

## Spectralink VIEW Certified Configuration Guide

# Fortinet

FortiGate/FortiWiFi Wireless Controllers (Series) 30D/E, 50E, 60D/E, 70D, 80D, 90D, 90E, 92D with FAP421E, FAP423E, FAPS421E, FAPS422E, FAPS423E

FortiGate Controllers (Series) 100D, 200D, 330D, 400D, 500D, 600C, 600D, 800C, 800D, 900D, 1000, 2000, 3000, FG-5000, FG-VM with FAP421E, FAP423E, FAPS421E, FAPS422E, FAPS423E

## Copyright Notice

© 2017 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink's products are trademarks and/or service marks of Spectralink Corporation and are common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Spectralink.

All rights reserved under the International and pan-American Copyright Conventions. No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Spectralink Corporation.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

## Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

## Contact Information

### US Location

+1 800-775-5330

Spectralink Corporation  
2560 55th Street  
Boulder, CO 80301  
USA

[info@spectralink.com](mailto:info@spectralink.com)

### Denmark Location

+45 7560 2850

Spectralink Europe ApS  
Bygholm Soepark 21 E Stuen  
8700 Horsens  
Denmark

[infoemea@spectralink.com](mailto:infoemea@spectralink.com)

### UK Location

+44 (0) 20 3284 1536

Spectralink Europe UK  
329 Bracknell, Doncastle Road  
Bracknell, Berkshire, RG12 8PE  
United Kingdom

[infoemea@spectralink.com](mailto:infoemea@spectralink.com)

# Contents

<b>Introduction</b> .....	<b>5</b>
<b>Certified Product Summary</b> .....	<b>5</b>
<b>Known Limitations</b> .....	<b>6</b>
<b>Spectralink References</b> .....	<b>6</b>
<i>Support Documents</i> .....	<i>7</i>
<i>White Papers</i> .....	<i>7</i>
<b>Product Support</b> .....	<b>8</b>
<b>Chapter 1: Network Topology</b> .....	<b>9</b>
<b>Chapter 2: Initial Administrative Setup</b> .....	<b>10</b>
<b>Connecting to the FortiGate</b> .....	<b>10</b>
<i>Using the GUI</i> .....	<i>10</i>
<i>Using CLI</i> .....	<i>10</i>
<b>Registering the FortiGate</b> .....	<b>10</b>
<b>Upgrading the Firmware</b> .....	<b>11</b>
<b>Chapter 3: Configure the Environment</b> .....	<b>12</b>
<b>Physical Interfaces</b> .....	<b>12</b>
<i>From the Web GUI</i> .....	<i>12</i>
<i>From the CLI</i> .....	<i>12</i>
<b>Static Route to Gateway</b> .....	<b>13</b>
<i>From the Web GUI</i> .....	<i>13</i>
<i>From the CLI</i> .....	<i>13</i>
<b>Radius Server Identification</b> .....	<b>14</b>
<i>From the Web</i> .....	<i>14</i>
<i>From the CLI</i> .....	<i>14</i>
<b>Chapter 4: Configure Wi-Fi</b> .....	<b>15</b>
<b>Configure SSIDs</b> .....	<b>15</b>
<i>From the Web</i> .....	<i>15</i>
<i>From the CLI</i> .....	<i>19</i>
<b>Configure QoS Profiles (voice/control priorities)</b> .....	<b>20</b>
<i>From the CLI</i> .....	<i>20</i>
<b>Configure FortiAP Profiles</b> .....	<b>21</b>
<i>From the Web</i> .....	<i>21</i>
<i>From the CLI</i> .....	<i>22</i>
<b>Configure Managed FortiAPs</b> .....	<b>23</b>

<i>From the Web</i> .....	23
<i>From the CLI</i> .....	24

# Introduction

Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between PIVOT™ by Spectralink® (PIVOT) and 84-Series Wireless Telephones and WLAN infrastructure products.

The products listed below have been tested in Spectralink's lab and have passed VIEW Certification.

