

DNA Spaces Captive Portal with AireOS Controller Configuration Example

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Connect the WLC to Cisco DNA Spaces](#)

[Create the SSID on DNA Spaces](#)

[ACL configuration on the controller](#)

[Captive Portal without RADIUS Server on DNA Spaces](#)

[Captive Portal with RADIUS Server on DNA Spaces](#)

[Create the portal on DNA Spaces](#)

[Configure the Captive Portal Rules on DNA Spaces](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure captive portals using Cisco DNA Spaces with an AireOS controller.

Contributed by Andres Silva Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Command Line Interface (CLI) or Graphic User Interface (GUI) access to the wireless controllers
- Cisco DNA Spaces

Components Used

The information in this document is based on these software and hardware versions:

- 5520 Wireless LAN Controller version 8.10.112.0

Configure

Network Diagram



DNA Spaces



and configure the rules to allow communication between the wireless clients to DNA Spaces as follows. Replace the IP addresses with the ones given by DNA Spaces for the account in use:

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	

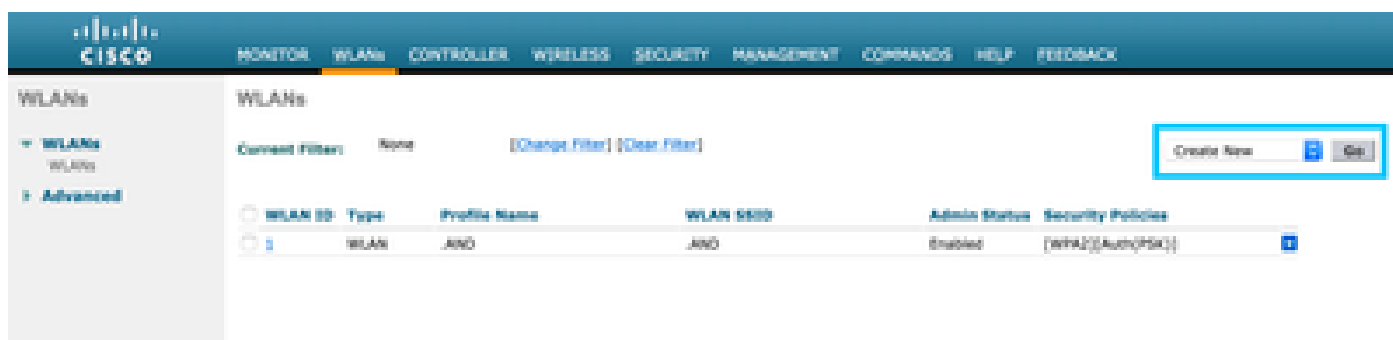
Note: To get the IP addresses of DNA Spaces to be allowed in the ACL, click on the **Configure Manually** option from the SSID created in step 3 of section **Create the SSID on DNA Spaces** under the ACL configuration section.

The SSID can be configured to use a RADIUS Server or without it. If that Session Duration, Bandwidth Limit, or Seamlessly Provision Internet is configured in the **Actions** section of the Captive Portal Rule configuration, the SSID needs to be configured with a RADIUS Server, otherwise, there is no need to use the RADIUS Server. All kinds of portals on DNA Spaces are supported on both configurations.

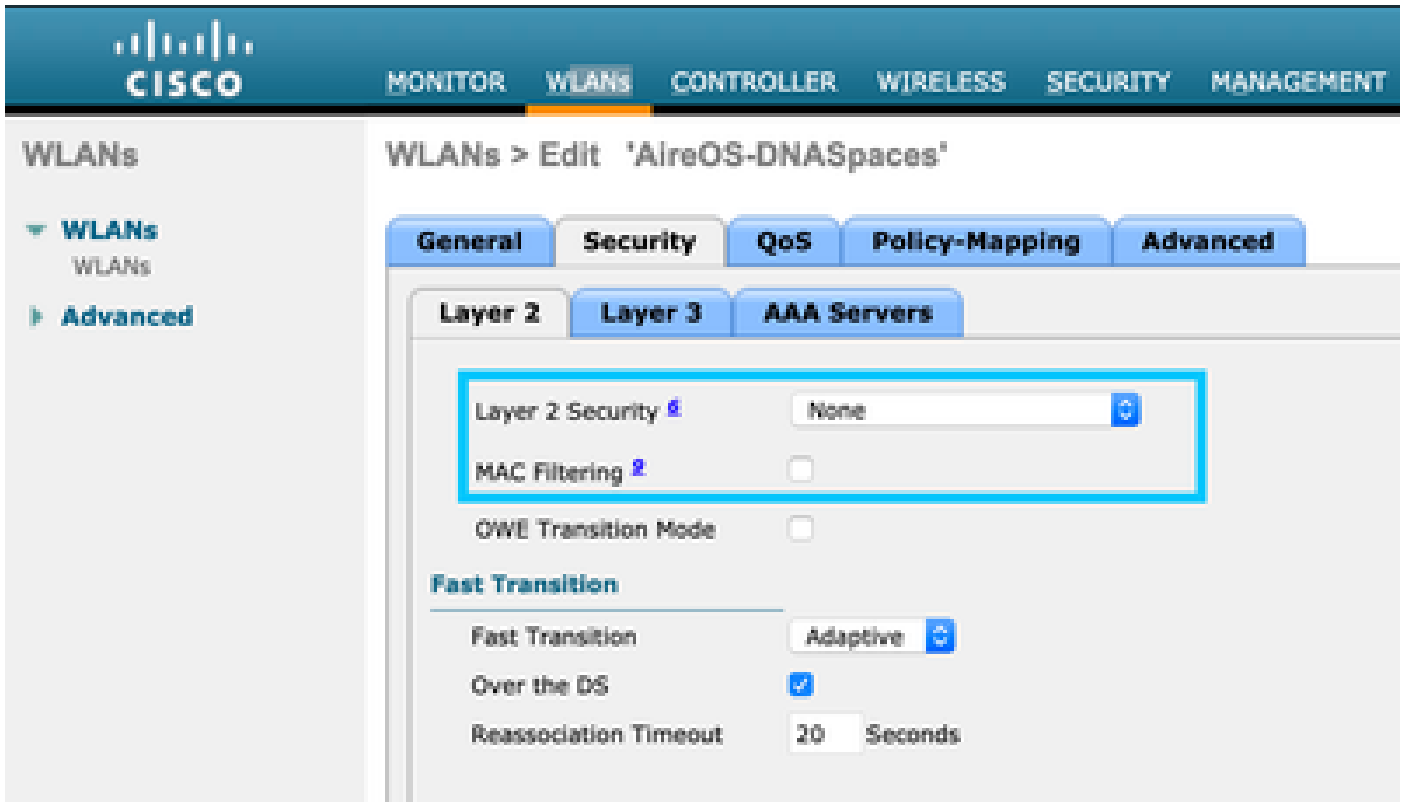
Captive Portal without RADIUS Server on DNA Spaces

SSID configuration on the controller

Step 1. Navigate to **WLAN > WLANs**. Create a new WLAN. Configure the Profile Name and SSID. Make sure the SSID name is the same as the configured in step 3 of section **Create the SSID on DNA Spaces**.



