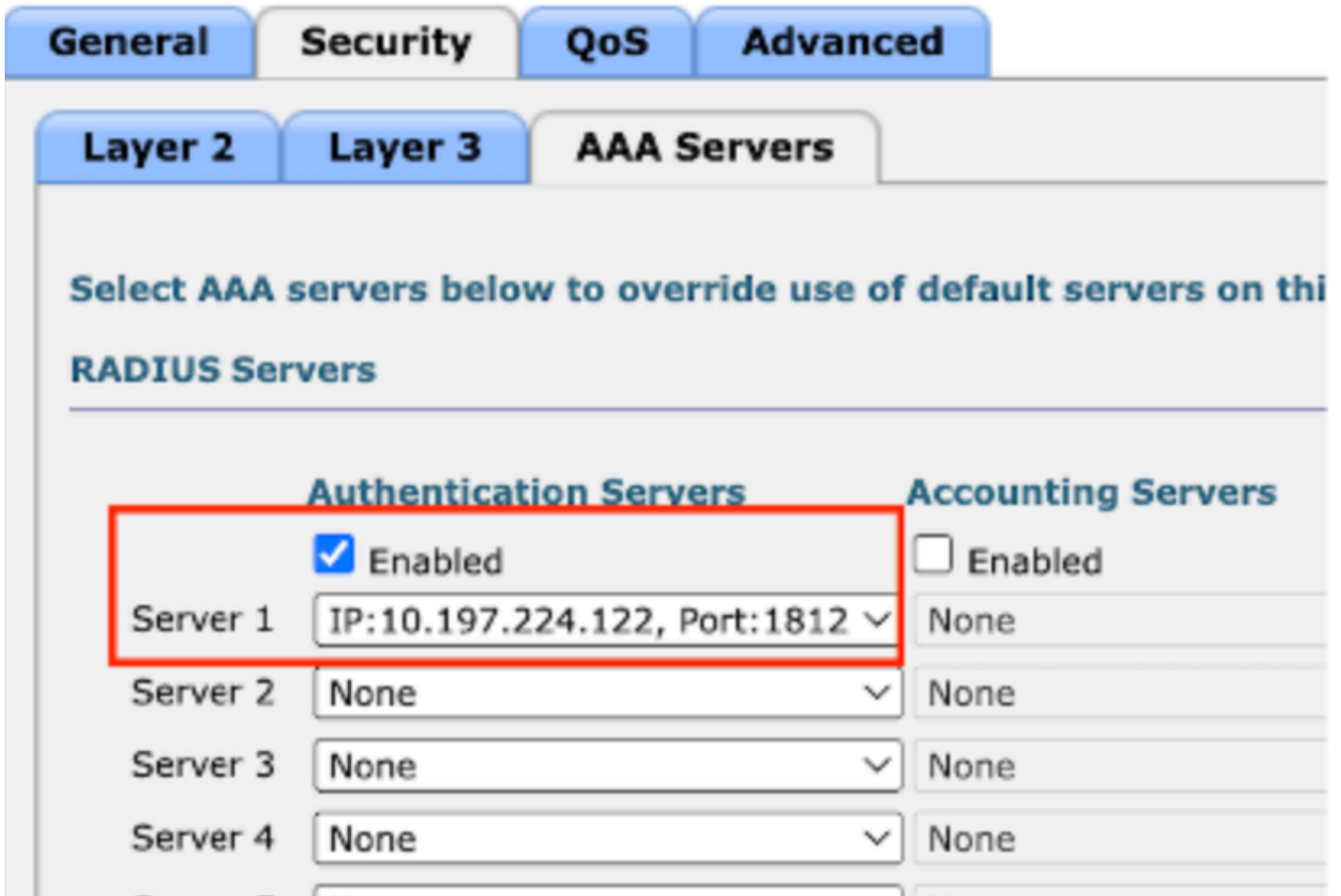
The screenshot shows the 'Security' tab of a configuration interface, specifically the 'Layer 3' sub-tab. The 'Layer 3 Security' is set to 'Web Authentication'. The 'Preauthentication ACL' is set to 'Pre-Auth_ACL' for IPv4 and 'None' for IPv6. The 'Override Global Config' checkbox is unchecked.

Layer 3 Security	Web Authentication	
Preauthentication ACL	IPv4 Pre-Auth_ACL	IPv6 None
Override Global Config ²⁰	<input type="checkbox"/> Enable	

Ficha Seguridad de LAN para invitados

Paso 4: Vaya a Seguridad > Servidor AAA.

Seleccione el menú desplegable y asigne el servidor RADIUS al perfil de LAN de invitado.



Asignar el servidor RADIUS al perfil LAN de invitado

Paso 5: Vaya a WLAN. Pase el ratón sobre el icono desplegable del perfil de LAN de invitado y seleccione Anclas de movilidad.



Paso 6: Seleccione Mobility Anchor Create para configurar el controlador como anclaje de exportación para este perfil de LAN de invitado.



Creación de anclaje de movilidad

Configuración de invitado por cable en AireOS 5520 anclado a Catalyst 9800



Topología de red

Configuración en el WLC 5520 Externo

Configuración de interfaz del controlador

Paso 1: Vaya a Controlador > Interfaces > Nuevo. Configure un nombre de interfaz, ID de VLAN y habilite la LAN de invitado.

