

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 Turbodrive, 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 Turbodrive 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 <u>www.extremenetworks.com/company/legal/trademarks</u>.

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:
 - o AP8533 / AP8432 full support
 - o AP7522 / AP7532 / AP7562 limited to AP7522/7532/7562
 - o 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.

	Managed Access Points				
VC Type	AP8533	AP8432	AP7522 AP7532 AP7562	AP7602 AP7622	AP7612 AP7632 AP7662
AP8533 AP8432					
AP7632 AP7662	×	×	×	×	Ø
AP7522 AP7532 AP7562	×	×		×	×
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					

Table below provides a similar information in a different format:

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

WiNG v5.9 - Adaptive Networks
Username admin
Password Passed
6/201-2017 Extreme Networks Inc. All Johns meanered
9 2004-2017. Loterne reavoirs, ind. Ai lights reserved.

Please change the defau	ult password
Your system is currently usir is recommended that you ch from unauthorized network a	ng the factory default login credentials. It nange the default password to protect access.
New Password	*****
Retype to Confirm	*****
Apply	Logout



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
Introduction	E Function Highlight
Access Point Settings	Access Point Settings: Virtual Controller AP, Standalone AP, or Dependent AP
🗍 Network Topology	Network Topology: Bridge or Router Operation LAN Configuration
물물 LAN Configuration	Radio Configuration
물물 WAN Configuration	WAN Configuration Wireless I AN Setup
Padio Configuration	Location, Country Code, Time Zone, Date and Time
말 Wireless LAN Setup	Summary and Save/Commit
5 System Information	
Summary and 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.
	All Back Die Next Save/Commit Cancel

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:





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:

Initial Setup Wizard (AP8533)	×
Navigation Panel	Access Point Type
 ✓ Introduction ✓ Access Point Settings ∴ Network Topology B LAN Configuration B WAN Configuration Wireless LAN Setup System Information ∭ Summary and Commit 	 Access Point Type Ortual Controller AP- When more than one access point is deployed, a single access point can function as a futual Controller AP and manage Dependent mode access points. Up to 24 Dependant APs can be connected to a 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. Ortual 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. Ortual Controller AP. Select this option to deploy this access point as an autonomous "fat" access point. Ortopted to Controller - Select this option when you want the AP to adopt to a controller. The AP will discover fat connected controllers automatically. It will also try to discover controllers were as 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 IP manually below. Virtual Controller Management Interface VLAN Virtual Controller Management Interface IP Tot. 16. 56. 254/ 24 What is this? *
	Gancel Save/Commit Cancel

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	LAN Configuration
Navigation Panel ✓ Introduction ✓ Access Point Settings ✓ Network Topology 물료 LAN Configuration ♥ Radio Configuration ■ Wireless LAN Setup Image: System Information ■ Summary and Commit	LAN Configuration Bease configure interface settings for LAN (VLAN 1) which will be used by wireless clients
	Image: Save/Commit Cancel

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

Initial Setup Wizard (AP8533)	×
Navigation Panel	Radio Configuration
Navigation Panel ✓ Introduction ✓ Access Point Settings ✓ Network Topology ✓ LAN Configuration ⑦ Radio Configuration ⑧ Wireless LAN Setup ⑧ System Information ⑨ Summary and Commit	Radio Configuration
	del Back De Next Save/Commit Cancel

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

Initial Setup Wizard (AP8533)	x
Navigation Panel	Wireless LAN Setup
 Introduction Access Point Settings Network Topology LAN Configuration Radio Configuration Wireless LAN Setup System Information Summary and Commit 	WLAN 1 WLAN 2 Image: Configuration Image: Configuration Image: Configuration Image
	44 Back Next Save/Commit Cancel

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*:

Initial Setup Wizard (AP8533)	×
Navigation Panel	System Information
 Introduction Access Point Settings Network Topology 	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.
 LAN Configuration Radio Configuration Wireless LAN Setup System Information Summary and Commit 	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:

Initial Setup Wizard (AP8533)		×
Navigation Panel	Summary and Commit	
 Introduction Access Point Settings Network Topology 	Access Point Settings Page	ndent AP
 LAN Configuration Radio Configuration Wireless LAN Setup 	Network Topology Page — Network Topology Bridge M	ode
System Information Summary and Commit	불물 LAN Configuration Page — LAN Configuration Type VLAN ID for the LAN Interface	Use DHCP 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
		H Back De Next Save/Commit Cancel

