DNA Spaces Captive Portal with AireOS Controller配置示例

目錄

簡介

本文檔介紹如何使用帶有AireOS控制器的Cisco DNA Spaces配置捕獲型門戶。

作者：Andres Silva Cisco TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- 對無線控制器的命令列介面(CLI)或圖形使用者介面(GUI)訪問
- Cisco DNA Space

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 5520無線LAN控制器版本8.10.112.0

設定

網路圖表

組態

將WLC連線到Cisco DNA Spaces

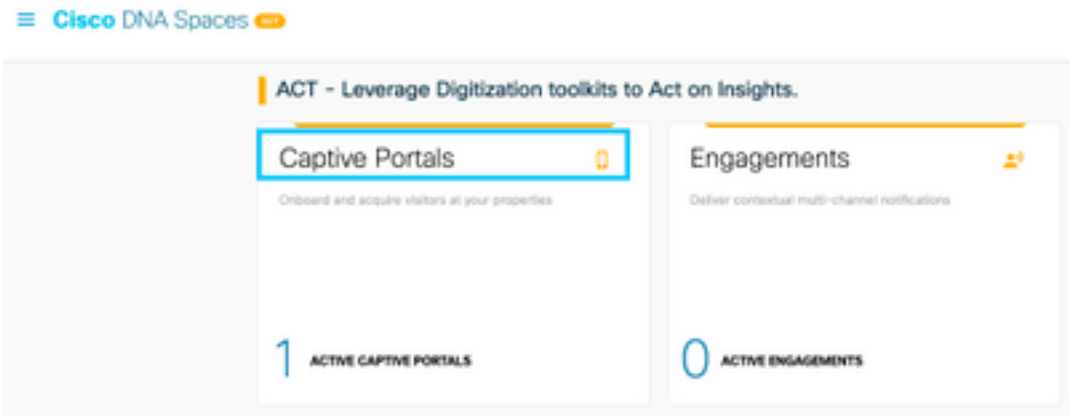
控制器需要使用任何可用的設定（直接連線）、通過DNA空間聯結器或使用CMX Tethering連線到DNA空間。

在本示例中，雖然強制網路門戶的配置方式對所有設定都相同，但直接連線選項仍在使用中。

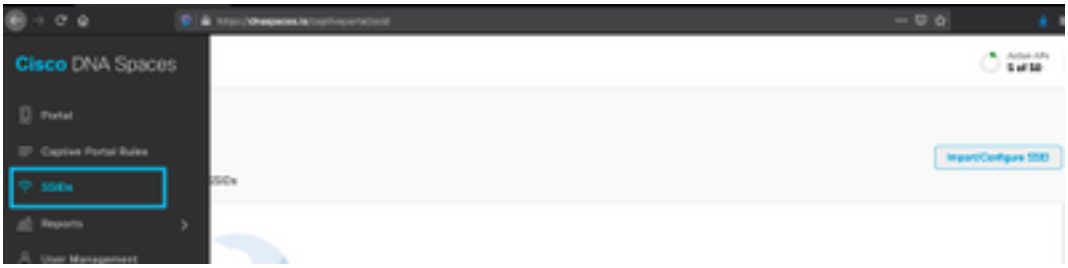
若要將控制器連線到Cisco DNA Spaces，它必須能夠通過HTTPS訪問Cisco DNA Spaces雲。有關如何將控制器連線到DNA Spaces的詳細資訊，請參閱以下連結：DNA Spaces Direct Connect配置示例

在DNA空間上建立SSID

步驟1.在DNA Spaces的控制面板中按一下**Captive Portals**:



步驟2.按一下頁面左上角的三行圖示開啟強制網路門戶選單，然後按一下**SSID:**

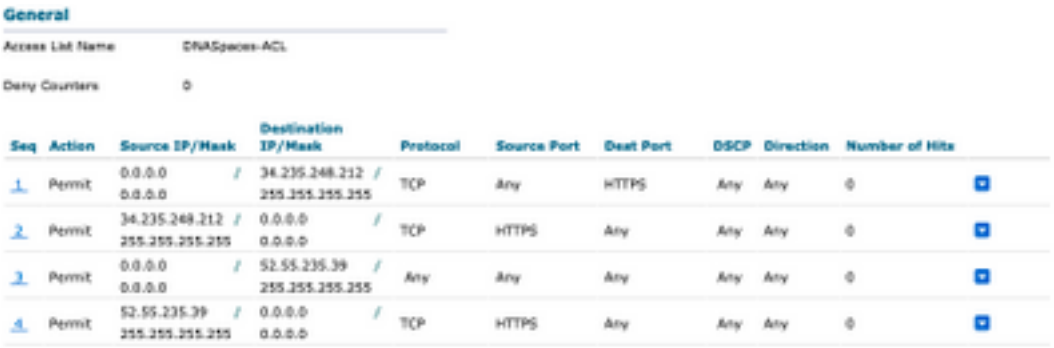


步驟3.按一下**Import/Configure SSID**，選擇**CUWN(CMX/WLC)**作為「Wireless Network」型別，然後輸入SSID名稱：

控制器上的ACL配置

需要預先驗證ACL，因為這是Web驗證SSID，並且一旦無線裝置連線到SSID並收到IP地址，裝置的策略管理器狀態將變為**Webauth_Reqd**狀態，並且ACL將應用到客戶端會話以限制裝置可以訪問的資源。

