Configure Spaces Captive Portal with Catalyst 9800 WLC

Contents

Introduction

This document describes how to configure captive portals on Cisco Spaces.

Prerequisites

This document allows clients on the Catalyst 9800 Wireless LAN Controller (C9800 WLC) to use Spaces as an external web authentication log in page.

Requirements

Cisco recommends that you have knowledge of these topics:

- Command Line Interface (CLI) or Graphic User Interface (GUI) access to the 9800 wireless controllers
- Cisco Spaces

Components Used

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

- 9800-L controller version 16.12.2s

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Web Authentication is a simple Layer 3 authentication method without the need for a supplicant or client utility. This can be done

a) With the Internal Page on C9800 WLC either as is or post modifications.

b) With customized log in bundle uploaded to C9800 WLC.

c) Custom log in page hosted on an external server.

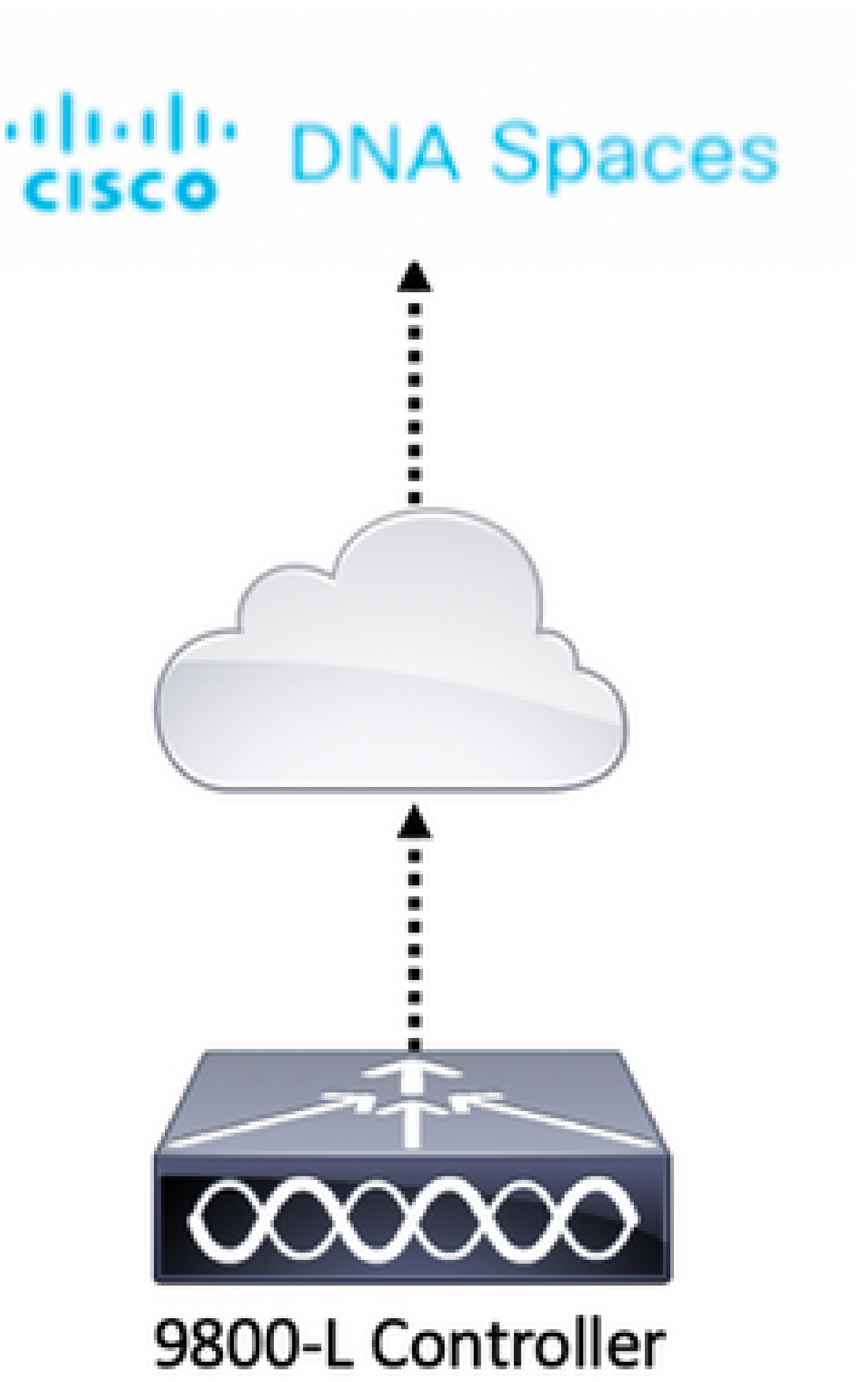
To leverage the captive portal provided by Spaces is essentially a way to implement external web authentication for clients on C9800 WLC.

External webauth process is described in detail at: Web-Based Authentication on Cisco Catalyst 9800 Series Controllers

On C9800 WLC, the virtual-ip address is defined the global parameter-map and is typically 192.0.2.1

Configure

Network Diagram


cisco DNA Spaces
9800-L Controller

```
Extended IP access list WA-sec-10.235.248.212
10 permit tcp any host 10.235.248.212 eq www
20 permit tcp any host 10.235.248.212 eq 443
30 permit tcp host 10.235.248.212 eq www any
40 permit tcp host 10.235.248.212 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-10.235.248.212
10 deny tcp any host 10.235.248.212 eq www
20 deny tcp any host 10.235.248.212 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

WA-sec-10.235.248.212 is called as such because it is an automatic Web auth (WA) security (sec) ACL or portal ip 10.235.248.212. Security ACLs defined what is allowed (on permit) or dropped (on deny). Wa-v4-int is an intercept ACL, that is a punt ACL or redirect ACL, and defines what is sent to CPU for redirection (on permit) or what is sent to dataplane (on deny).

WA-v4-int10.235.248.212 is applied first on traffic coming from the client and keeps HTTP(s) traffic towards Spaces portal IP 10.235.248.212 on the dataplane (not drop or forward action yet, just hand over to dataplane). It sends to CPU (for redirection except virtual IP traffic which is serviced by the web server) all HTTP(s) traffic. Other types of traffic are given to the dataplane.

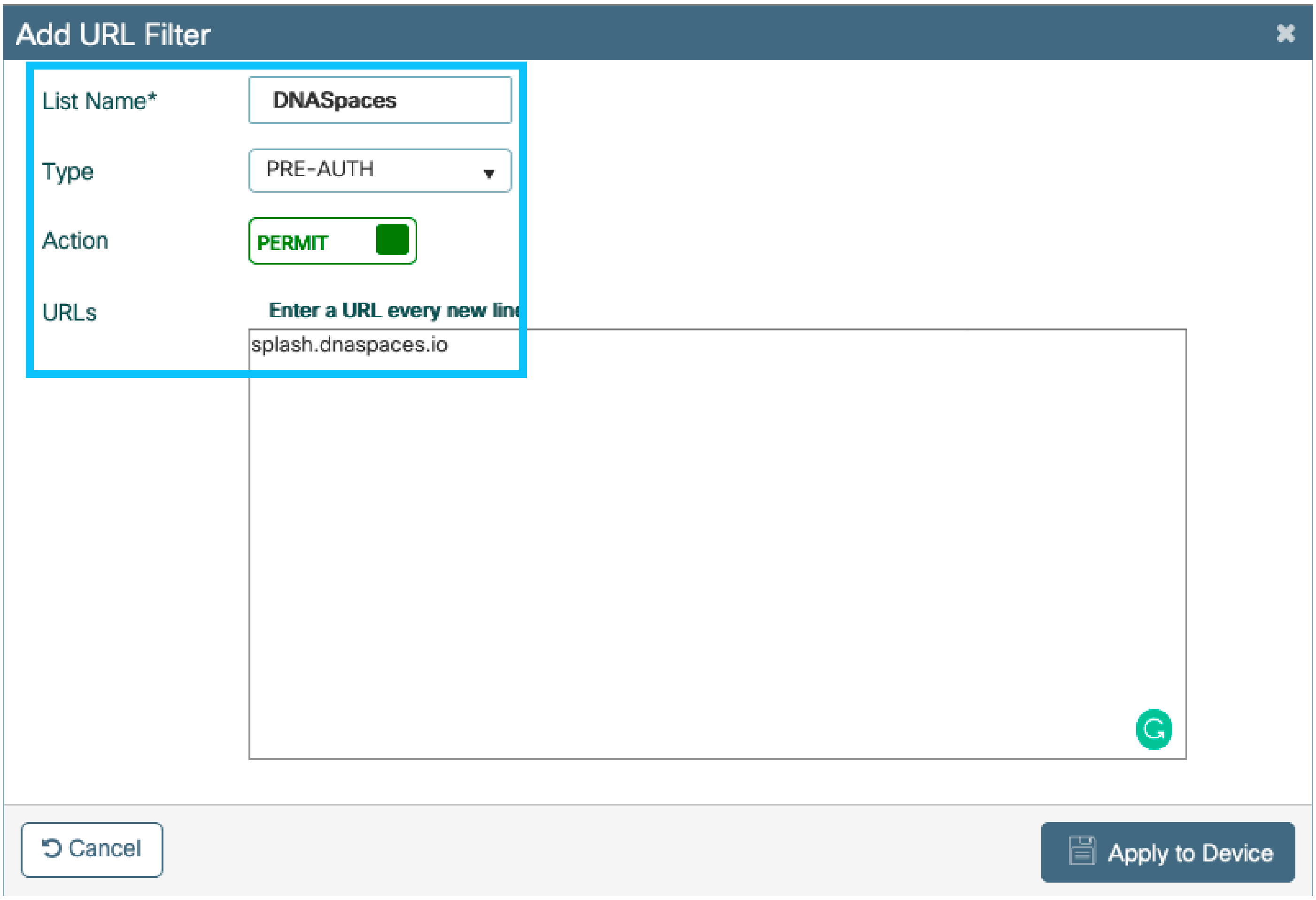
WA-sec-10.235.248.212 permits HTTP and HTTPS traffic to the Cisco DNA space IP 10.235.248.212 that you configured in the web authentication parameter map and it also allows DNS and DHCP traffic and drops the rest. HTTP traffic to be intercepted was already intercepted before it hits this ACL and therefore does not need to be covered by this ACL.

Note: To get the IP addresses of Spaces to be allowed in the ACL, click the **Configure Manually** option from the SSID created in step 3 of section **Create the SSID on Spaces** under the ACL configuration section. An example is located in the section, What are the IP addresses that Spaces use, at the end of the document.

Spaces uses 2 IP addresses and the mechanism in step 1 only allows for one portal IP to be allowed. To allow pre-authentication access to more HTTP resources, you need to use URL filters which dynamically makes holes in the intercept (redirect) and security (preauth) ACLs for the IPs related to the website whose URL you enter in the URL filter. DNS requests are dynamically snooped for the 9800 to learn the IP address of those URLs and add it to the ACLs dynamically.

Step 2. Configure the URL filter to allow the Spaces domain.

Navigate to **Configuration > Security > URL Filters**. Click **+Add** and configure the list name. Select **PRE-AUTH** as the type, **PERMIT** as the action, and the URL **splash.dnaspaces.io** (or .eu if you use the EMEA portal):



List Name* DNASpaces

Type PRE-AUTH

Action PERMIT

URLs Enter a URL every new line

splash.dnaspaces.io

CLI configuration:

<#root>

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

`urlfilter list <url-filter name>`

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

`action permit`

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

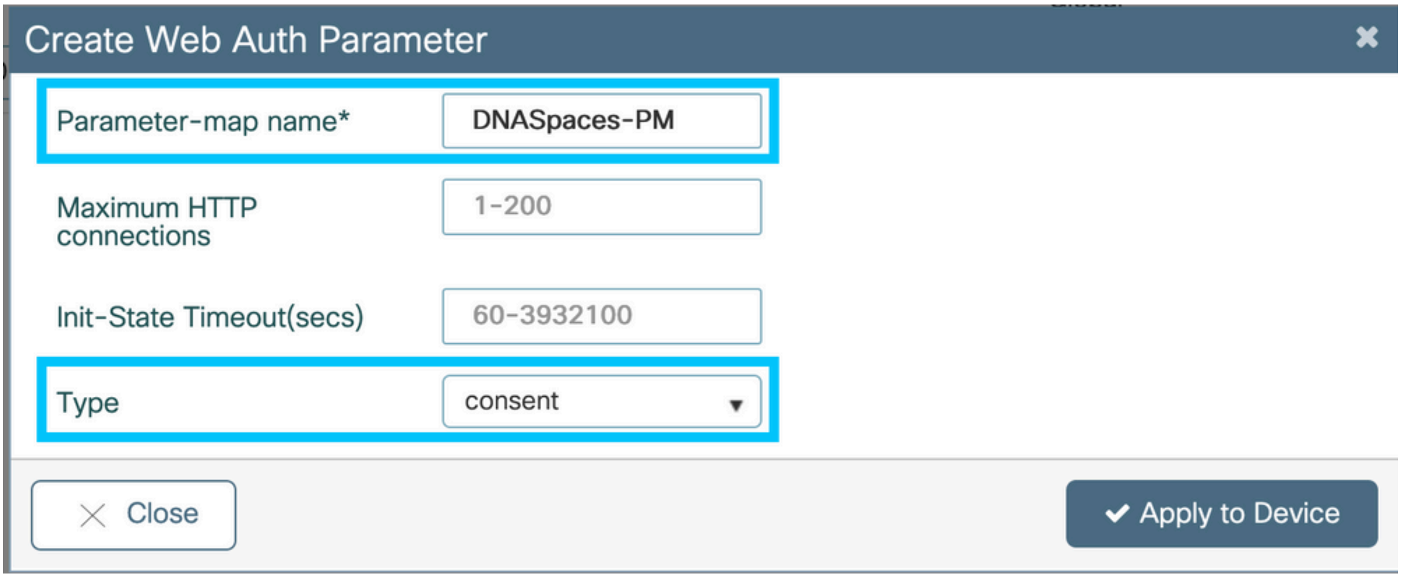
`url splash.dnaspaces.io`

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 Spaces are supported on both configurations.

Captive Portal without RADIUS Server on Spaces

Web Auth Parameter Map Configuration on the 9800 Controller

Step 1. Navigate to **Configuration** > **Security** > **Web Auth**. Click **+Add** to create a new parameter map. In the window that pops-up, configure the parameter map name, and select **Consent** as the type:



Create Web Auth Parameter

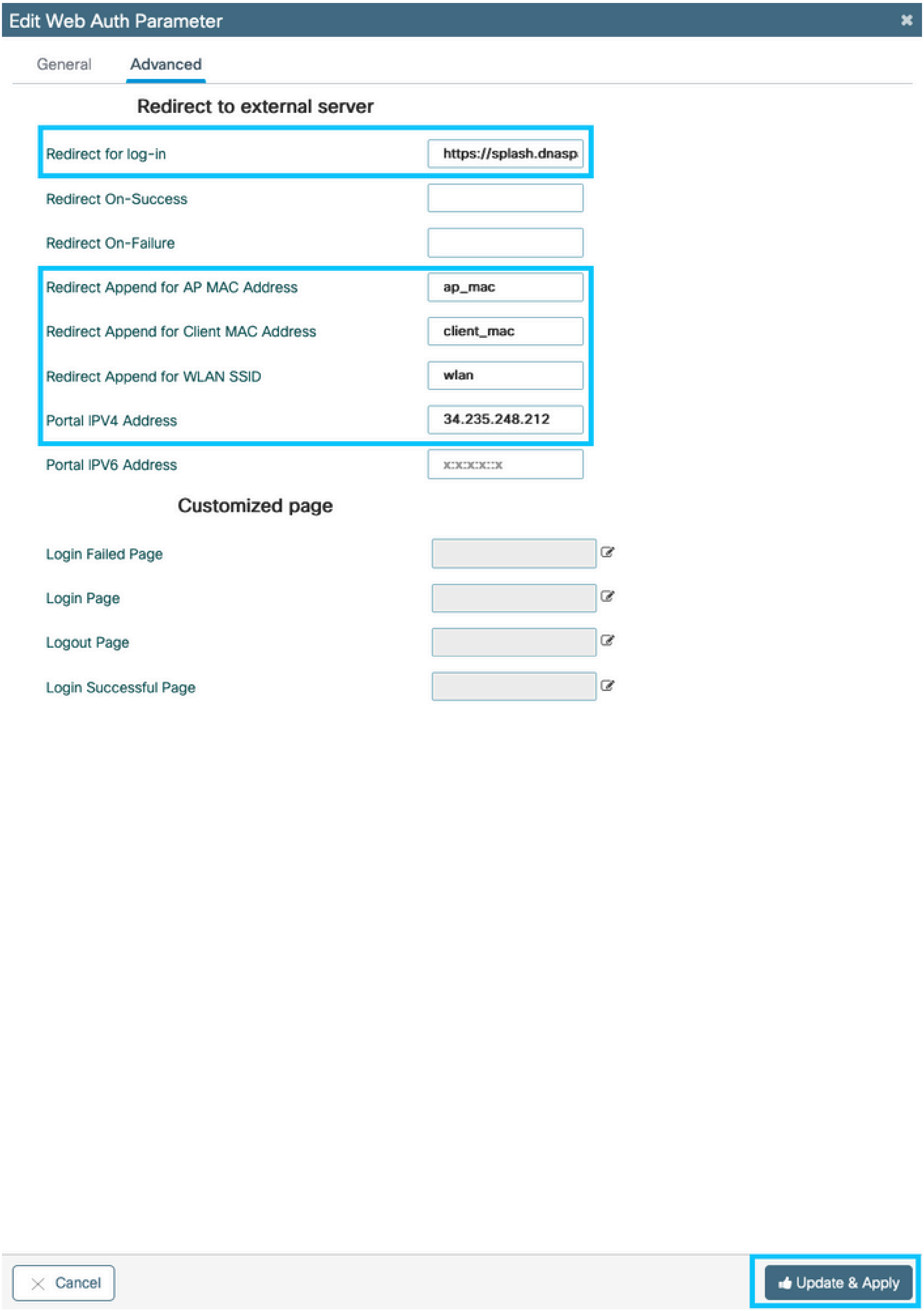
Parameter-map name* DNASpaces-PM

Maximum HTTP connections 1-200

Init-State Timeout(secs) 60-3932100

Type consent

Step 2. Click the **parameter map** configured in the previous step, navigate to the **Advanced** tab and enter the Redirect for log-in URL, Append for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID and portal IPv4 Address as illustrated. Click **Update & Apply**:



Redirect to external server

Redirect for log-in	https://splash.dnasp
Redirect On-Success	
Redirect On-Failure	
Redirect Append for AP MAC Address	ap_mac
Redirect Append for Client MAC Address	client_mac
Redirect Append for WLAN SSID	wlan
Portal IPV4 Address	34.235.248.212
Portal IPV6 Address	x:x:x:x::x

Customized page

Login Failed Page	
Login Page	
Logout Page	
Login Successful Page	

Note: To get the splash page URL and the IPv4 redirect address, click the **Configure Manually** option in the SSID page of Spaces. This is illustrated in the, What is the URL that Spaces portal use, at the end of the document.

Note: Cisco Spaces portal can resolve to two IP addresses, but the 9800 controller allows only one IP address to be configured. Choose any of those IP addresses and configure it on the parameter map as the Portal IPv4 Address.

Note: Ensure that both Virtual IPv4 and IPv6 addresses are configured in the global web auth parameter map. If the Virtual IPv6 is not configured, the clients are sometimes redirected to the internal portal instead of the configured Spaces portal. This is why a Virtual IP must always be configured. 192.0.2.1 can be configured as Virtual IPv4 and FE80:0:0:0:903A::11E4 as Virtual IPV6. There are little to no reasons to use other IPs than those.

CLI Configuration:

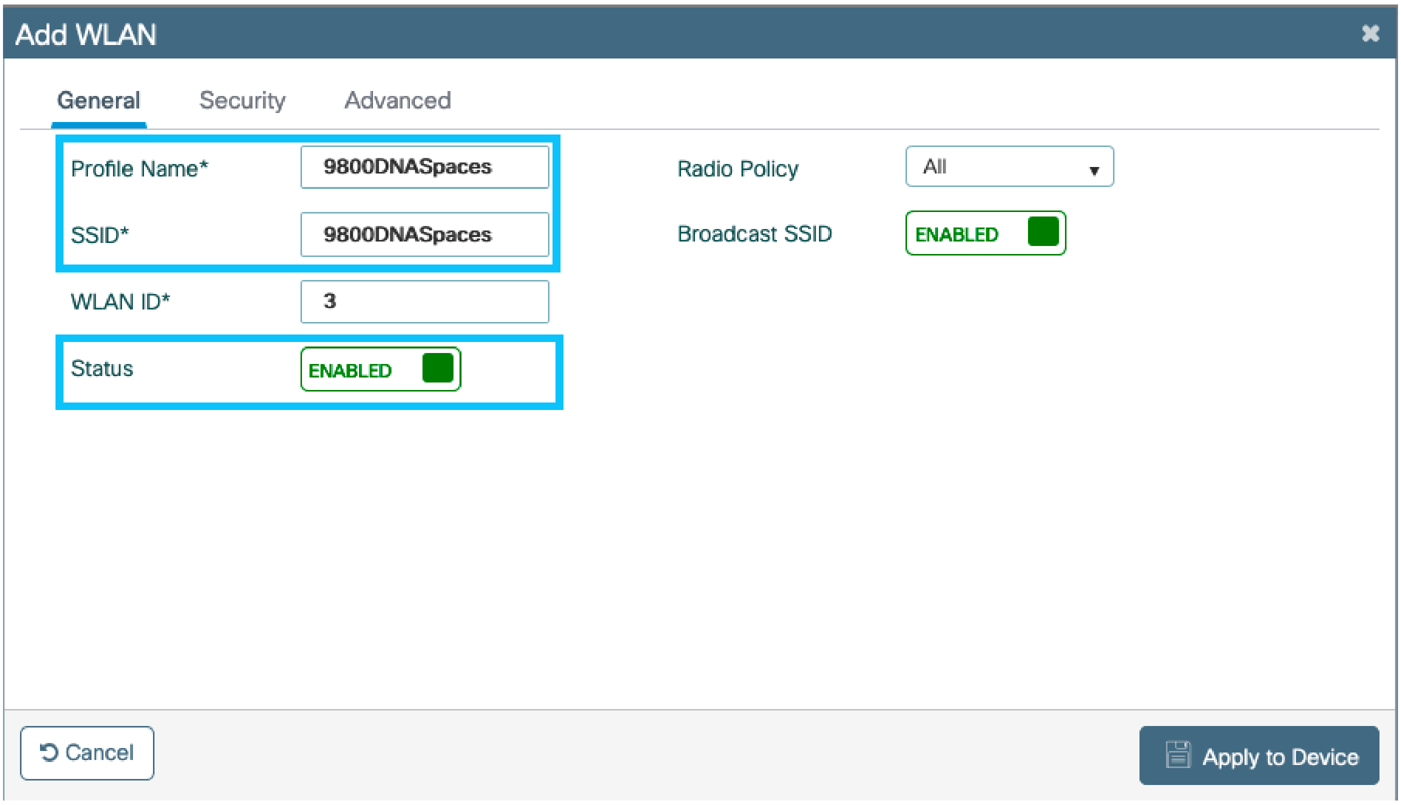
<#root>

