

# Implémenter un accès défini par logiciel pour les réseaux sans fil avec DNA

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[SD-Access](#)

[Architecture sans fil SD-Access](#)

[Aperçu](#)

[Rôles et terminologie SDA](#)

[Réseaux sous-jacents et superposés](#)

[Workflows de base](#)

[Joindre AP](#)

[Client à bord](#)

[Itinéraires des clients](#)

[Configurer](#)

[Diagramme du réseau](#)

[Détection et mise en service WLC dans Cisco DNA](#)

[Ajouter un WLC](#)

[Ajouter des points d'accès](#)

[Créer un SSID](#)

[Provisionner le WLC](#)

[Provisionnement des points d'accès](#)

[Créer un site de fabric](#)

[Ajouter un WLC au fabric](#)

[Joindre AP](#)

[Client à bord](#)

[Vérifier](#)

[Vérification de la configuration du fabric sur WLC et Cisco DNA](#)

[Dépannage](#)

[Le client n'obtient pas d'adresse IP](#)

[Le SSID n'est pas diffusé](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment implémenter SDA pour la technologie sans fil liée au WLC activé par le fabric et accéder au LAP sur Cisco DNA.

# Conditions préalables

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration des contrôleurs LAN sans fil (WLC) du 9800
- Points d'accès légers (LAP)
- ADN Cisco

## Composants utilisés

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

- WLC 9800-CL Cisco IOS® XE, version 17.9.3
- Points d'accès Cisco : 9130AX, 3802E, 1832I
- Cisco DNA version 2.3.3.7

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.

## SD-Access

L'accès défini par logiciel établit et applique automatiquement des politiques de sécurité sur l'ensemble du réseau, avec des règles dynamiques et une segmentation automatisée, et permet à l'utilisateur final de contrôler et de configurer la façon dont les utilisateurs se connectent à leur réseau. SD-Access établit un niveau de confiance initial avec chaque terminal connecté et le surveille en permanence pour vérifier à nouveau son niveau de confiance. Si un terminal ne se comporte pas normalement ou si une menace est détectée, l'utilisateur final peut immédiatement le confiner et agir, avant que la violation ne se produise, réduire les risques pour l'entreprise et protéger ses ressources. Solution entièrement intégrée et facile à déployer et à configurer sur les réseaux nouveaux et déployés.

SD-Access est une technologie Cisco qui est une évolution du réseau de campus traditionnel qui fournit un réseau basé sur l'intention (IBN) et un contrôle central des politiques à l'aide de composants SDN (Software-Defined Networking).

Trois piliers réseau de SD-Access :

1. Un fabric réseau : Il s'agit d'une abstraction du réseau lui-même qui prend en charge les superpositions programmables et la virtualisation. Le fabric de réseau prend en charge l'accès filaire et sans fil, lui permet d'héberger plusieurs réseaux logiques segmentés les uns par rapport aux autres et définis selon l'objectif de l'entreprise.

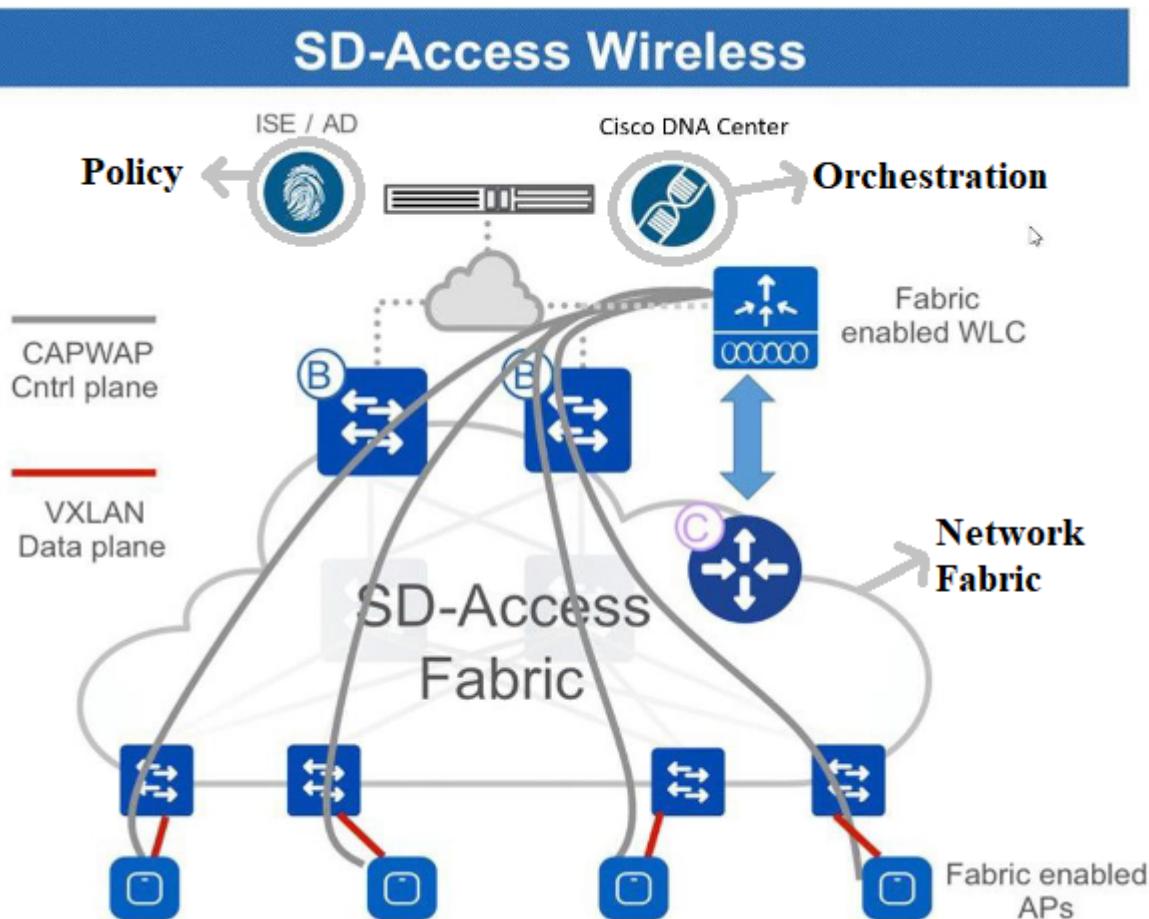
2. Orchestration : Cisco DNA est le moteur d'orchestration de SDA. Cisco DNA fonctionne comme un contrôleur SDN. Il met en oeuvre des politiques et des modifications de configuration dans le fabric. Intègre également un outil qui prend en charge la conception du réseau et prend en charge les opérations de télémétrie du réseau en temps réel et l'analyse des performances via DNA Assurance. Le rôle de Cisco DNA est d'orchestrer la structure du réseau pour apporter des modifications aux politiques et aux intentions du réseau en matière de sécurité, de qualité de service (QoS) et de microsegmentation.
3. Policy (politique) : Identity Services Engine (ISE) est l'outil qui définit la stratégie réseau. ISE organise la segmentation des périphériques et des noeuds en réseaux virtuels. ISE définit également les balises de groupe évolutives (SGT) utilisées par les périphériques d'accès pour segmenter le trafic utilisateur lorsqu'il entre dans le fabric. Les SGR sont chargés d'appliquer la politique de microsegmentation définie par ISE.

SDA repose sur une orchestration centralisée. La combinaison de Cisco DNA en tant que moteur d'orchestration programmable, d'ISE en tant que moteur de politiques et d'une nouvelle génération de commutateurs programmables en fait un système de fabric beaucoup plus flexible et facile à gérer que tout ce qui a pu être réalisé auparavant.



Remarque : Ce document traite spécifiquement de la technologie sans fil SD-Access.

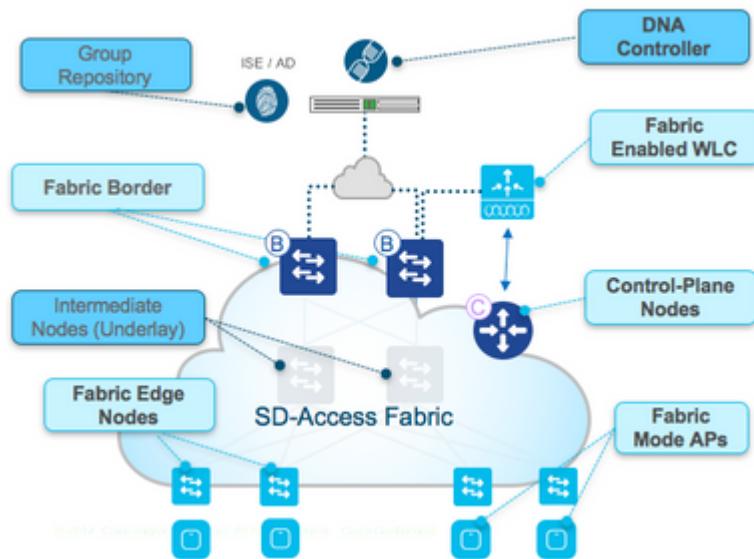
Le fabric de réseau se compose des éléments suivants :



L'intégration sans fil au fabric présente plusieurs avantages pour le réseau sans fil, par exemple : la simplification, la mobilité avec des sous-réseaux étendus sur des sites physiques ; et la microsegmentation avec une politique centralisée cohérente dans les domaines filaire et sans fil. Il permet également au contrôleur de se défaire du plan de données pour transférer des tâches tout en continuant à fonctionner en tant que services centralisés et plan de contrôle pour le réseau sans fil. Ainsi, l'évolutivité du contrôleur sans fil est augmentée car il n'a plus besoin de traiter le trafic du plan de données, comme dans le modèle FlexConnect.

