

Configuración de DNA Spaces Captive Portal con Catalyst 9800 WLC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Conecte el controlador 9800 a Cisco DNA Spaces](#)

[Crear el SSID en espacios de ADN](#)

[Configuración de ACL y filtro de URL en el controlador 9800](#)

[Portal cautivo sin servidor RADIUS en espacios DNA](#)

[Configuración del mapa de parámetro de autenticación web en el controlador 9800](#)

[Cree el SSID en el controlador 9800](#)

[Configuración del perfil de política en el controlador 9800](#)

[Configuración de la etiqueta de política en el controlador 9800](#)

[Portal cautivo con servidor RADIUS en espacios DNA](#)

[Configuración del mapa de parámetro de autenticación web en el controlador 9800](#)

[Configuración de servidores RADIUS en el controlador 9800](#)

[Cree el SSID en el controlador 9800](#)

[Configuración del perfil de política en el controlador 9800](#)

[Configuración de la etiqueta de política en el controlador 9800](#)

[Configurar el mapa de parámetro global](#)

[Crear el portal en espacios de ADN](#)

[Configuración de las reglas del portal cautivo en espacios DNA](#)

[Obtener información específica de DNA Spaces](#)

[¿Cuáles son las direcciones IP que utilizan los espacios de ADN?](#)

[¿Cuál es la URL que utiliza el portal de inicio de sesión de DNA Spaces ?](#)

[¿Cuáles son los detalles del servidor RADIUS para DNA Spaces ?](#)

[Verificación](#)

[Troubleshoot](#)

[Problemas comunes](#)

[Seguimiento siempre activo](#)

[Depuración condicional y seguimiento activo por radio](#)

[Ejemplo de un intento exitoso](#)

Introducción

Este documento describe cómo configurar portales cautivos en Cisco DNA Spaces.

Prerequisites

Este documento permite a los clientes en el controlador de LAN inalámbrica Catalyst 9800 (C9800 WLC) utilizar espacios DNA como una página de login de autenticación web externa.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso mediante interfaz de línea de comandos (CLI) o interfaz gráfica de usuario (GUI) a los controladores inalámbricos 9800
- Espacios de ADN de Cisco

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador 9800-L versión 16.12.2s

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

Antecedentes

La autenticación Web es un método de autenticación de capa 3 simple sin necesidad de un suplicante o una utilidad de cliente. Esto se puede hacer

- a) Con la página interna en C9800 WLC ya sea como está o modificaciones post
- b) Con un paquete de inicio de sesión personalizado cargado en el WLC C9800
- c) Página de inicio de sesión personalizada alojada en un servidor externo

Aprovechar el portal cautivo proporcionado por DNA Spaces es esencialmente una manera de implementar la autenticación web externa para los clientes en C9800 WLC.

El proceso de webauth externo se describe en detalle en:

<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>

En C9800 WLC, la dirección de IP virtual se define como el mapa de parámetros global y es normalmente 192.0.2.1

Configurar

Diagrama de la red



Conecte el controlador 9800 a Cisco DNA Spaces

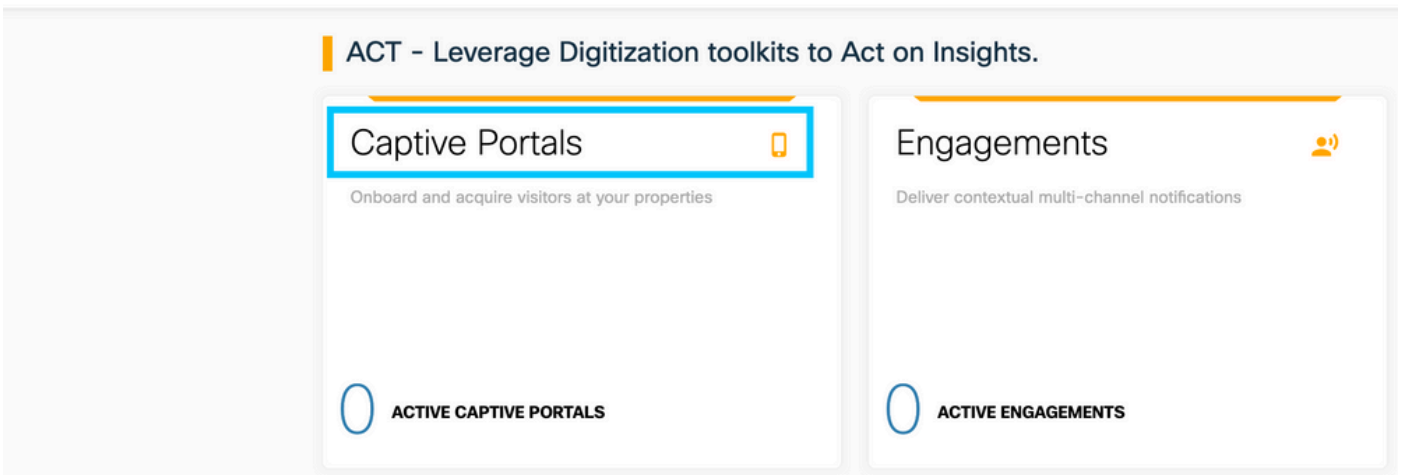
El controlador debe estar conectado a Espacios de ADN con cualquiera de las opciones: Conexión directa, a través del Conector de Espacios de ADN o con anclaje CMX.

En este ejemplo, la opción Conexión directa está en uso, aunque los portales cautivos se configuran de la misma manera para todas las configuraciones.

