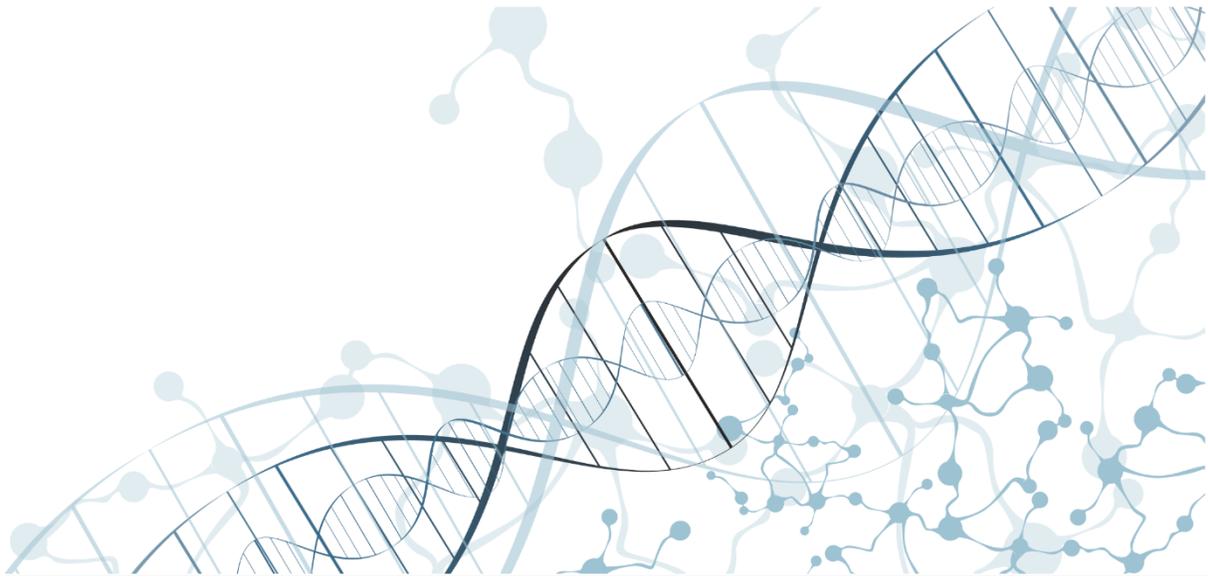




Cisco Remote Workforce Solution- Wireless



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

TECHNOLOGY USE CASE	5
USE CASE: TELEWORKER WITH WIRELESS DEVICES	5
DESIGN OVERVIEW	6
DEPLOYMENT COMPONENTS.....	6
CISCO WIRELESS LAN CONTROLLERS.....	6
CISCO TELEWORKER ACCESS POINTS	7
CORPORATE FIREWALL.....	7
DESIGN MODELS.....	7
CISCO AP (TELEWORKER) WORKFLOW	8
STEPS REQUIRED TO CONFIGURE TELEWORKER AP	9
CONFIGURE FLEX-PROFILE FOR TELEWORKER AP.....	11
CONFIGURE AP JOIN PROFILE FOR DTLS ENCRYPTION	12
CONFIGURE SITE TAG FOR TELEWORKER AP.....	14
TAG THE AP BEFORE AP JOINS.....	15
CISCO NETWORK PLUG AND PLAY (PNP) FOR TELEWORKER DEPLOYMENT.....	25
PREREQUISITES.....	26
CLOUD PLUG AND PLAY CONNECT REDIRECT TO WLC	26
CLOUD PLUG AND PLAY DEVICE PROVISIONING.....	26
CREATE A SMART ACCOUNT	26
CREATE A CONTROLLER PROFILE	27
ADDING CISCO ACCESS POINT TO THE DEVICES LIST.....	30
UMBRELLA FOR TELEWORKER WLAN.....	34
CONFIGURING THE REMOTE LAN	38
CONFIGURE REMOTE LAN POLICY	40
ADDING WLANS/RLANS TO A POLICY TAG	42
SPLIT TUNNELING FOR TELEWORKER AP	46
CREATING SPLIT-ACL	47
ASSIGNING THE SPLIT ACL ON FLEX PROFILE.....	47
ASSIGN THE ACL AS THE SPLIT MAC ACL ON POLICY PROFILE	48
CISCO CATALYST C9105W AS TELEWORKER ACCESS POINT.....	50
CONNECTING CISCO TELEWORKER ACCESS POINT	51
CLEARING PERSONAL SSID	56



LIMITATIONS & RESTRICTIONS	56
TELEWORKER ASSURANCE FROM CISCO DNA CENTER.....	57
REFERENCE DOCUMENTS AND VODS.....	63





Technology Use Case

Providing employees access to corporate network and services from a remote environment poses challenges for both the end user and IT operations. For the home-based teleworker, it is critical that access to business services be reliable, consistent and secure, providing an experience that is as similar as office in the organization's facility. In addition, the solution must also support a wide range of teleworking employees who have varying skill sets, making it critical to have a streamlined and simplified way to implement the teleworker solution.

Cisco Teleworker Access Point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The user's experience at the remote location is the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security. Users may also need access to Cloud Applications (for e.g. Office365, AWS etc.) so it's important to also have a direct access to cloud with Teleworker AP (split tunneling) option.

Use Case: Teleworker with Wireless Devices

Teleworkers require always-on secure access to networked business services from a remote home office. Wireless access provides easy mobility and setup within the home office, and consistent device configuration allows for easy mobility between the home office and on site at the corporate location.

This design guide enables the following network capabilities:

- Common wireless device configuration for onsite and teleworker wireless access
- Authentication through IEEE 802.1X for employees and encryption for all information sent and received to the organization's main location
- Simplified IT provisioning for the home office, which reduces setup time and supports varying levels of end-user skills
- Mobility and flexibility for voice endpoints at the teleworker location



Design Overview

The Cisco Teleworker solution is based on Cisco OEAP (OfficeExtend AP) feature it is specifically designed for the teleworker who primarily uses wireless devices. The solution consists of the following components:

Cisco Aironet Access Point

All 11ac wave2 (indoor) - OEAP1810, 1810W,1815T/W/I, 1840, 1830,1850 Series
2800/3800/4800 Series AP

Cisco Catalyst Access Points

All Cisco Catalyst C9100 Series APs

Cisco C9800 Wireless LAN Controller

C9800-CL (Private Cloud), C9800-L, C9800-40, C9800-80
Recommended Software 17.3 release

Cisco AireOS Wireless LAN Controller

CT-3504, 5520, 8540
Recommended Software 8.10MR3 release

Deployment Components

The Teleworker deployment is built around three main components: Cisco wireless LAN Controllers, Cisco Access Points and Corporate Firewall

Cisco Wireless LAN Controllers

Cisco wireless LAN controllers are responsible for system-wide WLAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco Teleworker Access Points to support business-critical wireless applications for teleworkers. Cisco wireless LAN controllers provide the control, scalability, security, and reliability that network managers need to build a secure, scalable teleworker environment.

To allow users to connect their corporate devices to the organization's on-site wireless network, the Cisco teleworker solution offers the same wireless Secure Set Identifiers (SSIDs) at teleworker's home as those that support data and voice inside the organization.



Cisco Teleworker Access Points

Cisco has dedicated Teleworker APs like 1810 and 1815T but mostly all Cisco APs can run the teleworker/OEAP functionality. Teleworker APs require a centralized Wireless LAN Controller, as the Access Point communicates with the WLC resources, it will download its configuration and synchronize its software/firmware image, if required. Cisco Access Points establishes a secure Datagram Transport Layer Security (DTLS) connection to the controller to offer remote WLAN connectivity using the same profile as at the corporate office. Secure tunneling allows all traffic to be validated against centralized security policies and minimizes the management overhead associated with home-based firewalls.

Cisco Teleworker access points delivers full 802.11ac and 802.11ax wireless performance and avoids congestion caused by residential devices because it operates simultaneously in the 2.4-GHz and the 5-GHz radio frequency bands. Cisco Teleworker Access Points usually connected to a NATed home-router environment, provides wired and wireless segmentation of home and corporate traffic, which allows for home device connectivity without introducing security risks to corporate policy.

Corporate Firewall

The Wireless LAN Controller should be placed in DMZ and the corporate Firewall must allow CAPWAP Control and CAPWAP Data traffic through the Firewall to the Wireless LAN Controller. The general configuration on the firewall is to allow CAPWAP control and CAPWAP management port numbers through the firewall.

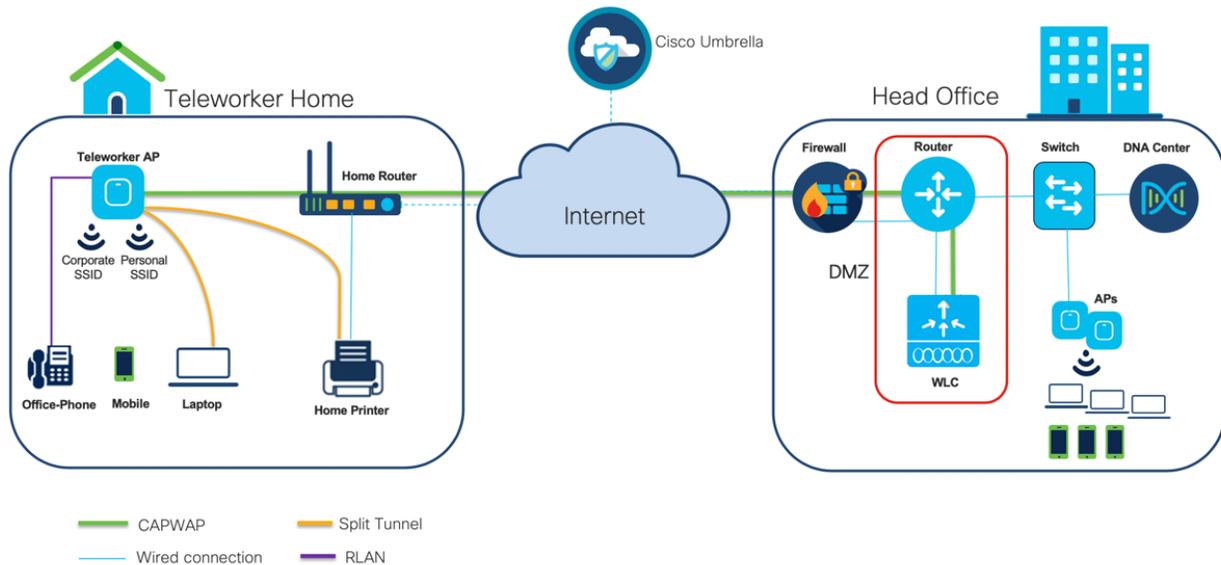
Note: The UDP 5246 and 5247 ports need to be opened on the firewall for communication between the Wireless LAN controller and the Cisco Teleworker Access Points

Design Models

For the most flexible and secure deployment of Cisco Teleworker solution deploy a dedicated controller using Cisco Catalyst 9800 Series Controllers or Cisco AireOS Wireless Controllers. In the dedicated design model, the controller is directly connected to the Internet edge demilitarized zone (DMZ) and traffic from the Internet is terminated in the DMZ versus on the internal network, while client traffic is still directly connected to the internal network.



Figure 1. Cisco Teleworker Design Model



Cisco AP (Teleworker) Workflow

The following steps describe the workflow carried out by the admin and teleworker to connect the Teleworker Access Point to the corporate Wireless LAN Controller:

- Admin acquires the AP inventory recorded before shipping to employee.
- Admin can utilize Cisco Network Plug & Play to provision the access points with WLC IP address.
- Admin can provide teleworker with an Access Point primed with the IP address of the corporate Wireless LAN controller. Alternatively, the teleworker/employee can prime the Access Point by entering the IP address of the Wireless LAN Controller in the local configuration screen of the Access Point.
- The teleworker connects the WAN port (on OEAP1810 & 1815T Models) dedicated Teleworker Access Point or PoE LAN port (on other AP models) to one of the home internet router LAN interfaces.
- The Access Point will obtain an IP address from the home internet router and will initiate a join request to the corporate Wireless LAN Controller



- After the Access Point joins the corporate Wireless LAN Controller, it can advertise the corporate SSID, extending the same security methods and services across the WAN to the teleworker's remote home location
- If Remote LAN (RLAN) is configured on Wired LAN ports of the Supported Access Points (OEAP1810,1815T,1815W,1850,2800, 3800 and C9105W, devices can be connected to the corporate network via the Wired LAN ports
- Teleworker can additionally configure a Personal SSID on the Access Point for home wireless network.

Steps Required to Configure Teleworker AP

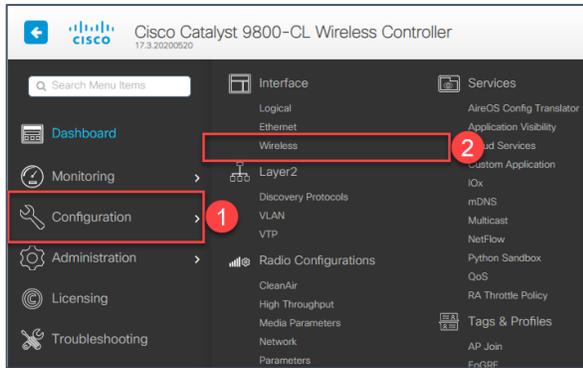
1. Configure WLC C9800 for NAT
2. Configure Flex-Profile for Teleworker AP – to enable OEAP option
3. Configure AP Join Profile – For DTLS encryption and Priming AP
4. Configure Site Tag for Teleworker AP
5. Tag the AP before AP Joins
6. Setup Cisco Network Plug and Play (PnP) for ease of deployment.

Configure WLC C9800 for NAT

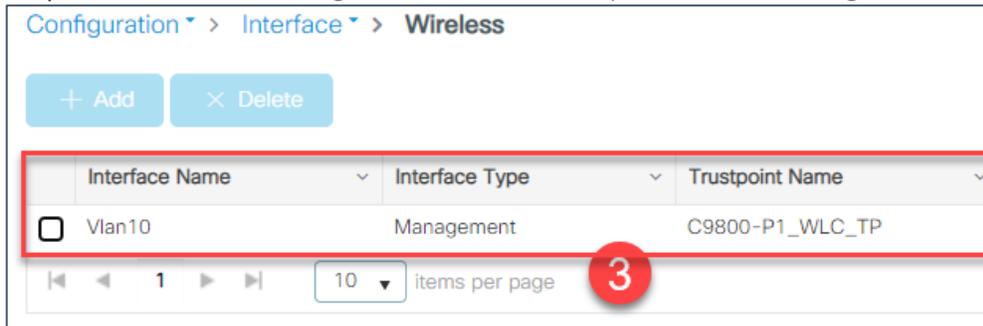
The Internet edge firewall usually works as a Network Address Translation (NAT) device and translates the IP address of the WLC management interface in the DMZ to a publicly reachable IP address so Teleworker Access Point at employee location can reach the WLC. However, in order for the Access Point to communicate with the WLC, the publicly reachable address must also be configured on the WLC management interface. It is required to use 1:1 NAT mapping for the WLC's IP address, meaning that the WLC's private IP is mapped statically to a single public IP (no Port Address Translation is possible).

To configure the WLC for NAT, perform the following steps:

Step 1: On the C9800 WLC GUI navigate to **Configuration → Interface → Wireless**

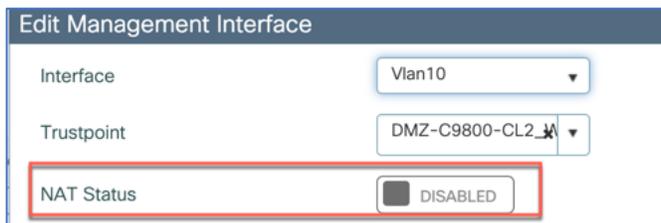


Step 2: Click on the Management interface to open the Edit Management Interface dialog box



Step 3: Click on NAT Status to Enabled

This opens the IP address box, to assign the Public NAT IP.



Step 4: Fill the Public IP of the WLC and From CAPWAP Discovery option select Private, Public or both

Private – This Includes private IP in CAPWAP Discovery Response. For Example: If WLC mgmt. IP is 10.10.10.3 and APs on corporate network can discover and join WLC through this management IP address.

Public – Includes public IP in CAPWAP Discovery Response. The public option allows WLC to advertise external IP and allows AP's on Public network discover and join on Public IP of WLC. Both options can be enabled as well. For WLC behind NAT make sure the Public IP is enabled.



