ExtremeWireless WiNG

Virtual Controller Quick Start Guide

Abstract: This guide will follow through the steps required to deploy WiNG Virtual Controller (a.k.a VC) running on the AP with automatic VC failover and be able to manage a mixture of Access Points in the same deployment.

Published: October 2017

Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000
www.extremenetworks.com

Contents

Pre-Requisites

- WiNG 5.9.1.1 and beyond.
- Supported Access Points as Heterogeneous VC:
    - AP8533 / AP8432 – full support
    - AP7522 / AP7532 / AP7562 – limited to AP7522/7532/7562
    - AP7632 / AP7662 – limited to AP7612/7632/7662
- Supported adopted Access Points: AP7522 / AP7532 / AP7562/ AP7602 / AP7612 / AP7622 / AP7632 / AP7662 / AP8432 / AP8533.

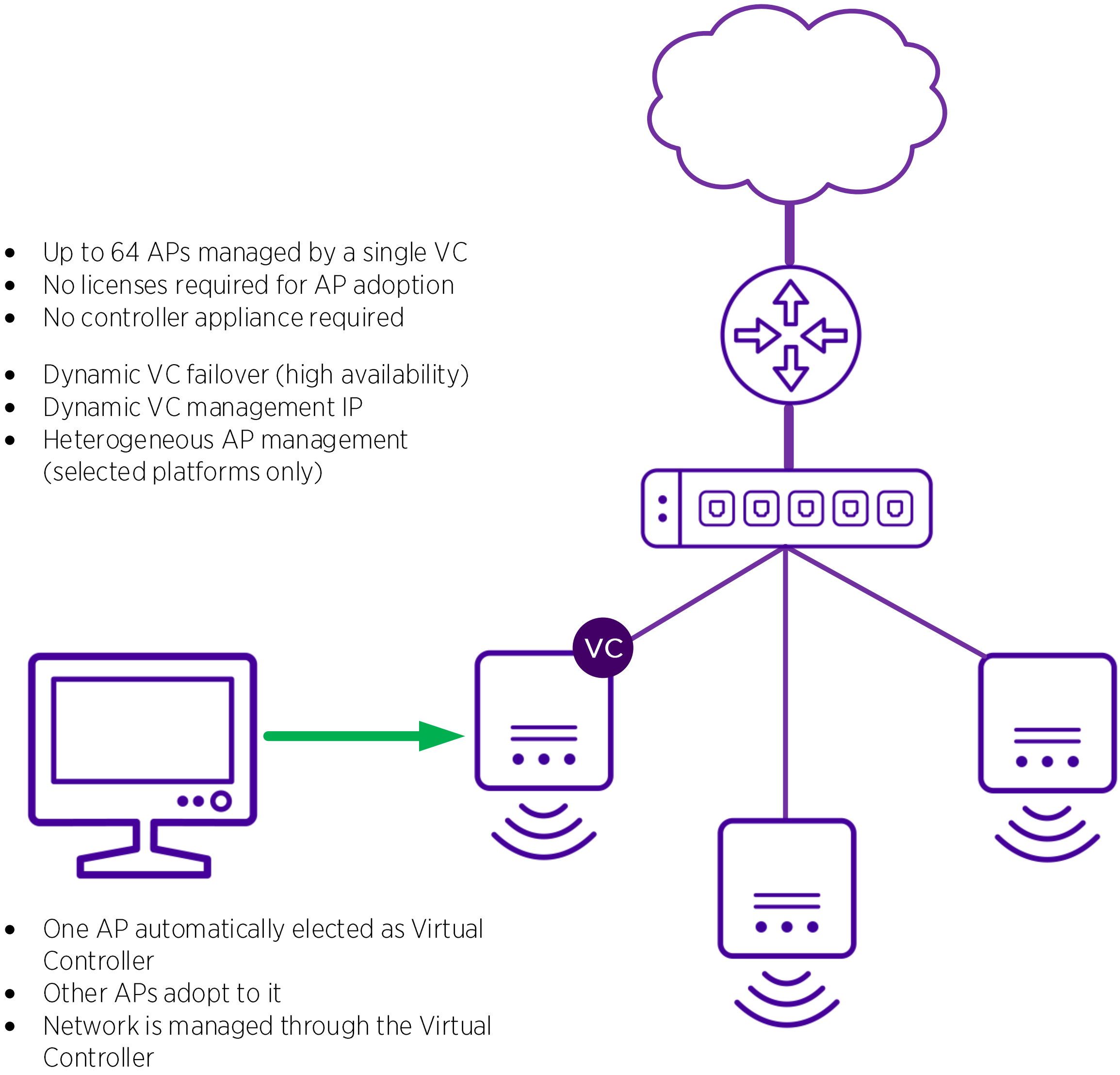
VirtualController – Overview

Virtual Controller functionality running on the AP is a cost effective enterprise grade controller-less solution for single site deployments (single or multiple buildings connected in the same Layer 2 domain).

Prior to 5.9.1 WiNG release Virtual Controller functionality was limited to manage of the like- Access Points only, whereas WiNG 5.9.1 provided heterogeneous AP management on selected AP platforms to allow mixed AP environments managed by the same Virtual Controller AP.

In addition, WiNG 5.9 release added support for Dynamic Virtual Controller feature, which allows automatic VC failover and dynamic VC management IP address to provide high availability for these kind of deployments. Automatic failover is based on the RF Domain Manager election process, where the most powerful AP model wins (for example AP7632 wins over AP7612, AP8432 wins over AP7632 and so on) or if there are multiple AP of the same model the AP with the lowest MiNT ID will break a tie.

The following diagram outlines Virtual Controller deployment:

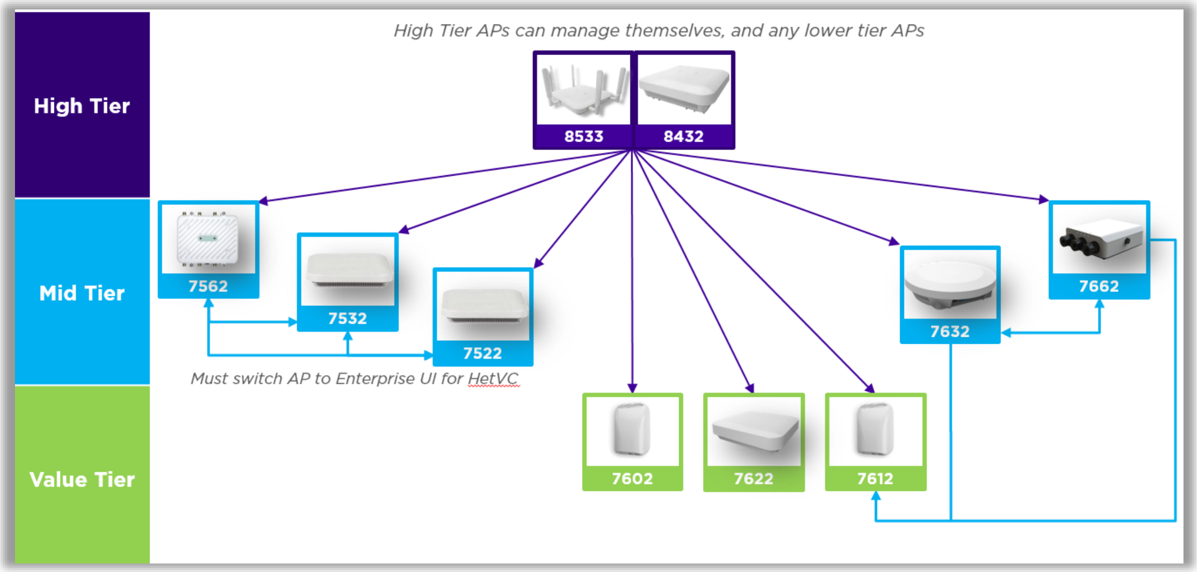


- Up to 64 APs managed by a single VC
- No licenses required for AP adoption
- No controller appliance required

- Dynamic VC failover (high availability)
- Dynamic VC management IP
- Heterogeneous AP management (selected platforms only)

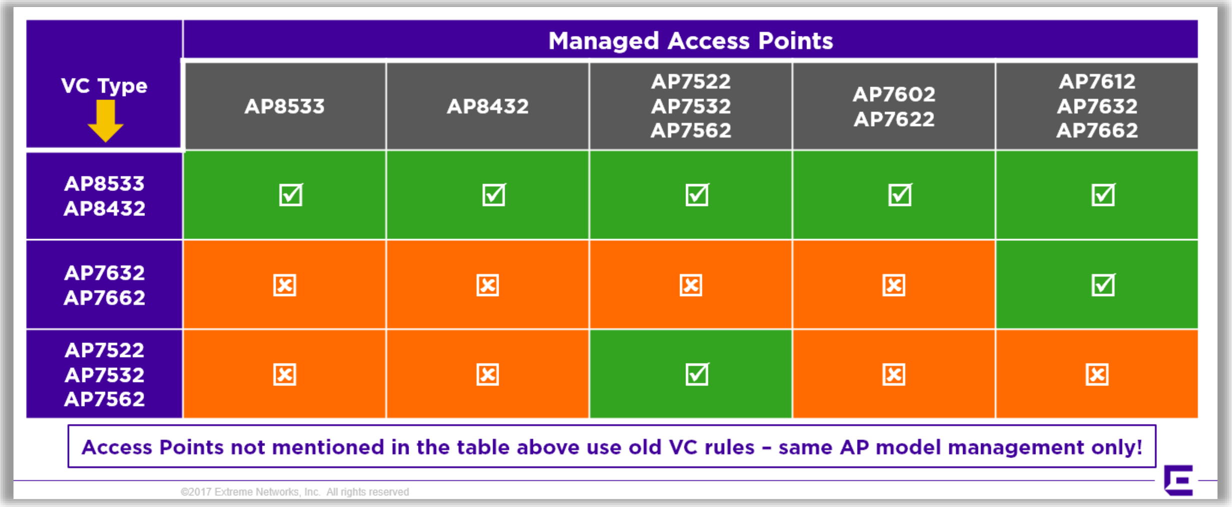
- One AP automatically elected as Virtual Controller
- Other APs adopt to it
- Network is managed through the Virtual Controller

The following diagram outlines supported Heterogeneous VC deployment modes:


High Tier
Mid Tier
Value Tier
High Tier APs can manage themselves, and any lower tier APs
8533
8432
7562
7532
7522
7632
7662
7602
7622
7612
Must switch AP to Enterprise UI for HetVC

For the Access Points not mentioned in the diagram above the old rule applies where they can only manage like- AP models only.

Table below provides a similar information in a different format:



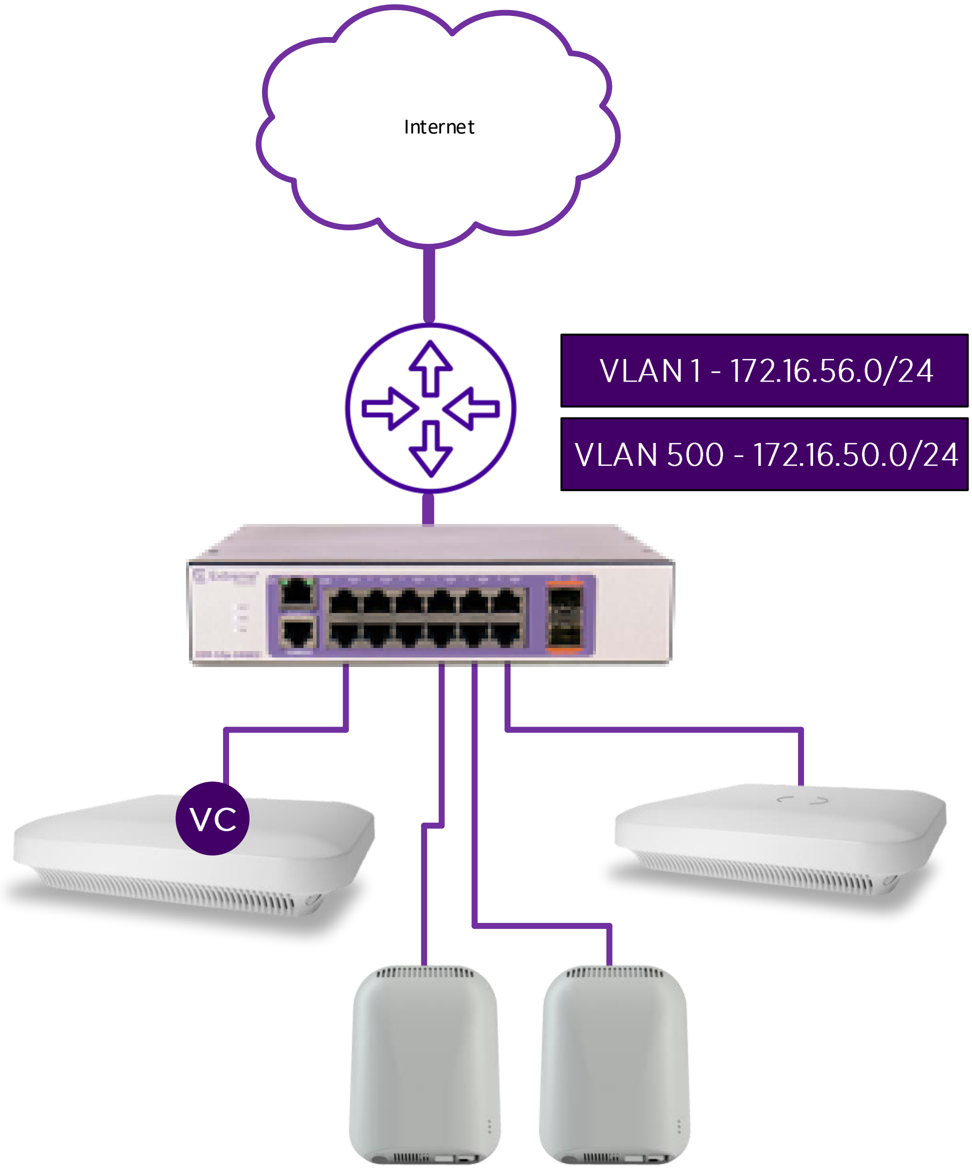
VC Type	Managed Access Points				
	AP8533	AP8432	AP7522 AP7532 AP7562	AP7602 AP7622	AP7612 AP7632 AP7662
AP8533 AP8432	☑	☑	☑	☑	☑
AP7632 AP7662	☒	☒	☒	☒	☑
AP7522 AP7532 AP7562	☒	☒	☑	☒	☒

Access Points not mentioned in the table above use old VC rules – same AP model management only!

©2017 Extreme Networks, Inc. All rights reserved

VirtualController – Deployment Example

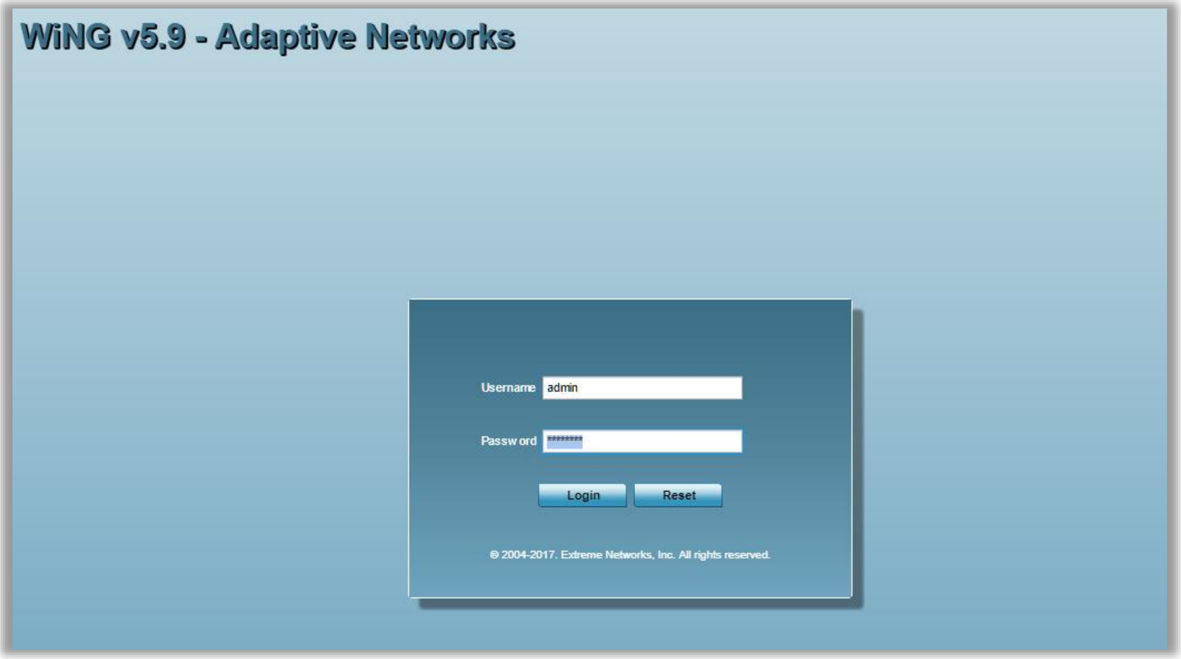
In this guide we will have the following setup, but similar steps can be used for any other supported Heterogeneous VC combination. In our example we are going to have 2x AP8533s and 2x AP7612s, plugged into the same Extreme 220 12 port switch, where local router provides DHCP / DNS / NAT services:



Step 1 – Login to one of the AP8533s via HTTPS

First you should login to the Web UI interface of one of the AP8533s (or any AP that you are planning to use as a Virtual Controller). You can either find the IP address of the Access Point via your DHCP server or use default Zeroconf IP address (169.254.0.0/16) if no DHCP server is locally available. Note that by default only HTTPS and SSH interfaces are opened. Use default credentials *admin / admin123*:

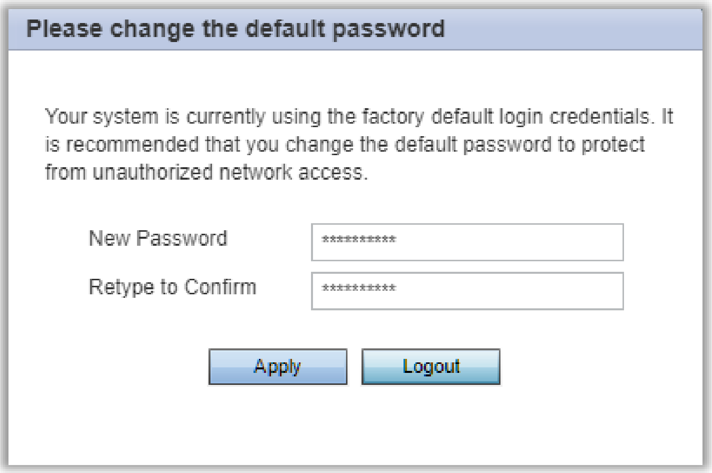
Note: from now on Virtual Controller and VC will refer to the same term



Username admin

Password ********

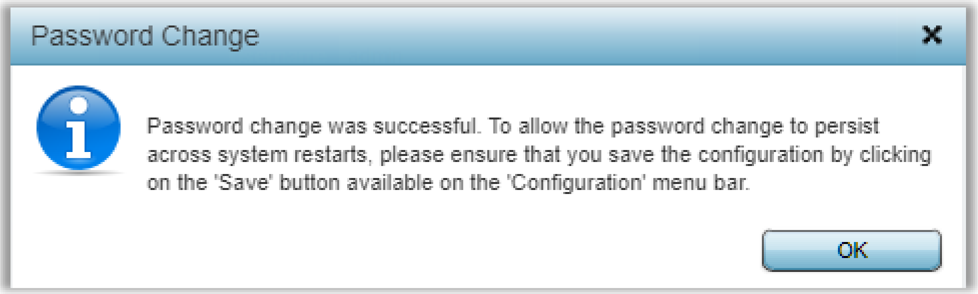
© 2004-2017. Extreme Networks, Inc. All rights reserved.


Please change the default password

Your system is currently using the factory default login credentials. It is recommended that you change the default password to protect from unauthorized network access.

New Password ***********

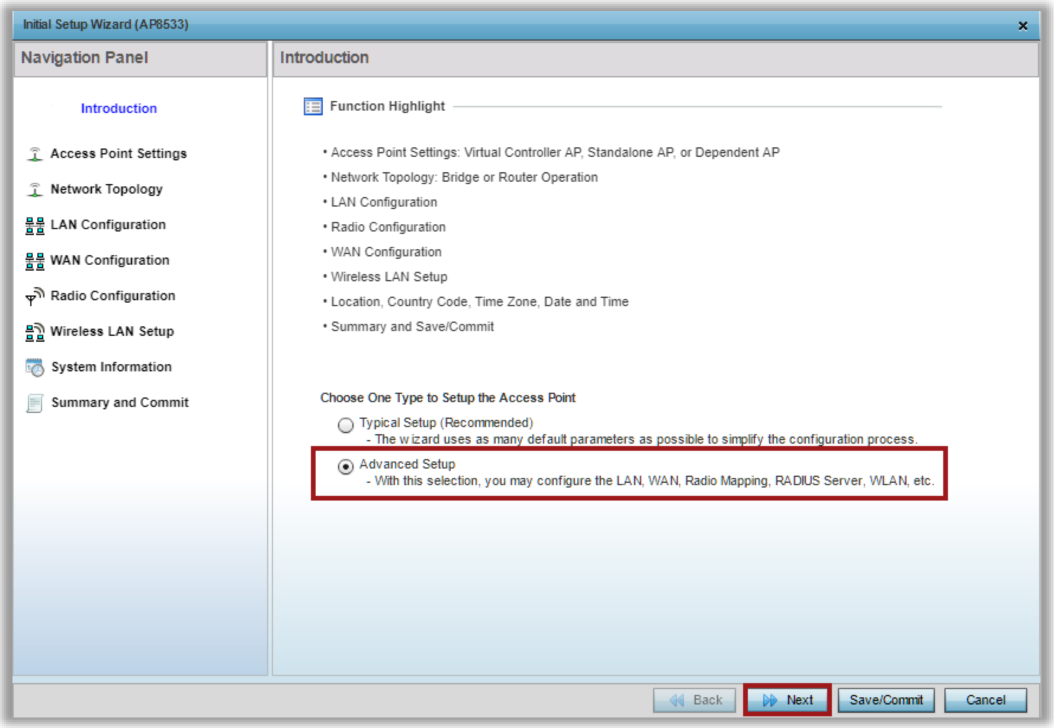
Retype to Confirm ***********


Password Change

Password change was successful. To allow the password change to persist across system restarts, please ensure that you save the configuration by clicking on the 'Save' button available on the 'Configuration' menu bar.

Step 2 – Go through the Installation Wizard

On the next screen Installation Wizard will appear automatically, which we are going to use in “Advanced Setup” mode:



Initial Setup Wizard (AP8533)

Navigation Panel

Introduction

Function Highlight

- Access Point Settings: Virtual Controller AP, Standalone AP, or Dependent AP
- Network Topology: Bridge or Router Operation
- LAN Configuration
- Radio Configuration
- WAN Configuration
- Wireless LAN Setup
- Location, Country Code, Time Zone, Date and Time
- Summary and Save/Commit

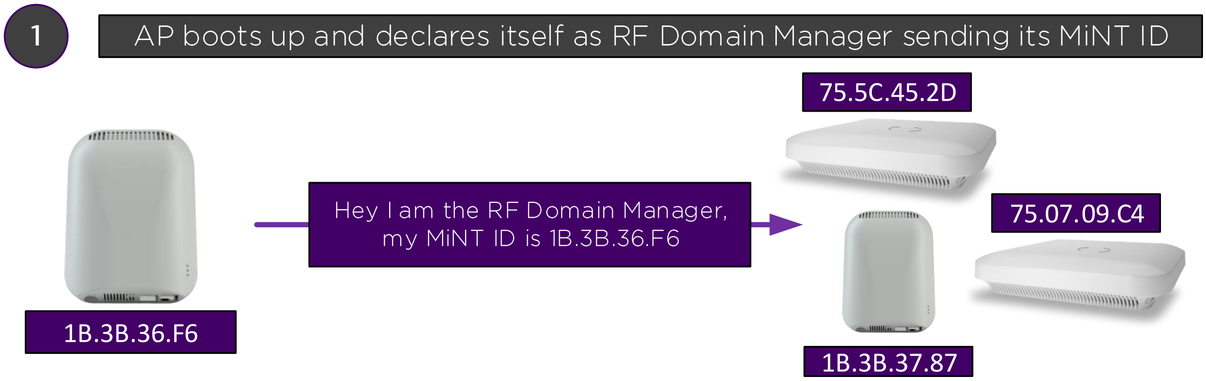
Choose One Type to Setup the Access Point

○ Typical Setup (Recommended)
- The wizard uses as many default parameters as possible to simplify the configuration process.

● Advanced Setup
- With this selection, you may configure the LAN, WAN, Radio Mapping, RADIUS Server, WLAN, etc.

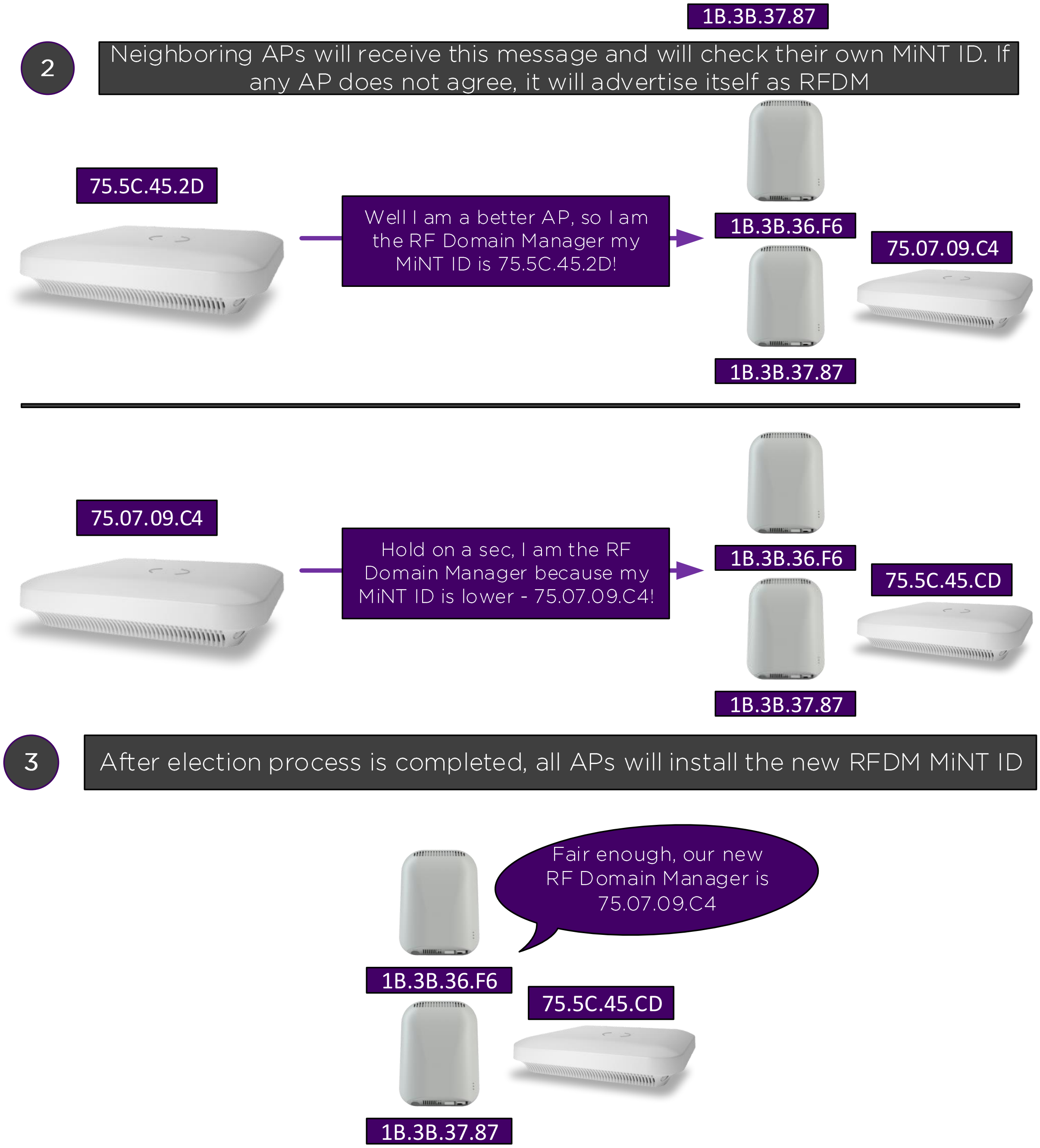
On the next screen you will be prompted to select the mode in which this AP will function. In our example we are going to use “Virtual Controller AP Auto”, which will enable Virtual Controller functionality, but will also provide automatic Virtual Controller failover in case current VC is unavailable, as well as an option to configure dynamic Virtual Controller management IP address that will failover with VC role.

Note that Virtual Controller Auto election relies on the RF Domain Manager election process. In other words – if the AP becomes elected as RF Domain Manager it automatically becomes the Virtual Controller. The following outlines general RF Domain Manager election process:



1 AP boots up and declares itself as RF Domain Manager sending its MiNT ID

Hey I am the RF Domain Manager, my MiNT ID is 1B.3B.36.F6



1B.3B.37.87

2 Neighboring APs will receive this message and will check their own MiNT ID. If any AP does not agree, it will advertise itself as RFDM

75.5C.45.2D

Well I am a better AP, so I am the RF Domain Manager my MiNT ID is 75.5C.45.2D!

1B.3B.36.F6

75.07.09.C4

1B.3B.37.87

75.07.09.C4

Hold on a sec, I am the RF Domain Manager because my MiNT ID is lower - 75.07.09.C4!