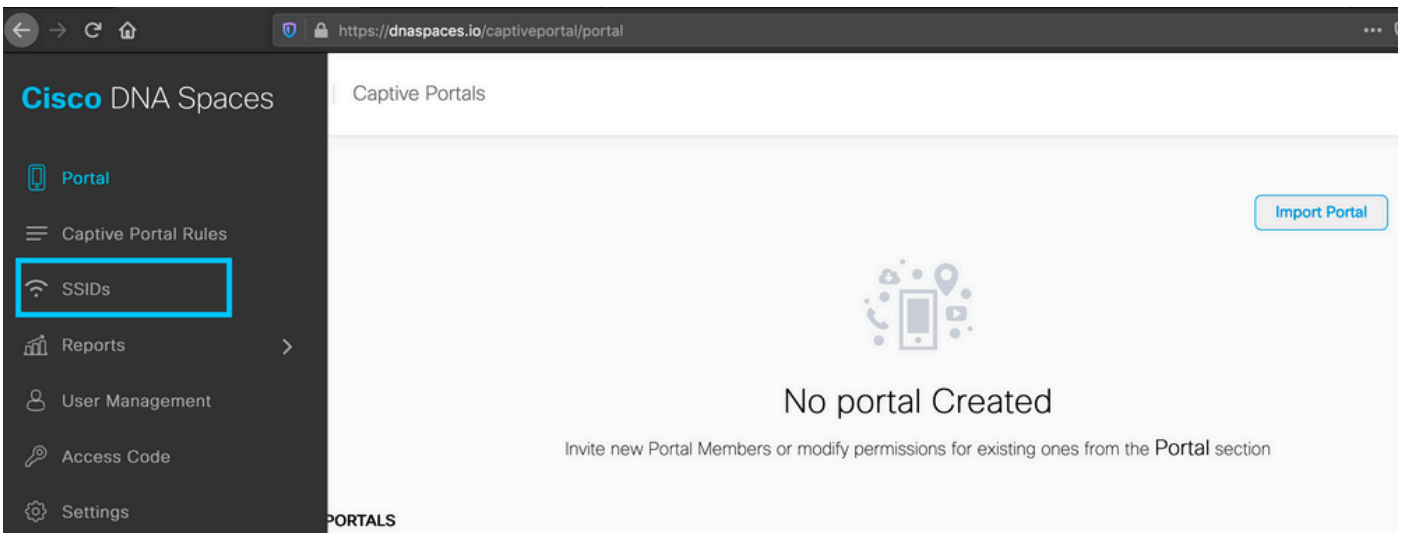
Para conectar el controlador a Cisco DNA Spaces, debe ser capaz de alcanzar Cisco DNA Spaces Cloud sobre HTTPS. Para obtener más información sobre cómo conectar el controlador 9800 a los espacios de DNA, consulte este enlace: [Espacios de DNA - Conexión directa del controlador 9800](#)

Crear el SSID en espacios de ADN

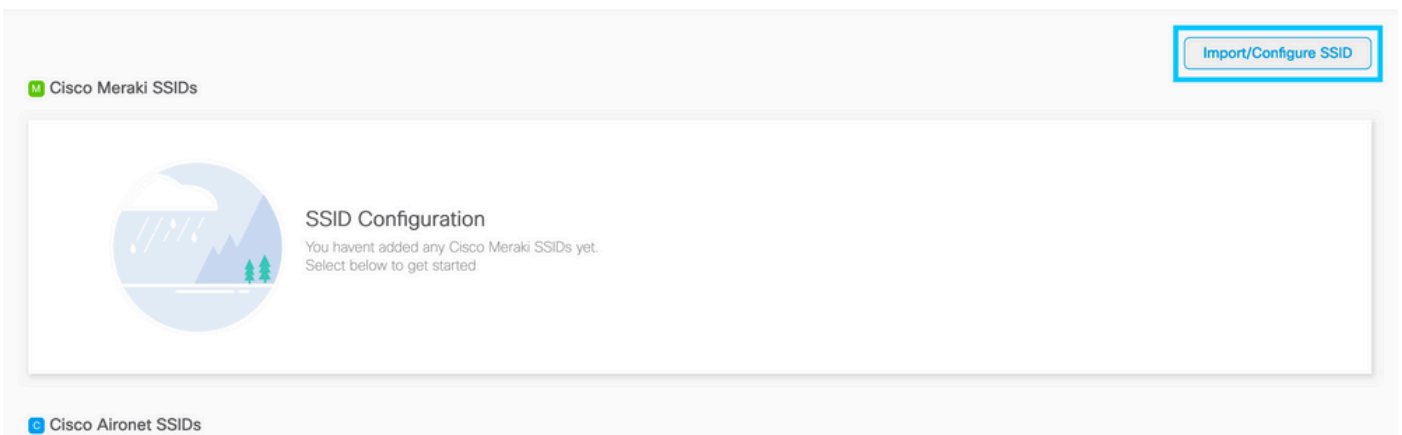
Paso 1. Haga clic en **Portales cautivos** en el panel de Espacios de ADN:



Paso 2. Abra el menú específico del portal cautivo, haga clic en el icono de tres líneas en la esquina superior izquierda de la página y haga clic en **SSIDs**:



Paso 3. Haga clic en **Import/Configure SSID**, seleccione **CUWN (CMX/WLC)** como el tipo "Wireless Network" (Red inalámbrica) e introduzca el nombre de SSID:



Configuración de ACL y filtro de URL en el controlador 9800

No se permite el tráfico de un cliente inalámbrico en la red hasta que se haya completado la autenticación. En el caso de la autenticación web, para completarla, un cliente inalámbrico se

conecta a este SSID, recibe una dirección IP y luego el estado del administrador de políticas de cliente se mueve al estado **Webauth_reqd**. Dado que el cliente aún no está autenticado, se descarta todo el tráfico que se origina en la dirección IP del cliente, excepto DHCP y DNS y HTTP (que se intercepta y redirige).

De forma predeterminada, el 9800 crea ACL preautenticación codificadas cuando configuramos una WLAN de autenticación web. Estas ACL codificadas permiten DHCP, DNS y el tráfico al servidor de autenticación web externo. Todo lo demás se redirige como cualquier tráfico http. Sin embargo, si necesita permitir el paso de un tipo de tráfico no HTTP específico, puede configurar una ACL previa a la autenticación. A continuación, tendría que imitar el contenido de la ACL anterior a la autenticación codificada (del paso 1 de esta sección) y aumentarla según sus necesidades.

