

# Konfiguration und Fehlerbehebung für DNA-Bereiche und Catalyst 9800 oder Embedded Wireless Controller (EWC) mit Direct Connect

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurieren des Controllers](#)

[Stammzertifikat installieren](#)

[Konfiguration über Webschnittstelle](#)

[Konfiguration über CLI](#)

[EWC in die Standorthierarchie importieren](#)

[Organisieren der Standorthierarchie in Cisco DNA-Bereichen](#)

[Fehlerbehebung und häufige Probleme](#)

[Häufige Probleme](#)

[Radioaktive Nachverfolgung](#)

## Einführung

Anstelle von Mobility Express können die neuesten Access Points der Cisco Serie 9000 (9115, 9117, 9120, 9130) das EWC-Image (Embedded Wireless Controller) ausführen. EWC basiert auf dem Cisco 9800 WLC-Code und ermöglicht es einem der Access Points, als Controller für bis zu 100 weitere APs zu fungieren.

Der EWC oder der Catalyst 9800 können auf drei verschiedene Arten mit der DNA Spaces Cloud verbunden werden:

1. Direkte Verbindung
2. über DNA Spaces Connector
3. über Cisco Connected Mobile Xperience (CMX) vor Ort oder VM

Die Integration in DNA Spaces wird auf jeder Version von EWC unterstützt. Dieser Artikel behandelt die Einrichtung und Fehlerbehebung von Direct Connection nur für den EWC auf einem Catalyst AP und den 9800, da das Verfahren identisch ist.

**Wichtig:** Direkte Verbindung wird nur für Bereitstellungen von bis zu 50 Clients empfohlen. Verwenden Sie für größere Geräte den DNA Spaces Connector.

## Voraussetzungen

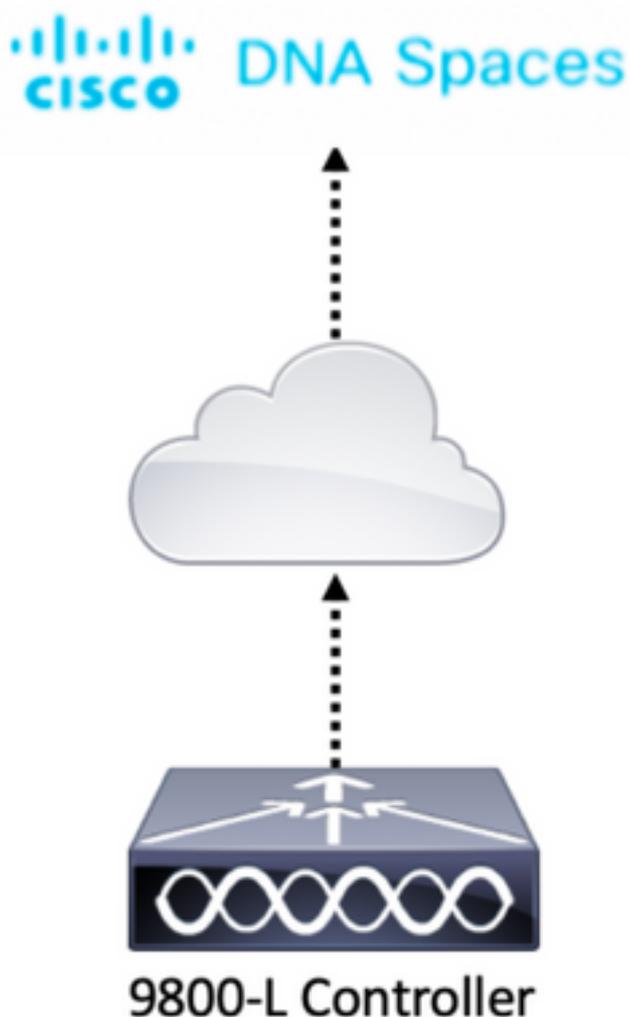
## Verwendete Komponenten

- Integriertes Wireless Controller-Image der Version 17.1.1s oder Catalyst 9800-L mit 16.12.1
- AP 9115
- DNA Spaces Cloud

Bei den in diesem Artikel beschriebenen Schritten wird davon ausgegangen, dass der EWC oder 9800 bereits bereitgestellt wurde und über eine funktionierende Webschnittstelle und SSH verfügt.

## Konfigurieren

### Netzwerkdiagramm



### Konfigurieren des Controllers

DNA Spaces Cloud-Knoten und der Controller kommunizieren über das HTTPS-Protokoll. In dieser Testeinrichtung wurde der Controller hinter einer NAT mit vollständigem Internetzugang platziert.

