

# Configuration du portail captif DNA Spaces avec le WLC Catalyst 9800

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Connexion du contrôleur 9800 à Cisco DNA Spaces](#)

[Créer le SSID sur les espaces DNA](#)

[Configuration des listes de contrôle d'accès et des filtres URL sur le contrôleur 9800](#)

[Portail captif sans serveur RADIUS sur les espaces DNA](#)

[Configuration de la carte de paramètres d'authentification Web sur le contrôleur 9800](#)

[Créer le SSID sur le contrôleur 9800](#)

[Configuration du profil de stratégie sur le contrôleur 9800](#)

[Configurez la balise de stratégie sur le contrôleur 9800](#)

[Portail captif avec serveur RADIUS sur les espaces DNA](#)

[Configuration de la carte de paramètres d'authentification Web sur le contrôleur 9800](#)

[Configuration des serveurs RADIUS sur le contrôleur 9800](#)

[Créer le SSID sur le contrôleur 9800](#)

[Configuration du profil de stratégie sur le contrôleur 9800](#)

[Configurez la balise de stratégie sur le contrôleur 9800](#)

[Configurez la carte de paramètres globale](#)

[Créer le portail sur DNA Spaces](#)

[Configuration des règles du portail captif sur les espaces DNA](#)

[Obtenir des informations spécifiques de DNA Spaces](#)

[Quelles sont les adresses IP utilisées par les espaces DNA ?](#)

[Quelle est l'URL utilisée par le portail de connexion DNA Spaces ?](#)

[Quels sont les détails du serveur RADIUS pour les espaces DNA ?](#)

[Vérifier](#)

[Dépannage](#)

[Problèmes courants](#)

[Suivi toujours actif](#)

[Débogage conditionnel et traçage Radio Active](#)

[Exemple d'une tentative réussie](#)

## Introduction

Ce document décrit comment configurer des portails captifs sur Cisco DNA Spaces.

# Conditions préalables

Ce document permet aux clients sur le contrôleur LAN sans fil Catalyst 9800 (C9800 WLC) d'utiliser les espaces DNA comme page de connexion d'authentification Web externe.

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès aux contrôleurs sans fil 9800 via l'interface de ligne de commande ou l'interface utilisateur graphique
- Espaces Cisco DNA

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur 9800-L version 16.12.2s

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

L'authentification Web est une méthode d'authentification de couche 3 simple qui ne nécessite pas d'utilitaire demandeur ou client. Cela peut être fait

- a) Avec la page interne sur le WLC C9800 soit tel quel, soit après les modifications
- b) Avec le bundle de connexion personnalisé téléchargé sur le WLC C9800
- c) Page de connexion personnalisée hébergée sur un serveur externe

Exploiter le portail captif fourni par DNA Spaces est essentiellement un moyen de mettre en oeuvre une authentification Web externe pour les clients sur le WLC C9800.

Le processus d'authentification Web externe est décrit en détail à l'adresse :

<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>

Sur le WLC C9800, l'adresse ip virtuelle est définie comme la carte-paramètre globale et est généralement 192.0.2.1

## Configurer

### Diagramme du réseau



## Connexion du contrôleur 9800 à Cisco DNA Spaces

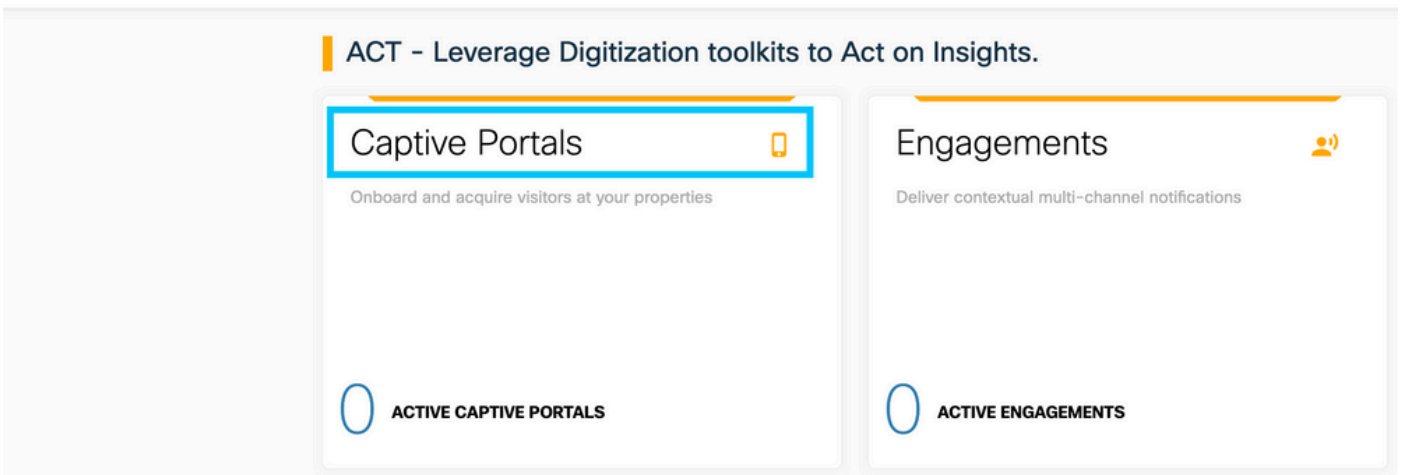
Le contrôleur doit être connecté à DNA Spaces avec l'une des options suivantes : Direct Connect, via DNA Spaces Connector ou avec CMX Tethering.

Dans cet exemple, l'option Connexion directe est utilisée, bien que les portails captifs soient configurés de la même manière pour toutes les configurations.

