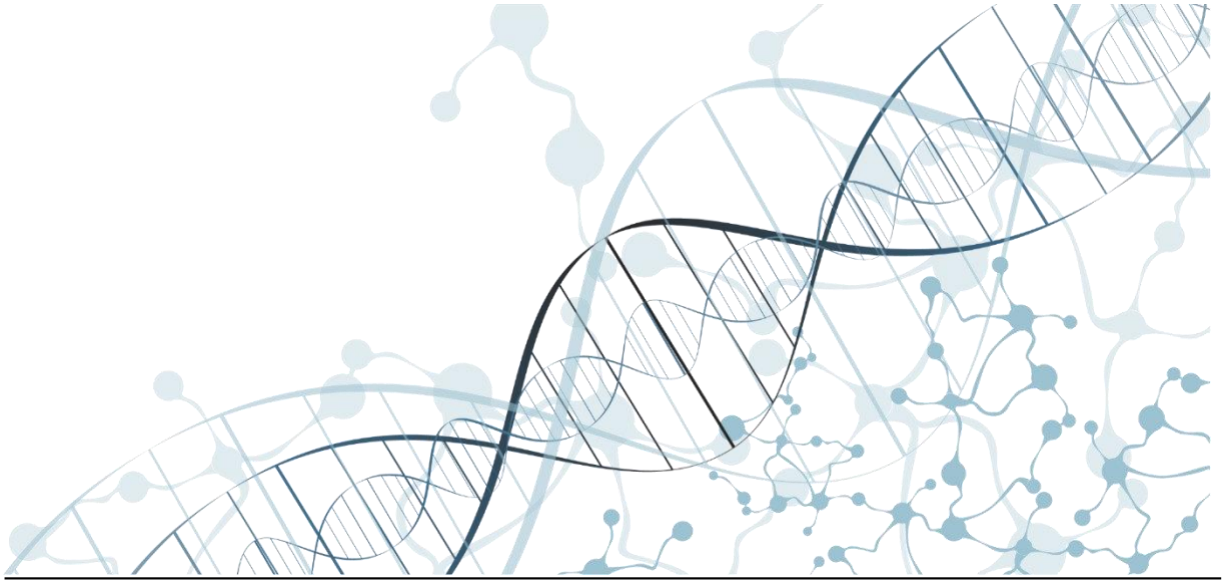
Cisco Intelligent Capture Deployment Guide



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

Table of Contents

OVERVIEW OF CISCO DNA CENTER'S INTELLIGENT CAPTURE 3

RECOMMENDED SOFTWARE REQUIREMENTS 3
SUPPORTED DEVICE SIDE SOFTWARE & HARDWARE REQUIREMENTS 4
PREREQUISITE: INSTALL INTELLIGENT CAPTURE PACKAGE ONTO CISCO DNA CENTER 6
DAY 0 CONFIGURATION – SETTING UP CISCO DNA CENTER TO USE INTELLIGENT CAPTURE 7
Day 0 Configuration Part 1 - Build a Site Hierarchy 7
Step 1: Navigate to the Network Hierarchy Page 7
Step 2: Create Sites, Building, and Floors 8
Step 3: Navigate to the Network Settings Page 10
Step 4: Configure Network Settings and Device Credentials 11
Day 0 Configuration Part 2 - Discovery and Inventory 12
Step 1: Navigate to the Discovery application 12
Step 2: Discover Controllers and Access Points onto Cisco DNA Center 13
Step 3: Navigate to Inventory 15
Step 4: Assign Discovered Device to Site Hierarchy 16
Step 5: Place your Access Points onto your Floor Map 18
Day 0 Configuration Part 3 - Integrate Cisco DNA Center with Cisco CMX 21
Step 1: Add WLC Instance into CMX 21
Step 2: Add CMX into Cisco DNA Center 22
Day 0 Configuration Part 4 - Integrate Cisco DNA Center with vNAM 25
Step 1: Bring up vNAM on an ESXI 25
Step 2: Configure vNAM to Establish Communication with Cisco DNA Center 26
Step 3: Configure Cisco DNA Center to Establish Communication with vNAM 27
DAY 1 - INTELLIGENT CAPTURE FEATURES AND USE CASES 30
Day 1 Access Point Intelligent Capture 30
Step 1: Enabling AP Stats Capture 30
Step 2: Navigate to the Intelligent Capture AP Page 33
Step 3: Viewing the Intelligent Capture AP RF Statistics Page 35
Step 4: Navigating to and Enabling Spectrum Analysis 38
Step 5: Viewing Spectrum Analysis Data 39
Day 1 Client Intelligent Capture 43
Step 1: Navigate to Intelligent Capture Client Page 43
Step 2: Enabling and Viewing Data Packet Capture Data 45
Step 3: Enabling and View Live Capture Data 47
Step 4: Scheduling a Live Capture Data 48
Step 5: Viewing Client Statistics Data 50
Step 6: Enabling and Viewing Anomaly Stats Capture 52
DEVICE SIDE CONFIGURATIONS AND SHOW COMMANDS 57
AireOS WLC Show Commands 57
AireOS WLC Configuration Commands 58
IOS-XE WLC Show Commands 62
IOS-XE WLC Configuration Commands 62
AP Show Commands 65

USEFUL LINKS 66

© 2020 Cisco Systems, Inc. All rights reserved.

Overview of Cisco DNA Center's Intelligent Capture

Cisco DNA Center is the foundational controller and analytics platform at the heart of Cisco's intent-based networking solution. The software platform offers a centralized intuitive management system that makes it fast and easy to design, provision, and apply policies across your network environment. Cisco DNA Center UI provides an intuitive end-to-end network visibility, and uses network insights to optimize network performance and deliver the best user and application experience.

Built on top of this technology is Intelligent Capture, which is Cisco's newest state-of-the-art intent-based networking solution. Intelligent Capture has the purpose of providing users with live technical insight into various wireless metrics from both the client and access point perspective, to allow a user to easily resolve even the most difficult wireless issues.

Intelligent Capture provides support for a direct communication link between Cisco DNA Center and access points (APs), so each of the APs can communicate with Cisco DNA Center directly. Using this channel, the Cisco DNA Center can receive packet capture data, AP and client statistics, and spectrum data. With the direct link from the AP to Cisco DNA Center via gRPC, Intelligent Capture allows you to access data from APs that is not available from wireless controllers.

This deployment guide covers the details in regards to the configuration of Cisco DNA Center, access points, and controllers related to the configuration of Intelligent Capture.

Recommended Software Requirements

- Cisco DNA Center Release 2.1.1.0
- Cisco WLC & AP Release AireOS 8.10MR3 or IOS-XE 17.3.1
- Cisco Connect Mobile Experiences (CMX) Release 10.6.2-89
- Cisco Prime Virtual Network Analysis Module (vNAM) Release 6.4.2

Cisco DNA Center & Device Side Recommended Compatibility Matrix		
DNAC Release	**WLC Release**	
	AireOS	**IOS-XE**
2.1.1.x	8.10MR3	17.3.1
1.3.3.x	8.10MR2	17.2.1
1.3.1.x	8.10MR1	16.12.1s
1.3.0.x	8.8.MR2	16.11.1c

Table 1. This table depicts the recommended compatibility between Cisco DNA Center, and devices.

Note: This document is based on the recommended Cisco DNA Center Release v2.1.1 and Controller/AP release of either 8.10MR3 or 17.3.1. Some software features are not supported on an earlier software release.

© 2020 Cisco Systems, Inc. All rights reserved.

Supported Device Side Software & Hardware Requirements

Supported Cisco AireOS Wireless Controllers		
Device	**Minimum Supported Software Version**	**Recommended Software Version**
Cisco 3504 Wireless Controller	8.8.125.0	8.10MR3
Cisco 5520 Wireless Controller	8.8.125.0	8.10MR3
Cisco 8540 Wireless Controller	8.8.125.0	8.10MR3

Table 2. Cisco Wireless Controllers that support Intelligent Capture.

Supported Cisco Catalyst Wireless Controllers		
Device	**Minimum Supported Software Version**	**Recommended Software Version**
Embedded Wireless Controller	16.12.1s	17.3.1
Cisco Catalyst 9800-CL Wireless Controller	16.12.1s	17.3.1
Cisco Catalyst 9800-L Wireless Controller	16.12.1s	17.3.1
Cisco Catalyst 9800-40 Wireless Controller	16.12.1s	17.3.1
Cisco Catalyst 9800-80 Wireless Controller	16.12.1s	17.3.1

Table 3. Cisco Catalyst Wireless Controllers that support Intelligent Capture.

Supported Cisco APs				
	AireOS Software		**IOS-XE Software**	
Device	**Minimum Version**	**Recommended Version**	**Minimum Version**	**Recommended Version**
Aironet 1540 AP	8.10.105.0	8.10MR3	16.12.1s	17.3.1
Aironet 1560 AP	8.10.105.0	8.10MR3	16.12.1s	17.3.1
Aironet 1815 AP	8.10.105.0	8.10MR3	16.12.1s	17.3.1
Aironet 1830 AP	8.10.105.0	8.10MR3	16.12.1s	17.3.1
Aironet 1840 AP	8.10.105.0	8.10MR3	16.12.1s	17.3.1
Aironet 1850 AP	8.10.105.0	8.10MR3	16.12.1s	17.3.1
Aironet 2800 AP	8.8.125.0	8.10MR3	16.12.1s	17.3.1
Aironet 3800 AP	8.8.125.0	8.10MR3	16.12.1s	17.3.1
Aironet 4800 AP	8.8.125.0	8.10MR3	16.12.1s	17.3.1
Catalyst 9105 AP	8.10MR3	8.10MR3	17.3.1	17.3.1
Catalyst 9115 AP	8.10.105.0	8.10MR3	16.12.1s	17.3.1
Catalyst 9120 AP	8.10.105.0	8.10MR3	16.12.1s	17.3.1
Catalyst 9130 AP	8.10MR3	8.10MR3	17.3.1	17.3.1
Catalyst IW6300 Heavy Duty AP	8.10.105.0	17.1.1s	8.10.105.0	17.1.1s
Catalyst ESW6300 Embedded Services AP	8.10.105.0	17.1.1s	8.10.105.0	17.1.1s

Table 4. Cisco APs that support Intelligent Capture.

© 2020 Cisco Systems, Inc. All rights reserved.

Intelligent Capture Feature Compatibility Matrix							
Feature	**WLC Type**	**Support AP Model Series**					
		18xx 1540	**2800 3800 1560**	**4800**	**C9115**	**C9120**	**C9130**
Anomaly Detection Onboarding PCAP AP Stats Client Stats	AireOS	8.10	8.8 MR2	8.8 MR2	8.10	8.10	8.10 MR3
	IOS-XE	16.12.1s	16.12.1s	16.12.1s	16.12.1s	16.12.1s	17.3.1
Data PCAP	AireOS	N/A	N/A	8.8 MR2	N/A	N/A	8.10 MR3
	IOS-XE	N/A	N/A	16.12.1s	N/A	N/A	17.3.1
Spectrum Analysis	AireOS	N/A	8.8 MR2	8.8 MR2	N/A	8.10 MR2	8.10 MR3
	IOS-XE	N/A	16.12.1s	16.12.1s	N/A	17.2.1	17.3.1

Table 5. Intelligent Capture Feature Compatibility with Device Side Hardware and Software

© 2020 Cisco Systems, Inc. All rights reserved.

Prerequisite: Install Intelligent Capture Package onto Cisco DNA Center

Cisco DNA Center provides the option to download a separate Intelligent Capture package called **Automation – Intelligent Capture**.

To download and install this package, follow the steps below:

1. Log into Cisco DNA Center.
2. Click on the hamburger menu at the top left-hand corner of the screen.
3. Click on **System** then **Software Updates**.
4. Click **Installed Apps** on the left-hand side of the screen.
5. Scroll down to **Assurance** and you will find the **Automation – Intelligent Capture** package ready for download and installation.

Note: If you do not see the **Automation – Intelligent Capture** package from the steps above, please reach out to either a Cisco's Account Sales Representative, or an Account Sales Engineer to acquire additional support.

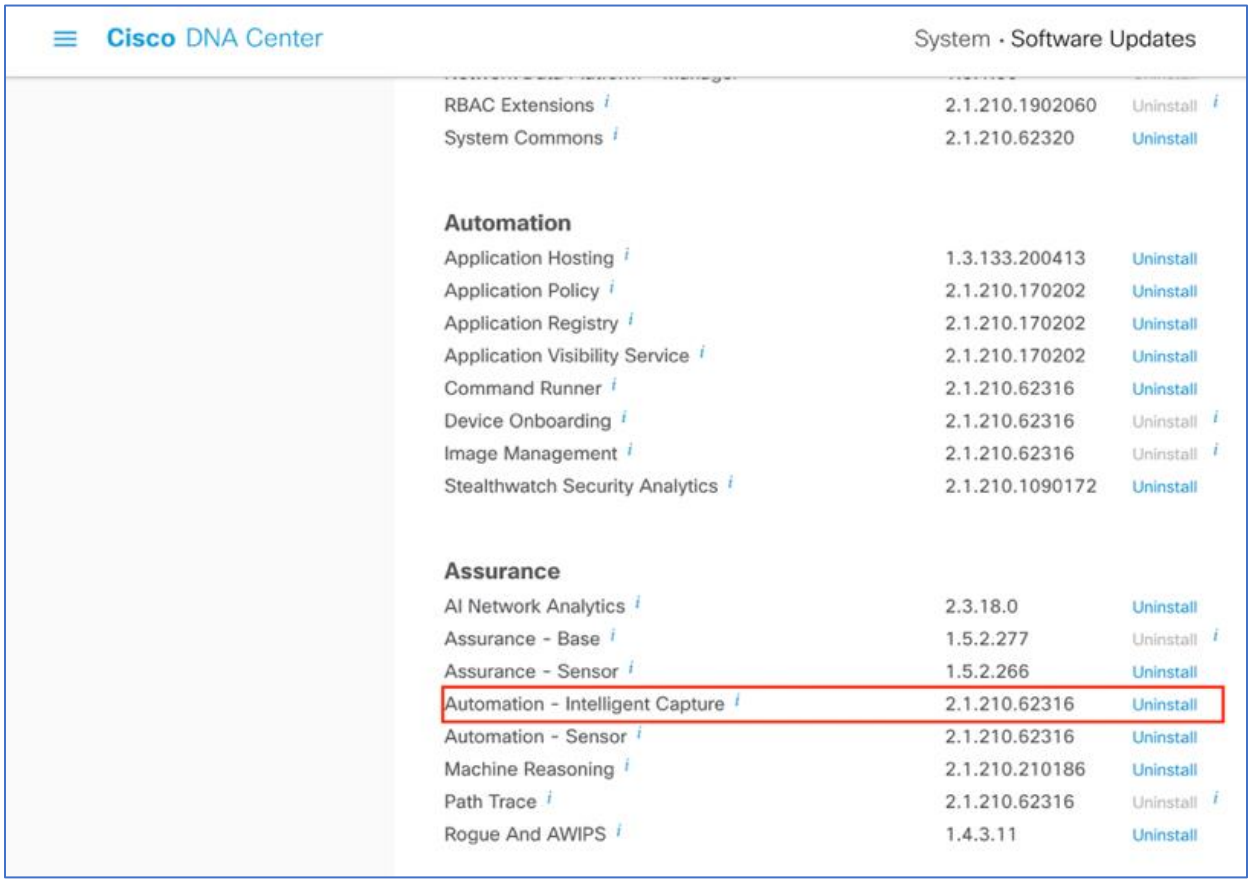


Figure 1. Location of Intelligent Package within Software Updates Page

© 2020 Cisco Systems, Inc. All rights reserved.

Day 0 Configuration – Setting up Cisco DNA Center to Use Intelligent Capture

The purpose of the following DAY 0 sub sections is to provide users with step by step instructions with regards to the day 0 configurations necessarily to begin using Intelligent capture.

Day 0 Configuration Part 1 - Build 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 2.****).*

2. ***Option 2:*** *Click on the hamburger menu at the top left-hand corner of the screen. Click on* ***Design*** *then* ***Network Hierarchy*** *(****Figure 3.****).*

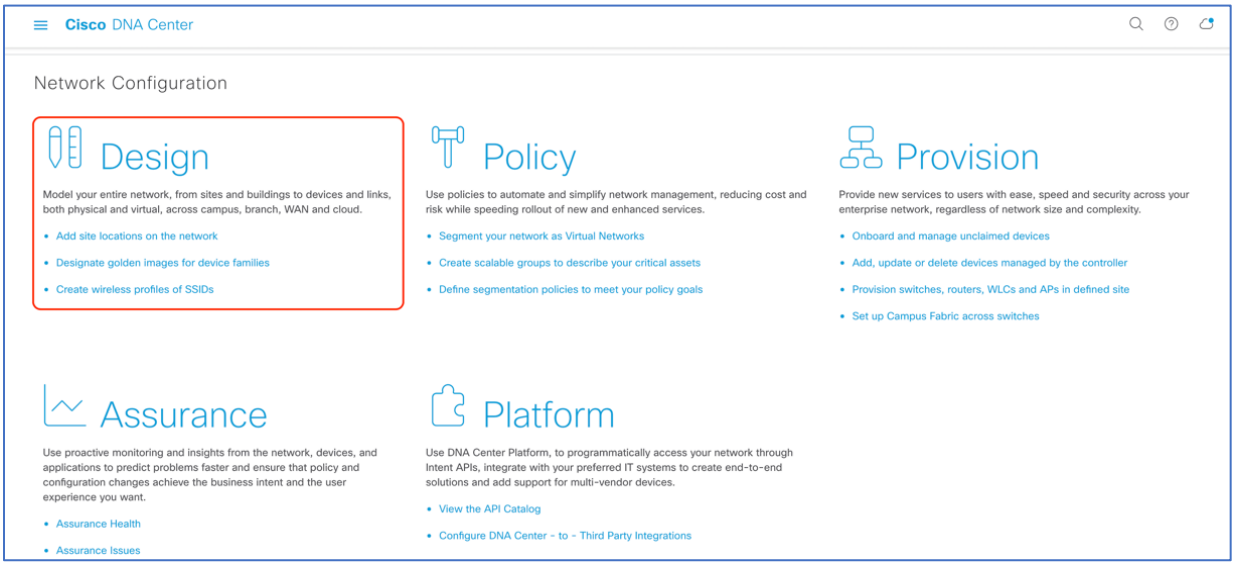


Figure 2. Location of the Design Page on Cisco DNA Center's Home Page.

© 2020 Cisco Systems, Inc. All rights reserved.

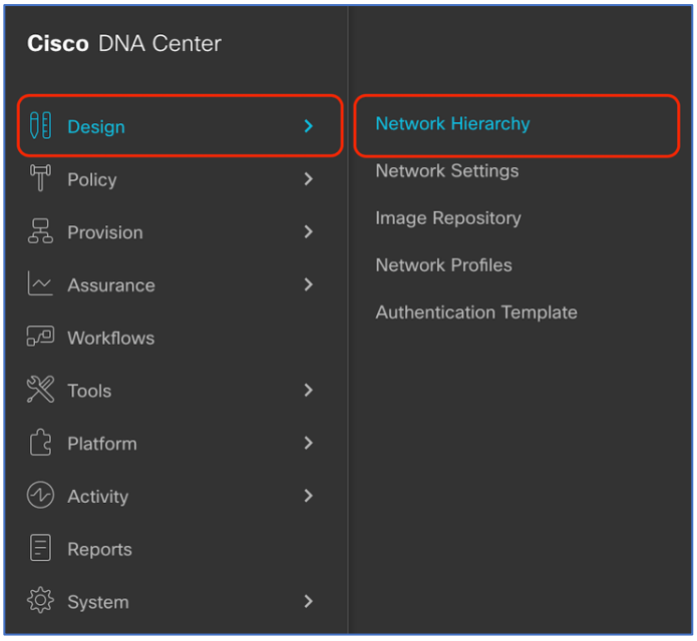


Figure 3. Location of Network Hierarchy from the Hamburger Menu.

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 4.**), 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 5.**) 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 6.**).*
    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.

© 2020 Cisco Systems, Inc. All rights reserved.

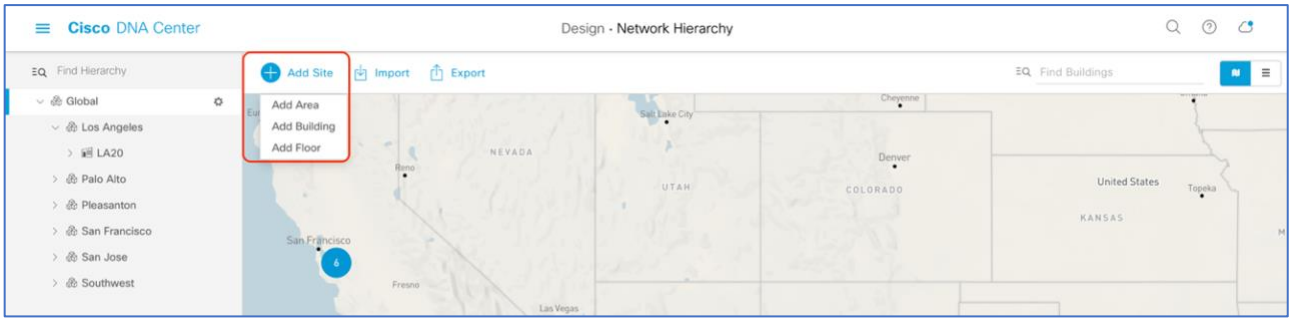


Figure 4. Clicking on **Add Site** Within the Design – Network Hierarchy page

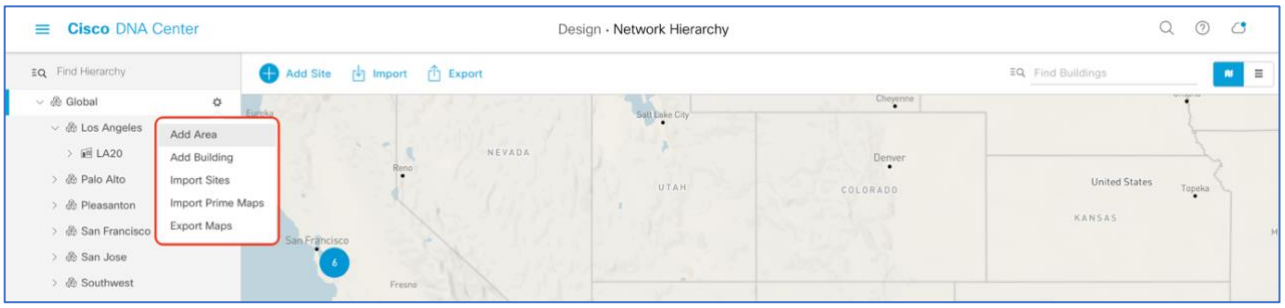


Figure 5. Clicking on the gear icon Next to a Site Within the Design – Network Hierarchy page

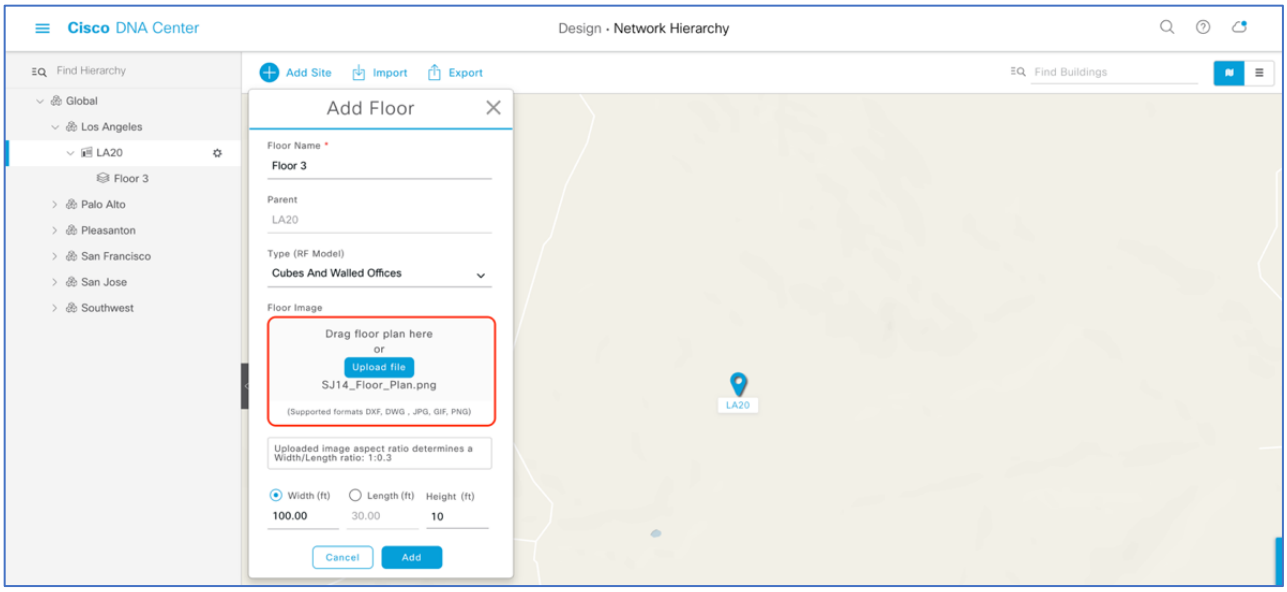


Figure 6. Location of the **Upload file** to upload a floor plan during floor creation

© 2020 Cisco Systems, Inc. All rights reserved.

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 hamburger menu at the top left-hand corner of the screen. Click on **Design** then **Network Settings** (**Figure 7.**).*

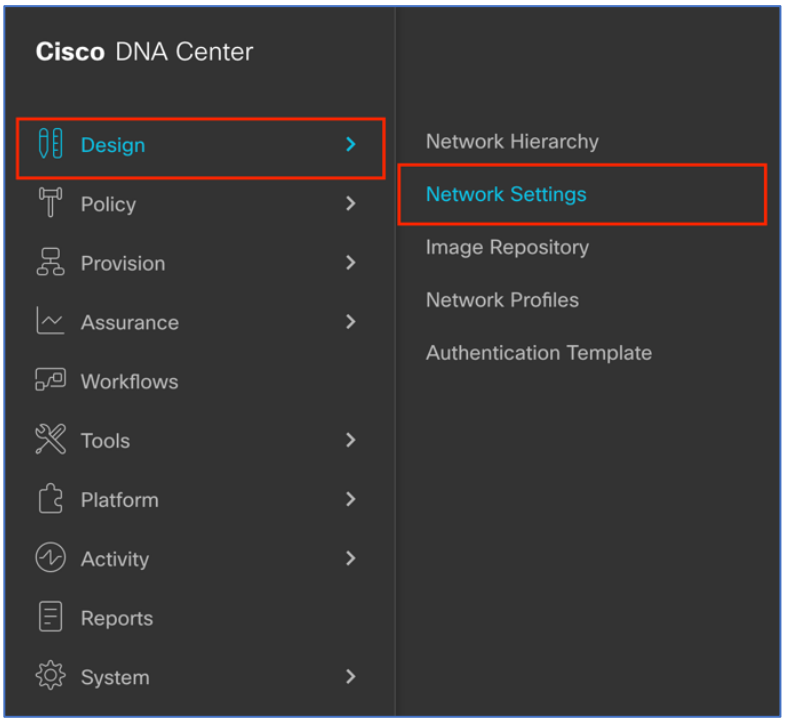


Figure 7. Location of Network Settings from the Hamburger Menu.