figuration 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 Running Config Adopted APs Guest User Infiguration of AP8533 version 5.9.1.1-004D Ion 2.5 Iti-Identity-group default I default-Ingerprints Incess-list BROADCAST-MULTICAST-CONTROL Intit cp any any rule-precedence 10 rule-description "permit all TCP traffic" Intit up any eq 67 any eq dhopc rule-precedence 11 rule-description "fermit DHCP replies" I yu dany range 137 138 any rule-precedence 21 rule-description "deny Vindows netbios" I yin any bed 52 552 555 555 555 555 555 555 555 555	×
Running Config Adopted APs Guest User Infiguration of AP8533 version 5.9.1.1-004D ion 2.5 It-identity-group default 1 default-Ingerprints :ccess-list BROADCAST-MULTICAST-CONTROL mit top any any rule-precedence 10 rule-description "permit AIT CP traffic" mit udp any eq 67 any eq dhopc rule-precedence 11 rule-description "demy windows netbios" y udp any range 137 138 any range 137 138 any range 137 138 any rule-precedence 21 rule-description "demy Vindows netbios" y in any best 25 25 25 25 25 25 100 rule-precedence 21 rule-description "demy P multicast"	d only if the device is configured as controller else will be empty
Running Config Adopted APs Guest User	
nfiguration of AP8533 version 5.9.1.1-004D ion 2.5 it-identity-group default 1 default-Ingerprints :cess-list BROADCAST-MULTICAST-CONTROL mit top any any rule-precedence 10 rule-description "permit all TCP traffic" mit udp any eq 67 any eq 0thopc rule-precedence 11 rule-description "permit DHCP replies" y udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios" y in any bary 224.0.0.04 rule-precedence 21 rule-description "deny IP multicast"	
Infiguration of AP8533 version 5.9.1.1-004D ion 2.5 it-identity-group default 1 default-Ingerprints ccess-list BROADCAST-MULTICAST-CONTROL mit top any any rule-precedence 10 rule-description "permit all TCP traffic" mit udp any eq 67 any eq 0thopc rule-precedence 11 rule-description "permit DHCP replies" y udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios" y in any bary 224.0.0.04 rule-precedence 21 rule-description "deny IP multicast"	
ion 2.5 it-identity-group default id default-fingerprints ::cess-list BROADCAST-MULTICAST-CONTROL mit top any any rule-precedence 10 rule-description "permit all TCP traffic" mit udp any eq 67 any eq dhopc rule-precedence 11 rule-description "germit DHCP replies" y udp any range 137 138 any rule-precedence 20 rule-description "deny windows netbios" y lp any 224.0.0.04 rule-precedence 21 rule-description "deny IP multicast" y lp any 224.0.0.04 rule-precedence 21 rule-description "deny IP multicast"	
ion 2.5 it-identity-group default default-fingerprints ccess-list BROADCAST-MULTICAST-CONTROL mit top any any rule-precedence 10 rule-description "permit all TCP traffic" mit up any eq 67 any eq dhopc rule-precedence 11 rule-description "germit DHCP replies" y up any rgel 317 133 any rule-precedence 20 rule-description "deny windows netbios" y in any bas 252 552 555 555 rule-precedence 21 rule-description "deny IP multicast"	
nt-identity-group default 1 default-fingerprints xcess-list BROADCAST-MULTICAST-CONTROL mit top any any rule-precedence 10 rule-description "permit all TCP traffic" mit udp any eq 67 any eq dhopc rule-precedence 11 rule-description "permit DHCP replies" y udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios" y ip any 224.0.0.04 rule-precedence 21 rule-description "deny IP multicast" y in any bas 255 255 255 255 255 255 255 255 255 25	
nt-identily-group default d default-fingerprints :cess-list BROADCAST-MULTICAST-CONTROL mit top any any rule-precedence 10 rule-description "permit all TCP traffic" mit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies" y udp any range 137 138 mito-precedence 20 rule-description "deny Windows netbios" y ip any 224.0.0.04 rule-precedence 21 rule-description "deny IP multicast" y in any bas 25 52 55 55 55 55 55 55 55 55 55 55 55	
In-deminy-group derainin default-lingreprints :cess-list BROADCAST-MULTICAST-CONTROL mit top any any rule-precedence 10 rule-description "permit all TCP traffic" mit udp any eq 67 any eq dhopc rule-precedence 11 rule-description "germit DHCP replies" y udp any range 137 138 any rule-precedence 20 rule-description "deny windows netbios" y ip any 224.0.0.04 rule-precedence 21 rule-description "deny IP multicast" y in any bas 25 52 552 555 255 255 255 255 255 255	
ccess-list BROADCAST-MULTICAST-CONTROL mil top any any rule-precedence 10 rule-description "permit all TCP traffic" mil udp any eq 67 any eq dhopc rule-precedence 11 rule-description "permit DHCP replies" y udp any range 137 133 any runge 137 133 any rule-precedence 20 rule-description "deny windows netbios" y ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast" y in any bat 255 255 255 255 255 255 255 255 255	
ccess-list BROADCAST-MULTICAST-CONTROL mill top any any rule-precedence 10 rule-description "permit all TCP traffic" mill udp any eq 67 any eq dhopc rule-precedence 11 rule-description "permit DHCP replies" y udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios" y ip any 224.0.0.04 rule-precedence 21 rule-description "deny IP multicast" y in any bast 255 255 255 255 255 255 255 255 255	
mit top any any rule-precedence 10 rule-description "permit all TCP traffic" mit udp any eq 67 any eq dhopc rule-precedence 11 rule-description "permit DHCP replies" y udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios" y ip any 224.0.0.04 rule-precedence 21 rule-description "deny IP multicast" y in any bast 255 255 255 555 rule-precedence 22 nule-description "deny IP nondecast"	
mit uop any eq o', any eq oncjc ruie-precedence i i ruie-oescription permit UHCP replies y ud any range 137 138 any range 137 138 any ruie-precedence 20 ruie-description "deny windows netbios" y i pany 224.0.0.04 ruie-precedence 21 ruie-description "deny IP multicast" y i pany bat 255 255 255 255 ruie-precedence 22 nuie-description "deny IP local broadcast"	
y ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast" vi pa ny 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"	
v in any host 255 255 255 255 rule-precedence 22 rule-description "deny IP local broadcast"	
mit 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:

WiNG v5.9	Dashboard C	onfiguration Dia	gnostics Operati	ions Statistics			533 A	admin 💦
Devices Wireless Net	work Security Ser	vices Managemen	t			5 1 F	Revert 🛛 📥 Commit	🕞 Commit and Save
🔐 RF Domain	Profile							0
System Profile	Profile	Type	Auto-Provisioning	Eirewall Policy	Wireless Client Role	DHCP Server Policy	Management Policy	RADIUS Server Policy
🧼 Virtual Controller		1360	Policy	· nonun · onoy	Policy	billor borrorronoy	management r eney	in the control in only
Device Overrides	default-ap8533	🧅 AP8533		default			default	
5 Event Policy								

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):

WING v5.9	Dashboard		onfiguration [)iagnostics Opera	tions Statistics	_		8533 2	admin	Þ
Devices Wireless Netw	ork Security	Serv	vices Managerr	ient			51	Revert 🛃 Commit	Commi	t and Save
RF Domain	Profile									0
Virtual Controller	Profile	۲	Туре	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	DHCP Server Policy	Management Policy	RADIUS Se	rver Policy
Device Overrides	default-ap8533		🧅 AP8533		default			default		
Event Policy										
Auto-Provisioning Policy										
Drofilo										
▼ Ddefault-ap8533										
74-67-F7-07-09-C4										
4-67-F7-5C-45-2D	1									
Type to search	Type to search in	tables			6				Row Cou	nt: 1
b					-	Add	Edit Delete	Copy F	lename	Replace

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*:

rofile 1 / Indoor-APs	Туре	💅 ANYAP	•								(
General	Virtual Controller										
Power											
Adoption	Virtual Controller										
Wired 802.1x	Set as Virtual 0	Controller AP	0								
Interface	2 Enable Auto Ele	ection of VC	1	\checkmark							
Ethernet Ports	Auto Provisioning	Rule									
Virtual Interfaces	Adopt Unknow	n APs Autom	atically 🚯	🖌 🕛 (Applicabl	e only if AP i	configured	l as Virtual C	ontroller)			
Port Channels											
Radios	Management Inter	ace of Auto-I	Elected Virt	ual Controller							
PPPoE	3 IP Address of Au	to-elected VC	/	172, 16, 56,	254/ 24	-					
Bluetooth	Reachable VLAN		01	(1 to 4,09	14)	-					
Network	Network Time Protoc	ol (NTP)	•	 ♥) * ·							
Security	Server IP	Key	Key	Preferred	Autokey	Version	Minimum	Maximum			
VRRP		Number					Polling	Polling	Ŵ		
Critical Resources	1 time nist gov	1	******	** ¥	×	0	64	1024	命		
Services			-	~	~	-					
Management											
Mesh Point								+ Add	Row		
Advanced	RF Domain Manager										
	Capable		0 🗸								
	Priority		0	1 (1 to	255)						

