Application Hosting on Catalyst Access Points

Deployment Guide

Contents

Overview

Enterprise wireless networks are a rapidly growing part of today’s technology. They are becoming more mission-critical each day as new companies migrate to wireless solutions as a means to run their business. As wireless networks grow exponentially, we as a society are becoming more connected than ever before, giving us the ability to solve once seemingly complex problems with simple yet elegant solutions. However, these endless technological possibilities have also triggered a surge of both dependency and the expectation that technology must continue to better every aspect of our daily lives. The Internet of Things (IoT) has arisen, in part, as a result of these expectations, and Cisco’s state-of-the-art technology known as Application Hosting on Catalyst Access Points was created to help spearhead this movement.

Cisco’s Application Hosting on Catalyst Access Points feature provides users with the ability to load third-party containerized Cisco® IOx applications directly onto Cisco Catalyst™ access points and to leverage them as an IoT gateway. Once loaded, the third-party application gains complete access to specific access point software and hardware resources. Depending on the IOx application developed, it is able to promptly communicate with third-party software through its internal VLAN, or with hardware through its external-facing USB port. A typical business running a Cisco powered wireless infrastructure will have access points deployed throughout all employee-inhabited facilities. Giving third-party vendors the ability to create applications and leverage these access points as IoT gateways has created endless possibilities for the IoT movement.

This document covers the deployment of Application Hosting on Catalyst Access Points feature with Cisco Catalyst Center.

Disclaimer: Cisco claims customer support for any application lifecycle management issues; however, for any problems related to a Cisco partner’s IoT USB connector, application server, or IoT device, please reach out to them directly.

Supported software

Table 1. Cisco Catalyst Center and Cisco IOS® XE software compatibility matrix

Cisco Catalyst Center software release	Cisco IOS XE WLC software release
2.1.2.x and above	17.3.1 and above

Supported hardware

Table 2. Supported access points

Access point product ID	OS type
C9105AXI	AP-COS
C9105AXW	AP-COS
C9115AX	AP-COS
C9117AX	AP-COS
C9120AX	AP-COS
C9130AX	AP-COS
C9124AX	AP-COS

Access point product ID	OS type
C9136I	AP-COS
C9162I	AP-COS
C9164I	AP-COS
C9166I	AP-COS

Note: C9136I is supported starting from Cisco IOS XE Release 17.7.1.

Note: CW9164I/9166I is supported starting from Cisco IOS XE Release 17.9.1.

Note: CW9162I is supported starting from Cisco IOS XE Release 17.9.2/17.10.1.

Note: CW9166D1 is supported starting from Cisco IOS XE Release 17.12.1.

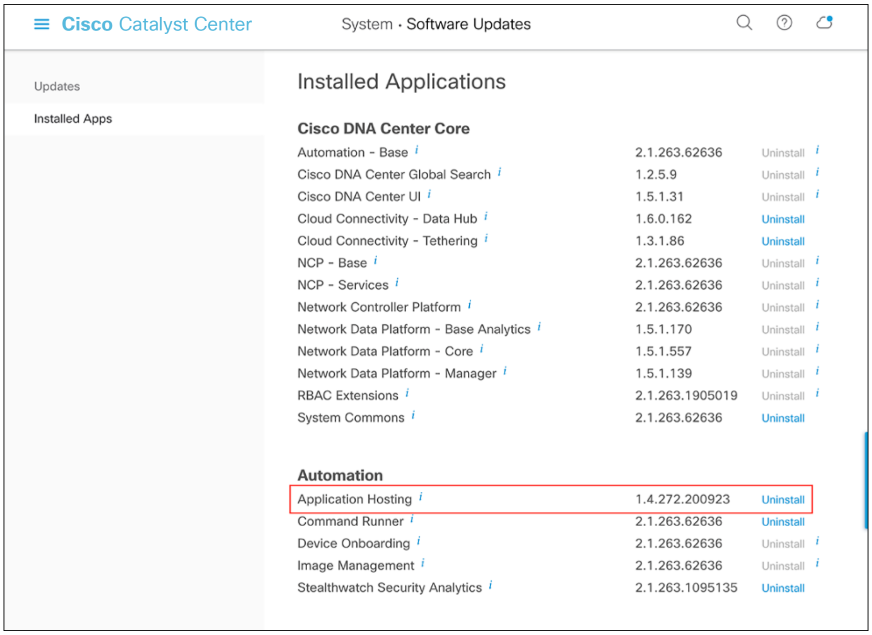
Table 3. Supported wireless LAN controllers

Wireless LAN controller product ID	OS type
C9800-CL	Cisco IOS XE
C9800-L	Cisco IOS XE
C9800-40	Cisco IOS XE
C9800-80	Cisco IOS XE

Prerequisite: Installing the Application Hosting package from Cisco Catalyst Center

Cisco Catalyst Center provides the option to download a package called **Application Hosting**. You can download and install this package on top of the base Cisco Catalyst Center software.

- To install the Application Hosting package, log in to Cisco Catalyst Center and open the menu in the top left corner.
- Click System > Software Updates, then click Installed Apps on the left. Scroll down to Automation and you will find the package available for download or installation (**Figure 1**).



≡ Cisco Catalyst Center   System · Software Updates

Updates

Installed Apps

Installed Applications

Cisco DNA Center Core

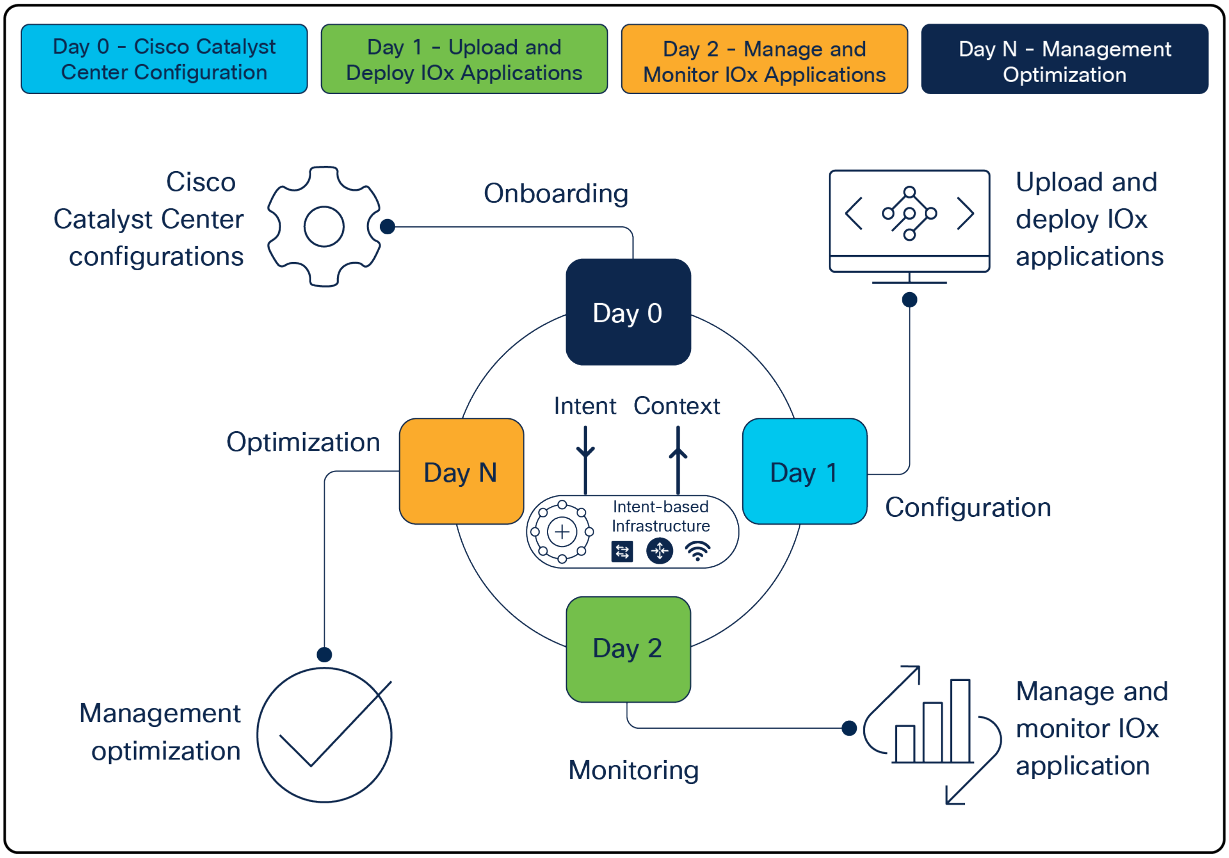
Automation - Base	2.1.263.62636	Uninstall
Cisco DNA Center Global Search	1.2.5.9	Uninstall
Cisco DNA Center UI	1.5.1.31	Uninstall
Cloud Connectivity - Data Hub	1.6.0.162	Uninstall
Cloud Connectivity - Tethering	1.3.1.86	Uninstall
NCP - Base	2.1.263.62636	Uninstall
NCP - Services	2.1.263.62636	Uninstall
Network Controller Platform	2.1.263.62636	Uninstall
Network Data Platform - Base Analytics	1.5.1.170	Uninstall
Network Data Platform - Core	1.5.1.557	Uninstall
Network Data Platform - Manager	1.5.1.139	Uninstall
RBAC Extensions	2.1.263.1905019	Uninstall
System Commons	2.1.263.62636	Uninstall

Automation

Application Hosting	1.4.272.200923	Uninstall
Command Runner	2.1.263.62636	Uninstall
Device Onboarding	2.1.263.62636	Uninstall
Image Management	2.1.263.62636	Uninstall
Stealthwatch Security Analytics	2.1.263.1095135	Uninstall

Figure 1.
Location of the Application Hosting package

High-level deployment workflow



Day 0 - Cisco Catalyst Center Configuration
Day 1 - Upload and Deploy IOx Applications
Day 2 - Manage and Monitor IOx Applications
Day N - Management Optimization
Cisco Catalyst Center configurations
Onboarding
Upload and deploy IOx applications
Day 0
Intent
Context
Optimization
Day N
Day 1
Intent-based Infrastructure
Configuration
Day 2
Management optimization
Monitoring
Manage and monitor IOx application

Figure 2.
Steps for deploying Application Hosting

Day 0: Cisco Catalyst Center configurations

Note: Skip to day 1 if you have already completed day-0 Cisco Catalyst Center configuration.

- Create a network hierarchy site (area, building, floors) via the Network Hierarchy page.
- Optional: Configure the network hierarchy settings via the Network Settings page.
- Discover the wireless controller (WLC) and access points via the Discovery page.
- Assign the WLC and access points to the network hierarchy created via the Inventory page.

Day 1: Upload and deploy IOx applications

- Upload a third-party IOx application to Cisco Catalyst Center via the IoT Services page.
- Deploy the uploaded application to specific access points.

Day 2: Manage and monitor IOx applications

- Establish communication between the third-party application and its application server.
- Begin managing and monitoring the applications deployed on the access points.

Day N: Optimize management

- Validate how the deployed applications are performing in the field.
- Develop software enhancements based on analysis and upgrade your applications.
- Repeat the deployment workflow from day 1.

Topology

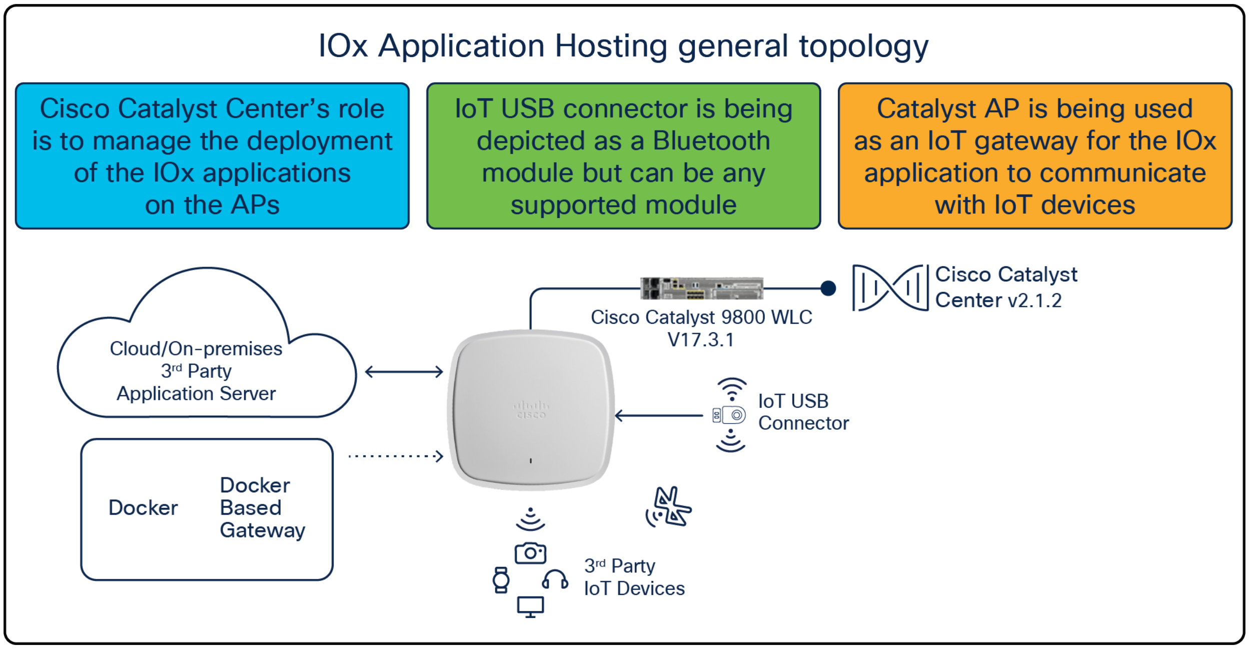

IOx Application Hosting general topology
Cisco Catalyst Center's role is to manage the deployment of the IOx applications on the APs
IoT USB connector is being depicted as a Bluetooth module but can be any supported module
Catalyst AP is being used as an IoT gateway for the IOx application to communicate with IoT devices
Cisco Catalyst Center v2.1.2
Cisco Catalyst 9800 WLC V17.3.1
Cloud/On-premises 3rd Party Application Server
IoT USB Connector
Docker
Docker Based Gateway
3rd Party IoT Devices

Figure 3.
IOx Application Hosting general topology

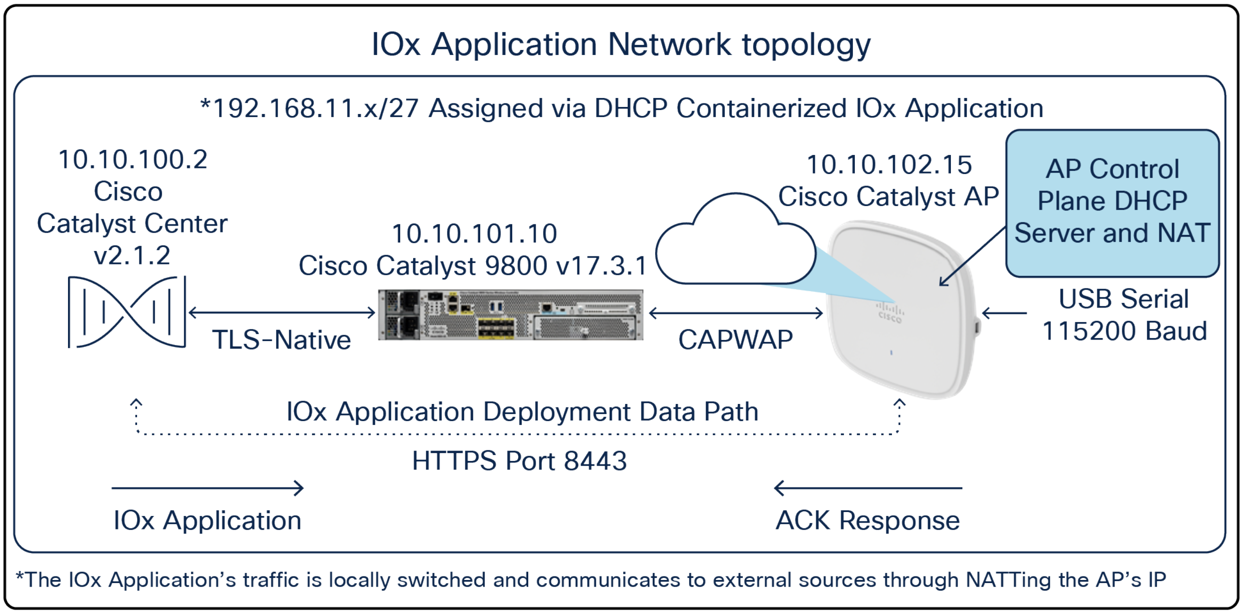

IOx Application Network topology
*192.168.11.x/27 Assigned via DHCP Containerized IOx Application
10.10.100.2
Cisco
Catalyst Center
v2.1.2
10.10.101.10
Cisco Catalyst 9800 v17.3.1
10.10.102.15
Cisco Catalyst AP
AP Control
Plane DHCP
Server and NAT
TLS-Native
CAPWAP
USB Serial
115200 Baud
IOx Application Deployment Data Path
HTTPS Port 8443
IOx Application
ACK Response
*The IOx Application's traffic is locally switched and communicates to external sources through NATTing the AP's IP

Figure 4.
IOx Application Hosting network topology

By default, your application will receive an IP address from 192.168.11.x/27 through Dynamic Host Configuration Protocol (DHCP) and communicates externally from your access point through Network Address Translation (NAT). This means that the IOx application will by default have the same IP address as the access point from the perspective of external applications. If this is an issue, please refer to the data segmentation section below.

Data segmentation

This section provides you with information about how the IOx application's data is segmented when communicating externally from the access point.

With default settings, the IOx application deployed on the access point will communicate externally by using NAT to translate the AP's management IP (**Figure 5**.). While this works fine, since the IOx application's data uses the same VLAN as the access point's traffic, there is no segmentation.

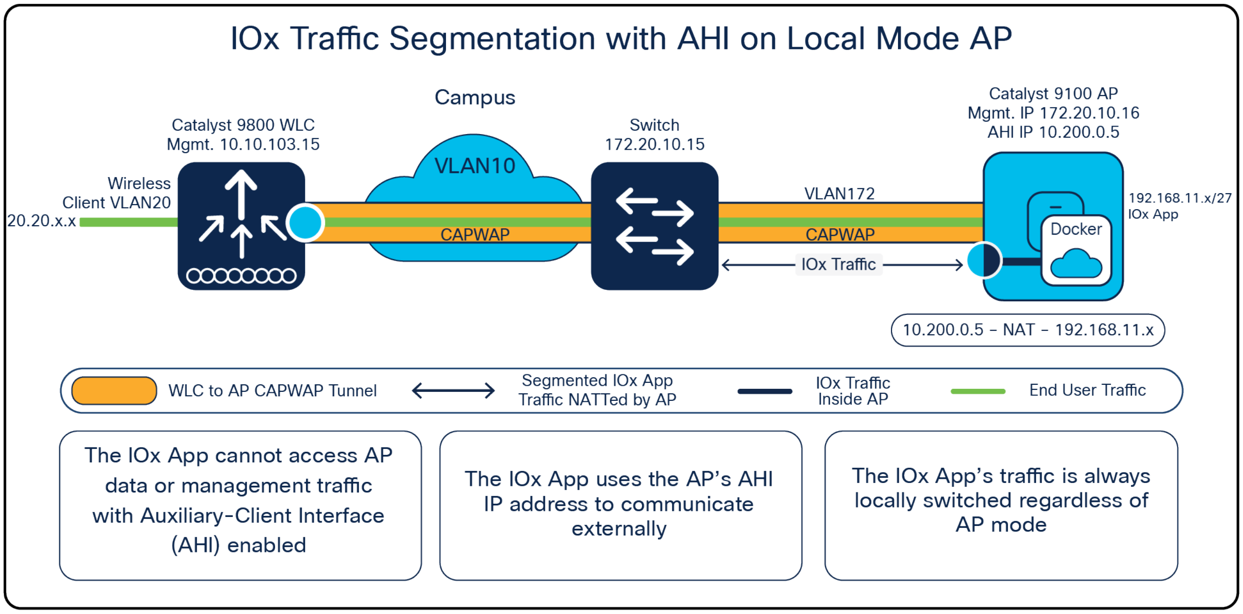

IOx Traffic Segmentation with AHI on Local Mode AP
Campus
VLAN10
CAPWAP
Catalyst 9800 WLC
Mgmt. 10.10.103.15
Wireless
Client VLAN20
20.20.x.x
Switch
172.20.10.15
VLAN172
CAPWAP
IOx Traffic
Catalyst 9100 AP
Mgmt. IP 172.20.10.16
AHI IP 10.200.0.5
Docker
192.168.11.x/27
IOx App
10.200.0.5 – NAT – 192.168.11.x
WLC to AP CAPWAP Tunnel
Segmented IOx App Traffic NATTed by AP
IOx Traffic Inside AP
End User Traffic
The IOx App cannot access AP data or management traffic with Auxiliary-Client Interface (AHI) enabled
The IOx App uses the AP's AHI IP address to communicate externally
The IOx App's traffic is always locally switched regardless of AP mode

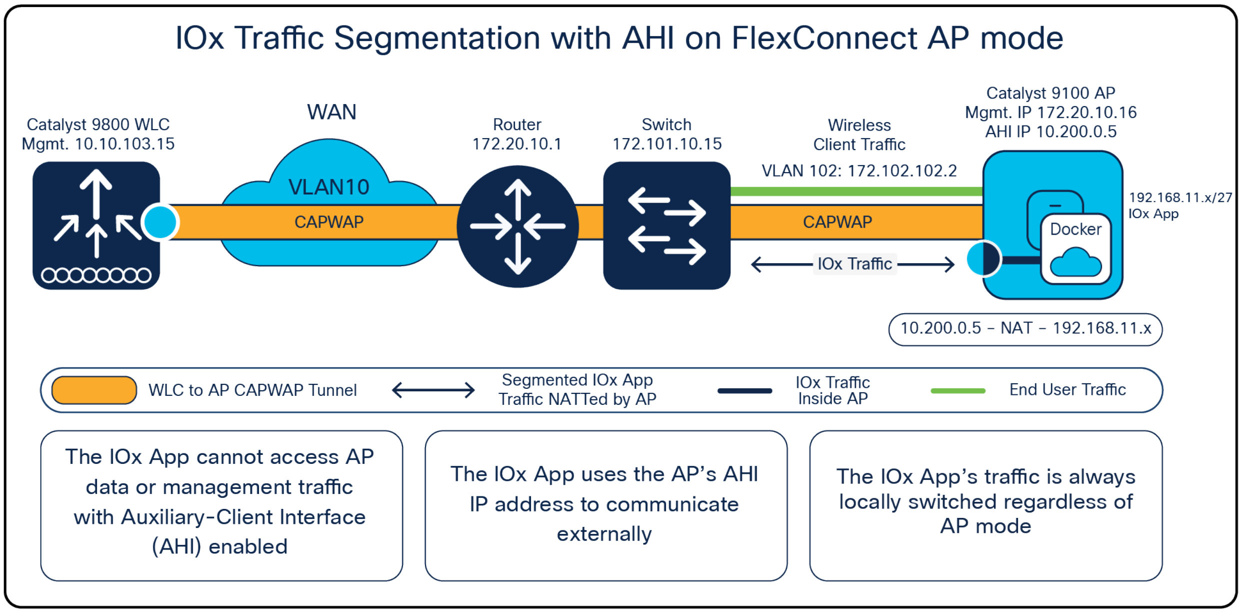
Figure 5.
IOx traffic segmentation on a Local Mode access point

To configure proper segmentation, we can configure something known as an auxiliary-client interface (AHI) on an access point group within your WLC that's associated with your Application Hosting access points.

```
Nolan_eWLC#config terminal
Nolan_eWLC(config)# <AP Join Profile Name>
Nolan_eWLC(config-ap-profile)# auxiliary-client interface vlan-id <VLAN ID>
```

Note: Ensure that the VLAN ID included in the command above exists within your controller.