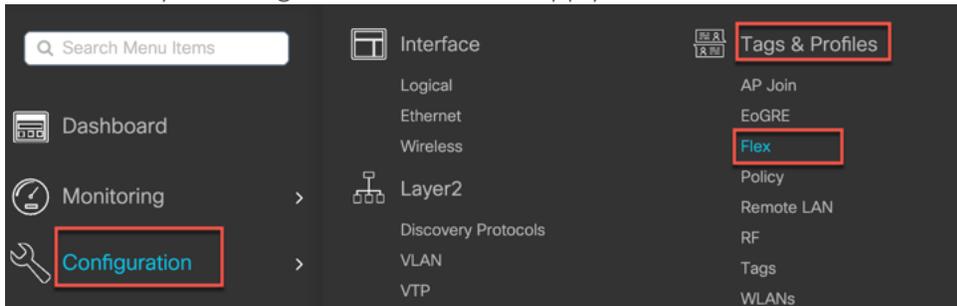
Edit Management Interface

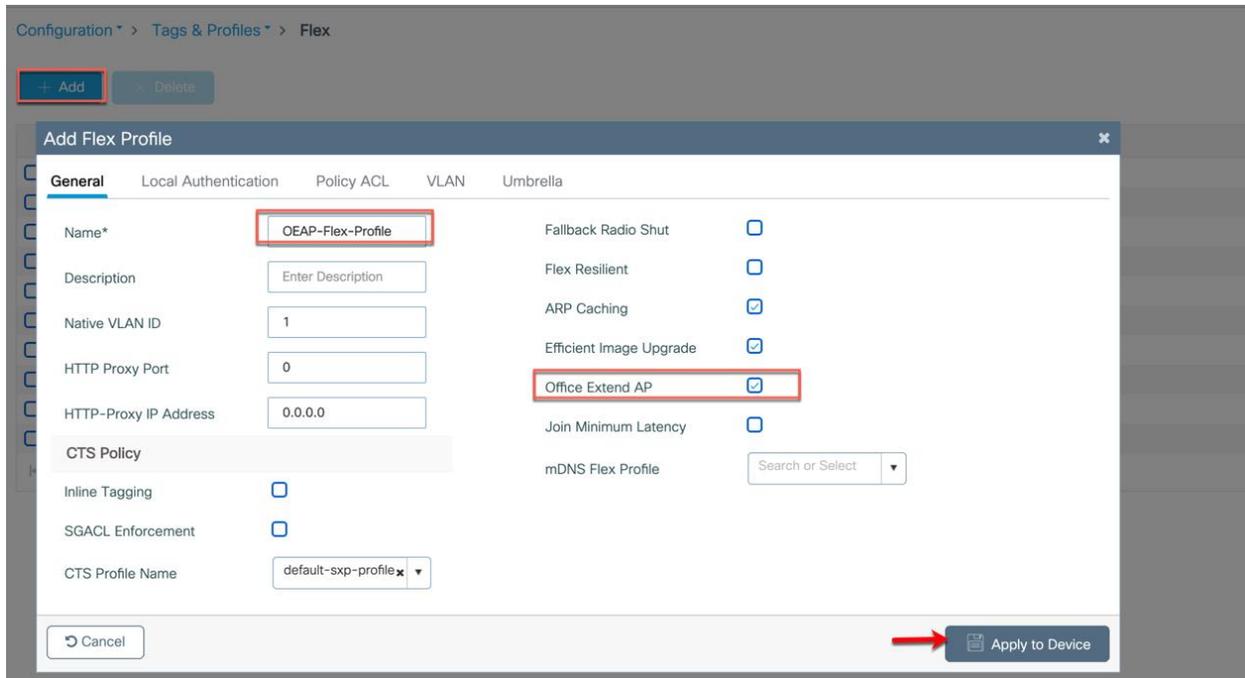
Interface	Vlan10
Trustpoint	DMZ-C9800-CL2_1
NAT Status	ENABLED 4
IPv4 / IPv6 Server Address	128.107.254.10 5
CAPWAP Discovery	6 <input checked="" type="checkbox"/> Private 7 <input checked="" type="checkbox"/> Public

Configure Flex-Profile for Teleworker AP

The Office Extend configuration is part of flex profile so user either needs to create a custom flex profile or can use the default-flex-profile to enable it. This function will convert the APs to OEAP

Step 5: Navigate to **Configuration** → **Tags & Profiles** → **Flex** and modify the default-flex-profile (or create a custom one by clicking +Add then Name the Flex Profile and then enable Office Extend AP by checking the box then click Apply

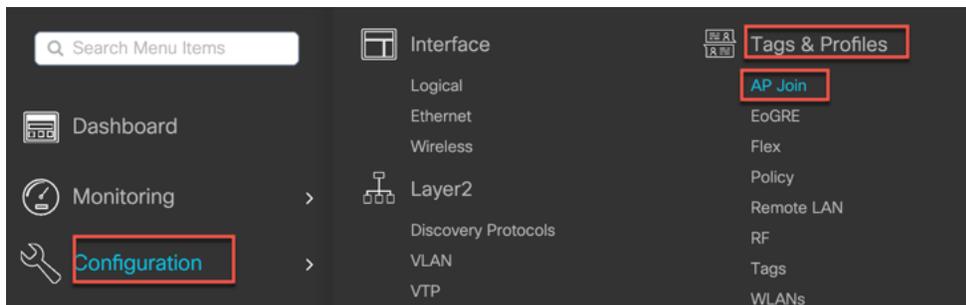




Note: The Access Point will reboot and after reboot, it will operate as a Teleworker/OfficeExtend Access Point.

Configure AP Join Profile for DTLS encryption

Step 6: Go to Configuration → Tags & Profiles → AP Join



Now create a new AP join profile specific for OEAP by clicking **+Add**, name the profile and go to General tab. If the admin wants to provide local access of the OEAP to individual users, then Enable Local Access, otherwise do not enable. Enabling Local Access, gives the OEAP end users to have GUI access to the OEAP and configure private SSID settings.

Also, enable Link Encryption.



Add AP Join Profile

General Client CAPWAP AP Management Security ICap QoS

Name* OEAP-Profile1

Description Site 1

LED State

LAG Mode

NTP Server 0.0.0.0

GAS AP Rate Limit

Apphost

OfficeExtend AP Configuration

Local Access

Link Encryption

Rogue Detection

Cancel Apply to Device

Now go to **CAPWAP> High Availability>Primary Controller** configure the Name and IP Address of WLC.

Edit AP Join Profile

General Client CAPWAP AP Management Security ICap QoS

High Availability Advanced

CAPWAP Timers

Fast Heartbeat Timeout(sec)* 0

Heartbeat Timeout(sec)* 30

Discovery Timeout(sec)* 10

Primary Discovery Timeout(sec)* 120

Primed Join Timeout(sec)* 0

Retransmit Timers

Count* 5

Interval (sec)* 3

Backup Controller Configuration

Enable Fallback

Primary Controller

Name WLC

IPv4/IPv6 Address 1: 10.10.10.10

Secondary Controller

Name Enter Name

IPv4/IPv6 Address

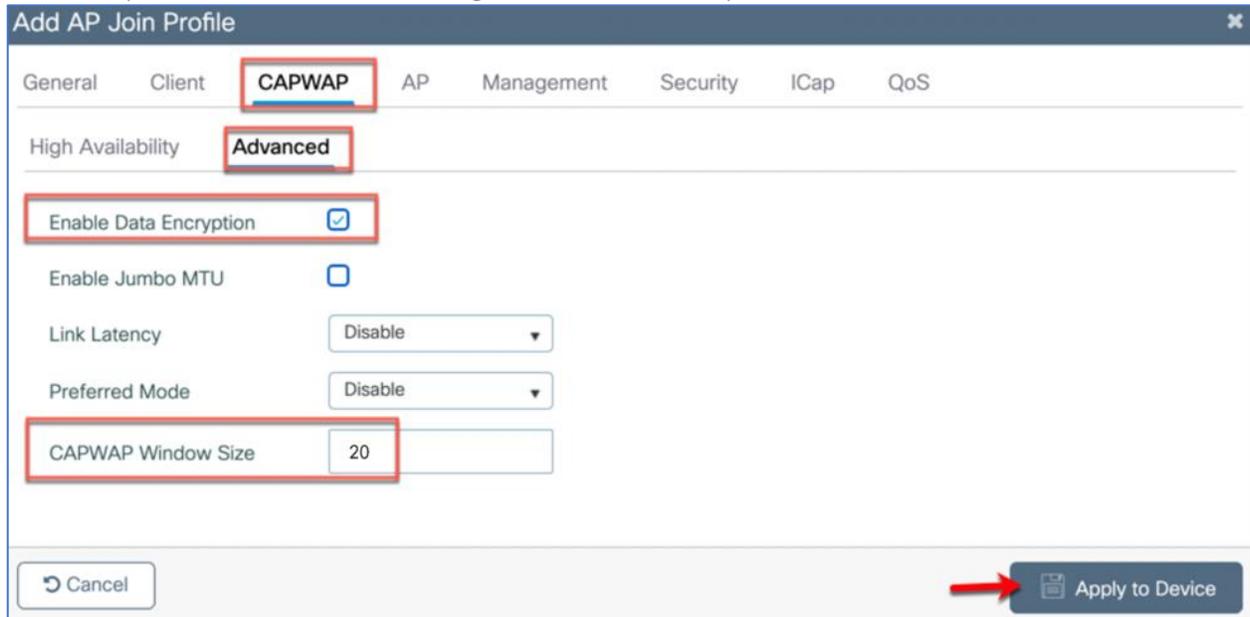
Go to **Advanced tab** and **Enable Data Encryption** by checking the box and then click **Apply**. This is to secure the traffic traversing the internet is encrypted.

Admin can also configure the CAPWAP Windows Size option which gives a high-performance



boost for CAPWAP control in high latency links. Max value possible is 50 and the recommended Value is 20.

For example: It increases the AP image download time by at least 10 times

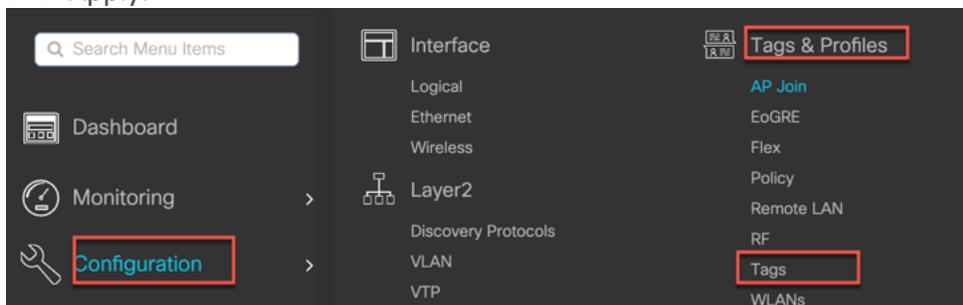


Configure Site Tag for Teleworker AP

OEAP mode is part of Flex profile and AP needs to be in flex connect mode for enabling the OEAP functionality, in order to do that the site tag needs to be configured for remote site.

Step 7: Go to **Configuration → Tags & Profiles → Tags** and click **+Add** a new Site tag for OEAP that is to be mapped to the Flex Profile from the previous step.

Make sure that **Enable Local Site** box is **unchecked** (this will convert the APs to FlexConnect when they inherit this tag). Then Name the site tag and select the AP Join Profile and Flex Profile then click **Apply**.



Edit Site Tag

Name* **2**

Description

AP Join Profile **3**

Flex Profile **4**

Fabric Control Plane Name

Enable Local Site **1**

6

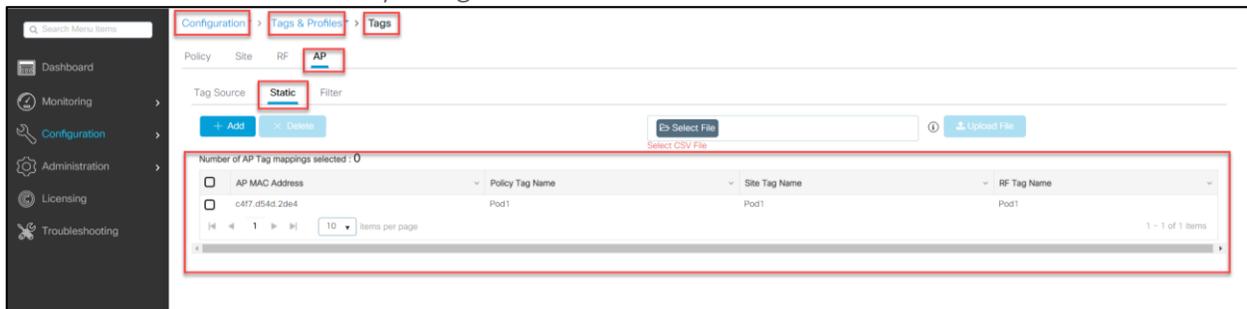
Tag the AP before AP Joins

Now the APs need to be tagged with the appropriate policy-tag, site-tag and rf-tag, once the APs join the WLC they can inherit those tags. There are multiple ways to associate tags to APs

Option 1: Admin can add the AP MAC Manually along with the TAG names

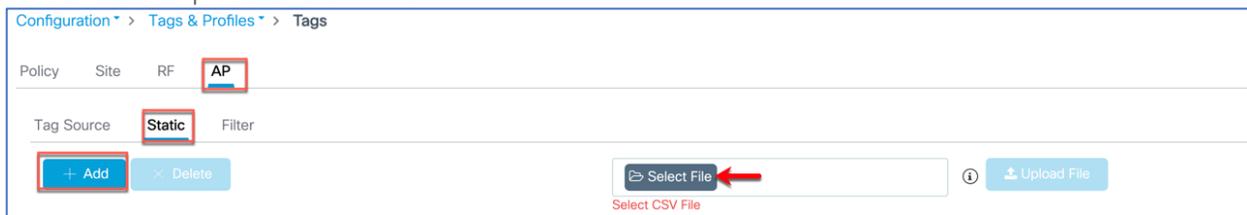
Note: The AP MAC is the Ethernet MAC which is available on the AP label

Step 8a: From WLC navigate to **Configuration > Tags & Profiles > Tags > AP > Static** click on **+Add** and add the AP MAC Manually along with the TAG names



Option 2: Admin can also import the CSV file with AP MAC and Tags. Sample CSV shown below

Step 8b: From WLC navigate to **Configuration > Tags & Profiles > Tags > AP > Static** click on the **Select File** to upload the CSV file





	A	B	C	D
1	AP04EB.409E.1056	Corp-Policy	OEAP-US	default-rf-profile
2	AP04EB.7503.20D4	Corp-Policy	OEAP-US	default-rf-profile
3	AP04EB.609D.892e	Corp-Policy	OEAP-US	default-rf-profile

CSV file should have the following columns.
AP MAC Address*,Policy Tag Name,Site Tag Name,RF Tag Name
(*Mandatory)

Option 3: Admin can also tag the APs through Filter Rule

Step 8c: From WLC navigate to **Configuration > Tags & Profiles > Tags > AP > Filter** click on **+Add** and enter the following then click **Apply to Device**

Rule Name: Admin configured name

AP name regex: The regular expression is to identify APs name (in the example AP* is used so any AP joining WLC with the name AP in it will inherit the respective tags)

Active: Yes/No

Priority: From 0-1023 with 0 being the highest

Policy Tag Name: Select the policy tag from the drop-down list

Site tag Name: Select the site tag from the drop-down list

RF tag Name: Select the site tag from the drop-down list

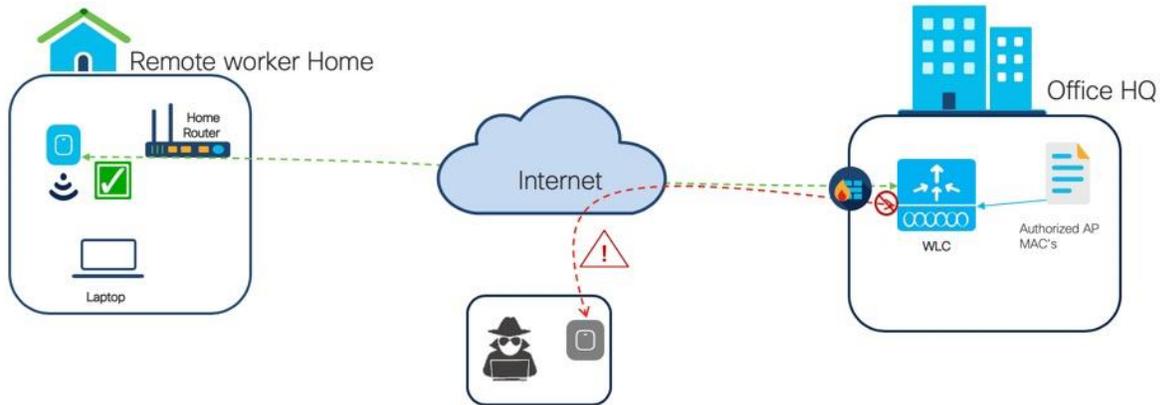
The screenshot shows the Cisco WLC configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > Tags. The 'AP' tab is selected, and the 'Filter' tag source is chosen. The '+ Add' button is highlighted. Below the table, the 'Associate Tags to AP' dialog box is open, showing the following configuration:

Rule Name*	TeleWorker-Site1	Policy Tag Name	OEAP-PolicyTag
AP name regex*	AP*	Site Tag Name	OEAP-SiteTag
Active	YES	RF Tag Name	default-rf-tag
Priority*	0		

The 'Apply to Device' button is highlighted with a red arrow.

Configuring AP Authentication (Optional)

Access point authentication ensures only authorized access points can connect to the controller. Since the WLC IP is Publicly reachable if access points know the WLC IP it will try to join to that WLC.



When admin want to control which access points can connect to the corporate WLC then AP authentication policy can be used to prevent unauthorized APs from joining WLC.

The AP can be authorized by the WLC either by the Serial Number of the AP or by the MAC address of the AP. AP Authorization by Serial Number involves less overhead, as it's easier to obtain the Serial Number from the Smart Account and secondly Cloud PnP uses the AP Serial Number to redirect to the AP to the WLC (The Cloud PnP is described in detail in a later section in this document).

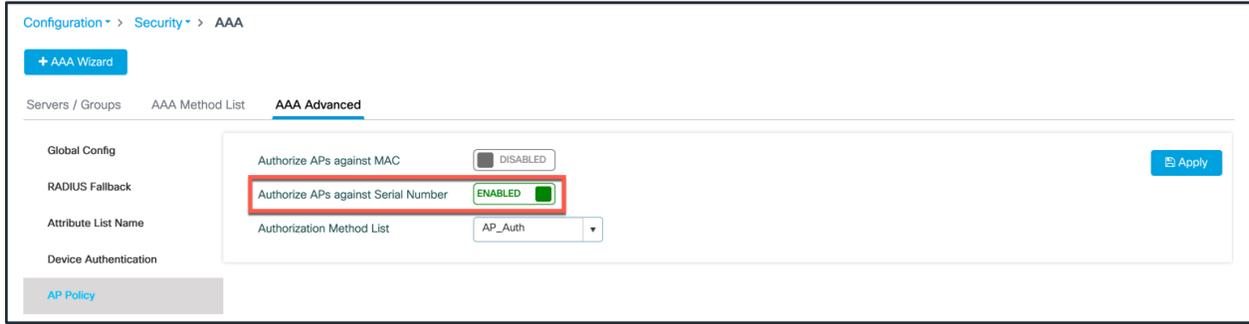
Note: AP Authorization by Serial Number is supported from IOS-XE Release 17.3.2

If admin want to allow any access point to connect to the Wireless LAN Controller, then skip this section.

Navigate to **Configuration>Security>AAA>AAA Advanced>AP Policy** and enable '**Authorize APs against Serial Number**' (or) '**Authorize APs against MAC**'.

Note: AP Authorization is either Serial Number or MAC and only one should be enabled. If both are enabled, then WLC expects the presence of both the Serial Number and the MAC Address of the AP to be in its database to authorize the AP.

