

# Configurar o portal cativo do DNA Spaces com o Catalyst 9800 WLC

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Conecte o controlador 9800 aos Cisco DNA Spaces](#)

[Criar o SSID em espaços do DNA](#)

[Configuração de ACL e filtro de URL no controlador 9800](#)

[Portal cativo sem servidor RADIUS em espaços do DNA](#)

[Configuração do Mapa de parâmetros de autenticação da Web no controlador 9800](#)

[Crie o SSID no controlador 9800](#)

[Configure o Policy Profile no controlador 9800](#)

[Configure a marcação de política no controlador 9800](#)

[Portal cativo com servidor RADIUS em espaços do DNA](#)

[Configuração do Mapa de parâmetros de autenticação da Web no controlador 9800](#)

[Configuração de servidores RADIUS no controlador 9800](#)

[Crie o SSID no controlador 9800](#)

[Configure o Policy Profile no controlador 9800](#)

[Configure a marcação de política no controlador 9800](#)

[Configurar o mapa de parâmetros globais](#)

[Criar o portal no DNA Spaces](#)

[Configurar as regras do portal cativo em espaços do DNA](#)

[Obter informações específicas do DNA Spaces](#)

[Quais são os endereços IP que o DNA Spaces usa?](#)

[Qual é a URL usada pelo portal de login do DNA Spaces?](#)

[Quais são os detalhes do servidor RADIUS para o DNA Spaces ?](#)

[Verificar](#)

[Troubleshoot](#)

[Problemas comuns](#)

[Rastreamento sempre ativo](#)

[Depuração condicional e rastreamento radioativo](#)

[Exemplo de uma tentativa bem-sucedida](#)

## Introduction

Este documento descreve como configurar portais cativos no Cisco DNA Spaces.

# Prerequisites

Este documento permite que os clientes no Catalyst 9800 Wireless LAN Controller (C9800 WLC) usem o DNA Spaces como uma página de login de autenticação da Web externa.

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso à Interface de Linha de Comando (CLI - Command Line Interface) ou à Interface Gráfica de Usuário (GUI - Graphic User Interface) dos controladores sem fio 9800
- Cisco DNA Spaces

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador 9800-L versão 16.12.2s

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

A Autenticação da Web é um método simples de autenticação da Camada 3 sem a necessidade de um suplicante ou utilitário cliente. Isso pode ser feito

- a) Com a página interna na WLC C9800 como está ou após modificações
- b) Com pacote de login personalizado carregado para a WLC C9800
- c) Página de login personalizada hospedada em um servidor externo

Utilizar o portal cativo fornecido pelo DNA Spaces é essencialmente uma maneira de implementar a autenticação da Web externa para clientes no C9800 WLC.

O processo de webauth externo é descrito em detalhes em:

<https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/web-authentication/b-configuring-web-based-authentication-on-cisco-catalyst-9800-series-controllers/m-external-web-authentication-configuration.html>

Na WLC C9800, o endereço ip virtual é definido como o mapa de parâmetros global e é tipicamente 192.0.2.1

## Configurar

### Diagrama de Rede



## Conecte o controlador 9800 aos Cisco DNA Spaces

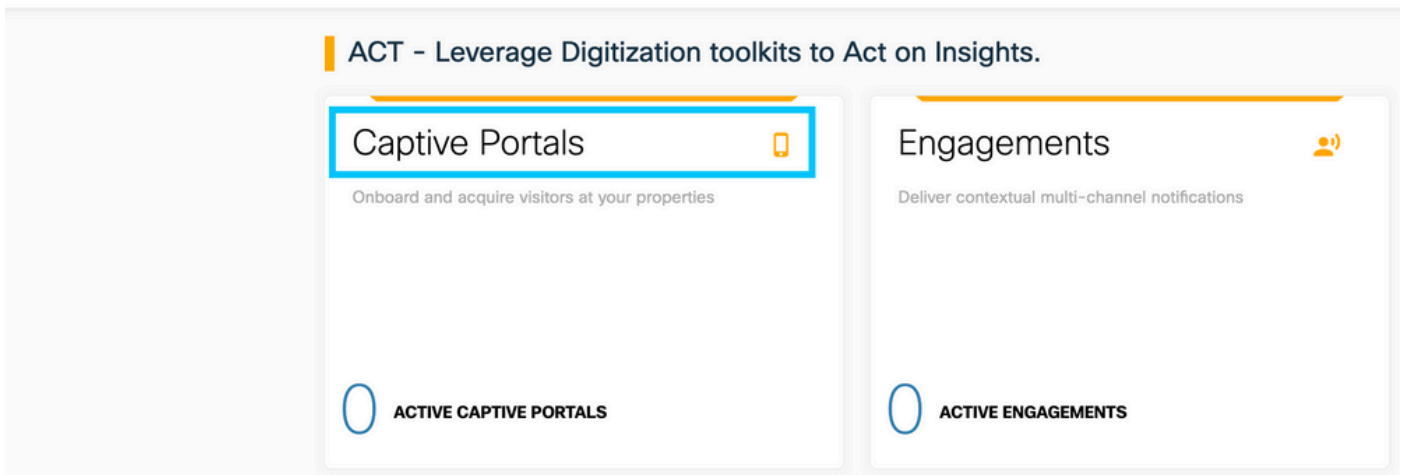
O controlador precisa ser conectado ao DNA Spaces com qualquer uma das opções - Direct Connect, via DNA Spaces Connector ou com CMX Tethering.

Neste exemplo, a opção Direct Connect está em uso, embora os portais cativos sejam configurados da mesma forma para todas as configurações.

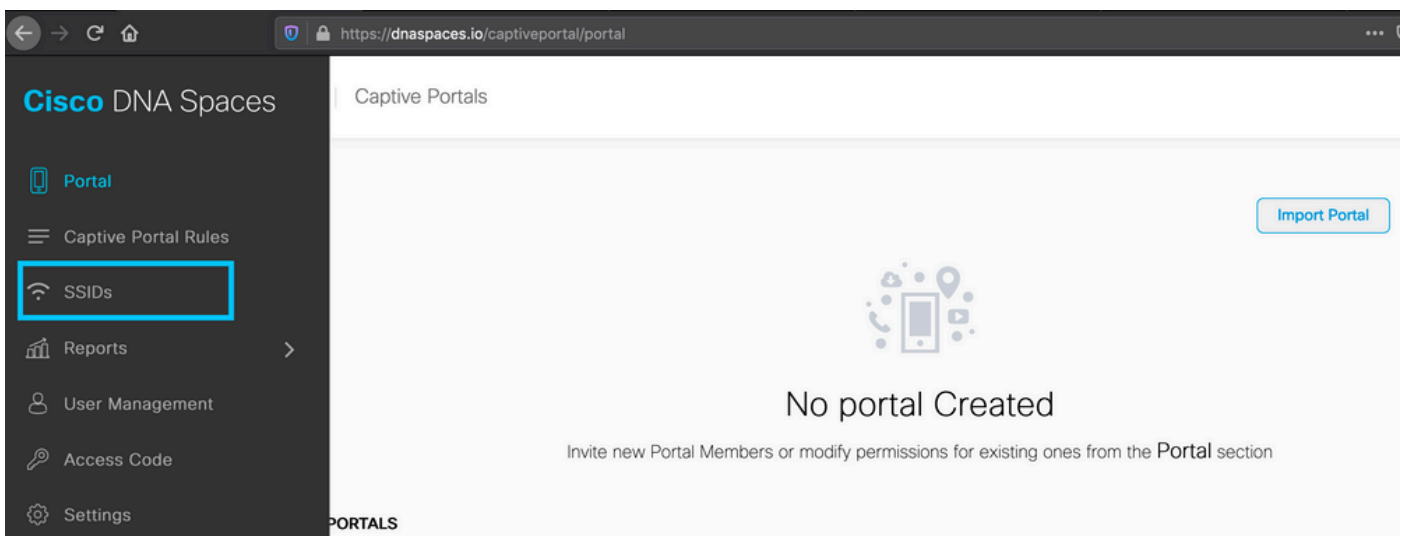
Para conectar o controlador ao Cisco DNA Spaces, ele deve ser capaz de acessar o Cisco DNA Spaces Cloud via HTTPS. Para obter mais informações sobre como conectar o controlador 9800 ao DNA Spaces, consulte este link: [DNA Spaces - 9800 Controller Direct Connect](#)

