FortiWiFi and FortiAP - Configuration Guide

Version 6.2.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

April 6, 2022
FortiWiFi and FortiAP 6.2.2 Configuration Guide
01-622-481070-20220406

TABLE OF CONTENTS

Change log **8**
What's new in this release **9**
Introduction **10**
Wireless network equipment 10
FortiAP units 10
FortiGate units 10
FortiWiFi units 11
Wireless management topologies 11
Integrated wireless management 11
Cloud AP management 12
Dedicated wireless controller 12
Related products for wireless networks 12
FortiPlanner 12
FortiManager 13
FortiAnalyzer 13
Wireless network configuration **14**
SSIDs on FortiWiFi units 15
Reserved VLAN IDs 15
Wireless network configuration tasks 16
Setting your geographic location 17
Creating a FortiAP profile 17
Defining a wireless network interface (SSID) 20
Configuring DHCP for WiFi clients 23
Configuring security 24
WPA-Personal security 25
WPA-Enterprise security 25
Captive portal security 26
Adding a MAC filter 28
Limiting the number of clients 30
Enabling multicast enhancement 30
Defining SSID groups 31
Configuring dynamic user VLAN assignment 31
VLAN assignment by RADIUS 31
VLAN assignment by VLAN pool 33
Configuring user authentication 34
WPA2 Enterprise authentication 35
WiFi single sign-on (WSSO) authentication 36
Assigning WiFi users to VLANs dynamically 36
MAC-based authentication 36
Authenticating guest WiFi users 37
Configuring firewall policies for the SSID 37
Configuring the built-in access point on a FortiWiFi unit 38
Enforcing UTM policies on a local bridge SSID 39

Access point configuration 41
Network topology of managed APs 42
Discovery and authorization of APs 44
Configuring the network interface for the AP unit 45
Pre-authorizing a FortiAP unit 46
Enabling and configuring a discovered AP 46
Disabling the automatic discovery of unknown FortiAPs 47
Enabling the automatic authorization of extension devices 47
Assigning the same FortiAP profile to multiple FortiAP units 48
Overriding the FortiAP profile 48
FortiAP CLI access 49
Accessing the FortiAP CLI through the FortiAP Ethernet port 49
Accessing the FortiAP CLI through the FortiGate 49
FortiAP Configuration mode 49
Resetting FortiAP to enter the Configuration mode 50
Accessing the GUI of the FortiAP Configuration mode 50
Accessing the CLI of the FortiAP Configuration mode 52
FortiAP unit firmware upgrade 53
Checking the FortiAP unit firmware version 53
Upgrading FortiAP firmware from the FortiGate unit 53
Upgrading FortiAP firmware from the FortiAP unit 53
Advanced WiFi controller discovery 54
Controller discovery methods 54
Wireless client load balancing for high-density deployments 57
Access point handoff 57
Frequency handoff or band-steering 57
Handoff configuration 57
FortiAP groups 58
LAN port options 59
Configuring a port to WAN-LAN operation mode 59
Bridging a LAN port with an SSID 60
Bridging a LAN port with the WAN port 60
Configuring FortiAP LAN ports 60
Aggregating multiple LAN ports 62
IP fragmentation of packets in CAPWAP tunnels 63
Overriding IP fragmentation settings on a FortiAP 64
CAPWAP bandwidth formula 64
LLDP protocol 65
LED options 65
Wireless mesh configuration 67
Wireless mesh deployment modes 68
Firmware requirements 68
Types of wireless mesh 68
Fast-roaming for mesh backhaul link 70
Configuring a meshed WiFi network 70
Creating the mesh root SSID 70
Creating the FortiAP profile 70

Configuring the mesh root AP ... 71
Configuring the mesh leaf FortiAPs ... 72
Authorizing leaf APs ... 73
Creating security policies ... 73
Viewing the status of the mesh network ... 73
Configuring a point-to-point bridge ... 73
Hotspot 2.0 ANQP configuration ... 75
WiFi network with wired LAN configuration ... 79
Combining WiFi network and wired LAN with a software switch ... 79
VLAN configuration ... 81
Additional configuration ... 81
Configuring a FortiAP local bridge (private cloud-managed AP) ... 81
Continued FortiAP operation when WiFi controller connection is down ... 84
Using bridged FortiAPs for increased scalability ... 84
Remote WLAN FortiAPs ... 85
Configuring the FortiGate for remote FortiAPs ... 85
Enable split tunneling options ... 85
Apply split tunneling ... 85
Configure split tunneling behavior ... 86
Enable split tunneling on SSIDs ... 87
Configure a FortiAP unit to connect to FortiGate ... 87
Preauthorize a FortiAP unit for automatic authorization ... 88
Features for high-density deployments ... 89
Performing the firmware upgrade of multiple FortiAPs ... 89
Controlling the power save feature ... 89
11n radio powersave optimization ... 89
Configuring the broadcast packet suppression ... 90
Converting multicast streams to unicast ... 91
Ignoring weak or distant clients ... 91
Turning off the 802.11b protocol ... 92
Disabling low data rates ... 92
Enabling the automatic TX power control ... 93
Enabling the frequency band load-balancing ... 93
Setting the handoff RSSI threshold ... 93
Enabling the AP load balancing ... 94
Setting the AP load balance threshold ... 94
Setting the Application Control feature ... 94
Managing the FortiAP group and setting the dynamic VLAN assignment ... 95
Sharing tunnel SSIDs within a single managed FortiAP ... 95
Enabling the manual quarantine of devices on FortiAP (tunnel mode) ... 95
Enabling host quarantine per SSID ... 96
Locating a FortiAP with LED blinking ... 97
Uploading a FortiAP image on the wireless controller ... 97
Configuring control message off-loading ... 98

Wireless network protection **99**
Wireless Intrusion Detection System 99
Rogue AP detection 100
WIDS client de-authentication rate for DoS attacks 100
WiFi data channel encryption 100
Configuring encryption on a FortiGate unit 101
Configuring encryption on a FortiAP unit 101
Protected Management Frames and Opportunistic Key Caching support 101
Bluetooth Low Energy scan 102
Preventing local bridge traffic from reaching the LAN 103
FortiAP-S bridge mode security profiles 103
DHCP snooping and option-82 data insertion 104
Wireless network monitoring **106**
Monitoring wireless clients 106
Monitoring rogue APs 107
On-wire rogue AP detection technique 107
Rogue AP scanning as a background activity 108
Configuring rogue scanning 108
Using the Rogue AP Monitor 109
Suppressing rogue APs 110
Monitoring wireless network health 111
Monitoring FortiAP with SNMP 112
Downloading the FortiAP MIB and Fortinet Core MIB files 112
FortiAP SNMP trap messages 112
FortiAP SNMP queries 113
Wireless network examples **114**
Basic wireless network example 114
Configuring authentication for wireless users 114
Configuring the SSID 115
Adding the SSID to the FortiAP Profile 116
Configuring security policies 116
Connecting the FortiAP units 117
Wireless network example with FortiSwitch 119
Configuring FortiLink 120
Connecting the FortiSwitch 121
Configuring a wireless VLAN 121
Connecting the FortiAP units 122
Complex wireless network example 122
Scenario example 122
Configuration example 123
Configuring authentication for employee wireless users 123
Configuring authentication for guest wireless users 124
Configuring the SSIDs 125
Configuring the FortiAP profile 127
Configuring firewall policies 128
Connecting the FortiAP units 130

FortiWiFi unit as a wireless client **133**
FortiWiFi unit in client mode 133
Configuring a FortiWiFi unit as a wireless client 134
Controlled AP selection support in FortiWiFi client mode 134
Support for location-based services **136**
Configuring location tracking 136
Automatic deletion of outdated presence data 136
FortiPresence push REST API 137
Viewing device location data on a FortiGate unit 137
Troubleshooting **139**
FortiAP shell command 139
Signal strength issues 139
Asymmetric power issue 140
Frequency interference 142
Throughput issues 143
Link testing 143
Performance testing 143
IP packet fragmentation prevention in CAPWAP tunnels 144
Slow DTLS response 144
Client connection issues 145
Debugging client connection issues 145
Checking the WiFi password 146
FortiAP connection issues 147
Debugging FortiAP connection issues 147
Best practices for OSI common sources of wireless issues 150
Best practices for Layer 1 150
Best practices for Layer 2 151
Best practices for Layer 3 and above 152
Packet sniffer 153
CAPWAP packet sniffer 153
Wireless traffic packet sniffer 154
Debug commands 157
Sample outputs 157
Extension information support 157
FortiAP CLI configuration and diagnostics commands **159**
Configuration commands 159
Diagnostics commands 163
FortiAP REST API **165**

Change log

Date	Change description
2019-12-19	Initial release. See What's new in this release on page 9.
2020-01-21	Updated Configuring dynamic user VLAN assignment on page 31.
2020-03-20	Updated Advanced WiFi controller discovery on page 54 with a sample for DNS configuration.
2020-04-21	Updated Remote WLAN FortiAPs on page 85. Added a note about GUI changes in the FortiOS 6.2.3 Interface tab.
2020-06-10	Updated Packet sniffer on page 153.
2020-07-01	Updated DARRP CLI configuration commands in Creating a FortiAP profile on page 17.
2020-9-30	Updated Hotspot 2.0 ANQP configuration on page 75 with instructions for attaching hotspot profiles to a VAP.
2020-11-17	Updated DARRP scheduling commands in Creating a FortiAP profile on page 17.
2021-02-01	Updated the instructions for adding a MAC filter in Configuring security on page 24
2021-08-04	Added Wireless network example with FortiSwitch on page 119.
2021-08-12	Edited GUI steps in Enforcing UTM policies on a local bridge SSID on page 39 and FortiAP-S bridge mode security profiles on page 103.
2021-11-11	Updated Advanced WiFi controller discovery on page 54.
2021-12-01	Updated Configuring dynamic user VLAN assignment on page 31 and Configuring rogue scanning on page 108.
2022-04-06	Updated Configuring the built-in access point on a FortiWiFi unit on page 38 and Creating a FortiAP profile on page 17.

What's new in this release

FortiOS 6.2.2 wireless includes the following changes:

- New GUI in **WiFi & Switch Controller > Managed FortiAPs** to facilitate easier management and more visibility.
- Improvements to **WiFi & Switch Controller > WiFi Maps**.
- Enable LLDP by default when creating new WTP (or FortiAP) profiles; existing profiles are not affected.
- Enable Channel Utilization by default when creating new WTP (or FortiAP) profiles; existing profiles are not affected. Users can monitor the utilized channels for each AP radio from **Monitor > WiFi Health Monitor**.
- Move the `darrp-optimize` and `darrp-optimize-schedules` configurations from a global object to VDOM object.
  - Previously DARRP configured settings have been converted as well:

FOS 6.2.0 and earlier:

```
config wireless-controller timers
   set darrp-optimize 0
   set darrp-day monday tuesday
        wednesday thursday friday
   set darrp-time "01:30"
end
```

FOS 6.2.1 and later:

```
config firewall schedule recurring
   edit "tmp-darrp-optimize-0"
      set start 01:30
      set end 01:31
      set day monday tuesday wednesday
           thursday friday
   next
end
config wireless-controller setting
   set darrp-optimize 86400
   set darrp-optimize-schedules "tmp-
        darrp-optimize-0"
end
```

- Add a new external portal-type, `external-auth` for when `captive-portal` is enabled on local-bridge VAP.
- Add support for a `username-case-sensitive` option when configuring the `user radius` setting.

For more information about the FortiOS 6.2.2 wireless features, see the FortiOS Release Notes.

For more information about new FortiAP-S and FortiAP-W2 6.2.2 features, see the FortiAP-S and FortiAP-W2 Release Notes.

Introduction

This guide describes how to configure a wireless network and access points using FortiGate (or FortiWiFi) units and FortiAP units.

Wireless network equipment

This section includes an overview of Fortinet wireless network equipment:

- FortiAP units on page 10
- FortiGate units on page 10
- FortiWiFi units on page 11

FortiAP units

FortiAP units are thin wireless access points (AP) supporting the latest Wi-Fi technologies (multi-user MIMO 802.11ac Wave 1 and Wave 2, 4x4) as well as 802.11n, and the demand for plug and play deployment. FortiAP units come in various form factors (desktop, indoor, outdoor, or wall jack). Indoor and outdoor units can have internal or external antennas.

For large deployments, some FortiAP models support a mesh mode of operation in which control and data backhaul traffic between APs and the controller are carried on a dedicated wireless network. Users can roam seamlessly from one AP to another.

In dual-radio models, each radio can function as an AP or as a dedicated monitor. The monitoring function is also available during AP operation, subject to traffic levels.

FortiAP, FortiAP-C, FortiAP-S, FortiAP-W2, and FortiAP-U units are available in a variety of models to address specific use cases and management modes. For detailed information about the various models currently available, see the Fortinet website.

For assistance in choosing an AP, visit the AP product selector.

FortiGate units

A FortiGate unit is an industry leading enterprise firewall. In addition to consolidating all the functions of a network firewall, IPS, anti-malware, VPN, WAN optimization, Web filtering, and application control in a single platform, FortiGate also has an integrated Wi-Fi controller. With this integrated Wi-Fi controller, a FortiGate unit can configure and manage access points such as FortiAP, FortiAP-C, FortiAP-S, FortiAP-W2, and FortiAP-U units.

For detailed information about FortiGate models currently available, see the Fortinet website.

FortiWiFi units

A FortiWiFi unit is a FortiGate with a built-in Wi-Fi. A FortiWiFi unit can:

- Provide an access point for clients with wireless network cards. This default mode is called the Access Point mode.

  or

- Connect to another wireless network. This is called Client mode. A FortiWiFi unit operating in client mode can only have one wireless interface.

  or

- Monitor access points within radio range. This is called Monitoring mode. You can designate the detected access points as Accepted or Rogue for tracking purposes. No access point or client operation is possible in this mode. However, you can enable monitoring as a background activity while the unit is in Access Point mode.

For detailed information about FortiWiFi models currently available, see the Fortinet website.

Wireless management topologies

This section includes the following three topologies available for the management of access points:

- Integrated wireless management on page 11
- Cloud AP management on page 12
- Dedicated wireless controller on page 12

Integrated wireless management

For the integrated wireless management of access points, you can:

- Use a FortiWiFi unit which is a FortiGate with a built-in Wi-Fi module (also called local Wi-Fi radio) that works as an access point.
- Connect external access points (FortiAP) to a FortiWiFi.
- Connect external FortiAP units to a FortiGate.

The integrated wireless management topology leverages the Wireless LAN and Switch controller built into the operating system of the FortiGate (or FortiWiFi) to provide secure Wi-Fi and easily configure and manage your access points.

The integrated wireless management topology is a good choice for a small to medium enterprise deployment. The FortiWiFi is well suited for small sites of less than 40 users and an area no larger than 3,000 square feet. A deployment with a FortiGate managing external APs can range from small sites of less than 40 users to large sites with hundreds of users and with an area greater than 3,000 square feet.

With a FortiGate or FortiWiFi unit, you can configure and manage FortiAP, FortiAP-C, FortiAP-S, FortiAP-W2, and FortiAP-U units.

Cloud AP management

FortiAP Cloud offers management capabilities for standalone FortiAPs that scale from individual organizations managing a handful of APs, to large enterprises managing several thousand APs. FortiAP Cloud allows you to provision, monitor, troubleshoot, and optimize your FortiAP deployment through a simple, intuitive, and easy-to-use cloud interface that is accessible from anywhere. With zero-touch deployment options, FortiAP Cloud eliminates the need for costly on-site technical expertise. A FortiAP Cloud license key ships with each FortiAP, allowing an administrator to quickly add APs to the service.

With the FortiAP Cloud provisioning and management portal, you can manage and configure FortiAP, FortiAP-C, FortiAP-S, FortiAP-W2, and FortiAP-U units.

For more details about FortiAP Cloud, see the FortiAP Cloud documentation.

Dedicated wireless controller

Some wireless deployments require high mobility with high performance and the Fortinet Wireless Controller can provide enterprise-class secure Wi-Fi to large and high-density environments. Dedicated WLAN controllers deliver seamless mobility, quick deployment, and easy capacity expansion with radio frequency virtualization for large numbers of access points.

The FortiWLC (wireless LAN controller) and FortiWLM (wireless LAN manager) platforms deliver seamless mobility and superior reliability with optimized client distribution and channel utilization. Both single- and multi-channel deployment options are supported, maximizing efficiency to make the most of available wireless spectrum.

The FortiWLC platform can manage FortiAP-U units.

For more details about the FortiWLC dedicated wireless LAN controller platform, see the FortiWLC and FortiWLM documentation.

Related products for wireless networks

This section discusses wireless network related products offered by Fortinet.

FortiPlanner

FortiPlanner provides a simple and intuitive user interface to help you with wireless LAN planning. FortiPlanner makes sure of a successful deployment with features such as the ability to import floor plans, select the type of AP and automatically calculate the required AP number and their placement. The built-in reporting automatically creates a complete plan along with the number of FortiAP units required and the exact stock keeping unit (SKU) codes for ordering.

For more information about FortiPlanner, see the Fortinet website and FortiPlanner documentation.

FortiManager

FortiManager is the full-featured central management solution for Fortinet products. To centrally manage wireless networks, FortiManager includes the following features:

- Global wireless management and monitoring
- Centralized SSID and radio policy configuration
- Centralized AP firmware upgrades
- Centralized rogue AP suppression

For more details about FortiManager, see the Fortinet website and FortiManager documentation.

FortiAnalyzer

FortiAnalyzer delivers critical insight into threats across the entire attack surface and provides instant visibility, situation awareness, real-time threat intelligence and actionable analytics, along with Network Operation Center and Security Operation Center (NOC-SOC) security analysis and operations perspective for the Fortinet Security Fabric.

FortiAnalyzer provides the following features:

- Centralized logs, searches, and reports
- Automated indicators of compromise (IOC)
- Real-time and historical views into network activity
- Advanced compliance reporting

For more details about FortiAnalyzer, see the Fortinet website and FortiAnalyzer documentation.

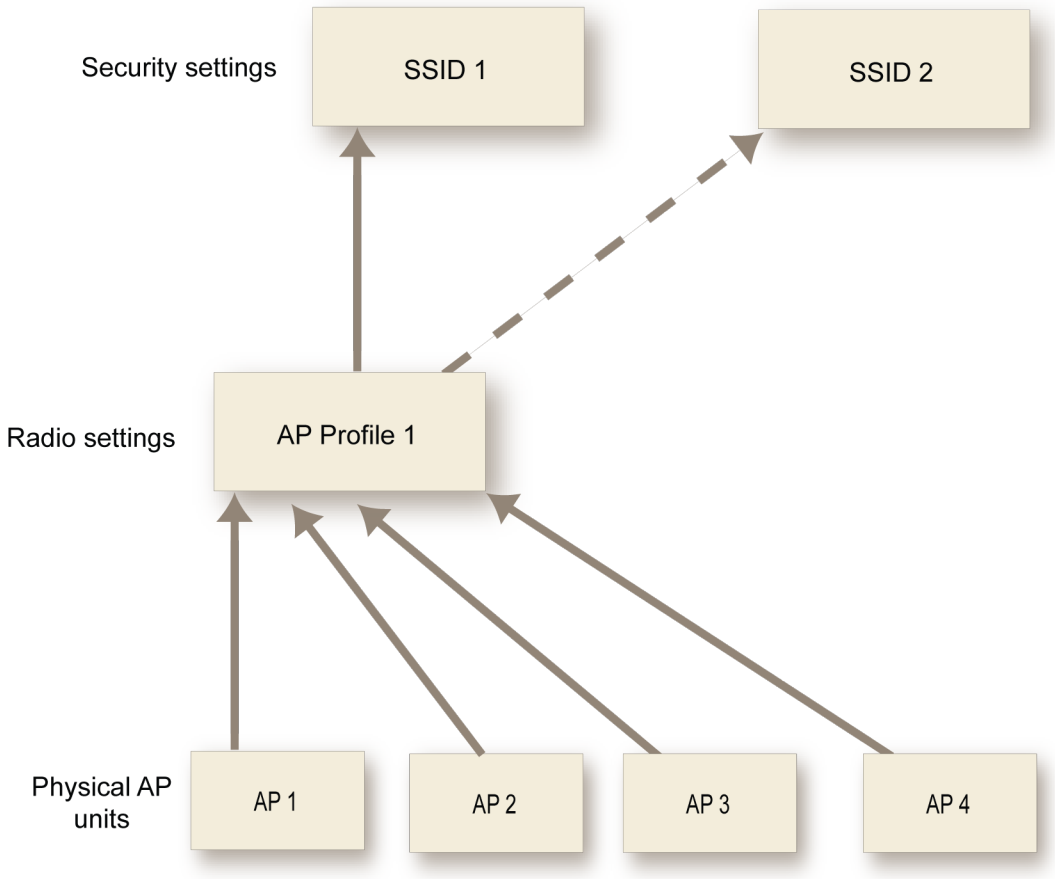
Wireless network configuration

When working with a FortiGate WiFi controller, you can configure your wireless network before you install any access points. If you are working with a standalone FortiWiFi unit, the access point hardware is already present but the configuration is quite similar. Both are covered in this section.

The FortiGate WiFi controller configuration is composed of three types of object: the SSID, the AP Profile and the physical Access Point.

- An **SSID** (service set identifier) defines a virtual wireless network interface, including security settings. One SSID is sufficient for a wireless network, regardless how many physical access points are provided. However, you may want to create multiple SSIDs to provide different services or privileges to different groups of users. Each SSID has separate firewall policies and authentication. Each radio in an access point can support up to eight SSIDs.
  A more common use of the term SSID is for the identifier that clients must use to connect to the wireless network. Each SSID (wireless interface) that you configure will have an SSID field for this identifier. In Managed Access Point configurations, you choose wireless networks by SSID values. In firewall policies, you choose wireless interfaces by their SSID name.
- An **AP Profile** defines the radio settings, such as band (802.11n for example) and channel selection. The AP Profile identifies the SSIDs to which it applies. Managed APs can use automatic profile settings or the settings of the AP profiles that you create.
- **Managed Access Points** represent local wireless APs on FortiWiFi units and FortiAP units that the FortiGate unit has discovered. There is one managed access point definition for each AP device. An access point definition can use automatic AP profile settings or select a FortiAP Profile. When automatic profile settings are used, the managed AP definition also selects the SSIDs to be carried on the AP.

Conceptual view of FortiGate WiFi controller configuration



SSIDs on FortiWiFi units

FortiWiFi units have a default SSID (wireless interface) named **wlan.** You can modify or delete this SSID as needed. As with external APs, the built-in wireless AP can be configured to carry any SSID.

The AP settings for the built-in wireless access point are located at **WiFi & Switch Controller > Local WiFi Radio**. The available operational settings are the same as those for external access points which are configured at **WiFi & Switch Controller > Managed FortiAPs**.

Reserved VLAN IDs

The following table lists the VLAN IDs reserved for internal use only. Do not use those VLAN IDs in FAP management VLAN, SSID static VLAN, and dynamically assigned VLAN.

