Validated Profile: Retail (Non-Fabric) Vertical

October 23, 2025

Solution overview

This document provides guidance and can be used as a validation reference for a typical retail enterprise network deployment.

Retail networks typically encompass hundreds of stores located remotely. Employing a centralized architecture can streamline network management and lower costs, while each individual store maintains its own self-contained network and direct internet connection to enhance performance and reliability. A secure, resilient network is critical for managing inventory, coordination, store operations, and business data.

For centralized architecture, Catalyst Center is a powerful network controller and management dashboard that helps retail enterprises through:

- Automation: Enable device discovery, Plug and Play device onboard, topology diagram, and template deployments.
- Software Image Management (SWIM) and inventory: Provide tools to manage and schedule an upgrade of system images for all Cisco devices, including RMA or replacement of devices.
- Cisco Catalyst Assurance: Monitor network, client, and service health, and troubleshoot issues.

The following features of wireless deployment are essential for retail:

- Cisco FlexConnect wireless technology enables organizations to configure and control remote-site wireless networks from headquarters, while allowing data traffic local switching to reduce network congestion and improve resilience.
- FlexConnect IP address overlapping enables IP address reuse across different FlexConnect sites to increase usage of IP subnets and support cookie-cutter configurations.
- Wireless mobility provides seamless and fast roaming through stores to streamline inventory management, improve store operations, and enhance customer experience.

The following features of network security play a crucial role in safeguarding the integrity of business and customer data:

- Wired networks: Dot1X, MAB, guest Wireless networks: Rogue detection, access point (AP) authentication, and so on.

Network high availability (HA) is vital for retail businesses. Technologies such as Stack, Hot Standby Router Protocol (HSRP), StackWise Virtual Link (SVL), WAN, wireless controller Stateful Switchover (SSO), and N+1 HA ensure that if a network component fails, business operations continue with minimal disruption.

Cisco Spaces provides location services to optimize inventory management and identify consumer traffic and data for personalized marketing.

Hardware and software specifications

The solution is validated with the hardware and software listed in this table. For the complete list of hardware and software supported, see the Cisco Catalyst Center Compatibility Matrix.

Role	Model name	Hardware platform	Software release	
Cisco Catalyst Center Controller	DN2-HW-APL-XL	Catalyst Center appliance 3-node cluster	2.3.7.7	2.3.7.9
Cisco Catalyst Center on ESXi (1,2)	DNA-SW-OVA	Catalyst Center on ESXi	2.3.7.7	2.3.7.9
Identity Management, RADIUS server	SNS-3695-K9	Secure Network Server for Cisco Identity Services Engine (ISE) application (large)	3.3 Patch 4	Cisco ISE, 3.3 Patch 4
Cisco wireless controller	C9800-80-K9	C9800-80-K9	17.9.6, 17.12.4	17.9.6,17.12.5
Cisco wireless controller	C9800-CL	Virtual wireless controller	17.9.6, 17.12.4	17.9.6,17.12.5
Cisco SD-WAN cEdge router	C8500-12X4QC	Cisco SD-WAN Edge platform	17.12.3a	17.12.5a
Cisco SD-WAN cEdge router	C8300-2N2S-4T2X	Cisco SD-WAN Edge platform	17.9.5a, 17.12.3a	17.12.5a
Remote site switch	C9500-24Y4C C9300-48P, T, U C9300-24U, UX	Cisco Catalyst 9300/9500	17.9.5, 17.12.4	17.9.6a, 17.12.5, 17.15.3, 17.12.5a
Remote site switch (legacy)	ISR4451 Cisco Catalyst 3850	Cisco Integrated Service Router Cisco Catalyst 3850	16.12.11	16.12.13
Cisco Spaces	Cisco Spaces Connector	Virtual connector	location-3.1.0.127, iot-services-3.1.3.44	location-3.1.0.127, iot-services-3.1.3.44
Ekahau	—	Ekahau Artificial Intelligence (AI) Pro software	11.0.2.219	11.0.2.219

1. See the “Limitations and Restrictions” section in the Cisco Catalyst Center 2.3.7.x on ESXi Release Notes for a description of its limitations and restrictions.

2. Unlike physical Cisco Catalyst Center appliances, you cannot connect VMs to create a three-node cluster. You need to use VMware vSphere to set up high availability. For more information, see the “High Availability" section in the *Cisco Catalyst Center 2.3.7.x on ESXi Administrator Guide*.

Solution use case scenarios

The use cases in this table were validated on the retail vertical profile. The use cases are categorized into various technology areas to show the breadth of deployment scenarios covered. These use cases evolve based on customer feedback.