Wired Guest requiere dos interfaces dinámicas.

En primer lugar, cree una interfaz dinámica de capa 2 y declárela como LAN de invitado. Esta interfaz sirve como interfaz de entrada para la LAN de invitado, donde se conectan físicamente los clientes con cables.

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

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

Interfaz de entrada

Paso 2: Vaya a Controlador > Interfaces > Nuevo. Configure un nombre de interfaz, ID de VLAN.

La segunda interfaz dinámica debe ser una interfaz de Capa 3 en el controlador; los clientes cableados reciben la dirección IP de esta subred de vlan. Esta interfaz sirve como interfaz de salida para el perfil de LAN de invitado.

Controller

Interfaces > Edit

General Information

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

Configuration

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

Physical Information

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

Interface Address

VLAN Identifier	2024
IP Address	10.105.211.85
Netmask	255.255.255.128
Gateway	10.105.211.1

Interfaz de salida

Configuración del puerto del switch

Los usuarios invitados por cable se conectan al switch de capa de acceso; estos puertos designados deben configurarse con VLAN en la que la LAN de invitado esté habilitada en el controlador

Configuración del puerto del switch de capa de acceso

```
interface gigabitEthernet <x/x/x>
```

```
description Acceso de invitado por cable
```

switchport access vlan 2020

switchport mode access

Finalizar

Configuración del puerto de link ascendente del controlador externo

interface TenGigabitEthernet<x/x/x>

description Puerto troncal al WLC externo

switchport mode trunk

switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2020

Finalizar

Configuración del puerto de enlace ascendente del controlador de anclaje

interface TenGigabitEthernet<x/x/x>

description Puerto troncal al WLC de anclaje

switchport mode trunk

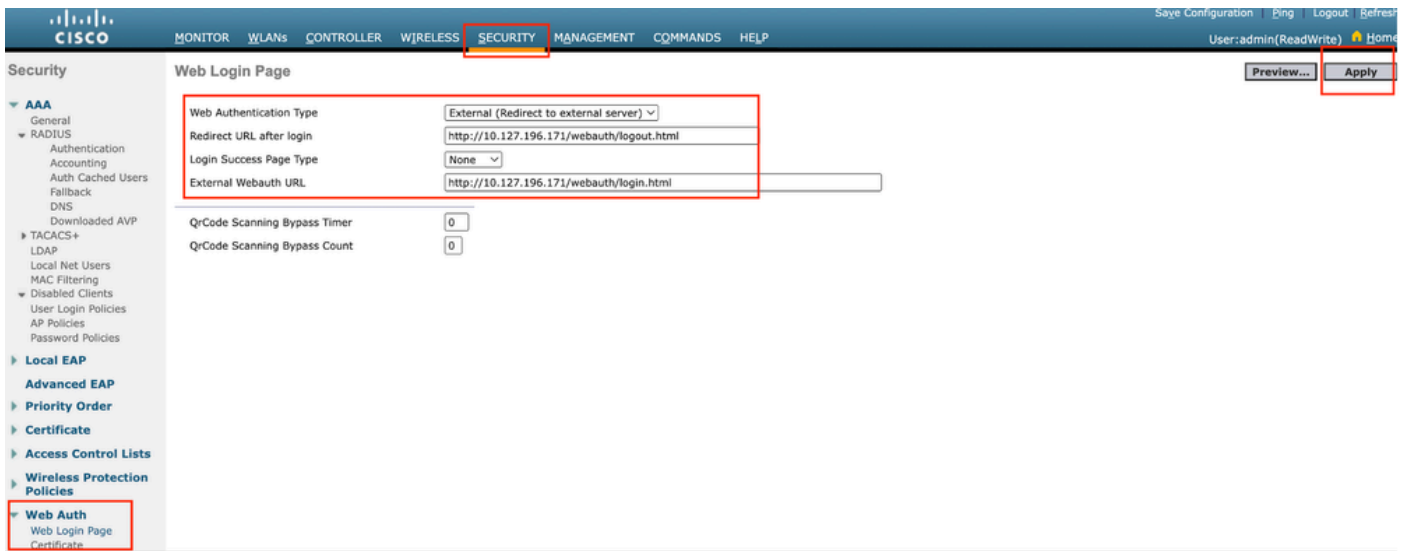
switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2024

Finalizar

Configurar autenticación web

Paso 1: Navegue hasta Seguridad > Autenticación Web > Página de Login Web. Establezca el tipo de autenticación Web en Externa (Redirigir a servidor externo) y configure la URL de autenticación Web externa. El URL de redireccionamiento después del login es opcional y se puede configurar si los clientes necesitan ser redirigidos a una página dedicada después de una autenticación exitosa.



Configuración de Web Auth

Configuración AAA:

Paso 1: Configuración del servidor RADIUS

Vaya a Seguridad > Radio > Autenticación > Nuevo.



Servidor Radius

Paso 2: Configure la IP del servidor RADIUS y el secreto compartido en el controlador. Cambie el estado del servidor a Habilitado y marque la casilla de verificación Usuario de red.

RADIUS Authentication Servers > New

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

Configuración del servidor

Configurar lista de control de acceso

Paso 1: Navegue hasta Seguridad > Lista de control de acceso y seleccione Nuevo. Cree una

ACL de autenticación previa que permita el tráfico a DNS y al servidor web externo.