步驟1.導覽至**Security > Access Control Lists > Access Control Lists**，按一下**New**，然後按如下方式配置規則以允許無線客戶端與DNA空間之間的通訊。使用所用帳戶的DNA空間提供的IP地址替換：



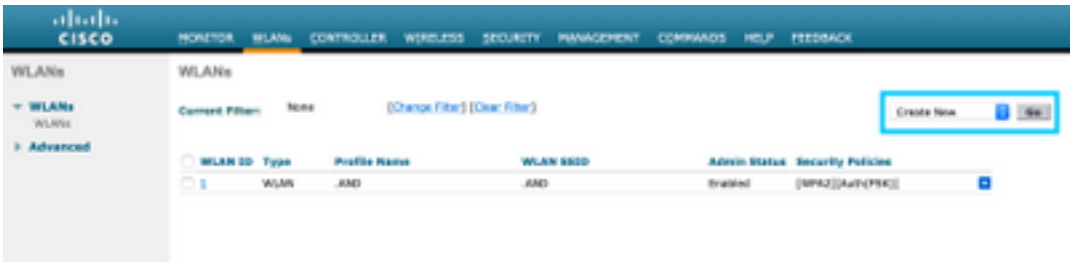
註：要獲取ACL中允許的DNA空間的IP地址，請在ACL配置部分下**在DNA空間上建立SSID一節的步驟3中建立的SSID中按一下Configure Manually**選項。

可以將SSID配置為使用RADIUS伺服器或不使用RADIUS伺服器。如果在Captive Portal Rule配置的**Actions**部分中配置了Session Duration、Bandwidth Limit或Inscilly Provision Internet，則需要使用RADIUS伺服器配置SSID，否則，無需使用RADIUS伺服器。兩種配置都支援DNA Spaces上的各種入口。

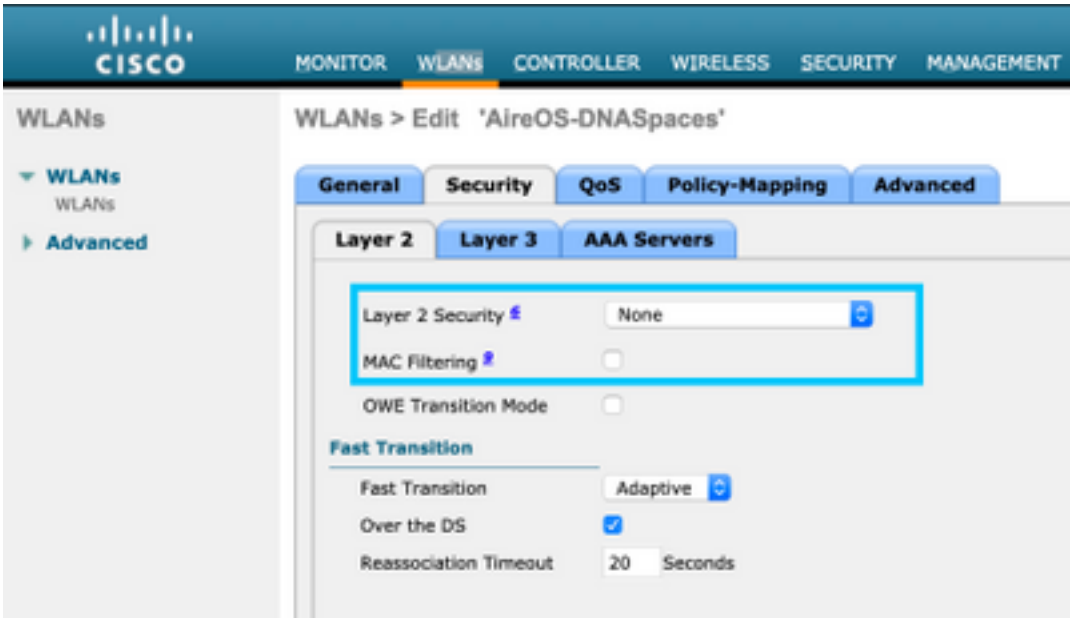
DNA空間上沒有RADIUS伺服器的強制網路門戶

控制器上的SSID配置

步驟1.導覽至**WLAN > WLANs。**建立一個新的 WLAN。配置配置檔名稱和SSID。確保SSID名稱與**在DNA空間中建立SSID** 一節的步驟3中配置的名稱相同。



步驟2.配置第2層安全性。導覽至WLAN configuration索引標籤中的**Security > Layer 2**索引標籤，然後從Layer 2 Security的下拉選單中選擇**None。**確保MAC過濾已禁用。



步驟3.配置第3層安全性。導覽至WLAN configuration索引標籤中的Security > Layer 3索引標籤，將Web **Policy設定為**第3層安全方**法，啟用Passthrough，設定預先驗證ACL，啟用Override Global Config**，將Web Auth Type設置為**External**，設定重新導向URL。

註：要獲取重定向URL，請點選**Configure Manually**選項，該選項位於SSID配置部分下**在DNA空間上建立SSID一節的步驟3中建立的SSID。**

