带AireOS控制器的DNA空间强制网络门户配置示例

目录

简介

本文档介绍如何使用Cisco DNA Spaces和AireOS控制器配置强制网络门户。

作者：Andres Silva Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 对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：

- 5520无线LAN控制器版本8.10.112.0

配置

网络图

配置

将WLC连接到思科DNA空间

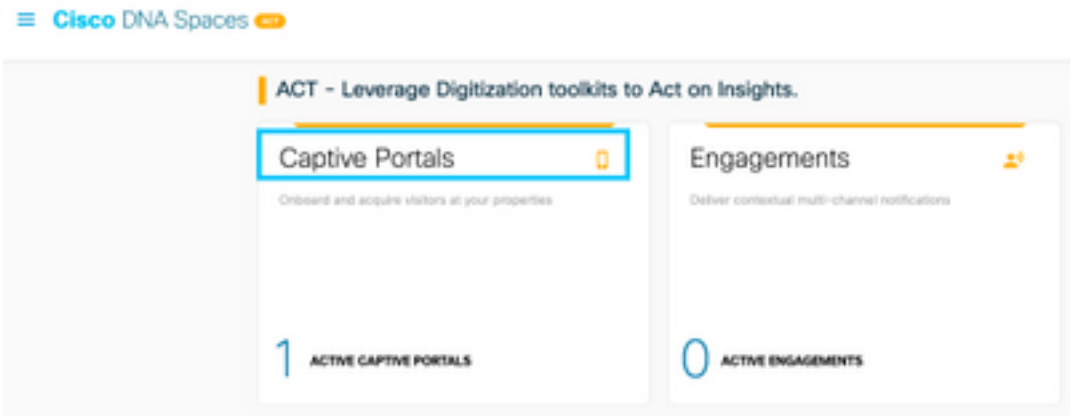
控制器需要使用任何可用的设置（直接连接）、通过DNA空间连接器或使用CMX Tethering连接到DNA空间。

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。

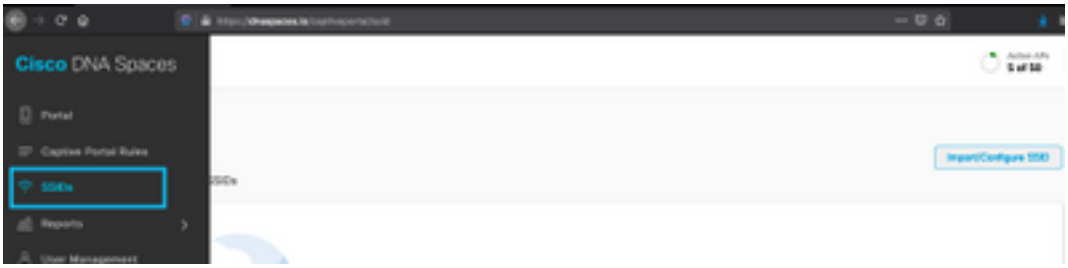
要将控制器连接到思科DNA空间，它必须能够通过HTTPS访问思科DNA空间云。有关如何将控制器连接到DNA空间的更多信息，请参阅以下链接：DNA空间直接连接配置示例

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：单击页面左上角的三行图标打开强制网络门户菜单，然后单击**SSID:**



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

控制器上的ACL配置

由于这是Web身份验证SSID，因此需要预身份验证ACL。当无线设备连接到SSID并收到IP地址时，设备的策略管理器状态将变为**Webauth_Reqd**状态，并且ACL将应用于客户端会话，以限制设备可以访问的资源。

步骤1:导航到**安全>访问控制列表>访问控制列表**，单击**新建**并配置规则以允许无线客户端之间到DNA空间的通信，如下所示。使用所用帐户的DNA空间提供的IP地址替换：

General

Access List Name: DNASpaces-ACL

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	34.235.248.212 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
2	Permit	34.235.248.212 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	52.55.235.39 / 255.255.255.255	Any	Any	Any	Any	Any	0
4	Permit	52.55.235.39 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

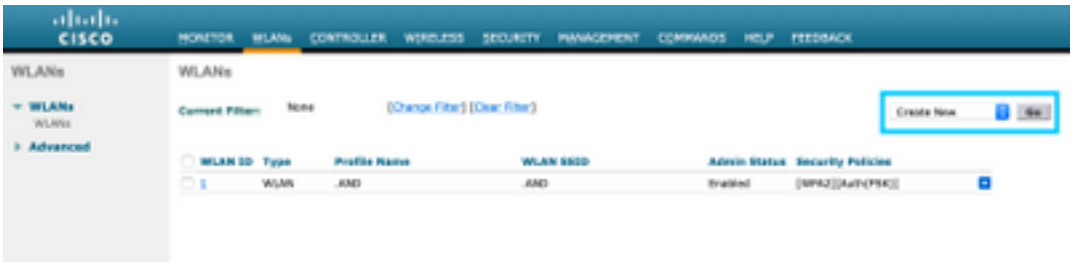
注：要获取ACL中允许的DNA空间的IP地址，请在ACL配置部分下的**在DNA空间上创建SSID部分**的第3步中创建的SSID中单击**Configure Manually**选项。