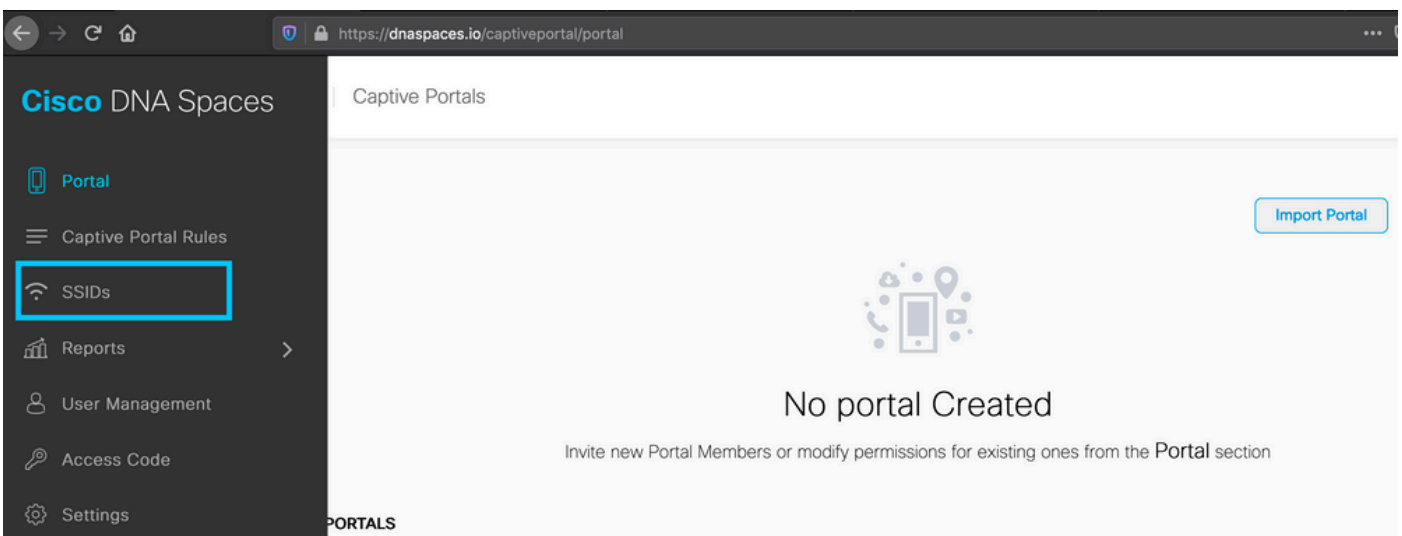
Pour connecter le contrôleur à Cisco DNA Spaces, il doit pouvoir accéder au cloud Cisco DNA Spaces via HTTPS. Pour plus d'informations sur la façon de connecter le contrôleur 9800 aux espaces DNA, reportez-vous à ce lien : [Espaces DNA - Connexion directe du contrôleur 9800](#)

## Créer le SSID sur les espaces DNA

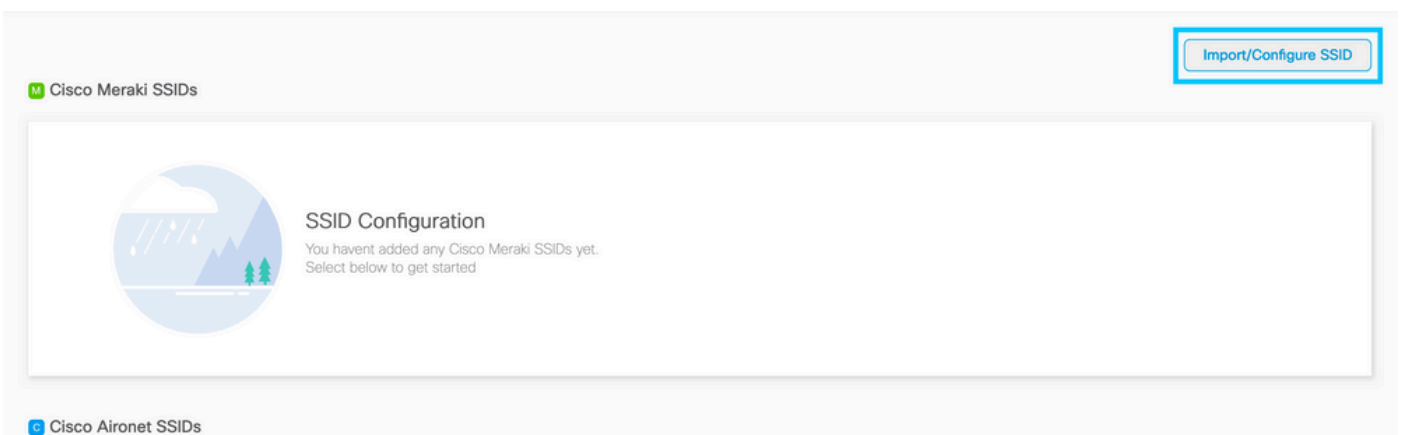
Étape 1. Cliquez sur **Captive Portals** dans le tableau de bord de DNA Spaces :



Étape 2. Ouvrez le menu spécifique au portail captif, cliquez sur l'icône des trois lignes dans le coin supérieur gauche de la page et cliquez sur **SSID** :



Étape 3. Cliquez sur **Import/Configure SSID**, sélectionnez **CUWN (CMX/WLC)** comme type de « réseau sans fil » et entrez le nom SSID :



## Configuration des listes de contrôle d'accès et des filtres URL sur le contrôleur 9800

Le trafic provenant d'un client sans fil n'est pas autorisé sur le réseau tant qu'il n'a pas terminé l'authentification. Dans le cas de l'authentification Web, afin de la terminer, un client sans fil se

connecte à ce SSID, reçoit une adresse IP, puis l'état du gestionnaire de stratégie client est déplacé à l'état **Webauth\_reqd**. Comme le client n'est pas encore authentifié, tout le trafic provenant de l'adresse IP du client est abandonné, à l'exception de DHCP et DNS et HTTP (qui sont interceptés et redirigés).

Par défaut, le 9800 crée des listes de contrôle d'accès pré-auth codées en dur lorsque nous configurons un WLAN d'auth. web. Ces listes de contrôle d'accès codées en dur autorisent le DHCP, le DNS et le trafic vers le serveur d'authentification Web externe. Tout le reste est redirigé comme n'importe quel trafic http.

Toutefois, si vous devez autoriser un type de trafic non HTTP spécifique à traverser, vous pouvez configurer une liste de contrôle d'accès de pré-authentification. Vous devez ensuite imiter le contenu de la liste de contrôle d'accès pré-auth codée en dur existante (à partir de l'étape 1 de cette section) et l'ajouter à vos besoins.