AP Authorization against Serial Number:



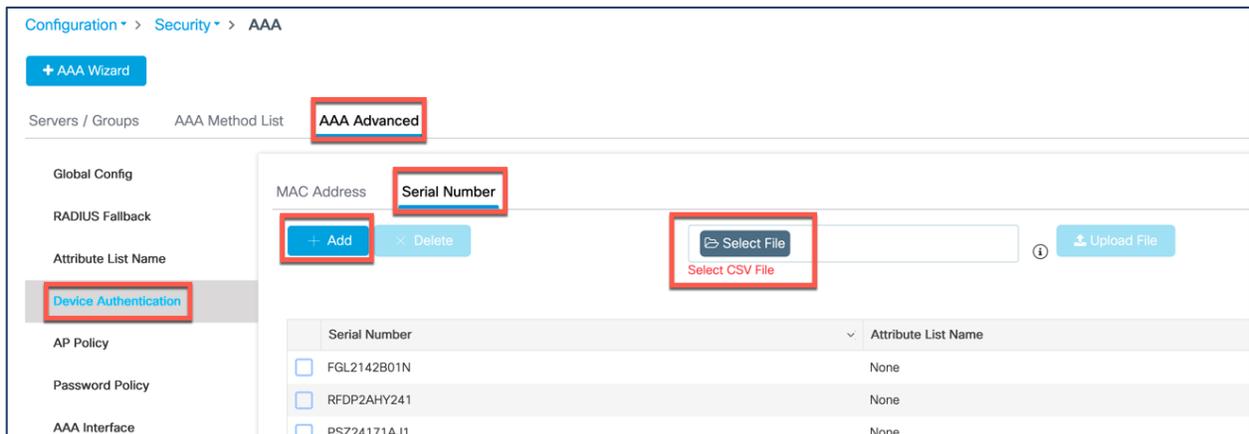
AP Authorization against MAC Address:



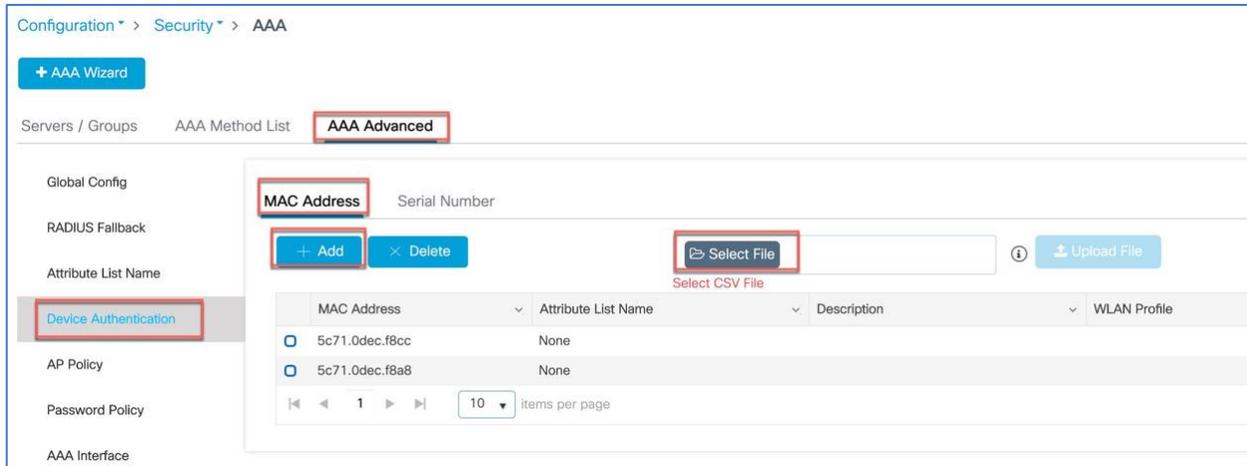
Ensure the Serial Number (or) the APs mac address are added to the WLC local database

From **Configuration>Security>AAA>AAA Advanced>Device Authentication** and add the Serial Number (or) Ethernet MAC address of the APs or upload a CSV file of Serial Number (or) device MAC addresses.

AP Device List addition with Serial Number:



AP Device List addition with MAC Address:



AP also can be externally authorized with ISE against MAC Address.

The following document provides the step by step details to enable AP authorization with ISE using MAC address.

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213916-catalyst-9800-wireless-controllers-ap-au.html>

Note: 17.3.2 supports only authorization of APs by ISE against MAC Address and does not support authorization of APs by Serial Number.

Configuring RF tag & profiles (Optional)

Admin can utilize the default-rf-tag or can create a custom RF profile and tag for teleworker deployment. Usually the teleworker home workplace is not a High-density RF environment and can be addressed with default-rf-tag with global RRM configuration.

Go to **Configuration > Radio Configuration > RRM > DCA** and set the Channel Width to 'Auto' and DBS Max Channel Width to **40 MHz** (40MHz should work for most cases)

Configuration > Radio Configurations > RRM

5 GHz Band 2.4 GHz Band FRA

General Coverage **DCA** TPC RF Grouping Spatial Reuse

Dynamic Channel Assignment Algorithm

Channel Assignment Mode

- Automatic
- Freeze Invoke Channel Update Once
- Off

Interval 10 minutes ▾

Anchortime 0 ▾

Avoid Foreign AP Interference

Avoid Cisco AP load

Avoid Non 5 GHz Noise

Avoid Persistent Non-wifi Interference

Channel Assignment Leader DMZ-C9800-CL2 (10.10.105.97)

Last Auto Channel Assignment 528 second(s) ago

DCA Channel Sensitivity medium ▾

Channel Width
 20 MHz 40 MHz 80 MHz 160 MHz Best

Dynamic Bandwidth Selection Max Channel Width
 20 MHz 40 MHz 80 MHz Max Allowed

Admin can also configure a custom rf profile to be tie it to rf tag for a particular teleworker site
 Navigate to **Configuration> Tags & Profiles> RF** and **+Add** to configure a new RF profile

Configuration > Tags & Profiles > RF

+ Add × Delete

From **General** tab name the RF profile and select the radio <2,4GHZ/5 GHz> and enable the status. Following example is of 5GHz radio band.



From General tab configure the name, Radio band as 2.4 GHz from the drop-down list and enable the Status.

Field	Value
Name*	OEAP-24gh
Radio Band	2.4 GHz Band
Status	ENABLE <input checked="" type="checkbox"/>
Description	OEAP RF profile for 2.4GHZ radio

Here go to 802.11 tab disable 802.11b rates and enable 6 Mbps as mandatory rate

Operational Rates	802.11n MCS Rates
1 Mbps: Disabled	Enabled Data Rates: [0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31]
2 Mbps: Disabled	
5.5 Mbps: Disabled	
6 Mbps: Mandatory	
9 Mbps: Supported	
11 Mbps: Disabled	
12 Mbps: Supported	
18 Mbps: Supported	
24 Mbps: Mandatory	
36 Mbps: Supported	
48 Mbps: Supported	
54 Mbps: Supported	

Enable	MCS Index
<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	1
<input checked="" type="checkbox"/>	2
<input checked="" type="checkbox"/>	3
<input checked="" type="checkbox"/>	4
<input checked="" type="checkbox"/>	5
<input checked="" type="checkbox"/>	6
<input checked="" type="checkbox"/>	7
<input checked="" type="checkbox"/>	8
<input checked="" type="checkbox"/>	9

Similarly, Go to RRM>TPC tab set higher Minimum power level or e.g. 11

General 802.11 **RRM** Advanced

General Coverage **TPC** DCA

Transmit Power Control

Maximum Power Level(dBm)*

Minimum Power Level(dBm)*

Power Threshold V1(dBm)*

From RRM>DCA tab disable the Avoid AP Foreign AP interference then click 'Apply to Device'

General 802.11 **RRM** Advanced

General Coverage TPC **DCA** Band Select

Dynamic Channel Assignment

Avoid AP Foreign AP Interference

DCA Channels 1 2 3 4 5 6 7 8 9 10 11 12 13 14

Once the RF profiles are configured, admin can attach them to a RF tag

Configuration > Tags & Profiles > RF

[+ Add](#) [x Delete](#)

	State	RF Profile Name	Band	Description
<input type="checkbox"/>		OEAP-5gh	5 GHz	OEAP rprofile for 5gh radio
<input type="checkbox"/>		OEAP-24gh	2.4 GHz	OEAP rprofile for 2.4gh radio

Go to Configuration>Tags & Profiles> Tags> RF> click +Add to create a RF Tag

Configuration > Tags & Profiles > Tags

Policy Site **RF** AP

[+ Add](#) [x Delete](#)

From the Add RF Tag window configure the Name and select the RF profiles from the 5/2.4 GHZ Band RF Profile drop-down list. Then click "Apply to Device"



Add RF Tag ✕

Name*	<input type="text" value="teleworker-rf-tag"/>
Description	<input type="text" value="Teleworker RF"/>
5 GHz Band RF Profile	<input type="text" value="OEAP-5gh"/> ▼
2.4 GHz Band RF Profile	<input type="text" value="OEAP-24gh"/> ▼

Admin can apply this RF tag to Teleworker APs as shown in the Tag the AP section above in this document.



Cisco Network Plug and Play (PnP) for Teleworker Deployment

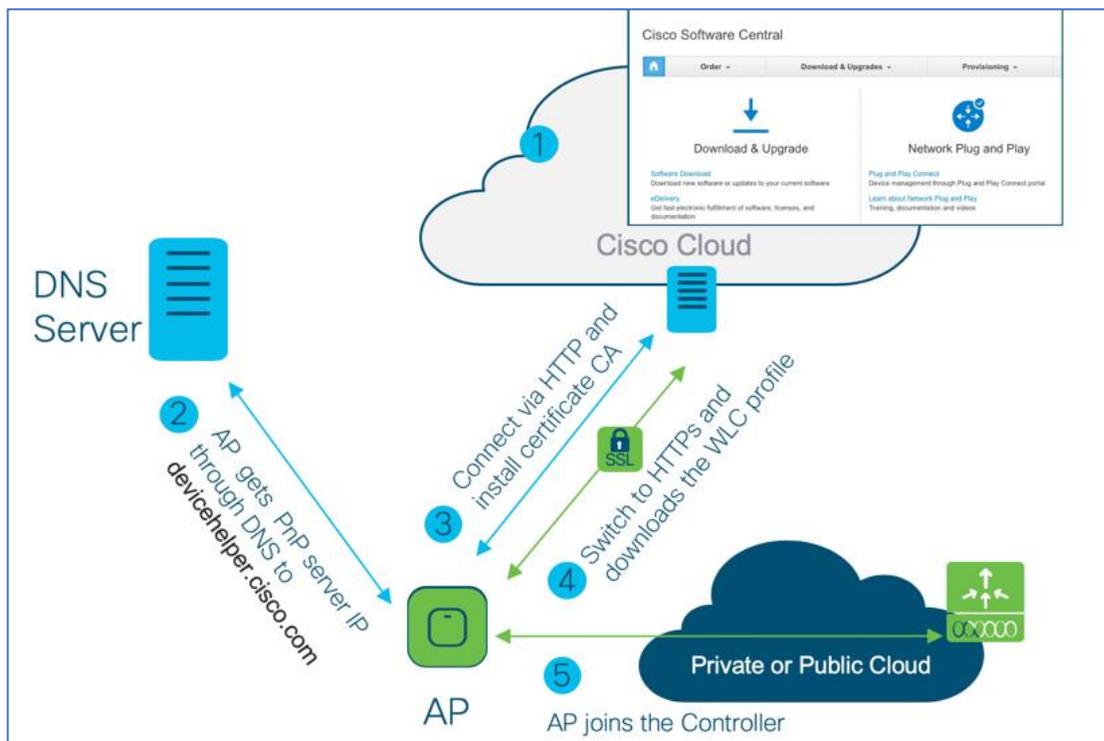
Cisco Network Plug and Play solution provides a simple, secure, unified, and integrated offering for enterprise network customers to ease new site rollouts for provisioning Cisco Access points. This solution allows use of Cloud Redirection service, which provide a unified approach to provision enterprise networks comprised of Cisco Access Points, Cisco routers, switches, with a near zero touch deployment experience.

You can use the Cisco Network Plug and Play portal to pre-provision the site and add Cisco access points to the site. This includes entering access point information to the device list and setting a controller profile (which contains WLC info like WLC public IP address)

When a teleworker /employee is provided with the teleworker AP and he powers up the access point, it auto-discovers the Cloud PNP server by using the DNS /cloud redirection service through devicehelper.cisco.com.

After the auto-discovery process is complete, the AP gets the WLC IP information from the controller profile on the Cloud PNP and then try to join the WLC.

Figure 2. Cloud PnP Workflow





Prerequisites

1. Cisco Smart account registration to access Cisco Network Plug and Play
2. Access Points–Cisco 802.11ac Wave 2 (indoor) and 11ax access out-of-box or factory reset to defaults. (APs should not have the previous WLC joined information otherwise PnP agent would not start)
3. Controller Configuration–WLC public IP address to be uploaded on Network PnP portal <https://software.cisco.com/>
4. AP should be configured with DNS server information through the local DHCP and be able to resolve and connect to devicehelper.cisco.com

Cloud Plug and Play Connect redirect to WLC

Cloud re-direction service uses Cisco Cloud PnP to re-direct Cisco access points to Cisco WLC. The minimal requirement is that the Access Points network have DHCP, DNS, and connectivity reachable to Cisco Cloud PnP.

Cloud Plug and Play Device Provisioning

This section describes the steps to redirect Cisco Access Points to Cisco WLC using Cloud Plug and Play Connect service.

To configure cloud Plug and Play connect redirect service, perform the following steps:

1. Create a Smart Account
2. Create Controller Profile
3. Adding Access Point to the devices list
4. Associate Access Point to Controller profile

Create a Smart Account

Step 1: Go to <http://software.cisco.com>



Step 2: Request a Smart Account or Log In (existing Smart Account holders)

The screenshot shows the Cisco Software Central interface. At the top, there is a navigation bar with the Cisco logo, a search icon, and language settings (AA, US, EN). A blue banner at the top right contains the text: "For faster routing of software licensing issues and final resolution, open a case with Support Case Manager (SCM) at <http://www.cisco.com/go/scm>. [Learn How!](#)".

The main content area is divided into several sections:

- Download & Upgrade:** Includes links for Software Download, eDelivery, Version Upgrade using MCE (marked as New), and Upgradeable Products.
- Network Plug and Play:** Includes links for Plug and Play Connect, Learn about Network Plug and Play, and Training, documentation and videos.
- License:** Includes links for Traditional Licensing, Smart Software Licensing, Enterprise Agreements, and View My Consumption.
- Order:** Includes links for Buy Directly from Cisco and End User License and SAAS Terms.
- Administration:** This section is highlighted with a red border and contains two columns of links:
 - All Users:** Get a Smart Account, Request Access to an Existing Smart Account, Manage Smart Account, and Learn about Smart Accounts.
 - Additional for Partners:** Request a Partner Holding Account, Request a Smart Account for your Customer, and Manage Pending Smart Accounts.

Create a Controller Profile

Step 1: Go to <http://software.cisco.com> and login via cisco.com account

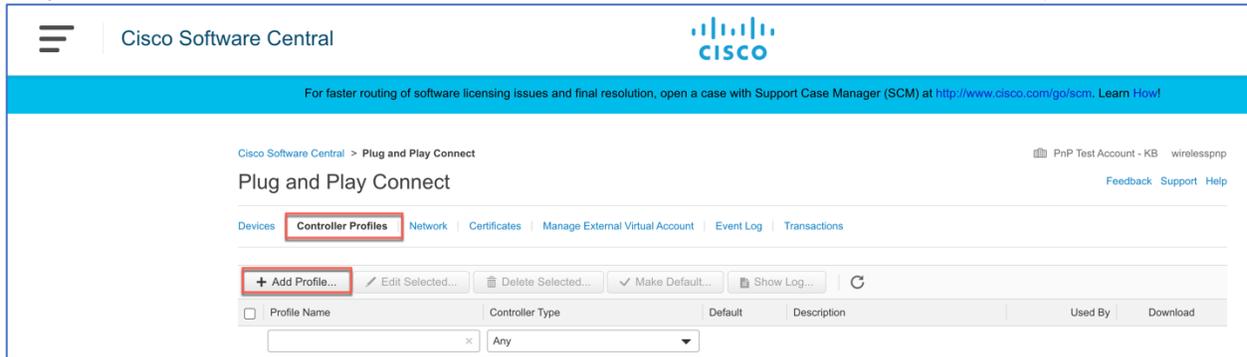
Step 2: Navigate to **Network Plug and Play > Plug and Play Connect**

This screenshot shows the "Network Plug and Play" section of the Cisco Software Central interface. The "Network Plug and Play" card is highlighted with a red border. Inside this card, the "Plug and Play Connect" link is also highlighted with a red border. The card contains the following text:

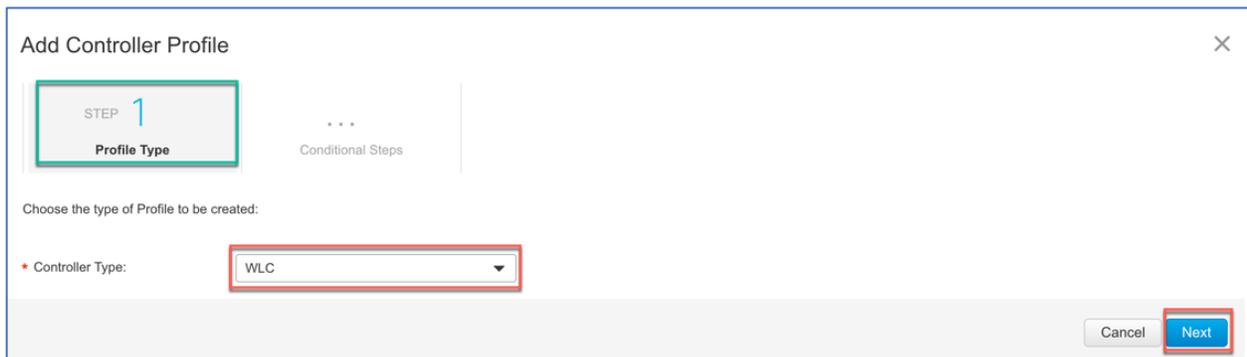
- Plug and Play Connect**
- Device management through Plug and Play Connect portal
- [Learn about Network Plug and Play](#)
- Training, documentation and videos



Step 3: Then click on **Controller Profiles > + Add Profile** to create a new controller profile



Step 4: Select **Controller Type** as **WLC** (IOS-XE or AireOS) from the drop-down list and click on **Next**.



Step 5: Enter the following and click **Next**.

Profile Name: Admin configured name

Description (optional): Admin configured description

Primary Controller: Select IPv4/IPv6 and enter the Public IP address of the WLC. Hostname/FQDN or URL is not supported.

