

Ejemplo de Configuración de DNA Spaces Captive Portal con Controlador AireOS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Conecte el WLC a Cisco DNA Spaces](#)

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

[Configuración de ACL en el controlador](#)

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

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

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

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

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar portales cautivos usando Cisco DNA Spaces con un controlador AireOS.

Colaboración de Andrés Silva, ingeniero del TAC de Cisco.

Prerequisites

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
- Espacios de ADN de Cisco

Componentes Utilizados

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

- Controlador de LAN inalámbrica 5520, versión 8.10.112.0

Configurar

Diagrama de la red



DNA Spaces




y configure las reglas para permitir la comunicación entre los clientes inalámbricos a los Espacios de ADN de la siguiente manera. Reemplace las direcciones IP por las direcciones proporcionadas por DNA Spaces para la cuenta en uso:

General

Access List Name: DNASpaces-ACL

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	34.235.248.212 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
2	Permit	34.235.248.212 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	52.55.235.39 / 255.255.255.255	Any	Any	Any	Any	Any	0
4	Permit	52.55.235.39 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

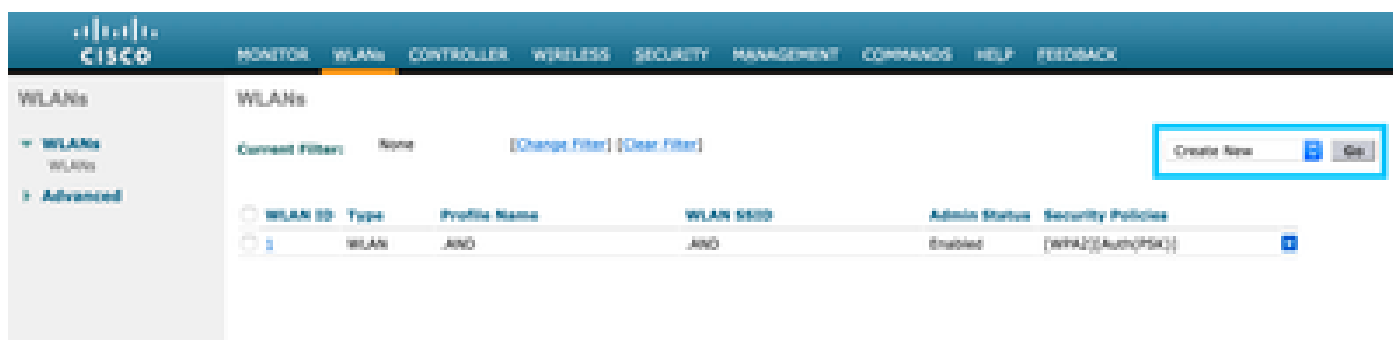
 Nota: Para obtener las direcciones IP de los Espacios de ADN que se permitirán en la ACL, haga clic en la opción Configure Manually del SSID creado en el paso 3 de la sección Create the SSID on DNA Spaces bajo la sección de configuración de ACL.

El SSID se puede configurar para utilizar un servidor RADIUS o sin él. Si la duración de la sesión, el límite de ancho de banda o el aprovisionamiento de Internet sin problemas se configuran en la sección Acciones de la configuración de la 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.

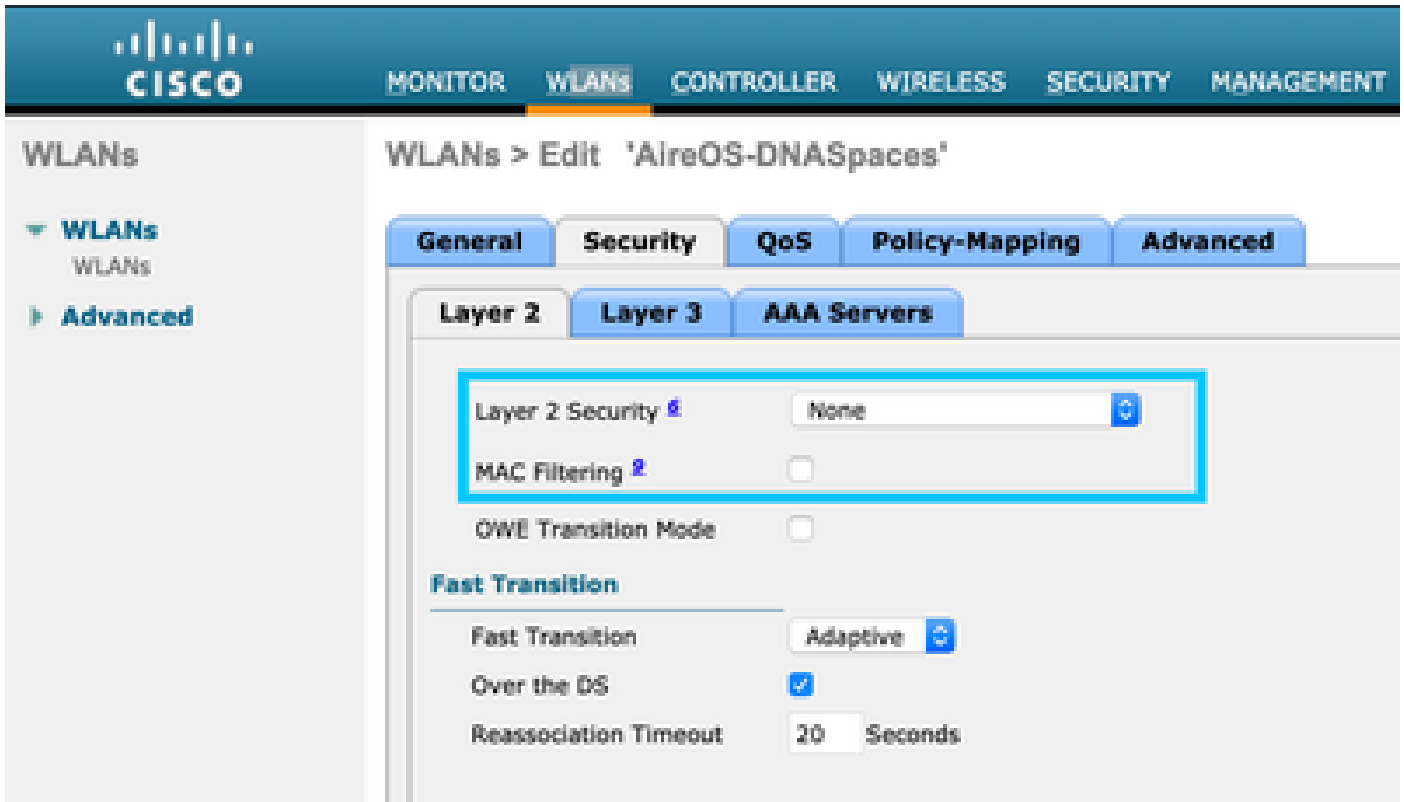
Portal cautivo sin servidor RADIUS en espacios DNA

Configuración de SSID en el controlador

Paso 1. Vaya a WLAN > WLANs. Cree una nueva WLAN. Configure el nombre del perfil y el SSID. Asegúrese de que el nombre SSID es el mismo que el configurado en el paso 3 de la sección Creación del SSID en Espacios de ADN.




