使用Catalyst 9800 WLC配置DNA空间强制网络门户

目录

简介

本文档介绍如何在Cisco DNA空间上配置强制网络门户。

先决条件

本文档允许Catalyst 9800无线LAN控制器(C9800 WLC)上的客户端使用DNA空间作为外部Web身份验证登录页。

要求

Cisco 建议您了解以下主题：

- 对9800无线控制器的命令行界面(CLI)或图形用户界面(GUI)访问
- 思科DNA空间

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 9800-L控制器版本16.12.2s

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Web身份验证是一种简单的第3层身份验证方法，不需要请求方或客户端实用程序。这可以做到

a)使用C9800 WLC上的“内部”页面（按原样或进行修改）

b)将自定义登录捆绑包上传到C9800 WLC

c)外部服务器上托管的自定义登录页

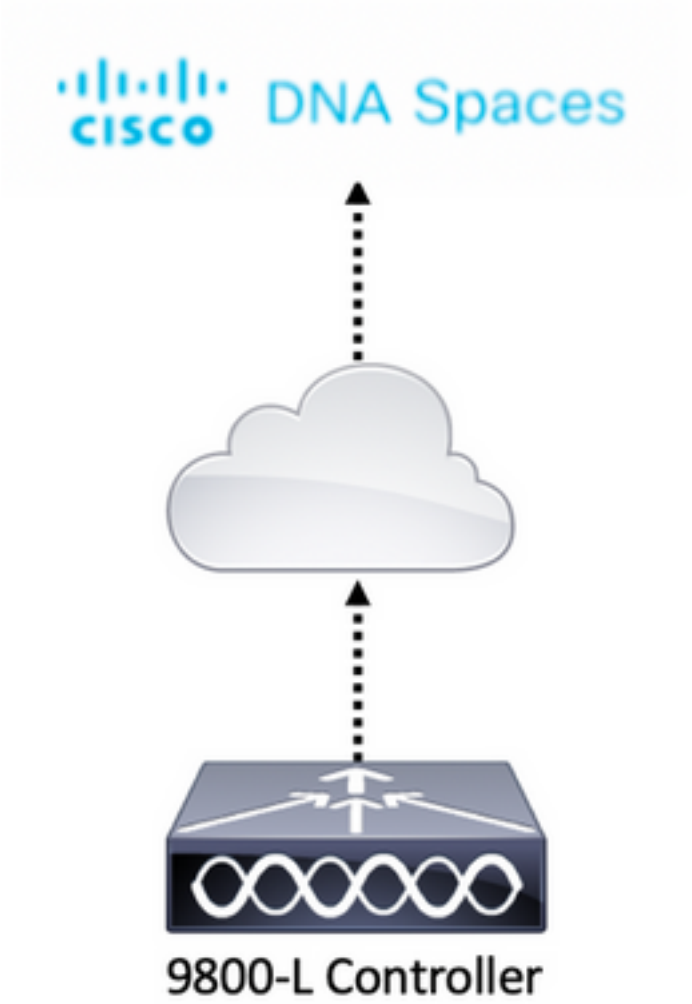
利用DNA Spaces提供的强制网络门户，实质上是一种在C9800 WLC上为客户端实施外部Web身份验证的方法。

外部Web身份验证过程详见
：https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/web-authentication/b-configuring-web-based-authentication-on-cisco-catalyst-9800-series-controllers/m-external-web-authentication-configuration.html

在C9800 WLC上，虚拟IP地址定义为全局参数映射，通常为192.0.2.1

配置

网络图



将9800控制器连接到思科DNA空间

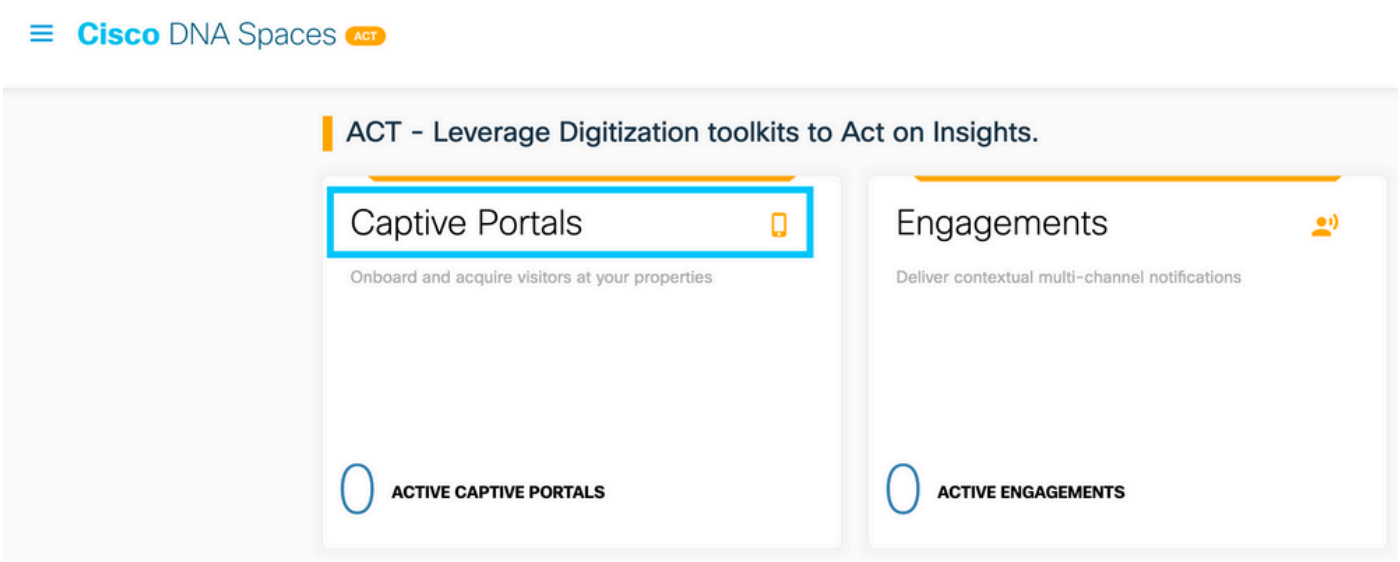
控制器需要通过任何选项（直接连接、通过DNA空间连接器或CMX Tethering）连接到DNA空间。

在本例中，虽然强制网络门户的配置方式对所有设置都相同，但直接连接选项仍在使用。

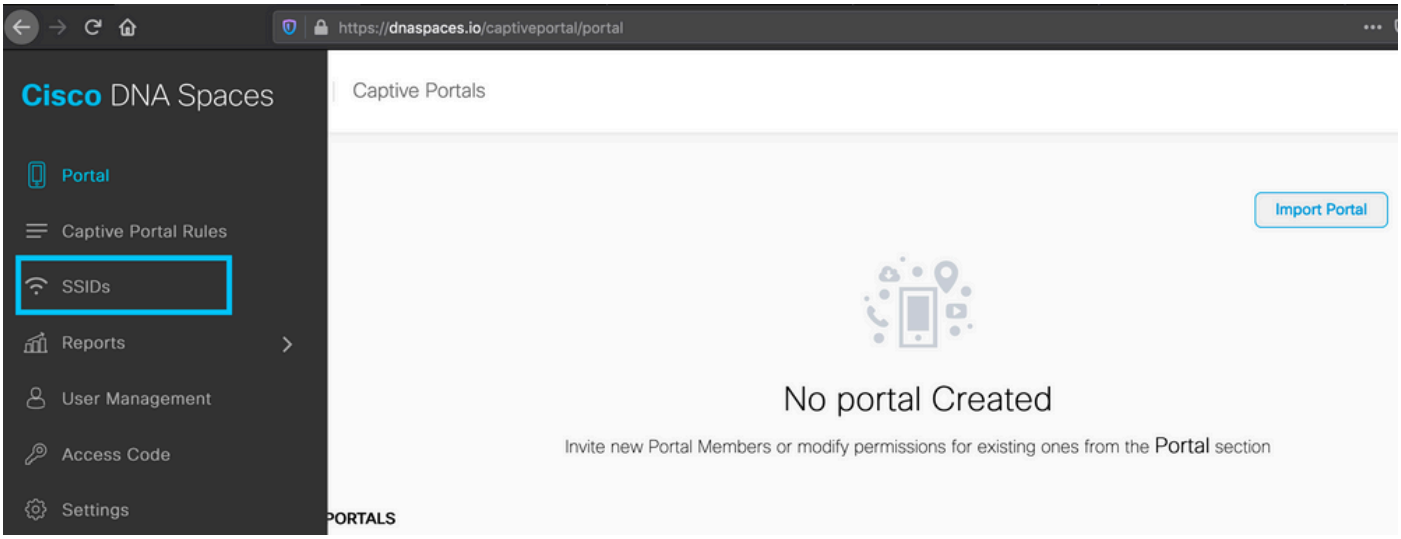
要将控制器连接到思科DNA空间，它必须能够通过HTTPS访问思科DNA空间云。有关如何将9800控制器连接到DNA空间的更多信息，请参阅以下链接： DNA空间 — 9800控制器直接连接

在DNA空间上创建SSID

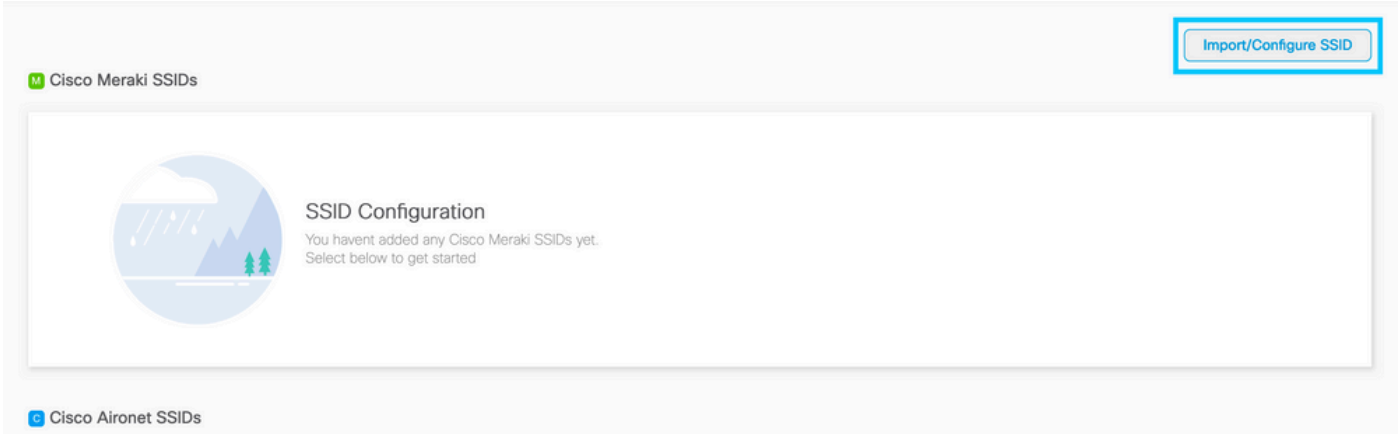
步骤1:点击DNA空间控制面板中的**强制网络门户**:



第二步：打开强制网络门户特定菜单，点击页面左上角的三行图标，然后点击**SSID:**



第三步：单击**Import/Configure SSID**，选择**CUWN(CMX/WLC)**作为“Wireless Network”类型并输入SSID名称：



9800控制器上的ACL和URL过滤器配置

在完成身份验证之前，不允许来自无线客户端的流量进入网络。在Web身份验证情况下，为了完成身份验证，无线客户端连接到此SSID，接收IP地址，然后将客户端策略管理器状态移至**Webauth_reqd**状态。由于客户端尚未进行身份验证，因此会丢弃来自客户端IP地址的所有流量，但

DHCP、DNS和HTTP除外（这些流量会被拦截并重定向）。

默认情况下，设置Web-auth WLAN时，9800会创建硬编码预身份验证ACL。这些硬编码ACL允许DHCP、DNS和流向外部Web身份验证服务器的流量。所有其余部分会像任何http流量一样重定向。
但是，如果需要允许特定非HTTP流量类型通过，则可以配置预身份验证ACL。然后，您需要模拟现有硬编码预身份验证ACL的内容（从本部分的第1步开始），并根据您的需求对其进行扩充。

