# Software-Defined Access implementeren voor draadloze communicatie met DNA

## Inhoud



## Inleiding

In dit document wordt beschreven hoe SDA kan worden geïmplementeerd voor draadloze technologie met betrekking tot fabric-compatibele WLC en LAP-toegang op Cisco DNA.

# Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van 9800 Wireless LAN-controllers (WLC)
- Lichtgewicht toegangspunten (LAP's)
- Cisco DNA

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 9800-CL WLC Cisco IOS® XE, versie 17.9.3
- Cisco-toegangspunten: 9130AX, 3802E, 1832I
- Cisco DNA versie 2.3.3.7

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# SD-Access

Software-Defined Access bepaalt en handhaaft automatisch beveiligingsbeleid in het hele netwerk, met dynamische regels en geautomatiseerde segmentatie, en stelt de eindgebruiker in staat om te bepalen en te configureren hoe de gebruikers verbinding maken met hun netwerk. SD-Access stelt een eerste niveau van vertrouwen in met elk eindpunt dat is verbonden en controleert het voortdurend om het niveau van vertrouwen opnieuw te verifiëren. Als een eindpunt zich niet normaal gedraagt of een bedreiging wordt gedetecteerd, kan de eindgebruiker het onmiddellijk insluiten en actie ondernemen voordat de inbreuk plaatsvindt, het bedrijfsrisico verminderen en zijn bronnen beschermen. Volledig geïntegreerde oplossing en eenvoudig te implementeren en te configureren op zowel nieuwe als geïmplementeerde netwerken.

SD-Access is een Cisco-technologie die een evolutie is van het traditionele campusnetwerk dat intent-based networking (IBN) en centrale beleidscontrole biedt met het gebruik van Software-Defined Networking (SDN) -componenten.

Drie netwerkgerichte pijlers van SD-Access:

1. Een netwerkstructuur: het is een abstractie van het netwerk zelf die programmeerbare overlays en virtualisatie ondersteunt. De netwerkverbinding ondersteunt zowel bekabelde als draadloze toegang, maakt het mogelijk om meerdere logische netwerken te hosten die van elkaar zijn gesegmenteerd en worden gedefinieerd door zakelijke intenties.

2. Orchestratie: Cisco DNA is de orkestrator engine van SDA. Cisco DNA functioneert als een SDN-controller. Het implementeert beleidsregels en configuratiewijzigingen in de fabric. Het bevat ook een tool die het netwerkontwerp ondersteunt en realtime telemetriebewerkingen en prestatieanalyses ondersteunt via DNA Assurance. De rol van Cisco DNA is om de netwerkstructuur te orkestreren om beleidswijzigingen en netwerkintentie te leveren voor beveiliging, Quality of Service (QoS) en microsegmentatie.
3. Identity Services Engine (ISE) is de tool die het netwerkbeleid definieert. ISE organiseert hoe de apparaten en knooppunten worden gesegmenteerd in virtuele netwerken. ISE definieert ook schaalbare groepstags (SGT's) die door toegangsapparaten worden gebruikt om gebruikersverkeer te segmenteren wanneer het de fabric binnenkomt. SGR's zijn verantwoordelijk voor het handhaven van het microsegmentatiebeleid dat door ISE is gedefinieerd.

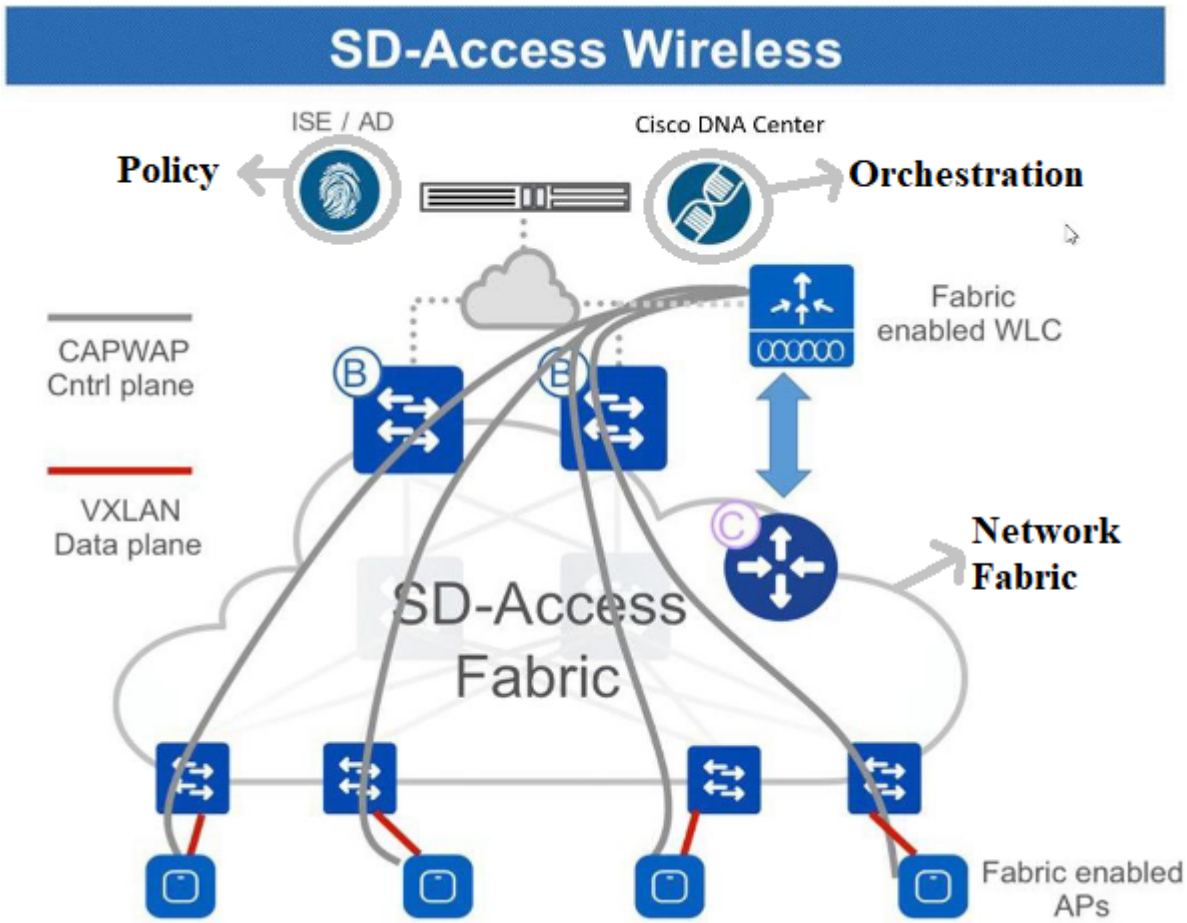
SDA is gebaseerd op gecentraliseerde orkestratie. De combinatie van Cisco DNA als de programmeerbare orkestratie-engine, ISE als de policy engine en een nieuwe generatie programmeerbare switches maakt het een veel flexibeler en beter beheersbaar stoffensysteem dan alles wat ooit is voorgekomen.

---

Opmerking: Dit document behandelt specifiek SD-Access Wireless.

---

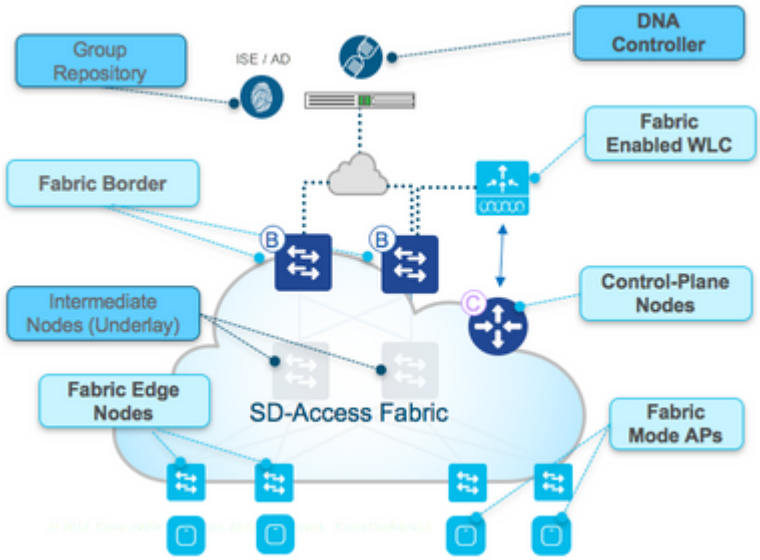
De netwerkstructuur bestaat uit deze elementen:



De draadloze integratie met fabric leidt tot verschillende voordelen voor het draadloze netwerk, bijvoorbeeld: het aanpakken van vereenvoudiging, mobiliteit met uitgerekte subnetten over fysieke locaties en microsegmentatie met gecentraliseerd beleid dat consistent is in zowel het bekabelde als het draadloze domein. Het stelt de controller ook in staat om het gegevensvlak af te werpen om taken door te sturen terwijl het blijft functioneren als de gecentraliseerde services en het controlevlak voor het draadloze netwerk. De schaalbaarheid van draadloze controllers is dus eigenlijk verhoogd omdat het geen dataverkeer meer hoeft te verwerken, vergelijkbaar met het FlexConnect-model.

# SD-Access draadloze architectuur

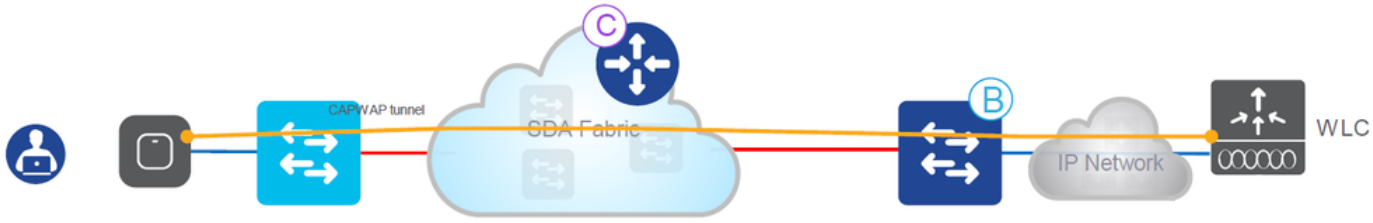
## Overzicht




Overzicht van SDA

Er zijn twee primaire SDA-ondersteunde modellen voor draadloze implementatie:

Een daarvan is een over-the-top (OTT)-methode, een traditionele CAPWAP-implementatie die bovenop een bekabeld netwerk is aangesloten. De SDA-fabric transporteert de CAPWAP-besturing en het dataverkeer naar de draadloze controller:

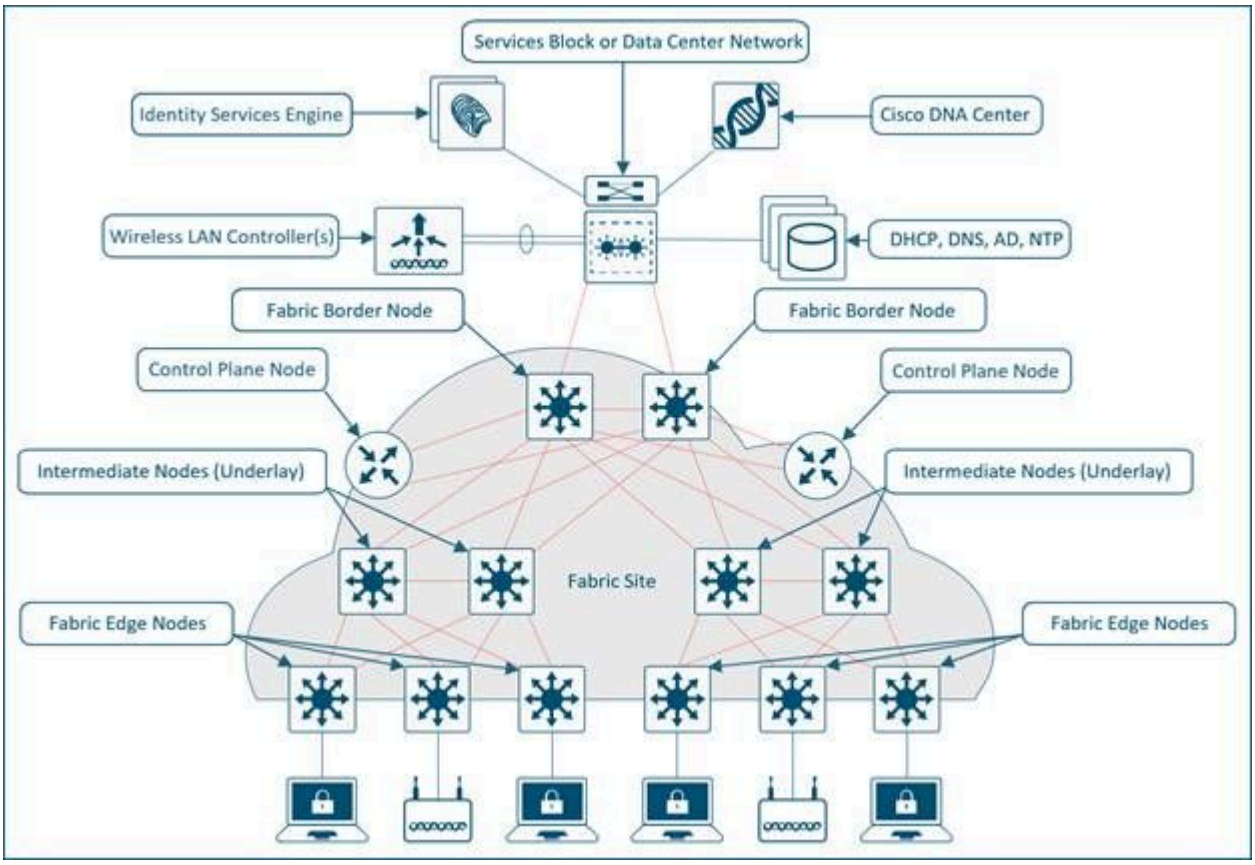



over-the-top-methode

In dit implementatiemodel is de SDA-fabric een transportnetwerk voor draadloos verkeer (een

model dat vaak wordt gebruikt bij migraties). Het toegangspunt werkt op dezelfde manier als de klassieke lokale modus: zowel de CAPWAP-besturing als de gegevensvlakken eindigen op de controller, wat betekent dat de controller niet rechtstreeks deelneemt aan de fabric. Dit model wordt vaak gebruikt wanneer bekabelde switches voor het eerst naar de SDA-fabric worden gemigreerd, maar het draadloze netwerk is nog niet klaar voor volledige fabric-overlay-integratie.

De andere implementatiemodellen zijn het volledig geïntegreerde SDA-model. Het draadloze netwerk is volledig geïntegreerd in de fabric en neemt deel aan overlays, waardoor verschillende WLAN's deel kunnen uitmaken van verschillende virtuele netwerken (VN's). De draadloze controller beheert alleen het CAPWAP-besturingsvlak (om toegangspunten te beheren) en het CAPWAP-gegevensvlak komt niet naar de controller:




Volledig geïntegreerd SDA-model

Het draadloze gegevensvlak wordt op dezelfde manier behandeld als bekabelde switches - elk toegangspunt vat gegevens in VXLAN samen en verzendt deze naar een knooppunt aan de rand van de fabric waar deze vervolgens naar een ander knooppunt aan de rand van de fabric wordt verzonden. De draadloze controllers moeten worden geconfigureerd als fabric-controllers, wat een wijziging is ten opzichte van hun normale werking.

