

Configuration et dépannage des espaces d'identification numérique et du Catalyst 9800 ou du contrôleur sans fil intégré (EWC) avec Direct Connect

Contenu

[Introduction](#)

[Conditions préalables](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurer le contrôleur](#)

[Installer le certificat racine](#)

[Configurer via l'interface Web](#)

[Configuration via CLI](#)

[Importer EWC dans la hiérarchie des emplacements](#)

[Organiser la hiérarchie des emplacements sur les espaces DNA Cisco](#)

[Dépannage et problèmes courants](#)

[Problèmes courants](#)

[Suivi Radioactif](#)

Introduction

Au lieu de Mobility Express, les derniers points d'accès Cisco 9000 (9115, 9117, 9120, 9130) sont capables d'exécuter l'image de contrôleur sans fil intégré (EWC). EWC est basé sur le code WLC Cisco 9800 et permet à l'un des points d'accès d'agir comme contrôleur pour 100 autres points d'accès maximum.

EWC ou Catalyst 9800 peuvent être connectés au cloud DNA Spaces de 3 manières différentes :

1. Connexion directe
2. Via le connecteur d'espace ADN
3. Via l'appliance Cisco Connected Mobile Xperience (CMX) sur site ou la machine virtuelle

L'intégration avec DNA Spaces est prise en charge sur chaque version de EWC. Cet article couvrira la configuration et le dépannage de Direct Connection uniquement pour l'EWC sur un point d'accès Catalyst et le 9800, car la procédure est identique.

Important : La connexion directe est recommandée uniquement pour les déploiements d'un maximum de 50 clients. Pour les plus grandes, utilisez le connecteur d'espace ADN.

Conditions préalables

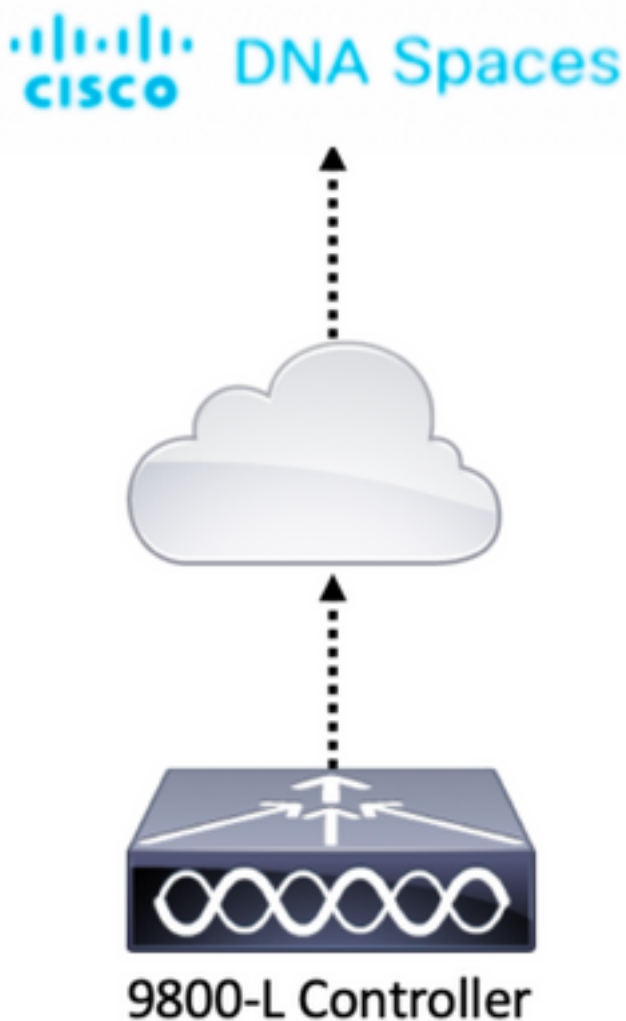
Components Used

- Image de contrôleur sans fil intégrée version 17.1.1s ou Catalyst 9800-L utilisant 16.12.1
- Point d'accès 9115
- Nuage DNA Spaces

Les étapes décrites dans cet article partent du principe que le CEE ou le 9800 a déjà été déployé et dispose d'une interface Web et d'un SSH opérationnels.

Configuration

Diagramme du réseau



Configurer le contrôleur

Les nœuds de cloud DNA Spaces et le contrôleur communiquent via le protocole HTTPS. Dans cette configuration de test, le contrôleur a été placé derrière une NAT avec un accès Internet complet.

Installer le certificat racine

Avant de configurer le contrôleur, un certificat racine DigiCert doit être téléchargé. SSH dans le contrôleur et exécutez :

```
WLC# conf t
Enter configuration commands, one per line. End with CNTL/Z.
WLC(config)# ip name-server <DNS ip>
WLC(config)# ip domain-lookup WLC(config)# crypto pki trustpool import url
https://www.cisco.com/security/pki/trs/ios.p7b
Reading file from http://www.cisco.com/security/pki/trs/ios.p7b
Loading http://www.cisco.com/security/pki/trs/ios.p7b !!!
% PEM files import succeeded.
```

Par défaut, EWC a configuré DNS à l'aide de serveurs DNS Cisco, mais il s'agira d'une étape requise pour un contrôleur 9800.

