Exemple de configuration du portail captif DNA Spaces avec contrôleur AireOS

Table des matières

Introduction

Ce document décrit comment configurer des portails captifs à l'aide de Cisco DNA Spaces avec un contrôleur AireOS.

Contribution de Andres Silva Ingénieur du centre d'assistance technique Cisco

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès aux contrôleurs sans fil 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 LAN sans fil 5520 version 8.10.12.0

Configurer

Diagramme du réseau

Configurations

Connectez le WLC à Cisco DNA Spaces

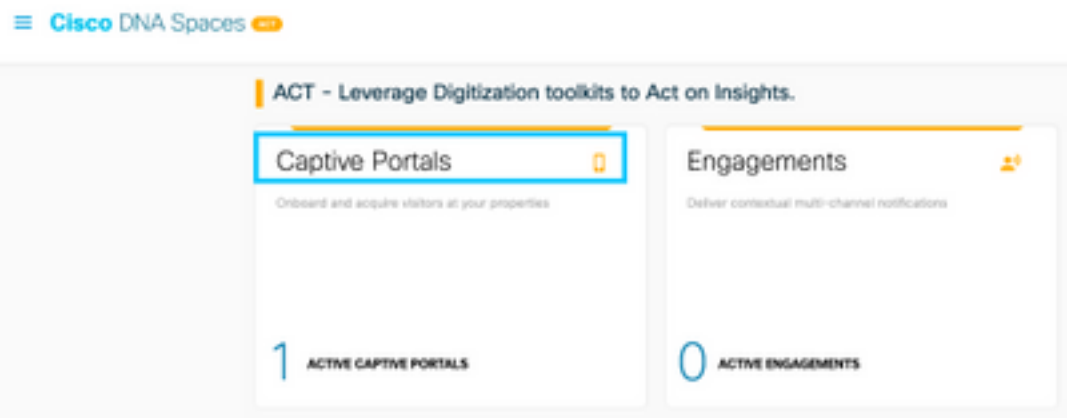
Le contrôleur doit être connecté à DNA Spaces à l'aide de l'une des configurations disponibles, Direct Connect, via DNA Spaces Connector ou à l'aide de CMX Tethering.

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

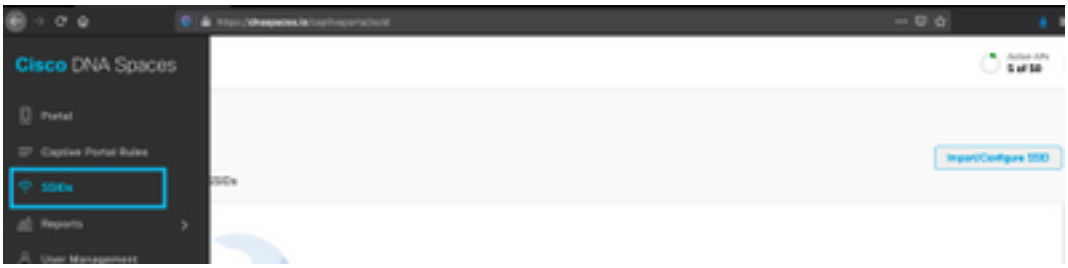
Pour connecter le contrôleur à Cisco DNA Spaces, il doit pouvoir accéder au cloud Cisco DNA Spaces via HTTPS. Pour plus d'informations sur la façon de connecter le contrôleur à des espaces DNA, référez-vous à ce lien : Exemple de configuration de connexion directe des espaces DNA

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 du portail captif en cliquant sur l'icône des trois lignes dans le coin supérieur gauche de la page, puis cliquez sur **SSID :**

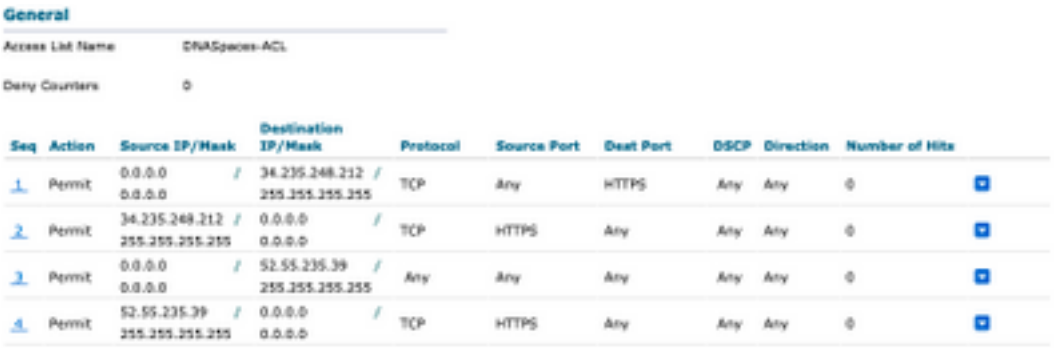


Étape 3. Cliquez sur **Import/Configure SSID**, sélectionnez **CUWN (CMX/WLC)** comme type de « réseau sans fil » et entrez le nom SSID :

Configuration ACL sur le contrôleur

Une ACL de pré-authentification est requise car il s'agit d'un SSID d'authentification Web, et dès que le périphérique sans fil se connecte au SSID et reçoit une adresse IP, l'état du gestionnaire de politiques du périphérique passe à l'état **Webauth_Reqd** et l'ACL est appliquée à la session client pour restreindre les ressources que le périphérique peut atteindre.

