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

Table des matières

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 :

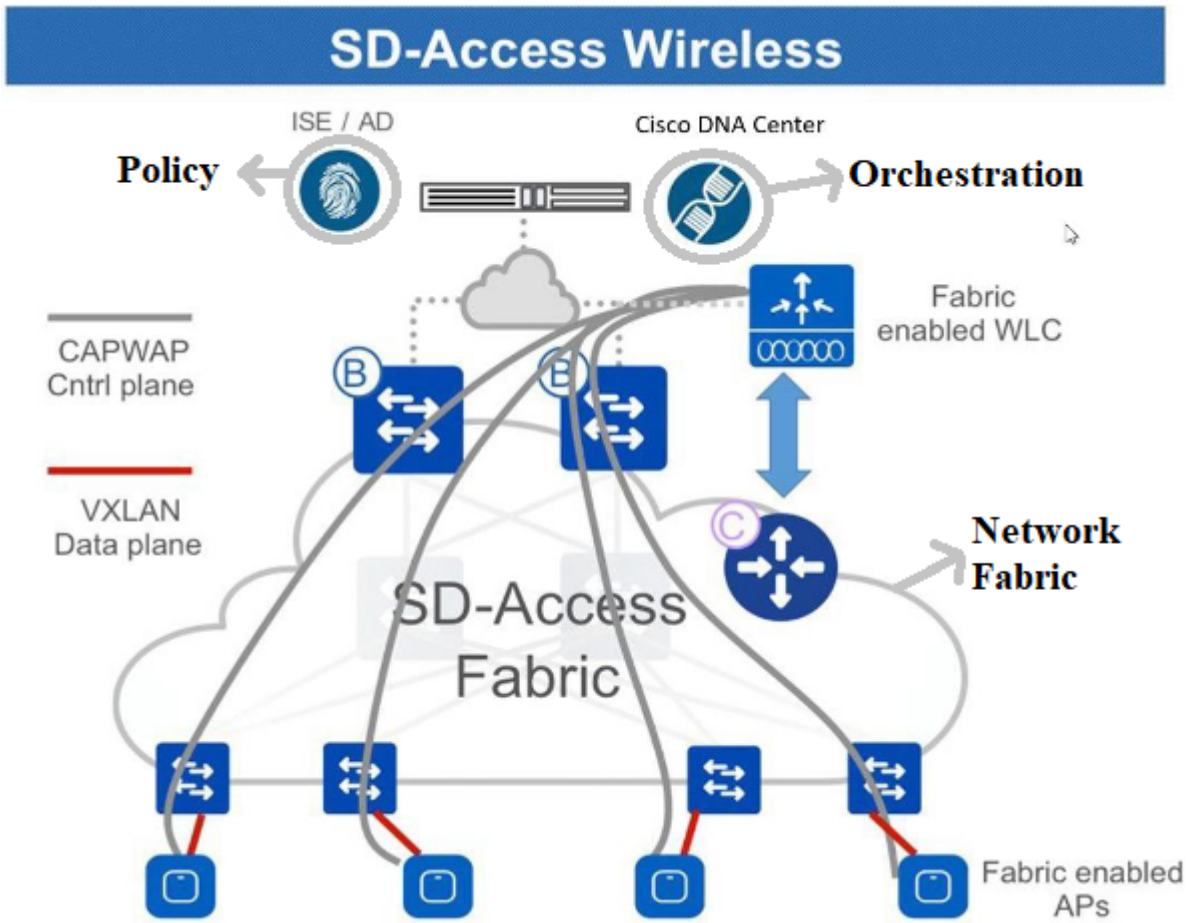
1. Un fabric réseau : Il s'agit d'une abstraction du réseau lui-même qui prend en charge les superpositions programmables et la virtualisation. Le fabric de réseau prend en charge l'accès filaire et sans fil, lui permet d'héberger plusieurs réseaux logiques segmentés les uns par rapport aux autres et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

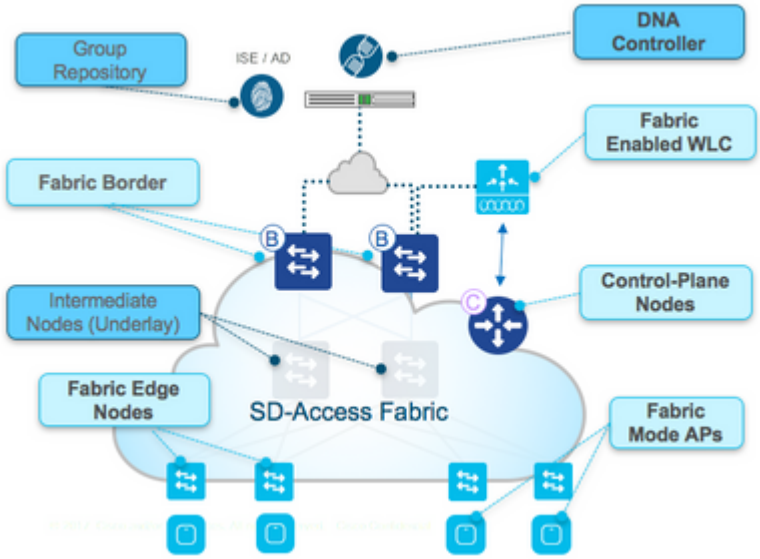


Éléments du fabric réseau

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

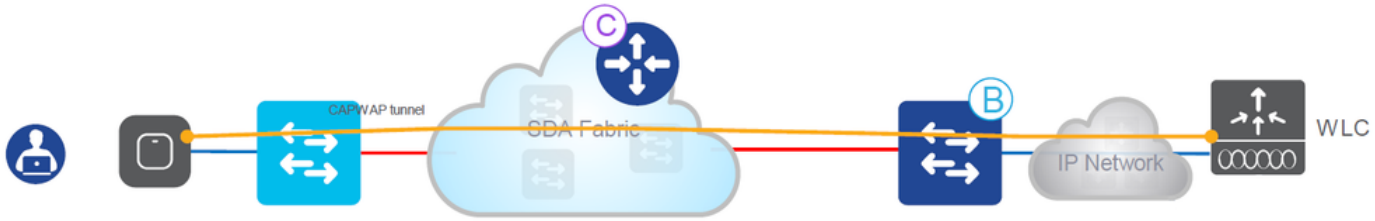
Aperçu



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 :

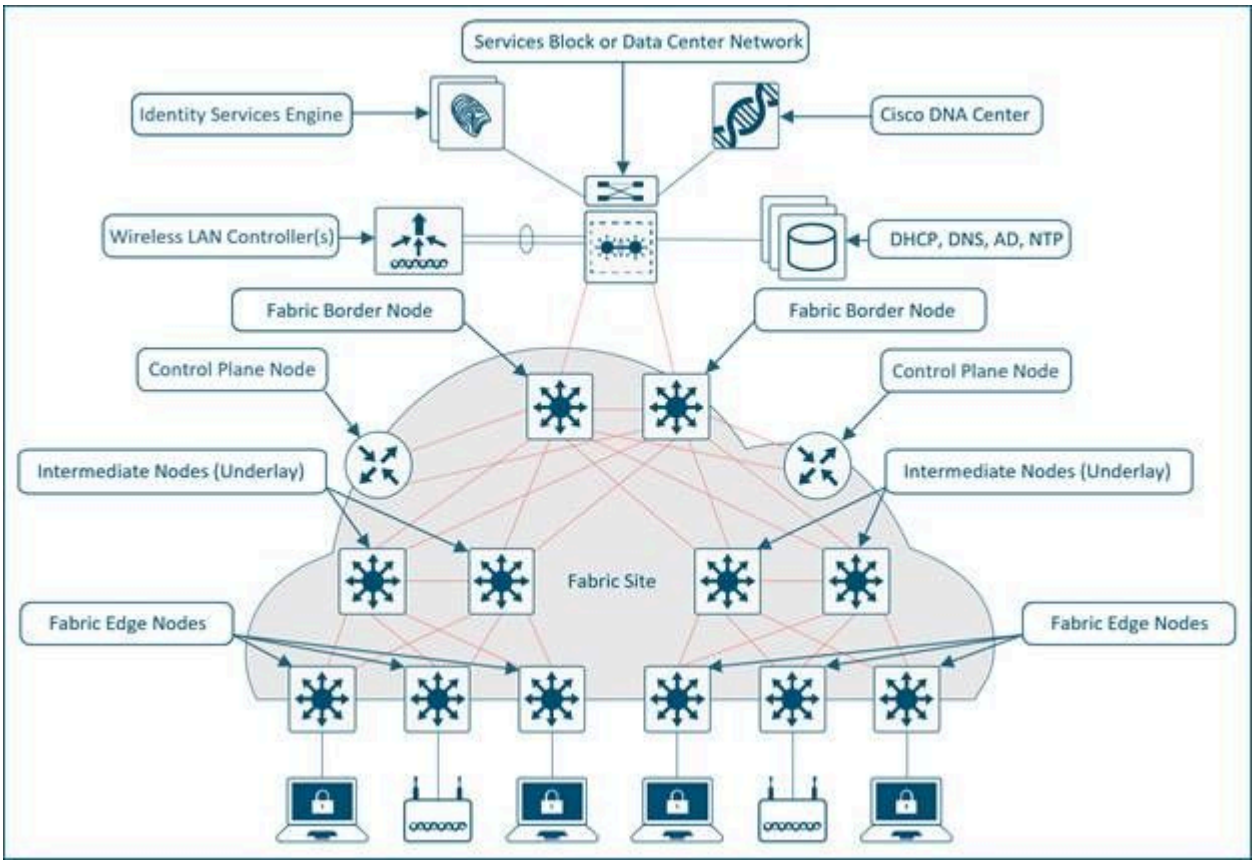


Méthode Par Capteur

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.

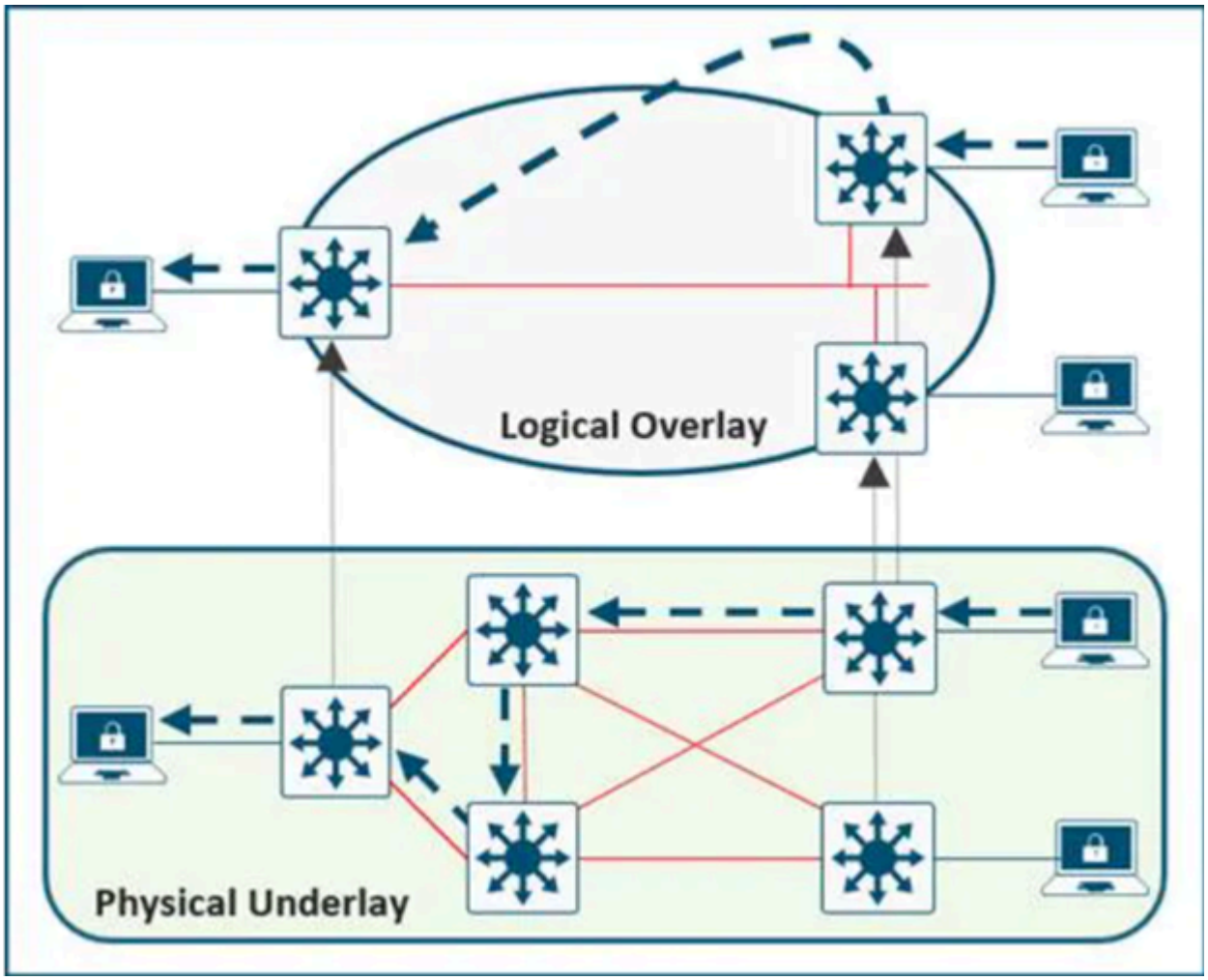
Un réseau de superposition est une topologie logique utilisée pour connecter virtuellement des périphériques, construite sur une topologie physique sous-jacente arbitraire. Il utilise d'autres attributs de transfert pour fournir des services supplémentaires qui ne sont pas fournis par le sous-jacent. 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 coeur de réseau traditionnel, il doit utiliser une fondation de couche 3 bien conçue qui offre des performances, une évolutivité et une haute disponibilité robustes.