© 2020 Cisco Systems, Inc. All rights reserved.

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 8.**).*

2. *Click on the **Add** button to create new credential entries (**Figure 9.**). Cisco DNA Center uses these credentials to discover the network devices.*

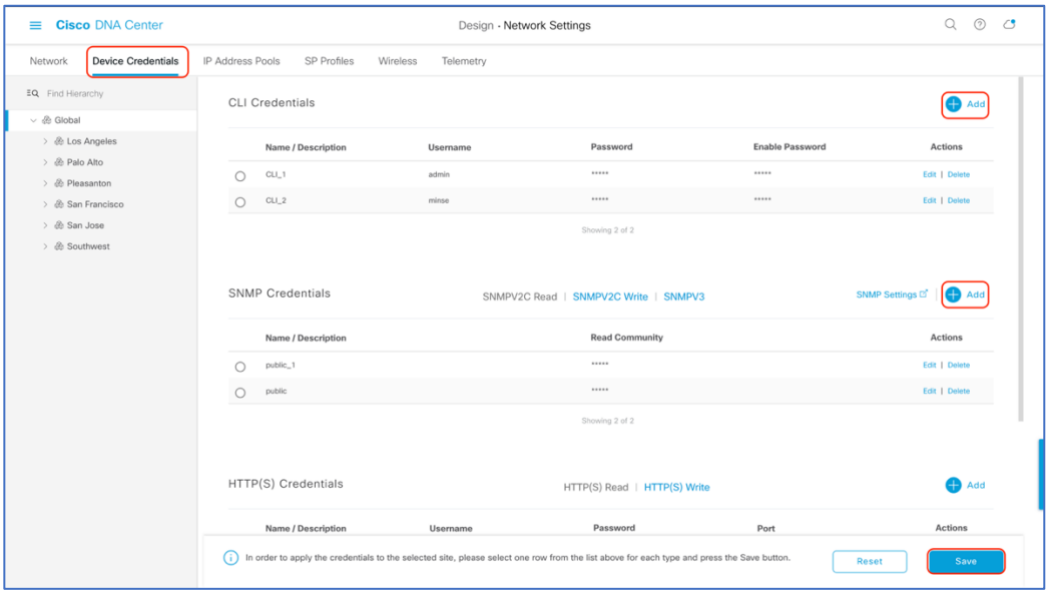


Figure 8. Workflow to Add Device Credentials to the Network Settings.

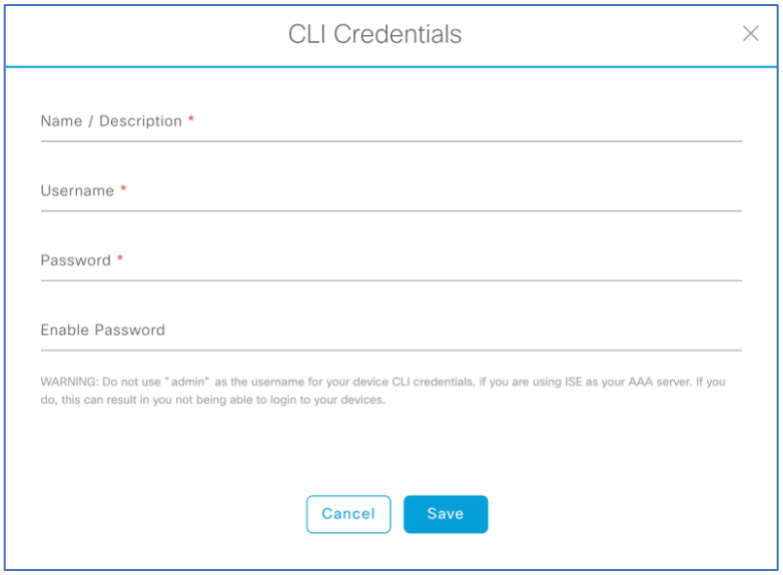


Figure 9. CLI credentials form that appears when clicking on Add in Figure 8.

© 2020 Cisco Systems, Inc. All rights reserved.

Day 0 Configuration Part 2 - 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 10. & 11)***

2. ***Option 2:*** *Click on the hamburger menu at the top left-hand corner of the screen. Click on* ***Tools*** *then* ***Discovery*** *(****Figure 12.****).*

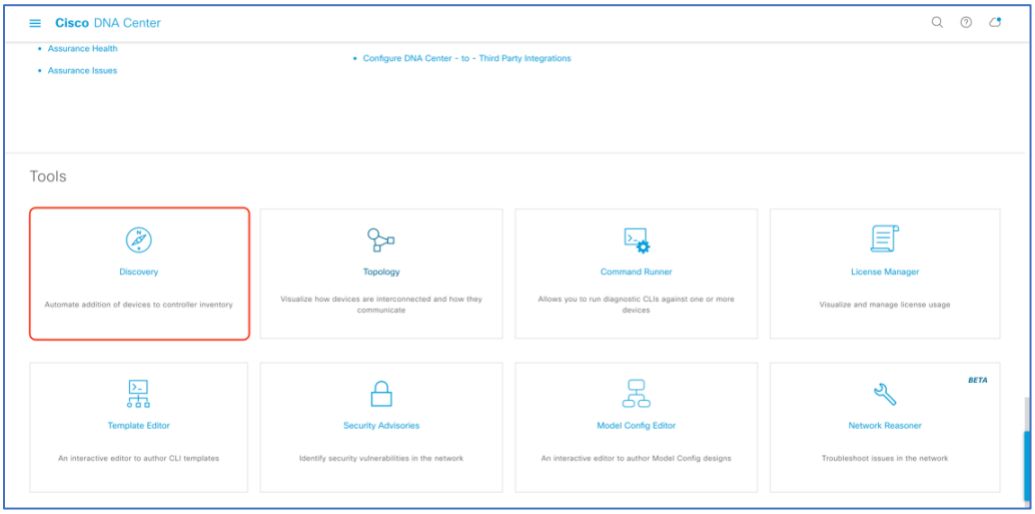


Figure 10. Location of Discovery button on Cisco DNA Center Homepage

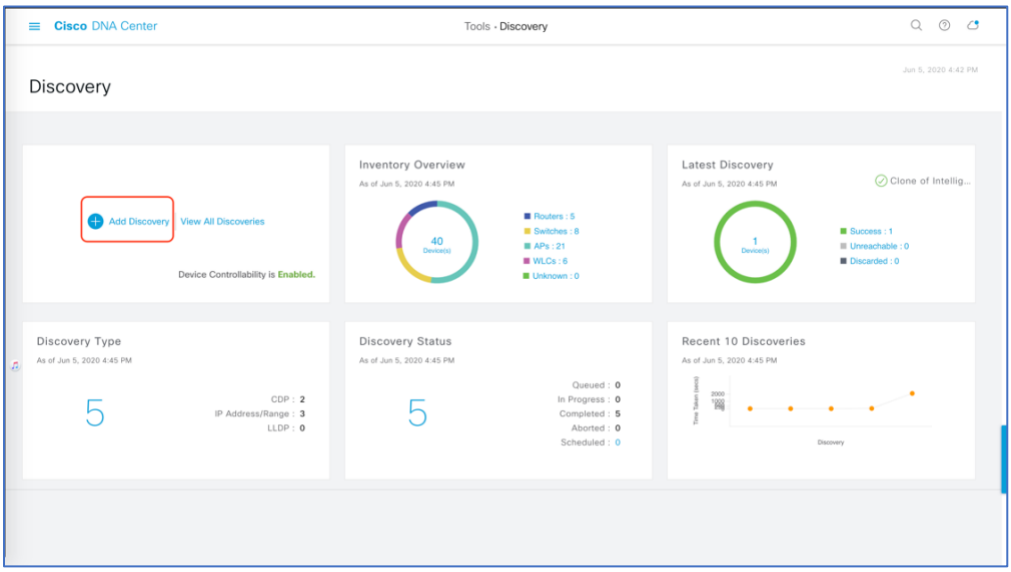


Figure 11. Location of Add Discovery button on Tools - Discovery Page

© 2020 Cisco Systems, Inc. All rights reserved.

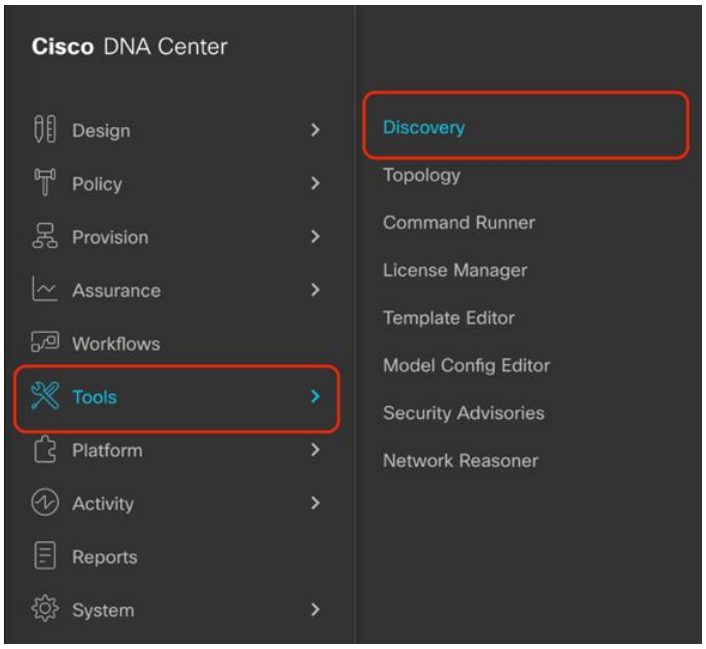


Figure 12. Location of Discovery within the Hamburger Menu

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

To Discover a WLC onto Cisco DNA Center Follow the Steps Below (**Figure 13.**):

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).*

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.

© 2020 Cisco Systems, Inc. All rights reserved.

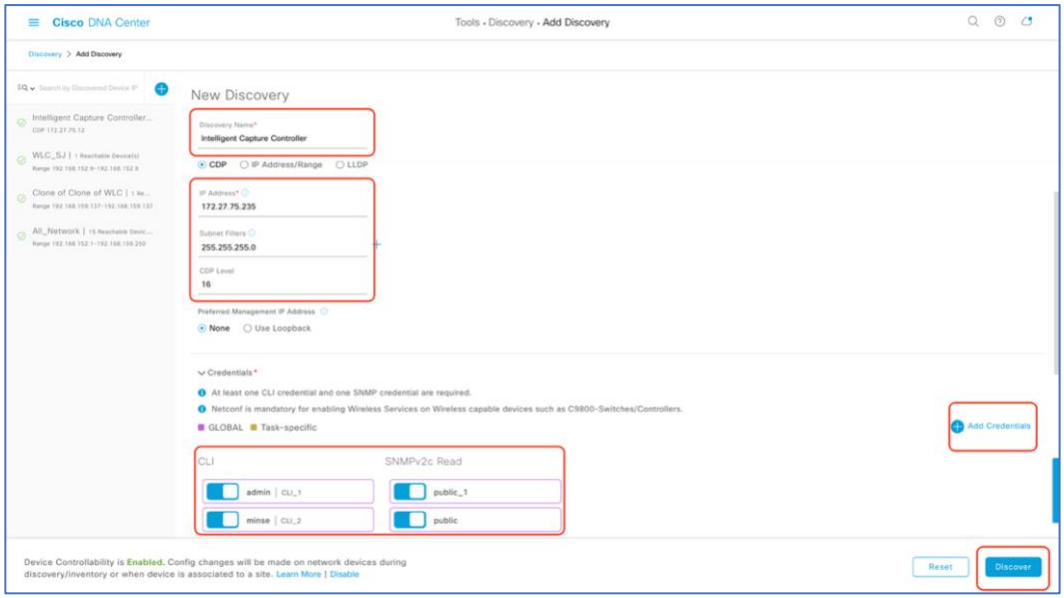


Figure 13. Discovery Page with Credentials Filled in and Ready for Discovery

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 14.**).*

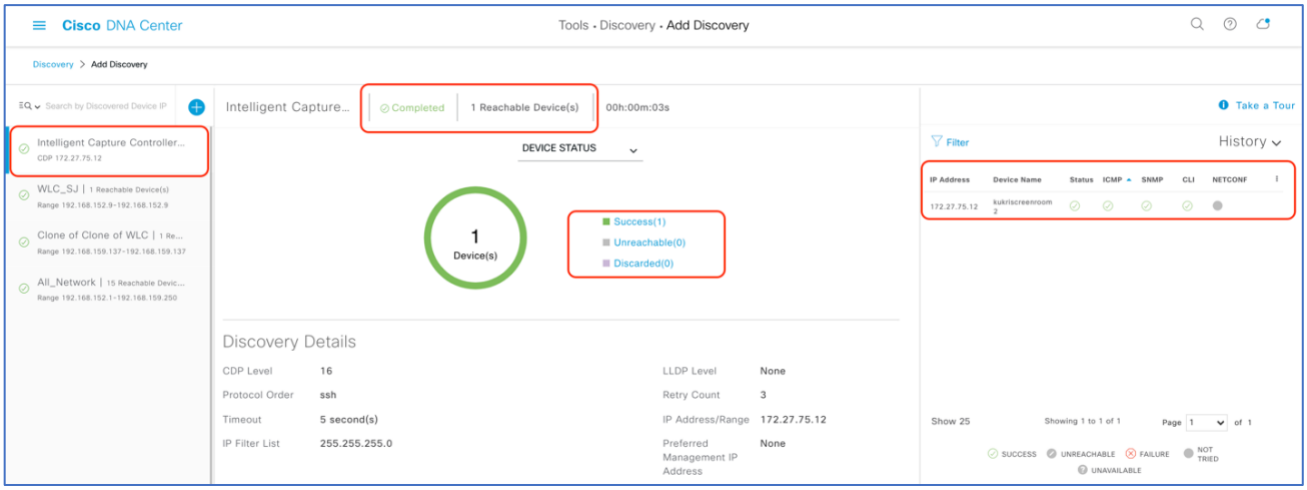


Figure 14. Success Discovery of WLC on the Discovery Page.

© 2020 Cisco Systems, Inc. All rights reserved.

Step 3: Navigate to Inventory

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

1. *Open up the hamburger menu, click on **Provision** then **Inventory** (**Figure 15.**)*

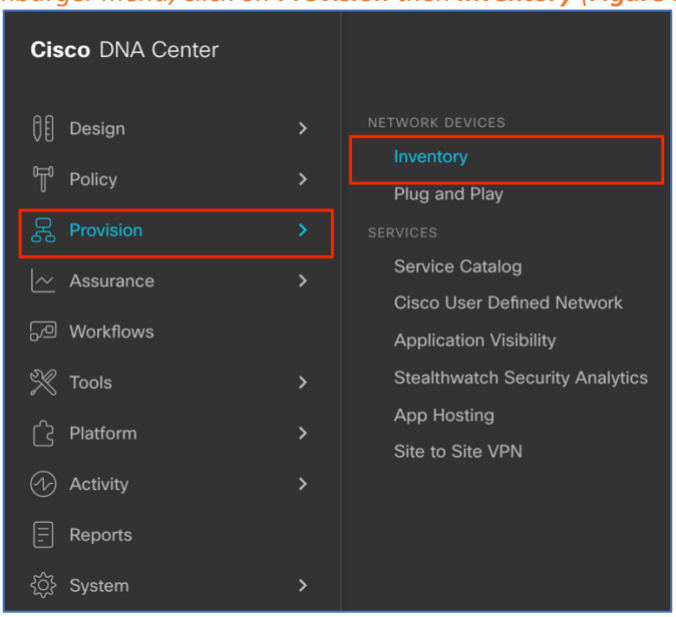


Figure 15. Location of Inventory within the Hamburger Menu.

2. *Click on the **Unassign Devices** to the left, and ensure that all devices are **Reachable** and the **Last Sync Status** is **Managed** (**Figure 16**).*
   a. It is critical that all devices are in Managed state for Cisco DNA Center Assurance functionalities to work. If not check the reachability of your devices.

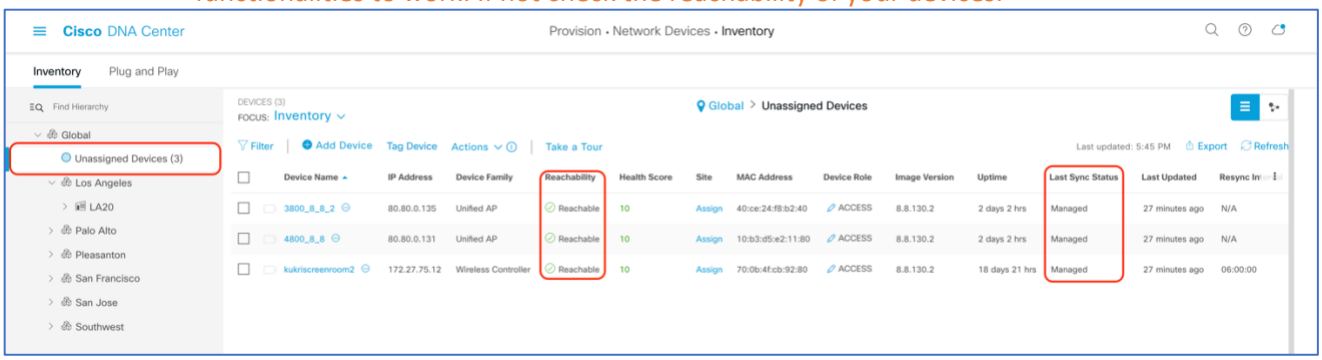


Figure 16. Discovered Device and the State of their Reachability and Last Sync Status

© 2020 Cisco Systems, Inc. All rights reserved.

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 17.****).*

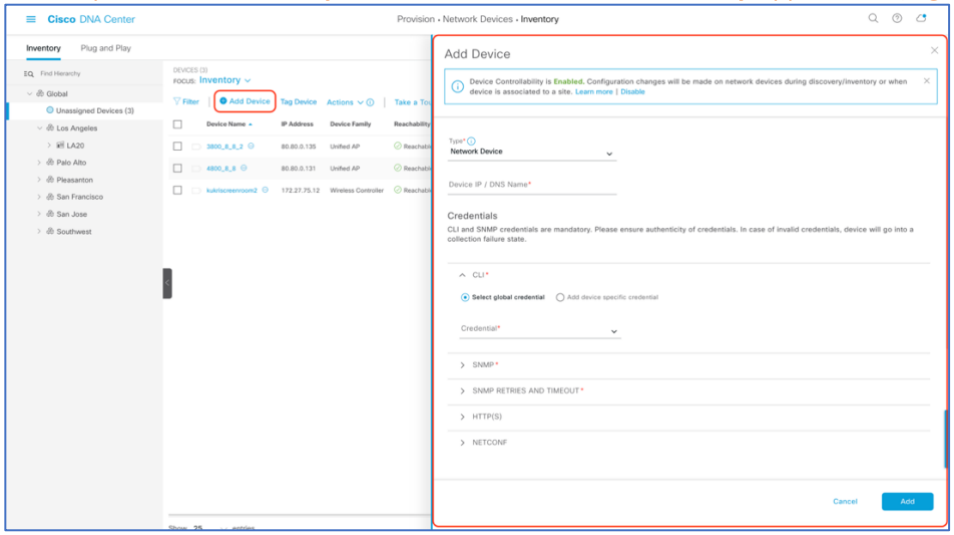


Figure 17. Add Device form that appears when you click on Add Device.

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 Intelligent Capture features to work.

- Pushed Cisco DNA Center Certificate.
- Enabled WLC Streaming Telemetry (WSA)
- Enabled AP Streaming telemetry (gRPC, TCP 32626)
- Configured Cisco DNA Center as a SNMP Trap Receiver.
- Configured Cisco DNA Center as a Syslog server

Note: As of release 2.1.1, Cisco DNA Center will send the WLC a Network Assurance Certificate that enables the WLC and APs to externalize data to Cisco DNA Center opposed to during the discovery workflow as done so in previous releases.

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

2. *Hover your cursor over* ***Action*** *then* ***Provision****, then click on* ***Assign Device to Site*** *(****Figure 18****).*

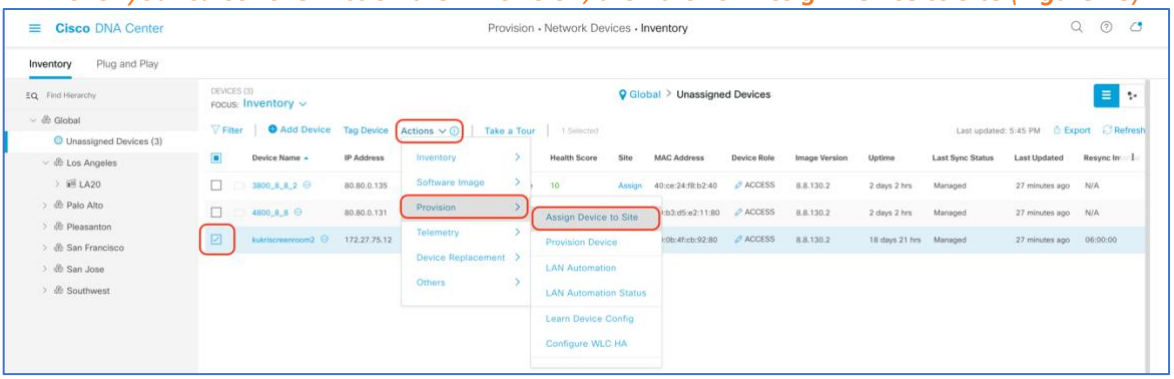


Figure 18. Assigning a WLC to a Site on the Inventory Page

© 2020 Cisco Systems, Inc. All rights reserved.

3. *Click on **Choose a Site** (**Figure 19.**).*

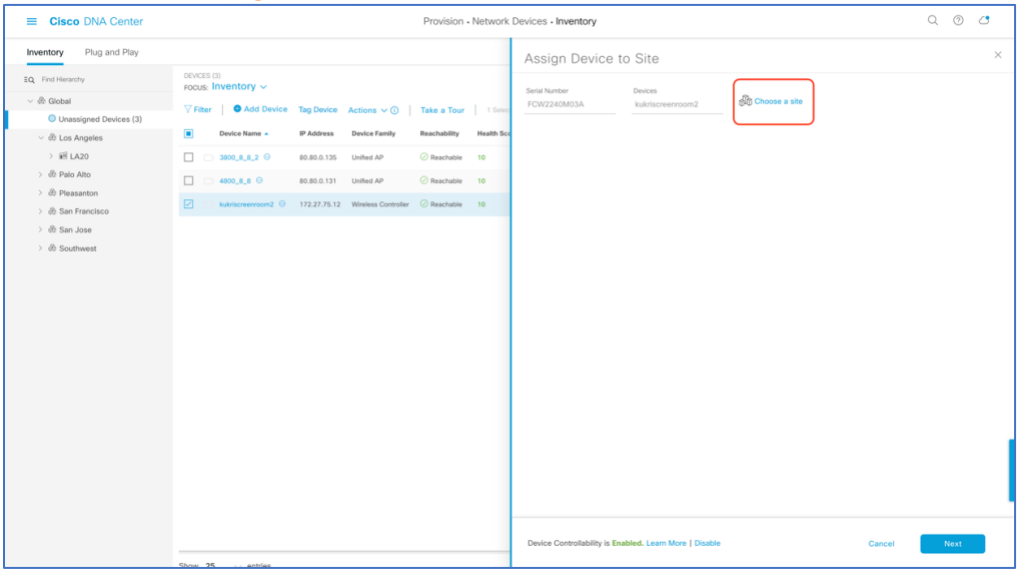


Figure 19. Menu that Appears when Clicking on Assign Device to Site in Figure 18.

4. *Click on the site you would like to assign the WLC to and hit save (**Figure 20.**).*

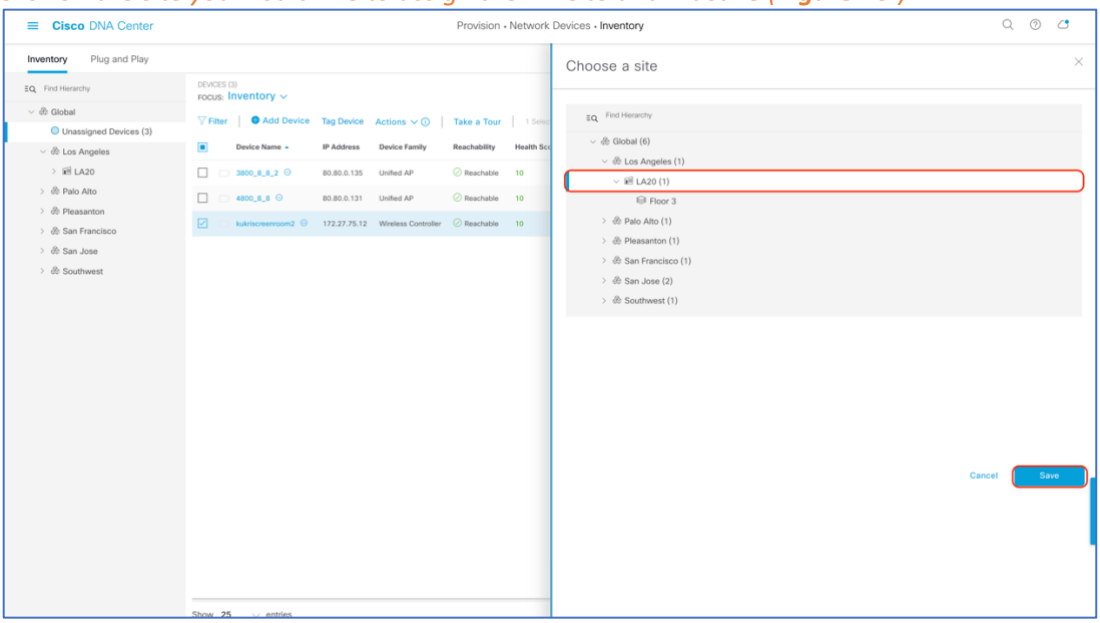


Figure 20. Site Hierarchy Selection Assignment Selection

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

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

© 2020 Cisco Systems, Inc. All rights reserved.