Étape 1. Accédez à **Security > Access Control Lists > Access Control Lists,** cliquez sur **New** et configurez les règles pour autoriser la communication entre les clients sans fil et les espaces DNA comme suit. Remplacez les adresses IP par celles fournies par les espaces DNA pour le compte utilisé :



> **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.

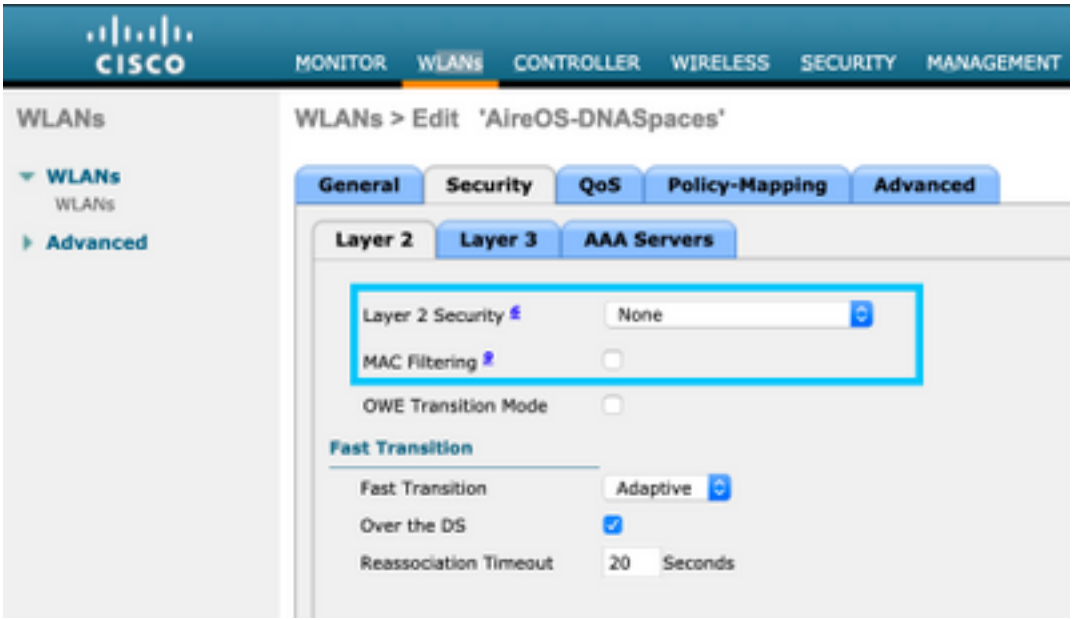
Le SSID peut être configuré pour utiliser un serveur RADIUS ou non. Si la durée de session, la limite de bande passante ou la configuration transparente d'Internet est configurée dans la section **Actions** de la configuration de la règle du portail captif, le SSID doit être configuré avec un serveur 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 SSID sur le contrôleur

Étape 1. Accédez à **WLAN > WLANs.** Créez un nouveau WLAN. Configurez le nom de profil et le SSID. Assurez-vous que le nom SSID est le même que celui configuré à l'étape 3 de la section **Créer le SSID sur des espaces d'ADN.**

Étape 2. Configurer la sécurité de couche 2 Accédez à l'onglet **Security > Layer 2** dans l'onglet WLAN configuration et sélectionnez **None** dans le menu déroulant de Layer 2 Security**.** Vérifiez que le filtrage MAC est désactivé.



Étape 3. Configurer la sécurité de couche 3 Accédez à l'onglet Security > Layer 3 dans l'onglet WLAN configuration, configure Web **Policy as the Layer 3 security method, Enable Passthrough, configure the preauthentication ACL, enable Override Global Config** as set the **Web Auth Type** as **External,** configure the Redirect URL.

Remarque : pour obtenir l'URL de redirection, cliquez sur l'option **Configure Manually**, à partir du SSID créé à l'étape 3 de la section **Create the SSID on DNA Spaces,** sous la section SSID configuration.