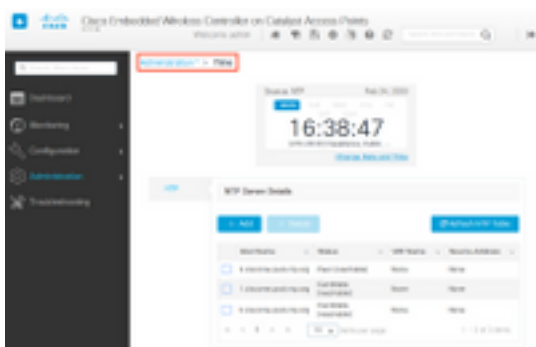
Pour vérifier que le certificat a été installé, exécutez :

```
EWC(config)#do show crypto pki trustpool | s DigiCert Global Root CA
cn=DigiCert Global Root CA
cn=DigiCert Global Root CA
```

Configurer via l'interface Web

Avant que le contrôleur puisse être connecté à DNA Spaces, il est nécessaire de configurer des serveurs NTP et DNS et de joindre au moins un point d'accès.

Ouvrez l'interface Web de l'EWC et accédez à **Administration > Time**. Assurez-vous que le WLC est synchronisé avec un serveur NTP. Par défaut, EWC est préconfiguré pour utiliser les serveurs NTP cisco.pool.ntp.org. Dans le cas du 9800, vous pouvez utiliser le même NTP ou votre serveur NTP préféré :



Accédez à **Administration > DNS** et vérifiez que le serveur DNS a été ajouté. Par défaut, EWC est préconfiguré pour utiliser les serveurs Cisco Open DNS :

Administration > DNS

DNS Loopback **ENABLED**

+ Add - Delete

IP Address
<input type="checkbox"/> 208.67.222.222,208.67.220.220

1 - 1 of 1 items

Sous **Configuration > Wireless > Access Points**, vérifiez qu'au moins un point d'accès a été joint. Ce point d'accès peut être identique à celui sur lequel le CEE est exécuté :

Configuration > Wireless > Access Points

▼ All Access Points

Current Primary: 9115

Current Stand...: Not Applicable

Preferred Mas...: Not Configured

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Policy Tag	Site Tag	RF Tag	Tag Source
9115	C9115AXI-E	2	✓	192.168.1.11	f80f.6f15.3fc0	Flex	Registered	Vasa5	default-site-tag	default-rf-tag	Static

1 - 1 of 1 access points

Dans le cloud DNA Spaces, naviguez de la page d'accueil à **Setup > Wireless Networks > Connect WLC/Catalyst 9800 Directement**. Cliquez sur **View Token** :

Connect your wireless network

Connect WLC/Catalyst 9800 Directly

View Token

Install Span Conditions

Import Controllers into Location Hierarchy

Basculer vers **Cisco Catalyst 9800**. Copier le jeton et l'URL :

Token for WLC to connect to DNA Spaces

WLC: Cisco Catalyst 9800

Follow the steps below to configure token in Cisco Catalyst 9800 Series Wireless Controller CLI

- Once you logged in,
 - type "config" command
- Execute the following steps in CLI mode
 - no nmsp cloud-services enable
 - nmsp cloud-services server url <https://vasilijeperovic.dnaspaces.eu>
 - nmsp cloud-services server token [TOKEN]

TOKEN

```
eyJ0eXAI0iJKV1QlLCJI
TYl8krprpmRq0g
```

DPGIANMbj4Pe-

 - nmsp cloud-services enable
- Exit from config
 - type "exit" command

Dans l'interface Web du WLC, accédez à **Configuration > Services > Services cloud > Espaces ADN**. Coller l'URL et le jeton d'authentification. Si le proxy HTTP est utilisé, spécifiez son adresse IP et son port.

Configuration > Services > Cloud Services

Network Assurance **DNA Spaces**

DNA Spaces Service Configuration

Enable Service

Service URL
Eg.
 https://<td_id>.cmxcisco.com

Authentication Token

HTTP Proxy (Hostname/IP)

Port

Apply

Vérifiez que la connexion a été correctement établie sous **Surveillance > Wireless > NMSP**. L'état du service doit afficher la flèche verte :

The screenshot shows the Cisco Embedded Wireless Controller web interface. The breadcrumb navigation is **Monitoring > Wireless > NMSP**. The main content area is divided into two columns: **DNA Spaces Services Status** and **DNA Spaces Services Statistics**.

DNA Spaces Services Status		DNA Spaces Services Statistics	
Server	https://vasilijeperovic.dnaspaces.eu	Tx DataFrames	7
IP Address	63.33.127.190	Rx DataFrames	2
DNA Spaces Service	Enabled	Tx Heartbeat Request	4
Connectivity	https UP	Heartbeat Timeout	0
Service Status	UP	Rx Subscr Request	2
Last Request Status	HTTP/2.0 200 OK	Tx DataBytes	512
Heartbeat Status	OK	Rx DataBytes	74
		Tx Heartbeat Fail	0
		Rx Data Fail	0
		Tx Data Fail	0

Ignorez le chapitre suivant et accédez à la “ Importer les contrôleurs dans la ” Hiérarchie des emplacements.