Step 5: Place your Access Points onto your 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.

1. *Navigate to the Network Hierarchy Page by clicking on the hamburger menu at the top left-hand corner of the screen. Click on **Design** then **Network Hierarchy** (**Figure 21.**).*

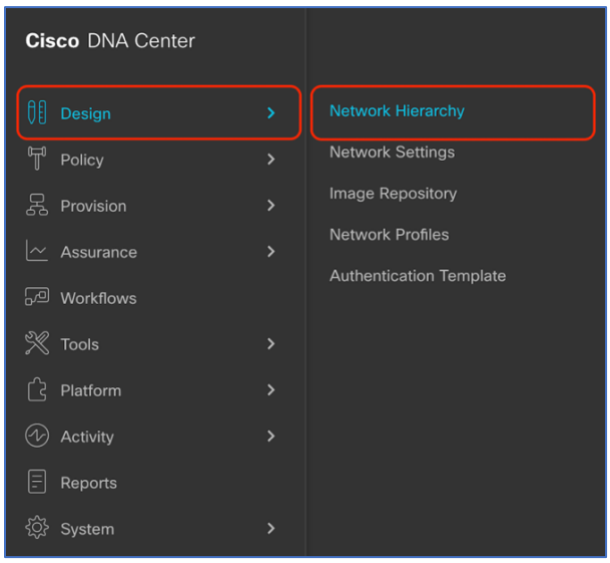


Figure 21. Location of Network Hierarchy from the hamburger menu.

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 22.**).

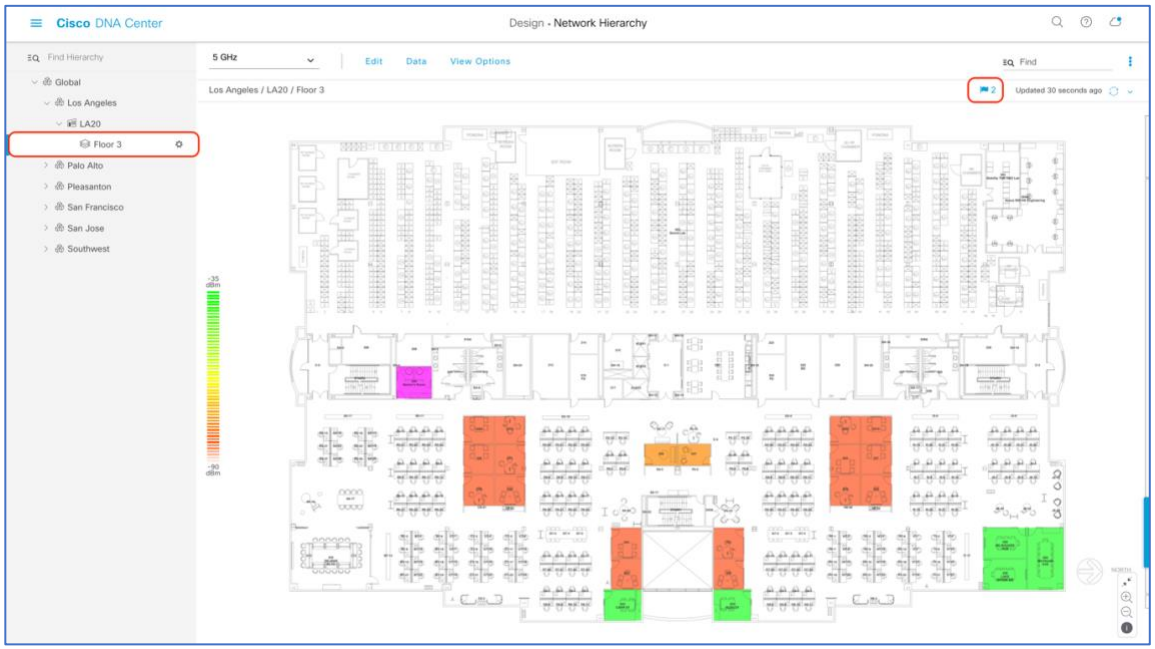


Figure 22. Network Hierarchy Page - Two APs Ready to Be Positioned onto the Floor Map

© 2020 Cisco Systems, Inc. All rights reserved.

4. *Click on **Edit** then on **Position** to place APs onto the map (**Figure 23.**).*

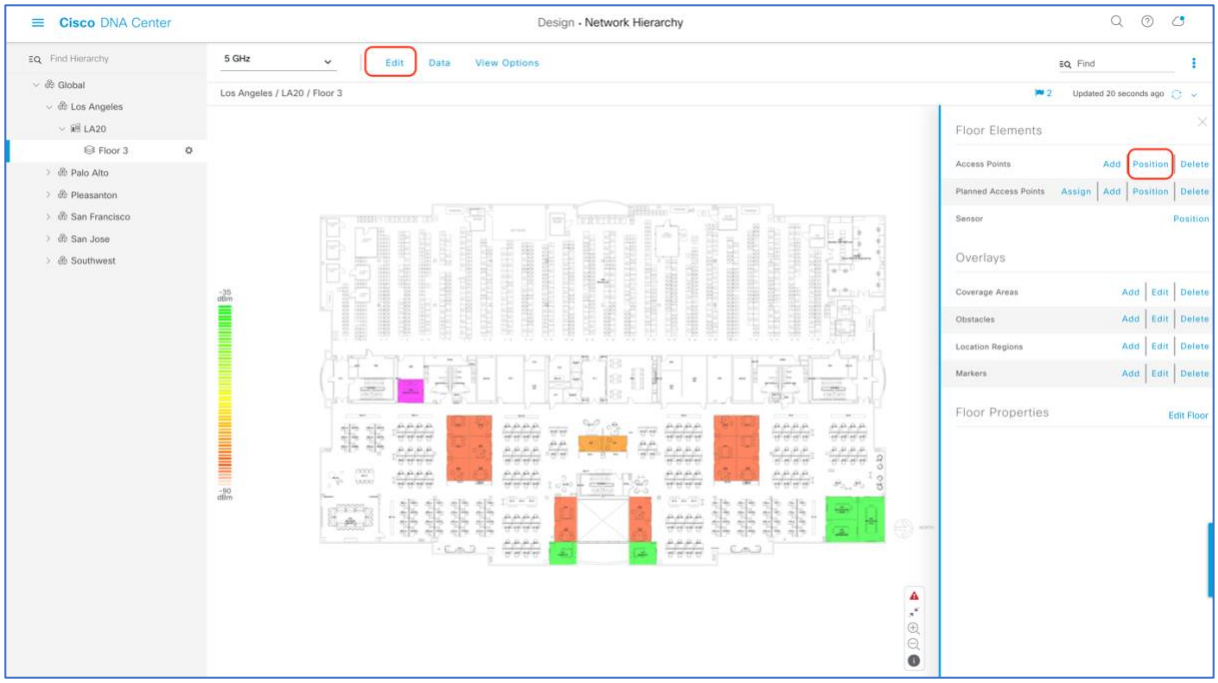


Figure 23. Network Hierarchy Page – Floor Elements Menu

5. *After placing the APs on the floor map, click the **Save** button to commit the change (**Figure 24.**).*

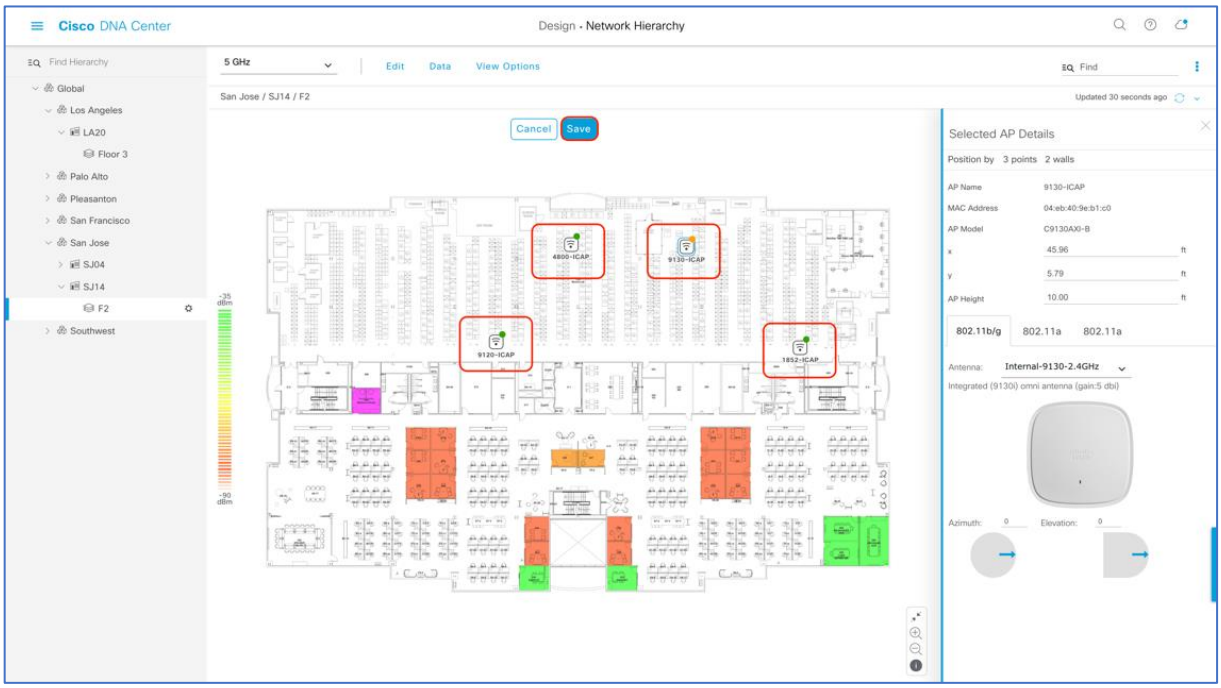


Figure 24. Network Hierarchy Page – With APs placed on the Floor Map

© 2020 Cisco Systems, Inc. All rights reserved.

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 25.**).*

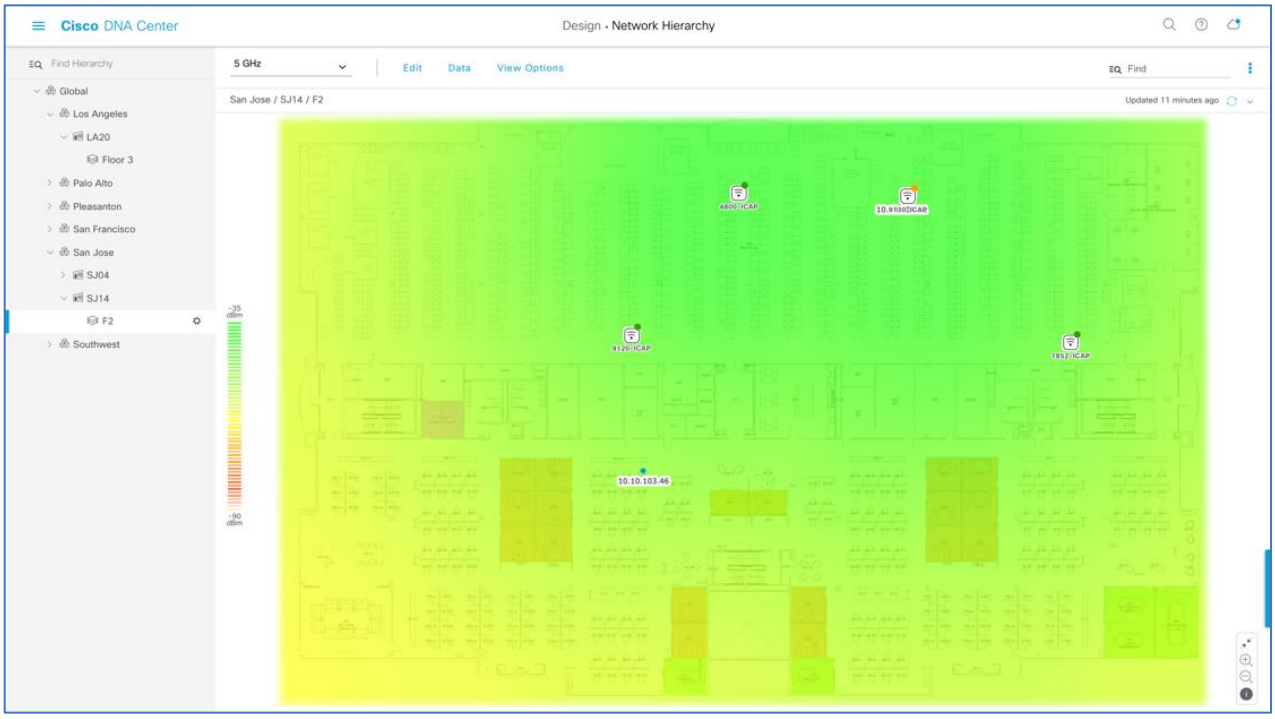


Figure 25. Network Hierarchy Page – Heat Map Displayed After APs are Positioned

Heat Map Color Legend	
Color	**Signal Strength**
Green	Strong RF Signal
Yellow	Good to Fair RF Signal
Orange	Fair to Poor RF Signal
Red	Bad RF Signal

Table 6. Heat Map Color Legend Displayed on Floor Map

© 2020 Cisco Systems, Inc. All rights reserved.

Day 0 Configuration Part 3 - Integrate Cisco DNA Center with Cisco CMX

Description: Integrating Cisco's Connect Mobile Experiences (CMX) with Cisco DNA Center will enable the floor map to locate and display an associated wireless client's current and historical location.

Section Goals: To properly integrate CMX with your Cisco DNA Center to view an associated wireless client's location.

Step 1: Add WLC Instance into CMX

In order to for CMX to send client location data to Cisco DNA Center, we need to add the WLC into CMX.

1. *Navigate to **System**, then scroll down to the **Controllers** section, then click on the **+** button to add new WLC (**Figure 26.**).*

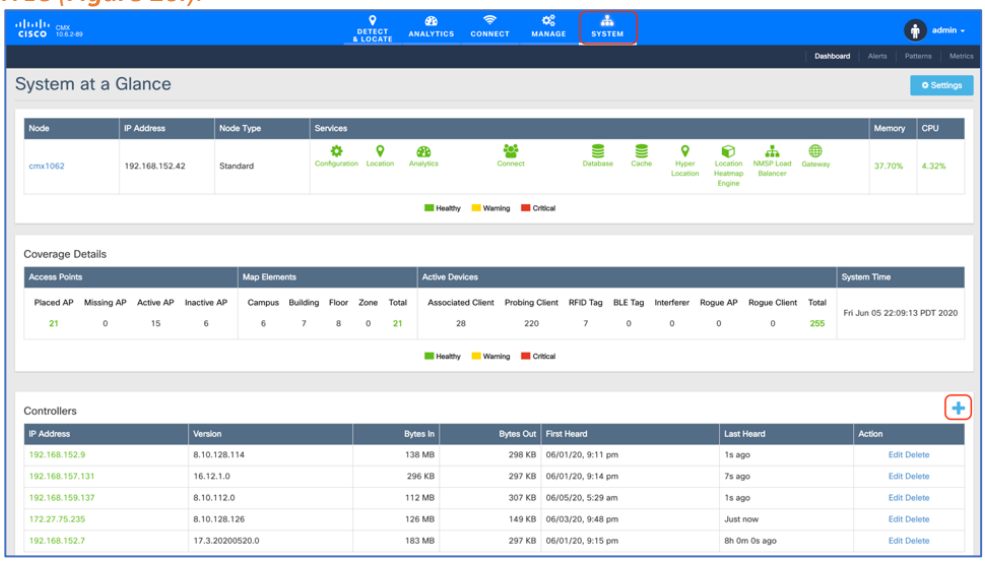


Figure 26. CMX System Page Where we can Add a Controller

2. Click on **Advanced** in the **SETTINGS** modal box that appeared, and choose your controller's Type (AireOS or Polaris), add your controller's IP and SNMP Write Community, then click on save to commit the change (**Figure 27.**).

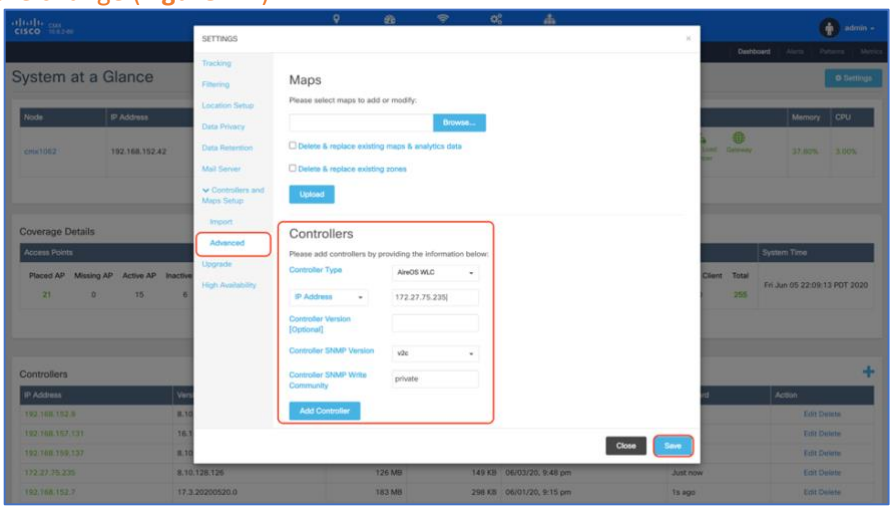
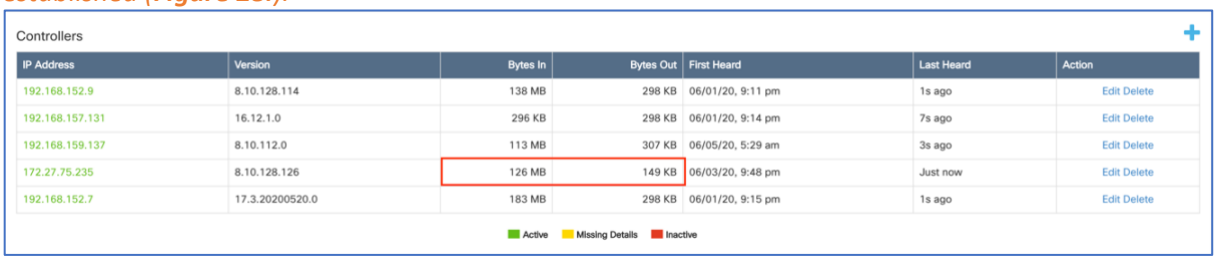


Figure 27. CMX Add Controller Settings Modal Box

© 2020 Cisco Systems, Inc. All rights reserved.

3. *Ensure that within a couple minutes, you should be able to see the **Bytes In** and **Bytes Out** counter increment which signifies that the communication between the WLC and CMX has been established (**Figure 28.**).*



Controllers

IP Address	Version	Bytes In	Bytes Out	First Heard	Last Heard	Action
192.168.152.9	8.10.128.114	138 MB	298 KB	06/01/20, 9:11 pm	1s ago	Edit Delete
192.168.157.131	16.12.1.0	296 KB	298 KB	06/01/20, 9:14 pm	7s ago	Edit Delete
192.168.159.137	8.10.112.0	113 MB	307 KB	06/05/20, 5:29 am	3s ago	Edit Delete
172.27.75.235	8.10.128.126	126 MB	149 KB	06/03/20, 9:48 pm	Just now	Edit Delete
192.168.152.7	17.3.20200520.0	183 MB	298 KB	06/01/20, 9:15 pm	1s ago	Edit Delete

Active Missing Details Inactive

Figure 28. Bytes In and Bytes Out Incrementing Depicting a WLC Properly Connected with CMX

Step 2: Add CMX into Cisco DNA Center

1. *On Cisco DNA Center, open up the hamburger menu click on **System** then **Settings** (**Figure 29.**)*

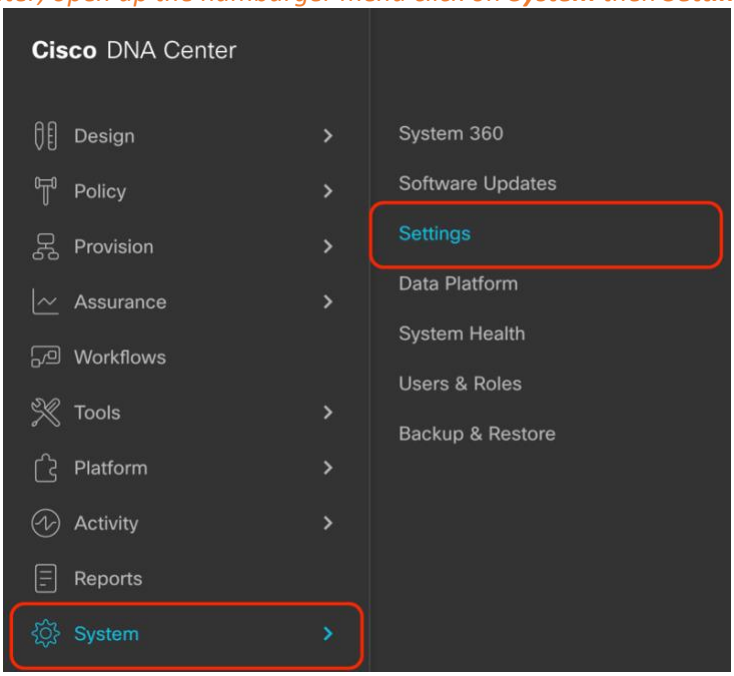


Figure 29. Location of Settings within the Hamburger Menu

2. *On the search bar to the left, type in **CMX**, then click on **CMX Servers** (**Figure 30.**)*

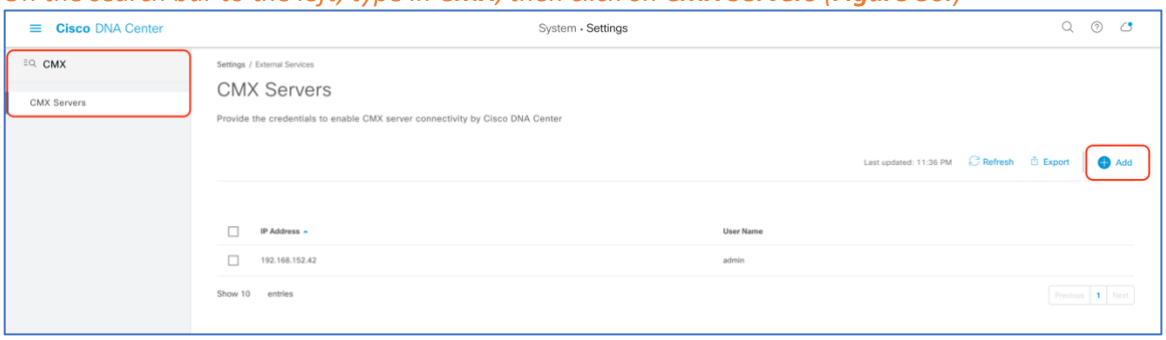


Figure 30. Location of CMX Servers within the Settings Page

© 2020 Cisco Systems, Inc. All rights reserved.

3. *Click on the **Add** button then fill in the CMX IP Addresses, User Name, Password, SSH User Name, and SSH Password within the side menu. Click on the **Add** button within the side menu to save your changes (**Figure 31.**)*

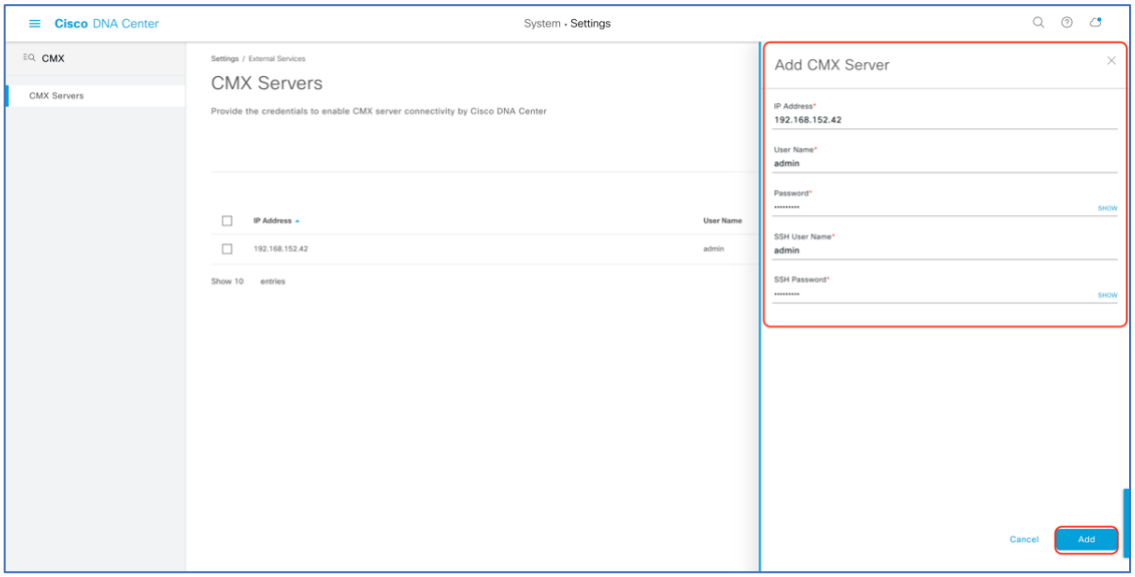


Figure 31. Providing CMX Credentials to Cisco DNA Center During Integration

4. *Now that CMX Integration is completed, navigate back to your floor under site hierarchy, click on the gear icon next to either the floor itself, or any parent site it falls under, then click on **Sync with CMX** to ensure that Cisco DNA Center and CMX are communicating properly (**Figure 32.**).*

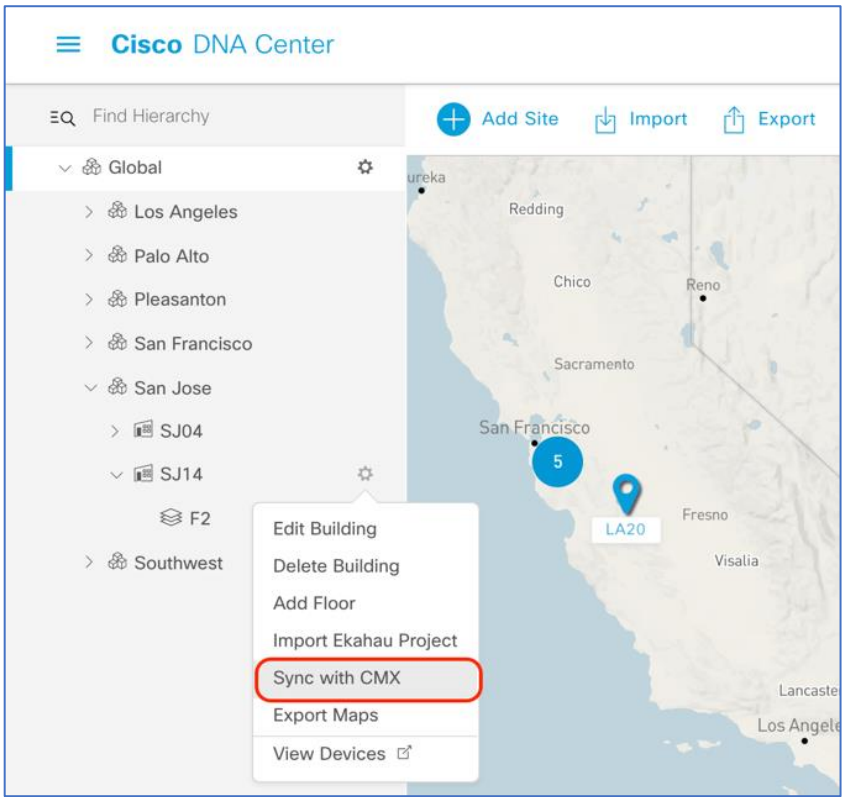


Figure 32. Location of Sync with CMX button

© 2020 Cisco Systems, Inc. All rights reserved.