在DNA空間上具有RADIUS伺服器的強制網路門戶

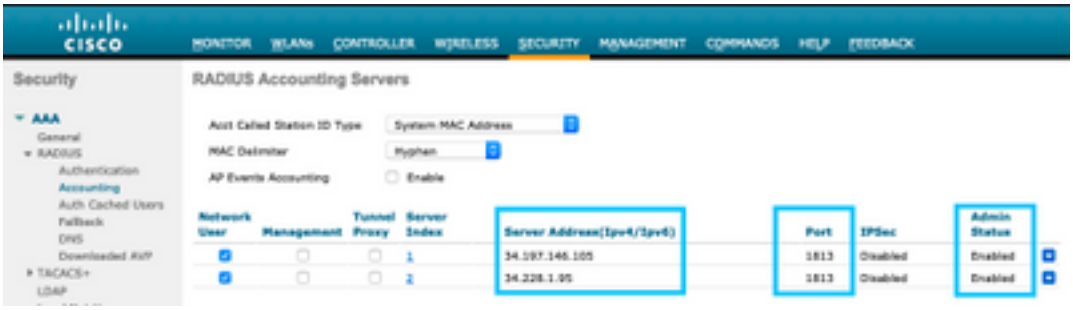
注意: DNA Spaces RADIUS伺服器僅支援來自控制器的PAP身份驗證。

控制器上的RADIUS伺服器配置

步驟1.導覽至**Security > AAA > RADIUS > Authentication**，按一下**New**，然後輸入RADIUS伺服器資訊。Cisco DNA Spaces充當RADIUS伺服器以進行使用者身份驗證，它可以在兩個IP地址上做出響應。配置兩台RADIUS伺服器：

註：要獲取主伺服器和輔助伺服器的RADIUS IP地址和金鑰，請按一下**在DNA空間上建立SSID部分步驟3中建立的SSID中的Configure Manually選項，然後導航至RADIUS Server Configuration部分。**

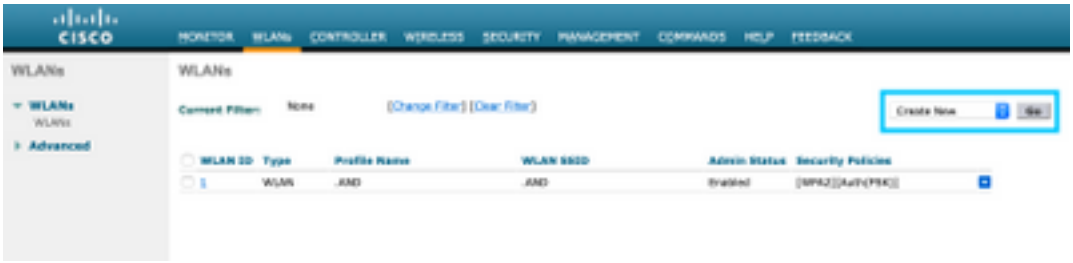
步驟2.配置記帳RADIUS伺服器。導覽至**Security > AAA > RADIUS > Accounting**，然後按一下**New**。配置相同的RADIUS伺服器：



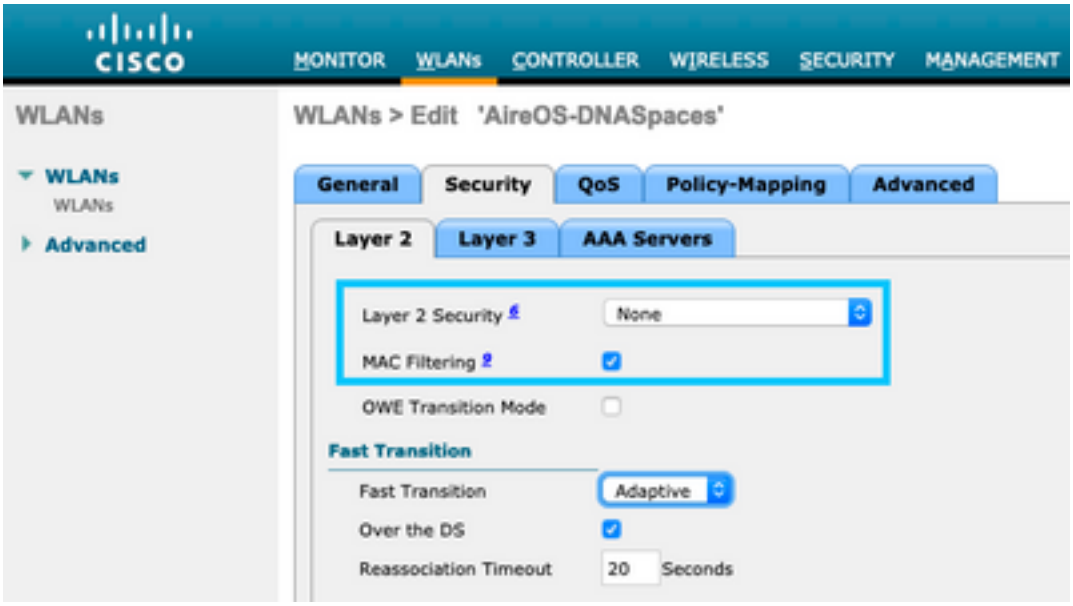
控制器上的SSID配置

> **重要**資訊：在開始SSID配置之前，請確保Controller > General下的**Web Radius** Authentication設定為「PAP」。