Focus area	Use cases
Day zero to day 1	
New site bringup	Bring up a new site with wired devices in Catalyst Center: • Discover devices and topologies • Provision configurations • Deploy device configuration templates
	Deploy wireless networks for a new site in Catalyst Center: • Upload a floor map under a Catalyst Center site • Add new APs with Plug and Play, assign new APs to the new site location, and locate them on the floor map • Create and provision FlexConnect wireless profiles and policies on the new site
Location service	Integrate with Cisco Spaces Monitor real-time device locations and client behavior
Day-*n* operation	
Wireless	Manage and provision wireless networks with Catalyst Center: • Modify wireless settings and network profiles • Create new SSIDs and update existing SSIDs • Update profiles, tags, AP zones, and so on • Onboard new APs with Plug and Play • RMA or refresh APs through Catalyst Center workflows • Change AP locations and reprovision APs
Security	Manage and provision network security with Catalyst Center: • Monitor threats and manage rogue rules and aWIPS profiles • Configure guest access Wi-Fi with traffic segmentation • Apply MAB/DOT1x authentication for AP onboarding • Configure wired and wireless endpoint security policies, such as Dot1X and PSK • Scan network devices and provide security advisories
Inventory management	Manage network inventory with Catalyst Center, including: • Onboard devices via Plug and Play • Discover devices by IP address or Cisco Discovery Protocol (CDP) • RMA broken devices • Run compliance checks • Move devices between locations • Manage device certificates • Manage password changes

Focus area	Use cases
Device configuration	Manage device configurations with Catalyst Center, including: • Use device templates to deploy new configurations • Track device configuration changes • Use Assurance audit logs to monitor any errors that occurred during configuration
Software image management (SWIM)	Manage device software and schedules upgrades with Catalyst Center, including: • Upgrade network routers and switches, including SLV pairs and stack switches • Upgrade wireless devices, including wireless controller SSO pairs and C9800-CL virtual machines • Schedule AP rolling upgrades • Generate SWIM reports
System health and utilization monitoring	Monitor network and device health, client endpoints, and network utilizations with Assurance, including: • Monitor network device health and utilizations • Monitor system health for each location • Monitor network services, such as AAA and DHCP • Monitor wireless controllers and APs • Monitor the number of wired and wireless clients and details
Troubleshooting	Troubleshoot network issues with Catalyst Center, including: • SSH into devices and run CLI commands • Compare device configuration changes • Run a path trace and discover any link failures • Analyze the root cause of high CPU utilization • Check audit logs for troubleshooting applications or device PKI certificates
System and network robustness	
Wireless	Verify system-level resiliency during the following events: • Wireless controller failover (N+1 wireless controller) • Wireless controller SSO • Single AP failure
WAN	Verify system-level resiliency during the following events: • Remote sites lose WAN connectivity • Remote sites recover WAN connectivity • When remote site APs cannot reach wireless controllers, FlexConnect APs enter standalone mode
Local device	Verify system-level resiliency during the following events: • Distribution layer SVL failover • Stack access switch member failure • Link failure between distribution and access switches
Latency	With 100 ms latency, FlexConnect Local Authentication is applied to reduce the latency requirements of the remote sites.

Focus area	Use cases
Cisco Identity Services Engine (ISE)	Verify system-level resiliency during the following events: • Policy Service Node (PSN) failure • Policy Administration Node (PAN) failover • Cisco ISE PSN change • Cisco ISE upgrade