5. *Navigate back to CMX and observe that the floor map added on Cisco DNA Center has been success imported (Figure 33).*

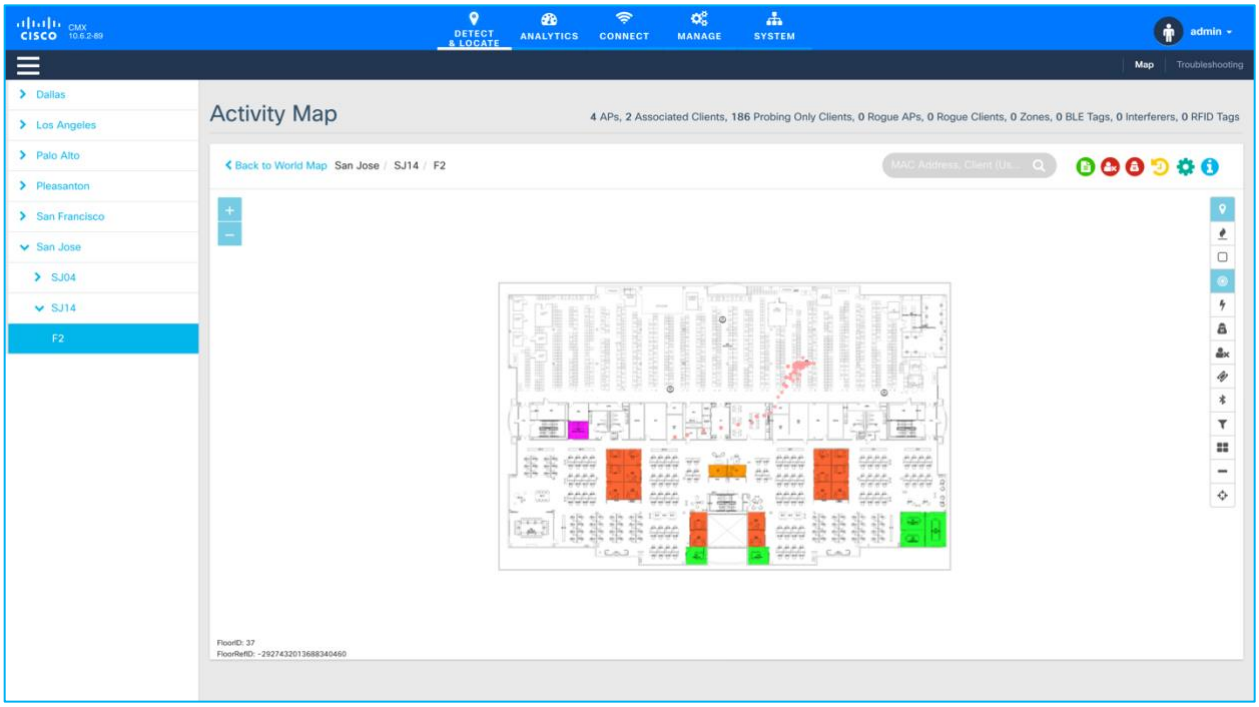


Figure 33. Floor Map from CMX has been Imported from Cisco DNA Center

6. *Ensure that if you have any clients joined to your APs, you should begin able to see them on the heat map within a couple of minutes (**Figure 34.**).*

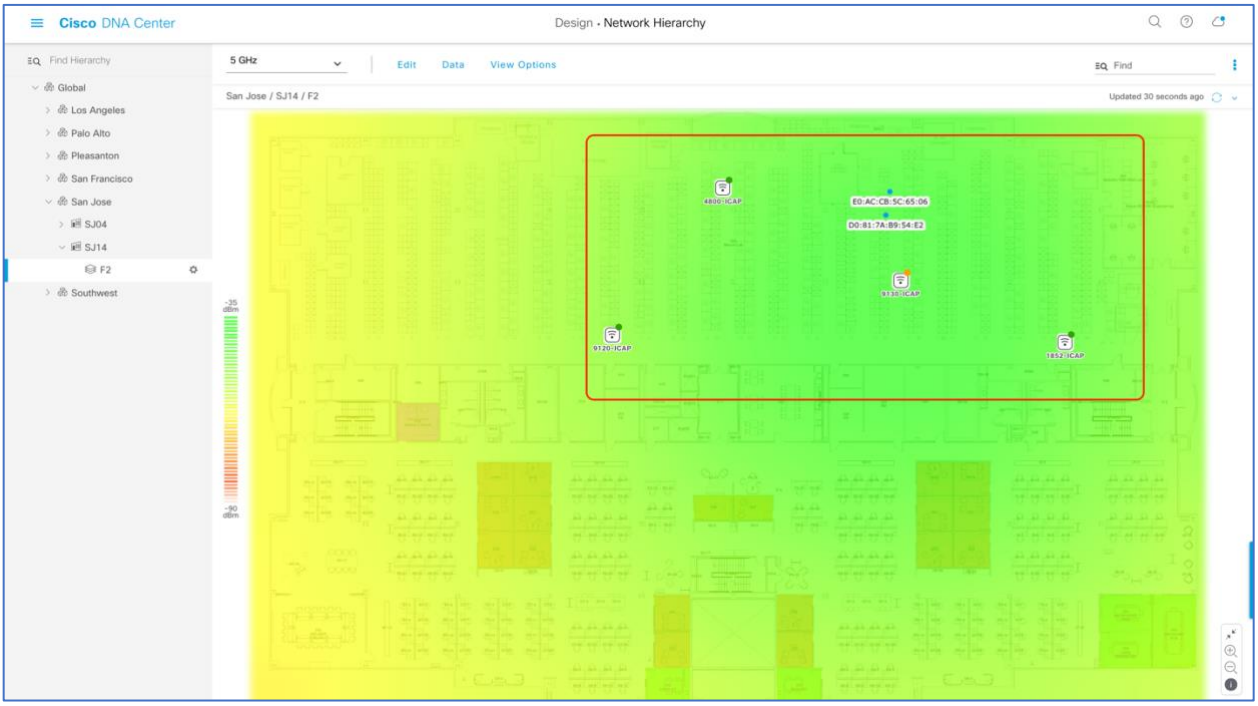


Figure 34. Client Location Shows Up on the Floor's Heat Map

© 2020 Cisco Systems, Inc. All rights reserved.

Day 0 Configuration Part 4 - Integrate Cisco DNA Center with vNAM

Description:

- The Prime vNAM provides all of the functionality found in NAM, permitting consistent application awareness, comprehensive performance analytics, and deep network visibility.

- The Prime vNAM allows network administrators to:
  - Gain Layer 4-7 application visibility using Cisco Network-based Application Recognition 2 (NBAR2) natively in NAM to help identify and improve the performance of business-critical applications
  - Analyze network usage by applications, hosts or virtual machines, and conversations to identify bottlenecks that may affect performance and availability
  - Troubleshoot performance problems consistently across physical and virtual environments using detailed flow- and packet-based analytics
  - Eliminate the need to backhaul the data to a centralized location by using the integrated web-based interface for remote management and monitoring
  - Validate infrastructure updates such as QoS policy changes

Section Goals: To properly integrate vNAM with your Cisco DNA Center to provide a deep network visibility when using Intelligent Capture's Data Packet Capture Feature.

Step 1: Bring up vNAM on an ESXI

1. Use the following link to acquire the vNAM 6.4.2 OVA File and bring it up on your ESXI (**Figure 35.**) http://cs.co/9009GHYGV

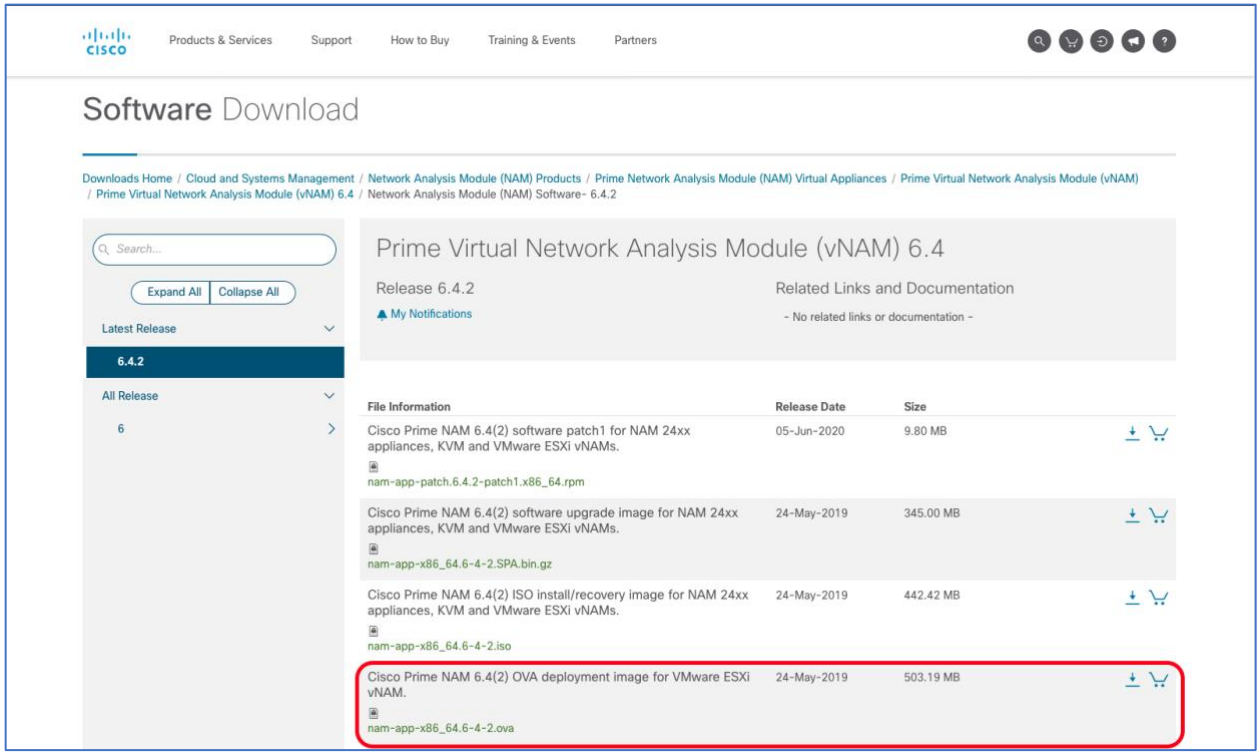


Figure 35. Location of vNAM 6.4.2 OVA File

© 2020 Cisco Systems, Inc. All rights reserved.

Step 2: Configure vNAM to Establish Communication with Cisco DNA Center

1. *Log into the vNAM console through ESXi and login with the default credentials root/root.*

2. *Run the following command to determine if any data ports have been assigned an IP address:*
    1. ***show data-port ip-addresses***

3. *If no port/address pairs are displayed, then assign an IP address to data-port 1 by running the command:*
    1. ***data-port 1 ip-address <IP to Assign to vNAM >***
    2. *Note: Record the IP address as it will be used in the DNAC configuration steps.*

4. *Set up the database export function by issuing the command:*
    1. ***cdb-export collector 1 ip-address <IP of Cisco DNA Center>***

5. *Verify the change by issuing the following command:*
    1. ***show cdb-export 1***

6. *Run the following command to verify that autocreate-data-source is enabled for ERSPAN:*
    1. ***show autocreate-data-source***

7. *If ERSPAN autocreation is not enabled, then run the following command:*
    1. ***autocreate-data-source erspan***

8. *Run the following command to verify that the vNAM is configured to use an NTP server:*
    1. ***show time***

9. *If the NAM time is not synchronized with an NTP server, run the following commands:*
    1. ***time*** *(to enter the time subcommand menu)*
    2. ***sync ntp <name or IP address of NTP server>***

© 2020 Cisco Systems, Inc. All rights reserved.

Step 3: Configure Cisco DNA Center to Establish Communication with vNAM

10. *Navigate to the **GRPC-COLLECTOR** page by opening up the hamburger menu, clicking on **System** then **Data Platform** (**Figure 36.**).*

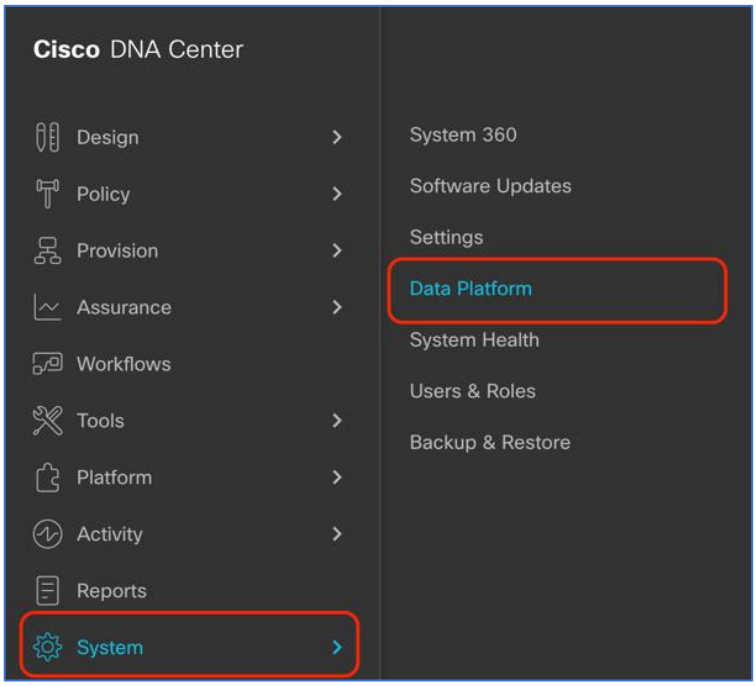


Figure 36. Location of Data Platform Within the Hamburger Menu

11. *Click on **Collector** then scroll down and click on **GRPC-COLLECTOR** (**Figure 37.**).*

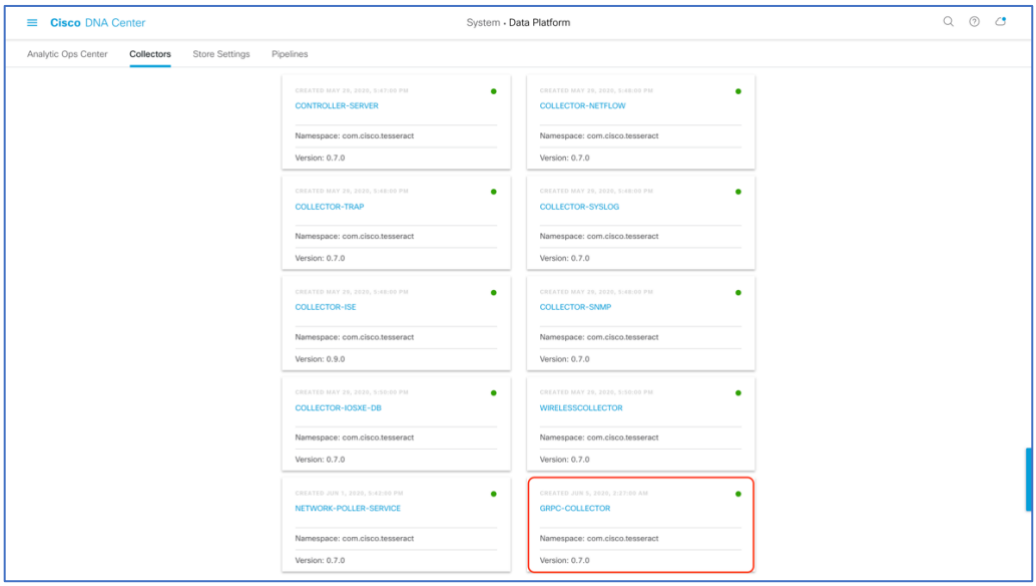


Figure 37. GRPC-COLLECTOR Button Within Data Platform

© 2020 Cisco Systems, Inc. All rights reserved.

12. *Click on **Add** then fill in the following information (**Figure 38.**):*
    1. *Click on the **DNA Agent Export** Check box.*
    2. *Enter in the vNAM IP within **DNA Agent IP Address**.*
    3. *Provide any unique name under **Configuration Name**.*
    4. *Click on **Save Configuration**.*

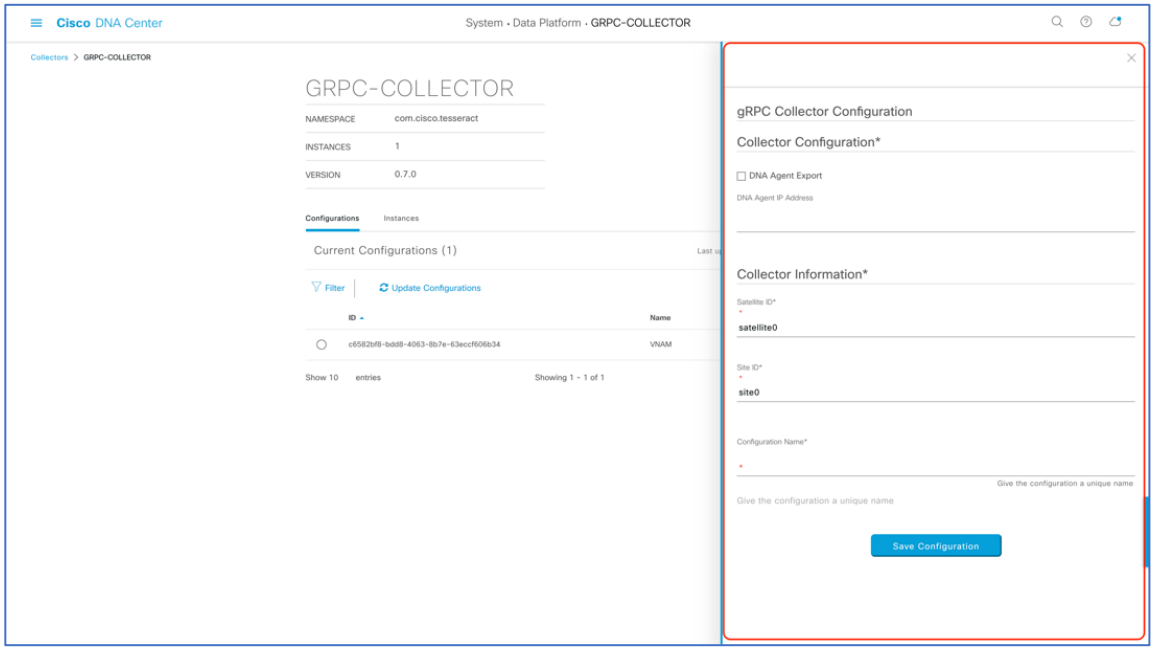


Figure 38. Credentials Required to Connect vNAM with Cisco DNA Center

13. *Ensure the GRPC Collector has been save and the entry is listed (**Figure 39.**).*

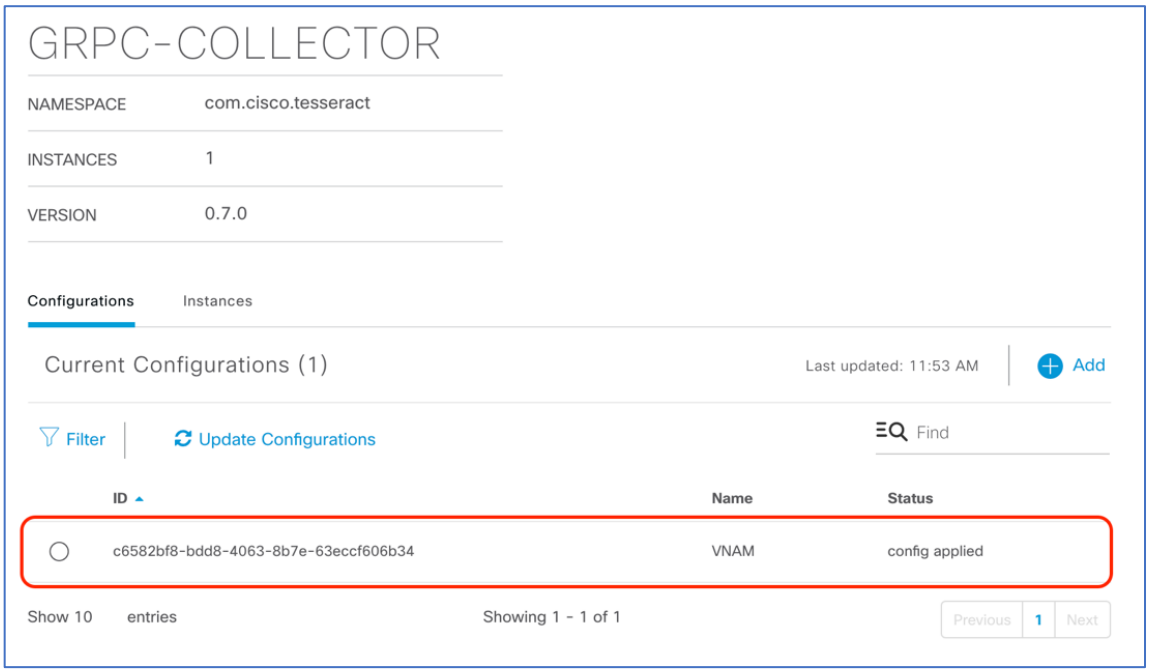


Figure 39. GRPC Collector Entry Created

© 2020 Cisco Systems, Inc. All rights reserved.

Note:

- Only one GRPC-COLLECTOR configuration should be added. If more than one is added, only the last added configuration will be used.

- Once the **DNA Agent Export** box has been checked, NAM integration is enabled for any client with full packet capture enabled which will be discussed in a later section.

© 2020 Cisco Systems, Inc. All rights reserved.

Day 1 - Intelligent Capture Features and Use Cases

The purpose of the following sub sections is to provide users with step by step instructions with regards to enabling each of the Intelligent Capture feature from first the AP perspective then to the client perspective. The section will also provide users with a deep understanding of each of the use cases and the details for how they are used to troubleshoot and issue.

Intelligent Capture feature names on Cisco DNA Center slightly differs from the names on the device side. When you enable certain features from Cisco DNA Center, multiple features are actually being enabled from the device side.

Intelligent Capture Feature Enablement Mapping – Device Side to Cisco DNA Center	
Cisco DNA Center Feature Name	**WLC & AP Side Feature Name**
Data Packet Capture	Full Packet Capture
Live Capture	Partial Packet Capture Client Filtered Stats
AP Stats Capture	AP WLAN Statistics AP Radio Statistics Client Statistics
Anomaly Stats Capture	Anomaly Detection Anomaly Packet Capture Anomaly Individual Reports Anomaly Summary Reports
Spectrum Analysis	Spectrum Analysis

Table 7. This table will depict the device side features (right) that are enabled when you enable a feature from the Cisco DNA Center side (left).

Day 1 Access Point Intelligent Capture

Description: Intelligent Capture for the access point offers two main features, (1) Always-On Real-Time RF monitoring and (2) On-Demand Spectrum Analysis.

Section: To enable and view Intelligent Capture data for AP RF Statistics and Spectrum Analysis.

Step 1: Enabling AP Stats Capture

When AP Stats Capture is enabled, Cisco DNA Center is actually enabling two feature, AP RF Stats and Client RF Stats.

1. *Navigate to the **Intelligent Capture Settings** page by opening the hamburger menu, then clicking on **Assurance** then **Intelligent Capture Settings** (**Figure 40.**).*

© 2020 Cisco Systems, Inc. All rights reserved.