Controllers met verbindingsmogelijkheden communiceren met het controlevlak van de verbinding, registreren Layer 2-client-MAC-adressen en Layer 2 Virtual Network Identifier (VNI)-informatie. De toegangspunten zijn verantwoordelijk voor de communicatie met draadloze eindpunten en helpen het VXLAN-gegevensvliegtuig door inkapseling en het ontkapselen van verkeer.

## SDA rollen en terminologie

De netwerkstructuur bestaat uit deze elementen:

- Control-Plane Node: Dit is het locatietoewijzingssysteem (hostdatabase) dat deel uitmaakt van het besturingsvlak van het Location Separator Protocol (LISP), dat de endpoint identity (EID) beheert voor locatierelaties (of apparaatrelaties). Ofwel het controlevlak kan een speciale router zijn die de functies van het controlevlak biedt, ofwel het kan naast andere netwerkelementen van de stof bestaan.

- Fabric Border Nodes: Doorgaans een router die functioneert op de grens tussen externe netwerken en de SDA-structuur, die routeringsservices biedt naar de virtuele netwerken in de structuur. Het verbindt externe Layer 3-netwerk(en) met de SDA-structuur.

- Fabric Edge Nodes: Apparaat in de fabric dat niet-fabric-apparaten, zoals switches, toegangspunten en routers, verbindt met de SDA-fabric. Dit zijn de knooppunten die de virtuele overlays tussen tunnels en VN's met Virtual eXtensible LAN (VXLAN) maken en de SGT's opleggen aan fabric-gebonden verkeer. De netwerken aan beide zijden van de rand van de stof bevinden zich in het SDA-netwerk. Ze verbinden bekabelde eindpunten met de SD-Access-fabric.

- Tussenliggende knooppunten: deze knooppunten bevinden zich in de kern van de SDA-structuur en maken verbinding met rand- of randknooppunten. De tussenliggende knooppunten gewoon doorsturen SDA-verkeer als IP-pakketten, zich niet bewust dat er meerdere virtuele netwerken betrokken zijn.

- Fabric WLC: draadloze controller die is ingeschakeld voor de verbinding en die deelneemt aan het SDA-besturingsvlak, maar die het CAPWAP-gegevensvlak niet verwerkt.

- Verbindingsmodus-toegangspunten: toegangspunten die zijn ingeschakeld voor de verbinding. Draadloos verkeer is VXLAN-ingekapseld op het toegangspunt, waardoor het via een edge-node naar de fabric kan worden verzonden.

- Cisco DNA (DNAC): De Enterprise SDN-controller voor het Software Defined Access (SDA) fabric overlay-netwerk en is verantwoordelijk voor zowel automatiserings- als verzekeringstaken. Het kan ook worden gebruikt voor sommige automatiseringstaken en gerelateerde taken voor de netwerkapparaten die de onderlaag vormen (dat is niet-SDA-gerelateerd).

- ISE: De Identity Services Engine (ISE) is een verbeterd beleidsplatform dat verschillende rollen en functies kan vervullen, niet in de laatste plaats die van de verificatie-, autorisatie- en boekhoudserver (AAA). ISE werkt doorgaans samen met Active Directory (AD), maar gebruikers kunnen lokaal en op ISE zelf worden geconfigureerd voor kleinere implementaties.

---

Opmerking: het besturingsvlak is een essentieel onderdeel van de SDA-architectuur, dus het wordt aanbevolen om het op een veerkrachtige manier in te zetten.

---

# Onderliggende en overlappende netwerken

De SDA-architectuur maakt gebruik van fabric-technologie die programmeerbare virtuele netwerken (overlay-netwerken) ondersteunt die op een fysiek netwerk (een onderliggend netwerk) worden uitgevoerd.

Een stof is een overlay.

Een Overlay-netwerk is een logische topologie die wordt gebruikt om apparaten virtueel te verbinden, gebouwd over een willekeurige fysieke Underlay-topologie. Het maakt gebruik van alternatieve forward attributen om extra diensten te leveren die niet door de Underlay worden geleverd. Het is gemaakt bovenop de onderlaag om een of meer gevirtualiseerde en gesegmenteerde netwerken te maken. Vanwege de software-gedefinieerde aard van overlays, is het mogelijk om ze op zeer flexibele manieren aan te sluiten zonder de beperkingen van fysieke connectiviteit. Het is een eenvoudige manier om beveiligingsbeleid af te dwingen, omdat de overlay programmeerbaar kan zijn om één fysiek exit-punt te hebben (de fabric border node) en één firewall kan worden gebruikt om de netwerken erachter te beschermen (of ze zich kunnen bevinden). Overlay omvat verkeer met het gebruik van VXLAN. VXLAN omvat complete Layer 2-frames voor transport over de onderlaag, waarbij elk overlay-netwerk wordt geïdentificeerd door een VXLAN-netwerkidentificatie (VNI). Overlay-fabrics zijn vaak complex en vereisen een aanzienlijke hoeveelheid beheerdersoverhead voor nieuwe virtuele netwerken die worden geïmplementeerd of voor het implementeren van beveiligingsbeleid.

Voorbeelden van overlays in het netwerk:

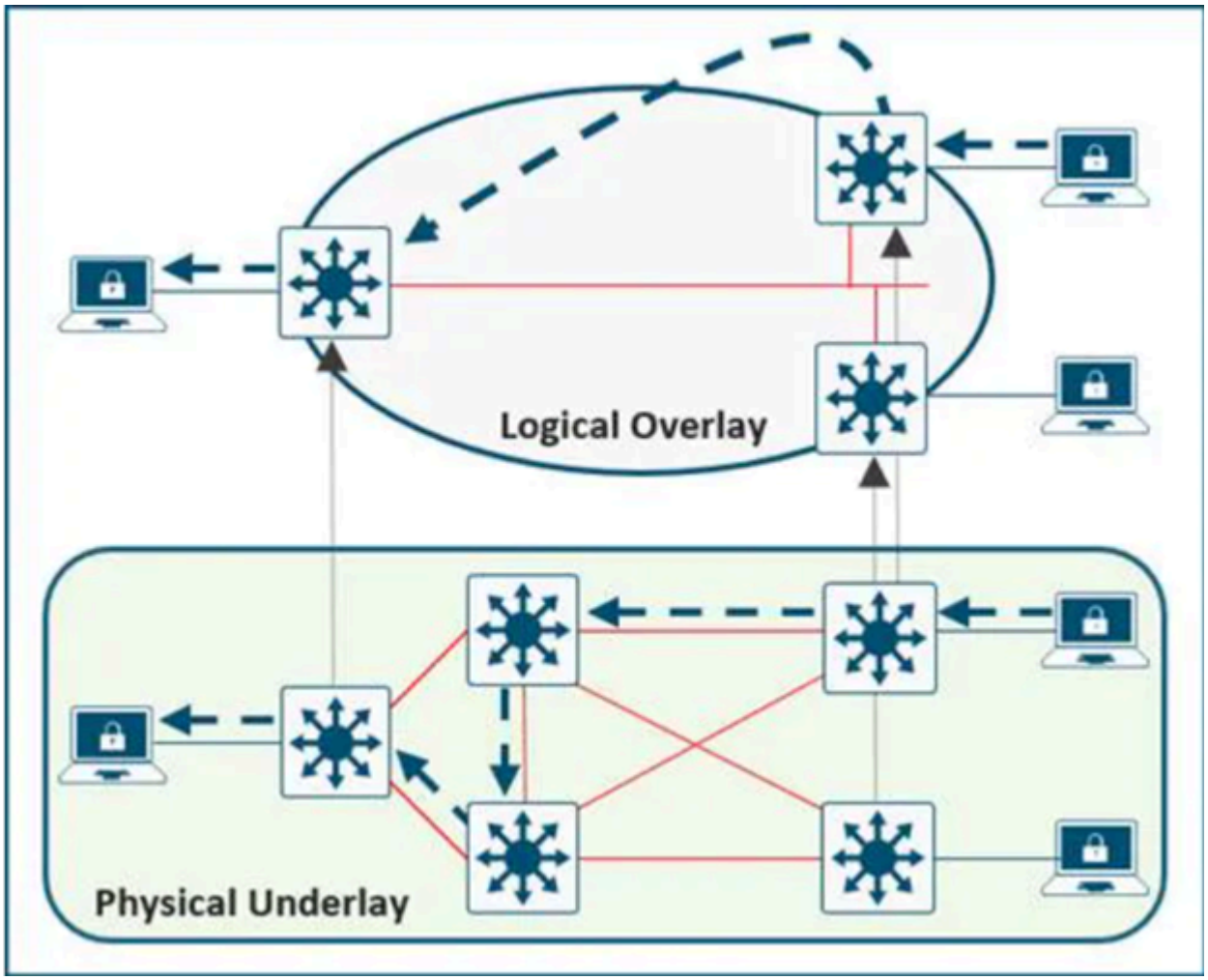
- GRE, mGRE
- MPLS, VPLS
- IPSec, DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI

Een onderliggend netwerk wordt gedefinieerd door de fysieke knooppunten zoals switches, routers en draadloze toegangspunten die worden gebruikt om het SDA-netwerk te implementeren. Alle netwerkelementen van de onderlaag moeten IP-connectiviteit tot stand brengen via het gebruik van een routeringsprotocol. Hoewel het onderliggende netwerk waarschijnlijk geen gebruik zal maken van het traditionele toegangs-, distributie- of kernmodel, moet het een goed ontworpen Layer 3-fundering gebruiken die robuuste prestaties, schaalbaarheid en hoge beschikbaarheid biedt.

---

Opmerking: SDA ondersteunt IPv4 in het onderliggende netwerk en IPv4 en/of IPv6 in overlaynetwerken.

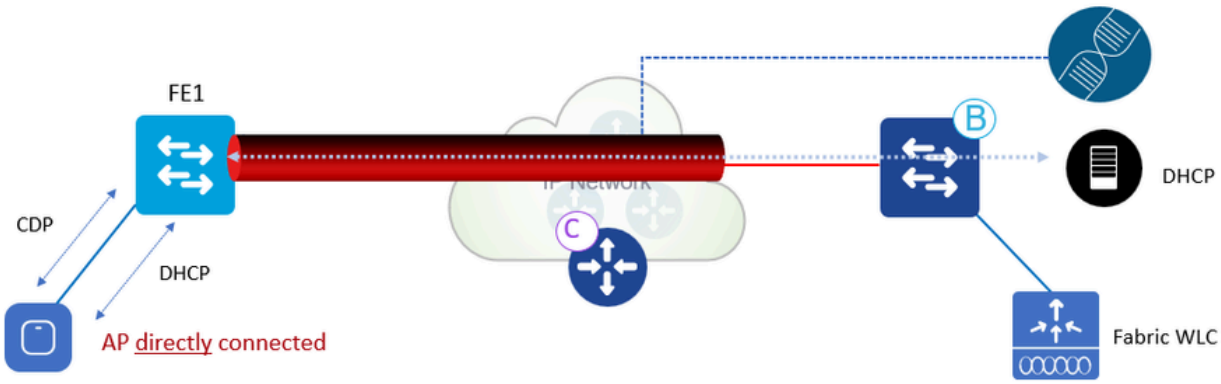
---




Onderliggende en overlappende netwerken

# Basisworkflows

## AP Join




Deelnemen aan werkstroom voor toegangspunt

Deelnemen aan werkstroom toegangspunt:

1. Beheerder configureert AP-pool in DNAC in INFRA_VN. Cisco DNA voorziet vooraf een

configuratie op alle Fabric Edge-knooppunten om automatisch AP's aan boord te krijgen.

2. Het toegangspunt is aangesloten en wordt ingeschakeld. Fabric Edge ontdekt dat het een toegangspunt is via CDP en past de macro toe om de interfacesjabloon (of de interfacesjabloon) toe te wijzen aan de switch-poort van het juiste VLAN.

3. AP krijgt een IP-adres via DHCP in de overlay.

4. Fabric Edge registreert het IP-adres en de MAC (EID) van het toegangspunt en werkt het controlevlak (CP) bij.

5. AP leert WLC's IP met traditionele methoden. Fabric AP wordt toegevoegd als toegangspunt voor de lokale modus.

6. WLC controleert of het geschikt is voor textiel (Wave 2 of Wave 1 AP's).

7. Als AP wordt ondersteund voor Fabric, vraagt WLC de CP om te weten of AP is verbonden met Fabric.

8. Controlevliegtuig (CP) antwoordt op WLC met RLOC. Dit betekent dat AP is aangesloten op Fabric en wordt weergegeven als "Fabric enabled".

9. WLC voert een L2 LISP-registratie uit voor AP in CP (dat wil zeggen AP "speciale" beveiligde clientregistratie). Dit wordt gebruikt om belangrijke metagegevens van WLC door te geven aan de Fabric Edge.

10. In reactie op deze proxyregistratie meldt Control Plane (CP) Fabric Edge en geeft de metagegevens door die zijn ontvangen van WLC (vlag die aangeeft dat het een toegangspunt en het IP-adres van het toegangspunt is).

11. Fabric Edge verwerkt de informatie, leert dat het een toegangspunt is en maakt een VXLAN-tunnelinterface met het opgegeven IP-adres (optimalisatie: de switch is klaar voor clients om toe te treden).

De opdrachten debug/show kunnen worden gebruikt om de werkstroom van de AP-join te verifiëren en te valideren.

Besturingsplane

DEBUG LISP CONTROL-plane ALL

lisp instance-id <L3 instance-id> ipv4-server weergeven (moet het IP-adres van het toegangspunt weergeven dat is geregistreerd door edge-switch waarop het toegangspunt is aangesloten.)

lisp instance-id <L2 instance-id> ethernetserver weergeven (Moet zowel de AP-radio als het Ethernet-mac-adres, de AP-radio die is geregistreerd door de WLC en de Ethernet-mac weergeven door de edge-switch waar het AP is aangesloten.)

Edge-switch

debug access-tunnel all

DEBUG LISP CONTROL-plane ALL

Overzicht toegangstunnel weergeven

lisp-instantie < L2 instance id> Ethernet-database wlc-toegangspunten weergeven (Hier moet de AP-radio mac worden weergegeven.)

