



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

© 2012–2017 Extreme Networks, Inc. All Rights Reserved.

AccessAdapt, Alpine, Altitude, BlackDiamond, Direct Attach, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrives, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Ridgeline, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, XNV, the Extreme Networks logo, the Alpinelogo, the BlackDiamond logo, the Extreme Turbodrives logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is the property of InMon Corporation.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

For additional information on Extreme Networks trademarks, see www.extremenetworks.com/company/legal/trademarks.

Contents

Pre-Requisites.....	4
VirtualController – Overview.....	5
VirtualController – Deployment Example	7
Step 1 – Login to one of the AP8533s via HTTPS	8
Step 2 – Go through the Installation Wizard.....	9
Step 3 – Managing mixed AP environment - Profiles.....	16
Step 4 – Managing mixed AP environment – Auto Provisioning Policy	23
Step 5 – Adopted AP Upgrades.....	31
Step 6 – ExtremeNSight Integration.....	35
Step 7 – 802.1X SSID with External RADIUS.....	36
VirtualController – Verification & Monitoring	44
VirtualController – Frequently Asked Questions.....	49
Terms & Condition of Use.....	51
Revision History.....	52

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.

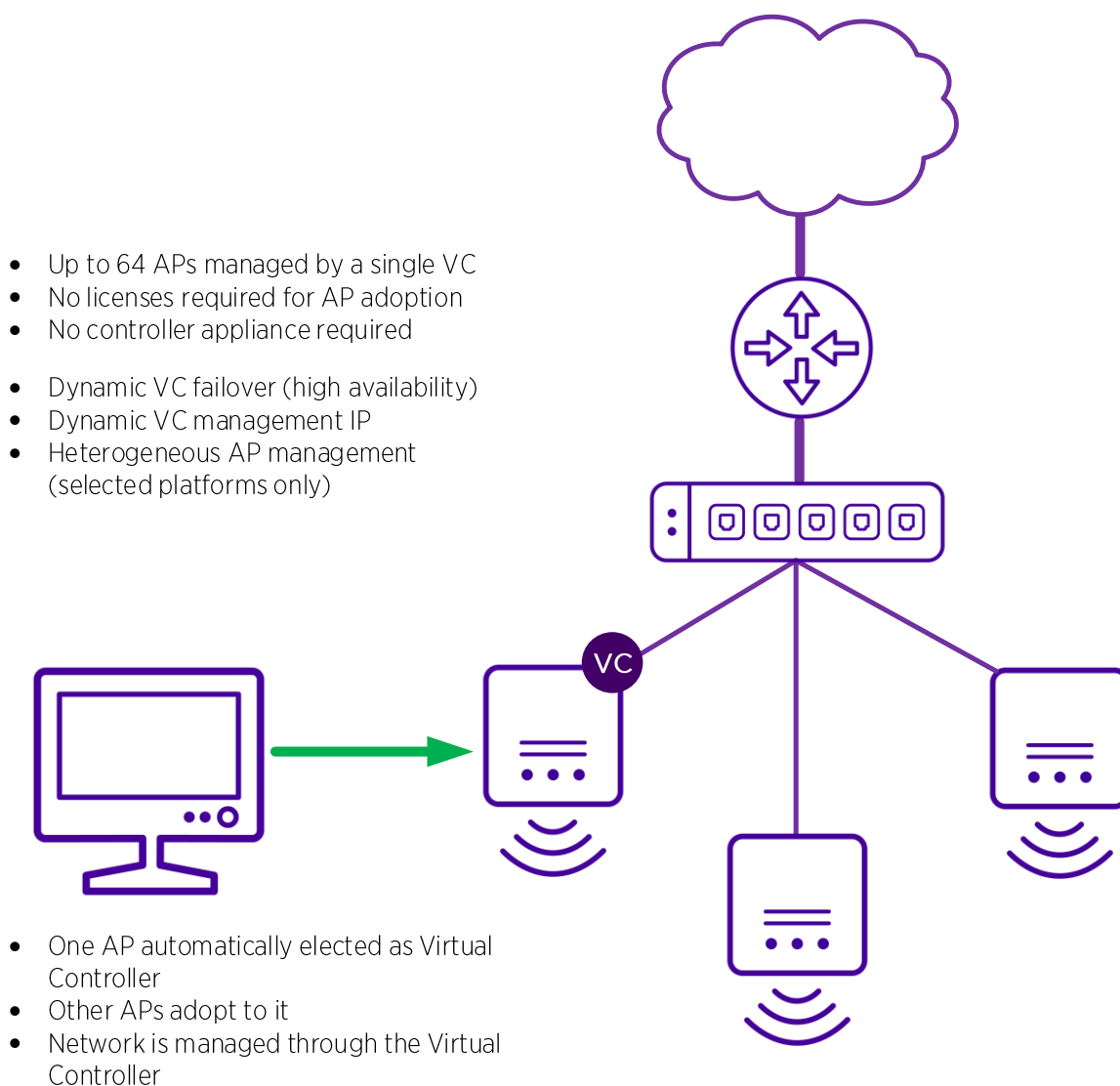
VirtualController – Overview

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).

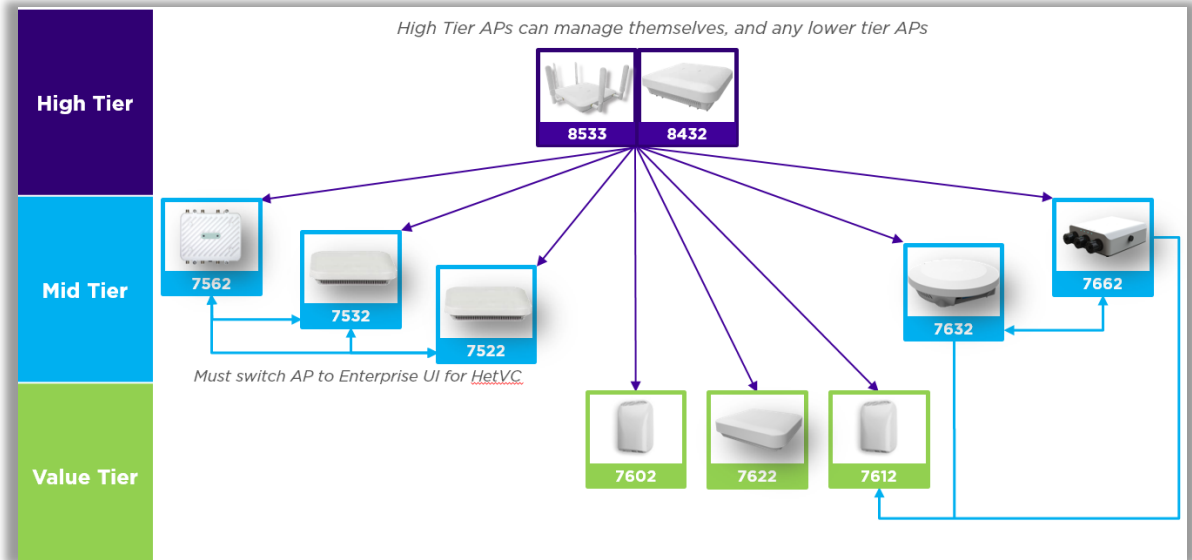
Prior to 5.9.1 WiNG release Virtual Controller functionality was limited to manage of the like- Access Points only, whereas WiNG 5.9.1 provided heterogeneous AP management on selected AP platforms to allow mixed AP environments managed by the same Virtual Controller AP.

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:



The following diagram outlines supported Heterogeneous VC deployment modes:



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:

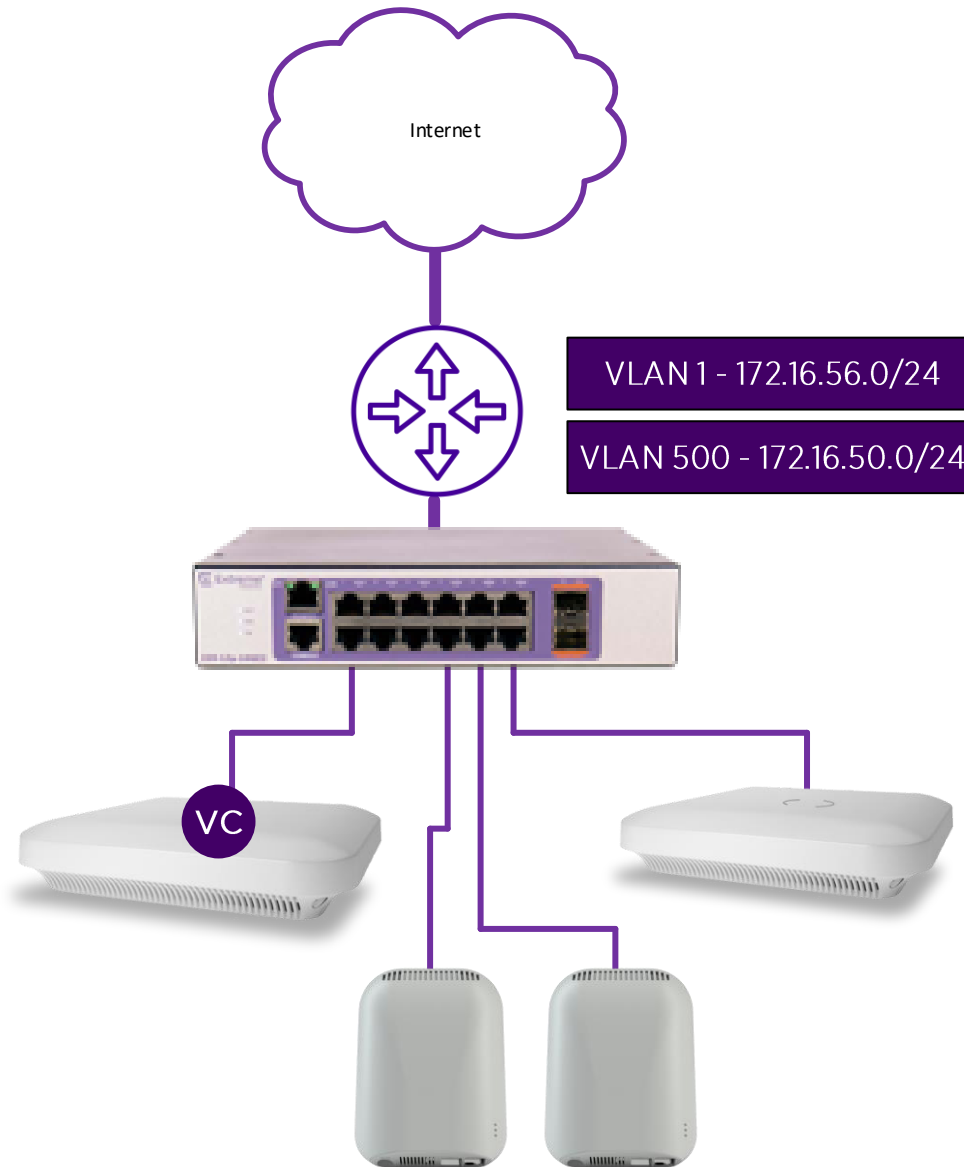
VC Type ↓	Managed Access Points				
	AP8533	AP8432	AP7522 AP7532 AP7562	AP7602 AP7622	AP7612 AP7632 AP7662
AP8533 AP8432	✓	✓	✓	✓	✓
AP7632 AP7662	✗	✗	✗	✗	✓
AP7522 AP7532 AP7562	✗	✗	✓	✗	✗

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

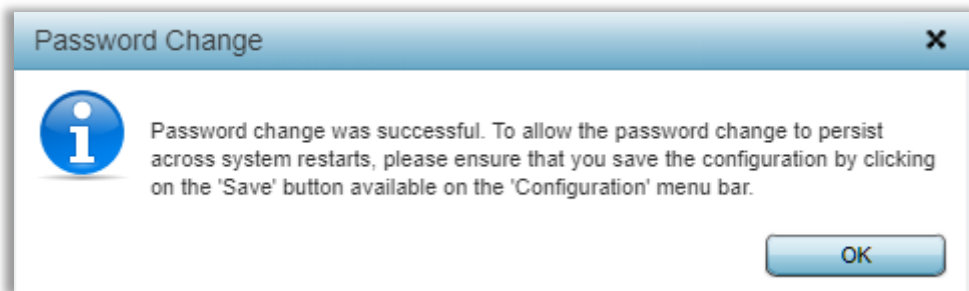
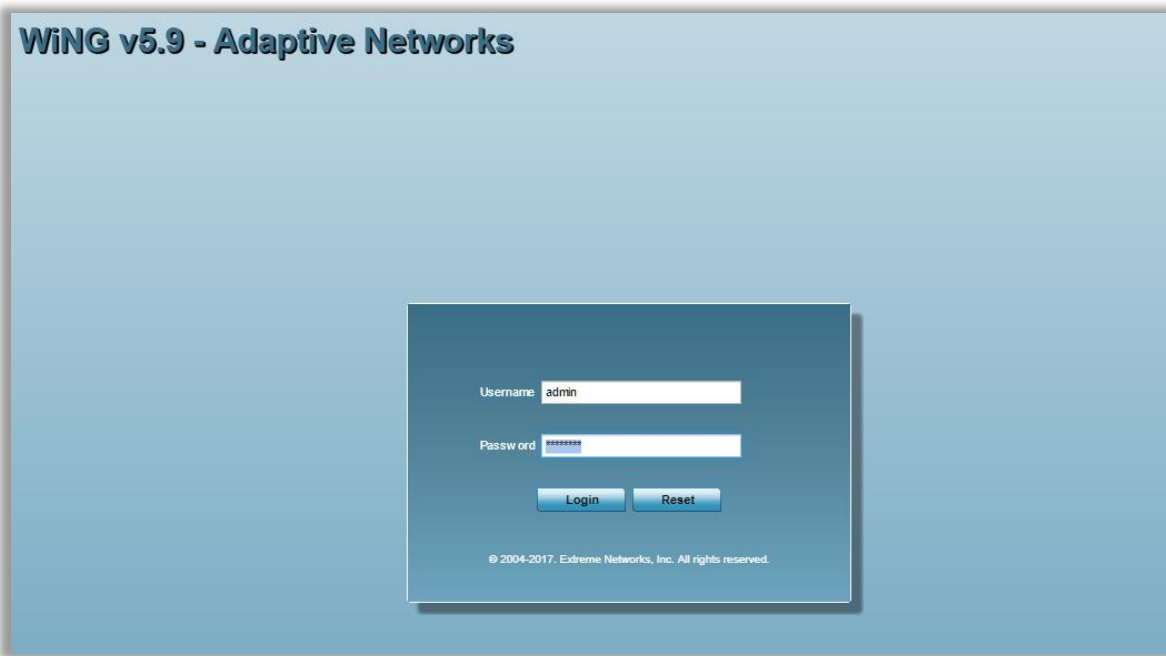
In this guide we will have the following setup, but similar steps can be used for any other supported Heterogeneous VC combination. In our example we are going to have 2x AP8533s and 2x AP7612s, plugged into the same Extreme 220 12 port switch, where local router provides DHCP / DNS / NAT services:



Step 1 - Login to one of the AP8533s via HTTPS

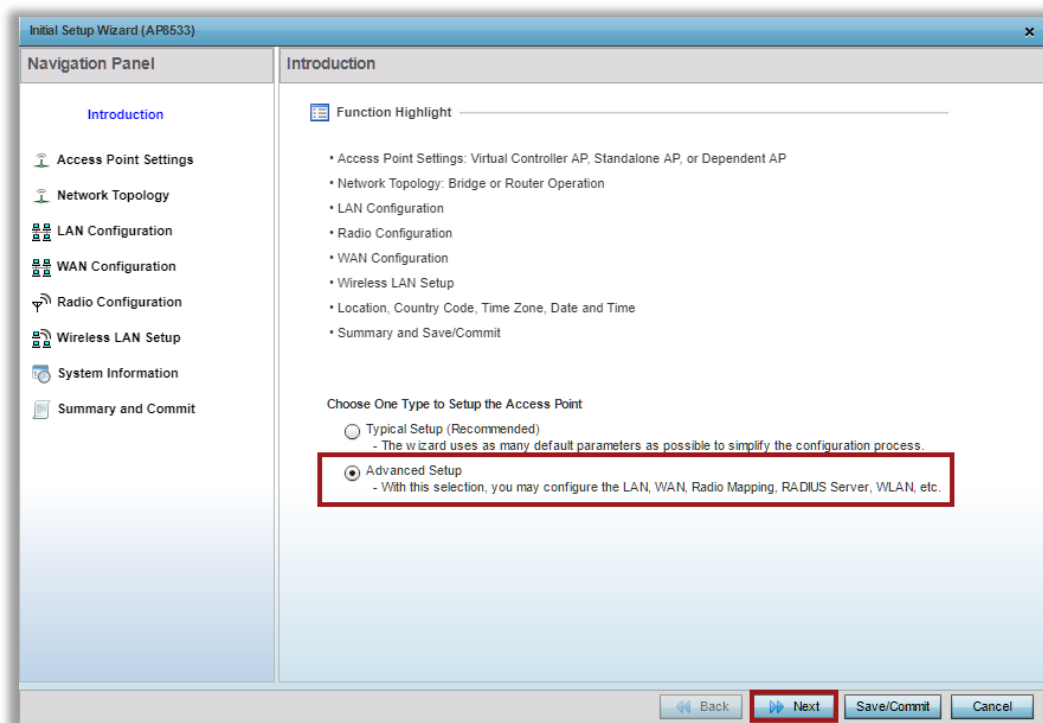
First you should login to the Web UI interface of one of the AP8533s (or any AP that you are planning to use as a Virtual Controller). You can either find the IP address of the Access Point via your DHCP server or use default Zeroconf IP address (169.254.0.0/16) if no DHCP server is locally available. 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