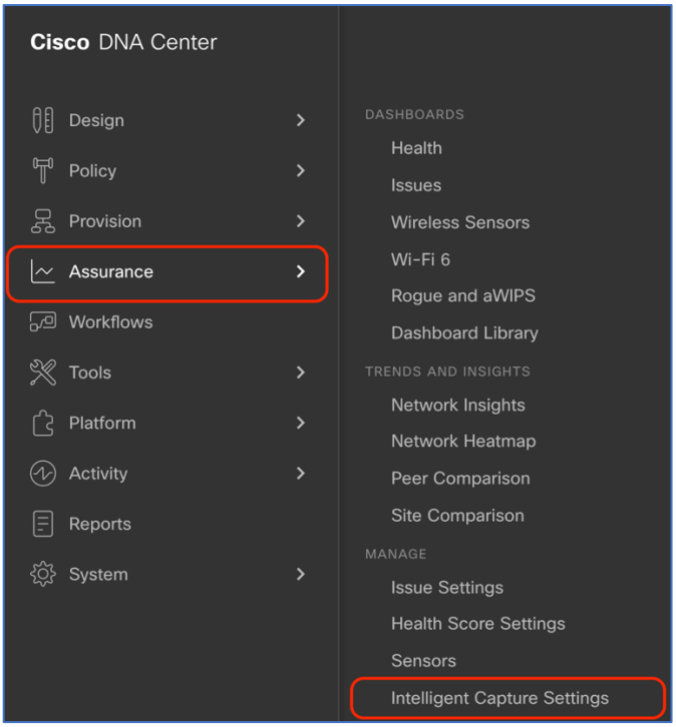


Figure 40. Location of Intelligent Capture Settings on the Hamburger Menu

1. ***Option 1 Enable Specific APs Only*** *- Click on* ***Access Point****, then click on* ***Specific – select specific APs and enable*** *to select individual APs from your site, then click on* ***Enable*** *to enable Intelligent Capture (****Figure 41.****).*

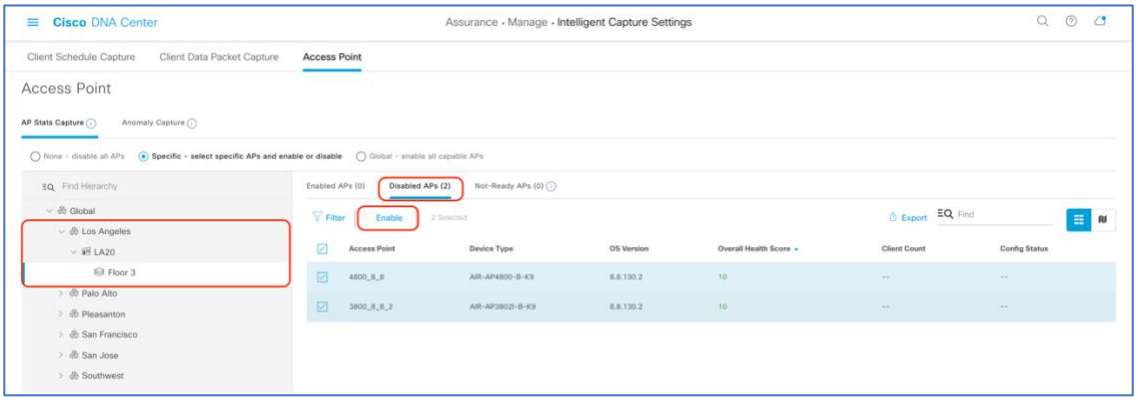


Figure 41. Selecting and Enabling APs from the Specific – select specific APs and enable Section

© 2020 Cisco Systems, Inc. All rights reserved.

2. *Ensure the APs move from the **Disabled APs Column** to the **Enabled APs** column (**Figure 42.**).*
   - Note: The blue dot next to the AP symbolizes that the device was just newly discovered.

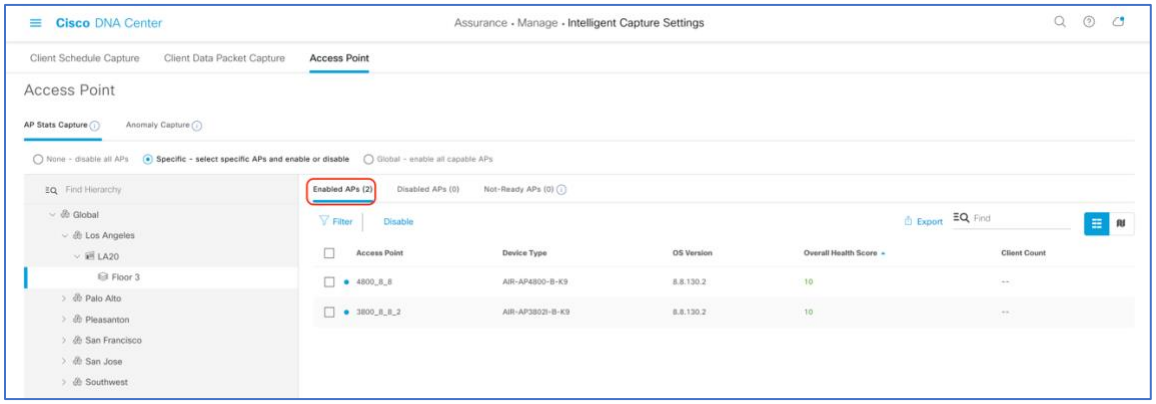


Figure 42. AP Stats Intelligent Capture is Enabled at a Specific AP Level

3. *Option 2 Enable All APs – Click on **Global – all capable APs are enabled** to enable Intelligent Capture on APs on this Cisco DNA Center Cluster then ensure the page changes to show **Globally Enabled** (**Figure 43.**).*

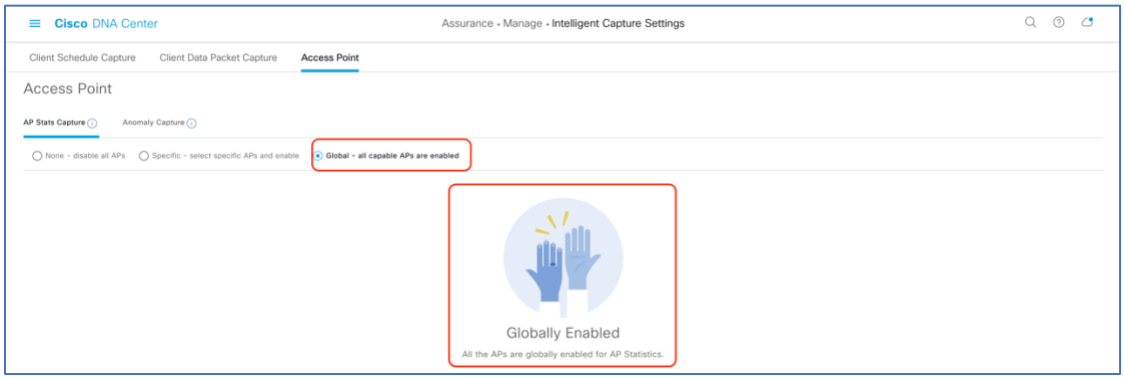


Figure 43. AP Stats Intelligent Capture is Enabled at a Global Level

Note:

- When AP Stats Capture is being enabled, there will be a loading bar indicating the estimated time it will take for the configuration to complete (**Figure 44.**).

- Cisco DNA Center can support up to enabling 1000 APs for AP Stats Capture.

- The user can leave this screen during this time without it affecting the configuration.

© 2020 Cisco Systems, Inc. All rights reserved.

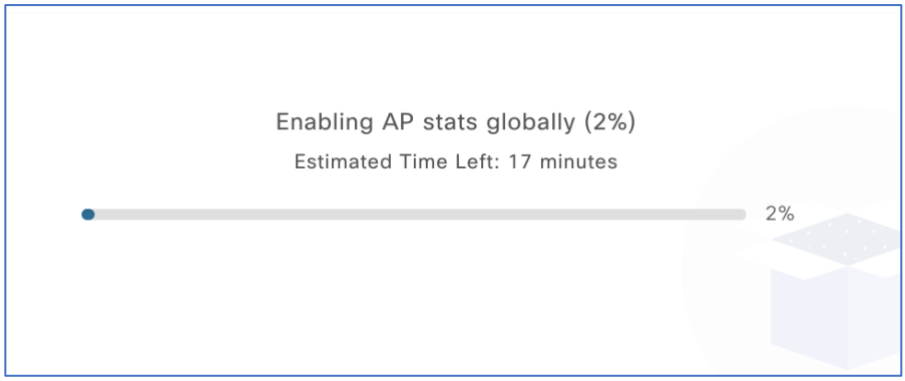


Figure 44. Loading Bar Indicating the Time It'll Take to Push the Intelligent Capture Configuration to WLC

Step 2: Navigate to the Intelligent Capture AP Page

1. **Option 1 Inventory Page** - Navigate to the Intelligent Capture AP **RF Statistics** Page by Clicking on the three dots next your selected AP within the inventory, clicking on **View 360** (**Figure 45.**).

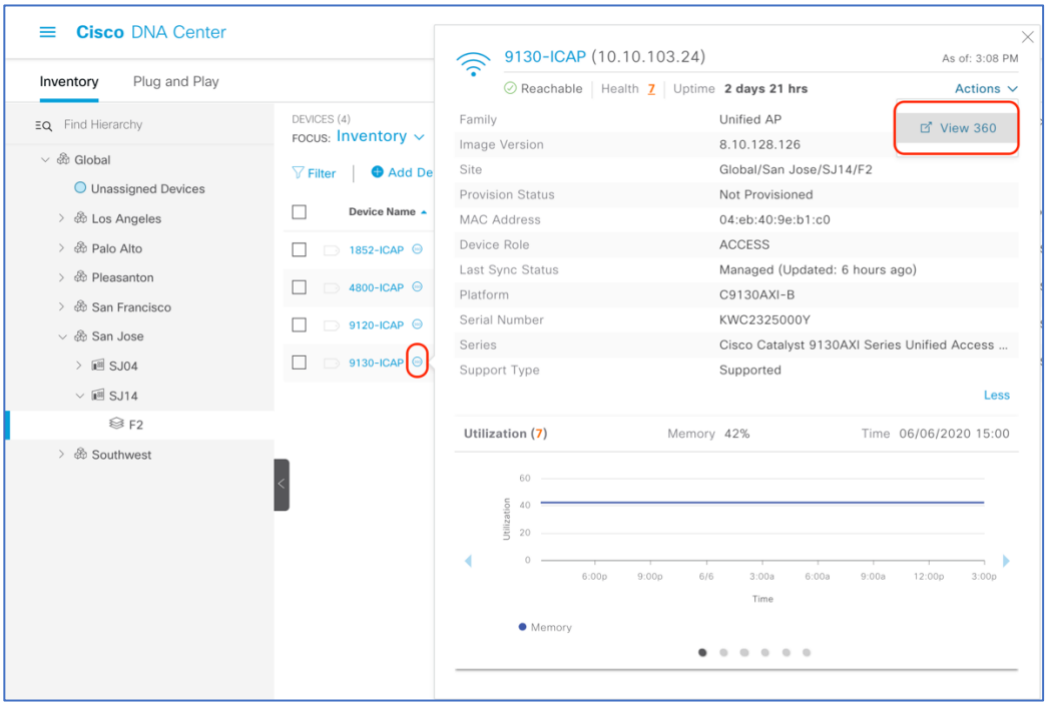


Figure 45. How to Enter Access Point Device 360 Page from Inventory

© 2020 Cisco Systems, Inc. All rights reserved.

2. ***Option 2 Network Health Page*** *– Navigate to the Network Heath Page by opening the hamburger menu at the top right-hand corner of the page, clicking on* ***Assurance*** *then* ***Health****, then* ***Network****, then Scrolling down to the* ***Network Devices table*** *at the bottom and click on an AP you want to view (****Figure 46.****).*

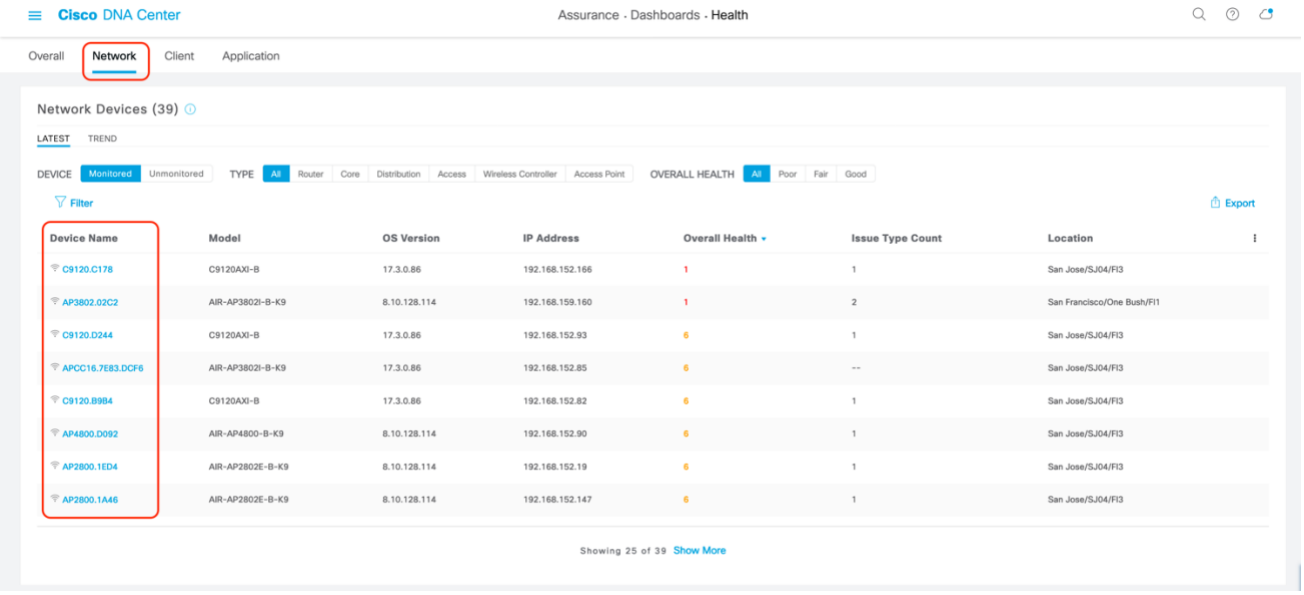


Figure 46. Navigate to the AP 360 Page through the Network Health Page

3. Click on the **Intelligent Capture** button to enter the AP **RF Statistics** Page (**Figure 47.**).

Figure 47. Intelligent Capture Button on AP Device 360 Page

© 2020 Cisco Systems, Inc. All rights reserved.

Step 3: Viewing the Intelligent Capture AP RF Statistics Page

Description: The AP RF Statistics page provides users will an in-depth analytical view of the various Radio and WLAN related wireless metrics regarding an AP's radio.

Purpose: To provide a trend view of the historical wireless metrics of an AP's radio that will give user insight into why users may be experiencing wireless problems such as poor signal, onboarding issues, throughput issues, etc.

Note: The AP RF Statistics page is displayed per serving radio. By default, when you enter this page, you will show up on radio 0. If you click on the menu (**Figure 48.**), you will have an option to view the AP RF Statistics for any of the AP's serving radios.

AP RF Stats Feature Description	
Trend Chart Name	**Description**
Clients	Client Count Trend.
Top Clients with Tx Failed Packets by SSID	Tx Packet Error Count Per Client Categorized by SSID Broadcasted by the AP.
Channel Utilization	Channel utilization % trend categorized by: 1. This AP (Tx + Rx) – This AP's Channel Utilization %. 2. Other Wi-Fi – Nearby AP's Channel Utilization %. 3. Non-Wi-Fi – Any non-Wi-Fi RF.
Channel Utilization by this Radio	Real time view of This AP (Tx + Rx) by client and packet count per broadcasted SSID.
Tx Frame Count per Type	Data & Management Frames Trend.
Total Frame Error over the air	Rx & Tx Frame Count from all its neighbors from the same channel.
Tx Power and Noise Floor	AP Radio's Tx Power Setting & Surrounding Noise Floor Trend.
Multicast/Broadcast Counter	Multicast & Broadcast Counter Trend.

Table 8. Description of Each Trend Chart within Figure 48 & 49.

© 2020 Cisco Systems, Inc. All rights reserved.

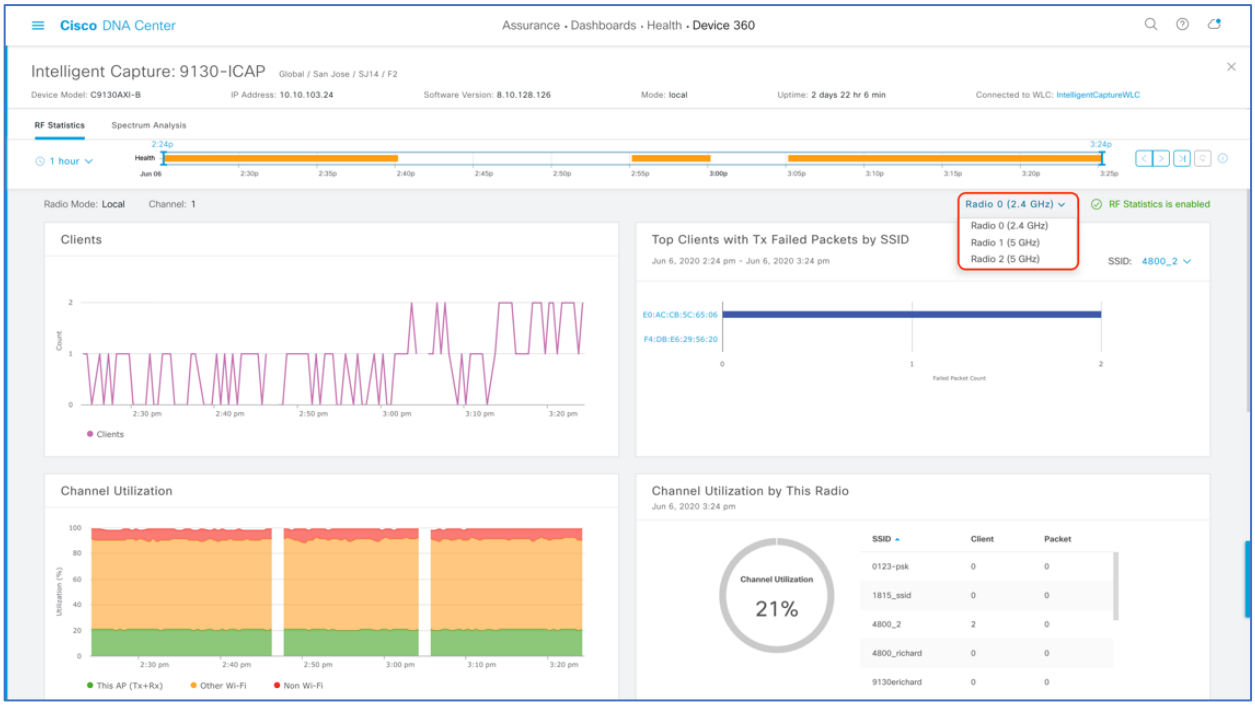


Figure 48. Top Half of AP RF Stats Page

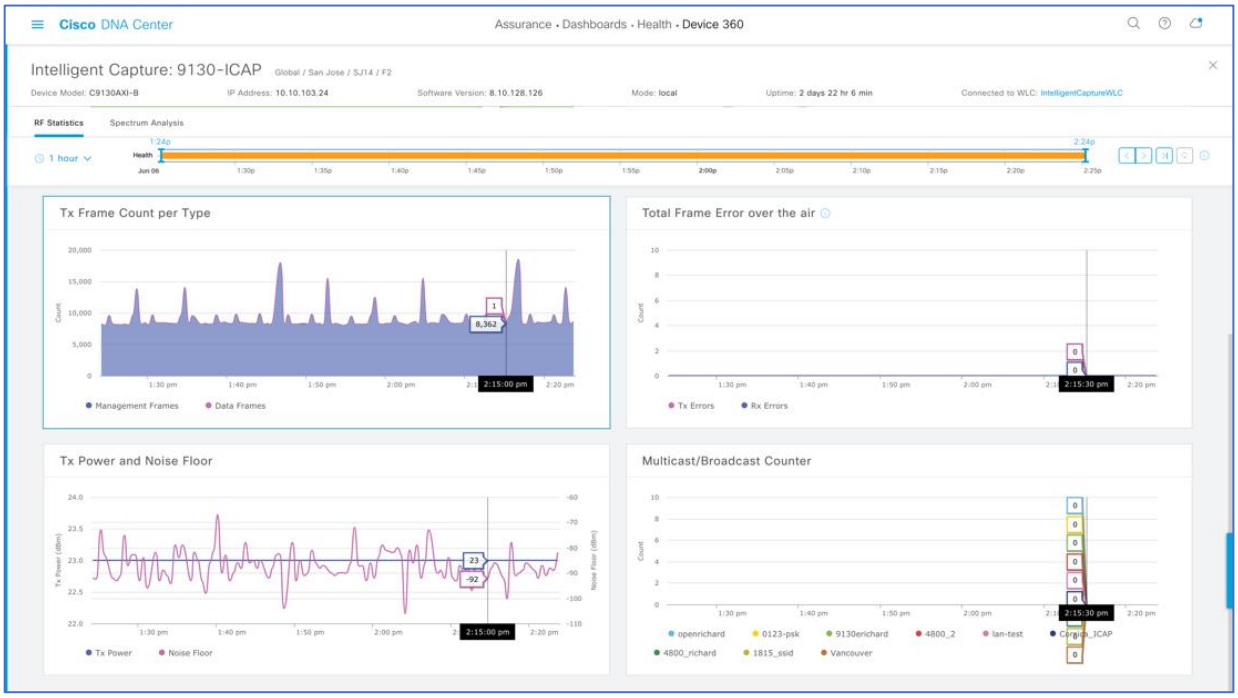


Figure 49. Bottom Half of AP RF Stats Page

© 2020 Cisco Systems, Inc. All rights reserved.

1. *To zoom into a particular widget, drag your cursor across a trend chart (**Figure 50.**)*

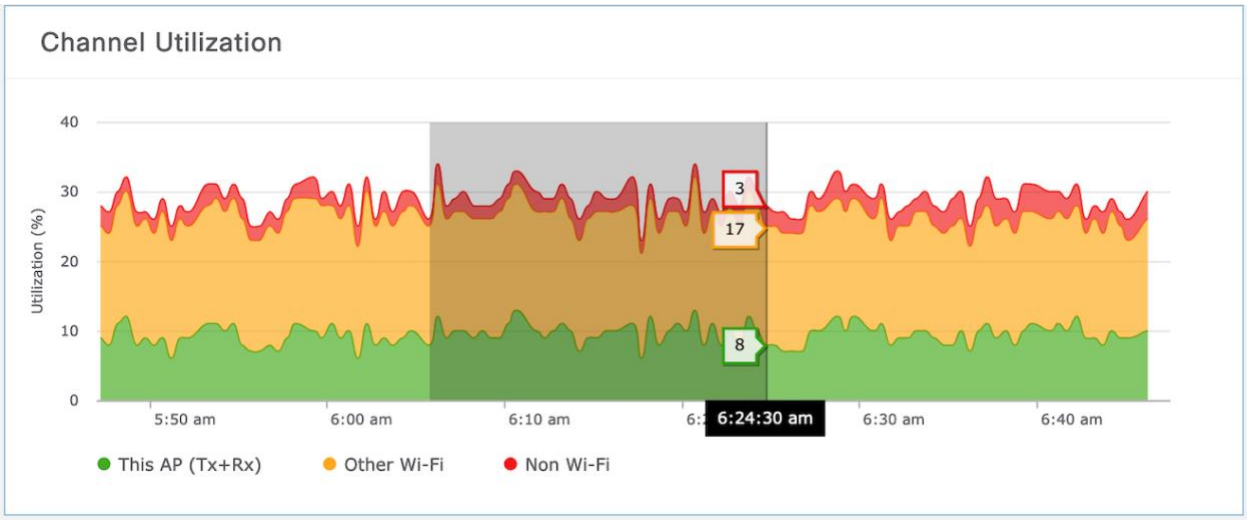


Figure 50. Zooming into an AP RF Stats Trend Chart for the 5GHz Radio.

2. The network time travel bar at the top allows a user to do the following:
   a. View Intelligent Capture data for up to 14 days in the past.
      - *Click on either the clock to select a data & time in the past to view (on the left), or click on the left or right arrow on the right. (**Figure 51.**)*
      - Note: The left or right arrow network time travel toggle will by default move the time backwards or forward by one hour.

   b. Change the time width for each of the trend widgets.
      - *Click on the drop-down menu on the left, which defaults at 1 hour, but can be toggled to 3 or 7 hours. (**Figure 51.**)*
      - Note: The amount of time the left and right arrow described above will travel is based on this time width configured.

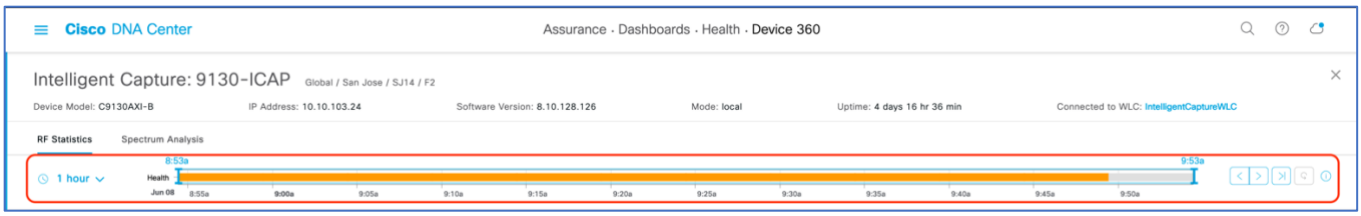


Figure 51. AP RF Statistics Network Time Travel Feature.

© 2020 Cisco Systems, Inc. All rights reserved.

Step 4: Navigating to and Enabling Spectrum Analysis

1. *Navigate to the Spectrum Analysis page by clicking on the **Spectrum Analysis** tab at the top of the AP **RF Statistics** Page (**Figure 52.**).*

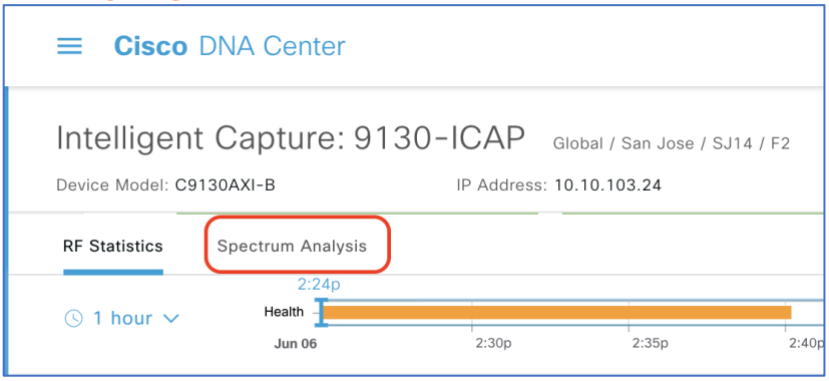


Figure 52. Location of Spectrum Analysis Tab on the AP RF Statistics Page.

2. *Click on **Start Spectrum Analysis** to Enable the feature on this AP (**Figure 53.**).*

Figure 53. Location of Start Spectrum Analysis Button.

© 2020 Cisco Systems, Inc. All rights reserved.

Step 5: Viewing Spectrum Analysis Data

Description: Spectrum Analysis provides users with insight into the Spectrum activities around their AP through three main view charts, (1) **Channel by Amplitude**, (2) **Channel by Time**, and (3) **Interference and Duty Cycle** (**Figures 54-58.**)

- **Channel by Amplitude:**
  - **Persistent FFT:** Shows the aggregated amplitude and frequency of the spectral energy observed over the past five mins (**Figure** 54.).
  - **Realtime FFT:** Shows only the most recent amplitude and frequency of the spectral energy observed (**Figure 55**).
  - **Note:** By default, displays RF activity in a persistent FFT manner but can be toggled to show it in a Realtime FFT manner at the top (**Figure 54.**).
  - **Color Interpretation:** The color in the charts represents the number of overlapping signals and can be interpreted by level of intensity with the color legend (**Figure 54.**).
    - Blue means low number of overlapping signals.
    - Red means high number of overlapping signals.
- **Channel by Time:**
  - This chart is also known as the swept spectrogram, and displays a waterfall view of the aggregated swept spectrogram data for last 5min (**Figure 54 & 56.**).
- **Interference and Duty Cycle:**
  - This chart uses the FFT Duty Cycle report from the AP's CleanAir Feature to show the duty cycles and surrounding interferences (**Figure 57 & 58.**).