FortiAP model	VLAN ID reserved for internal use
FAP-C24JE	898 and 899

FortiAP model	VLAN ID reserved for internal use
FAP-S221E, FAP-S223E, FAP-221E, FAP-222E, FAP-223E, and FAP-224E	97 and 98

Wireless network configuration tasks

To configure a wireless network, perform the following tasks:

1. Setting your geographic location on page 17
2. Creating a FortiAP profile on page 17
3. Defining a wireless network interface (SSID) on page 20
4. Configuring security on page 24
5. Defining SSID groups on page 31
6. Configuring dynamic user VLAN assignment on page 31
7. Configuring user authentication on page 34
8. Configuring firewall policies for the SSID on page 37
9. Configuring the built-in access point on a FortiWiFi unit on page 38
10. Enforcing UTM policies on a local bridge SSID on page 39

For AP configuration details, see Access point configuration on page 41.

On FortiGate model 30D, GUI configuration of the WiFi controller is disabled by default. To enable it, enter the following CLI commands:

```
config system global
  set gui-wireless-controller enable
end
```

The WiFi and Switch Controllers are enabled through the Feature Store (under **System > Feature Visibility**). However, they are separately enabled and configured to display in the GUI via the CLI.

To enable both WiFi and Switch Controllers, enter the following CLI commands:

```
config system global
   set wireless-controller enable
   set switch-controller enable
end
```

To enable the GUI display for both controllers, enter the following CLI commands::

```
config system settings
   set gui-wireless-controller enable
   set gui-switch-controller enable
end
```

Setting your geographic location

The maximum allowed transmitter power and permitted radio channels for WiFi networks depend on the region in which the network is located. By default, the WiFi controller is configured for the United States. If you are located in any other region, set your geographic location before you begin the wireless network configuration.

To change the location setting - CLI

To change the country to France, for example, enter

```
config wireless-controller setting
   set country FR
end
```

To see the list of country codes, enter a question mark ('?') instead of a country code.

Before changing the country setting, you must remove all FortiAP Profiles. To do this, go to **WiFi & Switch Controller > FortiAP Profiles**.

To view all country and region codes, and regulatory domains - CLI

The following CLI command can be entered to view a list of the country and region codes, and regulatory domains supported by Fortinet:

```
cw_diag -c all-countries
```

Below is a table showing a sample of the list displayed by entering this command:

Country-code	Region-code	Domain	ISO-name	Name
0	A	FCC3 & FCCA	NA	NO_COUNTRY_SET
8	W	NULL1 & WORLD	AL	ALBANIA
12	W	NULL1 & WORLD	DZ	ALGERIA
16	A	FCC3 & FCCA	AS	AMERICAN SAMOA
...	...	...	...	...

Creating a FortiAP profile

A FortiAP profile defines radio settings for a particular platform (FortiAP model). The profile also selects which SSIDs (virtual APs) the APs will carry. FortiAP units contain two radio transceivers, making it possible, for example, to provide both 2.4 GHz 802.11b/g/n and 5 GHz 802.11a/n service from the same access point. The radios can also be used for monitoring, used for the Rogue AP detection feature.

You can modify existing FortiAP profiles or create new ones of your own.

To configure a FortiAP profile - GUI

1. Go to **WiFi & Switch Controller > FortiAP Profiles** and select **Create New**.
2. Enter a **Name** for the FortiAP Profile.
3. In **Platform**, select the FortiWiFi or FortiAP model to which this profile applies.
4. If split tunneling is used, in **Split Tunneling Subnets**, enter a comma-separated list all of the destination IP address ranges that should ***not*** be routed through the FortiGate WiFi controller.
5. For each radio, enter:

Mode	Select the type of mode. **Disabled** – the radio is disabled. **Access Point** – the platform is an access point. **Dedicated Monitor** – the platform is a dedicated monitor. See Wireless network monitoring on page 106.
WIDS Profile	Optionally, select a Wireless Intrusion Detection (WIDS) profile. See Wireless network protection on page 99.
Radio Resource Provision	Select to enable the distributed radio resource provisioning (DARRP) feature. This feature measures utilization and interference on the available channels and selects the clearest channel at each access point. The measurement can be repeated periodically to respond to changing conditions.
Client Load Balancing	Select Frequency Handoff or AP Handoff as needed. See Wireless client load balancing for high-density deployments on page 57.
Band	Select the wireless protocols that you want to support. The available choices depend on the radio's capabilities. Where multiple protocols are supported, the letter suffixes are combined: "802.11g/b" means 802.11g **and** 802.11b. Note that on two-radio units such as the FortiAP-221C it is not possible to put both radios on the same band.
Channel Width	Select channel width for 802.11ac or 802.11n on 5 GHz.
Short Guard Interval	Select to enable the short guard interval for 802.11ac or 802.11n on 5 GHz.
Channels	Select the channel or channels to include. The available channels depend on which IEEE wireless protocol you selected in **Band**. By default, all available channels are enabled.
TX Power Control	Enable automatic or manual adjustment of transmit power, specifying either minimum and maximum power levels in dBm or as a percentage.

TX Power	When **TX Power Control** is set to **Auto**, the **TX Power** is set by default to a range of 10-17 dBm. Set the range between 1 and 20 for both the lower and upper limits. When **TX Power Control** is set to **Manual**, the **TX Power** is set by default to 100% of the maximum power permitted in your region. To change the level, drag the slider.
SSIDs	Select **Auto** or **Manual**. Selecting **Auto** eliminates the need to re-edit the profile when new SSIDs are created. However, you can still select SSIDs individually using **Manual**. Note that bridge mode SSIDs cannot be manually selected for FortiWiFi local radio platforms. Automatic assignment of SSIDs (**Auto**) is not available for FortiAPs in **Local Bridge** mode. The option is hidden on both the Managed FortiAP settings and the FortiAP Profile assigned to that AP.

Radio 1 settings are the same as Radio 2 settings except for the options for **Channel**.

Radio 2 settings are available only for FortiAP models with dual radios.

6. Click **OK**.

To configure a FortiAP profile - CLI

This example configures a FortiAP-220B to carry all SSIDs on Radio 1 but only SSID example_wlan on Radio 2.

```
config wireless-controller wtp-profile
   edit guest_prof
      config platform
         set type 220B
      end
      config radio-1
         set mode ap
         set band 802.11g
         set vap-all enable
      end
      config radio-2
         set mode ap
         set band 802.11g
         set vaps example_wlan
      end
   end
```

To enable DARRP - CLI

To prevent interference between APs, the FortiOS WiFi Controller includes the Distributed Automatic Radio Resource Provisioning (DARRP) feature. Through DARRP, each FortiAP unit autonomously and periodically determines the channel that is best suited for wireless communications. FortiAP units select their channel so that they do not interfere with each other in large-scale deployments where multiple access points have overlapping radio ranges.

In this example, DARRP is enabled for both radios in the FAP321C-default profile:

```
config wireless-controller wtp-profile
   edit FAP321C-default
      config radio-1
         set darrp enable
      end
      config radio-2
```

```
        set darrp enable
      end
   end
```

To set DARRP timing - CLI

DARRP periodically runs based on the "`darrp-optimize`" timer within active schedules. By default, DARRP runs once a day (every 86400 seconds) from 1:00am to 1:30am, 7 days a week (recurring). You can change the timer and select up to 16 schedules in the CLI.

FortiOS provides the following default settings:

```
config firewall schedule recurring
   edit "default-darrp-optimize"
      set start 01:00
      set end 01:30
      set day sunday monday tuesday wednesday thursday friday saturday
   next
end


config wireless-controller setting
   set darrp-optimize 86400
   set darrp-optimize-schedules "default-darrp-optimize"
end
```

Confine DARRP activity to a low-traffic period to reduce interruption caused by channel change.

Defining a wireless network interface (SSID)

You begin configuring your wireless network by defining one or more SSIDs to which your users can connect. When you create an SSID, a virtual network interface is also created with the **Name** you specified in the SSID configuration.

If a software switch interface contains an SSID (but only one), the WiFi SSID settings are available in the switch interface settings.

To create a new SSID

1. Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID**.
2. Fill in the SSID fields as described below.

To edit the settings of an existing SSID

1. Either
   - Go to **WiFi & Switch Controller > SSID**.
     or
   - Go to **Network > Interfaces**.
     WiFi interfaces list the SSID beside the interface **Name**.
2. Edit the SSID fields, as needed.

SSID fields

Interface Name	Enter a name for the SSID interface.
Type	WiFi SSID.
Traffic Mode	**Tunnel** — Tunnel to Wireless Controller — Data for WLAN passes through WiFi Controller. This is the default. **Bridge** — Local bridge with FortiAP Interface — FortiAP unit Ethernet and WiFi interfaces are bridged. **Mesh** — Mesh Downlink — Radio receives data for WLAN from mesh backhaul SSID.
IP/Network Mask	Enter the IP address and netmask for the SSID.
IPv6 Address	Enter the IPv6 address. This is available only when IPv6 has been enabled on the unit.
Administrative Access	Select which types of administrative access are permitted on this SSID.
IPv6 Administrative Access	If you have IPv6 addresses, select the permitted IPv6 administrative access types for this SSID.
DHCP Server	To assign IP addresses to clients, enable DHCP server. You can define IP address ranges for a DHCP server on the FortiGate unit or relay DHCP requests to an external server. If the unit is in transparent mode, the DHCP server settings will be unavailable. For more information, see Configuring DHCP for WiFi clients on page 23.
Device Detection	Detect connected device type. Enabled by default.
Active Scanning	Enabled by default.
WiFi Settings	
SSID	Enter the SSID. By default, this field contains `fortinet`.
Security Mode	Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface. Additional security mode options are available in the CLI. For more information, see Configuring security on page 24.
	Captive Portal – authenticates users through a customizable web page.
	WPA2-Personal – WPA2 is WiFi Protected Access version 2. There is one pre-shared key (password) that all users use.

	WPA2-Personal with Captive Portal – The user will need to know the pre-shared key and will also be authenticated through the custom portal.
	WPA2-Enterprise – similar to WPA2-Personal, but is best used for enterprise networks. Each user is separately authenticated by user name and password.
	Other choices are: **WPA3-Enterprise**, **WPA3-SAE**, **WPA3-SAE-Transition**, **OWE**, and **OSEN**.
Pre-shared Key	Available only when **Security Mode** is **WPA2-Personal**. Enter the encryption key that the clients must use.
Authentication	Available only when **Security Mode** is **WPA2-Enterprise**. Select one of the following: **RADIUS Server** — Select the RADIUS server that will authenticate the clients. **Local** – Select the user group(s) that can authenticate.
Portal Type	Available only when **Security Mode** is **Captive Portal**. Choose the captive portal type. Authentication is available with or without a usage policy disclaimer notice.
Authentication Portal	**Local** - portal hosted on the FortiGate unit **External** - enter FQDN or IP address of external portal
User Groups	Select permitted user groups for captive portal authentication.
Exempt List	Select exempt lists whose members will not be subject to captive portal authentication.
Customize Portal Messages	Click the listed portal pages to edit them.
Redirect after Captive Portal	Optionally, select **Specific URL** and enter a URL for user redirection after captive portal authentication. By default, users are redirected to the URL that they originally requested.
Allow New WiFi Client Connections When Controller Is Down	This option is available for local bridge SSIDs with WPA-Personal security. See Continued FortiAP operation when WiFi controller connection is down on page 84.
Broadcast SSID	Optionally, disable broadcast of SSID. By default, the SSID is broadcast.
Schedule	Select when the SSID is enabled. You can choose any schedule defined in **Policy & Objects > Objects > Schedules**.
Block Intra-SSID Traffic	Select to enable the unit to block intra-SSID traffic.
Maximum Clients	Select to limit the number of clients permitted to connect simultaneously. Enter the limit value.
Split Tunneling	Select to enable some subnets to remain local to the remote FortiAP. Traffic for these networks is not routed through the WiFi Controller. Specify split-tunnel networks in the FortiAP Profile. See Remote WLAN FortiAPs on page 85.
Optional VLAN ID	Enter the ID of the VLAN this SSID belongs to. Enter 0 for non-VLAN operation. See Reserved VLAN IDs on page 15.

Enable Explicit Web Proxy	Select to enable explicit web proxy for the SSID.
Listen for RADIUS Accounting Messages	Enable if you are using RADIUS-based single sign-on (SSO).
Secondary IP Address	Optionally, enable and define secondary IP addresses. Administrative access can be enabled on secondary interfaces.
Comments	Enter a description or comment for the SSID.

To configure a virtual access point (SSID) - CLI

The example below creates an access point with SSID “example” and WPA2-Personal security. The wireless interface is named example_wlan.

WiFi SSIDs include a schedule that determines when the WiFi network is available. The default schedule is Always. You can choose any schedule (but not schedule group) that is defined in **Policy & Objects > Objects > Schedules**.

```
config wireless-controller vap
   edit example_wlan
      set ssid "example"
      set broadcast-ssid enable
      set security wpa2-only-personal
      set passphrase "hardtoguess”
      set schedule always
      set vdom root
   end
config system interface
   edit example_wlan
      set ip 10.10.120.1 255.255.255.0
   end
```

Configuring DHCP for WiFi clients

Wireless clients need to have IP addresses. If you use RADIUS authentication, each user’s IP address can be stored in the Framed-IP-Address attribute. Otherwise, you need to configure a DHCP server on the WLAN interface to assign IP addresses to wireless clients.

To configure a DHCP server for WiFi clients - GUI

1. Go to **WiFi & Switch Controller > SSID** and edit your SSID entry.
2. In **DHCP Server** select **Enable**.
3. In **Address Range**, select **Create New**.
4. In the **Starting IP** and **End IP** fields, enter the IP address range to assign.
   By default an address range is created in the same subnet as the wireless interface IP address, but not including that address.
5. Set the **Netmask** to an appropriate value, such as 255.255.255.0.
6. Set the **Default Gateway** to **Same as Interface IP**.
7. Set the **DNS Server** to **Same as System DNS**.

8. If you want to restrict access to the wireless network by MAC address, see Adding a MAC filter on page 28.
9. Select **OK**.

To configure a DHCP server for WiFi clients - CLI

In this example, WiFi clients on the example_wlan interface are assigned addresses in the 10.10.120.2-9 range to connect with the WiFi access point on 10.10.120.1.

```
config system dhcp server
   edit 0
      set default-gateway 10.10.120.1
      set dns-service default
      set interface example_wlan
      set netmask 255.255.255.0
      config ip-range
         edit 1
            set end-ip 10.10.120.9
            set start-ip 10.10.120.2
         end
      end
```

You cannot delete an SSID (wireless interface) that has DHCP enabled on it.

Configuring security

An SSID supports the following security modes:

- Open
- Captive portal
- Wi-Fi Protected Access version 2 (WPA2), WPA2-Personal and WPA2-Enterprise
- WPA3-Enterprise
- WPA3-Simultaneous Authentication of Equals (SAE)
- WPA3-SAE Transition
- Opportunistic Wireless Encryption (OWE)
- OWE Transition
- OSU Server-Only Authenticated L2 Encryption Network (OSEN)

WPA2 security with a pre-shared key for authentication is called WPA2-Personal. This can work well for one person or a small group of trusted people. But, as the number of users increases, it is difficult to distribute new keys securely and there is increased risk that the key could fall into the wrong hands.

A more secure form of WPA2 security is WPA2-Enterprise. Users each have their own authentication credentials, verified through an authentication server, usually RADIUS. FortiOS can also authenticate WPA2-Enterprise users through its built-in user group functionality. FortiGate user groups can include RADIUS servers and can select users by RADIUS user group. This makes possible Role-Based Access Control (RBAC).

By default, WPA2 security encrypts communication using Advanced Encryption Standard (AES). But some older wireless clients support only Temporal Key Integrity Protocol (TKIP). You can change the encryption to TKIP or negotiable TKIP-AES in the CLI. For example, to accommodate clients with either TKIP or AES, enter:

```
config wireless-controller vap
   edit example_wlan
      set security wpa-personal
      set passphrase "hardtoguess"
      set encrypt TKIP-AES
   end
```

Captive portal security connects users to an open web portal defined in replacement messages. To navigate to any location beyond the web portal, the user must pass FortiGate user authentication.

WPA-Personal security

WPA2-Personal security setup requires only the preshared key that you will provide to your clients.

To configure WPA2-Personal security - GUI

1. Go to **WiFi & Switch Controller > SSID** and edit your SSID entry.
2. In **Security Mode**, select **WPA2 Personal**.
3. In **Pre-shared Key**, enter a key between 8 and 63 characters long.
4. Select **OK**.

To configure WPA2-Personal security - CLI

```
config wireless-controller vap
   edit example_wlan
      set security wpa2-personal
      set passphrase "hardtoguess"
   end
```

WPA-Enterprise security

If you will use FortiOS user groups for authentication, go to **User & Device > User > User Groups** and create those groups first. The groups should be Firewall groups.

If you will use a RADIUS server to authenticate wireless clients, you must first configure the FortiGate unit to access the RADIUS server.

To configure FortiGate unit access to the RADIUS server - GUI

1. Go to **User & Device > RADIUS Servers** and select **Create New**.
2. Enter a **Name** for the server.
3. **a.** In **Primary Server** area:
   i. **IP/Name** — enter the network name or IP address for the server.
   ii. **Secret** — enter the shared secret used to access the server.
4. Optionally, enter the information for a secondary or backup RADIUS server.
5. Select **OK**.

To configure the FortiGate unit to access the RADIUS server - CLI

```
config user radius
   edit exampleRADIUS
      set auth-type auto
      set server 10.11.102.100
      set secret aoewmntiasf
   end
```

RADIUS Change of Authorization (CoA) support

The CoA feature enables the FortiGate to receive a client disconnect message from the RADIUS server. This is used to disconnect clients when their time, credit or bandwidth had been used up. Enable this on the RADIUS server using the CLI:

```
config user radius
   edit <name>
      set radius-coa enable
end
```

To configure WPA-Enterprise security - GUI

1. Go to **WiFi & Switch Controller > SSID** and edit your SSID entry.
2. In **Security Mode**, select **WPA2 Enterprise**.
3. In **Authentication**, do one of the following:
   - If you will use a RADIUS server for authentication, select **RADIUS** Server and then select the RADIUS server.
   - If you will use a local user group for authentication, select **Local** and then select the user group(s) permitted to use the wireless network.
4. Select **OK**.

To configure WPA-Enterprise security - CLI

```
config wireless-controller vap
   edit example_wlan
      set security wpa2-enterprise
      set auth radius
      set radius-server exampleRADIUS
   end
```

Captive portal security

Captive portal security provides an access point that initially appears open. The wireless client can connect to the AP with no security credentials. The AP responds to the client's first HTTP request with a web page requesting user name and password. Until the user enters valid credentials, no communication beyond the AP is permitted.

The captive portal can be hosted on the FortiGate unit, or externally. For details see

Configuring WiFi captive portal security - FortiGate captive portal on page 27

Configuring WiFi captive portal security - external server on page 27

For general information about captive portals, see the Captive Portal chapter of the Authentication Guide.

Configuring WiFi captive portal security - FortiGate captive portal

The built-in FortiGate captive portal is simpler than an external portal. It can even be customized if needed.

To configure a WiFi Captive Portal - GUI:

1. Go to **WiFi & Switch Controller > SSID** and create your SSID.
   If the SSID already exists, you can edit the SSID or you can edit the WiFi interface in **Network > Interfaces**.
2. In **Security Mode**, select **Captive Portal**.
3. Enter

Portal Type	The portal can provide authentication and/or disclaimer, or perform user email address collection.
Authentication Portal	Local
User Groups	Select permitted user groups or select **Use Groups from Policies**, which permits the groups specified in the security policy.
Exempt List	Select exempt lists whose members will not be subject to captive portal authentication.
Customize Portal Messages	Click the link of the portal page that you want to modify. For more information see the Captive Portal chapter of the Authentication Guide.

4. Select **OK**.

Configuring WiFi captive portal security - external server

An external captive portal is a web page on a web server. The essential part of the web portal page is a script that gathers the user's logon credentials and sends back to the FortiGate a specifically-formatted POST message. The portal page can also contain links to local information such as legal notices, terms of service and so on. Without authenticating, the user cannot access any other information. This is sometimes called a "walled garden".

On the captive portal page, the user submits credentials, which the script returns to the FortiGate at the URL **https://<FGT_IP>:1000/fgtauth** with data **magic=session_id&username=<username>&password=<password>**.
(The magic value was provided in the initial FortiGate request to the web server.)

To ensure that credentials are communicated securely, enable the use of HTTPS for authentication:

```
config user setting
   set auth-secure-http enable
end
```

To configure use of an external WiFi Captive Portal - GUI:

1. Go to **WiFi & Switch Controller > SSID** and create your SSID.
   If the SSID already exists, you can edit the SSID or you can edit the WiFi interface in **Network > Interfaces**.
2. In **Security Mode**, select **Captive Portal**.

3. Enter

Portal Type	The portal can provide authentication and/or disclaimer, or perform user email address collection.
Authentication Portal	External - enter the FQDN or IP address of the external portal. Typically, this is the URL of a script. Do **not** include the protocol (http:// or https://) part of the URL.
User Groups	Select permitted user groups or select **Use Groups from Policies**, which permits the groups specified in the security policy.
Exempt List	Select exempt lists whose members will not be subject to captive portal authentication.
Redirect after Captive Portal	Original Request Specific URL - enter URL

4. Select **OK**.

Adding a MAC filter

On each SSID or FortiAP, you can create a MAC address filter list to either permit or exclude a list of clients identified by their MAC addresses.

This is actually not as secure as it appears. Someone seeking unauthorized access to your network can obtain MAC addresses from wireless traffic and use them to impersonate legitimate users. A MAC filter list should only be used in conjunction with other security measures such as encryption.

To block a specific client from connecting to an SSID using a MAC filter - CLI

1. Create a wireless controller address with the client's MAC address, and set the policy to deny:

```
config wireless-controller address
   edit "client_1"
      set mac b4:ae:2b:cb:d1:72
      set policy deny
   next
end
```

2. Create a wireless controller address group using the above address and setting the default policy to allow:

```
config wireless-controller addrgrp
   edit mac_grp
      set addresses "client_1"
      set default-policy allow
   next
end
```

3. On the VAP, select the above address group:

```
config wireless-controller vap
   edit wifi-vap
      set ssid "Fortinet-psk"
      set security wpa2-only-personal
      set passphrase fortinet
      set address-group "mac_grp"
```

```
   next
end
```

The client's MAC address (*b4:ae:2b:cb:d1:72* in this example) will be denied a connection to the SSID (*Fortinet-psk*), but other clients (such as *e0:33:8e:e9:65:01*) will be allowed to connect.