After AHI is configured for your access point group, all access points within the access point group will now acquire an IP address from the AHI VLAN's DHCP pool. When the IOx application needs to communicate externally, it will do so through the AHI's IP rather than the access point's management IP. Since the IOx application and the access point's traffic now use different VLAN IDs, there is proper segmentation between the two. Observe that the same concept applies whether the access point is in Local or Cisco FlexConnect® mode and a Cisco fabric deployment. (see **Figure 6** and **Figure 7.**)

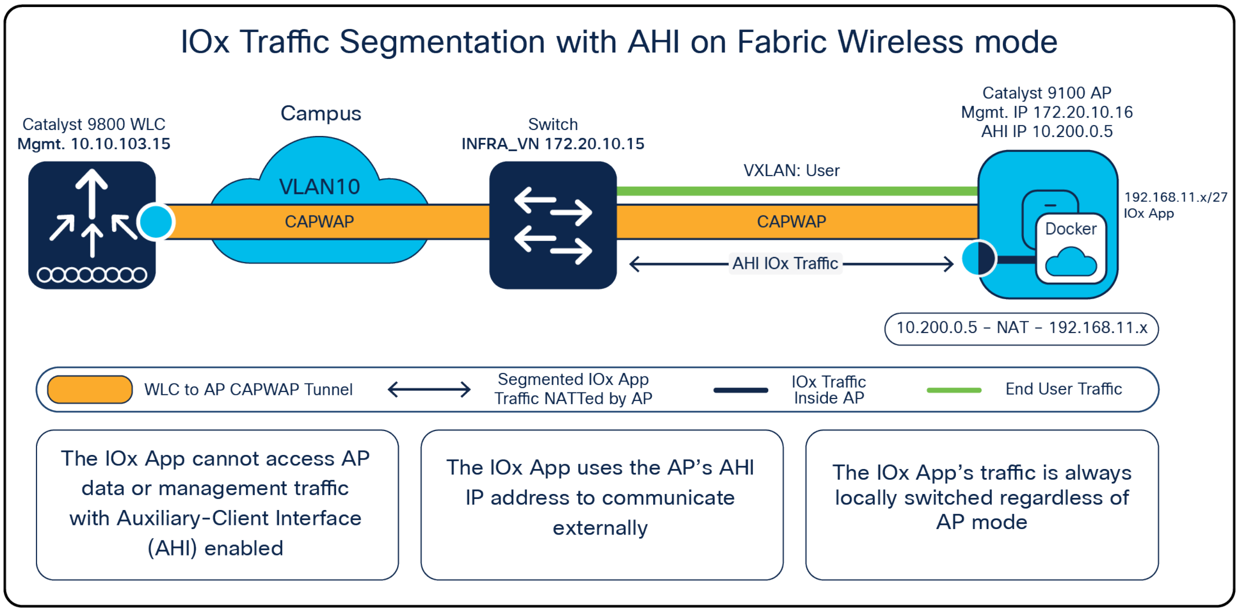


The IOx App cannot access AP data or management traffic with Auxiliary-Client Interface (AHI) enabled

The IOx App uses the AP's AHI IP address to communicate externally

The IOx App's traffic is always locally switched regardless of AP mode

Figure 6.
IOx traffic segmentation with an auxiliary-client interface configured on a FlexConnect Mode access point



The IOx App cannot access AP data or management traffic with Auxiliary-Client Interface (AHI) enabled

The IOx App uses the AP's AHI IP address to communicate externally

The IOx App's traffic is always locally switched regardless of AP mode

Figure 7.
IOx traffic segmentation with an auxiliary-client interface configured in Fabric Wireless Mode

Day 0: Set up the Cisco Catalyst Center configuration

This section provides step-by-step instructions for the day-0 configuration necessary to begin using Application Hosting on Catalyst Access Points.

Note: Skip to the day-1 section if you have already completed day-0 Cisco Catalyst Center configuration.

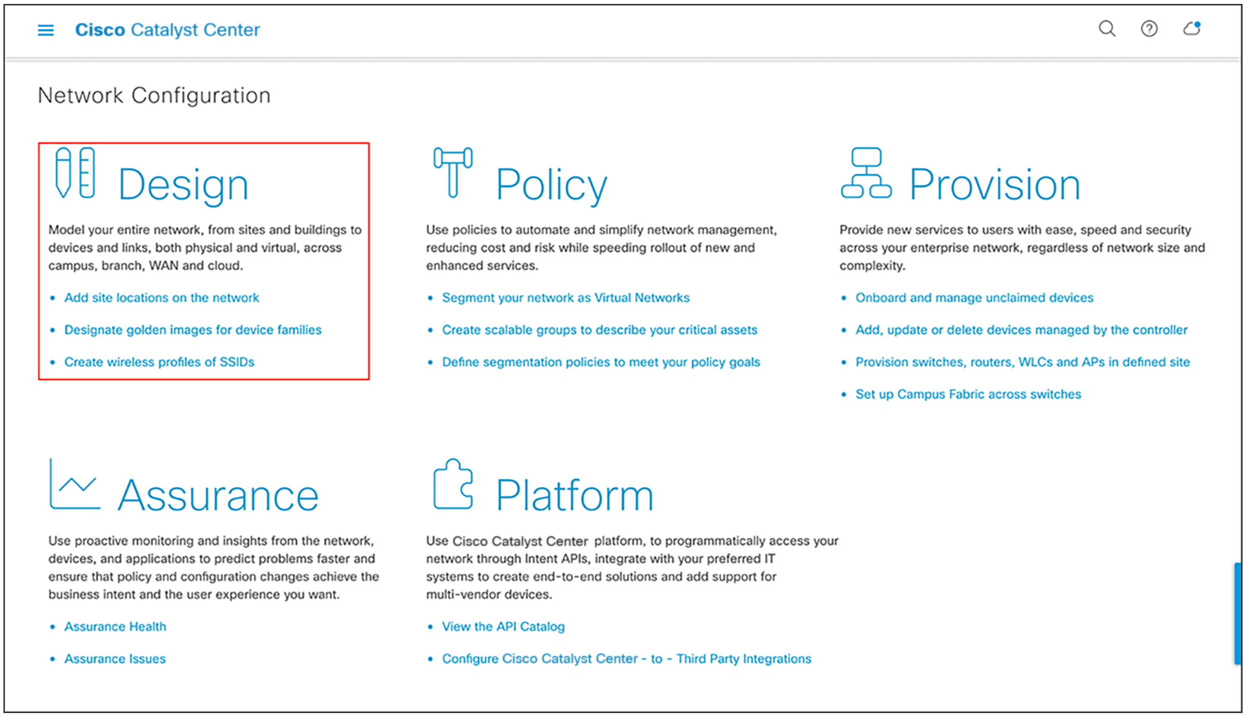
Part 1: Day-0 configuration – Building a site hierarchy

Description: Cisco Catalyst Center's Design page provides a robust design application that allow customers of every size and scale to easily define their physical sites and common resources.

Section goals: Create and configure network hierarchy sites and settings to define shared services, device credentials, and Simple Network Management Protocol (SNMP) community strings.

Step 1: Navigate to the Network Hierarchy page

- Option 1: Log in to Cisco Catalyst Center. Scroll down to the Network Configuration section and choose Design (**Figure 8**).
- Option 2: Click on the menu in the top left corner of the screen. Click Design and then Network Hierarchy (**Figure 9**).



Network Configuration

Design

Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.

- Add site locations on the network
- Designate golden images for device families
- Create wireless profiles of SSIDs

Policy

Use policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.

- Segment your network as Virtual Networks
- Create scalable groups to describe your critical assets
- Define segmentation policies to meet your policy goals

Provision

Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.

- Onboard and manage unclaimed devices
- Add, update or delete devices managed by the controller
- Provision switches, routers, WLCs and APs in defined site
- Set up Campus Fabric across switches

Assurance

Use proactive monitoring and insights from the network, devices, and applications to predict problems faster and ensure that policy and configuration changes achieve the business intent and the user experience you want.

- Assurance Health
- Assurance Issues

Platform

Use Cisco Catalyst Center platform, to programmatically access your network through Intent APIs, integrate with your preferred IT systems to create end-to-end solutions and add support for multi-vendor devices.

- View the API Catalog
- Configure Cisco Catalyst Center - to - Third Party Integrations

Figure 8.
Location of the Design page on Cisco Catalyst Center's homepage

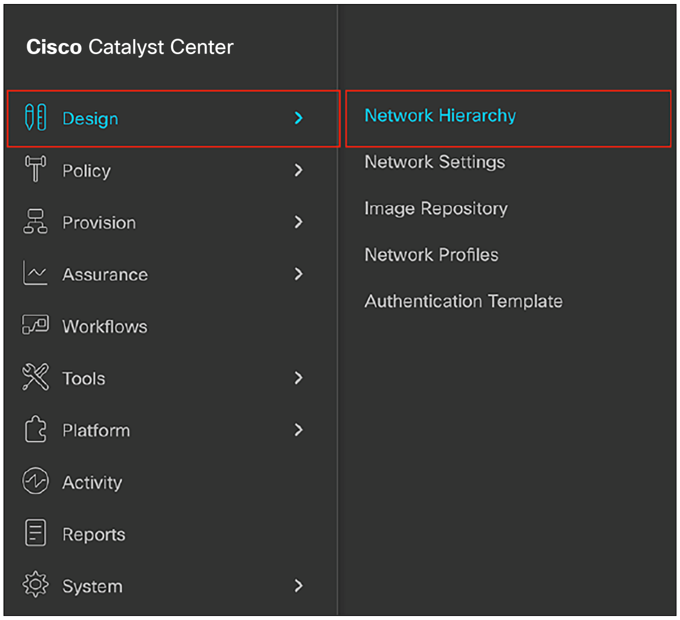


Figure 9.
Location of Network Hierarchy from the menu

Step 2: Create sites, building, and floors

To allow Cisco Catalyst Center to group devices based on location, begin by laying out a hierarchy of areas, building, and floors as required to accurately represent the location of your network. A site hierarchy lets you enable unique network settings and IP spaces for different groups of devices.

- Option 1: To create a site, click the Add Site button (**Figure 10**). A menu will open up providing an option to create a child area, building, or floor within a desired site.
- Option 2: To create a site, click the gear icon (**Figure 11**) next to the site under which you would like to create a child site.
- When creating a floor, click Upload file to upload a floor of a building (**Figure 12**).
- Floor plans must be in the DXF, DWG, JPG, GIF, or PNG format.

The behavior of Cisco Catalyst Center is to inherit settings from the global level into subsequent levels in the hierarchy. This enables consistency across large domains while providing administrators the flexibility to adapt and change an individual building or floor.

Notes:

- You can create areas and buildings only within the Global site or other areas, and can create floors only within buildings.
- When creating a building within a design hierarchy, it is critical that you use a real physical street address for your sites. Cisco Catalyst Center uses the street address to select the country codes for the wireless implementation.

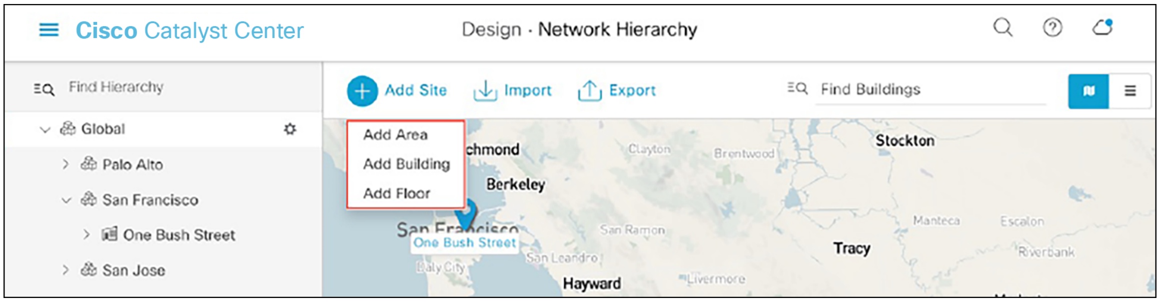


Figure 10.
Clicking Add Site within the Design – Network Hierarchy page

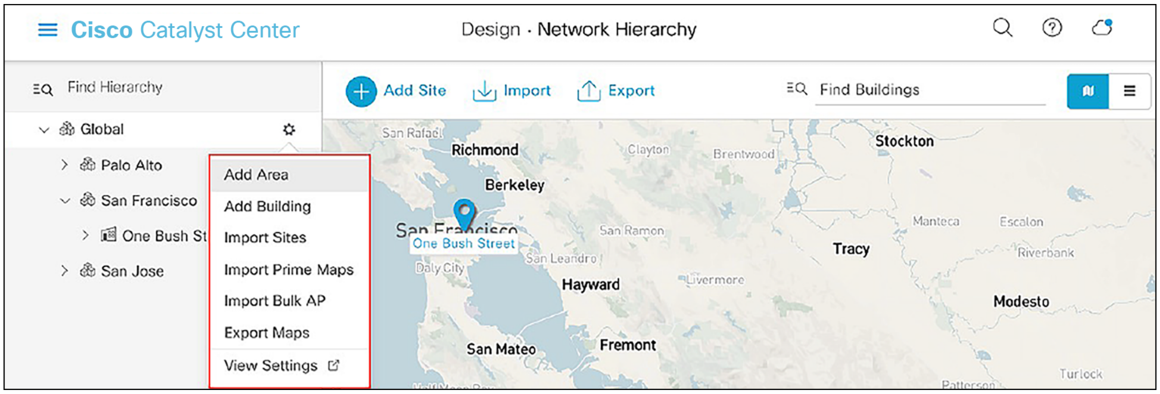
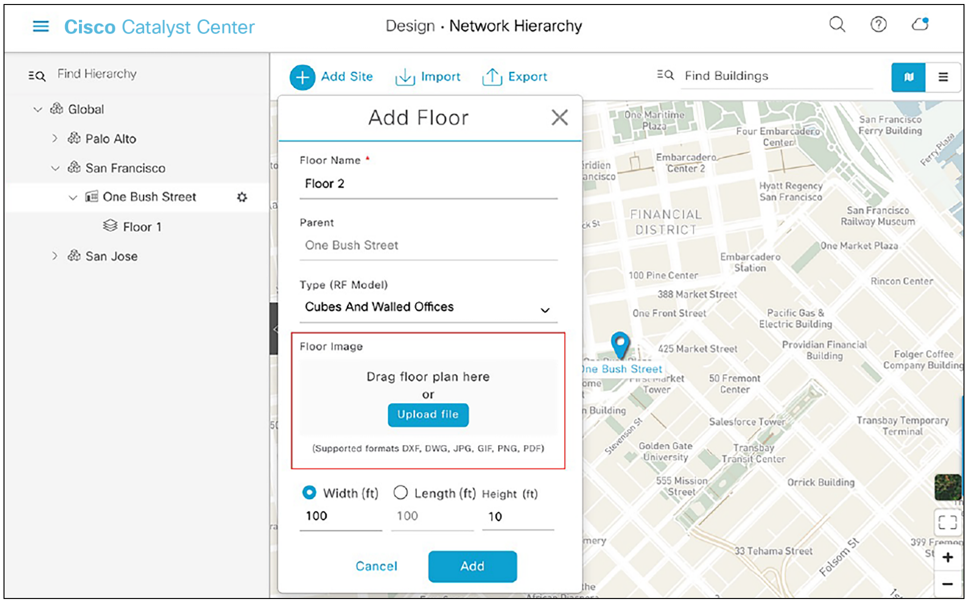


Figure 11.
Clicking the gear icon next to an area within the Design – Network Hierarchy page



Floor Name * Floor 2

Parent One Bush Street

Type (RF Model) Cubes And Walled Offices

Floor Image
Drag floor plan here
or
Upload file
(Supported formats DXF, DWG, JPG, GIF, PNG, PDF)

● Width (ft) 100 ○ Length (ft) 100 Height (ft) 10

Figure 12.
Location of the Upload file button to upload a floor plan during floor creation

Step 3: Navigate to the Network Settings page

Cisco Catalyst Center lets you save common resources and settings with the Network Settings application. Information pertaining to the enterprise can be stored and reused across the network.

- To navigate to the Network Settings page, open the menu in the top left corner of the screen. Click Design and then Network Settings (**Figure 13**).

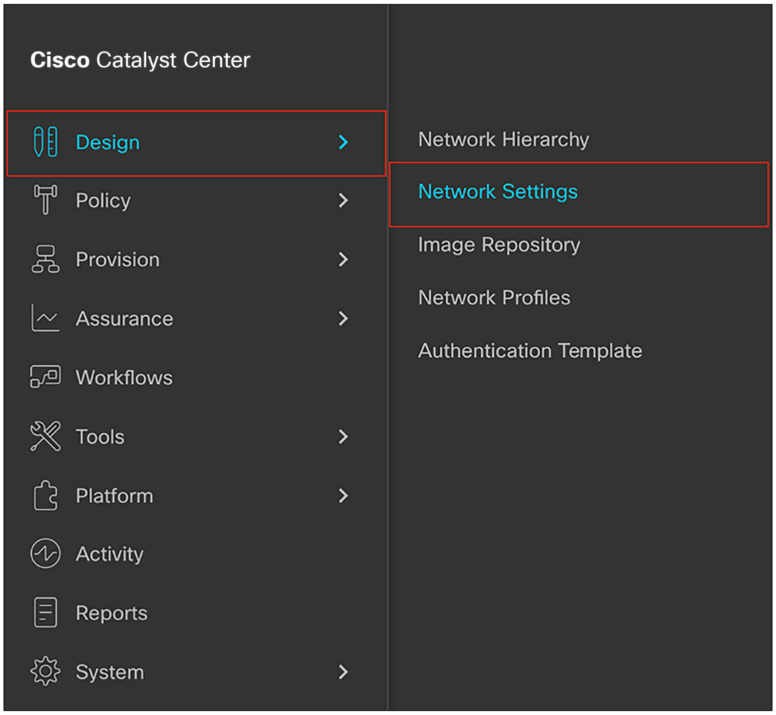
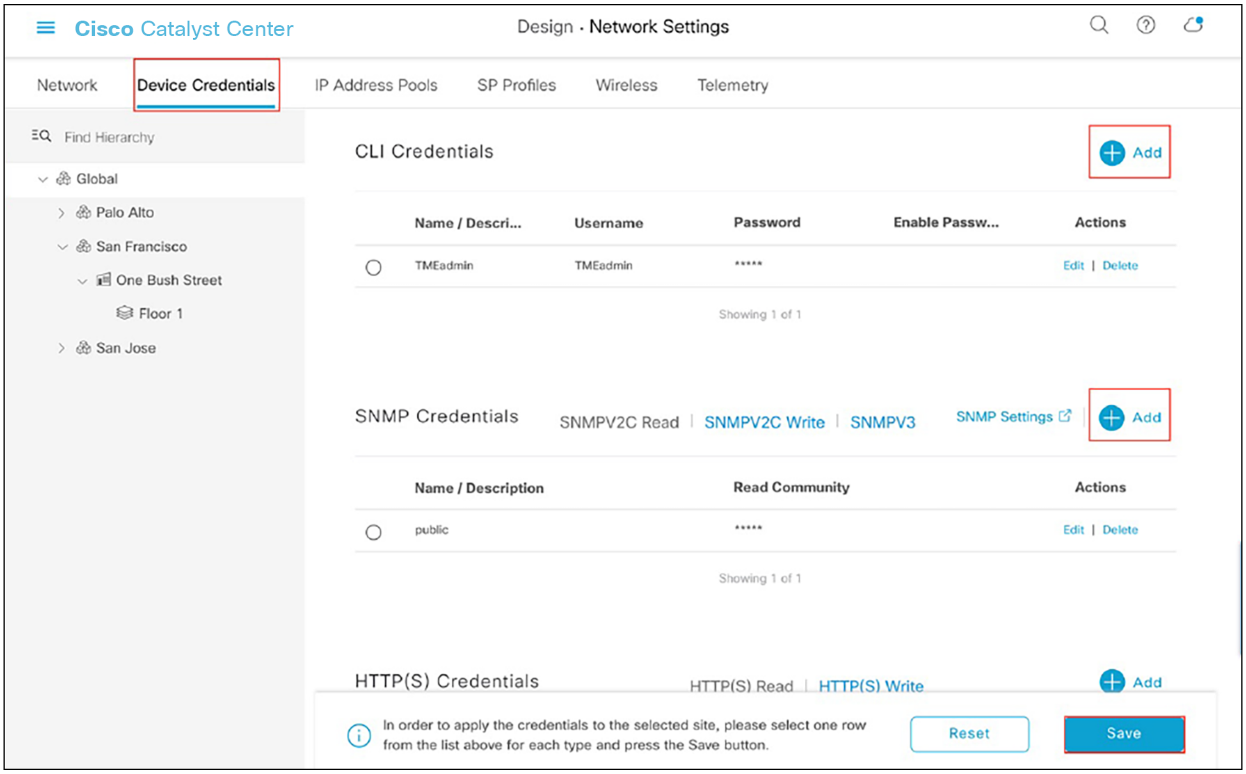


Figure 13.
Location of Network Settings from the menu

Step 4: Configure network settings and device credentials

This is where you configure all device-related network settings. By default, Cisco Catalyst Center's IP address is pre-populated in the Syslog Server and SNMP Server fields. This will enable syslog and Simple Network Management Protocol (SNMP) traps to be sent to Cisco Catalyst Center from network devices when a WLC is added to Cisco Catalyst Center.

- Click the Device Credentials sub-tab to view the existing device Command-Line Interface (CLI) credentials and SNMP community strings (**Figure 14**).
- Click the Add button to create new credential entries using the CLI Credentials form (**Figure 15**). Cisco Catalyst Center uses these credentials to discover the network devices.



CLI Credentials

	Name / Descri...	Username	Password	Enable Passw...	Actions
○	TMEadmin	TMEadmin	*****		Edit | Delete

Showing 1 of 1

SNMP Credentials

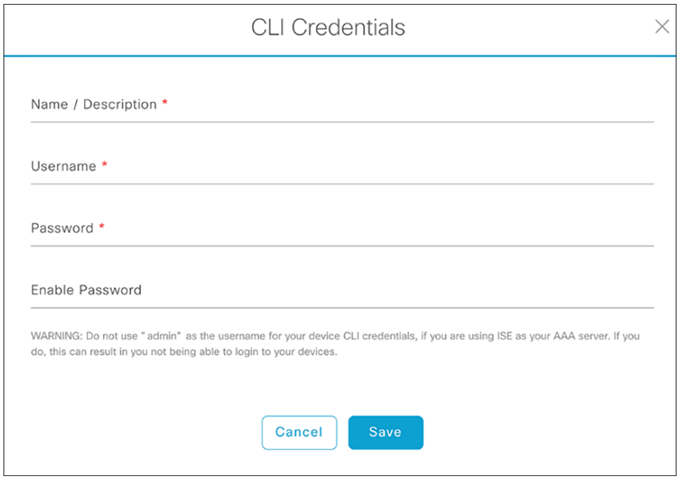
	Name / Description	Read Community	Actions
○	public	*****	Edit | Delete

Showing 1 of 1

HTTP(S) Credentials

In order to apply the credentials to the selected site, please select one row from the list above for each type and press the Save button.

Figure 14.
Adding device credentials to the network settings



CLI Credentials

Name / Description *

Username *

Password *

Enable Password

WARNING: Do not use "admin" as the username for your device CLI credentials, if you are using ISE as your AAA server. If you do, this can result in you not being able to login to your devices.

Figure 15.
CLI Credentials form

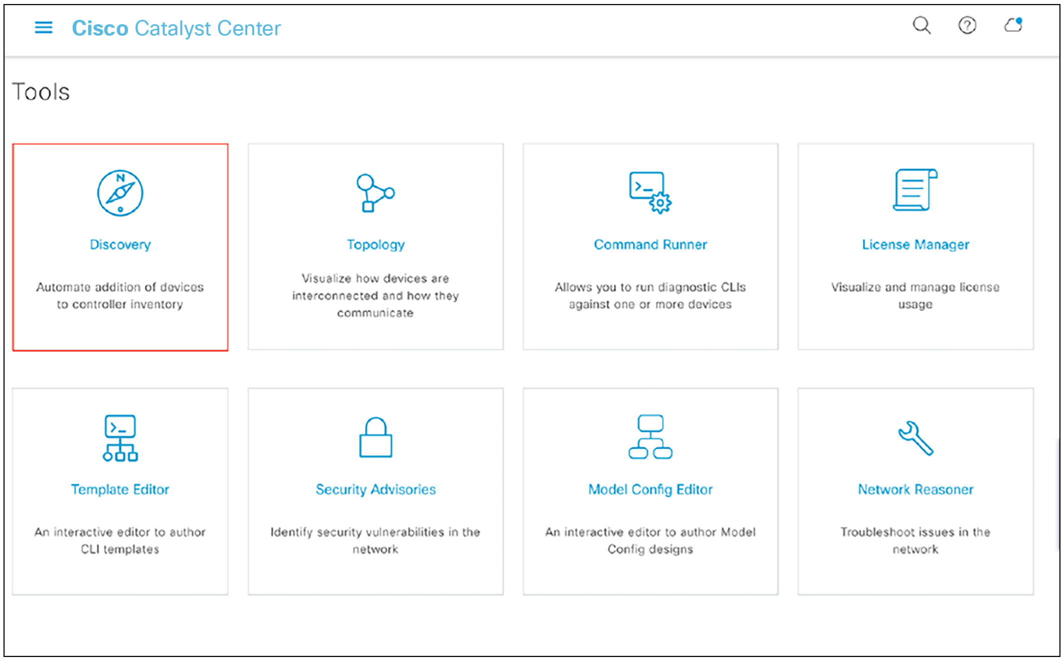
Part 2: Day-0 configuration – Discovery and inventory

Description: Cisco Catalyst Center’s **Discovery** application allows a network administrator to add their network device to the platform.

