

# Configurar, verificar e solucionar problemas de convidado com fio no controlador de LAN sem fio

## Contents

---

---

## Introdução

Este documento descreve como configurar, verificar e solucionar problemas de acesso de convidado com fio no 9800 e no IRCM com autenticação da Web externa.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

WLC 9800

WLC AireOS

Túnel de mobilidade

ISE

Supõe-se que um túnel de mobilidade entre as duas WLCs tenha sido estabelecido antes da configuração do acesso de convidado com fio.

Este aspecto está fora do escopo deste exemplo de configuração. Para obter instruções detalhadas, consulte o documento anexo intitulado [Configurando topologias de mobilidade no 9800](#)

### Componentes Utilizados

9800 WLC versão 17.12.1

5520 WLC versão 8.10.185.0

ISE versão 3.1.0.518

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

## Configurar convidado com fio no Catalyst 9800 ancorado em outro Catalyst 9800

Diagrama de Rede



Topologia de rede

## Configuração em WLC 9800 externa

Configurar mapa de parâmetros da Web

Etapa 1: Navegue até Configuration > Security > Web Auth, selecione Global, verifique o endereço IP virtual do controlador e o mapeamento de pontos confiáveis e verifique se o tipo está definido como webauth.

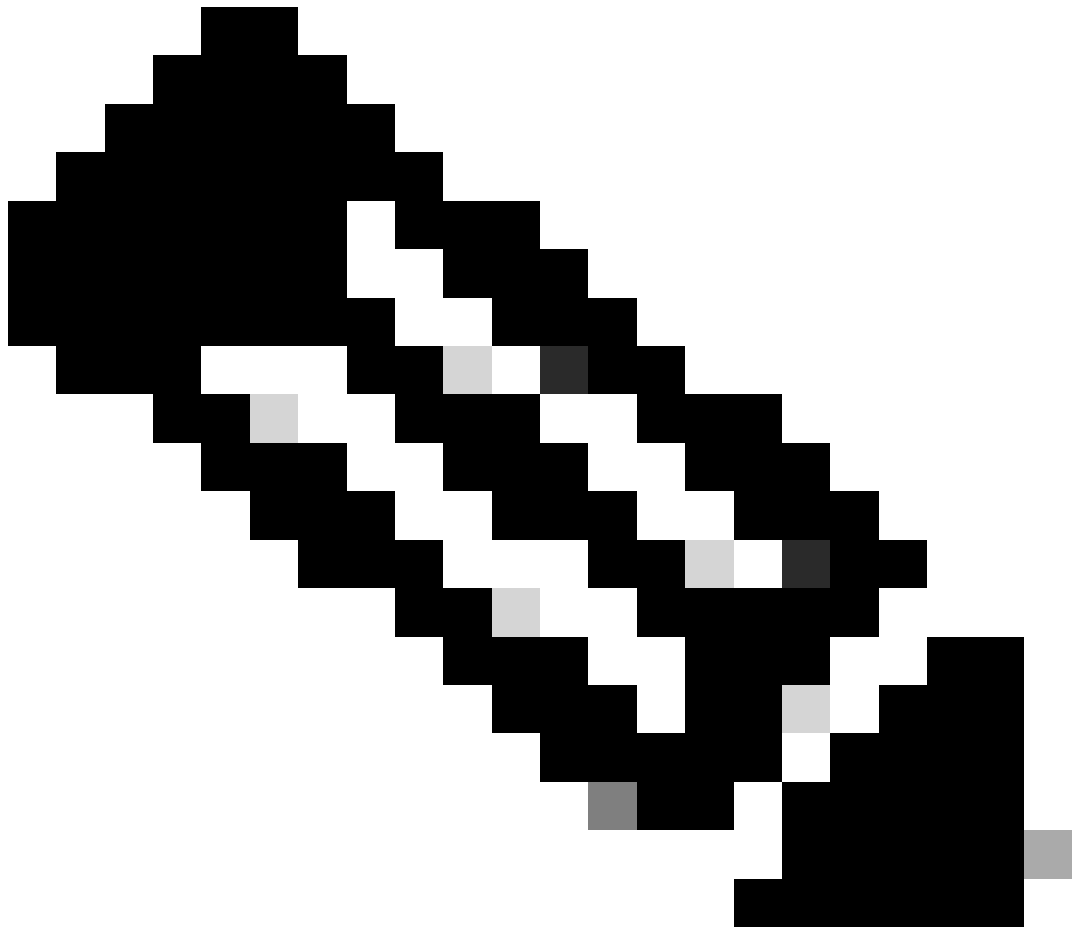
Configuration > Security > Web Auth

**Edit Web Auth Parameter**

**General**    Advanced

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

Mapa de parâmetros globais



Observação: a interceptação de Web Auth HTTPs é uma configuração opcional. Se o redirecionamento de HTTPS for necessário, a opção HTTPS de interceptação de Autenticação da Web deverá ser habilitada. No entanto, essa configuração não é recomendada, pois aumenta o uso da CPU.

Etapa 2: Na guia Avançado, configure o URL da página da Web externa para o redirecionamento do cliente. Defina "Redirect URL for Login" e "Redirect On-Failure"; "Redirect On-Success" é opcional. Depois de configurada, uma visualização da URL de redirecionamento é exibida no perfil Web Auth.

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

Guia Avançado

## Configuração 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

Observação: neste cenário, o mapa de parâmetros globais é usado. De acordo com o requisito, configure um mapa de parâmetros da Web personalizado selecionando Adicionar e, defina o URL de redirecionamento na guia Avançado. As configurações de Ponto de Confiança e IP Virtual são herdadas do perfil global.

## Configurações de AAA:

Etapa 1: Crie um servidor Radius:

Navegue para Configuration > Security > AAA, clique em "Add" na seção Server/Group e, na página "Create AAA Radius Server", insira o nome do servidor, o endereço IP e o segredo compartilhado.

The screenshot displays the 'Create AAA Radius Server' configuration window. The interface includes a breadcrumb trail: Configuration > Security > AAA. A '+ AAA Wizard' button is present at the top left. Below the breadcrumb, there are tabs for 'Servers / Groups', 'AAA Method List', and 'AAA Advanced'. The 'Servers / Groups' tab is active, and within it, the 'Servers' sub-tab is selected. A '+ Add' button is highlighted with a red box. The main configuration area contains the following fields and controls:

- Name\***: Text input field.
- Server Address\***: Text input field with a dropdown menu showing 'IPv4/IPv6/Hostname'.
- PAC Key**: Checkable field, currently unchecked.
- Key Type**: Dropdown menu with 'Clear Text' selected.
- Key\***: Text input field.
- Confirm Key\***: Text input field.
- Auth Port**: Text input field with '1812' entered.
- Acct Port**: Text input field with '1813' entered.
- Server Timeout (seconds)**: Text input field with '1-1000' entered.
- Retry Count**: Text input field with '0-100' entered.
- Support for CoA**: Checkable field, currently checked and labeled 'ENABLED'.
- CoA Server Key Type**: Dropdown menu with 'Clear Text' selected.
- CoA Server Key**: Text input field.
- Confirm CoA Server Key**: Text input field.
- Automate Tester**: Checkable field, currently unchecked.

At the bottom of the window, there is a 'Cancel' button on the left and an 'Apply to Device' button on the right.

Configuração de servidor RADIUS

## Configuração de CLI

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

Etapa 2: Crie um grupo de servidores RADIUS:

Selecione "Adicionar" na seção Grupos de servidores para definir um grupo de servidores e alternar os servidores a serem incluídos na configuração do 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

## Configuração de CLI

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

Etapa 3: Configure a lista de métodos AAA:

Navegue até a guia AAA Method List (Lista de métodos AAA), selecione Add (Adicionar) em Authentication (Autenticação), defina um nome de lista de métodos com Type (Tipo) como "login" (login) e Group type (Tipo de grupo) como "Group" (Grupo) e mapeie o grupo de servidores de autenticação configurado na seção Assigned Server Group (Grupo de servidores atribuídos).

The screenshot shows the Cisco configuration interface for AAA Method List. The breadcrumb navigation is Configuration > Security > AAA. The main menu includes Servers / Groups, AAA Method List (highlighted with a red box), and AAA Advanced. The left sidebar has Authentication (highlighted with a red box), Authorization, and Accounting. The main content area is titled 'Quick Setup: AAA Authentication' and contains the following fields:

- Method List Name\*: ISE-List (highlighted with a red box)
- Type\*: login (highlighted with a red box)
- Group Type: group (highlighted with a red box)
- Fallback to local:
- Available Server Groups: A list of server groups including tacacs, undefined, Radius-Group, Test-group, test-group, undefined, and tacacs1.
- Assigned Server Groups: A list containing ISE-Group (highlighted with a red box).

Lista de métodos de autenticação

## Configuração de CLI

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

## Configurar perfil de Diretiva

Etapa 1: Navegue até Configuration > Tags & Profiles > Policy, nomeie seu novo perfil na guia General e ative-o usando a alternância de status.

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 da política

Etapa 2: na guia Access Policies, atribua uma vlan aleatória quando o mapeamento da vlan for concluído no controlador âncora. Neste exemplo, a vlan 1 está configurada



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

Guia Política de acesso

Etapa 3: Na guia Mobility, alterne o controlador Anchor para Primary (1) e, opcionalmente, configure os túneis de mobilidade Secondary (Secundária) e Tertiary (Terciária) para requisitos de redundância

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
<ul style="list-style-type: none"> <li> 10.106.40.11 →</li> <li> 10.76.118.75 →</li> <li> 10.76.118.74 →</li> </ul>	<ul style="list-style-type: none"> <li> 10.76.118.70 Primary (1) ←</li> </ul>

Mapa de mobilidade

Configuração de CLI

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

## Configurar perfil de LAN de convidado

Etapa 1: Navegue até Configuration > Wireless > Guest LAN, selecione Add, configure um nome de perfil exclusivo, habilite a VLAN com fio, insira o ID da VLAN para usuários convidados com fio e alterne o status do perfil para Enabled.

General	Security
Profile Name*	Client Association Limit
Guest LAN ID*	Wired VLAN Status
mDNS Mode	Wired VLAN ID*
Status	

Guest-Profile

2000

1

ENABLE

Bridging

2024

ENABLE

Perfil de LAN de convidado

Etapa 2: na guia Segurança, ative a Autenticação da Web, mapeie o mapa do parâmetro Autenticação da Web e selecione o servidor Radius na lista suspensa Autenticação.

