DNA Spaces Captive Portal with AireOS Controller Configuration Example

Contents

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

Configurations

Connect the WLC to Cisco DNA Spaces

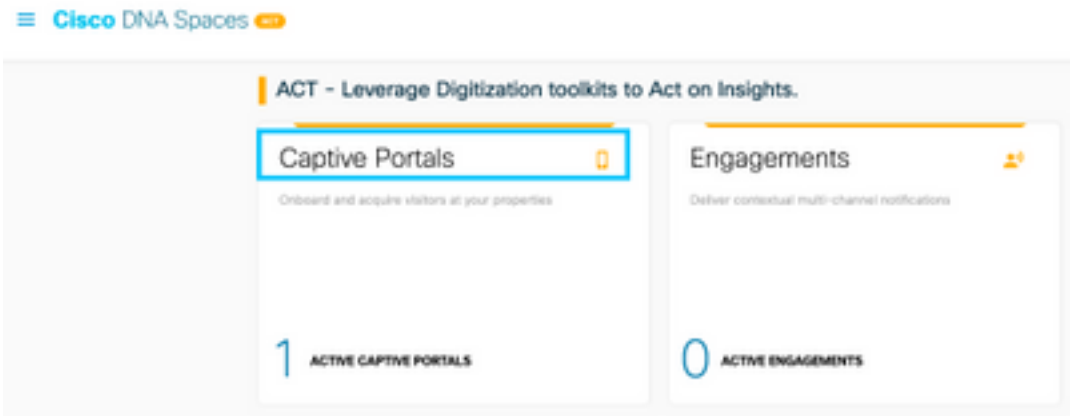
The controller needs to be connected to DNA Spaces using any of the available setups, Direct Connect, via DNA Spaces Connector or using CMX Tethering.

In this example, the Direct Connect option is in use, although captive portals are configured the same way for all the setups.

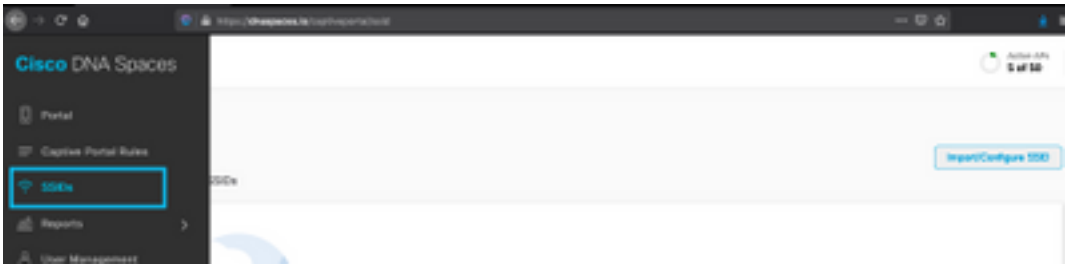
To connect the controller to Cisco DNA Spaces, it must be able to reach Cisco DNA Spaces cloud over HTTPS. For more information on how to connect the controller to DNA Spaces refer to this link: DNA Spaces Direct Connect Configuration Example

Create the SSID on DNA Spaces

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



Step 2. Open the captive portal menu by clicking the three lines icon in the upper left corner of the page, and click on **SSIDs:**

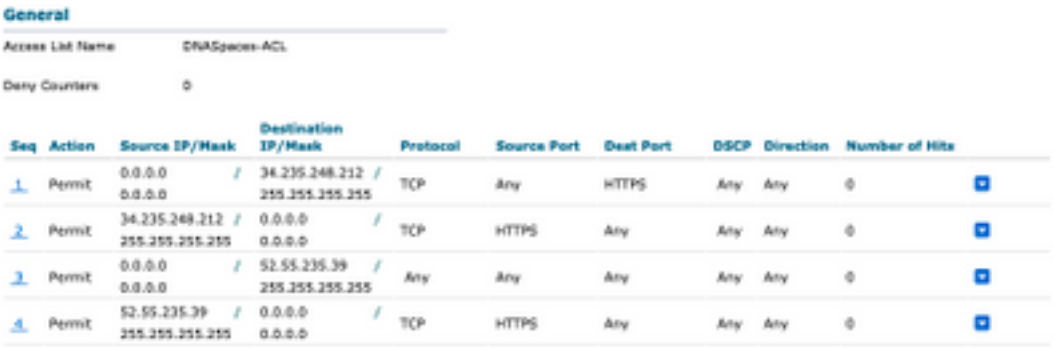


Step 3. Click on **Import/Configure SSID**, select **CUWN (CMX/WLC)** as the "Wireless Network" type, and enter the SSID name:

ACL configuration on the controller

A pre-authentication ACL is required as this is a web authentication SSID, and as soon as the wireless device connects to the SSID and receives an IP address, the device's policy manager state moves to the **Webauth_Reqd** state and the ACL is applied to the client session to restrict the resources the device can reach.

