

# 使用Catalyst 9800 WLC配置DNA空間捕獲門戶

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[將9800控制器連線到思科DNA空間](#)

[在DNA空間上建立SSID](#)

[9800控制器上的ACL和URL過濾器配置](#)

[DNA空間上沒有RADIUS伺服器的強制網路門戶](#)

[9800控制器上的Web身份驗證引數對映配置](#)

[在9800控制器上建立SSID](#)

[在9800控制器上配置策略配置檔案](#)

[在9800控制器上配置策略標籤](#)

[在DNA空間上具有RADIUS伺服器的強制網路門戶](#)

[9800控制器上的Web身份驗證引數對映配置](#)

[9800控制器上的RADIUS伺服器配置](#)

[在9800控制器上建立SSID](#)

[在9800控制器上配置策略配置檔案](#)

[在9800控制器上配置策略標籤](#)

[配置全域性引數對映](#)

[在DNA Spaces上建立入口](#)

[在DNA空間上配置強制網路門戶規則](#)

[從DNA空間獲取特定資訊](#)

[DNA Spaces使用哪些IP地址？](#)

[DNA Spaces登入門戶使用的URL是什麼？](#)

[DNA Spaces的RADIUS伺服器詳細資訊是什麼？](#)

[驗證](#)

[疑難排解](#)

[常見問題](#)

[永遠線上跟蹤](#)

[條件式偵錯和無線電主動式追蹤](#)

[成功嘗試的示例](#)

## 簡介

本文檔介紹如何在Cisco DNA Spaces上配置強制網路門戶。

## 必要條件

本檔案允許Catalyst 9800無線LAN控制器(C9800 WLC)上的使用者端使用DNA Spaces作為外部Web驗證登入頁面。

## 需求

思科建議您瞭解以下主題：

- 對9800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：

- 9800-L控制器版本16.12.2s

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

Web驗證是一種簡單的第3層驗證方法，不需要請求方或客戶端實用程式。這可以做到

- a)使用C9800 WLC上的內部頁面（原樣或進行修改）
- b)自訂登入套件上傳到C9800 WLC
- c)外部伺服器上託管的自定義登入頁面

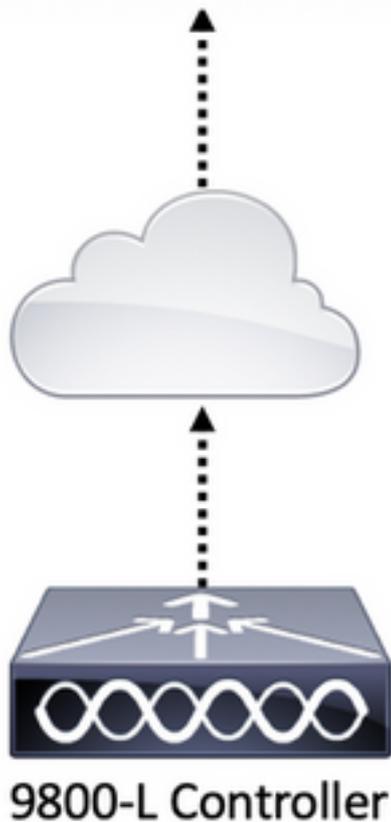
利用DNA Spaces提供的捕獲型門戶本質上是為C9800 WLC上的客戶端實施外部Web身份驗證的一種方式。

外部webauth程式詳述：<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，虛擬IP位址定義為全域引數映像，通常為192.0.2.1

## 設定

### 網路圖表



## 將9800控制器連線到思科DNA空間

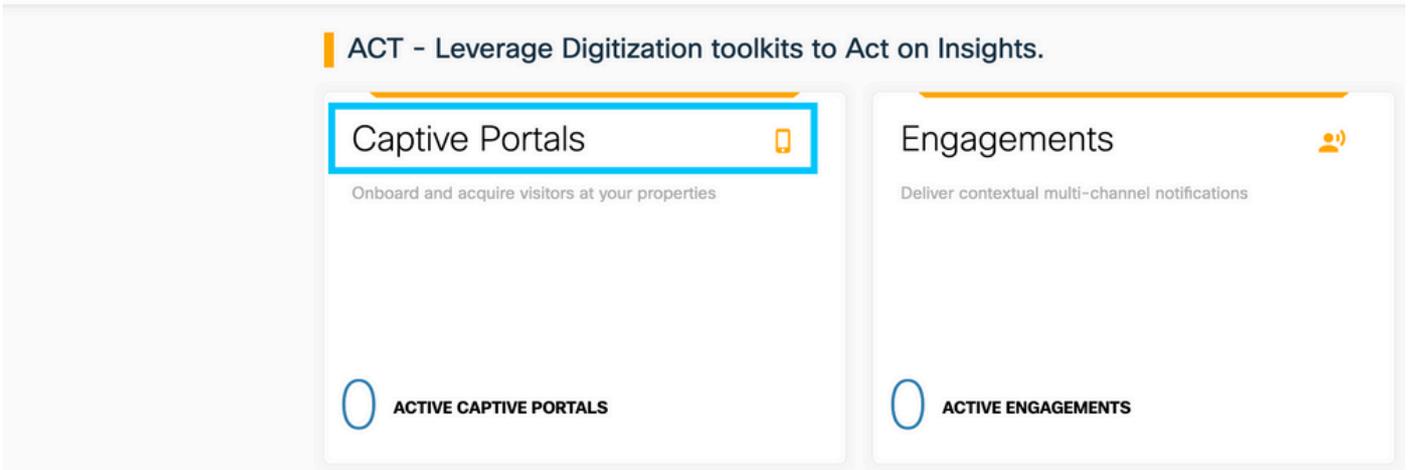
控制器需要使用任何選項 — 直接連線、通過DNA空間聯結器或CMX Tethering連線到DNA空間。