### Stammzertifikat installieren

Bevor der Controller konfiguriert wird, muss ein DigiCert-Root-Zertifikat heruntergeladen werden. SSH in den Controller einstecken und ausführen:

```
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.
```

Bei EWC ist DNS standardmäßig mit Cisco DNS-Servern konfiguriert. Dies ist jedoch ein erforderlicher Schritt für einen 9800-Controller.

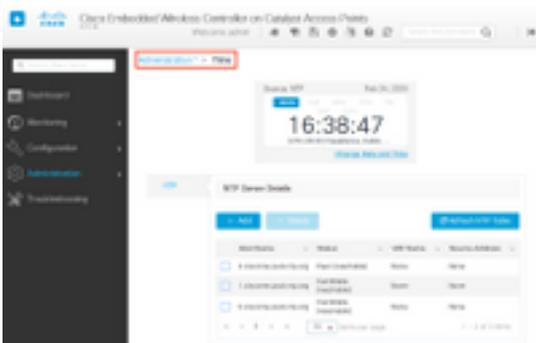
Führen Sie folgende Schritte aus, um zu überprüfen, ob das Zertifikat installiert wurde:

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

## Konfiguration über Webschnittstelle

Bevor der Controller mit DNA Spaces verbunden werden kann, muss er NTP- und DNS-Server einrichten und mindestens einen Access Point haben.

Öffnen Sie die Webschnittstelle des EWC, und navigieren Sie zu **Administration > Time**. Stellen Sie sicher, dass der WLC mit einem NTP-Server synchronisiert ist. In der Standardeinstellung ist EWC für die Verwendung der NTP-Server `ciscome.pool.ntp.org` vorkonfiguriert. Im Fall des 9800 können Sie dasselbe NTP oder den von Ihnen bevorzugten NTP-Server verwenden:



Navigieren Sie zu **Administration > DNS**, und überprüfen Sie, ob der DNS-Server hinzugefügt wurde. Standardmäßig ist der EWC für die Verwendung von Cisco Open DNS-Servern vorkonfiguriert:

Cisco Embedded Wireless Controller on Catalyst Access Points  
17.1.15  
Welcome admin

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

Überprüfen Sie unter **Konfiguration > Wireless > Access Points**, ob mindestens ein Access Point hinzugefügt wurde. Dieser AP kann derselbe sein, auf dem der EWC ausgeführt wird:

Cisco Embedded Wireless Controller on Catalyst Access Points  
17.1.15  
Welcome admin

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

Navigieren Sie in der DNS Spaces Cloud von der Startseite zu **Setup > Wireless Networks > Connect WLC/Catalyst 9800 Direct**. Klicken Sie auf **Token anzeigen**:

Connect your wireless network

Connect WLC/Catalyst 9800 Direct

1. Install BIOS Conditions  
2. Configure Tokens in WLC  
3. Import Controllers into Location Hierarchy

Show Token

Wechseln Sie zur Registerkarte **Cisco Catalyst 9800**. Kopieren Sie den Token und die 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://vasilijeperovic.dnaspaces.eu>
  - c. nmsp cloud-services server token [TOKEN]

TOKEN

```
eyJ0eXAI0iJKV1QlLCJI...JPGIANMbj4Pe-
```

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

Navigieren Sie in der WLC-Webschnittstelle zu **Configuration > Services > Cloud Services > DNA Spaces**. Geben Sie URL und Authentifizierungstoken ein. Wenn ein HTTP-Proxy verwendet wird, geben Sie dessen IP-Adresse und Port an.

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

Überprüfen Sie, ob die Verbindung unter **Monitoring > Wireless > NMSP** erfolgreich hergestellt wurde. Der Servicestatus muss mit einem grünen Pfeil versehen sein:

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		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

Überspringen Sie das nächste Kapitel und gehen Sie zu "Controller in die Standorthierarchie importieren".

## Konfiguration über CLI

Überprüfen Sie, ob NTP konfiguriert und synchronisiert ist:

```
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

```

Neue NTP-Server können mit dem Befehl `ntp server <ntp_ip_addr>` hinzugefügt werden.