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。

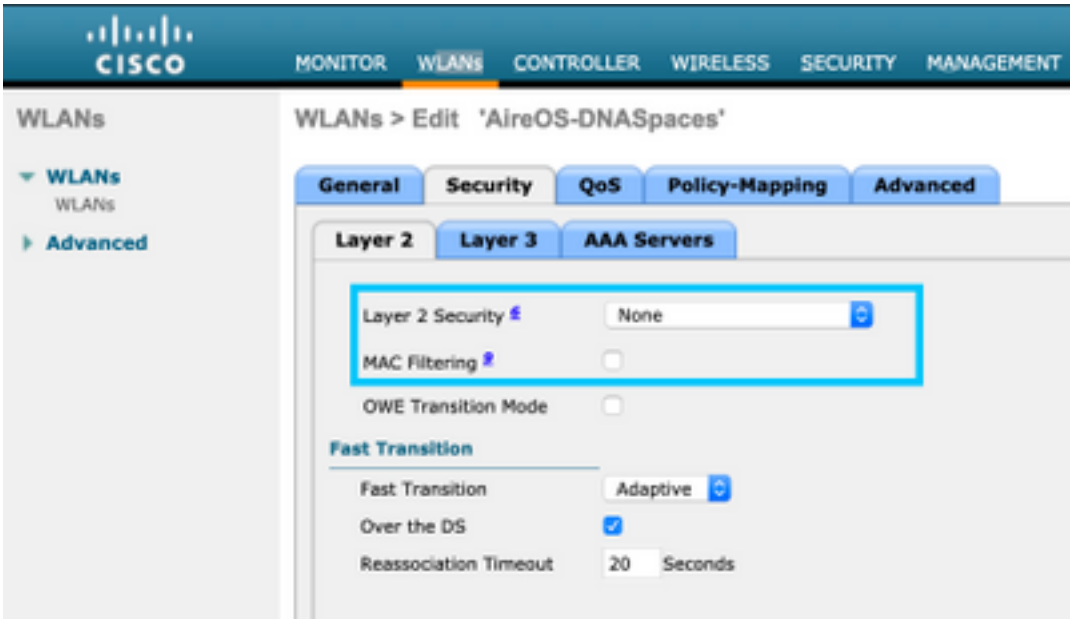
DNA空间上没有RADIUS服务器的强制网络门户

控制器上的SSID配置

步骤1:导航到**WLAN > WLANs。**创建新的WLAN。配置配置文件名称和SSID。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：配置第2层安全性。导航到WLAN Configuration选项卡中的**Security > Layer 2**选项卡，然后从Layer 2 Security的下拉菜单中选择**None。**确保MAC过滤已禁用。



第三步：配置第3层安全性。导航到WLAN configuration选项卡中的Security > Layer 3选项卡，将Web **Policy配置为第3层安全方法，Enable Passthrough，配置预身份验证ACL，启用Override Global Config**，将**Web Auth Type**设置为**External，**配置Redirect URL。

注：要获取重定向URL，请点击**Configure Manually**选项，该选项位于SSID配置部分下**Create the SSID on DNA Spaces第3步中创建的SSID**中。

在DNA空间上具有RADIUS服务器的强制网络门户

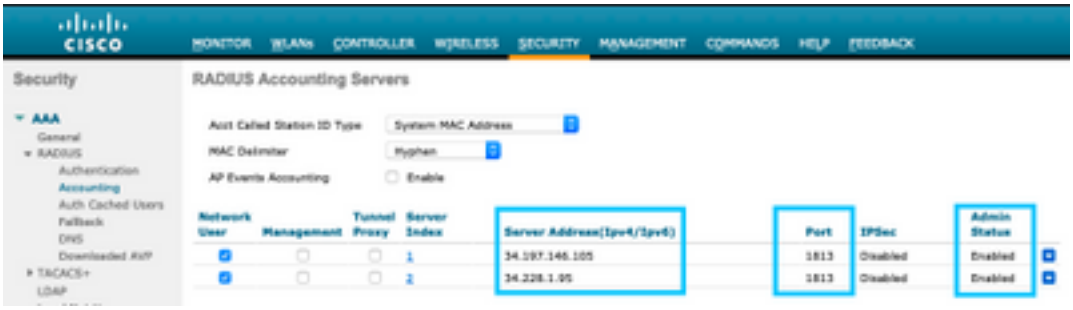
注意:DNA空间RADIUS服务器仅支持来自控制器的PAP身份验证。

控制器上的RADIUS服务器配置

步骤1:导航到**安全> AAA > RADIUS >身份验证**，单击**新建**并输入RADIUS服务器信息。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。配置两台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。**