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 des serveurs RADIUS sur le contrôleur

Étape 1. Accédez à **Security > AAA > RADIUS > Authentication,** cliquez sur **New** et entrez les informations du serveur RADIUS. Cisco DNA Spaces joue le rôle de serveur RADIUS pour

l'authentification des utilisateurs et peut répondre sur deux adresses IP. Configurez les deux serveurs RADIUS :

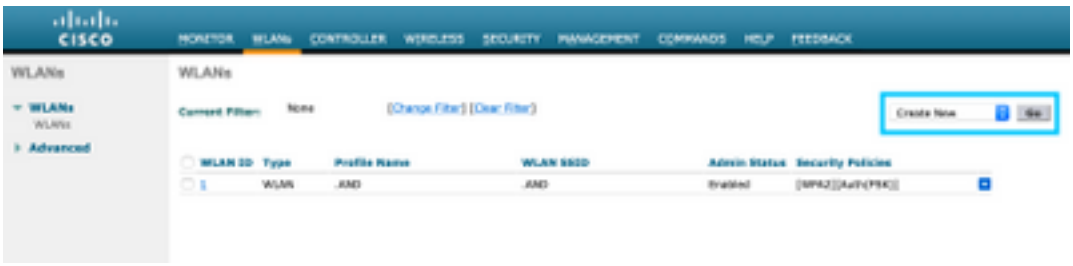
> **Remarque** : pour obtenir l'adresse IP et la clé secrète RADIUS pour les serveurs principal et secondaire, cliquez sur l'option **Configure Manually** du SSID créé à l'étape 3 de la section **Create the SSID on DNA Spaces** et accédez à la section **RADIUS Server Configuration**.

Étape 2. Configurez le serveur RADIUS de gestion des comptes. Accédez à **Security > AAA > RADIUS > Accounting** et cliquez sur **New**. Configurez les deux mêmes serveurs RADIUS :

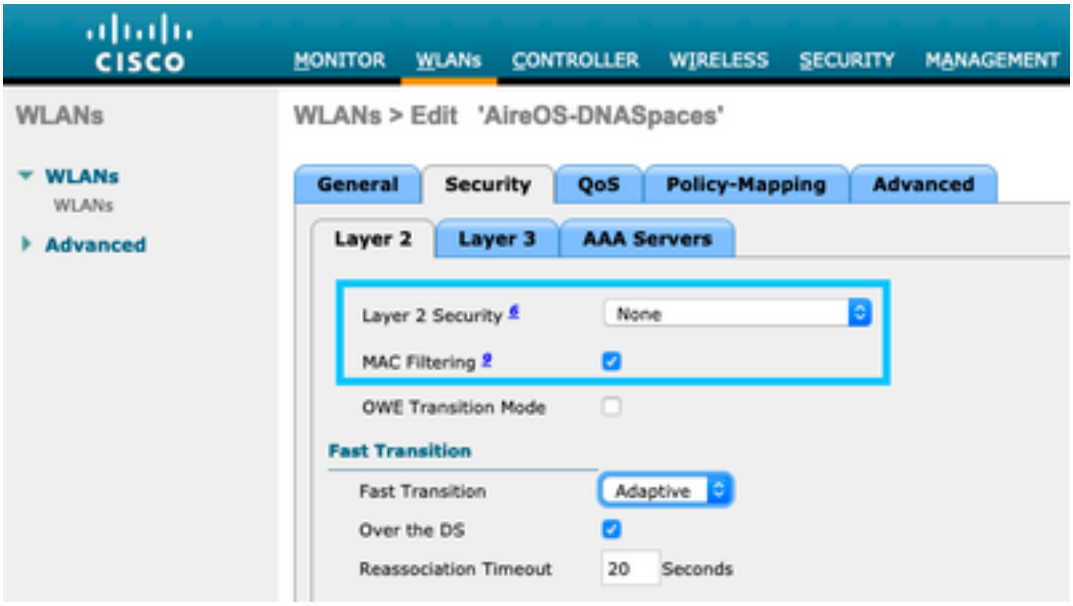
Configuration SSID sur le contrôleur

> **Important** : avant de commencer la configuration SSID, assurez-vous que l'**authentification Web Radius** est définie sur « PAP » sous Controller > General.

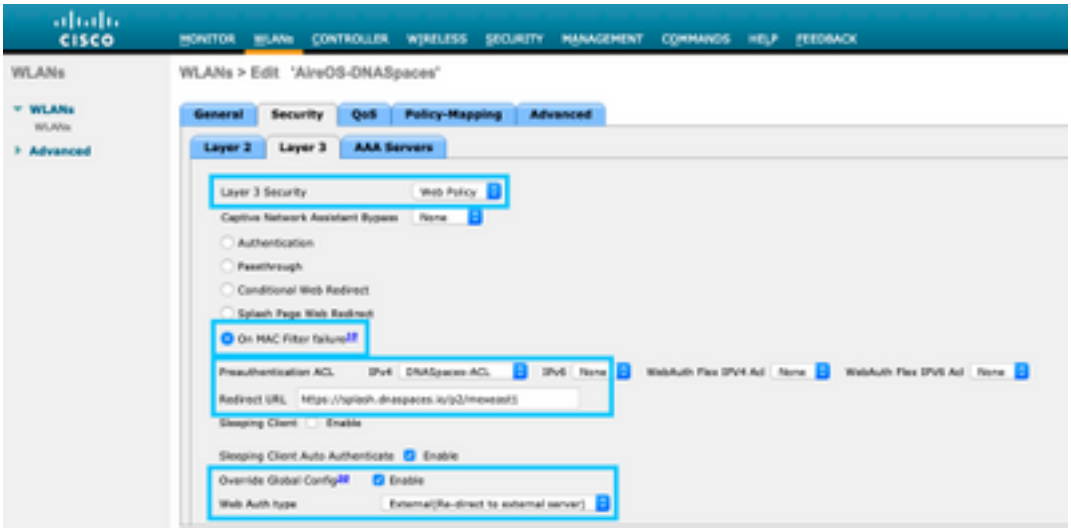
Étape 1. Accédez à **WLAN > WLANs.** Créez un nouveau WLAN. Configurez le nom de profil et le SSID. Assurez-vous que le nom SSID est le même que celui configuré à l'étape 3 de la section **Créer le SSID sur des espaces d'ADN.**



