Application Hosting on Catalyst APs Deployment Guide

Americas Headquarters
Cisco Systems, Inc. 170 West Tasman Drive
San Jose, CA 95134-1706 USA
http://www.cisco.com
Tel: 408 526-4000 800
553-NETS (6387)

Table of Contents

Overview of Application Hosting on Catalyst Access Points

Enterprise wireless networks are a rapidly growing part of today's age of 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 now more connected than ever before, giving us the ability to solve once seemingly complex problems with simple yet elegant solutions. However, this enablement of endless technological possibilities has also triggered a surge of both dependency and expectation that technology must continue to better every aspect of our daily lives. Thus, the concept of Internet-of-Thing was created, and to spearhead such a movement; Cisco has created a state-of-the-art technology known as Application Hosting on Catalyst APs.

Cisco's Application Hosting on Catalyst APs feature at a high-level provides users with the ability to load 3rd party containerized IOx applications directly onto Cisco's access points to leverage them as an IoT gateway. Once loaded, the 3rd party application now gains complete access to specific access point software and hardware resources. Depending on the IOx application developed, it can have the ability to promptly communicate with 3rd party software through its internal VLAN, and 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. With the ability for 3rd party vendors to create applications and leverage these access points as IoT gateways, it has created endless possibilities for the Internet-of-Things movement.

This document covers the deployment of Cisco's Application Hosting on Catalyst APs feature with Cisco DNA Center.

Supported Software

Table 1. Cisco DNA Center and IOx-XE Software Compatibility Matrix

Cisco DNA Center Software Release	IOS-XE WLC Software Release
2.1.1.x	17.3.1

Supported Hardware

Table 2. Supported Access Points

Access Point PID	OS Type
C9105AXI	AP-COS
C9105AXW	AP-COS
C9115AX	AP-COS
C9117AX	AP-COS
C9120AX	AP-COS
C9130AX	AP-COS

Table 3. Supported Wireless LAN controllers

Wireless LAN Controller PID	OS Type
C9800-CL	IOS-XE
C9800-L	IOS-XE
C9800-40	IOS-XE
C9800-80	IOS-XE

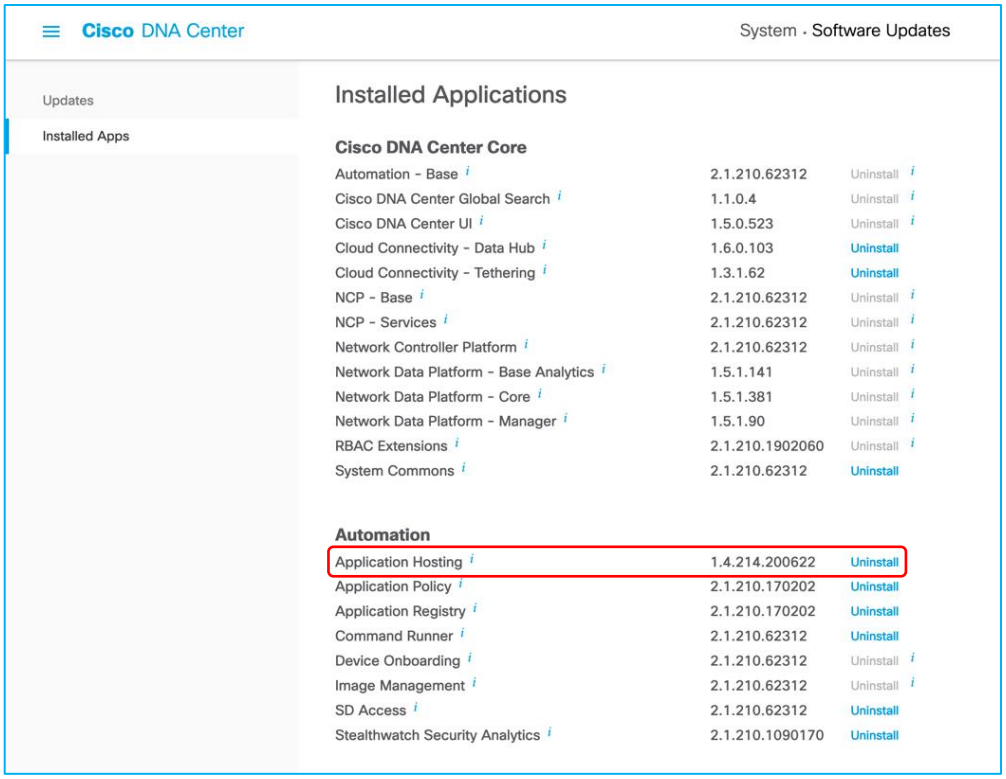
Prerequisite: Installing the Application Hosting Package from Cisco DNA Center

Cisco DNA Center provides the option to download an Application Hosting package called **Application Hosting**. You will be able to download and install these packages on top of the base Cisco DNA Center software.

1. *To install the App Hosting Packages, log in to Cisco DNA Center and open the menu in the top left corner.*

2. *Click **System > Software Updates**, then click **Installed Apps** on the left. Scroll down to **Automation** and you will find the packages available there for download or install (**Figure 1**).*

Figure 1. Location of the Application Hosting package



Application Hosting High-level Deployment Workflow

Figure 2. Application Hosting Deployment Steps

Day 0: Setup Cisco DNA Center Day 0 Configurations

Note: Skip to Day 1 if you already have Day 0 Cisco DNA Center configuration completed.

1. Create a Network Hierarchy Site (Area, Building, Floors) via the Network Hierarchy page.
2. **Optional:** Configure the Network Hierarchy settings via the Network Settings page.
3. Discover WLC & access points via the Discovery page.
4. Assign WLC & access points to the Network Hierarchy created via the Inventory page.

Day 1: Upload & Deploy IOx Application

1. Upload a 3rd party IOx application to Cisco DNA Center via the IoT Services page.
2. Deploy the uploaded application to specific access points.

Day 2: Monitor IOx Application

1. Configure the 3rd party application's 3rd party management system to begin managing and monitor the applications deployed on the access points.

Application Hosting on Catalyst APs Topology

Figure 3. IOx Application Hosting General Topology

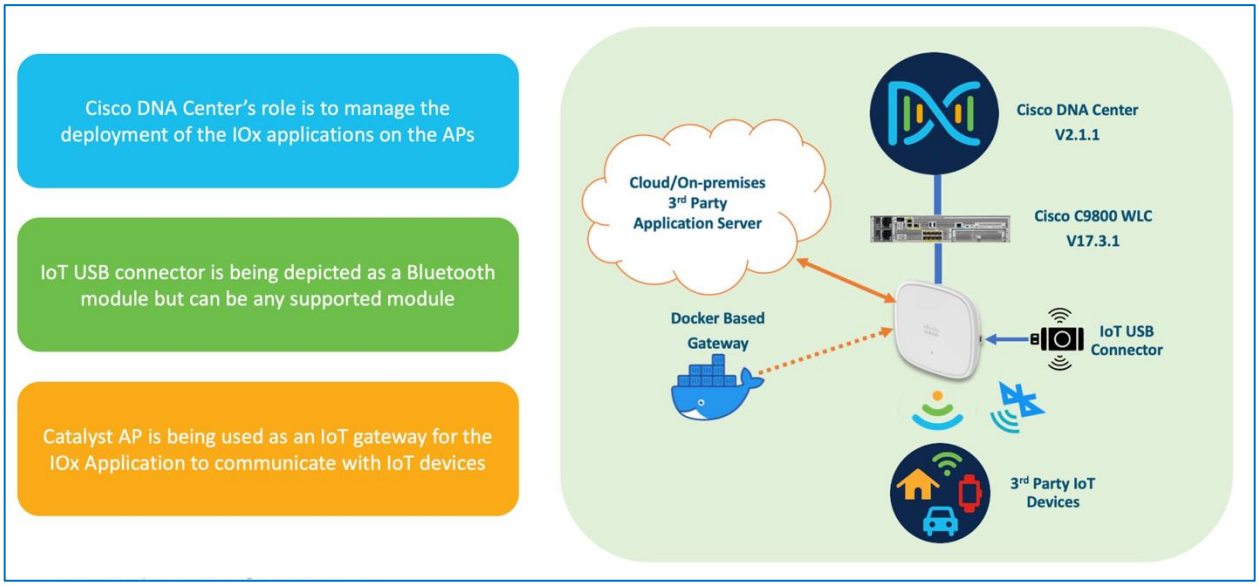
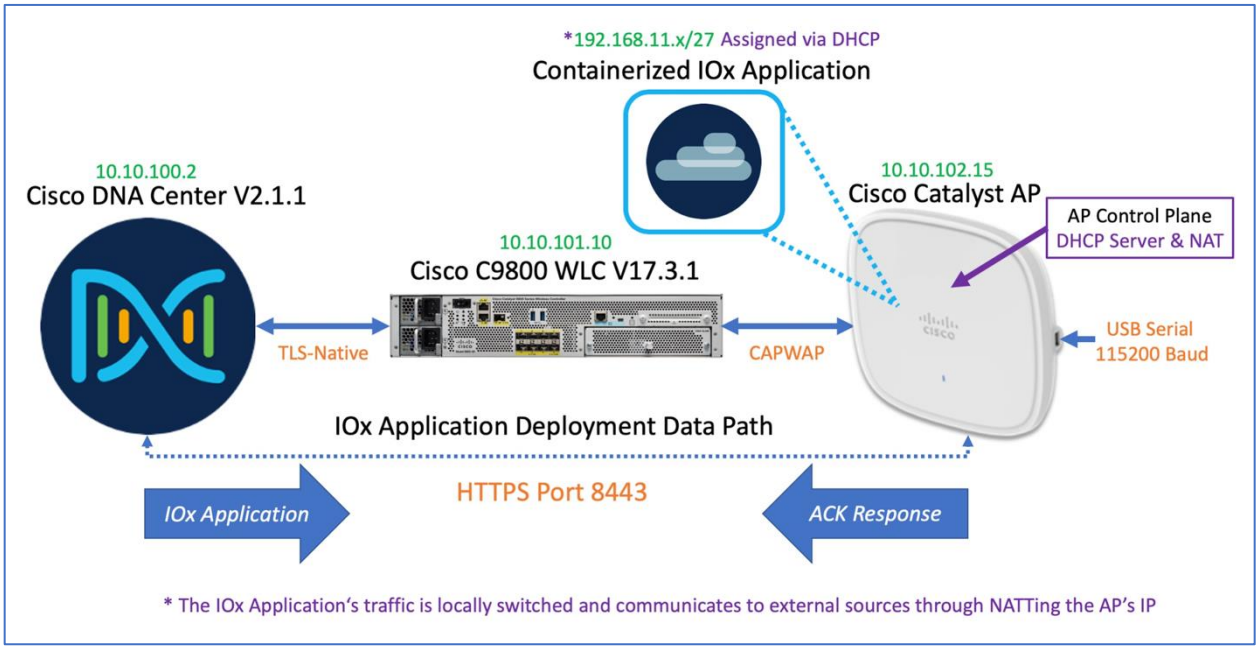


Figure 4. IOx Application Network Topology



Day 0: Setup Cisco DNA Center Configuration

The purpose of the following section is to provide users with step by step instructions with regards to the day 0 configurations necessarily to begin using Application Hosting on Catalyst APs.

Note: Skip to the Day 1 section if you already have Day 0 Cisco DNA Center configuration completed.

Part 1 Day 0 Configuration - Building a Site Hierarchy

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

Section Goals: To create and configure Network Hierarchy sites & settings to define shared services, device credentials, and SNMP community strings.

Step 1: Navigate to the Network Hierarchy Page

1. ***Option 1:*** *Log in to Cisco DNA Center UI. Scroll down to the* ***Network Configurations*** *section and choose* ***Design*** *(****Figure 5.****).*

2. ***Option 2:*** *Click on the menu at the top left-hand corner of the screen. Click on* ***Design*** *then* ***Network Hierarchy*** *(****Figure 6.****).*

Figure 5. Location of the Design Page on Cisco DNA Center's Home Page.

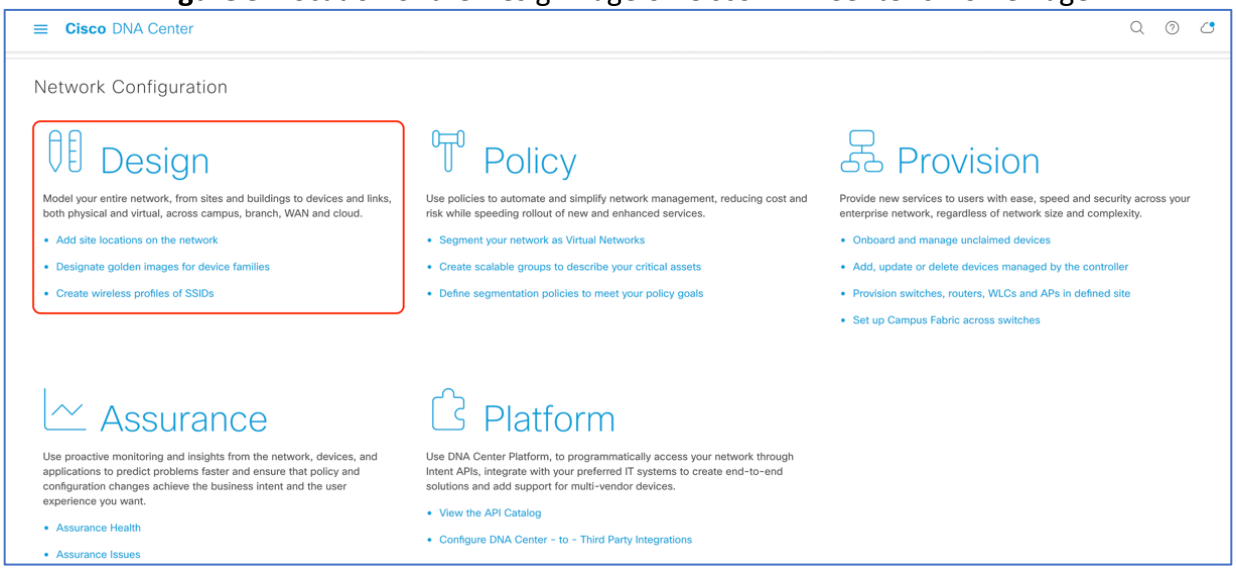
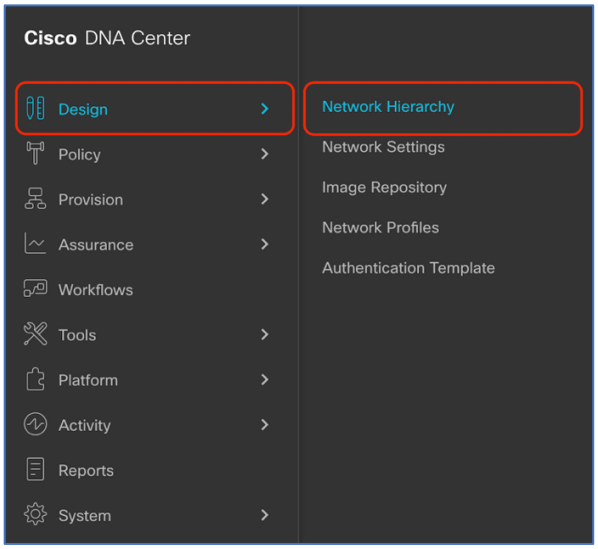


Figure 6. Location of Network Hierarchy from the Menu.



Step 2: Create Sites, Building, and Floors

To allow Cisco DNA 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.

1. *Option 1 - To create a site, click on the **Add Site Button** (**Figure 7.**), and a menu will open up and provide you an option to create a child Area, Building or Floor within a desired site.*

2. *Option 2 – To create a site, click on the gear icon (**Figure 8.**) next to the site you would like to create a child site under.*

3. *When creating a floor, click on **Upload file** to upload a floor of a building (**Figure 9.**).*
    a. Floor plans must be in the format of DXF, DWG, JPG, GIF, or PNG.

The behavior of Cisco DNA 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 only create areas and buildings within the Global site or other areas, and can only create Floors within Buildings.

- When creating a building within design hierarchy, it is critical that you use a real physical street address for your sites. Cisco DNA Center uses the street address to select the country codes for the wireless implementation.

