Implemente un acceso definido por software para redes inalámbricas con DNA

Contenido

Introducción

Este documento describe cómo implementar SDA para la tecnología inalámbrica relacionada con el WLC habilitado para el entramado y el LAP de acceso en el DNA de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de controladores LAN inalámbricos (WLC) 9800
- Puntos de acceso ligeros (LAP)
- DNA de Cisco

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 9800-CL WLC Cisco IOS® XE, versión 17.9.3
- Puntos de acceso de Cisco: 9130AX, 3802E, 1832I
- Cisco DNA versión 2.3.3.7

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

SD-Access.

El acceso definido por software establece y aplica automáticamente políticas de seguridad en toda la red, con reglas dinámicas y segmentación automatizada, y permite al usuario final controlar y configurar la forma en que los usuarios se conectan a su red. SD-Access establece un nivel inicial de confianza con cada terminal conectado y lo supervisa continuamente para volver a verificar su nivel de confianza. Si un terminal no se comporta con normalidad o se detecta una amenaza, el usuario final puede contenerlo inmediatamente y tomar medidas, antes de que se produzca una brecha, reducir el riesgo empresarial y proteger sus recursos. Solución totalmente integrada y fácil de implementar y configurar tanto en redes nuevas como implementadas.

SD-Access es una tecnología de Cisco que representa una evolución de la red de campus tradicional que ofrece redes basadas en intención (IBN) y control de políticas central con el uso de componentes de redes definidas por software (SDN).

Tres pilares de red de SD-Access:

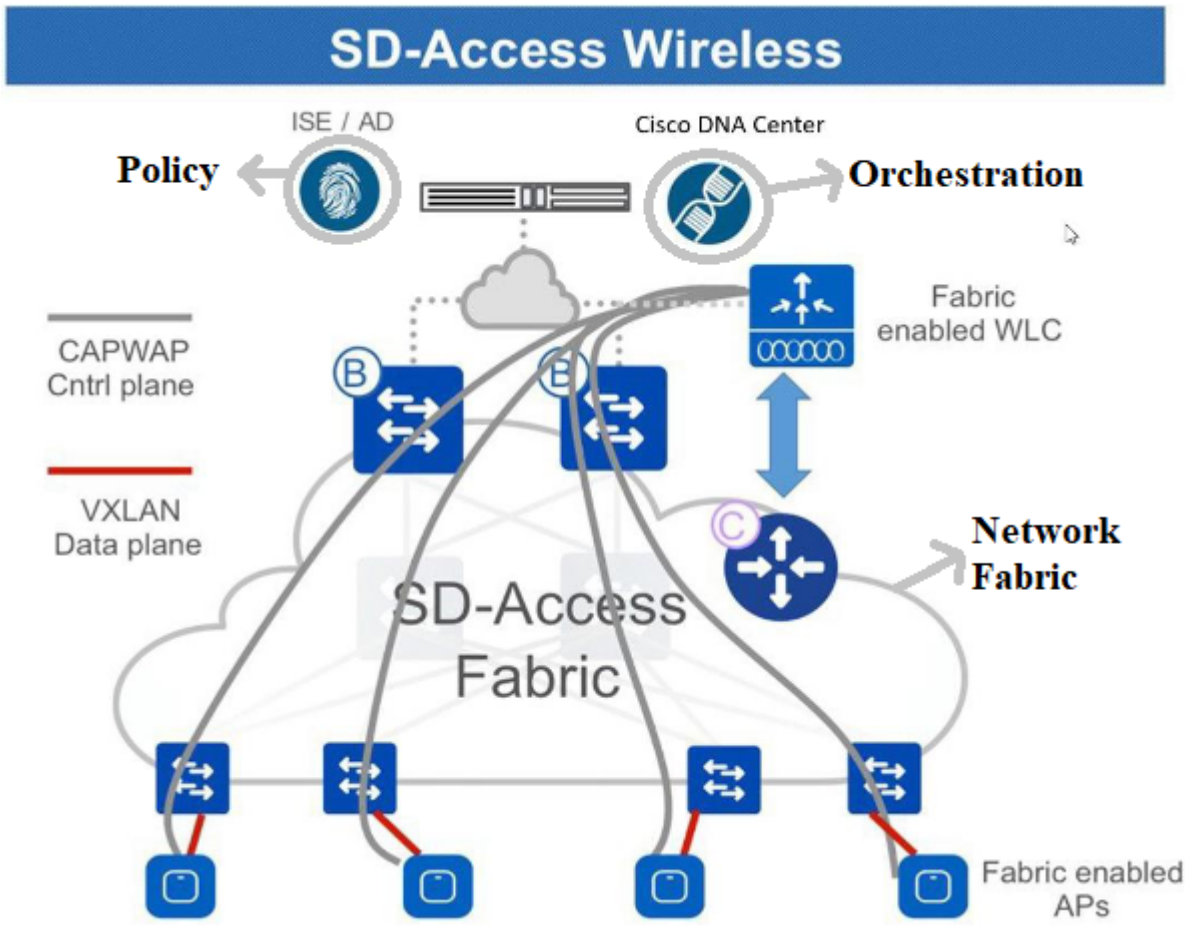
1. Un fabric de red: Se trata de una abstracción de la propia red que admite superposiciones programables y virtualización. El fabric de red admite el acceso por cable e inalámbrico y permite alojar varias redes lógicas segmentadas entre sí y definidas por objetivos empresariales.

2. Orquestación: Cisco DNA es el motor de orquestación de SDA. Cisco DNA funciona como un controlador SDN. Implementa políticas y cambios de configuración en el fabric. También incorpora una herramienta compatible con el diseño de red y con las operaciones de telemetría de red en tiempo real y los análisis de rendimiento a través de DNA Assurance. La función de Cisco DNA es orquestar el fabric de red para ofrecer cambios en las políticas y las intenciones de la red en cuanto a seguridad, calidad del servicio (QoS) y microsegmentación.
3. Política: Identity Services Engine (ISE) es la herramienta que define la política de red. ISE organiza el modo en que los dispositivos y los nodos se segmentan en redes virtuales. ISE también define etiquetas de grupo escalables (SGT) que utilizan los dispositivos de acceso para segmentar el tráfico de los usuarios a medida que entra en el fabric. Los SGR son responsables de aplicar la política de microsegmentación definida por ISE.

SDA se basa en una orquestación centralizada. Las combinaciones de Cisco DNA como motor de orquestación programable, ISE como motor de políticas y una nueva generación de switches programables lo convierten en un sistema de fabric mucho más flexible y gestionable que cualquier otro que se haya presentado anteriormente.

Nota: Este documento trata específicamente sobre SD-Access Wireless.

El fabric de red se compone de los siguientes elementos:

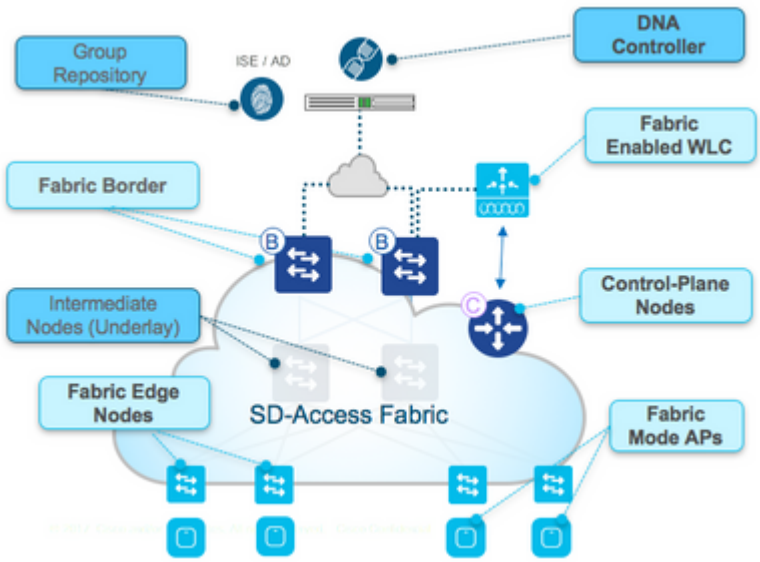


Elementos del fabric de red

La integración inalámbrica en el fabric conlleva varias ventajas para la red inalámbrica, por ejemplo: abordando la simplificación, la movilidad con subredes extendidas a través de ubicaciones físicas; y microsegmentación con una política centralizada que es uniforme en los dominios conectados por cable e inalámbricos. También permite al controlador reducir el plano de datos para reenviar tareas mientras sigue funcionando como el plano de control y servicios centralizados para la red inalámbrica. Por lo tanto, la escalabilidad del controlador inalámbrico se ve aumentada porque ya no es necesario procesar el tráfico del plano de datos, de forma similar al modelo FlexConnect.

Arquitectura inalámbrica de acceso SD

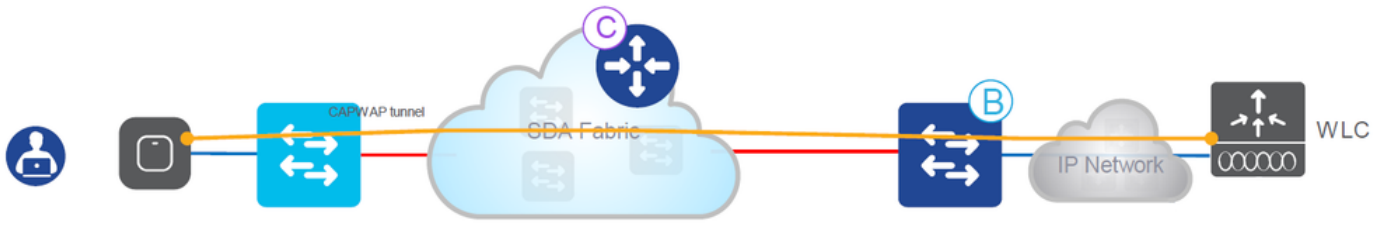
Overview



Descripción general de SDA

Existen dos modelos de implementación inalámbrica SDA principales compatibles:

Uno es un método de transmisión libre (OTT), una implementación CAPWAP tradicional conectada en la parte superior de una red por cable de fabric. El fabric SDA transporta el control CAPWAP y el tráfico del plano de datos al controlador inalámbrico:

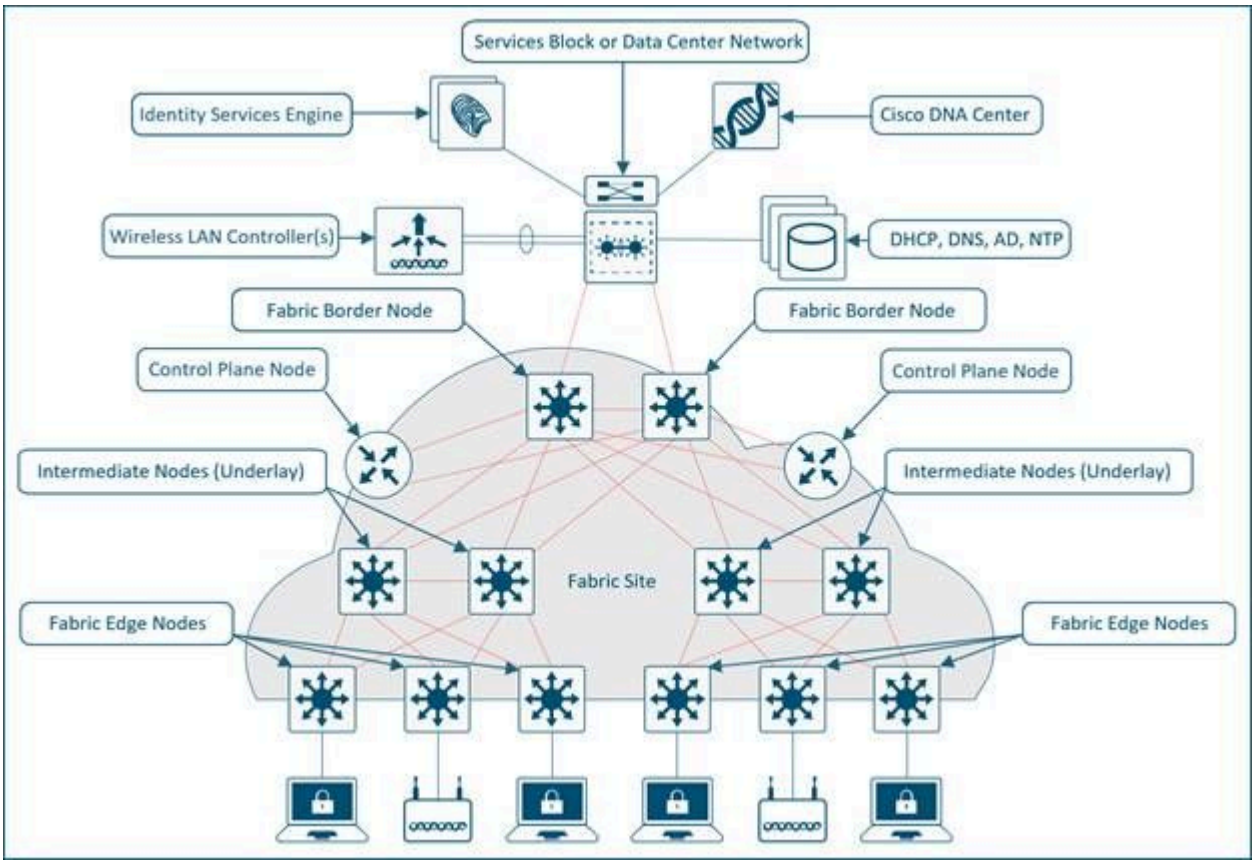


Método Over-The-Top

En este modelo de implementación, el fabric SDA es una red de transporte para el tráfico

inalámbrico (un modelo que se suele implementar en las migraciones). El AP funciona de manera muy similar al modo local clásico: tanto los planos de datos como de control CAPWAP terminan en el controlador, lo que significa que el controlador no participa directamente en el fabric. Este modelo se utiliza a menudo cuando los switches por cable se migran por primera vez al fabric SDA, pero la red inalámbrica todavía no está preparada para la integración completa de la superposición del fabric.

Los otros modelos de implementación utilizan el modelo SDA totalmente integrado. La red inalámbrica está totalmente integrada en el fabric y participa en superposiciones, lo que permite que diferentes WLAN formen parte de diferentes redes virtuales (VPN). El controlador inalámbrico solo administra el plano de control CAPWAP (para administrar los AP), y el plano de datos CAPWAP no llega al controlador:



Modelo SDA completamente integrado

El plano de datos inalámbricos se gestiona de forma similar a los switches por cable: cada punto de acceso encapsula los datos en VXLAN y los envía a un nodo de la frontera del fabric, donde a continuación se envían a través del fabric a otro nodo de la frontera. Los controladores inalámbricos deben configurarse como controladores de fabric, lo que supone una modificación con respecto a su funcionamiento normal.

Los controladores habilitados para fabric se comunican con el plano de control de fabric, registra las direcciones MAC de los clientes de capa 2 y la información del identificador de red virtual (VNI) de capa 2. Los AP son responsables de la comunicación con los terminales inalámbricos y ayudan al plano de datos VXLAN mediante el encapsulamiento y el tráfico de desencapsulamiento.

Terminología y funciones de SDA

El fabric de red se compone de los siguientes elementos:

- Nodo del plano de control: Se trata del sistema de asignación de ubicaciones (base de datos de host) que forma parte del plano de control del protocolo de separación de ubicaciones (LISP), que gestiona la identidad de terminales (EID) para las relaciones de ubicación (o las relaciones de dispositivos). El plano de control puede ser un router dedicado que proporcionó funciones de plano de control o puede coexistir con otros elementos de la red del fabric.
- Nodos de límite de fabric: Normalmente, un router que funciona en el borde entre las redes externas y el fabric SDA, que proporciona servicios de routing a las redes virtuales del fabric. Conecta las redes externas de capa 3 al fabric SDA.
- Nodos periféricos del fabric: Dispositivo del fabric que conecta dispositivos que no son de fabric, como switches, puntos de acceso y routers al fabric SDA. Estos son los nodos que crean los túneles superpuestos virtuales y las VLAN con la LAN extensible virtual (VXLAN) e imponen las SGT en el tráfico enlazado al fabric. Las redes de ambos lados del extremo del fabric se encuentran dentro de la red SDA. Conectan los terminales con cables al fabric de acceso SD.
- Nodos intermedios: Estos nodos se encuentran dentro del núcleo del fabric SDA y se conectan a nodos de borde o de borde. Los nodos intermedios simplemente reenvían el tráfico SDA como paquetes IP, sin darse cuenta de que hay varias redes virtuales involucradas.
- WLC de fabric: Controlador inalámbrico habilitado para fabric que participa en el plano de control SDA pero que no procesa el plano de datos CAPWAP.
- AP de modo de fabric: Puntos de acceso habilitados para fabric. El tráfico inalámbrico se encapsula en VXLAN en el AP, lo que permite enviarlo al fabric a través de un nodo de borde.
- DNA de Cisco (DNAC): El controlador de SDN empresarial para la red de superposición de fabric de acceso definido por software (SDA) y es responsable de las tareas de automatización y garantía. También se puede utilizar para algunas tareas de automatización y relacionadas con los dispositivos de red que forman la base (que no están relacionados con SDA).
- ISE: Identity Services Engine (ISE) es una plataforma de políticas mejorada que puede prestar servicio a una gran variedad de roles y funciones, entre los que destaca el servidor de autenticación, autorización y contabilidad (AAA). ISE suele interactuar con Active Directory (AD), pero los usuarios se pueden configurar localmente, así como en ISE para implementaciones más pequeñas.