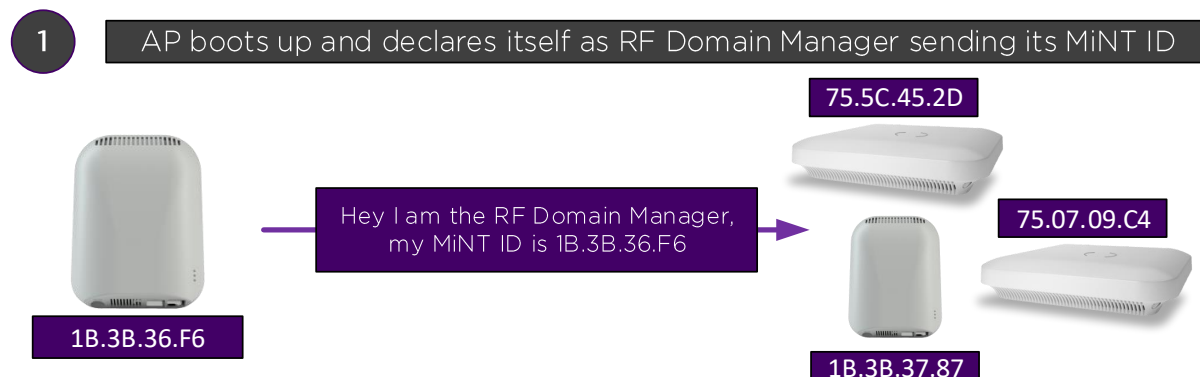
Step 2 – Go through the Installation Wizard

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

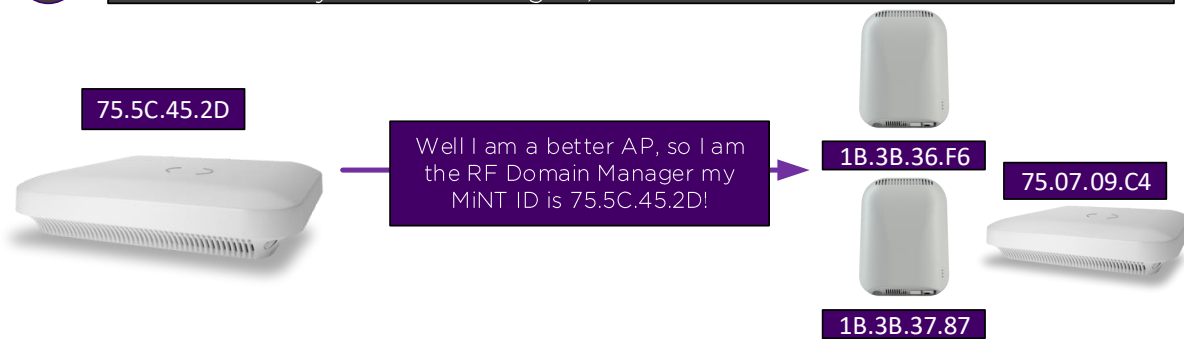


On the next screen you will be prompted to select the mode in which this AP will function. In our example we are going to use “Virtual Controller AP Auto”, which will enable Virtual Controller functionality, but will also provide automatic Virtual Controller failover in case current VC is unavailable,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

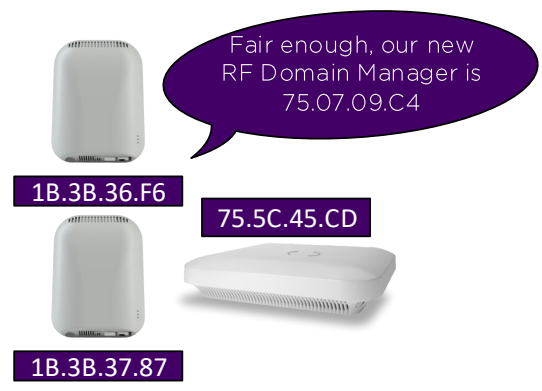
Note that Virtual Controller Auto election relies on the RF Domain Manager election process. In other words – if the AP becomes elected as RF Domain Manager it automatically becomes the Virtual Controller. The following outlines general RF Domain Manager election process:



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 1B.3B.37.87



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

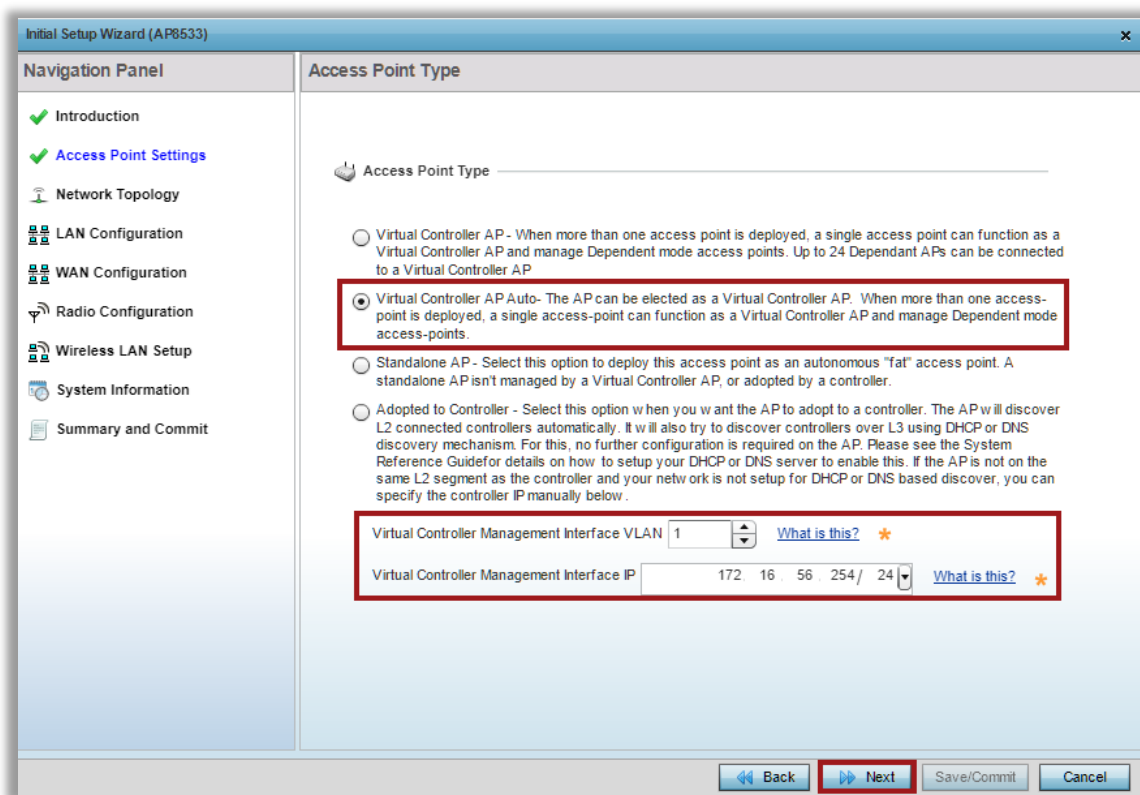


Generally, it is recommended to enable Auto VC feature only on the same-tier Access Points, like AP8432 and AP8533 and don't mix multiple AP tiers (refer to the Heterogeneous VC diagram in the Overview section of this document). The reason is that while failover to the lower tier AP will work (for example 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)

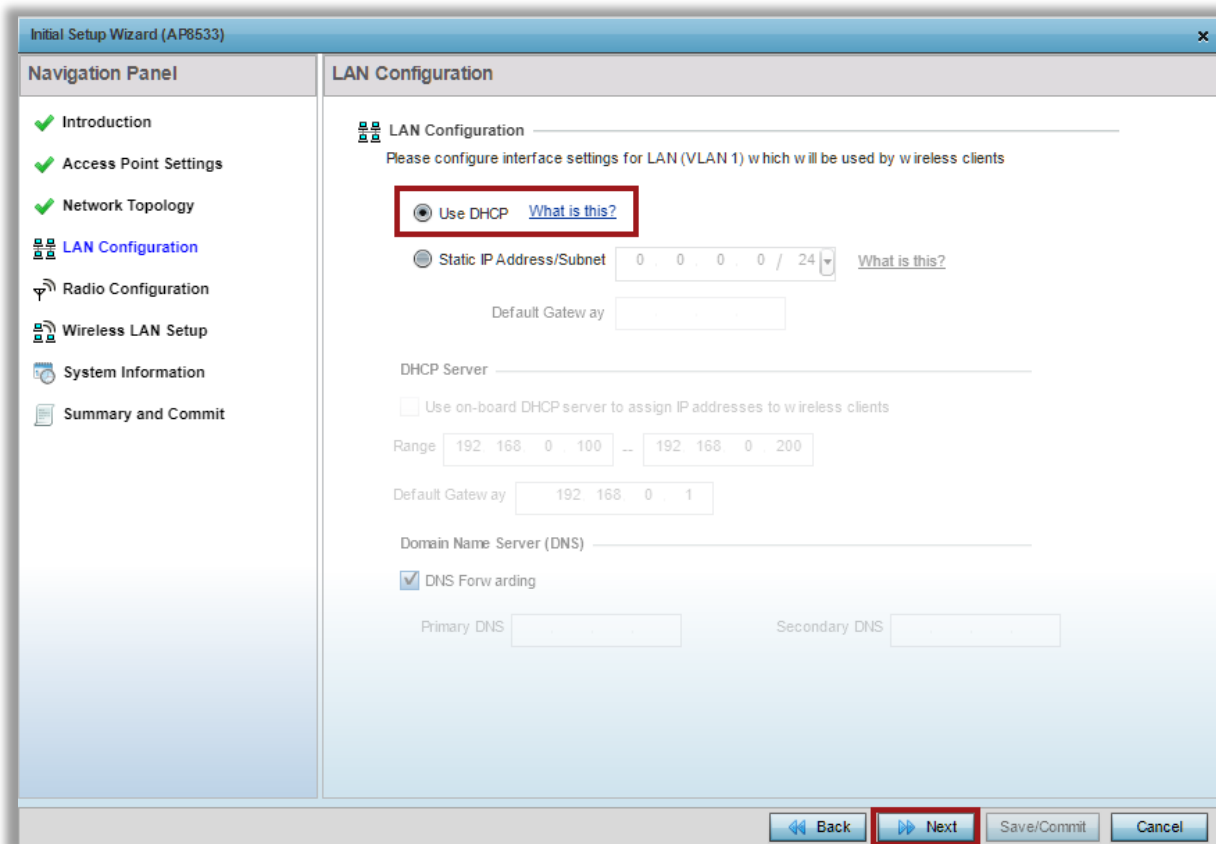
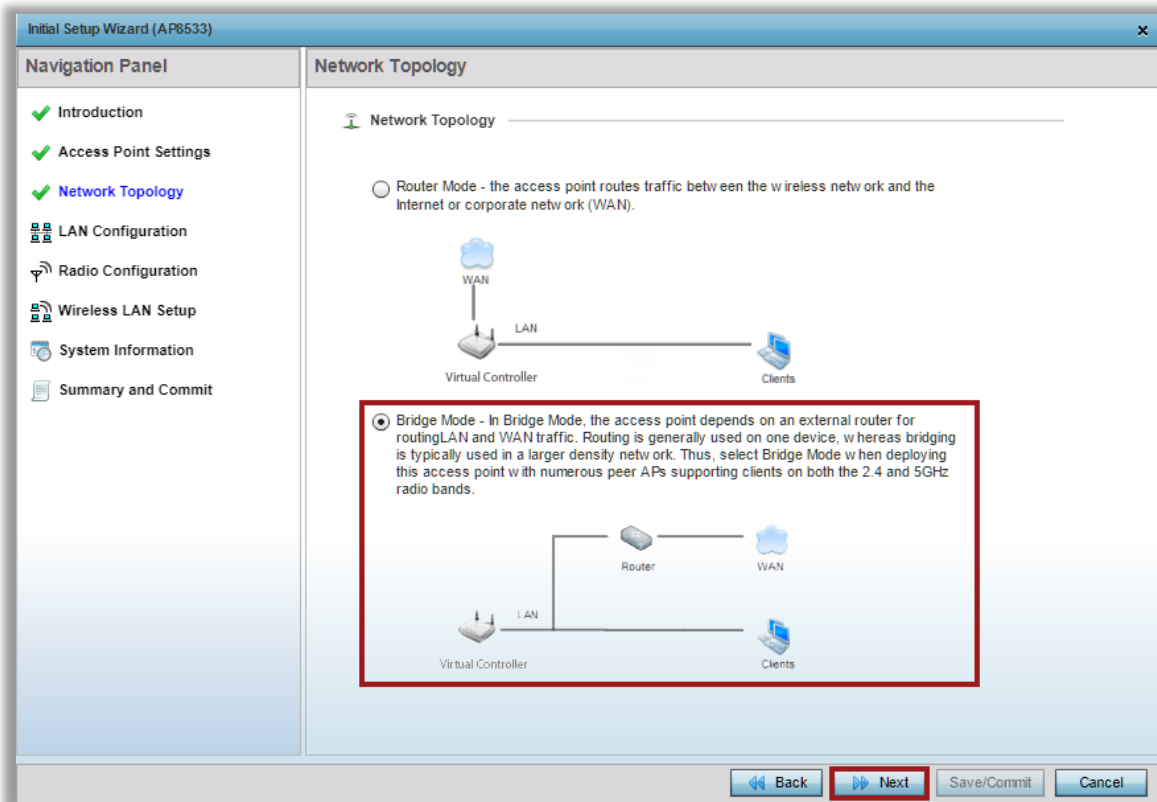
Virtual Controller Management VLAN Interface - this is the management VLAN ID that Virtual Controller will use to adopt and manage Access Points. By default, all APs will use untagged VLAN 1 for management. It is recommended to keep VLAN 1 unchanged and untagged for ease of deployment and management.

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

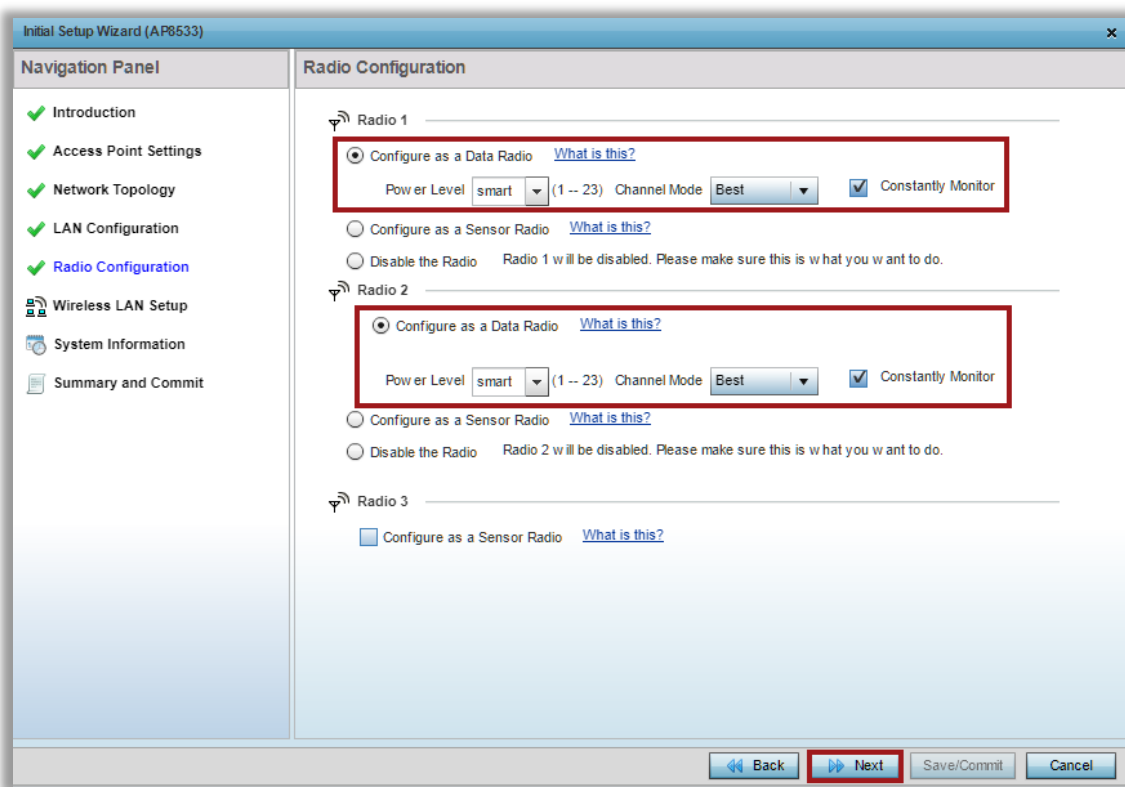
on this interface. Note that VC management IP address should be inside the same subnet as the management network:



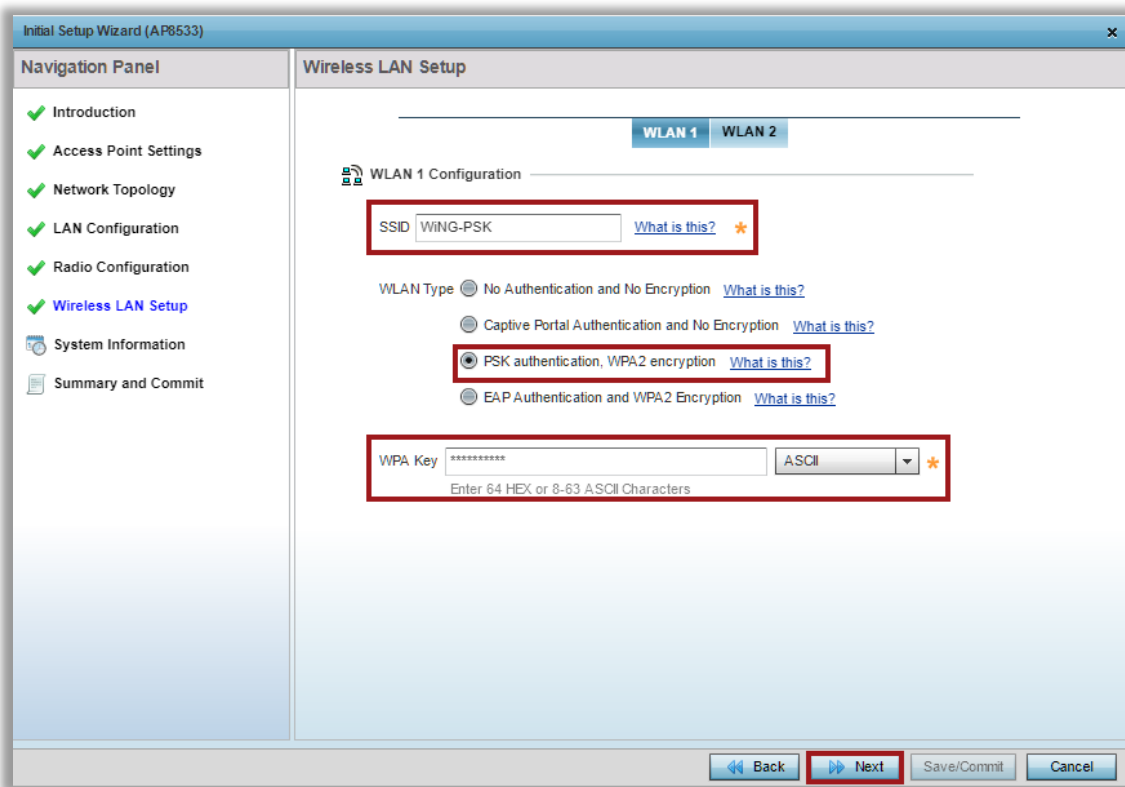
On the Network Topology screen there are two modes to select. For the purposes of this guide we will use Bridged mode, as local router is providing DHCP / NAT services. Optionally Router mode can be selected so that an AP can act as DHCP / NAT router for the wireless clients if required.