步骤1:检验当前的硬编码ACL

CLI 配置：

```
Andressi-9800L#show ip access list

Extended IP access list WA-sec-34.235.248.212
10 permit tcp any host 34.235.248.212 eq www
20 permit tcp any host 34.235.248.212 eq 443
30 permit tcp host 34.235.248.212 eq www any
40 permit tcp host 34.235.248.212 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-34.235.248.212
10 deny tcp any host 34.235.248.212 eq www
20 deny tcp any host 34.235.248.212 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

WA-sec-34.235.248.212就是这样调用的，因为它是一个自动Web身份验证(WA)安全(sec)ACL或门户ip“34.235.248.212”。安全ACL定义了允许的内容（在允许时）或丢弃的内容（在拒绝时）

Wa-v4-int是拦截ACL，即传送ACL或重定向ACL，定义哪些内容发送到CPU进行重定向（在允许时）或者哪些内容发送到数据平面（在拒绝时）。

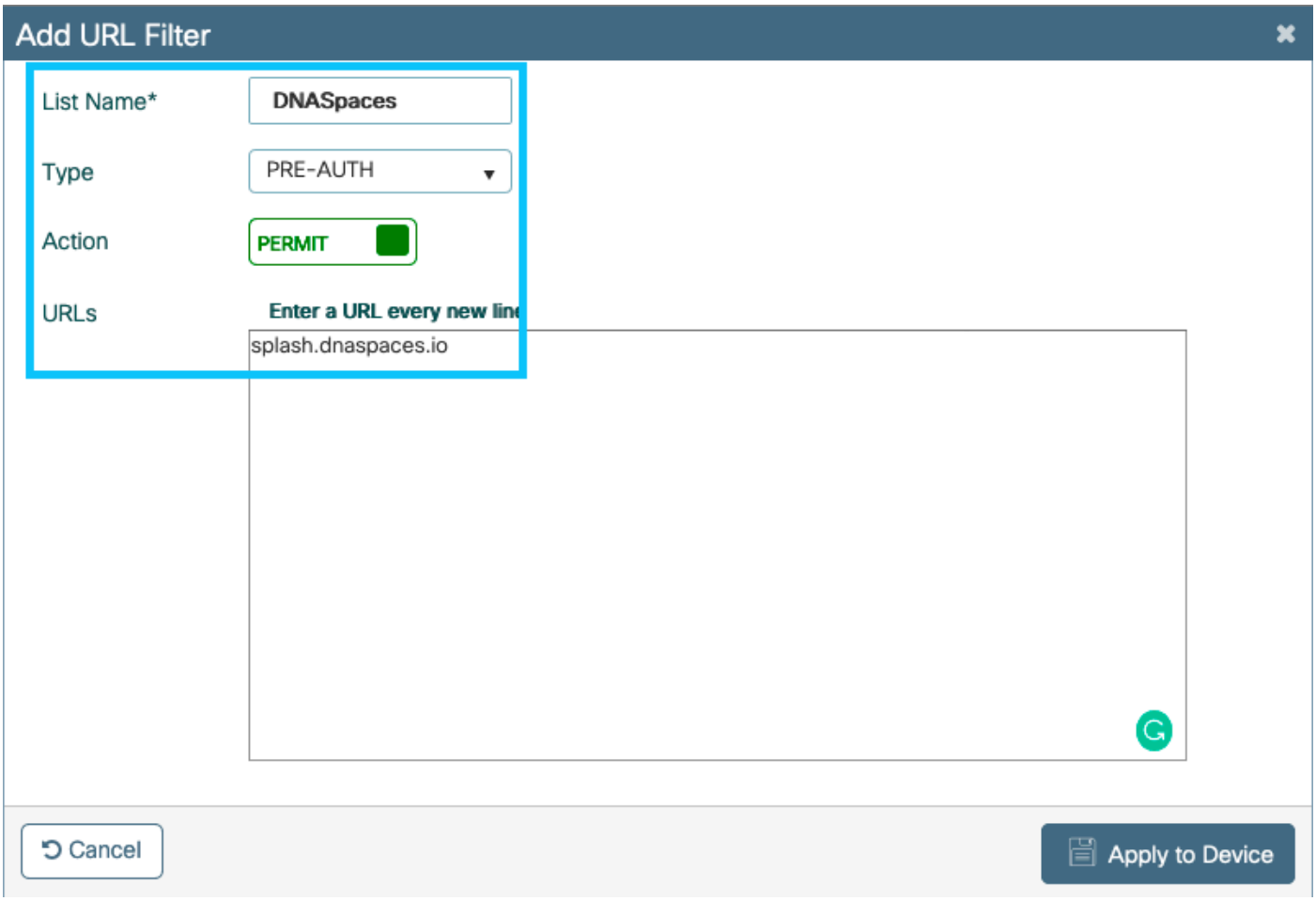
WA-v4-int34.235.248.212首先应用于来自客户端的流量，并将指向DNA空间门户IP 34.235.248.212的HTTP流量保留在数据平面上（尚未丢弃或转发操作，只需移交给数据平面）。它将所有HTTP流量发送到CPU（除了由Web服务器服务的虚拟IP流量外，重定向除外）。其他类型的流量则提供给数据平面。

WA-sec-34.235.248.212允许发往您在Web身份验证参数映射中配置的DNA空间IP 34.235.248.212的HTTP和HTTPS流量，还允许DNS和DHCP流量并丢弃其余流量。要拦截的HTTP流量在到达此ACL之前已被拦截，因此无需由此ACL覆盖。

> **注**：要获取ACL中允许的DNA空间的IP地址，请在ACL配置部分下的**在DNA空间上创建SSID部分**的第3步中创建的SSID中单击**Configure Manually**选项。一个示例位于文档末尾的“DNA空间使用哪些IP地址”部分。

DNA空间使用2个IP地址，并且步骤1中的机制只允许一个门户IP。要允许对更多HTTP资源进行预身份验证访问，您需要使用URL过滤器，该过滤器会在与您在URL过滤器中输入其URL的网站相关的IP动态地造成拦截（重定向）和安全（预身份验证）ACL的漏洞。动态监听DNS请求，使9800获知这些URL的IP地址并将其动态添加到ACL。

第二步：配置URL过滤器以允许DNA空间域。导航到Configuration > Security > URL Filters，点击**+Add**并配置列表名称，选择**PRE-AUTH**作为类型，操作为**PERMIT**,URLsplash.dnaspaces.io（如果使用EMEA门户，则选择.eu）：



CLI 配置：

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

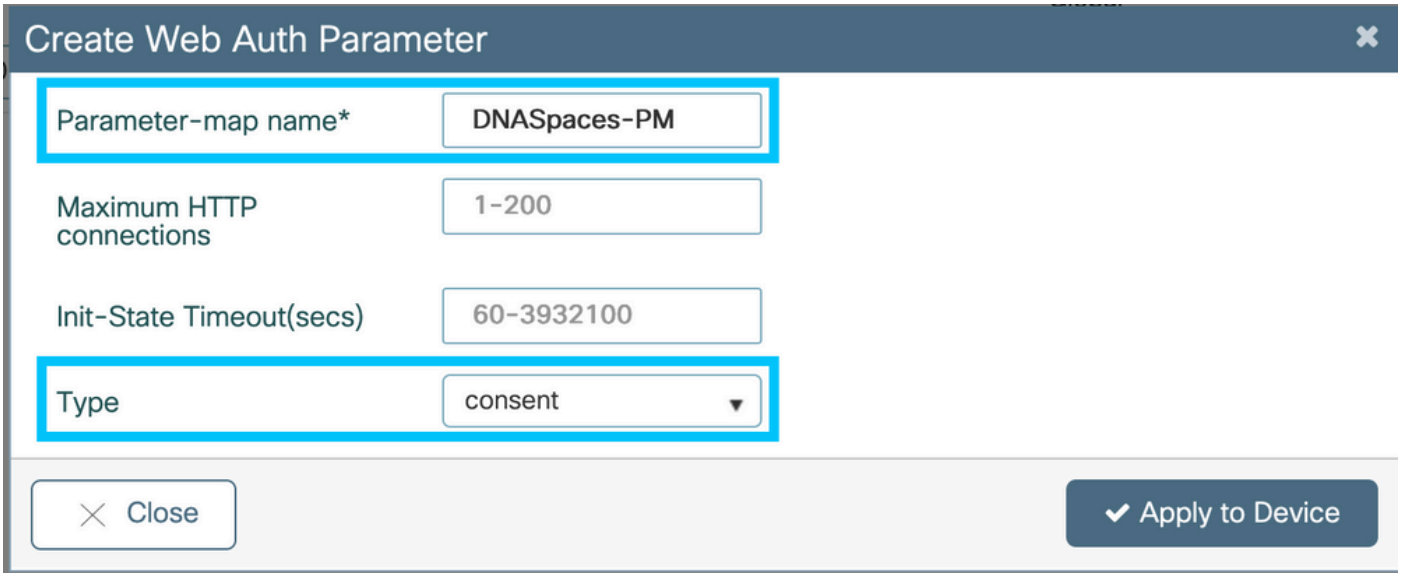
```
Andressi-9800L(config-urlfilter-params)#action permit
Andressi-9800L(config-urlfilter-params)#url splash.dnaspaces.io
```

可以将SSID配置为使用RADIUS服务器或不使用RADIUS服务器。如果会话持续时间、带宽限制或无缝调配Internet在强制网络门户规则配置的**操作**部分配置，则需要使用RADIUS服务器配置SSID，否则无需使用RADIUS服务器。两种配置都支持DNA空间上的各种门户。

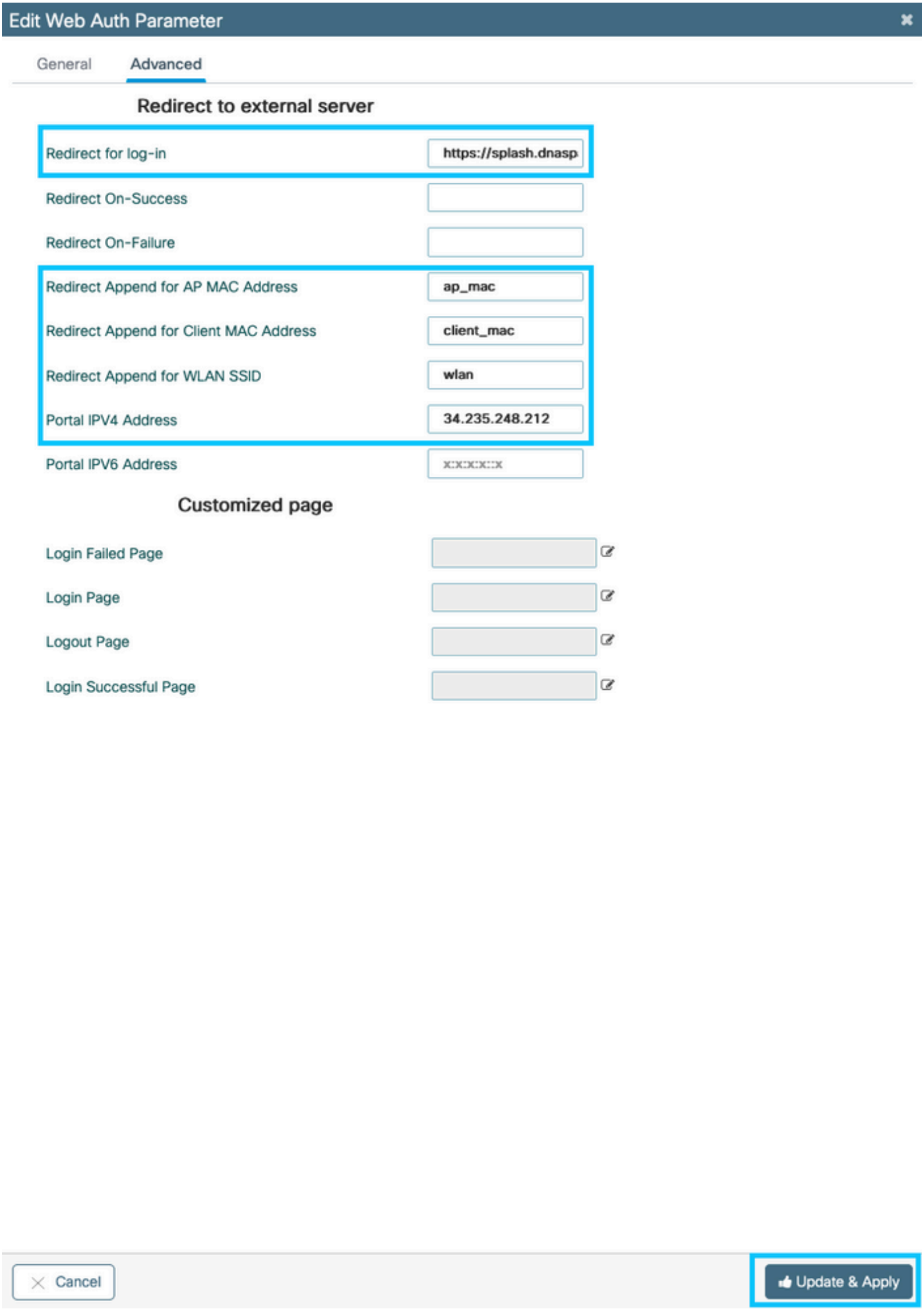
DNA空间上没有RADIUS服务器的强制网络门户

9800控制器上的Web身份验证参数映射配置

步骤1:导航到**配置>安全> Web身份验证**，单击**+添加**以创建新的参数映射。在弹出的窗口中，配置参数映射名称，然后选择**Consent**作为类型：



第二步：单击上一步中配置的参数映射，导航到**Advanced**选项卡，然后输入Redirect for log-in URL、Append for AP MAC Address、Append for Client MAC Address、Append for WLAN SSID and portal IPv4 Address，如图所示，单击Update & Apply:


Edit Web Auth Parameter
General
Advanced
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
Cancel
Update & Apply

注意：要获取启动页URL和IPv4重定向地址，请点击DNA空间的SSID页面中的**Configure Manually**（手动配置）选项。本文档末尾的“DNA空间门户使用哪个URL？”中对此进行了说明

注意:Cisco DNA Spaces门户可以解析为两个IP地址，但9800控制器只允许配置一个IP地址，选择其中任一IP地址并在参数映射上将其配置为门户IPv4地址。

注：确保 虚拟IPv4和IPv6地址都在全局Web身份验证参数映射中配置。如果未配置虚拟IPv6，客户端有时会被重定向到内部门户，而不是配置的DNA空间门户。这就是必须始终配置虚拟IP的原因。“192.0.2.1”可以配置为虚拟IPv4，而FE80:0:0:903A::11E4配置为虚拟IPV6。除了这些IP，很少有或根本没有理由使用其它IP。

CLI 配置：

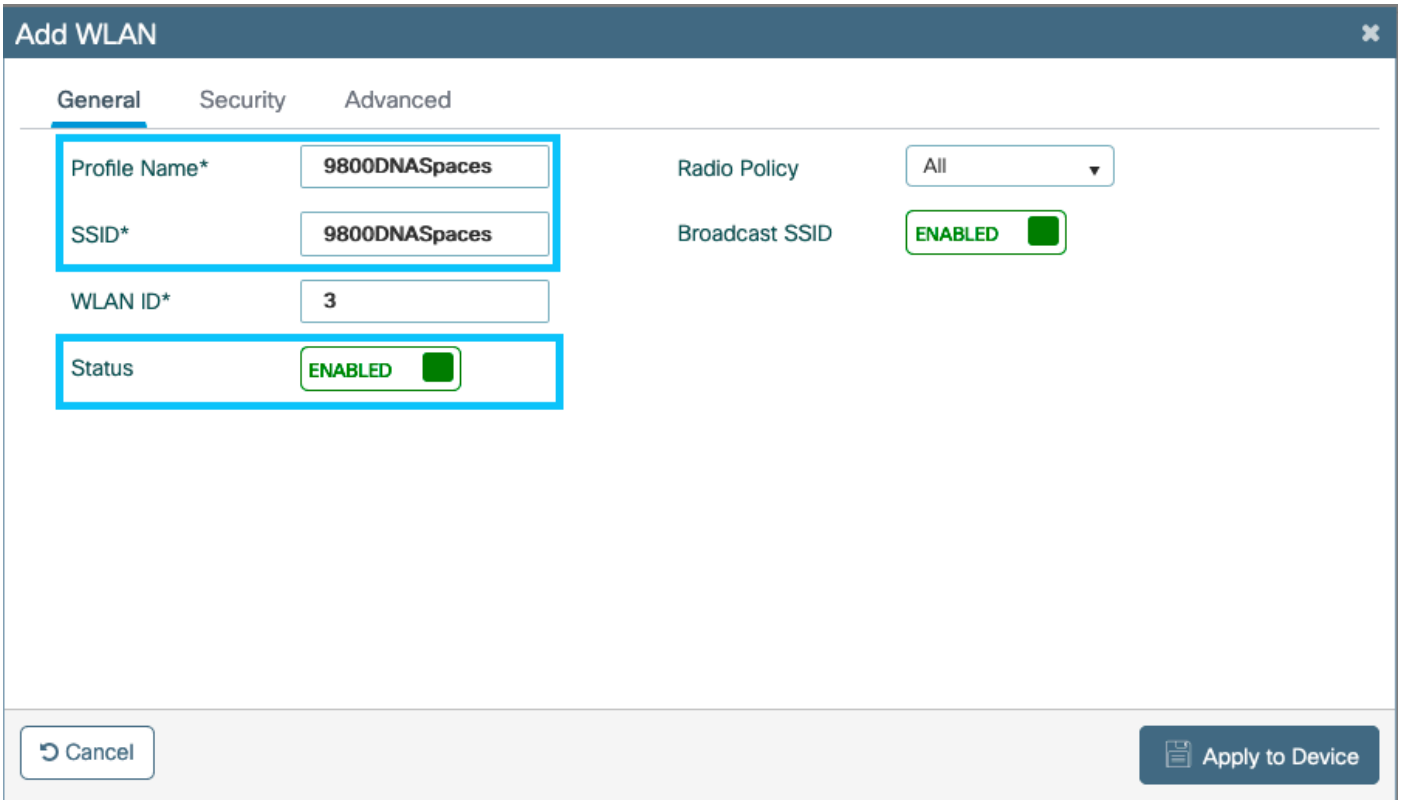
```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type consent
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
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
```

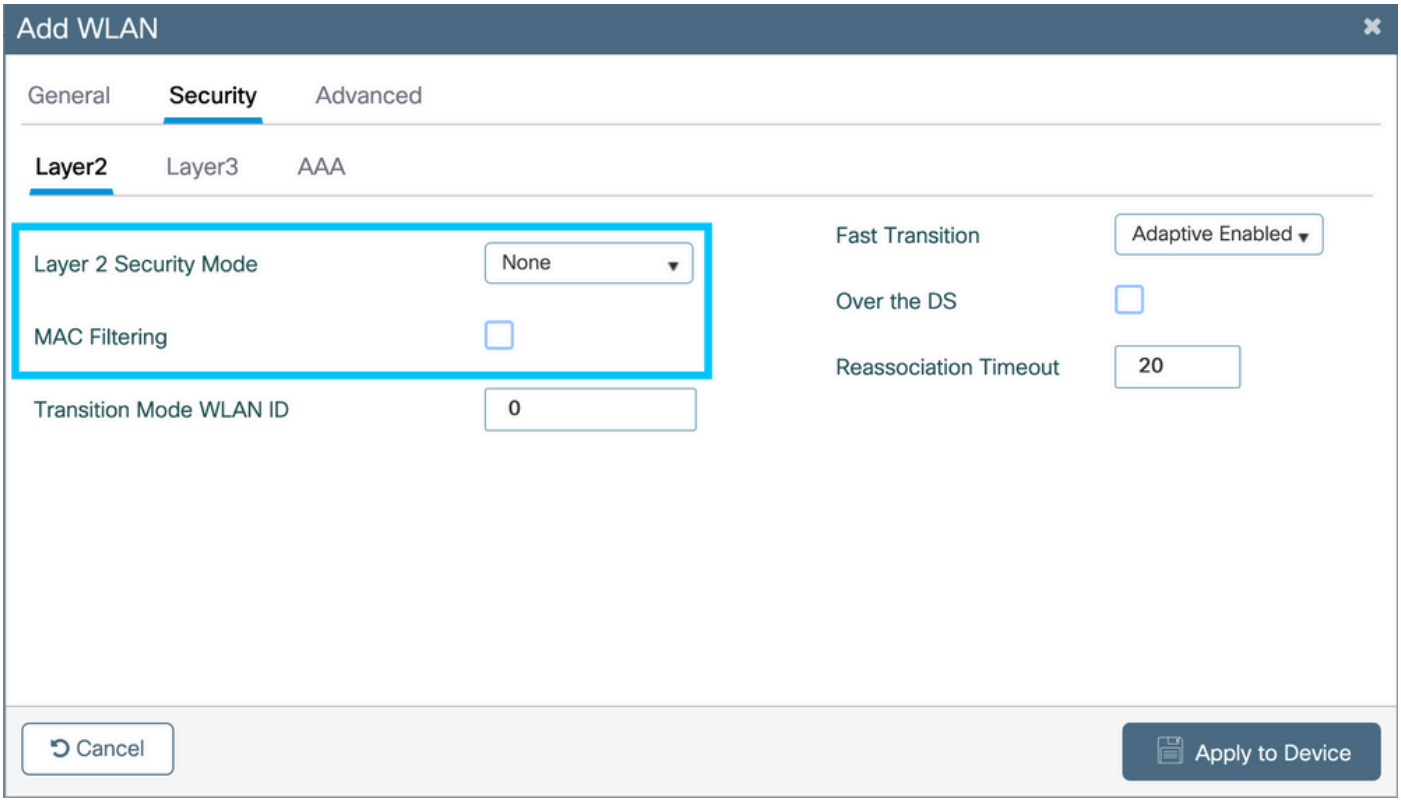
```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

在9800控制器上创建SSID

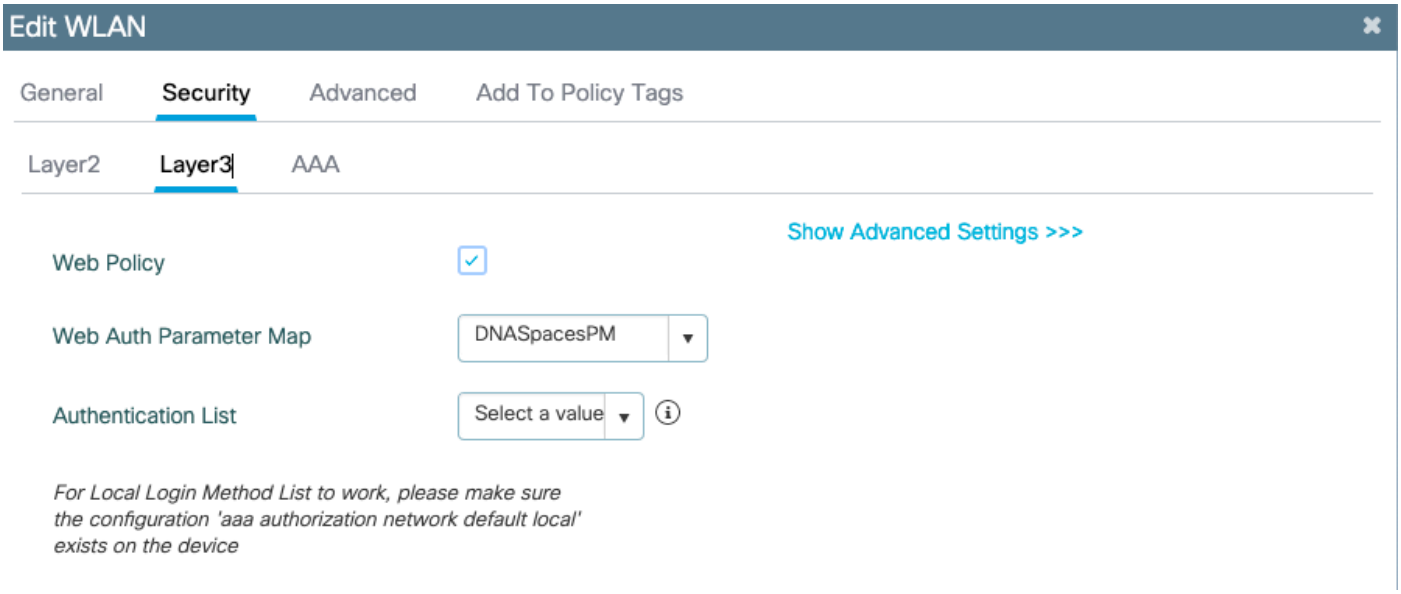
步骤1:导航到**配置>标签和配置文件> WLAN**，单击**+添加。**配置配置文件名称、SSID并启用WLAN。确保SSID名称与**在DNA空间上创建SSID**部分步骤3中配置的名称相同。



第二步：导航到**Security > Layer2。将Layer 2 Security Mode设置为None**，确保MAC Filtering处于禁用状态。