Figure 7. Clicking **Add Site** Within the Design – Network Hierarchy page

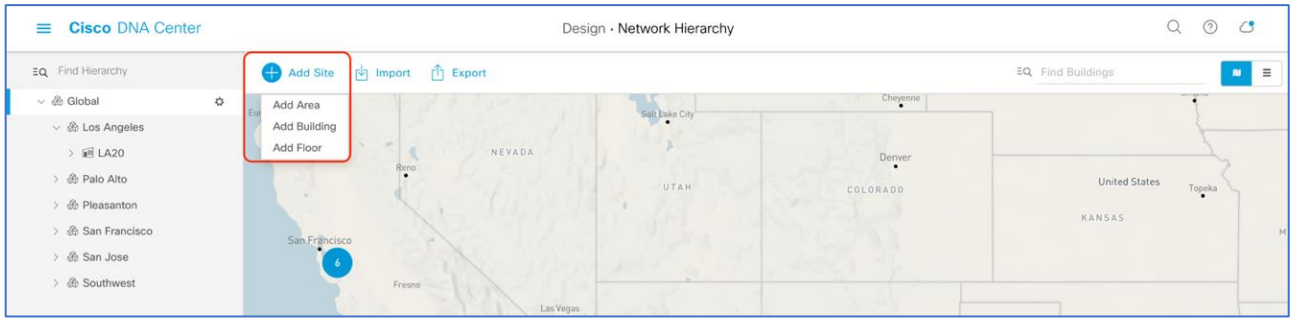


Figure 8. Clicking the gear icon Next to an area Within the Design – Network Hierarchy page

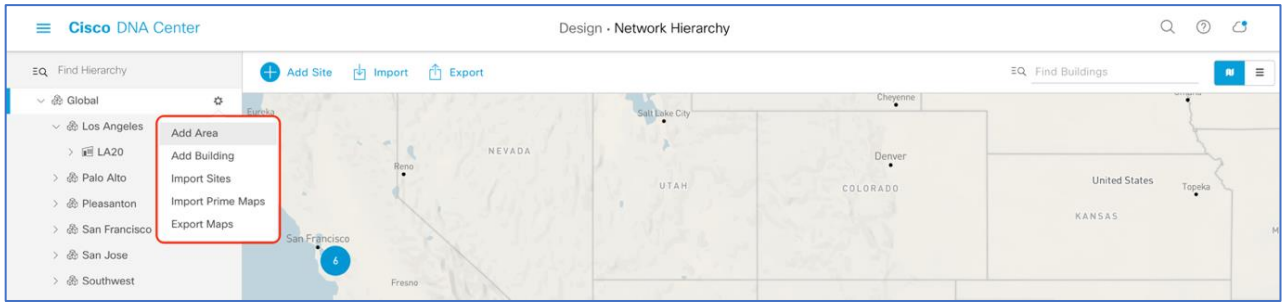
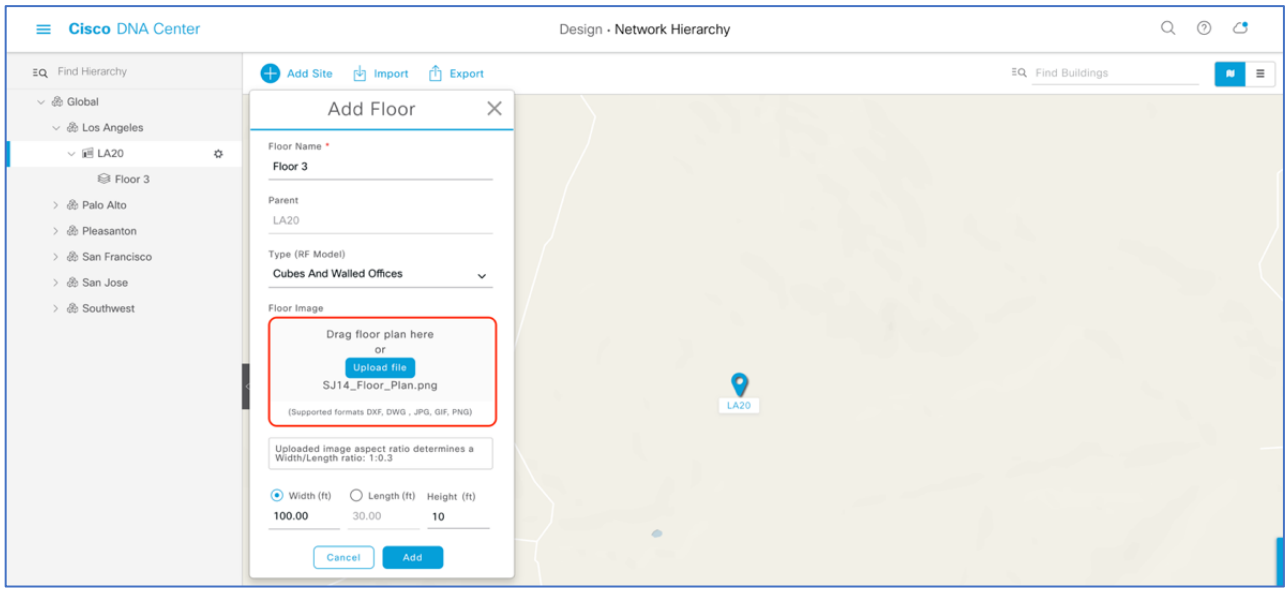


Figure 9. Location of the **Upload file** to upload a floor plan during floor creation

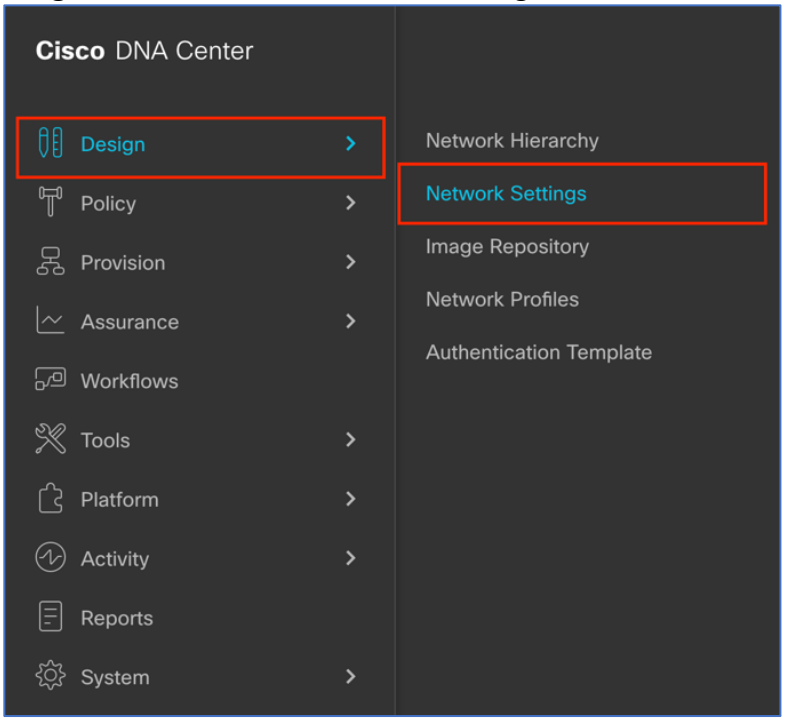


Step 3: Navigate to the Network Settings Page

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

1. *To navigate to the **Network Settings** page, open the menu at the top left-hand corner of the screen. Click on **Design** then **Network Settings** (**Figure 10.**).*

Figure 10. 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 DNA Center's IP address is prepopulated in the **Syslog Server** and **SNMP Server** fields. This will enable syslog and SNMP traps to be sent to Cisco DNA Center from network devices when a WLC is added to Cisco DNA Center.

1. *Click the **Device Credentials** subtab to view the existing device CLI credentials and SNMP community strings (**Figure 11.**).*

2. *Click on the **Add** button to create new credential entries (**Figure 12.**). Cisco DNA Center uses these credentials to discover the network devices.*

Figure 11. Workflow to Add Device Credentials to the Network Settings.

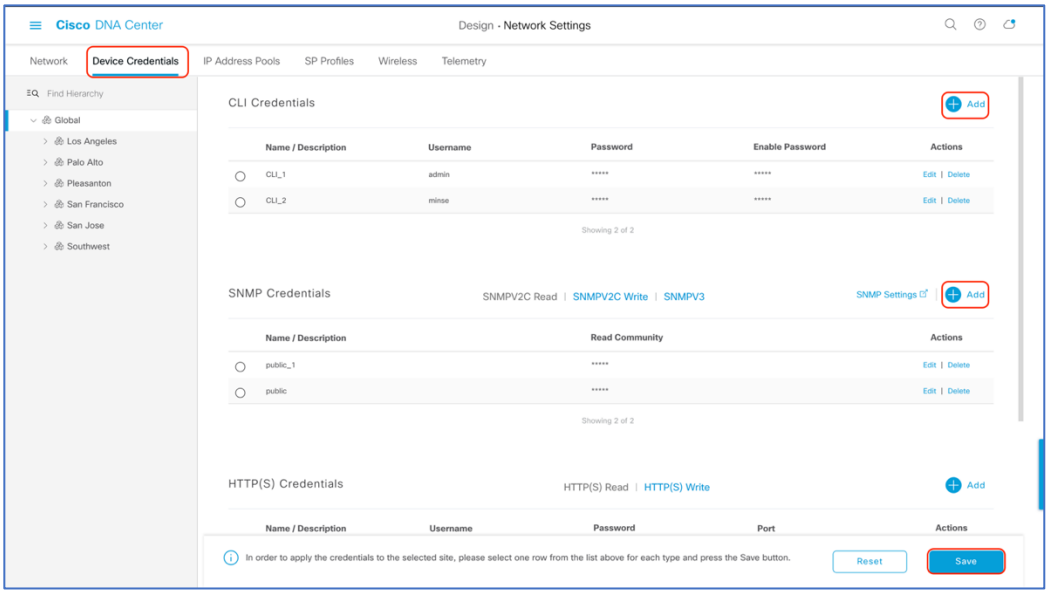
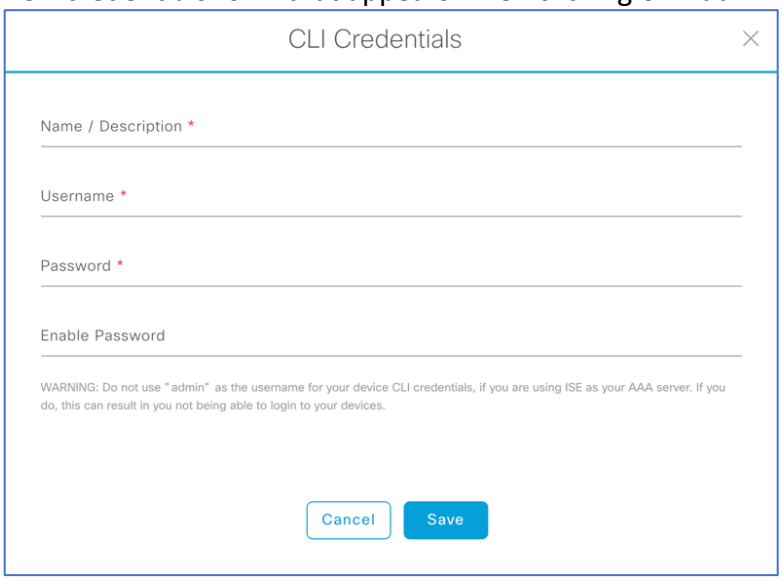


Figure 12. CLI credentials form that appears when clicking on Add in Figure 10.



Part 2 Day 0 Configuration - Discovery and Inventory

Description: Cisco DNA Center's **Discovery** application allows a network admin to add their network device onto the platform.

Section Goals: To discover WLC and APs and assign them to the site created in the section prior.

Step 1: Navigate to the Discovery Application

1. ***Option 1:*** *From the homepage, scroll down to the bottom and click on* ***Discovery*** *then* ***Add Discovery (Figure 13. & 14.)***

2. ***Option 2:*** *Click on the menu at the top left-hand corner of the screen. Click on* ***Tools*** *then* ***Discovery*** *(****Figure 15.****).*

Figure 13. Location of Discovery button on Cisco DNA Center Homepage

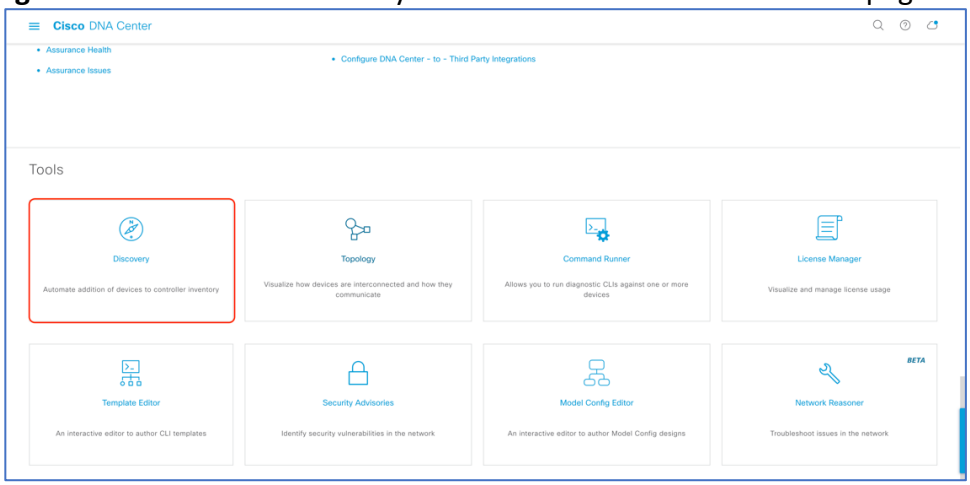


Figure 14. Location of Add Discovery button on Tools - Discovery Page

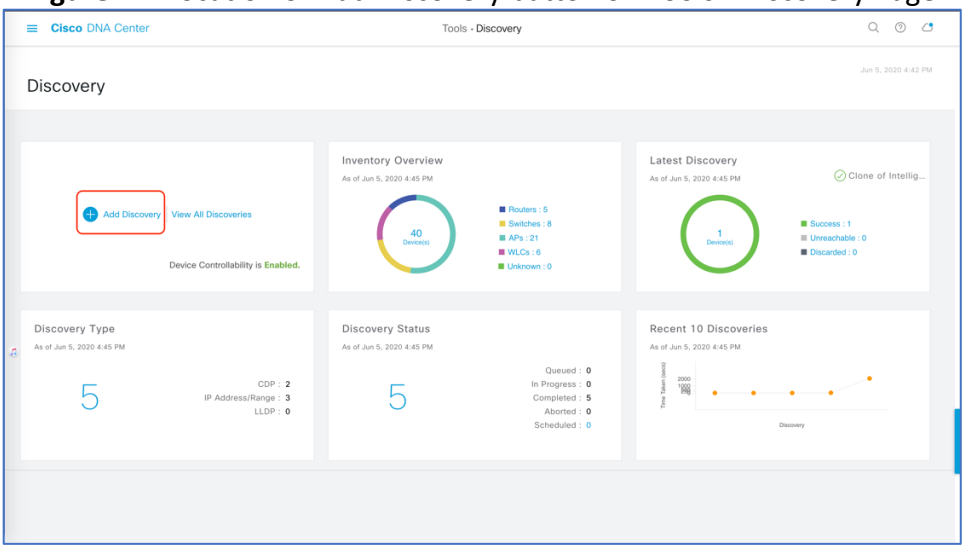
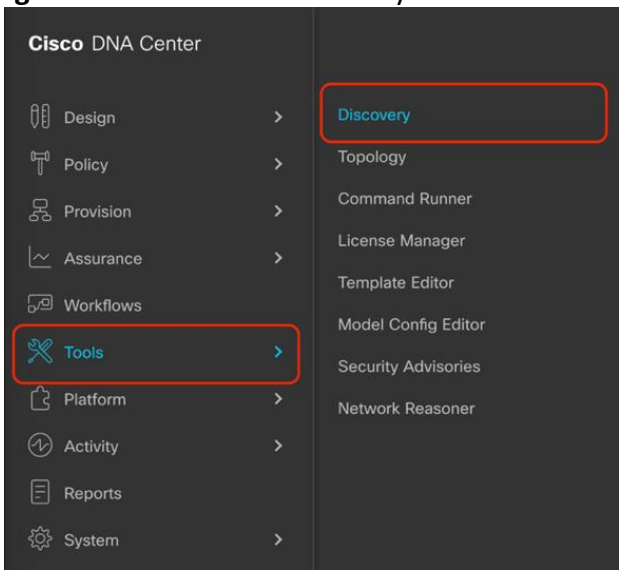


Figure 15. Location of Discovery within the Menu



Step 2: Discover Controllers and Access Points onto Cisco DNA Center

To Discover a WLC onto Cisco DNA Center Follow the Steps Below (**Figure 16.**):

1. *Enter a Discovery name (any unique name for purpose of classification on the discovery page).*

2. *Enter either a single or range of IP addresses via one of the protocols (CDP, Range, LLDP).*
    a. *Warning: WLC & APs must be on a routable network to Cisco DNA Center for Application Hosting on Catalyst APs to work; NATTed Networks are NOT supported and neither are Fabric Networks.*

3. *Enter the SSH username & password, and SNMP read & write credentials (clicking on **Add Credentials**)*

4. *If you're discovering an IOS-XE controller, enter **NETCONF** Port as 830 and run the following commands on the controller CLI.*
    a. *aaa new-model*
    b. *aaa authentication login default local*
    c. *aaa authorization exec default local*

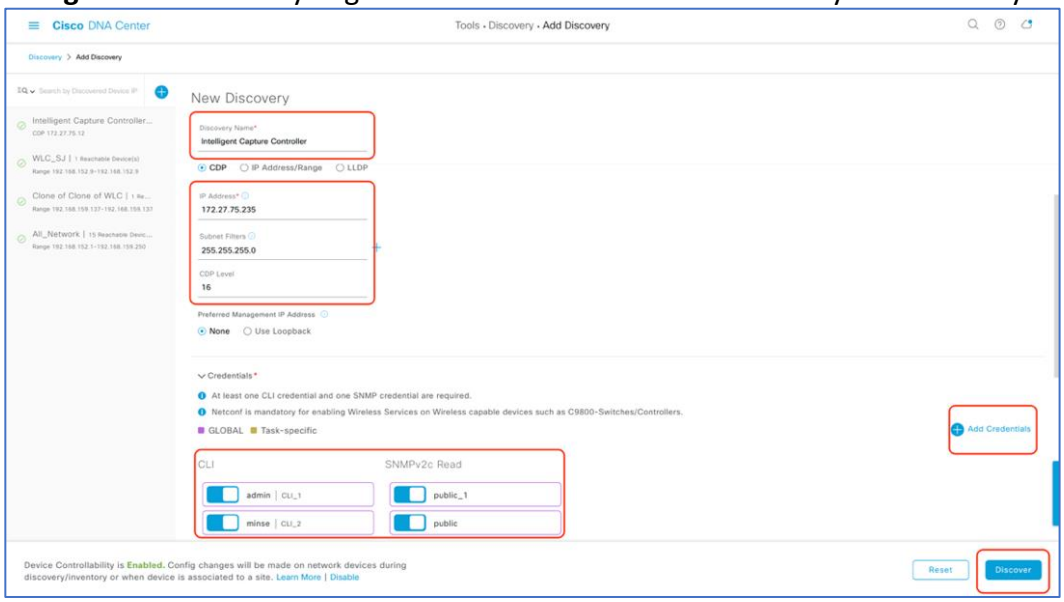
5. *When details are filled in you, click on the **Discover** button.*

Note:

- When you discover a WLC, all it's joined APs will also be discovered onto Cisco DNA Center's Inventory.