Step 1. Navigate to **Security > Access Control Lists > Access Control Lists,** click on **New** 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:



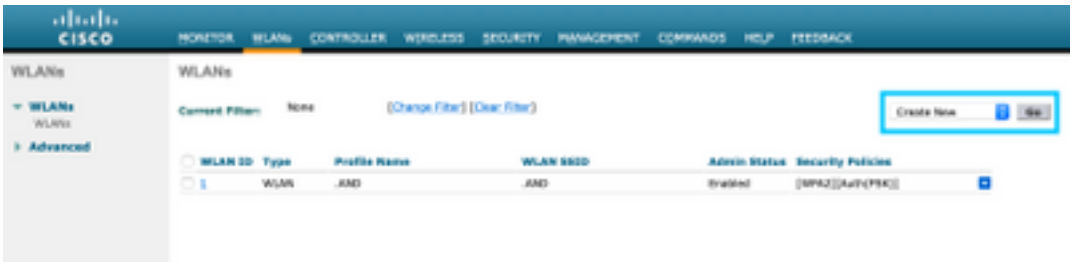
> **Note**: To get the IP addresses of DNA Spaces to be allowed in the ACL, click on the **Configure Manually** option from the SSID created in step 3 of section **Create the SSID on DNA Spaces** under the ACL configuration section.

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.

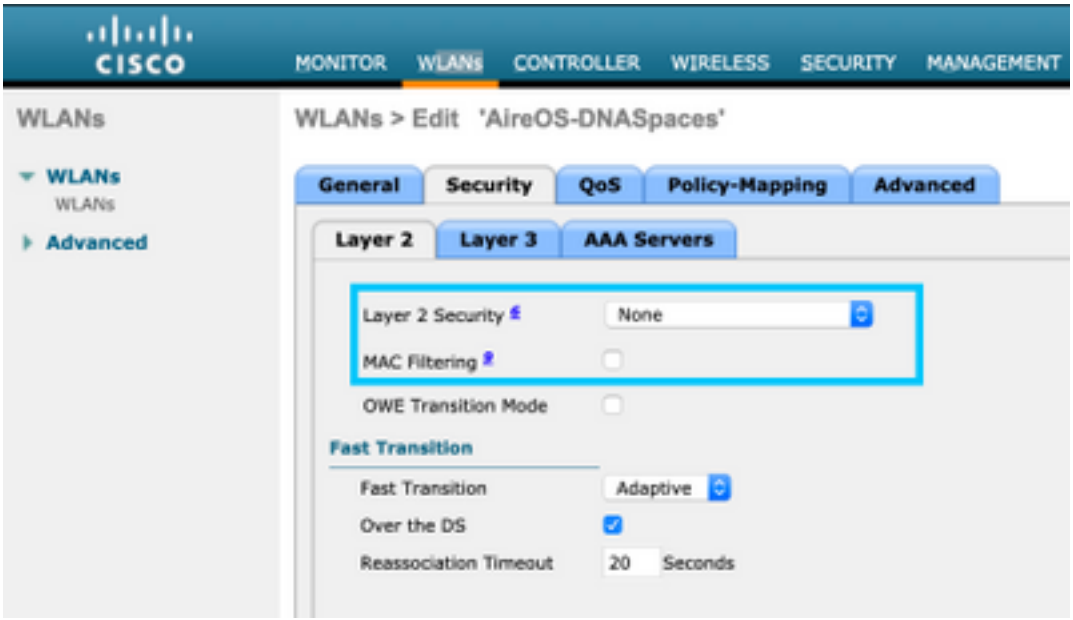
Captive Portal without RADIUS Server on DNA Spaces

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.

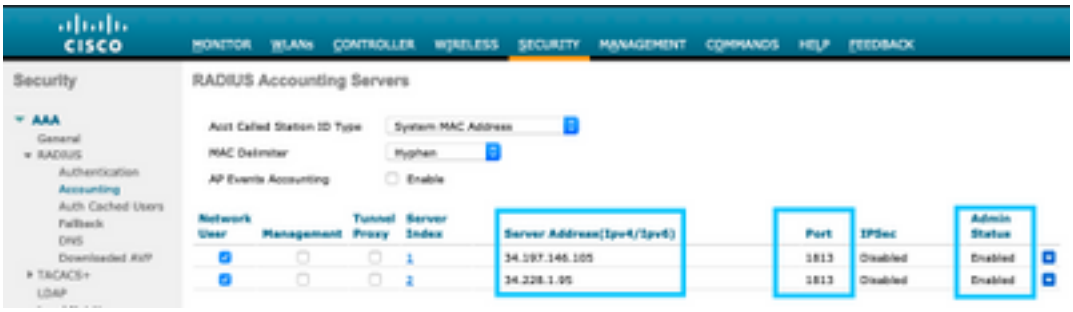
RADIUS Servers configuration on the controller