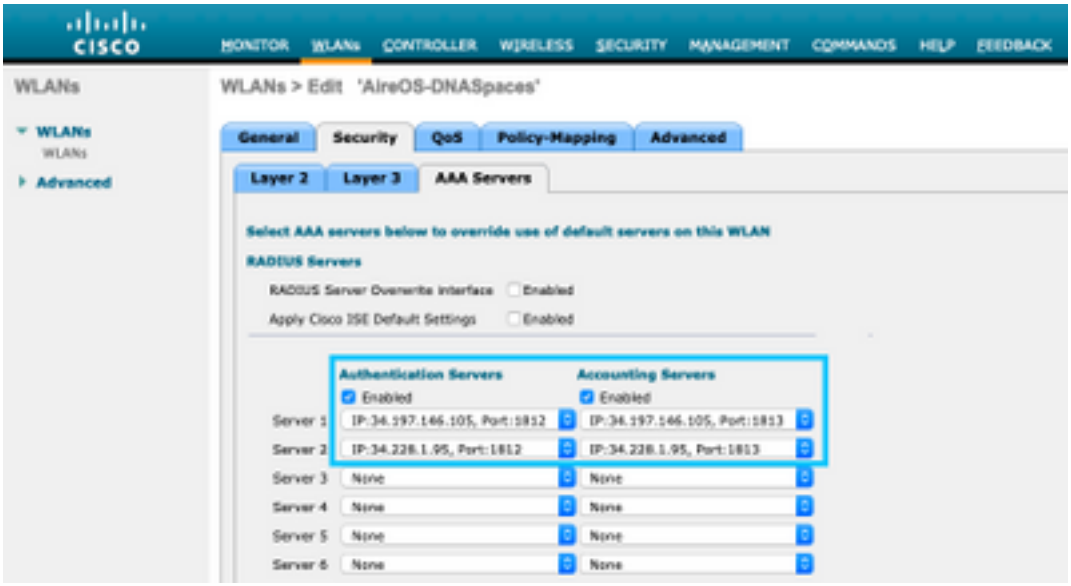
Étape 2. Configurer la sécurité de couche 2 Accédez à l'onglet **Security > Layer 2** dans l'onglet WLAN configuration. Configurez la sécurité de couche 2 sur **Aucun**. Activez le filtrage Mac.



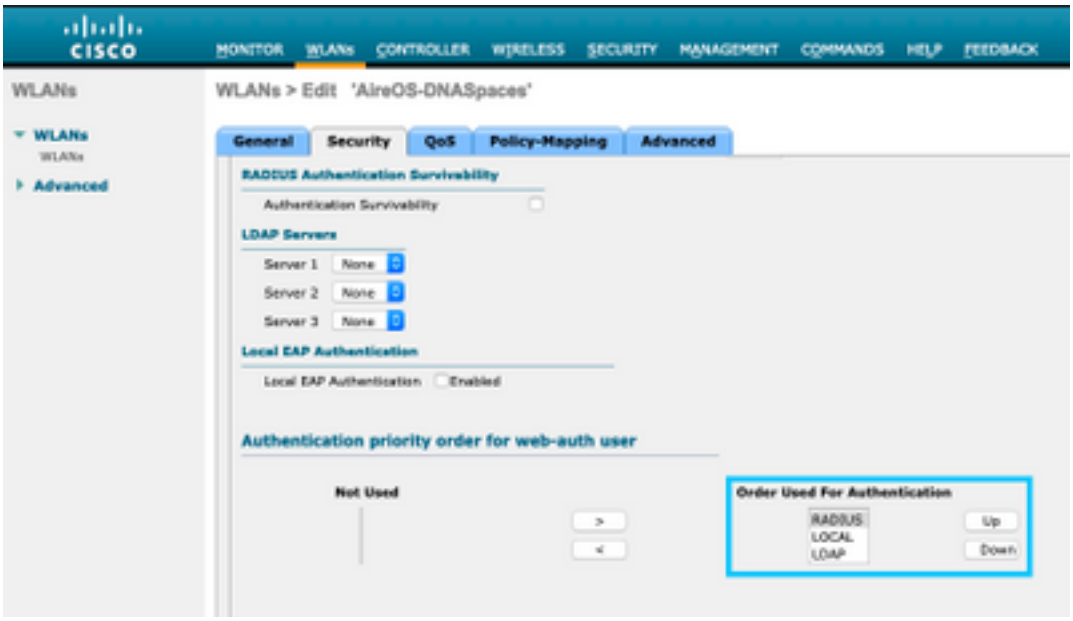
Étape 3. Configurer la sécurité de couche 3 Accédez à l'onglet Security > Layer 3 dans l'onglet WLAN configuration, configure Web **Policy as the Layer 3 security method, Enable On Mac Filter failure, configure the preauthentication ACL, enable Override Global Config** as set the **Web Auth Type** as **External,** configure the Redirect URL.