Paso 2. Configuración de la seguridad de capa 2. Vaya a la pestaña Security > Layer 2 en la pestaña WLAN configuration y seleccione as None en el menú desplegable Layer 2 Security. Asegúrese de que el filtrado de MAC está desactivado.




Paso 3. Configuración de la seguridad de capa 3. Navegue hasta la pestaña Security > Layer 3 en la pestaña de configuración WLAN, configure la política web como el método de seguridad de la capa 3, habilite Passthrough, configure la ACL de preautenticación, habilite Override Global Config como set the Web Auth Type as External, configure la URL de redirección.



 Nota: Para obtener la URL de redirección, haga clic en la opción Configure Manually (Configurar manualmente) del SSID creado en el paso 3 de la sección Create the SSID on DNA Spaces (Crear el SSID en espacios de ADN), en la sección de configuración de SSID.

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 de servidores RADIUS en el controlador

Paso 1. Navegue hasta Seguridad > AAA > RADIUS > Autenticación, haga clic en Nuevo e ingrese la información del servidor RADIUS. Cisco DNA Spaces actúa como servidor RADIUS para la autenticación de usuarios y puede responder en dos direcciones IP. Configure ambos servidores RADIUS:

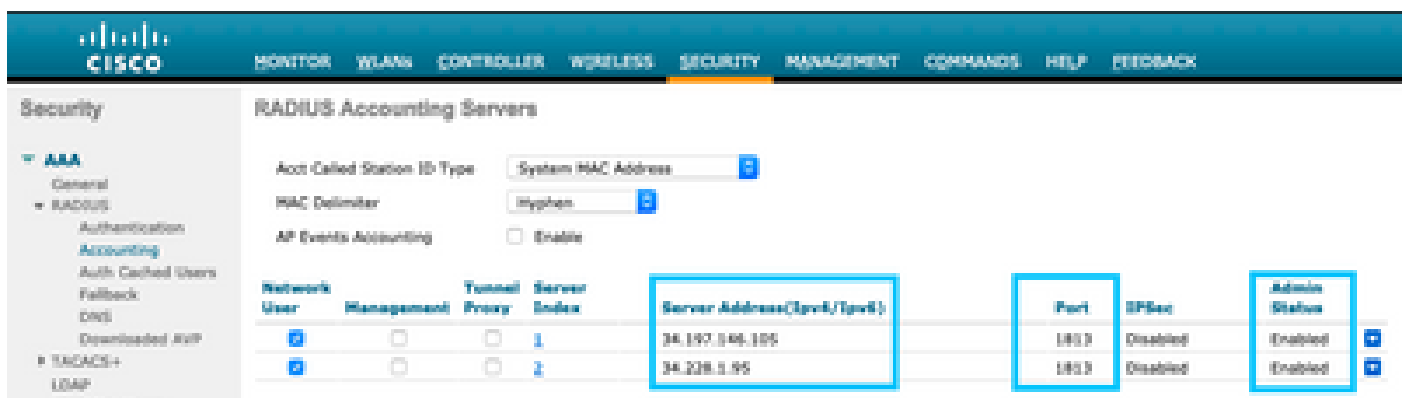


The screenshot shows the Cisco DNA Security configuration page for RADIUS Authentication Servers. The left sidebar shows the navigation menu with 'AAA' expanded to 'RADIUS' and 'Authentication' selected. The main content area shows the configuration for two RADIUS servers. The 'Auth-Called Station ID Type' is set to 'AP MAC Address SSID'. The 'Use AES Key Wrap' checkbox is unchecked. The 'MAC Delimiter' is set to 'Hyphen'. The 'Framed IP(s)' is set to 'None'. The table below shows the configuration for two servers:

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	34.197.146.100	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2	34.208.1.95	1812	Disabled	Enabled

 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 servidor RADIUS de cuentas. Navegue hasta Seguridad > AAA > RADIUS > Contabilización y haga clic en Nuevo. Configure los mismos servidores RADIUS:




The screenshot shows the Cisco DNA Security configuration page for RADIUS Accounting Servers. The left sidebar shows the navigation menu with 'AAA' expanded to 'RADIUS' and 'Accounting' selected. The main content area shows the configuration for two RADIUS servers. The 'Acc-Called Station ID Type' is set to 'System MAC Address'. The 'MAC Delimiter' is set to 'Hyphen'. The 'AP Events Accounting' checkbox is unchecked. The table below shows the configuration for two servers:

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	34.197.146.100	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	34.208.1.95	1812	Disabled	Enabled

Configuración de SSID en el controlador

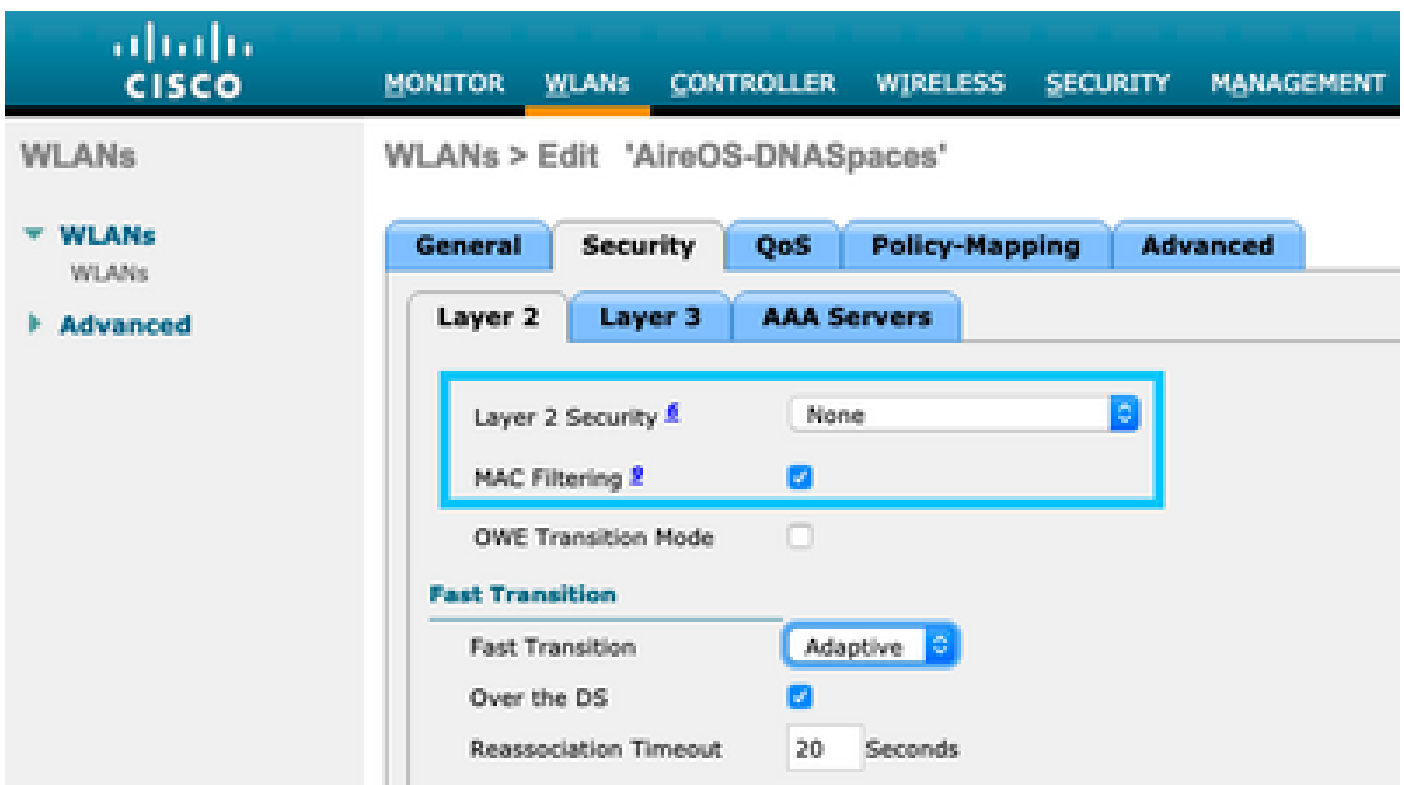
 Importante: Antes de comenzar con la configuración SSID, asegúrese de que Web Radius