Section goals: Discover the WLC and access points and assign them to the site created in the previous section.

Step 1: Navigate to the Discovery application

- Option 1: From the homepage, scroll down to the bottom and click Discovery and then Add Discovery (**Figures 16** and **17**).
- Option 2: Click on the menu in the top left corner of the screen. Click Tools and then Discovery (**Figure 18**).



Discovery
Automate addition of devices to controller inventory

Topology
Visualize how devices are interconnected and how they communicate

Command Runner
Allows you to run diagnostic CLIs against one or more devices

License Manager
Visualize and manage license usage

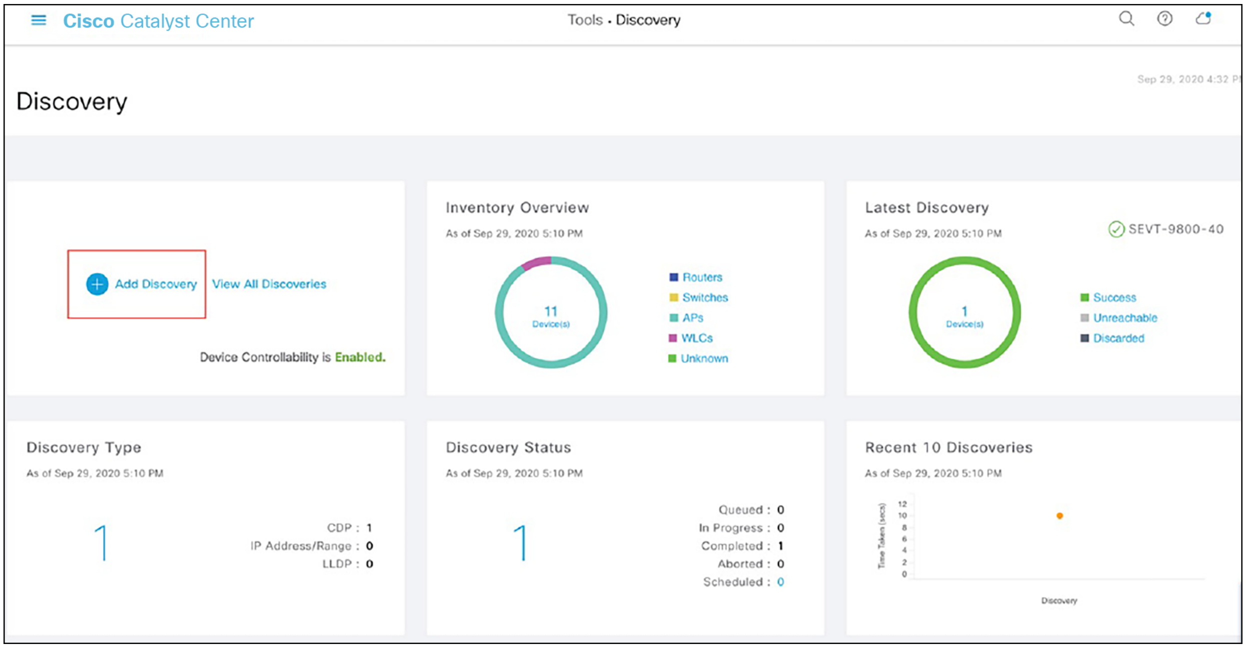
Template Editor
An interactive editor to author CLI templates

Security Advisories
Identify security vulnerabilities in the network

Model Config Editor
An interactive editor to author Model Config designs

Network Reasoner
Troubleshoot issues in the network

Figure 16.
Location of Discovery button on the Cisco Catalyst Center homepage



Device Controllability is Enabled.

As of Sep 29, 2020 5:10 PM

Discovery Type: 1
CDP : 1
IP Address/Range : 0
LLDP : 0

Discovery Status: 1
Queued : 0
In Progress : 0
Completed : 1
Aborted : 0
Scheduled : 0

Figure 17.
Location of the Add Discovery button on the Tools – Discovery page

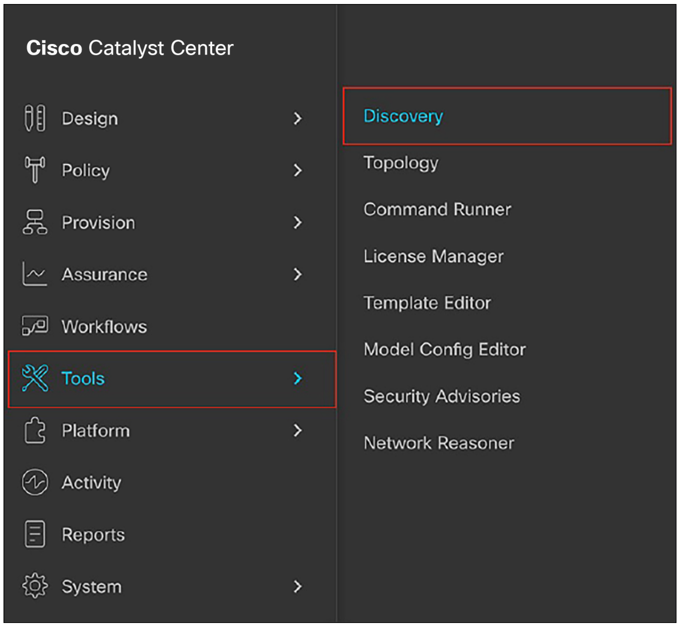


Figure 18.
Location of Discovery within the menu

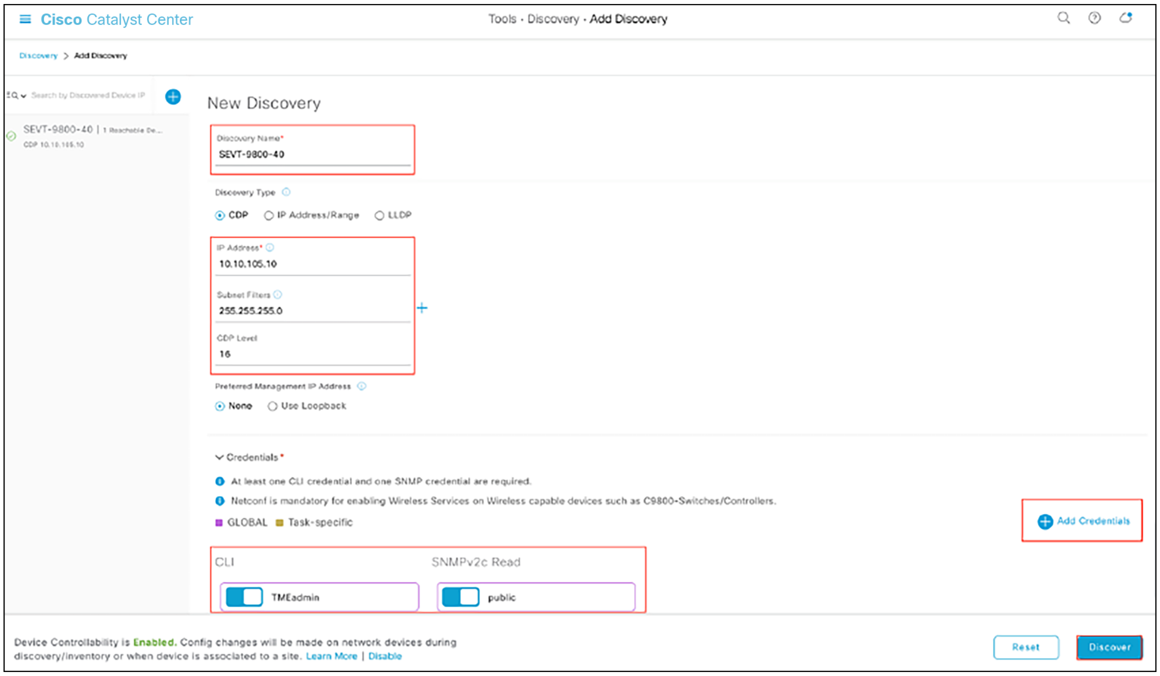
Step 2: Discover controllers and access points and add them to Cisco Catalyst Center

To discover a WLC and add it to Cisco Catalyst Center, follow the steps below (**Figure 19**):

- Enter a Discovery name (any unique name for the purpose of classification on the Discovery page).
- Enter either a single IP address or a range of IP addresses via one of the protocols (Cisco Discovery Protocol, range, or Link Layer Discovery Protocol [LLDP]).
- **Warning: The WLC and access points must be on a routable network to Cisco Catalyst Center for Application Hosting on Catalyst Access Points to work. NAT networks are NOT supported, and neither are fabric networks.**
- Enter the SSH username and password and SNMP read and write credentials (by clicking Add Credentials).
- If you're discovering a Cisco IOS XE controller, enter the NETCONF port as 830 and run the following commands on the controller CLI:
  - aaa new-model
  - aaa authentication login default local
  - aaa authorization exec default local
- When the details are filled in, click the Discover button.

Notes:

- When you discover a WLC, all of its joined access points will also be discovered and added to Cisco Catalyst Center's inventory.
- All the CLI credentials defined in the Design section are displayed here on the Discovery page.



Cisco Catalyst Center
Tools · Discovery · Add Discovery
Discovery > Add Discovery
Search by Discovered Device IP
SEVT-9800-40 | 1 Reachable De...
CDP 10.10.105.10
New Discovery
Add Credentials
Reset
Discover

Discovery Name*: SEVT-9800-40

Discovery Type: ● CDP ○ IP Address/Range ○ LLDP

IP Address*: 10.10.105.10

Subnet Filters: 255.255.255.0

CDP Level: 16

Preferred Management IP Address: ● None ○ Use Loopback

Credentials*

At least one CLI credential and one SNMP credential are required.

Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers.

🟪 GLOBAL 🟨 Task-specific

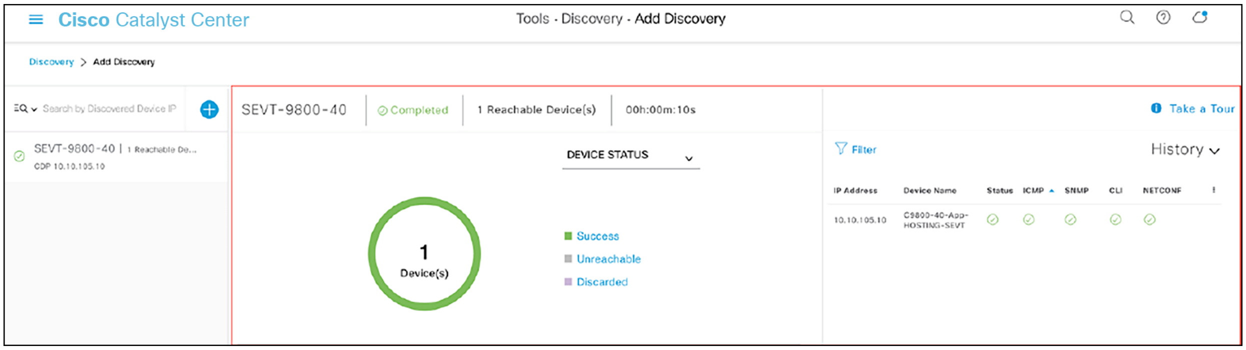
CLI: TMEadmin

SNMPv2c Read: public

Device Controllability is Enabled. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn More | Disable

Figure 19.
Discovery page with credentials filled in and ready for discovery

- After the discovery process completes, ensure that the status of ICMP (Internet Control Message Protocol), SNMP, and CLI is green for every device that has been discovered (**Figure 20**).



Cisco Catalyst Center
Tools · Discovery · Add Discovery
Discovery > Add Discovery
Search by Discovered Device IP
SEVT-9800-40 | 1 Reachable De...
CDP 10.10.105.10
DEVICE STATUS
1
Device(s)
Success
Unreachable
Discarded
Take a Tour
Filter
History

SEVT-9800-40 | Completed | 1 Reachable Device(s) | 00h:00m:10s

IP Address	Device Name	Status	ICMP	SNMP	CLI	NETCONF
10.10.105.10	C9800-40-App-HOSTING-SEVT	✓	✓	✓	✓	✓

Figure 20.
Successful discovery of a WLC as shown on the Discovery page

Step 3: Navigate to and manage inventory

After the discovery process is complete, navigate to the Inventory application, where your discovered devices will be listed.

- Open up the menu and click Provision and then Inventory (**Figure 21**).

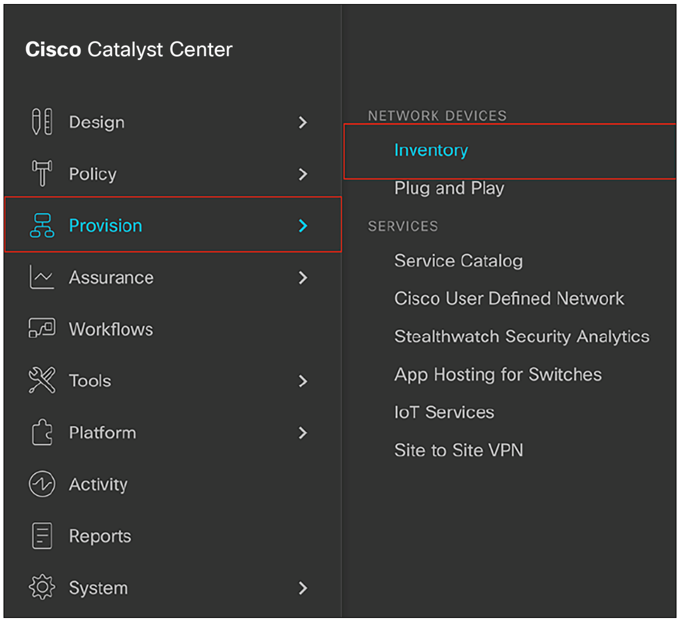
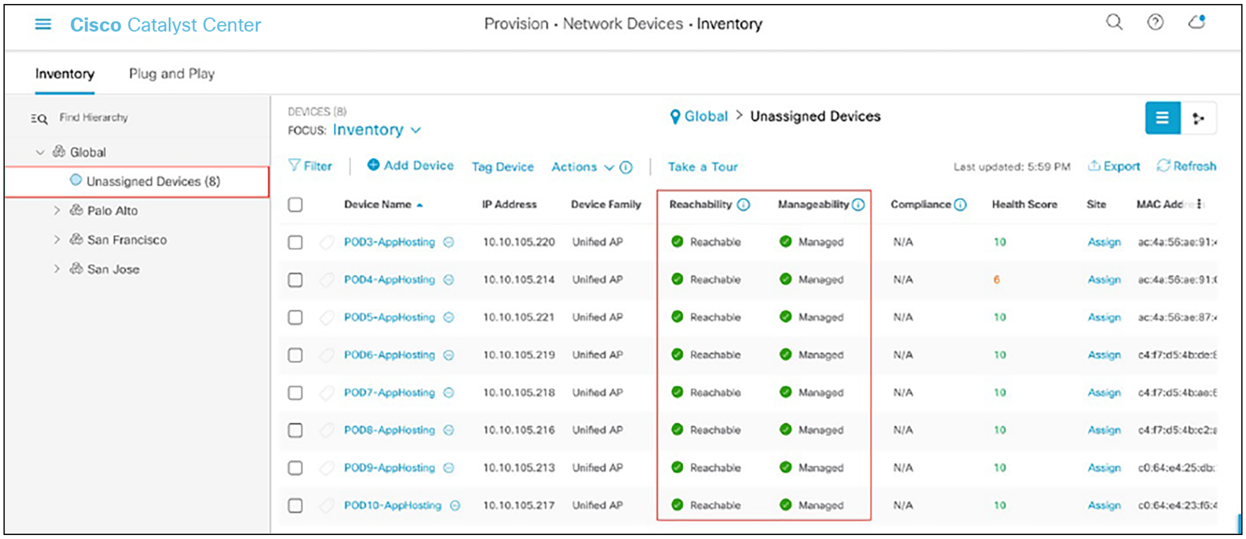


Figure 21.
Location of Inventory within the menu

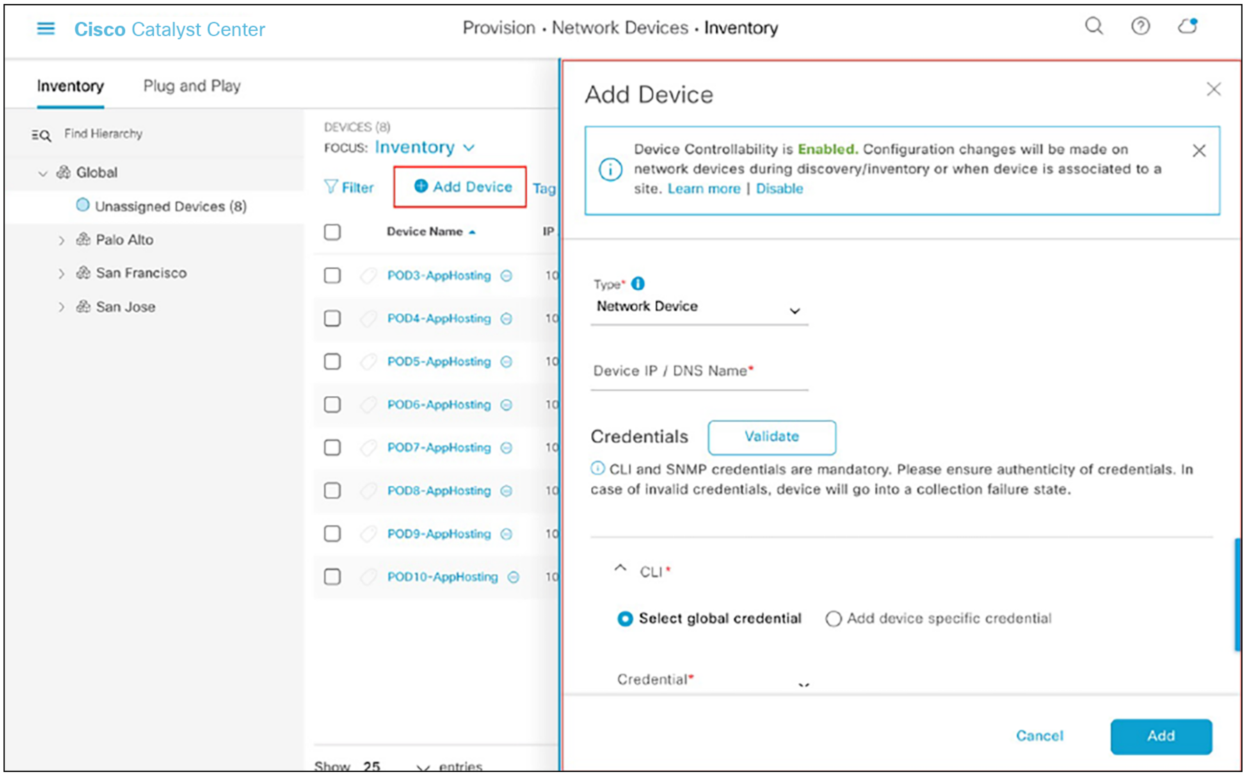
- Click Unassigned Devices on the left and ensure that all devices are Reachable and that their Manageability state is Managed (**Figure 22**).
- It is critical for all devices to be in the Managed state for Application Hosting functionality to work. If any are not, check the reachability of the devices.



☐	Device Name	IP Address	Device Family	Reachability	Manageability	Compliance	Health Score	Site	MAC Add
☐	POD3-AppHosting	10.10.105.220	Unified AP	● Reachable	● Managed	N/A	10	Assign	ac:4a:56:ae:91:
☐	POD4-AppHosting	10.10.105.214	Unified AP	● Reachable	● Managed	N/A	6	Assign	ac:4a:56:ae:91:
☐	POD5-AppHosting	10.10.105.221	Unified AP	● Reachable	● Managed	N/A	10	Assign	ac:4a:56:ae:87:
☐	POD6-AppHosting	10.10.105.219	Unified AP	● Reachable	● Managed	N/A	10	Assign	c4:f7:d5:4b:de:
☐	POD7-AppHosting	10.10.105.218	Unified AP	● Reachable	● Managed	N/A	10	Assign	c4:f7:d5:4b:ae:
☐	POD8-AppHosting	10.10.105.216	Unified AP	● Reachable	● Managed	N/A	10	Assign	c4:f7:d5:4b:c2:
☐	POD9-AppHosting	10.10.105.213	Unified AP	● Reachable	● Managed	N/A	10	Assign	c0:64:e4:25:db:
☐	POD10-AppHosting	10.10.105.217	Unified AP	● Reachable	● Managed	N/A	10	Assign	c0:64:e4:23:f6:

Figure 22.
Reachability and Manageability status of discovered devices

- Optional: If you would like to manually add a controller to the inventory, click the Add Device button and provide the same information as was given in the Discovery application (**Figure 23**).



Device Controllability is Enabled. Configuration changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn more | Disable

Type* Network Device

Device IP / DNS Name*

Credentials

CLI and SNMP credentials are mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.

CLI*

● Select global credential ○ Add device specific credential

Credential*

Figure 23.
Add Device form

Step 4: Assign discovered devices to the site hierarchy

After discovery and site assignment, Cisco Catalyst Center will have automatically pushed/enabled the following configuration to the WLC and access points. This configuration is required for Application Hosting on Catalyst Access Points to work.

- Pushed a Cisco Catalyst Center certificate
- Configured Cisco Catalyst Center as an SNMP trap receiver
- Configured Cisco Catalyst Center as a syslog server
- Click the check box next to a device that you would like to assign to a site.
- Hover your cursor over Actions and then Provision, then click Assign Device to Site (**Figure 24**).

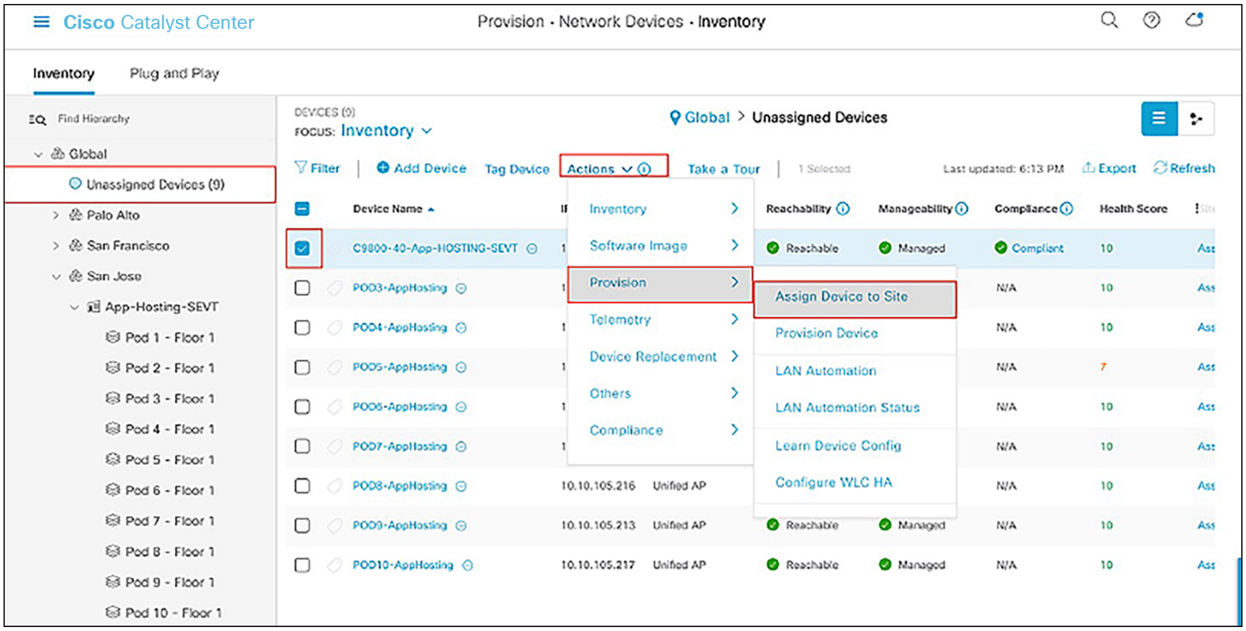


Figure 24.
Assigning a WLC to a site on the Inventory page

- Click Choose a Site (**Figure 25**).