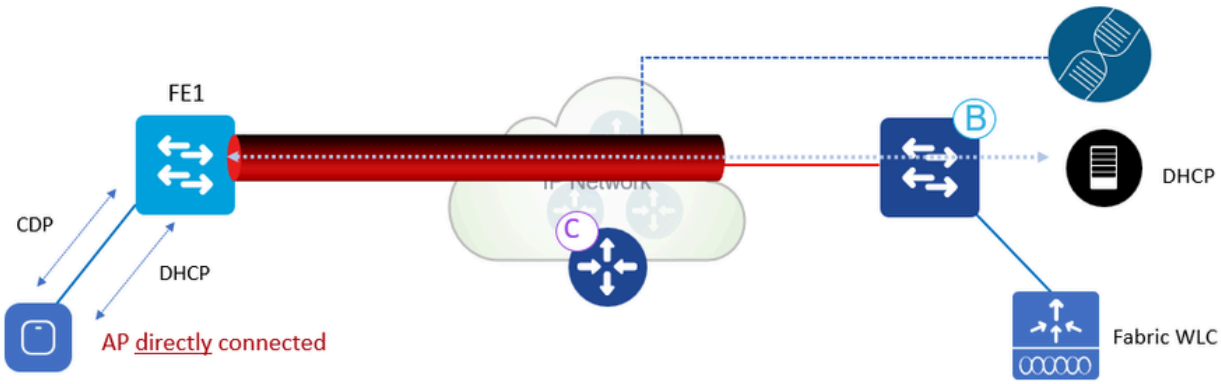
Remarque : SDA prend en charge IPv4 dans le réseau sous-jacent et IPv4 et/ou IPv6 dans les réseaux superposés.



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 préprovisionne

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 wncd chassis active r0 lisp-agent-api debug

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

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

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

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

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

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

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

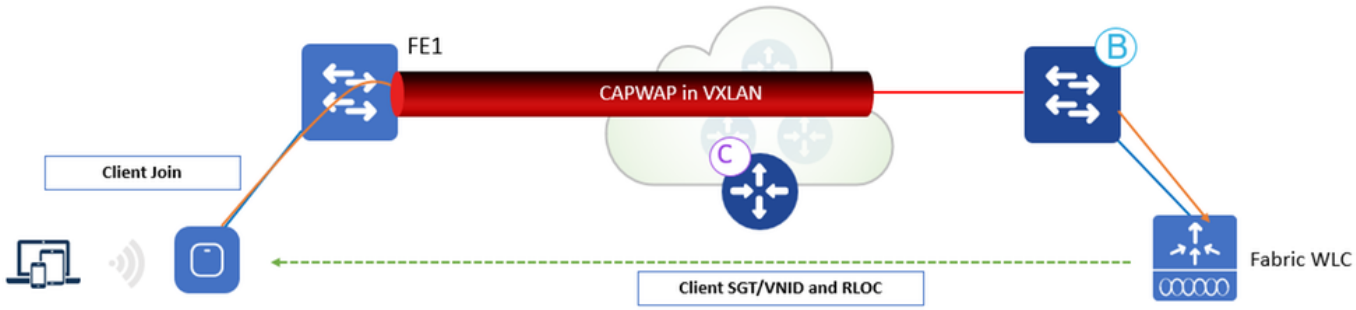
set platform software trace wncd chassis active r0 lisp-agent-ha debug

set platform software trace wncd 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

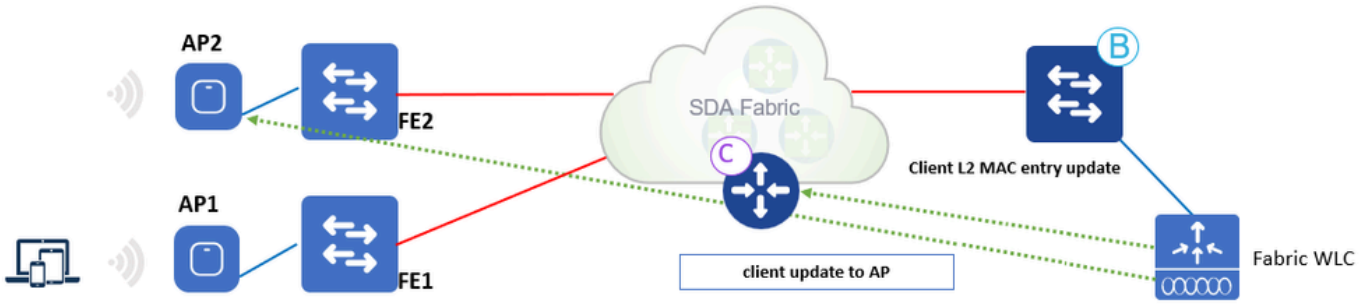
debug lisp control-plane all

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

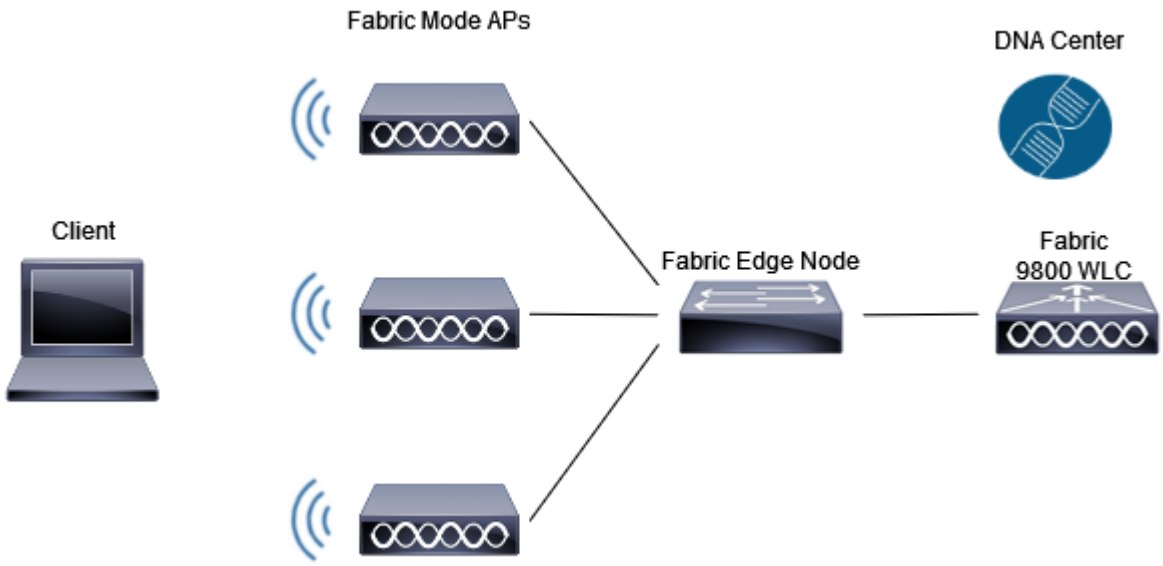


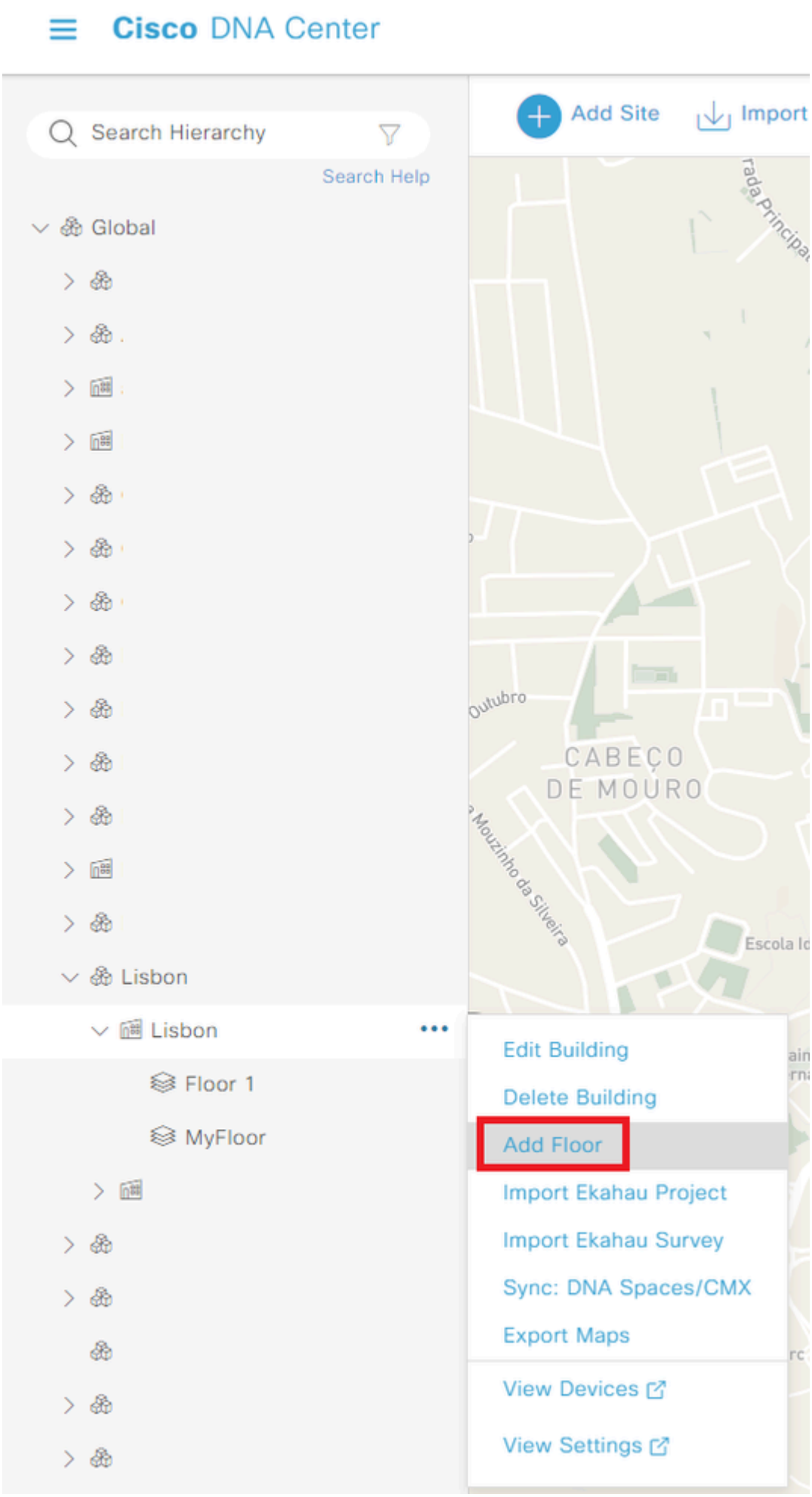
Diagramme du réseau

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.

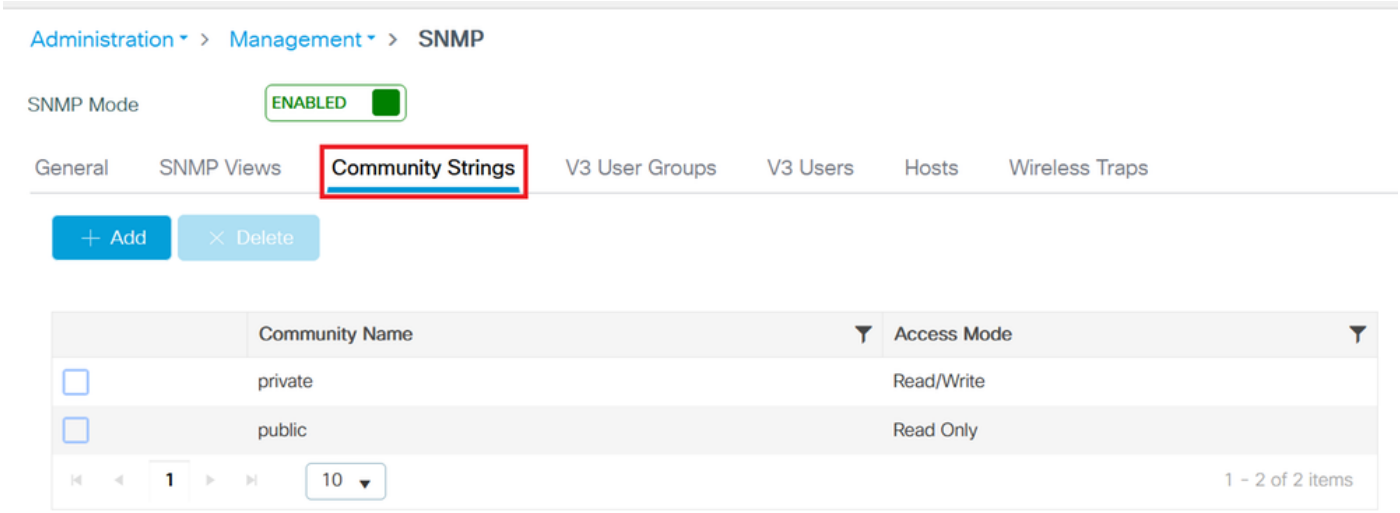
Naviguez jusqu'à Design > Network Hierarchy et entrez le bâtiment/étage, ou vous pouvez créer un étage, comme illustré dans l'image :