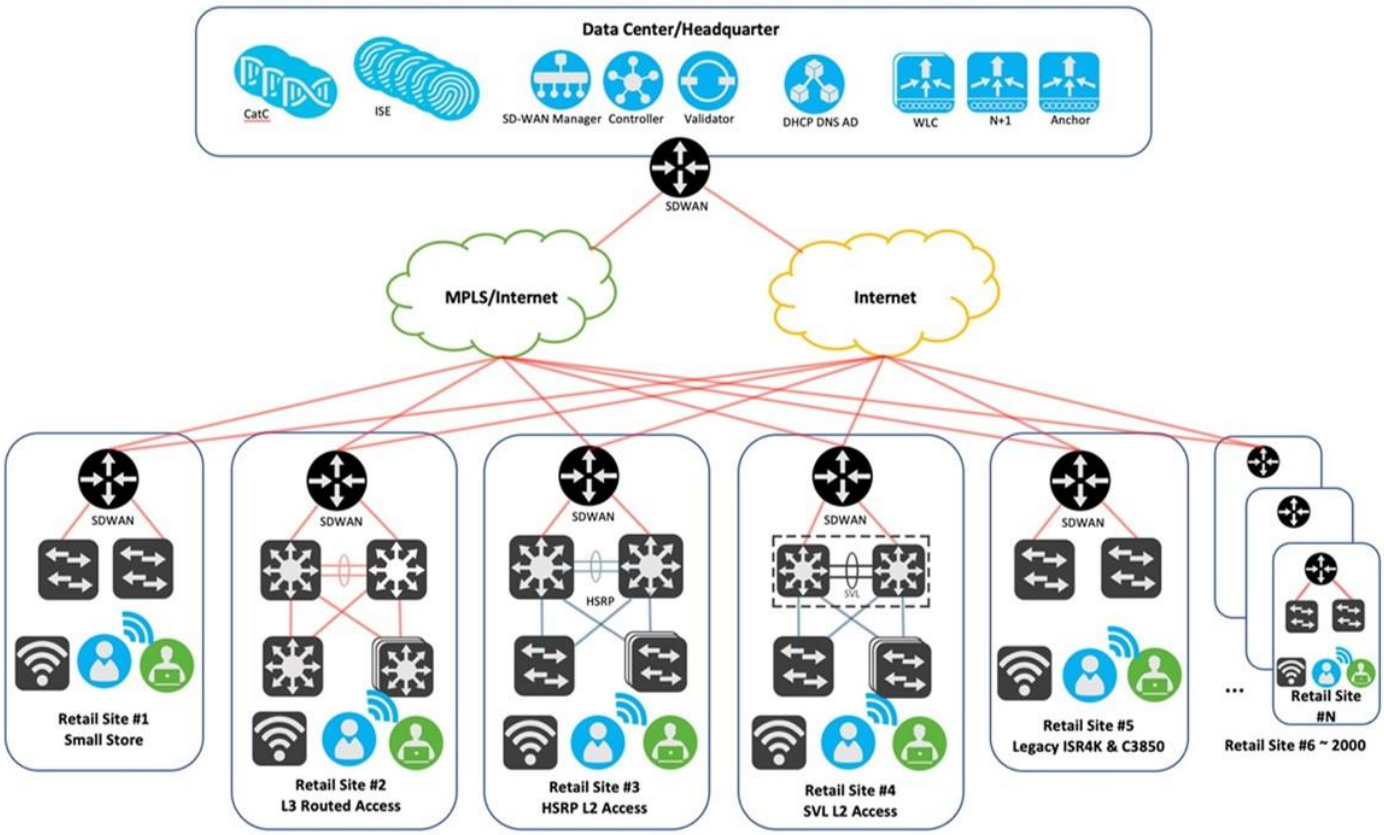
Topology

One Catalyst Center three-node, 112-core cluster is deployed in the sample topology. A distributed Cisco ISE cluster is integrated with the Catalyst Center cluster. The Cisco ISE cluster deployment includes two PANs, two monitoring (MnT) nodes, a Platform Exchange Grid (pxGrid), and multiple PSNs.

The Catalyst Center cluster manages 2000 remote sites connected using two WAN networks. The sites are configured accordingly:

- Data center or headquarter site:
- One Catalyst Center cluster
- One Cisco ISE cluster
- Cisco SD-WAN: Manager, Validator, Controller
- Two wireless controller SSO pairs; each pair manages 5000 APs of 1000 sites
- Two wireless controllers provide N+1 redundancy
- One guest anchor wireless controller
- Multiple servers for DHCP, DNS, AD, NTP, and so on
- 1900 small store sites: one floor, one switch, and two APs per site
- 50 medium store sites: one floor, two switches, and 10 APs per site
- 30 super store sites: two floors, 10 switches, and 50 APs per site
- 20 distribution centers or warehouse sites: two floors, 50 switches, and 210 APs per site This figure shows the logical topology of the retail vertical solution test bed

Figure 1. Solution test logical topology



- Retail Site #1 represents the small retail site deployment, where a Cisco Catalyst 9300 switch is used as a Layer 2 access switch. A Catalyst 8300 router is used and Cisco SD-WAN services.
- Retail Site #2 represents the medium to super large retail site deployment, where multiple Catalyst 9300 switches are used as Layer 3 routed access switches. A Catalyst 9300/9500 switch pair is used in the distribution layer. A Catalyst 8300 router is used for Cisco SD-WAN services.
- Retail Site #3 represents the super large retail site, distribution center, or warehouse deployment, where multiple Catalyst 9300 switches (and stacks) are used as Layer 2 access switches. A Catalyst 9300 and Catalyst 9500 switch pair is used in the distribution layer. HSRP is configured for load balancing. A Catalyst 8300 router is used for Cisco SD-WAN services.
- Retail Site #4 represents the medium to super large retail site deployment, where multiple Catalyst 9300 switches (and stacks) are used as Layer 2 access switches. A Catalyst 9500 switch SVL pair is used in the distribution layer. A Catalyst 8300 router is used for Cisco SD-WAN services.
- Retail Site #5 represents the legacy retail site deployment, where Catalyst 3850 switches are used as Layer 2 access switches. A Cisco ISR 4000 router is used for Cisco SD-WAN services.
- Retail Sites #6 represents 2000 sites simulated by tools. Devices and APs are assigned for each site.

Scale

Solution test verified the scale numbers listed in the following table on a 112-core second-generation Catalyst Center appliance. For the software and hardware capacity, see the Cisco Catalyst Center Data Sheet.

Attribute	Scale numbers
AP	10,000 (5000 APs/wireless controller) distributed across 200 sites
Network devices	300
Wireless endpoints	300,000
Network profiles	1
Retail site	200
Buildings and floors	400
SSIDs	2
WCLs	7 (for two wireless controller SSO pairs, 2 for an N+1 HA wireless controller, and 1 for a guest anchor)

The Catalyst Center on ESXi virtual appliance supports the same scale numbers as a 44-core second-generation physical Catalyst Center appliance for small-scale environments. For more information, see the "Deployment Requirements" section in the *Cisco Catalyst Center 2.3.7.x on ESXi Deployment Guide*.

Solution key notes

These next sections provide an overview of the Cisco SD-Access architecture and solution components.

This section describes technical notes that are useful for deploying the retail vertical profile.