## Certified Product Summary

Manufacturer:	Fortinet, Inc.			
Certified products:	Controllers (Series): 30D/E, 50E, 60D/E, 70D, 80D, 90D, 90E, 92D, 100D, 200D, 330D, 400D, 500D, 600C, 600D, 800C, 800D, 900D, 1000, 2000, 3000, FG-5000, FG-VM Access Points: FAP421E, FAP423E, FAPS421E, FAPS422E, FAPS423E			
AP Radio(s):	2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n/ac)			
Security:	None, WEP, WPA-PSK, WPA2-PSK			
QoS:	Wi-Fi Standard for Spectralink 84-Series and PIVOT			
Network topology:	Bridged			
AP and WLC software version approved:	5.6.0-1449			
<i>Handset* models tested:</i>	<i>Spectralink 8741/8742/8744/8753 Wireless Telephone (PIVOT)</i>			
Handset radio mode:	802.11b	802.11b/g	802.11bgn	802.11a, 802.11an, 802.11ac
Meets VIEW minimum call capacity per AP:	8	8	8	10
<i>Handset models tested:</i>	<i>Spectralink 8440/8441/8450/8452/8453 Wireless Telephone</i>			
Handset radio mode:	802.11b	802.11b/g	802.11bgn	802.11a & 802.11an
Meets VIEW minimum call capacity per AP:	8	8	8	10

\*Spectralink handset models and their OEM derivatives are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as "Spectralink Wireless Telephones", "phones" or "handsets".

\*\* Maximum calls tested per the VIEW Certification Test Plan. The certified product may actually support a higher number of maximum calls

## Known Limitations

- Spectralink PIVOT handsets manufactured with 2.4+ and 84-series manufactured with 5.3.4+ ship with 802.11n disabled.
- PTT (Push-to-Talk) was tested with multicast to unicast (multicast-enhance) enabled
- WMM\_AC is applied only to Voice packets and not to SIP control packets in the Fortinet product.
- WPA2-Enterprise implementation on Fortinet has an interoperability conflict with Spectralink phones for OKC roaming. This problem will be corrected in the next release, 5.6.1, expected about 8/1/2017.
- DFS Channels are available in the next Fortinet release 5.6.1, expected about 8/1/2017.

## Spectralink References

All Spectralink documents are available at <http://support.spectralink.com>.

The screenshot shows the Spectralink Support website. At the top, there is a navigation bar with links for Partner Access, Spectralink.com, Contact Support, and a search icon. Below this is the Spectralink logo with the tagline 'solving every day' and the word 'support'. A secondary navigation bar contains links for PRODUCT RESOURCES, RMAs, SERVICE REQUESTS, and CUSTOMER MANAGEMENT. The main content area features a 'Welcome to Spectralink Support' message and a search prompt: 'Find resources for your product, or log in for more support options.' Below this is a 'PRODUCT RESOURCES' section with a search box for product documents and downloads, including dropdowns for Product Category (set to 'Wi-Fi') and Product Type (set to '- Any -'), and a 'FIND' button. To the right of the search box are links for 'Find all product resources', including 'All Documents & Downloads', 'Feature Requests', 'Product Alerts', 'Service Policies', 'FAQs', and 'Contact Support'. Below the search section are two columns: 'RMAs AND SERVICE REQUESTS' and 'CUSTOMER MANAGEMENT', each with a lock icon. The RMA section includes links for RMA Status, RMA Forms, RMA Requests, My Company's RMA's, My Service Requests, and My Company's Service Requests. The CUSTOMER MANAGEMENT section includes links for Warranty and Entitlement Lookup, My Company's Entitlements, and Batch Warranty and Entitlement Lookup. At the bottom of the page, there is a copyright notice: '© 2013 Spectralink Corporation, All rights reserved. Terms and Conditions | Product Warranty'.

## To go to a specific product page:

Select the Product Category and Product Type from the dropdown lists and then select the product from the next page. All resources for that particular product are displayed by default under the All tab. Documents, downloads and other resources are sorted by the date they were created so the most recently created resource is at the top of the list. You can further sort the list by the tabs across the top of the list to find exactly what you are looking for. Click the title to open the link.

## Support Documents

*PIVOT by Spectralink Configuration Guide* The PIVOT Configuration Guide provides detailed information about PIVOT menu items that have been developed specifically for the PIVOT handset.