## Architecture sans fil SD-Access

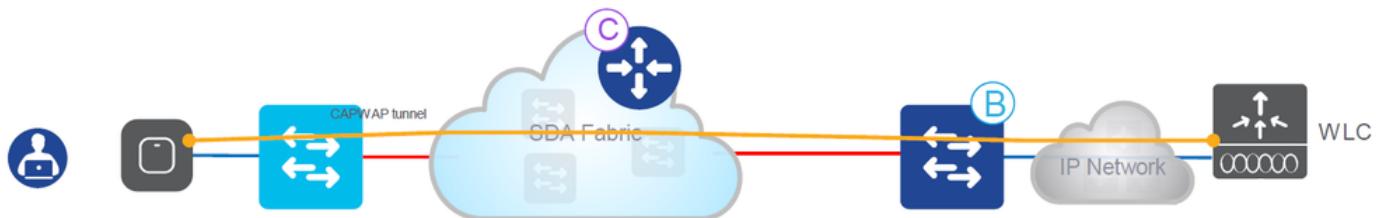
### Aperçu



Présentation SDA

Il existe deux principaux modèles de déploiement sans fil pris en charge par SDA :

L'une est une méthode OTT (over-the-top), un déploiement CAPWAP traditionnel connecté au-dessus d'un réseau câblé de fabric. La structure SDA transporte le trafic du plan de données et du contrôle CAPWAP vers le contrôleur sans fil :

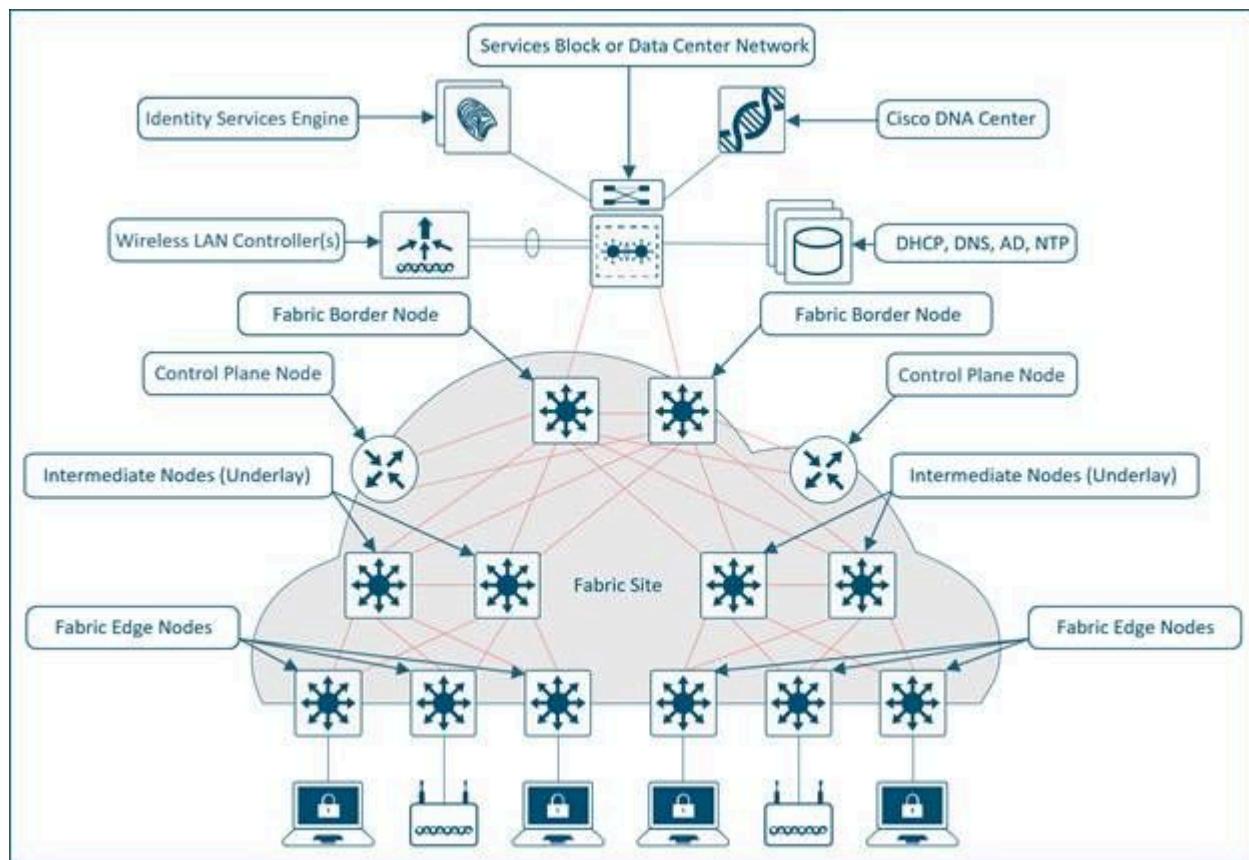


Méthode Par Capteur

Dans ce modèle de déploiement, le fabric SDA est un réseau de transport pour le trafic sans fil (modèle souvent déployé lors de migrations). Le point d'accès fonctionne de façon très similaire

au mode local classique : le contrôle CAPWAP et les plans de données se terminent sur le contrôleur, ce qui signifie que le contrôleur ne participe pas directement au fabric. Ce modèle est souvent utilisé lors de la migration initiale de commutateurs filaires vers le fabric SDA, mais le réseau sans fil n'est pas encore prêt pour une intégration de superposition de fabric complète.

Les autres modèles de déploiement sont des modèles SDA entièrement intégrés. Le réseau sans fil est entièrement intégré au fabric et participe aux superpositions. Il permet à différents WLAN de faire partie de différents réseaux virtuels (VN). Le contrôleur sans fil gère uniquement le plan de contrôle CAPWAP (pour gérer les points d'accès), et le plan de données CAPWAP ne parvient pas au contrôleur :



Modèle SDA entièrement intégré

Le plan de données sans fil est géré de la même manière que les commutateurs câblés : chaque point d'accès encapsule les données dans un VXLAN et les envoie à un noeud de périphérie de fabric, où elles sont ensuite envoyées à travers le fabric vers un autre noeud de périphérie. Les contrôleurs sans fil doivent être configurés en tant que contrôleurs de fabric, ce qui constitue une modification de leur fonctionnement normal.

Les contrôleurs activés par le fabric communiquent avec le plan de contrôle du fabric, il enregistre les adresses MAC des clients de couche 2 et les informations VNI (Virtual Network Identifier) de couche 2. Les points d'accès sont responsables de la communication avec les points d'extrémité sans fil et assistent le plan de données VXLAN par l'encapsulation et le trafic de désencapsulation.

## Rôles et terminologie SDA

Le fabric de réseau se compose des éléments suivants :

- Noeud du plan de contrôle : Il s'agit du système de mappage d'emplacement (base de données hôte) qui fait partie du plan de contrôle LISP (Location Separator Protocol), qui gère l'identité de point d'extrémité (EID) avec les relations d'emplacement (ou les relations de périphérique). Soit le plan de contrôle peut être un routeur dédié qui a fourni des fonctions de plan de contrôle, soit il peut coexister avec d'autres éléments du réseau de fabric.
- Noeuds en limite du fabric : En général, il s'agit d'un routeur qui fonctionne à la frontière entre les réseaux externes et le fabric SDA et qui fournit des services de routage aux réseaux virtuels du fabric. Il connecte les réseaux externes de couche 3 au fabric SDA.
- Noeuds de périphérie de fabric : Périphérique au sein du fabric qui connecte des périphériques non-fabric, tels que des commutateurs, des points d'accès et des routeurs au fabric SDA. Il s'agit des noeuds qui créent les tunnels de superposition virtuels et les réseaux virtuels avec le réseau local virtuel extensible (VXLAN) et qui imposent les balises de groupe de sécurité au trafic lié au fabric. Les réseaux des deux côtés de la périphérie du fabric se trouvent à l'intérieur du réseau SDA. Ils connectent les terminaux filaires au fabric SD-Access.
- Noeuds intermédiaires : Ces noeuds se trouvent au coeur du fabric SDA et se connectent aux noeuds de périphérie ou de périphérie. Les noeuds intermédiaires transfèrent simplement le trafic SDA sous forme de paquets IP, sans savoir que plusieurs réseaux virtuels sont impliqués.
- WLC de fabric : Contrôleur sans fil activé par le fabric et participant au plan de contrôle SDA, mais ne traitant pas le plan de données CAPWAP.
- Points d'accès en mode fabric : Points d'accès activés pour le fabric. Le trafic sans fil est encapsulé par VXLAN au niveau du point d'accès, ce qui permet de l'envoyer dans le fabric via un noeud de périphérie.
- Cisco DNA (DNAC) : Le contrôleur SDN d'entreprise pour le réseau de fabric SDA (Software Defined Access) et est responsable des tâches d'automatisation et d'assurance. Il peut également être utilisé pour certaines tâches d'automatisation et connexes pour les périphériques réseau qui forment la couche sous-jacente (qui n'est pas liée à SDA) ainsi.
- ISE: Identity Services Engine (ISE) est une plate-forme de politiques améliorée qui peut servir une variété de rôles et de fonctions, dont le moindre n'est pas celui du serveur AAA (Authentication, Authorization and Accounting). ISE interagit généralement avec Active Directory (AD), mais les utilisateurs peuvent également être configurés localement sur ISE lui-même pour des déploiements plus petits.



Remarque : Le plan de contrôle est un élément essentiel de l'infrastructure de l'architecture SDA. Il est donc recommandé de le déployer de manière résiliente.

# Réseaux sous-jacents et superposés

L'architecture SDA utilise une technologie de fabric qui prend en charge les réseaux virtuels programmables (réseaux superposés) qui s'exécutent sur un réseau physique (réseau sous-jacent).

Un tissu est une superposition.

Un réseau de superposition est une topologie logique utilisée pour connecter virtuellement des périphériques, construite sur une topologie physique sous-jacente arbitraire. Il utilise d'autres attributs de transfert pour fournir des services supplémentaires qui ne sont pas fournis par le sous-jacent. Il est créé au-dessus du sous-réseau pour créer un ou plusieurs réseaux virtualisés et segmentés. En raison de la nature logicielle des superpositions, il est possible de les connecter de manière très flexible sans les contraintes de connectivité physique. Il s'agit d'un moyen simple d'appliquer des politiques de sécurité, car la superposition peut être programmée pour avoir un point de sortie physique unique (le noeud de périphérie de fabric) et un pare-feu peut être utilisé pour protéger les réseaux derrière elle (qu'ils puissent être localisés ou non). La superposition encapsule le trafic avec l'utilisation de VXLAN. VXLAN encapsule des trames de couche 2 complètes pour le transport à travers le réseau sous-jacent, chaque réseau superposé étant identifié par un identificateur de réseau VXLAN (VNI). Les fabrics de superposition sont généralement complexes et nécessitent une charge administrative importante sur les nouveaux réseaux virtuels déployés ou pour mettre en oeuvre des politiques de sécurité.