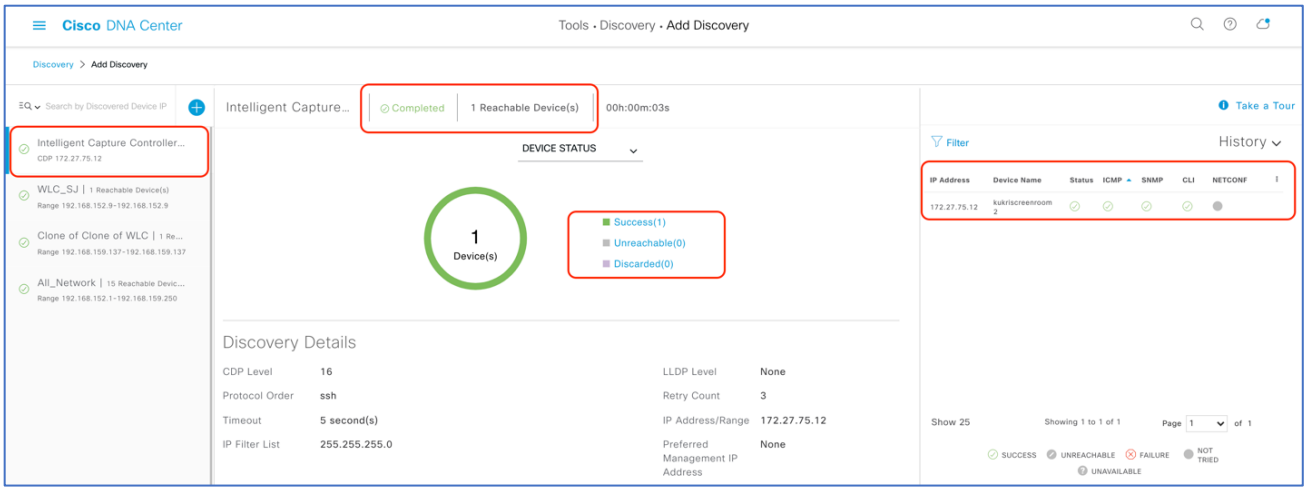
- All the CLI credentials defined in the **Design** section are displayed here on the discovery page.

Figure 16. Discovery Page with Credentials Filled in and Ready for Discovery



6. *After the discovery process completes, ensure that the status of ICMP, SNMP, and CLI sections are green for every device that has been discovered (**Figure 17.**).*

Figure 17. Success Discovery of WLC on the Discovery Page.

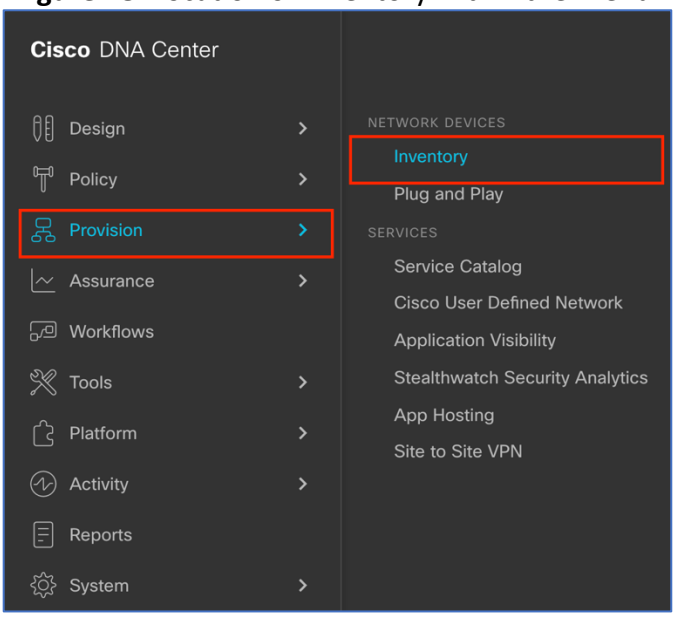


Step 3: Navigate to and Manage Inventory

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

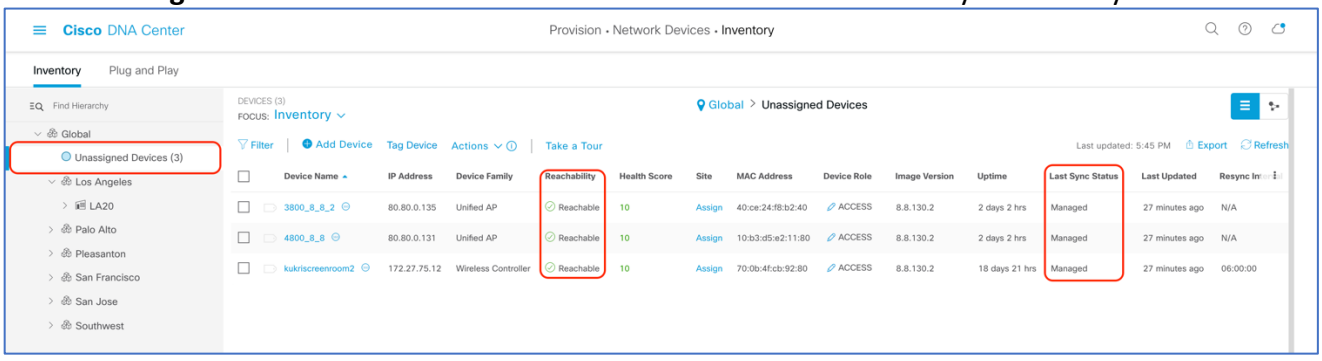
1. *Open up the menu, click on **Provision** then **Inventory** (**Figure 18.**)*

Figure 18. Location of Inventory within the Menu.



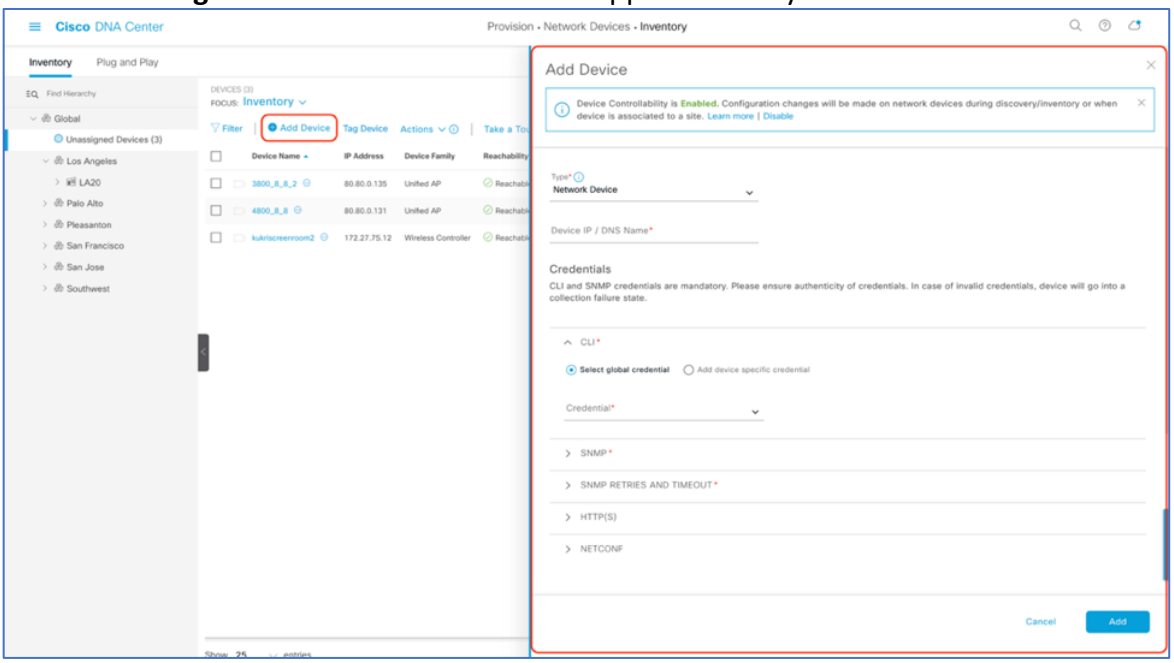
2. *Click on the **Unassign Devices** to the left and ensure that all devices are **Reachable,** and the **Last Sync Status** is **Managed** (**Figure 19.**).*
    a. It is critical that all devices are in Managed state for AP App Hosting functionalities to work. If not check the reachability of your devices.

Figure 19. Discovered Device and the State of their Reachability and Last Sync Status



3. ***Optional:*** *If you would like to manually add a controller to the inventory, click on the* ***Add Device*** *button, and provide the same information as done on the* ***Discovery*** *application (****Figure 20.****).*

Figure 20. Add Device form that appears when you click on Add Device.



Step 4: Assign Discovered Device to Site Hierarchy

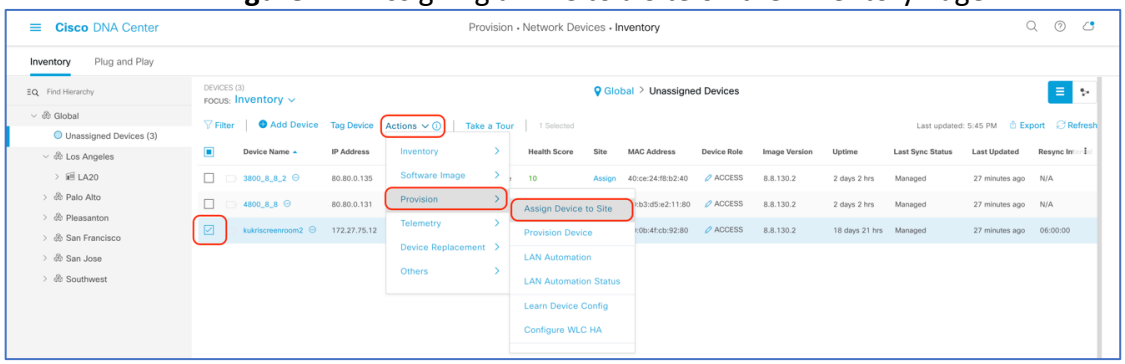
After discovery and site assignment, Cisco DNA Center will have automatically pushed/enabled the following configuration to the WLC and APs required for Application Hosting on Catalyst APs to work.

- Pushed Cisco DNA Center Certificate.
- Configured Cisco DNA Center as a SNMP Trap Receiver.
- Configured Cisco DNA Center as a Syslog server

1. *Click on the check box next to your device that you would like to assign to a site (**Figure 21.**).*

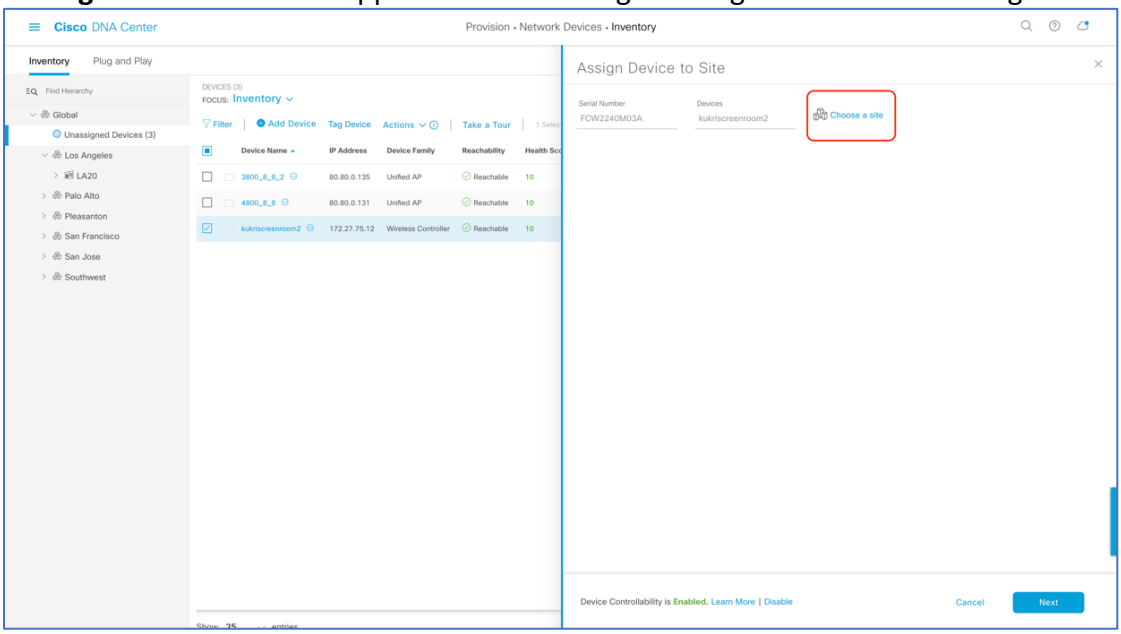
2. *Hover your cursor over **Action** then **Provision**, then click on **Assign Device to Site** (**Figure 21.**).*

Figure 21. Assigning a WLC to a Site on the Inventory Page



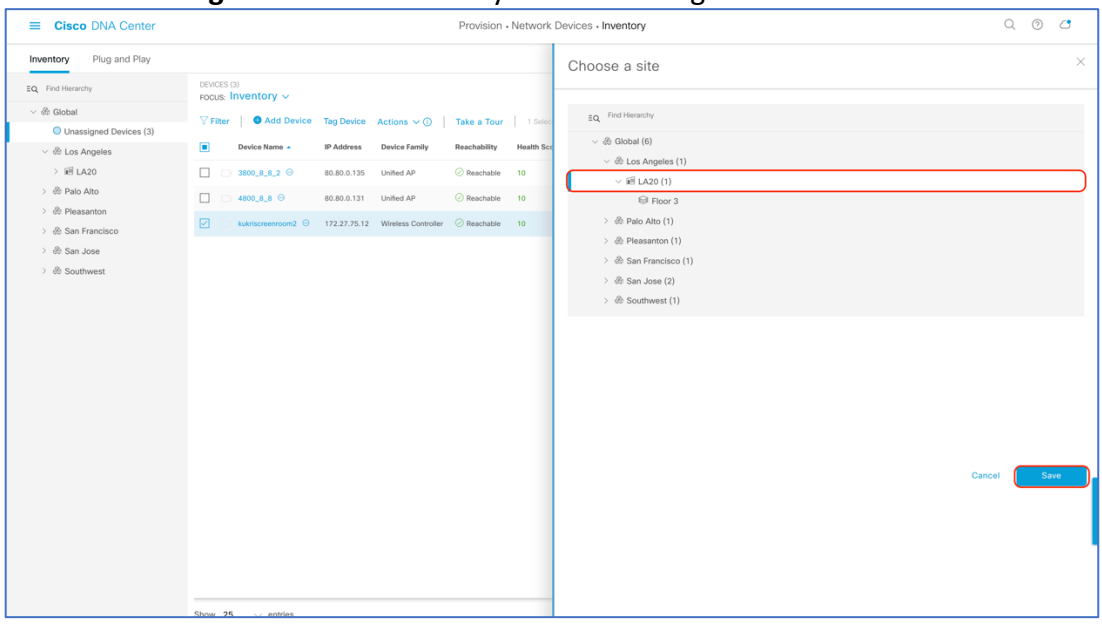
3. *Click on **Choose a Site** (**Figure 22.**).*

Figure 22. Menu that Appears when Clicking on Assign Device to Site in Figure 21.