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

General	Name	Ty	pe	Description	Admin	Status	RF Mode	Channel	Transmit Power
Power	radio1	Ra	dio	radio1	~	Enabled	2.4 GHz WLAN	smart	smart
Adoption	radio2	Ra	idio	radio2	 ✓ 	Enabled	5 GHz WLAN	smart	smart
Interface	radio3	Ra	idio	radio3	~	Enabled	Sensor	smart	smart
Ethernet Ports									
Virtual Interfaces									
Port Channels									
Radios									
PPPoE	_								
Network									
Security									
VRRP									
Critical Resources									
Services									
Management									
Mesh Point									
Advanced									

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						0
-	Radio Settings	WLAN Mapping / Mesh Mapping	Legacy Mesh	Client Bridge Settings	Advanced Settings	
WLAN/BSS Mappings						
C Radio		WLANS Wian1				
Advanced Mappi	ng					B Create New WLAN

		Radio Settings	WLAN Mapping / Mesh N	lapping Legacy Mesh	Client Bridge Settings	Advanced Settings	
WLAN	l/BSS Mappings						
	Radio		B WLANS	1			
0	<u>∎</u> wian1(adv	ertised)	× •				
	Advanced Mapping						B Create New WLAN
						1	2
						№ ок	Reset Exit

Profile Indoor-APs Type	ANYAP								6
General	Name	۲	Туре	Description	Admir	n Status	RF Mode	Channel	Transmit Power
Power	radio1		Radio	radio1	~	Enabled	2.4 GHz WLAN	smart	smart
Adoption	radio2		Radio	radio2	~	Enabled	5 GHz WLAN	smart	smart
▼ Interface	radio3		Radio	radio3	~	Enabled	Sensor	smart	smart
Ethernet Ports									
Virtual Interfaces									
Port Channels									
Radios									
PPPoE									
Network									
 Security 									
VRRP									
Critical Resources									
Services									
 Management 									
Mesh Point									
Advanced									
	Tractore	in Antol	-						Bau Countri - C
	Type to search	in tables	\$						Row Count: 3
							Add	Edit	Replace Exit

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

Radios	i							×
Name	adio2							0
		Radio Settings	WLAN Mappir	g / Mesh Mapping	Legacy Mesh	Client Bridge Settings	Advanced Settings	
WLAN	/BSS Mappings							
	😽 Radio		-	WLANs				
				wlan1				
0			<					
-			" >					
	Advanced Mapping							副 Create New WLAN

Radio Settings	WLAN Mapping / Mesh Mapping	Legacy Mesh	Client Bridge Settings	Advanced Settings	
WLAN/BSS Mappings					
Radio	ULANS				
0	<				
Advanced Mapping					음] Create New WLAN
				1	2

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:

Profile Indoor-APs Type	ANYAP					0
General	Name (A)	Туре	Description	Admin Status	VLAN	IP Address
Power						
Adoption						
▼ Interface						
Ethernet Ports						
Virtual Interfaces						
Port Channels						
Radios						
PPPoE						
Network						
▶ Security						
VRRP						
Critical Resources						
Services						
▶ Management						
Mesh Point						
Advanced						
	Type to search in tables					Row Count: 0
				Add	Edit Delete	Replace Exit
				Auu	Delete	LAN LAN



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:

5 Revert	🛃 Commit	Commit and Save
N		

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?

WiNG v5.9	ash	board	Configuration	Diagnostics	Оре	erations	Statistic	s
Devices Wireless Network	Sec	urity	Services Manag	ement				
RF Domain	F	rofile of	lefault-ap8533 Ty	/pe AP8533				
System Profile		Genera	1	Name	(A)	Type		Description
🥧 Virtual Controller		Power		vlan1		VLAN		
Device Overrides		Adoptio	n					
🗱 Event Policy		Wired 8	02.1x					
Auto-Provisioning Policy	Π,	r Interfac	e					
		Ether	net Ports					
		Virtua	I Interfaces					
	E	Port 0	Channels					
		Radio	IS					
		PPPo	E					
		Blueto	poth					
Profile	Ŀ	Network	k					
Indoor-APs		Security	/					
▼ Adefault-ap8533	_	VRRP						
4-67-F7-07-09-C4	4	Critical	Resources					
074-67-F7-5C-45-2D		Service	s					
		Manage	ement					
		Mesh P	oint					
	ŀ	Advanc	ed					

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:

WING v5.9 Das	shboard Config	guration Diagnostics	Operations S	Statistics		🕹 арв533 🔢	🔒 admin 🛛 🚺
Devices Wireless Network S	ecurity Services	Management				🅤 Revert 📥 Co	ommit 🛛 📊 Commit and Sav
RF Domain	Device Override	s					0
System Profile	System Name	Device	Туре	Area	Floor	Floor Number	Overrides
JVirtual Controller	ap8533-0709C4	74-67-F7-07-09-C4	🌙 AP8533			1	Clear
Device Overrides	ap8533-5C452D	74-67-F7-5C-45-2D	🧅 AP8533			1	
Event Policy							
Auto-Provisioning Policy							
Device							
d ap8533-0709C4 →							
ap8533-5C452D							
•							
Type to search	Type to search in tab	les				3	Row Count: 2
	<u> </u>					Add Edit	Delete Replace

Rasic		-
Basic Certificates Wired 802.1x RF Domain Overrides Profile Overrides General Adoption Interface Network Security VRRP Critical Resources Services Management Mesh Point Advanced	Configuration System Name ap8533-0709C4 Latitude Coordinate (-90.0000 - 90.0000) Longitude Coordinate (-180.0000 - 180.0000) Location Area Profile Profile <t< th=""><th></th></t<>	
	DK Reset Exit	