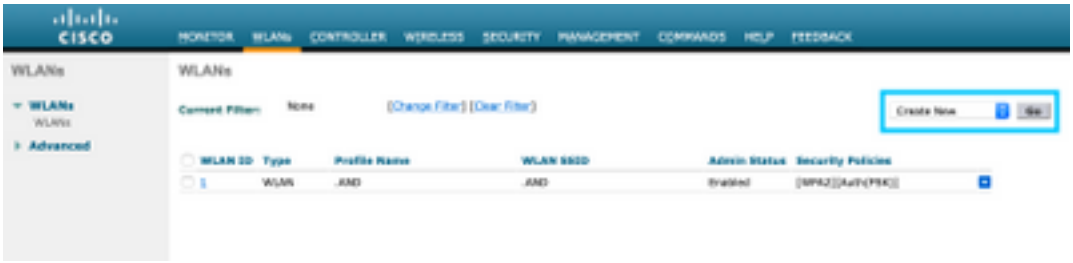
第二步：配置记帐RADIUS服务器。导航到**Security > AAA > RADIUS > Accounting**，然后单击**New**。配置相同的两台RADIUS服务器：



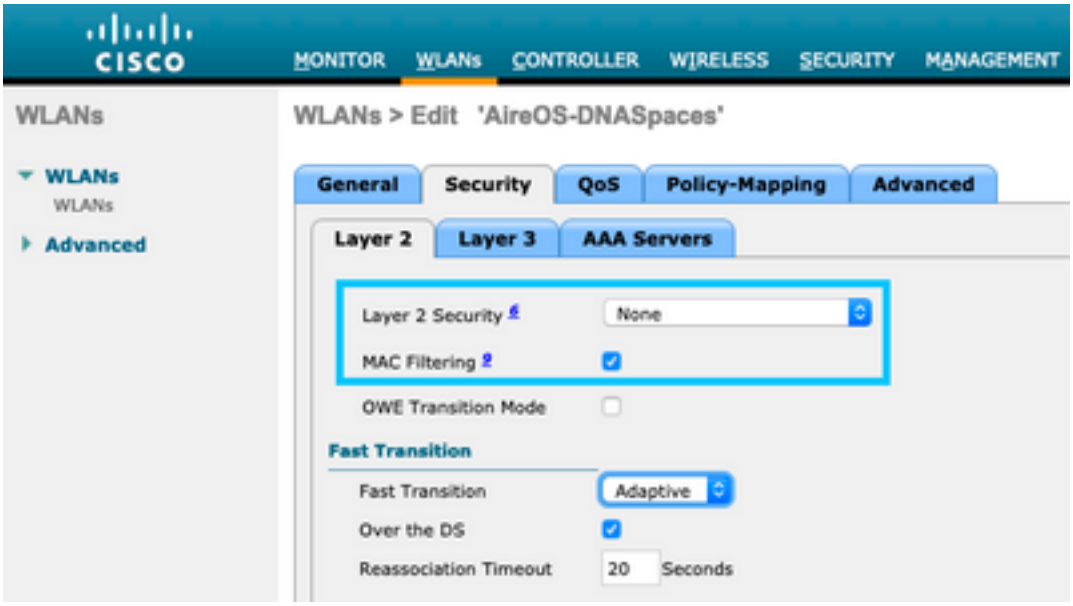
控制器上的SSID配置

> **重要**信息：在开始配置SSID之前，请确保在Controller > General下将**Web Radius** Authentication设置为“PAP”。

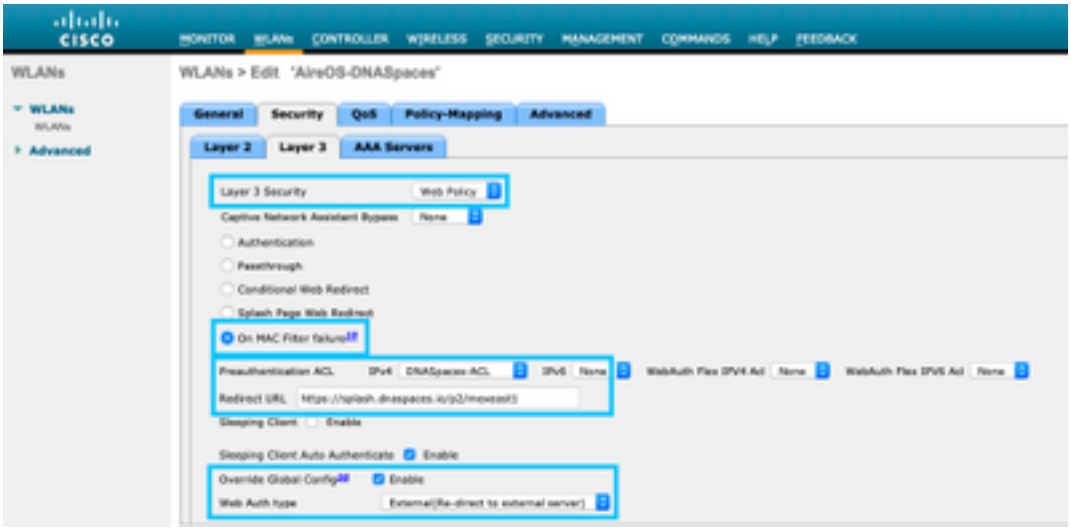
步骤1:导航到**WLAN > WLANs。**创建新的WLAN。配置配置文件名称和SSID。确保SSID名称与**在DNA空间上创建SSID**部分步骤3中配置的名称相同。