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。

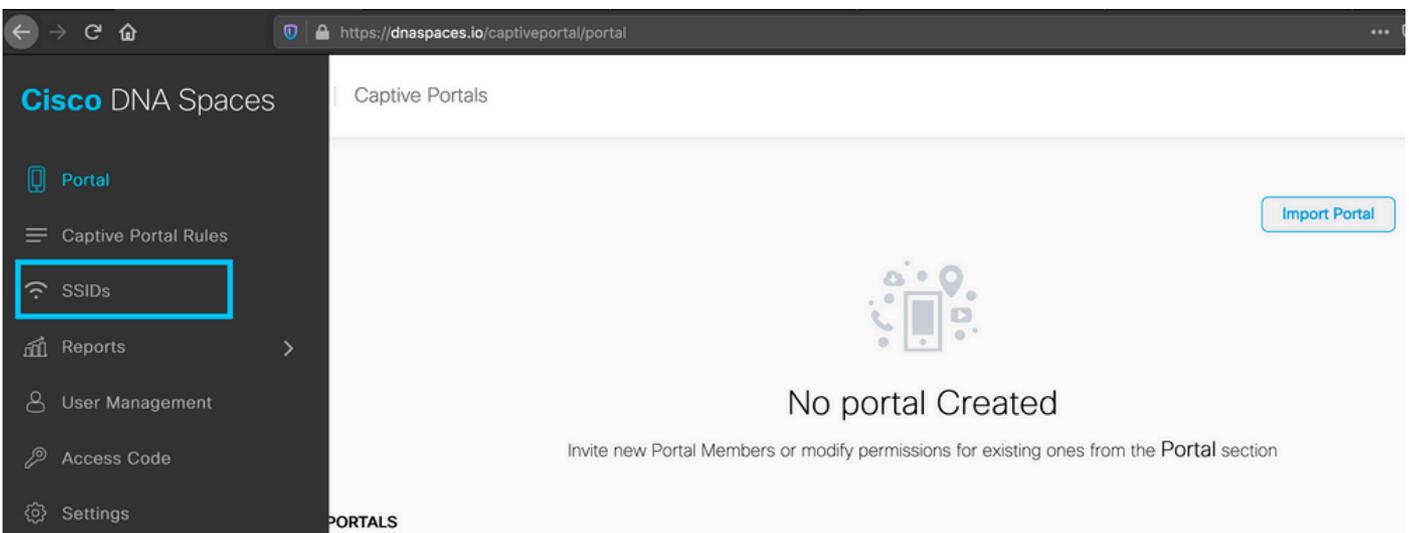
若要將控制器連線到Cisco DNA Spaces，它必須能夠通過HTTPS訪問Cisco DNA Spaces Cloud。有關如何將9800控制器連線到DNA空間的詳細資訊，請參閱以下連結：[DNA Spaces - 9800 Controller Direct Connect](#)

## 在DNA空間上建立SSID

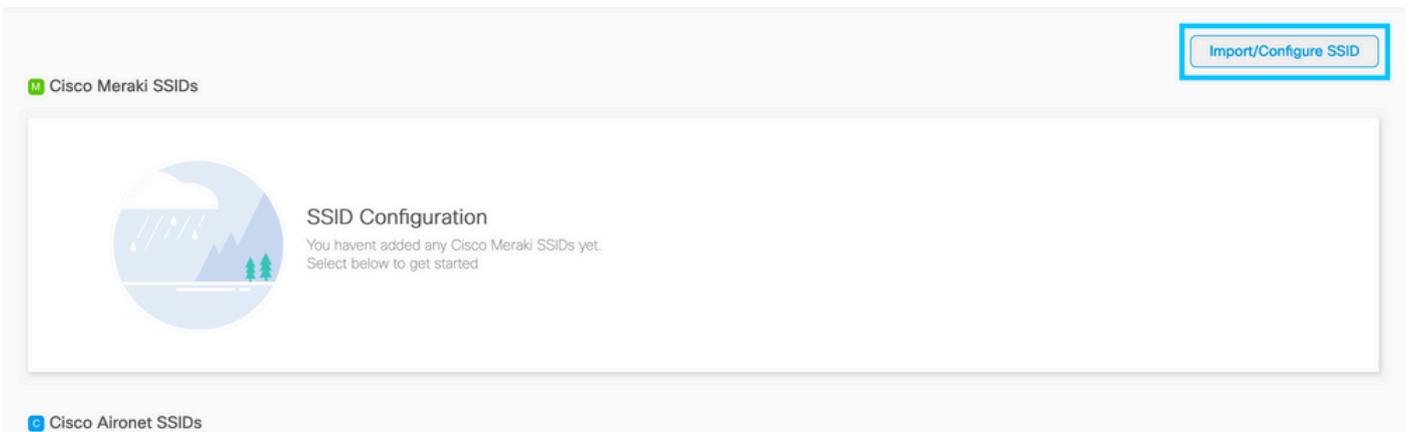
步驟1.在DNA Spaces的控制面板中按一下**Captive Portals**:



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



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



## 9800控制器上的ACL和URL過濾器配置

在完成身份驗證之前，不允許來自無線客戶端的流量進入網路。進行Web驗證時，為了完成驗證，無線客戶端連線到此SSID，收到IP地址，然後將客戶端策略管理器狀態移至Webauth\_reqd狀態。由於客戶端尚未通過身份驗證，因此除了DHCP、DNS和HTTP（被攔截並重定向）之外，所有來

自客戶端IP地址的流量都會被丟棄。

預設情況下，當設定web-auth WLAN時，9800會建立硬式編碼預先驗證ACL。這些硬式編碼ACL允許DHCP、DNS和流量到達外部Web身份驗證伺服器。所有其餘部分像任何http流量一樣被重定向

。但是，如果您需要允許特定非HTTP流量型別通過，則可以配置預先身份驗證ACL。然後，您需要模仿現有的硬式編碼預先驗證ACL的內容（在本節的步驟1中），並將其擴充到符合您的需要。