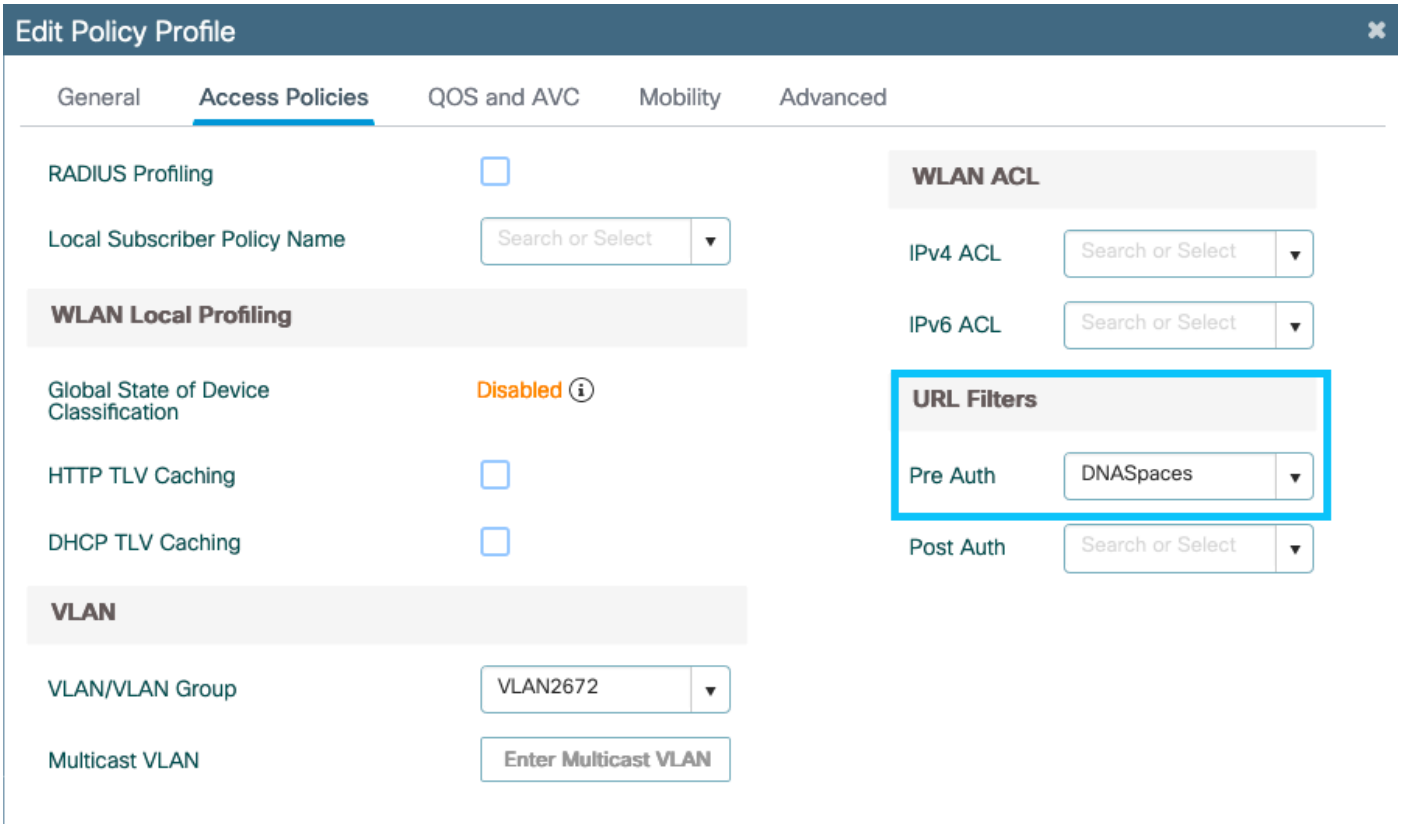


第三步：导航到**Security > Layer3。**启用Web策略，配置Web身份验证参数映射。单击**Apply to Device。**



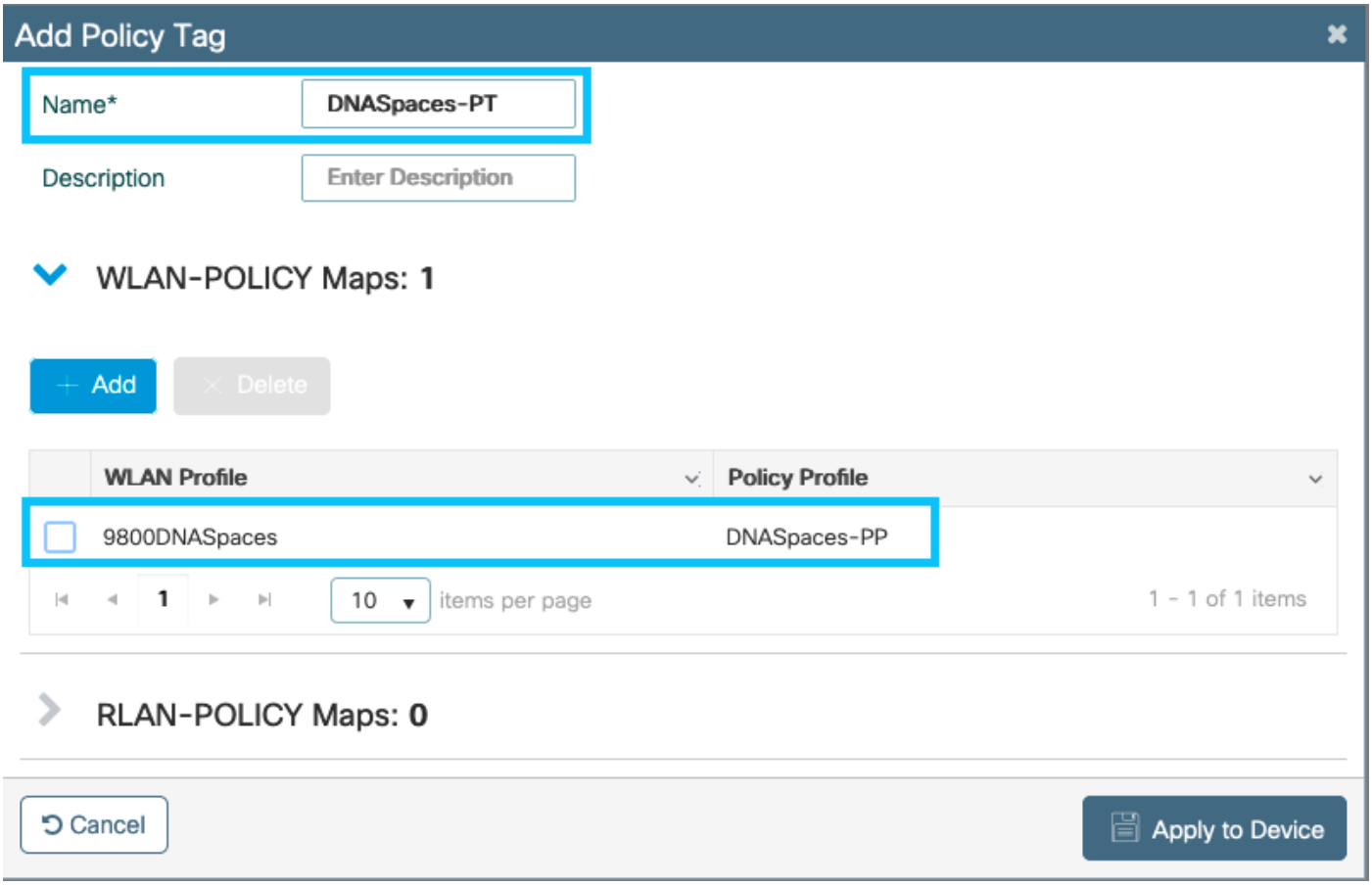
在9800控制器上配置策略配置文件

步骤1:导航到**Configuration > Tags & Profiles > Policy**，然后创建新的策略配置文件或使用默认策略配置文件。在访问策略(Policies)选项卡中，配置客户端VLAN并添加URL过滤器。

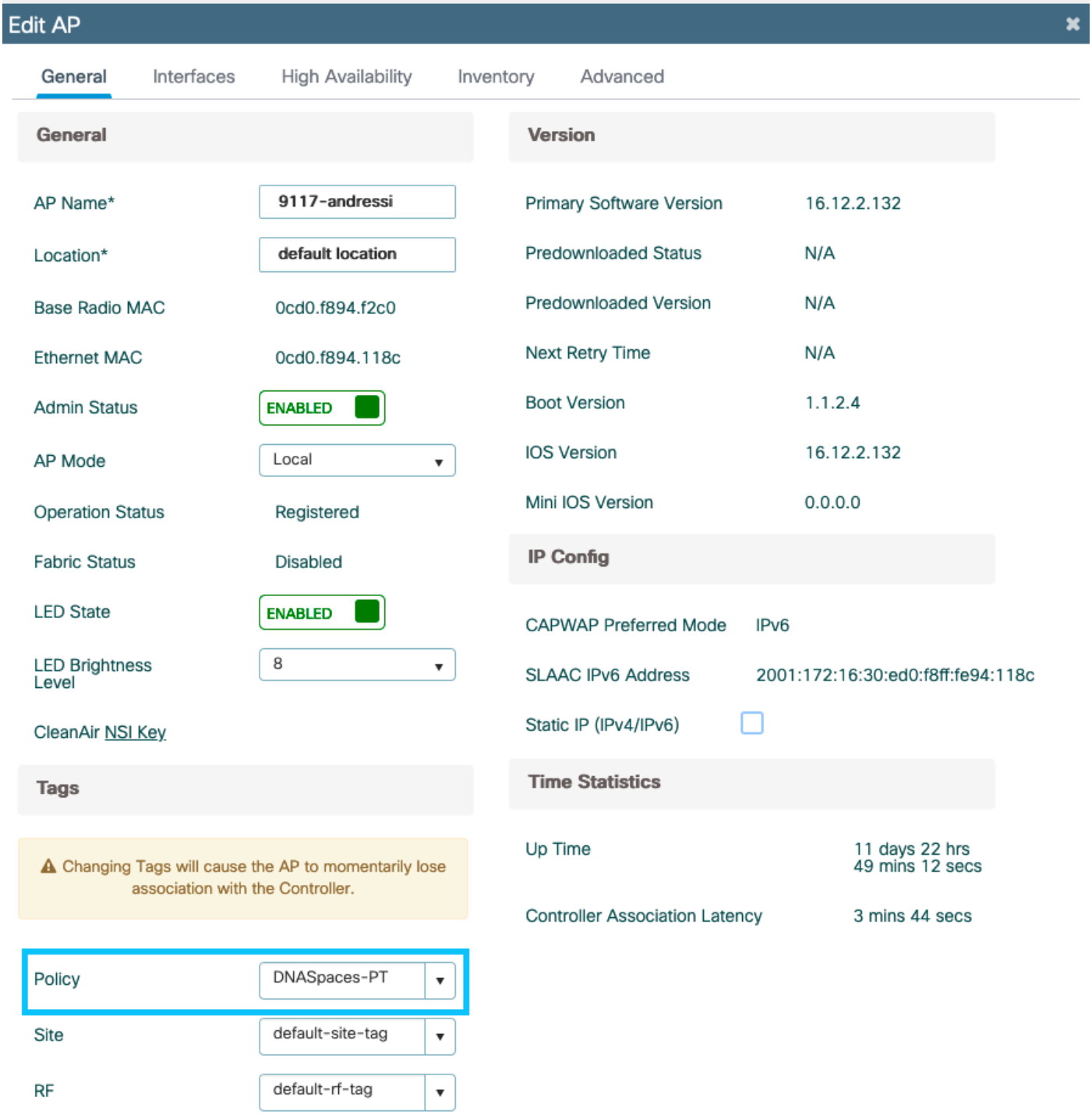


在9800控制器上配置策略标记

步骤1:导航到**配置>标记和配置文件>策略。**创建新的策略标记或使用默认策略标记。将WLAN映射到策略标记中的策略配置文件。



第二步：将策略标记应用于AP以广播SSID。导航到**Configuration > Wireless > Access Points**，选择有问题的AP并添加策略标记。这会导致AP重新启动其CAPWAP隧道并返回到9800控制器：



CLI 配置：

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

```
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
Andressi-9800L(config-wlan)#no shutdown

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

```
Andressi-9800L(config-wireless-policy)#vlan <id>
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter
```

```
Andressi-9800L(config-wireless-policy)#no shutdown
```

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

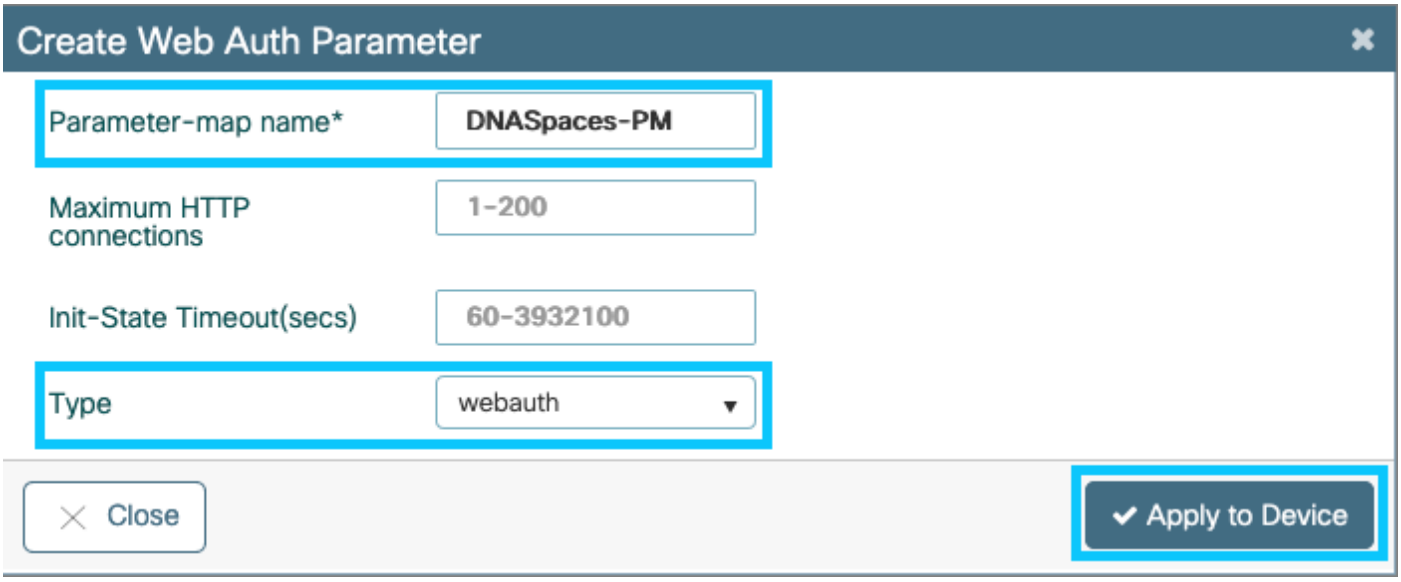
```
Andressi-9800L(config-policy-tag)#wlan
```

在DNA空间上具有RADIUS服务器的强制网络门户

注意:DNA空间RADIUS服务器仅支持来自控制器的PAP身份验证。

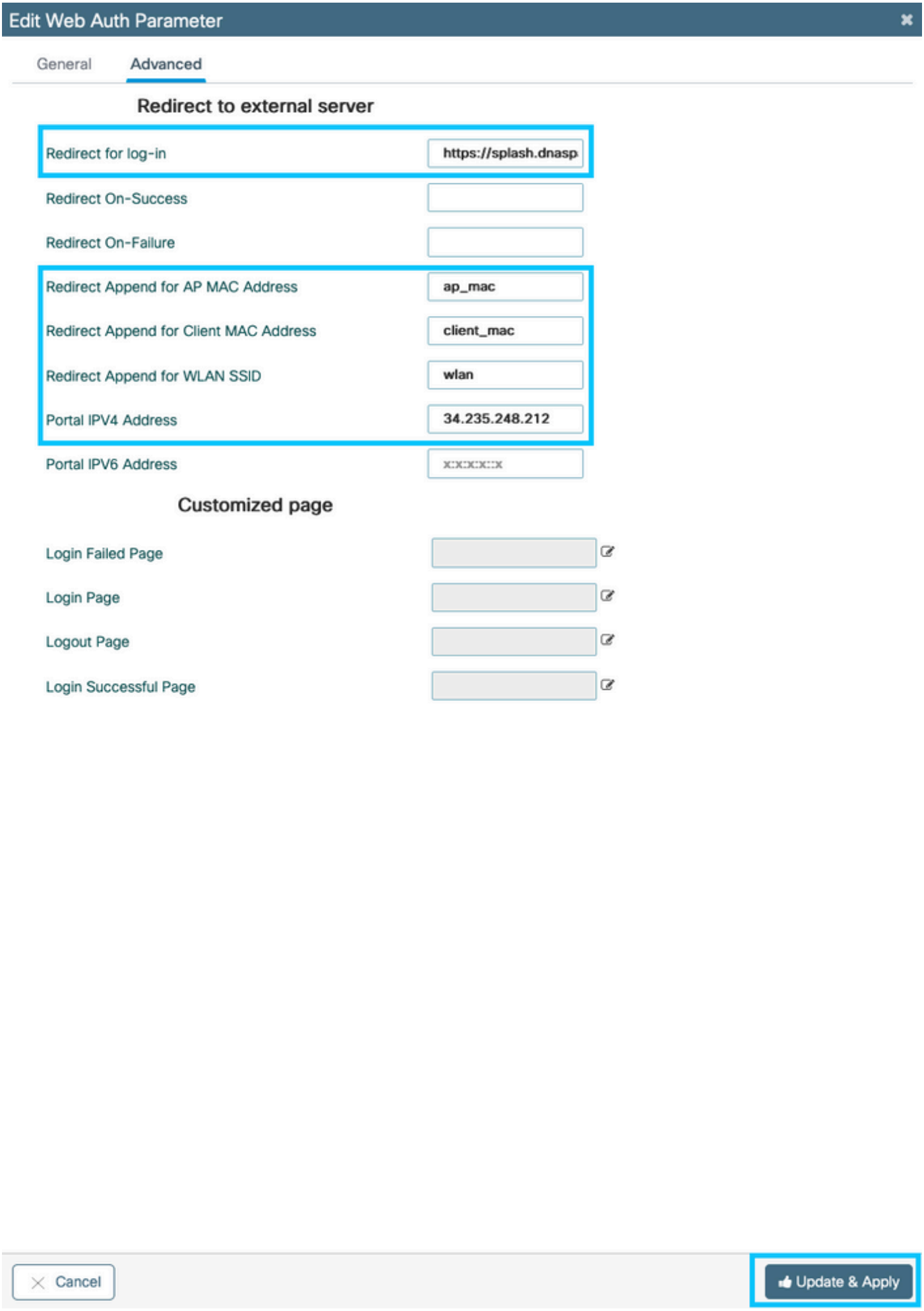
9800控制器上的Web身份验证参数映射配置

步骤1:创建网络身份验证参数映射。导航到**Configuration > Security > Web Auth**，单击**+Add**，然后配置参数映射名称，然后选择**webauth**作为类型：



第二步：单击在步骤1中配置的参数映射，单击**Advanced**，然后输入Redirect for log-in、Append for AP MAC Address、Append for Client MAC Address、Append for WLAN SSID and portal IPv4

Address。单击**Update & Apply:**


Edit Web Auth Parameter
General
Advanced
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
Cancel
Update & Apply

注：要获取启动页URL和IPv4重定向地址，请分别点击在DNA空间上创建SSID**部分**在WLC直接连接中创建SSID**部分**创建访问控制列表配置**部分下的Configure Manually**选项。

注意：Cisco DNA Spaces门户可以解析为两个IP地址，但9800控制器仅允许配置一个IP地址，一个案例选择参数映射中要配置的任何一个IP地址作为门户IPv4地址。

注意： 确保在全局Web身份验证参数映射中同时配置虚拟IPv4和IPv6地址。如果未配置虚拟IPv6，客户端有时会被重定向到内部门户而不是配置的DNA空间门户。这就是必须始终配置虚拟IP的原因。“192.0.2.1”可以配置为虚拟IPv4，而FE80:0:0:903A::11E4配置为虚拟IPV6。除了这些IP，很少有或根本没有理由使用其它IP。

CLI 配置：

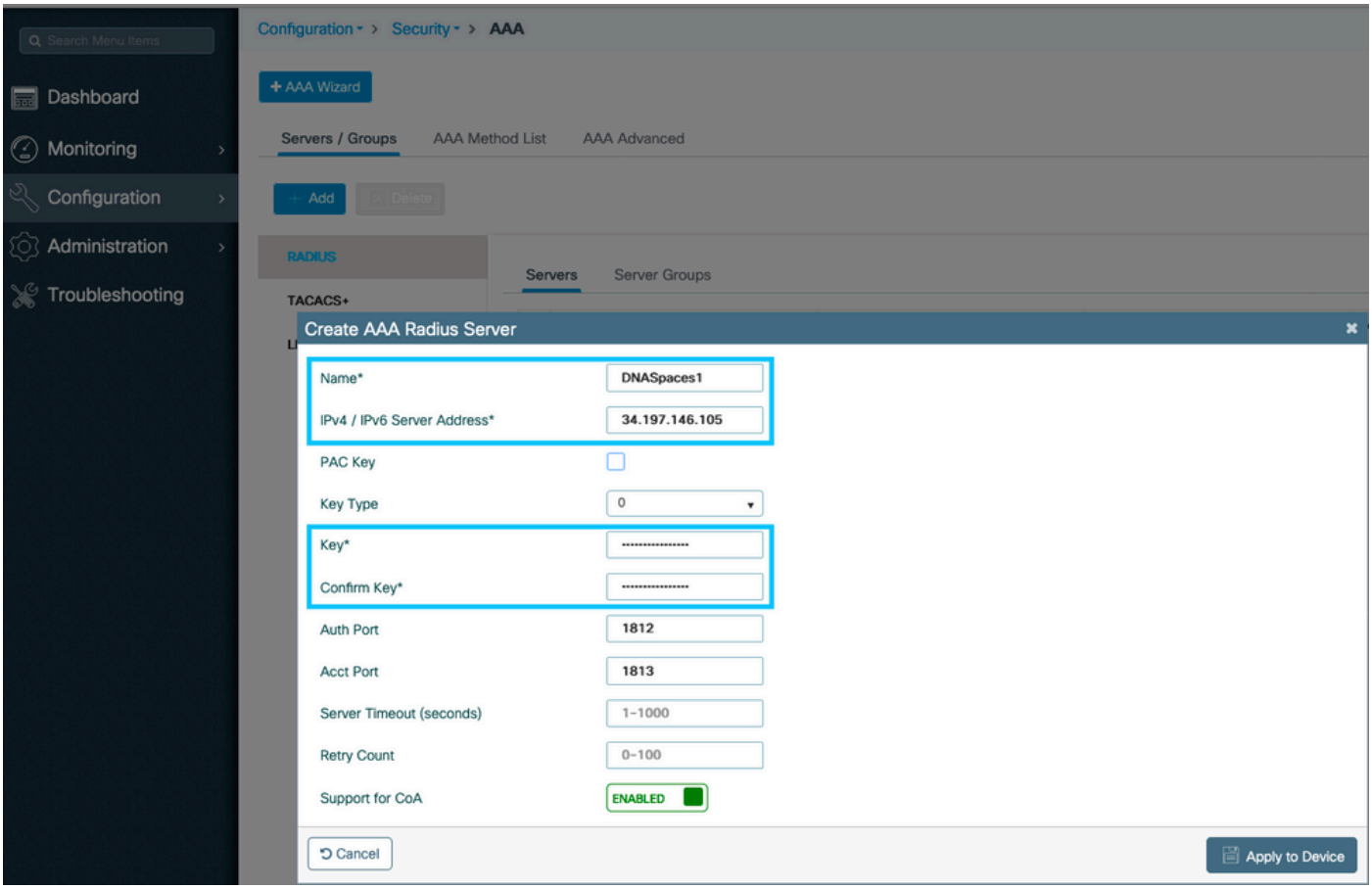
```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type webauth
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
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
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