4. *Click on the site you would like to assign the WLC to and hit save (**Figure 23.**).*

Figure 23. Site Hierarchy Selection Assignment Selection



5. *Click on the button **Next** > **Assign.***

6. *Repeat the same steps for your access points.*

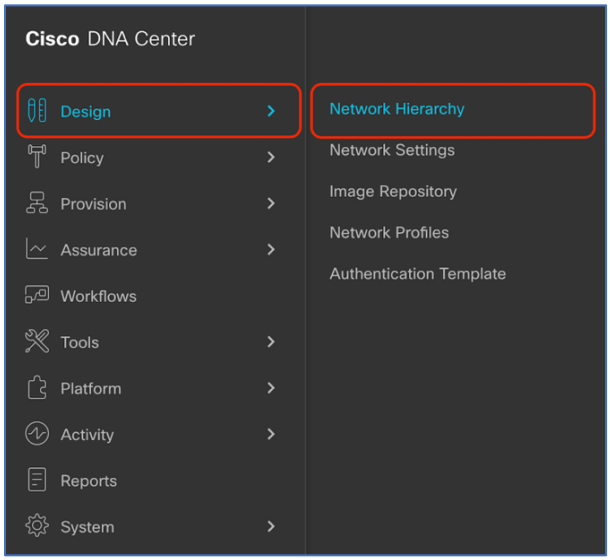
Step 5: Place your Access Points onto the Floor Map

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 point.

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

1. *Navigate to the Network Hierarchy Page by clicking on the menu at the top left-hand corner of the screen. Click on **Design** then **Network Hierarchy** (**Figure 24.**).*

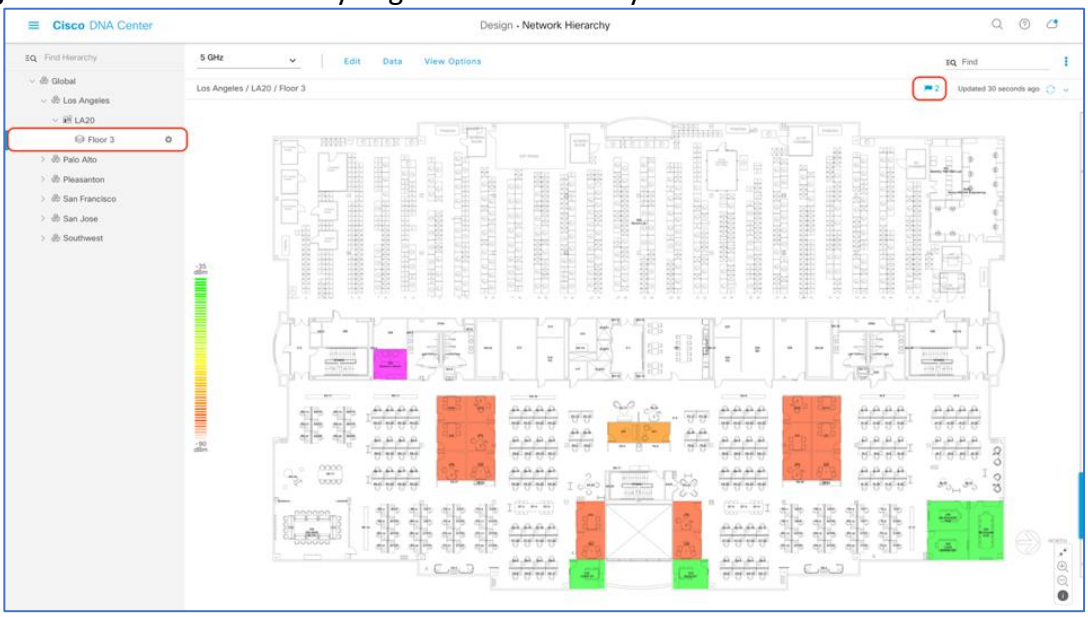
Figure 24. Location of Network Hierarchy from the menu.



2. *Expand **Global** > **the building you created** then click on the floor you've assigned APs to.*

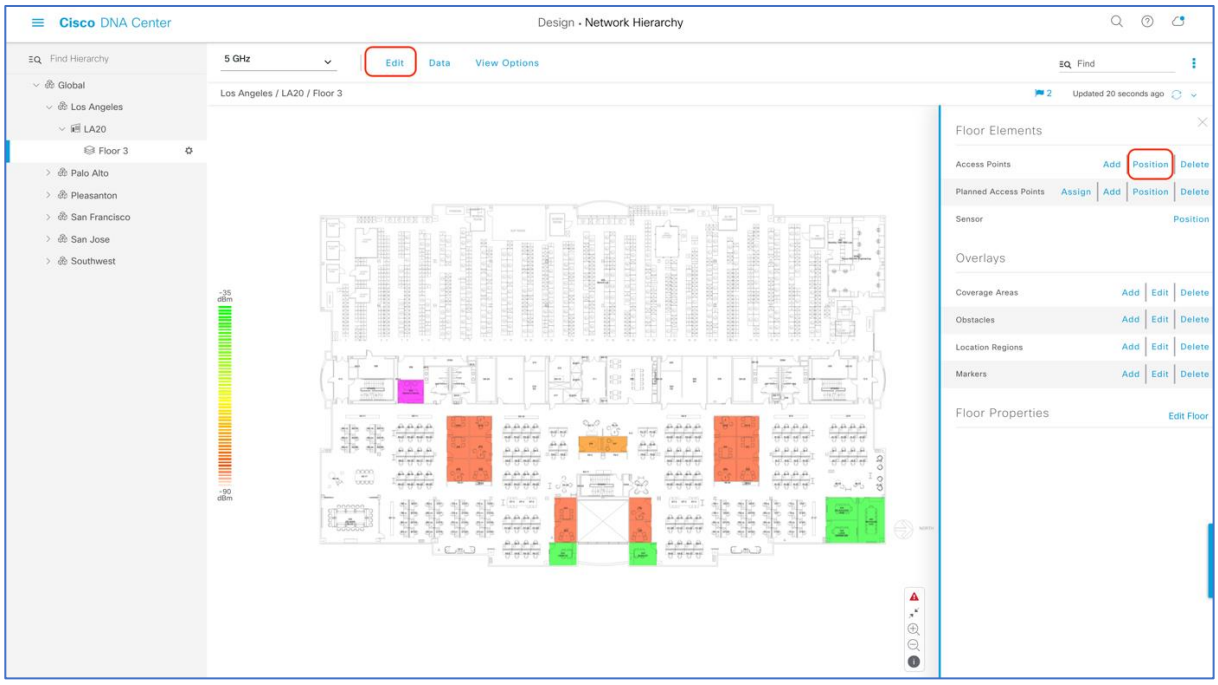
3. Observe the blue flag on the right which represents the number of APs that are ready to be placed onto the map (**Figure 25.**).

Figure 25. Network Hierarchy Page - Two APs Ready to Be Positioned onto the Floor Map



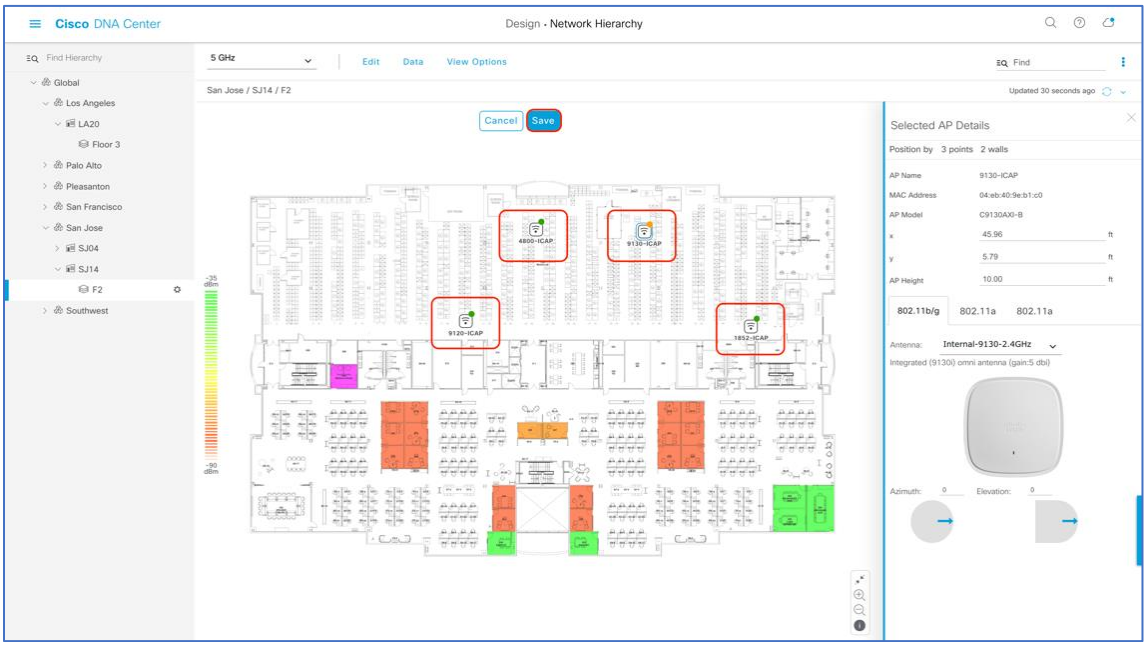
4. *Click on **Edit** then on **Position** to place APs onto the map (**Figure 26.**).*

Figure 26. Network Hierarchy Page – Floor Elements Menu



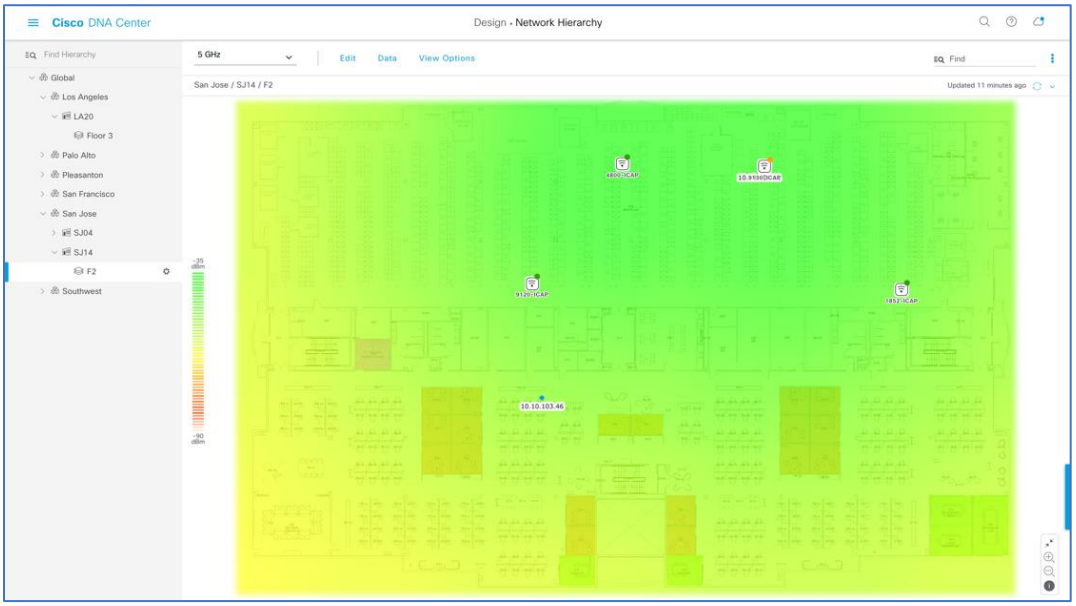
5. *After placing the APs on the floor map, click the **Save** button to commit the change (**Figure 27.**).*

Figure 27. Network Hierarchy Page – With APs placed on the Floor Map



6. *Ensure at this point, a color coated heat map should show up on the Floor Map which depicts the AP's surrounding RF (**Figure 28.**).*

Figure 28. Network Hierarchy Page – Heat Map Displayed After APs are Positioned



Day 1: Upload & Deploy IOx Application

The purpose of the following section is to provide users with step by step instructions with regards to uploading their IOx Application to Cisco DNA Center, then deploying to their desired access point(s).

Part 1 Day 1 Configuration – Upload IOx Application

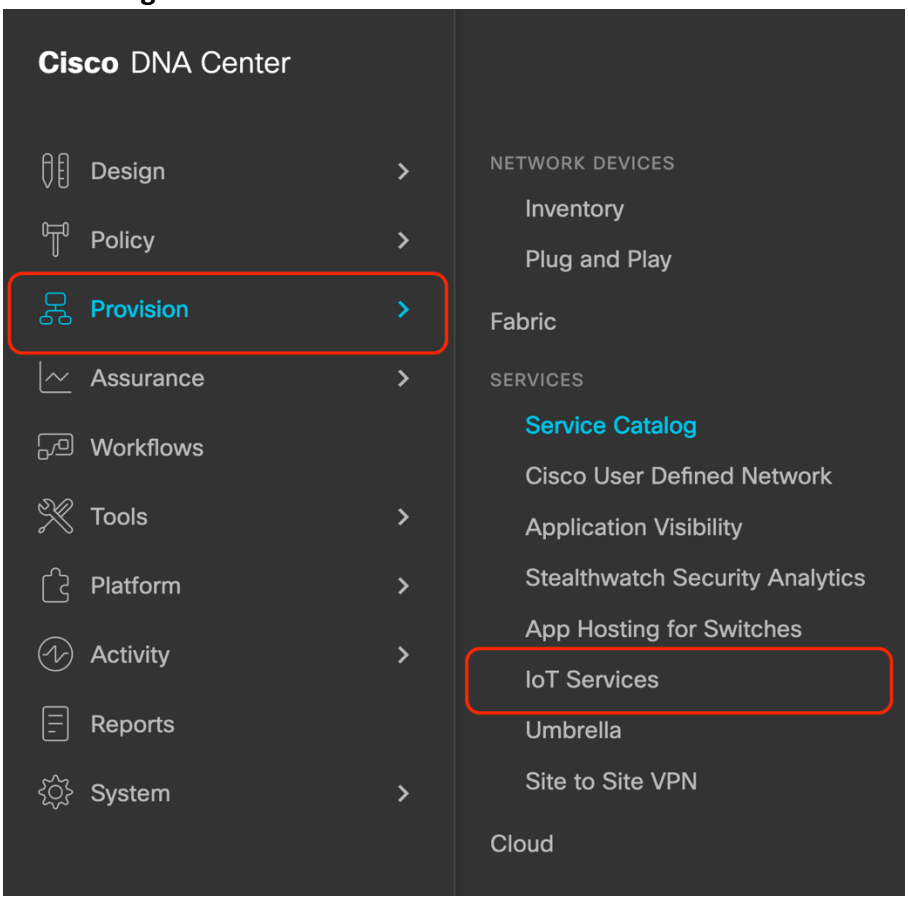
Description: Cisco DNA Center's IoT services page provides an intuitive graphical user interface for users to upload and manage their 3rd party application they would like to deploy onto their access points.

Section Goals: To upload an IOx application into Cisco DNA 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

1. *Open the menu, click on **Provision** then **IoT Services to enter the App Hosting page (Figure 29.)***

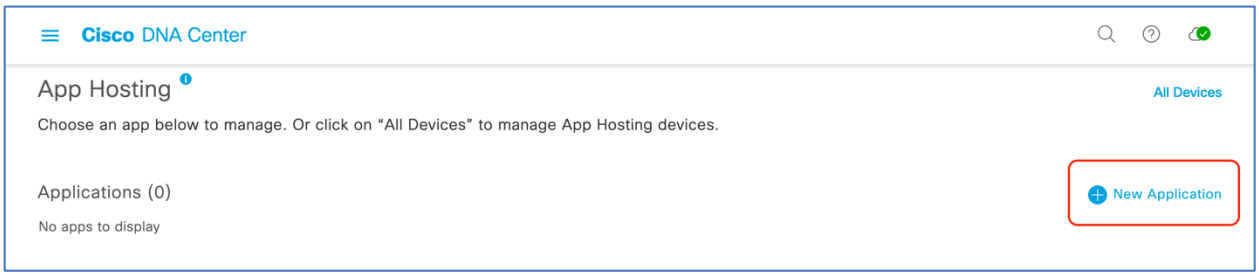
Figure 29. Location of IoT services within the menu.



Step 2: Upload the IOx Application to Cisco DNA Center

1. *Click on **New Application** on the right-hand side of the screen (**Figure. 30.**)*

Figure 30. Location of New Application button on the App Hosting page.

