使用DNA配置软件定义的无线接入

目录

简介

- 要求

SD-Access

- 概述

底层网络和重叠网络

- AP加入
- 板载客户端
- 添加WLC
- 添加接入点
- 创建 SSID
- 调配WLC
- 调配接入点
- 创建交换矩阵站点
- 将WLC添加到交换矩阵
- AP加入
- 客户端未获取IP地址

简介

本文档介绍如何在Cisco Catalyst Center上通过支持交换矩阵的WLC和接入点实施无线SDA。

先决条件

要求

所需的知识包括：

- 9800无线LAN控制器(WLC)配置
- 轻量接入点(LAP)
- 思科DNA

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 9800-CL WLC Cisco IOS® XE，版本17.9.3
- 思科接入点：9130AX、3802E、1832I
- 思科DNA版本2.3.3.7

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

SD-Access

软件定义访问(SD-Access)通过使用动态规则和自动分段在整个网络中自动实施安全策略。

SD-Access为每个连接的终端建立初始信任级别，并持续监控终端以重新验证该信任。

如果终端行为异常或检测到威胁，管理员可以立即遏制该终端并在漏洞发生之前采取行动。这样可以降低业务风险并保护资源。

SD-Access已集成，可在新网络和现有网络中部署。

SD-Access是思科的一项技术，是传统园区网络的演进，通过使用软件定义网络(SDN)组件提供基于意图的网络(IBN)和中央策略控制。

SD-Access的三个以网络为中心的支柱：

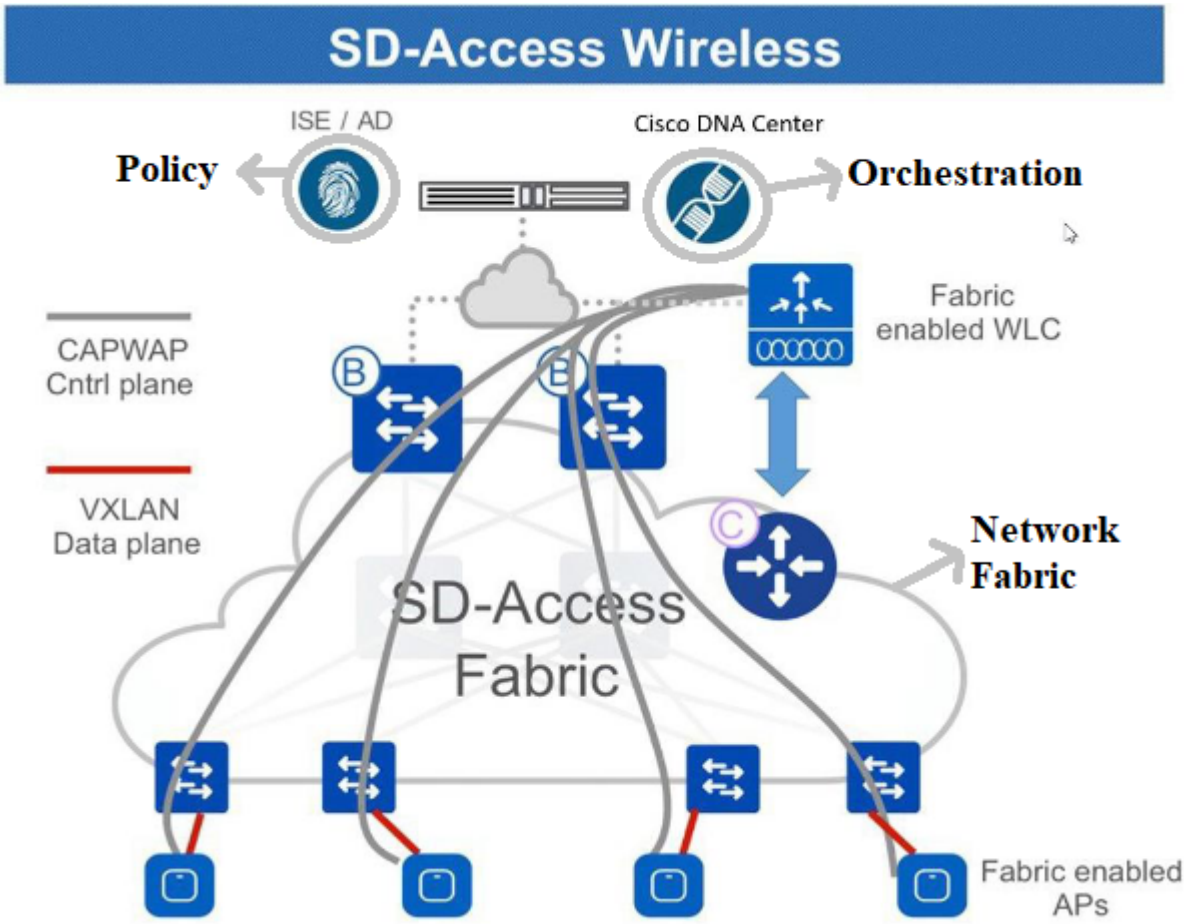
1. 网络交换矩阵：它是网络本身的抽象，支持可编程的重叠和虚拟化。网络交换矩阵同时支持有线和无线访问，允许它托管多个逻辑网络，这些网络彼此分割并根据业务意图进行定义。
2. 协调：思科DNA是SDA的协调引擎。Cisco DNA的功能类似于SDN控制器。它在交换矩阵中实施策略和配置更改。还集成了支持网络设计、支持通过思科DNA保证进行实时网络遥测操作和性能分析的工具。思科DNA的作用是协调网络交换矩阵，为安全性、服务质量(QoS)和微分段提供策略更改和网络意图。
3. Policy（策略）：身份服务引擎(ISE)是定义网络策略的工具。ISE组织如何将设备和节点分割为虚拟网络。ISE还定义访问设备在进入交换矩阵时用于划分用户流量的可扩展组标记(SGT)。SGR负责实施ISE定义的微分段策略。

SDA建立在集中协调的基础上。思科DNA作为可编程协调引擎、ISE作为策略引擎，以及新一代可编程交换机的组合，使其成为比以往任何产品都更灵活、更易于管理的交换矩阵系统。



注意：本文档专门介绍SD-Access无线。

网络交换矩阵由以下元素组成：



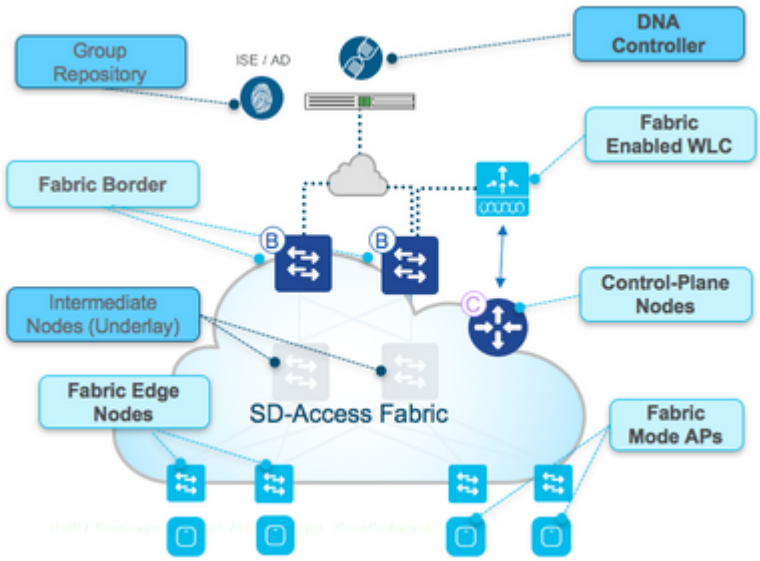
网络交换矩阵元素

网络交换矩阵元素

与交换矩阵的无线集成可为无线网络带来多种优势，例如：跨物理位置实现简化、扩展子网移动性；以及微分段，采用在有线和无线域上一致的集中策略。它还使控制器能够剥离数据平面以转发职责，同时继续充当无线网络的集中服务和控制平面。因此，无线控制器的可扩展性实际上得到了提高，因为它不再需要像FlexConnect模型那样处理数据平面流量。

SD访问无线架构

概述

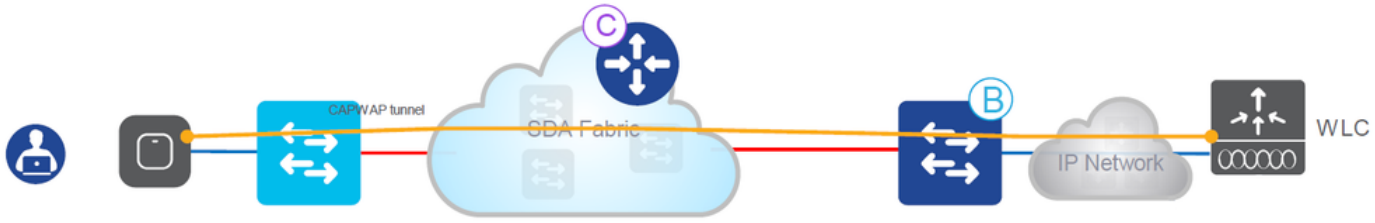


SDA概述

SDA概述

支持两种主要SDA的无线部署模式：

一种是机顶盒设备(OTT)方法，即连接交换矩阵有线网络顶部的传统CAPWAP部署。SDA交换矩阵将CAPWAP控制和数据平面流量传输到无线控制器：

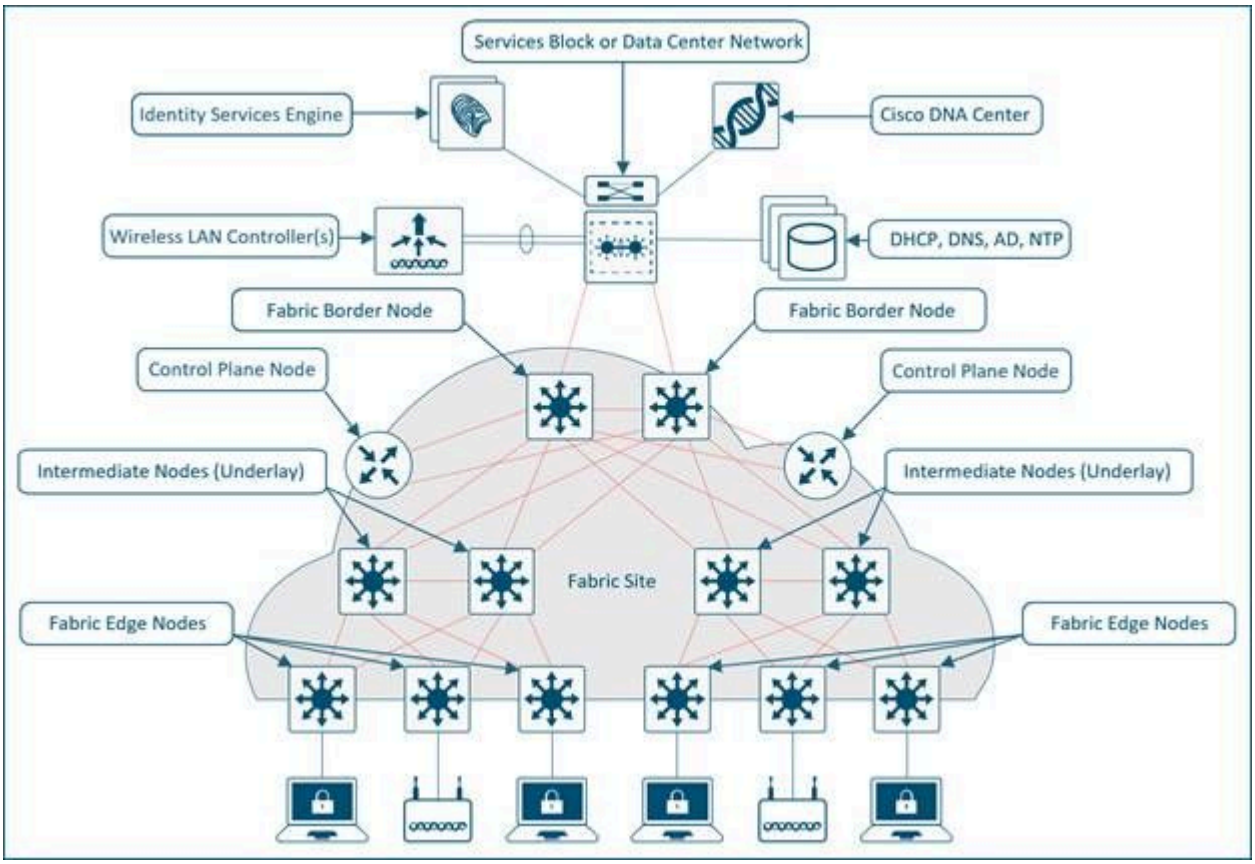


Over-The-Top方法

Over-The-Top方法

在此部署模式中，SDA交换矩阵是无线流量的传输网络（通常在迁移中部署）。 AP的工作方式与经典本地模式非常相似：capwap控制平面和数据平面都终止在控制器上，这意味着控制器不会直接参与交换矩阵。当有线交换机首次迁移到SDA交换矩阵，但无线网络尚未准备好完全交换矩阵重叠集成时，通常使用此模式。

其他部署模式为完全集成的SDA模式。无线网络完全集成到交换矩阵并参与重叠，它允许不同的WLAN成为不同虚拟网络(VN)的一部分。 无线控制器仅管理CAPWAP控制平面（用于管理AP），并且CAPWAP数据平面不会进入控制器：



完全集成的SDA模型

完全集成的SDA模型

无线数据平面的处理方式与有线交换机类似 — 每个AP将数据封装在VXLAN中并将其发送到交换矩阵边缘节点，然后通过该交换矩阵将数据发送到另一个边缘节点。无线控制器必须配置为交换矩阵控制器，这是对其正常运行的修改。

支持交换矩阵的控制器与交换矩阵控制平面通信，它注册第2层客户端MAC地址和第2层虚拟网络标识符(VNI)信息。AP负责与无线终端进行通信，并通过封装和解封流量来协助VXLAN数据平面。

SDA角色和术语

网络交换矩阵由以下元素组成：

- 控制平面节点：这是位置映射系统（主机数据库），是位置分隔协议(LISP)控制平面的一部分，用于管理终端身份(EID)到位置关系（或设备关系）。 控制平面可以是提供控制平面功能的专用路由器，也可以与其他交换矩阵网络元素共存。

- 交换矩阵边界节点：通常是在外部网络和SDA交换矩阵之间的边界工作的路由器，为交换矩阵中的虚拟网络提供路由服务。它将外部第3层网络连接到SDA交换矩阵。

- 交换矩阵边缘节点：交换矩阵内用于将非交换矩阵设备（例如交换机、AP和路由器）连接到SDA交换矩阵的设备。这些节点通过虚拟可扩展局域网(VXLAN)创建虚拟重叠隧道和VN，并将SGT应用于交换矩阵绑定的流量。交换矩阵边缘两侧的网络位于SDA网络内部。它们将有线终端连接到SD-Access交换矩阵。

- 中间节点：这些节点位于SDA交换矩阵的核心内，并连接到边缘或边界节点。中间节点只需将SDA流量作为IP数据包转发，而不知道有多个虚拟网络参与。

- 交换矩阵WLC:已启用交换矩阵并参与SDA控制平面但不处理CAPWAP数据平面的无线控制器。

- 交换矩阵模式AP:支持交换矩阵的接入点。无线流量在AP上采用VXLAN封装，因此可以通过边缘节点将其发送到交换矩阵。

- 思科DNA(DNAC):用于软件定义接入(SDA)交换矩阵重叠网络的企业SDN控制器，负责自动化和保证任务。它还可以用于构成底层网络设备的某些自动化和相关任务（即与SDA无关）。

- ISE:身份服务引擎(ISE)是一个增强型策略平台，可以服务于各种角色和功能，尤其是身份验证、授权和记帐(AAA)服务器。ISE通常与Active Directory(AD)进行交互，但用户可以在本地配置，也可以在ISE自身上进行配置，以实现更小的部署。

```
None
```

注意：控制平面是SDA架构的关键基础设施部分，因此建议以可恢复的方式部署。

底层网络和重叠网络

SDA架构采用交换矩阵技术，支持在物理网络（底层网络）上运行的可编程虚拟网络（重叠网络）。

交换矩阵是重叠。

重叠网络是一种逻辑拓扑，用于虚拟连接设备，构建于任意物理底层拓扑之上。它使用备用转发属性来提供基础未提供的其他服务。它在底层上创建，用于创建一个或多个虚拟化和分段网络。由于重叠由软件定义，因此能够以非常灵活的方式连接它们而不受物理连接的限制。这是实施安全策略的简单方法，因为重叠可以可编程为具有单个物理出口点（交换矩阵边界节点），并且可以使用一个防火墙来保护其后的网络（无论这些网络是否可以定位）。 重叠使用VXLAN封装流量。

VXLAN封装整个第2层帧以便在底层传输，每个重叠网络由VXLAN网络标识符(VNI)标识。 重叠交换矩阵往往比较复杂，在部署的新虚拟网络或实施安全策略时，需要大量的管理员开销。

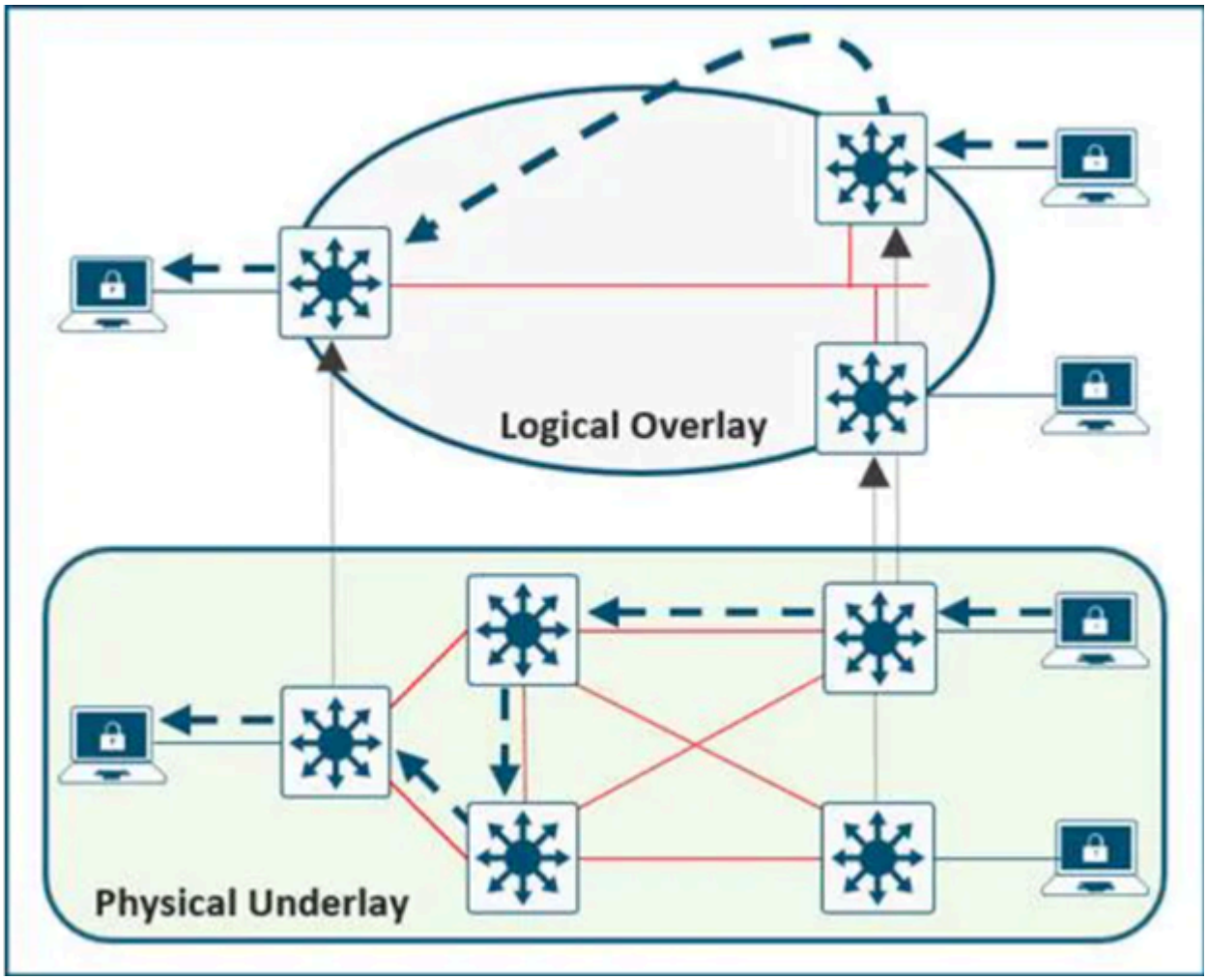
网络重叠示例：

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

底层网络由用于部署SDA网络的物理节点（如交换机、路由器和无线AP）定义。底层的所有网络元素都必须使用路由协议建立IP连接。虽然底层网络不太可能使用传统的接入、分布以及核心模式，但是它必须使用设计良好的第3层基础，以提供强大的性能、可扩展性和高可用性。

```
None
```