Paso 1. Verificar las ACL codificadas actualmente

Configuración 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
```

Se llama a WA-sec-34.235.248.212 como tal porque es una ACL de seguridad (sec) de autenticación web automática o una IP de portal "34.235.248.212". Las ACL de seguridad definieron lo que se permite (al permitir) o se suprime (al denegar)

Wa-v4-int es una ACL de intercepción, es decir, una ACL de punteo o ACL de redirección y define lo que se envía a la CPU para redirección (al permitir) o lo que se envía al plano de datos (al denegar).

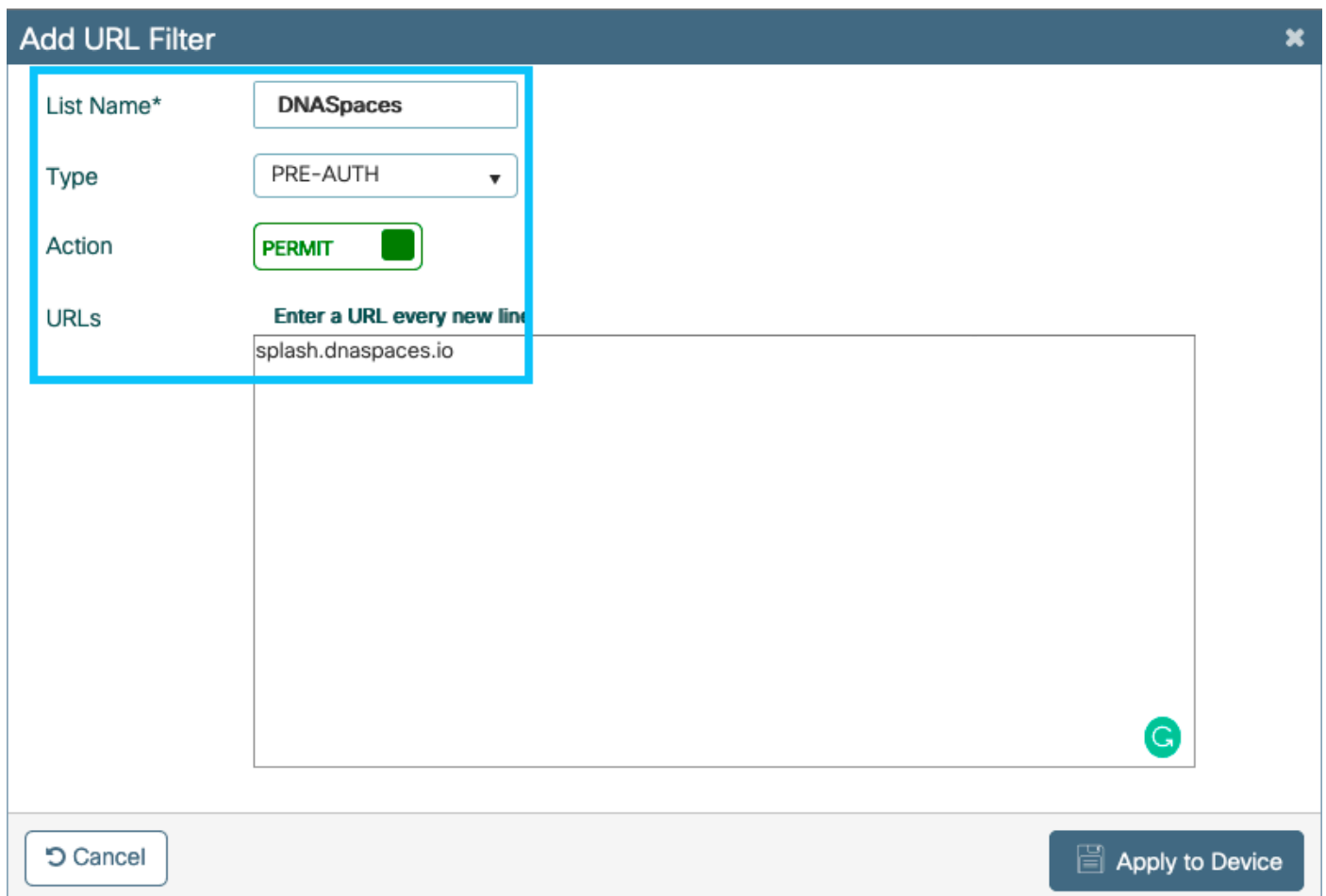
WA-v4-int34.235.248.212 se aplica en primer lugar en el tráfico que viene del cliente y mantiene el tráfico HTTP(s) hacia el portal de DNA Spaces IP 34.235.248.212 en el plano de datos (no descartar o reenviar la acción todavía, simplemente pasar al plano de datos). Envía a la CPU (para la redirección, excepto el tráfico de IP virtual que atiende el servidor web) todo el tráfico HTTP(s). Otros tipos de tráfico se asignan al plano de datos.

WA-sec-34.235.248.212 permite el tráfico HTTP y HTTPS al espacio de ADN IP 34.235.248.212 que configuró en el mapa de parámetros de autenticación web y también permite el tráfico DNS y DHCP y descarta el resto. El tráfico HTTP que se interceptará ya se interceptó antes de que llegue a esta ACL y, por lo tanto, no necesita estar cubierto por esta ACL.

Nota: Para obtener las direcciones IP de los Espacios de ADN que se permitirán en la ACL, haga clic en la opción **Configure Manually** del SSID creado en el paso 3 de la sección **Create the SSID on DNA Spaces bajo la sección de configuración de ACL**. Un ejemplo se encuentra en la sección "Cuáles son las direcciones IP que utilizan los Espacios de ADN" al final del documento.

DNA Spaces utiliza 2 direcciones IP y el mecanismo del paso 1 sólo permite que se permita una IP de portal. Para permitir el acceso de autenticación previa a más recursos HTTP, debe utilizar filtros de URL que de forma dinámica hagan agujeros en las ACL de intercepción (redireccionamiento) y seguridad (preautenticación) para las IP relacionadas con el sitio web cuya URL introduzca en el filtro de URL. Las solicitudes de DNS se sondean dinámicamente para que el 9800 detecte la dirección IP de esas URL y la agregue a las ACL dinámicamente.

Paso 2. Configure el filtro de URL para permitir el dominio Espacios de ADN. Navegue hasta Configuration > Security > URL Filters, haga clic en **+Add** y configure el nombre de la lista, seleccione **PRE-AUTH** como tipo, action as **PERMIT** y la URL splash.dnaspaces.io (o .eu si utiliza el portal EMEA):



Configuración de CLI:

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

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

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

El SSID se puede configurar para utilizar un servidor RADIUS o sin él. Si esa Duración de sesión, Límite de ancho de banda o Provisión fluida de Internet se configura en la sección **Acciones** de la configuración de Regla de portal cautivo, el SSID debe configurarse con un servidor RADIUS; de lo contrario, no es necesario utilizar el servidor RADIUS. En ambas configuraciones se admiten todo tipo de portales en espacios DNA.

Portal cautivo sin servidor RADIUS en espacios DNA

Configuración del mapa de parámetro de autenticación web en el controlador 9800

Paso 1. Navegue hasta **Configuration > Security > Web Auth**, haga clic en **+Add** para crear un nuevo mapa de parámetro. En la ventana emergente, configure el nombre del mapa de parámetro y seleccione **Consent** como el tipo:

Create Web Auth Parameter

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

Close Apply to Device

Paso 2. Haga clic en el mapa de parámetros configurado en el paso anterior, navegue hasta la pestaña **Advanced** e ingrese el URL de redireccionamiento para el login, Append for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID and portal IPv4 Address como se ilustra. Haga clic en 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

Nota: Para obtener la URL de la página de bienvenida y la dirección de redirección IPv4, haga clic en la opción **Configure Manually** (Configurar manualmente) de la página SSID de DNA Spaces (Espacios de ADN). Esto se ilustra en la sección "¿Cuál es la URL que el portal DNA Spaces utiliza?" al final del documento

Nota: El portal Cisco DNA Spaces puede resolver a dos direcciones IP, pero el controlador 9800 permite que se configure solamente una dirección IP, elija cualquiera de esas direcciones IP y configúrela en el mapa de parámetros como la dirección IPv4 del portal.

Nota: asegúrese de que las direcciones IPv4 e IPv6 virtuales se configuran en el mapa de parámetros de autenticación web global,. Si el IPv6 virtual no está configurado, los clientes a veces se redirigen al portal interno en lugar del portal de espacios de ADN configurado. Por este motivo, siempre debe configurarse una IP virtual. "192.0.2.1" se puede configurar como IPv4 virtual y FE80:0:0:903A::11E4 como IPV6 virtual. Hay pocas o ninguna razón para utilizar otras IPs además de esas.

Configuración 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
```