Nota: El plano de control es una parte fundamental de la infraestructura de la arquitectura SDA, por lo que se recomienda implementarlo de forma flexible.

Redes subyacentes y superpuestas

La arquitectura SDA utiliza tecnología de fabric que admite redes virtuales programables (redes superpuestas) que se ejecutan en una red física (una red subyacente).

Una tela es una superposición.

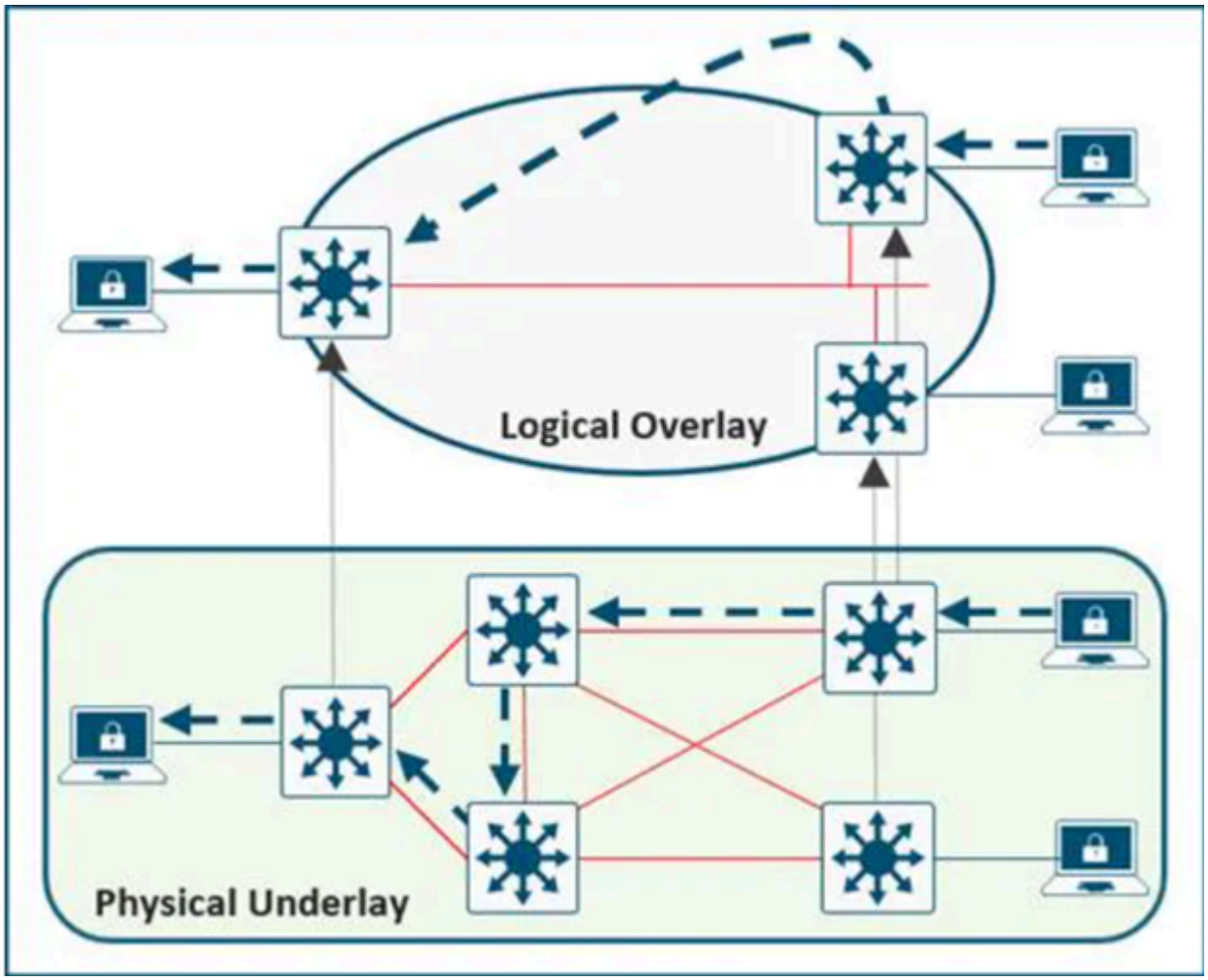
Una red superpuesta es una topología lógica utilizada para conectar dispositivos virtualmente, construida sobre una topología subyacente física arbitraria. Utiliza atributos de reenvío alternativos para proporcionar servicios adicionales que no proporciona el subyacente. Se crea sobre la capa subyacente para crear una o más redes virtualizadas y segmentadas. Debido a la naturaleza definida por software de las superposiciones, es posible conectarlas de formas muy flexibles sin las limitaciones de la conectividad física. Se trata de una forma sencilla de aplicar políticas de seguridad, ya que la superposición puede programarse para tener un único punto de salida físico (el nodo de borde del fabric) y se puede utilizar un firewall para proteger las redes detrás de él (independientemente de si se pueden localizar). La superposición encapsula el tráfico con el uso de VXLAN. VXLAN encapsula tramas de capa 2 completas para su transporte a través de la capa subyacente con cada red superpuesta identificada por un identificador de red VXLAN (VNI). Los fabrics superpuestos suelen ser complejos y requieren una cantidad significativa de sobrecarga del administrador en las nuevas redes virtuales implementadas o para implementar políticas de seguridad.

Ejemplos de redes superpuestas:

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

Una red subyacente está definida por los nodos físicos, como switches, routers y puntos de acceso inalámbricos, que se utilizan para implementar la red SDA. Todos los elementos de red de la capa subyacente deben establecer la conectividad IP mediante el uso de un protocolo de routing. Aunque no es probable que la red subyacente utilice el modelo de núcleo, distribución y acceso tradicional, debe utilizar una base de capa 3 bien diseñada que ofrezca un sólido rendimiento, escalabilidad y alta disponibilidad.

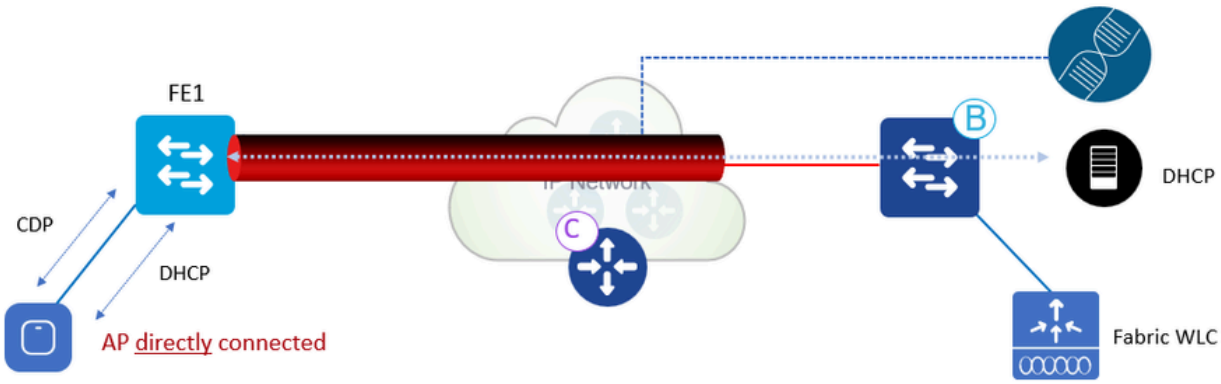
Nota: SDA admite IPv4 en la red subyacente e IPv4 o IPv6 en redes superpuestas.



Redes subyacentes y superpuestas

Flujos de trabajo básicos

Incorporación de AP



Flujo de trabajo de unión a PA

Flujo de trabajo de unión a PA:

1. El administrador configura el conjunto de AP en DNAC en INFRA_VN. Cisco DNA

preaprovisiona una configuración en todos los nodos de frontera del fabric para incorporar automáticamente los puntos de acceso.

2. El AP está conectado y se enciende. Fabric Edge detecta que es un AP a través de CDP y aplica la macro para asignar (o la plantilla de interfaz) el puerto del switch a la VLAN correcta.

3. AP obtiene una dirección IP vía DHCP en la superposición.

4. Fabric Edge registra la dirección IP y MAC (EID) de los AP y actualiza el plano de control (CP).

5. AP aprende WLC IP con métodos tradicionales. El AP de entramado se une como un AP de modo local.

6. El WLC verifica si es apto para el entramado (AP del Wave 2 o del Wave 1).

7. Si el AP se soporta para el entramado, el WLC consulta el CP para saber si el AP está conectado al entramado.

8. El plano de control (CP) responde al WLC con RLOC. Esto significa que el punto de acceso está conectado al fabric y se muestra como "habilitado para fabric".

9. El WLC hace un registro del LISP del L2 para el AP en el CP (que es registro "especial" seguro del cliente del AP). Esto se utiliza para pasar información importante de metadatos del WLC al borde del entramado.

10. En respuesta a este registro de proxy, el plano de control (CP) notifica al borde del entramado y pasa los metadatos recibidos del WLC (indicador que dice que es un AP y la dirección IP del AP).

11. Fabric Edge procesa la información, aprende que es un AP y crea una interfaz de túnel VXLAN a la IP especificada (optimización: el lado del switch está listo para que los clientes se unan).

Los comandos debug/show se pueden utilizar para verificar y validar el flujo de trabajo de unión de AP.

Plano de Control

debug lisp control-plane all

show lisp instance-id <L3 instance id> ipv4 server (Debe mostrar la dirección IP del AP registrada por el switch periférico donde está conectado el AP).

show lisp instance-id <L2 instance id> ethernet server (Debe mostrar la radio AP, así como la dirección mac ethernet, la radio AP registrada por el WLC y la mac ethernet por el switch de borde donde está conectado el AP).

Switch perimetral

debug access-tunnel all

debug lisp control-plane all

show access-tunnel summary

show lisp instance < L2 instance id> ethernet database wlc access-points (Debe mostrar la MAC de radio AP aquí.)

WLC

show fabric ap summary

Depuraciones de WLC LISP

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

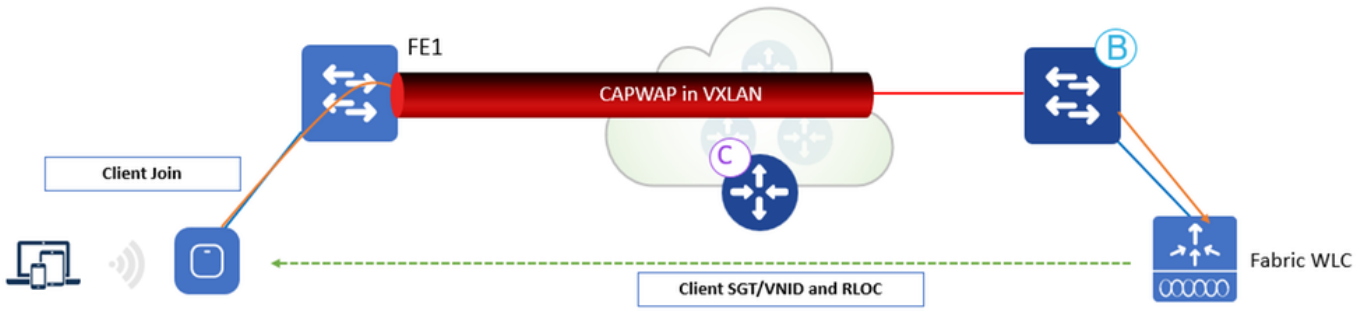
set platform software trace wncd chassis active r0 lisp-agent-ha debug

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

Punto de Acceso

show ip tunnel fabric

Cliente incorporado



Flujo de trabajo integrado del cliente

Flujo de trabajo integrado del cliente:

1. El cliente se autentica en una WLAN habilitada para Fabric. WLC obtiene SGT de ISE, actualiza AP con L2VNID y SGT del cliente junto con IP RLOC. El WLC conoce el RLOC del AP de la base de datos interna.

2. El proxy WLC registra la información del cliente L2 en CP; Este es un mensaje modificado por LISP para pasar información adicional, como la SGT del cliente.

3. El extremo del fabric recibe la notificación del PC y agrega el MAC del cliente en L2 a la tabla de reenvío, y va a buscar la política de ISE en función de la SGT del cliente.

4. El cliente inicia la solicitud DHCP.

5. AP lo encapsula en VXLAN con información de VNI L2.

6. Fabric Edge asigna VNID L2 a la interfaz VLAN y reenvía DHCP en la superposición (igual que para un cliente de fabric cableado).

7. El cliente recibe una dirección IP de DHCP.

8. El snooping DHCP (y/o ARP para estática) activa el registro de EID del cliente por parte del Fabric Edge en el CP.

Los comandos debug/show se pueden utilizar para verificar y validar el flujo de trabajo interno del cliente.

Plano de Control

debug lisp control-plane all

Switch perimetral

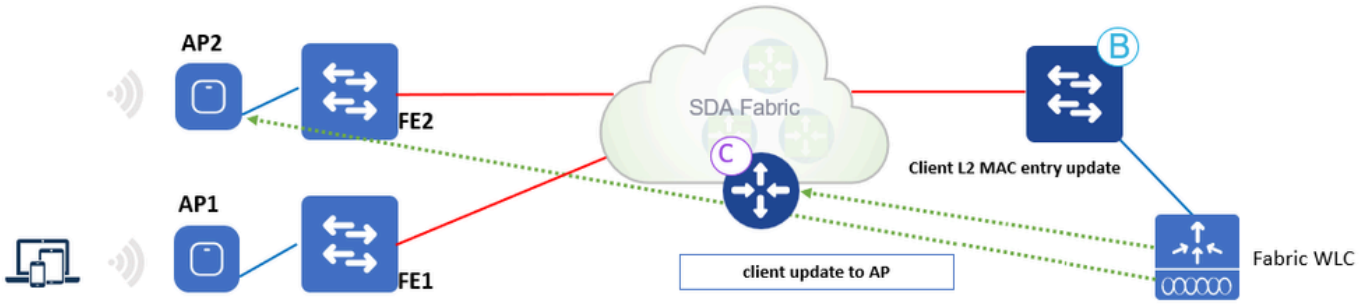
debug lisp control-plane all

debug ip dhcp snooping packet/event

WLC

Para la comunicación LISP, los mismos debugs que se unen al AP.

Itinerancia de clientes



Flujo de trabajo de itinerancias del cliente

Flujo de trabajo de itinerancias del cliente:

1. El cliente se traslada a AP2 en FE2 (itinerancia entre switches). El WLC es notificado por el AP.

2. El WLC actualiza la tabla de reenvío en el AP con la información del cliente (SGT, RLOC).

3. El WLC actualiza la entrada L2 MAC en el PC con el nuevo borde 2 de la estructura RLOC.

4. CP notifica a continuación:

   - Fabric Edge FE2 (switch de itinerancia a) para agregar el MAC del cliente a la tabla de reenvío que apunta al túnel VXLAN.
   - Fabric Edge FE1 (switch de itinerancia) para limpiar el cliente inalámbrico.