Step 2. Configure layer 2 security. Navigate to the **Security > Layer 2** tab in the WLAN configuration tab and select as **None** from the drop-down menu of Layer 2 Security. Make sure MAC Filtering is disabled.



Step 3. Configure layer 3 security. Navigate to the **Security > Layer 3** tab in the WLAN configuration tab, configure **Web Policy** as the Layer 3 security method, Enable **Passthrough**, configure the preauthentication ACL, enable **Override Global Config** as set the **Web Auth Type** as **External**, configure the Redirect URL.



 **Note:** To get the redirect URL, click on the **Configure Manually** option, from the SSID created in step 3 of section **Create the SSID on DNA Spaces**, under the SSID configuration section.

Captive Portal with RADIUS Server on DNA Spaces

 **Note:** DNA Spaces RADIUS server only supports PAP authentication coming from the controller.


RADIUS Servers configuration on the controller

Step 1. Navigate to **Security > AAA > RADIUS > Authentication**, click on **New** and enter the RADIUS server information. Cisco DNA Spaces acts as the RADIUS server for user authentication and it can respond on two IP addresses. Configure both RADIUS servers:

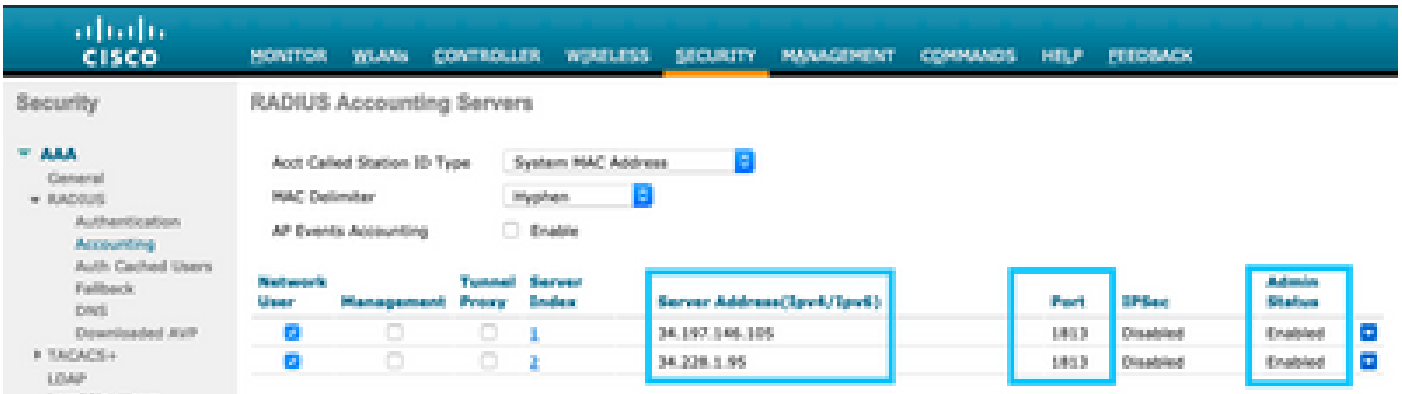


The screenshot shows the 'RADIUS Authentication Servers' configuration page. The 'Auth Called Station ID Type' is set to 'AP MAC Address SSID'. The 'Use AES Key Wrap' checkbox is unchecked. The 'MAC Delimiter' is set to 'Hyphen' and 'Framed RTT' is '1000'. Below these settings is a table with two server entries:

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	34.187.346.105	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2	34.238.1.95	1812	Disabled	Enabled

 **Note:** To get RADIUS IP address and secret key for both primary and secondary servers, click on the **Configure Manually** option from the SSID created in step 3 of section **Create the SSID on DNA Spaces** and navigate to the **RADIUS Server Configuration** section.


Step 2. Configure the accounting RADIUS Server. Navigate to **Security > AAA > RADIUS > Accounting** and click on **New**. Configure same both RADIUS servers:



The screenshot shows the 'RADIUS Accounting Servers' configuration page. The 'Auth Called Station ID Type' is set to 'System MAC Address'. The 'MAC Delimiter' is set to 'Hyphen' and 'AP Events Accounting' is unchecked. Below these settings is a table with two server entries:

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	34.187.346.105	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	34.238.1.95	1812	Disabled	Enabled