## Criar o SSID em espaços do DNA

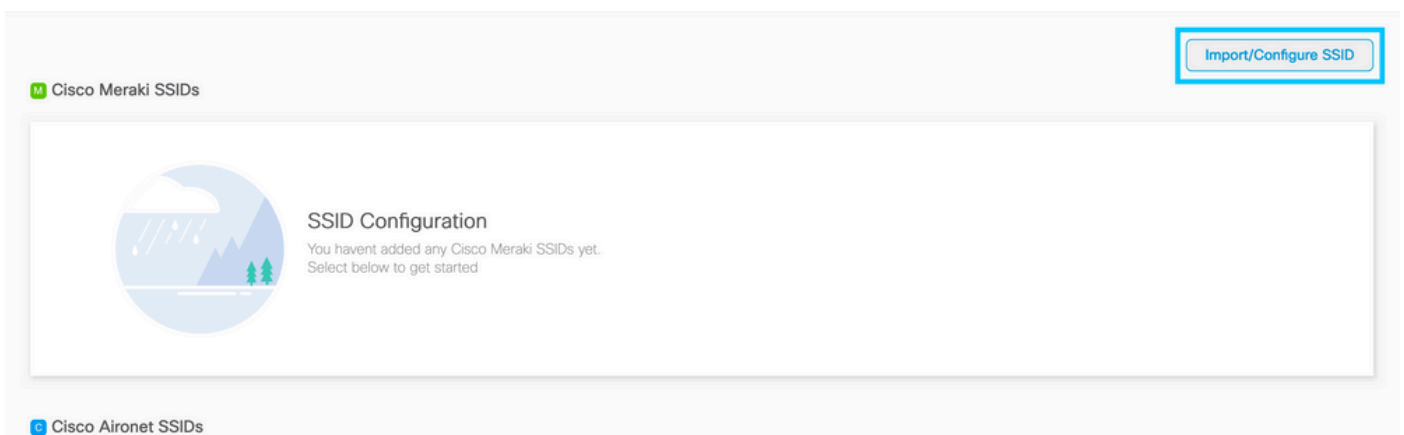
Etapa 1. Clique em **Portais cativos** no painel do DNA Spaces:



Etapa 2. Abra o menu específico do portal cativo, clique no ícone de três linhas no canto superior esquerdo da página e clique em **SSIDs**:



Etapa 3. Clique em **Import/Configure SSID**, selecione **CUWN (CMX/WLC)** como o tipo de "Wireless Network" e insira o nome do SSID:



## Configuração de ACL e filtro de URL no controlador 9800

O tráfego de um cliente sem fio não é permitido na rede até que a autenticação seja concluída. No caso da autenticação da Web, para concluí-la, um cliente sem fio se conecta a esse SSID,

recebe um endereço IP e o estado do gerenciador de políticas do cliente é movido para o **estado Webauth\_reqd**. Como o cliente ainda não foi autenticado, toda a origem de tráfego do endereço IP do cliente é descartada, exceto DHCP e DNS e HTTP (que são interceptados e redirecionados).

Por padrão, o 9800 cria ACLs de pré-autenticação codificadas quando configuramos uma WLAN de autenticação da Web. Essas ACLs codificadas permitem DHCP, DNS e tráfego para o servidor de autenticação da Web externo. Todo o restante é redirecionado como qualquer tráfego http. No entanto, se você precisar permitir o tipo de tráfego não-HTTP específico através do, você pode configurar uma ACL de pré-autenticação. Você precisaria então imitar o conteúdo da ACL pré-autenticação codificada existente (a partir da etapa 1 desta seção) e aumentá-la de acordo com suas necessidades.

## Etapa 1. Verificar as ACLs codificadas atualmente

### Configuração de CLI:

```
Andressi-9800L#show ip access list
```

```
Extended IP access list WA-sec-34.235.248.212
```

```
10 permit tcp any host 34.235.248.212 eq www
20 permit tcp any host 34.235.248.212 eq 443
30 permit tcp host 34.235.248.212 eq www any
40 permit tcp host 34.235.248.212 eq 443 any
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit udp any any eq bootpc
80 permit udp any any eq bootps
90 deny ip any any
```

```
Extended IP access list WA-v4-int-34.235.248.212
```

```
10 deny tcp any host 34.235.248.212 eq www
20 deny tcp any host 34.235.248.212 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

WA-sec-34.235.248.212 é chamado dessa forma porque é uma ACL de segurança (seg) de autenticação da Web automática ou ip de portal "34.235.248.212". As ACLs de segurança definiram o que é permitido (na permissão) ou descartado (na negação)

Wa-v4-int é uma ACL de interceptação, ou seja, uma ACL de punt ou de redirecionamento e define o que é enviado à CPU para redirecionamento (na permissão) ou o que é enviado ao painel de dados (na negação).

O WA-v4-int34.235.248.212 é aplicado primeiro no tráfego que vem do cliente e mantém o tráfego HTTP(s) em direção ao IP 34.235.248.212 do portal do DNA Spaces no dataplane (não ação de derivação ou encaminhamento ainda, simplesmente entregue ao dataplane). Envia para a CPU (para redirecionamento, exceto para o tráfego IP virtual, que é atendido pelo servidor Web) todo o tráfego HTTP(s). Outros tipos de tráfego são fornecidos ao plano de dados.

O WA-sec-34.235.248.212 permite o tráfego HTTP e HTTPS para o IP 34.235.248.212 do espaço do DNA que você configurou no mapa de parâmetros de autenticação da Web e também permite o tráfego DNS e DHCP e descarta o restante. O tráfego HTTP a ser interceptado já foi interceptado antes de atingir essa ACL e, portanto, não precisa ser coberto por essa ACL.

**Observação:** para obter os endereços IP dos espaços do DNA a serem permitidos na ACL, clique na opção **Configurar manualmente** do SSID criado na etapa 3 da seção **Criar o SSID nos espaços do DNA** na seção de configuração da ACL. Um exemplo está localizado na seção "Quais são os endereços IP que o DNA Spaces usa" no final do documento.

O DNA Spaces usa 2 endereços IP e o mecanismo da etapa 1 permite apenas que um IP do portal seja permitido. Para permitir o acesso de pré-autenticação a mais recursos HTTP, você precisa usar filtros de URL que dinamicamente fazem brechas nas ACLs de interceptação (redirecionamento) e segurança (pré-autenticação) para os IPs relacionados ao site cuja URL você digita no filtro de URL. As solicitações DNS são rastreadas dinamicamente para que o 9800 aprenda o endereço IP desses URLs e adicione-o às ACLs dinamicamente.

Etapa 2. Configure o filtro de URL para permitir o domínio do DNA Spaces. Navegue para Configuration > Security > URL Filters, clique em **+Add** e configure o nome da lista, selecione **PRE-AUTH** como o tipo, ação como PERMIT e a URL splash.dnaspaces.io (ou .eu se você usar o portal da EMEA):

The screenshot shows the 'Add URL Filter' configuration window. The 'List Name\*' field is set to 'DNASpaces'. The 'Type' dropdown is set to 'PRE-AUTH'. The 'Action' is set to 'PERMIT' with a green square indicator. The 'URLs' field contains 'splash.dnaspaces.io'. The window has a 'Cancel' button on the bottom left and an 'Apply to Device' button on the bottom right.

Configuração de CLI:

```
Andressi-9800L(config)#urlfilter list
```

```
Andressi-9800L(config-urlfilter-params)#action permit
```

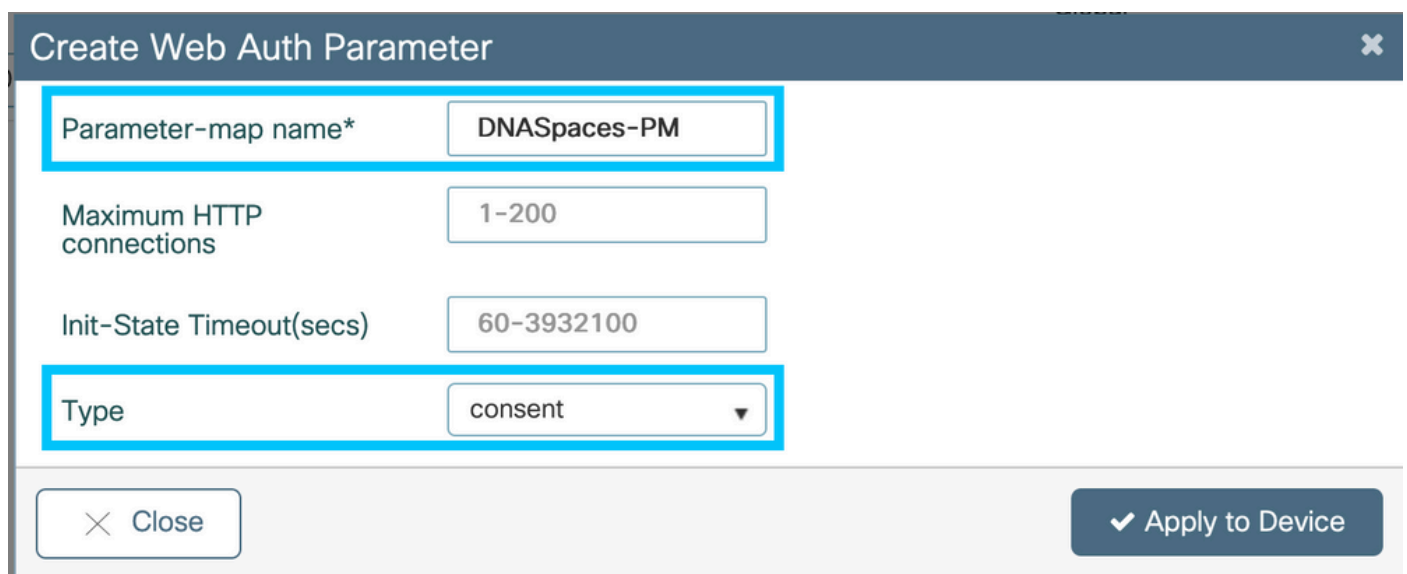
```
Andressi-9800L(config-urlfilter-params)#url splash.dnaspaces.io
```

O SSID pode ser configurado para usar um servidor RADIUS ou sem ele. Se a Duração da sessão, o Limite de largura de banda ou o Provisionamento contínuo da Internet estiverem configurados na seção **Ações** da configuração Regra de portal cativo, o SSID precisará ser configurado com um Servidor RADIUS; caso contrário, não haverá necessidade de usar o Servidor RADIUS. Há suporte para todos os tipos de portais nos espaços do DNA em ambas as configurações.

## Portal cativo sem servidor RADIUS em espaços do DNA

### Configuração do Mapa de parâmetros de autenticação da Web no controlador 9800

Etapa 1. Navegue até **Configuration > Security > Web Auth**, clique em **+Add** para criar um novo mapa de parâmetros. Na janela pop-up, configure o nome do mapa de parâmetros e selecione **Consentimento** como o tipo:



The screenshot shows a 'Create Web Auth Parameter' dialog box. The title bar is dark blue with a close button (X) on the right. The main area is light gray and contains four input fields, each with a blue border. The first field is 'Parameter-map name\*' with the value 'DNASpaces-PM'. The second field is 'Maximum HTTP connections' with the value '1-200'. The third field is 'Init-State Timeout(secs)' with the value '60-3932100'. The fourth field is 'Type' with a dropdown menu showing 'consent'. At the bottom, there are two buttons: 'Close' (with a close icon) and 'Apply to Device' (with a checkmark icon).

Etapa 2. Clique no mapa de parâmetros configurado na etapa anterior, navegue até a guia **Advanced** e insira o Redirect for log-in URL, Append for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID and portal IPv4 Address, conforme ilustrado. Clique em **Update & Apply**:

General

**Advanced**

**Redirect to external server**

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address

Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

**Customized page**

Login Failed Page  

Login Page  

Logout Page  

Login Successful Page  

✕ Cancel

 Update & Apply



**Observação:** para obter o URL da página inicial e o endereço de redirecionamento IPv4, clique na opção **Configurar manualmente** na página SSID do DNA Spaces. Isso é ilustrado no final do documento "Qual é o URL que o portal do DNA Spaces usa?"

**Observação:** o portal Cisco DNA Spaces pode resolver para dois endereços IP, mas o controlador 9800 permite que apenas um endereço IP seja configurado, escolha qualquer um desses endereços IP e configure-o no mapa de parâmetros como o Endereço IPv4 do portal.

**Observação:** verifique se os endereços IPv4 e IPv6 virtuais são configurados no mapa de parâmetros de autenticação da Web global. Se o IPv6 virtual não estiver configurado, os clientes às vezes serão redirecionados para o portal interno em vez do portal do DNA Spaces configurado. É por isso que um IP virtual deve sempre ser configurado. "192.0.2.1" pode ser configurado como IPv4 virtual e FE80:0:0:0:903A::11E4 como IPV6 virtual. Há poucos ou nenhum motivo para usar outros IPs além desses.

## Configuração de CLI:

```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type consent
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

## Crie o SSID no controlador 9800

Etapa 1. Navegue até **Configuration > Tags & Profiles > WLANs** e clique em **+Add**. Configure o Nome do perfil, SSID e ative a WLAN. Certifique-se de que o nome SSID seja igual ao nome configurado na etapa 3 da seção **Criar o SSID em espaços do DNA**.

### Add WLAN

General Security Advanced

Profile Name\* 9800DNASpaces

SSID\* 9800DNASpaces

WLAN ID\* 3

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED

Cancel Apply to Device

Etapa 2. Navegue até **Segurança > Camada 2**. Defina o modo de segurança da camada 2 como **None**, certifique-se de que a filtragem MAC esteja desativada.

### Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode None

MAC Filtering

Transition Mode WLAN ID 0

Fast Transition Adaptive Enabled

Over the DS

Reassociation Timeout 20

Cancel Apply to Device

Etapa 3. Navegue até **Segurança > Camada 3**. Habilite a Política da Web, configure o mapa de parâmetros de autenticação da Web. Clique em **Apply to Device**.

**Edit WLAN** ✕

General **Security** Advanced Add To Policy Tags

---

Layer2 **Layer3** AAA

---

[Show Advanced Settings >>>](#)

Web Policy

Web Auth Parameter Map

Authentication List  ⓘ

*For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device*

## Configure o Policy Profile no controlador 9800

Etapa 1. Navegue até **Configuration > Tags & Profiles > Policy** e crie um novo Policy Profile ou use o Policy Profile padrão. Na guia Access Policies (Políticas de acesso), configure a VLAN cliente e adicione o filtro de URL.

**Edit Policy Profile** ✕

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

---

RADIUS Profiling

Local Subscriber Policy Name

**WLAN Local Profiling**

Global State of Device Classification **Disabled** ⓘ

HTTP TLV Caching

DHCP TLV Caching

**VLAN**

VLAN/VLAN Group

Multicast VLAN

**WLAN ACL**

IPv4 ACL

IPv6 ACL

**URL Filters**

Pre Auth

Post Auth

## Configure a marcação de política no controlador 9800

Etapa 1. Navegue até **Configuration > Tags & Profiles > Policy**. Crie uma nova Marca de Diretiva ou use a marca de diretiva padrão. Mapeie a WLAN para o perfil de política na etiqueta de política.

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input type="checkbox"/> 9800DNASpaces	DNASpaces-PP

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

Etapa 2. Aplique a etiqueta de política ao AP para transmitir o SSID. Navegue até **Configuration > Wireless > Access Points**, selecione o AP em questão e adicione a etiqueta de política. Isso faz com que o AP reinicie seu túnel CAPWAP e junte-se de volta ao controlador 9800:

General

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Version

Primary Software Version	16.12.2.132
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	16.12.2.132
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv6
SLAAC IPv6 Address	2001:172:16:30:ed0:f8ff:fe94:118c
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

Time Statistics

Up Time	11 days 22 hrs 49 mins 12 secs
Controller Association Latency	3 mins 44 secs

Configuração de CLI:

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown
```

```
Andressi-9800L(config)#wireless profile policy
```

```
Addresssi-9800L(config-wireless-policy)#vlan <id>  
Addresssi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter
```

```
Addresssi-9800L(config-wireless-policy)#no shutdown
```

```
Addresssi-9800L(config)#wireless tag policy
```

```
Addresssi-9800L(config-policy-tag)#wlan
```

## Portal cativo com servidor RADIUS em espaços do DNA

**Observação:** o servidor RADIUS do DNA Spaces oferece suporte apenas à autenticação PAP proveniente do controlador.

### Configuração do Mapa de parâmetros de autenticação da Web no controlador 9800

Etapa 1. Crie um mapa de parâmetros de autenticação da Web. Navegue para **Configuration > Security > Web Auth**, clique em **+Add**, configure o nome do mapa de parâmetros e selecione **webauth** como o tipo:

### Create Web Auth Parameter ✕

Parameter-map name*	DNASpaces-PM
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	webauth ▼

✕ Close ✓ Apply to Device

Etapa 2. Clique no mapa de parâmetros configurado na etapa 1, clique em **Advanced** e insira Redirect for log-in, Append for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID and portal IPv4 Address. Clique em **Atualizar e aplicar**:

General

**Advanced**

**Redirect to external server**

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address

Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

**Customized page**

Login Failed Page  

Login Page  

Logout Page  

Login Successful Page  

✕ Cancel

 Update & Apply



**Observação:** para obter o URL da página inicial e o endereço de redirecionamento IPv4, clique na opção **Configurar manualmente** do SSID criado na etapa 3 da seção **Criar o SSID em espaços do DNA** sob a seção **Criando os SSIDs na conexão direta da WLC Criando a configuração da lista de controle de acesso**, respectivamente.

**Observação:** o portal Cisco DNA Spaces pode resolver para dois endereços IP, mas o controlador 9800 permite que apenas um endereço IP seja configurado. Em um caso, escolha qualquer um desses endereços IP a ser configurado no mapa de parâmetros como o **Endereço IPv4** do portal.

**Note:** Verifique se os endereços IPv4 e IPv6 virtuais estão configurados no mapa de parâmetros de autenticação da Web global. Se o IPv6 virtual não estiver configurado, os clientes às vezes serão redirecionados para o portal interno em vez do portal do DNA Spaces configurado. É por isso que um IP virtual deve sempre ser configurado. "192.0.2.1" pode ser configurado como IPv4 virtual e FE80:0:0:0:903A::11E4 como IPv6 virtual. Há poucos ou nenhum motivo para usar outros IPs além desses.

### Configuração de CLI:

```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type webauth
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

### Configuração de servidores RADIUS no controlador 9800

Etapa 1. Configure os servidores RADIUS. O Cisco DNA Spaces atua como um servidor RADIUS para autenticação de usuário e pode responder em dois endereços IP. Navegue para **Configuration > Security > AAA**, clique em **+Add** e configure os dois servidores RADIUS:

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add - Delete

RADIUS Servers Server Groups

TACACS+

Create AAA Radius Server

Name\* DNASpaces1

IPv4 / IPv6 Server Address\* 34.197.146.105

PAC Key

Key Type 0

Key\* .....

