Implementazione dell'accesso definito dal software per wireless con DNA

Sommario

Introduzione

Questo documento descrive come implementare SDA per la tecnologia wireless relativa ai WLC abilitati per fabric e accedere ai LAP su Cisco DNA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione dei Wireless LAN Controller (WLC) 9800
- LAP (Lightweight Access Point)
- Cisco DNA

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Accesso SD

L'accesso definito dal software stabilisce e applica automaticamente i criteri di sicurezza in tutta la rete, con regole dinamiche e segmentazione automatizzata, e consente all'utente finale di controllare e configurare il modo in cui gli utenti si connettono alla rete. SD-Access stabilisce un livello iniziale di attendibilità per ogni endpoint connesso e lo controlla continuamente per verificarne nuovamente il livello di attendibilità. Se un endpoint non si comporta normalmente o viene rilevata una minaccia, l'utente finale può contenerlo immediatamente e intervenire prima che si verifichi la violazione, riducendo i rischi aziendali e proteggendo le risorse. Soluzione completamente integrata e facile da installare e configurare su reti nuove e distribuite.

SD-Access è una tecnologia Cisco che rappresenta un'evoluzione della tradizionale rete di campus che offre una rete basata su intent (IBN) e il controllo centralizzato delle policy con l'utilizzo di componenti Software-Defined Networking (SDN).

Tre pilastri di accesso SD incentrati sulla rete:

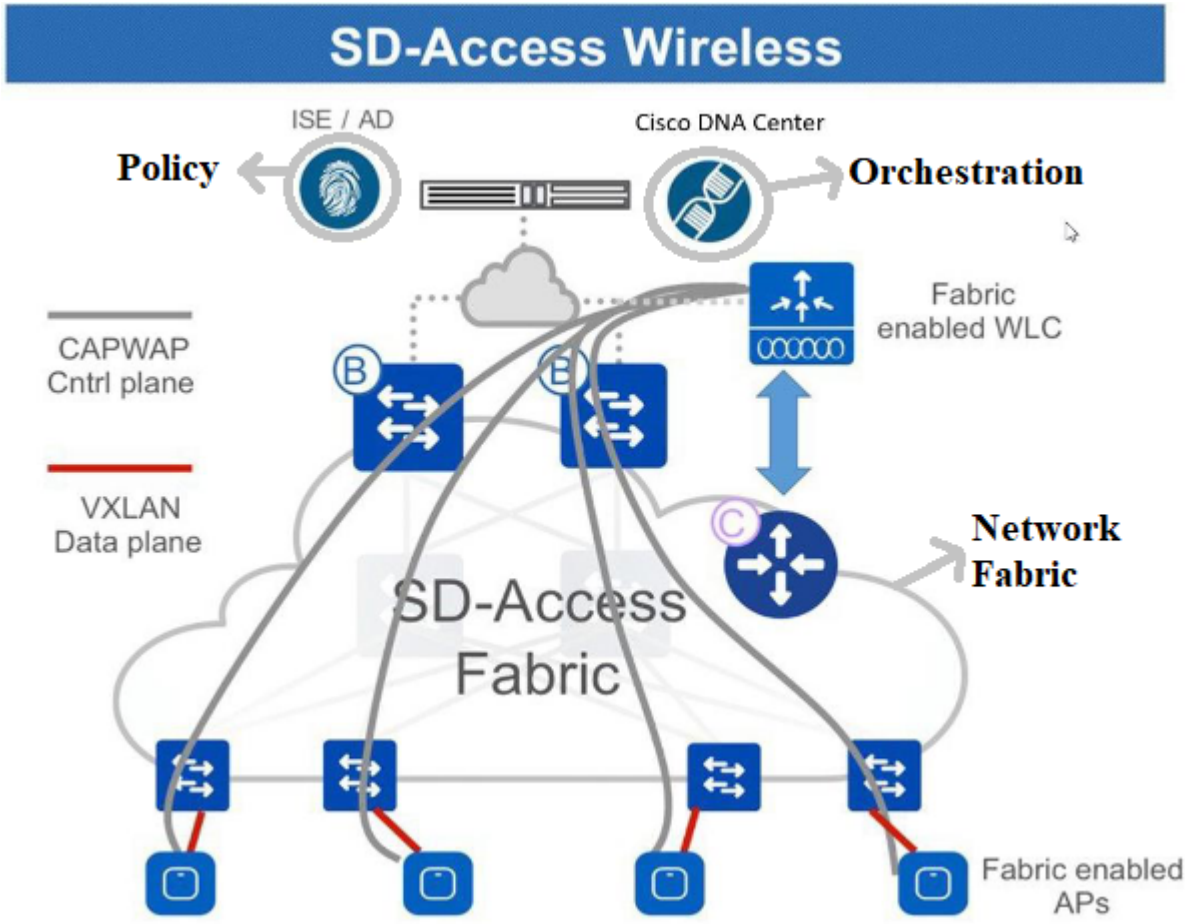
1. Un fabric di rete: Si tratta di un'astrazione della rete stessa che supporta sovrapposizioni programmabili e virtualizzazione. La struttura di rete supporta sia l'accesso cablato che wireless e consente di ospitare più reti logiche segmentate tra loro e definite in base alle finalità aziendali.

2. Orchestrazione: Cisco DNA è il motore di orchestrazione di SDA. Cisco DNA funziona come un controller SDN. Implementa policy e modifiche alla configurazione nel fabric. Incorpora inoltre uno strumento che supporta la progettazione della rete e le operazioni di telemetria di rete in tempo reale e l'analisi delle prestazioni tramite DNA Assurance. Il ruolo di Cisco DNA è quello di orchestrare il fabric di rete per apportare modifiche alle policy e all'intento della rete per la sicurezza, la qualità del servizio (QoS) e la microsegmentazione.
3. Policy: Identity Services Engine (ISE) è lo strumento che definisce i criteri di rete. ISE organizza la segmentazione di dispositivi e nodi in reti virtuali. ISE definisce anche i SGT (Scalable Group Tag) utilizzati dai dispositivi di accesso per segmentare il traffico degli utenti quando entrano nella struttura. Le SGR sono responsabili di implementare la policy di microsegmentazione definita da ISE.

L'architettura SDA è basata su un'orchestrazione centralizzata. Le combinazioni di Cisco DNA come motore di orchestrazione programmabile, ISE come motore delle regole e una nuova generazione di switch programmabili lo rendono un sistema fabric molto più flessibile e gestibile di qualsiasi cosa sia venuta prima.

Nota: Questo documento tratta in modo specifico di SD-Access Wireless.

Il fabric di rete è composto dai seguenti elementi:

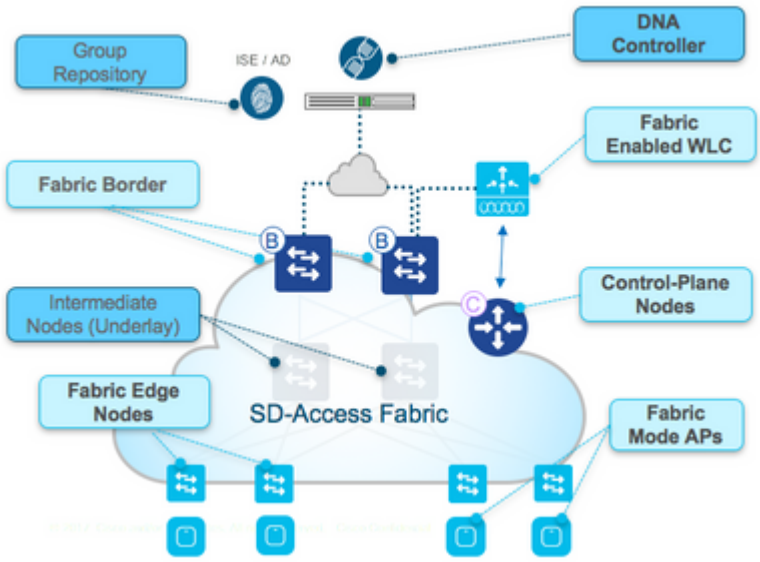


Elementi di Network Fabric

L'integrazione wireless con il fabric comporta diversi vantaggi per la rete wireless, ad esempio: la semplificazione, la mobilità con subnet allungate tra siti fisici; e la microsegmentazione con regole centralizzate che siano coerenti su entrambi i domini cablati e wireless. Consente inoltre al controllore di scartare il data plane per inoltrare i compiti mentre continua a funzionare come servizio centralizzato e control plane per la rete wireless. Di conseguenza, la scalabilità del controller wireless è in realtà aumentata perché non è più necessario elaborare il traffico del data plane, come avviene per il modello FlexConnect.

Architettura wireless ad accesso SD

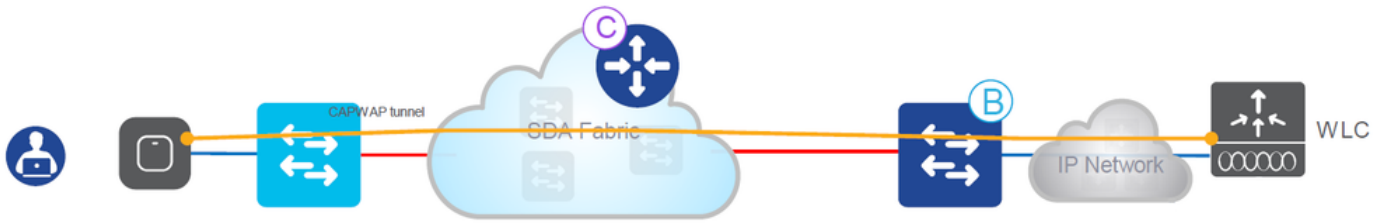
Panoramica



Panoramica su SDA

Esistono due modelli di distribuzione wireless principali supportati da SDA:

La prima è un metodo OTT (over-the-top), un'implementazione CAPWAP tradizionale connessa su una rete cablata fabric. Il fabric SDA trasporta il controllo CAPWAP e il traffico del data plane al controller wireless:

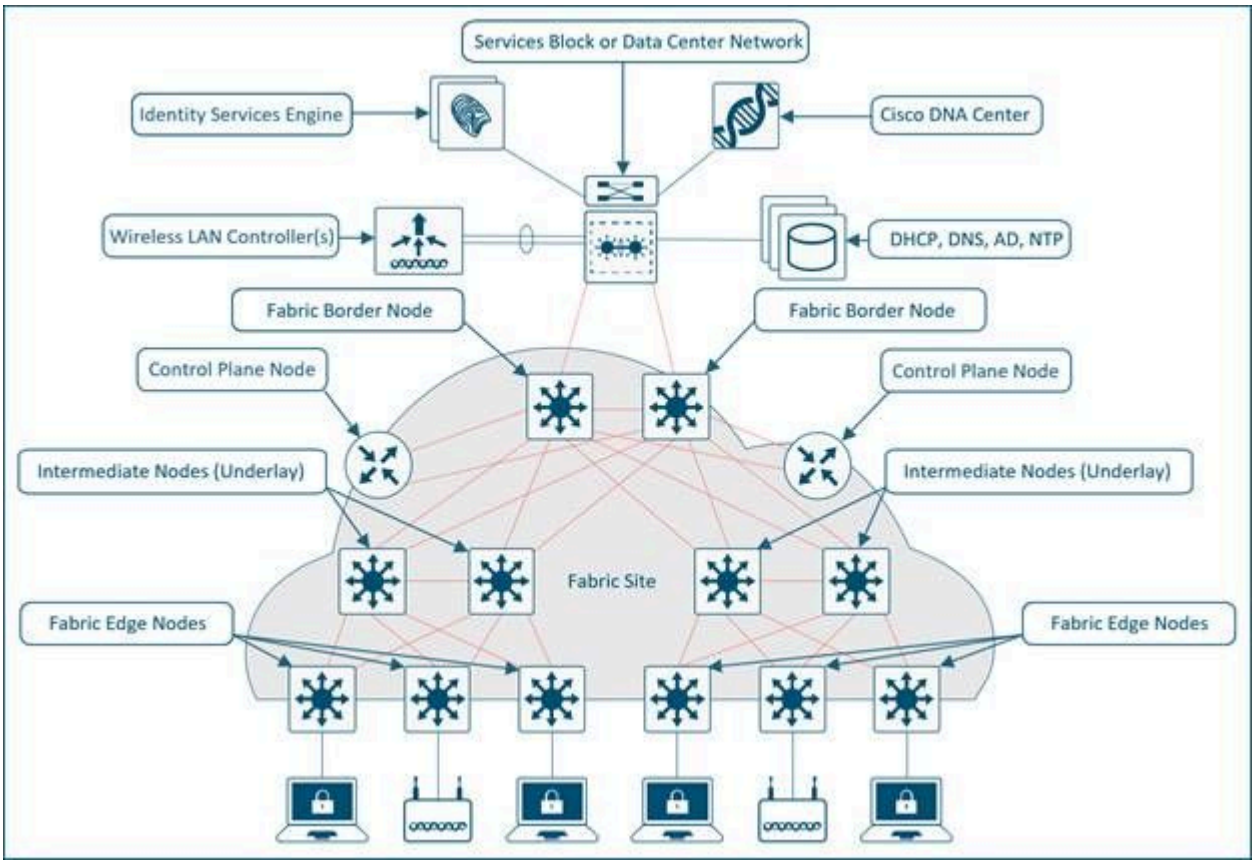


Metodo Over-The-Top

In questo modello di distribuzione, il fabric SDA è una rete di trasporto per il traffico wireless (un modello spesso implementato nelle migrazioni). L'access point funziona in modo molto simile alla modalità locale classica: sia il controllo CAPWAP che i piani dati terminano sul controller, il che significa che il controller non partecipa direttamente al fabric. Questo modello viene spesso

utilizzato quando viene eseguita la migrazione degli switch cablati al fabric SDA, ma la rete wireless non è ancora pronta per l'integrazione completa della sovrapposizione del fabric.

Gli altri modelli di distribuzione sono il modello SDA completamente integrato. La rete wireless è completamente integrata nel fabric e partecipa agli overlay; consente a diverse WLAN di far parte di diverse reti virtuali (VN). Il controller wireless gestisce solo il control plane CAPWAP (per gestire i punti di accesso) e il data plane CAPWAP non viene recapitato al controller:



Modello SDA completamente integrato

Il piano dati wireless viene gestito in modo simile agli switch cablati: ogni punto di accesso incapsula i dati nella VXLAN e li invia a un nodo periferico della struttura, dove vengono quindi inviati a un altro nodo periferico della struttura. I controller wireless devono essere configurati come controller fabric, il che rappresenta una modifica rispetto al loro normale funzionamento.

I controller abilitati all'infrastruttura comunicano con il control plane dell'infrastruttura, registrano gli indirizzi MAC dei client di layer 2 e le informazioni VNI (Virtual Network Identifier) di layer 2. Gli access point sono responsabili della comunicazione con gli endpoint wireless e assistono il data plane VXLAN dall'incapsulamento e dal traffico di deincapsulamento.

Ruoli e terminologia SDA

Il fabric di rete è composto dai seguenti elementi:

- Nodo Control-Plane: Si tratta del sistema di mappatura della posizione (database host) che fa parte del piano di controllo del protocollo LISP (Location Separator Protocol), che gestisce l'identità dell'endpoint (EID) alle relazioni di posizione (o alle relazioni tra dispositivi). Il

control plane può essere un router dedicato che fornisce le funzioni del control plane oppure può coesistere con altri elementi della rete fabric.

- Nodi del bordo dell'infrastruttura: In genere un router che funziona al confine tra le reti esterne e il fabric SDA, che fornisce servizi di routing alle reti virtuali nel fabric. Collega le reti esterne di layer 3 al fabric SDA.
- Nodi Fabric Edge: Dispositivo all'interno della struttura che connette dispositivi non di struttura, ad esempio switch, AP e router alla struttura SDA. Si tratta dei nodi che creano le sovrapposizioni virtuali dei tunnel e delle VN con la VXLAN (Virtual eXtensible LAN) e impongono le SGT al traffico associato alla struttura. Le reti su entrambi i lati del lato del fabric si trovano all'interno della rete SDA. Collegano gli endpoint cablati al fabric SD-Access.
- Nodi intermedi: Questi nodi si trovano all'interno del nucleo del fabric SDA e si connettono a nodi di bordo o di bordo. I nodi intermedi si limitano a inoltrare il traffico SDA come pacchetti IP, ignari del fatto che vi siano più reti virtuali coinvolte.
- WLC fabric: Controller wireless abilitato per il fabric che partecipa al control plane SDA ma non elabora il data plane CAPWAP.
- AP modalità fabric: Punti di accesso abilitati per l'infrastruttura. Il traffico wireless è incapsulato tramite VXLAN sull'access point, che consente di inviarlo al fabric tramite un nodo edge.
- Cisco DNA (DNAC): Enterprise SDN Controller per la rete di sovrapposizione del fabric SDA (Software Defined Access) ed è responsabile sia delle attività di automazione che delle attività di verifica. Può anche essere utilizzato per alcune attività di automazione e correlate per i dispositivi di rete che costituiscono l'underlay (che non è correlato a SDA).
- ISE: Identity Services Engine (ISE) è una piattaforma di policy avanzata in grado di supportare una vasta gamma di ruoli e funzioni, non ultima quella del server di autenticazione, autorizzazione e accounting (AAA). ISE interagisce in genere con Active Directory (AD), ma è possibile configurare gli utenti sia localmente che sulla stessa ISE per installazioni di dimensioni inferiori.