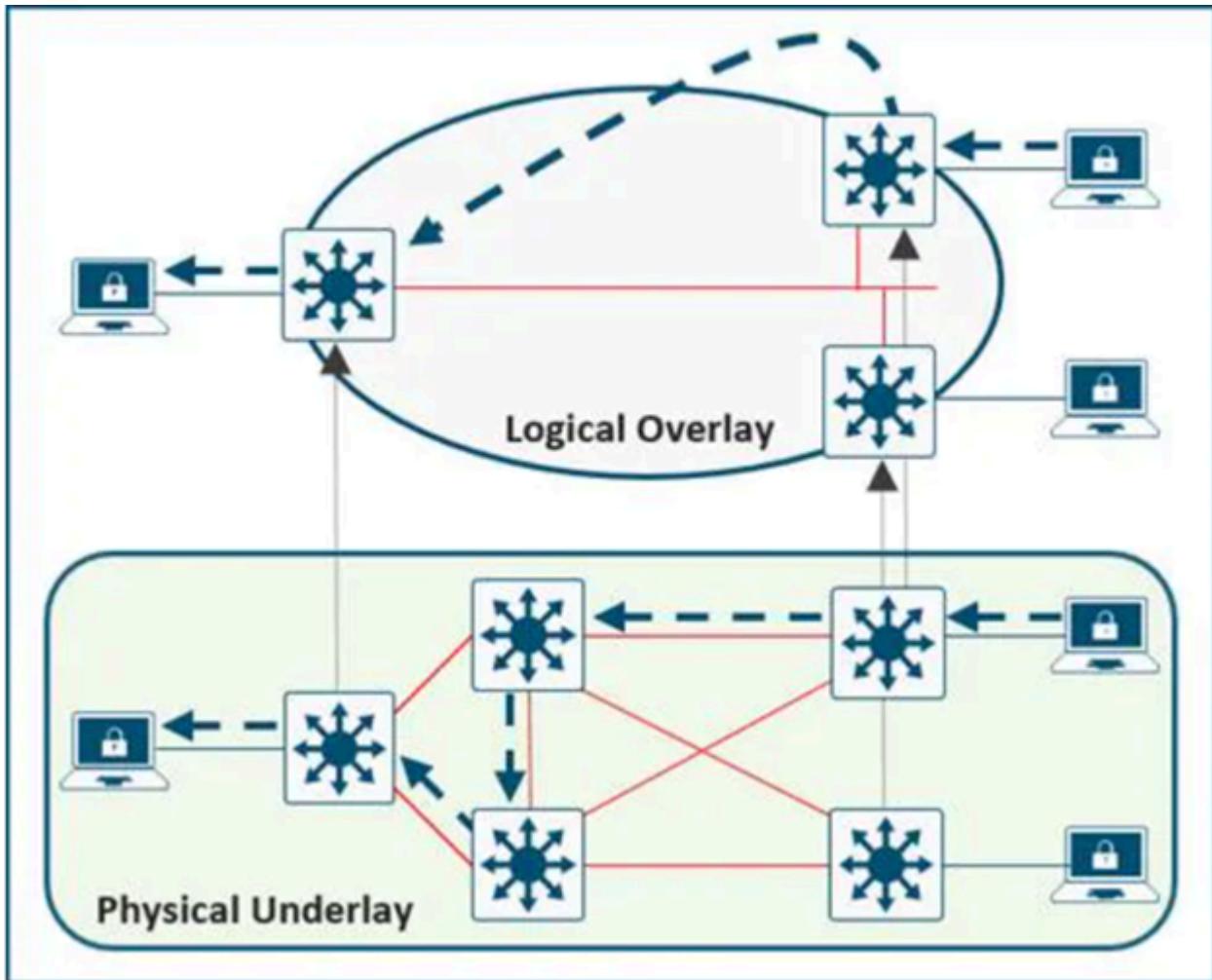
Exemples de superpositions réseau :

- GRE, mGRE
- MPLS, VPLS
- IPSec, DMVPN
- CAPWAP
- ZÉZAIEMENT
- OTV
- DFA
- ACI

Un réseau sous-jacent est défini par les noeuds physiques tels que les commutateurs, les routeurs et les points d'accès sans fil qui sont utilisés pour déployer le réseau SDA. Tous les éléments du réseau sous-jacent doivent établir une connectivité IP via l'utilisation d'un protocole de routage. Bien qu'il soit peu probable que le réseau sous-jacent utilise le modèle d'accès, de distribution et de cœur de réseau traditionnel, il doit utiliser une fondation de couche 3 bien conçue qui offre des performances, une évolutivité et une haute disponibilité robustes.



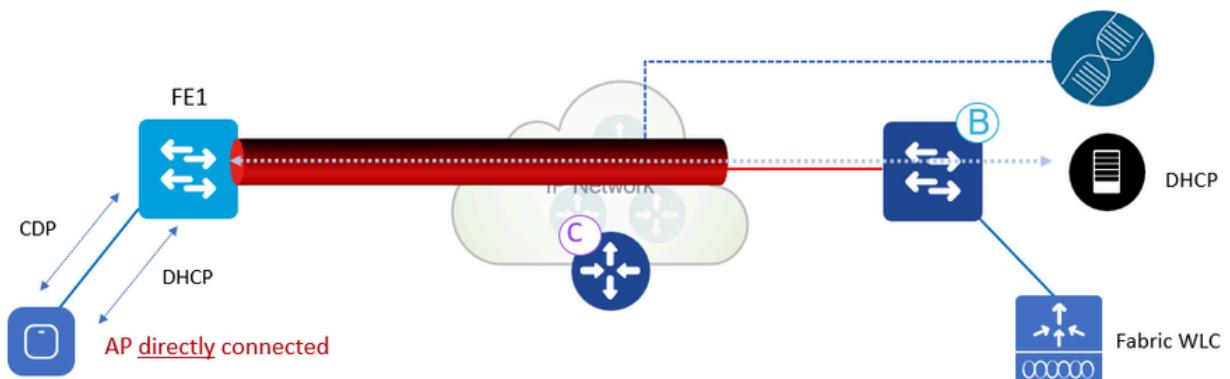
Remarque : SDA prend en charge IPv4 dans le réseau sous-jacent et IPv4 et/ou IPv6 dans les réseaux superposés.



Réseaux sous-jacents et superposés

## Workflows de base

Joindre AP



Workflow de jointure AP

Flux de connexion AP :

1. L'administrateur configure le pool AP dans DNAC dans INFRA\_VN. Cisco DNA prévisionne

une configuration sur tous les noeuds de périphérie de fabric pour intégrer automatiquement les points d'accès.

2. Le point d'accès est branché et se met sous tension. Fabric Edge détecte qu'il s'agit d'un point d'accès via CDP et applique la macro pour affecter (ou le modèle d'interface) le port de commutateur au VLAN approprié.

3. AP obtient une adresse IP via DHCP dans la superposition.

4. Fabric Edge enregistre l'adresse IP et MAC (EID) des points d'accès et met à jour le plan de contrôle (CP).

5. AP apprend IP WLC avec des méthodes traditionnelles. Le point d'accès de fabric se joint en tant que point d'accès en mode local.

6. Le WLC vérifie s'il est compatible avec le fabric (points d'accès de phase 2 ou 1).

7. Si AP est pris en charge pour le fabric, WLC interroge le PC pour savoir si AP est connecté au fabric.

8. Le plan de contrôle (CP) répond au WLC avec RLOC. Cela signifie que le point d'accès est connecté au fabric et est indiqué comme « Fabric enabled » (activé par le fabric).

9. WLC effectue un enregistrement LISP L2 pour AP dans CP (c'est-à-dire un enregistrement client sécurisé « spécial » AP). Il est utilisé pour transmettre des informations de métadonnées importantes du WLC à la périphérie du fabric.

10. En réponse à cet enregistrement de proxy, le plan de contrôle (CP) notifie la périphérie du fabric et transmet les métadonnées reçues du WLC (indicateur indiquant qu'il s'agit d'un point d'accès et de l'adresse IP du point d'accès).

11. Fabric Edge traite les informations, apprend qu'il s'agit d'un point d'accès et crée une interface de tunnel VXLAN vers l'adresse IP spécifiée (optimisation : côté commutateur est prêt pour les clients à se joindre).

Les commandes debug/show peuvent être utilisées pour vérifier et valider le workflow de jointure AP.

Plan de contrôle

debug lisp control-plane all

show lisp instance-id <L3 instance id> ipv4 server (Doit afficher l'adresse IP du point d'accès enregistrée par le commutateur de périphérie auquel le point d'accès est connecté.)

show lisp instance-id <L2 instance id> ethernet server (Doit afficher la radio AP ainsi que l'adresse MAC Ethernet, la radio AP enregistrée par le WLC et la mac Ethernet par le commutateur de périphérie auquel l'AP est connecté.)

Commutateur de périphérie

debug access-tunnel all

debug lisp control-plane all

show access-tunnel summary

show lisp instance < ID d'instance L2> ethernet database wlc access-points (Doit afficher le point d'accès radio mac ici.)

WLC

show fabric ap summary

Débogages LISP WLC

set platform software trace wncl chassis active r0 lisp-agent-api debug

set platform software trace wncl chassis active r0 lisp-agent-db debug

set platform software trace wncl chassis active r0 lisp-agent-fsm debug

set platform software trace wncl chassis active r0 lisp-agent-internal debug

set platform software trace wncl chassis active r0 lisp-agent-lib debug

set platform software trace wncl chassis active r0 lisp-agent-lispmsg debug

set platform software trace wncl chassis active r0 lisp-agent-shim debug

set platform software trace wncl chassis active r0 lisp-agent-transport debug

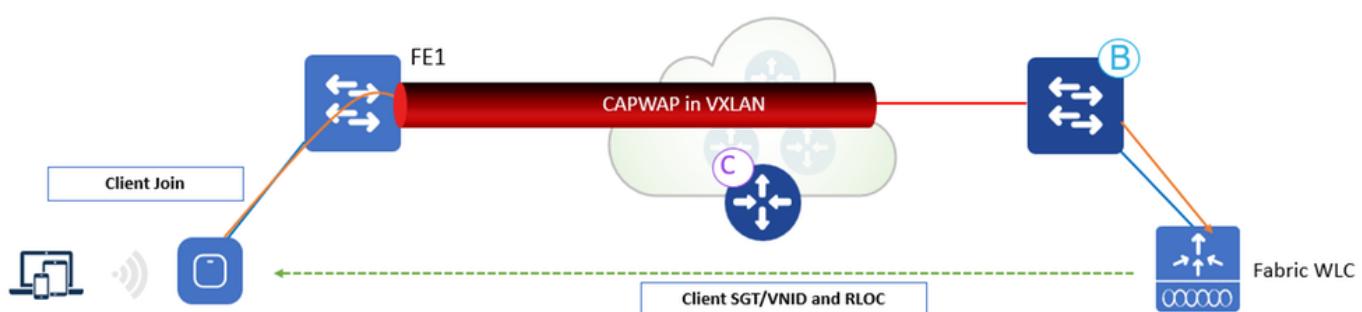
set platform software trace wncl chassis active r0 lisp-agent-ha debug

set platform software trace wncl chassis active r0 ewlc-infra-evq debug

Point d'accès

show ip tunnel fabric

Client à bord



### Workflow intégré au client :

1. Le client s'authentifie auprès d'un WLAN compatible Fabric. WLC obtient SGT de ISE, met à jour AP avec L2VNID client et SGT ainsi que RLOC IP. WLC connaît le RLOC du point d'accès depuis la base de données interne.
2. Le proxy WLC enregistre les informations de couche 2 du client dans CP ; Il s'agit d'un message LISP modifié pour transmettre des informations supplémentaires, comme le client SGT.
3. La périphérie du fabric est avertie par le processeur et ajoute l'adresse MAC du client dans la couche 2 à la table de transfert, puis va chercher la stratégie à partir d'ISE en fonction de l'adresse SGT du client.
4. Le client lance la requête DHCP.
5. Le point d'accès l'encapsule dans VXLAN avec les informations VNI de couche 2.
6. Fabric Edge mappe le VNID de couche 2 à l'interface VLAN et transfère DHCP dans la superposition (comme pour un client de fabric câblé).
7. Le client reçoit une adresse IP du serveur DHCP.
8. La surveillance DHCP (et/ou ARP pour la surveillance statique) déclenche l'enregistrement de l'EID du client par la périphérie du fabric sur le PC.