Confirm Key\* .....

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA **ENABLED**

Cancel Apply to Device

**Observação:** para obter o endereço IP RADIUS e a chave secreta para servidores primários e secundários, clique na opção **Configurar manualmente** do SSID criado na etapa 3 da seção **Criar o SSID nos espaços do DNA** e navegue até a seção **Configuração do servidor RADIUS**.

Etapa 2. Configure o grupo de servidores RADIUS e adicione ambos os servidores RADIUS. Navegue para **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups**, clique em **+add**, configure o nome do Server Group, MAC-Delimiter como **Hyphen**, MAC-Filtering como **MAC** e atribua os dois servidores RADIUS:

+ AAA Wizard

Servers / Groups    AAA Method List    AAA Advanced

+ Add

- Delete

RADIUS

TACACS+

LDAP

Servers    Server Groups

Name    Server 1    Server 2

0    10 items per page

Create AAA Radius Server Group

Name\*    DNASpaces

Group Type    RADIUS

MAC-Delimiter    hyphen

MAC-Filtering    mac

Dead-Time (mins)    1-1440

Available Servers

[Empty list box]

>

<

Assigned Servers

DNASpaces1  
DNASpaces2

Cancel

Apply to Device

Etapa 3. Configure uma lista de Método de autenticação. Navegue para **Configuration > Security > AAA > AAA Method List > Authentication**, clique em **+add**. Configure o nome da Lista de métodos, selecione **login** como o tipo e atribua o Grupo de servidores:

Configuration > Security > AAA

+ AAA Wizard

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

Authentication

Authorization

Accounting

+ Add   - Delete

Name	Type	Group Type	Group1	Group2
<input type="checkbox"/> default	dot1x	local	N/A	N/A

10 items per page

### Quick Setup: AAA Authentication

Method List Name\*   DNASpaces

Type\*   login

Group Type   group

Fallback to local  

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- DNASpaces

Cancel   Apply to Device

Etapa 4. Configure uma lista de Método de Autorização. Navegue para **Configuration > Security > AAA > AAA Method List > Authorization**, clique em **+add**. Configure o nome da Lista de métodos, selecione **network** como o tipo e atribua o Grupo de servidores:

Configuration > Security > AAA

+ AAA Wizard

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

Authentication

**Authorization**

Accounting

+ Add    × Delete

Name	Type	Group Type	Group1	Group2
<input type="checkbox"/> MeshAP	credential-download	local	N/A	N/A

10 items per page

### Quick Setup: AAA Authorization

Method List Name\*    DNASpaces

Type\*    network

Group Type    group

Fallback to local   

Authenticated   

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- DNASpaces

Cancel    Apply to Device

## Crie o SSID no controlador 9800

Etapa 1. Navegue até **Configuration > Tags & Profiles > WLANs** e clique em **+Add**. Configure o Nome do perfil, SSID e ative a WLAN. Certifique-se de que o nome SSID seja igual ao nome configurado na etapa 3 da seção **Criar o SSID em espaços do DNA**.

### Add WLAN ✕

General Security Advanced

Profile Name\* 9800DNASpaces Radio Policy All

SSID\* 9800DNASpaces Broadcast SSID **ENABLED**

WLAN ID\* 3

Status **ENABLED**

↶ Cancel 📄 Apply to Device

Etapa 2. Navegue até **Segurança > Camada 2**. Defina o modo de segurança da camada 2 como **None**, ative a filtragem MAC e adicione a lista de autorização:

### Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode None

MAC Filtering

Transition Mode WLAN ID 0

Authorization List\* DNASpaces

Fast Transition Disabled

Over the DS

Reassociation Timeout 20

↶ Cancel 📄 Apply to Device

Etapa 3. Navegue até **Segurança > Camada 3**. Habilite a Política da Web, configure o mapa do parâmetro de autenticação da Web e a Lista de autenticação. Ative On Mac Filter Failure (Falha de filtro On Mac) e adicione a ACL de pré-autenticação. Clique em **Apply to Device**.

## Add WLAN



General **Security** Advanced

Layer2 **Layer3** AAA

Web Policy	<input checked="" type="checkbox"/>
Web Auth Parameter Map	DNASpaces-PM
Authentication List	DNASpaces

*For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device*

<< Hide

On Mac Filter Failure	<input checked="" type="checkbox"/>
-----------------------	-------------------------------------

Splash Web Redirect	<input type="checkbox"/> DISABLED
---------------------	-----------------------------------

### Preauthentication ACL

IPv4	DNASpaces-ACL
------	---------------

IPv6	None
------	------

Cancel

Apply to Device

## Configure o Policy Profile no controlador 9800

Etapa 1. Navegue até **Configuration > Tags & Profiles > Policy** e crie um novo Policy Profile ou use o Policy Profile padrão. Na guia Access Policies (Políticas de acesso), configure a VLAN cliente e adicione o filtro de URL.

## Edit Policy Profile



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

RADIUS Profiling	<input type="checkbox"/>
Local Subscriber Policy Name	Search or Select

### WLAN Local Profiling

Global State of Device Classification **Disabled** ⓘ

HTTP TLV Caching	<input type="checkbox"/>
------------------	--------------------------

DHCP TLV Caching	<input type="checkbox"/>
------------------	--------------------------

### VLAN

VLAN/VLAN Group	VLAN2672
-----------------	----------

Multicast VLAN	Enter Multicast VLAN
----------------	----------------------

### WLAN ACL

IPv4 ACL	Search or Select
----------	------------------

IPv6 ACL	Search or Select
----------	------------------

### URL Filters

Pre Auth	DNASpaces
----------	-----------

Post Auth	Search or Select
-----------	------------------

Etapa 2. Na guia Avançado, ative AAA Override e, opcionalmente, configure a lista de métodos de contabilização:

Edit Policy Profile ✕

---

General
Access Policies
QOS and AVC
Mobility
Advanced

**WLAN Timeout**

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

**AAA Policy**

Allow AAA Override

NAC State

Policy Name

Accounting List

Fabric Profile

Umbrella Parameter Map

mDNS Service Policy  [Clear](#)

**WLAN Flex Policy**

VLAN Central Switching

Split MAC ACL

**Air Time Fairness Policies**

2.4 GHz Policy

5 GHz Policy

## Configure a marcação de política no controlador 9800

Etapa 1. Navegue até **Configuration > Tags & Profiles > Policy**. Crie uma nova Marca de Diretiva ou use a marca de diretiva padrão. Mapeie a WLAN para o perfil de política na etiqueta de política.



### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input type="checkbox"/> 9800DNASpaces	DNASpaces-PP

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

Etapa 2. Aplique a etiqueta de política ao AP para transmitir o SSID. Navegue até **Configuration > Wireless > Access Points**, selecione o AP em questão e adicione a etiqueta de política. Isso faz com que o AP reinicie seu túnel CAPWAP e junte-se de volta ao controlador 9800:

General

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Version

Primary Software Version	16.12.2.132
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	16.12.2.132
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv6
SLAAC IPv6 Address	2001:172:16:30:ed0:f8ff:fe94:118c
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

Time Statistics

Up Time	11 days 22 hrs 49 mins 12 secs
Controller Association Latency	3 mins 44 secs

Configuração de CLI:

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#ip access-group web
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
```

```
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#mac-filtering
```

```
Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth authentication-list
```

```
Andressi-9800L(config-wlan)#security web-auth on-macfilter-failure
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown
```

```
Andressi-9800L(config)#wireless profile policy
```

```
Andressi-9800L(config-wireless-policy)#aaa-override
Andressi-9800L(config-wireless-policy)#accounting-list
```

```
Andressi-9800L(config-wireless-policy)#vlan <id>
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter
```

```
Andressi-9800L(config-wireless-policy)#no shutdown
```

```
Andressi-9800L(config)#wireless tag policy
```

```
Andressi-9800L(config-policy-tag)#wlan
```

## Configurar o mapa de parâmetros globais

Etapa não recomendada : execute esses comandos para permitir o redirecionamento HTTPS, mas observe que o redirecionamento no tráfego HTTPS do cliente não é necessário se o sistema operacional do cliente fizer a detecção cativa do portal e causar utilização mais intensa da CPU e sempre emitir um aviso de certificado. Portanto, é recomendável evitar configurá-lo, a menos que seja necessário para um caso de uso muito específico.