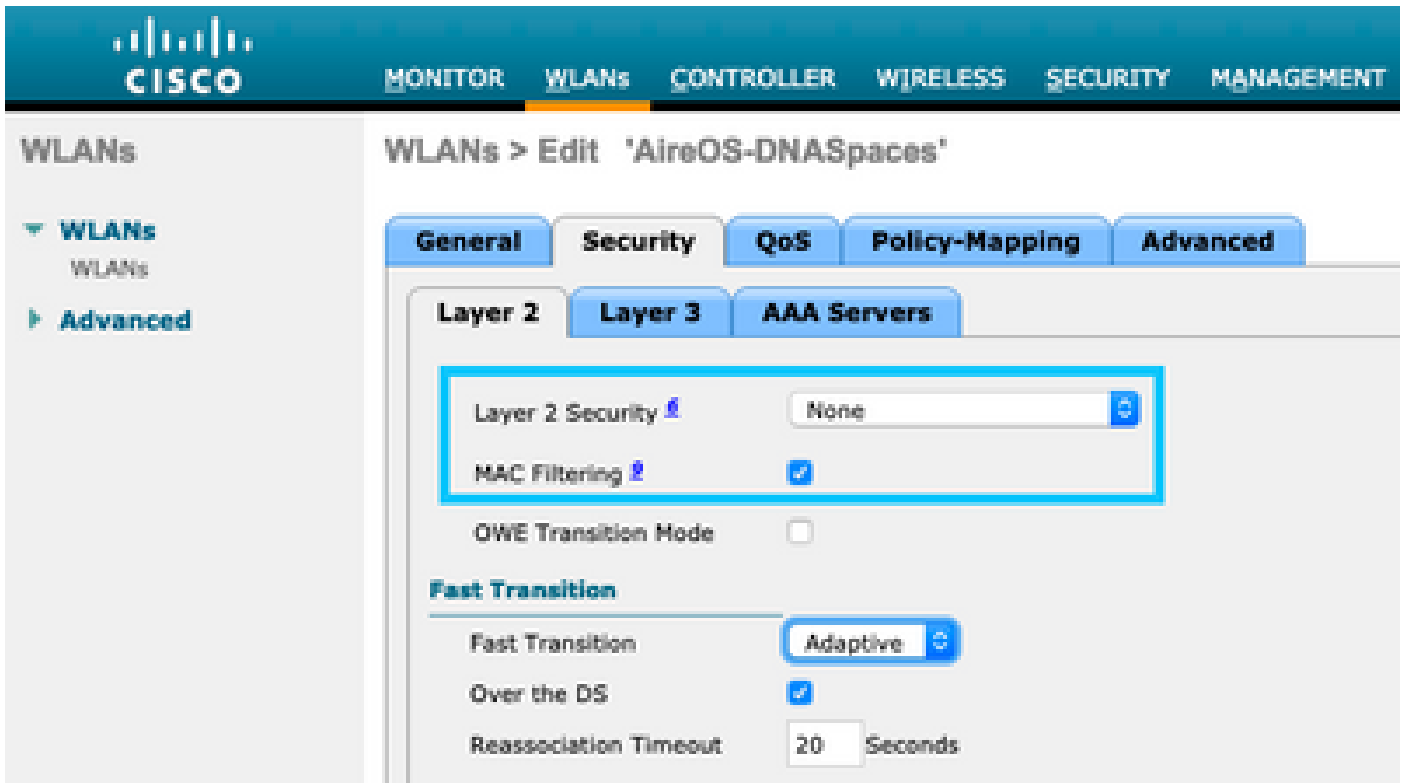
SSID configuration on the controller

 **Important:** Before starting with the SSID configuration, make sure that **Web Radius Authentication** is set to "PAP" under Controller > General.

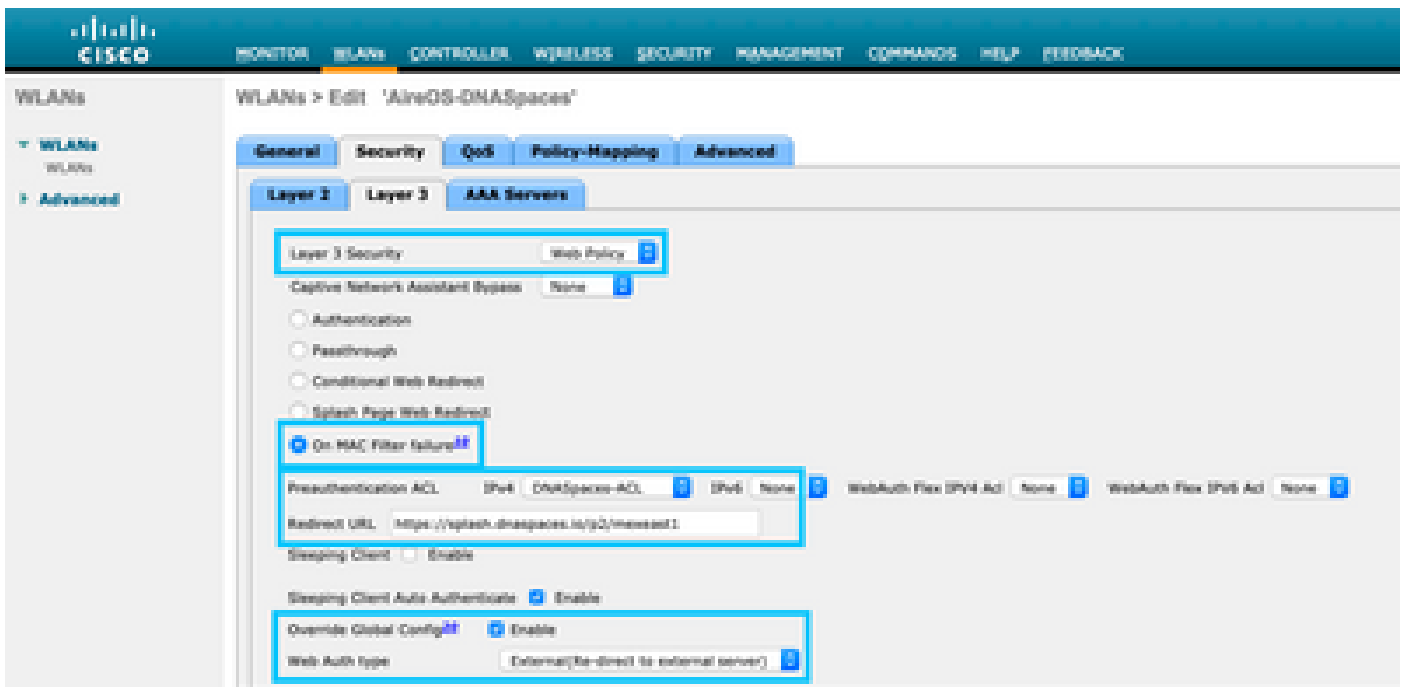
Step 1. Navigate to **WLAN > WLANs**. Create a new WLAN. Configure the Profile Name and SSID. Make sure the SSID name is the same as the configured in step 3 of section **Create the SSID on DNA Spaces**.



