

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

 Cisco 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	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	TCP	HTTPS	Any	Any	Any	0	
3	Permit	0.0.0.0 /0	92.55.235.39 /255.255.255.255	Any	Any	Any	Any	Any	0	
4	Permit	53.55.235.39 /255.255.255.255	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**.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	ANO	ANO	Enabled	[WPA2] Auth[PSK]

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.

The screenshot shows the Cisco AireOS-DNAspaces WLAN configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The left sidebar shows 'WLANs' and 'Advanced'. The main title is 'WLANs > Edit 'AireOS-DNAspaces''. The tab bar at the top has tabs for General, Security, QoS, Policy-Mapping, Advanced, Layer 2, Layer 3 (which is selected), and AAA Servers. The Layer 3 tab contains sections for Layer 2 Security (set to None), MAC Filtering (unchecked), OWE Transition Mode (unchecked), Fast Transition (set to Adaptive), Over the DS (checked), and Reassociation Timeout (set to 20 Seconds). A blue box highlights the 'Layer 2 Security' dropdown.

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.

This screenshot shows the same WLAN configuration interface as above, but with more fields highlighted with blue boxes. In the Layer 3 Security section, 'Web Policy' is selected. Under 'Passthrough' options, 'Passthrough' is checked. In the 'Preauthentication ACL' section, 'DnASpaces-ACL' is selected. In the 'Override Global Config' section, 'Enable' is checked and 'Web Auth Type' is set to 'External(Re-direct to external server)'. Other fields like 'Captive Network Assistant Response', 'Authentication', 'Conditional Web Redirect', 'Splash Page Web Redirect', 'On MAC Filter Failure', 'Web policy done locally on AP', 'Or Code Scanning', 'Redirect URL', 'Email Input', 'Sleeping Client', 'Sleeping Client Auto Authenticate', and 'WebAuth File (Pre-Auth)' are also visible but not highlighted.

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:

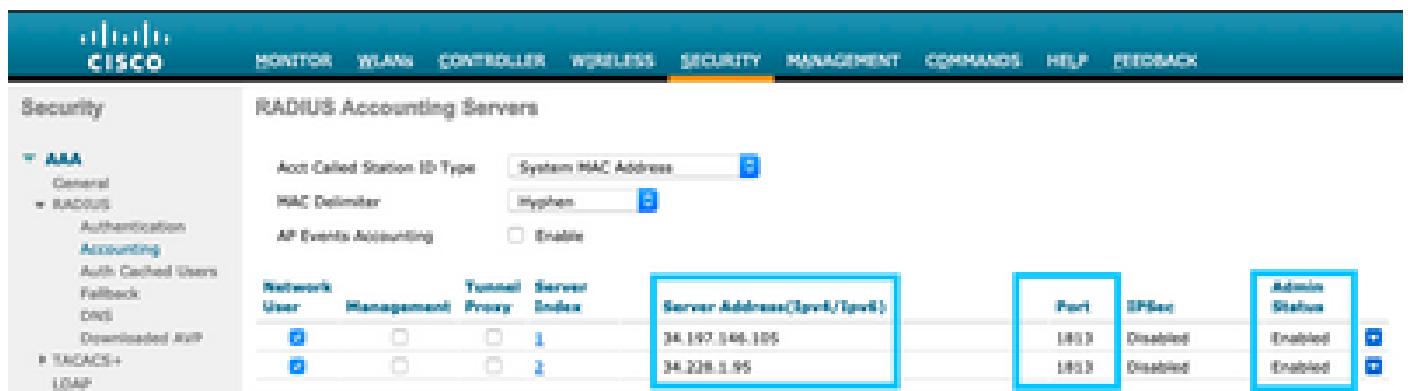


Network	User	Management	Tunnel	Server	Address
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	34.197.2.86:500
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	34.238.1.85

Port	IPSec	Admin Status
1812	Disabled	Enabled
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:



Network	User	Management	Tunnel	Server	Address
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	34.197.2.86:100
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	34.238.1.85:100

Port	IPSec	Admin Status
1813	Disabled	Enabled
1813	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**.

The screenshot shows the Cisco AireOS interface under the 'WLANs' tab. On the left, there's a navigation tree with 'WLANs' selected. The main area displays a table for WLAN profiles. One profile is listed: 'ano' (Type: WLAN, Profile Name: ano, WLAN ID: ano, Admin Status: Enabled, Security Policies: [wlan1] Auth(Pax)]. There are buttons for 'Create New' and 'Get'.