# Edit Guest LAN Profile

General

**Security**

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List



Guia Segurança de LAN de convidado

## Configuração 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
```

## MAP de LAN de convidado

Navegue até Configuration > Wireless > Guest LAN.

Na seção de configuração Guest LAN MAP, selecione Add e mapeie o perfil Policy e o perfil 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

MAP de LAN de convidado

## Configuração de CLI

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

## Configuração na WLC Anchor 9800

### Configurar mapa de parâmetros da Web

Etapa 1: Navegue até Configuration > Security > Web Auth, selecione Global, verifique o endereço IP virtual do controlador e o mapeamento de pontos confiáveis e verifique se o tipo está definido como webauth.

Configuration > Security > Web Auth

+ Add   × Delete

Parameter Map Name

- global
- Web-Filter

1   10

### Edit Web Auth Parameter

General   Advanced

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

Etapa 2: Na guia Avançado, configure o URL da página da Web externa para o redirecionamento do cliente. Defina "Redirect URL for Login" e "Redirect On-Failure"; "Redirect On-Success" é opcional.

Depois de configurada, uma visualização da URL de redirecionamento é exibida no perfil Web Auth.

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	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	x::x::x::x

## Configuração 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
```

## Configurações de AAA:

Etapa 1: Crie um servidor Radius:

Navegue para Configuration > Security > AAA, clique em Add na seção Server/Group e, na página "Create AAA Radius Server", insira o nome do servidor, o endereço IP e o segredo compartilhado.

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

Configuração de servidor RADIUS

## Configuração de CLI

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

Etapa 2: Crie um grupo de servidores RADIUS:

Selecione Add na seção Server Groups para definir um grupo de servidores e alternar os servidores a serem incluídos na configuração do grupo.

Name*	ISE-Group
Group Type	RADIUS

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

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

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

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

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

Available Servers

Assigned Servers

--



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

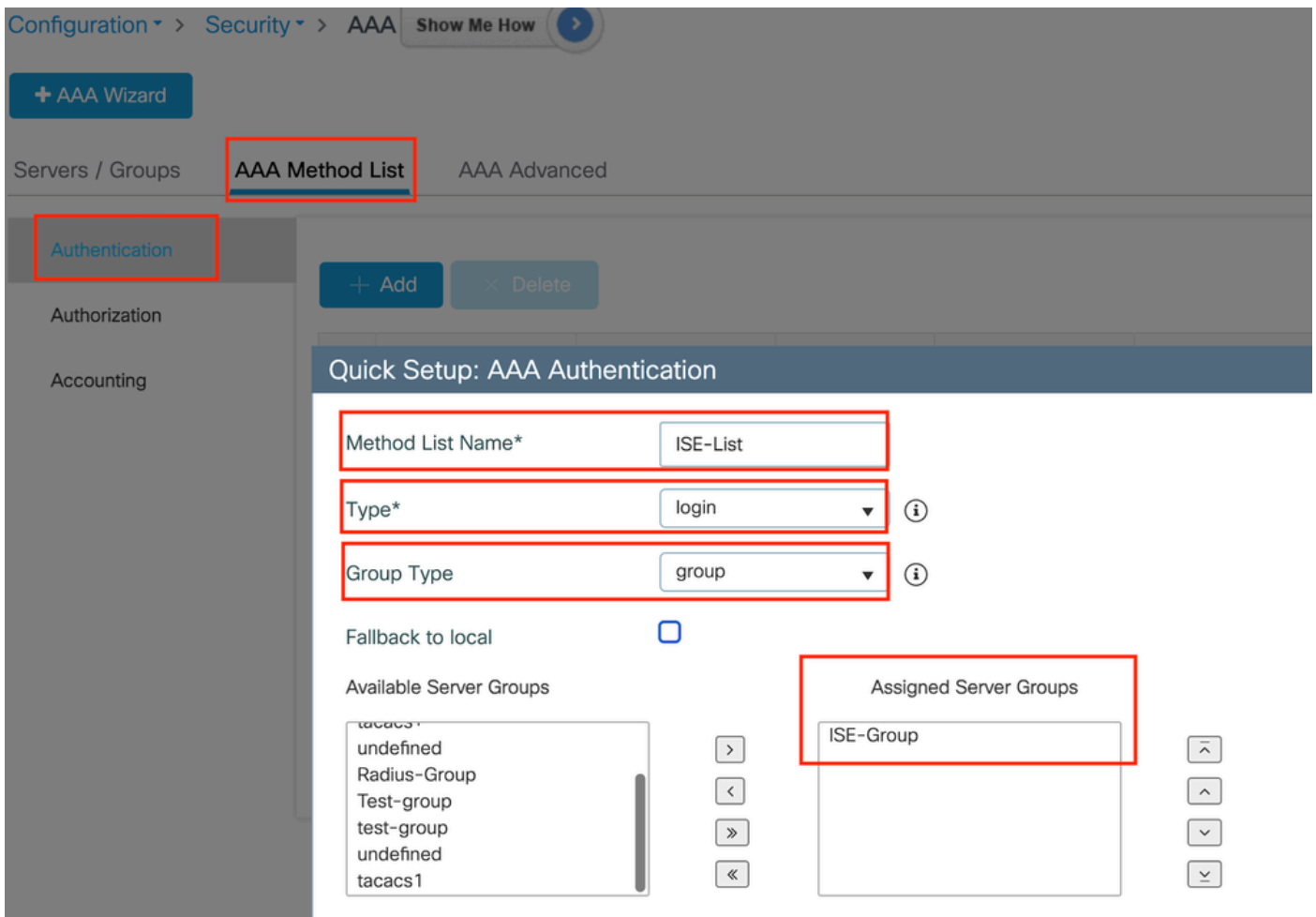
Grupo de raio de âncora

### Configuração de CLI

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

Etapa 3: Configure a lista de métodos AAA:

Navegue até a guia AAA Method List, selecione Add em Authentication, defina um nome de lista de métodos com Type como "login" e Group type como "Group" e mapeie o grupo de servidores de autenticação configurado na seção Assigned Server Group.



Lista de métodos de autenticação

## Configuração de CLI

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

## Configurar perfil de Diretiva

Etapa 1: Navegue até Configuration > Tag & Profiles > Policy, configure o perfil de política com o mesmo nome do controlador externo e habilite o 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 âncora

Etapa 2: nas Políticas de acesso, mapeie a vlan do cliente com fio na lista suspensa

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

### WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select

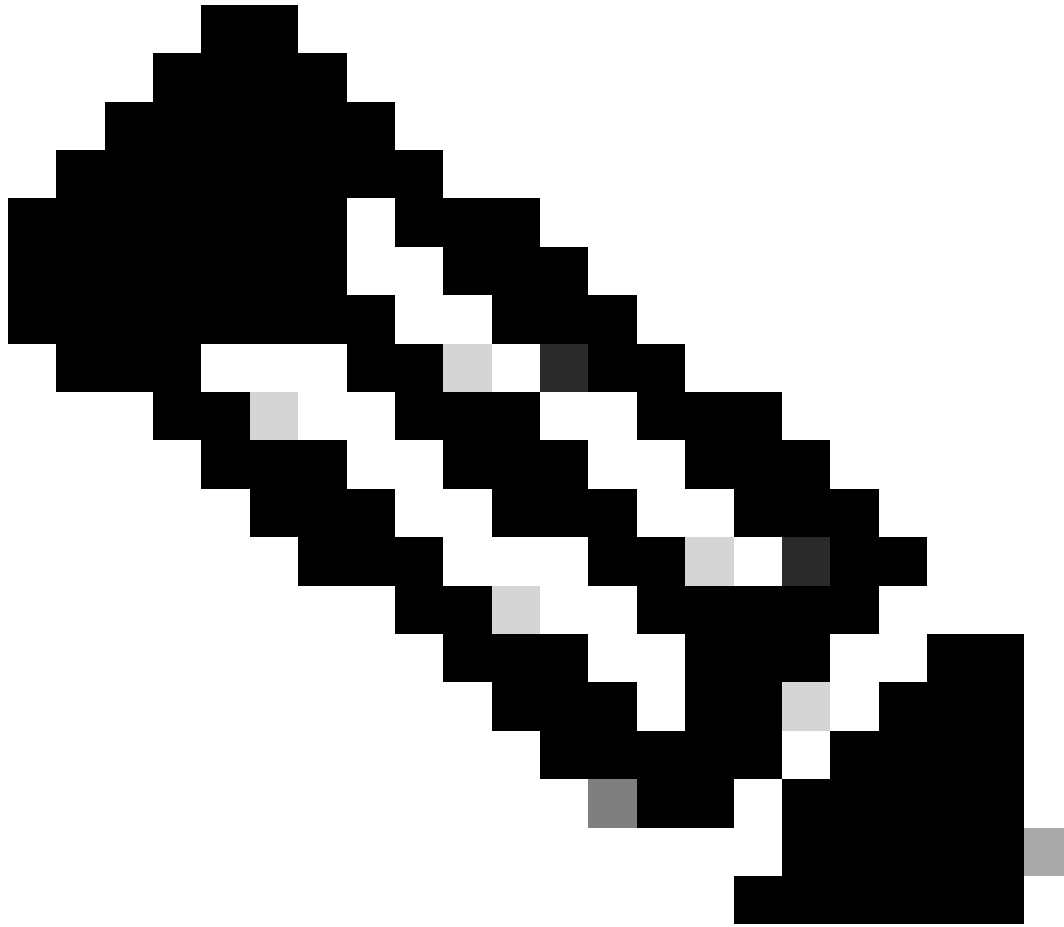


### VLAN

VLAN/VLAN Group

VLAN2024





Observação: a configuração do perfil de política deve corresponder nos controladores Externo e Âncora, exceto na VLAN.

---

Etapa 3: Na guia Mobility, marque a caixa 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)

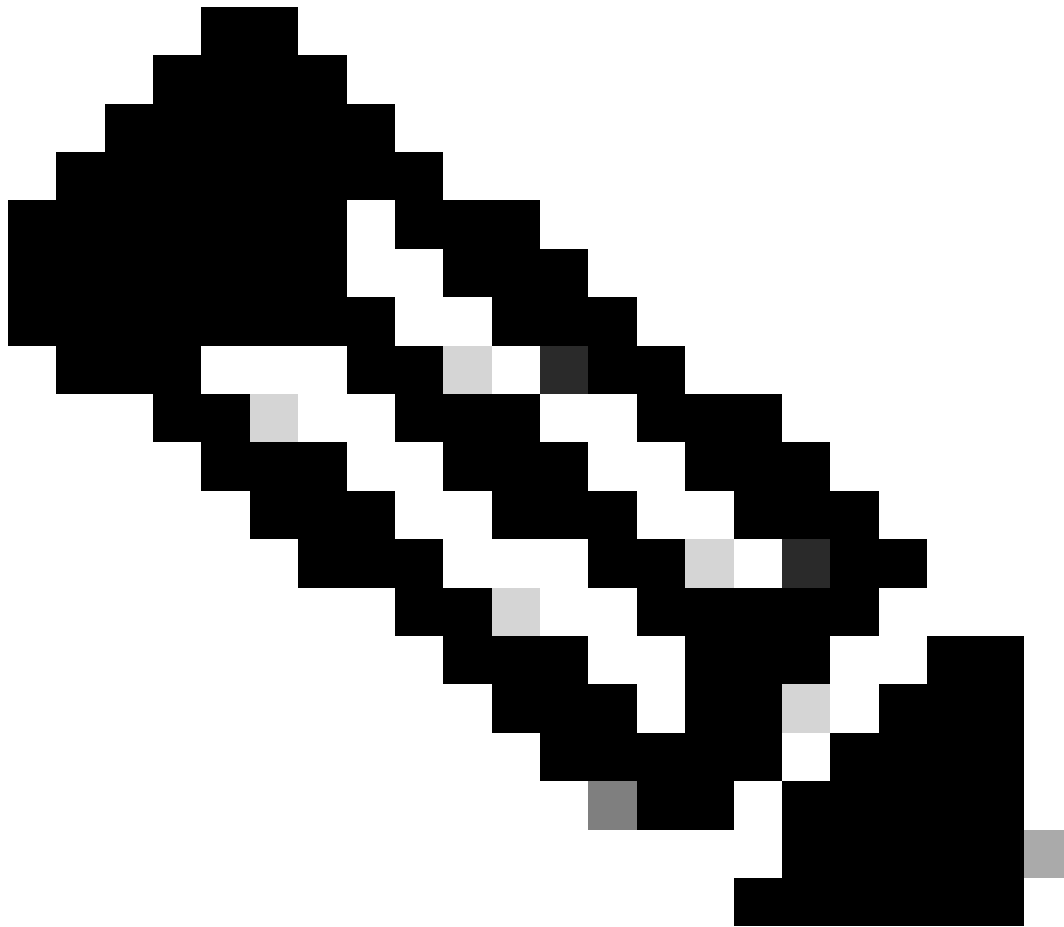
Selected (0)