*Spectralink 87-Series Wireless Telephone Deployment Guide* The Deployment Guide provides sequential information for provisioning and deploying the handsets. It covers deployment using the SLIC tool and CMS as well as manual deployment.

The *Spectralink 84-Series Wireless Telephone Administration Guide* provides a comprehensive list of every parameter available on Spectralink 84-Series Wireless Telephones.

The *Spectralink 84-Series Deployment Guide* is your essential reference for provisioning and deploying Spectralink 84-Series handsets in any environment.

The *Web Configuration Utility User Guide* explains how to use a web browser to configure the Spectralink 84-Series handsets on a per handset basis.

*Best Practices for Deploying Spectralink 87-Series Handsets* provides detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets.

## White Papers

Spectralink White Papers are available at <http://www.spectralink.com/resources/white-papers>.

For the Spectralink 84-Series Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 84-Series Handsets* for detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets.

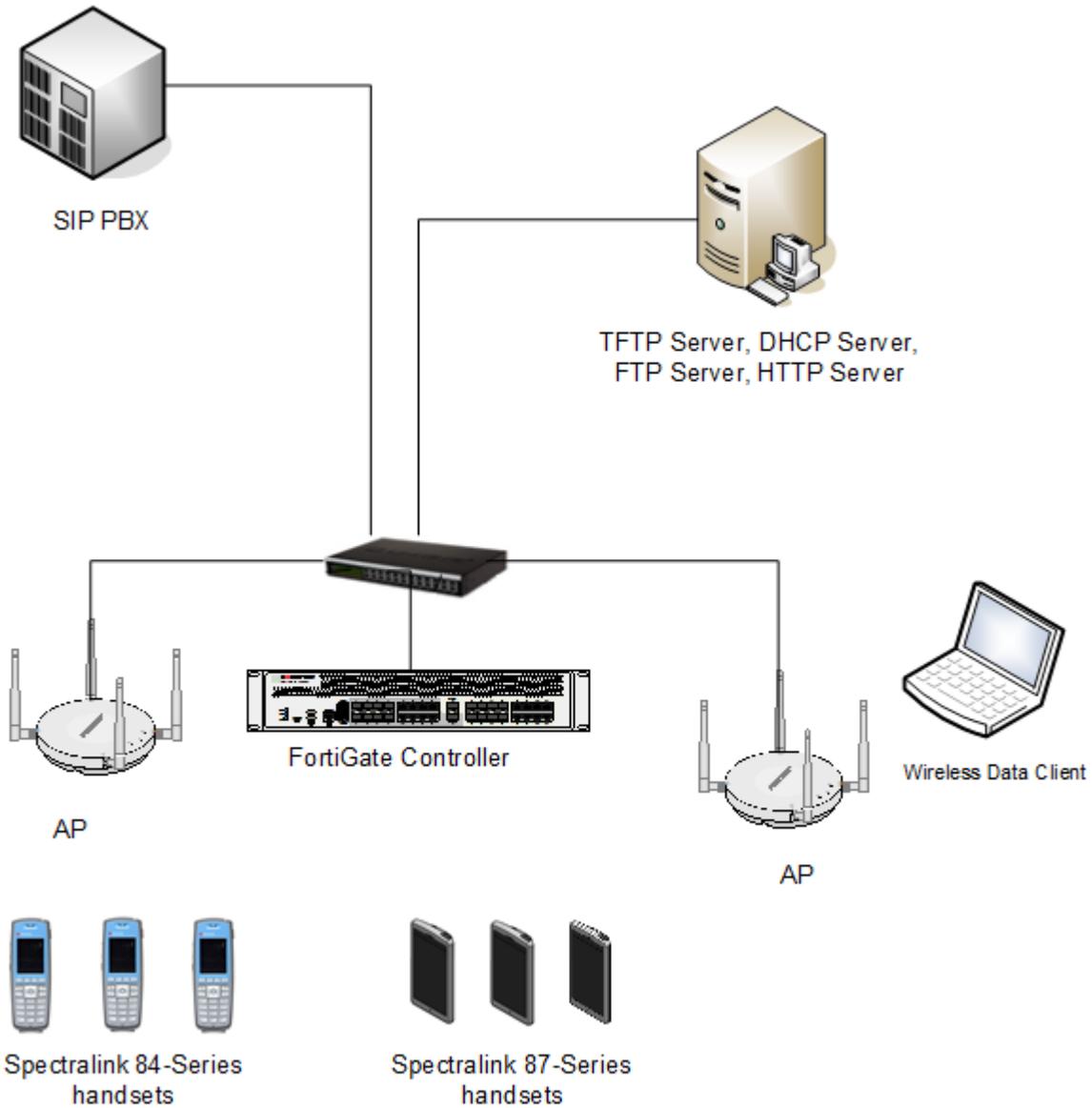
For additional details on RF deployment please see *The challenges of ensuring excellent voice quality in a Wi-Fi workplace* and *Deploying Enterprise-Grade Wi-Fi Telephony*.