Add Controller Profile

STEP 1 ✓ Profile Type | **STEP 2 Profile Settings** | STEP 3 Review | STEP 4 Confirmation

Profile Settings:

- Profile Name:
- Description:
- Default Profile:
- Deployment Type:
- Primary Controller:
- Secondary Controller:

Cancel Back **Next**

Step 6: Review the entries and click on Submit button to add the Controller Profile and finally the confirmation message will appear that the controller profile was successfully created then click Done.

Add Controller Profile

STEP 1 ✓ Profile Type | STEP 2 ✓ Profile Settings | **STEP 3 Review** | STEP 4 Confirmation

Review the following options to make sure they are correct before you Submit the changes.

Profile Type: Controller Type: WLC

Profile Settings:

- Profile Name: OEAP-SITE1
- Description: OEAP-USA Location
- deploymentType: Customer Hosted
- Primary IPv4 Address: 128.1.1.1

Cancel Back **Submit**

Add Controller Profile

STEP 1 ✓ Profile Type | STEP 2 ✓ Profile Settings | STEP 3 ✓ Review | **STEP 4 Confirmation**

✓ The controller profile "OEAP-SITE1" was successfully created.

Done

The created profile will appear in the Controller Profile list
 © 2020 Cisco Systems, Inc. All rights reserved.



Cisco Software Central > Plug and Play Connect

PnP Test Account - KB wirelesspnp

Plug and Play Connect

Feedback Support Help

Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account | Event Log | Transactions

+ Add Profile... Edit Selected... Delete Selected... Make Default... Show Log...

<input type="checkbox"/>	Profile Name	Controller Type	Default	Description	Used By	Download
<input type="checkbox"/>	OEAP-SITE1	WLC		OEAP-USA Location	0	--

Adding Cisco Access Point to the Devices List

Step 1: Navigate to **Plug and Play Connect** then click on **Devices** tab.

Step 2: Click on **+Add Devices** button to add a new device

Cisco Software Central > Plug and Play Connect

PnP Test Account - KB wirelesspnp

Plug and Play Connect

Feedback Support Help

Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account | Event Log | Transactions

+ Add Devices... + Add Software Devices... Edit Selected... Delete Selected... Enable External Management... Transfer selected...

<input type="checkbox"/>	Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
<input type="checkbox"/>			Any	Any	Select Range	Any	Clear Filters

Step 3: Import a CSV file with the Device info or select Enter Device info manually option.

Click Next. User can download a sample csv file to enter the devices info.

Note: In CCW there is a default option that will add the device in PNP Cloud automatically, unless the user disables it.



Cisco Software Central > Plug and Play Connect PnP Test Account - KB wirelesspnp

Plug and Play Connect

[Feedback](#) [Support](#) [Help](#)

[Devices](#) | [Controller Profiles](#) | [Network](#) | [Certificates](#) | [Manage External Virtual Account](#) | [Event Log](#) | [Transactions](#)

Add Device(s)

STEP 1
Identify Source

STEP 2
Identify Device(s)

STEP 3
Review & Submit

STEP 4
Results

Identify Source [Download Sample CSV](#)

Select one of the following two options to add devices:

Import using a CSV file

Enter Device info manually

Step 4: Click on +Identify Device button. The Identify Device window will pop up. Enter Serial Number, select Base PID from the drop-down list, and Controller Profile (created earlier) or from previously created profiles. Click on the **Save** button followed by **Next** button.

Plug and Play Connect [Feedback](#) [Support](#) [Help](#)

[Devices](#) | [Controller Profiles](#) | [Network](#) | [Certificates](#) | [Manage External Virtual Account](#) | [Event Log](#) | [Transactions](#)

Add Device(s)

STEP 1 ✓
Identify Source

STEP 2
Identify Device(s)

STEP 3
Review & Submit

STEP 4
Results

Identify Devices

Enter device details by clicking Identify Device button and click Next to proceed to the next step. 0 All | 0 Valid | 0 Errors | 0 Existing

Row	Serial Number	Base PID	Certificate Serial Number	SDWAN Type	Controller	Description	Actions
No Devices to display.							



Identify Device

Serial Number: PSZ23461UG

Base PID: C9105AXI-B

Certificate Serial Number: ex. 01E9478D

Controller Profile: OEAP-SITE1

Description: Enter short optional description for this device.

Add Additional SUDI

SUDI Serial Number	Certificate Serial Number	Actions
No Devices to display.		

Cancel Save

Add Device(s)

STEP 1 Identify Source ✓

STEP 2 Identify Device(s)

STEP 3 Review & Submit

STEP 4 Results

Identify Devices

Enter device details by clicking Identify Device button and click Next to proceed to the next step.

1 All | 1 Valid | 0 Errors | 0 Existing

+ Identify Device...

Row	Serial Number	Base PID	Certificate Serial Number	SDWAN Type	Controller	Description	Actions
1	PSZ234619UG	C9105AXI-B	--	--	OEAP-SITE1	--	

Showing 1 Record

Cancel Back Next

Step 5: Review the entries and click on **Submit** button to add the Device.

Add Device(s)

STEP 1 Identify Source ✓

STEP 2 Identify Device(s) ✓

STEP 3 Review & Submit

STEP 4 Results

Review & Submit

Submit action will submit following 1 newly identified device(s).

Row	Serial Number	Base PID	Certificate Serial Number	SDWAN Type	Controller	Description
1	PSZ234619UG	C9105AXI-B	--	--	OEAP-SITE1	--

Showing 1 Record

Cancel Back Submit

Step 6: Once the device is successfully added then click **Done**.



Add Device(s)

STEP 1 ✓ Identify Source | STEP 2 ✓ Identify Device(s) | STEP 3 ✓ Review & Submit | **STEP 4 Results**

Attempted to add 1 device(s)

✓ **Successfully added 1 device(s) !**
It may take a few minutes for the new devices to show up in the Devices table. Please wait a minute or two and refresh the page as needed.

[Done](#)

Step 7: Verify that the Device has been added and the status is “Pending (Redirection)” in orange. When the device redirection is successful the status will show “Redirect Successful”

The AP will get the WLC information from Cisco PnP Connect and will then join the respective WLC.

Cisco Software Central > Plug and Play Connect PnP Test Account - KB wirelesspnp

Plug and Play Connect [Feedback](#) [Support](#) [Help](#)

[Devices](#) | [Controller Profiles](#) | [Network](#) | [Certificates](#) | [Manage External Virtual Account](#) | [Event Log](#) | [Transactions](#)

[+ Add Devices...](#) [+ Add Software Devices...](#) [Edit Selected...](#) [Delete Selected...](#) [Enable External Management...](#) [Transfer selected...](#) [Refresh](#)

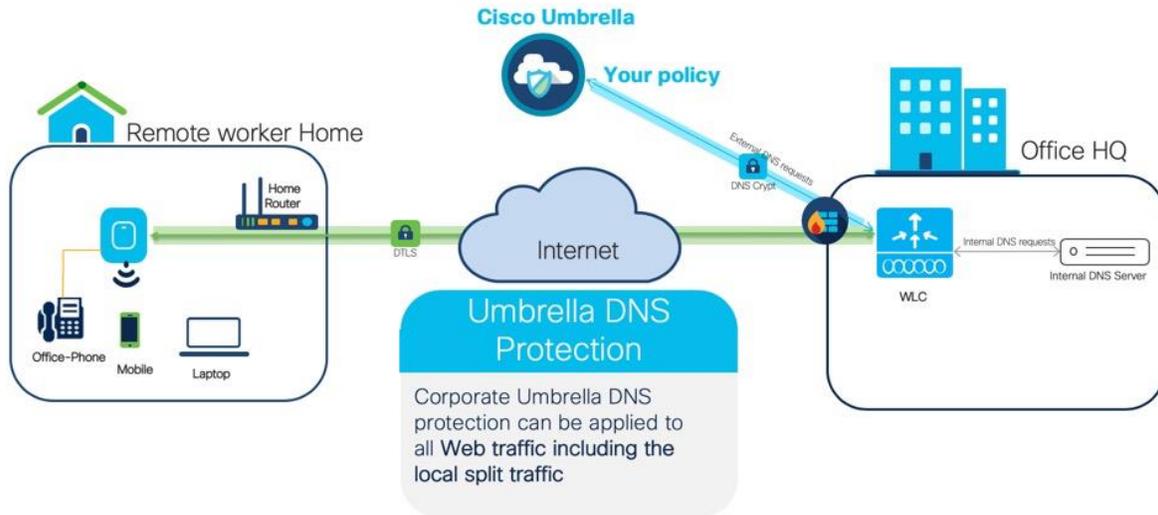
<input type="checkbox"/>	Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
<input type="checkbox"/>	PS2234619UG	C9105AXI-B	Access Point	OEAP-SITE1	2020-Jul-14, 22:22:51	Pending (Redirection)	Show Log... ▼
<input type="checkbox"/>	FCW2214N4FU OEAP	AIR-AP1815I-B-K9	Access Point	OEAP-WLC-PROFILE	2020-Jun-17, 01:06:25	Redirect Successful	Show Log... ▼

Showing All 2 Records



Umbrella for Teleworker WLAN

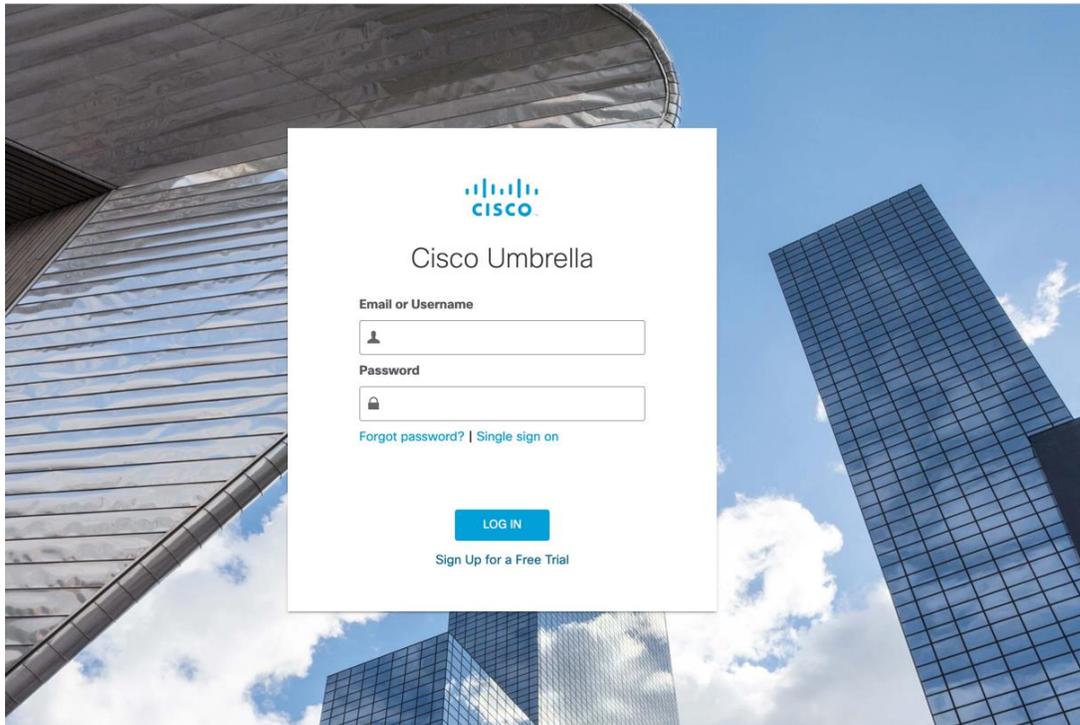
Cisco Umbrella is a Cloud delivered network security service, which gives insights to protect devices from malware and breach protection in real time. It uses evolving big data and data mining methods to proactively predict attacks also do category-based filtering. This is not specific to Teleworker but can be you utilized to have an added protection of the corporate clients.



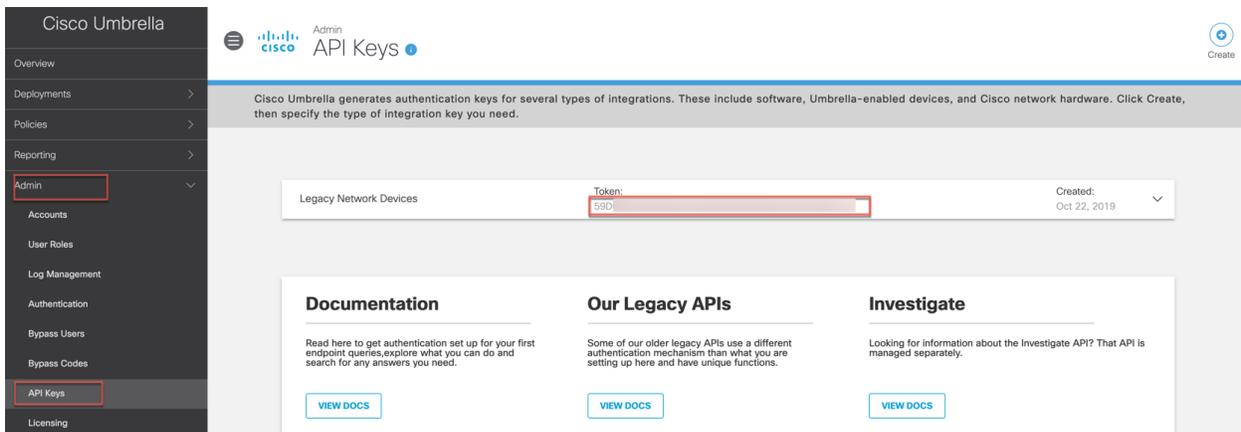
Prerequisites:

- Cisco Umbrella provisioning involves creating a user account on Cisco Umbrella cloud. Subscription is per account and Cisco Umbrella offers 14-day obligation free trial license.
- Permanent License is covered under DNA Advantage license Subscription.
- WLC direct reachability to the Internet or through the proxy server.

Step 1: Login to your account at <https://login.umbrella.com/>



Step 2: From Cisco Umbrella main dashboard landing page, go to **Admin>API** on copy the API TOKEN as shown below.



Step 3: From WLC navigate to **Configuration>Security> Threat Defense>Umbrella**. Enter Umbrella API Token to register
Admin can also define the corporate internal sites or list the domains for DNS splitting.
In Whitelist Domains add the domain names or a regex name which needs to be internally split and hit Enter key.
By default, Umbrella Parameter Map is set to **'global'** but admin can define custom umbrella parameter map by assigning a name and hit Enter key. Then click **Apply**



Configuration > Security > Threat Defense > umbrella

[Unconfigure Umbrella](#)

Registration Token* [Click here to get your Token](#)

Organization ID 2029748

Whitelist Domains

Enable DNS packets encryption

Umbrella Parameter Map

[Apply](#)

Note: Refresh the page to verify the Organization ID is not stating 'None' if it is this means that the device did not register to Umbrella cloud.

Step 4: Now go to **Configuration>Tags & Profiles>Policy** and click on policy profile name on which admin wants to configure umbrella parameter map and then go to **Advanced tab** Select the **Umbrella Parameter Map** from the drop-down list.

DNS traffic redirect state to Force (even if user try to change the device DNS manually on the client it would always use Umbrella DNS)

Then click **"Update & Apply to Device"** button

Note: Admin can also configure QoS & AVC policies as well for a particular Policy Profile.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg/quality-of-service.html



Configuration > Tags & Profiles > Policy

General Access Policies QoS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec) 1800

Idle Timeout (sec) 300

Idle Threshold (bytes) 0

Client Exclusion Timeout (sec) 60

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

NAC Type RADIUS

Policy Name default-aaa-policy

Umbrella

Fabric Profile Search or Select

mDNS Service Policy default-mdns-service

Hotspot Server Search or Select

User Defined (Private) Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map Teleworker-Umbrella

Flex DHCP Option for DNS DISABLED

DNS Traffic Redirect FORCE

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL Search or Select

Air Time Fairness Policies

Cancel Update & Apply to Device

On Cisco Umbrella admin can attach this Parameter Map profile to the Umbrella Cloud policies to do category-based filtering on sites and domains to allow, deny or just monitor the devices accessing the internet.

For Umbrella Policies creation and configurations please visit the umbrella docs

<https://docs.umbrella.com/deployment-umbrella/docs>

<https://docs.umbrella.com/deployment-umbrella/docs/create-and-apply-policies>

Cisco Umbrella

Overview

Deployments

Policies

Management

All Policies

Policy Components

Destination Lists

Content Categories

Application Settings

Security Settings

Block Page Appearance

Reporting

Admin

Ali Ali
ENG - Training

Sorted by Order of Enforcement

1 TeleWorker-Policy Applied To 1 Identity Contains 4 Policy Settings Last Modified Jul 16, 2020

What would you like to protect?