Repeat the same steps for the second Access Point:

vices Wireless Network	Security Services N	lanagement				5 Revert 🛛 📥 Comr	nit 🛛 🔚 Commit and
RF Domain	Device Overrides						
System Profile	System Name	Device	Туре	Area	Floor	Floor Number	Overrides
Virtual Controller	ap8533-0709C4	74-67-F7-07-09-C4	J AP8533			1	Clear
Device Overrides	ap8533-5C452D	74-67-F7-5C-45-2D	J AP8533			1	
Event Policy							
Auto-Provisioning Policy							
	-						
	1						

Basic	Carlingation	
Basic Certificates Wired 802.1x RF Domain Overrides General Adoption Interface Network Security VRRP Critical Resources Services Management Mesh Point Advanced	Corfiguration System Name aps533-5C4520 Littude Coordinate icglude Coordinate ic	

Commit&Save changes:

5 Revert 📥 Commit	Commit and Save

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

WiNG v5.9	Das	shboard	Configu	iration	Diagnosti
Devices Wireless Network	S	ecurity	Services	Manag	ement
RF Domain		Profile			
System Profile		Profile		Туре	
🧅 Virtual Controller			۲		
Device Overrides		default-	ap8533	aps 🧼	3533
📆 Event Policy		Indoor-A	\Ps	an'	YAP
Auto-Provisioning Policy					
V Profile					
▼ 🛄 Indoor-APs					
🥧 74-67-F7-07-09-C4	-				
🕁 74-67-F7-5C-45-2D	4				
default-ap8533 الم					

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.

WiNG v5.9	Dashboard Configuration Diagnostics Operations Statistics	📥 AP8533 🚺 🚺 🛦 admin 🚺
Devices Wireless Network	Security Services Management	튓 Revert 陆 Commit 🔚 Commit and Save
RF Domain	Auto-Provisioning	0
System Profile	Auto-Provisioning Policy	Rerun Policy Rules Every Time AP Adopted
🧅 Virtual Controller		
Device Overrides		
Event Policy		
Auto-Provisioning Policy		
Auto-Provisioning		
	1	
	1	
Tau ta suat	Type to search in tables	Row Count: 0
Type to search		
		Aud Edit Replace
Auto-Pro	visioning Policy to VA	Continue Evit
Auto-FTO		Continue

First, let's create an Auto-Provisioning policy.

Rule

Now let's add a new AutoProvisioning Rule:

			Ri	les Default			_
Rule Precedence	Operation	Device Type	Match Type	Argument 1	Argument 2	RF Domain Name /	Profile Name
G						Alias Name	
ype to search in table	5						Row Count: 0
					Add Edit	Delete Re	place Exit

e Precedence 😰	(1 to 10,000)	
o-Provisioning Policy		
Operation	2	
Operation	allow 🔻	
Pavias Tuns	3	
Device Type	🐓 anyap 🔻	
Match Parameters	4	
Match Type	Many 🔻	
lan to Profile / PE Domain		
RF Domain Name / Alias		
Profile Name	P Indor-APs	
lap to Area		
Area	0	
ha ta Flace	0	
Eleor		
1001	0	
st Controller		
Controller	1 Hostname	
Pool	1 (1 to 2)	
nd Controller		
Controller	0 Hostname v	
Pool	1 (1 to 2)	
outing 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. Ildp-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
 - I. 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:

General	Cor	ntroller Group							
Power	_	Preferred Grou	P ()						
Adoption	Cor	ntroller VLAN -							
r Interface		VLAN	0 1	(1 to 4,094	4)				
Ethernet Ports				Ŀ					
Virtual Interfaces	Au	to-Provisioning	Policy						
Port Channels		Auto Descisioni	Deliau						
Radios		Auto-Provisioni	ng Policy	✓ VC					
PPP0E		Learn and Save	e Netw ork Confi	guration 📵 🗹					
Network	Cor	ntroller Hello Inte	erval						
Security									
VRRP		Hello Interval		4 (1 to 1	201				
Critical Resources					.07				
Services		Adjacency H	old Time 2	- (2 to 600)					
Management									
Mesh Point	Cor	ntroller Adoption	n Settings						
Advanced		Offline Duration		10	(5 to 43,2	00)			
	Cor	ntroller Hostnan	ies						
		Host	Pool	Pouting Level	ID Sec Secure	ID Sec. GW	Force	Demote V/DN	
		11031	FUUI	Routing Level	IF SEC SECURE	IF 360 GW	Torce	Client	Ô
	0								
								+ Add	Row

Commit&Save changes:



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

🛐 System 👻	System						
" default 🕤			н	eaith Inventory			
	Devices		Offline Devices		System Security		
			RF Domain	Devices Offline	Threat Level	۲	RF Domain
			default	0	✔ 1 (Low)		default
	Online Offline						
	Online Offline Device Types		RF Quality				
	Online Offline Device Types Device Type O Online	Offline	RF Quality Worst 5	RF Domain			
	Online Offline Device Types Device Type Online AP7612 2	Offline 0	RF Quality Worst 5	RF Domain default			
	Online Offline Device Types Device Type () Online AP7612 2 AP8533 2	Offline 0 0	RF Quality Worst 5 100 (NA)	 RF Domain default 			
	Online Offline Offline Device Types Device Type () Online △ AP7612 2 △ AP8533 2	Offline 0 0	RF Quality Worst 5 100 (NA)	(c) RF Domain default			
	Online Offline Offline Device Types Device Type () Online AP7612 2 AP8533 2	Offline 0 0	RF Quality Worst 5 100 (NA)	(c) RF Domain default			
	Online Offline Device Types Device Type (a) Online AP7612 2 AP8533 2	Offline 0 0	RF Quality Worst 5 100 (NA)	(c) RF Domain default			
	Online Offline Device Types Device Type (a) Online AP7612 2 AP8533 2	Offline 0 0	RF Quality Worst 5 100 (NA)	(c) RF Domain 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:

WiNG v5.9	Dashboard Configuration	on Di	iagnostics Ope	erations Statis	tics		🔶 Ар8533		admin 🄀
System									
⊟ System ▼	System								. 🧿
uoradit 🕑	😣 Health		Adopted Device (a)	Туре	RF Domain Name	Model Number	Config Status	Adoption Time	Startup Time
	Inventory	+	ap7612-3B36F6	d AP7612	default	AP-7612-680B30-	version-mismatch	Wed Oct 25 2017 11	Wed Oct 25 2017 10:0
	Adopted Devices		ap7612-3B3787	d AP7612	default	AP-7612-680B30-	version-mismatch	Wed Oct 25 2017 11	Tue Oct 24 2017 04:58
	Pending Adoptions	•	ap8533-5C452D	🧅 AP8533	default	AP-8533-68SB40-	version-mismatch	Wed Oct 25 2017 11	Tue Oct 24 2017 04:52
	Offline Devices								
	Device Upgrade								
	WIPS Summary								