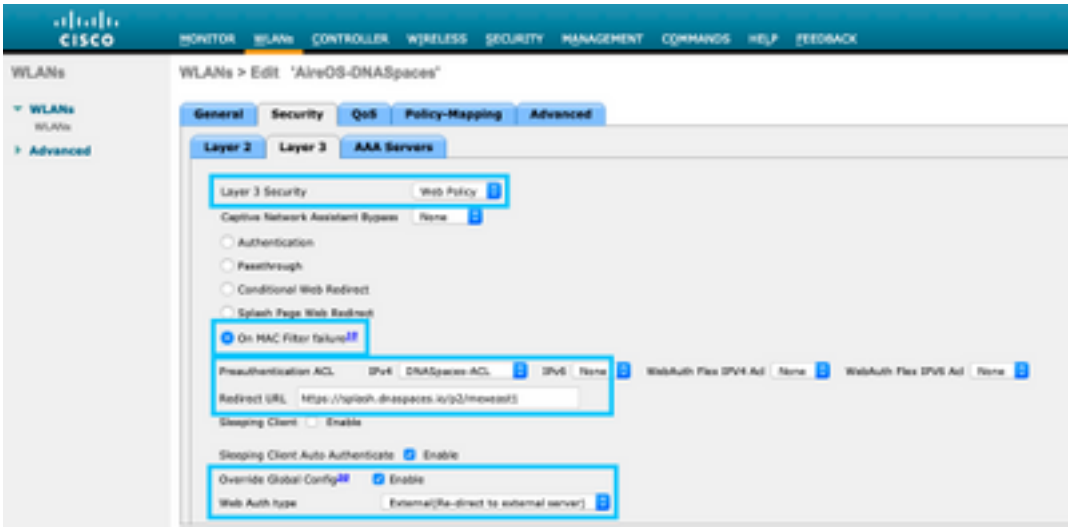
步驟1.導覽至**WLAN > WLANs。**建立一個新的 WLAN。配置配置檔名稱和SSID。確保SSID名稱與**在DNA空間中建立SSID** 一節的步驟3中配置的名稱相同。



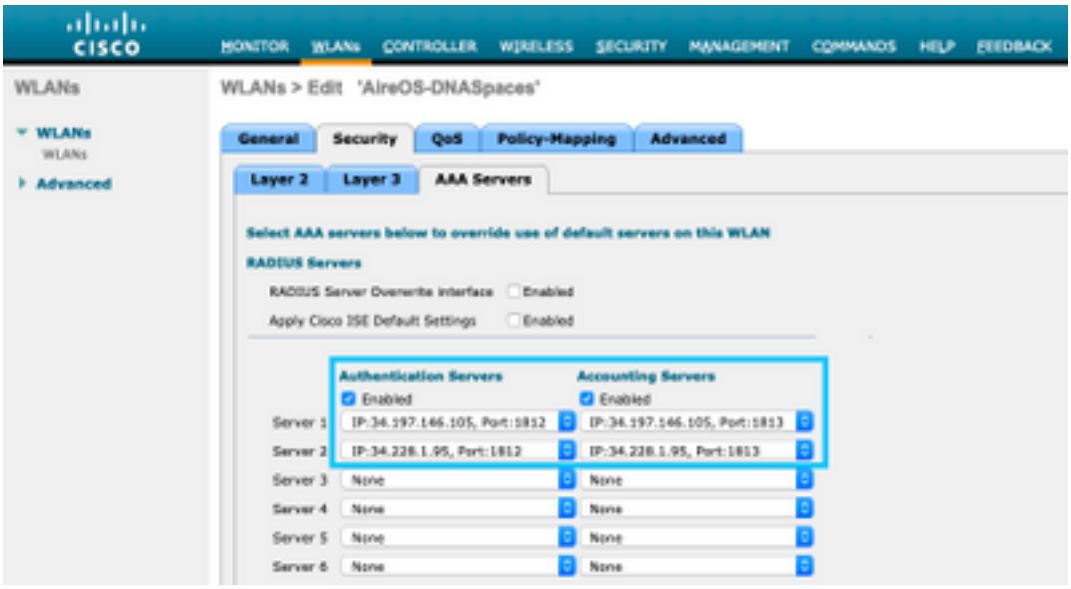
步驟2.配置第2層安全性。導覽至WLAN configuration索引標籤中的**Security > Layer 2**索引標籤。將第2層安全配置為**None**。啟用Mac過濾。