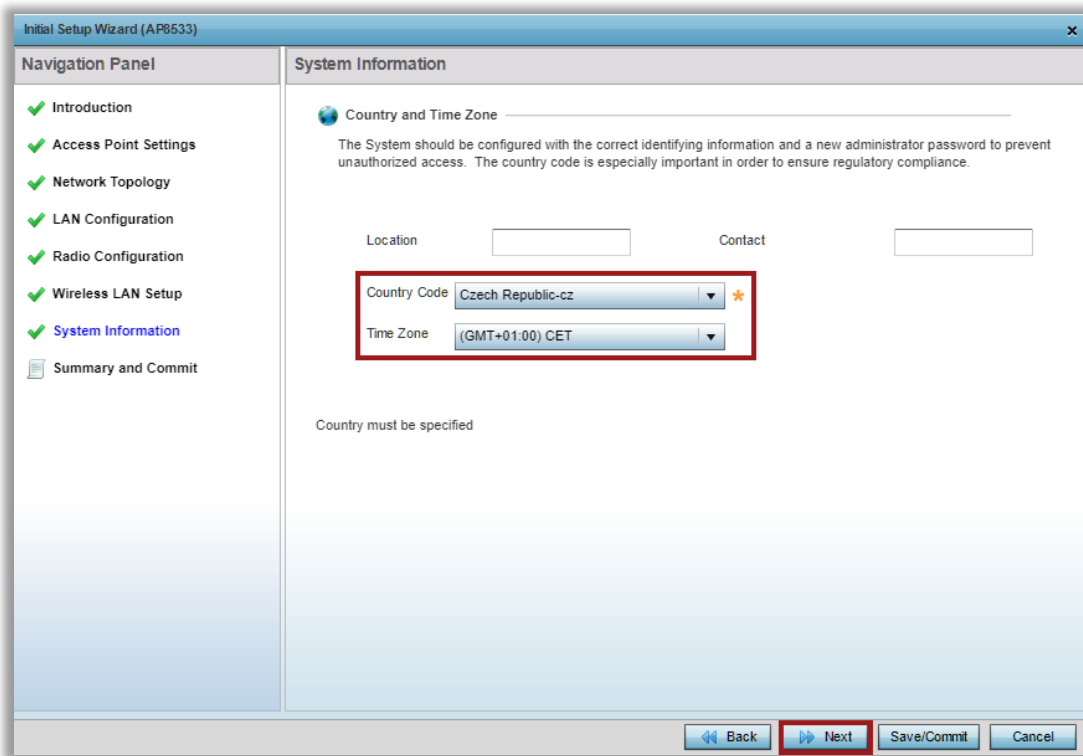
On the next screen select desired Radio Interface mode and click next:



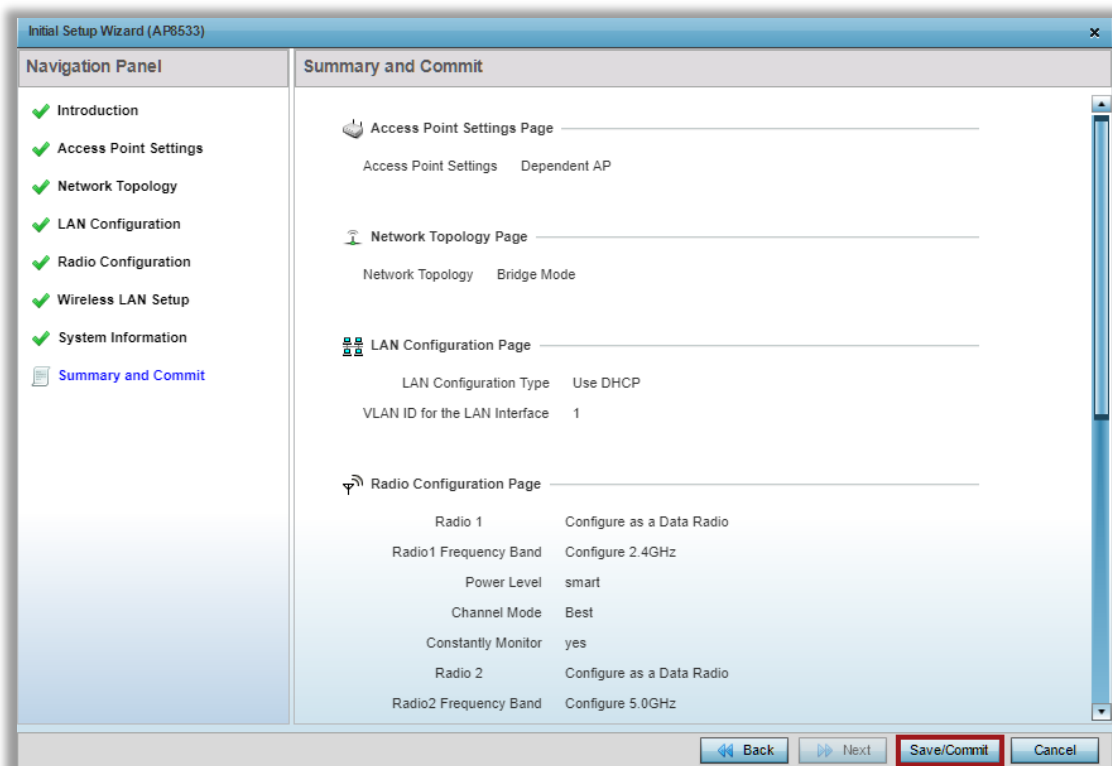
On the Wireless LAN Setup screen we are going to create one SSID with CCMP encryption and PSK authentication:

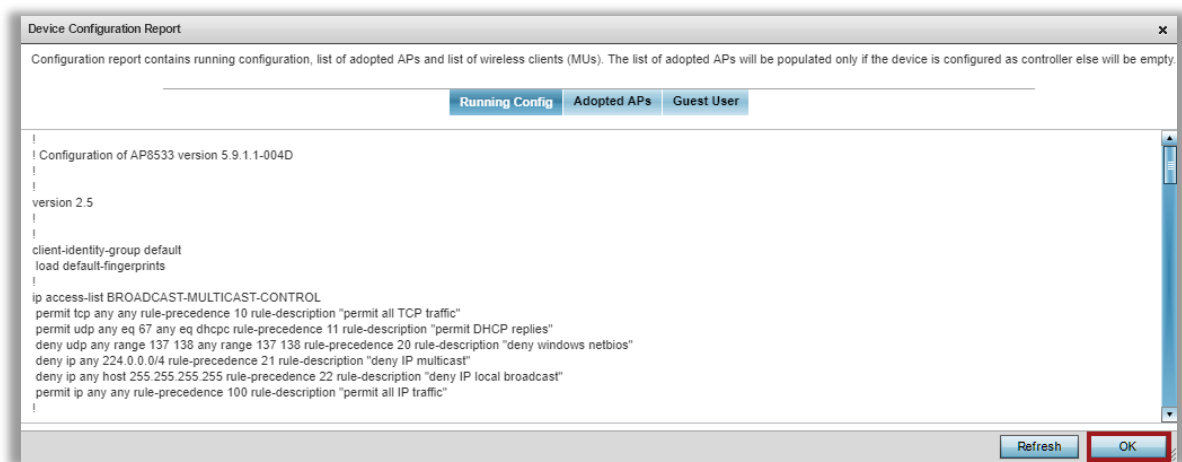


On the final configuration screen select *Country Code* so that AP can apply local regulatory rules and start advertising SSIDs, specify correct *Timezone* and then click *Next*:



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:



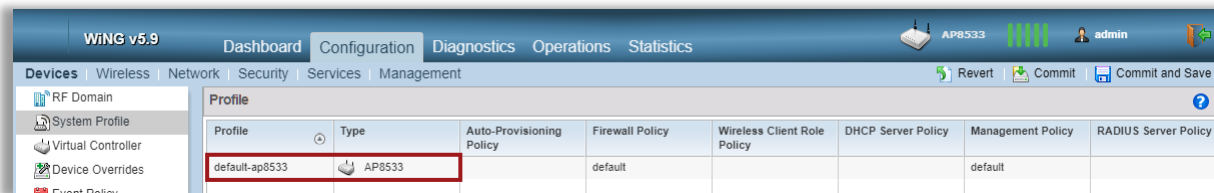


Immediately after finishing with the installation wizard we can see another AP8533 as online. Why don't we see other AP types? Read through the next 2 steps.

Step 3 – Managing mixed AP environment - Profiles

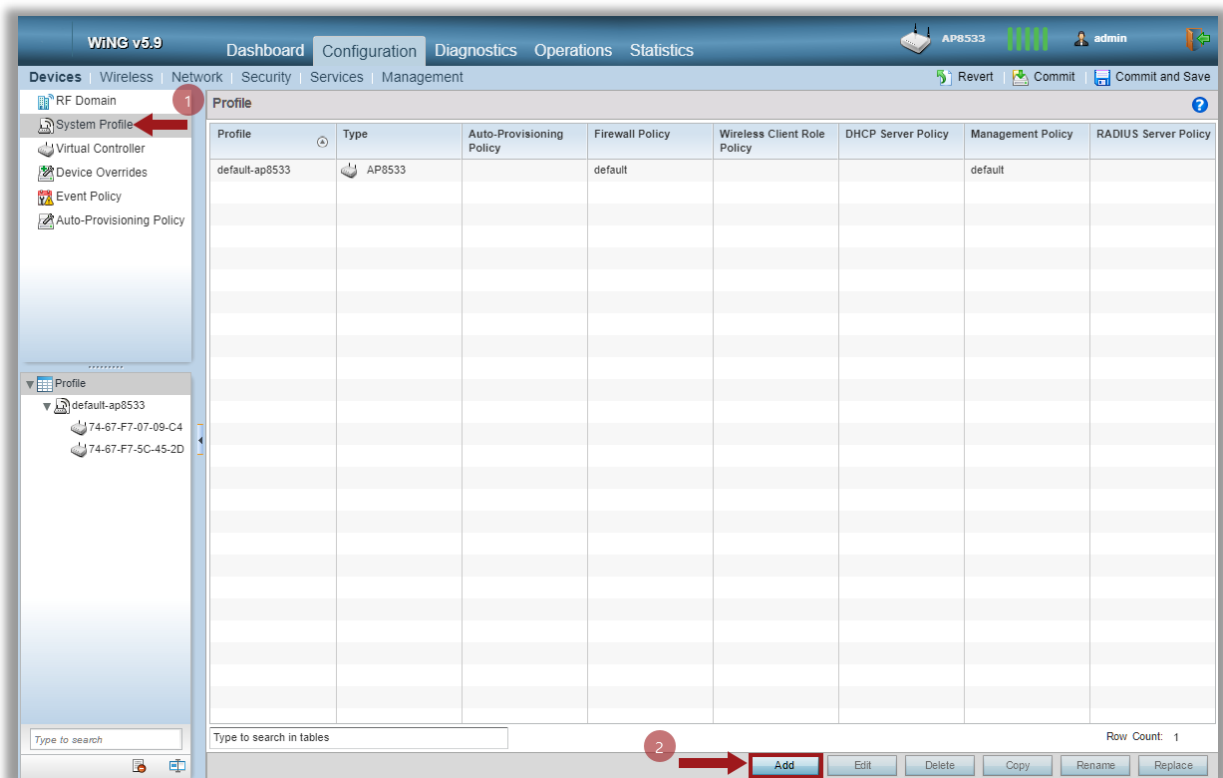
ExtremeWireless WiNG utilizes the concept of AP Profile to apply common configuration parameters, policies, Wireless LANs etc. to a group of Access Points, so that it is not needed to configure each and every AP individually.

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:

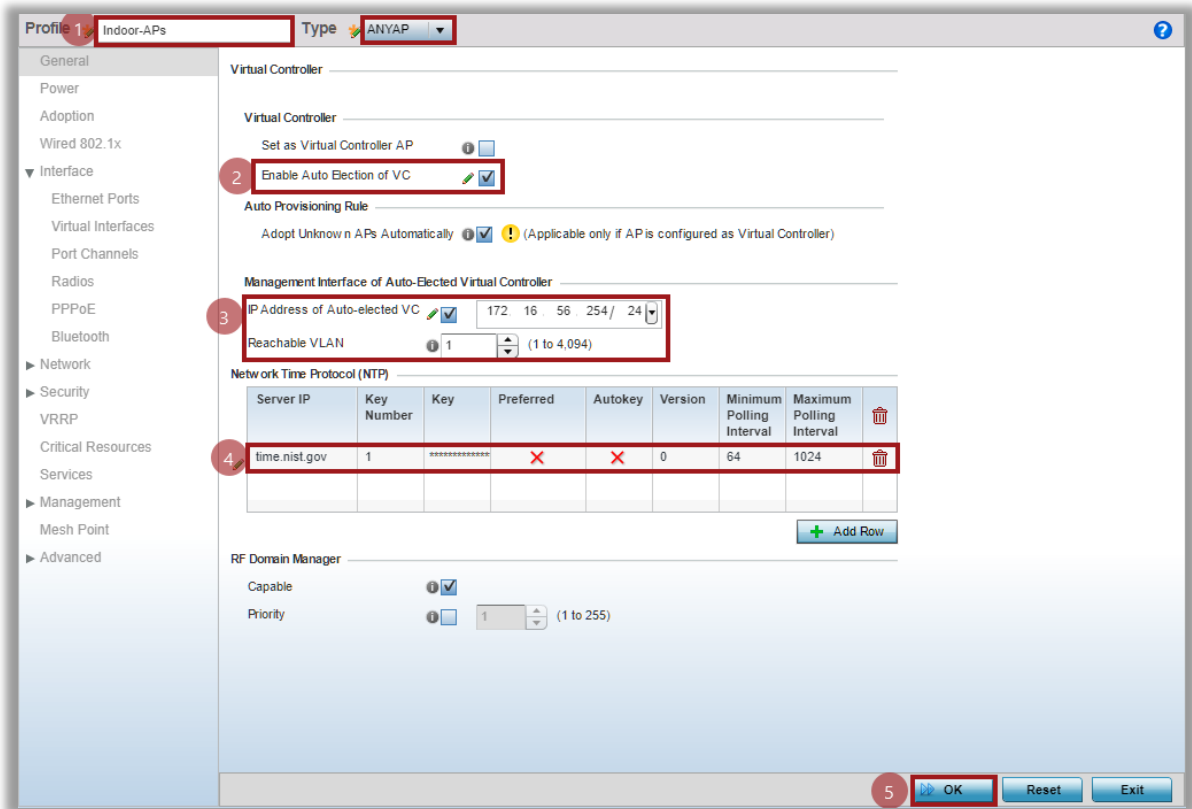


In order to manage multiple AP types, we need to utilize “anyap” Profiles, which can be used, as the name suggests, by any AP model types.