Configuration via CLI

Vérifiez que NTP est configuré et synchronisé :

```
EWC#show ntp associations
```

```

address      ref clock  st  when  poll reach  delay  offset  disp
*~45.87.76.3 193.79.237.142638 1024 377 10.919 -4.315 1.072
+~194.78.244.172 172.16.200.253 2646 1024 377 15.947 -2.967 1.084
+~91.121.216.238 193.190.230.66 2856 1024 377 8.863 -3.910 1.036
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

```

De nouveaux serveurs NTP peuvent être ajoutés à l'aide de la commande `ntp server <ntp_ip_addr>`.

Vérifiez que les serveurs DNS ont été configurés :

```
EWC#show ip name-servers
```

```

208.67.222.222
208.67.220.220

```

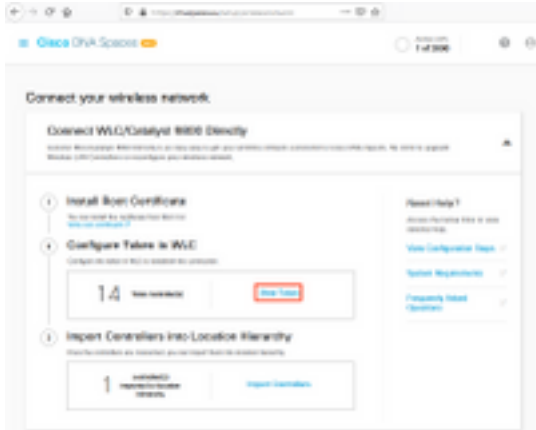
De nouveaux serveurs DNS peuvent être ajoutés à l'aide de la commande `ip name-server <dns_ip>`.

Pour confirmer que le point d'accès a été joint :

```
EWC#show ap status
```

AP Name	Status	Mode	Country
9115	Enabled	Local	BE

Comme mentionné précédemment, accédez au cloud DNA Spaces, puis accédez à **Setup > Wireless Networks > Connect WLC/Catalyst 9800 Directement** et cliquez sur **View Token** :



Basculer vers **Cisco Catalyst 9800**. Copier le jeton et l'URL :

Token for WLC to connect to DNA Spaces

WLC **Cisco Catalyst 9800**

Follow the steps below to configure token in Cisco Catalyst 9800 Series Wireless Controller CLI

- 1 Once you logged in,
 - a. type "config" command
- 2 Execute the following steps in CLI mode
 - a. no nmsp cloud-services enable
 - b. nmsp cloud-services server url **https://vasilijepovic.dnaspaces.eu**
 - c. nmsp cloud-services server token **[TOKEN]**

TOKEN

eyJ0eXAI0iJKV1QILCJI TYI8krprmq0g JPGIANMbj4Pe-

 - d. nmsp cloud-services enable
- 3 Exit from config
 - a. type "exit" command

Exécutez les commandes suivantes :

```
CL-9800-01(config)#no nmsp cloud-services enable
CL-9800-01(config)#nmsp cloud-services server url [URL]
CL-9800-01(config)#nmsp cloud-services server token [TOKEN]
CL-9800-01(config)#nmsp cloud-services enable
CL-9800-01(config)#exit
```

Pour vérifier que la connexion au cloud DNA Spaces a été établie correctement, exécutez :

```
CL-9800-01#show nmsp cloud-services summary
```

```
CMX Cloud-Services Status
```

```
-----  
Server : https://vasilijeperovic.dnaspaces.eu
```

```
CMX Service : Enabled
```

```
Connectivity : https: UP
```

```
Service Status : Active
```

```
Last IP Address : 63.33.127.190
```

```
Last Request Status : HTTP/2.0 200 OK
```

```
Heartbeat Status : OK
```