WLC

Fabric AP-overzicht weergeven

WLC LISP-debugs

Platform Software Traceer WNCD Chassis Active R0 LISP-Agent-API debug instellen

Set Platform Software Trace WNCD Chassis Active R0 LISP-Agent-DB Debug

Debug. platformsoftware traceren WNCD-chassis actief R0 LISP-Agent-FSM

Platform Software Traceer WNCD Chassis Active R0 LISP-Agent-internal debug instellen

Debugging platformsoftware traceren WNCD-chassis actief R0 LISP-Agent-LIB

Debug. platformsoftware traceren WNCD-chassis actief R0 LISP-Agent-Lispmsg

Set Platform Software Trace WNCD Chassis Active R0 LISP-Agent-SHIM Debug

Set Platform Software Trace WNCD Chassis Active R0 LISP-Agent-Transport Debug

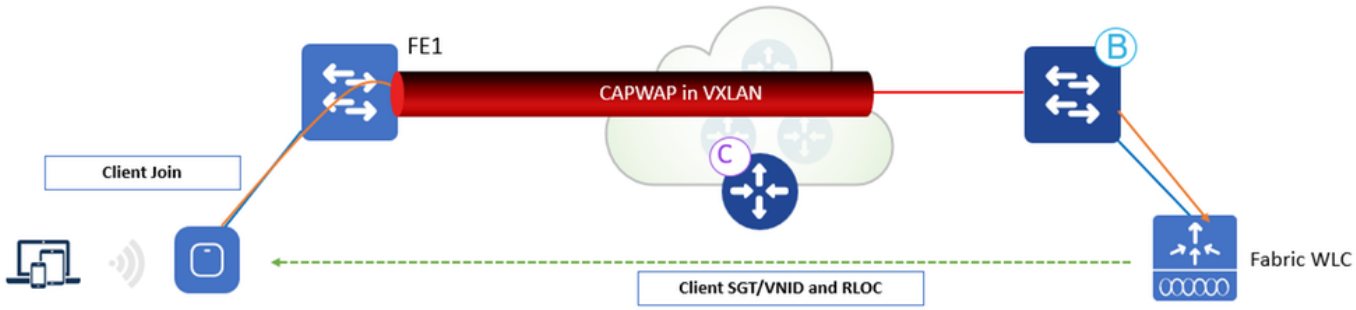
Set Platform Software Trace WNCD Chassis Active R0 LISP-Agent-HA debug

Set Platform Software Trace WNCD Chassis Active R0 EWLC-INFRA-EVQ debug

Access point

Toon IP-tunnelstof

## Client aan boord



Client Onboard Workflow:

1. De client verifieert de verbinding met een WiFi-verbinding. WLC krijgt SGT van ISE, updates AP met client L2VNID en SGT samen met RLOC IP. WLC kent RLOC van AP van interne database.

2. WLC-proxy registreert client L2-informatie in CP; dit is LISP-gewijzigd bericht om aanvullende informatie door te geven, zoals de client SGT.

3. Fabric edge krijgt een melding van CP en voegt client MAC in L2 toe aan de forward table en gaat het beleid van ISE ophalen op basis van de client SGT.

4. Klant initieert DHCP-verzoek.

5. AP vat het samen in VXLAN met L2 VNI-informatie.

6. Fabric Edge koppelt L2 VNID aan VLAN-interface en stuurt DHCP door in de overlay (hetzelfde als voor een bekabelde Fabric-client).

7. De klant ontvangt een IP-adres van DHCP.

8. DHCP-snooping (en/of ARP voor statisch) activeert de EID-registratie van de client door de Fabric Edge naar de CP.

De opdrachten voor foutopsporing/weergeven kunnen worden gebruikt om de onboard workflow van de client te verifiëren en te valideren.

Besturingsplane

DEBUG LISP CONTROL-plane ALL

Edge-switch

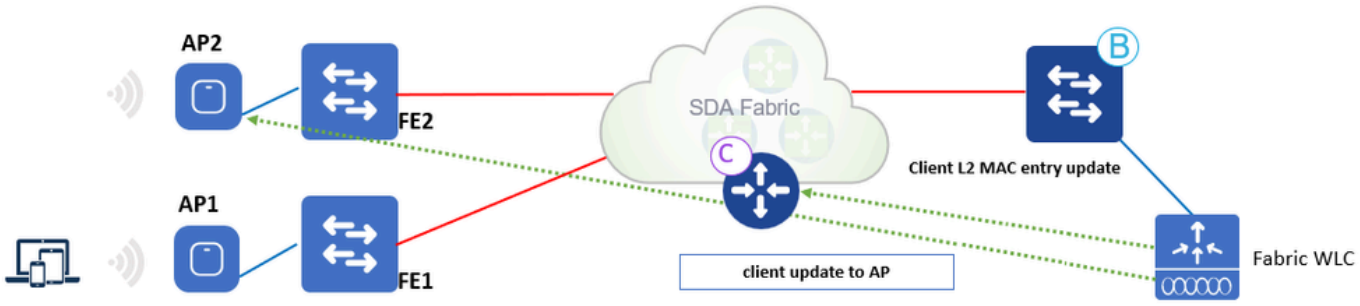
DEBUG LISP CONTROL-plane ALL

Debug IP DHCP-snooppakket/gebeurtenis

WLC

Voor LISP-communicatie worden dezelfde debugs als AP toegevoegd.

## Client Roams




Workflow Client Roams

Workflow Client Roams:

1. Cliënt roamt naar AP2 op FE2 (roaming tussen switches). WLC wordt op de hoogte gebracht door AP.

2. WLC werkt forward table bij op AP met clientinfo (SGT, RLOC).

3. WLC werkt de L2 MAC-vermelding in CP bij met de nieuwe RLOC Fabric Edge 2.

4. CP meldt vervolgens:

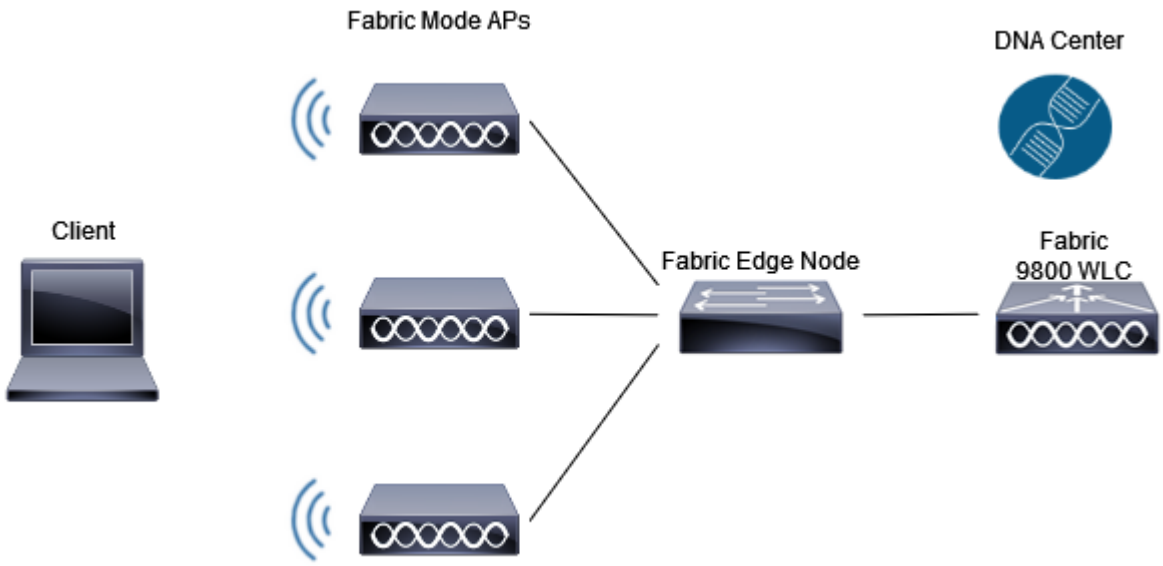
- Fabric Edge FE2 (roam-to-switch) om de client-MAC toe te voegen aan de voorwaartse tabel die naar de VXLAN-tunnel wijst.
- Fabric Edge FE1 (roam-from-switch) om de draadloze client op te schonen.

5. Fabric Edge werkt het L3-item (IP) in de CP-database bij wanneer het verkeer ontvangt.

6. Roam is Layer 2 omdat Fabric Edge 2 dezelfde VLAN-interface heeft (Anycast GW).

# Configureren

## Netwerkdiagram



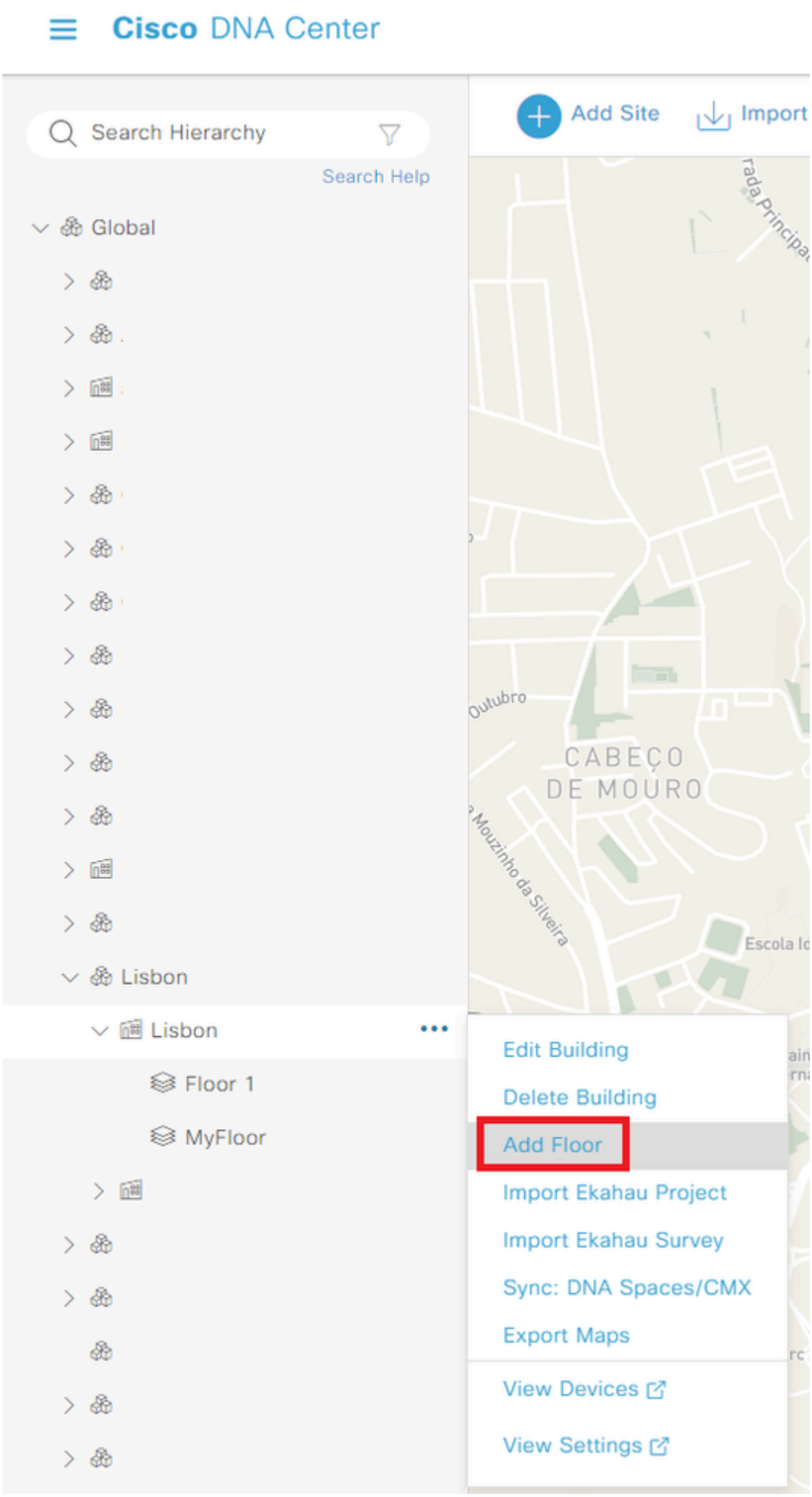

Netwerkdiagram

# WLC-detectie en -levering in Cisco DNA

## WLC toevoegen

Stap 1. Navigeer naar de locatie waar u de WLC wilt toevoegen. U kunt een nieuw gebouw/vloer toevoegen.

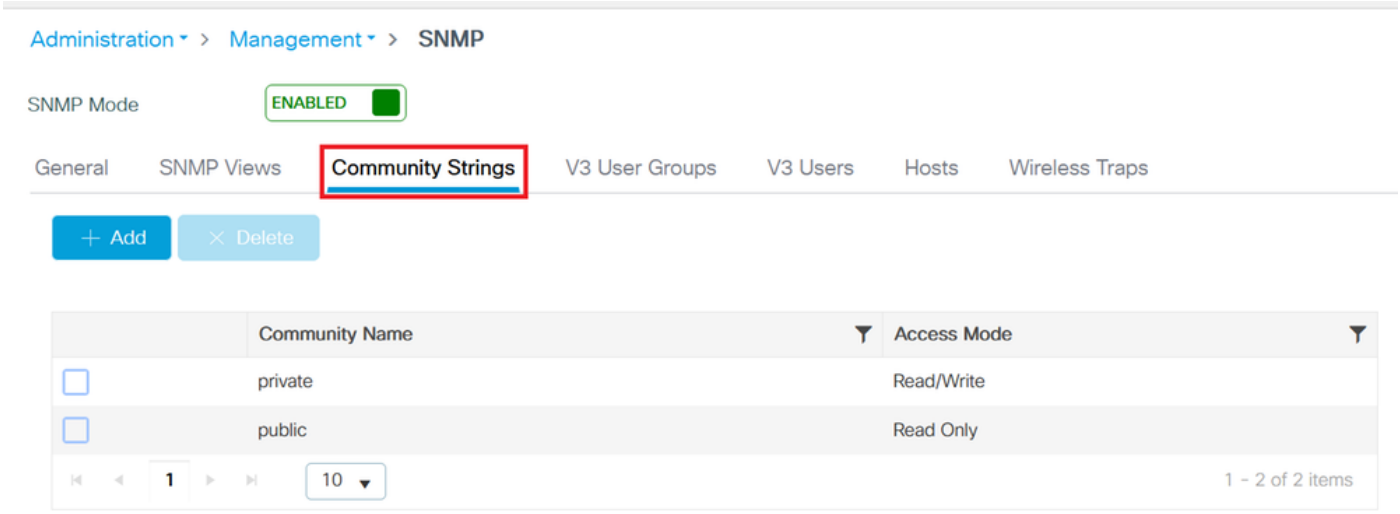
Navigeer naar Ontwerp > Netwerkhiërarchie en betreed het gebouw / vloer, of u kunt een nieuwe verdieping maken, zoals weergegeven in de afbeelding:




Nieuwe vloer maken

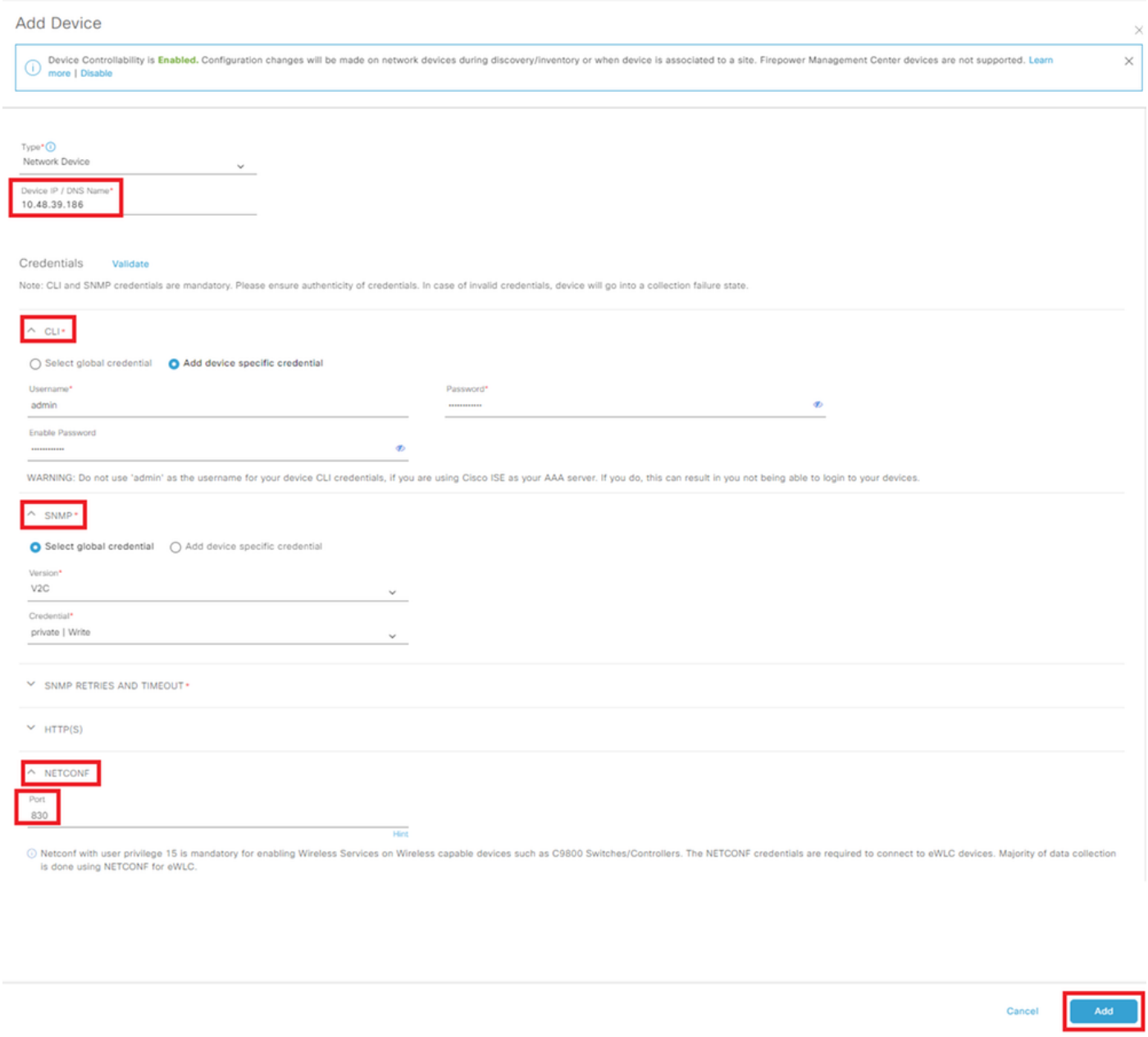
Stap 2. Voeg een vloer toe. U kunt ook een afbeelding van de plant van de vloer uploaden

en controleer de geconfigureerde tekenreeks. U moet de juiste SNMP-communitytekenreeks toevoegen wanneer u de WLC toevoegt aan het Cisco-DNA en ervoor zorgen dat netconf-yang is ingeschakeld op de 9800 WLC met opdrachten voor de netconf-yang-status weergeven. Klik aan het einde op Toevoegen:




SNMP-configuratie

Stap 5. Voeg het WLC IP-adres, de CLI-referenties (de referenties die Cisco DNA gebruikt om in te loggen op de WLC en deze moeten worden geconfigureerd op de WLC voordat deze wordt toegevoegd aan Cisco DNA), de SNMP-tekenreeks toe en controleer of de NETCONF-poort is geconfigureerd op poort 830:




WLC toevoegen

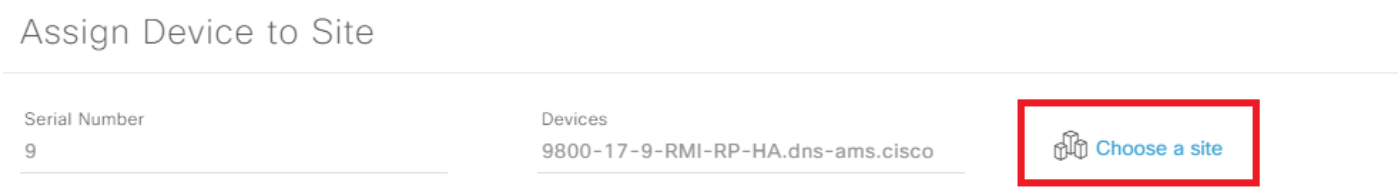
De WLC verschijnt als NA omdat Cisco DNA nog steeds in sync-proces is:


WLC in Sync-proces

Wanneer het synchronisatieproces is voltooid, kunt u de WLC-naam, het IP-adres zien, als deze bereikbaar is, en de beheerde en softwareversie:

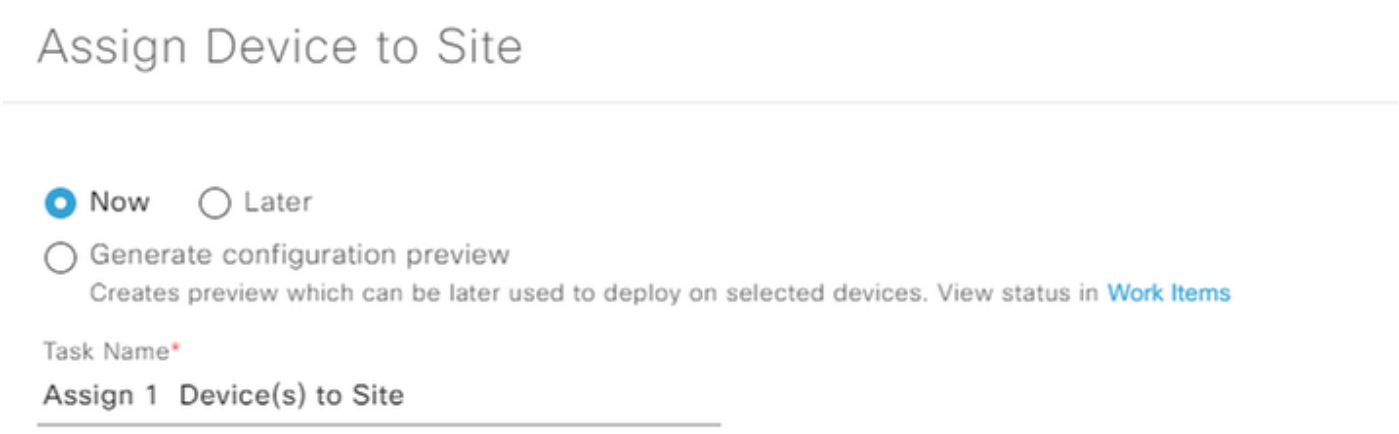

WLC gesynchroniseerd

Stap 6. Wijs de WLC toe aan een site. Klik in de lijst met apparaten op Toewijzen en kies een site:




Apparaat toewijzen aan site

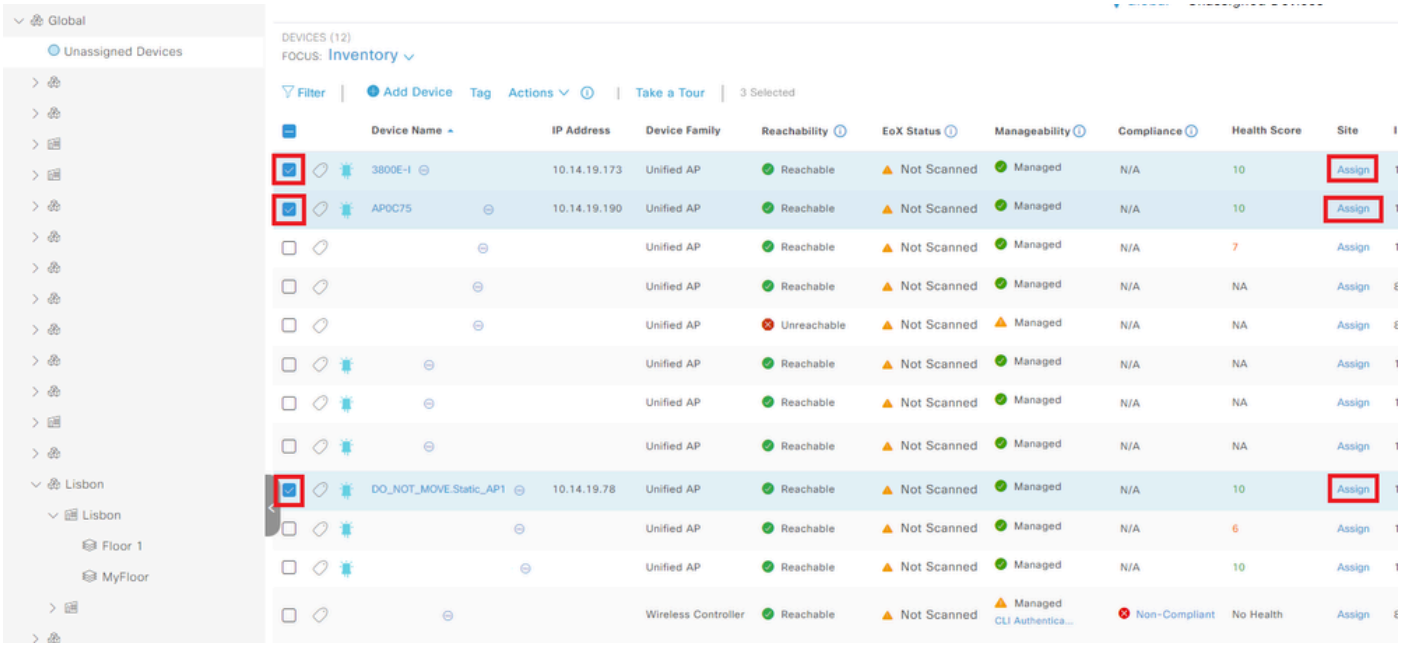
U kunt ervoor kiezen om de site nu of later toe te wijzen:




Apparaat nu of later aan site toewijzen

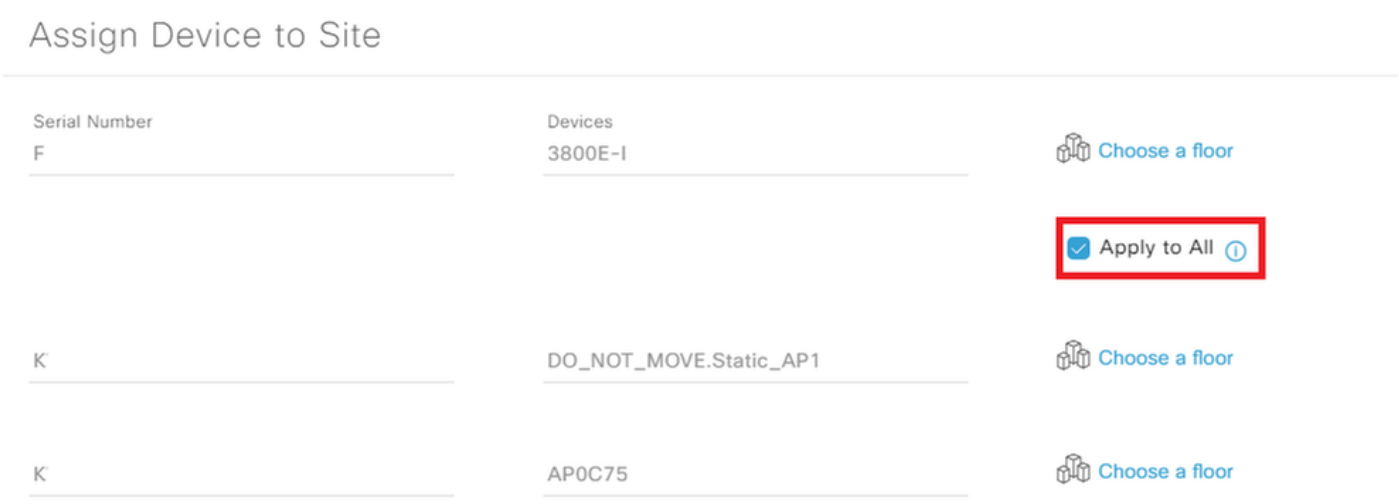
## Toegangspunten toevoegen

Stap 1.Zodra de WLC is toegevoegd en bereikbaar, navigeert u naar Voorzieningen > Inventarisatie > Globaal > Niet-toegewezen apparaten en zoekt u naar de toegangspunten die u hebt toegevoegd aan uw WLC:



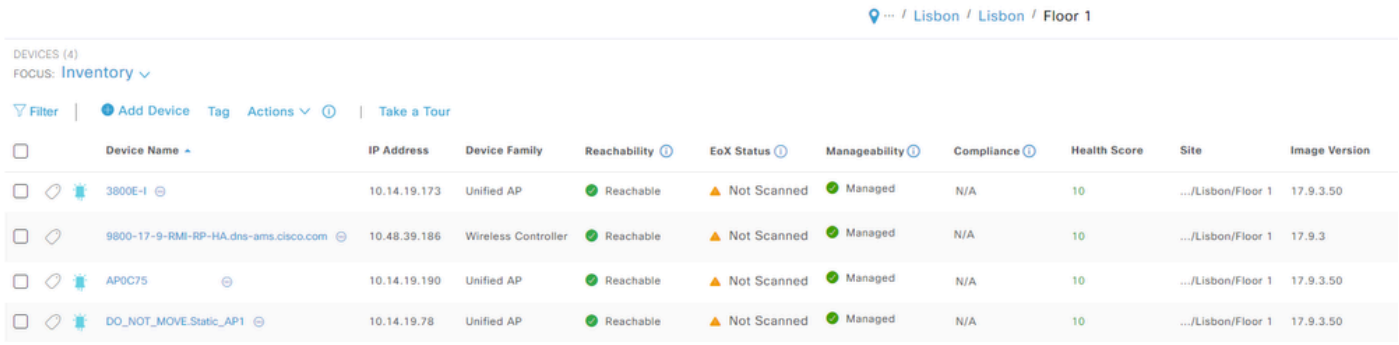

Toegangspunten toevoegen

Stap 2. Selecteer de optie Toewijzen. Wijs de toegangspunten toe aan een site. Vink het vakje Toepassen op iedereen aan om de configuratie voor meer dan één apparaat tegelijk te maken.