Cree el SSID en el controlador 9800

Paso 1. Vaya a **Configuration > Tags & Profiles > WLANs**, haga clic en **+Add**. Configure el nombre del perfil, SSID y habilite la WLAN. Asegúrese de que el nombre SSID es el mismo nombre que el configurado en el paso 3 de la sección **Creación del SSID en Espacios de ADN**.

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

Paso 2. Vaya a **Seguridad > Capa 2**. Establezca el Modo de seguridad de capa 2 en **Ninguno**, asegúrese de que el Filtrado de MAC está desactivado.

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

Paso 3. Vaya a **Seguridad > Capa 3**. Habilite la política web y configure el mapa de parámetro de autenticación web. Haga clic en **Aplicar al dispositivo**.

Edit WLAN ✕

General
Security
Advanced
Add To Policy Tags

Layer2
Layer3
AAA

[Show Advanced Settings >>>](#)

Web Policy

Web Auth Parameter Map DNASpacesPM ▼

Authentication List Select a value ▼ ⓘ

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

Configuración del perfil de política en el controlador 9800

Paso 1. Vaya a **Configuration > Tags & Profiles > Policy** y cree un nuevo perfil de política o utilice el perfil de política predeterminado. En la pestaña Políticas de acceso, configure la VLAN del cliente y agregue el filtro de URL.

Edit Policy Profile ✕

General
Access Policies
QOS and AVC
Mobility
Advanced

RADIUS Profiling

Local Subscriber Policy Name Search or Select ▼

WLAN Local Profiling

Global State of Device Classification Disabled ⓘ

HTTP TLV Caching

DHCP TLV Caching

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 ▼

Configuración de la etiqueta de política en el controlador 9800

Paso 1. Vaya a **Configuration > Tags & Profiles > Policy** . Cree una nueva etiqueta de directiva o utilice la etiqueta de directiva predeterminada. Asigne la WLAN al perfil de política en la 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

Paso 2. Aplique la etiqueta de política al AP para difundir el SSID. Vaya a **Configuration > Wireless > Access Points**, seleccione el AP en cuestión y agregue la etiqueta de política. Esto hace que el AP reinicie su túnel CAPWAP y vuelva a unirse al 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