 Authentication esté configurado como "PAP" en Controller > General.

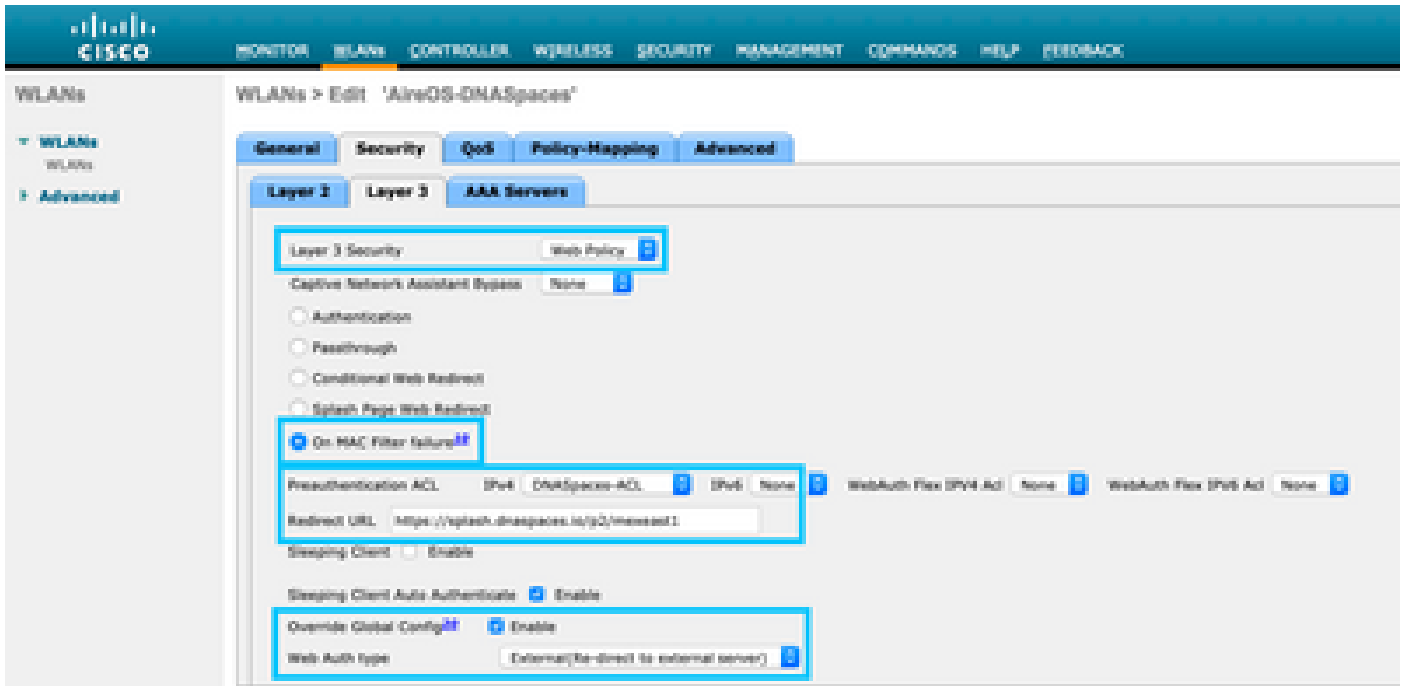
Paso 1. Vaya a WLAN > WLANs. Cree una nueva WLAN. Configure el nombre del perfil y el SSID. Asegúrese de que el nombre SSID es el mismo que el configurado en el paso 3 de la sección Creación del SSID en Espacios de ADN.