Anchor IP

Anchor IP

Anchor IP

Exportar Ancora



Observação: essa configuração designa a controladora Wireless LAN (WLC) 9800 como a WLC âncora para qualquer WLAN associada ao perfil de política especificado. Quando uma WLC 9800 externa redireciona clientes para a WLC âncora, ela fornece detalhes sobre a WLAN e o Perfil de política atribuído ao cliente. Isso permite que a WLC âncora aplique o perfil de política local apropriado com base nas informações recebidas.

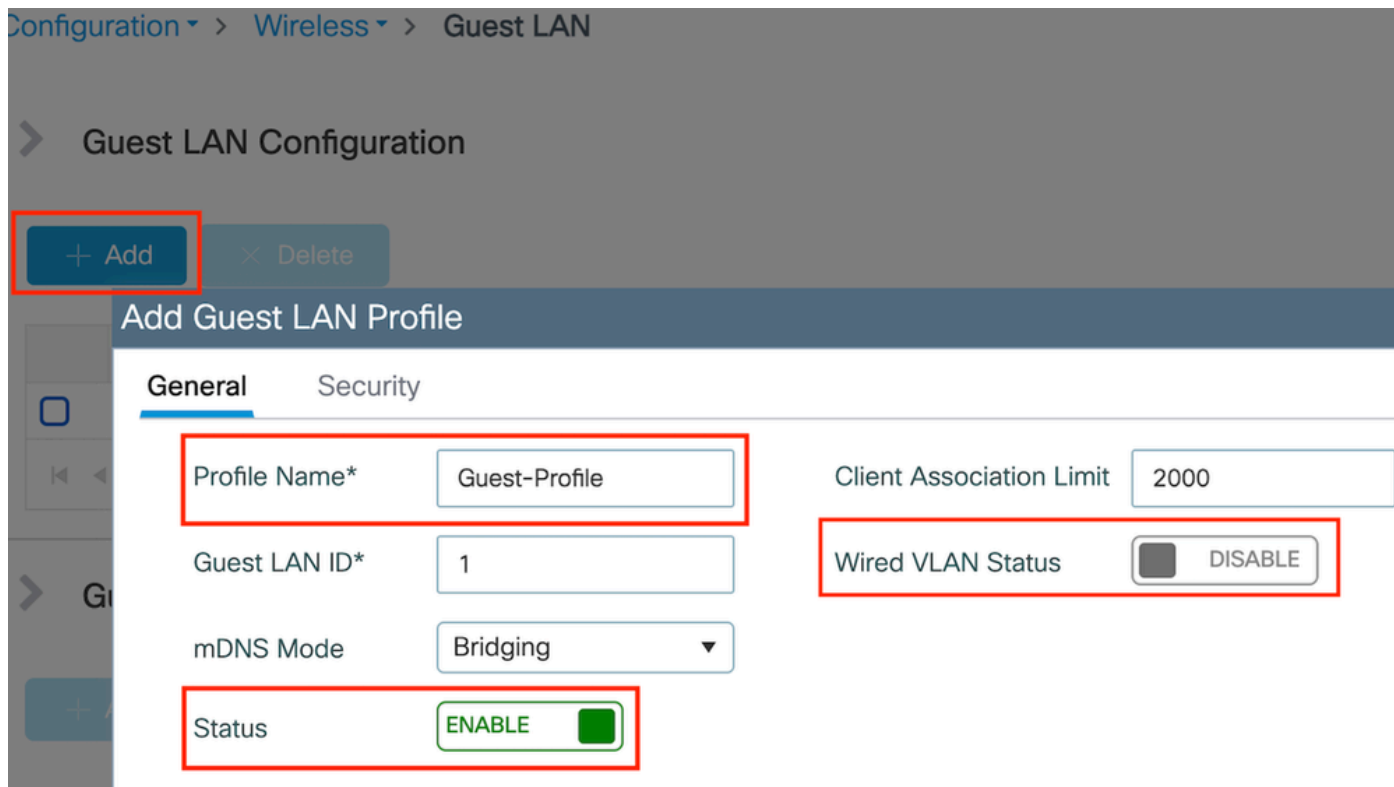
---

## Configuração de CLI

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

## Configurar perfil de LAN de convidado

Etapa 1: Navegue até Configuration > Wireless > Guest LAN e selecione Add para criar e configurar o perfil de LAN de convidado. Verifique se o nome do perfil corresponde ao do controlador externo. Observe que a VLAN com fio deve ser desativada no controlador Anchor.



Perfil de LAN de convidado

Etapa 2: nas configurações de segurança, habilite Web Auth e configure o mapa do parâmetro Web Auth e a Lista de autenticação.

## Edit Guest LAN Profile

General

**Security**

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

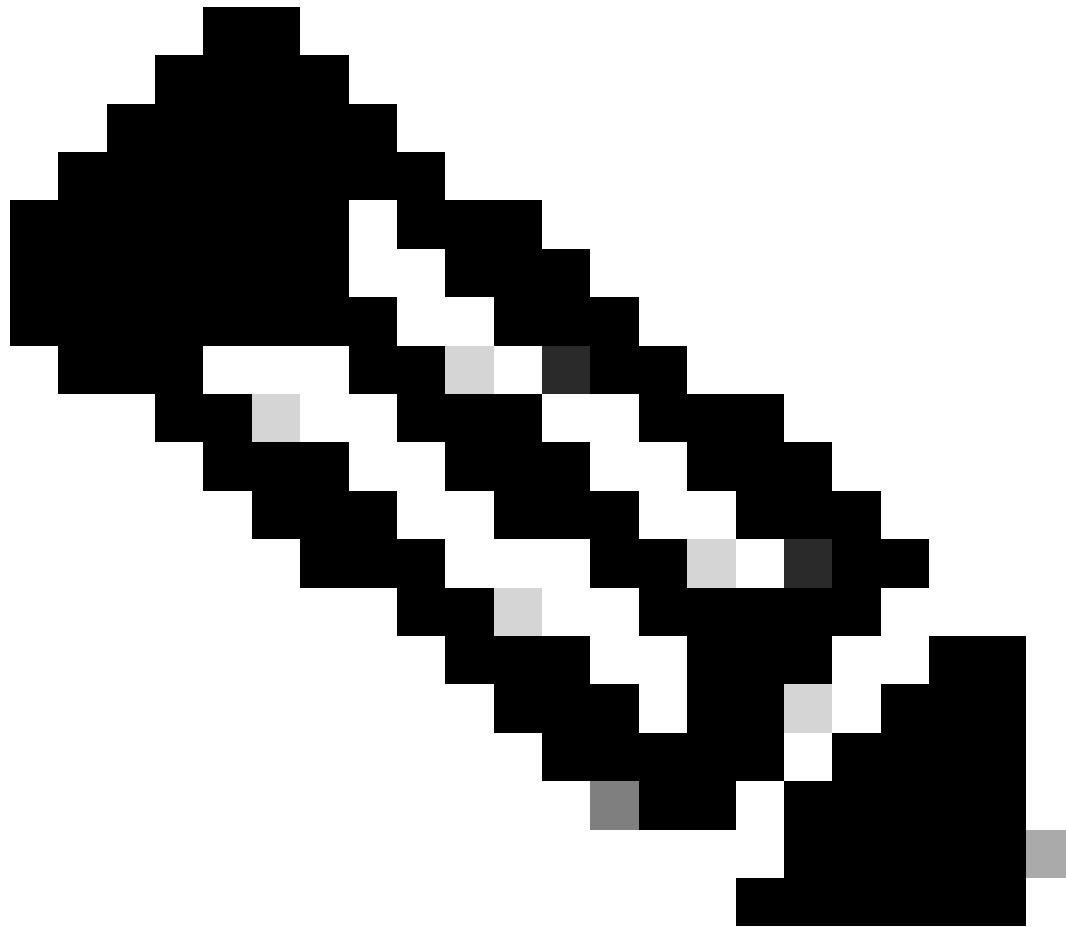
global



Authentication List

ISE-List





Observação: a configuração do perfil de LAN de convidado deve ser idêntica entre os controladores Foreign e Anchor, exceto para o status da VLAN com fio

---

## Configuração de CLI

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

## MAP de LAN de convidado

Etapa 1: Navegue até Configuration > Wireless > Guest LAN. Na seção de configuração Guest LAN MAP, selecione Add e mapeie o perfil de política para o 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

MAP de LAN de convidado

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

## Configurar convidado com fio no Catalyst 9800 ancorado no controlador AireOS 5520



Topologia de rede

## Configuração em WLC 9800 externa

## Configurar mapa de parâmetros da Web

Etapa 1: Navegue até Configuration > Security > Web Auth e selecione Global. Verifique se o endereço IP virtual do controlador e do ponto de confiança estão mapeados corretamente no perfil, com o tipo definido como webauth.