Importer EWC dans la hiérarchie des emplacements

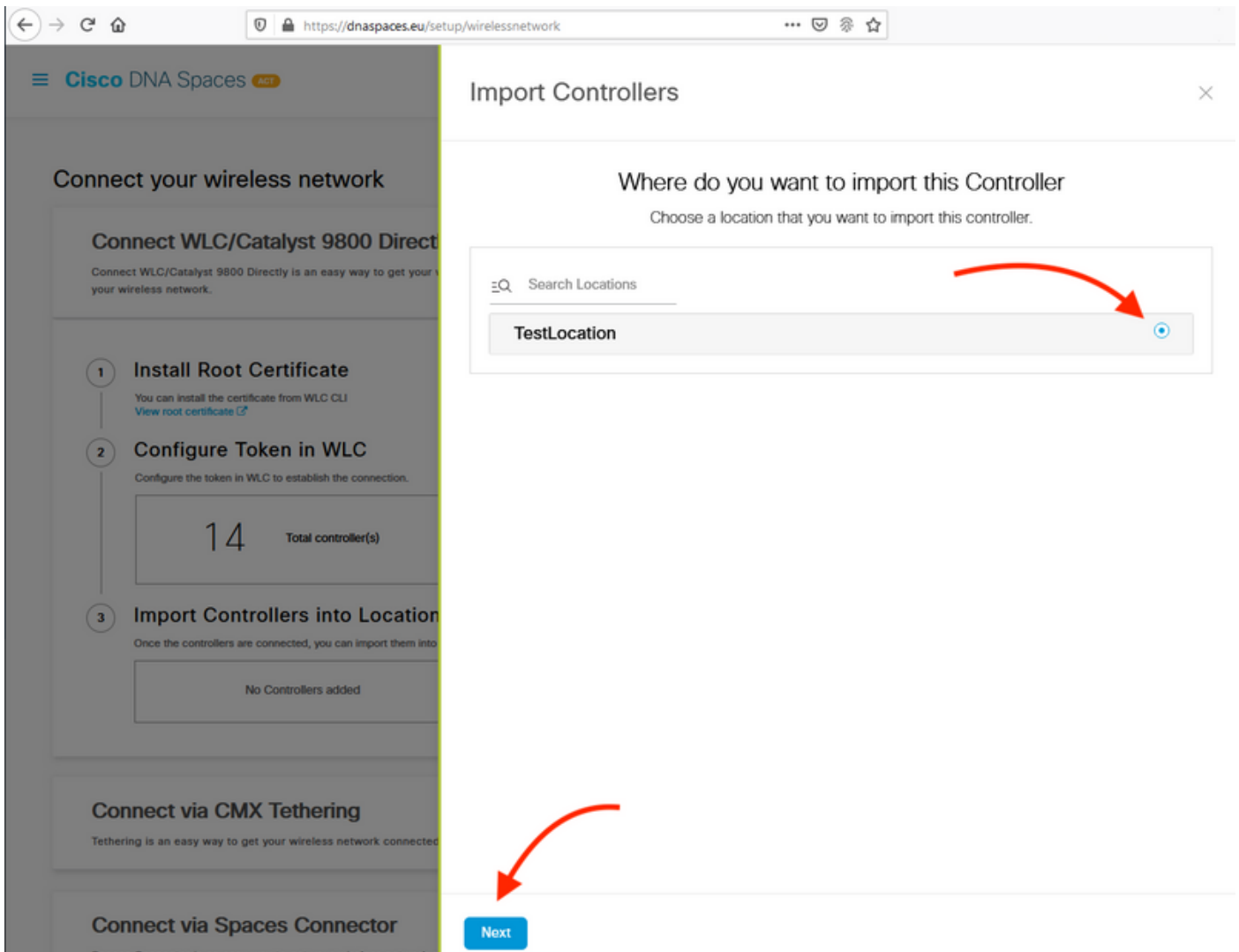
Étape 1. Le reste de la configuration sera fait dans DNA Spaces. Sous **Setup > Wireless Networks > Connect WLC/Catalyst 9800 Directement**, cliquez sur **Import Controllers**.

The screenshot displays the Cisco DNA Spaces web interface for connecting WLC/Catalyst 9800 controllers. The main heading is "Connect WLC/Catalyst 9800 Directly". Below the heading, there is a brief description: "Connect WLC/Catalyst 9800 Directly is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network." The interface is structured into three numbered steps:

- 1 Install Root Certificate**: "You can install the certificate from WLC CLI" with a link "View root certificate".
- 2 Configure Token in WLC**: "Configure the token in WLC to establish the connection." Below this, a box displays "14 Total controller(s)" and a "View Token" button.
- 3 Import Controllers into Location Hierarchy**: "Once the controllers are connected, you can import them into location hierarchy" Below this, a box displays "1 controller(s) imported to location hierarchy" and a red-bordered "Import Controllers" button.

On the right side, there is a "Need Help?" section with the text "Access the below links to view detailed help." and three links: "View Configuration Steps", "System Requirements", and "Frequently Asked Questions". The top navigation bar includes the Cisco DNA Spaces logo and "Active APs 1 of 2000".

Étape 2. Cochez la case d'option en regard de votre nom de compte et cliquez sur Suivant. Si certains emplacements ont déjà été ajoutés, ils apparaîtront dans la liste ci-dessous :



Étape 3. Recherchez votre adresse IP de contrôleur, cochez la case en regard de celle-ci et appuyez sur **Suivant** :



Étape 4. Comme aucun autre emplacement n'a été ajouté, cliquez simplement sur Terminer :



Étape 5. L'invite indiquant que le WLC a été correctement importé dans la hiérarchie d'emplacements s'affiche :



Controller successfully
imported to location
hierarchy!

Total controllers added : 1
Total number of APs : 1
Total number of Locations : 0

Would you like to organize your location
hierarchy

Yes, take me to location hierarchy

No, Continue with Setup

Maintenant que le WLC a été correctement connecté au cloud, vous pouvez commencer à utiliser toutes les autres fonctionnalités de DNA Spaces.