1B.3B.36.F6

75.5C.45.CD

1B.3B.37.87

3 After election process is completed, all APs will install the new RFDM MiNT ID

Fair enough, our new RF Domain Manager is 75.07.09.C4

1B.3B.36.F6

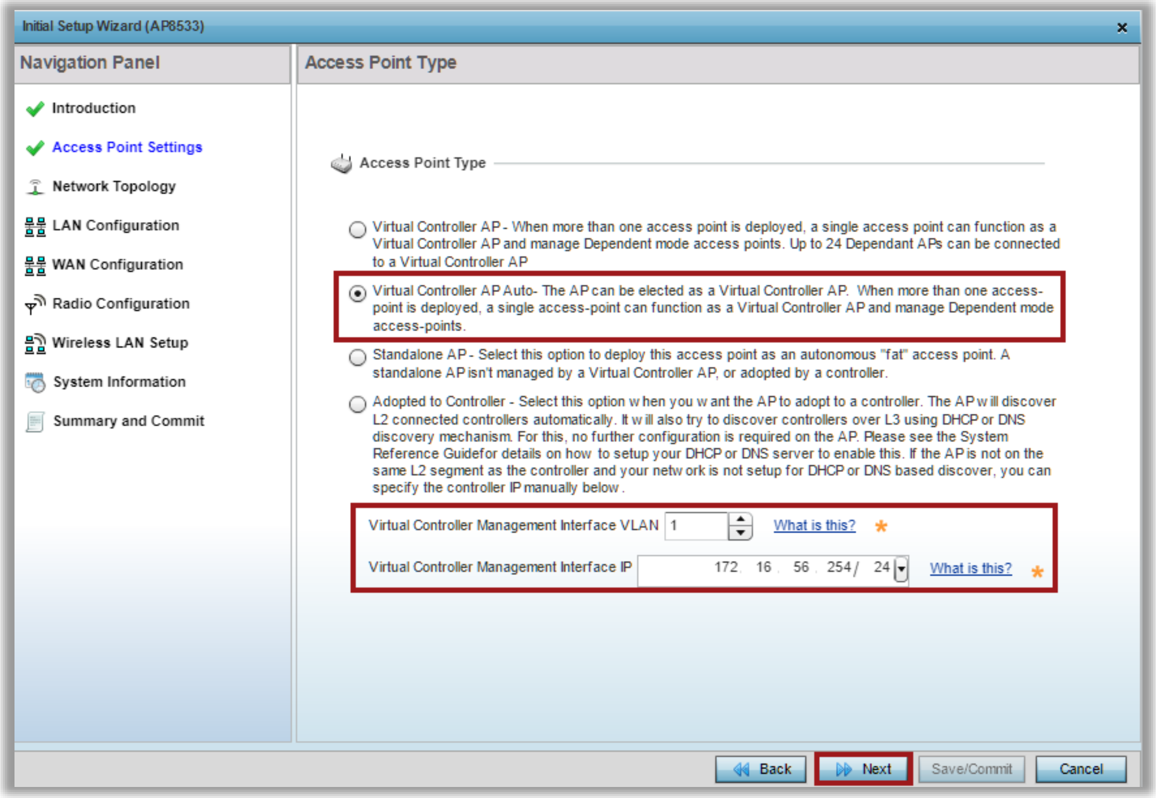
75.5C.45.CD

1B.3B.37.87

Generally, it is recommended to enable Auto VC feature only on the same-tier Access Points, like AP8432 and AP8533 and don't mix multiple AP tiers (refer to the Heterogeneous VC diagram in the Overview section of this document). The reason is that while failover to the lower tier AP will work (for example AP8533 acting as VC becomes unavailable and AP7632 takes over in VC role), reverse process will not be seamless (following previous example when AP8533 will be re-installed into the network it will not receive any synced configuration from the AP7632)

Virtual Controller Management VLAN Interface – this is the management VLAN ID that Virtual Controller will use to adopt and manage Access Points. By default, all APs will use untagged VLAN 1 for management. It is recommended to keep VLAN 1 unchanged and untagged for ease of deployment and management.

The Virtual Controller Management IP Interface is an address that the current Virtual Controller will install as a secondary interface so that an admin could use it for network management. This is useful as it allows all the APs to obtain their IPv4 addressing via DHCP and use statically configured VC IP address for management, so only VC AP will respond on this interface. Note that VC management IP address should be inside the same subnet as the management network:



Access Point Type

Access Point Type

○ Virtual Controller AP - When more than one access point is deployed, a single access point can function as a Virtual Controller AP and manage Dependent mode access points. Up to 24 Dependant APs can be connected to a Virtual Controller AP

● Virtual Controller AP Auto- The AP can be elected as a Virtual Controller AP. When more than one access-point is deployed, a single access-point can function as a Virtual Controller AP and manage Dependent mode access-points.

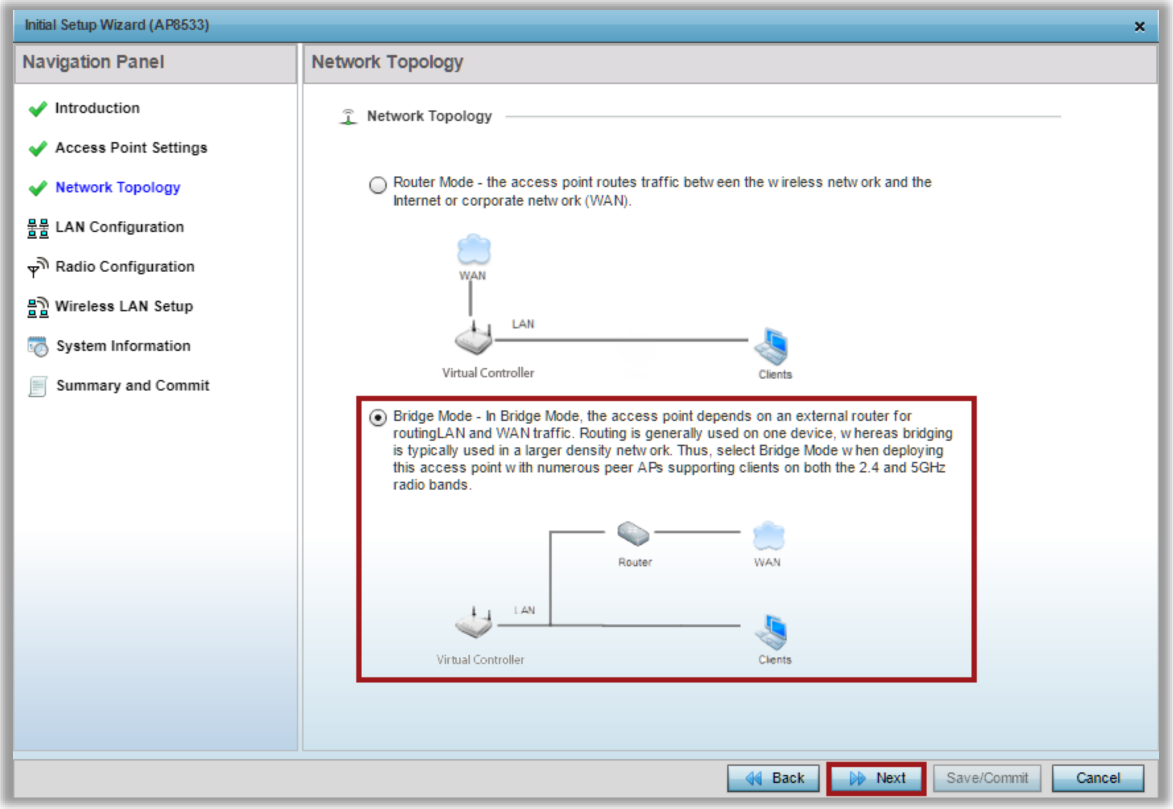
○ Standalone AP - Select this option to deploy this access point as an autonomous "fat" access point. A standalone AP isn't managed by a Virtual Controller AP, or adopted by a controller.

○ Adopted to Controller - Select this option w hen you w ant the AP to adopt to a controller. The AP w ill discover L2 connected controllers automatically. It w ill also try to discover controllers over L3 using DHCP or DNS discovery mechanism. For this, no further configuration is required on the AP. Please see the System Reference Guidefor details on how to setup your DHCP or DNS server to enable this. If the AP is not on the same L2 segment as the controller and your netw ork is not setup for DHCP or DNS based discover, you can specify the controller IP manually below .

Virtual Controller Management Interface VLAN 1 What is this? *

Virtual Controller Management Interface IP 172 . 16 . 56 . 254 / 24 What is this? *

On the Network Topology screen there are two modes to select. For the purposes of this guide we will use Bridged mode, as local router is providing DHCP / NAT services. Optionally Router mode can be selected so that an AP can act as DHCP / NAT router for the wireless clients if required.



Initial Setup Wizard (AP8533)

Navigation Panel

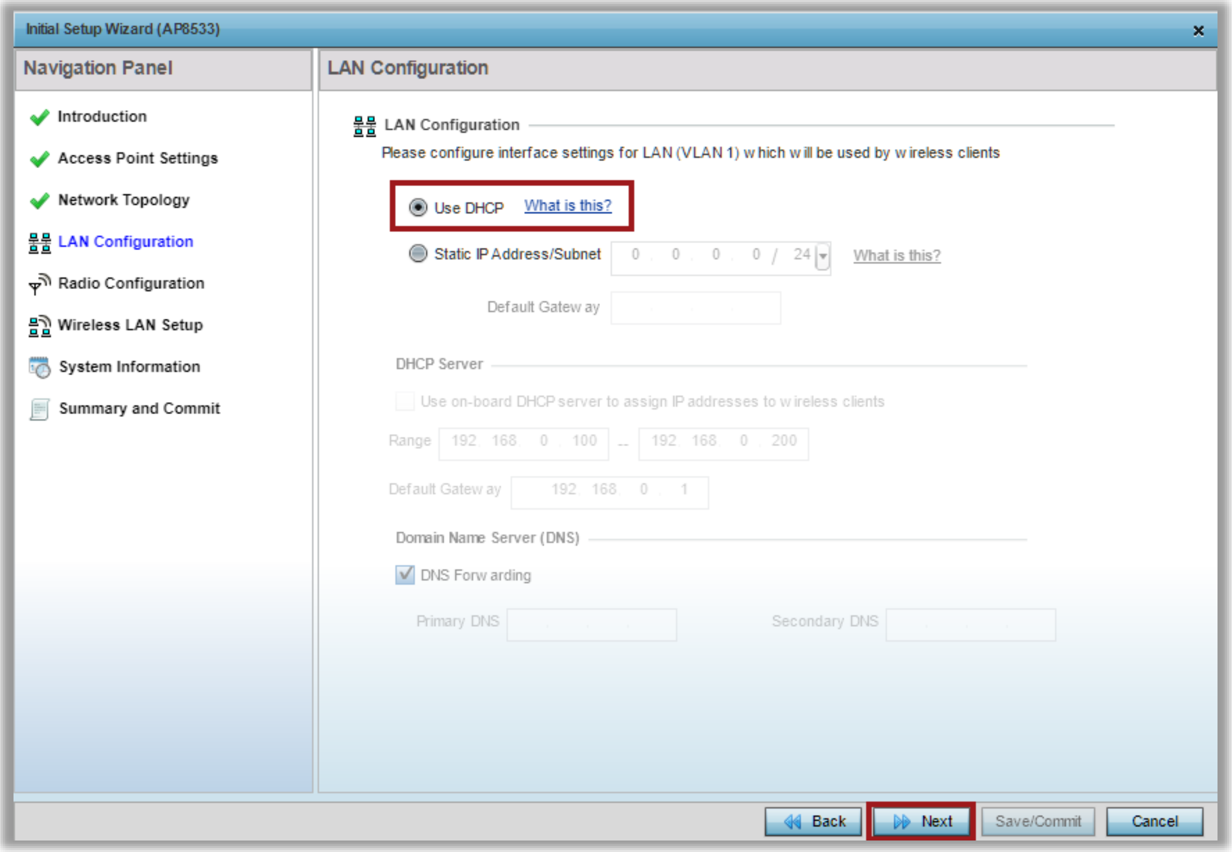
- ✓ Introduction
- ✓ Access Point Settings
- ✓ Network Topology
- LAN Configuration
- Radio Configuration
- Wireless LAN Setup
- System Information
- Summary and Commit

Network Topology

Network Topology

○ Router Mode - the access point routes traffic betw een the w ireless netw ork and the Internet or corporate netw ork (WAN).

● Bridge Mode - In Bridge Mode, the access point depends on an external router for routingLAN and WAN traffic. Routing is generally used on one device, w hereas bridging is typically used in a larger density netw ork. Thus, select Bridge Mode w hen deploying this access point w ith numerous peer APs supporting clients on both the 2.4 and 5GHz radio bands.



Initial Setup Wizard (AP8533)

Navigation Panel

- ✓ Introduction
- ✓ Access Point Settings
- ✓ Network Topology
- LAN Configuration
- Radio Configuration
- Wireless LAN Setup
- System Information
- Summary and Commit

LAN Configuration

LAN Configuration

Please configure interface settings for LAN (VLAN 1) w hich w ill be used by w ireless clients

● Use DHCP What is this?

○ Static IP Address/Subnet 0 . 0 . 0 . 0 / 24 What is this?

Default Gatew ay

DHCP Server

□ Use on-board DHCP server to assign IP addresses to w ireless clients

Range 192 . 168 . 0 . 100 -- 192 . 168 . 0 . 200

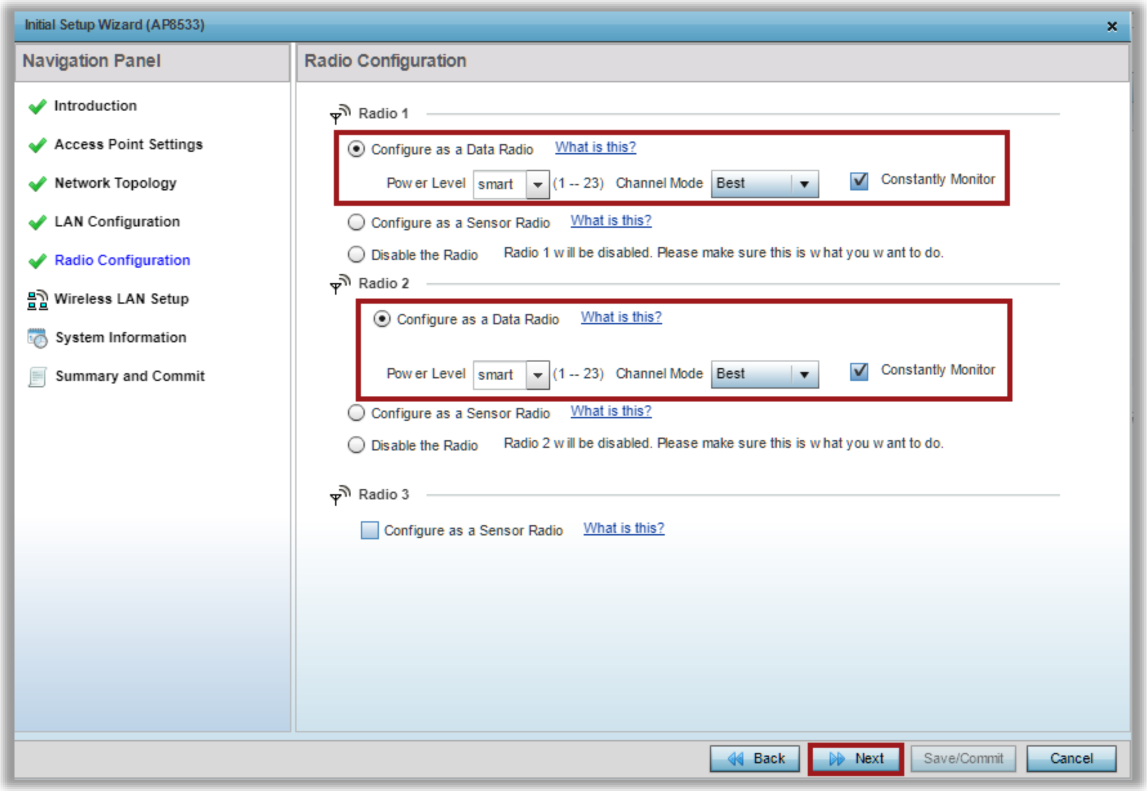
Default Gatew ay 192 . 168 . 0 . 1

Domain Name Server (DNS)

☑ DNS Forw arding

Primary DNS Secondary DNS

On the next screen select desired Radio Interface mode and click next:



Initial Setup Wizard (AP8533)

Navigation Panel

- ✓ Introduction
- ✓ Access Point Settings
- ✓ Network Topology
- ✓ LAN Configuration
- ✓ Radio Configuration
- Wireless LAN Setup
- System Information
- Summary and Commit

Radio Configuration

Radio 1

● Configure as a Data Radio What is this?

Pow er Level: smart (1 -- 23) Channel Mode: Best ☑ Constantly Monitor

○ Configure as a Sensor Radio What is this?

○ Disable the Radio Radio 1 w ill be disabled. Please make sure this is w hat you w ant to do.

Radio 2

● Configure as a Data Radio What is this?

Pow er Level: smart (1 -- 23) Channel Mode: Best ☑ Constantly Monitor

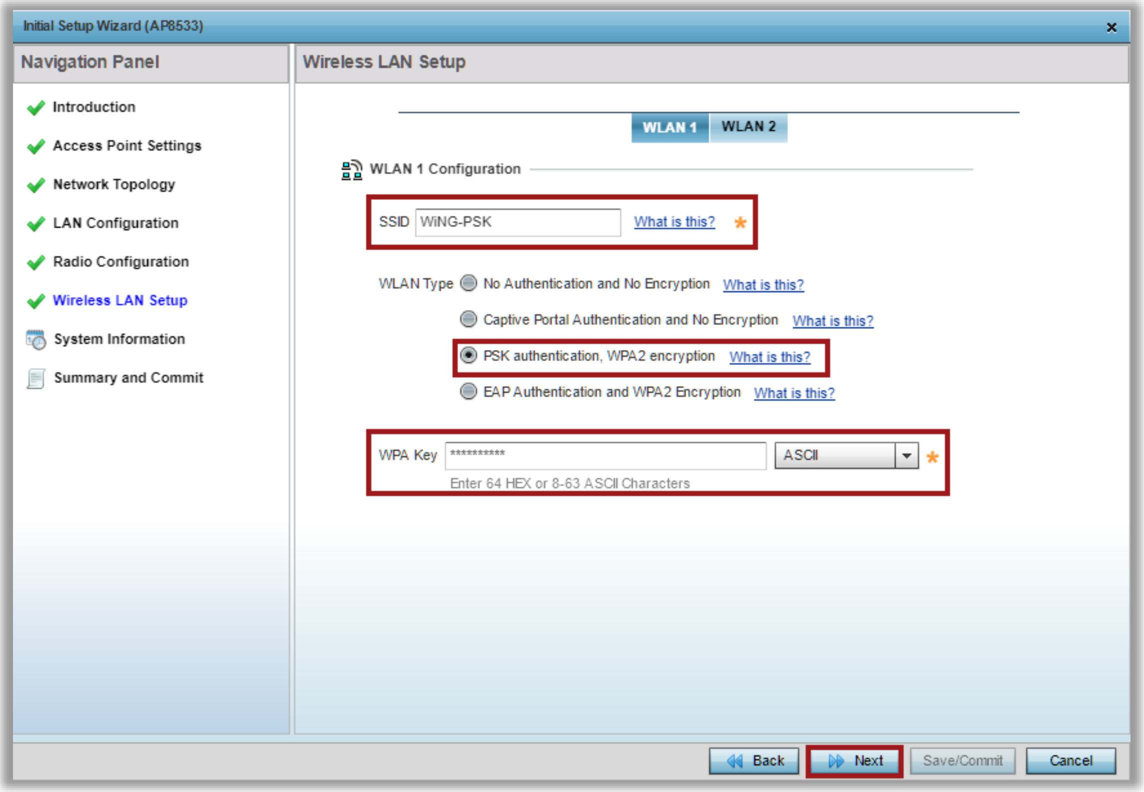
○ Configure as a Sensor Radio What is this?

○ Disable the Radio Radio 2 w ill be disabled. Please make sure this is w hat you w ant to do.

Radio 3

□ Configure as a Sensor Radio What is this?

On the Wireless LAN Setup screen we are going to create one SSID with CCMP encryption and PSK authentication:



Initial Setup Wizard (AP8533)

Navigation Panel

- ✓ Introduction
- ✓ Access Point Settings
- ✓ Network Topology
- ✓ LAN Configuration
- ✓ Radio Configuration
- ✓ Wireless LAN Setup
- System Information
- Summary and Commit

Wireless LAN Setup

WLAN 1 | WLAN 2

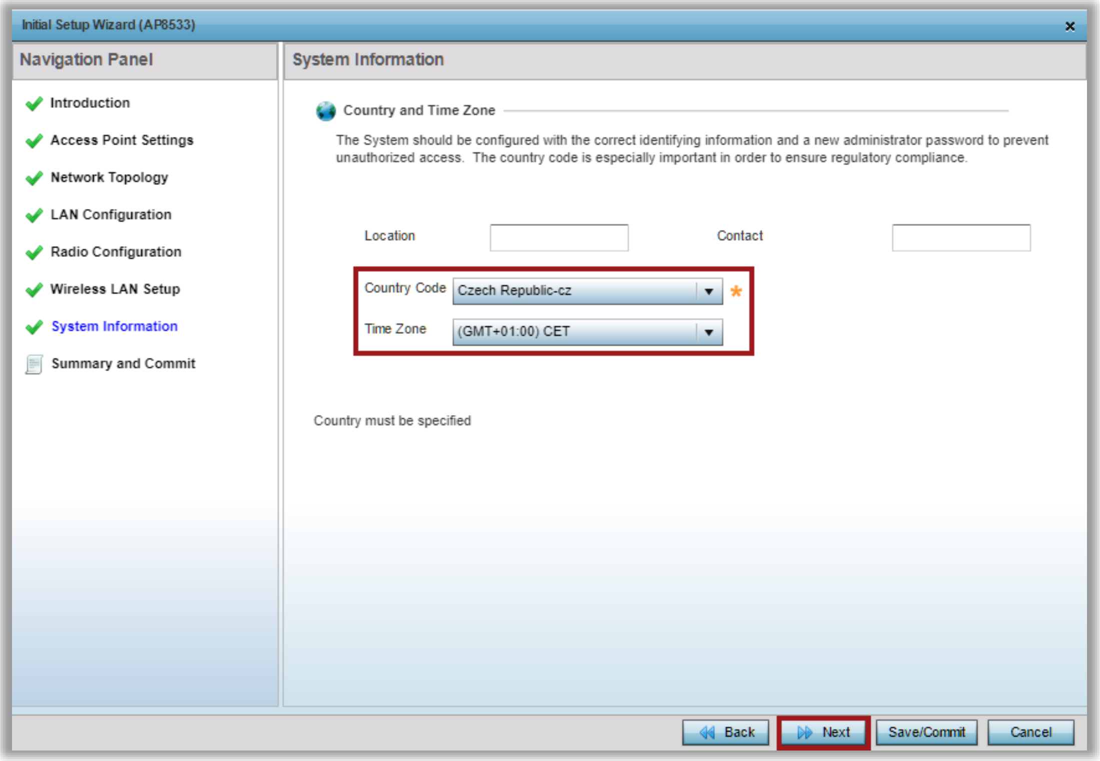
WLAN 1 Configuration

SSID: WiNG-PSK What is this? *

WLAN Type:
○ No Authentication and No Encryption What is this?
○ Captive Portal Authentication and No Encryption What is this?
● PSK authentication, WPA2 encryption What is this?
○ EAP Authentication and WPA2 Encryption What is this?

WPA Key: ********** ASCII *
Enter 64 HEX or 8-63 ASCII Characters

On the final configuration screen select *Country Code* so that AP can apply local regulatory rules and start advertising SSIDs, specify correct *Timezone* and then click *Next*:



System Information

Country and Time Zone

The System should be configured with the correct identifying information and a new administrator password to prevent unauthorized access. The country code is especially important in order to ensure regulatory compliance.

Location

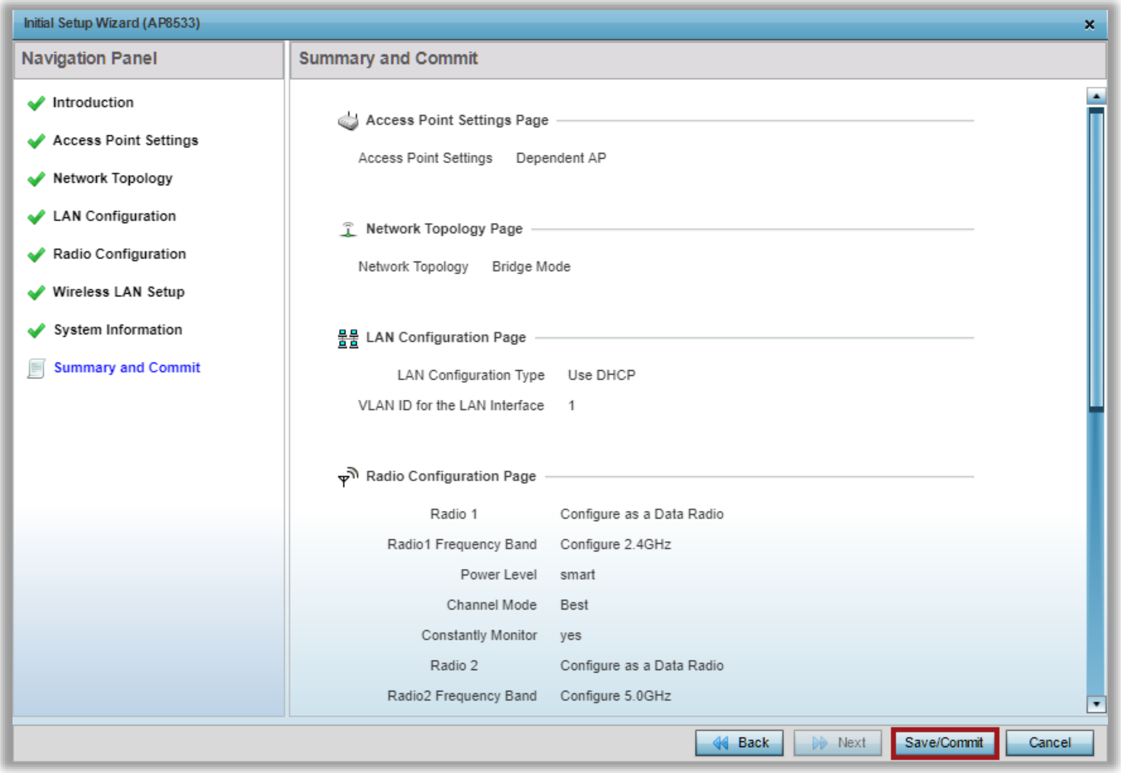
Contact

Country Code: Czech Republic-cz *

Time Zone: (GMT+01:00) CET

Country must be specified

Last page provides a summary of all the changes done using the Installation Wizard at which point you can click on *Save/Commit* button to apply them:



Summary and Commit

Access Point Settings Page

Access Point Settings: Dependent AP

Network Topology Page

Network Topology: Bridge Mode

LAN Configuration Page

LAN Configuration Type: Use DHCP

VLAN ID for the LAN Interface: 1

Radio Configuration Page

Radio 1: Configure as a Data Radio

Radio1 Frequency Band: Configure 2.4GHz

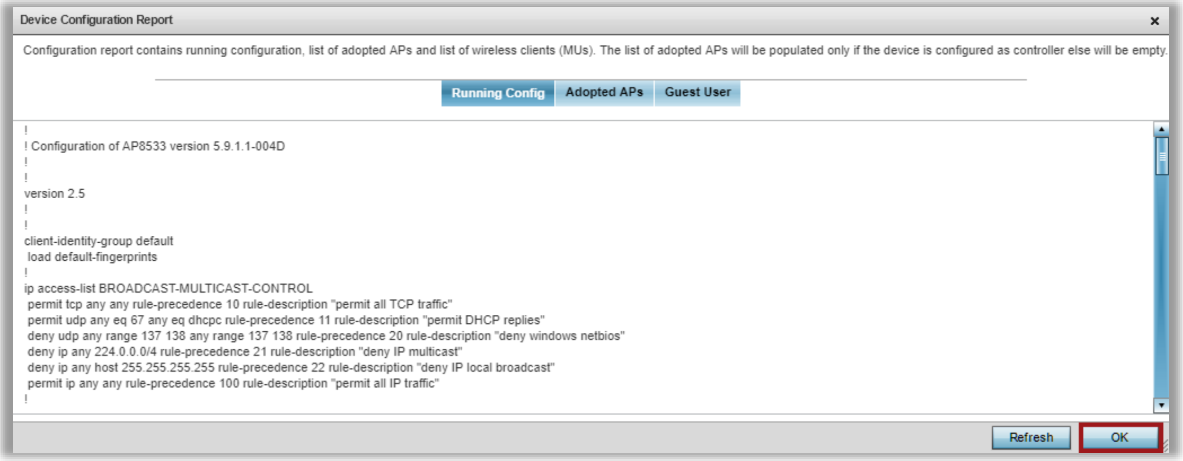
Power Level: smart

Channel Mode: Best

Constantly Monitor: yes

Radio 2: Configure as a Data Radio

Radio2 Frequency Band: Configure 5.0GHz



Configuration report contains running configuration, list of adopted APs and list of wireless clients (MUs). The list of adopted APs will be populated only if the device is configured as controller else will be empty.

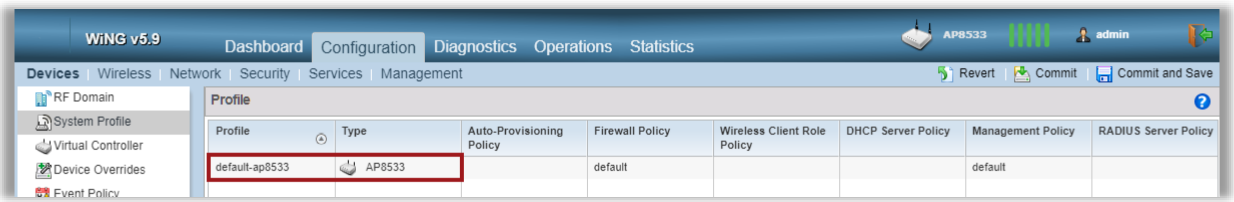
```
!
! Configuration of AP8533 version 5.9.1.1-004D
!
!
version 2.5
!
!
client-identity-group default
 load default-fingerprints
!
ip access-list BROADCAST-MULTICAST-CONTROL
 permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
 permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
 deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios"
 deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
 deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
 permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
```

Immediately after finishing with the installation wizard we can see another AP8533 as online. Why don’t we see other AP types? Read through the next 2 steps.

Step 3 – Managing mixed AP environment - Profiles

ExtremeWireless WiNG utilizes the concept of AP Profile to apply common configuration parameters, policies, Wireless LANs etc. to a group of Access Points, so that it is not needed to configure each and every AP individually.