Select Identities

Search Identities

All Identities / Network Devices

pod3-ewc

pod4-ewc

pod5-ewc

pod6-ewc

pod7-ewc

pod8-ewc

pod9-ewc

Teleworker-Umbrella

1 Selected REMOVE ALL

Teleworker-Umbrella

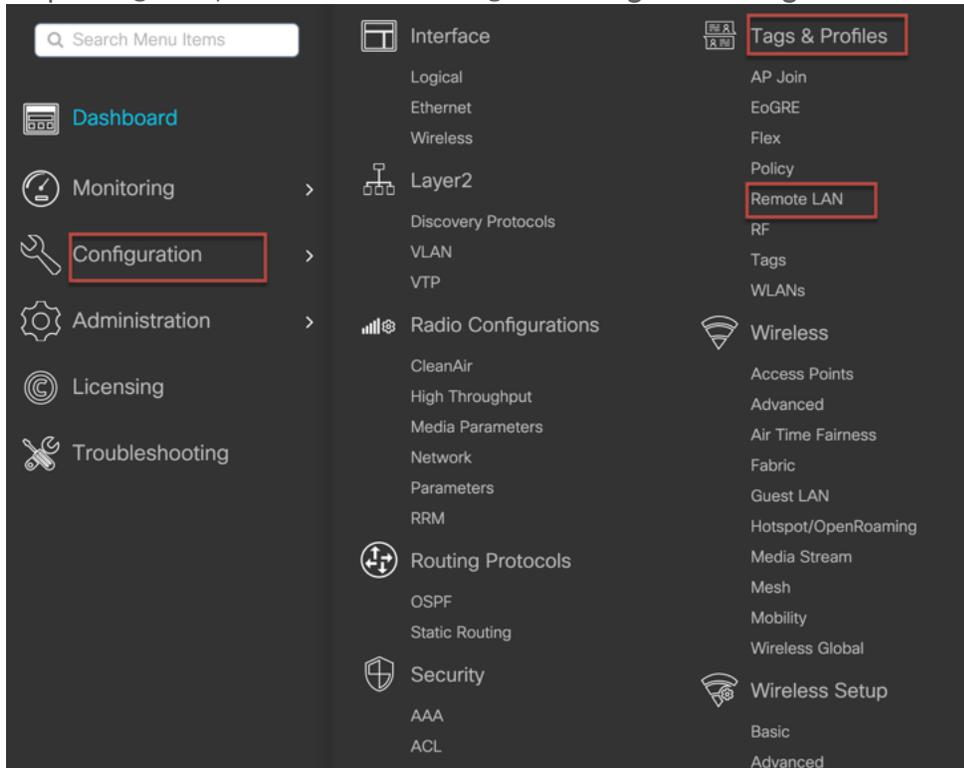
CANCEL SET & RETURN



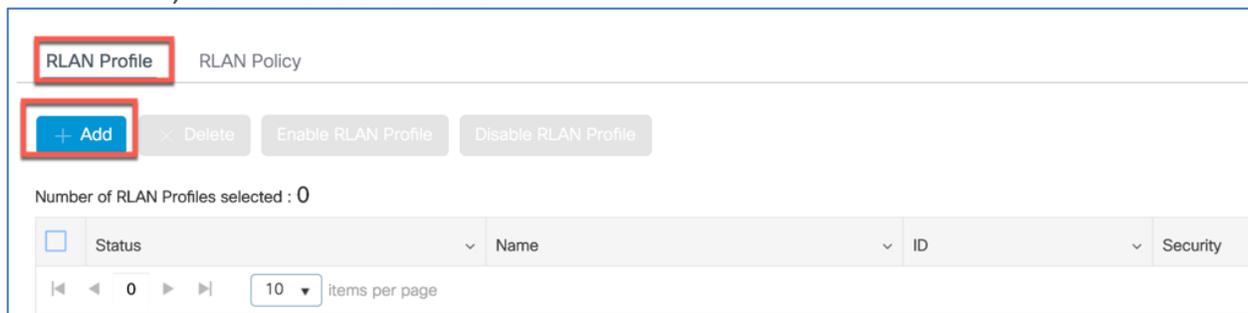
Configuring the Remote LAN(RLAN)

A remote LAN is similar to a WLAN except it is mapped to one of the Ethernet ports on the back of the Cisco Access Point.

Step 1: Login to your C9800 WLC and go to **Configuration>Tags & Profiles> Remote LAN**



Step 2: From RLAN Profile tab click on **+Add** and then from **General** tab configure the RLAN Profile Name, RLAN ID and enable the **Status**



Add RLAN Profile

General Security

Profile Name*

RLAN ID*

Status ENABLED

Client Association Limit

mDNS Mode

Step 3: Go to the **Security>Layer2** user can Enable 802.1X or if kept disabled in it is open state with no authentication. User can also configure RLAN for webauth from Layer3 tab. In this example we are using 802.1X.

From the Authentication List select the Radius server and click **“Apply to Device”**.

Note: The Radius server needs to be configured first if not already configured.

For Radius/AAA configuration on C9800 please refer to the following document

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214490-configure-radius-and-tacacs-for-gui-and.html>

Add RLAN Profile

General **Security**

Layer2 Layer3 AAA

802.1x ENABLED

MAC Filtering

Authentication List [Clear](#)



Configuration > Tags & Profiles > Remote LAN

RLAN Profile RLAN Policy

+ Add × Delete Enable RLAN Profile Disable RLAN Profile

Number of RLAN Profiles selected : 0

<input type="checkbox"/>	Status	Name	ID	Security
<input type="checkbox"/>	●	...-RLAN	1	[open]
<input type="checkbox"/>	●	...-RLAN	2	[open]
<input type="checkbox"/>	●	...-RLAN	3	[802.1X]
<input type="checkbox"/>	●	RLAN-1	4	[802.1X]

Configure Remote LAN Policy

Step 1: Select RLAN Policy tab and click +Add to configure RLAN policy.

Configuration > Tags & Profiles > Remote LAN

RLAN Profile **RLAN Policy**

+ Add × Delete

Step 2: From **General** tab configure the following

Policy Name: User define name

Status: User can enable to disable the policy,

PoE: Enables or disables PoE -If user want to enable PoE on RLAN port1 (PSE-LAN1) then check PoE box.

Enable Central Switching and DHCP and then click “Apply to Device”.

Add RLAN Policy

General Access Policies Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this policy.

Policy Name* **RLAN-dot1x**

Description Enter Description

Status **ENABLED**

PoE ←

Power Level 4

RLAN Switching Policy

Central Switching **ENABLED**

Central DHCP **ENABLED**

Step 3: From **Access Policies** tab configure the following



Select the VLAN: This VLAN will be used as egress point of Teleworker user’s Corporate Network access. i.e. wired clients connecting to this RLAN will be assigned the VLAN centrally from the 9800.

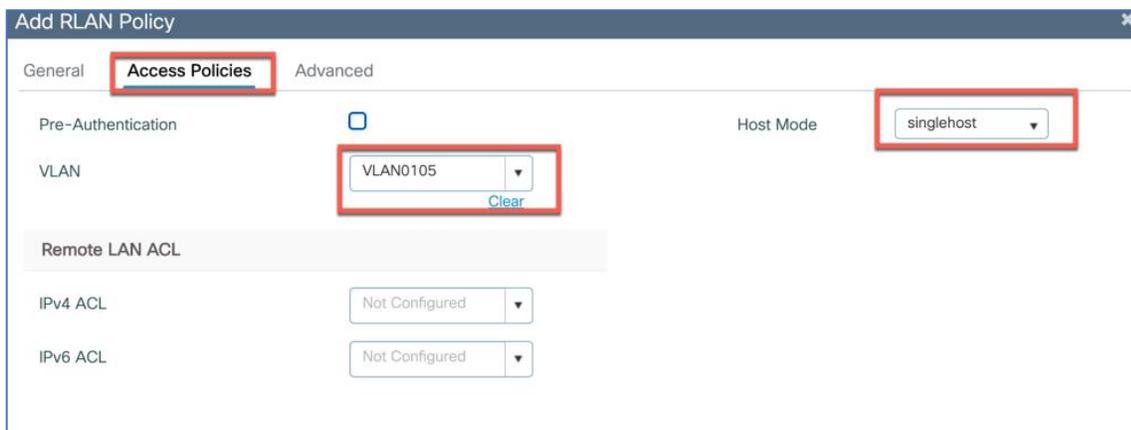
Select the Host mode: admin can choose the mode as singlehost, multihost or multidomain

Single-Host Mode—Is the default host mode. In this mode, the switch port allows only a single host to be authenticated and passes traffic one by one.

Multi-Host Mode—The first device to authenticate opens up to the switch port, so that all other devices can use the port. You need not authenticate other devices independently, if the authenticated device becomes authorized the switch port is closed.

Multi-Domain Mode—The authenticator allows one host from the data domain and another from the voice domain. This is a typical configuration on switch ports with IP phones connected.

Note: Multi-Domain Mode is not supported in the 17.3 release.



Note: For a RLAN profile with open-auth configuration, you must map the RLAN-policy with single host mode. Mapping RLAN-policy with multi-host or multi-domain mode is not supported. If the RLAN is used for IP phone the voice VLAN can be tied to the RLAN policy.

Step 4: From Advanced tab configure the following

Violation Mode: It is a port security method and replace is a default behavior.

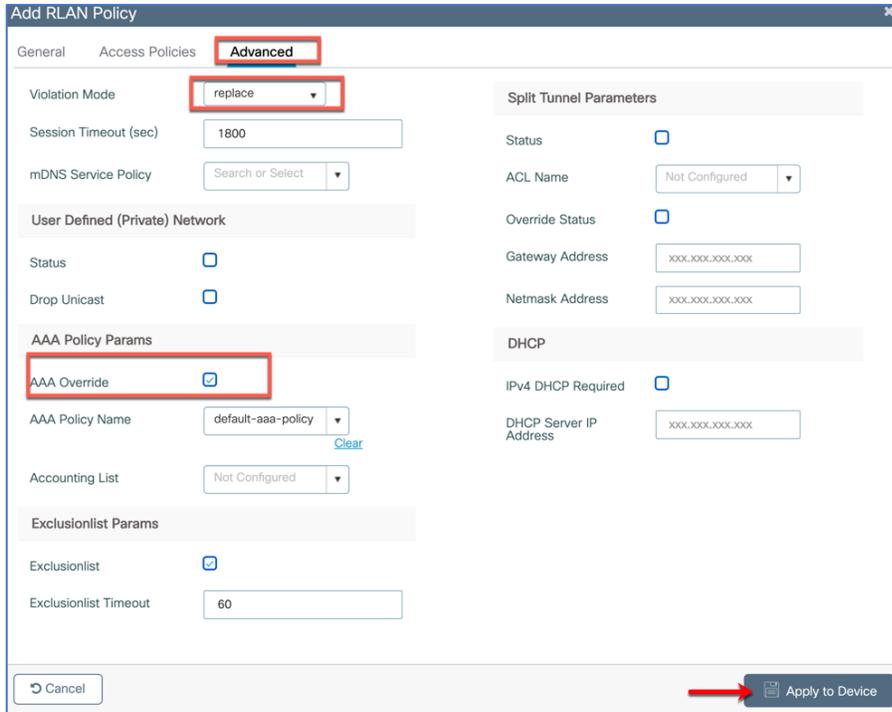
Replace—Removes the current session and initiates authentication for the new host.

Protect—Drops packets with unexpected MAC addresses without generating a system message.

Shutdown—Disables the port

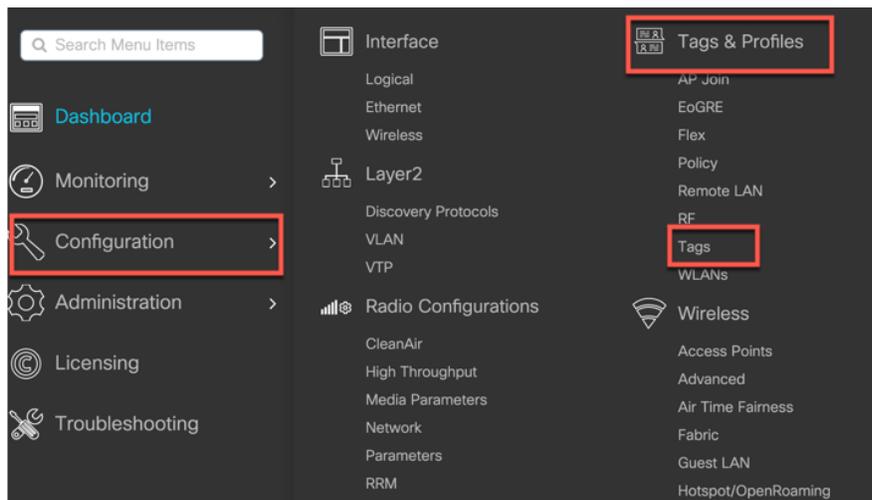
Check **AAA Override** if using Radius to send and attributes to override.

Click **‘Apply to Device’**



Adding WLANs/RLANs to a Policy Tag

Step 1: Go to Configuration > Tags & Profiles > Tags > Policy



Policy Tag helps in mapping the WLAN/RLAN profiles to the particular policy profile. Admin can create a new policy tag or use the pre-configured ones to add WLANs and RLANS.

Step 2: From the option **WLAN-POLICY Maps** user can use **+Add** to configure a new WLAN or apply pre-configured WLANs to policy profiles mapping.



Similarly, from **RLAN-POLICY Maps** click **+Add** and select the Port ID on which user want to apply the RLAN profile and also select the RLAN policy.

Note: Ports 1 and 2 are used as RLAN ports, Port 3 is a dedicated local port on C9105W and 1815T/W. User can connect their laptop to Port 3 to access internet and the local Teleworker AP configurations.

Then click on the tick “” to add the RLAN-Policy MAP



Note: RLAN is supported in APs that have more than one Ethernet port. For e.g. C9105W, OEAP1810/1810W/1815T/1815W/1850/2800/3800) AP4800 AUX port does not support RLAN. If RLAN port is connected to a switch or hub then only 4 devices can be connected behind it.

Step 3: Apply it by clicking “Apply to Device”

Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name* OEAP-PolicyTag

Description Teleworker Policy Tag

WLAN-POLICY Maps: 1

+ Add - Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> AA-Employee	OEAP-PP

1 - 1 of 1 items

RLAN-POLICY Maps: 1

+ Add - Delete

Port ID	RLAN Profile	RLAN Policy Profile
<input type="checkbox"/> 1	RLAN-1	RLAN-dot1x

1 - 1 of 1 items

Cancel Update & Apply to Device

The configured RLAN Policy will show the status enabled.



Configuration > Tags & Profiles > Remote LAN

RLAN Profile **RLAN Policy**

+ Add - Delete

Name	Status
RLAN-dot1x	✓

Step4: To enable the port on APs admin can go to the **Configuration>Wireless>Access Points** and select the Teleworker AP with the RLAN port then go to **Interfaces>LAN Port Settings** then select the LAN ports to enable/disable them or check the Status of the LAN Ports.

General **Interfaces** High Availability Inventory ICap Advanced Support Bundle

Radio Interfaces

Slot No	Interface	Band	Admin Status	Operation Status	Spectrum Admin Status	Spectrum Operation Status	Regulatory Domain
0	802.11n - 2.4 GHz	All	Enabled	⬇️	Disabled	⬇️	-A
1	802.11ac	All	Enabled	⬆️	Disabled	⬇️	-B

10 items per page 1 - 2 of 2 items

Power Over Ethernet Settings

Power Type/Mode: Power Injector/Normal Mode
PoE Pre-Standard Switch: Disabled
PoE Power Injector MAC Address: Disabled

USB Settings

USB Module Type: [blank]
USB Operational State: Enabled
USB Module State: [DISABLED]
USB Override: [DISABLED]

Link Aggregation (LAG)

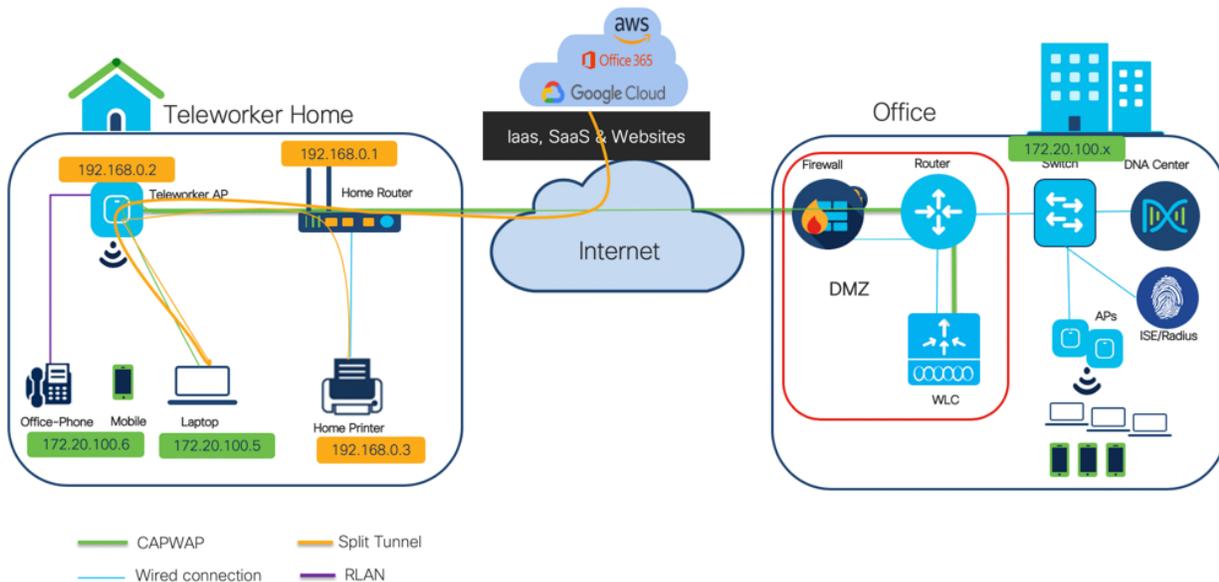
LAG Support for AP: No

LAN Port Settings

Port ID	Status	VLAN ID	PoE	Power Level	RLAN
LAN1	✓	105	✓	NA	✓
LAN2	✓	105	NA	NA	✓
LAN3	✓	0	NA	NA	⊘

Split Tunneling for Teleworker AP

Split Tunneling introduces a mechanism by which the traffic sent by the client will be classified, based on packet content, using ACLs. Matching packets are switched locally from Teleworker AP and the rest of the packets are centrally switched over CAPWAP.



Use Case 1: Local device access while connected to corporate network

The Split Tunneling functionality is an added advantage for Teleworker setup where clients on a Corporate SSID can talk to devices on a local network (printers, wired machine on a Remote LAN Port, or wireless devices on a Personal SSID) directly without consuming WAN bandwidth by sending packets over CAPWAP.

Use Case 2: CAPWAP data tunnel Optimization

Applications like webex-meetings, SharePoint, Office365, box, dropbox etc. all live in the cloud as a SaaS applications. Teleworkers use these daily as part of their work, to access these the traffic do not need to go all the way to the Corporate HQ network in the tunnel which can cause extra latency, to avoid this admin can use split-tunneling feature on WLC.

The way it can be achieved is by applying the split-tunnel to send only the corporate IP addresses



centrally and switch all other traffic locally. The split-ACL supported is a five tuple IP ACL (which can take IP, protocols and ports as part of ACL rules)

While crafting this ACL admin can make sure all the DNS traffic is centrally switched so that it gets the benefit of Umbrella security even for the traffic that is getting locally switched due to split ACL.

Creating Split-ACL

Navigate to **Configuration > Security > ACL** click **+Add** to create a new ACL of type IPv4 extended.

Note: when creating the ACL, a deny statement means “not splitting the traffic” so it’s traffic that is sent in the CAPWAP tunnel. A permit statement means permit the “splitting of that traffic” and hence the traffic exits locally at the AP. Therefore, admin can create a ‘Deny rule’ for centrally switched traffic and create a ‘Permit rule’ for locally switched traffic.