Configuración 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
```

```
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
```

Portal cautivo con servidor RADIUS en espacios DNA

Nota: El servidor RADIUS de Espacios de ADN sólo soporta la autenticación PAP proveniente del controlador.

Configuración del mapa de parámetro de autenticación web en el controlador 9800

Paso 1. Cree un mapa de parámetro de autenticación Web. Navegue hasta **Configuration > Security > Web Auth**, haga clic en **+Add**, configure el nombre del mapa de parámetro y seleccione **webauth** como el 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

Paso 2. Haga clic en el mapa de parámetros configurado en el paso 1, haga clic en **Advanced** e ingrese el Redireccionamiento para el inicio de sesión, Append for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID and portal IPv4 Address. Haga clic en **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

Nota: Para obtener la URL de la página de inicio y la dirección de redirección IPv4, haga clic en la opción **Configure Manually** del SSID creado en el paso 3 de la sección **Create the SSID on DNA Spaces** bajo la sección **Creating the SSIDs in WLC Direct Connect** sección **Creating the Access Control List configuration** respectivamente.

Nota: El portal Cisco DNA Spaces puede resolver a dos direcciones IP, pero el controlador 9800 permite que se configure solamente una dirección IP; en un caso, elija cualquiera de esas direcciones IP para configurarse en el mapa de parámetros como la dirección IPv4 del portal.

Nota: Asegúrese de que las direcciones IPv4 e IPv6 virtuales estén configuradas en el mapa de parámetros de autenticación web global. Si no se configura el IPv6 virtual, a veces los clientes se redirigen al portal interno en lugar del portal de espacios de DNA configurado. Por este motivo, siempre debe configurarse una IP virtual. "192.0.2.1" se puede configurar como IPv4 virtual y FE80:0:0:0:903A::11E4 como IPV6 virtual. Hay pocas o ninguna razón para utilizar otras IPs además de esas.

Configuración de CLI:

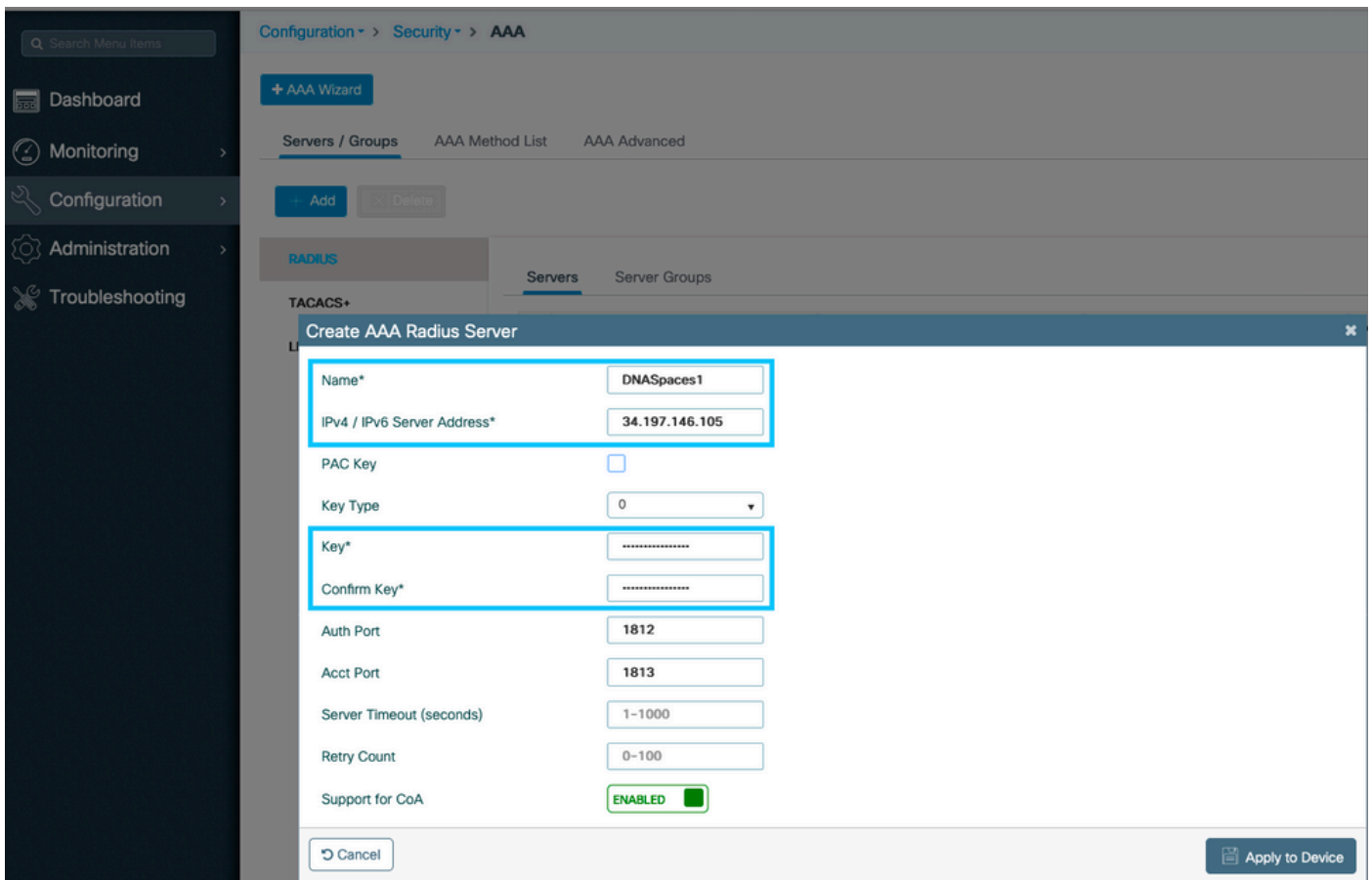
```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type webauth
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
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
```

Configuración de servidores RADIUS en el controlador 9800

Paso 1. Configure los servidores RADIUS. Cisco DNA Spaces actúa como servidor RADIUS para la autenticación de usuarios y puede responder en dos direcciones IP. Navegue hasta **Configuration > Security > AAA**, haga clic en **+Add** y configure ambos servidores RADIUS:



Nota: Para obtener la dirección IP de RADIUS y la clave secreta para los servidores primario y secundario, haga clic en la opción **Configure Manually** del SSID creado en el paso 3 de la sección **Create the SSID on DNA Spaces** y navegue hasta la sección **RADIUS Server Configuration**.

Paso 2. Configure el grupo de servidores RADIUS y agregue ambos servidores RADIUS. Navegue hasta **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups**, haga clic en **+add**, configure el nombre del grupo de servidores, MAC-Delimiter as **Hyphen**, MAC-Filtering as **MAC**, y asigne los dos 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

>

<

Assigned Servers

DNASpaces1
DNASpaces2

Cancel

Apply to Device

Paso 3. Configure una lista de métodos de autenticación. Navegue hasta **Configuration > Security > AAA > AAA Method List > Authentication**, haga clic en **+add**. Configure el nombre de la lista de métodos, seleccione **login** como tipo y asigne el 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

Paso 4. Configure una lista de métodos de autorización. Vaya a **Configuration > Security > AAA > AAA Method List > Authorization**, haga clic en **+add**. Configure el nombre de la lista de métodos, seleccione **network** como tipo y asigne el 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

Cree el SSID en el controlador 9800

Paso 1. Vaya a **Configuration > Tags & Profiles > WLANs**, haga clic en **+Add**. Configure el nombre del perfil, SSID y habilite la WLAN. Asegúrese de que el nombre SSID es el mismo nombre que el configurado en el paso 3 de la sección **Creación del SSID en Espacios de ADN**.

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

Paso 2. Vaya a **Seguridad > Capa 2**. Establezca el Modo de Seguridad de Capa 2 en **Ninguno**, habilite el Filtrado MAC y agregue la Lista de Autorización:

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

Paso 3. Vaya a **Seguridad > Capa 3**. Habilite la política web, configure el mapa de parámetro de autenticación web y la lista de autenticación. Habilite On Mac Filter Failure y agregue la ACL de autenticación previa. Haga clic en **Aplicar al dispositivo**.

Add WLAN ✕

General
Security
Advanced

Layer2
Layer3
AAA

Web Policy

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

Splash Web Redirect DISABLED

Preauthentication ACL

IPv4 DNASpaces-ACL

IPv6 None

↶ Cancel

📄 Apply to Device

Configuración del perfil de política en el controlador 9800