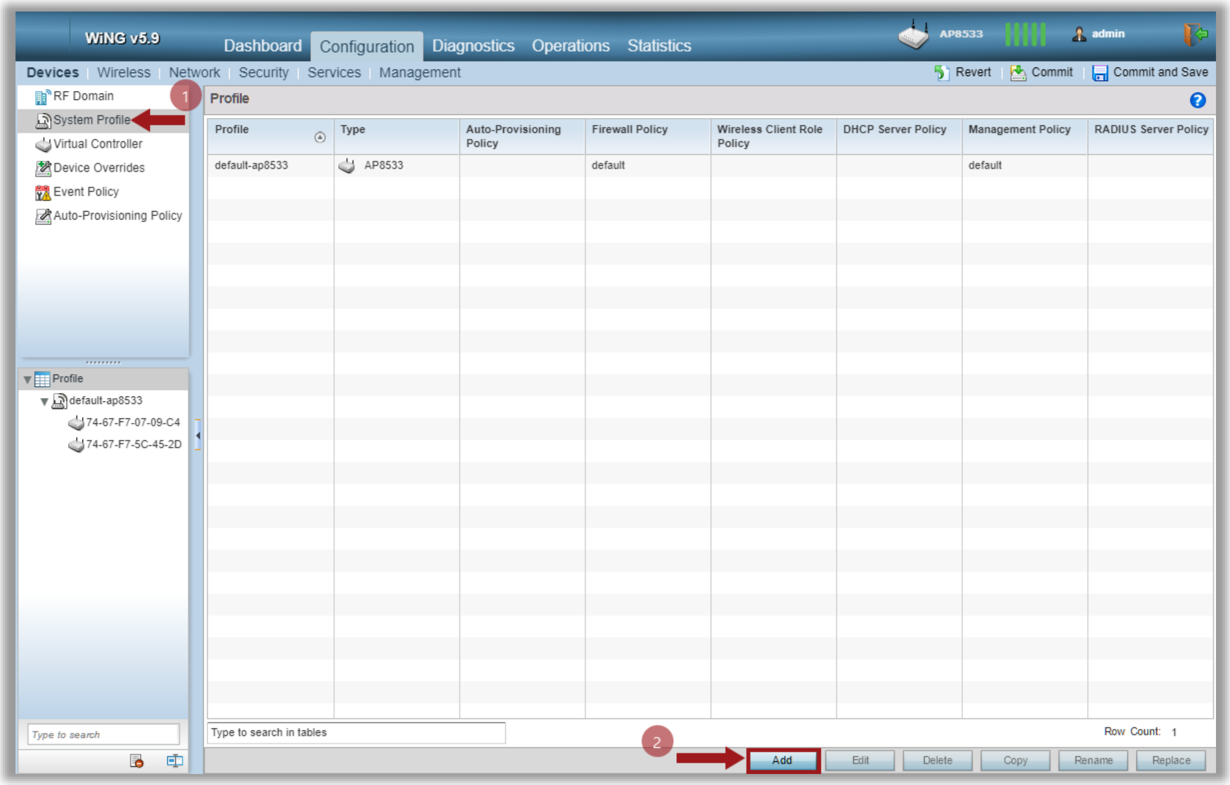
By default, Virtual Controller will use device specific AP profile that can only be used by like- Access Point types, in our example it is AP8533 default profile:



Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
default-ap8533	AP8533		default			default	

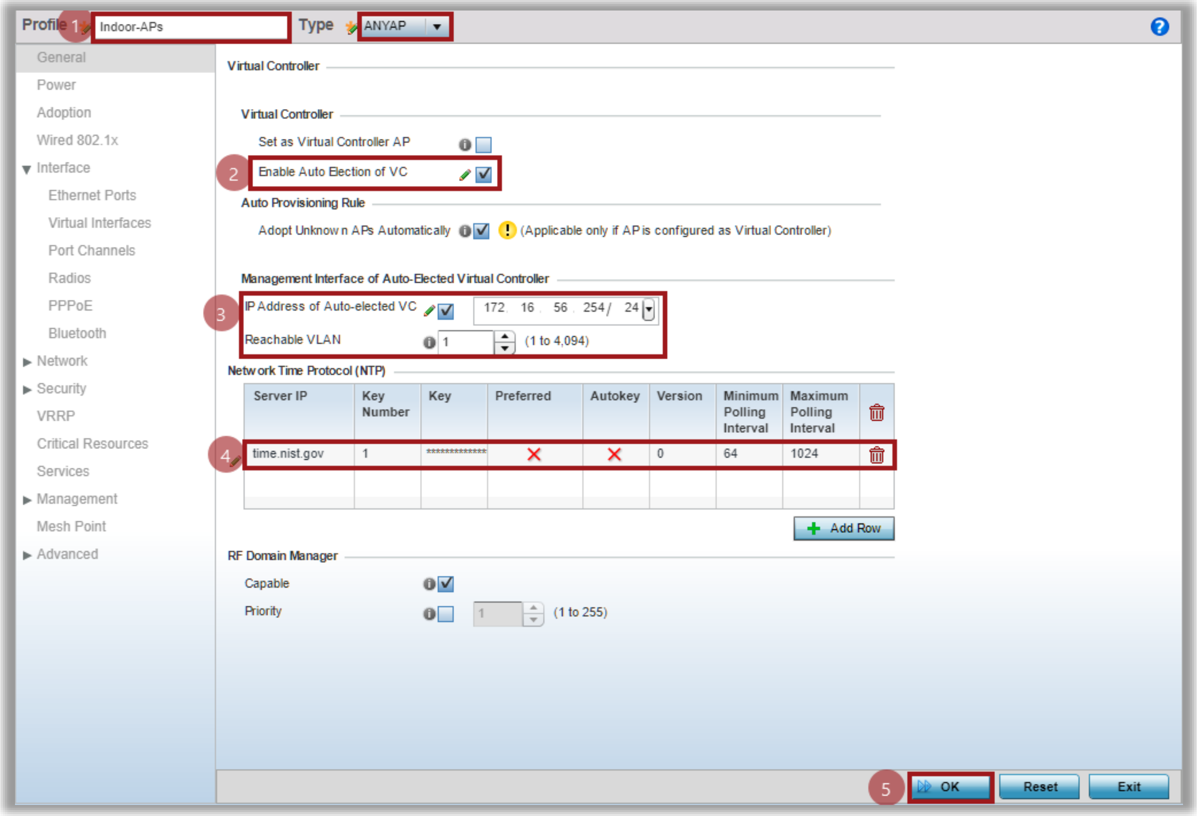
In order to manage multiple AP types, we need to utilize “anyap” Profiles, which can be used, as the name suggests, by any AP model types.

Let’s create a new *anyap* Profile for our Access Points, but first – login to the Virtual Controller UI using VC management IP address (do NOT connect to the real IP address of the AP you configured before):



Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
default-ap8533	AP8533		default			default	

Set AP Profile name, select Profile type as *ANYAP*, enable *Auto Election of VC*, specify *VC management IP address*, specify *NTP server*, then click *OK*:



1 Profile: Indoor-APs Type: ANYAP

Virtual Controller

Virtual Controller

Set as Virtual Controller AP □

2 Enable Auto Election of VC ☑

Auto Provisioning Rule

Adopt Unknown APs Automatically ☑ (Applicable only if AP is configured as Virtual Controller)

Management Interface of Auto-Elected Virtual Controller

3 IP Address of Auto-elected VC ☑ 172 . 16 . 56 . 254 / 24

Reachable VLAN 1 (1 to 4,094)

Network Time Protocol (NTP)

Server IP	Key Number	Key	Preferred	Autokey	Version	Minimum Polling Interval	Maximum Polling Interval
4 time.nist.gov	1	*************	✗	✗	0	64	1024

Add Row

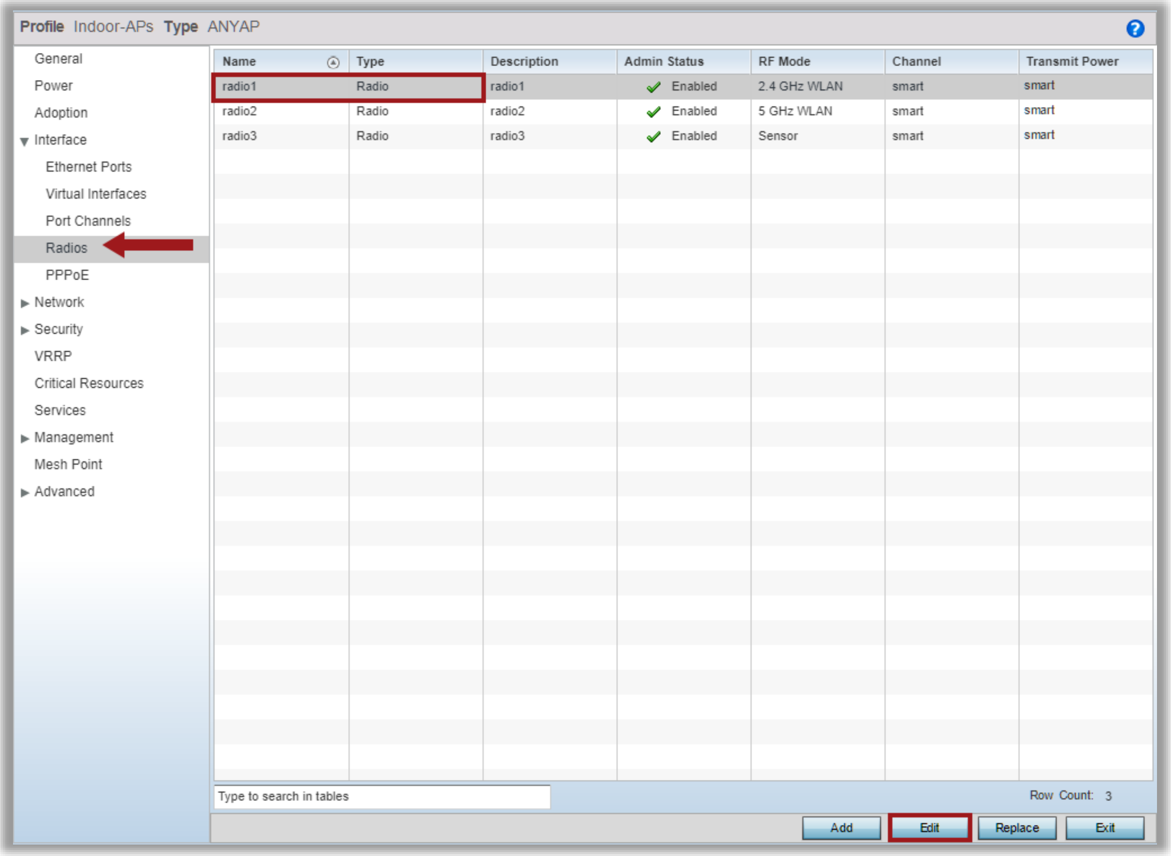
RF Domain Manager

Capable ☑

Priority □ 1 (1 to 255)

5 OK Reset Exit

Move to the *Interface > Radios* section of the AP Profile and edit *radio 1* (2.4GHz) interface:

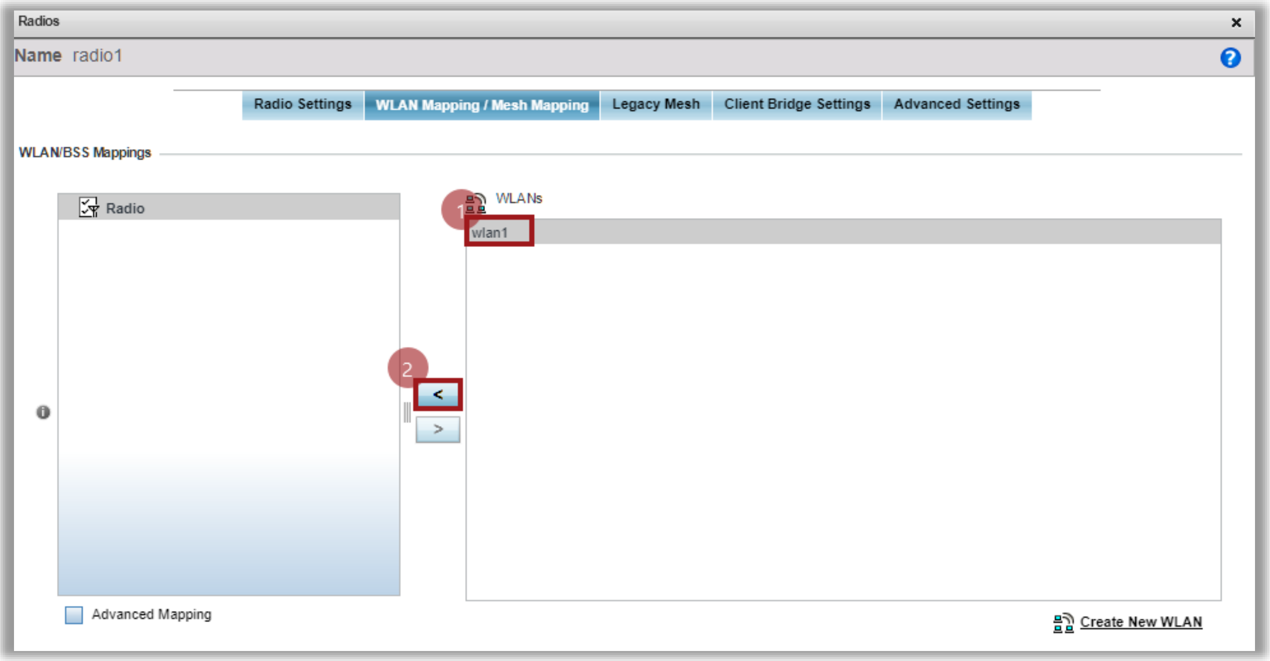


Profile Indoor-APs Type ANYAP

Name	Type	Description	Admin Status	RF Mode	Channel	Transmit Power
radio1	Radio	radio1	✓ Enabled	2.4 GHz WLAN	smart	smart
radio2	Radio	radio2	✓ Enabled	5 GHz WLAN	smart	smart
radio3	Radio	radio3	✓ Enabled	Sensor	smart	smart

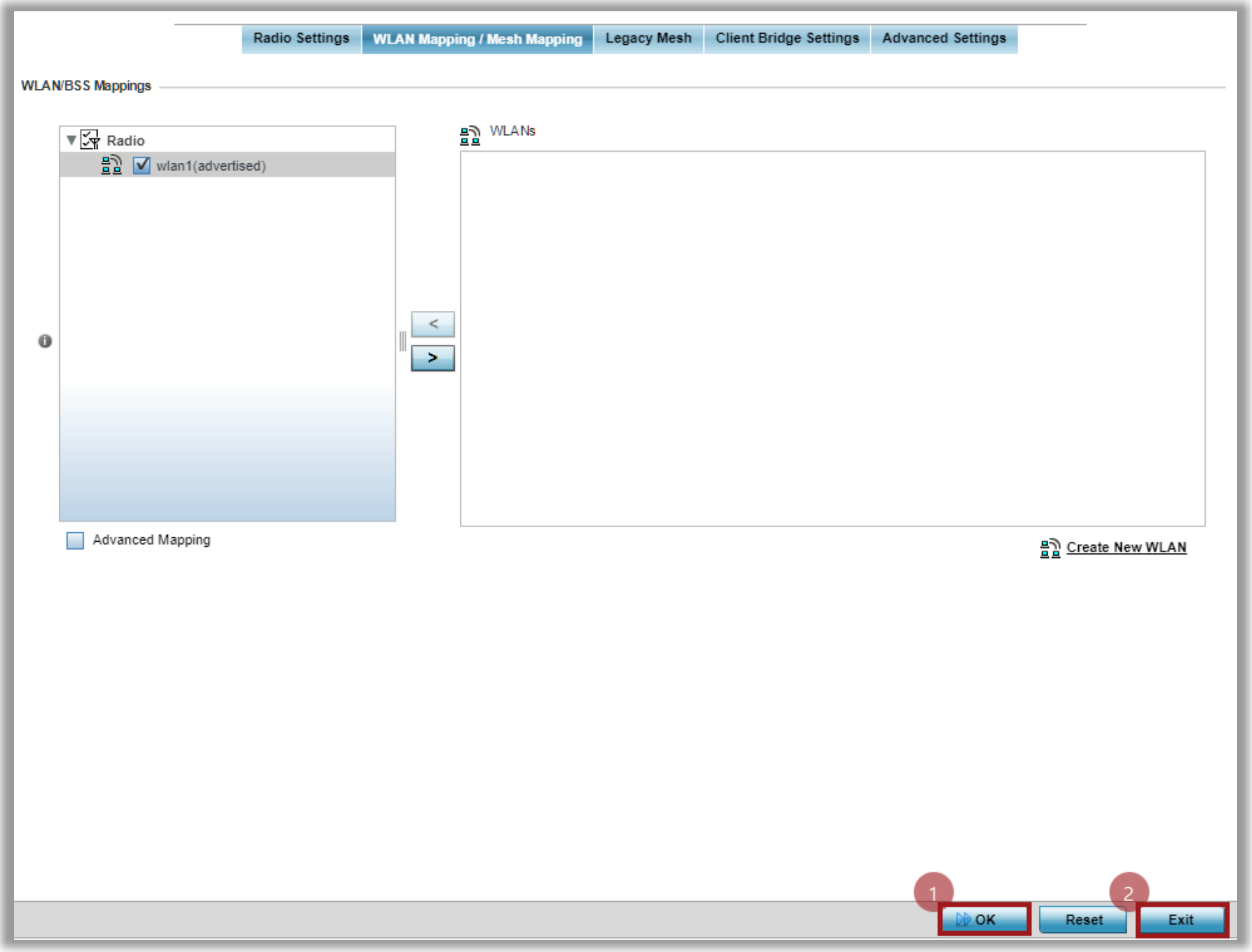
Row Count: 3

Switch to the *WLAN Mapping / Mesh Mapping* tab and move the Wireless LAN created during the Installation Wizard process to the radio. This will effectively advertize that particular WLAN/SSID on a particular radio:

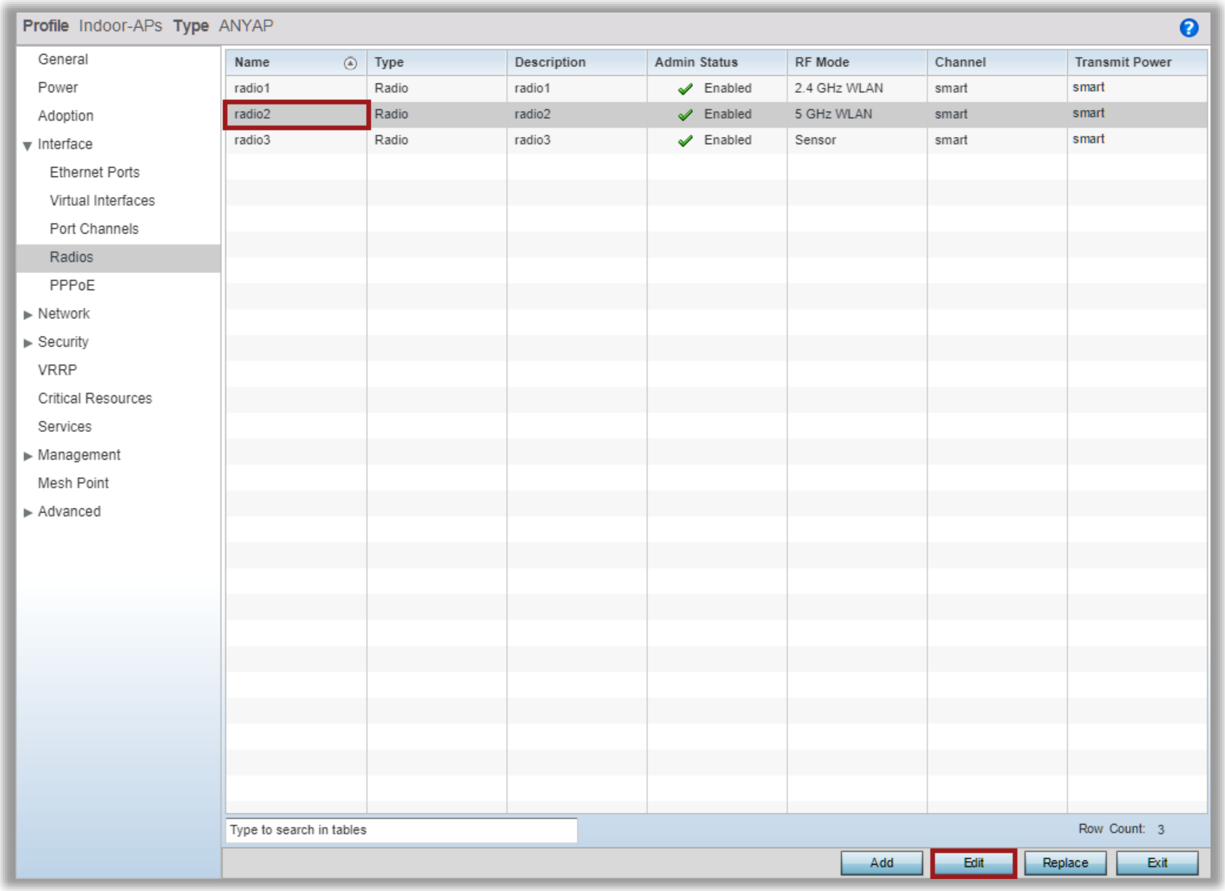


Radios

Name radio1


Radio Settings
WLAN Mapping / Mesh Mapping
Legacy Mesh
Client Bridge Settings
Advanced Settings
WLAN/BSS Mappings
Radio
☑ wlan1(advertised)
WLANs
<
>
□ Advanced Mapping
Create New WLAN
1
2
OK
Reset
Exit

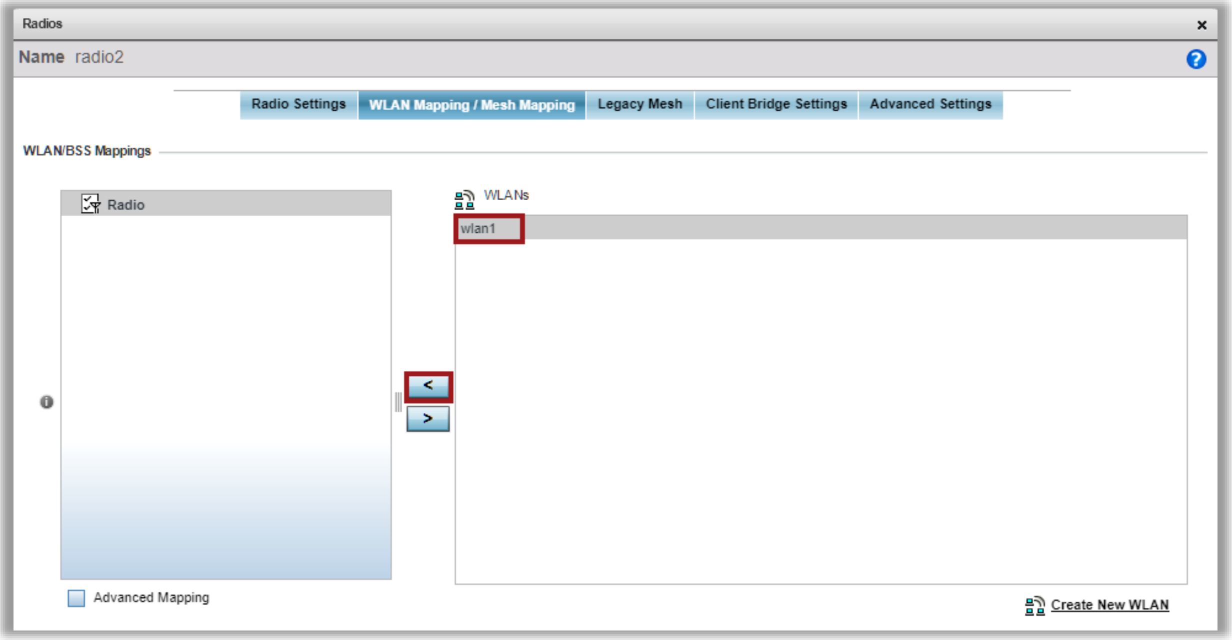
Repeat the steps for the second radio interface (5GHz):



Profile Indoor-APs **Type** ANYAP

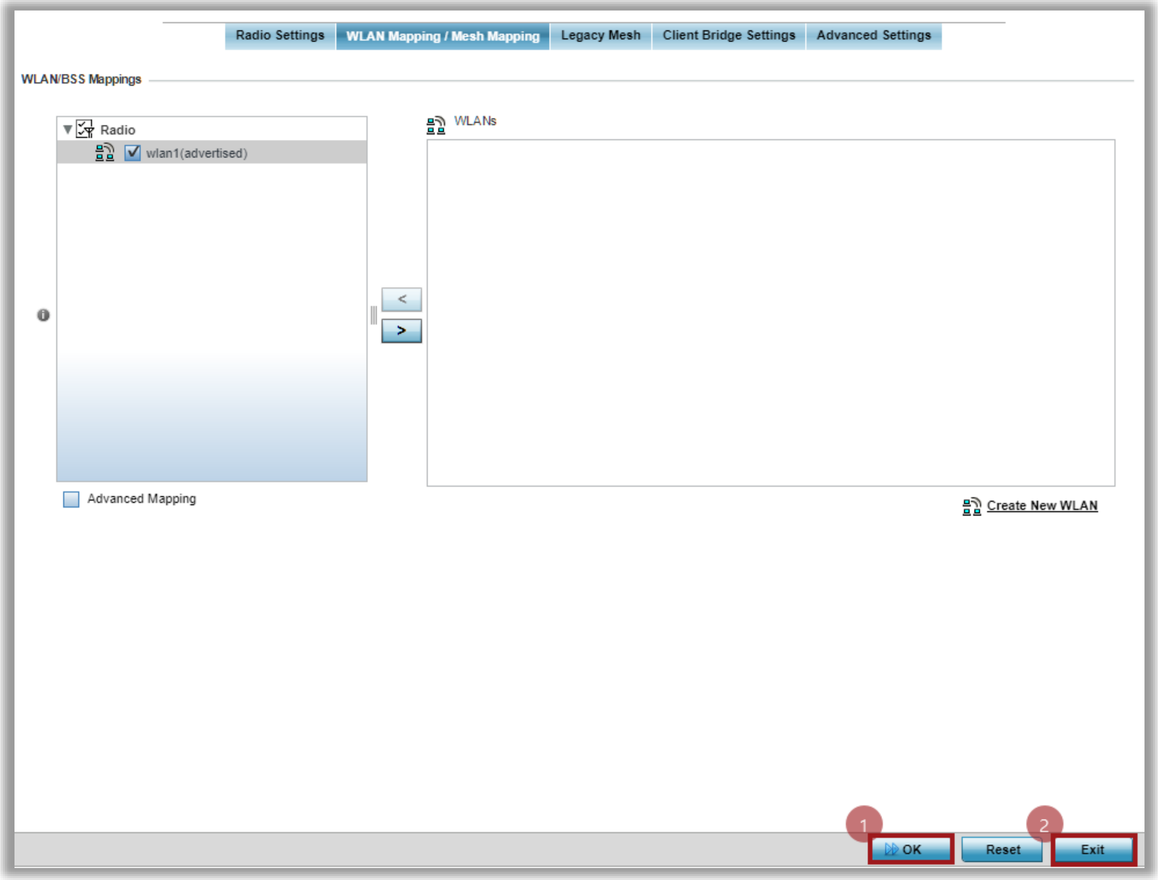
Name	Type	Description	Admin Status	RF Mode	Channel	Transmit Power
radio1	Radio	radio1	✓ Enabled	2.4 GHz WLAN	smart	smart
radio2	Radio	radio2	✓ Enabled	5 GHz WLAN	smart	smart
radio3	Radio	radio3	✓ Enabled	Sensor	smart	smart

Row Count: 3

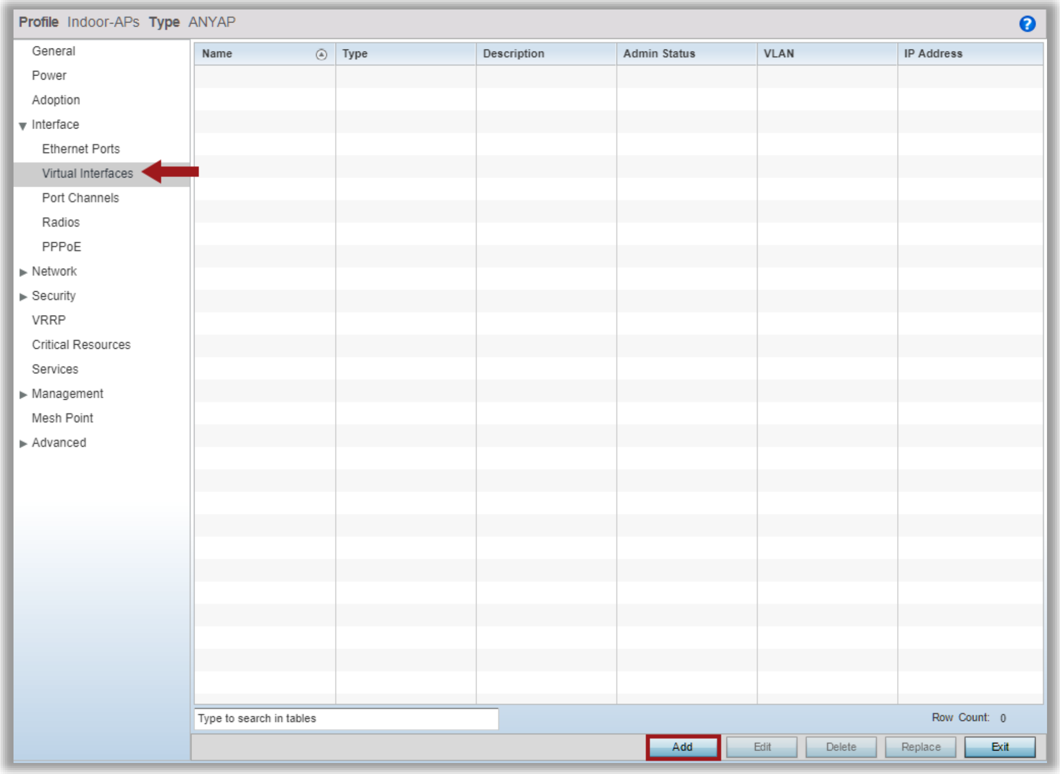


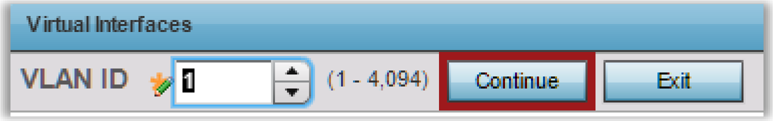
Radios

Name radio2

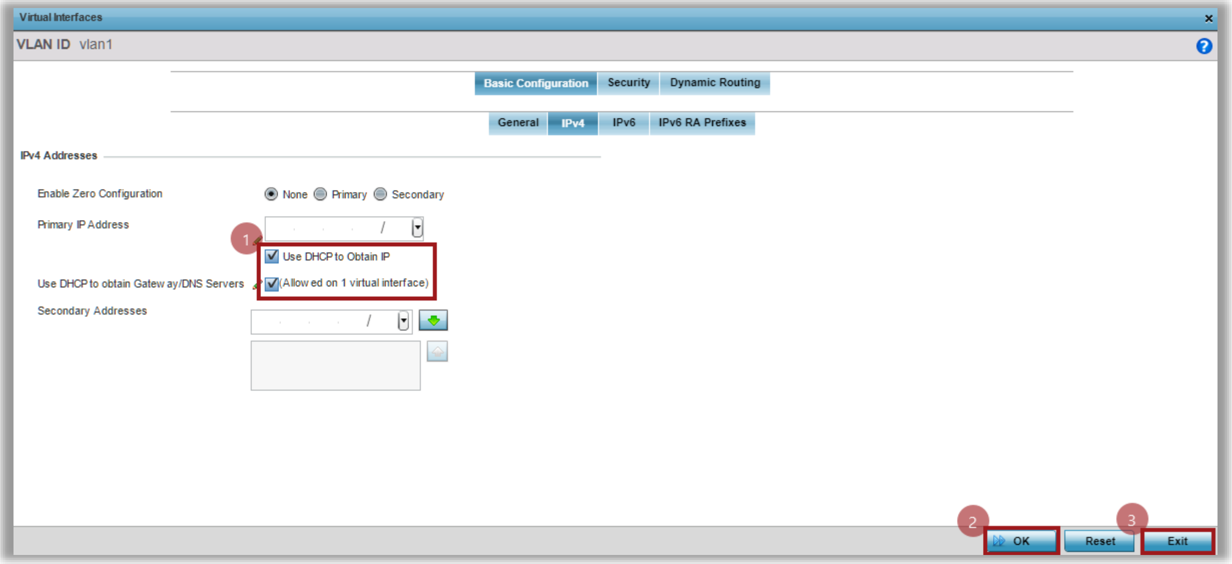


Lastly, create a *Switch Virtual Interface* (SVI) and allow the AP to obtain IPv4 addressing via DHCP. Note that by default any new AP profile does not have any SVI defined, so if this step is skipped, AP won't get any IP address at all:





VLAN ID 1 (1 - 4,094)



VLAN ID vlan1

IPv4 Addresses

Enable Zero Configuration ● None ○ Primary ○ Secondary

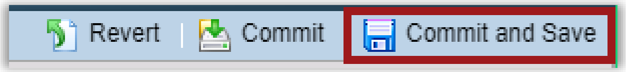
Primary IP Address . . . /

☑ Use DHCP to Obtain IP

Use DHCP to obtain Gateway/DNS Servers ☑ (Allowed on 1 virtual interface)

Secondary Addresses . . . /

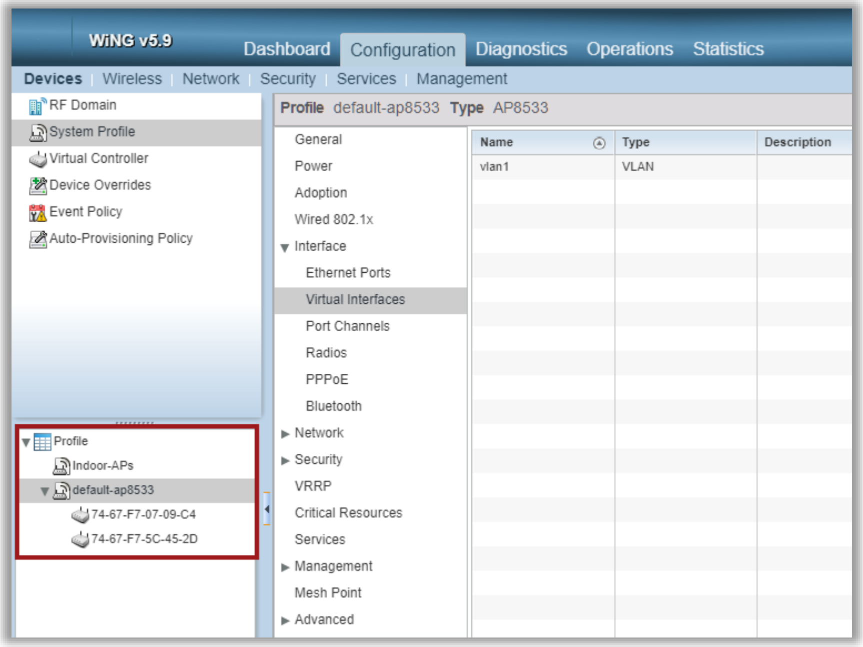
Commit and Save changes. Note that *Commit* action applies changed and saves them to the running configuration that does not survive AP reboot, while *Commit&Save* action saves changes to both running and startup configs, which will be saved across AP reboots:



Step 4 – Managing mixed AP environment – Auto Provisioning Policy

Now that you have created the new AP profile, how you can use it?