### 步驟1.驗證目前的硬式編碼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
```

之所以這樣呼叫WA-sec-34.235.248.212，是因為它是自動Web驗證(WA)安全(sec)ACL或入口ip「34.235.248.212」。安全ACL定義了允許的（允許時）或丟棄的（拒絕時）內容

Wa-v4-int是攔截ACL，即點選ACL或重定向ACL，並定義將哪些內容傳送到CPU進行重定向（在允許時）或傳送到資料平面（在拒絕時）。

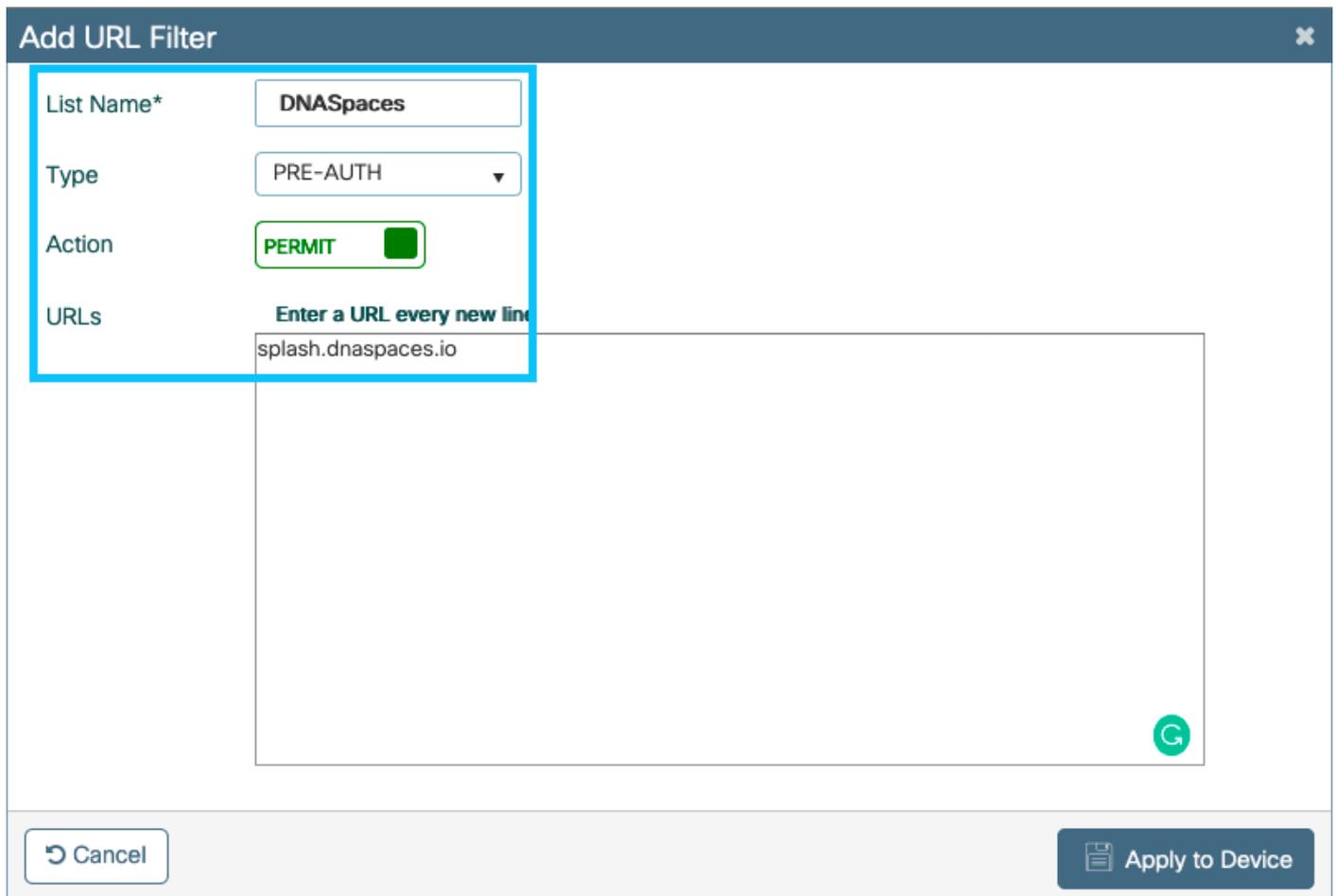
WA-v4-int34.235.248.212首先應用於來自客戶端的流量，並將指向DNA空間門戶IP 34.235.248.212的HTTP流量保留在資料平面上（尚未丟棄或轉發操作，只需切換到資料平面即可）。它將所有HTTP(s)流量傳送到CPU（除了由Web伺服器服務的虛擬IP流量以外的重定向）。其他型別的流量會提供給資料平面。

WA-sec-34.235.248.212允許流向在Web驗證引數對映中配置的DNA空間IP 34.235.248.212的HTTP和HTTPS流量，還允許DNS和DHCP流量並丟棄其餘流量。要攔截的HTTP流量在到達此ACL之前已遭攔截，因此無需此ACL涵蓋這些流量。

**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。在文檔末尾的「DNA空間使用的IP地址是什麼」一節中有一個示例。

DNA Spaces使用2個IP位址，而步驟1中的機制僅允許一個入口IP。若要允許預先驗證存取更多HTTP資源，您需要使用URL過濾器，此過濾器會針對您在URL過濾器中輸入其URL的網站，動態地在擷取（重新導向）和安全(preauth)ACL中建立漏洞。DNS請求被動態探聽，以使9800獲知這些URL的IP地址並將其動態新增到ACL。

步驟2.配置URL過濾器以允許DNA空間域。導覽至Configuration > Security > URL Filters，按一下+Add並設定清單名稱，選擇PRE-AUTH作為型別，選擇PERMIT作為URL splash.dnaspaces.io（如果使用EMEA入口網站，則為.eu）：



The screenshot shows the 'Add URL Filter' configuration interface. The 'List Name\*' field is set to 'DNASpaces'. The 'Type' dropdown is set to 'PRE-AUTH'. The 'Action' radio button is set to 'PERMIT'. The 'URLs' field contains the text 'splash.dnaspaces.io'. The interface includes a 'Cancel' button and an 'Apply to Device' button.

CLI配置：

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