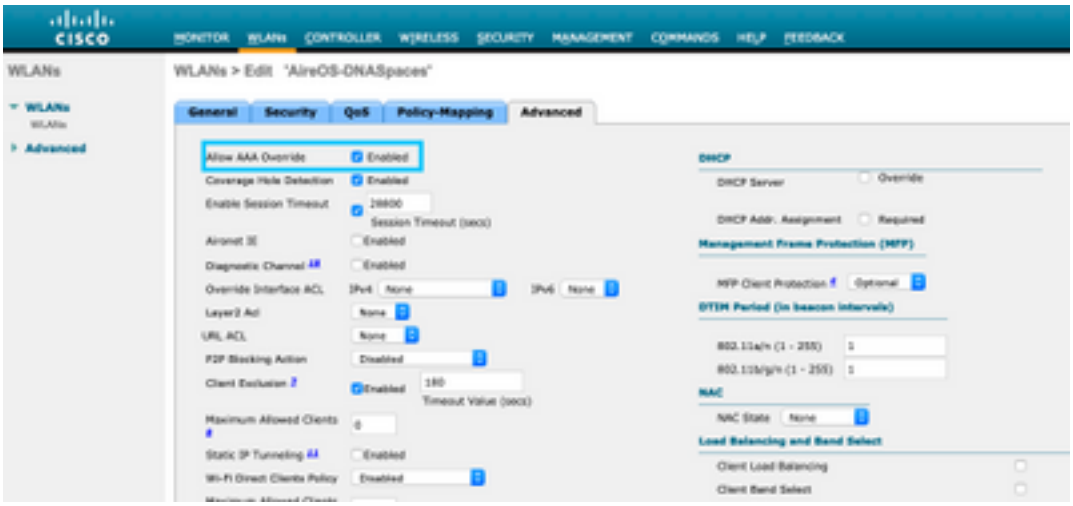
Étape 4. Configurer des serveurs AAA Accédez à l'onglet **Security > AAA Servers** dans l'onglet WLAN configuration, activez **Authentication Servers** and **Accounting Servers** et dans le menu déroulant choisissez les deux serveurs RADIUS :



Étape 6. Configurez l'**ordre de priorité d'authentification pour les utilisateurs Web-auth**. Accédez à l'onglet **Security > AAA Servers** dans l'onglet WLAN configuration, et définissez RADIUS en premier dans l'ordre.

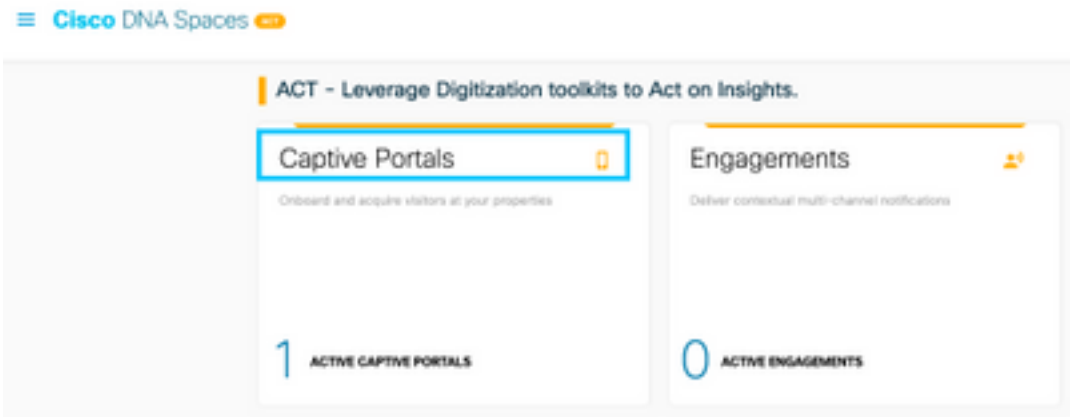


Étape 7. Accédez à l'onglet **Advanced** dans l'onglet WLAN configuration et activez **Allow AAA Override.**