Wireless FlexConnect at remote sites

The FlexConnect solution enables retail operations to configure and control APs in remote sites from the corporate headquarters through a WAN link without deploying a controller at each site. The FlexConnect APs can also switch client data traffic locally and perform client authentication locally when the connection to the controller is lost. When connected to the controller, these APs can send traffic back to the controller and also perform local authentication.

The controller software has a more robust fault tolerance method to FlexConnect APs. Whenever a FlexConnect AP disassociates from a controller, it moves to the standalone mode. The connection between the clients and the FlexConnect APs is maintained, providing the client with seamless connectivity. When both the AP and controller have the same configuration, the connection between the clients and APs is maintained.

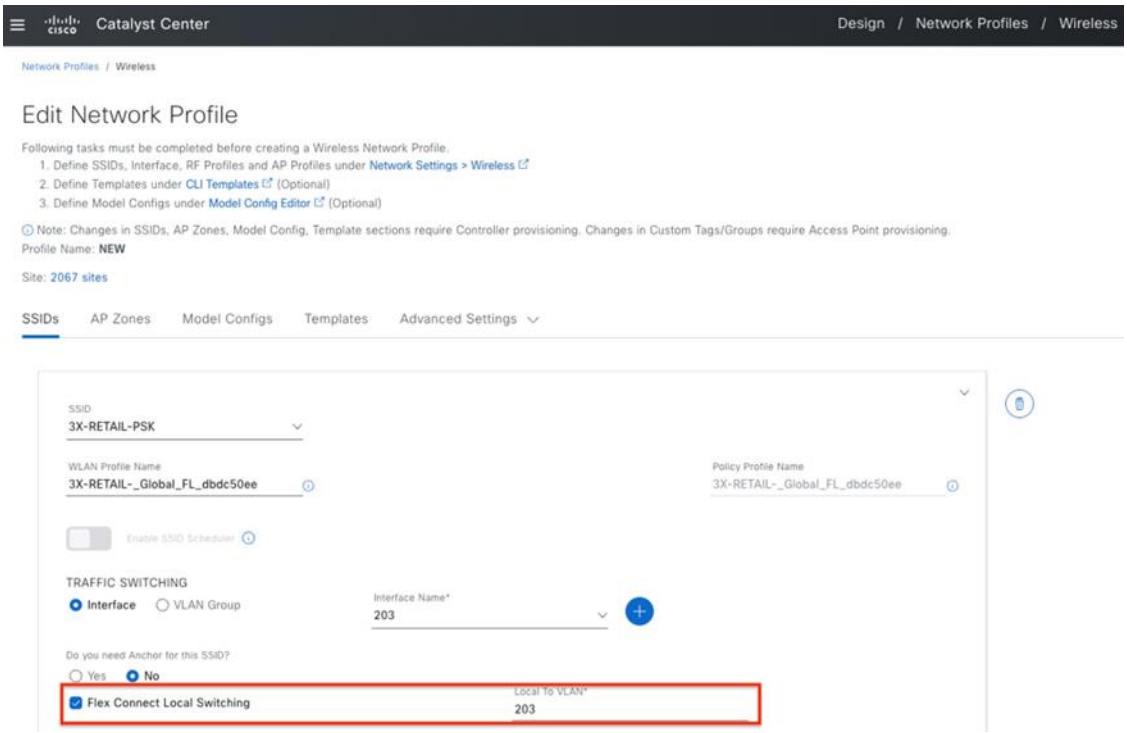
Procedure 1. To configure FlexConnect on Catalyst Center:

Step 1. Configure for wireless:

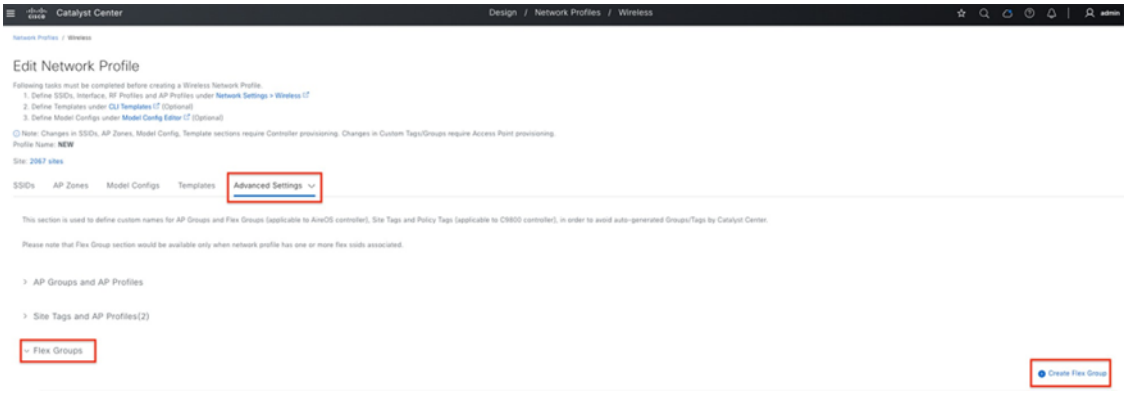
a. From the main menu, choose **Design > Network Profiles > Wireless**.

b. Choose the wireless profile.