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:

T	Summary	Adopted Device Upgrade	File Management	Adopted Device Restart	Captive Por	rtal Pages	Crypto CMP Certificate	
Adopted Device Upgra	de							0
		Device Upgr	ade List Device In	nage File Upgrade Status	Upgrade H	listory		
Device Image Type					ſ	Images C	On Device	
Device image Type AP65						Device Typ	versi	on
2						AP7632	none	
Protocol local 🔻						AP7622	none	
File Name		3				AP7662	none	
		Q Browse	Upload			AP7602	none	
						AP7612	none	
						AP8533	none	
						AP7562	none	
						AP8432	none	
						AP7522	none	
						AP7532	none	
I								

Summary Adopted Device Upgrade File Management Adopted Device Restart Captive P	ortal Pages Crypto CMP Cer	tificate
lopted Device Upgrade		
Device Upgrade List Device Image File Upgrade Status Upgrade	History	
	Images On Device	
Device Image Type AP8533	Device Type	Version
	AP7632	none
rotocol local v	AP7622	none
	AP7662	none
Brow se	AP7602	none
	AP7612	none
	AP8533	none
	AP7562	none
	AP8432	none
	AP7522	none
	AP7532	none

	Summary	Adopted Device Upgrade	File Management	Adopted Device Restart	Captive Portal Pages	Crypto CMP Certificate	
opted Device Upgra	ade						
		Device Upgr	ade List Device In	nage File Upgrade Status	Upgrade History		
	522				Images	On Device	
Device image Type APo	533				Device Ty	rpe Version	
					AP7632	none	
rotocol local 🔻					AP7622	none	
					AP7662	none	
AP8533-5.9	.1.1-004D.img	Q Browse	Upload		AP7602	none	
	Status				× AP7612	none	
	Status	MAC	Message		AP8533	5.9.1.1-004D	
	success		Image Uploade	ed Successfully	AP7562	none	
					AP8432	none	
					AP7522	none	
					AP7532	none	
					_		
			ОК	Details >> 📋 Clip	board		

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):

Adopted Device Upgrade List Device Image File Upgrade Status Upgrade History Device Image Type AP7612 Protocol local File Name AP7612-LEAN-5.9.1.1-004D img C Browse Upload Device Upgrade List Device Image File Upgrade Status Upgrade History Images On Device Device Type Version AP7632 none AP7632 none AP7662 none AP7602 none	0
Device Upgrade List Device Image File Upgrade Status Upgrade Histor Device Image Type AP7612 Protocol Image On Device Protocol Image On Device File Name AP7612-LEAN-5.9.1.1-004D.img Image On Device	
Device Image Type AP7612 Images On Device Protocol local Protocol AP7632 none File Name AP7612-LEAN-5.9.1.1-004D.img Q. Browse Guide AP7602 none	
Device mage type Device Type Version AP7632 none AP7632 none Flie Name AP7612-LEAN-5.9.1.1-004D.img Q Browse Upload AP762 none AP7612-LEAN-5.9.1.1-004D.img Q Browse Upload AP7602 none	
Protocol Q Browse Upload AP7632 none File Name AP7612-LEAN-5.9.1.1-004D.img Q Browse Upload AP7602 none AP7612-LEAN-5.9.1.1-004D.img Q Browse Upload AP7602 none	
Protocol Coll AP7622 none File Name AP7612-LEAN-5.9.1.1-004D img Q Brow se Upload AP7602 none AP7602 none AP7602 none AP7602 none	
File Name AP7612-LEAN-5.9.1.1-004D.img Q Brow set Upload AP762 none AP7602 none AP7602 none AP7602 none	
AP7612-LEAR-5.9.1.1-004D.Img Q Browse Q Opicial 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:

WING v5.9 Dash	board Configu	ration Diagnostics Ope	rations Statistics		AP8533 ((()))	🔒 admin 🛛 🎼
Devices Certificates SMART RF						
🖃 🌍 System 👻						
🖃 🏢 default 😔 👥 🚹		St	ummary Device Upgrade Ci	aptive Portal Pages Re-elect C	ontroller	
	Device Upgrade	e				0
🗉 🥥 ap7612-3B3787 🕤			2			
🗉 🧔 ap8533-5C452D 🕞			Device Upgrade List Upg	grade Status Upgrade History		
		Device Type List All	Upor	rade from Controller		
		Sebadulad Upgrada Time V Neu	40040047	(HH:MM)	Debagt C Staggarad Debagt	
		Scheduled opgrade nine Million	0		Staggered Rebool	
		Scheduled Reboot Time Mov	v 10/24/2017 📰 0		orce Upgrade	
	All Devices					
	Hostname	MAC Address	Device Type	Version	PE Domain	
		452D 74.67 E7.50 45.2	2D 308533	5.9.1.0.021D	default	
	ap0555-50	36E6 R2 50 01 3R 36 6	ED ap0555	5.0.1.0.020D	default	
	ap7612-30	2707 D0-50-01-3D-30-F	-o ap7012	5.9.1.0-029R	default	
	ap/612-36	5/6/ B6-50-01-5B-5/-6	ap7012	5.9.1.0-029R	deraun	
	-					
Search					4	Class Linters
Search					Upgrade	Clear History

Status		×
Status	MAC	Message
success	74-67-F7-07-09-C4	Number of devices added for upgrade: 3
		OK Details >> 📋 Clipboard

		Summary	Adopted Device	Upgrade F	ile Management	Adopted Device Restart	Captive Portal	Pages (Crypto CMP Certifi	cate
٩	opted Device	e Upgrade								(
			[Device Upgrade	e List Device Ima	ge File Upgrade Status	Upgrade His	tory		
In	arado Statur									
γþ	grade status	>								
	Number of devic	es currently bein	g upgraded 3	Nur	nber of devices w aiti	ng in queue to be upgraded	1	Number of	devices marked for	cancellation 0
	Number of devic	es currently bein	g rebooted 0	Nur	nber of devices w aiti	ng in queue to be rebooted	0			
	Device Tupe	Heatnama	MAC Address	Basult	Ungrada Tima	Debast Time	Drograad	Detries	Last Status	Ungraded Pu
4	AD7642	nostname	Do E0.04 2D 21	Result	Upgrade Time	Repool Time	Progress	Retties	Ctart Upgrade f	opgraded By
	AP7012	ap/012-3030F	74 67 57 50 4	downloading	Immediate	Immediate	EC	2	Start Opgrade i	ap8533-0709C4
	AP0333	ap0555-50452	R8 50 01 3B 3	downloading	Immediate	Immediate	45	0	-	ap8533-0709C4
1	AP/012	ap/012-303/0	D0-30-01-3D-3	downloading	inineulate	Inneulate	40	U	-	apo555-070904
	porade Progress					downloading				
-1						a contracting				
										Cancel