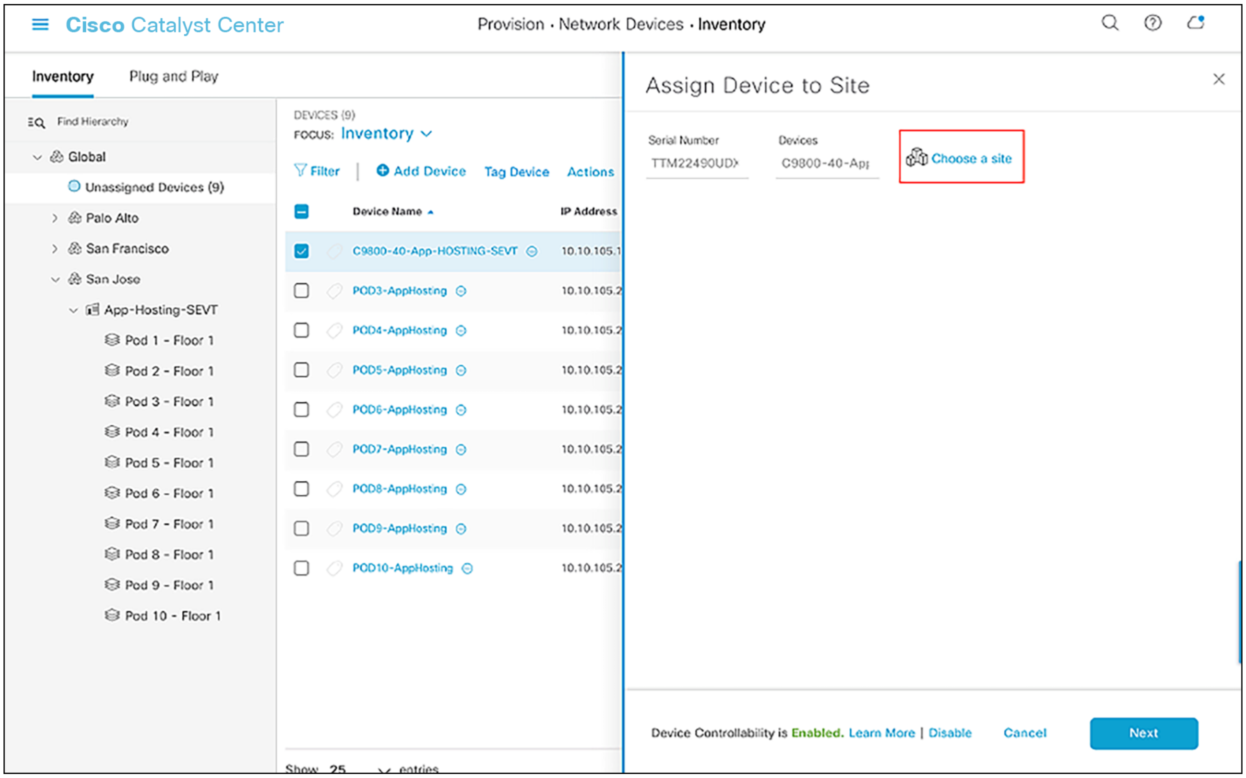
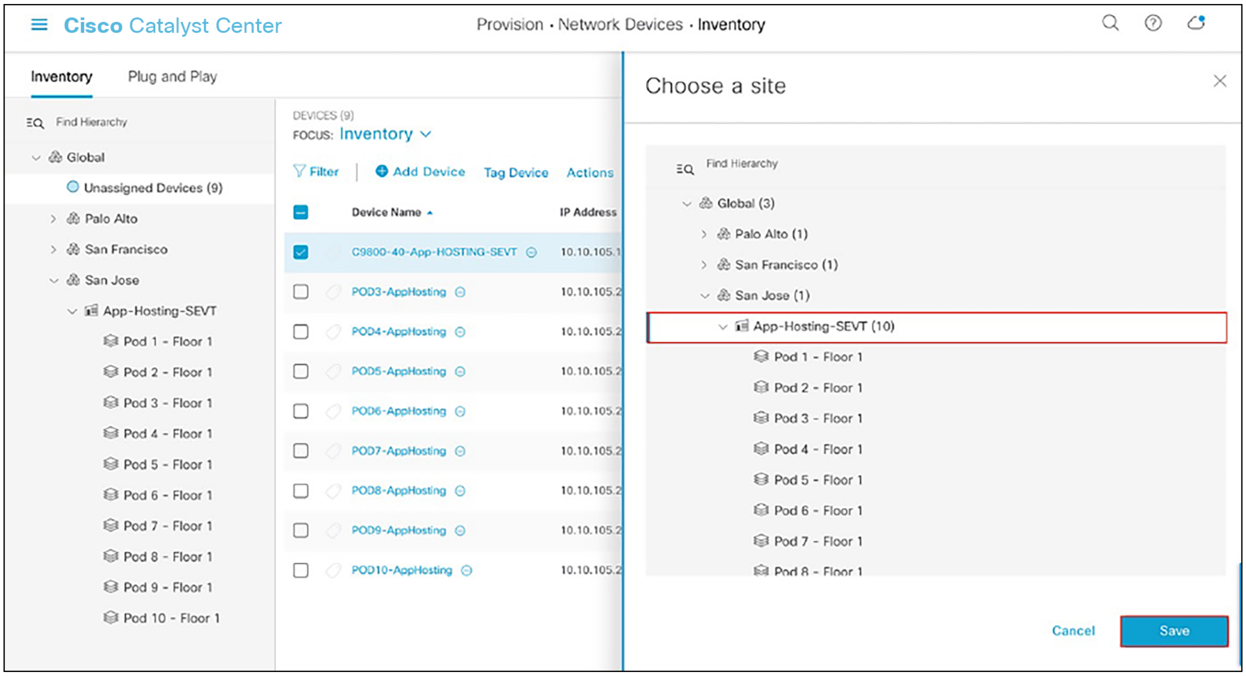


Figure 25.
Assign Device to Site menu

- Click on the site to which you would like to assign the WLC and then click Save (**Figure 26**).



	Device Name	IP Address
☑	C9800-40-App-HOSTING-SEVT	10.10.105.1
□	POD3-AppHosting	10.10.105.2
□	POD4-AppHosting	10.10.105.2
□	POD5-AppHosting	10.10.105.2
□	POD6-AppHosting	10.10.105.2
□	POD7-AppHosting	10.10.105.2
□	POD8-AppHosting	10.10.105.2
□	POD9-AppHosting	10.10.105.2
□	POD10-AppHosting	10.10.105.2

Figure 26.
Choosing a site

- Click Next and then Assign.
- Repeat the same steps for your access points.

Step 5: Place your access points onto the floor map

The purpose of placing your access points onto your floor map is to provide you with a heat map visualization of the RF environment surrounding your access points.

Note: This step is not required for Application Hosting on Catalyst Access Points but is recommended to complete your day-0 configuration.

- Navigate to the Network Hierarchy page by opening the menu in the top left corner of the screen. Click Design and then Network Hierarchy (**Figure 27**).

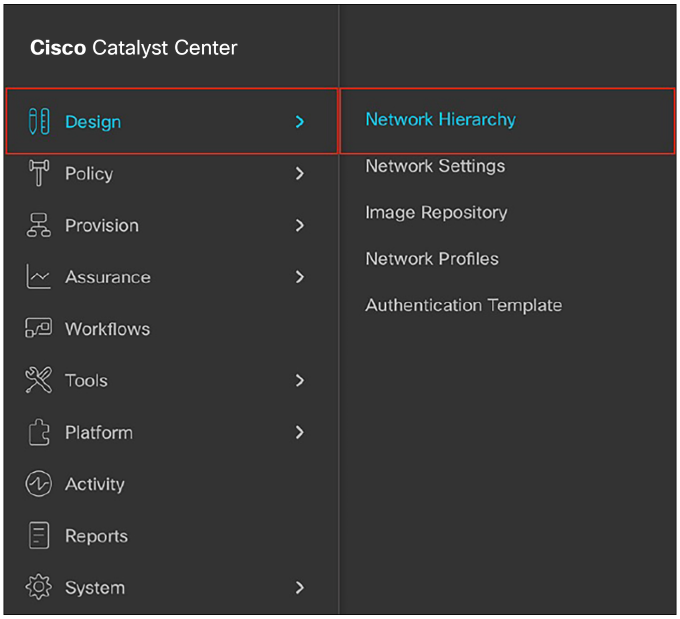


Figure 27.
Location of Network Hierarchy in the menu

- Expand Global > [the building you created], then click on the floor you've assigned access points to.
- Observe the blue flag on the right, which indicates the number of access points that are ready to be placed onto the map (**Figure 28**).

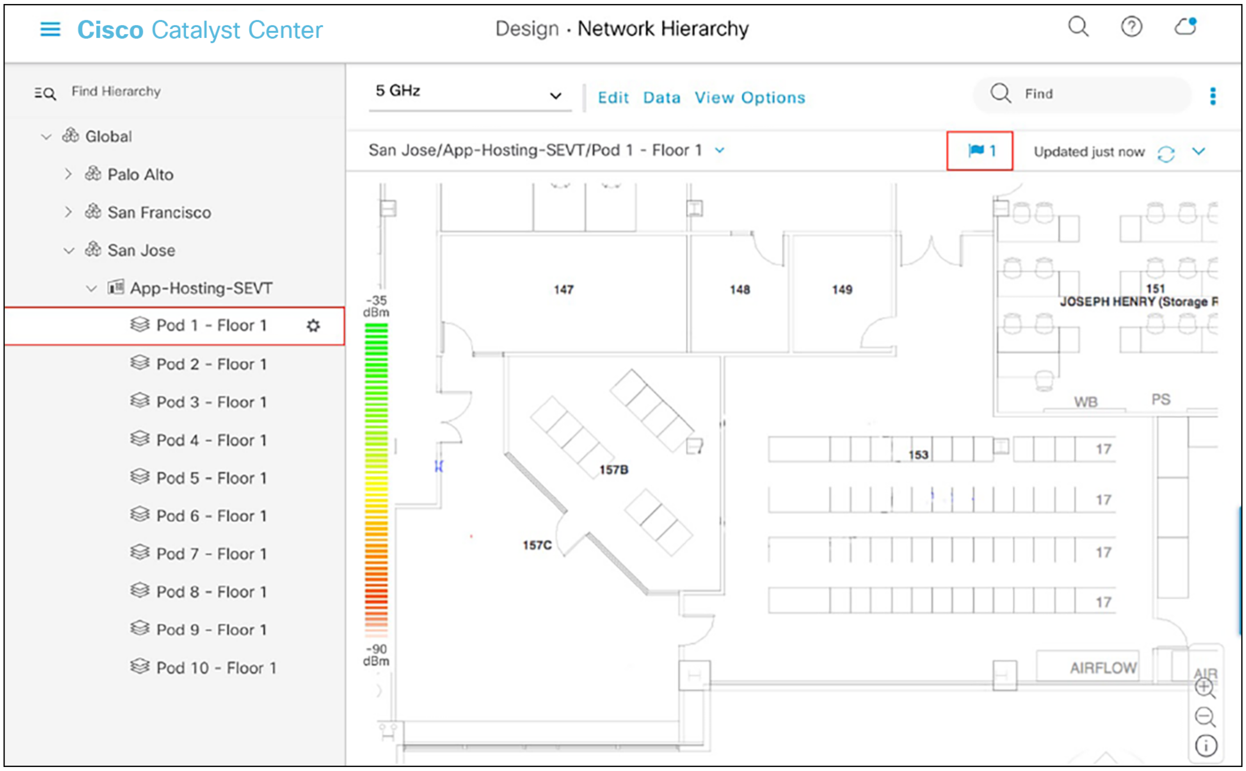


Figure 28.
Network Hierarchy page, with an access point ready to be positioned

- Click Edit and then Position to place access points onto the map (**Figure 29**).

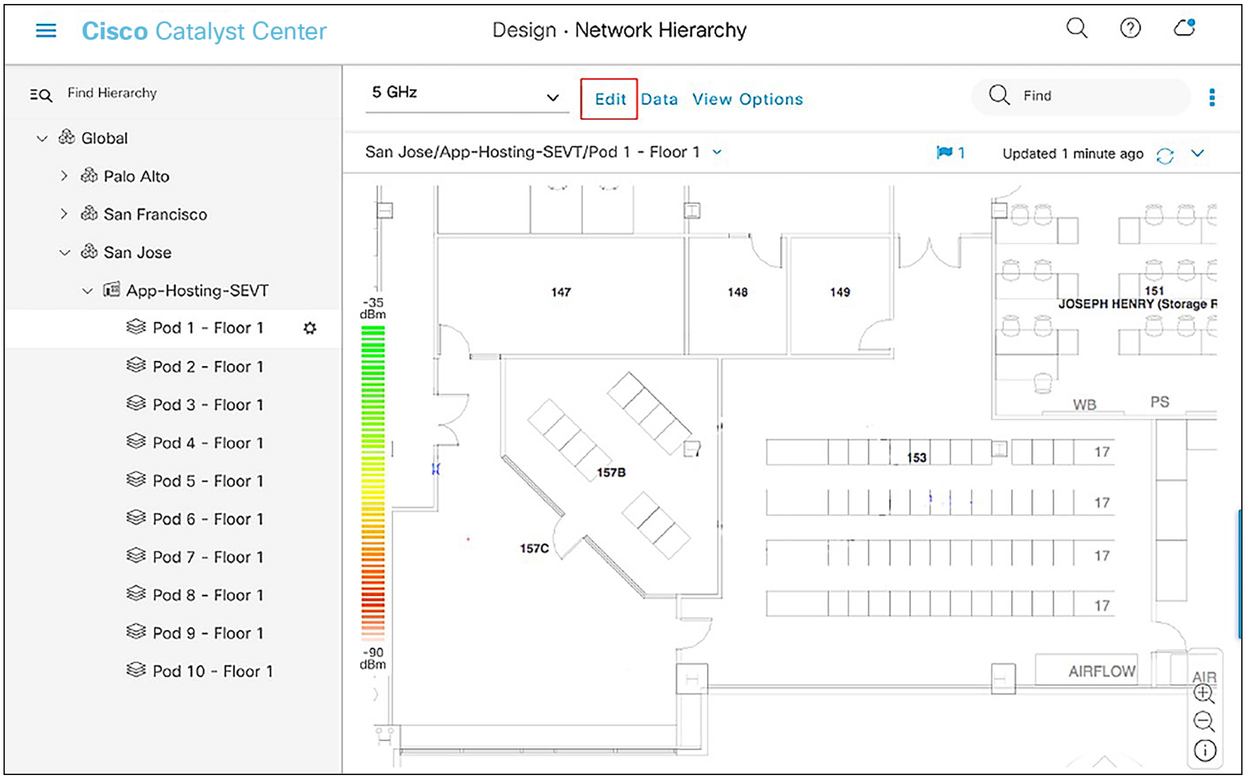
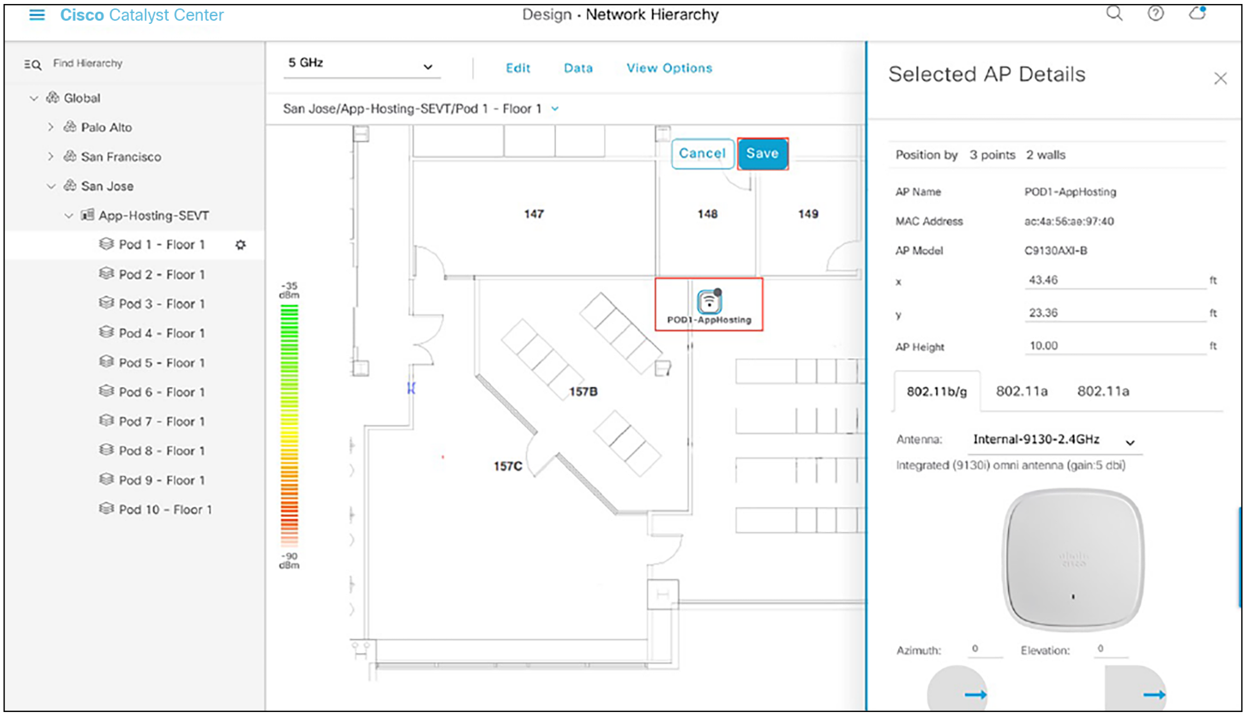


Figure 29.
Network Hierarchy page – Floor elements menu

- After placing the access points on the floor map, click Save to commit the change (**Figure 30**).



Selected AP Details

Position by 3 points 2 walls

AP Name	POD1-AppHosting
MAC Address	ac:4a:56:ae:97:40
AP Model	C9130AXI-B
x	43.46 ft
y	23.36 ft
AP Height	10.00 ft

802.11b/g 802.11a 802.11a

Antenna: Internal-9130-2.4GHz
Integrated (9130i) omni antenna (gain:5 dbi)

Azimuth: 0 Elevation: 0

Figure 30.
Network Hierarchy page, with access points placed on the floor map

- At this point, a color-coded heat map should show up on the floor map, depicting the access points' surrounding RF environment (**Figure 31**).

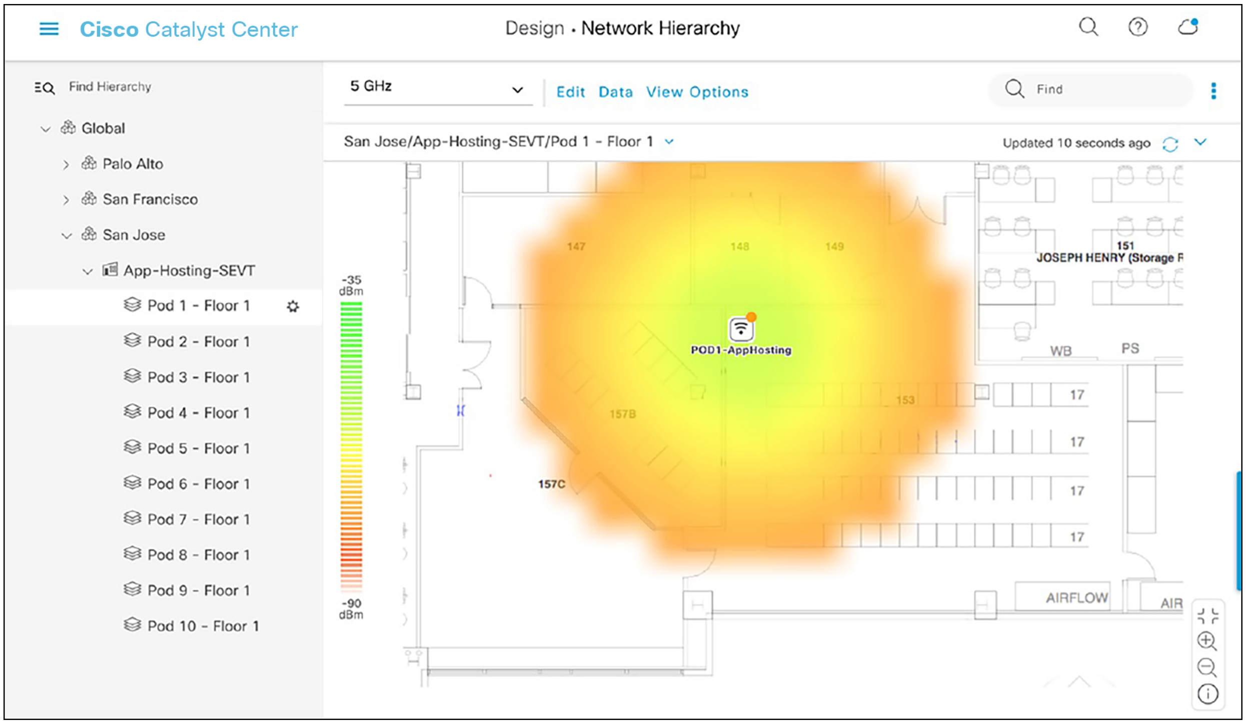


Figure 31.
Network Hierarchy page, with heat map displayed after access points are positioned

Day 1: Upload and deploy an IOx application

This section provides step-by-step instructions for uploading an IOx application to Cisco Catalyst Center and then deploying it to the desired access points.

Part 1: Day-1 configuration – Uploading an IOx application

Description: Cisco Catalyst Center's IoT Services page provides an intuitive way to upload and manage third-party applications that you would like to deploy on your access points.

Section goals: Upload an IOx application into Cisco Catalyst Center's repository so it can be ready for deployment to the desired network hierarchy location or access point.

Step 1: Navigate to the IoT Services page

- Open the menu and click Provision and then IoT Services to enter the App Hosting page (**Figure 32**).

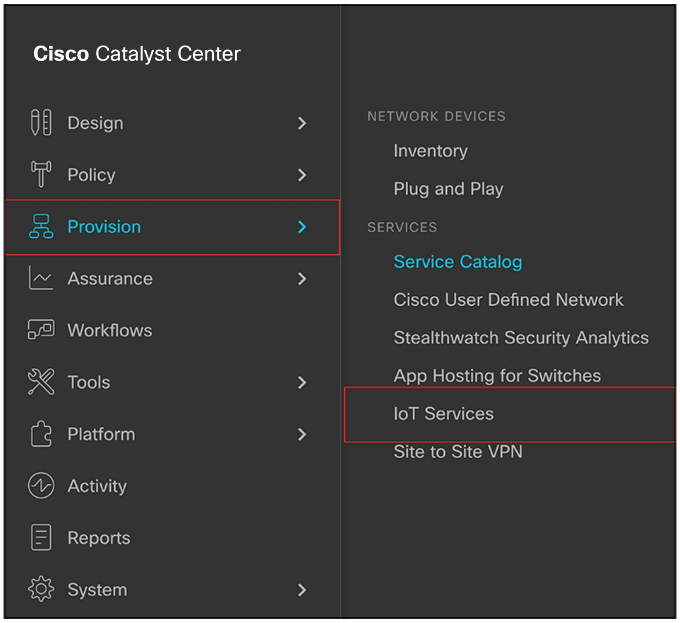


Figure 32.
Location of IoT Services within the menu

Step 2: Upload the IOx application to Cisco Catalyst Center

- Click New Application on the right side of the screen (**Figure 33**).