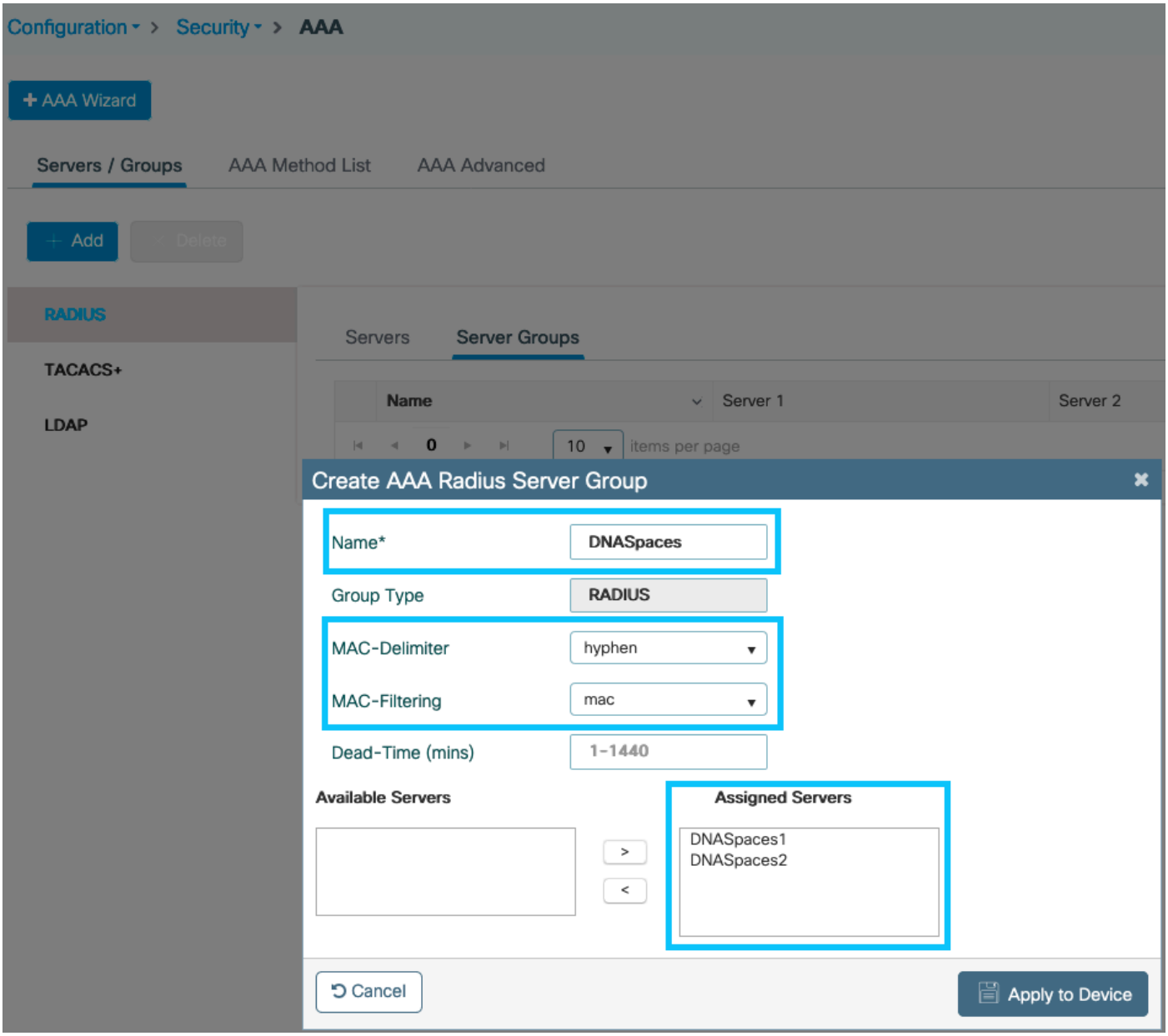
9800控制器上的RADIUS服务器配置

步骤1:配置RADIUS服务器。Cisco DNA Spaces充当RADIUS服务器进行用户身份验证，它可以对两个IP地址做出响应。导航到**Configuration > Security > AAA**，点击**+Add**并配置两个RADIUS服务器：

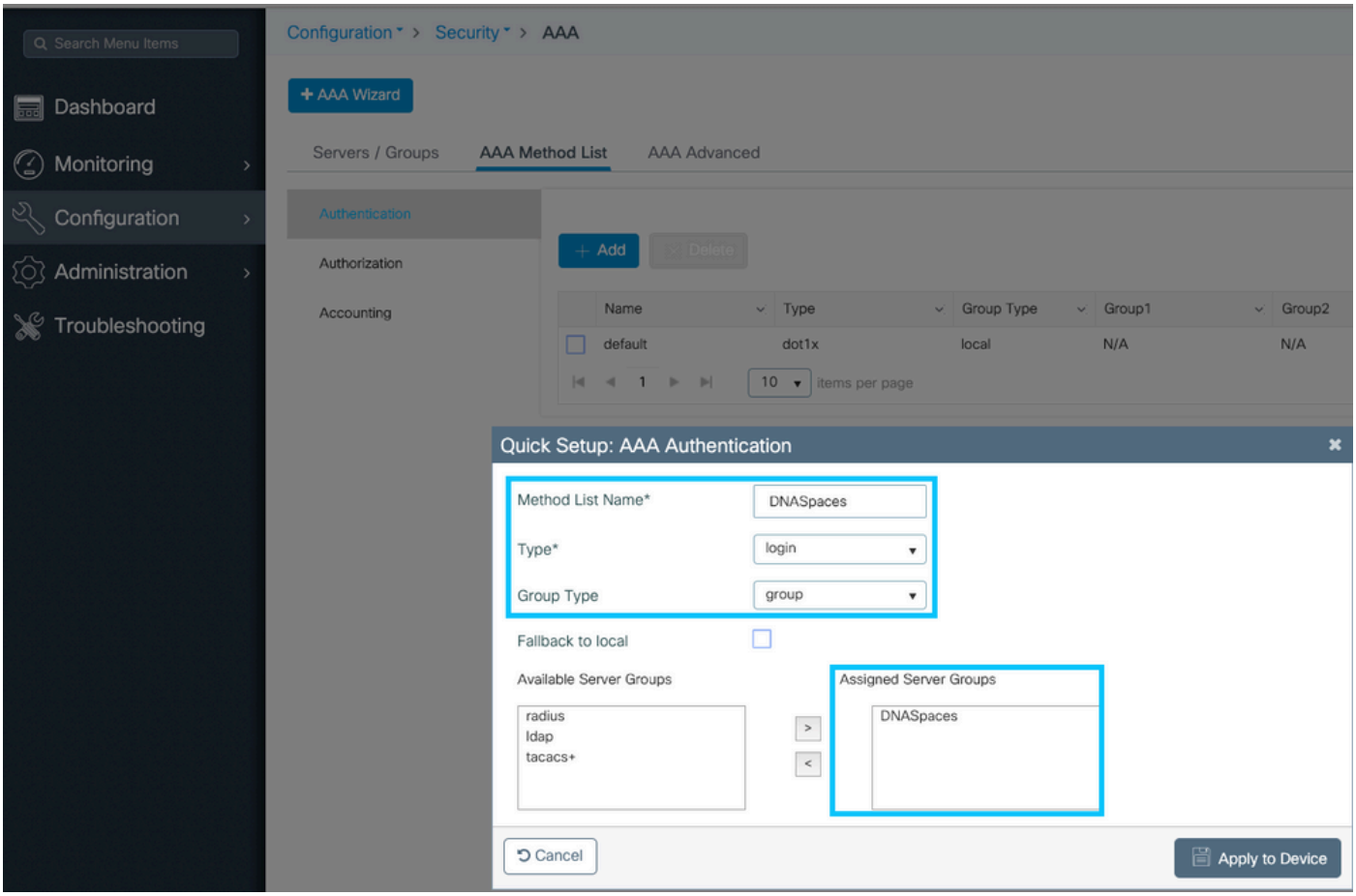


注：要获取主服务器和辅助服务器的RADIUS IP地址和密钥，请点击**在DNA空间上创建SSID**部分**第3步中创建的SSID中的Configure Manually**选项，然后导航至**RADIUS Server Configuration部分。**

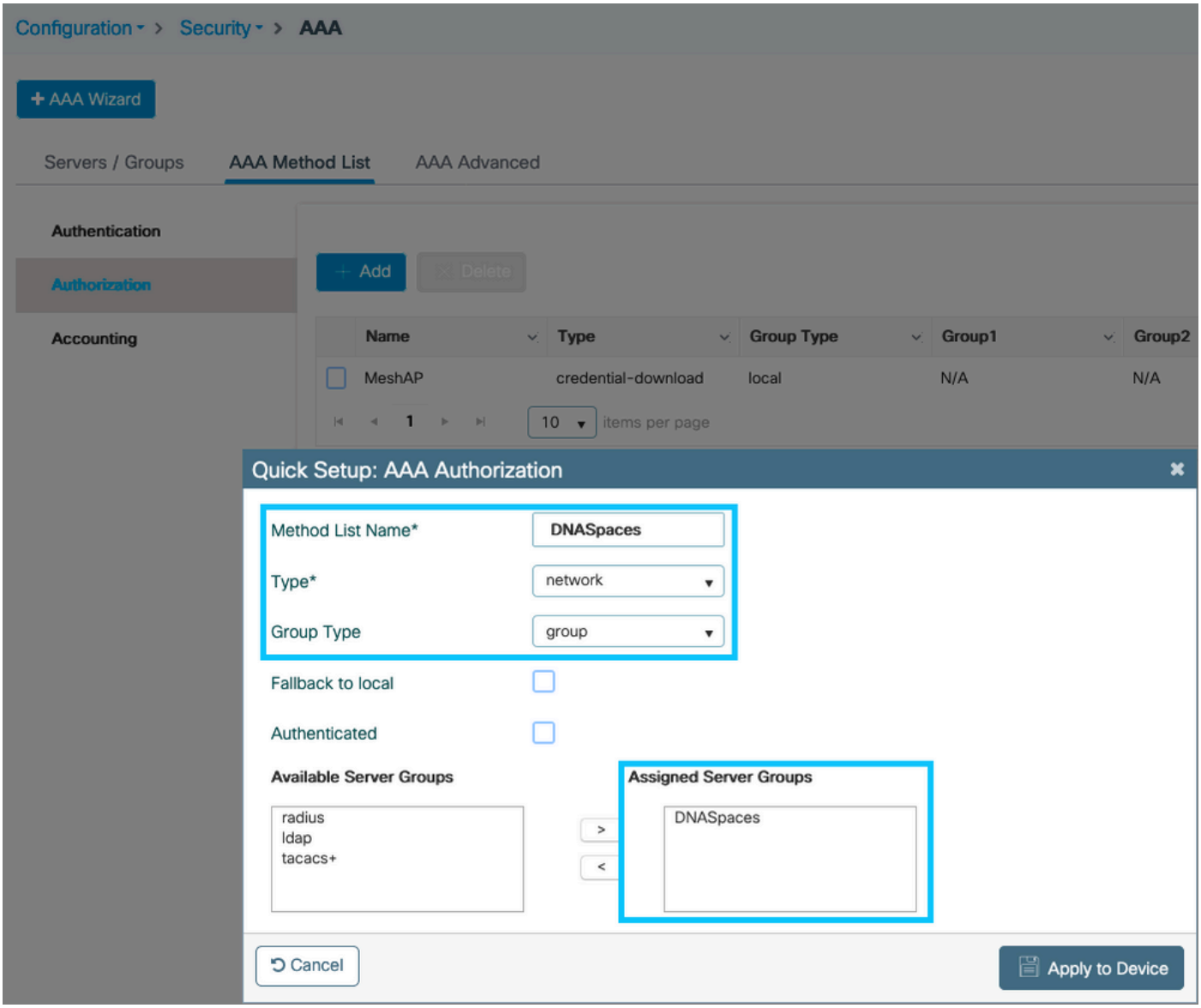
第二步：配置RADIUS服务器组并添加两个RADIUS服务器。导航到**Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups**，单击**+add**，将Server Group name、MAC-Delimiter as **Hyphen**、MAC-Filtering as **MAC**，然后分配两个RADIUS服务器：



第三步：配置身份验证方法列表。导航到Configuration > Security > AAA > AAA Method List > Authentication，点击+add。配置方法列表名称，选择login作为类型并分配服务器组：