```
Andressi-9800L(config)#

parameter-map type webauth <map name>


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 <splashpage URL>

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 <IP Address>

Andressi-9800L(config-params-parameter-map)#

logout-window-disabled

Andressi-9800L(config-params-parameter-map)#

success-window-disabled
```

Create the SSID on the 9800 Controller

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **WLANs**. Click **+Add**. Configure the Profile Name, SSID, and enable the WLAN. Make sure the SSID name is the same name as the configured in step 3 of section **Create the SSID on Spaces**.



Add WLAN

General | Security | Advanced

Profile Name* 9800DNASpaces

SSID* 9800DNASpaces

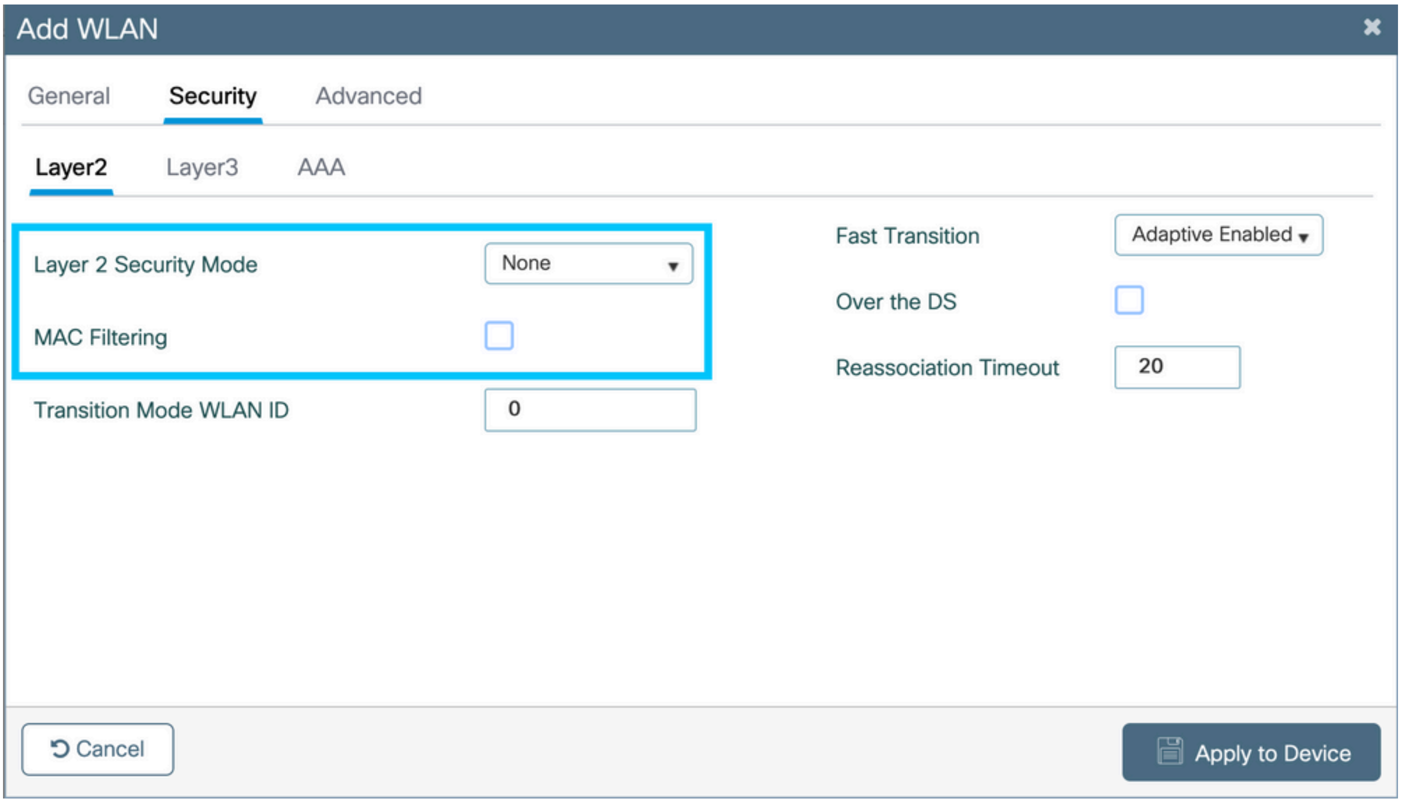
WLAN ID* 3

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED

Step 2. Navigate to **Security** > **Layer2**. Set the Layer 2 Security Mode to **None**. Make sure MAC Filtering is disabled.



Add WLAN

General | Security | Advanced

Layer2 | Layer3 | AAA

Layer 2 Security Mode None

MAC Filtering □

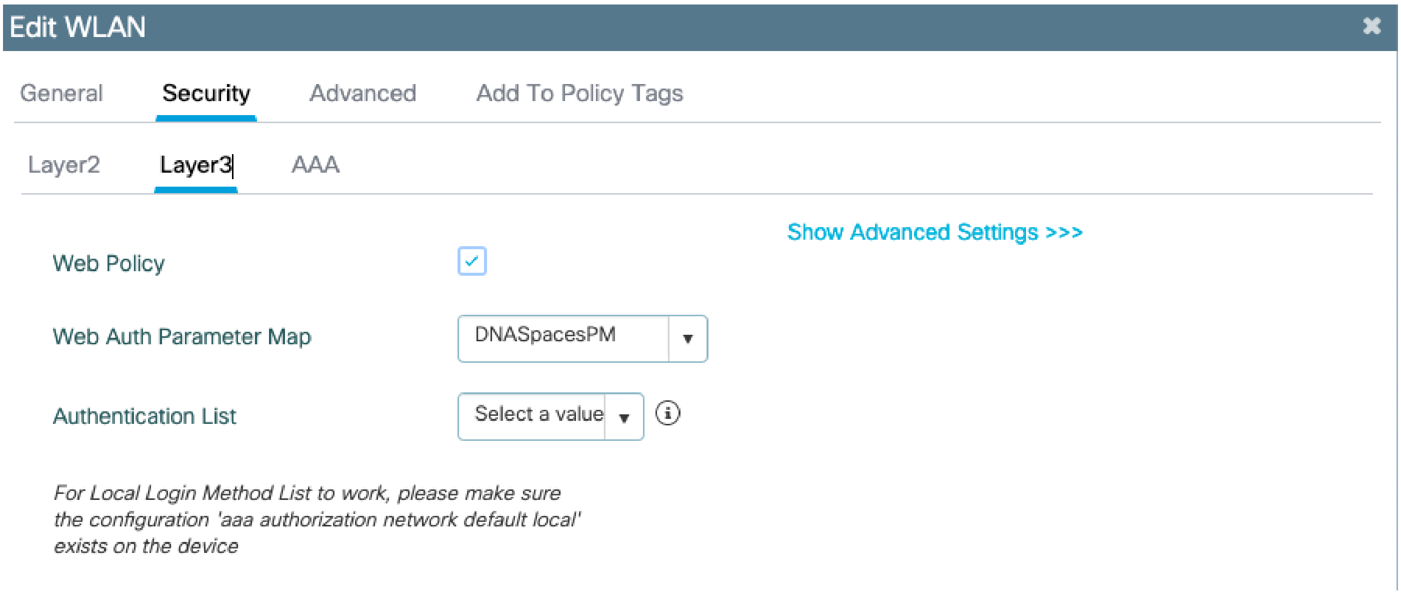
Transition Mode WLAN ID 0

Fast Transition Adaptive Enabled

Over the DS □

Reassociation Timeout 20

Step 3. Navigate to **Security** > **Layer3**. Enable Web Policy, and configure the web auth parameter map. Click **Apply to Device**.



Web Policy ☑

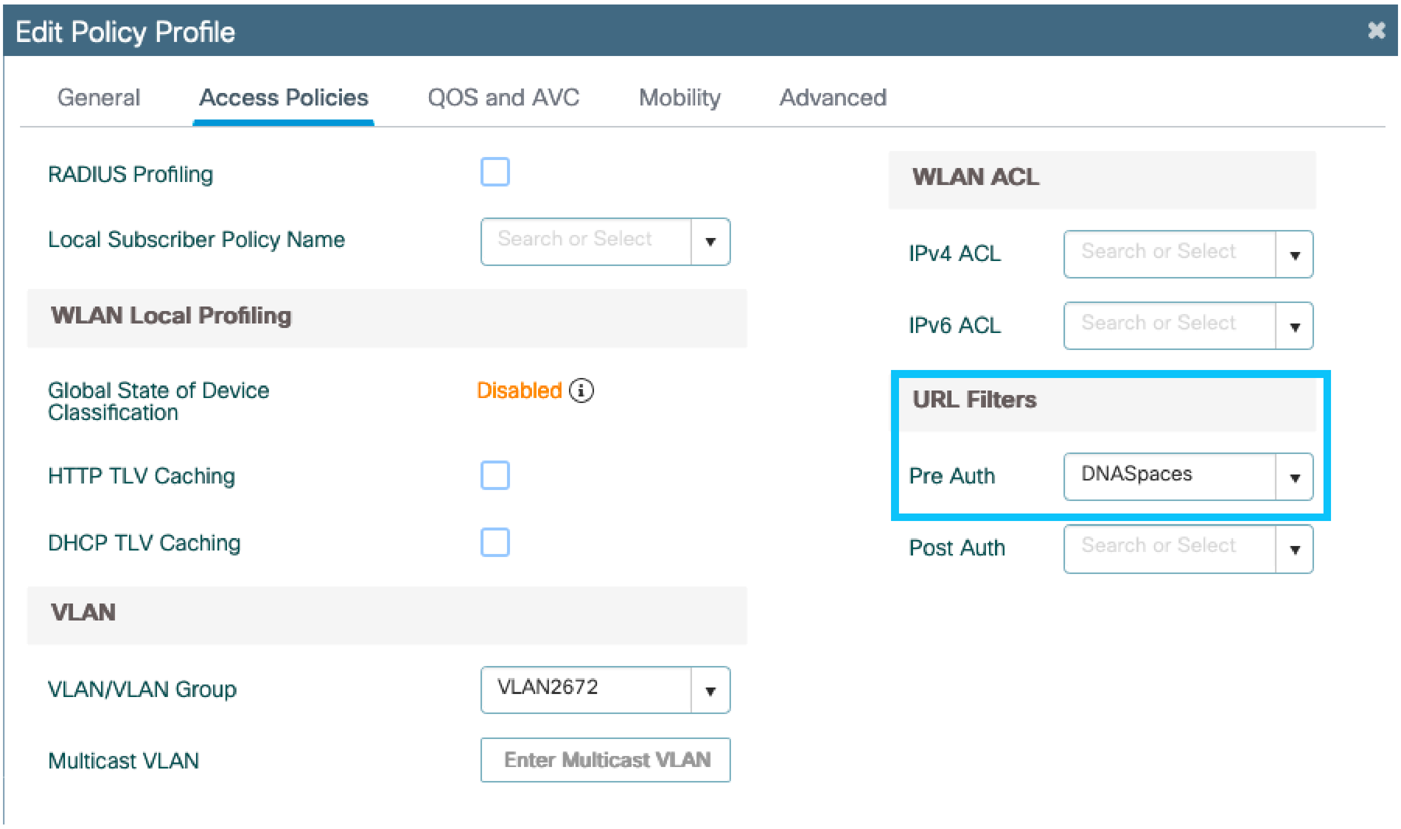
Web Auth Parameter Map: DNASpacesPM

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

Configure Policy Profile on the 9800 Controller

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **Policy** and create a new Policy Profile or use the default Policy Profile. In the access Policies tab, configure the client VLAN and add the URL filter.



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

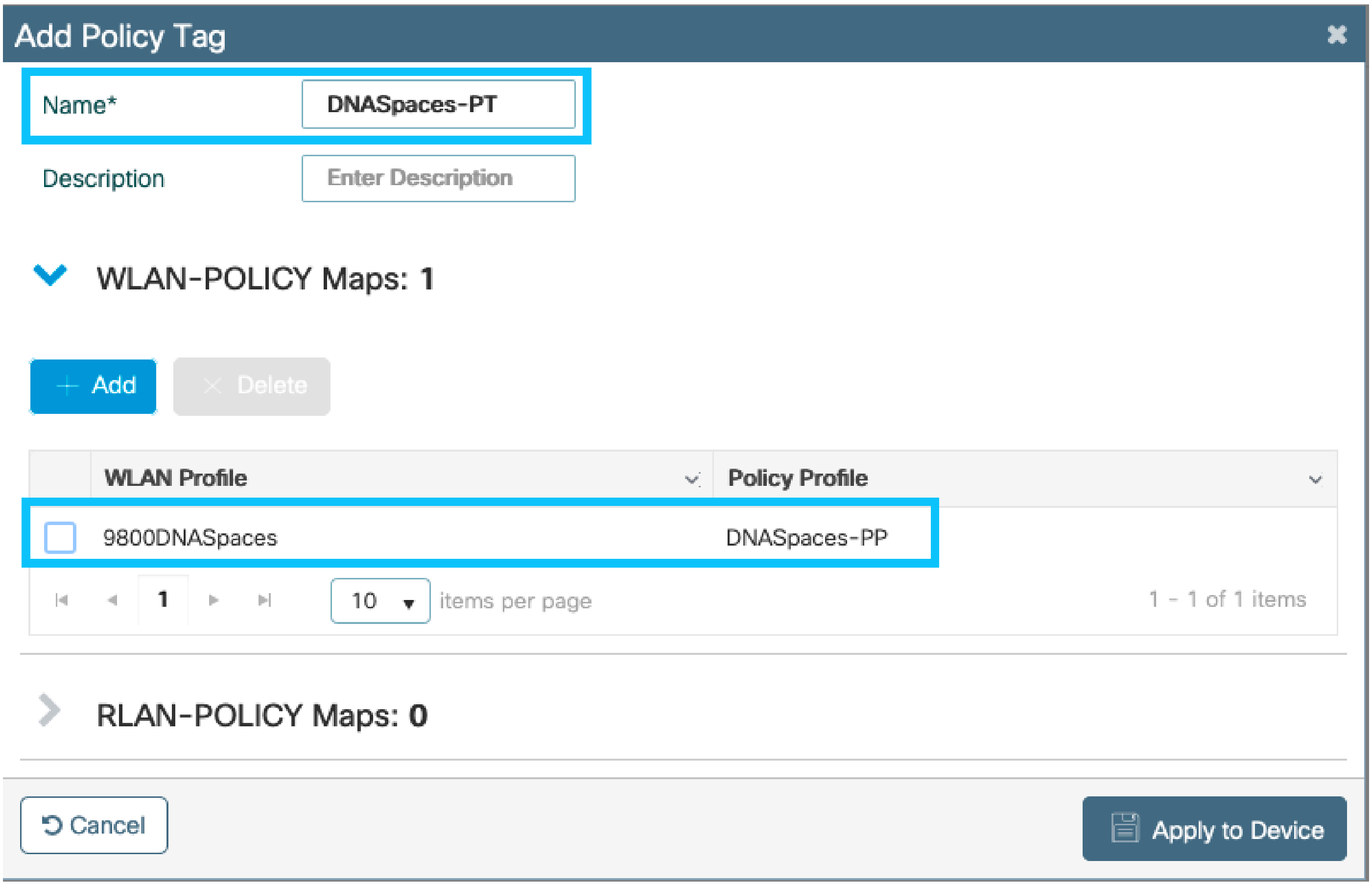
URL Filters

Pre Auth: DNASpaces

Post Auth: Search or Select

Configure Policy Tag on the 9800 Controller

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **Policy**. Create a new Policy Tag or use the default policy tag. Map the WLAN to the Policy Profile in the Policy Tag.

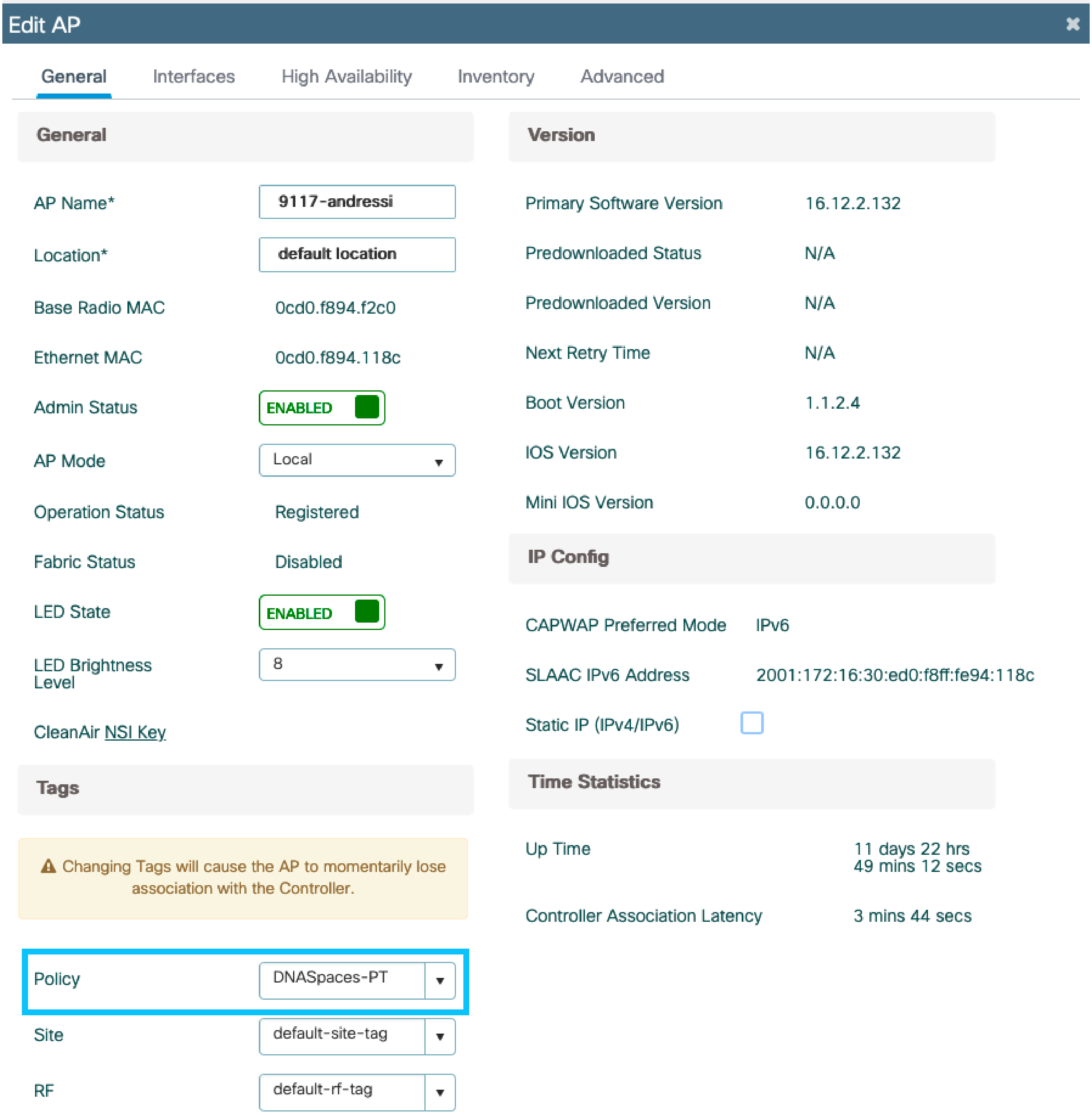


Name*: DNASpaces-PT

WLAN Profile	Policy Profile
9800DNASpaces	DNASpaces-PP

10 items per page

Step 2. Apply the Policy Tag to the AP to broadcast the SSID. Navigate to **Configuration** > **Wireless** > **Access Points**. Select the AP in question and add the Policy Tag. This causes the AP to restart its CAPWAP tunnel and join back to the 9800 controller:



Edit AP

General | Interfaces | High Availability | Inventory | Advanced

General

AP Name*	9117-andressi
Location*	default location
Base Radio MAC	0cd0.f894.f2c0
Ethernet MAC	0cd0.f894.118c
Admin Status	ENABLED
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled
LED State	ENABLED
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)	□

Time Statistics

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

CLI Configuration:

<#root>

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

`wlan <Profile name> <WLAN ID> <SSID Name>`