The screenshot shows the Cisco ISE Security page. The 'SECURITY' tab is highlighted in the top navigation bar. On the left sidebar, 'Access Control Lists' is highlighted. The main content area is titled 'Access Control Lists > Edit' and shows the 'General' tab for the 'Pre-Auth_ACL' list. Below this, there is a table of rules:

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

Lista de acceso para permitir el tráfico al servidor web

Configurar perfil de LAN de invitado

Paso 1: Vaya a WLAN > Create New > Go.

The screenshot shows the Cisco ISE WLANs page. The 'WLANs' tab is highlighted in the top navigation bar. On the left sidebar, 'WLANs' is highlighted. The main content area shows the 'WLANs' section with a 'Current Filter: None' and links for '[Change Filter]' and '[Clear Filter]'. A 'Create New' button with a dropdown arrow and a 'Go' button are highlighted with a red box.

Perfil de LAN de invitado

Seleccione Type as Guest LAN (Tipo como LAN de invitado) y configure un nombre de perfil. Se debe configurar el mismo nombre en el perfil de política y en el perfil de LAN de invitado del controlador de anclaje 9800.

WLANs > New

Type

Guest LAN

Profile Name

Guest-Profile

ID

3

Perfil de LAN de invitado

Paso 2: en la ficha General, asigne la interfaz de entrada y salida en el perfil de LAN de invitado.

La interfaz de ingreso es la vlan a la que se conectan físicamente los clientes cableados.

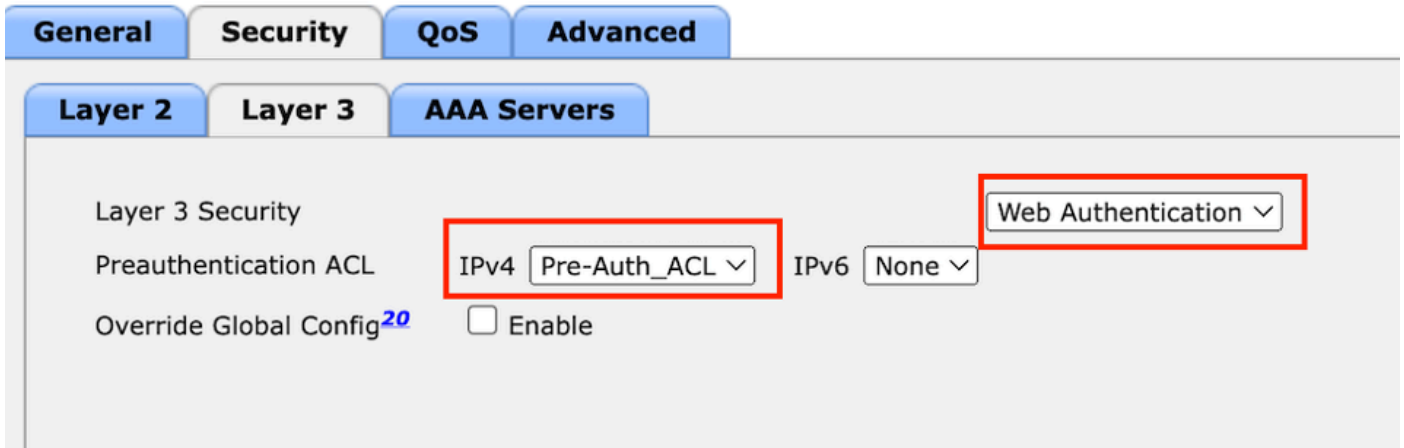
La interfaz de salida es la subred de VLAN que los clientes solicitan para la dirección IP.

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

Perfil de LAN de invitado

Paso 3: Vaya a Seguridad > Capa 3.