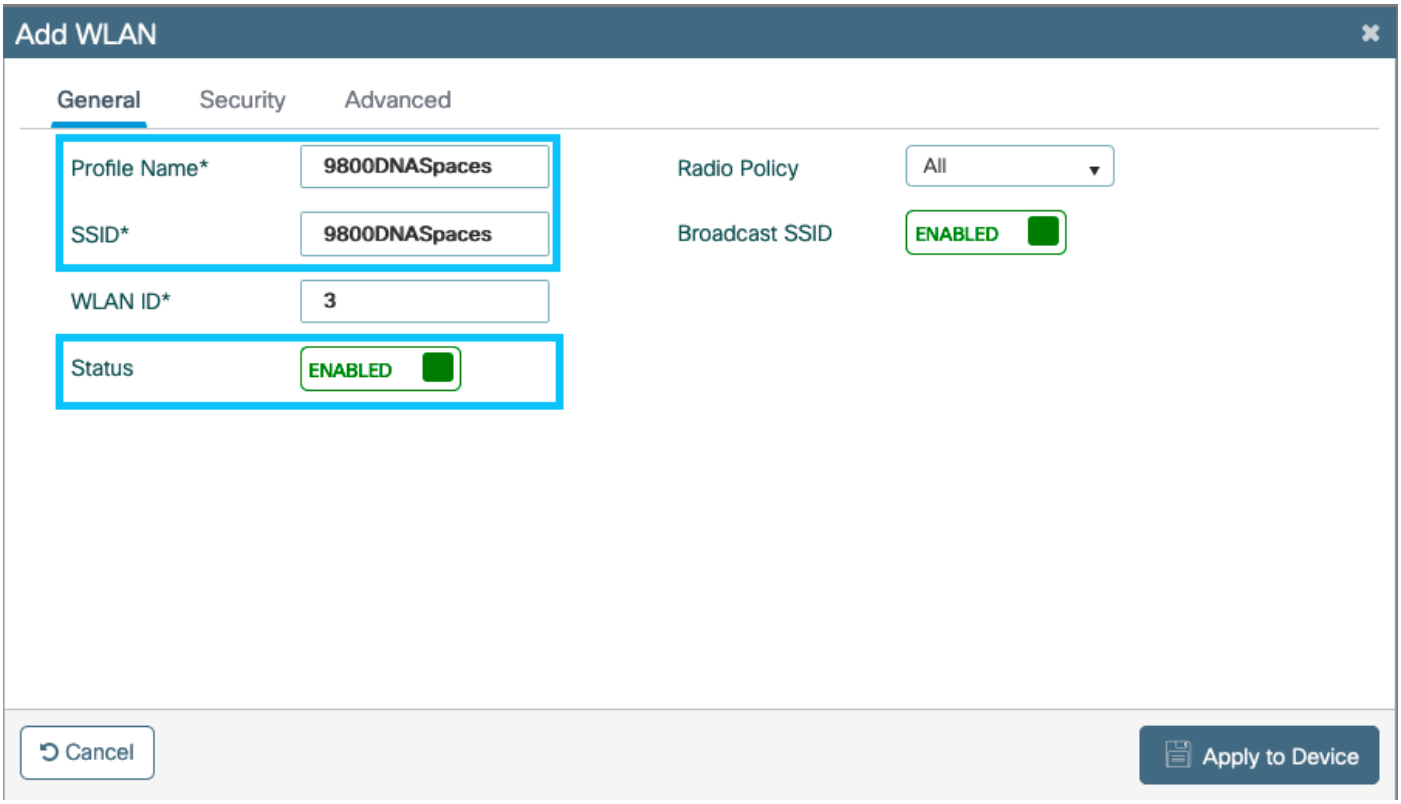


第四步：配置授权方法列表。导航到**Configuration > Security > AAA > AAA Method List > Authorization**，点击**+add**。配置方法列表名称，选择**network**作为类型并分配服务器组：

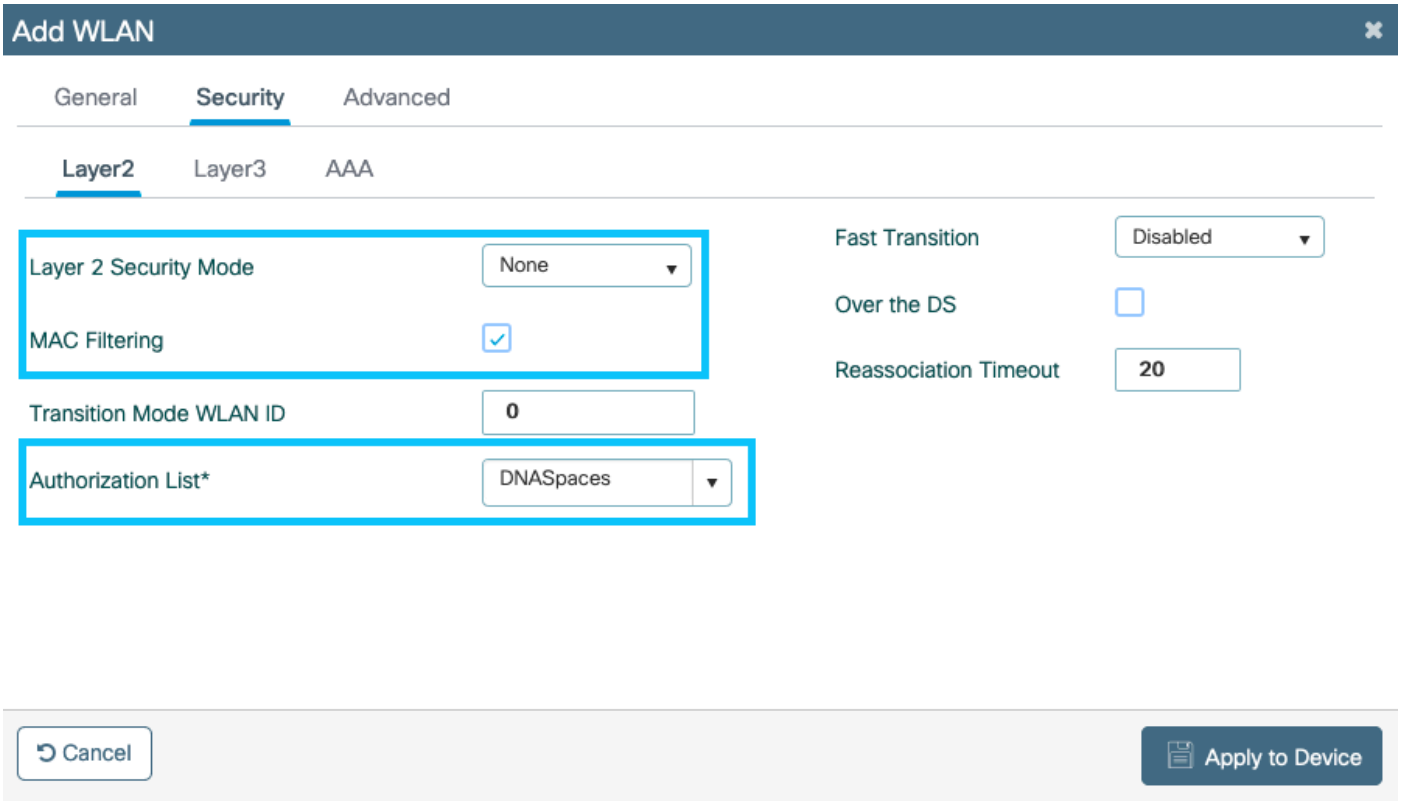


在9800控制器上创建SSID

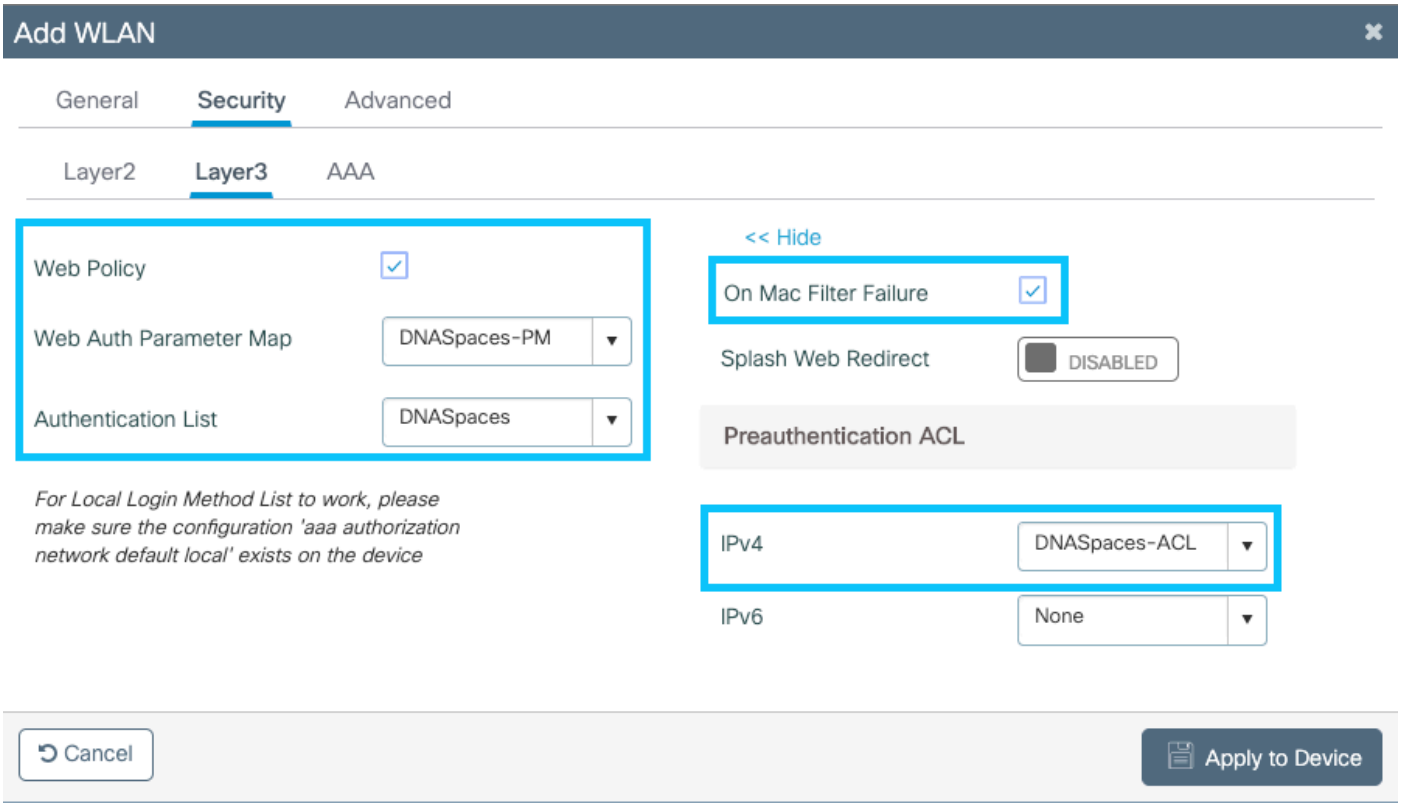
步骤1:导航到**配置>标签和配置文件> WLAN**，单击**+添加。**配置配置文件名称、SSID并启用WLAN。确保SSID名称与**在DNA空间上创建SSID**部分步骤3中配置的名称相同。



第二步：导航到**Security > Layer2。**将第2层安全模式设置为**None，启**用MAC过滤并添加授权列表：

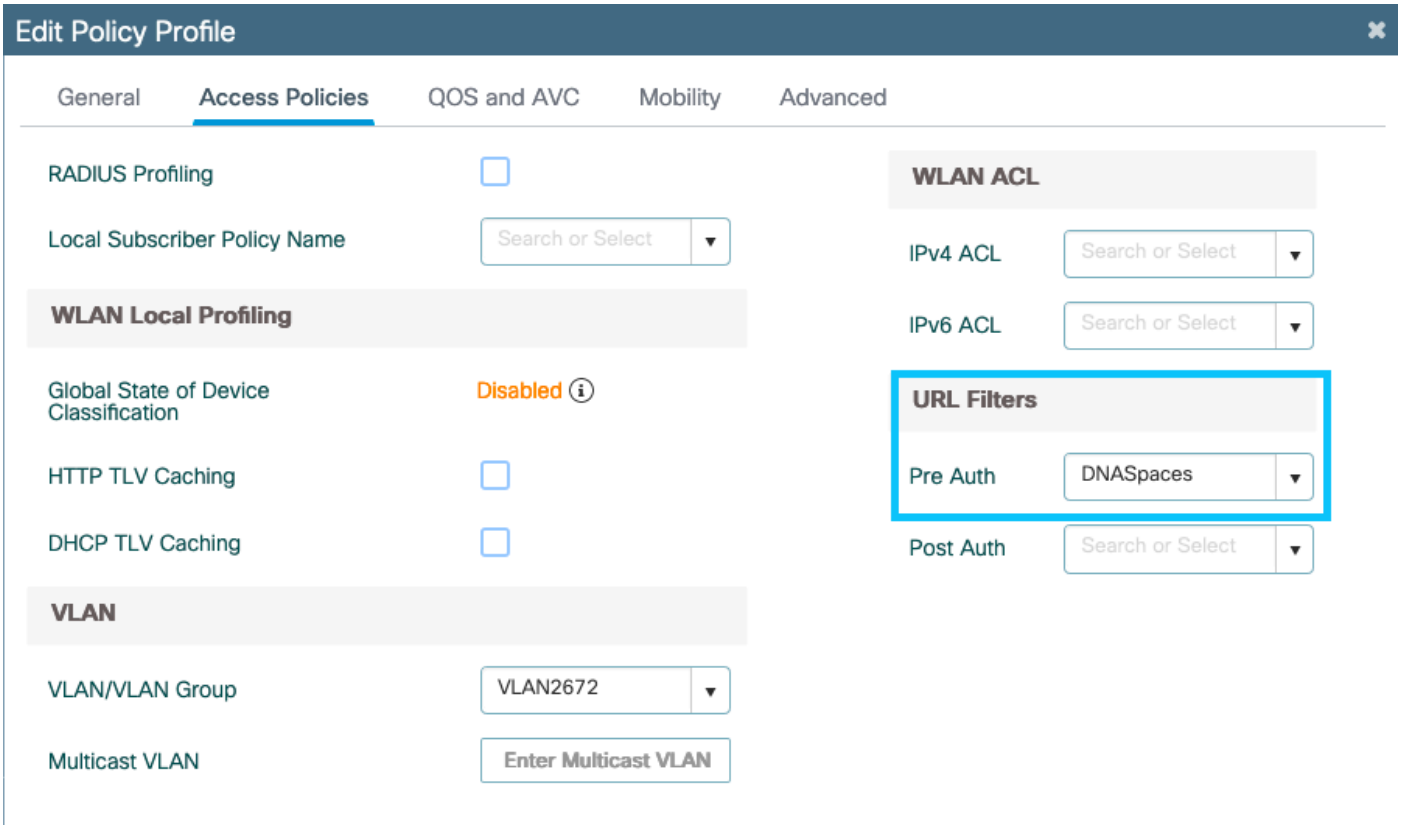


第三步：导航到**Security > Layer3。**启用Web策略，配置Web身份验证参数映射和身份验证列表。启用Mac过滤器失败并添加预身份验证ACL。单击**Apply to Device。**

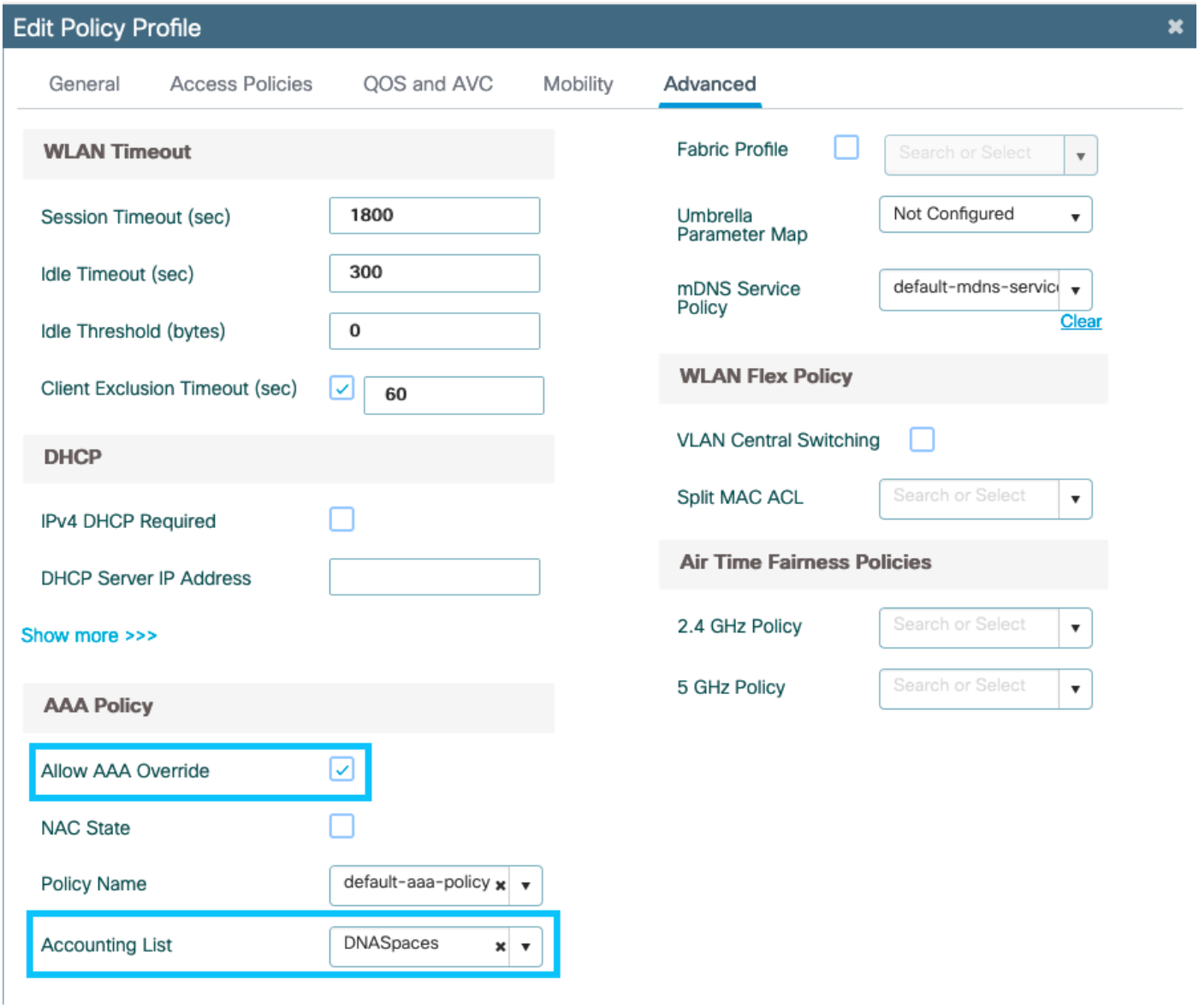


在9800控制器上配置策略配置文件

步骤1:导航到**Configuration > Tags & Profiles > Policy**，然后创建新的策略配置文件或使用默认策略配置文件。在访问策略(Policies)选项卡中，配置客户端VLAN并添加URL过滤器。