注意：SDA在底层网络中支持IPv4，在重叠网络中支持IPv4和/或IPv6。

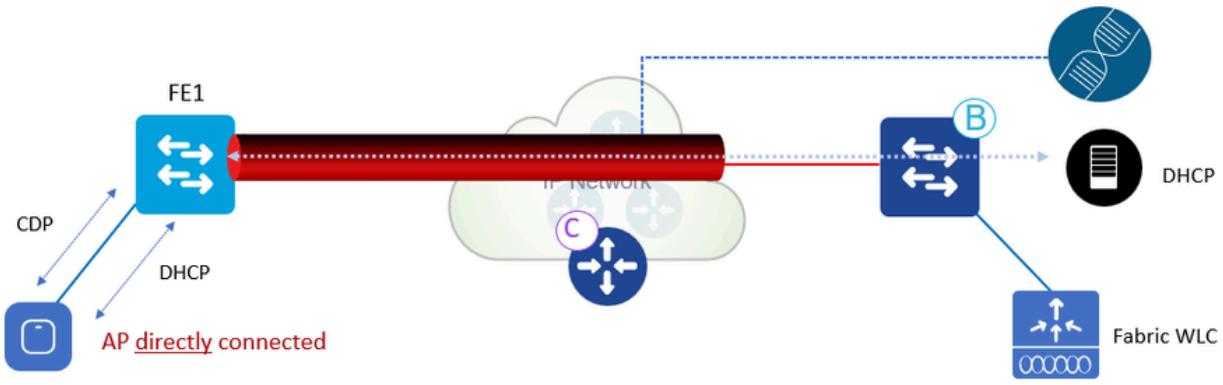


底层网络和重叠网络

底层网络和重叠网络

基本工作流程

AP加入



AP加入工作流

AP加入工作流：

1.管理员在INFRA_VN的Catalyst Center中配置AP池。思科DNA在所有交换矩阵边缘节点上预调配配置以自动板载AP。

2. AP已插入并通电。交换矩阵边缘通过CDP发现它是AP，并应用宏将交换机端口分配到正确的VLAN（或接口模板）。

3. AP通过DHCP在重叠中获取IP地址。

4.交换矩阵边缘注册AP IP地址和MAC(EID)并更新控制平面(CP)。

5. AP使用传统方法学习WLC的IP。交换矩阵AP作为本地模式AP加入。

6. WLC检查它是否支持交换矩阵（第2波或第1波AP）。

7.如果交换矩阵支持AP，WLC将查询CP以了解AP是否连接到交换矩阵。

8.控制平面(CP)使用RLOC回复WLC。这意味着AP已连接到交换矩阵，并且显示为“交换矩阵已启用”。

9. WLC为CP中的AP执行L2 LISP注册（即AP“特殊”安全客户端注册）。 这用于将重要的元数据信息从WLC传递到交换矩阵边缘。

10.响应此代理注册，控制平面(CP)通知交换矩阵边缘并传递从WLC接收的元数据（表示它是AP且来自AP子网的IP地址的标志）。

11.交换矩阵边缘处理该信息，它获知其为AP并创建到指定IP的VXLAN隧道接口(优化：交换机侧已准备好客户端加入)。

debug/show命令可用于验证和验证AP加入工作流程。

控制层面

```
debug lisp control-plane all
```

```
show lisp instance-id <L3 instance id> ipv4 server
```

（必须显示由连接AP的边缘交换机注册的AP IP地址。）

```
show lisp instance-id <L2 instance id> ethernet server
```

(必须显示AP无线电以及以太网MAC地址。AP无线电由WLC注册，以太网MAC地址由连接AP的边缘交换机注册。)

边缘交换机

```
debug access-tunnel all
```

```
debug lisp control-plane all
```

```
show access-tunnel summary
```

```
show lisp instance < L2 instance id> ethernet database wlc access-points
```

（必须在此处显示AP无线电MAC地址。）

WLC

```
show fabric ap summary
```

WLC LISP调试

```
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
```

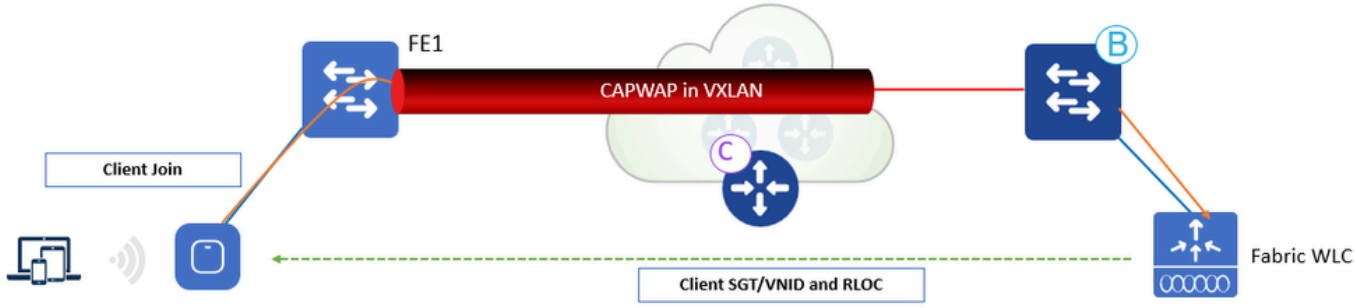
```
set platform software trace wncd chassis active r0 lisp-agent-ha debug
```

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

访问点

```
show ip tunnel fabric
```

板载客户端



客户端板载工作流程

客户端板载工作流程

客户端板载工作流：

1.客户端对支持交换矩阵的WLAN进行身份验证。WLC从ISE获取SGT，更新具有客户端L2VNID的AP和SGT以及RLOC IP。WLC从内部数据库知道AP的RLOC。

2. WLC代理在CP中注册客户端L2信息；这是LISP修改的消息，用于传递其他信息，如客户端SGT。

3.交换矩阵边缘通过CP收到通知，并将L2中的客户端MAC添加到转发表，然后根据客户端SGT从ISE获取策略。

4.客户端发起DHCP请求。

5. AP使用L2 VNI信息将其封装在VXLAN中。

6.交换矩阵边缘将L2 VNID映射到VLAN接口并在重叠中转发DHCP（与有线交换矩阵客户端相同）。

7.客户端从DHCP接收IP地址。

8. DHCP监听（和/或静态ARP）触发交换矩阵边缘向CP注册客户端EID。

debug/show命令可用于验证和验证客户端板载工作流程。

控制层面

debug lisp control-plane all

边缘交换机

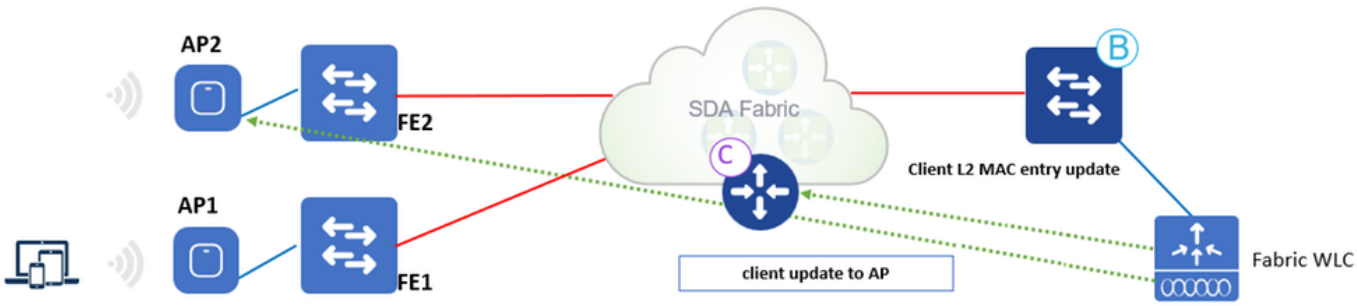
debug lisp control-plane all

```
debug ip dhcp snooping packet/event
```

WLC

对于LISP通信，调试与AP加入相同。

客户端漫游



客户端漫游工作流程

客户端漫游工作流程

客户端漫游工作流程：

1.客户端在FE2上漫游到AP2（交换机间漫游）。WLC通过AP收到通知。

2. WLC使用客户端信息(SGT、RLOC)更新AP上的转发表。

3. WLC使用新的RLOC交换矩阵边缘2更新CP中的第2层MAC条目。

4. CP然后通知：

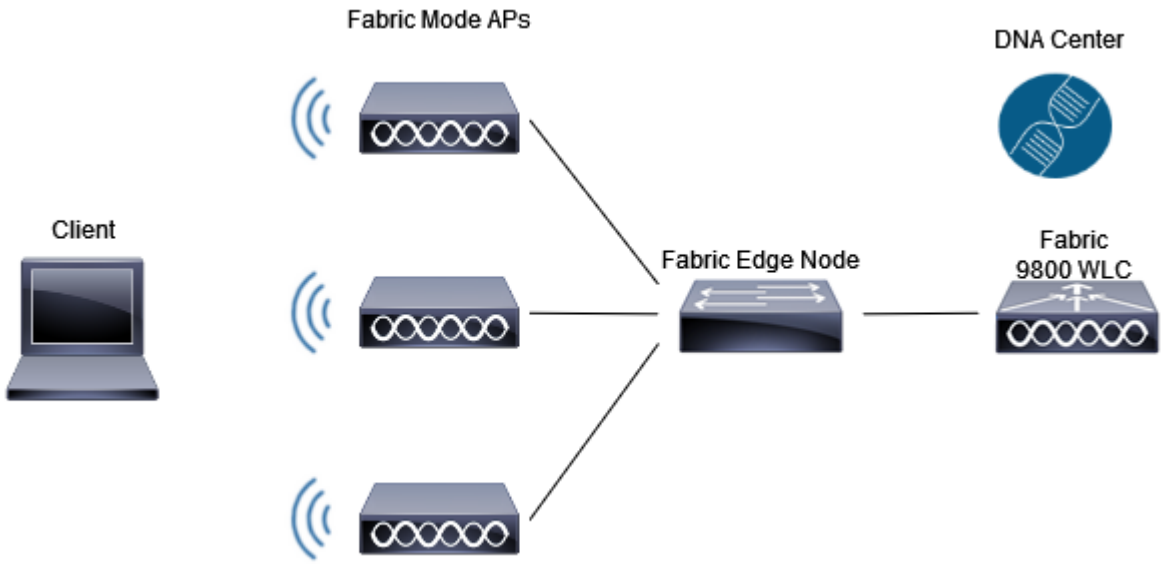
- 交换矩阵边缘FE2（漫游到交换机）将客户端MAC添加到指向VXLAN隧道的转发表。
- 交换矩阵边缘FE1（漫游交换机），用于清理无线客户端。

5.交换矩阵边缘在收到流量后更新CP数据库中的L3条目(IP)。

6.漫游是第2层，因为交换矩阵边缘2具有相同的VLAN接口（任播GW）。

配置

网络图



网络图

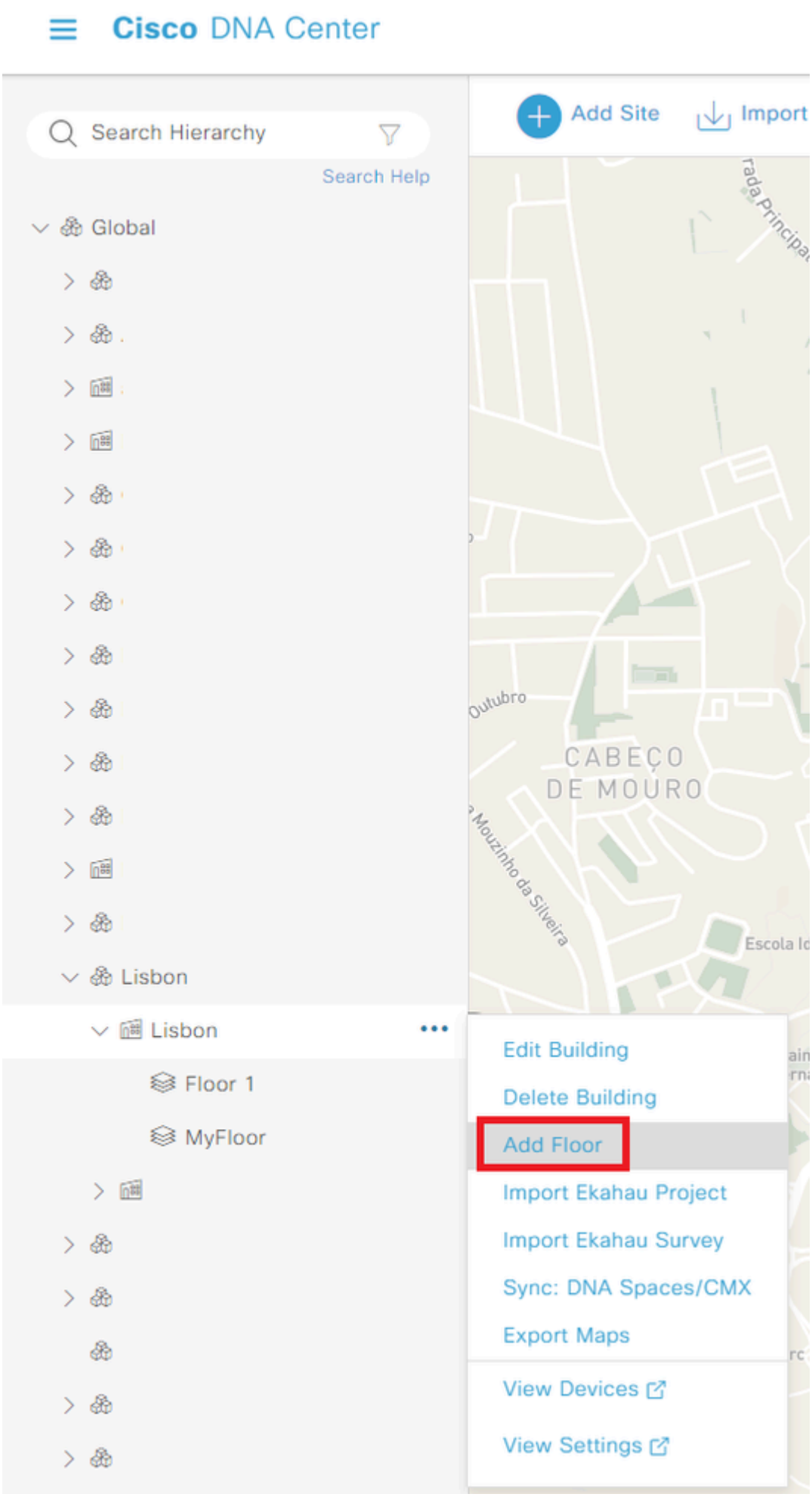
网络图

Cisco Catalyst Center中的WLC发现和调配

添加WLC

步骤1.导航到要添加WLC的位置。您可以添加新的建筑/楼层。

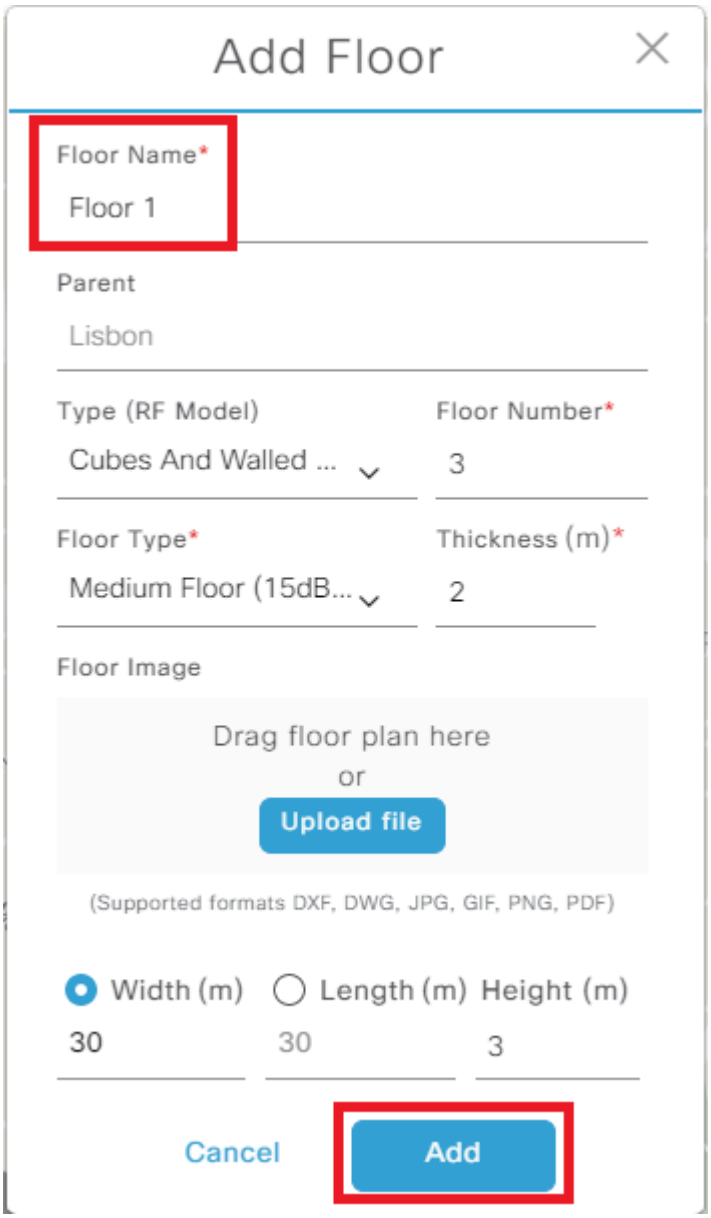
导航到设计>网络层次结构，然后输入建筑/楼层，或创建新楼层，如图所示：


Cisco DNA Center
Search Hierarchy
Search Help
Global
Lisbon
Lisbon
Floor 1
MyFloor
Add Site
Import
CABEÇO
DE MOURO
Edit Building
Delete Building
Add Floor
Import Ekahau Project
Import Ekahau Survey
Sync: DNA Spaces/CMX
Export Maps
View Devices
View Settings