Überprüfen Sie, ob DNS-Server konfiguriert wurden:

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

```

208.67.222.222
208.67.220.220

```

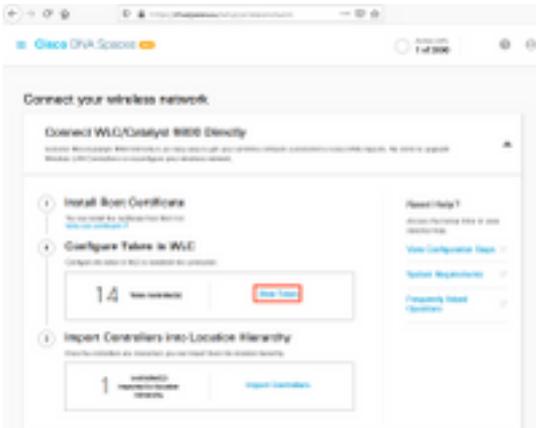
Neue DNS-Server können mit dem Befehl `ip name-server <dns_ip>` hinzugefügt werden.

So bestätigen Sie, dass der Access Point hinzugefügt wurde:

EWC#**show ap status**

AP Name	Status	Mode	Country
9115	Enabled	Local	BE

Wie bereits erwähnt, greifen Sie auf die DNS Spaces Cloud zu, navigieren Sie zu **Setup > Wireless Networks > Connect WLC/Catalyst 9800 Direct** und klicken Sie auf **View Token**:



Wechseln Sie zur Registerkarte **Cisco Catalyst 9800**. Kopieren Sie den Token und die 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://vasilijeperovic.dnaspaces.eu**
  - c. nmsp cloud-services server token [TOKEN]

TOKEN

**eyJ0eXAI0iJKV1QlL0Jl... JPGIANMbj4Pe-**

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

Führen Sie die folgenden Befehle aus:

```
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
```

Führen Sie folgende Schritte aus, um zu überprüfen, ob die Verbindung mit der DNS Spaces Cloud erfolgreich hergestellt wurde:

```
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
```

## EWC in die Standorthierarchie importieren

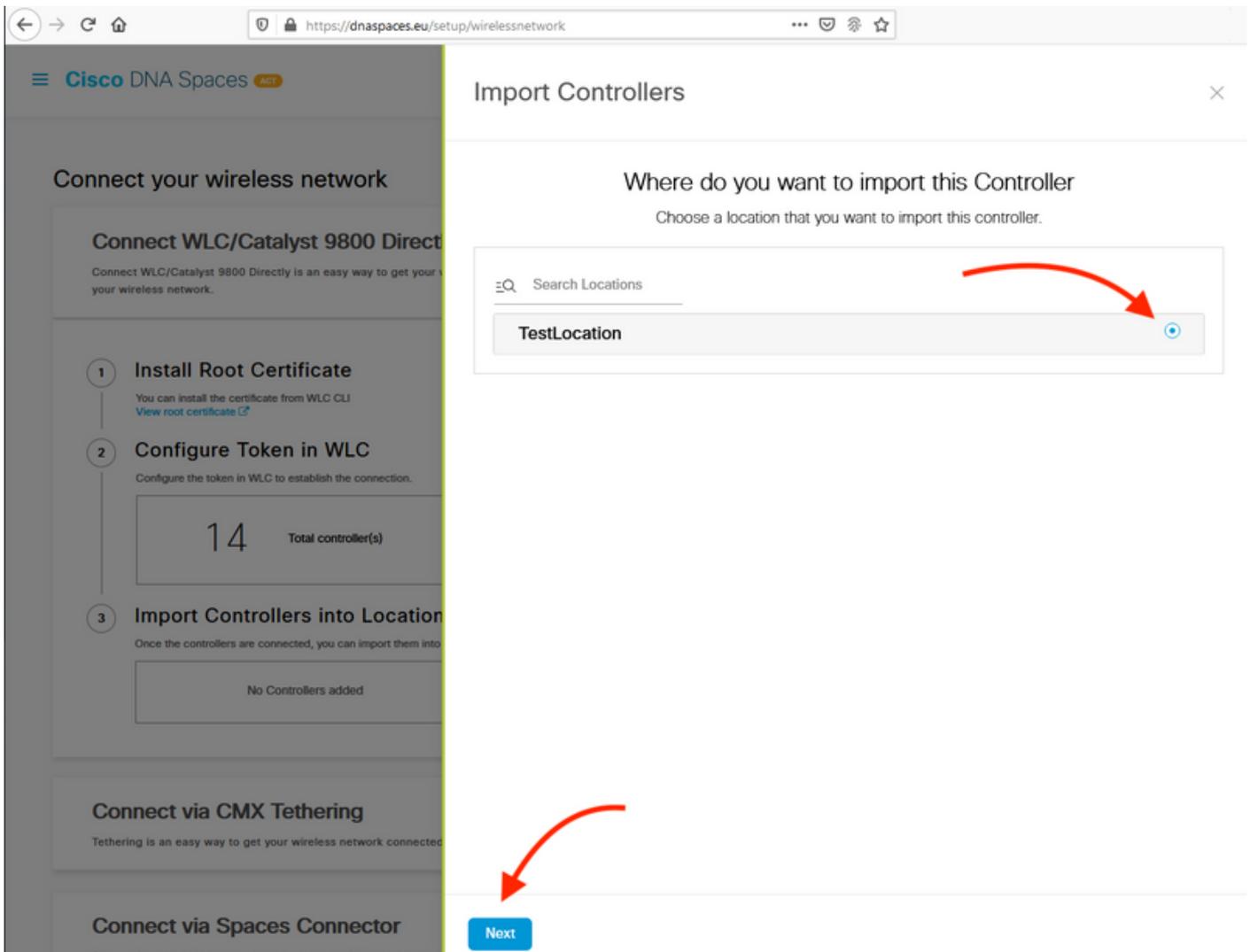
Schritt 1: Die restliche Konfiguration erfolgt in DNA-Bereichen. Klicken Sie unter **Setup > Wireless Networks > Connect WLC/Catalyst 9800 Direct** auf **Import Controllers (Controller importieren)**.