Les commandes debug/show peuvent être utilisées pour vérifier et valider le workflow intégré du client.

#### Plan de contrôle

debug lisp control-plane all

Commutateur de périphérie

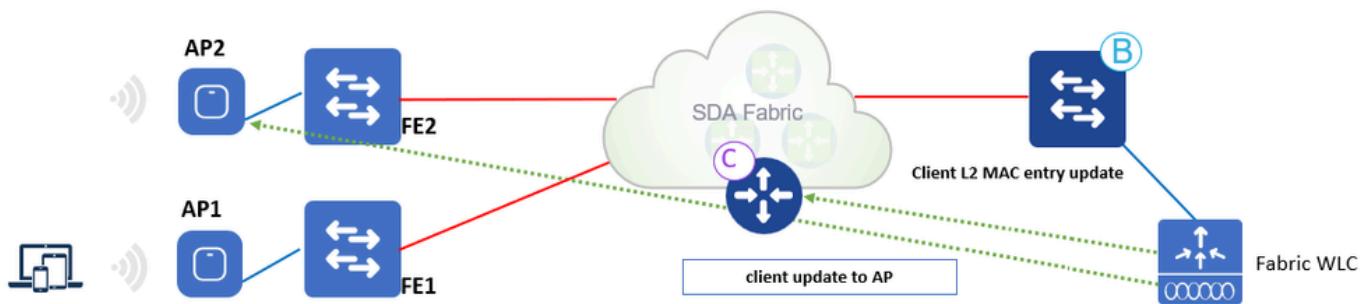
debug lisp control-plane all

debug ip dhcp snooping packet/event

#### WLC

Pour la communication LISP, mêmes débogages que la jointure AP.

#### Itinéraires des clients



Flux de travail Itinérance client

Flux de travail des itinéraires client :

1. Le client se déplace vers AP2 sur FE2 (itinérance entre commutateurs). WLC reçoit une notification par AP.
2. Le WLC met à jour la table de transfert sur le point d'accès avec les informations du client (SGT, RLOC).
3. WLC met à jour l'entrée MAC L2 dans CP avec le nouveau RLOC Fabric Edge 2.
4. CP notifie ensuite :
  - Fabric Edge FE2 (commutateur d'itinérance) pour ajouter l'adresse MAC du client à la table de transfert qui pointe vers le tunnel VXLAN.
  - Fabric Edge FE1 (commutateur d'itinérance) pour effectuer le nettoyage du client sans fil.
5. Fabric Edge met à jour l'entrée L3 (IP) dans la base de données CP dès qu'il reçoit le trafic.
6. L'itinérance est de couche 2, car la périphérie de fabric 2 possède la même interface VLAN (Anycast GW).

## Configurer

Diagramme du réseau

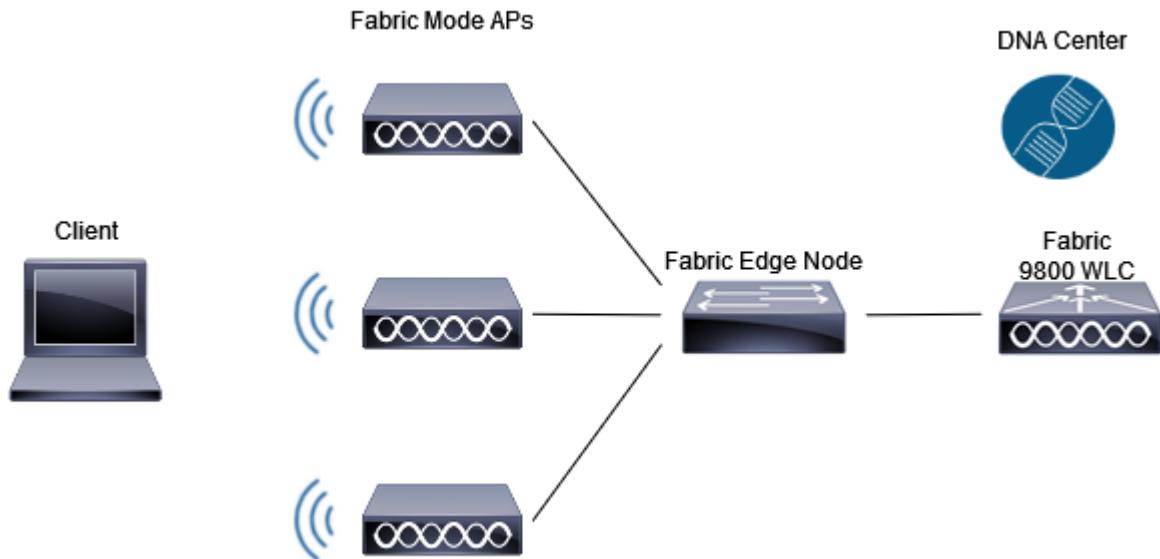


Diagramme du réseau

## Détection et mise en service WLC dans Cisco DNA

### Ajouter un WLC

Étape 1. Accédez à l'emplacement où vous souhaitez ajouter le WLC. Vous pouvez ajouter un nouveau bâtiment/étage.

Naviguez jusqu'à Design > Network Hierarchy et entrez le bâtiment/étage, ou vous pouvez créer un étage, comme illustré dans l'image :

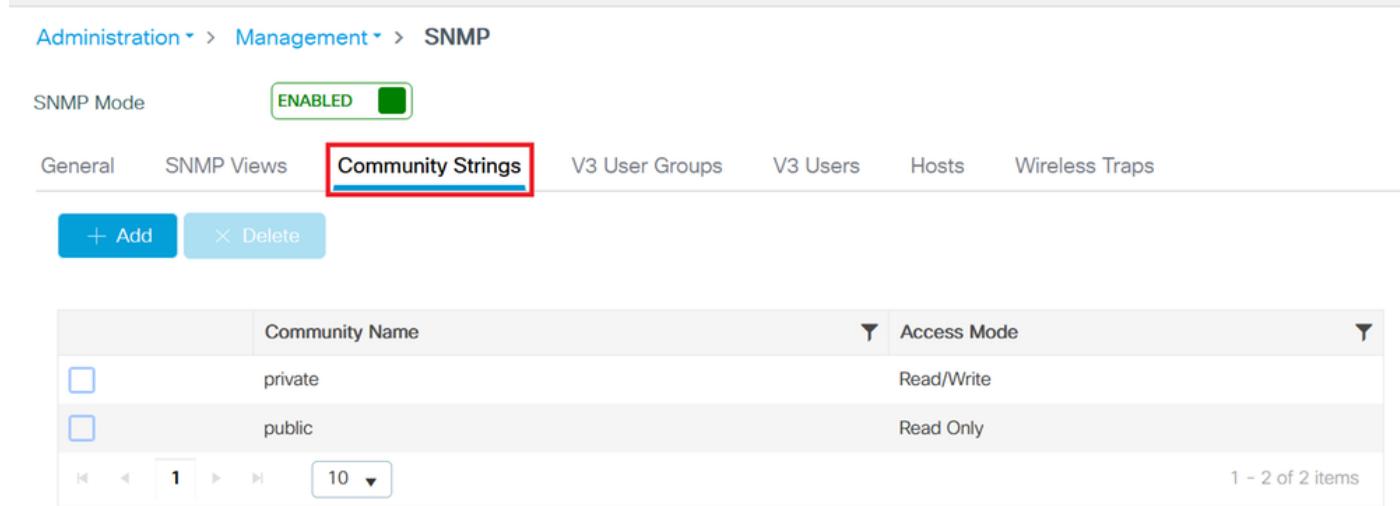
≡ Cisco DNA Center

The screenshot shows the Ekahau Site Survey mobile application. On the left, a sidebar displays a hierarchical list of sites and floors. The 'Lisbon' site is expanded, showing 'Floor 1' and 'MyFloor' under the 'Lisbon' folder. On the right, a map of the 'CABEÇO DE MOURO' area is displayed, with several buildings outlined in white and green. A context menu is open over one of the buildings, listing options: 'Edit Building', 'Delete Building', 'Add Floor' (which is highlighted with a red box), 'Import Ekahau Project', 'Import Ekahau Survey', 'Sync: DNA Spaces/CMX', 'Export Maps', 'View Devices', and 'View Settings'.

## Créer un étage

Étape 3. Ajuster du sol. Vous pouvez également télécharger une image de la plante du sol.

et vérifiez la chaîne configurée. Vous devez ajouter la chaîne de communauté SNMP correcte lorsque vous ajoutez le WLC sur Cisco DNA, et vous assurer que netconf-yang est activé sur le WLC 9800 avec les commandes show netconf-yang status. À la fin, cliquez sur Add:



Administration > Management > SNMP

SNMP Mode: ENABLED

General SNMP Views **Community Strings** V3 User Groups V3 Users Hosts Wireless Traps

+ Add × Delete

|                          | Community Name | Access Mode |
|--------------------------|----------------|-------------|
| <input type="checkbox"/> | private        | Read/Write  |
| <input type="checkbox"/> | public         | Read Only   |

1 - 2 of 2 items

Configuration SNMP

Étape 5. Ajoutez l'adresse IP WLC, les identifiants CLI (les identifiants que Cisco DNA utilise pour se connecter au WLC et ceux-ci doivent être configurés sur le WLC avant de l'ajouter à Cisco DNA), la chaîne SNMP, et vérifiez si le port NETCONF est configuré sur le port 830 :

## Add Device

Device Controllability is **Enabled**. Configuration changes will be made on network devices during discovery/inventory or when device is associated to a site. Firepower Management Center devices are not supported. [Learn more](#) | [Disable](#)

Type\* **Network Device**

Device IP / DNS Name\* **10.48.39.186**

Credentials [Validate](#)

Note: CLI and SNMP credentials are mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.

**CLI**

Select global credential  Add device specific credential

Username\* **admin**

Enable Password **\*\*\*\*\***

WARNING: Do not use 'admin' as the username for your device CLI credentials, if you are using Cisco ISE as your AAA server. If you do, this can result in you not being able to login to your devices.

**SNMP**

Select global credential  Add device specific credential

Version\* **V2C**

Credential\* **private | Write**

SNMP RETRIES AND TIMEOUT\*

HTTP(S)

**NETCONF**

Port **830**

Hint

Netconf with user privilege 15 is mandatory for enabling Wireless Services on Wireless capable devices such as C9800 Switches/Controllers. The NETCONF credentials are required to connect to eWLC devices. Majority of data collection is done using NETCONF for eWLC.