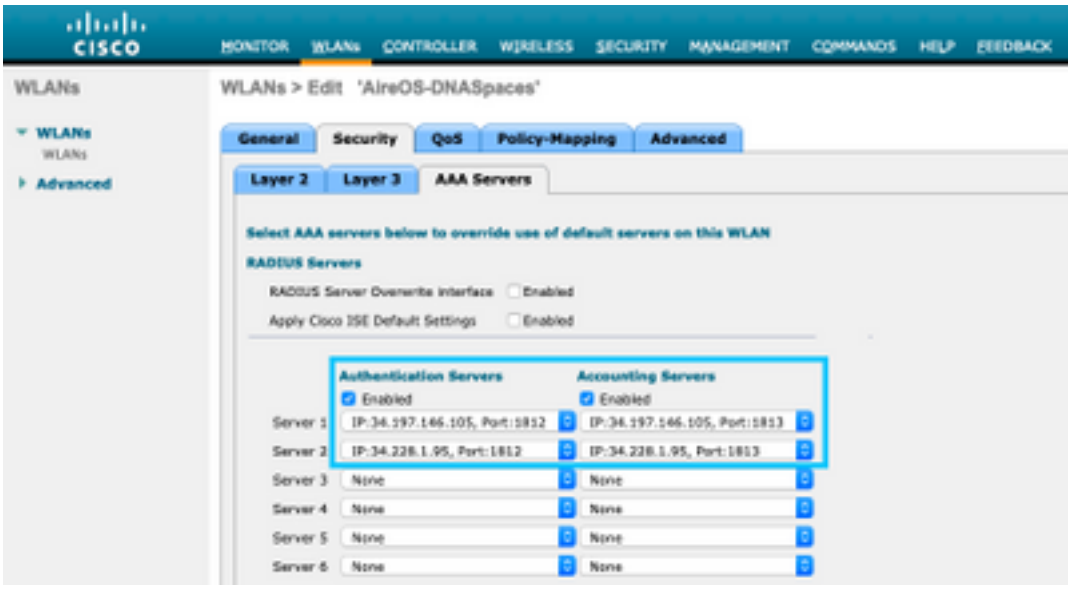
第二步：配置第2层安全性。导航到WLAN Configuration选项卡中的**Security > Layer 2**选项卡。将第2层安全配置为**None**。启用Mac过滤。



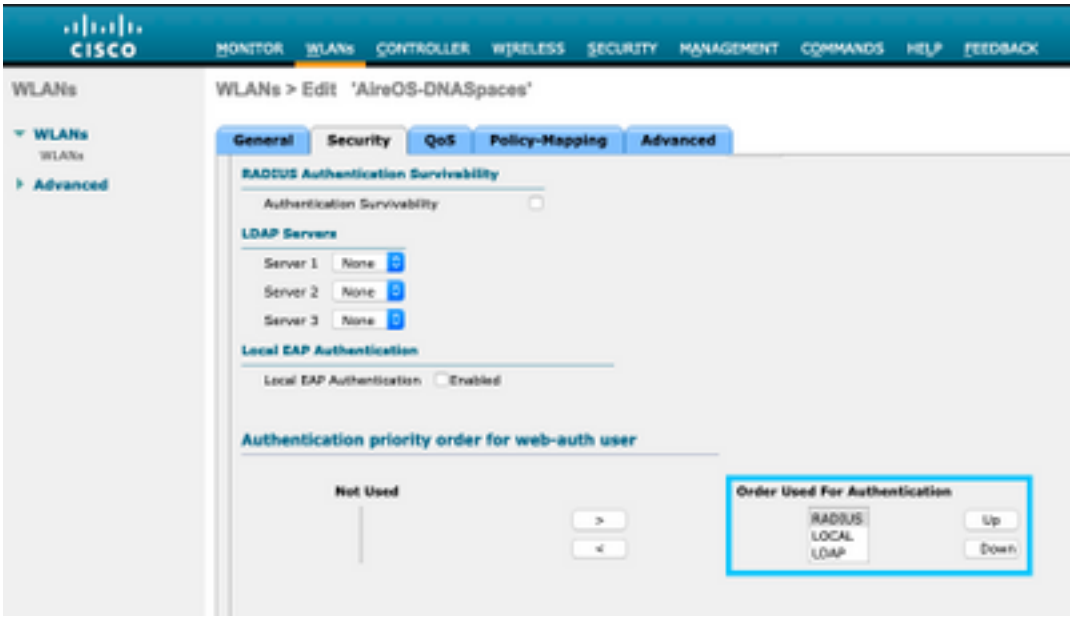
第三步：配置第3层安全性。导航到WLAN configuration选项卡中的Security > Layer 3选项卡，将Web **Policy配置为第3层安全方法，Enable On Mac Filter failure，配置预身份验证ACL，启用Override Global Config**，将**Web Auth Type设置为External，配置Redirect URL。**