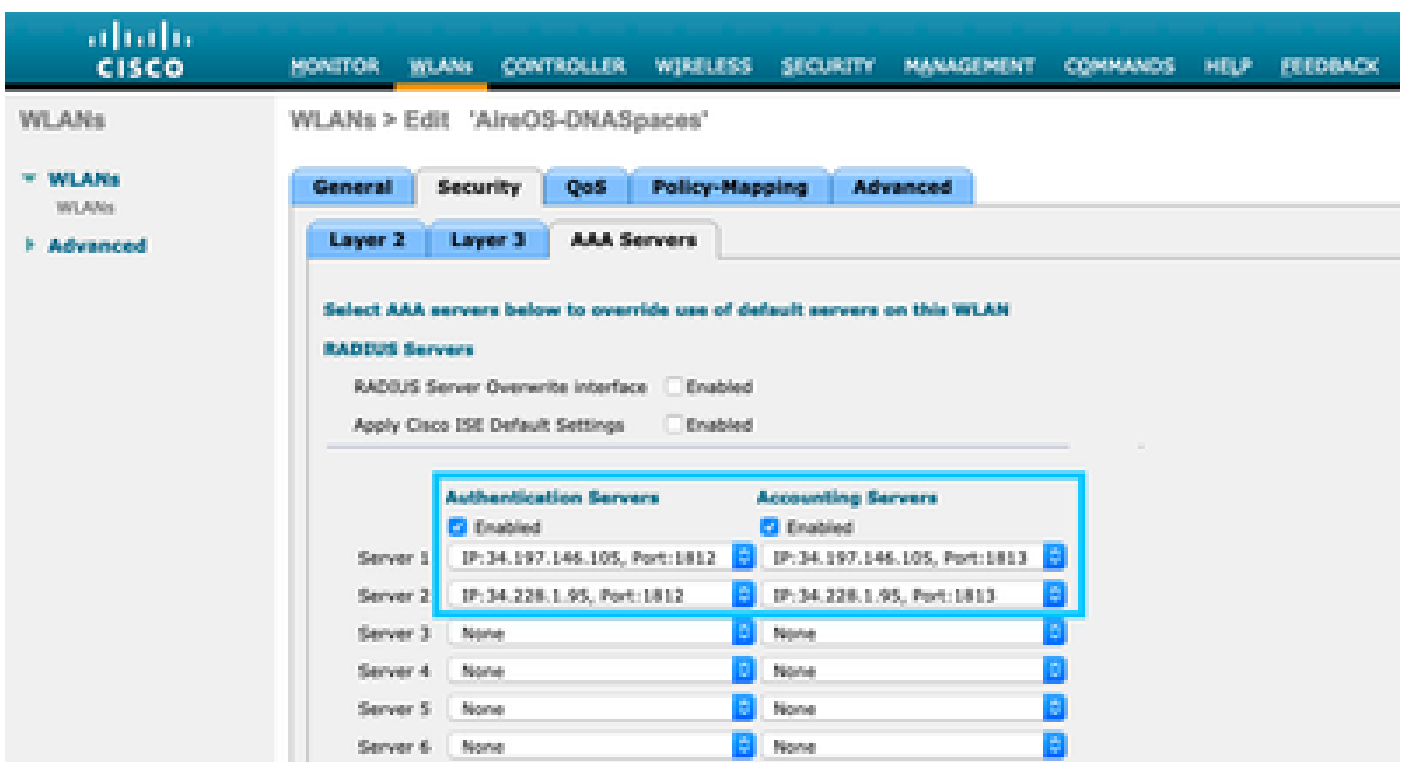
Step 2. Configure layer 2 security. Navigate to the **Security > Layer 2** tab in the WLAN configuration tab. Configure Layer 2 Security as **None**. Enable Mac Filtering.



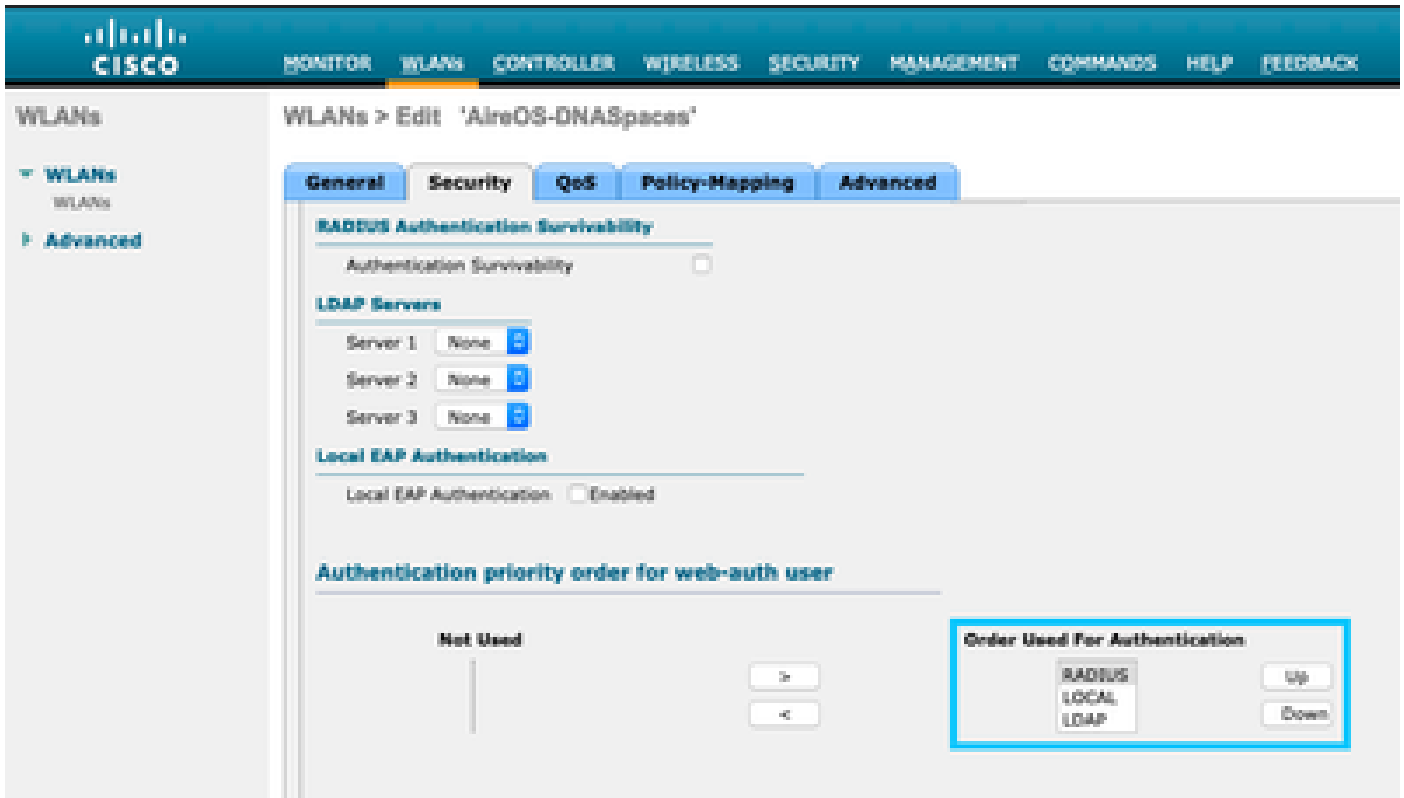
Step 3. Configure layer 3 security. Navigate to the **Security > Layer 3** tab in the WLAN configuration tab, configure **Web Policy** as the Layer 3 security method, Enable **On Mac Filter failure**, configure the preauthentication ACL, enable **Override Global Config** as set the **Web Auth Type** as **External**, configure the Redirect URL.