```
Andressi-9800L(config-wlan)#
```

`no security wpa`

```
Andressi-9800L(config-wlan)#
```

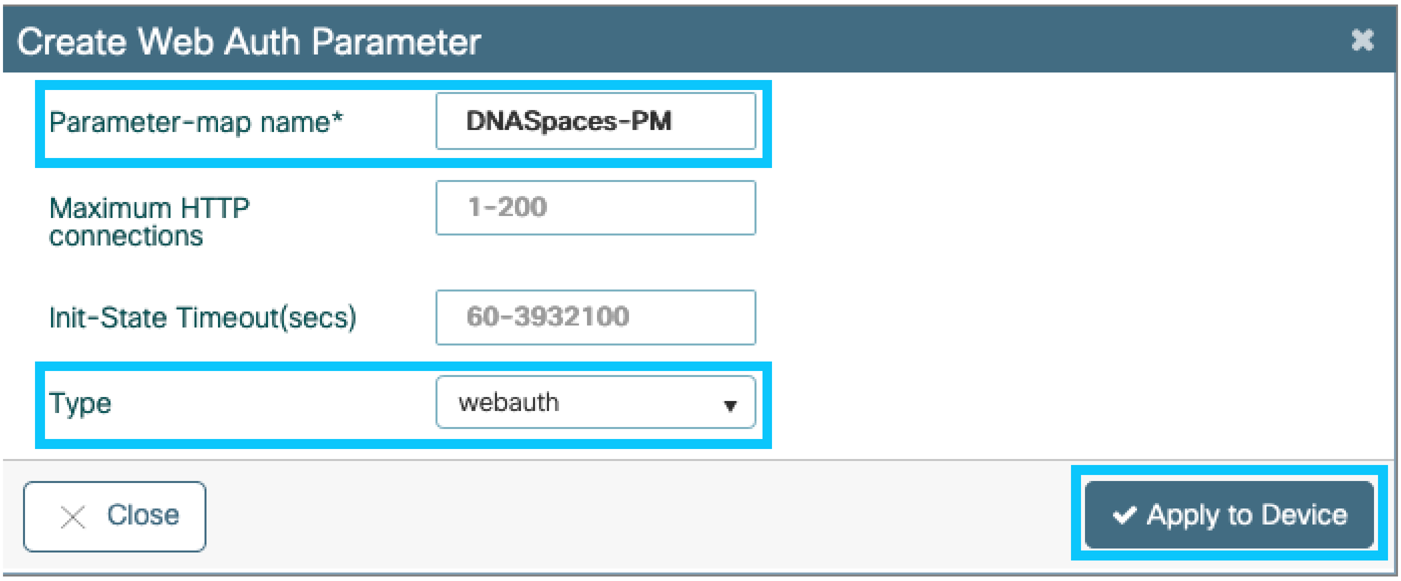
```
no security wpa akm dot1x

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 <map name>

Andressi-9800L(config-wlan)#

no shutdown


Andressi-9800L(config)#

wireless profile policy <policy-profile-name>



Andressi-9800L(config-wireless-policy)#

vlan

 <id>
Andressi-9800L(config-wireless-policy)#

urlfilter list pre-auth-filter <url-filter name>

Andressi-9800L(config-wireless-policy)#

no shutdown


Andressi-9800L(config)#

wireless tag policy <policy-tag-name>

Andressi-9800L(config-policy-tag)#

wlan <Profile name> policy <policy-profile-name>
```

Captive Portal with RADIUS Server on Spaces

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

Web Auth Parameter Map Configuration on the 9800 Controller

Step 1. Create a web auth parameter map. Navigate to **Configuration** > **Security** > **Web Auth**. Click **+Add**, and configure the parameter map name, and select **webauth** as the type:



Create Web Auth Parameter

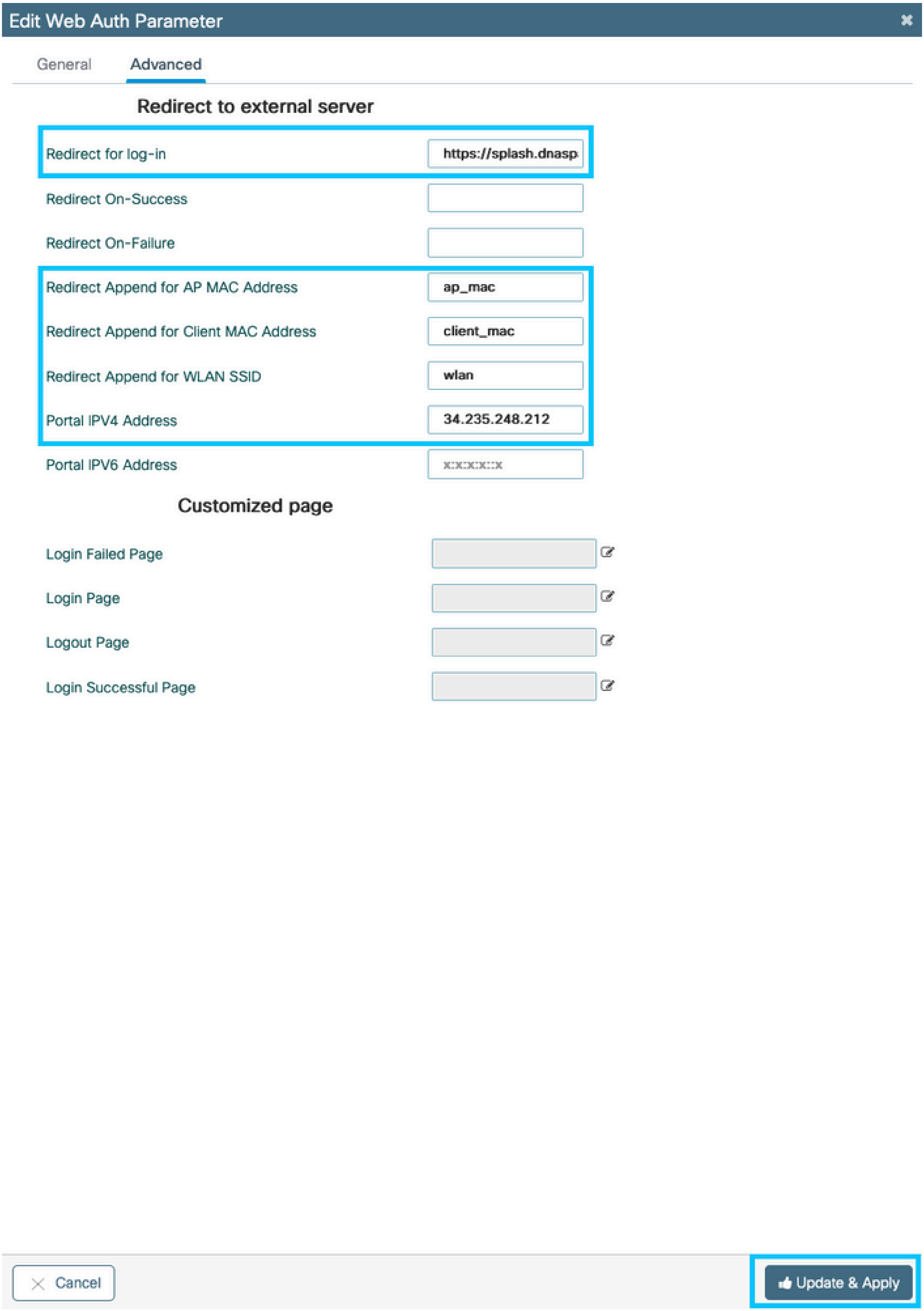
Parameter-map name* DNASpaces-PM

Maximum HTTP connections 1-200

Init-State Timeout(secs) 60-3932100

Type webauth

Step 2. Click the parameter map configured in step 1. Click **Advanced** and enter the Redirect for log-in, Append for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID and portal IPv4 Address. Click **Update & Apply**:



Edit Web Auth Parameter

Redirect to external server

Redirect for log-in	https://splash.dnasp
Redirect On-Success	
Redirect On-Failure	
Redirect Append for AP MAC Address	ap_mac
Redirect Append for Client MAC Address	client_mac
Redirect Append for WLAN SSID	wlan
Portal IPV4 Address	34.235.248.212
Portal IPV6 Address	x:x:x:x::x

Customized page

Login Failed Page	
Login Page	
Logout Page	
Login Successful Page	

Note: To get the splash page URL and the IPv4 redirect address, click the **Configure Manually** option from the SSID created in step 3 of section **Create the SSID on Spaces** under the **Creating the SSIDs in WLC Direct Connect** section **Creating the Access Control List configuration** section respectively.

Note: Cisco Spaces portal can resolve to two IP addresses, but the 9800 controller allows only one IP address to be configured, one case choose any of those IP addresses to be configured on the parameter map as the Portal IPv4 Address.

Note: Make sure both Virtual IPv4 and IPv6 addresses are configured in the global web auth parameter map. If the Virtual IPv6 is not configured, the clients are sometimes redirected to the internal portal instead of the configured Spaces portal. This is why a Virtual IP must always be configured 192.0.2.1 and can be configured as Virtual IPv4 and FE80:0:0:0:903A::11E4 as Virtual IPV6. There are little to no reasons to use other IPs than those.

CLI Configuration:

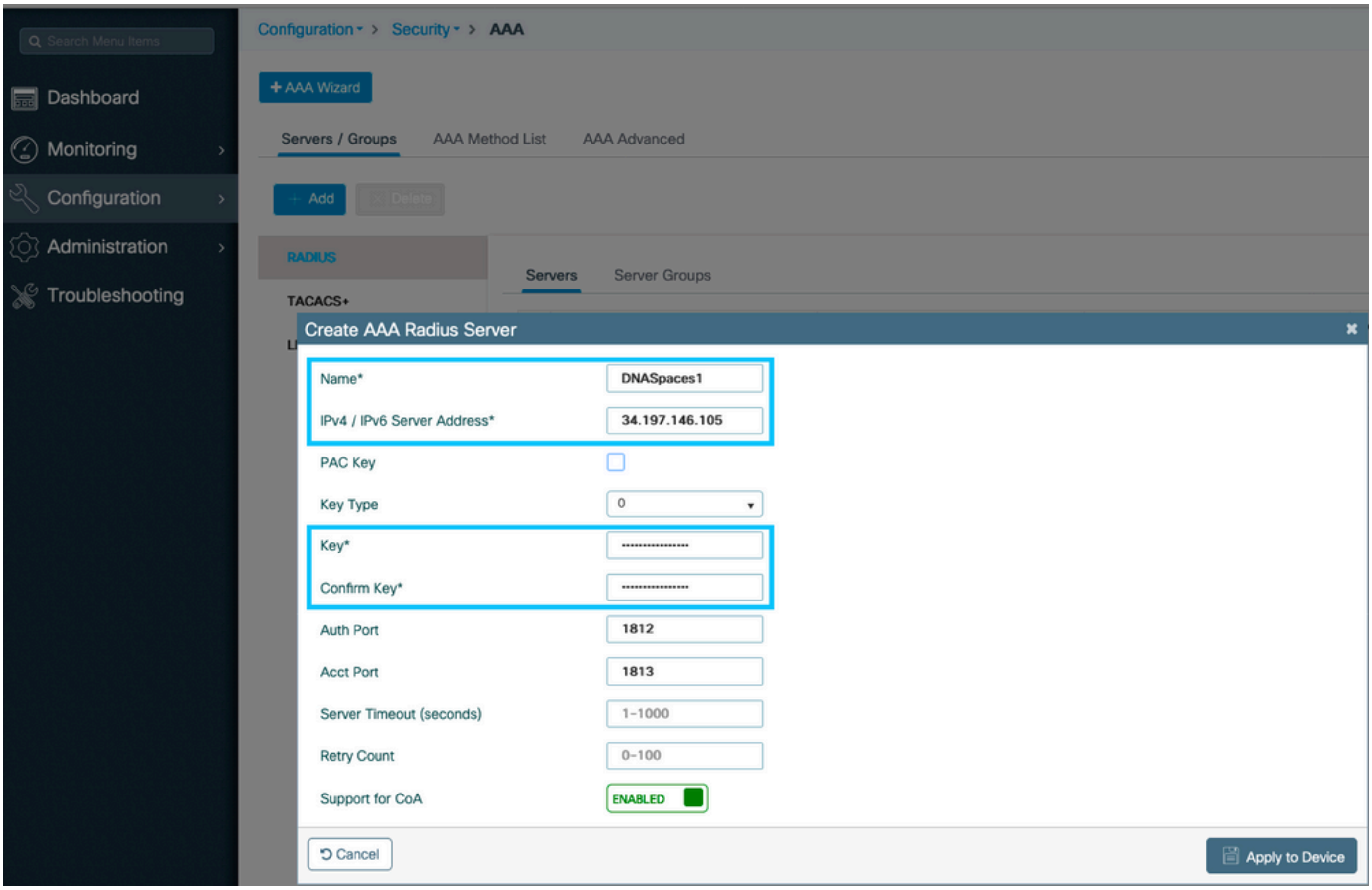
<#root>