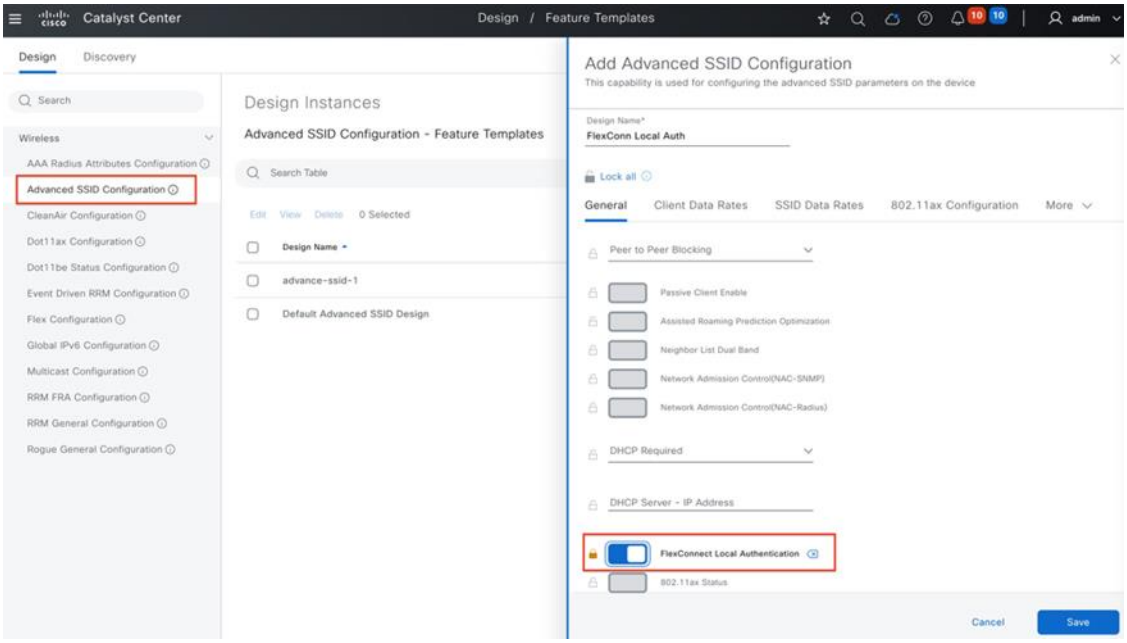
c. In the **SSIDs** tab, check the **Flex Connect Local Switching** check box.



Step 2. Create Flex Groups by choosing **Advanced Settings > Flex Groups**.



Step 3. Configure FlexConnect Local Authorization, by choosing **Design > Feature Templates > Advanced SSID Configuration**.



IP address overlapping

In FlexConnect deployments, by default, if you reuse the same IP subnets at separate locations, wireless controllers detect multiple client sessions with the same IP address as IP THEFT. As a result, clients are blocklisted.

In the FlexConnect Deployment feature, the Overlapping Client IP Address capability allows you to overlap IP addresses across multiple FlexConnect sites while keeping all the supported functionalities in FlexConnect deployments. Network administrators can use a cookie-cutter configuration across sites with the same subnets to simplify management and integrate separate networks without concern of IP addresses overlapping.

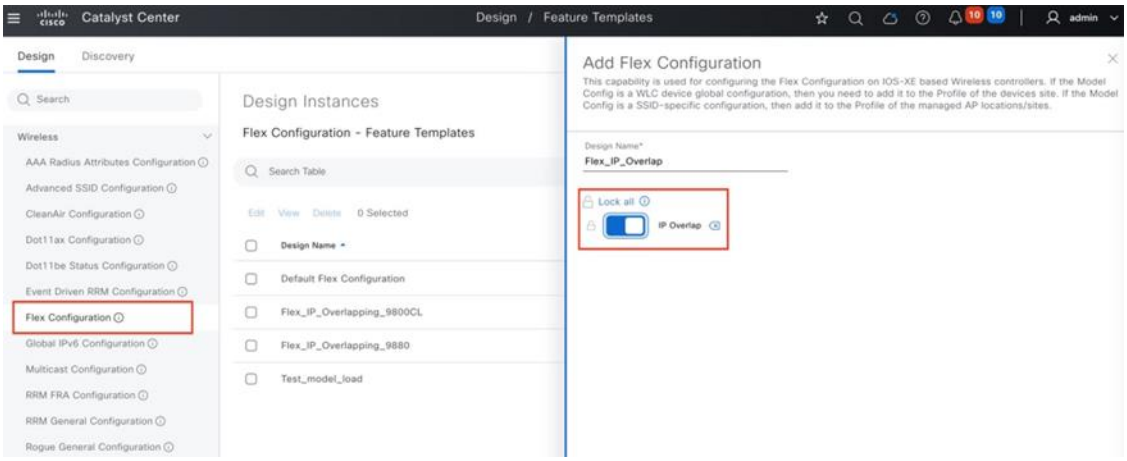
Procedure 2. To enable IP address overlap on Catalyst Center:

Step 1. Create a model configuration:

a. Choose **Design > Feature Templates > Flex Configuration**.

b. Click **Add** in the upper-right corner.

c. On the **Add Flex Configuration** slide-in pane, toggle on **IP Overlap** to enable IP address overlap.