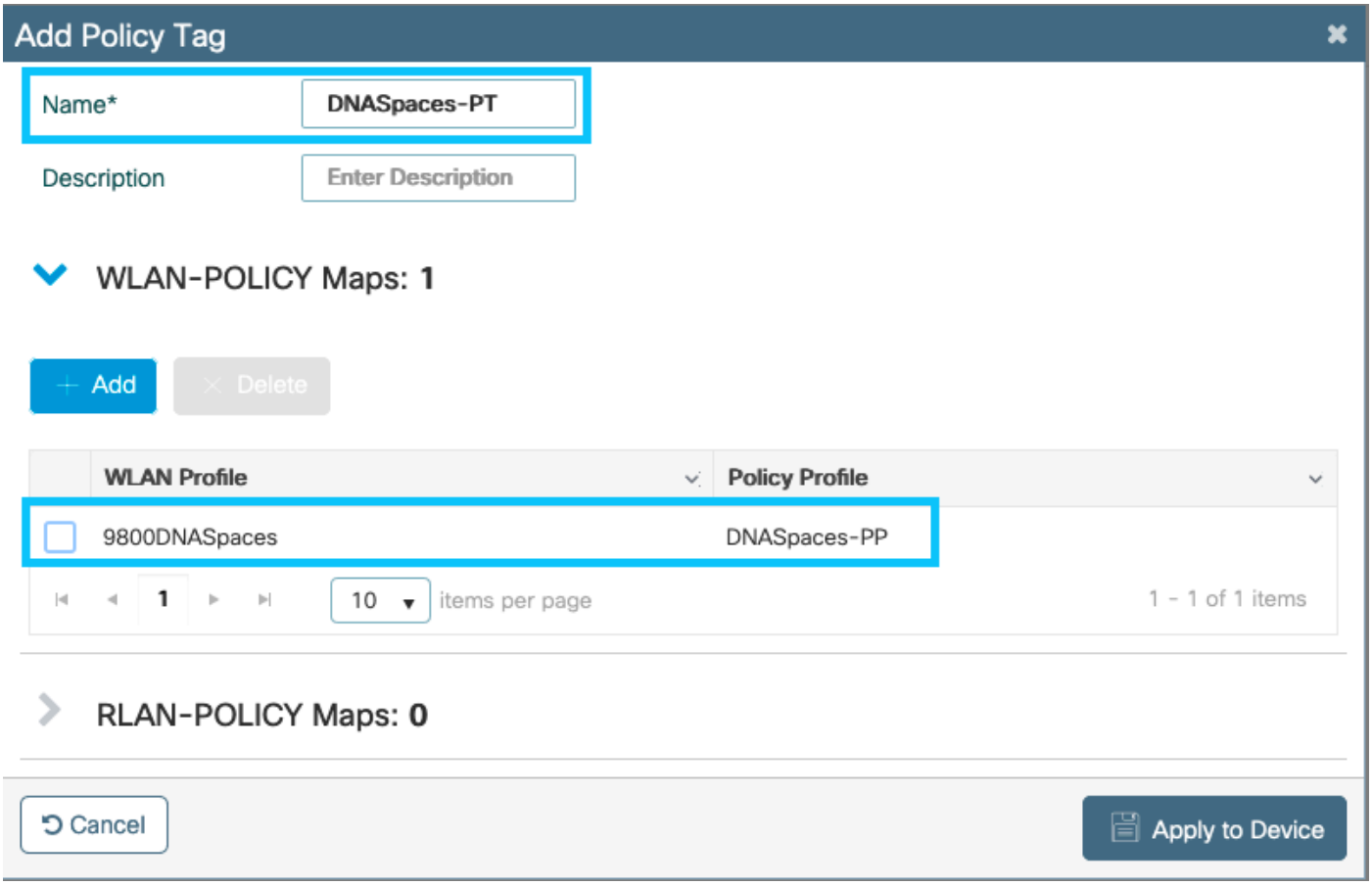


第二步：在Advanced选项卡中，启用AAA Override并选择性地配置记帐方法列表：

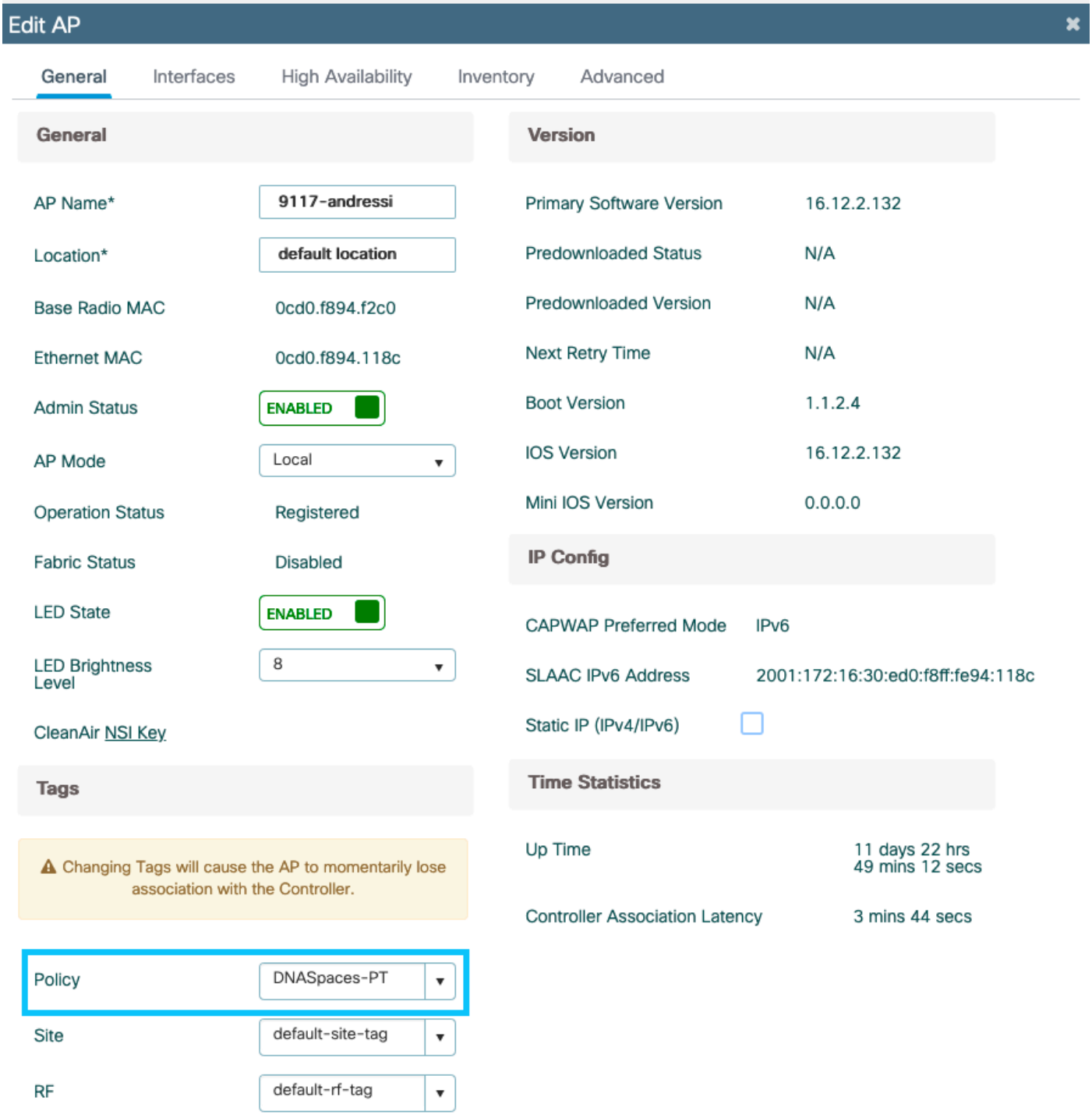


在9800控制器上配置策略标记

步骤1:导航到**配置>标记和配置文件>策略。**创建新的策略标记或使用默认策略标记。将WLAN映射到策略标记中的策略配置文件。



第二步：将策略标记应用于AP以广播SSID。导航到**Configuration > Wireless > Access Points**，选择有问题的AP并添加策略标记。这会导致AP重新启动其CAPWAP隧道并返回到9800控制器：



CLI 配置：

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

```
Andressi-9800L(config-wlan)#ip access-group web
```

```
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




Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth authentication-list




Andressi-9800L(config-wlan)#security web-auth on-macfilter-failure
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown

Andressi-9800L(config)#wireless profile policy




Andressi-9800L(config-wireless-policy)#aaa-override
Andressi-9800L(config-wireless-policy)#accounting-list




Andressi-9800L(config-wireless-policy)#vlan <id>
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter




Andressi-9800L(config-wireless-policy)#no shutdown

Andressi-9800L(config)#wireless tag policy




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

配置全局参数映射

不推荐的步骤：运行这些命令以允许HTTPS重定向，但是请注意，如果客户端操作系统执行强制网络门户检测并导致更严重的CPU使用率并始终抛出证书警告，则不需要在客户端HTTPS流量中重定向。因此，建议避免进行配置，除非需要特定使用案例。