Nota: Il control plane è un componente dell'infrastruttura critica dell'architettura SDA, pertanto si consiglia di implementarlo in modo resiliente.

Reti Underlay e Overlay

L'architettura SDA utilizza la tecnologia fabric che supporta le reti virtuali programmabili (overlay networks) che vengono eseguite su una rete fisica (underlay network).

Un tessuto è un Overlay.

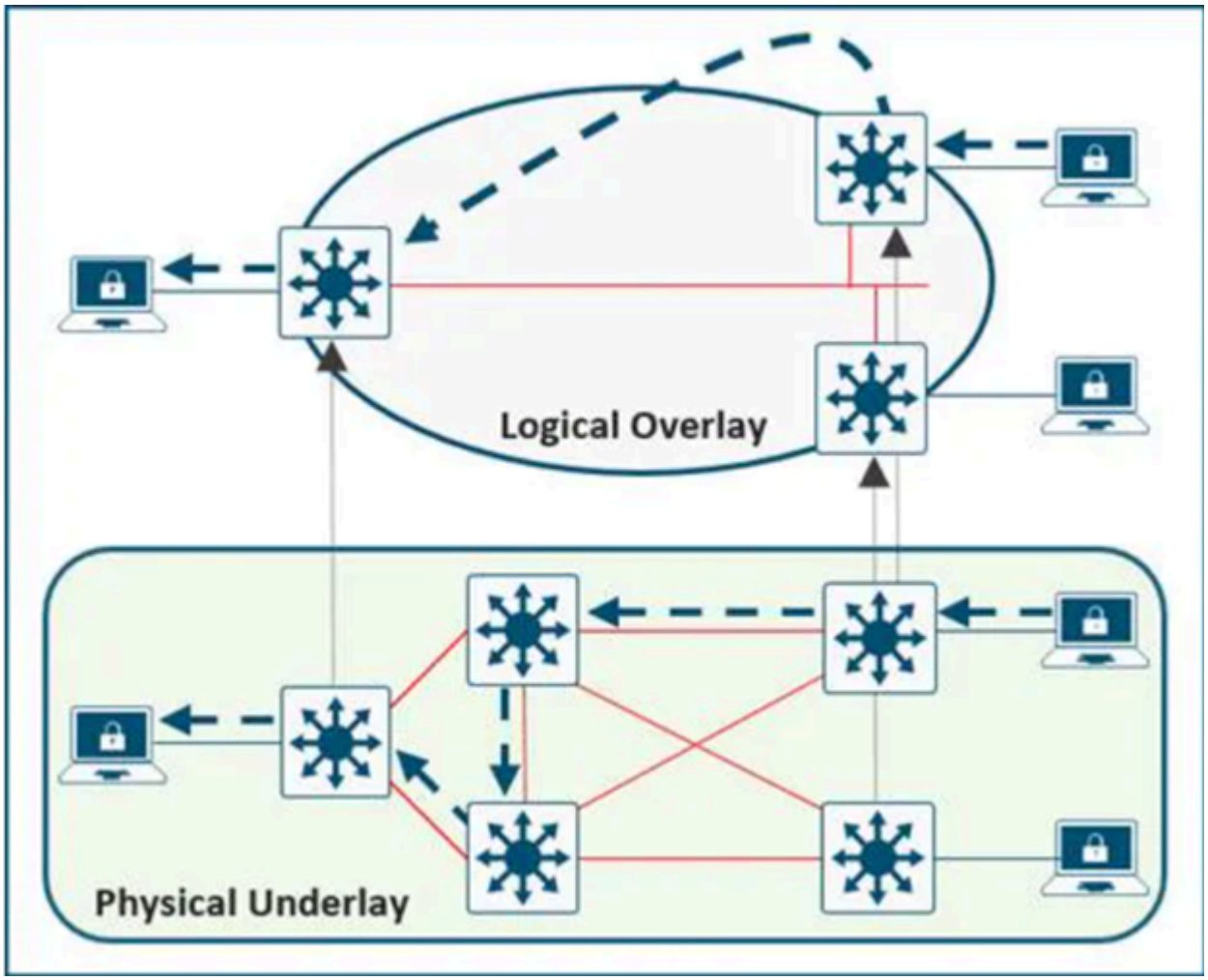
Una rete di overlay è una topologia logica utilizzata per connettere virtualmente i dispositivi, costruita su una topologia di underlay fisica arbitraria. Vengono utilizzati attributi di inoltro alternativi per fornire servizi aggiuntivi non forniti dall'applicazione sottostante. Viene creato sulla parte superiore della base per creare una o più reti virtualizzate e segmentate. Grazie alla natura software delle sovrapposizioni, è possibile collegarle in modo molto flessibile senza i vincoli della connettività fisica. È un modo semplice per applicare i criteri di sicurezza, poiché la sovrapposizione può essere programmabile per avere un singolo punto di uscita fisico (il nodo del bordo dell'infrastruttura) e un firewall può essere utilizzato per proteggere le reti dietro di esso (se possono essere individuate). L'overlay incapsula il traffico con l'uso della VXLAN. VXLAN incapsula frame completi di layer 2 per il trasporto attraverso la struttura sottostante con ciascuna rete di sovrapposizione identificata da un VXLAN Network Identifier (VNI). Le strutture sovrapposte tendono ad essere complesse e richiedono un notevole sovraccarico da parte degli amministratori sulle nuove reti virtuali installate o per implementare i criteri di sicurezza.

Esempi di sovrapposizioni di rete:

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

Una rete Underlay è definita dai nodi fisici, quali switch, router e punti di accesso wireless, utilizzati per distribuire la rete SDA. Tutti gli elementi di rete dell'alloggiamento devono stabilire la connettività IP tramite l'uso di un protocollo di routing. Anche se è improbabile che la rete sottostante utilizzi il tradizionale modello di accesso, distribuzione e core, deve utilizzare una base Layer 3 ben progettata che offra prestazioni affidabili, scalabilità ed elevata disponibilità.

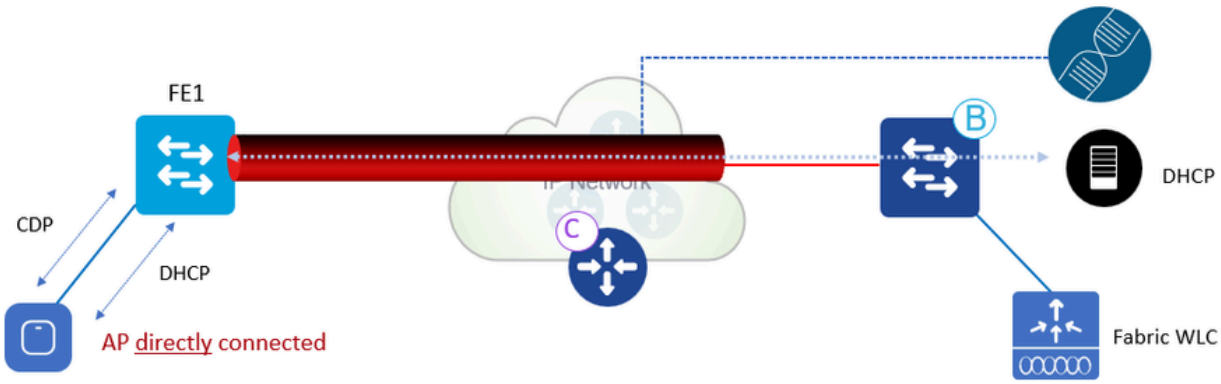
Nota: SDA supporta IPv4 nella rete sottostante e IPv4 e/o IPv6 nelle reti sovrapposte.



Reti Underlay e Overlay

Workflow di base

Join AP



Flusso di lavoro di aggiunta AP

Flusso di lavoro di aggiunta AP:

1. L'amministratore configura il pool AP in DNAC in INFRA_VN. Cisco DNA esegue il pre-

provisioning di una configurazione su tutti i nodi Fabric Edge per l'integrazione automatica dei punti di accesso.

2. L'access point è collegato alla rete elettrica e si accende. Fabric Edge scopre di essere un access point tramite CDP e applica la macro per assegnare (o il modello di interfaccia) alla porta dello switch la VLAN corretta.

3. AP ottiene un indirizzo IP tramite DHCP nella sovrapposizione.

4. Fabric Edge registra l'indirizzo IP e l'indirizzo MAC (EID) degli access point e aggiorna il Control Plane (CP).

5. AP apprende l'IP dei WLC con i metodi tradizionali. L'access point fabric viene aggiunto come access point in modalità locale.

6. Il WLC verifica se è compatibile con la struttura (access point Wave 2 o Wave 1).

7. Se l'access point è supportato per l'infrastruttura, WLC chiede all'access point se è connesso all'infrastruttura.

8. Il Control Plane (CP) risponde al WLC con RLOC. Questo significa che il punto di accesso è collegato al fabric e viene visualizzato come "Fabric enabled".

9. WLC esegue una registrazione LISP L2 per AP in CP (ossia una registrazione client sicura "speciale" AP). Viene utilizzato per passare importanti informazioni sui metadati dal WLC al Fabric Edge.

10. In risposta a questa registrazione proxy, Control Plane (CP) notifica Fabric Edge e passa i metadati ricevuti dal WLC (flag che indica che si tratta di un access point e l'indirizzo IP dell'access point).

11. Fabric Edge elabora le informazioni, apprende di essere un access point e crea un'interfaccia tunnel VXLAN per l'IP specificato (ottimizzazione: il lato switch è pronto per l'aggiunta dei client).

I comandi debug/show possono essere utilizzati per verificare e convalidare il flusso di lavoro del join AP.

Piano di controllo

debug lisp control-plane all

show lisp instance-id <ID istanza L3> server ipv4 (deve mostrare l'indirizzo IP dell'access point registrato dallo switch periferico a cui è connesso l'access point).

show lisp instance-id <L2 instance id> server ethernet (deve mostrare la radio AP, nonché l'indirizzo MAC ethernet, la radio AP registrata dal WLC e la mac ethernet dallo switch periferico a cui è connesso l'access point).

Edge switch

debug access-tunnel all

debug lisp control-plane all

show access-tunnel summary

show lisp instance < L2 instance id> ethernet database wlc access-points (visualizzare qui la radio mac del punto di accesso).

WLC

mostra riepilogo ap infrastruttura

Debug 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

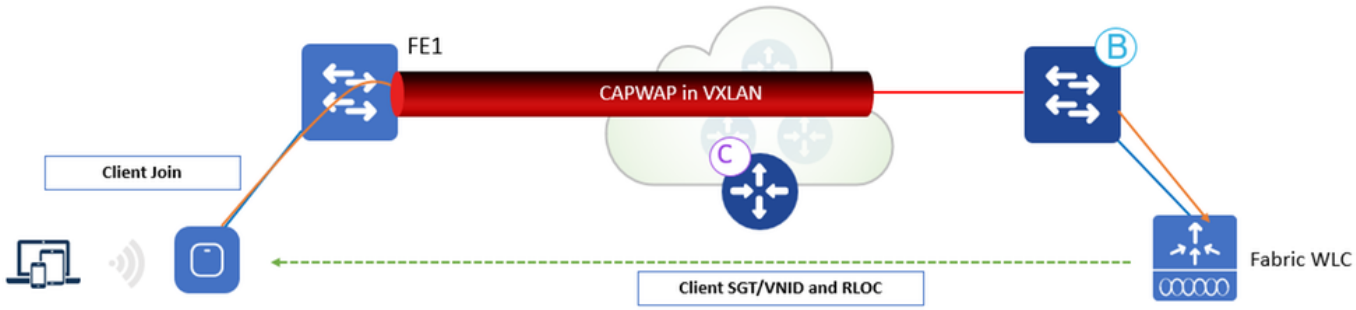
set platform software trace wncd chassis active r0 lisp-agent-ha debug

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

Access Point

show ip tunnel fabric

Client integrato



Flusso di lavoro integrato nel client:

1. Il client esegue l'autenticazione su una WLAN abilitata per Fabric. WLC ottiene SGT da ISE, aggiorna l'access point con il client L2VNID e SGT insieme all'IP RLOC. Il WLC conosce il RLOC dell'access point dal database interno.

2. Il proxy WLC registra le informazioni L2 del client in CP; Questo è il messaggio LISP modificato per passare informazioni aggiuntive, come il client SGT.

3. Fabric Edge riceve la notifica da CP e aggiunge l'indirizzo MAC client in L2 alla tabella di inoltro e va a recuperare la policy da ISE basata sul SGT client.

4. Il client avvia la richiesta DHCP.

5. AP incapsula il pacchetto nella VXLAN con le informazioni VNI L2.

6. Fabric Edge mappa il VNID L2 all'interfaccia VLAN e inoltra il DHCP nella sovrapposizione (come per un client Fabric cablato).

7. Il client riceve un indirizzo IP da DHCP.

8. Lo snooping DHCP (e/o ARP per statico) attiva la registrazione dell'EID del client da parte del perimetro della struttura al PC.

I comandi debug/show possono essere usati per verificare e convalidare il flusso di lavoro onboard del client.

Piano di controllo

debug lisp control-plane all

Edge switch

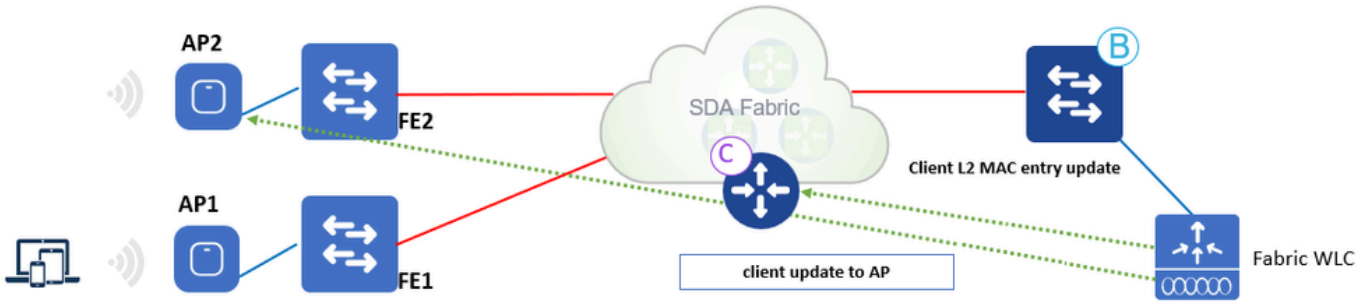
debug lisp control-plane all

pacchetto/evento di snooping ip dhcp di debug

WLC

Per la comunicazione LISP, sono presenti gli stessi debug di AP join.

Roam client



Flusso di lavoro roaming client

Flusso di lavoro roaming client:

1. Il client esegue il roaming verso AP2 su FE2 (roaming inter-switch). Il WLC riceve una notifica dall'access point.

2. WLC aggiorna la tabella di inoltro sull'access point con le informazioni sul client (SGT, RLOC).

3. WLC aggiorna la voce MAC L2 in CP con il nuovo RLOC Fabric Edge 2.

4. CP comunica quindi:

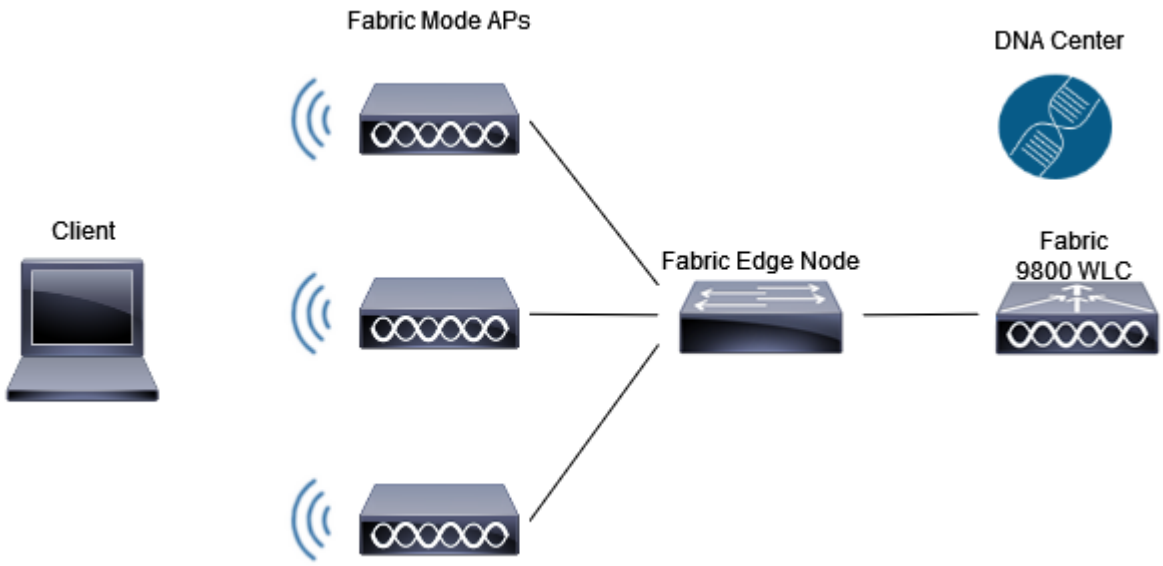
- Fabric Edge FE2 (roaming verso lo switch) per aggiungere l'indirizzo MAC del client alla tabella di inoltro che punta al tunnel VXLAN.
- Fabric Edge FE1 (switch da roaming) per eseguire la pulizia del client wireless.