The screenshot displays the Cisco DNA Spaces web interface for configuring wireless networks. The main heading is "Connect WLC/Catalyst 9800 Directly". Below this, there are three numbered steps:

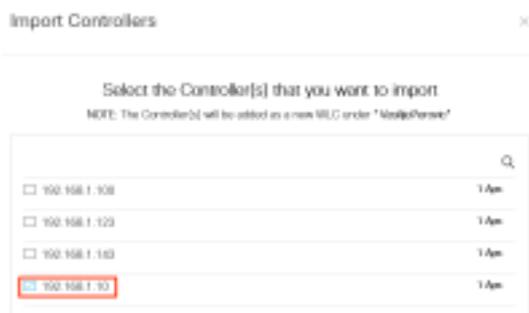
- 1 Install Root Certificate**: You can install the certificate from WLC CLI. [View root certificate](#)
- 2 Configure Token in WLC**: Configure the token in WLC to establish the connection. A box shows "14 Total controller(s)" and a [View Token](#) button.
- 3 Import Controllers into Location Hierarchy**: Once the controllers are connected, you can import them into location hierarchy. A box shows "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 links to "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".

Schritt 2: Aktivieren Sie das Optionsfeld neben Ihrem Kontonamen, und klicken Sie auf Weiter. Wenn Sie bereits einige Standorte hinzugefügt haben, werden diese in der folgenden Liste angezeigt:



Schritt 3: Suchen Sie die IP-Adresse des Controllers, aktivieren Sie das Kontrollkästchen neben dieser, und drücken Sie **Weiter**:



Schritt 4: Da keine weiteren Standorte hinzugefügt wurden, klicken Sie auf Fertig stellen:



Schritt 5: Eine Aufforderung, zu bestätigen, dass der WLC erfolgreich in die Standorthierarchie importiert wurde, wird angezeigt:



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

Nachdem der WLC erfolgreich mit der Cloud verbunden wurde, können Sie alle anderen DNA-Spaces-Funktionen verwenden.

**Hinweis:** Der NMSP-Datenverkehr verwendet immer die Wireless-Management-Schnittstelle für die Kommunikation mit DNA Spaces oder CMX. Dies kann in der Controller-Konfiguration des 9800 nicht geändert werden. Die Schnittstellenummer ist irrelevant, wobei die Schnittstelle, die auf dem 9800-Controller als Wireless Management Interface (Wireless-Verwaltungsschnittstelle) zugewiesen ist, verwendet wird.

## Organisieren der Standorthierarchie in Cisco DNA-Bereichen

Wenn eine neue Standorthierarchie gewünscht wird oder wenn in Schritt 4 des Abschnitts **Import the 9800 controller to Cisco DNA Spaces (9800-Controller in Cisco DNA-Bereiche importieren)** keine Standorte hinzugefügt wurden, können Sie diese manuell konfigurieren.

Die Standorthierarchie ist eines der wichtigsten Merkmale von DNA-Bereichen, da sie für Analyseinformationen verwendet wird und auf dieser Grundlage die Regeln der Captive Portals konfiguriert werden. Je detaillierter die Standorthierarchie ist, desto präziser ist die Kontrolle über die Regeln des Captive Portals und über die Informationen, die aus DNA Spaces abgerufen werden können.