```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#intercept-https-enable
```

**Observação:** você deve ter um certificado SSL válido para o IP virtual instalado no Cisco Catalyst 9800 Series Wireless Controller.

Etapa 1. Copie o arquivo certificado assinado com a extensão .p12 para um servidor TFTP e execute este comando para transferir e instalar o certificado no controlador 9800:

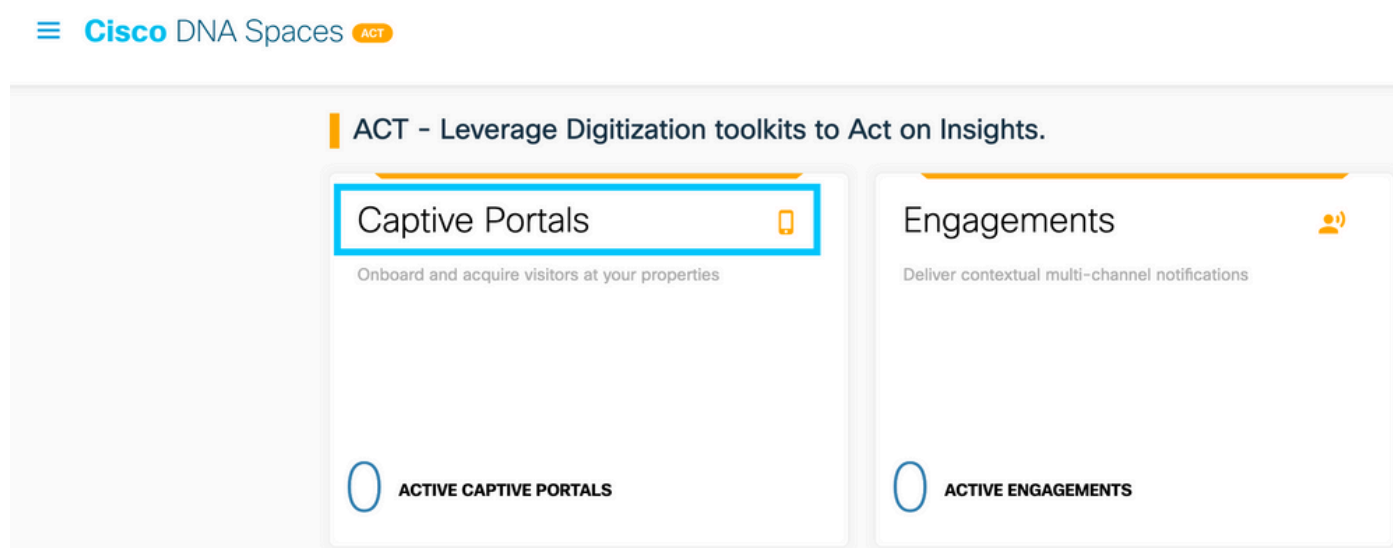
```
Andressi-9800L(config)#crypto pki import
```

Etapa 2. Para mapear o certificado instalado para o mapa de parâmetros de autenticação da Web, execute estes comandos:

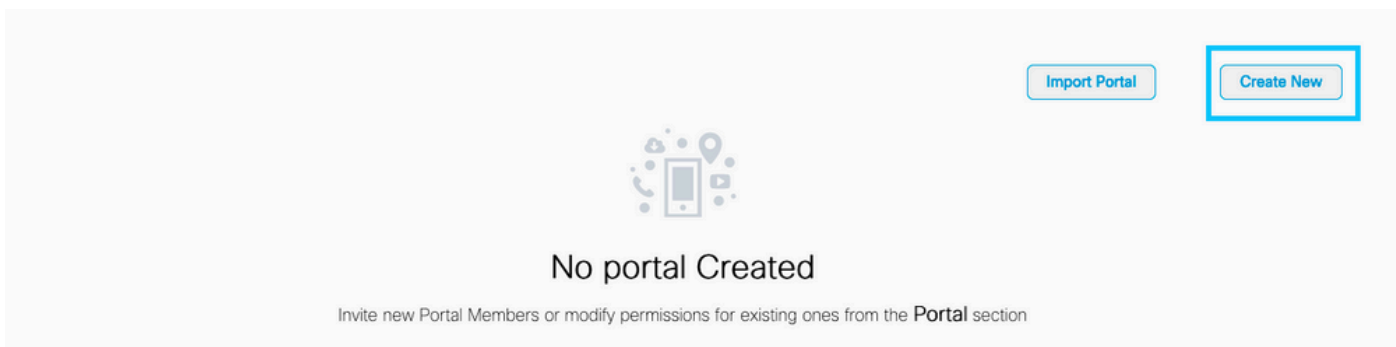
```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#trustpoint
```

## Criar o portal no DNA Spaces

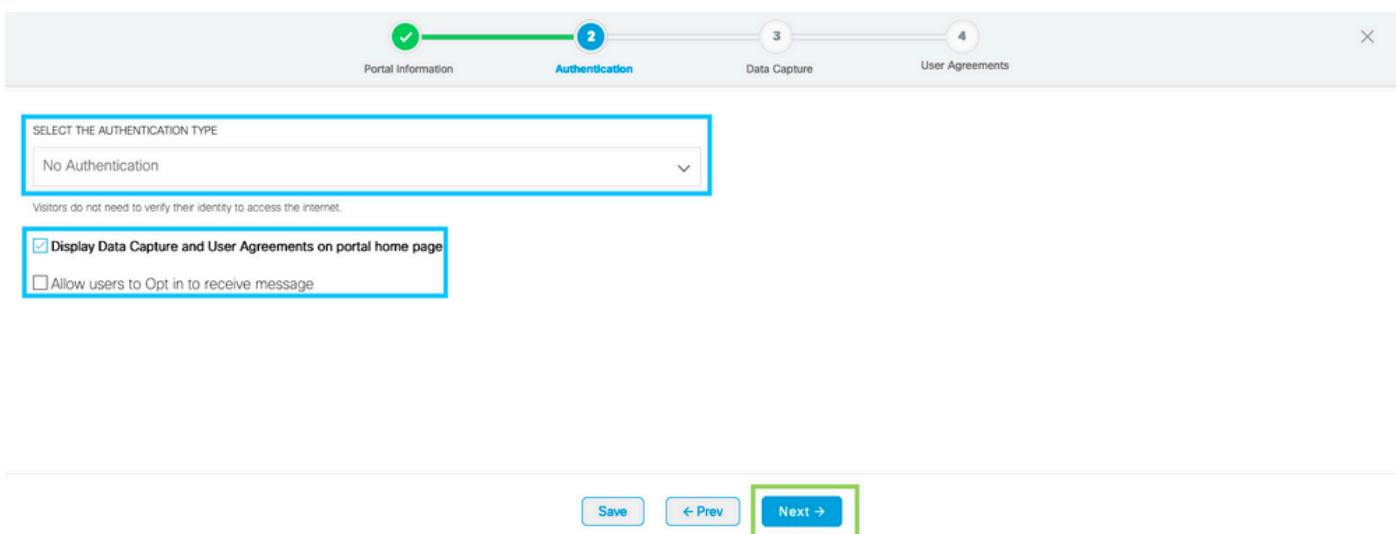
Etapa 1. Clique em **Portais cativos** no painel do DNA Spaces:



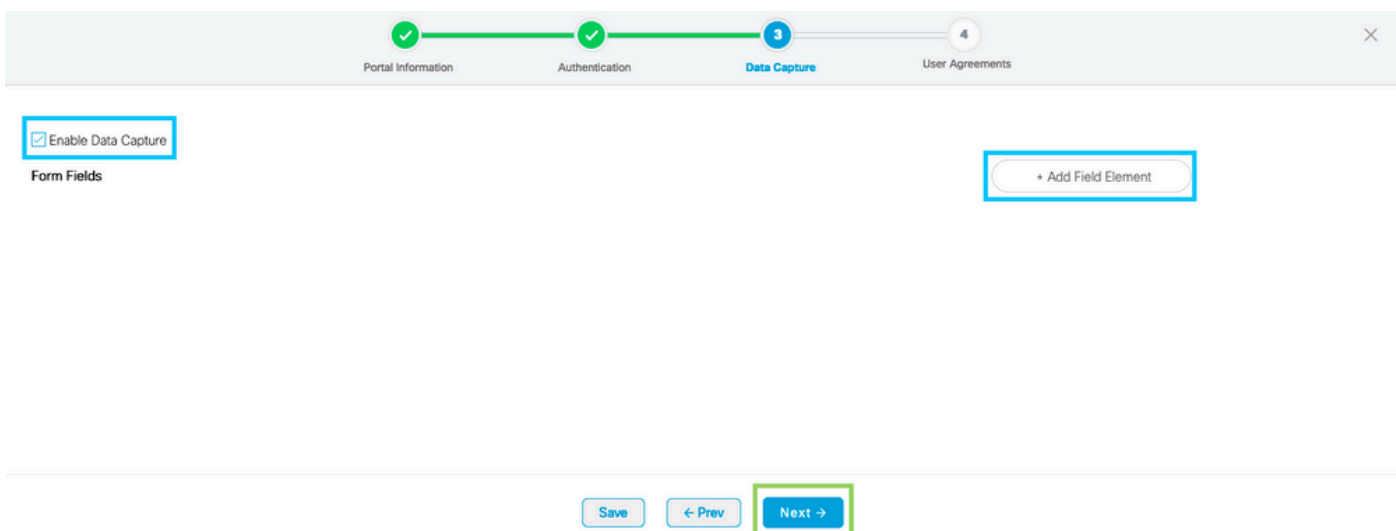
Etapa 2. Clique em **Criar novo**, insira o nome do portal e selecione os locais que podem usar o portal:



Etapa 3. Selecione o tipo de autenticação, escolha se deseja exibir a captura de dados e os contratos de usuário na home page do portal e se os usuários têm permissão para optar por receber uma mensagem. Clique em Next:



Etapa 4. Configurar elementos de captura de dados. Se você quiser capturar dados dos usuários, marque a caixa **Enable Data Capture** e clique em **+Add Field Element** para adicionar os campos desejados. Clique em Next:



Etapa 5. Marque **Ativar termos e condições** e clique em **Salvar e configurar o portal**:

Progress bar: Portal Information, Authentication, Data Capture, **User Agreements**

This section allows you to enable and configure Terms & Conditions and Privacy policy Statements.

Enable Terms & Conditions

TERMS & CONDITION MESSAGE

English

Rich text editor toolbar: Bold, Italic, Underline, Strikethrough, Text color, Background color, Bulleted list, Numbered list, Indent, Outdent, Link, Unlink, Undo, Redo, Font size, Text color, Background color, Font style, Font weight, Font color, Font background color, Font size, Text color, Background color, Font style, Font weight, Font color, Font background color.

Wi-Fi Terms of Use, Last updated: September 27, 2013.

These Wi-Fi Terms & Conditions Of Use (the Wi-Fi Terms) together with the TERMS OF USE govern your use of the Wi-Fi service.

Description of the Service

The Service provides you with wireless access to the Internet within the premises. We do not, as an ordinary practice, proactively monitor the activities of those who use the Service or exercise any editorial control over any material transmitted, hosted or posted using the Service to ensure that users comply with these Wi-Fi Terms and/or the law, although it reserves the right to do so.

Buttons: Save, < Prev, **Save & Configure Portal**

Etapa 6. Edite o portal conforme necessário. Clique em **Salvar**:

LOCATIONS: 1 Location ✓ | AUTH TYPE: No Authentication ✓ | USER AGREEMENTS: Enabled ✓ | DATA CAPTURE: Email, Mobile Number ✓

PORTAL EDITOR - Select a section to configure. Drag the items to reorder modules.

- Brand Name
- Welcome Message**
- Notice
- Data Capture
- Venue Map
- Videos
- Feedback
- Help
- Get Apps
- Get Internet
- Promos & Offers

+ Add Module

WELCOME MESSAGE

First time visitor welcome text

Welcome to Cisco Mexico

Add a custom message for Repeat visitors

Hi \${firstName} \${lastName}, Welcome to \${location}.

**Note**  
If any variables used in the message above are not available, we will default to the message shown for first time visitors.

PORTAL PREVIEW: Home Screen

ACME Company

Welcome to Cisco Mexico

**SIGN-UP FOR WIFI**

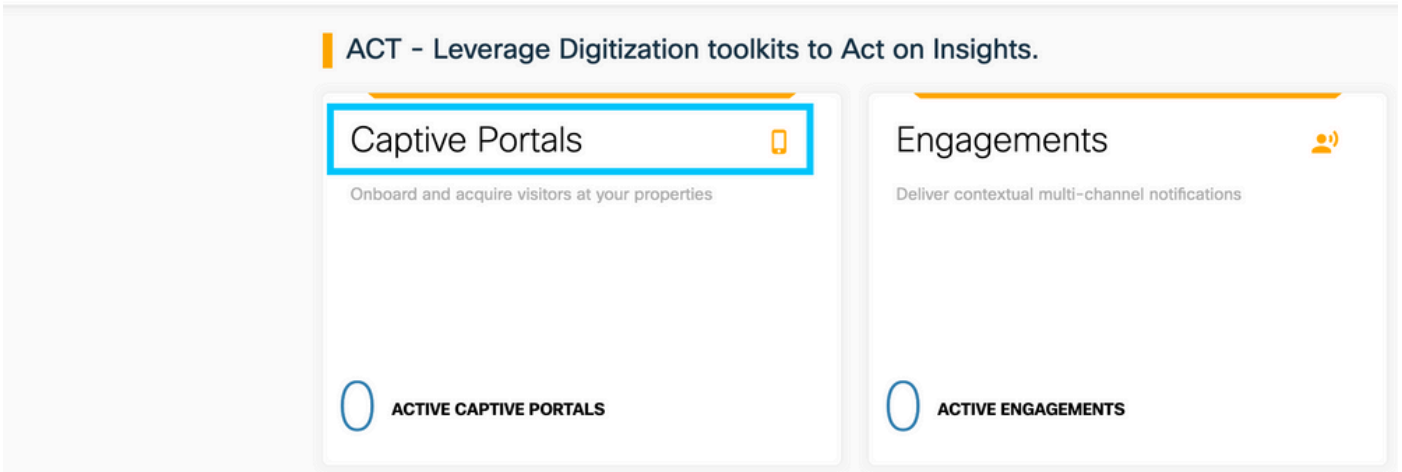
Email Address: [Input Field]

Mobile Number: [Input Field]

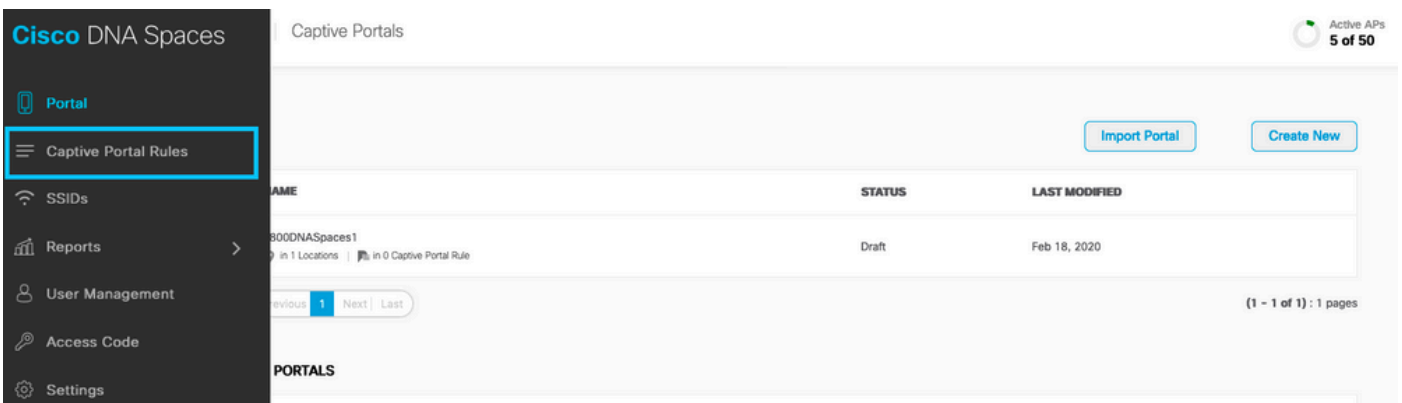
Buttons: Save, Cancel

## Configurar as regras do portal cativo em espaços do DNA

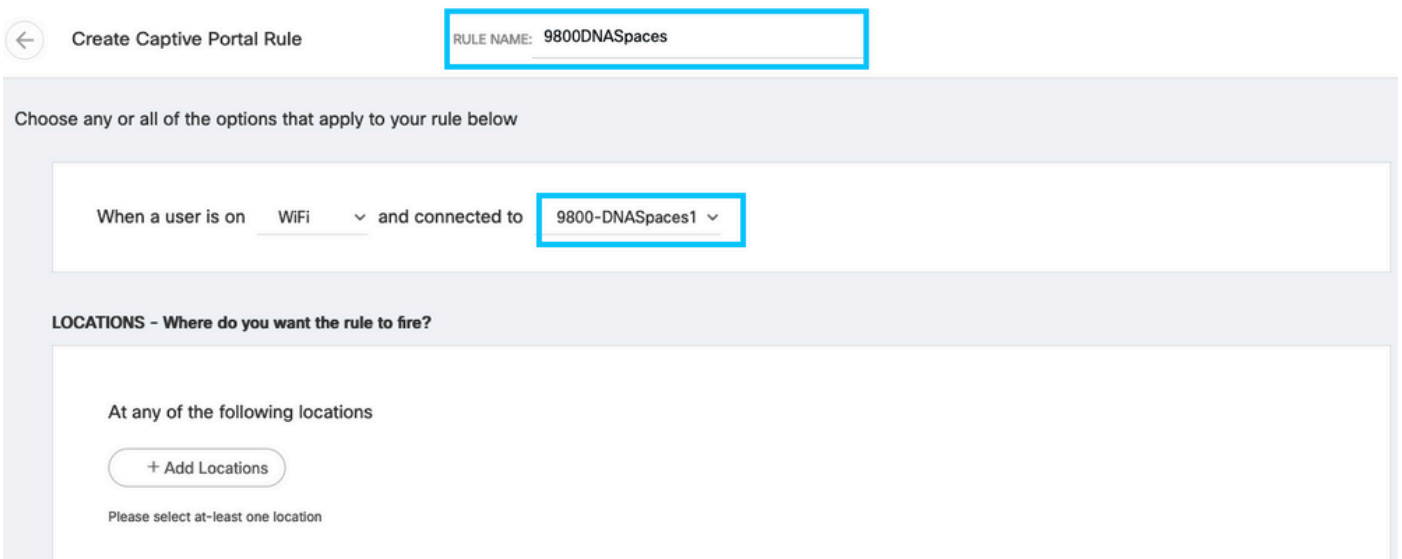
Etapa 1. Clique em **Portais cativos** no painel do DNA Spaces:



Etapa 2. Abra o menu do portal cativo e clique em **Captive Portal Rules**:



Etapa 3. Clique em + Criar nova regra. Insira o nome da regra e escolha o SSID configurado anteriormente.



Etapa 4. Selecione os locais em que o portal está disponível. Clique em + Adicionar locais na seção LOCAIS . Escolha o desejado na Hierarquia de locais.

## Choose Locations

### Location Hierarchy

MEX-EAST-1	<input type="checkbox"/>
+ 5508-1-CMX	<input type="checkbox"/>
+ 5508-2-Connector	<input type="checkbox"/>
+ 5520-1-DirectConnect	<input type="checkbox"/>
9800L-DirectConnect	<input checked="" type="checkbox"/>

### Selected Locations

9800L-DirectConnect X

Etapa 5. Escolha a ação do portal cativo. Nesse caso, quando a regra é atingida, o portal é mostrado. Clique em **Salvar e publicar**.

#### ACTIONS

Show Captive Portal  
Choose a Portal to be displayed to Users when they connect to the wifi.

9800DNASpaces1

Session Duration

Bandwidth Limit

Seamlessly Provision Internet  
Directly provision internet without showing any authentication

Deny Internet  
Stop users from accessing the internet

Tags these users as  
Choose - Associate/Disassociate users to chosen tags.

+ Add Tags

Trigger API

**Save & Publish** Save

#### SCHEDULE

#### ACTION

Show Captive Portal  
Portal : 9800DNASpaces1

## Obter informações específicas do DNA Spaces

### Quais são os endereços IP que o DNA Spaces usa?

Para verificar quais endereços IP os espaços do DNA usam para o portal em sua região, vá para a página Portal cativo na página inicial do DNA Space. Clique em **SSID** no menu esquerdo e, em seguida, clique em **Configure manualmente** em seu SSID. Os endereços IP são mencionados no exemplo da ACL. Esses são os endereços IP do portal para uso nas ACLs e no mapa de parâmetros de autenticação da Web. Os DNA Spaces usam outros endereços IP para a conectividade geral de NMSP/nuvem do plano de controle.





Na primeira seção do pop-up exibido, a etapa 7 mostra os endereços IP mencionados na definição da ACL. Você não precisa seguir essas instruções e criar qualquer ACL, apenas anote os endereços IP. Esses são os IPs usados pelo portal na sua área

## Configure



### Creating the Access Control List

To create the access control list, perform the following steps:

- 1 Log in to the WLC Direct Connect with your WLC Direct Connect credentials.
- 2 Choose **Security > Access Control Lists > Access Control Lists**.  
For FlexConnect local mode, choose **Security > Access Control Lists > FlexConnect ACLs**.
- 3 To add an ACL, click **New**.
- 4 In the **New** page that appears, enter the following:
  - a. In the **Access Control List Name** field, enter a name for the new ACL.
 

**Note:**  
You can enter up to 32 alphanumeric characters.
  - b. Choose the ACL type as **IPv4**.
 

**Note:**  
This option is not available for FlexConnect ACLs.
  - c. Click **Apply**.
- 5 When the **Access Control Lists** page reappears, click the name of the new ACL.
- 6 In the **Edit** page that appears, click **Add New Rule**. The **Rules > New** page appears.
- 7 Configure a rule for this ACL with the following wall garden ranges.

No	Dir	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP	Action
1.	Any	0.0.0.0/0.0.0.0	54.77.207.183/255.255.255.255	TCP	Any	HTTPS	Any	Permit
2.	Any	54.77.207.183/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit
3.	Any	0.0.0.0/0.0.0.0	34.252.175.120/255.255.255.255	TCP	Any	HTTPS	Any	Permit
4.	Any	34.252.175.120/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit

## Qual é a URL usada pelo portal de login do DNA Spaces?

Para verificar qual URL do portal de login os DNA Spaces usam para o portal em sua região, vá para a página **Portal Captival** na página inicial do DNA Space. Clique em **SSID** no menu esquerdo e, em seguida, clique em **Configure manualmente** em seu SSID.



Role para baixo na janela pop-up exibida e, na segunda seção, a etapa 7 mostra o URL que você precisa configurar em seu mapa de parâmetros no 9800.

### Creating the SSIDs in WLC Direct Connect

To create the SSIDs in the WLC Direct Connect, perform the following steps:

- 1 In the WLC Direct Connect main window, click the **WLANS** tab.
- 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.
- 3 In the New page that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.
- 4 Click **Apply**.  
The WLAN added appears in the WLANS page.
- 5 Click the WLAN you have newly created.
- 6 Choose **Security > Layer 2**, and configure the Layer 2 Security as **None**.
- 7 In the **Layer 3 tab**, do the following configurations:
  - a. From the Layer 3 security drop-down list, choose **Web Policy**.
  - b. Choose the **Passthrough** radio button.
  - c. In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL created earlier.
  - d. Select the Enable check box for the Sleeping Client.
  - e. Select the Enable check box for the Override Global Config.
  - f. From the Web Auth Type drop-down list, choose **External**.
  - g. In the URL field that appears, enter the Cisco DNA Spaces splash URL.

<https://splash.dnaspaces.eu/p2/emeabru2>

### Quais são os detalhes do servidor RADIUS para o DNA Spaces ?

Para descobrir quais são os endereços IP do servidor RADIUS que você precisa usar, bem como o segredo compartilhado, vá para a página do Portal cativo na página inicial do DNA Space. Clique em **SSID** no menu esquerdo e, em seguida, clique em **Configure manualmente** em seu SSID.



Na janela pop-up exibida, role para baixo na 3ª seção (RADIUS) e a etapa 7 fornece o IP/porta e o segredo compartilhado para autenticação radius. A contabilidade é opcional e é abordada na etapa 12.

- 7 In the New page that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1812
Secret Key: emeab1299E2PqvJK

- 8 Choose **Radius > Accounting**.

The Radius Accounting Servers page appears.

- 9 From the Acct Called Station ID Type, choose **AP MAC Address:SSID**.

- 10 From the MAC Delimiter drop-down list, choose **Hyphen**.

- 11 Click **New**.

- 12 In the New page that appears, enter the details of the radius server for accounting, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1813
Secret Key: emeab1299E2PqvJK

## Verificar

Para confirmar o status de um cliente conectado ao SSID, navegue para **Monitoring > Clients**, clique no endereço MAC do dispositivo e procure Policy Manager State:

Client	
360 View <b>General</b> QOS Statistics   ATF Statistics   Mobility History   Call Statistics	
Client Properties   AP Properties   Security Information   Client Statistics   QOS Properties	
Wireless LAN Id	1
WLAN Profile Name	9800-DNASpaces1
Wireless LAN Network Name (SSID)	9800-DNASpaces1
BSSID	10b3.d694.00ef
Uptime(sec)	64 seconds
Session Timeout	1800 sec (Remaining time: 1762 sec)
Session Warning Time	Timer not running
Client Active State	Active
Power Save mode	OFF
Current TxRateSet	m2 ss1
Supported Rates	9.0,18.0,36.0,48.0,54.0
Join Time Of Client	03/11/2020 17:47:25 Central
Policy Manager State	Run

## Troubleshoot

### Problemas comuns

1. Se a interface virtual no controlador não tiver endereço IP configurado, os clientes serão redirecionados para o portal interno em vez do portal de redirecionamento configurado no mapa de parâmetros.
2. Se os clientes receberem um *erro 503* enquanto forem redirecionados para o portal nos DNA Spaces, verifique se o controlador está configurado na **Hierarquia de Locais** nos DNA Spaces.

### Rastreamento sempre ativo

O WLC 9800 fornece recursos de rastreamento sempre conectados. Isso garante que todos os erros relacionados à conectividade do cliente, avisos e mensagens de nível de aviso sejam constantemente registrados e que você possa exibir registros de uma condição de incidente ou falha após sua ocorrência.

**Observação:** Dependendo do volume de logs que está sendo gerado, você pode voltar de algumas horas a vários dias.

Para visualizar os rastreamentos que a WLC 9800 coletou por padrão, você pode se conectar via SSH/Telnet à WLC 9800 e executar estas etapas (certifique-se de que esteja registrando a sessão em um arquivo de texto).

Etapa 1. Verifique a hora atual do controlador para que você possa acompanhar os registros no tempo de volta até quando o problema ocorreu.