```
Addresssi-9800L(config-urlfilter-params)#action permit
```

```
Addresssi-9800L(config-urlfilter-params)#url splash.dnaspaces.io
```

可以將SSID配置為使用RADIUS伺服器或不使用RADIUS伺服器。如果在強制網路門戶規則配置操作部分中配置了會話持續時間、頻寬限制或無縫調配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

### 9800控制器上的Web身份驗證引數對映配置

步驟1.導覽至Configuration > Security > Web Auth，然後按一下+Add以建立一個新的引數映像。在彈出的視窗中，配置引數對映名稱，然後選擇Consent作為型別：

### Create Web Auth Parameter ✕

|                          |              |
|--------------------------|--------------|
| Parameter-map name*      | DNASpaces-PM |
| Maximum HTTP connections | 1-200        |
| Init-State Timeout(secs) | 60-3932100   |
| Type                     | consent ▼    |

✕ Close ✓ Apply to Device

步驟2. 按一下上一步中配置的引數對映，導航到**高級**頁籤，然後輸入針對登入URL的重新導向、針對AP MAC地址的追加、針對客戶端MAC地址的追加、針對WLAN SSID和入口IPv4地址的追加，如圖所示，按一下**更新和應用**：

General

**Advanced**

**Redirect to external server**

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address

Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

**Customized page**

Login Failed Page  

Login Page  

Logout Page  

Login Successful Page  

✕ Cancel

 Update & Apply

**注意：**要獲取啟動顯示頁面URL和IPv4重定向地址，請按一下DNA空間SSID頁面中的 **Configure Manually** (手動配置) 選項。本文檔末尾的「DNA Spaces portal使用的URL是什麼？」中對此進行了說明

**註：**Cisco DNA Spaces門戶可以解析為兩個IP地址，但9800控制器僅允許配置一個IP地址，選擇其中任何IP地址，並在引數對映上將其配置為門戶IPv4地址。

**註：**確保 虛擬IPv4和IPv6地址都在全域性Web身份驗證引數對映中配置。如果未配置虛擬IPv6，客戶端有時會被重定向到內部門戶，而不是配置的DNA空間門戶。這就是必須始終配置虛擬IP的原因。「192.0.2.1」可以配置為虛擬IPv4,FE80:0:0:903A::11E4配置為虛擬IPV6。除了這些IP，很少有或根本沒有理由使用其他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控制器上建立SSID

步驟1.導覽至**Configuration > Tags & Profiles > WLANs**，然後按一下**+Add**。配置配置檔名稱、SSID並啟用WLAN。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。

**Add WLAN** ✕

General   Security   Advanced

Profile Name\*    Radio Policy

SSID\*    Broadcast SSID  ENABLED

WLAN ID\*

Status  ENABLED

步驟2.導覽至**Security > Layer2**。將Layer 2 Security Mode ( 第2層安全模式 ) 設定為**None(無)**，確保MAC Filtering ( MAC過濾 ) 已禁用。

**Add WLAN** ✕

General   **Security**   Advanced

**Layer2**   Layer3   AAA

Layer 2 Security Mode    Fast Transition

MAC Filtering    Over the DS

Transition Mode WLAN ID    Reassociation Timeout

步驟3.導覽至**Security > Layer3**。啟用Web策略，配置Web身份驗證引數對映。按一下**Apply to Device**。

Edit WLAN ✕

---

General
Security
Advanced
Add To Policy Tags

---

Layer2
Layer3
AAA

[Show Advanced Settings >>>](#)

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*

### 在9800控制器上配置策略配置檔案

步驟1. 導航到 **Configuration > Tags & Profiles > Policy**，然後建立新的策略配置檔案或使用預設策略配置檔案。在訪問策略頁籤中，配置客戶端VLAN並新增URL過濾器。

Edit Policy Profile ✕

---

General
Access Policies
QOS and AVC
Mobility
Advanced

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 ▼

### 在9800控制器上配置策略標籤

步驟1. 導航到 **Configuration > Tags & Profiles > Policy**。建立新的策略標籤或使用預設策略標籤。將WLAN對映到策略標籤中的策略配置檔案。

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 1

| WLAN Profile                           | Policy Profile |
|--|----------------|
| <input type="checkbox"/> 9800DNASpaces | DNASpaces-PP   |

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

步驟2.將Policy Tag (策略標籤) 應用於AP以廣播SSID。導航到**Configuration > Wireless > Access Points**，選擇有問題的AP並新增策略標籤。這會導致AP重新啟動其CAPWAP隧道並返回到9800控制器：

General

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

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) | <input type="checkbox"/>          |

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

Time Statistics

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

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
```

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

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

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

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

## 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。

### 9800控制器上的Web身份驗證引數對映配置

步驟1. 建立web auth引數映像。導覽至Configuration > Security > Web Auth，按一下+Add，然後設定引數圖名稱，然後選擇webauth作為型別：

### Create Web Auth Parameter ✕

|                          |              |
|--------------------------|--------------|
| Parameter-map name*      | DNASpaces-PM |
| Maximum HTTP connections | 1-200        |
| Init-State Timeout(secs) | 60-3932100   |
| Type                     | webauth ▼    |

✕ Close ✓ Apply to Device

步驟2. 按一下在步驟1中配置的引數對映，按一下**Advanced**，然後輸入用於登入的重新導向、Append for AP MAC Address、Append for Client MAC Address、Append for WLAN SSID and

portal IPv4 Address。按一下「Update & Apply:

General

**Advanced**

**Redirect to external server**

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address

Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

**Customized page**

Login Failed Page  

Login Page  

Logout Page  

Login Successful Page  

✕ Cancel

 Update & Apply

**註：**要獲取啟動顯示頁面URL和IPv4重定向地址，請分別在在WLC直接連線中建立SSID一節建立訪問控制清單配置一節的在DNA空間上建立SSID步驟3中建立的SSID中按一下**Configure Manually**選項。

**注意：**Cisco DNA Spaces門戶可以解析為兩個IP地址，但9800控制器僅允許配置一個IP地址，其中一個案例選擇引數對映中要配置的任何一個IP地址作為門戶IPv4地址。

**附註：**確保在全域性Web身份驗證引數對映中同時配置虛擬IPv4和IPv6地址。如果未配置虛擬IPv6，客戶端有時會被重定向到內部門戶，而不是配置的DNA空間門戶。這就是必須始終配置虛擬IP的原因。「192.0.2.1」可以配置為虛擬IPv4,FE80:0:0:903A::11E4配置為虛擬IPV6。除了這些IP，很少有或根本沒有理由使用其他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伺服器配置