Die Funktion für die Standorthierarchie in DNA Spaces funktioniert auf dieselbe Weise wie die traditionelle Hierarchie von Cisco Prime Infrastructure oder Cisco CMX, aber die Benennung ist ganz anders. Wenn der Controller in die Standorthierarchie importiert wird, stellt er die Entsprechung des **Campus** aus der traditionellen Hierarchie dar. unter dem Controller können **Gruppen** erstellt werden, die **Gebäuden** entsprechen; Dann können unter den Gruppen **Netzwerke** konfiguriert werden, die den **Stockwerken** entsprechen, und schließlich können unter den Netzwerken Zonen erstellt werden, die auf derselben Ebene bleiben wie in der herkömmlichen Standorthierarchie. Zusammenfassend ist dies die Äquivalenz:

Tabelle 1: Gleichwertigkeit zwischen den traditionellen Hierarchieebenen und den Ebenen der DNA-Räume.

DNA-Spaces-Hierarchie	Traditionelle Hierarchie
Controller (Wireless-Netzwerk)	Campus
Gruppe	Gebäude
Netzwerk	Boden
Zone	Zone

Schritt 1: Konfigurieren Sie eine Gruppe. Je nach Geschäftsfeld organisieren Gruppen mehrere Standorte oder Zonen basierend auf der geografischen Lage, der Marke oder einer anderen Gruppierung. Navigieren Sie zur **Standorthierarchie**, bewegen Sie die Maus auf dem vorhandenen Wireless-Controller, und klicken Sie auf **Gruppe erstellen**.



Um den Namen der Standortebene zu ändern, bewegen Sie den Mauszeiger im Netzwerk, und klicken Sie auf "**Umbenennen**".

Schritt 2: Geben Sie den Gruppennamen ein, und wählen Sie den **nicht konfigurierten** Standort aus, der alle mit dem Controller importierten Access Points enthält. Diese APs werden dann nach Bedarf Netzwerken und Zonen zugeordnet. Klicken Sie auf **Hinzufügen**.

**Add Group** ✕

---

---

Select Location

Unconfigured

---

Schritt 3: Erstellen Sie ein Netzwerk. Ein Netzwerk oder ein Standort wird in Cisco DNA Spaces definiert als alle Access Points in einem als Standort konsolidierten physischen Gebäude. Bewegen Sie die Maus auf die Gruppe, und klicken Sie auf **Netzwerk hinzufügen**.

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

MORE ACTIONS

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

**Hinweis:** Dies ist der wichtigste Knoten in der Standorthierarchie, da hier geschäftliche Einblicke und Standortanalyseberechnungen generiert werden.

Schritt 4: Geben Sie den Netzwerknamen und das Präfix für den Access Point ein, und klicken Sie auf **Abrufen**. DNA Spaces ruft alle APs ab, die diesem Controller mit diesem Präfix zugeordnet sind, und ermöglicht es, die Access Points dem Boden hinzuzufügen. Es kann nur ein Präfix eingegeben werden.

### Add Network ✕

10.10.30.5

NETWORK NAME  
Second Floor

ACCESS POINT PREFIX  
28 Fetch

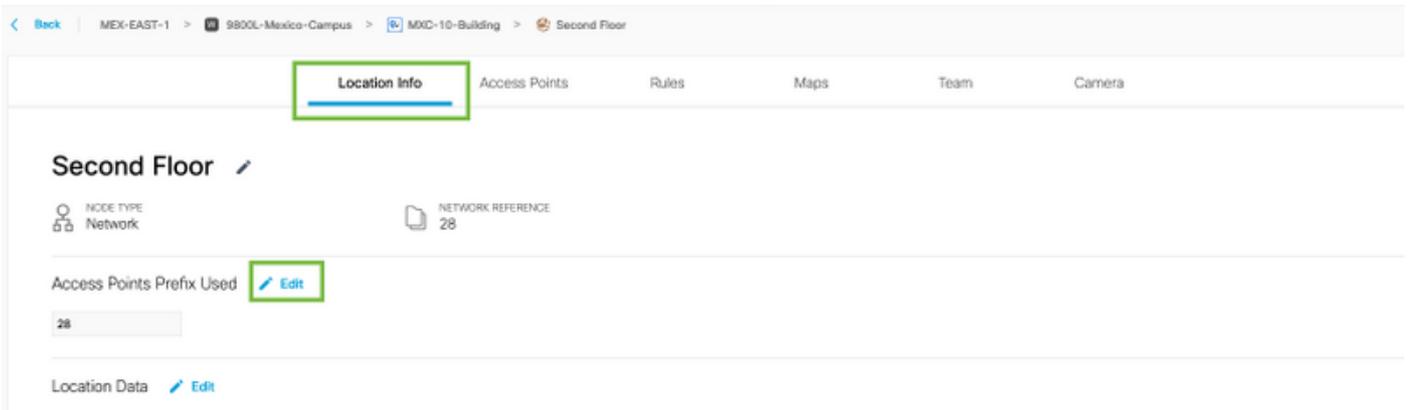
Matching access points will be shown below