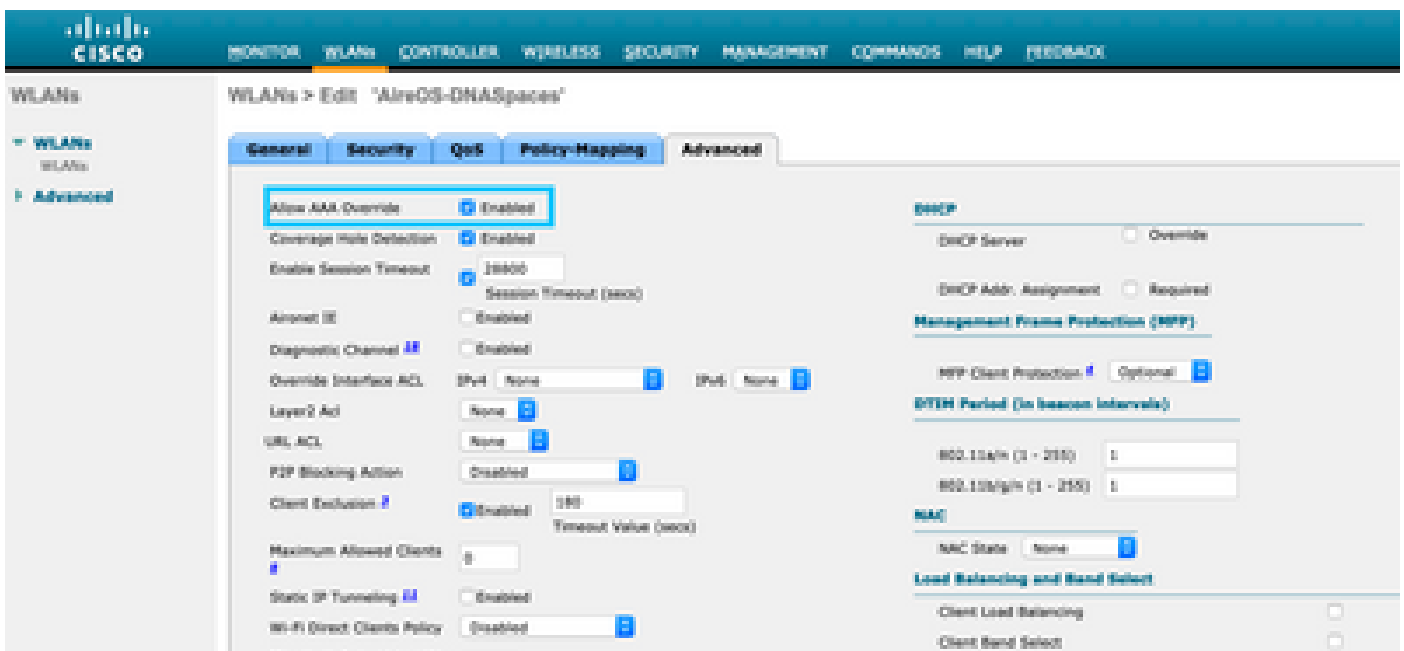
Step 4. Configure AAA Servers. Navigate to the **Security > AAA Servers** tab in the WLAN configuration tab, enable **Authentication Servers** and **Accounting Servers** and from the drop-down menu choose the two RADIUS servers:



Step 6. Configure the **Authentication Priority** order for web-auth users. Navigate to the **Security > AAA Servers** tab in the WLAN configuration tab, and set RADIUS as first in order.

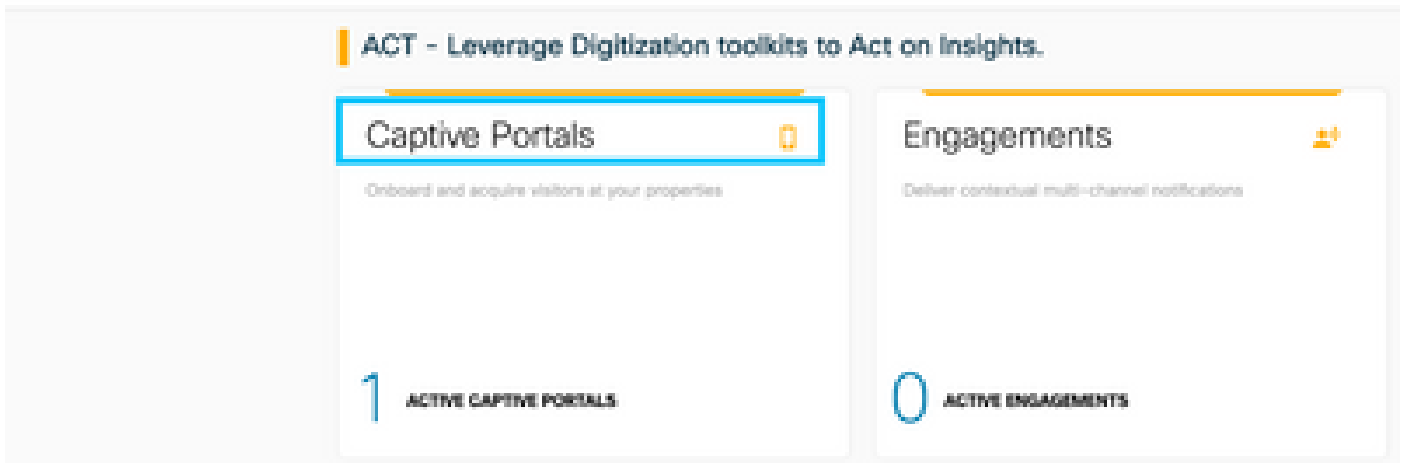


Step 7. Navigate to the **Advanced** tab in the WLAN configuration tab and enable **Allow AAA Override**.