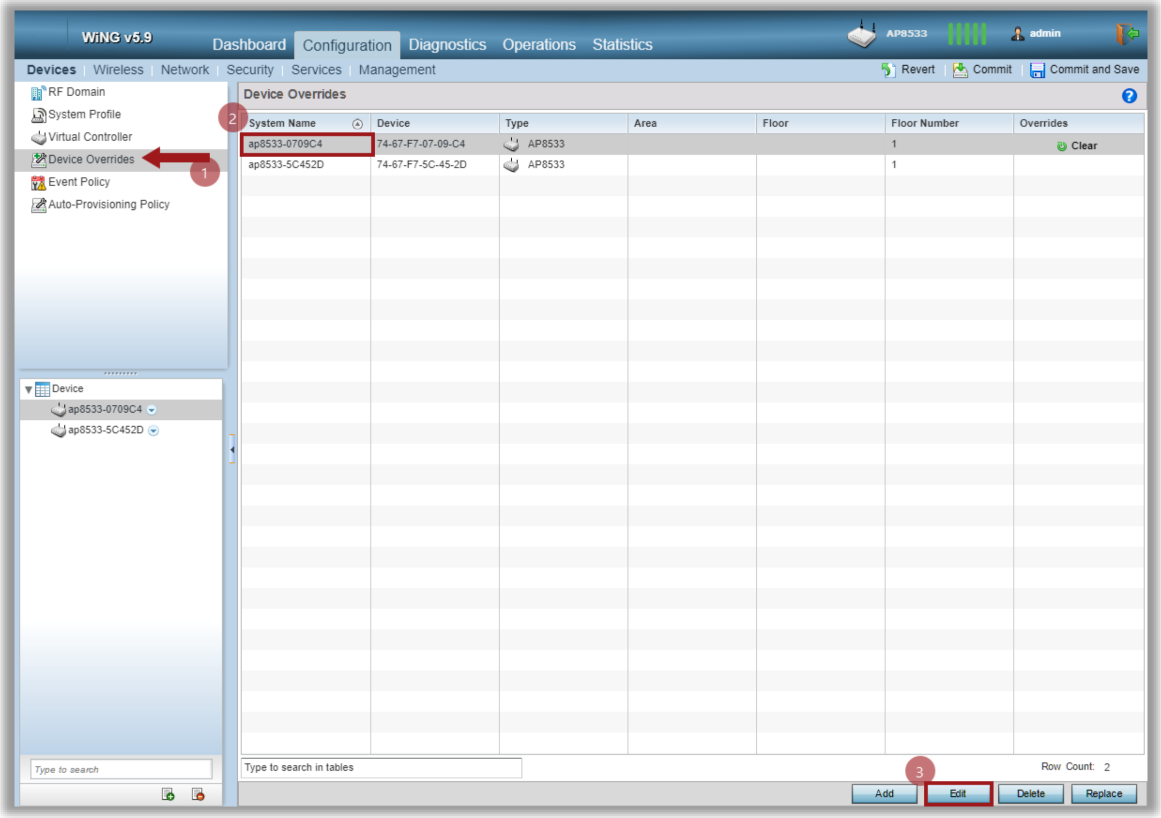
If you check under System Profile Configuration section, you can still see that both AP8533s are using the old default-ap8533 profile. How to update it?



Profile default-ap8533 **Type** AP8533

Name	Type	Description
vlan1	VLAN	

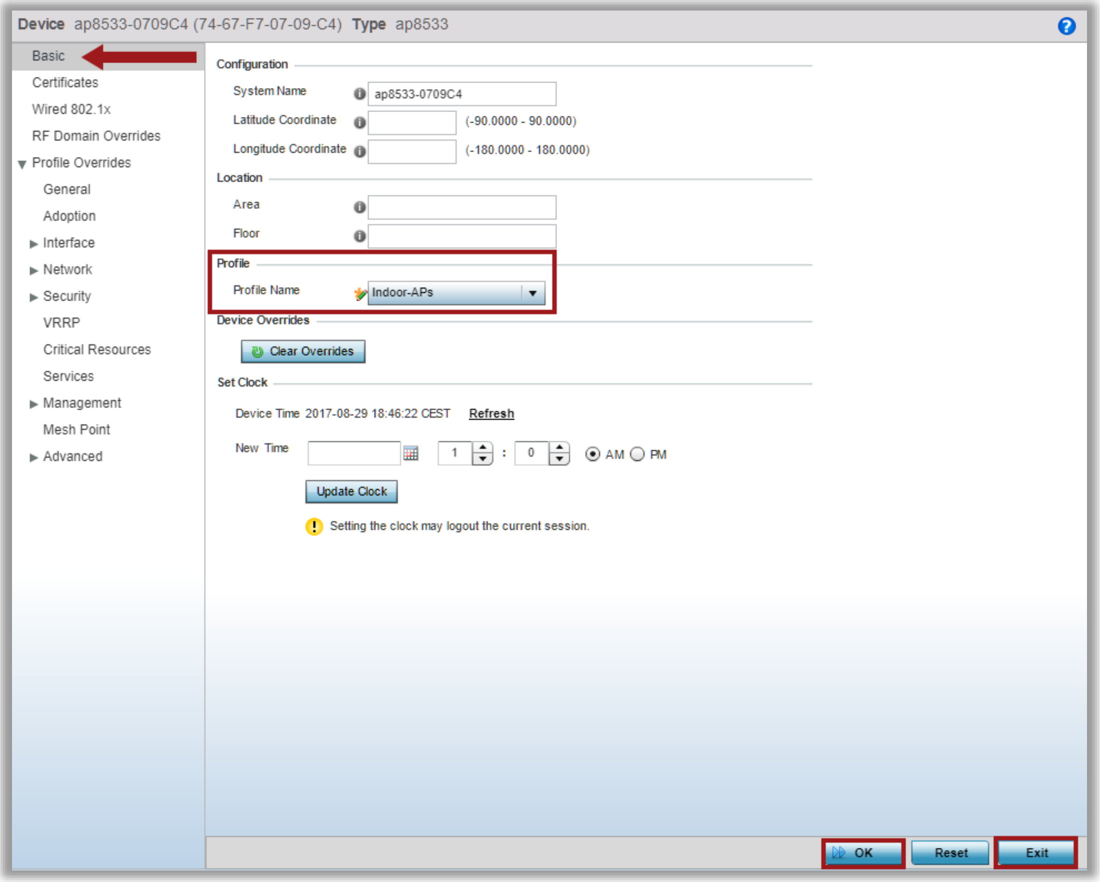
One option is to assign profiles statically under Device Overrides tab. This is what we are going to do with our existing two Access Points:



Device Overrides

System Name	Device	Type	Area	Floor	Floor Number	Overrides
ap8533-0709C4	74-67-F7-07-09-C4	AP8533			1	Clear
ap8533-5C452D	74-67-F7-5C-45-2D	AP8533			1	

Row Count: 2



Device ap8533-0709C4 (74-67-F7-07-09-C4) **Type** ap8533

Configuration

System Name: ap8533-0709C4

Latitude Coordinate: (-90.0000 - 90.0000)

Longitude Coordinate: (-180.0000 - 180.0000)

Location

Area:

Floor:

Profile

Profile Name: Indoor-APs

Device Overrides

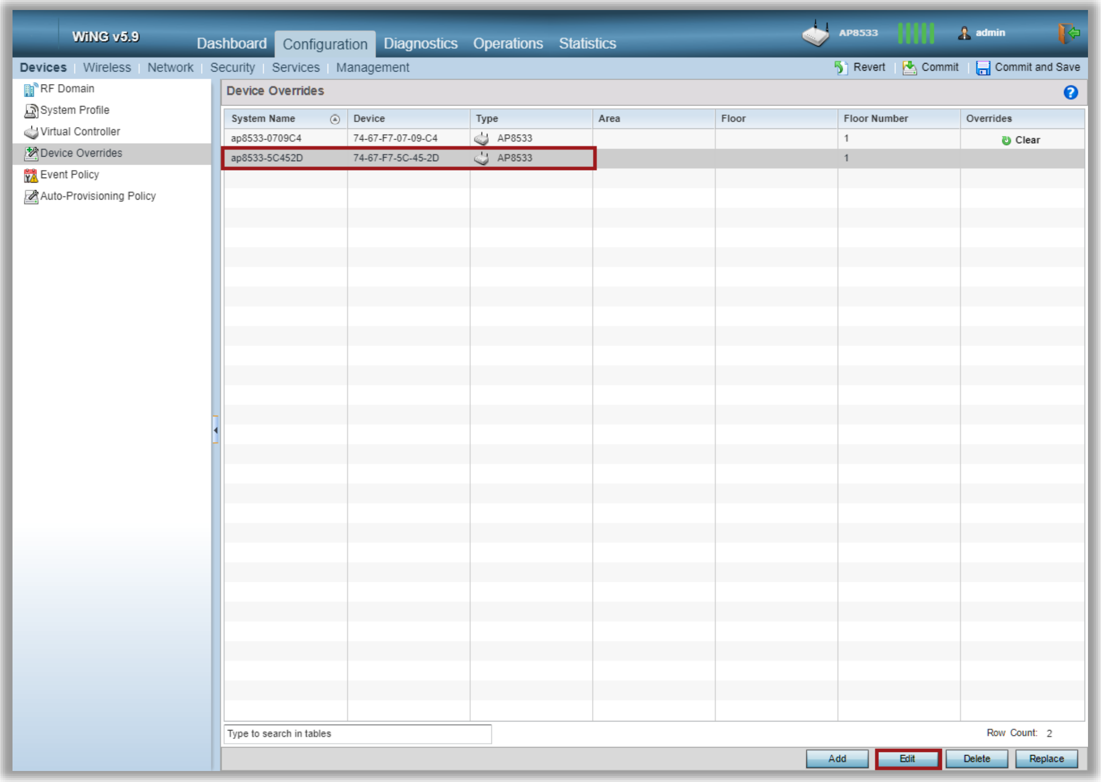
Set Clock

Device Time 2017-08-29 18:46:22 CEST **Refresh**

New Time: 1 : 0 ● AM ○ PM

Setting the clock may logout the current session.

Repeat the same steps for the second Access Point:

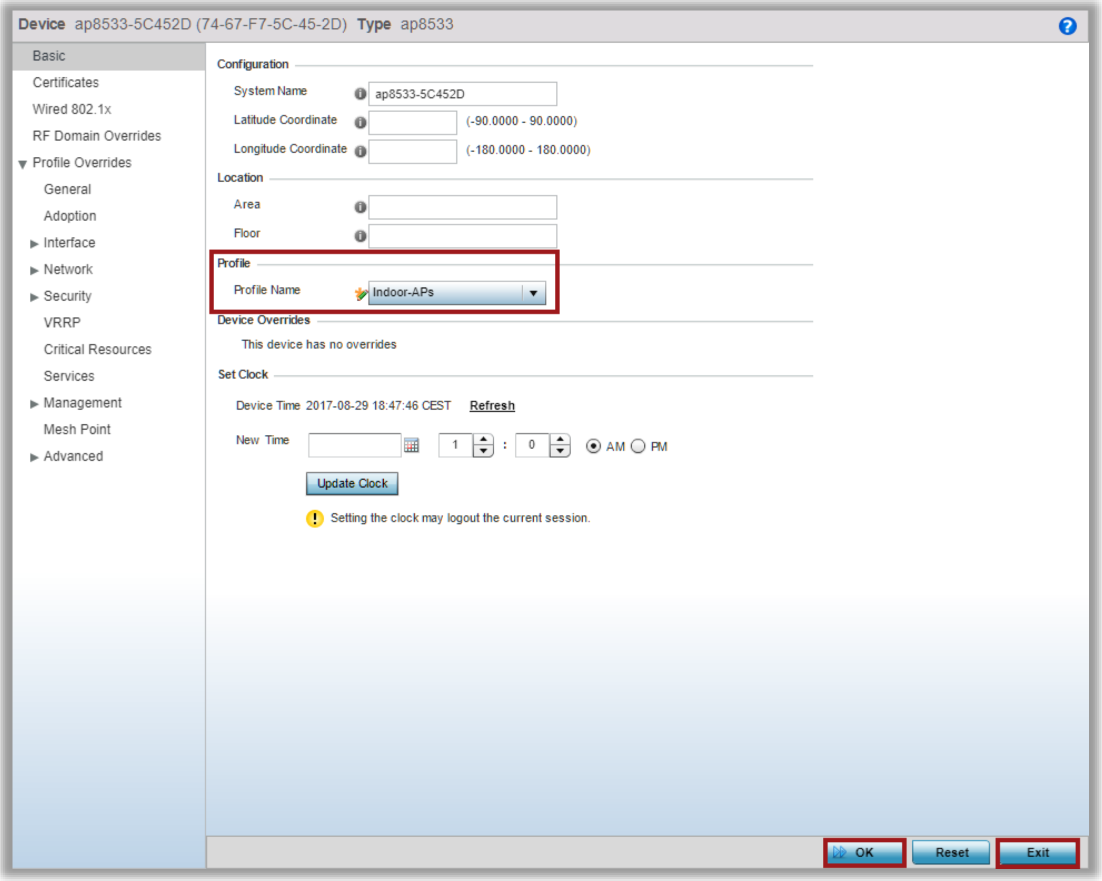


Device Overrides

System Name	Device	Type	Area	Floor	Floor Number	Overrides
ap8533-0709C4	74-67-F7-07-09-C4	AP8533			1	Clear
ap8533-5C452D	74-67-F7-5C-45-2D	AP8533			1	

Type to search in tables

Row Count: 2



Device ap8533-5C452D (74-67-F7-5C-45-2D) Type ap8533

Configuration

System Name: ap8533-5C452D

Latitude Coordinate: (-90.0000 - 90.0000)

Longitude Coordinate: (-180.0000 - 180.0000)

Location

Area:

Floor:

Profile

Profile Name: Indoor-APs

Device Overrides

This device has no overrides

Set Clock

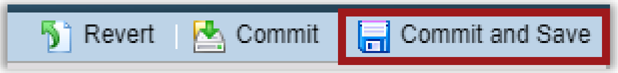
Device Time 2017-08-29 18:47:46 CEST Refresh

New Time: 1 : 0 ● AM ○ PM

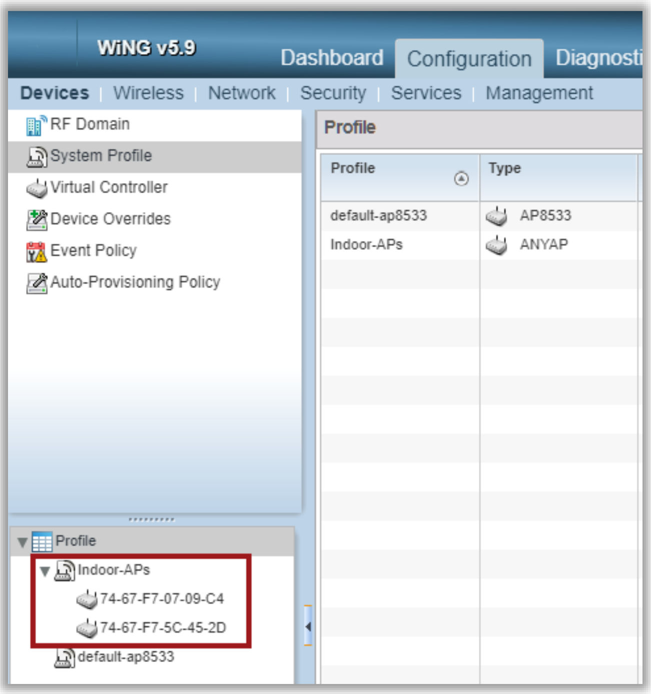
Update Clock

Setting the clock may logout the current session.

Commit&Save changes:



Now let's verify if our APs are using the new Profile:



Profile

Profile	Type
default-ap8533	AP8533
Indoor-APs	ANYAP

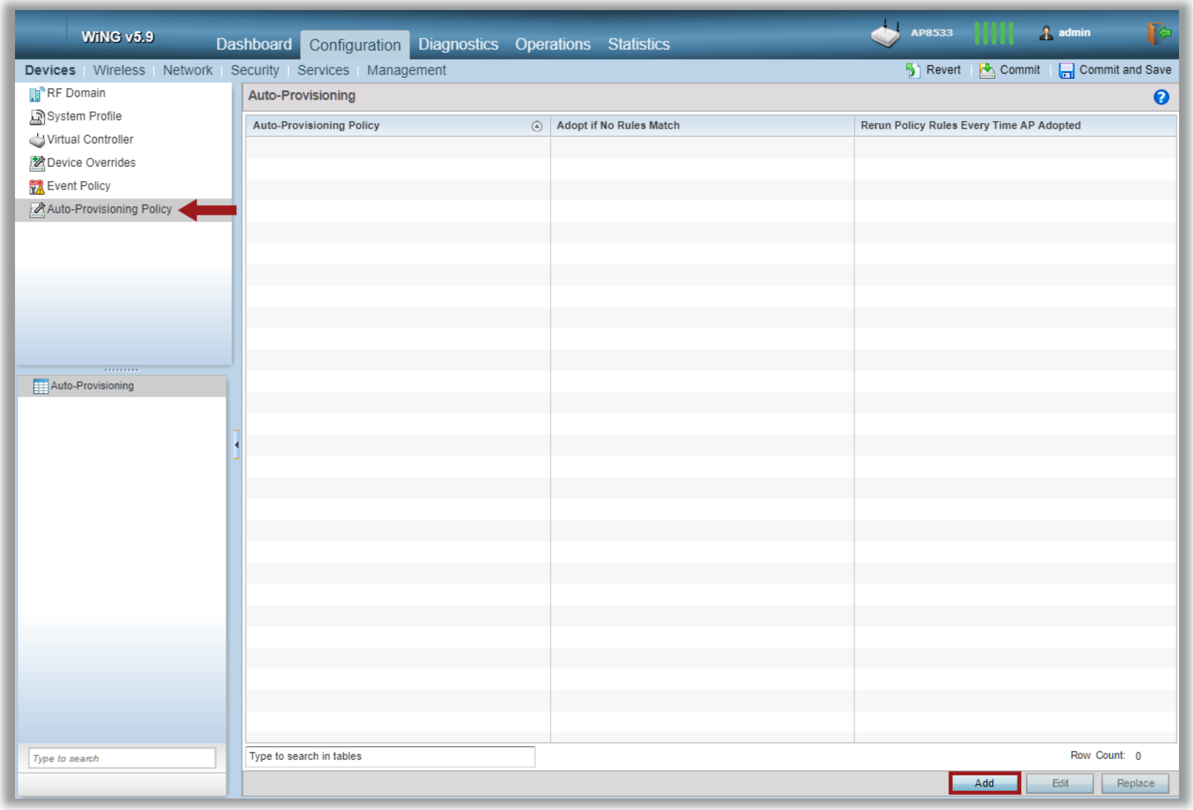
While assigning Profile statically is a viable option, it might take a lot of effort and time when managing dozens of Access Points and is prone to human errors. There is an alternative and recommended solution.

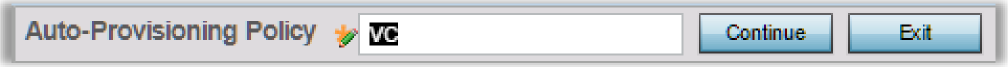
WiNG provides an automated way to assign Profiles using Auto-Provisioning Policy.

How it works? Whenever a new out-the-box AP discovers a Virtual Controller on the network (at Layer2), it will send an adoption request and some additional information to identify itself, such as its MAC address, Model Number, Serial Number, source IP/Subnet, Hostname, and so on and so on. Virtual Controller can utilize AutoProvisioning Rules to automatically assign different Profiles based on the information received from the APs.

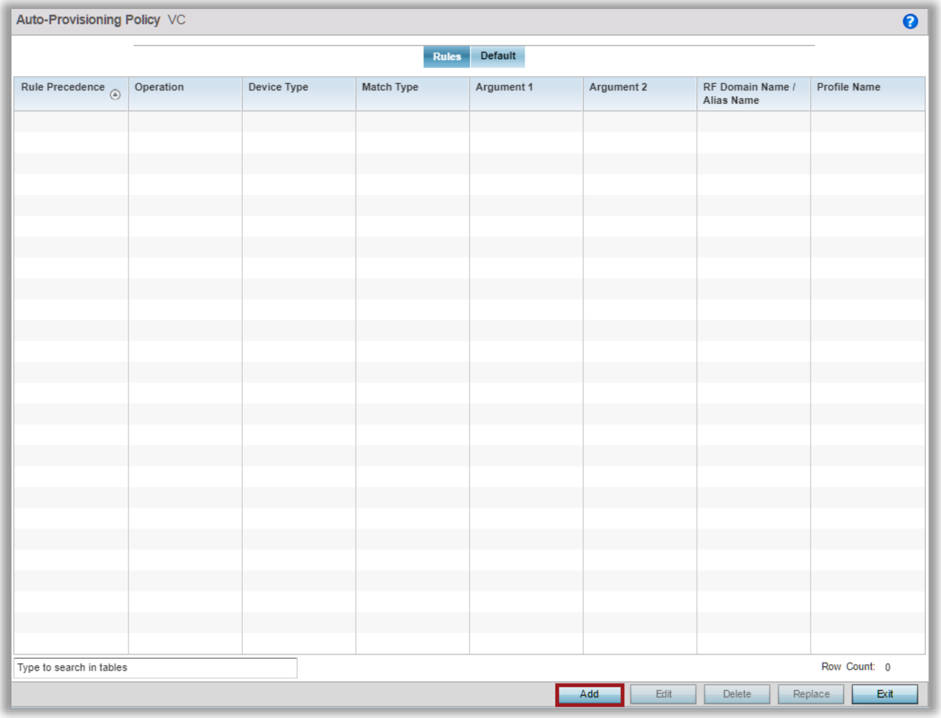
In our example we will allow any Access Point to adopt to our Virtual Controller and get the new “Indoor-APs” profile.

First, let’s create an *Auto-Provisioning policy*:




Auto-Provisioning Policy: VC

Now let's add a new AutoProvisioning Rule:

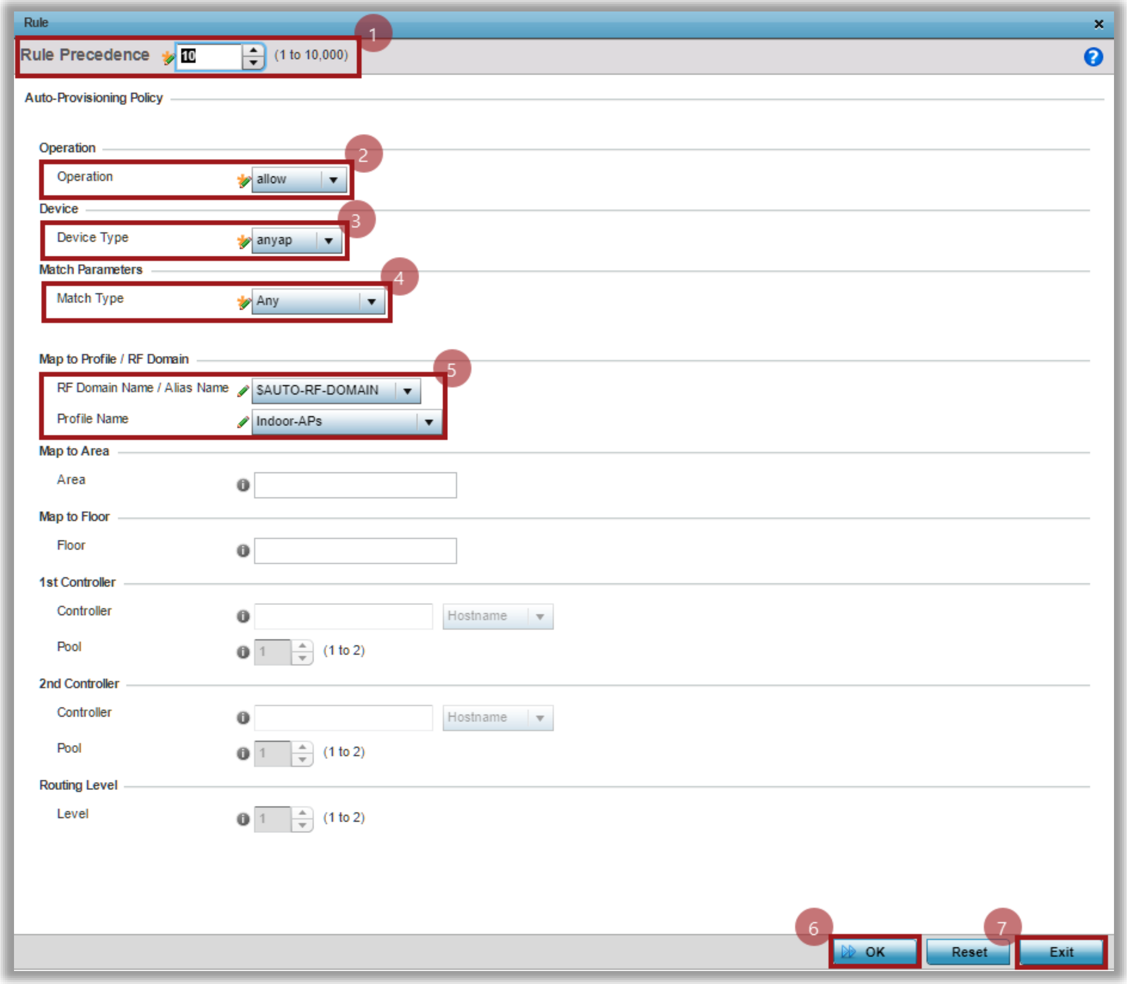


Auto-Provisioning Policy VC

Rule Precedence	Operation	Device Type	Match Type	Argument 1	Argument 2	RF Domain Name / Alias Name	Profile Name

Type to search in tables

Row Count: 0



Rule

Rule Precedence: 10 (1 to 10,000)

Auto-Provisioning Policy

Operation

Operation: allow

Device

Device Type: anyap

Match Parameters

Match Type: Any

Map to Profile / RF Domain

RF Domain Name / Alias Name: $AUTO-RF-DOMAIN

Profile Name: Indoor-APs

Map to Area

Area:

Map to Floor

Floor:

1st Controller

Controller: Hostname

Pool: 1 (1 to 2)

2nd Controller

Controller: Hostname

Pool: 1 (1 to 2)

Routing Level

Level: 1 (1 to 2)

Let’s take a look at what all the options above mean:

1- **Rule Precedence** – this is effectively a rule order inside the AutoProvisioning Policy. The policy works on a principle “first match wins”.

2- **Operation** – it can be *allow* or *deny* adoption, so for example an admin can explicitly deny certain APs adoption based on match criteria (use-case: “*I don’t want APs from switch2 to adopt to my VC*”)

3- **Device Type** – this option specifies which AP type will match the rule. It can be device specific, like AP8533 or AP7622, etc. or it can match to any AP type.