AP's toewijzen aan site

Navigeer naar uw verdieping en u kunt alle apparaten zien die eraan zijn toegewezen - WLC en AP's:



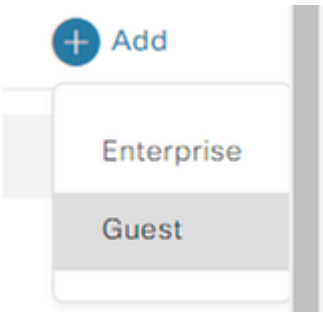

Apparaten toegewezen aan de site

## SSID maken

Stap 1. Navigeer naar Ontwerp > Netwerkinstellingen > Draadloos > Globaal en voeg een SSID toe:

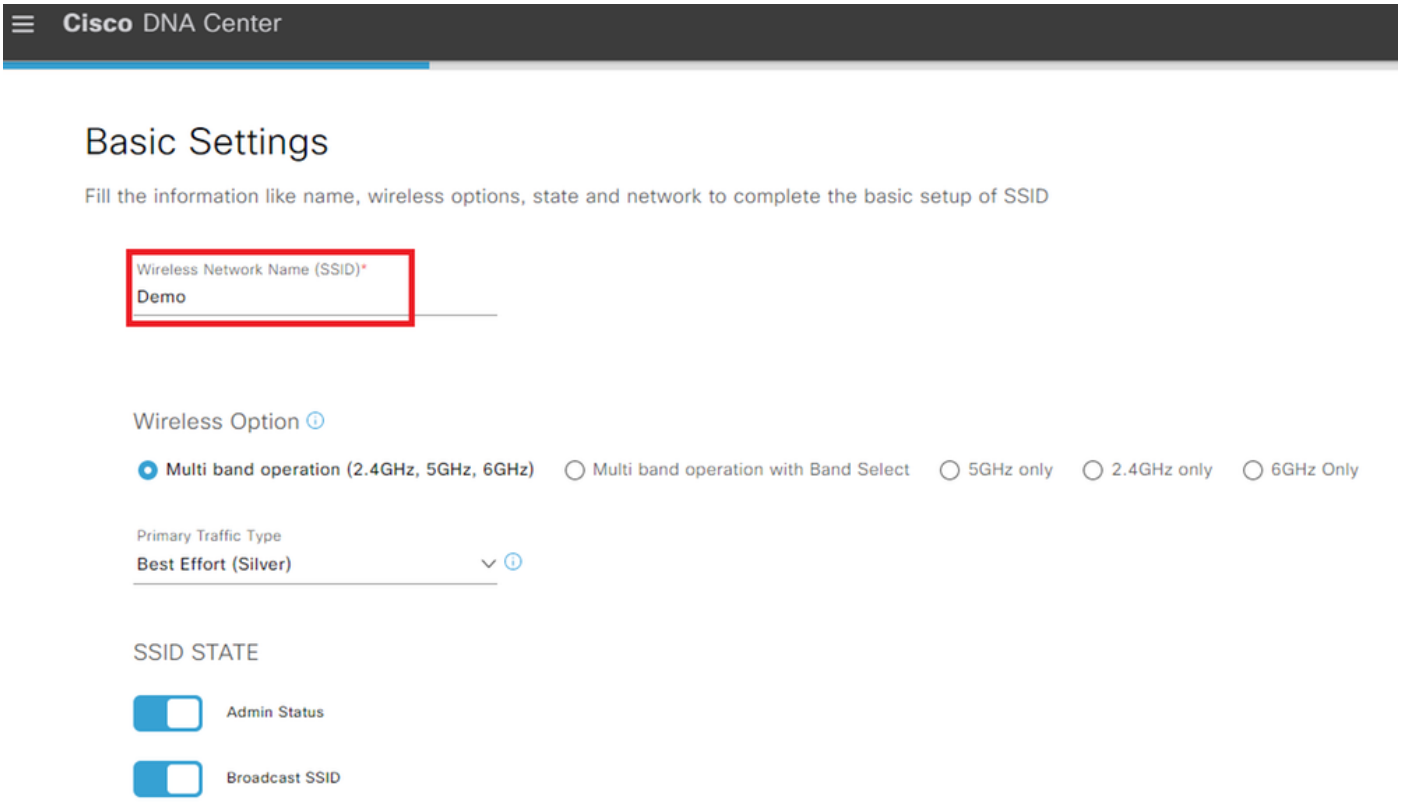

SSID maken

U kunt een Enterprise-SSID of een gast-SSID maken. In deze demo wordt een gast-SSID gemaakt:

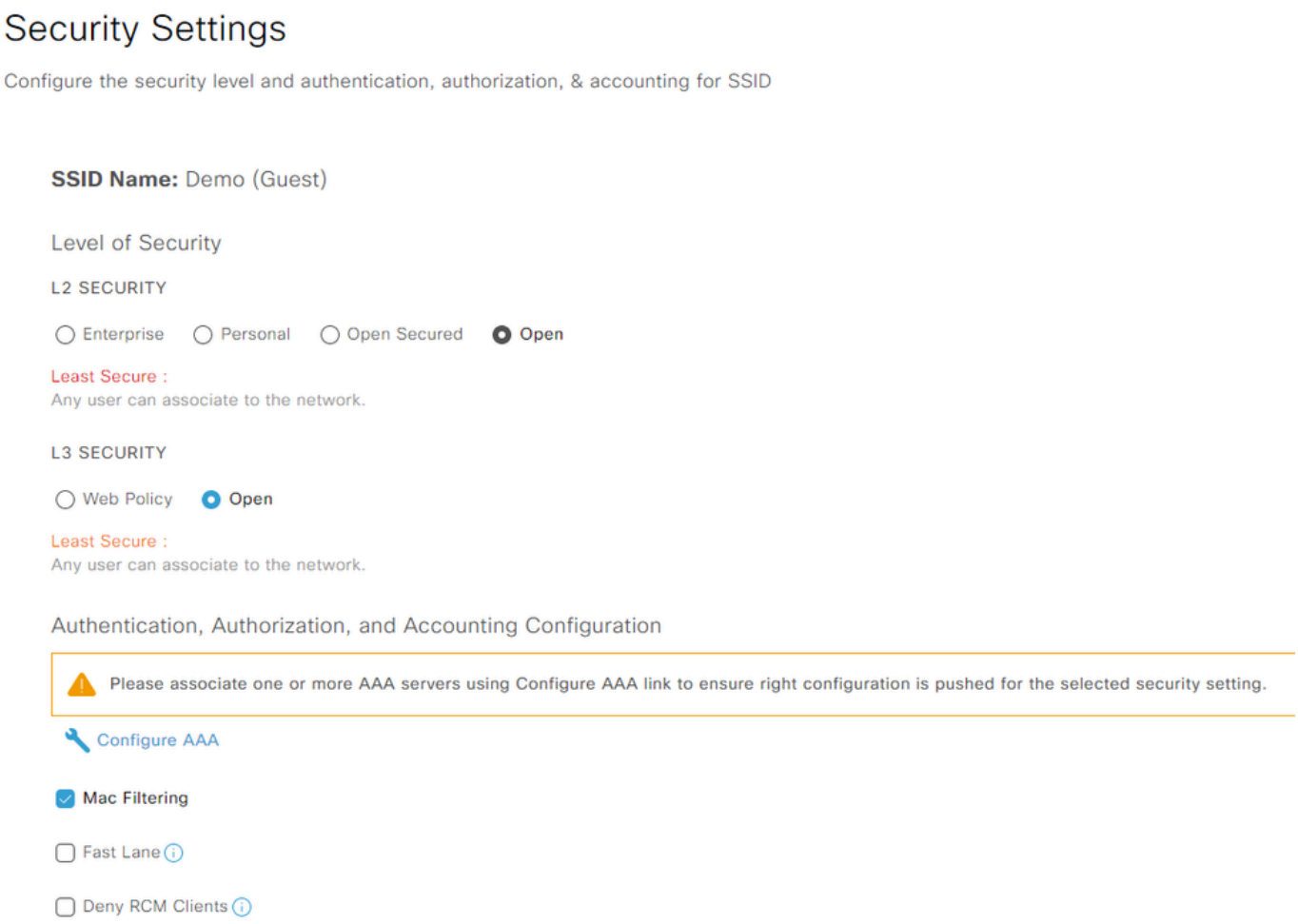



Enterprise- of gast-SSID

Stap 2. Kies de instelling die u wilt voor de SSID. In dit geval wordt een open SSID gemaakt. De beheerdersstatus en de Broadcast-SSID moeten zijn ingeschakeld:




Basisinstellingen SSID



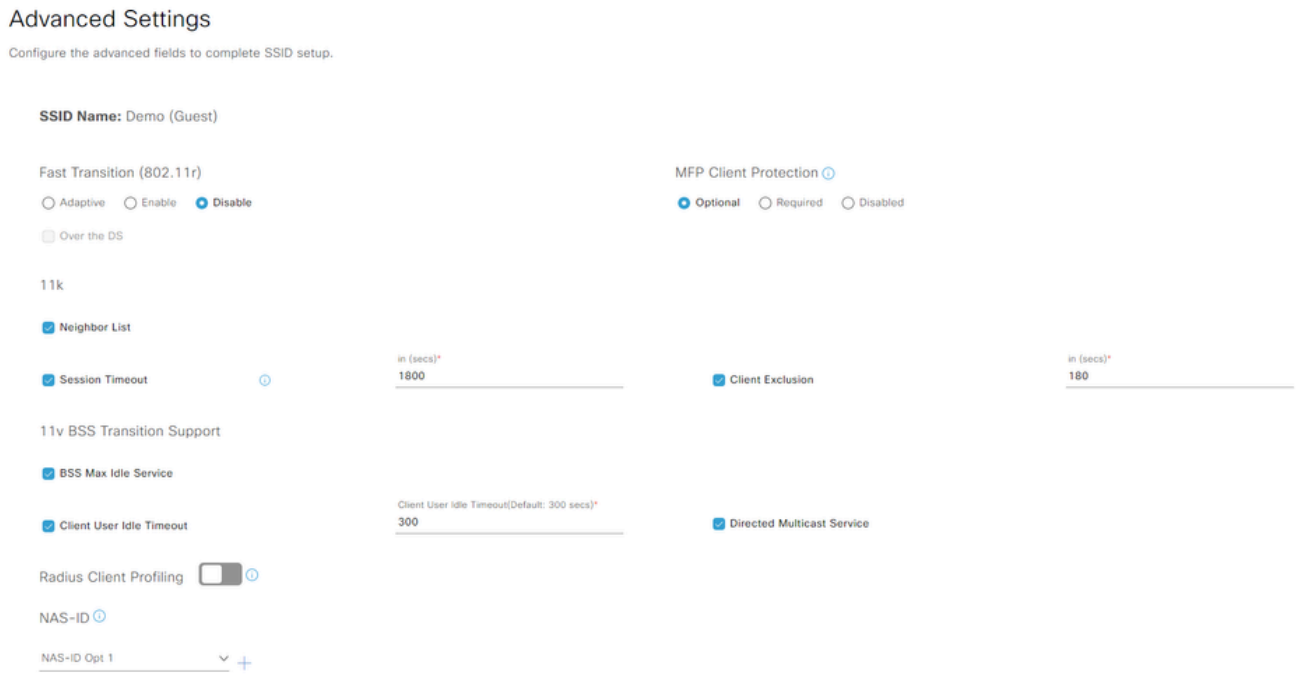

Beveiligingsinstellingen SSID

---

⚠ Let op: vergeet niet om de AAA-server voor de SSID te configureren en te koppelen. De standaardmethodenlijst wordt toegewezen als er geen AAA-servers zijn geconfigureerd.

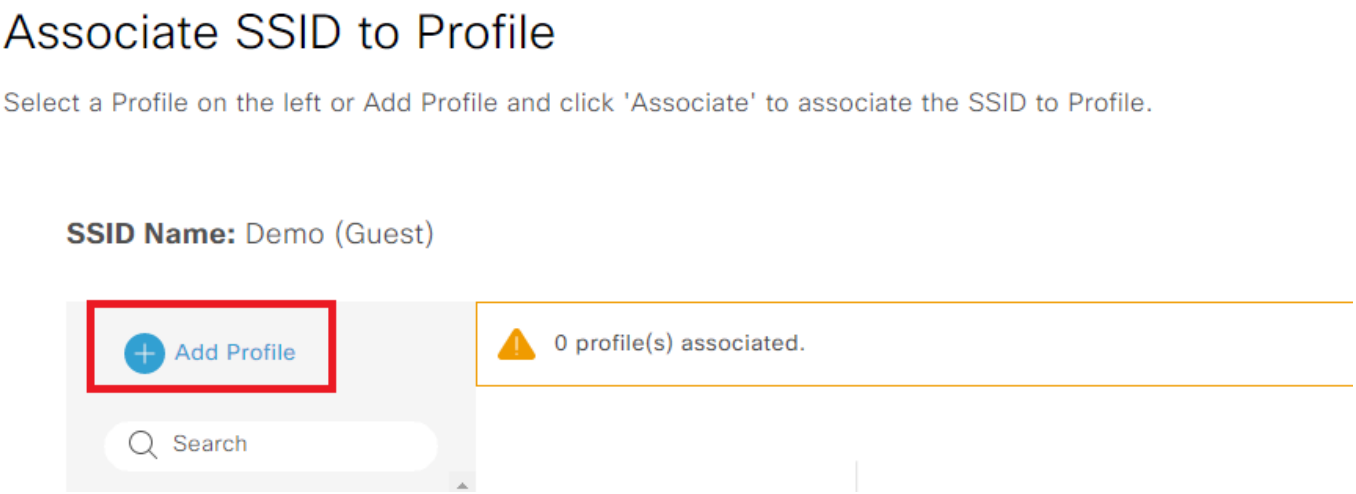
---

Wanneer u op volgende klikt, ziet u geavanceerde instellingen voor uw SSID:



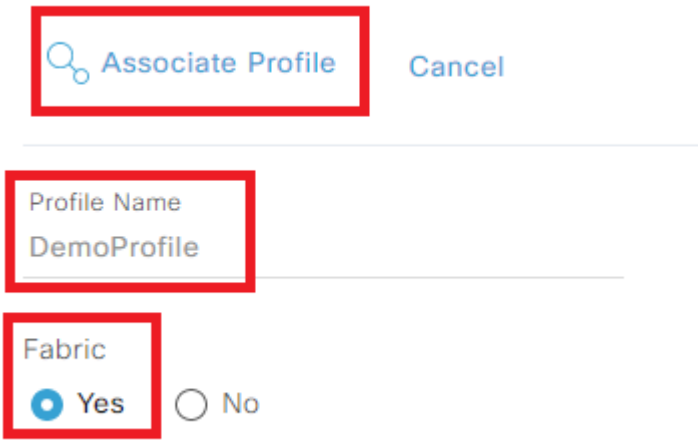

Geavanceerde SSID-instellingen

Stap 3. Nadat de SSID is gemaakt, moet u deze koppelen aan een profiel. Klik op Profiel toevoegen:




Profiel toevoegen

Stap 4. Geef een naam aan het profiel, selecteer Verbinding en klik aan het einde op Profiel koppelen:




Associatieprofiel

U krijgt een overzicht van de SSID en het profiel dat u hebt gemaakt:

# 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) |

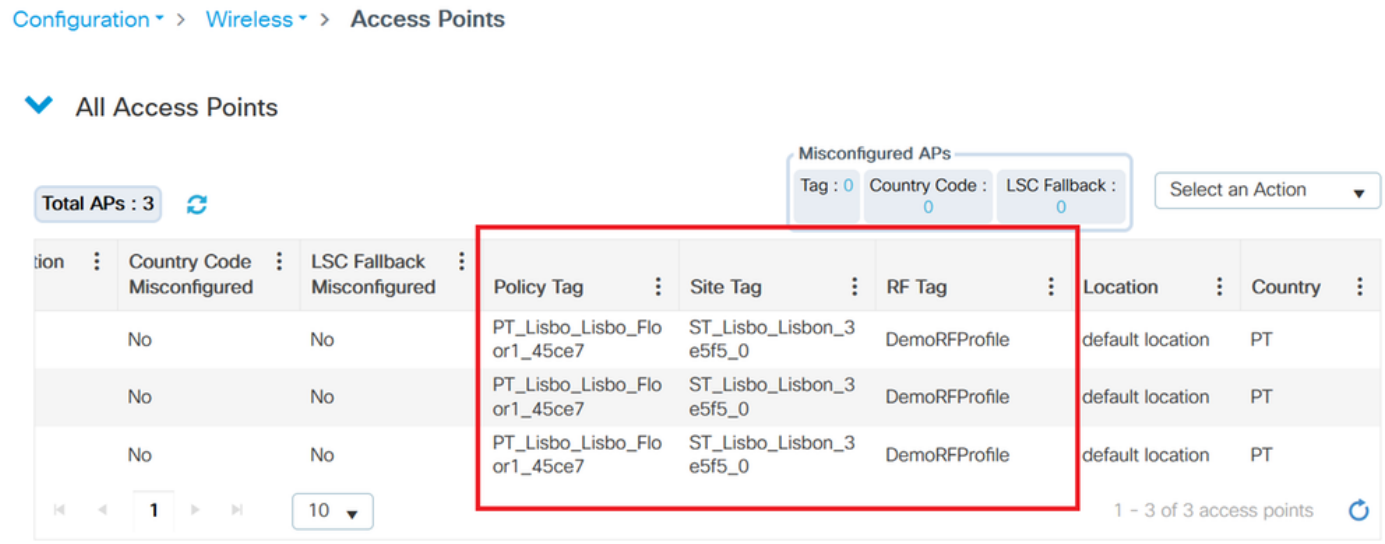
SSID-overzicht

Stap 5. Een nieuw netwerkprofiel configureren

: bij het inrichten van de toegangspunten, die al deel uitmaken van de geconfigureerde vloer voor het geselecteerde RF-profiel, moeten deze worden verwerkt en opnieuw worden opgestart.

De toegangspunten zijn nu voorzien.

Stap 6. Navigeer aan de WLC-kant naar Configuratie > Draadloos > Toegangspunten. Controleer of de AP-tags zijn gepusht vanuit Cisco DNA:



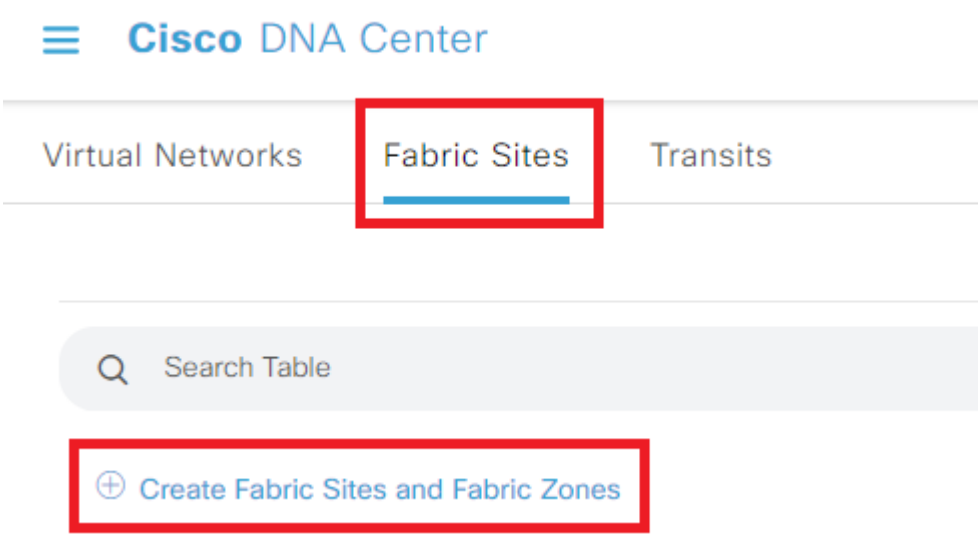

Tags op AP's

Stap 7. Navigeer naar Configuratie > Tags en profielen > WLAN's en controleer of de SSID vanuit Cisco DNA is gepusht:


WLAN

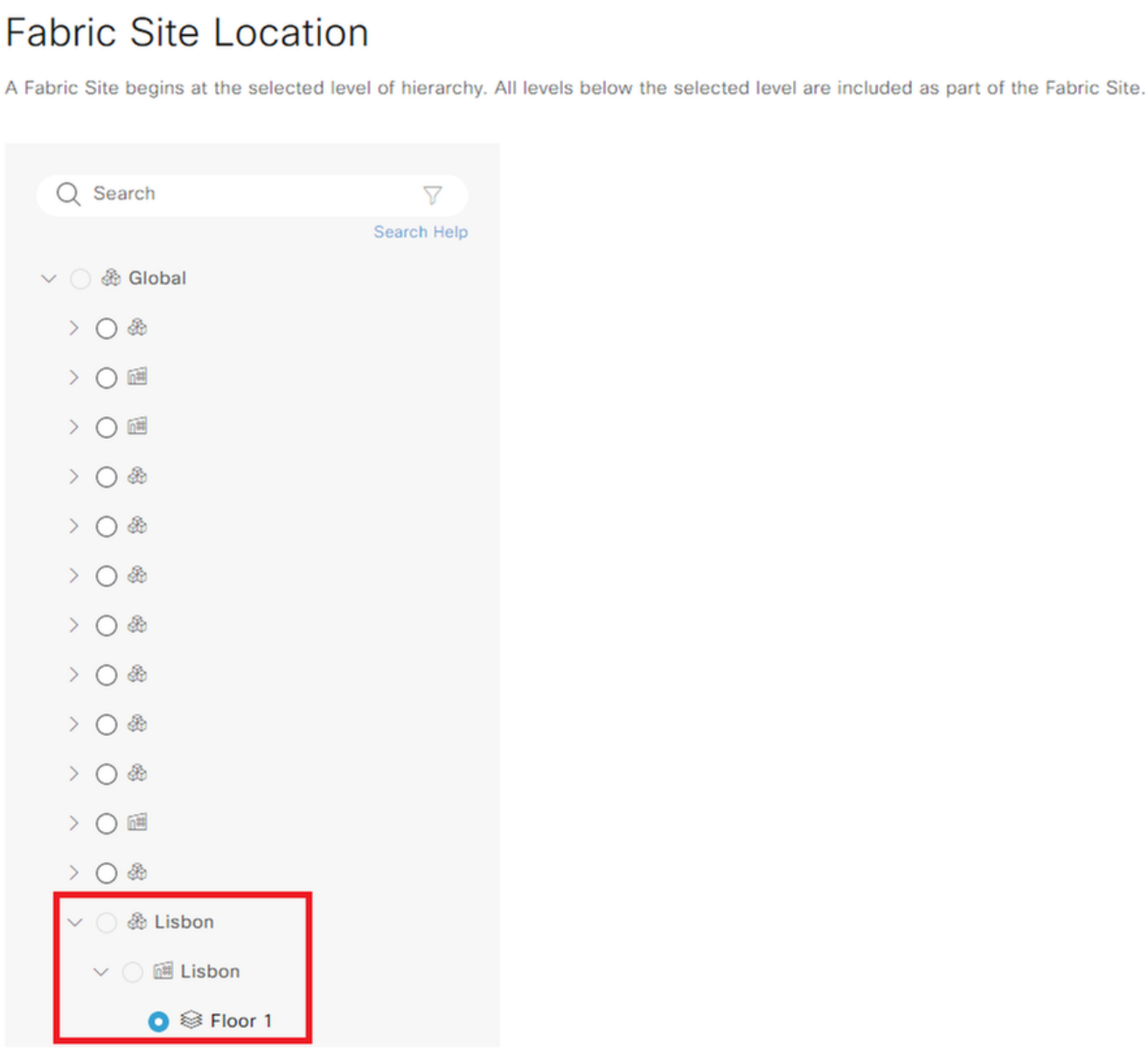
## Fabric-site maken

Stap 1. Navigeer naar Voorzieningen > Fabric Sites. Een fabric-site maken:



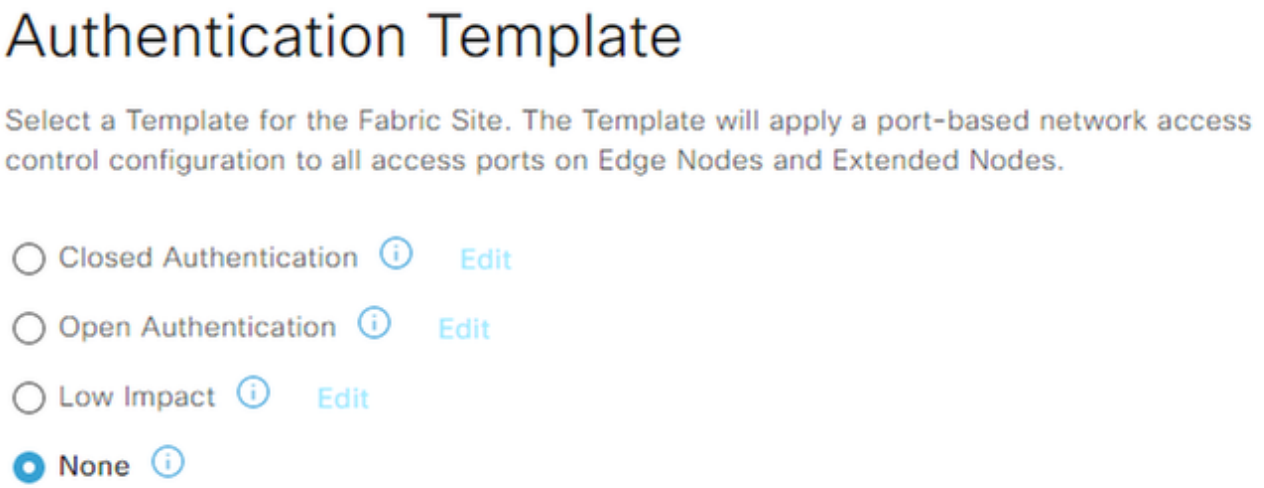

Fabric-sites maken

Stap 2. Selecteer het gebouw/de vloer voor uw stoffensite:



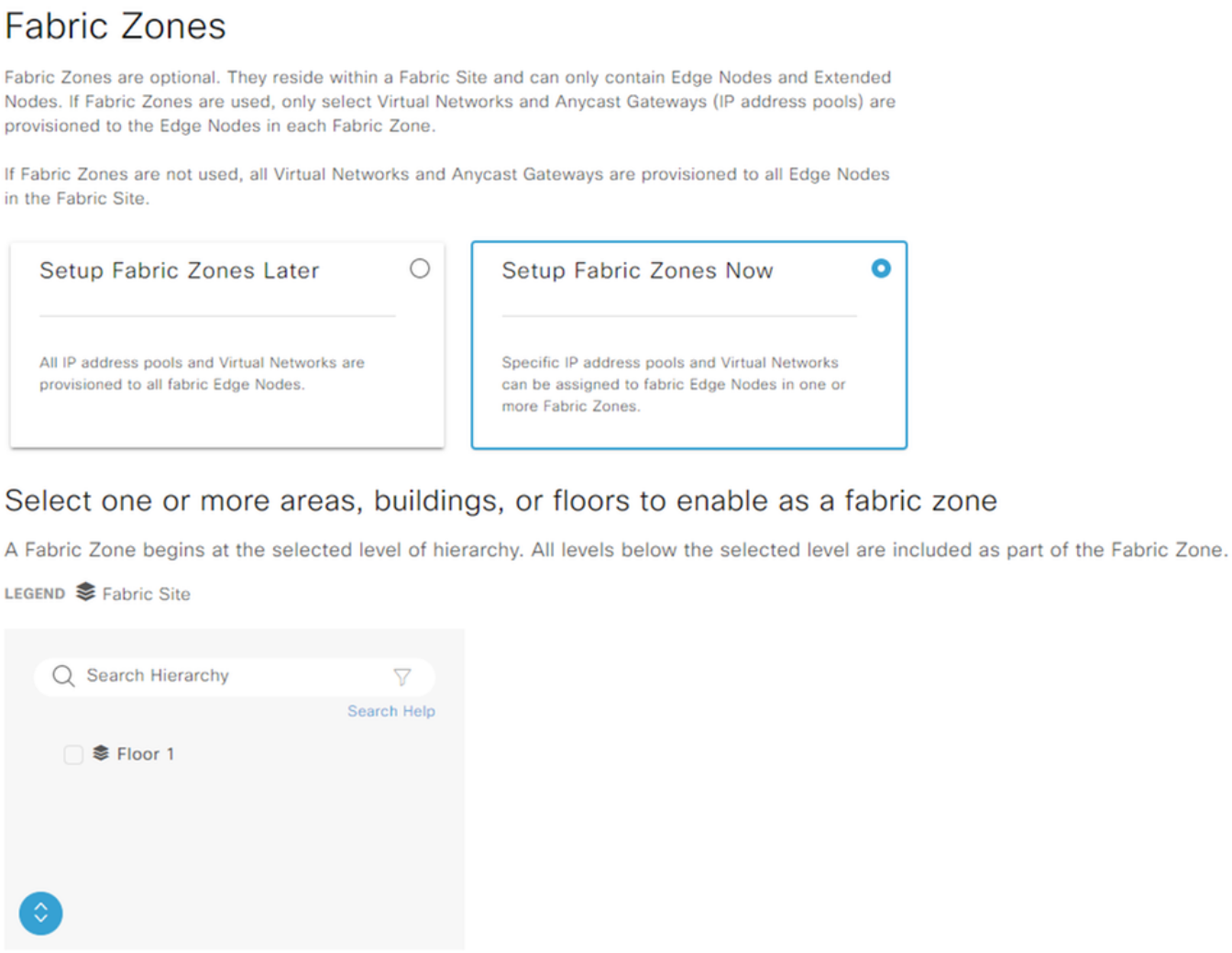
Fabric-site selecteren

Stap 3. Selecteer een verificatie-sjabloon. In deze demo werd Geen toegepast:



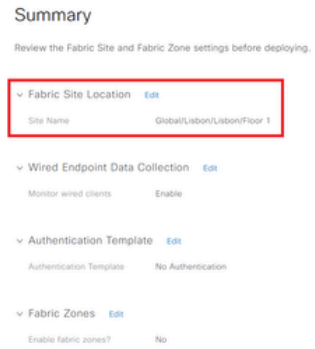

Authenticatiesjabloon

Stap 3. U kunt kiezen of u de fabric zone nu of later wilt instellen:



Fabric Zones instellen

Stap 4. Controleer de instellingen van uw stoffenzone. Als alles goed is, selecteert u Implementeren:





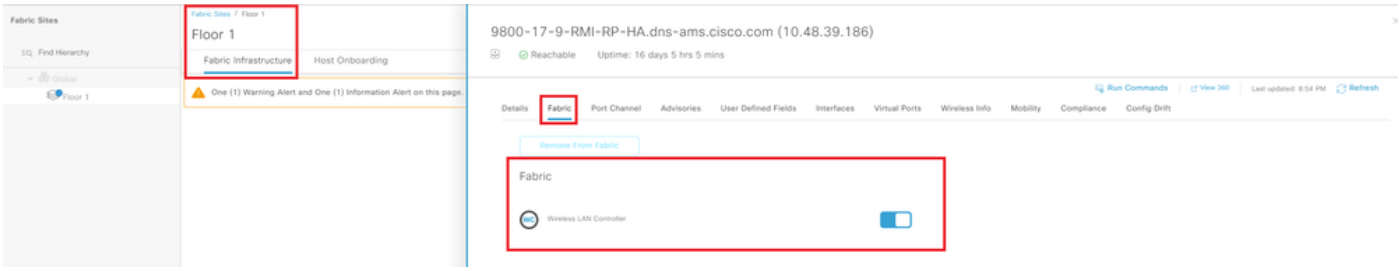
Fabric-site implementeren

U hebt een website gemaakt:


Fabric-site maken

## WLC aan weefsel toevoegen

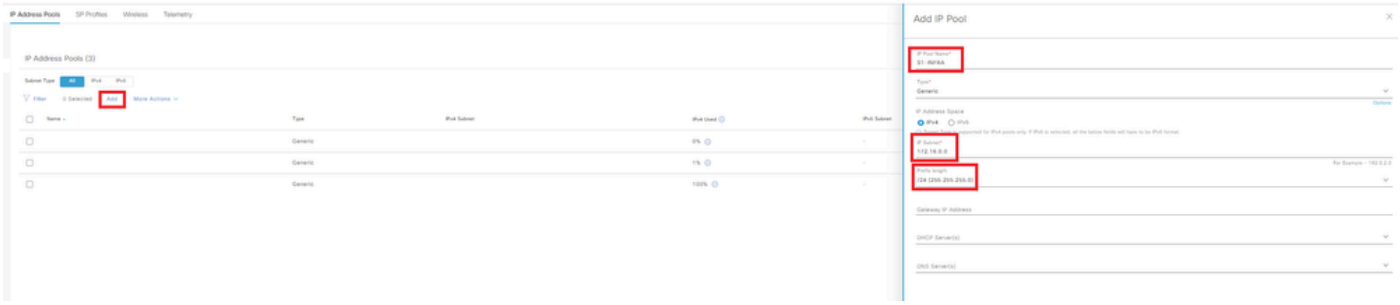
Navigeer naar Provision > Fabric Sites en selecteer uw Fabric-site. Klik boven aan je WLC en navigeer naar het tabblad Fabric. Schakel fabric in voor de WLC en selecteer Toevoegen:




WLC aan weefsel toevoegen

## AP Join

Stap 1. Ga naar Ontwerp > Netwerkinstellingen > IP-adresgroepen. Maak een IP-adressengroep aan.



IP-adresgroep

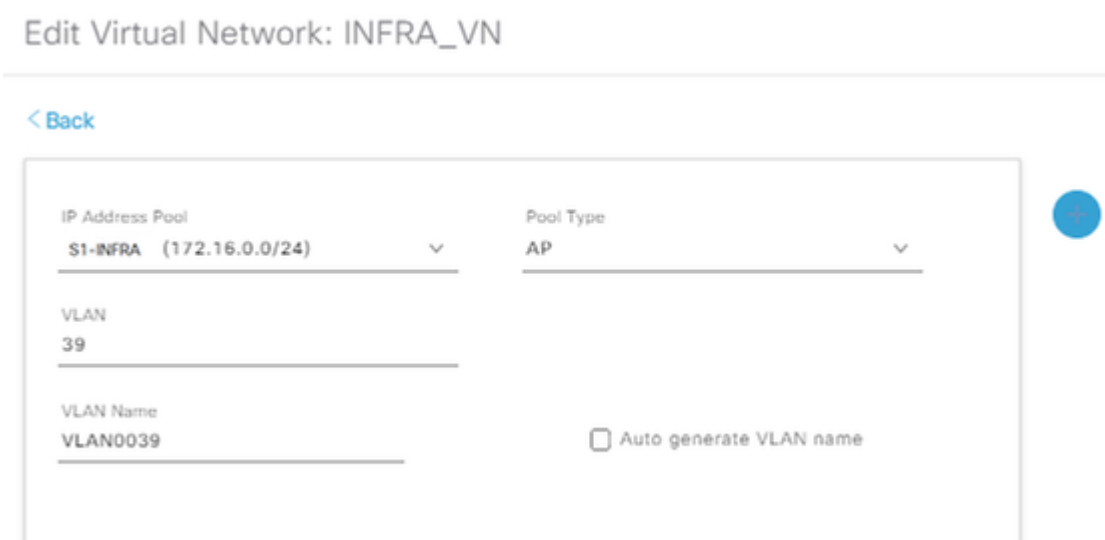
Stap 2. Navigeer naar Provision > Fabric Sites en selecteer uw Fabric-site. Navigeer naar Host Onboarding > Virtuele netwerken.

INFRA_VN wordt geïntroduceerd om eenvoudig AP's aan boord te hebben. AP's bevinden zich in de Fabric-overlay, maar INFRA_VN is toegewezen aan de globale routeringstabel. Alleen toegangspunten en uitgebreide knooppunten kunnen tot INFRA_VN behoren. Layer 2 Extension wordt automatisch ingeschakeld en L2 LISP-service wordt ingeschakeld.

Selecteer INFRA_VN > Toevoegen:

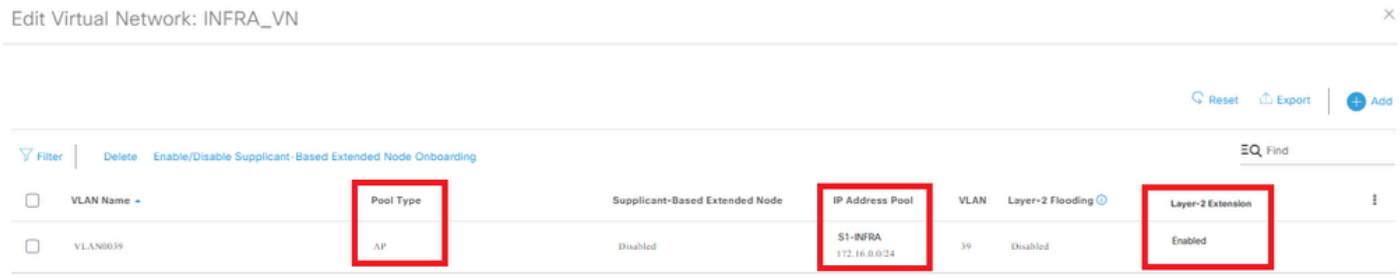
Virtueel netwerk bewerken

Stap 3. Voeg een IP-adresgroep toe met groepstype als toegangspunt:



Virtueel netwerk S1-INFRA bewerken

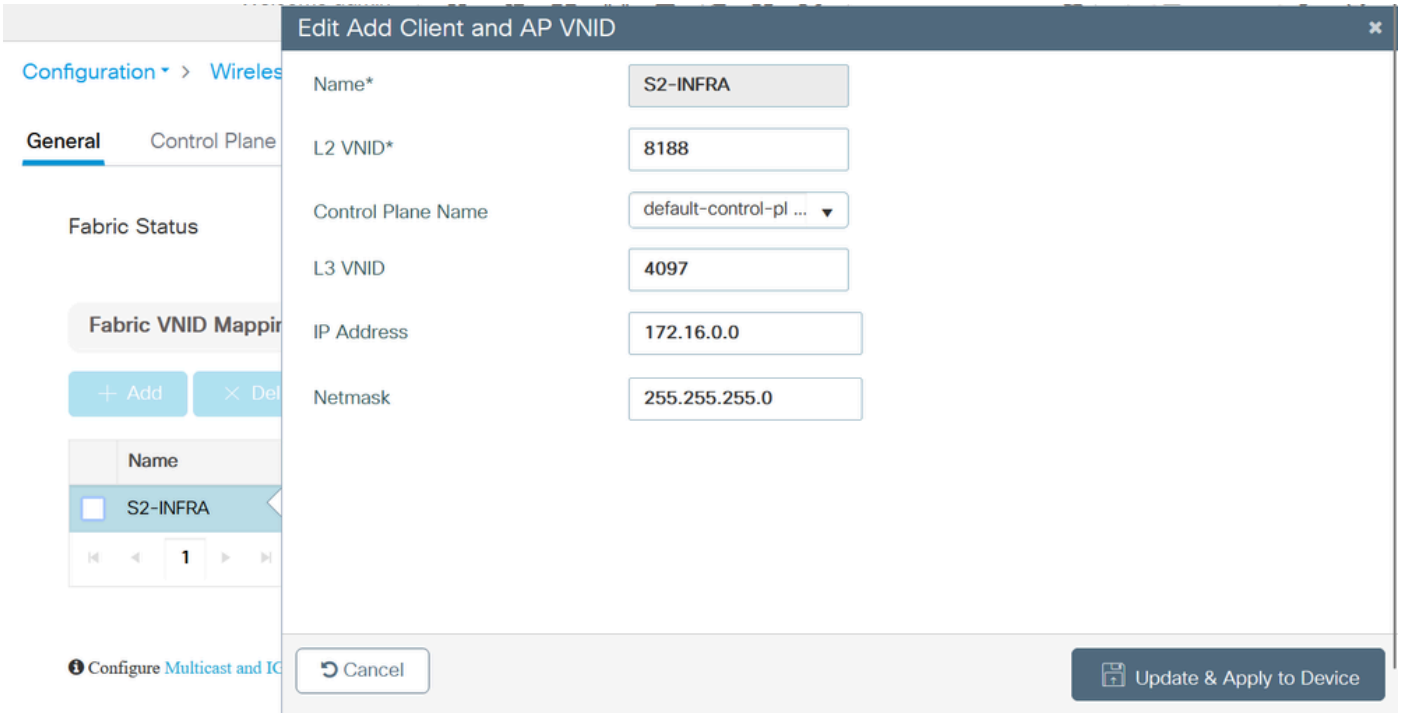
Stap 4. Controleer of de Layer-2-extensie is ingeschakeld.




Virtueel netwerk bewerken

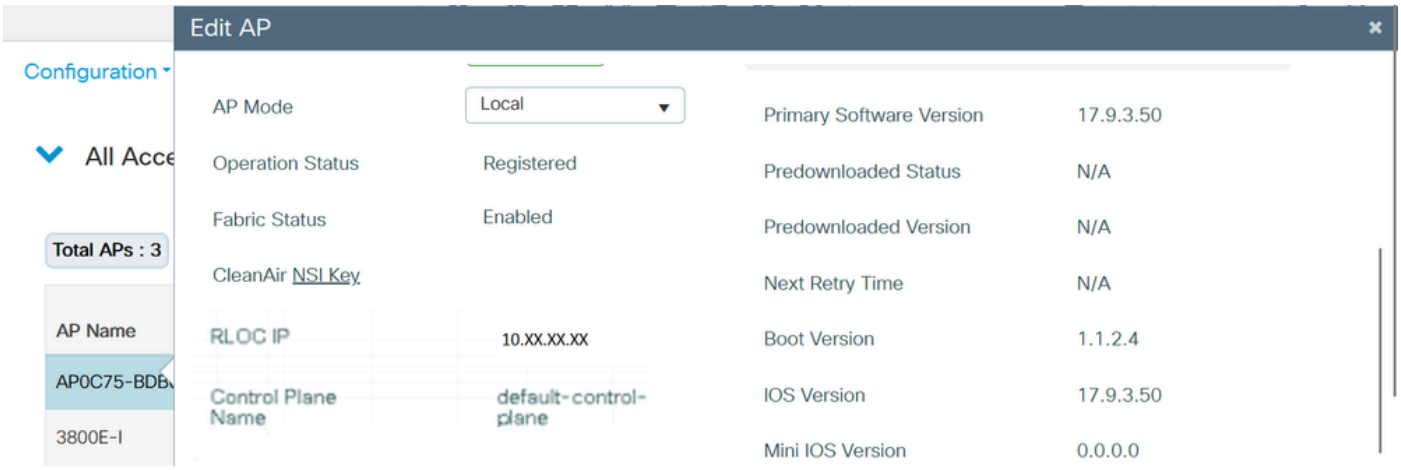
Met Pool Type = AP en Layer-2-extensie naar ON maakt Cisco DNA verbinding met de WLC en stelt de Fabric-interface in op VN_ID-toewijzing voor het AP-subnet voor zowel L2 als L3 VN_ID's.

Stap 5. Navigeer aan de kant van de WLC GUI naar Configuratie > Draadloos > Verbinding > Algemeen. Een nieuwe client en AP VN_ID toevoegen:




Nieuwe client en AP VN_ID toevoegen

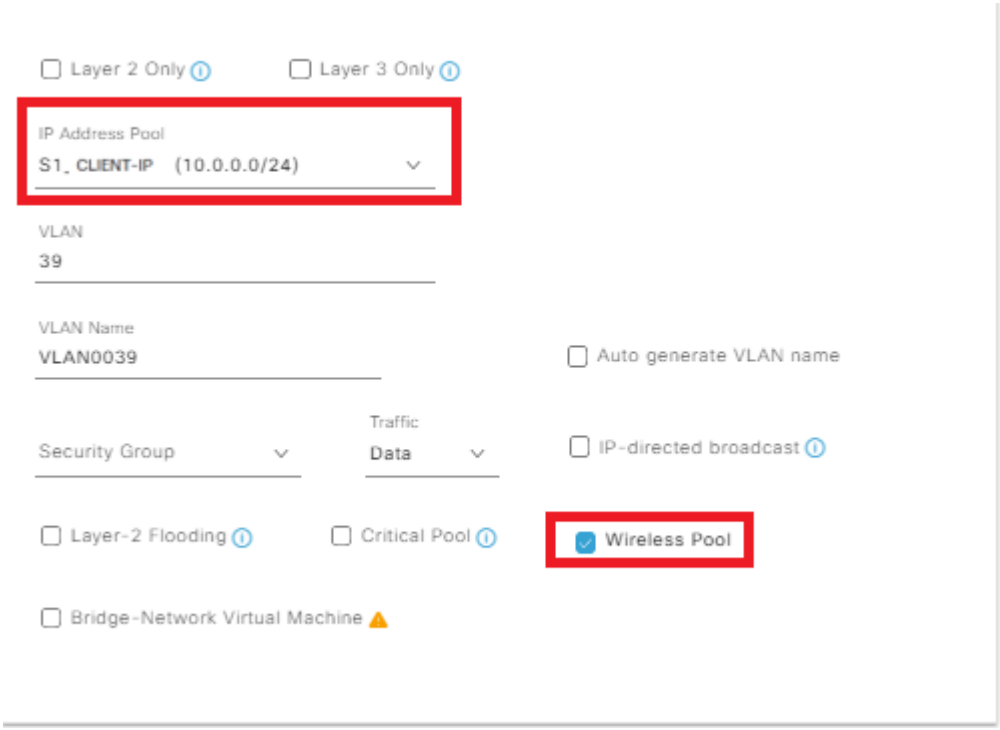
Stap 6. Ga naar Configuratie > Draadloos > Toegangspunten. Selecteer één toegangspunt in de lijst. Controleer of de verbindingsstatus is ingeschakeld, het IP-adres van het controlevlak en de naam van het controlevlak:




Fabric-status van toegangspunt controleren

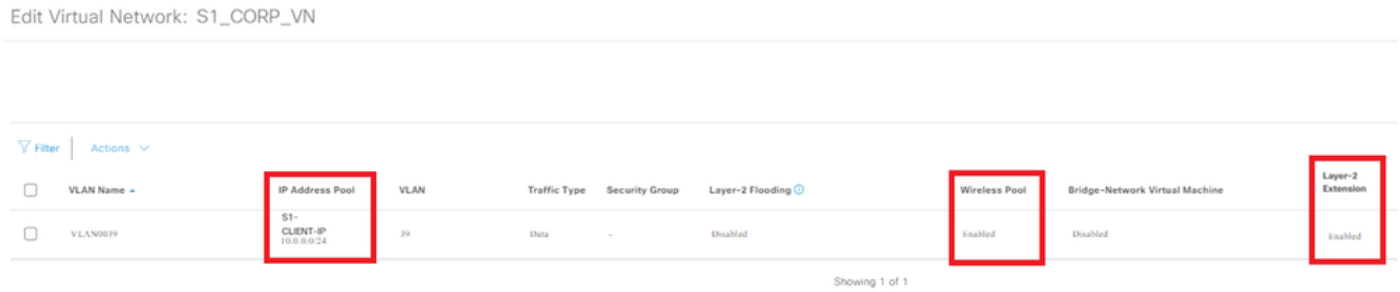
## Client aan boord

Stap 1. Voeg de pool toe aan het virtuele netwerk en controleer of de schakelaar Layer-2-extensie is ingeschakeld om de L2 LISP- en Layer 2-subnetextensie in te schakelen op de clientpool/het subnet. In Cisco DNA 1.3.x kunt u het niet uitschakelen.