## Étape 1. Vérifier les ACL codées en dur actuelles

Configuration CLI :

```
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 est appelé en tant que tel, car il s'agit d'une liste de contrôle d'accès de sécurité automatique pour l'authentification Web (WA) ou de l'adresse IP de portail « 34.235.248.212 ». Les listes de contrôle d'accès de sécurité définissent ce qui est autorisé (sur autorisation) ou abandonné (sur refus)

Wa-v4-int est une liste de contrôle d'accès d'interception, c'est-à-dire une liste de contrôle d'accès ponctuelle ou de redirection, qui définit ce qui est envoyé au processeur pour redirection (sur autorisation) ou ce qui est envoyé au plan de données (sur refus).

WA-v4-int34.235.248.212 est appliqué en premier sur le trafic provenant du client et conserve le trafic HTTP(s) vers le portail DNA Spaces IP 34.235.248.212 sur le plan de données (pas encore d'action « drop » ou « forward », juste passer au plan de données). Il envoie à l'UC (pour la redirection, sauf le trafic IP virtuel qui est desservi par le serveur Web) tout le trafic HTTP. D'autres types de trafic sont donnés au plan de données.

WA-sec-34.235.248.212 autorise le trafic HTTP et HTTPS vers l'espace d'ADN IP 34.235.248.212 que vous avez configuré dans la carte de paramètre d'authentification Web, autorise également le trafic DNS et DHCP et supprime le reste. Le trafic HTTP à intercepter a déjà été intercepté avant d'atteindre cette liste de contrôle d'accès et n'a donc pas besoin d'être couvert par cette liste.

**Remarque** : pour obtenir les adresses IP des espaces DNA autorisés dans la liste de contrôle d'accès, cliquez sur l'option **Configure Manually (Configurer manuellement)** du SSID créé à l'étape 3 de la section **Create the SSID on DNA Spaces (Créer le SSID sur les espaces DNA)** sous la section ACL configuration. Un exemple se trouve dans la section « Quelles sont les adresses IP utilisées par les espaces ADN » à la fin du document.

DNA Spaces utilise 2 adresses IP et le mécanisme de l'étape 1 ne permet qu'une seule adresse IP de portail. Pour permettre l'accès de pré-authentification à davantage de ressources HTTP, vous devez utiliser des filtres d'URL qui font dynamiquement des trous dans les ACL d'interception (redirection) et de sécurité (pré-auth) pour les IP liées au site Web dont vous entrez l'URL dans le filtre d'URL. Les requêtes DNS sont surveillées dynamiquement pour que le 9800 apprenne l'adresse IP de ces URL et l'ajoute aux listes de contrôle d'accès dynamiquement.

Étape 2. Configurez le filtre d'URL pour autoriser le domaine d'espaces d'ADN. Accédez à Configuration > Security > URL Filters, cliquez sur **+Add** et configurez le nom de la liste, sélectionnez **PRE-AUTH** comme type, action comme **PERMIT** et l'URL **splash.dnaspaces.io** (ou .eu si vous utilisez le portail EMEA) :

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' is set to 'PERMIT' with a green toggle switch. The 'URLs' field contains the text 'splash.dnaspaces.io'. The interface includes a 'Cancel' button and an 'Apply to Device' button.

Configuration CLI :

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

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

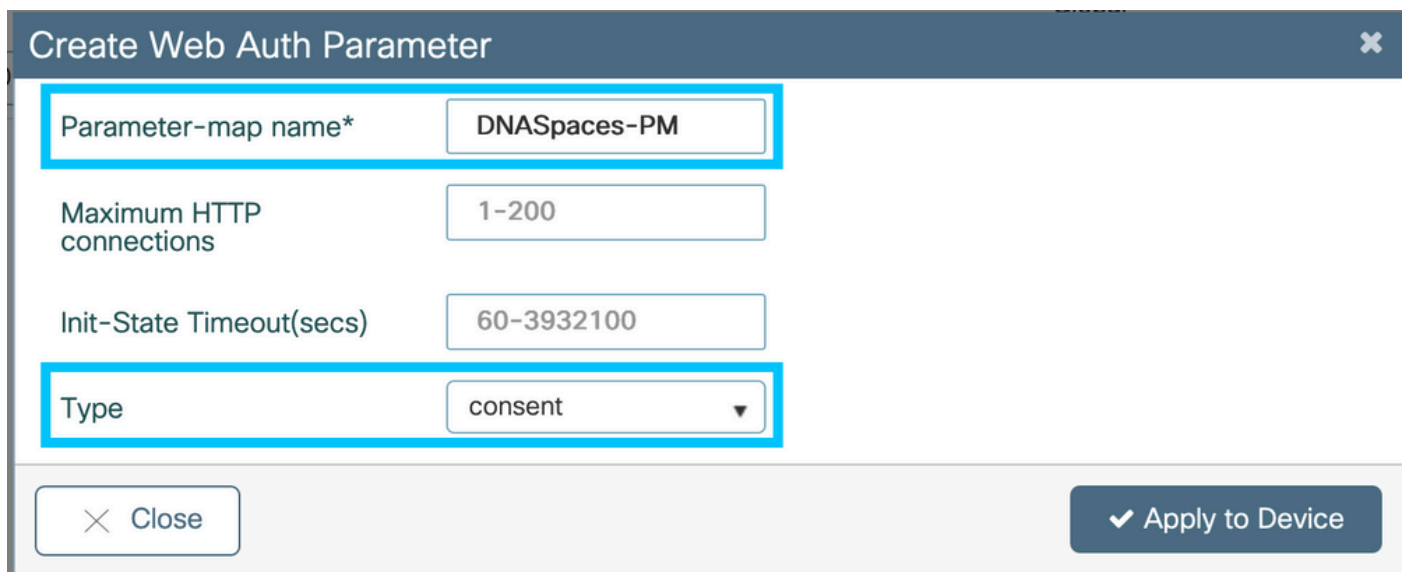
Andressi-9800L(config-urlfilter-params)#url splash.dnaspaces.io

Le SSID peut être configuré pour utiliser un serveur RADIUS ou non. Si la durée de session, la limite de bande passante ou la configuration transparente d'Internet est configurée dans la section **Actions** de la configuration de la règle du portail captif, le SSID doit être configuré avec un serveur RADIUS, sinon, il n'est pas nécessaire d'utiliser le serveur RADIUS. Tous les types de portails sur les espaces ADN sont pris en charge sur les deux configurations.

## Portail captif sans serveur RADIUS sur les espaces DNA

### Configuration de la carte de paramètres d'authentification Web sur le contrôleur 9800

Étape 1. Accédez à **Configuration > Security > Web Auth**, cliquez sur **+Add** pour créer une nouvelle carte de paramètres. Dans la fenêtre qui s'affiche, configurez le nom du mappage de paramètre et sélectionnez **Consent** comme type :



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

Étape 2. Cliquez sur le mappage de paramètres configuré à l'étape précédente, accédez à l'onglet **Advanced**, et entrez Redirect for log-in URL, Append for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID and portal IPv4 Address comme illustré. Cliquez sur **Update & Apply** :

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


XXXXXXXXXX

**Customized page**


Login Failed Page


Login Page


Logout Page

Login Successful Page

✕ Cancel

 Update & Apply



**Remarque** : pour obtenir l'URL de la page d'accueil et l'adresse de redirection IPv4, cliquez sur l'option **Configure Manually** dans la page SSID de DNA Spaces. Ceci est illustré dans la section « Quelle est l'URL utilisée par le portail DNA Spaces ? » à la fin du document

**Remarque** : le portail Cisco DNA Spaces peut se résoudre en deux adresses IP, mais le contrôleur 9800 ne permet de configurer qu'une seule adresse IP. Choisissez l'une de ces adresses IP et configurez-la sur la carte de paramètres en tant qu'adresse IPv4 du portail.

**Remarque** : assurez-vous que les adresses IPv4 et IPv6 virtuelles sont configurées dans la carte des paramètres d'authentification Web globale. Si l'IPv6 virtuel n'est pas configuré, les clients sont parfois redirigés vers le portail interne au lieu du portail des espaces DNA configuré. C'est pourquoi une adresse IP virtuelle doit toujours être configurée. « 192.0.2.1 » peut être configuré comme IPv4 virtuel et FE80:0:0:0:903A::11E4 comme IPV6 virtuel. Il n'y a pas ou peu de raisons d'utiliser d'autres adresses IP que celles-ci.

Configuration CLI :