These White Papers identify issues and solutions based on Spectralink's extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with Spectralink Wireless Telephones.

## *Product Support*

If you encounter difficulties or have questions regarding the configuration process, please contact Fortinet customer service at <https://www.fortinet.com/support-and-training/support/contact.html> or Spectralink at [support.spectralink.com](https://support.spectralink.com).

# Chapter 1: Network Topology



**Note: Example configuration shown**

This is a modified diagram and not all components are shown for every system type.

# Chapter 2: Initial Administrative Setup

## Connecting to the FortiGate

Connect the FortiGate's **wan** interface to your ISP-supplied equipment, and then connect the internal network to the FortiGate's default **lan** interface.

### Using the GUI

Browse to <http://docs.fortinet.com/fortigate/admin-guides>. Find the appropriate "Getting Started" guide for the FortiOS version you are using. Follow the directions in the "Connecting to the GUI using a web browser" section. The FortiExplorer application may also be used. At the time of this writing, it is only released in an Apple IOS version.



#### Note: CLI-only features

There are several features that are only available using the Command Line Interface (CLI), rather than appearing in the GUI.

From the GUI, you can open the CLI console so that it automatically opens to the object you wish to configure. For example, to edit a firewall policy, right-click on the policy in the policy list (**Policy & Objects > IPv4 Policy**) and select **Edit in CLI**.

The CLI console will appear, with the commands to access this part of the configuration added automatically

### Using CLI

Browse to <http://docs.fortinet.com/fortigate/admin-guides>. Find the appropriate "Getting Started" guide for the FortiOS version you are using. Follow one of the Connection options described in the "Using the CLI" section. The FortiExplorer application may also be used. At the time of this writing, it is only released in an Apple IOS version.

## Registering the FortiGate

Follow the directions in the "Registration" section of the "Getting Started" guide.

## *Upgrading the Firmware*

Follow the directions in the “Firmware” section of the “Getting Started” guide to backup/restore the system (if desired), download firmware, and install firmware. The firmware may also be installed using a scheduled upgrade at a convenient time, as described in the “Controlled upgrade” section.

# Chapter 3: Configure the Environment

## Physical Interfaces

The connections to the wired network can be defined from either the web GUI or from CLI.

### From the Web GUI

- 1 Navigate to **Network>Interfaces**.
- 2 Click on the name of the port to be configured, i.e. **wan1**.
- 3 Click on **Edit**.
- 4 Select the Desired **Addressing mode**, i.e. **Manual** or **DHCP**.
- 5 Enter the parameters for the desired addressing mode, such as **IP/Network Mask** for a **Manual** connection.
- 6 Check the methods allowed for **Administrative Access**

Dashboard	>	Edit Interface
FortiView	>	
Network	>	
Interfaces	☆	
DNS		
Packet Capture		
SD-WAN		
SD-WAN Status Check		
SD-WAN Rules		
Static Routes		
Policy Routes		
RIP		
OSPF		
BGP		
Multicast		

Interface Name	wan1 (90:6C:AC:4B:40:B0)
Alias	<input type="text"/>
Link Status	Up
Type	Physical Interface
Role	Undefined

Address	
Addressing mode	<b>Manual</b> DHCP PPPoE Dedicated to FortiSwitch
IP/Network Mask	<input type="text" value="172.29.109.100/255.255.255.128"/>

Administrative Access	
IPv4	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input checked="" type="checkbox"/> CAPWAP
	<input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input checked="" type="checkbox"/> TELNET <input type="checkbox"/> FTM
	<input type="checkbox"/> RADIUS Accounting <input type="checkbox"/> FortiTelemetry