Step 1. Navigate to **Security > AAA > RADIUS > Authentication,** click on **New** and enter the RADIUS server information. Cisco DNA Spaces acts a the RADIUS server for user authentication

and it can respond on two IP addresses. Configure both RADIUS servers:

> **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:

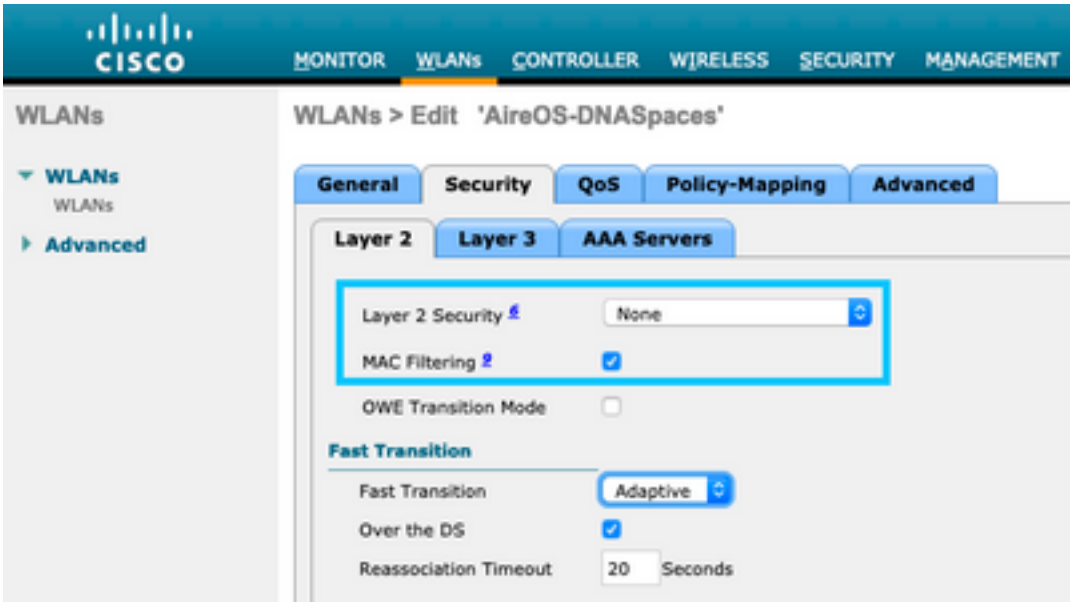


SSID configuration on the controller

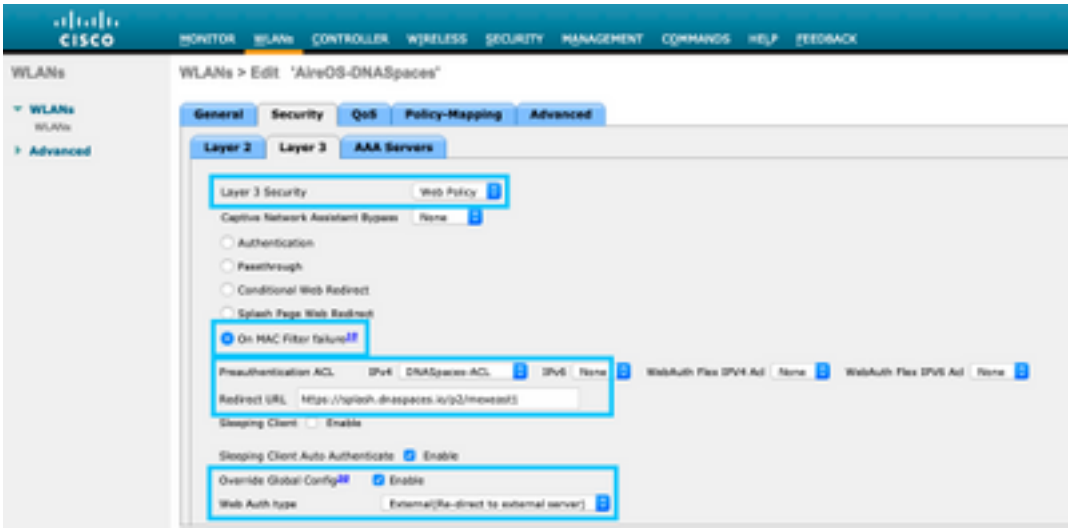
> **Important**: Before starting with the SSID configuration, make sure that **Web Radius Authentication** is set to "PAP" under Controller > General.