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

Mapa de Parâmetros da Web

Etapa 2: Na guia Avançado, especifique o URL da página da Web externa para o qual os clientes devem ser redirecionados. Configure a URL de redirecionamento para login e Redirecionar em caso de falha. A configuração Redirect On-Success é 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>

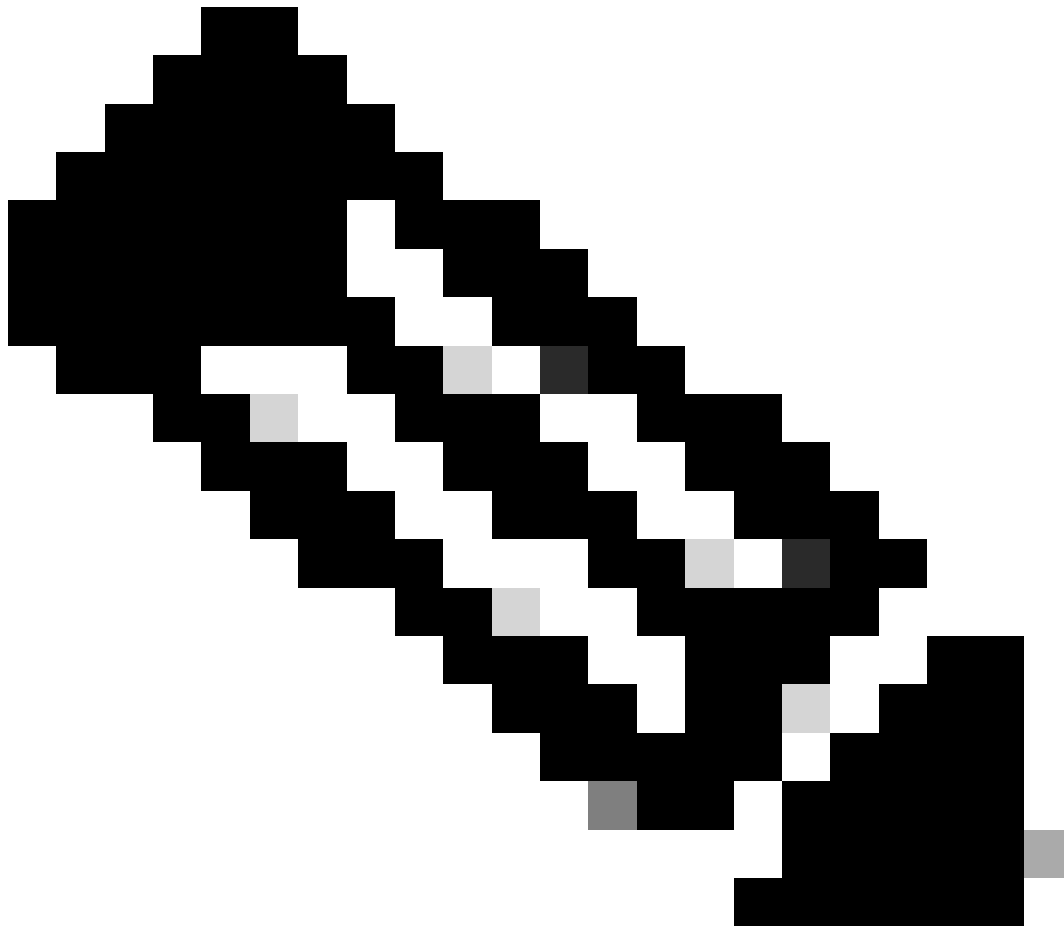
### Redirect to external server

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"/>

Guia Avançado

## Configuração 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
```



Observação: para a configuração AAA, consulte os detalhes de configuração fornecidos na seção "" para o WLC 9800 externo.

---

## Configurar perfil de Diretiva

Etapa 1: Navegue até Configuration > Tags & Profiles > Policy. Selecione Add e, na guia General, forneça um nome para o perfil e ative a alternância de status.

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 política

Etapa 2: Na guia Access Policies (Políticas de acesso), atribua uma VLAN aleatória.

General	<b>Access Policies</b>	QOS and AVC	Mobility	Advanced
RADIUS Profiling	<input type="checkbox"/>			
HTTP TLV Caching	<input type="checkbox"/>			
DHCP TLV Caching	<input type="checkbox"/>			
<b>WLAN Local Profiling</b>				
Global State of Device Classification		Disabled ⓘ		
Local Subscriber Policy Name		<input type="text" value="Search or Select"/>	▼	↗
<b>VLAN</b>				
VLAN/VLAN Group		<input type="text" value="1"/>	▼	ⓘ
Multicast VLAN		<input type="text" value="Enter Multicast VLAN"/>		

Políticas de acesso

Etapa 3: Na guia Mobility, alterne o controlador Anchor e defina sua prioridade como Primary (Primário) (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

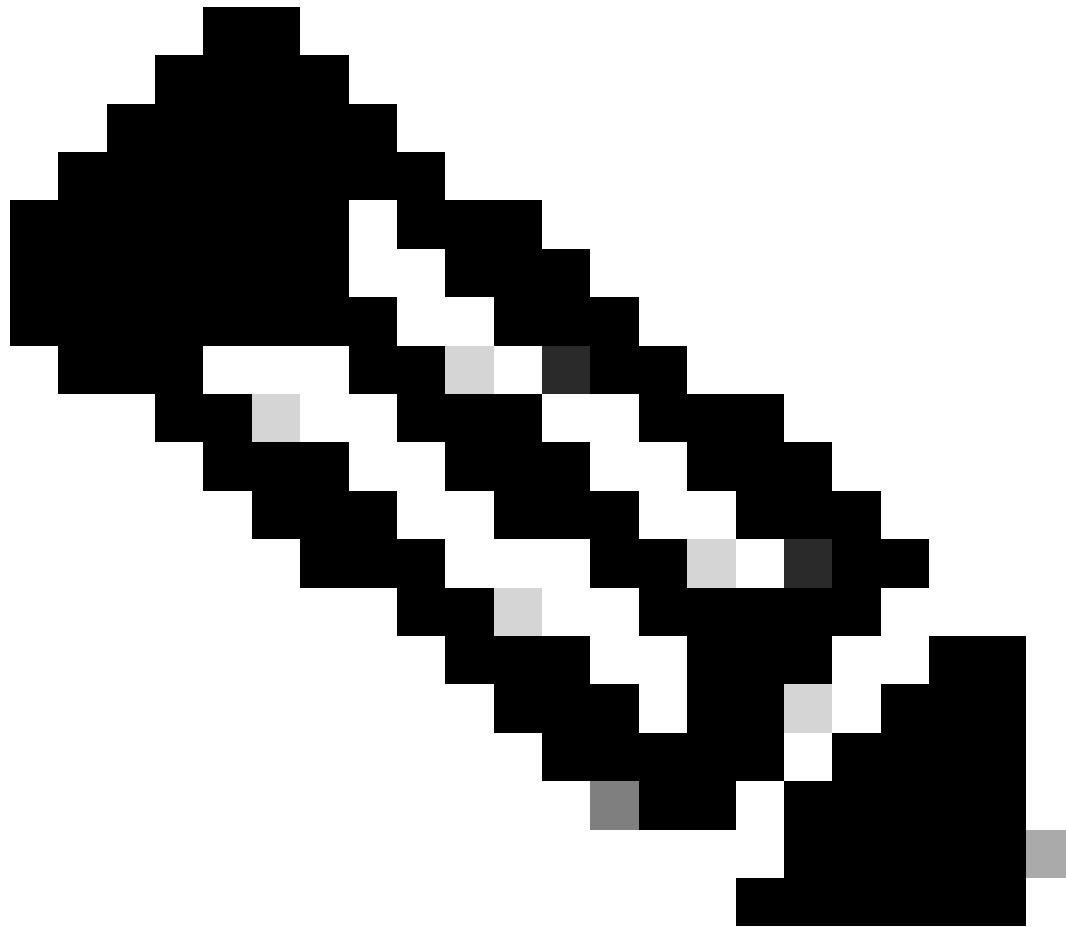
 10.76.6.156	→
---	---

#### Selected (1)

Anchor IP

Anchor Priority

 10.76.118.74	Primary (1) ▼
--	---------------



Observação: o perfil de política da 9800 Foreign WLC deve corresponder ao perfil de LAN de convidado da 5520 Anchor WLC, exceto para a configuração de vlan

---

## Configuração 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 convidado

Etapa 1: Navegue até Configuration > Wireless > Guest LAN e selecione Add. Configure um



nome de perfil exclusivo e habilite a VLAN com fio, especificando a ID da VLAN dedicada para usuários convidados com fio. Por fim, alterne o status do perfil para Enabled.

## 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 convidado

Etapa 2: Na guia Security, ative Web Auth, mapeie o mapa do parâmetro Web Auth e selecione o servidor RADIUS na lista suspensa Authentication.

## General

## Security

### Layer3

Web Auth

ENABLE

Web Auth Parameter Map

global

Authentication List

ISE-List

---

Observação: o nome do perfil de LAN de convidado deve ser o mesmo para a controladora 9800 Foreign e 5520 Anchor

---

## Configuração de CLI

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

## MAP de LAN de convidado

Etapa 1: Navegue até Configuration > Wireless > Guest LAN. Na seção de configuração Guest LAN MAP, selecione Add e mapeie o perfil de política para o perfil de LAN de convidado.

> 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

MAP de LAN de convidado

## Configuração de CLI

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

## Configuração em Anchor 5520 WLC

### Configurar Autenticação da Web

Etapa 1: Navegue até Segurança > Autenticação da Web > Página de login na Web. Defina o tipo de Autenticação da Web como Externa (Redirecionar para servidor externo) e configure a URL de Autenticação da Web externa. A opção Redirect URL after login é opcional e pode ser configurada se os clientes precisarem ser redirecionados para uma página dedicada após a autenticação bem-sucedida.

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

## Configurações de AAA:

Etapa 1: Configure o servidor radius

Navegue até Security > Radius > Authentication > New.



Servidor Radius

Etapa 2: Configure o IP do servidor RADIUS e o segredo compartilhado no controlador. Alterne o status do servidor para Enabled e marque a caixa de seleção Network User.

## RADIUS Authentication Servers > New

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

Configuração do servidor

### Configurar Lista de Controle de Acesso

Etapa 1: Navegue até Segurança > Lista de controle de acesso e selecione Novo. Crie uma ACL

de pré-autenticação que permita o tráfego para o DNS e o servidor Web externo.

The screenshot shows the Cisco Meraki Security interface. The 'SECURITY' tab is highlighted. On the left sidebar, 'Access Control Lists' is selected. The main area displays 'Access Control Lists > Edit' for the 'Pre-Auth\_ACL' list. A table lists six 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 acesso para permitir o tráfego para o servidor Web

## Configurar perfil de LAN de convidado

Etapa 1: Navegue até WLANs > selecione Create New .

Selecione Type como Guest LAN e configure o mesmo nome do perfil de política do controlador 9800 Foreign.

The screenshot shows the Cisco Meraki WLANs page. The 'WLANs' tab is selected. A 'Create New' button with a dropdown arrow and a 'Go' button are highlighted with a red box.

Criar LAN de Convidado

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

Perfil de LAN de convidado

Etapa 2: Mapeie as interfaces de entrada e saída no perfil da LAN de convidado.

Neste caso, a interface de entrada não é nenhuma porque a interface de entrada é o túnel EoIP

do controlador externo.

A interface de saída é a VLAN à qual o cliente com fio se conecta fisicamente .

The screenshot shows the 'Security' tab of a configuration page for a 'Guest' profile. The 'Profile Name' is 'Guest' and the 'Type' is 'Guest LAN'. The 'Status' is 'Enabled'. Under 'Security Policies', 'Web-Auth' is selected, with a note: '(Modifications done under security tab will appear after applying the changes.)'. The 'Ingress Interface' is set to 'None' and the 'Egress Interface' is set to 'wired-vlan-11'. The 'NAS-ID' is 'none'.

Perfil de LAN de convidado

Etapa 3: Na guia Segurança, selecione a segurança da camada 3 como Autenticação da Web e mapeie a ACL de pré-autenticação.

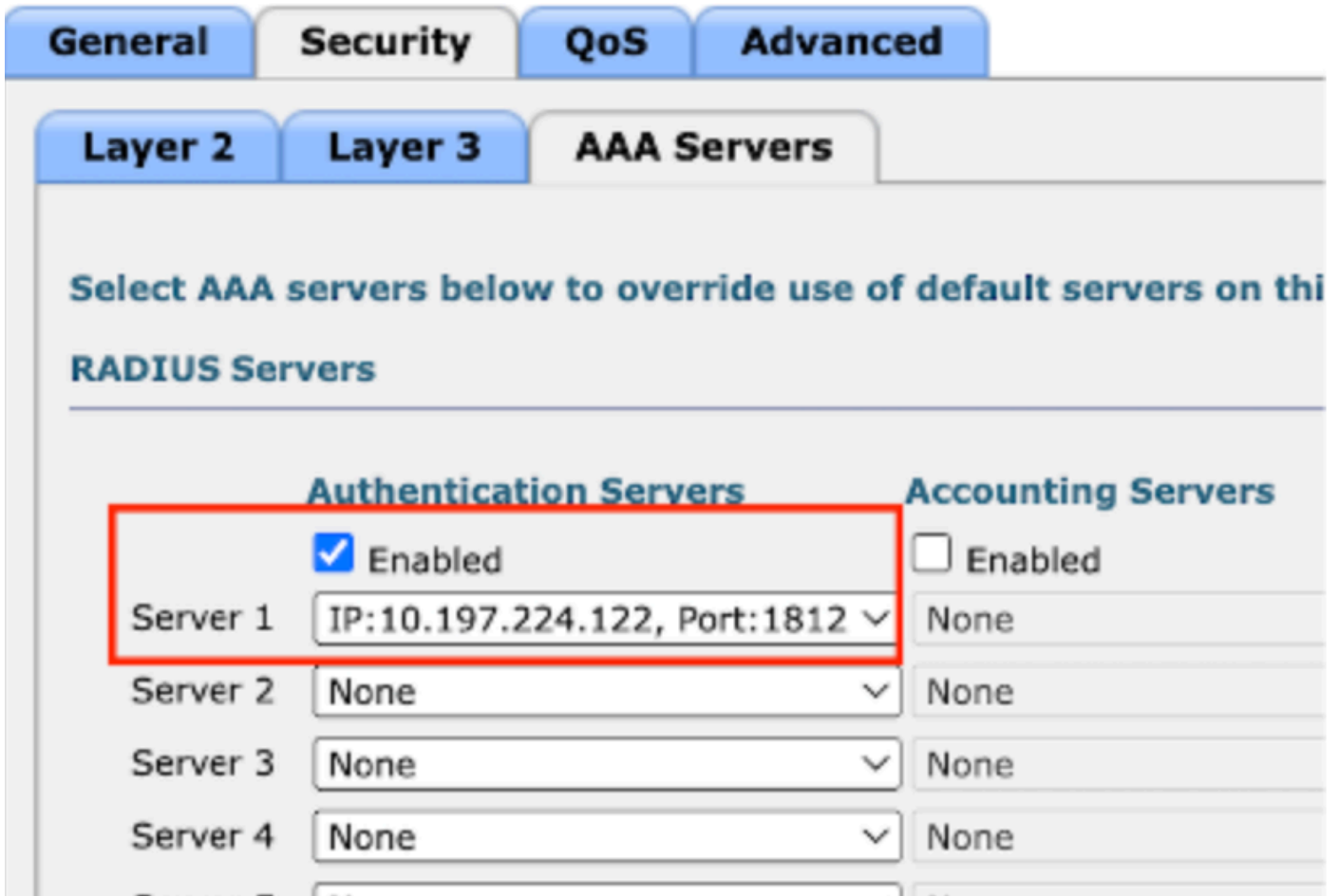
### WLANs > Edit 'Guest'

The screenshot shows the 'AAA Servers' tab of a configuration page for a 'Guest' profile. Under 'Layer 3 Security', 'Web Authentication' is selected. The 'Preauthentication ACL' is set to 'Pre-Auth\_ACL' for IPv4 and 'None' for IPv6. The 'Override Global Config' checkbox is unchecked.

Guia Segurança de LAN de convidado

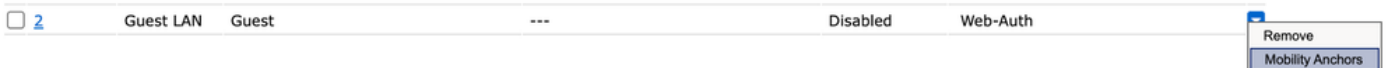
Etapa 4: Navegue até Security > AAA Server.

Selecione a lista suspensa e mapeie o servidor radius para o perfil de LAN de convidado.

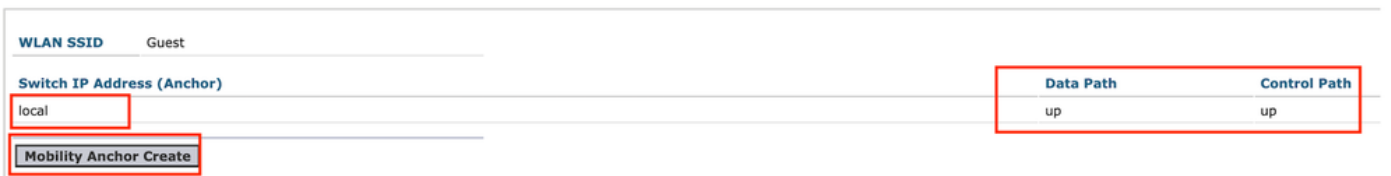


Mapear o servidor radius para o perfil de LAN do convidado

Etapa 5: Navegue até WLAN. Passe o mouse sobre o ícone suspenso do perfil de LAN de convidado e selecione Âncoras de mobilidade.



Etapa 6: Selecione Mobility Anchor Create para configurar o controlador como âncora de exportação para este perfil de LAN de convidado.



Criação de âncora de mobilidade

Configurar convidado com fio no AireOS 5520 ancorado no Catalyst 9800





Topologia de rede

## Configuração em WLC 5520 Externo

### Configuração da interface do controlador

Etapa 1: Navegue até Controller > Interfaces > New. Configure um nome de interface, ID de VLAN e ative a LAN de convidado.

O convidado com fio exige duas interfaces dinâmicas.

Primeiro, crie uma interface dinâmica de Camada 2 e designe-a como LAN de convidado. Essa interface serve como interface de entrada para a LAN de convidado, onde os clientes com fio se conectam fisicamente.

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 a red box. 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 set to 'none'.
- Physical Information:** Port Number is '1', Backup Port is '0', and Active Port is '1'.
- Interface Address:** VLAN Identifier is '2020' (highlighted in red), DHCP Proxy Mode is 'Global', and 'Enable DHCP Option 82' is unchecked.

Interface de entrada

Etapa 2: Navegue até Controller > Interfaces > New. Configure um nome de interface, ID de VLAN.

A segunda interface dinâmica deve ser uma interface de Camada 3 no controlador; os clientes com fio recebem o endereço IP dessa sub-rede vlan. Essa interface serve como interface de saída para o perfil de LAN de convidado.

Controller

General

Icons

Inventory

**Interfaces**

Interface Groups

Multicast

▶ Network Routes

▶ Fabric Configuration

▶ Redundancy

▶ Mobility Management

Ports

▶ NTP

▶ CDP

▶ PMIPv6

▶ Tunneling

▶ IPv6

▶ mDNS

▶ Advanced

Lawful Interception

Interfaces > Edit

General Information

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

Configuration

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

Physical Information

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

Interface Address

VLAN Identifier	2024
IP Address	10.105.211.85
Netmask	255.255.255.128
Gateway	10.105.211.1

Interface de saída

Configuração da porta do switch

Os usuários convidados com fio conectam-se ao switch da camada de acesso, essas portas designadas devem ser configuradas com uma VLAN na qual a LAN de convidado esteja habilitada no controlador

Configuração da porta do switch da camada de acesso

interface gigabitEthernet <x/x/x>

description Acesso para Convidado com Fio