4- **Match Type** – this is where AutoProvisioning flexibility lies. A rule can match an AP based on these criteria:

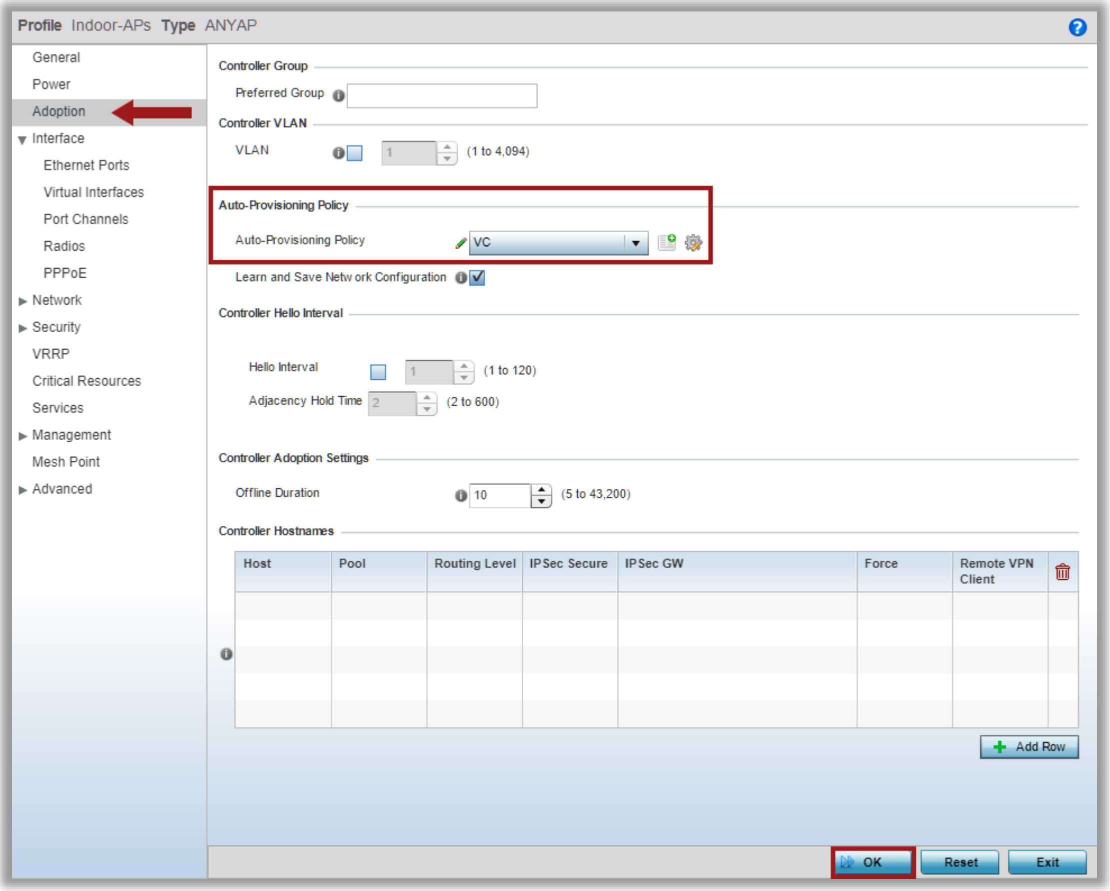
a.	any	Match any device
b.	area	Area name or string alias
c.	cdp-match	Match device location based on CDP snoop
d.	dhcp-option	Match the value of DHCP option
e.	floor	Floor name or string alias
f.	fqdn	Match the value of FQDN
g.	ip	Match device IP address
h.	lldp-match	Match device location based on LLDP snoop
i.	mac	Match device MAC address
j.	model-number	Match device model number
k.	serial-number	Match device serial number
l.	vlan	Match device VLAN

In our example we are going to use “any” match for simplicity.

5- **RF Domain** – in VC deployments always use $AUTO-RF-DOMAIN option. This will automatically assign the same RF Domain to the adopted AP, as the one VC is using right now.

6- **Profile Name** – specify which AP Profile to assign to the adopted Access Point. In our case we will set it to “Indoor-APs” profile that we’ve created in the previous step.

After the Auto-Provisioning rule is created, we will need to assign this policy to the AP profile in order to activate it. Go back to the Indoor-APs profile and move to the Adoption tab:



Profile Indoor-APs Type ANYAP

Controller Group

Preferred Group

Controller VLAN

VLAN □ 1 (1 to 4,094)

Auto-Provisioning Policy

Auto-Provisioning Policy VC

Learn and Save Netw ork Configuration ☑

Controller Hello Interval

Hello Interval □ 1 (1 to 120)

Adjacency Hold Time 2 (2 to 600)

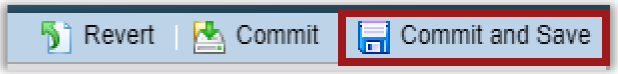
Controller Adoption Settings

Offline Duration 10 (5 to 43,200)

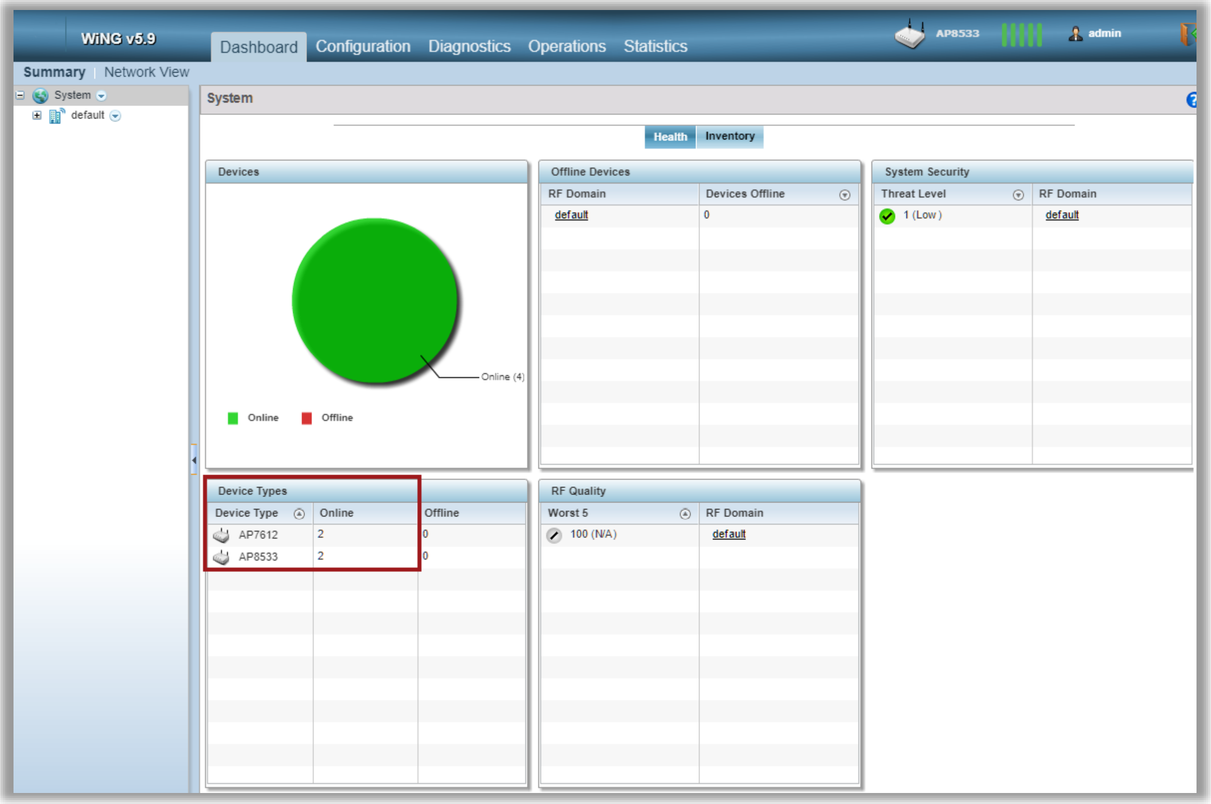
Controller Hostnames

Host	Pool	Routing Level	IPSec Secure	IPSec GW	Force	Remote VPN Client

Commit&Save changes:



Now just after few seconds we can see other Access Points online and in adopted state:



Offline Devices

RF Domain	Devices Offline
default	0

System Security

Threat Level	RF Domain
✓ 1 (Low)	default

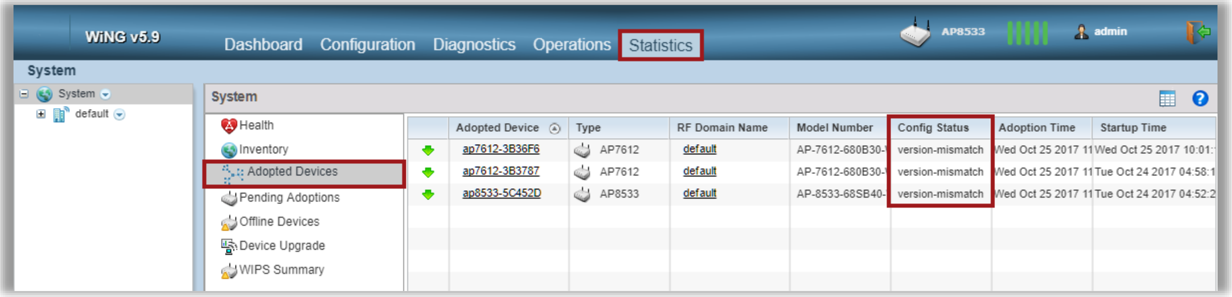
Device Types

Device Type	Online	Offline
AP7612	2	0
AP8533	2	0

RF Quality

Worst 5	RF Domain
100 (N/A)	default

However, it might happen that adopted Access Points will have a different firmware version and therefore will adopt in the version-mismatch state, which will prevent them from getting any configuration updates from the VC:



	Adopted Device	Type	RF Domain Name	Model Number	Config Status	Adoption Time	Startup Time
⬇	ap7612-3B36F6	AP7612	default	AP-7612-680B30-	version-mismatch	Wed Oct 25 2017 11	Wed Oct 25 2017 10:01:
⬇	ap7612-3B3787	AP7612	default	AP-7612-680B30-	version-mismatch	Wed Oct 25 2017 11	Tue Oct 24 2017 04:58:1
⬇	ap8533-5C452D	AP8533	default	AP-8533-68SB40-	version-mismatch	Wed Oct 25 2017 11	Tue Oct 24 2017 04:52:2

How to upgrade them? Read on the next section.

Step 5 – Adopted AP Upgrades

In a Virtual Controller environment, VC is responsible for upgrading the whole network.

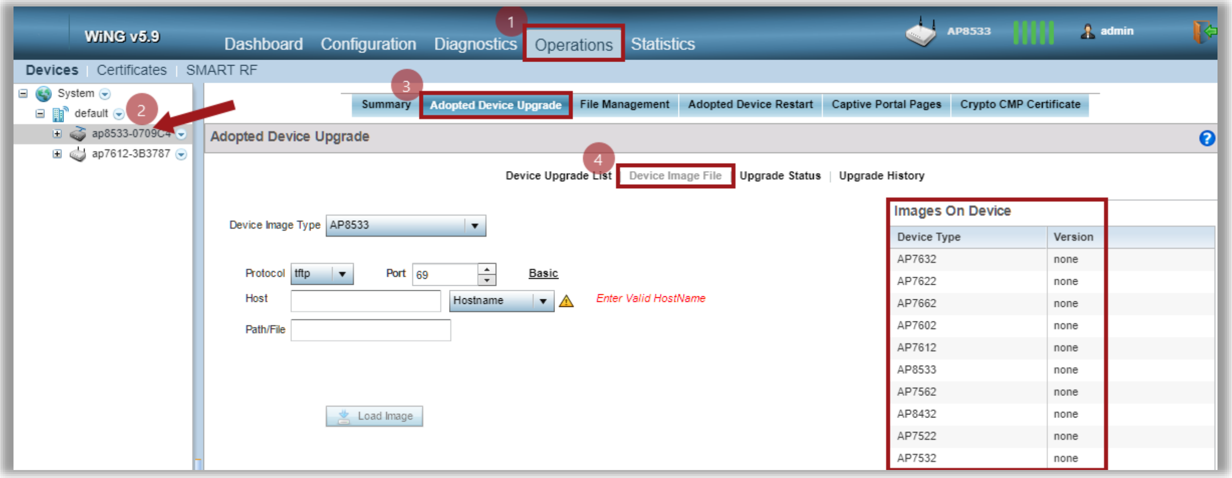
This is done via uploading desired AP image to the Virtual Controller and then initializing AP upgrade procedure.

Note that different AP families will have different Firmware files and each firmware file is stored on the VC flash memory, and eventually consumes flash storage.

For that reason, by default VC does not have any images stored locally out-of-the-box, so we have to upload them first to allow our VC to upgrade all adopted APs.

In our example we will need separate images for AP7612 and AP8533s.

As you can see in the below screen, by default none of the APs have the image pre-loaded on the VC:



Device Image Type AP8533

Protocol tftp

Port 69

Host

Hostname

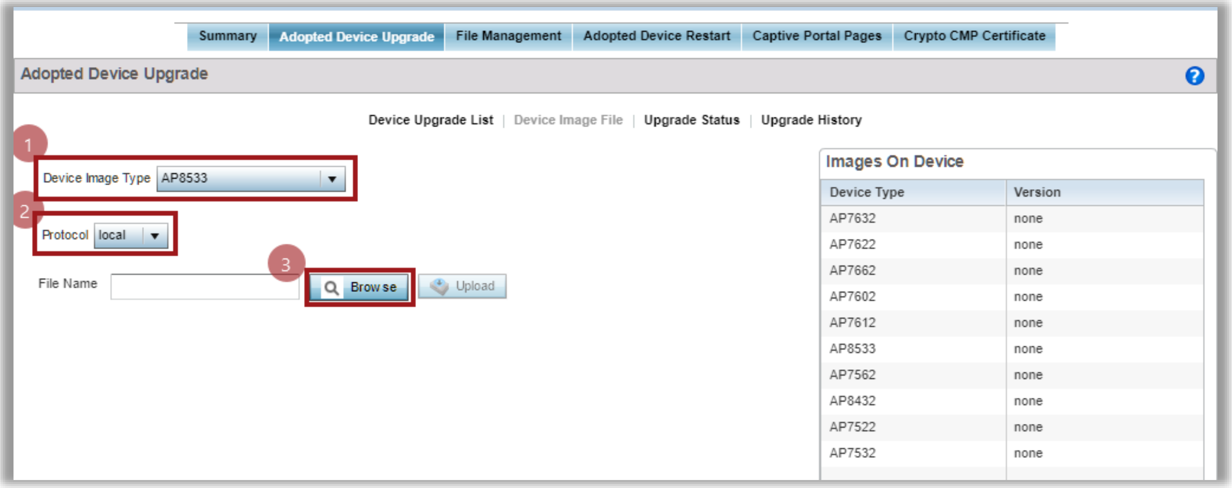
Enter Valid HostName

Path/File

Images On Device

Device Type	Version
AP7632	none
AP7622	none
AP7662	none
AP7602	none
AP7612	none
AP8533	none
AP7562	none
AP8432	none
AP7522	none
AP7532	none

Let’s upload an image for AP8533s using a file stored locally on the laptop:



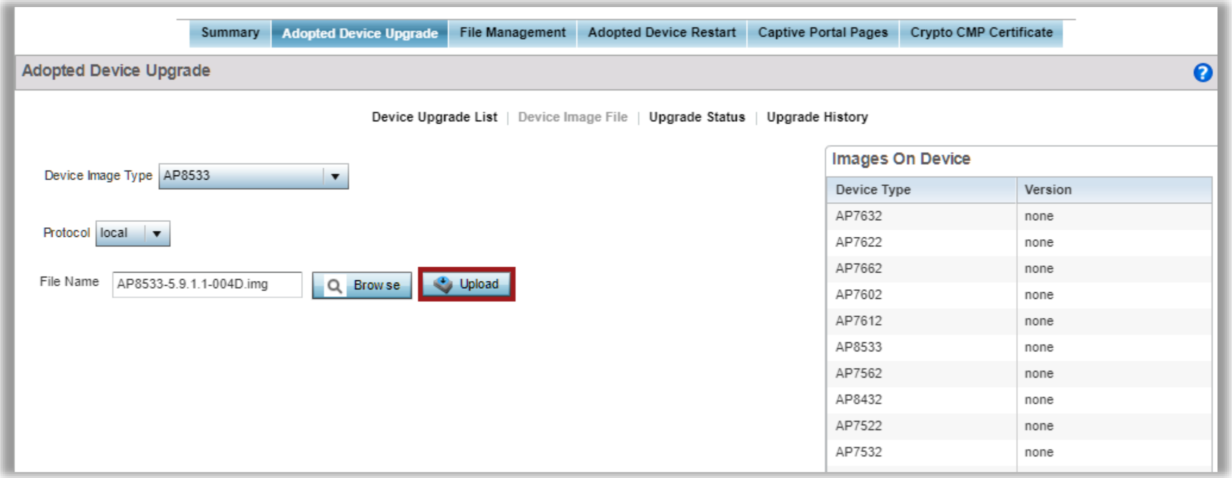
1 Device Image Type AP8533

2 Protocol local

File Name

Images On Device

Device Type	Version
AP7632	none
AP7622	none
AP7662	none
AP7602	none
AP7612	none
AP8533	none
AP7562	none
AP8432	none
AP7522	none
AP7532	none



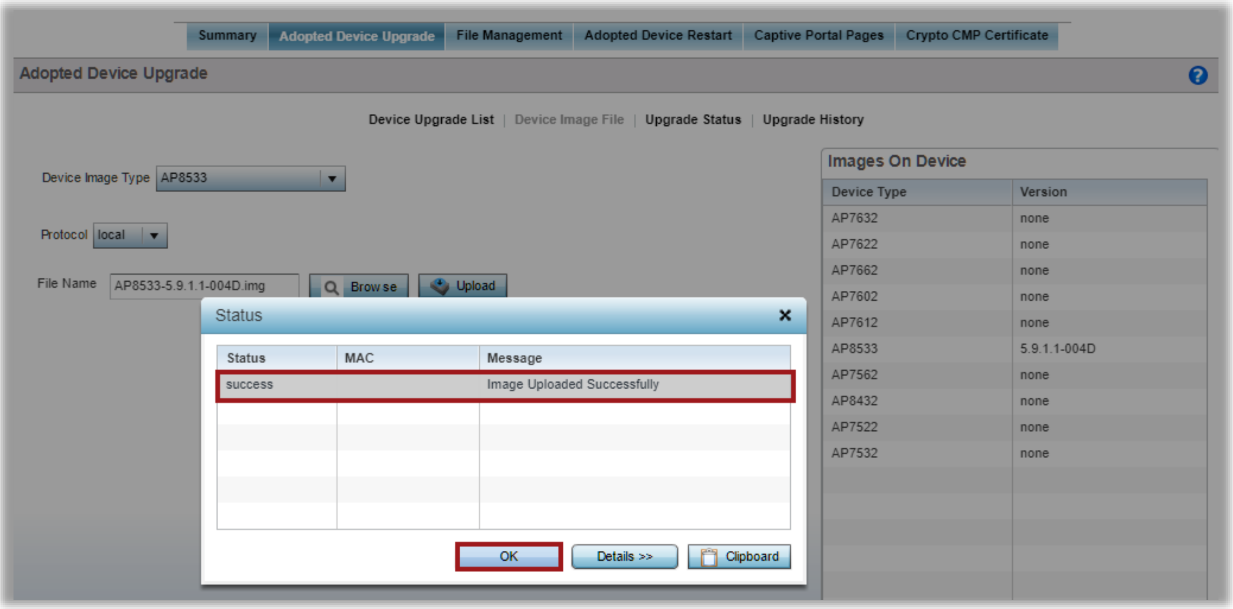
Device Image Type: AP8533

Protocol: local

File Name: AP8533-5.9.1.1-004D.img

Images On Device

Device Type	Version
AP7632	none
AP7622	none
AP7662	none
AP7602	none
AP7612	none
AP8533	none
AP7562	none
AP8432	none
AP7522	none
AP7532	none



Device Image Type: AP8533

Protocol: local

File Name: AP8533-5.9.1.1-004D.img

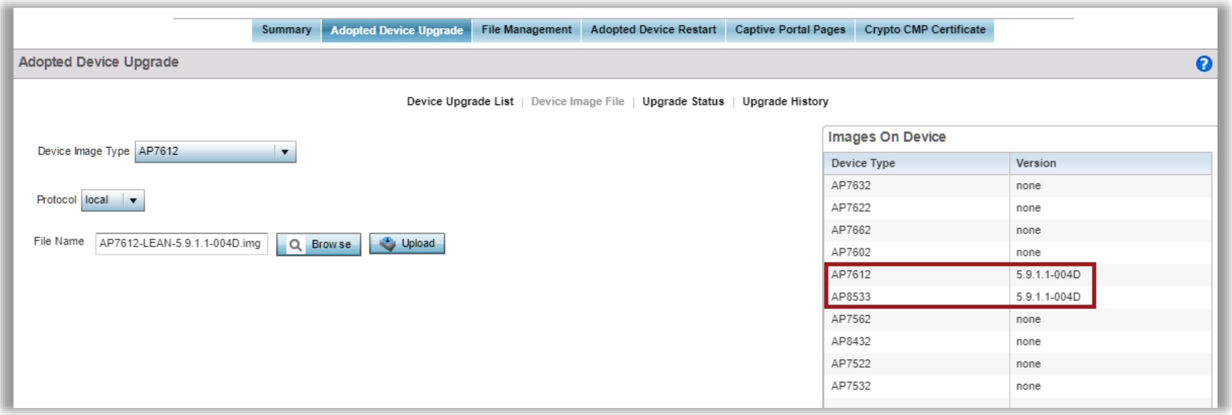
Status

Status	MAC	Message
success		Image Uploaded Successfully

Images On Device

Device Type	Version
AP7632	none
AP7622	none
AP7662	none
AP7602	none
AP7612	none
AP8533	5.9.1.1-004D
AP7562	none
AP8432	none
AP7522	none
AP7532	none

Repeat the steps to upload firmware file for AP7612. Verify that you have all images available on the Virtual Controller (each respective AP type will have current version based on the image you have uploaded):



Device Image Type: AP7612

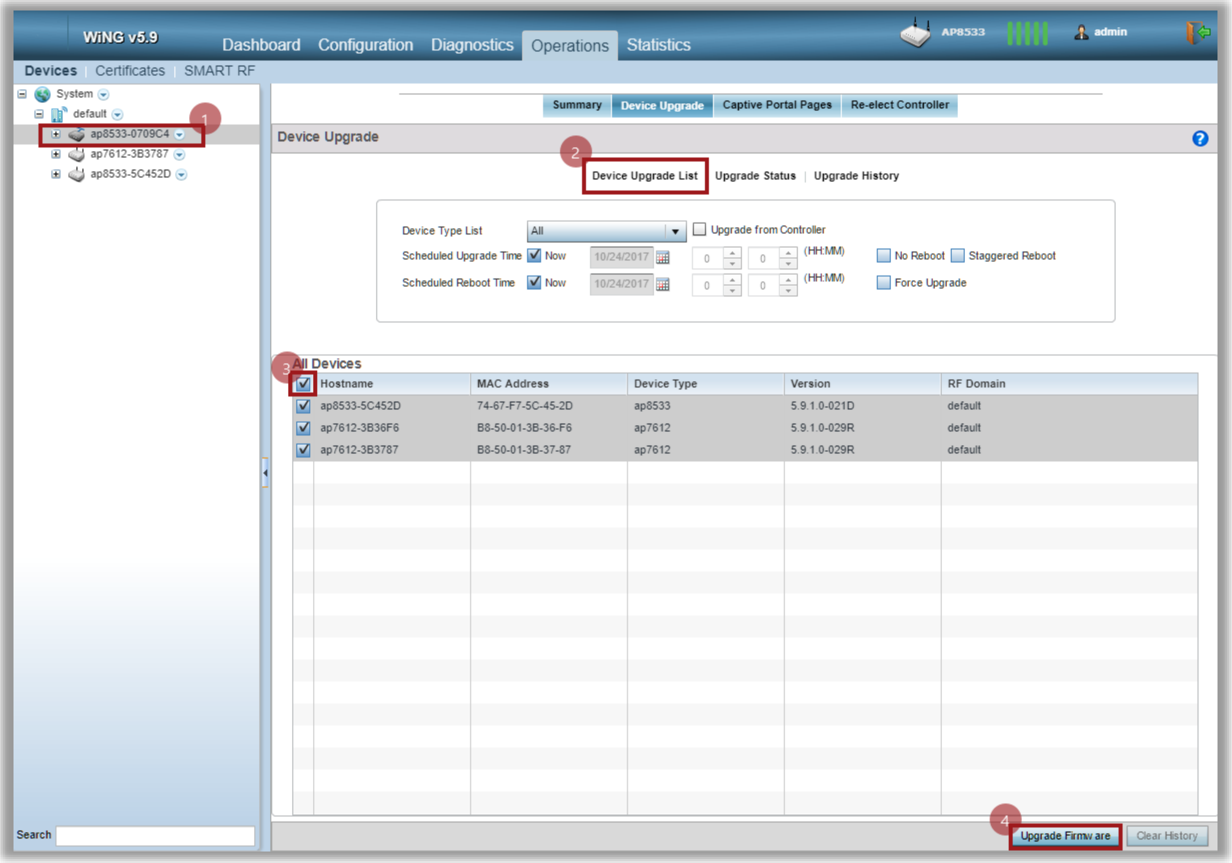
Protocol: local

File Name: AP7612-LEAN-5.9.1.1-004D.img

Images On Device

Device Type	Version
AP7632	none
AP7622	none
AP7662	none
AP7602	none
AP7612	5.9.1.1-004D
AP8533	5.9.1.1-004D
AP7562	none
AP8432	none
AP7522	none
AP7532	none

Now we can proceed with the adopted AP upgrade. Move to the Device Upgrade List tab:



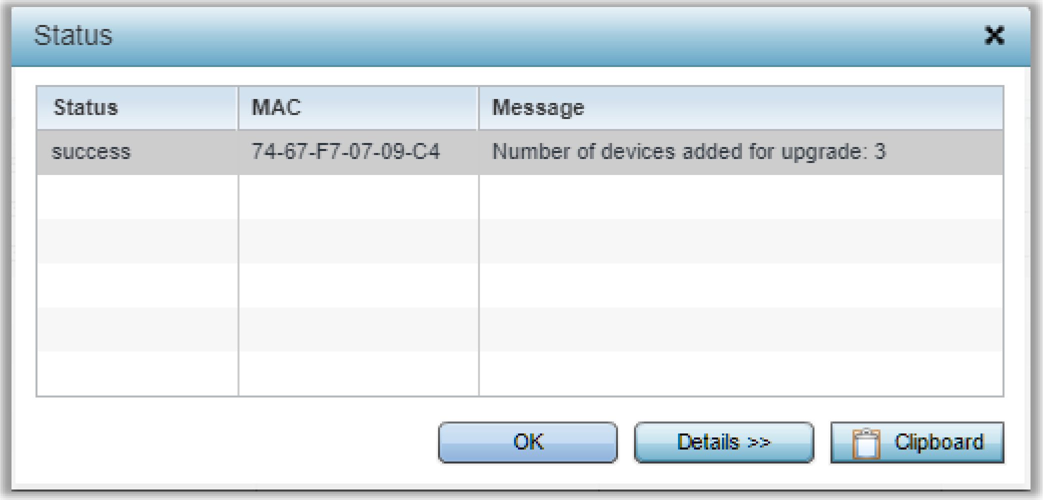
Device Type List: All ☐ Upgrade from Controller

Scheduled Upgrade Time ☑ Now 10/24/2017 0 0 (HH:MM) ☐ No Reboot ☐ Staggered Reboot

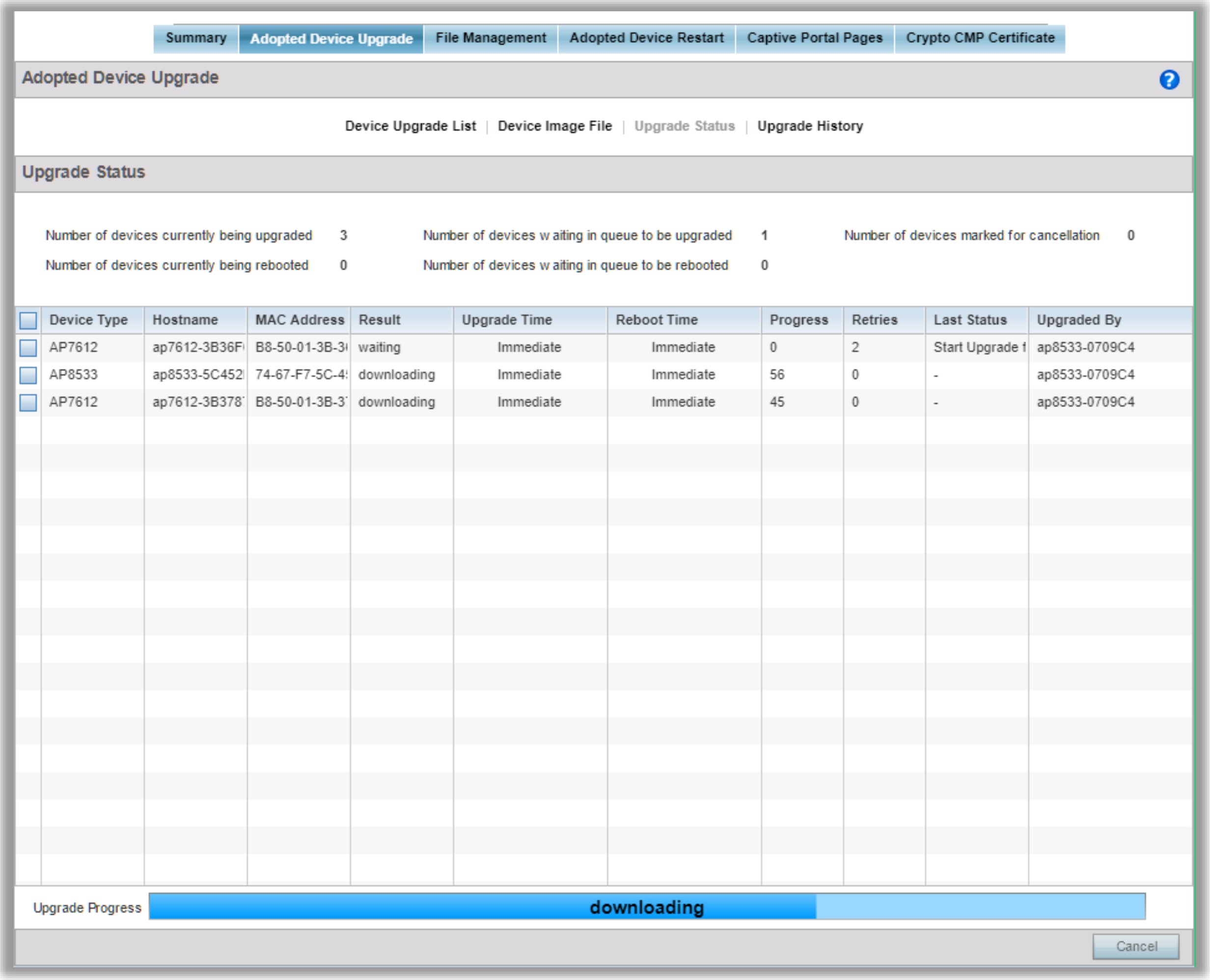
Scheduled Reboot Time ☑ Now 10/24/2017 0 0 (HH:MM) ☐ Force Upgrade

All Devices

☑	Hostname	MAC Address	Device Type	Version	RF Domain
☑	ap8533-5C452D	74-67-F7-5C-45-2D	ap8533	5.9.1.0-021D	default
☑	ap7612-3B36F6	B8-50-01-3B-36-F6	ap7612	5.9.1.0-029R	default
☑	ap7612-3B3787	B8-50-01-3B-37-87	ap7612	5.9.1.0-029R	default



Status	MAC	Message
success	74-67-F7-07-09-C4	Number of devices added for upgrade: 3



Adopted Device Upgrade

Upgrade Status

Number of devices currently being upgraded	3	Number of devices w aiting in queue to be upgraded	1	Number of devices marked for cancellation	0
Number of devices currently being rebooted	0	Number of devices w aiting in queue to be rebooted	0		

□	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
□	AP7612	ap7612-3B36F	B8-50-01-3B-3	waiting	Immediate	Immediate	0	2	Start Upgrade f	ap8533-0709C4
□	AP8533	ap8533-5C452	74-67-F7-5C-4	downloading	Immediate	Immediate	56	0	-	ap8533-0709C4
□	AP7612	ap7612-3B378	B8-50-01-3B-3	downloading	Immediate	Immediate	45	0	-	ap8533-0709C4

Upgrade Progress downloading

How to upgrade the Virtual Controller itself? After the image is uploaded from the previous step, simple click on the drop-down button next to the Virtual Controller icon and click on firmware upgrade:

Step 6 – ExtremeNSight Integration

Virtual Controller deployment can be integrated into a standalone NSight server to provide network performance analytics, custom dashboards, reporting and advanced troubleshooting tools.