```
Andressi-9800L(config)#parameter-map type webauth global
```

```
Andressi-9800L(config-params-parameter-map)#intercept-https-enable
```

注：您必须拥有适用于Cisco Catalyst 9800系列无线控制器中安装的虚拟IP的有效SSL证书。

步骤1:将扩展名为.p12的签名证书文件复制到TFTP服务器，并运行此命令以传输证书并将其安装到9800控制器：

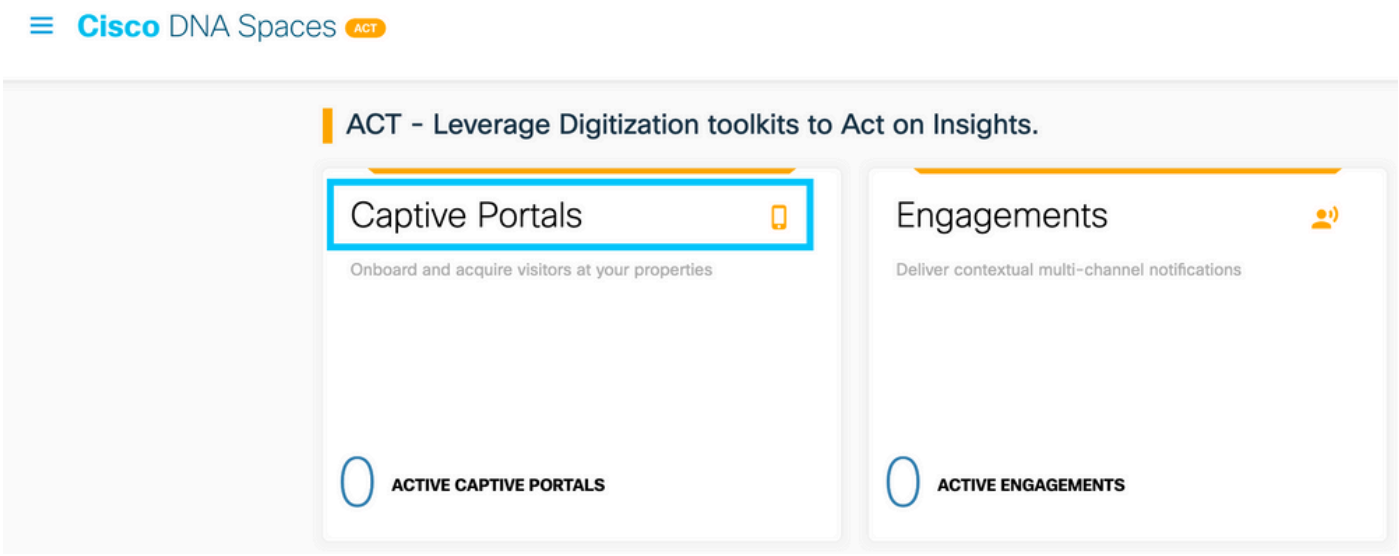
```
Andressi-9800L(config)#crypto pki import
```

第二步：要将已安装证书映射到Web身份验证参数映射，请运行以下命令：

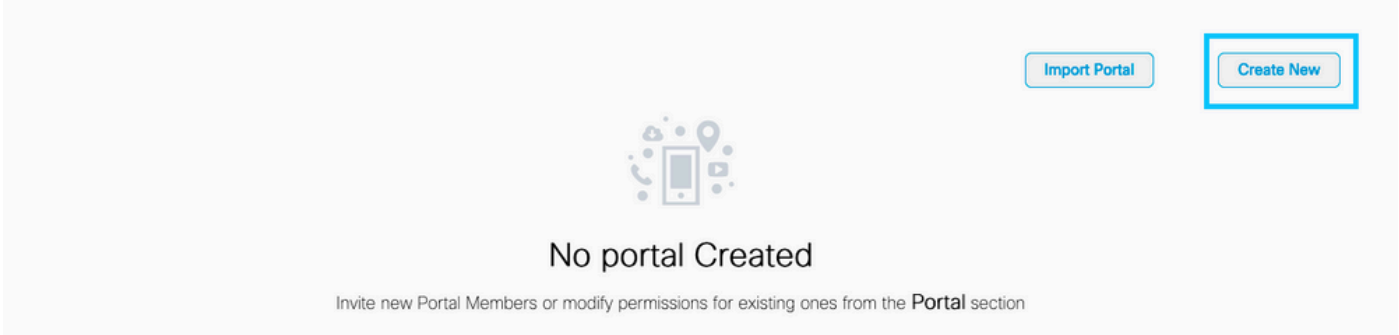
```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#trustpoint
```

在DNA空间上创建门户

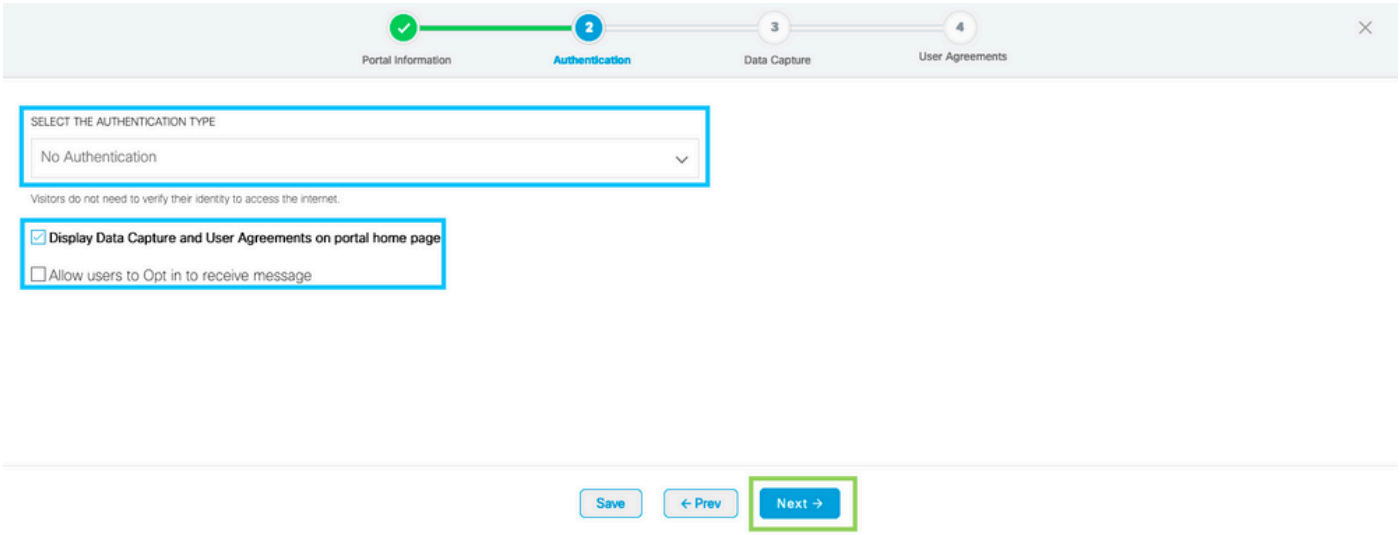
步骤1:点击DNA空间控制面板中的**强制网络门户**:



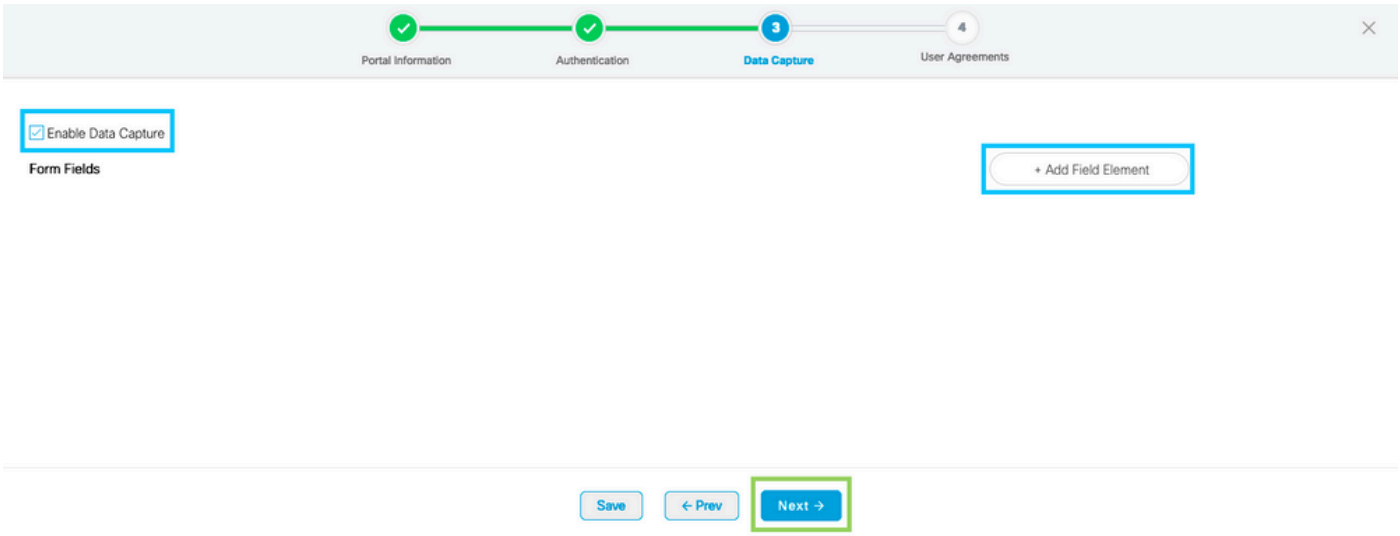
第二步：单击**Create New**，输入门户名称并选择可使用门户的位置：



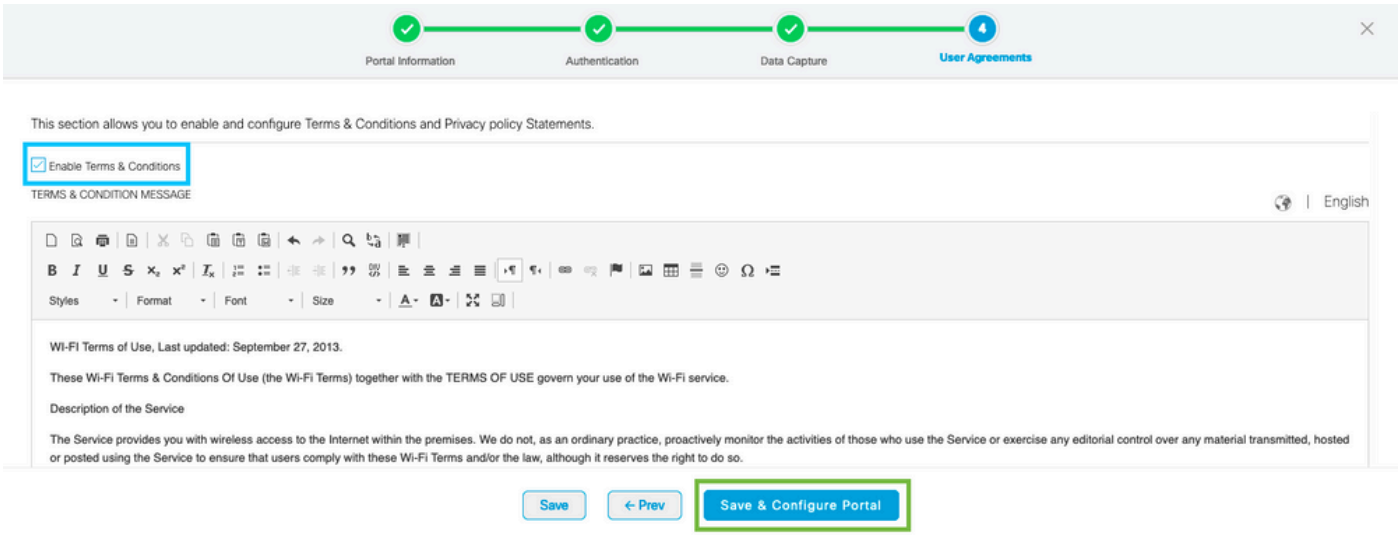
第三步：选择身份验证类型，选择是否要在门户主页上显示数据捕获和用户协议，以及是否允许用户选择接收消息。单击“下一步”：



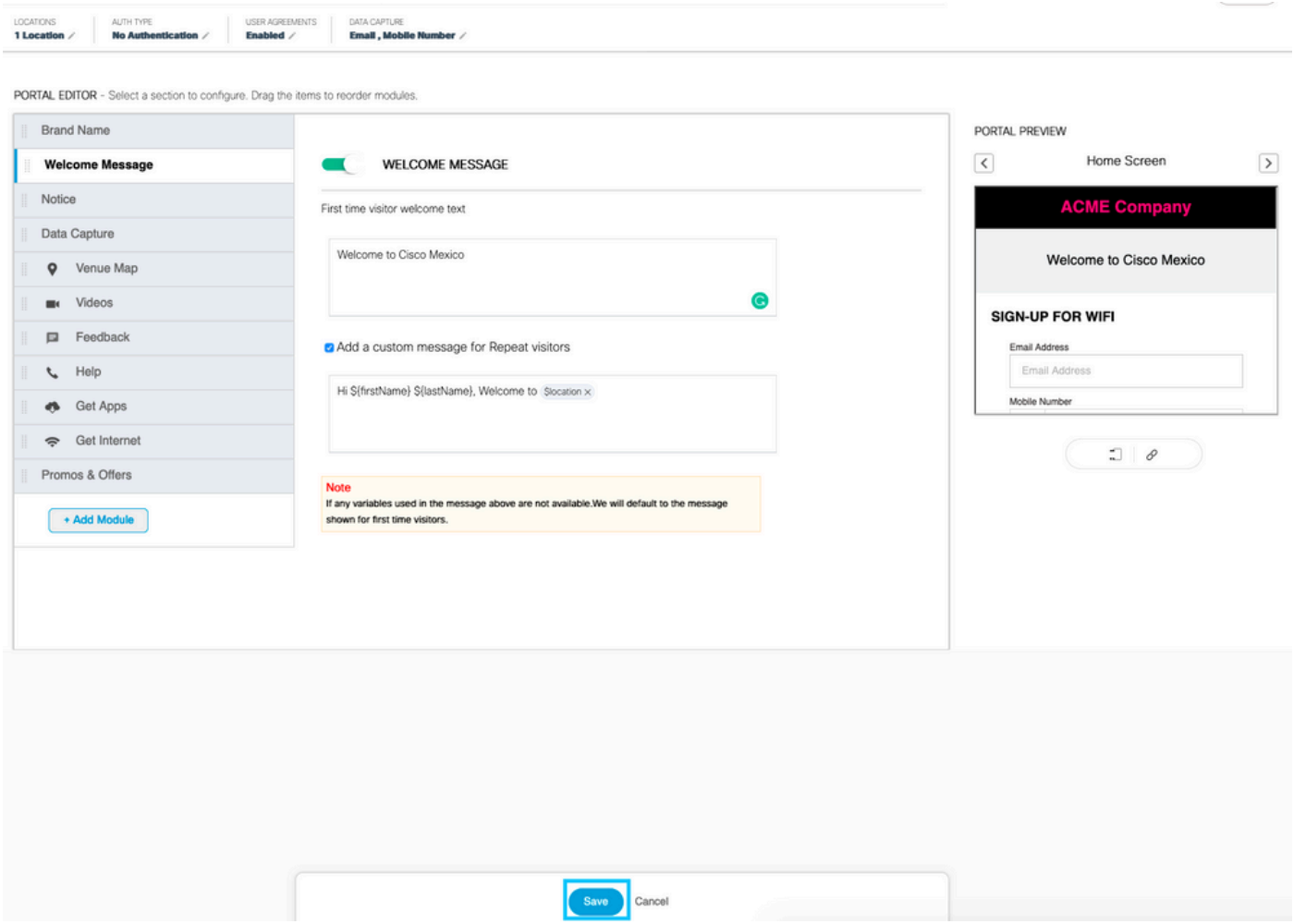
第四步：配置数据捕获元素。如果要捕获来自用户的数据，请选中**Enable Data Capture**框，然后单击**+Add Field Element**以添加所需的字段。单击“下一步”：



第五步：选中**Enable Terms & Conditions**，然后单击**Save & Configure Portal**:

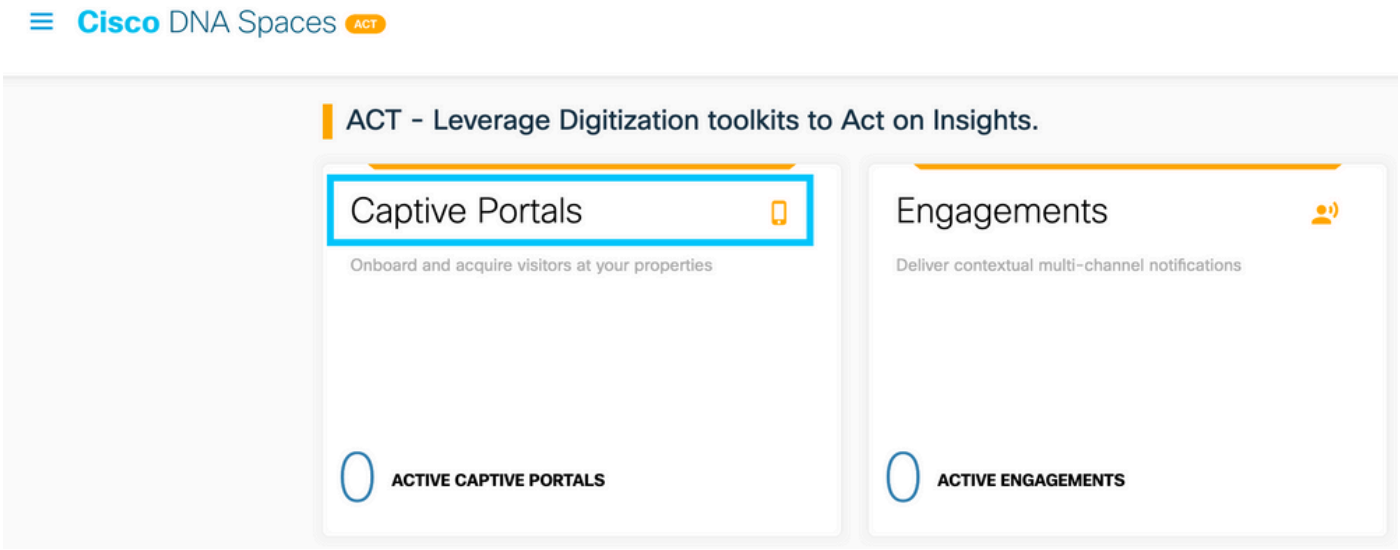


第六步：根据需要编辑门户，点击**保存**：

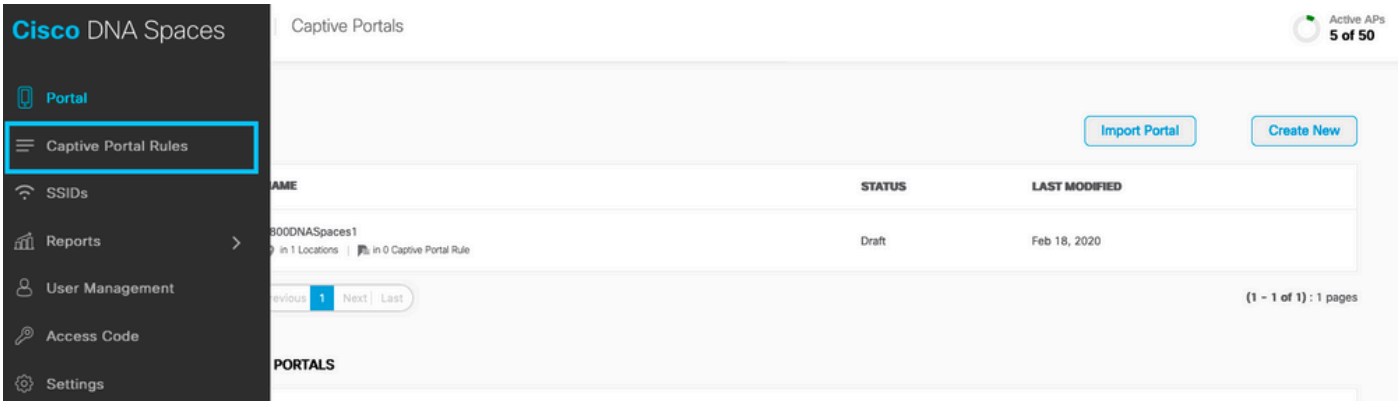


在DNA空间上配置强制网络门户规则

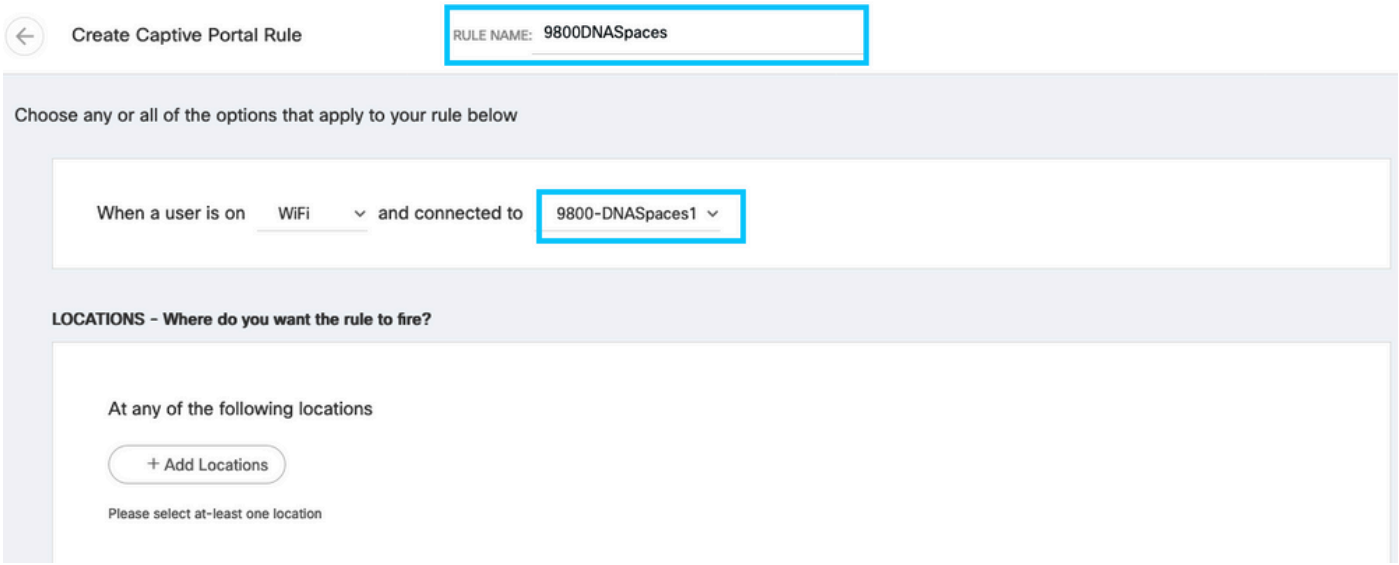
步骤1:点击DNA空间控制面板中的**强制网络门户**:



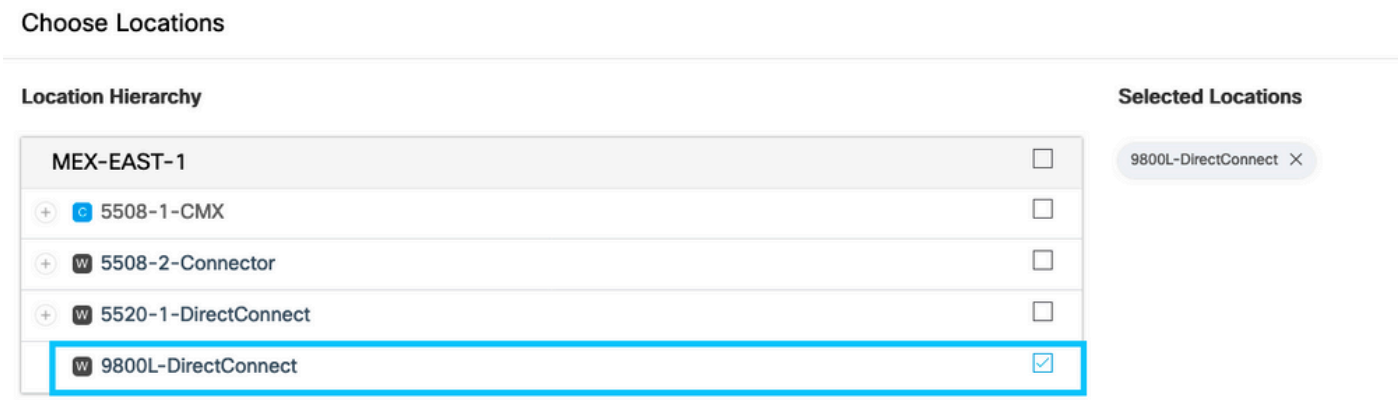
第二步：打开强制网络门户菜单，然后点击**强制网络门户规则：**



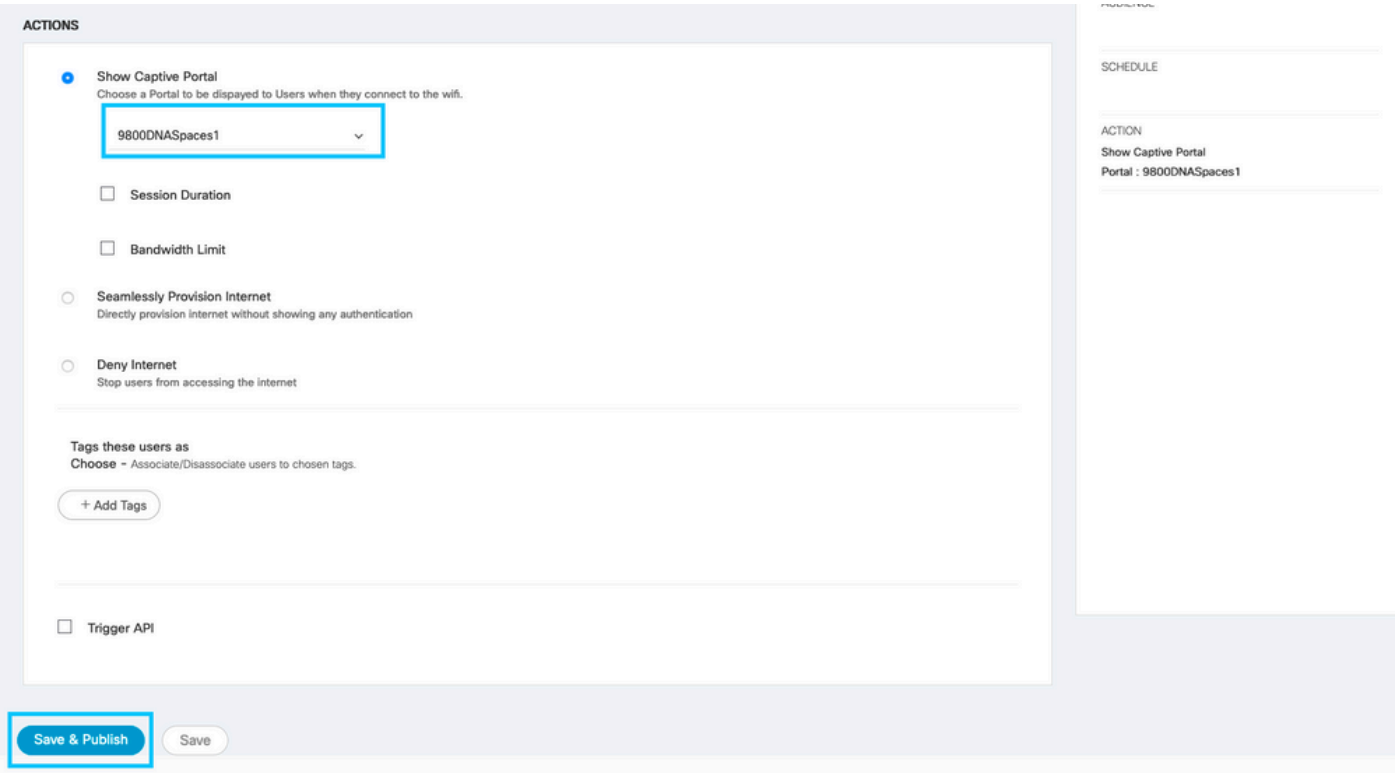
第三步：单击**+ Create New Rule**。输入规则名称，选择先前配置的SSID。



第四步：选择门户可用的位置。在**LOCATIONS**部分中单击**+**添加位置。从Location Hierarchy（位置层次结构）中选择所需的位置。



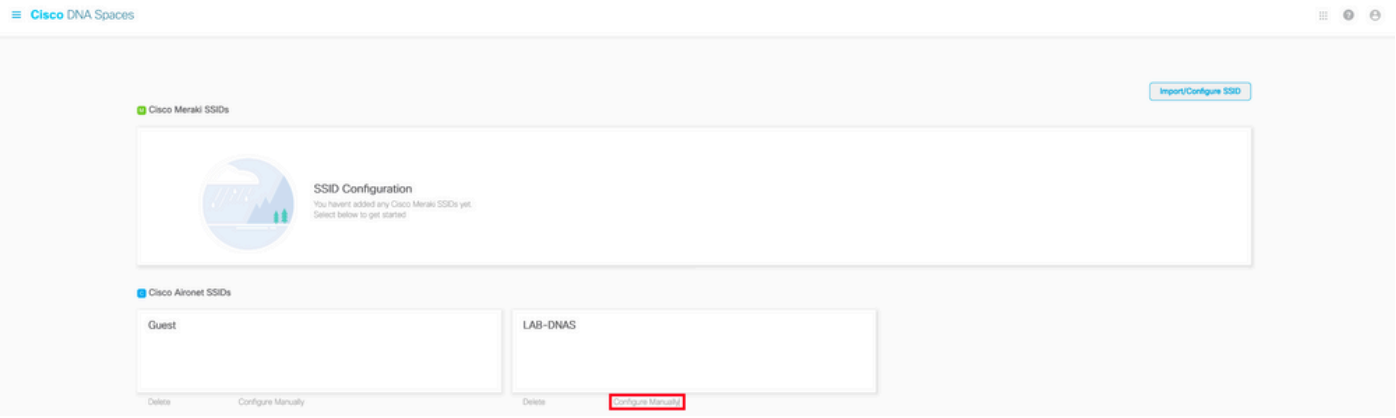
第五步：选择强制网络门户的操作。在这种情况下，当规则被命中时，将显示门户。单击**保存并发布**。



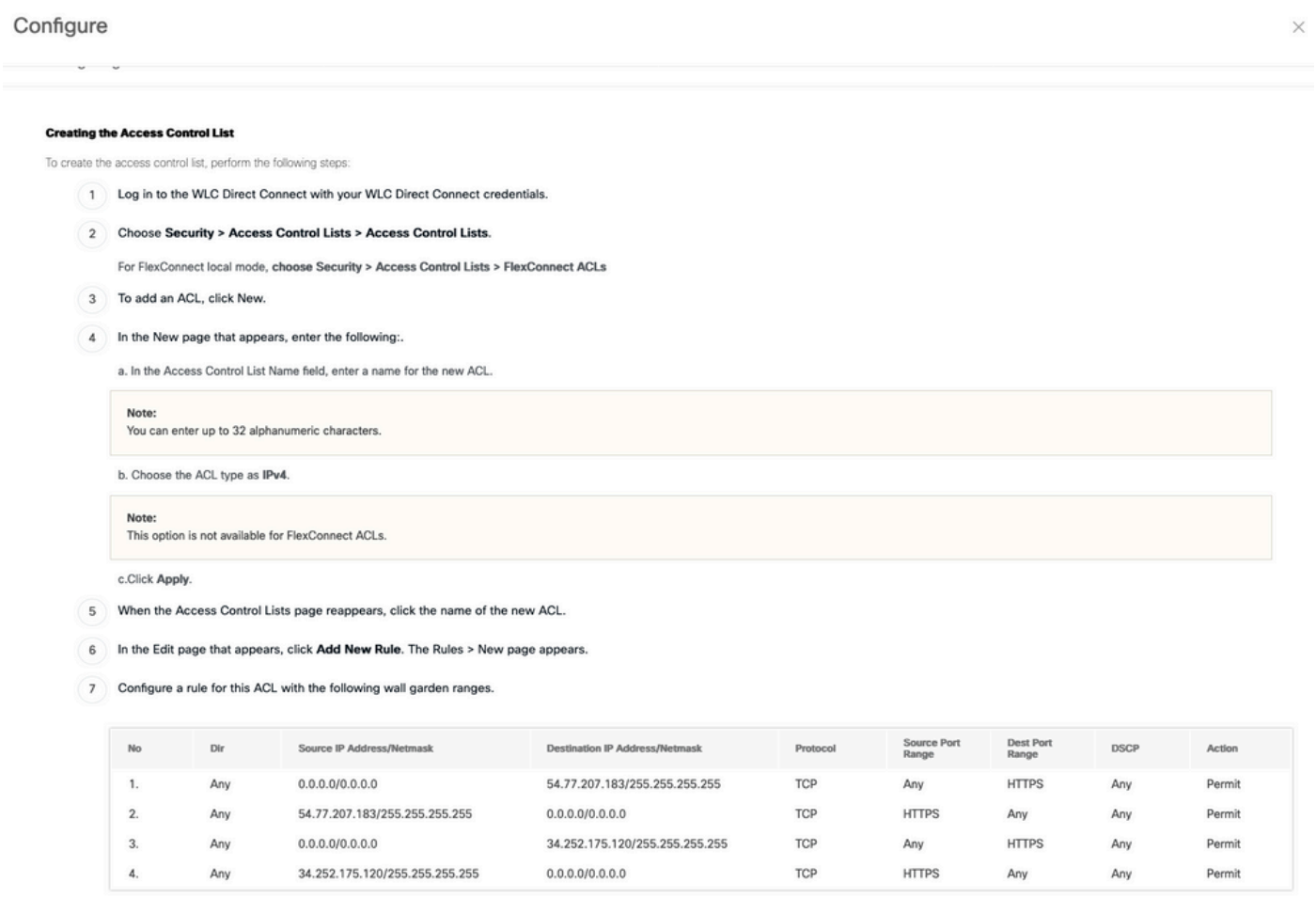
从DNA空间获取特定信息

DNA空间使用哪些IP地址？

要验证您所在区域的IP地址DNA空间用于门户的内容，请转到DNA空间主页上的Captival Portal页面。单击左侧菜单中的**SSID**，然后单击SSID下的**手动配置**。ACL示例中提到了IP地址。这些是用于ACL和webauth参数映射的门户的IP地址。DNA空间使用其他IP地址来实现控制平面的整体NMSP/云连接。



在出现的弹出窗口的第一部分中，步骤7显示了ACL定义中提到的IP地址。您不需要执行这些操作并创建任何ACL，只需记下IP地址即可。这些是您所在区域的门户所使用的IP



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**.

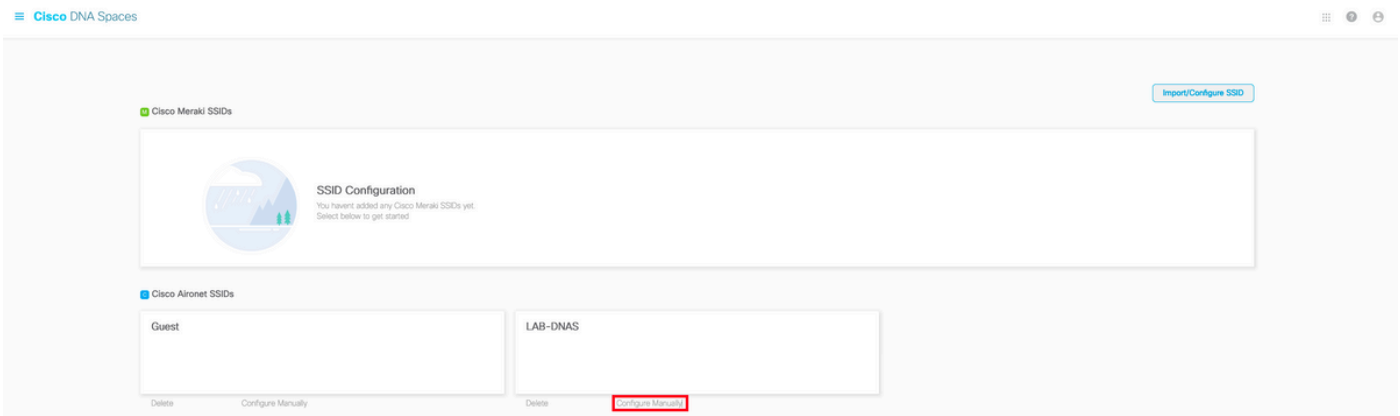
   Note:
   This option is not available for FlexConnect ACLs.

   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

DNA空间登录门户使用哪个URL?

要验证您所在地区的登录门户URL DNA空间用于该门户的内容，请转到DNA空间主页上的Captival门户页面。单击左侧菜单中的**SSID**，然后单击SSID下的**手动配置**。



在出现的弹出窗口中向下滚动，在第二部分中，步骤7显示必须在9800上的参数映射中配置的URL。

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.

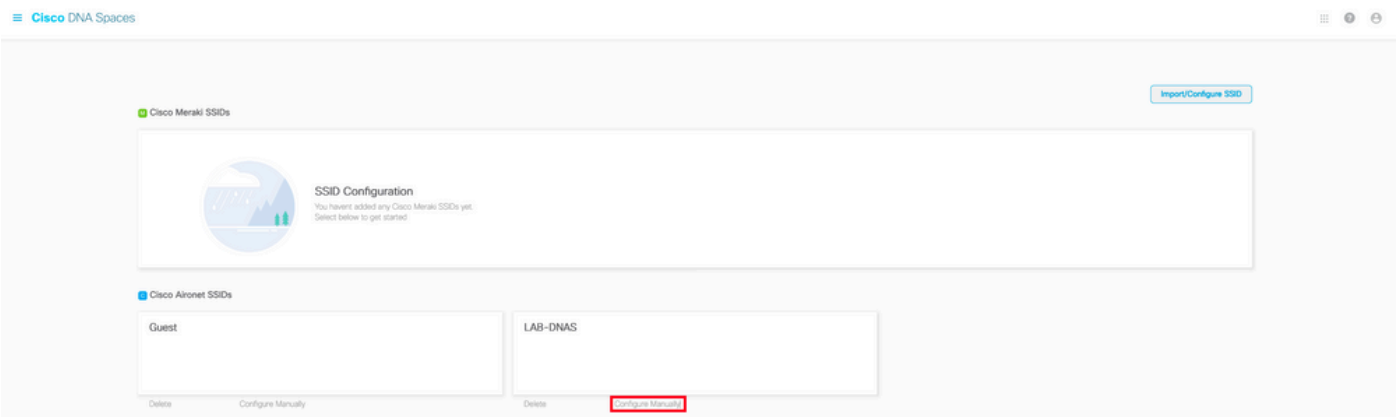
   f.From the Web Auth Type drop-down list, choose **External** .

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

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

DNA空间的RADIUS服务器详细信息是什么？

要了解您需要使用的RADIUS服务器IP地址以及共享密钥，请转到DNA Space主页上的Captival Portal页面。单击左侧菜单中的**SSID**，然后单击SSID下的**手动配置**。



在显示的弹出窗口中，向下滚动第3部分(RADIUS)，第7步为您提供IP/端口和用于RADIUS身份验证的共享密钥。记帐是可选的，在步骤12中介绍。

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**.

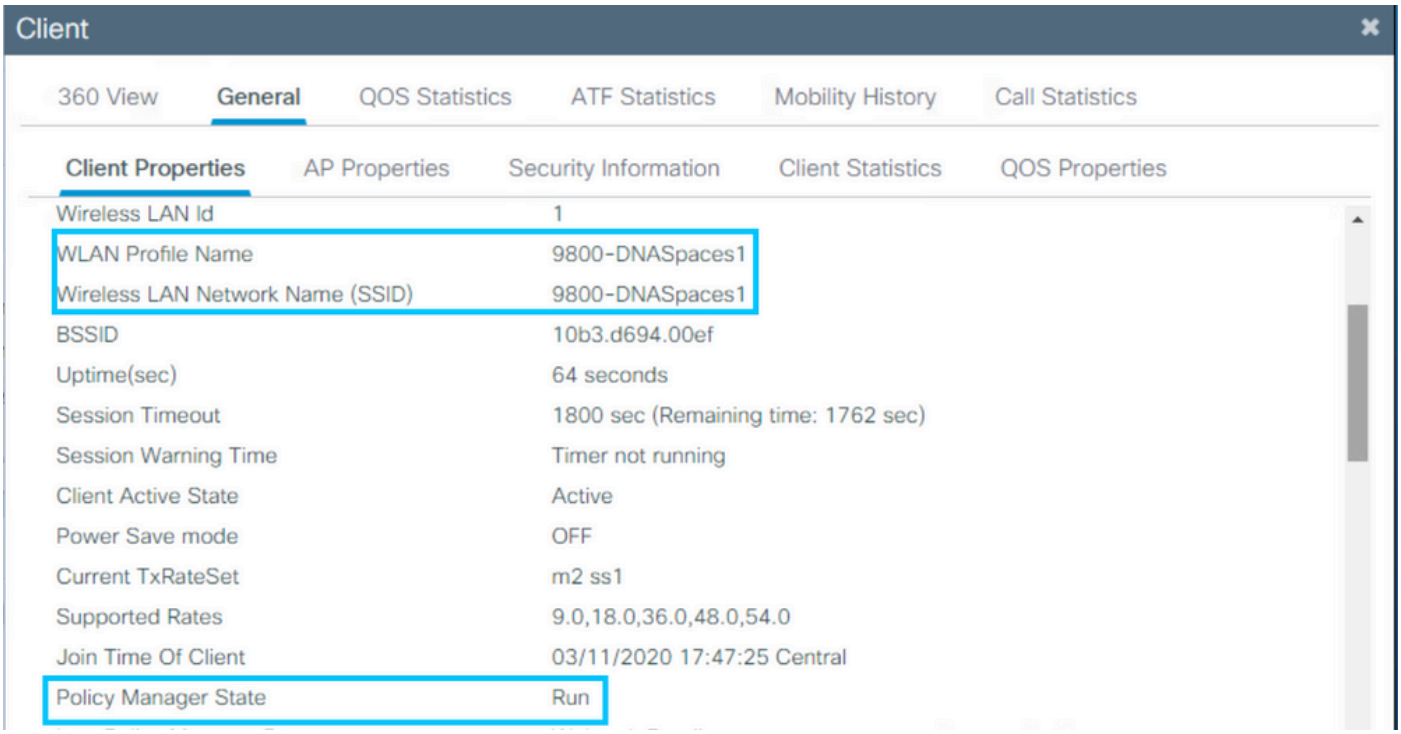
Host: 52.51.31.103,34.241.1.84

Port: 1813

Secret Key: emeab1299E2PqvUK

验证

要确认连接到SSID的客户端的状态，请导航到**Monitoring > Clients**，单击设备的MAC地址并查找Policy Manager State:



故障排除

常见问题

1.如果控制器上的虚拟接口未配置IP地址，客户端将被重定向到内部门户，而不是在参数映射中配置的重定向门户。

2.如果客户端在重定向到DNA空间上的门户时收到*503*错误，请确保在DNA空间上的**位置层次结构**中配置控制器。

永远在线跟踪

WLC 9800 提供无间断跟踪功能。这可确保持续记录所有客户端连接相关的错误、警告和通知级别消息，并且您可以在发生事故或故障情况后查看其日志。

> **注**：根据生成的日志量，您可以将时间从几个小时缩短到几天。

要查看9800 WLC默认收集的跟踪，可以通过SSH/Telnet连接到9800 WLC并执行这些步骤（确保您将会话记录到文本文件）。

步骤1:检查控制器当前时间，以便您可以在问题发生之前的时间跟踪日志。