5. Fabric Edge aggiorna la voce L3 (IP) nel database CP in base al traffico ricevuto.

6. Il roaming è sul layer 2, poiché il fabric Edge 2 ha la stessa interfaccia VLAN (Anycast GW).

Configurazione

Esempio di rete



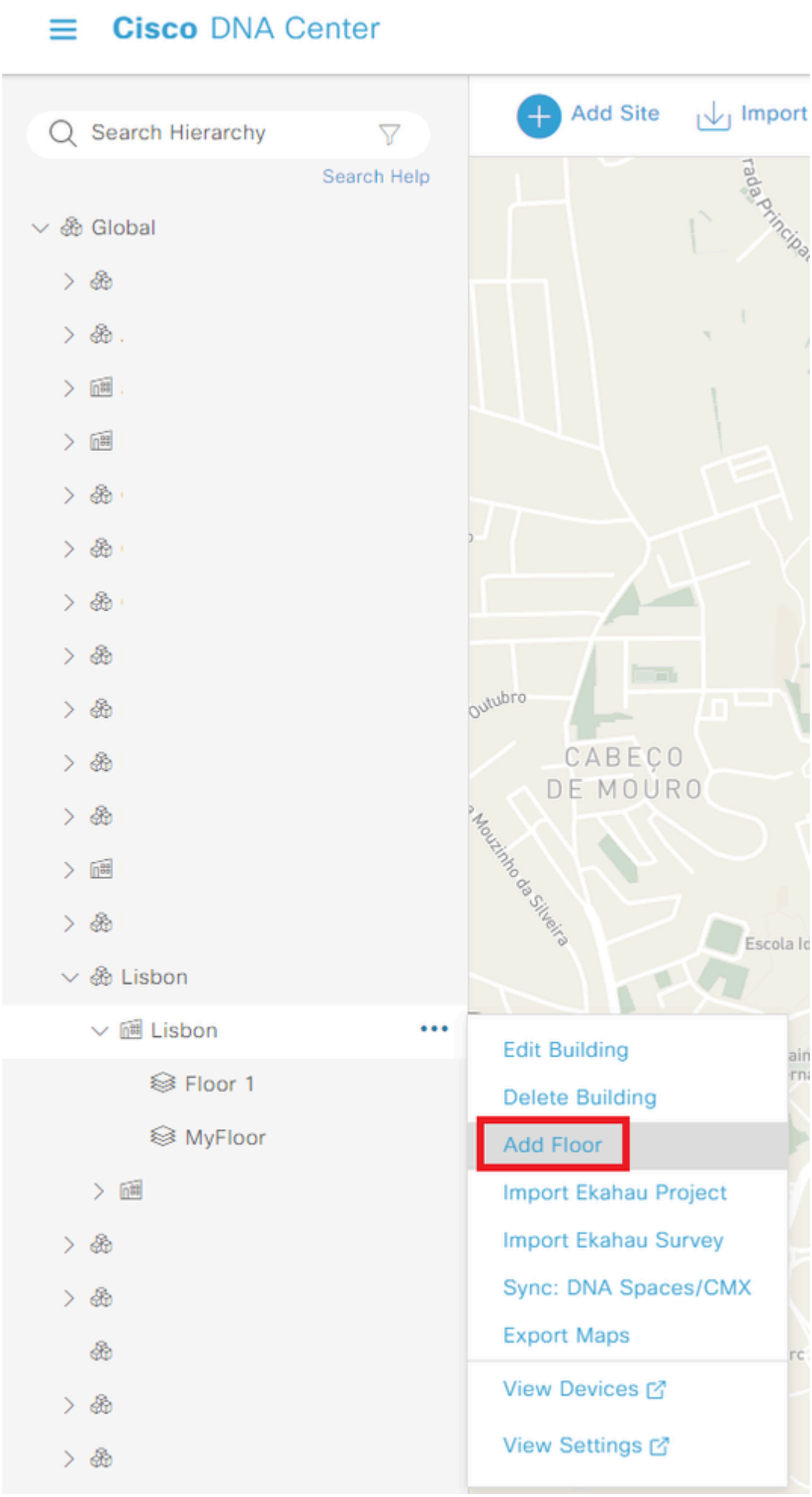
Esempio di rete

Rilevamento e provisioning WLC in Cisco DNA

Aggiungi WLC

Passaggio 1. Passare alla posizione in cui si desidera aggiungere il WLC. È possibile aggiungere un nuovo edificio/piano.

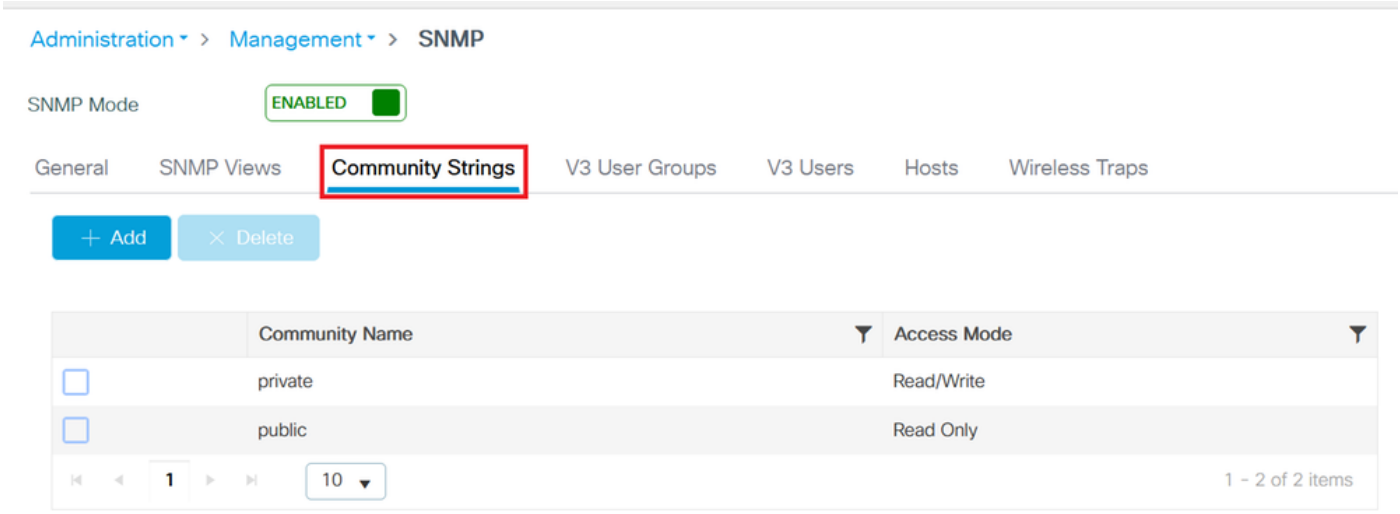
Passare a Progettazione > Gerarchia di rete e inserire l'edificio/piano, oppure è possibile creare un nuovo piano, come mostrato nell'immagine:



Crea nuovo piano

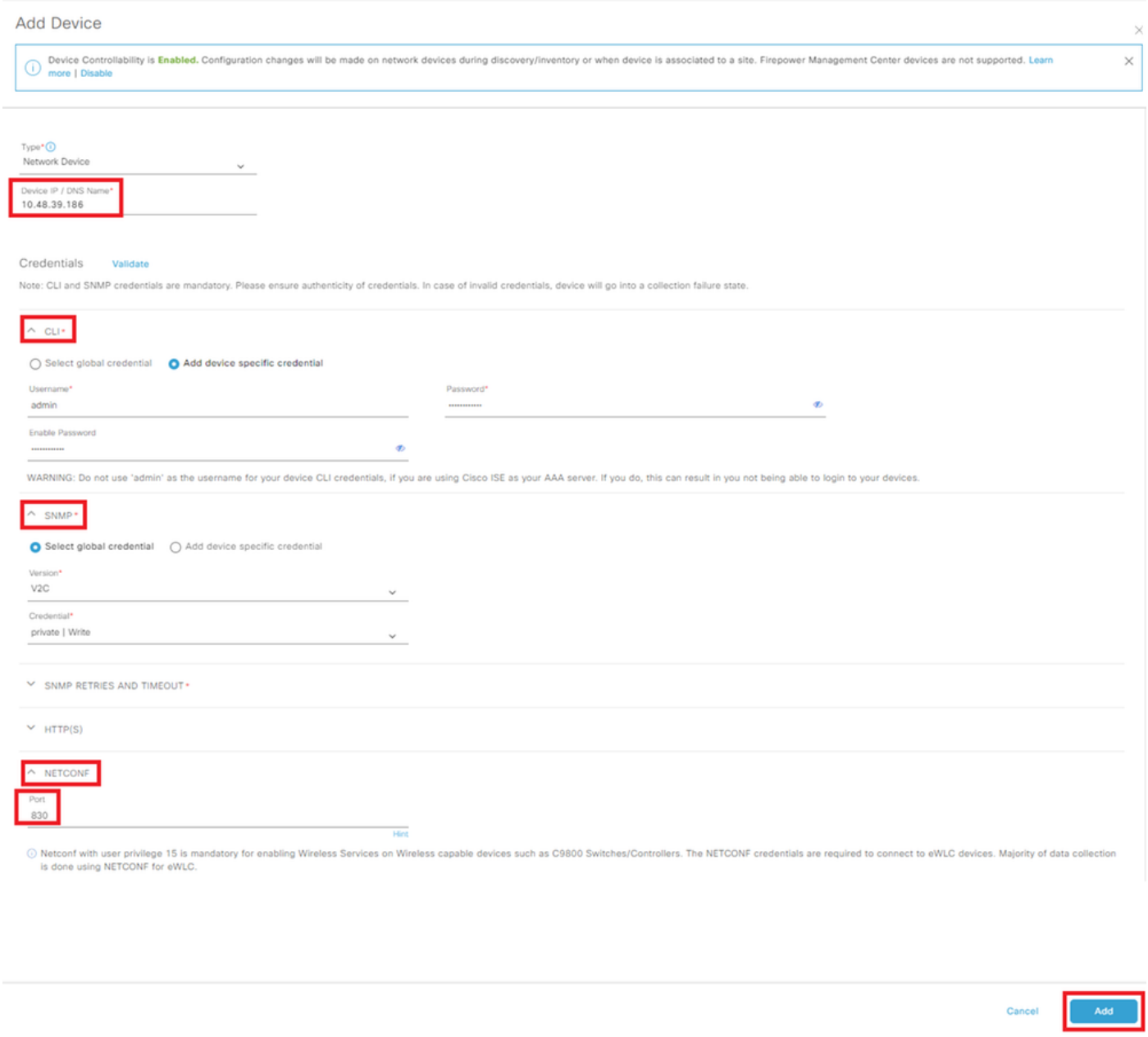
Passaggio 2. Aggiungere il

(Amministrazione > Gestione > SNMP > Stringhe della community), quindi verificare la stringa configurata. Quando si aggiunge il WLC sul Cisco DNA, è necessario aggiungere la stringa della community SNMP corretta e verificare che netconf-yang sia abilitato sul WLC 9800 con i comandi show netconf-yang status. Alla fine, fare clic su Add (Aggiungi):



Configurazione SNMP

Passaggio 5. Aggiungere l'indirizzo IP del WLC, le credenziali CLI (le credenziali che Cisco DNA utilizza per accedere al WLC e che devono essere configurate sul WLC prima di aggiungerle a Cisco DNA), la stringa SNMP e verificare se la porta NETCONF è configurata sulla porta 830:



Aggiungi WLC

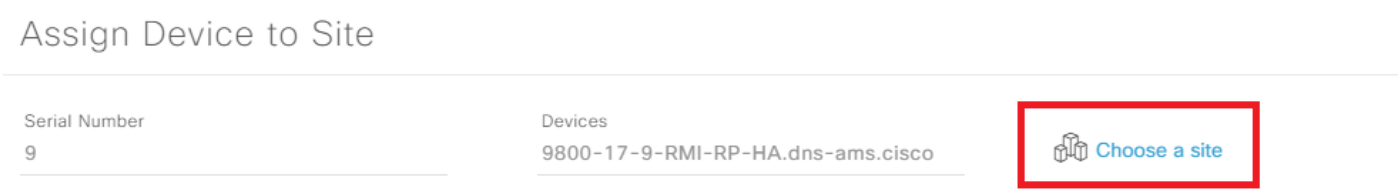
Il WLC si mostra come NA perché Cisco DNA è ancora in processo di sincronizzazione:

WLC in processo di sincronizzazione

Al termine del processo di sincronizzazione, è possibile visualizzare il nome del WLC, l'indirizzo IP, se raggiungibile, gestito e la versione del software:

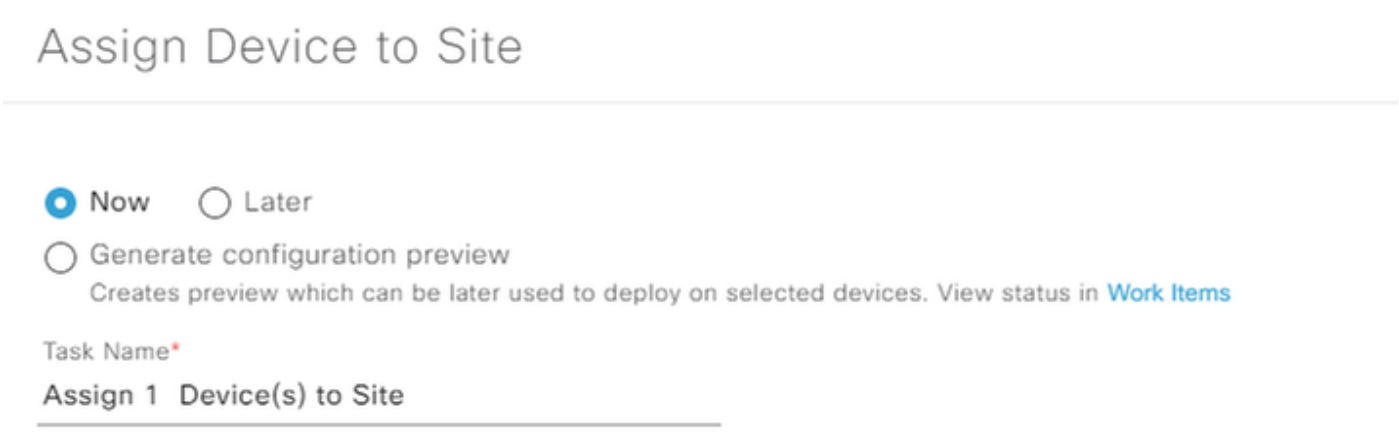
WLC sincronizzato

Passaggio 6. Assegnare il WLC a un sito. Nell'elenco dei dispositivi, fare clic su Assegna, quindi scegliere un sito:



Assegna dispositivo al sito

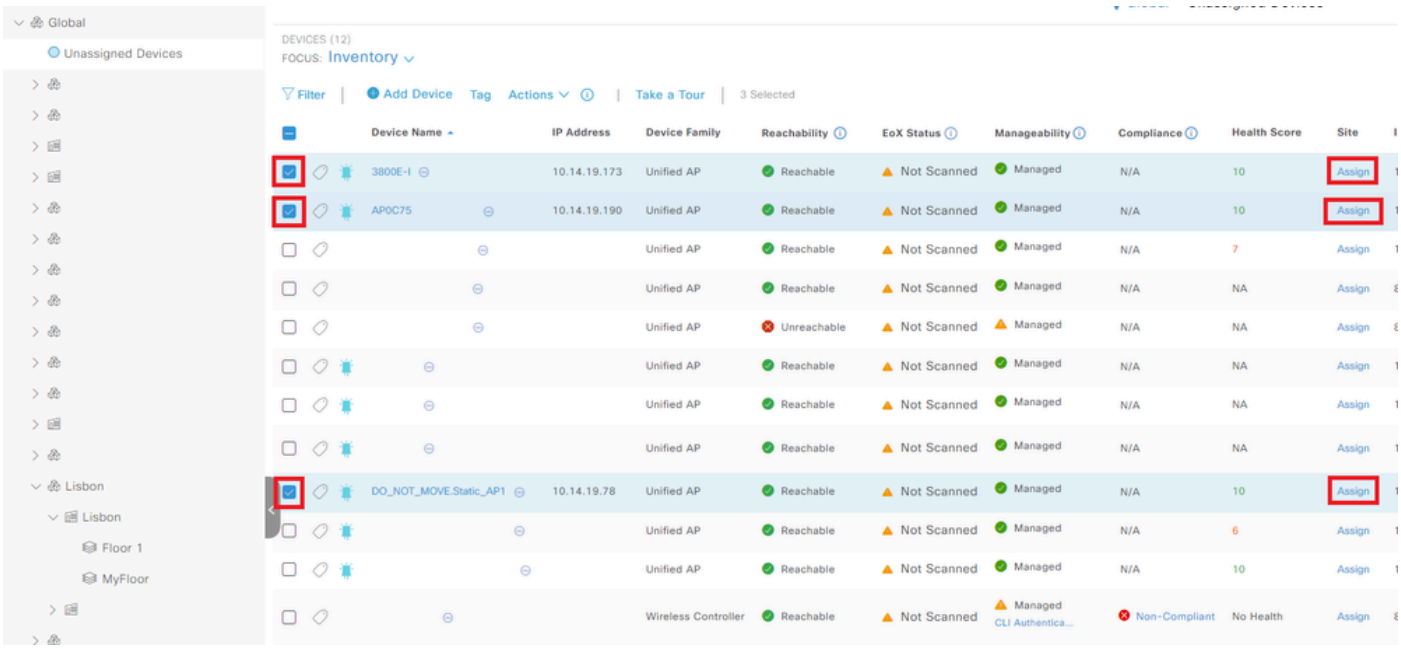
È possibile decidere di assegnare il sito subito o in un secondo momento:



Assegna dispositivo al sito ora o in seguito

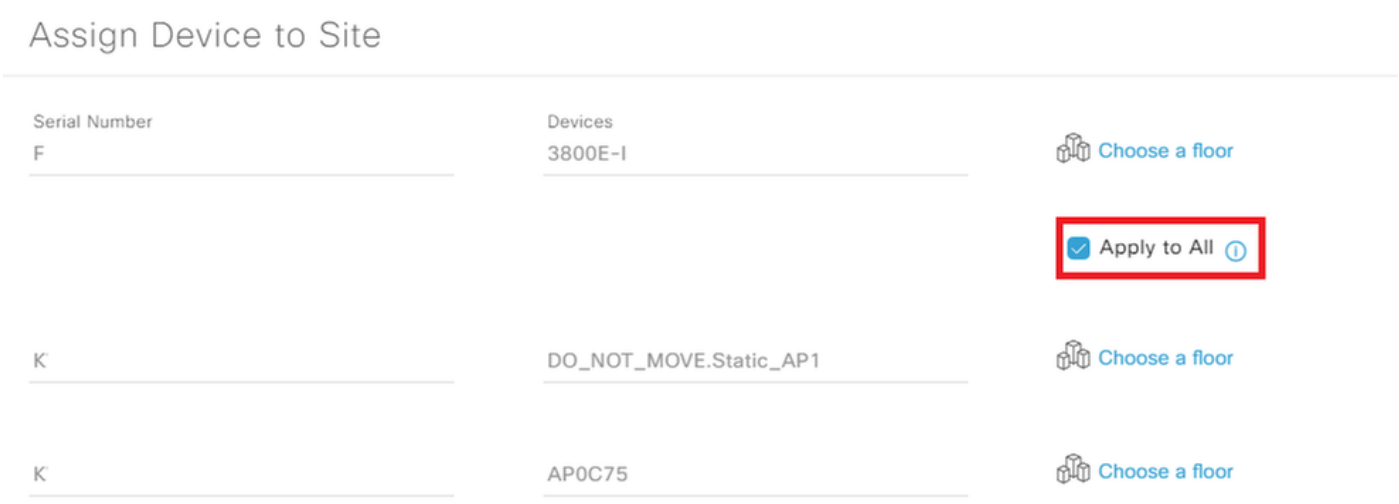
Aggiungi Access Point

Passaggio 1. Dopo aver aggiunto il WLC e averlo raggiunto, selezionare Provisioning > Inventario > Globale > Dispositivi non assegnati e cercare gli AP aggiunti al WLC:



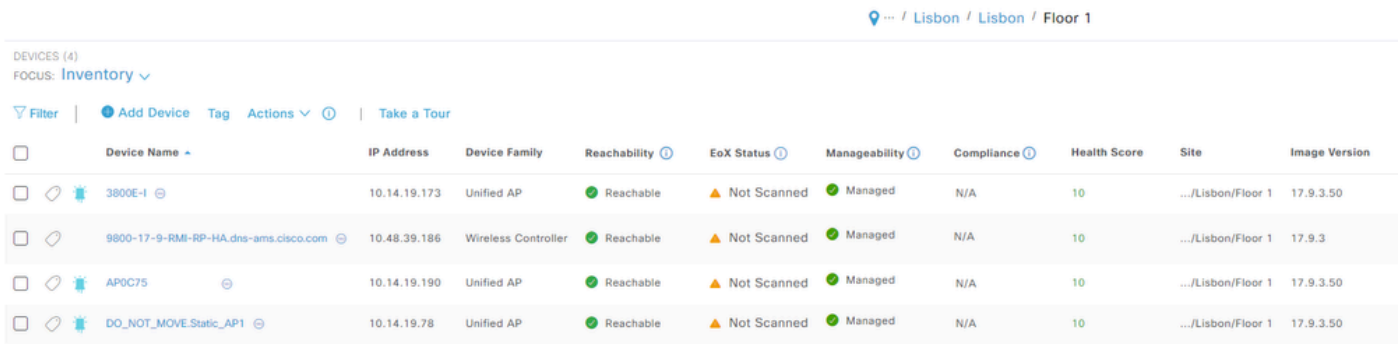
Aggiungi Access Point

Passaggio 2. Selezionare l'opzione Assegna. Assegnare gli access point a un sito. Selezionare la casella Applica a tutte per eseguire la configurazione per più dispositivi contemporaneamente.



Assegna access point al sito

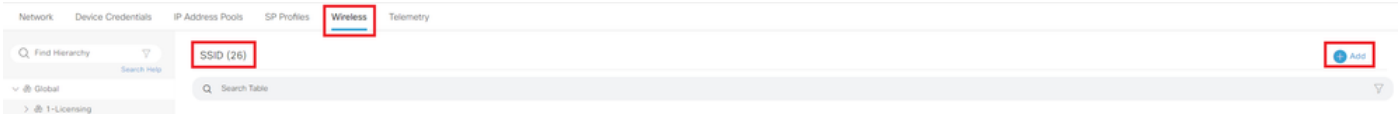
Spostarsi sul pavimento e visualizzare tutti i dispositivi assegnati - WLC e AP:



Dispositivi assegnati al sito

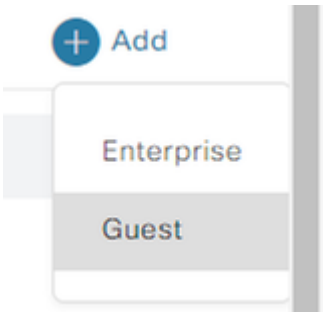
Crea SSID

Passaggio 1. Passare a Progettazione > Impostazioni di rete > Wireless > Globale e aggiungere un SSID:



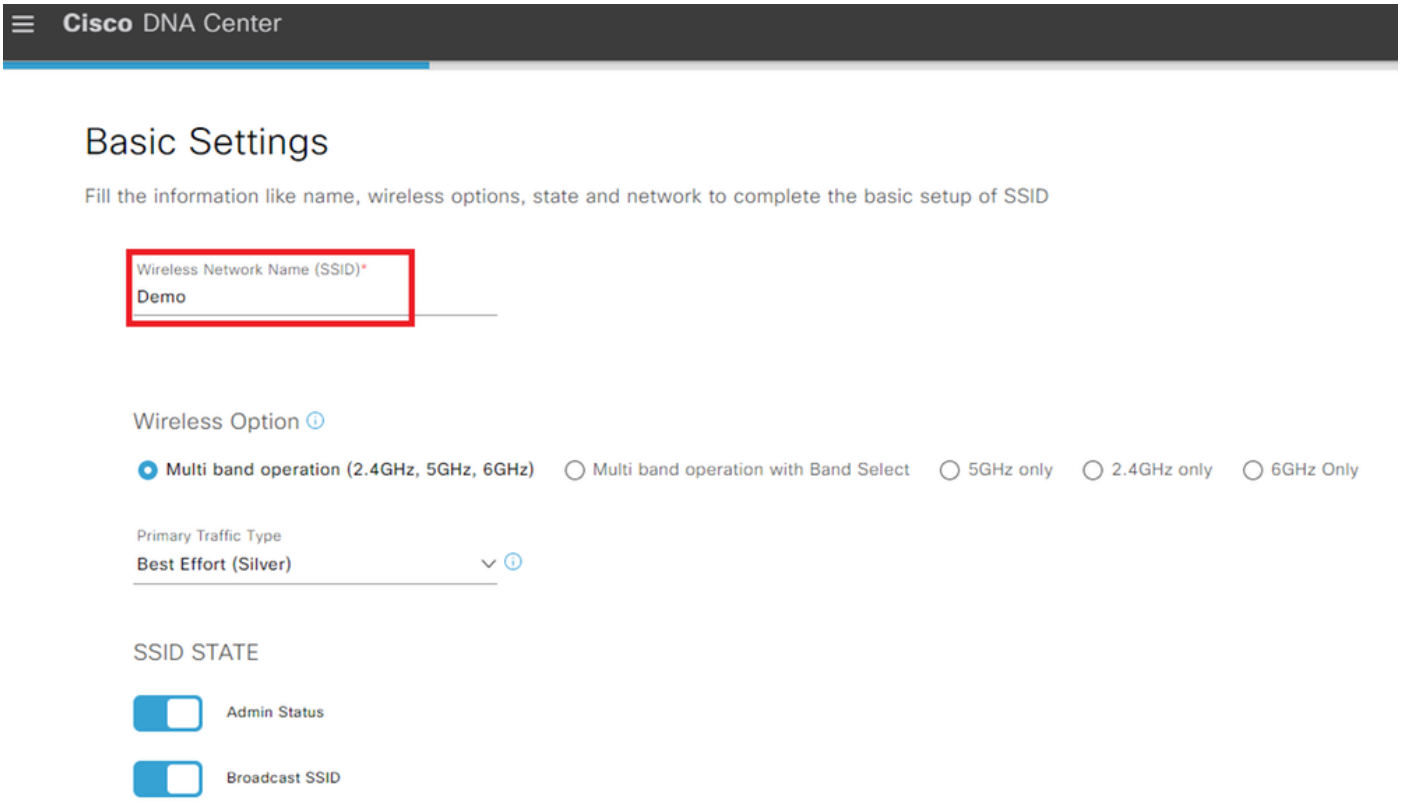
Crea SSID

È possibile creare un SSID Enterprise o un SSID Guest. In questa demo viene creato un SSID guest:

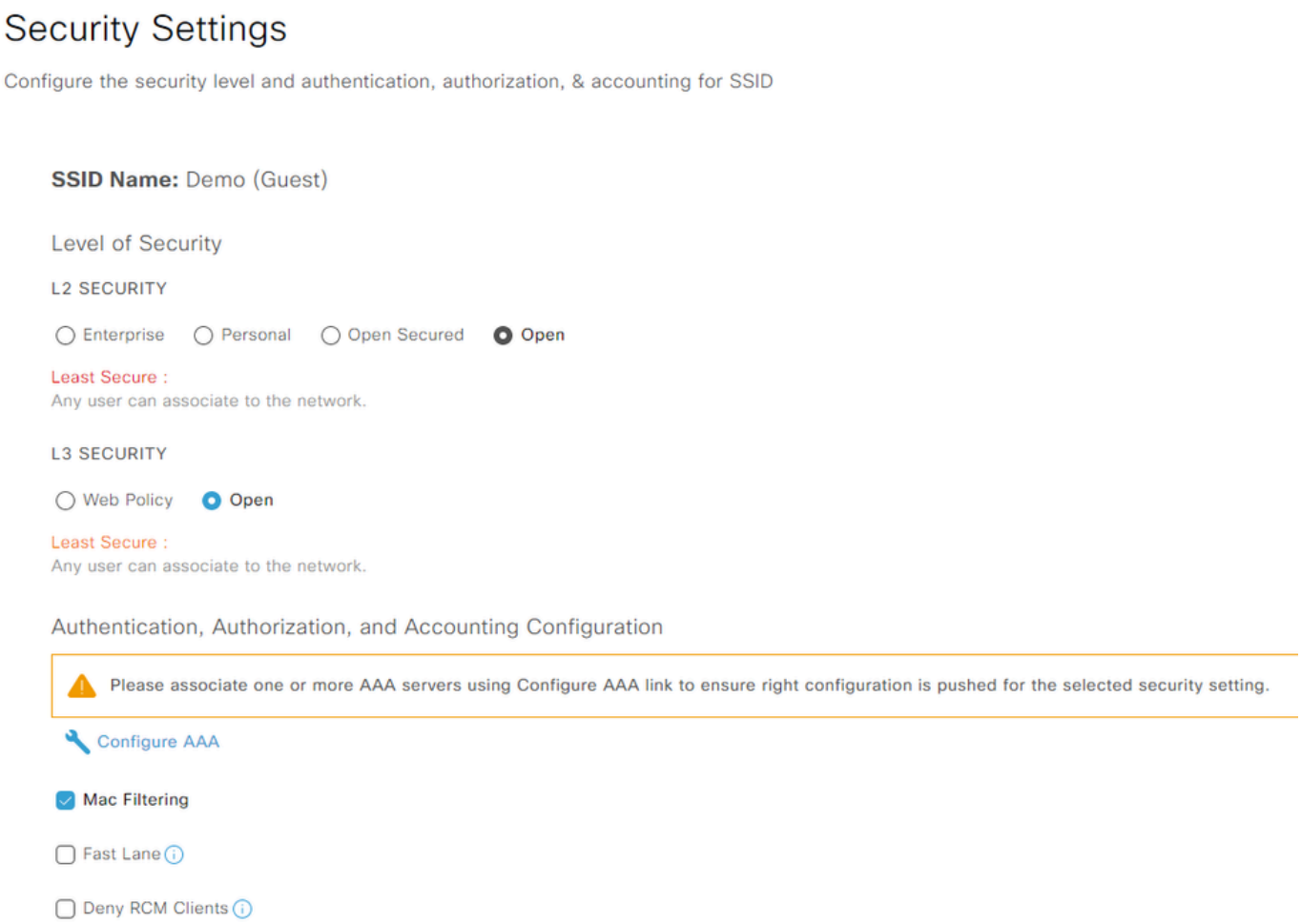


SSID aziendale o guest

Passaggio 2. Scegliere l'impostazione desiderata per l'SSID. In questo caso, viene creato un SSID aperto. Lo stato di amministrazione e Broadcast SSID devono essere abilitati:



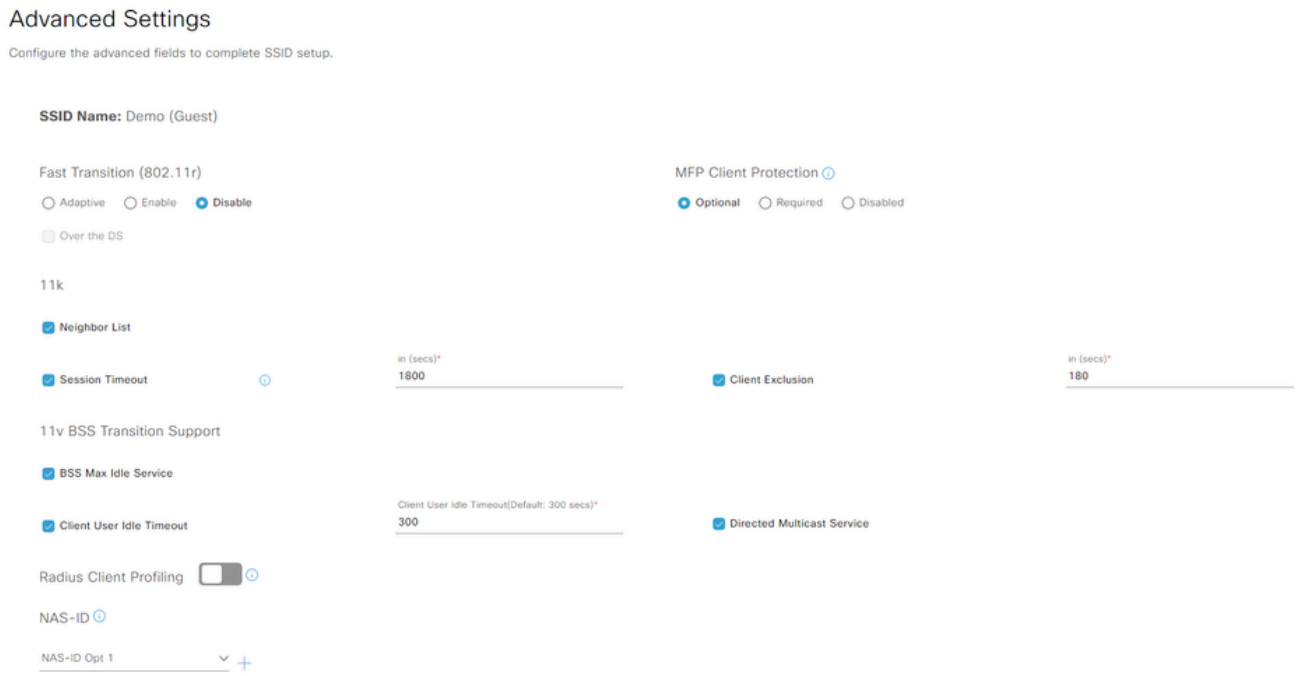
Impostazioni di base SSID



Impostazioni di sicurezza SSID

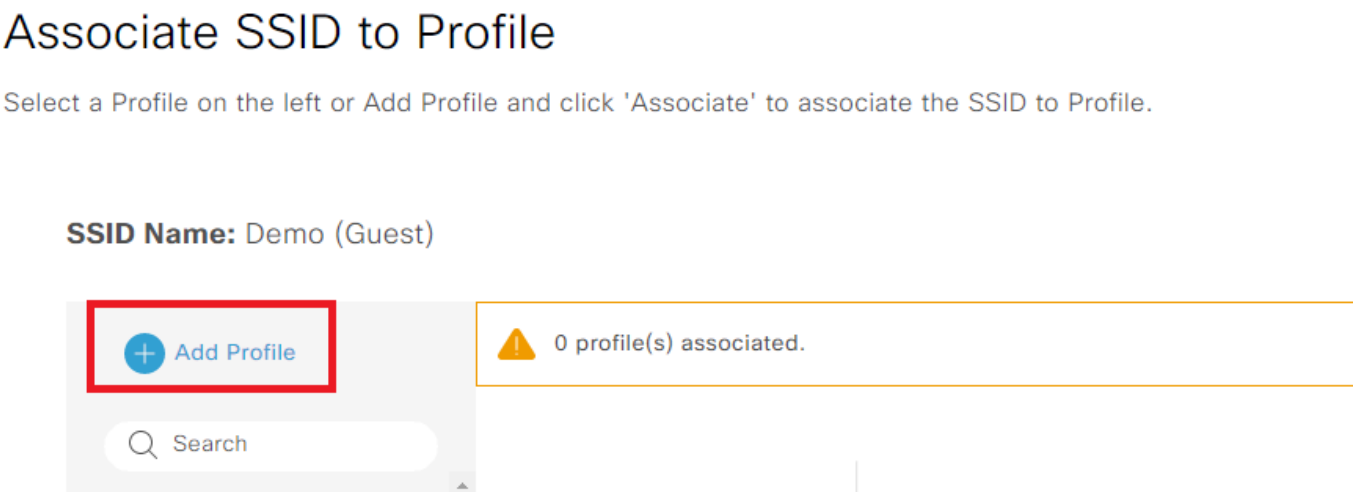
⚠ Attenzione: Non dimenticare di configurare e associare il server AAA per l'SSID. Se non è configurato alcun server AAA, viene eseguito il mapping dell'elenco di metodi predefinito.

Quando si fa clic su avanti, è possibile visualizzare le impostazioni avanzate per il proprio SSID:



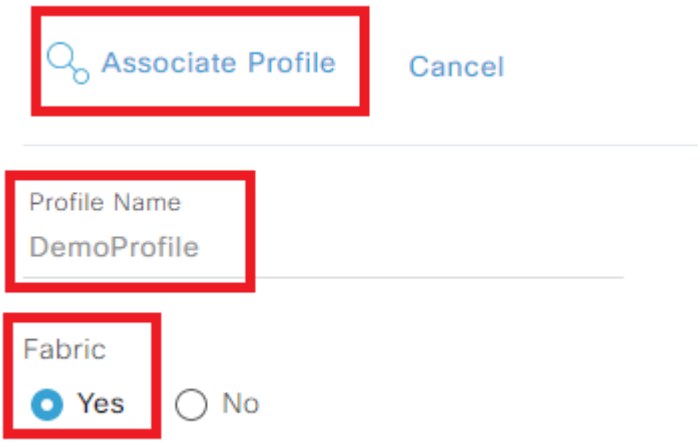
Impostazioni avanzate SSID

Passaggio 3. Dopo la creazione dell'SSID, è necessario associarlo a un profilo. Fare clic su Aggiungi profilo:



Aggiungi profilo

Passaggio 4. Assegnare un nome al profilo, selezionare Fabric e fare clic su Associa profilo:



Associa profilo

Viene visualizzato un riepilogo del SSID e del profilo creati:

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)

Riepilogo SSID

Passaggio 5. Configurare un nuovo profilo di rete:

Design > Network Settings > Wireless > Global (Progettazione > Impostazioni di rete > Wireless > Globale) e aggiungere il nuovo profilo RF:

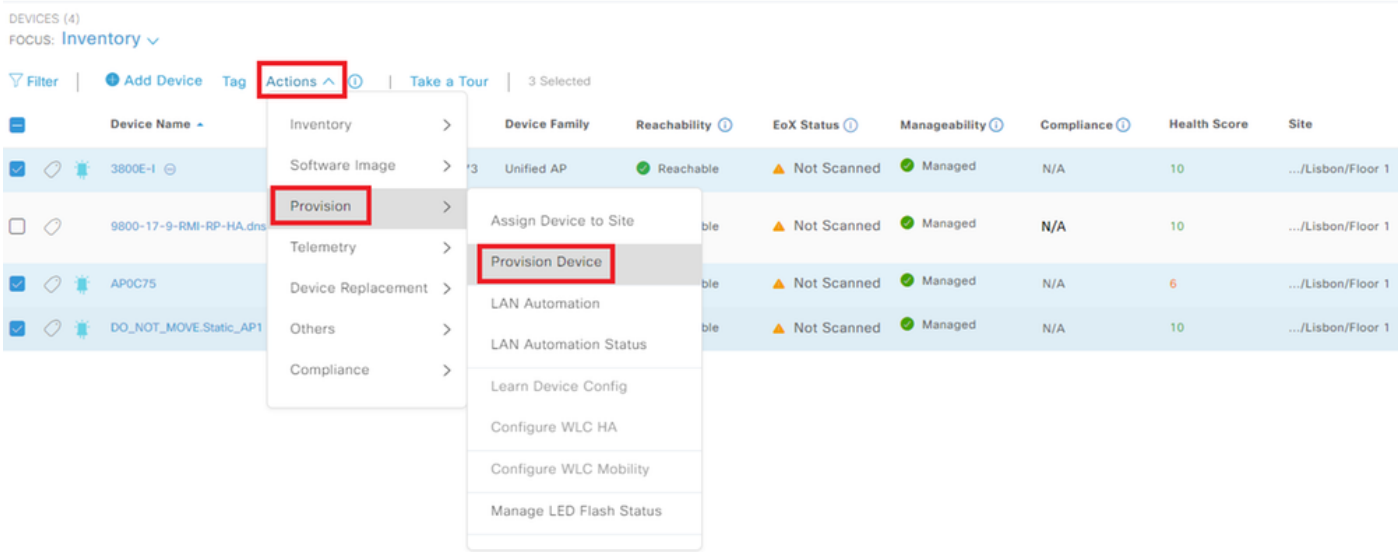
Aggiungi profilo RF

Passaggio 8. (Facoltativo) Assegnare un nome al profilo RF e selezionare le impostazioni che si desidera configurare. In questa demo sono state configurate le impostazioni predefinite. Fare clic su Salva:

Aggiungi profilo RF di base

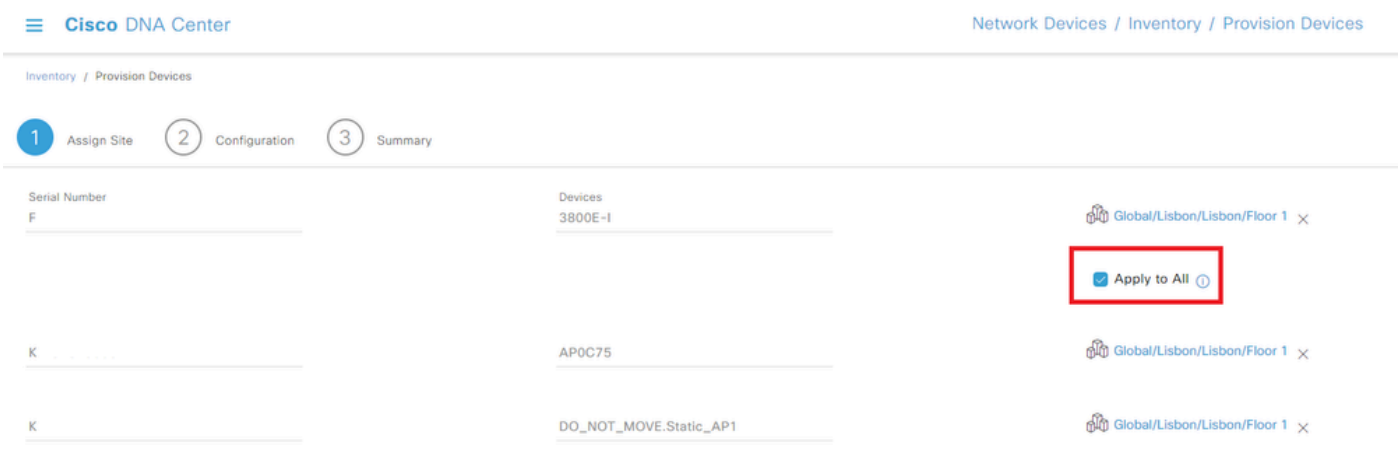
Provisioning dei punti di accesso

Passaggio 1. Passare all'edificio/piano. Selezionare i punti di accesso e Azioni > Provisioning > Provisioning dispositivo:



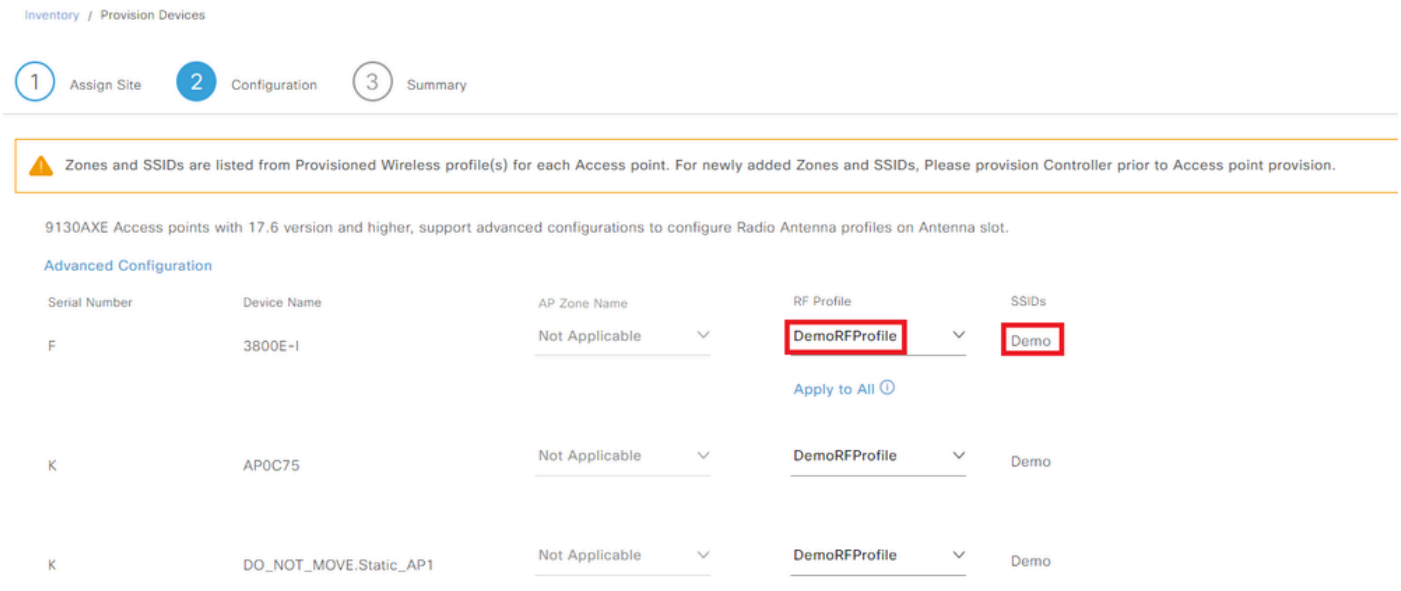
Provisioning dei punti di accesso

Passaggio 2. Verificare che il sito assegnato sia corretto e selezionare Applica a tutte:



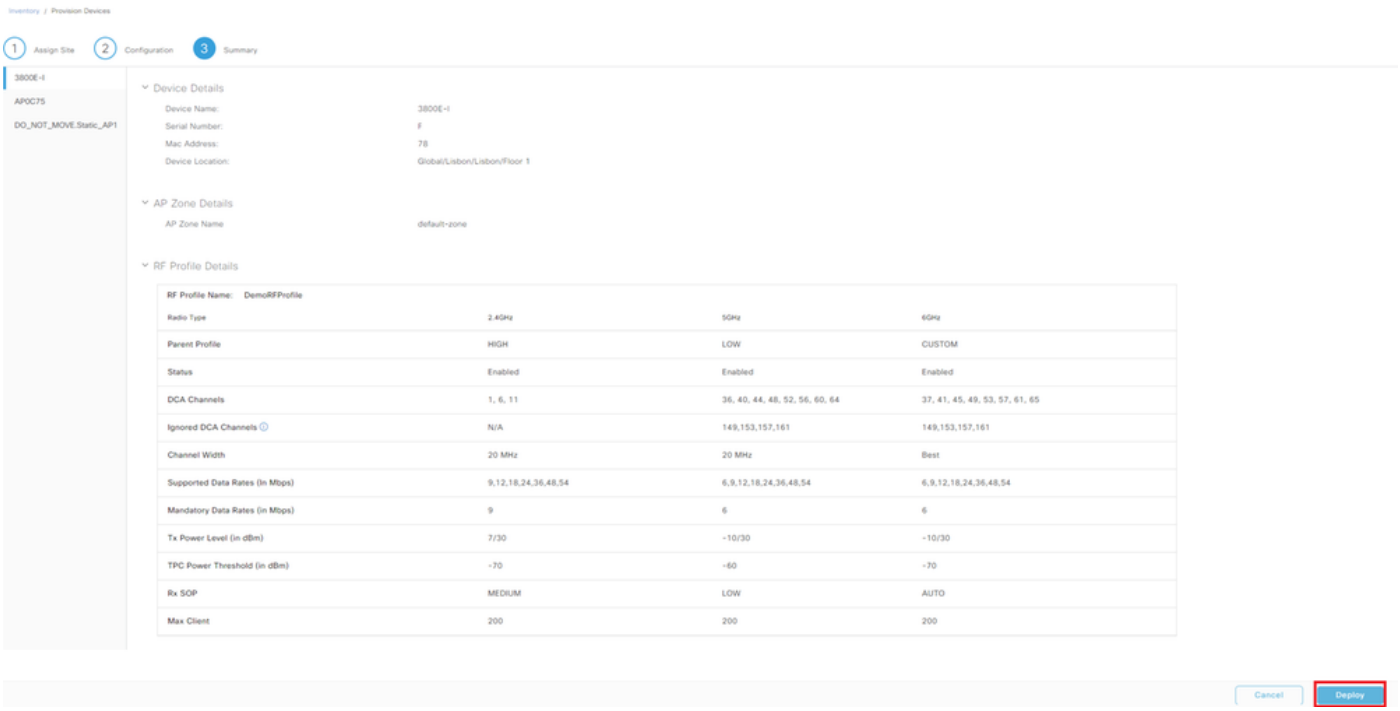
Assegna sito ai punti di accesso

Passaggio 3. Selezionare un profilo RF dall'elenco a discesa e verificare che il SSID sia corretto:



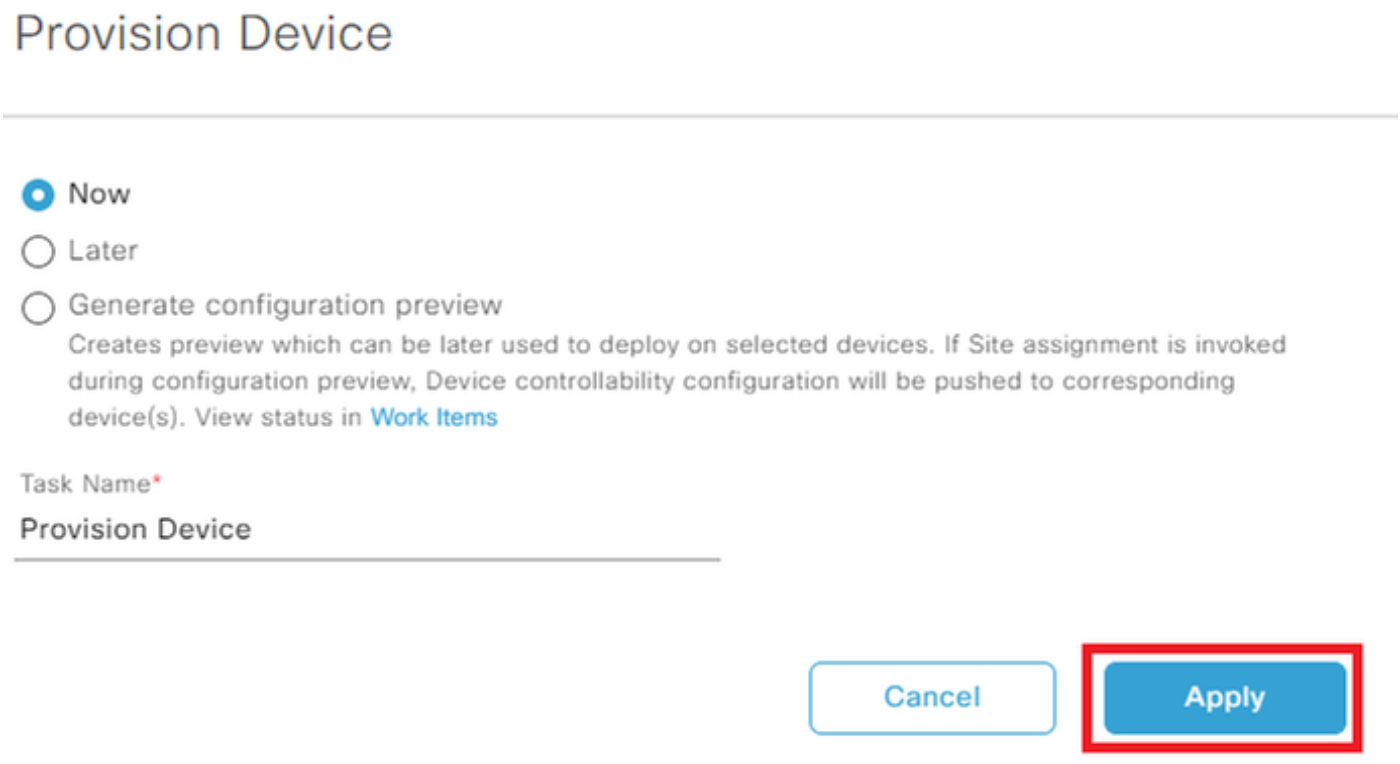
Seleziona profilo RF

Passaggio 4. Verificare le impostazioni sui punti di accesso. Se tutto è corretto, selezionare Distribuisci:



Distribuisci provisioning AP

Passaggio 5. Il provisioning del dispositivo può essere implementato al momento o in un secondo momento. Alla fine, selezionare Applica:

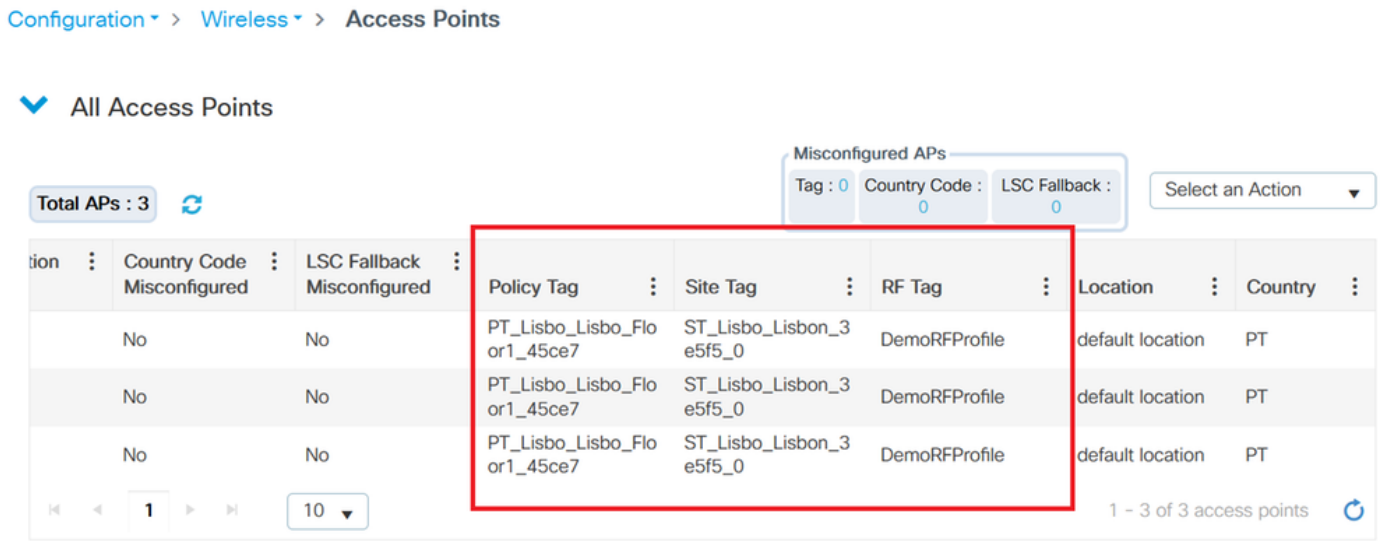


Esegui provisioning dei punti di accesso ora o in seguito

⚠ Attenzione: Quando si esegue il provisioning, gli access point, che fanno già parte della base configurata per il profilo RF selezionato, devono essere elaborati e riavviati.

Provisioning degli access point completato.

Passaggio 6. Sul lato WLC, selezionare Configurazione > Wireless > Access Point. Verificare che i tag AP siano stati spinti da Cisco DNA:



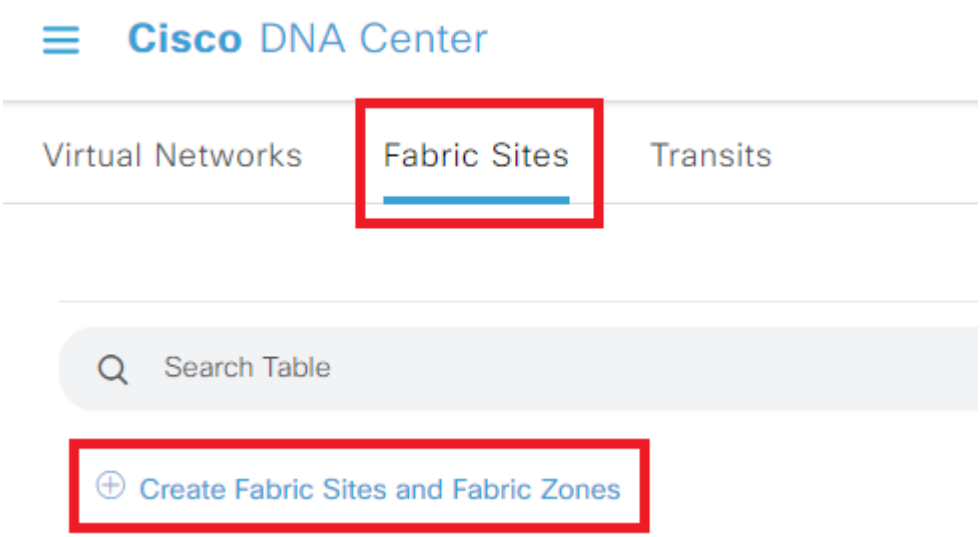
Tag su access point

Passaggio 7. Passare a Configurazione > Tag e profili > WLAN e verificare che l'SSID sia stato inviato da Cisco DNA:

WLAN

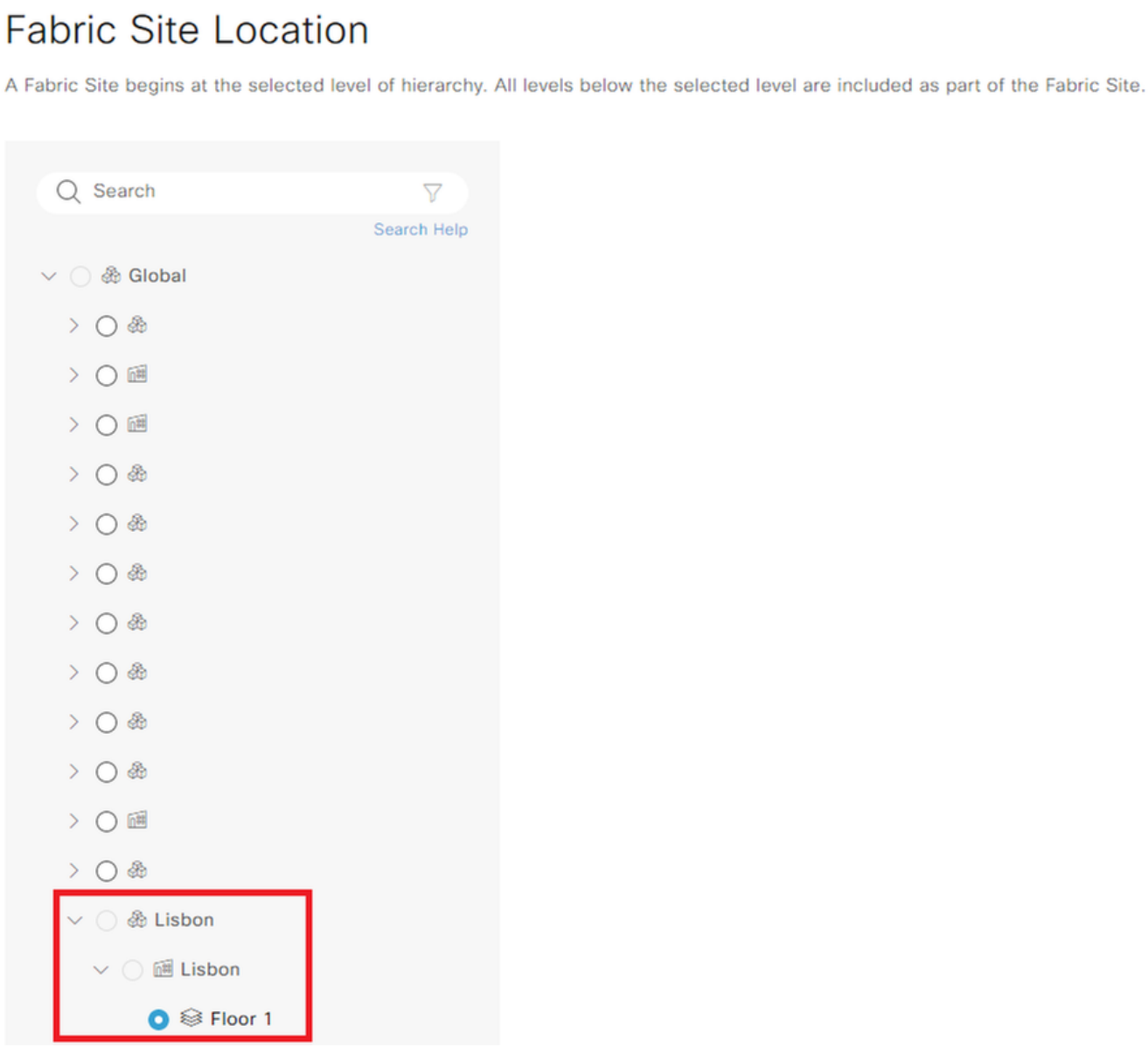
Crea sito fabric

Passaggio 1. Passare a Provisioning > Siti fabric. Creare un sito infrastruttura:



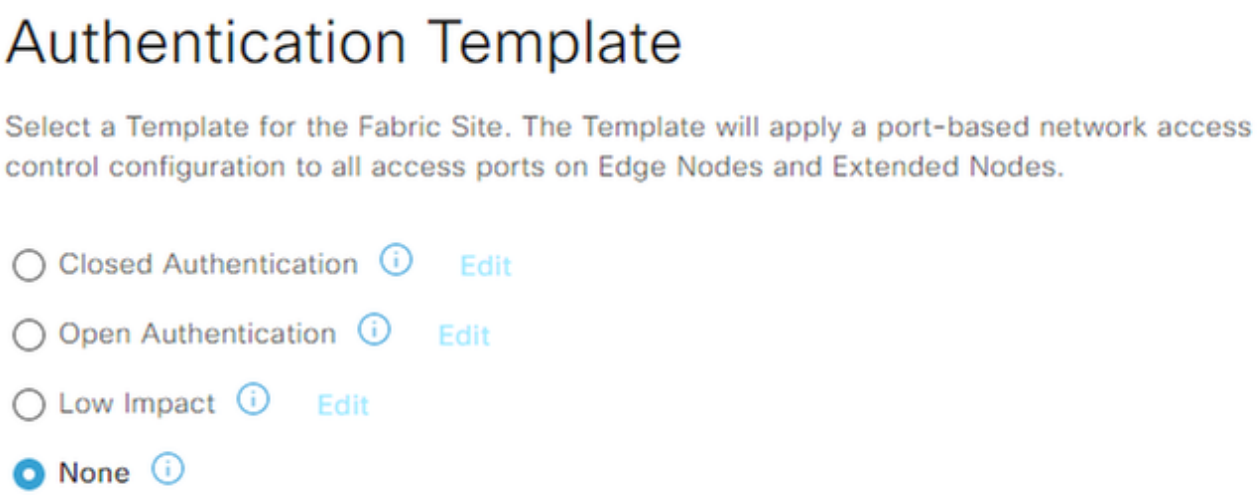
Crea siti fabric

Passaggio 2. Selezionare l'edificio/piano per la sede del fabric:



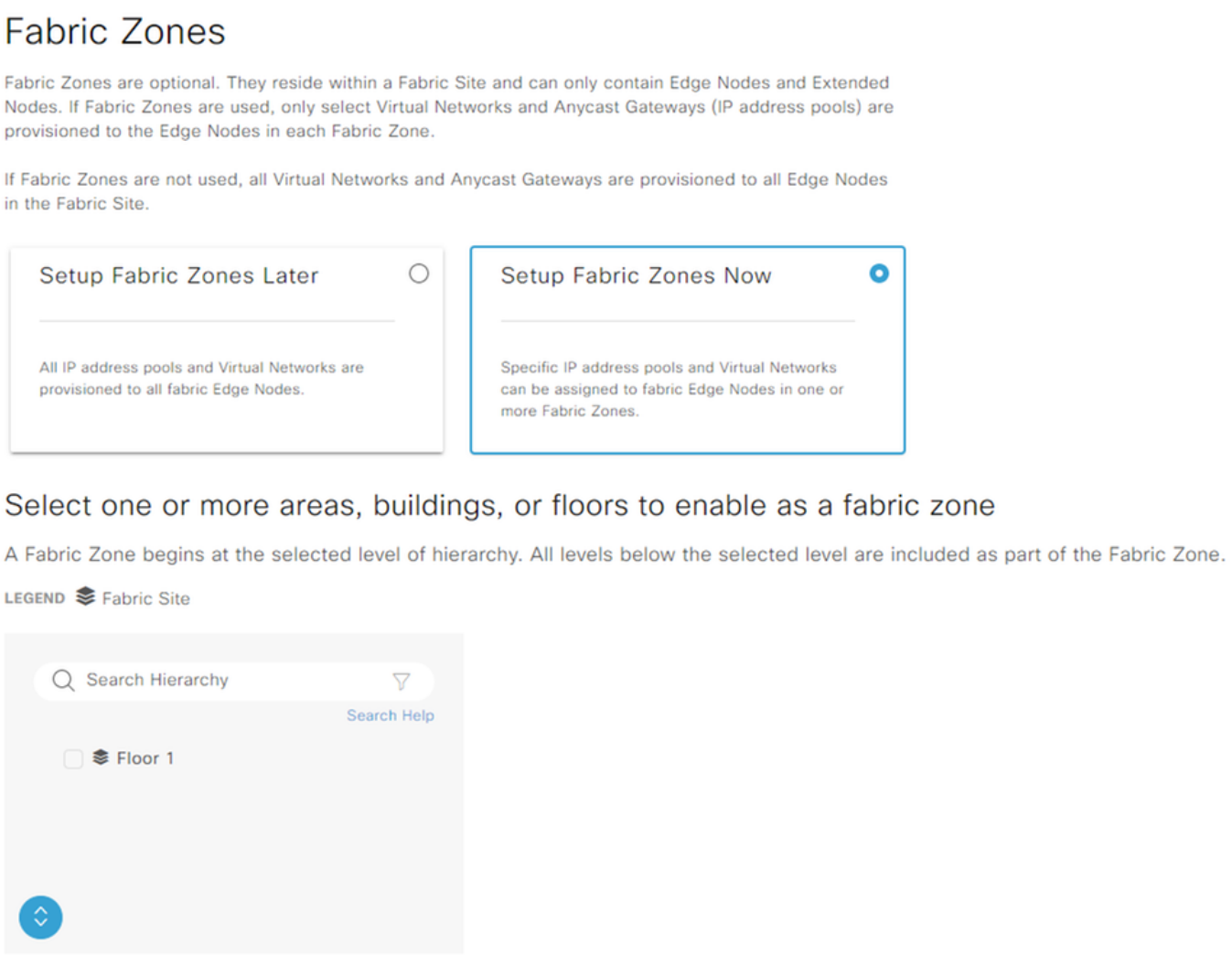
Seleziona sito fabric

Passaggio 3. Selezionare un modello di autenticazione. In questa demo, Nessuno è stato applicato:



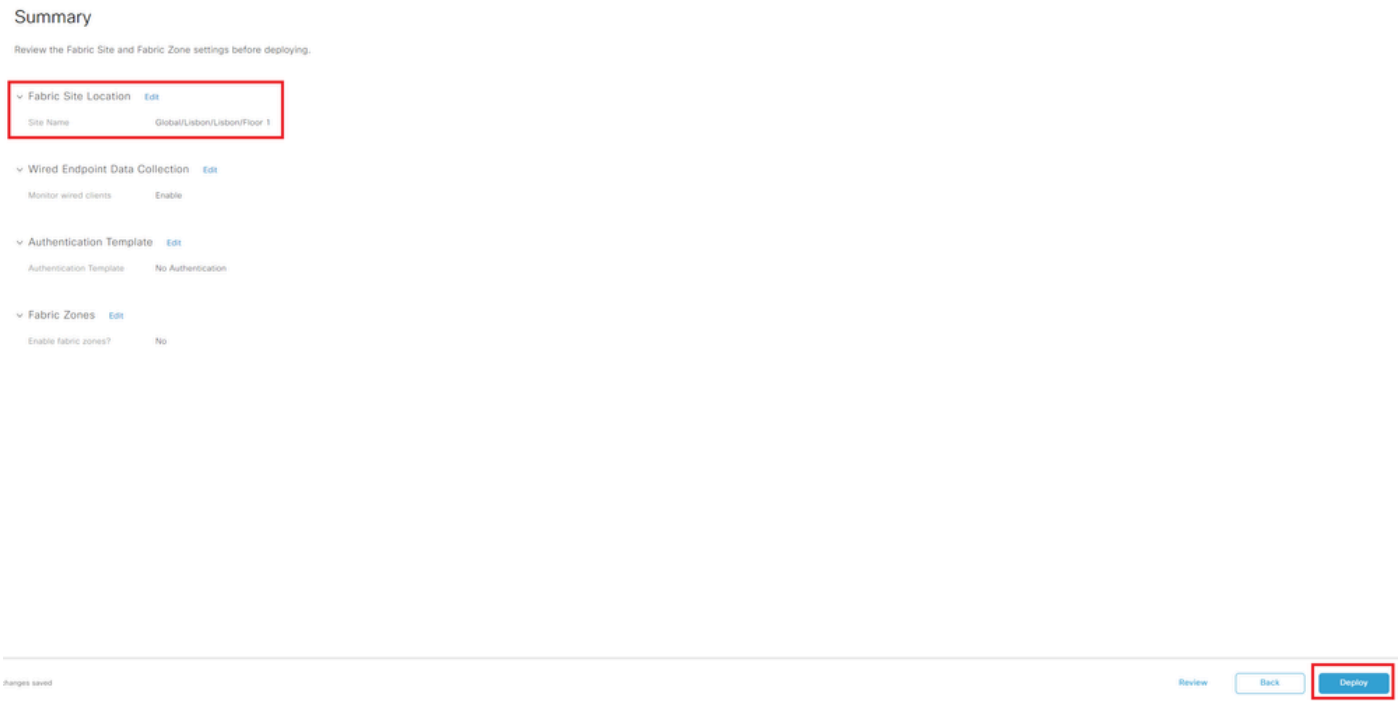
Modello di autenticazione

Passaggio 3. È possibile scegliere se impostare la zona struttura subito o in un secondo momento:



Imposta zone fabric

Passaggio 4. Verificare le impostazioni dell'area di infrastruttura. Se tutto è corretto, selezionare Distribuisci:



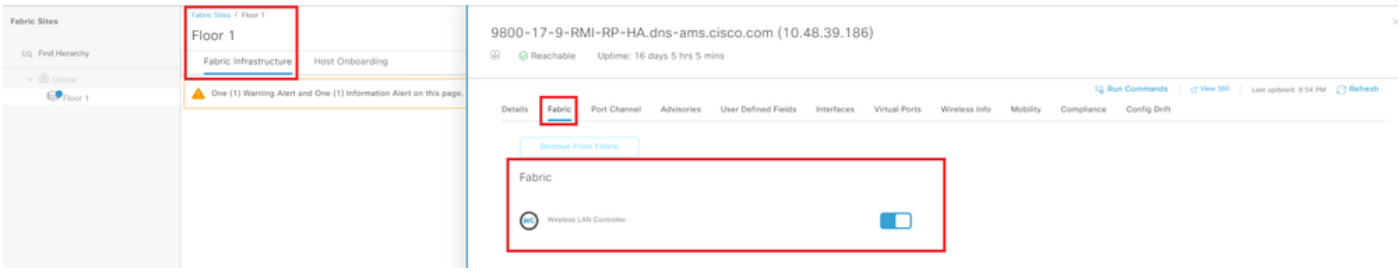
Distribuisci sito fabric

È stato creato un sito fabric:

Creazione sito fabric

Aggiungi WLC a fabric

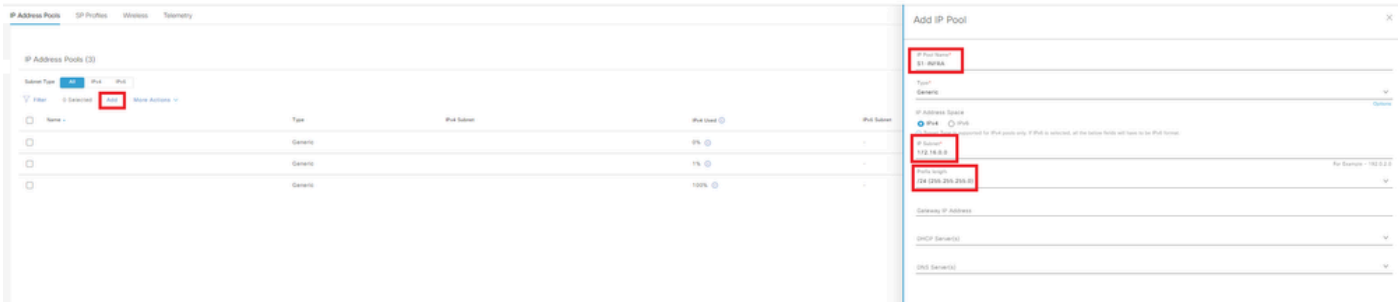
Passare a Provisioning > Siti fabric e selezionare il sito fabric. Fare clic nella parte superiore del WLC e selezionare la scheda Fabric. Abilitare l'infrastruttura al WLC e selezionare Add:



Aggiungi WLC a fabric

Join AP

Passaggio 1. Passare a Progettazione > Impostazioni di rete > Pool di indirizzi IP. Creare un pool di indirizzi IP.



Pool di indirizzi IP

Passaggio 2. Passare a Provisioning > Siti fabric e selezionare il sito fabric. Passare a Host Onboarding > Virtual Networks (Caricamento host > Reti virtuali).

INFRA_VN è stato introdotto per semplificare i punti di accesso integrati. I punti di accesso sono sovrapposti alla struttura, ma INFRA_VN è mappato alla tabella di routing globale. Solo i punti di accesso e i nodi estesi possono appartenere a INFRA_VN. L'estensione di livello 2 viene attivata automaticamente e il servizio LISP L2 viene attivato.

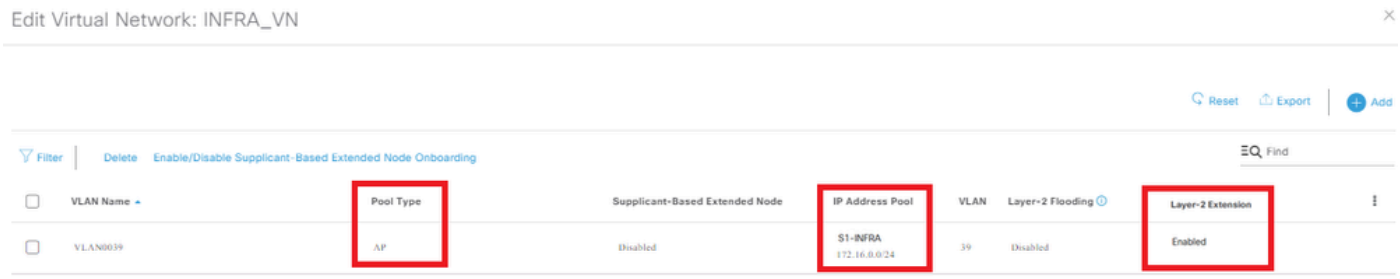
Selezionare INFRA_VN > Aggiungi:

Modifica rete virtuale

Passaggio 3. Aggiungere un pool di indirizzi IP con il tipo di pool AP:

Modifica S1-INFRA rete virtuale

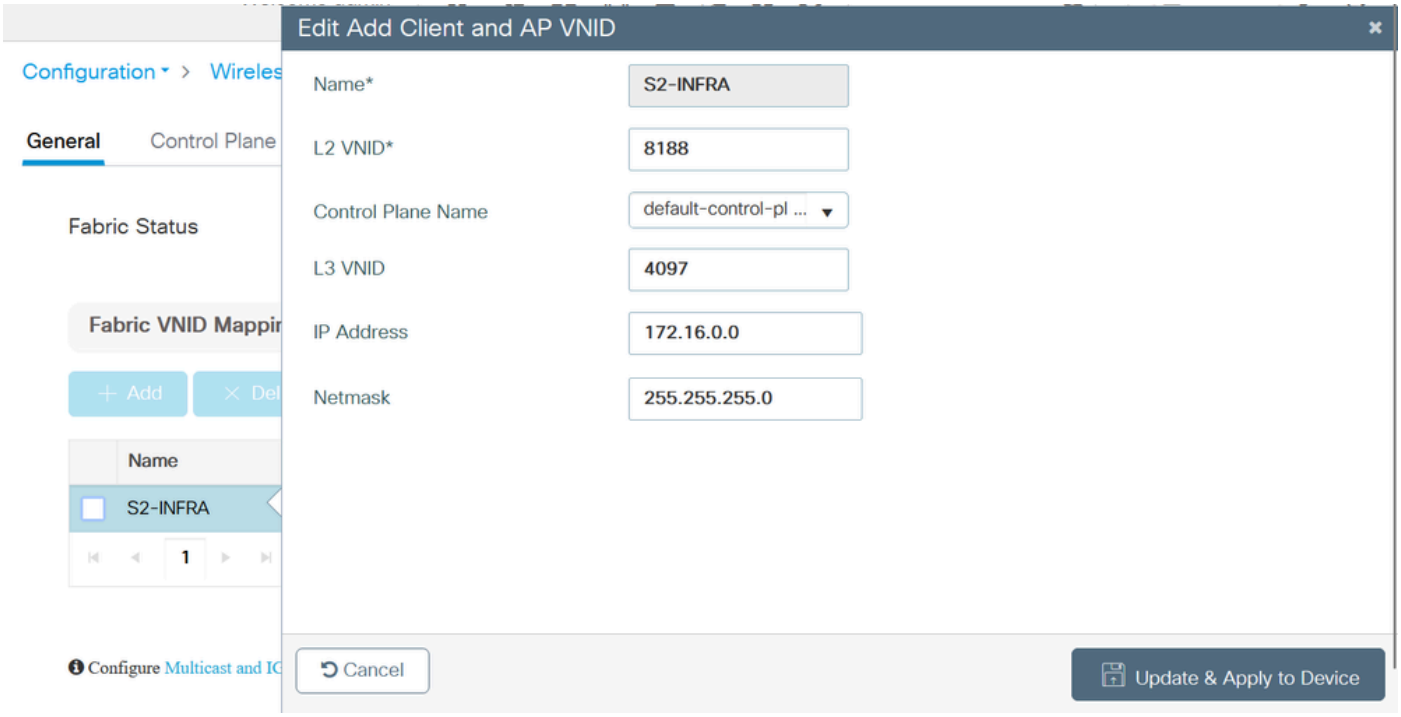
Passaggio 4. Verificare se l'estensione di livello 2 è abilitata.



Modifica rete virtuale

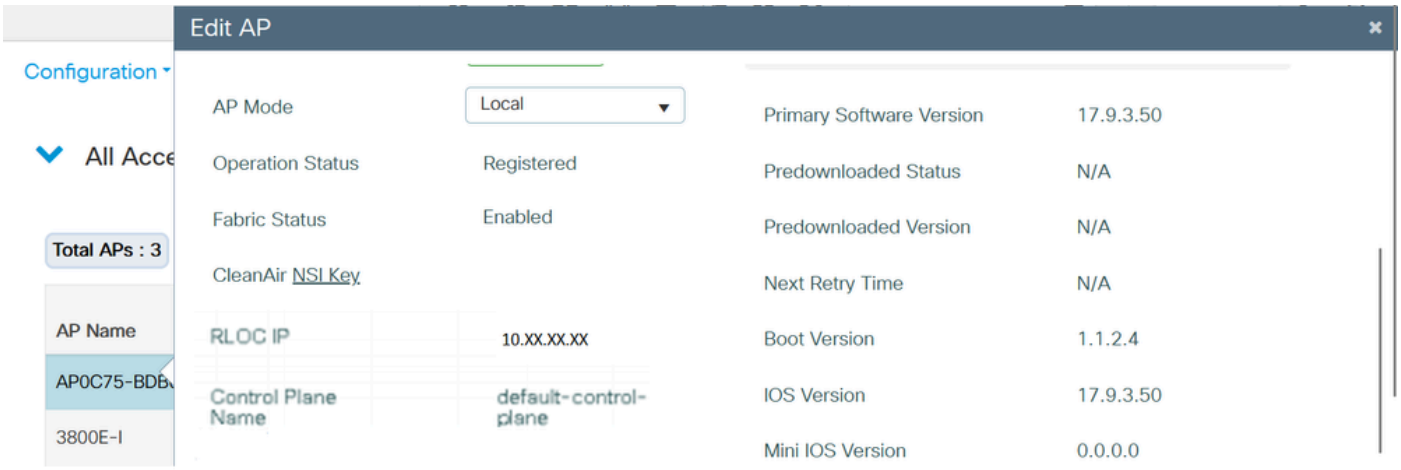
Con il tipo di pool = AP e l'estensione di livello 2 impostata su ON, Cisco DNA si connette al WLC e imposta l'interfaccia di fabric sul mapping VN_ID per la subnet AP per entrambi i VN_ID L2 e L3.

Passaggio 5. Sul lato GUI del WLC, selezionare Configuration > Wireless > Fabric > General (Configurazione > Wireless > Fabric > Generale). Aggiungere un nuovo client e un VN_ID AP:



Aggiungi nuovo client e AP VN_ID

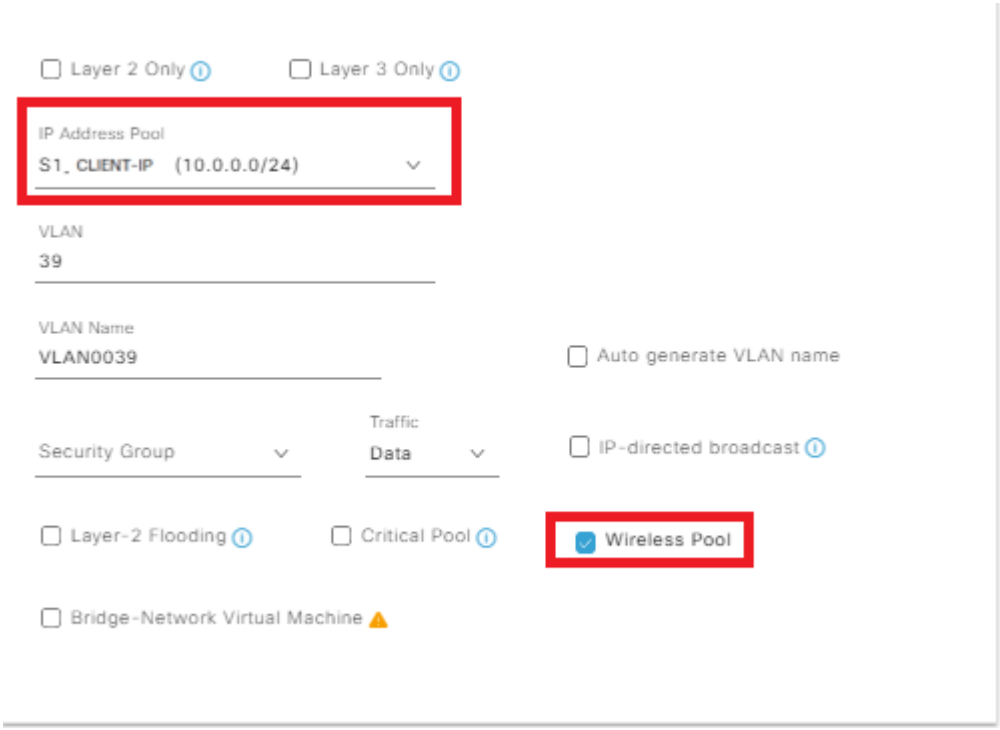
Passaggio 6. Passare a Configurazione > Wireless > Access Point. Selezionare un punto di accesso dall'elenco. Verificare che lo stato dell'infrastruttura sia Abilitato, che l'indirizzo IP del control plane e il nome del control plane:



Verifica dello stato dell'infrastruttura AP

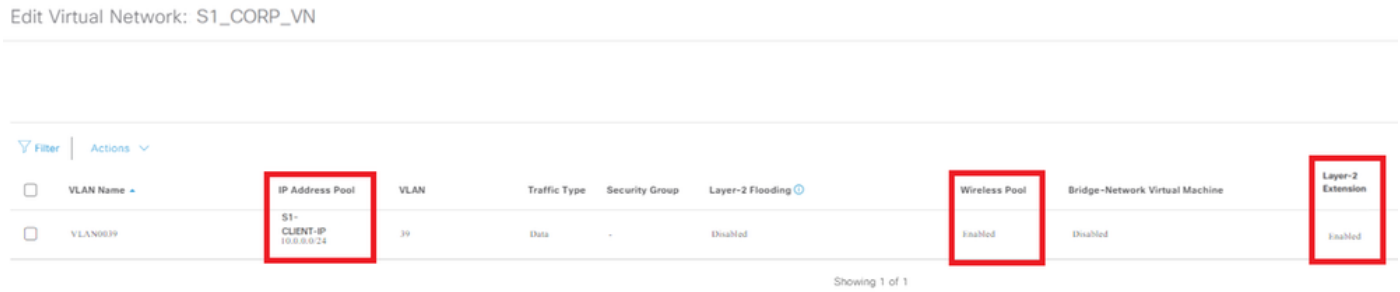
Client integrato

Passaggio 1. Aggiungere il pool alla rete virtuale e verificare che l'opzione Estensione di livello 2 sia attivata per abilitare l'estensione LISP L2 e l'estensione subnet di livello 2 nel pool/subnet client. In Cisco DNA 1.3.x non è possibile disabilitarlo.