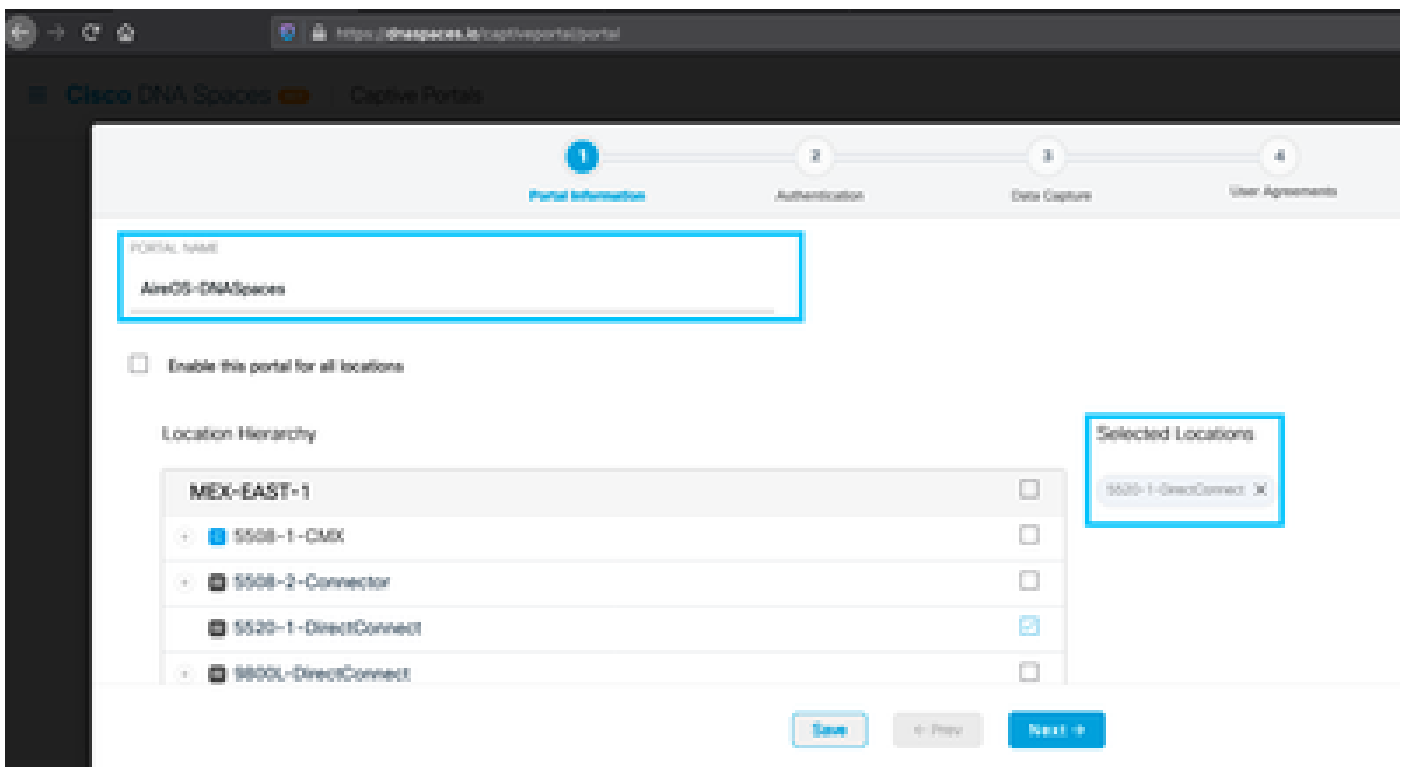


Create the portal on DNA Spaces

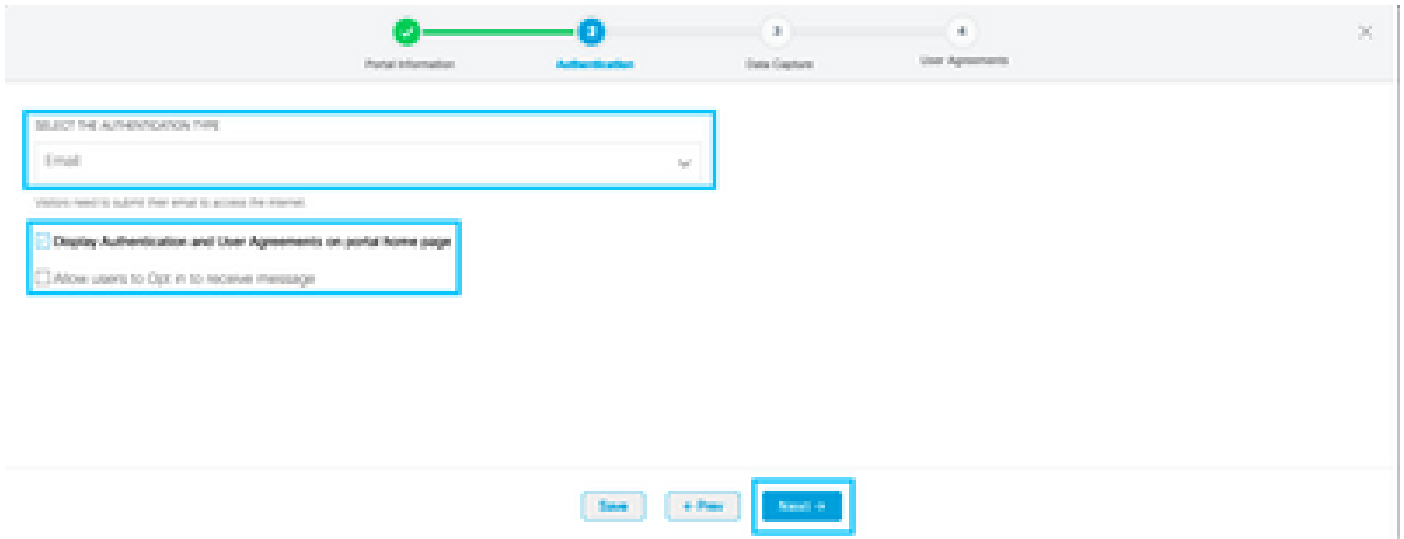
Step 1. Click on **Captive Portals** in the dashboard of DNA Spaces:



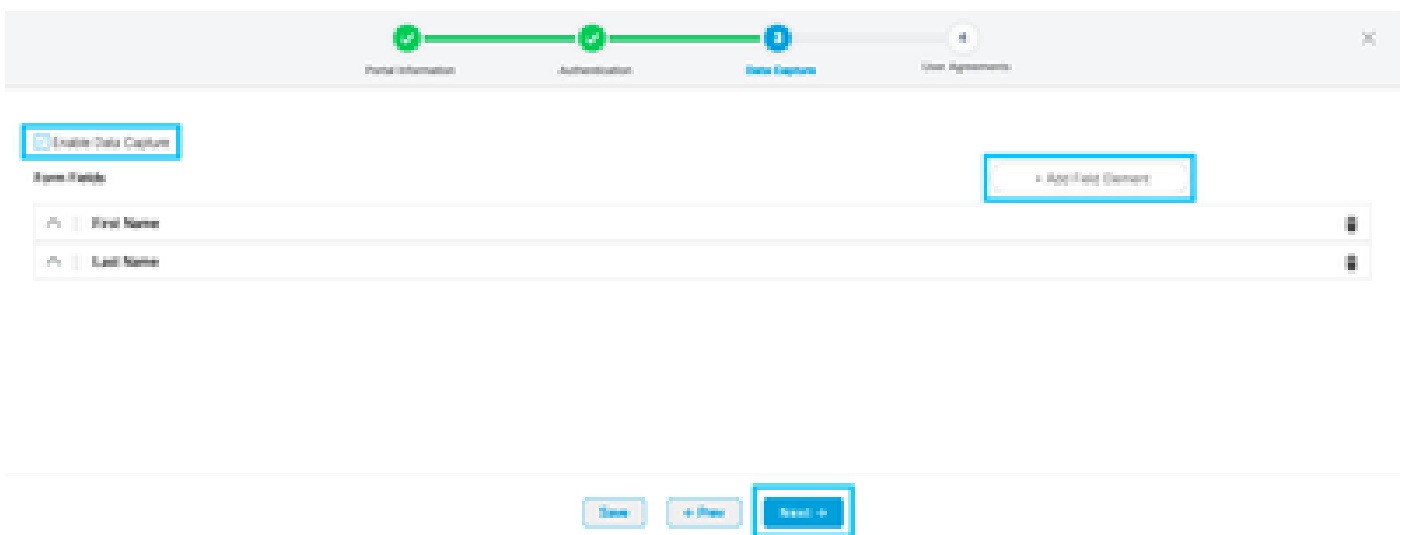
Step 2. Click on **Create New**, enter the portal name, and select the locations that can use the portal:



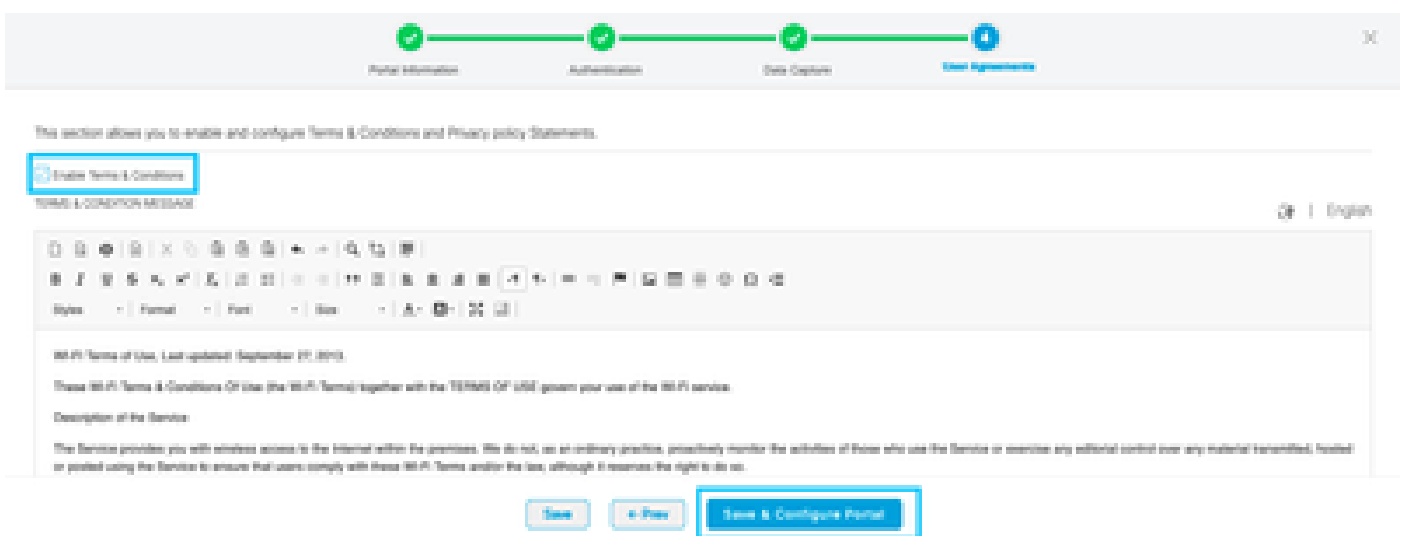
Step 3. Select the authentication type, choose if you want to display data capture and user agreements on the portal home page and if users are allowed to Opt-in to receive a message. Click **Next**:



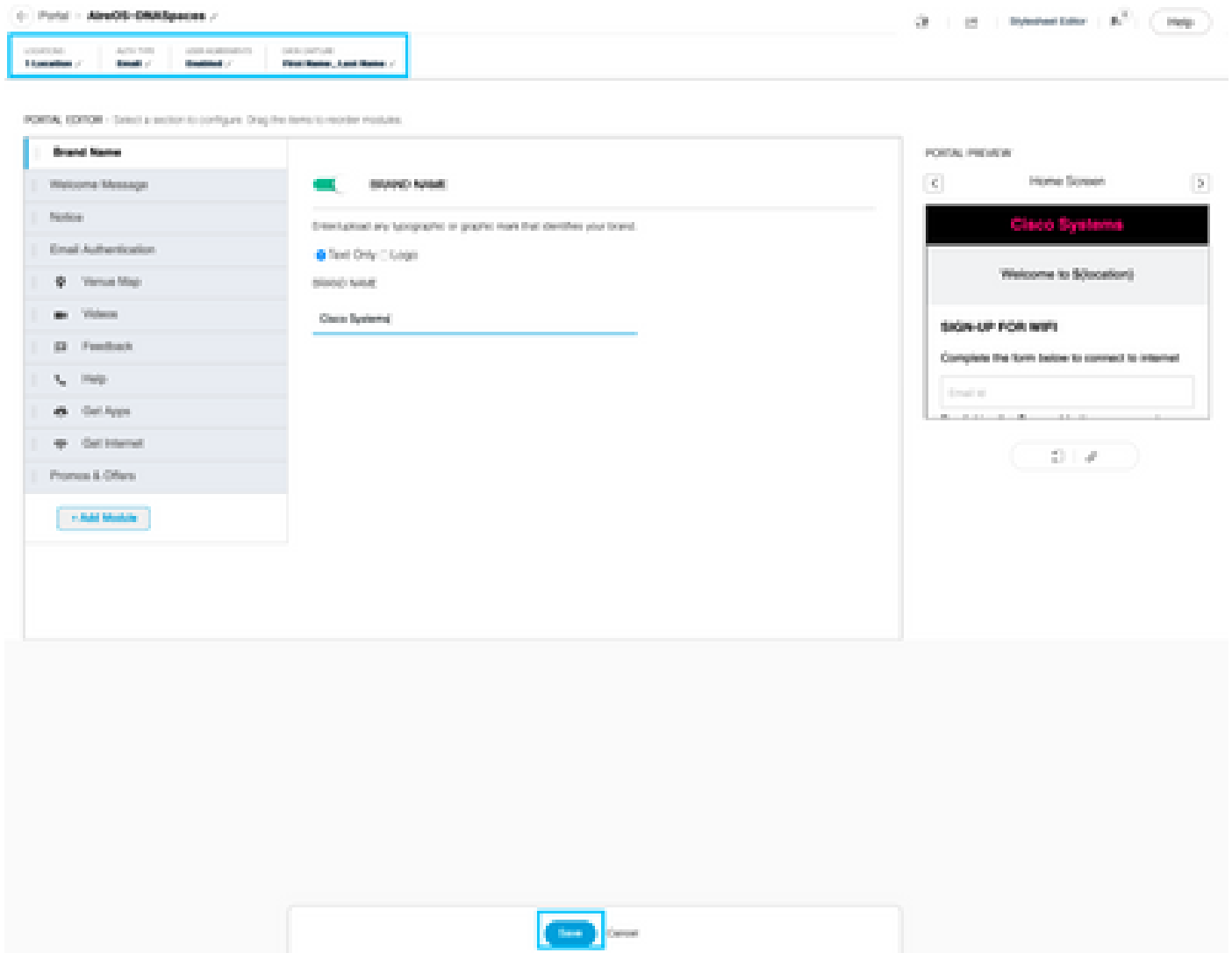
Step 4. Configure Data capture elements. If you want to capture data from the users, check the **Enable Data Capture** box and click on **+Add Field Element** to add the desired fields. Click **Next**:



Step 5. Check the **Enable Terms & Conditions** and click **Save & Configure Portal**:

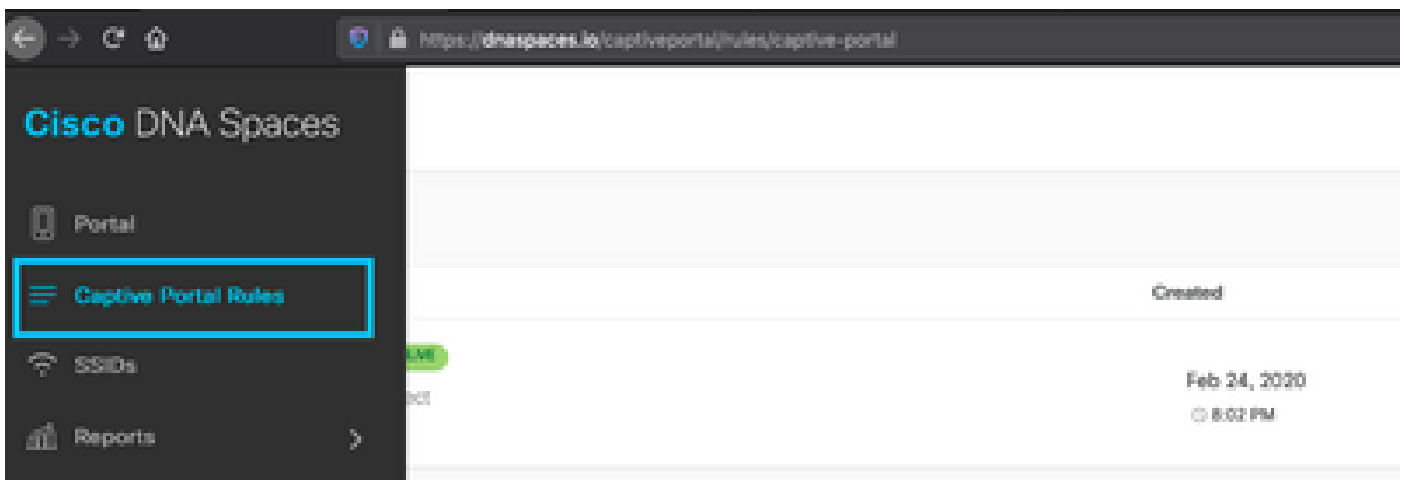


Step 6. Edit the portal as needed, Click on **Save**:



Configure the Captive Portal Rules on DNA Spaces

Step 1. Open the captive portal menu and click on **Captive Portal Rules**:



Step 2. Click + **Create New Rule**. Enter the rule name, choose the SSID previously configured, and select the locations this portal rule is available for:

← Create Captive Portal Rule NewOS-DMZAccess

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

When a user is on WiFi and connected to NewOS-DMZAccess

LOCATIONS - Where do you want the rule to fire?

At any of the following locations:

+ Add Locations

NewOS-DMZAccess

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

SUMMARY

RULE NAME
NewOS-DMZAccess

SCHEDULE
When user is on WiFi and connected to NewOS-DMZAccess

LOCATIONS
For all locations under
NewOS-DMZAccess

ACTIONS
Show Captive Portal

Step 3. Choose the action of the captive portal. In this case, when the rule is hit, the portal is shown. Click **Save & Publish**.

ACTIONS

Show Captive Portal
Choose a Portal to be displayed to users when they connect to the wifi.
NewOS-DMZAccess

Session Duration

Bandwidth Limit

Seamlessly Provision Internet
Directly provision internet without showing any authentication

Deny Internet
Block users from accessing the internet

Tag these users as
Choose a Resource/Resource to assign tags
+ Add Tags

Trigger API

SUMMARY

SCHEDULE

ACTION
Show Captive Portal
Portal - NewOS-DMZAccess

Save & Publish Save

Verify

To confirm the status of a client connected to the SSID navigate to **Monitor > Clients**, click on the MAC address and look for Policy Manager State:

Max Number of Records 10 Clear AVC Stats

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	POCC	Not Implemented
Mobility Move Count	0	Channel Agility	Not Implemented
Policy Manager State	EUM	Timeout	0
		WEP State	WEP Disable

Troubleshoot

The following command can be enabled in the controller prior to testing to confirm the association and authentication process of the client.

```
<#root>
(5520-Andressi) >
debug client <Client-MAC-Address>
(5520-Andressi) >
debug web-auth redirect enable mac <Client-MAC-Address>
```

This is the output from a successful attempt to identify each of the phases during the association/authentication process while connecting to an SSID with no RADIUS server:

802.11 association/authentication:

```
*apfOpenDt1Socket: 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
```

DHCP and Layer 3 authentication:

```
*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://sp
*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
```

Layer 3 authentication successful, move the client to the RUN state:

```
*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 mobil

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