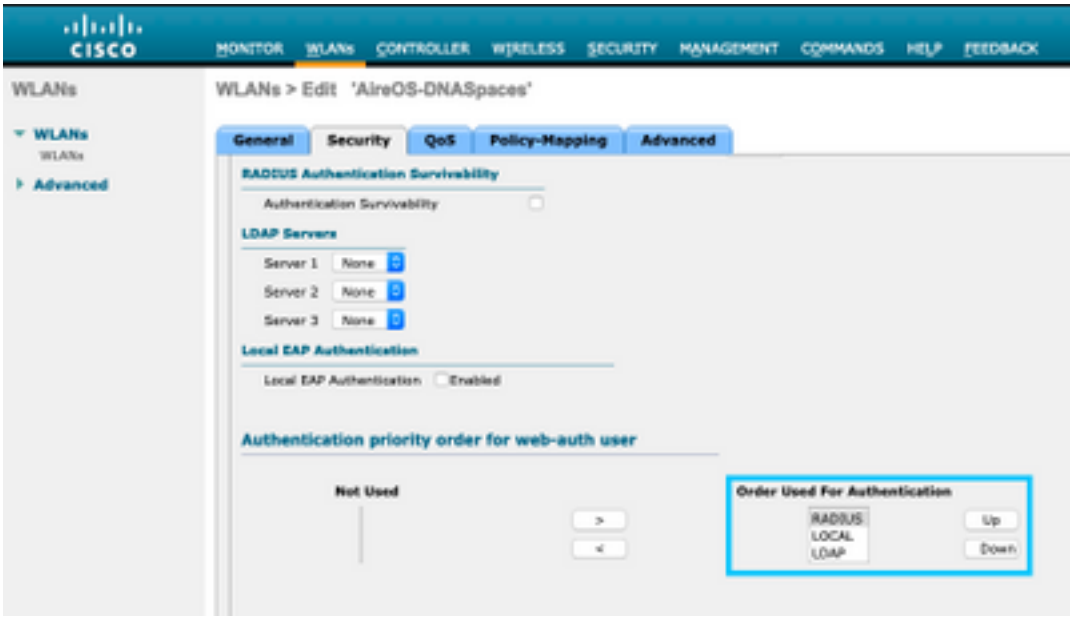
步驟3.配置第3層安全性。導覽至WLAN configuration索引標籤中的Security > Layer 3索引標籤，將Web **Policy設定為**第3層安全方**法，Enable On Mac Filter failure，設定預先驗證ACL，啟用Override Global Config**，將Web Auth Type設定為**External**，設定重新導向URL。



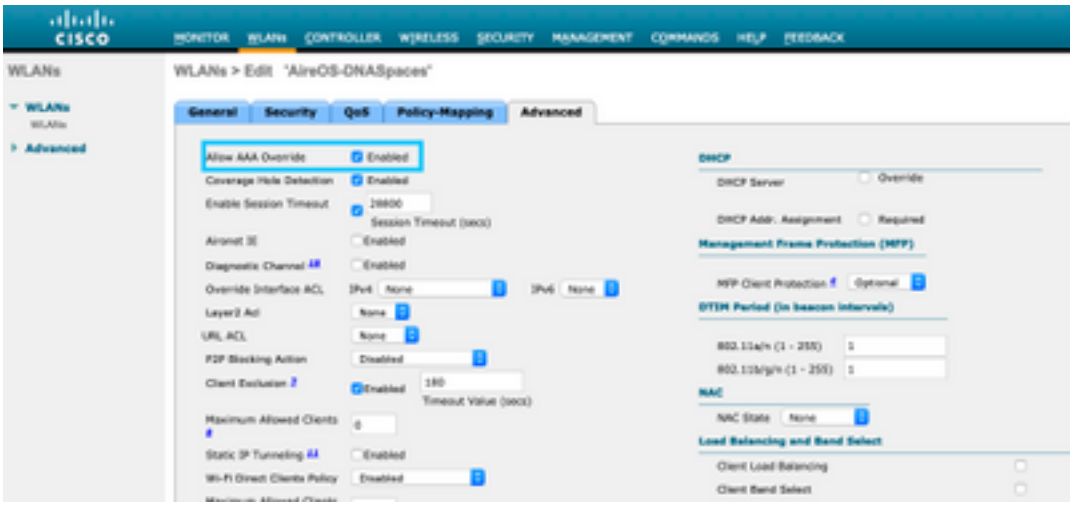
步驟4.配置AAA伺服器。導覽至WLAN configuration索引標籤中的**Security > AAA Servers**索引標籤，啟用**Authentication Servers**和**Accounting Servers**，然後從下拉選單中選擇兩個RADIUS伺服器：



步驟6.為Web-**auth使用者配置Authentication Priority順序**。導覽至WLAN configuration索引標籤中的**Security > AAA Servers**索引標籤，然後按順序設定RADIUS。