Note: Le trafic NMSP utilise toujours l'interface de gestion sans fil pour communiquer avec DNA Spaces ou CMX. Impossible de modifier ceci dans la configuration du contrôleur 9800. Le numéro d'interface n'est pas pertinent, quelle que soit l'interface affectée en tant qu'interface de gestion sans fil sur le contrôleur 9800 sera utilisée.

Organiser la hiérarchie des emplacements sur les espaces DNA Cisco

Si une nouvelle hiérarchie d'emplacements est souhaitée ou si aucun emplacement n'a été ajouté à l'étape 4 de la section **Importer le contrôleur 9800 dans Cisco DNA Spaces**, vous pouvez les configurer manuellement.

La hiérarchie des emplacements est l'une des caractéristiques les plus importantes des espaces d'ADN car elle est utilisée pour les informations d'analyse et en fonction de cela, les règles des portails captifs sont configurées. Plus la hiérarchie de localisation est granulaire, plus le contrôle sur les règles du portail captif et sur les informations qui peuvent être récupérées à partir de DNA Spaces est granulaire.

La fonction de hiérarchie des emplacements sur les espaces ADN fonctionne de la même manière que la hiérarchie traditionnelle de Cisco Prime Infrastructure ou de Cisco CMX, mais le nom est très différent. Lorsque le contrôleur est importé dans la hiérarchie d'emplacement, il représente l'équivalent du **campus** de la hiérarchie traditionnelle ; sous le contrôleur, **des groupes** peuvent être créés qui sont équivalents aux **bâtiments** ; ensuite, sous les groupes, **les réseaux** peuvent être configurés qui sont l'équivalent des **étages**, enfin, sous les réseaux, des zones peuvent être créées qui restent dans le même niveau qu'auparavant dans la hiérarchie d'emplacement traditionnelle. En résumé, voici l'équivalence :

Tableau 1 . Équivalence entre les niveaux hiérarchiques traditionnels et les niveaux des espaces d'ADN.

Hiérarchie des espaces ADN	Hiérarchie traditionnelle
Contrôleur (réseau sans fil)	Campus
Groupe	Bâtiment
Réseau	Étage
Zone	Zone

Étape 1. Configurez un groupe. Les groupes organisent plusieurs emplacements ou zones en fonction de la géolocalisation, de la marque ou de tout autre type de regroupement selon l'entreprise. Accédez à **Hiérarchie des emplacements**, passez la souris sur le contrôleur sans fil existant et cliquez sur **Créer un groupe**.



Pour modifier le nom du niveau d'emplacement, faites glisser la souris sur le réseau et cliquez sur « Renommer ».

Étape 2. Entrez le nom du groupe et sélectionnez l'emplacement **Non configuré**, car il inclut tous les AP importés avec le contrôleur, ces AP seront mappés ensuite aux réseaux et aux zones selon les besoins. Cliquez sur **Add**.

The 'Add Group' dialog box is shown. It has a title bar 'Add Group' with a close button. Below the title bar is a text input field containing 'MXC-10-Building'. Below that is a 'Select Location' section with a radio button selected for 'Unconfigured'. At the bottom of the dialog, there are two buttons: 'Add' and 'Cancel'.

Étape 3. Créer un réseau. Un réseau ou un emplacement est défini dans Cisco DNA Spaces comme tous les points d'accès d'un bâtiment physique consolidés en tant que site. Placez le pointeur de la souris sur Groupe et cliquez sur **Ajouter un réseau**.

MEX-EAST-1		11	8	0	4	0	0
+	5508-1-CMX	1	1	0	2	0	0
+	5508-2-Connector-Campus	2	2	0	0	0	0
+	5520-DirectConnect	2	1	0	1	0	0
-	9800L-Mexico-Campus	1	1	0	0	0	0
+	MXC-10-Building	1	1	0	0	0	0
+	efmLocation	2	2	0	0	0	0
+	Lisboa	3	1	0	0	0	0

MORE ACTIONS

- Rename MXC-10-Bui...
- Create Group
- Edit Group
- Add Network**
- Add/Edit Metadata
- Delete Location

Note: Il s'agit du noeud le plus important de la hiérarchie des emplacements, car les analyses de l'entreprise et les calculs d'analyse des emplacements sont générés à partir d'ici.

Étape 4. Entrez le nom du réseau et le préfixe du point d'accès, puis cliquez sur **Récupérer**. DNA Spaces récupère tous les AP associés à ce contrôleur avec ce préfixe et permet d'ajouter les AP au sol. Un seul préfixe peut être entré.