Créer un étage

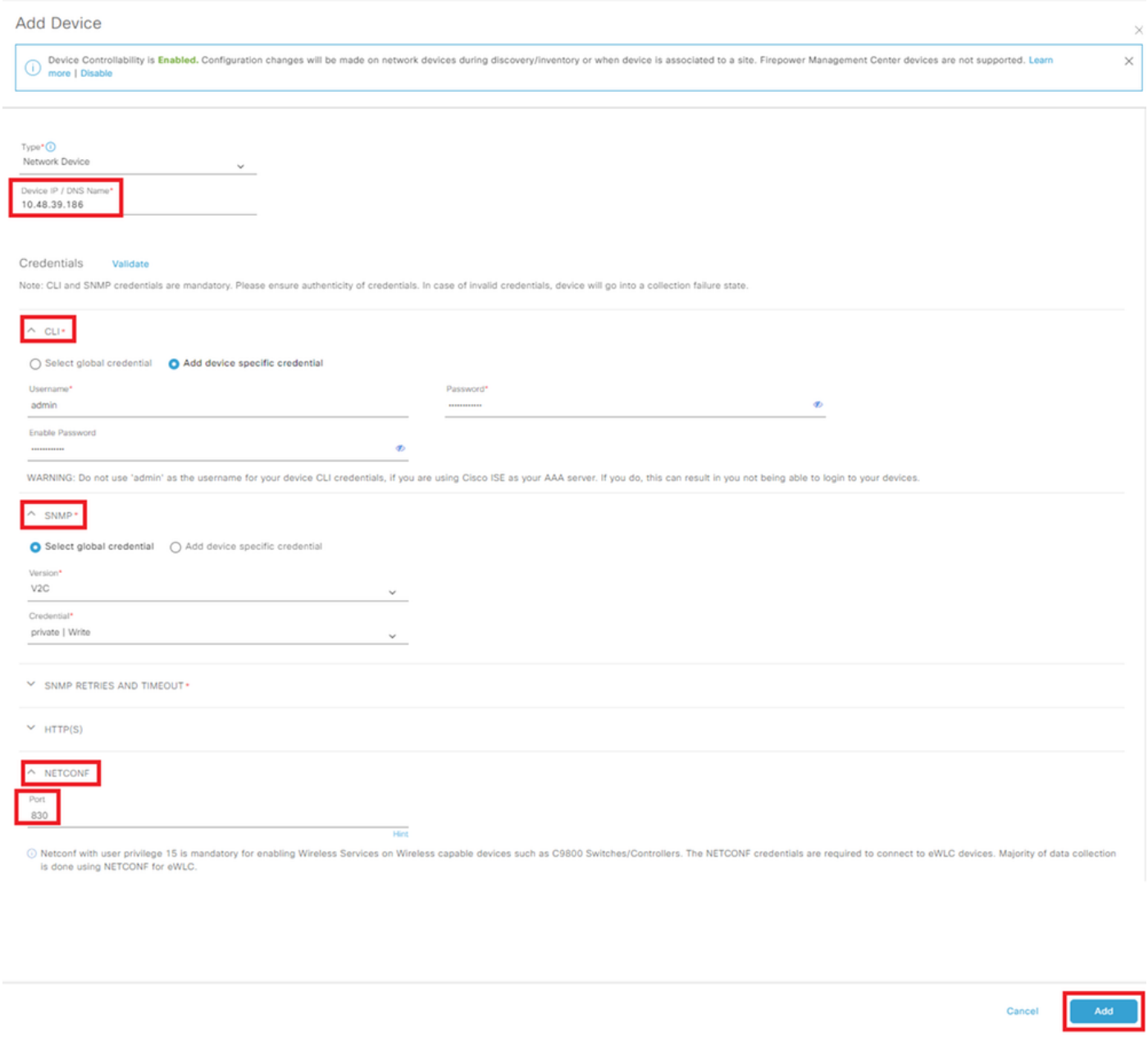
Étape 2. Ajouter du sol. Vous pouvez également télécharger une image de la plante du sol

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:



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 :



Ajouter un WLC

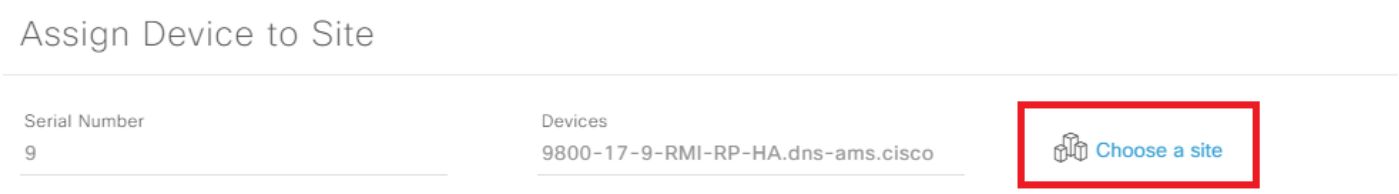
Le WLC apparaît comme NA car Cisco DNA est toujours en cours de synchronisation :

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 :

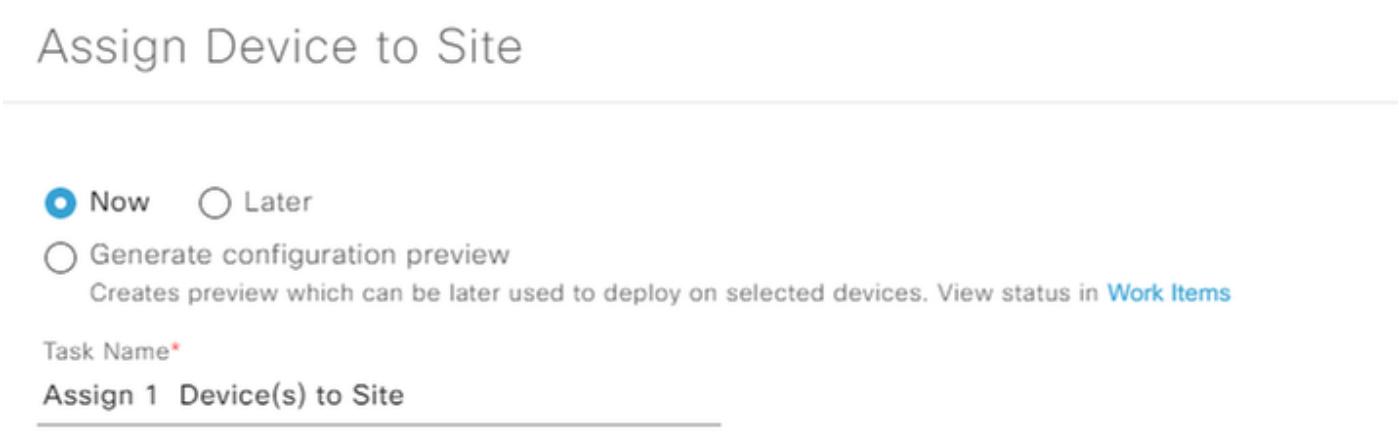
WLC synchronisé

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



Attribuer un périphérique au site

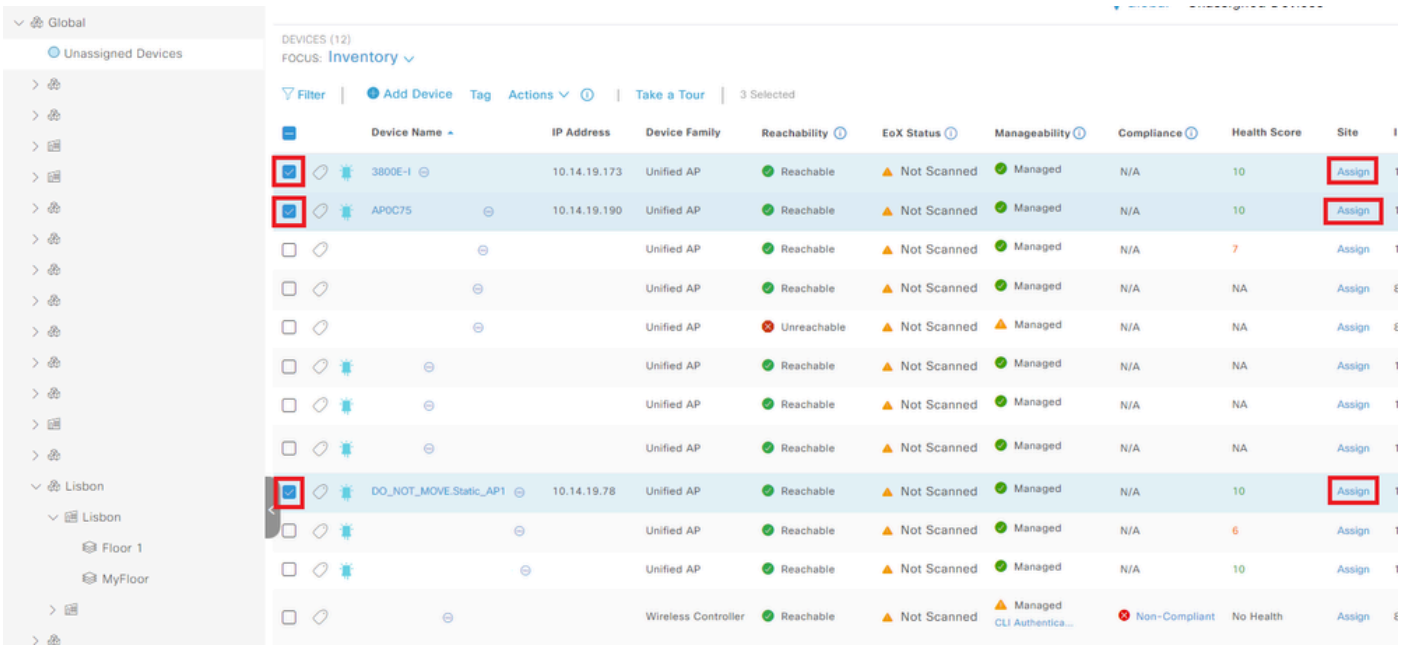
Vous pouvez décider d'attribuer le site maintenant ou ultérieurement :



Affecter un périphérique au site maintenant ou ultérieurement

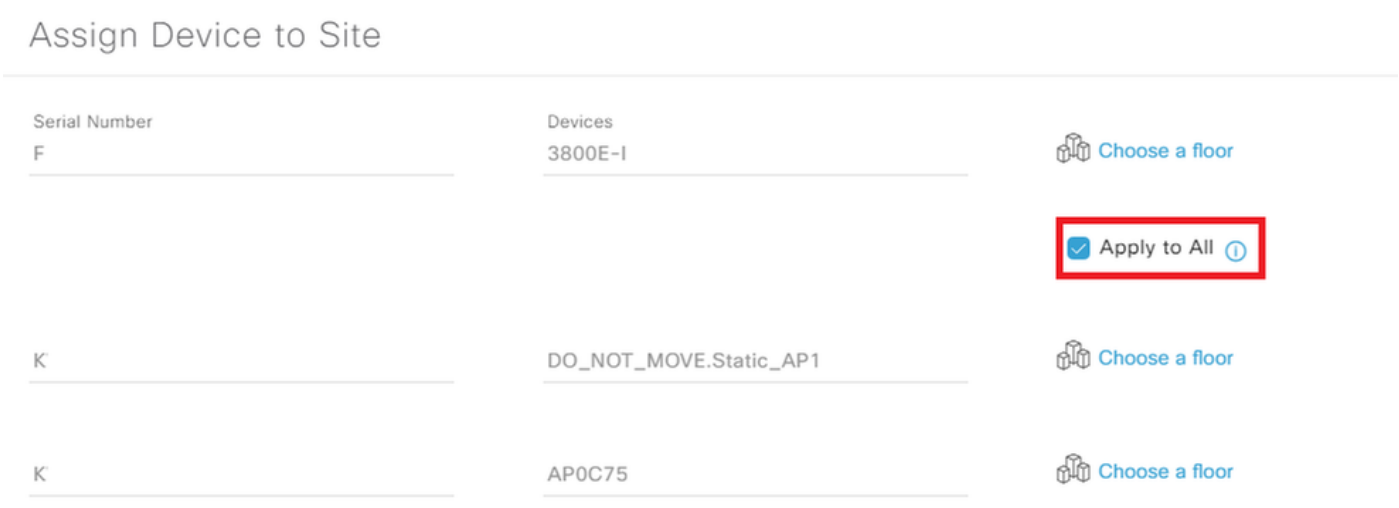
Ajouter des points d'accès

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



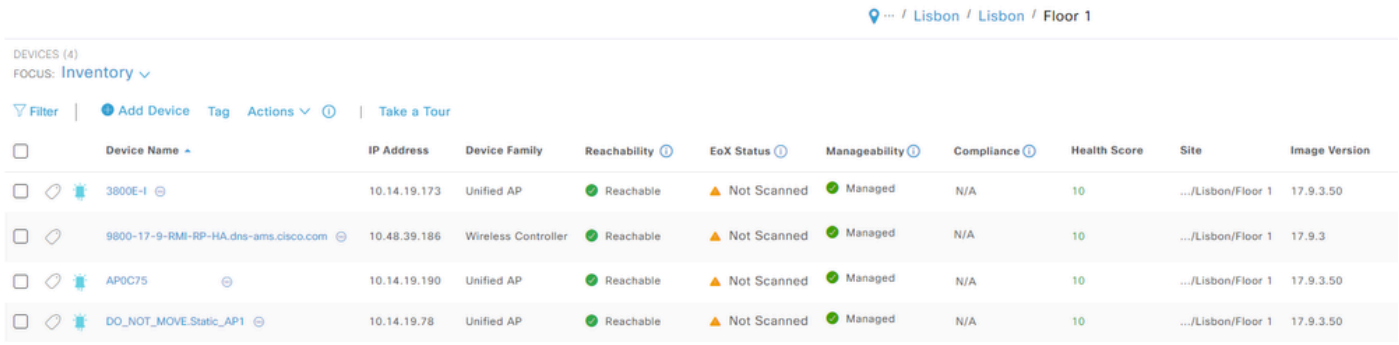
Ajouter des points d'accès

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.