### From the CLI

```
config system interface
  edit "<port number>"
    set mode "<IP Addressing Scheme Static or DHCP>"
    set ip "<IP Address with Netmask>"
```

## Static Route to Gateway

The default gateway must be defined so that the controller can reach the network

### From the Web GUI

- 1 Navigate to **Network>Static Routes**.
- 2 Click on **Create New**.
- 3 Select the physical interface for the static route to the gateway from the **Device** dropdown.
- 4 Enter the **IP** address for the route in the **Gateway** field.

The screenshot shows the 'New Static Route' configuration window. It features a tabbed interface with 'Subnet' selected. The fields are as follows:

- Destination:** 0.0.0.0/0.0.0.0
- Device:** wan1
- Gateway:** 172.29.109.1
- Administrative Distance:** 10
- Comments:** (empty)
- Status:** Enabled

At the bottom, there are 'OK' and 'Cancel' buttons.

### From the CLI

```
config router static
edit "<Entry>"
set gateway "<IP Address Of the Gateway>"
set device "<Physical Interface Connected to Gateway>"
```

## Radius Server Identification

### From the Web

- 1 Navigate to **User & Device>RADIUS Servers**.
- 2 Click on **Create New**.
- 3 Enter the **Name**, **Primary Server IP/Name**, and **Primary Server Secret**.
- 4 Touch **OK**.

The screenshot displays the 'New RADIUS Server' configuration page in the Fortinet web interface. The left sidebar shows the navigation menu with 'RADIUS Servers' highlighted. The main content area contains the following fields and options:

- Name:** Central Radius Server
- Primary Server IP/Name:** 172.29.100.3
- Primary Server Secret:** [Redacted]
- Secondary Server IP/Name:** [Empty]
- Secondary Server Secret:** [Empty]
- Authentication Method:**  Default  Specify
- NAS IP:** [Empty]
- Include in every User Group:**

At the bottom right of the form, there are two buttons:  and .

### From the CLI

```
config user radius
  edit "<Name of the Radius-Server>"
    set server "<ip address of the Radius Server>"
    set secret "<Radius Server Secret>"
```

# Chapter 4: Configure Wi-Fi

## Configure SSIDs

### From the Web

- 1 Navigate to **WiFi & Switch Controller>SSID**.
- 2 Click on **Create New** and select **SSID** from the dropdown list.
- 3 For all security types:
  - a Enter an Interface Name.
  - b Choose **WiFi SSID** from the dropdown list for **Type**.
  - c Enter the **SSID** name for on the wireless.
  - d Set the **Traffic Mode** to **Bridge** (only topology tested).
  - e The **Broadcast Suppression** was tested with the default setting of on and a list of **ARPs for known clients** and **DHCP Uplink** and was found to have good performance.
- 4 Enter security-specific items:
  - a Open security – choose **Open** from the **Security Mode** dropdown list.

FortiGate 100D FG100D3G16802582 admin

Dashboard > New Interface

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Managed FortiAPs

**SSID** ☆

FortiAP Profiles

WIDS Profiles

Log & Report >

Monitor >

Interface Name: Guest

Alias:

Type: WiFi SSID

Traffic Mode: Tunnel Bridge Mesh

WiFi Settings

SSID: Guest

Security Mode: Open

Local Authentication:

Schedule: always

Block Intra-SSID Traffic:

Maximum Clients:

Optional VLAN ID: 0

Broadcast Suppression:  ARPs for known clients ×  
DHCP Uplink ×

Filter clients by MAC Address

RADIUS server:

Status

Comments: 0/255

OK Cancel

## b WPA2-PSK

- i Choose **WPA2 Personal** from the **Security Mode** dropdown list.
- ii Enter the value for the **Pre-shared Key** and enter the same value in the phones.