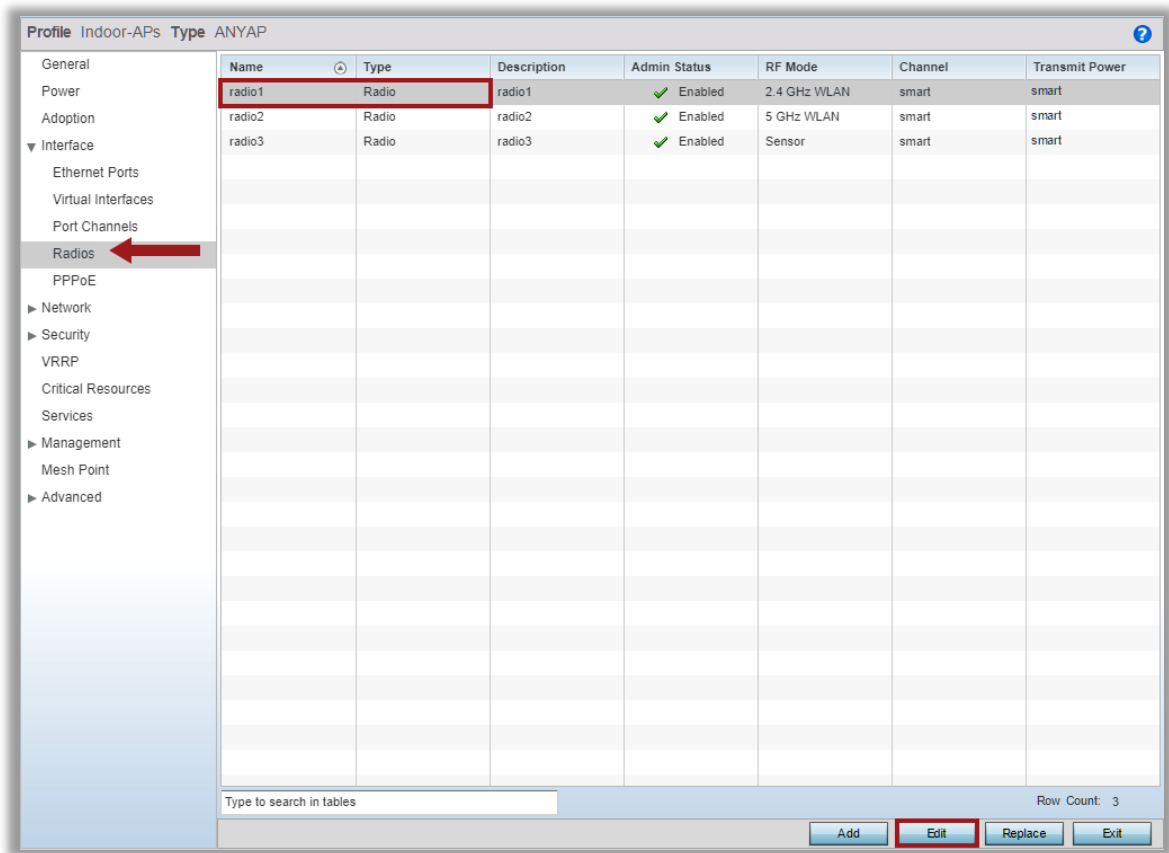
Let’s create a new *anyap* Profile for our Access Points, but first – login to the Virtual Controller UI using VC management IP address (do NOT connect to the real IP address of the AP you configured before):



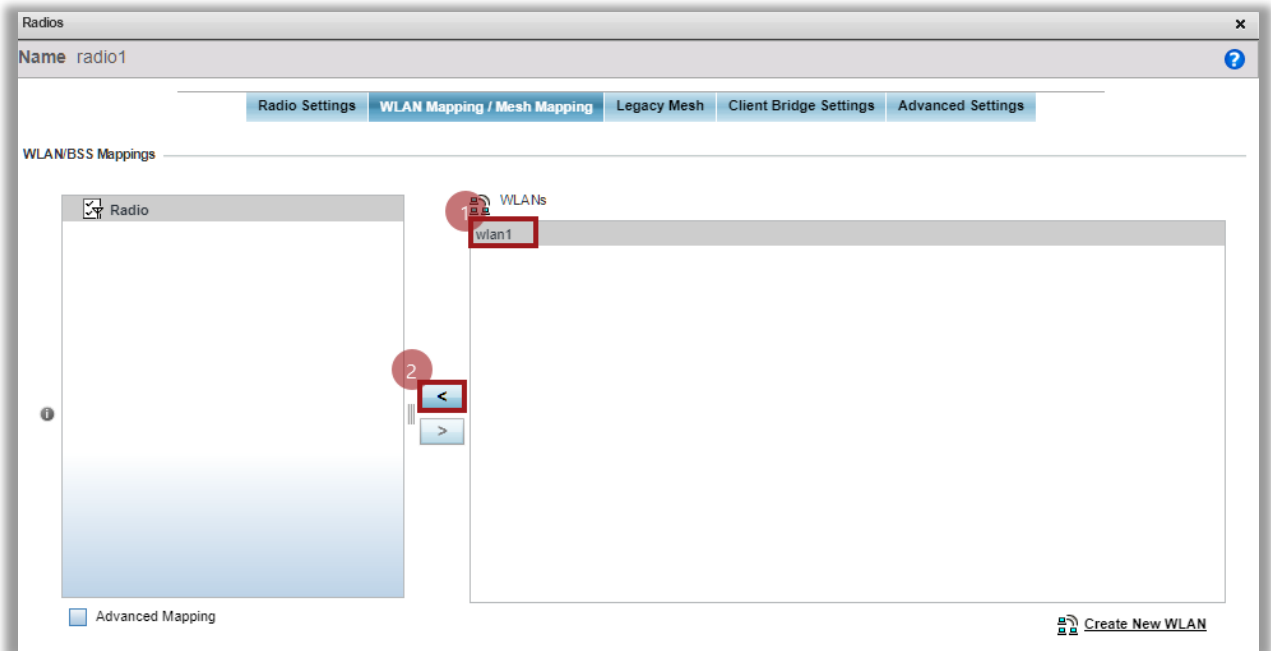
Set AP Profile name, select Profile type as *ANYAP*, enable *Auto Election of VC*, specify *VC management IP address*, specify *NTP server*, then click *OK*:

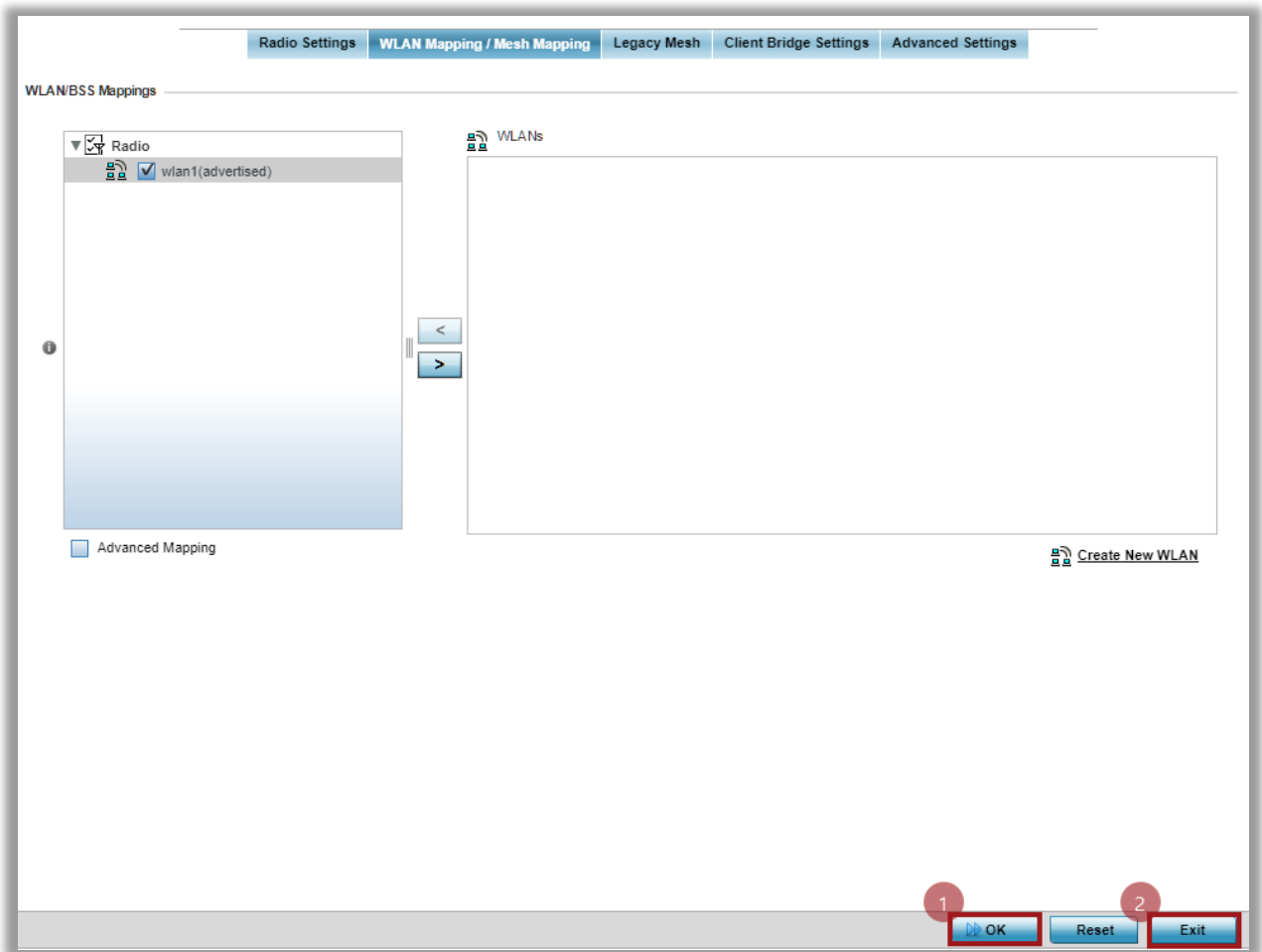


Move to the *Interface > Radios* section of the AP Profile and edit *radio 1* (2.4GHz) interface:



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:





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

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

Radio Settings | **WLAN Mapping / Mesh Mapping** | Legacy Mesh | Client Bridge Settings | Advanced Settings

WLAN/BSS Mappings

Radio

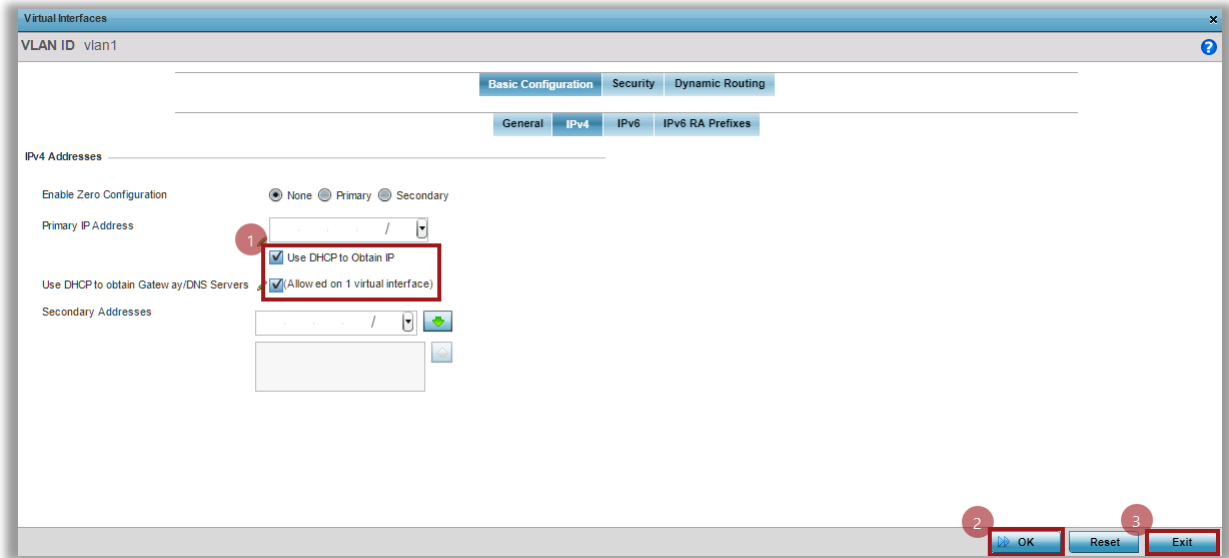
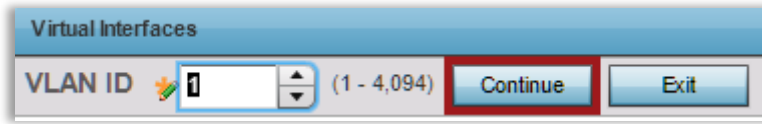
WLANs

wlan1

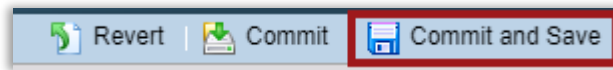
< >

Advanced Mapping

Create New WLAN



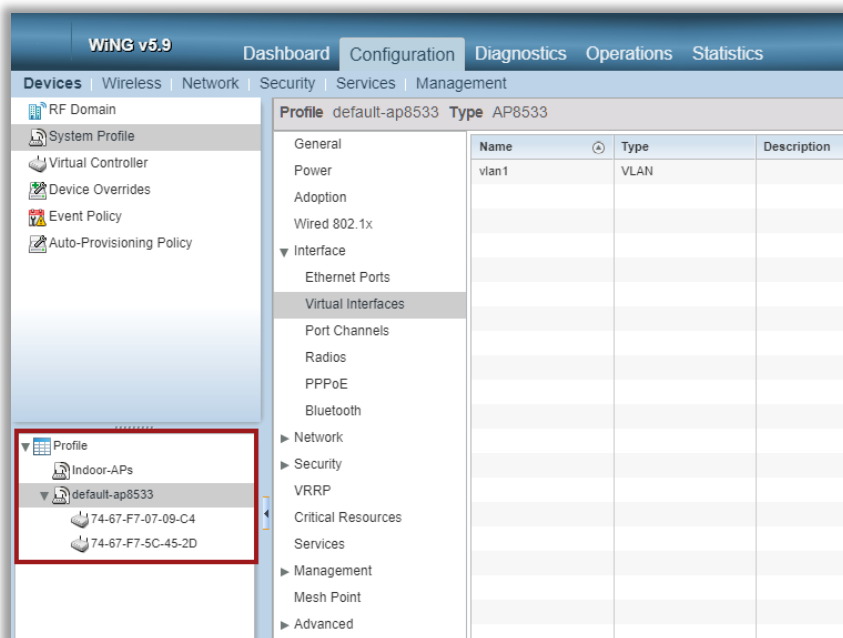
Commit and Save changes. Note that *Commit* action applies changed and saves them to the running configuration that does not survive AP reboot, while *Commit&Save* action saves changes to both running and startup configs, which will be saved across AP reboots:



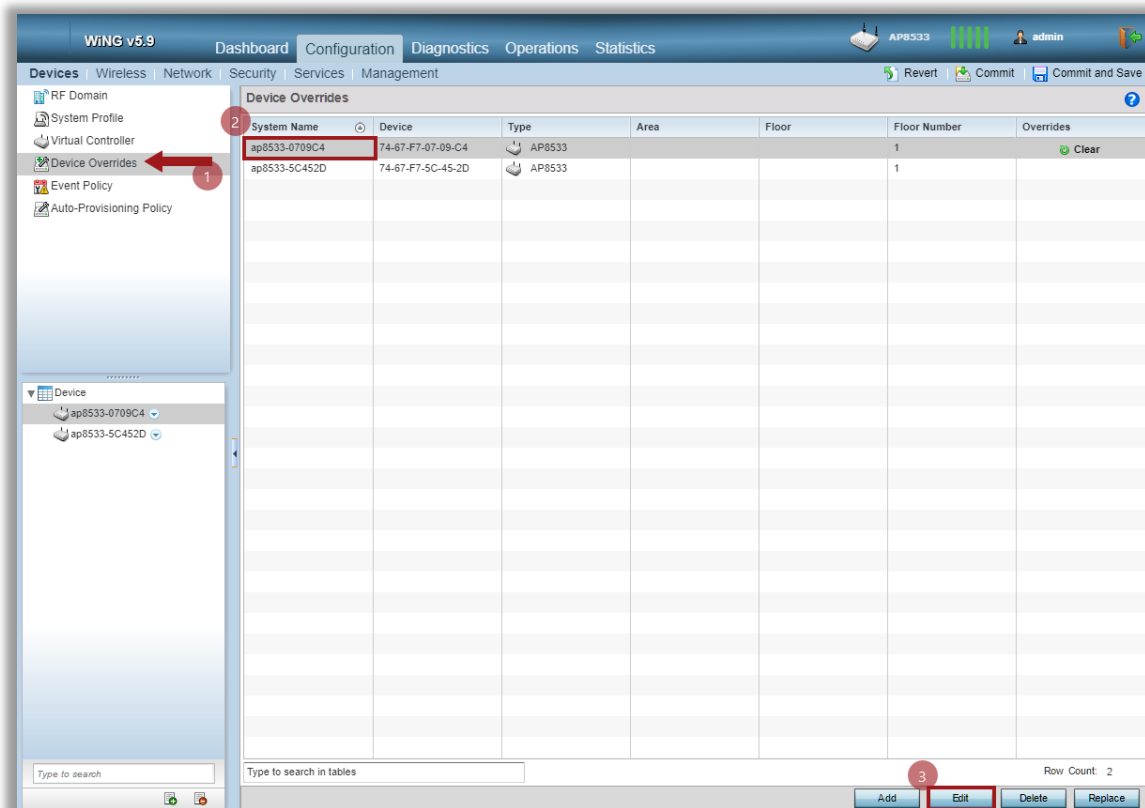
Step 4 – Managing mixed AP environment – Auto Provisioning Policy

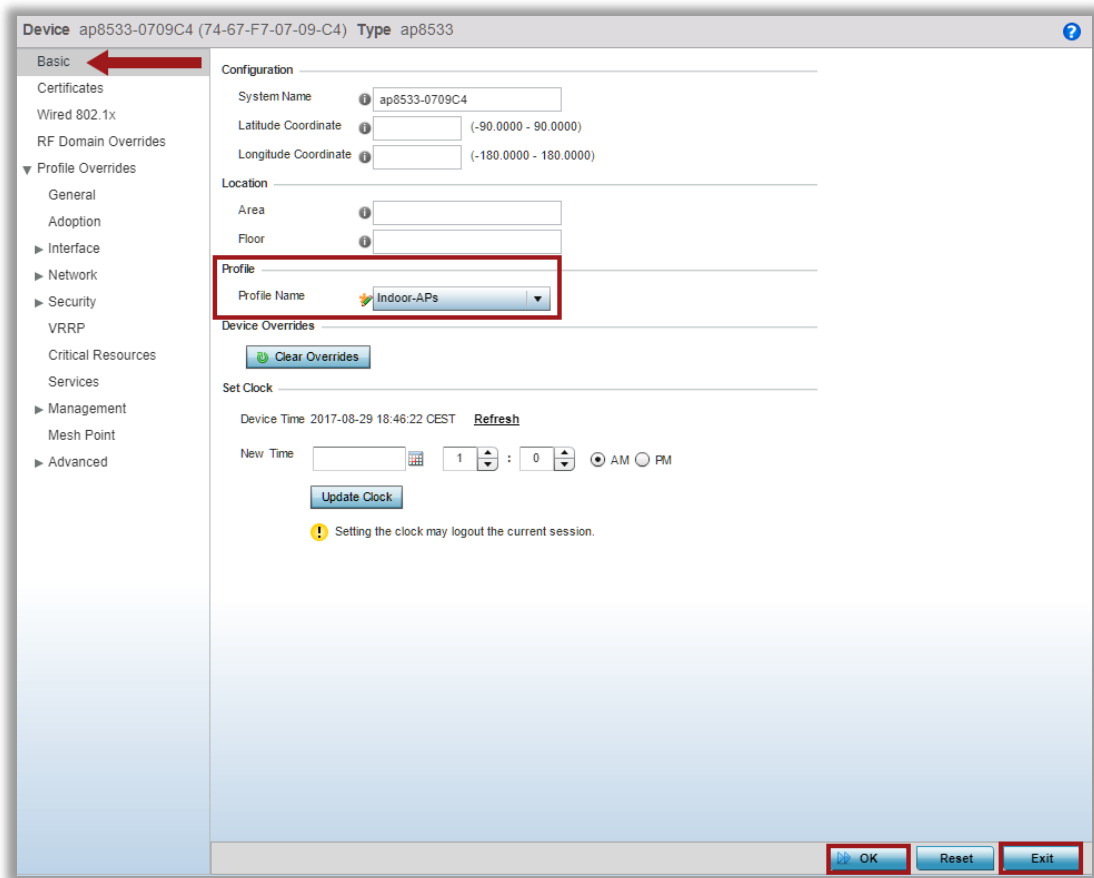
Now that you have created the new AP profile, how you can use it?