```
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
```

## Créez le SSID sur le contrôleur 9800

Étape 1. Accédez à **Configuration > Tags & Profiles > WLANs**, cliquez sur **+Add**. Configurez le nom de profil, le SSID et activez le WLAN. Assurez-vous que le nom SSID est le même que celui configuré à l'étape 3 de la section **Créer le SSID sur les espaces DNA**.

### Add WLAN

General Security Advanced

Profile Name\* 9800DNASpaces

SSID\* 9800DNASpaces

WLAN ID\* 3

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED

Cancel Apply to Device

Étape 2. Accédez à **Security > Layer2**. Définissez le mode de sécurité de la couche 2 sur **None**, assurez-vous que le filtrage MAC est désactivé.

### Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode None

MAC Filtering

Transition Mode WLAN ID 0

Fast Transition Adaptive Enabled

Over the DS

Reassociation Timeout 20

Cancel Apply to Device

Étape 3. Accédez à **Security > Layer3**. Activez la stratégie Web, configurez la carte des paramètres d'authentification Web. Cliquez sur **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*

## Configuration du profil de stratégie sur le contrôleur 9800

Étape 1. Accédez à **Configuration > Tags & Profiles > Policy** et créez un nouveau profil de stratégie ou utilisez le profil de stratégie par défaut. Dans l'onglet Access Policies, configurez le VLAN client et ajoutez le filtre d'URL.

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 ▼

## Configurez la balise de stratégie sur le contrôleur 9800

Étape 1. Accédez à **Configuration > Tags & Profiles > Policy**. Créez une nouvelle balise de stratégie ou utilisez la balise de stratégie par défaut. Mappez le WLAN au profil de stratégie dans la balise de stratégie.

### 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

Étape 2. Appliquez la balise de stratégie au point d'accès pour diffuser le SSID. Accédez à **Configuration > Wireless > Access Points**, Sélectionnez le point d'accès en question et ajoutez la balise Policy. Cela entraîne le point d'accès à redémarrer son tunnel CAPWAP et à se joindre à nouveau au contrôleur 9800 :

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

Configuration CLI :

```
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
```

## Portail captif avec serveur RADIUS sur les espaces DNA

**Remarque** : le serveur RADIUS DNA Spaces prend uniquement en charge l'authentification PAP provenant du contrôleur.

### Configuration de la carte de paramètres d'authentification Web sur le contrôleur 9800

Étape 1. Créez une carte de paramètres d'authentification Web. Accédez à **Configuration > Security > Web Auth**, cliquez sur **+Add**, et configurez le nom de la carte de paramètre, et sélectionnez **webauth** comme type :

### 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

Étape 2. Cliquez sur le mappage de paramètres configuré à l'étape 1, cliquez sur **Advanced** et entrez Redirect for log-in, Append for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID and portal IPv4 Address. Cliquez sur **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



**Remarque** : pour obtenir l'URL de la page d'accueil et l'adresse de redirection IPv4, cliquez sur l'option **Configure Manually** du SSID créé à l'étape 3 de la section **Create the SSID on DNA Spaces** sous la section **Creating the SSIDs in WLC Direct Connect** section **Creating the Access Control List configuration** respectivement.

**Remarque** : le portail Cisco DNA Spaces peut être résolu en deux adresses IP, mais le contrôleur 9800 ne permet de configurer qu'une seule adresse IP. Dans un cas, choisissez n'importe laquelle de ces adresses IP à configurer sur la carte de paramètres en tant qu'adresse IPv4 du portail.

**Remarque** : Assurez-vous que les adresses IPv4 et IPv6 virtuelles sont configurées dans la carte de paramètres d'authentification Web globale. Si l'adresse IPv6 virtuelle n'est pas configurée, les clients sont parfois redirigés vers le portail interne au lieu du portail des espaces DNA configuré. C'est pourquoi une adresse IP virtuelle doit toujours être configurée. « 192.0.2.1 » peut être configuré comme IPv4 virtuel et FE80:0:0:0:903A::11E4 comme IPV6 virtuel. Il n'y a pas ou peu de raisons d'utiliser d'autres adresses IP que celles-ci.

#### Configuration CLI :