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

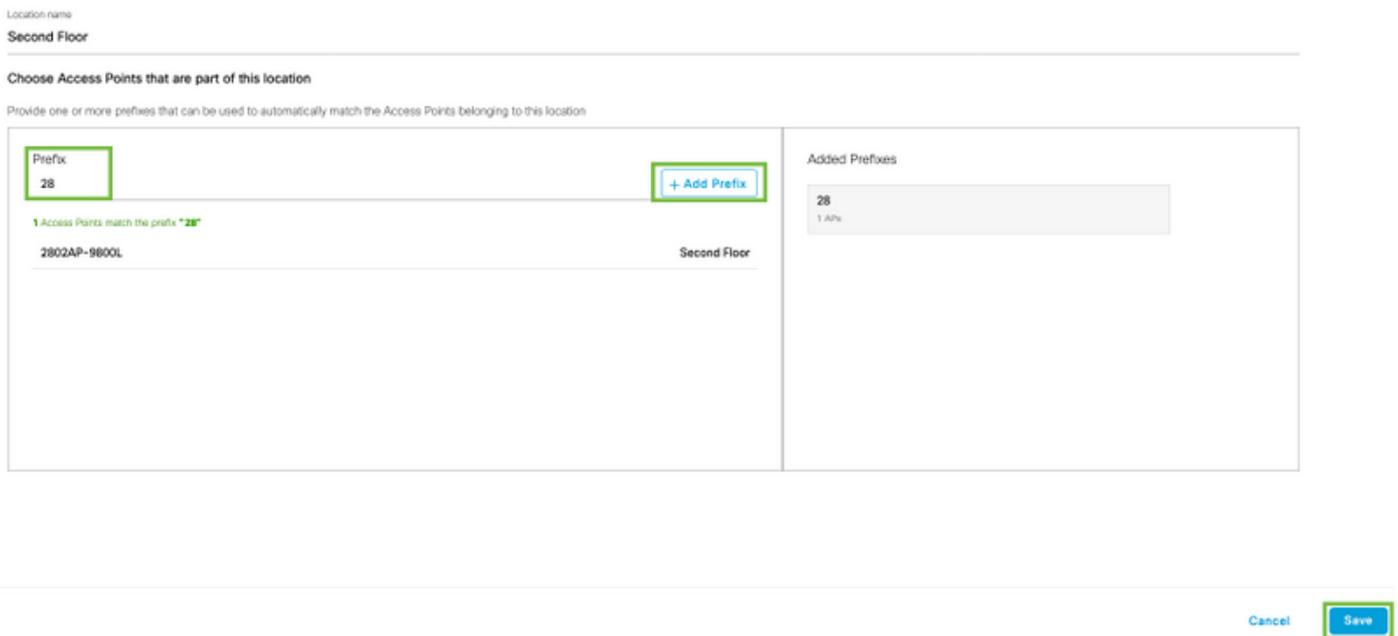
2802AP-9800L

Done

Schritt 5: Falls mehr Präfixe im Netzwerk benötigt werden. Klicken Sie auf den Netzwerknamen, und klicken Sie auf der Registerkarte **Standortinformationen** auf die Schaltfläche **Bearbeiten** neben **Zugangspunktpräfix verwendet**.



Geben Sie den Präfixnamen ein, klicken Sie auf **+Präfix hinzufügen**, und **speichern**. Wiederholen Sie diese Schritte für alle Präfixe, um die APs dem Netzwerk zuzuordnen und die APs später Zonen zuzuordnen.



Schritt 6: Erstellen einer Zone. Eine Zone ist eine Zusammenstellung von Access Points innerhalb eines Gebäudeabschnitts. Sie kann anhand der Abteilungen eines physischen Gebäudes oder einer Organisation definiert werden. Bewegen Sie die Maus über das Netzwerk, und wählen Sie **Bereich hinzufügen** aus.