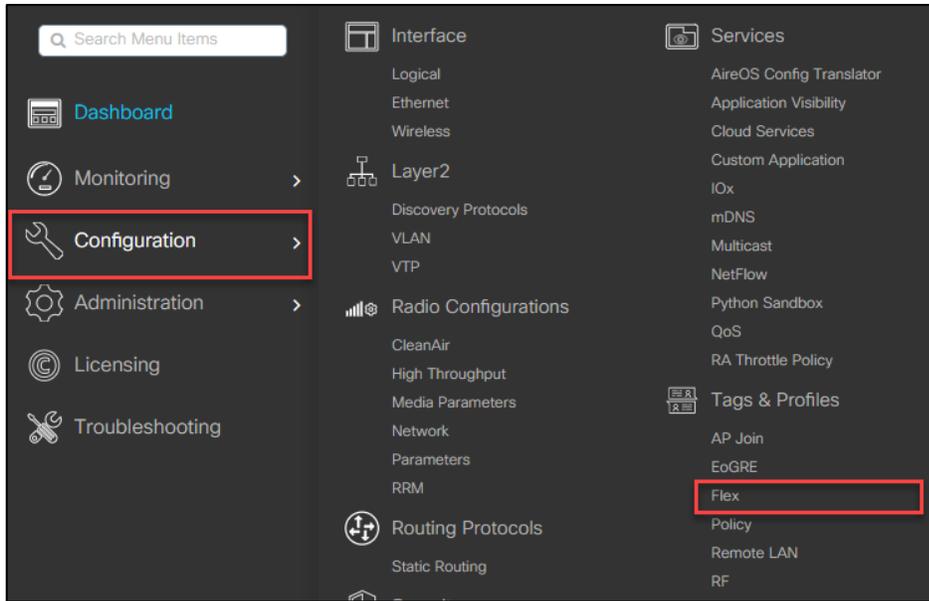
Create a deny rule for the centrally switched traffic- Corporate networks, DNS, TCP/UDP
Create a permit rule for the locally switched traffic -home network) and HTTP/HTTPS

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	deny	any		172.20.0.0	0.0.255.255	ip			None	Disabled
20	deny	any		10.10.0.0	0.0.255.255	ip			None	Disabled
25	deny	any		any		udp		eq domain	None	Disabled
26	deny	any		any		tcp		eq domain	None	Disabled
30	permit	any		any		tcp		eq www	None	Disabled
40	permit	any		any		tcp		eq 443	None	Disabled
45	permit	any		192.168.0.0	0.0.255.255	ip			None	Disabled
50	deny	any		any		ip			None	Disabled

Assigning the Split ACL on Flex Profile

Once the user has created the ACL it needs to be assigned to the flex profile so the APs for of the flex profile can download the split ACL.

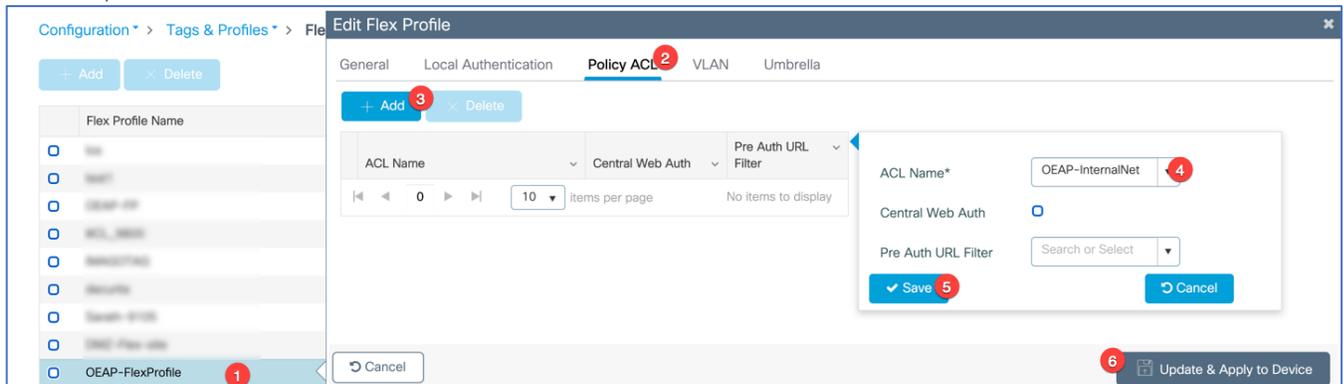
Step 1: Navigate to **Configuration > Tags & Profile > Flex**



Step 2: Click on the flex profile on which user want to apply the ACL to edit Flex Profile configuration

Navigate to **Policy ACL** > **Add** the select the ACL Name from the drop-down list click **Save and Update and Apply**

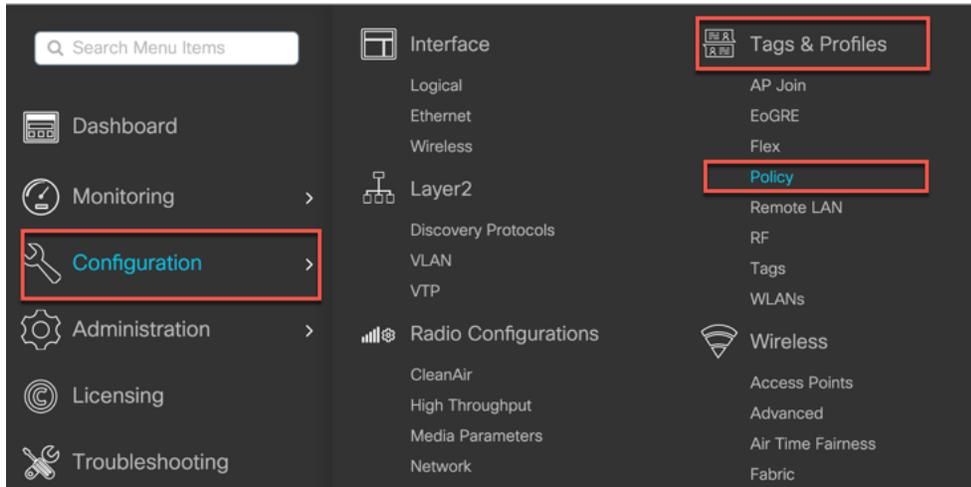
This helps the ACLs to be downloaded on to the AP's.



Assign the ACL as the Split mac ACL on policy profile

To apply the Split ACL we need to map it to the Policy Profile

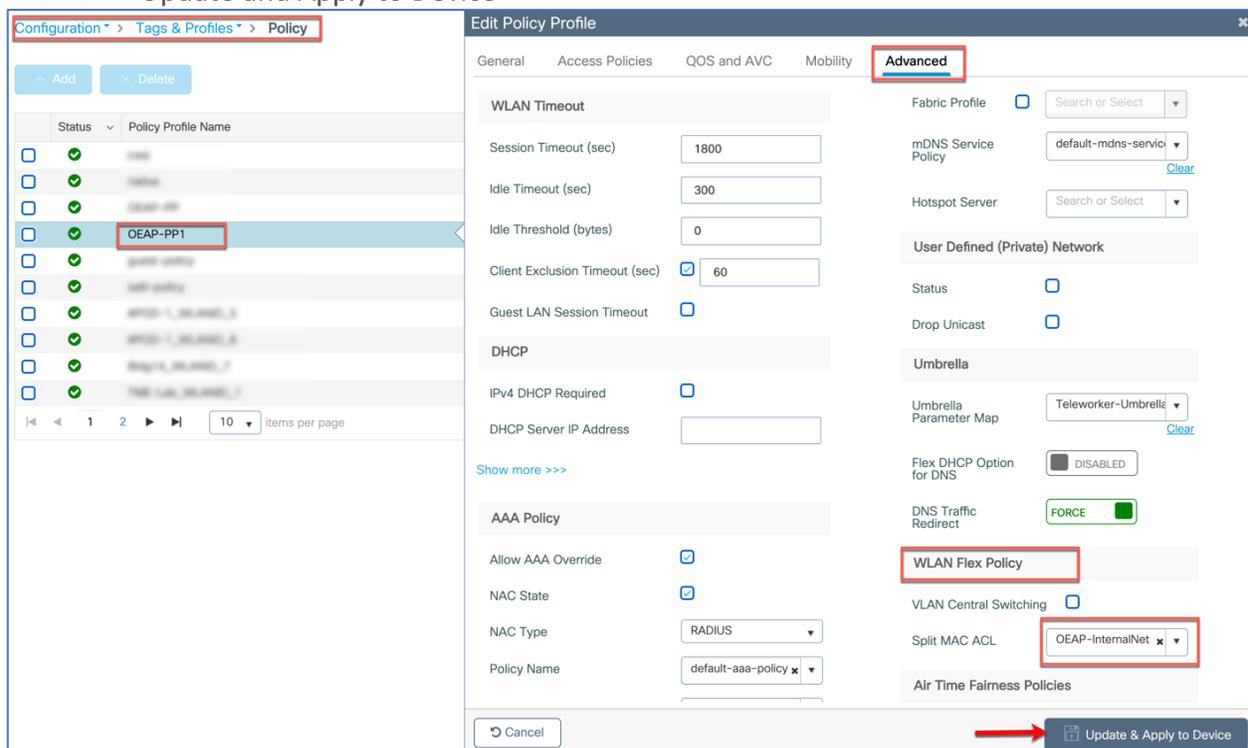
Step 1: Navigate to **Configuration > Tags & Profile > Policy**



Step 2: Click on the Policy Profile Name on which admin/user wants to configure Split ACL. In the Edit Policy Profile window navigate to Advanced tab.

Under **WLAN Flex Policy > Split MAC ACL** select the Split ACL (which admin created) from the drop-down list.

Then click **Update and Apply to Device**





Cisco Catalyst C9105W as Teleworker Access Point

The Cisco Catalyst C9105W Series Access Point offer a compact, wall plate-mountable access point, ideal for hospitality, cruise ships, residential halls or other multi-dwelling-unit deployments. The C9105W Series combines 802.11ax wireless and MultiGigabit Ethernet wired connectivity into a sleek device, built to take advantage of existing cabling infrastructure. This combination provides best in class performance while reducing total cost of ownership.

Cisco C9105W Access Point can be also used as dedicated Teleworker AP and supports a number of features:

Interfaces

- 1x 100/1000/2500 Multigigabit Ethernet (RJ-45)
- 3 x 100/1000 Gig Ethernet (RJ-45) – Port 1-2 (RLAN ports) & Port 3 (dedicated Local LAN port)
- 1 x Pass-through port
- Management console port (RJ-45)
- USB 2.0

DTLS

- Control–DTLS is enabled for Control
- Data–DTLS is enabled for client traffic tunneled back to the corporate Wireless LAN Controller

Authentication and Security

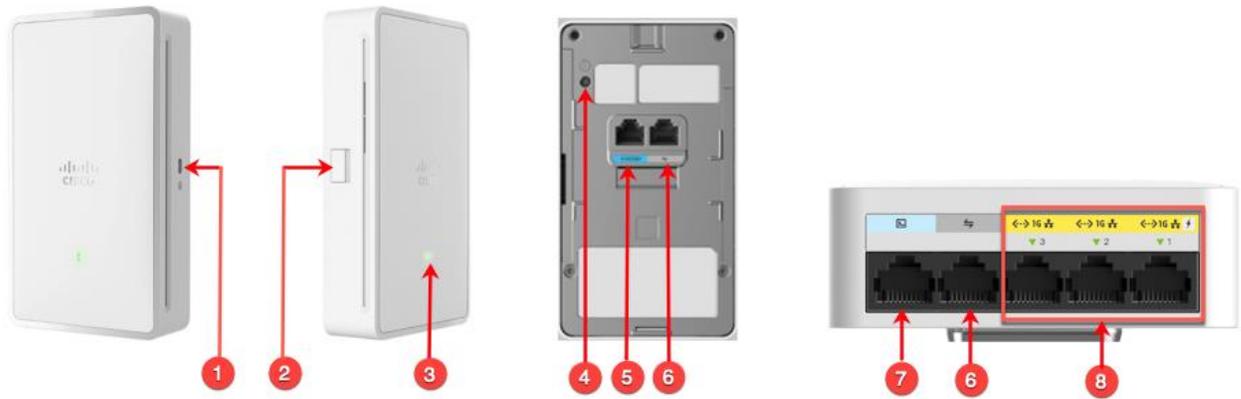
- Advanced Encryption Standard (AES) for Wi-Fi Protected Access (WPA2/WPA3)
- 802.1X, RADIUS authentication, authorization and accounting (AAA) on WLAN and RLAN
- 802.11i
- MAC filtering
- Rogue and WIPs

Personal SSID support

- Personal SSID support for local home networking
- LAN 3 is a dedicated local port for local AP access

WLAN and RLAN

A total of 8 WLANs and 2 RLANs are supported on Cisco Teleworker APs. One can have more than 8 WLANs associated on the Site-Tag(C9800) / AP group (AireOS) but only the first 8 WLANs would be usable.



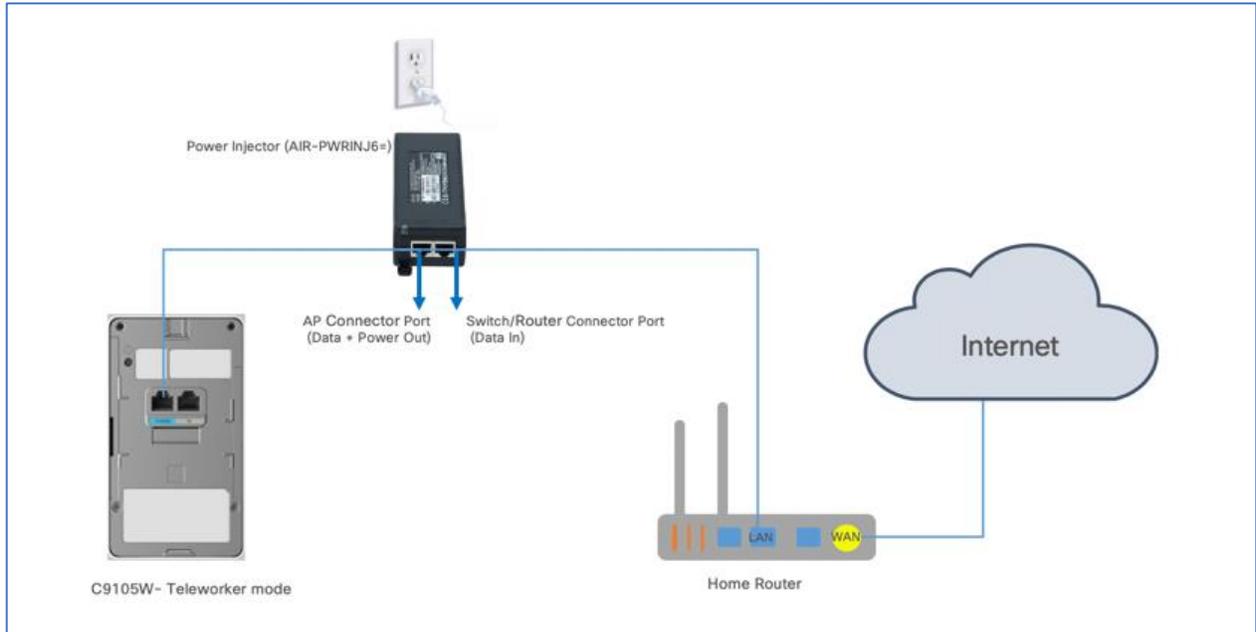
Interfaces in Figure	Interfaces as shown on C9105W	Description
1	Security	Kensington Security Slot
2	USB	USB 2.0
3	LED	Multi-color LED Status indicator. Colors supported are Red, Green, Amber
4	Mode	When pressed for more than 20s, it will reset the AP to factory defaults
5	MGig PoE Port 	2.5 MultiGig Port to power the AP and for Up-link connectivity to the internet.
6	Pass-Through Port 	Pass through port on the AP
7	Console Port 	For Console access of the AP RJ-45
8	PSE-LAN1, LAN2, LAN3 	LAN Ethernet Ports, PSE-LAN1 and LAN2 can be tunneled back to WLC. LAN 3 is a dedicated LAN port for accessing local UI of C9105W Note: NAT is auto enabled on port3 and Personal SSID when the internal DHCP is enabled.

Connecting Cisco Teleworker Access point

The Cisco (Teleworker) APs requires minimal configuration by the end user. For environments where zero-touch end user deployments are required, the corporate IT department or network-integration partner should pre-configure the Cisco Teleworker AP with the address of the corporate Wireless LAN controller, as described in previous sections of this document.



Step 1: Connect the PoE port marked **←→25G** on the back of the Cisco Teleworker Access Point to your home router/gateway PoE port or have a power injector to power the AP. The Cisco C9105W Access Point gets an IP address from the home router/ gateway.