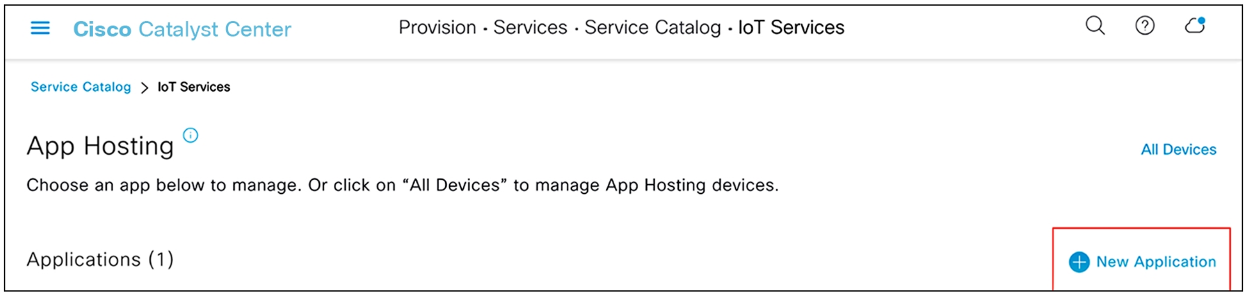
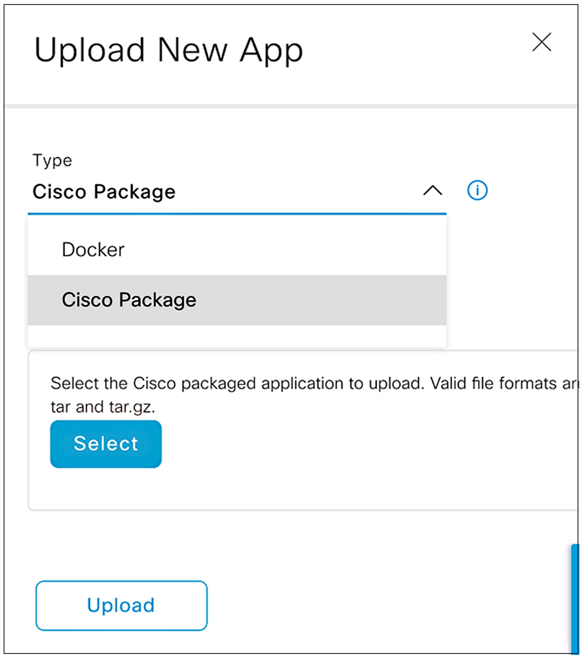

Cisco Catalyst Center
Provision · Services · Service Catalog · IoT Services
Service Catalog > IoT Services
App Hosting
All Devices
Choose an app below to manage. Or click on “All Devices” to manage App Hosting devices.
Applications (1)
New Application

Figure 33.
Location of the New Application button on the App Hosting page

- Click the Type drop-down menu and select an application type (**Figure 34**).
- **Option 1: Docker**
    - Choose this option if the application you are uploading is a Docker app saved as a .tar file using the Docker Save command**.**
- **Option 2: Cisco Package**
    - Choose this option if the application you are uploading has been packaged using the Cisco app-packaging toolchain.
- For more information regarding the package types above, visit the following link: https://developer.cisco.com/docs/iox/


Upload New App

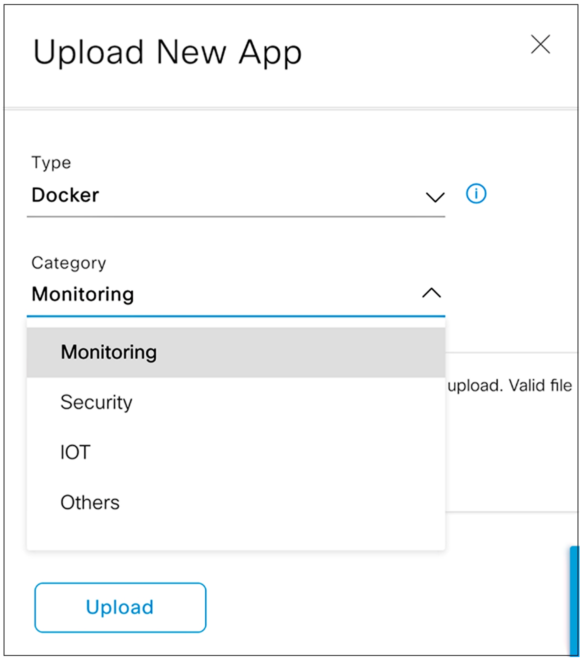
Type

Cisco Package

Select the Cisco packaged application to upload. Valid file formats ar
tar and tar.gz.

Figure 34.
Choosing an application type

- Click the Category drop-down menu and select an application category (**Figure 35**).
- The categories are Monitoring, Security, IoT, and Others.



Upload New App

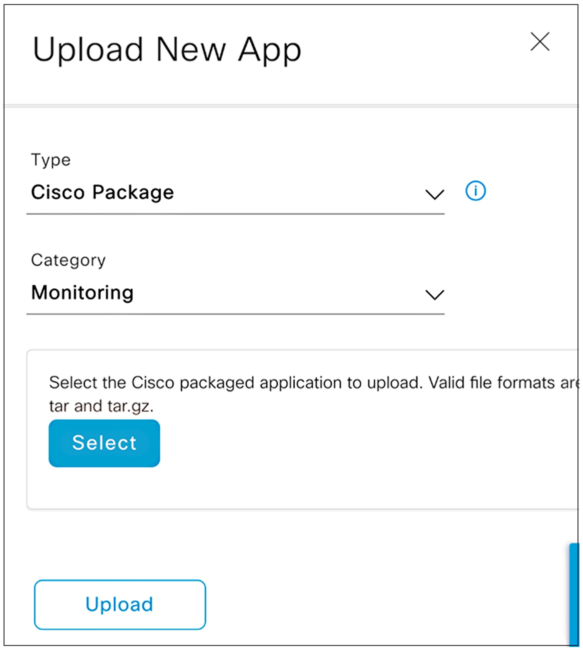
Type
Docker

Category
Monitoring

upload. Valid file

Figure 35.
Choosing an application category

- Click the Select button and select a file to upload, then click Upload to upload the file (**Figure 36**).



Upload New App

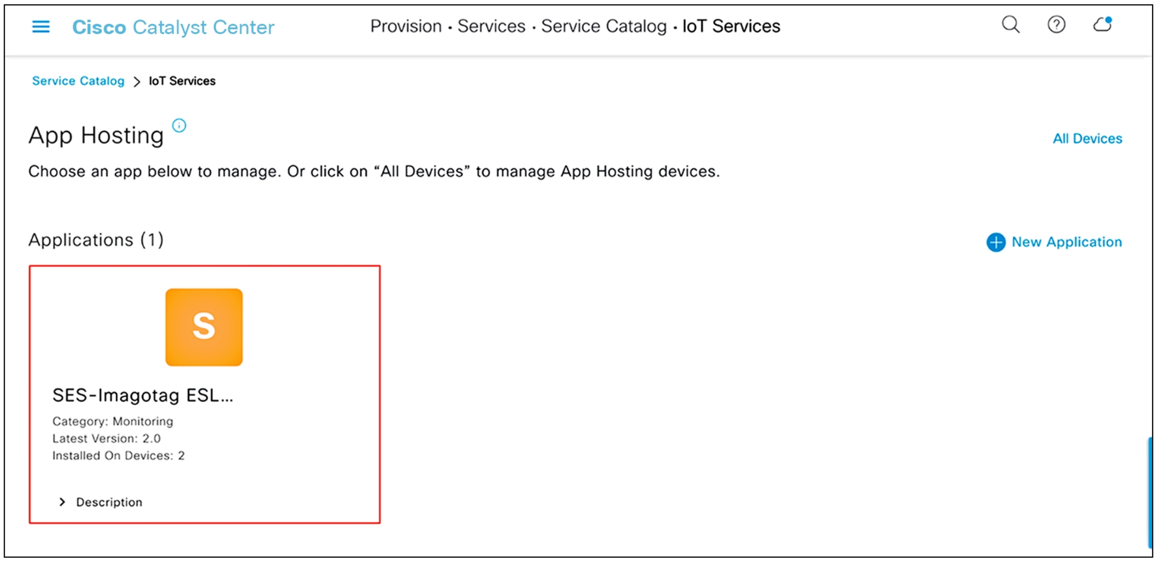
Type
Cisco Package

Category
Monitoring

Select the Cisco packaged application to upload. Valid file formats ar
tar and tar.gz.

Figure 36.
Location of the Select and Upload buttons

- Ensure that the application you’ve uploaded now appears within the App Hosting page (**Figure 37**).
- IOx applications can be discovered and downloaded via the following link: https://developer.cisco.com/ecosystem/spp/
    - Optional: If you would like to manage the application, click on it to enter the application’s management page.


Cisco Catalyst Center
Provision · Services · Service Catalog · IoT Services
Service Catalog > IoT Services
All Devices
New Application
S
Description

App Hosting

Choose an app below to manage. Or click on “All Devices” to manage App Hosting devices.

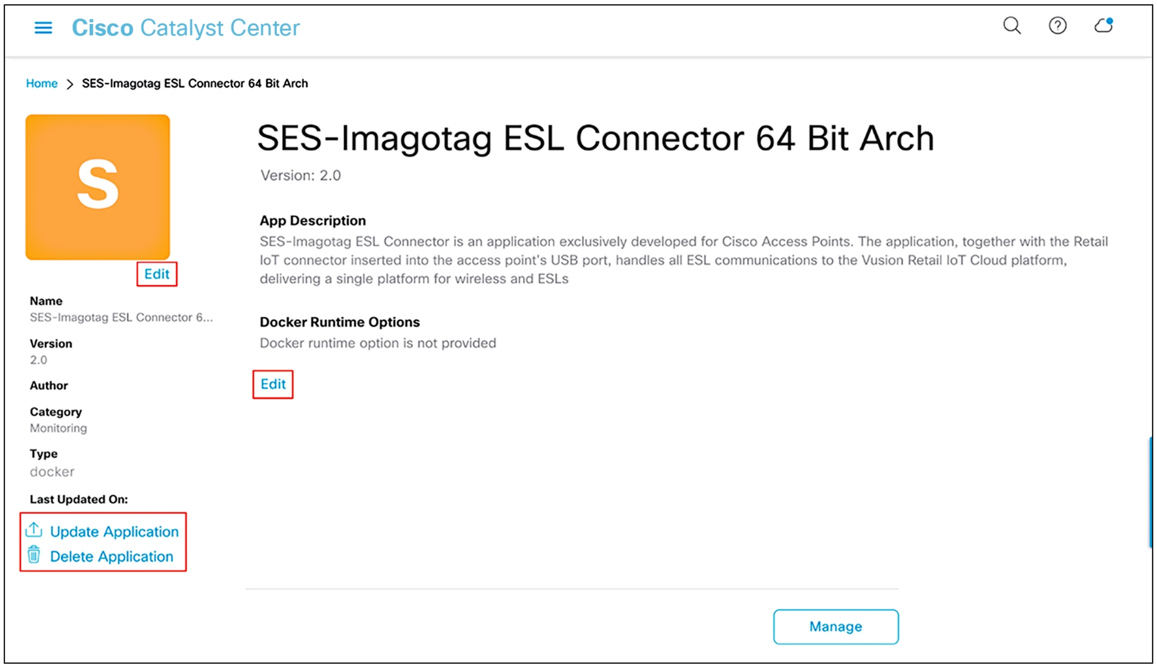
Applications (1)

SES-Imagotag ESL...

Category: Monitoring
Latest Version: 2.0
Installed On Devices: 2

Figure 37.
Location of an application after being uploaded

- (a) To upload a new version of this application, click the Update Application button. (b) To delete the application, click the Delete Application button. (c) To edit the application’s description, click the Edit button (**Figure 38**).



SES-Imagotag ESL Connector 64 Bit Arch

Version: 2.0

App Description

SES-Imagotag ESL Connector is an application exclusively developed for Cisco Access Points. The application, together with the Retail IoT connector inserted into the access point's USB port, handles all ESL communications to the Vusion Retail IoT Cloud platform, delivering a single platform for wireless and ESLs

Docker Runtime Options

Docker runtime option is not provided

Name
SES-Imagotag ESL Connector 6...

Version
2.0

Author

Category
Monitoring

Type
docker

Last Updated On:

Figure 38.
Application management page

Part 2: Day-1 configuration – Deploying an IOx application

Description: Cisco Catalyst Center's Enable IoT Services workflow allows you to easily deploy your application to either a location or a specific access point.

Section goals: Deploy an IOx application to all devices within a network hierarchy site created earlier.

Step 1: Navigate to the Enable IoT Services workflow

- Open the menu, then click Workflows (**Figure 39**).

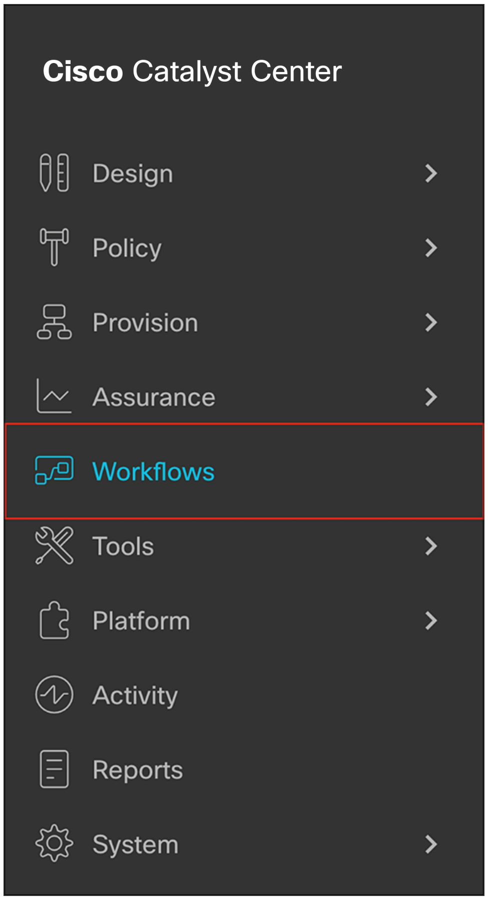
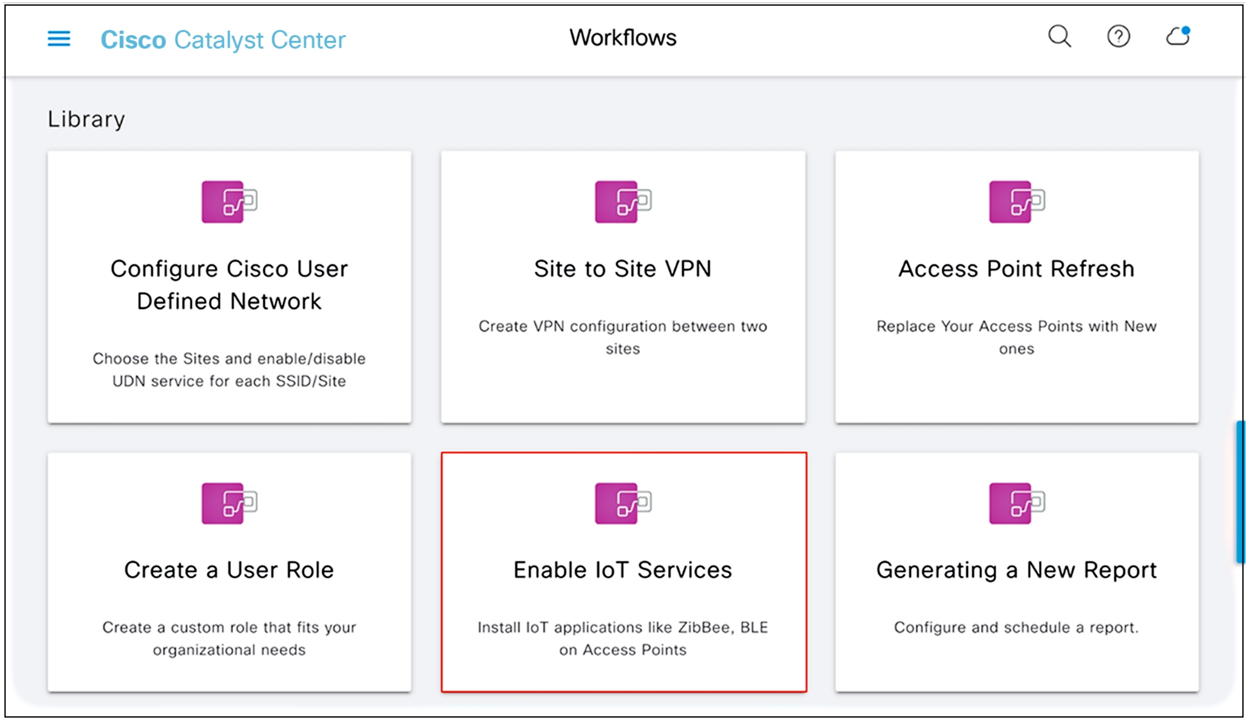


Figure 39.
Location of Workflows on the menu.

- Scroll down and click on the grid labeled Enable IoT Services to begin the deployment workflow (**Figure 40**). Click the Let's Do It button in the modal box that appears (**Figure 41**).



Cisco Catalyst Center

Workflows

Library

Configure Cisco User Defined Network

Choose the Sites and enable/disable UDN service for each SSID/Site

Site to Site VPN

Create VPN configuration between two sites

Access Point Refresh

Replace Your Access Points with New ones

Create a User Role

Create a custom role that fits your organizational needs

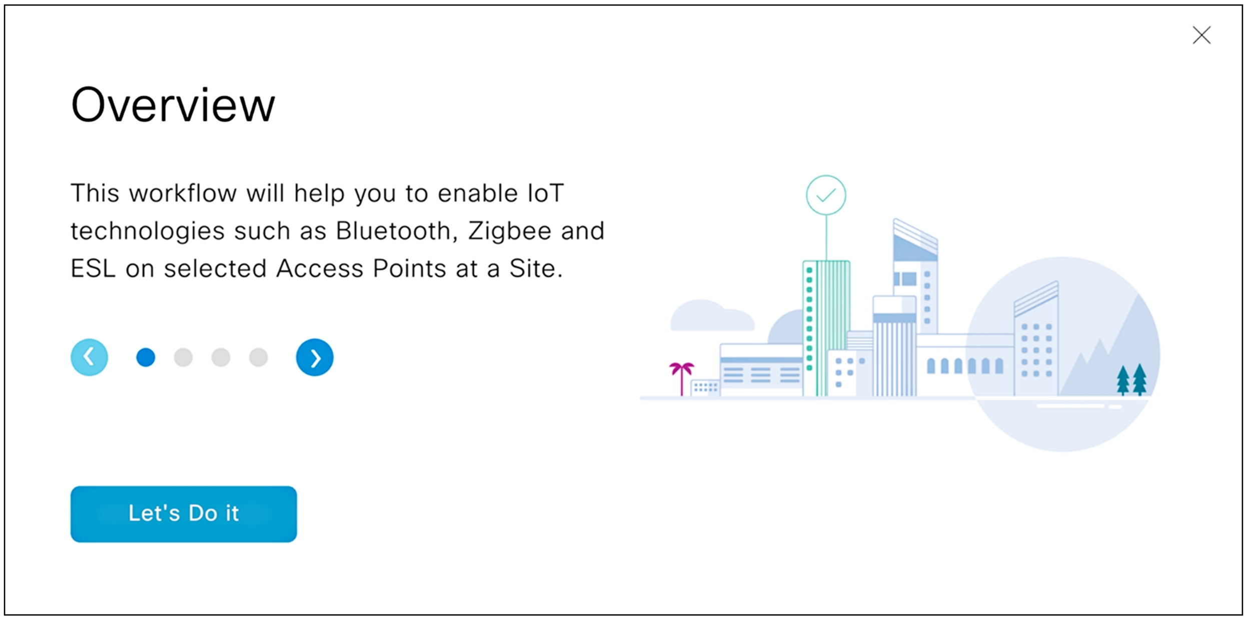
Enable IoT Services

Install IoT applications like ZibBee, BLE on Access Points

Generating a New Report

Configure and schedule a report.

Figure 40.
Location of the Enable IoT Services option



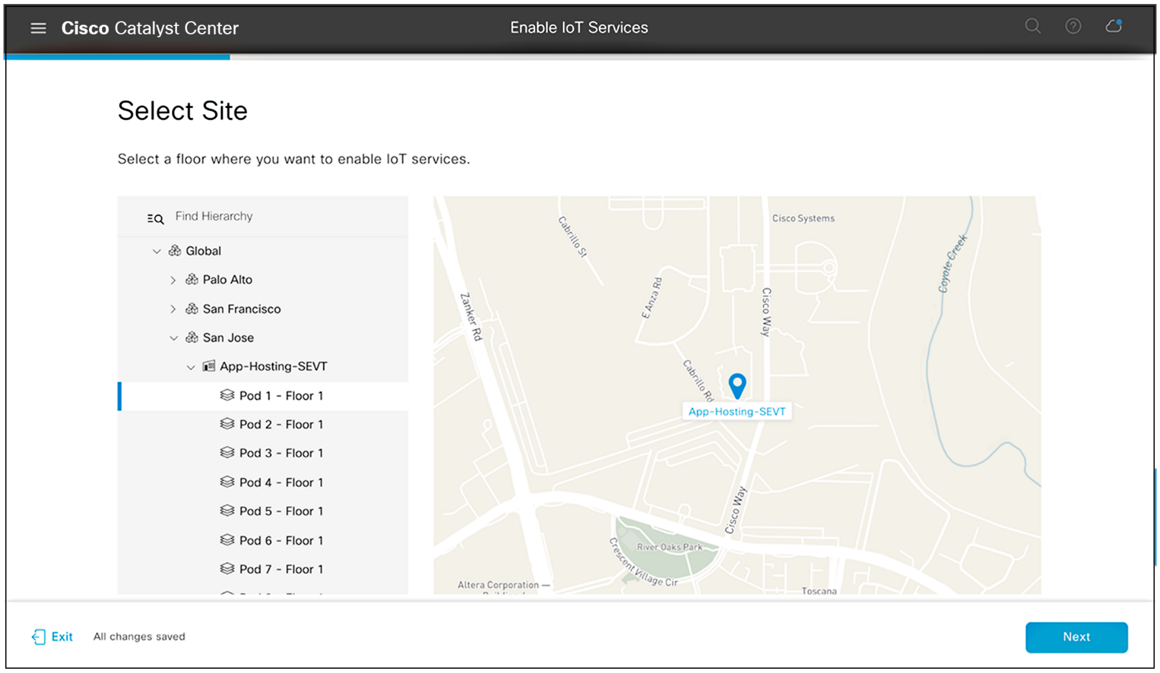
Overview

This workflow will help you to enable IoT technologies such as Bluetooth, Zigbee and ESL on selected Access Points at a Site.

Figure 41.
Modal box for the Enable IoT Services option

Step 2: Deploy the application to access points on a floor

- Select a floor within the network hierarchy where you'd like to deploy the application, then click Next (**Figure 42**).



Cisco Catalyst Center — Enable IoT Services

Select Site

Select a floor where you want to enable IoT services.

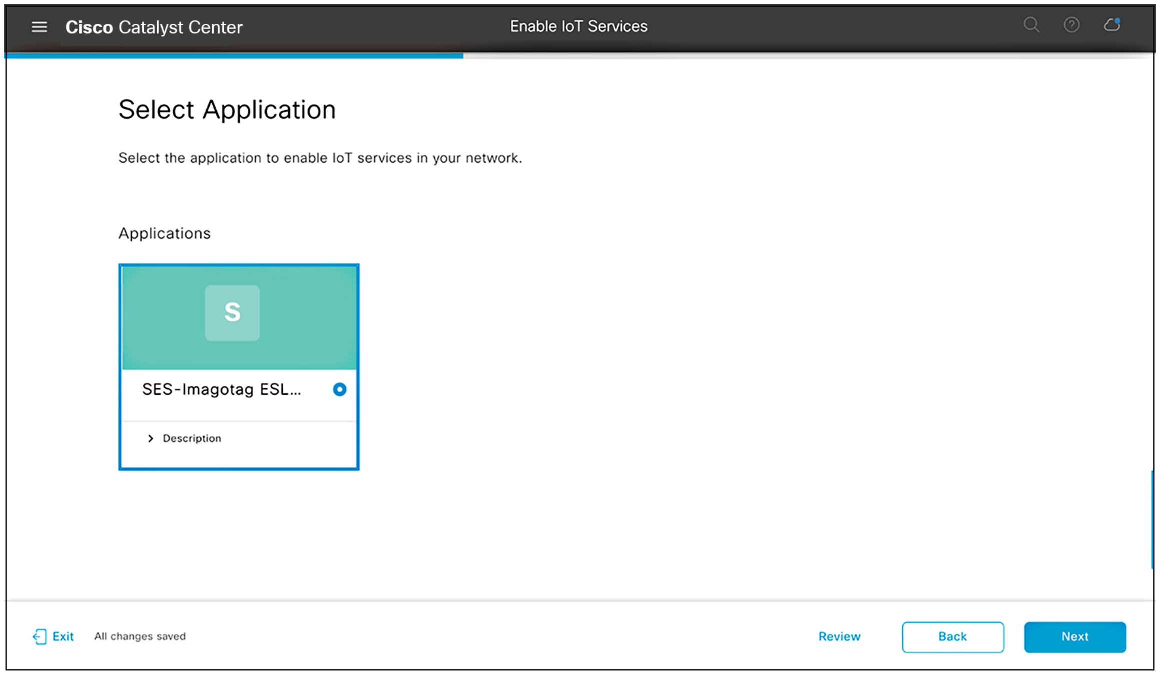
Find Hierarchy

- Global
  - Palo Alto
  - San Francisco
  - San Jose
    - App-Hosting-SEVT
      - Pod 1 - Floor 1
      - Pod 2 - Floor 1
      - Pod 3 - Floor 1
      - Pod 4 - Floor 1
      - Pod 5 - Floor 1
      - Pod 6 - Floor 1
      - Pod 7 - Floor 1

All changes saved

Figure 42.
Selecting a floor

- Select the image that you would like to deploy to devices on that floor, then click Next (**Figure 43**).