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.**

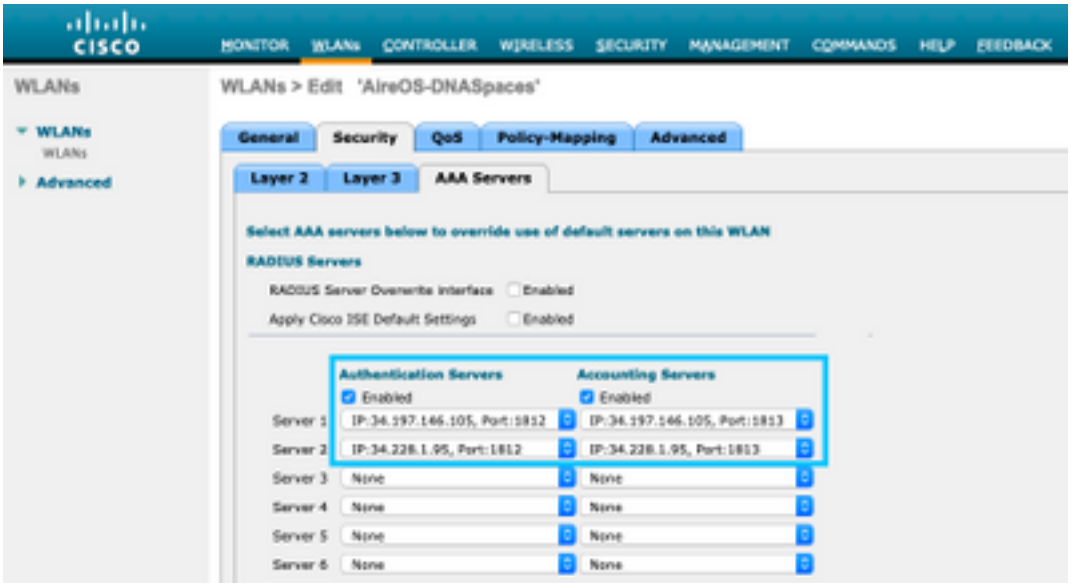
Step 2. Configure layer 2 security. Navigate to the **Security > Layer 2** tab in the WLAN configuration tab. Configure Layer 2 Security as **None**. Enable Mac Filtering.



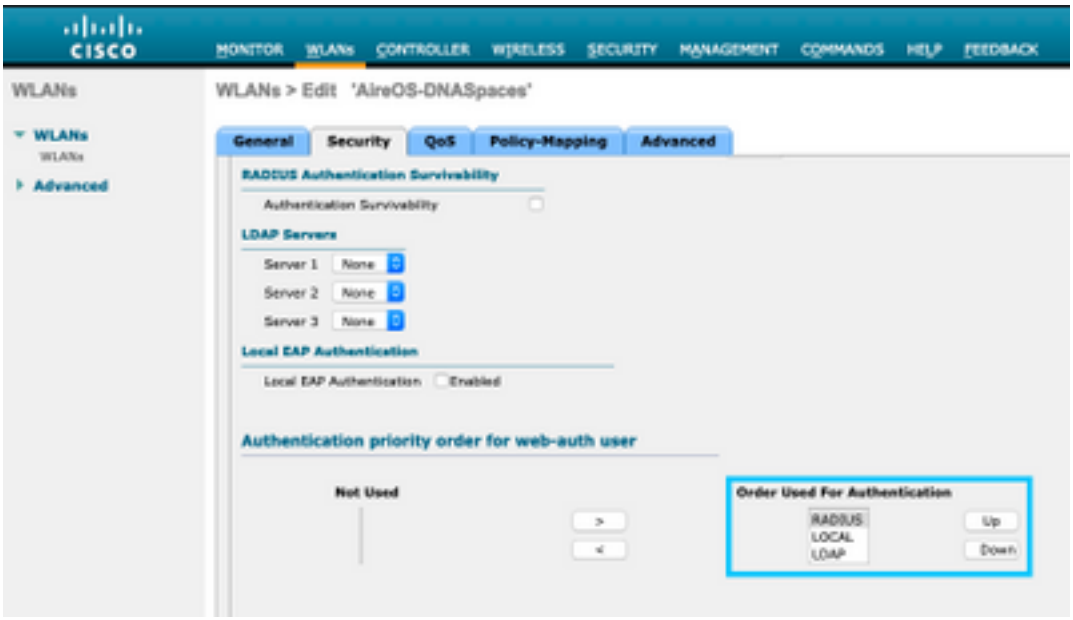
Step 3. Configure layer 3 security. Navigate to the **Security > Layer 3** tab in the WLAN configuration tab, configure **Web Policy** as the Layer 3 security method, Enable **On Mac Filter failure**, configure the preauthentication ACL, enable **Override Global Config** as set the **Web Auth Type**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