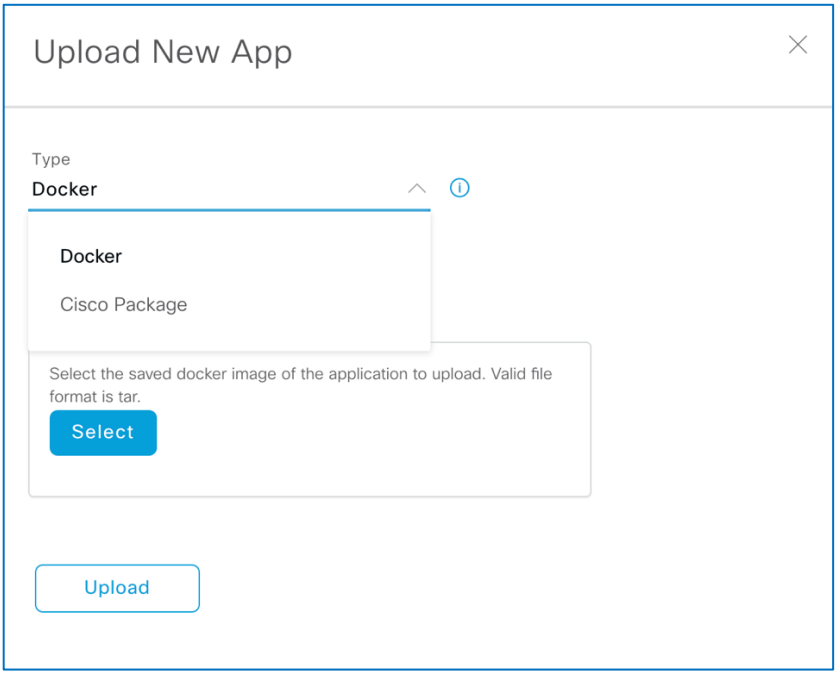


2. *Click on the Type drop down menu and select an application type (**Figure. 31**)*
    a. *Option 1 – Docker*
        i. *Choose this option if the app you are uploading is a docker app saved as a tar file using the docker save command.*

    b. *Option 2 – Cisco Package*
        i. *Choose this option if the app you are uploading has been packaged using the Cisco app packaging toolchain.*

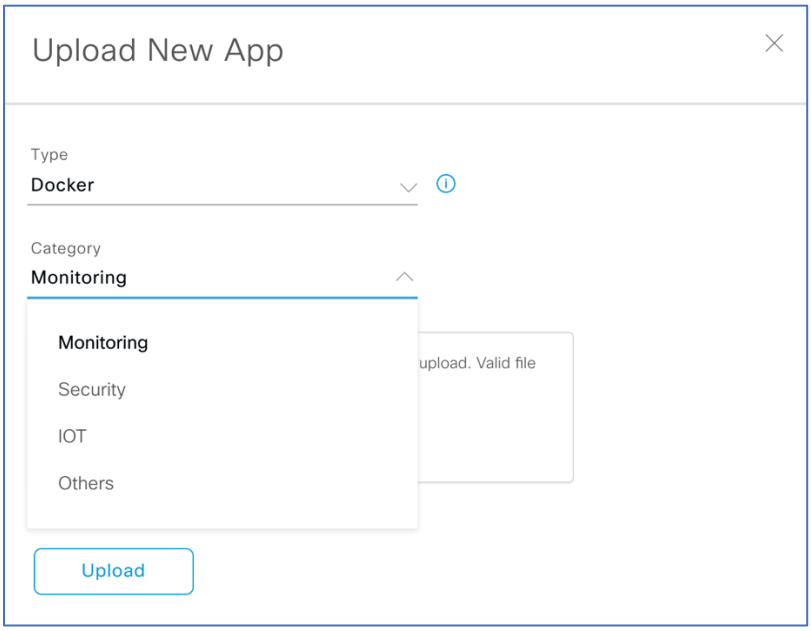
    c. *For more information regarding both package types above, please visit the following link:* https://developer.cisco.com/docs/iox/

Figure 31. Location of Type drop down menu within the New Application Upload Workflow.



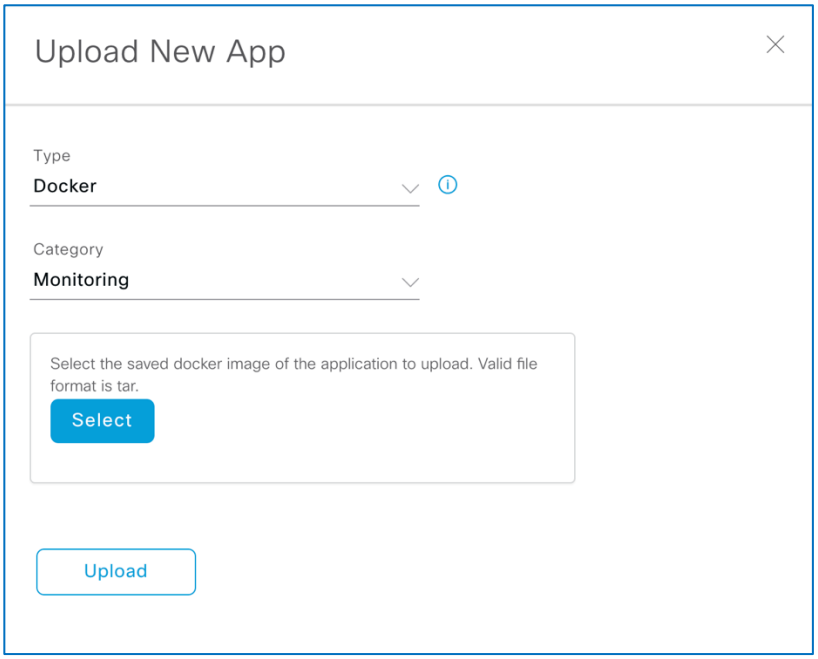
3. *Click on the Category drop down menu and select an application category (**Figure 32.**)*
    a. *Options – (1) Monitoring, (2) Security, (3) IOT, (4) Others*

Figure 32. Location of Category drop down menu within the New Application Upload Workflow.



4. *Click on the Select button to select a file to upload, then click upload to upload the file (**Figure 33.**).*

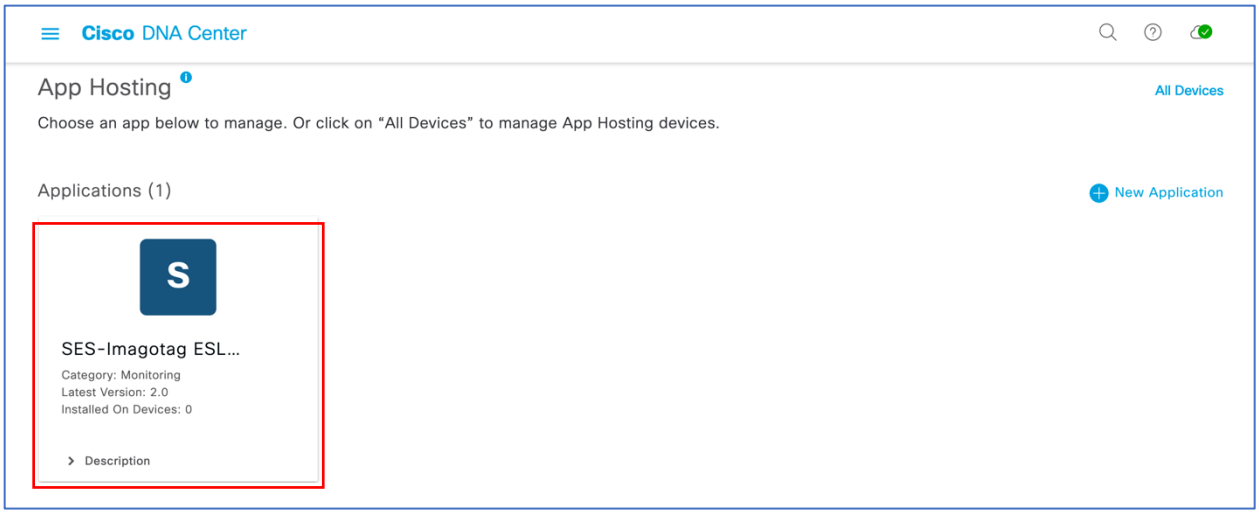
Figure 33. Location of Select & Upload button within the New Application Upload Workflow.



5. *Ensure the application you've uploaded now appears within the App Hosting page (**Figure 34.**).*
    a. *IOx applications can be discovered and downloaded via the following link:* https://developer.cisco.com/ecosystem/spp/

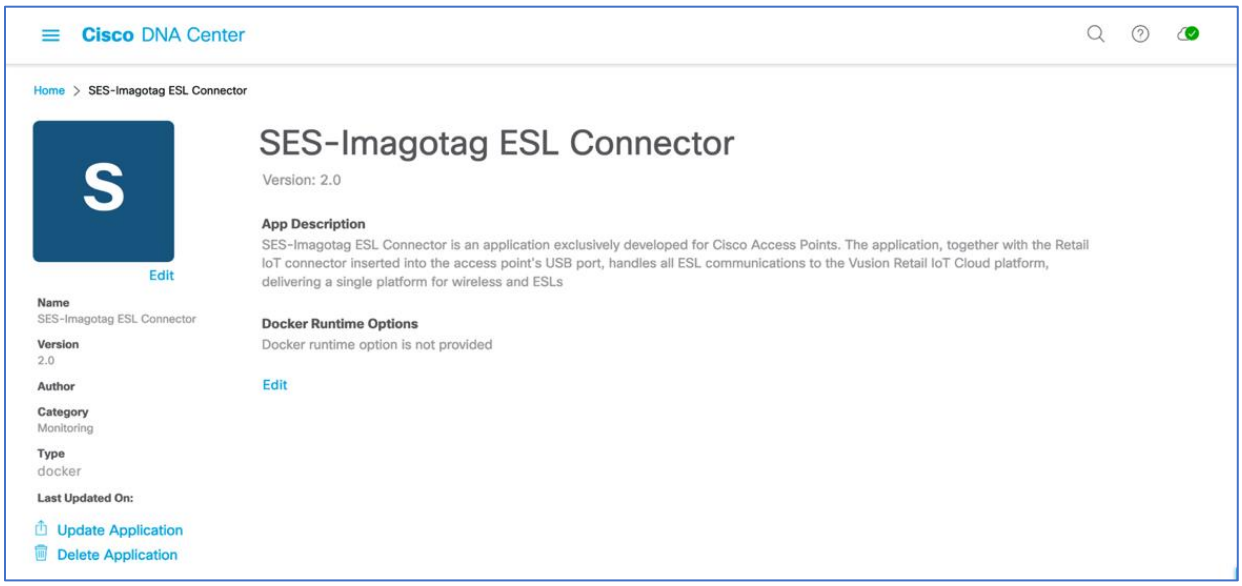
6. *Optional – If you would like to manage the application, click on it to enter the application's management page (**Figure 34.**).*

Figure 34. Location of an application after being uploaded.



7. *(1) To update the application, click on the **Update Application** button, (2) To delete the application, click on the **Delete Application** button, (3) To edit the application's description, click on the **Edit** button (**Figure 35.**)*

Figure 35. Application Management page.



Part 2 Day 1 Configuration – Deploy IOx Application

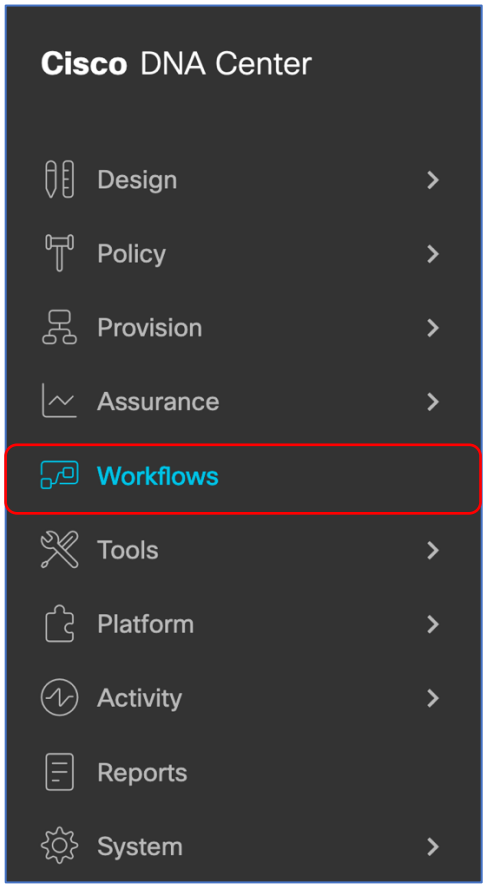
Description: Cisco DNA Center's Enable IoT services workflow allows you to easily deploy your application to either a location or specific access point.

Section Goals: To deploy an IOx application to all devices within a Network Hierarchy site created earlier.

Step 1: Navigate to the Enable IoT Services Workflow

1. *Open the menu, then click on **Workflows** (**Figure 36.**).*

Figure 36. Location of Workflows on the menu.



2. *Scroll down and click on the grid labeled **Enable IoT Services** to begin the deployment workflow (**Figure 37.**) and click on the **Let's Do it** button on the modal box that appears (**Figure 38.**).*

Figure 37. Location of the Enable IoT Services grid within workflows.

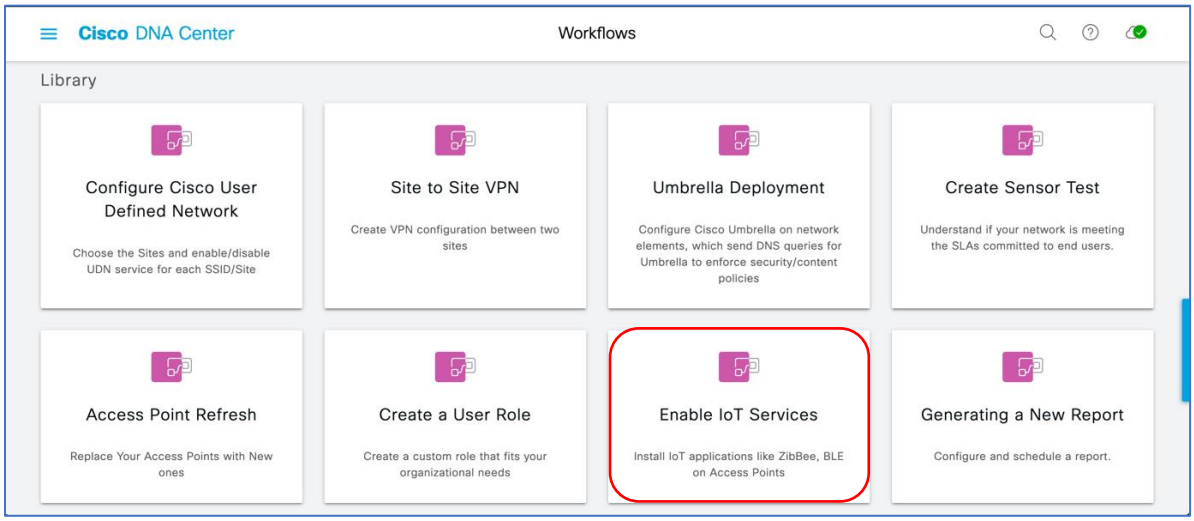
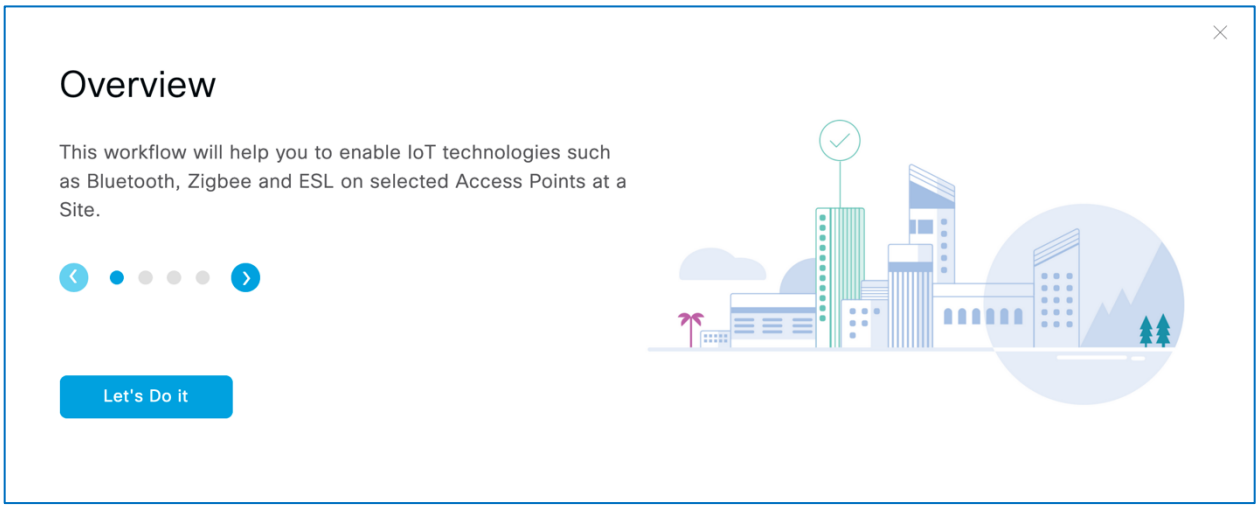


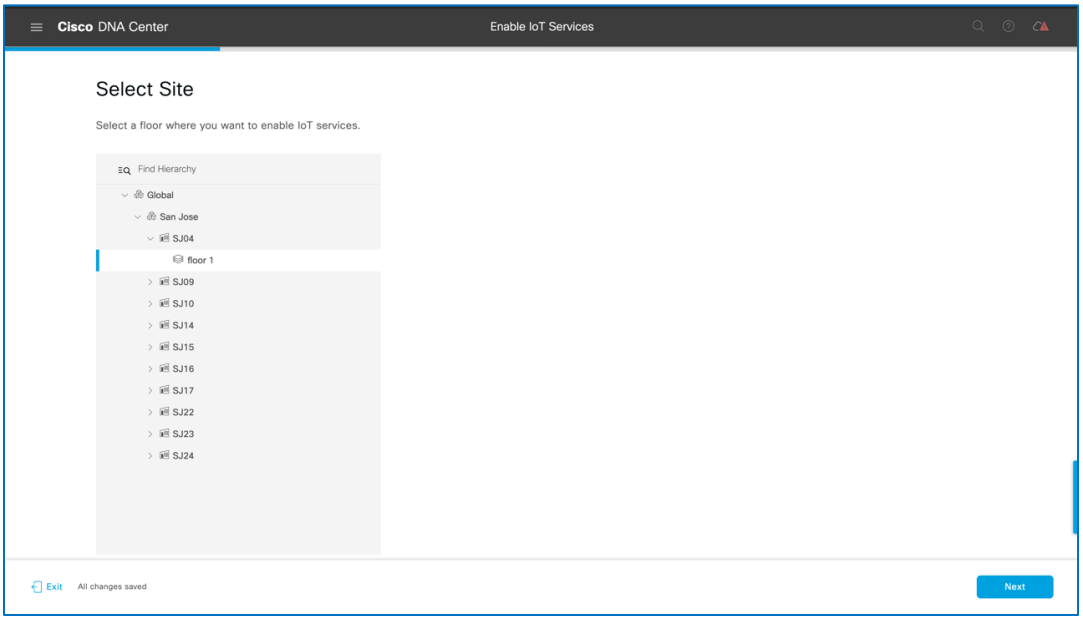
Figure 38. Modal box that appears when the Enable IoT Services grid is clicked.