```
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
```

#### Configuration des serveurs RADIUS sur le contrôleur 9800

Étape 1. Configurer les serveurs RADIUS. Cisco DNA Spaces joue le rôle de serveur RADIUS pour l'authentification des utilisateurs et peut répondre sur deux adresses IP. Accédez à **Configuration > Security > AAA**, cliquez sur **+Add** et configurez les deux serveurs RADIUS :

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  

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

Cancel   Apply to Device

**Remarque** : pour obtenir l'adresse IP et la clé secrète RADIUS pour les serveurs principal et secondaire, cliquez sur l'option **Configure Manually** du SSID créé à l'étape 3 de la section **Create the SSID on DNA Spaces** et accédez à la section **RADIUS Server Configuration**.

Étape 2. Configurez le groupe de serveurs RADIUS et ajoutez les deux serveurs RADIUS. Accédez à **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups**, cliquez sur **+add**, configurez le nom du groupe de serveurs, MAC-Delimiter comme **Hyphen**, MAC-Filtering comme **MAC**, et attribuez les deux serveurs RADIUS :

+ 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

[Empty list box]

>

<

Assigned Servers

DNASpaces1  
DNASpaces2

Cancel

Apply to Device

Étape 3. Configurez une liste de méthodes d'authentification. Accédez à **Configuration > Security > AAA > AAA Method List > Authentication**, cliquez sur **+add**. Configurez le nom de la liste de méthodes, sélectionnez **login** comme type et attribuez le groupe de serveurs :

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

Étape 4. Configurez une liste de méthodes d'autorisation. Accédez à **Configuration > Security > AAA > AAA Method List > Authorization**, cliquez sur **+add**. Configurez le nom de la liste de méthodes, sélectionnez **network** comme type et attribuez le groupe de serveurs :

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

## Créez le SSID sur le contrôleur 9800

Étape 1. Accédez à **Configuration > Tags & Profiles > WLANs**, cliquez sur **+Add**. Configurez le nom de profil, le SSID et activez le WLAN. Assurez-vous que le nom SSID est le même que celui configuré à l'étape 3 de la section **Créer le SSID sur les espaces DNA**.

**Add WLAN** ✕

General Security Advanced

Profile Name\*  Radio Policy  ▼

SSID\*  Broadcast SSID

WLAN ID\*

Status

Étape 2. Accédez à **Security > Layer2**. Définissez le mode de sécurité de couche 2 sur **None**, activez le filtrage MAC et ajoutez la liste d'autorisations :

**Add WLAN** ✕

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode  ▼

MAC Filtering

Transition Mode WLAN ID

Authorization List\*  ▼

Fast Transition  ▼

Over the DS

Reassociation Timeout

Étape 3. Accédez à **Security > Layer3**. Activez la stratégie Web, configurez la carte des paramètres d'authentification Web et la liste d'authentification. Activez Échec du filtre sur Mac et ajoutez la liste de contrôle d'accès de préauthentification. Cliquez sur **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

## Configuration du profil de stratégie sur le contrôleur 9800

Étape 1. Accédez à **Configuration > Tags & Profiles > Policy** et créez un nouveau profil de stratégie ou utilisez le profil de stratégie par défaut. Dans l'onglet Access Policies, configurez le VLAN client et ajoutez le filtre d'URL.

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 ▼

Étape 2. Dans l'onglet Avancé, activez AAA Override et configurez éventuellement la liste des méthodes de comptabilisation :

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

## Configurez la balise de stratégie sur le contrôleur 9800

Étape 1. Accédez à **Configuration > Tags & Profiles > Policy**. Créez une nouvelle balise de stratégie ou utilisez la balise de stratégie par défaut. Mappez le WLAN au profil de stratégie dans la balise de stratégie.



### 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

Étape 2. Appliquez la balise de stratégie au point d'accès pour diffuser le SSID. Accédez à **Configuration > Wireless > Access Points**, Sélectionnez le point d'accès en question et ajoutez la balise Policy. Cela entraîne le point d'accès à redémarrer son tunnel CAPWAP et à se joindre à nouveau au contrôleur 9800 :

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

Configuration CLI :