To allow a specific client to connect to an SSID using a MAC filter - CLI

1. Create a wireless controller address with the client's MAC address, and set the policy to allow:
```
config wireless-controller address
   edit "client_1"
      set mac b4:ae:2b:cb:d1:72
      set policy allow
   next
end
```
2. Create a wireless controller address group using the above address and setting the default policy to deny:
```
config wireless-controller addrgrp
   edit mac_grp
      set addresses "client_1"
      set default-policy deny
   next
end
```
3. On the VAP, select the above address group:
```
config wireless-controller vap
   edit wifi-vap
      set ssid "Fortinet-psk"
      set security wpa2-only-personal
      set passphrase fortinet
      set address-group "mac_grp"
   next
end
```

The client's MAC address (*b4:ae:2b:cb:d1:73* in this example) will be allowed to connect to the SSID (*Fortinet-psk*), but other clients (such as *e0:33:8e:e9:65:01*) will be denied a connection.

To block a specific client from connecting to a WTP or FortiAP - CLI

```
config wireless-controller wtp-profile
   edit "FAP-profile"
      config deny-mac-list
         edit 1
            set mac 00:09:11:ef:37:67
         next
   end
end
```

You can log in to the FortiAP CLI to see the list of denied MAC addresses with the following command:

```
cw_diag -c deny-mac-list
```

WTP Configured Access Control List:

00:09:11:ef:37:67

----------Total 1 MAC entries----------

You can also see the denied event recorded from the FortiGate wireless event log.

Limiting the number of clients

You might want to prevent overloading of your access point by limiting the number of clients who can associate with it at the same time. Limits can be applied per SSID, per AP, or per radio.

To limit the number of clients per SSID - GUI

1. Go to **WiFi & Switch Controller > SSID** and edit your SSID.
2. Turn on **Maximum Clients** and enter the maximum number of clients in **Limit Concurrent WiFi Clients**.

To limit the number of clients per AP- CLI

Edit the wtp-profile (FortiAP profile), like this:

```
config wireless-controller wtp-profile
   edit "FAP221C-default"
      set max-clients 30
   end
```

To limit the number of clients per radio - CLI

Edit the wtp-profile (FortiAP profile), like this:

```
config wireless-controller wtp-profile
   edit "FAP221C-default"
      config radio-1
         set max-clients 10
      end
      config radio-2
         set max-clients 30
      end
   end
```

Enabling multicast enhancement

FortiOS can translate multicast traffic into unicast traffic to send to clients, maintaining its own multicast client through IGMP snooping. You can configure this in the CLI:

```
config wireless-controller vap
   edit example_wlan
      set multicast-enhance enable
      set me-disable-thresh 32
   end
```

If the number of clients on the SSID is larger than `me-disable-thresh`, multicast enhancement is disabled.

Defining SSID groups

Optionally, you can define SSID groups. An SSID group has SSIDs as members and can be specified just like an SSID in a FortiAP Profile.

To create an SSID group - GUI

Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID Group**. Give the group a **Name** and choose **Members** (SSIDs, but not SSID groups).

To create an SSID group - CLI:

```
config wireless-controller vap-group
   edit vap-group-name
      set vaps "ssid1" "ssid2"
   end
```

Configuring dynamic user VLAN assignment

Clients connecting to the WiFi network can be assigned to a VLAN. You can do this with RADIUS attributes when the user authenticates or with VLAN pooling when the client associates with a particular FortiAP. You cannot use both of these methods at the same time.

VLAN assignment by RADIUS

You can assign each individual user to a VLAN based on information stored in the RADIUS authentication server. If the user's RADIUS record does not specify a VLAN ID, the user is assigned to the default VLAN for the SSID.

The RADIUS user attributes used for the VLAN ID assignment are:

Attribute type	Attributes value	Note
IETF 64 (Tunnel-Type)	13	VLAN
IETF 65 (Tunnel-Medium-Type)	6	IEEE-802
IETF 81 (Tunnel-Private-Group-ID)	1–4094	One VLAN ID per user. See Reserved VLAN IDs on page 15.

To configure dynamic VLAN assignment, you need to:

1. Configure access to the RADIUS server.
2. Create the SSID and enable dynamic VLAN assignment.
3. Create a FortiAP Profile and add the local bridge mode SSID to it.
4. Create the VLAN interfaces and their DHCP servers.
5. Create security policies to allow communication from the VLAN interfaces to the Internet.
6. Authorize the FortiAP unit and assign the FortiAP Profile to it.

To configure access to the RADIUS server

1. Go to **User & Device > RADIUS Servers** and select **Create New**.
2. Enter a **Name**, the name or IP address in **Primary Server IP/Name**, and the server secret in **Primary Server Secret**.
3. Select **OK**.

To create the dynamic VLAN SSID

1. Go to **WiFi & Switch Controller > SSID**, select **Create New > SSID** and enter:

Name	An identifier, such as dynamic_vlan_ssid.
Traffic Mode	Local bridge or Tunnel, as needed.
SSID	An identifier, such as DYNSSID.
Security Mode	WPA2 Enterprise
Authentication	RADIUS Server. Select the RADIUS server that you configured.

2. Select **OK**.
3. Under Additional Settings, enable **Dynamic VLAN assignment**. If you do not see the toggle, you can enable from the CLI:

```
config wireless-controller vap
   edit dynamic_vlan_ssid
      set dynamic-vlan enable
      set vlanid 10
   end
```

Optionally, you can also assign a VLAN ID to set the default VLAN for users without a VLAN assignment. See Reserved VLAN IDs on page 15.

To create the FortiAP profile for the dynamic VLAN SSID

1. Go to **WiFi & Switch Controller > FortiAP Profiles**, select Create New and enter:

Name	A name for the profile, such as dyn_vlan_profile.
Platform	The FortiAP model you are using. If you use more than one model of FortiAP, you will need a FortiAP Profile for each model.
Radio 1 and Radio 2	
SSID	Select the SSID you created (example dynamic_vlan_ssid). Do not add other SSIDs.

2. Adjust other radio settings as needed.
3. Select **OK**.

To create the VLAN interfaces

1. Go to **Network > Interfaces** and select **Create New > Interface**.
2. Enter:

Name	A name for the VLAN interface, such as VLAN100.
Interface	The physical interface associated with the VLAN interface.
VLAN ID	The numeric VLAN ID, for example 100.
Addressing mode	Select Manual and enter the IP address / Network Mask for the virtual interface.
DHCP Server	Enable and then select Create New to create an address range.

3. Select **OK**.
4. Repeat the preceding steps to create other VLANs as needed.

Security policies determine which VLANs can communicate with which other interfaces. These are the simple Firewall Address policy without authentication. Users are assigned to the appropriate VLAN when they authenticate.

To connect and authorize the FortiAP unit

1. Connect the FortiAP unit to the FortiGate unit.
2. Go to **WiFi & Switch Controller > Managed FortiAPs**.
3. When the FortiAP unit is listed, double-click the entry to edit it.
4. In **FortiAP Profile**, select the FortiAP Profile that you created.
5. Select **Authorize**.
6. Select **OK**.

VLAN assignment by VLAN pool

In an SSID, you can define a VLAN pool. As clients associate to an AP, they are assigned to a VLAN. A VLAN pool can

- assign a specific VLAN based on the AP's FortiAP group, usually for network configuration reasons, or
- assign one of several available VLANs for network load balancing purposes (tunnel mode SSIDs only)

See Reserved VLAN IDs on page 15.

To assign a VLAN by FortiAP group - CLI

In this example, VLAN 101, 102, or 103 is assigned depending on the AP's FortiAP group.

```
config wireless-controller vap
   edit wlan
      set vlan-pooling wtp-group
      config vlan-pool
         edit 101
            set wtp-group wtpgrp1
         next
         edit 102
            set wtp-group wtpgrp2
         next
         edit 101
            set wtp-group wtpgrp3
         end
      end
   end
```

Load balancing

There are two VLAN pooling methods used for load balancing:

The choice of VLAN can be based on any one of the following criteria:

- **round-robin** - from the VLAN pool, choose the VLAN with the smallest number of clients
- **hash** - choose a VLAN from the VLAN pool based on a hash of the current number of SSID clients and the number of entries in the VLAN pool

If the VLAN pool contains no valid VLAN ID, the SSID's static VLAN ID setting is used.

To assign a VLAN by round-robin selection - CLI

In this example, VLAN 101, 102, or 103 is assigned using the round-robin method:

```
config wireless-controller vap
   edit wlan
      set vlan-pooling round-robin
      config vlan-pool
         edit 101
         next
         edit 102
         next
         edit 103
         end
      end
   end
```

To assign a VLAN by hash-based selection - CLI

In this example, VLAN 101, 102, or 103 is assigned using the hash method:

```
config wireless-controller vap
   edit wlan
      set vlan-pooling hash
      config vlan-pool
         edit 101
         next
         edit 102
         next
         edit 103
         end
      end
   end
```

Configuring user authentication

You can perform user authentication when the wireless client joins the wireless network and when the wireless user communicates with another network through a firewall policy. WEP and WPA-Personal security rely on legitimate users knowing the correct key or passphrase for the wireless network. The more users you have, the more likely it is that the key or passphrase will become known to unauthorized people. WPA-Enterprise and captive portal security provide

separate credentials for each user. User accounts can be managed through FortiGate user groups or an external RADIUS authentication server.

WPA2 Enterprise authentication

Enterprise authentication can be based on the local FortiGate user database or on a remote RADIUS server. Local authentication is essentially the same for WiFi users as it is for wired users, except that authentication for WiFi users occurs when they associate their device with the AP. Therefore, enterprise authentication must be configured in the SSID. WiFi users can belong to user groups just the same as wired users and security policies will determine which network services they can access.

If your WiFi network uses WPA2 Enterprise authentication verified by a RADIUS server, you need to configure the FortiGate unit to connect to that RADIUS server.

Configuring connection to a RADIUS server - GUI

1. Go to **User & Device > RADIUS Servers** and select **Create New**.
2. Enter a **Name** for the server.
   This name is used in FortiGate configurations. It is not the actual name of the server.
3. In **Primary Server** area:
   a. **IP/Name** — enter the network name or IP address for the server.
   b. **Secret** — enter the shared secret used to access the server.
4. Optionally, enter the information for a secondary or backup RADIUS server.
5. Select **OK**.

To configure the FortiGate unit to access the RADIUS server - CLI

```
config user radius
   edit exampleRADIUS
      set auth-type auto
      set server 10.11.102.100
      set secret aoewmntiasf
   end
```

To implement WPA2 Enterprise security, you select this server in the SSID security settings. See Defining a wireless network interface (SSID) on page 20.

To use the RADIUS server for authentication, you can create individual FortiGate user accounts that specify the authentication server instead of a password, and you then add those accounts to a user group. Or, you can add the authentication server to a FortiGate user group, making all accounts on that server members of the user group.

Creating a wireless user group

Most wireless networks require authenticated access. To enable creation of firewall policies specific to WiFi users, you should create at least one WiFi user group. You can add or remove users later. There are two types of user group to consider:

- A Firewall user group can contain user accounts stored on the FortiGate unit or external authentication servers such as RADIUS that contain and verify user credentials.
- A Fortinet single sign-on (FSSO) user group is used for integration with Windows Active Directory or Novell eDirectory. The group can contain Windows or Novell user groups who will be permitted access to the wireless LAN.

WiFi single sign-on (WSSO) authentication

WSSO is RADIUS-based authentication that passes the user's user group memberships to the FortiGate. For each user, the RADIUS server must provide user group information in the Fortinet-Group-Name attribute. This information is stored in the server's database. After the user authenticates, security policies provide access to network services based on user groups.

1. Configure the RADIUS server to return the Fortinet-Group-Name attribute for each user.
2. Configure the FortiGate to access the RADIUS server, as described in WPA2 Enterprise authentication on page 35.
3. Create firewall user groups on the FortiGate with the same names as the user groups listed in the RADIUS database. Leave the groups empty.
4. In the SSID choose WPA2-Enterprise authentication. In the **Authentication** field, select **RADIUS Server** and choose the RADIUS server that you configured.
5. Create security policies as needed, using user groups (**Source User(s)** field) to control access.

When a user authenticates by WSSO, the firewall monitor **Monitor > Firewall User Monitor**) shows the authentication method as WSSO.

Assigning WiFi users to VLANs dynamically

Some enterprise networks use Virtual LANs (VLANs) to separate traffic. In this environment, to extend network access to WiFi users might appear to require multiple SSIDs. But it is possible to automatically assign each user to their appropriate VLAN from a single SSID. To accomplish this requires RADIUS authentication that passes the appropriate VLAN ID to the FortiGate by RADIUS attributes. Each user's VLAN assignment is stored in the user database of the RADIUS server.

1. Configure the RADIUS server to return the following attributes for each user:
   Tunnel-Type (value: VLAN)
   Tunnel-Medium-Type (value: IEEE-802)
   Tunnel_Private-Group-Id (value: the VLAN ID for the user's VLAN)
2. Configure the FortiGate to access the RADIUS server.
3. Configure the SSID with WPA2-Enterprise authentication. In the **Authentication** field, select **RADIUS Server** and choose the RADIUS server that you will use.
4. Create VLAN subinterfaces on the SSID interface, one for each VLAN. Set the VLAN ID of each as appropriate. You can do this on the **Network > Interfaces** page.
5. Enable Dynamic VLAN assignment for the SSID. For example, if the SSID interface is "office", enter:
```
config wireless-controller vap
   edit office
      set dynamic-vlan enable
   end
```
6. Create security policies for each VLAN. These policies have a WiFi VLAN subinterface as **Incoming Interface** and allow traffic to flow to whichever **Outgoing Interface** these VLAN users will be allowed to access.

MAC-based authentication

Wireless clients can also be authenticated by MAC address. A RADIUS server stores the allowed MAC address for each client and the wireless controller checks the MAC address independently of other authentication methods.

MAC-based authentication must be configured in the CLI. In the following example, MAC-based authentication is added to an existing access point "vap1" to use RADIUS server hq_radius (configured on the FortiGate):

```
config wireless-controller vap
   edit vap1
      set radius-mac-auth enable
      set radius-mac-auth-server hq_radius
   end
```

Authenticating guest WiFi users

The FortiOS Guest Management feature enables you to easily add guest accounts to your FortiGate unit. These accounts are authenticate guest WiFi users for temporary access to a WiFi network managed by a FortiGate unit.

To implement guest access, you need to

1. Go to **User & Device > User Groups** and create one or more guest user groups.
2. Go to **User & Device > Guest Management** to create guest accounts. You can print the guest account credentials or send them to the user as an email or SMS message.
3. Go to **WiFi & Switch Controller > SSID** and configure your WiFi SSID to use captive portal authentication. Select the guest user group(s) that you created.

Guest users can log into the WiFi captive portal with their guest account credentials until the account expires.

Configuring firewall policies for the SSID

For users on the WiFi LAN to communicate with other networks, firewall policies are required. This section describes creating a WiFi network to Internet policy.

Before you create firewall policies, you need to define any firewall addresses you will need.

To create a firewall address for WiFi users - GUI

1. Go to **Policy & Objects > Addresses**.
2. Select **Create New**, enter the following information and select **OK**.

Name	Enter a name for the address. For example, wifi_net.
Type	Select **Subnet.**
Subnet / IP Range	Enter the subnet address. For example, 10.10.110.0/24.
Interface	Select the interface where this address is used. For example, example_wifi.

To create a firewall address for WiFi users - CLI

```
config firewall address
   edit "wifi_net"
      set associated-interface "example_wifi"
      set subnet 10.10.110.0 255.255.255.0
   end
```

To create a firewall policy - GUI

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. In **Incoming Interface**, select the wireless interface.
3. In **Source Address**, select the address of your WiFi network, wifi_net for example.
4. In **Outgoing Interface**, select the Internet interface, for example, **port1**.
5. In **Destination Address**, select **All**.
6. In **Service**, select ALL, or select the particular services that you want to allow, and then select the right arrow button to move the service to the **Selected Services** list.
7. In **Schedule**, select **always**, unless you want to define a schedule for limited hours.
8. In **Action**, select ACCEPT.
9. Select **Enable NAT**.
10. Optionally, set up UTM features for wireless users.
11. Select **OK**.

To create a firewall policy - CLI

```
config firewall policy
   edit 0
      set srcintf "example_wifi"
      set dstintf "port1"
      set srcaddr "wifi_net"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set nat enable
   end
```

Configuring the built-in access point on a FortiWiFi unit

FortiWiFi does not support bridge mode SSIDs.

Both FortiGate and FortiWiFi units have the WiFi controller feature. If you configure a WiFi network on a FortiWiFi unit, you can also use the built-in wireless capabilities in your WiFi network as one of the access points.

If Virtual Domains are enabled, you must select the VDOM to which the built-in access point belongs. You do this in the CLI. For example:

```
config wireless-controller global
   set local-radio-vdom vdom1
end
```

To configure the FortiWiFi unit's built-in WiFi access point

1. Go to **WiFi & Switch Controller > Local WiFi Radio**.
2. Select a FortiAP profile to apply to the FortiWiFi access point (see Creating a FortiAP profile on page 17 and select **FortiWiFi local radio** as the platform).
3. Optionally, you can override settings configured in the FortiAP profile.
4. Click **Apply**.

If you want to connect external APs such as FortiAP units, see Access point configuration on page 41.

Enforcing UTM policies on a local bridge SSID

If a bridge mode SSID is configured for a managed FortiAP-S (or smart FortiAP), you can add a security profile group to the wireless controller configuration that allows you to apply the following security profile features to the traffic over the bridge SSID:

- AntiVirus
- Scan Botnets
- Intrusion Prevention
- Application Control
- Web Filter

Configure Security Profile Groups - GUI

1. Go to **WiFi & Switch Controller > SSID** and select the bridge mode SSID assigned to the FortiAP Profile that you want to configure.
2. In the selected SSID, enable the **Security profile group** option.
3. From the Security profile group drop-down field, you can either edit the **wifi-default** profile or select **Create** to make a new one.

   The Security Profile Group window loads.
4. Enable or disable **Logging**.
5. Enable or disable **Scan Botnets**.

   This option is enabled by default. If you enable this option, select **Blocked** or **Monitor**.
6. Under **Security Profiles**, you can enable or disable the **AntiVirus**, **Web Filter**, **Application Control**, and **Intrusion Prevention** profiles. To view available profiles or create new ones, click the drop-down field.
7. Click **OK** to save your Security Profile Group changes.
8. Click **OK** to save your SSID changes.

Configure Security Profile Groups - CLI

You configure security profile groups on managed smart FortiAPs by using the `config wireless-controller utm-profile` command. Then, you can assign a security profile group by using the `set utm-profile` command under `config wirelesscontroller vap`, after `local-bridging` is set to `enable`.

Note that the default `utm-profile`, named `wifi-default`, has all applicable options within the command set to `wifi-default`.

To view all available profiles that you can assign, type "`?`". For example, "`set ips-sensor ?`".

```
config wireless-controller utm-profile
   edit <name>
      set comment <comment>
      set utm-log {enable | disable}
      set ips-sensor <name>
      set application-list <name>
      set antivirus-profile <name>
      set webfilter-profile <name>
      set scan-botnet-connections {disable | block | monitor}
   next
end

config wireless-controller vap
   edit <name>
      set local-bridging enable
      set utm-profile <name>
   next
end
```

To debug the wireless-controller configurations related to security profile groups, use the following diagnose command:

```
diagnose wireless-controller wlac_hlp
```

Access point configuration

This section describes how to configure access points for your wireless network.

FortiAP units discover WiFi controllers. The administrator of the WiFi controller authorizes the FortiAP units that the controller can manage.

In most cases, FortiAP units can find WiFi controllers through the wired Ethernet without any special configuration. Review the Network topology of managed APs on page 42 section to make sure that your method of connecting the FortiAP unit to the WiFi controller is valid. Then, you are ready to follow the procedures in Discovery and authorization of APs on page 44.

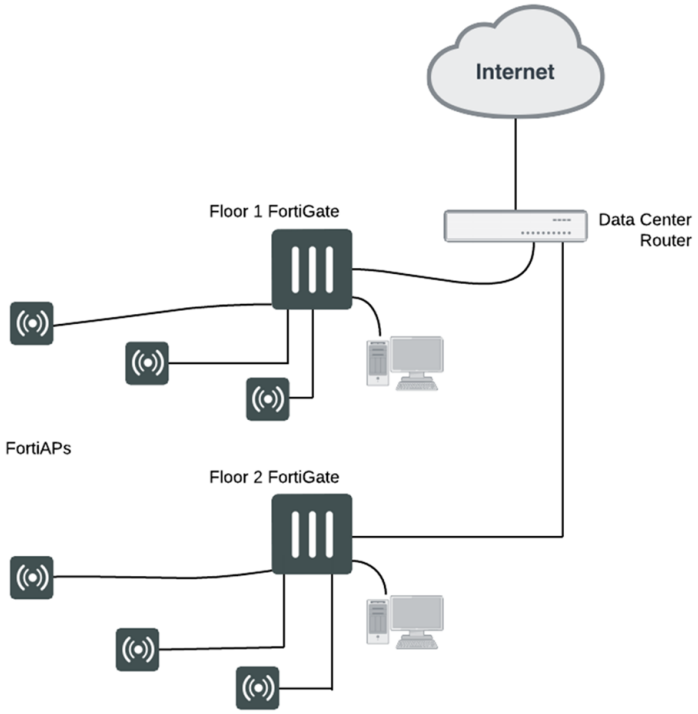
If your FortiAP units are unable to find the WiFi controller, refer to Advanced WiFi controller discovery on page 54 for detailed information about the FortiAP unit controller discovery methods and how you can configure them.

Network topology of managed APs

The FortiAP unit can be connected to the FortiGate unit in any of the following ways:

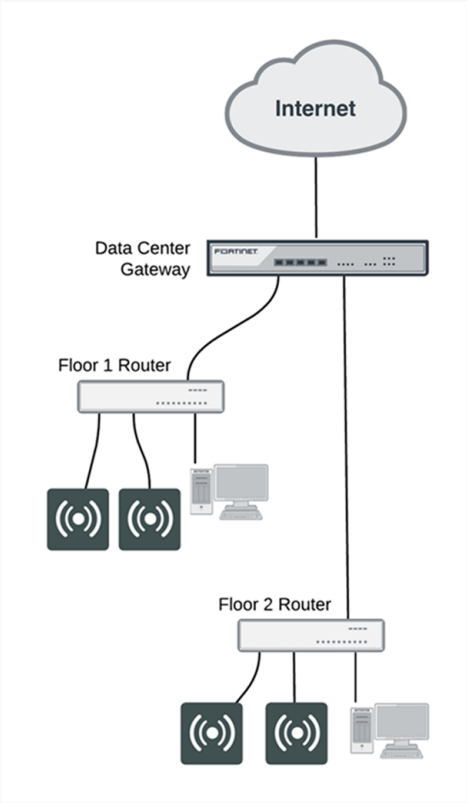
- **Direct connection**: The FortiAP unit is directly connected to the FortiGate unit with no switches between them. This configuration is common for locations where the number of FortiAPs matches the number of internal ports available on the FortiGate. In this configuration, the FortiAP unit requests an IP address from the FortiGate unit, enters discovery mode and quickly finds the FortiGate WiFi controller. This configuration is also known as a wirecloset deployment.