Purpose: The purpose of Spectrum Analysis is to provide users with an insight as to what's going on in the RF surrounding their AP so they can better understand why wireless issues can be occurring to their clients.

Notes:

- The Spectrum Analysis chart shows data for the past five minutes.
- Starting from software release 8.10MR3 and 17.3.1, APs started to support buffered FFT, which means that the AP will store the last 30 seconds of spectrum analysis data in its ring buffer, then externalize burst spectrum analysis data to Cisco DNA Center to quickly populate the last 30 seconds of spectrum data.
- Spectrum Analysis is only supported on Aironet 2800/3800/4800 & Catalyst 9120/9130 series APs.
- When enabled, a configuration will be sent to the WLC to enable the CleanAir feature followed up by the feature itself.
- When enabled on the Aironet 4800 AP, by default, Cisco DNA Center will attempt to enable the feature on the AP's 3rd radio.
- If the 3rd radio is being used for other features such as Hyperlocation or Data Packet Capture, it will resort to enabling the features on serving radios 0/1.

© 2020 Cisco Systems, Inc. All rights reserved.

- With the feature enabled on the 3rd radio, you will be able to view all RF activity on all channels for both 2.4 & 5 GHz band. When enabled on radio 0/1, you will only be able to view RF activity for the channels the AP's radios are currently serving.
- When enabled on the Catalyst 9120 and 9130 APs, Spectrum Analysis is enabled on the RF ASIC analytics radio.

1. The Spectrum Analysis Page is displayed per band (2.4GHz & 5GHz) and can be toggled via the menu shown at the top (**Figure 54.**).

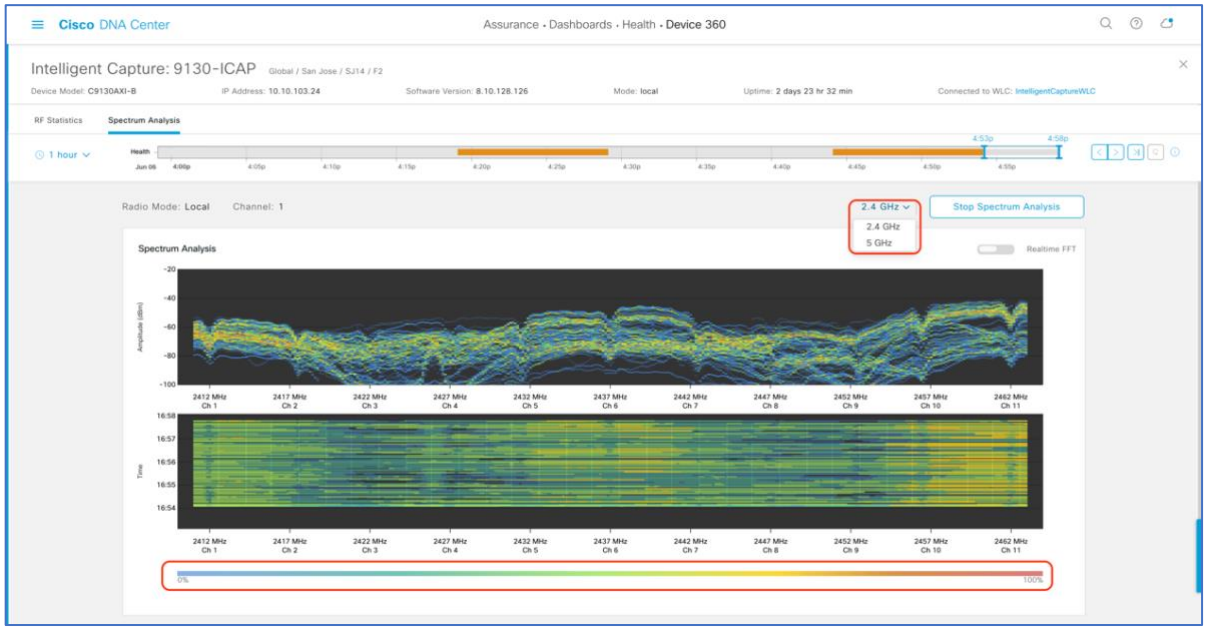


Figure 54. 2.4GHz Spectrum Analysis with Persistent FFT Enabled

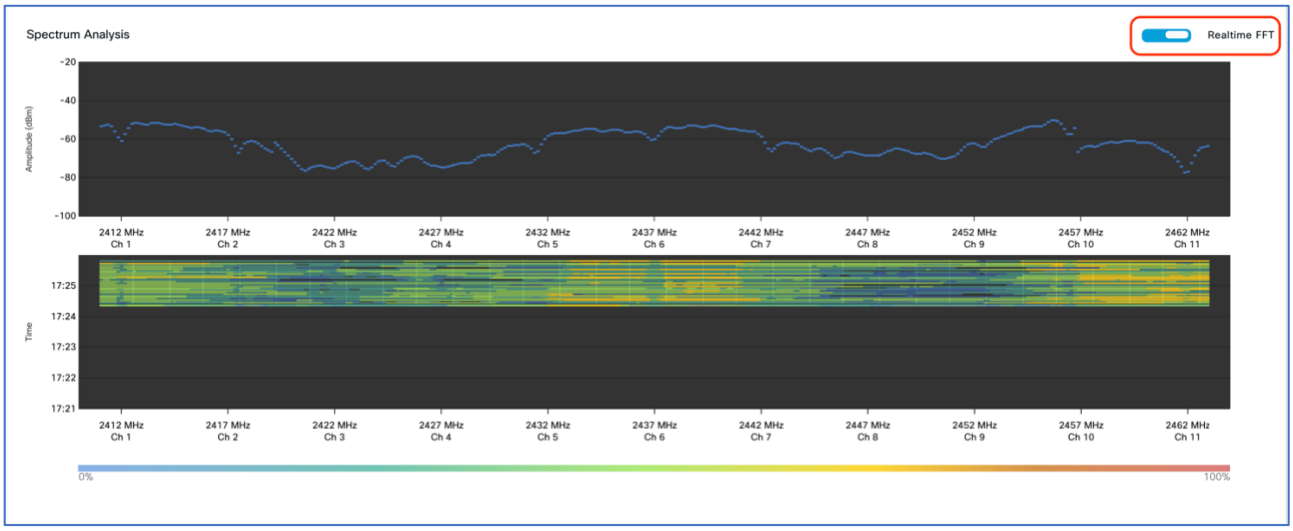


Figure 55. 2.4GHz Spectrum Analysis with Real Time FFT Enabled

© 2020 Cisco Systems, Inc. All rights reserved.

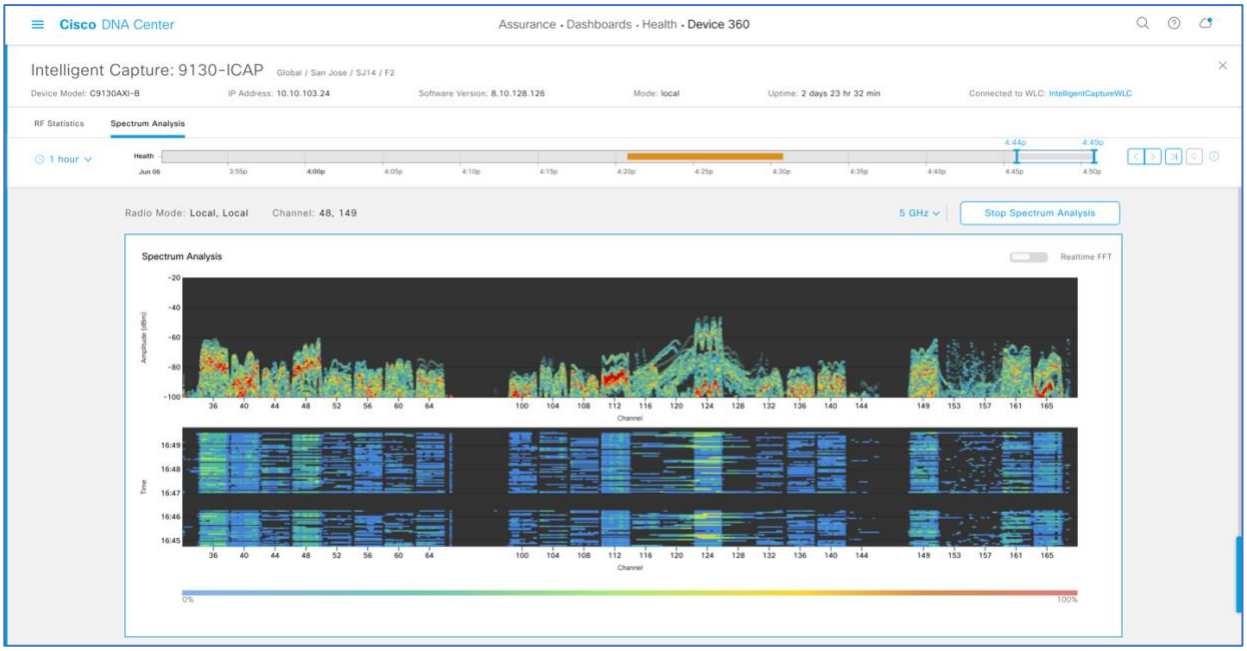


Figure 56. 5GHz Spectrum Analysis with Persistent FFT Enabled

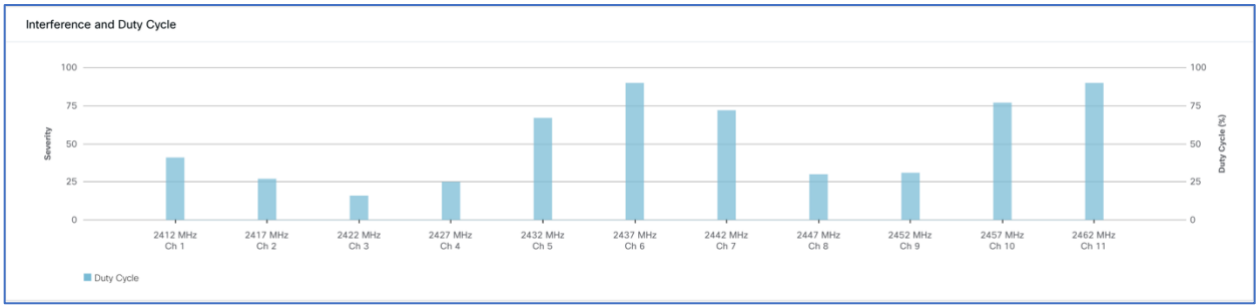


Figure 57. 2.4GHz Interference and Duty Cycle Chart

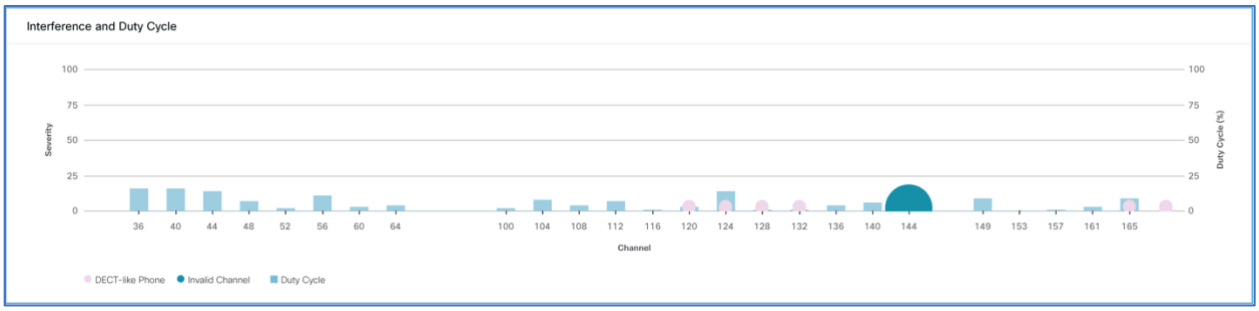


Figure 58. 5GHz Interference and Duty Cycle Chart

© 2020 Cisco Systems, Inc. All rights reserved.

2. *To zoom into the Spectrum Analysis charts, drag your cursor across the chart (**Figure 59.**)*

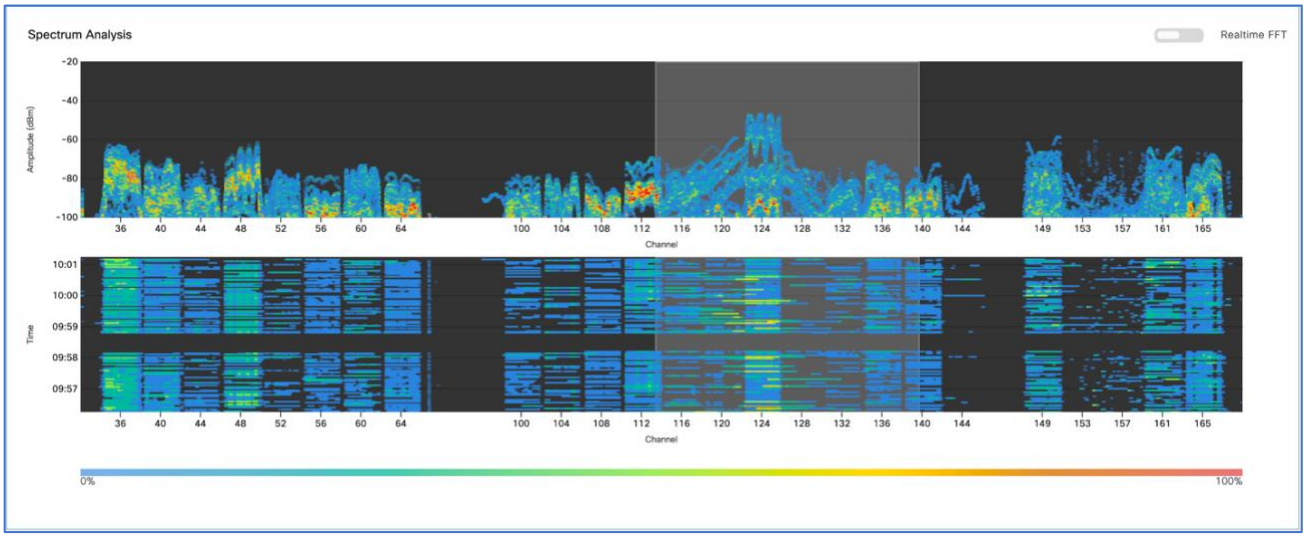


Figure 59. Zooming into the Spectrum Analysis Charts

3. The network time travel bar at the top allows a user to do the following:
    1. View Intelligent Capture data for up to 14 days in the past.
        - *Click on either the clock to select a data & time in the past to view (on the left), or click on the left or right arrow on the right. (**Figure 60.**)*
        - Note: The left or right arrow network time travel toggle will by default move the time backwards or forward by one hour.
    2. Change the time width for each of the trend widgets.
        - *Click on the drop-down menu on the left, which defaults at 1 hour, but can be toggled to 3 or 7 hours. (**Figure 60.**)*
        - Note: The amount of time the left and right arrow described above will travel is based on this time width configured.

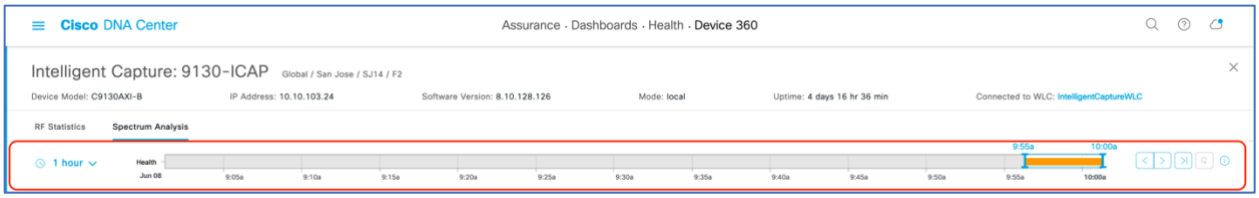


Figure 60. Spectrum Analysis Network Time Travel Feature.

© 2020 Cisco Systems, Inc. All rights reserved.

Day 1 Client Intelligent Capture

Description: Intelligent Capture for the client offers two main features, (1) Data Packet Capture (2) Live Capture, (3) Anomaly Detection and Packet Capture, (4) Client RF Stats.

Section: To enable and view all Intelligent Capture client-side data.

Step 1: Navigate to Intelligent Capture Client Page

1. **Option 1 Hamburger Menu** - Open the hamburger menu, click on Assurance then Health (Figure 61.).

2. Click on the Client tab to navigate to client health (**Figure 62.**).

3. Scroll down to the Client Devices table and click on the client you want to view (**Figure 62.**).

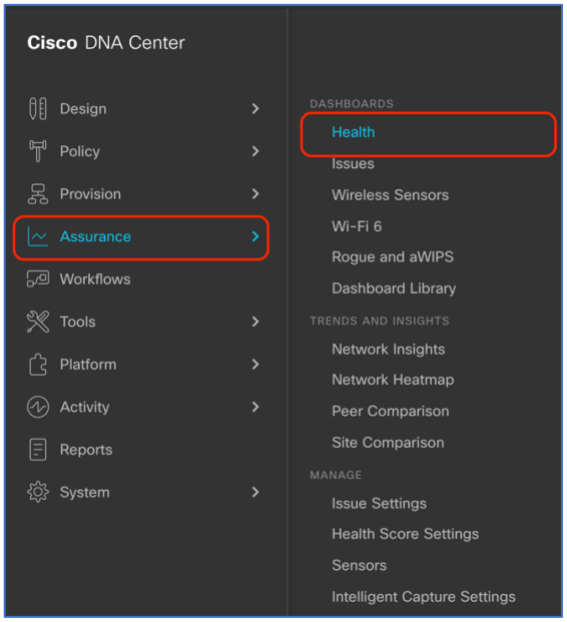


Figure 61. Location of Health in the Hamburger Menu.

© 2020 Cisco Systems, Inc. All rights reserved.

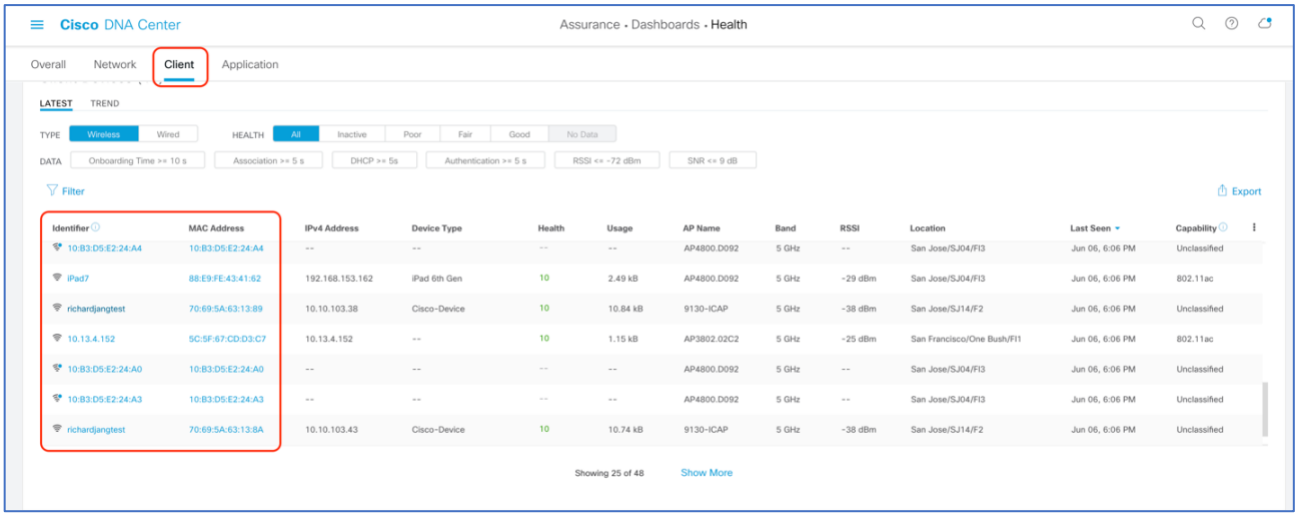


Figure 62. Location of the Client Device Table on the Client Health Page

4. ***Option 2 Search*** *– Click on the magnifying glass at the top right-hand corner of any page.*
    1. *Enter in either the client mac address, IP address, the username the client used to join a 802.1x network (**Figure 63.**).*

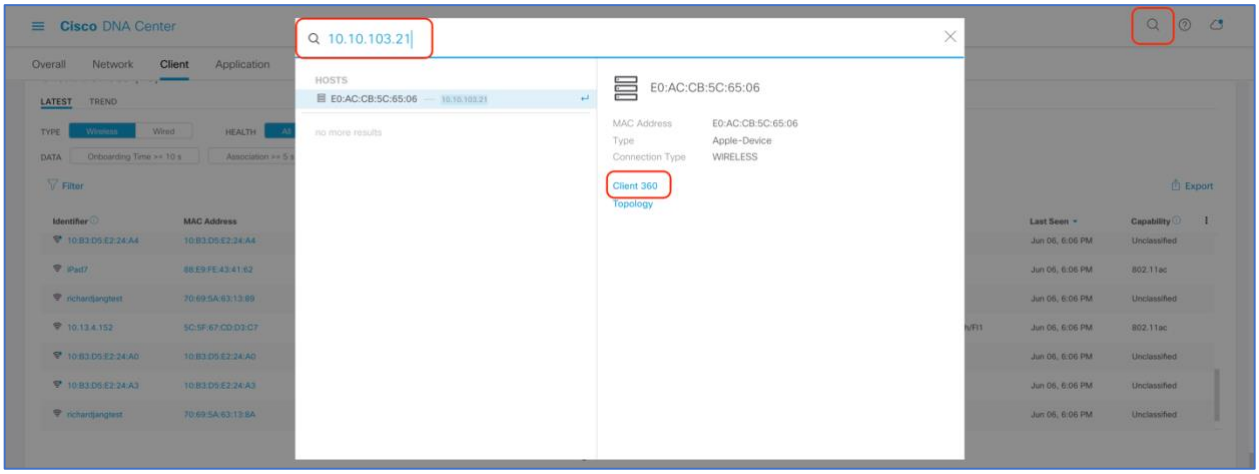


Figure 63. Entering the client 360 page via the search functionality

5. *On the top right-hand side of the screen, click on the **Intelligent Capture** button to enter the Intelligent Capture client page (**Figure 64.**).*

Figure 64. Location of the Intelligent Capture button on the Client 360 Page.

© 2020 Cisco Systems, Inc. All rights reserved.

6. At this point, you will have arrived at the Intelligent Capture Client Page (**Figure 65.**).

Figure 65. Intelligent Capture Client Page

Step 2: Enabling and Viewing Data Packet Capture Data

Description: Enabling Data Packet Capture will allow supported Access Points (Aironet 4800 & Catalyst 9130) to capture both the data and management packets of a single client and send this data to Cisco DNA Center in an unencrypted manner.

Purpose: The purpose of this feature is to provide a packet level insight into any issue such as onboarding or throughput. The ability to view packets in an unencrypted form provides users with the ability to understand the issue at hand on a level that was not possible in debugging prior to Intelligent Capture.

Note:

- Only a single client can be targeted by Data Packet Capture at once on an entire Cisco DNA Center cluster.
- Packet capture files will be stored at a size of up to 100MB before a new file is created.
- In the scenario that a client roams from one data packet capture supported AP to another, the Cisco DNA Center will stitch all the packet captures into one for the user to download.

1. *To enable data packet capture, click on **Run Data Packet Capture** at the top of the page (**Figure 64.**).*

2. *To view the packet captures sent from the AP, click on the **Download** button at the top of the page to open a menu of all previous data packet captures taken (**Figure 64.**).*

© 2020 Cisco Systems, Inc. All rights reserved.

3. *To download the packet capture file to your local computer, click on the down arrow beneath the **Download** column next to the packet capture you would like to download (**Figure 66.**).*

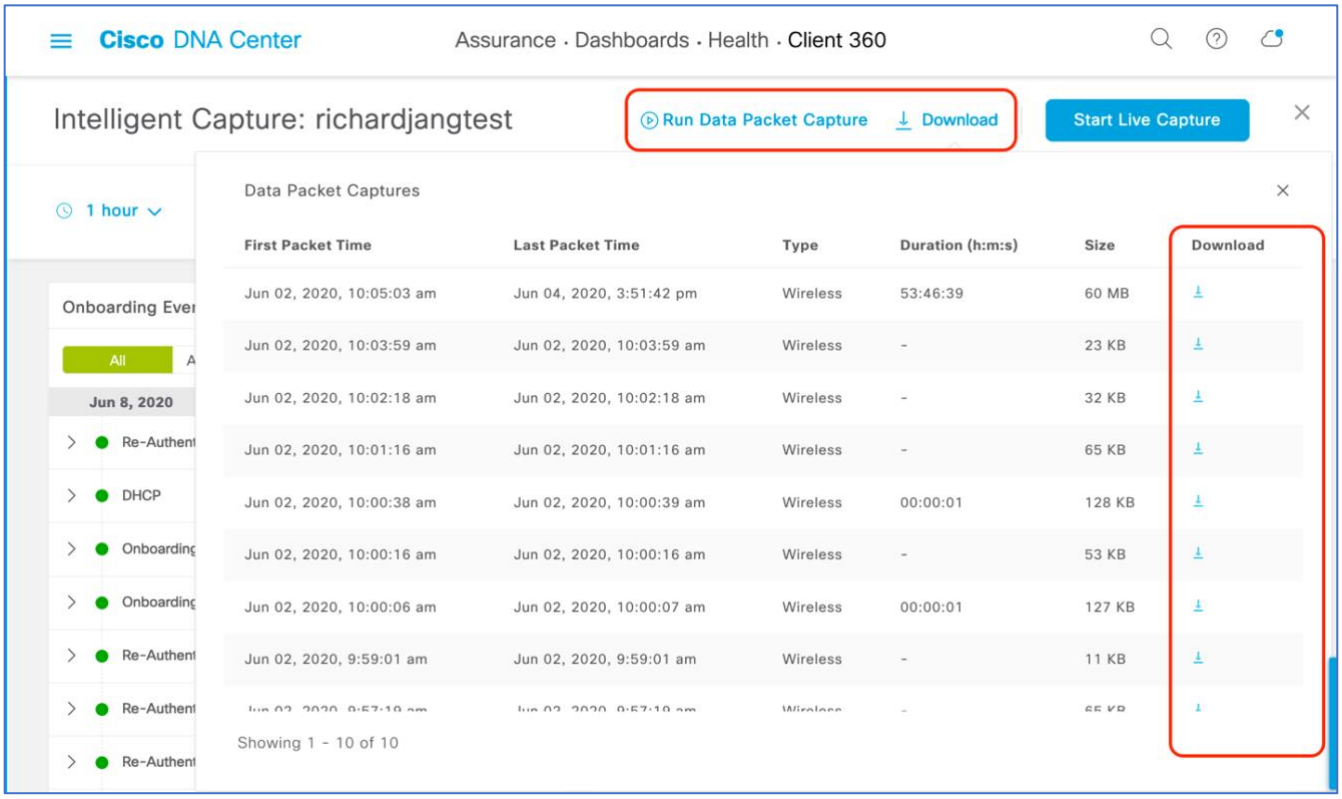


Figure 66. Enabling Data Packet Capture, and Download Packets Captured.