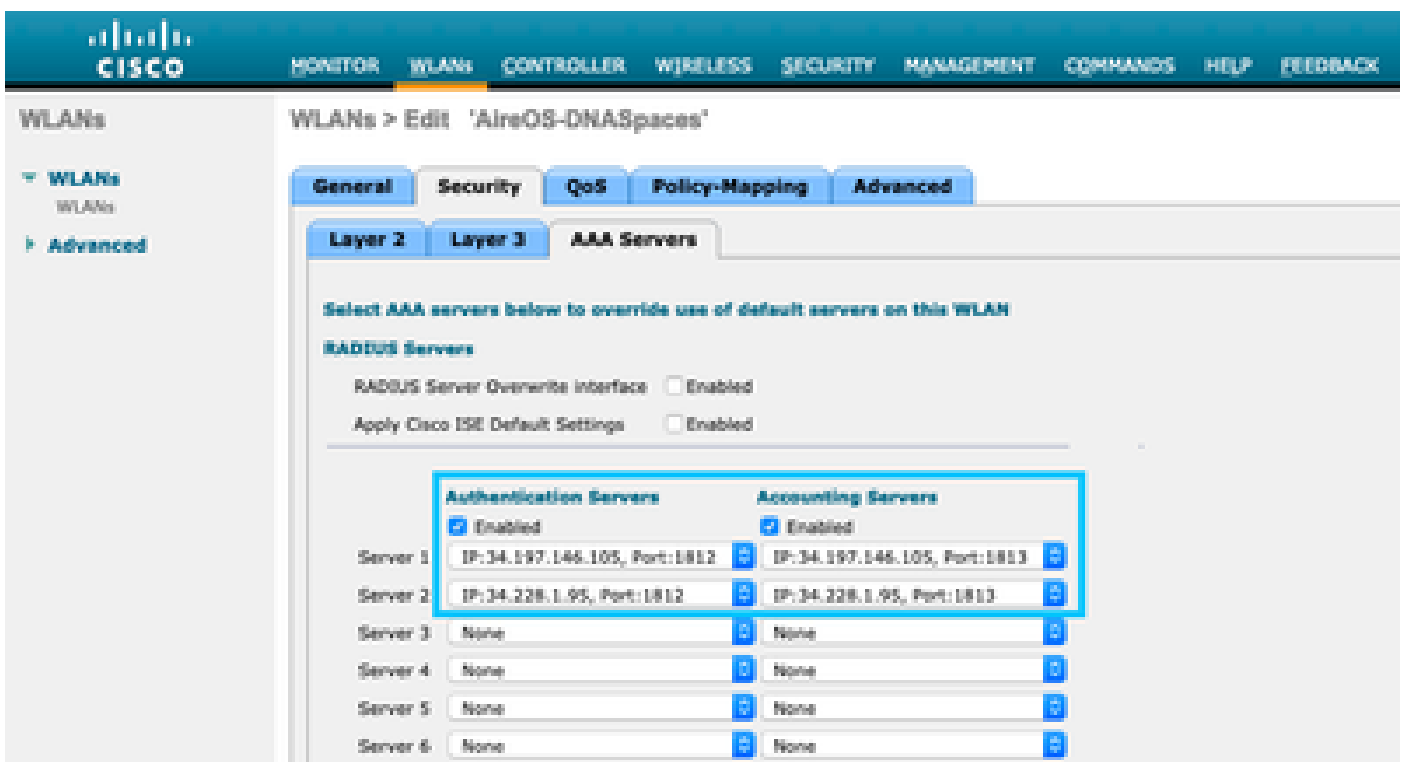
Paso 2. Configuración de la seguridad de capa 2. Vaya a la pestaña Security > Layer 2 en la pestaña de configuración WLAN. Configure la Seguridad de Capa 2 como Ninguna. Active el filtrado de Mac.



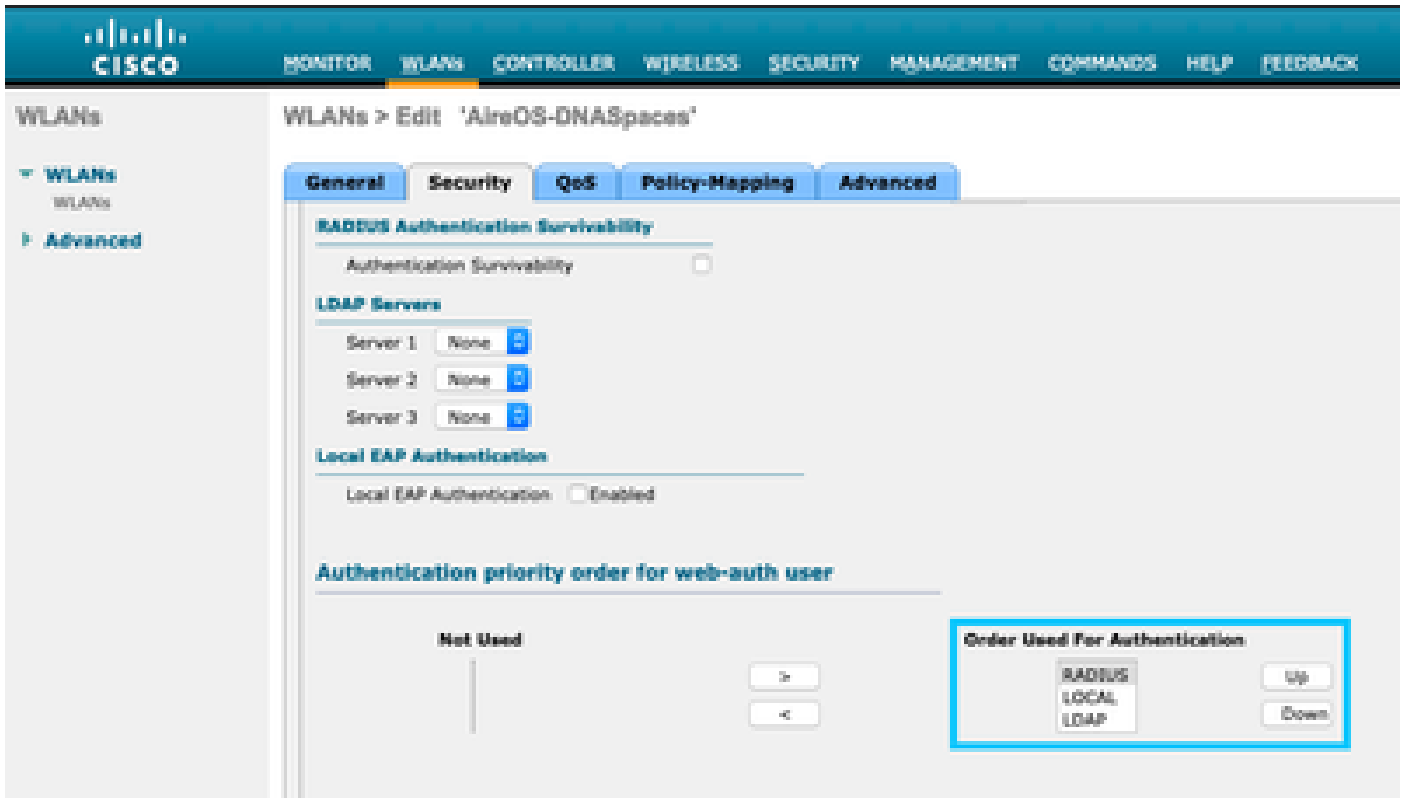
Paso 3. Configuración de la seguridad de capa 3. Vaya a la pestaña Security > Layer 3 en la pestaña de configuración WLAN, configure Web Policy como el método de seguridad de la Capa 3, Enable On Mac Filter failure, configure la ACL de preautenticación, habilite Override Global Config como set the Web Auth Type as External, configure la URL de redirección.