Cancel **Add**

## Ajouter un WLC

Le WLC apparaît comme NA car Cisco DNA est toujours en cours de synchronisation :

| <input type="checkbox"/> | <input checked="" type="checkbox"/> | NA | 10.48.39.186 | <span>Reachable</span> | Not Available | <span>Managed</span> | N/A | NA | Assign |
|--------------------------|-------------------------------------|----|--------------|------------------------|---------------|----------------------|-----|----|--------|
|--------------------------|-------------------------------------|----|--------------|------------------------|---------------|----------------------|-----|----|--------|

WLC en cours de synchronisation

Une fois le processus de synchronisation terminé, vous pouvez voir le nom du WLC, l'adresse IP, s'il est accessible, géré et la version du logiciel :

|                          |                                     |                                       |                           |                     |                        |               |                      |     |           |        |        |
|--------------------------|-------------------------------------|---------------------------------------|---------------------------|---------------------|------------------------|---------------|----------------------|-----|-----------|--------|--------|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | 9800-17-9-RMI-RP-HA.dns-ams.cisco.com | <span>10.48.39.186</span> | Wireless Controller | <span>Reachable</span> | Not Available | <span>Managed</span> | N/A | No Health | Assign | 17.9.3 |
|--------------------------|-------------------------------------|---------------------------------------|---------------------------|---------------------|------------------------|---------------|----------------------|-----|-----------|--------|--------|

WLC synchronisé

Étape 6. Attribution du WLC à un site Dans la liste des périphériques, cliquez sur Assign et choisissez un site :

## Assign Device to Site

Serial Number  
9

Devices  
9800-17-9-RMI-RP-HA.dns-ams.cisco

 Choose a site

Attribuer un périphérique au site

Vous pouvez décider d'attribuer le site maintenant ou ultérieurement :

## Assign Device to Site

Now  Later

Generate configuration preview

Creates preview which can be later used to deploy on selected devices. View status in [Work Items](#)

Task Name\*

Assign 1 Device(s) to Site

Affecter un périphérique au site maintenant ou ultérieurement

## Ajouter des points d'accès

Étape 1.Une fois le WLC ajouté et accessible, naviguez à Provisioner > Inventaire > Global > Unassigned Devices et recherchez les AP que vous avez joint à votre WLC :

| Global                              |   |             |              |                     |   |   |   |   |              |                                       |
|-------------------------------------|---|-------------|--------------|---------------------|---|---|---|---|--------------|---------------------------------------|
| Unassigned Devices                  |   |             |              |                     |   |   |   |   |              |                                       |
| DEVICES (12)<br>FOCUS: Inventory    |   |             |              |                     |   |   |   |   |              |                                       |
|                                     |   | Device Name | IP Address   | Device Family       | Reachability  | EoX Status  | Manageability   | Compliance  | Health Score | Site                                  |
| <input checked="" type="checkbox"/> |  | 3800E-I     | 10.14.19.173 | Unified AP          |  Reachable   |  Not Scanned |  Managed | N/A   | 10           | <input type="button" value="Assign"/> |
| <input checked="" type="checkbox"/> |  | AP0C75      | 10.14.19.190 | Unified AP          |  Reachable   |  Not Scanned |  Managed | N/A   | 10           | <input type="button" value="Assign"/> |
| <input type="checkbox"/>            |  |             |              | Unified AP          |  Reachable   |  Not Scanned |  Managed | N/A   | 7            | <input type="button" value="Assign"/> |
| <input type="checkbox"/>            |  |             |              | Unified AP          |  Reachable   |  Not Scanned |  Managed | N/A   | NA           | <input type="button" value="Assign"/> |
| <input type="checkbox"/>            |  |             |              | Unified AP          |  Unreachable |  Not Scanned |  Managed | N/A   | NA           | <input type="button" value="Assign"/> |
| <input type="checkbox"/>            |  |             |              | Unified AP          |  Reachable   |  Not Scanned |  Managed | N/A   | NA           | <input type="button" value="Assign"/> |
| <input type="checkbox"/>            |  |             |              | Unified AP          |  Reachable   |  Not Scanned |  Managed | N/A   | NA           | <input type="button" value="Assign"/> |
| <input type="checkbox"/>            |  |             |              | Unified AP          |  Reachable   |  Not Scanned |  Managed | N/A   | NA           | <input type="button" value="Assign"/> |
| <input type="checkbox"/>            |  |             |              | Wireless Controller |  Reachable   |  Not Scanned |  Managed |  Non-Compliant | No Health    | <input type="button" value="Assign"/> |
| <input type="checkbox"/>            |  |             |              |                     |   |   |   |   |              |                                       |

Ajouter des points d'accès

Étape 2. Sélectionnez l'option Affecter. Attribuez les AP à un site. Cochez la case Apply to All (Appliquer à tout) pour configurer plusieurs périphériques à la fois.

## Assign Device to Site

The screenshot shows the 'Assign Device to Site' interface. It lists three devices assigned to site 'K':

- Device 1: Serial Number F, Device 3800E-I, Site K, with a checked 'Apply to All' checkbox.
- Device 2: Serial Number K, Device DO\_NOT\_MOVE.Static\_AP1, Site K.
- Device 3: Serial Number K, Device AP0C75, Site K.

Attribuer des points d'accès au site

Naviguez jusqu'à votre étage et vous pouvez voir tous les périphériques qui lui sont assignés - WLC et AP :

The screenshot shows a device inventory table with the following data:

| Device Name                           | IP Address   | Device Family       | Reachability | EoX Status  | Manageability | Compliance | Health Score | Site               | Image Version |
|---------------------------------------|--------------|---------------------|--------------|-------------|---------------|------------|--------------|--------------------|---------------|
| 3800E-I                               | 10.14.19.173 | Unified AP          | Reachable    | Not Scanned | Managed       | N/A        | 10           | .../Lisbon/Floor 1 | 17.9.3.50     |
| 9800-17-9-RMI-RP-HA.dns-ams.cisco.com | 10.48.39.186 | Wireless Controller | Reachable    | Not Scanned | Managed       | N/A        | 10           | .../Lisbon/Floor 1 | 17.9.3        |
| AP0C75                                | 10.14.19.190 | Unified AP          | Reachable    | Not Scanned | Managed       | N/A        | 10           | .../Lisbon/Floor 1 | 17.9.3.50     |
| DO_NOT_MOVE.Static_AP1                | 10.14.19.78  | Unified AP          | Reachable    | Not Scanned | Managed       | N/A        | 10           | .../Lisbon/Floor 1 | 17.9.3.50     |

Périphériques affectés au site

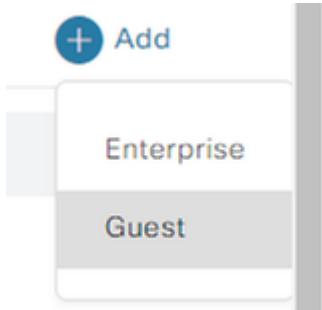
## Créer un SSID

Étape 1. Accédez à Design > Network Settings > Wireless > Global et ajoutez un SSID :

The screenshot shows the 'Wireless' tab in the network settings. The 'SSID' section is highlighted with a red box. A red box also highlights the 'Add' button in the top right corner.

Créer un SSID

Vous pouvez créer un SSID d'entreprise ou un SSID invité. Dans cette démonstration, un SSID invité est créé :



SSID d'entreprise ou invité

Étape 2. Choisissez le paramètre que vous souhaitez pour le SSID. Dans ce cas, un SSID ouvert est créé. L'état Admin et le SSID de diffusion doivent être activés :



## Basic Settings

Fill the information like name, wireless options, state and network to complete the basic setup of SSID

Wireless Network Name (SSID)\*

A text input field with the value 'Demo'. The entire input field is highlighted with a red rectangular border.

### Wireless Option ⓘ

- Multi band operation (2.4GHz, 5GHz, 6GHz)  Multi band operation with Band Select  5GHz only  2.4GHz only  6GHz Only

Primary Traffic Type

Best Effort (Silver)



### SSID STATE

Admin Status

Broadcast SSID

Paramètres de base SSID

# Security Settings

Configure the security level and authentication, authorization, & accounting for SSID

**SSID Name:** Demo (Guest)

Level of Security

L2 SECURITY

Enterprise    Personal    Open Secured    Open

**Least Secure :**

Any user can associate to the network.

L3 SECURITY

Web Policy    Open

**Least Secure :**

Any user can associate to the network.

Authentication, Authorization, and Accounting Configuration



Please associate one or more AAA servers using Configure AAA link to ensure right configuration is pushed for the selected security setting.



[Configure AAA](#)

Mac Filtering

Fast Lane [i](#)

Deny RCM Clients [i](#)

Paramètres de sécurité SSID



**Mise en garde :** N'oubliez pas de configurer et d'associer le serveur AAA pour le SSID. La liste de méthodes par défaut est mappée si aucun serveur AAA n'est configuré.

Lorsque vous cliquez sur next, vous pouvez voir les paramètres avancés de votre SSID :

## Advanced Settings

Configure the advanced fields to complete SSID setup.

**SSID Name:** Demo (Guest)

Fast Transition (802.11r)

Adaptive  Enable  Disable

Over the DS

11k

Neighbor List

MFP Client Protection [?](#)

Optional  Required  Disabled

Session Timeout [?](#)  in (secs)\*

Client Exclusion [?](#)  in (secs)\*

11v BSS Transition Support

BSS Max Idle Service

Client User Idle Timeout [?](#)  Client User Idle Timeout(Default: 300 secs)\*

Directed Multicast Service

Radius Client Profiling  [?](#)

NAS-ID [?](#)

NAS-ID Opt. 1 [-](#) [+](#)

Paramètres SSID avancés

Étape 3. Après la création du SSID, vous devez l'associer à un profil. Cliquez sur Ajouter un profil :

## Associate SSID to Profile

Select a Profile on the left or Add Profile and click 'Associate' to associate the SSID to Profile.

**SSID Name:** Demo (Guest)

 Add Profile

 0 profile(s) associated.

 Search

Ajouter un profil

Étape 4. Attribuez un nom au profil, sélectionnez Fabric et, à la fin, cliquez sur Associate Profile:

## Associate Profile

Cancel

Profile Name

DemoProfile

Fabric

Yes

No

Associer un profil

Un résumé du SSID et du profil que vous avez créés s'affiche :

# Summary

Review all changes

## ✓ Basic Settings [Edit](#)

|                      |  |
|----------------------|--|
| SSID Name            | Demo                                   |
| Primary Traffic Type | Best Effort (Silver) <a href="#">i</a> |
| Admin Status         | Yes                                    |
| Broadcast SSID       | Yes                                    |

---

## ✓ Security Settings [Edit](#)

|                  |      |
|------------------|------|
| L2 Security      | open |
| L3 Security      | open |
| AAA Servers      |      |
| Mac Filtering    | Yes  |
| Fast Lane        | No   |
| Deny RCM Clients | No   |
| Enable Posture   | No   |
| ACL Name         |      |

---

## ✓ Advanced Settings [Edit](#)

|                           |          |
|---------------------------|----------|
| Fast Transition (802.11r) | Disable  |
| Over the DS               | No       |
| MFP Client Protection     | Optional |
| Session Timeout           | 1800     |
| Client Exclusion          | 180      |
| Radius Client Profiling   | No       |
| NAS-ID                    |          |

---

## ✓ Network Profile Settings [Edit](#)

|             |                     |
|-------------|---------------------|
| DemoProfile | Fabric (Associated) |
|-------------|---------------------|

Récapitulatif SSID

que vous souhaitez configurer. Dans cette démonstration, les paramètres par défaut ont été configurés. Cliquez sur Enregistrer :

Wireless / Create RF Profile

This RF-Profile will be provisioned on the wireless lan controller during Access Point (AP) Network Provision or Access Point Plug and Play Onboarding. It will also be pushed during WLC network provisioning when the RF profile is associated to a network profile configured under advanced settings for AireOS controllers.