创建新楼层

创建新楼层

步骤2.添加层。您还可以上传楼层工厂的图像。

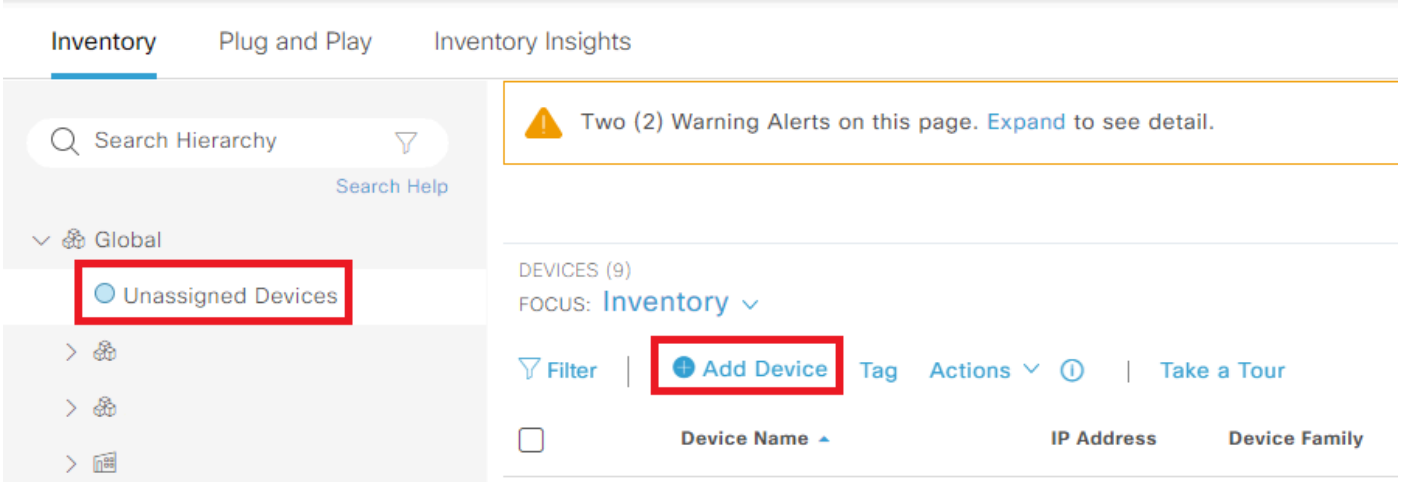


添加新楼层

添加新楼层

第3步：导航到Provision > Inventory，然后使用Add Device添加WLC。向Cisco DNA用于访问WLC的WLC添加用户名/密码。

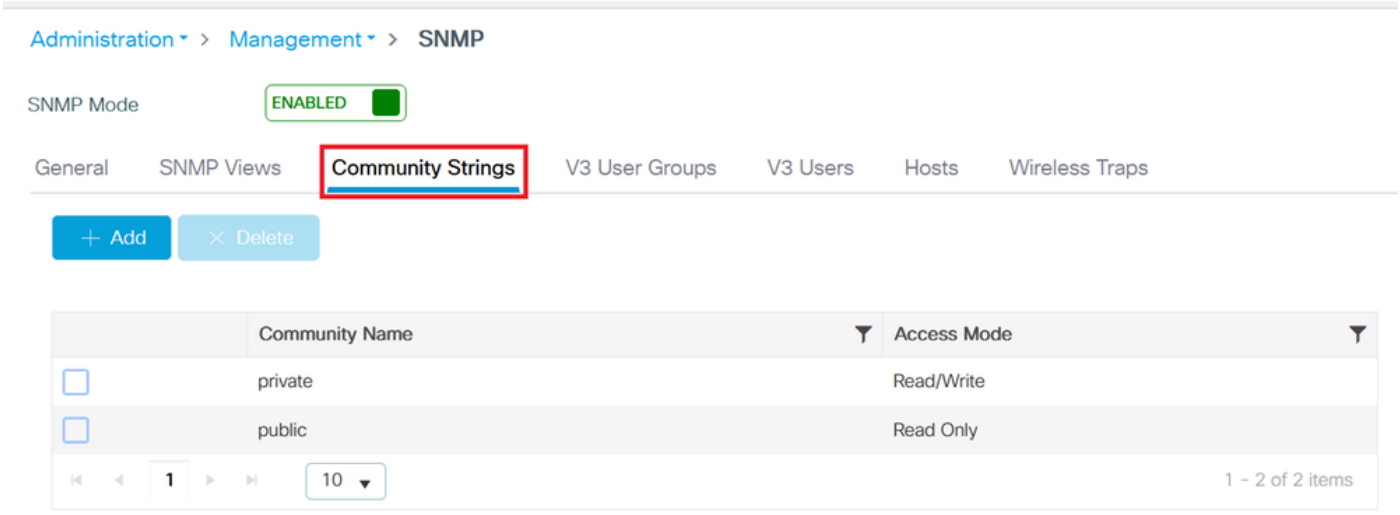
在Add Device对话框中，输入WLC管理IP地址和Cisco Catalyst Center用于登录控制器的CLI凭证。



添加设备

添加设备

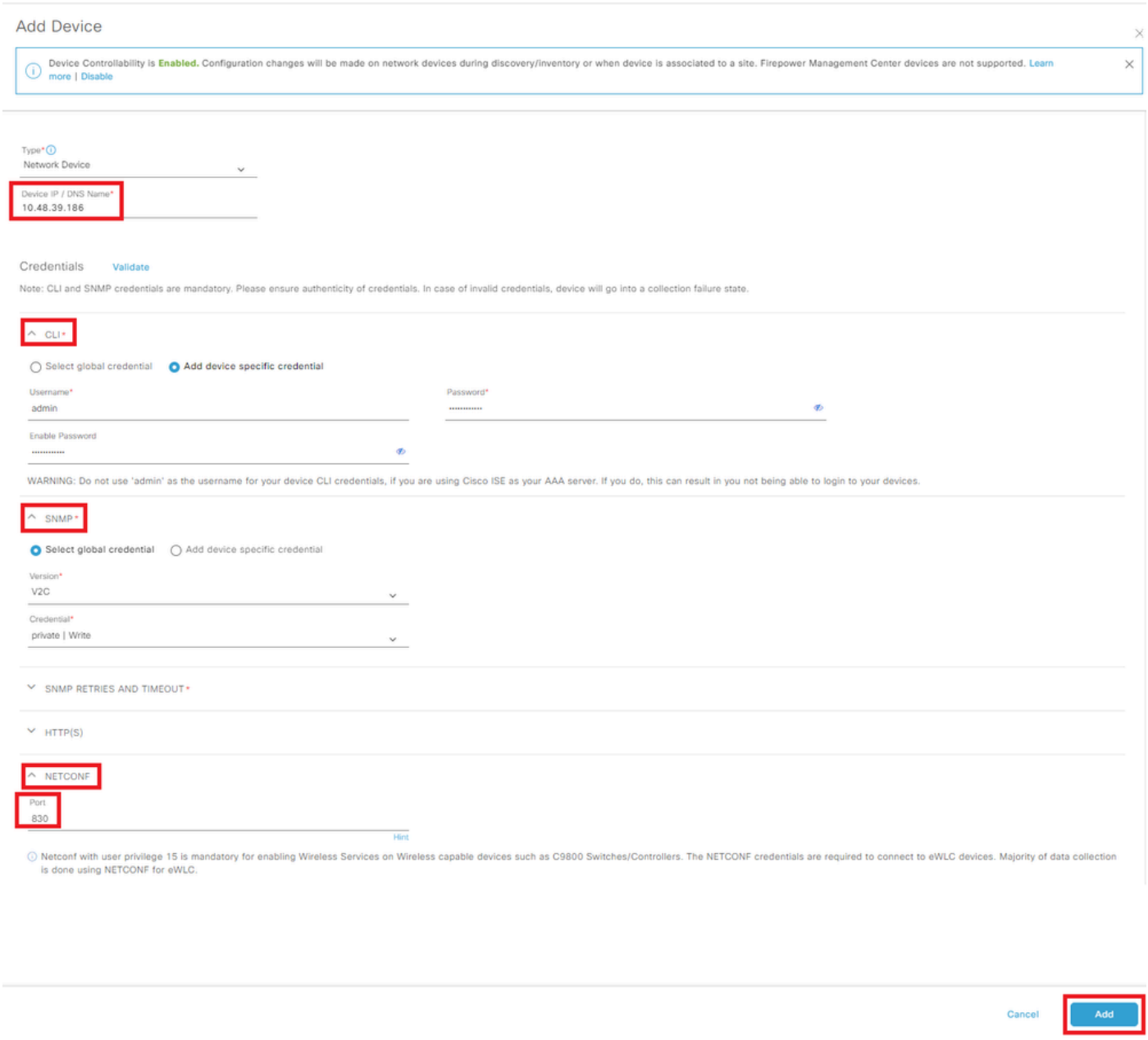
第4步：在WLC GUI上，导航到管理>管理> SNMP >社区字符串，并验证配置的字符串。在Cisco DNA中添加WLC时，添加正确的SNMP社区字符串，并确保在9800 WLC上启用netconf-yang。运行命令show netconf-yang status。最后，单击Add:



SNMP配置

SNMP配置

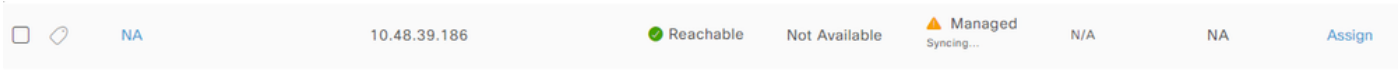
第5步：添加WLC IP地址、CLI凭证（思科DNA用于登录到WLC的凭证，且这些凭证必须在将其添加到思科DNA之前在WLC上配置）、SNMP字符串，并验证是否在端口830上配置了NETCONF端口：



添加WLC

添加WLC

WLC显示为NA，因为思科DNA仍处于同步过程中：



同步进程中的WLC

同步进程中的WLC

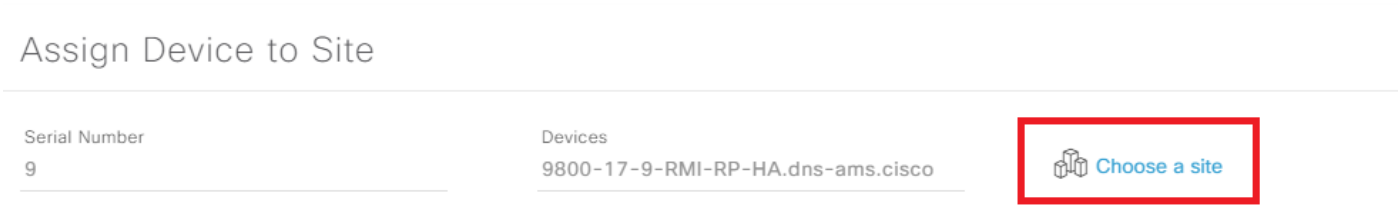
完成同步过程后，您可以看到WLC名称、IP地址（如果可访问）、受管和软件版本：



WLC已同步

WLC已同步

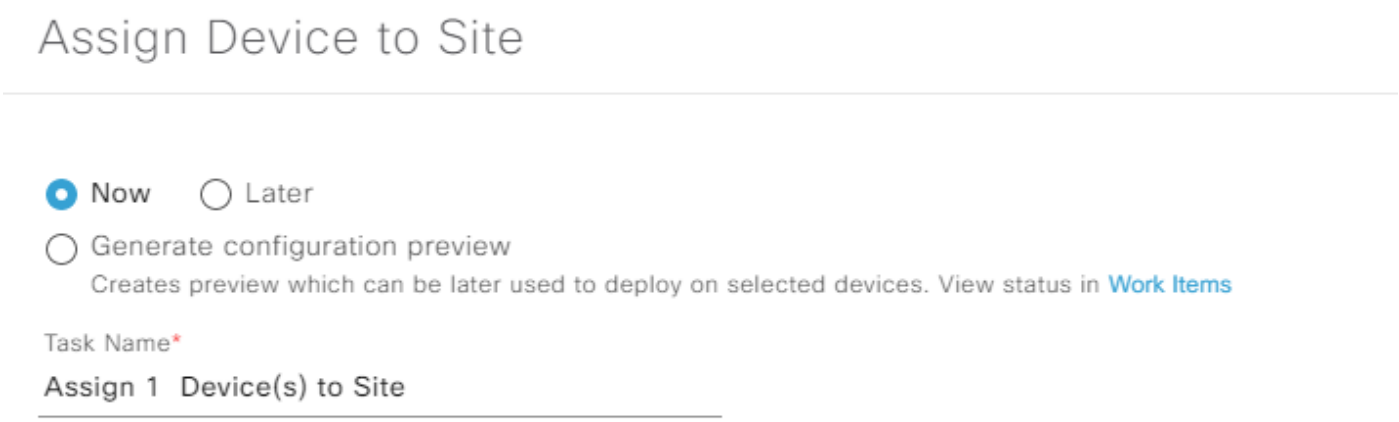
步骤6.将WLC分配到站点。在设备列表中，单击Assign并选择site:



将设备分配到站点

将设备分配到站点

您可以决定现在或以后分配站点：

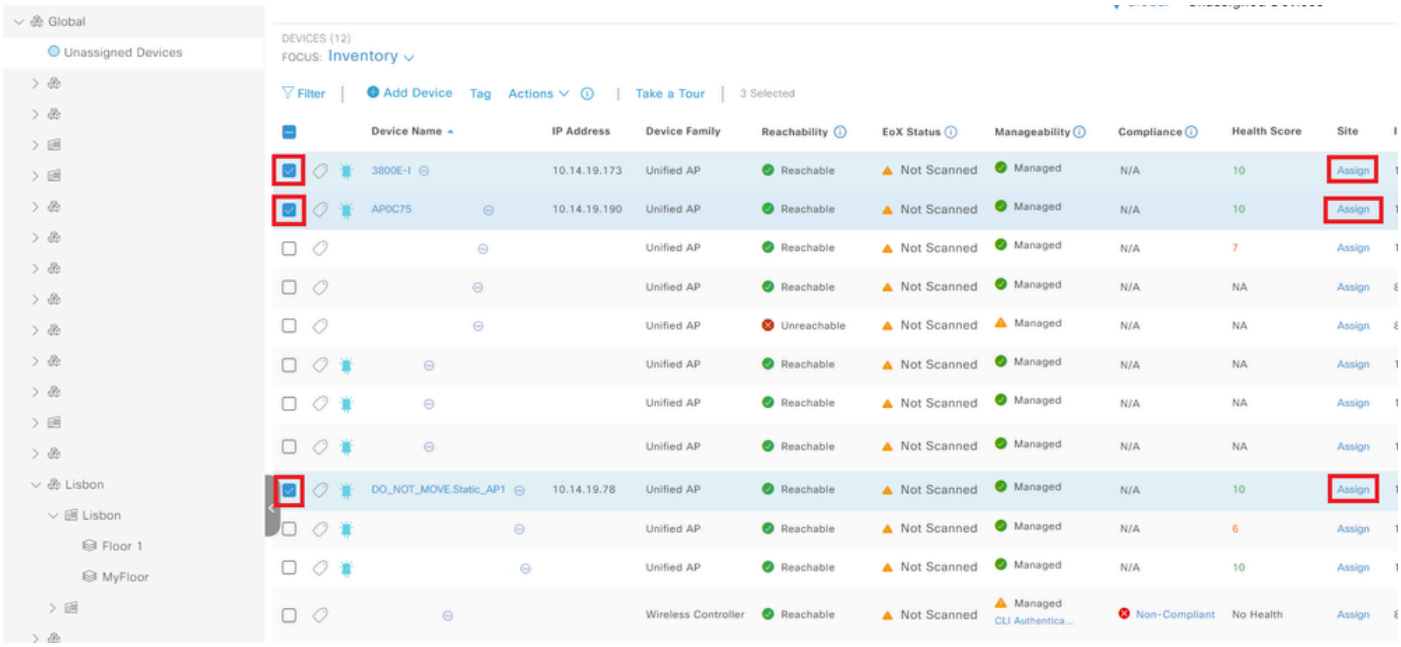


立即或稍后将设备分配到站点

立即或稍后将设备分配到站点

添加接入点

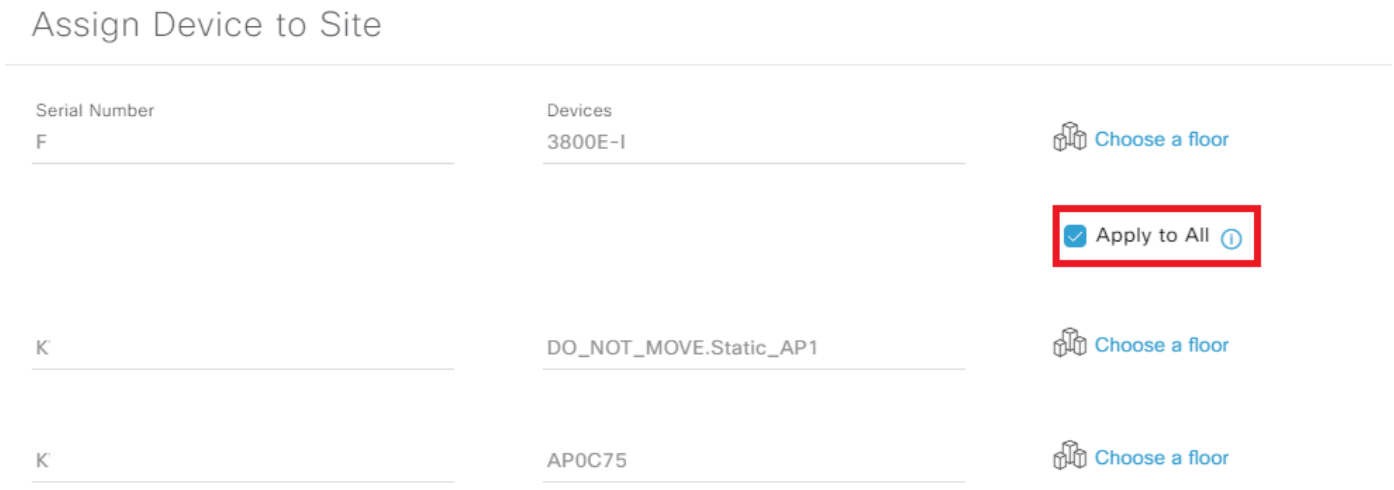
第1步：添加并访问WLC后，导航到调配>库存>全局>未分配设备，并搜索加入到WLC的AP:



添加接入点

添加接入点

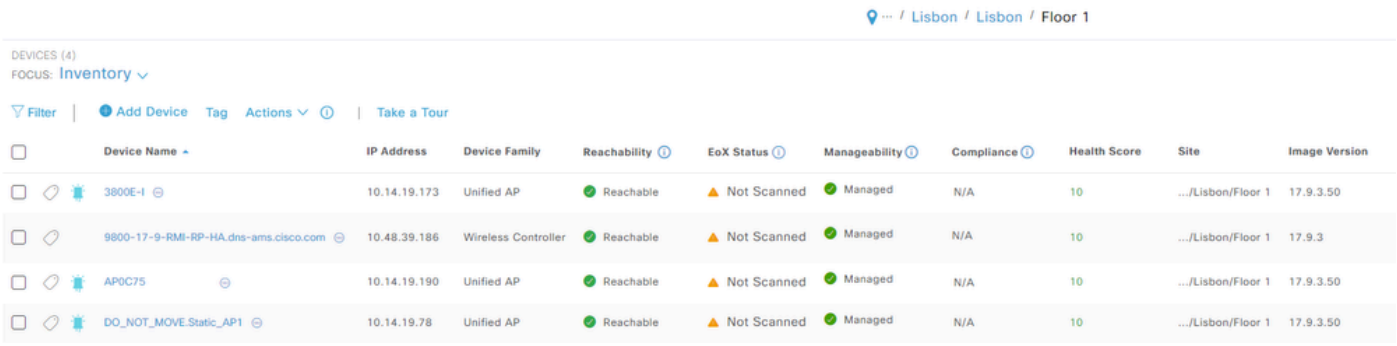
步骤2.单击Assign。选择目标站点。选中Apply to All复选框以将分配应用到多个设备。



将AP分配到站点

将AP分配到站点

导航至楼层，您可以看到分配给楼层的所有设备 — WLC和AP:

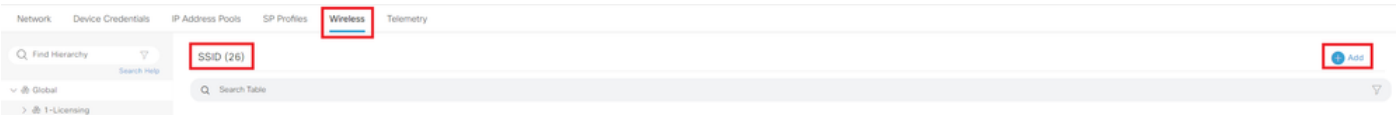


分配给站点的设备

分配给站点的设备

创建 SSID

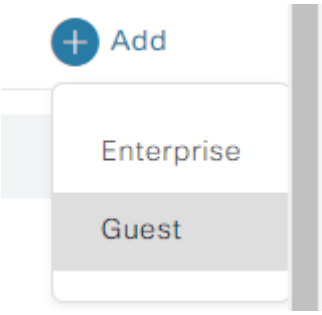
步骤1.导航到Design > Network Settings > Wireless > Global并添加SSID:



创建 SSID

创建 SSID

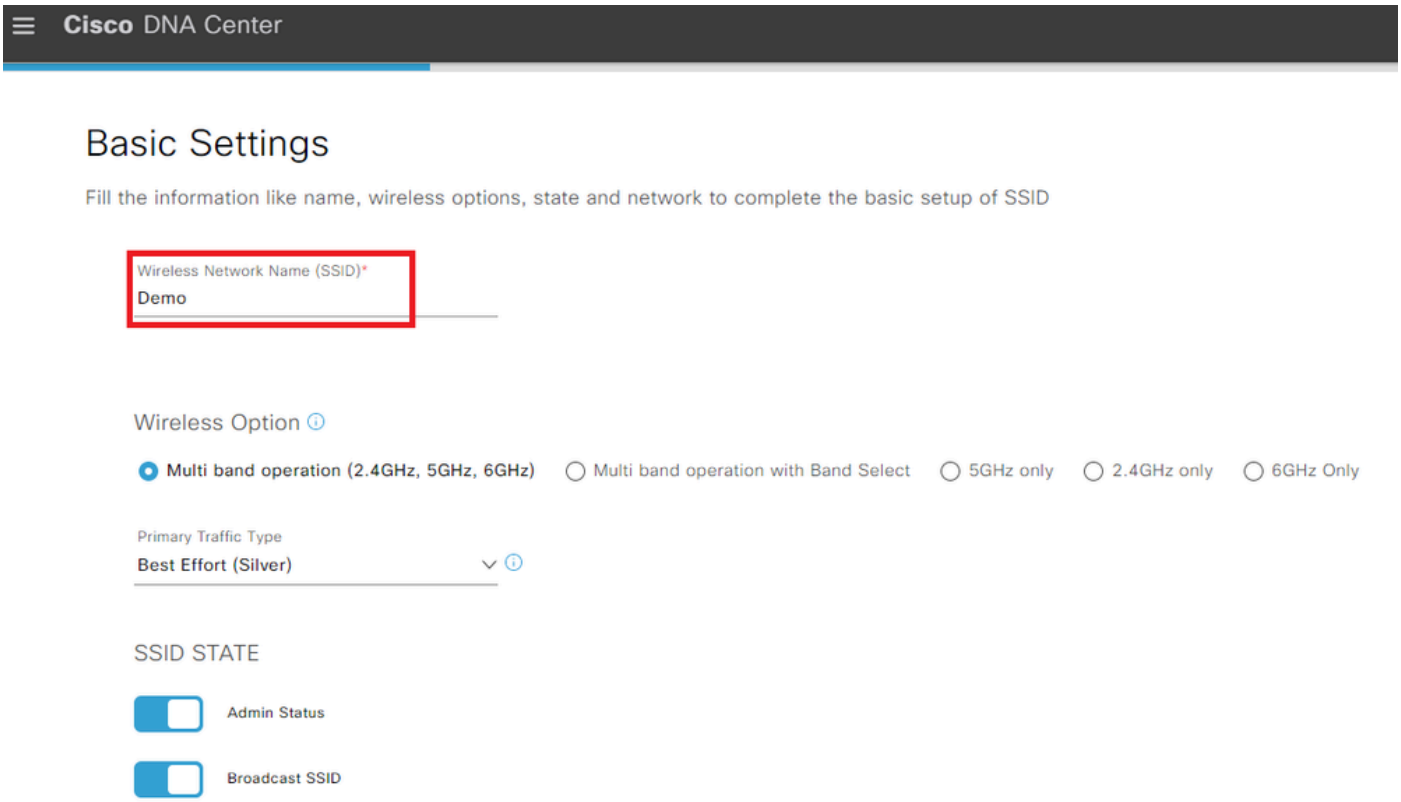
您可以创建Enterprise SSID或Guest SSID。在本演示中，创建访客SSID:



企业或访客SSID

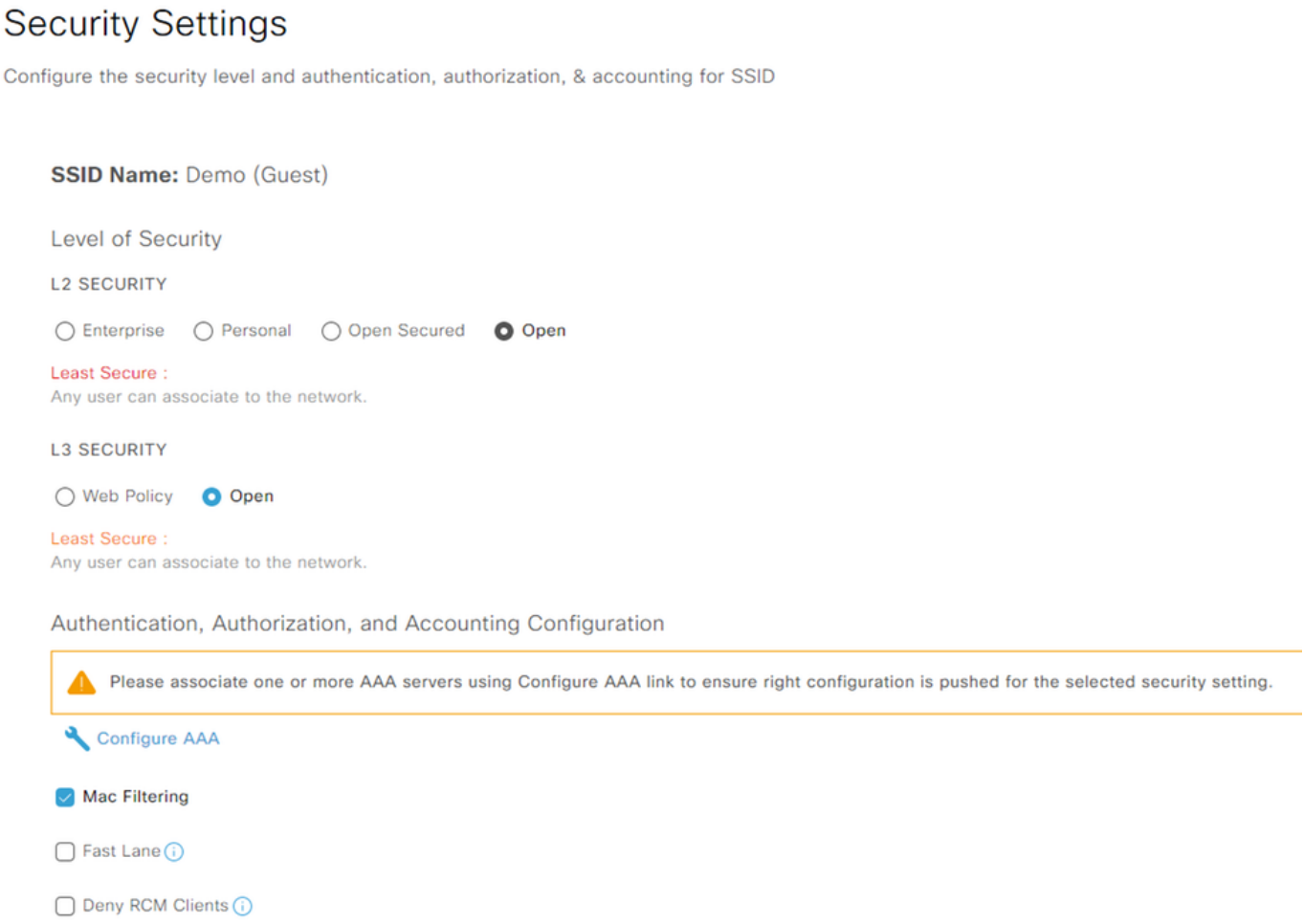
企业或访客SSID

步骤2.选择要的SSID设置。在这种情况下，会创建一个开放式SSID。必须启用管理状态和广播SSID:



SSID基本设置

SSID基本设置

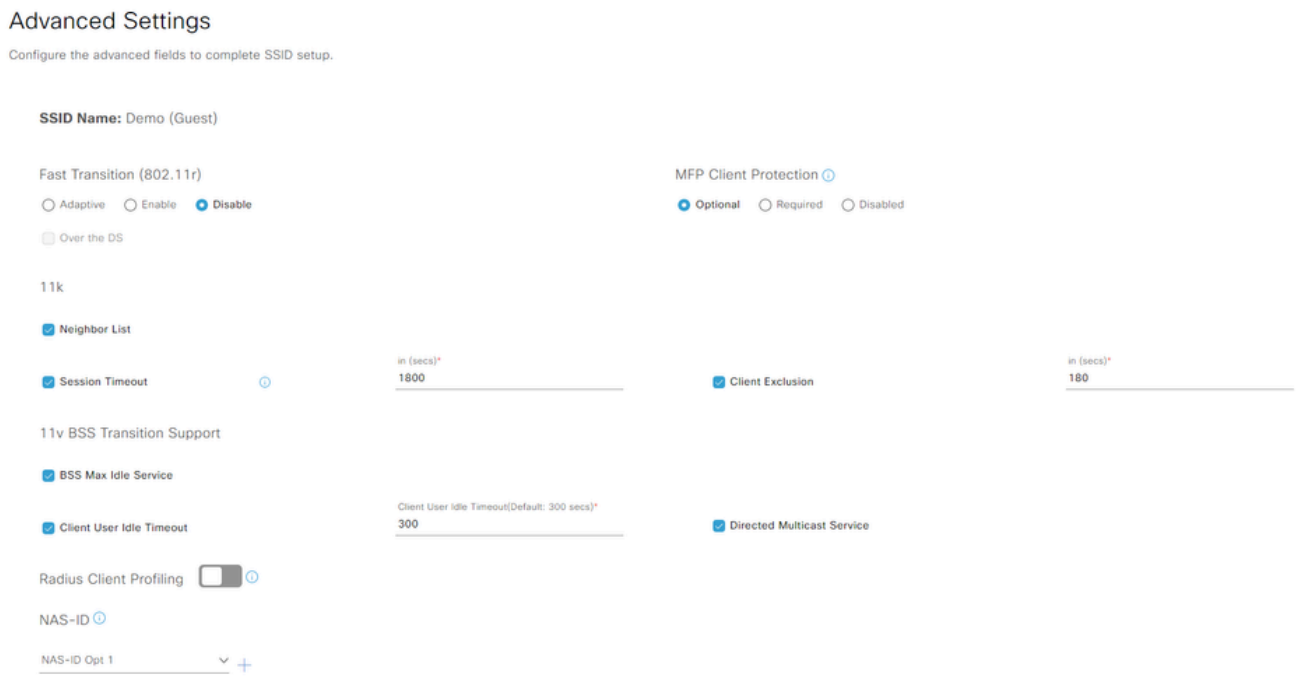


SSID安全设置

SSID安全设置

警告：不要忘记为SSID配置和关联AAA服务器。如果未配置AAA服务器，则映射默认方法列表。

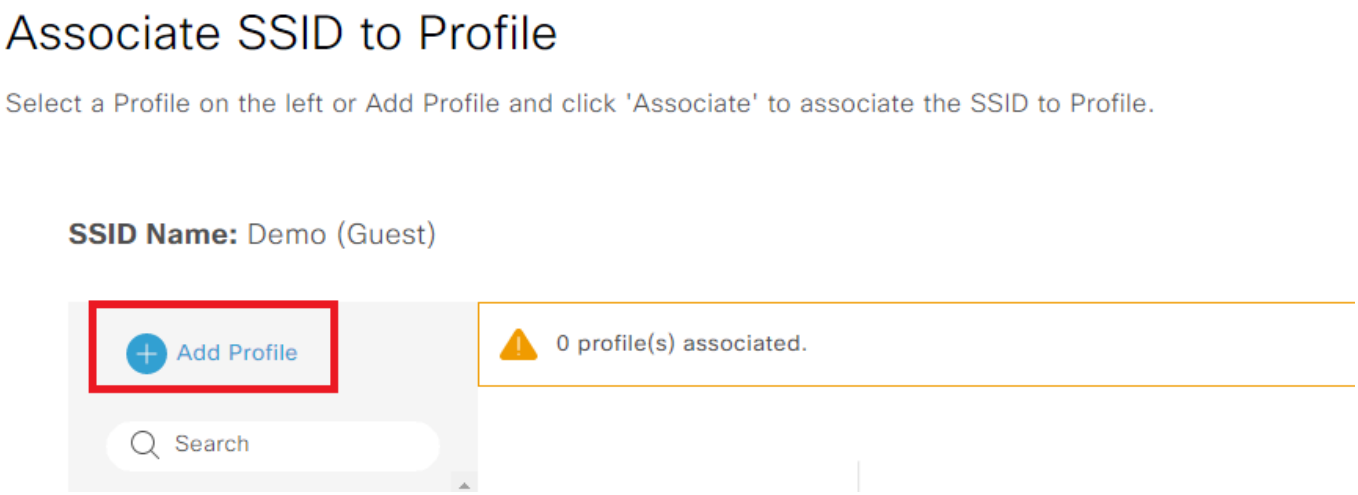
单击next时，您可以看到您的SSID的高级设置：



SSID高级设置

SSID高级设置

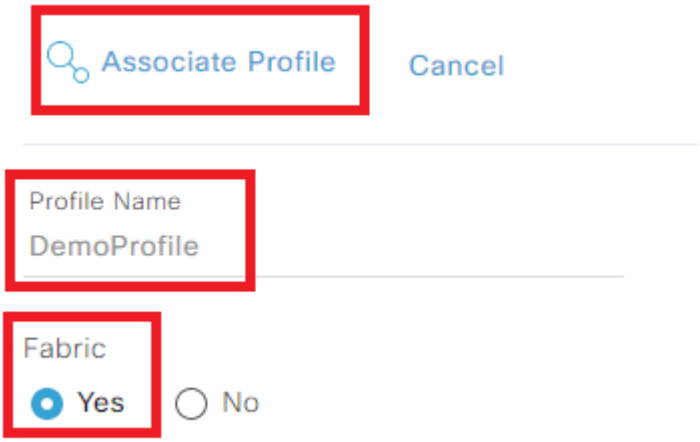
步骤3.创建SSID后，需要将其与配置文件关联。单击Add Profile:



添加配置文件

添加配置文件

第4步：为配置文件命名，选择Fabric，然后点击Associate Profile:



关联配置文件

关联配置文件

系统将显示您创建的SSID和配置文件的摘要：

Summary

Review all changes

Basic Settings Edit

SSID Name	Demo
Primary Traffic Type	Best Effort (Silver)
Admin Status	Yes
Broadcast SSID	Yes

Security Settings Edit

L2 Security	open
L3 Security	open
AAA Servers	
Mac Filtering	Yes
Fast Lane	No
Deny RCM Clients	No
Enable Posture	No
ACL Name	

Advanced Settings Edit

Fast Transition (802.11r)	Disable
Over the DS	No
MFP Client Protection	Optional
Session Timeout	1800
Client Exclusion	180
Radius Client Profiling	No
NAS-ID	

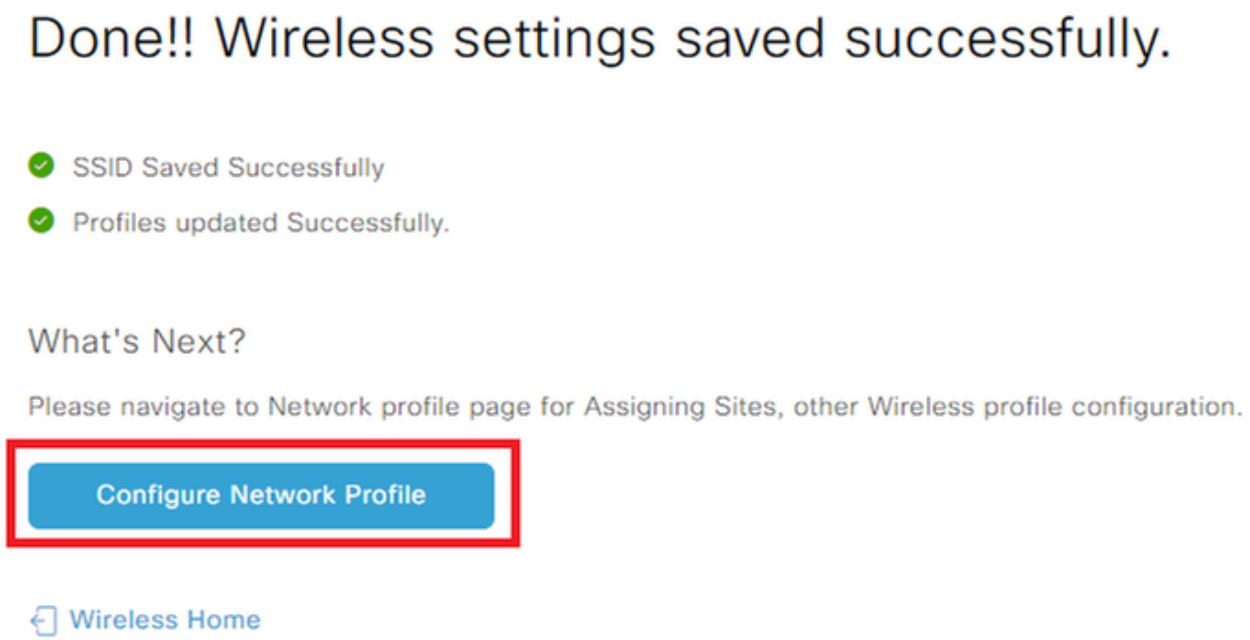
Network Profile Settings Edit

DemoProfile	Fabric (Associated)

SSID摘要

SSID摘要

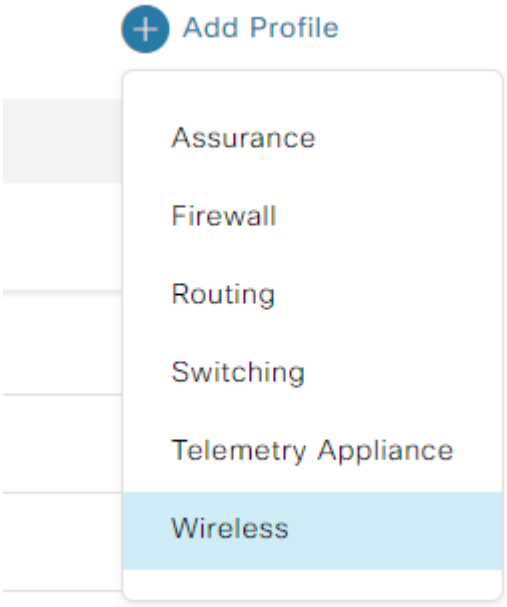
步骤5.配置新的网络配置文件:



配置网络配置文件

配置网络配置文件

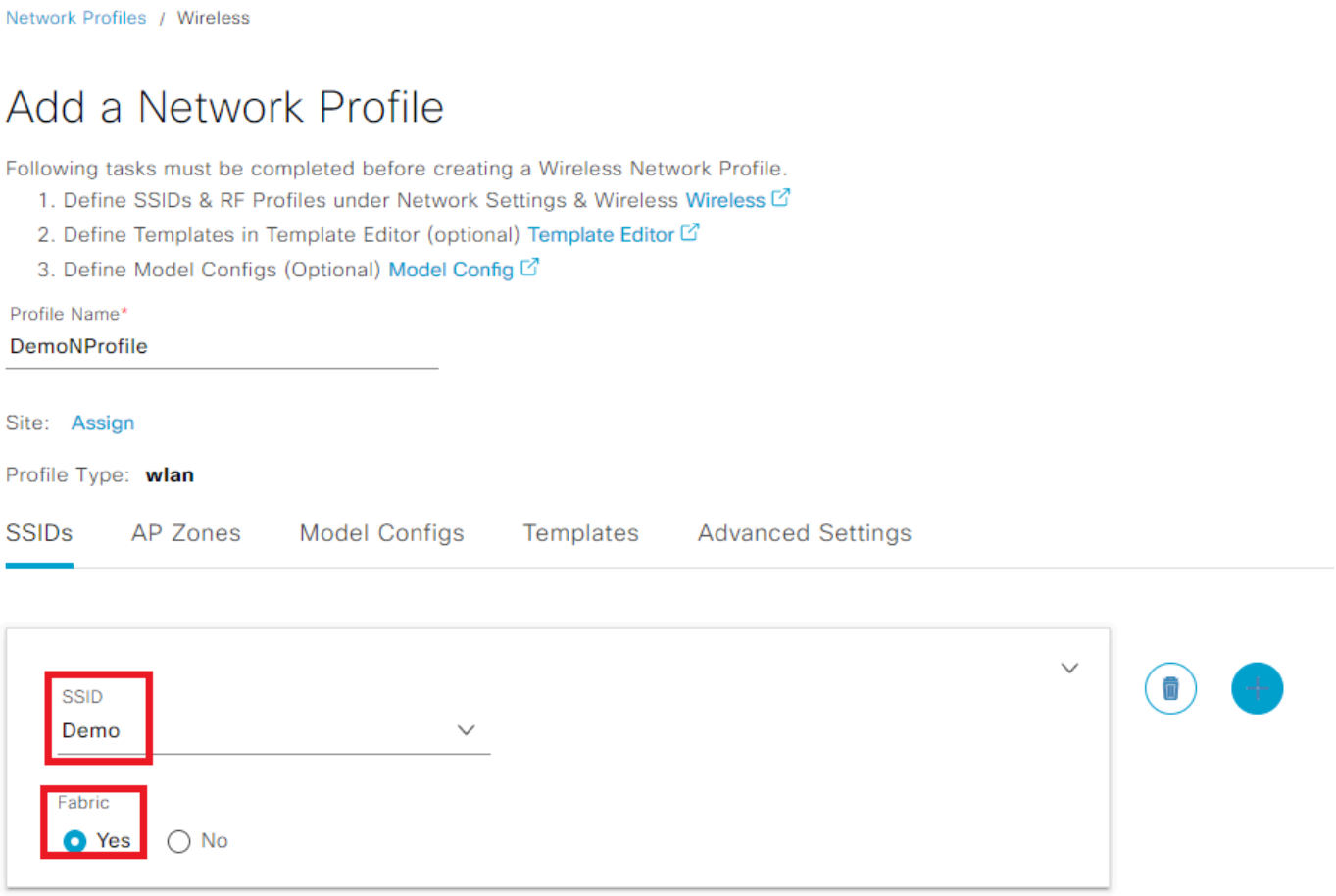
要创建新的网络配置文件而不创建新的SSID，请导航到设计>网络配置文件，选择添加配置文件>无线:



添加无线网络配置文件

添加无线网络配置文件

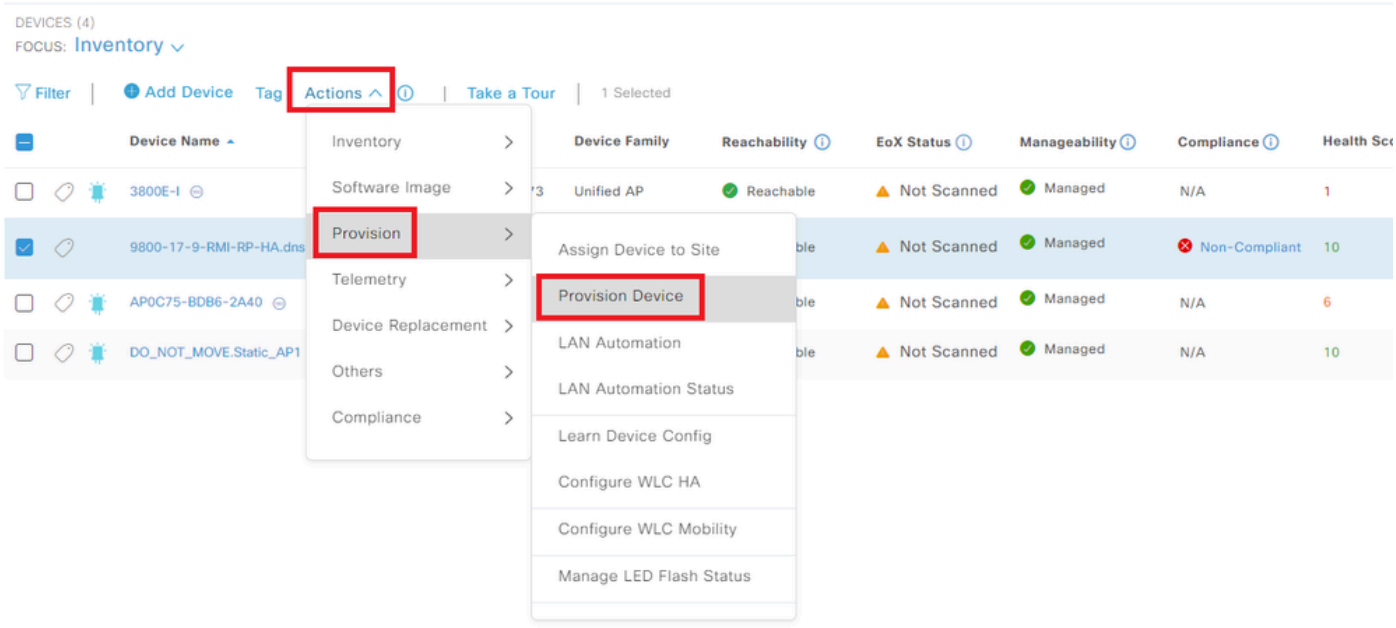
步骤6.创建网络配置文件。为其指定名称并关联SSID:



创建网络配置文件

调配WLC

步骤1.导航到您的建筑/楼层。选择WLC和Actions > Provision > Provision Device:



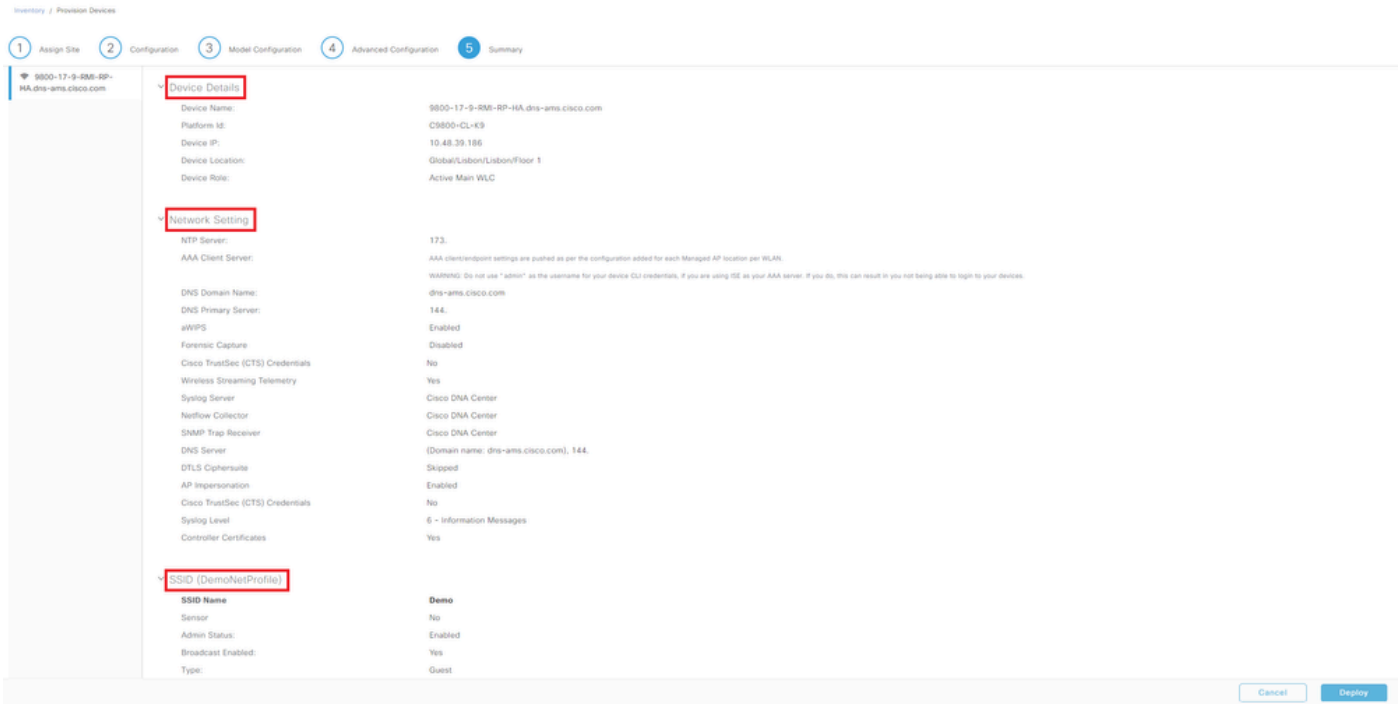
调配WLC

调配WLC

步骤2.在调配WLC配置之前先对其进行检验。确保您添加AP位置：



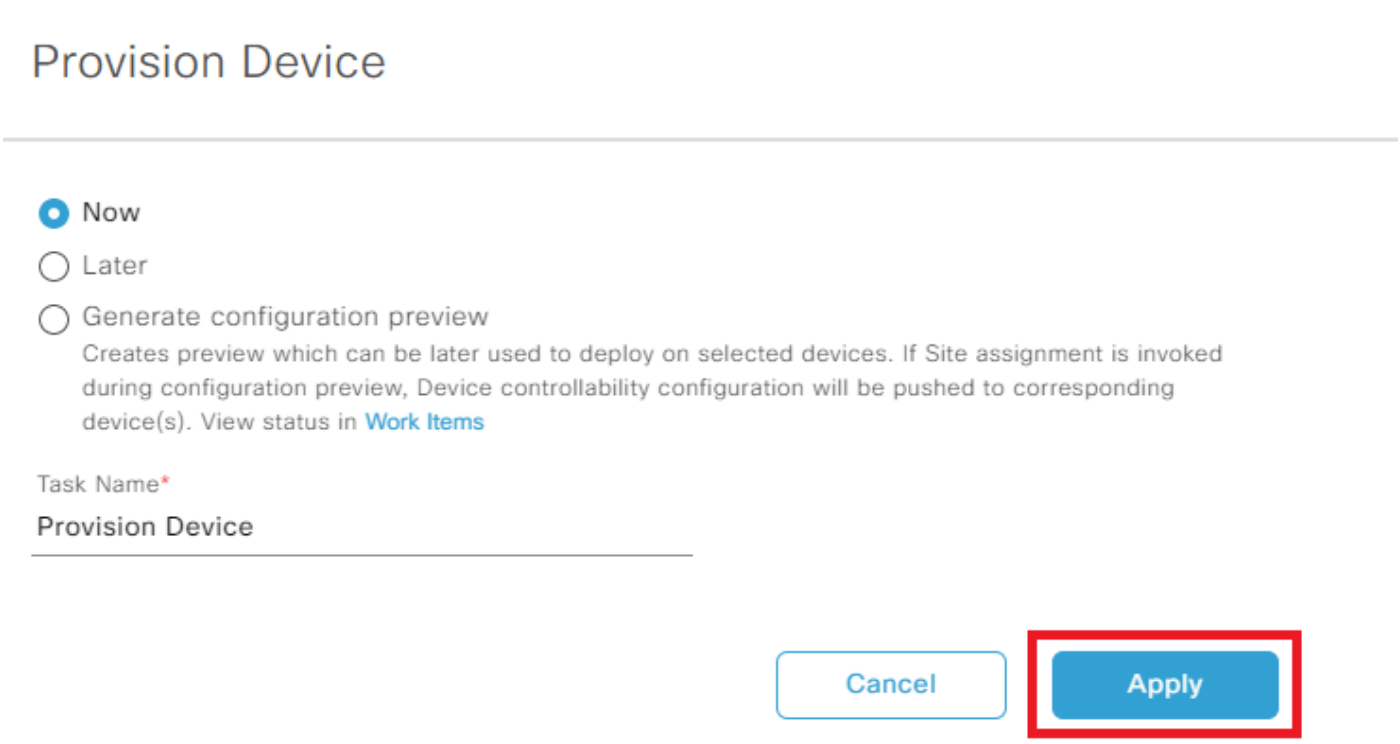
步骤3.在调配设备之前，检验设备详细信息、网络设置和SSID。如果一切正常，请选择部署:



部署WLC调配

部署WLC调配

步骤4.设备调配可立即部署或稍后部署。最后，选择Apply:

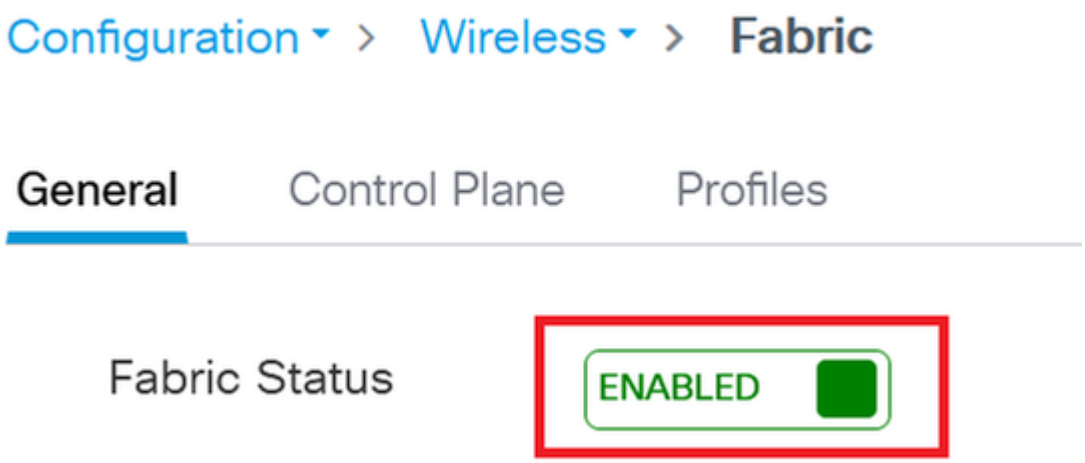


现在或以后调配WLC

现在或以后调配WLC

WLC现在已调配。

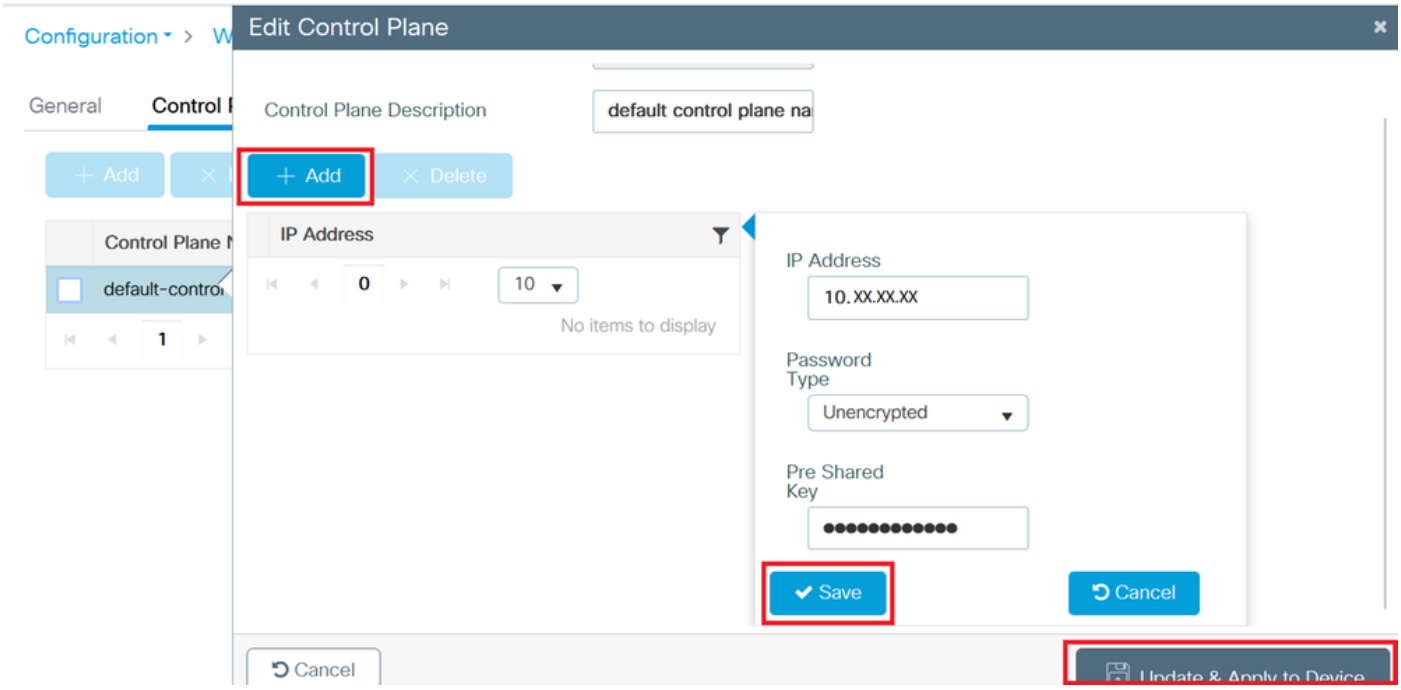
第5步：在WLC端，导航到配置>无线>交换矩阵并启用交换矩阵状态:



启用交换矩阵状态

启用交换矩阵状态

步骤6.导航到配置>无线>交换矩阵>控制平面并编辑控制平面。添加IP地址和PSK。单击Update & Apply to Device:



添加控制平面

添加控制平面

步骤7.（可选）创建新的RF配置文件。导航到Design > Network Settings > Wireless > Global并添加新的RF配置文件:



添加RF配置文件

添加RF配置文件

步骤8.（可选）为RF配置文件指定名称，并选择要配置的设置。在本演示中，配置了默认设置。单击Save:

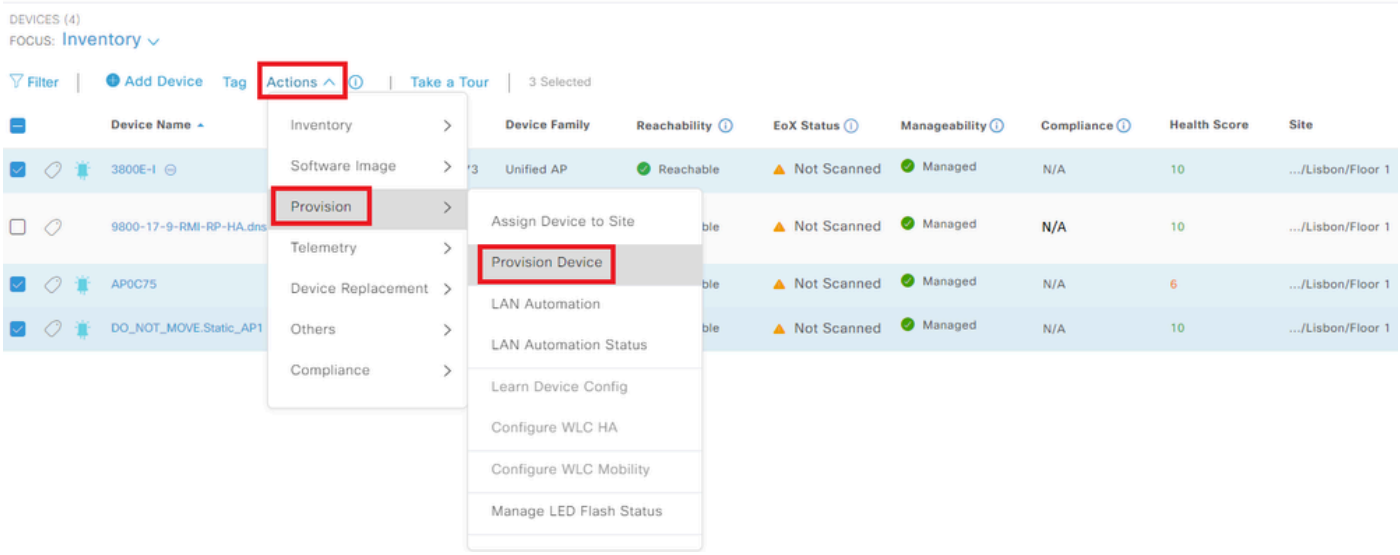


添加基本RF配置文件

添加基本RF配置文件

调配接入点

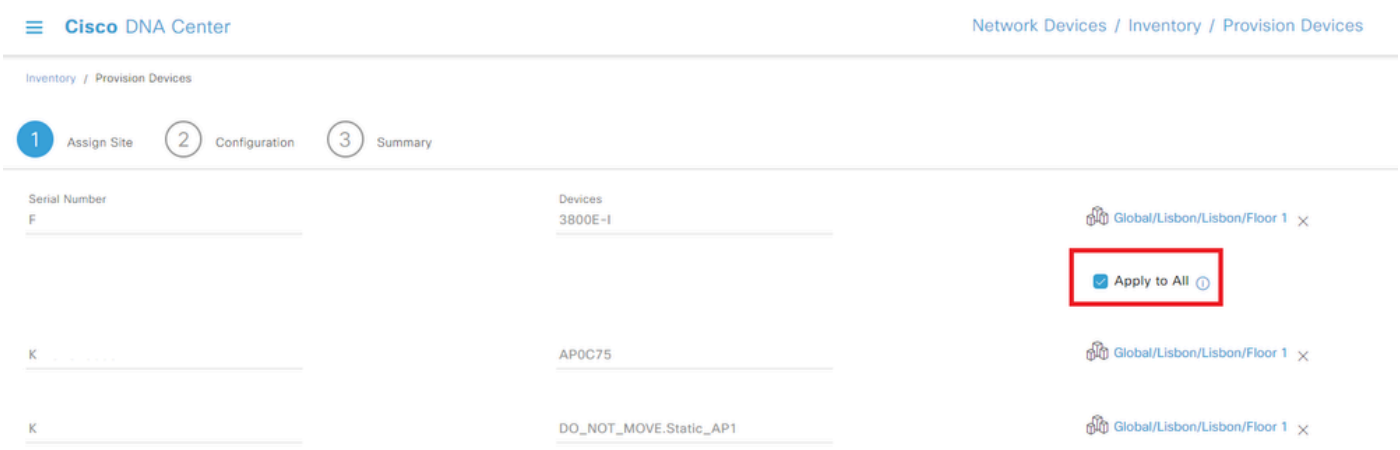
步骤1.导航到您的建筑/楼层。选择APs和Actions > Provision > Provision Device:



调配AP

调配AP

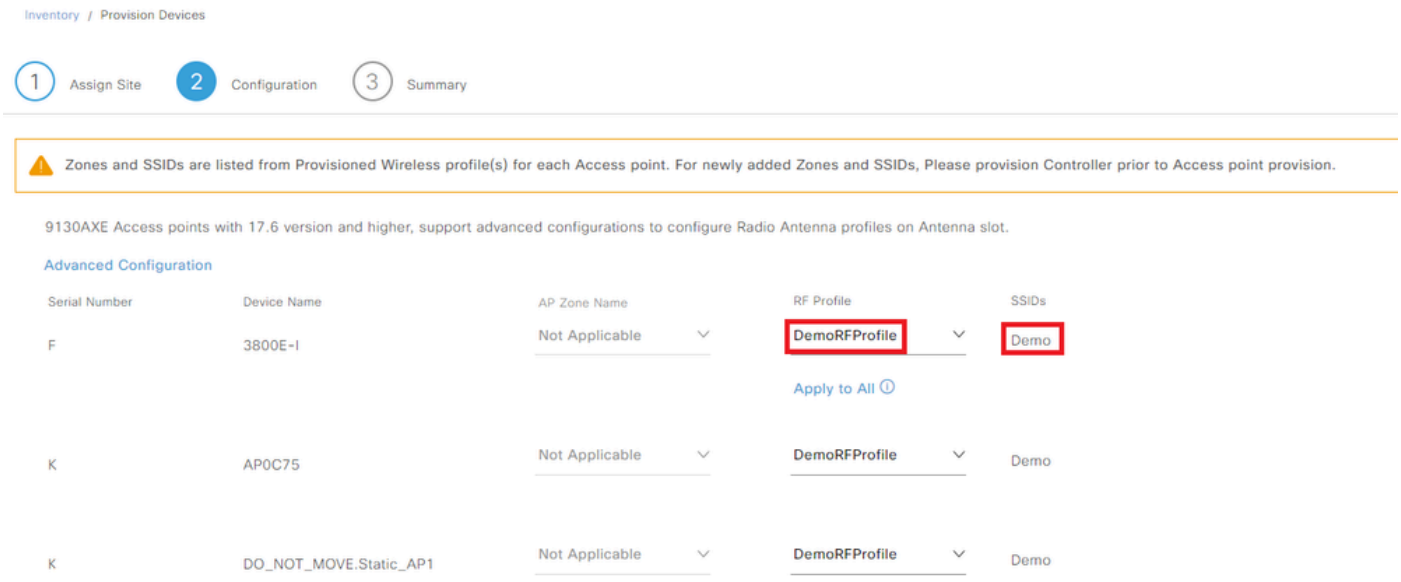
步骤2.验证分配的站点是否正确并选择应用到全部:



将站点分配给AP

将站点分配给AP

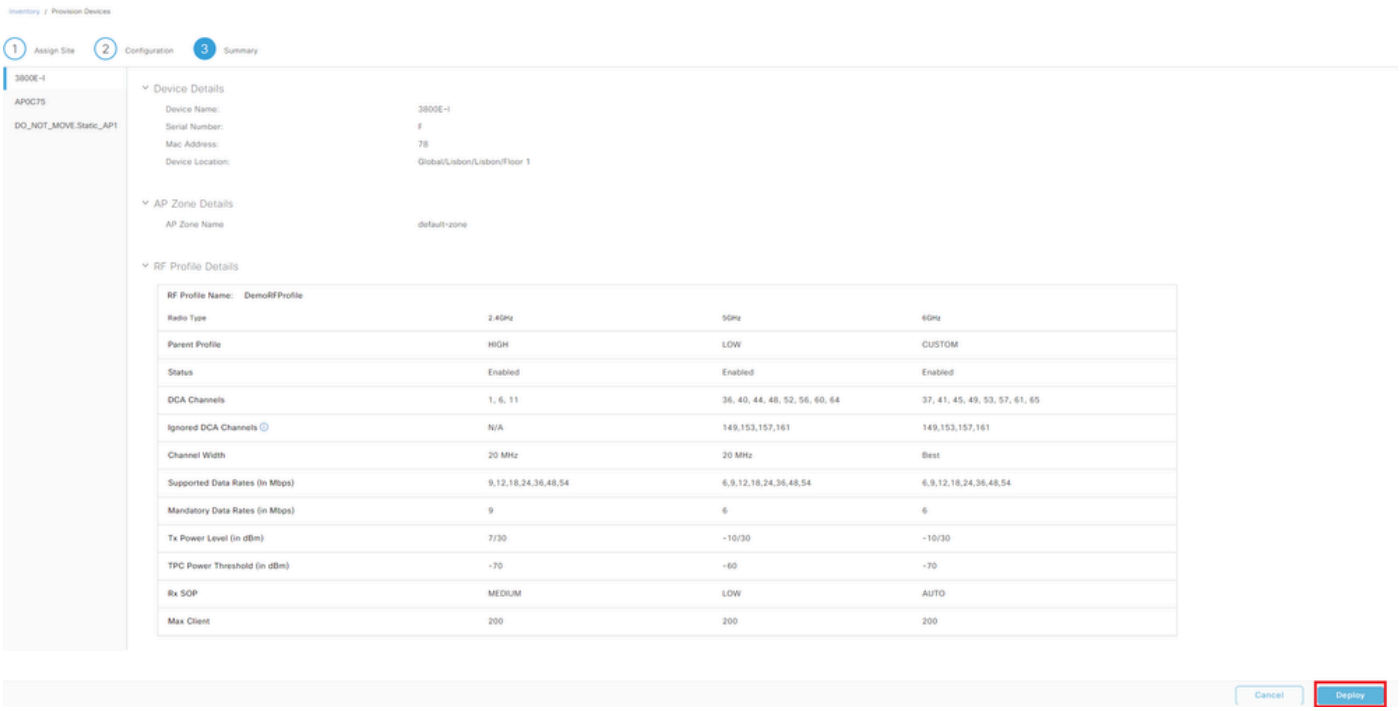
步骤3.从下拉列表中选择RF Profile并验证SSID是否正确：



选择RF配置文件

选择RF配置文件

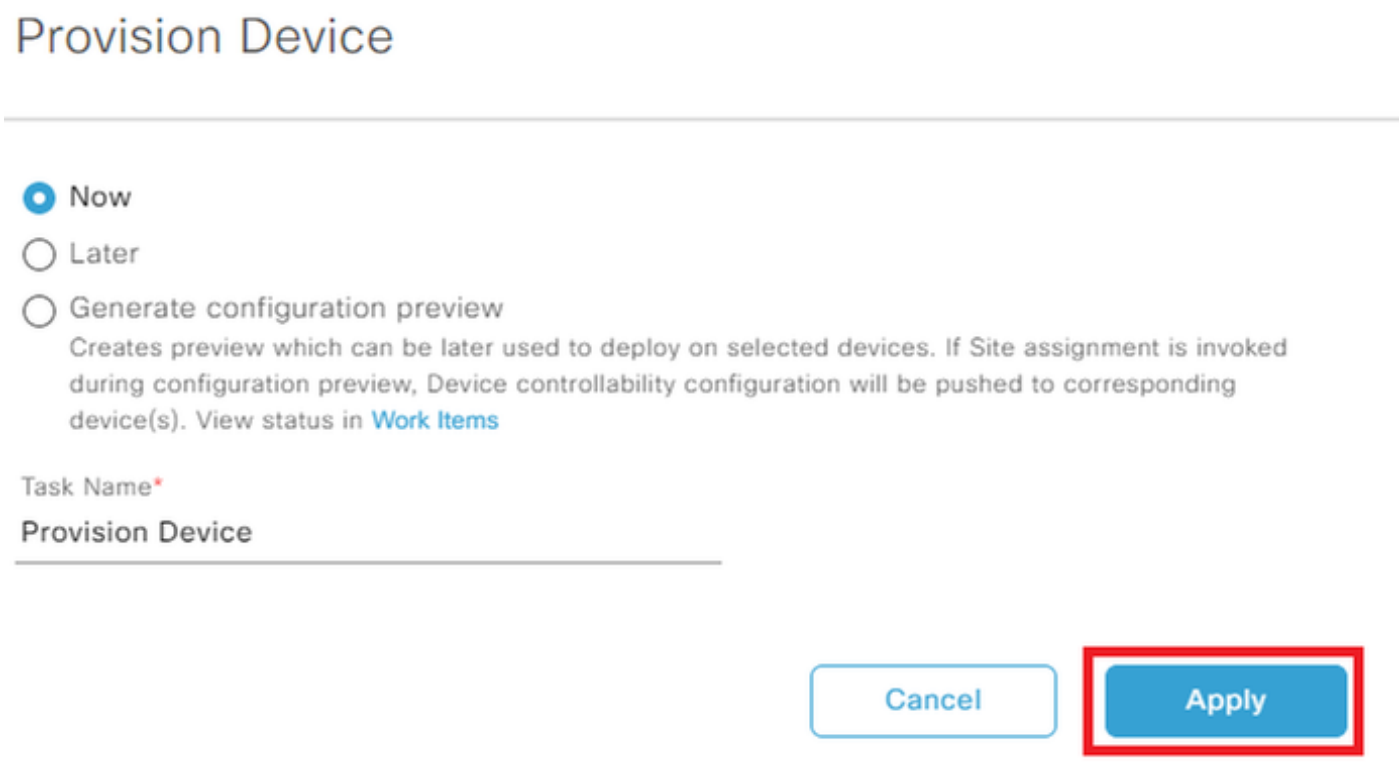
步骤4.检验AP上的设置。如果一切正常，请选择部署:



部署无线接入点调配

部署无线接入点调配

步骤5.设备调配可立即部署，也可稍后部署。最后，选择Apply:



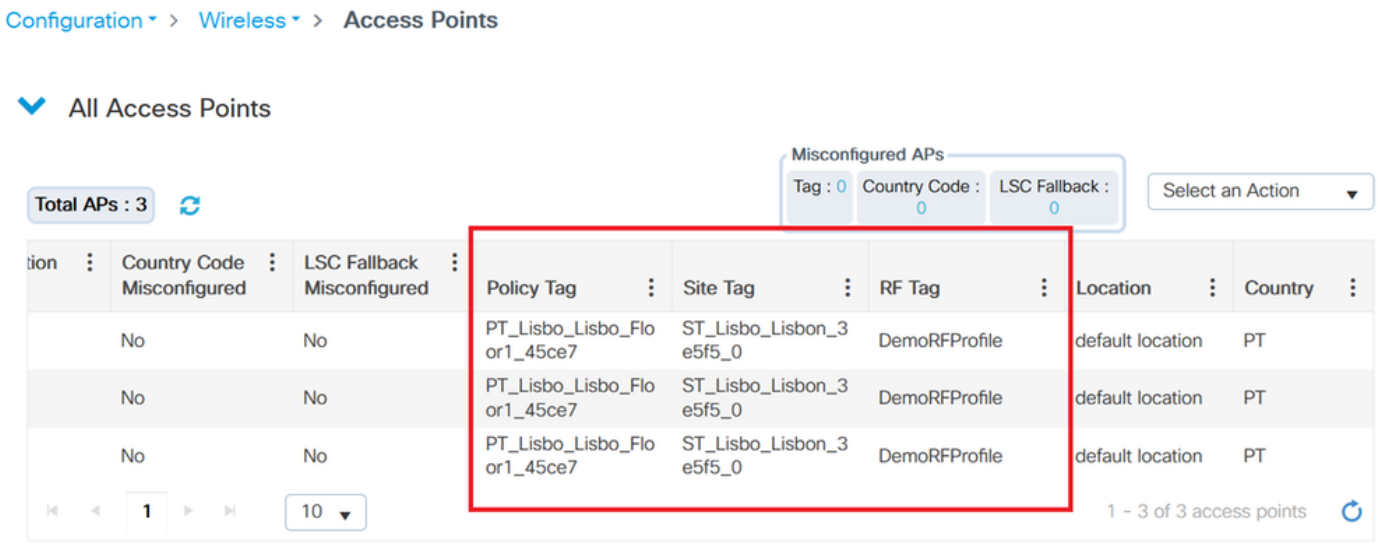
现在或以后调配AP

现在或以后调配AP

⚠ 警告：当调配无线接入点时（已属于为选定RF配置文件配置的楼层）将进行处理和重新启动。

AP现在已调配。

步骤6.在WLC端，导航到Configuration > Wireless > Access Points。验证AP标签是从思科DNA推送的：



AP上的标记

AP上的标记

第7步：导航到配置>标记和配置文件> WLAN，并验证是否已从Cisco DNA推送了SSID:

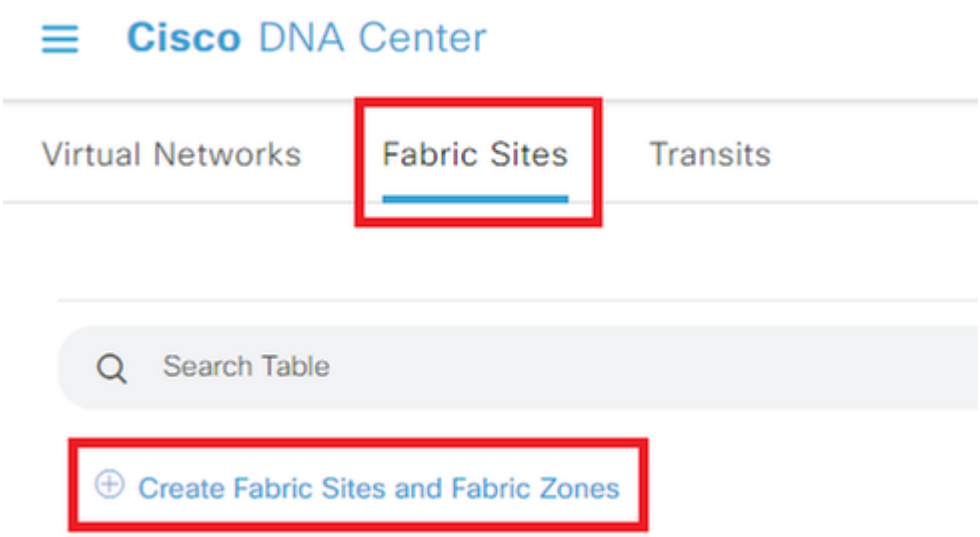


WLAN

WLAN

创建交换矩阵站点

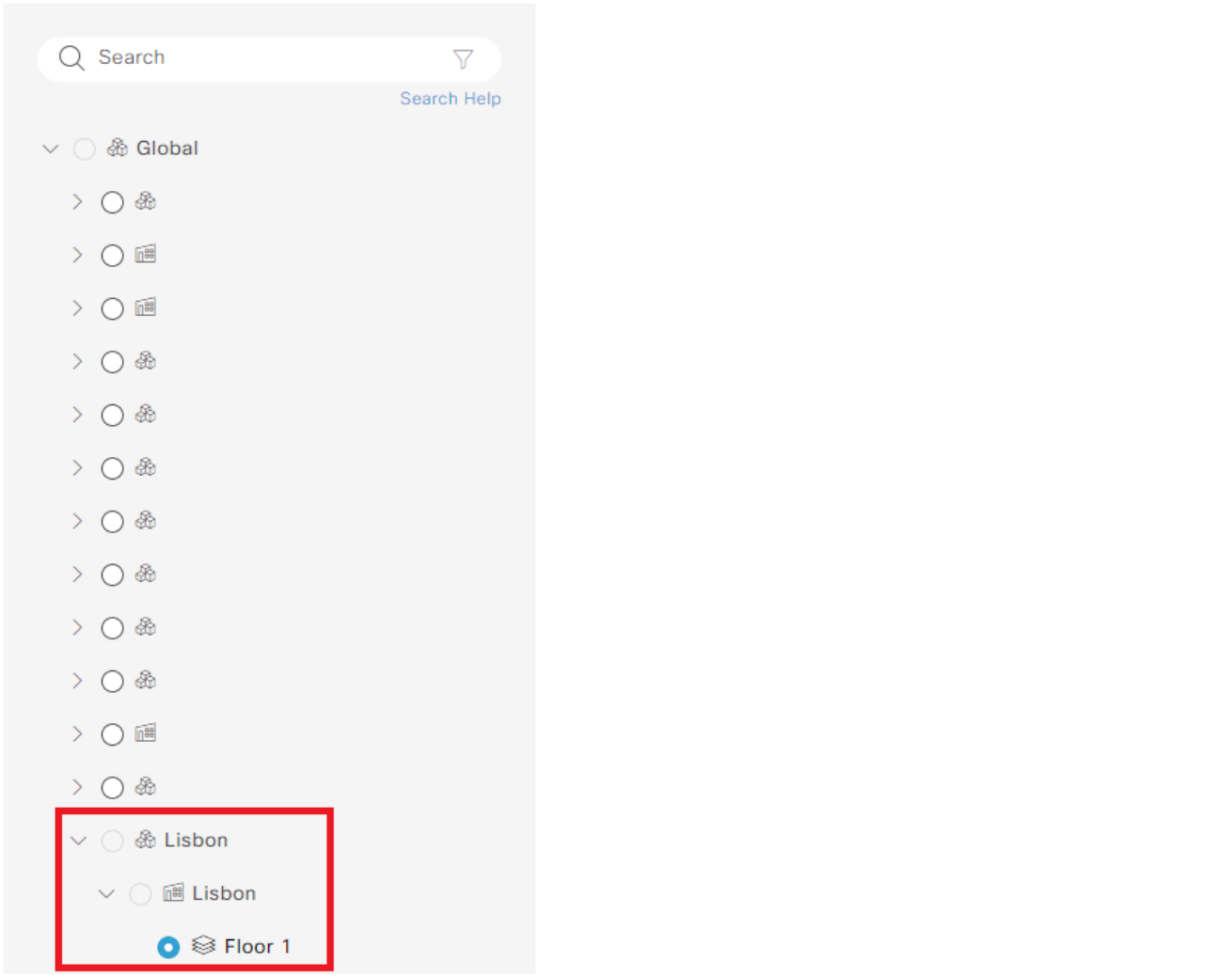
步骤1.导航到调配>交换矩阵站点。创建交换矩阵站点:



创建交换矩阵站点

创建交换矩阵站点

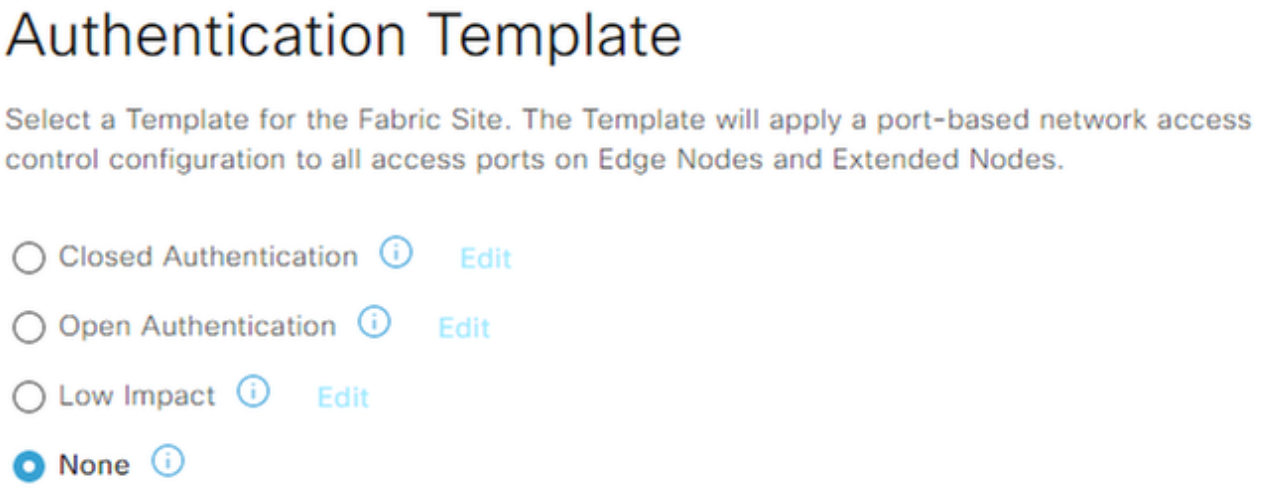
第2步：选择交换矩阵站点的建筑/楼层：



选择交换矩阵站点

选择交换矩阵站点

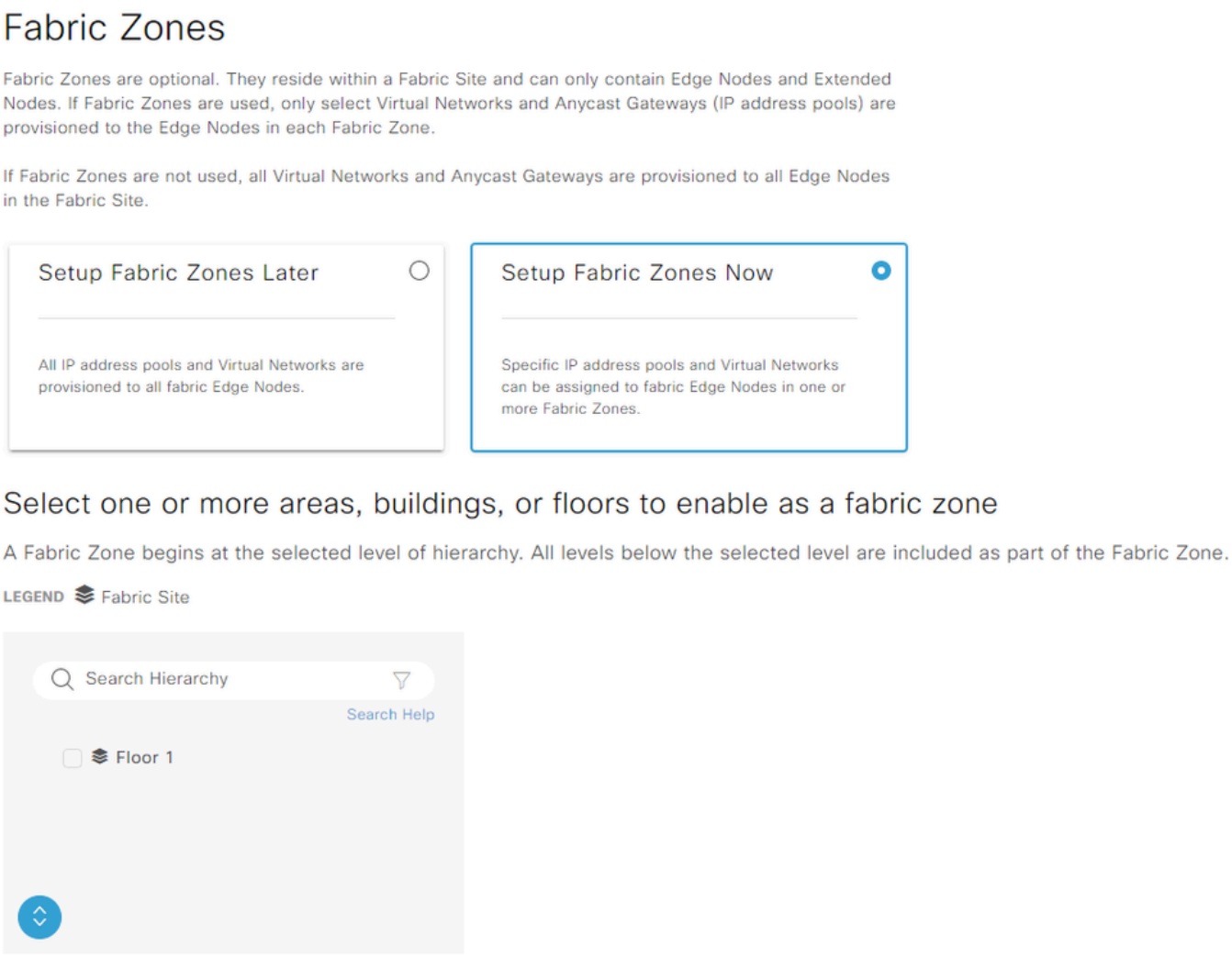
步骤3.选择身份验证模板。在本演示中，已应用None:



身份验证模板

身份验证模板

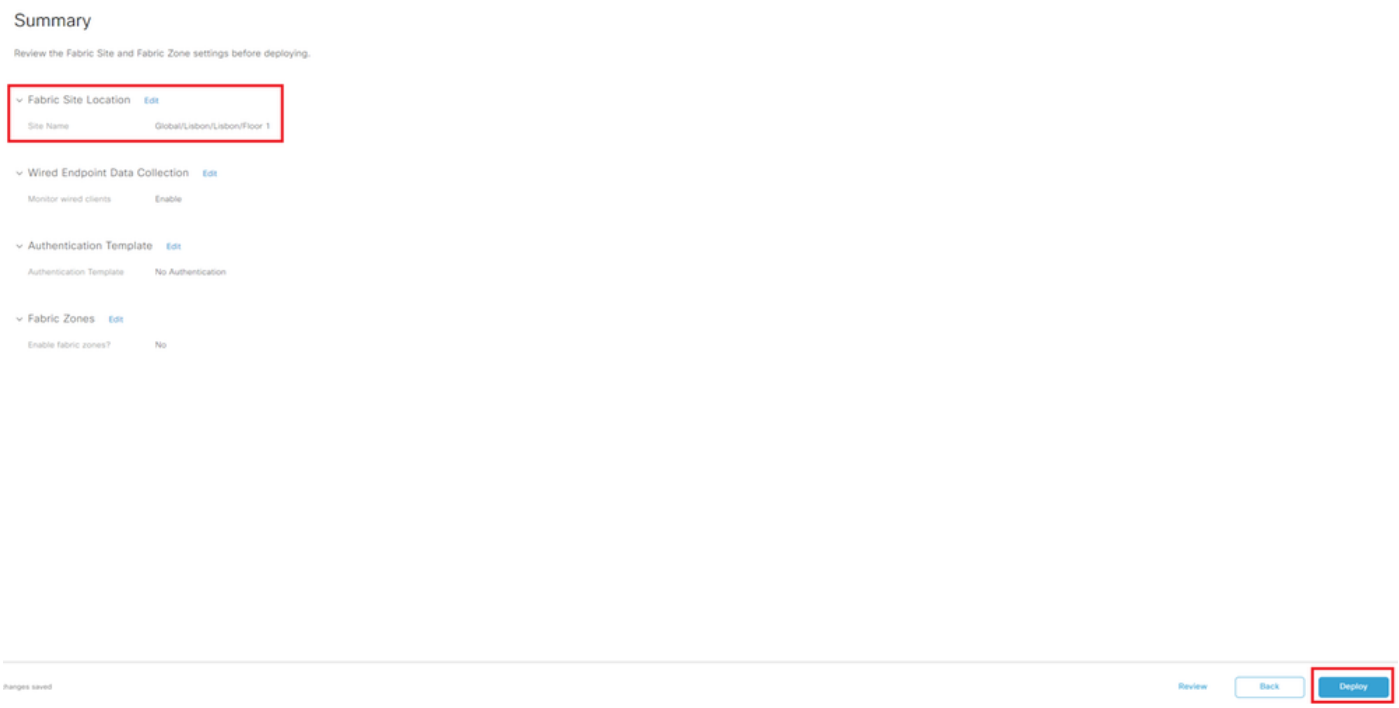
步骤3.您可以选择现在或以后设置交换矩阵区域：



设置交换矩阵区域

设置交换矩阵区域

步骤4.检验交换矩阵区域的设置。如果一切正常，请选择部署:



部署交换矩阵站点

部署交换矩阵站点

您已创建交换矩阵站点：

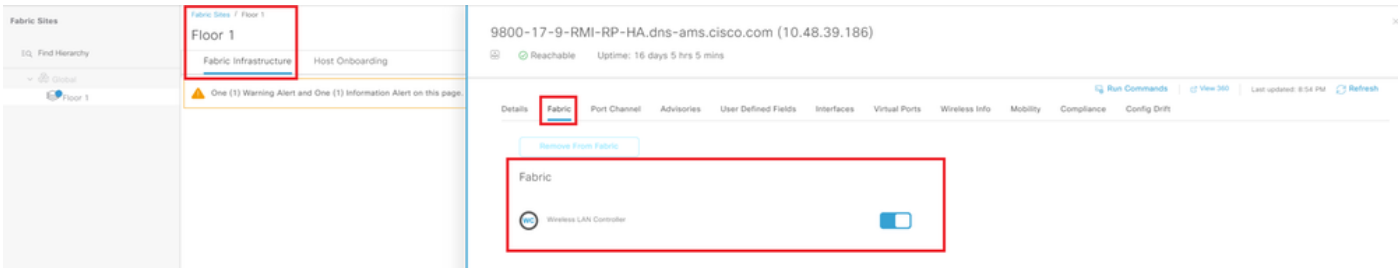


交换矩阵站点创建

交换矩阵站点创建

将WLC添加到交换矩阵

导航到调配>交换矩阵站点，然后选择您的交换矩阵站点。点击WLC的顶部，然后导航到Fabric选项卡。启用fabric到WLC，然后选择Add:

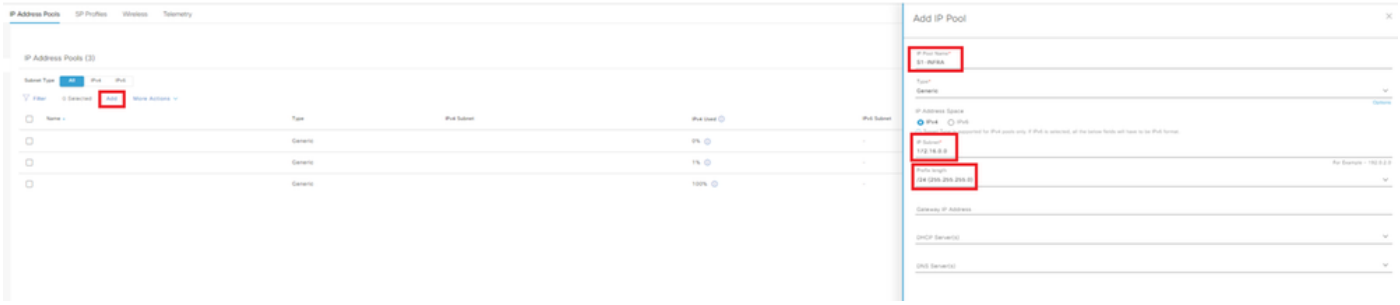


将WLC添加到交换矩阵

将WLC添加到交换矩阵

AP加入

步骤1.导航到Design > Network Settings > IP Address Pools。创建 IP 地址池.



IP Address Pool

IP Address Pool

第2步：导航到调配>交换矩阵站点，然后选择您的交换矩阵站点。导航到主机注册>虚拟网络。

引入INFRA_VN可轻松板载AP。AP位于交换矩阵重叠中，但INFRA_VN映射到全局路由表。只有AP和扩展节点可以属于INFRA_VN。自动启用第2层扩展并启用第2层LISP服务。

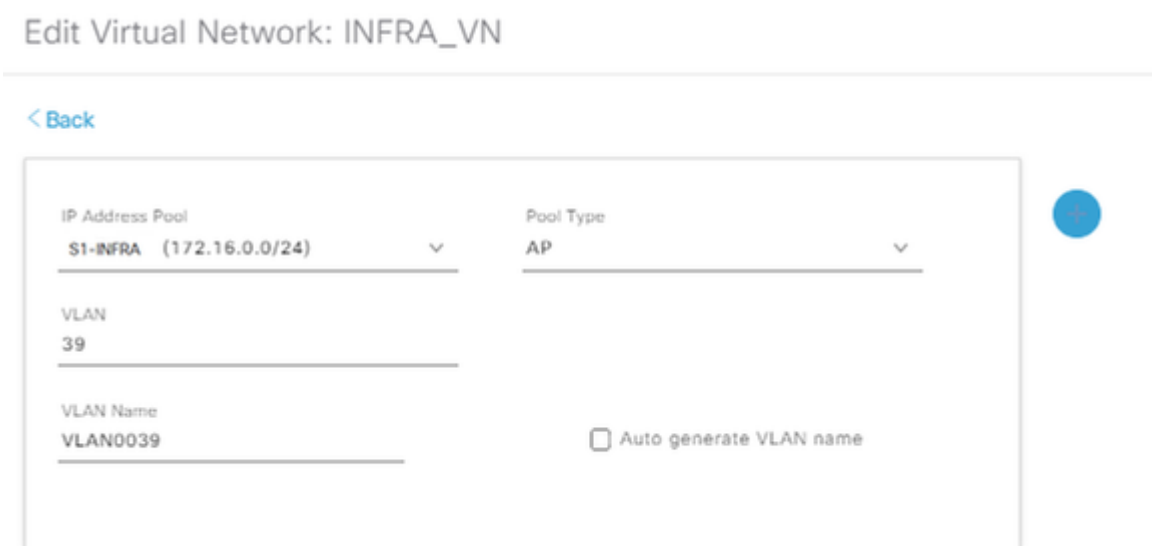
选择INFRA_VN > Add:



编辑虚拟网络

编辑虚拟网络

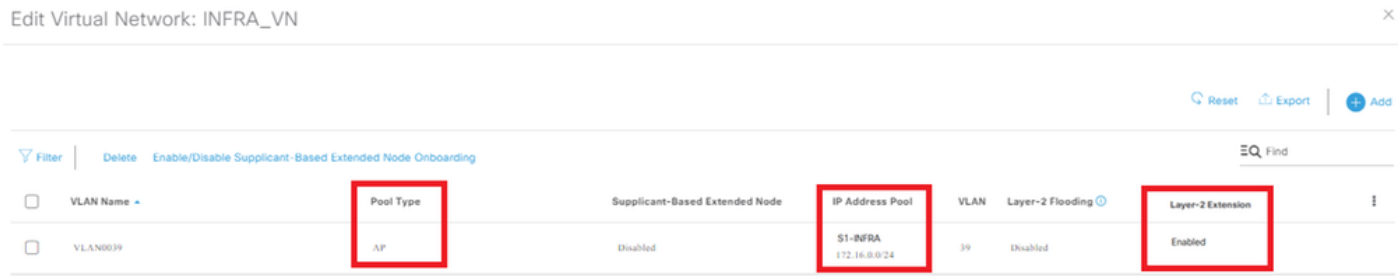
步骤3.将池类型为AP的IP地址池添加:



编辑虚拟网络S1-INFRA

编辑虚拟网络S1-INFRA

步骤4.检验第2层扩展是否已启用。

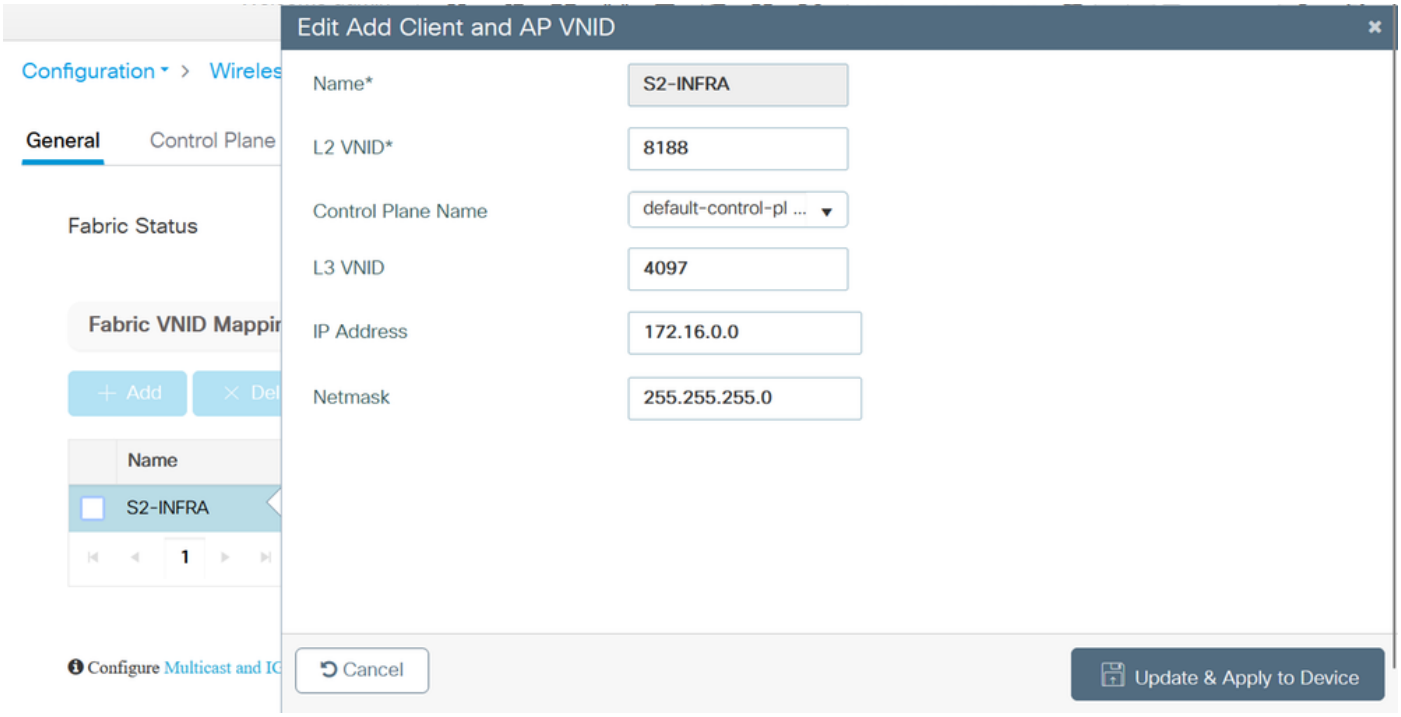


编辑虚拟网络

编辑虚拟网络

当池类型= AP且第2层扩展至ON时，Cisco DNA连接到WLC并为第2层和第3层VN_ID的AP子网将交换矩阵接口设置为VN_ID映射。

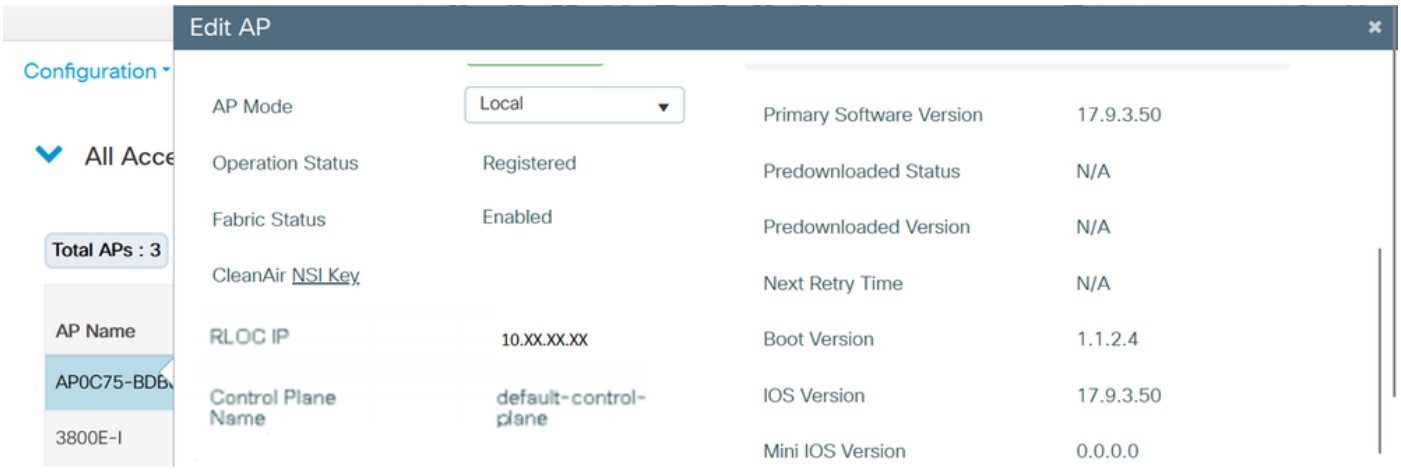
第5步：在WLC GUI侧，导航到配置>无线>交换矩阵>常规。添加新客户端和AP VN_ID:



添加新客户端和AP VN_ID

添加新客户端和AP VN_ID

步骤6.导航到配置>无线>接入点。从列表中选择一个AP。验证Fabric Status为Enabled、控制平面的IP地址和控制平面名称：



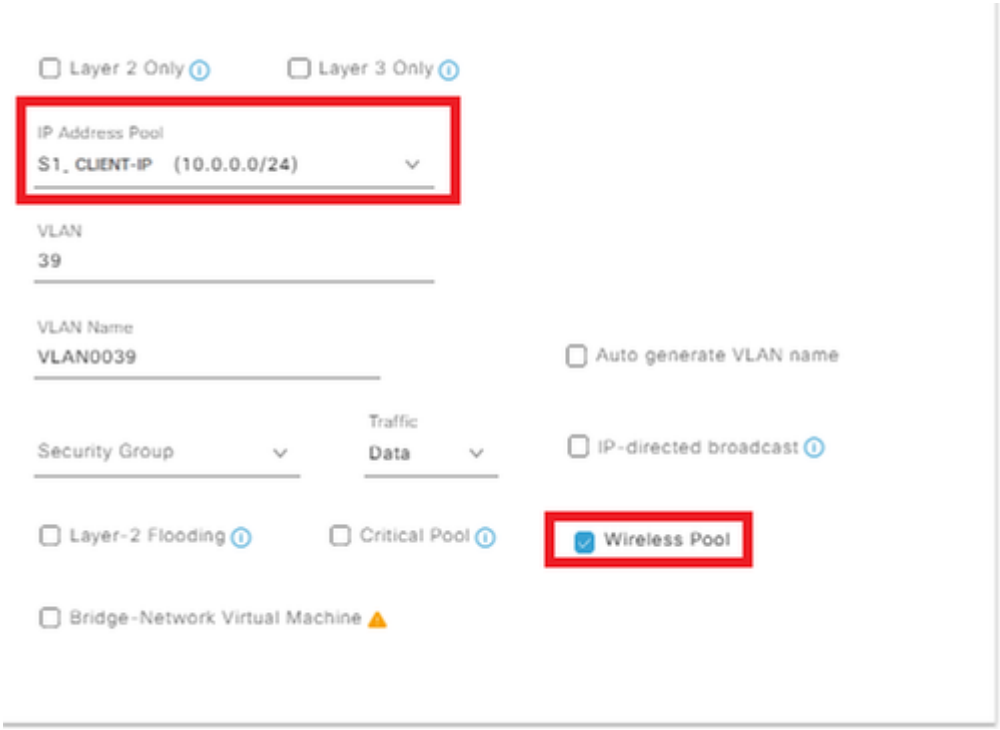
验证AP交换矩阵状态

验证AP交换矩阵状态

板载客户端

步骤1.将池添加到虚拟网络，并验证第2层扩展切换为ON，以启用客户端池/子网上的L2 LISP和第

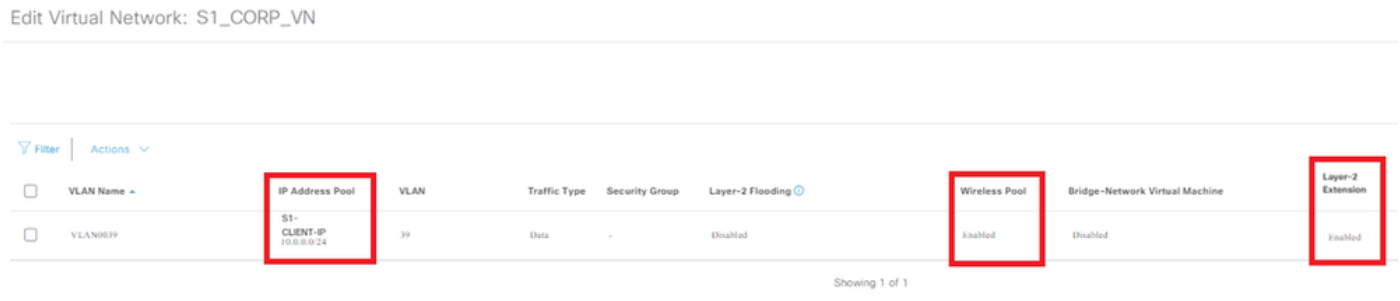
2层子网扩展。在Cisco DNA 1.3.x中，您不能禁用它。



添加IP地址池

添加IP地址池

步骤2.检验第2层扩展和无线池是否已启用。

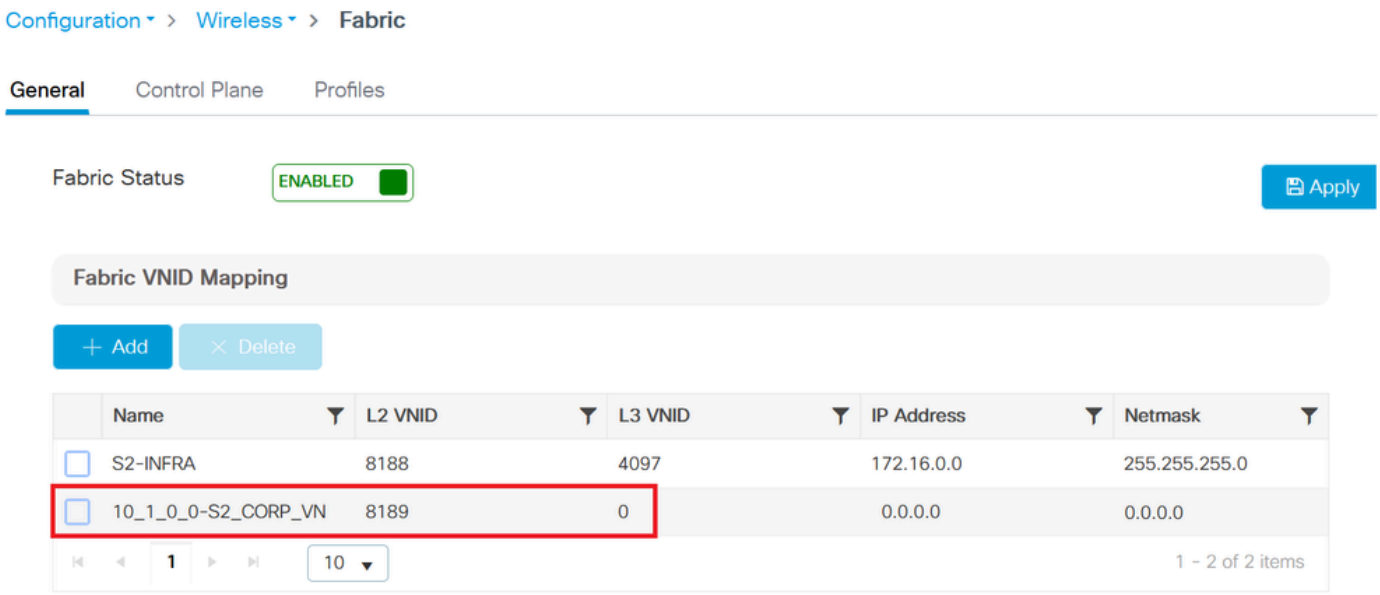


编辑虚拟网络

编辑虚拟网络

第 3 步：在WLC GUI侧，导航到Configuration > Wireless > Fabric > General。添加新客户端和AP VN_ID。

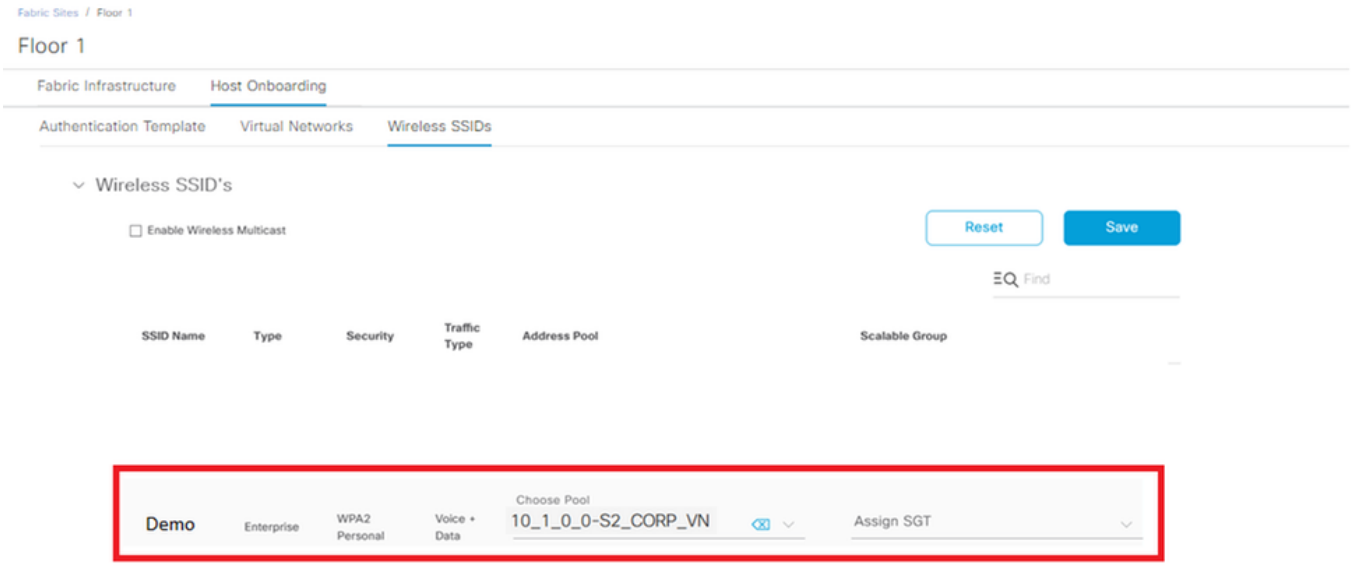
将池分配给虚拟网络后，对应的VNID映射交换矩阵接口将推送到控制器。这些都是L2 VNID。



添加新客户端和AP VN_ID

添加新客户端和AP VN_ID

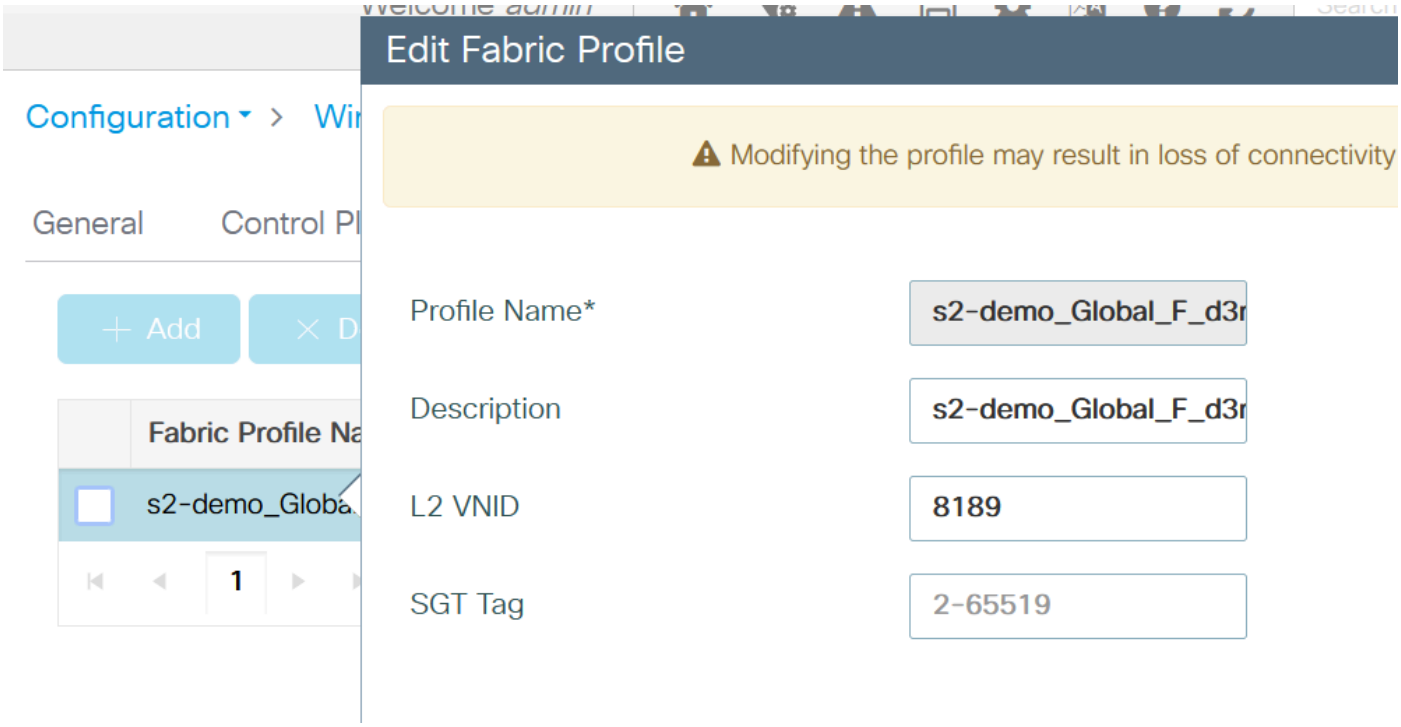
步骤4.将SSID映射到各自虚拟网络中的池：



映射SSID映射SSID

第5步：将具有L2 VNID的交换矩阵配置文件添加到所选池，并将策略配置文件映射到交换矩阵配置文件，为交换矩阵启用该配置文件。

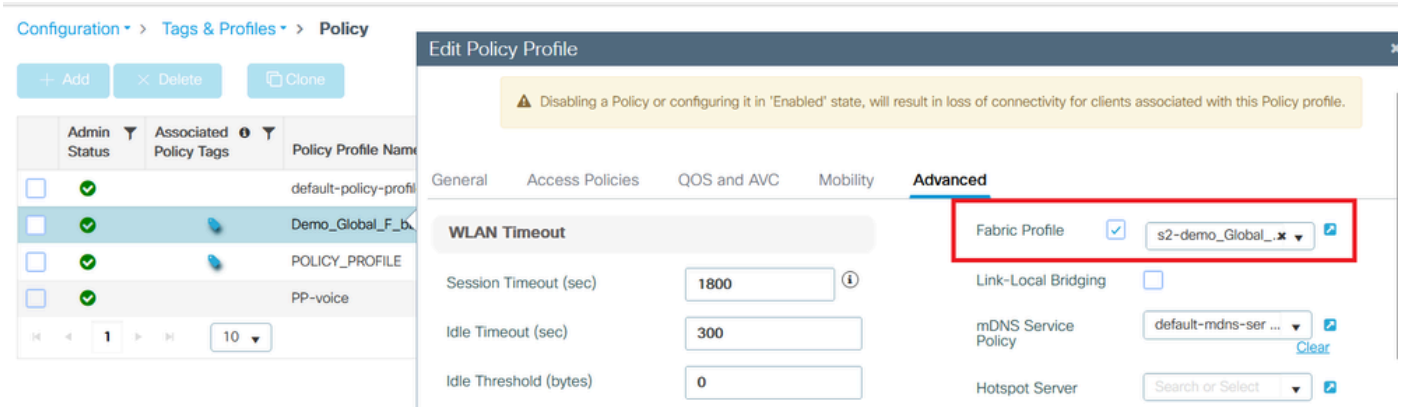
在WLC GUI侧，导航到Configuration > Wireless > Fabric > Profiles。



交换矩阵配置文件

交换矩阵配置文件

步骤6.导航到配置>标记和配置文件>策略。验证映射到策略配置文件的交换矩阵配置文件：



在策略上配置的交换矩阵配置文件在策略上配置的交换矩阵配置文件

验证

验证WLC和Cisco DNA上的交换矩阵配置

在WLC CLI上：

WLC1# show tech

WLC1# show tech wireless

控制平面配置：

路由器LISP

定位器表默认值

定位器集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#show lisp session

VRF默认会话总数：9，已建立：5

对等体状态打开/关闭输入/输出

172.16.201.202:4342上升3d07h 14/14

WLC 配置:

无线交换矩阵

wireless fabric control-plane default-control-plane

ip address 172.16.2.2 key 0 47aa5a

WLC1# show fabric map-server summary

MS-IP连接状态

172.16.1.2以上

WLC1# show wireless fabric summary

交换矩阵状态：启用

Control-plane:

名称IP地址密钥状态

---

default-control-plane 172.16.2.2 47aa5a Up

在WLC GUI上，导航到Configuration > Wireless > Fabric，并验证Fabric Status是否为Enabled。

导航到配置>无线>接入点。从列表中选择一个AP。验证Fabric Status（交换矩阵状态）是否为Enabled（启用）。

在Cisco DNA上，导航到Provision > Fabric Sites并验证您是否具有交换矩阵站点。在该交换矩阵站点上，导航到交换矩阵基础设施>交换矩阵，并验证WLC是否已作为交换矩阵启用。

故障排除

客户端未获取IP地址

步骤1.检验SSID是否为交换矩阵。在WLC GUI上，导航到Configuration > Tags & Profiles > Policy。选择策略并导航到高级。验证是否启用了交换矩阵配置文件。

步骤2.检查客户端是否停滞在IP learn状态。在WLC GUI上，导航到Monitoring > Wireless > Clients。检验客户端状态。

步骤3.检验策略是否需要DHCP。

步骤4.如果流量在AP — 边缘节点之间本地交换，请收集客户端连接的AP日志（客户端跟踪）。验证是否已转发DHCP发现。如果没有DHCP提供到达，则边缘节点上出现了问题。如果未转发DHCP，则AP上存在问题。

步骤5.您可以在边缘节点端口上收集EPC，以查看DHCP发现数据包。如果未看到DHCP发现数据包，则问题出在AP上。

未广播SSID

步骤1.检验AP无线电是否关闭。

步骤2.检查WLAN是否处于打开状态以及是否启用了广播SSID。

步骤3.如果AP已启用交换矩阵，请验证AP配置。导航到Configuration > Wireless > Access Points，选择一个AP，在General选项卡上，您可以看到Fabric Status Enabled和RLOC信息。

步骤4.导航到配置>无线>交换矩阵>控制平面。验证是否配置了控制平面（使用IP地址）。

步骤5.导航到配置>标记和配置文件>策略。选择策略并导航到高级。验证是否启用了交换矩阵配置文件。

步骤6.导航到Cisco DNA，并重新执行创建SSID和调配WLC上的步骤。Cisco DNA必须再次将SSID推送到WLC。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。