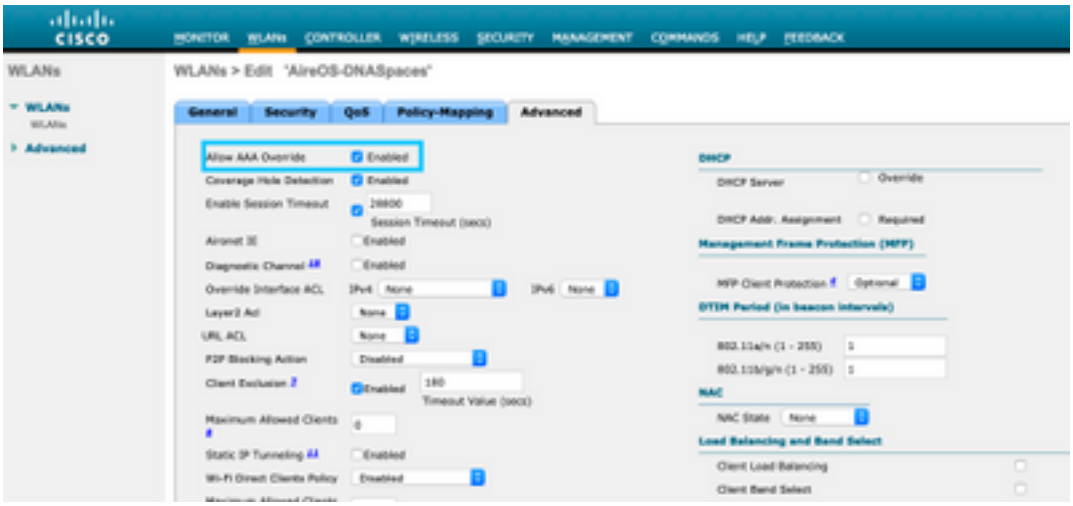
第四步：配置AAA服务器。导航到WLAN configuration选项卡中的**Security > AAA Servers**选项卡，启用**Authentication Servers**和**Accounting Servers**，然后从下拉菜单中选择两个RADIUS服务器：



第六步：配置Web-auth**用户的身份验证优先级顺序**。导航到WLAN configuration选项卡中的**Security > AAA Servers**选项卡，并将RADIUS设置为顺序中的第一个。

