Implemente o acesso definido por software para redes sem fio com DNA

Contents

Introdução

Este documento descreve como implementar o SDA para tecnologia sem fio relacionada à WLC ativada para estrutura e acessar o LAP no Cisco DNA.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- 9800 Configuração de Wireless LAN Controllers (WLC)
- Pontos de Acesso Lightweight (LAPs)
- DNA da Cisco

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- 9800-CL WLC Cisco IOS® XE, versão 17.9.3
- Pontos de acesso da Cisco: 9130AX, 3802E, 1832I
- Cisco DNA versão 2.3.3.7

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

SD-Access

O acesso definido por software estabelece e aplica automaticamente políticas de segurança em toda a rede, com regras dinâmicas e segmentação automatizada, além de permitir que o usuário final controle e configure como os usuários se conectam à rede. O acesso SD estabelece um nível inicial de confiança com cada endpoint conectado e monitora continuamente esse nível para verificar novamente o nível de confiança. Se um endpoint não se comporta normalmente ou um tratamento é detectado, o usuário final pode contê-lo imediatamente e agir, antes que a violação ocorra, reduzir o risco comercial e proteger seus recursos. Solução totalmente integrada e fácil de implantar e configurar em redes novas e implantadas.

SD-Access é uma tecnologia da Cisco que é uma evolução da rede de campus tradicional que oferece rede baseada em intenção (IBN) e controle de política central com o uso de componentes de rede definida por software (SDN).

Três pilares do acesso SD centrados na rede:

1. Uma estrutura de rede: É uma abstração da própria rede que suporta sobreposições programáveis e virtualização. A estrutura de rede suporta acesso com e sem fio, permite hospedar várias redes lógicas que são segmentadas uma da outra e são definidas de acordo com o objetivo comercial.
2. Orquestração O Cisco DNA é o mecanismo orquestrador do SDA. O Cisco DNA funciona

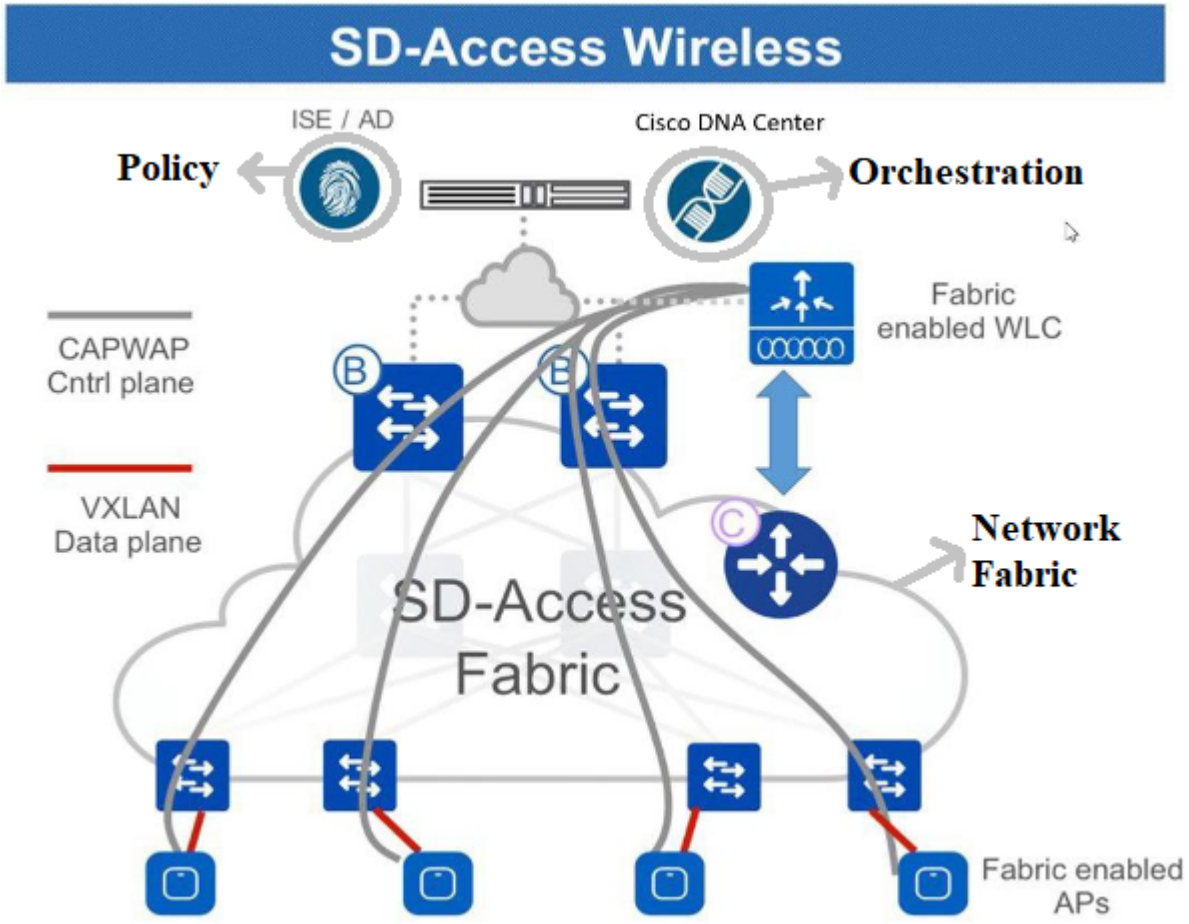
como um controlador de SDN. Ele implementa políticas e alterações de configuração na malha. Além disso, incorpora uma ferramenta que oferece suporte ao projeto de rede e às operações de telemetria de rede em tempo real e à análise de desempenho por meio do DNA Assurance. A função do Cisco DNA é orquestrar a estrutura de rede para fornecer alterações de política e intenção de rede para segurança, qualidade de serviço (QoS) e microssegmentação.

3. Política: O Identity Services Engine (ISE) é a ferramenta que define a política de rede. O ISE organiza como os dispositivos e os nós são segmentados em redes virtuais. O ISE também define tags de grupo escaláveis (SGTs) que são usadas pelos dispositivos de acesso para segmentar o tráfego do usuário à medida que ele entra na malha. Os SGRs são responsáveis por aplicar a política de microssegmentação definida pelo ISE.

O SDA foi desenvolvido com base na orquestração centralizada. As combinações do Cisco DNA como o mecanismo de orquestração programável, do ISE como o mecanismo de política e de uma nova geração de switches programáveis fazem dele um sistema de estrutura muito mais flexível e gerenciável do que qualquer outra coisa que tenha vindo antes.

Note: Este documento trata especificamente de acesso SD sem fio.

A estrutura de rede é composta destes elementos:

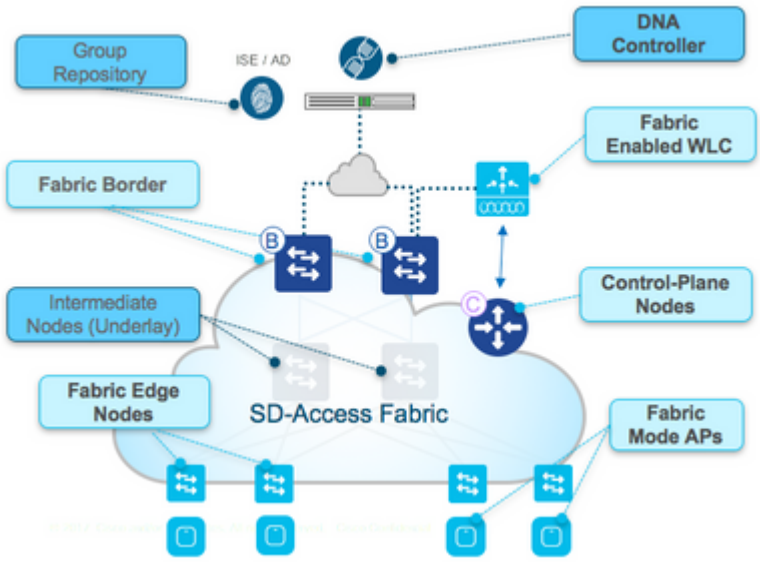


Elementos da estrutura de rede

A integração sem fio com a malha leva a várias vantagens para a rede sem fio, por exemplo: abordagem de simplificação, mobilidade com sub-redes estendidas em locais físicos; e microssegmentação com política centralizada que é consistente em ambos os domínios com e sem fio. Ele também permite que o controlador elimine o plano de dados para encaminhar tarefas enquanto continua a funcionar como o plano de controle e serviços centralizados para a rede sem fio. Assim, a escalabilidade do controlador sem fio é realmente aumentada porque não precisa mais processar o tráfego do plano de dados, semelhante ao modelo FlexConnect.

Arquitetura sem fio com acesso SD

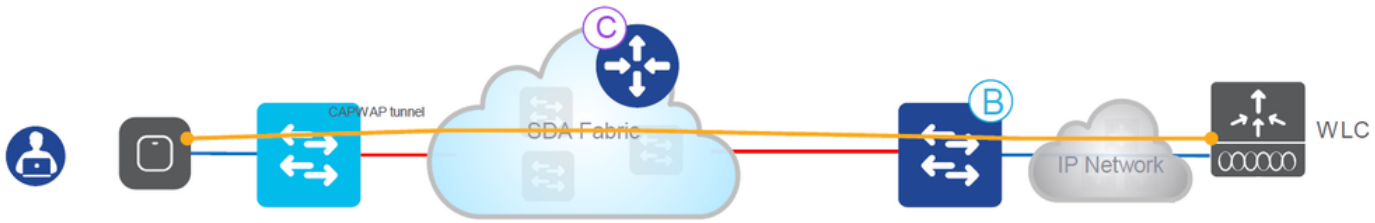
Overview



Visão geral do SDA

Há dois modelos principais de implantação sem fio compatíveis com SDA:

Um é um método over-the-top (OTT), uma implantação CAPWAP tradicional conectada sobre uma rede com fio em malha. A estrutura SDA transporta o controle CAPWAP e o tráfego do plano de dados para o controlador sem fio:

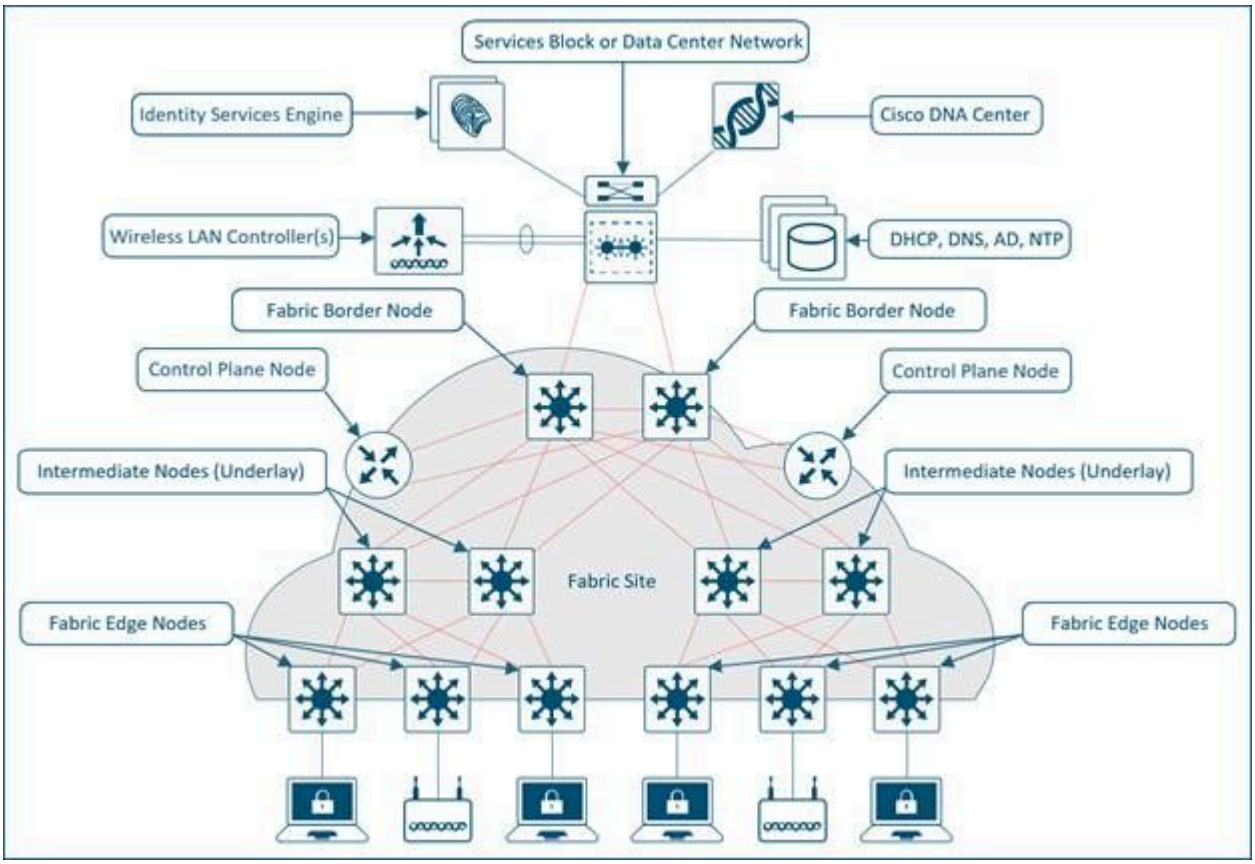


Método Over-The-Top

Nesse modelo de implantação, a malha SDA é uma rede de transporte para tráfego sem fio (um modelo frequentemente implantado em migrações). O AP funciona de forma muito semelhante ao modo Local clássico: o controle CAPWAP e os planos de dados terminam no controlador, o que significa que o controlador não participa diretamente da estrutura. Esse modelo é frequentemente

usado quando os switches com fio são migrados pela primeira vez para a estrutura SDA, mas a rede sem fio ainda não está pronta para a integração completa da sobreposição de estrutura.

Os outros modelos de implantação são o modelo SDA totalmente integrado. A rede sem fio é totalmente integrada à malha e participa de sobreposições, permitindo que diferentes WLANs façam parte de diferentes redes virtuais (VNs). A controladora sem fio gerencia apenas o plano de controle CAPWAP (para gerenciar APs) e o plano de dados CAPWAP não chega à controladora:



Modelo SDA totalmente integrado

O plano de dados sem fio é tratado de forma semelhante aos switches com fio - cada AP encapsula dados em VXLAN e os envia para um nó de borda de estrutura, onde são enviados através da estrutura para outro nó de borda. Os controladores sem fio devem ser configurados como controladores de estrutura, o que é uma modificação de sua operação normal.

Os controladores ativados por estrutura se comunicam com o plano de controle da estrutura, registram endereços MAC de cliente da camada 2 e informações do Identificador de Rede Virtual (VNI - Virtual Network Identifier) da camada 2. Os APs são responsáveis pela comunicação com terminais sem fio e auxiliam o plano de dados VXLAN pelo tráfego de encapsulamento e desencapsulamento.

Funções e terminologia do SDA

A estrutura de rede é composta destes elementos:

- Nó do plano de controle: Este é o sistema de mapeamento de local (banco de dados de host) que faz parte do plano de controle do Location Separator Protocol (LISP), que

gerencia a identidade do ponto final (EID) para as relações de local (ou relações de dispositivo). O plano de controle pode ser um roteador dedicado que forneceu funções do plano de controle ou pode coexistir com outros elementos de rede de estrutura.

- Nós de borda de malha: Normalmente, um roteador que funciona na fronteira entre redes externas e a estrutura SDA, que fornece serviços de roteamento para as redes virtuais na estrutura. Conecta redes externas de Camada 3 à estrutura SDA.
- Nós de borda de malha: Dispositivo dentro da malha que conecta dispositivos que não são da malha, como switches, APs e roteadores à malha SDA. Esses são os nós que criam os túneis de sobreposições virtuais e VNs com Virtual eXtensible LAN (VXLAN) e impõem os SGTs no tráfego vinculado à estrutura. As redes em ambos os lados da borda da estrutura estão dentro da rede SDA. Eles conectam endpoints com fio à malha SD-Access.
- Nós intermediários: Esses nós estão dentro do núcleo da estrutura do SDA e se conectam a nós de borda ou borda. Os nós intermediários simplesmente encaminham o tráfego SDA como pacotes IP, sem saber que há várias redes virtuais envolvidas.
- WLC de malha: Controlador sem fio habilitado para matriz e que participa do plano de controle SDA, mas não processa o plano de dados CAPWAP.
- APs do modo de estrutura: Pontos de acesso que são ativados para matriz. O tráfego sem fio é encapsulado por VXLAN no AP, o que permite que ele seja enviado para a estrutura através de um nó de borda.
- Cisco DNA (DNAC): O controlador de SDN empresarial para a rede de sobreposição de estrutura de Acesso Definido por Software (SDA) e é responsável por tarefas de automação e garantia. Ele também pode ser utilizado para algumas tarefas de automação e relacionadas para os dispositivos de rede que formam a base (não relacionada ao SDA).
- ISE: O Identity Services Engine (ISE) é uma plataforma de política avançada que pode atender a uma variedade de funções, não menos das quais é a do servidor de Autenticação, Autorização e Contabilidade (AAA). O ISE normalmente interage com o Ative Diretory (AD), mas os usuários podem ser configurados localmente, bem como no próprio ISE para implantações menores.

Note: O plano de controle é uma parte da infraestrutura crítica da arquitetura SDA, portanto, é recomendável que seja implantado de forma resiliente.