Attribuer des points d'accès au site

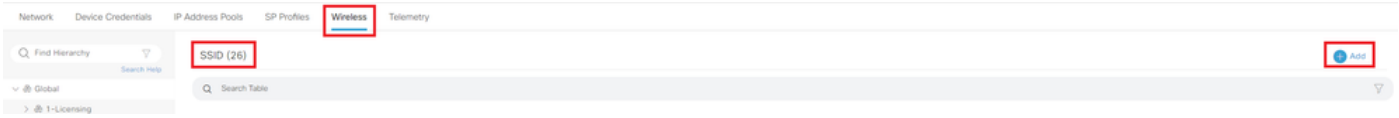
Naviguez jusqu'à votre étage et vous pouvez voir tous les périphériques qui lui sont assignés - WLC et AP :



Périphériques affectés au site

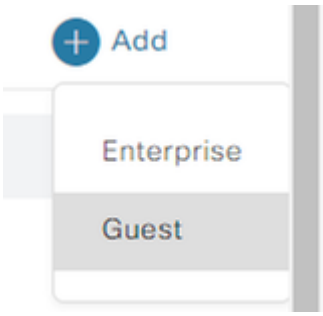
Créer un SSID

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



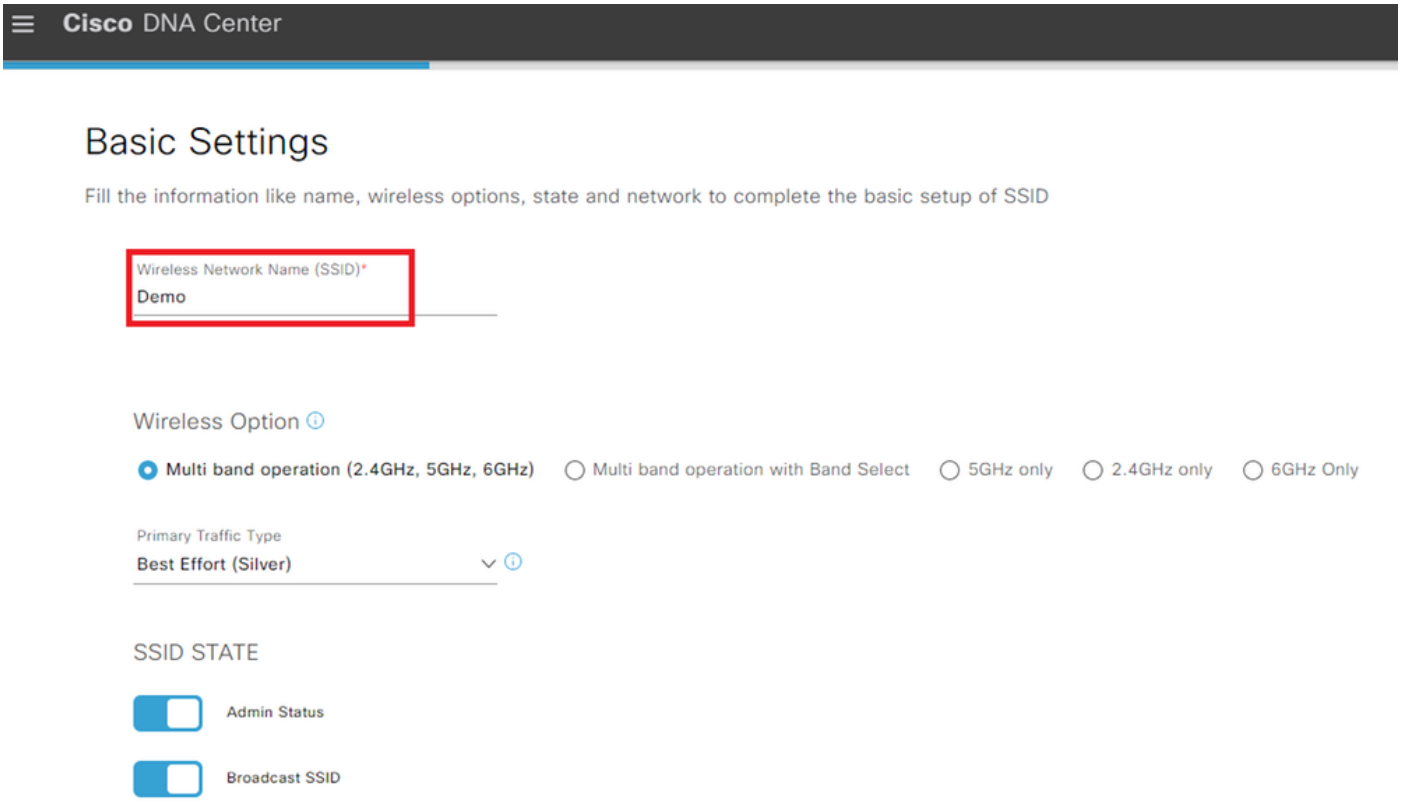
Créer un SSID

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

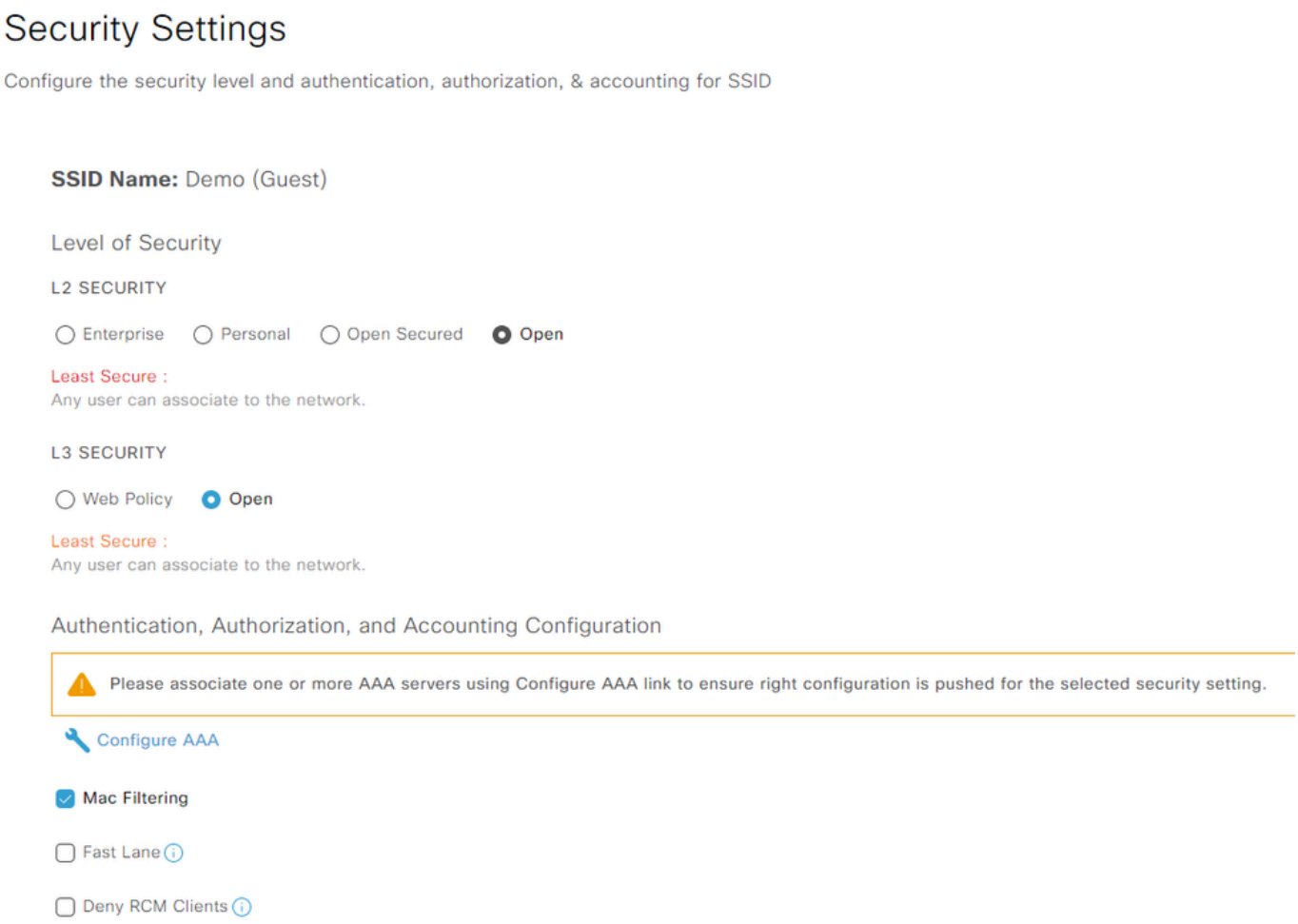


SSID d'entreprise ou invité

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 :



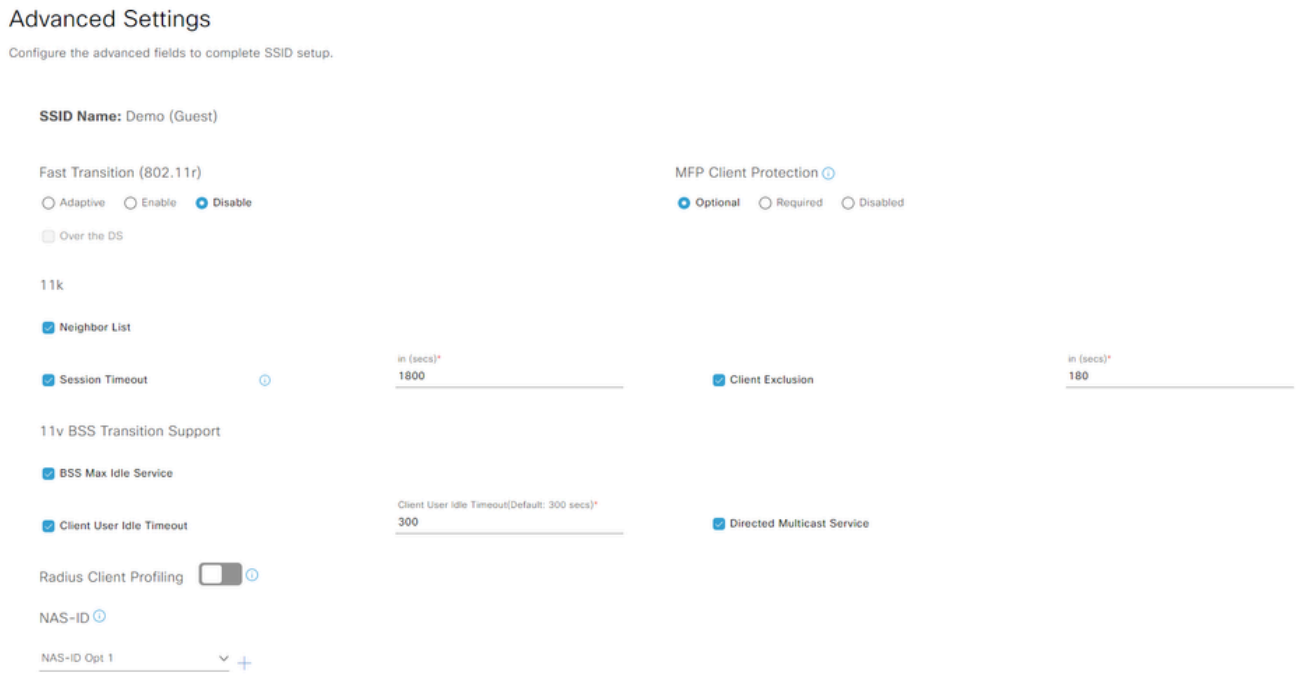
Paramètres de base SSID



Paramètres de sécurité SSID

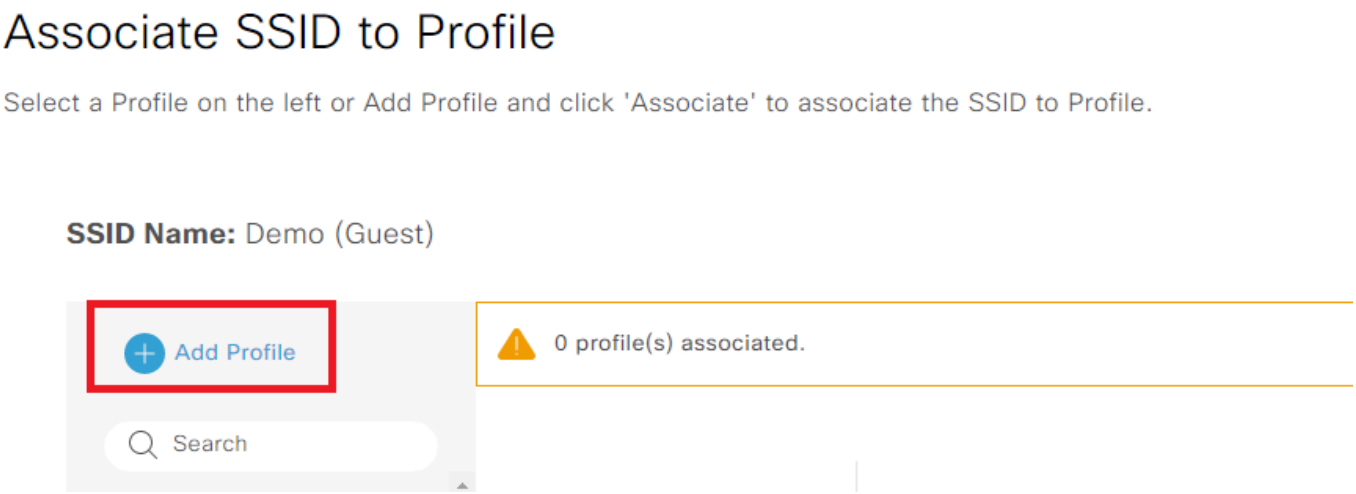
⚠ Mise en garde : N'oubliez pas de configurer et d'associer le serveur AAA pour le SSID. La liste de méthodes par défaut est mappée si aucun serveur AAA n'est configuré.