```
switchport access vlan 2020
```

```
switchport mode access
```

```
fim
```

Configuração de porta de uplink de controlador externo

```
interface TenGigabitEthernet<x/x/x>
```

```
description Porta de tronco para a WLC externa
```

```
trunk de modo de porta de comutação
```

```
switchport trunk native vlan 2081
```

```
switchport trunk allowed vlan 2081,2020
```

```
fim
```

Configuração de porta de uplink do controlador de âncora

```
interface TenGigabitEthernet<x/x/x>
```

```
description Porta de tronco para a WLC âncora
```

```
trunk de modo de porta de comutação
```

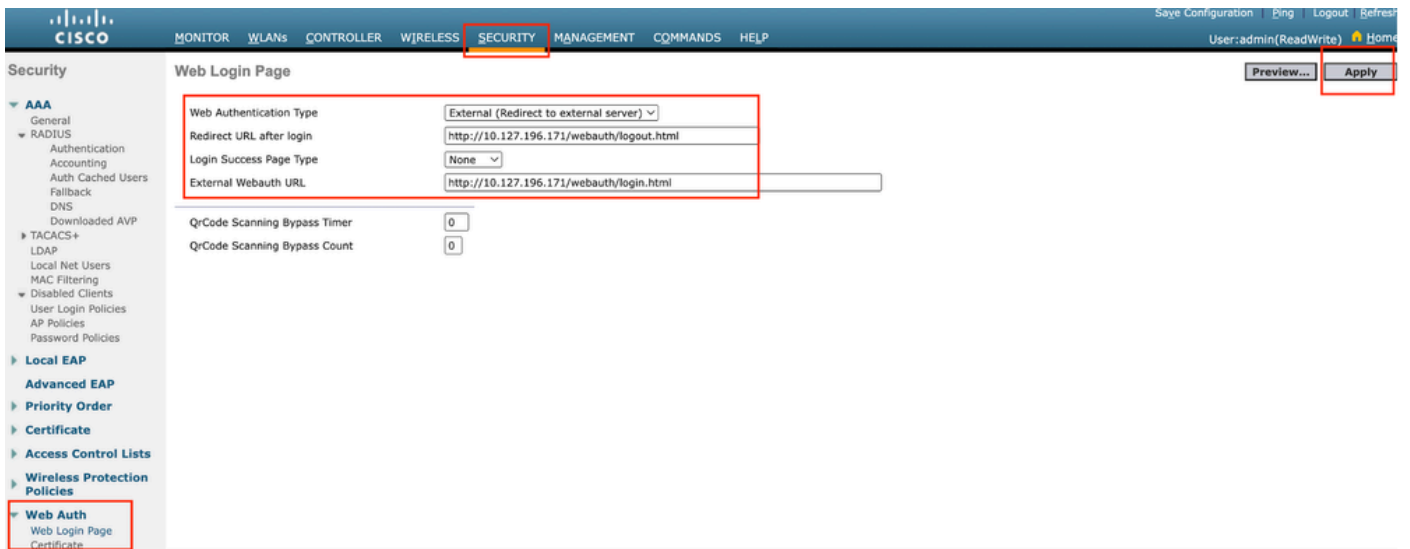
```
switchport trunk native vlan 2081
```

