Implementierung von Software-Defined Access für Wireless-Netzwerke mit DNA

Inhalt

Einleitung

In diesem Dokument wird die Implementierung von SDA für Wireless-Technologie im Zusammenhang mit Fabric-fähigem WLC und der Zugriff auf LAP über Cisco DNA beschrieben..

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der 9800 Wireless LAN Controller (WLC)
- Lightweight Access Points (LAP)
- Cisco DNA

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 9800-CL WLC Cisco IOS® XE, Version 17.9.3
- Cisco Access Points: 9130AX, 3802E, 1832I
- Cisco DNA Version 2.3.3.7

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

SD-Access

Mit Software-Defined Access werden Sicherheitsrichtlinien im gesamten Netzwerk mit dynamischen Regeln und automatisierter Segmentierung eingerichtet und automatisch durchgesetzt. Endbenutzer können so steuern und konfigurieren, wie die Benutzer eine Verbindung mit ihrem Netzwerk herstellen. SD-Access stellt für alle verbundenen Endgeräte eine anfängliche Vertrauensstufe her und überwacht diese kontinuierlich, um die Vertrauensstufe erneut zu überprüfen. Wenn sich ein Endgerät nicht normal verhält oder eine Bedrohung erkannt wird, kann der Endbenutzer sofort eindämmen und Maßnahmen ergreifen, bevor eine Sicherheitsverletzung stattfindet, das Geschäftsrisiko verringert und die Ressourcen schützt. Vollständig integrierte Lösung, einfache Bereitstellung und Konfiguration in neuen und bereitgestellten Netzwerken

SD-Access ist eine Technologie von Cisco, die eine Weiterentwicklung des traditionellen Campus-Netzwerks darstellt und absichtsbasierte Netzwerkfunktionen (IBN) sowie eine zentrale Richtlinienkontrolle unter Verwendung von SDN-Komponenten (Software-Defined Networking) bietet.

Die drei netzwerkzentrierten Grundpfeiler von SD-Access:

1. Eine Netzwerkstruktur: Es ist eine Abstraktion des Netzwerks, die programmierbare

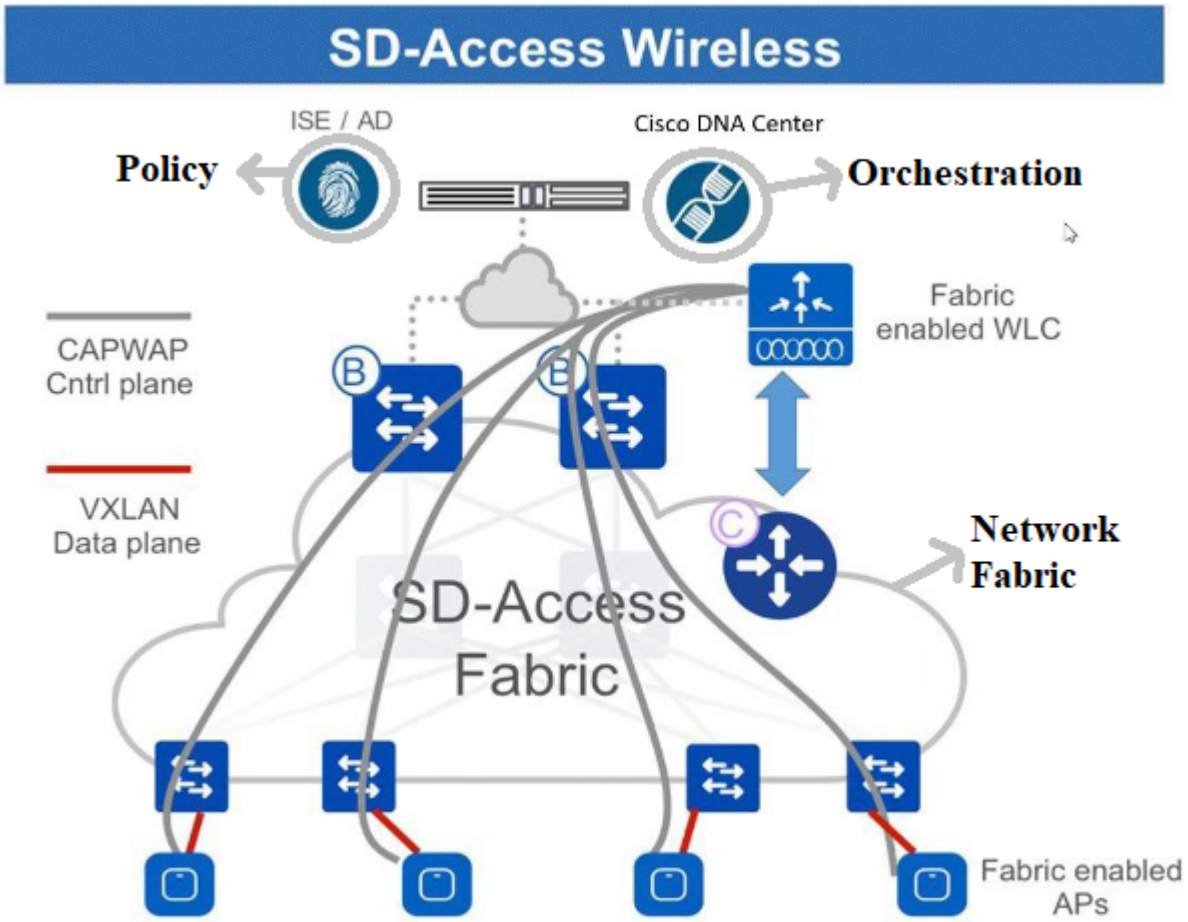
Overlays und Virtualisierung unterstützt. Die Netzwerk-Fabric unterstützt sowohl kabelgebundenen als auch Wireless-Zugriff und ermöglicht das Hosting mehrerer logischer Netzwerke, die voneinander segmentiert und nach Geschäftszweck definiert sind.

2. Orchestrierung: Cisco DNA ist die Orchestrierungs-Engine von SDA. Cisco DNA funktioniert wie ein SDN Controller. Sie implementiert Richtlinien und Konfigurationsänderungen in der Fabric. Darüber hinaus enthält es ein Tool, das das Netzwerkdesign unterstützt und über DNA Assurance Netzwerktelemetrie- und Leistungsanalysen in Echtzeit ermöglicht. Die Rolle der Cisco DNA besteht in der Orchestrierung der Netzwerk-Fabric zur Bereitstellung von Richtlinienänderungen und Netzwerkintent für Sicherheit, Quality of Service (QoS) und Mikrosegmentierung.
3. Richtlinie: Identity Services Engine (ISE) ist das Tool, das Netzwerkrichtlinien definiert. Die ISE organisiert, wie Geräte und Knoten in virtuelle Netzwerke segmentiert werden. Die ISE definiert außerdem skalierbare Group Tags (SGTs), die von Zugriffsgeräten zur Segmentierung des Benutzerdatenverkehrs beim Eintritt in die Fabric verwendet werden. Die SGRs müssen die von der ISE definierte Mikrosegmentierungsrichtlinie durchsetzen.

SDA basiert auf zentraler Orchestrierung. Die Kombination aus Cisco DNA als programmierbare Orchestrierungs-Engine, ISE als Richtlinien-Engine und einer neuen Generation programmierbarer Switches macht das Fabric-System weitaus flexibler und verwaltbarer als alles andere.

Anmerkung: Dieses Dokument behandelt speziell SD-Access Wireless.

Die Netzwerk-Fabric besteht aus folgenden Elementen:

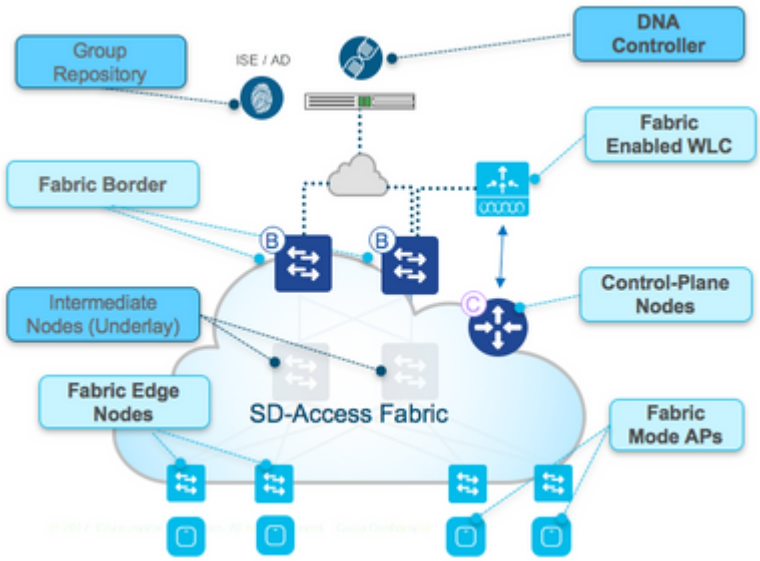


Elemente der Netzwerkstruktur

Die Wireless-Integration in die Fabric bietet u. a. folgende Vorteile für das Wireless-Netzwerk: Berücksichtigung von Vereinfachungen und Mobilität mit ausgedehnten Subnetzen über physische Standorte hinweg; und Mikrosegmentierung mit zentralisierten Richtlinien, die in der gesamten kabelgebundenen und Wireless-Domäne konsistent sind. Darüber hinaus kann der Controller Aufgaben auf der Datenebene weiterleiten, während er weiterhin als zentrale Services- und Kontrollebene für das Wireless-Netzwerk fungiert. Dadurch wird die Skalierbarkeit der Wireless-Controller sogar erhöht, da diese ähnlich wie beim FlexConnect-Modell keinen Datenverkehr auf Datenebene mehr verarbeiten müssen.

SD-Access Wireless-Architektur

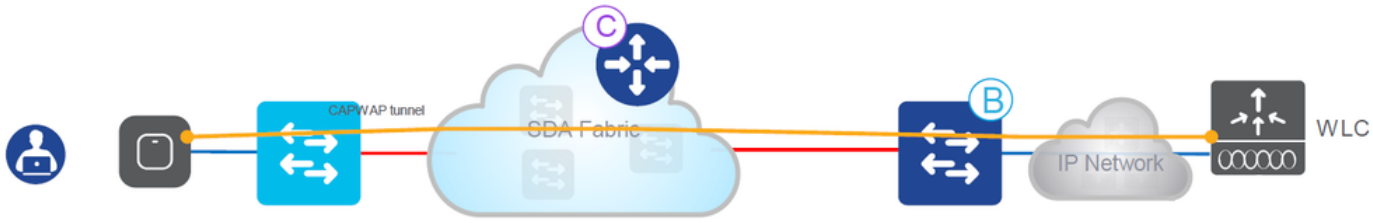
Überblick



SDA - Überblick

Es gibt zwei primäre SDA-unterstützte Wireless-Bereitstellungsmodelle:

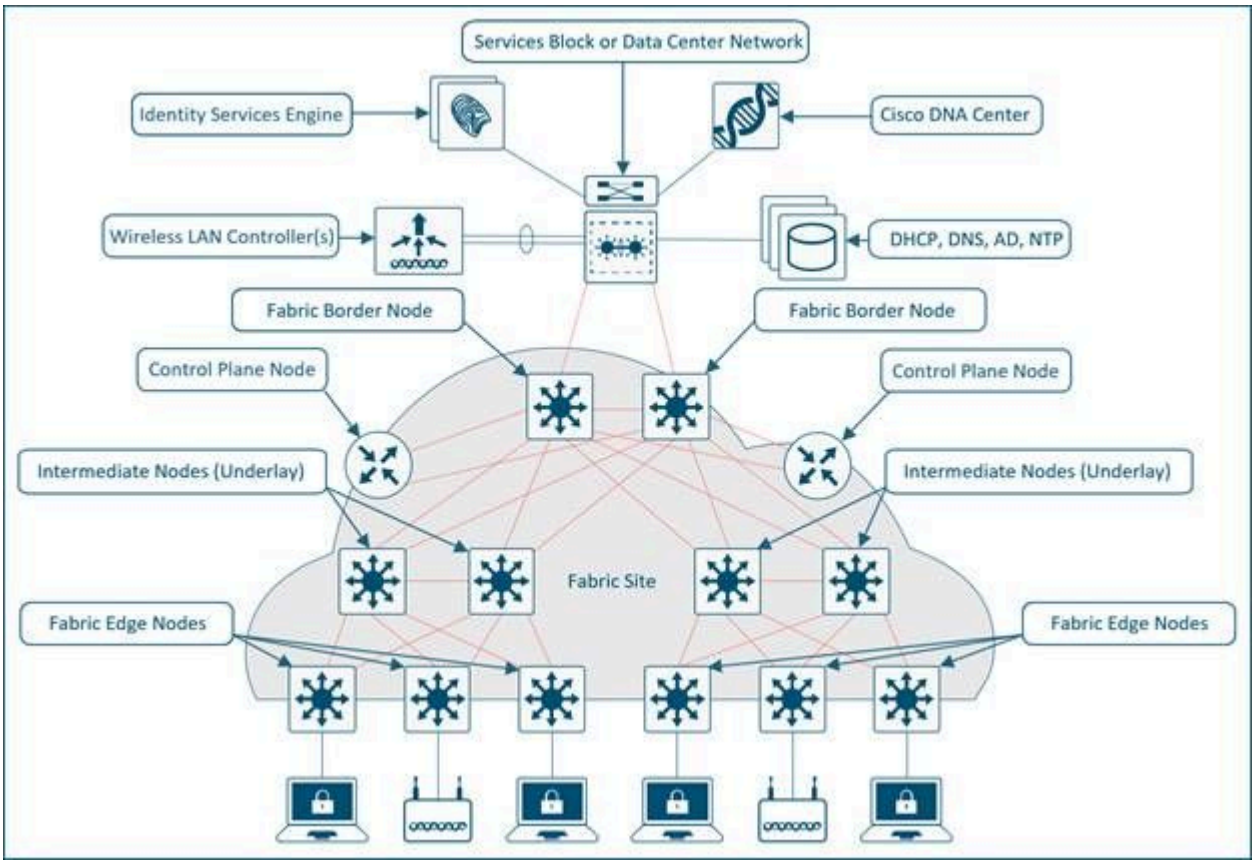
Bei der einen handelt es sich um eine OTT-Methode (Over-the-Top), eine herkömmliche CAPWAP-Bereitstellung, die mit einem kabelgebundenen Fabric-Netzwerk verbunden ist. Die SDA-Fabric transportiert den CAPWAP-Kontroll- und Datenebenenverkehr an den Wireless Controller:



Over-the-Top-Methode

Bei diesem Bereitstellungsmodell ist die SDA-Fabric ein Transportnetzwerk für Wireless-Datenverkehr (ein Modell, das häufig bei Migrationen eingesetzt wird). Der Access Point arbeitet sehr ähnlich wie der klassische lokale Modus: Sowohl die CAPWAP-Kontroll- als auch die Datenebene enden auf dem Controller, d. h. der Controller ist nicht direkt Teil der Fabric. Dieses Modell wird häufig verwendet, wenn kabelgebundene Switches zum ersten Mal in die SDA-Fabric migriert werden, das Wireless-Netzwerk jedoch noch nicht für eine vollständige Fabric-Overlay-Integration bereit ist.

Die anderen Bereitstellungsmodelle sind vollständig integrierte SDA-Modelle. Das Wireless-Netzwerk ist vollständig in die Fabric integriert und nimmt an Overlays teil. So können verschiedene WLANs Teil verschiedener virtueller Netzwerke (VNs) sein. Der Wireless Controller verwaltet nur die CAPWAP-Kontrollebene (zur Verwaltung der APs), und die CAPWAP-Datenebene kommt nicht zum Controller:



Vollständig integriertes SDA-Modell

Die Wireless-Datenebene wird ähnlich behandelt wie kabelgebundene Switches: Jeder WAP kapselt Daten in VXLAN und sendet sie an einen Fabric-Edge-Knoten, wo sie dann über das Fabric an einen anderen Edge-Knoten gesendet werden. Die Wireless-Controller müssen als Fabric-Controller konfiguriert werden, was eine Änderung gegenüber dem normalen Betrieb darstellt.

Fabric-fähige Controller kommunizieren mit der Fabric-Steuerungsebene, registrieren Layer-2-Client-MAC-Adressen und Layer-2-VNI-Informationen (Virtual Network Identifier). Die APs sind für die Kommunikation mit Wireless-Endgeräten zuständig und unterstützen die VXLAN-Datenebene durch Kapselung und Entkapselung des Datenverkehrs.

SDA-Rollen und -Terminologie

Die Netzwerk-Fabric besteht aus folgenden Elementen:

- Knoten der Kontrollebene: Hierbei handelt es sich um das Standortzuordnungssystem (Host-Datenbank), das Teil der LISP-Kontrollebene (Location Separator Protocol) ist und die EID-Beziehungen (Endpoint Identity) zu Standorten (oder Gerätebeziehungen) verwaltet. Die Kontrollebene kann entweder ein dedizierter Router sein, der Funktionen der Kontrollebene bereitstellt, oder sie kann mit anderen Elementen des Fabric-Netzwerks koexistieren.
- Fabric-Randknoten: In der Regel ein Router, der an der Grenze zwischen externen Netzwerken und der SDA-Struktur arbeitet und Routing-Services für die virtuellen Netzwerke in der Struktur bereitstellt. Sie verbindet externe Layer-3-Netzwerke mit der SDA-Fabric.