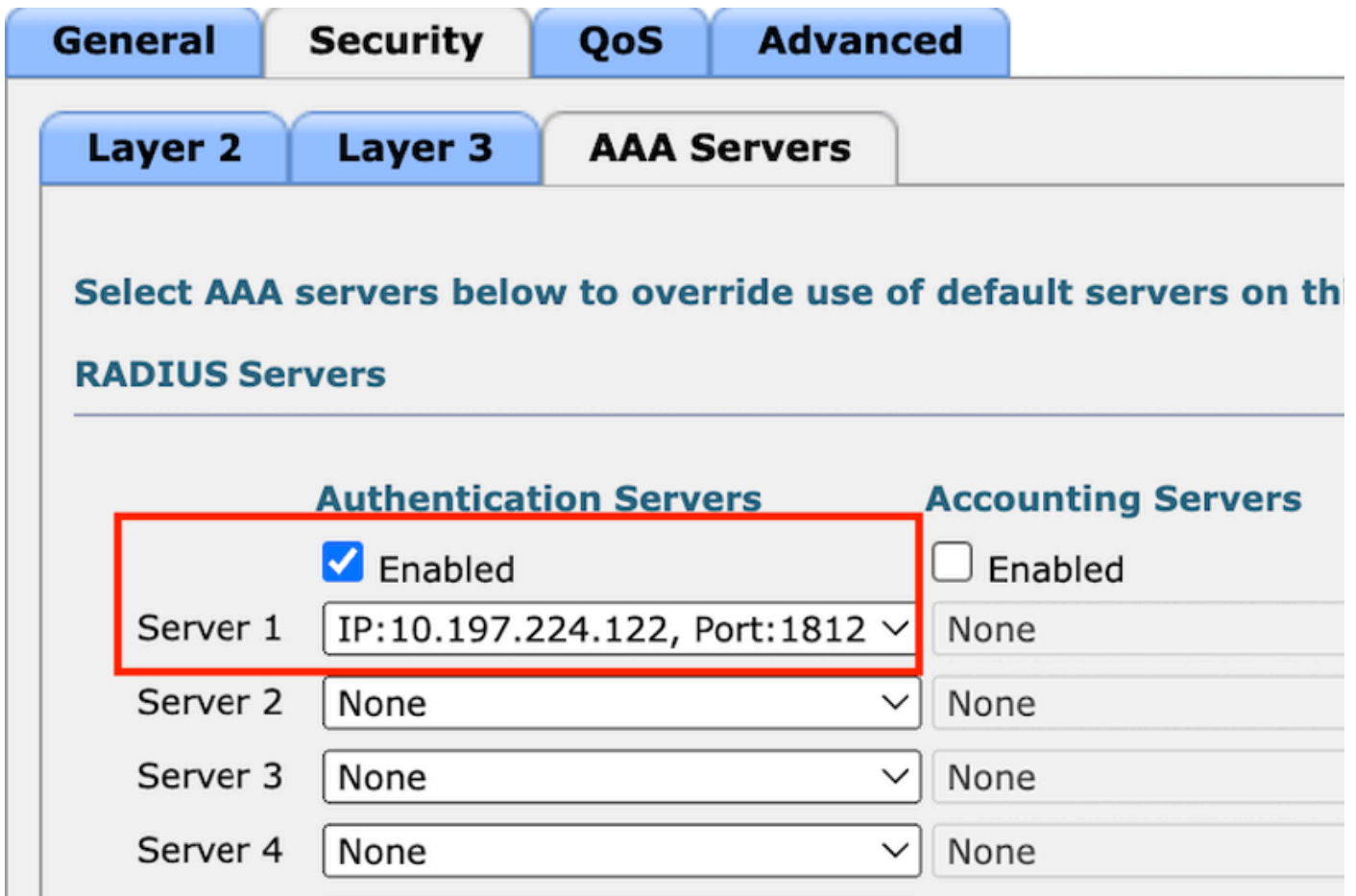
Seleccione Layer 3 Security como Web Authentication y asigne la ACL de autenticación previa.



Ficha Seguridad de capa 3

Paso 4:

En la pestaña de servidores AAA, asigne el servidor Radius y marque la casilla de verificación Enabled.



Asignación de servidores RADIUS al perfil de LAN de invitado

Paso 5: Vaya a la página WLAN, pase el cursor por el icono de descenso del perfil de LAN de invitado y seleccione Anclas de movilidad.

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

Anclas de movilidad

Paso 6: asigne el ancla de movilidad de la lista desplegable al perfil de LAN de invitado.

Mobility Anchors

WLAN SSID Guest-Profile

Switch IP Address (Anchor)

Switch IP Address (Anchor)

Foot Notes

local
10.106.39.41
10.76.6.156
 10.76.118.70

Data Path

Co

Asignación de anclaje de movilidad a LAN de invitado

Configuración en Anchor 9800 WLC

Configurar mapa de parámetro web

Paso 1: Vaya a Configuration > Security > Web Auth y seleccione Global. Verifique que la dirección IP virtual del controlador y el Trustpoint estén correctamente asignados en el perfil, con el tipo establecido en webauth.

General

Advanced

Parameter-map Name Maximum HTTP connections Init-State Timeout(secs) Type Captive Bypass Portal Disable Success Window Disable Logout Window Disable Cisco Logo Sleeping Client Status Sleeping Client Timeout (minutes) Virtual IPv4 Address Trustpoint Virtual IPv4 Hostname Virtual IPv6 Address Web Auth intercept HTTPs Enable HTTP server for Web Auth Disable HTTP secure server for Web Auth **Banner Configuration**Banner Title Banner Type None Banner Text Read From File

Mapa de parámetro web

Paso 2: en la pestaña Advanced, especifique la URL de la página web externa a la que se deben redirigir los clientes. Configure la URL de redireccionamiento para el inicio de sesión y redireccione en caso de fallo. El parámetro Redirigir cuando se realiza correctamente es una configuración opcional.

Preview of the Redirect URL:

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

Redirect to external server

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

Ficha Opciones avanzadas

Configuración de 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
```



Nota: Para la configuración AAA, consulte los detalles de configuración proporcionados en la sección "Configuración de invitado por cable en Catalyst 9800 anclado a otro Catalyst 9800" para el WLC 9800 externo.

Configurar perfil de directiva

Paso 1: Vaya a Configuración > Etiquetas y perfiles > Política. Configure el perfil de política con el mismo nombre utilizado para el perfil de LAN de invitado del controlador externo.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status ENABLED

Passive Client DISABLED

IP MAC Binding ENABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

Perfil de política

Paso 2: en la ficha Access Policies (Políticas de acceso), asigne la vlan del cliente por cable de la lista desplegable

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device
Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

VLAN2024



Multicast VLAN

Enter Multicast VLAN

Políticas de acceso

Paso 3: en la pestaña Mobility, marque la casilla Export Anchor.

Mobility Anchors

Export Anchor



Static IP Mobility



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

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

Ficha Movilidad

Configuración de CLI

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

Configurar perfil de LAN de invitado

Paso 1: Vaya a Configuration > Wireless > Guest LAN y seleccione Add para configurar el perfil de LAN de invitado y desactivar el estado de VLAN por cable.

El nombre del perfil de LAN de invitado en el anclaje debe ser el mismo que el perfil de LAN de invitado en el WLC extranjero.

General

Security

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

Perfil de LAN de invitado

Paso 2: en la pestaña Security, habilite Web Auth. Seleccione el mapa de parámetro de autenticación Web y la lista de autenticación de la lista desplegable

Edit Guest LAN Profile

General

Security

Layer3

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

Ficha Seguridad de LAN para invitados

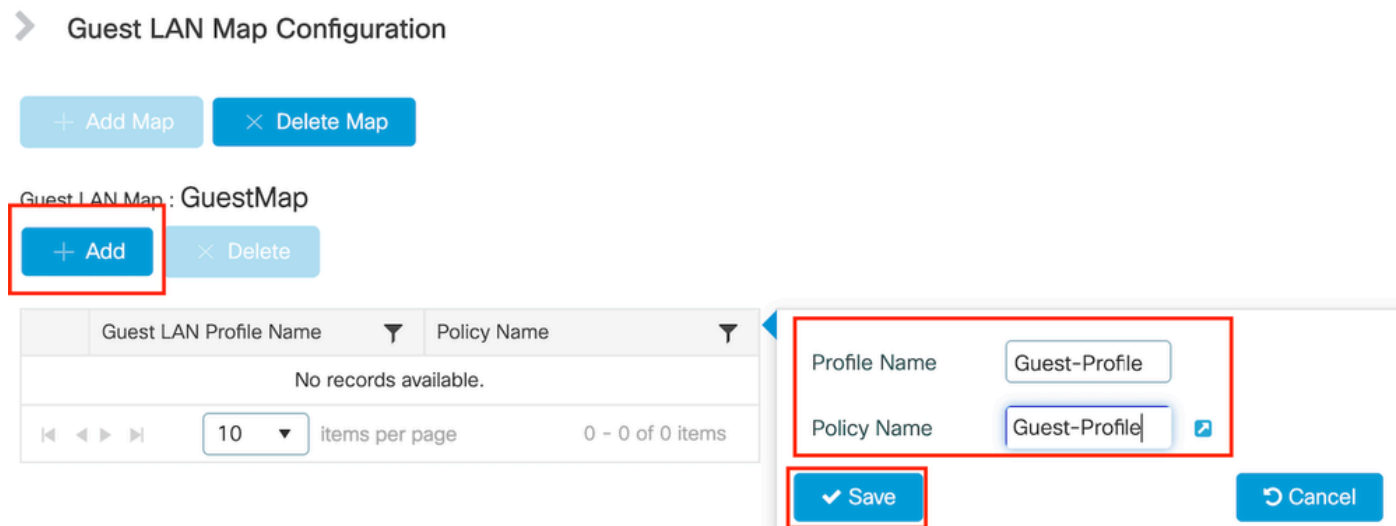
Configuración de CLI

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

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

MAPA LAN de invitado

Paso 1: Vaya a Configuration > Wireless > Guest LAN. En la sección de configuración Guest LAN MAP, seleccione Add y asigne el perfil de política al perfil de LAN de invitado.



MAPA LAN de invitado

Verificación

Validar configuración del controlador

```
#show guest-lan summary
```

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 <nombre de perfil> (Si se utiliza un perfil de parámetro web personalizado)

#show wireless guest-lan-map summary

GLAN Profile Name	Policy Name
Guest	Guest

Resumen de movilidad inalámbrica de #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
```

Validar estado de directiva de cliente

En Extranjero,

#show wireless client summary

El estado del administrador de directivas de cliente en el controlador externo es EJECUTADO después de que el cliente se asocie correctamente.

<#root>

MAC Address	AP Name	Type ID	State	Protocol	Method
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

```

En anclaje,

La transición del estado del cliente se debe supervisar en el controlador de anclaje.

El estado del administrador de políticas de cliente está pendiente de autenticación 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

Una vez que el cliente se autentica, el estado del administrador de políticas pasa al estado RUN.

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

#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 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

El cliente pasa al estado EJECUCIÓN después de una autenticación web correcta.

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

Después de la autenticación, el cliente pasa al estado RUN.

<#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

Troubleshoot

debug del controlador AireOS

Habilitar depuración de cliente

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

Para comprobar si la depuración está habilitada

```
>show debugging
```

Para deshabilitar la depuración

```
debug disable-all
```

9800 Seguimiento radioactivo

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

Pasos para habilitar el seguimiento radioactivo:

Asegúrese de que todas las depuraciones condicionales estén inhabilitadas.