```
Andressi-9800L(config)#

parameter-map type webauth <map name>


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 <splashpage URL>

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 <IP Address>

Andressi-9800L(config-params-parameter-map)#

logout-window-disabled

Andressi-9800L(config-params-parameter-map)#

success-window-disabled
```

RADIUS Servers Configuration on the 9800 Controller

Step 1. Configure the RADIUS servers. Cisco Spaces acts as the RADIUS server for user authentication and it can respond to two IP addresses. Navigate to **Configuration** > **Security** > **AAA**. Click **+Add** and configure both RADIUS servers:



Create AAA Radius Server

Name* DNASpaces1

IPv4 / IPv6 Server Address* 34.197.146.105

PAC Key □

Key Type 0

Key* ••••••••••••••••

Confirm Key* ••••••••••••••••

Auth Port 1812

Acct Port 1813

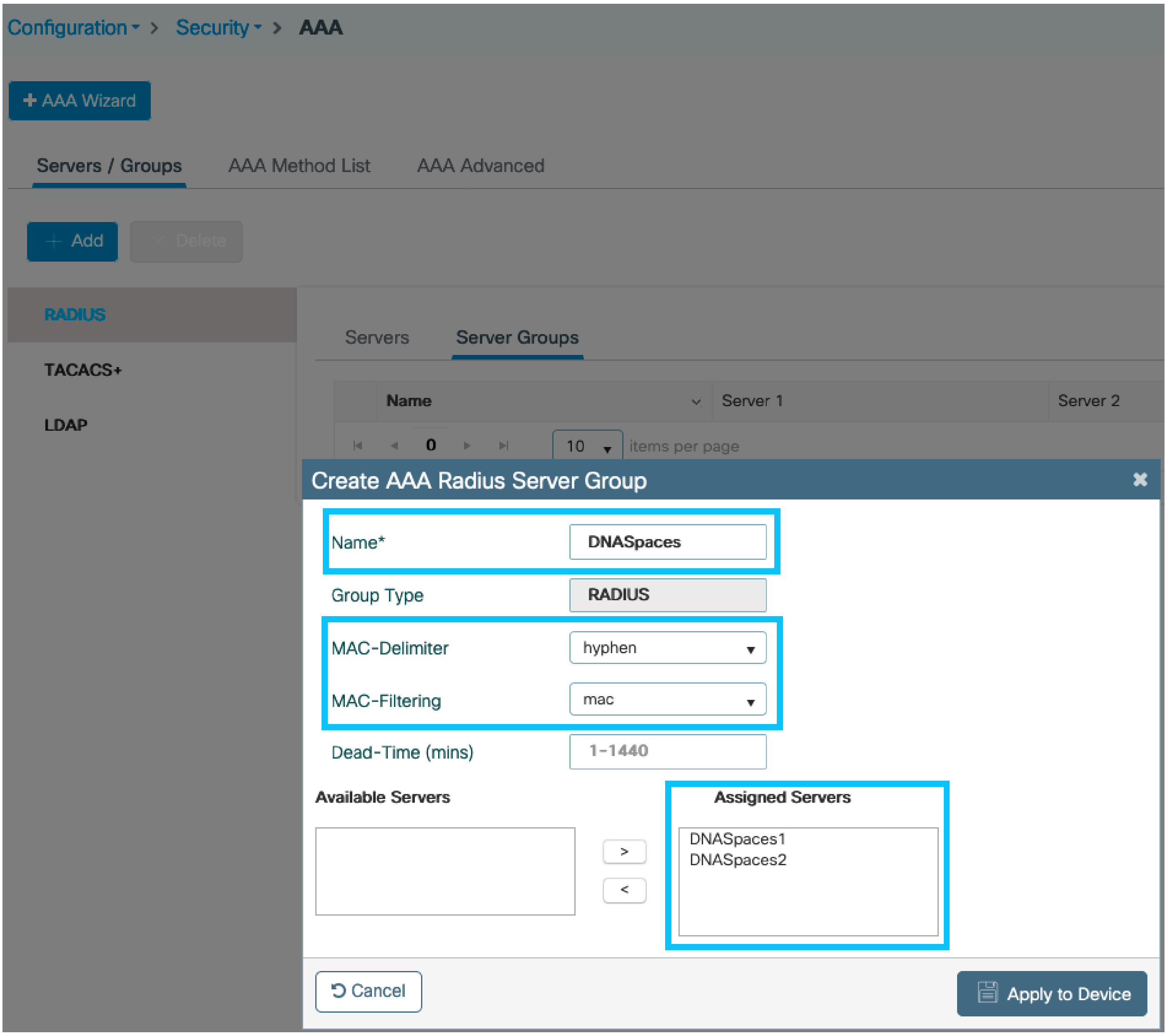
Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ENABLED

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

Step 2. Configure the RADIUS Server Group and add both RADIUS servers. Navigate to **Configuration** > **Security** > **AAA** > **Servers / Groups** > **RADIUS** > **Server Groups**, click **+add**, configure the Server Group name, MAC-Delimiter as **Hyphen**, MAC-Filtering as **MAC**, and assign the two RADIUS servers:



Name*: DNASpaces

Group Type: RADIUS

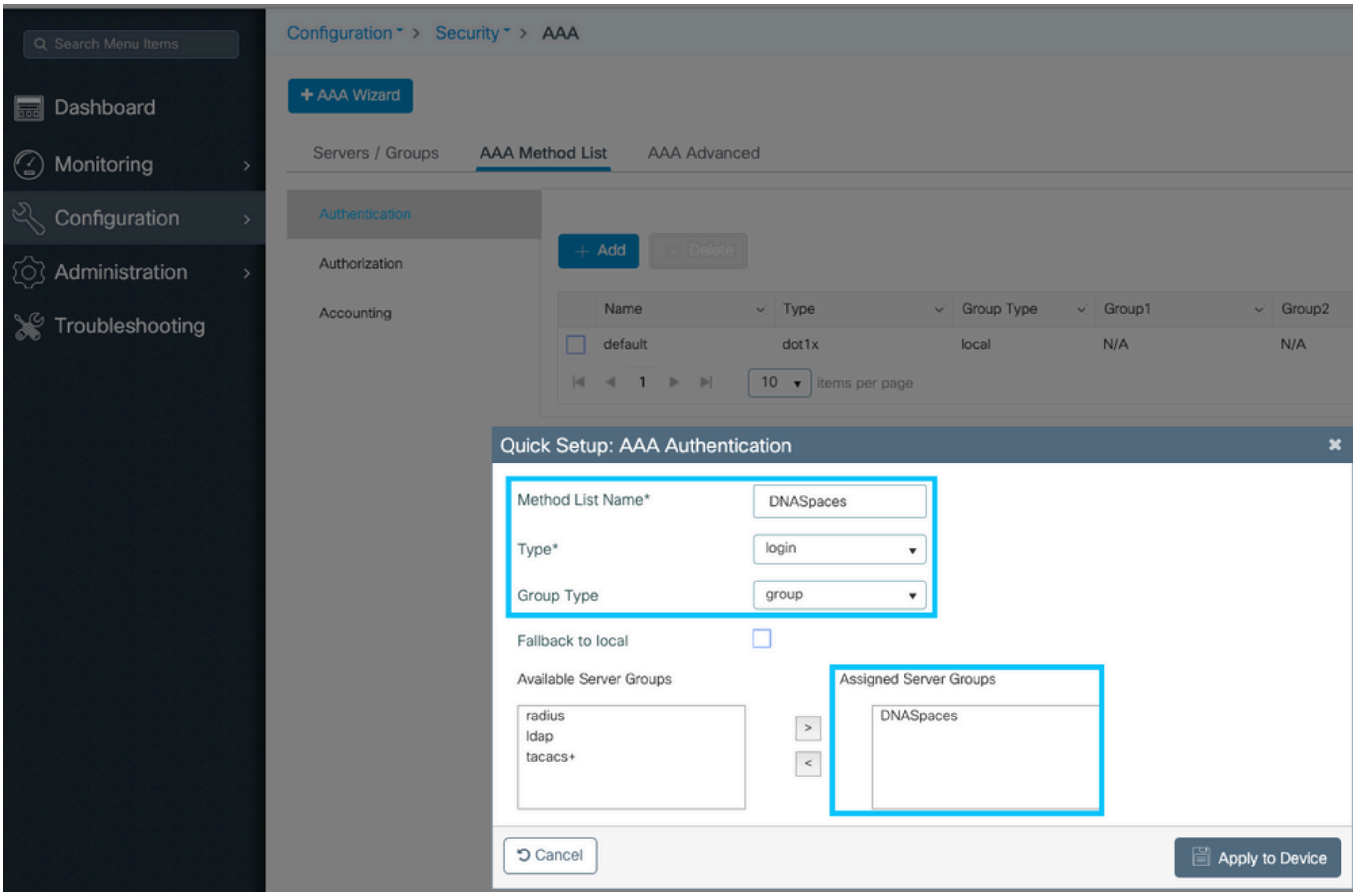
MAC-Delimiter: hyphen

MAC-Filtering: mac

Dead-Time (mins): 1-1440

Assigned Servers: DNASpaces1, DNASpaces2

Step 3. Configure an Authentication Method list. Navigate to **Configuration** > **Security** > **AAA** > **AAA Method List** > **Authentication**. Click **+add**. Configure the Method List name, select **login** as the type and assign the Server Group:



	Name	Type	Group Type	Group1	Group2
□	default	dot1x	local	N/A	N/A

Quick Setup: AAA Authentication

Method List Name* DNASpaces

Type* login

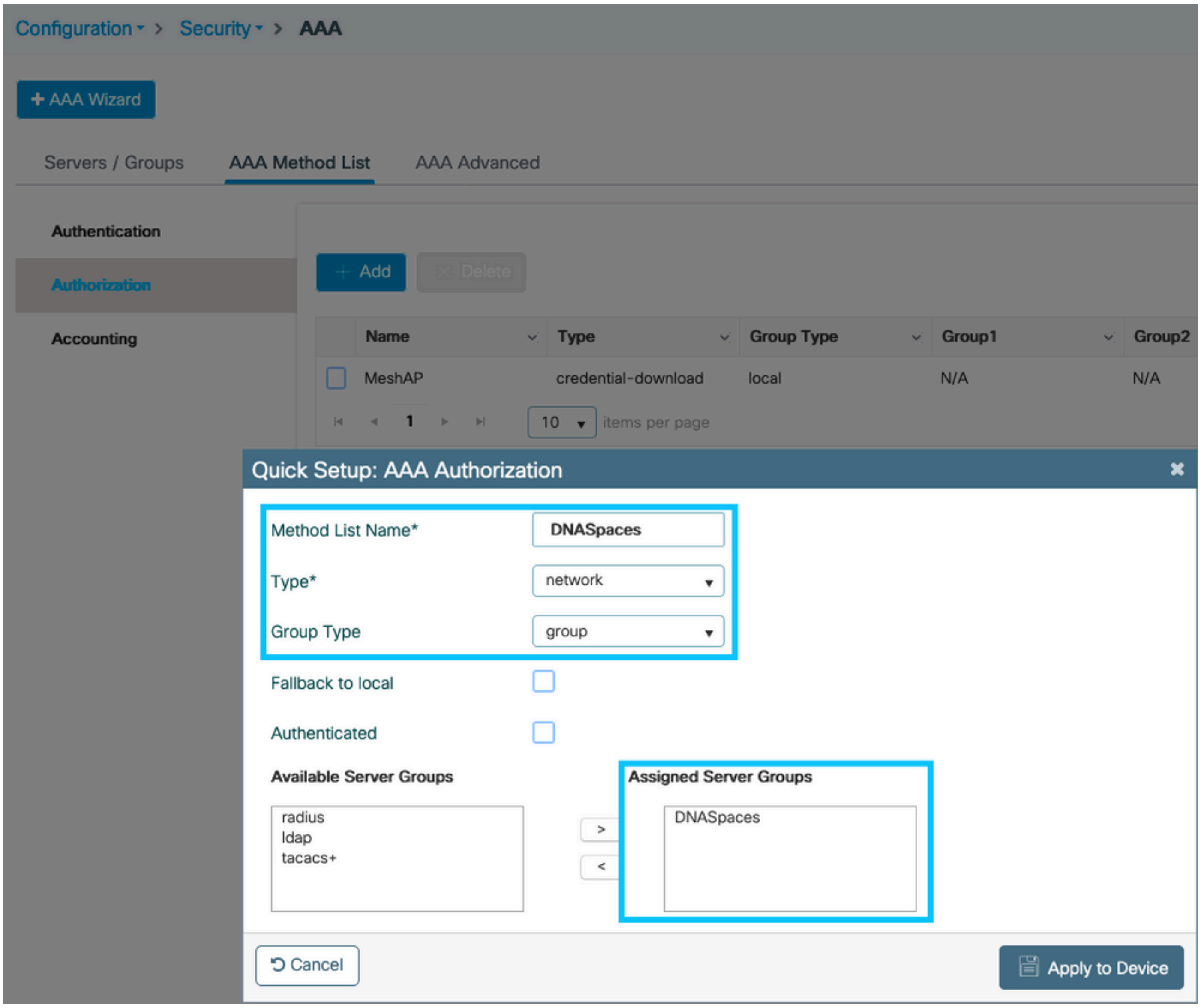
Group Type group

Fallback to local □

Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: DNASpaces

Step 4. Configure an Authorization Method list. Navigate to **Configuration** > **Security** > **AAA** > **AAA Method List** > **Authorization**, click **+add**. Configure the Method List name, select **network** as the type and assign the Server Group:



Name	Type	Group Type	Group1	Group2
MeshAP	credential-download	local	N/A	N/A

Quick Setup: AAA Authorization

Method List Name* DNASpaces

Type* network

Group Type group

Fallback to local □

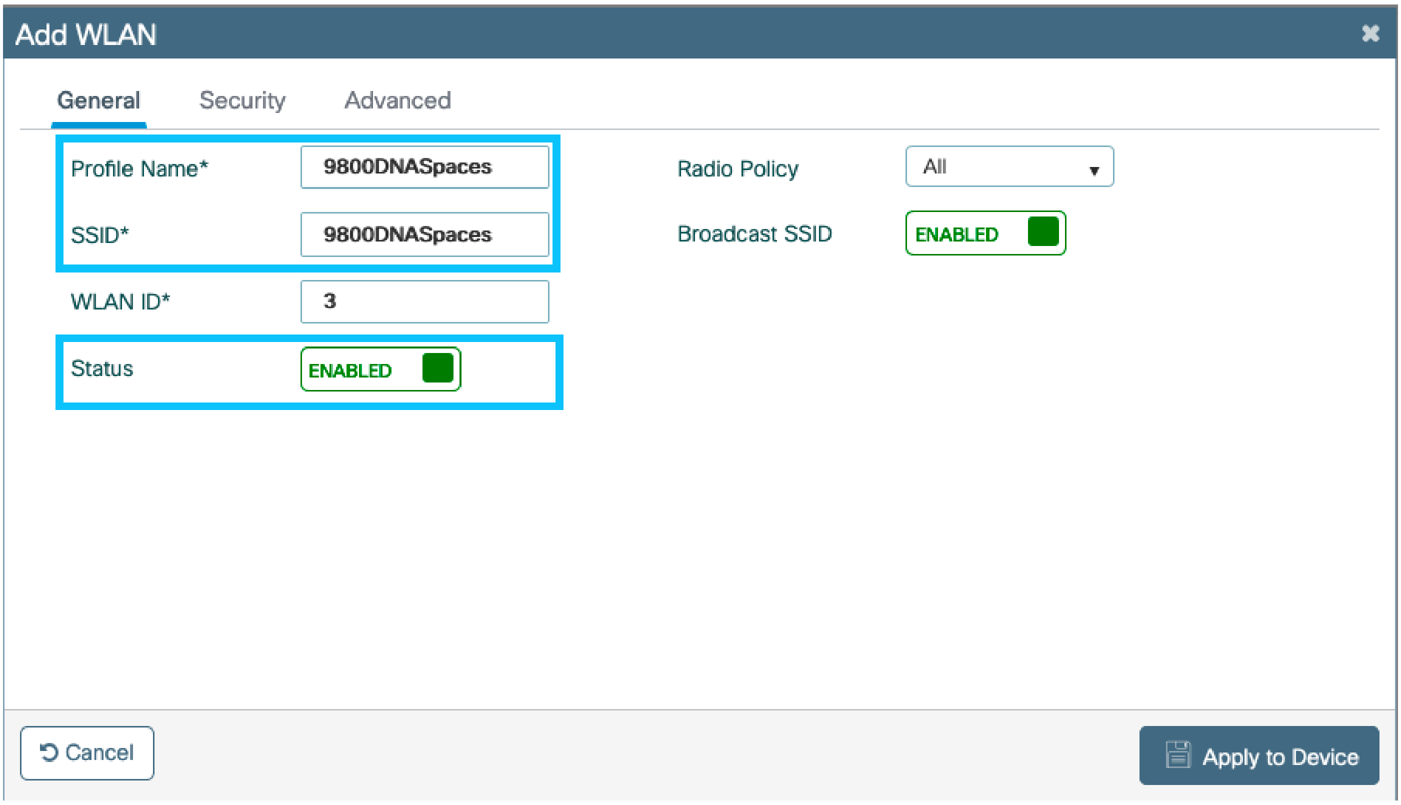
Authenticated □

Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: DNASpaces

Create the SSID on the 9800 Controller

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **WLANs**, click **+Add**. Configure the Profile Name, SSID and enable the WLAN. Make sure the SSID name is the same name as the configured in step 3 of section **Create the SSID on Spaces**.



Profile Name* 9800DNASpaces

SSID* 9800DNASpaces

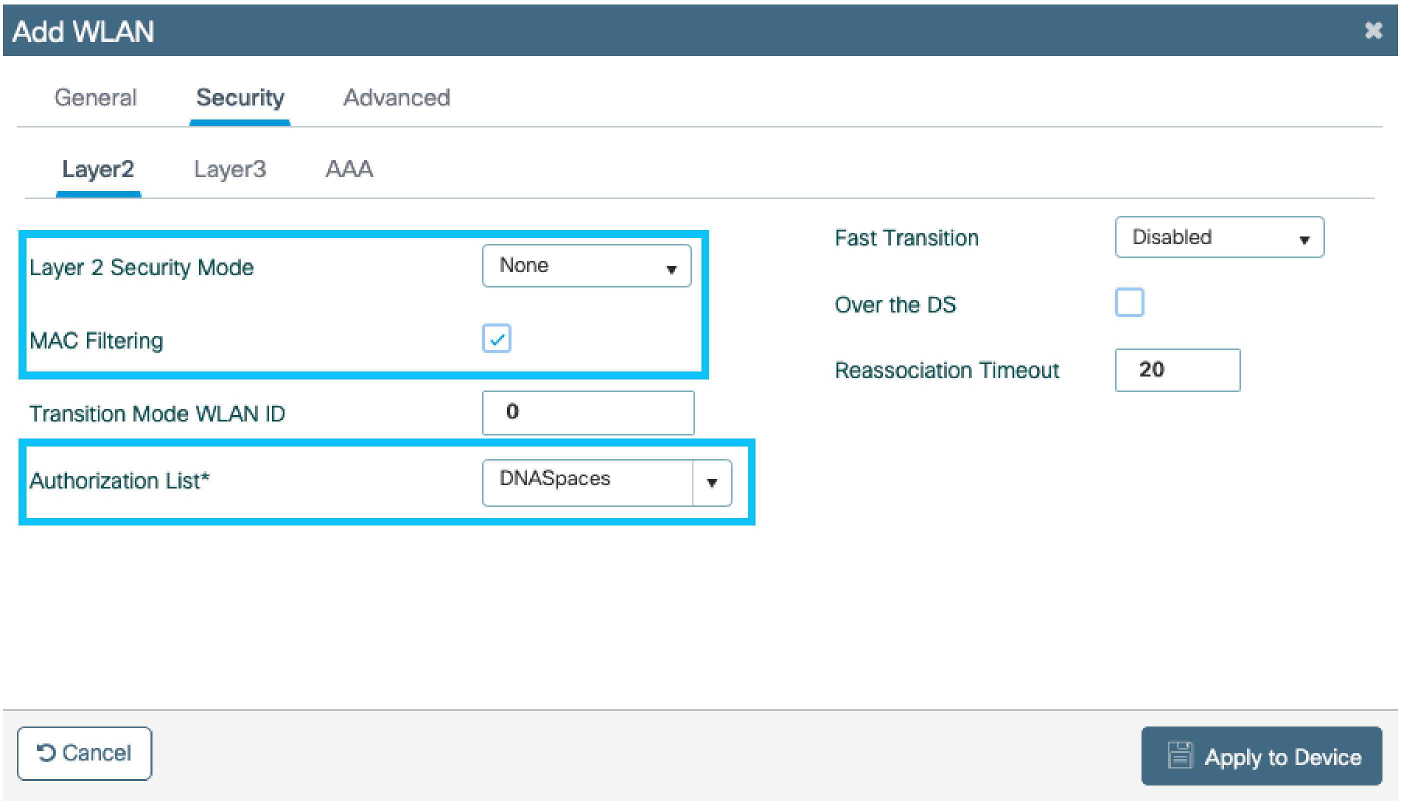
WLAN ID* 3

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED

Step 2. Navigate to **Security** > **Layer2**. Set the Layer 2 Security Mode to **None**, enable **MAC Filtering** and add the **Authorization List**:



Layer 2 Security Mode None

MAC Filtering ☑

Transition Mode WLAN ID 0

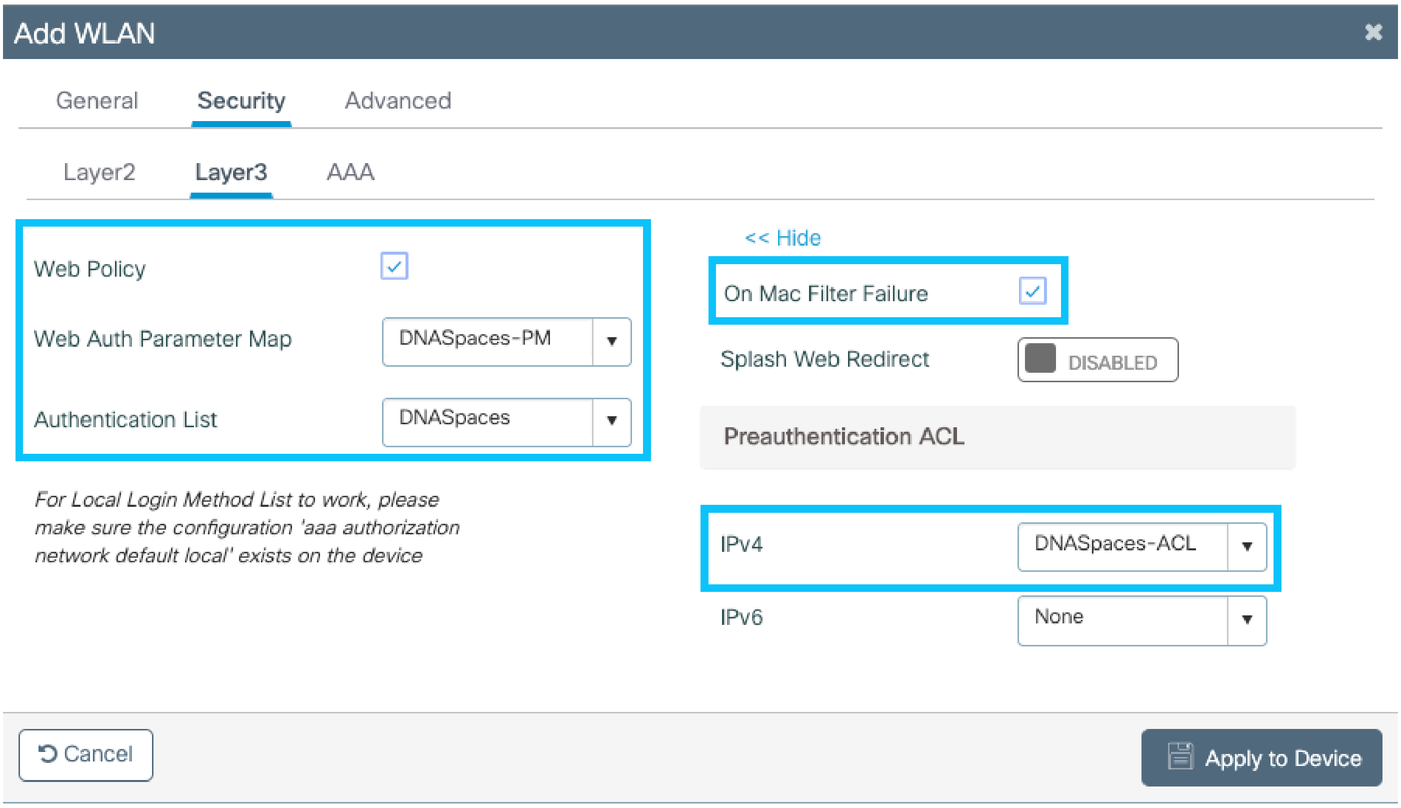
Authorization List* DNASpaces

Fast Transition Disabled

Over the DS □

Reassociation Timeout 20

Step 3. Navigate to **Security** > **Layer3**. Enable **Web Policy**, configure the web auth parameter map and the Authentication List. Enable **On Mac Filter Failure** and add the Preauthentication ACL. Click **Apply to Device**.



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

On Mac Filter Failure ☑

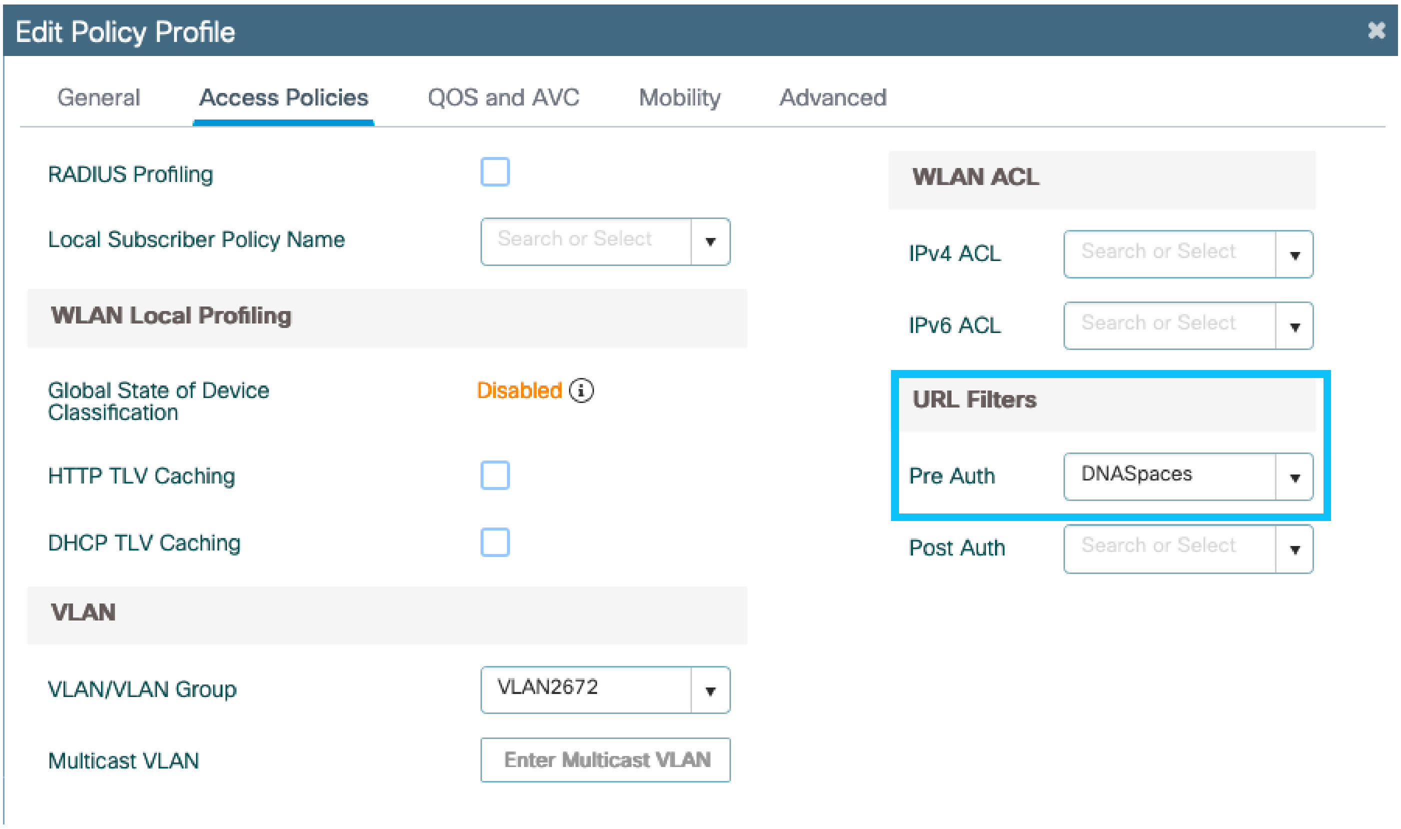
Splash Web Redirect: DISABLED

IPv4: DNASpaces-ACL

IPv6: None

Configure Policy Profile on the 9800 Controller

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **Policy** and create a new Policy Profile or use the default Policy Profile. In the access Policies tab, configure the client VLAN and add the URL filter.



RADIUS Profiling □

Local Subscriber Policy Name: Search or Select

Global State of Device Classification: Disabled ⓘ

HTTP TLV Caching □

DHCP TLV Caching □

VLAN/VLAN Group: VLAN2672

Multicast VLAN: Enter Multicast VLAN

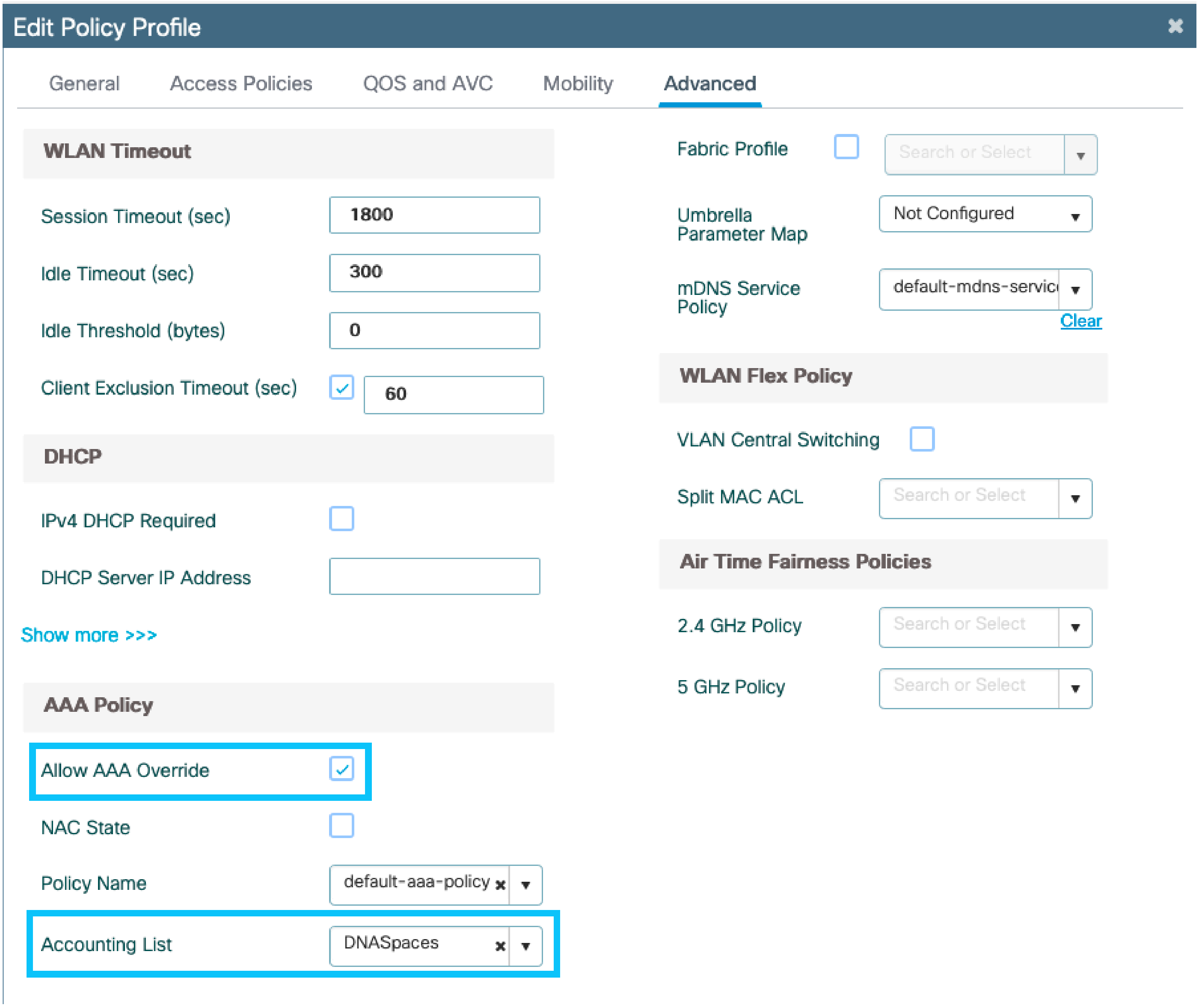
IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

Pre Auth: DNASpaces

Post Auth: Search or Select

Step 2. In the **Advanced tab**, enable **AAA Override** and optionally configure the accounting method list:



Edit Policy Profile

General | Access Policies | QOS and AVC | Mobility | Advanced

WLAN Timeout

Session Timeout (sec): 1800

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 60

DHCP

IPv4 DHCP Required: □

DHCP Server IP Address:

Show more >>>

AAA Policy

Allow AAA Override: ☑

NAC State: □

Policy Name: default-aaa-policy

Accounting List: DNASpaces

Fabric Profile: □ Search or Select

Umbrella Parameter Map: Not Configured

mDNS Service Policy: default-mdns-servic Clear

WLAN Flex Policy

VLAN Central Switching: □

Split MAC ACL: Search or Select

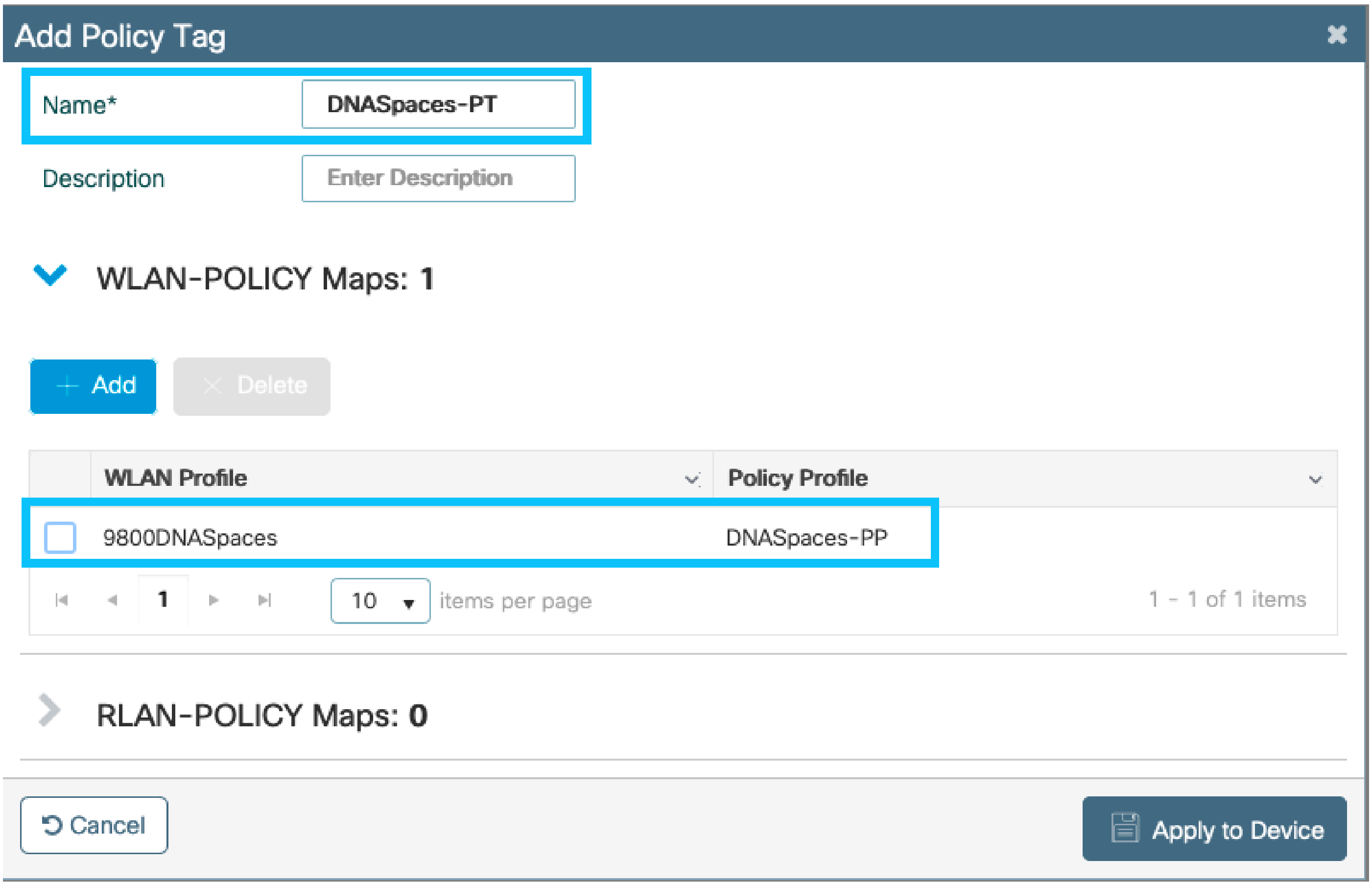
Air Time Fairness Policies

2.4 GHz Policy: Search or Select

5 GHz Policy: Search or Select

Configure Policy Tag on the 9800 Controller

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **Policy**. Create a new Policy Tag or use the default policy tag. Map the WLAN to the Policy Profile in the Policy Tag.



Add Policy Tag

Name*: DNASpaces-PT

Description: Enter Description

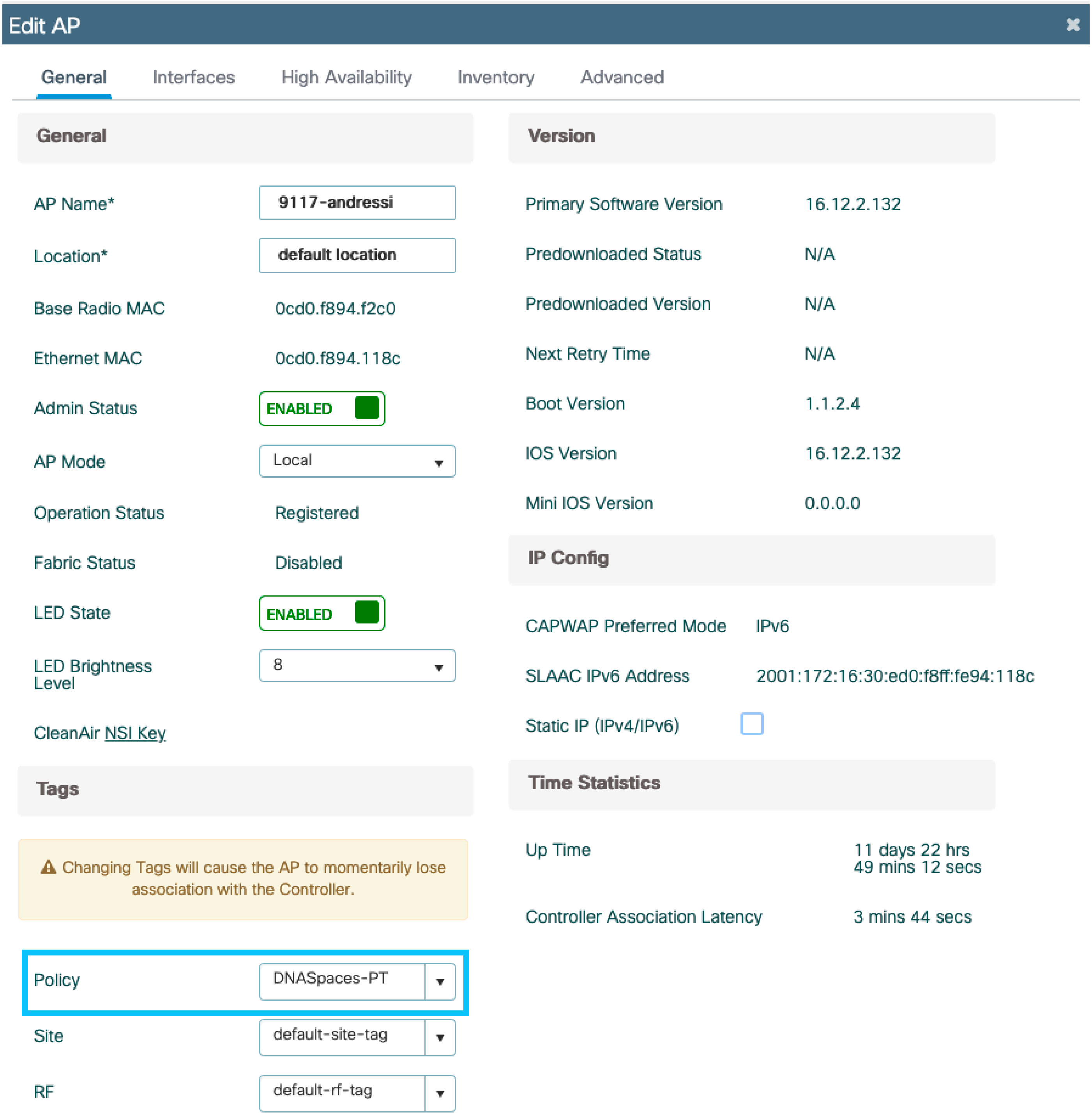
WLAN-POLICY Maps: 1

	WLAN Profile	Policy Profile
□	9800DNASpaces	DNASpaces-PP

1 – 1 of 1 items

RLAN-POLICY Maps: 0

Step 2. Apply the Policy Tag to the AP to broadcast the SSID. Navigate to **Configuration** > **Wireless** > **Access Points**, select the AP in question, and add the Policy Tag. This causes the AP to restart its CAPWAP tunnel and join back to the 9800 controller:



Edit AP

General

AP Name*: 9117-andressi

Location*: default location

Base Radio MAC: 0cd0.f894.f2c0

Ethernet MAC: 0cd0.f894.118c

Admin Status: ENABLED

AP Mode: Local

Operation Status: Registered

Fabric Status: Disabled

LED State: ENABLED

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): □

Time Statistics

Up Time: 11 days 22 hrs 49 mins 12 secs

Controller Association Latency: 3 mins 44 secs

CLI Configuration:

<#root>