Redes de Sobreposição e de Sobreposição

A arquitetura SDA utiliza tecnologia de estrutura que suporta redes virtuais programáveis (redes de sobreposição) que são executadas em uma rede física (uma rede de base).

Uma estrutura é uma sobreposição.

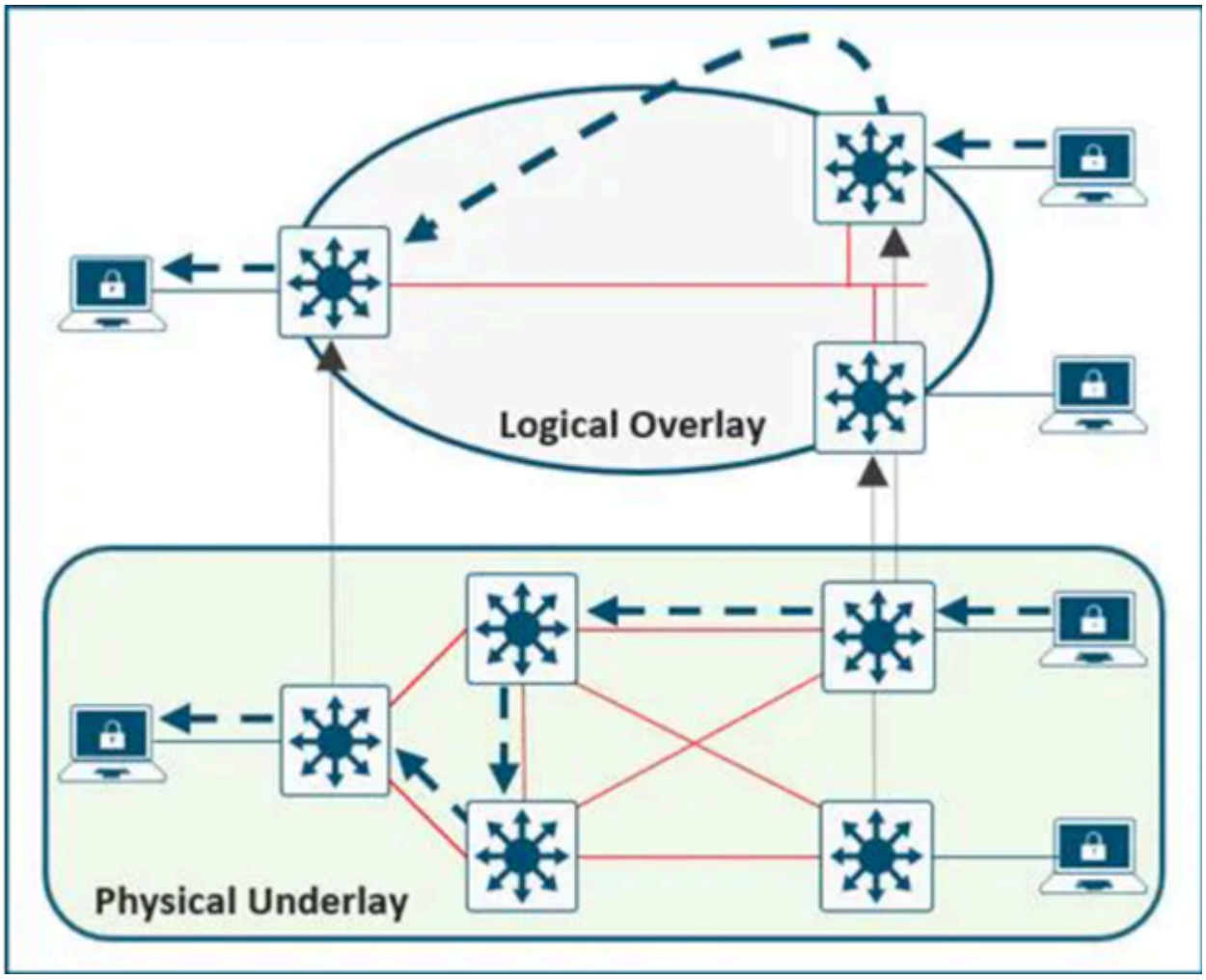
Uma rede de sobreposição é uma topologia lógica usada para conectar virtualmente dispositivos, criada sobre uma topologia de subjacência física arbitrária. Ele usa atributos de encaminhamento alternativos para fornecer serviços adicionais que não são fornecidos pela subjacência. Ele é criado sobre a base para criar uma ou mais redes virtualizadas e segmentadas. Devido à natureza definida por software das sobreposições, é possível conectá-las de formas muito flexíveis sem as restrições da conectividade física. É uma maneira fácil de aplicar políticas de segurança, já que a sobreposição pode ser programável para ter um único ponto de saída físico (o nó de borda de malha) e um firewall pode ser usado para proteger as redes atrás dele (se elas podem ser localizadas). A sobreposição encapsula o tráfego com o uso de VXLAN. A VXLAN encapsula quadros completos da camada 2 para transporte através da subjacência com cada rede de sobreposição identificada por um identificador de rede (VNI) da VXLAN. As estruturas de sobreposição tendem a ser complexas e exigem uma quantidade significativa de sobrecarga do administrador em novas redes virtuais implantadas ou para implementar políticas de segurança.

Exemplos de sobreposições de rede:

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

Uma rede Underlay é definida pelos nós físicos, como switches, roteadores e APs sem fio, que são usados para implantar a rede SDA. Todos os elementos de rede da camada subjacente devem estabelecer conectividade IP por meio do uso de um protocolo de roteamento. Embora não seja provável que a rede subjacente use o modelo tradicional de acesso, distribuição e núcleo, ela deve usar uma base de Camada 3 bem projetada que forneça desempenho robusto, escalabilidade e alta disponibilidade.

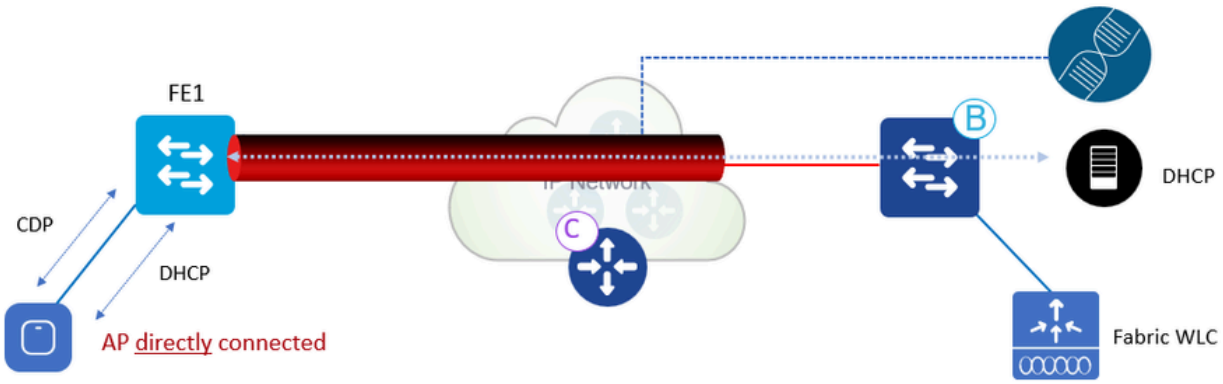
Note: O SDA suporta IPv4 na rede subjacente e IPv4 e/ou IPv6 em redes sobrepostas.



Redes de Sobreposição e de Sobreposição

Fluxos de trabalho básicos

Junção AP



Fluxo de trabalho de ingresso no AP

Fluxo de trabalho de ingresso no AP:

1. O administrador configura o pool de APs no DNAC no INFRA_VN. O Cisco DNA pré-provisiona

uma configuração em todo o Fabric Edge Node para integrar automaticamente APs.

2. O AP está conectado e é ligado. O Fabric Edge descobre que é um AP via CDP e aplica a macro para atribuir (ou o modelo de interface) a porta do switch à VLAN certa.

3. O AP obtém um endereço IP via DHCP na sobreposição.

4. Borda de malha registra o endereço IP e o MAC (EID) dos APs e atualiza o plano de controle (CP).

5. O AP aprende IP de WLCs com métodos tradicionais. O AP de estrutura se une como um AP de modo local.

6. A WLC verifica se ela é compatível com a estrutura (APs Wave 2 ou Wave 1).

7. Se o AP for suportado para Fabric, o WLC consulta o CP para saber se o AP está conectado ao Fabric.

8. Plano de Controle (CP) responde à WLC com RLOC. Isso significa que o AP está conectado à estrutura e é mostrado como "Fabric enabled".

9. A WLC faz um registro L2 LISP para AP no CP (isto é, registro de cliente seguro "especial" de AP). Isso é usado para passar informações importantes de metadados da WLC para a borda da malha.

10. Em resposta a esse registro de proxy, o Plano de Controle (CP) notifica a Borda da Estrutura e passa os metadados recebidos da WLC (flag que diz que é um AP e o endereço IP do AP).

11. Fabric Edge processa as informações, ele aprende que é um AP e cria uma interface de túnel VXLAN para o IP especificado (otimização: o lado do switch está pronto para o ingresso dos clientes).

Os comandos debug/show podem ser usados para verificar e validar o fluxo de trabalho de junção de AP.

Controle o plano

debug lisp control-plane all

show lisp instance-id <L3 instance id> ipv4 server (Deve mostrar o endereço IP do AP registrado pelo switch de borda onde o AP está conectado).

show lisp instance-id <L2 instance id> servidor ethernet (Deve mostrar o rádio do AP, bem como o endereço MAC da ethernet, o rádio do AP registrado pela WLC e o mac da ethernet pelo switch de borda onde o AP está conectado.)

Switch de borda

debug access-tunnel all

debug lisp control-plane all

show access-tunnel summary

show lisp instance < L2 instance id> ethernet database wlc access-points (Deve mostrar a MAC de rádio do AP aqui.)

WLC

show fabric ap summary

Depurações de WLC LISP

set platform software trace wncd chassis ative r0 lisp-agent-api debug

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

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

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

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

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

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

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

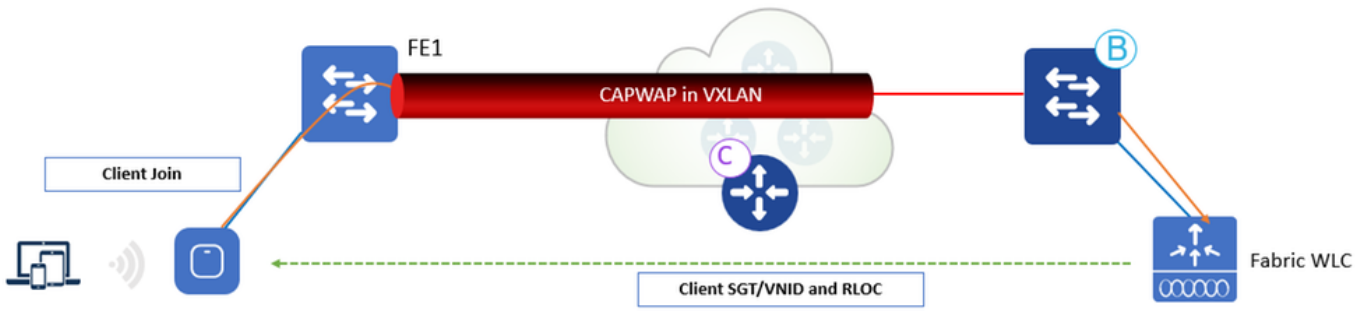
set platform software trace wncd chassis ative r0 lisp-agent-ha debug

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

Ponto de acesso

show ip tunnel fabric

Cliente integrado



Fluxo de trabalho integrado do cliente

Fluxo de trabalho integrado do cliente:

1. O cliente autentica em uma WLAN habilitada para Malha. A WLC obtém o SGT do ISE, atualiza o AP com o L2VNID e o SGT do cliente junto com o IP RLOC. A WLC conhece o RLOC do AP do banco de dados interno.

2. O proxy da WLC registra as informações da L2 do cliente no CP; esta é uma mensagem modificada de LISP para passar informações adicionais, como o SGT do cliente.

3. A borda da malha é notificada pelo PC e adiciona o MAC cliente em L2 à tabela de encaminhamento e busca a política do ISE com base no SGT do cliente.

4. O cliente inicia a solicitação DHCP.

5. O AP o encapsula na VXLAN com informações da L2 VNI.

6. Borda de malha mapeia a VNID da L2 para a interface VLAN e encaminha o DHCP na sobreposição (o mesmo que para um cliente de malha com fio).

7. O cliente recebe um endereço IP do DHCP.

8. O rastreamento de DHCP (e/ou ARP para estático) aciona o registro EID do cliente pelo Fabric Edge para o CP.

Os comandos debug/show podem ser usados para verificar e validar o fluxo de trabalho integrado do cliente.

Controle o plano

debug lisp control-plane all

Switch de borda

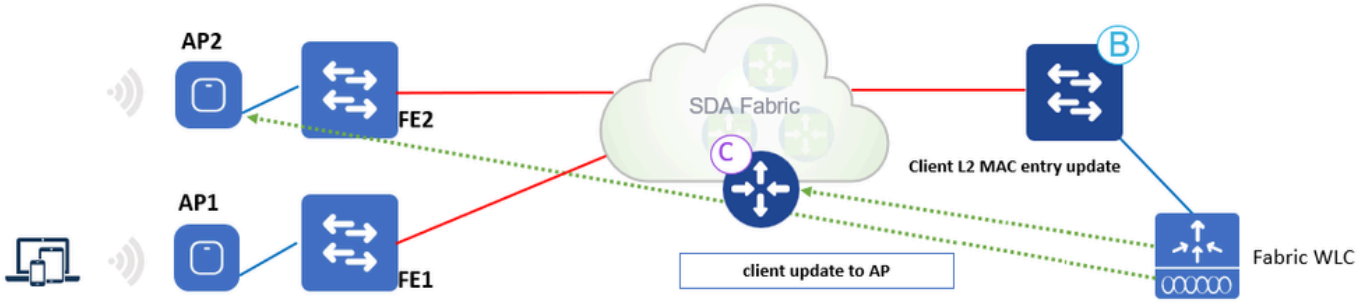
debug lisp control-plane all

debug ip dhcp snooping packet/event

WLC

Para a comunicação LISP, as mesmas depurações que a junção AP.

Roaming de Clientes



Fluxo de Trabalho de Roams do Cliente

Fluxo de trabalho de roaming de clientes:

1. O cliente faz roaming para o AP2 no FE2 (roaming entre switches). A WLC é notificada pelo AP.

2. A WLC atualiza a tabela de encaminhamento no AP com informações do cliente (SGT, RLOC).

3. A WLC atualiza a entrada MAC de L2 no PC com o novo RLOC Fabric Edge 2.

4. A CP notifica então:

- Fabric Edge FE2 (roam-to-switch) para adicionar o MAC cliente à tabela de encaminhamento que aponta para o túnel VXLAN.
- Fabric Edge FE1 (roam-from switch) para fazer a limpeza do cliente sem fio.