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.

The screenshot shows the Cisco AireOS interface under the 'WLANs' tab, specifically the 'Edit "AireOS-DNAspaces"' configuration. The 'Security' tab is active. Within the 'Layer 3' sub-tab, the 'Layer 2 Security' dropdown is set to 'None'. The 'MAC Filtering' checkbox is checked. Other settings like 'OWE Transition Mode' and 'Fast Transition' are also visible.

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.

The screenshot shows the Cisco AireOS-DNAspaces WLAN configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar has sections for WLANs (selected) and Advanced. The main area is titled 'WLANs > Edit 'AireOS-DNAspaces''. The tabs at the top are General, Security, QoS, Policy-Mapping, and Advanced. The sub-tab selected is Layer 3, which is highlighted in blue. Under Layer 3, the 'AAA Servers' tab is also highlighted. The 'Layer 3 Security' section is active, indicated by a blue border. It contains the following settings:

- Captive Network Assistant System:** None
- Authentication:** On MAC Filter (selected)
- Preauthentication ACL:** IPv4: DNAspaces-ACL, IPv6: None
- Redirect URL:** https://dnaspace.dnaspaces.local/g2/moved1
- Steaming Client:** Enabled
- Steaming Client Auto Authenticate:** Enabled
- Override Global Config:** Enabled
- Web Auth Type:** External (to direct to external server)

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:

The screenshot shows the Cisco AireOS-DNAspaces WLAN configuration interface. The top navigation bar and sidebar are identical to the previous screenshot. The main area is titled 'WLANs > Edit 'AireOS-DNAspaces''. The tabs at the top are General, Security, QoS, Policy-Mapping, and Advanced. The sub-tab selected is Layer 3, which is highlighted in blue. Under Layer 3, the 'AAA Servers' tab is also highlighted. The 'Select AAA servers below to override use of default servers on this WLAN' message is displayed. The 'RADIUS Servers' section contains the following settings:

- RADIUS Server Overwrite Interface:** Enabled
- Apply Cisco ISE Default Settings:** Enabled

The 'Authentication Servers' and 'Accounting Servers' sections are highlighted with a blue border. Both sections have the 'Enabled' checkbox checked. The table lists six servers, with the first two being configured:

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP: 34.197.146.105, Port: 1812	<input checked="" type="checkbox"/> Enabled IP: 34.197.146.105, Port: 1813
Server 2	<input checked="" type="checkbox"/> Enabled IP: 34.228.1.95, Port: 1812	<input checked="" type="checkbox"/> Enabled IP: 34.228.1.95, Port: 1813
Server 3	<input type="checkbox"/> None	<input type="checkbox"/> None
Server 4	<input type="checkbox"/> None	<input type="checkbox"/> None
Server 5	<input type="checkbox"/> None	<input type="checkbox"/> None
Server 6	<input type="checkbox"/> None	<input type="checkbox"/> None

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.

WLANs > Edit 'AireOS-DNAspaces'

General Security QoS Policy-Mapping Advanced

RADIUS Authentication Survivability

Authentication Survivability

LDAP Servers

Server 1: None

Server 2: None

Server 3: None

Local EAP Authentication

Local EAP Authentication: Enabled

Authentication priority order for web-auth user

Not Used

Order Used For Authentication

RADIUS LOCAL LDAP

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

WLANs > Edit 'AireOS-DNAspaces'

General Security QoS Policy-Mapping Advanced

Allow AAA Override

Coverage Hole Detection

Enable Session Timeout 36000 Session Timeout (sec)

Aironet ID Enabled

Diagnostic Channel Enabled

Override Interface ACL

Layer 2 ACL

URL ACL

PPPoE Blocking Action

Client Elevation Enabled Timeout Value (sec): 180

Maximum Allowed Clients

Static IP Tuning Enabled

Wi-Fi Direct Clients Policy

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

Management Frame Protection (MFP)

MFP Client Protection Optional

BTIM Period (in seconds intervals)

802.11ax (1 - 255)

802.11bgn (1 - 255)