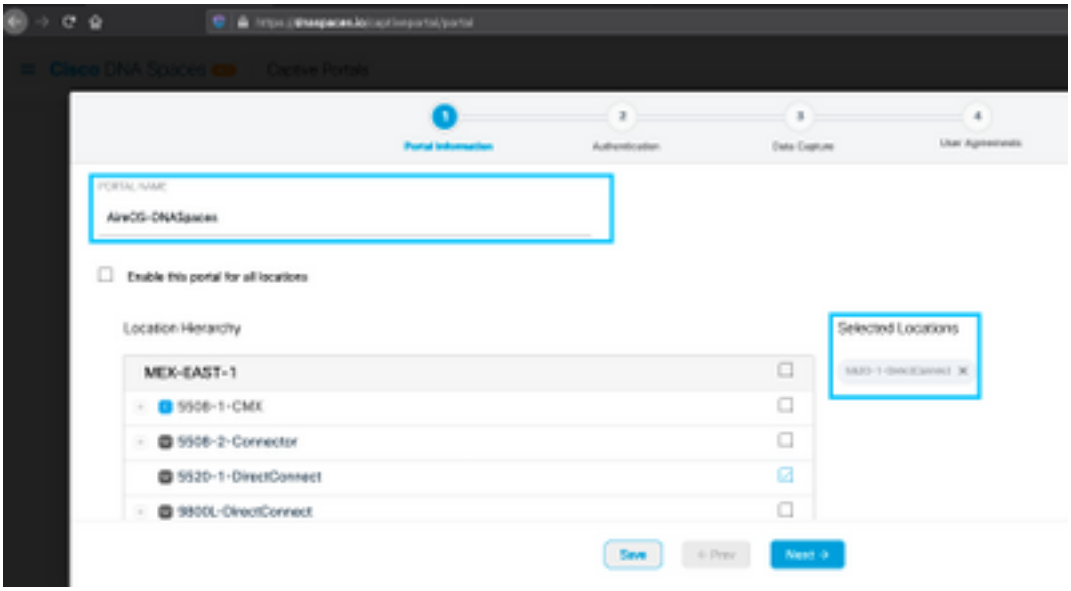


Créez le portail sur DNA Spaces

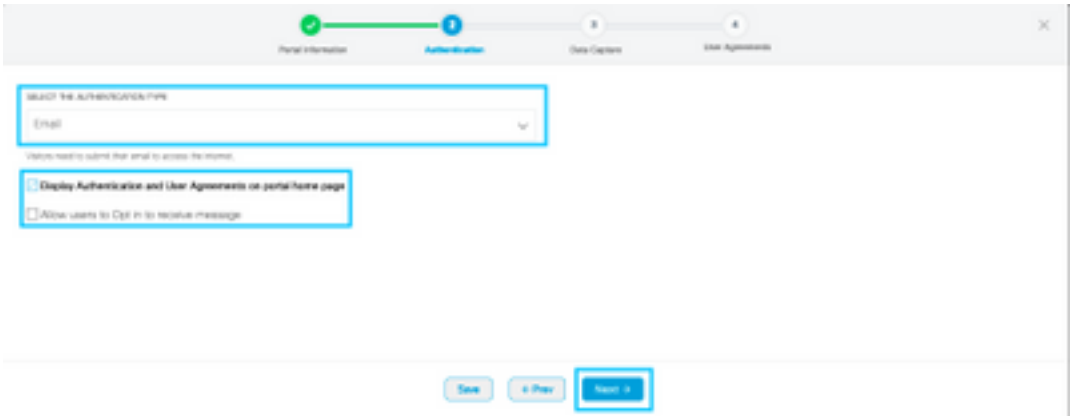
Étape 1. Cliquez sur **Captive Portals** dans le tableau de bord de DNA Spaces :



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

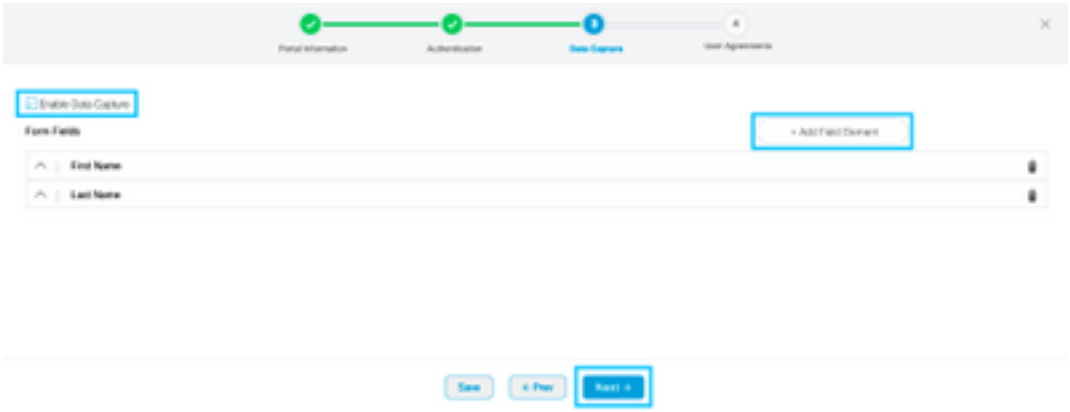


Étape 3. Sélectionnez le type d'authentification, choisissez si vous souhaitez afficher la capture de données et les accords utilisateur sur la page d'accueil du portail et si les utilisateurs sont autorisés à s'inscrire pour recevoir un message. Cliquez sur **Suivant** :