5. Fabric Edge atualiza a entrada L3 (IP) no banco de dados CP ao receber o tráfego.

6. Roam é a Camada 2, pois Fabric Edge 2 tem a mesma interface VLAN (Anycast GW).

Configurar

Diagrama de Rede

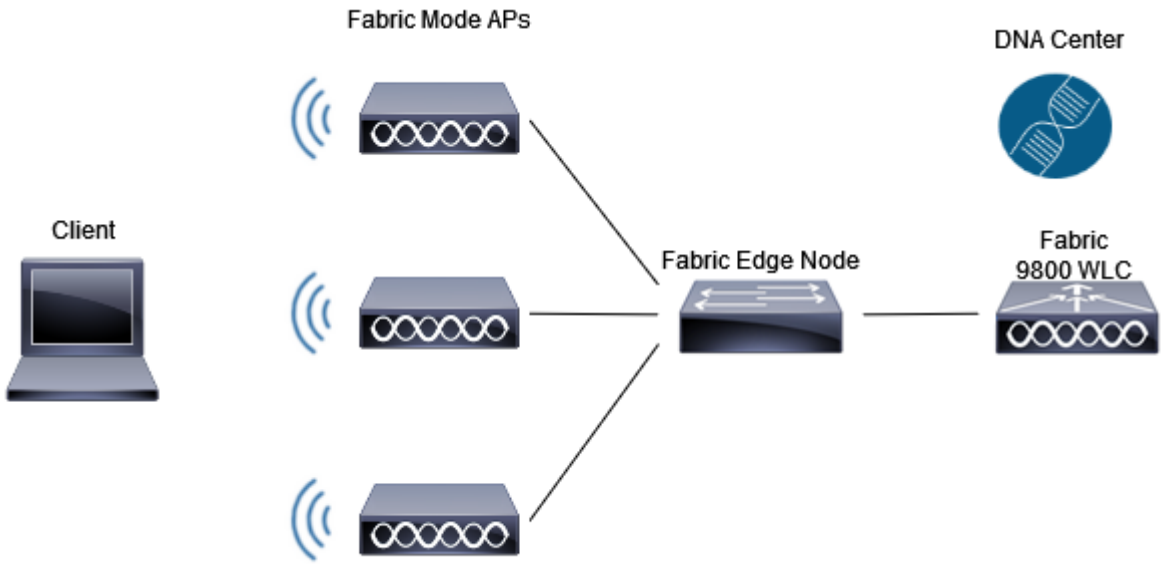


Diagrama de Rede

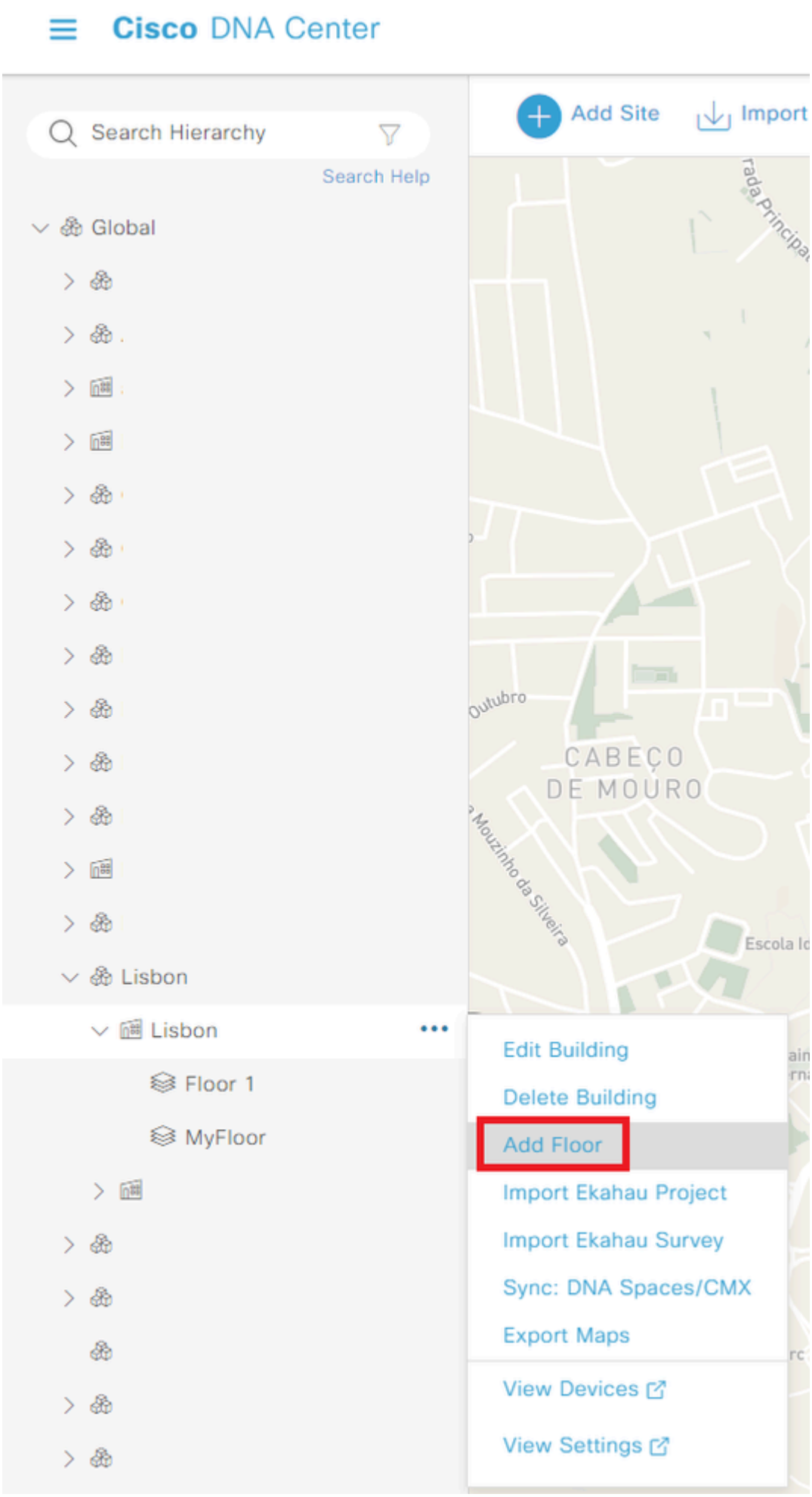
Descoberta e provisionamento de WLC no Cisco DNA

Adicionar WLC

Etapa 1. Navegue até o local onde você deseja adicionar a WLC. Você pode adicionar um novo

edifício/andar.

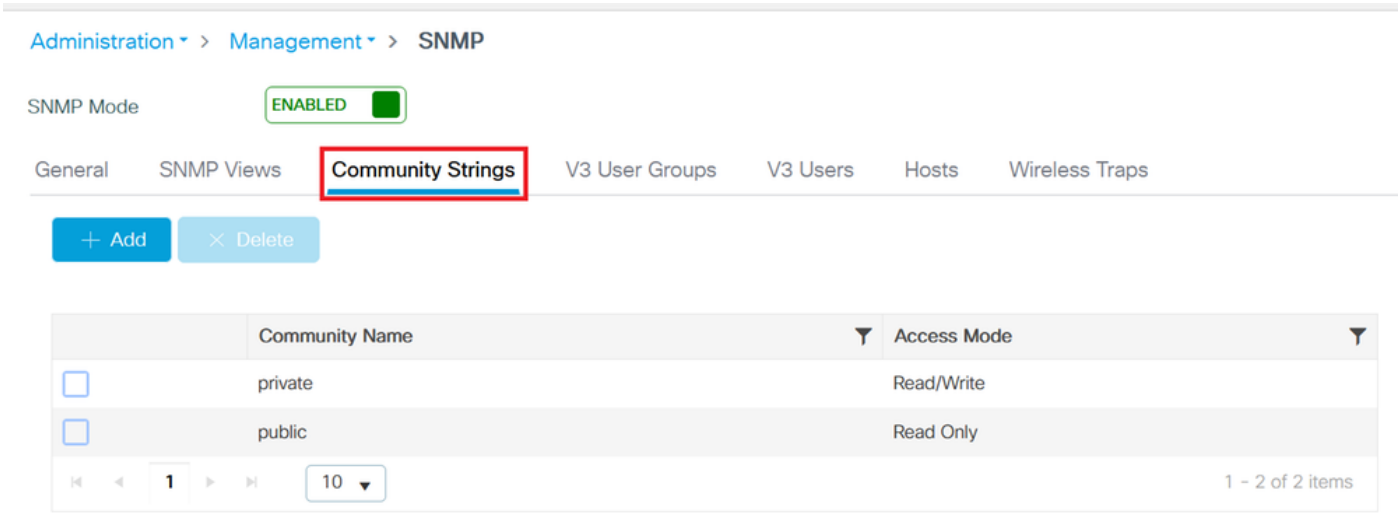
Navegue até Design > Network Hierarchy e entre no edifício/andar, ou você pode criar um novo andar, como mostrado na imagem:



Criar novo andar

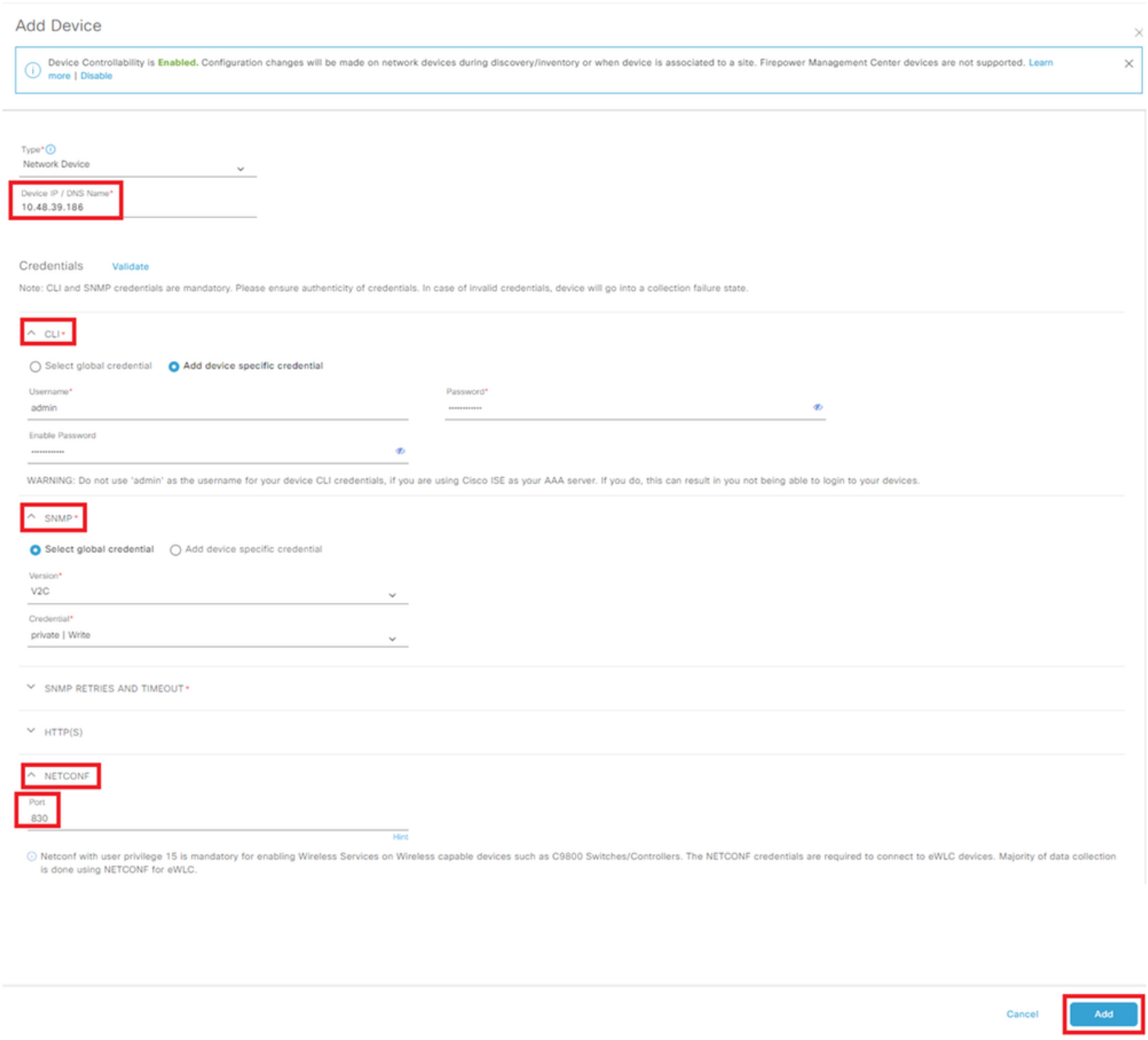
Etapa 2. Adicionar andar. Você também pode carregar uma imagem da planta do chão de fábrica

e verifique a string configurada. Você precisa adicionar a série de comunidade SNMP correta ao adicionar a WLC no Cisco DNA e garantir que o netconf-yang esteja habilitado na WLC 9800 com os comandos show netconf-yang status. No final, clique em Adicionar:



Configuração de SNMP

Etapa 5. Adicione o endereço IP da WLC, as credenciais da CLI (as credenciais que o Cisco DNA usa para fazer login na WLC e elas devem ser configuradas na WLC antes de adicioná-la ao Cisco DNA), a string SNMP e verifique se a porta NETCONF está configurada na porta 830:

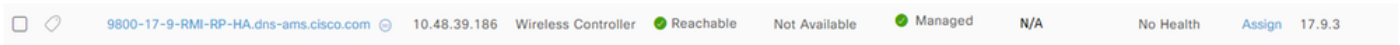


Adicionar WLC

A WLC aparece como NA porque o Cisco DNA ainda está em processo de sincronização:

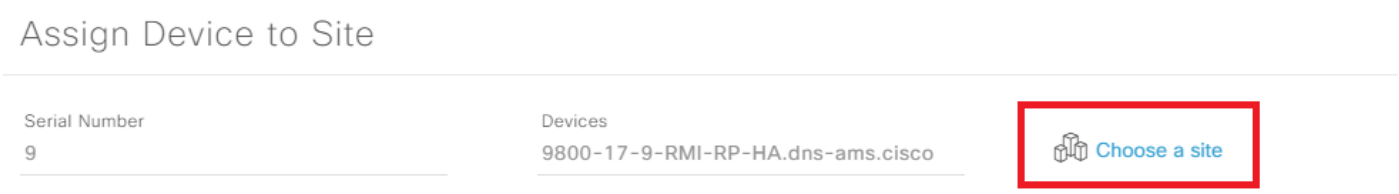
WLC em processo de sincronização

Ao concluir o processo de sincronização, você poderá ver o nome da WLC, o endereço IP, se estiver acessível, gerenciado e a versão do software:



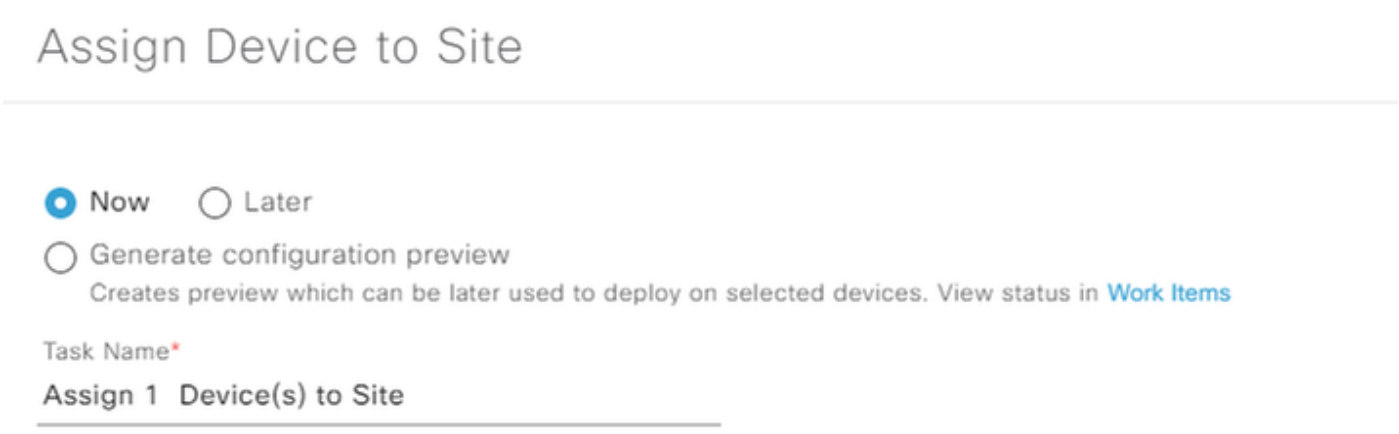
WLC sincronizado

Etapa 6. Atribuir a WLC a um site. Na lista de dispositivos, clique em Atribuir e escolha um site:



Atribuir dispositivo ao site

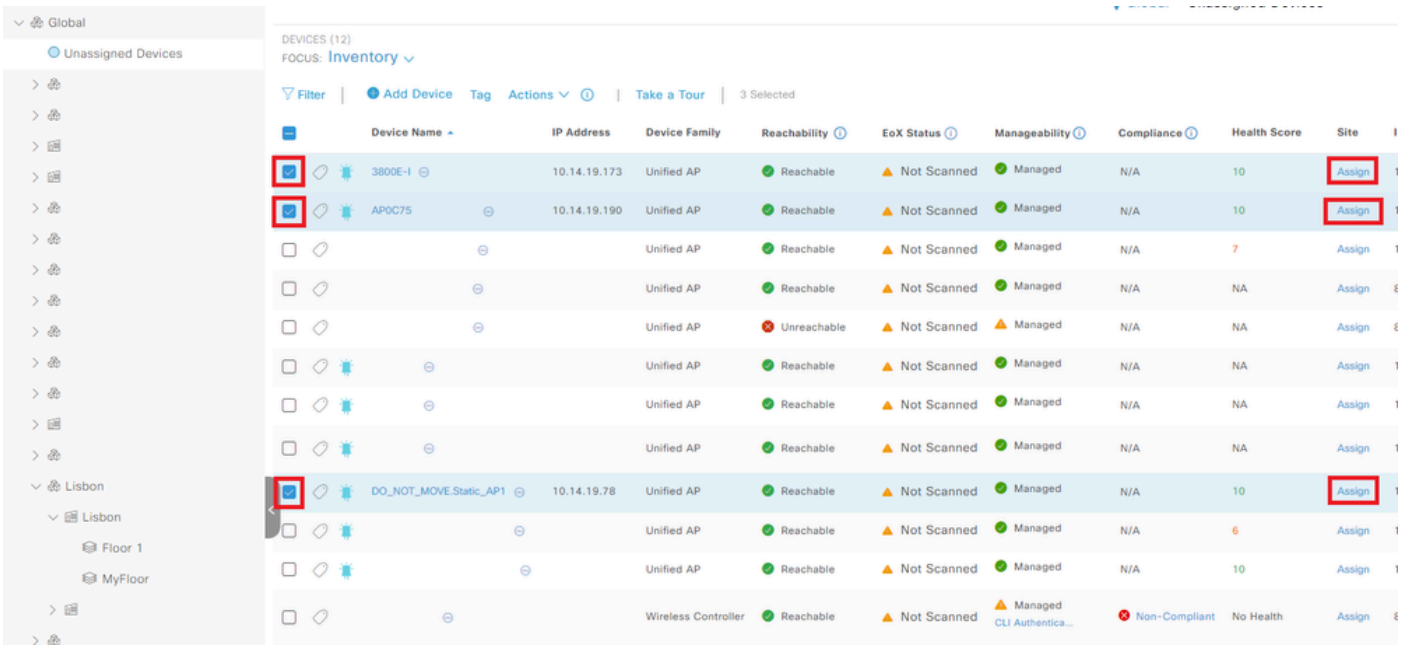
Você pode decidir atribuir o site agora ou mais tarde:



Atribuir dispositivo ao site agora ou depois

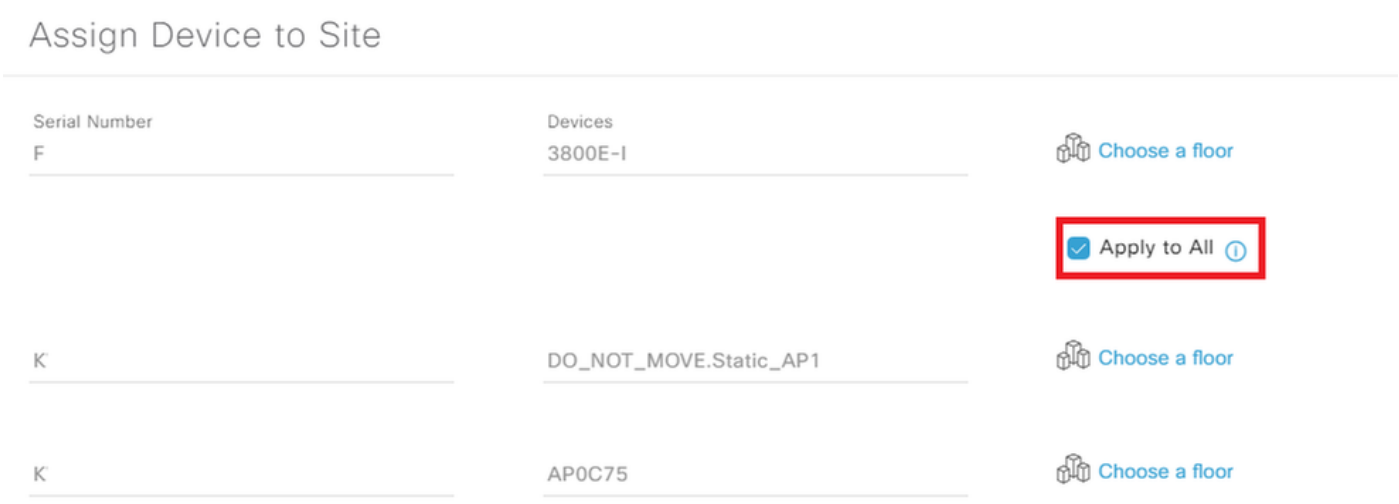
Adicionar pontos de acesso

Etapa 1.Assim que a WLC for adicionada e estiver acessível, navegue para Provision > Inventory > Global > Unassigned Devices e procure os APs que você associou à sua WLC:



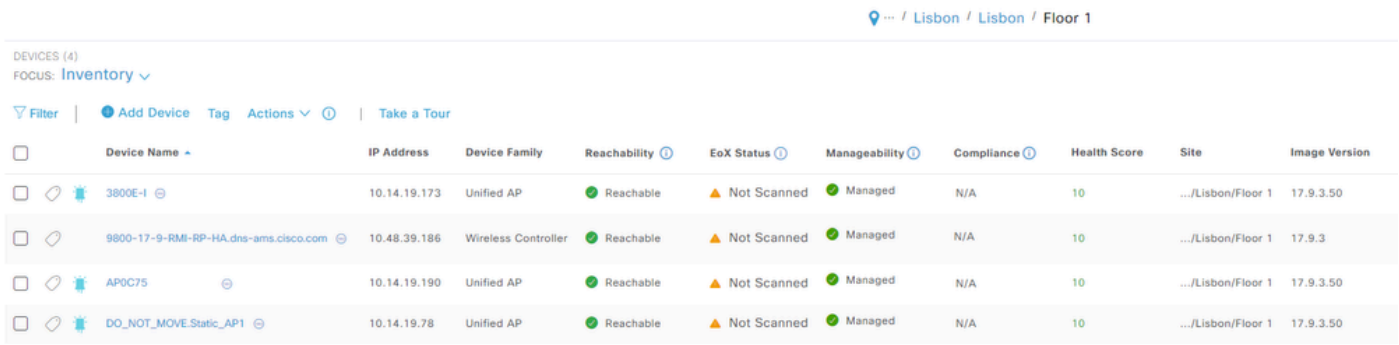
Adicionar pontos de acesso

Etapa 2. Selecione a opção Atribuir. Atribua os APs a um site. Marque a caixa Apply to All para fazer a configuração para mais de um dispositivo ao mesmo tempo.



Atribuir APs ao site

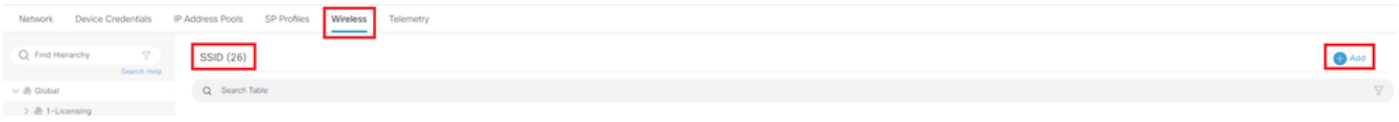
Navegue até seu andar e você poderá ver todos os dispositivos atribuídos a ele - WLC e APs:



Dispositivos Atribuídos ao Site

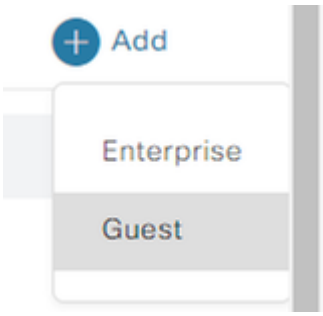
Criar SSID

Etapa 1. Navegue até Design > Network Settings > Wireless > Global e adicione um SSID:



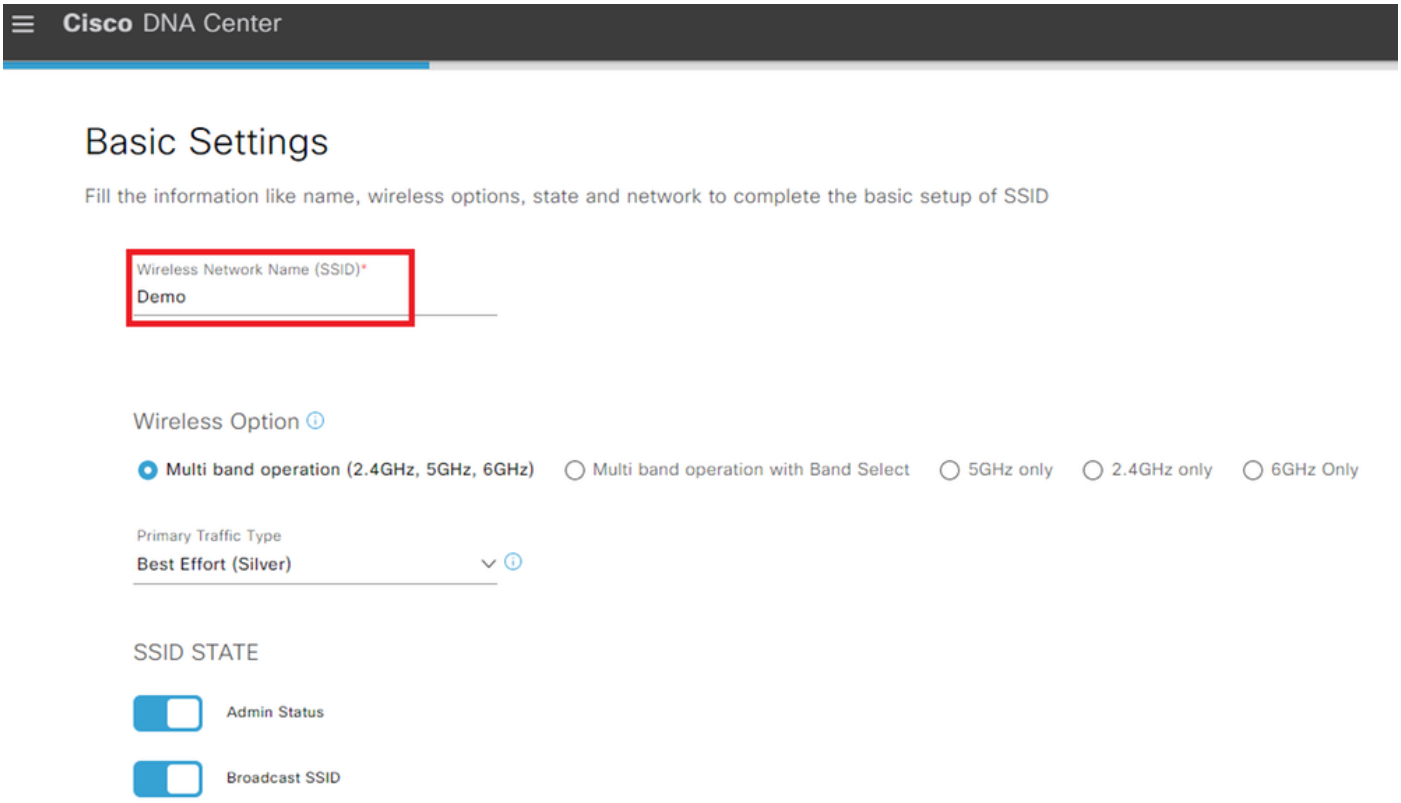
Criar SSID

Você pode criar um Enterprise SSID ou um Guest SSID. Nesta demonstração, um SSID de convidado é criado:

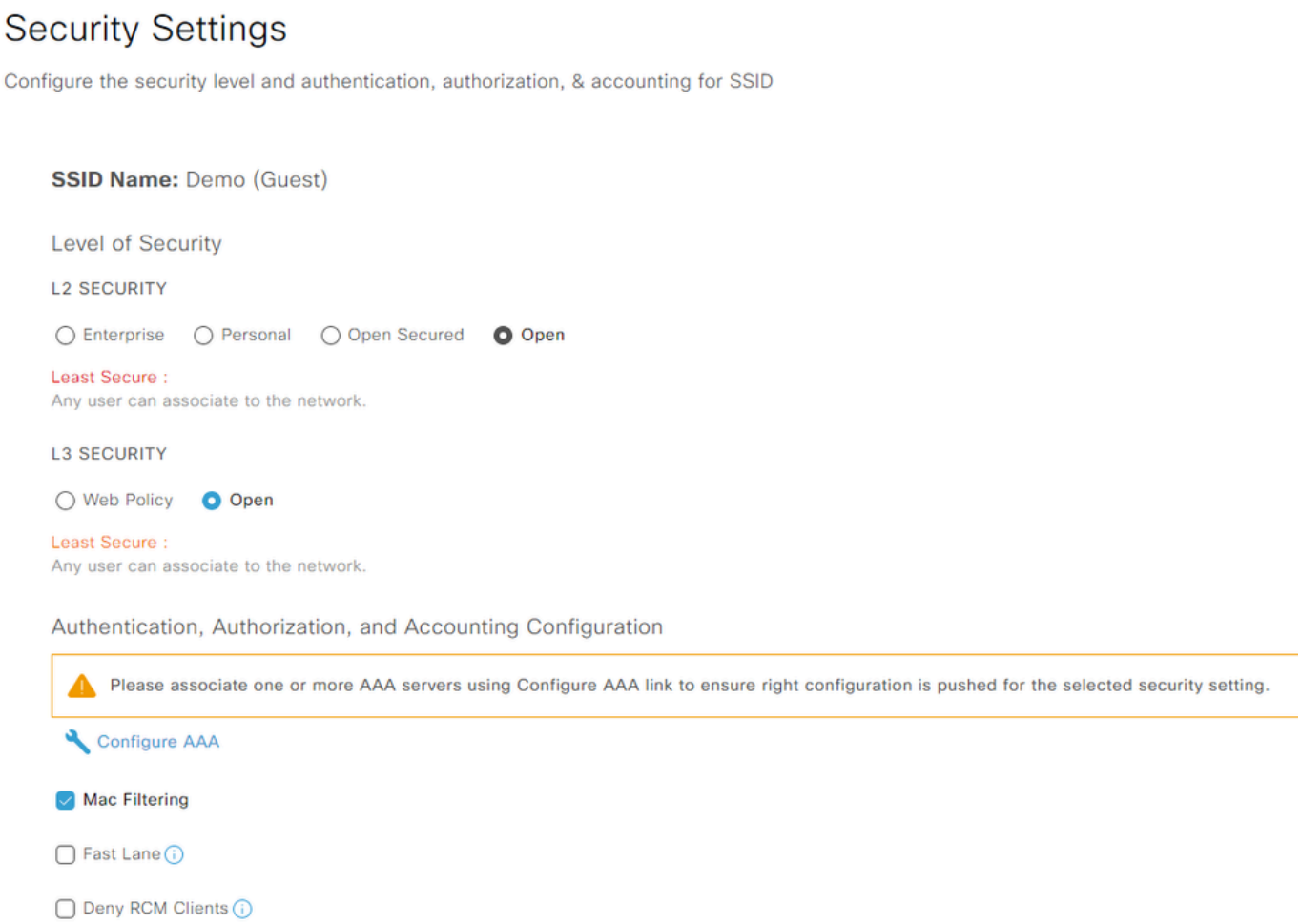


SSID corporativo ou convidado

Etapa 2. Escolha a configuração desejada para o SSID. Nesse caso, um SSID aberto é criado. O status do administrador e o SSID de difusão devem ser habilitados:



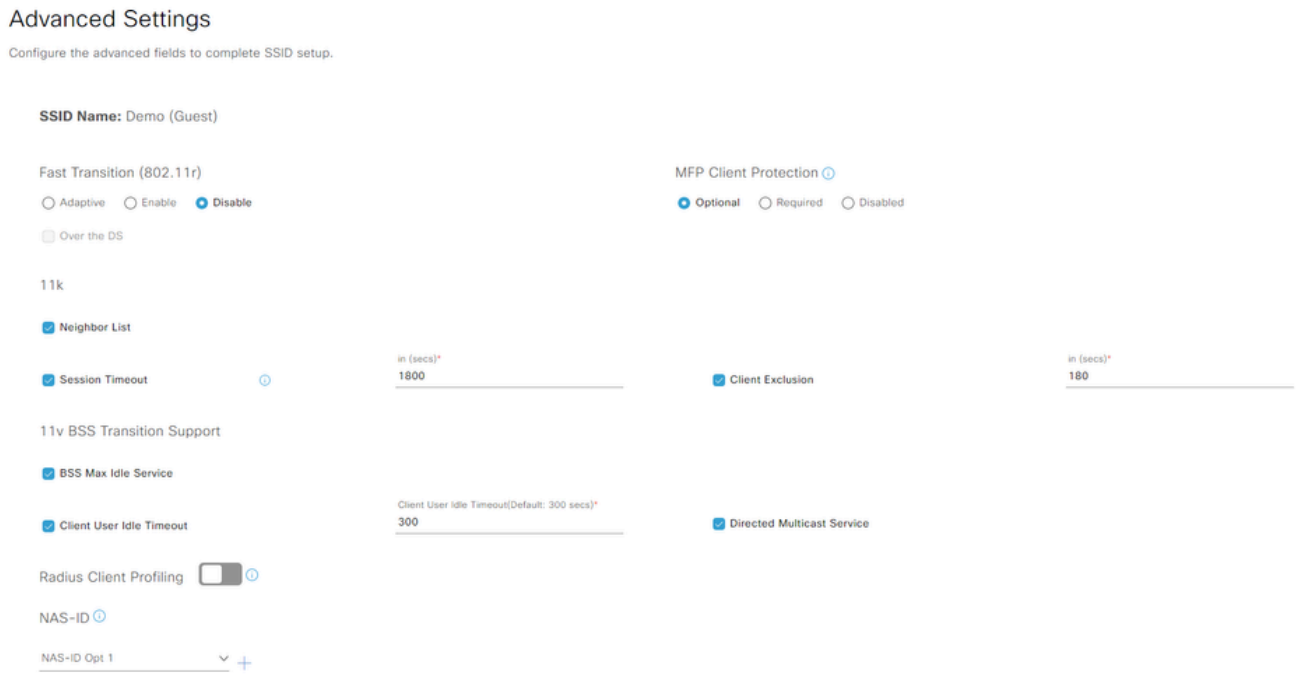
Configurações básicas de SSID



Configurações de segurança SSID

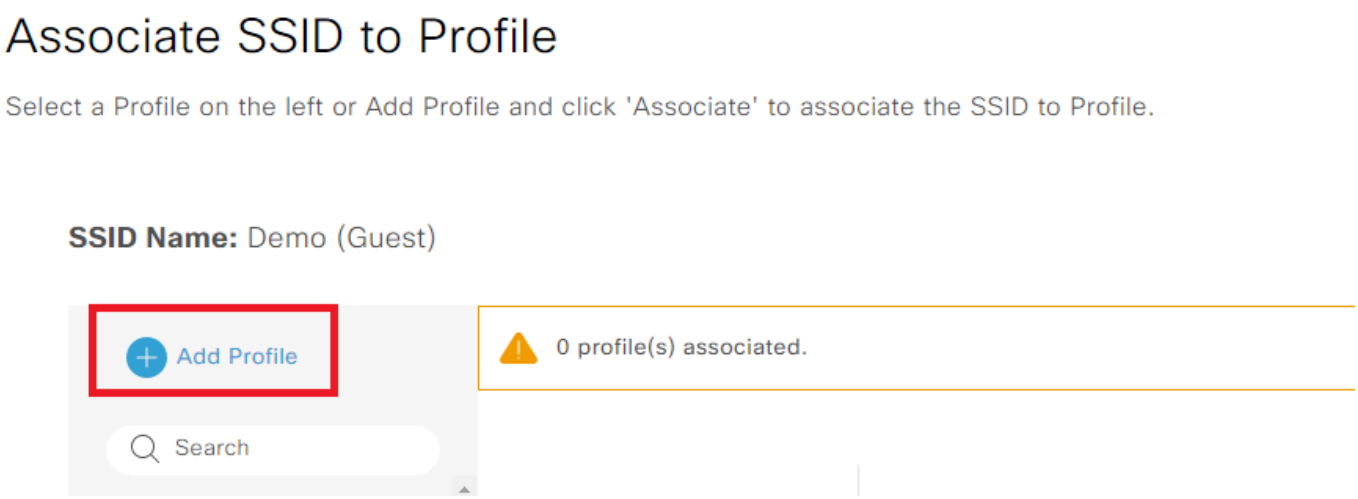
⚠ Caution: Não se esqueça de configurar e associar o servidor AAA para o SSID. A lista de métodos padrão será mapeada se nenhum servidor AAA estiver configurado.