Schritt 7: Konfigurieren Sie den **Zonennamen**, wählen Sie die Access Points für die Zone aus, und klicken Sie auf **Hinzufügen**:

Add Zone



Wireless-Zone

Select Access Points

Network Access Points

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

Add

## Fehlerbehebung und häufige Probleme

### Häufige Probleme

Die Webseite unter **Überwachung > Wireless > NMSP** (oder unter dem Befehl `nmsp cloud-services summary` angezeigt wird) zeigt normalerweise genügend Informationen über den Verbindungsfehler an. Einige häufige Fehler finden Sie in den Screenshots unten:

1. Wenn kein DNS konfiguriert ist, wird die Fehlermeldung "*Übertragungsfehler (6): Der Hostname konnte nicht aufgelöst werden*" wird angezeigt:

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	Transfer error (6): Couldn't resolve host name	Rx Subscr Request	0
Last Request Status		Tx DataBytes	0
		Rx DataBytes	0
Heartbeat Status		Tx Heartbeat Fail	1
		Rx Data Fail	0
		Tx Data Fail	0

Das Zertifikat wird nicht installiert oder das NTP wird nicht konfiguriert. Die Fehlermeldung lautet: "Übertragungsfehler (60): SSL-Peer-Zertifikat oder SSH-Remote-Schlüssel war nicht in Ordnung":

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	Transfer error (60): SSL peer certificate or SSH remote key was not OK	Rx Subscr Request	0
Last Request Status		Tx DataBytes	0
		Rx DataBytes	0
Heartbeat Status		Tx Heartbeat Fail	1
		Rx Data Fail	0
		Tx Data Fail	0

## Radioaktive Nachverfolgung

Wie alle anderen Controller der Serie 9800 unterstützt auch EWC stets aktive Radioactive Traces. Um diese zu erfassen und zu sehen, warum die Verbindung nicht hergestellt wird, muss bekannt sein, an welche DNS Spaces-IP-Adresse der EWC herantritt. Diese finden Sie unter **Monitor > Wireless > NMSP** oder über die CLI:

```
EWC#show nmsp status
```

```
NMSP Status
```