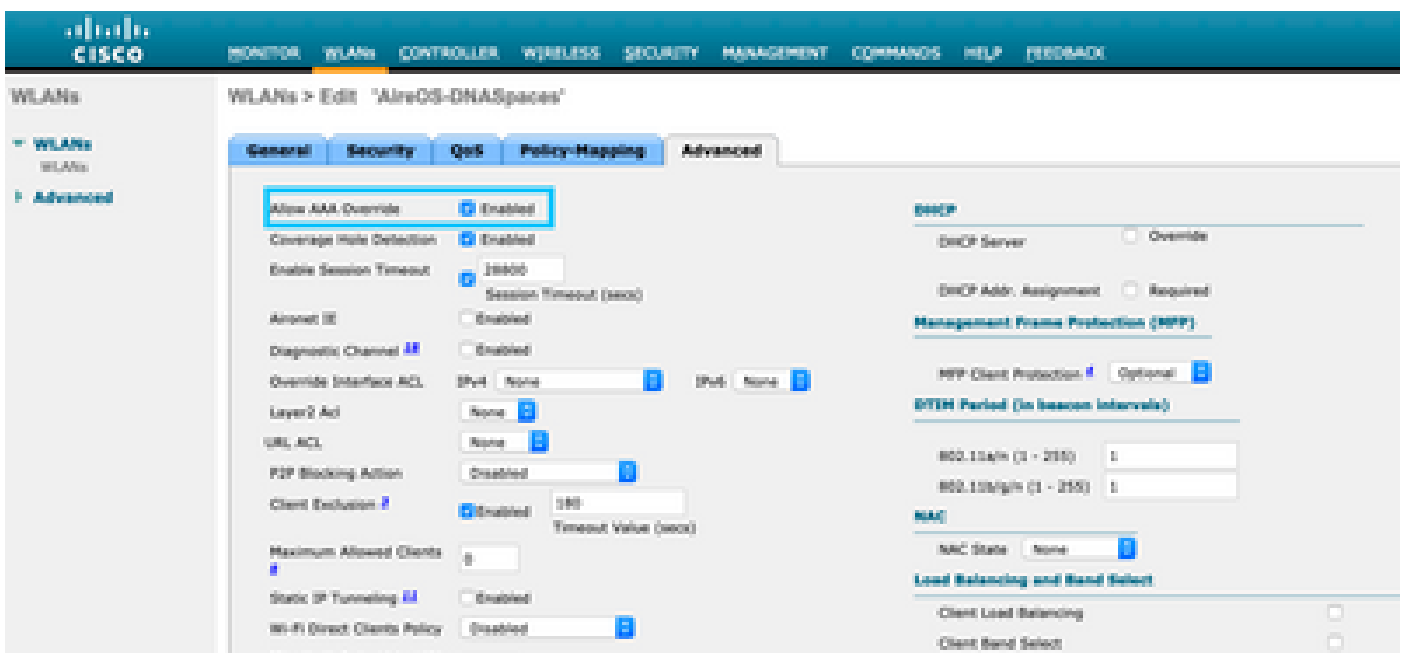
Paso 4. Configuración de servidores AAA. Navegue hasta la pestaña Security > AAA Servers en la pestaña de configuración WLAN, habilite Authentication Servers y Accounting Servers y en el menú desplegable elija los dos servidores RADIUS:



Paso 6. Configure el orden de prioridad de autenticación para los usuarios de autenticación Web. Navegue hasta la pestaña Security > AAA Servers en la pestaña de configuración de WLAN y establezca RADIUS como el primero en orden.

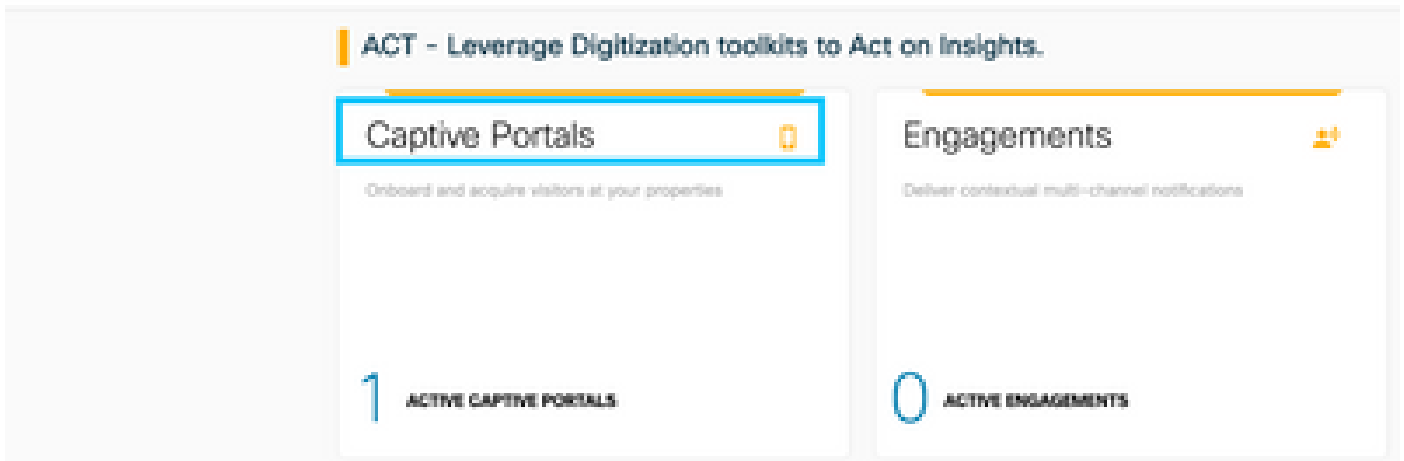


Paso 7. Vaya a la pestaña Advanced en la pestaña WLAN configuration y habilite Allow AAA Override.