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



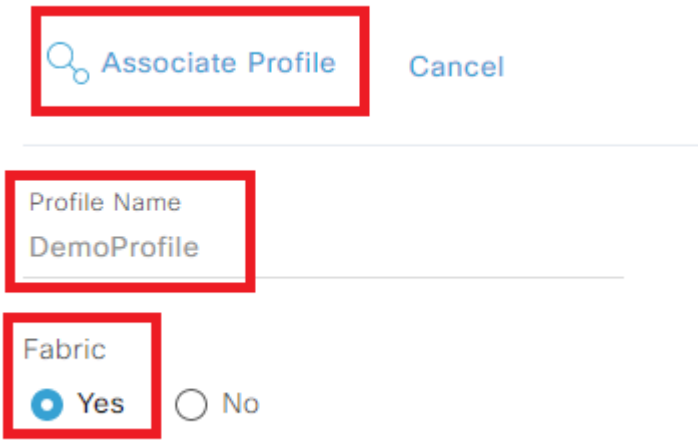
Paramètres SSID avancés

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



Ajouter un profil

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



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)
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

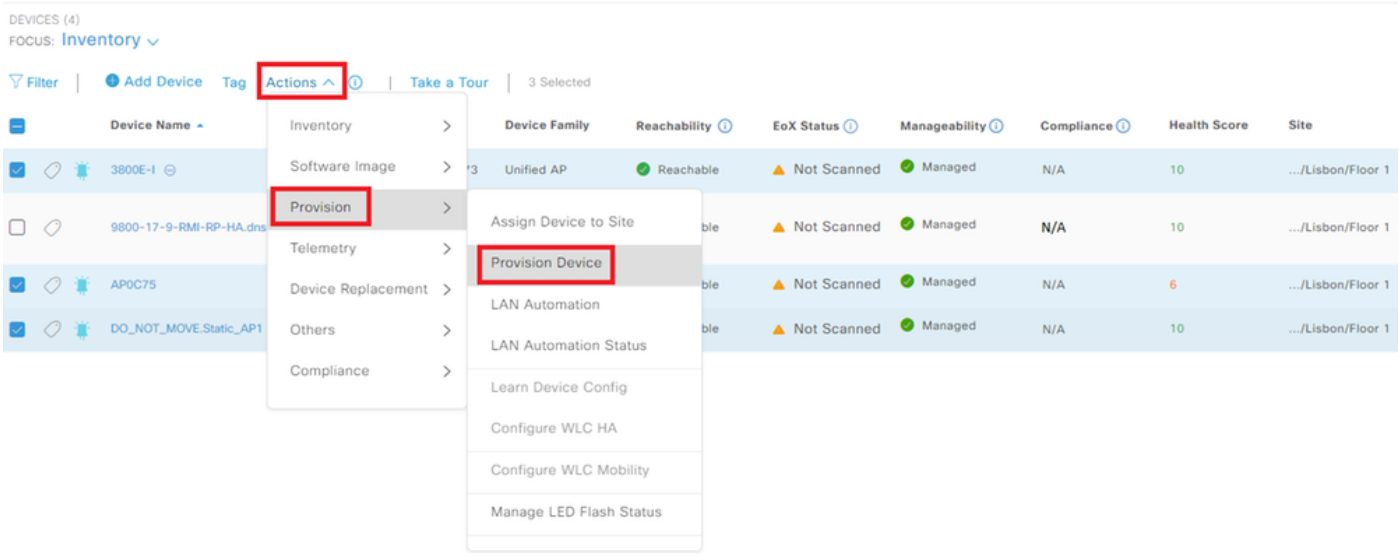
Étape 5. Configuration d'un nouveau profil réseau :

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

Ajouter un profil RF de base

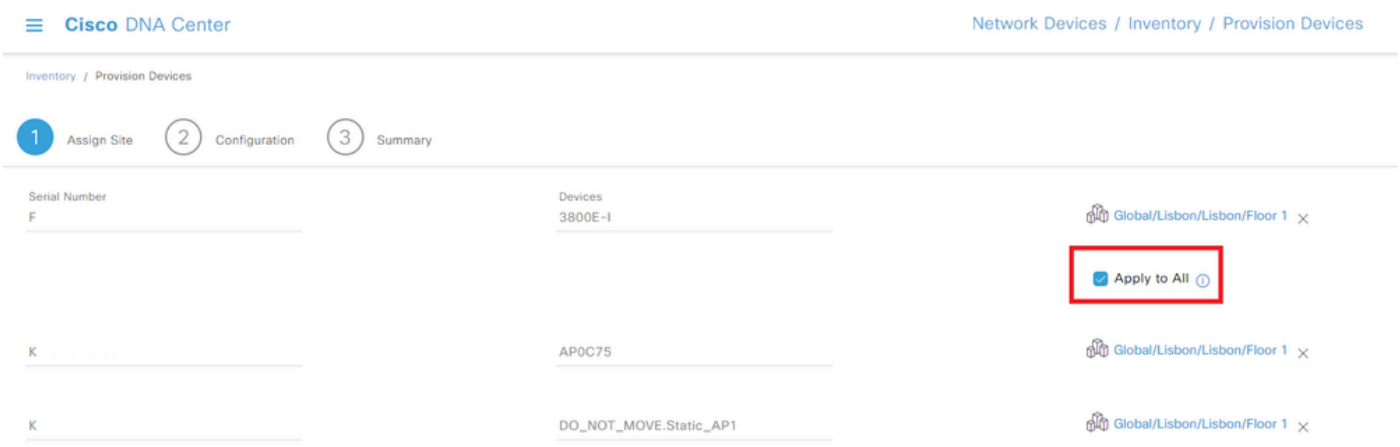
Provisionnement des points d'accès

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



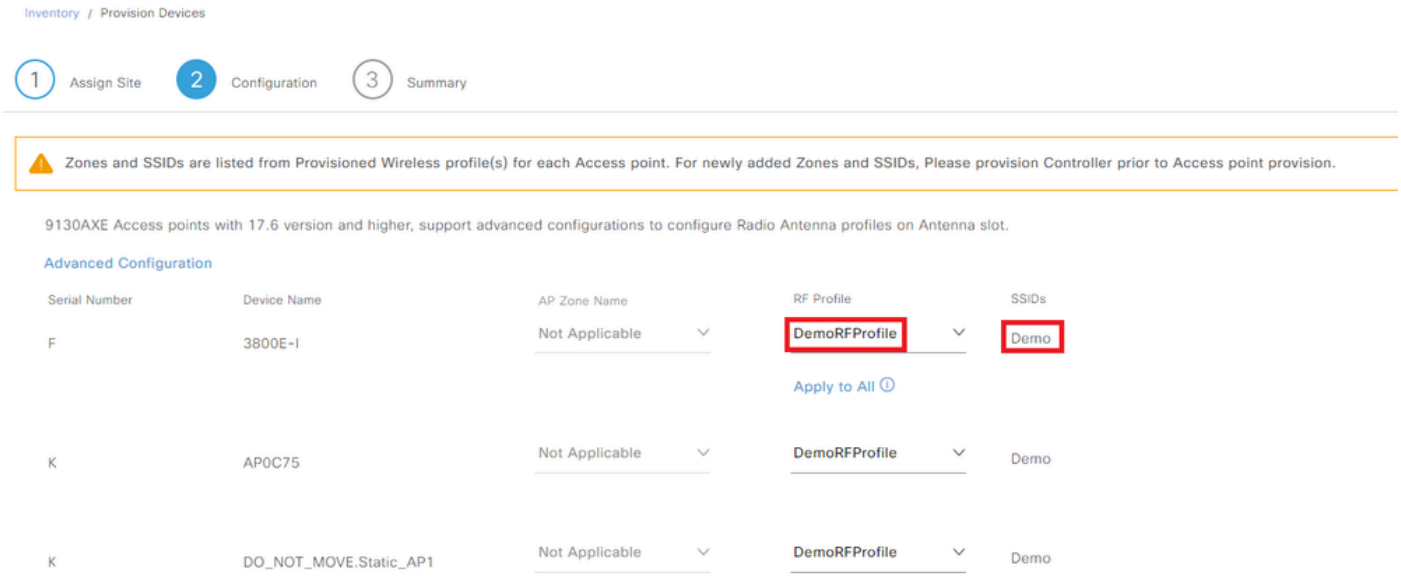
Provisionnement des points d'accès

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



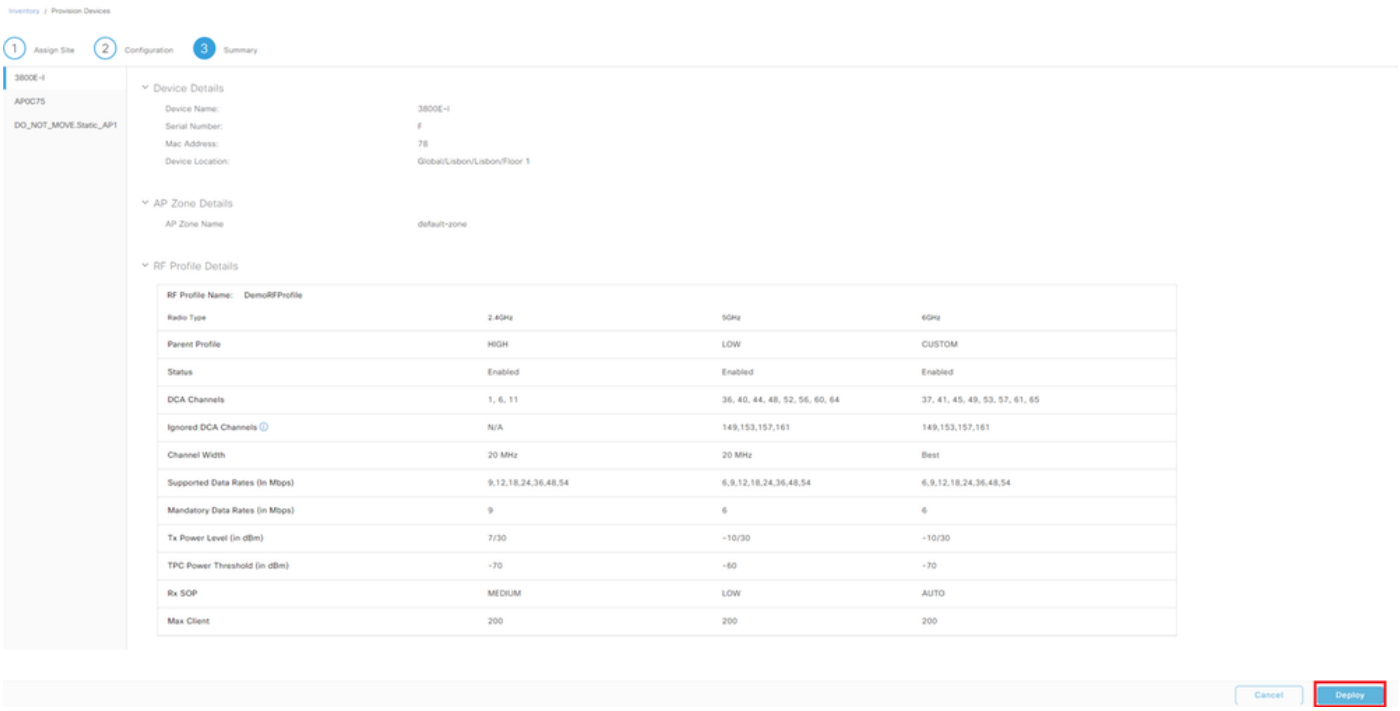
Attribuer un site aux points d'accès

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



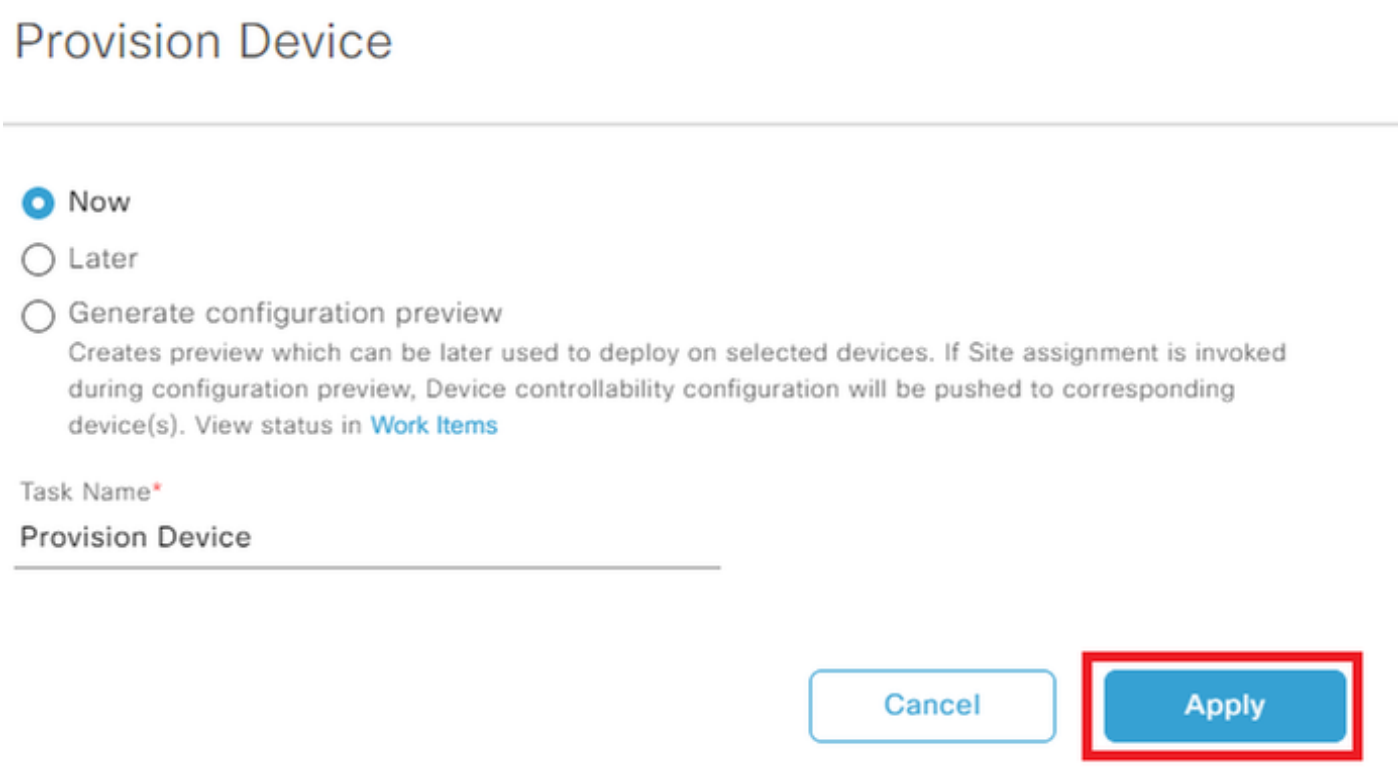
Sélectionner un profil RF

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



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 :