Add Network ✕

10.10.30.5

NETWORK NAME
Second Floor

ACCESS POINT PREFIX
28 Fetch

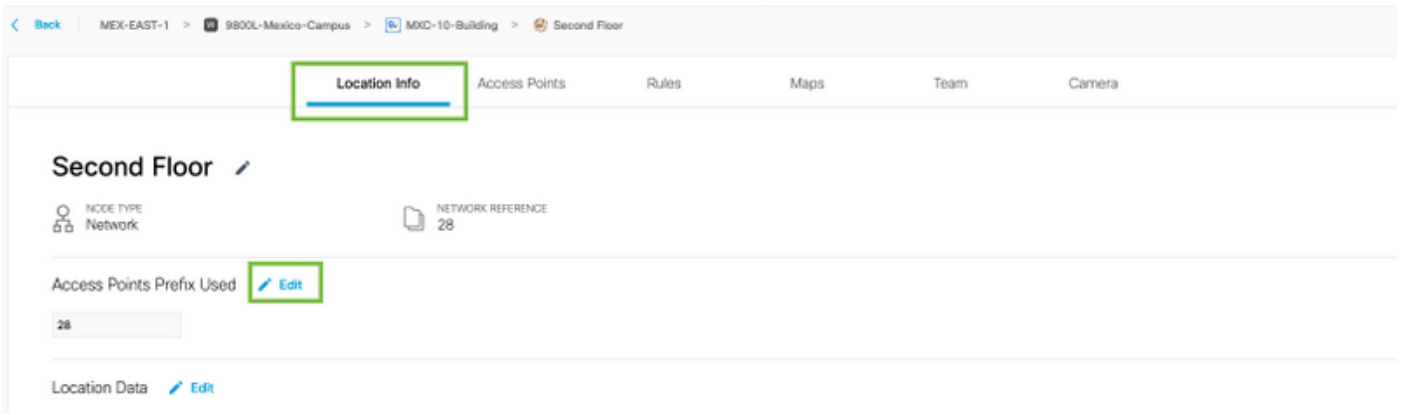
Matching access points will be shown below

1 Following access points are discovered based on provided prefix and will be added to this network.

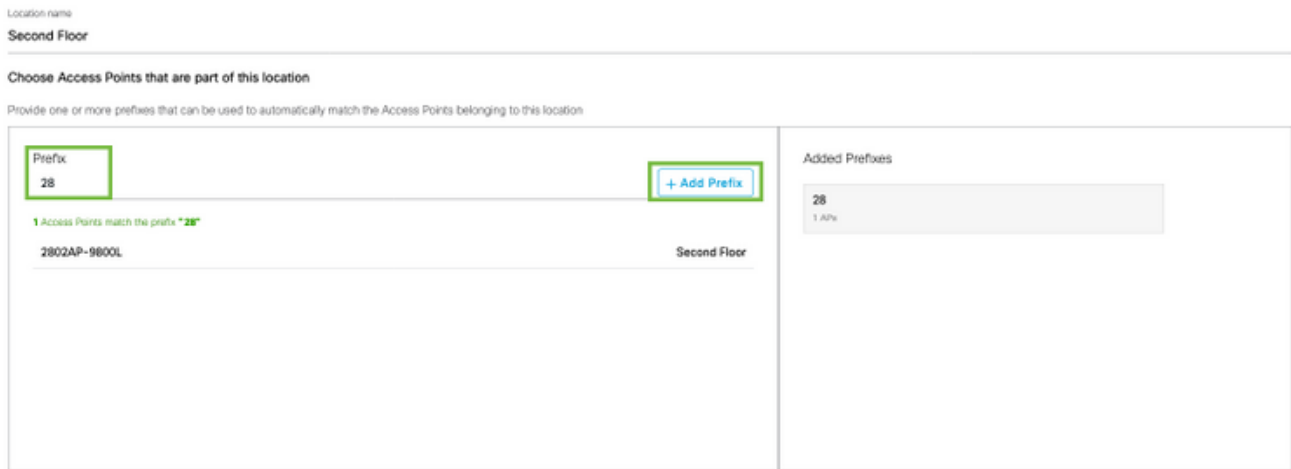
2802AP-9800L

Done

Étape 5. Si davantage de préfixes sont nécessaires sur le réseau. Cliquez sur le nom du réseau, dans l'onglet **Informations sur l'emplacement**, cliquez sur le bouton **Modifier** en regard de **Préfixe des points d'accès utilisé**.