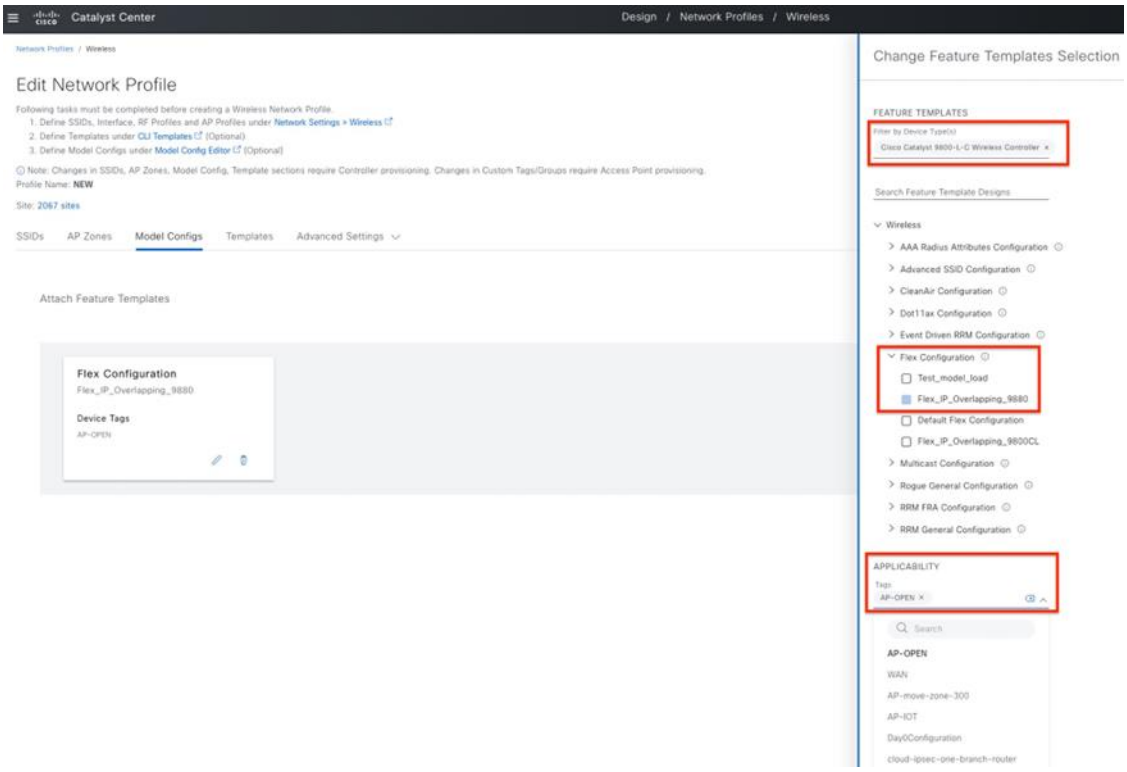
Step 2. Add the model configuration to network profiles:

a. From the main menu, choose **Design > Network Profiles**.

b. Choose the profile.

c. Choose **Model Config > Add Model Config**.

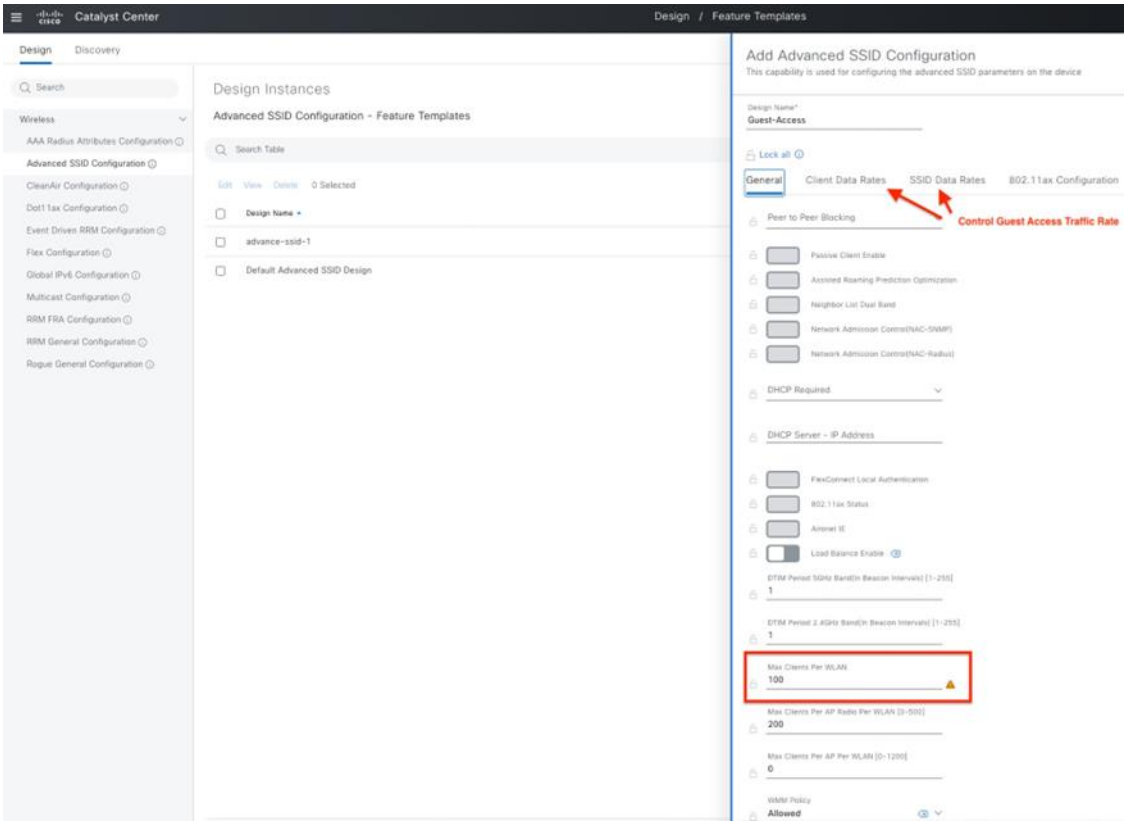
d. On the **Add Model Config** slide-in pane, choose the wireless controller type and FlexConnect model configuration and add the corresponding AP tags.