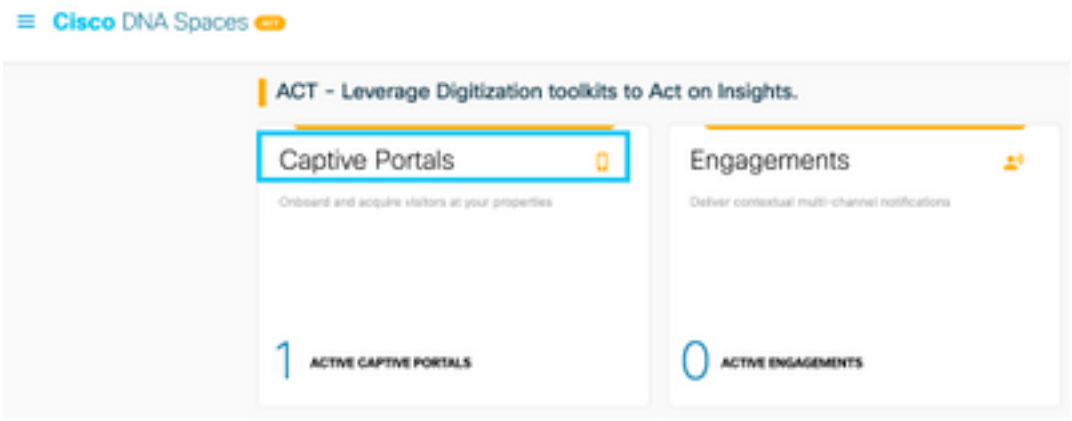


步驟7.導覽至WLAN configuration索引標籤中的**Advanced**索引標籤，然後啟用**Allow AAA Override**。

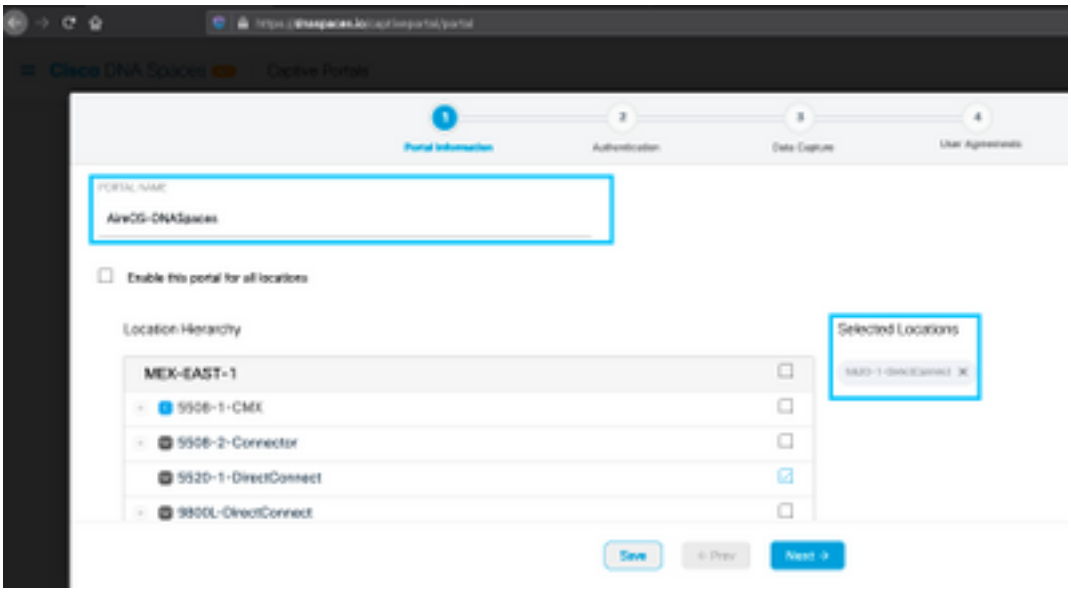


在DNA Spaces上建立入口

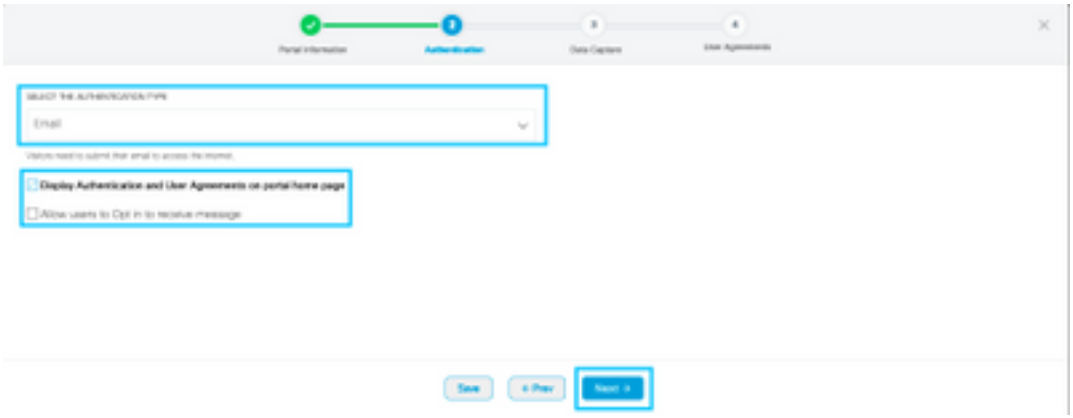
步驟1.在DNA Spaces的控制面板中按一下**Captive Portals**:



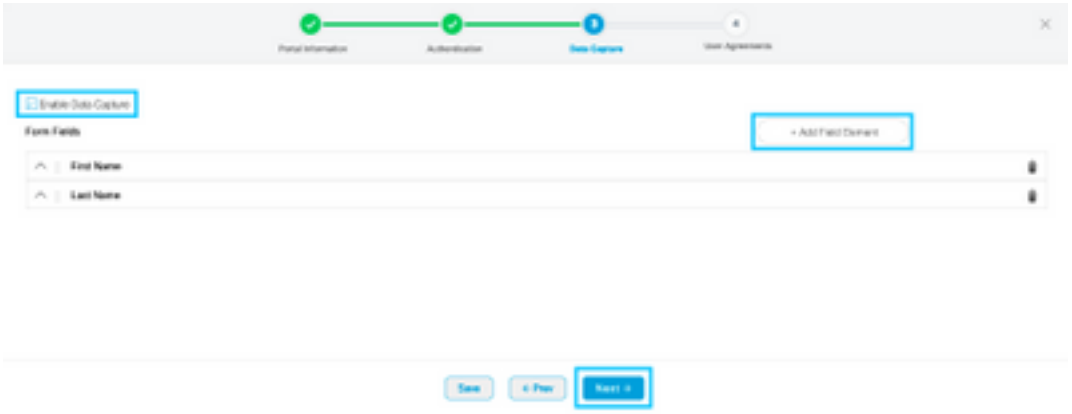
步驟2.按一下**Create New**，輸入門戶名稱，然後選擇可以使用該門戶的位置：