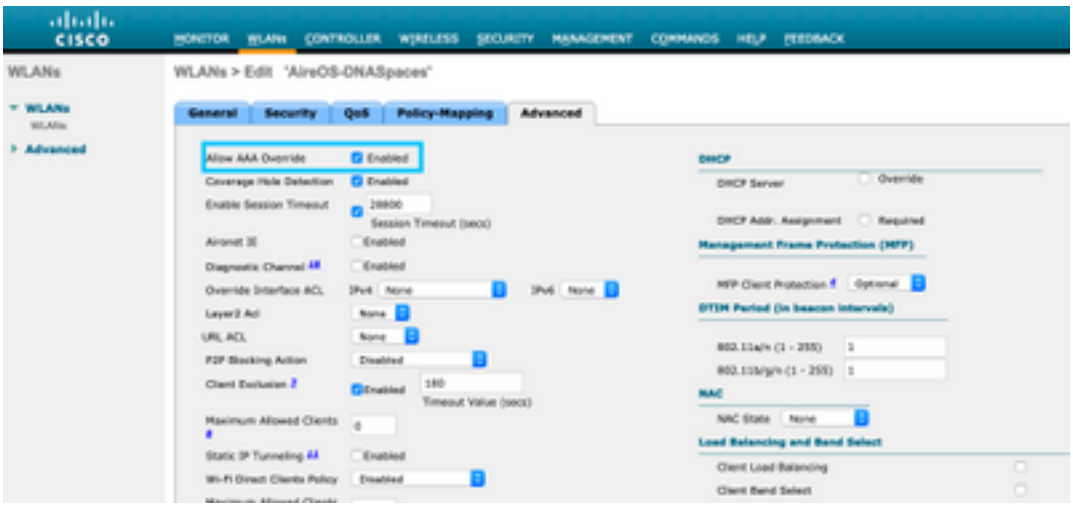
Step 4. Configure AAA Servers. Navigate to the **Security > AAA Servers** tab in the WLAN configuration tab, enable **Authentication Servers** and **Accounting Servers** and from the drop-down menu choose the two RADIUS servers:



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.

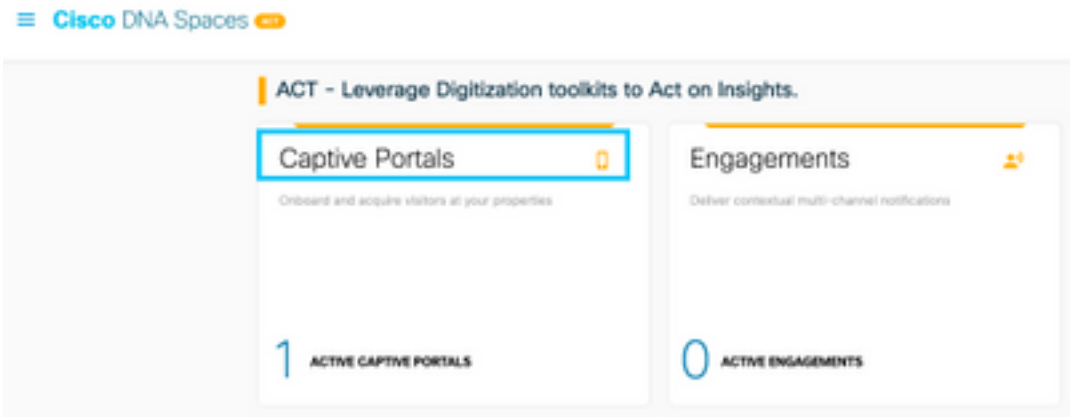


Step 7. Navigate to the **Advanced** tab in the WLAN configuration tab and enable **Allow AAA Override.**