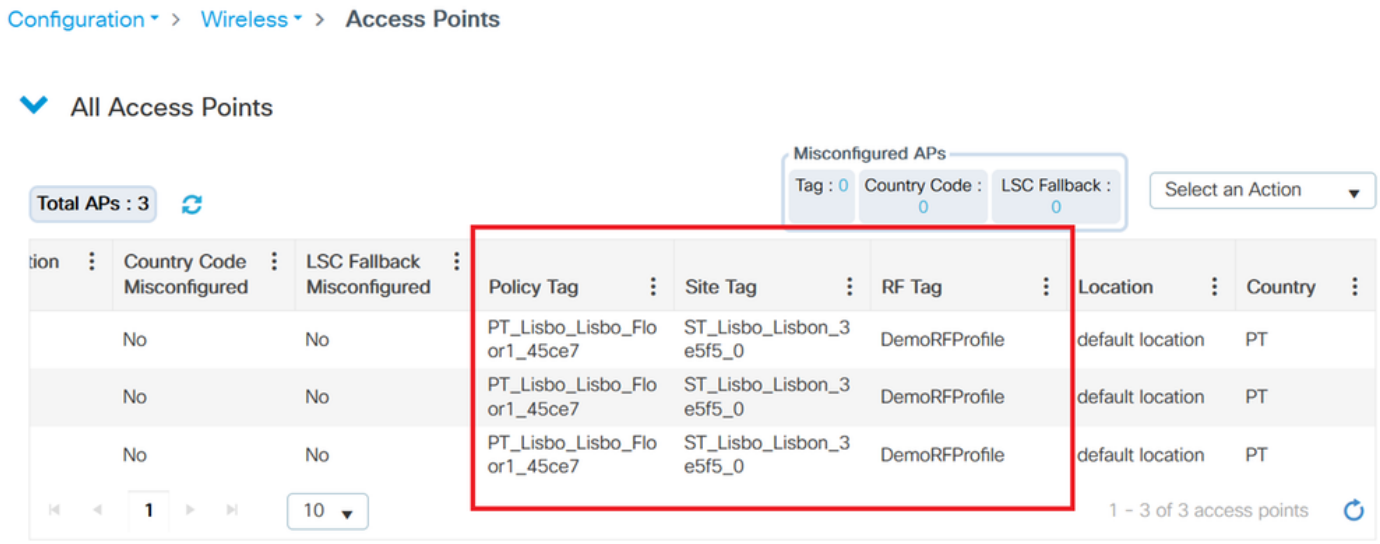


Provisionner les points d'accès maintenant ou ultérieurement

⚠ 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 :