Create Wireless Radio Frequency Profile

Profile Name\*

PROFILE TYPE

2.4 GHz

Parent Profile

High  Medium (Typical)  Low  Custom

DCA Channel

Select All

1 4 11

Advanced Options

Select All

Show Advanced

Supported Data Rate

Enable 802.11b data rates

Mandatory Data Rates Choose upto two data rate

1 2 5.5 6 9 11 12 18 24 36 48 54

TX Power Configuration

Power Level

-10dBm 10dBm 30dBm RX SDR Medium

Save

Ajouter un profil RF de base

## Provisionnement des points d'accès

Étape 1. Accédez à votre bâtiment/étage. Sélectionnez APs et Actions > Provisionner > Provisionner le périphérique :

DEVICES (4)

FOCUS: Inventory

Actions

| Device Name             | Inventory          | Device Family           | Reachability | EoX Status  | Manageability | Compliance | Health Score | Site               |
|-------------------------|--------------------|-------------------------|--------------|-------------|---------------|------------|--------------|--------------------|
| 3800E-I                 | 3                  | Unified AP              | Reachable    | Not Scanned | Managed       | N/A        | 10           | .../Lisbon/Floor 1 |
| 9800-17-9-RMI-RP-HA.dns | Provision          | Assign Device to Site   | Reachable    | Not Scanned | Managed       | N/A        | 10           | .../Lisbon/Floor 1 |
| AP0C75                  | Telemetry          | Provision Device        | Reachable    | Not Scanned | Managed       | N/A        | 6            | .../Lisbon/Floor 1 |
| DO_NOT_MOVE_Static_AP1  | Device Replacement | LAN Automation          | Reachable    | Not Scanned | Managed       | N/A        | 10           | .../Lisbon/Floor 1 |
|                         | Others             | LAN Automation Status   | Reachable    | Not Scanned | Managed       | N/A        |              |                    |
|                         | Compliance         | Learn Device Config     | Reachable    | Not Scanned | Managed       | N/A        |              |                    |
|                         |                    | Configure WLC HA        | Reachable    | Not Scanned | Managed       | N/A        |              |                    |
|                         |                    | Configure WLC Mobility  | Reachable    | Not Scanned | Managed       | N/A        |              |                    |
|                         |                    | Manage LED Flash Status | Reachable    | Not Scanned | Managed       | N/A        |              |                    |

Provisionnement des points d'accès

Étape 2. Vérifiez si le site attribué est correct et sélectionnez Apply to All :

1 Assign Site    2 Configuration    3 Summary

|                    |                        |   |
|--------------------|------------------------|---|
| Serial Number<br>F | Devices<br>3800E-I     | Global/Lisbon/Lisbon/Floor 1 <span style="float: right;">X</span> |
| K                  | AP0C75                 | Global/Lisbon/Lisbon/Floor 1 <span style="float: right;">X</span> |
| K                  | DO_NOT_MOVE.Static_AP1 | Global/Lisbon/Lisbon/Floor 1 <span style="float: right;">X</span> |

Attribuer un site aux points d'accès

Étape 3. Sélectionnez un profil RF dans la liste déroulante et vérifiez que le SSID est le bon :

1 Assign Site    2 Configuration    3 Summary

|  |                        |                                |                                    |                      |
|--|------------------------|--------------------------------|------------------------------------|----------------------|
| Zones and SSIDs are listed from Provisioned Wireless profile(s) for each Access point. For newly added Zones and SSIDs, Please provision Controller prior to Access point provision. |                        |                                |                                    |                      |
| 9130AXE Access points with 17.6 version and higher, support advanced configurations to configure Radio Antenna profiles on Antenna slot.   |                        |                                |                                    |                      |
| <b>Advanced Configuration</b>  |                        |                                |                                    |                      |
| Serial Number<br>F   | Device Name<br>3800E-I | AP Zone Name<br>Not Applicable | RF Profile<br><b>DemoRFProfile</b> | SSIDs<br><b>Demo</b> |
| K  | AP0C75                 | Not Applicable                 | DemoRFProfile                      | Demo                 |
| K  | DO_NOT_MOVE.Static_AP1 | Not Applicable                 | DemoRFProfile                      | Demo                 |

Sélectionner un profil RF

Étape 4 : vérification des paramètres des points d'accès Si tout va bien, sélectionnez Déployer :

1 Assign Site 2 Configuration 3 Summary

3800E-I  
AP0075  
DO\_NOT\_MOVE\_Static\_API

Device Details

|                  |                              |
|------------------|------------------------------|
| Device Name:     | 3800E-I                      |
| Serial Number:   | F                            |
| Mac Address:     | 78                           |
| Device Location: | Global/Lisbon/Lisbon/Floor 1 |

AP Zone Details

|              |              |
|--------------|--------------|
| AP Zone Name | default-zone |
|--------------|--------------|

RF Profile Details

|                                |                                |
|--------------------------------|--------------------------------|
| RF Profile Name:               | DemoRFProfile                  |
| Radio Type                     | 2.4GHz                         |
| 5GHz                           | 6GHz                           |
| Parent Profile                 | HIGH                           |
| LOW                            | CUSTOM                         |
| Status                         | Enabled                        |
| Enabled                        | Enabled                        |
| DCA Channels                   | 1, 6, 11                       |
| 36, 40, 44, 48, 52, 56, 60, 64 | 37, 41, 45, 49, 53, 57, 61, 65 |
| Ignored DCA Channels           | N/A                            |
| 149,153,157,161                | 149,153,157,161                |
| Channel Width                  | 20 MHz                         |
| 20 MHz                         | Best                           |
| Supported Data Rates (in Mbps) | 9,12,18,24,36,48,54            |
| 6,9,12,18,24,36,48,54          | 6,9,12,18,24,36,48,54          |
| Mandatory Data Rates (in Mbps) | 9                              |
| 6                              | 6                              |
| Tx Power Level (in dBm)        | 7/30                           |
| -10/30                         | -10/30                         |
| TPC Power Threshold (in dBm)   | -70                            |
| -60                            | -70                            |
| Rx SOP                         | MEDIUM                         |
| LOW                            | AUTO                           |
| Max Client                     | 200                            |
| 200                            | 200                            |

Cancel

Deploy

Déploiement de provisionnements AP

Étape 5. La mise en service du périphérique peut être déployée à tout moment ou ultérieurement. À la fin, sélectionnez Apply :

## Provision Device

Now

Later

Generate configuration preview

Creates preview which can be later used to deploy on selected devices. If Site assignment is invoked during configuration preview, Device controllability configuration will be pushed to corresponding device(s). View status in [Work Items](#)

Task Name\*

Provision Device

Cancel

Apply

Provisionner les points d'accès maintenant ou ultérieurement



Mise en garde : Lors du provisionnement, les points d'accès, qui font déjà partie de l'étage configuré pour le profil RF sélectionné, doivent être traités et redémarrés.

Les points d'accès sont maintenant provisionnés.

Étape 6. Côté WLC, accédez à Configuration > Wireless > Access Points. Vérifiez que les balises AP ont été poussées à partir de Cisco DNA :

Configuration > Wireless > Access Points

▼ All Access Points

| Total APs : 3 |                            |                            | Misconfigured APs       |               |                  | Select an Action |         |
|---------------|----------------------------|----------------------------|-------------------------|---------------|------------------|------------------|---------|
| tion          | Country Code Misconfigured | LSC Fallback Misconfigured | Policy Tag              | Site Tag      | RF Tag           | Location         | Country |
| No            | No                         | PT_Lisbo_Lisbo_Flor1_45ce7 | ST_Lisbo_Lisbon_3e5f5_0 | DemoRFProfile | default location | PT               |         |
| No            | No                         | PT_Lisbo_Lisbo_Flor1_45ce7 | ST_Lisbo_Lisbon_3e5f5_0 | DemoRFProfile | default location | PT               |         |
| No            | No                         | PT_Lisbo_Lisbo_Flor1_45ce7 | ST_Lisbo_Lisbon_3e5f5_0 | DemoRFProfile | default location | PT               |         |

Balises sur les points d'accès

Étape 7. Accédez à Configuration > Tags & Profiles > WLANs et vérifiez que le SSID a été poussé à partir de Cisco DNA :

Configuration > Tags & Profiles > WLANs

| Selected WLANs : 0              |                         | WLAN Wizard |      |                      |  |
|---------------------------------|-------------------------|-------------|------|----------------------|--|
| <input type="checkbox"/> Status | Name                    | ID          | SSID | Security             |  |
| <input type="checkbox"/>        | Demo_Global_NF_986e8d08 | 17          | Demo | [open],MAC Filtering |  |

WLAN

## Créer un site de fabric

Étape 1. Accédez à Provisionner > Sites de fabric. Créez un site de fabric :

Virtual Networks

Fabric Sites

Transits

 Search Table

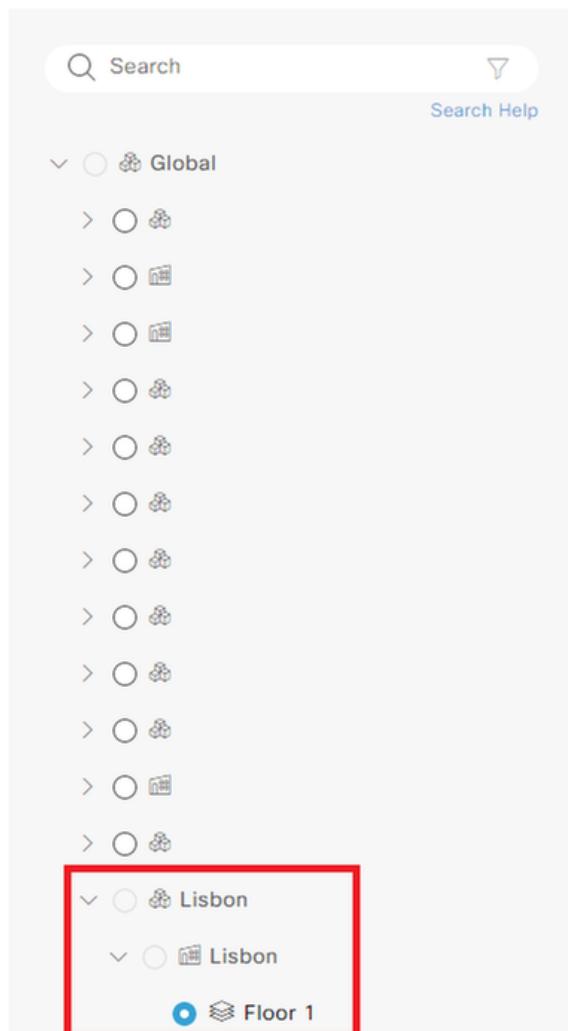
 Create Fabric Sites and Fabric Zones

Créer des sites de fabric

Étape 2. Sélectionnez le bâtiment/étage de votre site de fabric :

## Fabric Site Location

A Fabric Site begins at the selected level of hierarchy. All levels below the selected level are included as part of the Fabric Site.