```
clear platform condition all
```

Habilite debug para la dirección MAC especificada.

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

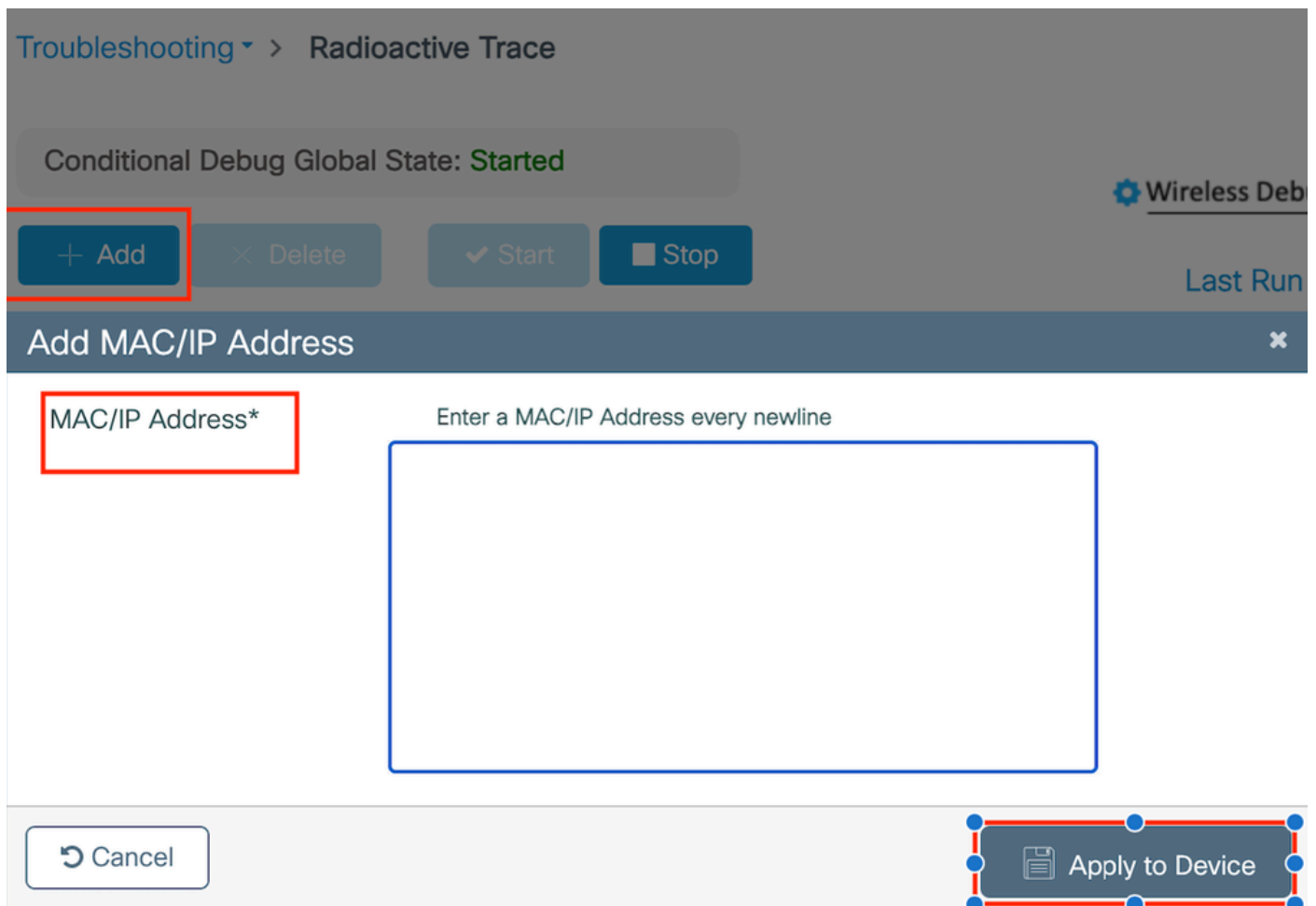
Copie el archivo en un servidor externo.

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

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,



Habilitar el seguimiento de RA en WebUI

Captura de paquetes integrada

Vaya a Troubleshooting > Packet Capture. 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.

Troubleshooting > Packet Capture

+ Add × Delete

Create Packet Capture ✕

Capture Name*

Filter*

Monitor Control Plane





Inner Filter Protocol DHCP

Inner Filter MAC


Buffer Size (MB)*

Limit by* secs == 1.00 hour

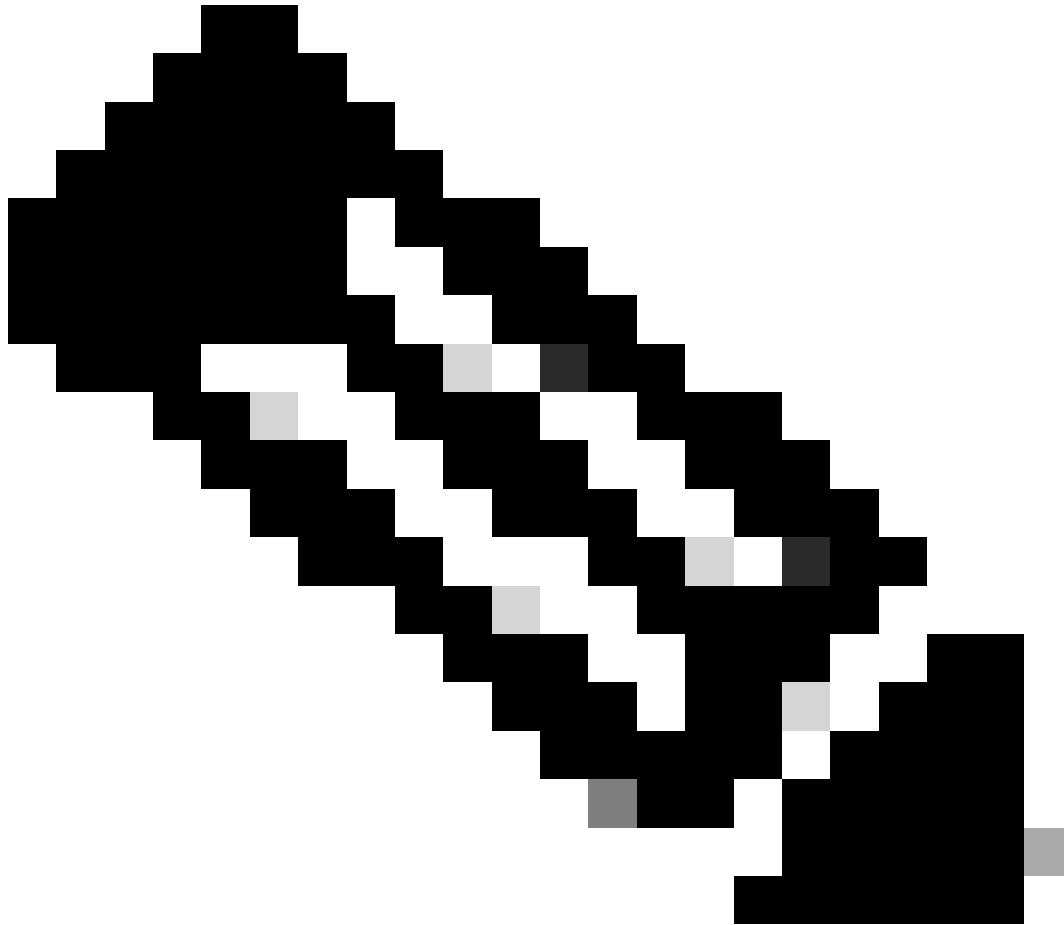
Available (12)

 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.

Navegue hasta Troubleshooting > Packet Capture y seleccione Start para capturar paquetes.

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

Iniciar captura de paquetes

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
```