Direct connection deployment



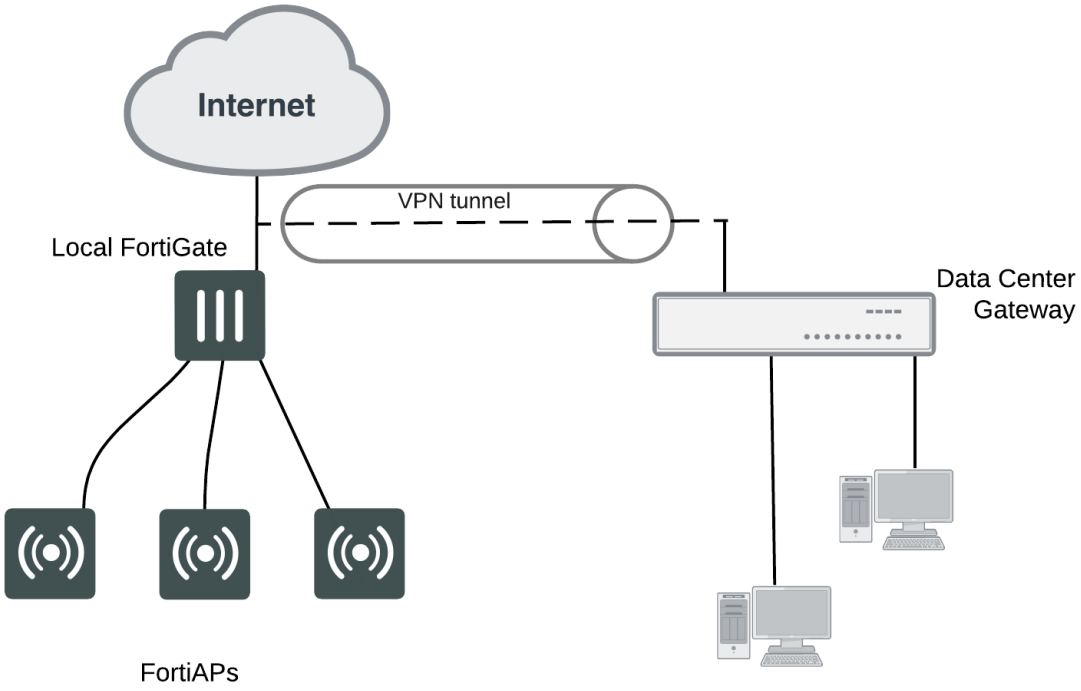
- **Switched connection**: The FortiAP unit is connected to the FortiGate WiFi controller by an Ethernet switch operating in L2 switching mode or L3 routing mode. There must be a routable path between the FortiAP unit and the FortiGate unit and ports 5246 and 5247 must be open. This configuration is also known as a gateway deployment.

Switched connection deployment



- **Connection over WAN**: The FortiGate WiFi controller is off-premises and connected by a VPN tunnel to a local FortiGate. In this method of connectivity, it's best to configure each FortiAP with the static IP address of the WiFi controller. Each FortiAP can be configured with three WiFi controller IP addresses for redundant failover. This configuration is also known as a data center remote management deployment.

Connection-over-WAN deployment



Discovery and authorization of APs

To complete the discovery and authorization of APs, perform the following tasks:

- Configuring the network interface for the AP unit on page 45
- Pre-authorizing a FortiAP unit on page 46
- Enabling and configuring a discovered AP on page 46
- Disabling the automatic discovery of unknown FortiAPs on page 47
- Enabling the automatic authorization of extension devices on page 47
- Assigning the same FortiAP profile to multiple FortiAP units on page 48
- Overriding the FortiAP profile on page 48

Configuring the network interface for the AP unit

The interface to which you connect your wireless access point needs an IP address. No administrative access, DNS Query service or authentication should be enabled.

In this example, the FortiAP units connect to port3 and are controlled through IP addresses on the 10.10.70.0/24 network.

To configure the interface for the AP unit - GUI

1. Go to **Network > Interfaces**, and edit the interface to which the AP unit connects (in this example, port3).
2. In **Addressing mode**, select **Manual.**
3. In **IP/Network Mask**, enter an IP address and netmask for the interface (in this example, 10.10.70.1/255.255.255.0).
4. In the Administrative Access section, go to **IPv4** and select the **CAPWAP** checkbox.

   Note: In FortiOS 6.2.3 and later, select the **Security Fabric Connection** checkbox.
5. When FortiAP units are connected to the interface on FortiGate (directly or through a switch), you can go to the Edit Interface section and set the **Role** to **LAN**.

   Selecting the LAN role loads the DHCP Server toggle. If you enable **DHCP Server**, the GUI can automatically set the DHCP IP range based on the interface IP address.
6. Click **OK**.

To configure the interface for the AP unit - CLI

In the CLI, you must configure the interface IP address and DHCP server separately.

Configure the interface for FortiOS 6.2.2 and earlier:

```
config system interface
   edit "port3"
      set mode static
      set ip 10.10.70.1 255.255.255.0
      set allowaccess capwap
   next
end
```

Configure the interface for FortiOS 6.2.3 and later:

```
config system interface
   edit "port3"
      set mode static
      set ip 10.10.70.1 255.255.255.0
      set allowaccess fabric
   next
end
```

Configure the DHCP server:

```
config system dhcp server
   edit 3
      set interface "port3"
      config ip-range
         edit 1
            set start-ip 10.10.70.2
            set end-ip 10.10.70.254
         next
```

```
        end
        set default-gateway 10.10.70.1
        set netmask 255.255.255.0
        set vci-match enable
        set vci-string "FortiAP"
    next
end
```

The optional `vci-match` and `vci-string` fields ensure that the DHCP server will provide IP addresses only to FortiAP units.

Pre-authorizing a FortiAP unit

If you enter the FortiAP unit information in advance, the unit is authorized and begins to function when it is connected.

To pre-authorize a FortiAP unit

1. Go to **WiFi & Switch Controller > Managed FortiAPs** and select **Create New**.
   On some models the **WiFi Controller** menu is called **WiFi & Switch Controller**.
2. Enter the **Serial Number** of the FortiAP unit.
3. Configure the **Wireless Settings** as required.
4. Select **OK**.

Enabling and configuring a discovered AP

1. Connect the FortiAP unit to the FortiGate unit. Within two minutes, the **WiFi & Switch Controller > Managed FortiAPs** page displays the discovered FortiAP unit.
2. Select the FortiAP unit and authorize that unit.

Discovered access point unit

When you authorize (enable) a FortiAP unit, it is configured by default to use the default FortiAP profile (determined by model). You can create and select a different profile, if needed. The FortiAP profile defines the entire configuration for the AP.

To add and configure the discovered AP unit - GUI

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
   This configuration also applies to local WiFi radio on FortiWiFi models.
2. Select the FortiAP unit from the list and edit it.
3. Optionally, enter a **Name**. Otherwise, the unit will be identified by serial number.
4. Select **Authorize**.
5. Select a **FortiAP Profile**.
6. Select **OK**.

The physical access point is now added to the system. If the rest of the configuration is complete, it should be possible to connect to the wireless network through the AP.

To add the discovered AP unit - CLI

First get a list of the discovered access point unit serial numbers:

```
get wireless-controller wtp
```

Add a discovered unit and associate it with AP-profile1, for example:

```
config wireless-controller wtp
   edit FAP22A3U10600118
      set admin enable
      set wtp-profile AP-profile1
   end
```

To view the status of the added AP unit

```
config wireless-controller wtp
   edit FAP22A3U10600118
   get
```

The `join-time` field should show a time, not “N/A”. See the preceding GUI procedure for more information.

Disabling the automatic discovery of unknown FortiAPs

By default, FortiGate adds newly discovered FortiAPs to the Managed FortiAPs list, awaiting the administrator's authorization. Optionally, you can disable this automatic registration function to avoid adding unknown FortiAPs. A FortiAP will be registered and listed only if its serial number has already been added manually to the Managed FortiAPs list. AP registration is configured on each interface.

To disable automatic discovery and registration, enter the following command:

```
config system interface
   edit port15
      set ap-discover disable
end
```

Enabling the automatic authorization of extension devices

To simplify adding FortiAP or FortiSwitch devices to your network, you can enable automatic authorization of devices as they are connected, instead of authorizing each one individually.

This feature is only configurable in the CLI.

To enable automatic authorization on all dedicated interfaces

```
config system global
   set auto-auth-extension-device enable
end
```

To enable automatic authorization per-interface

```
config system interface
```

```
   edit <port>
      set auto-auth-extension-device enable
end
```

Assigning the same FortiAP profile to multiple FortiAP units

The same profile can now be applied to multiple managed FortiAP units at the same time. To do this, do the following:

1. Go to **WiFi & Switch Controller > Managed FortiAPs** to view the AP list.
2. Select all FortiAP units you wish to apply the profile to.
3. Right click on one of the selected FortiAPs and select **Assign Profile**.
4. Choose the profile you wish to apply.

Overriding the FortiAP profile

In the FortiAP configuration **WiFi & Switch Controller > Managed FortiAPs**, there are several radio settings under **Override Radio 1** and **Override Radio 2**. You can choose to set a value independently of the FortiAP profile setting. When each of the radios are disabled, you will see what the FortiAP Profile has each of the settings configured to.

Band	The available options depend on the capability of the radio. Overriding **Band** also overrides **Channel**s. Make appropriate settings in **Channels**.
Channels	Choose channels. The available channels depend on the Band.
TX Power Control	If you enable **Auto**, adjust to set the power range in dBm. If you enable **Manual**, adjust the slider. The 100% setting is the maximum power permitted in your region. See Setting your geographic location on page 17.
SSIDs	Select **Auto** or **Manual**. Selecting **Auto** eliminates the need to re-edit the profile when new SSIDs are created. However, you can still select SSIDs individually using **Manual**.

To override radio settings in the CLI

In this example, Radio 1 is set to 802.11n on channel 11, regardless of the profile setting.

```
config wireless-controller wtp
   edit FP221C3X14019926
      config radio-1
         set override-band enable
         set band 802.11n
         set override-channel enable
         set channel 11
      end
```

You can override settings for band, channel, vaps (SSIDs), and TX power.

Outside of configuring radio settings, you can also override FortiAP LED state, WAN port mode, IP Fragmentation prevention method, spectrum analysis, split tunneling, and login password settings.

FortiAP CLI access

This section explains how to access the FortiAP CLI through the FortiAP Ethernet port or the FortiGate.

Accessing the FortiAP CLI through the FortiAP Ethernet port

The FortiAP unit has a CLI through which some configuration options can be set.

To access the FortiAP CLI through the FortiAP Ethernet port

1. Connect your computer to the FortiAP Ethernet interface, either directly with a cross-over cable or through a separate switch or hub.
2. Change your computer IP address to 192.168.1.3
3. Using SSH, connect to IP address 192.168.1.2.
4. Ensure that FortiAP is in a private network with no DHCP server for the static IP address to be accessible.
5. Login with user name admin and no password.
6. Enter commands, as needed.
7. Optionally, use the `passwd` command to assign an administrative password for better security.
8. Save the configuration by entering the following command:
   ```
   cfg -c .
   ```
9. Unplug the FortiAP and then plug it back in, in order for the configuration to take effect.

Accessing the FortiAP CLI through the FortiGate

After the FortiAP has been installed, physical access to the unit can be inconvenient. You can access the FortiAP CLI of a connected FortiAP unit through the FortiGate unit that controls it.

To access the FortiAP CLI through the FortiGate

1. In the FortiGate GUI, go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Right click the row of the FortiAP that you want to connect to and then select **>_ Connect to CLI**.
   The CLI Console window opens.
3. If the password prompt appears, then enter the required password. By default, there is no password.
4. When you are finished using the FortiAP CLI, enter `exit`.
5. To close the CLI Console window, click the X in the top right corner of the window.

FortiAP Configuration mode

To facilitate the initial deployment, you can reset FortiAP to enter the Configuration mode. With your Wi-Fi device, you can access the FortiAP Configuration mode GUI, and then configure FortiAP.

The FortiAP Configuration mode is available on FortiAP-S and FortiAP-W2, E models.

When FortiAP is in Configuration mode, the following behaviors apply:

- FortiAP broadcasts its SSID as FAP-config-<serial-number>.
- FortiAP does not broadcast any SSID configured by its controller.
- Only one WiFi client can connect to the broadcasted SSID.
- This SSID is open in NAT mode to allow internet connectivity.
- The transmit power for the broadcasted SSID is tuned down to 1 dBm on each radio, so the broadcasted SSID can only be connected to from a nearby location.
- FortiAP automatically exits the Configuration mode after 30 minutes or if you reboot FortiAP.

FortiAP enters the Configuration mode when you hold the reset button for 5 to 10 seconds while FortiAP is booted up.

Reset button behavior

Reset duration (seconds)	Action
less than 5	Reboot
5 to 10	Configuration mode
more than 10	Factory reset

Resetting FortiAP to enter the Configuration mode

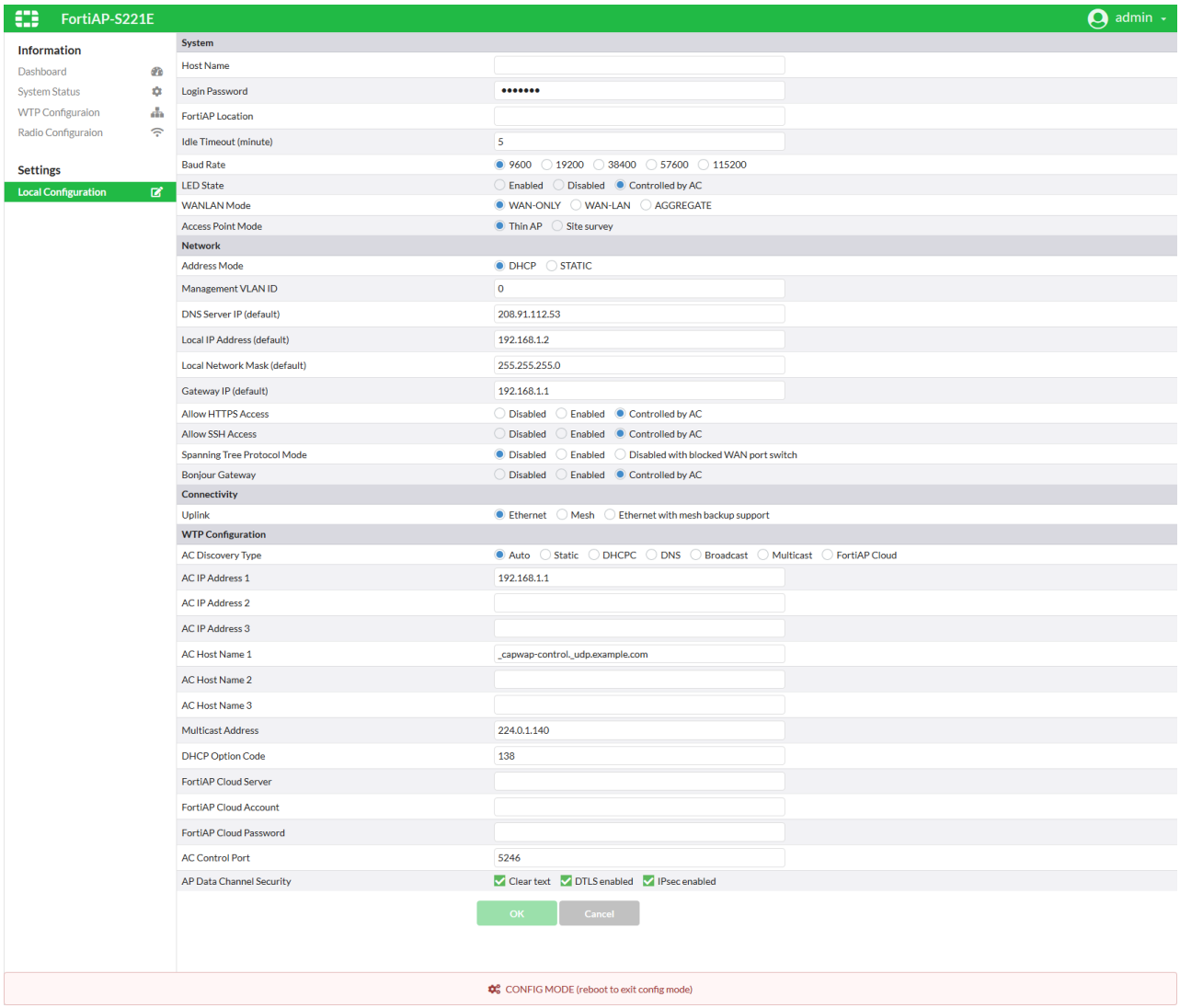
1. Make sure FortiAP is booted up.
2. Use a pin to push and hold the reset button for 5 to 10 seconds.
   FortiAP reboots and then enters the Configuration mode.
   FortiAP starts to broadcast an open security SSID FAP-config-<serial-number>, for example FAP-config-FP421E3X16000715.
3. You can now access the GUI or CLI of the FortiAP Configuration mode by performing:
   - the recommended procedure, Accessing the GUI of the FortiAP Configuration mode on page 50
   - or Accessing the CLI of the FortiAP Configuration mode on page 52

Accessing the GUI of the FortiAP Configuration mode

***Note**:* This is the recommended procedure.

1. Use only one Wi-Fi device to connect to the SSID FAP-config-<serial-number>.
2. Open a web browser and visit https://192.168.100.1.
3. In the **User Name** field, type admin.
4. In the **Password** field, type the password associated with the admin account.
   The FortiAP Dashboard window opens with a CONFIG MODE red banner at the bottom.
5. Under Settings, click **Local Configuration**.

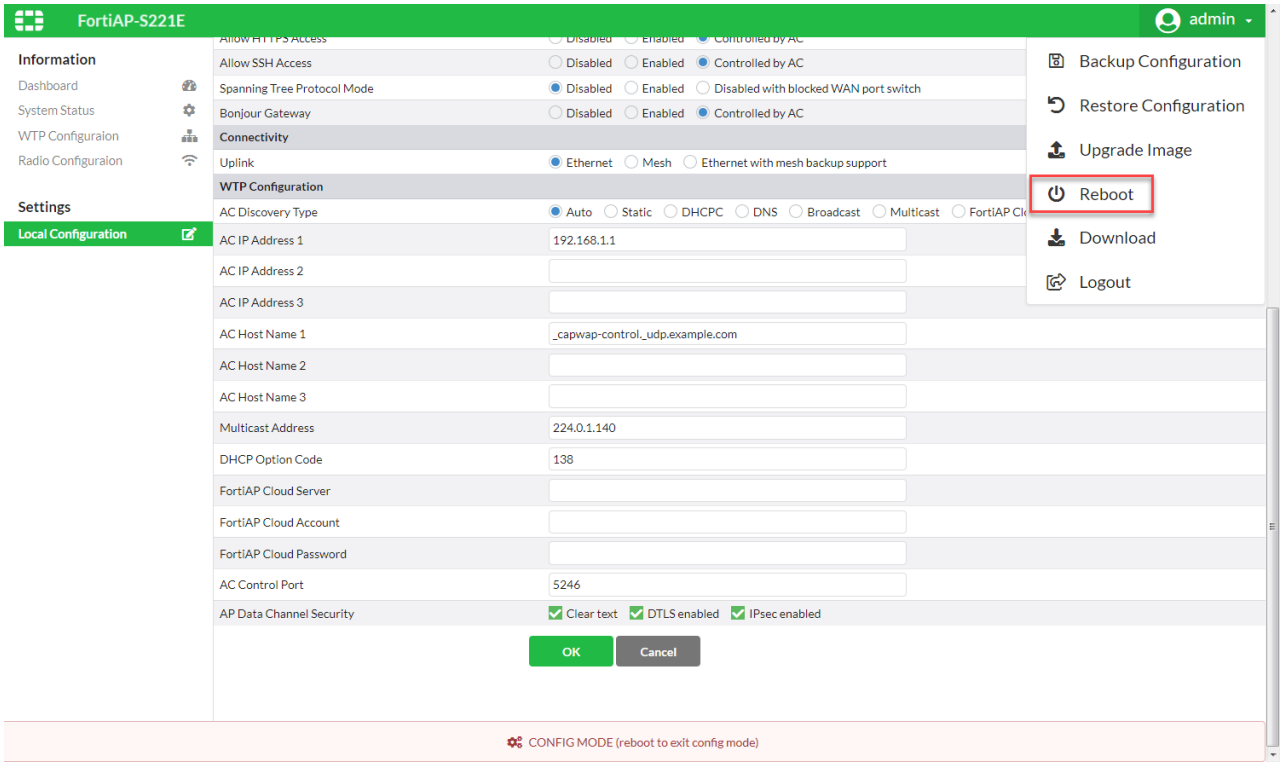
FortiAP Config Mode - Local Configuration



6. Make configuration changes.
7. To save configuration changes, click **OK**.

8. To exit the Configuration mode, go to the admin menu at the top-right corner and click **Reboot**.

FortiAP Config Mode - Reboot



9. To confirm the system reboot, click **Yes**.
10. When the web browser displays a System Rebooting message, you can close the web browser window. Configuration changes take effect after FortiAP restarts.

Accessing the CLI of the FortiAP Configuration mode

1. To connect to FortiAP, you can:
   a. start a secure shell (SSH) session with the IP address of the FortiAP, or
   b. start a console session, if your FortiAP has a console port.
2. Use *admin*, as the login user.
3. Type the password associated with the admin account.
4. Make configuration changes. For details about FortiAP CLI commands, see FortiAP CLI configuration and diagnostics commands on page 159.
5. To save configuration changes, type:

   ```
   cfg -c
   ```

6. To exit the Configuration mode, type:

   ```
   reboot
   ```

   Configuration changes take effect after FortiAP restarts.

FortiAP unit firmware upgrade

You can view and upgrade the FortiAP unit firmware from the FortiGate unit that acts as its WiFi controller.

Checking the FortiAP unit firmware version

To view the list of FortiAP units that the FortiGate unit manages, go to **WiFi & Switch Controller > Managed FortiAPs**. The **OS Version** column shows the current firmware version running on each AP.

Upgrading FortiAP firmware from the FortiGate unit

You can upgrade the FortiAP firmware using either the GUI or the CLI. Only the CLI method can update all FortiAP units at once.

To upgrade FortiAP unit firmware - GUI

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Right-click the FortiAP unit in the list and select **Upgrade**.
   or
   Click the row of the FortiAP that you want to upgrade, and click **Edit**. In Firmware, click **Upgrade**.
3. Upgrade using FortiGuard, or select **Browse** and locate the firmware upgrade file.
4. Click **Upgrade**.
5. When the upgrade process completes, select **OK**.
   The FortiAP unit restarts.