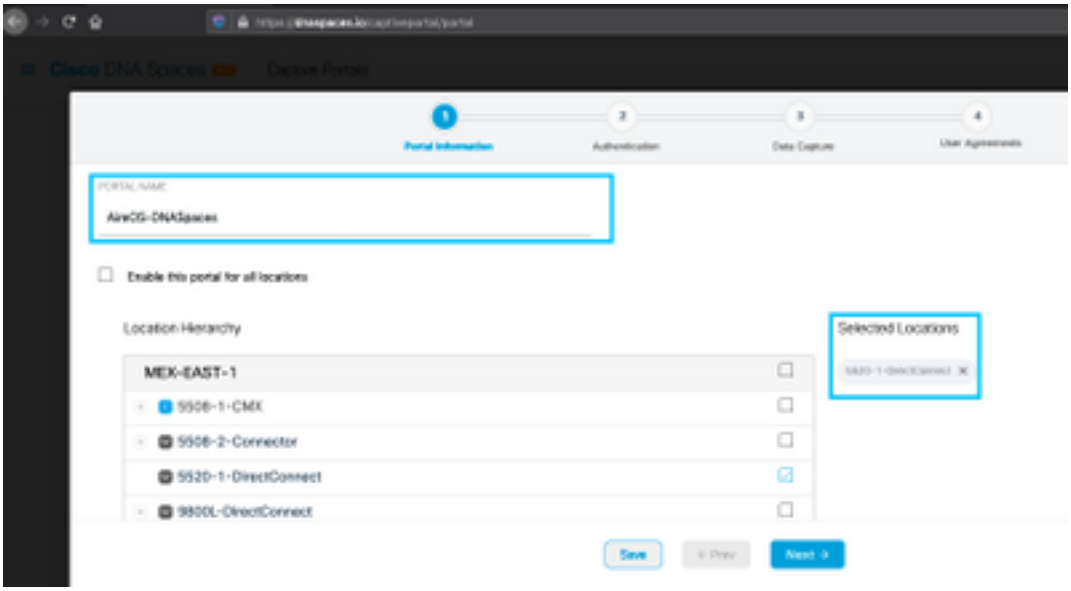


Create the portal on DNA Spaces

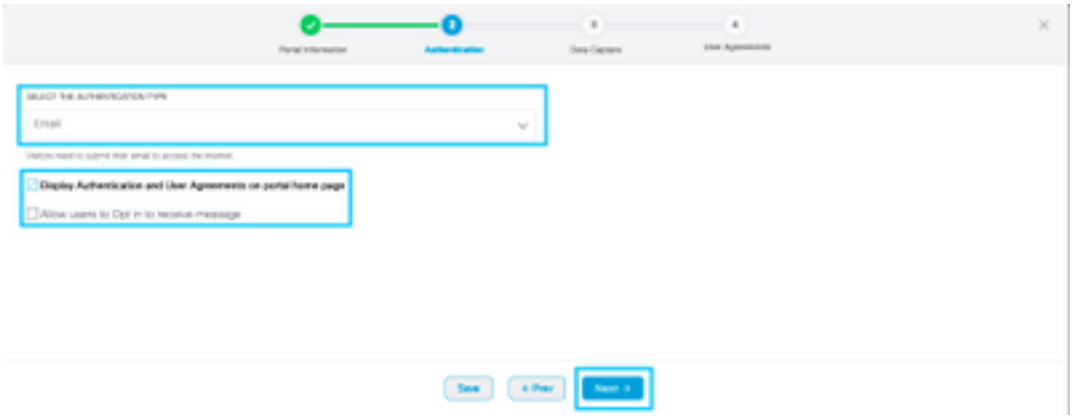
Step 1. Click on **Captive Portals** in the dashboard of DNA Spaces:



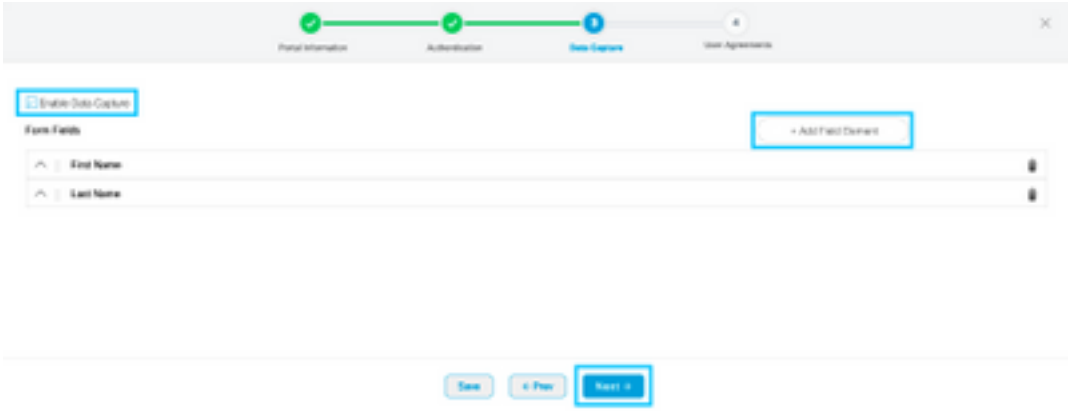
Step 2. Click on **Create New,** enter the portal name, and select the locations that can use the portal:



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**:

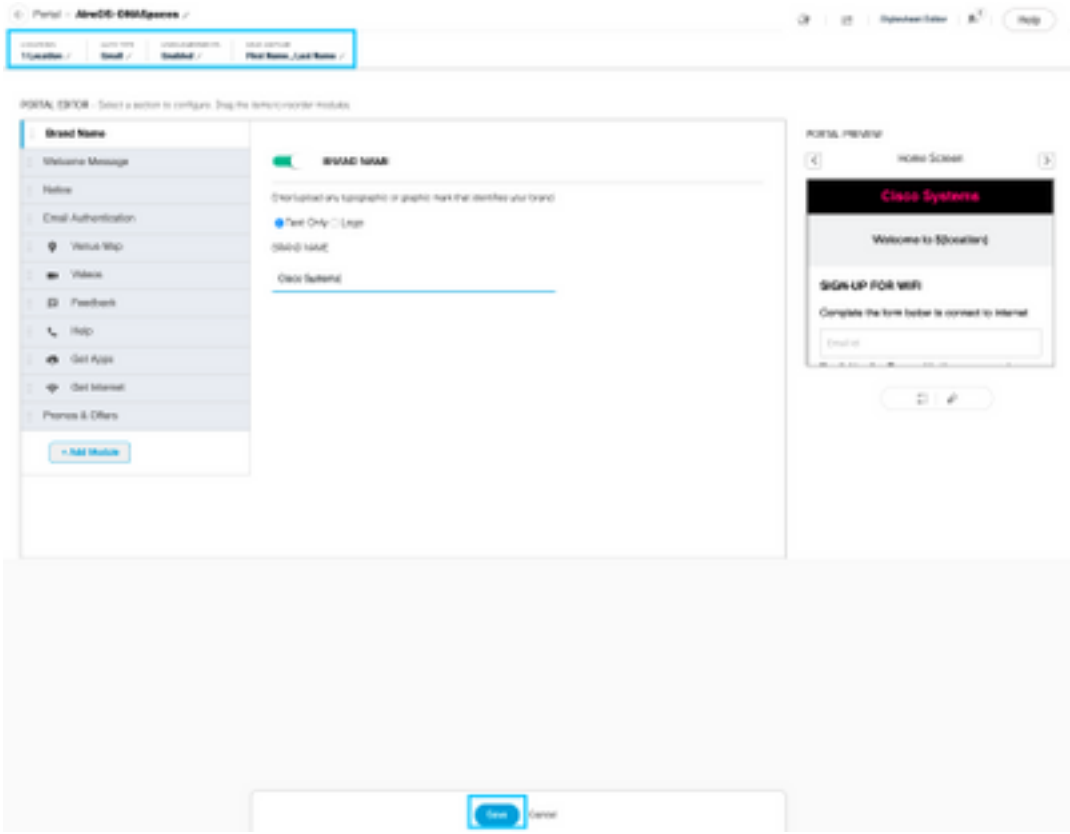


Step 4. Configure Data capture elements. If you want to capture data from the users, check the **Enable Data Capture** box and click on **+Add Field Element** to add the desired fields. Click **Next**:



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

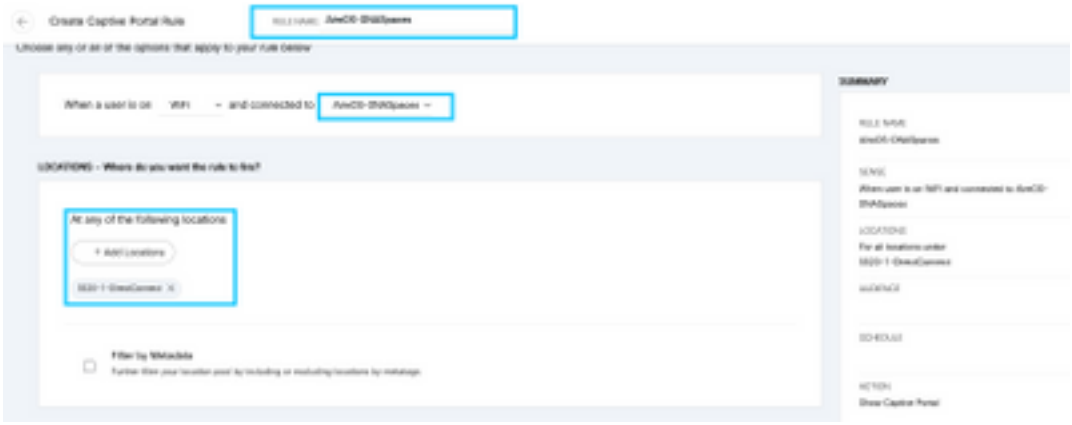
Step 6. Edit the portal as needed, Click on **Save:**