```
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
```

## Configurez la carte de paramètres globale

Étape non recommandée : Exécutez ces commandes pour permettre la redirection HTTPS, mais notez que la redirection dans le trafic HTTPS client n'est pas nécessaire si le système d'exploitation client détecte un portail captif et entraîne une utilisation CPU plus importante et lance toujours un avertissement de certificat. Il est donc recommandé d'éviter de le configurer sauf si cela est nécessaire pour un cas d'utilisation très spécifique.

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

**Remarque** : vous devez disposer d'un certificat SSL valide pour l'adresse IP virtuelle installée dans le contrôleur sans fil de la gamme Cisco Catalyst 9800.

Étape 1. Copiez le fichier certifié signé portant l'extension .p12 sur un serveur TFTP et exécutez cette commande pour transférer et installer le certificat dans le contrôleur 9800 :

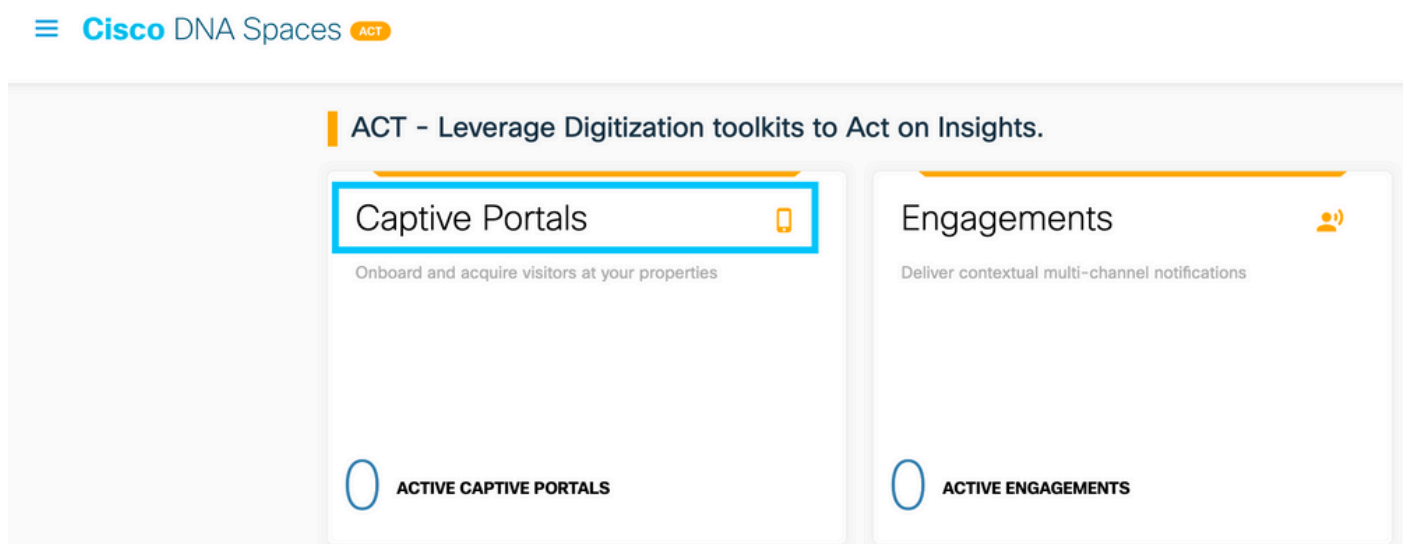
```
Andressi-9800L(config)#crypto pki import
```

Étape 2. Pour mapper le certificat installé à la carte de paramètre d'authentification Web, exécutez ces commandes :

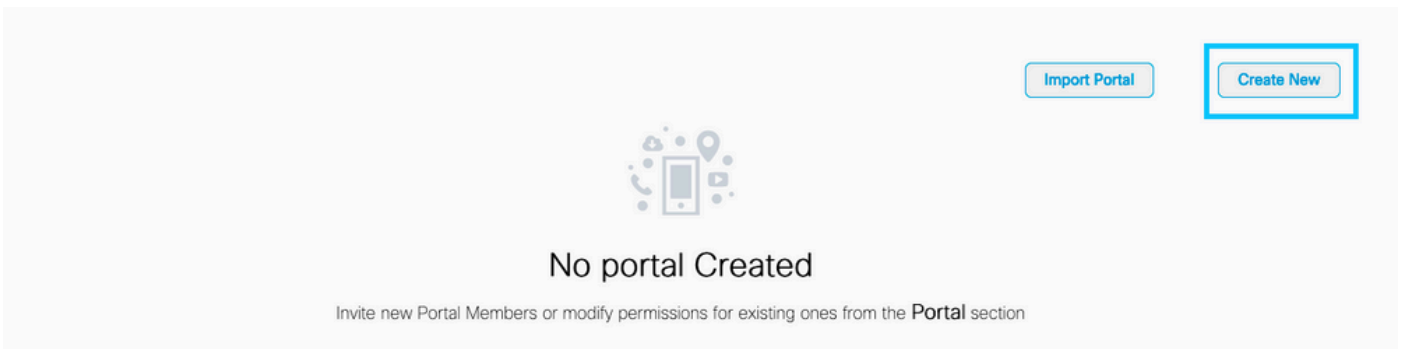
```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#trustpoint
```

## Créez le portail sur DNA Spaces

Étape 1. Cliquez sur **Captive Portals** dans le tableau de bord de DNA Spaces :



Étape 2. Cliquez sur **Create New**, entrez le nom du portail et sélectionnez les emplacements qui peuvent utiliser le portail :



Étape 3. Sélectionnez le type d'authentification, choisissez si vous souhaitez afficher la capture de données et les accords utilisateur sur la page d'accueil du portail et si les utilisateurs sont autorisés à s'inscrire pour recevoir un message. Cliquez sur **Suivant** :

Étape 4. Configurez les éléments de capture de données. Si vous voulez capturer des données des utilisateurs, cochez la case **Enable Data Capture** et cliquez sur **+Add Field Element** pour ajouter les champs désirés. Cliquez sur **Suivant** :

Étape 5. Cochez la case **Enable Terms & Conditions** et cliquez sur **Save & Configure Portal** :

✓ Portal Information   
 ✓ Authentication   
 ✓ Data Capture   
 4 User Agreements

This section allows you to enable and configure Terms & Conditions and Privacy policy Statements.

Enable Terms & Conditions

TERMS & CONDITION MESSAGE English

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.

Étape 6. Modifiez le portail si nécessaire, cliquez sur **Enregistrer** :

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

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

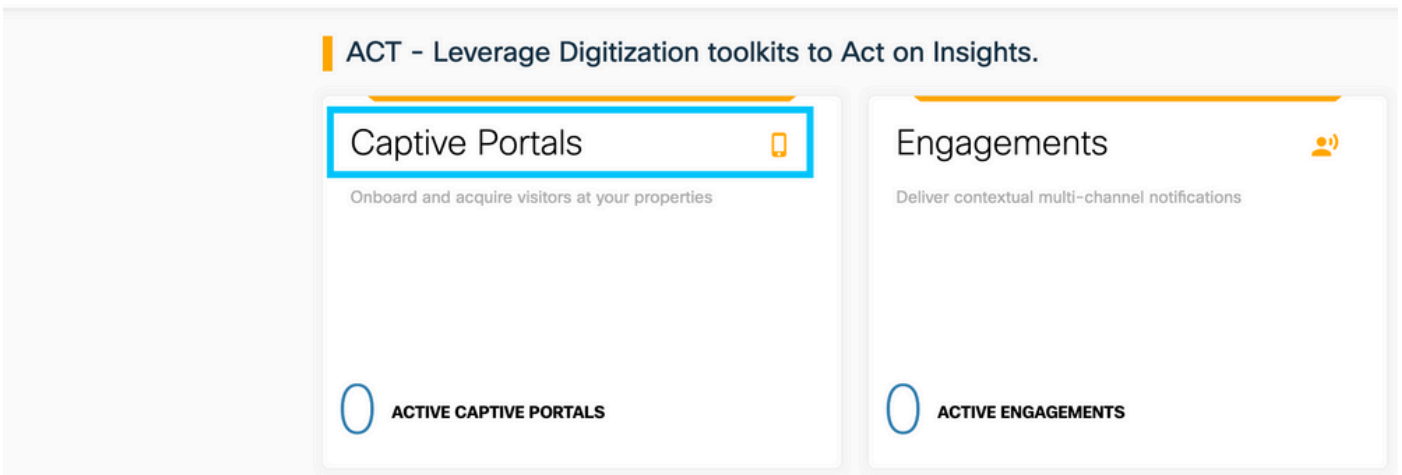
**SIGN-UP FOR WIFI**

Email Address

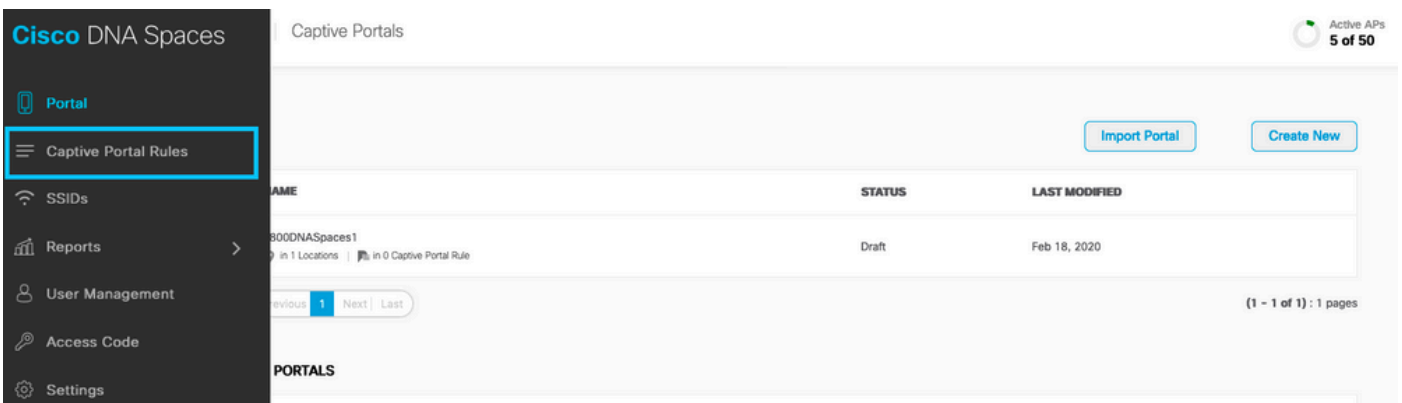
Mobile Number

## Configuration des règles du portail captif sur les espaces DNA

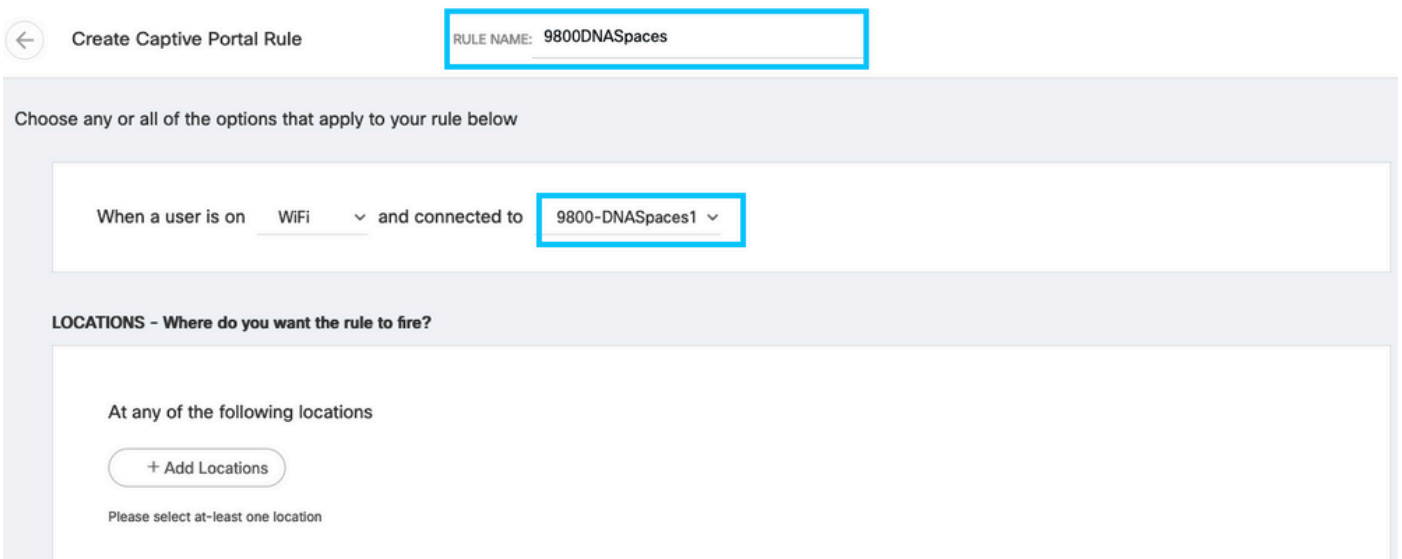
Étape 1. Cliquez sur **Captive Portals** dans le tableau de bord de DNA Spaces :



Étape 2. Ouvrez le menu du portail captif et cliquez sur **Règles du portail captif** :



Étape 3. Cliquez sur **+ Créer une règle**. Entrez le nom de la règle, puis choisissez le SSID précédemment configuré.



Étape 4. Sélectionnez les emplacements dans lesquels le portail est disponible. Cliquez sur **+ Ajouter des emplacements** dans la section **EMPLACEMENTS**. Sélectionnez la hiérarchie souhaitée dans la hiérarchie des emplacements.

## Choose Locations

### Location Hierarchy

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

### Selected Locations

9800L-DirectConnect X

Étape 5. Sélectionnez l'action du portail captif. Dans ce cas, lorsque la règle est activée, le portail s'affiche. Cliquez sur **Enregistrer et publier**.

#### 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

## Obtenir des informations spécifiques de DNA Spaces

### Quelles sont les adresses IP utilisées par les espaces DNA ?

Afin de vérifier quelles adresses IP les espaces DNA utilisent pour le portail dans votre région, allez à la page du portail Captival sur la page d'accueil de l'espace DNA. Cliquez sur **SSID** dans le menu de gauche, puis cliquez sur **Configure manually** sous votre SSID. Les adresses IP sont mentionnées dans l'exemple de liste de contrôle d'accès. Il s'agit des adresses IP du portail à utiliser dans les listes de contrôle d'accès et la carte de paramètres webauth. Les espaces DNA utilisent une autre adresse IP pour la connectivité NMSP/cloud globale du plan de contrôle.