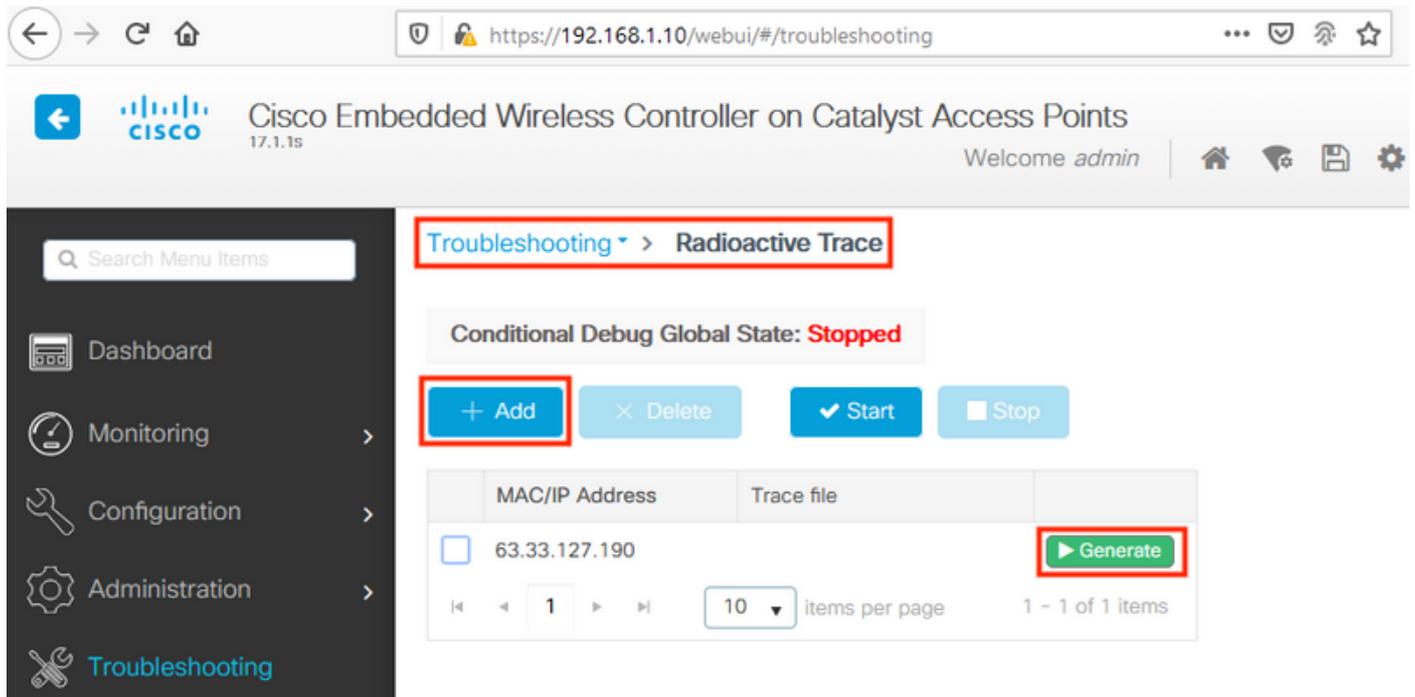
```
-----
```

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

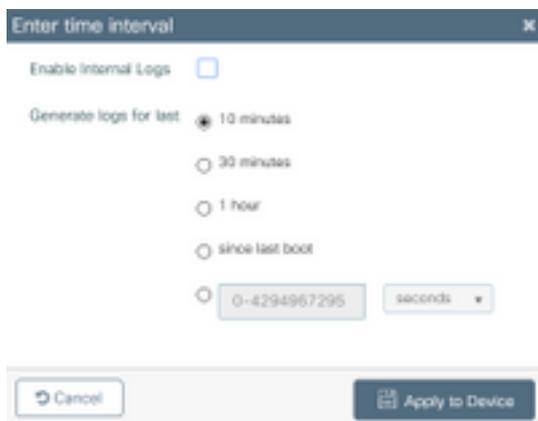
```
-----
```

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

Der EWC in dieser Testeinrichtung ist mit 63.33.127.190 verbunden. Kopieren Sie diese IP-Adresse, und navigieren Sie zu **Troubleshooting > Radioactive Trace**. Klicken Sie auf Hinzufügen, fügen Sie die IP-Adresse ein, und klicken Sie auf Generieren:



Wählen Sie **Protokolle** für die letzten 10 Minuten **erstellen** aus, und klicken Sie auf Übernehmen. Durch die Aktivierung interner Protokolle können große Datenmengen generiert werden, die schwer zu analysieren sein können:



**Hinweis:** Fehlerhaft konfigurierte DNS-, NTP- und fehlende Zertifikate generieren keine radioaktiven Spuren.

Beispiel für eine Radioaktive Nachverfolgung in einem Fall, in dem die Firewall das HTTPS

blockiert:

```
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmosp-main] [11100]: (note): CMX [63.33.127.190]:[32]: closing
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmosp-https] [11100]: (debug): Called 'is_ready'
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmosp-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}: [nmosp-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}: [nmosp-enc] [11100]: (debug): Decoding control message structure
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmosp-enc] [11100]: (debug): Control structure was successfully decoded from message
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmosp-db] [11100]: (debug): Retrieving CMX entry: 32
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmosp-db] [11100]: (ERR): CMX entry 32 not found
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmosp-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}: [nmosp-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}: [nmosp-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}: [nmosp-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}: [nmosp-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}: [nmosp-main] [11100]: (note): CMX [63.33.127.190]:[32]: down
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmosp-main] [11100]: (debug): NMSP timer 0xab774af4: close
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmosp-https] [11100]: (debug): Decrease reference count for https_con object: Now it's 1
```

Beispiel für Radioactive Trace für eine erfolgreiche Verbindung mit der Cloud:

```
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmosp-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}: [nmosp-https] [11100]: (debug): Cloud authentication 2 step failed, trying legacy mode
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmosp-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}: [nmosp-https] [11100]: (debug): tenant ID: vasilijeperovic
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmosp-https] [11100]: (debug): hostname is: data.dnaspaces.eu
2020/02/24 18:53:20.635 {nmspd_R0-0}{1}: [nmosp-https] [11100]: (note): Starting authentication V1 using Heartbeat URL https://data.dnaspaces.eu/api/config/v1/nmospconfig and Data URL https://data.dnaspaces.eu/networkdata
2020/02/24 18:53:20.635 {nmspd_R0-0}{1}: [nmosp-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}: [nmosp-https] [11100]: (debug): tenant ID: vasilijeperovic
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmosp-https] [11100]: (debug): hostname is: data.dnaspaces.eu
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmosp-https] [11100]: (debug): Authenticator V1 get heartbeat host: https://data.dnaspaces.eu/api/config/v1/nmospconfig
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmosp-https] [11100]: (debug): Authenticator V1 get access token: eyJ0eX[information omitted]rpmRq0g
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmosp-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}: [nmosp-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

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.