To upgrade FortiAP unit firmware - CLI

1. Upload the FortiAP image to the FortiGate unit.
   For example, the Firmware file is FAP_22A_v4.3.0_b0212_fortinet.out and the server IP address is 192.168.0.100.
   ```
   execute wireless-controller upload-wtp-image tftp FAP_22A_v4.3.0_b0212_fortinet.out
        192.168.0.100
   ```
   If your server is FTP, change `tftp` to `ftp`, and if necessary add your user name and password at the end of the command.
2. Verify that the image is uploaded:
   ```
   execute wireless-controller list-wtp-image
   ```
3. Upgrade the FortiAP units:
   ```
   exec wireless-controller reset-wtp all
   ```
   If you want to upgrade only one FortiAP unit, enter its serial number instead of `all`.

Upgrading FortiAP firmware from the FortiAP unit

You can connect to a FortiAP unit's internal CLI to update its firmware from a TFTP server on the same network. This method does not require access to the wireless controller.

1. Place the FortiAP firmware image on a TFTP server on your computer.
2. Connect the FortiAP unit to a separate private switch or hub or directly connect to your computer via a cross-over cable.
3. Change your computer IP address to 192.168.1.3.
4. Using SSH, connect to IP address 192.168.1.2.
   This IP address is overwritten if the FortiAP is connected to a DHCP environment. Ensure that the FortiAP unit is in a private network with no DHCP server.
5. Login with the username “admin” and no password.
6. Enter the following command.
   For example, the FortiAP image file name is FAP_22A_v4.3.0_b0212_fortinet.out.
   ```
   restore FAP_22A_v4.3.0_b0212_fortinet.out 192.168.1.3
   ```

Advanced WiFi controller discovery

A FortiAP unit can use any of six methods to locate a controller. By default, FortiAP units cycle through all six of the discovery methods. In most cases there is no need to make configuration changes on the FortiAP unit.

There are exceptions. The following section describes the WiFi controller discovery methods in more detail and provides information about configuration changes you might need to make so that discovery will work.

Controller discovery methods

There are six methods that a FortiAP unit can use to discover a WiFi controller. Below is the list of AC discovery methods used in sequence, if the FortiAP discovery type is set to auto:

1(static) → 2(dhcp) → 3(dns) → 7(fortiapcloud) → 5(multicast) → 6(broadcast)

For every discovery type, FortiAP sends out discovery requests and sets a timer, an interval defined as a random number of seconds (between 2 and 180, default is 5 seconds), which is set via the CLI:

CLI syntax

```
config wireless-controller timers
   set discovery-interval 5
end
```

After the timeout is reached, FortiAP sends out another discovery request, up to a maximum of 3 times.

After about 3 - 15 seconds, if FortiAP has no AC connection, it will switch to another discovery type and repeat the above process until the last one (**broadcast**) fails, which will lead to SULKING state.

After about 30 seconds, FortiAP will go into an AC_IP_DISCVER state. After the AC IP is found, it will go to IDLE state, and will eventually go to the DISCOVERY state, and repeat the above process again.

Note that, while the process above is showcasing the auto discovery method, it's recommended to set the AC_DISCOVERY_TYPE to your used method in order to reduce downtime.

Static IP configuration

If FortiAP and the controller are not in the same subnet, broadcast and multicast packets cannot reach the controller. The admin can specify the controller's static IP on the AP unit. The AP unit sends a discovery request message in unicast to the controller. Routing must be properly configured in both directions.

To specify the controller's IP address on a FortiAP unit

```
cfg -a AC_IPADDR_1="192.168.0.100"
```

By default, the FortiAP unit receives its IP address, netmask, and gateway address by DHCP. If you prefer, you can assign these statically.

To assign a static IP address to the FortiAP unit

```
cfg -a ADDR_MODE=STATIC
cfg -a AP_IPADDR="192.168.0.100"
cfg -a AP_NETMASK="255.255.255.0"
cfg -a IPGW=192.168.0.1
cfg -c
```

For information about connecting to the FortiAP CLI, see FortiAP CLI access on page 49.

DHCP

If you use DHCP to assign an IP address to your FortiAP unit, you can also provide the WiFi controller IP address at the same time. This is useful if the AP is located remotely from the WiFi controller and other discovery techniques will not work. Since the AP sequentially goes through all the different discovery methods, DHCP has the best ratio between configuration and time for discovery.

When you configure the DHCP server, configure Option 138 to specify the WiFi controller IP address(es). The most direct method is to input an IP address in hexadecimal format. For example, 192.168.0.1 converts to C0A80001.

For DHCP servers that support inputting other option types, you can select the "IP" type and then input a regular IP address.

You can also input multiple addresses (concatenated in hexadecimal format). The first address has the highest priority.

If Option 138 is used for some other purpose on your network, you can use a different option number if you configure the AP units to match.

To change the FortiAP DHCP option code

To use option code 139 for example, enter

```
cfg -a AC_DISCOVERY_DHCP_OPTION_CODE=139
```

For information about connecting to the FortiAP CLI, see FortiAP CLI access on page 49.

DNS

The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response. Allow DNS lookup of the hostname configured in the AP by using the AP parameter "`AC_HOSTNAME_1`".

By default, the `AC_HOSTNAME_1` parameter is set to `_capwap-control._udp.example.com`.

To change the default parameter

1. From the FortiAP CLI, enter the following commands:
   ```
   cfg -a AC_HOSTNAME_1=<yourcompany.com>
   cfg -c
   ```
2. Add an A record to the DNS server to resolve the configured domain.

FortiAP Cloud

The access point can discover FortiAP Cloud by doing a DNS lookup of the hardcoded FortiAP Cloud AP controller hostname "apctrl1.fortinet.com". The FortiAP Cloud AC discovery technique finds the AC info from apctl1.fortinet.com using HTTPS.

FortiAP Cloud - APController: `apctrl1.fortinet.com:443 208.91.113.187:443`

Broadcast request

The AP unit broadcasts a discovery request message to the network and the controller replies. The AP and the controller must be in the same broadcast domain. No configuration adjustments are required.

Multicast request

The AP unit sends a multicast discovery request and the controller replies with a unicast discovery response message. The AP and the controller do not need to be in the same broadcast domain if multicast routing is properly configured.

The default multicast destination address is 224.0.1.140. It can be changed through the CLI. The address must be same on the controller and AP.

To change the multicast address on the controller

```
config wireless-controller global
   set discovery-mc-addr 224.0.1.250
end
```

To change the multicast address on a FortiAP unit

```
cfg -a AC_DISCOVERY_MC_ADDR="224.0.1.250"
```

For information about connecting to the FortiAP CLI, see FortiAP CLI access on page 49.

Wireless client load balancing for high-density deployments

Wireless load balancing allows your wireless network to distribute wireless traffic more efficiently among wireless access points and available frequency bands. FortiGate wireless controllers support the following types of client load balancing:

- Access point handoff - the wireless controller signals a client to switch to another access point.
- Frequency handoff - the wireless controller monitors the usage of 2.4 GHz and 5 GHz bands, and signals clients to switch to the lesser-used frequency.

Load balancing is not applied to roaming clients.

Access point handoff

Access point handoff wireless load balancing involves the following:

- If the load on an access point (ap1) exceeds a threshold (of for example, 30 clients) then the client with the weakest signal will be signaled by wireless controller to drop off and join another nearby access point (ap2).
- When one or more access points are overloaded (for example, more than 30 clients) and a new client attempts to join a wireless network, the wireless controller selects the least busy access point that is closest to the new client and this access point is the one that responds to the client and the one that the client joins.

Frequency handoff or band-steering

Encouraging clients to use the 5 GHz WiFi band if possible enables those clients to benefit from faster interference-free 5GHz communication. The remaining 2.4 GHz clients benefit from reduced interference.

The WiFi controller probes clients to determine their WiFi band capability. It also records the RSSI (signal strength) for each client on each band.

If a new client attempts to join the network, the controller looks up that client's MAC address in its wireless device table and determines if it is a dual band device. If it is not a dual band device, then it is allowed to join. If it is a dual band device, then its RSSI on 5 GHz is used to determine whether the device is close enough to an access point to benefit from movement to 5 GHz frequency.

If both conditions of 1) dual band device and 2) RSSI value is strong, then the wireless controller does not reply to the join request of the client. This forces the client to retry a few more times and then timeout and attempt to join the same SSID on 5 GHz. Once the Controller see this new request on 5 GHz, the RSSI is again measured and the client is allowed to join. If the RSSI is below threshold, then the device table is updated and the controller forces the client to timeout again. A client's second attempt to connect on 2.4 GHz will be accepted.

Handoff configuration

From the GUI, edit a custom AP profile and select **Frequency Handoff** and **AP Handoff** as required for each radio on the AP.

From the CLI, you configure wireless client load balancing thresholds for each custom AP profile. Enable access point handoff and frequency handoff separately for each radio in the custom AP profile.

```
config wireless-controller wtp-profile
   edit new-ap-profile
      set handoff-rssi <rssi_int>
```

```
      set handoff-sta-thresh <clients_int>
      config radio-1
         set frequency-handoff {disable | enable}
         set ap-handoff {disable | enable}
      end
      config radio-2
         set frequency-handoff {disable | enable}
         set ap-handoff {disable | enable}
      end
   end
```

Where:

- `handoff-rssi` is the RSSI threshold. Clients with a 5 GHz RSSI threshold over this value are load balanced to the 5 GHz frequency band. Default is 25. Range is 20 to 30.
- `handoff-sta-thresh` is the access point handoff threshold. If the access point has more clients than this threshold it is considered busy and clients are changed to another access point. Default is 30, range is 5 to 25.
- `frequency-handoff` enable or disable frequency handoff load balancing for this radio. Disabled by default.
- `ap-handoff` enable or disable access point handoff load balancing for this radio. Disabled by default.

Frequency handoff must be enabled on the 5 GHz radio to learn client capability.

FortiAP groups

FortiAP groups facilitate the application of FortiAP profiles to large numbers of FortiAPs. A FortiAP can belong to no more than one FortiAP group. A FortiAP group can include only one model of FortiAP.

Through the VLAN pool feature, a FortiAP group can be associated with a VLAN to which WiFi clients will be assigned. For more details about VLAN pool assignment, see VLAN assignment by VLAN pool on page 33.

To create a FortiAP group - GUI

1. Go to **WiFi & Switch Controller > Managed FortiAPs** and select **Create New > Managed AP Group**.
2. Give the group a **Name**.
3. Choose **Members**.
4. Click **OK**.

To create a FortiAP group - CLI

In this example, `wtp-group-1` is created for a FortiAP-221C and one member device is added.

```
config wireless-controller wtp-group
   edit wtp-group-1
      set platform-type 221C
      config wtp-list
         edit FP221C3X14019926
      end
   end
```

LAN port options

FortiAPs have at least one Ethernet port that operates as a WAN port to provide management connection to a WiFi Controller such as FortiGate or FortiAP Cloud. Some FortiAP models have multiple LAN ports that can provide wired network access.

There are some differences in LAN configuration among FortiAP models.

FortiAP models, including FAP-21D, FAP-24D, and FAP-C24JE, have one WAN port and one or more LAN ports. By default, the LAN ports are offline. You can directly configure LAN port operation via the web UI of a WiFi Controller, or in the FortiGate CLI (`config wireless-controller wtp-profile` > `config lan`).

FortiAP models, including FAP-320C, FAP-421E, and FAP-U421EV, have two ports, labeled LAN1 and LAN2. By default, LAN1 and LAN2 are direct pass-through ports, and can work as the WAN interface. When necessary, the LAN1 and LAN2 ports can be re-configured for WAN-LAN operation.

This section covers the following topics:

- Configuring a port to WAN-LAN operation mode on page 59
- Bridging a LAN port with an SSID on page 60
- Bridging a LAN port with the WAN port on page 60
- Configuring FortiAP LAN ports on page 60

Configuring a port to WAN-LAN operation mode

Some FortiAP models have two LAN ports instead of having both a WAN port and a LAN port. You can configure one of the LAN ports to operate under the WAN-LAN mode. To configure a port to WAN-LAN operation, you must first configure the CLI in the FortiGate, and then in the CLI of the FortiAP.

To configure a port to WAN-LAN operation

1. Access the FortiGate CLI.
2. Select the "`wan-lan`" option in the `wtp-profile`, for example:

   ```
   config wireless-controller wtp-profile
      edit <profile_name>
         set wan-port-mode wan-lan
      end
   ```

   By default, the `wan-port-mode` is set to `wan-only`.

   Once the `wan-port-mode` is set to `wan-lan`, LAN Port options become available in the web UI and the CLI of WiFi controller, similar to FortiAP models that have labeled WAN and LAN ports.
3. Access the FortiAP CLI (see FortiAP CLI access on page 49).
4. Enable the WAN-LAN mode. The method varies depending on the FortiAP model type.
   - Enabling WAN-LAN mode on FortiAP, FortiAP-S, and FortiAP-W2 models:

     ```
     cfg -a WANLAN_MODE=WAN-LAN
     cfg -c
     ```

     Note: By default, `WANLAN_MODE` is set to `WAN-ONLY`.
   - Enabling WAN-LAN mode on FortiAP-U models:

     ```
     cfg -a FAP_ETHER_TRUNK=3
     ```

```
cfg -c
```

Note: By default, `FAP_ETHER_TRUNK` is set to `0`.

5. Once the WiFi Controller and the FortiAP are both configured, LAN1 will work as the WAN interface and LAN2 will work as the LAN interface.

Bridging a LAN port with an SSID

Bridging a LAN port with a FortiAP SSID combines traffic from both sources to provide a single broadcast domain for wired and wireless users.

In this configuration:

- The IP addresses for LAN clients come from the DHCP server that serves the wireless clients.
- Traffic from LAN clients is bridged to the SSID's VLAN. Dynamic VLAN assignment for hosts on the LAN port is not supported.
- Wireless and LAN clients are on the same network and can communicate locally, via the FortiAP.
- Any host connected to the LAN port will be taken as authenticated. RADIUS MAC authentication for hosts on the LAN port is not supported.

For configuration instructions, see Configuring FortiAP LAN ports on page 60.

Bridging a LAN port with the WAN port

Bridging a LAN port with the WAN port enables the FortiAP unit to be used as a hub which is also an access point.

In this configuration

- The IP addresses for LAN clients come from the WAN directly and will typically be in the same range as the AP itself.
- All LAN client traffic is bridged directly to the WAN interface.
- Communication between wireless and LAN clients can only occur if a policy on the FortiGate unit allows it.

For configuration instructions, see Configuring FortiAP LAN ports on page 60.

Configuring FortiAP LAN ports

You can configure FortiAP LAN ports for APs through a FortiAP Profile. A profile applies to APs that are the same model and share the same configuration. If you have multiple models or different configurations, you might need to create several FortiAP Profiles. You can also override FortiAP Profile configurations by editing the individual AP directly.

Configuring FortiAP LAN ports using profiles

FortiAP profiles apply configurations to multiple APs of the same model.

To configure FortiAP LAN ports - GUI

1. If your FortiAP unit has LAN ports, but no WAN ports, enable LAN port options in the CLI. See Configuring a port to WAN-LAN operation mode on page 59.
2. Go to **WiFi & Switch Controller > FortiAP Profiles**.

3. Edit the default profile for your FortiAP model or select **Create New**.
4. If you are creating a new profile, enter a **Name** and select the correct **Platform** (model).
5. Select SSIDs.
6. In the **LAN Port** section, set **Mode** to **Bridge to** and select an SSID or **WAN Port** as needed.
   On some models with multiple LAN ports, you can set **Mode** to **Custom** and configure the LAN ports individually. Enable each port that you want to use and select an SSID or **WAN Port** as needed.
7. Select **OK**.

Be sure to select this profile when you authorize your FortiAP units.

To configure FortiAP LAN ports - CLI

In this example, the default FortiAP-11C profile is configured to bridge the LAN port to the office SSID.

```
config wireless-controller wtp-profile
   edit FAP11C-default
      config lan
         set port-mode bridge-to-ssid
         set port-ssid office
      end
   end
end
```

In this example, the default FortiAP-28C profile is configured to bridge LAN port1 to the office SSID and to bridge the other LAN ports to the WAN port.

```
config wireless-controller wtp-profile
   edit FAP28C-default
      config lan
         set port1-mode bridge-to-ssid
         set port1-ssid office
         set port2-mode bridge-to-wan
         set port3-mode bridge-to-wan
         set port4-mode bridge-to-wan
         set port5-mode bridge-to-wan
         set port6-mode bridge-to-wan
         set port7-mode bridge-to-wan
         set port8-mode bridge-to-wan
      end
   end
```

In this example, the default FortiAP-320C profile is configured to bridge the LAN port to the office SSID.

```
config wireless-controller wtp-profile
   edit FAP320C-default
      set wan-port-mode wan-lan
      config lan
         set port-mode bridge-to-ssid
         set port-ssid office
      end
   end
end
```

Configuring individual FortiAP LAN ports

For an individual AP, you can override the FortiAP profile settings by editing device configurations directly.

To override FortiAP Profile LAN port configurations - GUI

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Select the FortiAP unit from the list and select **Edit**.
3. Select the **FortiAP Profile**, if this has not already been done.
4. In the **LAN Port** section, select **Override**.
   The options for **Mode** are shown.
5. Set **Mode** to **Bridge to** and select an SSID or **WAN Port**, or **NAT to WAN** as needed.
   On some models with multiple LAN ports, you can set **Mode** to **Custom** and configure the LAN ports individually. Enable and configure each port that you want to use.
6. Select **OK**.

To override FortiAP Profile LAN port configurations - GUI

In this example, a FortiAP unit's configuration overrides the FortiAP Profile to bridge the LAN port to the office SSID.

```
config wireless-controller wtp
   edit FP320C3X14020000
      set wtp-profile FAP320C-default
      set override-wan-port-mode enable
      set wan-port-mode wan-lan
      set override-lan enable
      config lan
         set port-mode bridge-to-ssid
         set port-ssid office
      end
   end
```

Aggregating multiple LAN ports

Certain FortiAP models including FAP-320C, FAP-421E, and FAP-U421EV, have two ports, labeled LAN1 and LAN2. These ports can be re-configured to function as one aggregated link, per IEEE 802.3ad Link Aggregation Control Protocol (LACP), allowing data traffic across both ports to increase the overall throughput and support redundancy.

Note: You can only enable the Link Aggregation Control Protocol (LACP) from the FortiAP CLI. The commands for enabling LACP differ depending on the FortiAP model type.

To enable LACP on a FortiAP, FortiAP-S, or FortiAP-W2 model - CLI

1. Access the CLI of your FortiAP (see FortiAP CLI access on page 49).
2. In the FortiAP CLI, set the `WANLAN_MODE` parameter to `AGGREGATE` by entering the following command:
   ```
   cfg -a WANLAN_MODE=AGGREGATE
   ```
   Note: By default, `WANLAN_MODE` is set to `WAN-ONLY`.
3. Save the changes to the device flash with the following command:
   ```
   cfg -c
   ```

To enable LACP on a FortiAP U model - CLI

1. Access the CLI of your FortiAP (see FortiAP CLI access on page 49).
2. In the FortiAP CLI, set the `FAP_ETHER_TRUNK` parameter to `2` by entering the following command:
   ```
   cfg -a FAP_ETHER_TRUNK=2
   ```
   Note: By default, `FAP_ETHER_TRUNK` is set to `0`.
3. Save the changes to the device flash with the following command:
   ```
   cfg -c
   ```

IP fragmentation of packets in CAPWAP tunnels

A common problem with controller-based WiFi networks is reduced performance due to IP fragmentation of packets in the CAPWAP tunnel.

Fragmentation can occur because of CAPWAP tunnel overhead increasing packet size. If the original wireless client packets are close to the maximum transmission unit (MTU) size for the network (usually 1500 bytes for Ethernet networks unless jumbo frames are used) the resulting CAPWAP packets may be larger than the MTU, causing the packets to be fragmented. Fragmenting packets can result in data loss, jitter, and decreased throughput.

The FortiOS/FortiAP solution to this problem is to cause wireless clients to send smaller packets to FortiAP devices, resulting in 1500-byte CAPWAP packets and no fragmentation. The following options configure CAPWAP IP fragmentation control:

```
config wireless-controller wtp-profile
   edit FAP321C-default
      set ip-fragment-preventing {tcp-mss-adjust | icmp-unreachable}
      set tun-mtu-uplink {0 | 576 | 1500}
      set tun-mtu-downlink {0 | 576 | 1500}
   end
end
```

By default, `tcp-mss-adjust` is enabled, `icmp-unreachable` is disabled, and `tun-mtu-uplink` and `tun-mtu-downlink` are set to 0.

To set `tun-mtu-uplink` and `tun-mtu-downlink`, use the default TCP MTU value of 1500. This default configuration prevents packet fragmentation because the FortiAP unit limits the size of TCP packets received from wireless clients so the packets don't have to be fragmented before CAPWAP encapsulation.

The `tcp-mss-adjust` option causes the FortiAP unit to limit the maximum segment size (MSS) of TCP packets sent by wireless clients. The FortiAP does this by adding a reduced MSS value to the SYN packets sent by the FortiAP unit when negotiating with a wireless client to establish a session. This results in the wireless client sending packets that are smaller than the `tun-mtu-uplink` setting, so that when the CAPWAP headers are added, the CAPWAP packets have an MTU that matches the `tun-mtu-uplink` size.

The `icmp-unreachable` option affects all traffic (UDP and TCP) between wireless clients and the FortiAP unit. This option causes the FortiAP unit to drop packets that have the "Don't Fragment" bit set in their IP header and that are large enough to cause fragmentation and then send an ICMP packet -- type 3 "ICMP Destination unreachable" with code 4 "Fragmentation Needed and Don't Fragment was Set" back to the wireless controller. This should cause the wireless client to send smaller TCP and UDP packets.

Overriding IP fragmentation settings on a FortiAP

If the FortiAP Profile settings for IP fragmentation are not appropriate for a particular FortiAP, you can override the settings on that specific unit.

```
config wireless-controller wtp
   edit FAP321C3X14019926
      set override-ip-fragment enable
      set ip-fragment-preventing {tcp-mss-adjust | icmp-unreachable}
      set tun-mtu-uplink {0 | 576 | 1500}
      set tun-mtu-downlink {0 | 576 | 1500}
   end
end
```

CAPWAP bandwidth formula

The following section provides information on how to calculate the control plane CAPWAP traffic load in local bridging. The formula provided can help estimate the approximate package bandwidth cost. This is important for knowing precisely how much bandwidth is required on a WAN link for a centralized FortiGate managing hundreds of access points.

There are multiple factors that might affect the volume of CAPWAP control traffic, including the number of stations there are and large WiFi events.

The Ethernet/IP/UDP/CAPWAP uplink header cost should be approximately 66 bytes.

The tables below depict basic and commonly used optional CAPWAP bandwidth costs, on a per-AP basis.

Note the following:

- **STA:** The number of stations associated with the FortiAP.
- **ARP scan:** Finds hidden devices in your network.
- **VAP:** The number of VAPS held by the FortiAP.
- **Radio:** The number of radios (maximum of two) enabled by the FortiAP.