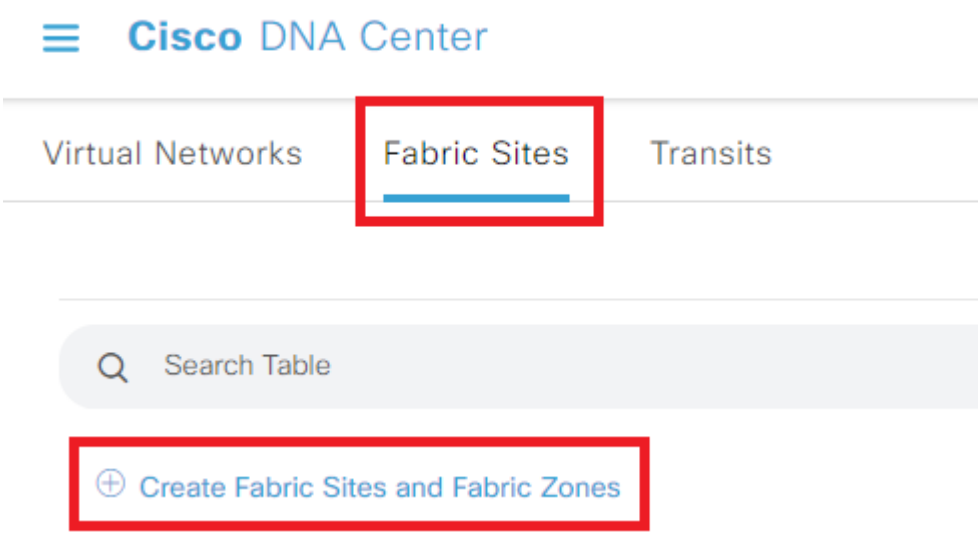
Balises sur les points d'accès

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

WLAN

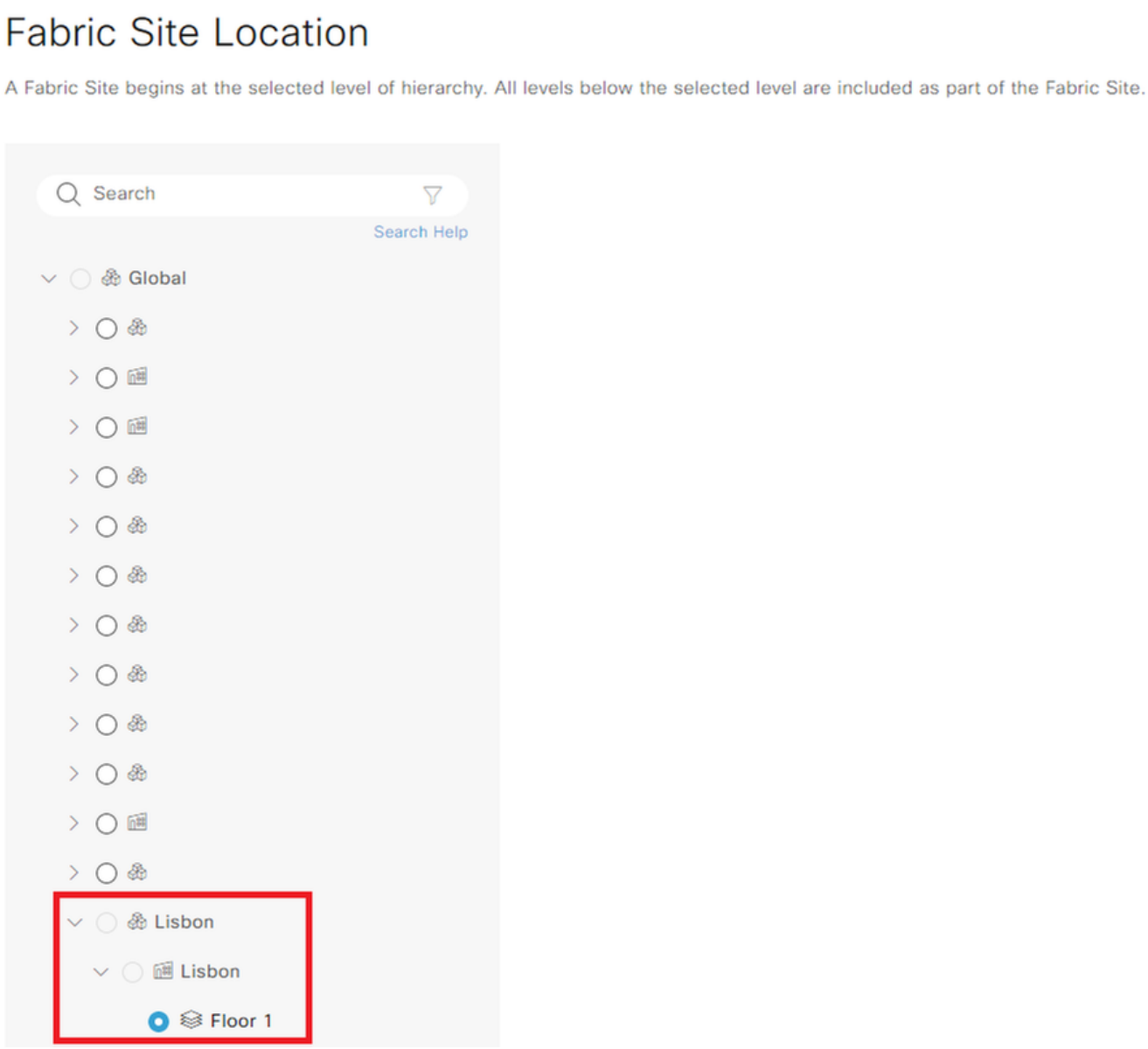
Créer un site de fabric

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



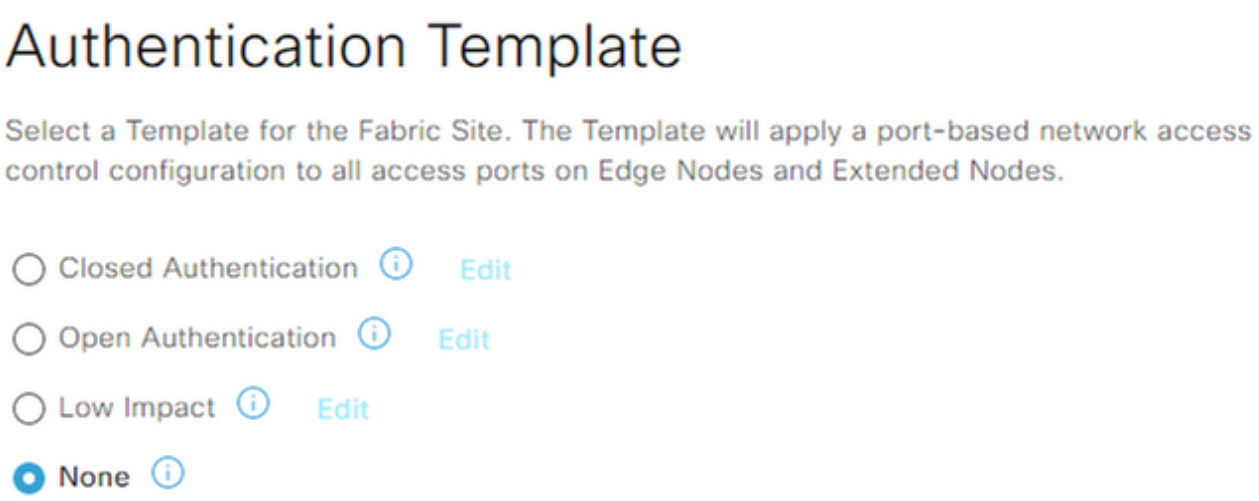
Créer des sites de fabric

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



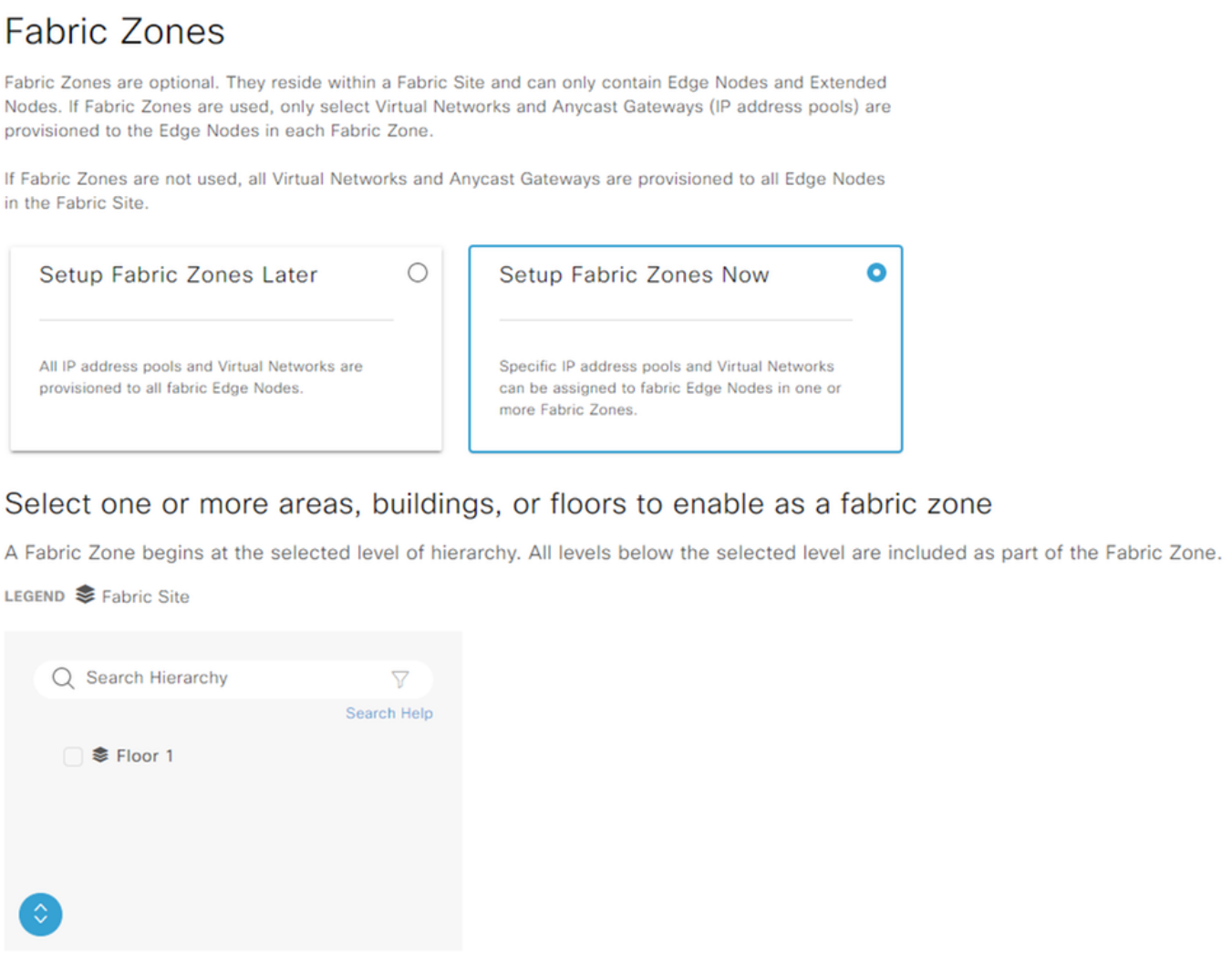
Sélectionner le site de fabric

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



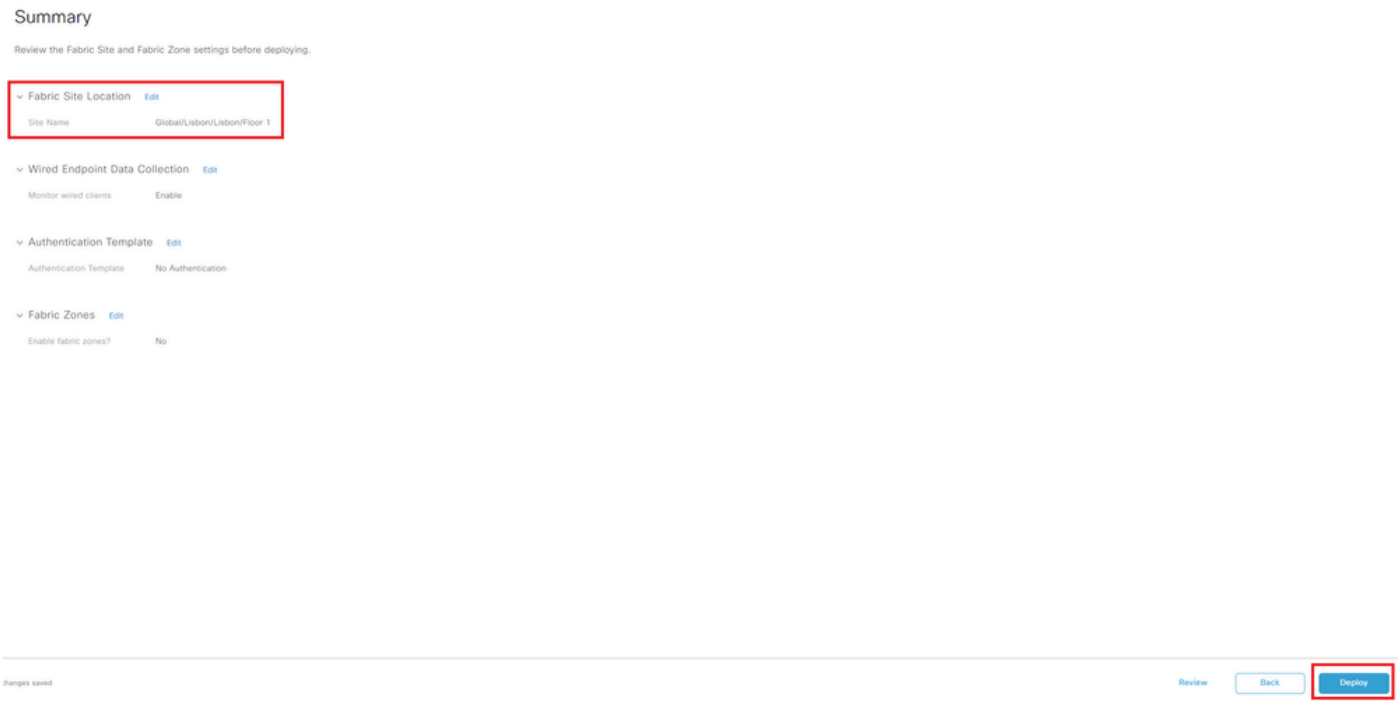
Modèle d'authentification

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



Configuration des zones de fabric

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



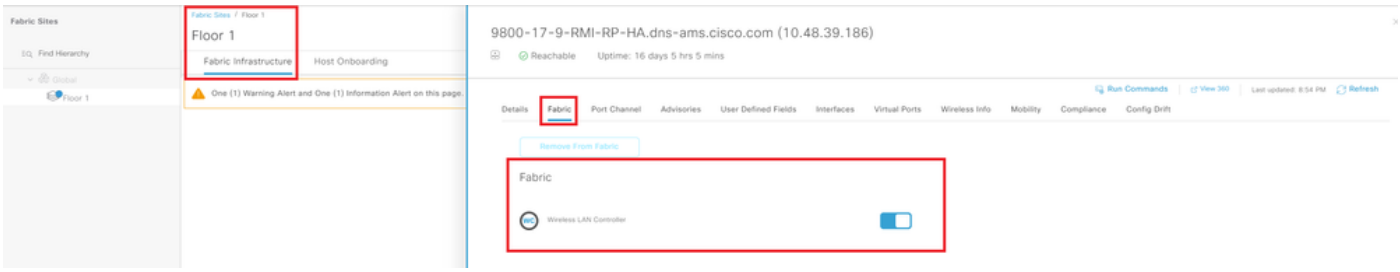
Déployer le site de fabric

Vous avez créé un site de fabric :

Création du site de fabric

Ajouter un WLC au fabric

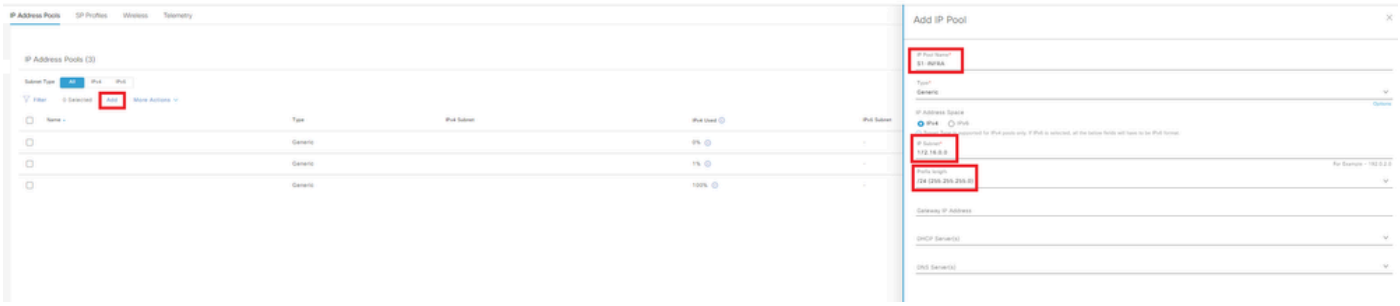
Accédez à Provisionner > Sites de fabric et sélectionnez votre site de fabric. Cliquez sur le haut de votre WLC et naviguez jusqu'à l'onglet Fabric. Activez le fabric sur le WLC, et sélectionnez Add:



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 Provisionner > 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.

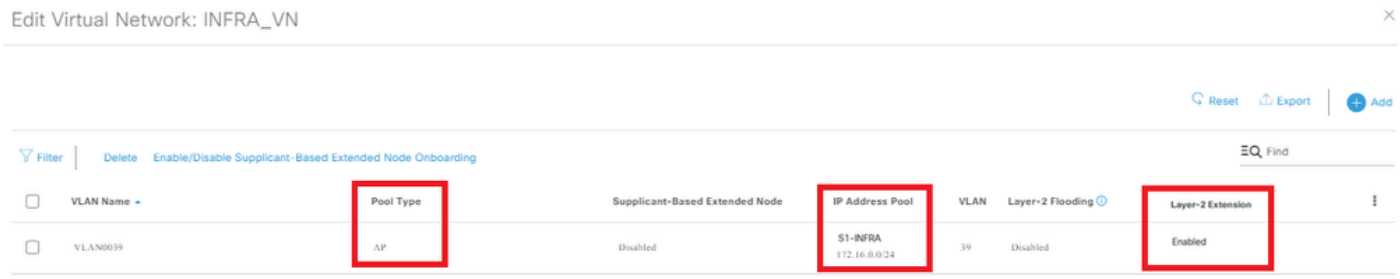
Sélectionnez INFRA_VN > Ajouter :

Modifier le réseau virtuel

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

Modifier le réseau virtuel S1-INFRA

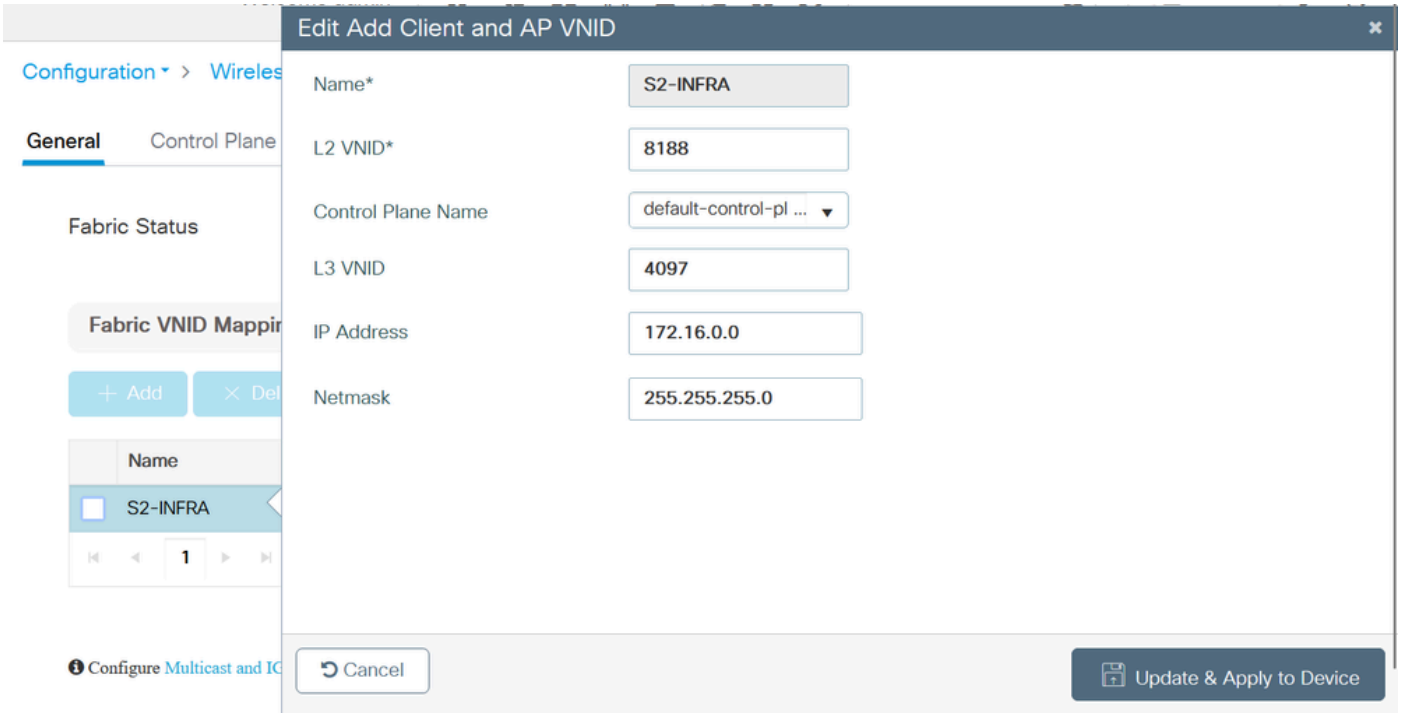
Étape 4 : vérification de l'activation de l'extension de couche 2



Modifier le réseau virtuel

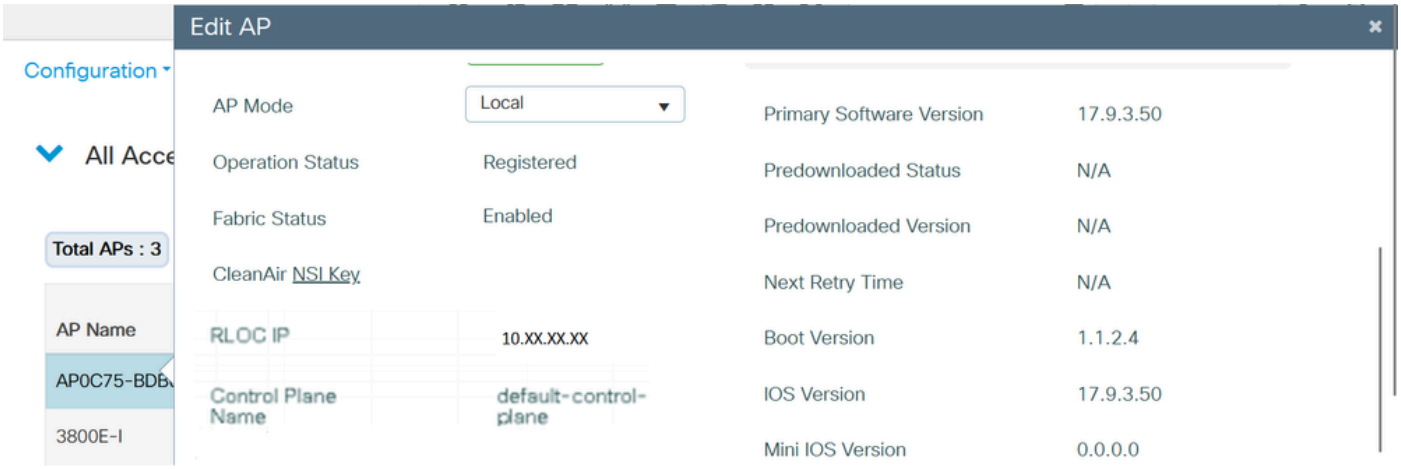
Avec Pool Type = AP et l'extension de couche 2 sur ON, Cisco DNA se connecte au WLC et définit l'interface de fabric sur le mappage VN_ID pour le sous-réseau AP pour les ID de VLAN L2 et L3.