步驟3.選擇身份驗證型別，選擇是否要在門戶首頁上顯示資料捕獲和使用者協定，以及是否允許使用者選擇接收消息。按一下「**Next**」：

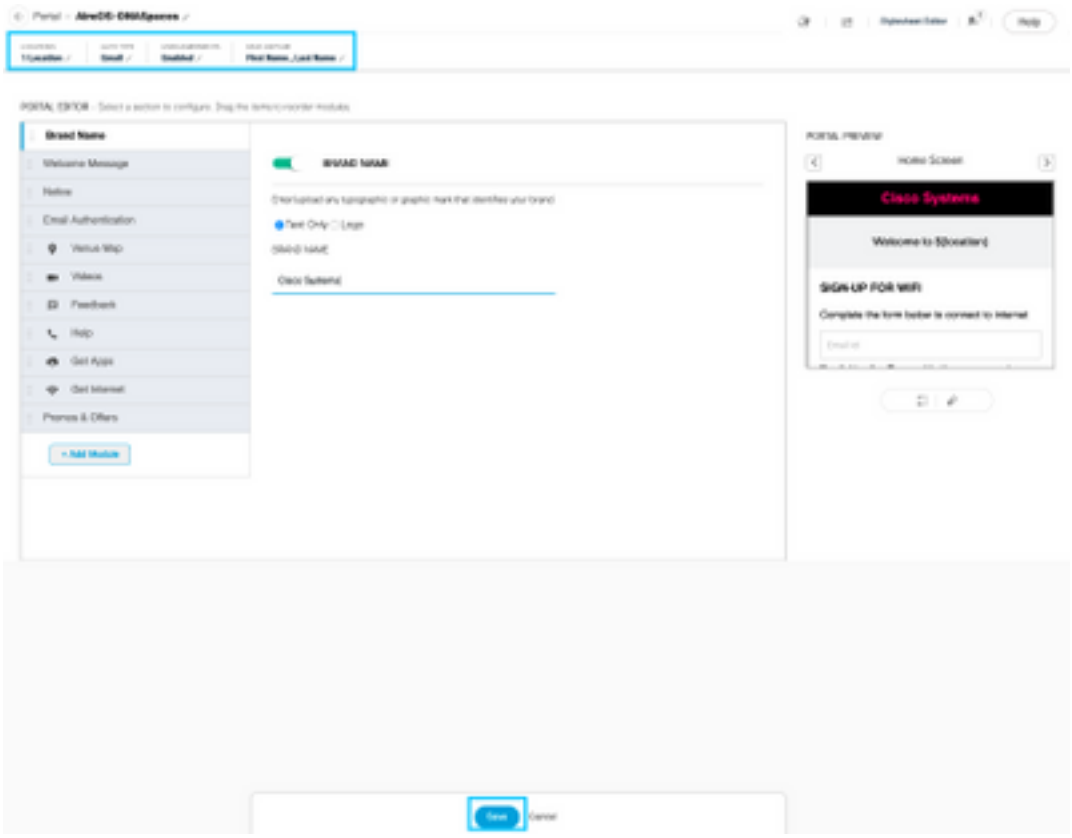


步驟4.配置資料捕獲元素。如果要從使用者捕獲資料，請選中**Enable Data Capture**框，然後按一下**+Add Field Element**以新增所需的欄位。按一下「**Next**」：



步驟5.選中**Enable Terms & Conditions**，然後按一下**Save & Configure Portal**:

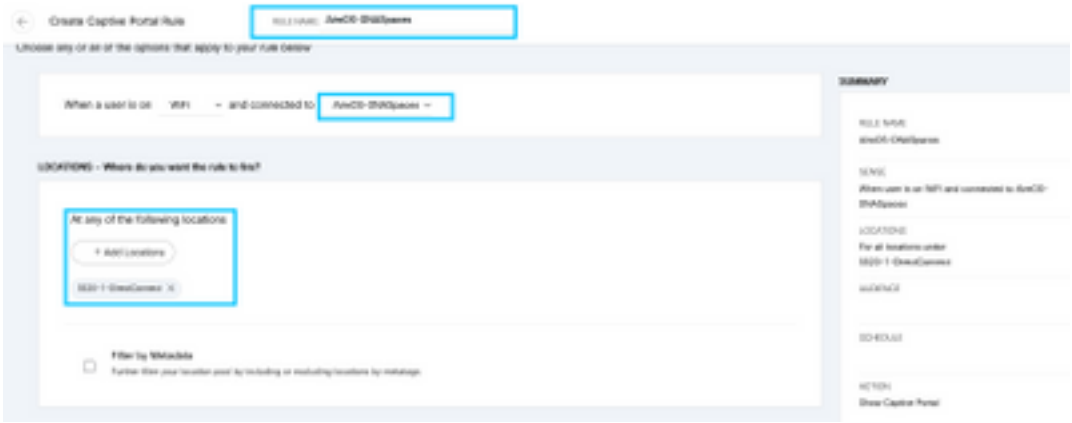
步驟6.根據需要編輯門戶，按一下**Save:**



在DNA空間上配置強制網路門戶規則

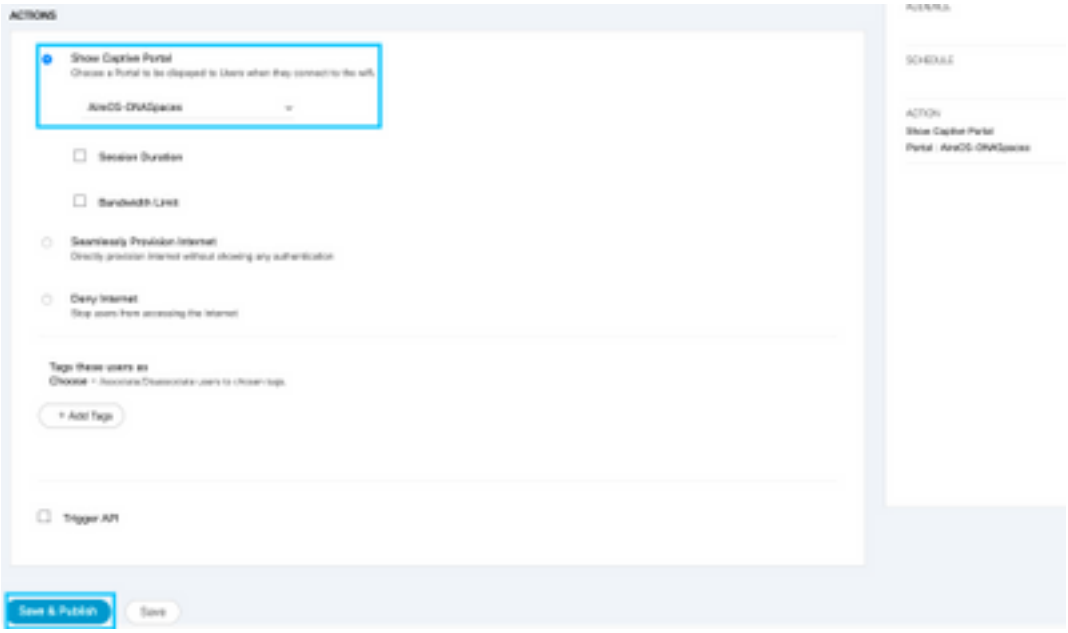
步驟1.開啟強制網路門戶選單，然後按一下**強制網路門戶規則：**

步驟2.按一下「**+ Create New Rule**」。輸入規則名稱，選擇先前配置的SSID，並選擇此入口規則可用於的位置：



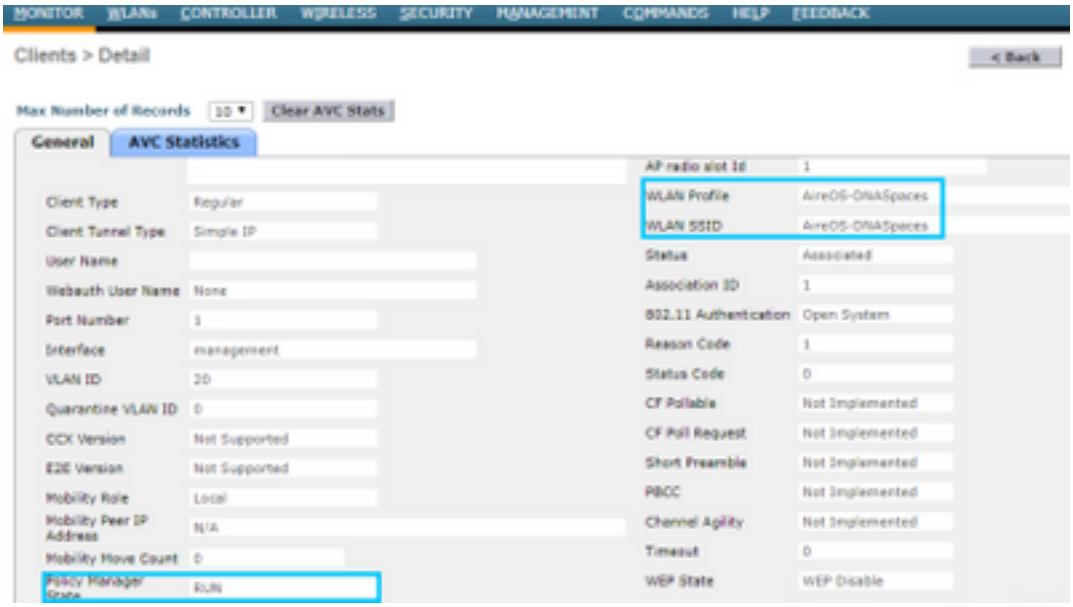
步驟3.選擇強制網路門戶的操作。在這種情況下，當規則被命中時，將顯示入口。按一下「**Save &**

Publish」。



驗證

要確認連線到SSID的客戶端的狀態，請導航到**Monitor > Clients**，按一下MAC地址並查詢Policy Manager State:



疑難排解

在測試確認客戶端的關聯和身份驗證過程之前，可以在控制器中啟用以下命令。

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

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

以下是連線到沒有RADIUS伺服器的SSID時，在關聯/身份驗證過程中成功嘗試識別每個階段的輸出：

802.11關聯/身份驗證：

```
*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層身份驗證：

```
*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層身份驗證成功，將客戶端移動到RUN狀態：

```
*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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。