步驟1.配置RADIUS伺服器。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。導覽至**Configuration > Security > AAA**，按一下**+Add**，然後設定兩個RADIUS伺服器：

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups    AAA Method List    AAA Advanced

+ Add    - Delete

RADIUS

Servers    Server Groups

TACACS+

Create AAA Radius Server

|                             |   |
|-----------------------------|---|
| Name*                       | DNASpaces1                                  |
| IPv4 / IPv6 Server Address* | 34.197.146.105                              |
| PAC Key                     | <input type="checkbox"/>                    |
| 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 <input checked="" type="checkbox"/> |

Cancel    Apply to Device

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RADIUS伺服器組並新增兩個RADIUS伺服器。導覽至Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups，按一下+add，設定Server Group name，將MAC-Delimiter設定為連字元，將MAC-Filtering設定為MAC，然後分配兩個RADIUS伺服器：

+ AAA Wizard

Servers / Groups    AAA Method List    AAA Advanced

+ Add

Delete

RADIUS

TACACS+

LDAP

Servers    Server Groups

Name    Server 1    Server 2

0    10 items per page

### Create AAA Radius Server Group

Name\*    DNASpaces

Group Type    RADIUS

MAC-Delimiter    hyphen

MAC-Filtering    mac

Dead-Time (mins)    1-1440

Available Servers

>

<

Assigned Servers

DNASpaces1  
DNASpaces2

Cancel

Apply to Device

步驟3.配置身份驗證方法清單。導航到Configuration > Security > AAA > AAA Method List > Authentication，然後單擊+add。配置方法清單名稱，選擇login作為型別並分配伺服器組：

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups   **AAA Method List**   AAA Advanced

Authentication

Authorization

Accounting

+ Add   - Delete

| Name                             | Type  | Group Type | Group1 | Group2 |
|----------------------------------|-------|------------|--------|--------|
| <input type="checkbox"/> default | dot1x | local      | N/A    | N/A    |

10 items per page

### 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

Cancel   Apply to Device

步驟4. 配置授權方法清單。導航到**Configuration > Security > AAA > AAA Method List > Authorization**，點選**+add**。配置方法清單名稱，選擇**network**作為型別並分配伺服器組：

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups    **AAA Method List**    AAA Advanced

Authentication

**Authorization**

Accounting

+ Add    × Delete

| Name                            | Type                | Group Type | Group1 | Group2 |
|---------------------------------|---------------------|------------|--------|--------|
| <input type="checkbox"/> MeshAP | credential-download | local      | N/A    | N/A    |

10 items per page

**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

Cancel    Apply to Device

## 在9800控制器上建立SSID

步驟1. 導覽至 Configuration > Tags & Profiles > WLANs，然後按一下+Add。配置配置檔名稱、SSID並啟用WLAN。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。

**Add WLAN** ✕

General   Security   Advanced

Profile Name\*    Radio Policy

SSID\*    Broadcast SSID  ENABLED

WLAN ID\*

Status  ENABLED

步驟2.導覽至Security > Layer2。將第2層安全模式設定為None，啟用MAC過濾並新增授權清單：

**Add WLAN** ✕

General   **Security**   Advanced

Layer2   Layer3   AAA

Layer 2 Security Mode    Fast Transition

MAC Filtering    Over the DS

Transition Mode WLAN ID    Reassociation Timeout

Authorization List\*

步驟3.導覽至Security > Layer3。啟用Web策略，配置Web身份驗證引數對映和身份驗證清單。在Mac過濾器失敗時啟用並新增預身份驗證ACL。按一下Apply to Device。

Add WLAN ✕

General
Security
Advanced

---

Layer2
Layer3
AAA

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

<< Hide  

On Mac Filter Failure

Splash Web Redirect DISABLED

Preauthentication ACL

IPv4 DNASpaces-ACL ▼

IPv6 None ▼

↶ Cancel

📄
Apply to Device

### 在9800控制器上配置策略配置檔案

步驟1. 導航到 **Configuration > Tags & Profiles > Policy**，然後建立新的策略配置檔案或使用預設策略配置檔案。在訪問策略頁籤中，配置客戶端VLAN並新增URL過濾器。

Edit Policy Profile ✕

General
Access Policies
QOS and AVC
Mobility
Advanced

---

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 ▼

步驟2. 在Advanced頁籤中，啟用AAA Override並選擇性地配置記帳方法清單：

### Edit Policy Profile ✕

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

---

#### WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

#### DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

#### AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List

Fabric Profile

Umbrella Parameter Map

mDNS Service Policy  [Clear](#)

#### WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

#### Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

## 在9800控制器上配置策略標籤

步驟1. 導航到 **Configuration > Tags & Profiles > Policy**。建立新的策略標籤或使用預設策略標籤。將WLAN對映到策略標籤中的策略配置檔案。

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 1

| WLAN Profile                           | Policy Profile |
|--|----------------|
| <input type="checkbox"/> 9800DNASpaces | DNASpaces-PP   |

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

步驟2.將Policy Tag ( 策略標籤 ) 應用於AP以廣播SSID。導航到**Configuration > Wireless > Access Points**，選擇有問題的AP並新增策略標籤。這會導致AP重新啟動其CAPWAP隧道並返回到9800控制器：

General

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

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) | <input type="checkbox"/>          |