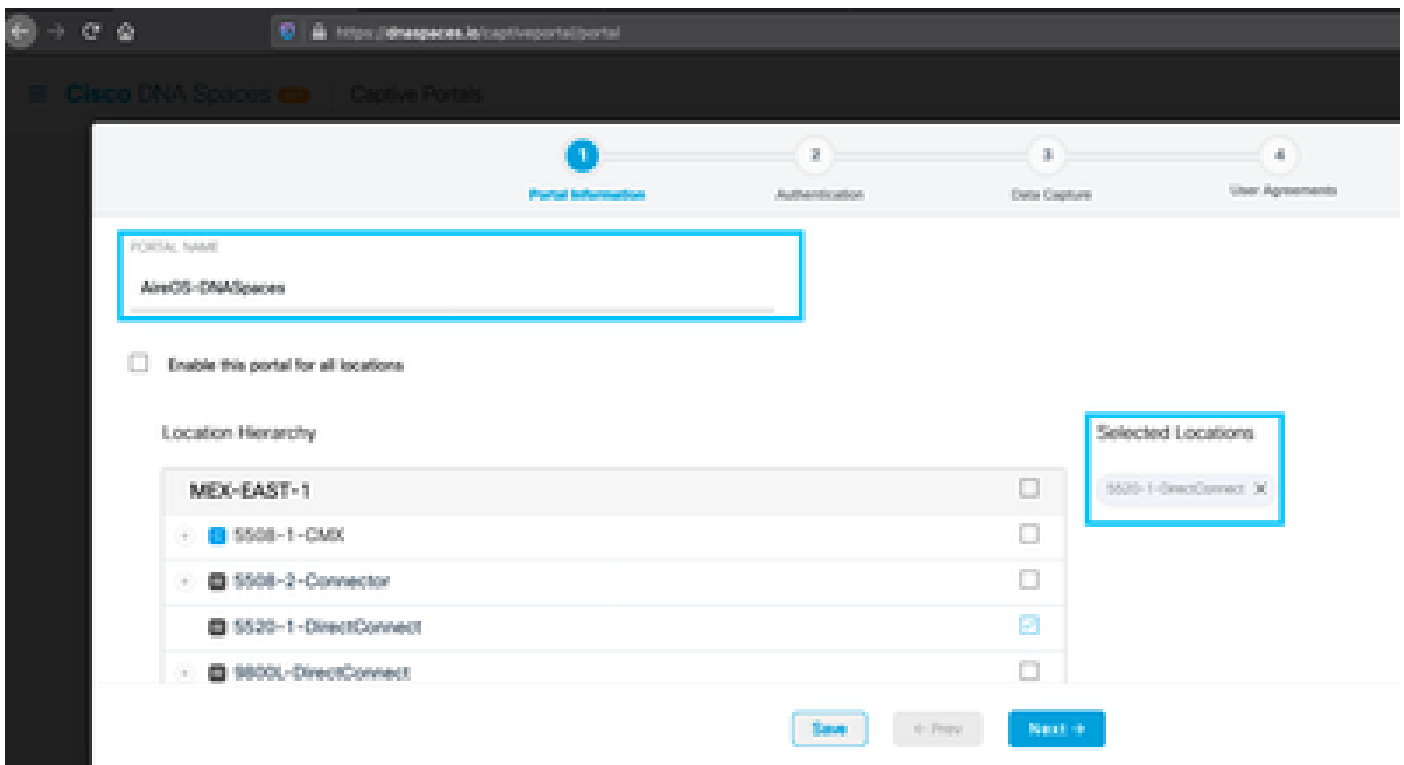


Crear el portal en espacios de ADN

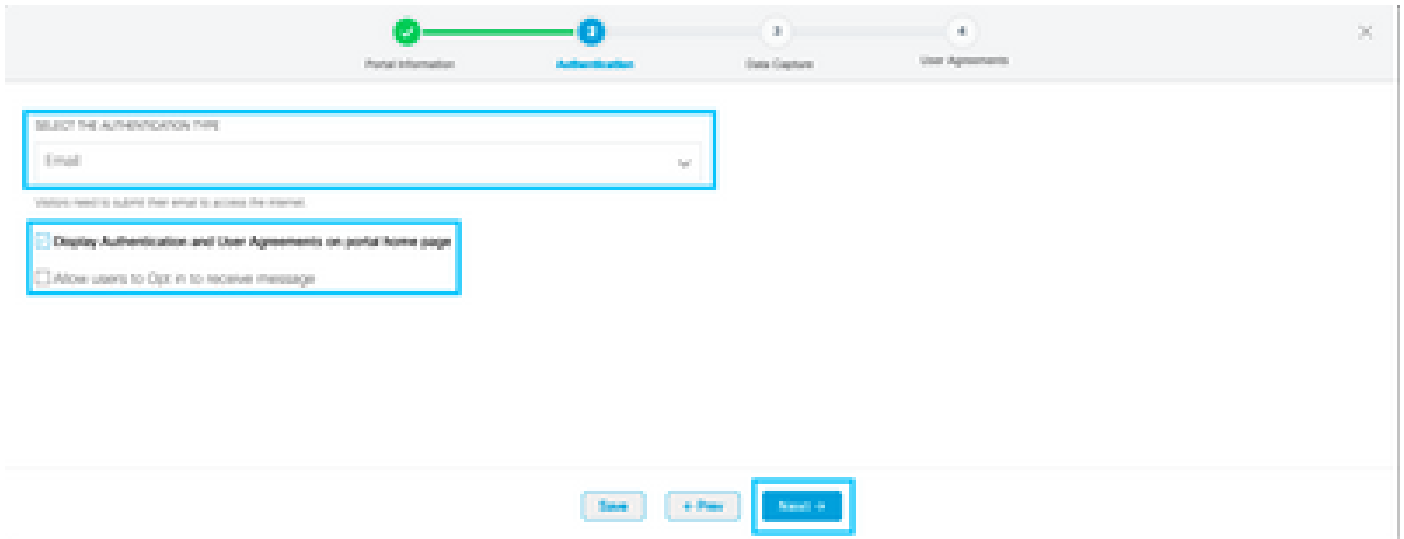
Paso 1. Haga clic en Portales cautivos en el panel de Espacios de ADN:



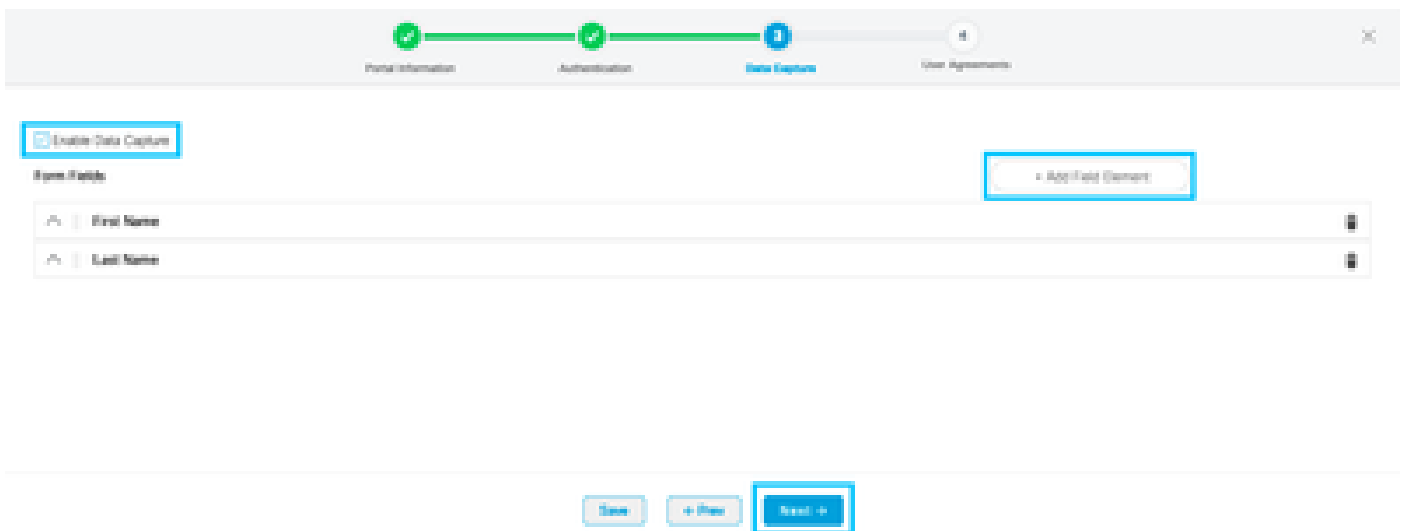
Paso 2. Haga clic en Create New, ingrese el nombre del portal y seleccione las ubicaciones que pueden utilizar el portal:



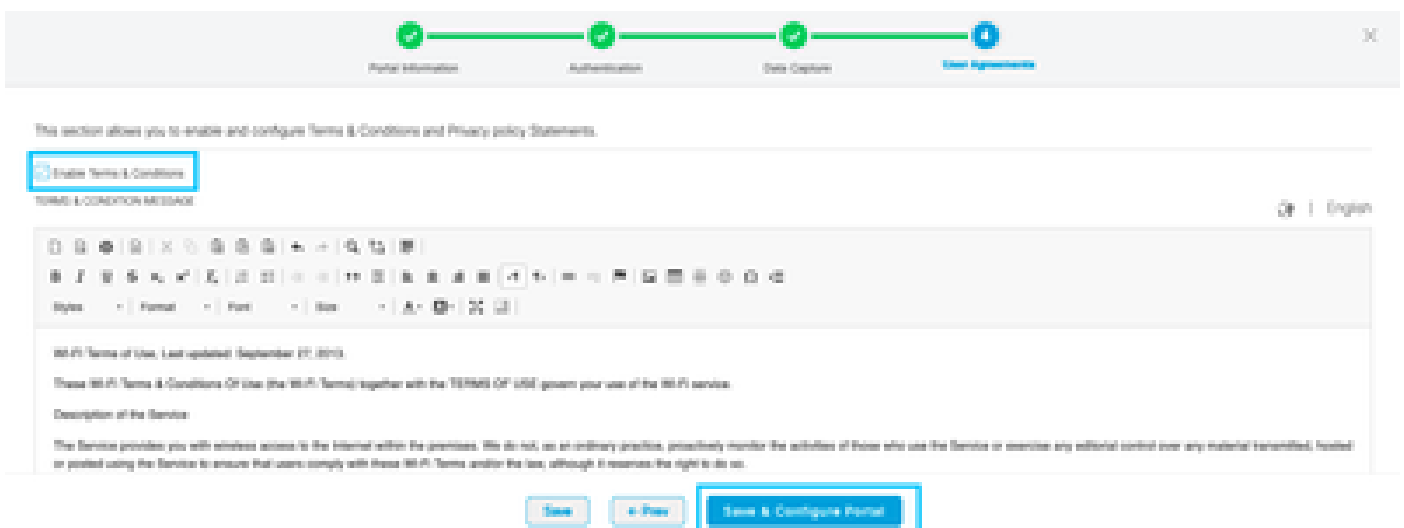
Paso 3. Seleccione el tipo de autenticación, elija si desea mostrar la captura de datos y los acuerdos de usuario en la página principal del portal y si los usuarios pueden participar para recibir un mensaje. Haga clic en Next (Siguiente):



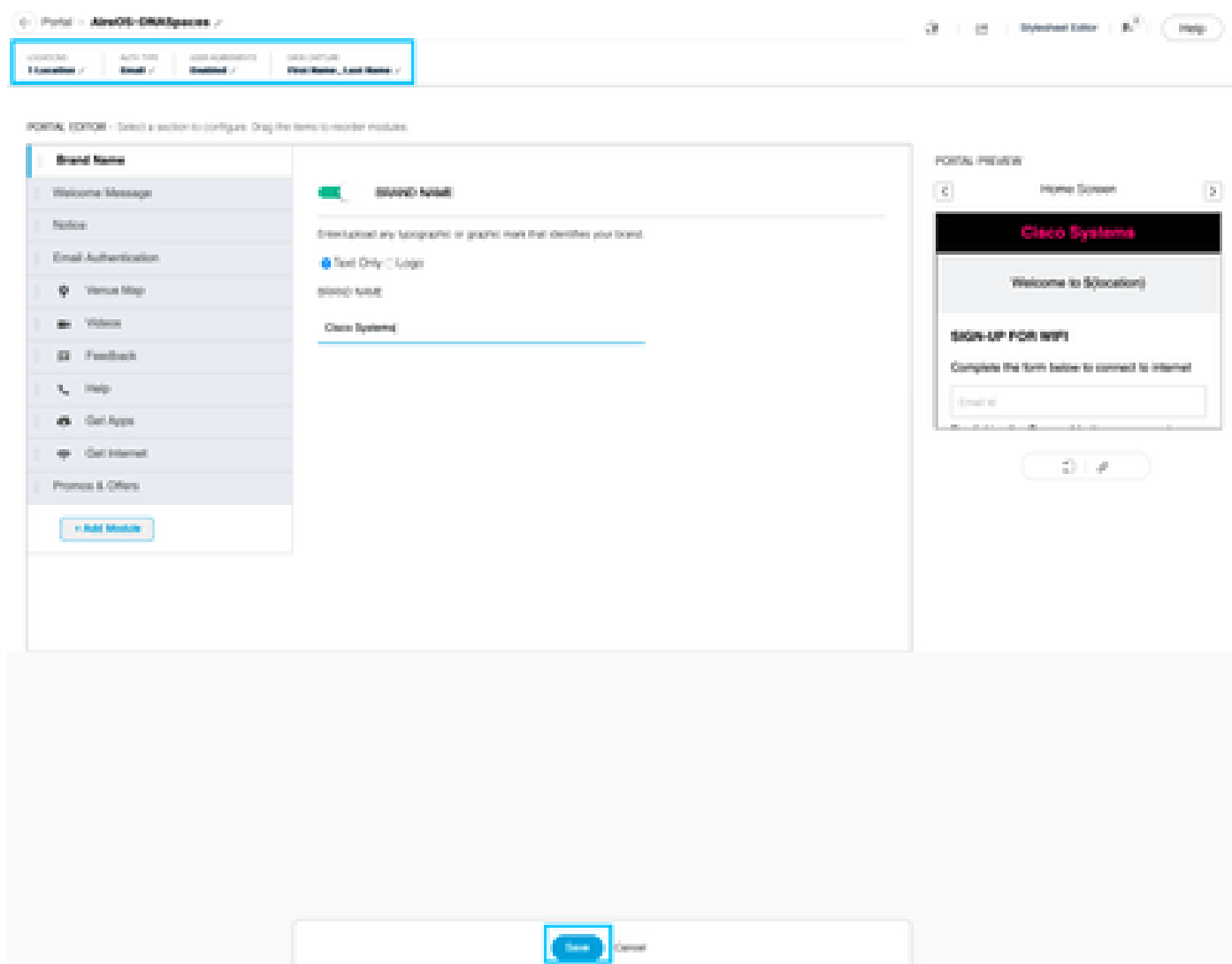
Paso 4. Configurar elementos de captura de datos. Si desea capturar datos de los usuarios, marque la casilla Enable Data Capture y haga clic en +Add Field Element para agregar los campos deseados. Haga clic en Next (Siguiente):