The screenshot shows the FortiGate 100D configuration page for a new WiFi SSID. The interface is titled "New Interface" and "WiFi Settings". The left sidebar shows the navigation menu with "WiFi & Switch Controller" selected, and "SSID" highlighted. The main configuration area includes the following fields and options:

- Interface Name:** WPA2PSK
- Alias:** (empty)
- Type:** WiFi SSID
- Traffic Mode:** Tunnel, Bridge (selected), Mesh
- WiFi Settings:**
  - SSID:** WPA2PSK
  - Security Mode:** WPA2 Personal
  - Pre-shared Key:** (masked with dots)
  - Local Authentication:** (disabled)
  - Schedule:** always
  - Block Intra-SSID Traffic:** (disabled)
  - Maximum Clients:** (disabled)
  - Optional VLAN ID:** 0
  - Broadcast Suppression:** (enabled)
    - ARPs for known clients (disabled)
    - DHCP Uplink (disabled)
  - Filter clients by MAC Address:** (disabled)
  - RADIUS server:** (disabled)
- Status:** (empty)
- Comments:** (empty)

At the bottom of the configuration area, there are "OK" and "Cancel" buttons.



### Note: Fast roaming not yet working

Fast roaming using OKC does not have good performance in the version described in this document. A fix will be available in the next GA release of the FortiOS. Phone calls on an SSID that has Enterprise security may experience audio gaps while roaming.

- c WPA2-Enterprise – for PEAP, EAP-FAST, and EAP-TLS on the handsets.
  - i Choose **WPA2 Enterprise** from the **Security Mode** dropdown list.

- ii Indicate whether the Radius server is the Fortinet (**Local**) or external (**RADIUS Server**). If the external Radius server has already been entered, it can be selected from the dropdown list. Alternatively, the edit button can be pressed which opens a window with the same parameters as described in [Radius Server Identification](#).

5 Touch **OK**.

6 From CLI

```
config wireless-controller vap
  edit "<name of SSID>"
    set multicast-enhance enable
```



**Note: Set multicast enhance from CLI**

The **multicast-enhance** parameter can only be set from CLI. It causes multicast (used for Push-to-talk on the phone) to be converted to unicast. This setting is required for acceptable network performance even if PTT is not in use.

## From the CLI

```
config wireless-controller vap
  edit "<name of SSID>"
```

### For open security:

```
  set security open
  set local-bridging enable
  set multicast-enhance enable
```

### For WPA2-PSK:

```
  set passphrase "XXXXXXXX"
  set local-bridging enable
  set multicast-enhance enable
```



### **Note: Fast roaming improvements coming**

Fast roaming using OKC does not have good performance in the version described in this document. A fix will be available in the next GA release of the FortiOS. Phone calls on an SSID that has Enterprise security may experience audio gaps while roaming.

### For PEAP, EAP-TLS, or EAP-FAST :

```
  set security wpa2-only-enterprise
```

### For an external radius server:

```
  set auth radius
  set radius-server "<radius server name>"
```

### For a local authentication server:

```
  set auth usergroup
  set usergroup "<user group name>"
  set local-bridging enable
  set multicast-enhance enable
```

## Configure QoS Profiles (voice/control priorities)



**Note: Qos profile settings only available from the CLI**

Video/voice prioritization and bandwidth control are only available from the CLI. These settings are essential to good network performance.

### From the CLI

```
config wireless-controller qos-profile
edit "<qos profile name>"
  call-admission-control enable
  bandwidth-admission-control enable
  bandwidth-capacity 2000
  burst enable
  wmm enable
  wmm-uapsd enable
  dscp-wmm-mapping enable
  dscp-wmm-vo 63 62 61 60 59 58 57 56 55 54 53 52 51 50 49 48
  dscp-wmm-vi 47 46 45 44 43 42 41 40 39 38 37 36 35 34 33 32
  dscp-wmm-be 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
  dscp-wmm-bk 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
```

## Configure FortiAP Profiles

FortiAP profiles set up general radio, channel, and bandwidth control policies for all APs of a certain model. They can be overridden by management settings, as described in the next section.