5. Fabric Edge actualiza la entrada L3 (IP) en la base de datos CP cuando recibe tráfico.

6. La itinerancia es de capa 2, ya que el Fabric Edge 2 tiene la misma interfaz VLAN (Anycast GW).

Configurar

Diagrama de la red

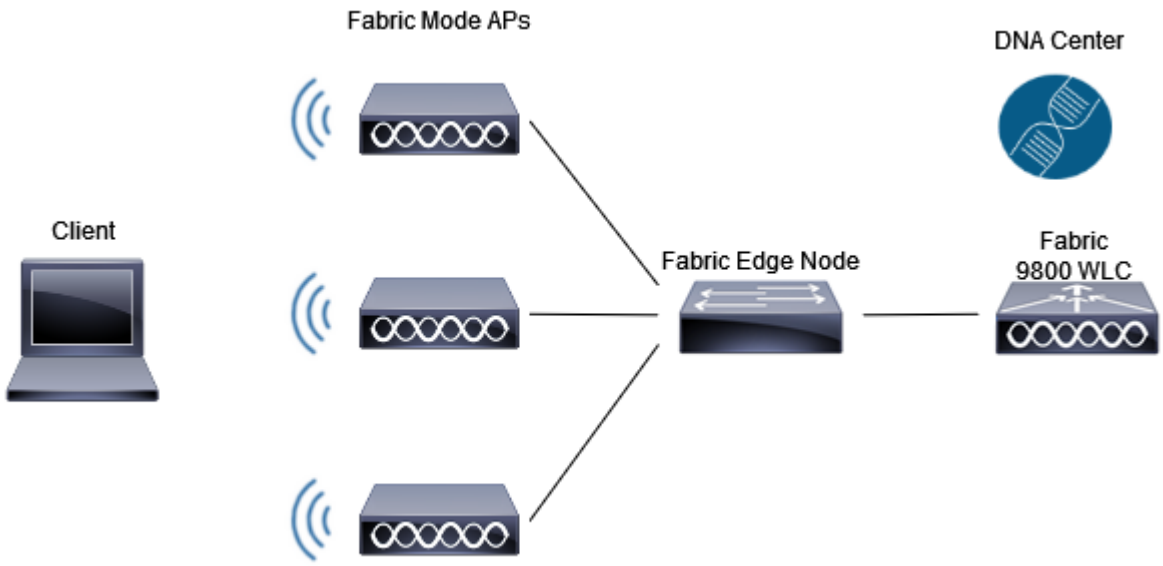


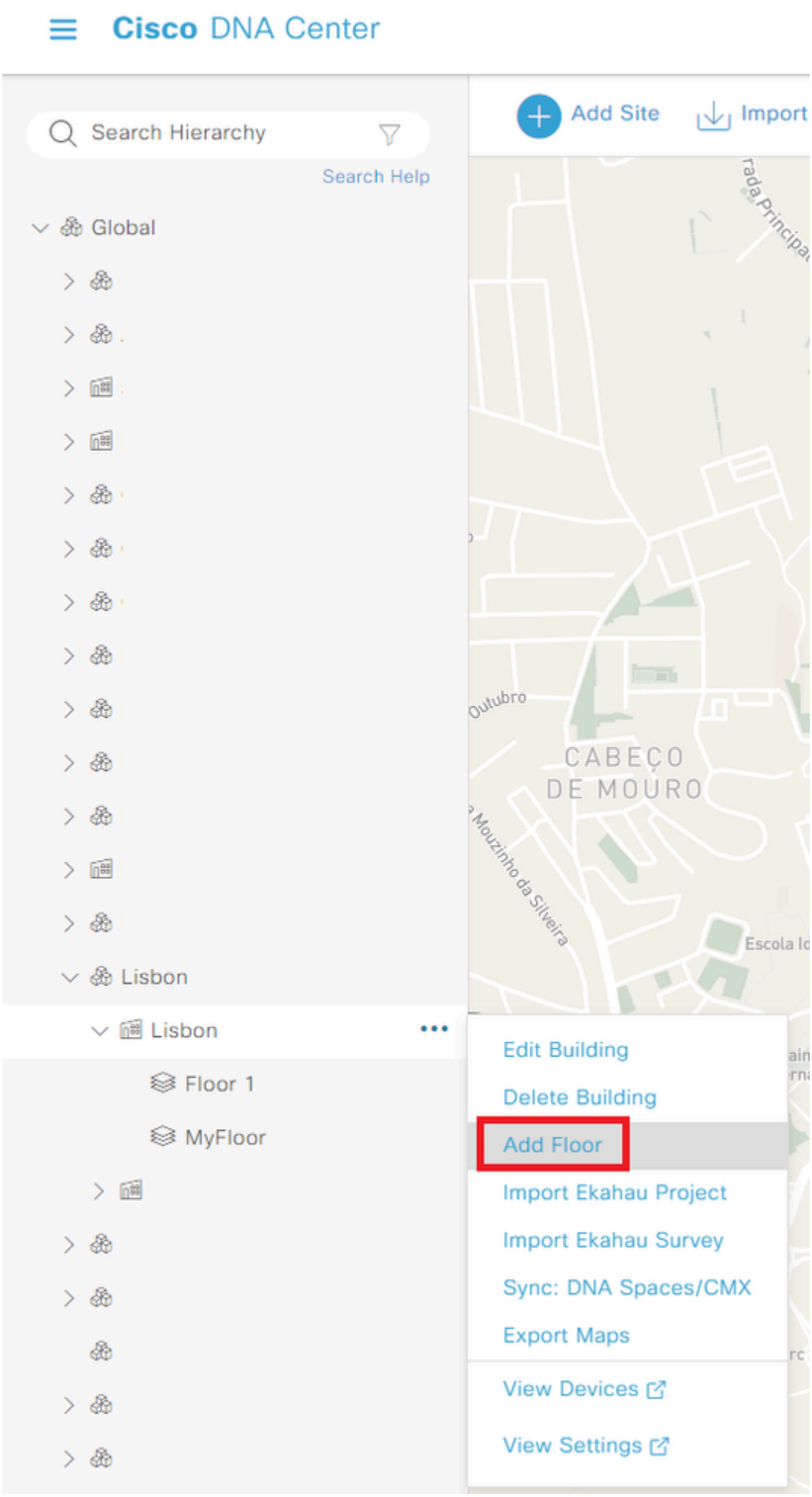
Diagrama de la red

Detección y provisión de WLC en DNA de Cisco

Agregar WLC

Paso 1. Navegue hasta la ubicación donde desea agregar el WLC. Puede añadir un nuevo edificio o planta.

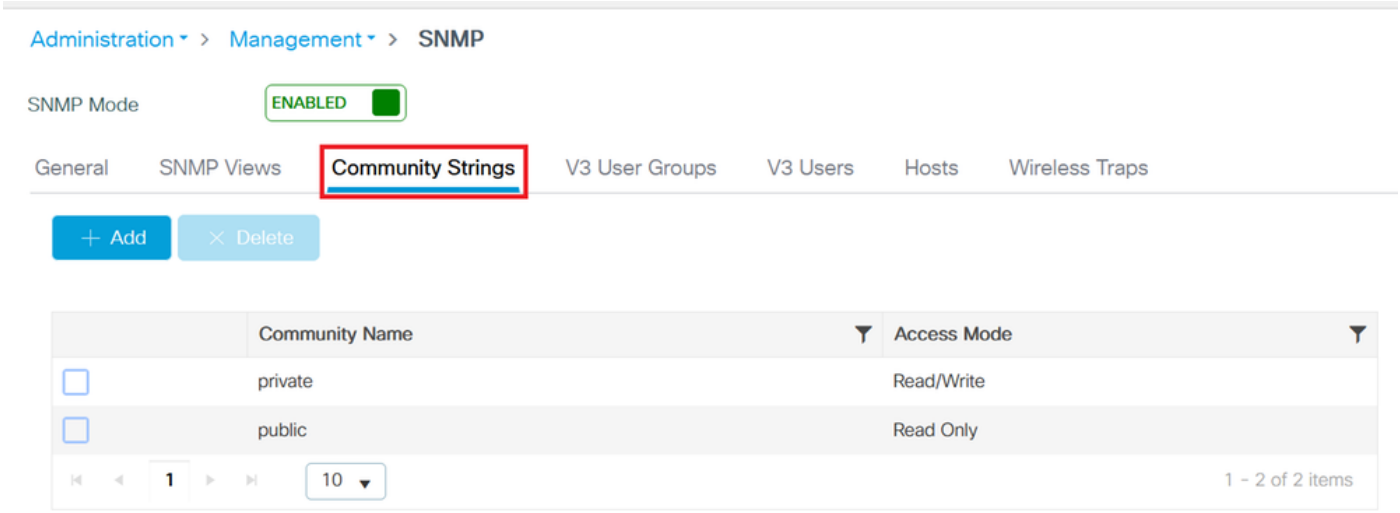
Navegue hasta Diseño > Jerarquía de red e ingrese al edificio/planta, o puede crear un nuevo piso, como se muestra en la imagen:



Crear nueva planta

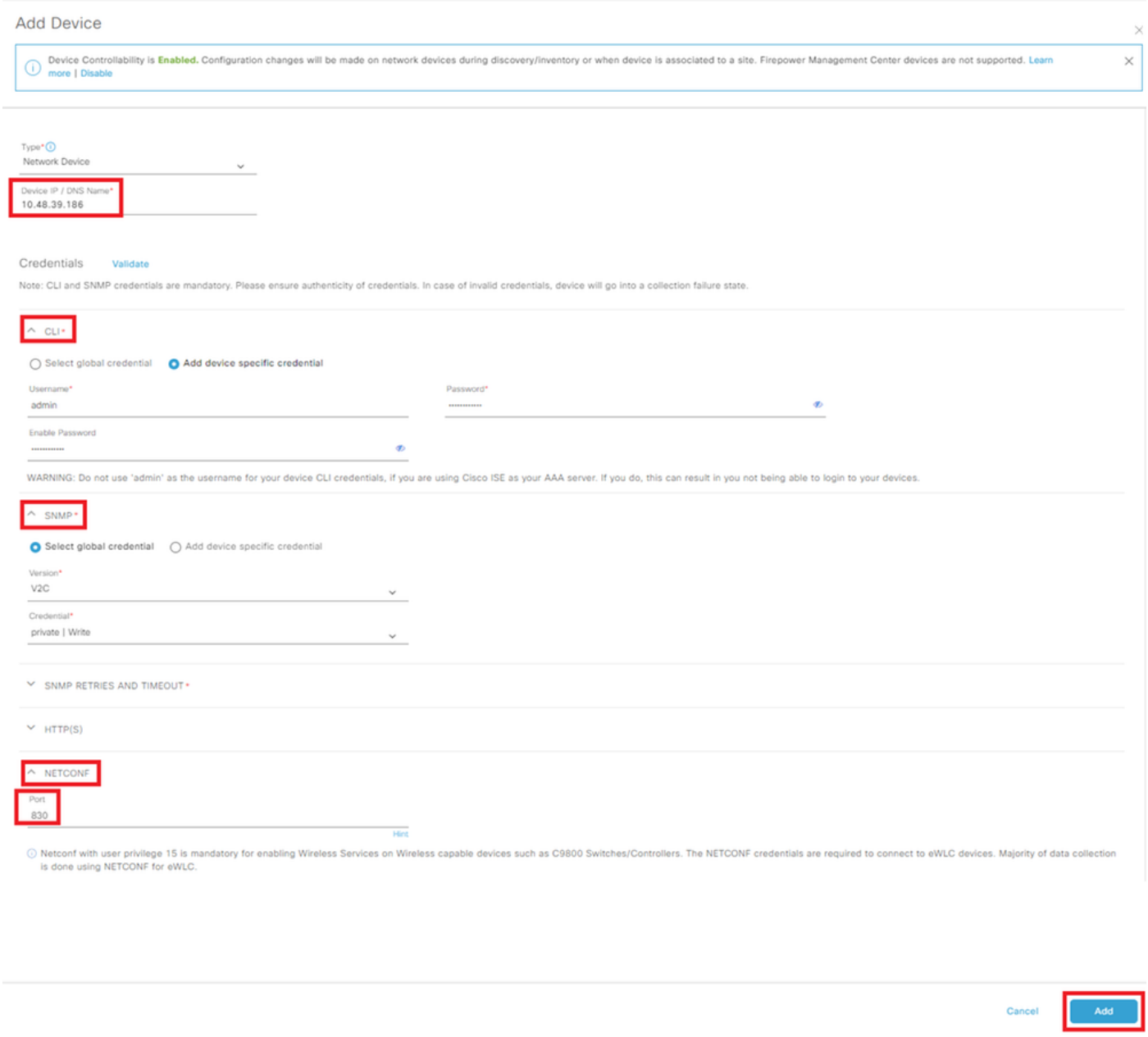
Paso 2. Agregue piso. También puede cargar una imagen de la planta del piso

y verifique la cadena configurada. Debe agregar la cadena de comunidad SNMP correcta cuando agrega el WLC en el ADN de Cisco, y asegurarse de que netconf-yang esté habilitado en el WLC 9800 con los comandos de estado show netconf-yang. Al final, haga clic en Add:



Configuración de SNMP

Paso 5. Agregue la dirección IP del WLC, las credenciales de CLI (las credenciales que Cisco DNA utiliza para iniciar sesión en el WLC y estas deben configurarse en el WLC antes de agregarlo al Cisco DNA), la cadena SNMP y verifique si el puerto NETCONF está configurado en el puerto 830:



Agregar WLC

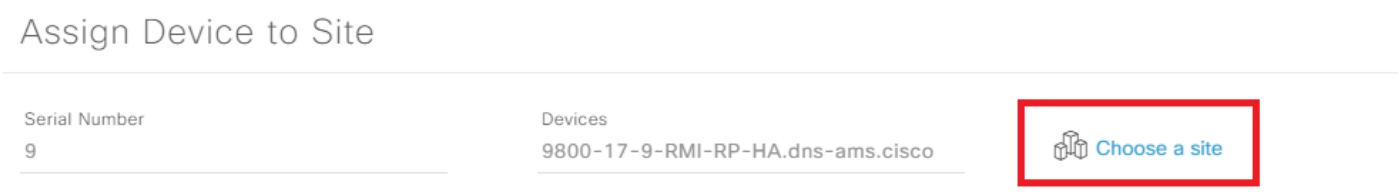
El WLC se muestra como NA porque el ADN de Cisco aún está en proceso de sincronización:

WLC en proceso de sincronización

Cuando termine el proceso de sincronización, puede ver el nombre del WLC, la dirección IP, si es accesible, administrado y la versión de software:

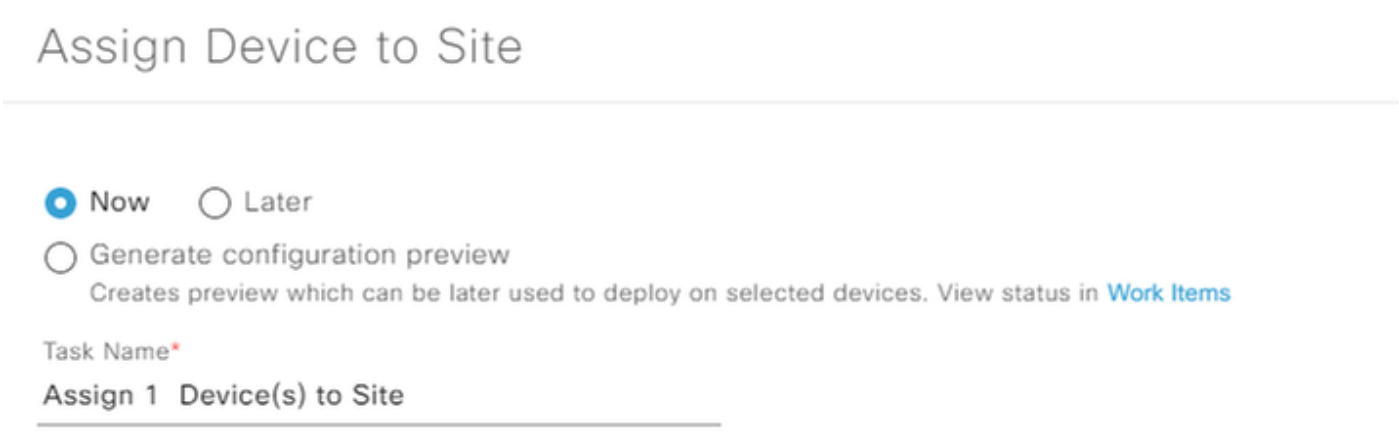
WLC sincronizado

Paso 6. Asigne el WLC a un sitio. En la lista de dispositivos, haga clic en Asignar y elija un sitio:



Asignar dispositivo al sitio

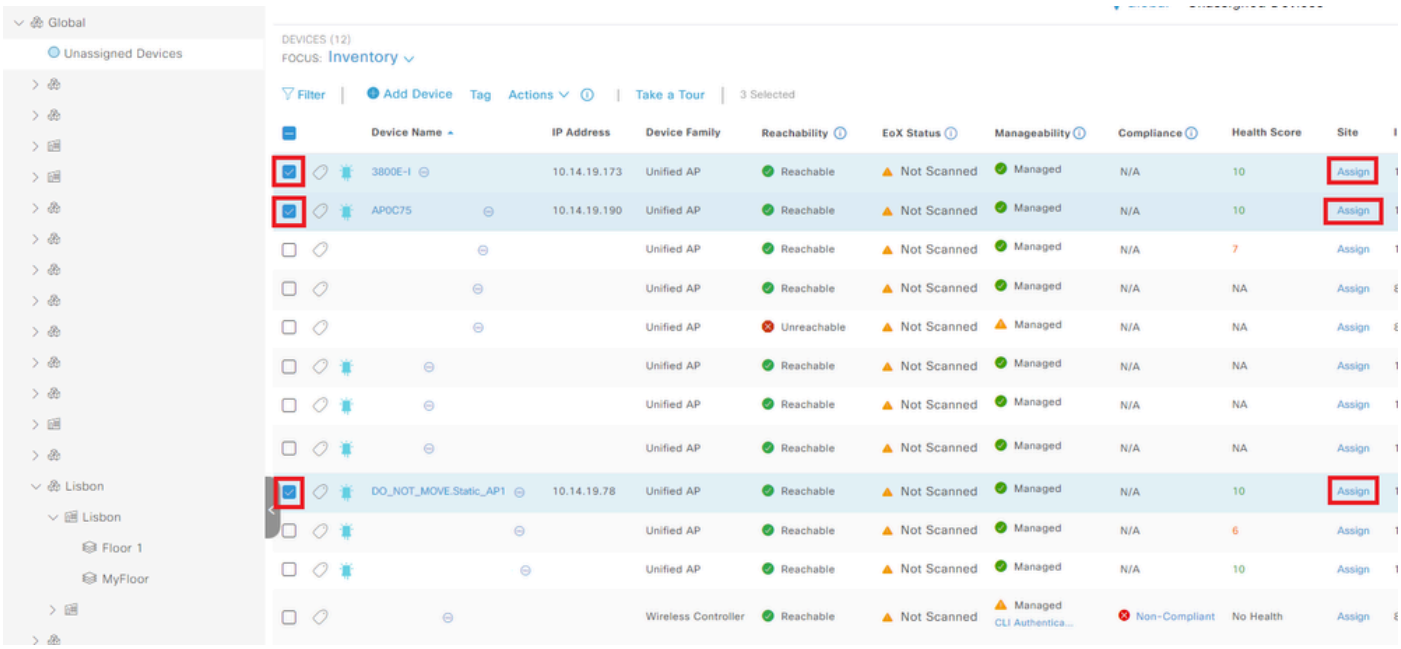
Puede decidir asignar el sitio ahora o más tarde:



Asignar dispositivo al sitio ahora o más tarde

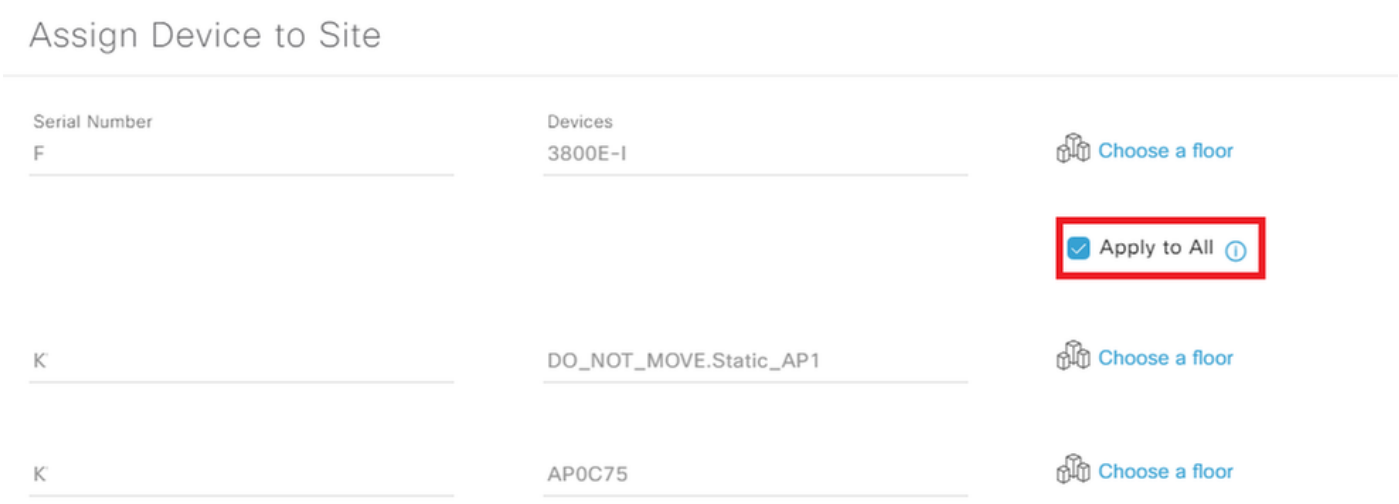
Agregar puntos de acceso

Paso 1.Una vez que el WLC es agregado y alcanzable, navegue a Provisión > Inventario > Global > Dispositivos no asignados y busque los AP que usted ha unido a su WLC:



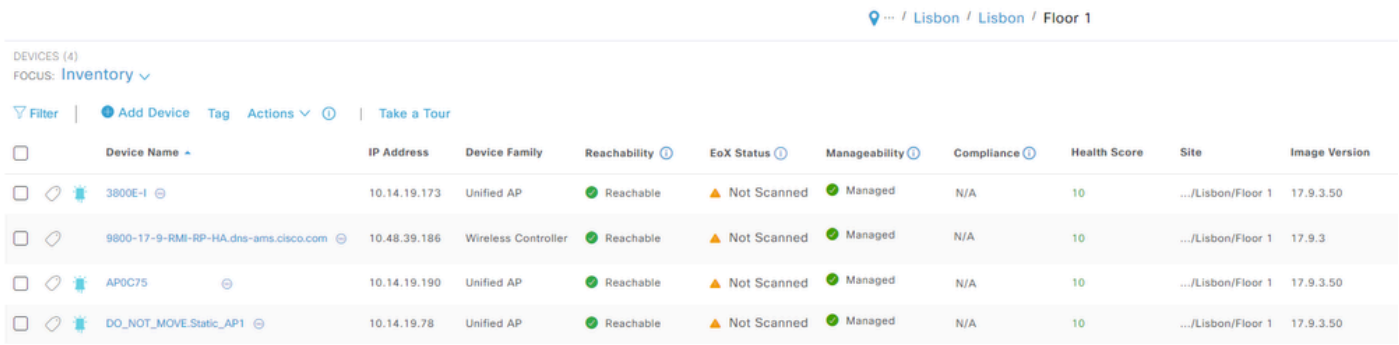
Agregar puntos de acceso

Paso 2. Seleccione la opción Asignar. Asigne los APs a un sitio. Marque la casilla Apply to All para realizar la configuración para más de un dispositivo al mismo tiempo.



Asignar puntos de acceso al sitio

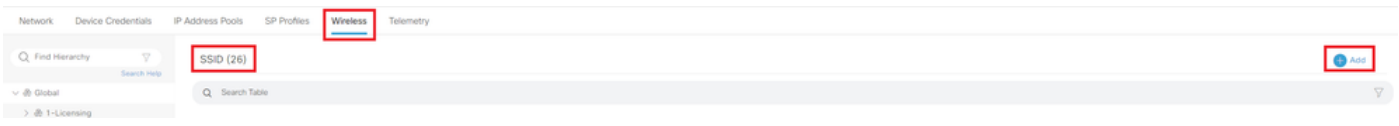
Navegue hasta su planta y podrá ver todos los dispositivos asignados a ella - WLC y AP:



Dispositivos asignados al sitio

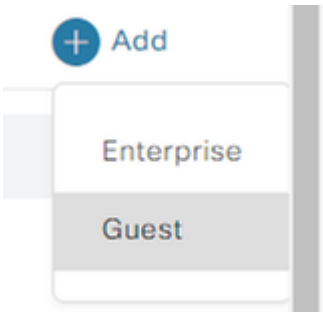
Crear SSID

Paso 1. Navegue hasta Diseño > Configuración de red > Inalámbrico > Global y agregue un SSID:



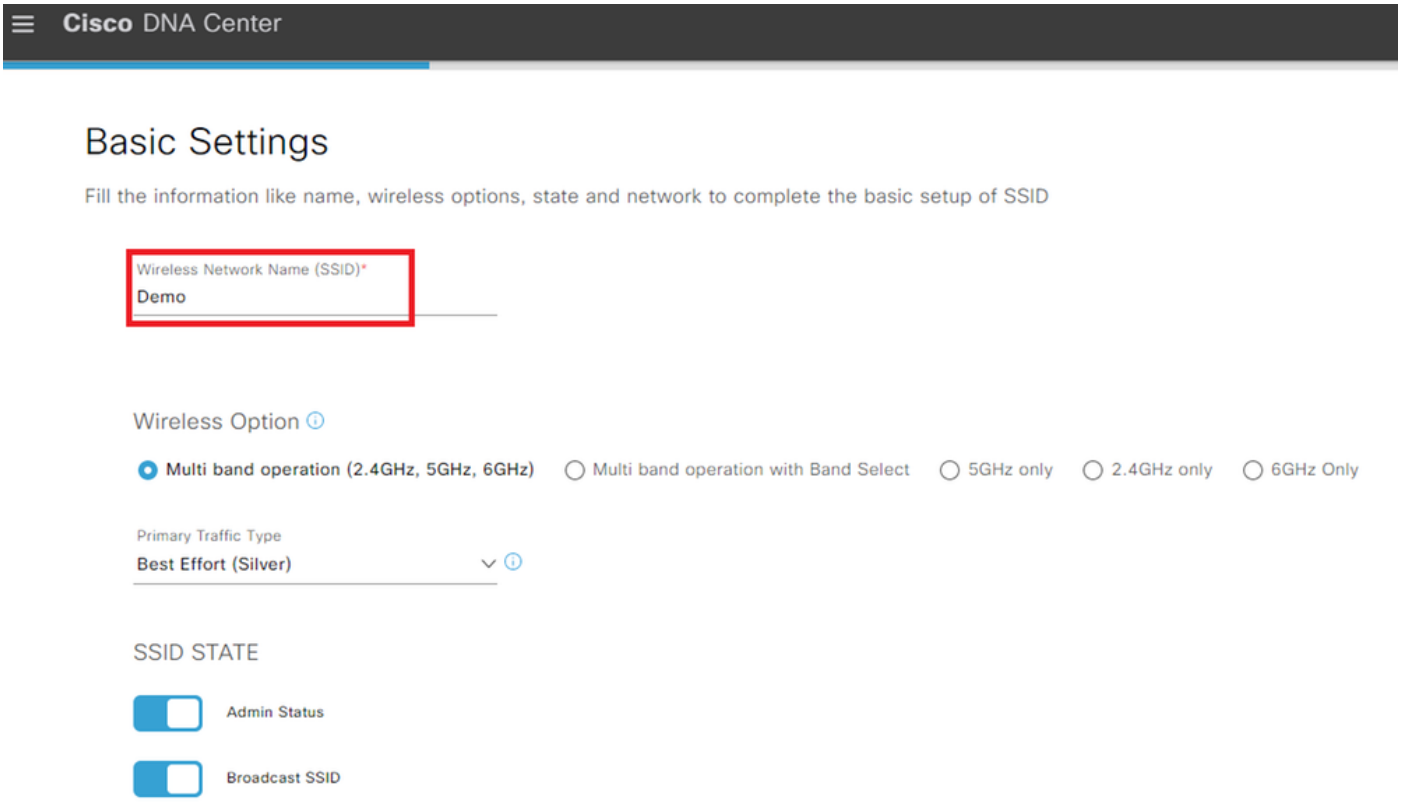
Crear SSID

Puede crear un Enterprise SSID o un Guest SSID. En esta demostración, se crea un SSID de invitado:

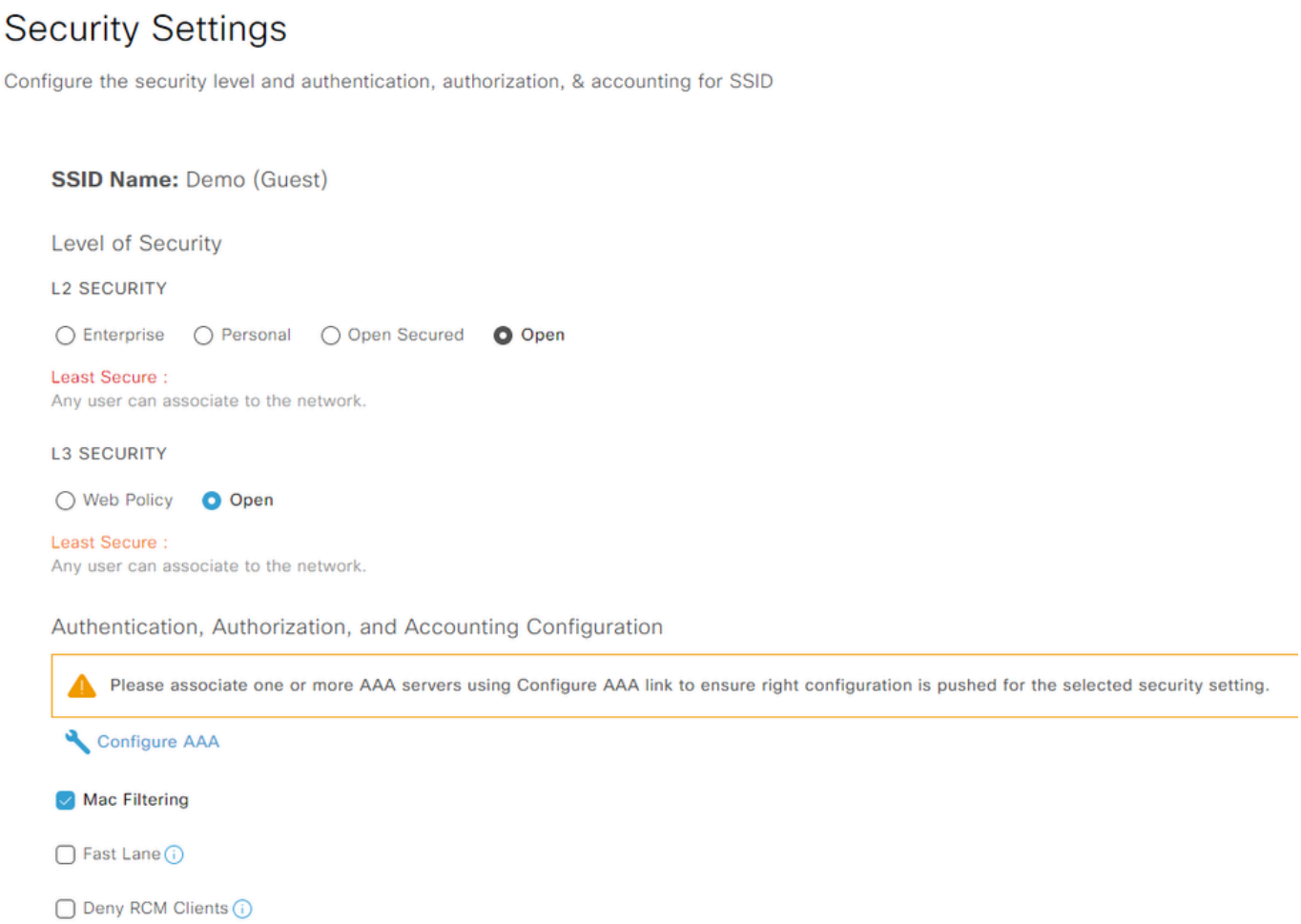


SSID de empresa o invitado

Paso 2. Elija la configuración que desee para el SSID. En este caso, se crea un SSID abierto. El estado del administrador y el SSID de difusión deben estar habilitados:



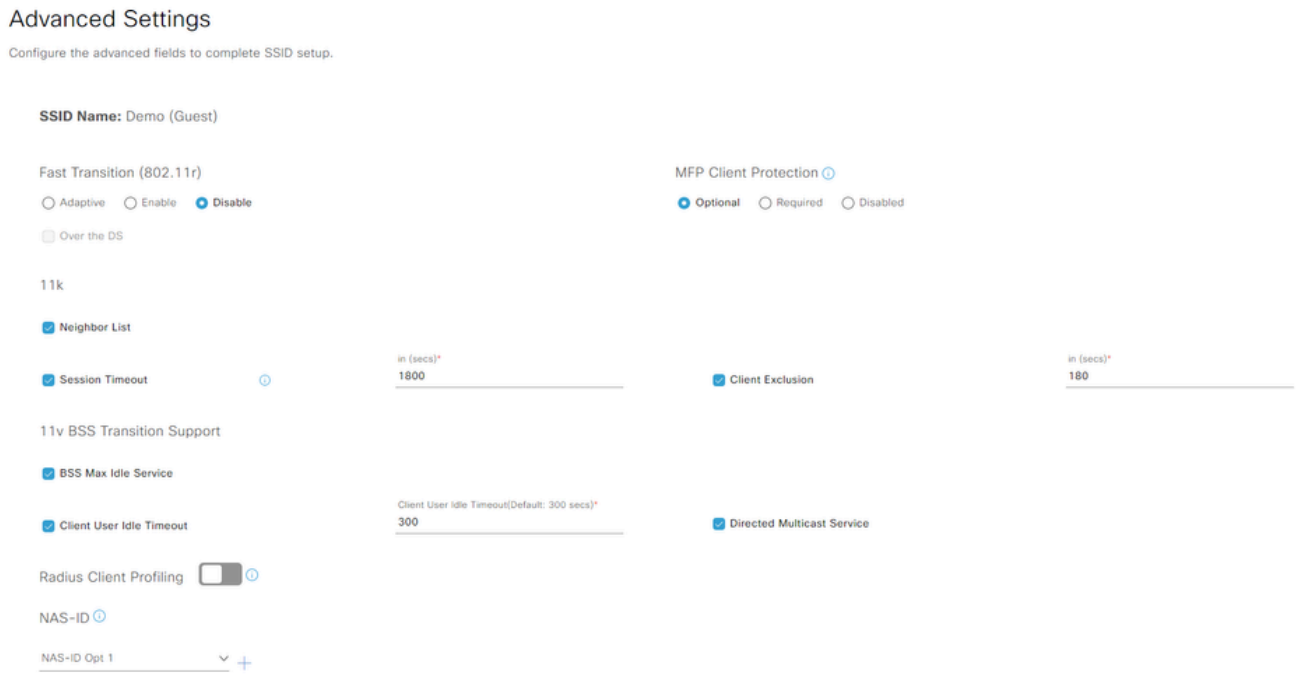
Configuración básica de SSID



Configuración de seguridad SSID

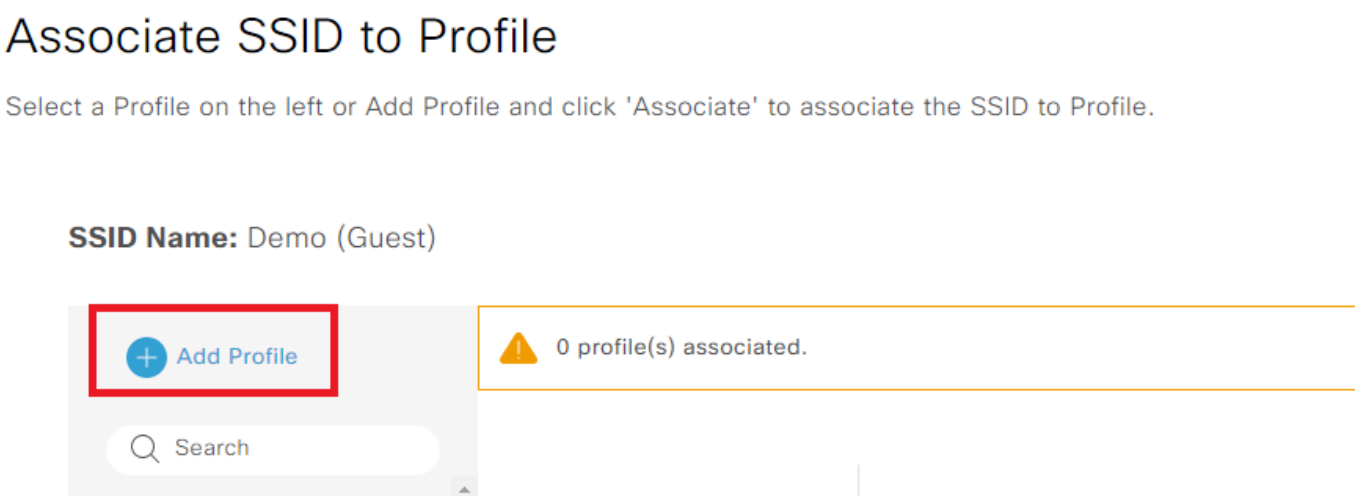
⚠ Precaución: No olvide configurar y asociar el servidor AAA para el SSID. La lista de métodos predeterminada se asigna si no se configuran servidores AAA.