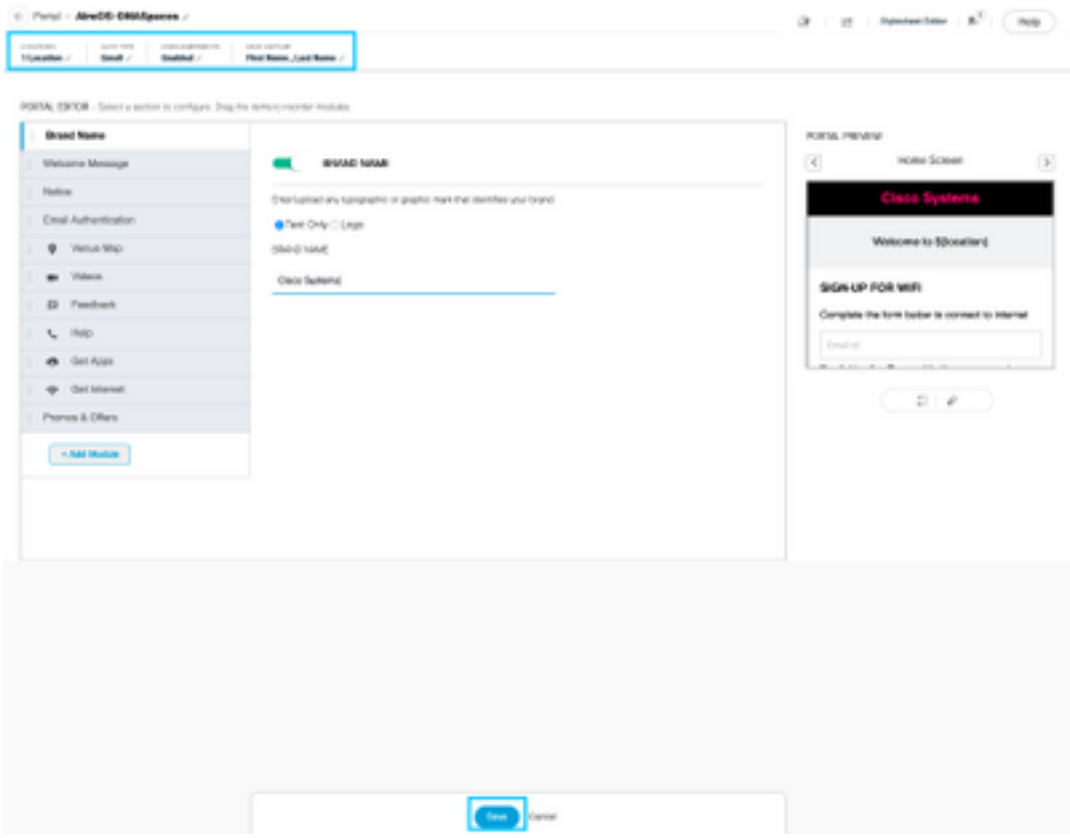
Étape 4. Configurez les éléments de capture de données. Si vous voulez capturer des données des utilisateurs, cochez la case **Enable Data Capture** et cliquez sur **+Add Field Element** pour

ajouter les champs désirés. Cliquez sur **Suivant** :



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

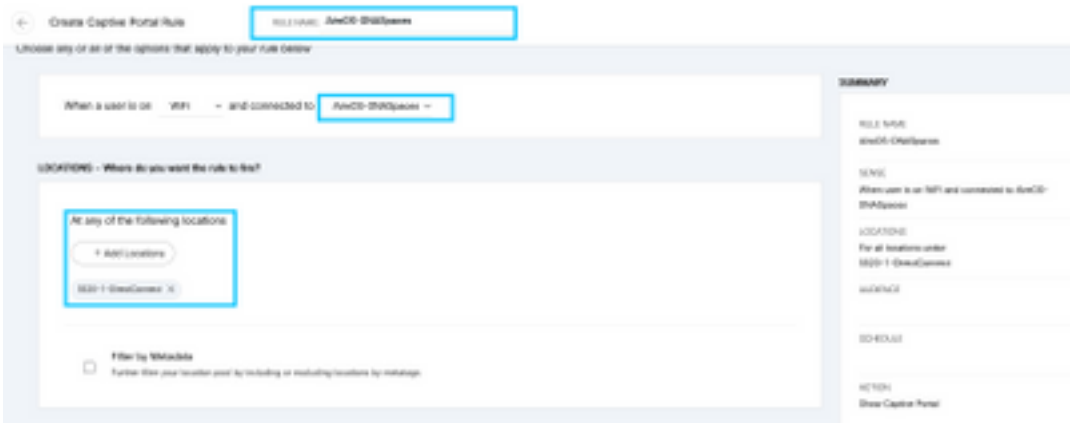
Étape 6. Modifiez le portail si nécessaire, cliquez sur **Enregistrer :**