This is especially useful when MSP partner or customer provides multi-tenanted VC deployments for each site, while aggregating analytics information at a single NSight server.

This guide will not cover NSight server deployment, but will cover Virtual Controller configuration required to integrate with NSight server.

Note that configuration is available in CLI only

First item to do is to rename the RF Domain from default to some unique name:

```
ap8533-0709C4#conf
Enter configuration commands, one per line.  End with CNTL/Z.
ap8533-0709C4(config)#rename rf_domain default VC-SITE-1
ap8533-0709C4(config)#commit write
```

Next step would be to configure location tree on the RF Domain to set Country/Region/City/Campus parameters so that they are logically grouped on the NSight server. In addition add geo-coordinates of the site to make Google Map work on NSight:

```
ap8533-0709C4(config)#rf-domain VC-SITE-1
ap8533-0709C4(config-rf-domain-VC-SITE-1)#tree-node country Czechia city Brno campus EXTR
ap8533-0709C4(config-rf-domain-VC-SITE-1)#geo-coordinates 49.180267 16.6035502
ap8533-0709C4(config-rf-domain-VC-SITE-1)#exit
ap8533-0709C4(config)#commit write
```

Now create NSight policy and point it to NSight server(s) IP address / FQDN:

```
ap8533-0709C4(config)#nsight-policy NSIGHT-CLIENT
ap8533-0709C4(config-nsight-policy-NSIGHT-CLIENT)#server host 192.168.7.83 https
ap8533-0709C4(config-nsight-policy-NSIGHT-CLIENT)#exit
ap8533-0709C4(config)#commit write
```

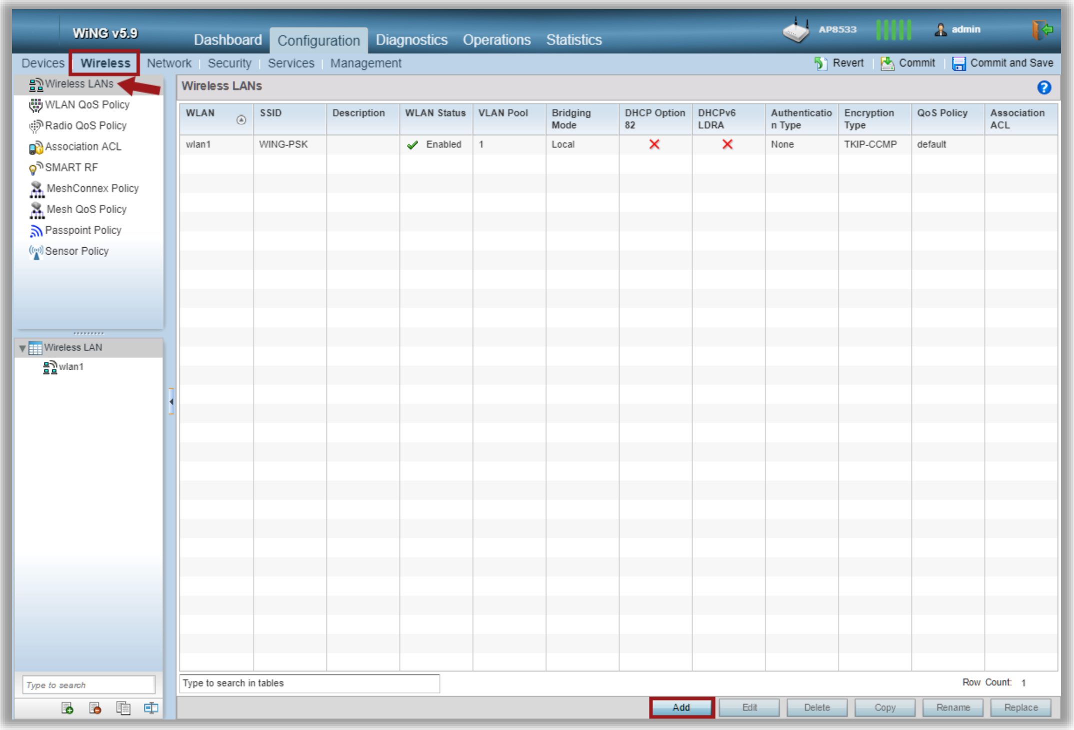
Lastly, assign NSight policy to the RF Domain. Additionally enable nsight sensor to allow NSight advanced troubleshooting tools like AP Test and Spectrum Analysis to work:

```
ap8533-0709C4(config)#rf-domain VC-SITE-1
ap8533-0709C4(config-rf-domain-VC-SITE-1)#use nsight-policy NSIGHT-CLIENT
ap8533-0709C4(config-rf-domain-VC-SITE-1)#nsight-sensor
ap8533-0709C4(config-rf-domain-VC-SITE-1)#commit write
```

Step 7 – 802.1X SSID with External RADIUS

The following section will show an example how to create an SSID with 802.1X authentication using external RADIUS Server. Clients will authenticate using PEAP-MSCHAPv2 via Microsoft NPS server:

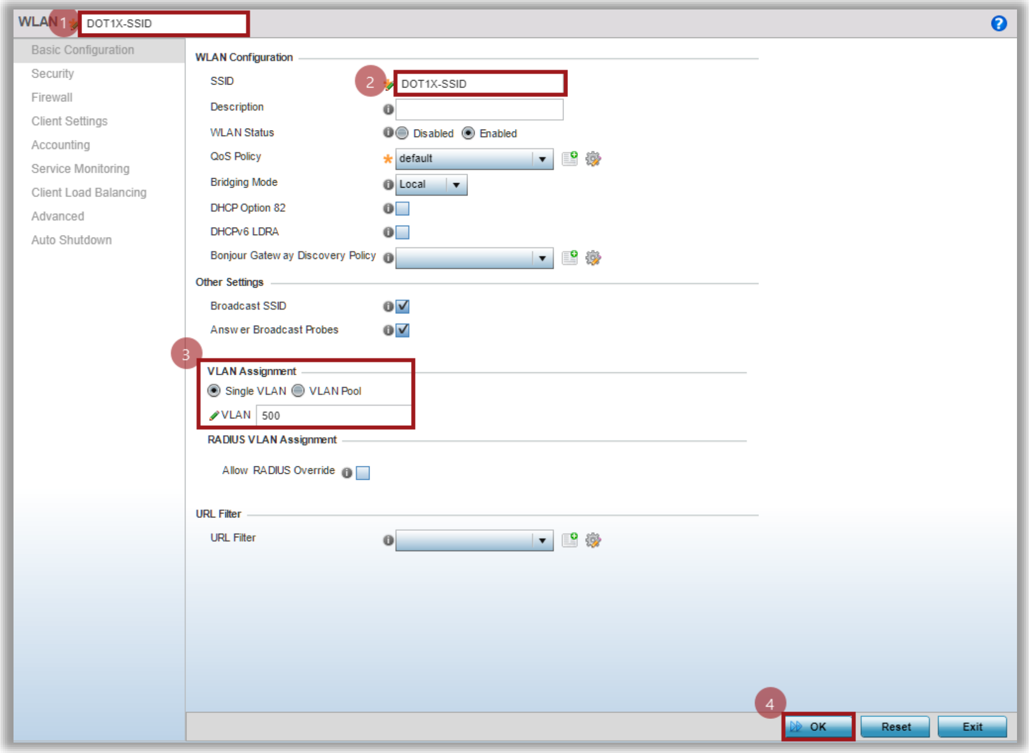
Navigate to Wireless > Wireless LANs and create a new WLAN:



Wireless LANs

WLAN	SSID	Description	WLAN Status	VLAN Pool	Bridging Mode	DHCP Option 82	DHCPv6 LDRA	Authentication Type	Encryption Type	QoS Policy	Association ACL
wlan1	WING-PSK		✓ Enabled	1	Local	✗	✗	None	TKIP-CCMP	default	

In this example we will name our SSID as "DOT1X-SSID" and we will place all the clients into a separate VLA N 500 that will be locally bridge by each AP.



WLAN DOT1X-SSID

WLAN Configuration

- SSID: DOT1X-SSID
- Description:
- WLAN Status: ○ Disabled ● Enabled
- QoS Policy: default
- Bridging Mode: Local
- DHCP Option 82: □
- DHCPv6 LDRA: □
- Bonjour Gatew ay Discovery Policy:

Other Settings

- Broadcast SSID: ☑
- Answ er Broadcast Probes: ☑

VLAN Assignment

- ● Single VLAN ○ VLAN Pool
- VLAN: 500

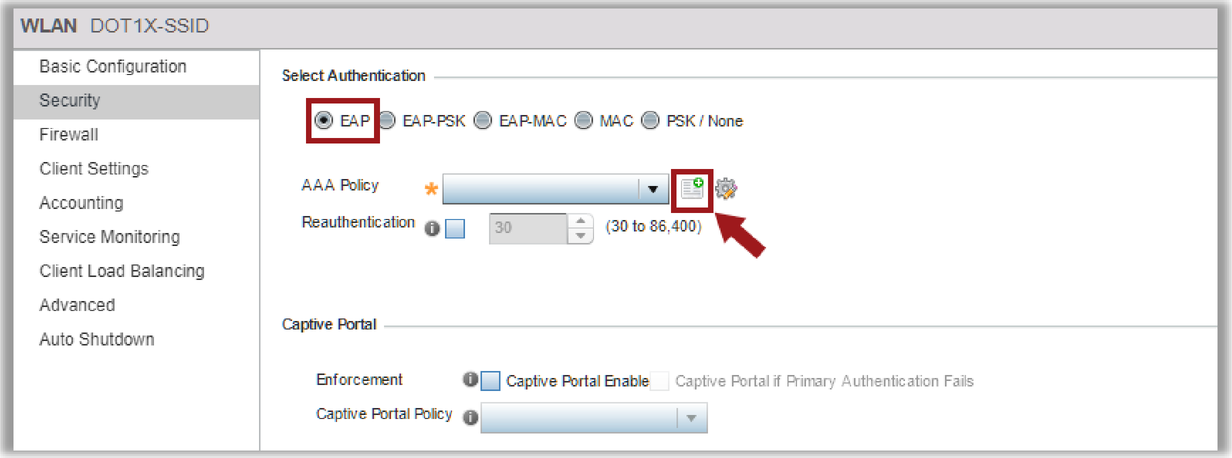
RADIUS VLAN Assignment

- Allow RADIUS Override: □

URL Filter

- URL Filter:

Move to the Security Tab. Enable EAP authentication and create a new AAA Policy that will point to one or more external RADIUS servers:



WLAN DOT1X-SSID

Select Authentication

● EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ○ PSK / None

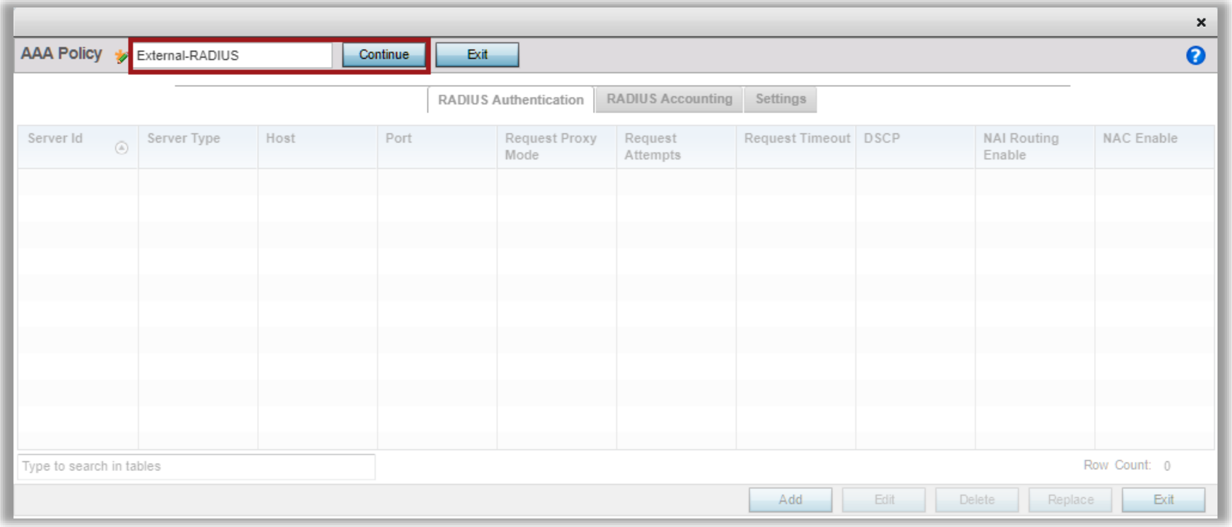
AAA Policy *

Reauthentication □ 30 (30 to 86,400)

Captive Portal

Enforcement □ Captive Portal Enable □ Captive Portal if Primary Authentication Fails

Captive Portal Policy

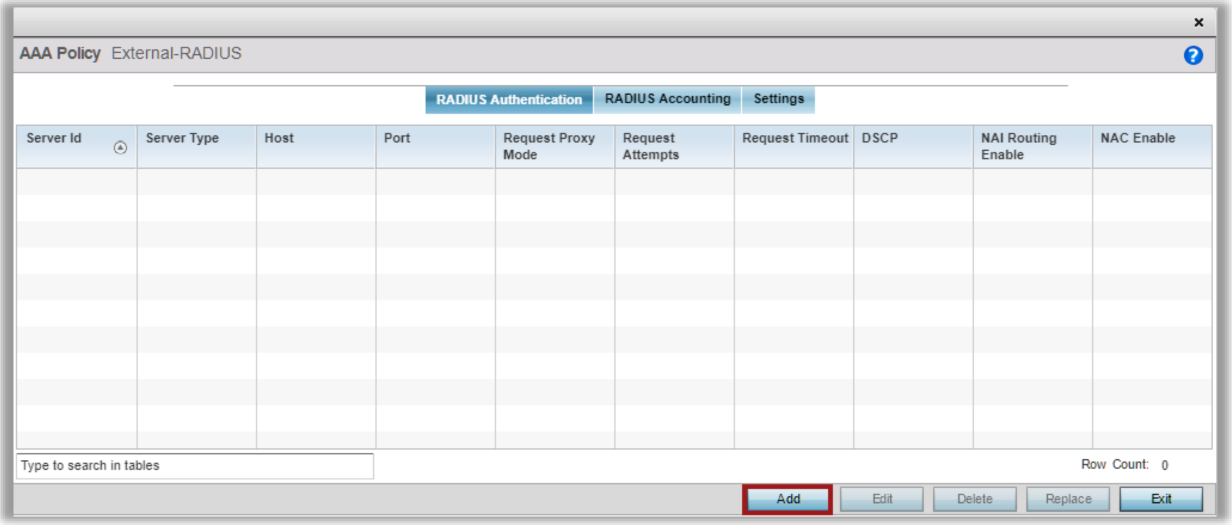


AAA Policy External-RADIUS

Server Id	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable

Type to search in tables

Row Count: 0



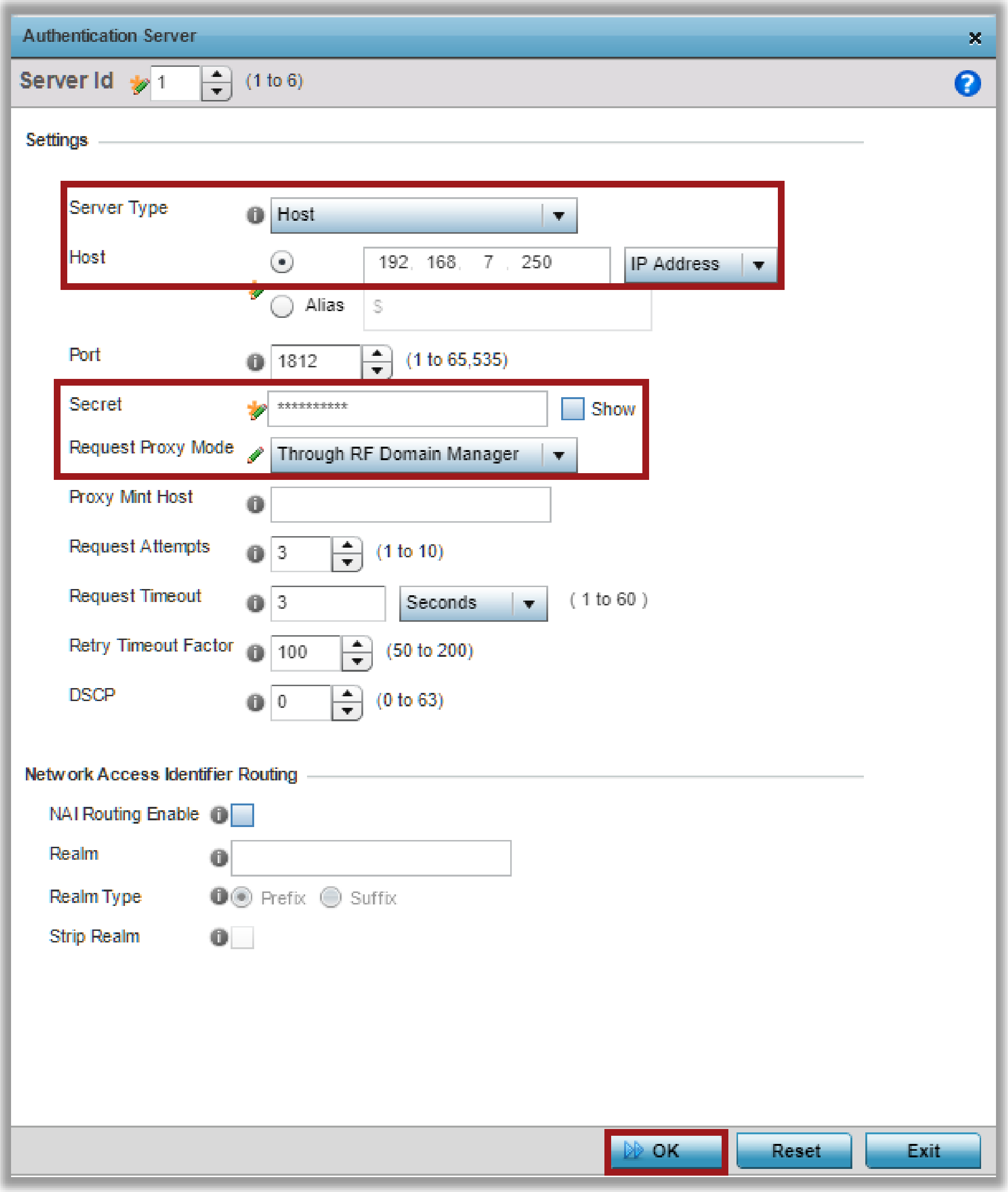
AAA Policy External-RADIUS

Server Id	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable

Type to search in tables

Row Count: 0

Specify RADIUS Server entry, provide IP address or FQDN of the external RADIUS server, RADIUS Secret and optionally select the proxy mode via RF Domain Manager (in this case RF Domain Manager is the same AP as Virtual Controller):



Server Id 1 (1 to 6)

Settings

Server Type: Host

Host: ● 192.168.7.250 IP Address

○ Alias $

Port: 1812 (1 to 65,535)

Secret: ********** □ Show

Request Proxy Mode: Through RF Domain Manager

Proxy Mint Host:

Request Attempts: 3 (1 to 10)

Request Timeout: 3 Seconds (1 to 60)

Retry Timeout Factor: 100 (50 to 200)

DSCP: 0 (0 to 63)

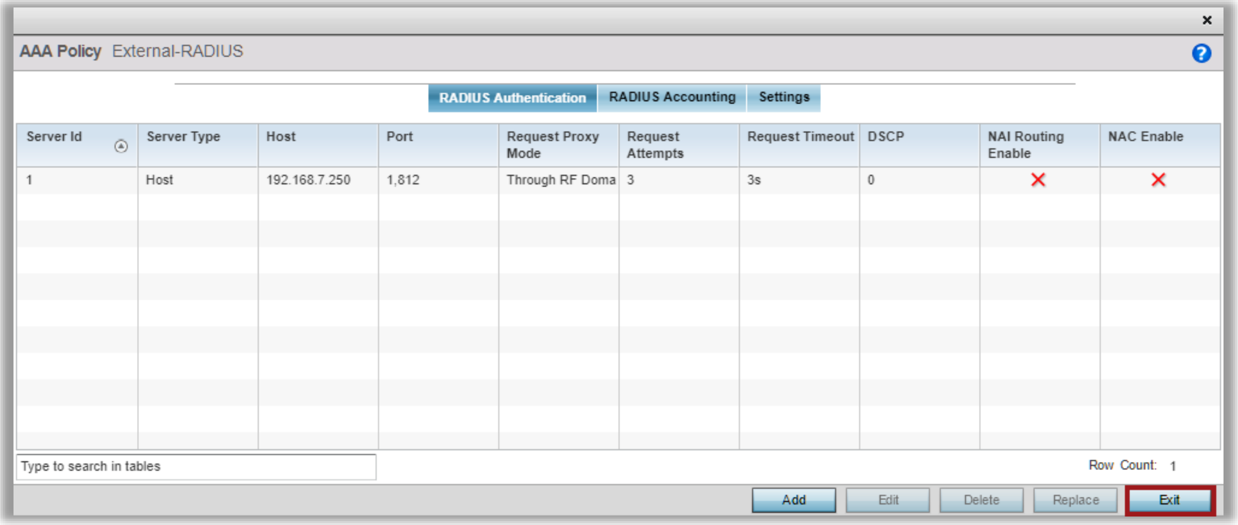
Network Access Identifier Routing

NAI Routing Enable □

Realm:

Realm Type: ● Prefix ○ Suffix

Strip Realm □



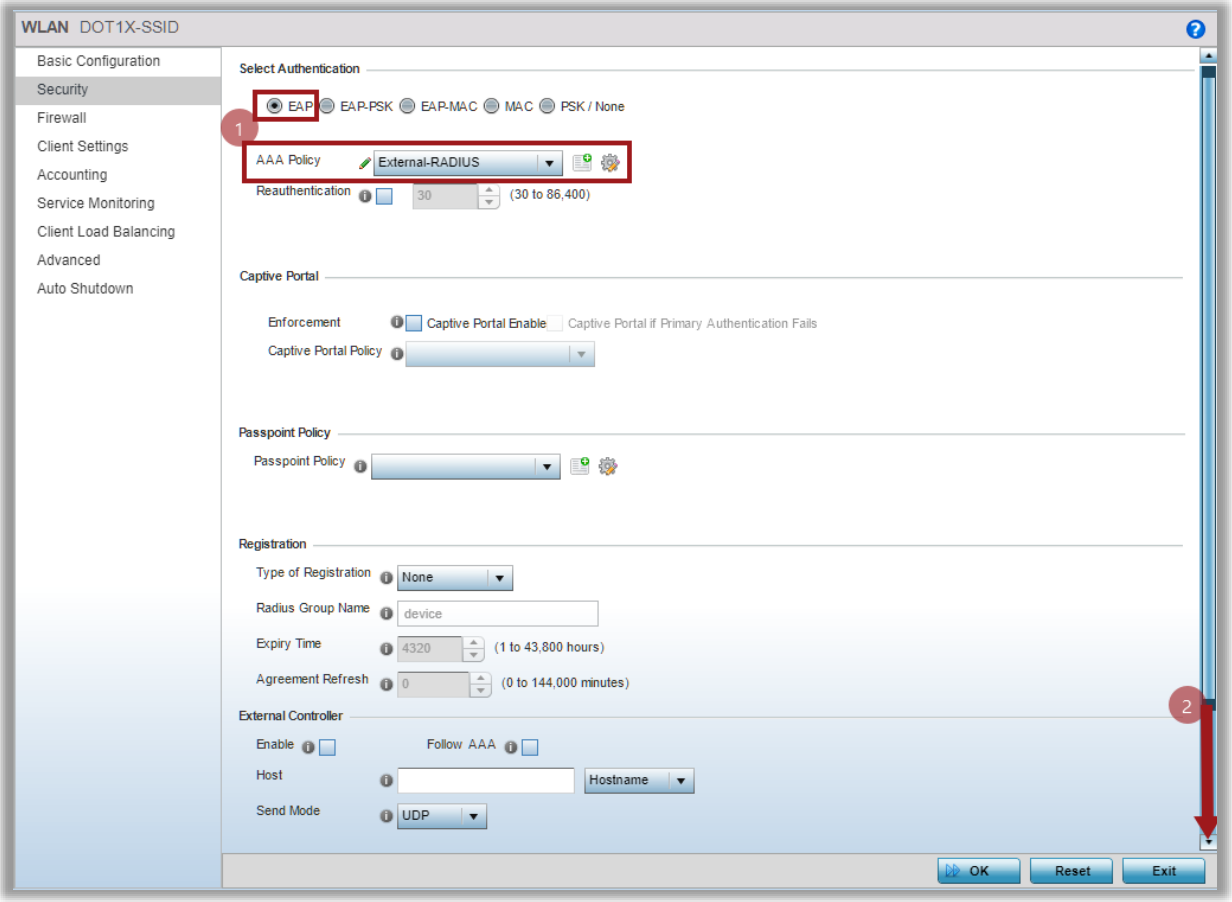
AAA Policy External-RADIUS

Server Id	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
1	Host	192.168.7.250	1,812	Through RF Doma	3	3s	0	✗	✗

Type to search in tables

Row Count: 1

Attach this new AAA Policy now and then scroll down within the same screen:



WLAN DOT1X-SSID

Select Authentication

● EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ○ PSK / None

AAA Policy: External-RADIUS

Reauthentication □ 30 (30 to 86,400)

Captive Portal

Enforcement □ Captive Portal Enable □ Captive Portal if Primary Authentication Fails

Captive Portal Policy

Passpoint Policy

Passpoint Policy

Registration

Type of Registration: None

Radius Group Name: device

Expiry Time: 4320 (1 to 43,800 hours)

Agreement Refresh: 0 (0 to 144,000 minutes)

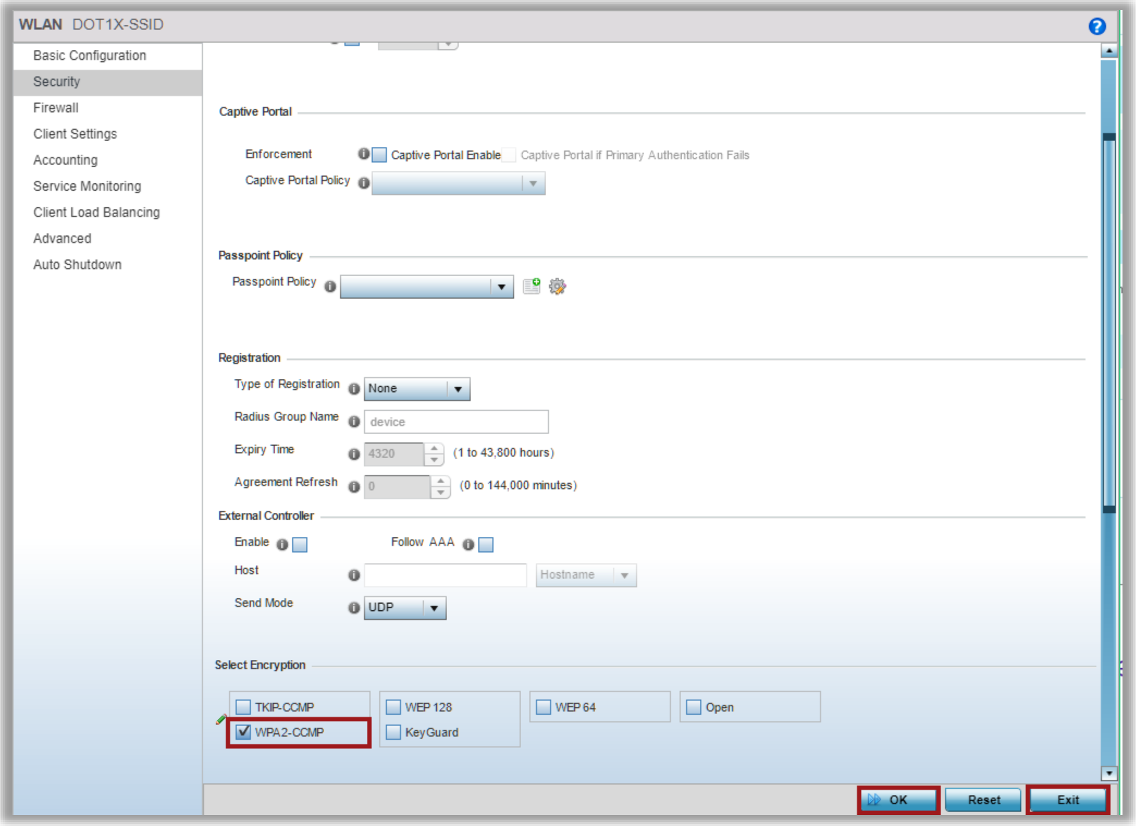
External Controller

Enable □ Follow AAA □

Host: Hostname

Send Mode: UDP

Set encryption ciphers to CCMP, click OK and then Commit&Save changes:



Captive Portal

Enforcement □ Captive Portal Enable □ Captive Portal if Primary Authentication Fails

Captive Portal Policy

Passpoint Policy

Passpoint Policy

Registration

Type of Registration: None

Radius Group Name: device

Expiry Time: 4320 (1 to 43,800 hours)

Agreement Refresh: 0 (0 to 144,000 minutes)

External Controller

Enable □ Follow AAA □

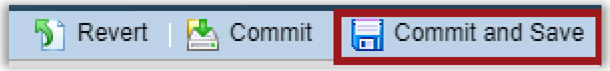
Host: Hostname

Send Mode: UDP

Select Encryption

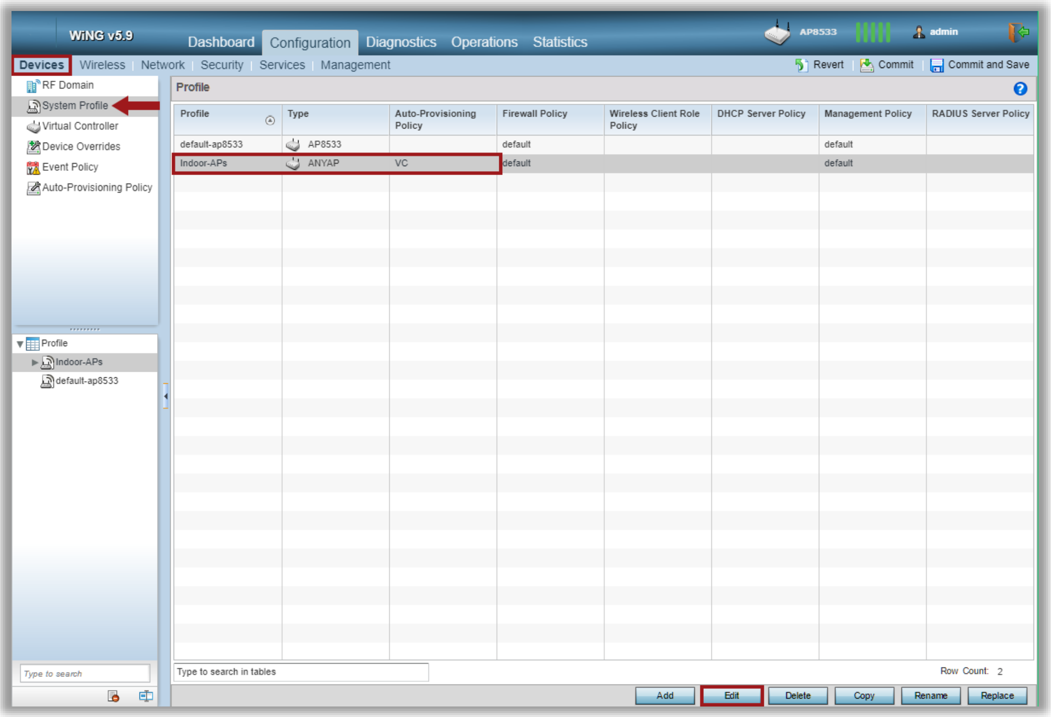
□ TKIP-CCMP □ WEP 128 □ WEP 64 □ Open

☑ WPA2-CCMP □ KeyGuard



Now go to the AP profile. We will need to assign this Wireless LAN to AP radio interfaces to allow advertizing of this SSID and lastly we will need to allow VLAN 500 on the GE interface of the AP.