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



Ajouter un nouveau client et AP VN_ID

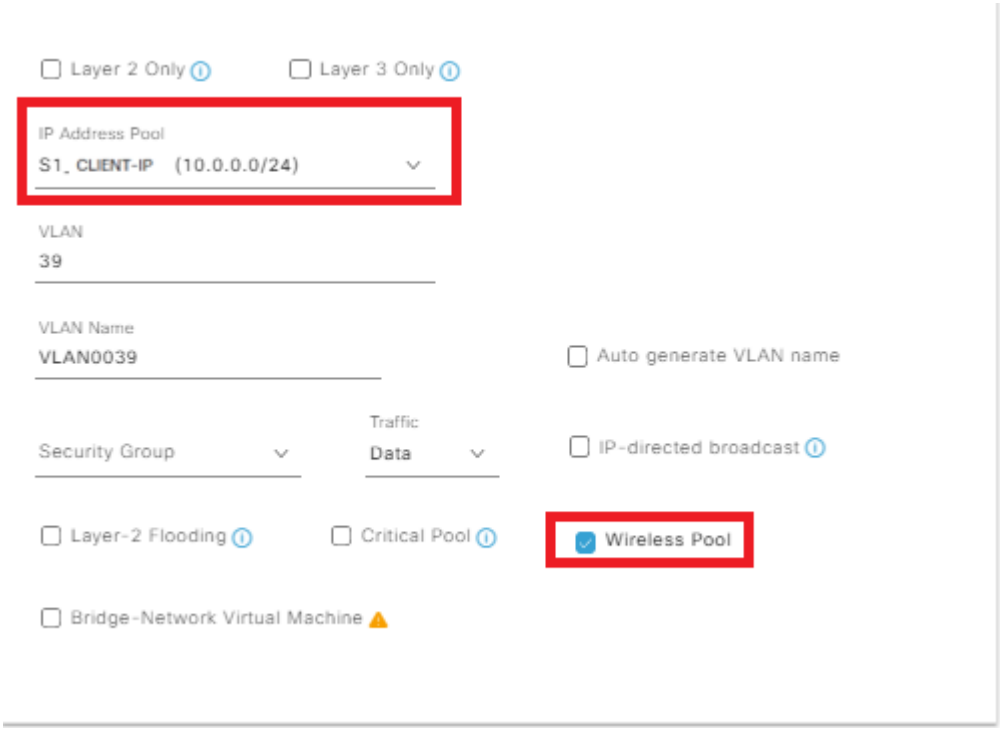
Étape 6. Accédez à Configuration > Wireless > Access Points. Sélectionnez un point d'accès dans la liste. Vérifiez que l'état du fabric est activé, l'adresse IP du plan de contrôle et le nom du plan de contrôle :



Vérifier l'état du fabric AP

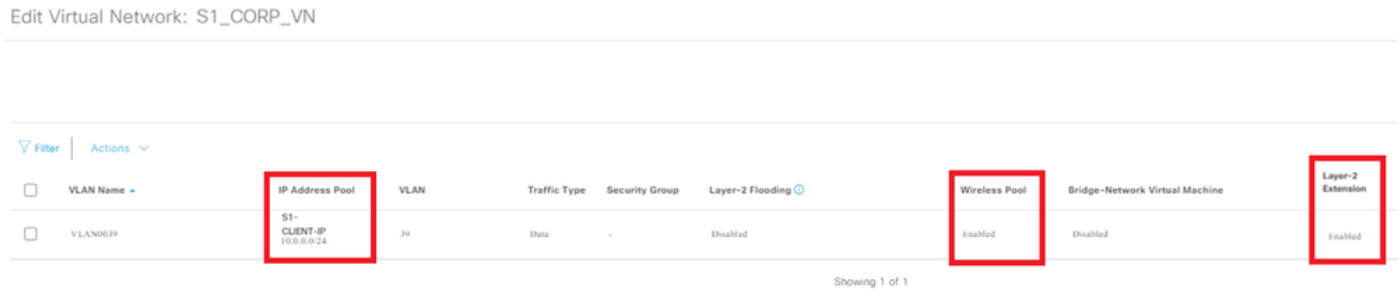
Client à bord

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.



Ajouter un pool d'adresses IP

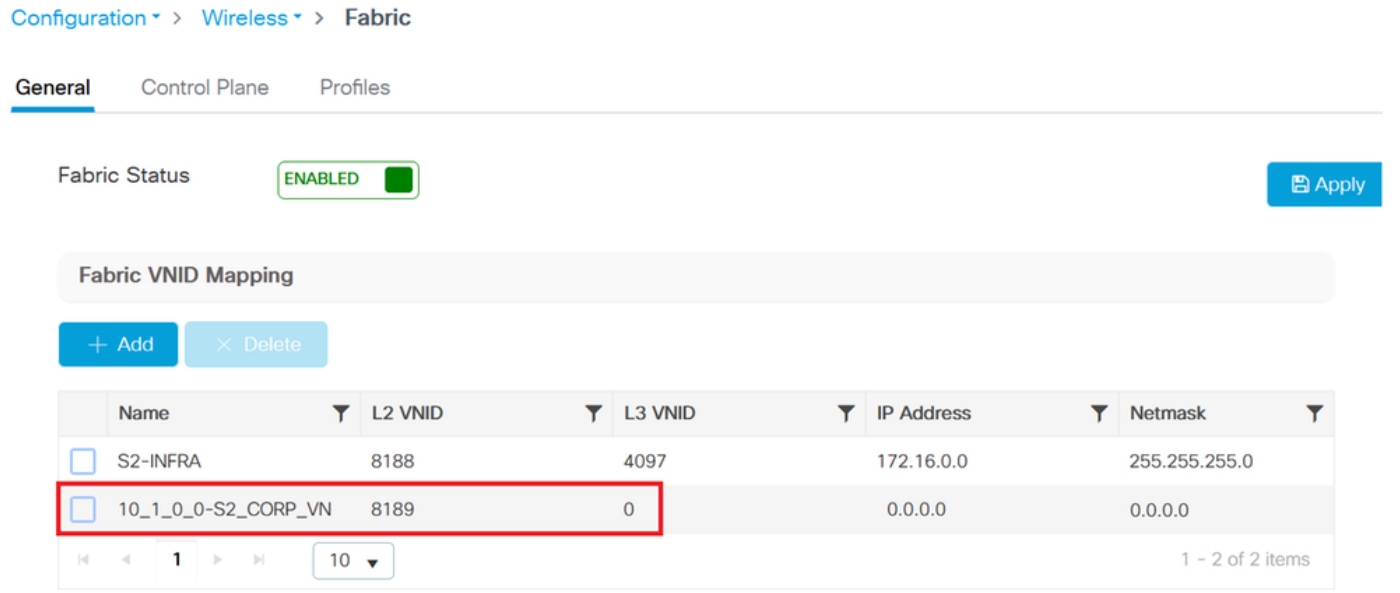
Étape 2 : vérification de l'activation de l'extension de couche 2 et du pool sans fil



Modifier le réseau virtuel

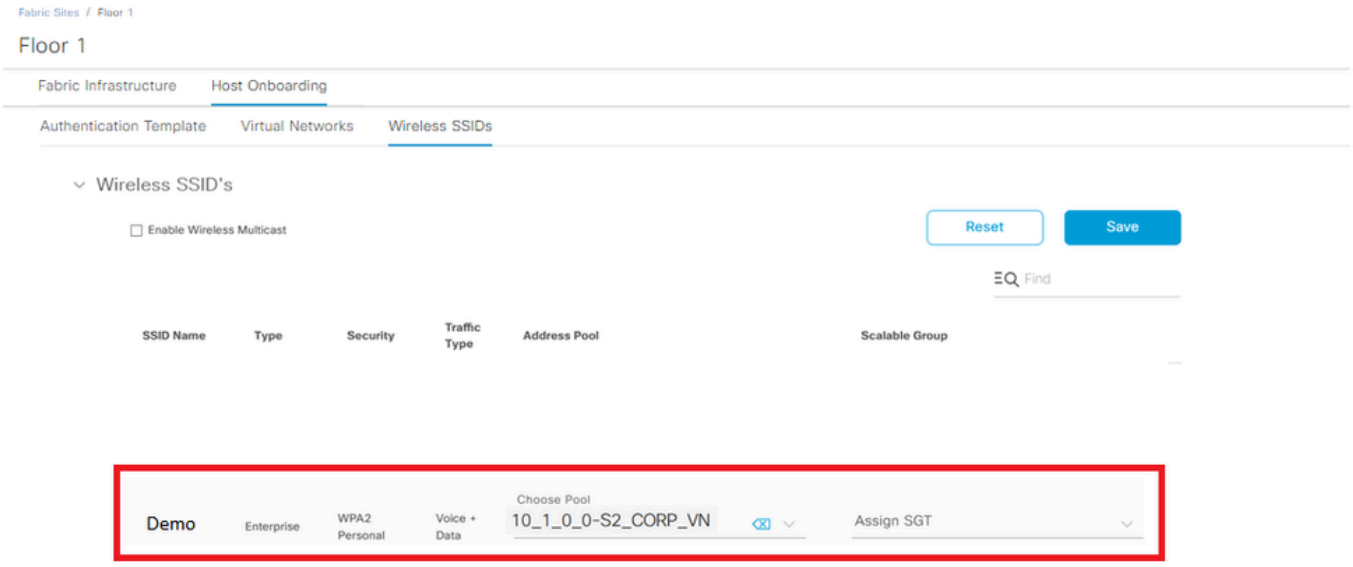
Étape 3. Du côté de l'interface graphique utilisateur WLC, naviguez vers Configuration > Wireless > Fabric > General. Ajoutez un nouveau client et un ID de VLAN AP.

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.



Ajouter un nouveau client et AP VN_ID

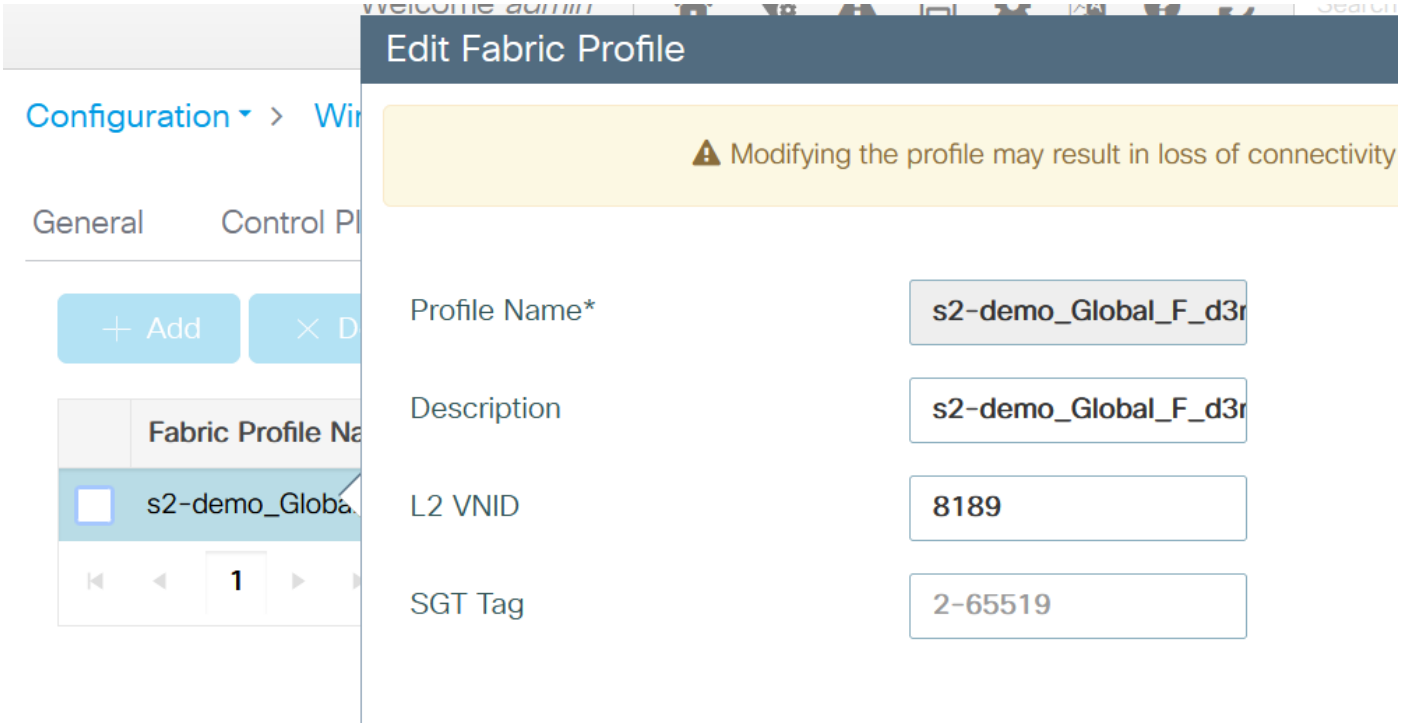
Étape 4. Les SSID sont mappés au pool dans les réseaux virtuels respectifs :



SSID mappés

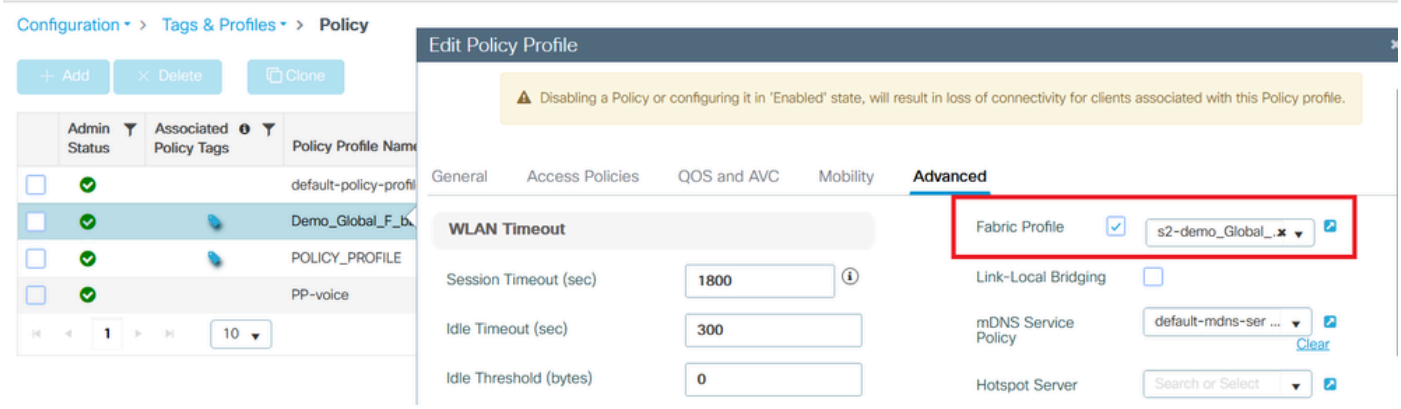
Étape 5. Un profil de fabric avec le VNID L2 est ajouté au pool choisi et le profil de stratégie est mappé au profil de fabric, il est activé pour le fabric.

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



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.