4. To view any ongoing or completed Data Packet Capture sessions, navigate to the Intelligent Capture Settings Page by opening the hamburger menu by clicking on **Assurance**, then **Intelligent Capture Settings** and you will arrive at the **Client Data Packet Capture** page (**Figure 67.**).

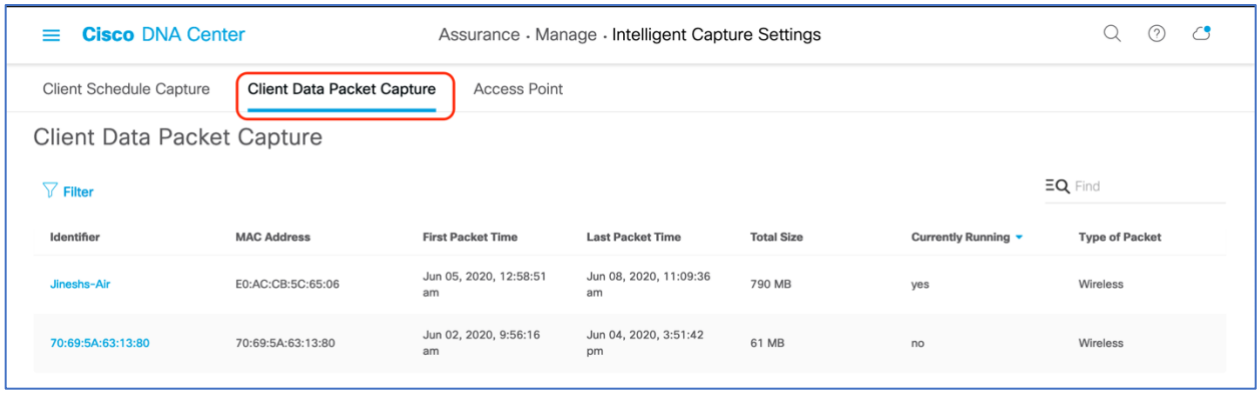


Figure 67. Viewing Ongoing or Completed Data Packet Capture Sessions.

© 2020 Cisco Systems, Inc. All rights reserved.

Step 3: Enabling and View Live Capture Data

Description: Enabling Live Capture will allow supported access points to send (1) onboarding packets and (2) client statistics data at a frequency of every 5 seconds as well as controllers to send onboarding events at a frequency of ever 2 second to Cisco DNA Center.

Purpose: The purpose of this feature is to target specific clients with onboarding issues to troubleshoot and have both the AP and WLCs dump as much relevant data about them as possible in live time for easy root cause analysis.

Notes:

- Live Capture can be enabled for up to 16 clients on the Cisco DNA Center at once.
- Live Capture will be enabled for 3 hours (unless manually stopped) once started.

1. *To enable Live Capture, click on **Start Live Capture** at the top of the page (**Figure 68.**).*

2. *To view the onboarding packets capture, look at the onboarding events viewer on the left of the page for events with a PCAP Symbol. Click on an event with this PCAP symbol to open up all details regarding this event, then scroll down to view the auto packet analyzer which to provide a graphical view of the onboarding packets captured (**Figure 68.**).*

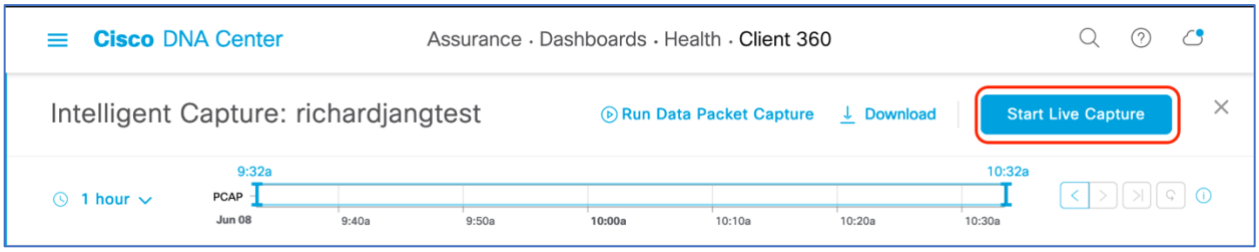


Figure 68. Enabling Live Capture.

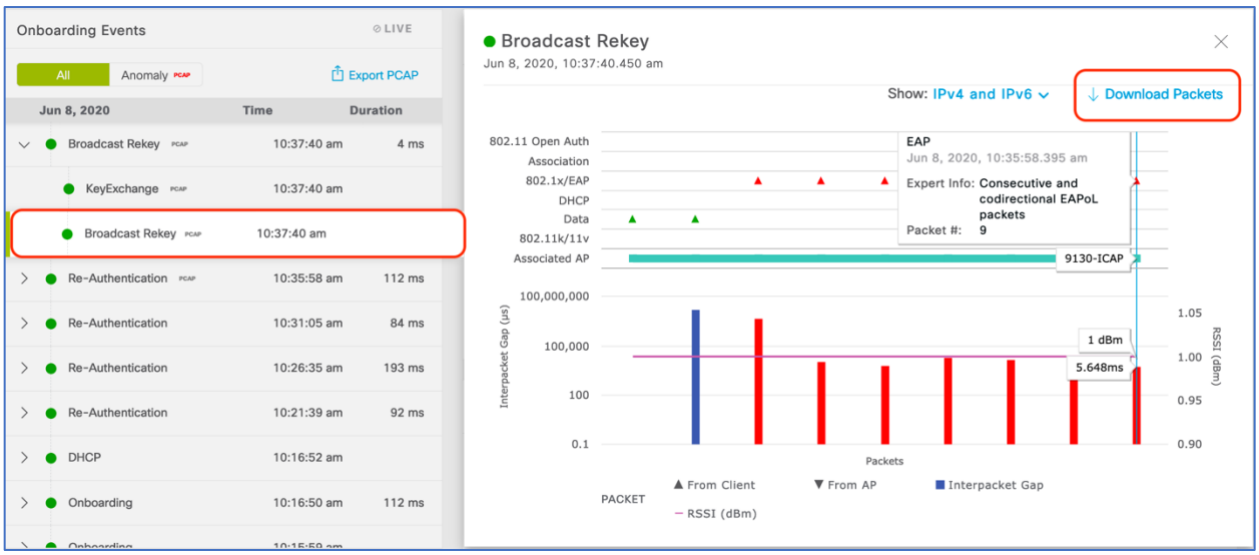


Figure 69. Onboarding Events Menu and Auto Packet Analyzer Depict Onboarding Packets

© 2020 Cisco Systems, Inc. All rights reserved.

Step 4: Scheduling a Live Capture Data

Description: This feature provides you the option to schedule a Live Capture described in step 3 above at a specific date & time for a specific duration (30 mins to 8 hours).

Purpose: If the Cisco DNA Center user knows of a reoccurring issue from a specific client that comes in at a specific time of day, this feature provides the ability to begin automatically capturing data on that client the moment they come into the proximity of the wireless network.

Note: You can schedule up to 12 scheduled Live Captures at once. As you recall, you can enable up to 16 live captures total, meaning that although you can only schedule 12 at once, you can manually enable the remaining 4 through the Intelligent Capture Client page.

1. *Navigate to the Intelligent Capture Settings Page by opening the hamburger menu by clicking on **Assurance**, then **Intelligent Capture Settings** and you will arrive at the **Client Schedule Capture** page (**Figure 70.**).*

2. *Click on **+ Schedule Client Capture** (**Figure 70.**).*

3. *Configure when you want to schedule a live capture, then provide either the User ID, Hostname, or MAC Address of the client you would like to capture and hit **Save** (**Figure 71.**).*

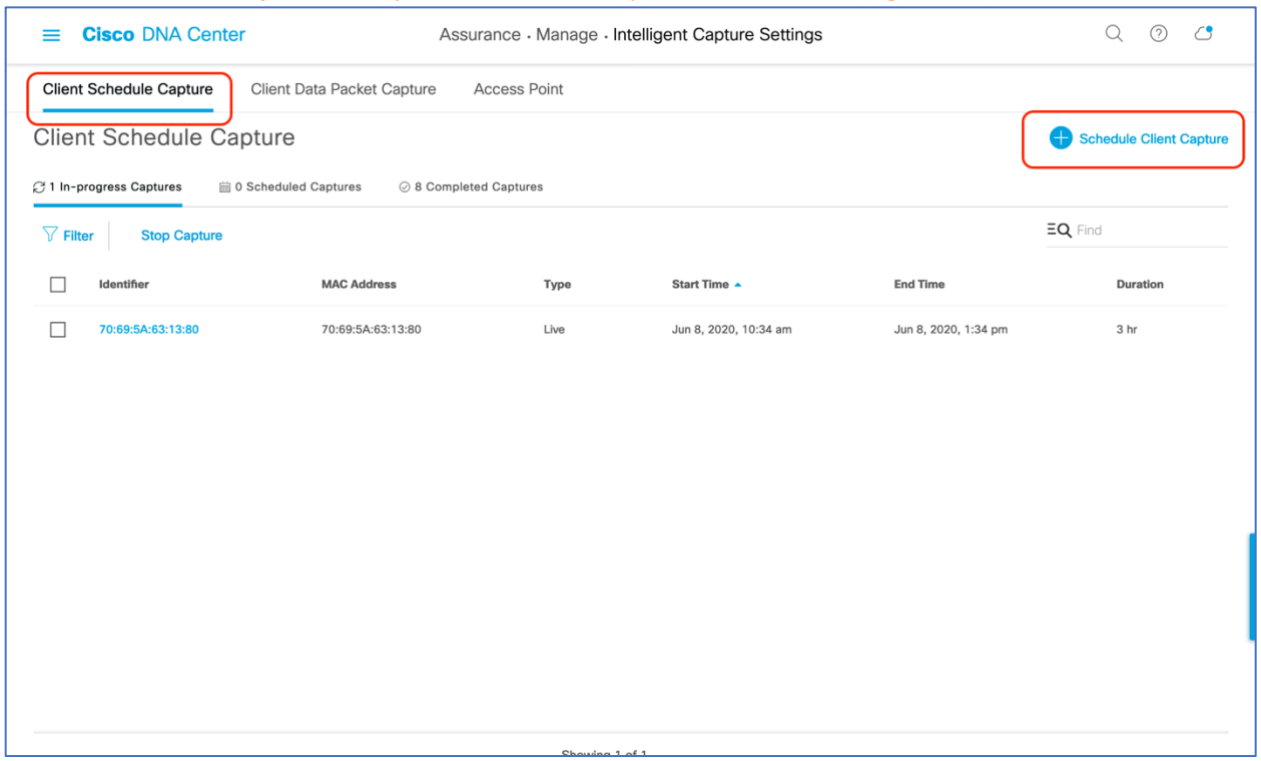


Figure 70. Scheduling a Live Capture on the Client Schedule Capture page.

© 2020 Cisco Systems, Inc. All rights reserved.

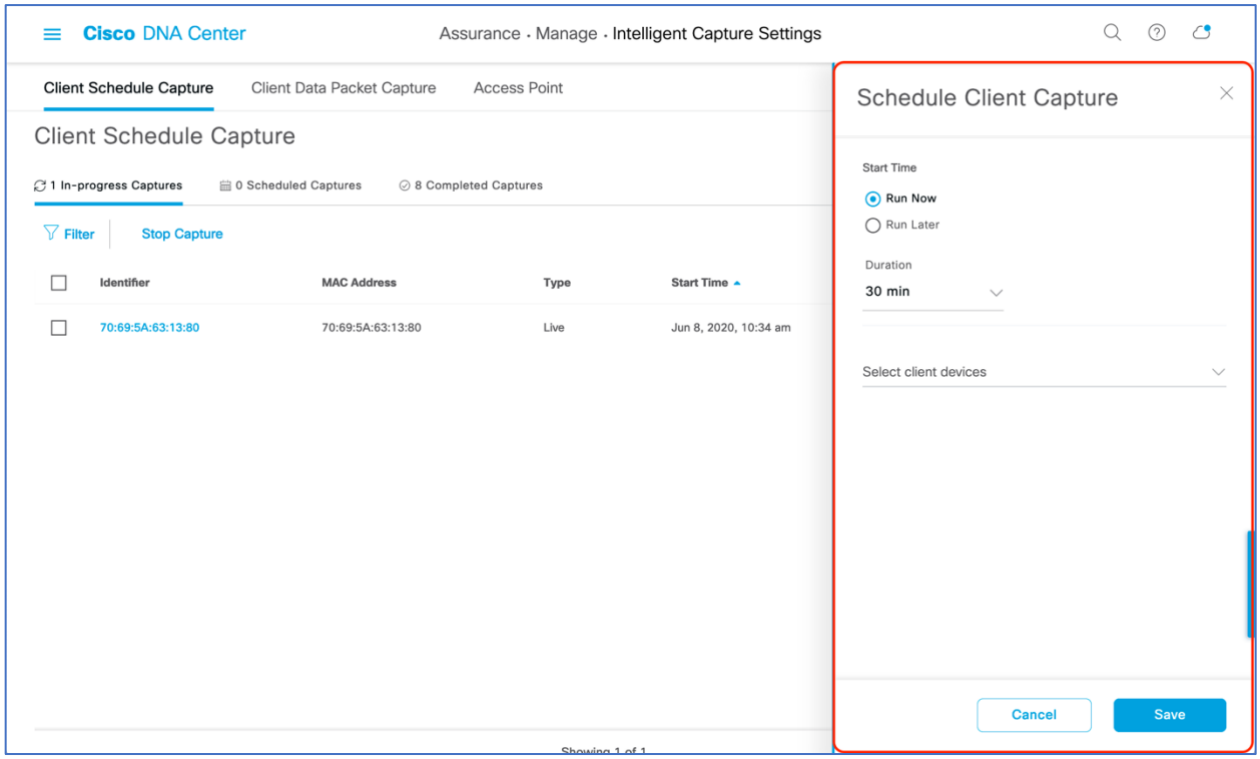


Figure 71. Schedule a Live Capture Menu

4. *To view the currently in progress scheduled or manually enabled live captures progress, click on In-Progress Captures (**Figure 72.**).*

5. *To view the live captures scheduled in the future, click on Schedule Captures (**Figure 72.**).*

6. *To view the scheduled or manually enabled live captures that have completed, click on Completed Captures (**Figure 72.**).*

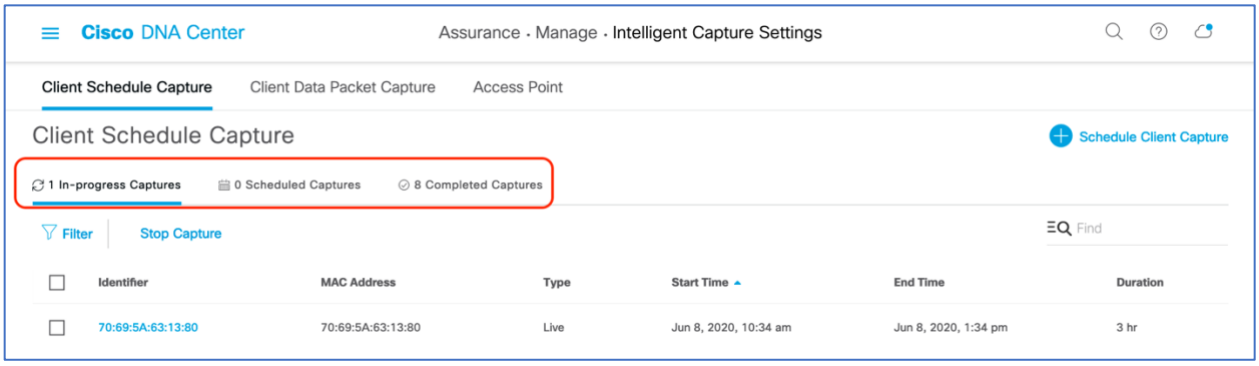


Figure 72. Viewing the various Live Capture Progresses

© 2020 Cisco Systems, Inc. All rights reserved.

Step 5: Viewing Client Statistics Data

Description: The Client RF Statistics Trend charts provide users with an in-depth analysis view regarding a client's connectivity to the wireless network.

Purpose: To provide a trend view of the historical wireless metrics of a client's connectivity to an AP that will give insight into why users may be experiencing wireless problems such as poor signal, onboarding issues, throughput issues, etc.

Client RF Stats Feature Description	
Trend Chart Category	**Description**
RSSI & SNR	Providing historical RSSI (dBm) and SNR (dB) insight per client.
Rx Average Data Rate & Rx Last Data Rate	Providing historical Rx Average Data Rate (bps) insight per client.
Tx Packets & Rx Packets	Providing historical Tx/Rx Packet Count insight per client.
Tx Packet Retry	Providing historical Tx Packet Retry insight per client.

Table 9. Description of Each Trend Chart within Figure 73.

1. To view current Client RF Stat data, scroll down on the Intelligent Capture Client Page (**Figure 73.**).

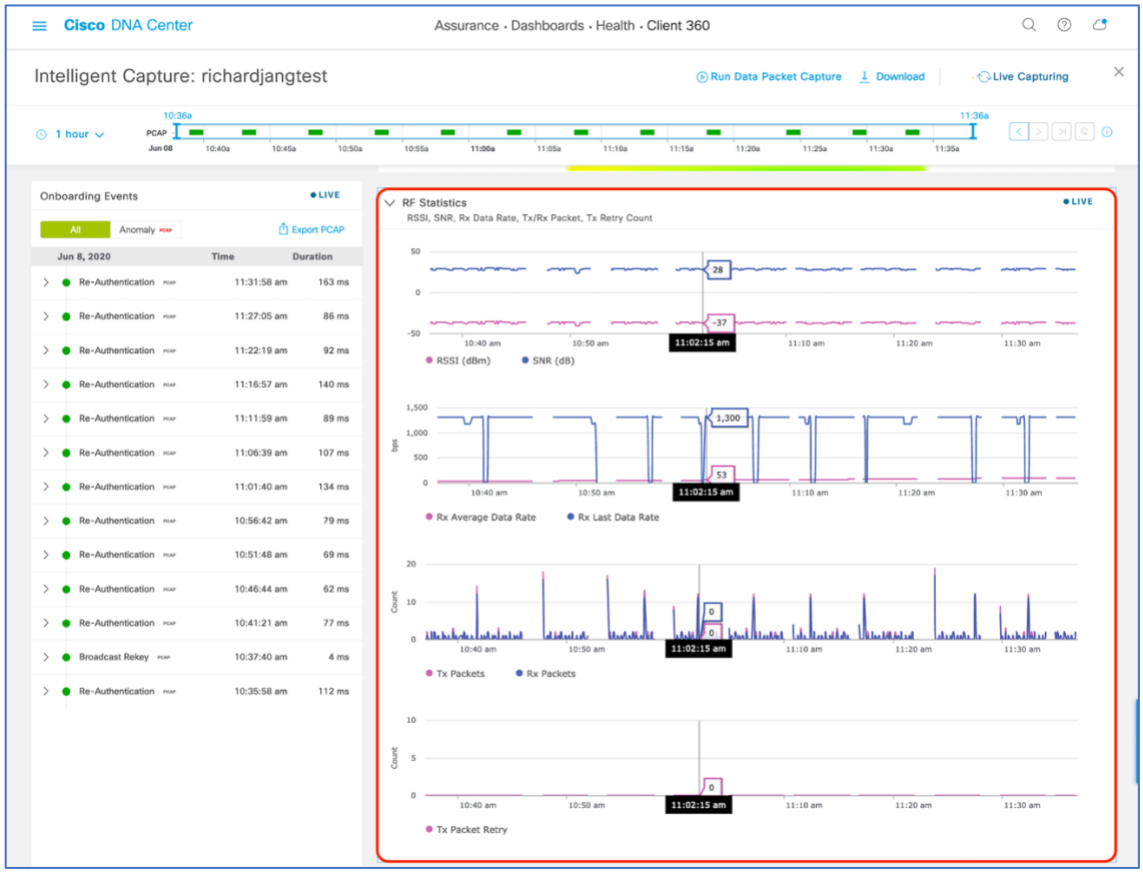


Figure 73. Location of Client RF Stats Charts.

© 2020 Cisco Systems, Inc. All rights reserved.

2. *To zoom into the Client RF Stats charts, drag your cursor across the chart (**Figure 74.**)*

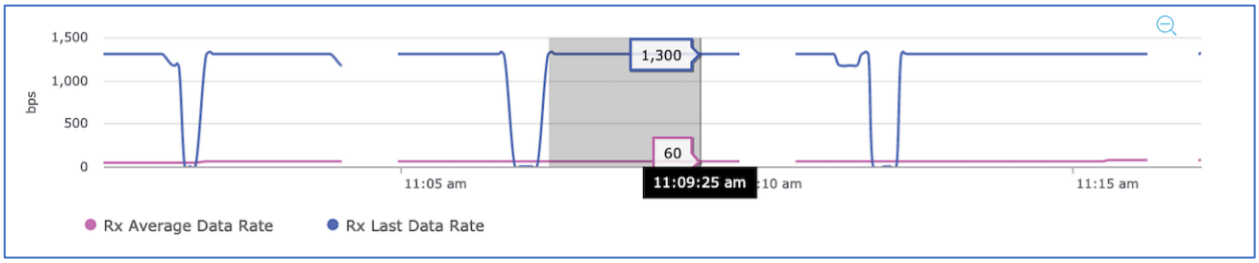


Figure 74. Zooming into the Client RF Stats Charts

3. The network time travel bar at the top allows a user to do the following:
   a. View Intelligent Capture data for up to 14 days in the past.
      - *Click on either the clock to select a data & time in the past to view (on the left), or click on the left or right arrow on the right. (**Figure 75.**)*
      - Note: The left or right arrow network time travel toggle will by default move the time backwards or forward by one hour.

   b. Change the time width for each of the trend widgets.
      - *Click on the drop-down menu on the left, which defaults at 1 hour, but can be toggled to 3 or 7 hours. (**Figure 75.**)*
      - Note: The amount of time the left and right arrow described above will travel is based on this time width configured.

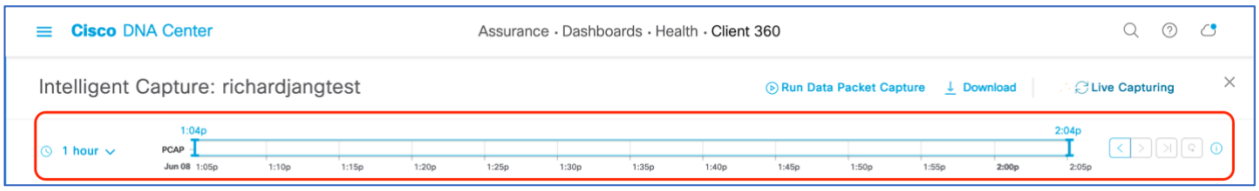


Figure 75. AP RF Statistics Network Time Travel Feature.

© 2020 Cisco Systems, Inc. All rights reserved.

Step 6: Enabling and Viewing Anomaly Stats Capture

Description: Anomaly Detection allows the WLC and APs to work together to detect client onboarding issues and send Cisco DNA Center both an Anomaly Event as well as packet captures depicting the issue that had occurred. The WLC's anomaly event will be the red onboarding event (signifying a failed event) that appears in the onboarding event viewer. The AP's anomaly event will be used to match the anomaly packets captured to the failed onboarding event the WLC had sent.

Purpose: The purpose of anomaly detection is to provide users with an immediate understanding of the any client onboarding issue that have occurred, provide an analysis and present a packet capture depicting the incident as proof.

Supported Onboarding Anomaly Scenarios	
Anomaly Type	**Description**
802.1x Timeout	Event is triggered when a client takes too long to respond to an AP's EAP Request.
DHCP Timeout	Event is triggered when either the DHCP Server's DHCP Offer or a Client's DHCP Request takes longer than the DHCP timeout time configured.
EAP ID Timeout	Event is triggered when a client takes too long to respond to an AP's EAP Request.
Invalid RSNIE within Association Request	Event is triggered when a client sends an association request to the AP with a corrupt RSNIE value.
4 Way Handshake Timeout	Event is triggered when a client ignores the M1 or M2 sent by the AP during the four-way handshake.
Unsupported Rates	Event is triggered when a client sends the AP an association request but with data rates that don't matched the mandatory data rates configured on the WLC.
Mismatching Replay Counters	Event is triggered when a retry packet's replay counters are not sent in proper incremental order.
Invalid MIC	Event is triggered when client sends either an invalid M2 or M4 during four-way handshake to the AP.
GTK Handshake Timeout	Event is triggered when a client either the client ignores the M1 or sends an invalid M2 during the reauthentication handshake.

Table 10. Onboarding Anomalies that an AP is able to detect and what they mean.

© 2020 Cisco Systems, Inc. All rights reserved.

In the case that anomaly packets are not seen with the red onboarding event, Cisco DNA Center will provide a reason for why this might be happening.