The image shows a hierarchical tree structure for selecting a Fabric Site location. The root node is 'Global', indicated by a tree icon and a downward arrow. Below 'Global', there are ten intermediate nodes, each represented by a circle icon and a tree icon. The last node in this sequence is highlighted with a red box. Below this highlighted node, there is a branch with two leaf nodes: 'Lisbon' and 'Floor 1'. The 'Floor 1' node is also highlighted with a red box. The entire tree structure is contained within a light gray box.

- Global
  - 
  - 
  - 
  - 
  - 
  - 
  - 
  - 
  - 
  - 
  - Lisbon
    - Floor 1

Sélectionner le site de fabric

Étape 3. Sélectionnez un modèle d'authentification. Dans cette démonstration, None a été appliqué :

## Authentication Template

Select a Template for the Fabric Site. The Template will apply a port-based network access control configuration to all access ports on Edge Nodes and Extended Nodes.

- Closed Authentication [i](#) [Edit](#)
- Open Authentication [i](#) [Edit](#)
- Low Impact [i](#) [Edit](#)
- None [i](#)

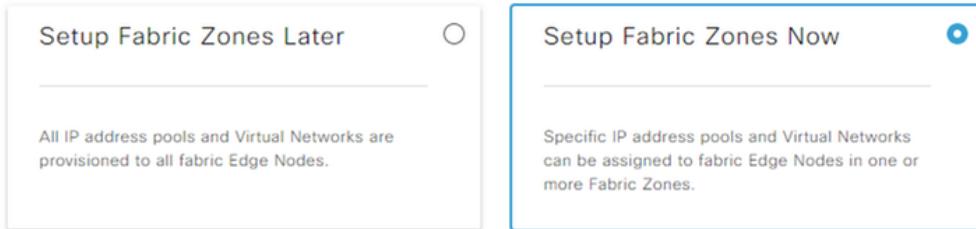
Modèle d'authentification

Étape 3. Vous pouvez choisir de configurer la zone de fabric maintenant ou ultérieurement :

## Fabric Zones

Fabric Zones are optional. They reside within a Fabric Site and can only contain Edge Nodes and Extended Nodes. If Fabric Zones are used, only select Virtual Networks and Anycast Gateways (IP address pools) are provisioned to the Edge Nodes in each Fabric Zone.

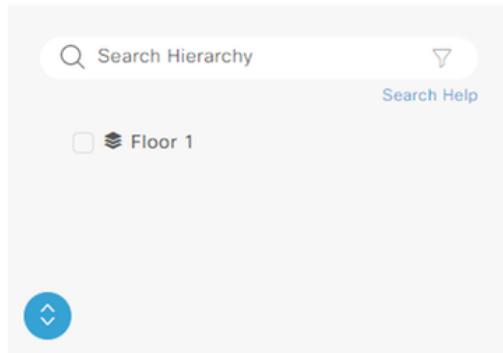
If Fabric Zones are not used, all Virtual Networks and Anycast Gateways are provisioned to all Edge Nodes in the Fabric Site.



Select one or more areas, buildings, or floors to enable as a fabric zone

A Fabric Zone begins at the selected level of hierarchy. All levels below the selected level are included as part of the Fabric Zone.

LEGEND  Fabric Site



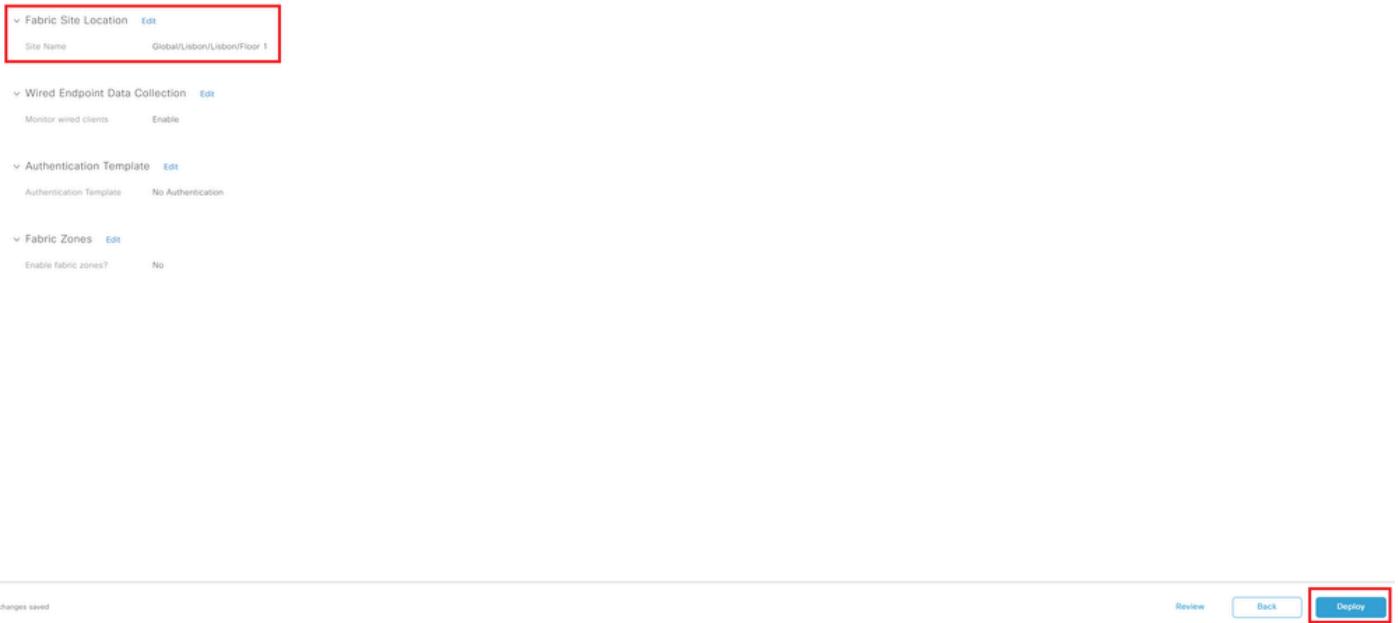
Configuration des zones de fabric

Étape 4 : vérification des paramètres de votre zone de fabric Si tout va bien, sélectionnez

Déployer :

## Summary

Review the Fabric Site and Fabric Zone settings before deploying.



Fabric Site Location [Edit](#)  
Site Name Global/Lisbon/Lisbon/Floor\_1

Wired Endpoint Data Collection [Edit](#)  
Monitor wired clients Enable

Authentication Template [Edit](#)  
Authentication Template No Authentication

Fabric Zones [Edit](#)  
Enable fabric zones? No

Changes saved [Review](#) [Back](#) [Deploy](#)

Déployer le site de fabric

Vous avez créé un site de fabric :

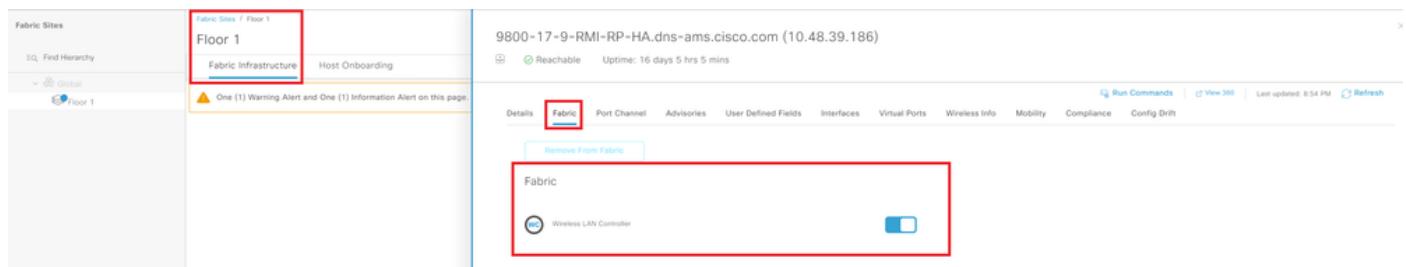
## Success! You created a Fabric Site.

Your Fabric Site, Global/Lisbon/Lisbon/Floor\_1, was created successfully. 

Création du site de fabric

### Ajouter un WLC au fabric

Accédez à Provisioner > Sites de fabric et sélectionnez votre site de fabric. Cliquez sur le haut de votre WLC et naviguez jusqu'à l'onglet Fabric. Activez le fabric sur le WLC, et sélectionnez Add:



Fabric Sites [Find Hierarchy](#) [Global](#) Floor 1 [Fabric Infrastructure](#) Host Onboarding

9800-17-9-RMI-RP-HA.dns-ams.cisco.com (10.48.39.186)  
Reachable Uptime: 16 days 5 hrs 5 mins

One (1) Warning Alert and One (1) Information Alert on this page

Run Commands View 360 Last updated: 8:54 PM Refresh

Details [Fabric](#) Port Channel [Advisories](#) [User Defined Fields](#) [Interfaces](#) [Virtual Ports](#) [Wireless Info](#) [Mobility](#) [Compliance](#) [Config Drift](#)

[Remove From Fabric](#)

Fabric

Wireless LAN Controller

Ajouter un WLC au fabric

### Joindre AP

Étape 1. Accédez à Design > Network Settings > IP Address Pools. Créez un pool d'adresses IP.

Pool d'adresses IP

Étape 2. Accédez à Provisioner > Sites de fabric et sélectionnez votre site de fabric. Naviguez jusqu'à Host Onboarding > Virtual Networks.

INFRA\_VN est introduit pour intégrer facilement les AP. Les points d'accès se trouvent dans la superposition de fabric, mais INFRA\_VN est mappé à la table de routage globale. Seuls les AP et les noeuds étendus peuvent appartenir à INFRA\_VN. L'extension de couche 2 est automatiquement activée et active le service LISP de couche 2.