Ao clicar em avançar, você poderá ver as configurações avançadas para o SSID:



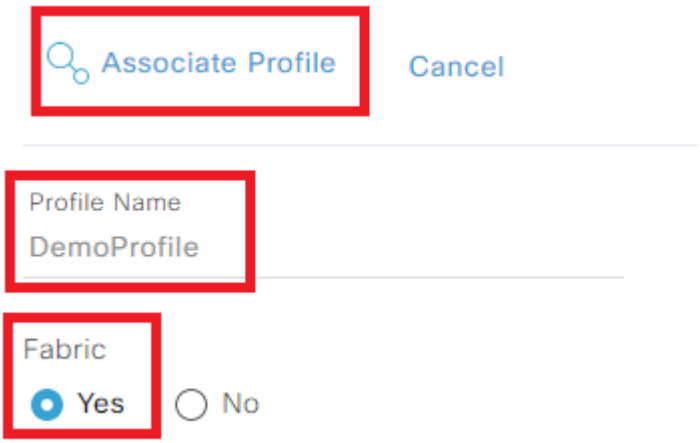
Configurações avançadas de SSID

Etapa 3. Após a criação do SSID, você precisa associá-lo a um perfil. Clique em Add Profile:



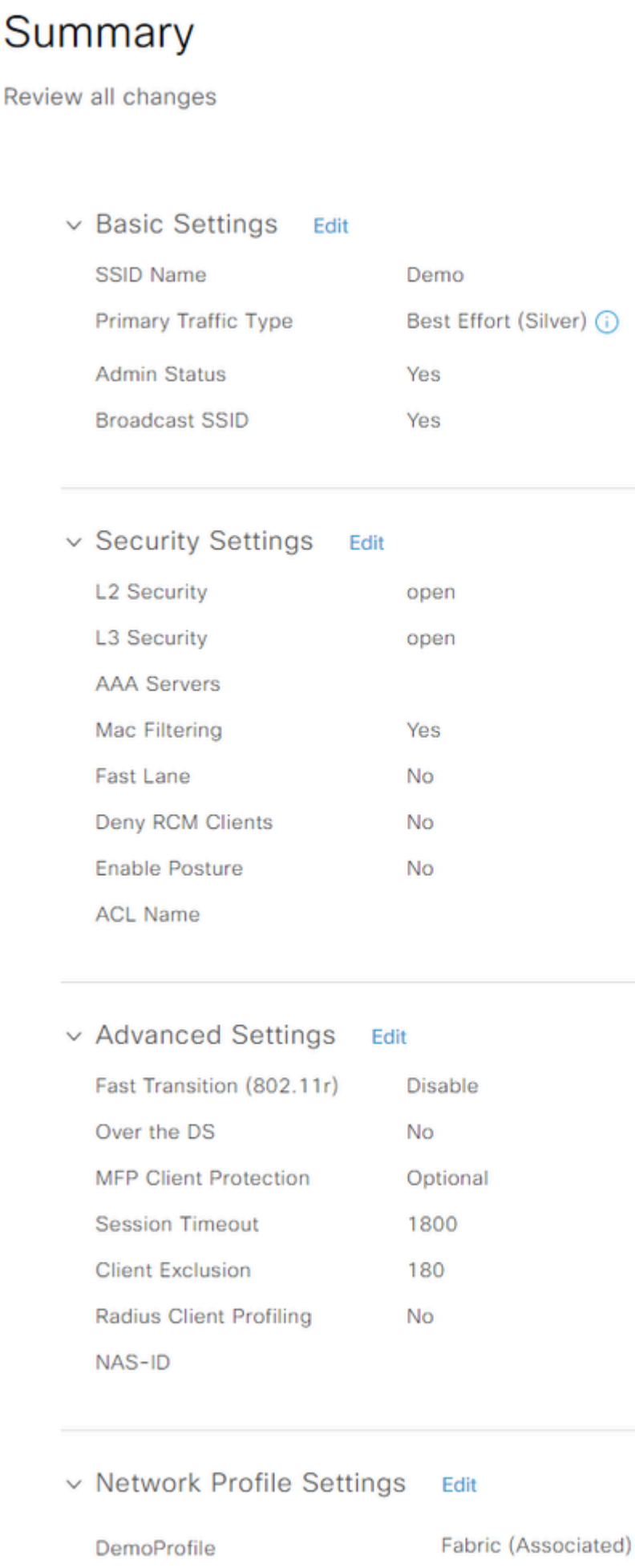
Adicionar perfil

Etapa 4. Dê um nome ao perfil, selecione Fabric e no final clique em Associar perfil:



Associar perfil

Você verá um resumo do SSID e do perfil que criou:



Resumo de SSID

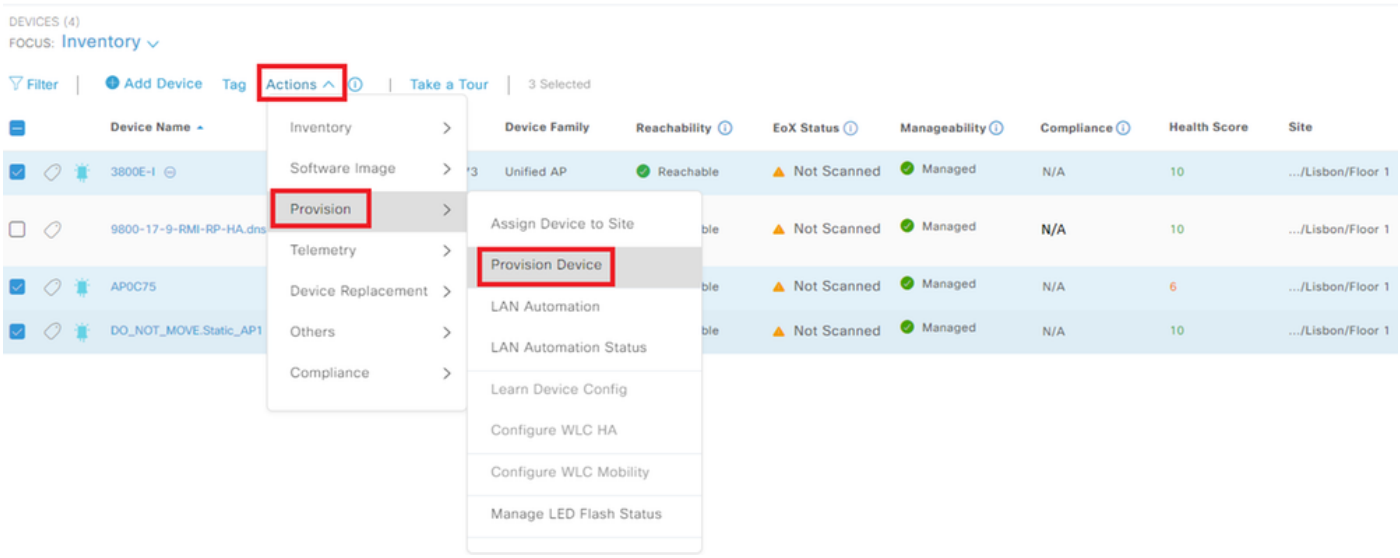
Etapa 5. Configurar um novo perfil de rede:

que deseja configurar. Nesta demonstração, as configurações padrão foram definidas. Clique em Salvar:

Adicionar perfil de RF básico

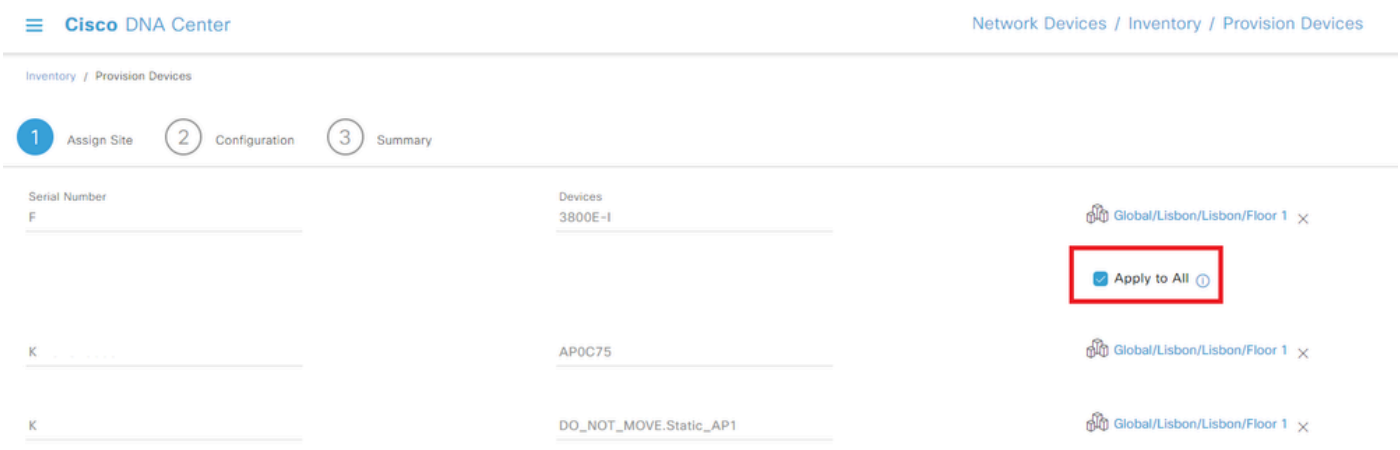
Provisionar Pontos de Acesso

Etapa 1. Navegue até o edifício/andar. Selecione os APs e Ações > Provisionar > Provisionar dispositivo:



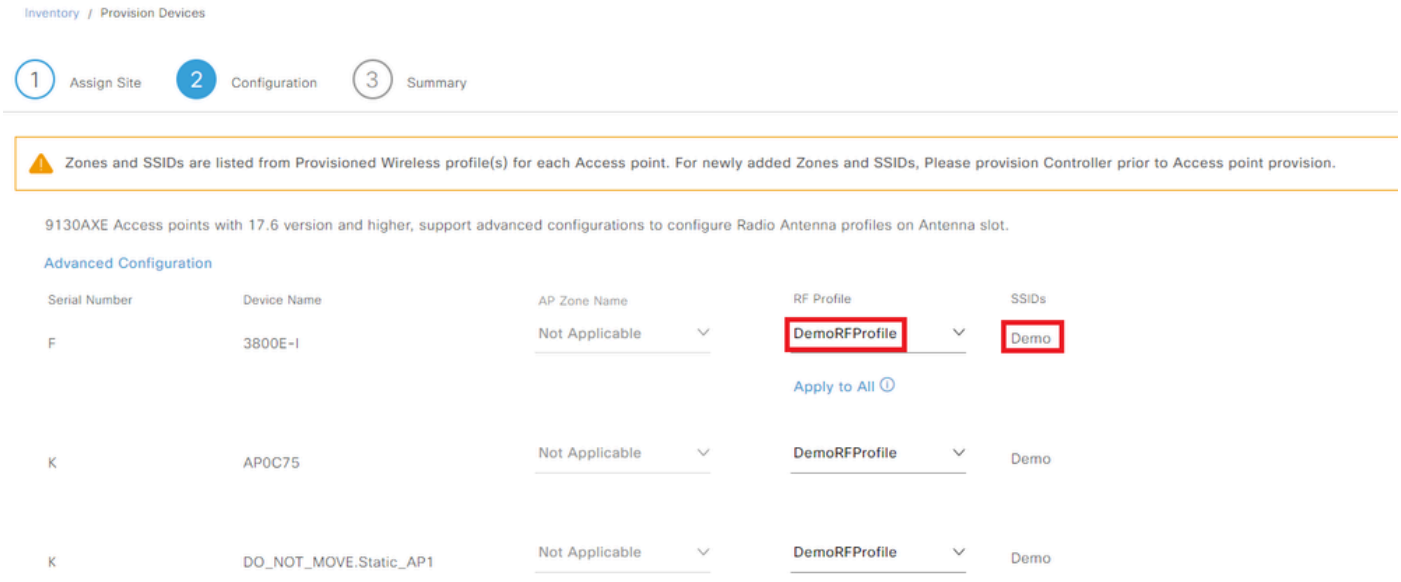
Provisionar APs

Etapa 2. Verifique se o site atribuído está correto e selecione Aplicar a todos:



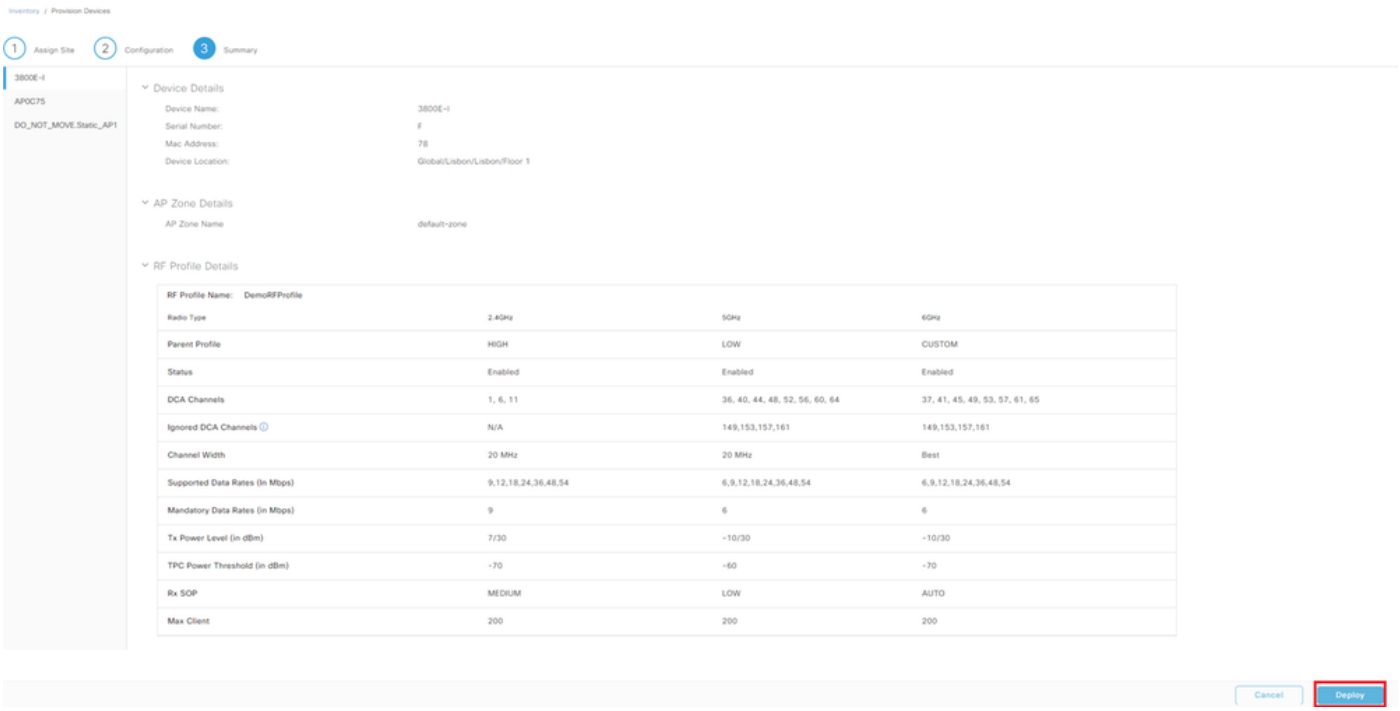
Atribuir site a APs

Etapa 3. Selecione um perfil de RF na lista suspensa e verifique se o SSID é o correto:



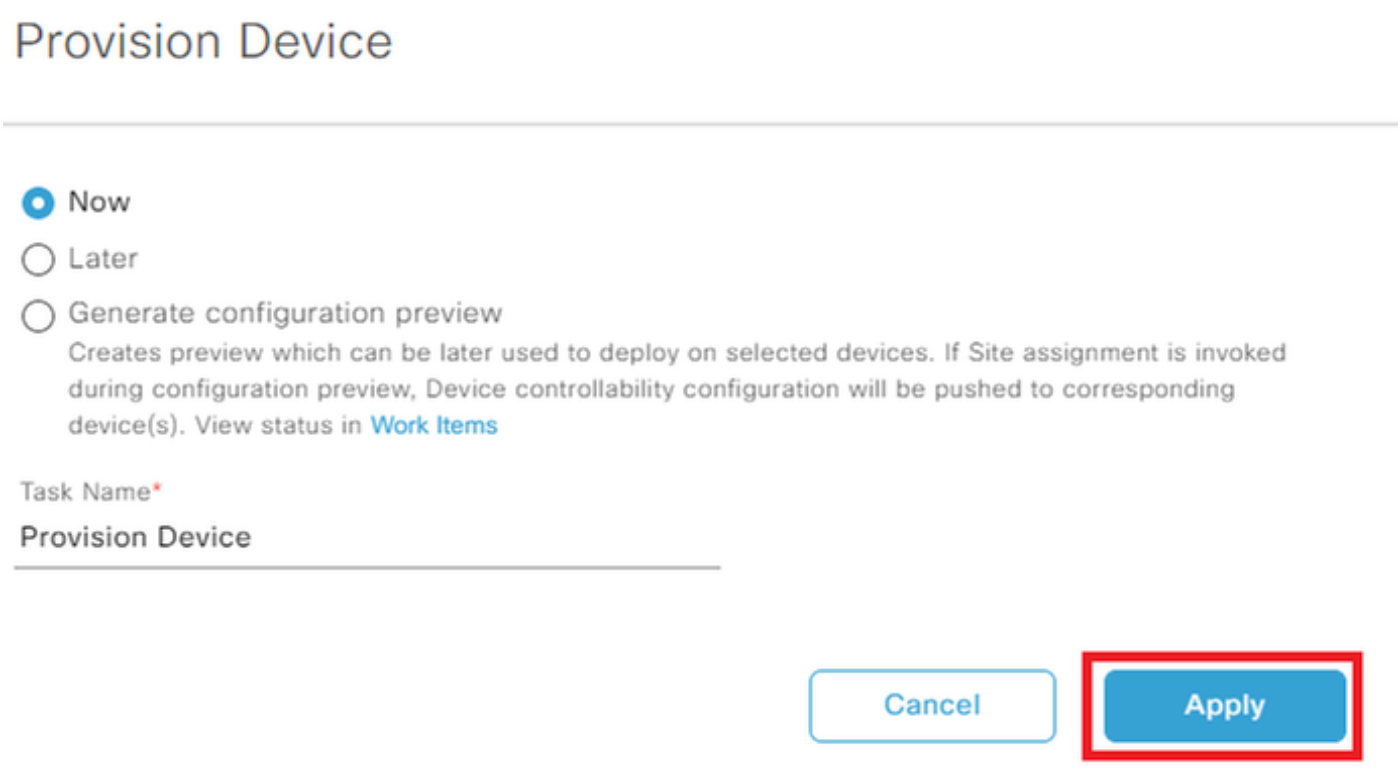
Selecionar perfil de RF

Etapa 4. Verifique as configurações nos APs. Se tudo estiver correto, selecione Implantar:



Implantar provisionamento de APs

Etapa 5. A provisão do dispositivo pode ser implantada no momento ou posteriormente. No final, selecione Aplicar:

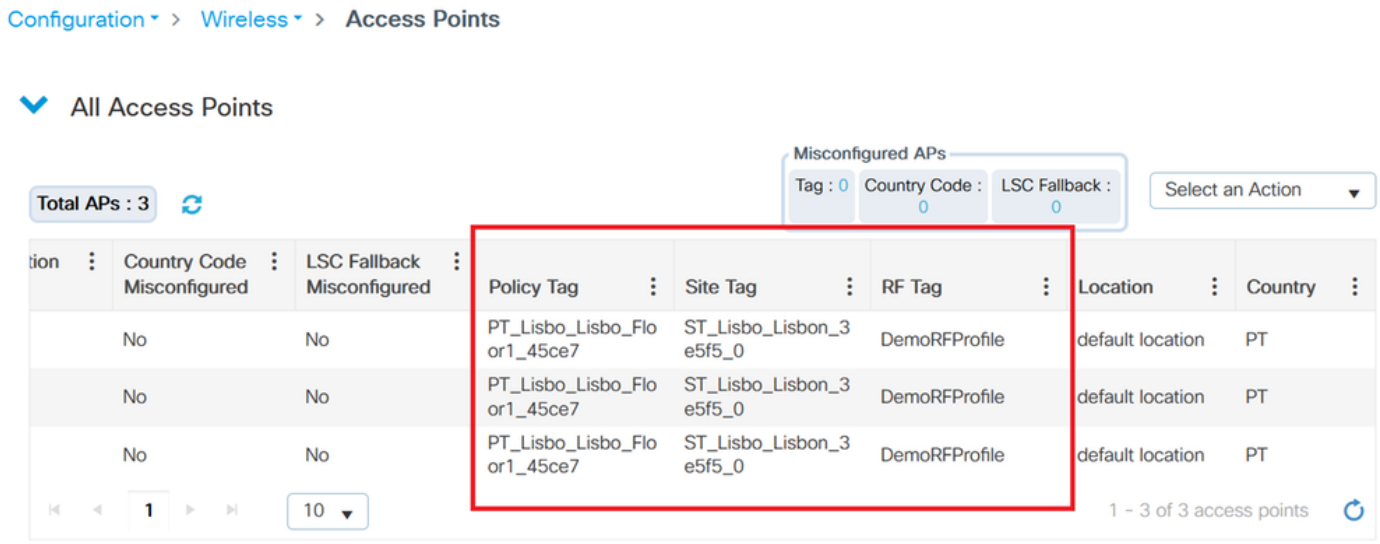


Provisionar APs Agora ou Mais Tarde

⚠ Caution: Ao provisionar os APs, que já fazem parte do chão-de-fábrica configurado para o perfil de RF selecionado, eles devem ser processados e reiniciados.

Os APs agora são provisionados.

Etapa 6. No lado da WLC, navegue para Configuration > Wireless > Access Points. Verifique se as marcas de AP foram enviadas do Cisco DNA:



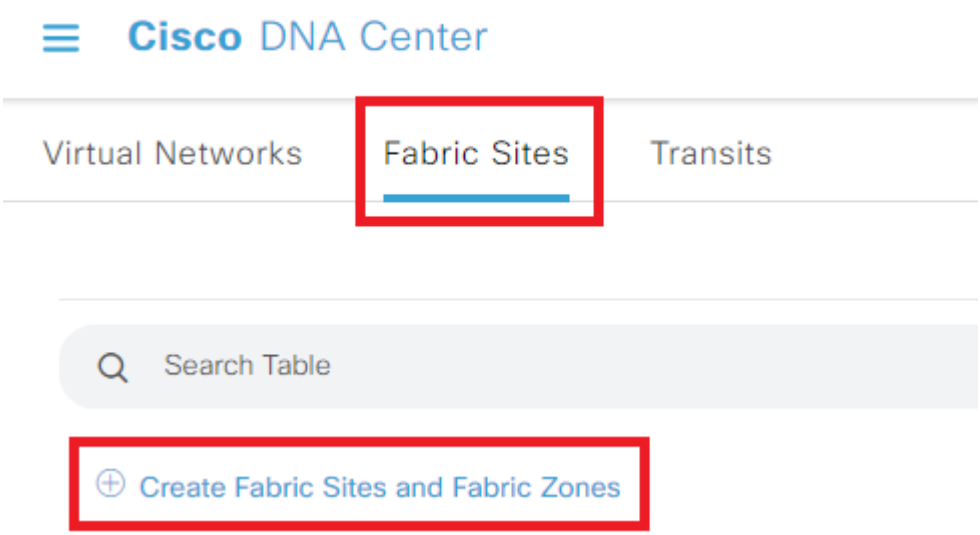
Marcas em APs

Etapa 7. Navegue até Configuration > Tags & Profiles > WLANs e verifique se o SSID foi enviado do Cisco DNA:

WLAN

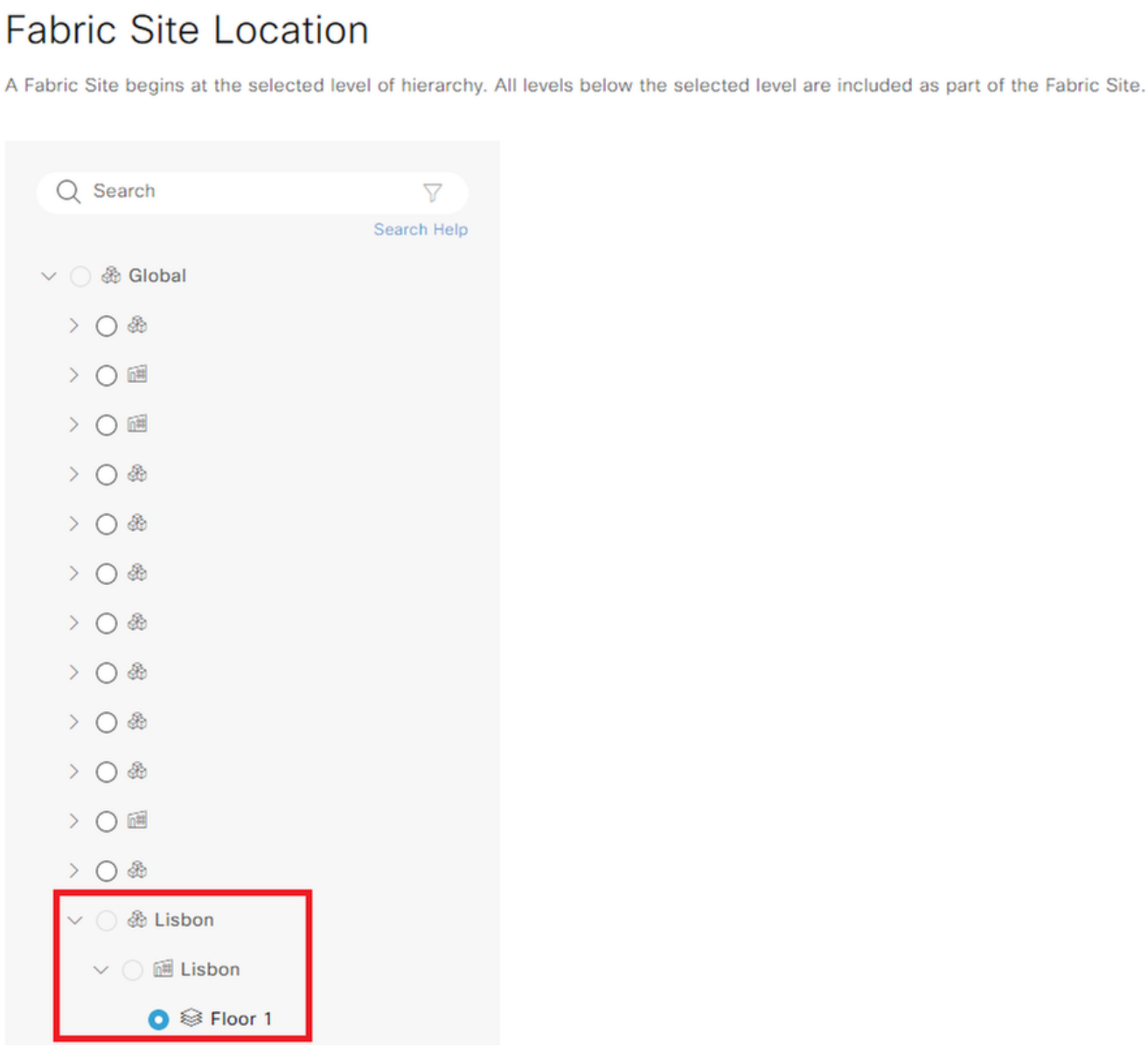
Criar Site de Malha

Etapa 1. Navegue até Provisionar > Sites de malha. Criar um site de malha:



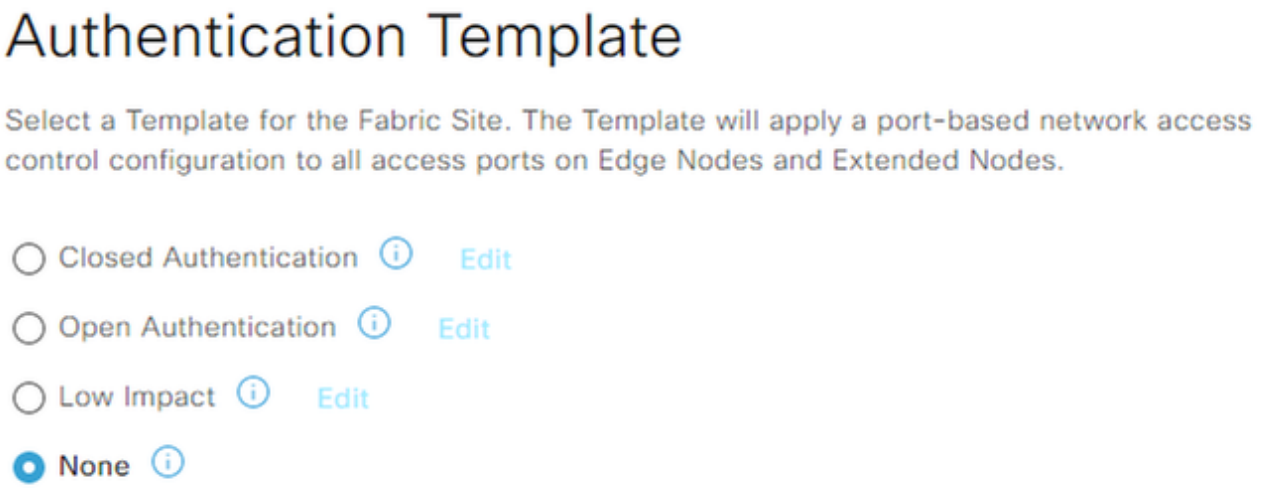
Criar Sites de Malha

Etapa 2. Selecione o edifício/andar para o local da estrutura:



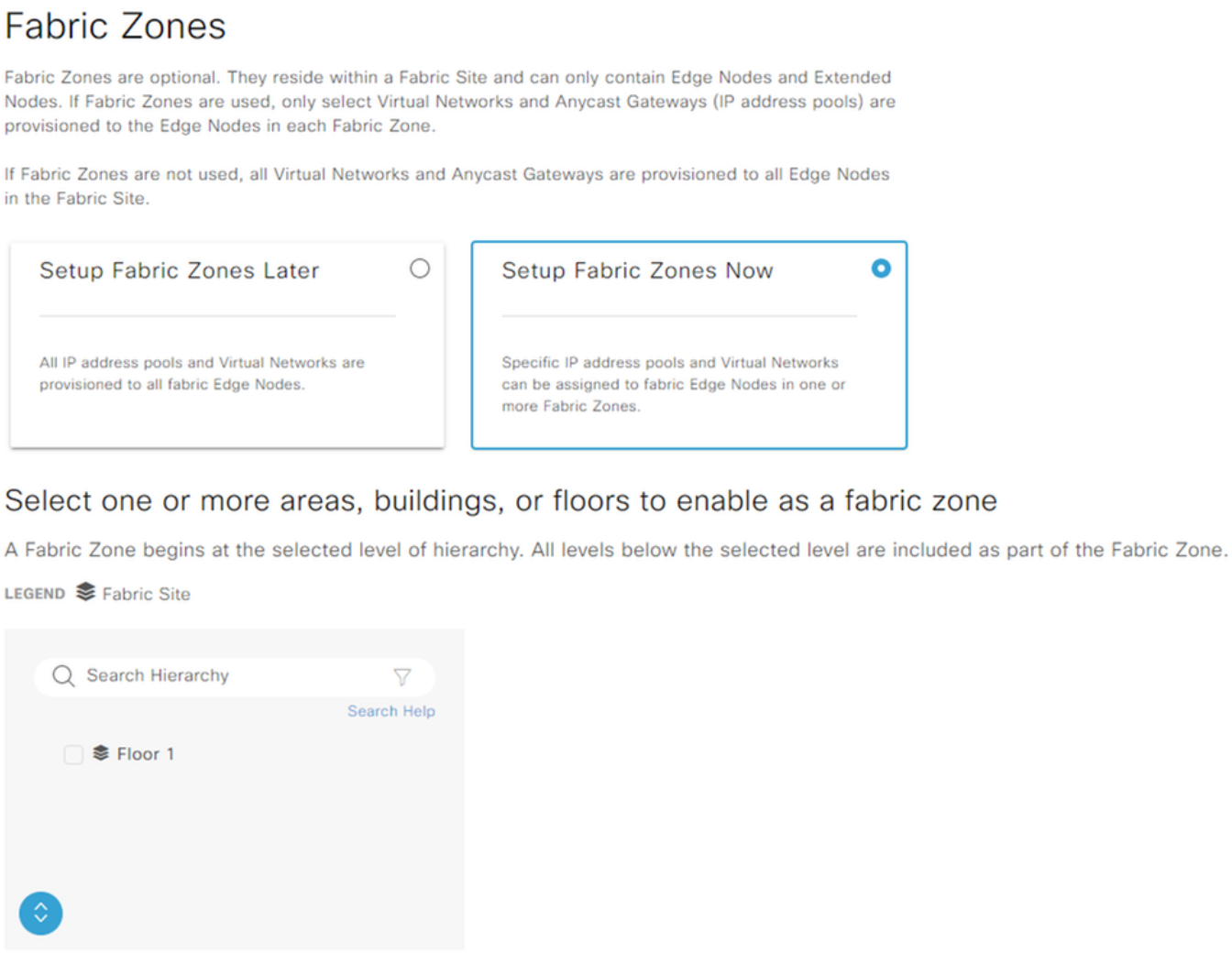
Selecionar Site de Malha

Etapa 3. Selecione um modelo de autenticação. Nesta demonstração, Nenhum foi aplicado:



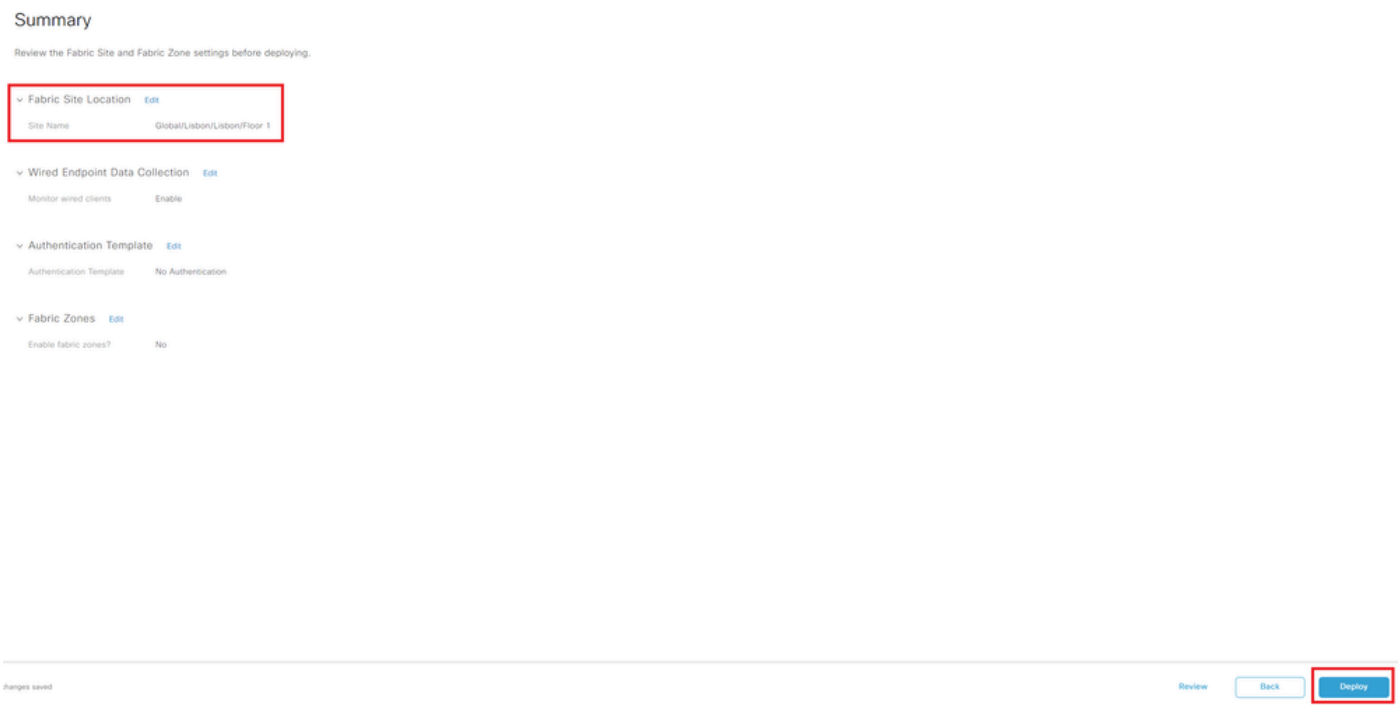
Modelo de autenticação

Etapa 3. Você pode escolher se deseja configurar a zona de malha agora ou mais tarde:



Configurar zonas de malha

Etapa 4. Verifique as configurações da zona de malha. Se tudo estiver correto, selecione Implantar:



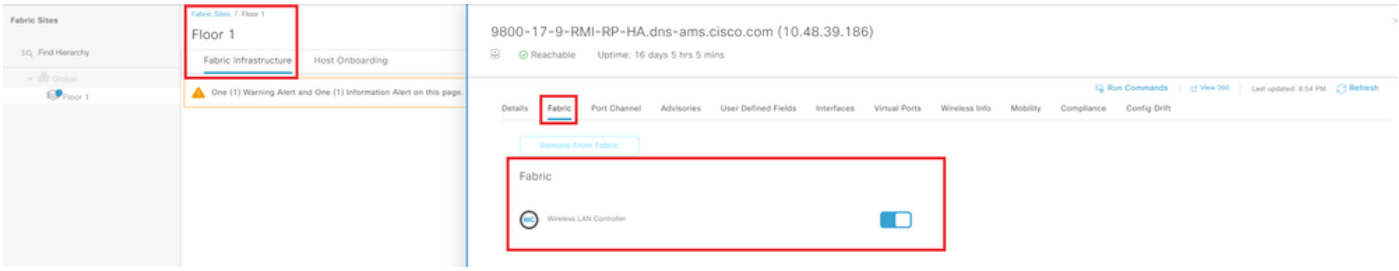
Implantar Site de Malha

Você criou um Site de Malha:

Criação de Site de Malha

Adicionar WLC à malha

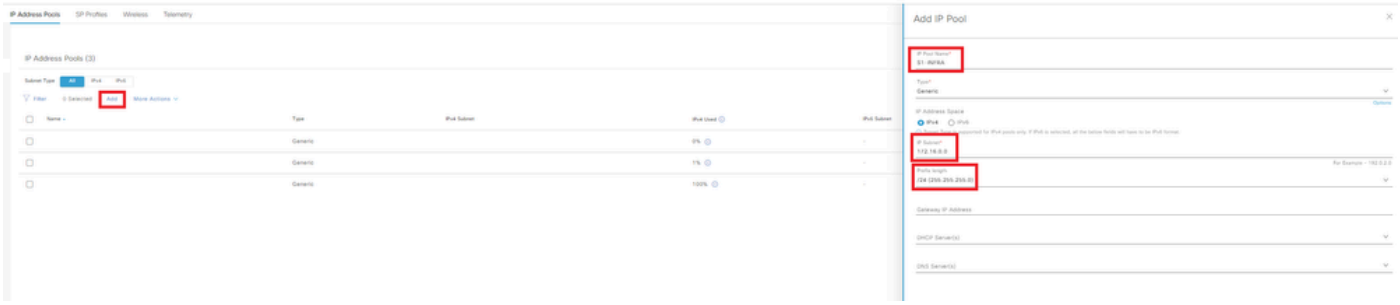
Navegue para Provisionar > Sites de estrutura e selecione o site de estrutura. Clique na parte superior da sua WLC e navegue até a guia Fabric. Habilite fabric para o WLC e selecione Add:



Adicionar WLC à malha

Junção AP

Etapa 1. Navegue até Design > Network Settings > IP Address Pools. Crie um pool de endereços IP.



Pool de Endereços IP

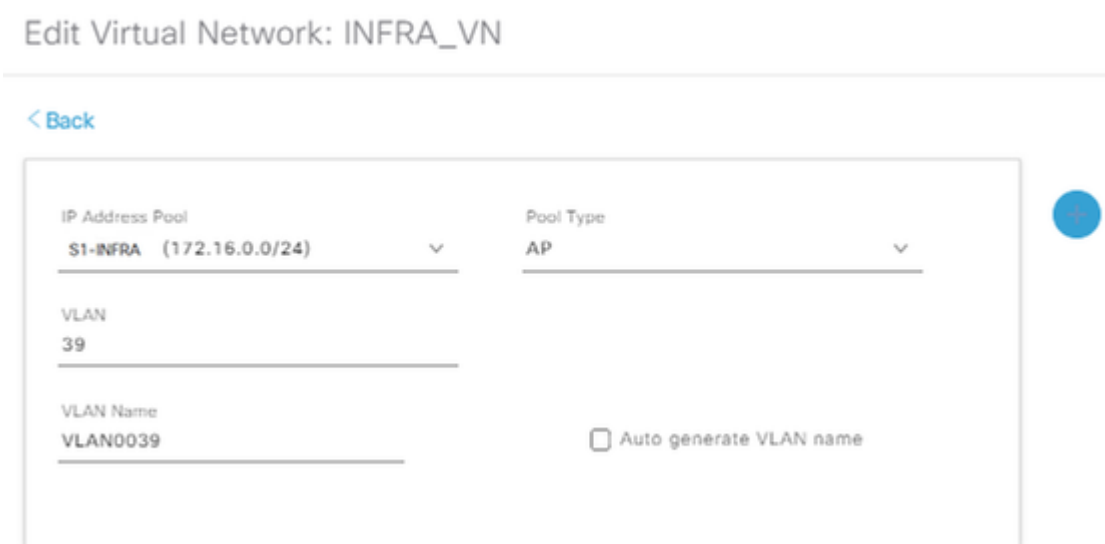
Etapa 2. Navegue até Provisionar > Sites de estrutura e selecione o site de estrutura. Navegue até Integração de host > Redes virtuais.

O INFRA_VN é introduzido para integrar facilmente APs. Os APs estão na sobreposição de estrutura, mas INFRA_VN é mapeado para a tabela de roteamento global. Somente APs e nós estendidos podem pertencer a INFRA_VN. A extensão da camada 2 é automaticamente ativada e ativa o serviço L2 LISP.

Selecione INFRA_VN > Adicionar:

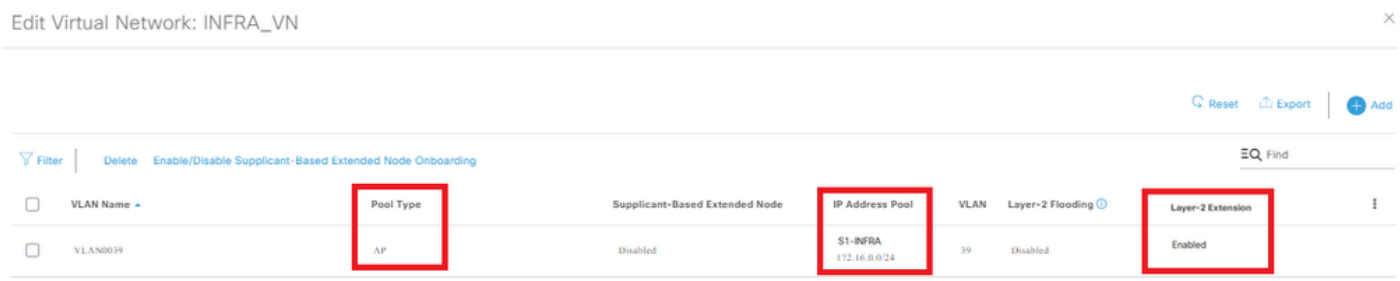
Editar rede virtual

Etapa 3. Adicionar um pool de endereços IP com tipo de pool como AP:



Editar rede virtual S1-INFRA

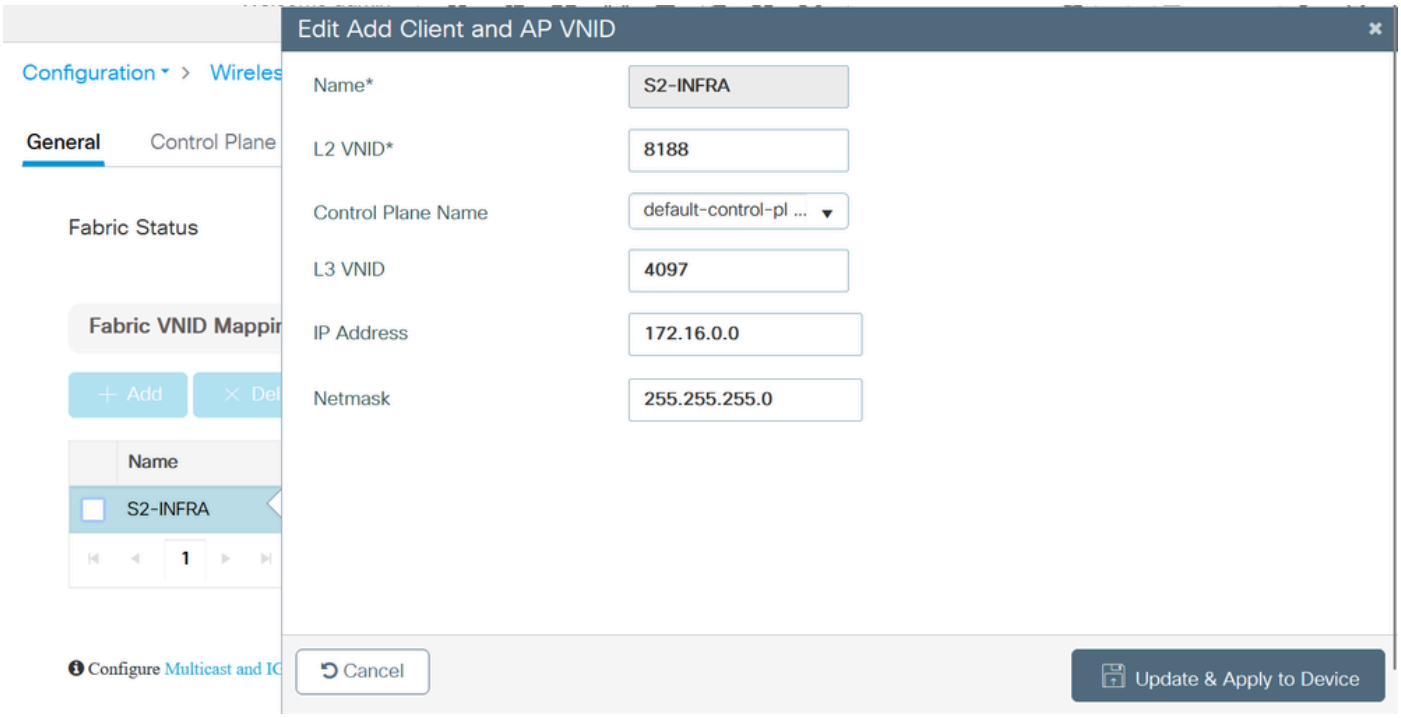
Etapa 4. Verificar se a extensão da camada 2 está ativada.



Editar rede virtual

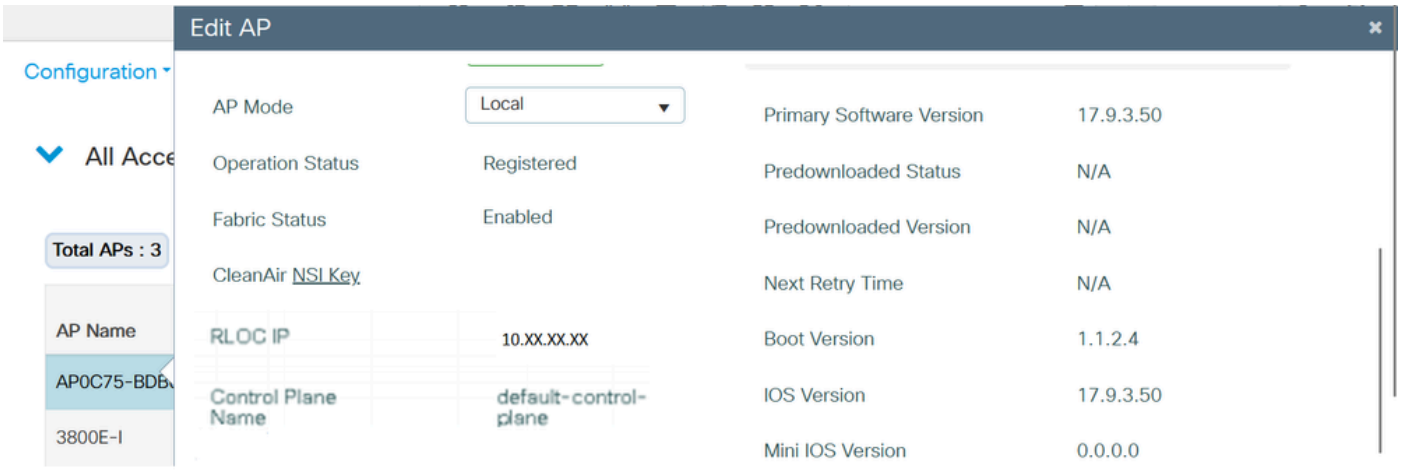
Com Tipo de pool = AP e extensão de Camada 2 para ON, o Cisco DNA se conecta à WLC e define a interface de estrutura para mapeamento VN_ID para a sub-rede AP para VN_IDs de L2 e L3.