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

Time Statistics

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

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
```

## 配置全域性引數對映

不推薦的步驟：運行這些命令以允許HTTPS重定向，但是請注意，如果客戶端作業系統執行強制網路門戶檢測並導致CPU使用率較高且始終拋出證書警告，則不需要在客戶端HTTPS流量中進行重定向。因此，建議避免進行配置，除非需要針對非常特定的使用情形。

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

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

**註：**您必須擁有安裝在Cisco Catalyst 9800系列無線控制器中的虛擬IP的有效SSL證書。

步驟1.將副檔名為.p12的已簽署憑證檔案複製到TFTP伺服器，然後運行此指令來傳輸憑證並將其安裝到9800控制器中：

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

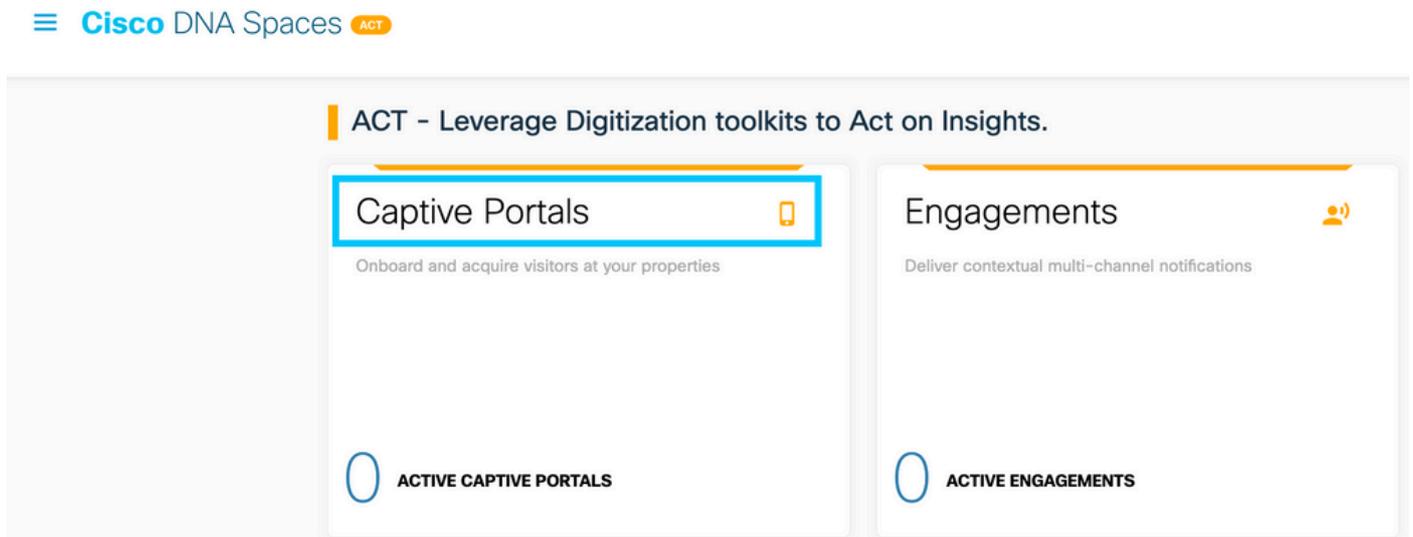
步驟2.若要將已安裝憑證對應到Web驗證引數對應，請執行以下命令：

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

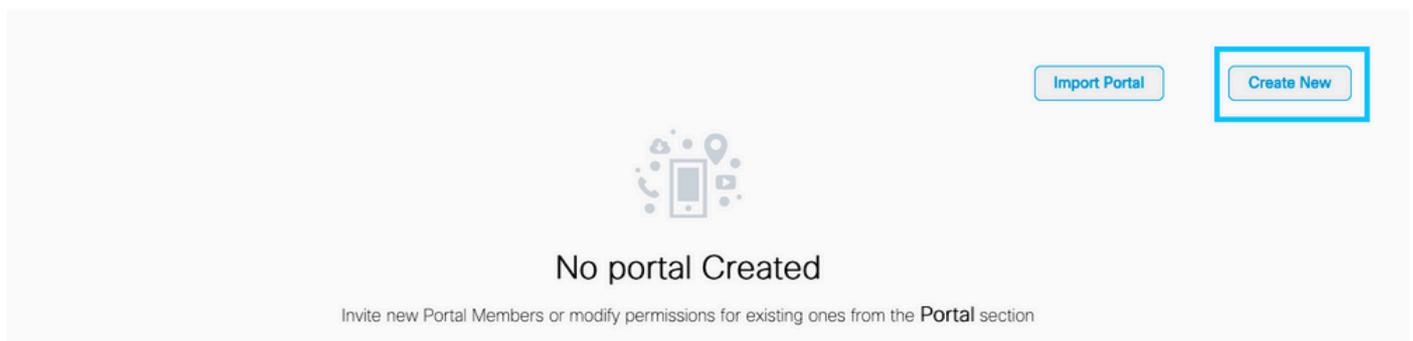
```
Andressi-9800L(config-params-parameter-map)#trustpoint
```

## 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**，輸入門戶名稱並選擇可使用門戶的位置：



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」：

The screenshot shows a progress bar at the top with four steps: Portal Information (1), Authentication (2), Data Capture (3), and User Agreements (4). Step 2, Authentication, is currently active. Below the progress bar, there is a dropdown menu labeled 'SELECT THE AUTHENTICATION TYPE' with 'No Authentication' selected. Below this, there are two checkboxes: 'Display Data Capture and User Agreements on portal home page' (checked) and 'Allow users to Opt in to receive message' (unchecked). At the bottom, there are three buttons: 'Save', '< Prev', and 'Next >' (highlighted with a green box).

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」：

The screenshot shows the progress bar with steps 1, 2, 3, and 4. Step 3, Data Capture, is active. Below the progress bar, there is a checkbox labeled 'Enable Data Capture' which is checked. Below this, there is a section titled 'Form Fields' and a button labeled '+ Add Field Element'. At the bottom, there are three buttons: 'Save', '< Prev', and 'Next >' (highlighted with a green box).

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

The screenshot shows the progress bar with steps 1, 2, 3, and 4. Step 4, User Agreements, is active. Below the progress bar, there is a checkbox labeled 'Enable Terms & Conditions' which is checked. Below this, there is a section titled 'TERMS & CONDITION MESSAGE' with a language selector set to 'English'. Below this, there is a rich text editor with a toolbar and a text area containing the following text: '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.' At the bottom, there are three buttons: 'Save', '< Prev', and 'Save & Configure Portal' (highlighted with a green box).

步驟6.根據需要編輯門戶，按一下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.

- Brand Name
- Welcome Message**
- Notice
- Data Capture
- Venue Map
- Videos
- Feedback
- Help
- Get Apps
- Get Internet
- Promos & Offers

+ Add Module

**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: Home Screen

ACME Company

Welcome to Cisco Mexico

**SIGN-UP FOR WIFI**

Email Address:

Mobile Number:

Save Cancel

## 在DNA空間上配置強制網路門戶規則

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

☰ Cisco DNA Spaces ACT

ACT - Leverage Digitization toolkits to Act on Insights.

**Captive Portals** 📱  
Onboard and acquire visitors at your properties

**Engagements** 😊  
Deliver contextual multi-channel notifications

0 ACTIVE CAPTIVE PORTALS

0 ACTIVE ENGAGEMENTS

步驟2. 開啟強制網路門戶選單，然後按一下**強制網路門戶規則**：

Cisco DNA Spaces | Captive Portals | Active APs 5 of 50

Portal

Captive Portal Rules

SSIDs

Reports

User Management

Access Code

Settings

Import Portal

Create New

| NAME           | STATUS | LAST MODIFIED |
|----------------|--------|---------------|
| 9800DNASpaces1 | Draft  | Feb 18, 2020  |

1 in 1 Locations | 0 in 0 Captive Portal Rule

Previous 1 Next Last

(1 - 1 of 1) : 1 pages

PORTALS

步驟3.按一下「+ Create New Rule」。輸入規則名稱，選擇先前配置的SSID。