Paso 5. Marque la opción Enable Terms & Conditions y haga clic en Save & Configure Portal:

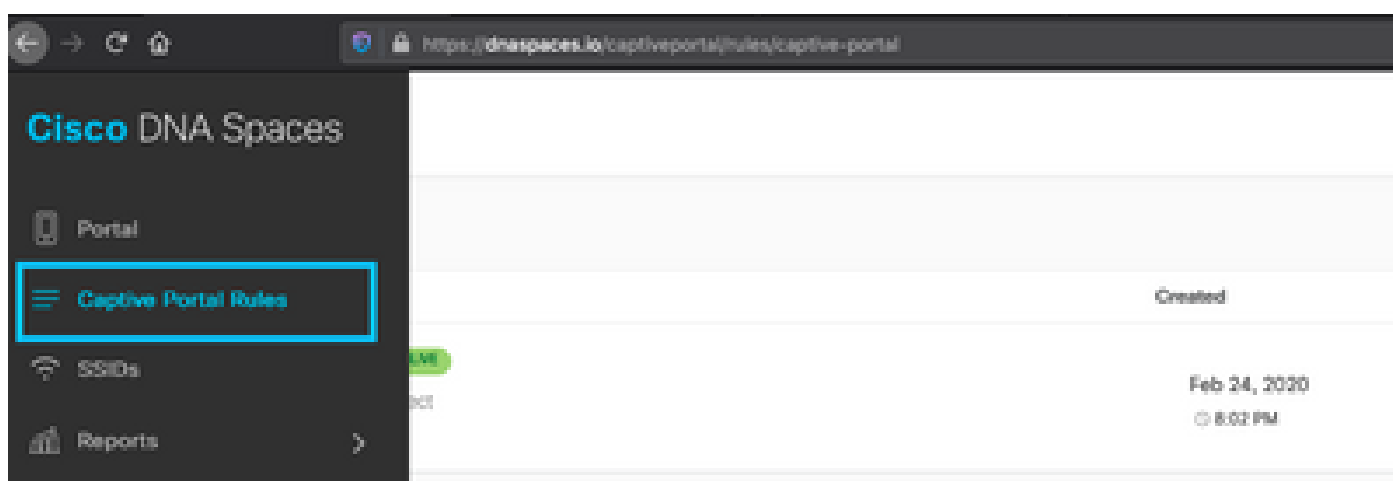


Paso 6. Edite el portal según sea necesario, haga clic en Guardar:



Configuración de las reglas del portal cautivo en espacios DNA

Paso 1. Abra el menú del portal cautivo y haga clic en Reglas del portal cautivo:



Paso 2. Haga clic en + Crear nueva regla. Introduzca el nombre de la regla, elija el SSID configurado anteriormente y seleccione las ubicaciones para las que esta regla de portal está

disponible:

+

Create Captive Portal Rule

Rule Name: AireOS-DMZSystem

Choose any or all of the options that apply to your rule below

When a user is on: WiFi and connected to: AireOS-DMZSystem

LOCATIONS - Where do you want the rule to be?

All any of the following locations

+ Add Locations

SSID-1-DMZSystem

Filter by Metadata

Further filter your location pool by including or excluding locations by metadata

SUMMARY

Rule Name: AireOS-DMZSystem

Device: AireOS-DMZSystem

Location: All any of the following under SSID-1 (DMZSystem)

Action: Show Captive Portal

Paso 3. 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.

AireOS-DMZSystem

Session Duration

Bandwidth Limit

Seamlessly Provision Internet

Directly provision internet without showing any authentication

Deny Internet

Stop users from accessing the internet

Tag these users as

Choose a Resource/ResourceID to assign tags

+ Add Tags

Trigger API

Save & Publish

Save

SUMMARY

SCHEDULE

ACTION

Show Captive Portal

Portal: AireOS-DMZSystem

Verificación

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

Max Number of Records 10

General		AVC Statistics	
Client Type	Regular	AP radio slot Id	1
Client Tunnel Type	Simple IP	WLAN Profile	AireOS-DNASpaces
User Name		WLAN SSID	AireOS-DNASpaces
Webauth User Name	None	Status	Associated
Port Number	1	Association ID	1
Interface	management	802.11 Authentication	Open System
VLAN ID	20	Reason Code	1
Quarantine VLAN ID	0	Status Code	0
CCX Version	Not Supported	CF Pollable	Not Implemented
EDE Version	Not Supported	CF Poll Request	Not Implemented
Mobility Role	Local	Short Preamble	Not Implemented
Mobility Peer IP Address	N/A	RFCC	Not Implemented
Mobility Move Count	0	Channel Agility	Not Implemented
Policy Manager State	RUN	Timeout	0
		WEP State	WEP Disable

Troubleshoot

El siguiente comando se puede habilitar en el controlador antes de la prueba para confirmar el proceso de asociación y autenticación del cliente.

```
<#root>
```

```
(5520-Andressi) >
```

```
debug client
```

```
(5520-Andressi) >
```

```
debug web-auth redirect enable mac
```

Este es el resultado de 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:

```
*apfOpenDtIsocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION REQUEST
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capability as 4
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Processing assoc-req station:34:e1:2d:23:a6:68
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode (1), Resu
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0 station:34:e1
```

Autenticación DHCP y de capa 3:

```
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP_REQD
*webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in HTTP GET
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68 user_agent = A
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to configure
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual IP, us
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Checking custom-web config for WLAN ID:1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Global status is 0 on WLAN
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- checking on WLAN web-auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Web-auth type External, using URL:https://spl
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now https:/
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio ), redirect URL is now ht
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now https:
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now https://splas
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is <HTML><HEAD><TITLE
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now https://splash.dn
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now https://splash.dnaspaces.io/p2/me

*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Message to be sent is
HTTP/1.1 200 OK
Location: https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- 200 send_data =HTTP/1.1 200 OK
Location: https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- send data length=688
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Url:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- cleaning up after send
```

Autenticación de capa 3 exitosa, mueva el cliente al estado RUN:

```
*emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68
*emWeb: Apr 09 21:49:57.634:
ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl_connection=0, secureweb=1

*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 WEBAUTH_NOL3SEC (14) Change state t
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode (0), Res
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result (0), R
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully plumbed mobili
```

*emWeb: Apr 09 21:49:57.634: User login successful, presenting login success page to user

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).