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:

erices micless net	work Securi	ty Services	Manageme	nt					5 1 F	Revert 🛛 📥 C	ommit 🛛 🕞 C	ommit and S
Wireless LANs	Wireless L/	ANs										
Radio QoS Policy	WLAN	SSID	Description	WLAN Status	VLAN Pool	Bridging Mode	DHCP Option 82	DHCPv6 LDRA	Authenticatio n Type	Encryption Type	QoS Policy	Associati ACL
Association ACL	wlan1	WING-PSK		Enabled	1	Local	×	×	None	TKIP-CCMP	default	
SMART RF												
X MeshConnex Policy												
Mesh QoS Policy												
Passpoint Policy												
Sensor Policy												
Wireless LAN												
	3											

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 VLA N 500 that will be locally bridge by each AP.

WLAN1 DOT1X-SSID		0
Basic Configuration	WLAN Configuration	
Security	SSID 2	DOT1X-SSID
Firewall	Description	0
Client Settings	WLAN Status	Disabled Fnabled
Accounting	QoS Policy	+ default • • • • ·
Service Monitoring	Bridging Mode	
Client Load Balancing	DHCP Ontion 82	
Advanced	DHCPv6 LDPA	
Auto Shutdown	Boniour Gatew av Discovery Policy	
	Other Settinge	
	Broadcast SSID	a.7
	A new or Broadcast Drobes	
	Answer broadcast robes	•
	VLAN Assignment	
	Single VLAN VLAN Pool	
	✓VLAN 500	
	RADIUS VLAN Assignment	
	Allow RADIUS Override 👩 🥅	
	URL Filter	
	URL Fitter	0 🗸 🖓
		4
		🕪 OK Reset Exit

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	
Basic Configuration	Select Authentication
Security	
Firewall	C EAP D EAP-PSK D EAP-MAC D MAC D PSK / None
Client Settings	
Accounting	
Service Monitoring	Readurentication 0 30 (30 to 86,400)
Client Load Balancing	•
Advanced	Confine Daniel
Auto Shutdown	
	Enforcement O Captive Portal Enable Captive Portal if Primary Authentication Fails
	Captive Portal Policy 👔

AA Policy	🏏 External-RADIU	s	Continue	Exit						
				RADIUS	Authentication	RADIUS Accounting	Settings			
Server Id	Server Type	Host	Port		Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
pe to search i	n tables									Row Count: 0
							Add			ce Exit

AAA Policy E	dernal-RADIUS								6				
	RADIUS Authentication RADIUS Accounting Settings												
Server Id 🏾	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable				
/pe to search in	tables							F	Row Count: 0				
						Add	Edit De	elete Replac	e Exit				

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):



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

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

WLAN DOT1X-SSID	0
Basic Configuration	Select Authentication
Security Firewall Client Settings Accounting Service Monitoring Client Load Balancing	EAP SEAP-PSK EAP-MAC MAC PSK / None AAA Policy External-RADIUS Reauthentication 30 (30 to 86,400)
Advanced Auto Shutdown	Captive Portal Enforcement Captive Portal Enable Captive Portal if Primary Authentication Fails Captive Portal Policy
	Passpoint Policy Passpoint Policy
	Registration
	Type of Registration 👔 None 🔻
	Expiry Time (1300 (1 to 43.800 hours)
	Agreement Refresh
	External Controller 2
	Enable Follow AAA Host Host
	Send Mode 🕕 UDP 🔻
	De CK Reset Exit

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

Basic Configuration	
Security	
irewall	Captive Portal
lient Settings	
ccounting	Enforcement O Captive Portal Enable Captive Portal if Primary Authentication Fails
ervice Monitoring	Captive Portal Policy
lient Load Balancing	
dvanced	
uto Shutdown	Passpoint Policy
	Passpoint Poicy 0
	Benjetration
	device
	Expiry Time 0 4320 (1 to 43,800 hours)
	Agreement Refresh 0 0 (0 to 144,000 minutes)
	External Controller
	Enable 🕦 Follow AAA 🕦
	Host I Hostname
	Send Mode
	Extend Execution
	TKIP-CCMP WEP 128 WEP 64 Open
	WPA2-CCMP

5	Revert	📥 Commit	Commit and Save

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:

WING v5.9	Dashboard C	onfiguration Dia	gnostics Opera	tions Statistics			8533 { #	admin 💦
Devices Wireless Net	work Security Ser	vices Managemen	t			51	Revert 💾 Commit	Commit and Save
RF Domain	Profile							0
System Profile	Profile Type		Auto-Provisioning	Firewall Policy	Wireless Client Role	DHCP Server Policy	Management Policy	RADIUS Server Policy
Urtual Controller	•	1	Policy		Policy			
Device Overrides	default-ap8533	AP8533	1/0	default			default	
Event Policy	Indoor-APS	ANTAP	vc	derault			delault	
Auto-Provisioning Policy								
r Profile ▶ ဤIndoor-APs ∭default-ap8533	3							
Type to search	Type to search in tables							Row Count: 2
😼 🗊					Add	Edit Delete	Copy R	ename Replace

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												
General	Name () Type	Description	Admin Status	RF Mode	Channel	Transmit Power					
Power	radio1	Radio	radio1	🖌 Enabled	2.4 GHz WLAN	smart	smart					
Adoption	radio2	Radio	radio2	🖌 Enabled	5 GHz WLAN	smart	smart					
Interface	radio3	Radio	radio3	🖌 Enabled	Sensor	smart	smart					
Ethernet Ports												
Virtual Interfaces												
Port Channels												
Radios												
PPPoE												
Network												
▶ Security												
VRRP												
Critical Resources												
Services												
Management												
Mesh Point												
Advanced												
	Type to search in tab	les					Row Count: 3					
					Add	Edit	Replace Exit					

Radios			×
Name radio2			0
Radio Setti	ngs WLAN Mapping / Mesh Mapping	Legacy Mesh Client Bridge Settings	Advanced Settings
WLAN/BSS Mappings			
▼ Image: Constraint of the second			
Advanced Mapping			물 <u> Create New WLAN</u>
Radios			
Name radio2			