```
# show clock
```

第二步：根据系统配置的指示，从控制器缓冲区或外部系统日志收集系统日志。这样可以快速查看系统运行状况和错误（如果有）。

```
# show logging
```

第三步：验证是否启用了任何调试条件。

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

> **注**：如果看到列出了任何条件，则意味着遇到启用条件（MAC地址、IP地址等）的所有进程的跟踪将记录到调试级别。这会增加日志量。因此，建议在非主动调试时清除所有条件

第四步：如果测试的mac地址未作为步骤3中的条件列出，请收集特定mac地址的始终在线通知级别跟踪。

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

您可以显示会话内容，也可以将文件复制到外部 TFTP 服务器。

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

条件调试和无线电主动跟踪

如果永远在线(always-on)跟踪不能为您提供足够的信息来确定所调查问题的触发器，则可以启用条件调试并捕获无线活动(RA)跟踪，该跟踪为与指定条件（本例中为客户端MAC地址）交互的所有进程提供调试级别跟踪。要启用条件调试，请执行以下步骤。

步骤1:确保未启用调试条件。

```
# clear platform condition all
```

第二步：为要监控的无线客户端MAC地址启用调试条件。

这些命令用于开始监控所提供的 MAC 地址，持续 30 分钟（1800 秒）。您可以选择延长监控时间，最多监控 2085978494 秒。

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

> **注**:**要一次监控多个客户端，请对每个mac地址运行debug wireless mac <aaaa.bbbb.cccc>命令。**
>
> **注意**:您不会在终端会话上看到客户端活动的输出，因为所有内容都在内部缓冲，供以后查看。

第三步：重现要监控的问题或行为。

第四步：如果在默认或配置的监控器时间开启之前重现问题，则停止调试。

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

监控时间结束或无线网络调试停止后，9800 WLC 会生成一个本地文件，其名称为：

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

第五步： 收集 MAC 地址活动的文件。 您可以将 ra trace.log 复制到外部服务器，也可以直接在屏幕上显示输出。

检查RA跟踪文件的名称

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

将文件复制到外部服务器：

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```

显示内容：

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

第六步：如果根本原因仍不明显，请收集内部日志，这些日志是调试级别日志的更详细视图。您无需再次调试客户端，因为我们只需进一步详细查看已收集并内部存储的调试日志。

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

> **注意**：此命令输出返回所有进程的所有日志记录级别的跟踪，而且数量相当大。在解析跟踪信息时如需帮助，请联系 Cisco TAC。

您可以将 ra-internal-FILENAME.txt 复制到外部服务器，也可以直接在屏幕上显示输出。

将文件复制到外部服务器：

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

显示内容：

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

步骤 7.删除调试条件。

```
# clear platform condition all
```

> **注意**：请确保在故障排除会话后始终删除调试条件。

成功尝试的示例

这是RA_trace的输出，表示在连接到没有RADIUS服务器的SSID时，在关联/身份验证过程中成功尝试识别每个阶段。

802.11关联/身份验证：

```
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-PP, AP Name: 2802AP-9800L, Ap Mac Address: 10b3.d694.00e0 BSSID MAC0000.0000.0000 wlan
ID: 1RSSI: 0, SNR: 32
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_STATUS: DOT11_STATUS_SUCCESS
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学习过程：

```
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
```

第3层身份验证：

```
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 state
[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
[10.10.30.42] dst [13.107.4.52] url [http://www.msftconnecttest.com/connecttest.txt]
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-
agent = Microsoft NCSI
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in
LOGIN state
[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
[10.10.30.42] dst [151.101.24.81] url [http://www.bbc.com/]
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-
agent = Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]POST rcvd when in
LOGIN state
```

第3层身份验证成功，将客户端移至RUN状态：

```
[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
(9800DNASpaces) for device with MAC: 34e1.2d23.a668
Managed client RUN state notification: 34e1.2d23.a668
Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RU
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。