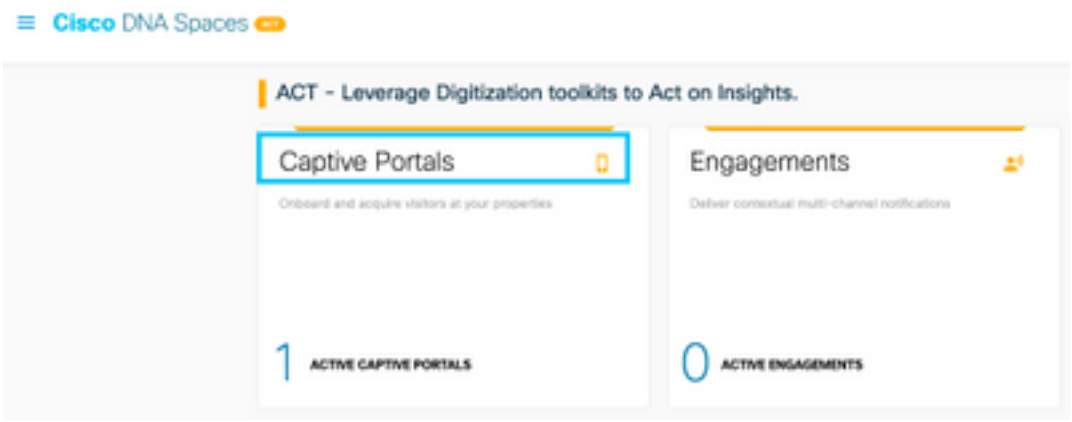


步骤 7.导航到WLAN配置选项卡中的**Advanced**选项卡，并启用**Allow AAA Override**。

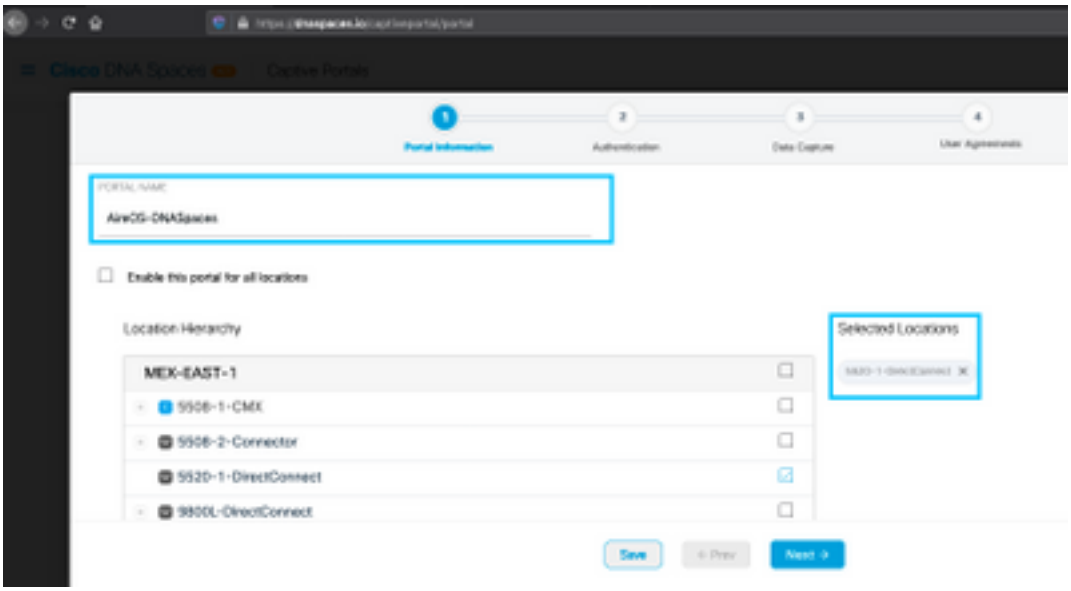


在DNA空间上创建门户

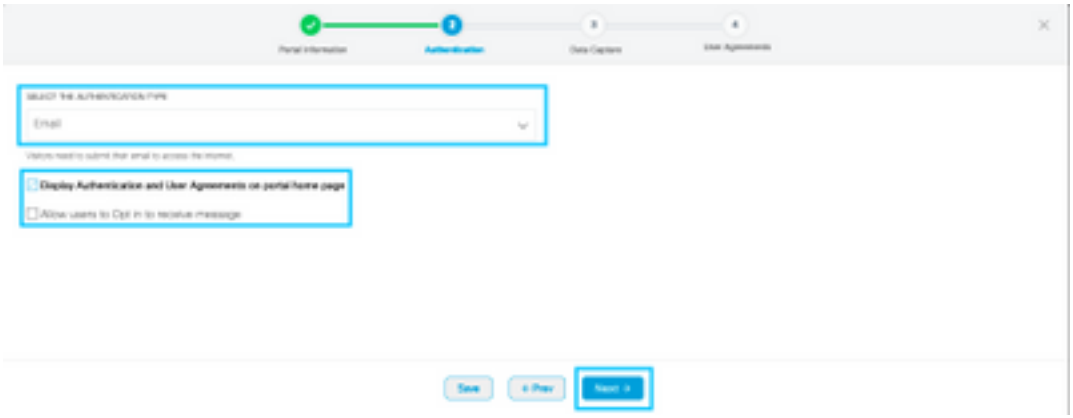
步骤1:点击DNA空间控制面板中的**强制网络门户**:



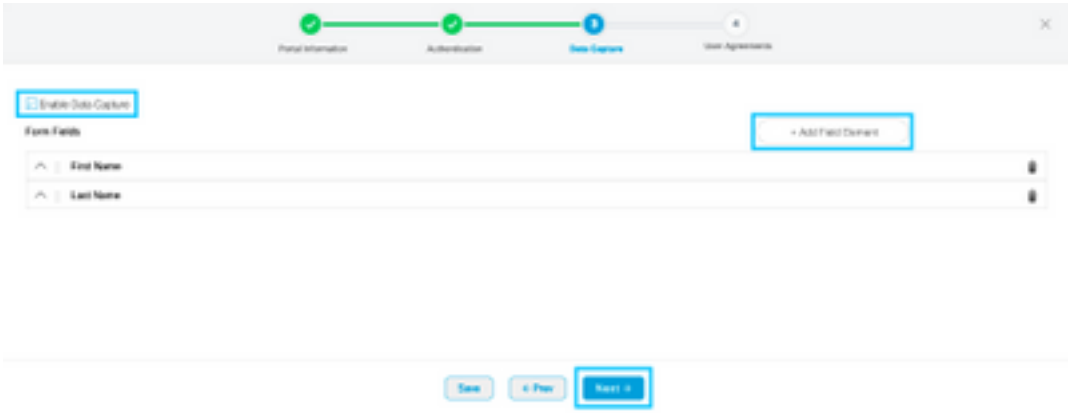
第二步：点击**Create New**，输入门户名称，并选择可使用门户的位置：



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”:

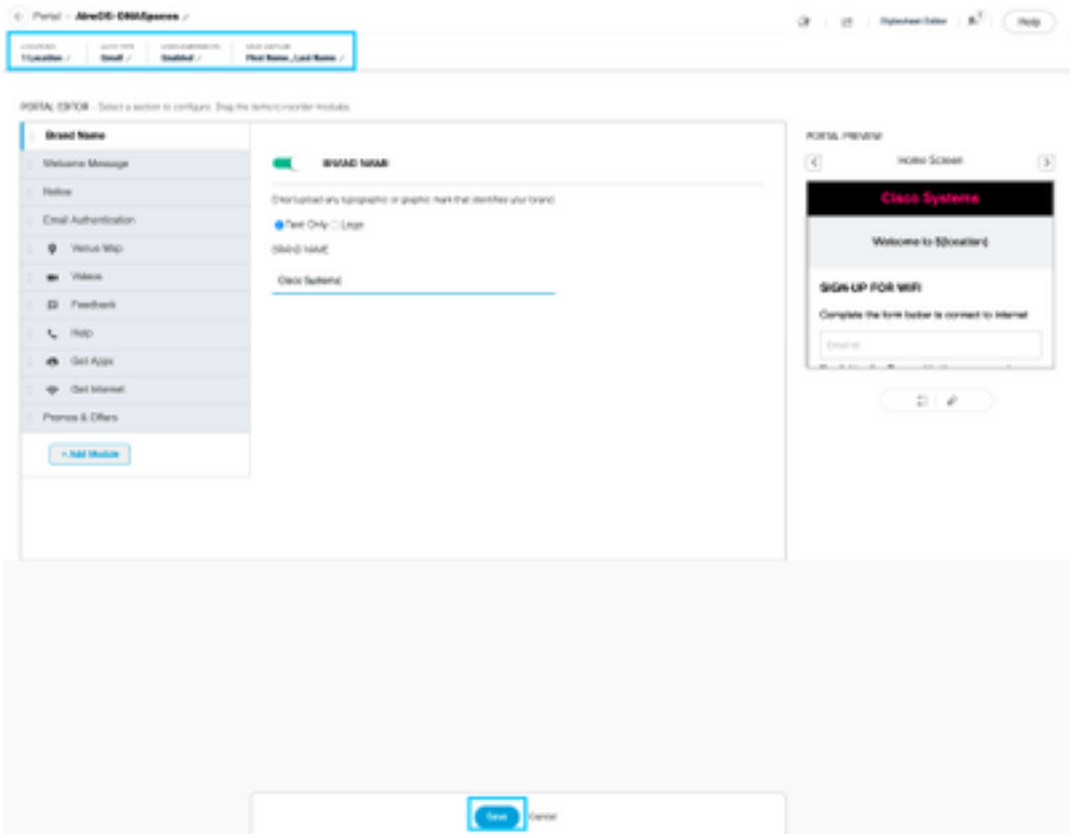


第四步：配置数据捕获元素。如果要捕获来自用户的数据，请选中**Enable Data Capture**框，然后单击**+Add Field Element**以添加所需的字段。单击“下一步”：