Basic per-AP CAPWAP bandwidth costs

Content	Time (seconds)	Payload (byte)	Package bandwidth cost (bps)
Echo Req	30	16	(66+16)*8/30=21.86
STA scan	30	25+20*sta	(66+25+20*sta)*8/30=24.26+5.3*sta
ARP scan	30	25+18*sta	(66+25+18*sta)*8/30=24.26+4.8*sta
STA CAP	30	25+19*sta	(66+25+19*sta)*8/30=24.26+5.1*sta
STA stats	1	25+41*sta	(66+25+41*sta)*8/1=728.0+328.0*sta
VAP stats	15	40+18*vap	(66+40+18*vap)*8/15=56.53+9.6*vap
Radio stats	15	25+25*radio	(66+25+25*radio)*8/15=48.53+13.3*radio

Content	Time (seconds)	Payload (byte)	Package bandwidth cost (bps)
Total:			908.7+343.2*sta+9.6*vap+13.3*radio

Commonly used optional per-AP CAPWAP bandwidth costs

Content	Time (seconds)	Payload (byte)	Package bandwidth cost (bps)
AP scan	30	25+63*scanned-ap	(66+25+63*scanned-ap)*8/30=24.26+16.8*scanned-ap
Total:			932.96+343.2*sta+9.6*vap+13.3*radio+16.8*scanned-ap

Enabling WIDS features, LLDP, MESH, FortiPresence, and Client Station Locating Service can lead to additional bandwidth consumption.

Example:

There are 100 FortiAPs, with 187 stations distributed among them. Each FortiAP holds five VAPs among their radios, and each enables two radios. The basic CAPWAP bandwidth cost would be:

908.7*100+343.2*187+9.6*5*100+13.3*2*100 = **162.51 kbps**

Additionally, if two FortiAPs enabled "AP scan", and suppose one scans 99 APs in each scan and the other scans 20 APs in each scan, the additional CAPWAP bandwidth cost would be:

(24.26+16.8*99)+(24.26+16.8*20) = **2 kbps**

LLDP protocol

The LLDP protocol is enabled by default when you create a new FortiAP profile. Each FortiAP using that profile can then send back information about the switch and port that it is connected to. You can also manage the LLDP protocol in the FortiAP Profile via the CLI.

To enable LLDP, enter the following:

```
config wireless-controller wtp-profile
   edit <profile-name>
      set lldp enable
end
```

LED options

Optionally, the status LEDs on FortiAP can be kept dark. This is useful in dormitories, classrooms, hotels, medical clinics, and hospitals where lights can distract or annoy occupants.

On FortiGate, the LED state is controlled in the FortiAP Profile. By default the LEDs are enabled. The setting is CLI-only. For example, to disable the LEDs on FortiAP-221C units controlled by the FAP221C-default profile, enter:

```
config wireless-controller wtp-profile
   edit FAP221C-default
      set led-state disable
   end
```

You can override the FortiAP Profile LED state setting on an individual FortiAP using the CLI. For example, to make sure the LEDs are disabled on one specific unit, enter:

```
config wireless-controller wtp
   edit FAP221C3X14019926
      set override-led-state enable
      set led-state disable
   end
```

The LED state is also controllable from the FortiAP unit itself. By default, the FortiAP follows the FortiAP Profile setting.

LED schedules

Use the command below (`led-schedule`) to assign recurring firewall schedules for illuminating LEDs on the FortiAP. This entry is only available when `led-state` is enabled, at which point LEDs will be visible when at least one of the schedules is valid.

Separate multiple schedule names with a space, as configured under `config firewall schedule group` and `config firewall schedule recurring`.

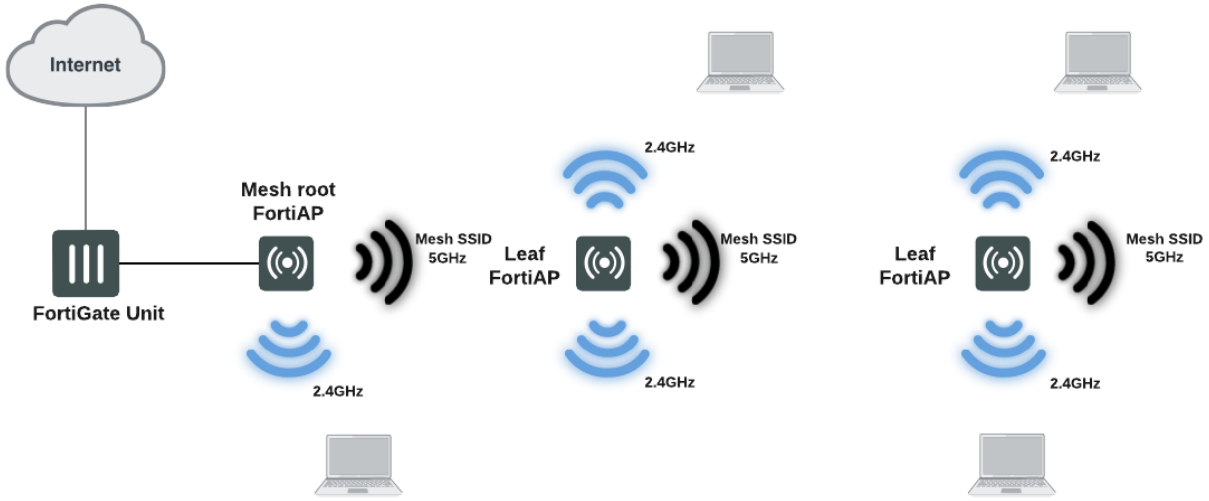
Syntax

```
config wireless-controller wtp-profile
   edit {name}
      set led-state {enable | disable}
      set led-schedules <name>
   next
end
```

Wireless mesh configuration

The access points of a WiFi network are usually connected to the WiFi controller through Ethernet wiring. A wireless mesh eliminates the need for Ethernet wiring by connecting WiFi access points to the controller by radio. This is useful where installation of Ethernet wiring is impractical.

Wireless mesh topology



A wireless mesh is a multiple access point (AP) network in which only one FortiAP unit is connected to the wired network. The other FortiAPs communicate with the controller over a separate backhaul SSID that isn't available to regular WiFi clients. The AP connected to the network by Ethernet is called the mesh root node. The backhaul SSID carries CAPWAP discovery, configuration, and other communications that would usually be carried on an Ethernet connection.

The root node can be a FortiAP unit or the built-in AP of a FortiWiFi unit. APs that serve regular WiFi clients are called leaf nodes. Leaf APs also carry the mesh SSID for more distant leaf nodes. A leaf node can connect to the mesh SSID directly from the root node or from any of the other leaf nodes. This provides redundancy in case of an AP failure.

All access points in a wireless mesh configuration must have at least one of their radios configured to provide mesh backhaul communication. As with wired APs, when mesh APs start up, they can be discovered by a FortiGate or FortiWiFi unit WiFi controller and authorized to join the network.

The backhaul SSID delivers the best performance when it is carried on a dedicated radio. On a two-radio FortiAP unit, for example, the 5 GHz radio could carry only the backhaul SSID while the 2.4 GHz radio carries one or more SSIDs that serve users. You can configure background WiFi scanning in this mode.

The backhaul SSID can also share the same radio with SSIDs that serve users. Performance is reduced because the backhaul and user traffic compete for the available bandwidth. Background WiFi scanning isn't available in this mode. One advantage of this mode is that a two-radio AP can offer WiFi coverage on both bands.

Wireless mesh deployment modes

There are two common wireless mesh deployment modes:

Wireless mesh	Access points are connected to a FortiGate or FortiWiFi unit WiFi controller. WiFi users connect to wireless SSIDs in the same way as on non-mesh WiFi networks.
Wireless bridging	Two LAN segments are connected together over a wireless link (the backhaul SSID). On the leaf AP, the Ethernet connection can be used to provide a wired network. Both WiFi and wired users on the leaf AP are connected to the LAN segment to which the root AP is connected.

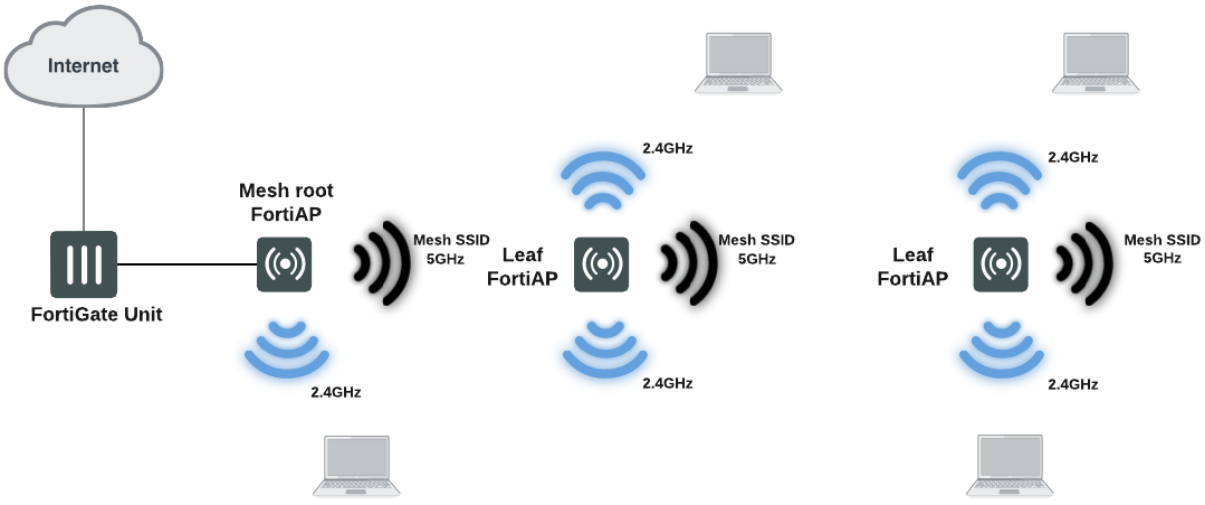
Firmware requirements

All FortiAP units that are part of the wireless mesh network must be upgraded to FortiAP firmware version 5.0, build 003, or higher. FortiAP-222B units must have their BIOS upgraded to version 400012. The FortiWiFi or FortiGate unit used as the WiFi controller must be running FortiOS firmware version 5.0 or higher.

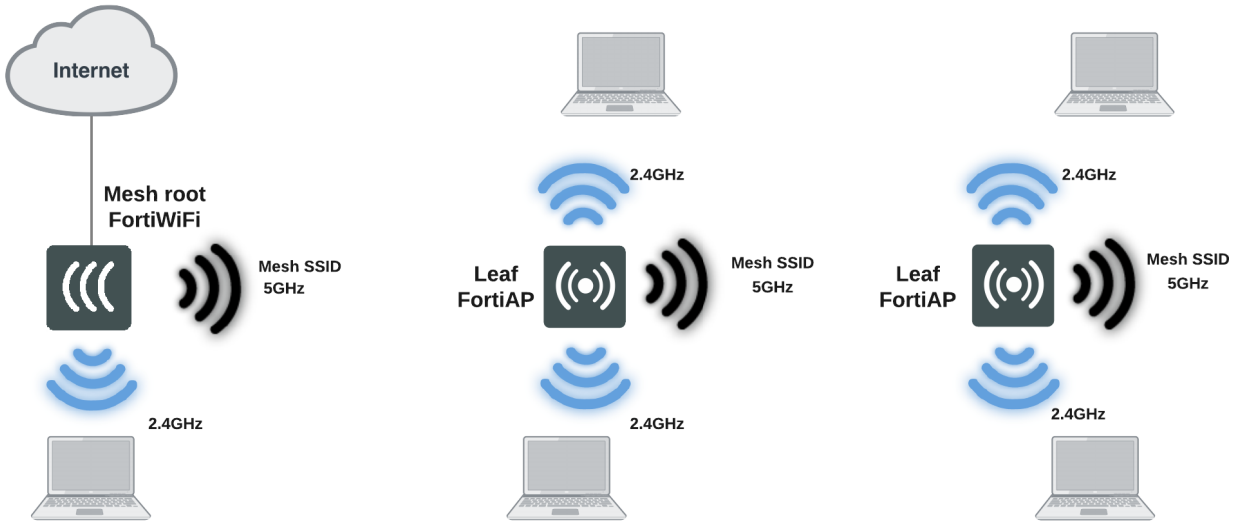
Types of wireless mesh

A WiFi mesh can provide access to widely-distributed clients. The mesh root AP which is directly connected to the WiFi controller can be either a FortiAP unit or the built-in AP of a FortiWiFi unit that is also the WiFi controller.

FortiAP units used as both mesh root AP and leaf AP

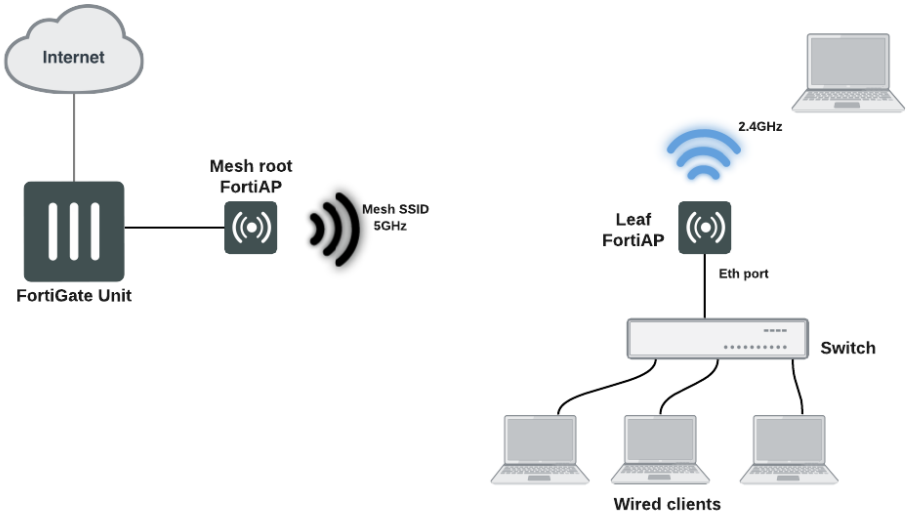


FortiWiFi unit as mesh root AP with FortiAP units as leaf APs



An alternate use of the wireless mesh is as a point-to-point relay. Both wired and WiFi users on the leaf AP side are connected to the LAN segment on the mesh root side.

Point-to-point wireless mesh



Fast-roaming for mesh backhaul link

Mesh implementations for leaf FortiAP can perform background scanning when the leaf AP is associated with the root. Various options for background scanning can be configured with the CLI. For more details about the mesh variables available in the FortiAP CLI, see Mesh variables on page 161

Configuring a meshed WiFi network

To configure a mesh WiFi network, perform the following tasks:

- Creating the mesh root SSID on page 70
- Creating the FortiAP profile on page 70
- Configuring the mesh root AP on page 71
- Configuring the mesh leaf FortiAPs on page 72
- Authorizing leaf APs on page 73
- Creating security policies on page 73
- Viewing the status of the mesh network on page 73

This section assumes that the end-user SSIDs already exist.

Creating the mesh root SSID

The mesh route SSID is the radio backhaul that conveys the user SSID traffic to the leaf FortiAPs.

To configure the mesh root SSID

1. Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID**.
2. Enter a **Name** for the WiFi interface.
3. In **Traffic Mode**, select **Mesh Downlink**.
4. Enter the **SSID**.
5. Set **Security Mode** to **WPA2 Personal** and enter the **Pre-shared key**.
   Remember the key because you need to enter it for the leaf FortiAP configuration.
6. Select **OK**.

Creating the FortiAP profile

Create a FortiAP profile for the meshed FortiAPs. If more than one FortiAP model is involved, you need to create a profile for each model. Typically, the profile is configured so that Radio 1 (5GHz) carries the mesh backhaul SSID while Radio 2 (2.4GHz) carries the SSIDs to which users connect.

For Radio 1, use the **Select SSIDs** option and choose only the backhaul SSID. The radio that carries the backhaul traffic must not carry other SSIDs.

Radio 2 carries user SSIDs and shouldn't carry the backhaul. Use the **Select SSIDs** option and choose the networks that you want to provide.

For more information, see Creating a FortiAP profile on page 17.

Configuring the mesh root AP

The mesh root AP can be either a FortiWiFi unit's built-in AP or a FortiAP unit.

To enable a FortiWiFi unit's local radio as mesh root

1. On the FortiWiFi unit, go to **WiFi & Switch Controller > Local WiFi Radio**.
2. Select **Enable WiFi Radio**.
3. In **SSID**, select **Select SSIDs**, then select the mesh root SSID.
4. Optionally, adjust **Tx Power** or select **Auto Tx Power Control**.
5. Select **Apply**.

In a network with multiple wireless controllers, make sure that each mesh root has a unique SSID. Other controllers using the same mesh root SSID may be detected as fake or rogue APs. Go to **WiFi & Switch Controller > SSID** to change the SSID.

To configure a network interface for the mesh root FortiAP unit

1. On the FortiGate unit, go to **Network > Interfaces**, and edit the interface to which the AP unit connects.
2. In **Addressing mode**, select **Manual.**
3. In **IP/Network Mask**, enter an IP address and netmask for the interface.
4. In the Administrative Access section, go to **IPv4** and select the **CAPWAP** checkbox.
   Note: In FortiOS 6.2.3 and later, select the **Security Fabric Connection** checkbox.
5. When FortiAP units are connected to the interface on FortiGate (directly or through a switch), you can go to the Edit Interface section and set the **Role** to **LAN**.
   Selecting the LAN role loads the DHCP Server toggle. If you enable **DHCP Server**, the GUI can automatically set the DHCP IP range based on the interface IP address.
6. Click **OK**.

At this point you can connect the mesh root FortiAP (see below). If you are planning to configure leaf FortiAPs through the wireless controller (see Configuring the mesh leaf FortiAPs on page 72), then connect the root unit later.

To enable the root FortiAP unit

1. Connect the root FortiAP unit's Ethernet port to the FortiGate network interface that you configured.
2. On the FortiGate unit, go to **WiFi & Switch Controller > Managed FortiAPs**.
   If the root FortiAP unit is not listed, wait 15 seconds and select **Refresh**. Repeat if necessary. If the unit is still missing after a minute or two, power cycle the root FortiAP unit and try again.
3. Right-click the FortiAP entry and choose your profile from the **Assign Profile** submenu.
4. Right-click the FortiAP entry and select **Authorize**.
   Initially, the **State** of the FortiAP unit is **Offline**. Periodically click **Refresh** to update the status. Within about two minutes, the state changes to **Online**.
5. Select **OK**.

Configuring the mesh leaf FortiAPs

The FortiAP units that serve as leaf nodes must be preconfigured. This involves changing the FortiAP unit's internal configuration. You can do this by direct connection or through the FortiGate wireless controller.

Method 1: Direct connection to the FortiAP

1. Configure the computer IP as 192.168.1.3.
2. Connect the computer to the FortiAP unit's Ethernet port and use the default IP address, 192.168.1.2.
3. Log in to the FortiAP as admin. By default, no password is set.
4. Enter the following commands:
   a. If you are using the GUI, go to **Connectivity > Uplink** and select the **Mesh** option. Then enter the **Mesh AP SSID** and **Mesh AP Password** (pre-shared key).
   b. If you are using the FortiAP CLI (SSH), enter the following commands, substituting your own SSID and password (pre-shared key):
   ```
   cfg -a MESH_AP_TYPE=1
   cfg -a MESH_AP_SSID=fortinet.mesh.root
   cfg -a MESH_AP_PASSWD=hardtoguess
   cfg -c
   exit
   ```
5. Disconnect the computer.
6. Power down the FortiAP.
7. Repeat the preceding steps for each leaf FortiAP.

Method 2: Connecting through the FortiGate unit

1. Connect the Ethernet port on the leaf FortiAP to the FortiGate network interface that you configured for FortiAPs. Connect the FortiAP unit to a power source unless PoE is used.
2. On the FortiGate unit, go to **WiFi & Switch Controller > Managed FortiAPs**.
   If the FortiAP unit is not listed, wait 15 seconds and select **Refresh**. Repeat if necessary. If the unit is still missing after a minute or two, power cycle the FortiAP unit and try again.
3. Select the discovered FortiAP unit and authorize it. Click **Refresh** every 10 seconds until the **State** indicator changes to **Online**.
4. Right-click the FortiAP and select **>_Connect to CLI**. The **CLI Console** window opens. Log in as "admin".
5. Enter the following commands, substituting your own SSID and password (pre-shared key):
   ```
   cfg -a MESH_AP_TYPE=1
   cfg -a MESH_AP_SSID=fortinet.mesh.root
   cfg -a MESH_AP_PASSWD=hardtoguess
   cfg -c
   exit
   ```
6. Disconnect the FortiAP and delete it from the **Managed FortiAP** list.
7. Repeat the preceding steps for each leaf FortiAP.

Authorizing leaf APs

When the root FortiAP is connected and online, apply power to the preconfigured leaf FortiAPs. The leaf FortiAPs will connect themselves wirelessly to the WiFi Controller through the mesh network. You must authorize each unit.

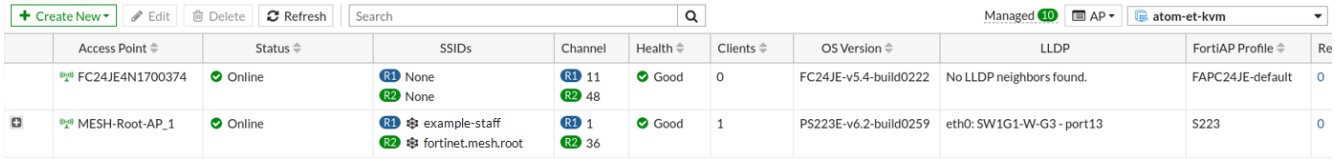
1. On the FortiGate unit, go to **WiFi & Switch Controller > Managed FortiAPs**. Periodically select **Refresh** until the FortiAP unit is listed. This can take up to three minutes.
   The **State** of the FortiAP unit should be **Waiting for Authorization**.
2. Right-click the FortiAP entry and choose your profile from the **Assign Profile** submenu.
3. Right-click the FortiAP entry and select **Authorize**.
   Initially, the **State** of the FortiAP unit is **Offline**. Periodically click **Refresh** to update the status. Within about two minutes, the state changes to **Online**.

Creating security policies

To permit traffic to flow from the end-user WiFi network to the network interfaces for the Internet and other networks, you need to create security policies and enable NAT.

Viewing the status of the mesh network

On the FortiGate unit, go to **WiFi & Switch Controller > Managed FortiAPs** to view the list of APs.



The **SSIDs** column lists the SSID of each FortiAP radio and uses icons to show the Traffic mode of each radio.

Bridge	
Mesh	
Tunnel	

To see more information about each radio, mouse over the **SSIDs** information.

Configuring a point-to-point bridge

To connect two wired network segments using a WiFi link, you can create a point-to-point bridge. The effect is the same as connecting the two network segments to the same wired switch.