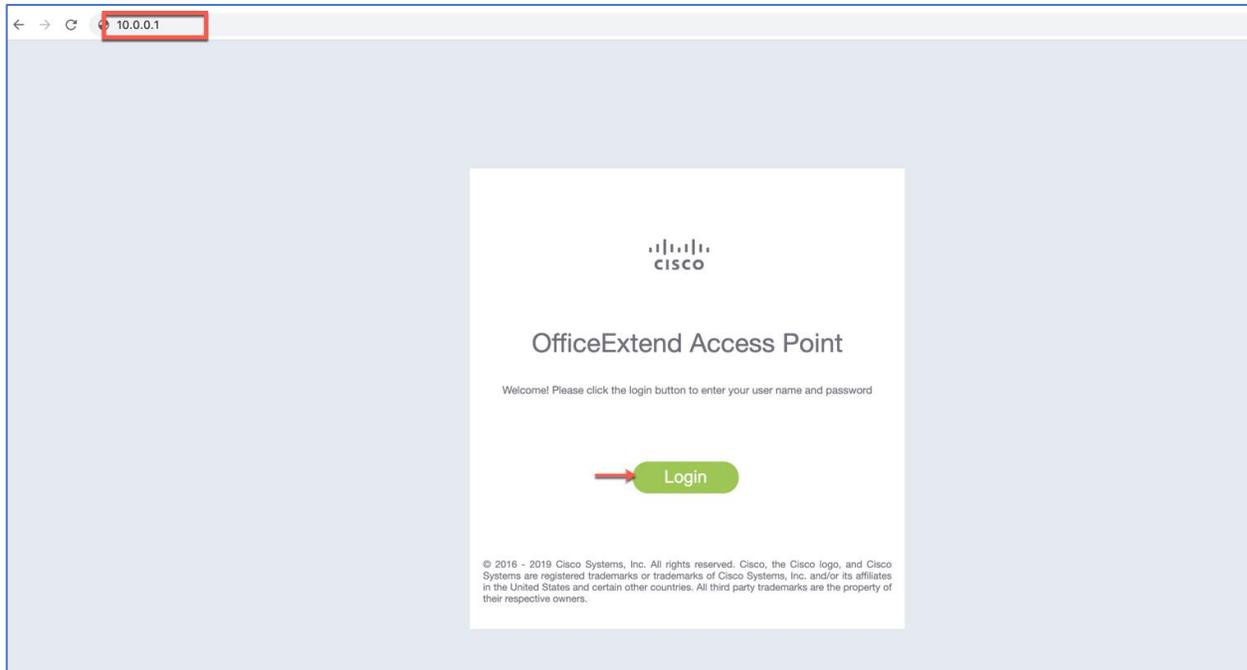


Step 2: After the Cisco C9105W (Teleworker)Access Point has booted up, connect a computer to the port labeled as 3. The computer gets an IP address from the default DHCP address pool of 10.0.0.0/24 (Teleworker AP has NAT enabled for client connecting to the local LAN port 3 or on Personal SSID)

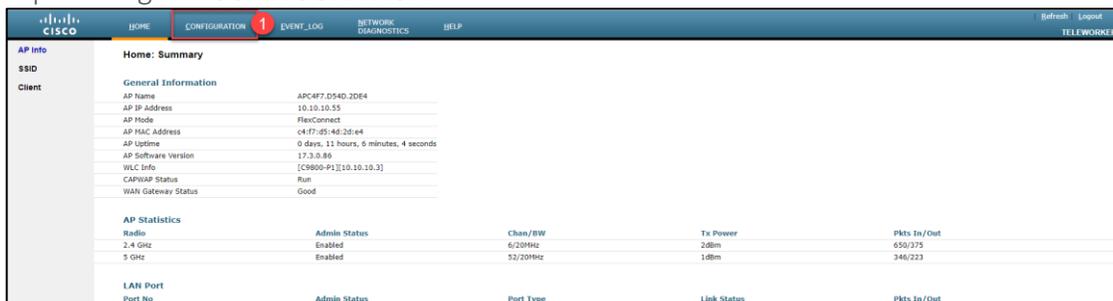


Step 3: Open a browser and navigate to the Access Point by using its default IP address:
<http://10.0.0.1/>

Note: For the other APs models which do not have additional LAN ports or Port3. User need to get the Teleworker AP IP by login into their home router and accessing 'Client List'



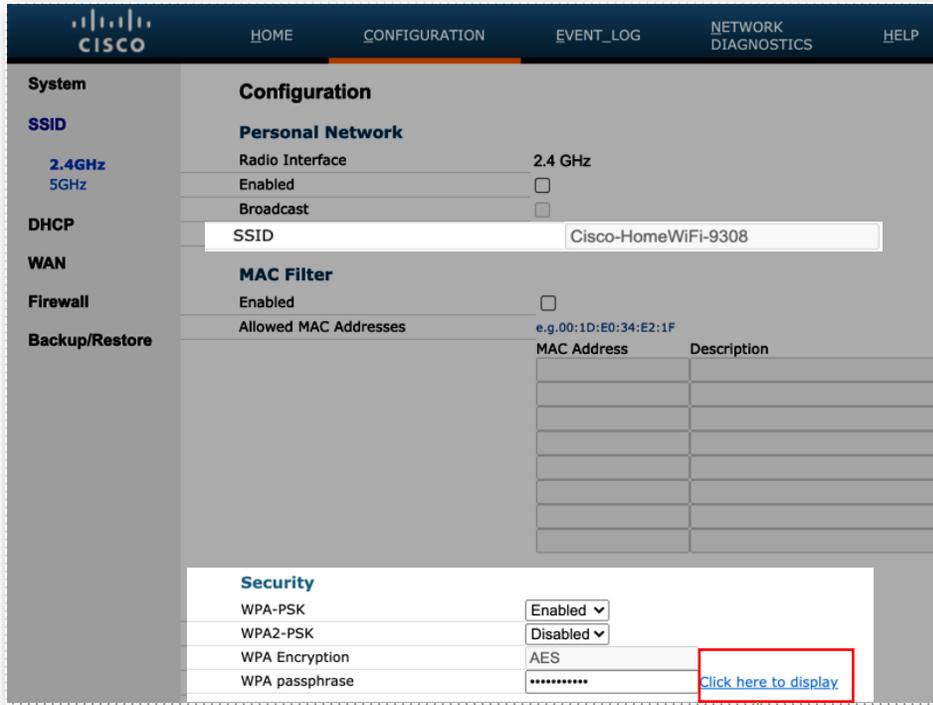
Step 4: Log in to the Administration page by using the default credentials **admin/admin**. The default credentials can be changed later configuration tab. The summary page appears. From top menu go to **CONFIGURATION**



Step 5: click on the SSID and select the 2.4 GHz or 5 GHz Radios. Enable the radio and configure the personal SSID and Passphrase and click Apply.

Note: The default Personal SSID in the OEAP is **“Cisco-HomeWiFi-<last 4 digits of MAC Address>”**. This makes the personal SSID broadcasted by the OEAP unique to some extent in the near vicinity. The user can change the default personal SSID if he/she wants to.

The default passphrase for the default personal SSID is the serial number of the device. The user can obtain the device password by clicking the link **“Click her to display”**. The passphrase is displayed in a separate tab.



Configuration

Personal Network

Radio Interface: 2.4 GHz

Enabled:

Broadcast:

SSID: Cisco-HomeWiFi-9308

MAC Filter

Enabled:

Allowed MAC Addresses: e.g. 00:1D:E0:34:E2:1F

MAC Address	Description

Security

WPA-PSK: Enabled

WPA2-PSK: Disabled

WPA Encryption: AES

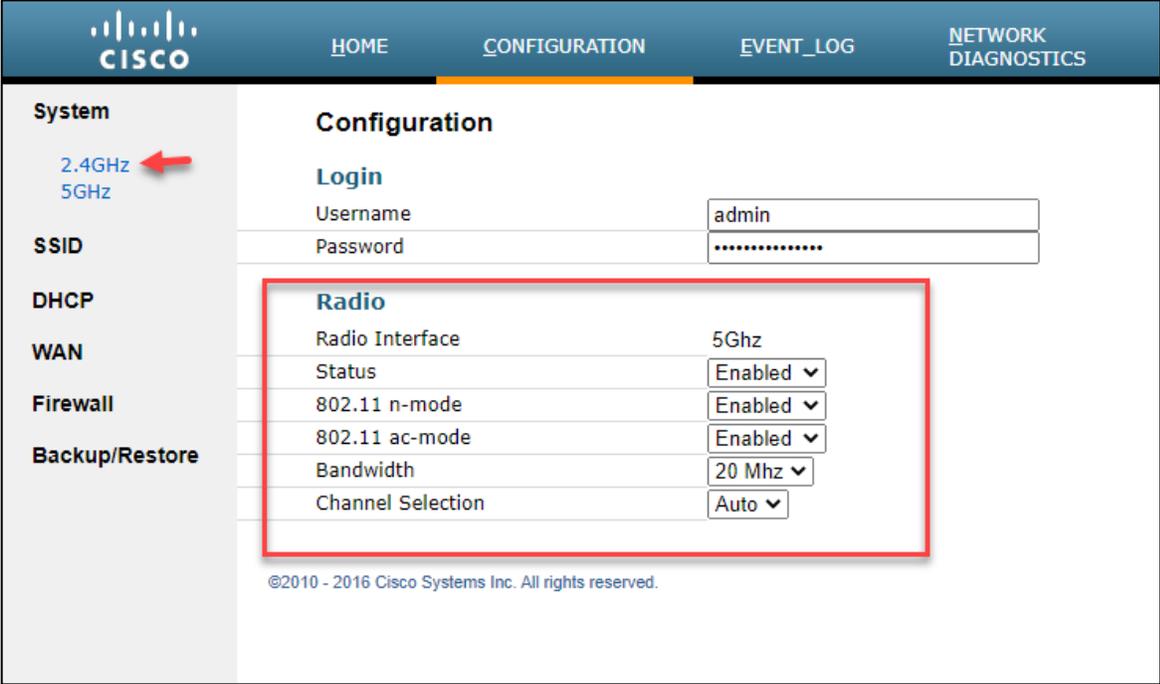
WPA passphrase:

[Click here to display](#)

← → ↻ ⓘ about:blank

The WPA passphrase is : FCW2135NFG8

Radio Settings: User can also change the radio settings if required from CONFIGURATION>System> <2.4GHz/5GHz>



Configuration

Login

Username: admin

Password:

Radio

Radio Interface: 5Ghz

Status: Enabled

802.11 n-mode: Enabled

802.11 ac-mode: Enabled

Bandwidth: 20 Mhz

Channel Selection: Auto

©2010 - 2016 Cisco Systems Inc. All rights reserved.



Local DHCP Server: User can also configure or change DHCP server settings if required from CONFIGURATION>DHCP

The screenshot shows the Cisco configuration interface for Local DHCP. The left sidebar has a menu with 'DHCP' selected. The main content area is titled 'Configuration' and 'Local DHCP'. It contains a table of settings:

IP Address ¹	10.0.23.1
Subnet Mask	255.255.255.0
Default Gateway	10.0.23.1
DHCP Server	Enabled ▾
DHCP Starting IP Address	10.0.23.10
DHCP Ending IP Address	10.0.23.250
DHCP Lease Time(minutes)	1440

Foot Notes:
1. DHCP server IP should not be in the same subnet of configured WLC IP.

Note: The default DHCP scope is 10.0.23.0/24 to avoid overlap with most Home Internet Router. If a home router has a scope that overlap with 10.0.23.0/24, it is required to change the Local DHCP pool to avoid the overlap.

WLC IP configuration: From CONFIGURATION>WAN

User can verify Controller IP Address or if required can enter the Public IP address of the primary WLC, and then click Apply.

The screenshot shows the Cisco configuration interface for WAN settings. The left sidebar has a menu with 'WAN' selected. The main content area is titled 'Configuration' and 'Controller'. It contains a table of settings:

IP Address	1
------------	---

Uplink IP Configuration

Static IP	<input type="checkbox"/>
IP Address	
Subnet Mask	
Default Gateway	
Domain Name	

DNS Configuration

Primary DNS Server	
Secondary DNS Server	

©2010 - 2016 Cisco Systems Inc. All rights reserved.

Clearing Personal SSID

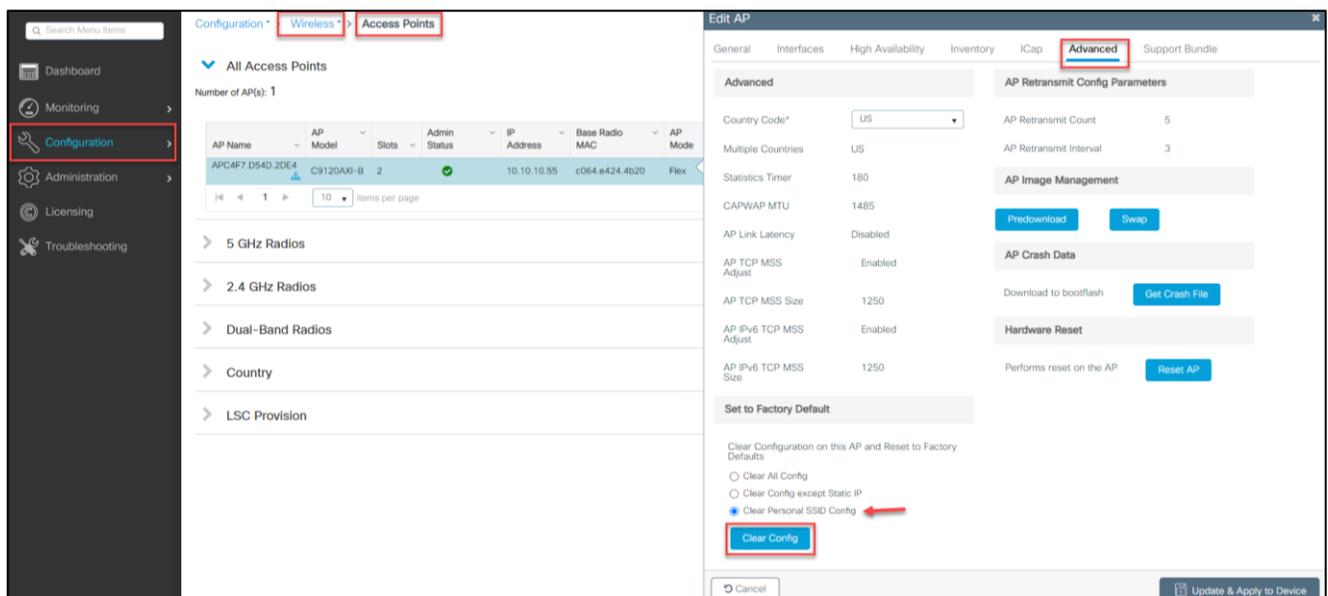
The admin can clear the personal SSID config on the Teleworker access point if required.

Step 1: Navigate to Configuration>Wireless>Access Points

Step 2: Click on the Access point on which admin wants to clear personal SSID the and Navigate to Advanced tab

Step 3: Select the Clear Personal SSID Config and press Clear Config button

This will clear the personal SSID config on the Teleworker access point



The screenshot shows the Cisco Meraki configuration interface. The navigation path is Configuration > Wireless > Access Points. The 'Advanced' tab is selected. In the 'Set to Factory Default' section, the 'Clear Personal SSID Config' radio button is selected and highlighted with a red arrow. The 'Clear Config' button is also highlighted with a red box.

Limitations and Restrictions

- Teleworker solution is not supported on Cisco Mobility Express, Embedded Wireless Controllers, AireOS virtual WLC (vWLC) and C9800-CL (Public cloud offering)
- APs with AUX 1850/2800/3800 can be used as RLAN port but 4800 AUX port does not support RLAN.
- Client roaming between different OEAPs Personal SSIDs is not support, supported only on corporate SSID.
- 8 WLANs and 2 RLANs are supported on Teleworker APs.
- Only 2 personal SSIDs can be created one for 2.4Ghz and one for 5Ghz
- A switch connected to any RLAN/LAN port on AP it supports 4 clients connected to it.
- Multicast and mDNS is not supported in split tunnel scenario.
- Rogue and WIPs is disabled by default on teleworker AP but can be enabled.



Teleworker Assurance from Cisco DNA Center

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. The Cisco DNA Center UI provides intuitive, end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

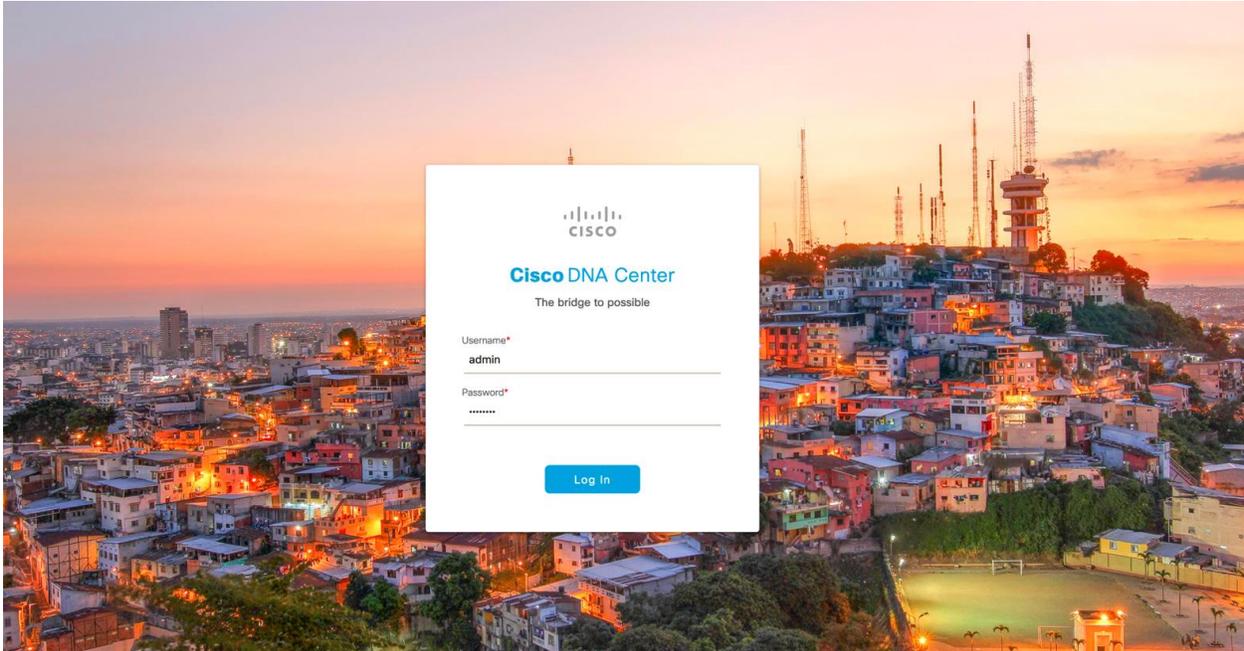
In this section of the guide we are just going to walk through the DNA Center Assurance (2.1.1) with respect to wireless components specifically wireless clients and access points health and Cisco Intelligent Capture (icap) for teleworker deployment use-case. Please refer to DNA Center installation and deployment guide for device setup and details.

Note: Teleworker Personal WLAN will not be monitored by DNA Center Assurance for privacy reasons.