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

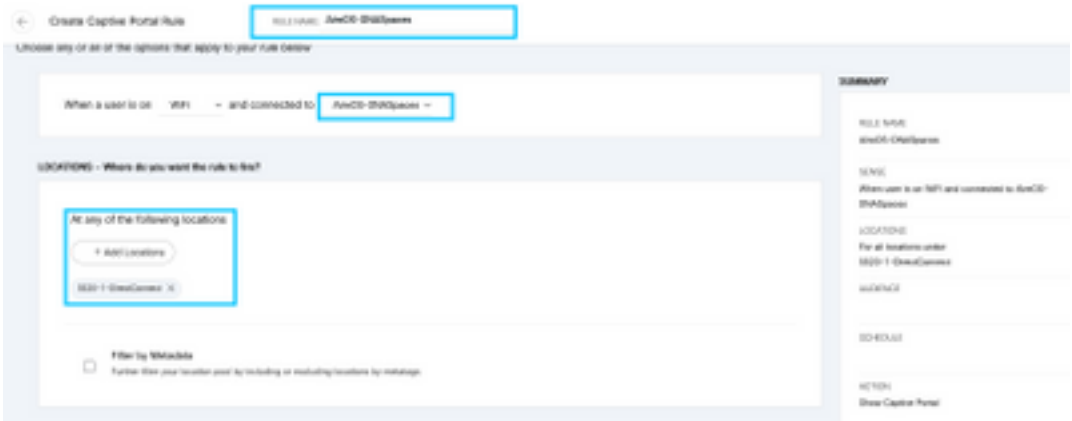
第六步：根据需要编辑门户，点击**保存：**



在DNA空间上配置强制网络门户规则

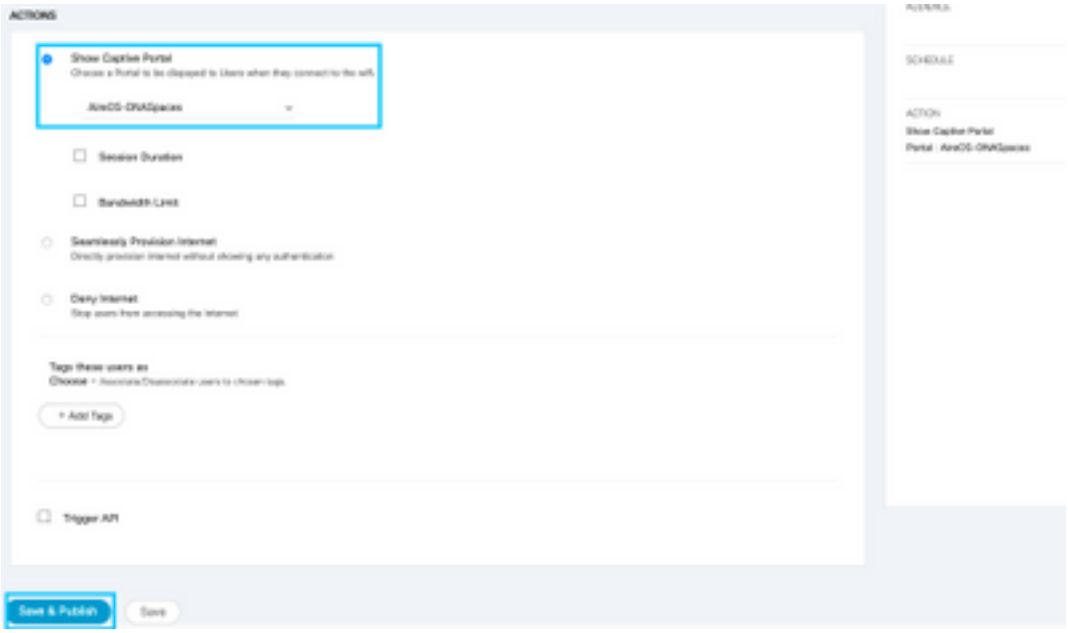
步骤1:打开强制网络门户菜单，然后点击**强制网络门户规则：**

第二步：单击**+ Create New Rule**。输入规则名称，选择先前配置的SSID，并选择此门户规则可用于的位置：



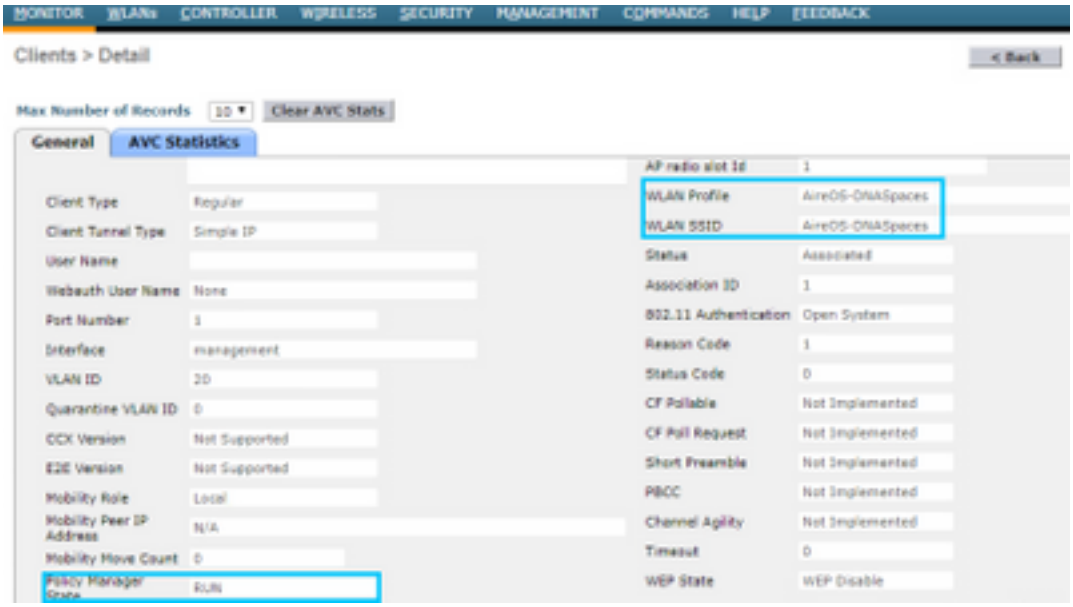
第三步：选择强制网络门户的操作。在这种情况下，当规则被命中时，将显示门户。单击**保存并发**

布。



验证

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



故障排除

在测试确认客户端的关联和身份验证过程之前，可以在控制器中启用以下命令。

```
(5520-Andressi) >debug client
```

```
(5520-Andressi) >debug web-auth redirect enable mac
```

以下是在连接到没有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的输出：

802.11关联/身份验证：

```
*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION
REQUEST on BSSID 70:d3:79:dd:d2:0f destination addr 70:d3:79:dd:d2:0f slotid 1
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capabiility as 4
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Processing assoc-req
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 ssid : AireOS-DNASpaces thread:bd271d6280
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode
(1), Result (0), Ssid (AireOS-DNASpaces), ApMac (70:d3:79:dd:d2:00), RSSI (-72), SNR (22)
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 on apVapId 1
```

DHCP和第3层身份验证：

```
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP_REQD
*webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in
HTTP GET, client mac=34:e1:2d:23:a6:68
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68
user_agent = AnyConnect Agent 4.7.04056
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual
IP, using virtual IP =192.0.2.1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Checking custom-web config for WLAN
ID:1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Global status is 0 on WLAN
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- checking on WLAN web-auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Web-auth type External, using
URL:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio ), redirect URL is
now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wla
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is
<HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"
content="no-cache"><META http-equiv="Pragma" content="
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=Ai
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=AireOS-DNASpaces&r

*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Message to be sent is
HTTP/1.1 200 OK
```

```
Location:
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- 200 send_data =HTTP/1.1 200 OK
Location:
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- send data length=688
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-
Url:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- cleaning up after send
```

第3层身份验证成功，将客户端移至RUN状态：

```
*emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68
*emWeb: Apr 09 21:49:57.634:
ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl_connection=0, secureweb=1

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

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

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）。