### From the Web

- 1 Navigate to **WiFi & Switch Controller>FortiAP Profiles**.
- 2 Click on **Create New**.
- 3 Give the profile a name in the **Name** field.
- 4 Set the **Platform** field to the model number.
- 5 In the radio sections, choose whether the radio is **Disabled**, provides wireless service (**Access Point**), or is a **Dedicated Monitor**.
- 6 **WIDS** (Wireless Intrusion Detection) profiles were not tested.
- 7 **Radio Resource Provision** (automatic best channel detection) was not tested.
- 8 Set the **Band, Channel Width, Short Guard Interval, Channels, Tx Power Control, and Tx Power** as desired to meet site design wireless cell coverages needs.
- 9 Choose the **SSIDs**. (In **Bridged** mode, **Manual** must be used.)
  - a Choose **Manual**.
  - b Click on the **+**.
  - c From the window, highlight the desired SSID names to choose them.
- 10 Click on **OK**.

The screenshot displays the FortiGate 100D configuration interface for a new FortiAP profile. The profile name is 'FAPS423E Profile'. The platform is set to 'FAPS423E' and the country/region is 'United States'. The AP login password is set to 'Leave Unchanged'. The configuration is shown for two radios:

- Radio 1:** Mode is 'Access Point'. WIDS Profile and Radio Resource Provision are disabled. Client Load Balancing is set to 'Frequency Handoff' and 'AP Handoff'. Band is '2.4 GHz' with '802.11n/g/b' selected. Channel Width is '20MHz'. Short Guard Interval is disabled. Channels 1, 6, and 11 are selected. TX Power Control is set to 'Manual' and TX Power is at 100%. SSIDs include 'VPEAP (VPEAP)'.
- Radio 2:** Mode is 'Access Point'. Radio Resource Provision is disabled. Client Load Balancing is set to 'Frequency Handoff' and 'AP Handoff'. Band is '5 GHz' with '802.11ac/n/a' selected. Channel Width is '20MHz'. Short Guard Interval is disabled.

The 'Select Entries' panel on the right shows a search bar and a list of entries: 'WIFI CONTROLLER SSID (4)', 'data (data)', 'VPEAP (VPEAP)', 'VPSK2 (VPSK2\_2)', and 'VTLS (VTLS)'. The 'VPEAP (VPEAP)' entry is highlighted.

## From the CLI

```
config wireless-controller wtp-profile
  edit "<Name of the FortiAP Profile>"
    config platform
      set type "<FortiAP Model>"
    config "<Radio ID>"
      set mode ap
      set band "<Radio Band a/b/g/n/ac>"
      set channel "<Desired Broadcasting Channel>"
      set channel-bonding "<Channel Width 20/40/80MHz>"
      set vap-all disable
```

```
set vap "<SSID>"
set call-admission-control enable
set bandwidth-admission-control enable
set bandwidth-capacity 2000
```

## Configure Managed FortiAPs

To set up values for specific APs, use the Managed FortiAPs section.

### From the Web

- 1 Navigate to **WiFi & Switch Controller>Managed FortiAPs**.
- 2 Click on **Create New**.
- 3 Enter the serial number of the AP in the **Serial Number** box. Note: the AP can be automatically discovered if connected to any of the physical ports of the Fortigate or if both the controller and the AP are in the same subnet.
- 4 Identify the **FortiAP Profile** to be assigned to the AP.
- 5 Override the **Band, Channels, Tx Power Control**, and SSID assignment method in the **FortiAP Profile** as desired.
- 6 Click on **OK**.

FortiGate 100D FG100D3G16802582

Dashboard > New Managed AP

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Managed FortiAPs ☆

SSID

FortiAP Profiles

WIDS Profiles

Log & Report >

Monitor >

Serial Number PS423E3X16000072

Name 423\_1

Comments Write a comment... 0/35

State

Authorized ✓

WTP Mode Normal

Wireless Settings

FortiAP Profile FAPS423E-default

Override Radio 1

Band  802.11n/g/b (2.4 GHz Band)

Channels  6

TX Power Control  5%

SSIDs  (None)

Override Radio 2

Band  802.11ac/n/a (5 GHz Band)

Channels  (Automatically assigned)

TX Power Control  10%

SSIDs  (Automatically assign Tunnel-mode SSIDs)

Override AP Login Password

OK Cancel

## From the CLI

```
config wireless-controller wtp
edit "<FortiAP Serial No>"
set admin "<Enable to be Managed by Fortigate>"
set wtp-profile "<FortiAp Profile Name>"
```

\*\*\*\*\*END OF DOCUMENT\*\*\*\*\*