Go to Devices > System Profile > Indoor-APs > Edit:



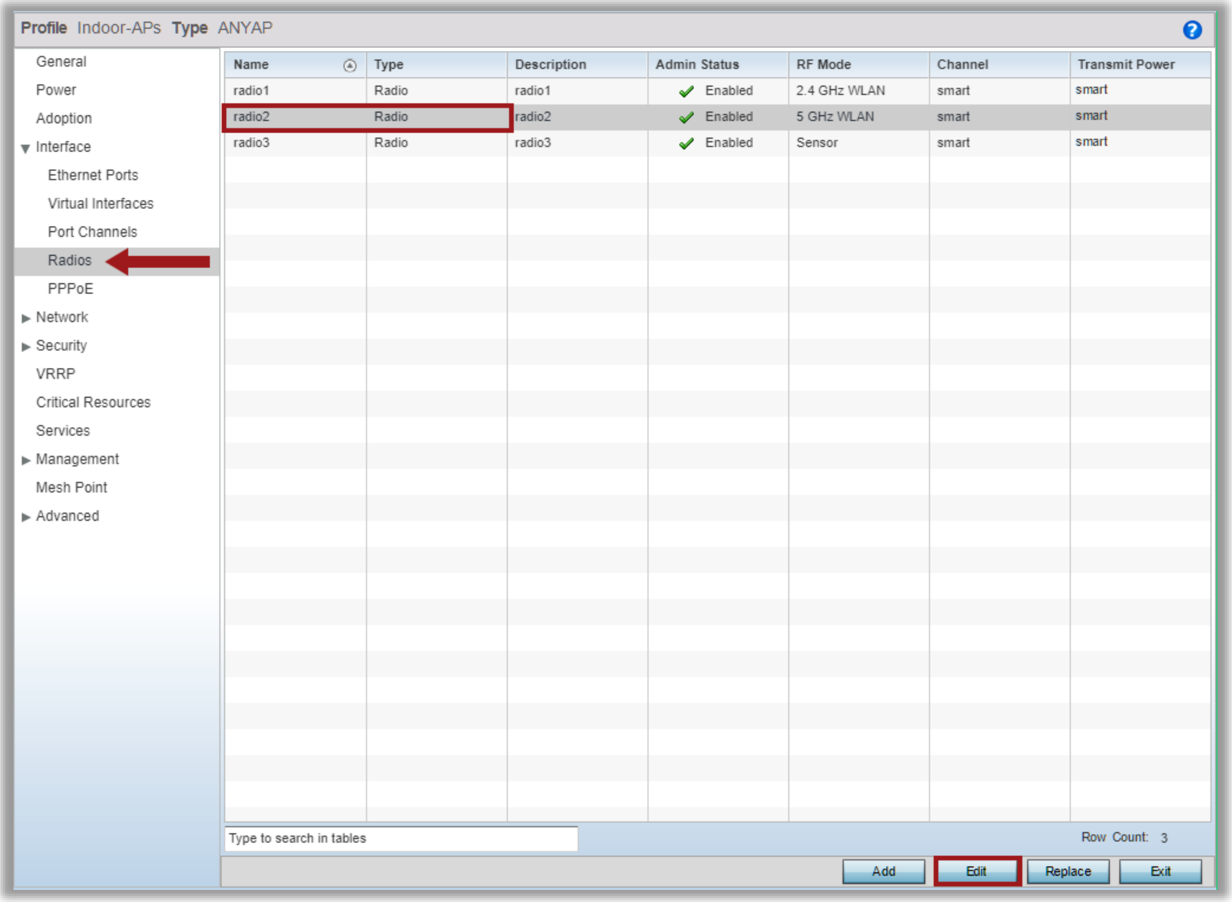
Profile

Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
default-ap8533	AP8533		default			default	
Indoor-APs	ANYAP	VC	default			default	

Type to search in tables

Row Count: 2

Under AP Profile go to **Interface > Radios** and edit radio2 interface (5GHz). In this example we will only advertize 802.1X SSID on the 5GHz band:

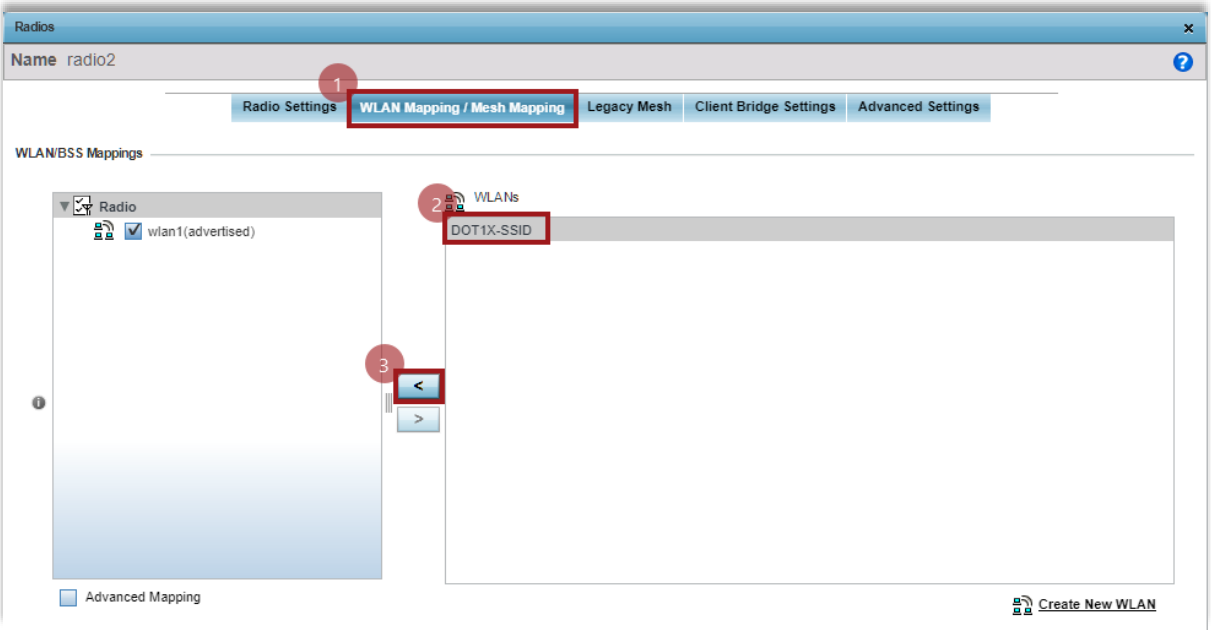


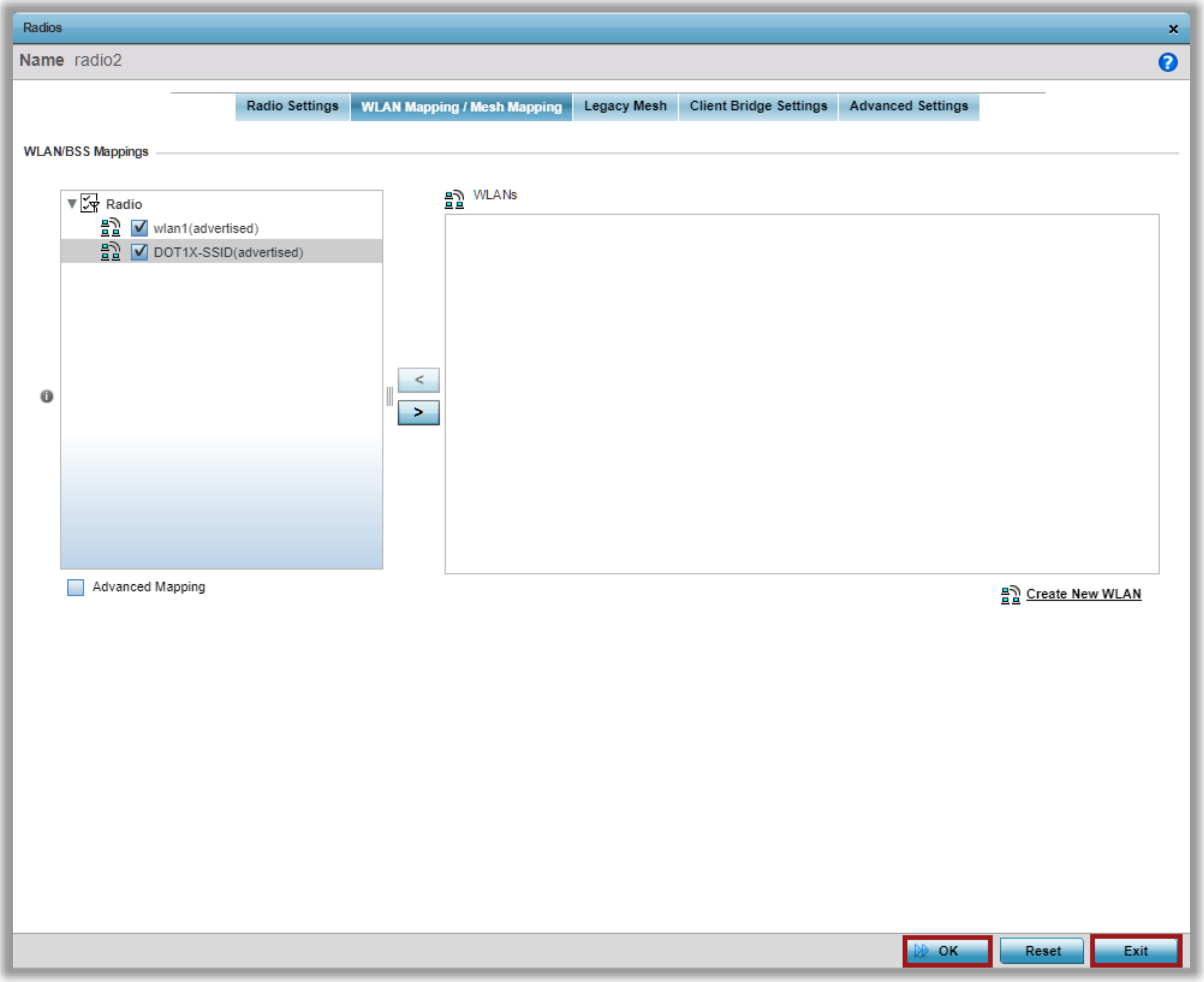
Profile Indoor-APs **Type** ANYAP

Name	Type	Description	Admin Status	RF Mode	Channel	Transmit Power
radio1	Radio	radio1	✓ Enabled	2.4 GHz WLAN	smart	smart
radio2	Radio	radio2	✓ Enabled	5 GHz WLAN	smart	smart
radio3	Radio	radio3	✓ Enabled	Sensor	smart	smart

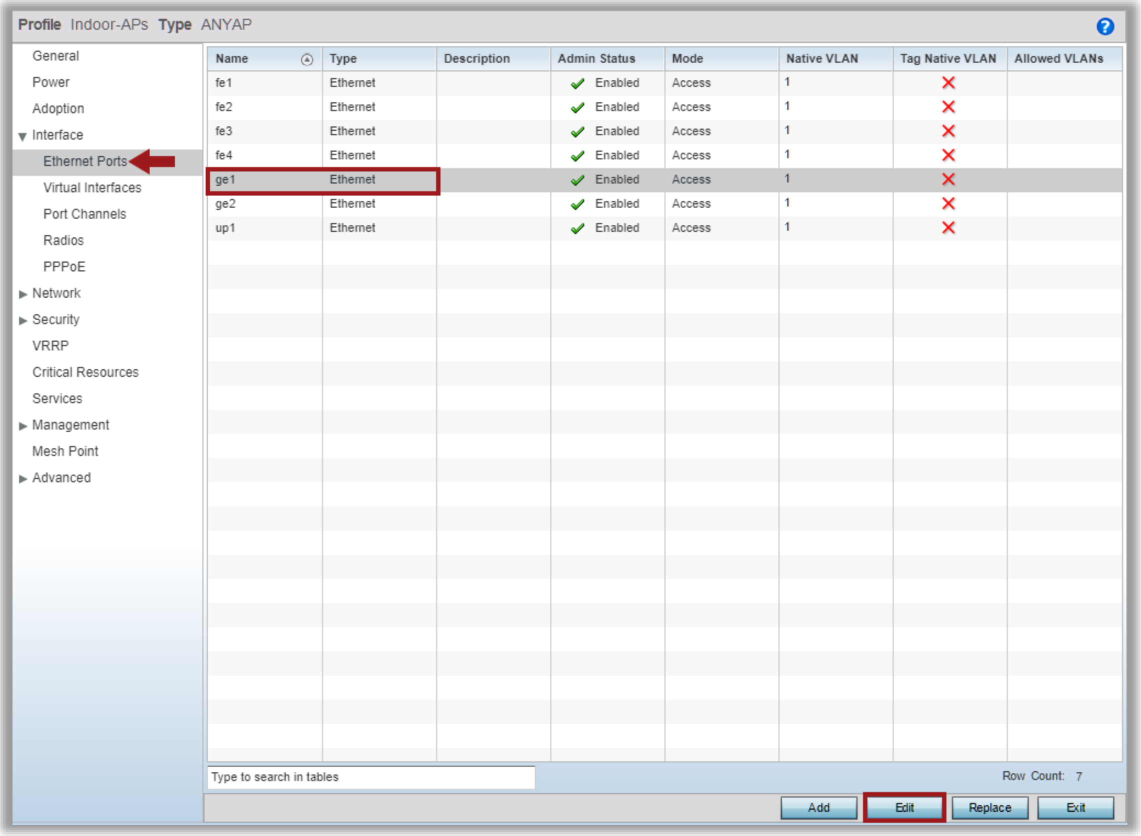
Type to search in tables

Row Count: 3





Move to **Ethernet Ports** tab and edit ge1 interface settings:



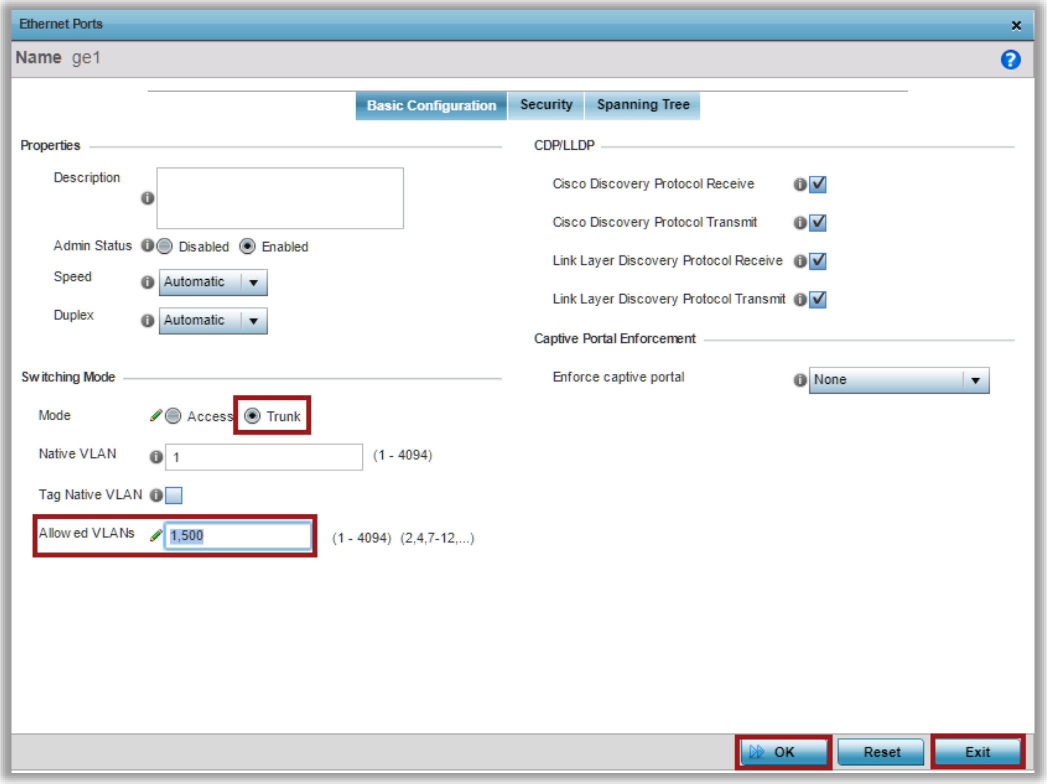
Profile Indoor-APs **Type** ANYAP

Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
fe1	Ethernet		✓ Enabled	Access	1	✗	
fe2	Ethernet		✓ Enabled	Access	1	✗	
fe3	Ethernet		✓ Enabled	Access	1	✗	
fe4	Ethernet		✓ Enabled	Access	1	✗	
ge1	Ethernet		✓ Enabled	Access	1	✗	
ge2	Ethernet		✓ Enabled	Access	1	✗	
up1	Ethernet		✓ Enabled	Access	1	✗	

Type to search in tables

Row Count: 7

Switch port mode from access to trunk and add VLAN 500 to the allowed VLAN list:



Ethernet Ports

Name ge1

Properties

Description

Admin Status ○ Disabled ● Enabled

Speed Automatic

Duplex Automatic

Switching Mode

Mode ○ Access ● Trunk

Native VLAN 1 (1 - 4094)

Tag Native VLAN □

Allowed VLANs 1,500 (1 - 4094) (2,4,7-12,...)

CDP/LLDP

Cisco Discovery Protocol Receive ☑

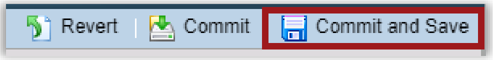
Cisco Discovery Protocol Transmit ☑

Link Layer Discovery Protocol Receive ☑

Link Layer Discovery Protocol Transmit ☑

Captive Portal Enforcement

Enforce captive portal None



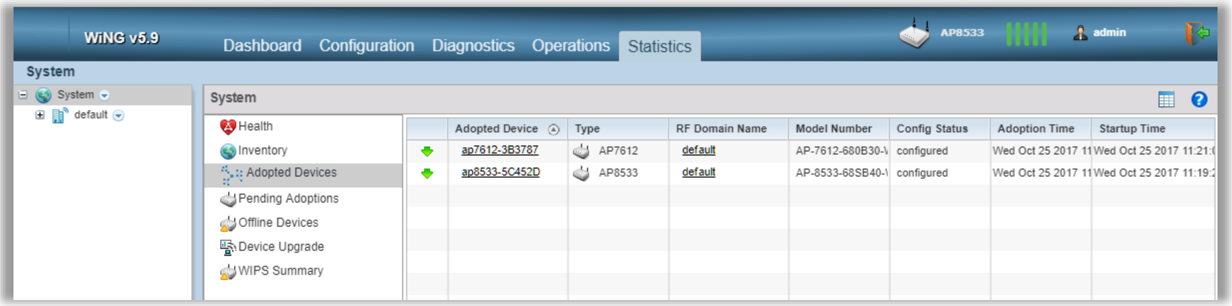
VirtualController – Verification & Monitoring

This section will go through some of the basic monitoring capabilities of the Virtual Controller Web UI interface for day to day operations.

Statistics in WiNG can be at the Site (RF Domain) level or a AP level:

AP Adoption Verification.

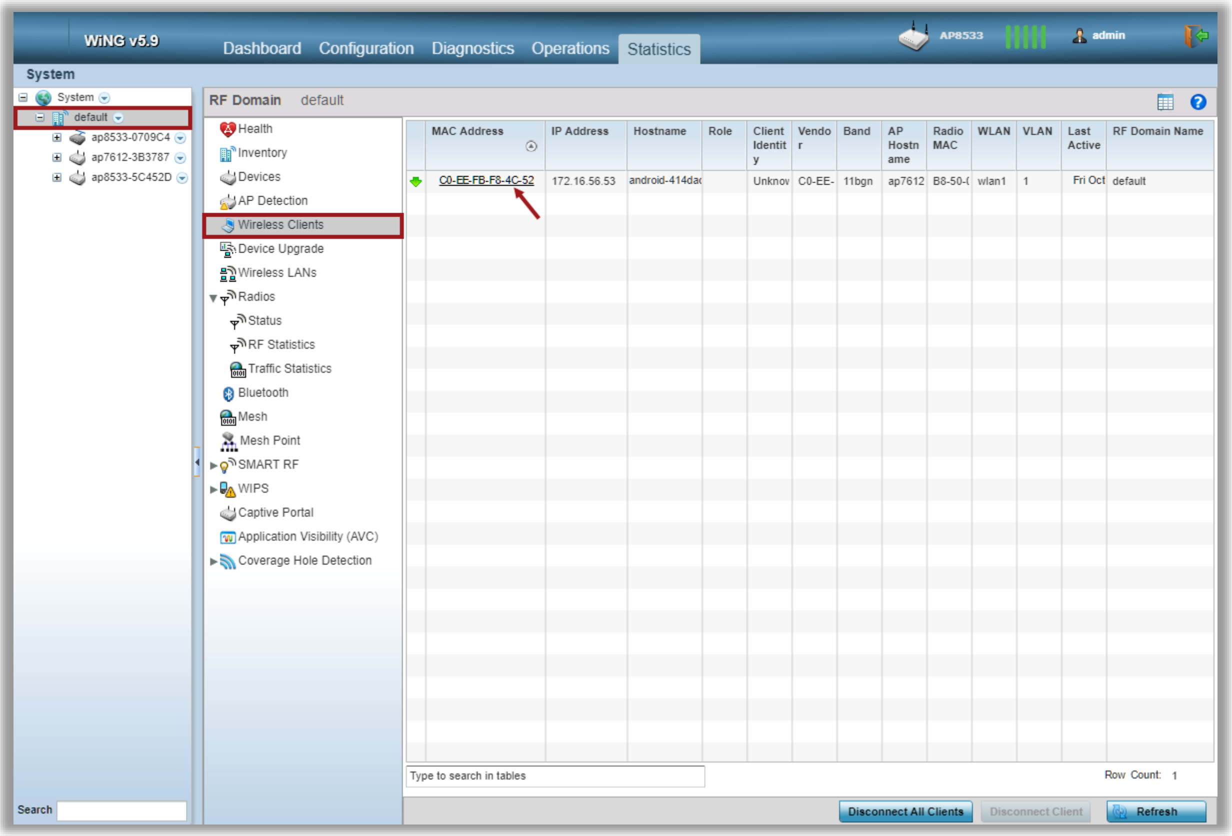
Statistics > Adopted Devices



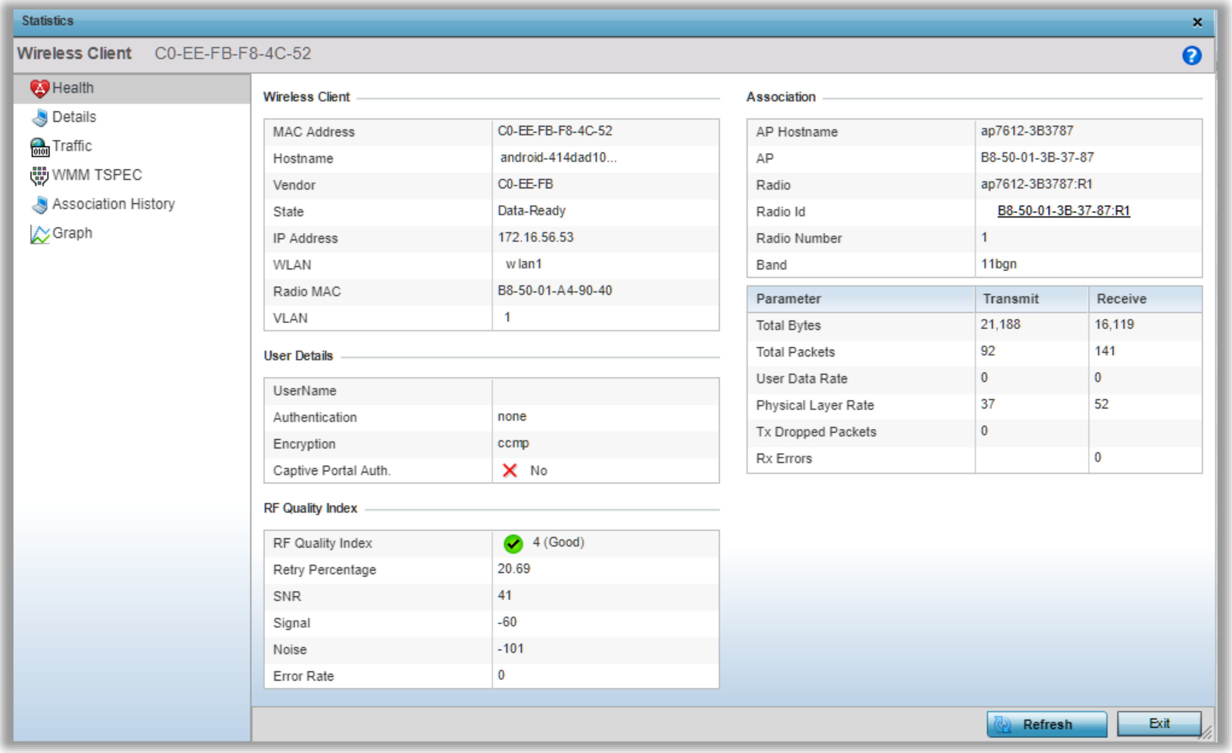
	Adopted Device	Type	RF Domain Name	Model Number	Config Status	Adoption Time	Startup Time
	ap7612-3B3787	AP7612	default	AP-7612-680B30-\	configured	Wed Oct 25 2017 11	Wed Oct 25 2017 11:21:(
	ap8533-5C452D	AP8533	default	AP-8533-68SB40-\	configured	Wed Oct 25 2017 11	Wed Oct 25 2017 11:19:2

Client Connections:

Statistics > {RF Domain Name} > Wireless Clients:



	MAC Address	IP Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active	RF Domain Name
	C0-EE-FB-F8-4C-52	172.16.56.53	android-414dac		Unknov	C0-EE-	11bgn	ap7612	B8-50-(	wlan1	1	Fri Oct	default



Wireless Client

MAC Address	C0-EE-FB-F8-4C-52
Hostname	android-414dad10...
Vendor	C0-EE-FB
State	Data-Ready
IP Address	172.16.56.53
WLAN	wlan1
Radio MAC	B8-50-01-A4-90-40
VLAN	1