You need to:

- Configure a mesh-backhaul SSID and a mesh root AP as described in Configuring the mesh root AP on page 71.
  Note: The mesh root AP for a point-to-point bridge must be a FortiAP unit, not the internal AP of a FortiWiFi unit.

- Configure a mesh leaf FortiAP as described in Configuring the mesh leaf FortiAPs on page 72 and add these steps to configure the Ethernet bridge:
  - If you are using the FortiAP GUI, select **Ethernet Bridge**.
  - If you are using the FortiAP CLI, insert the following command before the line reading `cfg -c`:
    `cfg -a MESH_ETH_BRIDGE=1`
- Connect the local wired network to the Ethernet port on the mesh leaf FortiAP unit. Users are assigned IP addresses from the DHCP server on the wired network connected to the mesh root FortiAP unit.

In general, the mesh-Ethernet bridge automatically detects VLAN ID tags in data packets and allows them to pass. When necessary, you can configure VLAN IDs for permanent support in a mesh-Ethernet bridge. To do this, enter the following commands in the mesh leaf FortiAP CLI:

```
cfg -a MESH_ETH_BRIDGE_VLANS=100,200,300
cfg -c
```

Hotspot 2.0 ANQP configuration

Hotspot 2.0 Access Network Query Protocol (ANQP) is a query and response protocol that defines seamless roaming services offered by an AP. To configure Hotspot 2.0 ANQP, use the CLI commands available under `config wireless-controller hostspot20`:

A hotspot profile needs to be attached to a VAP, and can only be attached to an enterprise security VAP. You can configure the security type and attach the hotspot profile with the following commands:

```
config wireless-controller vap
   edit {name}
      set security wpa2-only-enterprise
      set hotspot20-profile {string}
   next
end
```

Syntax

```
config wireless-controller hotspot20 anqp-3gpp-cellular
   edit {name}
      config mcc-mnc-list
         edit {id}
            set id {integer}
            set mcc {string}
            set mnc {string}
         next
   next
end

config wireless-controller hotspot20 anqp-ip-address-type
   edit {name}
      set ipv6-address-type {option}
      set ipv4-address-type {option}
   next
end

config wireless-controller hotspot20 anqp-nai-realm
   edit {name}
      config nai-list
         edit {name}
            set encoding {enable | disable}
            set nai-realm {string}
            config eap-method
               edit {index}
                  set method {option}
                  config auth-param
                     edit {index}
                        set id {option}
                        set val {option}
                  next
               next
```

```
        next
    next
end

config wireless-controller hotspot20 anqp-network-auth-type
    edit {name}
        set auth-type {option}
        set url {string}
    next
end

config wireless-controller hotspot20 anqp-roaming-consortium
    edit {name}
        config oi-list
            edit {index}
                set oi {string}
                set comment {string}
            next
    next
end

config wireless-controller hotspot20 anqp-venue-name
    edit {name}
        config value-list
            edit {index}
                set lang {string}
                set value {string}
            next
    next
end

config wireless-controller hotspot20 h2qp-conn-capability
    edit {name}
        set icmp-port {option}
        set ftp-port {option}
        set ssh-port {option}
        set http-port {option}
        set tls-port {option}
        set pptp-vpn-port {option}
        set voip-tcp-port {option}
        set voip-udp-port {option}
        set ikev2-port {option}
        set ikev2-xx-port {option}
        set esp-port {option}
    next
end

config wireless-controller hotspot20 h2qp-operator-name
    edit {name}
        config value-list
            edit {index}
                set lang {string}
                set value {string}
            next
    next
end
```

```
config wireless-controller hotspot20 h2qp-osu-provider
   edit {name}
      config friendly-name
         edit {index}
            set lang {string}
            set friendly-name {string}
         next
      set server-uri {string}
      set osu-method {option}
      set osu-nai {string}
      config service-description
         edit {service-id}
            set lang {string}
            set service-description {string}
         next
      set icon {string}
   next
end

config wireless-controller hotspot20 h2qp-wan-metric
   edit {name}
      set link-status {option}
      set symmetric-wan-link {option}
      set link-at-capacity {enable | disable}
      set uplink-speed {integer}
      set downlink-speed {integer}
      set uplink-load {integer}
      set downlink-load {integer}
      set load-measurement-duration {integer}
   next
end

config wireless-controller hotspot20 hs-profile
   edit {name}
      set access-network-type {option}
      set access-network-internet {enable | disable}
      set access-network-asra {enable | disable}
      set access-network-esr {enable | disable}
      set access-network-uesa {enable | disable}
      set venue-group {option}
      set venue-type {option}
      set hessid {mac address}
      set proxy-arp {enable | disable}
      set l2tif {enable | disable}
      set pame-bi {enable | disable}
      set anqp-domain-id {integer}
      set domain-name {string}
      set osu-ssid {string}
      set gas-comeback-delay {integer}
      set gas-fragmentation-limit {integer}
      set dgaf {enable | disable}
      set deauth-request-timeout {integer}
      set wnm-sleep-mode {enable | disable}
      set bss-transition {enable | disable}
      set venue-name {string}
      set roaming-consortium {string}
      set nai-realm {string}
```

```
      set oper-friendly-name {string}
      config osu-provider
         edit {name}
         next
      set wan-metrics {string}
      set network-auth {string}
      set 3gpp-plmn {string}
      set conn-cap {string}
      set qos-map {string}
      set ip-addr-type {string}
   next
end

config wireless-controller hotspot20 icon
   edit {name}
      config icon-list
         edit {name}
            set lang {string}
            set file {string}
            set type {option}
            set width {integer}
            set height {integer}
         next
   next
end

config wireless-controller hotspot20 qos-map
   edit {name}
      config dscp-except
         edit {index}
            set dscp
            set up
         next
      config dscp-range
         edit {index}
            set up
            set low
            set high
         next
   next
end
```

WiFi network with wired LAN configuration

This section includes the following topics:

- Combining WiFi network and wired LAN with a software switch on page 79
- Configuring a FortiAP local bridge (private cloud-managed AP) on page 81
- Using bridged FortiAPs for increased scalability on page 84

Combining WiFi network and wired LAN with a software switch

A WiFi network can be combined with a wired LAN so that WiFi and wired clients are on the same subnet. This is a convenient configuration for users.

Software switches are only available if your FortiGate is in Interface mode.

Wireless Mesh features cannot be used in conjunction with this configuration because they enable the FortiAP Local Bridge option.

To create the WiFi network and wired LAN configuration, you need to:

- Configure the SSID so that traffic is tunneled to the WiFi controller.
- Configure a software switch interface on the FortiGate unit with the WiFi and internal network interface as members.
- Configure Captive Portal security for the software switch interface.

To configure the SSID - GUI

1. Go to **WiFi & Switch Controller > SSID** and select **Create New**.
2. Complete the following fields:

Interface name	A name for the new WiFi interface.
Traffic Mode	Local bridge with FortiAP interface.
SSID	The SSID visible to users.
Security Mode	Configure security as you would for a regular WiFi network.
Pre-shared Key	A network access key for the SSID.

3. Click **OK**.
4. Go to **WiFi & Switch Controller > Managed FortiAPs**, select the FortiAP unit for editing.
5. Authorize the FortiAP unit.
   The FortiAP unit can carry regular SSIDs in addition to the Bridge SSID.

To configure the SSID - CLI

This example creates a WiFi interface “homenet_if” with SSID “homenet” using WPA-Personal security, passphrase “Fortinet1234”.

```
config wireless-controller vap
   edit "homenet_if"
      set vdom "root"
      set ssid "homenet"
      set security wpa-personal
      set passphrase "Fortinet1234"
   end
config wireless-controller wtp
   edit FAP22B3U11005354
      set admin enable
      set vaps "homenet_if"
   end
```

To configure the FortiGate software switch - GUI

1. Go to **Network > Interfaces** and select **Create New > Interface**.
2. Complete the following fields:

Interface Name	A name for the new interface. For example, `homenet_nw`.
Type	Software Switch
Physical Interface Members	Add homenet_if and the internal network interface.
Addressing mode	Select Manual and enter an address, for example `172.16.96.32/255.255.255.0`
DHCP Server	Enable and configure an address range for clients.
Security Mode	Select **Captive Portal**. Add the permitted **User Groups**.

3. Select **OK**.

To configure the FortiGate software switch - CLI

```
config system interface
   edit homenet_nw
      set ip 172.16.96.32 255.255.255.0
      set type switch
      set security-mode captive-portal
      set security-groups "Guest-group"
   end
config system interface
   edit homenet_nw
      set member "homenet_if" "internal"
   end
```

VLAN configuration

If your environment uses VLAN tagging, you assign the SSID to a specific VLAN in the CLI. See Reserved VLAN IDs on page 15. For example, to assign the homenet_if interface to VLAN 100, enter:

```
config wireless-controller vap
   edit "homenet_if"
      set vlanid 100
   end
```

Additional configuration

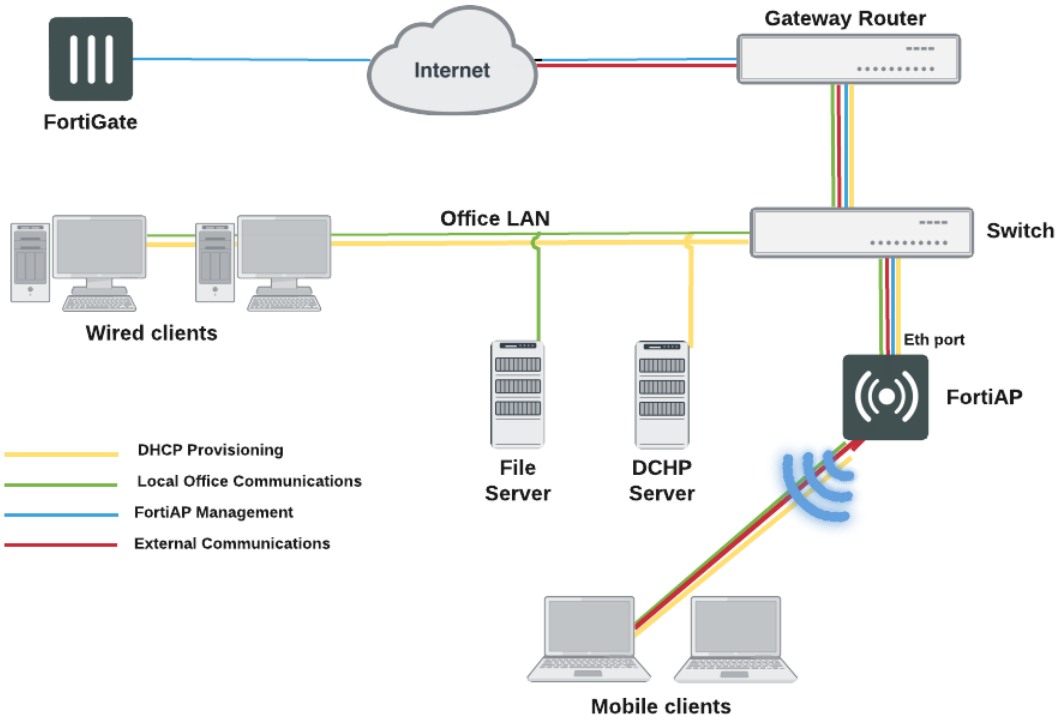
The configuration described above provides communication between WiFi and wired LAN users only. To provide access to other networks, create appropriate firewall policies between the software switch and other interfaces.

Configuring a FortiAP local bridge (private cloud-managed AP)

A FortiAP unit can provide WiFi access to a LAN, even when the wireless controller is located remotely. This configuration is useful for the following situations:

- Installations where the WiFi controller is remote and most of the traffic is local or uses the local Internet gateway
- Wireless-PCI compliance with remote WiFi controller
- Telecommuting, where the FortiAP unit has the WiFi controller IP address pre-configured and broadcasts the office SSID in the user's home or hotel room. In this case, data is sent in the wireless tunnel across the Internet to the office and you should enable encryption using DTLS.

Remotely-managed FortiAP providing WiFi access to local network



On the remote FortiGate wireless controller, the WiFi SSID is created with the **Bridge with FortiAP Interface** option selected. In this mode, no IP addresses are configured. The WiFi and Ethernet interfaces on the FortiAP behave as a switch. WiFi client devices obtain IP addresses from the same DHCP server as wired devices on the LAN.

The local bridge feature cannot be used in conjunction with Wireless Mesh features.

Block-Intra-SSID Traffic is available in Bridge mode. This is useful in hotspot deployments managed by a central FortiGate, but would also be useful in cloud deployments. Previously, this was only supported in Tunnel mode.

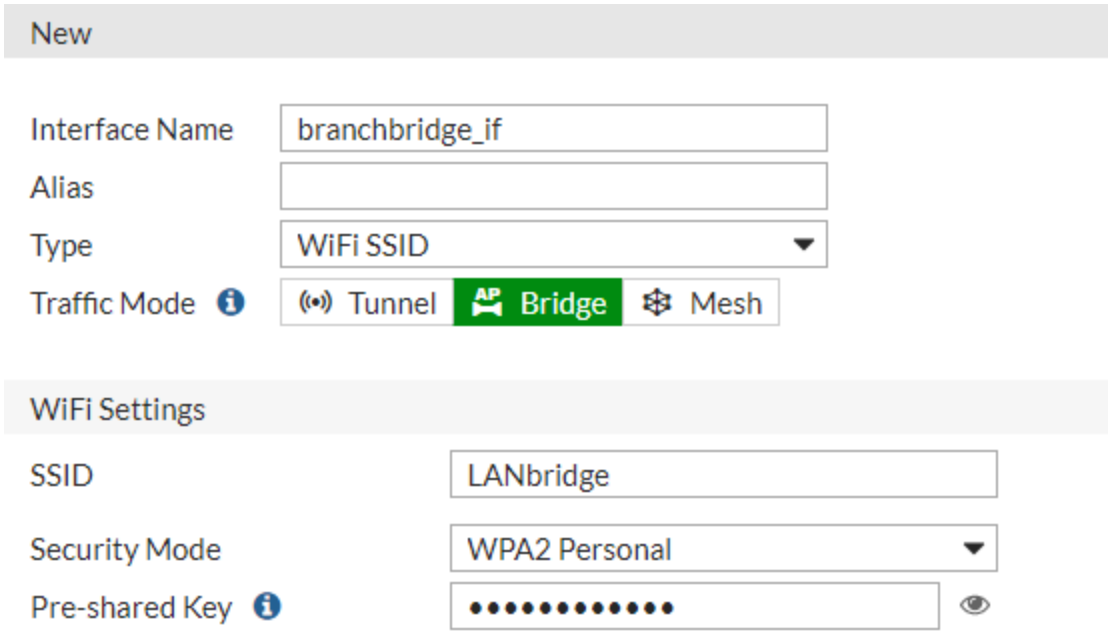
To configure a FortiAP local bridge - GUI

1. Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID**.
2. Complete the following fields:

Interface name	A name for the new WiFi interface.
Traffic Mode	Local bridge with FortiAP interface.
SSID	The SSID visible to users.
Security Mode	Configure security as you would for a regular WiFi network.
Pre-shared Key	A network access key for the SSID.

3. Click **OK**.
4. Go to **WiFi & Switch Controller > Managed FortiAPs** and select the FortiAP unit for editing.
5. Authorize the FortiAP unit.
   The FortiAP unit can carry regular SSIDs in addition to the Bridge SSID.

SSID configured for local bridge operation



To configure a FortiAP local bridge - CLI

This example creates a WiFi interface “branchbridge” with SSID “LANbridge” using WPA-Personal security, passphrase “Fortinet1234”.

```
config wireless-controller vap
   edit "branchbridge"
      set vdom "root"
      set ssid "LANbridge"
      set local-bridging enable
      set security wpa-personal
      set passphrase "Fortinet1234"
   end
config wireless-controller wtp
   edit FAP22B3U11005354
      set admin enable
      set vaps "branchbridge"
   end
```

- Disabling `local-bridging` forcefully disables `local-standalone`. Also, disabling either `local-bridging` or `local-standalone` forcefully disables `intra-vap-privacy`.
- Enabling `intra-vap-privacy` forcefully disables `local-standalone`.
- Enabling `local-standalone` forcefully enables `local-bridging`.

Continued FortiAP operation when WiFi controller connection is down

The wireless controller, or the connection to it, might occasionally become unavailable. During such an outage, clients already associated with a bridge mode FortiAP unit continue to have access to the WiFi and wired networks. Optionally, the FortiAP unit can also continue to authenticate users if the SSID meets these conditions:

- **Traffic Mode** is **Local bridge with FortiAP's Interface**.
  In this mode, the FortiAP unit does not send traffic back to the wireless controller.
- **Security Mode** is **WPA2 Personal**.
  These modes do not require the user database. In WPA2 Personal authentication, all clients use the same pre-shared key which is known to the FortiAP unit.
- **Allow New WiFi Client Connections When Controller is down** is enabled.
  This field is available only if the other conditions have been met.

The "LANbridge" SSID example would be configured like this in the CLI:

```
config wireless-controller vap
   edit "branchbridge"
      set vdom "root"
      set ssid "LANbridge"
      set local-bridging enable
      set security wpa-personal
      set passphrase "Fortinet1234"
      set local-authentication enable
   end
```

Using bridged FortiAPs for increased scalability

The FortiGate wireless controller can support more FortiAP units in local bridge mode than in the normal mode. But this is only true if you configure some of your FortiAP units to operate in remote mode, which supports only local bridge mode SSIDs.

The Managed FortiAP page (**WiFi & Switch Controller > Managed FortiAPs**) shows at the top right the current number of Managed FortiAPs. Hold the pointer over the number to see the maximum number that can be managed, "5/64" for example. The maximum number, however, is true only if all FortiAP units operate in remote mode. For more detailed information, consult the Maximum Values Table (in the Reference Manuals section). For each FortiGate model, there are two maximum values for managed FortiAP units: the total number of FortiAPs and the number of FortiAPs that can operate in normal mode.

To configure FortiAP units for remote mode operation

1. Create at least one SSID with **Traffic Mode** set to **Local bridge with FortiAP's Interface**.
2. Create a custom AP profile that includes *only* local bridge SSIDs.
3. Configure each managed FortiAP unit to use the custom AP profile. You also need to set the FortiAP unit's `wtp-mode` to `remote`, which is possible only in the CLI. The following example uses the CLI both to set `wtp-mode` and select the custom AP profile:
   ```
   config wireless-controller wtp
      edit FAP22B3U11005354
         set wtp-mode remote
         set wtp-profile 220B_bridge
      end
   ```

Remote WLAN FortiAPs

Remote WLAN FortiAP models enable you to provide a pre-configured WiFi access point to a remote or traveling employee. Once plugged in at home or in a hotel room, the FortiAP automatically discovers the enterprise FortiGate WiFi controller over the Internet and broadcasts the same wireless SSID used in the corporate office. Communication between the WiFi controller and the FortiAP is secure, eliminating the need for a VPN.

By default, all traffic from the remote FortiAP is sent to the FortiGate WiFi controller. If you want to use split tunneling, you can configure which traffic is routed to the FortiGate. Other general Internet traffic is routed unencrypted through the local gateway. Split tunneling avoids loading the FortiGate with unnecessary traffic and allows direct access to local private networks at the location of the FortiAP even if the connection to the WiFi controller goes down.

Configuring the FortiGate for remote FortiAPs

This section assumes that you have already defined SSIDs and now want to make them available to remote FortiAPs.

1. Create FortiAP profiles for the Remote LAN FortiAP models.

   If you were not already using Remote LAN FortiAP models, you will need to create FortiAP profiles for them. In the FortiAP profile, you specify the SSIDs that the FortiAP will broadcast. For more information, see Creating a FortiAP profile on page 17.
2. If you want to configure split tunneling, you must do the following:
   a. enable split tunneling in the FortiGate GUI
   b. apply split tunneling to a FortiAP profile
   c. configure split tunneling behavior in the FortiAP CLI
   d. enable split tunneling in the SSID
3. Configure a FortiAP to connect to FortiGate
4. Preauthorize a FortiAP for automatic authorization.

Enable split tunneling options

By default, split tunneling options are not visible in the FortiGate GUI. You can make these options visible using the following CLI command:

```
config system settings
   set gui-fortiap-split-tunneling enable
end
```

Once you enable split tunneling, you can apply it via the FortiAP profile.

Apply split tunneling

To apply split tunneling - FortiGate GUI

Go to **WiFi & Switch Controller > SSID** and edit your SSID. In the **WiFi Settings** section, enable **Split Tunneling**.

Go to **WiFi & Switch Controller > FortiAP Profiles** and edit the FortiAP Profile(s) that apply to the AP types used in the WiFi network. In the **Split Tunneling** section, enable **Include Local Subnet** and **Split Tunneling Subnet(s)**. You can enter a list of the destination IP address ranges.

- Depending on how you configure split tunneling behavior in the CLI (see Configure split tunneling behavior on page 86), you can decide if you want the listed IP addresses to be tunneled to the FortiGate, or if you want to avoid tunneling these IP addresses to the FortiGate.

Configure split tunneling behavior

There are two methods the FortiAP can use to tunnel networks from the remote AP:

- **Tunnel:** Define the subnets in the profile that you *want* to tunnel to the FortiGate. These are usually the IP subnets that contain internal corporate applications such as file shares.

  Uncheck the **Include Local Subet** option in the FortiAP profile if you want the remote wireless client to be able to communicate with internal devices at their home/remote site.
- **Local:** Define the subnets that you *do not* want to be tunneled back to the FortiGate. Use this method if you want all traffic to be inspected by the FortiGate, including traffic destined for the internet. This method is more secure but can add latency to the user's internet browsing.

  Check the **Include Local Subnet** option in the FortiAP profile if you want the remote wireless client to be able to communicate with internal devices at their home/remote site

From the FortiGate CLI, enter the following commands to change the split tunneling behavior in a FortiAP profile:

```
config wireless-controller wtp-profile
   edit <profile_name>
      set split-tunneling-acl-path {tunnel | local}
   end
end
```

To configure split tunneling addresses

In this example, split tunneling is configured on the example-ssid WiFi network. On FortiAP model 21D, traffic destined for the 192.168.x.x range will not be routed through the FortiGate WiFi controller. This private IP address range is typically used as a LAN by home routers.

```
config wireless-controller vap
   edit example-ssid
      set split-tunneling enable
   end

config wireless-controller wtp-profile
   edit FAP21D-default
      set split-tunneling-acl-local-ap-subnet enable
      config split-tunneling-acl
         edit 1
            set dest-ip 192.168.0.0 255.255.0.0
         end
      end
```

To enter multiple subnets, create a split-tunneling-acl entry for each one.

To override the split tunneling settings on a FortiAP

If the FortiAP Profile split tunneling settings are not appropriate for a particular FortiAP, you can override the settings on that unit.

```
config wireless-controller wtp
   edit FAP321C3X14019926
      set override-split-tunnel enable
      set split-tunneling-acl-local-ap-subnet enable
      config split-tunneling-acl
         edit 1
            set dest-ip 192.168.10.0 255.255.255.0
         end
      end
```

Enable split tunneling on SSIDs

Once you create your FortiAP profile, you need to enable split tunneling on the SSIDs you want to use on the remote APs.