Paso 1. Vaya a **Configuration > Tags & Profiles > Policy** y cree un nuevo perfil de política o utilice el perfil de política predeterminado. En la pestaña Políticas de acceso, configure la VLAN del cliente y agregue el filtro de URL.

Edit Policy Profile ✕

General
Access Policies
QOS and AVC
Mobility
Advanced

RADIUS Profiling

Local Subscriber Policy Name Search or Select

WLAN Local Profiling

Global State of Device Classification Disabled ⓘ

HTTP TLV Caching

DHCP TLV Caching

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

Paso 2. En la ficha Advanced (Avanzado), active AAA Override (Anulación de AAA) y, opcionalmente, configure la lista de métodos de contabilidad:

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

Configuración de la etiqueta de política en el controlador 9800

Paso 1. Vaya a **Configuration > Tags & Profiles > Policy** . Cree una nueva etiqueta de directiva o utilice la etiqueta de directiva predeterminada. Asigne la WLAN al perfil de política en la 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

Paso 2. Aplique la etiqueta de política al AP para difundir el SSID. Vaya a **Configuration > Wireless > Access Points**, seleccione el AP en cuestión y agregue la etiqueta de política. Esto hace que el AP reinicie su túnel CAPWAP y vuelva a unirse al controlador 9800:

General

AP Name*	9117-andressi
Location*	default location
Base Radio MAC	0cd0.f894.f2c0
Ethernet MAC	0cd0.f894.118c
Admin Status	ENABLED <input checked="" type="checkbox"/>
AP Mode	Local ▼
Operation Status	Registered
Fabric Status	Disabled
LED State	ENABLED <input checked="" type="checkbox"/>
LED Brightness Level	8 ▼
CleanAir NSI Key	

Tags

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

Policy	DNASpaces-PT ▼
Site	default-site-tag ▼
RF	default-rf-tag ▼

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"/>

Time Statistics

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

Configuración 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 el mapa de parámetro global

Paso no recomendado: ejecute estos comandos para permitir la redirección HTTPS, pero tenga en cuenta que la redirección en el tráfico HTTPS del cliente no es necesaria si el sistema operativo del cliente realiza una detección de portal cautivo y provoca un uso más intenso de la CPU y siempre emite una advertencia de certificado. Por lo tanto, se recomienda evitar configurarlo a menos que sea necesario para un caso práctico muy específico.

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

Nota: Debe tener un certificado SSL válido para la IP virtual instalada en el controlador inalámbrico Catalyst de Cisco serie 9800.

Paso 1. Copie el archivo certificado firmado con la extensión .p12 en un servidor TFTP y ejecute este comando para transferir e instalar el certificado en el controlador 9800:

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

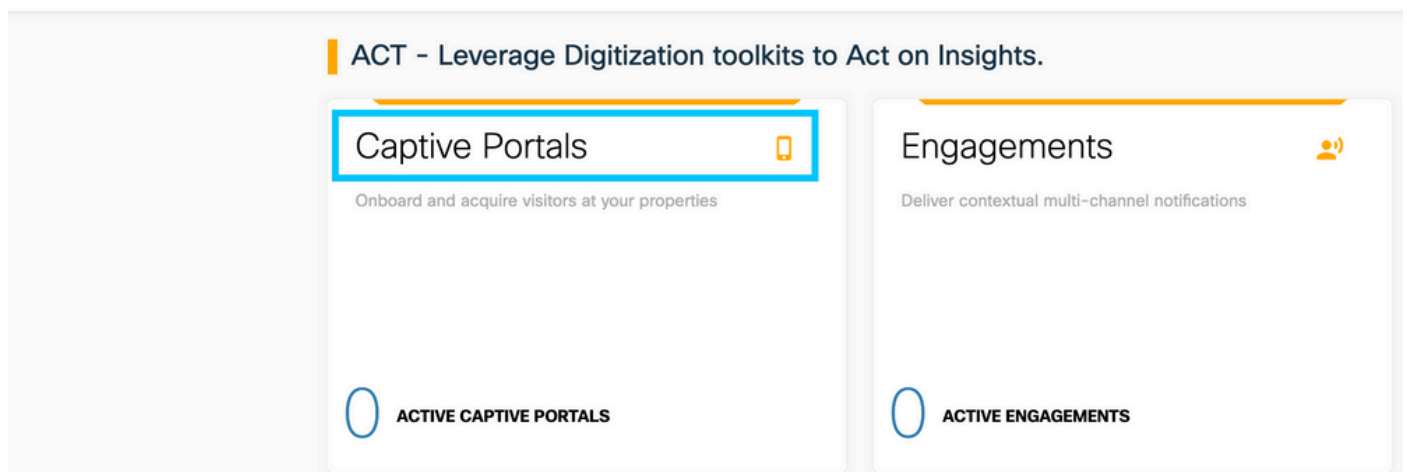
Paso 2. Para asignar el certificado instalado al mapa de parámetro de autenticación web, ejecute estos comandos:

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

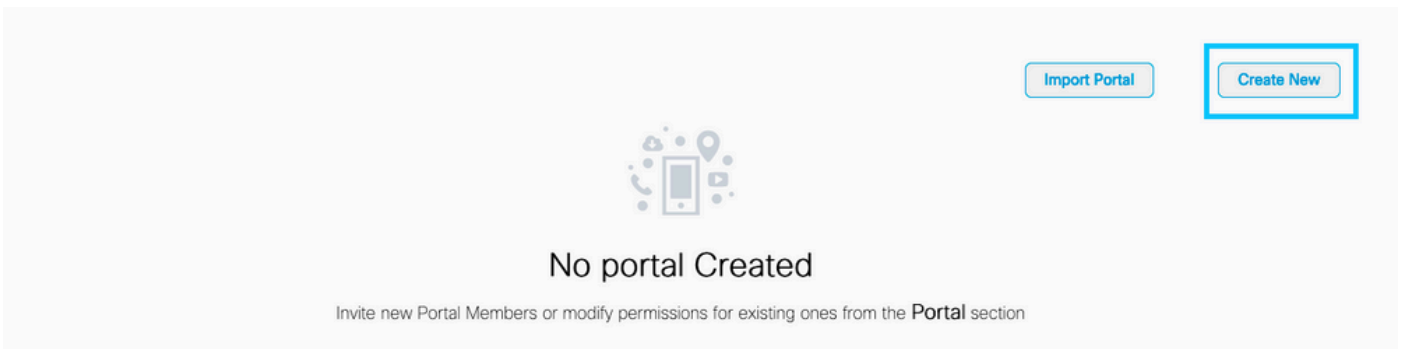
Crear el portal en espacios de ADN

Paso 1. Haga clic en **Portales cautivos** en el panel de Espacios de ADN:

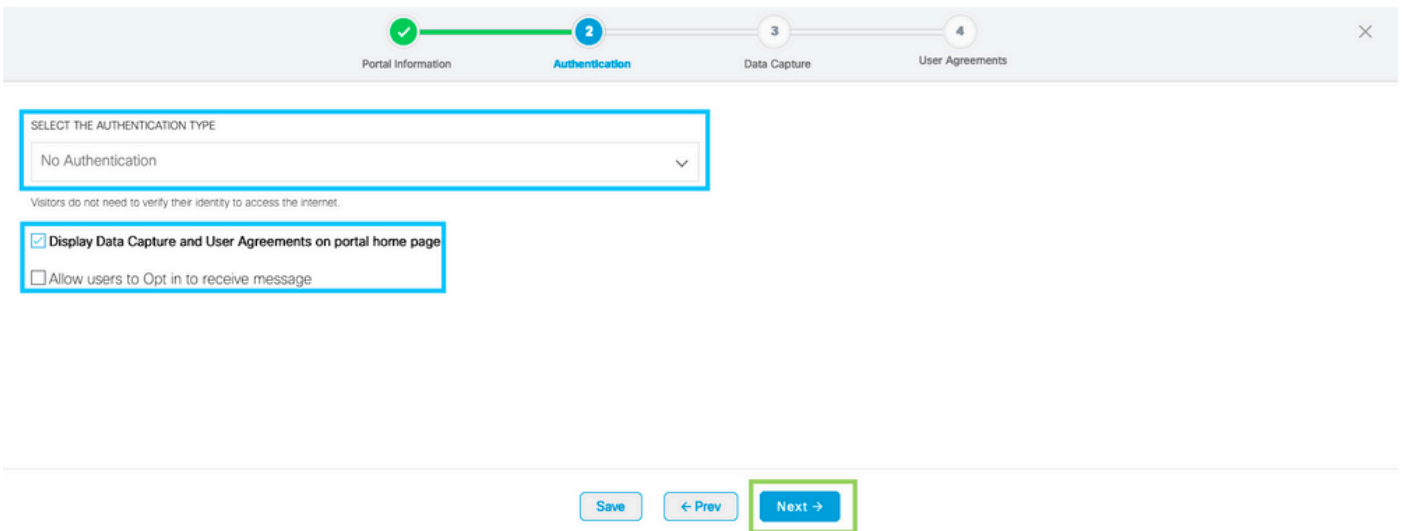
☰ Cisco DNA Spaces **ACT**



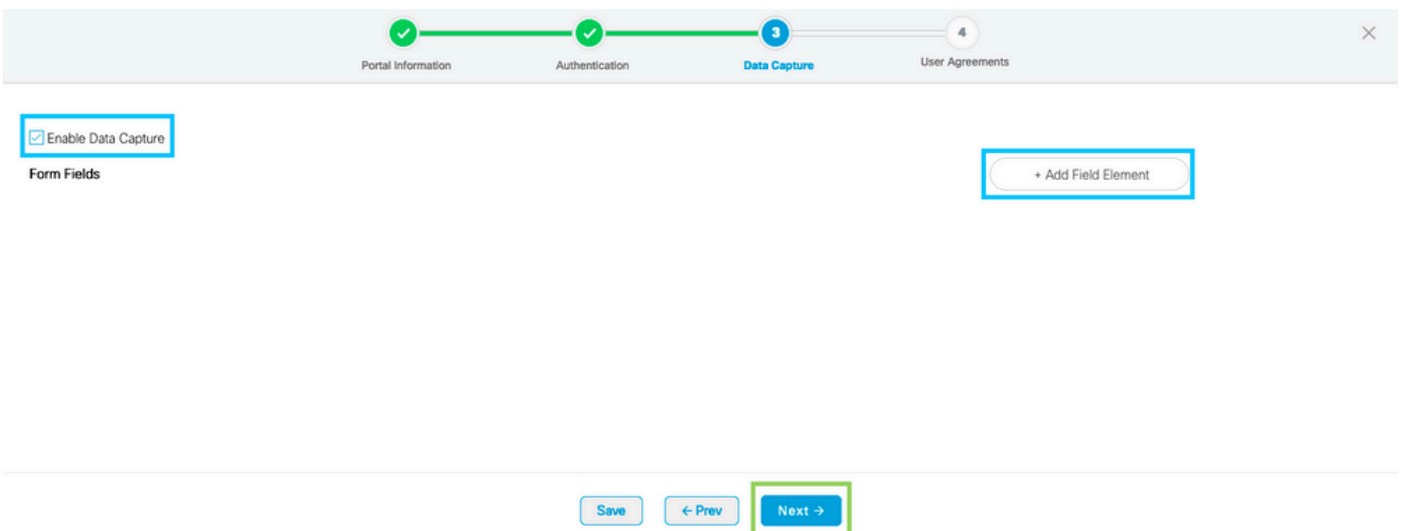
Paso 2. Haga clic en **Create New**, ingrese el nombre del portal y seleccione las ubicaciones que pueden utilizar el portal:



Paso 3. Seleccione el tipo de autenticación, elija si desea mostrar la captura de datos y los acuerdos de usuario en la página principal del portal y si los usuarios pueden participar para recibir un mensaje. Haga clic en Next (Siguiendo):



Paso 4. Configurar elementos de captura de datos. Si desea capturar datos de los usuarios, marque la casilla **Enable Data Capture** y haga clic en **+Add Field Element** para agregar los campos deseados. Haga clic en Next (Siguiendo):



Paso 5. Marque la opción **Enable Terms & Conditions** y haga clic en **Save & Configure 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, Undo, Redo, Link, Unlink, Image, Table, Media, Font size, Font color, Text background color, Text 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**

Paso 6. Edite el portal según sea necesario, haga clic en **Guardar**:

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

Configuración de las reglas del portal cautivo en espacios DNA

Paso 1. Haga clic en **Portales cautivos** en el panel de Espacios de ADN:

ACT - Leverage Digitization toolkits to Act on Insights.

Captive Portals

Onboard and acquire visitors at your properties

0 **ACTIVE CAPTIVE PORTALS**

Engagements

Deliver contextual multi-channel notifications

0 **ACTIVE ENGAGEMENTS**

Paso 2. Abra el menú del portal cautivo y haga clic en **Reglas del portal cautivo**:

The screenshot shows the Cisco DNA Spaces interface. On the left, a dark sidebar menu is open, with 'Captive Portal Rules' highlighted in blue. The main content area shows the 'Captive Portals' page with a table of rules. One rule is visible: '9800DNASpaces1' with a status of 'Draft' and a last modified date of 'Feb 18, 2020'. There are 'Import Portal' and 'Create New' buttons at the top right.