Aggiungi pool di indirizzi IP

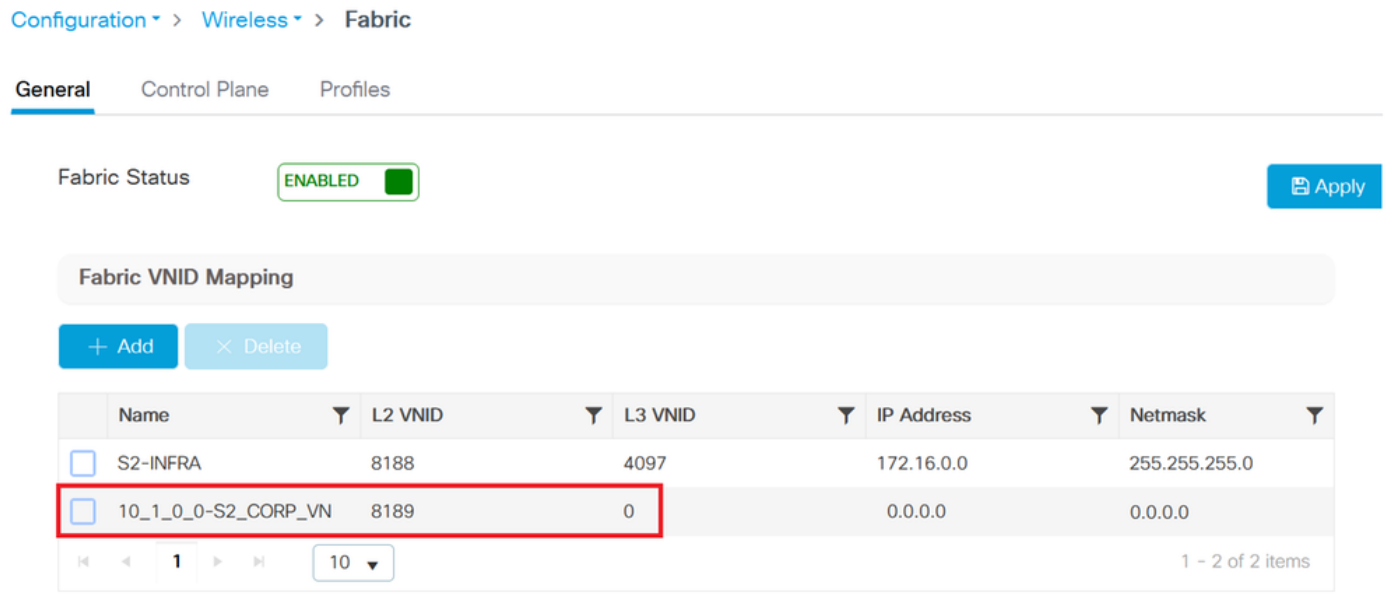
Passaggio 2. Verificare se l'estensione di livello 2 e il pool wireless sono abilitati.



Modifica rete virtuale

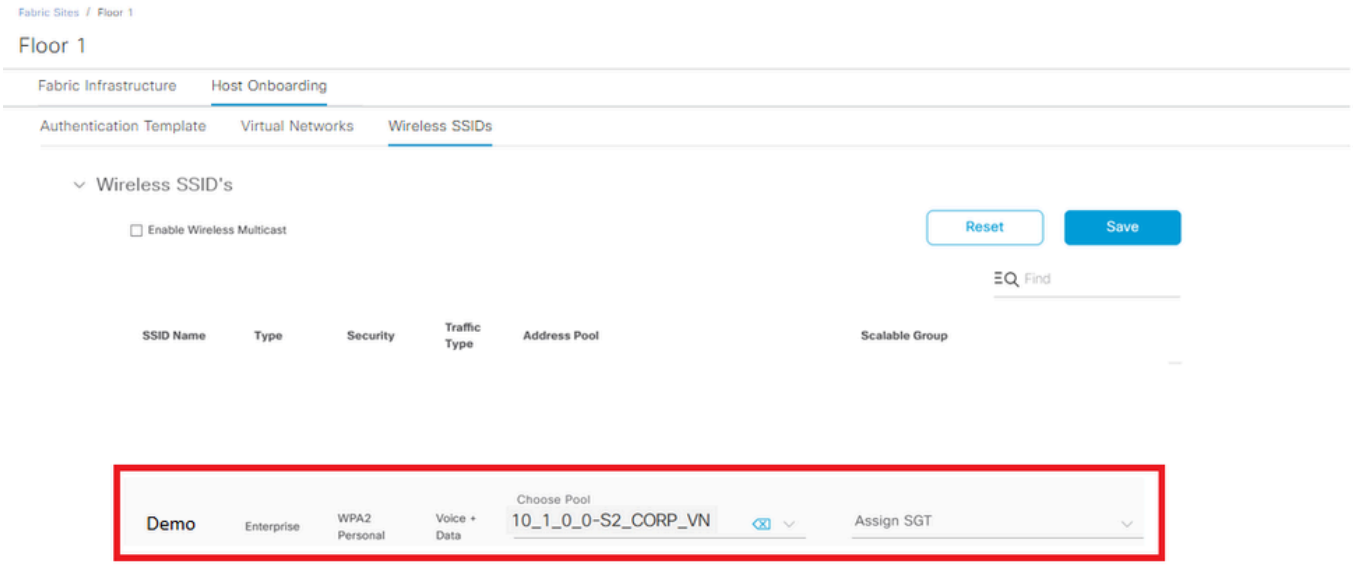
Passaggio 3. Sul lato GUI del WLC, selezionare Configuration > Wireless > Fabric > General (Configurazione > Wireless > Fabric > Generale). Aggiungere un nuovo client e un AP VN_ID.

Quando il pool viene assegnato alla rete virtuale, l'interfaccia dell'infrastruttura corrispondente al mapping VNID viene inviata al controller. Si tratta di VNID L2.



Aggiungi nuovo client e AP VN_ID

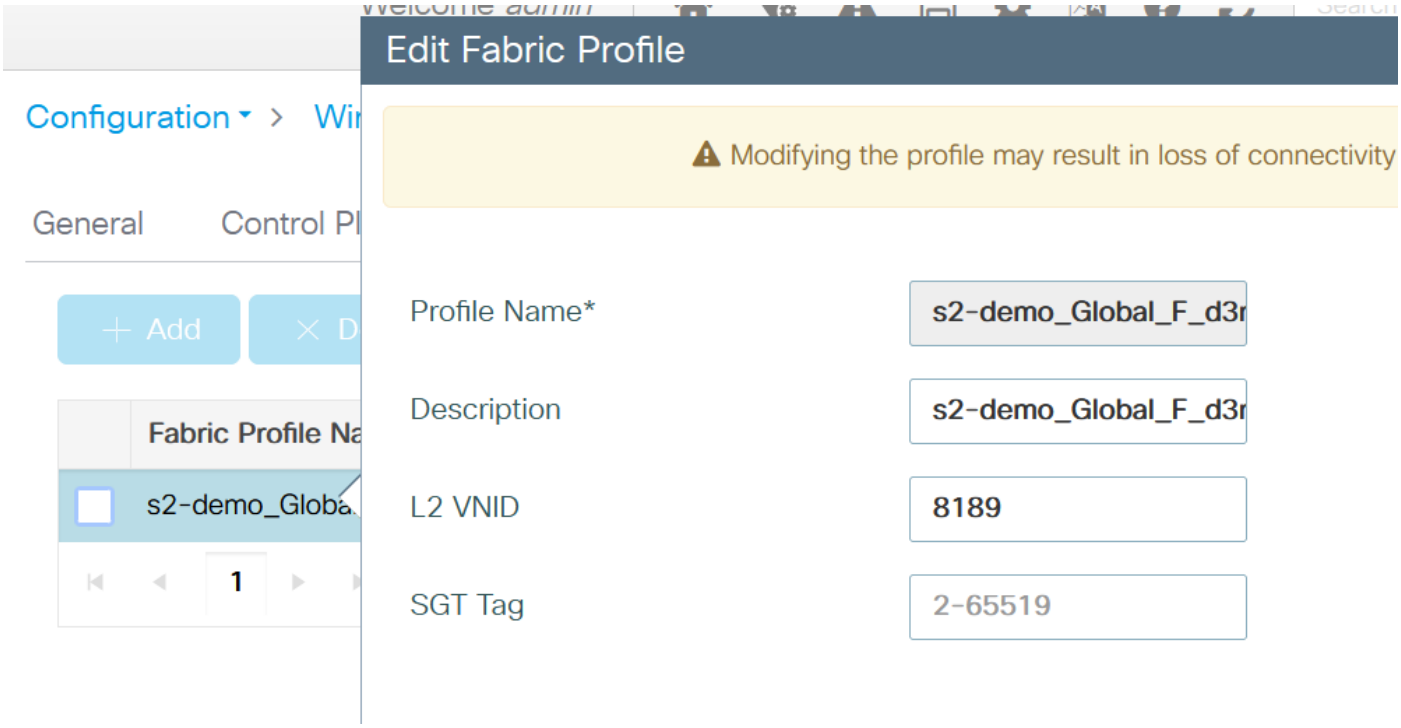
Passaggio 4. Gli SSID vengono mappati al pool nelle rispettive reti virtuali:



SSID mappati

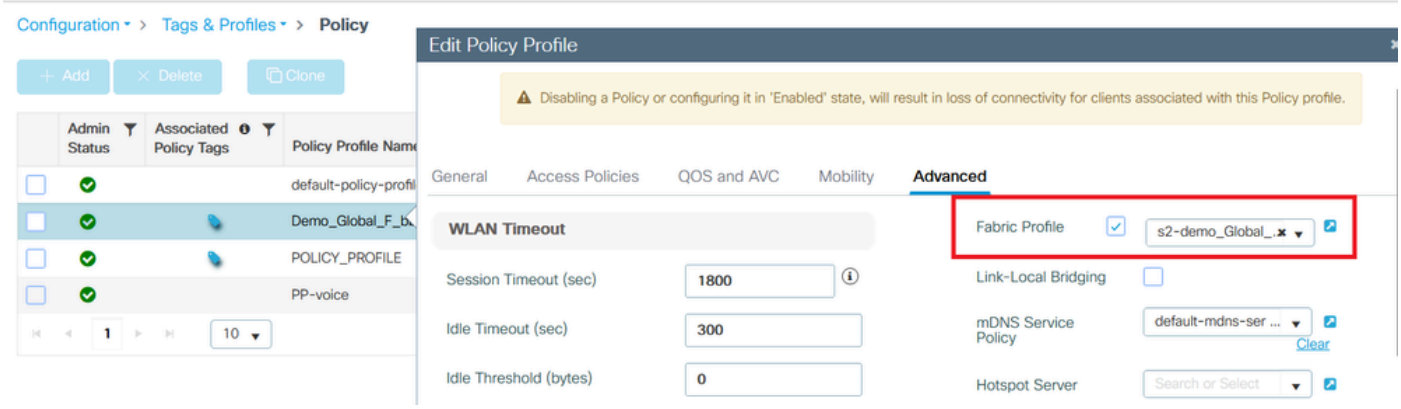
Passaggio 5. Un profilo di infrastruttura con VNID L2 viene aggiunto al pool scelto e il profilo dei criteri viene mappato al profilo di infrastruttura, è abilitato per Fabric.

Dal lato GUI del WLC, selezionare Configuration > Wireless > Fabric > Profiles (Configurazione > Wireless > Fabric > Profili).



Profilo fabric

Passaggio 6. Passare a Configurazione > Tag e profili > Criterio. Verificare il profilo infrastruttura mappato al profilo criteri:



Profilo infrastruttura configurato nel criterio

Verifica

Verifica della configurazione del fabric su WLC e Cisco DNA

Dalla CLI del WLC:

WLC1# show tech

WLC1# show tech wireless

Configurazione del control plane:

lisp router

tabella di localizzazione predefinita

WLC locator-set

172.16.201.202

exit-locator-set

!

sessione map-server WLC a apertura passiva

sito_uci

descrizione map-server configurato da Cisco DNA-Center

authentication-key 7 <Chiave>

Sessione lisp CB1-S1#sh

Sessioni per VRF predefinite, totale: 9, stabilito: 5

Stato Peer Attivo/Inattivo In/Out

172.16.201.202:4342 Su 3d07h 14/14

Configurazione WLC:

fabric wireless

wireless fabric control-plane default-control-plane

indirizzo ip 172.16.2.2, chiave 0 47aa5a

WLC1# show fabric map-server summary

Stato connessione MS-IP

—

172.16.1.2 SU

WLC1# show wireless fabric summary

Stato fabric: Attivato

Piano di comando:

Nome Indirizzo IP Stato chiave

—

default-control-plane 172.16.2.2 47aa5a Up

Dalla GUI del WLC, selezionare Configuration > Wireless > Fabric (Configurazione > Wireless > Fabric) e verificare se lo stato del fabric è Enabled (Abilitato).

Selezionare Configurazione > Wireless > Access Point. Selezionare un punto di accesso dall'elenco. Verificare che lo stato dell'infrastruttura sia Abilitato.

Su Cisco DNA, passare a Provisioning > Siti fabric e verificare se si dispone di un sito fabric. Sul sito dell'infrastruttura, passare a Fabric Infrastructure > Fabric e verificare se il WLC è abilitato come infrastruttura.

Risoluzione dei problemi

Il client non ottiene l'indirizzo IP

Passaggio 1. Verificare se l'SSID è fabric. Dalla GUI del WLC, selezionare Configurazione > Tag e profili > Criteri. Selezionare il criterio e passare a Avanzate. Verificare se il profilo dell'infrastruttura è abilitato.

Passaggio 2. Verificare se il client è bloccato nello stato di apprendimento IP. Dalla GUI del WLC, selezionare Monitoraggio > Wireless > Client. Verificare lo stato del client.

Passaggio 3. Verificare se il criterio è DHCP obbligatorio.

Passaggio 4. Se il traffico viene commutato localmente tra il nodo del punto di accesso e il nodo del bordo, raccogliere i log del punto di accesso (traccia del client) per la connessione del client. Verificare se il rilevamento DHCP è stato inoltrato. Se non viene ricevuta alcuna offerta DHCP, si verifica un errore nel nodo perimetrale. Se il protocollo DHCP non viene inoltrato, significa che si è verificato un errore nell'access point.

Passaggio 5. È possibile raccogliere un EPC sulla porta del nodo perimetrale per visualizzare i pacchetti DHCP discover. Se il comando DHCP discover packets non è visibile, il problema è nell'access point.

SSID non trasmesso

Passaggio 1. Verificare se le radio AP sono inattive.

Passaggio 2. Verificare che la WLAN sia nello stato attivo e che il SSID di trasmissione sia abilitato.

Passaggio 3. Verificare la configurazione del punto di accesso se il punto di accesso è abilitato per l'infrastruttura. Passare a Configurazione > Wireless > Access Point, selezionare un access point e nella scheda Generale è possibile visualizzare lo stato del fabric abilitato e le informazioni RLOC.

Passaggio 4. Passare a Configurazione > Wireless > Fabric > Control Plane. Verificare che il control plane sia configurato (con l'indirizzo IP).

Passaggio 5. Passare a Configurazione > Tag e profili > Criterio. Selezionare il criterio e passare a Avanzate. Verificare se il profilo dell'infrastruttura è abilitato.

Passaggio 6. Passare a Cisco DNA e ripetere la procedura su Crea SSID e Esegui provisioning WLC. Il Cisco DNA deve spingere di nuovo il SSID sul WLC.

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).