Dans la première section de la fenêtre contextuelle qui s'affiche, l'étape 7 vous montre les adresses IP mentionnées dans la définition de la liste de contrôle d'accès. Vous n'avez pas besoin de suivre ces instructions et de créer une liste de contrôle d'accès, il vous suffit de prendre note des adresses IP. Il s'agit des adresses IP utilisées par le portail de votre région

## 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

## Quelle est l'URL utilisée par le portail de connexion DNA Spaces ?

Afin de vérifier quelle URL de portail de connexion les espaces DNA utilisent pour le portail dans votre région, allez à la page du portail Captival sur la page d'accueil de l'espace DNA. Cliquez sur **SSID** dans le menu de gauche, puis cliquez sur **Configure manually** sous votre SSID.



Faites défiler vers le bas la fenêtre contextuelle qui apparaît et dans la deuxième section, l'étape 7 vous montre l'URL que vous devez configurer dans votre carte de paramètres sur le 9800.

### Creating the SSIDs in WLC Direct Connect

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

- 1 In the WLC Direct Connect main window, click the **WLANS** tab.
- 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.
- 3 In the New page that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.
- 4 Click **Apply**.  
The WLAN added appears in the WLANS page.
- 5 Click the WLAN you have newly created.
- 6 Choose **Security > Layer 2**, and configure the Layer 2 Security as **None**.
- 7 In the **Layer 3 tab**, do the following configurations:
  - a. From the Layer 3 security drop-down list, choose **Web Policy**.
  - b. Choose the **Passthrough** radio button.
  - c. In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL created earlier.
  - d. Select the Enable check box for the Sleeping Client.
  - e. Select the Enable check box for the Override Global Config.
  - f. From the Web Auth Type drop-down list, choose **External**.
  - g. In the URL field that appears, enter the Cisco DNA Spaces splash URL.

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

### Quels sont les détails du serveur RADIUS pour les espaces DNA ?

Pour connaître les adresses IP du serveur RADIUS que vous devez utiliser ainsi que le secret partagé, rendez-vous sur la page du portail Captival à la page d'accueil de DNA Space. Cliquez sur **SSID** dans le menu de gauche, puis cliquez sur **Configure manually** sous votre SSID.



Dans la fenêtre contextuelle qui s'affiche, faites défiler la section 3 (RADIUS) vers le bas et l'étape 7 vous indique l'adresse IP/port et le secret partagé pour l'authentification RADIUS. La comptabilité est facultative et est traitée à l'étape 12.

- 7 In the New page that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1812
Secret Key: emeab1299E2PqvJK

- 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: emeab1299E2PqvJK

## Vérifier

Pour confirmer l'état d'un client connecté au SSID, accédez à **Monitoring > Clients**, cliquez sur l'adresse MAC du périphérique et recherchez Policy Manager State :

Client	
360 View <b>General</b> QOS Statistics   ATF Statistics   Mobility History   Call Statistics	
Client Properties   AP Properties   Security Information   Client Statistics   QOS Properties	
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

## Dépannage

### Problèmes courants

1. Si aucune adresse IP n'est configurée sur l'interface virtuelle du contrôleur, les clients sont redirigés vers le portail interne au lieu du portail de redirection configuré dans la carte de paramètres.
2. Si les clients reçoivent une *erreur 503* alors qu'ils sont redirigés vers le portail sur les espaces DNA, assurez-vous que le contrôleur est configuré dans la **hiérarchie des emplacements** sur les espaces DNA.

### Suivi toujours actif

Le contrôleur WLC 9800 offre des fonctionnalités de traçage TOUJOURS ACTIVES. Cela garantit que tous les messages d'erreur, d'avertissement et de niveau de notification liés à la connectivité du client sont constamment consignés et que vous pouvez afficher les journaux d'un incident ou d'une défaillance après qu'il se soit produit.

**Remarque** : selon le volume de journaux générés, vous pouvez revenir en arrière de quelques heures à plusieurs jours.

Afin d'afficher les traces que le WLC 9800 a collectées par défaut, vous pouvez vous connecter via SSH/Telnet au WLC 9800 et effectuer ces étapes (Assurez-vous que vous consignez la session dans un fichier texte).

Étape 1. Vérifiez l'heure actuelle du contrôleur de sorte que vous puissiez suivre les journaux dans l'heure jusqu'à quand le problème s'est produit.