Cisco DNA Assurance User Guide, Release 2.1.1

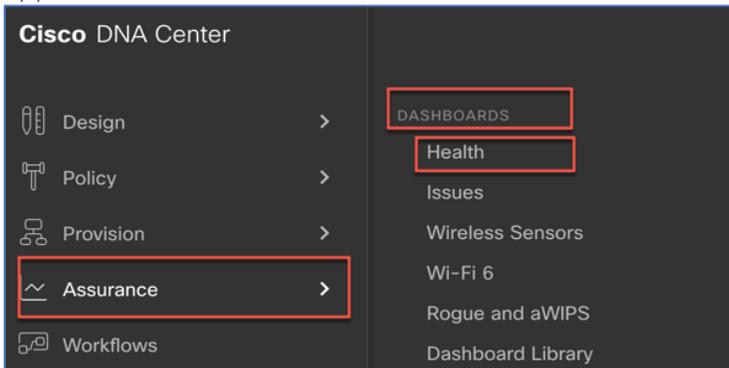
https://www-author3.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-1-1/b_cisco_dna_assurance_2_1_1 Ug/b_cisco_dna_assurance_2_1_1_ug_chapter_01110.html

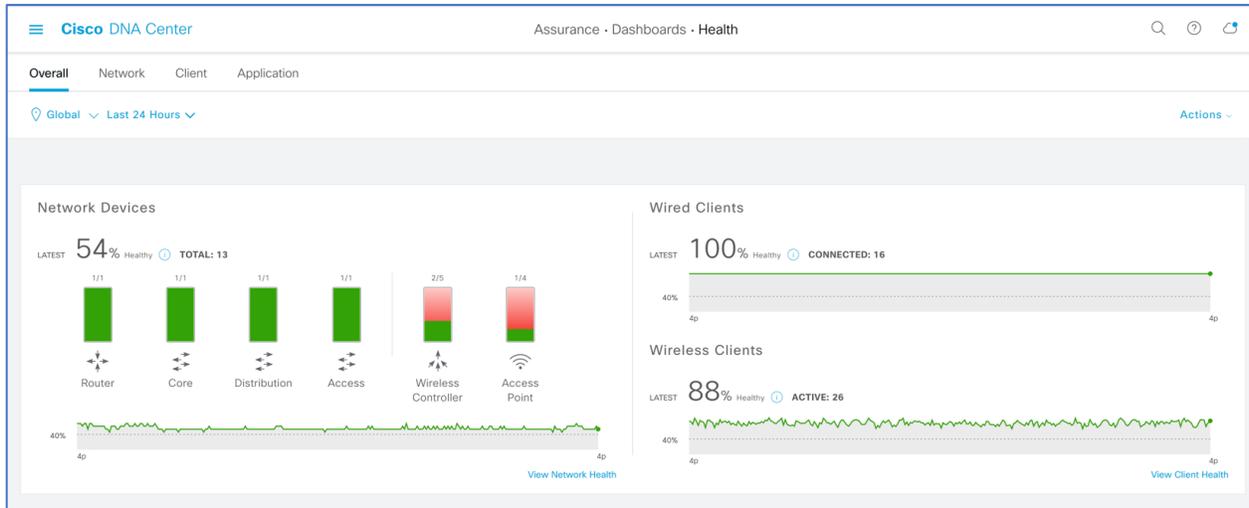
Login to the DNA Center with configured credentials



Cisco DNA Center (2.1.1) GUI, introduces a hamburger menu.

Step 1: Click the Menu icon () and choose Assurance > Health. The Overall health dashboard appears





Step 2: Click the Client tab to navigate to the Client Health page. Scroll down to the client devices table and click the client user want to view the client 360 page.

Client Devices (26)

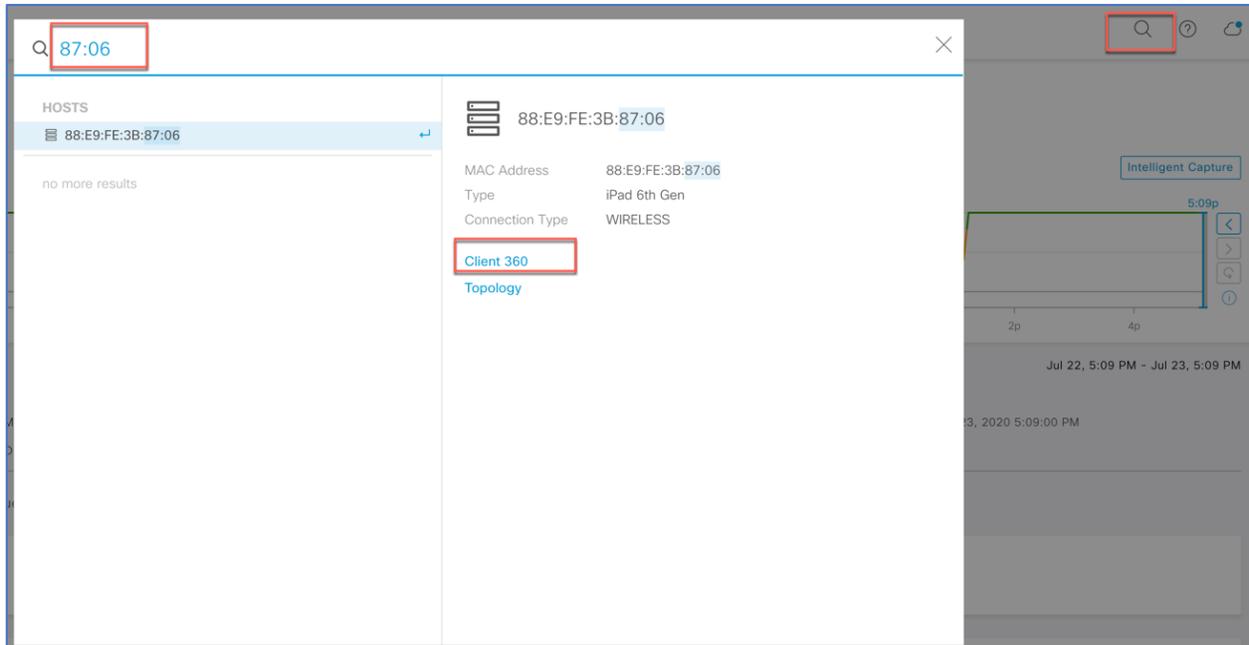
TYPE: **Wireless** | Wired | HEALTH: **All** | Inactive | Poor | Fair | Good | No Data

DATA: Onboarding Time >= 10 s | Association >= 5 s | DHCP >= 5 s | Authentication >= 5 s | RSSI <= -72 dBm | SNR <= 9 dB

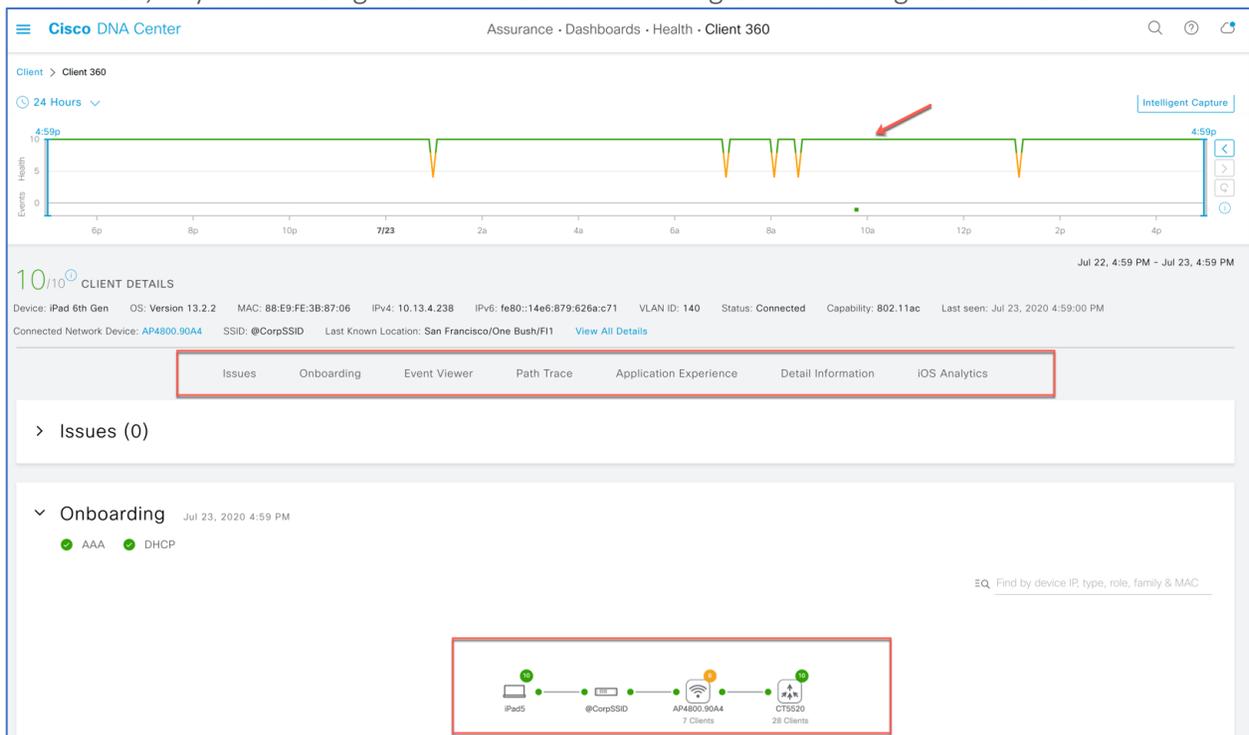
Identifier	IPv4 Address	Device Type	Health	Usage	AP Name	Band	RSSI	Location	Last Seen	Capability
SJC-B4-06	10.13.4.150	Sensor-Client-1800S	10	57.94 kB	AP4800.90A4	5 GHz	-23 dBm	San Francisco/One Bush/F11	Jul 23, 4:52 PM	802.11ac
SJC-B4-04	10.13.4.152	Sensor-Client-1800S	--	--	AP9120.B848	2.4 GHz	--	San Francisco/One Bush/F11	Jul 23, 4:52 PM	Unclassified
minse-HP-x2-210-G2	10.13.4.144	--	10	1.36 kB	AP4800.90A4	5 GHz	-56 dBm	San Francisco/One Bush/F11	Jul 23, 4:52 PM	802.11ac
SJC-B4-03	10.13.4.154	Sensor-Client-1800S	10	4.14 kB	AP9120.B848	5 GHz	-30 dBm	San Francisco/One Bush/F11	Jul 23, 4:52 PM	802.11ac
DESKTOP-VLU070D	10.13.4.121	Microsoft-Workstation	10	2.81 kB	AP4800.90A4	5 GHz	-40 dBm	San Francisco/One Bush/F11	Jul 23, 4:51 PM	802.11ac
iPad4	10.13.4.226	iPad 6th Gen	10	611.19 kB	AP003A.7DD9.FB76	5 GHz	-40 dBm	--	Jul 23, 4:51 PM	802.11ac

Showing 25 of 26 | [Show More](#)

User can also click on the magnifying glass in the top right corner of DNA Center page to search the client. Enter either the client MAC address, the IP address, or the username the client used to join an 802.1X network.



The client 360 view provides the holistic view about client statistics and details, on how client is onboarded, any issues being seen and detail onboarding events through Event Viewer.





Event Viewer

Filter EQ Find

Jul 23, 2020

Event	AP:AP4800.90A4 WLC:CT5520 WLAN:@CorpSSID	Time
Re-Authentication	AP:AP4800.90A4 WLC:CT5520 WLAN:@CorpSSID	4:47:10.388 PM - 4:47:11.530 PM
Broadcast Rekey	AP:AP4800.90A4 WLC:CT5520 WLAN:@CorpSSID	4:36:02.704 PM - 4:36:02.757 PM
Re-Authentication	AP:AP4800.90A4 WLC:CT5520 WLAN:@CorpSSID	4:17:28.176 PM - 4:17:29.374 PM
Re-Authentication	AP:AP4800.90A4 WLC:CT5520 WLAN:@CorpSSID	3:47:26.016 PM - 3:47:32.273 PM
Broadcast Rekey	AP:AP4800.90A4 WLC:CT5520 WLAN:@CorpSSID	3:34:28.148 PM - 3:34:28.194 PM
Re-Authentication	AP:AP4800.90A4 WLC:CT5520 WLAN:@CorpSSID	3:16:56.792 PM - 3:16:58.102 PM
DHCP	AP:AP4800.90A4 WLC:CT5520 WLAN:@CorpSSID	2:56:04.006 PM
Re-Authentication	AP:AP4800.90A4 WLC:CT5520 WLAN:@CorpSSID	2:46:10.316 PM - 2:46:11.473 PM
Broadcast Rekey	AP:AP4800.90A4 WLC:CT5520 WLAN:@CorpSSID	2:28:21.236 PM - 2:28:21.254 PM

Detailed Information

Status: Success

Details:

ROLE	LOCAL
WLC Name	CT5520
User Name	iPad5
Frequency(GHz)	5.0
IPv4	10.13.4.238
Radio	1
WLAN	@CorpSSID
AP Mac	F4:DB:E6:87:21:60
AP Name	AP4800.90A4
VLAN ID/VND	140

For client detail stats admin can view the Details Information view which comprises of (device info, Connectivity, RF stats and iOS Analytics) iOS Analytics is specifically for iOS devices to visualize how the iOS device is seeing the WiFi network.

Note: iOS Analytics is not supported on C9105, C9115 and C9120 Access Points

Client > Client 360

Detail Information Jul 23, 2020 5:09 PM

Device Info Connectivity RF iOS Analytics

Neighbor APs (4) Export

BSSID	AP Name	Channel	RSSI (dBm)	Location
F4:DB:E6:87:21:6F	AP4800.90A4	42	-49	Global/San Francisco/One Bush/F1
F4:DB:E6:87:21:60	AP4800.90A4	155	-51	Global/San Francisco/One Bush/F1
08:4F:F9:2E:DB:EF	AP9120.B848	155	-54	Global/San Francisco/One Bush/F1
00:2A:10:1A:FA:3F		58	-56	

Showing 1 - 4 of 4

Client Disassociation Details (0) Export

Time	Disassociation Reason	Disassociated AP	Session Duration	AP Location
No data to display				

For more comprehensive and detail troubleshooting admin can leverage intelligent capture (iCAP) feature to run packet capture for the device. The Intelligent Capture is located on device 360 page as shown. Click on the Intelligent capture

Cisco DNA Center Assurance · Dashboards · Health · Client 360

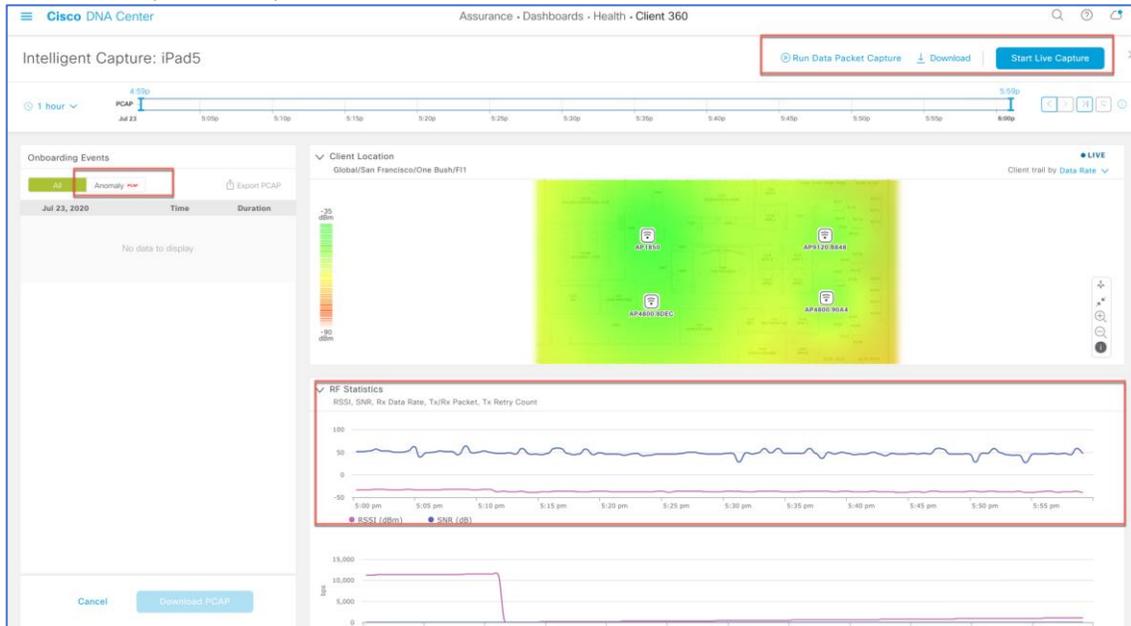
Client > Client 360

24 Hours Intelligent Capture



It opens the Intelligent Capture Client page and admin can run the live packet capture or anomaly PCAP, or run a data packet capture.

Note: Data packet capture is available on C9130 and 4800 Series APs



Once the packet capture is complete user can download the pcap file to perform further analysis.

First Packet Time	Last Packet Time	Type	Duration (h:mm:ss)	Size	Download
Jun 02, 2020, 10:05:03 am	Jun 04, 2020, 3:51:42 pm	Wireless	53:46:39	99 MB	Download
Jun 02, 2020, 10:03:59 am	Jun 02, 2020, 10:03:59 am	Wireless	-	23 KB	Download
Jun 02, 2020, 10:02:18 am	Jun 02, 2020, 10:02:18 am	Wireless	-	32 KB	Download
Jun 02, 2020, 10:01:16 am	Jun 02, 2020, 10:01:16 am	Wireless	-	85 KB	Download
Jun 02, 2020, 10:00:38 am	Jun 02, 2020, 10:00:39 am	Wireless	00:00:01	128 KB	Download
Jun 02, 2020, 10:00:16 am	Jun 02, 2020, 10:00:16 am	Wireless	-	53 KB	Download
Jun 02, 2020, 10:00:06 am	Jun 02, 2020, 10:00:07 am	Wireless	00:00:01	127 KB	Download
Jun 02, 2020, 9:59:01 am	Jun 02, 2020, 9:59:01 am	Wireless	-	11 KB	Download
Jun 02, 2020, 04:11:10 am	Jun 02, 2020, 04:11:10 am	Wireless	-	88 MB	Download



Reference documents and VODs

- OEAP Configuration Guide (AireOS 8.5): [Link](#)
- OEAP Configuration Guide (AireOS 8.8): [Link](#)
- OEAP AireOS guided configuration [video](#)
- OEAP C9800 guided configuration video: [Link](#)
- OEAP AireOS Split Tunnel configuration: [Link](#)

- OEAP Cisco Validated Design (AireOS): [Link](#)
- 1815T Deployment Guide: [Link](#)
- Cisco Wireless Solutions Software Compatibility Matrix: [Link](#)
- Cisco DNA Assurance User Guide, Release 2.1.1 : [Link](#)

<https://cdetsng.cisco.com/summary/#/defect/CSCv03650>

<https://cdetsng.cisco.com/summary/#/defect/CSCvu95312>

<https://cdetsng.cisco.com/summary/#/defect/CSCvu52695>

<https://cdetsng.cisco.com/summary/#/defect/CSCvu56555>



Legal Information

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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California. NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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

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

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in



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

Cisco Copyright
© 2020 Cisco Systems, Inc. All rights reserved.