IP-adresgroep toevoegen

Stap 2. Controleer of de Layer-2-extensie en de draadloze pool zijn ingeschakeld.



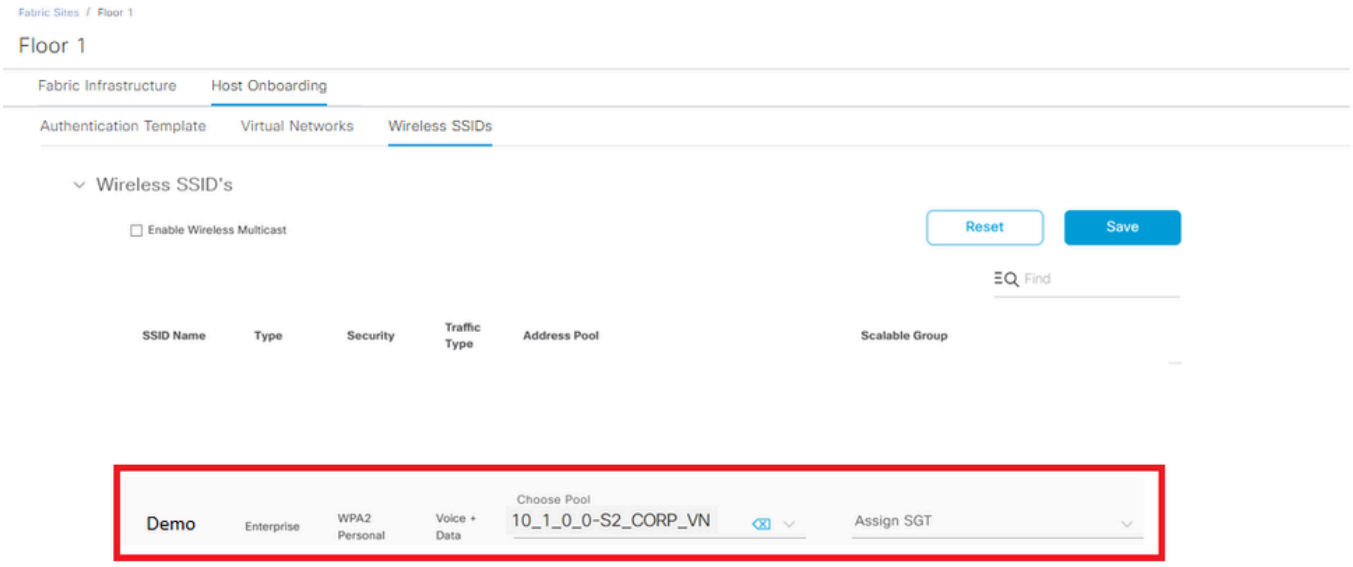

Virtueel netwerk bewerken

Stap 3. Navigeer aan de kant van de WLC GUI naar Configuratie > Draadloos > Verbinding > Algemeen. Voeg een nieuwe client en AP VN_ID toe.

Wanneer de pool is toegewezen aan het virtuele netwerk, wordt de corresponderende verbindingsinterface met VNID-toewijzing naar de controller geduwd. Dit zijn allemaal L2 VNID.


Nieuwe client en AP VN_ID toevoegen

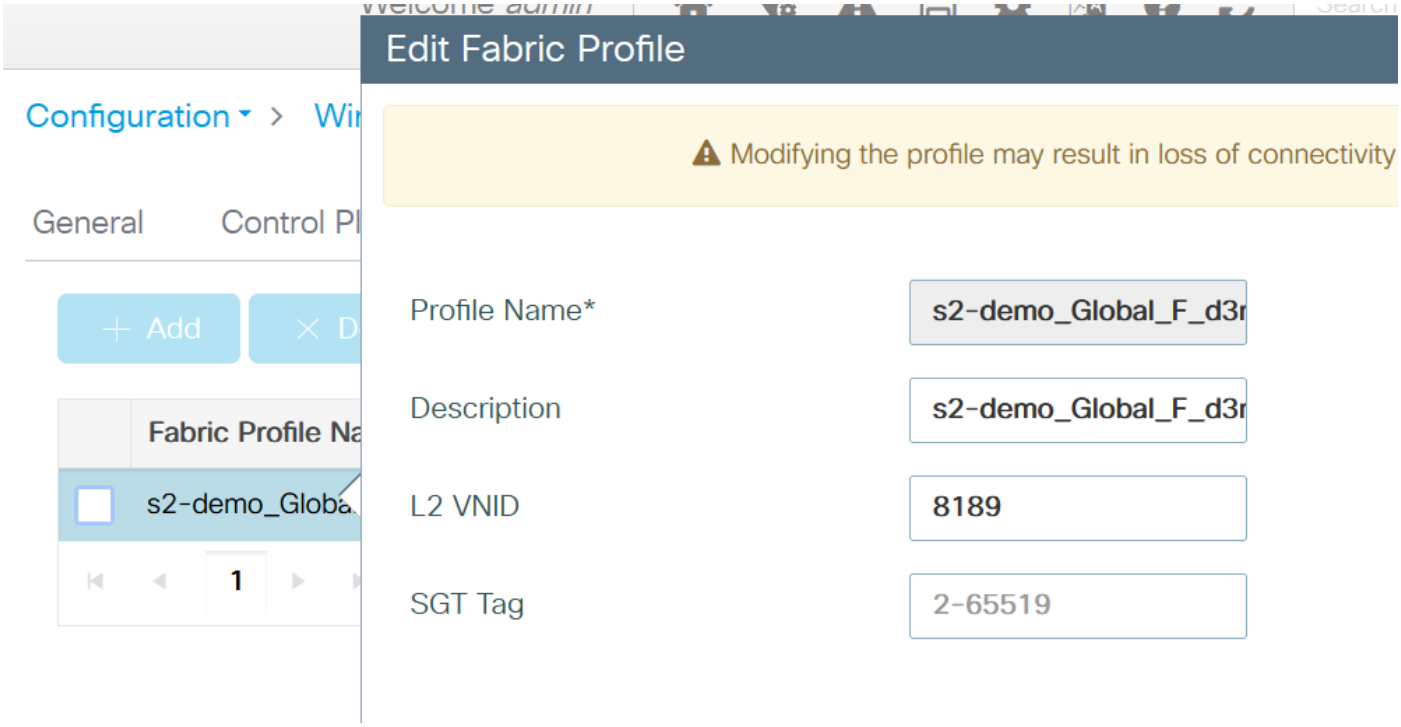
Stap 4. SSID's worden toegewezen aan de pool in de respectievelijke virtuele netwerken:




Toegewezen SSID's

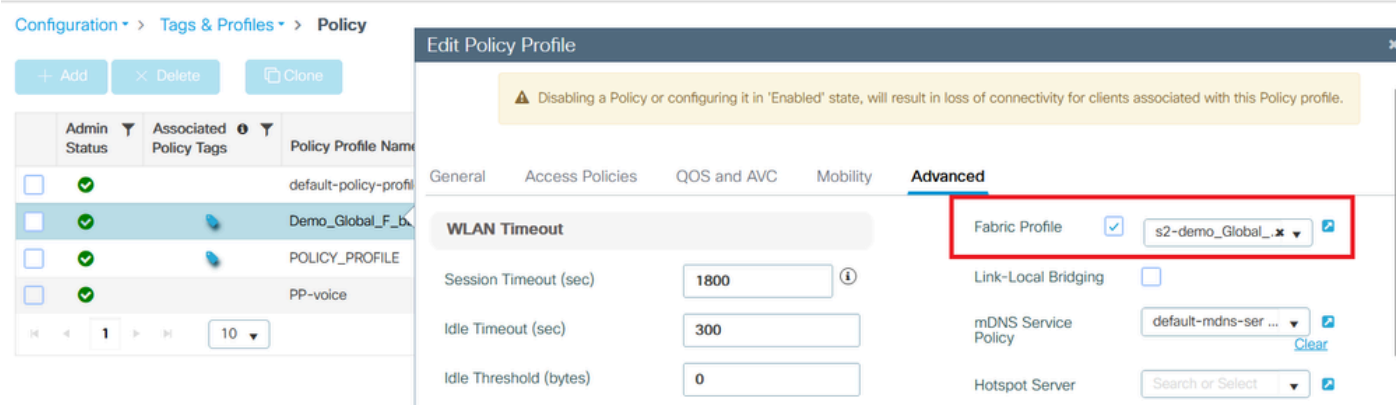
Stap 5. Een verbindingsprofiel met de L2 VNID wordt toegevoegd aan de gekozen groep en het beleidsprofiel wordt toegewezen aan het verbindingsprofiel.

Navigeer aan de kant van de WLC GUI naar Configuratie > Draadloos > Verbinding > Profielen.




Verbindingsprofiel

Stap 6. Navigeer naar Configuratie > Tags en profielen > Beleid. Controleer het structuurprofiel dat is toegewezen aan het beleidsprofiel:




Verbindingsprofiel geconfigureerd in het beleid

# Verifiëren

## Fabric-configuratie controleren op WLC en Cisco DNA

Op de WLC CLI:

WLC1# show tech

WLC1# toon draadloze technologie

Configuratie controlevlak:

routerlisp

locator-tabelstandaard

locator-set WLC

172.16.201.202

exit-locator-set

Ja!

passief-open WLC-kaartsessie-server

Site_UCI

beschrijving map-server geconfigureerd vanuit Cisco DNA-Center

verificatiesleutel 7 <sleutel>

CB1-S1#sh lisp-sessie

Sessies voor standaard VRF, totaal: 9, vastgesteld: 5

Peer-status Omhoog/Omlaag In/Uit

172.16.201.202:4342 Up 3d07h 14/14

WLC-configuratie:

draadloze verbinding

wireless fabric control-plane default-control-plane

IP-adres 172.16.2.2 sleutel 0 47AA5A

WLC1# overzicht fabric map-server weergeven

Status MS-IP-verbinding

---

172.16.1.2 OMHOOG

WLC1# overzicht van draadloze verbindingen weergeven

Fabric-status: ingeschakeld

Controlevlak:

Naam IP-adres Sleutelstatus

---

default-control-plane 172.16.2.2 47aa5a Omhoog

Navigeer in de WLC GUI naar Configuratie > Draadloos > Stabiel en controleer of de verbindingsstatus is ingeschakeld.

Ga naar Configuratie > Draadloos > Toegangspunten. Selecteer één toegangspunt in de lijst. Controleer of de verbindingsstatus is ingeschakeld.

Navigeer in Cisco DNA naar Provision > Fabric Sites en controleer of u een Fabric-site hebt. Navigeer op die fabric-site naar Fabric Infrastructure > Fabric en controleer of de WLC is ingeschakeld als fabric.

# Problemen oplossen

## Client krijgt geen IP-adres

Stap 1. Controleer of de SSID is gemaakt. Navigeer in WLC GUI naar Configuratie > Tags en profielen > Beleid. Selecteer het beleid en navigeer naar Geavanceerd. Controleer of het verbindingsprofiel is ingeschakeld.

Stap 2. Controleer of de client vastzit in de IP-leerstatus. Navigeer in WLC GUI naar Monitoring > Wireless > Clients. Controleer de status van de client.

Stap 3. Controleer of het beleid DHCP vereist.

Stap 4. Als het verkeer lokaal wordt geschakeld tussen AP - edge node, verzamelt u AP-logs (client-trace) voor de clientverbinding. Controleer of de DHCP-detectie is doorgestuurd. Als er geen DHCP-aanbieding binnenkomt, is er iets mis op de edge-node. Als de DHCP niet wordt doorgestuurd, is er iets mis op het toegangspunt.

Stap 5. U kunt een EPC verzamelen op de edge node-poort om de DHCP-detectiepakketten te zien. Als u de DHCP-detectiepakketten niet ziet, bevindt het probleem zich op het toegangspunt.

### SSID wordt niet uitgezonden

Stap 1. Controleer of de AP-radio's zijn uitgeschakeld.

Stap 2. Controleer of het WLAN is ingeschakeld en de SSID van de uitzending is ingeschakeld.

Stap 3. Controleer de configuratie van het toegangspunt als de verbinding van het toegangspunt is ingeschakeld. Navigeer naar Configuratie > Draadloos > Toegangspunten, selecteer één toegangspunt en op het tabblad Algemeen ziet u Fabric Status Ingeschakeld en de RLOC-informatie.

Stap 4. Navigeer naar Configuratie > Draadloos > Verbinding > Controlevlak. Controleer of het controlevlak is geconfigureerd (met het IP-adres).

Stap 5. Navigeer naar Configuratie > Tags en profielen > Beleid. Selecteer het beleid en navigeer naar Geavanceerd. Controleer of het verbindingsprofiel is ingeschakeld.

Stap 6. Navigeer naar Cisco DNA en herhaal de stappen voor het maken van SSID en WLC. Het Cisco-DNA moet de SSID opnieuw naar de WLC pushen.

## Gerelateerde informatie

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.