```
Andressi-9800L(config)#

wlan <Profile name> <WLAN ID> <SSID Name>

Andressi-9800L(config-wlan)#

ip access-group web <ACL Name>

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 <authz name>


Andressi-9800L(config-wlan)#

security web-auth

Andressi-9800L(config-wlan)#

security web-auth authentication-list <auth name>

Andressi-9800L(config-wlan)#

security web-auth on-macfilter-failure

Andressi-9800L(config-wlan)#

security web-auth parameter-map <map name>

Andressi-9800L(config-wlan)#

no shutdown


Andressi-9800L(config)#

wireless profile policy <policy-profile-name>

Andressi-9800L(config-wireless-policy)#

aaa-override

Andressi-9800L(config-wireless-policy)#

accounting-list <acct name>

Andressi-9800L(config-wireless-policy)#

vlan

 <id>
Andressi-9800L(config-wireless-policy)#

urlfilter list pre-auth-filter <url-filter name>

Andressi-9800L(config-wireless-policy)#

no shutdown


Andressi-9800L(config)#

wireless tag policy <policy-tag-name>

Andressi-9800L(config-policy-tag)#

wlan <Profile name> policy <policy-profile-name>
```

Configure the Global Parameter Map

Unrecommended step : Run these commands to allow HTTPS redirection but note that redirecting in client HTTPS traffic is not needed if client operating system does captive portal detection and causes heavier CPU utilization, and always throws a certificate warning. It is recommended to avoid to configure it unless needed for a very specific use case.

```
<#root>

Andressi-9800L(config)#

parameter-map type webauth global

Andressi-9800L(config-params-parameter-map)#

intercept-https-enable
```

Note: You must have a valid SSL certificate for the virtual IP installed in Cisco Catalyst 9800 Series Wireless Controller.

Step 1. Copy signed certificate file with extension.p12 to a TFTP server and run this command to transfer and install the certificate into the 9800 controller:

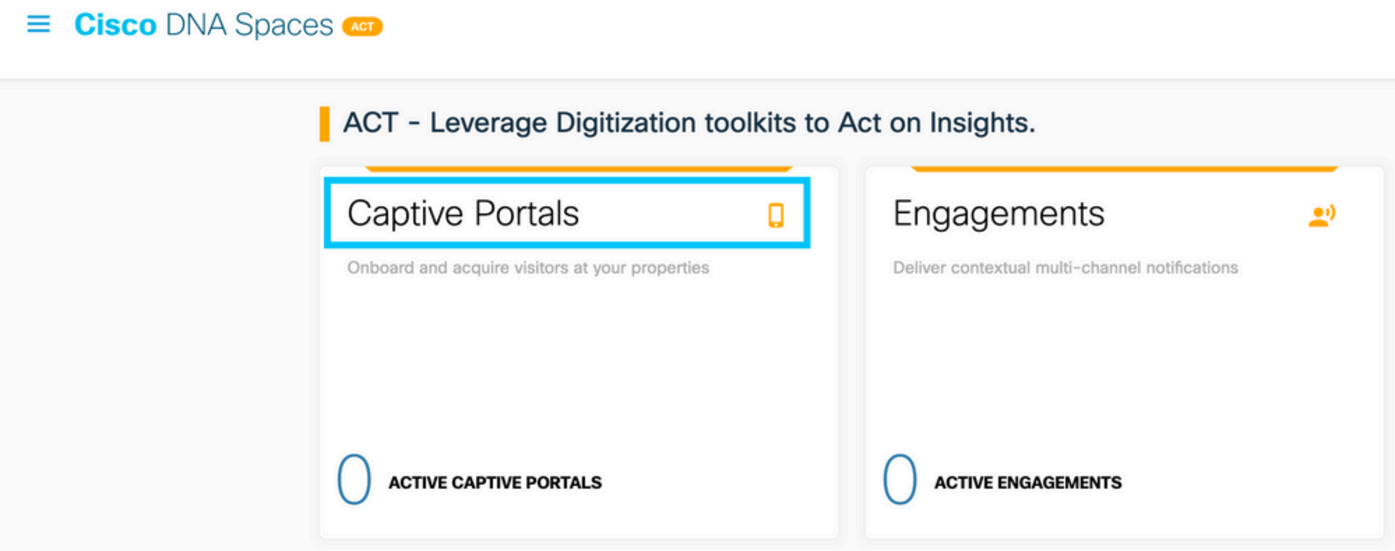
```
<#root>

Andressi-9800L(config)#

crypto pki import <name> pkcs12 tftp://<tftp server ip>:/ password <certificate password>
```

Step 2. To map the installed certificate to the web auth parameter map, run these commands:

```
<#root>

Andressi-9800L(config)#

parameter-map type webauth global


Andressi-9800L(config-params-parameter-map)#

trustpoint <installed trustpool name>
```

Create the Portal on Spaces

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



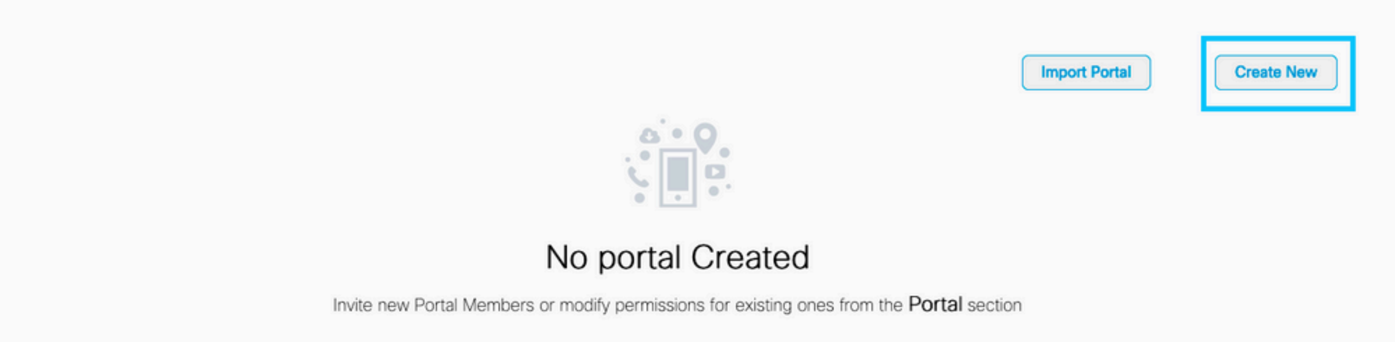
Onboard and acquire visitors at your properties

0 ACTIVE CAPTIVE PORTALS

Deliver contextual multi-channel notifications

0 ACTIVE ENGAGEMENTS

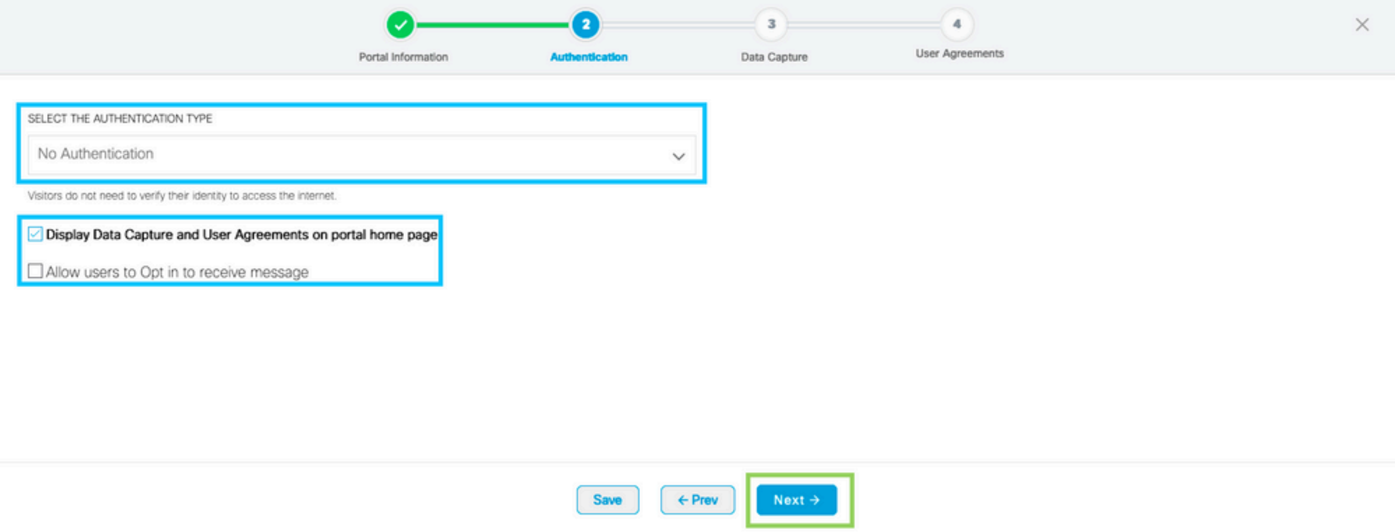
Step 2. Click **Create New**, enter the portal name, and select the locations that can use the portal:



No portal Created

Invite new Portal Members or modify permissions for existing ones from the Portal section

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

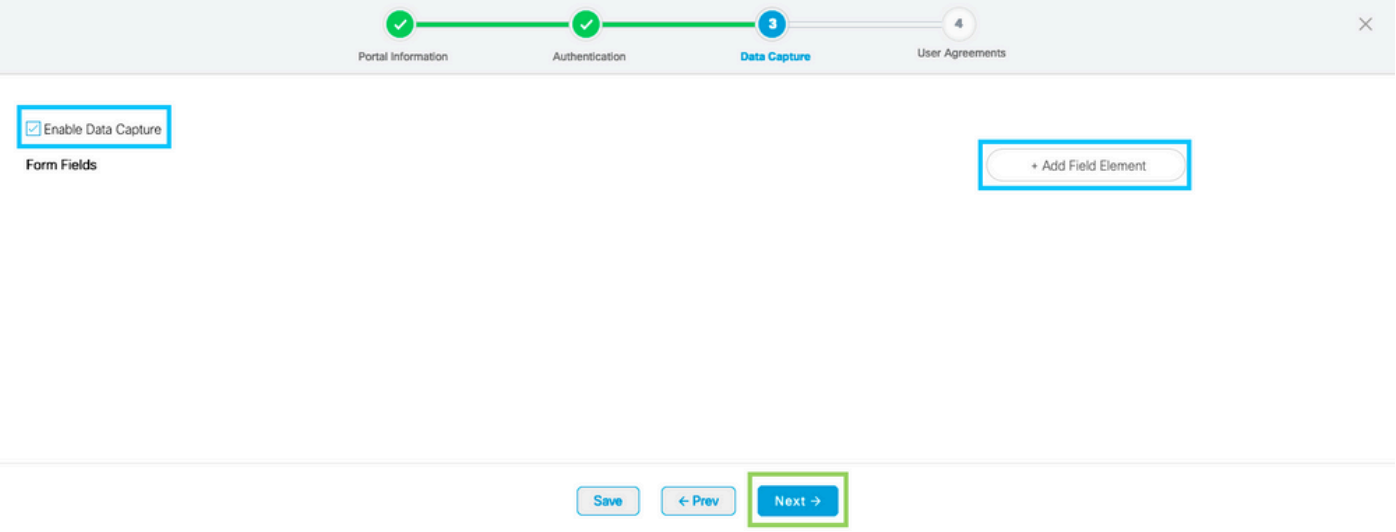
No Authentication

Visitors do not need to verify their identity to access the internet.

☑ Display Data Capture and User Agreements on portal home page

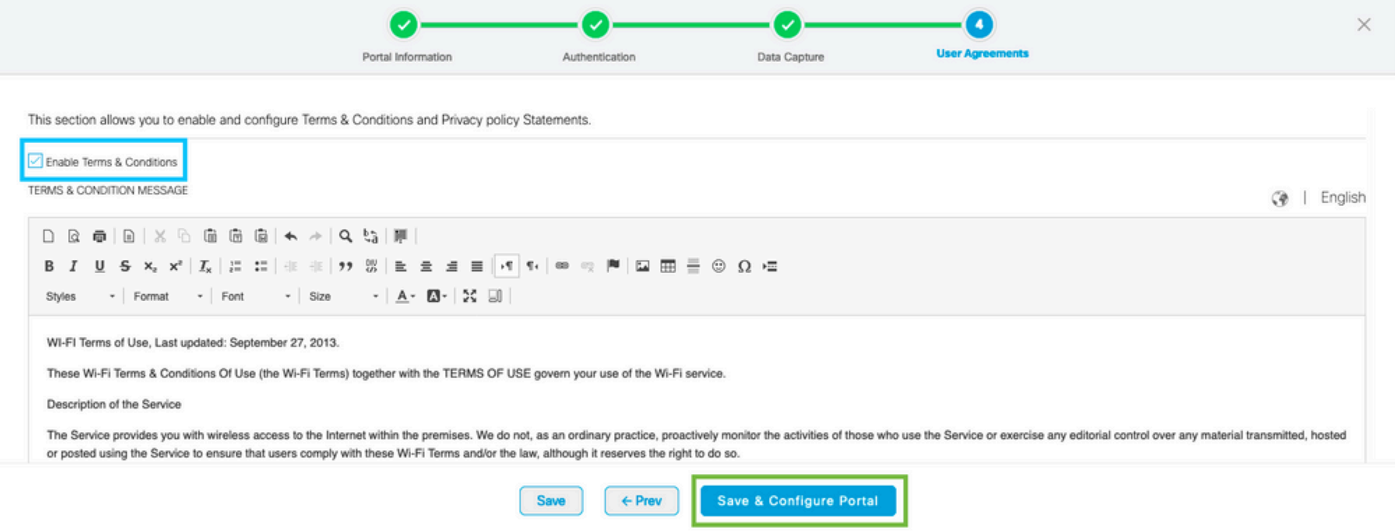
□ Allow users to Opt in to receive message

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



☑ Enable Data Capture

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

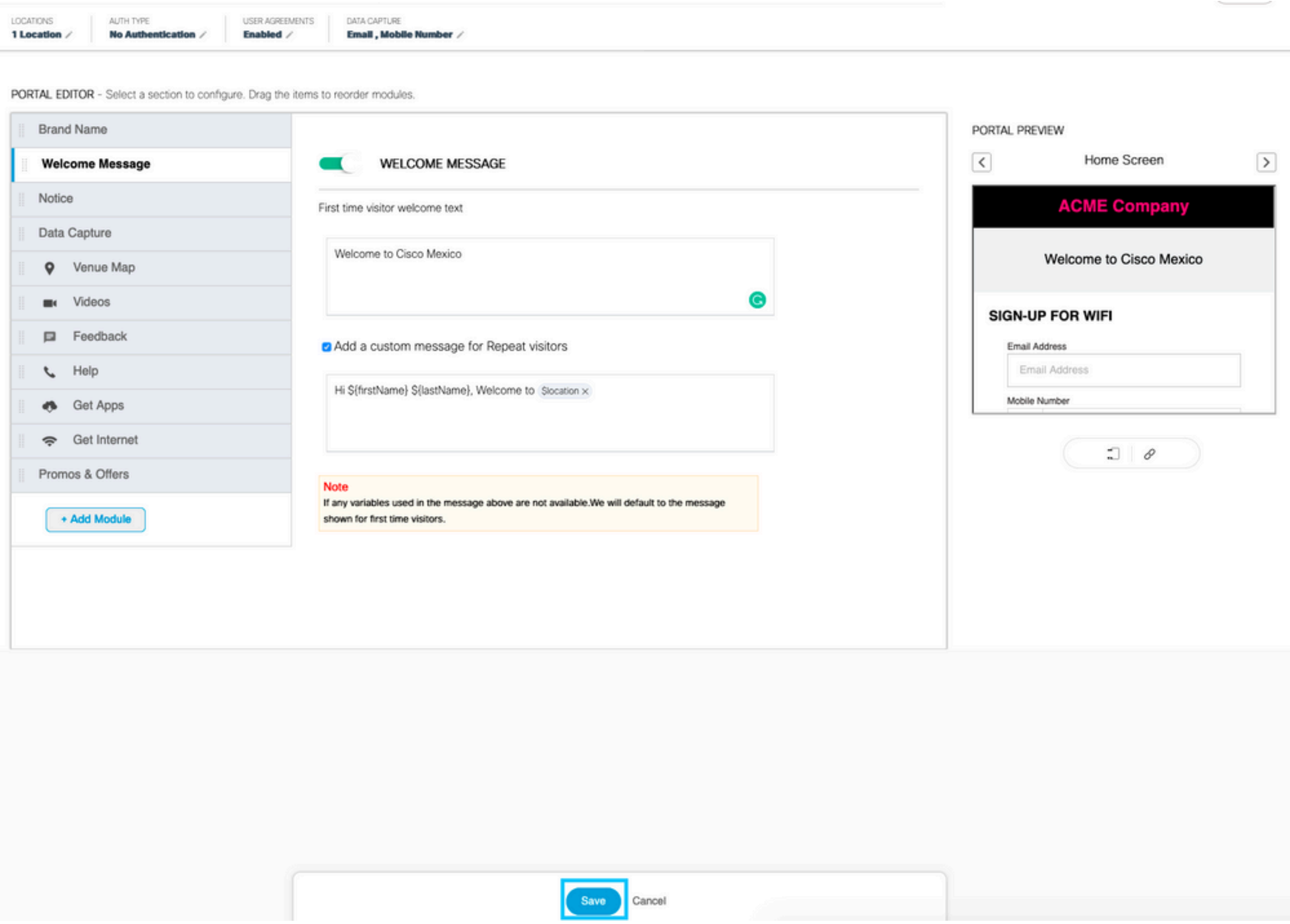
WI-FI Terms of Use, Last updated: September 27, 2013.

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.

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



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.

WELCOME MESSAGE

First time visitor welcome text: Welcome to Cisco Mexico

☑ Add a custom message for Repeat visitors

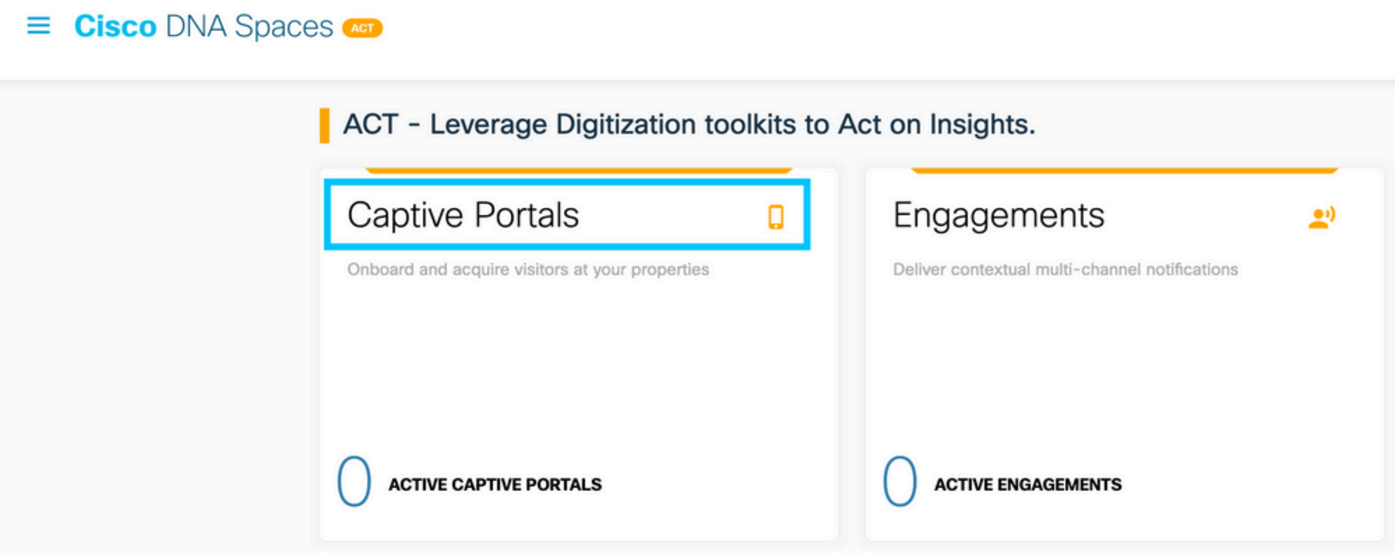
Hi ${firstName} ${lastName}, Welcome to $location

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

Configure the Captive Portal Rules on Spaces

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

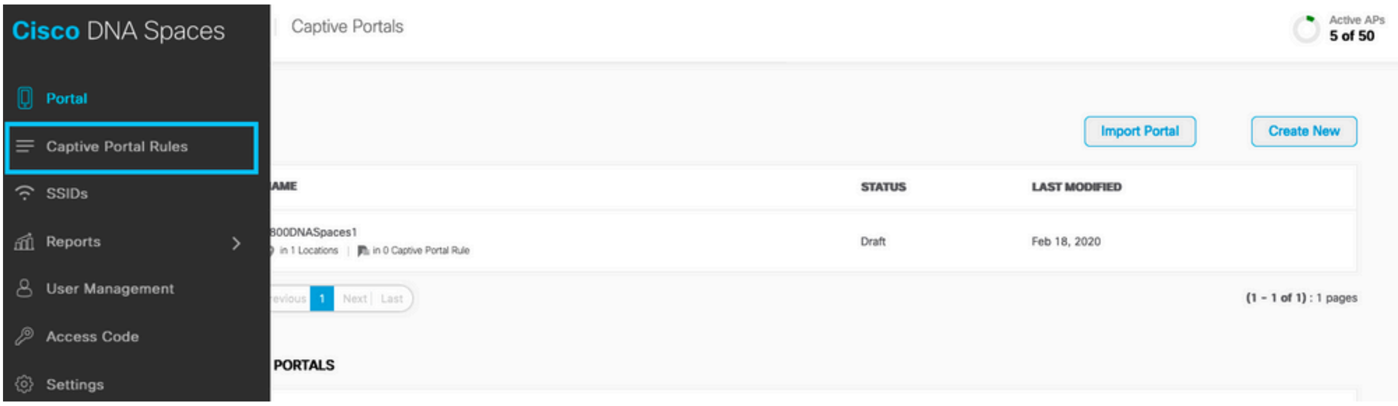


ACT - Leverage Digitization toolkits to Act on Insights.

Captive Portals: Onboard and acquire visitors at your properties

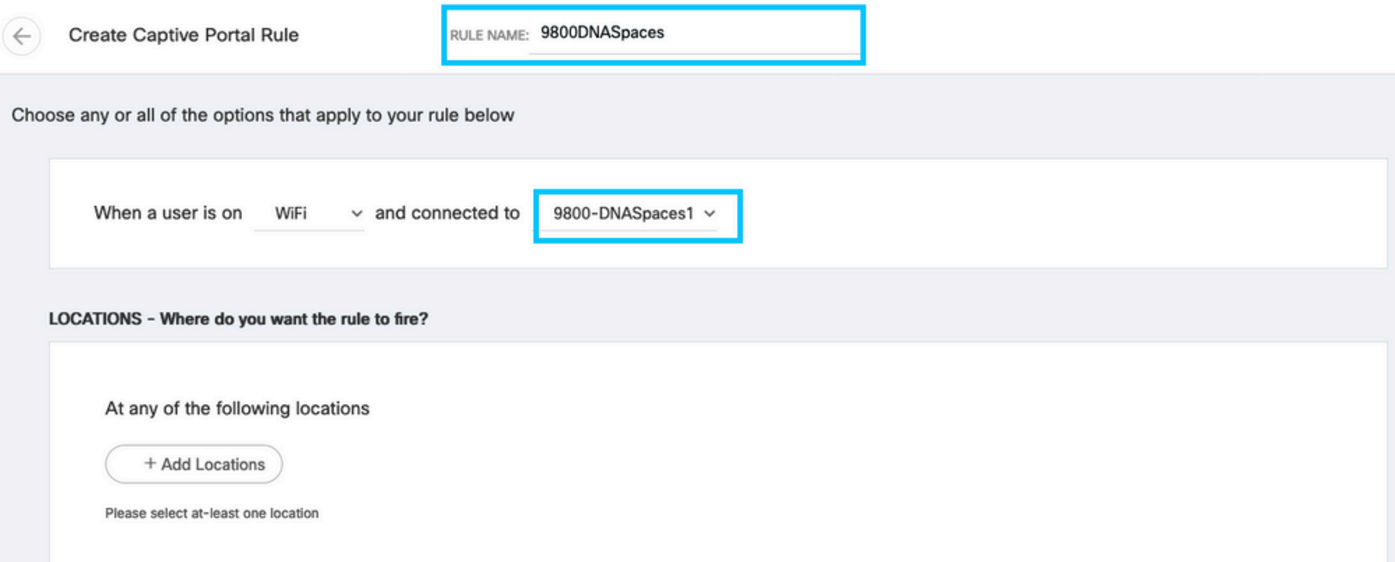
Engagements: Deliver contextual multi-channel notifications

Step 2. Open the captive portal menu and click **Captive Portal Rules:**



AME	STATUS	LAST MODIFIED
800DNASpaces1 in 1 Locations | in 0 Captive Portal Rule	Draft	Feb 18, 2020

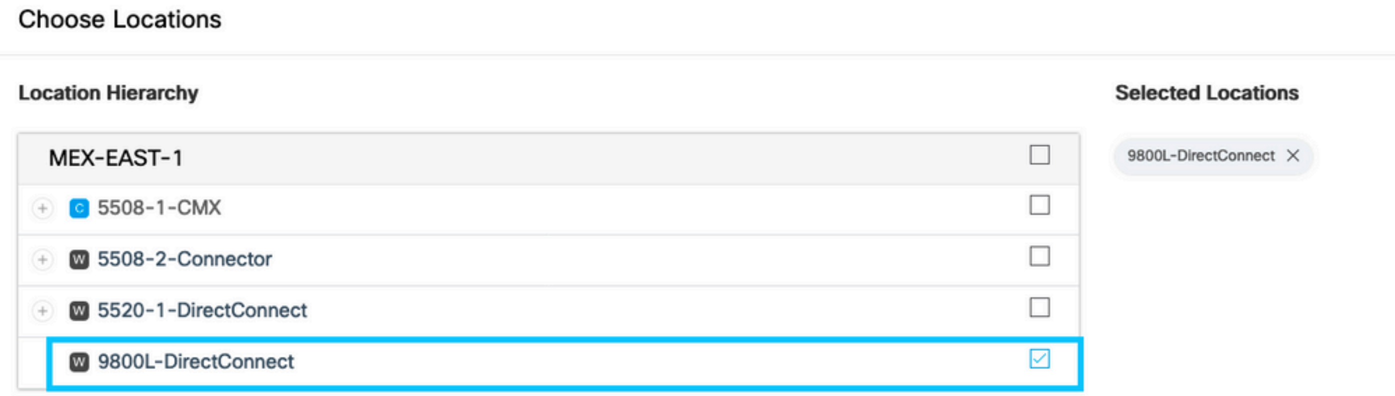
Step 3. Click **+ Create New Rule**. Enter the rule name, and choose the SSID previously configured.


Create Captive Portal Rule
Choose any or all of the options that apply to your rule below
LOCATIONS - Where do you want the rule to fire?
At any of the following locations
+ Add Locations
Please select at-least one location

RULE NAME: 9800DNASpaces

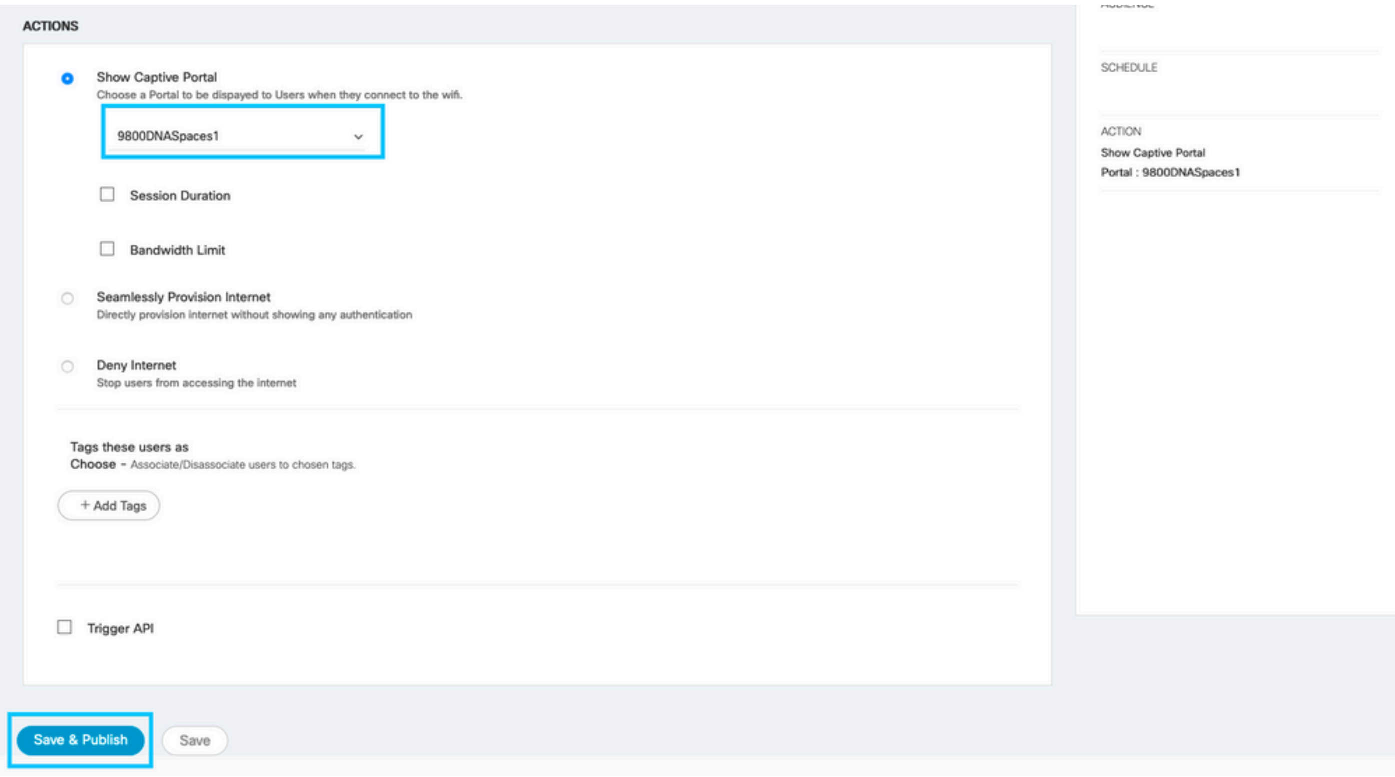
When a user is on WiFi and connected to 9800-DNASpaces1

Step 4. Select the locations in which the portal is available. Click **+ Add Locations** in the **LOCATIONS** section. Choose the desired one from the Location Hierarchy.



MEX-EAST-1 □
5508-1-CMX □
5508-2-Connector □
5520-1-DirectConnect □
9800L-DirectConnect ☑

Step 5. 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 dispayed 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.

□ Trigger API

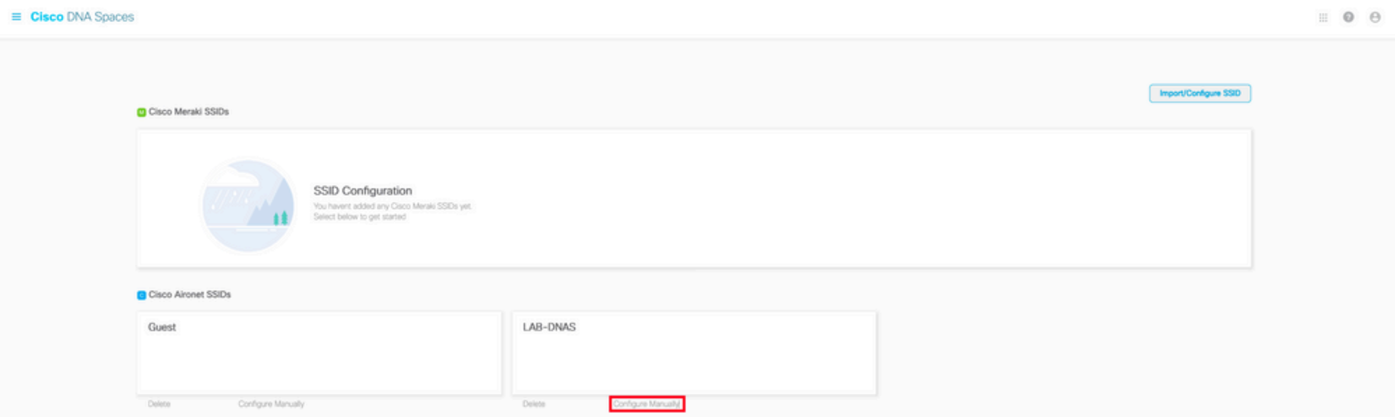
SCHEDULE

ACTION
Show Captive Portal
Portal : 9800DNASpaces1

Get Specific information from Spaces

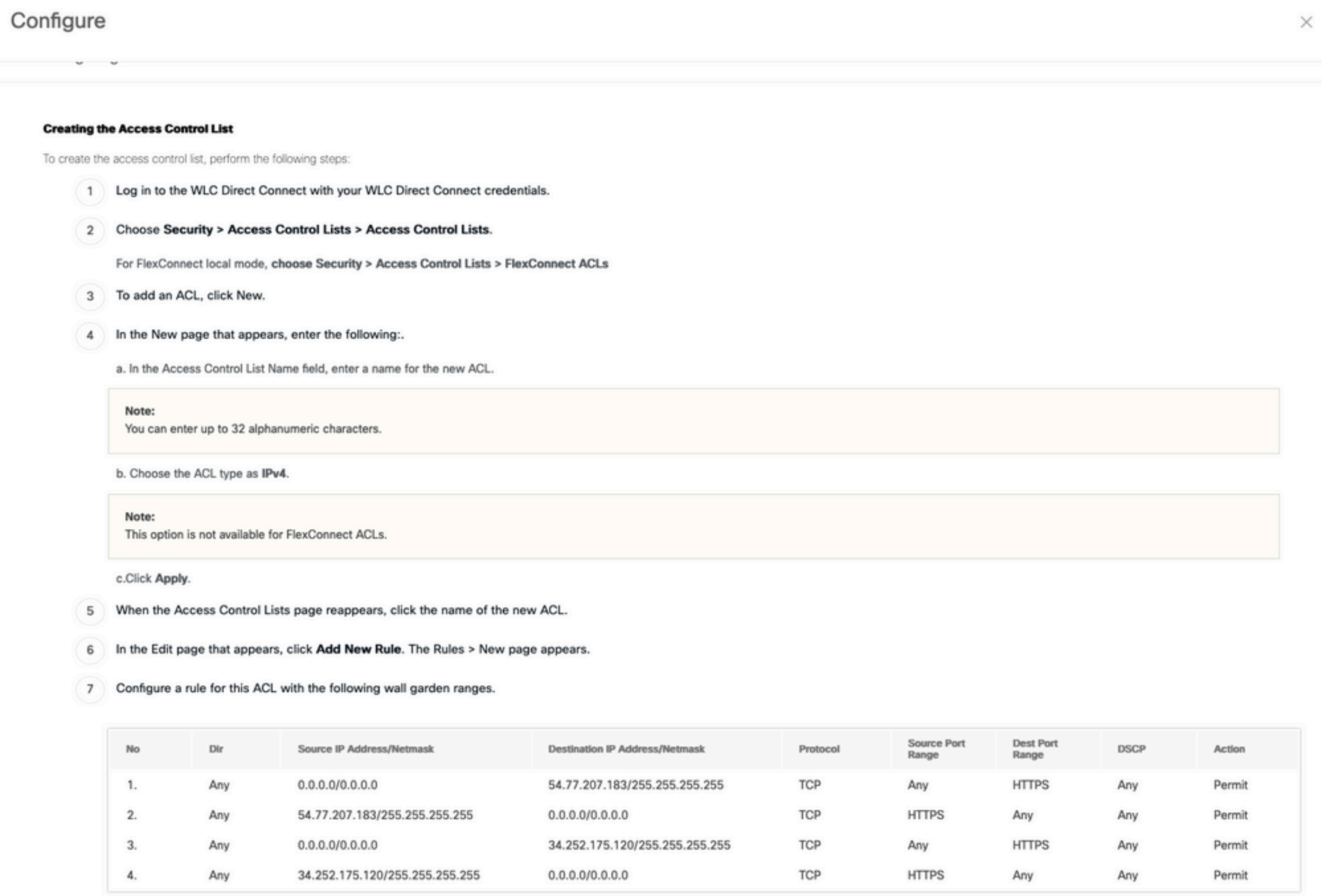
What are the IP Addresses that Spaces Use

In order to verify what IP addresses Spaces use for the portal in your region, navigate to the Captival Portal page on the Cisco DNA Space home. Click **SSID** in the left menu and then click **Configure manually** under your SSID. The IP addresses are mentioned in the ACL example. Those are the IP addresses of the portal for use in ACLs and webauth parameter map. Spaces use other IP address for the overall NMSP/cloud connectivity of the control plane.