RAK

RAK State

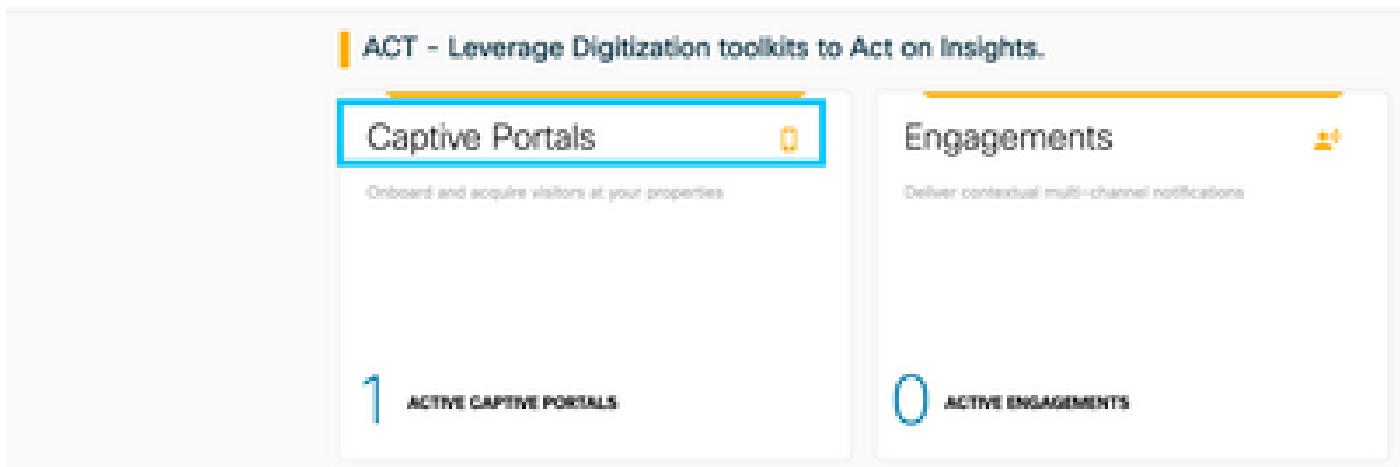
Load Balancing and Band Select

Client Load Balancing

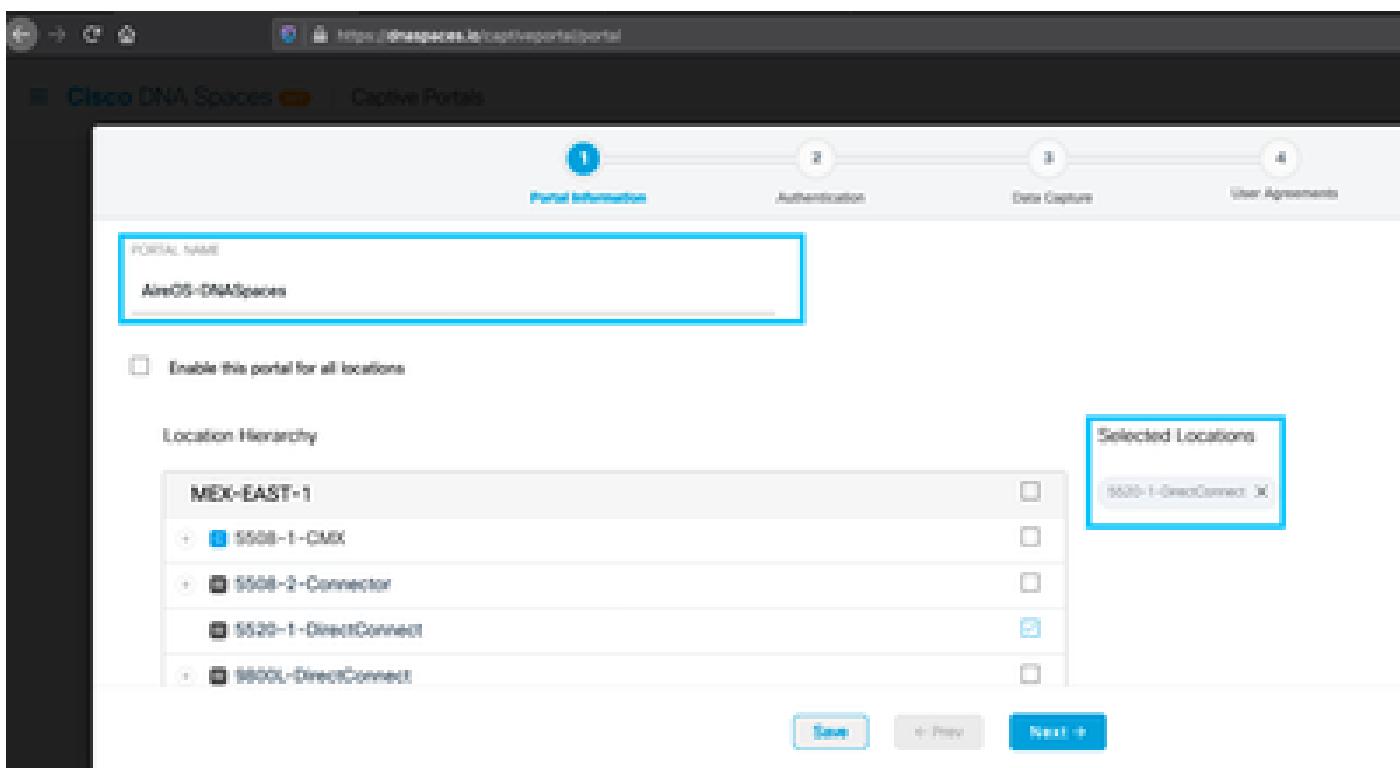
Client Band Select

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**:

SELECT THE AUTHENTICATION TYPE

Email

Instructions: Enter the email to access the portal.

Display Authentication and User Agreements on portal home page
 Allow users to Opt in to receive message

Next **+ Prev** **Save & 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**:

Enable Data Capture

Add Field Element

First Name

Last Name

Next **+ Prev** **Save & Next**

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

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

Enable Terms & Conditions

TERMS & CONDITION MESSAGE

MCA Terms of Use, Last updated September 20, 2017
 These MCA Terms & Conditions Of Use (the "MCA Terms") together with the TELMCA ("TEL") govern your use of the TEL service.
 Description of the Service:
 The Service provides you with wireless access to the Internet within the premises. We do not act as ordinary providers, privately monitor the activities of those who use the Service or exercise any editorial control over any material transmitted, posted or posted using the Service to ensure that users comply with these MCA Terms under the law, although it reserves the right to do so.

Save & Configure Portal

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

PORTAL: PORTALS - Click a section to configure. Drag the items to reorder modules.

Brand Name

Captive Portal Rules

Welcome Message

Footer

Email Authentication

Virtual Map

Values

Feedback

Help

Get Apps

Get Internet

Process & Offers

+ Add Module

PORTAL PREVIEW

Cisco Systems

Welcome to (location)

SIGN-UP FOR WiFi

Complete the form below to connect to internet

Email or

Configure the Captive Portal Rules on DNA Spaces

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

Cisco DNA Spaces

Portal

Captive Portal Rules

SSIDs

Reports

Created
Feb 24, 2020 8:03 PM

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:

The screenshot shows the 'Create Captive Portal Rule' interface. At the top, it says 'Create Captive Portal Rule' and 'Rule name: AerOS-DPAQspace'. Below that, it asks 'Choose any or all of the options that apply to your rule below'. A section titled 'LOCATION(S) - Where do you want the rule to hit?' contains a box labeled 'At any of the following locations' with a 'Add Locations' button and a selected location 'AEROS-DPAQspace'. There's also a 'Filter by Metadata' checkbox. To the right, a 'SUMMARY' panel lists the rule name and selected location.

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

The screenshot shows the 'Actions' section of the rule configuration. It includes a 'Show Captive Portal' section with a note 'Choose a portal to be displayed to users when they connect to the rule.' and a dropdown menu set to 'AerOS-DPAQspace'. Other action options like 'Session Duration' and 'Deny Internet' are listed but not selected. To the right, a summary panel shows the rule name and selected portal.

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:

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Clients > Detail < Back

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	AuraOS-DNA Spaces
User Name		WLAN SSID	AuraOS-DNA Spaces
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	OF Pollable	Not Implemented
E2E Version	Not Supported	OF Poll Request	Not Implemented
Mobility Role	Local	Short Preamble	Not Implemented
Mobility Peer IP Address	N/A	PBCC	Not Implemented
Mobility Move Count	0	Channel Agility	Not Implemented
Policy Manager Status	RUN	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:

```
*apfOpenDtSocket: 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 configured
*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
```

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
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode (0), Result (0)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result (0), Reason (0)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully plumbed mobile

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