- Fabric-Edge-Knoten: Gerät innerhalb der Fabric, das Nicht-Fabric-Geräte wie Switches, APs und Router mit der SDA-Fabric verbindet. Dabei handelt es sich um die Knoten, die die virtuellen Overlay-Tunnel und VNs mit Virtual eXtensible LAN (VXLAN) erstellen und die SGTs dem Fabric-gebundenen Datenverkehr auferlegen. Die Netzwerke auf beiden Seiten des Fabric-Edge befinden sich im SDA-Netzwerk. Sie verbinden kabelgebundene Endgeräte mit der SD-Access-Fabric.
- Zwischenknoten: Diese Knoten befinden sich im Kern der SDA-Fabric und sind mit Edge- oder Border-Knoten verbunden. Die zwischengeschalteten Knoten leiten den SDA-Datenverkehr lediglich als IP-Pakete weiter, ohne zu wissen, dass mehrere virtuelle Netzwerke involviert sind.
- Fabric-WLC: Wireless Controller, der Fabric-fähig ist und an der SDA-Kontrollebene beteiligt ist, die CAPWAP-Datenebene jedoch nicht verarbeitet.
- Fabric-Modus-APs: Fabric-fähige Access Points. Der Wireless-Datenverkehr wird am WAP VXLAN-gekapselt, sodass er über einen Edge-Knoten in die Fabric gesendet werden kann.
- Cisco DNA (DNAC): Der SDN-Controller der Enterprise-Klasse für das SDA-Fabric-Overlay-Netzwerk (Software Defined Access) ist für Automatisierungs- und Sicherheitsaufgaben zuständig. Es kann auch für einige Automatisierungs- und ähnliche Aufgaben für die Netzwerkgeräte genutzt werden, die das Underlay bilden (d. h. nicht SDA-bezogen).
- ISE: Die Identity Services Engine (ISE) ist eine erweiterte Richtlinienplattform, die eine Vielzahl von Rollen und Funktionen bereitstellen kann, nicht zuletzt die des AAA-Servers (Authentication, Authorization and Accounting). Die ISE interagiert in der Regel mit Active Directory (AD), Benutzer können jedoch für kleinere Bereitstellungen lokal sowie auf der ISE selbst konfiguriert werden.

Anmerkung: Die Kontrollebene ist ein wichtiger Infrastrukturbestandteil der SDA-Architektur. Daher wird empfohlen, sie ausfallsicher bereitzustellen.

Underlay- und Overlay-Netzwerke

Die SDA-Architektur nutzt Fabric-Technologie, die programmierbare virtuelle Netzwerke (Overlay-Netzwerke) unterstützt, die in einem physischen Netzwerk (einem Underlay-Netzwerk) ausgeführt werden.

Ein Stoff ist ein Overlay.

Ein Overlay-Netzwerk ist eine logische Topologie zur virtuellen Verbindung von Geräten, die auf einer beliebigen physischen Underlay-Topologie aufbaut. Er verwendet alternative Weiterleitungsattribute, um zusätzliche Services bereitzustellen, die nicht vom Underlay bereitgestellt werden. Sie wird auf der Basis erstellt, um ein oder mehrere virtualisierte und segmentierte Netzwerke zu erstellen. Aufgrund des softwaredefinierten Charakters von Overlays

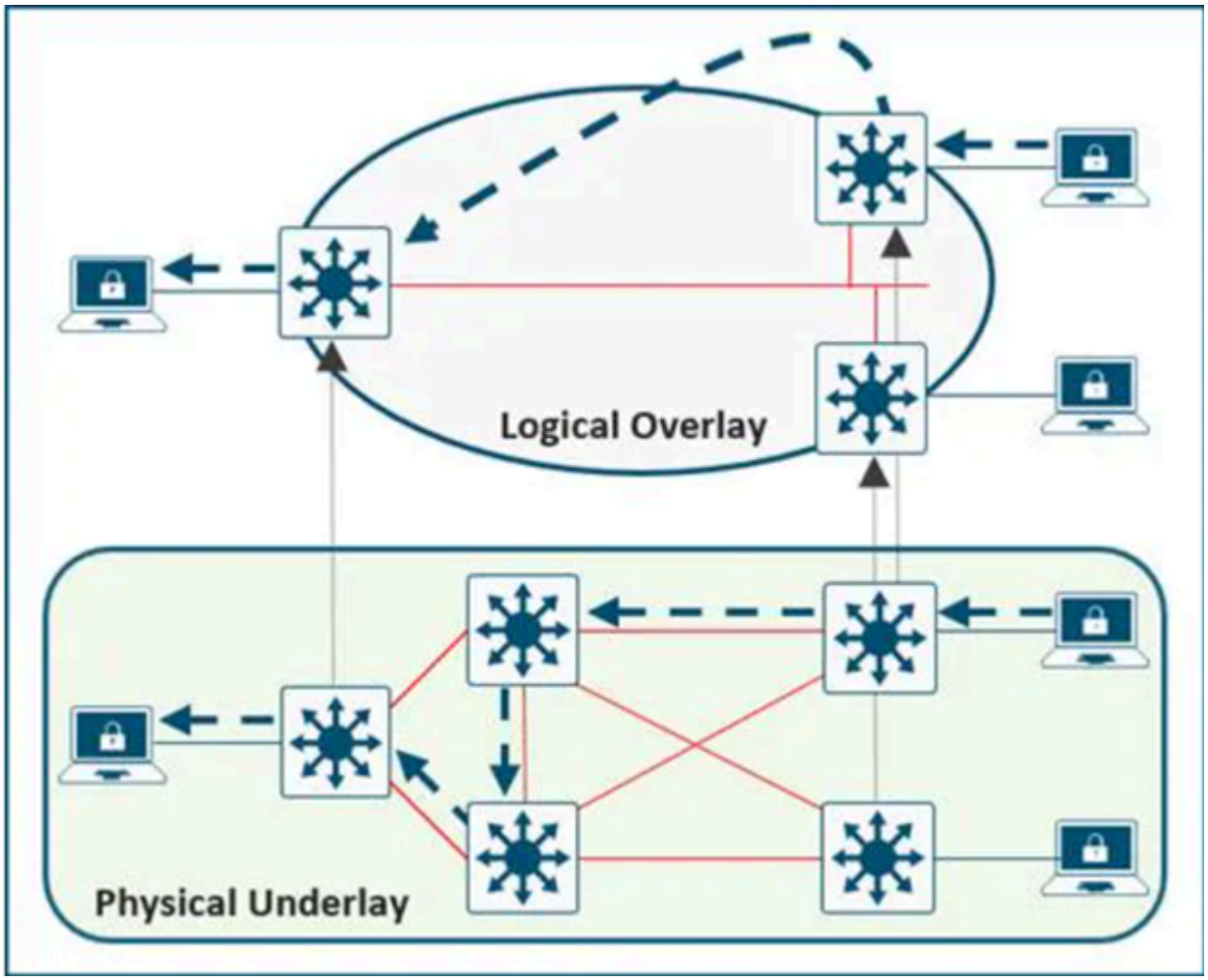
ist es möglich, diese auf sehr flexible Weise und ohne Einschränkungen der physischen Konnektivität zu verbinden. Dies ist eine einfache Möglichkeit zur Durchsetzung von Sicherheitsrichtlinien, da das Overlay so programmiert werden kann, dass es einen einzigen physischen Austrittspunkt (den Fabric Border Node) hat, und eine Firewall verwendet werden kann, um die Netzwerke dahinter zu schützen (unabhängig davon, ob sie sich befinden). Das Overlay kapselt den Datenverkehr mithilfe von VXLAN. VXLAN kapselt vollständige Layer-2-Frames für den Transport über das Underlay, wobei jedes Overlay-Netzwerk durch einen VXLAN Network Identifier (VNI) identifiziert wird. Overlay-Fabrics sind in der Regel komplex und erfordern einen hohen Administrator-Overhead bei der Bereitstellung neuer virtueller Netzwerke oder bei der Implementierung von Sicherheitsrichtlinien.

Beispiele für Netzwerk-Overlays:

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

Ein Underlay-Netzwerk wird durch die physischen Knoten wie Switches, Router und Wireless-APs definiert, die für die Bereitstellung des SDA-Netzwerks verwendet werden. Alle Netzwerkelemente des Underlays müssen über ein Routing-Protokoll eine IP-Konnektivität herstellen. Auch wenn das Underlay-Netzwerk wahrscheinlich nicht das herkömmliche Access-, Distribution- und Core-Modell verwendet, muss es eine gut konzipierte Layer-3-Grundlage verwenden, die robuste Leistung, Skalierbarkeit und hohe Verfügbarkeit bietet.

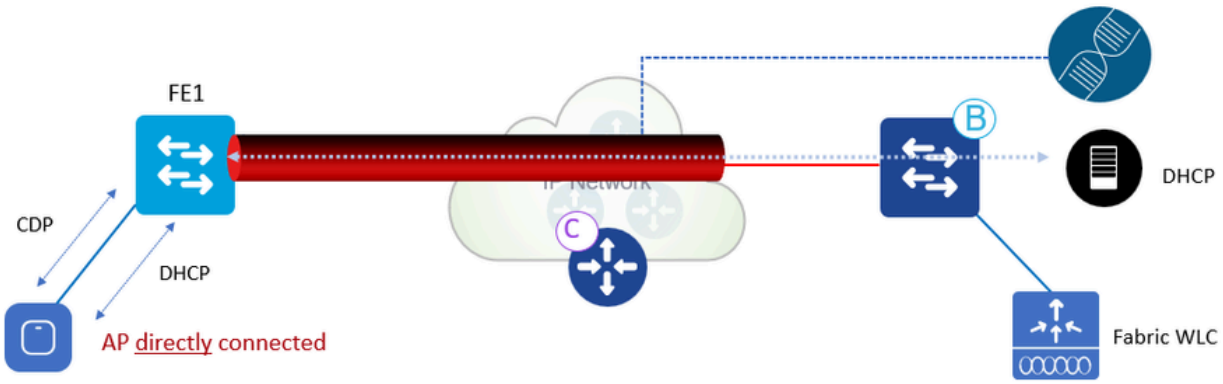
Anmerkung: SDA unterstützt IPv4 im Underlay-Netzwerk und IPv4 und/oder IPv6 in Overlay-Netzwerken.



Underlay- und Overlay-Netzwerke

Grundlegende Workflows

AP-Beitritt



AP-Join-Workflow

AP-Join-Workflow:

1. Admin konfiguriert den AP-Pool in DNAC in INFRA_VN. Cisco DNA stellt auf allen Fabric Edge-

Knoten eine Konfiguration bereit, um APs automatisch zu integrieren.

2. Der Access Point ist angeschlossen und hochgefahren. Fabric Edge erkennt, dass es sich um einen Access Point via CDP handelt, und wendet das Makro an, um dem Switch-Port das richtige VLAN zuzuweisen (oder die Schnittstellenvorlage anzuwenden).

3. AP bekommt eine IP-Adresse via DHCP im Overlay.

4. Fabric Edge registriert die IP-Adresse und MAC (EID) der APs und aktualisiert die Kontrollebene (CP).

5. AP lernt WLCs IP mit traditionellen Methoden. Der Fabric-AP wird als Zugangspunkt im lokalen Modus hinzugefügt.

6. WLC prüft, ob er Fabric-fähig ist (Wave 2- oder Wave 1-APs).

7. Wenn AP für Fabric unterstützt wird, fragt WLC den CP ab, um zu erfahren, ob AP mit Fabric verbunden ist.

8. Control Plane (CP) antwortet auf WLC mit RLOC. Das bedeutet, dass der Access Point mit dem Fabric verbunden ist und als "Fabric-fähig" angezeigt wird.

9. WLC führt eine L2-LISP-Registrierung für AP im CP durch (d. h. die AP-"spezielle" sichere Client-Registrierung). Hiermit werden wichtige Metadateninformationen vom WLC an den Fabric Edge übergeben.

10. Als Reaktion auf diese Proxy-Registrierung benachrichtigt Control Plane (CP) Fabric Edge und übergibt die vom WLC empfangenen Metadaten (Flag, das angibt, dass es sich um einen Access Point und die IP-Adresse des Access Points handelt).

11. Fabric Edge verarbeitet die Informationen, erkennt, dass es sich um einen AP handelt und erstellt eine VXLAN-Tunnelschnittstelle zur angegebenen IP (Optimierung: Switch-Seite ist bereit für den Beitritt von Clients).

Mit den Befehlen debug/show kann der AP-Join-Workflow überprüft und validiert werden.

Steuern Sie Fläche

debug lisp control-plane all

show lisp instance-id <L3 instance id> ipv4 server (Muss die vom Edge-Switch registrierte AP-IP-Adresse anzeigen, mit der der AP verbunden ist.)

show lisp instance-id <L2 instance id> Ethernet-Server (Muss die AP-Funk- sowie Ethernet-MAC-Adresse, die vom WLC registrierte AP-Funk und die Ethernet-MAC-Adresse des Edge-Switches anzeigen, mit dem der AP verbunden ist.)

Edge-Switch

debug access-tunnel all

debug lisp control-plane all

Übersicht über den Zugriffstunnel anzeigen

show lisp instance < L2 instance id> ethernet database wlc access-points (Muss den AP-Funk hier anzeigen.)

WLC

Fabric AP-Zusammenfassung anzeigen

WLC LISP-Debugging

set platform software trace wncd chassis active r0 lisp-agent-api debugging

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 debugging

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 debuggen

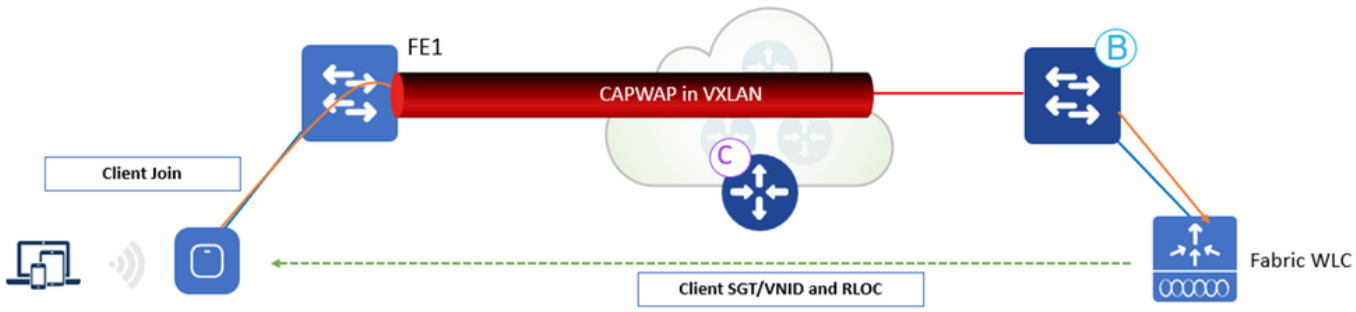
set platform software trace wncd chassis active r0 lisp-agent-ha debug

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

Access Point

IP-Tunnelstruktur anzeigen

Client integriert



Integrierter Client-Workflow

Client-Onboard-Workflow:

1. Der Client authentifiziert sich bei einem Fabric-fähigen WLAN. WLC erhält SGT von der ISE, aktualisiert AP mit dem Client L2VNID und SGT zusammen mit RLOC IP. WLC kennt den RLOC des AP aus der internen Datenbank.

2. WLC-Proxy registriert Client-L2-Info in CP; Diese Nachricht wurde von LISP modifiziert, um zusätzliche Informationen wie das Client-SGT weiterzugeben.

3. Fabric Edge wird vom CP benachrichtigt und fügt der Weiterleitungstabelle Client-MAC in L2 hinzu. Anschließend wird die Richtlinie basierend auf dem Client-SGT von der ISE abgerufen.

4. Der Client initiiert eine DHCP-Anforderung.

5. AP kapselt es in VXLAN mit L2 VNI-Informationen.

6. Fabric Edge weist L2-VNID der VLAN-Schnittstelle zu und leitet DHCP im Overlay weiter (wie bei einem kabelgebundenen Fabric-Client).

7. Der Client erhält eine IP-Adresse von DHCP.

8. DHCP-Snooping (und/oder ARP für statische) löst die EID-Registrierung des Clients durch den Fabric Edge beim CP aus.

Mit den Befehlen debug/show kann der integrierte Client-Workflow überprüft und validiert werden.

Steuern Sie Fläche

debug lisp control-plane all

Edge-Switch

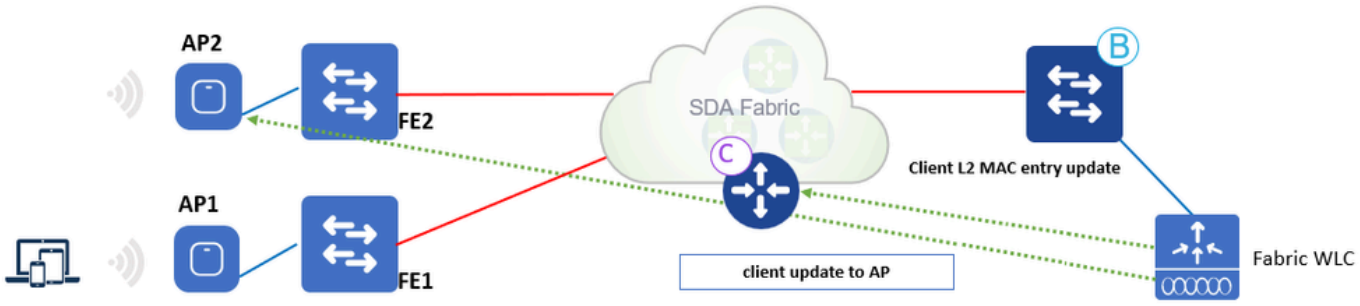
debug lisp control-plane all

debug ip dhcp snooping paket/event

WLC

Für die LISP-Kommunikation werden die gleichen Debugging-Anweisungen wie für den AP-Join verwendet.