Step 2: Deploy Application to Access Points on a Floor

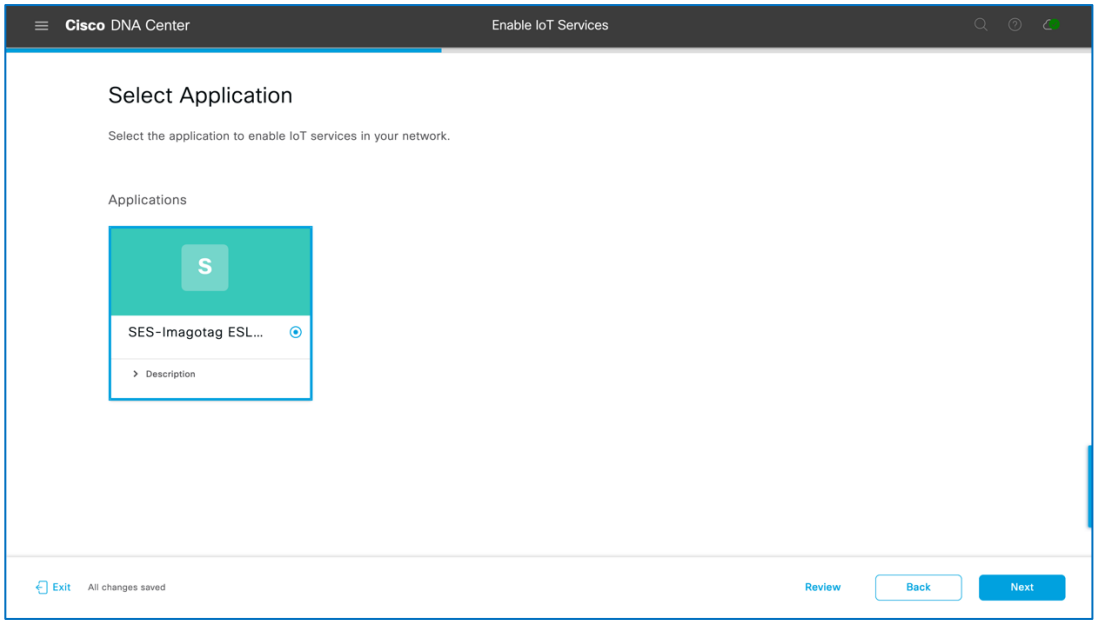
1. *Select a floor within the network hierarchy where you'd like to deploy the application, then hit next (**Figure 39.**).*

Figure 39. Selecting a floor to deploy the application to.



2. *Select the image that you would like to deploy to device on that floor, then hit **Next** (**Figure 40.**).*

Figure 40. Selecting Application to Deploy.



3. *Select the AP(s) on this floor you would like to deploy the image to, then hit **Next** (**Figure 41. & Figure 42.**).*
    a. *By default, the page will show an AP list view (**Figure 41.**); however, this can be toggled by clicking on the map icon to show a Network Hierarchy floor view (**Figure 42.**)*

    b. ***Note:** Make sure under the readiness column says Ready next to the AP you select.*

Figure 41. Selecting APs on the list view to deploy the application to

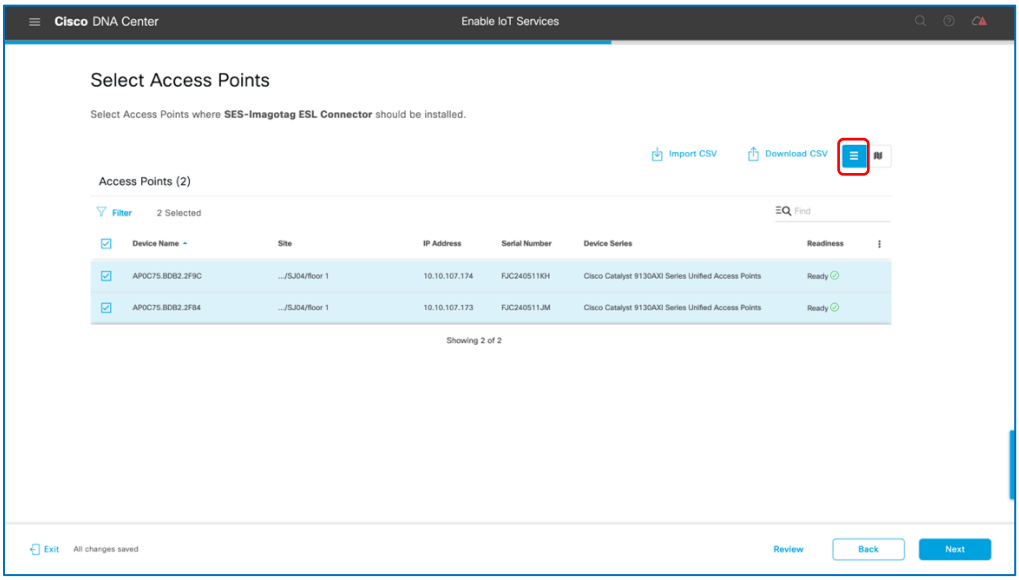
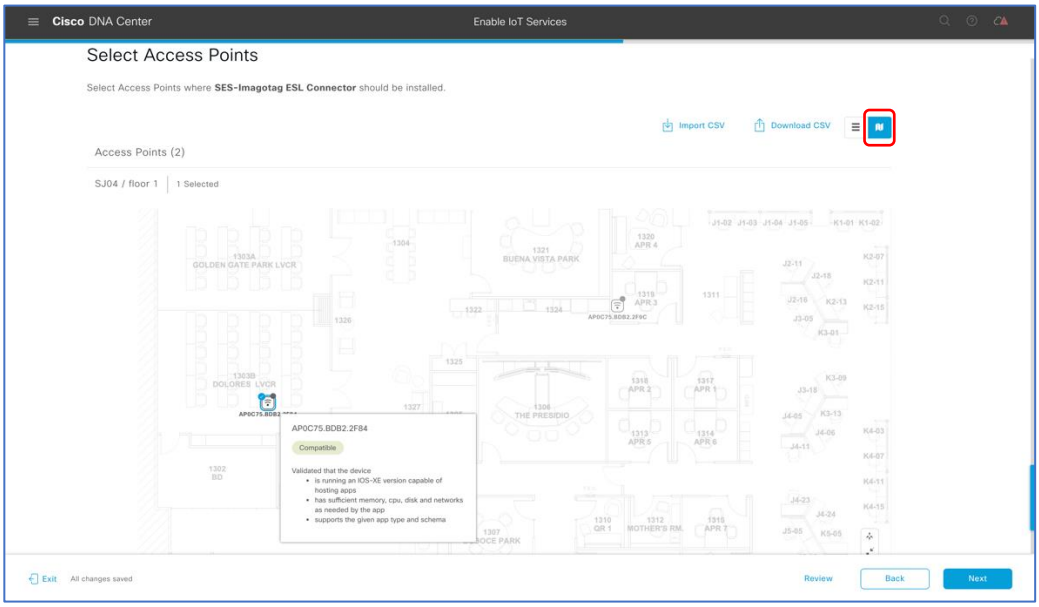
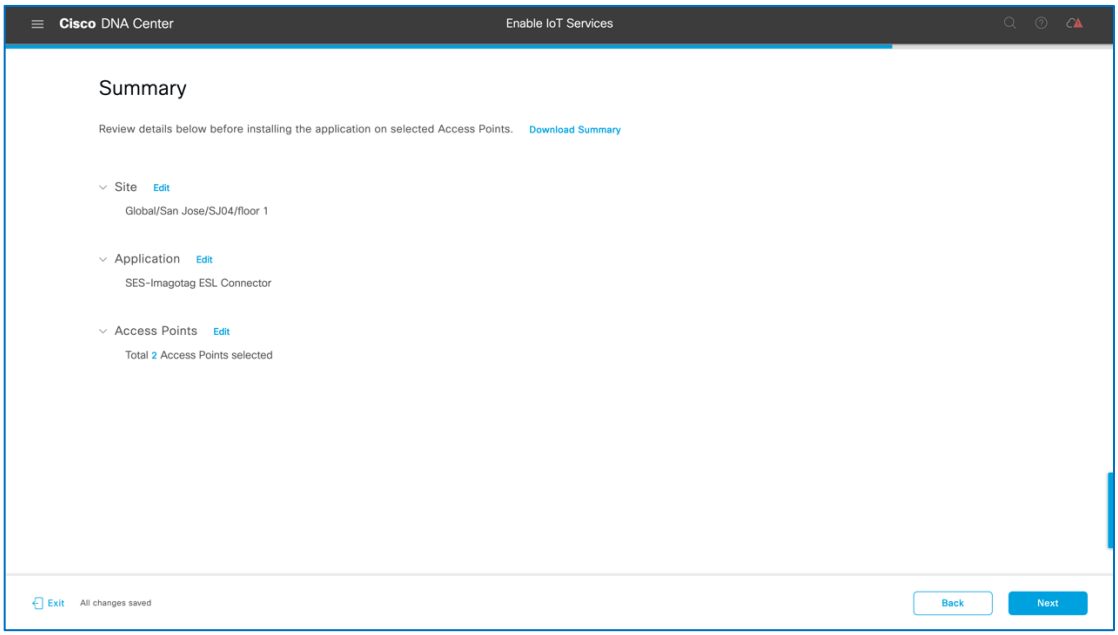


Figure 42. Selecting APs on the map view to deploy the application to



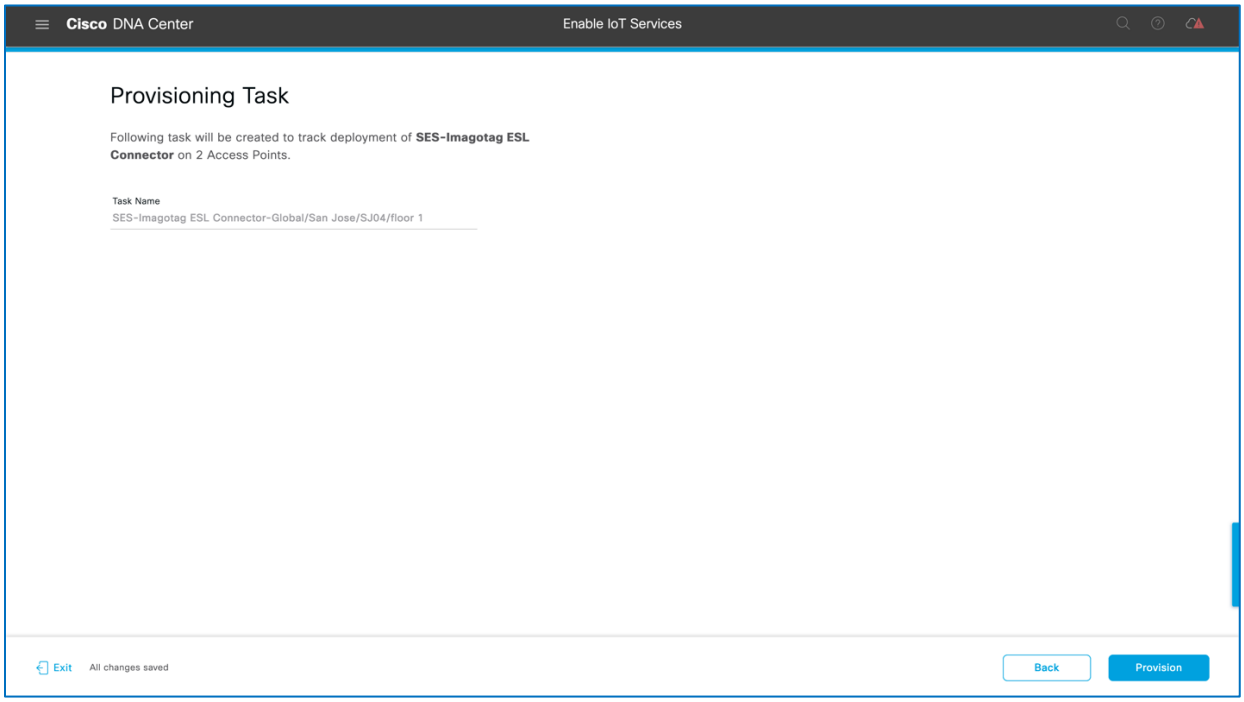
4. *Review that the application is being deployed to the intended site and access point(s), then hit **Next** (**Figure 43.**).*

Figure 43. Application Deployment Summary page.



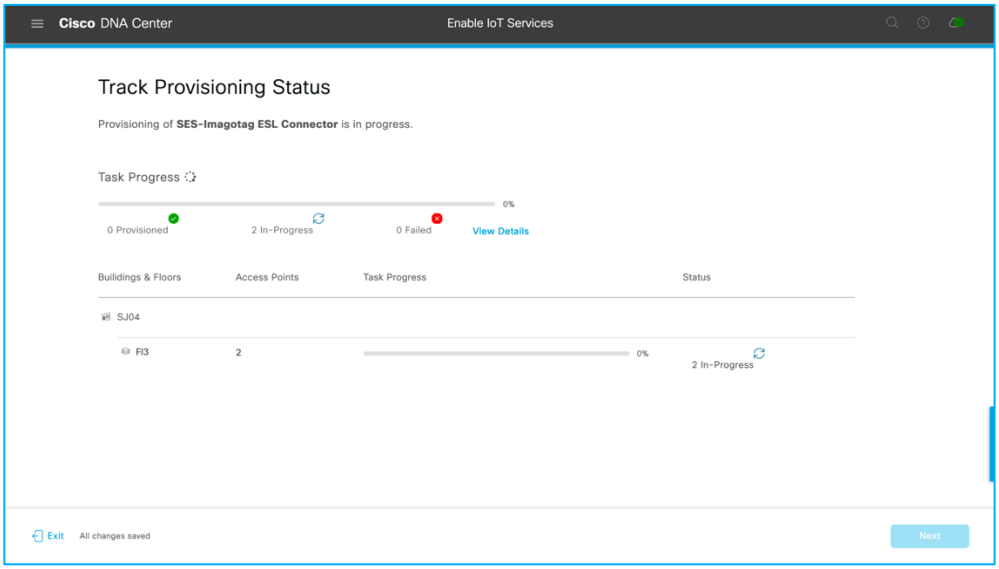
5. *Note down the name of your Task name for reference, then hit **Provision** (**Figure 44.**).*

Figure 44. Generated provisioning task name.