Al hacer clic en Next, podrá ver la configuración avanzada del SSID:



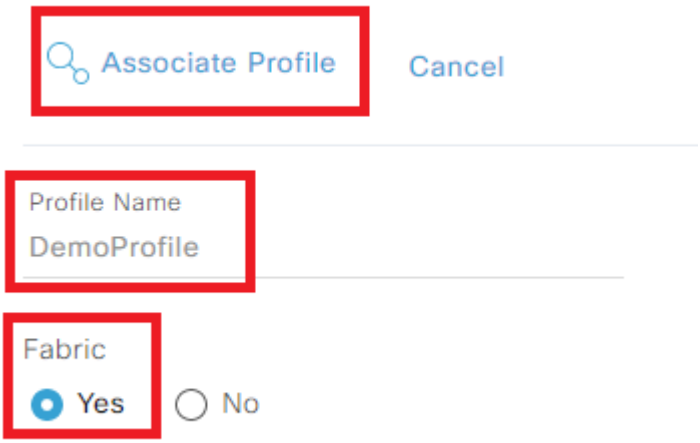
Configuración avanzada de SSID

Paso 3. Después de la creación del SSID, debe asociarlo a un perfil. Haga clic en Agregar perfil:



Agregar perfil

Paso 4. Dé un nombre al perfil, seleccione Fabric y al final haga clic en Associate Profile:



Asociar perfil

Aparecerá un resumen del SSID y el perfil que ha creado:

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)

Resumen de SSID

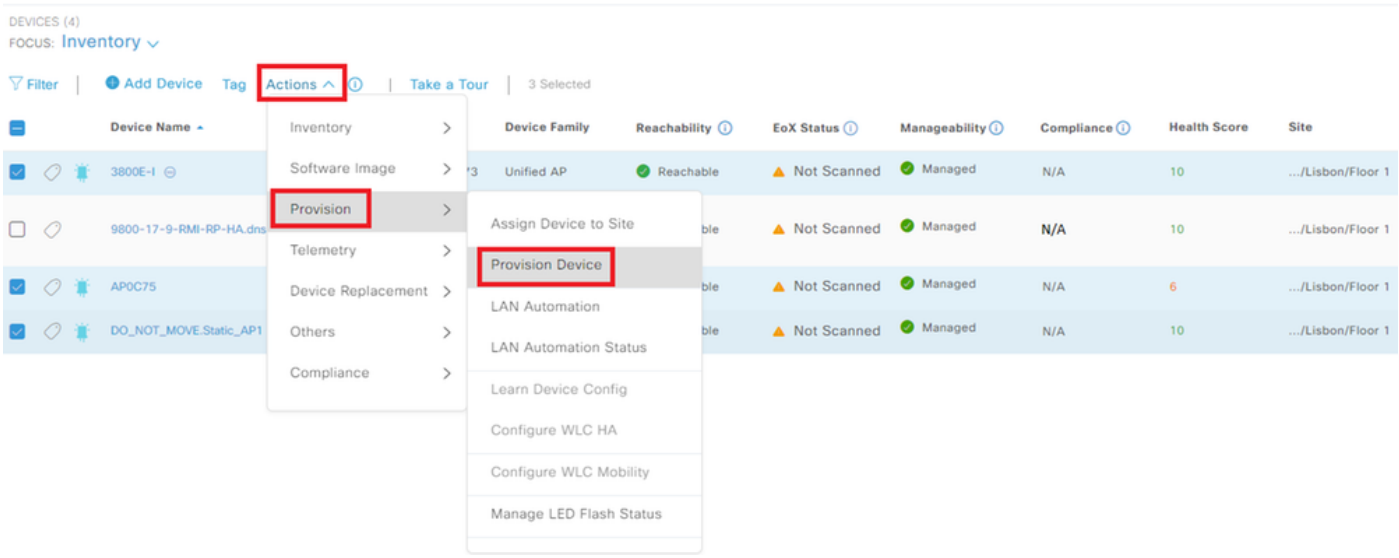
Paso 5. Configure un nuevo perfil de red:

que desee configurar. En esta demostración, se configuraron los parámetros predeterminados. Haga clic en Save (Guardar):

Agregar perfil de RF básico

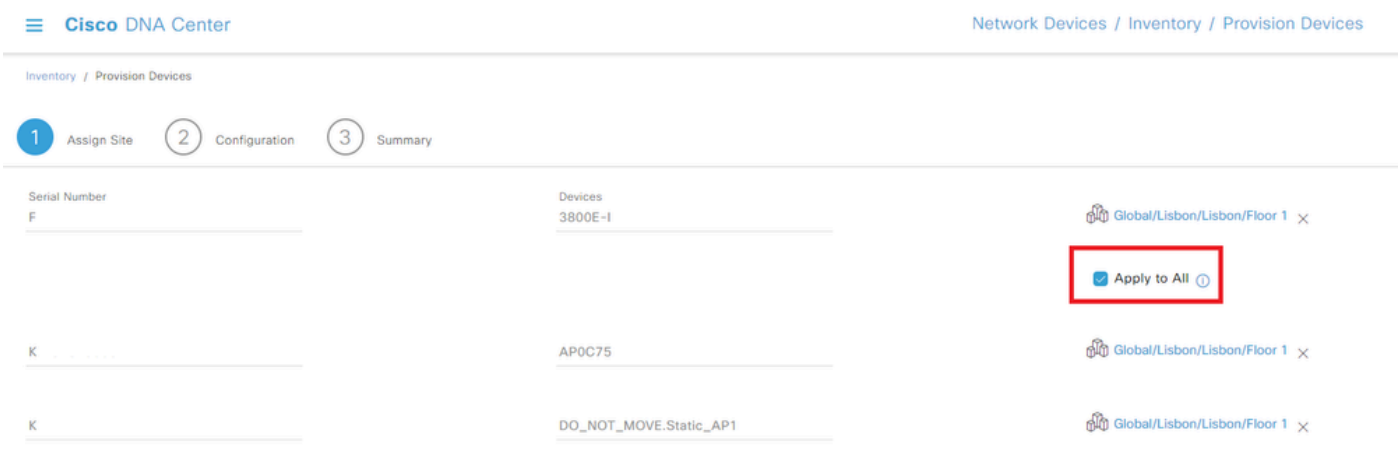
Aprovisionamiento de puntos de acceso

Paso 1. Desplácese hasta el edificio o planta. Seleccione APs y Actions > Provisioning > Provisioning Device:



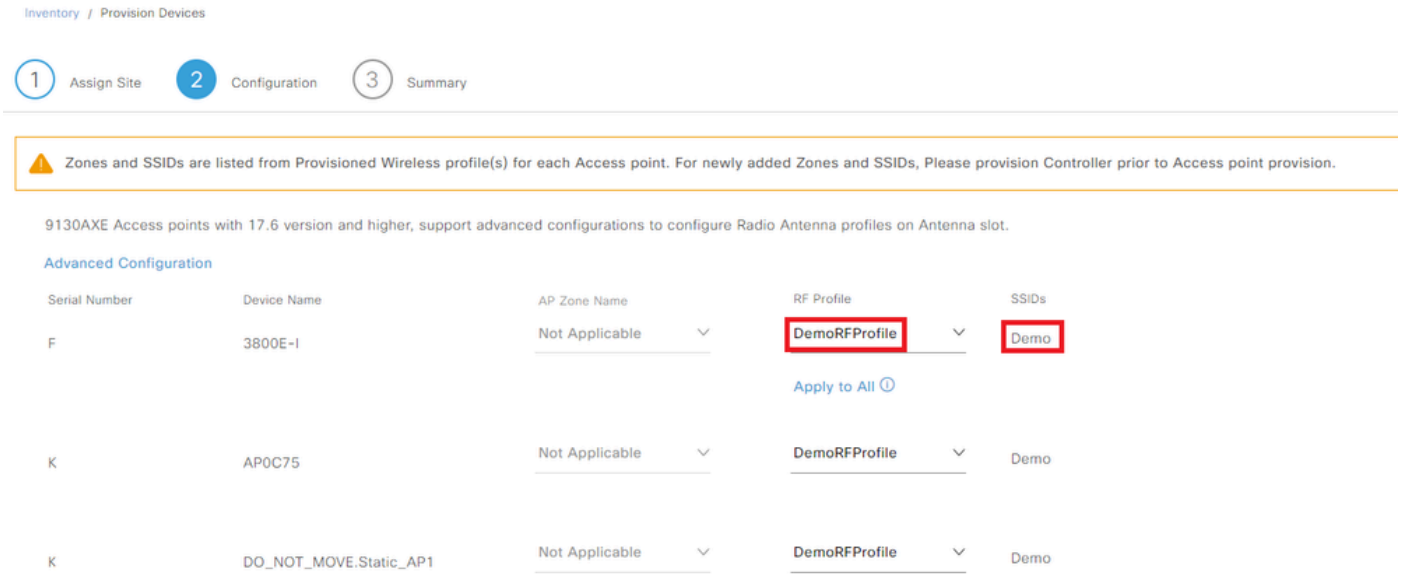
Aprovisionar puntos de acceso

Paso 2. Compruebe si el sitio asignado es correcto y seleccione Aplicar a todo:



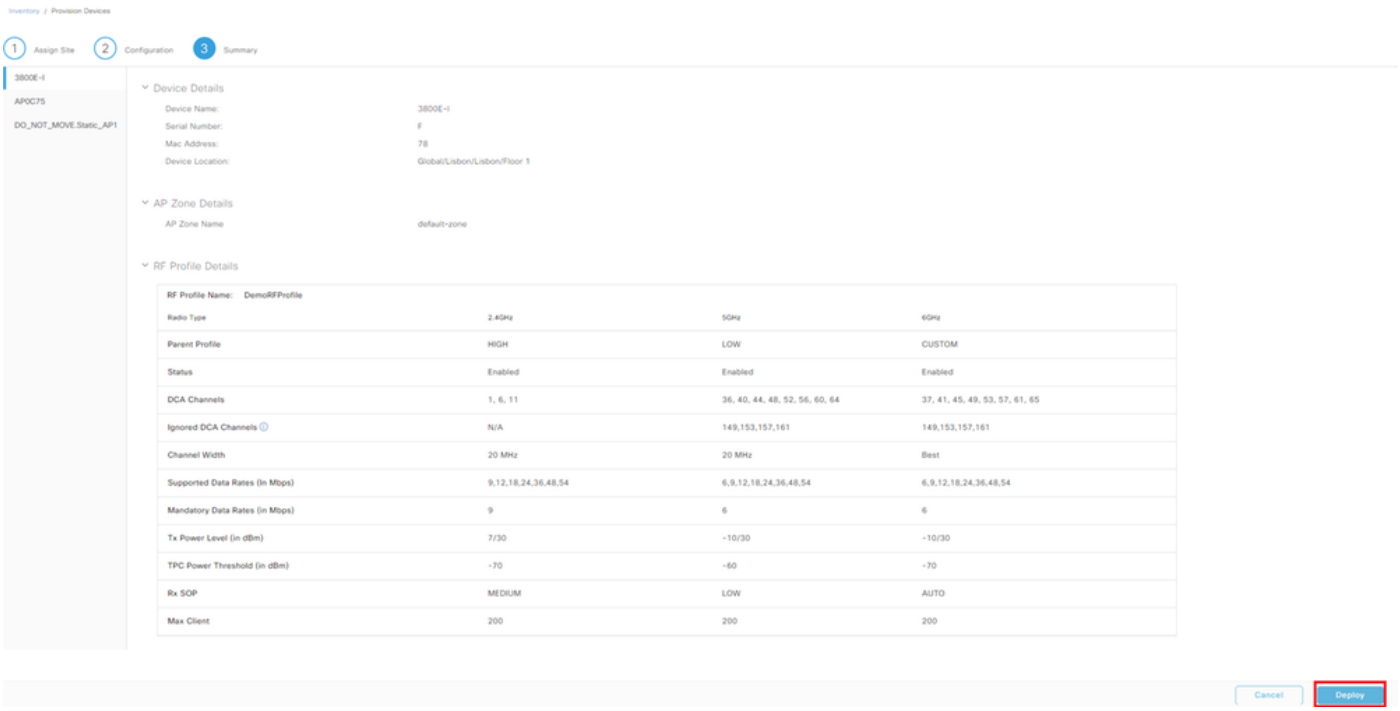
Asignar sitio a AP

Paso 3. Seleccione un perfil de RF de la lista desplegable y verifique si el SSID es el correcto:



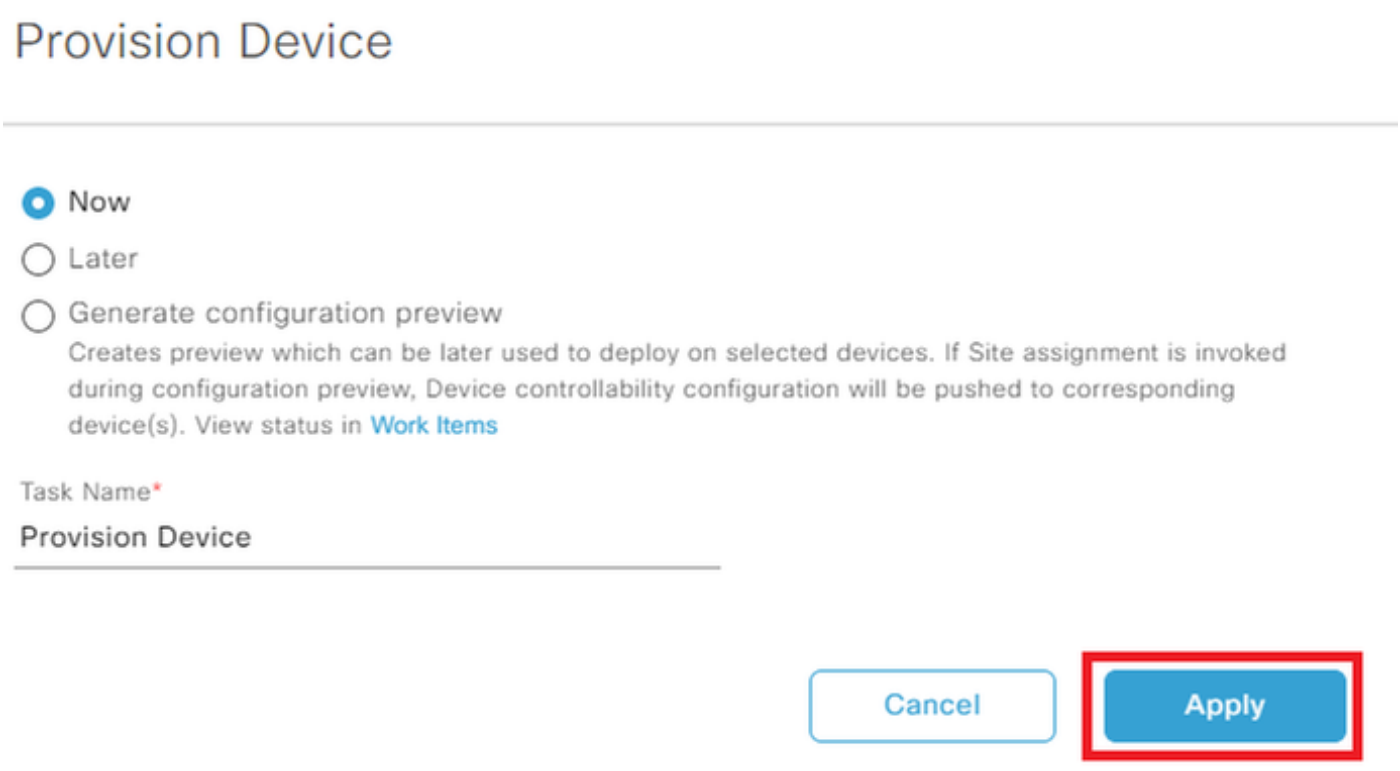
Seleccionar perfil de RF

Paso 4. Verifique la configuración en los AP. Si todo está correcto, seleccione Deploy:



Implementación de aprovisionamiento de puntos de acceso

Paso 5. El aprovisionamiento de dispositivos se puede implementar en este momento o más tarde. Al final, seleccione Apply:

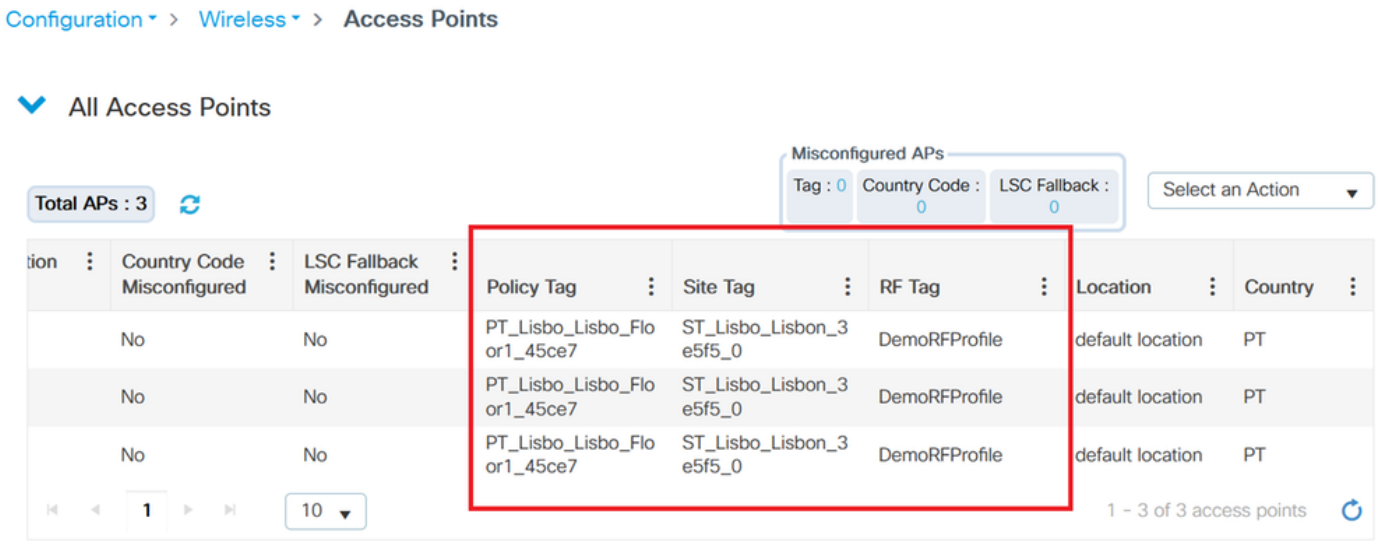


Aprovisionar puntos de acceso ahora o más tarde

⚠ Precaución: Cuando se aprovisionan los AP, que ya forman parte del suelo configurado para el perfil de RF seleccionado, se procesan y se reinician.

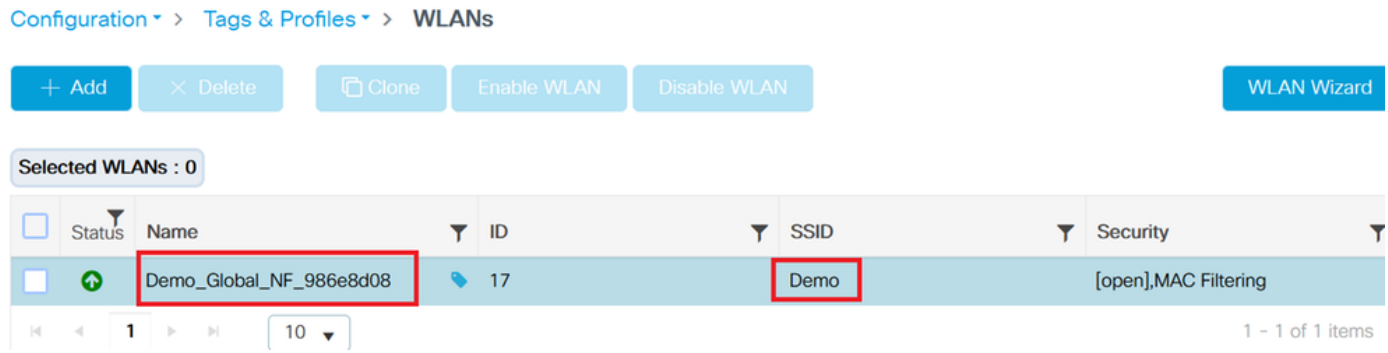
Los AP ahora están aprovisionados.

Paso 6. En el lado del WLC, navegue hasta Configuration > Wireless > Access Points. Verifique que las etiquetas AP se hayan enviado desde el ADN de Cisco:



Etiquetas en AP

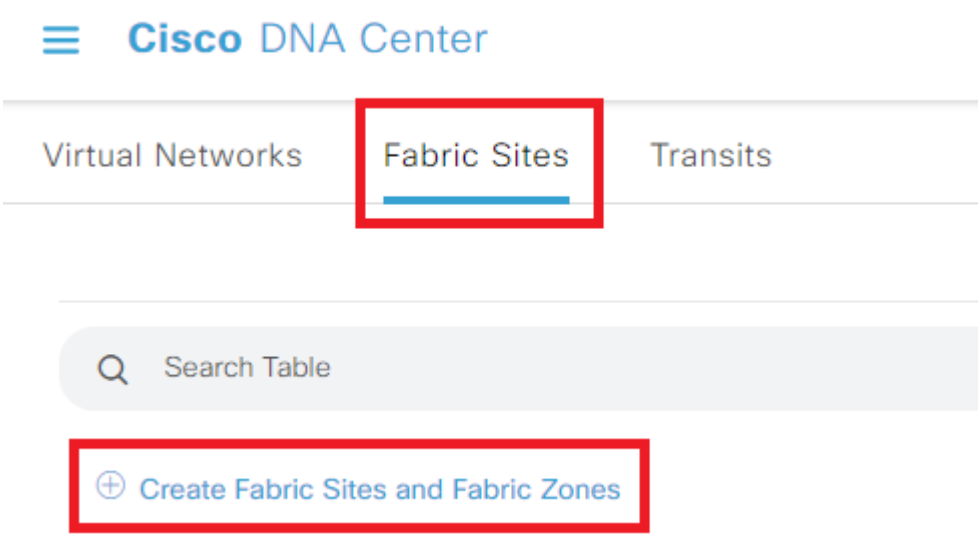
Paso 7. Navegue hasta Configuration > Tags & Profiles > WLANs y verifique que el SSID fue transferido desde Cisco DNA:



WLAN

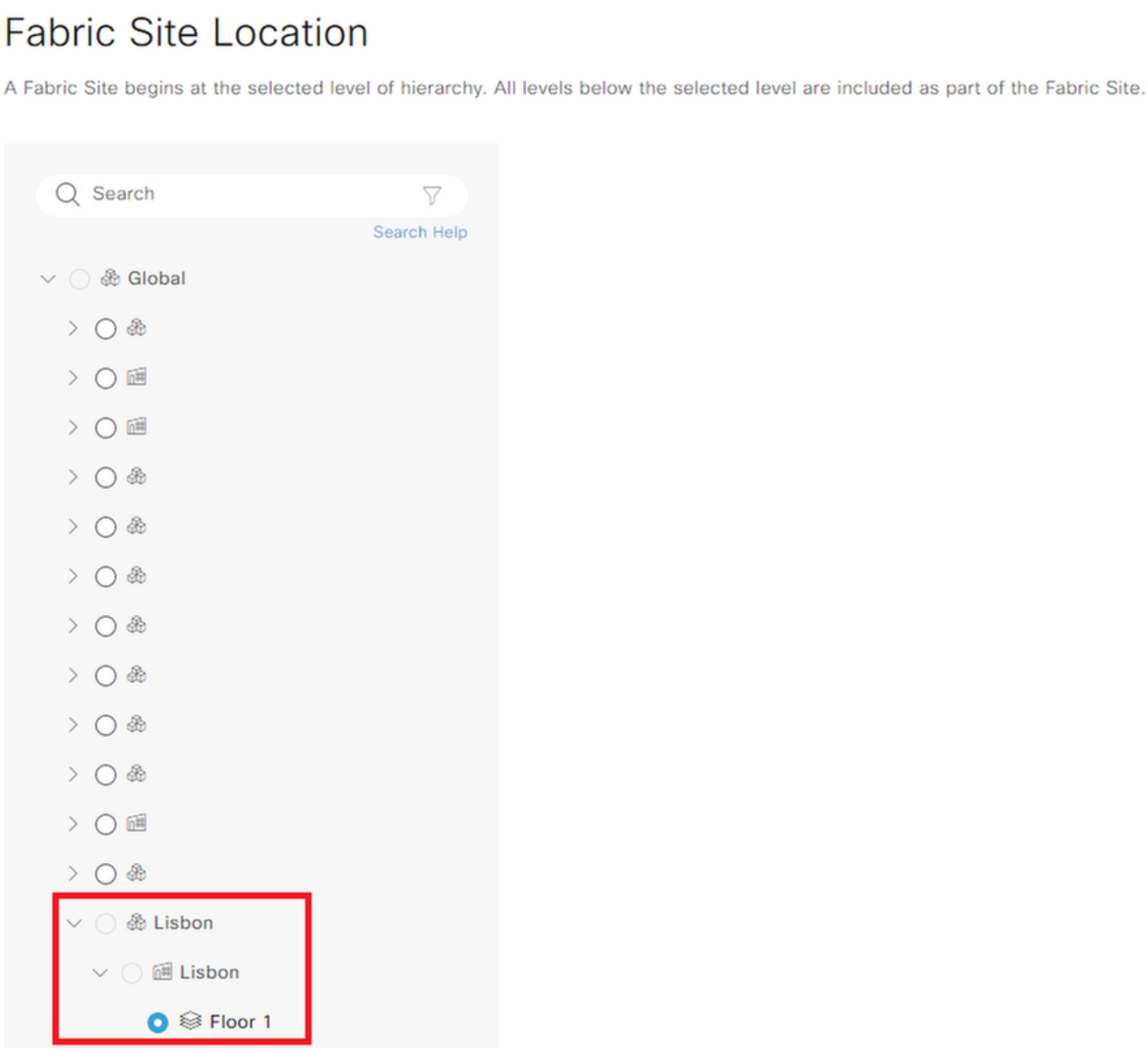
Crear sitio de fabric

Paso 1. Vaya a Aprovisionamiento > Sitios de fabric. Cree un sitio de fabric:



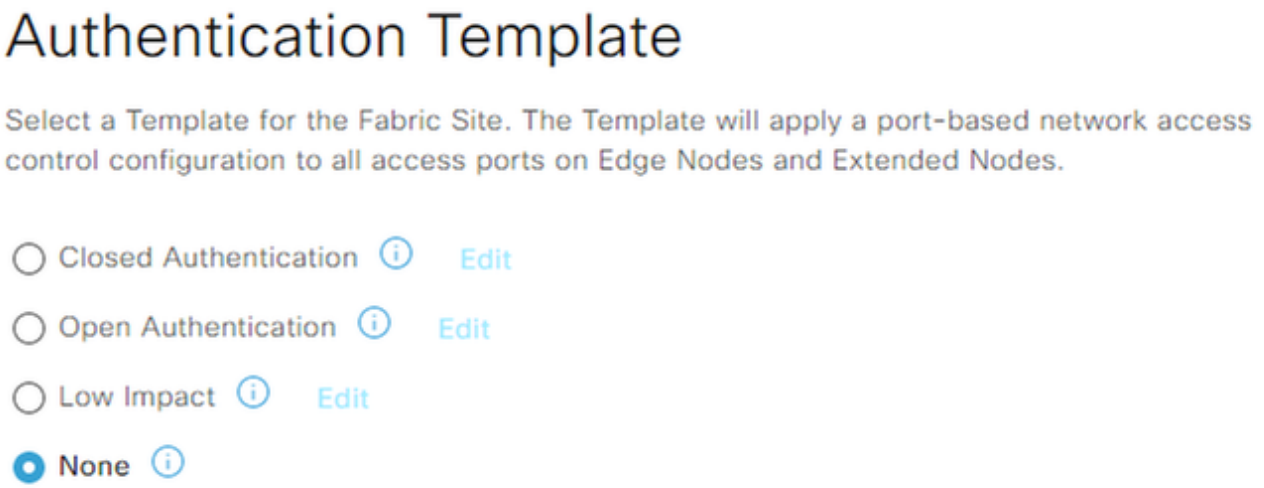
Crear sitios de fabric

Paso 2. Seleccione el edificio/planta para el sitio de fabric:



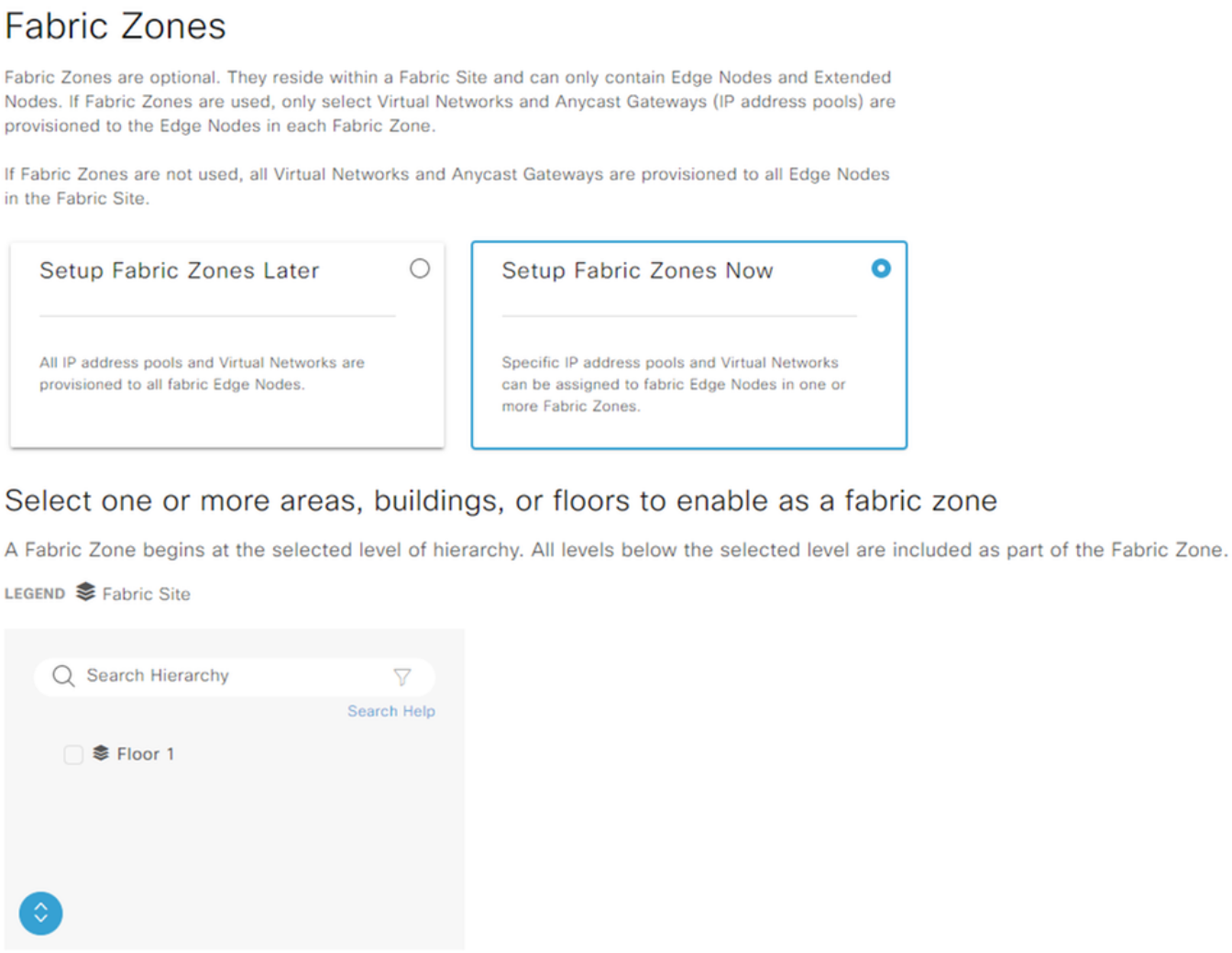
Seleccionar sitio de fabric

Paso 3. Seleccione una plantilla de autenticación. En esta demostración, se aplicó None:



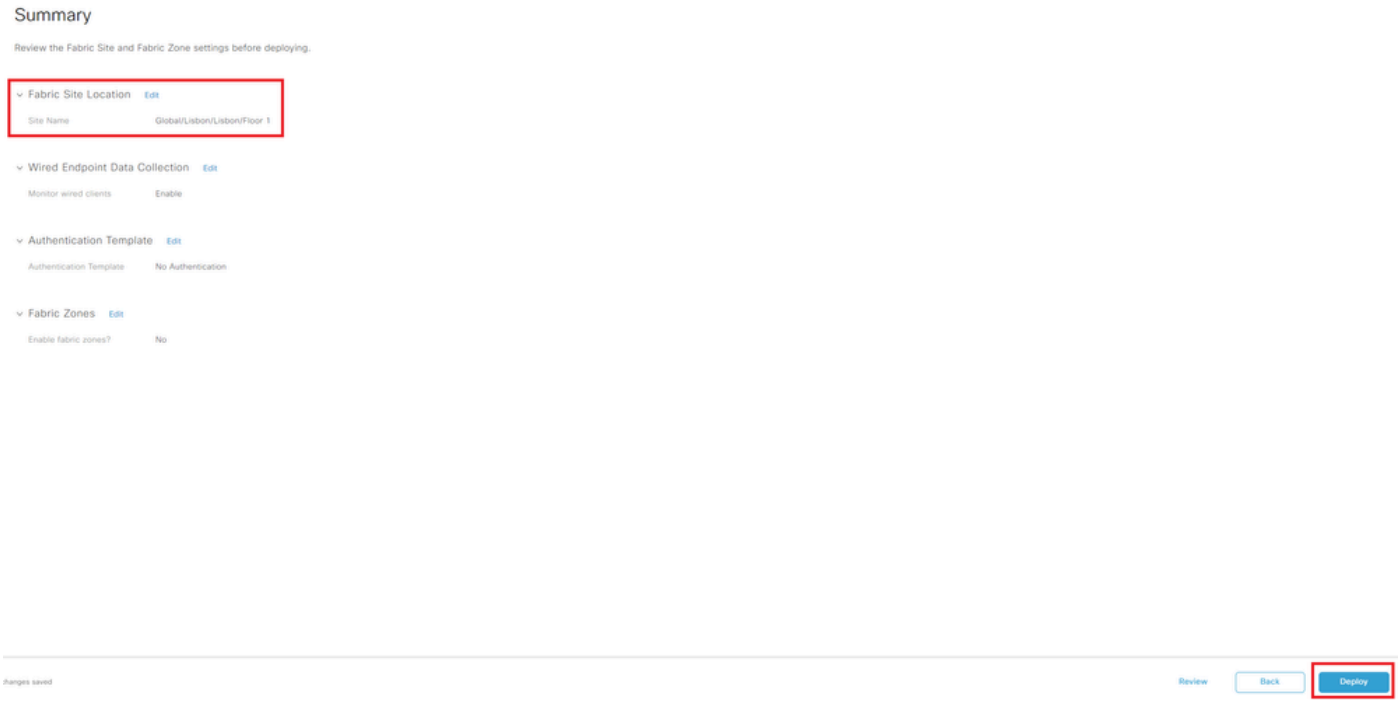
Plantilla de autenticación

Paso 3. Puede elegir si desea configurar la zona de fabric ahora o más tarde:



Configuración de zonas de fabric

Paso 4. Compruebe la configuración de la zona de fabric. Si todo está correcto, seleccione Deploy:



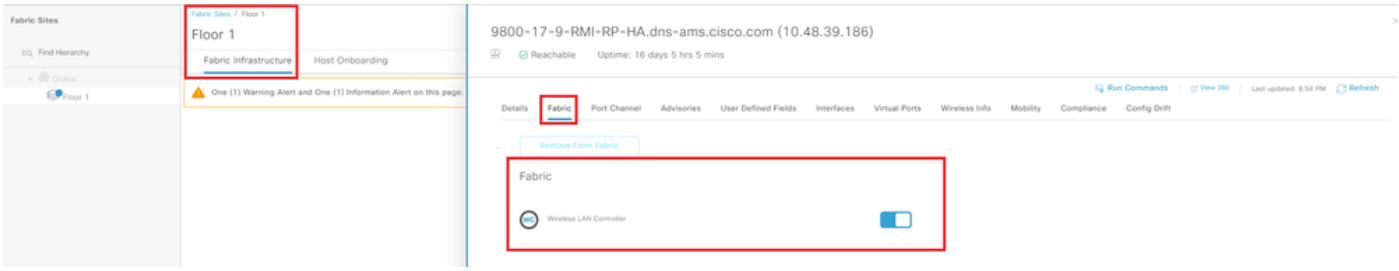
Implementar sitio de fabric

Ha creado un sitio de fabric:

Creación de sitios de fabric

Agregar WLC al fabric

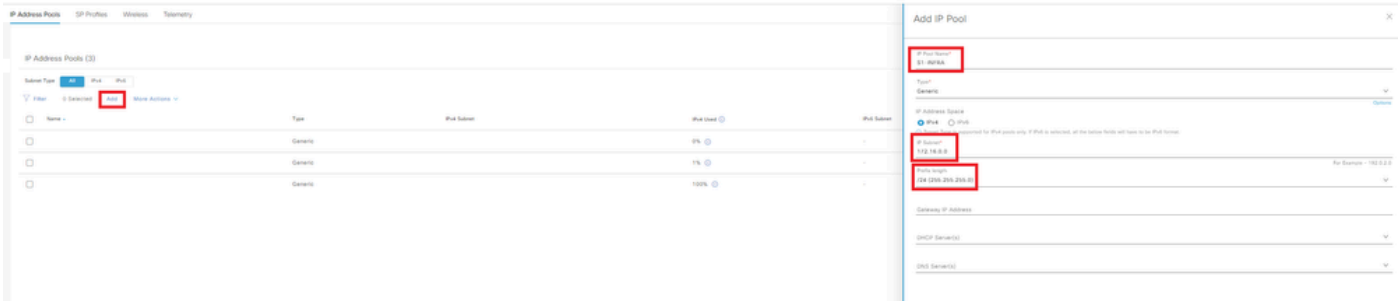
Navegue hasta Aprovisionamiento > Sitios de fabric y seleccione su sitio de fabric. Haga clic en la parte superior de su WLC y navegue a la pestaña Fabric. Habilite fabric al WLC y seleccione Add:



Agregar WLC al fabric

Incorporación de AP

Paso 1. Vaya a Diseño > Configuración de red > Pools de direcciones IP. Cree un pool de direcciones IP.



Conjunto de direcciones IP

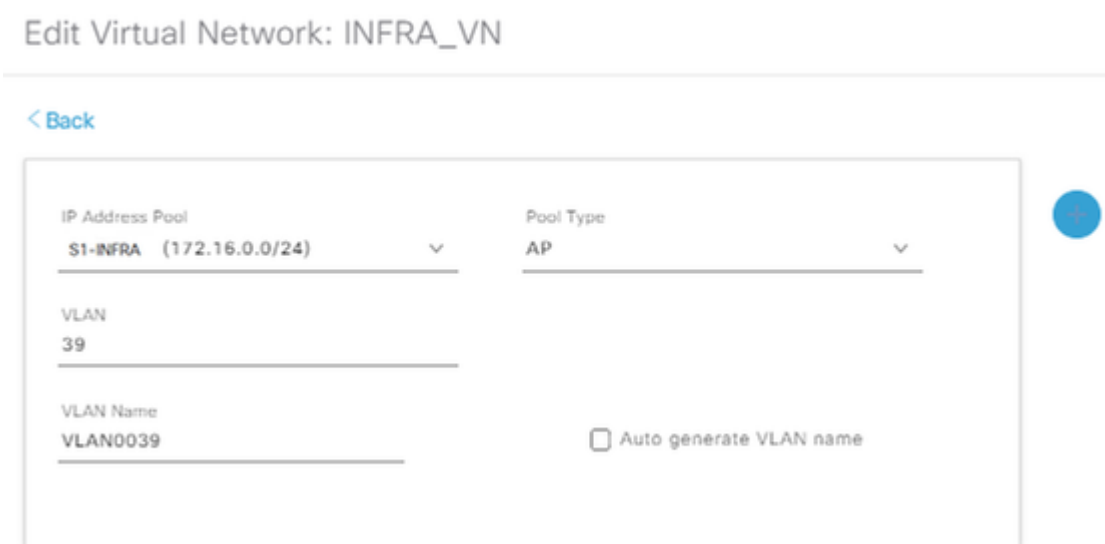
Paso 2. Navegue hasta Aprovisionamiento > Sitios de fabric y seleccione su sitio de fabric. Vaya a Host Onboarding > Virtual Networks.

INFRA_VN se introduce en los puntos de acceso fácilmente incorporados. Los AP se encuentran en la superposición del entramado, pero INFRA_VN está asignado a la tabla de ruteo global. Solo los AP y los nodos extendidos pueden pertenecer a INFRA_VN. La extensión de capa 2 se habilita automáticamente y activa el servicio LISP de capa 2.

Seleccione INFRA_VN > Agregar:

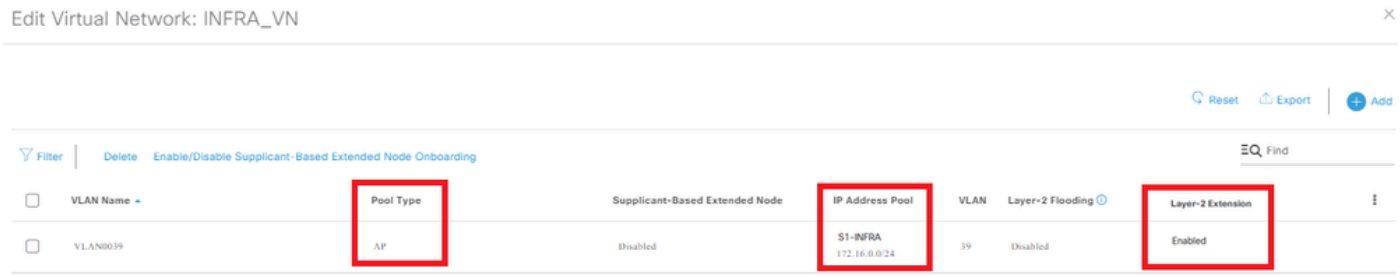
Editar red virtual

Paso 3. Agregue un Pool de Direcciones IP con el Tipo de Pool como AP:



Editar red virtual S1-INFRA

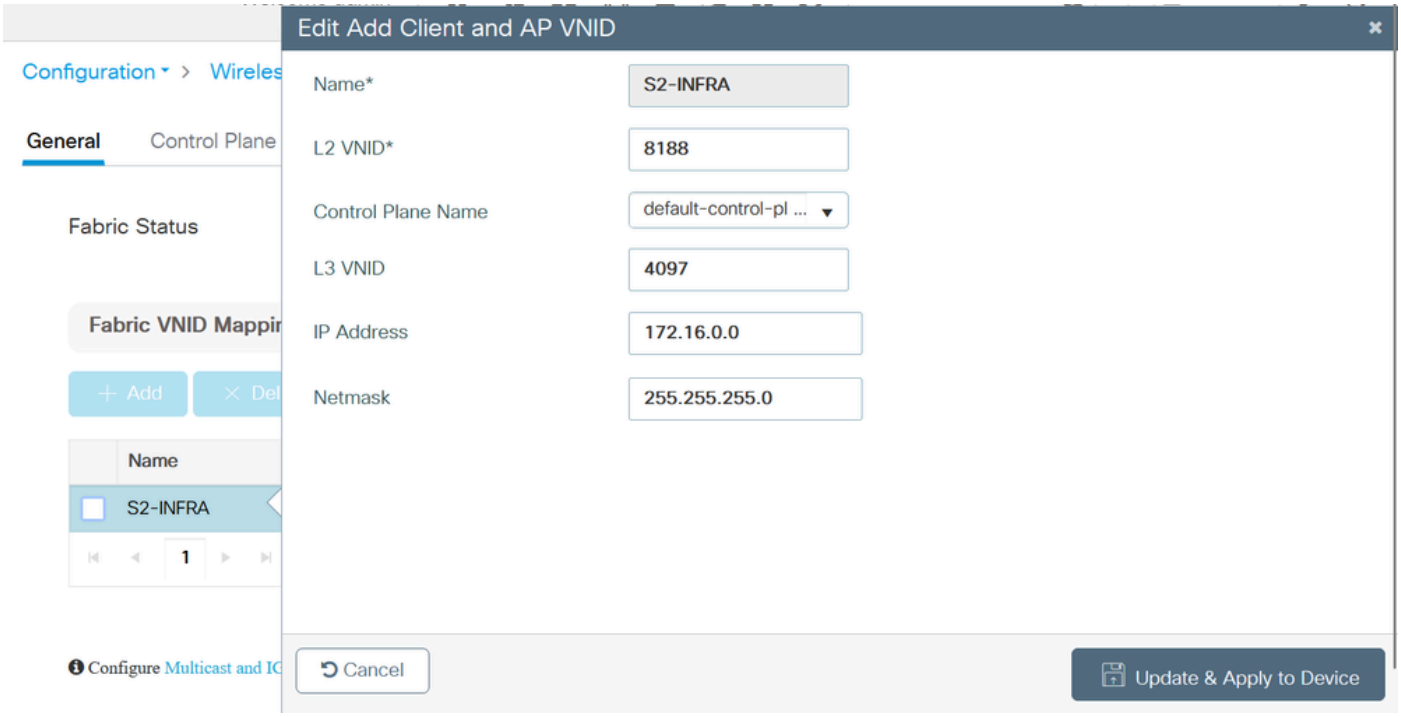
Paso 4. Compruebe si la extensión de capa 2 está habilitada.



Editar red virtual

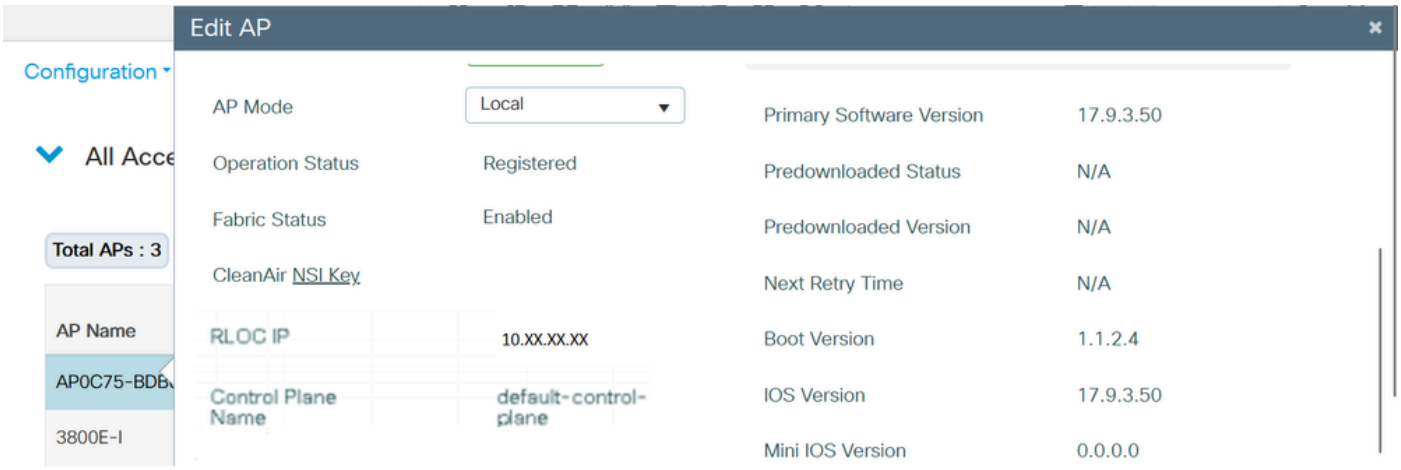
Con Pool Type = AP y Layer-2 extension a ON, Cisco DNA se conecta al WLC y configura la interfaz de Fabric para la asignación VN_ID para la subred de AP para VN_IDs L2 y L3.