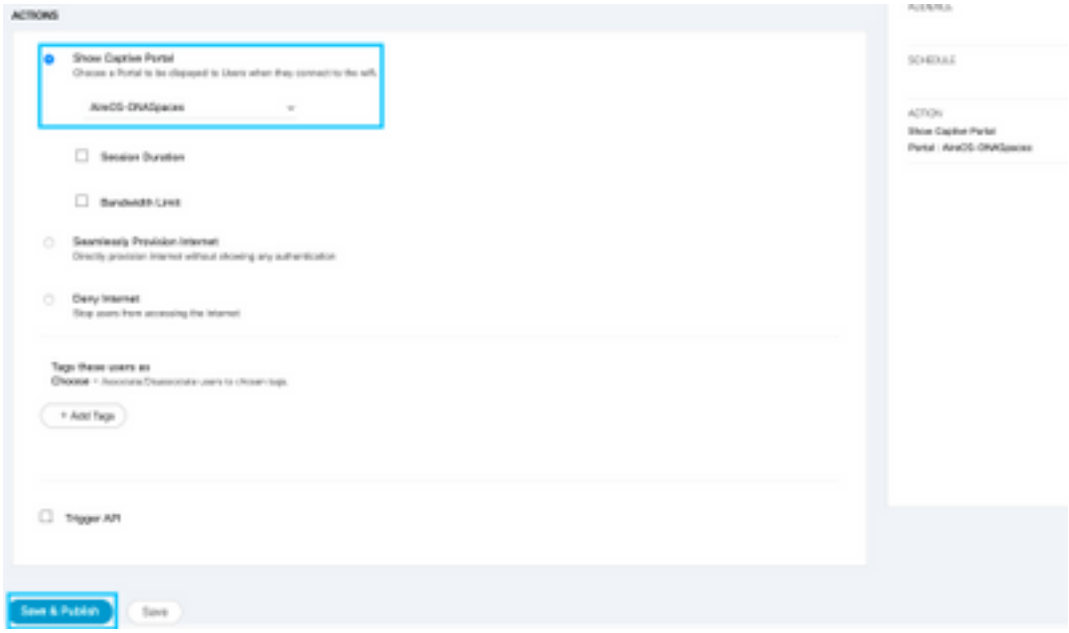
Configuration des règles du portail captif sur les espaces DNA

Étape 1. Ouvrez le menu du portail captif et cliquez sur **Règles du portail captif :**

Étape 2. Cliquez sur **+** Créer une règle. Entrez le nom de la règle, choisissez le SSID précédemment configuré et sélectionnez les emplacements pour lesquels cette règle de portail est disponible :

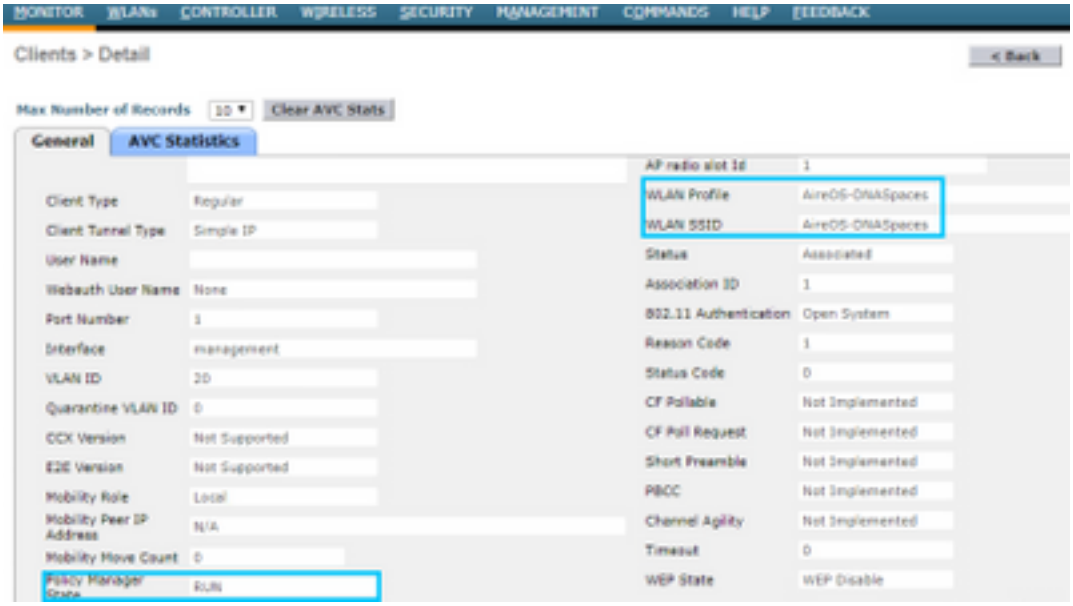


Étape 3. Sélectionnez l'action du portail captif. Dans ce cas, lorsque la règle est activée, le portail s'affiche. Cliquez sur **Enregistrer et publier.**



Vérifier

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



Dépannage

La commande suivante peut être activée dans le contrôleur avant le test pour confirmer le processus d'association et d'authentification du client.

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

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

Voici le résultat d'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 :

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

Authentification DHCP et de couche 3 :

```
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP_REQD
*webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in
HTTP GET, client mac=34:e1:2d:23:a6:68
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68
```

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

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

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

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

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

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

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.