Cisco Catalyst Center — Enable IoT Services

Select Application

Select the application to enable IoT services in your network.

Applications

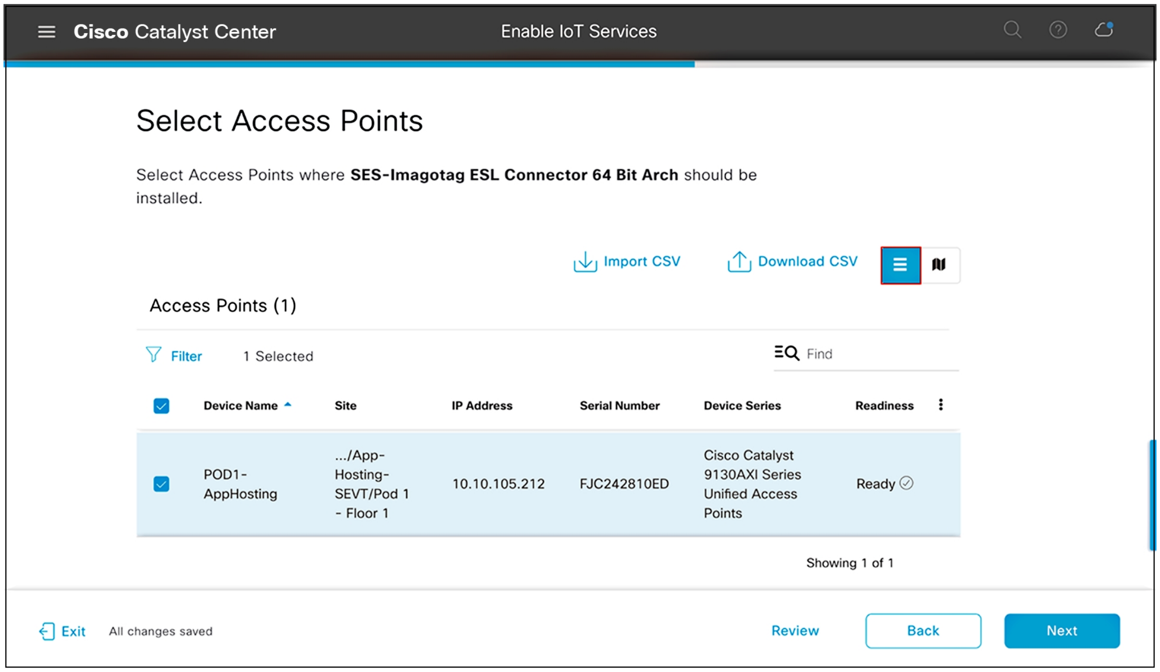
● SES-Imagotag ESL...

Description

All changes saved

Figure 43.
Selecting an application to deploy

- Select one or more access points on this floor that you would like to deploy the image to, then click Next.
- By default, the page will show an access point list view (**Figure 44**); however, this can be toggled by clicking on the map icon to show a network hierarchy floor view (**Figure 45**).
- **Note:** Make sure the Readiness column indicates Ready for the access points you select.



Cisco Catalyst Center

Enable IoT Services

Select Access Points

Select Access Points where **SES-Imagotag ESL Connector 64 Bit Arch** should be installed.

Access Points (1)

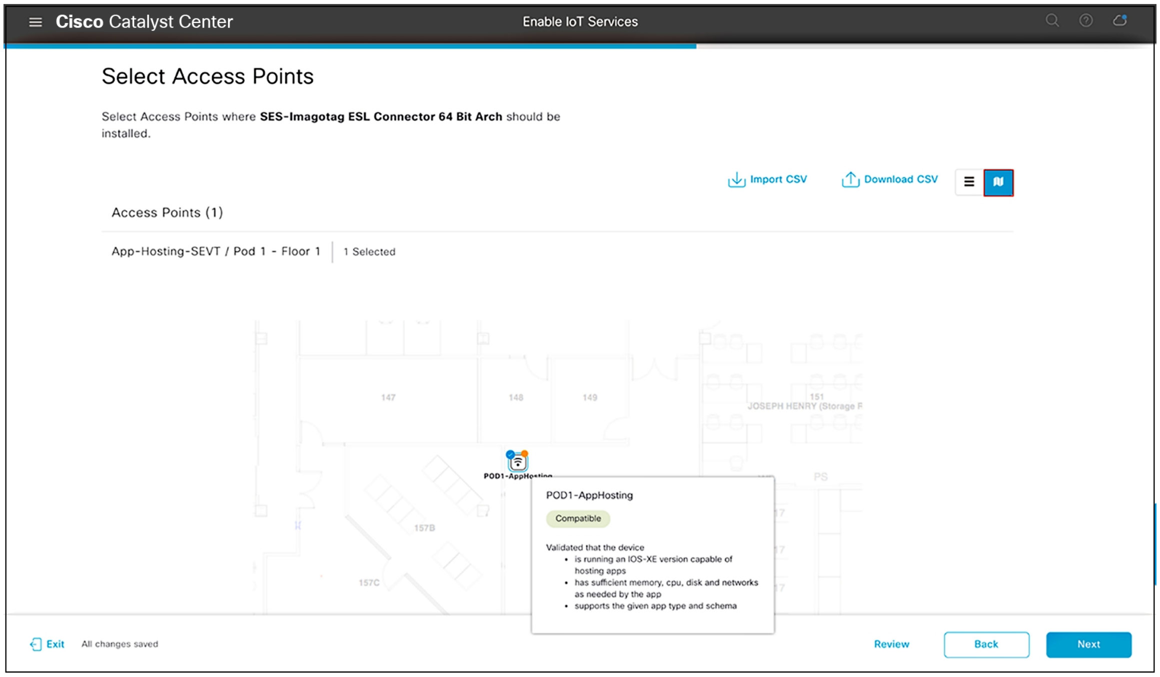
1 Selected

☑	Device Name	Site	IP Address	Serial Number	Device Series	Readiness
☑	POD1-AppHosting	.../App-Hosting-SEVT/Pod 1 - Floor 1	10.10.105.212	FJC242810ED	Cisco Catalyst 9130AXI Series Unified Access Points	Ready ✓

Showing 1 of 1

All changes saved

Figure 44.
Selecting access points from the list



Cisco Catalyst Center

Enable IoT Services

Select Access Points

Select Access Points where **SES-Imagotag ESL Connector 64 Bit Arch** should be installed.

Access Points (1)

App-Hosting-SEVT / Pod 1 - Floor 1 | 1 Selected

POD1-AppHosting

Compatible

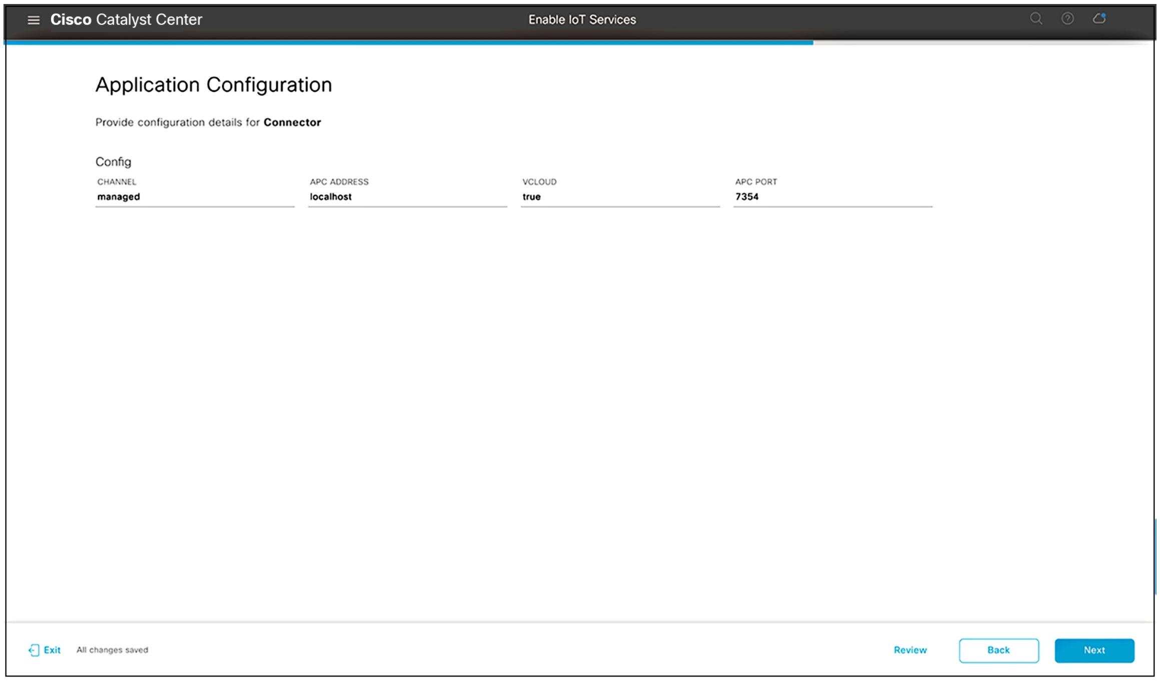
Validated that the device

- is running an IOS-XE version capable of hosting apps
- has sufficient memory, cpu, disk and networks as needed by the app
- supports the given app type and schema

All changes saved

Figure 45.
Selecting access points from the map

- On the Application Configuration page, input configurations for the IOx application specified by the IoT app vendor. These configurations will be implemented when the application is deployed to the AP (**Figure 46**).
- **Example:** The configuration can be used to point the IOx application to a specific application server.



Application Configuration

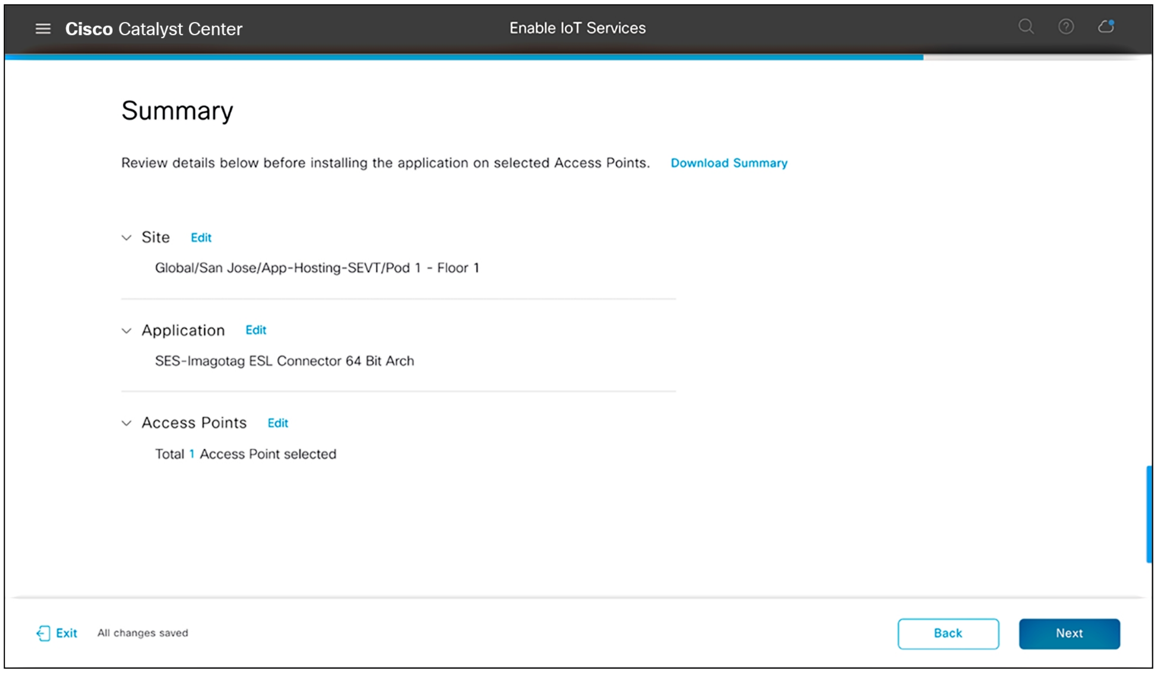
Provide configuration details for **Connector**

Config

CHANNEL	APC ADDRESS	VCLOUD	APC PORT
managed	localhost	true	7354

Figure 46.
Adding configurations to your IOx application

- On the Summary page, check that the application is being deployed to the intended site and access points, then click Next (**Figure 47**).



Summary

Review details below before installing the application on selected Access Points. Download Summary

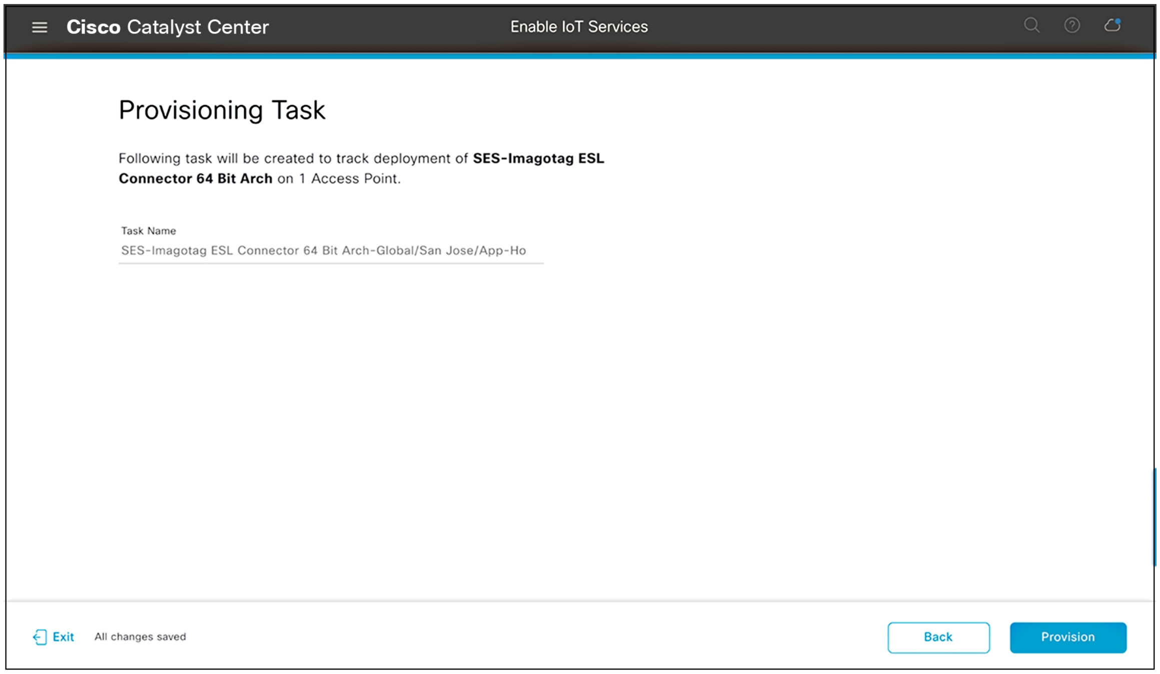
Site Edit
Global/San Jose/App-Hosting-SEVT/Pod 1 - Floor 1

Application Edit
SES-Imagotag ESL Connector 64 Bit Arch

Access Points Edit
Total 1 Access Point selected

Figure 47.
Summary page

- Note the task name for reference, then click Provision (**Figure 48**).



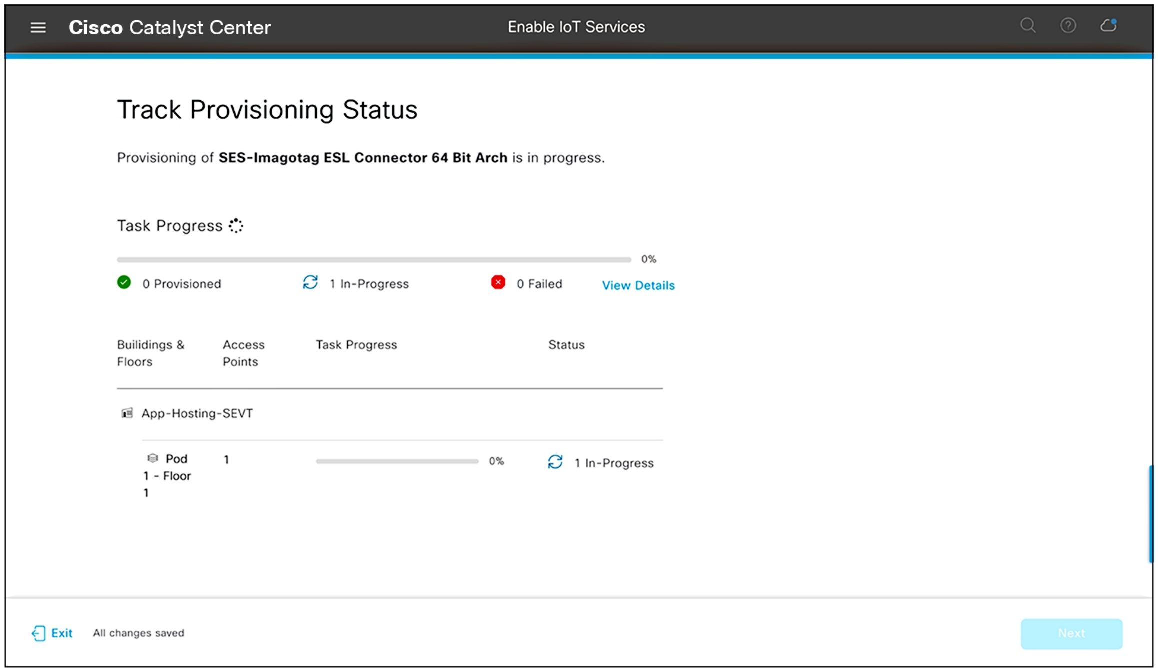
Provisioning Task

Following task will be created to track deployment of **SES-Imagotag ESL Connector 64 Bit Arch** on 1 Access Point.

Task Name
SES-Imagotag ESL Connector 64 Bit Arch-Global/San Jose/App-Ho

Figure 48.
Generated provisioning task name

- The application deployment process will begin (**Figure 49**).



Track Provisioning Status

Provisioning of **SES-Imagotag ESL Connector 64 Bit Arch** is in progress.

Task Progress

0%

0 Provisioned 1 In-Progress 0 Failed View Details

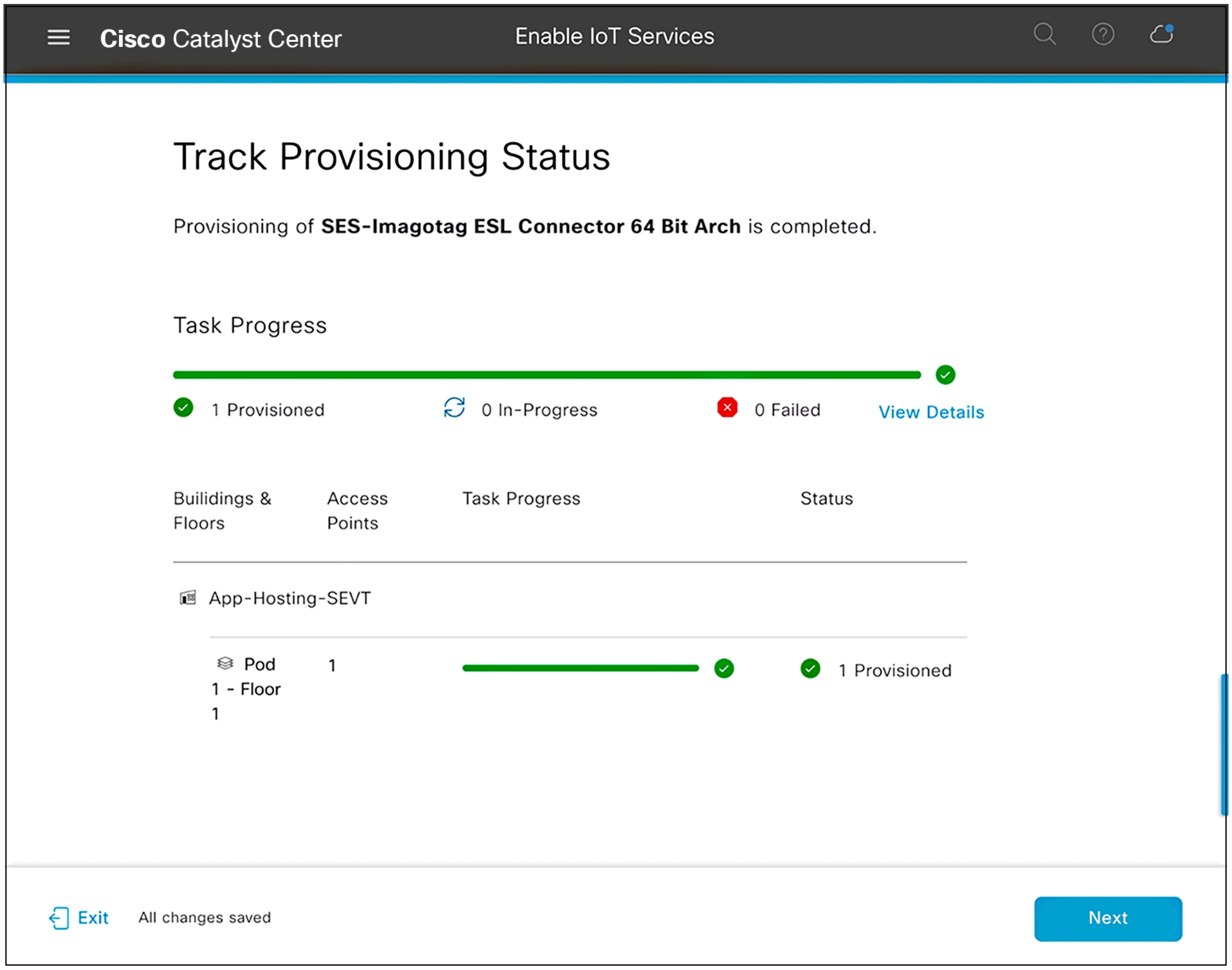
Builidings & Floors	Access Points	Task Progress	Status
App-Hosting-SEVT			
Pod 1 - Floor 1	1	0%	1 In-Progress

Figure 49.
Track Provisioning Status page

- If all steps were followed, you will see a Provisioned message (**Figure 50**).

Warning: If you attempt to deploy an application with a dependency on a USB attachment and the attachment is not detected, you will see a Failed message.

- After verifying the provisioning status of your application deployment, click Next.



Track Provisioning Status

Provisioning of **SES-Imagotag ESL Connector 64 Bit Arch** is completed.

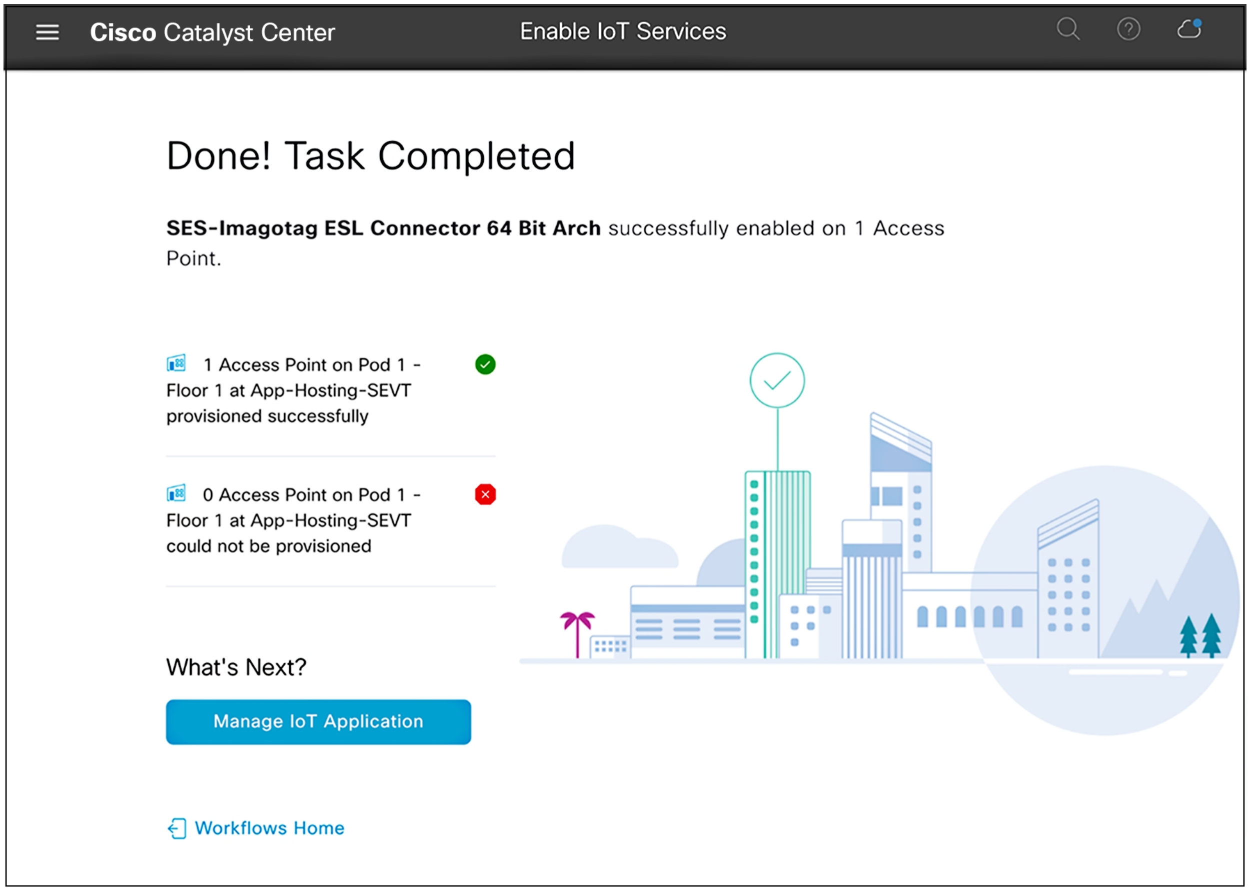
Task Progress

✓ 1 Provisioned   0 In-Progress   ✕ 0 Failed   View Details

Builidings & Floors	Access Points	Task Progress	Status
App-Hosting-SEVT			
Pod 1 - Floor 1	1	✓	✓ 1 Provisioned

Figure 50.
Success case when deploying an application to an access point

- Click the Manage IoT Application button to continue to the application’s management page (**Figure 51**).