User Details

UserName	
Authentication	none
Encryption	ccmp
Captive Portal Auth.	✗ No

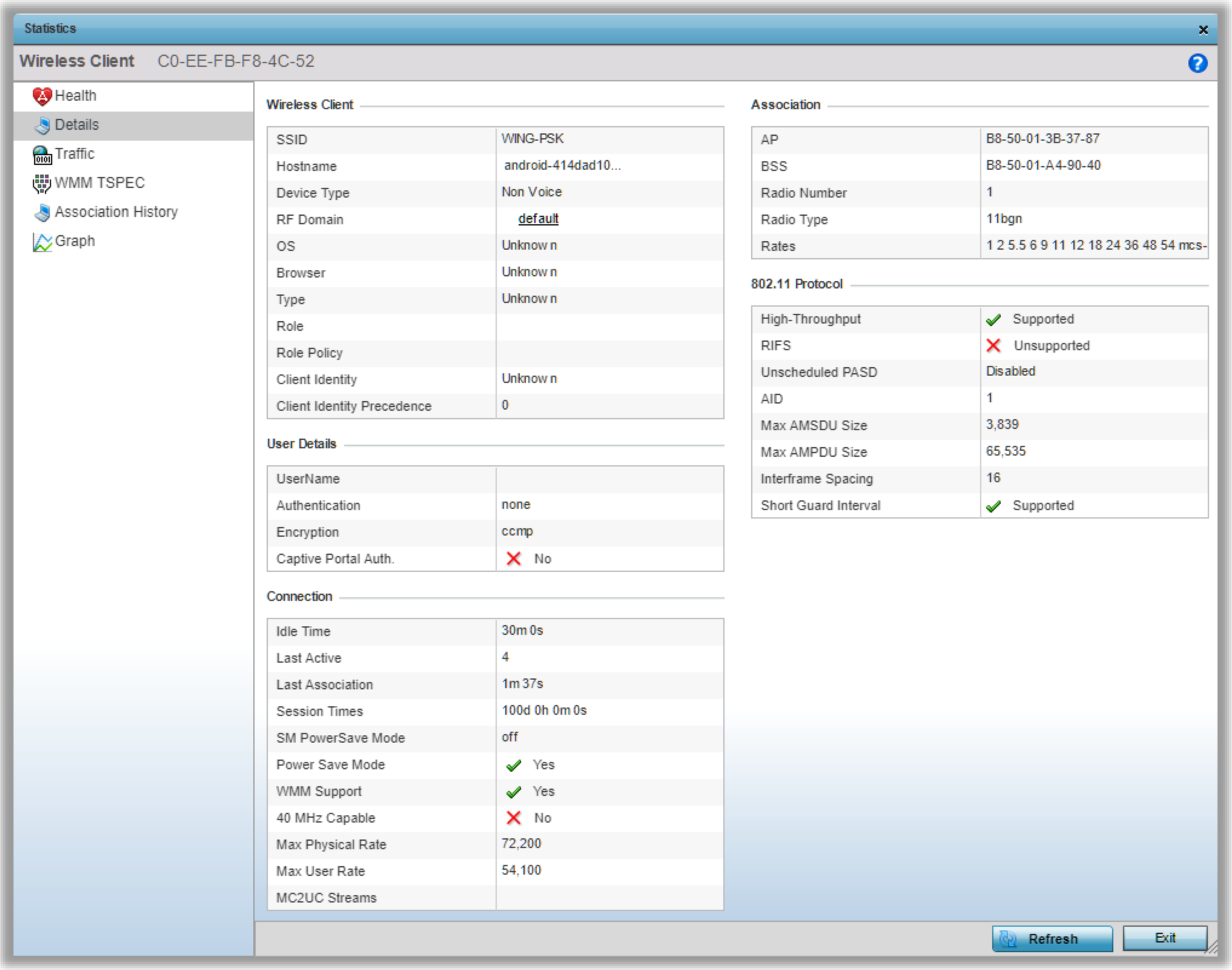
RF Quality Index

RF Quality Index	✓ 4 (Good)
Retry Percentage	20.69
SNR	41
Signal	-60
Noise	-101
Error Rate	0

Association

AP Hostname	ap7612-3B3787
AP	B8-50-01-3B-37-87
Radio	ap7612-3B3787:R1
Radio Id	B8-50-01-3B-37-87:R1
Radio Number	1
Band	11bgn

Parameter	Transmit	Receive
Total Bytes	21,188	16,119
Total Packets	92	141
User Data Rate	0	0
Physical Layer Rate	37	52
Tx Dropped Packets	0	
Rx Errors		0



Wireless Client

SSID	WING-PSK
Hostname	android-414dad10...
Device Type	Non Voice
RF Domain	default
OS	Unknown
Browser	Unknown
Type	Unknown
Role	
Role Policy	
Client Identity	Unknown
Client Identity Precedence	0

User Details

UserName	
Authentication	none
Encryption	ccmp
Captive Portal Auth.	✗ No

Connection

Idle Time	30m 0s
Last Active	4
Last Association	1m 37s
Session Times	100d 0h 0m 0s
SM PowerSave Mode	off
Power Save Mode	✓ Yes
WMM Support	✓ Yes
40 MHz Capable	✗ No
Max Physical Rate	72,200
Max User Rate	54,100
MC2UC Streams	

Association

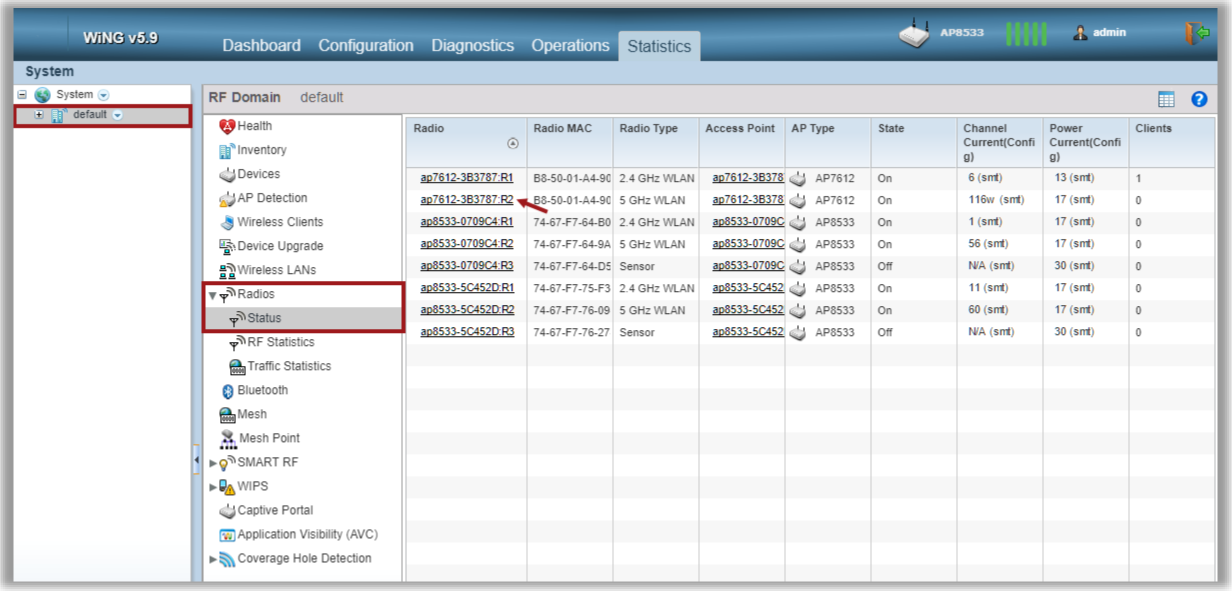
AP	B8-50-01-3B-37-87
BSS	B8-50-01-A4-90-40
Radio Number	1
Radio Type	11bgn
Rates	1 2 5.5 6 9 11 12 18 24 36 48 54 mcs-

802.11 Protocol

High-Throughput	✓ Supported
RIFS	✗ Unsupported
Unscheduled PASD	Disabled
AID	1
Max AMSDU Size	3,839
Max AMPDU Size	65,535
Interframe Spacing	16
Short Guard Interval	✓ Supported

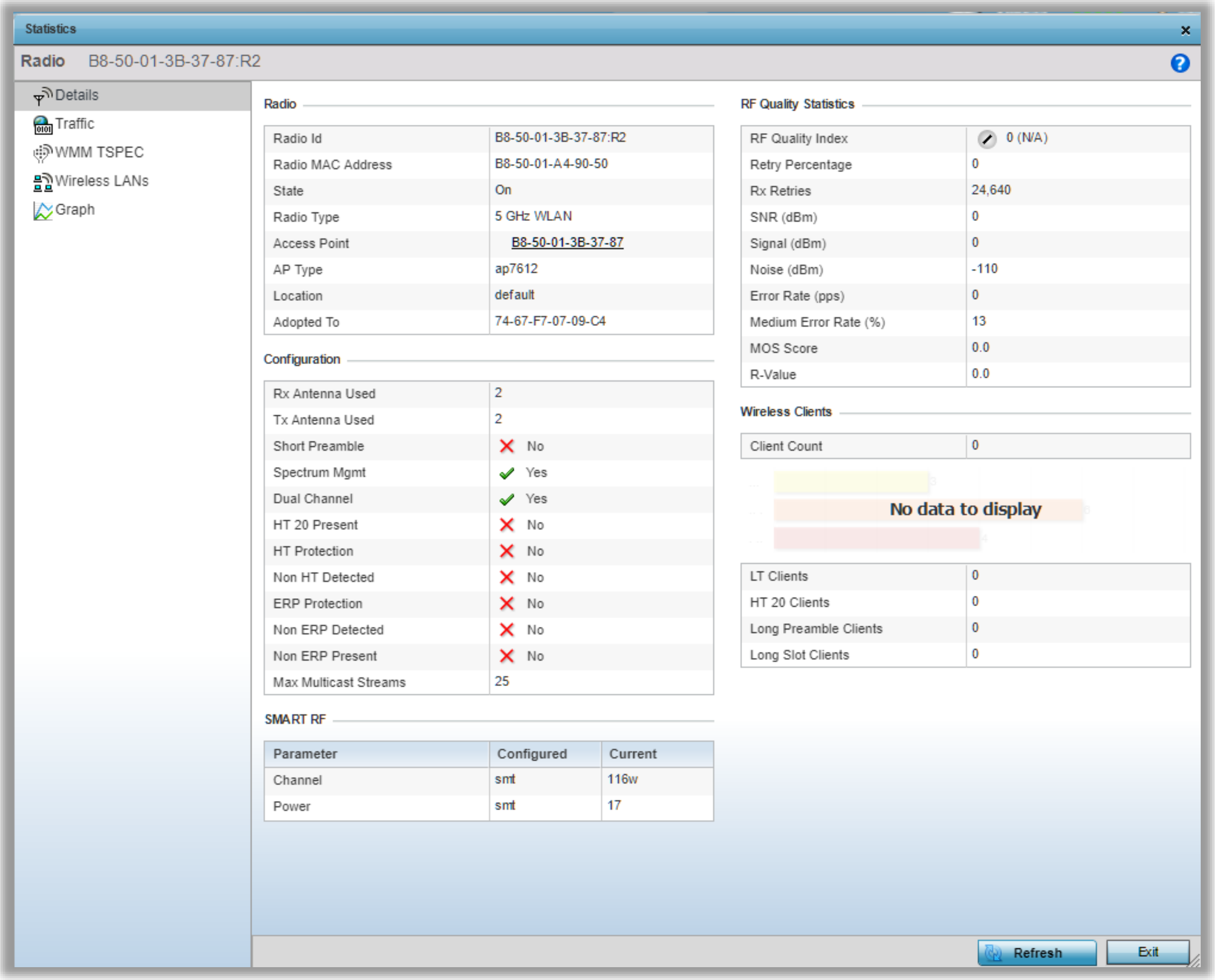
Radio Status and Statistics:

Statistics > {RF Domain Name} > Radios > Status:



RF Domain default

Radio	Radio MAC	Radio Type	Access Point	AP Type	State	Channel Current(Config)	Power Current(Config)	Clients
ap7612-3B3787:R1	B8-50-01-A4-90	2.4 GHz WLAN	ap7612-3B378	AP7612	On	6 (smt)	13 (smt)	1
ap7612-3B3787:R2	B8-50-01-A4-90	5 GHz WLAN	ap7612-3B378	AP7612	On	116w (smt)	17 (smt)	0
ap8533-0709C4:R1	74-67-F7-64-B0	2.4 GHz WLAN	ap8533-0709C	AP8533	On	1 (smt)	17 (smt)	0
ap8533-0709C4:R2	74-67-F7-64-9A	5 GHz WLAN	ap8533-0709C	AP8533	On	56 (smt)	17 (smt)	0
ap8533-0709C4:R3	74-67-F7-64-D5	Sensor	ap8533-0709C	AP8533	Off	N/A (smt)	30 (smt)	0
ap8533-5C452D:R1	74-67-F7-75-F3	2.4 GHz WLAN	ap8533-5C452	AP8533	On	11 (smt)	17 (smt)	0
ap8533-5C452D:R2	74-67-F7-76-09	5 GHz WLAN	ap8533-5C452	AP8533	On	60 (smt)	17 (smt)	0
ap8533-5C452D:R3	74-67-F7-76-27	Sensor	ap8533-5C452	AP8533	Off	N/A (smt)	30 (smt)	0



Radio B8-50-01-3B-37-87:R2

Radio

Radio Id	B8-50-01-3B-37-87:R2
Radio MAC Address	B8-50-01-A4-90-50
State	On
Radio Type	5 GHz WLAN
Access Point	B8-50-01-3B-37-87
AP Type	ap7612
Location	default
Adopted To	74-67-F7-07-09-C4

Configuration

Rx Antenna Used	2
Tx Antenna Used	2
Short Preamble	✗ No
Spectrum Mgmt	✓ Yes
Dual Channel	✓ Yes
HT 20 Present	✗ No
HT Protection	✗ No
Non HT Detected	✗ No
ERP Protection	✗ No
Non ERP Detected	✗ No
Non ERP Present	✗ No
Max Multicast Streams	25

SMART RF

Parameter	Configured	Current
Channel	smt	116w
Power	smt	17

RF Quality Statistics

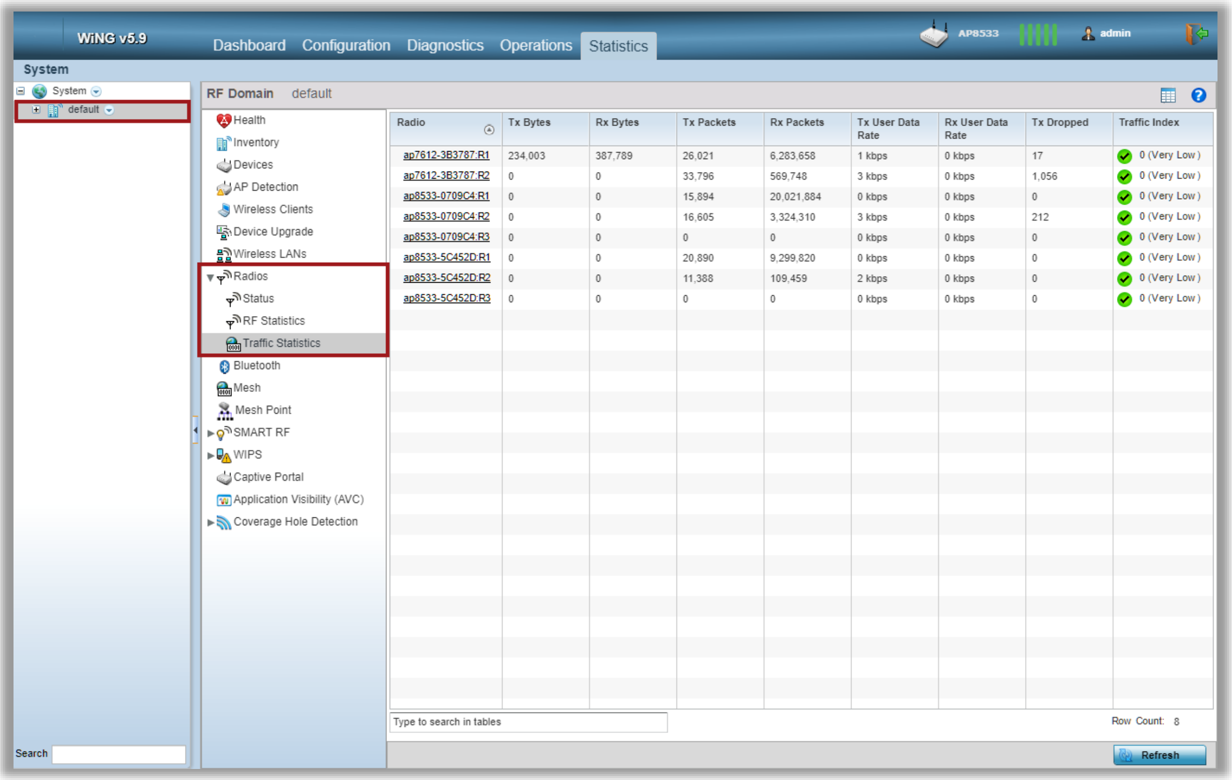
RF Quality Index	0 (N/A)
Retry Percentage	0
Rx Retries	24,640
SNR (dBm)	0
Signal (dBm)	0
Noise (dBm)	-110
Error Rate (pps)	0
Medium Error Rate (%)	13
MOS Score	0.0
R-Value	0.0

Wireless Clients

Client Count	0

No data to display

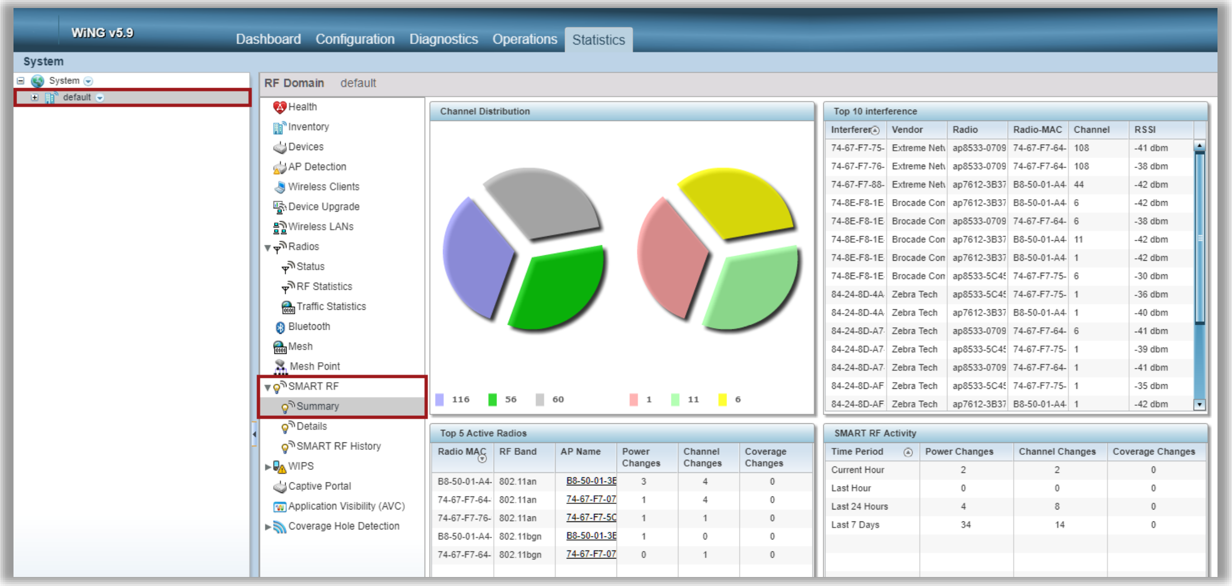
LT Clients	0
HT 20 Clients	0
Long Preamble Clients	0
Long Slot Clients	0



Radio	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets	Tx User Data Rate	Rx User Data Rate	Tx Dropped	Traffic Index
ap7612-3B3787:R1	234,003	387,789	26,021	6,283,658	1 kbps	0 kbps	17	✓ 0 (Very Low)
ap7612-3B3787:R2	0	0	33,796	569,748	3 kbps	0 kbps	1,056	✓ 0 (Very Low)
ap8533-0709C4:R1	0	0	15,894	20,021,884	0 kbps	0 kbps	0	✓ 0 (Very Low)
ap8533-0709C4:R2	0	0	16,605	3,324,310	3 kbps	0 kbps	212	✓ 0 (Very Low)
ap8533-0709C4:R3	0	0	0	0	0 kbps	0 kbps	0	✓ 0 (Very Low)
ap8533-5C452D:R1	0	0	20,890	9,299,820	0 kbps	0 kbps	0	✓ 0 (Very Low)
ap8533-5C452D:R2	0	0	11,388	109,459	2 kbps	0 kbps	0	✓ 0 (Very Low)
ap8533-5C452D:R3	0	0	0	0	0 kbps	0 kbps	0	✓ 0 (Very Low)

SMART RF Statistics:

Statistics > {RF Domain Name} > SMART RF > Summary:



Top 10 interference

Interferer	Vendor	Radio	Radio-MAC	Channel	RSSI
74-67-F7-75-	Extreme Netv	ap8533-0709	74-67-F7-64-	108	-41 dbm
74-67-F7-76-	Extreme Netv	ap8533-0709	74-67-F7-64-	108	-38 dbm
74-67-F7-88-	Extreme Netv	ap7612-3B37	B8-50-01-A4-	44	-42 dbm
74-8E-F8-1E	Brocade Con	ap7612-3B37	B8-50-01-A4-	6	-42 dbm
74-8E-F8-1E	Brocade Con	ap8533-0709	74-67-F7-64-	6	-38 dbm
74-8E-F8-1E	Brocade Con	ap7612-3B37	B8-50-01-A4-	11	-42 dbm
74-8E-F8-1E	Brocade Con	ap7612-3B37	B8-50-01-A4-	1	-42 dbm
74-8E-F8-1E	Brocade Con	ap8533-5C45	74-67-F7-75-	6	-30 dbm
84-24-8D-4A	Zebra Tech	ap8533-5C45	74-67-F7-75-	1	-36 dbm
84-24-8D-4A	Zebra Tech	ap7612-3B37	B8-50-01-A4-	1	-40 dbm
84-24-8D-A7	Zebra Tech	ap8533-0709	74-67-F7-64-	6	-41 dbm
84-24-8D-A7	Zebra Tech	ap8533-5C45	74-67-F7-75-	1	-39 dbm
84-24-8D-A7	Zebra Tech	ap8533-0709	74-67-F7-64-	1	-41 dbm
84-24-8D-AF	Zebra Tech	ap8533-5C45	74-67-F7-75-	1	-35 dbm
84-24-8D-AF	Zebra Tech	ap7612-3B37	B8-50-01-A4-	1	-42 dbm

Top 5 Active Radios

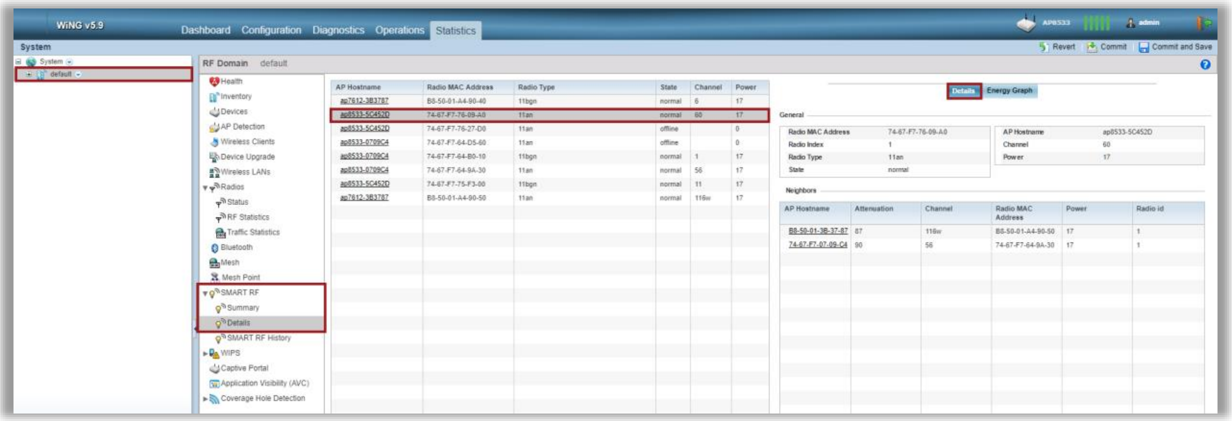
Radio MAC	RF Band	AP Name	Power Changes	Channel Changes	Coverage Changes
B8-50-01-A4-	802.11an	B8-50-01-3E	3	4	0
74-67-F7-64-	802.11an	74-67-F7-07	1	4	0
74-67-F7-76-	802.11an	74-67-F7-5C	1	1	0
B8-50-01-A4-	802.11bgn	B8-50-01-3E	1	0	0
74-67-F7-64-	802.11bgn	74-67-F7-07	0	1	0

SMART RF Activity

Time Period	Power Changes	Channel Changes	Coverage Changes
Current Hour	2	2	0
Last Hour	0	0	0
Last 24 Hours	4	8	0
Last 7 Days	34	14	0

SmartRF Neighbor radio table:

Statistics > {RF Domain Name} > SMART RF > Details:



AP Hostname	Radio MAC Address	Radio Type	State	Channel	Power
ap7612-3B3787	B8-50-01-A4-90-40	11bgn	normal	6	17
ap8533-5C452D	74-67-F7-76-09-A0	11an	normal	60	17
ap8533-5C452D	74-67-F7-76-27-D0	11an	offline		0
ap8533-0709C4	74-67-F7-64-D5-60	11an	offline		0
ap8533-0709C4	74-67-F7-64-B0-10	11bgn	normal	1	17
ap8533-0709C4	74-67-F7-64-9A-30	11an	normal	56	17
ap8533-5C452D	74-67-F7-75-F3-00	11bgn	normal	11	17
ap7612-3B3787	B8-50-01-A4-90-50	11an	normal	116w	17

General

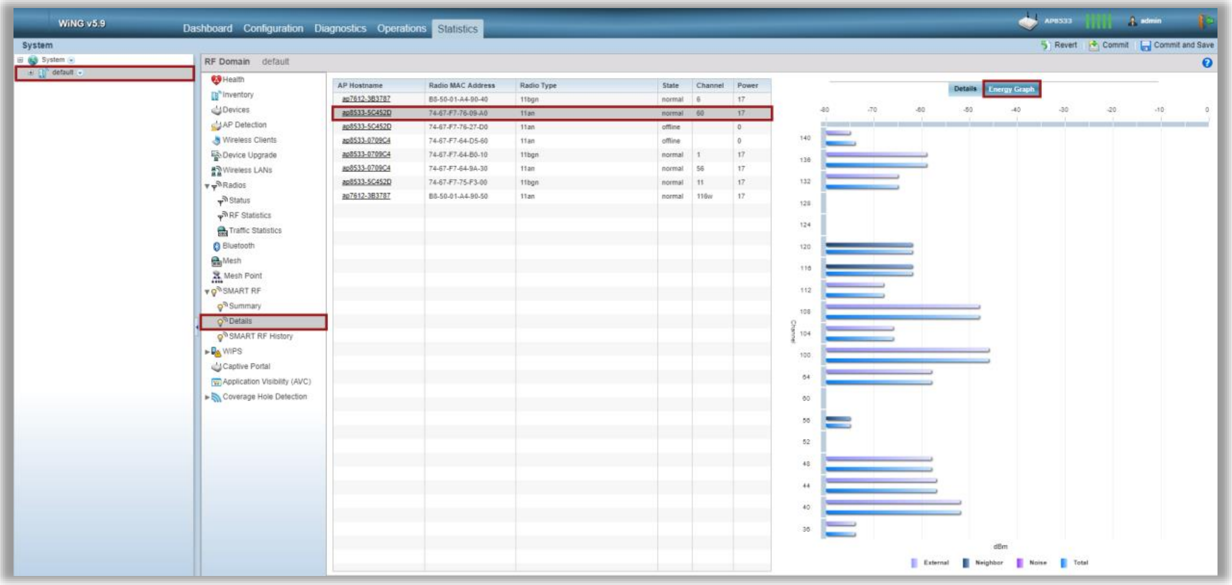
Radio MAC Address	74-67-F7-76-09-A0
Radio Index	1
Radio Type	11an
State	normal

AP Hostname	ap8533-5C452D
Channel	60
Power	17

Neighbors

AP Hostname	Attenuation	Channel	Radio MAC Address	Power	Radio id
B8-50-01-3B-37-87	87	116w	B8-50-01-A4-90-50	17	1
74-67-F7-07-09-C4	90	56	74-67-F7-64-9A-30	17	1

Statistics > {RF Domain Name} > SMART RF > Details > Energy Graph:



AP Hostname	Radio MAC Address	Radio Type	State	Channel	Power
ap7612-3B3787	B8-50-01-A4-90-40	11bgn	normal	6	17
ap8533-5C452D	74-67-F7-76-09-A0	11an	normal	60	17
ap8533-5C452D	74-67-F7-76-27-D0	11an	offline		0
ap8533-0709C4	74-67-F7-64-D5-60	11an	offline		0
ap8533-0709C4	74-67-F7-64-B0-10	11bgn	normal	1	17
ap8533-0709C4	74-67-F7-64-9A-30	11an	normal	56	17
ap8533-5C452D	74-67-F7-75-F3-00	11bgn	normal	11	17
ap7612-3B3787	B8-50-01-A4-90-50	11an	normal	116w	17

VirtualController – Frequently Asked Questions

Q: How many Access Points a Virtual Controller AP can manage?

A: Depends on the Virtual Controller Platform. The following table outlines VC maximum number of adopted APs:

Virtual Controller Platform	Maximum number of adopted APs
802.11n APs (AP6521, AP6522. AP6562, AP6532, AP8132, AP8122, AP8163, etc)	24
AP7502, AP7602, AP7622, AP7612, AP8222, AP8232	24
AP7522, AP7532, AP7562, AP7632. AP7662, AP8432, AP8533	64

Q: Is it necessary to purchase licenses to adopt and manage Access Points by the Virtual Controller?

A: No, all licenses are built-in, based on the numbers provided in the table above.

Q: What is the difference between Virtual Controller and RF Domain Manager?

A: Virtual Controller performs a function of a management plane (configuration of the whole site, monitoring etc), while RF Domain Manager performs a function of a control plane (aggregating statistics, coordinating SmartRF and WIPS logic for the whole site, etc). In a Virtual Controller deployment both functions resides on the Virtual Controller.

Q; Is Virtual Controller a recommended solution for multi site deployments?

A: No. For multi site distributed deployments it is recommended to use "real" WiNG Controller (virtualized or hardware based) in the NOC with remote sites being centrally managed. Virtual Controller is a solution for single site deployments. One exception to the rule – multi-tenant multi-site deployments, where configuration management has to be locally administered per site.

Q: Does Virtual Controller supports user data tunneling and/or IPSEC tunnels?

A: While Virtual Controller itself cannot terminate data tunnels like a hardware based controller appliance, all APs support L2TPv3 tunneling client functionality, which allows to terminate user data tunnels to any external L2TPv3 access concentrator (3rd party L2TPv3 compliant device or "zero-license" WiNG appliance, such as NX5500/NX7500/NX9610)

Q: Are there any features not supported on the Virtual Controller compared to the "real" WiNG controllers?

A: No, the feature set is identical, as both solutions run the same code.

Q: Does Virtual Controller support NSight integration?

A: Yes.

Q: Does Virtual Controller support ExtremeGuest integration?

A: Yes, please refer to the ExtremeGuest Deployment Guide for details.

Q: Does Virtual Controller support ExtremeControl / ExtremeManagement integration?

A: Virtual Controller supports ExtremeControl / ExtermeManagement integration in the same way a “real” WiNG controller does.

Terms & Condition of Use

Extreme Networks, Inc. reserves all rights to its materials and the content of the materials. No material provided by Extreme Networks, Inc. to a Partner (or Customer, etc.) may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, or incorporated into any other published work, except for internal use by the Partner and except as may be expressly permitted in writing by Extreme Networks, Inc.

This document and the information contained herein are intended solely for informational use. Extreme Networks, Inc. makes no representations or warranties of any kind, whether expressed or implied, with respect to this information and assumes no responsibility for its accuracy or completeness. Extreme Networks, Inc. hereby disclaims all liability and warranty for any information contained herein and all the material and information herein exists to be used only on an "as is" basis. More specific information may be available on request. By your review and/or use of the information contained herein, you expressly release Extreme from any and all liability related in any way to this information. A copy of the text of this section is an uncontrolled copy, and may lack important information or contain factual errors. All information herein is Copyright ©Extreme Networks, Inc. All rights reserved. All information contain in this document is subject to change without notice.

For additional information refer to:
http://www.extremenetworks.com/company/legal/terms/

Revision History

Date	Revision	Changes Made	Author
27th October 2017	1.0	Initial release	Slava Dementyev