6. *Observe that the application deployment process will begin (**Figure 45.**)*

Figure 45. *Track Provisioning Status page.*

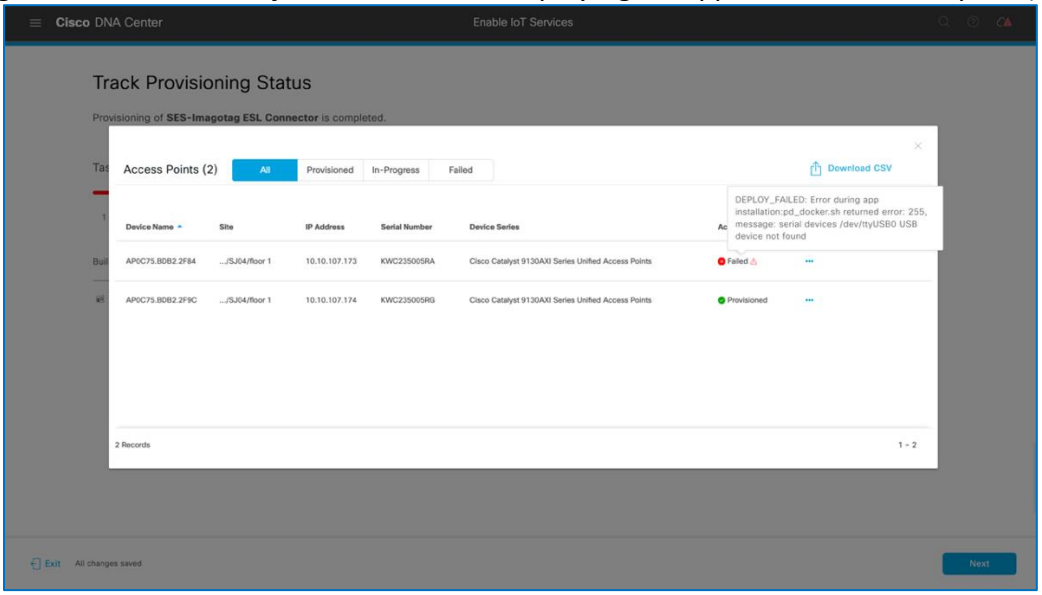


7. *If all steps prior was followed, you will observe a Provisioned message (**Figure 46.**).*

8. *Warning: If you attempt to deploy an application with a dependency on a USB attachment and the attachment is not detected, you will observe a **Failed** message (**Figure 46.**).*

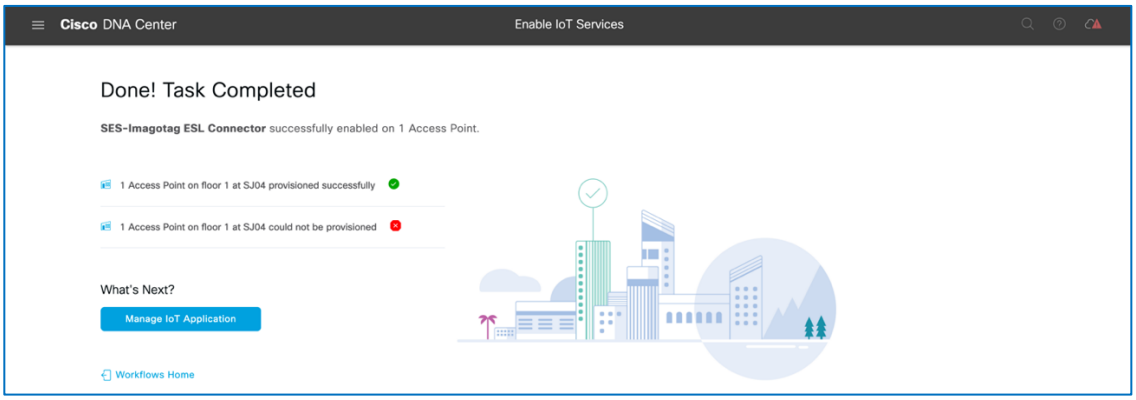
9. *After reading through the provisioning status of your application deployment, hit **Next** (**Figure 46.**).*

Figure 46. *Success and failure case when deploying an application to access point(s).*



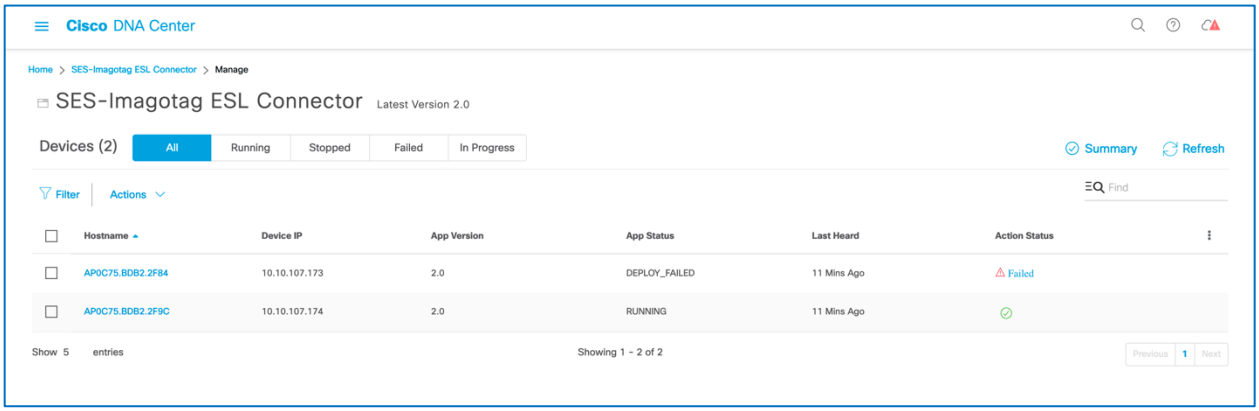
10. *Click on the Manage IoT Application button to continue to the application's management page* ***(Figure 47.)***

Figure 47. Enable IoT Service Workflow summary page.



11. *Observe on this Application Management page, you're able to manage the statuses of the applications deployed on your APs (****Figure 48.****).*

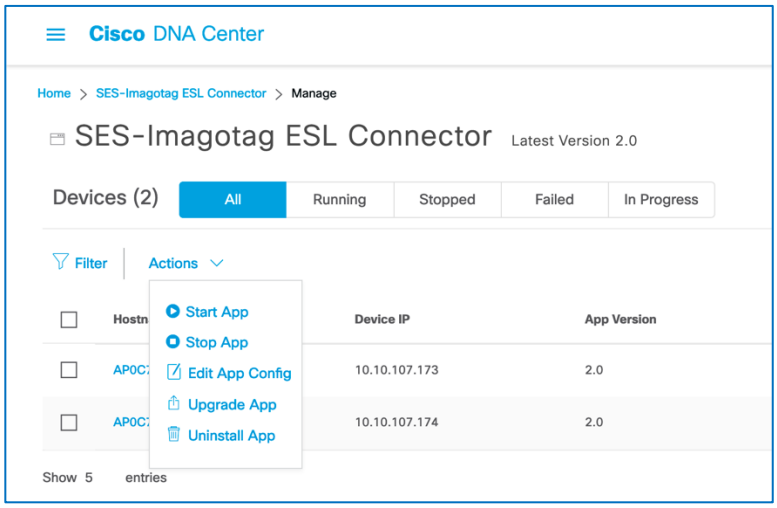
Figure 48. Application Management page.



Note: Observe beneath the **App Status** column, you can monitor the status of your application.

12. *In order to manage the application deployed to the access point, click on the **Actions** drop down menu (**Figure 49.**).*

Figure 49. Actions drop down menu within the Application Management page.



Note:

1.**Start App** – If you stopped your app via the **Stop App** button, you could start it again via this button.

2. **Stop App** – You can stop the loaded application from running. (Stopping an application does not delete or uninstall it).

3.**Edit App Config** – If your application requires additional configurations, you can edit it via this button.

4.**Upgrade App** – If you've uploaded a newer version of your use through the initial IoT Services workflow, you can click on the **Upgrade App** button to upgrade the application running on the AP to the new version.

5.**Uninstall App –** Hit this button to remove the application from your access point entirely.

13. *At this point, your application should be deployed successfully to your access point(s) and if desired, can verify this via the following AP CLI command (**Figure 50.**).*

Figure 50. Verifying the status of the IOx application deployed to the access point.

```
AP0C75.BDB2.2F9C#show iox applications
Total Number of Apps : 1
-------------------------
App Name                      : SES_Imagotag_ESL_Connector
   App Ip                     : 192.168.11.2
   App State                  : RUNNING
   App Token                  : 576fdae5-81a0-4e93-8093-afb050872c12
   App Protocol               : usb
   Number of Disconnects      : 0
   App Grpc Connection        : Down
   Rx Pkts From App           : 0
   Tx Pkts To App             : 0
   Tx Pkts To Wlc             : 0
   Rx Pkts From 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
```

Notes (Refer to **Figure 4.):**

- Your application will by default receive an IP from the 192.168.11.x/27 through DHCP, and can communicate externally from the AP through NAT. This means that the IOx App will by default have the same IP address as the AP from the perspective of external applications.
    - There can be a max of two IOx applications loaded on each AP (refer to #8 in the Common Questions section below).

- If required, an IOx application's traffic can be configured to route over a VLAN by configuring the aux client interface (app host interface) using the following command:
    - `configure ap apphostintf vlan [0-4094] address [static/dhcp] <ip> <nm> <gw>`

Day 2: Monitor IOx Application (Example)

At this point, your application should be successfully loaded onto your desired access points and ready for communication with your 3rd party management and monitoring system. However, this part of the process now entirely varies from application to application as it's completely dependent on the 3rd party application developers to design how they would like to manage and monitor their loaded application.

Disclaimer: The SES-imagotag ESL application discussed within 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.

Day 2 Configuration – Establish Communication from IOx App to Management Server

Description: This section will provide an example of how a specific application called SES-imagotag ESL will communicate with its 3rd party management and monitoring system.

Section Goals: To understand how SES-imagotag ESL's application begins communication to its 3rd party monitoring and management system.

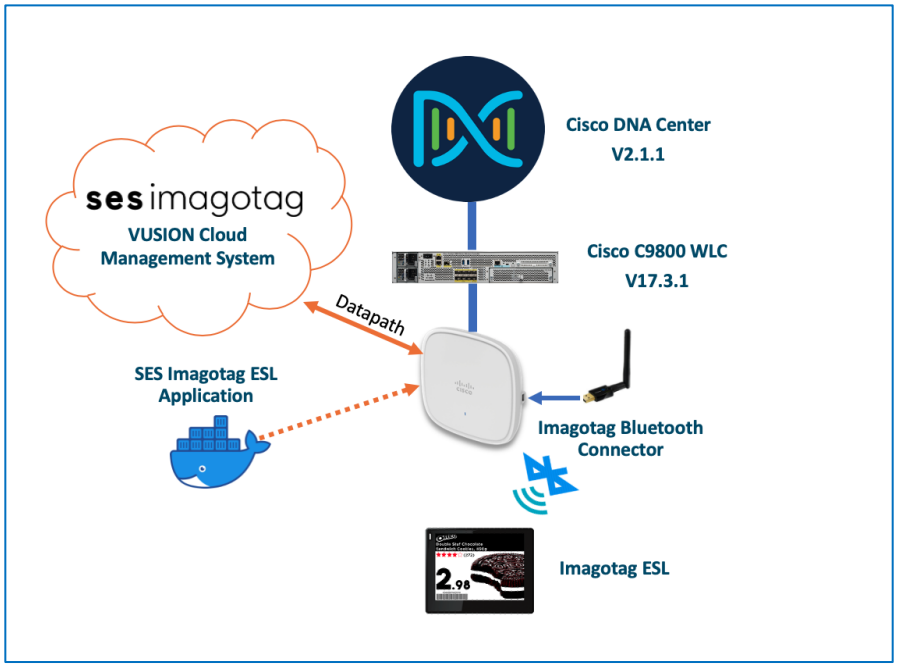
Prerequisite: Understanding the SES-imagotag ESL Solution & 3rd party management system

Background:

At a high level, the SES-imagotag ESL application leverages the USB port on an access point to communicate with ESLs (electronic shelf labels) through a USB Bluetooth dongle. A background on electronic shelf labels is that they're used in retail stores where they're deployed in place of regular price tags.

The advantage of these electronic shelf labels 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 to the various SES-imagotag ESL applications loaded 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 (Cloud Solution – VUSION Cloud) allowing for an organized end to end solution.

Figure 51. SES-imagotag ESL Solution Topology



Step 1: Obtain information required for IOx app external communication

Edit the communication script in the IOx App to start the communication service. This procedure must be performed on each WLAN AP with an active IoT Connector.

1. ***As a prerequisite, first obtain the following:***
   - *The IP address of the machine running your core service (<your CS IP>),*
   - *The ID from the label on each IoT Connector (<IoT AP-ID>),*
   - *A selected unique channel for each IoT Connector, from 0 to 10 (10, 9, 8, 5 preferred*)
2. *From the IOS SSH console, connect to the shell of the IOx application.*
   a. `#connect iox application`

Step 2: Edit IOx Application Communication Script

1. *Enter the following single command line in its entirety to modify the startup script.*
   a. ***Note:*** *Insert your specific settings in the* ***<placeholders>.***

```
# sed -i 's/id=40000/id=<IoT AP-ID>/g; s/USB0/ttyUSB0/g; s/--ca-
file=ca.pem//g; s/channel=2/channel=<channel 0..10>/g;
s/address=10.17.1.115/address=<your CS IP>/g; $ s/$/ --apc-port=7354/'
/opt/esl/communication-daemon/communication-daemon.sh
```

2. *The final version of the file should like the following.*

```
# cat /opt/esl/communication-daemon/communication-daemon.sh
   #!/bin/sh
   ./communication-daemon --ap-id=54074 --serial-port=/dev/ttyUSB0 --
   max-output-power=A --window-size=14 --connection-mode=outbound --
   device-model=standalone-board --ssl  --private-key-file=pk.pem --
   private-key-certificate-chain-file=chain.pem --channel=10 --apc-
   address=192.168.64.167 --apc-port=7354
```

Step 3: Restart Communication Script

1. *Restart the communication script for the changes made to take effect.*

```
# killall communication-daemon ; sleep 10 ; /opt/esl/communication-
daemon/communication-daemon.sh&
```

Note:

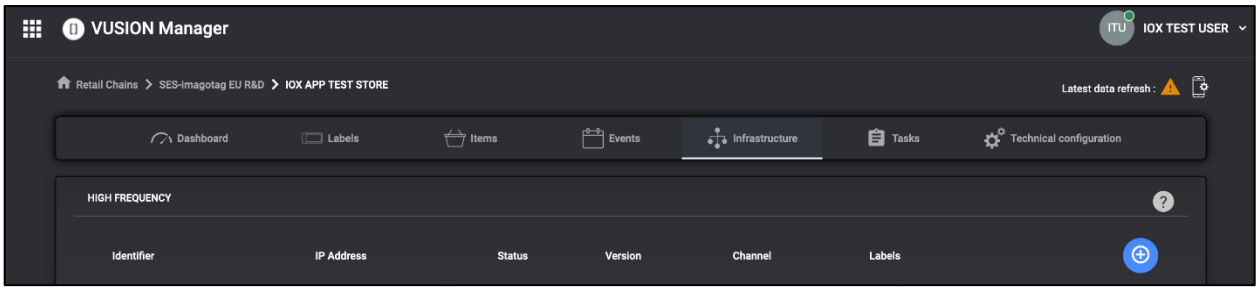
- The steps above must be repeated for each IOx application hosted within an access point.

- In the case an access point restarts, you don't need to re-edit the communication script; however, you must connect the IOx Application again as well as execute the service restart command.

Step 4: Adding SES-imagotag ESL IOx Application into VUSION (Cloud)

1. *Ensure that SES-imagotag authorizes your USB IoT Connector in order for VUSION Cloud to work properly.*

Figure 52. VUSION Cloud UI with SES-imagotag ESL Application Connected



Note:

- The USB IoT Connector hardware has an "AP ID" printed on the label.

- Please contact your SES Project Manager and share the AP ID for each USB IoT Connector that you have activated and enabled with the ESL IOx App.

Application Hosting on Catalyst APs Use Cases (Examples)

Cisco's Application Hosting on Catalyst APs provides endless possibilities to what you, as the developer, can accomplish in the field of the Internet of things. The purpose of this section is to offer you some ideas in terms of use cases to inspire you to build amazing applications.

Use Case 1: Healthcare

Background: In the year 2020, the world was hit by with a pandemic caused by a virus identified as COVID-19. Due to its contagious nature, the virus has caused devastating effects throughout the globe and has hospitalized hundreds of thousands of individuals.

Pain Points: The virus is known for its incredibly contagious nature, and infected individuals are required to be immediately quarantined away as an attempt to prevent a further spread. The contagiousness of this virus has caused immense inconvenience to both a patient's well-being and the medical facilities' ability to manage operations.

How AP App Hosting Addresses the Pain Points: With Application Hosting on Catalyst APs, you, as the developer can create applications that respond to external stimuli such as voice control technology devices (i.e., Google Home, Amazon Echo). Your IOx application can be programmed to use these received external parameters to trigger actions such as calling for a doctor, changing the temperature, adjusting the bed, etc. Such technology can be highly beneficial for increasing the convenience of bedridden patients and medical facilities' staff during COVID-19 who are attempting to maintain maximum social distancing.