```
switchport trunk allowed vlan 2081,2024
```

```
fim
```

## Configurar Autenticação da Web

Etapa 1: Navegue até Segurança > Autenticação da Web > Página de logon na Web. Defina o tipo de Autenticação da Web como Externa (Redirecionar para servidor externo) e configure a URL de Autenticação da Web externa. A opção Redirect URL after login é opcional e pode ser configurada se os clientes precisarem ser redirecionados para uma página dedicada após a autenticação bem-sucedida.



Configurações de Web Auth

## Configurações de AAA:

Etapa 1: Configure o servidor radius

Navegue até Security > Radius > Authentication > New.



Servidor Radius

Etapa 2: Configure o IP do servidor RADIUS e o segredo compartilhado no controlador. Alterne o status do servidor para Enabled e marque a caixa de seleção Network User.

## RADIUS Authentication Servers > New

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

Configuração do servidor

### Configurar Lista de Controle de Acesso

Etapa 1: Navegue até Segurança > Lista de controle de acesso e selecione Novo. Crie uma ACL

de pré-autenticação que permita o tráfego para o DNS e o 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 an 'Access List Name' of 'Pre-Auth\_ACL'. The 'Deny Counters' are set to 0. Below this is a table of rules:

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

Lista de acesso para permitir o tráfego para o servidor Web

## Configurar perfil de LAN de convidado

Etapa 1: Navegue até WLAN > Criar novo > Ir.

The screenshot shows the Cisco ISE WLANs page. The 'WLANs' tab is highlighted in the top navigation bar. Below the navigation bar, there is a 'Current Filter: None' section with links for '[Change Filter]' and '[Clear Filter]'. On the right side, there is a 'Create New' button with a dropdown arrow and a 'Go' button next to it.

Perfil de LAN de convidado

Selecione Type (Tipo) como Guest LAN (LAN de convidado) e configure um nome de perfil. O mesmo nome deve ser configurado no perfil de política e no perfil de LAN de convidado do controlador Âncora 9800.

## WLANs > New

Type

Guest LAN

Profile Name

Guest-Profile

ID

3

Perfil de LAN de convidado

Etapa 2: na guia Geral, mapeie a interface de entrada e saída no perfil de LAN de convidado.

A interface de entrada é a vlan à qual os clientes com fio se conectam fisicamente.

A interface de saída é a sub-rede vlan que os clientes solicitam para o endereço IP.

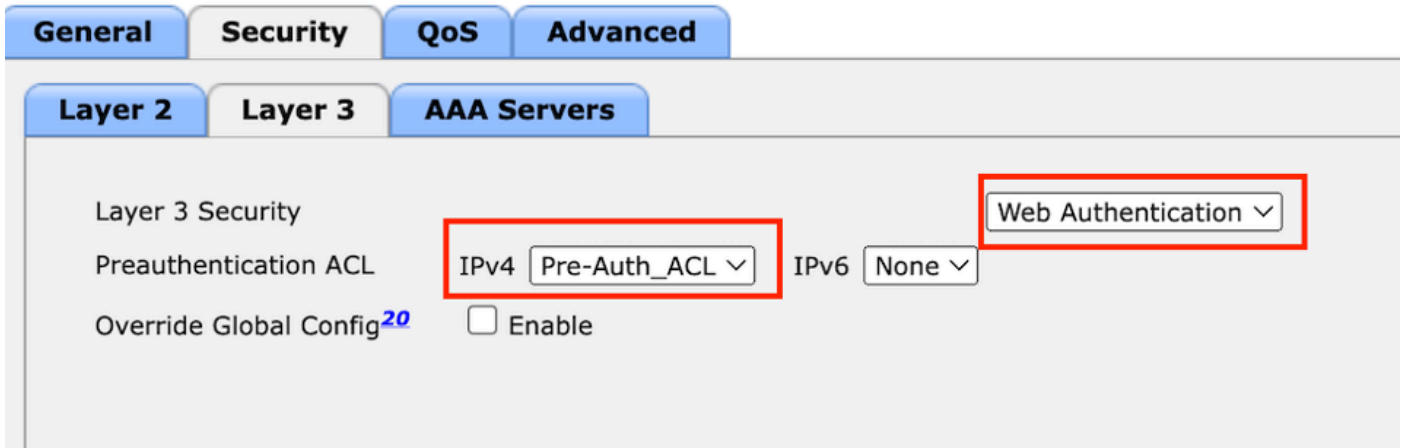
General	Security	QoS	Advanced
Profile Name	Guest-Profile		
Type	Guest LAN		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	<b>Web-Auth</b> (Modifications done under security tab will appear after applying th		
Ingress Interface	wired-guest		
Egress Interface	vlan2024		
NAS-ID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

Perfil de LAN de convidado

Etapa 3: Navegue até Segurança > Camada 3.

Selecione Layer 3 Security como Web Authentication e mapeie a ACL de pré-autenticação.

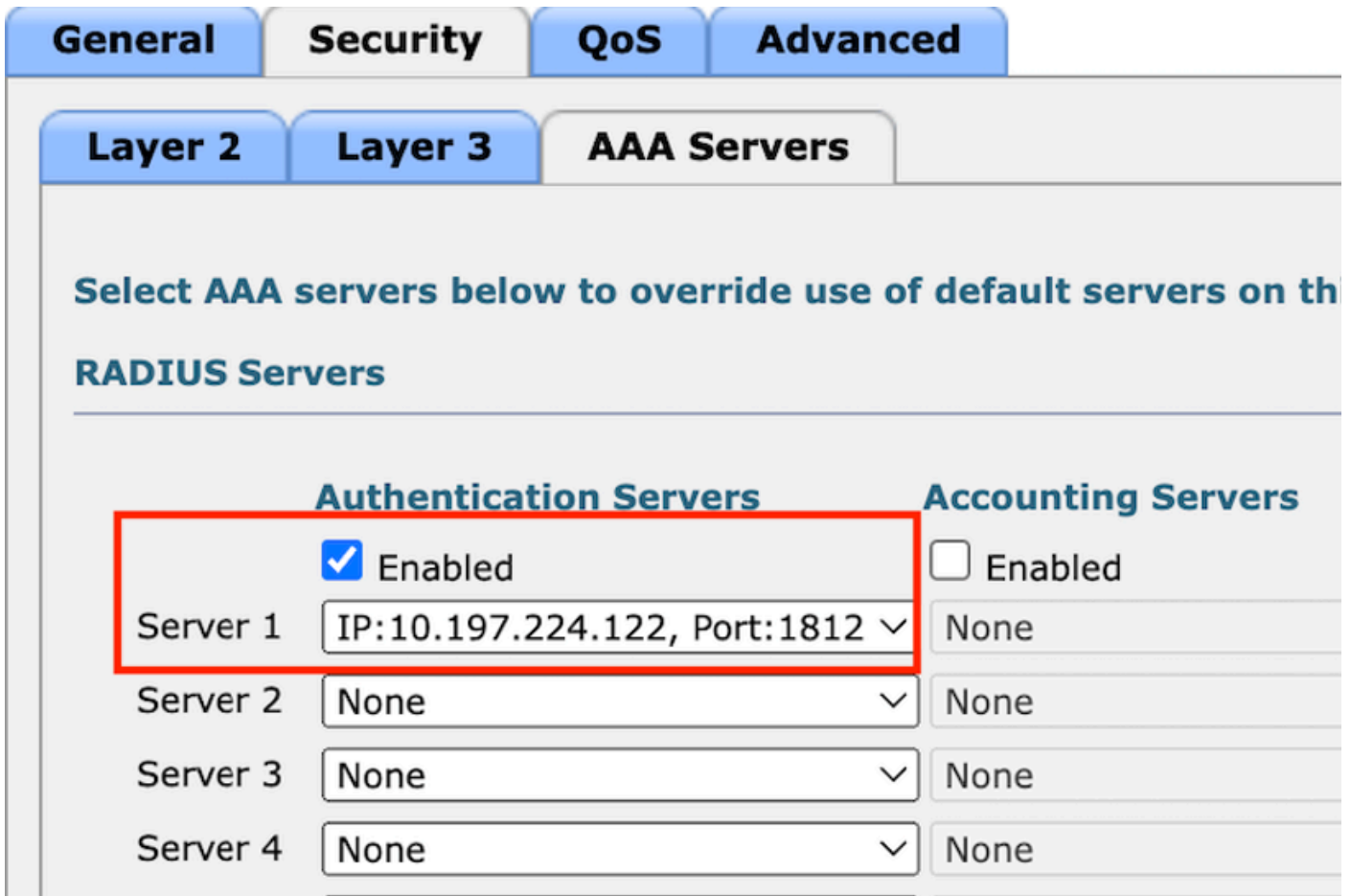




Guia de segurança da camada 3

Etapa 4:

Na guia AAA servers, mapeie o servidor Radius e marque a caixa de seleção Enabled.



Mapeando servidores radius para o perfil de LAN de convidado

Etapa 5: navegue até a página WLAN e passe o mouse sobre o ícone de dropdown do perfil de LAN de convidado e selecione Âncoras de mobilidade.



Etapa 6: mapeie a âncora de mobilidade na lista suspensa para o perfil de LAN de convidado.

### Mobility Anchors

WLAN SSID Guest-Profile

Switch IP Address (Anchor)

Mobility Anchor Create

Switch IP Address (Anchor)

Foot Notes

local  
10.106.39.41  
10.76.6.156  
✓ 10.76.118.70

Data Path

Co

Mapeando âncora de mobilidade para LAN de convidado

## Configuração na WLC Anchor 9800

### Configurar mapa de parâmetros da Web

Etapa 1: Navegue até Configuration > Security > Web Auth e selecione Global. Verifique se o endereço IP virtual do controlador e do ponto de confiança estão mapeados corretamente no perfil, com o tipo definido como 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

Etapa 2: Na guia Avançado, especifique o URL da página da Web externa para o qual os clientes devem ser redirecionados. Configure a URL de redirecionamento para login e Redirecionar em caso de falha. A configuração Redirect On-Success é opcional.

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>

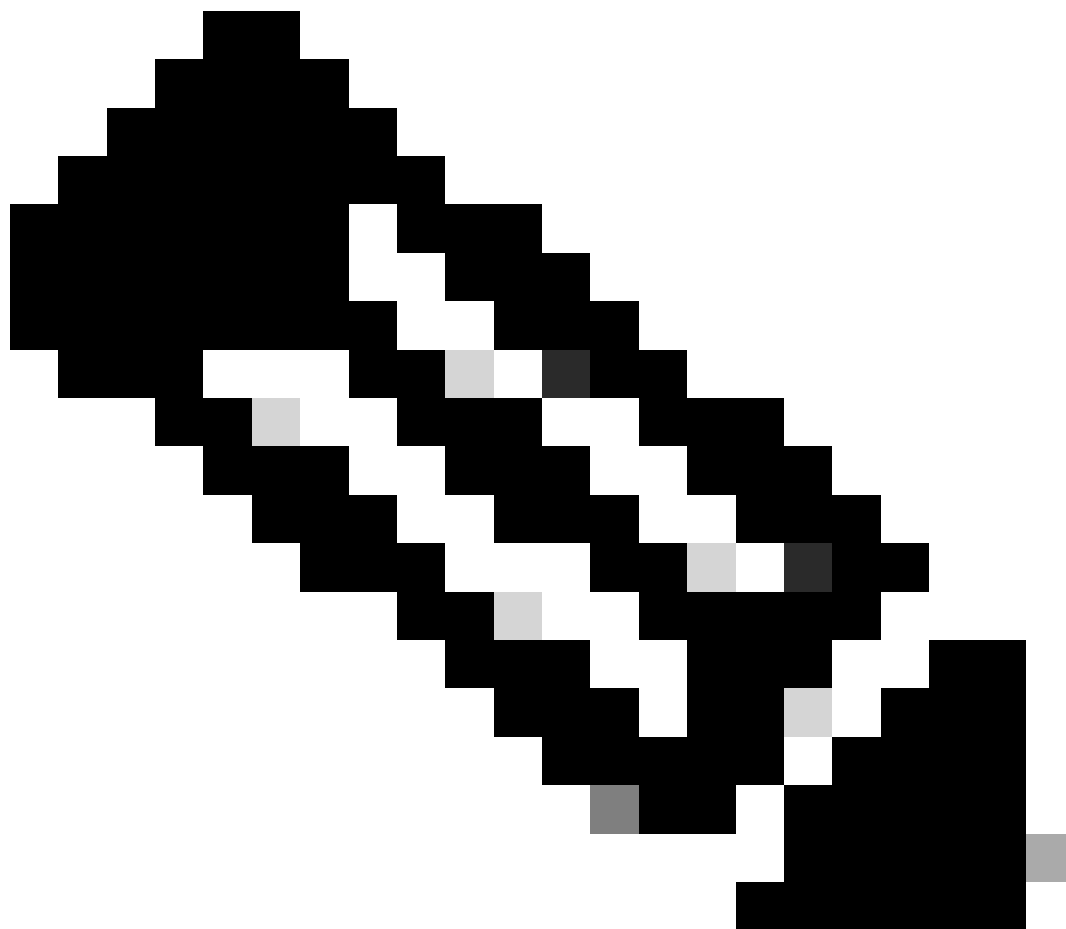
### Redirect to external server

Redirect URL for login	<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"/>

Guia Avançado

## Configuração 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
```