No Anomaly Packets Correlated Reasons	
Scenario	**Description**
No Packets due to all packets already sent for this Client	The AP already send packets for this client a moment ago.
No Packets Due to Anomaly Being Disabled on Cisco DNA Center	Anomaly Detection is not enabled.
No Packets Due to AP Throttling	By default, Anomaly Detection Individual reports throttling is set to 100 when the feature is enabled mean, only 100 anomaly events can be sent per AP to Cisco DNA Center every 5 mins. If more than 100 events are detected, those will not be sent until the 5 mins are up.
No Packets Due to Channel Busy	The channel that the AP's radio is serving on is too congested to capture packets.
No Packets Due to GRPC Link Error	There is a connectivity issue between the AP and Cisco DNA Center.
No Packets Due to High CPU	The AP has a CPU utilization of 90% or higher.
No Packets due to Packet Attachment being Disabled	Anomaly Packet Trace on the WLC is disabled.
No Packets due to Queue Empty	The AP already send packets for this client a moment ago.
No Packets Due to Reason Unknown	The AP's firmware has encountered an issue.
No Packets Due to Unsupported AP	The client is joined to an AP that does not support Intelligent Capture.

Table 11. Reasons why Anomaly Packets might not be Correlated with an Anomaly Onboarding Event.

4. *Navigate to the Intelligent Capture Settings and Enable Anomaly Stats Capture in the same manner as we enabled AP Stats Capture in the section prior (**Figure 74.**).*

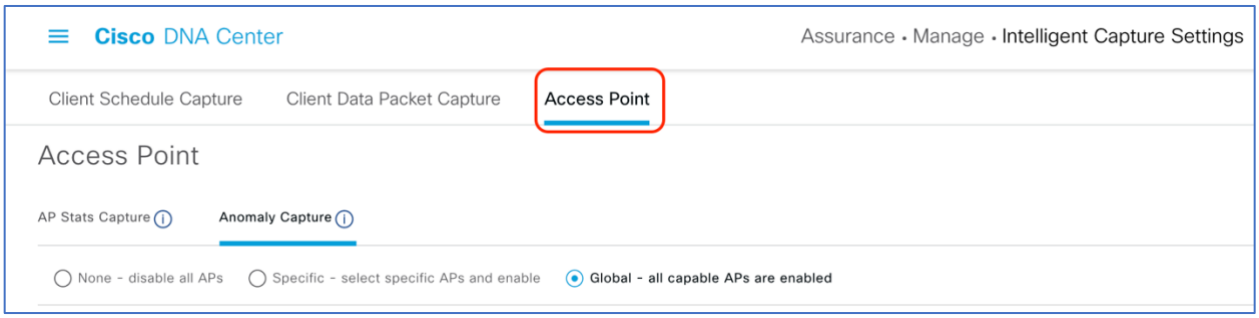


Figure 76. Location of Anomaly Stats Capture in the Intelligent Capture Settings Page

5. View the onboarding events viewer on the left, if a client onboarding anomaly had occurred, you will see a red event with a red PCAP symbol (same as how onboarding packet captures are displayed but just with red text). Expand this event with the down arrow to open up the child events within, and

© 2020 Cisco Systems, Inc. All rights reserved.

6. click on the red event (**Figure 77.**).

7. At the top of the anomaly event menu that opens, you will observe a plain text message depicting exactly which onboarding anomaly had occurred during this event (**Figure 77.**).

8. Scroll down the menu, you will be able to find the anomaly packets shown in the **Auto Packet Analyzer**, and be able to download it with the **Download Packets** button (**Figure 77.**).
    a. The top left half of the chart categorizes the different packets within the Anomaly Packet Capture (802.11 Open Auth, Association, 802.1x/EAP, DHCP, Data, 802.11k/11v).
    b. The red and blue bars measured by the bottom left Y-axis of the chart depicts the Interpacket Gap (us) of the packets. The bar is blue when there are no issues with the packets exchanged, but is shown red when the packets are determined to be the reason for an onboarding failure.
    c. The purple line measured by the bottom right Y-axis of the chart represents the RSSI between the AP and the Client during the packet exchanges.
    d. Each triangle within the chart represents a single packet, and the direction of the triangles represent the direction of the packet (Up means from Client to AP, Down means from AP to Client).
    e. Red triangles represent packets that caused the onboarding anomaly whereas green packets are properly exchanged packets.
    f. The horizontal green bar in the chart represents the AP that the client had been connected to during this packet capture. If the client had roamed between different APs, you will see a different color bar in portions of the chart when that had happened to represent what packets were sent by which AP.
    g. The white portion of the chart represents the time slot of the current event we're looking at whereas the gray portion of the chart represents the packet exchange activity that occurred prior to this anomaly. This feature has the purpose to provide users with a background as to what packet exchanged occurred prior to the onboarding failure.

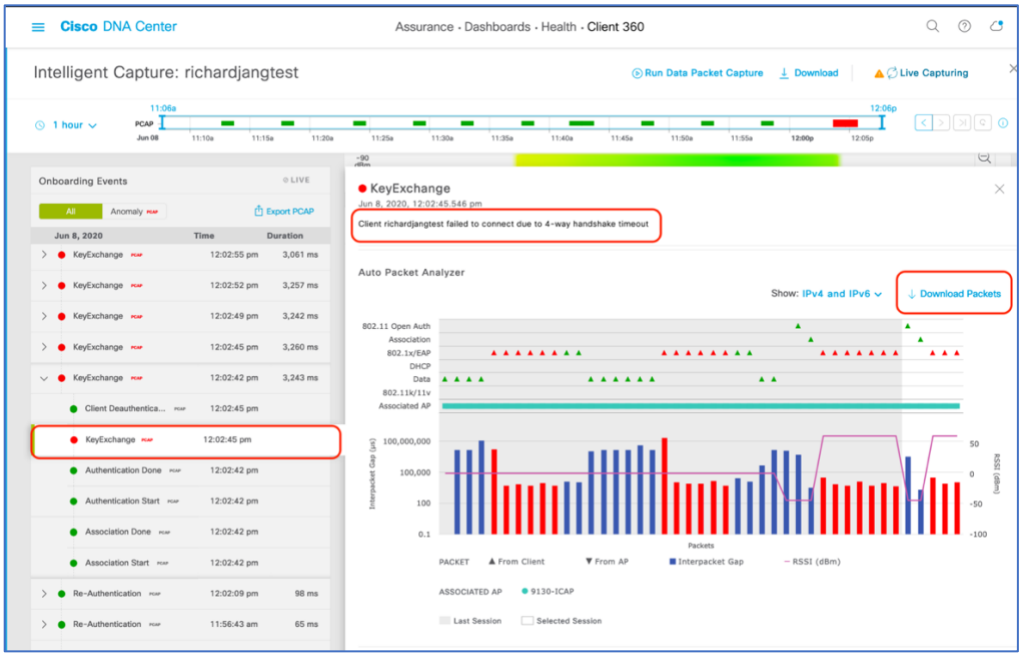


Figure 77. Viewing an Anomaly Event Message and Packets

© 2020 Cisco Systems, Inc. All rights reserved.

9. When you download the anomaly packets and open it up in Wireshark, you will observe that the packets downloaded represent what's shown in the auto packet analyzer identically (**Figure 78.**).
    a. You will be able to confirm that the issue that Intelligent Capture claimed to have happened really happened.
    b. Example: Intelligent Capture claimed the client onboarding failure was to onboard due to a 4-way handshake timeout. If you look into the packet capture below, you'll observe that the AP had sent the client three M1 message to start the 4-Way Handshake; however, the client never responded with an M2. The AP then sent the client a Deauthentication packet with the reason code of 4-Way Handshake Timeout.

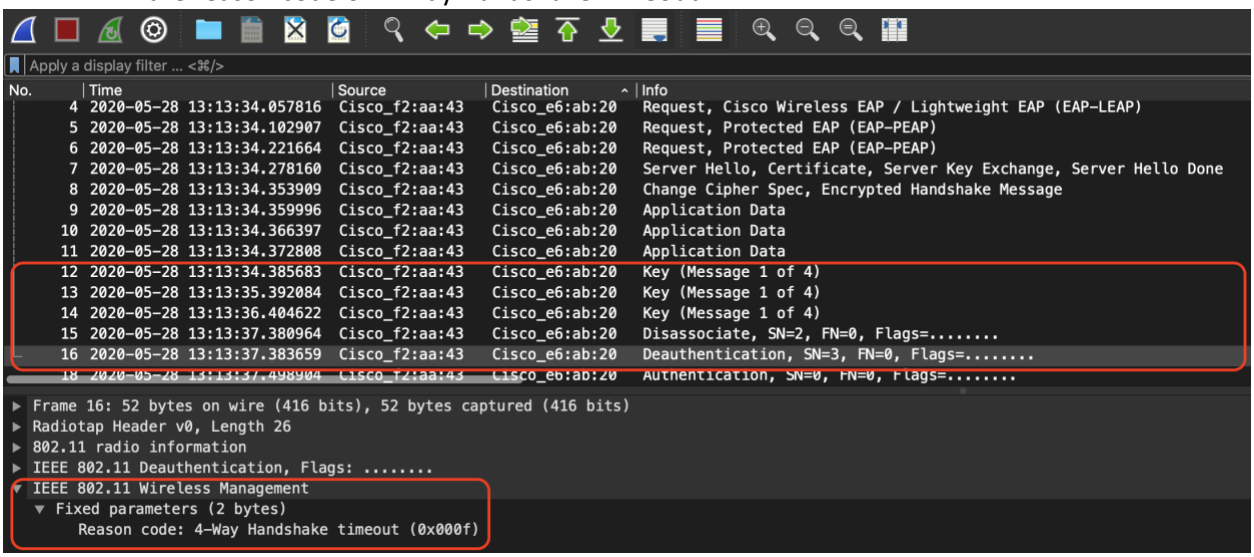


Figure 78. 4-Way Handshake Timeout Depicted by the Anomaly Packets

10. If you would like to filter the onboarding events viewer to show only the Anomaly Events with Anomaly PCAPs, click on the **Anomaly PCAP** tab at the top of the onboarding events viewer (**Figure 79.**)

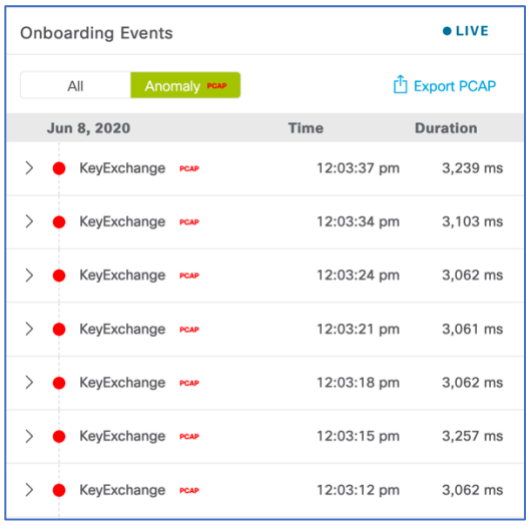


Figure 79. Filtering the Onboarding Events Viewer to Show Only Anomaly Events with PCAPs

© 2020 Cisco Systems, Inc. All rights reserved.

11. *If you wanted to download multiple anomaly or live capture packets, you can click on the **Export PCAP** button, and Cisco DNA Center will allow you to choose a range of onboarding events to download packets from. It will the stitch together these packets from your range of chosen event and allow you to download them as a single file (**Figure 80.**).*

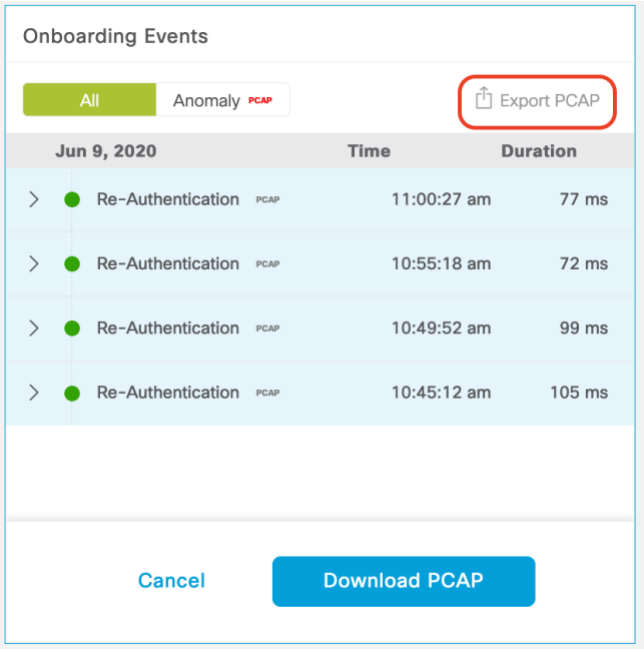


Figure 80. Downloading a Range of Anomaly or Live Capture Packets

© 2020 Cisco Systems, Inc. All rights reserved.

Device Side Configurations and Show Commands

Description: If you encounter an issue with Intelligent Capture, device side show & configuration commands will help you troubleshoot and root cause the issue.

Section: To understand the show & configuration commands for AireOS WLC, IOS-XE WLC, and access points.

AireOS WLC Show Commands

Viewing the Cisco DNA Center IP and GRPC port that are configured on joined APs:

- `show icap summary`

Viewing the Cisco DNA Center IP and statuses of the connection that are configured on the WLC:

- `show network assurance summary`

Viewing the enablement status of various Intelligent Capture features at a global, group, and AP level with varying levels of detail:

- `show icap {global | group} {summary | all}`
- `show icap {global | group} detail {full-packet-trace | partial-packet-trace | anomaly-detection | individual-report | summary-report | client-statistics | client-stats-filter | system-statistics | radio-statistics | memory-statistics | wlan-statistics | dns-statistics | interface-statistics | routing-statistics | rf-spectrum}`
- `show icap ap <AP Name> {summary | all | operational | capability}`
- `show icap ap <AP Name> detail {full-packet-trace | partial-packet-trace | anomaly-detection | individual-report | summary-report | client-statistics | client-stats-filter | system-statistics | radio-statistics | memory-statistics | wlan-statistics | dns-statistics | interface-statistics | routing-statistics | rf-spectrum}`

Viewing the serviceability statuses of joined APs at a global or per AP level which depict whether or not the AP's have a properly established connection with Cisco DNA Center.

- `show icap serviceability summary`
- `show icap serviceability detail all`
- `show icap serviceability detail ap <AP name>`

© 2020 Cisco Systems, Inc. All rights reserved.

Configuring the Intelligent Capture GRPC Port that AP will be using to externalize data:

- config icap server port <GRPC Port>

Configuring the Intelligent Capture IP that the WLC and APs will be externalizing data to:

- config network assurance url <Cisco DNA Center IP>

Enabling AP RF Statistics:

- config icap global subscription ap statistics {dns | interface | memory | radio | routing | system | wlan}
    - Only WLAN and radio statistics data are consumed on Cisco DNA Center.
    - Note: If you would like to enable the feature on a AP Group replace global with ap <AP Name> or group <AP Group Name> respectively.

Anomaly Detection Related Configurations:

- config icap global subscription client anomaly-detection enable
    - Description: Enabling APs to begin detecting client anomalies.

- config icap global subscription client anomaly-detection disable
    - Description: Disabling anomaly detection on APs.

- config icap global subscription client anomaly-detection filter {add | remove}
    - Adding or removing a Client MAC address for Anomaly Detection.
    - This configuration isn't enabled when the feature is enabled from Cisco DNA Center.

- config icap global subscription client anomaly-detection packet-trace trigger add ap

    - Enabling APs to send anomaly packets to Cisco DNA Center.

- config icap global subscription client anomaly-detection packet-trace trigger remove ap

    - Disabling APs to send anomaly packets to Cisco DNA Center.

- config icap global subscription client anomaly-detection report-individual enable

    - Enabling APs to send anomaly events to Cisco DNA Center.

© 2020 Cisco Systems, Inc. All rights reserved.

- config icap global subscription client anomaly-detection report-individual disable
  - Enabling APs to send anomaly events to Cisco DNA Center.

- config icap global subscription client anomaly-detection report-individual throttle <0 - 500>
  - Configuring a throttle limit to the # of anomaly event APs can send every to Cisco DNA Center every 5 minutes.
  - Note: 0 signifies no throttling.

- config icap global subscription client anomaly-detection report-summary enable
  - Enabling APs to send a summary report which contains all client anomalies detected over the past time frequency configured.

- config icap global subscription client anomaly-detection report-summary disable
  - Disabling APs to send a summary report which contains all client anomalies detected over the past time frequency configured.

- config icap global subscription client anomaly-detection report-summary frequency <3 – 60 mins>
  - Configuring a summary report frequency.

- config icap global subscription client anomaly-detection timeout dhcp <1 – 120 seconds>
  - Configuring the amount of time (seconds) that a DHCP server doesn’t reply to a client’s DHCP request before considering it to be an anomaly.

- Note: If you would like to enable the feature on a AP Group replace global with ap <AP Name> or group <AP Group Name> respectively.

Full Packet Capture Related Configurations:

- config icap global subscription client packet-trace full enable
  - Enabling full packet capture on the AP (equivalent to data packet capture on Cisco DNA Center).

- config icap global subscription client packet-trace full disable
  - Enabling full packet capture on the AP.

- config icap global subscription client packet-trace full filter

  - Configuring a client to capture data packets on.

© 2020 Cisco Systems, Inc. All rights reserved.

- Note: If you would like to enable the feature on a AP Group replace global with ap <AP Name> or group <AP Group Name> respectively.

Partial Packet Capture Related Configuration:

- config icap global subscription client packet-trace partial enable
  - Enabling partial packet capture on the AP (equivalent to one of the three features enabled when Live Capture is enabled on Cisco DNA Center).

- config icap global subscription client packet-trace partial disable
  - Enabling partial packet capture on the AP.

- config icap global subscription client packet-trace partial filter <Client MAC>
  - Configuring a client to capture onboarding packets on.

- config icap global subscription client packet-trace partial protocol {add | remove} all
  - Adding or removing all categories of onboarding packet filters for APs to send to Cisco DNA Center.

- config icap global subscription client packet-trace partial protocol {add | remove} cisco {all | ndp}
  - Adding or removing Cisco specific onboarding packet filters for APs to send to Cisco DNA Center.

- config icap global subscription client packet-trace partial protocol {add | remove} data {all | arp | dhcp | dhcpv6 | dns | eap | icmp | icmpv6}
  - Adding or removing data specific onboarding packet filters for APs to send to Cisco DNA Center.

- config icap global subscription client packet-trace partial protocol {add | remove} management {all | assoc | auth}
  - Adding or removing management specific onboarding packet filters for APs to send to Cisco DNA Center.

- Note: If you would like to enable the feature on an AP Group replace global with ap <AP Name> or group <AP Group Name> respectively.

Client Statistics Related Configurations:

- config icap global subscription client enable
  - Enabling regular client statistics (equivalent to one of the three features enabled when enabling AP Stats Capture on Cisco DNA Center).

© 2020 Cisco Systems, Inc. All rights reserved.

- config icap global subscription client disable
  - Disabling regular client statistic

- config icap global subscription client frequency <30-3600 seconds>
  - Configuring the frequency in which APs will send AP RF Statistics data to Cisco DNA Center.

- Note: If you would like to enable the feature on a AP Group replace global with ap <AP Name> or group <AP Group Name> respectively.

Client Filtered Statistics Related Configurations:

- config icap global subscription client statistics filter enable
  - Enabling filtered client statistics (equivalent to one of the three features enabled when enabling live capture on Cisco DNA Center).

- config icap global subscription client statistics filter enable
  - Disabling filtered client statistics

- config icap global subscription client statistics filter add <client MAC>
  - Configuring a client mac for the AP to send client statistics for.

- config icap global subscription client statistics filter remove
  - Removing a configured client statistics client MAC.

- config icap global subscription client statistics filter frequency <5-3600 seconds>

  - Configuring the frequency in which APs will send AP RF Statistics data to Cisco DNA Center.

- Note:
  - Difference between client statistics and client filtered statistics is that client filtered statistics allows for statistics data to be sent at 5 seconds interval opposed to a 30 seconds interval.

  - If you would like to enable the feature on an AP Group replace global with ap <AP Name> or group <AP Group Name> respectively.

© 2020 Cisco Systems, Inc. All rights reserved.

IOS-XE WLC Show Commands

Configuring the Intelligent Capture GRPC Port that AP will be using to externalize data:

- config icap server port <GRPC Port>

Configuring the Intelligent Capture IP that the WLC and APs will be externalizing data to:

- network-assurance url <Cisco DNA Center IP>

Viewing the Cisco DNA Center IP and statuses of the connection that are configured on the WLC:

- show network-assurance summary

Viewing all Intelligent Capture Features Enabled within all AP Profiles:

- show run | sec icap

Viewing the serviceability statuses of joined APs which depict whether or not the AP's have a properly established connection with Cisco DNA Center:

- Show ap icap serviceability {detail | summary}

IOS-XE WLC Configuration Commands

Configuring Intelligent Capture features for specific AP Profiles:

Note: For all configuration commands, first run the following two commands.

1. Configure terminal

2. Ap profile <AP Profile Name>

Enabling Spectrum Analysis:

- icap subscription ap rf spectrum

Enabling AP RF Statistics:

- icap subscription ap statistics {dns | interfaces | memory | radio | routing | system | wlan}
    - Only WLAN and radio statistics data are consumed on Cisco DNA Center.

Anomaly Detection Related Configurations:

- icap subscription client anomaly-detection enable
    - Description: Enabling APs to begin detecting client anomalies.

- icap subscription client anomaly-detection filter <Client MAC>
    - Configuring a Client MAC address for Anomaly Detection.

© 2020 Cisco Systems, Inc. All rights reserved.

- This configuration isn’t enabled when the feature is enabled from Cisco DNA Center.

- icap subscription client anomaly-detection packet-trace trigger ap
  - Enabling APs to send anomaly packets to Cisco DNA Center.

- icap subscription client anomaly-detection report-individual enable
  - Enabling APs to send anomaly events to Cisco DNA Center.

- icap subscription client anomaly-detection report-individual throttle <0-100>
  - Configuring a throttle limit to the # of anomaly event APs can send every to Cisco DNA Center every 5 minutes.

- icap subscription client anomaly-detection report-summary enable
  - Enabling APs to send a summary report which contains all client anomalies detected over the past time frequency configured.

- icap subscription client anomaly-detection report-summary frequency <3-60>
  - Configuring a summary report frequency.

- icap subscription client anomaly-detection timeout dhcp <1-120>
  - Configuring the amount of time (seconds) that a DHCP server doesn’t reply to a client’s DHCP request before considering it to be an anomaly.

Full Packet Capture Related Configurations:

- icap subscription client packet-trace full enable
  - Enabling full packet capture on the AP (equivalent to data packet capture on Cisco DNA Center).

- icap subscription client packet-trace full filter <client-mac>
  - Configuring a client to capture data packets on.

Partial Packet Capture Related Configuration:

- icap subscription client packet-trace partial enable
  - Enabling partial packet capture on the AP (equivalent to one of the three features enabled when Live Capture is enabled on Cisco DNA Center).

- icap subscription client packet-trace partial filter client <client-mac>
  - Configuring a client to capture onboarding packets on.

- icap subscription client packet-trace partial filter protocol all

© 2020 Cisco Systems, Inc. All rights reserved.

- Adding all categories of onboarding packet filters for APs to send to Cisco DNA Center.

- icap subscription client packet-trace partial filter protocol type cisco subtype {all | ndp}
  - Adding Cisco specific onboarding packet filters for APs to send to Cisco DNA Center.

- icap subscription client packet-trace partial filter protocol type data subtype {all | arp | dhcpv4 | dhcpv6 | dns | eap | icmpv4 | icmpv6}
  - Adding data specific onboarding packet filters for APs to send to Cisco DNA Center.

- icap subscription client packet-trace partial filter protocol type management subtype {all | assoc | auth | probe}
  - Adding management specific onboarding packet filters for APs to send to Cisco DNA Center.

Client Statistics Related Configurations:

- icap subscription client statistics enable
  - Enabling regular client statistics (equivalent to one of the three features enabled when enabling AP Stats Capture on Cisco DNA Center).

- icap subscription client statistics frequency <30-3600>
  - Configuring the frequency in which APs will send AP RF Statistics data to Cisco DNA Center.

Client Filtered Statistics Related Configurations:

- icap subscription client statistics filter enable
  - Enabling filtered client statistics (equivalent to one of the three features enabled when enabling live capture on Cisco DNA Center).

- icap subscription client statistics filter <client-mac>
  - Configuring a client mac for the AP to send client statistics for.

- icap subscription client statistics filter frequency <5-3600>
  - Configuring the frequency in which APs will send AP RF Statistics data to Cisco DNA Center.

- Note: Difference between client statistics and client filtered statistics is that client filtered statistics allows for statistics data to be sent at 5 seconds interval opposed to a 30 seconds interval.

© 2020 Cisco Systems, Inc. All rights reserved.

AP Show Commands

- Show ap icap anomaly-detection
  - Displaying all anomaly detection configurations pushed from WLC to AP as well as any anomalies detected.

- show ap icap anomaly-detection {connected | onboarding}
  - Connected: Anomaly Event details for clients already onboarded.

  - Onboarding: Anomaly Event details for clients that are currently onboarding.

- show ap icap client
  - Displaying joined client’s past onboarding events.

- show ap icap config {anomaly-detection | connection | packettrace-full | packettrace-partial | rf-spectrum | statistic}
  - Viewing the configuration history of these Intelligent Capture commands.

- show ap icap connection
  - Viewing the connection status between the AP and Cisco DNA Center.

- show ap icap counters
  - Viewing the number of full/partial/anomaly packets located within each queue within the firmware.

- show ap icap packets
  - Viewing the number of packets/events/messages sent or dropped for each Intelligent Capture feature.

- show ap icap subscription
  - Viewing the Intelligent Capture configurations currently enabled on the AP.

- show ap icap telemetry
  - Viewing the frequency configured for each Intelligent Capture feature on the AP.

© 2020 Cisco Systems, Inc. All rights reserved.

Useful Links

Cisco DNA Assurance User Guide, Release 2.1.1

- https://www-author3.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-1-1/b_cisco_dna_assurance_2_1_1_ug/b_cisco_dna_assurance_2_1_1_ug_chapter_01110.html

Cisco DNA Center Information

- https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html?dtid=osscdc000283

Cisco Prime Virtual Network Analysis Module (vNAM) Installation and Configuration Guide

- https://www.cisco.com/c/en/us/td/docs/net_mgmt/network_analysis_module_software/vNAM/install/guide/cisco_prime_vNAM_install_config_guide.pdf

Cisco Prime Virtual Network Analysis Module (vNAM) Information

- https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-virtual-network-analysis-module-vNAM/index.html

Cisco Prime Virtual Network Analysis Module 6.4.2 (vNAM) OVA

- https://software.cisco.com/download/home/286322801/type/282700108/release/6.4.2

Cisco CMX Configuration Guide, Release 10.6.0 and Later

- https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/getting_started_with_cisco_cmx.html

© 2020 Cisco Systems, Inc. All rights reserved.