Radio Settings	WLAN Mapping / Mesh Mapping	Legacy Mesh	Client Bridge Settings	Advanced Settings	
WLAN/BSS Mappings					
▼ 🔄 Radio இ〕 ✓ wlan1(advertised) இ〕 ✓ DOT1X-SSID(advertised)	물질 WLANs				
0					
Advanced Mapping					음] Create New WLAN
				🔊 ок	Reset Exit

Move to Ethernet Ports tab and edit ge1 interface settings:

0								1
General	Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLAN
Power	fe1	Ethernet		Enabled	Access	1	×	
Adoption	fe2	Ethernet		Enabled	Access	1	×	
v 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	×	
REPOR								
Natural								
▶ Network								
▶ Security								
VRRP								
Critical Resources								
Services								
 Management 								
Mesh Point								
Advanced								
				_				
	Type to searc	ch in tables						Row Count: 7

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

thernet Ports				
ame ge1				(
	Basic Configuration	Security	Spanning Tree	
roperties		CDP/LLD	P	
Description		Cisco	Discovery Protocol Receive	0
0		Cisco	Discovery Protocol Transmit	0 🗸
Admin Status 🛈 🔘 Disabled 💿 Enabled		Link L	ayer Discovery Protocol Receive	0 🗸
Speed 1 Automatic V		Link L	ayer Discovery Protocol Transmi	t 0 🗹
Duplex 1 Automatic V		Captive	Portal Enforcement	
witching Mode		Enfor	ce captive portal	None 🗸
Mode 🖉 🖉 Access 💿 Trunk				
Native VLAN 0 1	(1 - 4094)			
Tag Native VLAN ()				
Allow ed VLANs / 1.500	(1 - 4094) (2 4 7-12)			
-	(1-4004) (2,4,1-12,)			
			D d	K Reset Exit

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

WiNG v5.9	Dashboard Configuration	on Di	iagnostics Oper	ations Statis	tics		ф ар8533		admin 🚺
System									
⊟ System ▼	System								
deradit 🕑	😵 Health		Adopted Device (a)	Туре	RF Domain Name	Model Number	Config Status	Adoption Time	Startup Time
	 Inventory 	+	ap7612-3B3787	J AP7612	default	AP-7612-680B30-V	configured	Wed Oct 25 2017 11	Wed Oct 25 2017 11:21:0
	Adopted Devices	٠	ap8533-5C452D	J AP8533	default	AP-8533-68SB40-1	configured	Wed Oct 25 2017 11	Wed Oct 25 2017 11:19:2
	Pending Adoptions								
	Offline Devices								
	Device Upgrade								
	WIPS Summary								

Client Connections:

Statistics > {RF Domain Name} > Wireless Clients:

WiNG v5.9	Dashboard Configuration	n	Diagnostics O	perations	Statistics						AP853	33	111	🤱 ad	min 🎼
🖃 🌍 System 👻	RF Domain default														
■ 0 detault ■ ap533.0709C4 ⊕ ■ ap7612.383787 ⊕ ■ ap533.5C452D ⊕	No Definition Operation Previous Previous Previous		MAC Address	IP Address 172:16.56.53	Hostname android-414dax	Role	Client Identit y Unknov	Vendo r CO-EE-	Band	AP Hostn ame ap7612	Radio MAC B8-50-(WLAN WIAN1		Last Active Fri Oct	EII Comain Name default
Cumh		Тур	e to search in tables]			Discou		Clinate	Dire			Row Count: 1

Wireless Client CO-EE-FB-F8	-4C-52 Wireless Client MAC Address Hostname	C0-EE-FB-F8-4C-52	Association		6
Vealth Details	Wireless Client MAC Address Hostname	C0-EE-FB-F8-4C-52	Association		
👌 Details	MAC Address Hostname	C0-EE-FB-F8-4C-52			
₩WMM TSPEC	Vendor State IP Address WLAN Radio MAC VLAN User Details	android-414dad10 C0-EE-FB Data-Ready 172.16.56.53 w lan1 B8-50-01-A4-90-40 1	AP Hostname AP Radio Radio Id Radio Number Band Parameter Total Bytes Total Packets User Data Rate	ap7612-38378 B8-50-01-3B-3 ap7612-38378 <u>B8-50-01-3</u> 1 1 11bgn Transmit 21,188 92 0	7 7-87 7:R1 B-37-87:R1 Receive 16,119 141 0
	Authentication Encryption	none comp	Physical Layer Rate Tx Dropped Packets Rx Errors	37 0	52 0
	RF Quality Index RF Quality Index Retry Percentage SNR Signal Noise Error Rate	4 (Good) 20.69 41 -60 -101 0		Refres	h Exit

Statistics				×
Wireless Client CO-EE-F	B-F8-4C-52			Q
😣 Health	Wireless Client		Association	
S Details	SSID	WING-PSK	AP	B8-50-01-3B-37-87
🔂 Traffic	Hostname	android-414dad10	BSS	B8-50-01-A4-90-40
WMM TSPEC	Device Type	Non Voice	Radio Number	1
lassociation History	RF Domain	default	Radio Type	11bgn
💫 Graph	OS	Unknow n	Rates	1 2 5.5 6 9 11 12 18 24 36 48 54 mcs
	Browser	Unknow n		
	Туре	Unknow n	802.11 Protocol	
	Role		High-Throughput	✓ Supported
	Role Policy		RIFS	X Unsupported
	Client Identity	Unknow n	Unscheduled PASD	Disabled
	Client Identity Precedence	0	AID	1
			Max AMSDU Size	3,839
	User Details		Max AMPDU Size	65,535
	UserName		Interframe Spacing	16
	Authentication	none	Short Guard Interval	✓ Supported
	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			
				Refresh Exit

Radio Status and Statistics:

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

WING v5.9	Dashboard Configuration	n Diagnostics	Operations	Statistics	_			×8533 	🔒 admin		
System											
🖃 鳋 System 👻	RF Domain default									. 0	,
	😵 Health 🔝 Inventory	Radio	Radio MAC	Radio Type	Access Point	АР Туре	State	Channel Current(Confi g)	Power Current(Confi g)	Clients	1
	Jevices	ap7612-3B3787:R1	B8-50-01-A4-90	2.4 GHz WLAN	ap7612-3B378	🍏 AP7612	On	6 (smt)	13 (smt)	1	
	AP Detection	ap7612-3B3787:R2	B8-50-01-A4-90	5 GHz WLAN	ap7612-3B378	🍏 AP7612	On	116w (smt)	17 (smt)	0	
	I Wireless Clients	ap8533-0709C4:R1	74-67-F7-64-B0	2.4 GHz WLAN	ap8533-0709C	🧅 AP8533	On	1 (smt)	17 (smt)	0	
	Device Upgrade	ap8533-0709C4:R2	74-67-F7-64-9A	5 GHz WLAN	ap8533-0709C	🧅 AP8533	On	56 (smt)	17 (smt)	0	
	B Wireless LANs	ap8533-0709C4:R3	74-67-F7-64-D5	Sensor	ap8533-0709C	ap8533 🖒	Off	N/A (smt)	30 (smt)	0	
	Radios	ap8533-5C452D:R1	74-67-F7-75-F3	2.4 GHz WLAN	ap8533-5C452	AP8533	On	11 (smt)	17 (smt)	0	
	- → Status	ap8533-5C452D:R2	74-67-F7-76-09	5 GHz WLAN	ap8533-5C452	AP8533	On	60 (smt)	17 (smt)	0	
	RF Statistics	ap8533-5C452D:R3	74-67-F7-76-27	Sensor	ap8533-5C452	🧅 AP8533	Off	N/A (smt)	30 (smt)	0	
	Traffic Statistics										ł
	Bluetooth										
	📾 Mesh										Ц
	🔉 Mesh Point										
	SMART RF										Ц
	▶ ₽ WIPS										
	Captive Portal										
	Application Visibility (AVC)										
	► S Coverage Hole Detection										

B8-50-01-3B-3	7-87:R2						
etails	Radio		RF Quality Statistics				
raffic /MM TSPEC /ireless LANs raph	Radio Id Radio MAC Address State Radio Type Access Point AP Type Location Adopted To Configuration Rx Antenna Used Tx Antenna Used	B8-50-01-3B-37 B8-50-01-A4-90 On 5 GHz WLAN <u>B8-50-01-3B</u> ap7612 default 74-67-F7-07-09 2 2 2	-87:R2 -50 -57 -67 -64	RF Quality Index Retry Percentage Rx Retries SNR (dBm) Signal (dBm) Noise (dBm) Error Rate (pps) Medium Error Rate (%) MOS Score R-Value	 0 (N/A) 0 24,640 0 -110 13 0.0 0.0 		
	Short Preamble Spectrum Mgmt Dual Channel HT 20 Present HT Protection Non HT Detected ERP Brotection	× No ✓ Yes ✓ Yes × No × No × No		Client Count 0 No data to display LT Clients 0			
	Non ERP Detected Non ERP Present Max Multicast Streams SMART RF	× No × No 25		Long Preamble Clients Long Slot Clients	0		
	Parameter Channel Power	Configured smt smt	Current 116w 17				



SMART RF Statistics:



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

SmartRF Neighbor radio table:

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

Wild v59 Dashboard Configuration Diagnostics Operations Statistics 🧄 🖓 👘 р																			
em .											51 R	evert 🛃	Commit 🔂 Commit						
System 🕤	RF Domain default																		
g default 👻	Health	Image: Chancel and the state st											Internits Energy Graph						
	due Devices	##8533-5C452D	74-67-F7-76-09-A0	ttan	normal	60	17	General											
	Super Detection	ap8533-5C4520	74-67-F7-76-27-D0	11an	offline		0	Radio MAC Address	74-67-	F7-76-09-A0	AP Hostname		ap8533-5C452D						
	wireless Clients	800533-0/0964	74-67-F7-64-D5-60	11an	offine			Radio Index	1		Channel		60						
	Posterioe opgrade	and513.0709C4	74-67-67-64-00-10	11000	bormal	66	17	Radio rype 11an			POwer		1/						
	2 Sweekess LAWS	ap8533-5C452D	74.67.47.75.43.00	tibon	normal	11	17		- Contract										
	Ψ Ψ ^w Radios	ap7612-383787	R5.50.01.44.00.50	11a0	normal	116m	17	Neighbors											
	v [®] Status v RF Statistics							AP Hostname	Attenuation	Channel	Radio MAC Address	Power	Radio id						
	Traffic Statistics							88-50-01-38-37-87	87	116w	B8-50-01-A4-90-50	17	1						
	() Eluetooth							74-67-F7-07-09-C4	90	56	74-67-F7-64-9A-30	17	1						
	Mesh																		
	St. Mesh Point																		
	TO SMART RF	1																	
	Q [®] Summary																		
	Q [®] Details																		
	Q ³ SMART RF History																		
	. Q. WIPS																		
	Captive Portal																		
	Application Visibility (AVC)																		
	Coverage Hole Detection																		

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

WiNG v5.9	Dashboard Configuration Di	agnostics Operat	ions Statistics									APESS	uun	admin a
em .												5) Rev	ert 👌 Comm	t 🕞 Commit
System 🕤	RF Domain default													
a U octave •	Health	AP Hostname	Radio MAC Address	Radio Type	State	Channel	Power				Details Line	rgy Graph		
	a ¹ 4Devices	10/012-303/0/	80-50-01-A4-90-40	110gn	normal	0	17		-80 -70	-60	-50	-40 -30	-20	-10
	al AP Detection	ap(533-504520	74-07-67 72 72 77 00	1180	normal	00	-M			1	-			_
	Wireless Clients	ap8533.0709C4	74.87.57.64.05.60	tian	office			140						
	Eb Device Upgrade	ap8533-0709C4	74-67-F7-64-80-10	11bon	normal	1	17		_	-				
	B Wireless Lable	ap8533-0709C4	74-67-F7-64-9A-30	ttan	normal	56	17	138	_					
	- SRadins	ap8533-5C452D	74-87-F7-75-F3-00	11bgn	normal	15	17	132						
	Delahar	207612-383787	88-50-01-A4-90-50	11an	normal	1100	17							
	T Otelus							128	1					
	Y"RF Statistics							124						
	Traffic Statistics													
	Bluetooth							120						
	Mesh							110	_					
	X Mesh Point													
	▼ Q [®] SMART RF							112						
	Summary							108		_	-			
	Q [™] Details							9						
	SMART RF History							3 104						
	WIPS							100						
	Captive Portal													
	Application Visibility (AVC)							04						
	Coverage Hole Detection							60						
								50						
								48		_				
								1.27						
								40		_	_			
									_					
								- 36						
											dB	m		
										Extern	al 📕 Neighbo	Noise	Total	

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
27 th October 2017	1.0	Initial release	Slava Dementyev