Paso 3. Haga clic en **+ Crear nueva regla**. Introduzca el nombre de la regla y seleccione el SSID configurado anteriormente.

The screenshot shows the 'Create Captive Portal Rule' form. At the top, there is a back arrow and the title 'Create Captive Portal Rule'. A text input field for 'RULE NAME' contains '9800DNASpaces'. Below this, a section titled 'Choose any or all of the options that apply to your rule below' contains a dropdown menu for 'When a user is on' set to 'WiFi' and another dropdown for 'and connected to' set to '9800-DNASpaces1'. A section titled 'LOCATIONS - Where do you want the rule to fire?' contains the text 'At any of the following locations' and a '+ Add Locations' button. A note at the bottom says 'Please select at-least one location'.

Paso 4. Seleccione las ubicaciones en las que está disponible el portal. Haga clic en **+ Add Locations** en la sección **LOCATIONS**. Elija el que desee en la jerarquía de ubicaciones.

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

Paso 5. Elija la acción del portal cautivo. En este caso, cuando se alcanza la regla, se muestra el portal. Haga clic en **Guardar y 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

Obtener información específica de DNA Spaces

¿Cuáles son las direcciones IP que utilizan los espacios de ADN?

Para verificar qué direcciones IP utilizan los Espacios de ADN para el portal en su región, vaya a la página Portal del Festival en la página de inicio de Espacio de ADN. Haga clic en **SSID** en el menú de la izquierda y luego haga clic en **Configure manually** bajo su SSID. Las direcciones IP se mencionan en el ejemplo de ACL. Ésas son las direcciones IP del portal para su uso en ACL y mapa de parámetros de webauth. Los espacios de ADN utilizan otras direcciones IP para la conectividad general de NMSP/nube del plano de control.



En la primera sección de la ventana emergente que aparece, el paso 7 muestra las direcciones IP mencionadas en la definición de ACL. No es necesario que siga estas instrucciones y cree ninguna lista de control de acceso, simplemente tome nota de las direcciones IP. Estas son las IP que utiliza el portal en su zona

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

¿Cuál es la URL que utiliza el portal de inicio de sesión de DNA Spaces ?

Para verificar qué espacio de ADN de URL de portal de inicio de sesión utiliza para el portal en su región, vaya a la página Portal del Festival en la página de inicio de espacio de ADN. Haga clic en **SSID** en el menú de la izquierda y luego haga clic en **Configure manually** bajo su SSID.



Desplácese hacia abajo en la ventana emergente que aparece y, en la segunda sección, el paso 7 muestra la URL que debe configurar en el mapa de parámetros del 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>

¿Cuáles son los detalles del servidor RADIUS para DNA Spaces ?

Para averiguar cuáles son las direcciones IP del servidor RADIUS que necesita utilizar, así como el secreto compartido, vaya a la página Portal del Festival en la página de inicio de DNA Space. Haga clic en **SSID** en el menú de la izquierda y luego haga clic en **Configure manually** bajo su SSID.



En la ventana emergente que aparece, desplácese hacia abajo en la tercera sección (RADIUS) y el paso 7 le proporciona la dirección IP/puerto y el secreto compartido para la autenticación de RADIUS. La contabilidad es opcional y se trata en el paso 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

Verificación

Para confirmar el estado de un cliente conectado al SSID, navegue hasta **Monitoring > Clients**, haga clic en la dirección MAC del dispositivo y busque Policy Manager State:

Client	
360 View General 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 comunes

1. Si la interfaz virtual en el controlador no tiene ninguna dirección IP configurada, los clientes se redirigen al portal interno en lugar del portal de redirección configurado en el mapa de parámetros.
2. Si los clientes reciben un *error 503* mientras son redirigidos al portal en Espacios de ADN, asegúrese de que el controlador esté configurado en la **Jerarquía de Ubicación** en Espacios de ADN.

Seguimiento siempre activo

El WLC 9800 ofrece capacidades de seguimiento SIEMPRE ACTIVAS. Esto garantiza que todos los mensajes de nivel de aviso, advertencia y errores relacionados con la conectividad del cliente se registren constantemente y que pueda ver los registros de una condición de incidente o falla después de que haya ocurrido.

Nota: Dependiendo del volumen de registros que se generen, puede retroceder unas horas a varios días.

Para ver los seguimientos que el WLC 9800 recolectó por defecto, puede conectarse vía SSH/Telnet al WLC 9800 y hacer estos pasos (asegúrese de que está registrando la sesión en un archivo de texto).

Paso 1. Compruebe la hora actual del controlador para poder realizar un seguimiento de los registros en el tiempo hasta el momento en que ocurrió el problema.