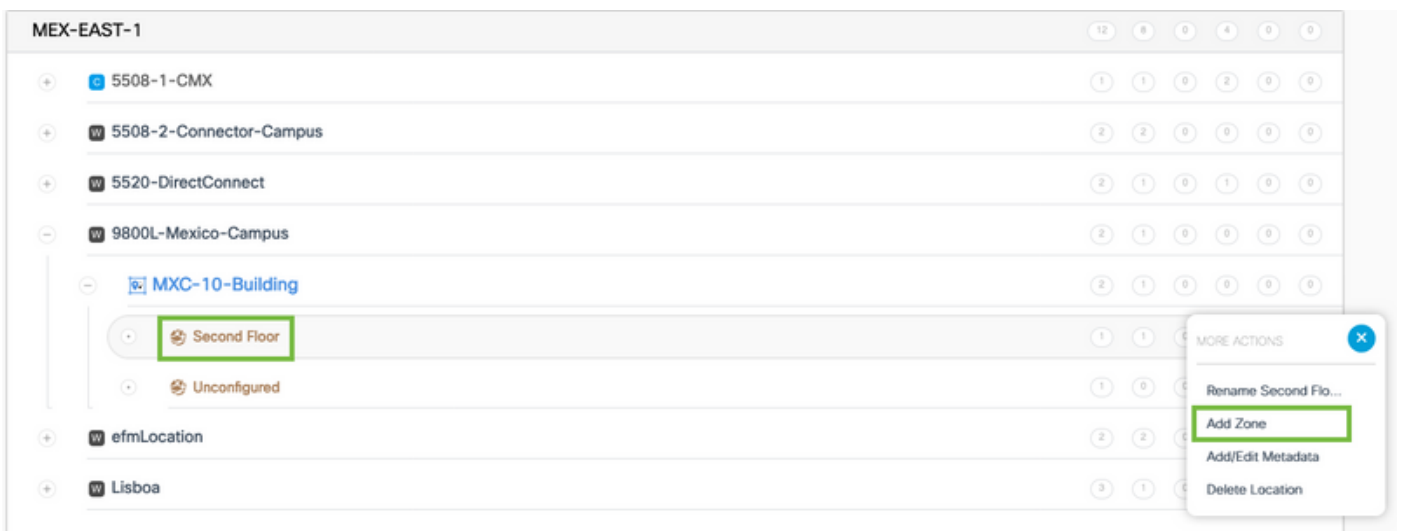


Entrez le nom du préfixe, cliquez sur **+Ajouter un préfixe** et **enregistrez**. Répétez l'opération pour tous les préfixes si nécessaire, cela mapperà les AP au réseau et permettra de mapper les AP aux zones plus tard.



Cancel **Save**

Étape 6. Créez une zone. Une zone est un ensemble de points d'accès au sein d'une section d'un bâtiment/d'un emplacement. Il peut être défini en fonction des départements d'un bâtiment physique ou d'une organisation. Placez le pointeur de la souris sur Réseau et sélectionnez **Ajouter une zone**.



Étape 7. Configurez le **nom de zone** et sélectionnez les points d'accès de la zone, puis cliquez sur **Ajouter** :

Add Zone 🔍 ✕

Wireless-Zone

Select Access Points
Network Access Points

2802AP-9800L (10:b3:d6:94:00:e0)

Add

Dépannage et problèmes courants

Problèmes courants

La page de l'interface Web sous **Surveillance > Wireless > NMSP** (ou exécution de la commande `show nmsp cloud-services summary`) affiche généralement suffisamment d'informations sur l'échec de connexion. Plusieurs erreurs courantes se trouvent dans les captures d'écran ci-dessous :

1. Lorsque DNS n'est pas configuré, le message d'erreur “ *Erreur de transfert (6) : Impossible de résoudre le nom d'hôte* ” apparaît :

The screenshot shows the Cisco Embedded Wireless Controller interface. The breadcrumb navigation is **Monitoring > Wireless > NMSP**. The page displays the following information:

DNA Spaces Services Status		DNA Spaces Services Statistics	
Server	https://vasilijeperovic.dnaspaces.eu	Tx DataFrames	0
IP Address	127.0.0.1	Rx DataFrames	0
DNA Spaces Service	Enabled	Tx Heartbeat Request	3
Connectivity	DOWN	Heartbeat Timeout	0
Service Status	⬇	Rx Subscr Request	0
Last Request Status	Transfer error (6): Couldn't resolve host name	Tx DataBytes	0
Heartbeat Status		Rx DataBytes	0
		Tx Heartbeat Fail	1
		Rx Data Fail	0
		Tx Data Fail	0

Le certificat n'étant pas installé ou NTP n'étant pas configuré, les deux résultats sont accompagnés du message d'erreur suivant : *“ Erreur de transfert (60) : Le certificat homologue SSL ou la clé distante SSH n'était pas OK ”* :

The screenshot shows the Cisco Embedded Wireless Controller interface. The breadcrumb navigation is **Monitoring > Wireless > NMSP**. The page displays the following information:

DNA Spaces Services Status		DNA Spaces Services Statistics	
Server	https://vasilijeperovic.dnaspaces.eu	Tx DataFrames	0
IP Address	208.67.222.222	Rx DataFrames	0
DNA Spaces Service	Enabled	Tx Heartbeat Request	2
Connectivity	DOWN	Heartbeat Timeout	0
Service Status	⬇	Rx Subscr Request	0
Last Request Status	Transfer error (60): SSL peer certificate or SSH remote key was not OK	Tx DataBytes	0
Heartbeat Status		Rx DataBytes	0
		Tx Heartbeat Fail	1
		Rx Data Fail	0
		Tx Data Fail	0

Suivi Radioactif

EWC, comme tous les autres contrôleurs 9800, prend en charge les traces radioactives toujours actives. Afin de les collecter et de voir pourquoi la connexion n'est pas établie, il est nécessaire de savoir à quelle adresse IP de l'espace ADN le CEE tend la main. Vous pouvez le trouver sous

Monitor > Wireless > NMSP ou via CLI :

```
EWC#show nmsp status
```

```
NMSP Status
```

```
-----
```

```
CMX IP Address      ActiveTx Echo Resp  Rx Echo Req  Tx Data Rx Data Transport
```

```
-----  
--
```

```
63.33.127.190      Active0              0             38           2           HTTPS
```