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?

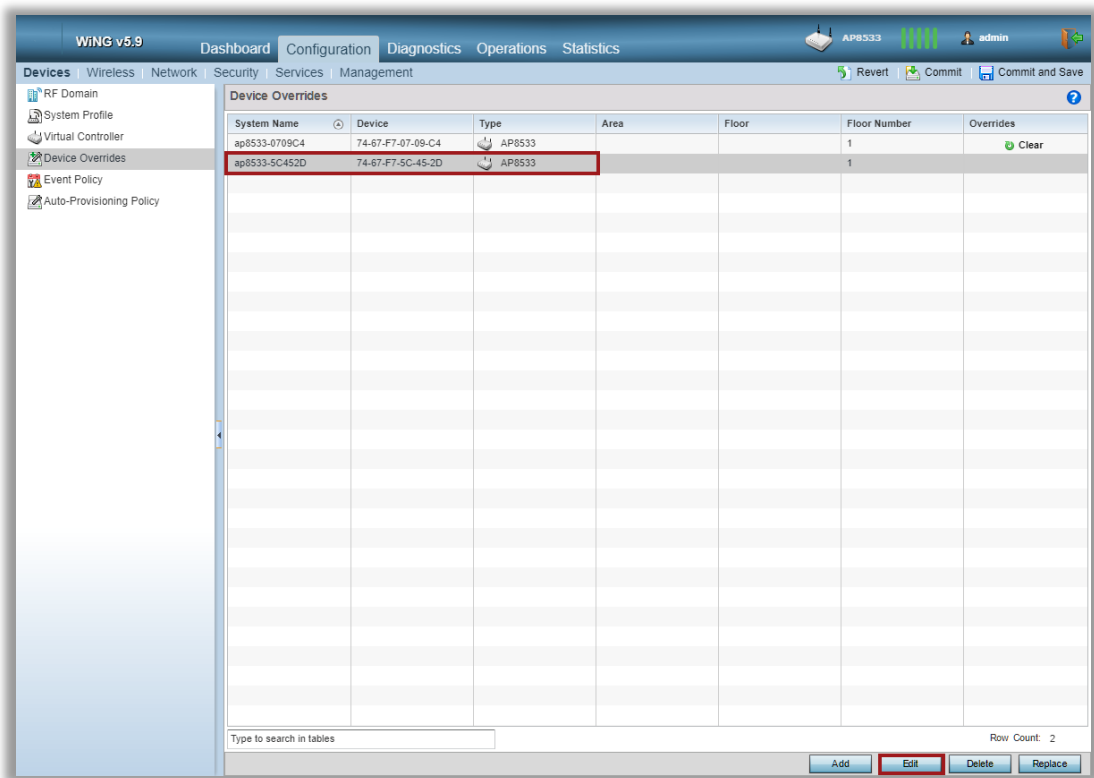


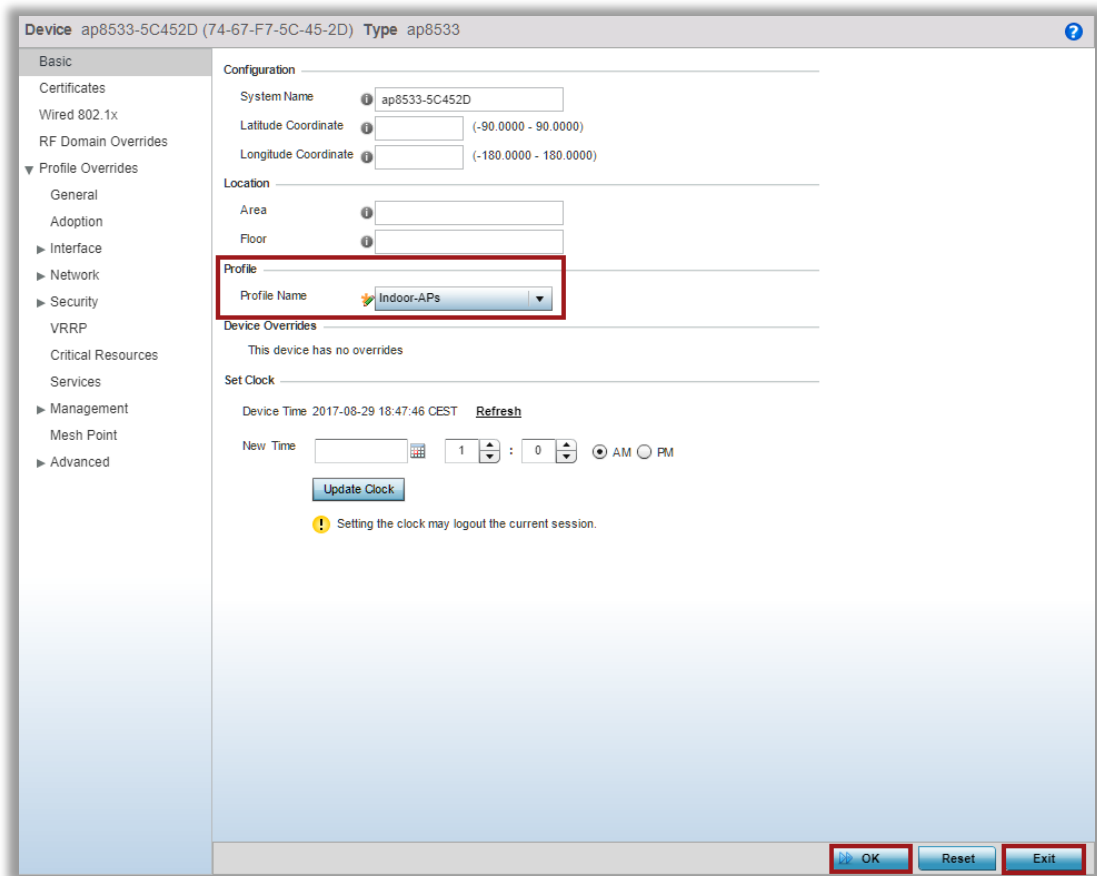
One option is to assign profiles statically under Device Overrides tab. This is what we are going to do with our existing two Access Points:



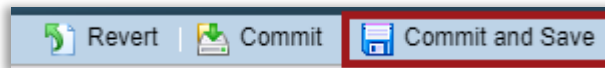


Repeat the same steps for the second Access Point:

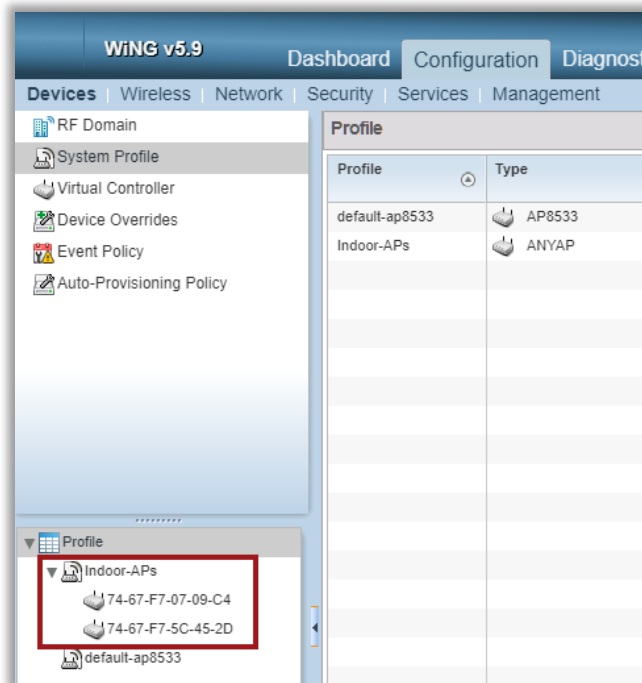




Commit&Save changes:



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



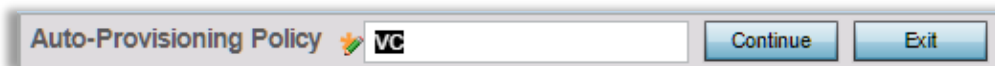
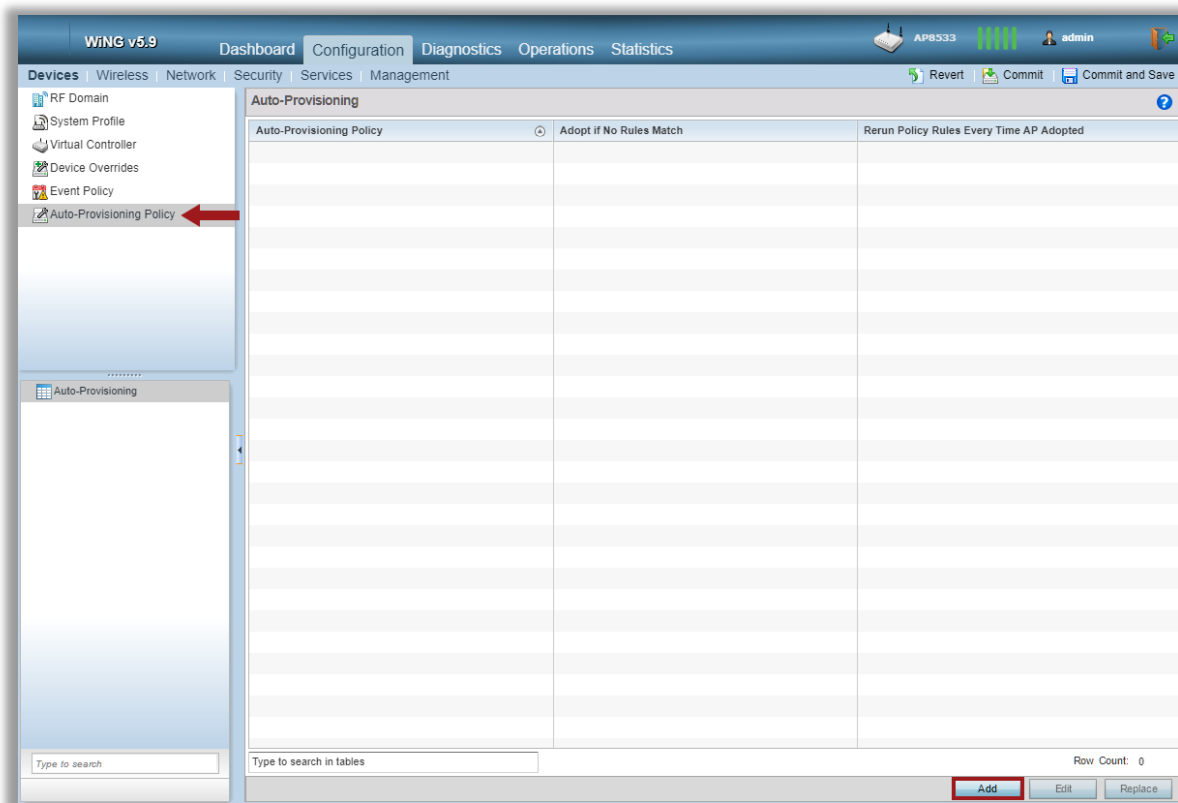
While assigning Profile statically is a viable option, it might take a lot of effort and time when managing dozens of Access Points and is prone to human errors. There is an alternative and recommended solution.

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*:



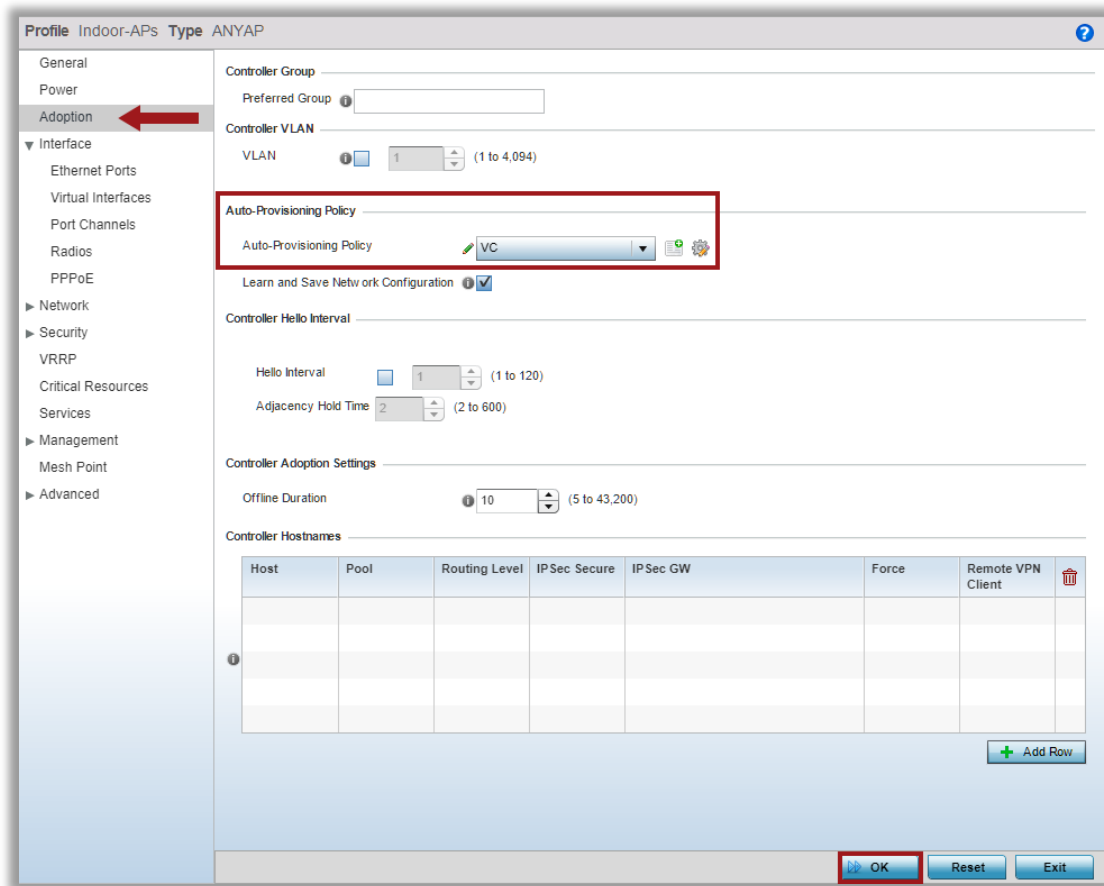
Let's take a look at what all the options above mean:

- 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

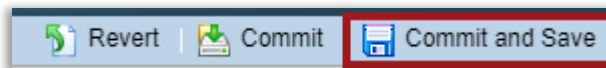
In our example we are going to use “any” match for simplicity.

- 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.

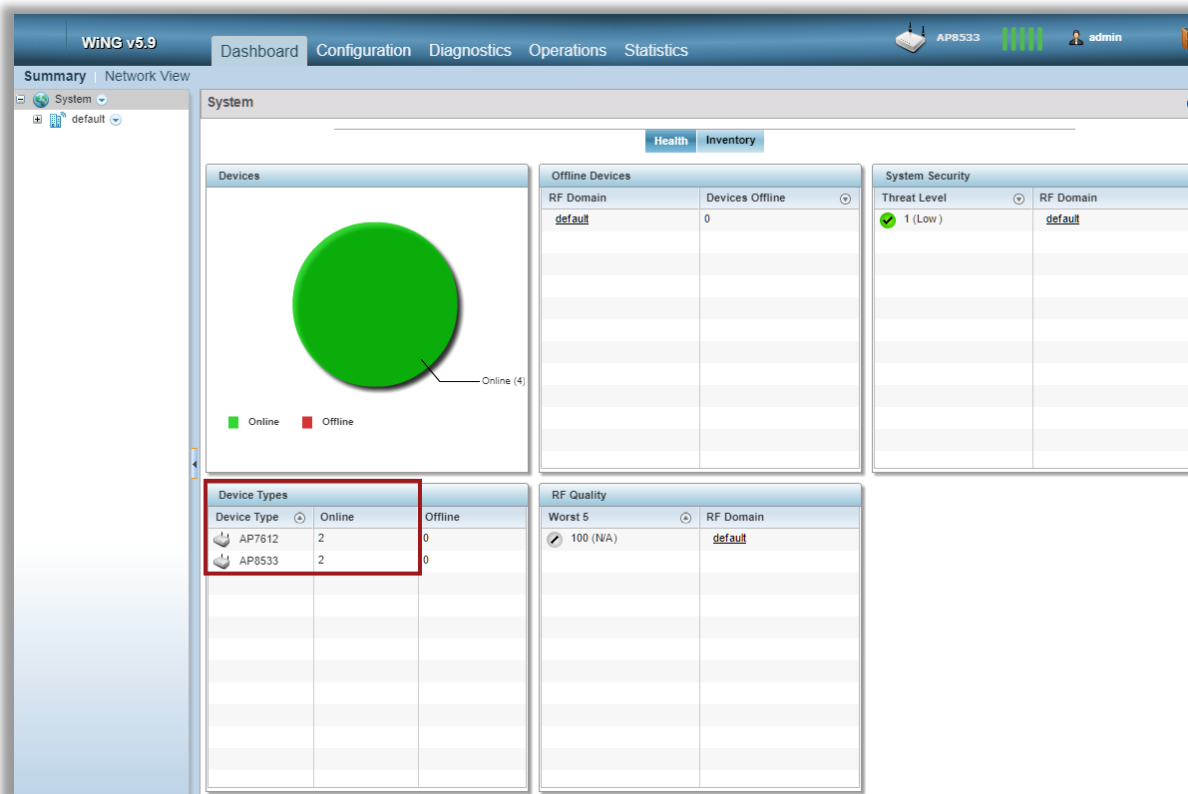
After the Auto-Provisioning rule is created, we will need to assign this policy to the AP profile in order to activate it. Go back to the Indoor-APs profile and move to the Adoption tab:



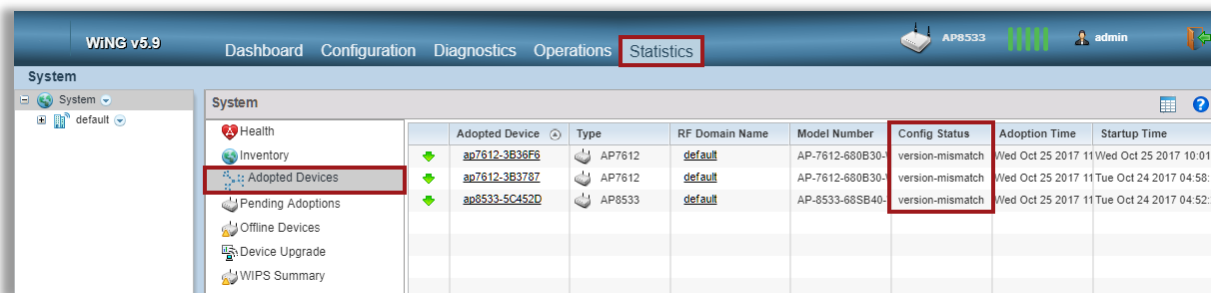
Commit&Save changes:



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



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:



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.