```
# show clock
```

Paso 2. Recopile registros del sistema del buffer del controlador o del registro del sistema externo según lo dicte la configuración del sistema. Esto proporciona una vista rápida del estado del sistema y de los errores, si los hubiera.

```
# show logging
```

Paso 3. Verifique si hay alguna condición de depuración habilitada.

```
# 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
-----|-----
```

Nota: Si ve alguna condición en la lista, significa que los seguimientos se están registrando en el nivel de depuración para todos los procesos que encuentran las condiciones habilitadas (dirección MAC, dirección IP, etc.). Esto aumenta el volumen de registros. Por lo tanto, se recomienda borrar todas las condiciones cuando no se depura activamente.

Paso 4. Si la dirección MAC en prueba no se incluyó como condición en el Paso 3, recopile los seguimientos del nivel de aviso siempre activo para la dirección MAC específica.

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

Puede mostrar el contenido de la sesión o copiar el archivo en un 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>
```

Depuración condicional y seguimiento activo por radio

Si los seguimientos siempre activos no proporcionan suficiente información para determinar el desencadenador del problema que se está investigando, puede habilitar la depuración condicional y capturar el seguimiento de Radio Activo (RA), que proporciona seguimientos de nivel de depuración para todos los procesos que interactúan con la condición especificada (dirección MAC del cliente en este caso). Para habilitar la depuración condicional, siga estos pasos.

Paso 1. Asegúrese de que no haya condiciones de depuración habilitadas.

```
# clear platform condition all
```

Paso 2. Habilite la condición de depuración para la dirección MAC del cliente inalámbrico que desea monitorear.

Estos comandos comienzan a monitorear la dirección MAC proporcionada durante 30 minutos (1800 segundos). Opcionalmente, puede aumentar este tiempo hasta 2 085 978 494 segundos.

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

Nota: Para monitorear más de un cliente a la vez, ejecute el comando `debug wireless mac<aaaa.bbbb.cccc>` por dirección MAC.

Nota: Usted no ve el resultado de la actividad del cliente en la sesión de terminal, ya que todo se almacena en buffer internamente para ser visto más tarde.

Paso 3. Reproduzca el problema o el comportamiento que desea monitorear.

Paso 4. Detenga las depuraciones si el problema se reproduce antes de que se agote el tiempo de monitoreo predeterminado o configurado.

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

Una vez que ha transcurrido el tiempo de monitoreo o se ha detenido la depuración inalámbrica, el WLC 9800 genera un archivo local con el nombre:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Paso 5. Recopile el archivo de la actividad de la dirección MAC. Puede copiar el archivo de seguimiento activo por radio .log en un servidor externo o mostrar el resultado directamente en la pantalla.

Verifique el nombre del archivo de seguimiento activo por radio

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

Copie el archivo en un servidor externo:

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

Muestre el contenido:

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

Paso 6. Si la causa raíz aún no es obvia, recopile los registros internos, que son una vista más detallada de los registros de nivel de depuración. No es necesario depurar el cliente de nuevo, ya que solo examinamos con más detalle los registros de depuración que ya se han recopilado y almacenado internamente.

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

Nota: Esta salida de comando devuelve seguimientos para todos los niveles de registro para todos los procesos y es bastante voluminosa. Utilice Cisco TAC para analizar estos seguimientos.

Puede copiar ra-internal-FILENAME.txt en un servidor externo o mostrar el resultado directamente en la pantalla.

Copie el archivo en un servidor externo:

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

Muestre el contenido:

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

Paso 7. Elimine las condiciones de depuración.

```
# clear platform condition all
```

Nota: Asegúrese de eliminar siempre las condiciones de depuración después de una sesión de troubleshooting.

Ejemplo de un intento exitoso

Este es el resultado de RA_traces para un intento exitoso de identificar cada una de las fases durante el proceso de asociación/autenticación mientras se conecta a un SSID sin servidor RADIUS.

Asociación/autenticación 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, 11r = False, 11w = False
DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED
Station Dot11 association is successful
```

Proceso de aprendizaje 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
```

Autenticación de capa 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

Autenticación de capa 3 exitosa, mueva el cliente al 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

Acerca de esta traducción

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

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

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