Refer to the figures below for the examples:

Figure 53. Application Hosting on Catalyst APs healthcare use cases

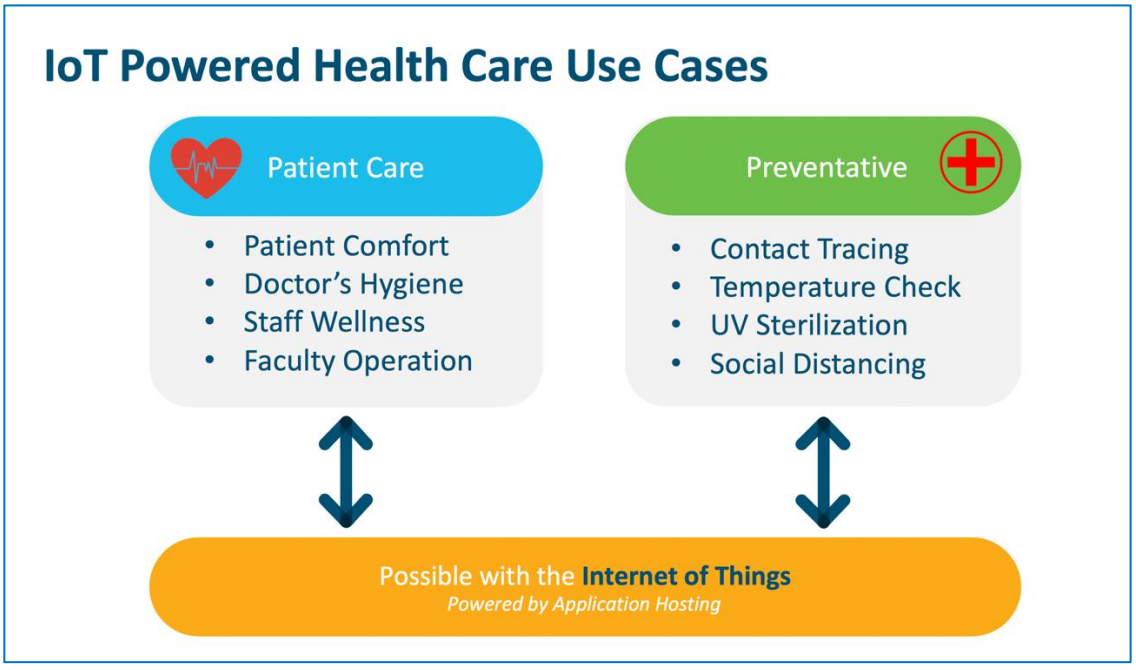


Figure 54. Leveraging voice speech to text software to control IoT devices

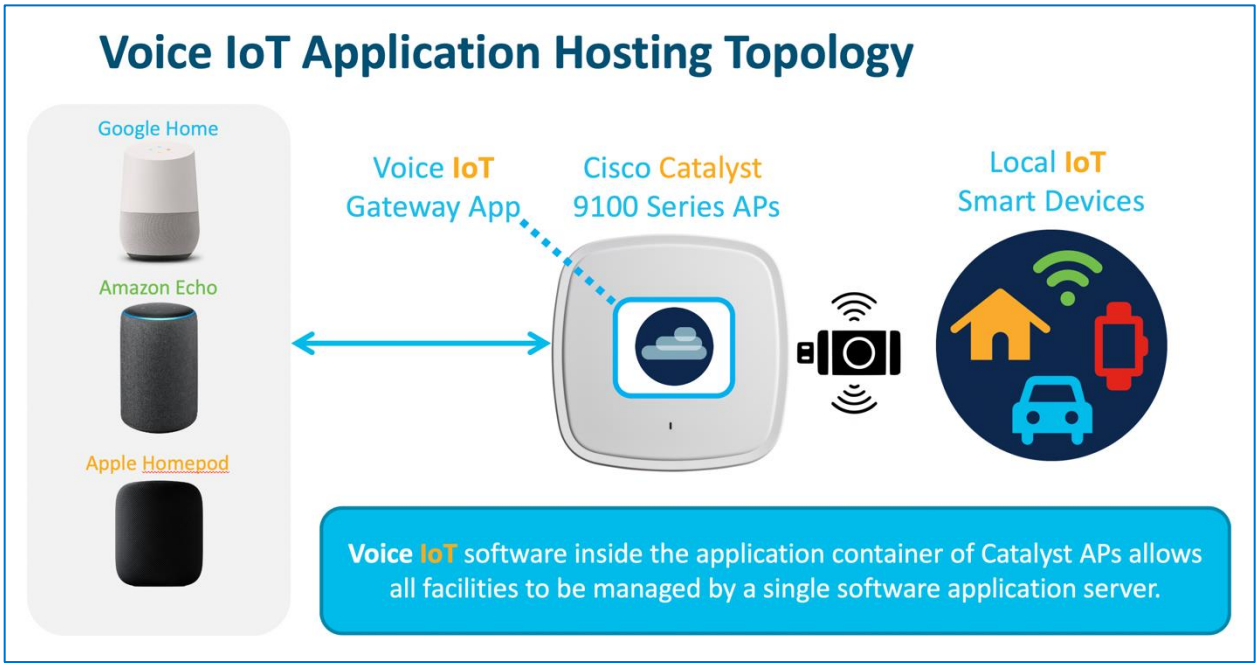
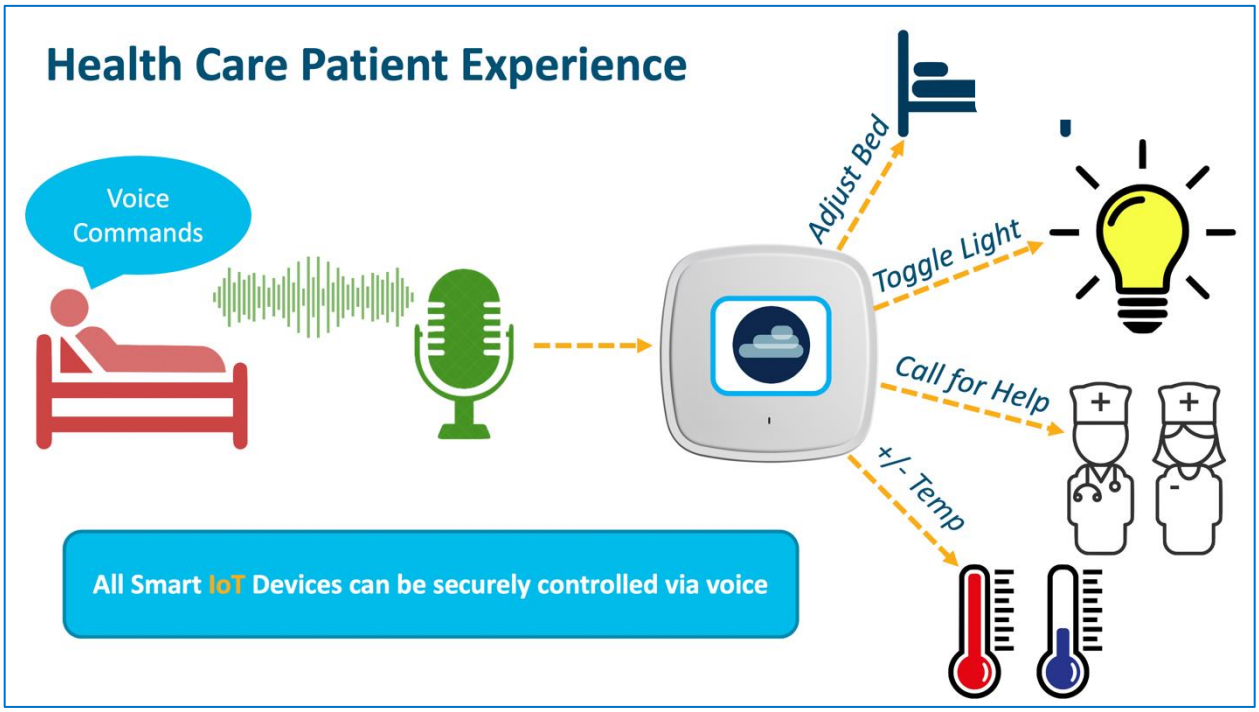


Figure 55. Patient room leveraging Application Hosting on Catalyst APs IoT topology



Use Case 2: Building Management System

Background: Imagine you manage the facilities of a sizeable multiregional enterprise spread through multiple countries.

Pain Points: The ability to manage these facilities and ensure 24/7 security can be an incredibly difficult task as there is too much to handle. What happens more often than not is a large handful of facilities managers are required to be onsite to ensure the safety and security of employees. Such a manual process requires not only costs the company lots of money to hire such employees but also leave security vulnerable for potential human error.

How AP App Hosting Addresses the Pain Points: With Application Hosting on Catalyst APs, you as the developer can create applications that directly communicate with smart building management devices throughout all facilities in multiple regions at once. You will have the ability to have all devices report information back to a central management server creating an incredibly convenient command center for facilities management.

Refer to the figures below for the examples:

Figure 56. Building Management System Sample Use Cases

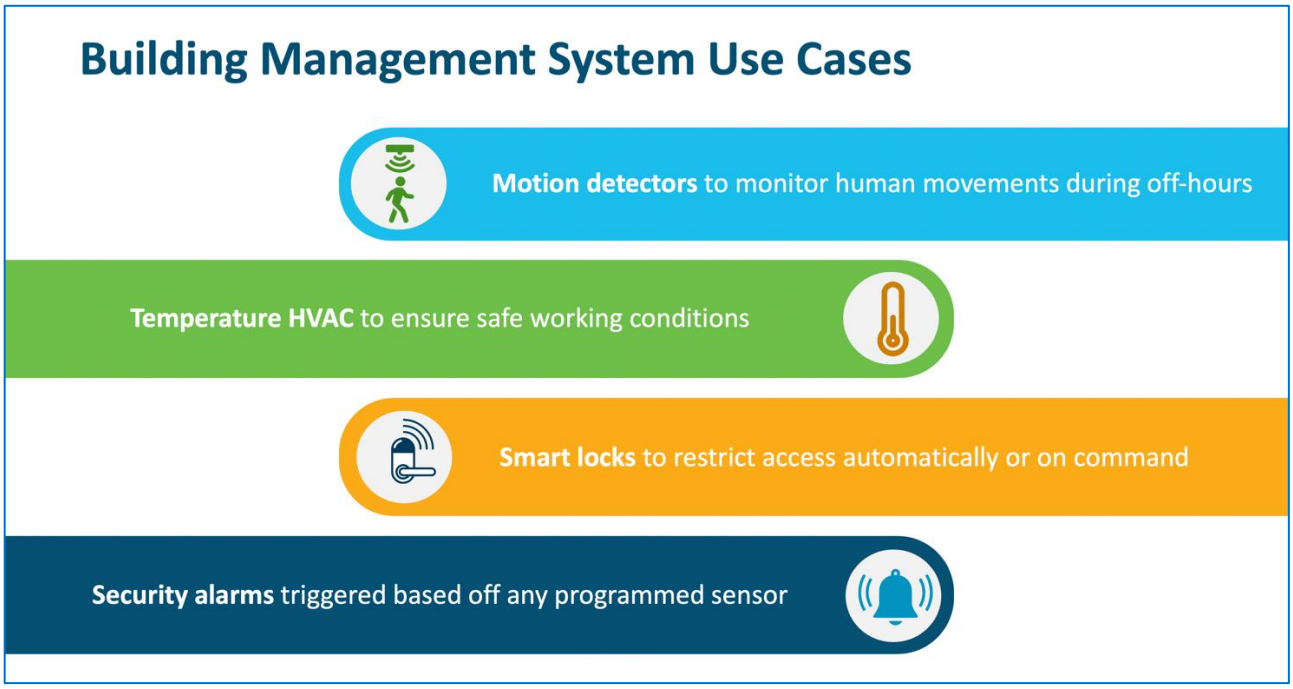
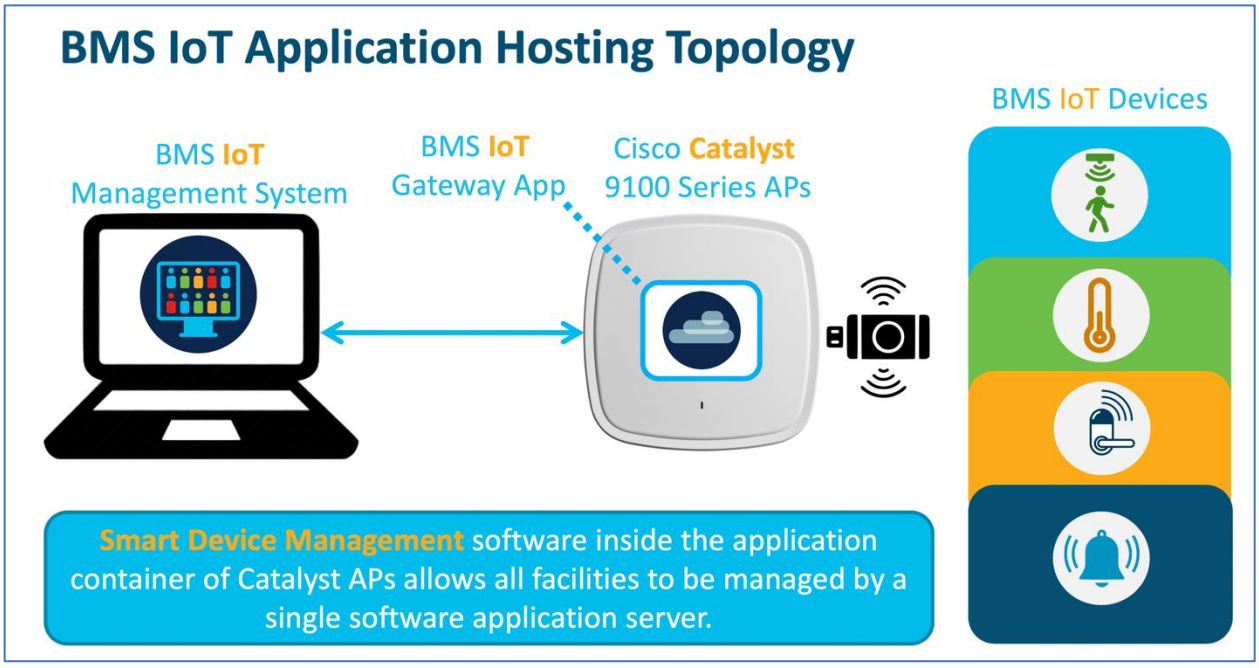


Figure 57. Smart BMS Devices Communicating to a BMS Manager through Catalyst APs



Useful CLI Commands

Access Point Commands:

1. **Viewing 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
```

2. **Viewing AP 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
```

3. **Verifying 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
```

IOS-XE WLC Commands:

1. **Viewing 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
```

2. **Viewing the USB module state of each joined access point along with other information.**
    a. **Note:** Below is only a snippet of entire 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
```

3. **Viewing 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
```

Common Questions

1. **What is access point's USB port's requirement?**
    a. USB Serial – 115200 Baud
    b. i.e., ttyUSB

2. **Does the access point need to be in a specific mode for the IOx application to operate?**
    a. The access point can be on either Local or Flexconnect mode; however, regardless of the AP's forwarding mode, the IOx application will always be switched locally from AP's ethernet port.

3. **Is Application Hosting on Catalyst APs Supported on AireOS Controller platforms?**
    a. No

4. **What licenses are required for Application Hosting on Catalyst APs?**
    a. From Cisco DNA Center perspective, a subscription to a DNA-Advantage license is required.
    b. From the IOx application server's perspective, the license is required separately from Cisco DNA Center, and varies based on vendor.

5. **Is Cisco DNA Center mandatory for Application Hosting on Catalyst APs Deployment/Management?**
    a. Yes, during actual IOx Application management, Cisco DNA Center is mandatory; however, during the IOx application development phase, just an access point and WLC is required.

6. **Can WLC/AP setup connect to Cisco DNA Center via NAT?**
    a. No, a direct connection is required for Application Hosting on Catalyst APs to work.

7. **Are there specific TCP ports that must be open for AP Application hosting to work?**
    a. Yes, the TCP port 8443 is used by Cisco DNA Center to deploy the IOx application to the access point.

8. **What are the power consumption specifications for each of the supported access points?**

Family	PoE-in DC Mode	Consumption at PD	Consumption at PSE with the worst-case cable	USB Status and Power Output
C9117	.3af	13.5	15.4	N
	.3at	25.0	29.3	N
	.3at	24.1	28.0	Y (4.5W)
	.3bt/UPoE	30	32.7	Y (4.5W)
	.3at/.3bt/UPoE	22.4	25.7/23.8/23.8	Y (4.5W)
C9115AXI	.3af	13	15.4	N
	.3at	16.0	18.9	N
	.3at	20.4	24.1	Y (3.75W)
C9115AXE	.3af	13	15.4	N
	.3at	17.0	20.1	N
	.3at	21.4	25.3	Y (3.75W)
	.3af	13.8	15.4	N
	.3at	20.5	23.2	N
	.3at	25.5	30.0	Y (4.5W)
C9130AXI/E	.3af	13.8	15.4	N
	.3at	25.5	30.0	Y (4.5W)
	.3bt	30.5	33.3	Y (4.5W)
C9105AXI	.3af/at	11	12.5	N/A
C9105AXW	.3af	13	14.9	N
	.3at	18.5	21.4	Y (4.5W)
	.3at	25.5	30	N

9. **What are the hardware specifications for each of the supported access points?**

AP	CPU Architecture	CPU Allocated (MFLOPS)	Max Memory Allocated (RAM)	Application Type	Max Number of Apps	Max Cores for IOx App	Max Storage	USB Support for IOx
C9105AXI	ARM 32 bit	1200	200 MB	Docker	2	2	64 MB	No
C9105AXW	ARM 32 bit	1200	200 MB	Docker	2	2	64 MB	Yes
C9115AX	ARM 64 bit	4800	400 MB	Docker	2	2	64 MB	Yes
C9117AX	ARM 64 bit	4800	400 MB	Docker	2	2	64 MB	Yes
C9120AX	ARM 64 bit	4800	400 MB	Docker	2	2	64 MB	Yes
C9130AX	ARM 64 bit	4800	400 MB	Docker	2	2	64 MB	Yes

Useful Links

All Cisco DNA Center Guides

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

IOx Application Guides

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

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

- 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

Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Copyright