Done! Task Completed

SES-Imagotag ESL Connector 64 Bit Arch successfully enabled on 1 Access Point.

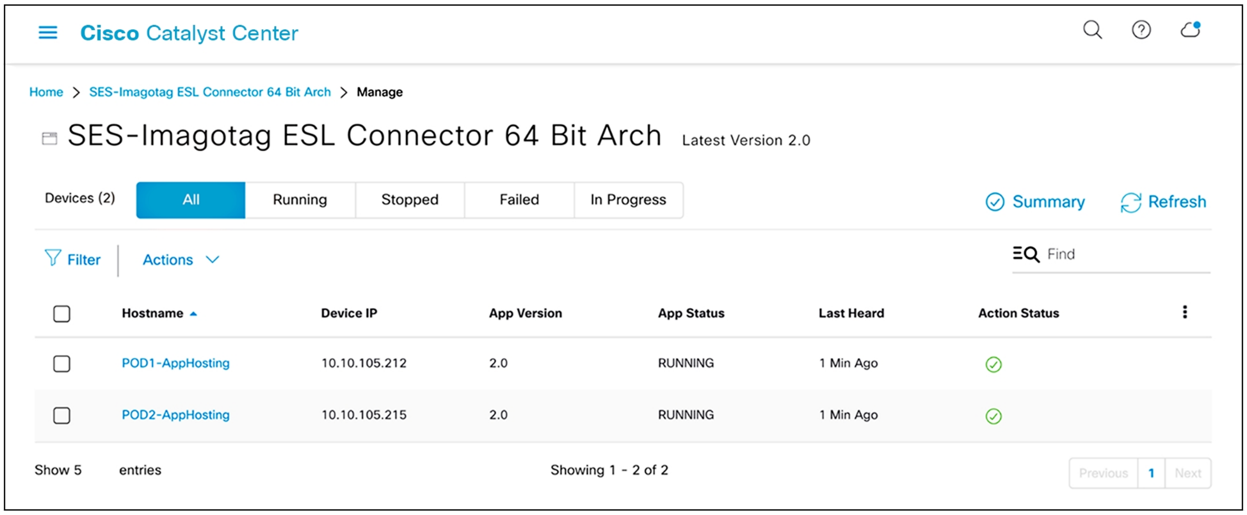
1 Access Point on Pod 1 - Floor 1 at App-Hosting-SEVT provisioned successfully ✓

0 Access Point on Pod 1 - Floor 1 at App-Hosting-SEVT could not be provisioned ✕

What's Next?

Figure 51.
Enable IoT Services workflow summary page

- On this application management page, you’re able to manage the status of the applications deployed on your access points (**Figure 52**).
- **Note:** If the App Status shows as RUNNING, the IOx application has been deployed to the access point successfully.



SES-Imagotag ESL Connector 64 Bit Arch Latest Version 2.0

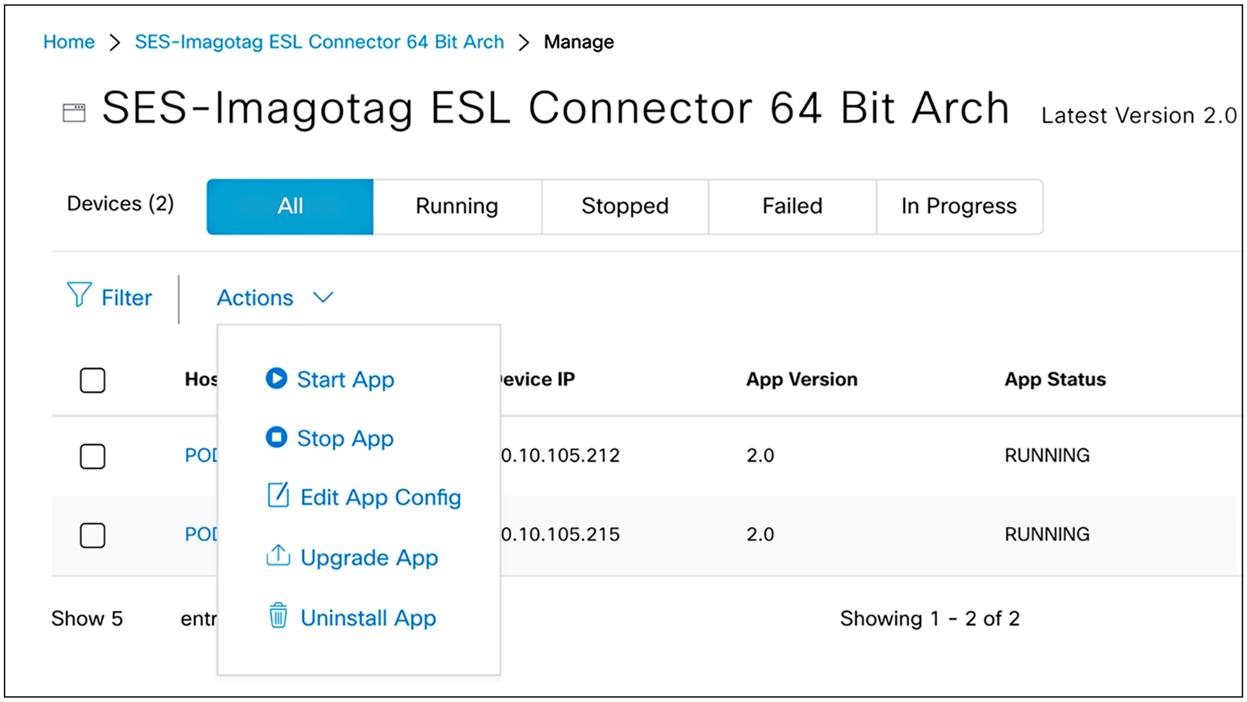
□	Hostname ▲	Device IP	App Version	App Status	Last Heard	Action Status
□	POD1-AppHosting	10.10.105.212	2.0	RUNNING	1 Min Ago	✓
□	POD2-AppHosting	10.10.105.215	2.0	RUNNING	1 Min Ago	✓

Show 5 entries

Showing 1 - 2 of 2

Figure 52.
Application management page

- To manage the application deployed to the access points, click the Actions drop-down menu (**Figure 53**).



	Hos	evice IP	App Version	App Status
□	POI	0.10.105.212	2.0	RUNNING
□	POI	0.10.105.215	2.0	RUNNING

Show 5 entr

Showing 1 - 2 of 2

Figure 53.
Actions drop-down menu within the application management page

Notes:

- **Start App:** If you stopped your application via the **Stop App** button, you can start it again via this button.
- **Stop App:** You can stop the loaded application from running. (Stopping an application does not delete or uninstall it.)
- **Edit App Config:** Allows you to change the configurations you've initially deployed the application with.
- **Upgrade App:** If you've uploaded a new version of your application in the application's management page (**Figure 39**), you can click the **Upgrade App** button to upgrade the version running on the access points to the new version.
- **Uninstall App:** Choose this option to remove the application from your access points entirely.

Day 2: Monitor the IOx application (example)

At this point, your application should be successfully loaded onto your desired access points and ready for communication with your third-party management and monitoring system. This next part of the process varies from application to application, as it's completely dependent on the design created by the third-party application developers for managing and monitoring their loaded application.

Disclaimer: The SES-imagotag ESL application discussed in this section should be used purely as a reference. If you are deploying an actual SES-imagotag ESL solution, please contact SES-imagotag for their vendor-specific deployment guide. (https://www.ses-imagotag.com/en/contact/)

Day-2 configuration – Establishing communication between the IOx application and the management server

Description: This section provides an example of how a specific application called SES-imagotag ESL communicates with its third-party management and monitoring system.

Section goals: Understand how the SES-imagotag ESL application (one of our many supported applications) begins communicating with its third-party monitoring and management system.

Prerequisite: Understanding the SES-imagotag ESL solution and third-party management system.

Background

The SES-imagotag ESL application uses the USB port on an access point to communicate with electronic shelf labels (ESLs) through a USB BLE dongle. ESLs are used in retail stores, where they're deployed in place of regular price tags.

The advantage of ESLs is that item prices can be updated remotely and users can easily locate any item through a mobile application. These features are accomplished by allowing the ESLs deployed throughout the store to communicate with the various SES-imagotag ESL applications loaded onto Cisco access points, which are also deployed throughout the store through a USB Bluetooth dongle. All of the deployed SES-imagotag ESL applications are managed by a central ESL management system (VUSION Cloud), allowing for an organized, end-to-end solution.

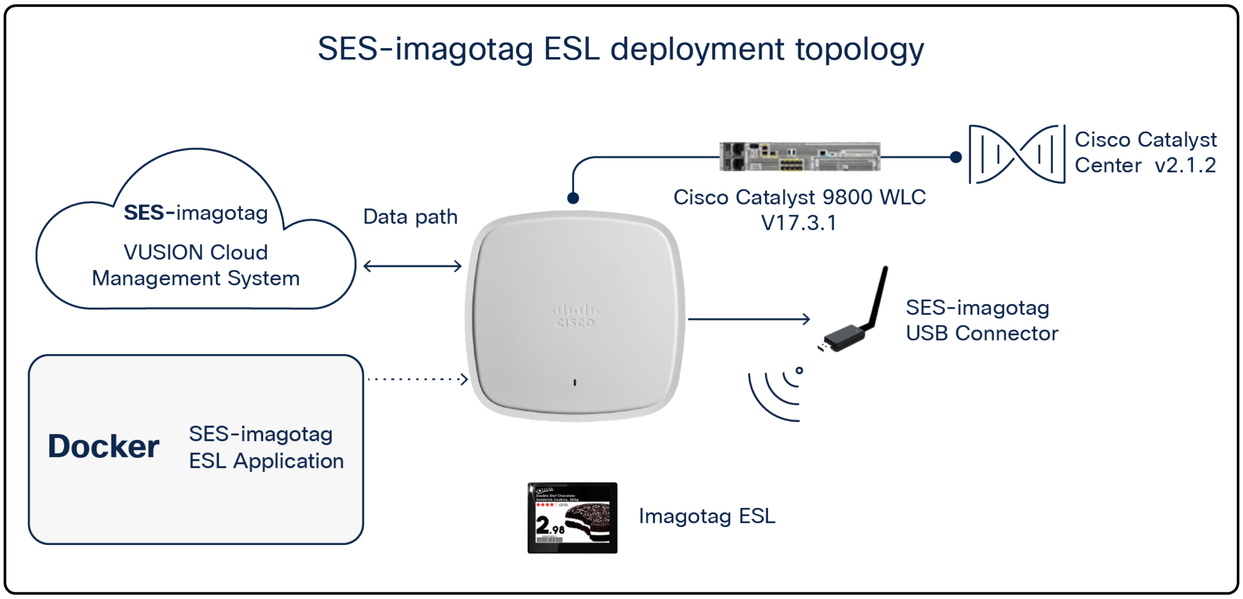


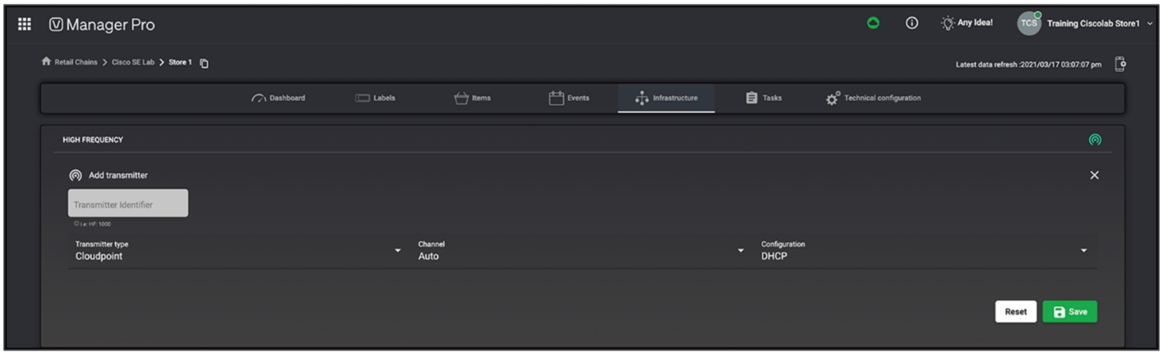
Figure 54.
SES-imagotag ESL solution topology

Prerequisite steps:

1. Ensure that the network topology is the same as depicted in Figure 55.
2. When deploying the SES-imagotag ESL application to the access point, ensure that the following configurations have been set:
    - APC_ADDRESS=<VUSION Cloud URL specified by SES-imagotag>
    - APC_PORT=7354
    - CHANNEL=<channel # you would like your SES-imagotag USB connector to broadcast>
    - VCLOUD=false

Step 1: Add your SES-imagotag USB dongle into VUSION Cloud:

- Log in to VUSION Cloud.
- Navigate to Infrastructure, click Add, then input the Transmitter ID, which is the AP ID printed directly on the SES-imagotag USB dongle, then click Save.
    a **Note:** If your app was deployed to the access point with the proper configurations, it should show that it is connected.



Latest data refresh :2021/03/17 03:07:07 pm

HIGH FREQUENCY

Add transmitter

Transmitter Identifier

i.e: HF: 1000

Transmitter type: Cloudpoint

Channel: Auto

Configuration: DHCP

Figure 55.
Adding the SES-imagotag USB dongle's ID into VUSION Cloud

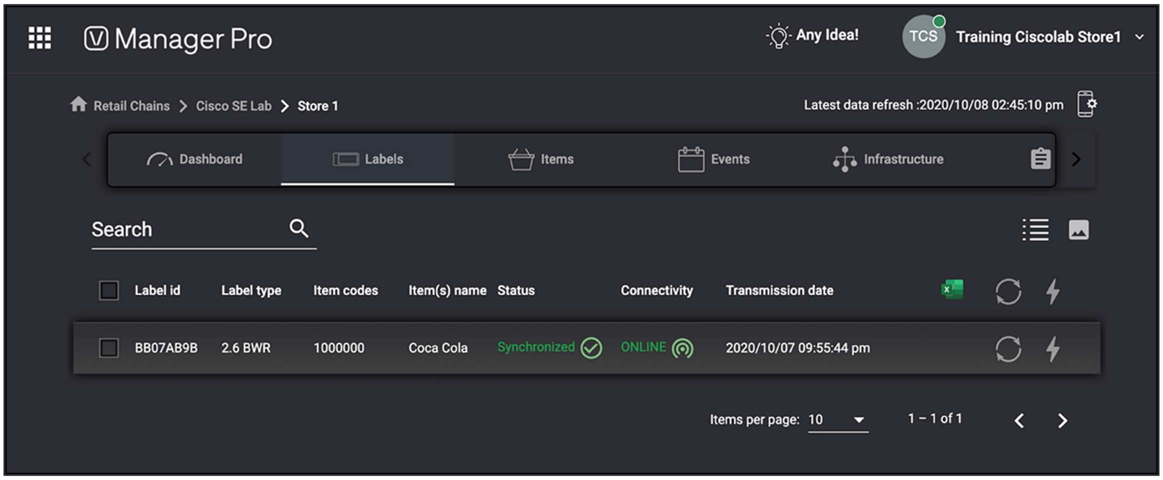
Step 2: Add an ESL into VUSION Cloud

- Navigate to Labels, click the up arrow on the right, and enter the label ID, which can be found directly on the ESL, then click Save.

Step 3: Associate an item to the ESL

Items are essentially the picture plus the price of the items you're planning to advertise on the ESL screens. This step assumes that the items have already been imported into VUSION Cloud.

- Navigate to Items and copy the item code for one of the items you'd like to display on the ESL you've added to VUSION cloud in the previous step.
- Navigate to Labels, click the ESL you've added, click Matchings, add the item code into the Item code input field, then click Synchronize. After some time, VUSION Cloud will show that the ESL is successfully connected and synchronized.


Manager Pro
Any Idea!
TCS Training Ciscolab Store1
Retail Chains > Cisco SE Lab > Store 1
Dashboard
Labels
Items
Events
Infrastructure
Search

Latest data refresh :2020/10/08 02:45:10 pm

□	Label id	Label type	Item codes	Item(s) name	Status	Connectivity	Transmission date
□	BB07AB9B	2.6 BWR	1000000	Coca Cola	Synchronized ✓	ONLINE	2020/10/07 09:55:44 pm

Items per page: 10

1 – 1 of 1

Figure 56.
SES-imagotag ESL synchronized properly with the assigned item

Step 4: Verify on the physical ESL

- The ESL you've added should now also show the item you associated with it in the previous step.

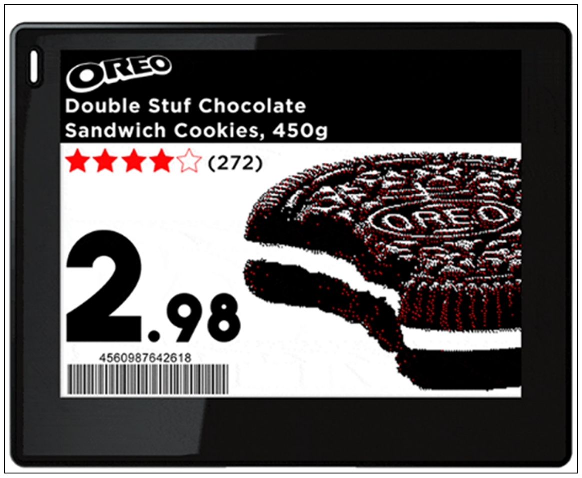


Figure 57.
Physical SES-imagotag ESL

Sample use cases

Cisco's Application Hosting on Catalyst Access Points provides endless possibilities to developers working in the field of IoT. This section offers some ideas of use cases as inspiration.

Use case 1: Healthcare

Background: A pandemic hit the world in 2020, caused by a virus identified as COVID-19. Due to its contagious nature, the virus has caused devastating effects throughout the globe.

Pain points: Infected individuals must be quarantined immediately to prevent further spread of the virus. The contagiousness of this virus has caused immense impacts on both patients' well-being and medical facilities' ability to manage operations.

How Application Hosting can address the pain points: With Application Hosting on Catalyst Access Points, you can create applications that respond to external stimuli such as voice control devices (i.e., Google Home, Amazon Echo). Your IOx application can use these received external parameters to trigger actions such as calling for a nurse, changing the temperature, adjusting the bed, etc. Such technology increases the convenience of bedridden patients and helps medical facility staff maintain maximum social distancing during COVID-19.

The figures below illustrate these examples.

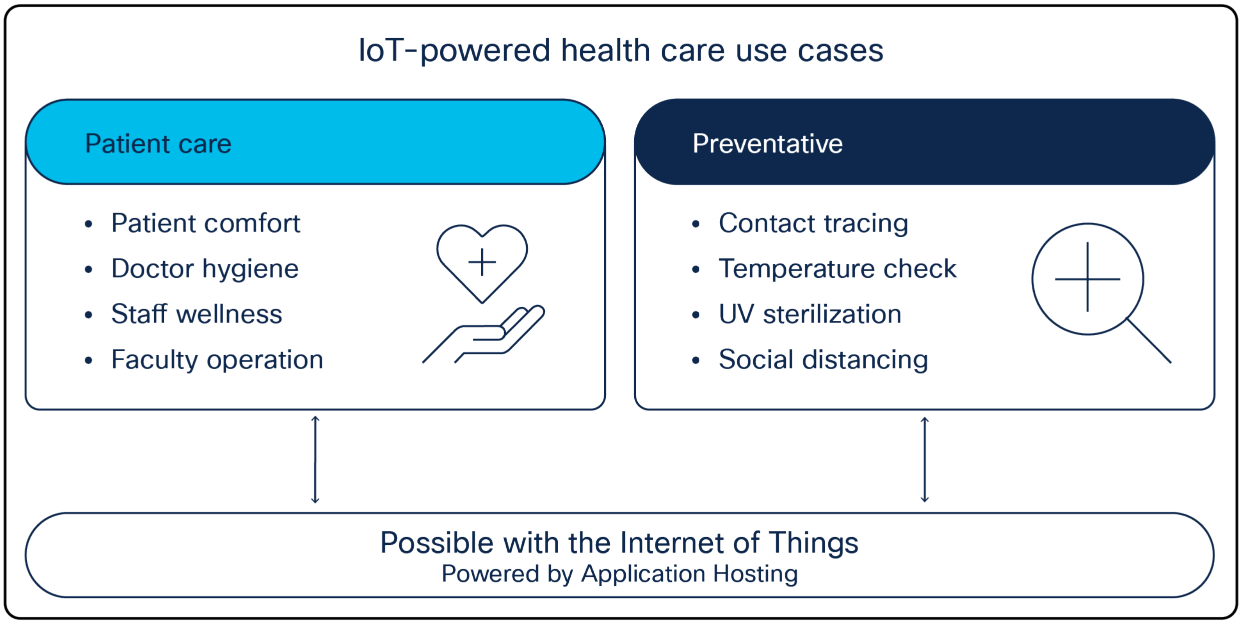


Figure 58.
Application Hosting healthcare use cases

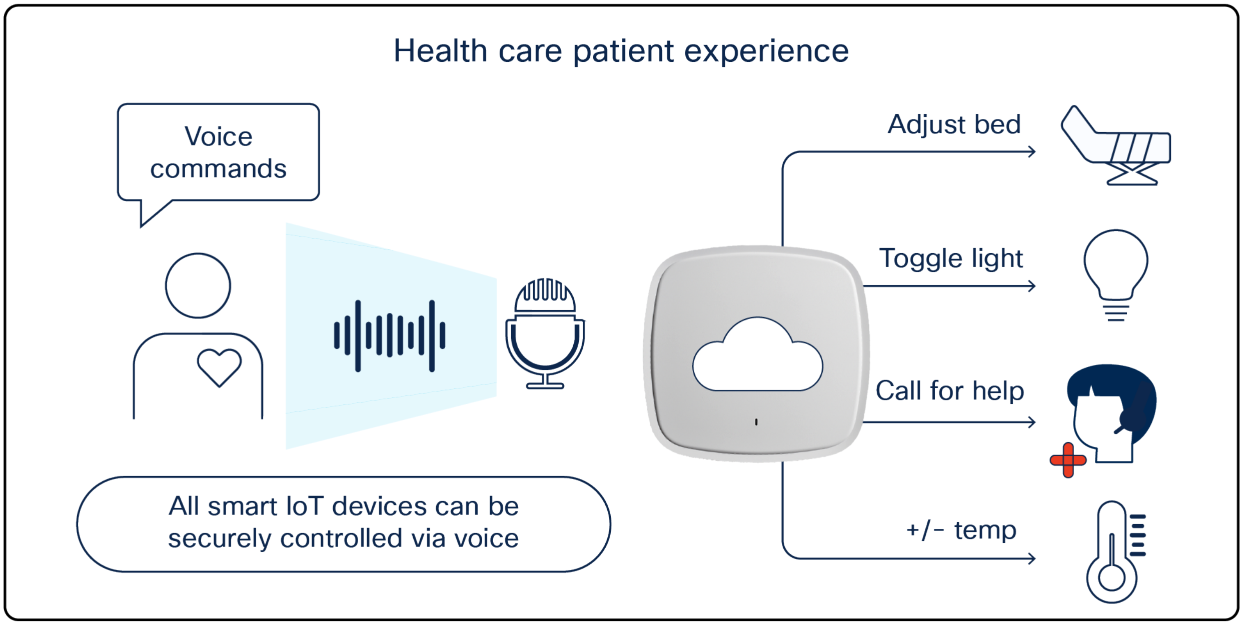

Health care patient experience
Voice commands
All smart IoT devices can be securely controlled via voice
Adjust bed
Toggle light
Call for help
+/- temp

Figure 59.
Using Application Hosting on Catalyst Access Points in a patient room

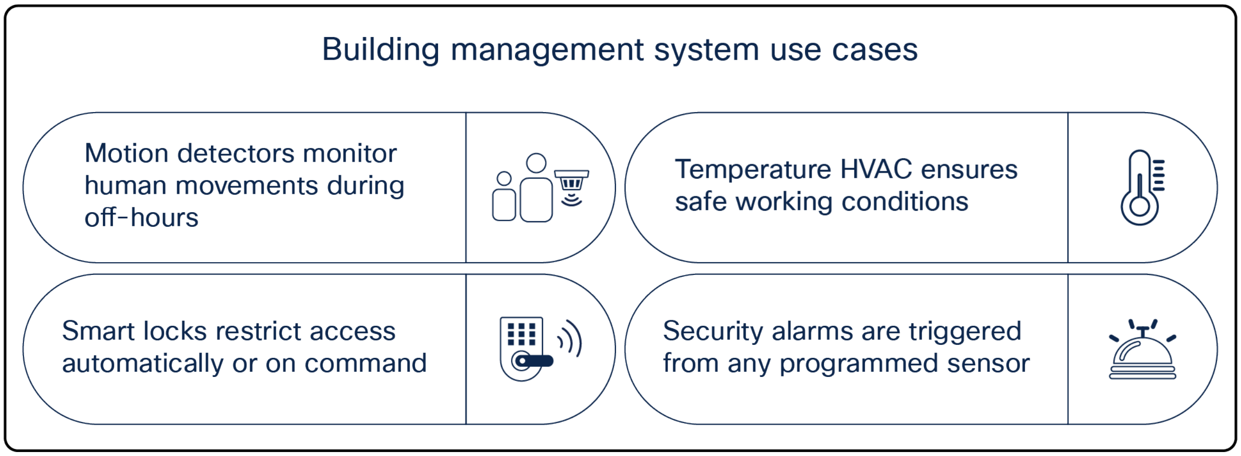
Use case 2: Building management system

Background: A sizable multiregional enterprise is looking for smarter ways to manage facilities spread through multiple countries.