Create Captive Portal Rule

RULE NAME: 9800DNASpaces

Choose any or all of the options that apply to your rule below

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

LOCATIONS - Where do you want the rule to fire?

At any of the following locations

+ Add Locations

Please select at-least one location

步驟4.選擇門戶可用的位置。在LOCATIONS部分中按一下+ Add Locations。從位置層次結構中選擇所需的一個。

#### Choose Locations

Location Hierarchy

|                        |                                     |
|------------------------|-------------------------------------|
| MEX-EAST-1             | <input type="checkbox"/>            |
| + 5508-1-CMX           | <input type="checkbox"/>            |
| + 5508-2-Connector     | <input type="checkbox"/>            |
| + 5520-1-DirectConnect | <input type="checkbox"/>            |
| + 9800L-DirectConnect  | <input checked="" type="checkbox"/> |

Selected Locations

9800L-DirectConnect

步驟5.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」。

**ACTIONS**

**Show Captive Portal**  
Choose a Portal to be displayed 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.

+ Add Tags

---

Trigger API

Save & Publish Save

**SCHEDULE**

**ACTION**  
Show Captive Portal  
Portal : 9800DNASpaces1

## 從DNA空間獲取特定資訊

### DNA Spaces使用哪些IP地址？

要驗證您所在區域的DNA空間用於門戶的IP地址，請轉到DNA空間首頁上的Captive門戶頁面。按一下左側選單中的**SSID**，然後按一下SSID下的**Configure manually**。ACL範例中會提到IP位址。這些是ACL和webauth引數對映中使用的入口的IP地址。DNA Spaces將其他IP地址用於控制平面的整體NMSP/雲連線。

Cisco DNA Spaces

Import/Configure SSID

Cisco Meraki SSIDs

**SSID Configuration**  
You haven't added any Cisco Meraki SSIDs yet.  
Select below to get started!

Cisco Aronnet SSIDs

Guest LAB-DNAS

Delete Configure Manually Delete **Configure Manually**

在出現的彈出視窗的第一部分，步驟7顯示了ACL定義中提到的IP地址。您不需要執行這些說明並建立任何ACL，只需記下IP地址即可。這些是您所在地區的門戶使用的IP

**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 Spaces 登入門戶使用的 URL 是什麼？**

若要驗證您所在區域門戶使用的登入門戶 URL DNA 空間，請轉到 DNA 空間首頁上的 Captival 門戶頁面。按一下左側選單中的 **SSID**，然後按一下 SSID 下的 **Configure manually**。

☰ Cisco DNA Spaces

☰ ● ● ●

The screenshot shows the Cisco DNA Spaces interface. At the top right, there is a button labeled 'Import/Configure SSID'. Below this, there is a section for 'Cisco Meraki SSIDs' which is currently empty. Underneath, there is a section for 'Cisco Aironet SSIDs'. This section contains two entries: 'Guest' and 'LAB-DNAS'. Each entry has a 'Delete' button and a 'Configure Manually' button. The 'Configure Manually' button for the 'LAB-DNAS' entry is highlighted with a red box.

在出現的彈出視窗中向下滾動，在第二部分中，步驟 7 顯示必須在 9800 上的引數對映中配置的 URL。

## Creating the SSIDs in WLC Direct Connect

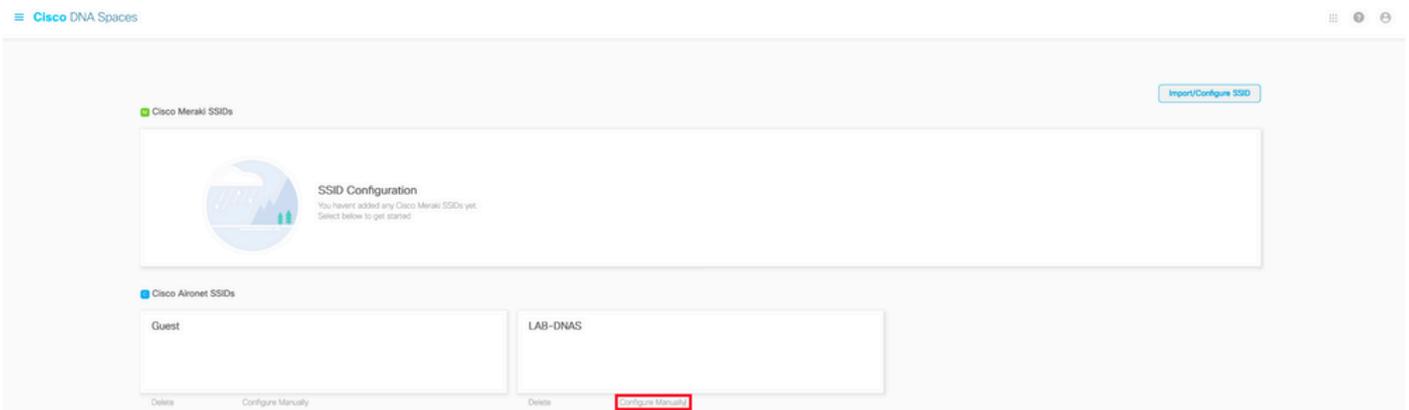
To create the SSIDs in the WLC Direct Connect, perform the following steps:

- 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 Spaces的RADIUS伺服器詳細資訊是什麼？

要瞭解您需要使用的RADIUS伺服器IP地址以及共用金鑰，請轉到DNA Space首頁上的Captival Portal頁面。按一下左側選單中的**SSID**，然後按一下SSID下的**Configure manually**。



在顯示的彈出視窗中，向下滾動第3部分(RADIUS)，第7步為您提供IP/埠和用於RADIUS身份驗證的共用金鑰。記帳是可選的，在步驟12中進行了說明。

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   |

## 驗證

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

The screenshot shows the 'Client' monitoring interface. The 'General' tab is selected, and the 'Client Properties' sub-tab is active. The following table displays the client's details:

| Property                         | Value                               |
|----------------------------------|-------------------------------------|
| 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                                 |

## 疑難排解

### 常見問題

1.如果控制器上的虛擬介面未設定IP位址，則使用者端會重新導向到內部入口網站，而不是在引數對映中設定的重新導向入口網站。

2.如果客戶端在重定向到DNA Spaces上的門戶時收到503錯誤，請確保在DNA Spaces的位置層次中配置控制器。

## 永遠線上跟蹤

WLC 9800 提供永不間斷的追蹤功能。這可確保所有與客戶端連線相關的錯誤、警告和通知級別消息持續記錄，並且您可以在發生事故或故障情況後檢視其日誌。

**注意：**根據生成的日誌量，您可以將時間從幾小時縮短到幾天。

若要檢視9800 WLC在預設情況下蒐集的追蹤，可以透過SSH/Telnet連線到9800 WLC，並執行這些步驟（確保作業階段記錄到文字檔中）。

步驟1.檢查控制器當前時間，這樣您就可以跟蹤問題發生時之前的日誌。