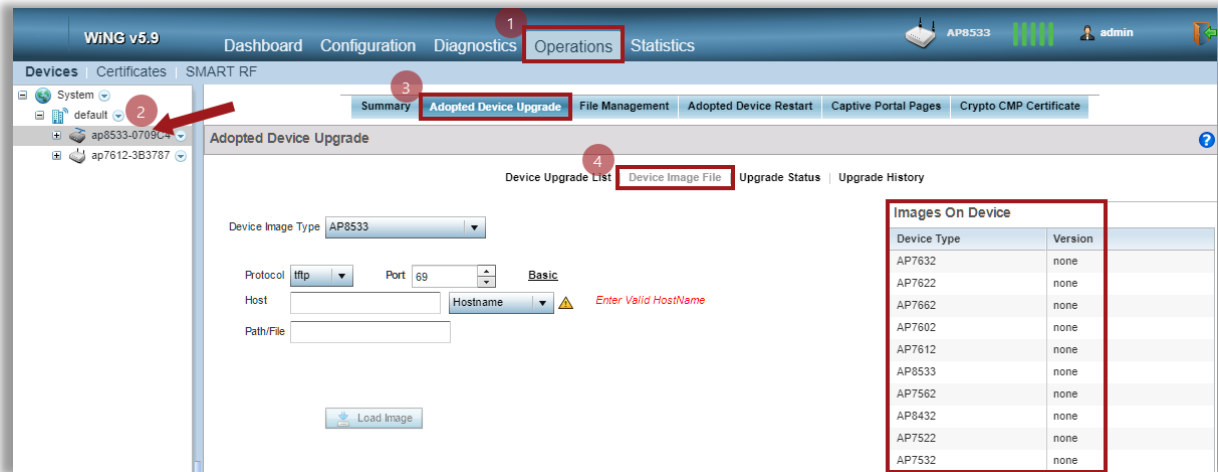
This is done via uploading desired AP image to the Virtual Controller and then initializing AP upgrade procedure.

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.

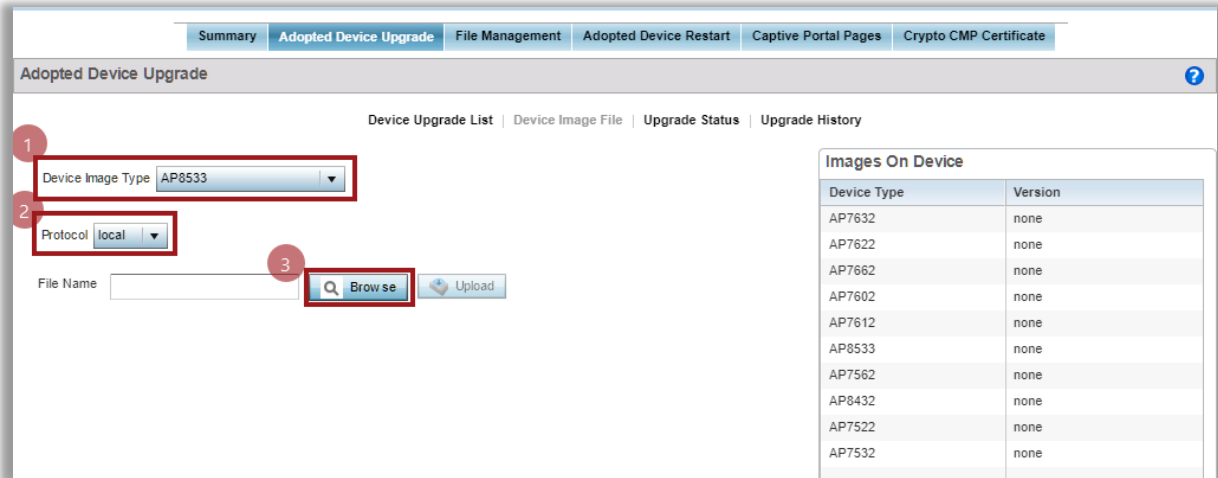
For that reason, by default VC does not have any images stored locally out-of-the-box, so we have to upload them first to allow our VC to upgrade all adopted APs.

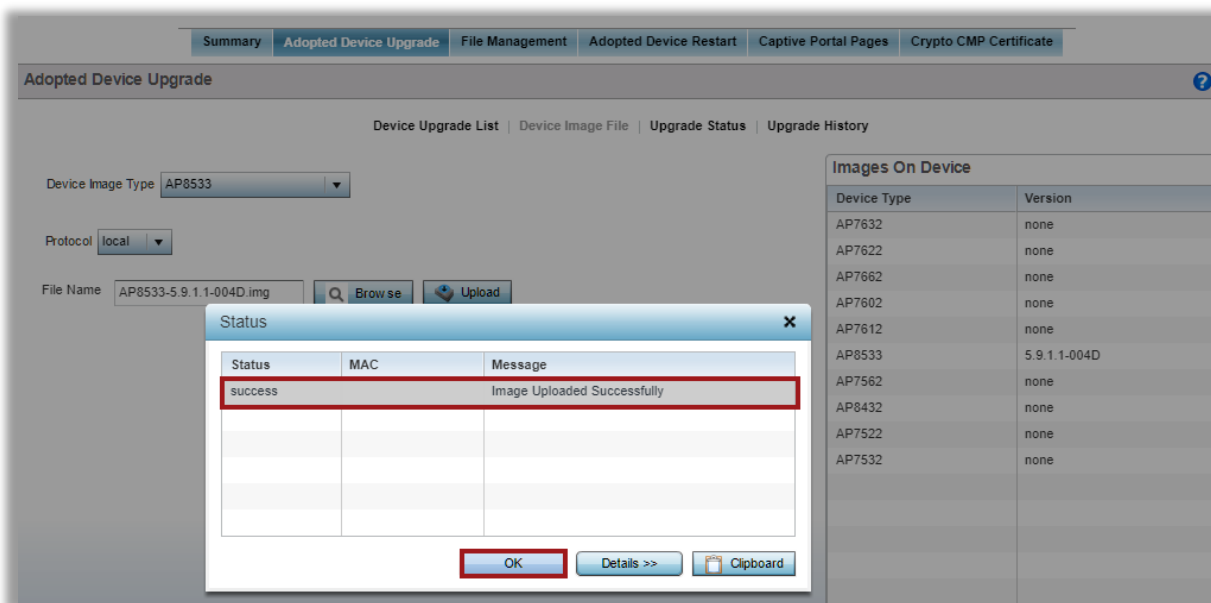
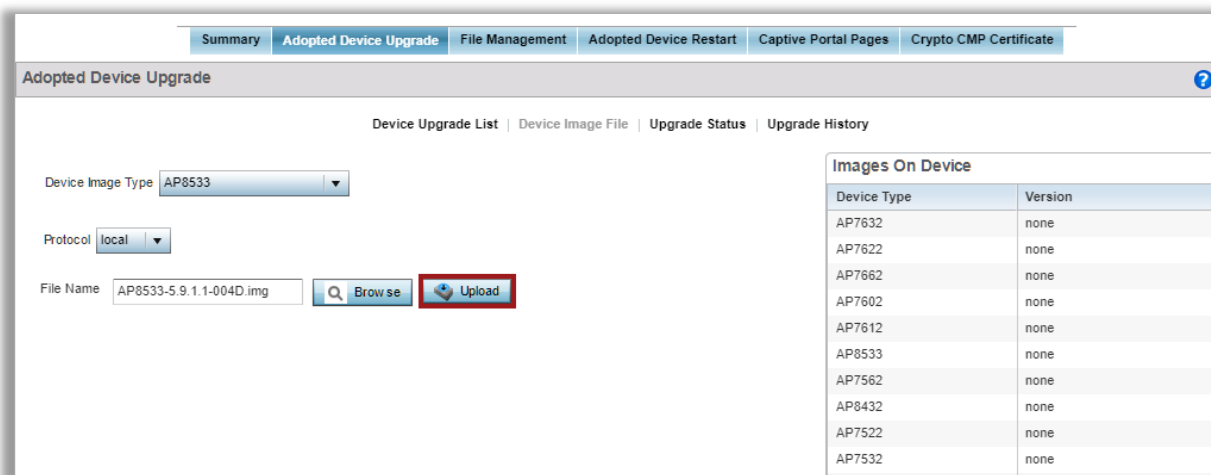
In our example we will need separate images for AP7612 and AP8533s.

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



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





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):



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

The screenshot shows the WiNG v5.9 interface for device management. The 'Device Upgrade' section is active, displaying a list of devices. The table below shows the following data:

Hostnames	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	B6-50-01-3B-37-87	ap7612	5.9.1.0-029R	default

The 'Status' dialog box displays the following information:

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

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
```

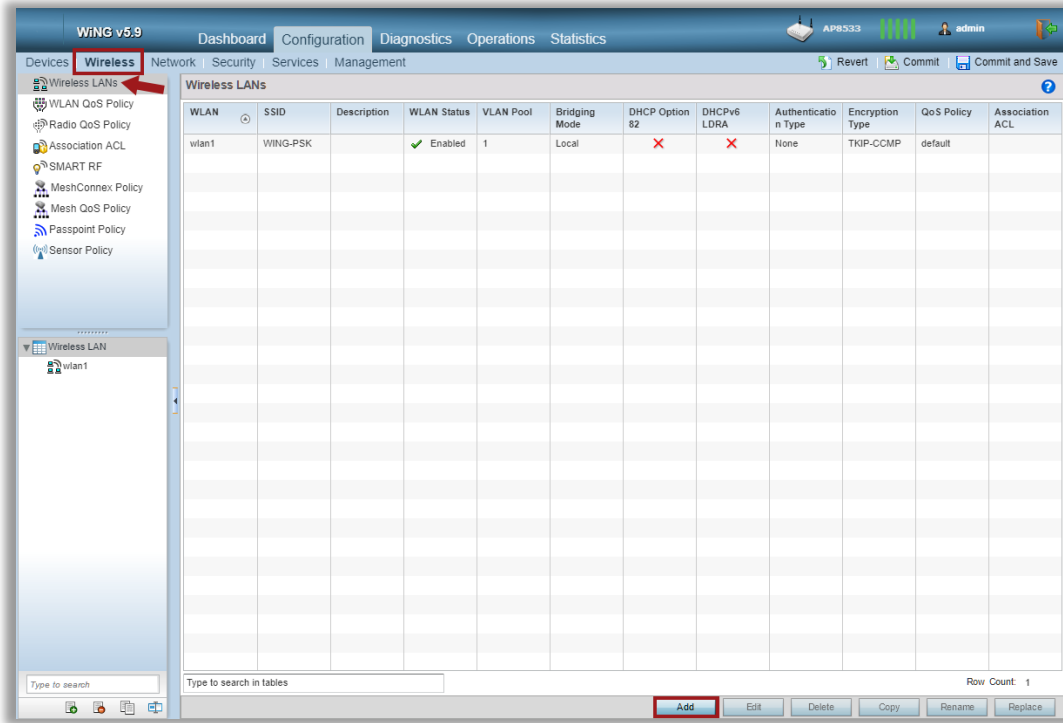
Lastly, assign NSight policy to the RF Domain. Additionally enable nsight sensor to allow NSight advanced troubleshooting tools like AP Test and Spectrum Analysis to work:

```
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
```

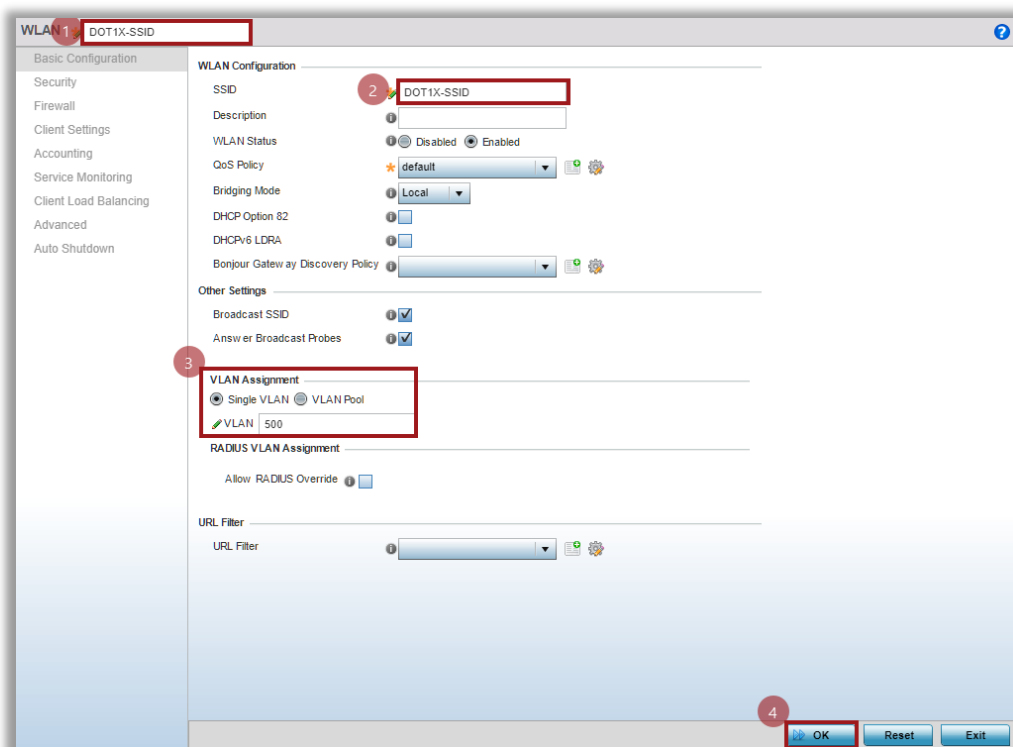
Step 7 – 802.1X SSID with External RADIUS

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:

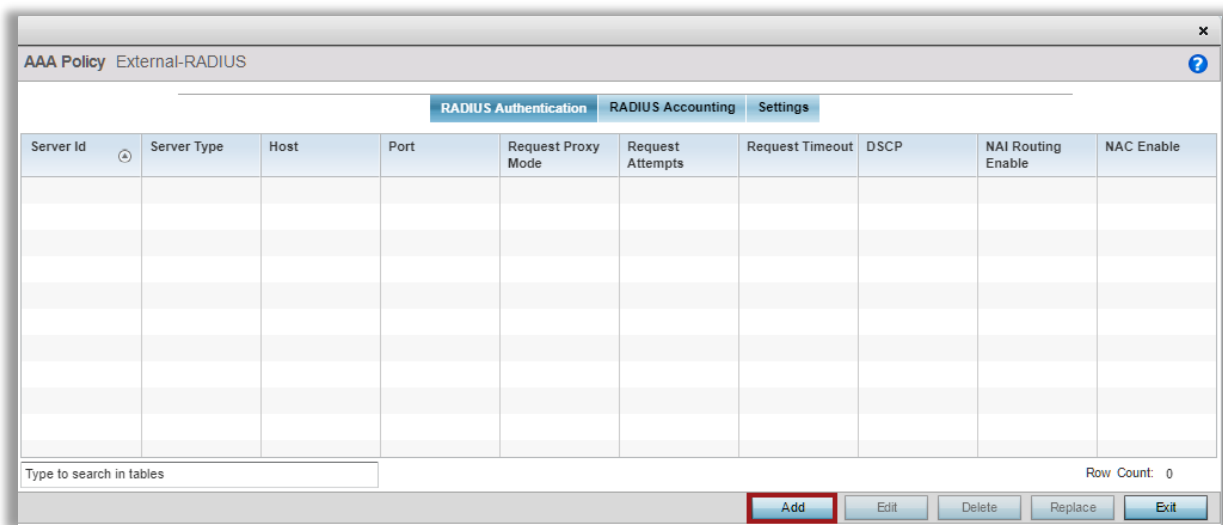
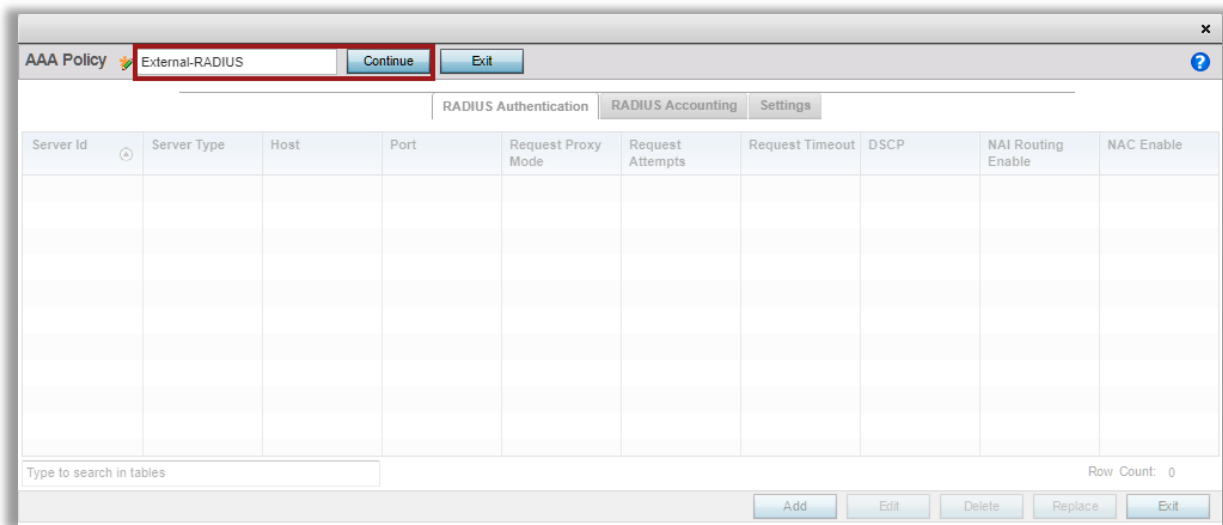
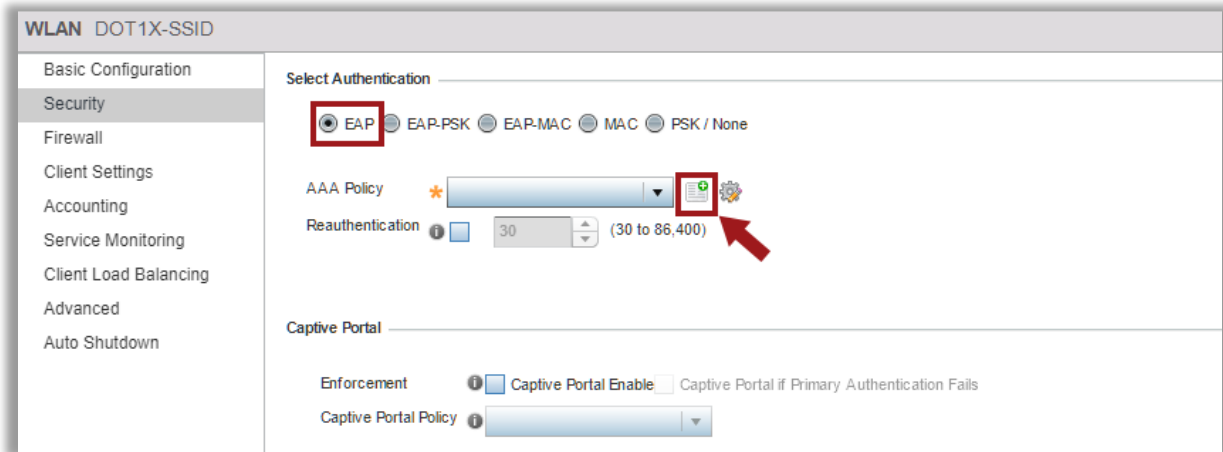
Navigate to **Wireless > Wireless LANs** and create a new WLAN:



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

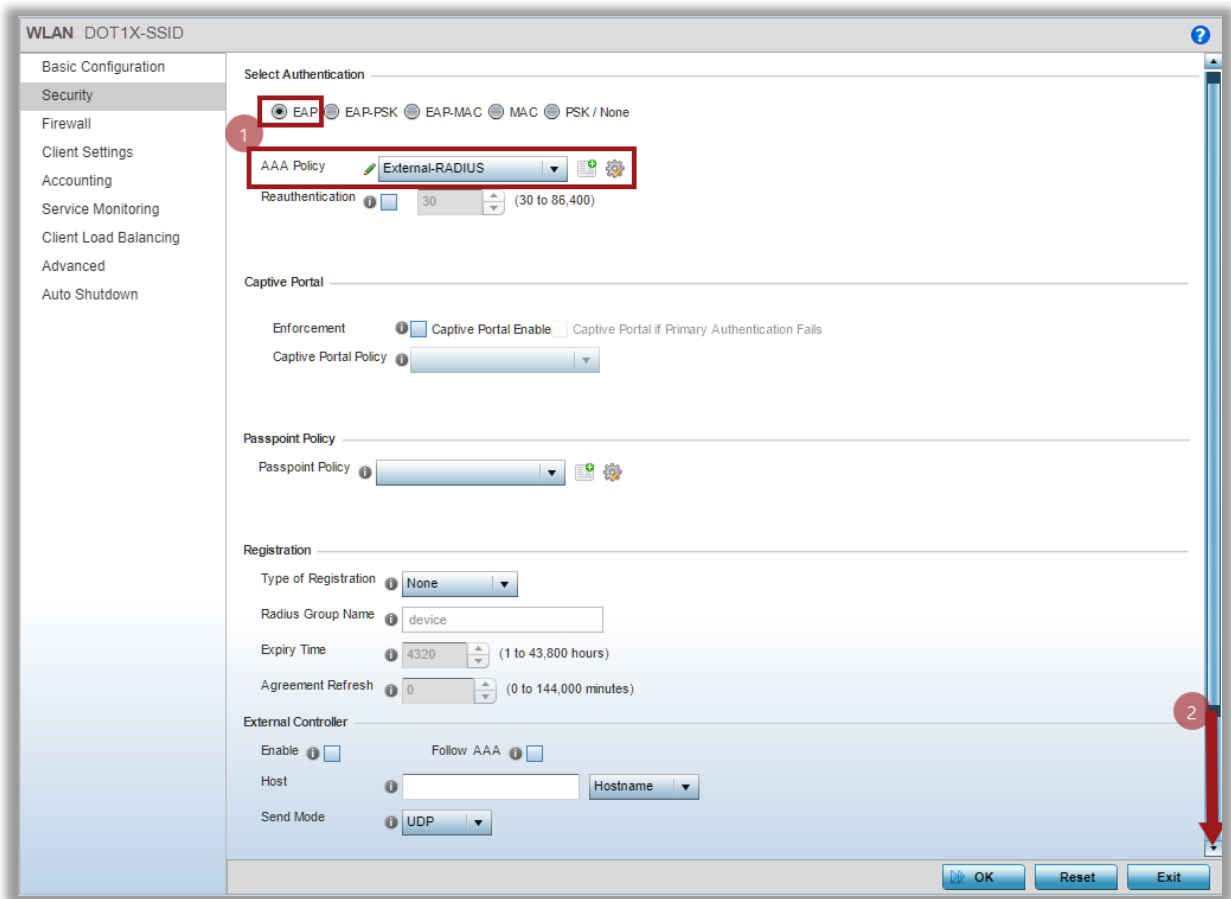


Move to the Security Tab. Enable EAP authentication and create a new AAA Policy that will point to one or more external RADIUS servers:

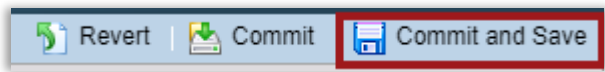
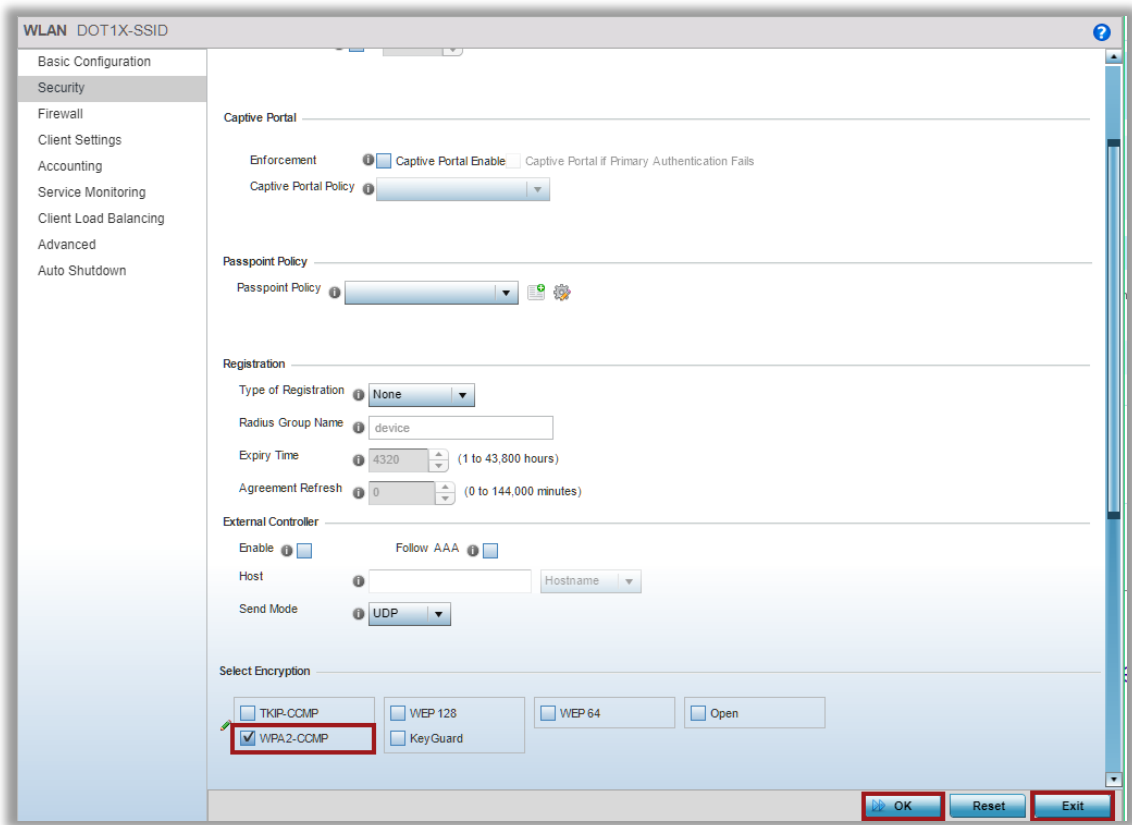


Specify RADIUS Server entry, provide IP address or FQDN of the external RADIUS server, RADIUS Secret and optionally select the proxy mode via RF Domain Manager (in this case RF Domain Manager is the same AP as Virtual Controller):

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

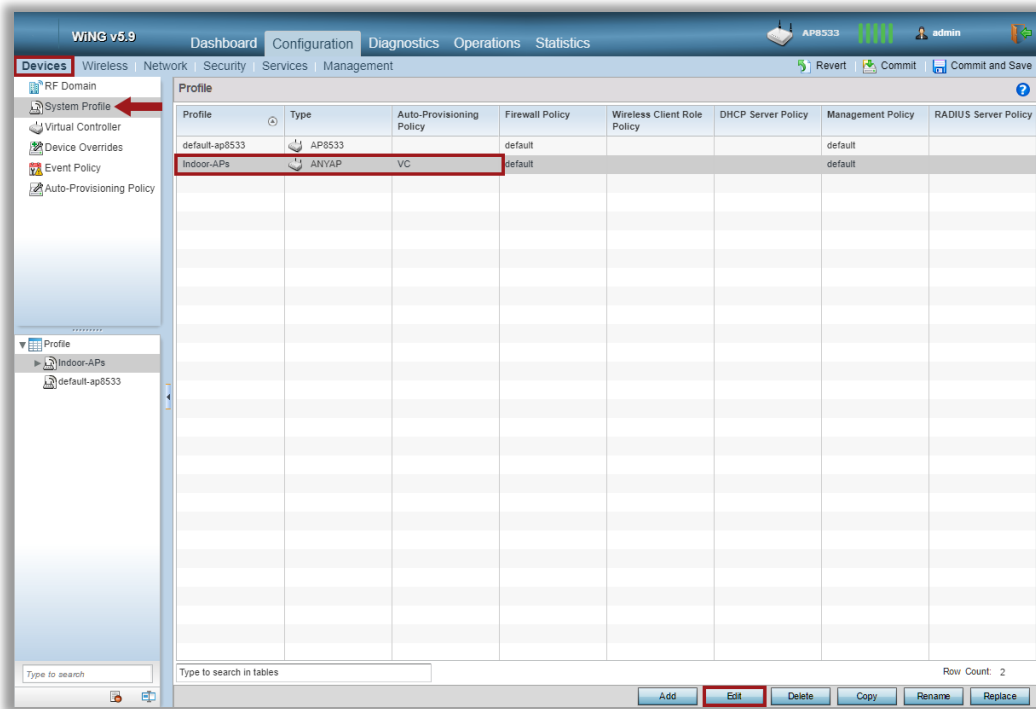


Set encryption ciphers to CCMP, click OK and then Commit&Save changes:

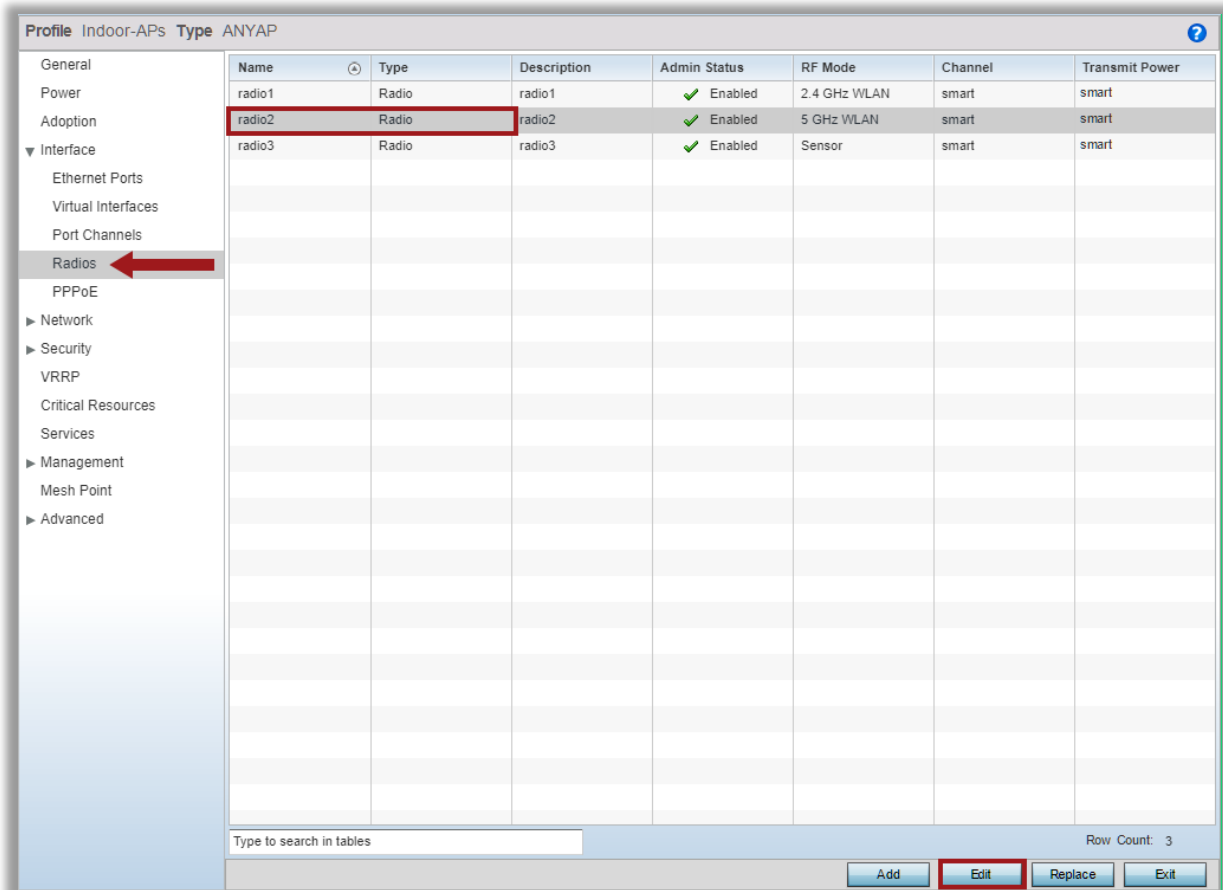


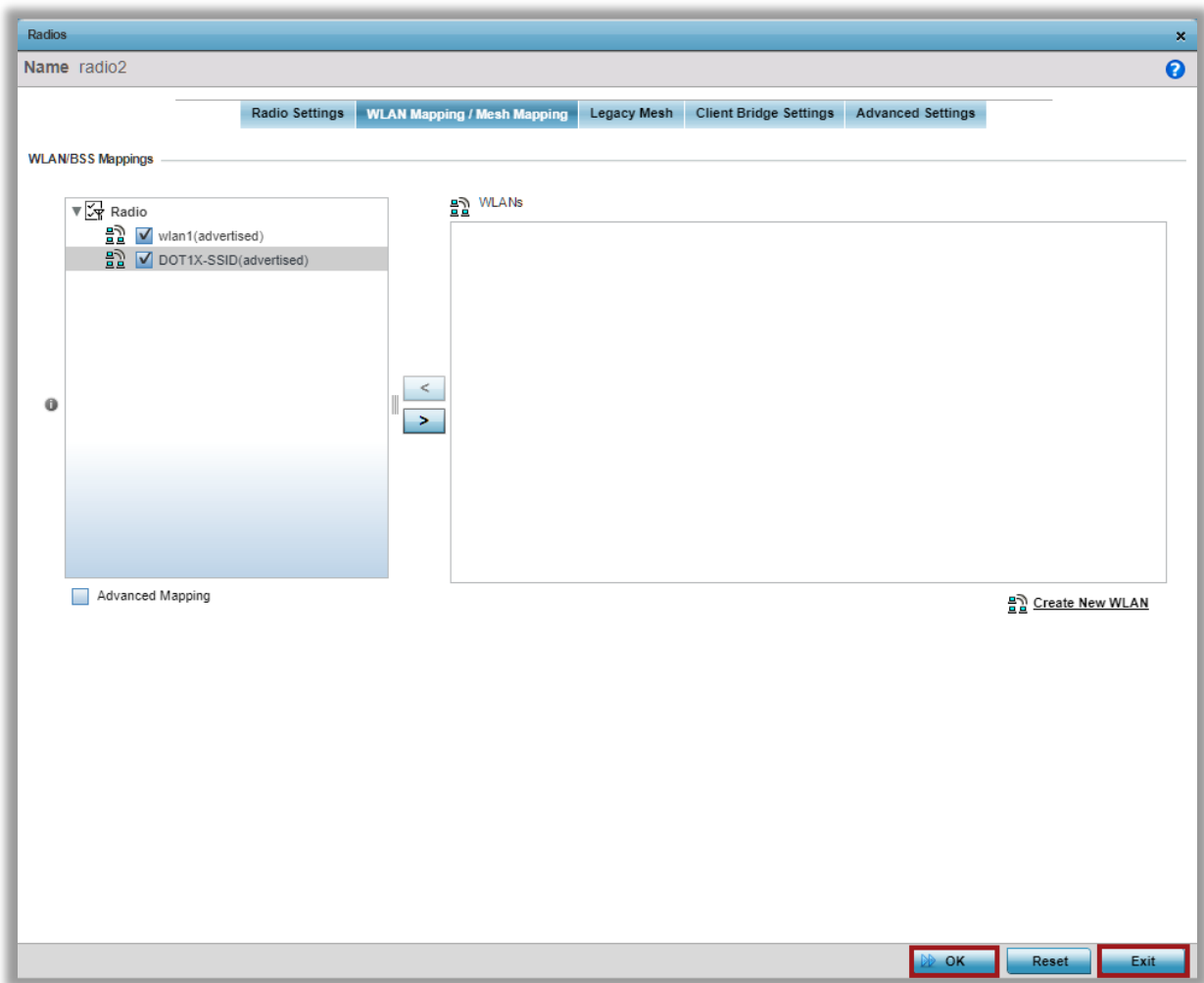
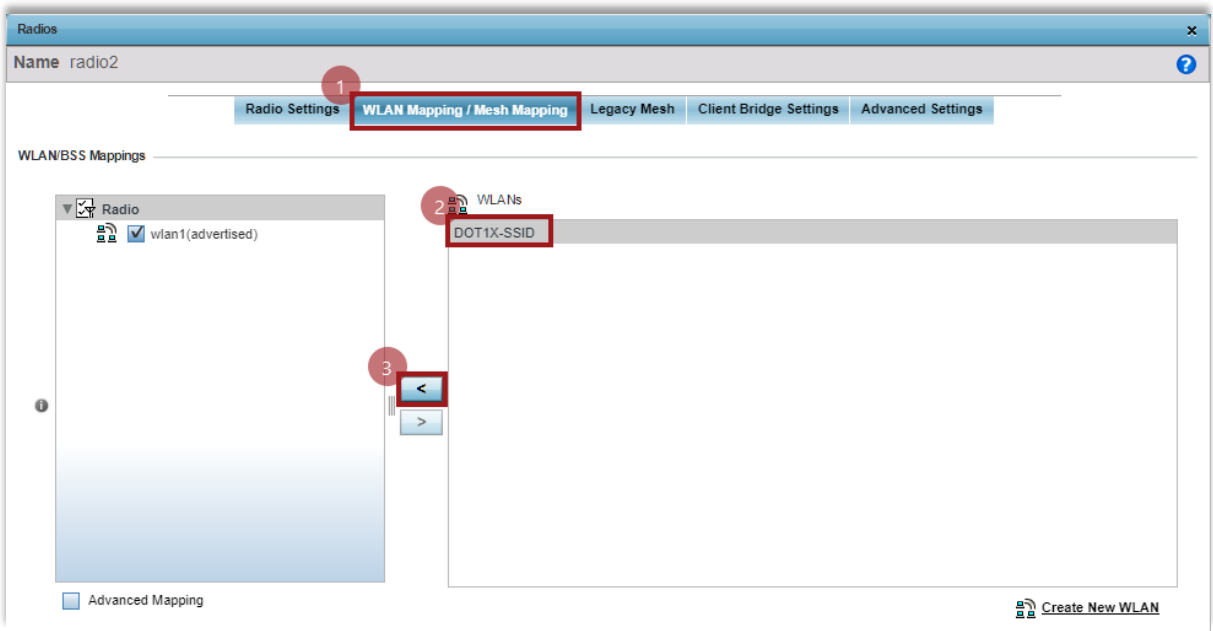
Now go to the AP profile. We will need to assign this Wireless LAN to AP radio interfaces to allow advertizing of this SSID and lastly we will need to allow VLAN 500 on the GE interface of the AP.

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



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:





Move to Ethernet Ports tab and edit ge1 interface settings:

Profile Indoor-APs Type ANYAP

General	Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
Power	fe1	Ethernet		✓ Enabled	Access	1	✗	
Adoption	fe2	Ethernet		✓ Enabled	Access	1	✗	
▼ Interface	fe3	Ethernet		✓ Enabled	Access	1	✗	
Ethernet Ports	fe4	Ethernet		✓ Enabled	Access	1	✗	
Virtual Interfaces	ge1	Ethernet		✓ Enabled	Access	1	✗	
Port Channels	ge2	Ethernet		✓ Enabled	Access	1	✗	
Radios	up1	Ethernet		✓ Enabled	Access	1	✗	
PPPoE								
▶ Network								
▶ Security								
VRRP								
Critical Resources								
Services								
▶ Management								
Mesh Point								
▶ Advanced								

Type to search in tables Row Count: 7

Add Edit Replace Exit

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

Ethernet Ports

Name ge1

Basic Configuration Security Spanning Tree

Properties

Description

Admin Status Disabled Enabled

Speed

Duplex

Switching Mode

Mode Access Trunk

Native VLAN (1 - 4094)

Tag Native VLAN

Allowed VLANs (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

OK Reset Exit

Revert Commit Commit and Save

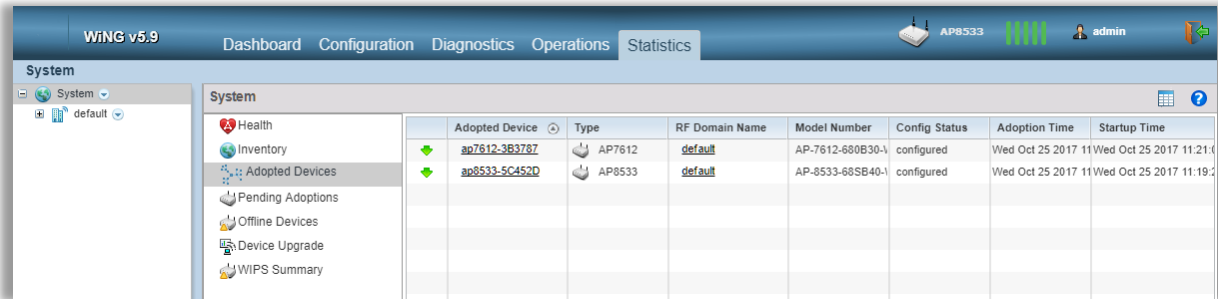
VirtualController – Verification & Monitoring

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:

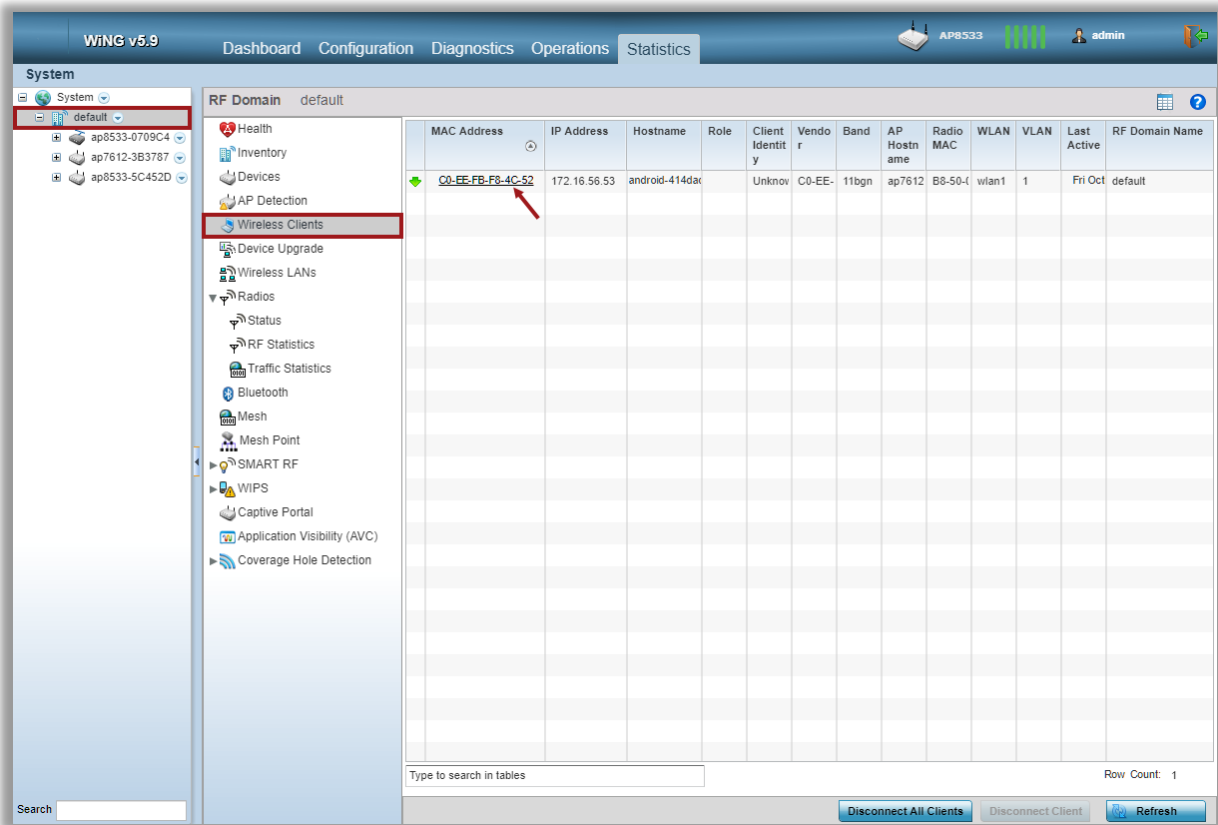
AP Adoption Verification.

Statistics > Adopted Devices



Client Connections:

Statistics > {RF Domain Name} > Wireless Clients:



Statistics Wireless Client C0-EE-FB-F8-4C-52

Health Details Traffic WMM TSPEC Association History Graph

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