Pain points: Managing these facilities and ensuring 24/7 security can be a difficult task. Often a large team of facilities managers must be onsite to ensure the safety and security of employees. Such a manual process increases personnel costs for the company and leaves security vulnerable to potential human error.

How Application Hosting can address the pain points: With Application Hosting on Catalyst Access Points, you can create applications that directly communicate with smart building management devices throughout all facilities in multiple regions at once. You can have all devices report information back to a central management server, creating a convenient command center for facilities management.

The figures below illustrate these examples.


Building management system use cases

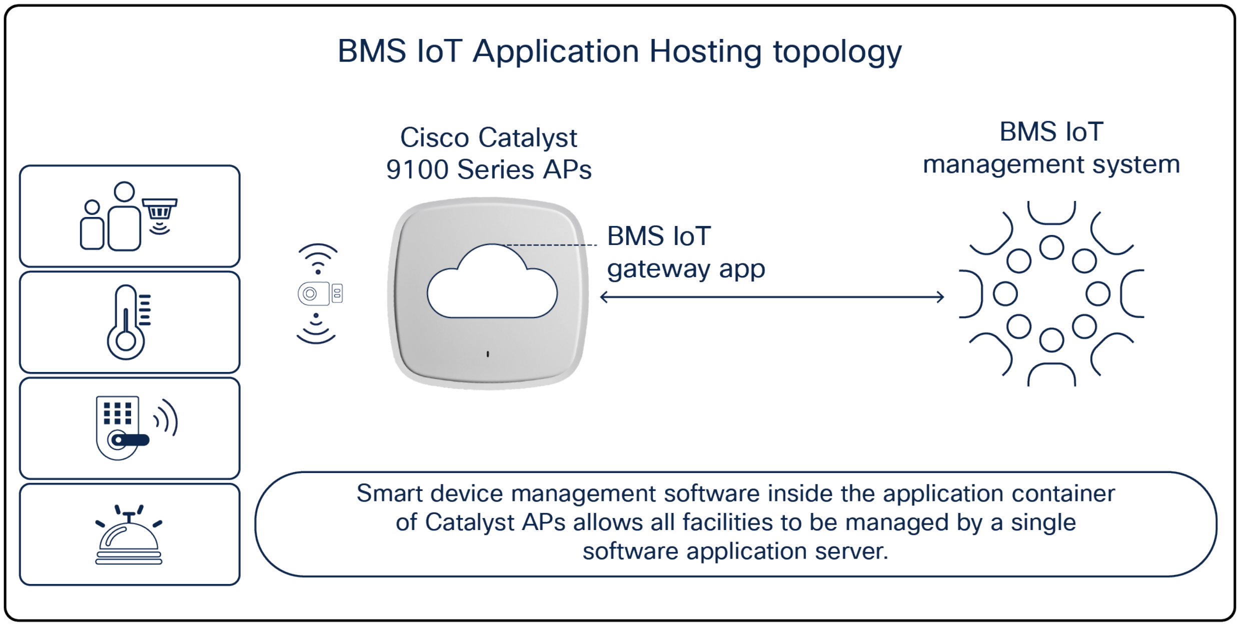
Motion detectors monitor human movements during off-hours

Temperature HVAC ensures safe working conditions

Smart locks restrict access automatically or on command

Security alarms are triggered from any programmed sensor

Figure 60.
Building management system sample use cases


BMS IoT Application Hosting topology

Smart device management software inside the application container of Catalyst APs allows all facilities to be managed by a single software application server.

Figure 61.
Smart devices communicating to a building management system through Catalyst access points

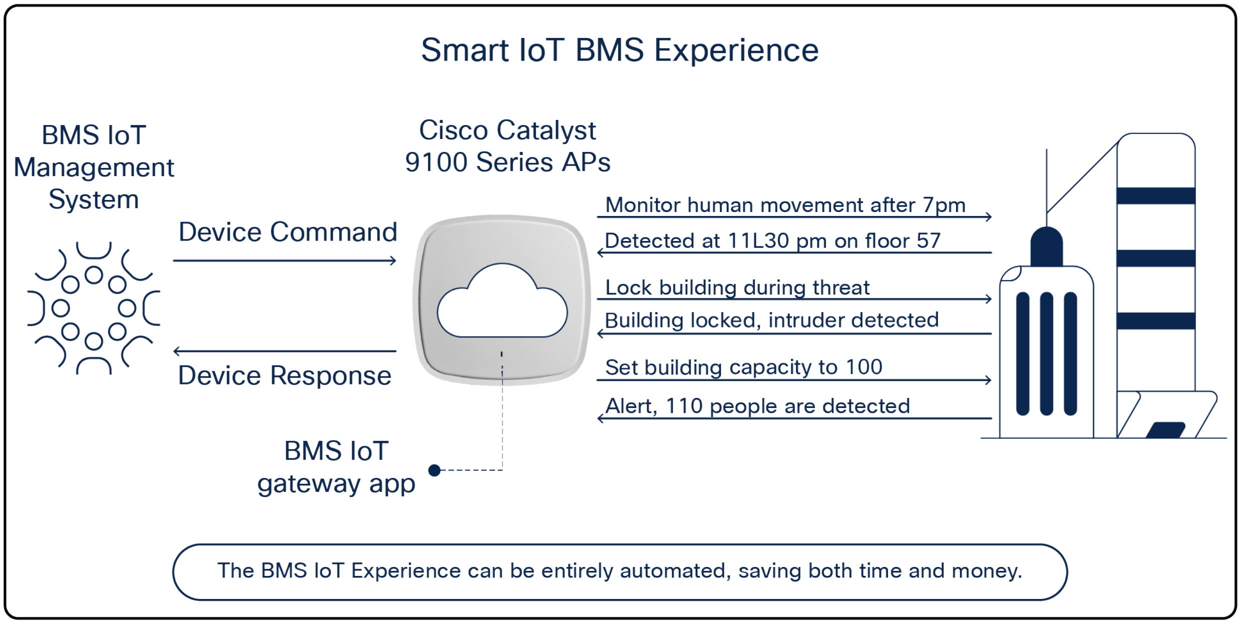

Smart IoT BMS Experience
BMS IoT Management System
Cisco Catalyst 9100 Series APs
Device Command
Device Response
Monitor human movement after 7pm
Detected at 11L30 pm on floor 57
Lock building during threat
Building locked, intruder detected
Set building capacity to 100
Alert, 110 people are detected
BMS IoT gateway app
The BMS IoT Experience can be entirely automated, saving both time and money.

Figure 62.
Leveraging Application Hosting to monitor multiple buildings

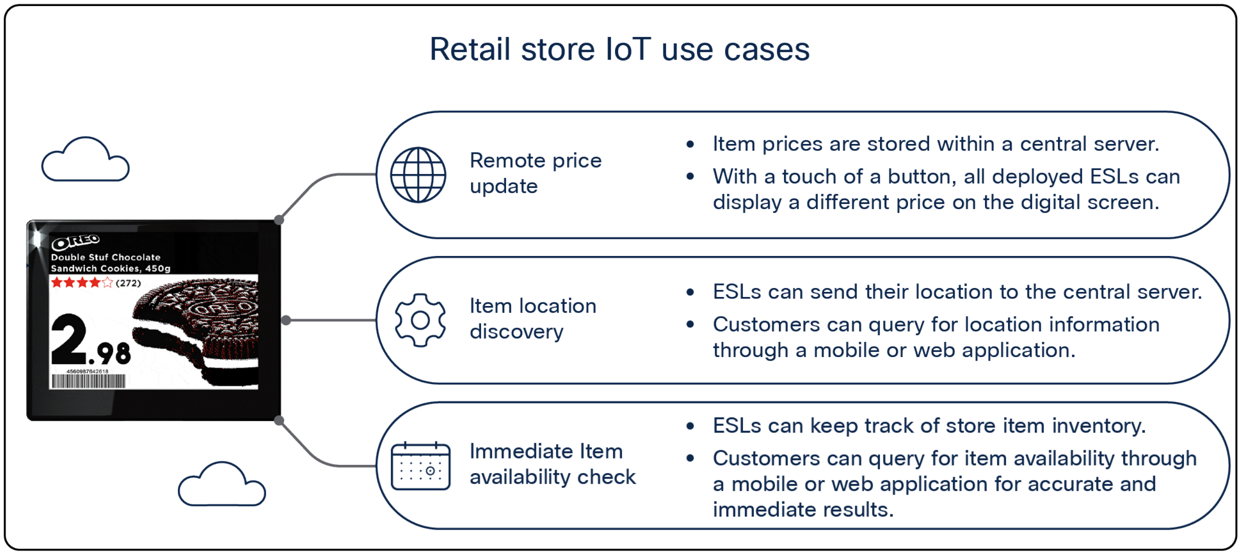
Use case 3: Retail stores

Background: The CEO of a large retail chain that directly competes with other e-commerce platforms such as Amazon is seeking ways to reduce overhead.

Pain points: It is difficult for in-store retailers to compete with the flexible management of an e-commerce platform. Tasks such as changing the prices of items, helping customers locate items in-store, and even showing the availability of specific items all require significantly higher overhead in a physical store than online.

How Application Hosting can address the pain points: With Application Hosting, you can create applications that directly communicate with ESLs. ESLs are used in place of standard price tags and enable in-store retailers to update item prices remotely from a computer, and to discover the availability and physical location of any item in the store through a web or mobile application.

The figures below illustrate these use cases.



Retail store IoT use cases

Remote price update

- Item prices are stored within a central server.
- With a touch of a button, all deployed ESLs can display a different price on the digital screen.

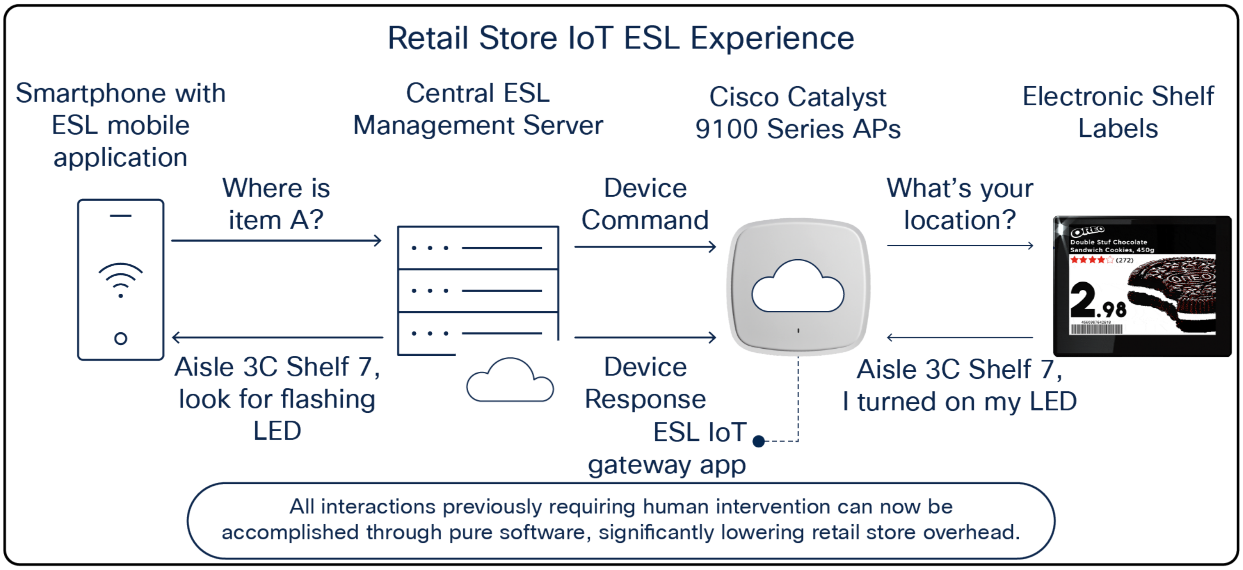
Item location discovery

- ESLs can send their location to the central server.
- Customers can query for location information through a mobile or web application.

Immediate Item availability check

- ESLs can keep track of store item inventory.
- Customers can query for item availability through a mobile or web application for accurate and immediate results.

Figure 63.
Retail store IoT use cases



Retail Store IoT ESL Experience

Smartphone with ESL mobile application
Central ESL Management Server
Cisco Catalyst 9100 Series APs
Electronic Shelf Labels
Where is item A?
Device Command
What's your location?
Aisle 3C Shelf 7, look for flashing LED
Device Response
Aisle 3C Shelf 7, I turned on my LED
ESL IoT gateway app
OREO
Double Stuf Chocolate Sandwich Cookies, 450g
(272)
2.98

All interactions previously requiring human intervention can now be accomplished through pure software, significantly lowering retail store overhead.

Figure 64.
Retail store IoT ESL experience

Useful CLI commands

Access point commands

- View the status of the application loaded onto the access point.

```
Nolan_AP#show iox applications
Total Number of Apps : 1
--------------------------
App Name : communication_daemon
App Ip : 192.168.11.2
App State : RUNNING
App Token : 0f690ed5-c341-4342-b5f3-7ab39ade8ea1
App Protocol : usb
App Grpc Connection : Down
Rx Pkts From App : 0
Tx Pkts To App : 0
Tx Pkts To Wlc : 0
Tx Data Pkts To DNASpaces : 0
Tx Cfg Resp To DNASpaces : 0
Rx KeepAlive from App : 0
Dropped Pkts : 0
App keepAlive Received On : NA
```

- View access point information as well as the information of any device connected via USB.

```
Nolan_AP#show inventory
NAME: C9130AX, DESCR: Cisco Catalyst 9130AX Series Access Point
PID: C9130AXI-B , VID: V01, SN: FJC240511KH

Entity Name         : USB Module
Detected            : Yes
Status              : Enabled
Product ID          : ea60
Vendor ID           : 10c4
Manufacturer        : Silicon Labs
Description         : CP2102N USB to UART Bridge Controller
Serial Number       : 0cd351d9f35
Max Power           : 100 mA
```

- Verify the IOx status on the access point

```
Nolan_AP#show iox status
IOx Status             : Enabled
CAF Status             : Up
CAF Token              : 9e054a32-d1ff-464e-aadd-6c5934959310
CAF Port               : 8443
```

Cisco IOS XE WLC commands

- View the status of the USB modules connected to all joined access points.

```
Nolan_eWLC#show ap module summary
Output of show ap module summary:
AP Name             External Module      External Module PID  External Module Description
------------------------------------------------------------------------------------------
Nolan_AP1           Enable               10c4/ea60/100        CP2102N USB to UART Bridge C
Nolan_AP2           Enable               10c4/ea60/100        CP2102N USB to UART Bridge C
```

- View the USB module state of each joined access point, along with other information.
- **Note:** Below is only a snippet of the show command output.

```
Nolan_eWLC #show ap config general
USB Module Type                                 : USB Module
USB Module State                                : Enabled
USB Operational State                           : Enabled
USB Override                                    : Disabled
```

- View the Application Hosting status of each joined access point.

```
Nolan_eWLC#show ap apphost summary
AP Name         AP Mac            Apphost Status          CAF Port         Apphost HW capable
---------------------------------------------------------------------------------------------
SS-2027         00ee.ab18.b620    Up                       8443             Yes
Axel-2036       04eb.409f.a000    Up                       8443             Yes
```

- Configure an auxiliary-client interface (AHI) for IOx app traffic segmentation,
- **Note:** Ensure that this VLAN exists within your Catalyst 9800 controller.

```
Nolan_eWLC#config terminal
Nolan_eWLC(config)# <AP Join Profile Name>
Nolan_eWLC(config-ap-profile)# auxiliary-client interface vlan-id <VLAN ID>
```

Common questions

Q. What Cisco Catalyst Center license is required for Application Hosting?

A. The customer must be subscribed to a Cisco DNA Advantage license.

Q. How many applications can be deployed to each access point?

A. Two applications can be deployed to each access point, contingent on available resources on the access point and the resources required by each application. However, a Cisco Catalyst Center Application Hosting application cannot be loaded parallel with a Cisco Spaces Indoor IoT Services application.

Q. How is data security handled in Application Hosting?

A. Application Hosting security is divided into three parts:

- Segmentation of traffic:

When a deployed application needs to communicate to sources external to the access point's network, it can do so using a VLAN different from the access point’s management VLAN. This is accomplished with a configurable featured called the auxiliary-client interface and is enabled through WLC CLI commands.

- AP Resource allocation:

Within the access point, there are resources (CPU, memory, storage) dedicated to Application Hosting. The Application Hosting application usages will never conflict with the access point's client-serving resources and vice versa.

- Data encryption:

Cisco provides the platform infrastructure to host the IoT application; therefore, any data encryption and security on those lines between the application and the IoT devices and between the application and the application server is taken care of by each partner's specific solution.

Q. Does the access point need a direct connection to Cisco Catalyst Center for application deployment and management?

A. Yes, the access point requires a direct, routable VLAN connection to Cisco Catalyst Center that isn't using NAT. The access point uses HTTPS with port 8443 to communicate with Cisco Catalyst Center. If a direct connection isn't available, application deployment and management will fail.

Q. What USB protocol do the access points use for Application Hosting?

A. USB serial.

Q. Is Application Hosting on Catalyst Access Points supported on Cisco AireOS wireless controller platforms?

A. No, Application Hosting on Catalyst Access Points is supported only on Cisco Catalyst wireless controller deployments.

Q. How is the maximum size of the IOx application calculated?

A. The size of the IOx application is the size of the file in its final compressed form (.tar). The package.tar file size should not exceed 10 MB.

When the IOx application is deployed on a Cisco Catalyst access point, the package.tar file is placed in the /tmp directory. Depending on your access point model, this /tmp directory has a maximum size of approximately 80 MB. The package.tar file contents are extracted into the /tmp directory, resulting in an artifacts.tar.gz file, which, when extracted, produces the rootfs file (rootfs.img). You need to copy this rootfs file (rootfs.img) into the /storage directory.

The total size of the original package.tar file and the extracted rootfs file size should not exceed the maximum size of the /tmp directory (~80 MB). Usually, when the contents of a 20-MB package.tar file are extracted, the resulting rootfs file size after extraction is nearly 60 MB.

Q. What are the resource specifications for hosting an application on each access point?

A. The following are the resource specifications for each access point:

Table 4. Application Hosting Platform Resource Specifications

Access point	CPU architecture	CPU allocated (MFLOPS)	Max memory allocated (RAM)	Application type	Maximum number of apps	Maximum cores for IOx app	Maximum storage	USB support for IOx
C9105AXI	ARM 32-bit	1200	100 MB	Docker	2	2	~10 MB	No
C9105AXW	ARM 32-bit	1200	100 MB	Docker	2	2	~10 MB	Yes
C9115AX	ARM 64-bit	4800	100 MB	Docker	2	2	~10 MB	Yes
C9117AX	ARM 64-bit	4800	100 MB	Docker	2	2	~10 MB	Yes
C9120AX	ARM 64-bit	4800	100 MB	Docker	2	2	~10 MB	Yes
C9130AX	ARM 64-bit	4800	100 MB	Docker	2	2	~10 MB	Yes
C9124AX	ARM 64-bit	4800	100 MB	Docker	2	2	~10 MB	No
C9136I	ARM 64-bit	4800	100 MB	Docker	2	2	~10 MB	Yes
CW9162I	ARM 64-bit	4800	100 MB	Docker	2	2	~10 MB	Yes
CW9164I	ARM 64-bit	4800	100 MB	Docker	2	2	~10 MB	Yes
CW9166I	ARM 64-bit	4800	100 MB	Docker	2	2	~10 MB	Yes
CW9166D1	ARM 64-bit	4800	100 MB	Docker	2	2	~10 MB	Yes

Q. What is the minimum Power over Ethernet (PoE) type for each access point to enable its USB port?

A. The following are the minimum PoE types to be used to enable each access point's USB port.

Table 5. Application Hosting Platform PoE Capabilities

Access point	PoE type	USB status and power output
C9105AXI	None, no USB port	No USB port
C9105AXW	802.3at	Y (4.5W)
C9115AXI/E	802.3at	Y (3.75W)
C9117AXI	802.3bt	Y (4.5W)
C9120AXI/E	802.3at	Y (4.5W)
C9130AXI/E	802.3bt	Y (4.5W)
C9124AXI/D	None, no USB port	No USB port
C9136I	802.3bt	Y (9W)
CW9162I	802.3at	Y (4.5W)
CW9164I	802.3bt	Y (4.5W)
CW9166I	802.3bt	Y (4.5W)
CW9166D1	802.3bt	Y (4.5W)

Q. How do I contact Cisco's Application Hosting Team for support or business inquiries?

A. Please contact apphosting_ap_support@cisco.com.

Useful links

All Cisco Catalyst Center guides

- Install and upgrade guides:

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-installation-guides-list.html

Frequently asked questions

- https://developer.cisco.com/docs/app-hosting-ap/#!faqs

IOx application guides

- Application Hosting on Catalyst 9100 Access Points:

https://developer.cisco.com/app-hosting-ap/

- Application Hosting on Cisco Catalyst Access Points:

https://developer.cisco.com/docs/app-hosting-ap/

- What Is IOx?

https://developer.cisco.com/docs/iox/#!introduction-to-iox/what-is-iox

- What Is ioxclient?

https://developer.cisco.com/docs/iox/#!what-is-ioxclient

- Tutorial: Build Sample Docker Type IOx App Using Docker Toolchain:

https://developer.cisco.com/docs/iox/#!tutorial-build-sample-docker-type-iox-app-using-docker-toolchain/tutorial-build-sample-docker-type-iox-app-using-docker-toolchain

Application Hosting video guides

- The Internet of Things – Application Hosting Overview and Use Cases
  - https://www.youtube.com/watch?v=ZDRkKOTLat8&ab_channel=CiscoWLAN
- The Internet of Things – Application Hosting Deployment and Technical Deep Dive
  - https://www.youtube.com/watch?v=0u3FGlRrdhU&ab_channel=CiscoWLAN

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA
01/24

C07-744305-05