Paso 5. En el lado de la GUI del WLC, navegue hasta Configuration > Wireless > Fabric > General. Agregue un nuevo cliente y AP VN_ID:



Agregar nuevo cliente y AP VN_ID

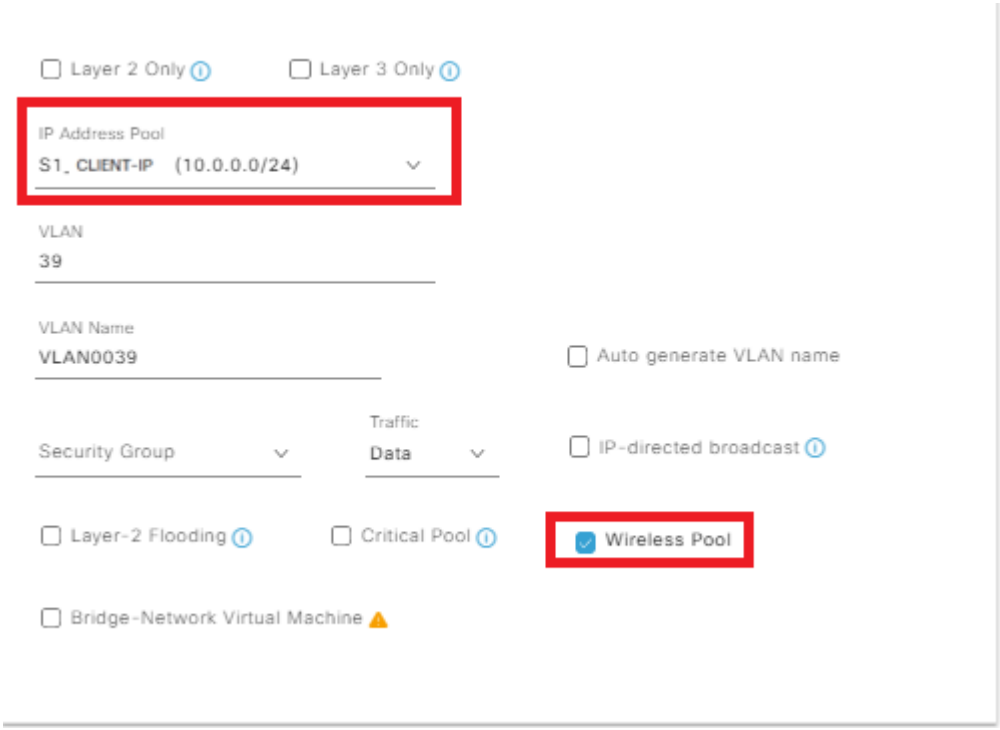
Paso 6. Navegue hasta Configuración > Inalámbrico > Puntos de acceso. Seleccione un AP de la lista. Verifique que el estado del fabric esté habilitado, la dirección IP del plano de control y el nombre del plano de control:



Verificar el estado del fabric AP

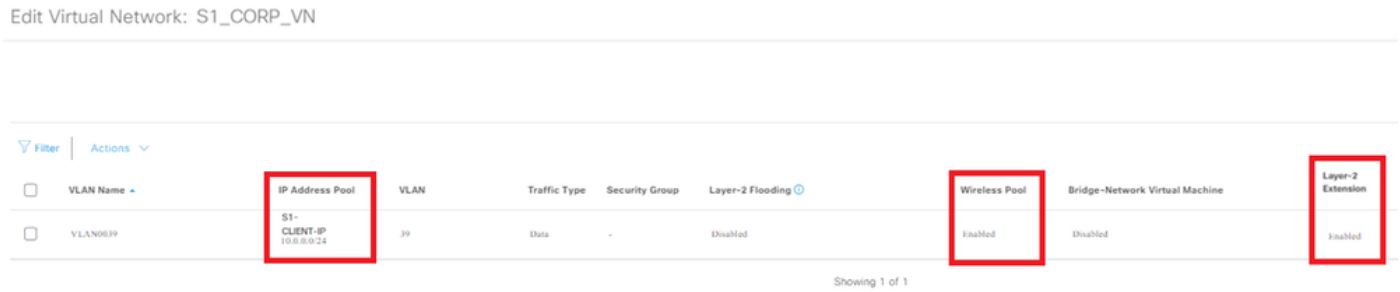
Cliente incorporado

Paso 1. Agregue el pool a la red virtual y verifique que la opción Layer-2 Extension esté ON para habilitar el LISP de capa 2 y la extensión de subred de capa 2 en el pool/subred del cliente. En Cisco DNA 1.3.x, no se puede inhabilitar.



Agregar conjunto de direcciones IP

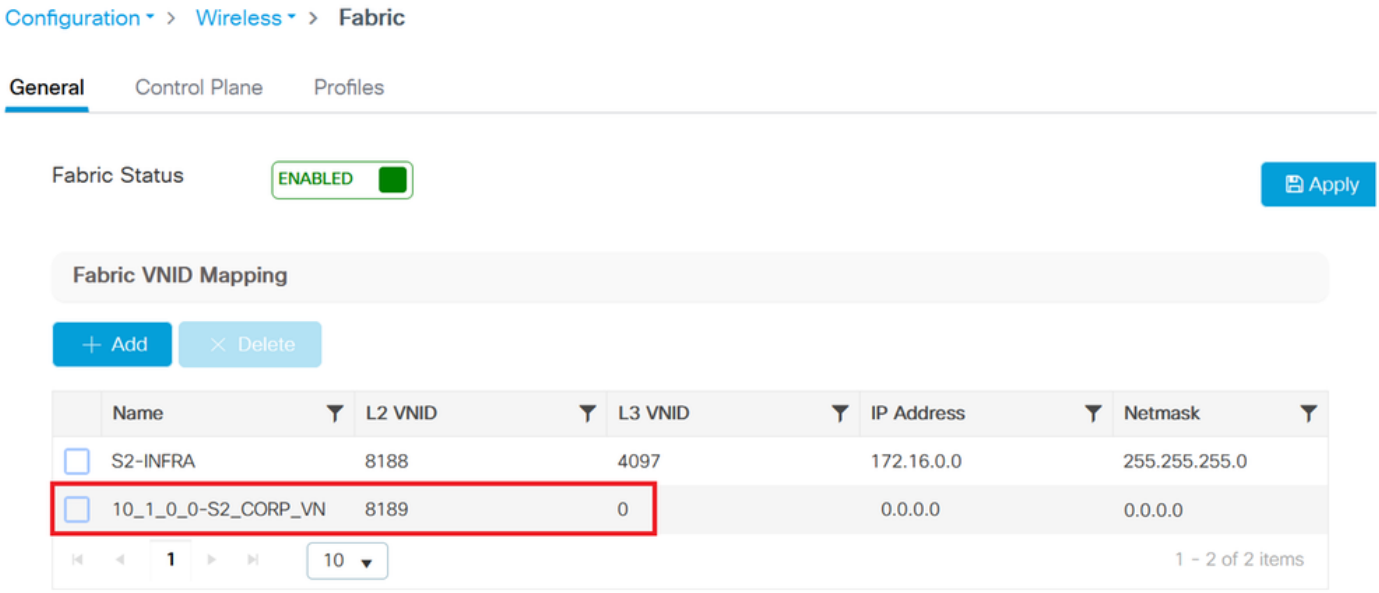
Paso 2. Verifique si la extensión de capa 2 y el conjunto inalámbrico están habilitados.



Editar red virtual

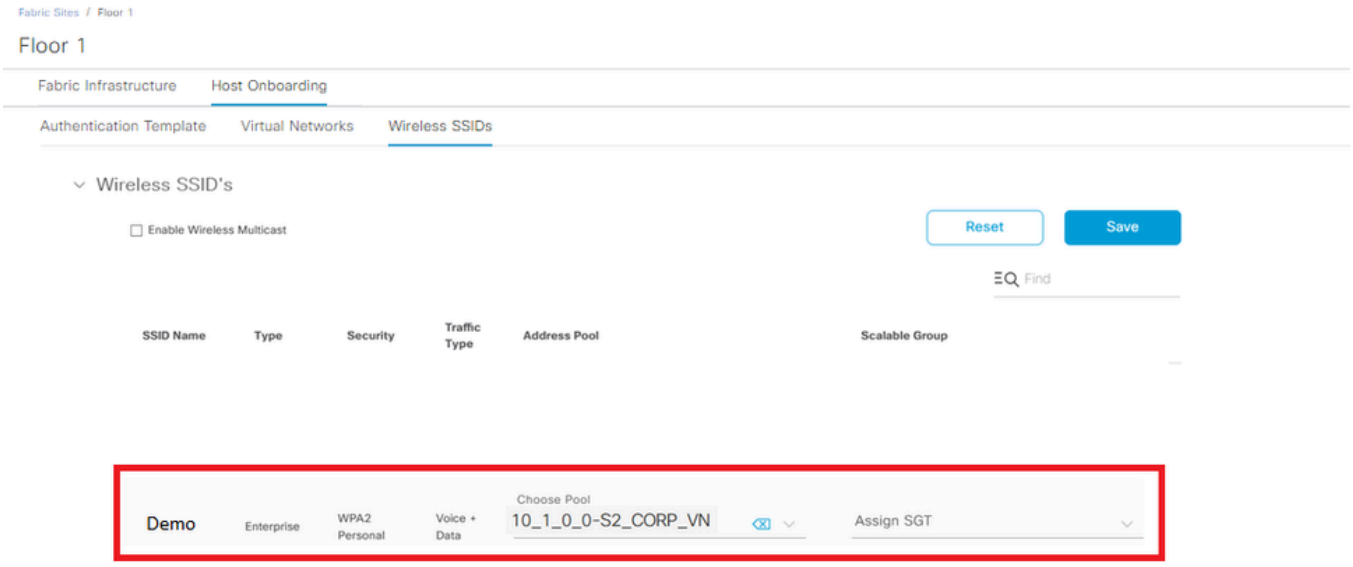
Paso 3. En el lado de la GUI del WLC, navegue hasta Configuration > Wireless > Fabric > General. Agregue un nuevo cliente y AP VN_ID.

Cuando el conjunto se asigna a la red virtual, la interfaz de fabric correspondiente a la asignación de VNID se envía al controlador. Todos ellos son VNID L2.



Agregar nuevo cliente y AP VN_ID

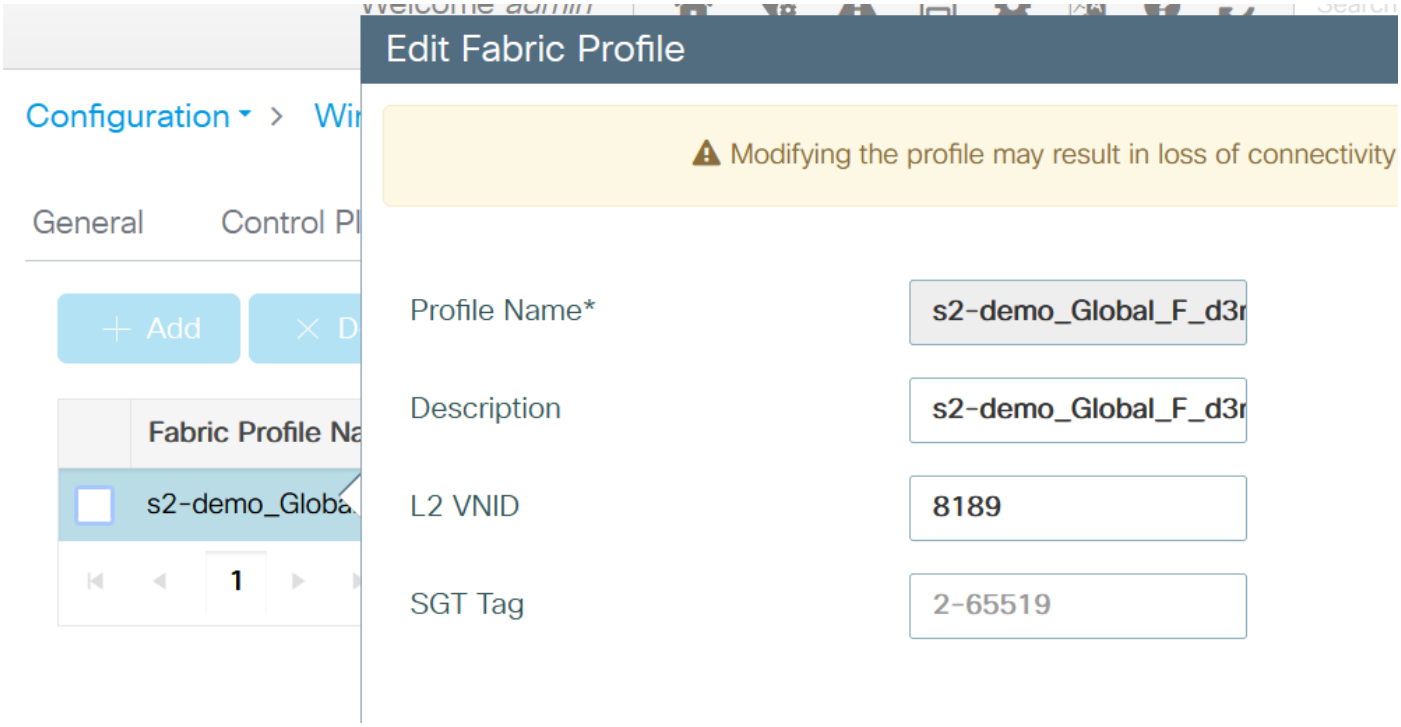
Paso 4. Los SSID se asignan al conjunto en las redes virtuales respectivas:



SSID asignados

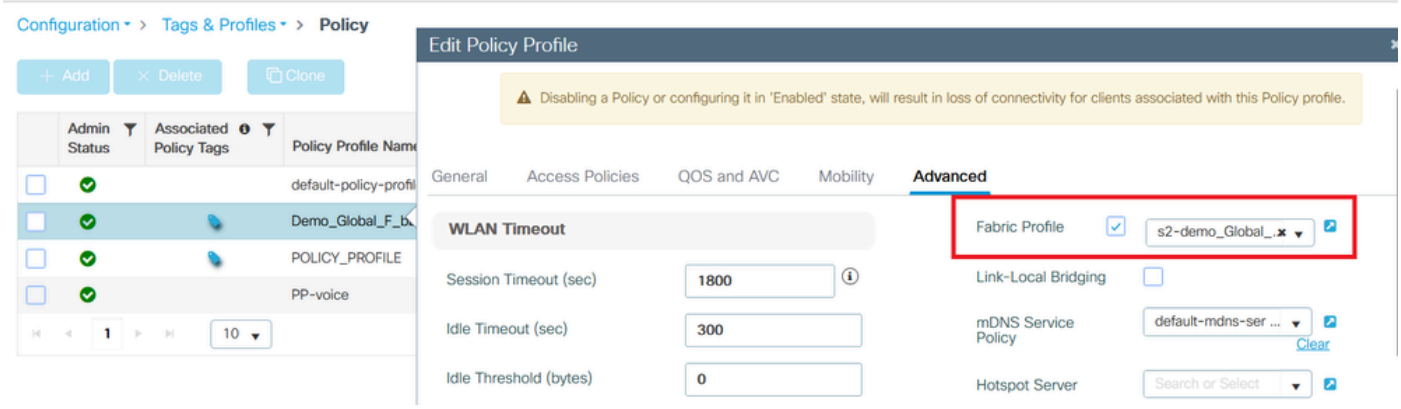
Paso 5. Se agrega un perfil de fabric con el VNID de capa 2 al grupo seleccionado y el perfil de política se asigna al perfil de fabric, que se habilita para el fabric.

En el lado de la GUI del WLC, navegue hasta Configuration > Wireless > Fabric > Profiles.



Perfil de fabric

Paso 6. Navegue hasta Configuración > Etiquetas y perfiles > Política. Verifique el perfil de fabric asignado al perfil de política:



Perfil de fabric configurado en la política

Verificación

Verifique la configuración del fabric en el WLC y el DNA de Cisco

En la CLI del WLC:

WLC1# show tech

WLC1# show tech wireless

Configuración del plano de control:

```
router lisp
 locator-table default
 locator-set WLC
  172.16.201.202
  exit-locator-set
  !
 map-server session passive-open WLC
 site_uci
  description map-server configured from Cisco DNA-Center
  authentication-key 7 <Key>
```

CB1-S1#sh lisp session

Sesiones por defecto de VRF, total: 9, establecido: 5

Estado de par arriba/abajo dentro/fuera

172.16.201.202:4342 Hasta 3d07h 14/14

Configuración de WLC:

tejido inalámbrico

wireless fabric control-plane default-control-plane

ip address 172.16.2.2 key 0 47aa5a

WLC1# show fabric map-server summary

Estado de la conexión MS-IP

172.16.1.2 UP

WLC1# show wireless fabric summary

Estado del fabric: Habilitado

Plano de control:

Name IP-address Key Status

---

default-control-plane 172.16.2.2 47aa5a Up

En la GUI del WLC navegue hasta Configuration > Wireless > Fabric y verifique si el estado del fabric está habilitado.

Vaya a Configuration > Wireless > Access Points . Seleccione un AP de la lista. Compruebe que el estado del fabric es Enabled (Activado).

En Cisco DNA, navegue hasta Aprovisionar > Sitios de fabric y verifique si tiene un sitio de fabric. En ese sitio de entramado, navegue hasta Fabric Infrastructure > Fabric y verifique si el WLC está habilitado como entramado.

Troubleshoot

El cliente no obtiene la dirección IP

Paso 1. Verifique si el SSID es fabric. En la GUI del WLC, navegue hasta Configuration > Tags & Profiles > Policy. Seleccione la política y desplácese hasta Avanzadas. Verifique si el perfil de fabric está habilitado.

Paso 2. Compruebe si el cliente está atascado en el estado de aprendizaje de IP. En la GUI del WLC, navegue hasta Monitoring > Wireless > Clients. Verifique el estado del cliente.

Paso 3. Verifique si la política es DHCP requerido.

Paso 4. Si el tráfico se conmuta localmente entre AP - nodo de borde, recopile los registros de AP (seguimiento del cliente) para la conexión del cliente. Verifique si se reenvía la detección DHCP. Si no llega ninguna oferta de DHCP, hay un problema en el nodo de borde. Si el DHCP no se reenvía, entonces algo está mal en el AP.

Paso 5. Puede recopilar un EPC en el puerto del nodo de borde para ver los paquetes de detección DHCP. Si no ve los paquetes de detección DHCP, el problema está en el AP.

SSID no se ha transmitido

Paso 1. Verifique si las radios AP están inactivas.

Paso 2. Verifique si la WLAN está en estado encendido y difunda el SSID habilitado.

Paso 3. Verifique la configuración del AP si el AP está habilitado para el entramado. Navegue hasta Configuration > Wireless > Access Points, seleccione one AP y en la pestaña General puede ver Fabric Status Enabled y la información de RLOC.

Paso 4. Vaya a Configuración > Inalámbrico > Fabric > Plano de control. Verifique si el plano de control está configurado (con la dirección IP).

Paso 5. Navegue hasta Configuración > Etiquetas y perfiles > Política. Seleccione la política y desplácese hasta Avanzadas. Verifique si el perfil de fabric está habilitado.

Paso 6. Navegue hasta Cisco DNA y vuelva a hacer los pasos en Crear SSID y Aprovisionar WLC. El DNA de Cisco debe empujar el SSID al WLC otra vez.

Información Relacionada

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).