<Reproduce the issue>

```
monitor capture TestPCap stop
```

```
show monitor capture TestPCap
```

Status Information for Capture TestPCap

Target Type:

Interface: TwoGigabitEthernet0/0/0, Direction: BOTH

Status : Inactive

Filter Details:

Capture all packets

Inner Filter Details:

Mac: 6c7e.67e3.6db9

Continuous capture: disabled

Buffer Details:

Buffer Type: LINEAR (default)

Buffer Size (in MB): 100

Limit Details:

Number of Packets to capture: 0 (no limit)

Packet Capture duration: 3600

Packet Size to capture: 0 (no limit)

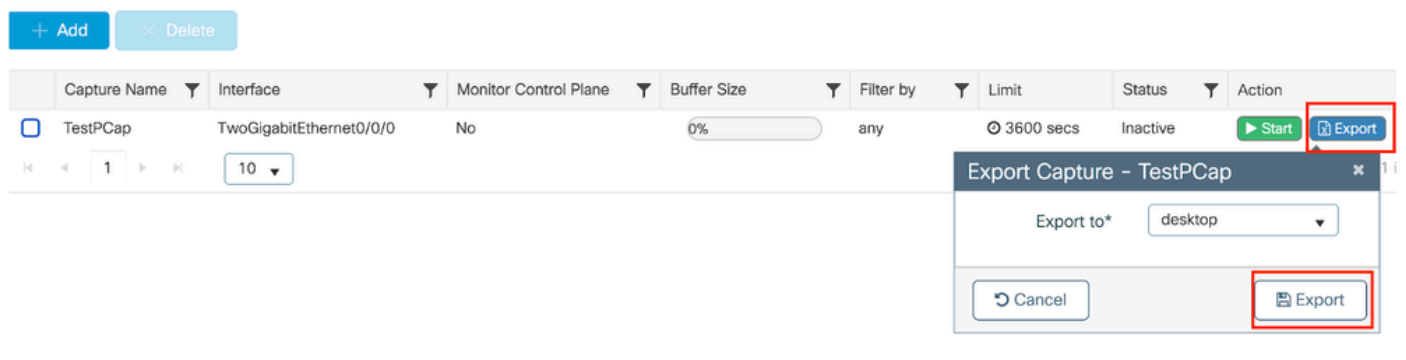
Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

Exportar captura de paquetes al servidor TFTP externo.

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

Navegue hasta Troubleshooting > Packet Capture y seleccione Export para descargar el archivo de captura en la máquina local.



Descargar EPC

Fragmentos de registro de trabajo

Registro de depuración del cliente del controlador externo AireOS

Paquete cableado recibido del cliente cableado

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

Solicitud de anclaje de exportación de edificio de controlador externo

*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

El controlador externo envía la solicitud de anclaje de exportación al controlador de anclaje.

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

El controlador de anclaje envía el reconocimiento de la solicitud de anclaje para el cliente

*Dot1x_NW_MsgTask_5: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Recvd Exp Anchor Ack for mobile a0:ce:c8:c3:

La función de movilidad para los clientes en el controlador externo se actualiza para exportar el controlador externo.