Remote location guest access

For remote stores, guest authentication cannot be done on a FlexConnect local authentication–enabled wireless LAN (WLAN). Instead, for guest access, a WLAN is set up with a centrally managed SSID tunneled back to a wireless controller in the DMZ zone. When associating a guest SSID to a profile on Catalyst Center, if an anchor wireless controller is checked, the **FlexConnectLocalSwitching** option is not available.

You can configure the max number of clients and max client data rate on a guest WLAN by choosing **Design > Feature Templates > Advanced SSID Configuration**. Then attach the model configuration to the network profiles, as displayed in this figure.



Local DHCP server

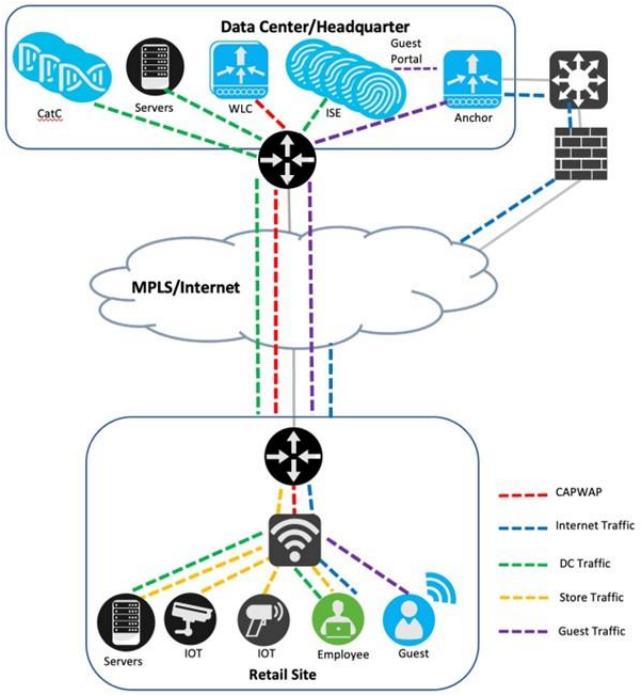
In a typical store site setup, a FlexConnect AP is linked to the local switch through a trunk interface with a native VLAN, and DHCP pools are set up on the local switch. The FlexConnect AP gets its IP address from the first DHCP pool (NATIVE) while the other DHCP pools (LOCAL-SWITCH) are reserved for wireless endpoints when they connect to a locally switched WLAN.

Location services by Cisco Spaces

Cisco Spaces is a location services platform that runs on the cloud and offers real-time location data and analytics for various industries. By using wireless APs and other network devices, the platform gathers data on individuals' movement and assets in physical spaces. Then this data is analyzed to generate insights into user behavior, traffic patterns, and other significant metrics. The Cisco Spaces Connector 2.3.4 was verified in a solution test. Currently, the Cisco Spaces Connector 3.0 does not support multiple interfaces.

Remote site traffic flow

When using the FlexConnect wireless deployment at remote store and warehouse sites, the traffic generated by business wireless endpoints is locally switched. AP Control and Provisioning of Wireless Access Points (CAPWAP) traffic and guest access are transmitted to the central wireless controller. Any store-to-store traffic is obstructed by the Cisco SD-WAN policy or TrustSec. Additionally, traffic to the internet and cloud-based applications can exit directly through the local internet link instead of being redirected to the data center. This can be achieved through the Cisco SD-WAN Direct Internet Access policies.



Cisco Intelligent Capture

Cisco Intelligent Capture (iCAP) offers real-time technical insights into various wireless metrics from the viewpoint of both the client and AP. iCAP provides a direct communication link between Catalyst Center and APs, enabling each of the APs to communicate with Catalyst Center directly. This channel allows Catalyst Center to receive packet capture (PCAP) data, AP and client statistics, and spectrum data, which may not be available through wireless controllers. With iCAP, even the most challenging wireless issues can be resolved effortlessly.