Dans cette configuration de test, le CEE se connecte à 63.33.127.190. Copiez cette adresse IP et accédez à **Dépannage > Suivi radioactif**. Cliquez sur Ajouter, collez l'adresse IP et cliquez sur Générer :

The screenshot shows the Cisco Embedded Wireless Controller web interface. The breadcrumb navigation is **Troubleshooting > Radioactive Trace**. The page title is "Conditional Debug Global State: Stopped". There are four buttons: "+ Add", "X Delete", "Start", and "Stop". The "+ Add" button is highlighted with a red box. Below the buttons is a table with the following content:

	MAC/IP Address	Trace file	
<input type="checkbox"/>	63.33.127.190		▶ Generate

Below the table, there is a pagination control showing "1" items per page and "1 - 1 of 1 items". The "Generate" button is highlighted with a red box.

Sélectionnez **Générer les journaux** pour les 10 dernières minutes et cliquez sur Appliquer. L'activation des journaux internes peut générer de grandes quantités de données difficiles à analyser :

The screenshot shows the "Enter time interval" dialog box. It has a close button (X) in the top right corner. The "Enable Internal Logs" checkbox is unchecked. The "Generate logs for last" section has radio buttons for "10 minutes" (selected), "30 minutes", "1 hour", and "since last boot". There is also a text input field with "0-4294967295" and a "seconds" dropdown menu. At the bottom, there are "Cancel" and "Apply to Device" buttons.

Remarque : DNS, NTP et absence de certificat mal configurés ne généreront pas de traces radioactives

Exemple de trace radioactive dans un cas où le pare-feu bloque le protocole HTTPS :

```
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (note): CMX [63.33.127.190]:[32]: closing
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Called 'is_ready'
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (info): CMX [63.33.127.190]:[32]: Processing connection event NMSP_APP_LBS_DOWN(201)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (info): Started or incremented transaction (TID: -1, ref count: 1, started: 0, abort: 0)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-enc] [11100]: (debug): Decoding control message structure
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-enc] [11100]: (debug): Control structure was successfully decoded from message
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (debug): Retrieving CMX entry: 32
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (ERR): CMX entry 32 not found
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (debug): CMX Pool processing NMSP message (id: event NMSP_APP_LBS_DOWN(201), length: 48, client: 0, CMX id: 32)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (info): Ending transaction (TID: -1, ref count: 1, started: 0, abort: 0)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (info): Ended transaction (TID: -1, ref count: 0, started: 0, abort: 0)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-client] [11100]: (debug): NMSP IPC sent message to NMSpd NMSP message (id: event NMSP_APP_LBS_DOWN(201), length: 48, client: 0, CMX id: 32) successfully
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (info): CMX [63.33.127.190]:[32]: successfully broadcasted IPC event NMSP_APP_LBS_DOWN(201)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (note): CMX [63.33.127.190]:[32]: down
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (debug): NMSP timer 0xab774af4: close
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Decrease reference count for https_con object: Now it's 1
```

Exemple de trace radioactive pour une connexion réussie avec le cloud :

```
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (note): Server did not reply to V2 method. Falling back to V1.
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Cloud authentication 2 step failed, trying legacy mode
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (note): Set connection status from HTTP_CON_AUTH_PROGRESS_2STEP to HTTP_CON_AUTH_IDLE
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): tenant ID: vasilijeperovic
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): hostname is: data.dnaspaces.eu
2020/02/24 18:53:20.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (note): Starting authentication V1 using Heartbeat URL https://data.dnaspaces.eu/api/config/v1/nmspconfig and Data URL https://data.dnaspaces.eu/networkdata
2020/02/24 18:53:20.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (note): Set connection status from HTTP_CON_AUTH_IDLE to HTTP_CON_AUTH_PROGRESS_1STEP
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): tenant ID: vasilijeperovic
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): hostname is: data.dnaspaces.eu
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Authenticator V1 get heartbeat host: https://data.dnaspaces.eu/api/config/v1/nmspconfig
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Authenticator V1 get access token: eyJ0eX[information omitted]rpmRq0g
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (debug): DNSs used for cloud services: 208.67.222.222,208.67.220.220
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Using nameservers:
```

208.67.222.222,208.67.220.220

2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): **IP resolution preference is set to IPv4**

2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): **Not using proxy for cloud services**

2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): Found bundle for host data.dnaspaces.eu: 0xab764f98 [can multiplex]

2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): Re-using existing connection! (#0) with host data.dnaspaces.eu

2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): **Connected to data.dnaspaces.eu (63.33.127.190) port 443 (#0)**

2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): Using Stream ID: 3 (easy handle 0xab761440)

2020/02/24 18:53:21.636 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): POST /api/config/v1/nmspconfig/192.168.1.10?recordType=nmsp_hrbt_init&jwttoken=eeyJ0eX[information omitted]70%3A69%3A5a%3A74%3A8e%3A58 HTTP/2

Host: data.dnaspaces.eu

Accept: */*

Accept-Encoding: gzip

2020/02/24 18:53:21.665 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): **We are completely uploaded and fine**

HTTP/2 200

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.