Client-Roaming



Client-Roaming-Workflow

Client-Roaming-Workflow:

1. Client wechselt auf FE2 zu AP2 (Inter-Switch-Roaming). WLC wird vom AP benachrichtigt.

2. WLC aktualisiert die Weiterleitungstabelle auf dem Access Point mit Client-Informationen (SGT, RLOC).

3. WLC aktualisiert den L2-MAC-Eintrag in CP mit dem neuen RLOC Fabric Edge 2.

4. CP teilt dann mit:

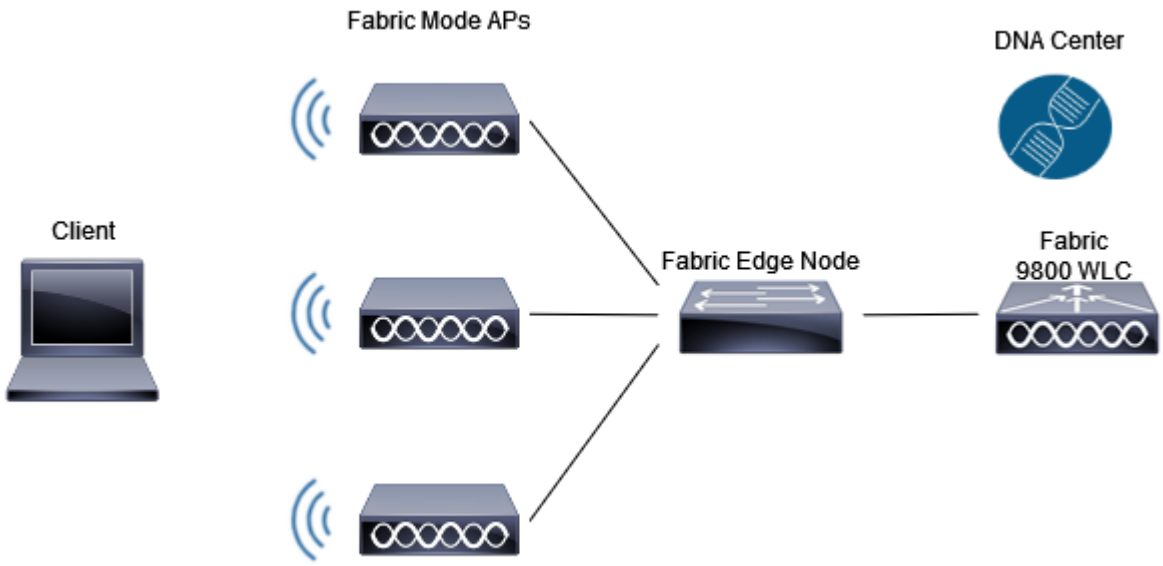
- Fabric Edge FE2 (Roam-to-Switch), um die Client-MAC zur Weiterleitungstabelle hinzuzufügen, die auf den VXLAN-Tunnel verweist.
- Fabric Edge FE1 (Roam-from-Switch) zur Bereinigung für den Wireless-Client.

5. Fabric Edge aktualisiert den L3-Eintrag (IP) in der CP-Datenbank, sobald Datenverkehr empfangen wird.

6. Roaming ist Layer 2, da Fabric Edge 2 über dieselbe VLAN-Schnittstelle (Anycast GW) verfügt.

Konfigurieren

Netzwerkdiagramm



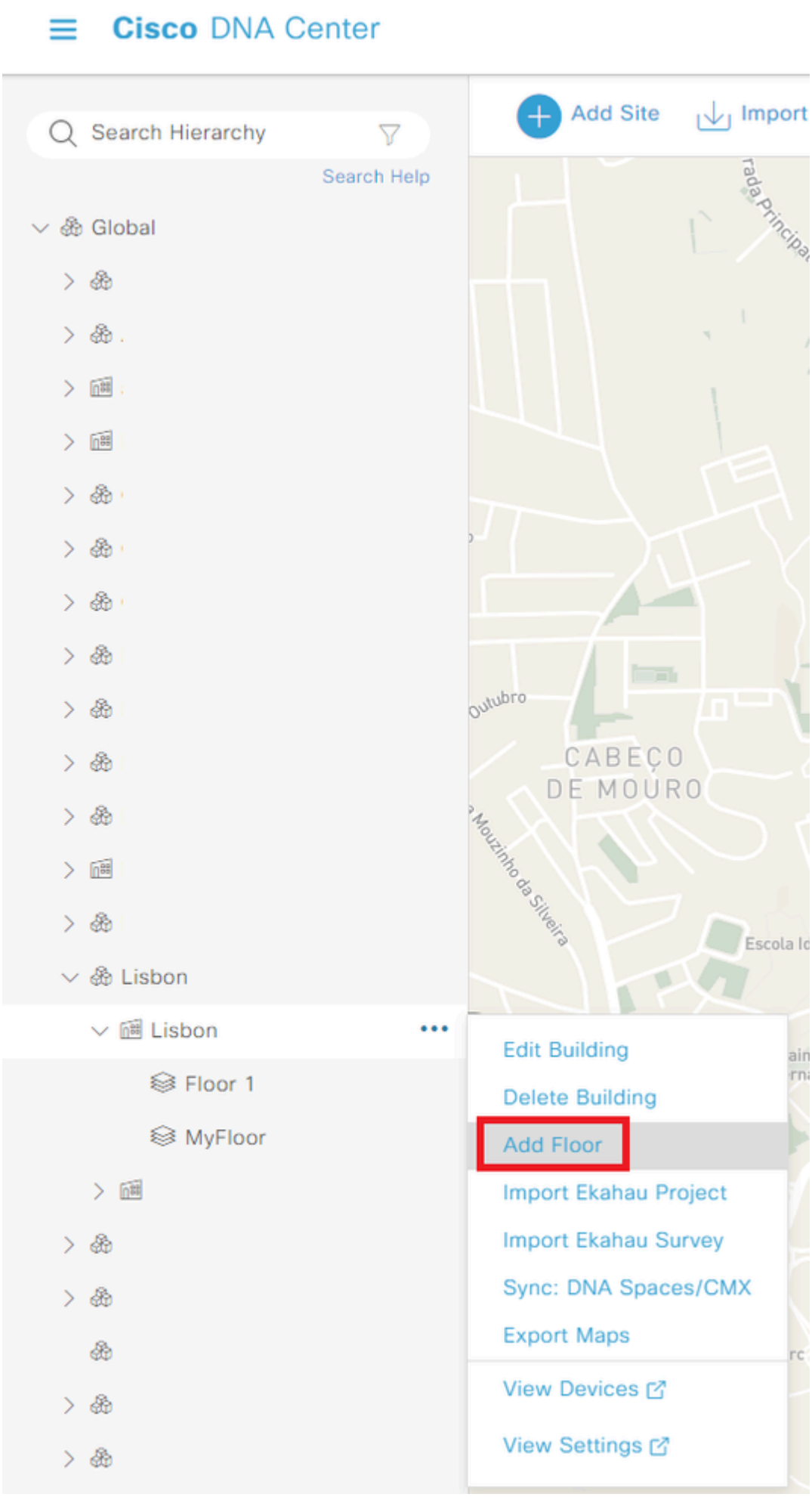
Netzwerkdiagramm

WLC-Erkennung und -Bereitstellung in Cisco DNA

WLC hinzufügen

Schritt 1: Navigieren Sie zu dem Ort, an dem Sie den WLC hinzufügen möchten. Sie können ein neues Gebäude/Stockwerk hinzufügen.

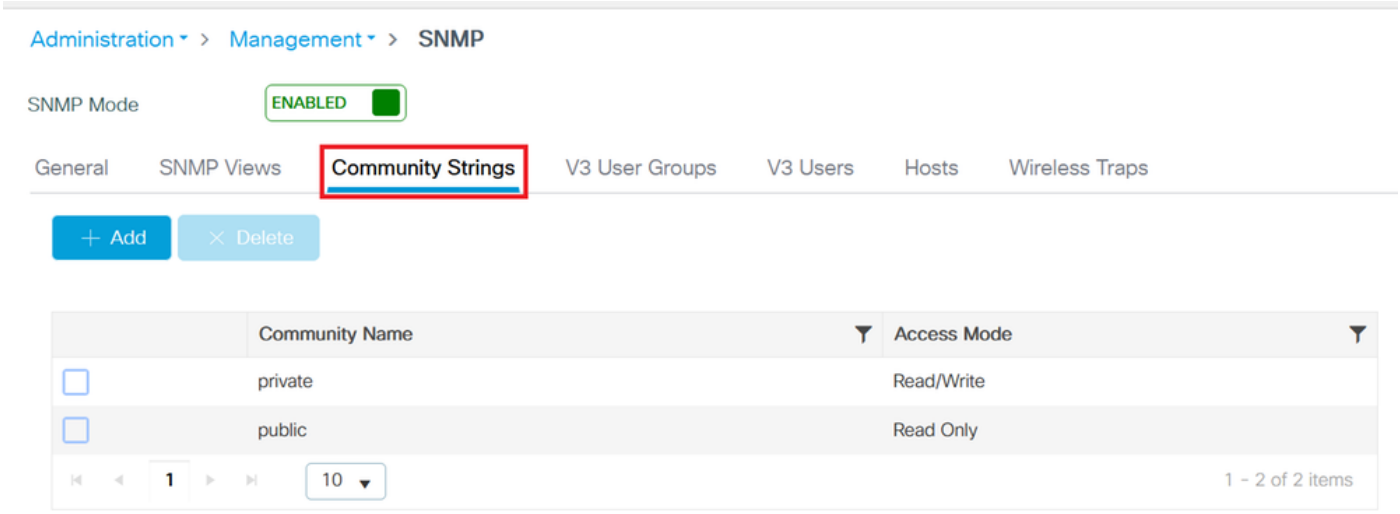
Navigieren Sie zu Design > Network Hierarchy, und geben Sie das Gebäude/Stockwerk ein. Sie können auch ein neues Stockwerk erstellen, wie in der Abbildung dargestellt:



Neue Ebene erstellen

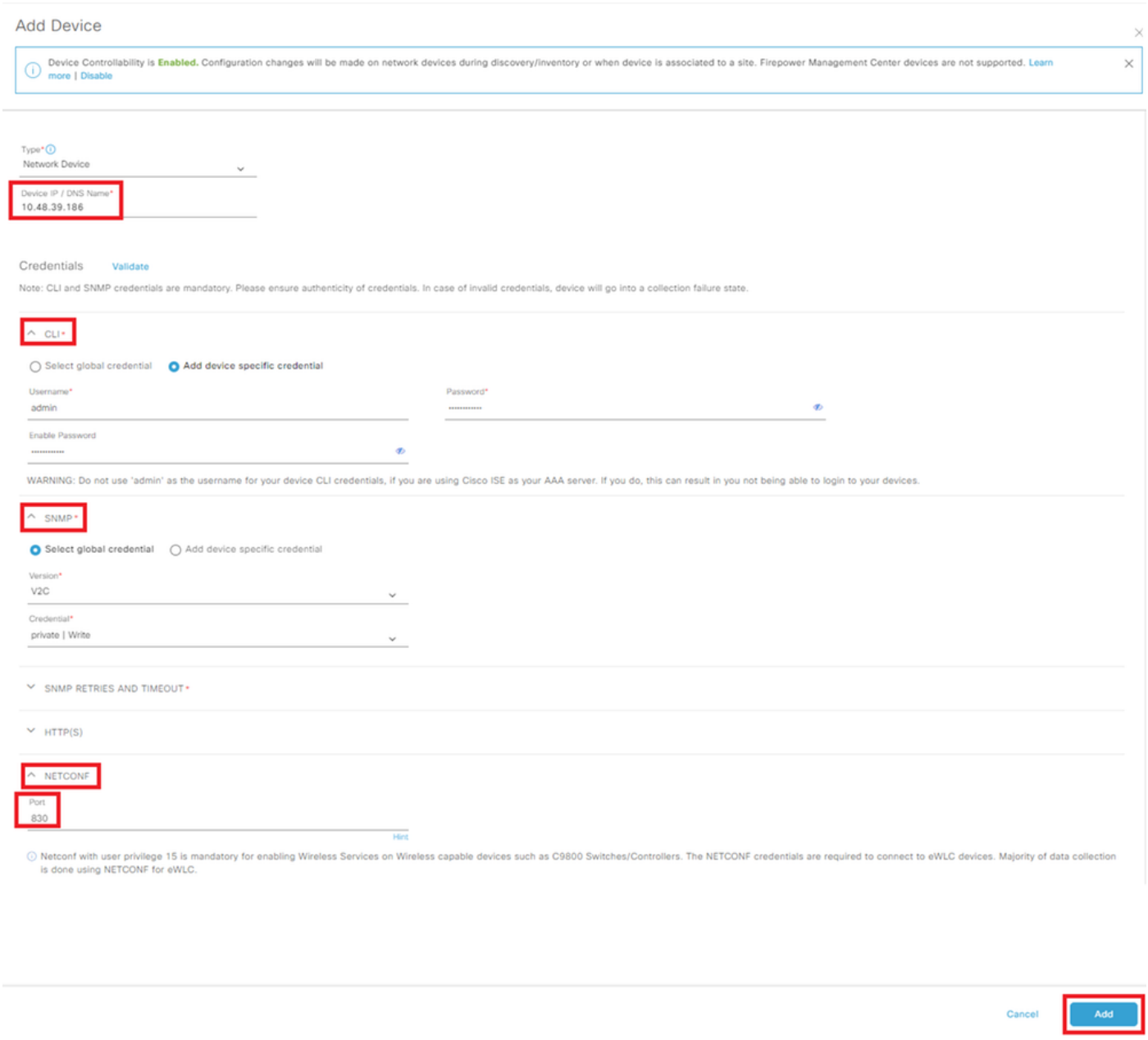
Schritt 2. Fügen Sie Etage hinzu. Sie können auch ein Bild der Anlage des Bodens hochladen

und überprüfen Sie die konfigurierte Zeichenfolge. Sie müssen den richtigen SNMP Community String hinzufügen, wenn Sie den WLC zur Cisco DNA hinzufügen, und sicherstellen, dass netconf-yang auf dem 9800 WLC mit den Befehlen show netconf-yang status aktiviert ist. Klicken Sie am Ende auf Hinzufügen:



SNMP-Konfiguration

Schritt 5: Fügen Sie die WLC-IP-Adresse, die CLI-Anmeldeinformationen (die von der Cisco DNA für die Anmeldung am WLC verwendet werden und auf dem WLC konfiguriert werden müssen, bevor sie zur Cisco DNA hinzugefügt werden), den SNMP-String hinzu, und überprüfen Sie, ob der NETCONF-Port auf Port 830 konfiguriert ist:

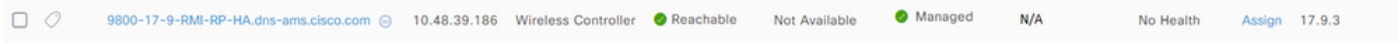


WLC hinzufügen

Der WLC wird als NA angezeigt, da die Cisco DNA noch synchronisiert ist:

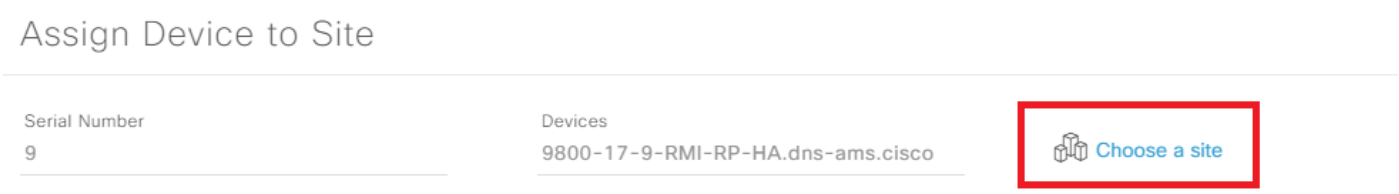
WLC im Synchronisierungsprozess

Wenn der Synchronisierungsvorgang abgeschlossen ist, werden der WLC-Name, die IP-Adresse, sowie die verwaltete und die Softwareversion angezeigt, sofern diese erreichbar ist:



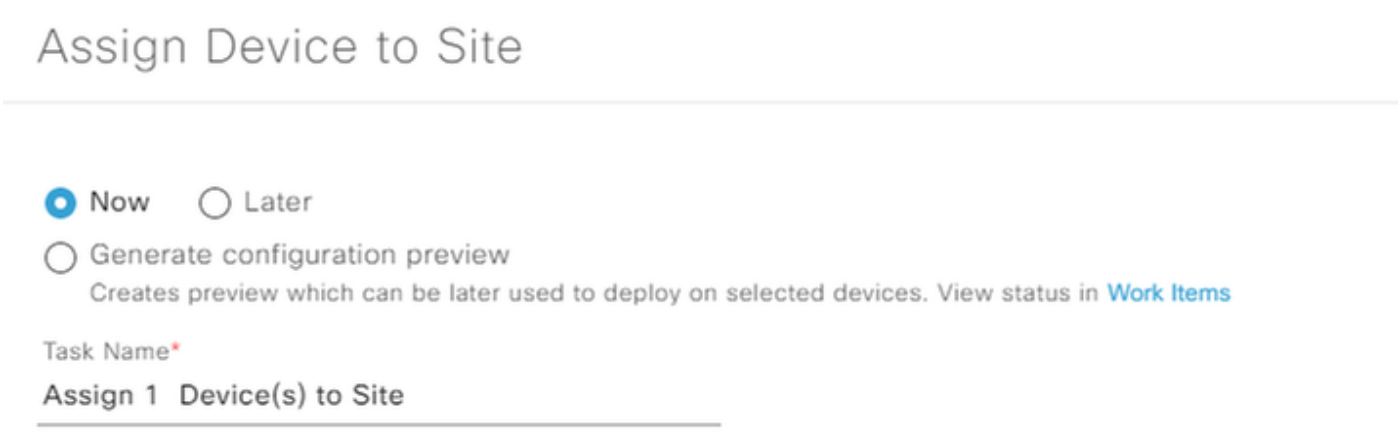
WLC synchronisiert

Schritt 6: Zuweisen des WLC zu einem Standort Klicken Sie in der Geräteliste auf Zuweisen, und wählen Sie einen Standort aus:



Gerät dem Standort zuweisen

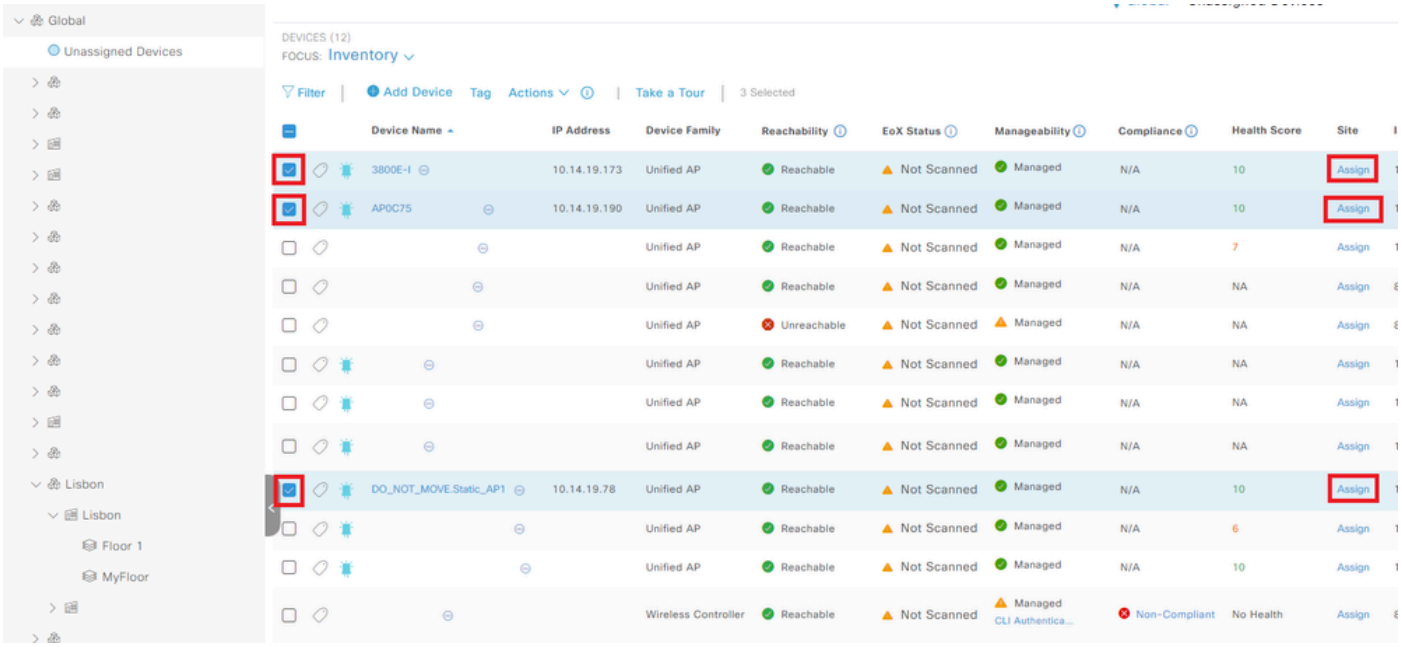
Sie können den Standort jetzt oder zu einem späteren Zeitpunkt zuweisen:



Gerät jetzt oder zu einem späteren Zeitpunkt dem Standort zuweisen

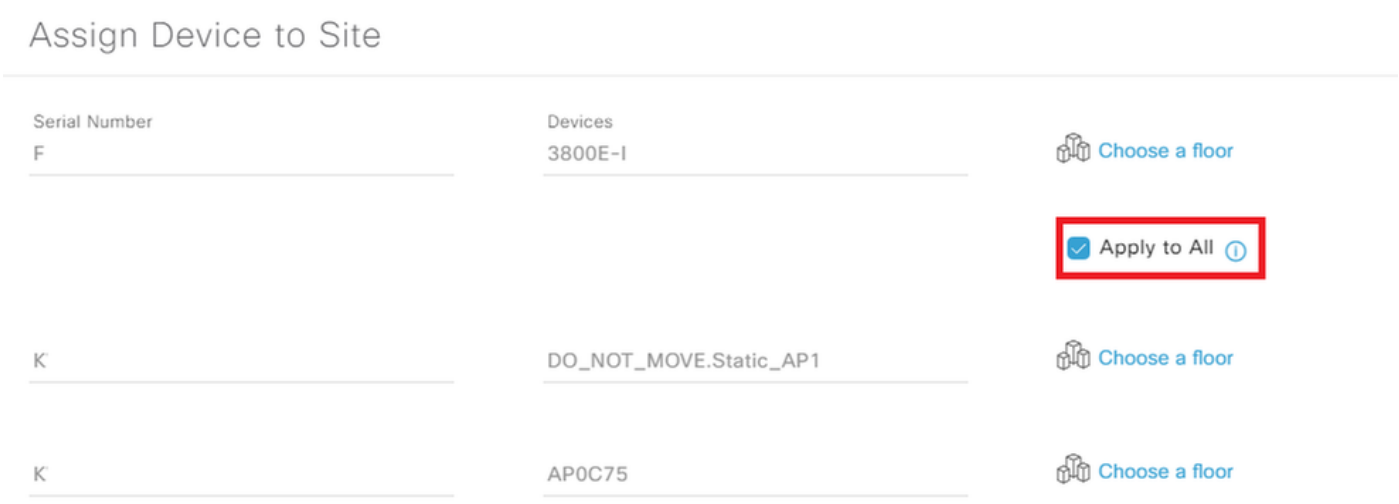
Access Points hinzufügen

Schritt 1:Sobald der WLC hinzugefügt wurde und erreichbar ist, navigieren Sie zu Provision > Inventory > Global > Unassigned Devices (Bereitstellung > Bestand > Global > Nicht zugewiesene Geräte) und suchen Sie nach den APs, die Sie Ihrem WLC hinzugefügt haben:



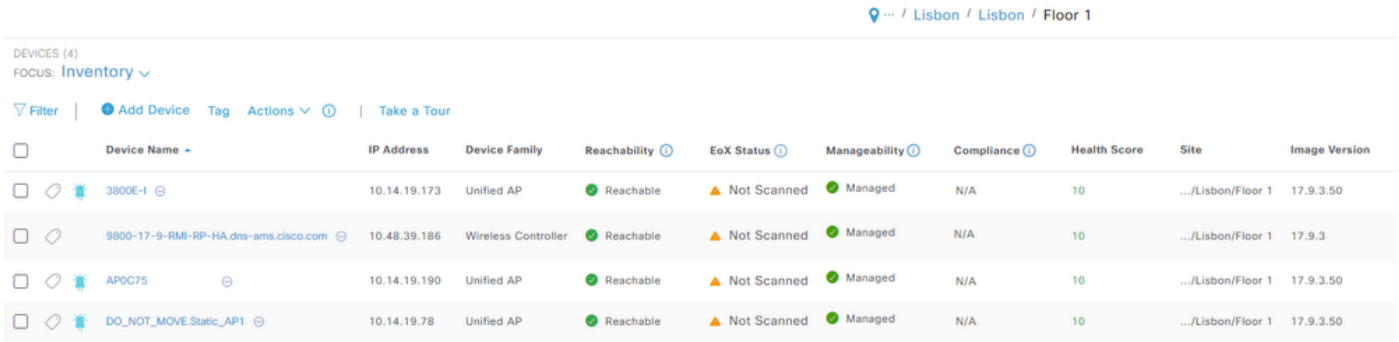
Access Points hinzufügen

Schritt 2: Wählen Sie die Option Zuordnen. Zuweisen der APs zu einem Standort Aktivieren Sie das Kontrollkästchen Auf alle anwenden, um die Konfiguration für mehrere Geräte gleichzeitig vorzunehmen.



Zuweisen von APs zum Standort

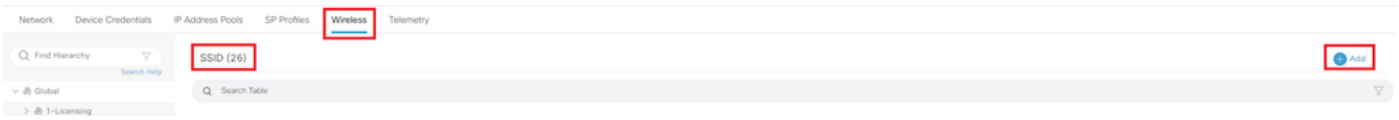
Navigieren Sie zu Ihrem Stockwerk, und Sie können alle ihm zugewiesenen Geräte sehen - WLC und APs:



Dem Standort zugewiesene Geräte

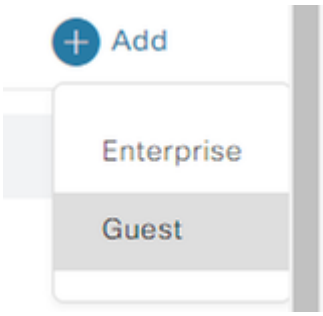
SSID erstellen

Schritt 1: Navigieren Sie zu Design > Network Settings > Wireless > Global, und fügen Sie eine SSID hinzu:



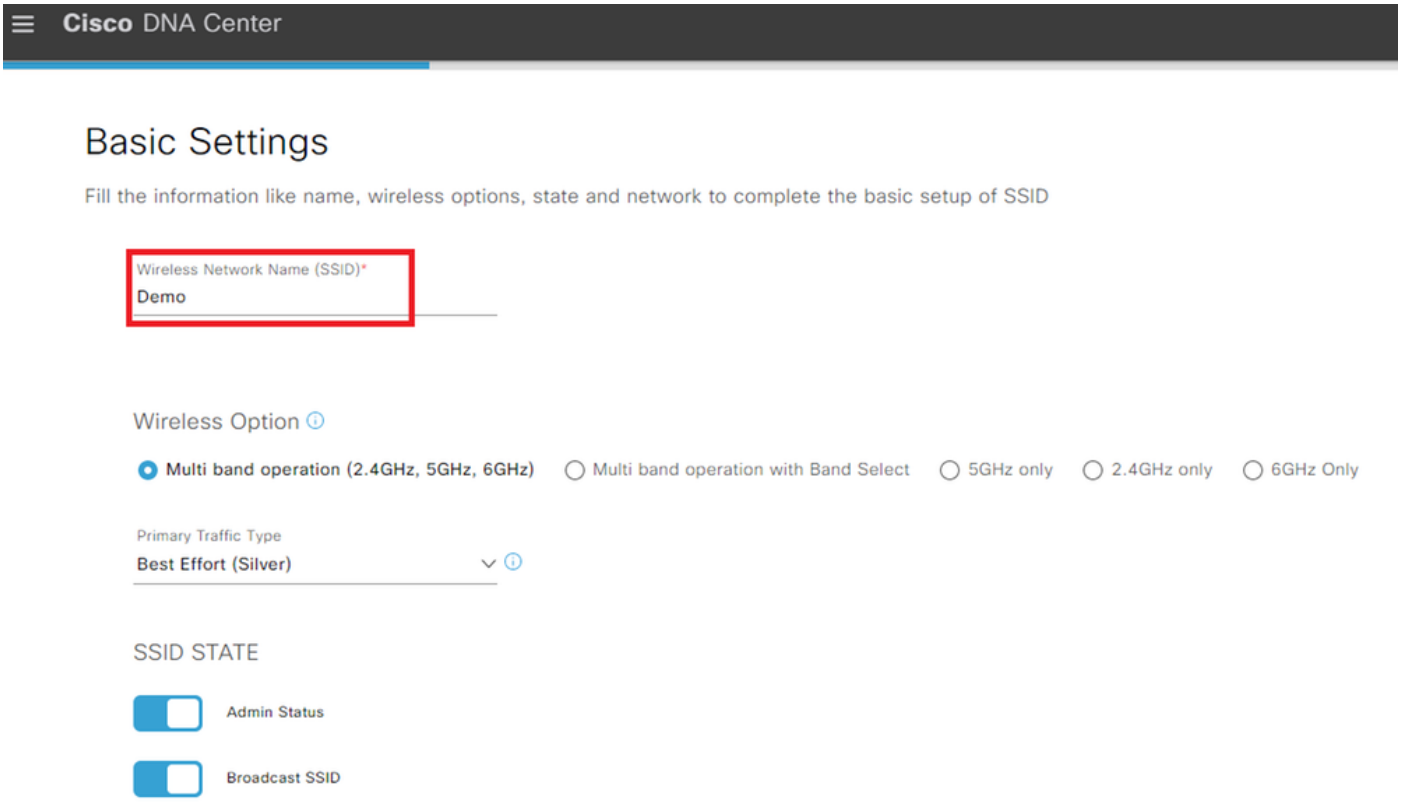
SSID erstellen

Sie können eine Unternehmens-SSID oder eine Gast-SSID erstellen. In dieser Demo wird eine Gast-SSID erstellt:

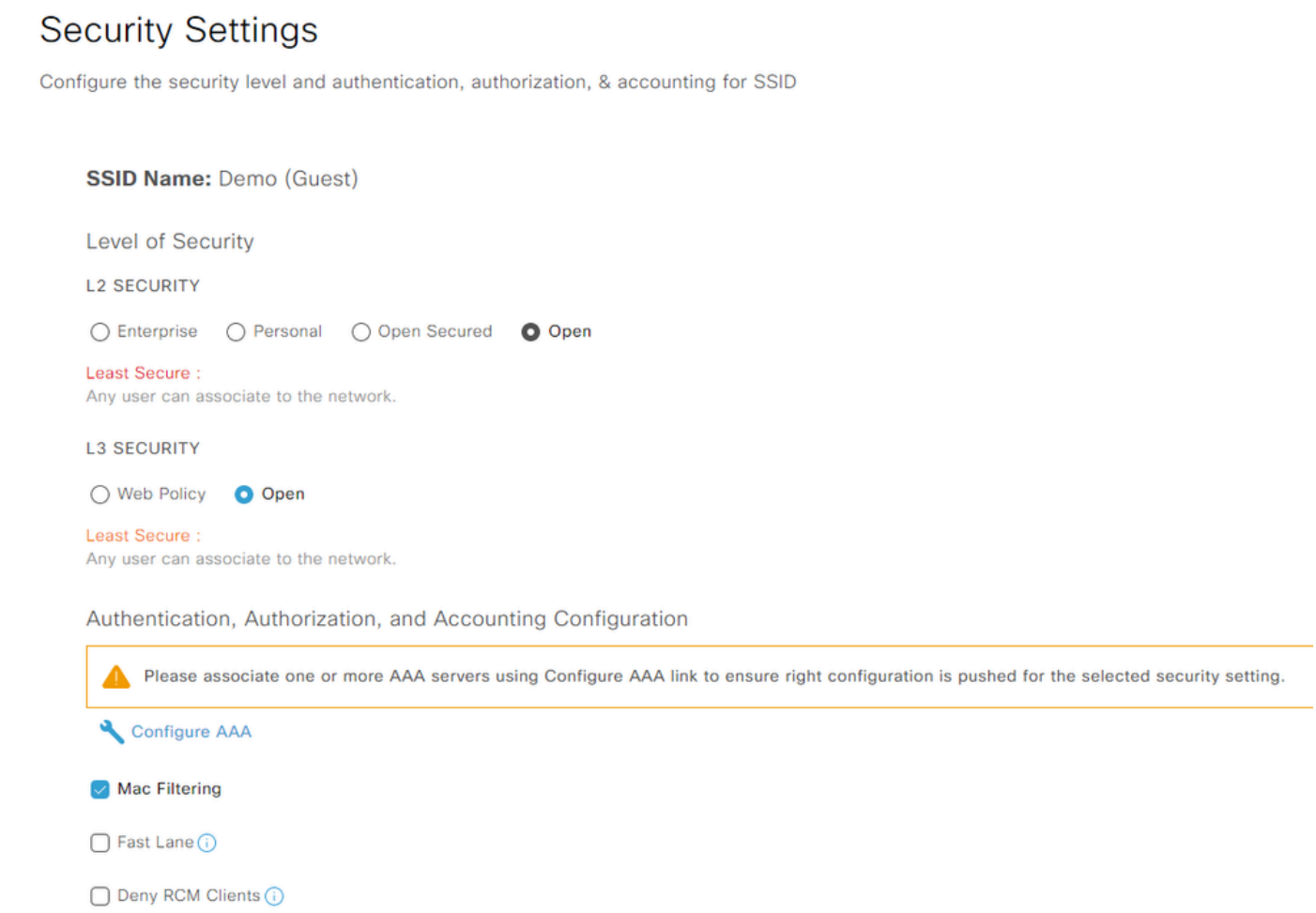


Unternehmens- oder Gast-SSID

Schritt 2: Wählen Sie die Einstellung für die SSID aus. In diesem Fall wird eine offene SSID erstellt. Admin-Status und Broadcast-SSID müssen aktiviert sein:



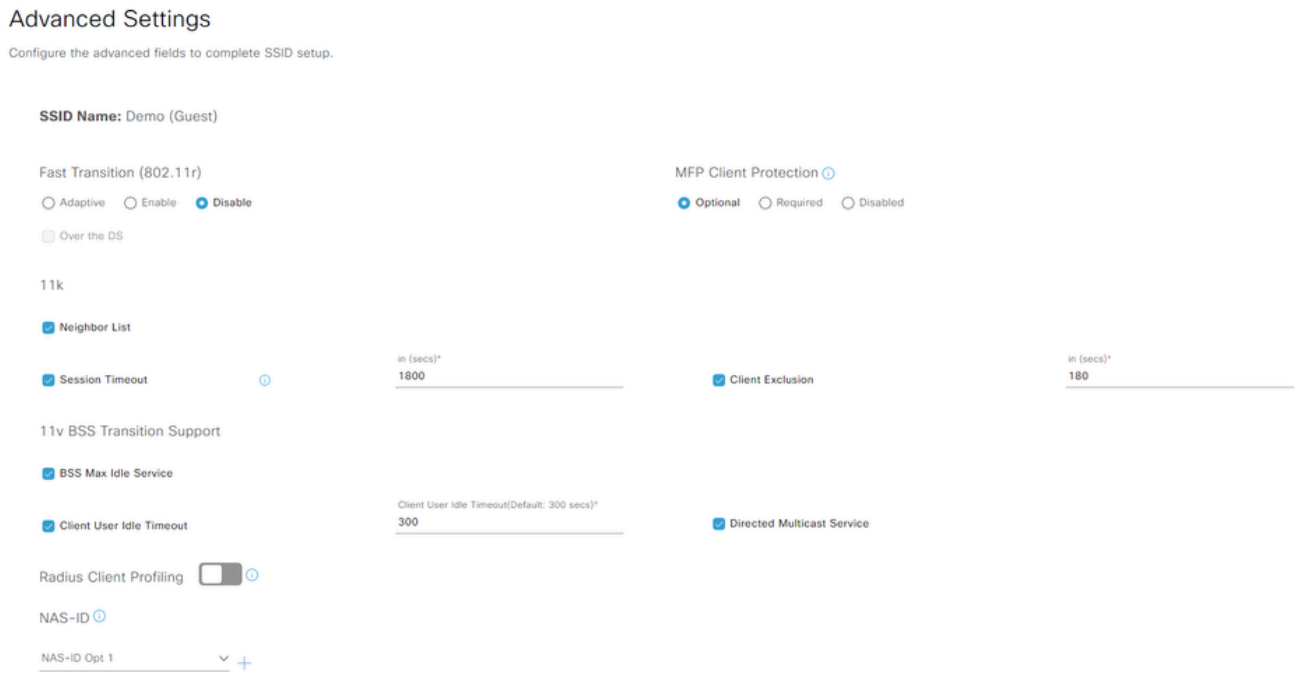
SSID-Grundeinstellungen



SSID-Sicherheitseinstellungen

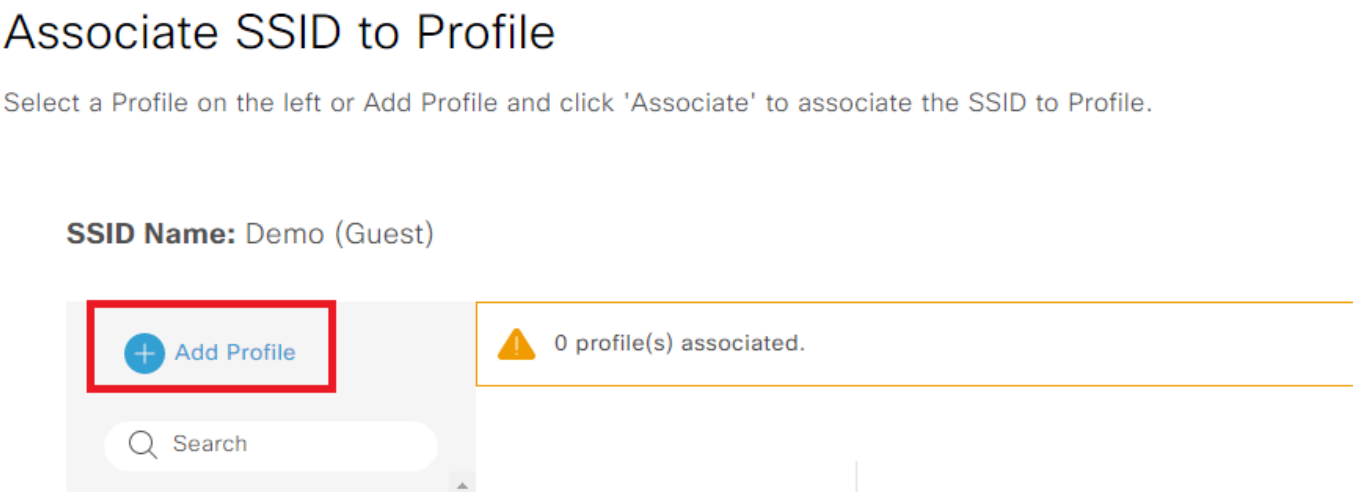
⚠ Vorsicht: Vergessen Sie nicht, einen AAA-Server für die SSID zu konfigurieren und zuzuordnen. Die Liste der Standardmethoden wird zugeordnet, wenn keine AAA-Server konfiguriert sind.

Wenn Sie auf Weiter klicken, werden die erweiterten Einstellungen für Ihre SSID angezeigt:



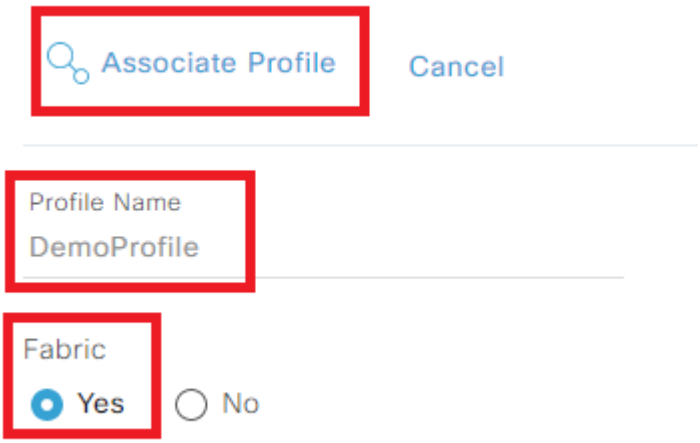
Erweiterte SSID-Einstellungen

Schritt 3: Nach der Erstellung der SSID müssen Sie sie einem Profil zuordnen. Klicken Sie auf Profil hinzufügen:



Profil hinzufügen

Schritt 4: Geben Sie dem Profil einen Namen, wählen Sie Fabric aus, und klicken Sie am Ende auf Associate Profile:



Profil zuordnen

Es wird eine Zusammenfassung der SSID und des Profils angezeigt, die Sie erstellt haben:

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-Zusammenfassung

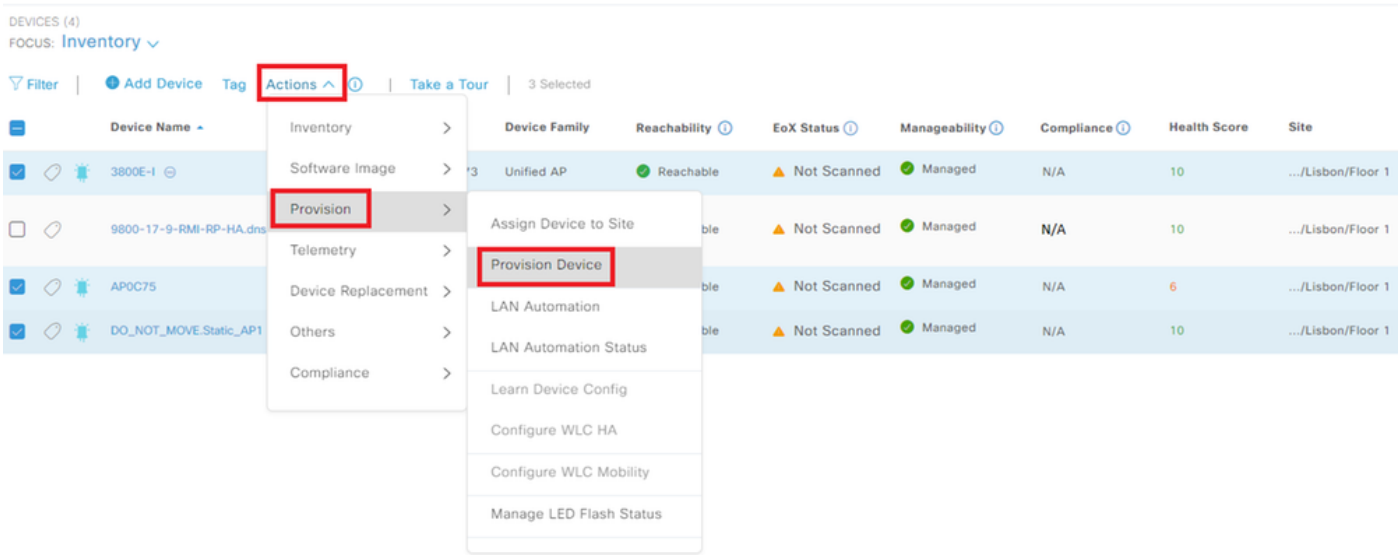
Schritt 5: Konfigurieren eines neuen Netzwerkprofils:

Sie konfigurieren möchten. In dieser Demo wurden die Standardeinstellungen konfiguriert. Klicken Sie auf Speichern:

Einfaches RF-Profil hinzufügen

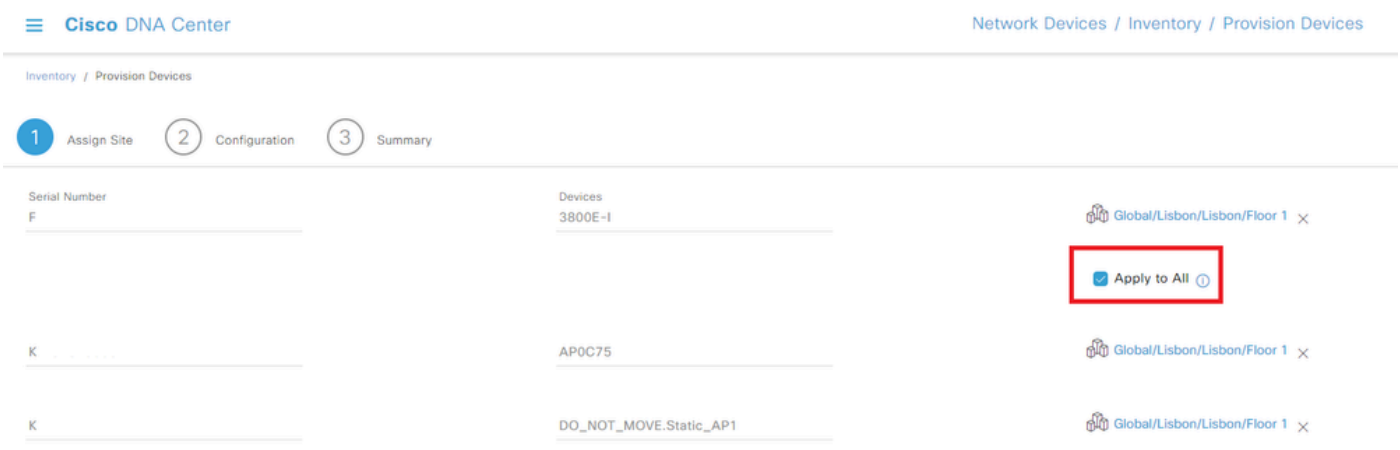
Access Points bereitstellen

Schritt 1: Navigieren Sie zu Ihrem Gebäude/Stockwerk. Wählen Sie APs und Aktionen > Bereitstellung > Gerät bereitstellen aus:



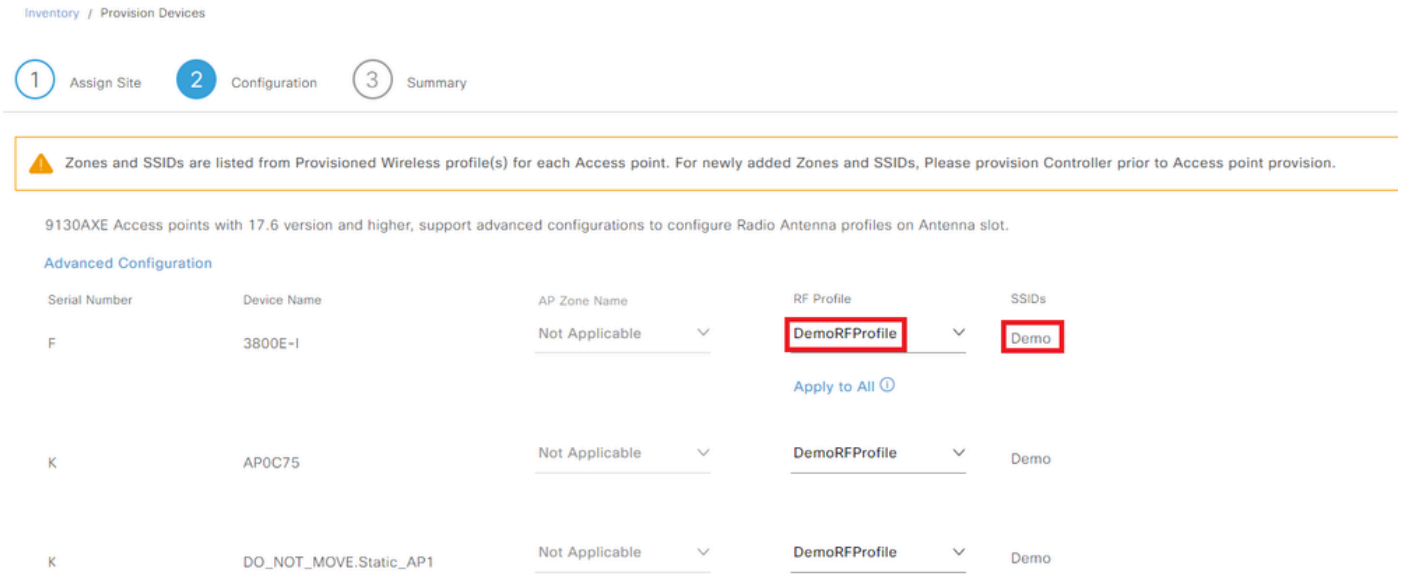
APs bereitstellen

Schritt 2: Überprüfen Sie, ob der zugewiesene Standort korrekt ist, und wählen Sie Auf alle anwenden aus:



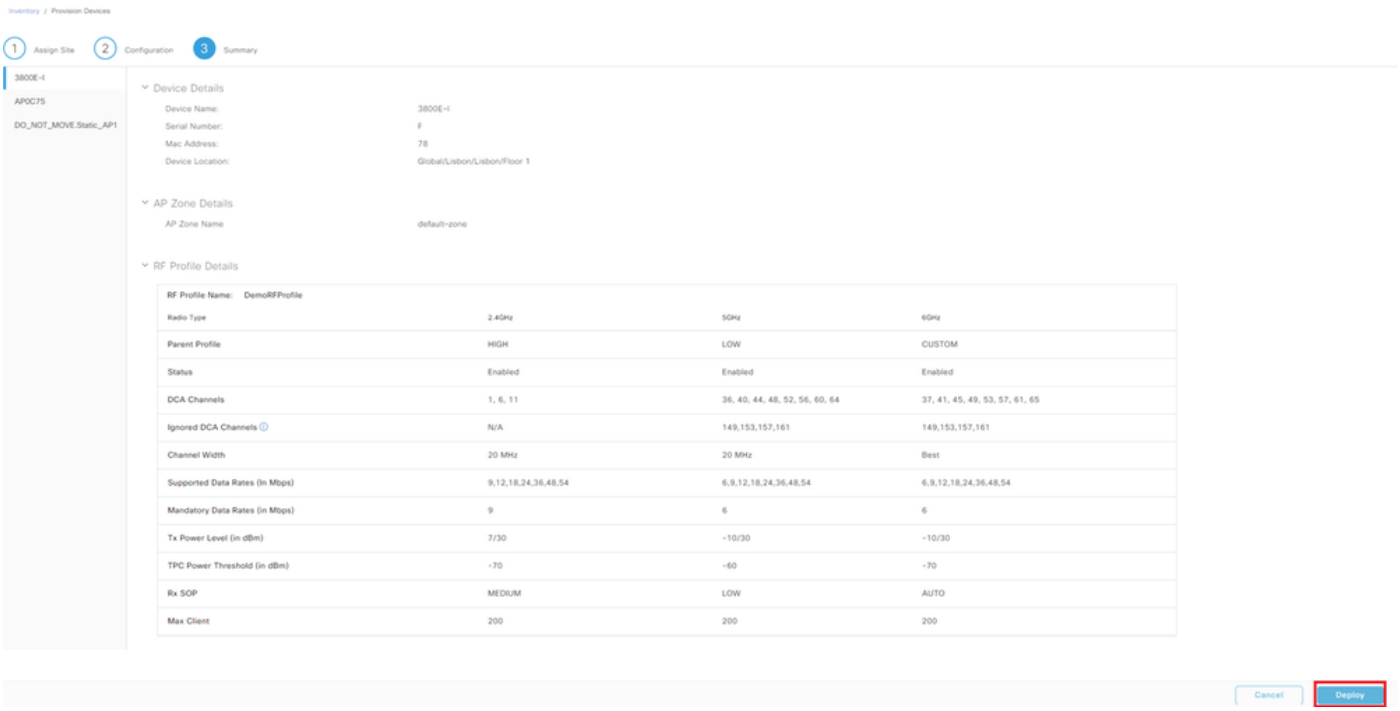
Zuweisen von Standorten zu APs

Schritt 3: Wählen Sie aus der Dropdown-Liste ein RF-Profil aus, und vergewissern Sie sich, dass die SSID die richtige ist:



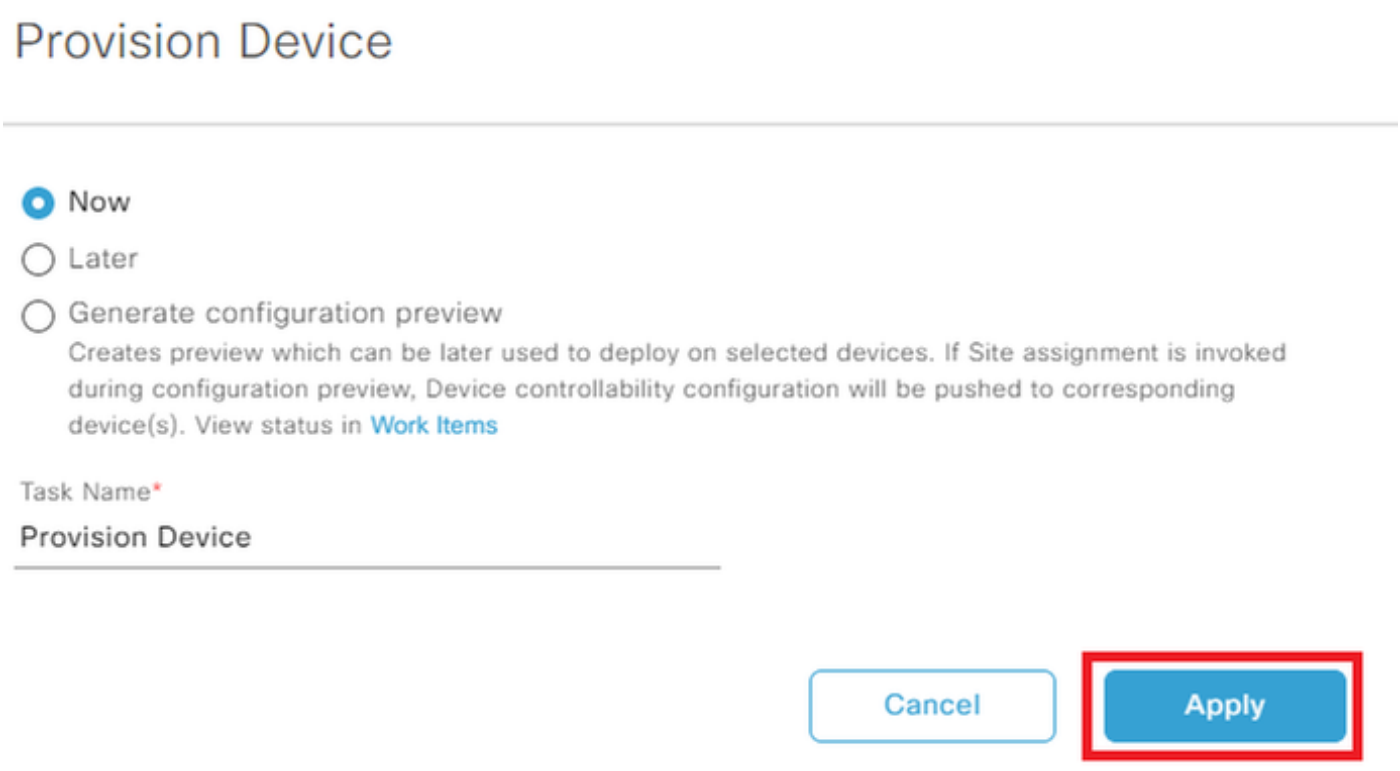
RF-Profil auswählen

Schritt 4: Überprüfen der Einstellungen der Access Points Wenn alles in Ordnung ist, wählen Sie Bereitstellen:



Bereitstellung der APs

Schritt 5: Die Gerätebereitstellung kann zu einem bestimmten Zeitpunkt oder zu einem späteren Zeitpunkt erfolgen. Wählen Sie am Ende Apply (Anwenden):

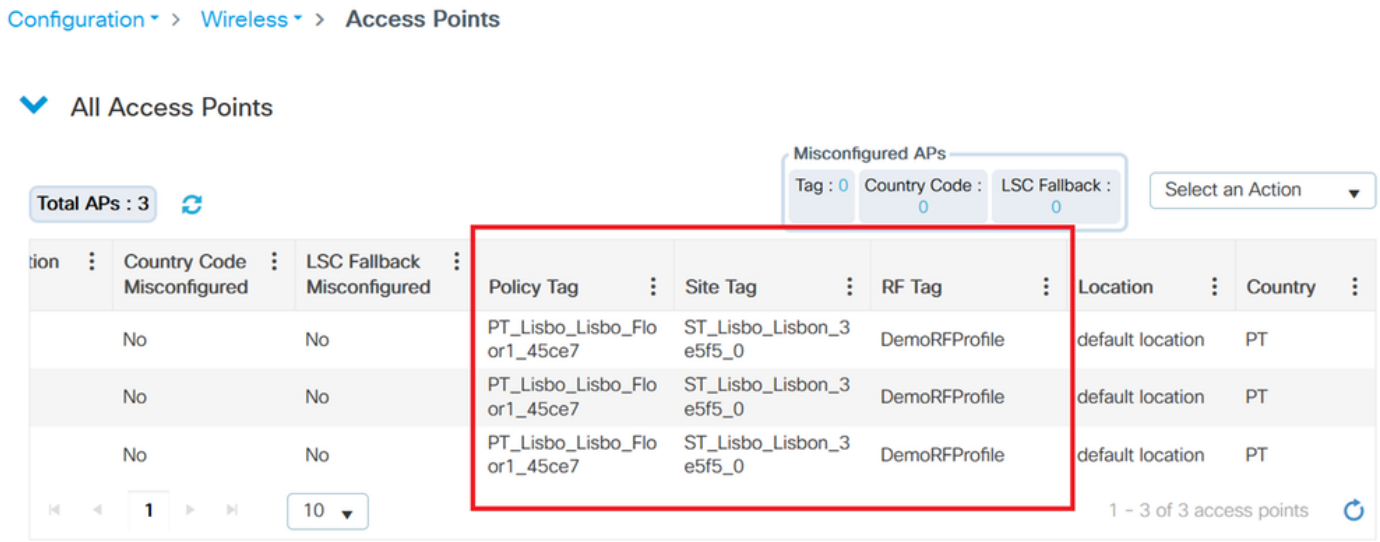


APs jetzt oder zu einem späteren Zeitpunkt bereitstellen

⚠ Vorsicht: Bei der Bereitstellung müssen die APs, die bereits Teil der konfigurierten Ebene für das ausgewählte HF-Profil sind, verarbeitet und neu gestartet werden.

Die APs werden jetzt bereitgestellt.

Schritt 6: Navigieren Sie auf der WLC-Seite zu Configuration > Wireless > Access Points. Überprüfen Sie, ob die AP-Tags von der Cisco DNA entfernt wurden:



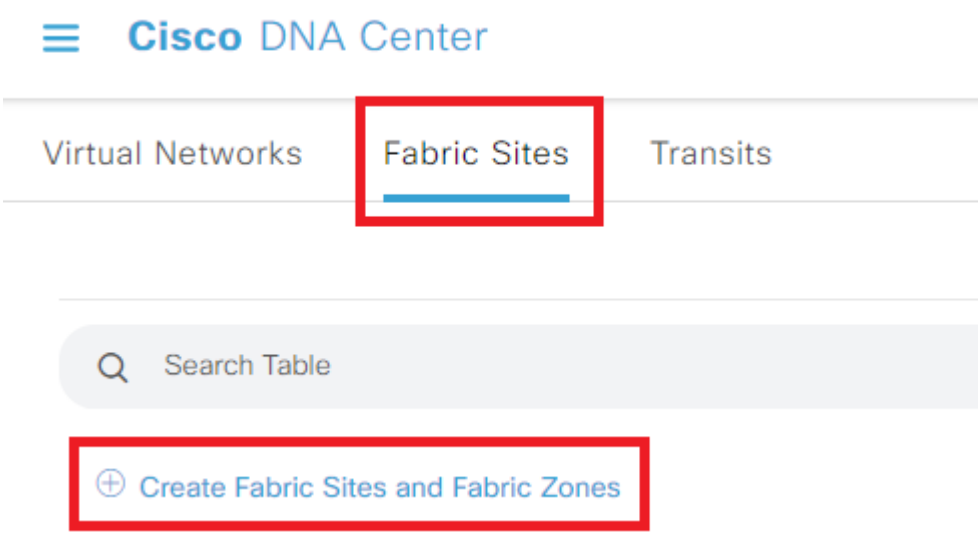
Tags auf APs

Schritt 7: Navigieren Sie zu Configuration > Tags & Profiles > WLANs, und vergewissern Sie sich, dass die SSID von Cisco DNA weitergeleitet wurde:

WLAN

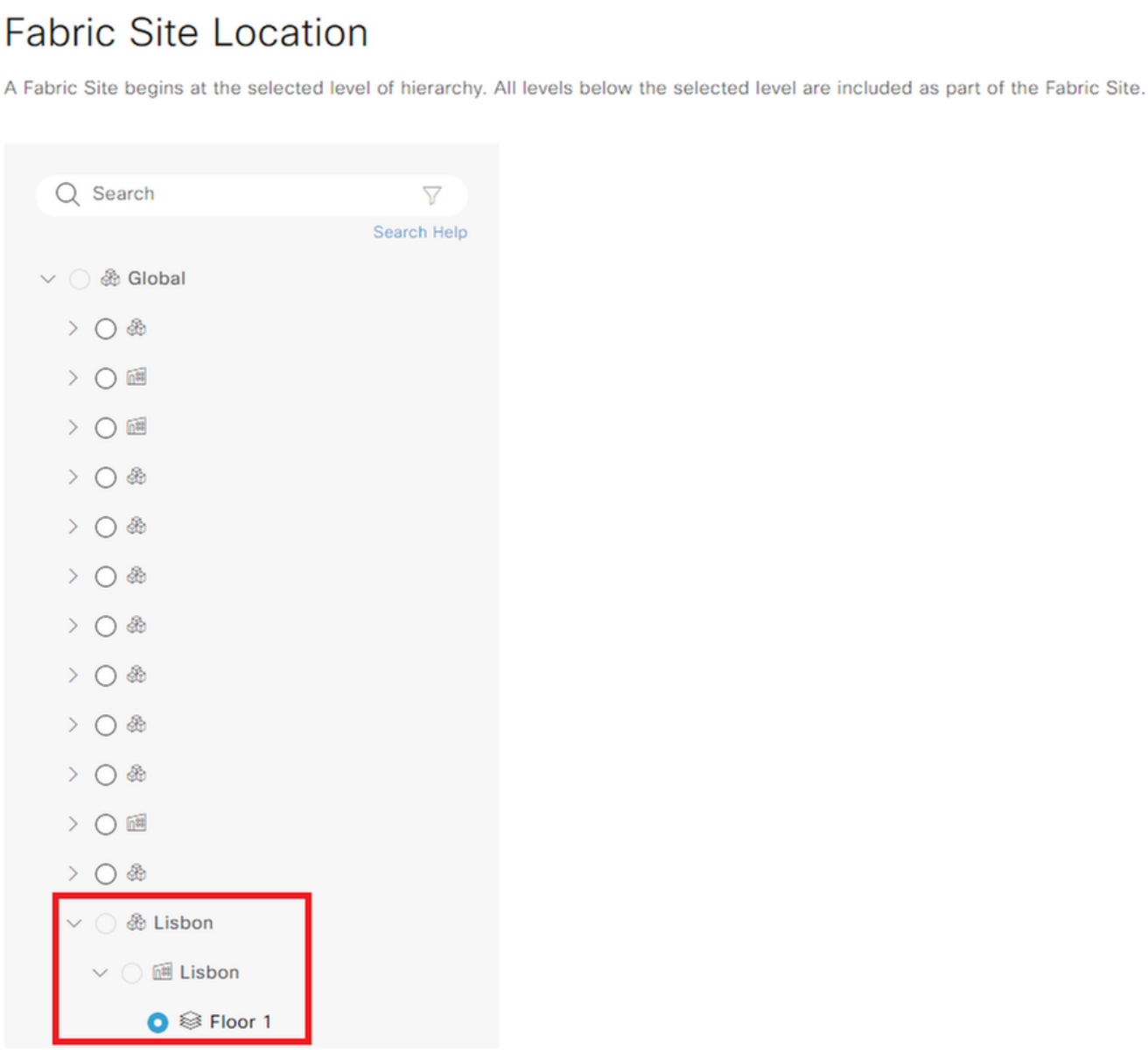
Fabric-Standort erstellen

Schritt 1: Navigieren Sie zu Bereitstellung > Fabric-Standorte. Erstellen Sie eine Fabric-Site:



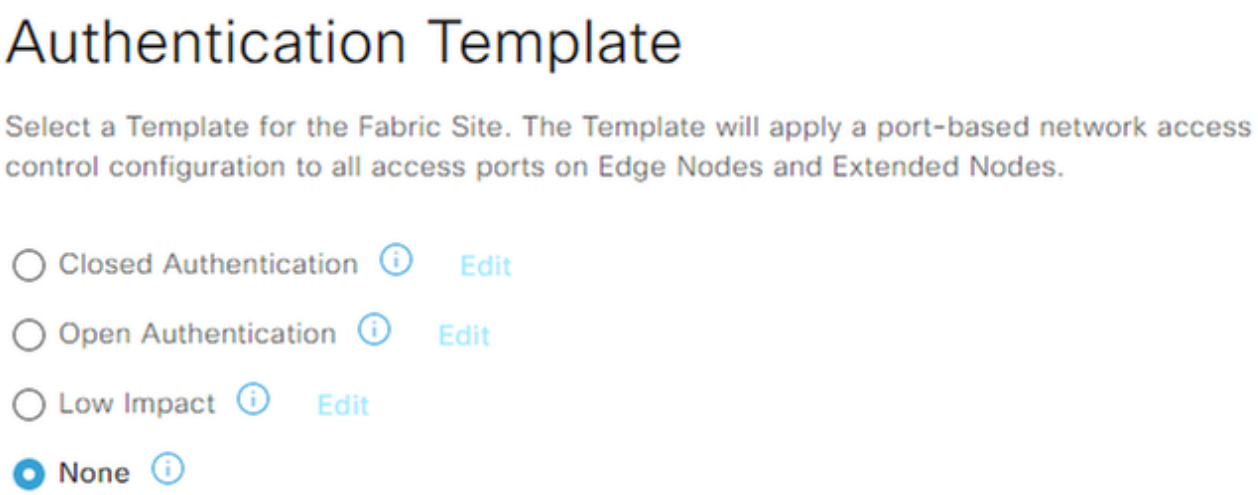
Fabric-Standorte erstellen

Schritt 2. Wählen Sie das Gebäude/Stockwerk für Ihre Fabric-Website:



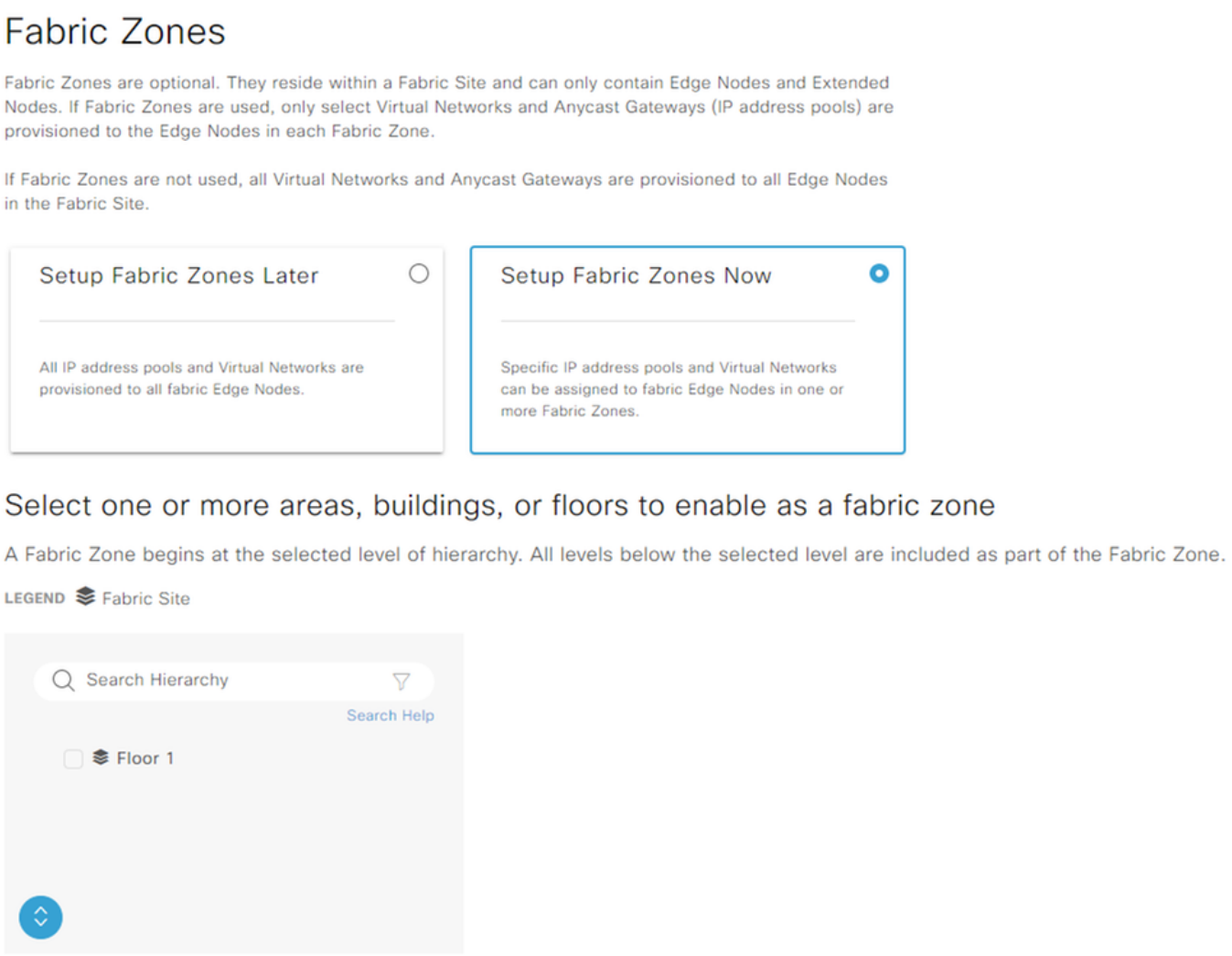
Fabric-Standort auswählen

Schritt 3: Wählen Sie eine Authentifizierungsvorlage aus. In dieser Demo wurde keine angewendet:



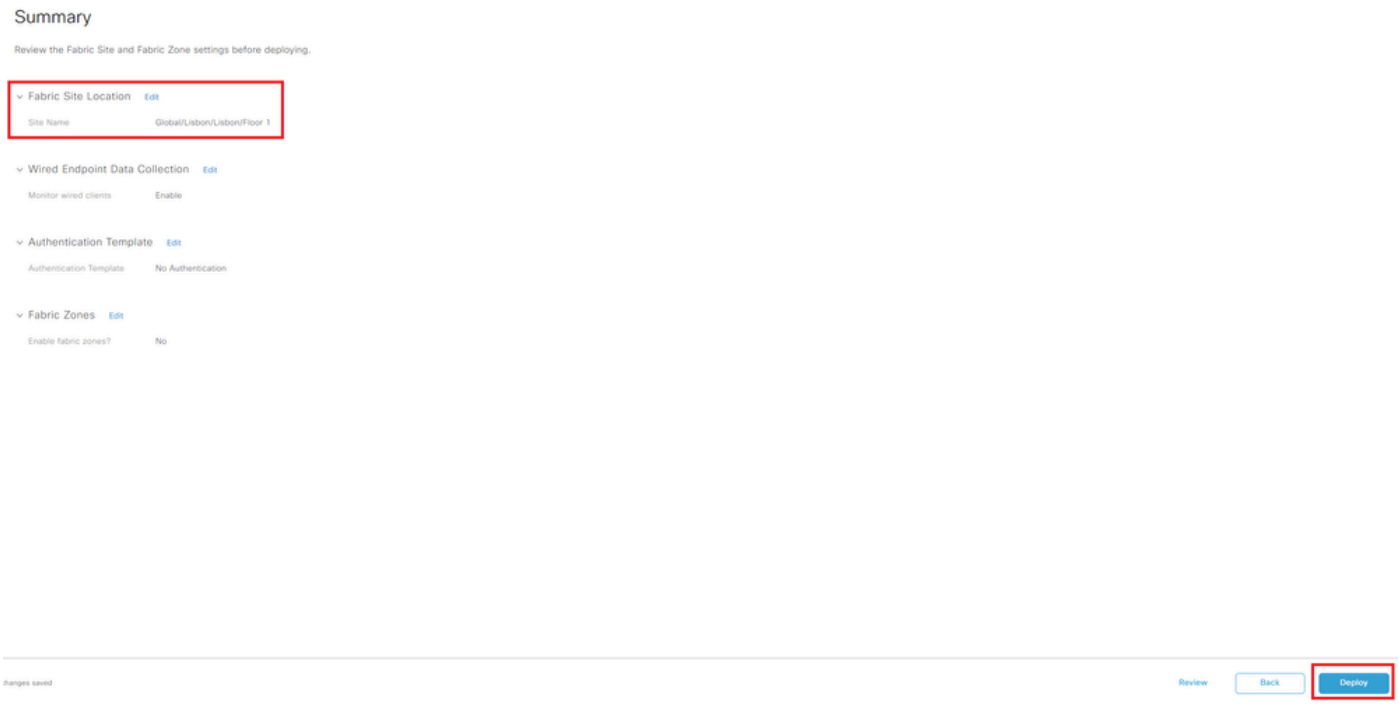
Authentifizierungsvorlage

Schritt 3. Sie können wählen, ob Sie die Fabric-Zone jetzt oder später einrichten möchten:



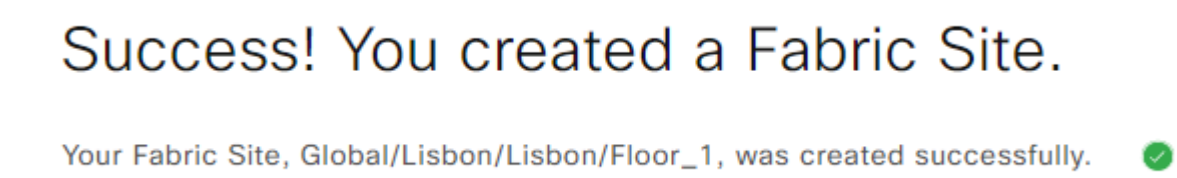
Fabric-Zonen einrichten

Schritt 4: Überprüfen der Einstellungen der Fabric-Zone Wenn alles in Ordnung ist, wählen Sie Bereitstellen:



Fabric-Standort bereitstellen

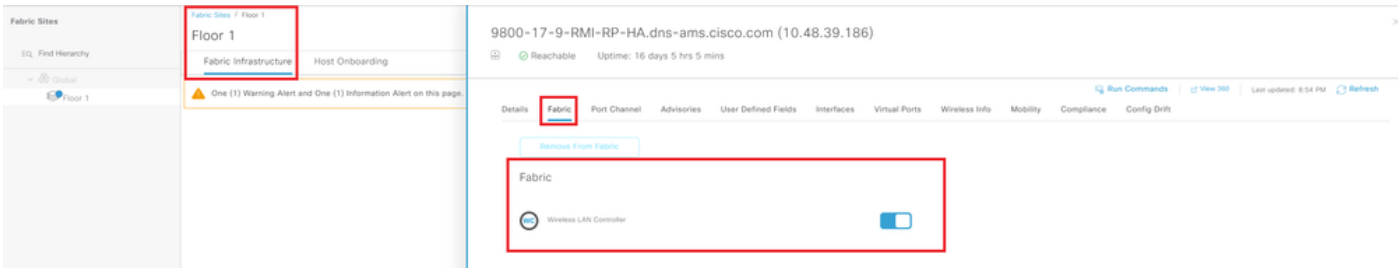
Sie haben einen Fabric-Standort erstellt:



Erstellung des Fabric-Standorts

WLC zur Fabric hinzufügen

Navigieren Sie zu Bereitstellung > Fabric-Standorte, und wählen Sie Ihre Fabric-Website aus. Klicken Sie auf den oberen Rand Ihres WLC, und navigieren Sie zur Registerkarte Fabric. Aktivieren Sie Fabric für den WLC, und wählen Sie Hinzufügen:

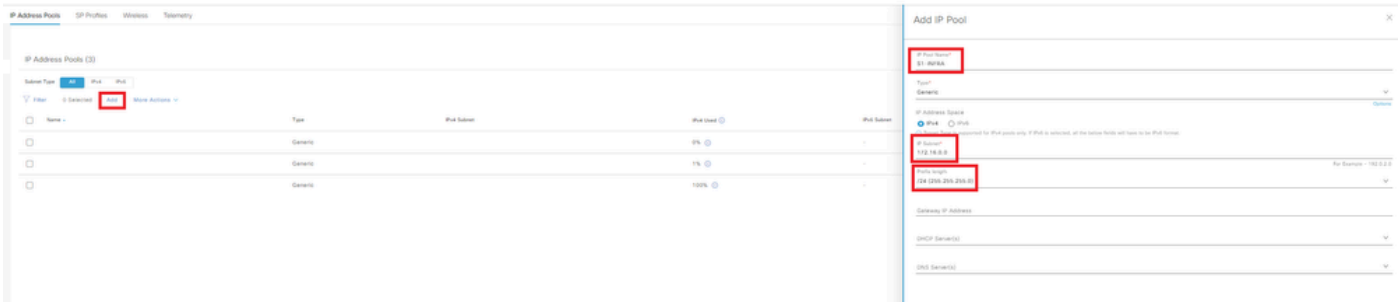


WLC zur Fabric hinzufügen

AP-Beitritt

Schritt 1: Navigieren Sie zu Design > Network Settings > IP Address Pools. Erstellen Sie einen IP-

Adresspool.



IP-Adresspool

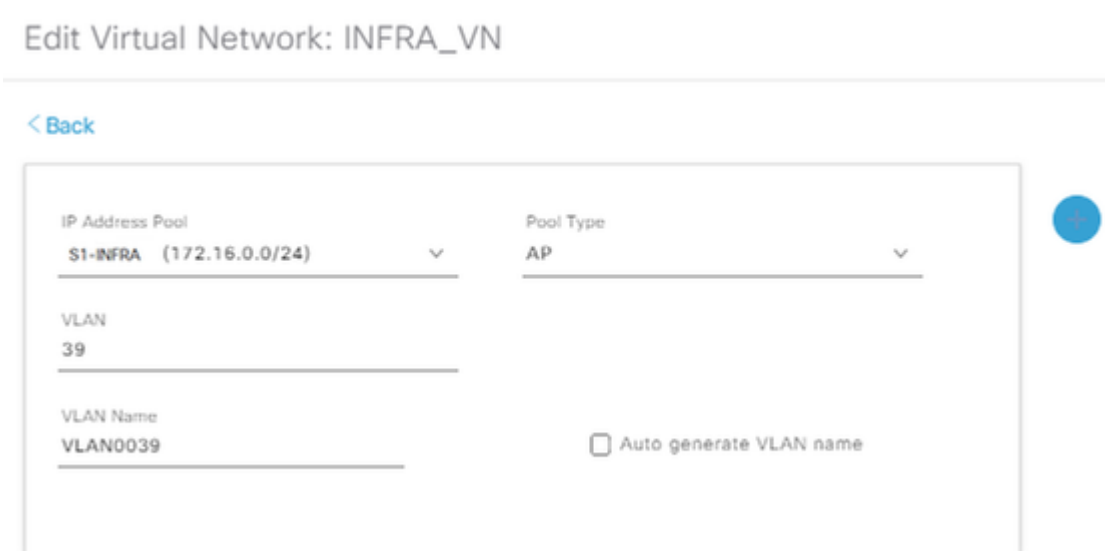
Schritt 2: Navigieren Sie zu Bereitstellung > Fabric-Standorte, und wählen Sie Ihre Fabric-Website aus. Navigieren Sie zu Host Onboarding > Virtual Networks.

INFRA_VN wird eingeführt, um APs einfach zu integrieren. APs befinden sich im Fabric-Overlay, aber INFRA_VN ist der globalen Routing-Tabelle zugeordnet. Nur APs und erweiterte Knoten können zu INFRA_VN gehören. Die Layer-2-Erweiterung wird automatisch aktiviert, und der L2-LISP-Service wird aktiviert.

Wählen Sie INFRA_VN > Hinzufügen aus:

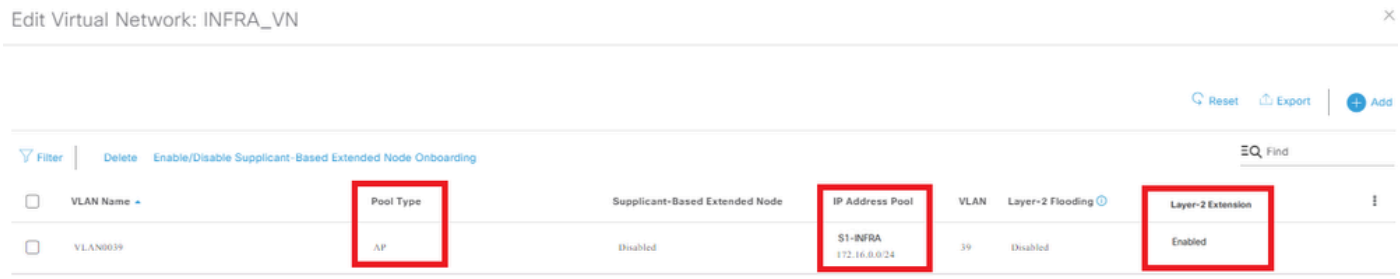
Virtuelles Netzwerk bearbeiten

Schritt 3: Fügen Sie einen IP-Adresspool mit dem Pool-Typ als AP hinzu:



Virtuelles Netzwerk S1-INFRA bearbeiten

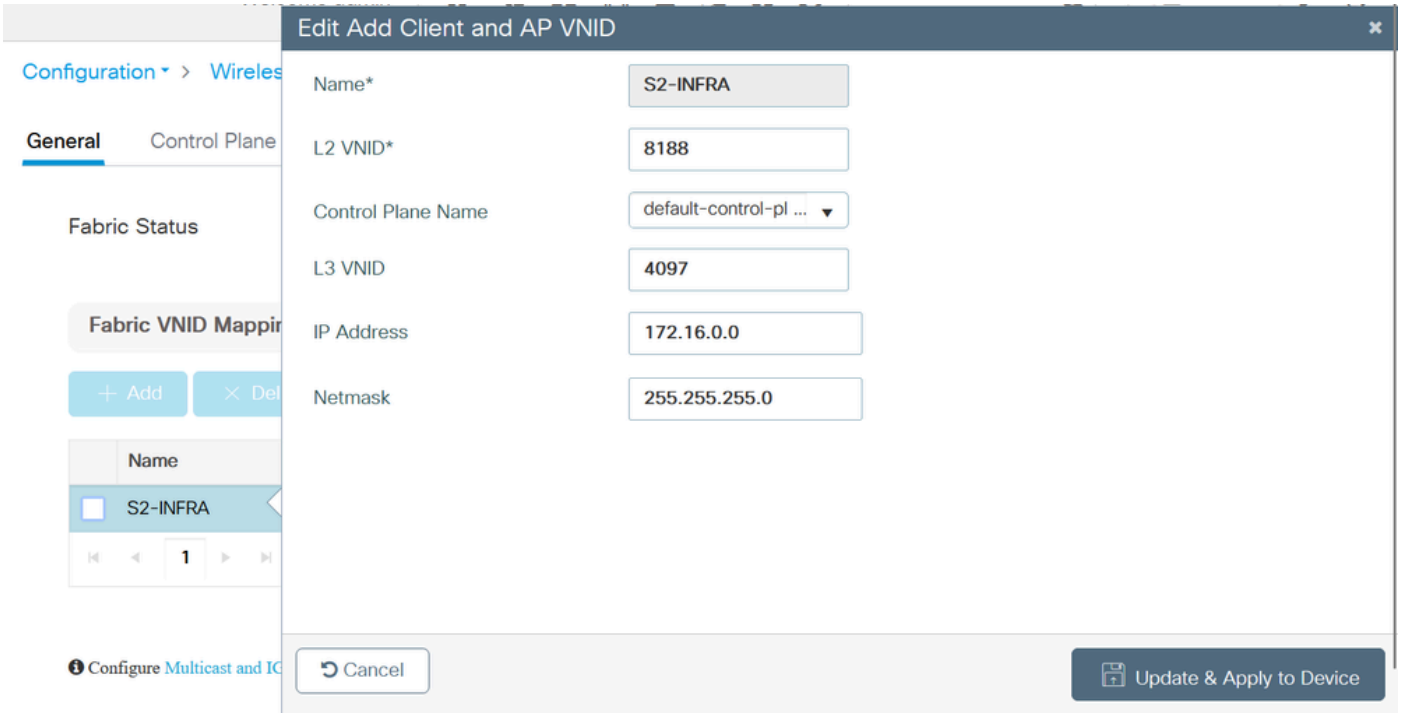
Schritt 4: Überprüfen, ob die Layer-2-Erweiterung aktiviert ist



Virtuelles Netzwerk bearbeiten

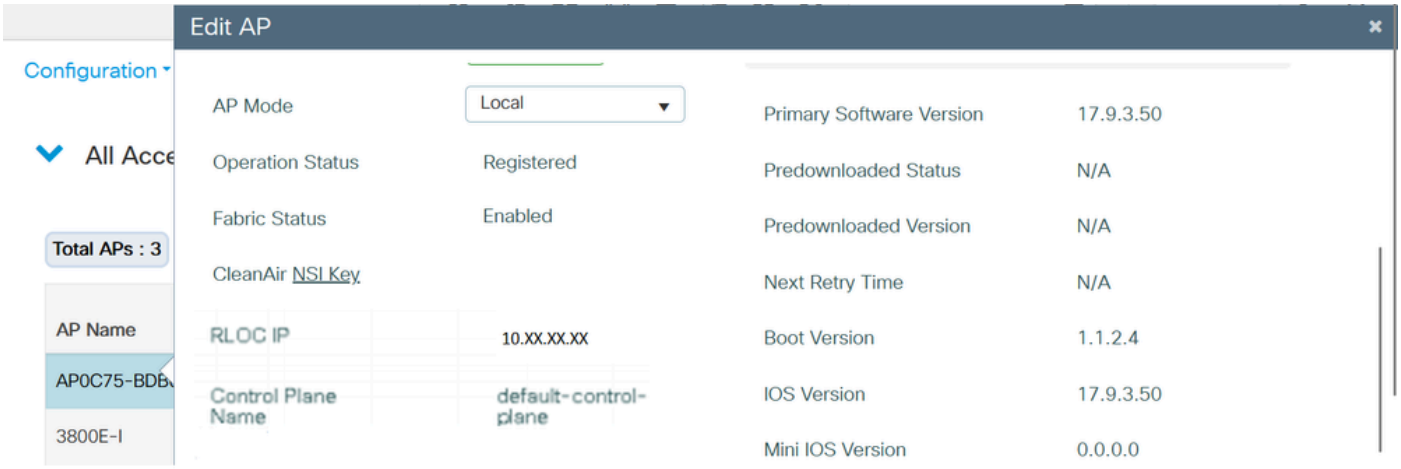
Mit Pool Type = AP und Layer-2-Erweiterung zu ON stellt die Cisco DNA eine Verbindung zum WLC her und setzt die Fabric-Schnittstelle für das AP-Subnetz für L2 und L3 VN_IDs auf VN_ID-Zuordnung.

Schritt 5: Navigieren Sie auf der WLC-GUI zu Configuration > Wireless > Fabric > General (Konfiguration > Wireless > Fabric > Allgemein). Fügen Sie einen neuen Client und eine AP VN_ID hinzu:



Neuen Client und AP VN_ID hinzufügen

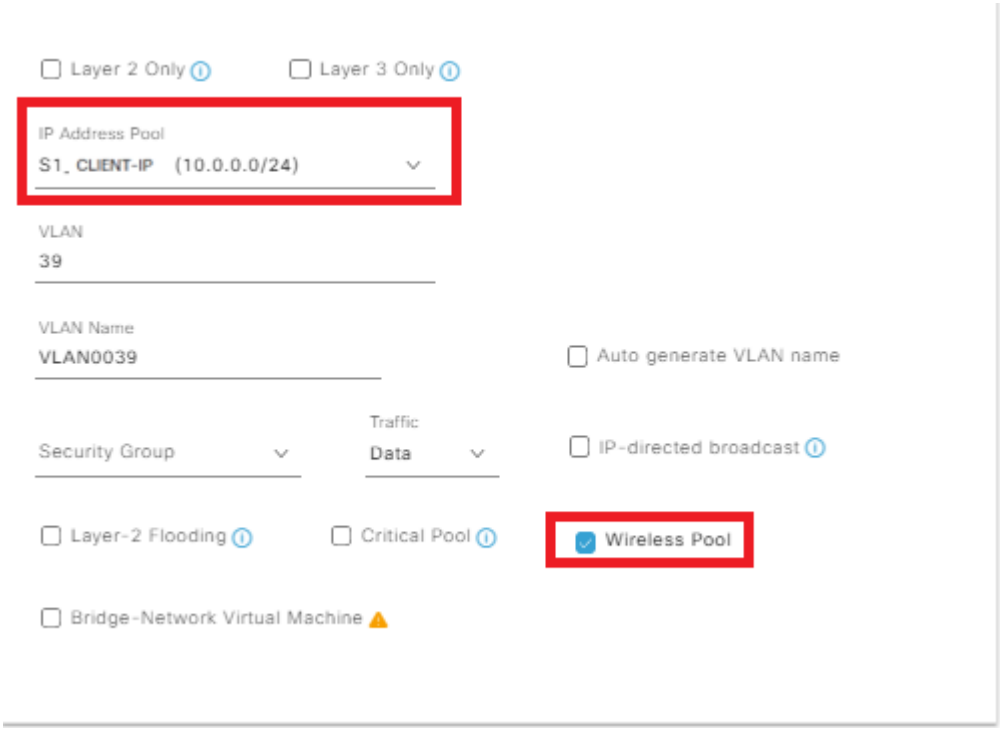
Schritt 6: Navigieren Sie zu Konfiguration > Wireless > Access Points. Wählen Sie einen Access Point aus der Liste aus. Überprüfen Sie, ob der Fabric-Status aktiviert ist, die IP-Adresse der Kontrollebene und der Name der Kontrollebene:



AP-Fabric-Status überprüfen

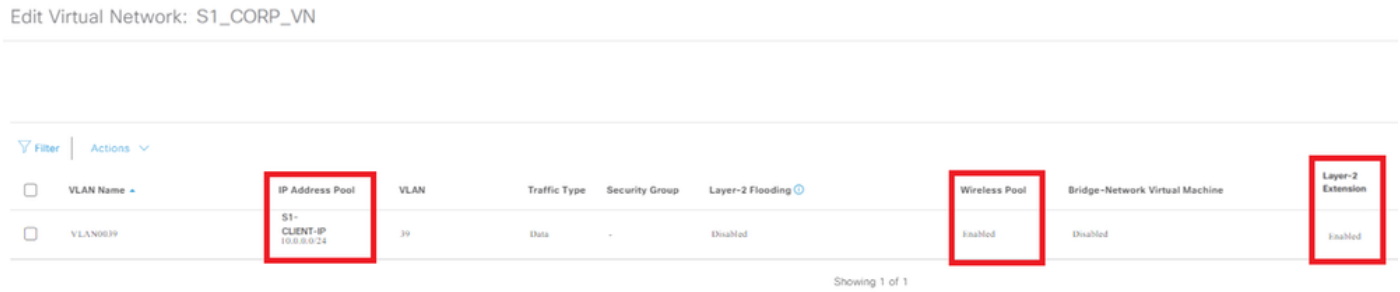
Client integriert

Schritt 1: Fügen Sie den Pool dem virtuellen Netzwerk hinzu, und überprüfen Sie, ob der Umschalter für die Layer-2-Erweiterung ON ist, um die L2-LISP- und Layer-2-Subnetzerweiterung im Client-Pool/Subnetz zu aktivieren. In Cisco DNA 1.3.x ist eine Deaktivierung nicht möglich.