Etapa 5. Na GUI da WLC, navegue para Configuration > Wireless > Fabric > General. Adicione um novo cliente e AP VN_ID:



Adicionar novo cliente e AP VN_ID

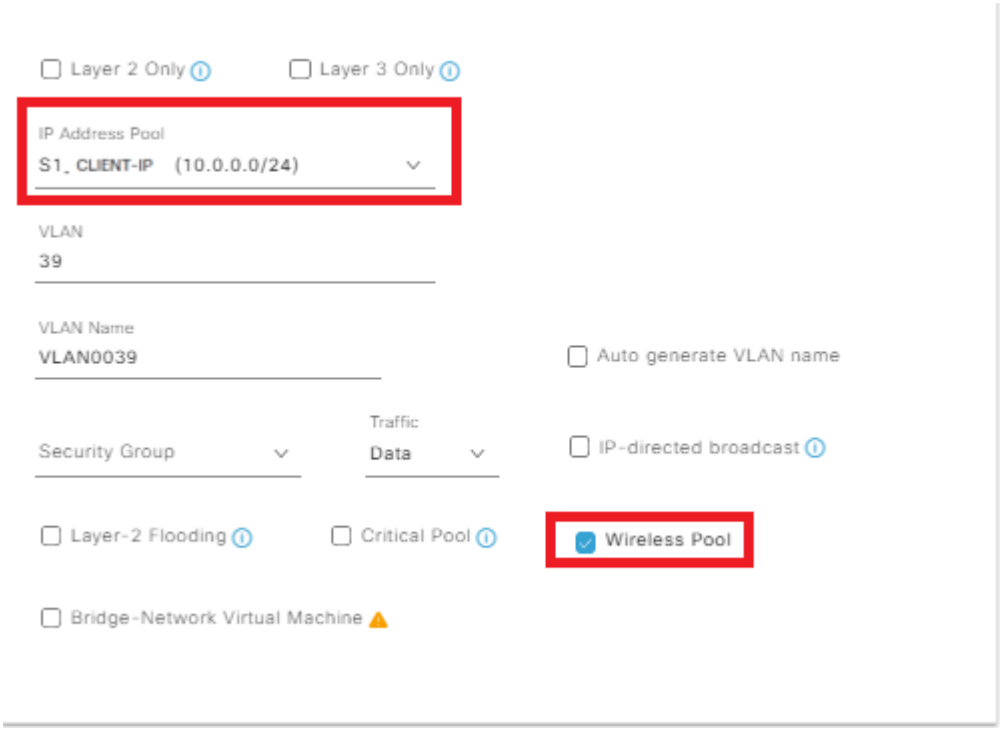
Etapa 6. Navegue até Configuration > Wireless > Access Points. Selecione um AP na lista. Verifique se Fabric Status está Enabled, o endereço IP do plano de controle e o nome do plano de controle:



Verificar o status da malha do AP

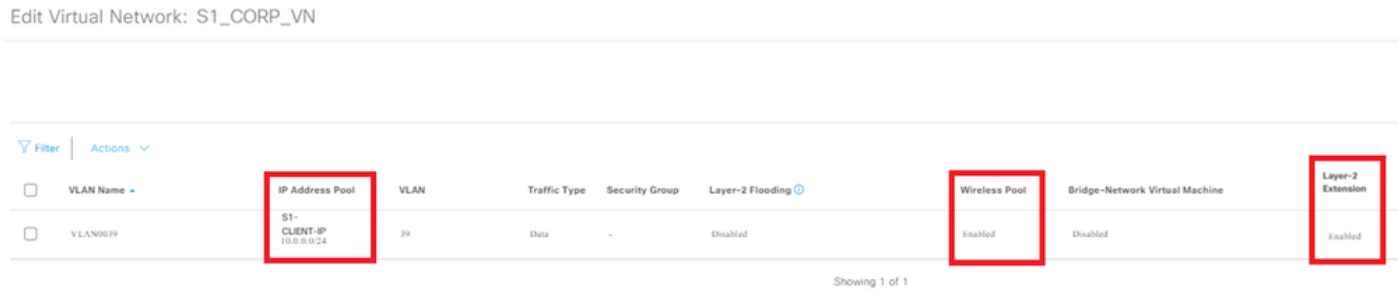
Cliente integrado

Etapa 1. Adicione o pool à Rede Virtual e verifique se a alternância de Extensão da Camada 2 está LIGADA para habilitar a extensão de sub-rede L2 LISP e da Camada 2 no Pool/sub-rede do cliente. No Cisco DNA 1.3.x, não é possível desativá-lo.



Adicionar Pool de Endereços IP

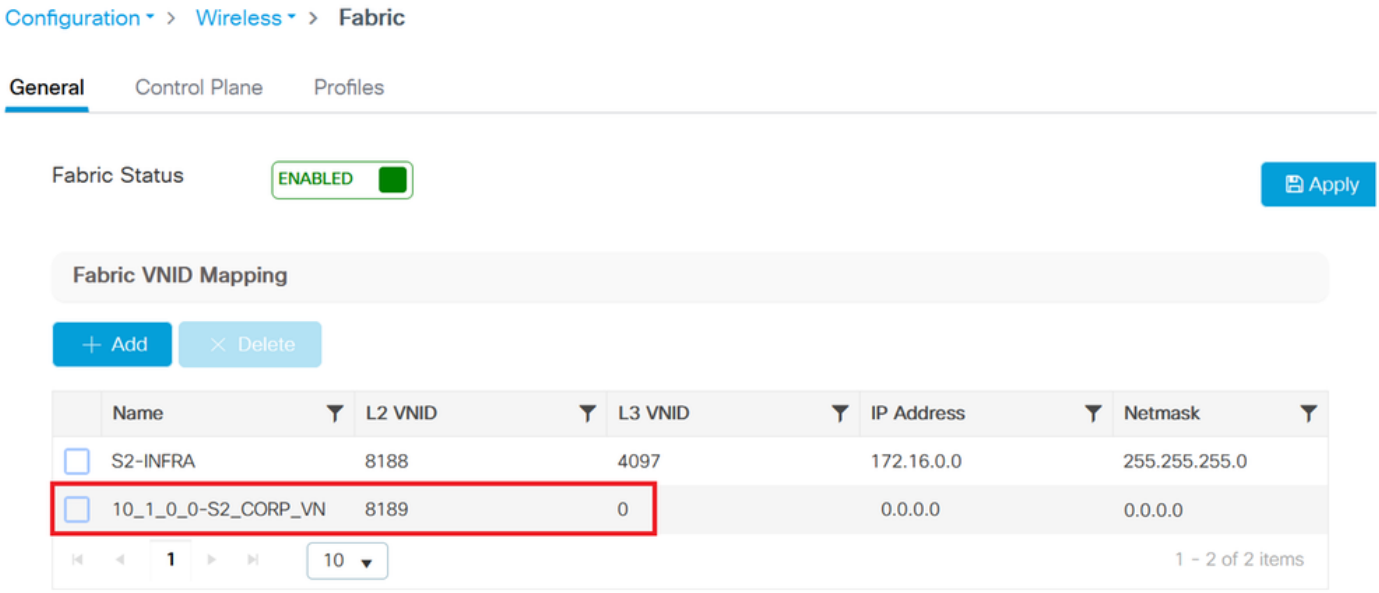
Etapa 2. Verificar se a extensão da camada 2 e o pool de conexões sem fio estão ativados.



Editar rede virtual

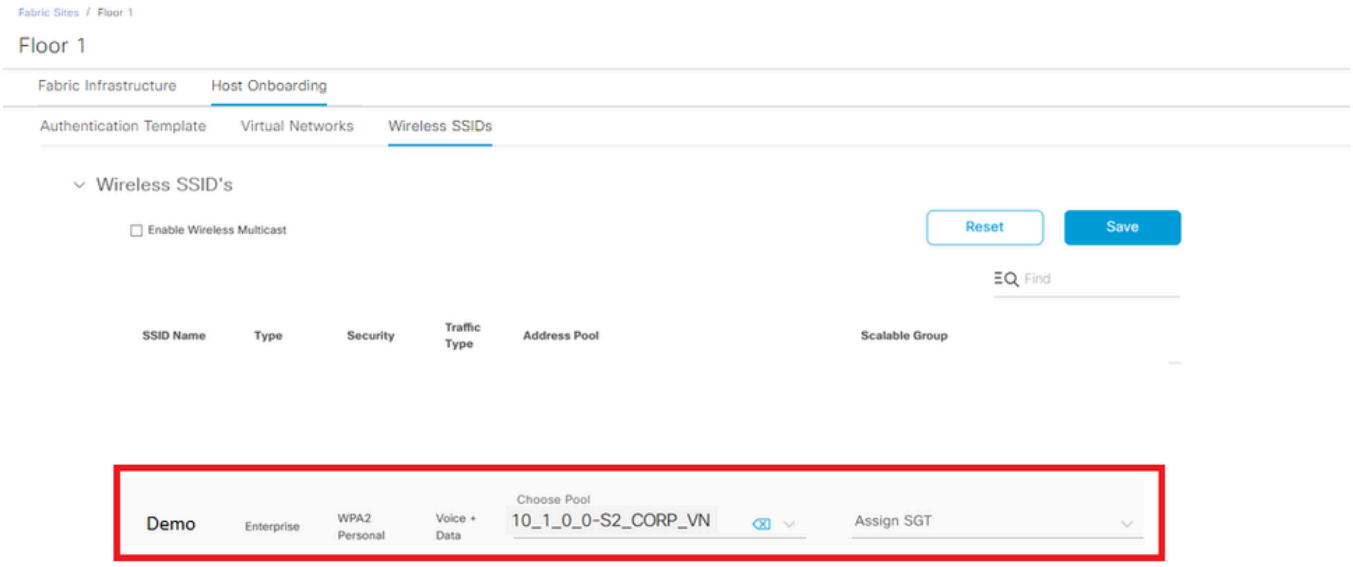
Etapa 3. Na GUI da WLC, navegue para Configuration > Wireless > Fabric > General. Adicione um novo cliente e AP VN_ID.

Quando o pool é atribuído à rede virtual, a interface de malha correspondente ao mapeamento VNID é enviada ao controlador. Todos são VNIDs de L2.



Adicionar novo cliente e AP VN_ID

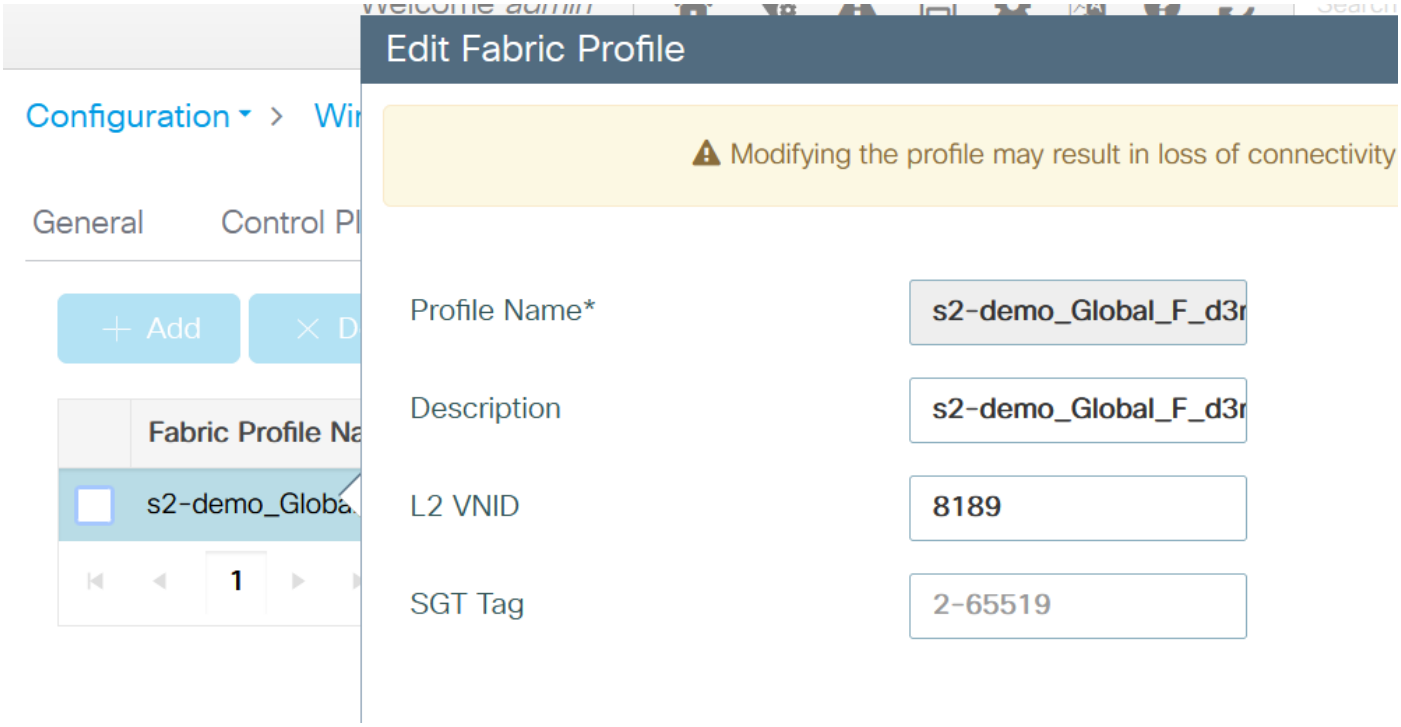
Etapa 4. Os SSIDs são mapeados para o pool nas respectivas redes virtuais:



SSIDs mapeados

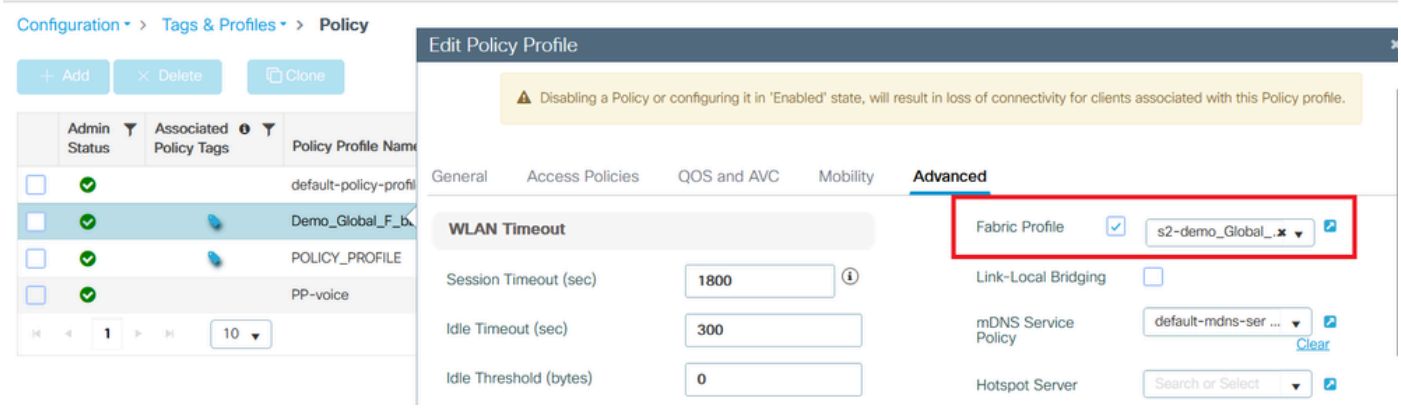
Etapa 5. Um perfil de estrutura com VNID L2 é adicionado ao pool escolhido e o perfil de política é mapeado para o perfil de estrutura, ele é ativado para a estrutura.

Na GUI da WLC, navegue para Configuration > Wireless > Fabric > Profiles.



Perfil de malha

Etapa 6. Navegue até Configuration > Tags & Profiles > Policy. Verifique o perfil de malha mapeado para o perfil de política:



Perfil de malha configurado na política

Verificar

Verificar a configuração da estrutura no WLC e no Cisco DNA

Na CLI da WLC:

WLC1#show tech

WLC1#show tech wireless

Configuração do plano de controle:

router lisp

padrão de tabela de localizador

locator-set WLC

172.16.201.202

exit-locator-set

!

map-server session passive-open WLC

site site_uci

description map-server configurado a partir do Cisco DNA-Center

authentication-key 7 <Key>

CB1-S1#sh lisp session

Sessões para VRF padrão, total: 9, com sede em: 5

Entrada/Saída Ativa/Inativa de Estado de Par

172.16.201.202:4342 Até 3d07h 14/14

Configuração da WLC:

malha sem fio

wireless fabric control-plane default-control-plane

ip address 172.16.2.2 key 0 47aa5a

WLC1#show fabric map-server summary

Status da conexão MS-IP

172.16.1.2 ATIVO

WLC1#show wireless fabric summary

Status da malha: Habilitado

Plano de controle:

Status da chave do endereço IP do nome

---

default-control-plane 172.16.2.2 47aa5a Up

Na GUI da WLC, navegue para Configuration > Wireless > Fabric e verifique se o Fabric Status está Enabled.

Navegue até Configuration > Wireless > Access Points. Selecione um AP na lista. Verifique se o status da estrutura está ativado.

No Cisco DNA, navegue para Provisionar > Sites de malha e verifique se você tem um site de malha. Nesse site de estrutura, navegue até Fabric Infrastructure > Fabric e verifique se a WLC está habilitada como estrutura.

Troubleshooting

O cliente não obtém o endereço IP

Etapa 1. Verifique se o SSID é fabric. Na GUI da WLC, navegue para Configuration > Tags & Profiles > Policy. Selecione a política e navegue até Advanced. Verifique se o Fabric Profile está habilitado.

Etapa 2. Verifique se o cliente está preso no estado de aprendizagem IP. Na GUI da WLC, navegue para Monitoring > Wireless > Clients. Verifique o estado do cliente.

Etapa 3. Verificar se a diretiva é DHCP.

Etapa 4. Se o tráfego for comutado localmente entre AP - nó de borda, colete logs de AP (rastreamento de cliente) para a conexão do cliente. Verifique se a descoberta de DHCP foi encaminhada. Se nenhuma oferta DHCP chegar, algo está errado no nó de borda. Se o DHCP não for encaminhado, algo está errado no AP.

Etapa 5. Você pode coletar um EPC na porta do nó de borda para ver o DHCP descobrir pacotes. Se você não vir os pacotes de descoberta DHCP, o problema está no AP.

SSID não transmitido

Etapa 1. Verificar se os rádios AP estão desligados.

Etapa 2. Verificar se a WLAN está no status e com o SSID de broadcast habilitado.

Etapa 3. Verificar a configuração do AP se o AP estiver ativado para a estrutura. Navegue para Configuration > Wireless > Access Points, selecione um AP e, na guia General, você poderá ver Fabric Status Enabled e as informações de RLOC.

Etapa 4. Navegue até Configuration > Wireless > Fabric > Control Plane. Verifique se o plano de controle está configurado (com o endereço IP).

Etapa 5. Navegue até Configuration > Tags & Profiles > Policy. Selecione a política e navegue até Advanced. Verifique se o Fabric Profile está habilitado.

Etapa 6. Navegue até Cisco DNA e refaça as etapas em Create SSID e Provision WLC. O Cisco DNA deve enviar o SSID para a WLC novamente.

Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.