To integrate iCAP with Catalyst Center, see the *Cisco Intelligent Capture Deployment Guide*.

Ekahau integration

Ekahau can integrate with Catalyst Center through Ekahau AI Pro. This integration allows network engineers to design, plan, and optimize Wi-Fi networks using Ekahau AI Pro. After, they can export the design to Catalyst Center for deployment.

With this integration, Ekahau AI Pro can import network topology information and client information from Catalyst Center, allowing network engineers to design their Wi-Fi network based on real network data. Then Ekahau AI Pro can export the design to Catalyst Center, where the network can be deployed and managed.

Also, this integration enables Ekahau AI Pro to receive network configuration information from Catalyst Center, such as the locations of APs and their associated configuration settings. This allows network engineers to easily monitor the wireless network and identify areas that require optimization.

Overall, the Ekahau AI Pro integration with Catalyst Center provides network engineers with a streamlined, efficient process for designing, planning, and optimizing Wi-Fi networks.

If you are using Catalyst Center-exported Ekahau projects, the schema version 1.7 used in Ekahau AI Pro Version 11.1.0 and later is not compatible. Although Ekahau AI Pro doesn't provide a support statement, you can use the earlier Version 11.0.2.219, which is compatible with the exported projects. We recommend using the supported version until the latest schema version is supported.

Latency impact

Latency can have a significant impact on retail operations and affect customer satisfaction. To ensure optimal performance, the round-trip latency between the AP and controller must not exceed 300 ms, and CAPWAP control packets should have priority over all other traffic. When it isn't possible to achieve the 300-ms round-trip latency, a practical solution is to configure the AP to perform local authentication.

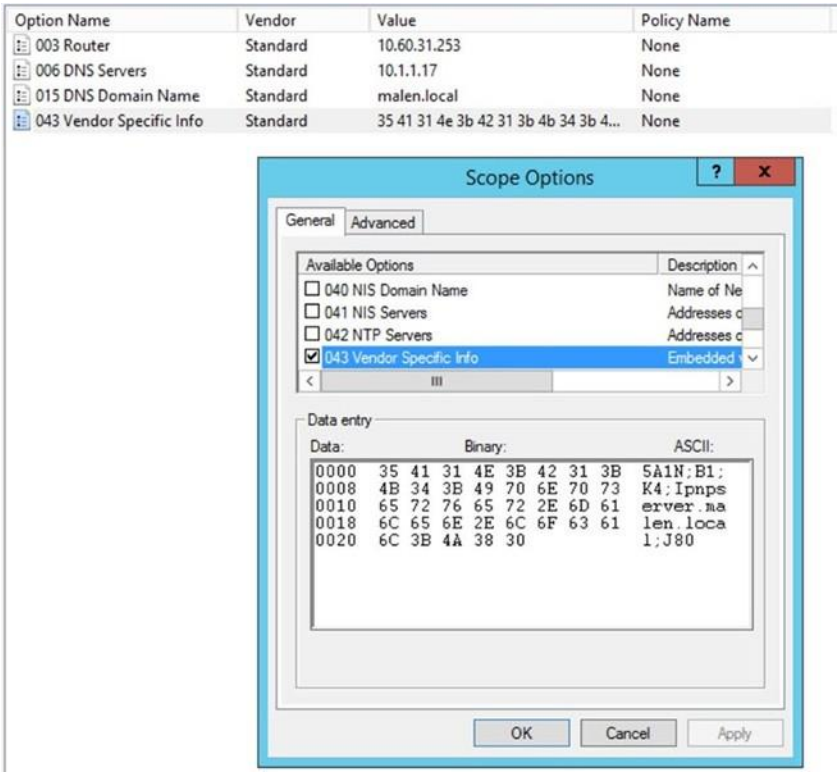
Onboard devices with Plug and Play

Plug and Play provisioning provides a way to automatically and remotely provision and onboard network devices with minimal network administrator and field personnel involvement.

If the Catalyst Center system certificate is issued by an external CA server, its common name (CN) should include the `pnpserver` hostname. Before starting Plug and Play, the DHCP pool should contain the option 43 string with the FQDN, B1, DNS server, and domain name.

See this sample DHCP pool configuration on a Cisco switch:

```
ip dhcp pool PnP_Pool network
214.2.64.0255.255.255.0
default-router 214.2.64.1
option 43 ascii "5A1D;B1;K4;Ipnpserver.<domain-name>;J80;"
domain-name <domain-name> dns-server <dns-server>
```



For details, see the Cisco Catalyst Center User Guide.

Configure access points workflow

To prevent Catalyst Center from running out of memory (OOM), we recommend that you limit the selection of APs to 2000 at a time when using the Configure Access Points workflow.

Technical references

FlexConnect Catalyst Wireless Branch Deployment Guide

Cisco Extended Enterprise Non-Fabric and SD-Access Fabric Design Guide

Cisco Catalyst Center Administrator Guide

Cisco Catalyst Assurance User Guide

Cisco Spaces