*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

El cliente pasó al estado de EJECUCIÓN.

*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 Rastreo radiactivo del controlador externo

El cliente se asocia al controlador.

2024/07/15 04:10:29.087608331 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

El descubrimiento de movilidad está en curso tras la asociación.

2024/07/15 04:10:29.091585813 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

2024/07/15 04:10:29.091605761 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

Una vez que se procesa la detección de movilidad, el tipo de itinerancia del cliente se actualiza a L3 solicitado.

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

El controlador externo está enviando la solicitud de anclaje de exportación al WLC de anclaje.

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 respuesta de anclaje de exportación se recibe del controlador de anclaje y la vlan se aplica desde el perfil de usuario.

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:

Una vez que se procesa la solicitud de anclaje de exportación, la función de movilidad del cliente se actualiza a Exportar a externo.

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

El cliente pasa al estado de aprendizaje de IP.

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

Después de aprender de IP, el cliente se mueve al estado RUN en el WLC extranjero.

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

Registro de depuración del cliente del controlador AireOS Anchor

Solicitud de anclaje de exportación recuperada del controlador externo.

```
*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
```

La VLAN de puente local se aplica para el cliente.

```
*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
```

El rol de movilidad se actualiza para exportar el anclaje y el estado del cliente asociado con transición.

```
*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 mer
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv (mm_listen.c:7933) Changi
```

La movilidad se ha completado, el estado del cliente está asociado y la función de movilidad es Export Anchor.

*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

La dirección IP del cliente se aprende en el controlador y el estado pasa de DHCP requerido a Web auth requerido.

*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

La URL de Webauth se está formulando agregando la URL de redirección externa y la dirección IP virtual del controlador.

*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://

Se añadió la dirección MAC y WLAN del cliente a la 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 final después de parquear el HTTP GET para el host 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.

La URL de redirección se envía al cliente en el paquete de respuesta 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

El cliente establece una conexión TCP con el host de URL de redirección. Una vez que los clientes envían el nombre de usuario y la contraseña de inicio de sesión en el portal, el controlador envía una solicitud RADIUS al servidor RADIUS

Una vez que el controlador recibe una aceptación de acceso, el cliente cierra la sesión TCP y pasa al estado 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 Anchor controller radioactivo trace

Mensaje de anuncio de movilidad para el cliente desde el controlador externo.

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

Solicitud de anclaje de exportación recibida del controlador externo cuando el cliente se asocia para la cual el controlador de anclaje envía una respuesta de anclaje de exportación que se puede verificar en el seguimiento de RA del controlador externo.

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

El cliente pasa al estado de asociación y la función de movilidad pasa al anclaje de exportación.

```
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
```

Se ha completado el aprendizaje de IP, se ha aprendido la IP del cliente a través de 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
```

El estado de la política del cliente está pendiente de autenticación web.

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

El protocolo de enlace TCP está suplantado por el controlador. Cuando el cliente envía un HTTP GET, se envía una trama de respuesta 200 OK que contiene la URL de redirección.

El cliente debe establecer un protocolo de enlace TCP con la URL de redirección y cargar la página.

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

Cuando el cliente envía las credenciales de inicio de sesión en la página del portal web, se envía un paquete de solicitud de acceso al servidor RADIUS para la autenticación.

```
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 se recibe del servidor RADIUS, webauth es exitoso.

```
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
```

La autenticación es satisfactoria y el estado de la política del cliente es RUN.

```
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
```

Análisis de captura de paquetes integrado

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

> Frame 806: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits)
> Ethernet II, Src: Cisco_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco_34:90:cb (6c:5e:3b:34:90:cb)
> Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.76.6.156
> User Datagram Protocol, Src Port: 16667, Dst Port: 16667
> Control And Provisioning of Wireless Access Points - Data
> Ethernet II, Src: Cisco_34:90:d4 (6c:5e:3b:34:90:d4), Dst: CeLink_c3:a9:b5 (a0:ce:c8:c3:a9:b5)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4095
> Internet Protocol Version 4, Src: 10.105.211.1, Dst: 10.105.211.69
> Transmission Control Protocol, Src Port: 80, Dst Port: 54351, Seq: 1, Ack: 108, Len: 743
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Location: http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://10.105.211.1/auth/discovery?architecture=9\r\n
Content-Type: text/html\r\n
> Content-Length: 527\r\n\r\n\r\n[HTTP response 1/1]
[Time since request: 0.000000000 seconds]
[Request in frame: 804]
[Request URI: http://10.105.211.1/auth/discovery?architecture=9]
File Data: 527 bytes

El cliente se redirige a la página del portal

La sesión se cierra después de recibir la URL de redirección.

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

La sesión TCP se cierra después de recibir la URL de redirección

El cliente inicia el protocolo de enlace de 3 vías TCP al host de URL de redirección y envía una solicitud GET HTTP.

Una vez que se carga la página, las credenciales de inicio de sesión se envían al portal, el controlador envía una solicitud de acceso al servidor RADIUS para autenticar al cliente.

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

Artículo relacionado

[Configuración de la función de movilidad de anclaje WLAN en Catalyst 9800](#)

[Ejemplo de Configuración de Wired Guest Access Using AireOS Controllers](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).