```
# show clock
```

Etapa 2. Colete syslogs do buffer do controlador ou do syslog externo, conforme ditado pela configuração do sistema. Isso fornece uma visão rápida da integridade do sistema e dos erros, se houver.

```
# show logging
```

Etapa 3. Verifique se as condições de depuração estão ativadas.

```
# show debugging
Cisco IOS-XE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

```
Cisco IOS-XE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address                               Port
-----|-----
```

**Observação:** se você vir qualquer condição listada, isso significa que os rastreamentos estão sendo registrados no nível de depuração para todos os processos que encontram as condições habilitadas (endereço mac, endereço IP, etc.). Isso aumentaria o volume de registros. Portanto, recomenda-se limpar todas as condições quando não estiver depurando ativamente

Etapa 4. Se o endereço mac em teste não foi listado como uma condição na Etapa 3, colete os rastreamentos de nível de aviso sempre ativo para o endereço mac específico.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file
always-on-<FILENAME.txt>
```

Você pode exibir o conteúdo da sessão ou copiar o arquivo para um servidor TFTP externo.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

## Depuração condicional e rastreamento radioativo

Se os rastreamentos sempre ativos não fornecerem informações suficientes para determinar o disparador do problema sob investigação, você poderá habilitar a depuração condicional e capturar o rastreamento de Radio Ative (RA), que fornece rastreamentos no nível de depuração para todos os processos que interagem com a condição especificada (endereço mac do cliente, neste caso). Para habilitar a depuração condicional, siga estas etapas.

Etapa 1. Verifique se não há condições de depuração ativadas.

```
# clear platform condition all
```

Etapa 2. Ative a condição de depuração para o endereço MAC do cliente sem fio que você deseja

monitorar.

Estes comandos começam a monitorar o endereço MAC fornecido por 30 minutos (1.800 segundos). Como alternativa, você pode aumentar esse tempo para até 2.085.978.494 segundos.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

**Observação:** para monitorar mais de um cliente de cada vez, execute o comando `debug wireless mac<aaaa.bbbb.cccc>` por endereço MAC.

**Observação:** você não vê a saída da atividade do cliente na sessão do terminal, pois tudo é armazenado em buffer internamente para ser visualizado posteriormente.

Etapa 3. Reproduza o problema ou comportamento que você deseja monitorar.

Etapa 4. Interrompa as depurações se o problema for reproduzido antes que o tempo de monitoramento padrão ou configurado acabe.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Depois que o `monitor-time` tiver passado ou a conexão sem fio de depuração for interrompida, o 9800 WLC gerará um arquivo local com o nome:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Etapa 5. Colete o arquivo da atividade do endereço MAC. Você pode copiar o registro de rastreamento de RA para um servidor externo ou exibir a saída diretamente na tela.

Verifique o nome do arquivo de rastreamentos de RA

```
# dir bootflash: | inc ra_trace
```

Copie o arquivo para um servidor externo:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log  
tftp://a.b.c.d/ra-FILENAME.txt
```

Mostre o conteúdo:

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

Etapa 6. Se a causa do problema ainda não for evidente, colete os registros internos, que são uma visualização mais detalhada dos registros de nível de depuração. Não é necessário depurar o cliente novamente, pois só examinamos mais detalhadamente os logs de depuração que já foram coletados e armazenados internamente.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> }  
to-file ra-internal-<FILENAME>.txt
```

**Observação:** a saída desse comando retorna rastros para todos os níveis de registro de todos os processos e é bastante volumosa. Entre em contato com o Cisco TAC para ajudar a analisar esses rastreamentos.

Você pode copiar o ra-internal-FILENAME.txt para um servidor externo ou exibir a saída diretamente na tela.

Copie o arquivo para um servidor externo:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Mostre o conteúdo:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Passo 7. Remova as condições de depuração.

```
# clear platform condition all
```

**Observação:** certifique-se de sempre remover as condições de depuração após uma sessão de Troubleshooting.

## Exemplo de uma tentativa bem-sucedida

Esta é a saída de RA\_traces de uma tentativa bem-sucedida de identificar cada uma das fases durante o processo de associação/autenticação durante a conexão a um SSID sem servidor RADIUS.

Associação/autenticação 802.11:

```
Association received. BSSID 10b3.d694.00ee, WLAN 9800DNASpaces, Slot 1 AP 10b3.d694.00e0,
2802AP-9800L
Received Dot11 association request. Processing started,SSID: 9800DNASpaces1, Policy profile:
DNASpaces-PP, AP Name: 2802AP-9800L, Ap Mac Address: 10b3.d694.00e0 BSSID MAC0000.0000.0000 wlan
ID: 1RSSI: 0, SNR: 32
Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
dot11 send association response. Sending association response with resp_status_code: 0
dot11 send association response. Sending assoc response of length: 144 with resp_status_code: 0,
DOT11_STATUS: DOT11_STATUS_SUCCESS
Association success. AID 1, Roaming = False, WGB = False, llr = False, llw = False
DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED
Station Dot11 association is successful
```

Processo de aprendizado de IP:

```
IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
Client IP learn successful. Method: ARP IP: 10.10.30.42
IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
Received ip learn response. method: IPLEARN_METHOD_AR
```

Autenticação da camada 3:

Triggered L3 authentication. status = 0x0, Success  
Client state transition: S\_CO\_IP\_LEARN\_IN\_PROGRESS -> S\_CO\_L3\_AUTH\_IN\_PROGRESS  
L3 Authentication initiated. LWA  
Client auth-interface state transition: S\_AUTHIF\_L2\_WEBAUTH\_DONE -> S\_AUTHIF\_WEBAUTH\_PENDING

Client auth-interface state transition: S\_AUTHIF\_L2\_WEBAUTH\_DONE -> S\_AUTHIF\_WEBAUTH\_PENDING  
[webauth-httpd] [17798]: (info): capwap\_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in INIT state  
[webauth-httpd] [17798]: (info): capwap\_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request  
[webauth-httpd] [17798]: (info): capwap\_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src [10.10.30.42] dst [13.107.4.52] url [http://www.msftconnecttest.com/connecttest.txt]  
[webauth-httpd] [17798]: (info): capwap\_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-agent = Microsoft NCSI  
[webauth-httpd] [17798]: (info): capwap\_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in LOGIN state  
[webauth-httpd] [17798]: (info): capwap\_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request  
[webauth-httpd] [17798]: (info): capwap\_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src [10.10.30.42] dst [151.101.24.81] url [http://www.bbc.com/]  
[webauth-httpd] [17798]: (info): capwap\_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-agent = Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko  
[webauth-httpd] [17798]: (info): capwap\_90000005[34e1.2d23.a668][10.10.30.42]POST rcvd when in LOGIN state

**Autenticação da camada 3 bem-sucedida, mova o cliente para o estado RUN:**

[34e1.2d23.a668:capwap\_90000005] Received User-Name 34E1.2D23.A668 for client 34e1.2d23.a668  
L3 Authentication Successful. ACL:[]  
Client auth-interface state transition: S\_AUTHIF\_WEBAUTH\_PENDING -> S\_AUTHIF\_WEBAUTH\_DONE  
%CLIENT\_ORCH\_LOG-6-CLIENT\_ADDED\_TO\_RUN\_STATE: Username entry (34E1.2D23.A668) joined with ssid (9800DNASpaces) for device with MAC: 34e1.2d23.a668  
Managed client RUN state notification: 34e1.2d23.a668  
Client state transition: S\_CO\_L3\_AUTH\_IN\_PROGRESS -> S\_CO\_RU



## 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.