Observação: para a configuração AAA, consulte os detalhes de configuração fornecidos na seção "Configurar convidado com fio no Catalyst 9800 ancorado em outro Catalyst 9800" para o Foreign 9800 WLC.

---

## Configurar perfil de Diretiva

Etapa 1: Navegue até Configuration > Tags & Profiles > Policy. Configure o perfil de política com o mesmo nome usado para o perfil de LAN de Convidado do controlador Externo.

**General**

Access Policies

QOS and AVC

Mobility

Advanced

Name\*

Guest-Profile

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 da política

Etapa 2: na guia Access Policies (Políticas de acesso), mapeie a vlan do cliente com fio na lista suspensa

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 acesso

Etapa 3: Na guia Mobility, marque a caixa de seleção 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

Guia Mobilidade

## Configuração 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 convidado

Etapa 1: Navegue até Configuration > Wireless > Guest LAN e selecione Add para configurar o perfil de LAN de convidado e desabilitar o status de VLAN com fio.

O nome do perfil de LAN de convidado em Âncora deve ser igual ao perfil de LAN de convidado em WLC externa.

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 convidado

Etapa 2: Na guia Security, habilite Web Auth. Selecione o mapa de parâmetros de Autenticação da Web e a Lista de autenticação na lista suspensa

## Edit Guest LAN Profile

General Security

### Layer3

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

Guia Segurança de LAN de convidado

### Configuração de CLI

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



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

## MAP de LAN de convidado

Etapa 1: Navegue até Configuration > Wireless > Guest LAN. Na seção de configuração Guest LAN MAP, selecione Add e mapeie o perfil de política para o perfil de LAN de convidado.

> 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: Guest-Profile

✓ Save    ↺ Cancel

MAP de LAN de convidado

## Verificar

Validar configuração do controlador

#show resumo de LAN de convidado

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

ID de LAN de convidado #show 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 global de webauth do tipo de mapa de parâmetros

<#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 <nome do perfil> (Se o perfil de parâmetro da Web personalizado for usado)

#show resumo do mapa de LAN de convidado sem fio

Table with 2 columns: GLAN Profile Name, Policy Name. Row 1: Guest, Guest.

#show resumo da mobilidade sem fio

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 da Política do cliente

No Estrangeiro,

#show resumo de cliente sem fio

O estado do gerenciador de políticas do cliente no controlador Externo é EXECUTADO depois que o cliente se associa com êxito.

<#root>

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

GLAN 1

Run

802.3

Web Auth

Export Foreign

>show client detail a0ce.c8c3.a9b5

<#root>

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

**Export Foreign**

Mobility Anchor IP Address.....

10.76.118.70

Security Policy Completed.....

**Yes**

Policy Manager State.....

**RUN**

Pre-auth IPv4 ACL Name..... Pre-Auth\_ACL

EAP Type..... Unknown

Interface.....

**wired-guest-egress**

VLAN..... 2024

Quarantine VLAN..... 0

Em Âncora,

A transição de estado do cliente deve ser monitorada no controlador de Âncora.

O estado do gerenciador de políticas do cliente está em Web Auth pendente.

<#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**

Depois que o cliente é autenticado, o estado do gerenciador de políticas passa para o 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 detalhes do endereço mac do cliente sem fio a0ce.c8c3.a9b5

<#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

O cliente passa para o estado EXECUTAR após a autenticação bem-sucedida da 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 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

Após as transições do cliente de autenticação para o 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

# Troubleshooting

## Depuração do controlador AireOS

Habilitar depuração de cliente

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

Para verificar se a depuração está habilitada

```
>show debugging
```

Para desativar a depuração

```
debug disable-all
```

## 9800 Traço radioativo

Ative o Radio Active Tracing para gerar rastreamentos de depuração de cliente para o endereço MAC especificado na CLI.

Etapas para ativar o rastreamento radioativo:

Verifique se todas as depurações condicionais estão desabilitadas.

```
clear platform condition all
```

Habilite a depuração para o endereço MAC especificado.

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

Após reproduzir o problema, desative a depuração para interromper a coleta de rastreamento do RA.