SSID Configuration
You havent added any Cisco Meraki SSIDs yet.
Select below to get started

In the first section of the pop up that appears, step 7 shows you the IP addresses mentioned in the ACL definition. You do not need to do those instructions and create any ACL, just take note of the IP addresses. Those are the IPs used by the portal in your area



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.

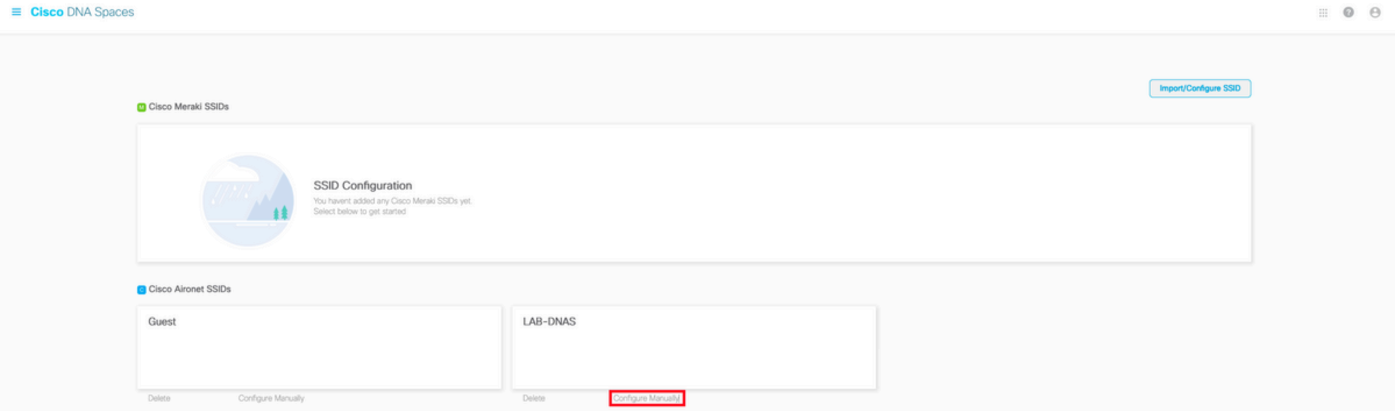
6 In the Edit page that appears, click **Add New Rule**. The Rules > New page appears.

7 Configure a rule for this ACL with the following wall garden ranges.

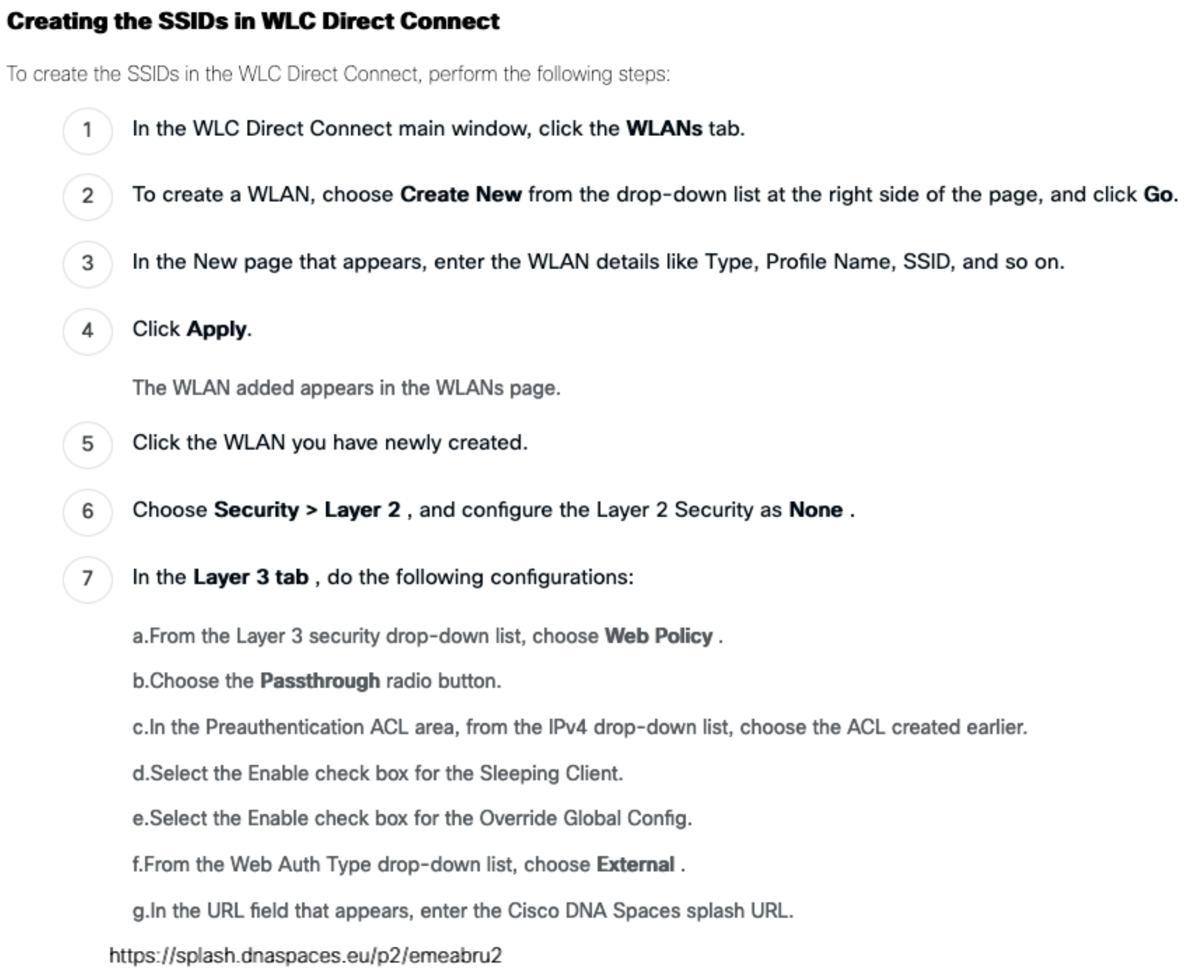
No	Dir	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP	Action
1.	Any	0.0.0.0/0.0.0.0	54.77.207.183/255.255.255.255	TCP	Any	HTTPS	Any	Permit
2.	Any	54.77.207.183/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit
3.	Any	0.0.0.0/0.0.0.0	34.252.175.120/255.255.255.255	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

What is the URL that the Spaces Log In Portal Uses

In order to verify what log in portal URL Spaces use for the portal in your region, navigate to the Captival Portal page on the Cisco DNA Space home. Click **SSID** in the left menu and then click **Configure manually** under your SSID.



Scroll down to the pop up that appears and in the second section, step 7 shows you the URL that you have to configure in your parameter map on the 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.

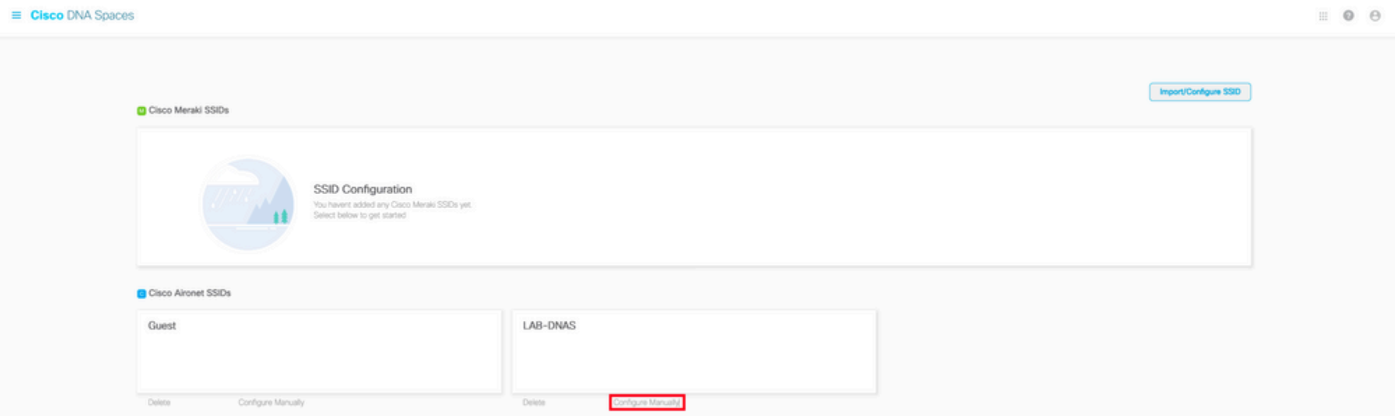
   f.From the Web Auth Type drop-down list, choose **External** .

   g.In the URL field that appears, enter the Cisco DNA Spaces splash URL.

https://splash.dnaspaces.eu/p2/emeabru2

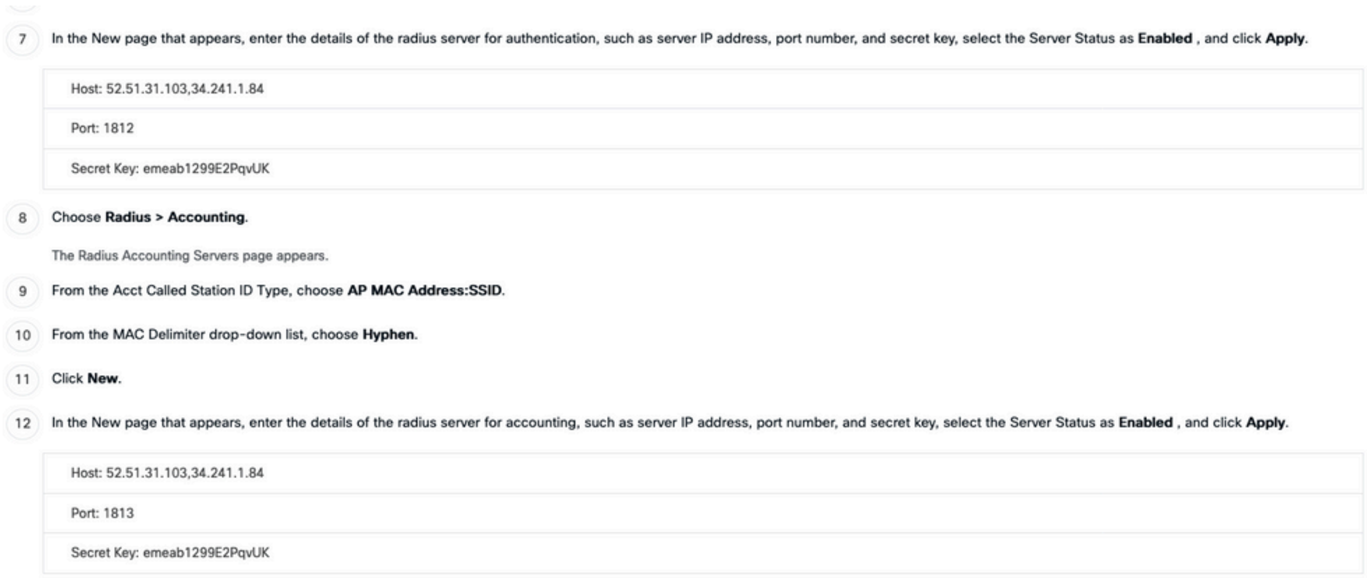
What are the RADIUS Server Details for Spaces

In order to find out what the RADIUS server IP addresses are that you need to use, as well as the shared secret, navigate to the Captival Portal page on the Cisco DNA Space home. Click **SSID** in the left menu and then click **Configure manually** under your SSID.



You havent added any Cisco Meraki SSIDs yet.
Select below to get started

In the pop up that appears, scroll down in the 3rd section (RADIUS), and step 7 gives you the IP/port and shared secret for radius authentication. Accounting is optional and is covered in step 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: emeab1299E2PqvUK

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**.

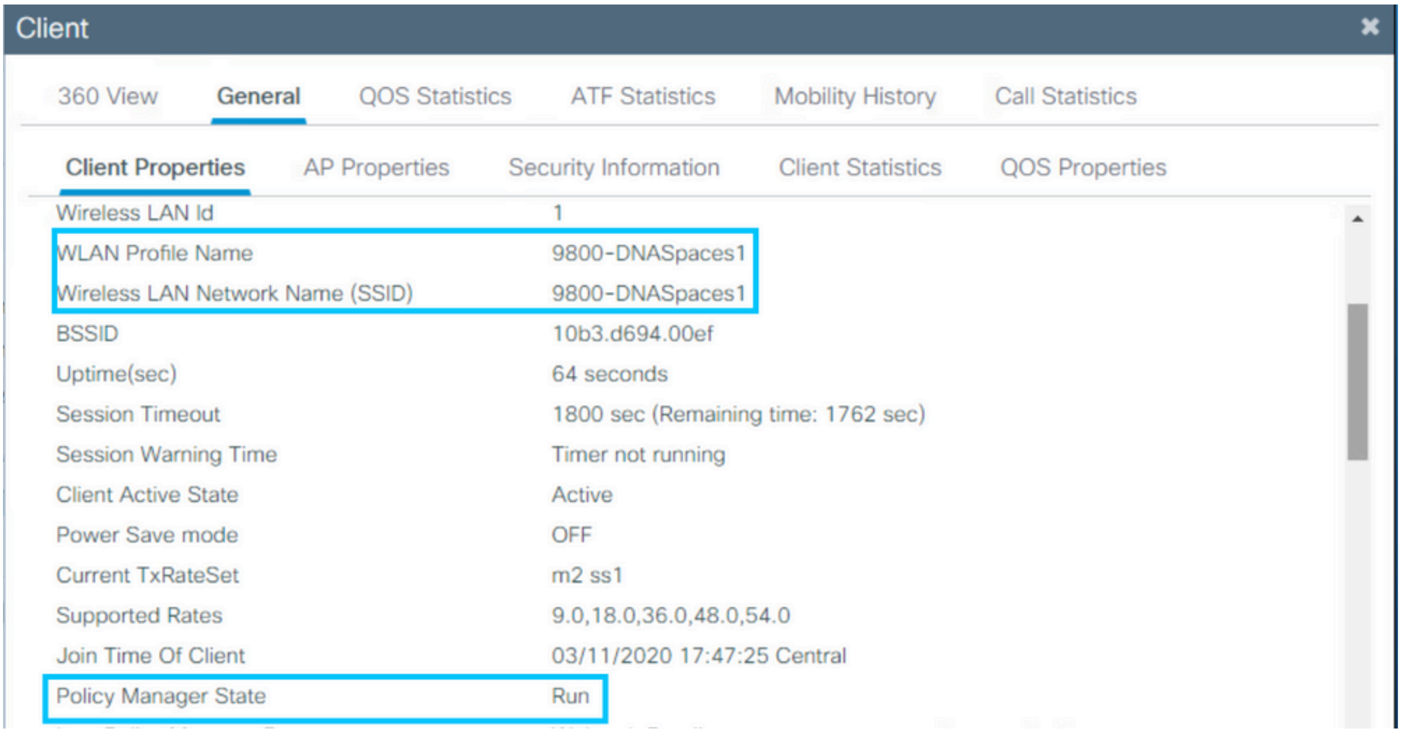
Host: 52.51.31.103,34.241.1.84

Port: 1813

Secret Key: emeab1299E2PqvUK

Verify

To confirm the status of a client connected to the SSID navigate to **Monitoring** > **Clients**. Click the MAC address of the device and look for Policy Manager State:



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

Common Issues

1. If the virtual interface on the controller has no IP address configured, the clients are redirected to the internal portal instead of the redirect portal configured in the parameter map.

2. If clients are receiving a 503 error while redirected to the portal on Spaces, make sure the controller is configured in the **Location Hierarchy** on Spaces.

Always-ON Tracing

WLC 9800 provides ALWAYS-ON tracing capabilities. This ensures all client connectivity related errors, warning, and notice level messages are constantly logged and you can view logs for an incident or failure condition after it has occurred.

Note: Depending on the volume of logs being generated, you can go back a few hours to several days.

In order to view the traces that 9800 WLC collected by default, you can connect via SSH/Telnet to the 9800 WLC and do these steps. Ensure you are logging the session to a text file.

Step 1. Check the controller current time so you can track the logs in the time back to when the issue happened.