IP-Adresspool hinzufügen

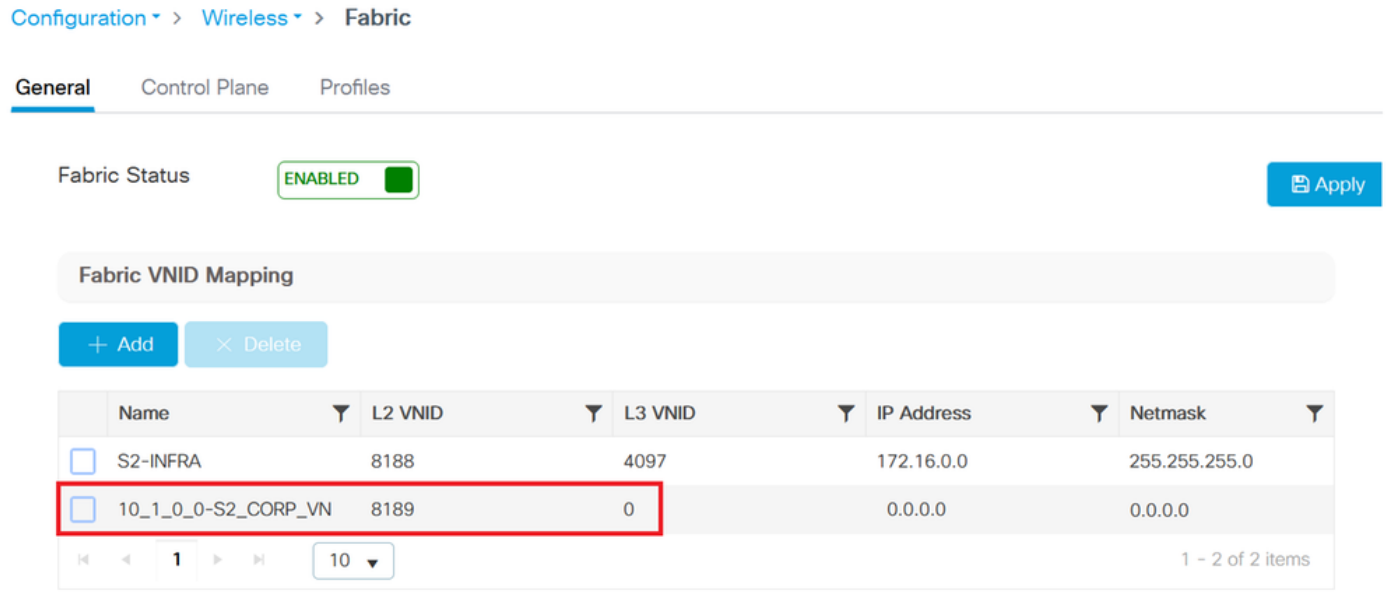
Schritt 2: Überprüfen, ob die Layer-2-Erweiterung und der Wireless-Pool aktiviert sind



Virtuelles Netzwerk bearbeiten

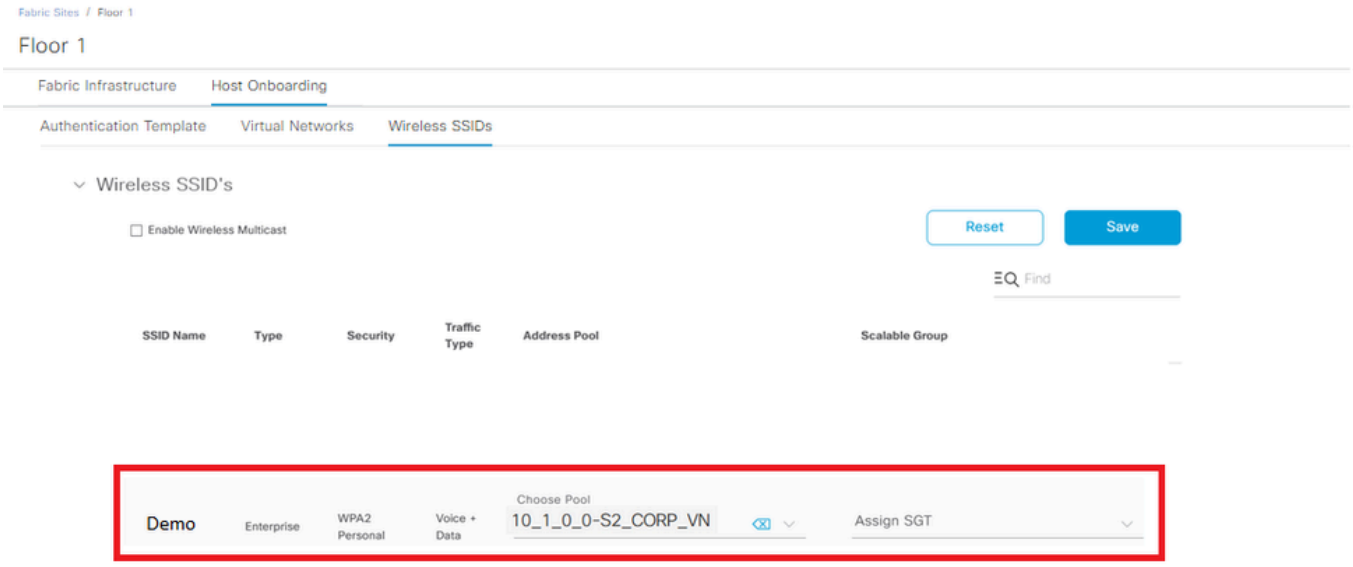
Schritt 3: Navigieren Sie auf der WLC-GUI-Seite zu Configuration > Wireless > Fabric > General (Konfiguration > Wireless > Fabric > Allgemein). Fügen Sie einen neuen Client und AP VN_ID hinzu.

Wenn der Pool dem virtuellen Netzwerk zugewiesen wird, wird die entsprechende Fabric-Schnittstelle zur VNID-Zuordnung an den Controller weitergeleitet. Dies sind alle L2-VNIDs.



Neuen Client und AP VN_ID hinzufügen

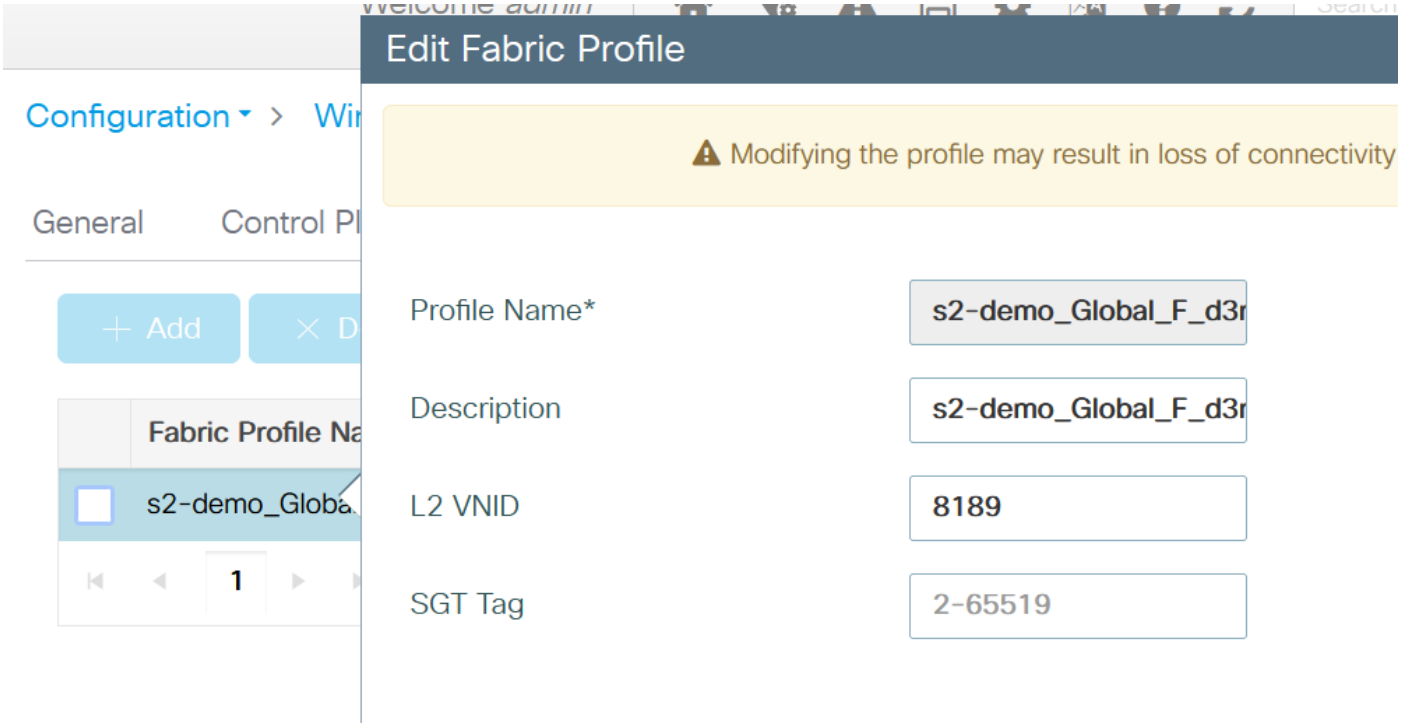
Schritt 4: SSIDs werden dem Pool in den jeweiligen virtuellen Netzwerken zugeordnet:



Zugeordnete SSIDs

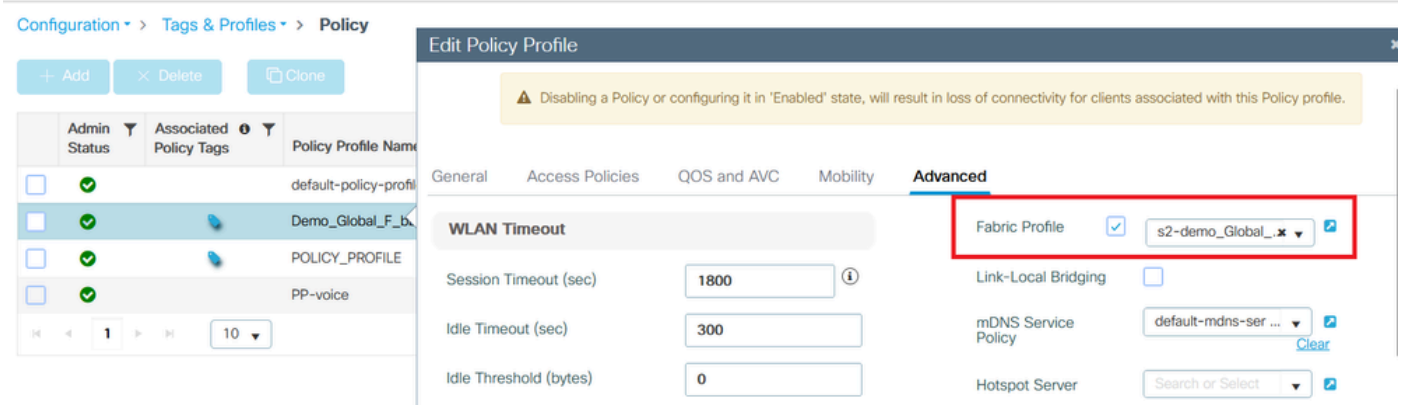
Schritt 5: Ein Fabric-Profil mit der L2-VNID wird zum ausgewählten Pool hinzugefügt, und das Richtlinienprofil wird dem Fabric-Profil zugeordnet. Es wird für Fabric aktiviert.

Navigieren Sie auf der WLC-GUI-Seite zu Configuration > Wireless > Fabric > Profiles.



Fabric-Profil

Schritt 6: Navigieren Sie zu Konfiguration > Tags und Profile > Richtlinie. Überprüfen Sie das dem Richtlinienprofil zugeordnete Fabric-Profil:



Auf der Richtlinie konfiguriertes Fabric-Profil

Überprüfung

Überprüfen der Fabric-Konfiguration auf WLC und Cisco DNA

In der WLC-CLI:

WLC1# show tech

WLC1# show tech wireless

Konfiguration der Kontrollebene:

Router-Schnittstelle

 Locator-Table-Standard

 Locator-Set WLC

  172.16.201.202

  Exit-Locator-Set

  !

 map-server session passive-open WLC

 Site site_uci

  description map-server configured from Cisco DNA-Center

  authentication-key 7 <Schlüssel>

CB1-S1#sh lisp-Sitzung

Sitzungen für VRF-Standard, gesamt: 9, eingerichtet: 5

Peer-Status aktiv/inaktiv ein-/ausgehend

172.16.201.2012:4342 Bis 3d07h 14/14

WLC-Konfiguration:

Wireless-Fabric

Wireless Fabric-Kontrollebene Standard-Kontrollebene

ip address 172.16.2.2 key 0 47aa5a

WLC1# Fabric Map-Server-Zusammenfassung anzeigen

Status der MS-IP-Verbindung

172.16.1.2 UP

WLC1# Zusammenfassung der Wireless-Fabric anzeigen

Fabric-Status: Aktiviert

Kontrollebene:

Name IP-Adresse Schlüsselstatus

---

default-control-plane 172.16.2.2 47aa5a Up

Navigieren Sie auf der WLC-GUI zu Configuration > Wireless > Fabric, und überprüfen Sie, ob der Fabric-Status aktiviert ist.

Navigieren Sie zu Konfiguration > Wireless > Access Points. Wählen Sie einen Access Point aus der Liste aus. Überprüfen Sie, ob der Fabric-Status aktiviert ist.

Navigieren Sie auf der Cisco DNA zu Provisioning > Fabric Sites, und überprüfen Sie, ob Sie eine Fabric Site verwenden. Navigieren Sie an diesem Fabric-Standort zu Fabric Infrastructure > Fabric, und überprüfen Sie, ob der WLC als Fabric aktiviert ist.

Fehlerbehebung

Client erhält keine IP-Adresse

Schritt 1: Überprüfen der Fabric der SSID Navigieren Sie in der WLC-GUI zu Configuration > Tags & Profiles > Policy. Wählen Sie die Richtlinie aus, und navigieren Sie zu Advanced (Erweitert). Überprüfen Sie, ob das Fabric-Profil aktiviert ist.

Schritt 2: Überprüfen Sie, ob der Client im IP-Lernstatus feststeckt. Navigieren Sie auf der WLC-GUI zu Monitoring > Wireless > Clients. Überprüfen Sie den Client-Status.

Schritt 3: Überprüfen Sie, ob die Richtlinie DHCP erforderlich ist.

Schritt 4: Wenn der Datenverkehr lokal zwischen dem AP-Edge-Knoten umgeschaltet wird, sammeln Sie AP-Protokolle (client-trace) für die Client-Verbindung. Überprüfen Sie, ob die DHCP-Erkennung weitergeleitet wird. Wenn kein DHCP-Angebot eingeht, ist am Edge-Knoten etwas falsch. Wenn der DHCP-Server nicht weitergeleitet wird, liegt am Access Point ein Fehler vor.

Schritt 5: Sie können einen EPC am Edge-Knoten-Port erfassen, um die DHCP-Ermittlungspakete anzuzeigen. Wenn die DHCP-Ermittlungspakete nicht angezeigt werden, liegt das Problem am Access Point.

SSID wird nicht übertragen

Schritt 1: Überprüfen Sie, ob die AP-Funkmodule ausgefallen sind.

Schritt 2: Überprüfen Sie, ob das WLAN den Status hat und die SSID für Broadcast aktiviert ist.

Schritt 3: Überprüfen der AP-Konfiguration, wenn AP Fabric-fähig ist Navigieren Sie zu Configuration > Wireless > Access Points, wählen Sie einen Access Point aus, und auf der Registerkarte General (Allgemein) werden Fabric Status Enabled (Fabric-Status aktiviert) und die RLOC-Informationen angezeigt.

Schritt 4: Navigieren Sie zu Konfiguration > Wireless > Fabric > Kontrollebene. Überprüfen Sie, ob die Kontrollebene konfiguriert ist (mit der IP-Adresse).

Schritt 5: Navigieren Sie zu Konfiguration > Tags und Profile > Richtlinie. Wählen Sie die Richtlinie aus, und navigieren Sie zu Advanced (Erweitert). Überprüfen Sie, ob das Fabric-Profil aktiviert ist.

Schritt 6: Navigieren Sie zur Cisco DNA, und wiederholen Sie die Schritte unter "SSID erstellen und WLC bereitstellen". Die Cisco DNA muss die SSID erneut an den WLC senden.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

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