Refresh Exit

Statistics Wireless Client C0-EE-FB-F8-4C-52

Health Details Traffic WMM TSPEC Association History Graph

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

Refresh Exit

Radio Status and Statistics:

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

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

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

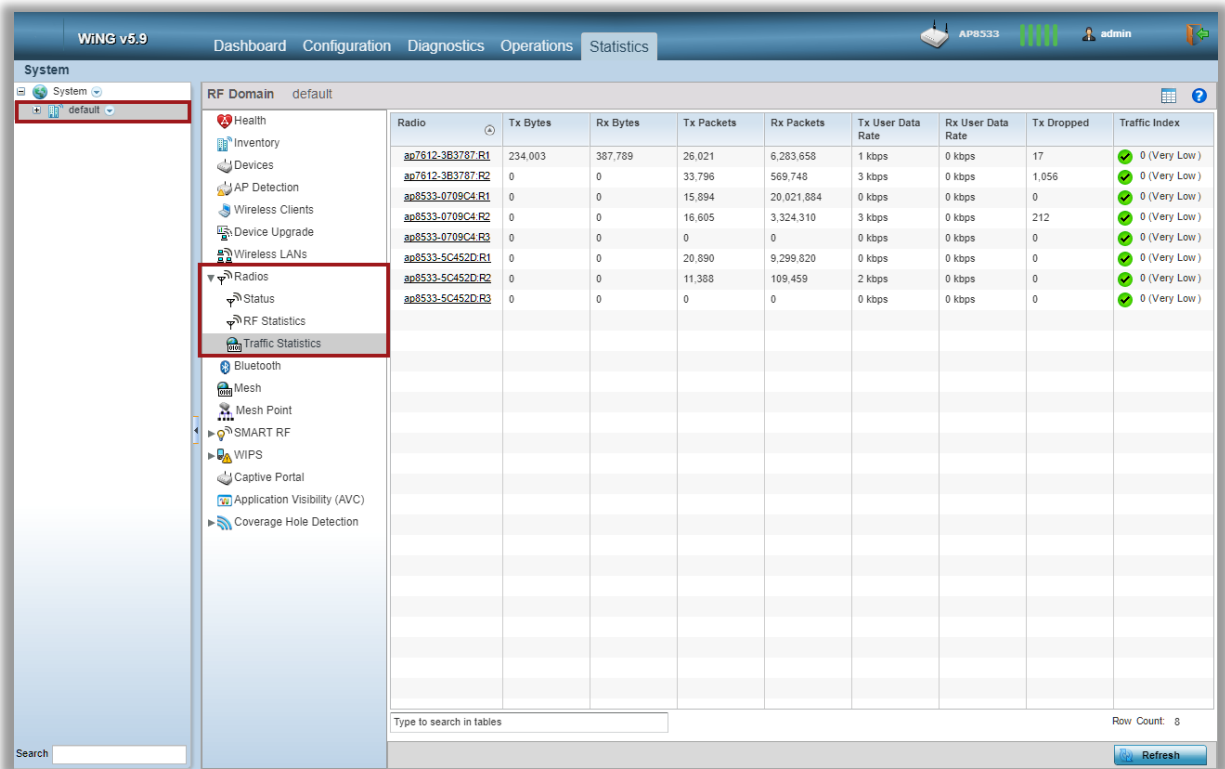
Parameter	Configured	Current
Channel	smt	116w
Power	smt	17

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	Value
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

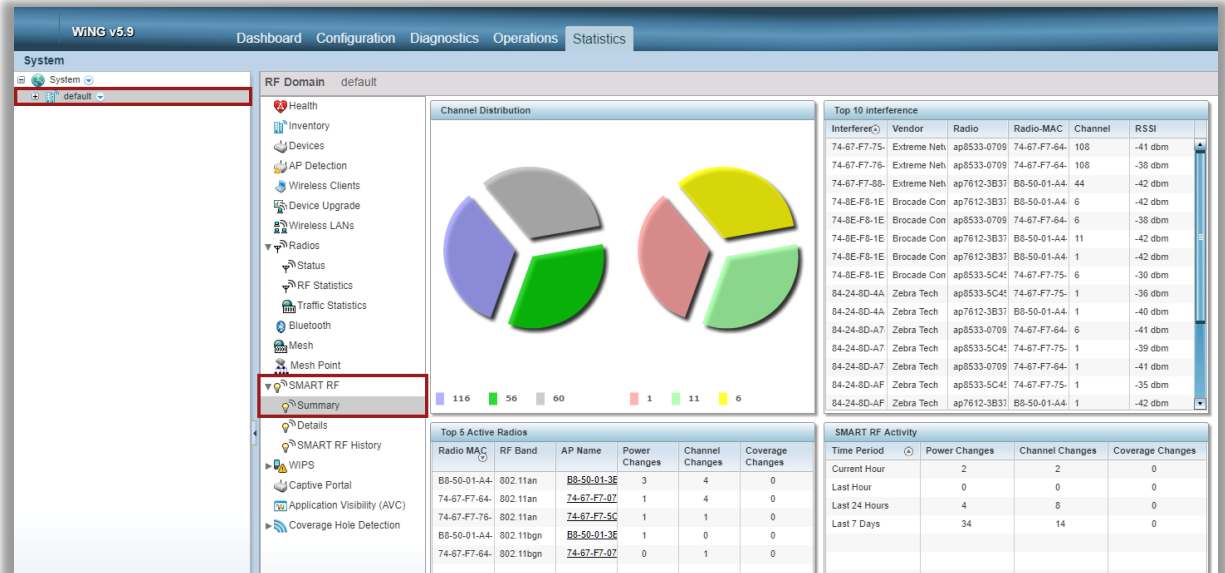
RF Quality Statistics	Value
RF Quality Index	0 (N/A)
Retry Percentage	0
Rx Retries	24,640
SNR (dBm)	0
Signal (dBm)	0
Noise (dBm)	-110
Error Rate (pps)	0
Medium Error Rate (%)	13
MOS Score	0.0
R-Value	0.0

Wireless Clients	Value
Client Count	0
No data to display	
LT Clients	0
HT 20 Clients	0
Long Preamble Clients	0
Long Slot Clients	0



SMART RF Statistics:

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



SmartRF Neighbor radio table:

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

The screenshot shows the WING v5.9 interface with the 'Statistics' tab selected. The left sidebar contains a navigation tree with 'SMART RF' expanded to 'Details'. The main content area features a table of radio statistics:

AP Hostname	Radio MAC Address	Radio Type	State	Channel	Power
ap7512-383787	88-58-01-44-80-40	11gn	normal	6	17
ap9333-5C452D	74-67-F7-76-09-A0	11an	normal	50	17
ap9333-5C452D	74-67-F7-76-27-00	11an	offline	0	0
ap9333-8739C4	74-67-F7-64-05-00	11an	offline	0	0
ap9333-8739C4	74-67-F7-64-80-10	11gn	normal	1	17
ap9333-8739C4	74-67-F7-64-8A-30	11an	normal	56	17
ap9333-5C452D	74-67-F7-75-F3-00	11gn	normal	11	17
ap7512-383787	88-58-01-44-80-90	11an	normal	110a	17

Summary information on the right includes:

- Radio MAC Address: 74-67-F7-76-09-A0
- Radio Index: 1
- Radio Type: 11an
- State: normal
- AP Hostname: ap9333-5C452D
- Channel: 60
- Power: 17

The 'Neighbors' table is currently empty.

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

The screenshot shows the WING v5.9 interface with the 'Statistics' tab selected. The left sidebar contains a navigation tree with 'SMART RF' expanded to 'Details'. The main content area features the same table of radio statistics as the previous screenshot. To the right of the table is an 'Energy Graph' showing dBm levels for various channels.

The Energy Graph displays dBm values for channels 20 through 140. The legend indicates four categories: External (blue), Neighbor (green), Noise (red), and Total (purple). The graph shows that the 'Total' dBm is consistently higher than the other categories across most channels, with values ranging from approximately 100 dBm to 140 dBm.

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 reside 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 support 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 / ExterneManagement 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
27 th October 2017	1.0	Initial release	Slava Dementyev