```
# show clock
```

步驟2.根據系統配置的指示，從控制器緩衝區或外部系統日誌中收集系統日誌。這樣可以快速檢視系統運行狀況和錯誤（如果有）。

```
# show logging
```

步驟3.驗證是否已啟用任何調試條件。

```
# 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
```

```
-----|-----
```

**註：**如果您看到列出了任何條件，則表示遇到啟用條件（mac地址、IP地址等）的所有進程的跟蹤將記錄到調試級別。如此可能會增加記錄量。因此，建議您在未主動偵錯時清除所有條件。

步驟4.如果測試的mac地址未作為步驟3中的條件列出，請收集特定mac地址的always-on通知級別跟蹤。

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

您可顯示作業階段中的內容，或可將檔案複製到外部 TFTP 伺服器。

```
# more bootflash:always-on-<FILENAME.txt>
```

```
or
```

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

## 條件式偵錯和無線電主動式追蹤

如果永遠線上(always-on)跟蹤未為您提供足夠的資訊來確定所調查問題的觸發因素，則可以啟用條件調試並捕獲無線活動(RA)跟蹤，該跟蹤為與指定條件（本例中為客戶端mac地址）互動的所有進程提供調試級別跟蹤。要啟用條件調試，請執行以下步驟。

步驟1.確保未啟用調試條件。

```
# clear platform condition all
```

步驟2.為要監控的無線客戶端mac地址啟用調試條件。

以下命令會開始監控提供的 MAC 位址 30 分鐘（1800 秒）。您可選擇將此時間增加至 2085978494 秒。

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

**注意:**若要一次監控多個使用者端，請對每個mac位址執行debug wireless mac <aaaa.bbb.cccc>命令。

**注意:**您看不到終端會話上客戶端活動的輸出，因為所有內容都在內部緩衝，供以後檢視。

步驟3.重現您要監控的問題或行為。

步驟4.如果在預設或配置的監控器時間開啟之前重現問題，則停止調試。

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

當監控時間結束或偵錯無線停止後，9800 WLC 會產生本機檔案，名稱如下：

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步驟5. 收集 MAC 位址活動的檔案。 您可將 ra\_trace.log 複製到外部伺服器，或將輸出內容直接顯示於螢幕上。

檢查RA跟蹤檔案的名稱

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

將檔案複製到外部伺服器：

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

顯示內容：

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

步驟6.如果根本原因仍不明顯，請收集內部日誌，這些日誌是調試級別日誌的更詳細檢視。您無需再次調試客戶端，因為我們只需進一步詳細檢視已收集並內部儲存的調試日誌。

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

**注意：**此命令輸出返回所有進程的所有日誌記錄級別的跟蹤，而且非常大。請聯絡 Cisco TAC 協助剖析此類追蹤。

您可將 ra-internal-FILENAME.txt 複製到外部伺服器，或將輸出內容直接顯示於螢幕上。

將檔案複製到外部伺服器：

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

顯示內容：

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

步驟7. 移除偵錯條件。

```
# clear platform condition all
```

**注意：**請確保在故障排除會話後始終刪除調試條件。

## 成功嘗試的示例

這是RA\_trace的輸出，表示在連線到沒有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。

802.11關聯/身份驗證：

```
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, llr = False, llw = False  
DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED  
Station Dot11 association is successful
```

IP學習流程：

```
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層身份驗證：

```
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層身份驗證成功，將客戶端移動到RUN狀態：**

```
[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
```

## 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）。