```
# show clock
```

Step 2. Collect syslogs from the controller buffer or the external syslog as dictated by the system configuration. This provides a quick view of the system health and errors if any.

```
# show logging
```

Step 3. Verify if any debug conditions are enabled.

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

Note: If you see any condition listed, it means the traces are being logged up to debug level for all the processes that encounter the enabled conditions (mac address, IP address, and soon). This would increase the volume of logs. Therefore, it is recommended to clear all conditions when not actively debugging

Step 4. If the mac address under test was not listed as a condition in Step 3, collect the always-on notice level traces for the specific mac address.

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

You can either display the content on the session or you can copy the file to an external TFTP server.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Conditional Debugging and Radio Active Tracing

If the always-on traces do not give you enough information to determine the trigger for the problem under investigation, you can enable conditional debugging and capture Radio Active (RA) trace, which provides debug level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debugging, do these steps.

Step 1. Ensure there are no debug conditions are enabled.

```
# clear platform condition all
```

Step 2. Enable the debug condition for the wireless client mac address that you want to monitor.

These commands start to monitor the provided mac address for 30 minutes (1800 seconds). You can optionally increase this time to up to 2,085,978,494 seconds.

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

Note: In order to monitor more than one client at a time, run debug **wireless mac <aaaa.bbbb.cccc>** command per mac address.

Note: You do not see the output of the client activity on the terminal session, as everything is buffered internally to be viewed later.

Step 3. Reproduce the issue or behavior that you want to monitor.

Step 4. Stop the debugs if the issue is reproduced before the default, or configured monitor time is up.

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

Once the monitor-time has elapsed, or the debug wireless has been stopped, the 9800 WLC generates a local file with the name:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Step 5. Collect the file of the mac address activity. You can either copy the ra trace.log to an external server, or display the output directly on the screen.

Check the name of the RA traces file

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

Copy the file to an external server:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

Display the content:

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

Step 6. If the root cause is still not obvious, collect the internal logs which are a more verbose view of debug level logs. You do not need to debug the client again as you only take a further detailed look at debug logs that have been already collected and internally stored.

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

Note: This command output returns traces for all logging levels for all processes and is quite voluminous. Please engage Cisco TAC to help parse through these traces.

You can either copy the ra-internal-FILENAME.txt to an external server or display the output directly on the screen.

Copy the file to an external server:

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

Display the content:

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

Step 7. Remove the debug conditions.

```
# clear platform condition all
```

Note: Ensure that you always remove the debug conditions after a troubleshooting session.

Example of a Successful Attempt

This is the output from the RA_traces for 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:

```
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-
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_
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
```

IP Learn process:

```
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
```

Layer 3 authentication:

```
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 stat
[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 [10.10.30.4
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-agent = Mic
```

```
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in LOGIN sta
[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 [10.10.30.4
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-agent = Moz
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]POST rcvd when in LOGIN st
```

Layer 3 authentication successful. Move the client to the RUN state:

```
[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 (9800DNA
Managed client RUN state notification: 34e1.2d23.a668
Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RU
```