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

Quando o rastreamento do RA é interrompido, o arquivo de depuração é gerado no bootflash do 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
```

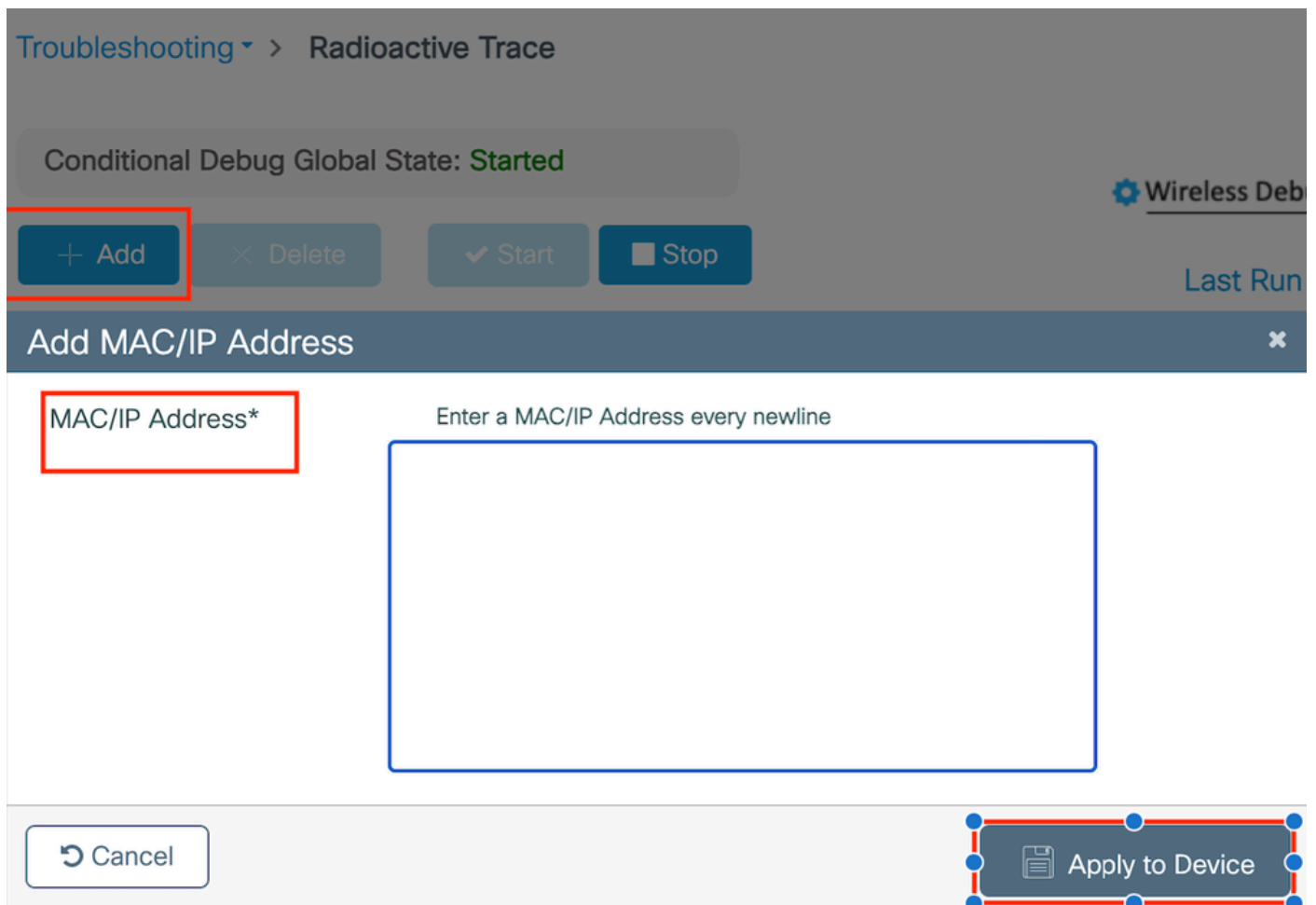
Copie o arquivo para um servidor externo.

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

Exibir o log de depuração:

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

Ativar rastreamento de RA na GUI,



Habilitar rastreamento de RA na WebUI

Captura de pacotes incorporada

Navegue até Troubleshooting > Captura de Pacotes. Insira o nome da captura e especifique o endereço MAC do cliente como o MAC do filtro interno. Defina o tamanho do buffer como 100 e

escolha a interface de uplink para monitorar os pacotes de entrada e saída.

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

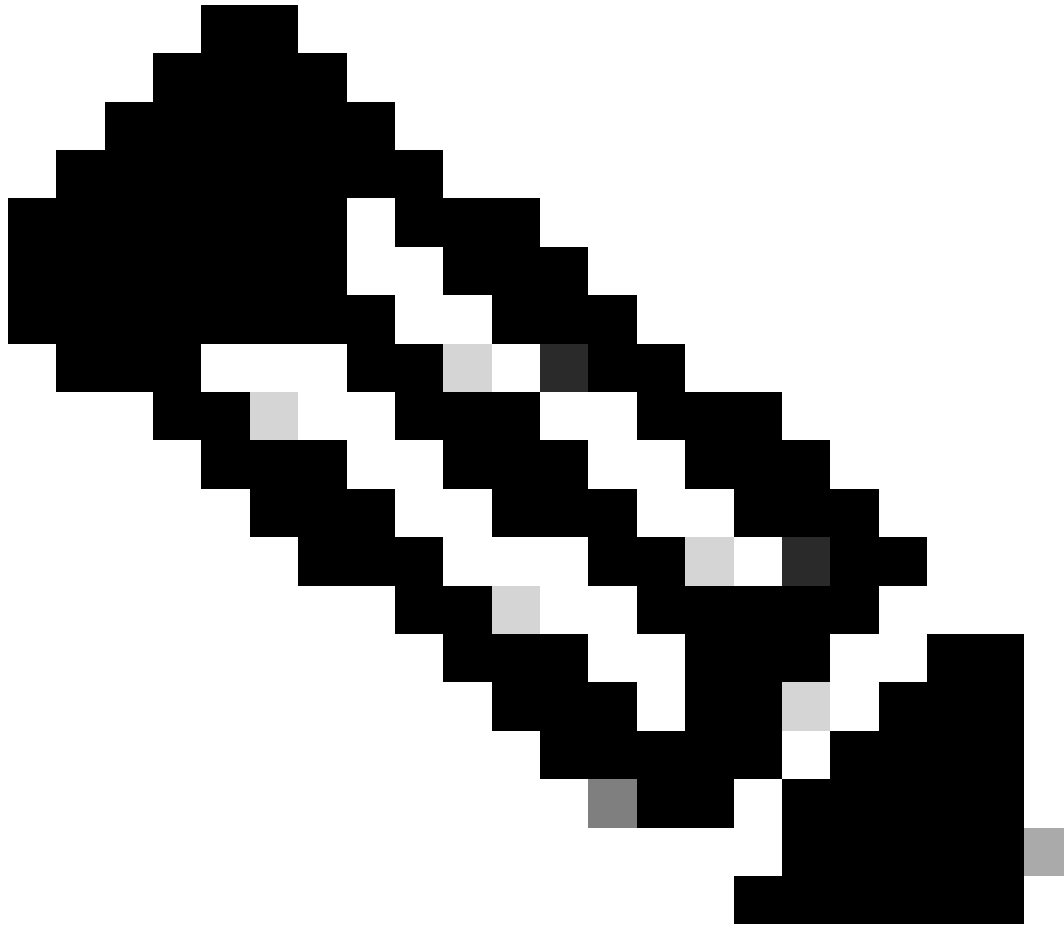
Available (12)

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

Selected (1)

 Tw0/0/0	←
---	---

Captura de pacotes incorporada



Observação: selecione a opção "Monitorar tráfego de controle" para visualizar o tráfego redirecionado para a CPU do sistema e injetado novamente no plano de dados.

Navegue até Troubleshooting > Packet Capture e selecione Start para capturar pacotes.

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 pacote

### Configuração 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)

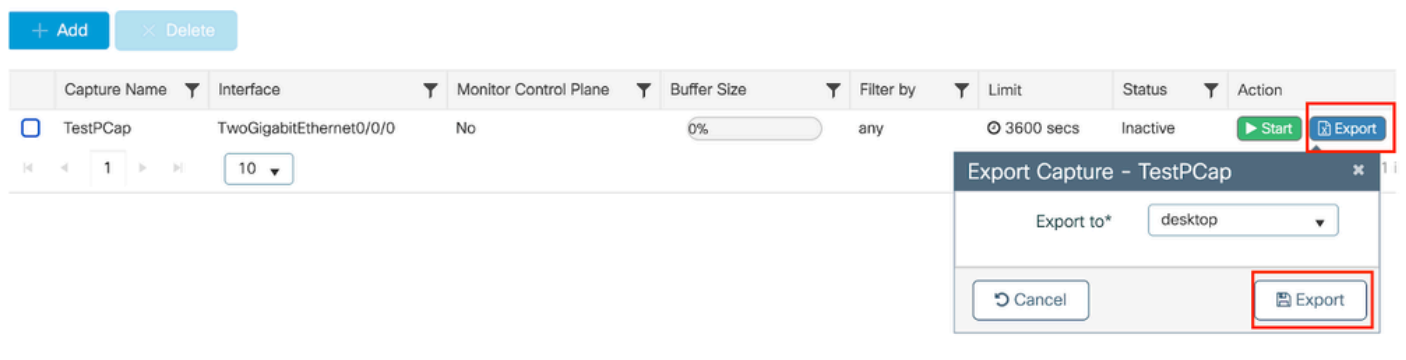
Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

Exportar captura de pacotes para um servidor TFTP externo.

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

Navegue até Troubleshooting > Packet Capture e selecione Export para fazer download do arquivo de captura na máquina local.



Faça o download do EPC

Trechos de log de trabalho

Log de depuração do cliente do AireOS Foreign Controller

Pacote com fio recebido do cliente com fio

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

Solicitação de âncora de exportação de construção 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
```

O controlador externo envia a solicitação de âncora Export ao controlador de âncora.

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

O controlador de âncora envia confirmação para a solicitação de âncora do 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:c
```

A função de mobilidade dos clientes no controlador Externo é atualizada para exportar 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
```

O cliente fez a transição para o estado RUN.

```
*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 radioativo de controlador estrangeiro

O cliente se associa ao controlador.

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

A descoberta de mobilidade está em andamento após a associação.

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

Uma vez processada a descoberta de mobilidade, o tipo de roam do cliente é atualizado para 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

O controlador externo está enviando a solicitação de âncora de exportação para a WLC Âncora.

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

A resposta Export Anchor é recebida do controlador Anchor e a vlan é aplicada do perfil do usuário.

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:

Depois que a solicitação de Âncora de Exportação for processada, a função de mobilidade do cliente será atualizada para Exportar para o Exterior.

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



O cliente faz a transição para o estado de aprendizagem 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
```

Após o aprendizado do IP, o cliente passa para o estado RUN na WLC externa.

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

Log de depuração do cliente do controlador AireOS Anchor

Solicitação de âncora de exportação recebida do 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
```

A vlan de bridging local é aplicada ao 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
```

A função de mobilidade é atualizada para Exportar Âncora e Estado do cliente transistenciado Associado.

```
*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
```

A mobilidade está concluída, o estado do cliente está associado e a função de mobilidade é Âncora de exportação.

\*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

O endereço IP do cliente é aprendido no controlador e o estado é transferido do DHCP necessário para a autenticação da Web necessária.

\*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

A URL de Webauth está sendo formulada adicionando a URL de redirecionamento externa e o endereço IP virtual do 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://

Adicionado o endereço MAC do cliente e a WLAN ao 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 depois de empacotar o HTTP GET para o 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.

A URL de redirecionamento é enviada ao cliente no pacote de resposta 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

O cliente estabelece uma conexão TCP com o host de url de redirecionamento. Depois que os clientes enviam o nome de usuário e a senha de login no portal, uma solicitação radius é enviada pelo controlador ao servidor radius

Quando a controladora recebe um Access-Accept, o cliente fecha a sessão TCP e passa para o 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 Rastreamento radioativo do controlador de âncora

Mensagem de anúncio de mobilidade para o cliente do controlador externo.

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

Solicitação de âncora de exportação recebida do controlador externo quando o cliente está se associando, para a qual a resposta de âncora de exportação é enviada pelo controlador de âncora, que pode ser verificada no rastreamento RA do controlador externo.

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

O cliente é movido para o estado de associação e a função de mobilidade é transicionada para Âncora de Exportação.

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

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

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

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

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

O aprendizado de IP é concluído, o IP do cliente aprendido através do 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
```

O estado da política do cliente está em autenticação da Web pendente.

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

O handshake TCP é falsificado pelo controlador. Quando o cliente envia um HTTP GET, um quadro de resposta 200 OK é enviado, contendo o URL de redirecionamento.

O cliente deve estabelecer um handshake TCP com o URL de redirecionamento e carregar a 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
```

Quando o cliente envia as credenciais de login na página do portal da Web, um pacote de solicitação de acesso é enviado ao servidor radius para autenticação.

```
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 é recebido do servidor radius, webauth é bem-sucedido.

```
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

A autenticação foi bem-sucedida e o estado da política do cliente é em EXECUÇÃO.

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

## Análise de captura de pacotes incorporada

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

> Frame 806: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits)  
> Ethernet II, Src: Cisco\_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco\_34:90:cb (6c:5e:3b:34:90:cb)  
> Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.76.6.156  
> User Datagram Protocol, Src Port: 16667, Dst Port: 16667  
> Control And Provisioning of Wireless Access Points - Data  
> Ethernet II, Src: Cisco\_34:90:d4 (6c:5e:3b:34:90:d4), Dst: CeLink\_c3:a9:b5 (a0:ce:c8:c3:a9:b5)  
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4095  
> Internet Protocol Version 4, Src: 10.105.211.1, Dst: 10.105.211.69  
> Transmission Control Protocol, Src Port: 80, Dst Port: 54351, Seq: 1, Ack: 108, Len: 743  
▼ Hypertext Transfer Protocol  
 > HTTP/1.1 200 OK\r\n  
 Location: http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=http://10.105.211.1/auth/discovery?architecture=9\r\n Content-Type: text/html\r\n Content-Length: 527\r\n \r\n [HTTP response 1/1]  
 [Time since request: 0.000000000 seconds]  
 [Request in frame: 804]  
 [Request URI: http://10.105.211.1/auth/discovery?architecture=9]  
 File Data: 527 bytes

O cliente é redirecionado para a página do portal

A sessão é fechada após o recebimento da URL de redirecionamento.

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

A sessão TCP é fechada após o recebimento da URL de redirecionamento

O cliente inicia o handshake triplo TCP para o host da URL de redirecionamento e envia uma solicitação HTTP GET.

Quando a página é carregada, as credenciais de login são enviadas no portal, o controlador envia uma solicitação de acesso ao servidor radius para autenticar o cliente.

Após a autenticação bem-sucedida, a sessão TCP para o servidor Web é fechada e, no controlador, o estado do gerenciador de políticas do cliente é transicionado para EXECUTAR.



## Artigo relacionado

[Configurar o recurso de mobilidade de âncora de WLAN no Catalyst 9800](#)

[Exemplo de configuração de acesso de convidado com fio usando controladores AireOS](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.