Sélectionnez INFRA\_VN > Ajouter :

Modifier le réseau virtuel

Étape 3. Ajout d'un pool d'adresses IP avec le type de pool AP :

Edit Virtual Network: INFRA\_VN

< Back

Modifier le réseau virtuel S1-INFRA

Étape 4 : vérification de l'activation de l'extension de couche 2

|                          |           |   |                                |                           |      | Reset            | Export            | Add |
|--------------------------|-----------|---|--------------------------------|---------------------------|------|------------------|-------------------|-----|
| Filter                   |           | Supplicant-Based Extended Node Onboarding |                                |                           | Find |                  |                   |     |
| <input type="checkbox"/> | VLAN Name | Pool Type                                 | Supplicant-Based Extended Node | IP Address Pool           | VLAN | Layer-2 Flooding | Layer-2 Extension | ⋮   |
| <input type="checkbox"/> | VLAN0039  | AP  | Disabled                       | S1-INFRA<br>172.16.0.0/24 | 39   | Disabled         | Enabled           |     |

Modifier le réseau virtuel

Avec Pool Type = AP et l'extension de couche 2 sur ON, Cisco DNA se connecte au WLC et définit l'interface de fabric sur le mappage VN\_ID pour le sous-réseau AP pour les ID de VLAN L2 et L3.

Étape 5. Côté interface graphique WLC, accédez à Configuration > Wireless > Fabric > General. Ajouter un nouveau client et un AP VN\_ID :

Configuration > Wireless > General

Edit Add Client and AP VNID

|                    |                        |
|--------------------|------------------------|
| Name*              | S2-INFRA               |
| L2 VNID*           | 8188                   |
| Control Plane Name | default-control-pl ... |
| L3 VNID            | 4097                   |
| IP Address         | 172.16.0.0             |
| Netmask            | 255.255.255.0          |

+ Add    × Del

Name

|          |   |
|----------|---|
| S2-INFRA | 1 |
|----------|---|

Configure Multicast and IC

Cancel    Update & Apply to Device

Ajouter un nouveau client et AP VN\_ID

Étape 6. Accédez à Configuration > Wireless > Access Points. Sélectionnez un point d'accès dans la liste. Vérifiez que l'état du fabric est activé, l'adresse IP du plan de contrôle et le nom du plan de contrôle :

| Edit AP           |                    |                       |                          |
|-------------------|--------------------|-----------------------|--------------------------|
| Configuration     | AP Mode            | Local                 | Primary Software Version |
| All Access Points | Operation Status   | Registered            | Predownloaded Status     |
| Total APs : 3     | Fabric Status      | Enabled               | Predownloaded Version    |
| AP Name           | CleanAir NSI Key   |                       | Next Retry Time          |
| AP0C75-BDB        | RLOC IP            | 10.XX.XX.XX           | Boot Version             |
| 3800E-I           | Control Plane Name | default-control-plane | IOS Version              |
|                   |                    |                       | Mini IOS Version         |

Vérifier l'état du fabric AP

## Client à bord

Étape 1 : ajout du pool au réseau virtuel et vérification que l'option Extension de couche 2 est activée pour activer l'extension de sous-réseau de couche 2 LISP et de couche 2 sur le pool/sous-réseau client Dans Cisco DNA 1.3.x, vous ne pouvez pas le désactiver.

Layer 2 Only  Layer 3 Only

IP Address Pool  
S1\_CLIENT-IP (10.0.0.0/24)

VLAN  
39

VLAN Name  
VLAN0039  Auto generate VLAN name

Security Group  Traffic  IP-directed broadcast

Layer-2 Flooding  Critical Pool  Wireless Pool

Bridge-Network Virtual Machine

Ajouter un pool d'adresses IP

Étape 2 : vérification de l'activation de l'extension de couche 2 et du pool sans fil

Modifier le réseau virtuel

Étape 3. Du côté de l'interface graphique utilisateur WLC, naviguez vers Configuration > Wireless > Fabric > General. Ajoutez un nouveau client et un ID de VLAN AP.

Lorsque le pool est attribué au réseau virtuel, le mappage de l'interface de fabric correspondante au VNID est transmis au contrôleur. Il s'agit de VNID de couche 2.

Configuration > Wireless > Fabric

General      Control Plane      Profiles

Ajouter un nouveau client et AP VN\_ID

Étape 4. Les SSID sont mappés au pool dans les réseaux virtuels respectifs :

## Floor 1

Fabric Infrastructure Host Onboarding

Authentication Template Virtual Networks Wireless SSIDs

Wireless SSID's

Enable Wireless Multicast

Reset Save

Find

| SSID Name | Type       | Security      | Traffic Type | Address Pool                       | Scalable Group |
|-----------|------------|---------------|--------------|------------------------------------|----------------|
| Demo      | Enterprise | WPA2 Personal | Voice + Data | Choose Pool<br>10_1_0_0-S2_Corp_VN | Assign SGT     |

SSID mappés

Étape 5. Un profil de fabric avec le VNID L2 est ajouté au pool choisi et le profil de stratégie est mappé au profil de fabric, il est activé pour le fabric.

Sur le côté GUI du WLC, naviguez vers Configuration > Wireless > Fabric > Profiles.

WELCOME TO THE WLC

Configuration > Wireless > Fabric > Profiles

Edit Fabric Profile

⚠️ Modifying the profile may result in loss of connectivity

|  |                      |                     |                      |  |                      |         |      |         |         |
|--|----------------------|---------------------|----------------------|--|----------------------|---------|------|---------|---------|
| General  | Control Plane        |                     |                      |  |                      |         |      |         |         |
| + Add  | X D                  |                     |                      |  |                      |         |      |         |         |
| <table border="1"> <tr> <td>Fabric Profile Name</td> <td>s2-demo_Global_F_d3r</td> </tr> <tr> <td><input checked="" type="checkbox"/> s2-demo_Global_F_d3r</td> <td></td> </tr> <tr> <td>1</td> <td></td> </tr> </table>                         |                      | Fabric Profile Name | s2-demo_Global_F_d3r | <input checked="" type="checkbox"/> s2-demo_Global_F_d3r |                      | 1       |      |         |         |
| Fabric Profile Name  | s2-demo_Global_F_d3r |                     |                      |  |                      |         |      |         |         |
| <input checked="" type="checkbox"/> s2-demo_Global_F_d3r   |                      |                     |                      |  |                      |         |      |         |         |
| 1  |                      |                     |                      |  |                      |         |      |         |         |
| <table border="1"> <tr> <td>Profile Name*</td> <td>s2-demo_Global_F_d3r</td> </tr> <tr> <td>Description</td> <td>s2-demo_Global_F_d3r</td> </tr> <tr> <td>L2 VNID</td> <td>8189</td> </tr> <tr> <td>SGT Tag</td> <td>2-65519</td> </tr> </table> |                      | Profile Name*       | s2-demo_Global_F_d3r | Description  | s2-demo_Global_F_d3r | L2 VNID | 8189 | SGT Tag | 2-65519 |
| Profile Name*  | s2-demo_Global_F_d3r |                     |                      |  |                      |         |      |         |         |
| Description  | s2-demo_Global_F_d3r |                     |                      |  |                      |         |      |         |         |
| L2 VNID  | 8189                 |                     |                      |  |                      |         |      |         |         |
| SGT Tag  | 2-65519              |                     |                      |  |                      |         |      |         |         |

Profil de fabric

Étape 6. Accédez à Configuration > Tags & Profiles > Policy. Vérifiez le profil de fabric mappé au profil de stratégie :

Profil de fabric configuré sur la stratégie

## Vérifier

### Vérification de la configuration du fabric sur WLC et Cisco DNA

Sur la CLI WLC :

WLC1# show tech

WLC1# show tech sans fil

Configuration du plan de contrôle :

routeur lisp

valeur par défaut du locator-table

WLC avec localisateur

172.16.201.202

positionneur de sortie

!

map-server session passive-open WLC

site site\_uci

description map-server configuré à partir de Cisco DNA-Center

authentication-key 7 <Clé>

CB1-S1#sh lisp session

Sessions pour VRF par défaut, total : 9, établi : 5

État homologue actif/inactif entrant/sortant

172.16.201.202:4342 Haut 3j07h 14/14

Configuration WLC :

fabric sans fil

wireless fabric control-plane default-control-plane

adresse ip 172.16.2.2 key 0 47aa5a

WLC1# show fabric map-server summary

État de la connexion MS-IP

---

172.16.1.2 UP

WLC1# show wireless fabric summary

État du fabric : Activée

Plan de contrôle :

Nom Adresse IP État de la clé

---

default-control-plane 172.16.2.2 47aa5a Up

Dans l'interface graphique du WLC, accédez à Configuration > Wireless > Fabric et vérifiez si l'état du fabric est Enabled.

Accédez à Configuration > Wireless > Access Points. Sélectionnez un AP dans la liste. Vérifiez que l'état du fabric est activé.

Sur Cisco DNA, accédez à Provisionnement > Fabric Sites et vérifiez si vous disposez d'un site de fabric. Sur ce site de fabric, accédez à Infrastructure de fabric > Fabric et vérifiez si le WLC est activé en tant que fabric.

## Dépannage

Le client n'obtient pas d'adresse IP

Étape 1 : vérification du fabric du SSID Sur l'interface graphique WLC, naviguez vers Configuration > Tags & Profiles > Policy. Sélectionnez la stratégie et accédez à Avancé. Vérifiez si le profil de fabric est activé.

Étape 2 : vérification de l'état d'apprentissage IP du client Sur l'interface graphique WLC, naviguez vers Monitoring > Wireless > Clients. Vérifiez l'état du client.

Étape 3 : vérification de la nécessité de la stratégie DHCP

Étape 4. Si le trafic est commuté localement entre AP - noeud de périphérie, collectez les journaux AP (client-trace) pour la connexion client. Vérifiez si la détection DHCP est transférée. Si aucune offre DHCP n'arrive, un problème se produit sur le noeud de périphérie. Si le DHCP n'est pas transféré, alors quelque chose ne va pas sur l'AP.

Étape 5. Vous pouvez collecter un EPC sur le port du noeud de périphérie pour voir les paquets de détection DHCP. Si vous ne voyez pas les paquets de détection DHCP, le problème se situe sur l'AP.

## Le SSID n'est pas diffusé

Étape 1. Vérifiez si les radios du point d'accès sont désactivées.

Étape 2 : vérification de l'état du WLAN et de l'activation du SSID de diffusion

Étape 3 : vérification de la configuration des points d'accès si le fabric est activé Accédez à Configuration > Wireless > Access Points, sélectionnez un point d'accès et dans l'onglet General, vous pouvez voir Fabric Status Enabled et les informations RLOC.

Étape 4. Accédez à Configuration > Wireless > Fabric > Control Plane. Vérifiez si le plan de contrôle est configuré (avec l'adresse IP).

Étape 5. Accédez à Configuration > Tags & Profiles > Policy. Sélectionnez la stratégie et accédez à Avancé. Vérifiez si le profil de fabric est activé.

Étape 6. Accédez à Cisco DNA et recommencez les étapes sur [Create SSID](#) et [Provisioning WLC](#). Cisco DNA doit à nouveau pousser le SSID vers le WLC.

## Informations connexes

- [Assistance technique de Cisco et téléchargements](#)

## 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.