```
# show clock
```

Étape 2. Collectez les syslogs à partir de la mémoire tampon du contrôleur ou du syslog externe, comme dicté par la configuration système. Cela permet d'obtenir un aperçu rapide de l'état du système et des erreurs éventuelles.

```
# show logging
```

Étape 3. Vérifiez si les conditions de débogage sont activées.

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

**Remarque** : si une condition est répertoriée, cela signifie que les traces sont enregistrées au niveau de débogage pour tous les processus qui rencontrent les conditions activées (adresse MAC, adresse IP, etc.). Cela augmenterait le volume de journaux. Par conséquent, il est recommandé d'effacer toutes les conditions lorsque le débogage n'est pas actif.

Étape 4. Si l'adresse MAC testée n'était pas répertoriée comme condition à l'étape 3, collectez les traces de niveau de notification toujours actif pour l'adresse MAC spécifique.

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

Vous pouvez soit afficher le contenu de la session, soit copier le fichier sur un serveur TFTP externe.

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

## Débogage conditionnel et traçage Radio Active

Si les traces toujours actives ne vous donnent pas suffisamment d'informations pour déterminer le déclencheur du problème en cours d'investigation, vous pouvez activer le débogage conditionnel et capturer la trace Radio Active (RA), qui fournit des traces de niveau de débogage pour tous les processus qui interagissent avec la condition spécifiée (adresse MAC du client dans ce cas). Pour activer le débogage conditionnel, procédez comme suit.

Étape 1. Assurez-vous qu'aucune condition de débogage n'est activée.

```
# clear platform condition all
```

Étape 2. Activez la condition de débogage pour l'adresse MAC du client sans fil que vous

souhaitez surveiller.

Ces commandes commencent à surveiller l'adresse MAC fournie pendant 30 minutes (1 800 secondes). Vous pouvez aussi augmenter ce délai pour qu'il atteigne jusqu'à 2085978494 secondes.

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

**Remarque** : Afin de surveiller plusieurs clients à la fois, exécutez la <aaaa.bbbb.cccc>commande de débogage sans fil mac par adresse MAC.

**Remarque** : vous ne voyez pas le résultat de l'activité du client sur la session du terminal, car tout est mis en mémoire tampon en interne pour être visualisé ultérieurement.

Étape 3. Reproduisez le problème ou le comportement que vous souhaitez surveiller.

Étape 4. Arrêtez le débogage si le problème est reproduit avant la fin du temps de surveillance par défaut ou configuré.

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

Une fois que le temps de surveillance s'est écoulé ou que le débogage sans fil a été arrêté, le contrôleur WLC 9800 génère un fichier local du nom de :

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Étape 5. Recueillir le fichier de l'activité de l'adresse MAC. Il est possible de copier le fichier de suivi RA .log sur un serveur externe ou d'afficher le résultat directement à l'écran.

Vérifiez le nom du fichier de suivi RA

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

Copiez le fichier sur un serveur externe :

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

Affichez-en le contenu :

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

Étape 6. Si vous ne trouvez toujours pas la cause première, collectez les journaux internes, qui peuvent vous offrir une vue plus détaillée des journaux de niveau de débogage. Vous n'avez pas besoin de déboguer à nouveau le client, car nous nous contentons d'examiner plus en détail les journaux de débogage qui ont déjà été collectés et stockés en interne.

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

to-file ra-internal-<FILENAME>.txt

**Remarque** : cette sortie de commande retourne des traces pour tous les niveaux de journalisation pour tous les processus et est assez volumineuse. Veuillez faire appel à Cisco TAC pour faciliter l'analyse de ces suivis.

Vous pouvez soit copier le fichier ra-internal-FILENAME.txt sur un serveur externe, soit afficher le résultat directement à l'écran.

Copiez le fichier sur un serveur externe :

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

Affichez-en le contenu :

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

Étape 7. Supprimez les conditions de débogage.

```
# clear platform condition all
```

**Remarque** : assurez-vous de toujours supprimer les conditions de débogage après une session de dépannage.

## Exemple d'une tentative réussie

Il s'agit du résultat de RA\_traces pour une tentative réussie d'identification de chacune des phases au cours du processus d'association/d'authentification lors de la connexion à un SSID sans serveur RADIUS.

Association/authentification 802.11 :

```
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
```

Processus d'apprentissage IP :

```
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
```

Authentification de couche 3 :

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

**Authentification de couche 3 réussie, déplacez le client à l'état d'exécution :**

[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



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.