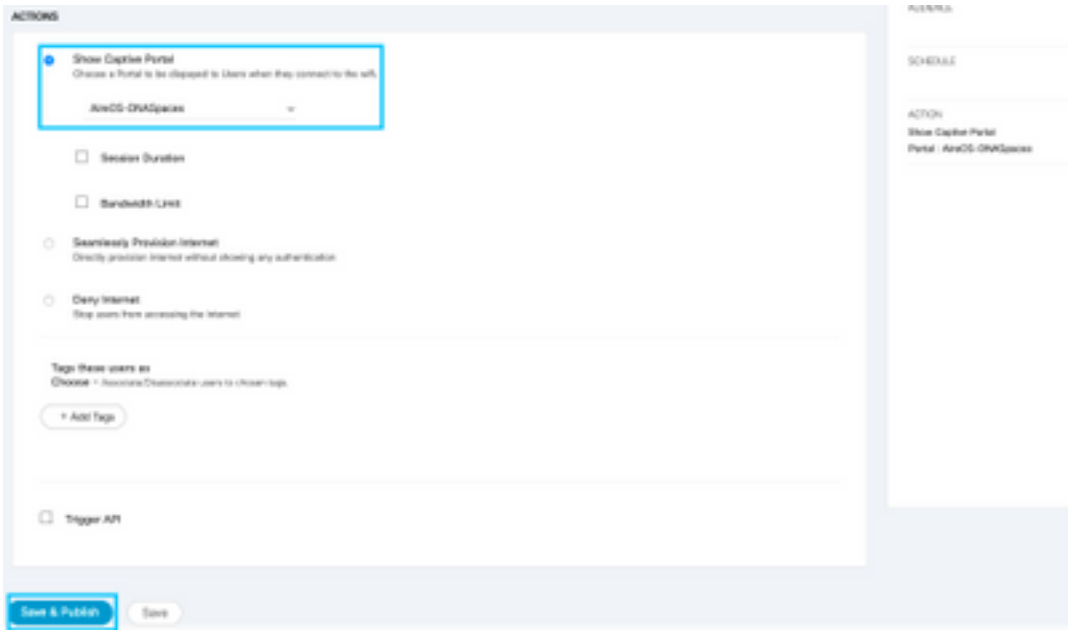
Configure the Captive Portal Rules on DNA Spaces

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:

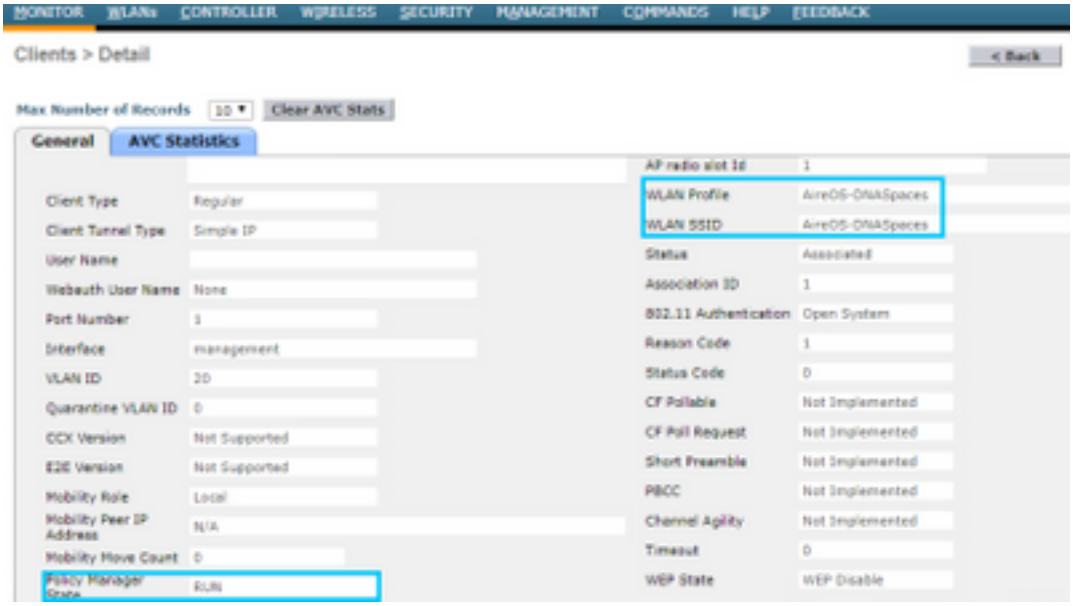


Step 3. Choose the action of the captive portal. In this case, when the rule is hit, the portal is shown. Click **Save & Publish.**



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:



Troubleshoot

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

```
(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:

```
*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION
REQUEST on BSSID 70:d3:79:dd:d2:0f destination addr 70:d3:79:dd:d2:0f slotid 1
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capabiility 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 AP:70:d3:79:dd:d2:00-01 ssid : AireOS-DNASpaces thread:bd271d6280
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode
(1), Result (0), Ssid (AireOS-DNASpaces), ApMac (70:d3:79:dd:d2:00), RSSI (-72), SNR (22)
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 on apVapId 1
```

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, client mac=34:e1:2d:23:a6:68
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68
user_agent = AnyConnect Agent 4.7.04056
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual
IP, using virtual IP =192.0.2.1
*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://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio ), redirect URL is
now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wla
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is
<HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"
content="no-cache"><META http-equiv="Pragma" content="
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=Ai
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=AireOS-DNASpaces&r

*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:d3:79:
dd:d2:00&client_mac=34:
*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:d3:79:
dd:d2:00&client_mac=34:e1:2d:23
*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 to RUN (20) last state WEBAUTH_NOL3SEC (14)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode
(0), Result (0), ServerIp (), UserName ()
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result
(0), Role (1), VLAN/VNID (20), Ipv4Addr (10.10.30.42), Ipv6Present (No)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255,URL ACL ID 255,URL ACL
Action 0)

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