1. Go to **WiFi & Switch Controller > SSID** and edit the SSIDs the remote AP will use.
2. Enable **Split tunneling**.
3. Click **OK**.

Configure a FortiAP unit to connect to FortiGate

Prior to providing a remote WLAN FortiAP unit to an employee, you need to preconfigure the FortiAP to connect to your FortiGate WiFi controller.

To pre-configure a FortiAP - GUI

1. Plug the FortiAP you want to deploy into a port or VLAN that has DHCP configured.
   - If no DHCP server is available, the default IP information to log in to the AP is:

     IP Address: 192.168.1.2

     Subnet Mask: 255.255.255.0

     DGW: 192.168.1.1
2. Look for the assigned IP Address on the router or DHCP server.

   If no DHCP server is available, use a cross-over cable to connect your Ethernet port directly to the LAN port on the AP.

   Note: You might need a power adapter for the FortiAP if POE is not available.
3. From a web browser, access your FortiAP at https://<FAP-IP> where <FAP-IP> is the IP address of the FortiAP.
4. Log in with username `admin` and no password.
5. From the FortiAP page, click **Local Configuration**.
6. In the **AC Discovery Type** field, select how you want the FortiAP to discover the controller and complete any required fields:

   For more information on discovery methods, refer to Advanced WiFi controller discovery on page 54.
   - **Auto:** Automatically cycle through all six of the discovery methods until it establishes an AC connection.
   - **Static:** Provide up to three Static IP Addresses (most likely the public facing IP addresses for remote workers).

- **DHCP:** Use DHCP Option 138.
- **DNS:** Provide up to three FQDN entries that are resolvable by the FortiAP.
- **FortiAP Cloud:** Enter your FortiAP Cloud username and password.

7. In the **AP Data Channel Security** field, select **IPsec Enabled**.
8. Click **OK** to save your changes.

To pre-configure a FortiAP - CLI

1. Connect the FortiAP to the FortiGate unit.
2. Go to **WiFi & Switch Controller > Managed FortiAPs** and wait for the FortiAP to be listed. Click **Refresh** periodically to see the latest information. Note the **Connected Via** IP address.
3. Right click the row of the FortiAP that you want to connect to and then select **>_ Connect to CLI**.
   The CLI Console window opens.
4. If the password prompt appears, then enter the required password. By default, no password is set.
5. Enter the following commands to set the FortiGate WiFi controller IP address. This IP address is the FortiGate Internet-facing IP address, in this example 172.20.120.142.
   ```
   cfg -a AC_IPADDR_1=172.20.120.142
   cfg -c
   ```
6. To log out of the FortiAP CLI, enter `exit`.

Preauthorize a FortiAP unit for automatic authorization

By preauthorizing FortiAP units, you facilitate their automatic authorization on the network. Also, you can assign each unit a unique name, such as the employee name, for easier tracking.

1. Go to **WiFi & Switch Controller > Managed FortiAPs** and create a new entry.
2. Enter the **Serial Number** of the FortiAP unit and give it a **Name**.
3. Select the appropriate **FortiAP Profile**.
4. Click **OK**.
5. Repeat steps 1 to 4 for each FortiAP.

Features for high-density deployments

High-density environments such as auditoriums, classrooms, and meeting rooms present a challenge to WiFi providers. When a large number of mobile devices try to connect to a WiFi network, difficulties arise because of the limited number of radio channels and interference between devices.

FortiOS and FortiAP devices provide several tools to mitigate the difficulties of high-density environments.

Performing the firmware upgrade of multiple FortiAPs

Administrators can perform the firmware upgrade of multiple FortiAPs in one click (under **WiFi & Switch Controller > Managed FortiAPs**), removing the need to upgrade each device one at a time.

Controlling the power save feature

Occasionally, voice calls can become disrupted. One way to alleviate this issue is by controlling the power save feature, or to disable it altogether.

Manually configure packet transmit optimization settings by entering the following command:

```
config wireless-controller wtp-profile
   edit <name>
      config <radio-1> | <radio-2>
         set transmit-optimize {disable | power-save | aggr-limit | retry-limit | sendbar}
```

- **disable:** Disable transmit optimization.
- **power-save:** Mark a client as power save mode if excessive transmit retries happen.
- **aggr-limit:** Set aggregation limit to a lower value when data rate is low.
- **retry-limit:** Set software retry limit to a lower value when data rate is low.
- **send-bar:** Do not send BAR frame too often.

11n radio powersave optimization

The following `powersave-optimize` parameters (under `config radio`) are used for 11n radios to optimize system performance for specific situations.

- **tim:** Set traffic indication map (TIM) bit for client in power save mode. TIM bit mask indicates to any sleeping listening stations if the AP has any buffered frames present. If enabled, the AP will always indicate to the connected client that there is a packet waiting in the AP, so it will help to prevent the client from entering a sleep state.
- **ac-vo:** Use Access Category (AC) Voice (VO) priority to send packets in the power save queue. AC VO is one of the highest classes/priority levels used to ensure quality of service (QoS). If enabled, when a client returns from a sleep state, the AP will send its buffered packet using a higher priority queue, instead of the normal priority queue.

- **no-obss-scan:** Do not put Overlapping Basic Service Set (OBSS), or high-noise (i.e. non-802.11), scan IE into a Beacon or Probe Response frame.
- **no-11b-rate:** Do not send frame using 11b data rate.
- **client-rate-follow:** Adapt transmitting PHY rate with receiving PHY rate from client. If enabled, the AP will integrate the current client's transmission PHY rate into its rate adaptation algorithm for transmitting.

Configuring the broadcast packet suppression

You can use broadcast packet suppression to reduce the traffic on your WiFi networks. In addition, some broadcast packets are unnecessary or even potentially detrimental to the network and should be suppressed. To configure broadcast suppression for each virtual access point, enter the following commands:

```
config wireless-controller vap
   edit <name>
      set broadcast-suppression {dhcp-up | dhcp-down | dhcp-starvation | arp-known | arp-
           unknown | arp-reply | arp-poison | arp-proxy | netbios-ns | netbios-ds | ipv6 |
           all-other-mc | all-other-bc}
   end
```

Option	Description
`dhcp-up`	Suppress DHCP discovery and request packets broadcast by WiFi clients. Forward DHCP packets to the Ethernet uplink only. Prevent malicious WiFi clients from acting as DHCP servers. Default setting.
`dhcp-down`	Suppress DHCP packets broadcast by the Ethernet downlink to WiFi clients. Prevent malicious WiFi clients from acting as DHCP servers.
`dhcp-starvation`	Suppress DHCP starvation attacks from malicious WiFi clients. Prevent malicious WiFi clients from depleting the DHCP address pool.
`arp-known`	Suppress ARP request packets broadcast to known WiFi clients. Instead, forward ARP packets as unicast packets to the known clients. Default setting.
`arp-unknown`	Suppress ARP request packets broadcast to unknown WiFi clients.
`arp-reply`	Suppress ARP reply packets broadcast by WiFi clients. Instead, forward the ARP packets as unicast packets to the clients with target MAC addresses.
`arp-poison`	Suppress ARP poison attacks from malicious WiFi clients. Prevent malicious WiFi clients from spoofing ARP packets.
`arp-proxy`	Suppress ARP request packets broadcast by the Ethernet downlink to known WiFi clients. Instead, send ARP reply packets to the Ethernet uplink, as a proxy for WiFi clients. The `arp-known` option must be set for `arp-proxy` to work.
`netbios-ns`	Suppress NetBIOS name services packets with UDP port 137.
`netbios-ds`	Suppress NetBIOS datagram services packets with UDP port 138.

Option	Description
ipv6	Suppress IPv6 broadcast packets.
all-other-mc	Suppress multicast packets not covered by any of the specific options.
all-other-bc	Suppress broadcast packets not covered by any of the specific options.

The default configuration enables both the `dhcp-up` and `arp-known` options. The following example leaves the default settings in place and also configures a virtual access point to suppress:

- unnecessary DHCP down link broadcast packets
- broadcast ARP requests for unknown WiFi clients
- other broadcast packets not specifically identified

```
config wireless-controller vap
   edit <name>
      set broadcast-suppression dhcp-up arp-known dhcp-down arp-unknown all-other-bc
   end
```

Converting multicast streams to unicast

FortiOS provides a multicast enhancement option (disabled by default) that converts multicast streams to unicast and improves performance in WiFi networks. Multicast data, such as streaming audio or video, is sent at a low data rate in WiFi networks. A unicast stream is sent to each client at high data rate that makes more efficient use of air time. To enable multicast-to-unicast conversion, enter the following commands:

```
config wireless-controller vap
   edit <vap_name>
      set multicast-enhance enable
   end
```

Ignoring weak or distant clients

Clients beyond the intended coverage area can have some impact on your high-density network. Your APs will respond to these clients' probe signals, consuming valuable air time. You can configure your WiFi network to ignore weak signals that most likely come from beyond the intended coverage area. The settings are available in the CLI:

```
config wireless-controller vap
   edit <vap_name>
      set probe-resp-suppression enable
      set probe-resp-threshold <level_int>
   end
```

vap_name is the SSID name.

probe-resp-threshold is the signal strength in dBm below which the client is ignored. The range is -95 to -20dBm. The default level is -80dBm.

Turning off the 802.11b protocol

By disabling support for the obsolete 802.11b protocol, you can reduce the air time that data frames occupy. These signals will now be sent at a minimum of 6 Mbps, instead of 1 Mbps. You can set this for each radio in the FortiAP profile, using the CLI:

```
config wireless-controller wtp-profile
   edit <name_string>
      config radio-1
         set powersave-optimize no-11b-rate
      end
```

Disabling low data rates

Each of the 802.11 protocols supports several data rates. By disabling the lowest rates, air time is conserved, allowing the channel to serve more users. You can set the available rates for each 802.11 protocol: a, b, g, n, ac. Data rates set as Basic are mandatory for clients to support. Other specified rates are supported.

The 802.11 a, b, and g protocols are specified by data rate. 802.11a can support 6,9,12, 18, 24, 36, 48, and 54 Mb/s. 802.11b/g can support 1, 2, 5.5, 6, 9,12, 18, 24, 36, 48, 54 Mb/s. Basic rates are specified with the suffix "basic", "12-basic" for example. The capabilities of expected client devices need to be considered when deciding the lowest Basic rate.

The 802.11n and ac protocols are specified by the Modulation and Coding Scheme (MCS) Index and the number of spatial streams.

- 802.11n with 1 or 2 spatial streams can support mcs0/1, mcs1/1, mcs2/1, mcs3/1, mcs4/1, mcs5/1, mcs6/1, mcs7/1,mcs8/2,mcs9/2, mcs10/2, mcs11/2, mcs12/2, mcs13/2, mcs14/2, mcs15/2.
- 802.11n with 3 or 4 spatial streams can support mcs16/3, mcs17/3, mcs18/3, mcs19/3, mcs20/3, mcs21/3, mcs22/3, mcs23/3, mcs24/4, mcs25/4, mcs26/4, mcs27/4, mcs28/4, mcs29/4, mcs30/4, mcs31/4.
- 802.11ac with 1 or 2 spatial streams can support mcs0/1, mcs1/1, mcs2/1, mcs3/1, mcs4/1, mcs5/1, mcs6/1, mcs7/1, mcs8/1, mcs9/1, mcs0/2, mcs1/2, mcs2/2, mcs3/2, mcs4/2, mcs5/2, mcs6/2, mcs7/2, mcs8/2, mcs9/2.
- 802.11ac with 3 or 4 spatial streams can support mcs0/3, mcs1/3, mcs2/3, mcs3/3, mcs4/3, mcs5/3, mcs6/3, mcs7/3, mcs8/3, mcs9/3, mcs0/4, mcs1/4, mcs2/4, mcs3/4, mcs4/4, mcs5/4, mcs6/4, mcs7/4, mcs8/4, mcs9/4

Here are some examples of setting basic and supported rates.

```
config wireless-controller vap
   edit <vap_name>
      set rates-11a 12-basic 18 24 36 48 54
      set rates-11bg 12-basic 18 24 36 48 54
      set rates-11n-ss34 mcs16/3 mcs18/3 mcs20/3 mcs21/3 mcs22/3 mcs23/3 mcs24/4 mcs25/4
      set rates-11ac-ss34 mcs0/3 mcs1/3 mcs2/3 mcs9/4 mcs9/3
   end
```

Enabling the automatic TX power control

High-density deployments usually cover a small area that has many clients. Maximum AP signal power is usually not required. Reducing the power reduces interference between APs. Fortinet recommends that you use FortiAP automatic power control. You can set this in the FortiAP profile.

1. Go to **WiFi & Switch Controller > FortiAP Profiles** and edit the profile for your AP model.
2. For each radio, enable **Auto TX Power Control** and set the **TX Power Low** and **TX Power High** levels. The default range of 10 to 17 dBm is recommended.

Enabling the frequency band load-balancing

In a high-density environment, it is important to make the best use of the two WiFi bands, 2.4 GHz and 5 GHz. The 5 GHz band has more non-overlapping channels and receives less interference from non-WiFi devices, but not all devices support it. Clients that are capable of 5 GHz operation should be encouraged to use 5 GHz rather than the 2.4 GHz band.

To load-balance the WiFi bands, you enable Frequency Handoff in the FortiAP profile. In the FortiGate GUI, go to **WiFi & Switch Controller > FortiAP Profiles** and edit the relevant profile to set Client Load Balancing to **Frequency Handoff**. Or, you can use the CLI:

```
config wireless-controller wtp-profile
   edit FAP221C-default
      config radio-1
         set frequency-handoff enable
      end
```

The FortiGate WiFi controller continuously performs a scan of all clients in the area and records their signal strength (RSSI) on each band. When Frequency Handoff is enabled, the AP does not reply to clients on the 2.4 GHz band that have sufficient signal strength on the 5 GHz band. These clients can associate only on the 5 GHz band. Devices that support only 2.4 GHz receive replies and associate with the AP on the 2.4 GHz band.

Setting the handoff RSSI threshold

The FortiAP applies load balancing to a client only if the client has a sufficient signal level on 5GHz. The minimum signal strength threshold is set in the FortiAP profile, but is accessible only through the CLI:

```
config wireless-controller wtp-profile
   edit FAP221C-default
      set handoff-rssi 25
   end
```

`handoff-rssi` has a range of 20 to 30. RSSI is a relative measure. The higher the number, the stronger the signal.

Enabling the AP load balancing

The performance of an AP is degraded if it attempts to serve too many clients. In high-density environments, multiple access points are deployed with some overlap in their coverage areas. The WiFi controller can manage the association of new clients with APs to prevent overloading.

To load-balance between APs, enable AP Handoff in the FortiAP profile. In the FortiGate GUI, go to **WiFi & Switch Controller > FortiAP Profiles** and edit the relevant profile to set Client Load Balancing to **AP Handoff**. Or, you can use the CLI:

```
config wireless-controller wtp-profile
   edit FAP221C-default
      config radio-1
         set ap-handoff enable
      end
```

When an AP exceeds the threshold (the default is 30 clients), the overloaded AP does not reply to a new client that has a sufficient signal at another AP.

Setting the AP load balance threshold

The thresholds for AP handoff are set in the FortiAP profile, but is accessible only through the CLI:

```
config wireless-controller wtp-profile
   edit FAP221C-default
      set handoff-sta-thresh 30
      set handoff-rssi 25
   end
```

`handoff-sta-thresh` sets the number of clients at which AP load balancing begins. It has a range of 5 to 35.

`handoff-rssi` sets the minimum signal strength that a new client must have at an alternate AP for the overloaded AP to ignore the client. It has a range of 20 to 30. RSSI is a relative measure. The higher the number, the stronger the signal.

Setting the Application Control feature

To prevent particular application types from consuming too much bandwidth, you can use the FortiOS Application Control feature.

1. Go to **Security Profiles > Application Control**. You can use the default profile or create a new one.
2. Click the category, select **Traffic Shaping** and then select the priority for the category.
   Repeat for each category to be controlled.
3. Select **Apply**.
4. Go to **Policy & Objects > IPv4 Policy** and edit your WiFi security policy.
5. In **Security Profiles**, set **Application Control** ON and select the security profile that you edited.
6. Select **OK**.

Managing the FortiAP group and setting the dynamic VLAN assignment

The FortiGate can create FortiAP Groups, under **WiFi & Switch Controller > Managed FortiAPs** by selecting **Create New > Managed AP Group**, where multiple APs can be managed. AP grouping allows specific profile settings to be applied to many APs all at once that belong to a certain AP group, simplifying the administrative workload.

Each AP can belong to one group only.

In addition, VLANs can be assigned dynamically based on the group which an AP belongs. When defining an SSID, under **WiFi & Switch Controller > SSID**, a setting called **VLAN Pooling** can be enabled where you can either assign the VLAN ID of the AP group the device is connected to, to each device as it is detected, or to always assign the same VLAN ID to a specific device. Dynamic VLAN assignment allows the same SSID to be deployed to many APs, avoiding the need to produce multiple SSIDs.

Sharing tunnel SSIDs within a single managed FortiAP

This feature provides the ability to move a tunnel mode virtual AP (VAP) into a VDOM, similar to an interface/VLAN in VDOMs. FortiAP is registered into the root VDOM.

Within a customer VDOM, customer VAPs can be created or added. In the root VDOM, the customer VAP can be added to the registered FortiAP. Any necessary firewall rules and interfaces can be configured between the two VDOMs.

Syntax

```
config wireless-controller global
   set wtp-share {enable | disable}
end
```

Enabling the manual quarantine of devices on FortiAP (tunnel mode)

Quarantined MAC addresses are blocked on the connected FortiAP from the network and the LAN. When a tunnel VAP is created, a sub-interface named **wqtn** is automatically created under tunnel interface. This sub-interface is added under a software switch.

To quarantine an SSID, go to **WiFi & Switch Controller > SSID**. Edit the SSID, and enable **Quarantine Host** is enabled under **WiFi Settings**.

Alternatively, you can quarantine an SSID using the CLI console. This feature consolidates previous CLI syntax for quarantining a host, so that the host does not need to be configured in multiple places (FortiAP and FortiSwitch). Host endpoints can be entered in a single place and the host will be quarantined throughout the access layer devices on the Fortinet Security Fabric.

You can only quarantine an SSID that is in Tunnel Mode.

Syntax - SSID:

```
config wireless-controller vap
   edit <name>
      set quarantine {enable | disable}
   next
end
```

Syntax - Software Switch, DHCP, and User Quarantine

```
config system switch-interface
   edit "wqt.root"
      set vdom "root"
      set member "wqtn.26.AV-Qtn"
   next
end

config system dhcp server
   edit <id>
      set interface "AV-Qtn"
      config ip-range
         edit <id>
            set start-ip 10.111.0.2
            set end-ip 10.111.0.254
         next
      ...

config user quarantine
   set quarantine {enable | disable}
end
```

To list stations in quarantine, use the following diagnose command:

```
diagnose wireless-controller wlac -c sta-qtn
```

Enabling host quarantine per SSID

Upon creating or editing an SSID, a **Quarantine Host** option is available to enable (by default) or disable quarantining devices that are connected in Tunnel-mode. The option to quarantine a device is available on **Topology** and **FortiView** WiFi pages.

When a host is put into quarantine VLAN, it will get its IP from the quarantine VLAN's DHCP server, and become part of the quarantined network.

Syntax

```
config wireless-controller vap
   edit <name>
      set quarantine {enable | disable}
```

```
   next
end
```

To list all stations in quarantine:

```
diagnose wireless-controller wlac -c sta-qtn
```

Locating a FortiAP with LED blinking

If you have an environment that contains numerous APs, and there is one AP that you need to frequently monitor, you can configure it to blink in the FortiAP Cloud web portal. The blinking AP will be easier to locate.

To start or stop LED blinking of a managed FortiAP, using the GUI:

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Right-click in the row of the device you want to control.
3. In the dialog box, scroll down to **LED Blink** and select **Start** or **Stop**.

The following models support LED blink control through the GUI, operating on FortiAP software 6.0.1, or later:

- FortiAP-112D, 221C, 223C, 224D, 320C, 321C
- FortiAP-S/W2

To start or stop LED blinking of a managed FortiAP, using the CLI:

```
execute wireless-controller led-blink <wtp-id> {on | on 10 | off}
```

The following models support LED blink control through the CLI, operating on FortiAP software 5.6.2, or later:

- FortiAP-112D, 221C, 223C, 224D, 320C, 321C
- FortiAP-S/W2

Uploading a FortiAP image on the wireless controller

Using the CLI to upgrade the FortiAP image is the preferred method especially for large deployments. Use the following CLI command to upload the desired FortiAP image on the wireless controller:

```
execute wireless-controller upload-wtp-image
```

After entering the command, reboot the FortiAP devices. This feature allows the administrator to configure all FortiAP devices to download the image from the controller at join time.

Syntax

```
config wireless-controller global
   set image-download {enable | disable}
end
```

To fine-tune this process, in order to deploy FortiAP image upgrades to a subset of devices for pilot testing, use the following command:

```
config wireless-controller wtp
   edit <name>
      set image-download {enable | disable}
   next
end
```

Configuring control message off-loading

Users can configure control message off-loading to optimize performance. This is especially useful in environments where the AP count is from 300 to 350 (with a device count between 1500 and 3000), where existing users are disconnected and unable to reauthenticate due to high CPU usage. This feature includes aeroscout enhancements.

Syntax

```
config wireless-controller global
   set control-message-offload {evp-frame | areoscout-tag | ap-list | sta-list | sta-cap-
        list | stats | aeroscout-mu}
end

config wireless-controller wtp-profile
   edit <name>
      set control-message-offload {enable | disable}
         config lbs
         set ekahau-blink-mode {enable | disable}
         set aeroscout {enable | disable}
         set aeroscout-server-ip <address>
         set aeroscount-server-port <UDP listening port>
         set aeroscout-mu {enable | disable}
   end
end
```

Wireless network protection

This section includes the following topics:

- Wireless Intrusion Detection System on page 99
- WiFi data channel encryption on page 100
- Protected Management Frames and Opportunistic Key Caching support on page 101
- Bluetooth Low Energy scan on page 102
- Preventing local bridge traffic from reaching the LAN on page 103
- FortiAP-S bridge mode security profiles on page 103
- DHCP snooping and option-82 data insertion on page 104

Wireless Intrusion Detection System

The FortiGate Wireless Intrusion Detection System (WIDS) monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts. When an attack is detected the FortiGate unit records a log message.

You can create a WIDS profile to enable these types of intrusion detection:

- Asleap Attack—ASLEAP is a tool used to perform attacks against LEAP authentication.
- Association Frame Flooding—A Denial of Service attack using a large number of association requests. The default detection threshold is 30 requests in 10 seconds.
- Authentication Frame Flooding—A Denial of Service attack using a large number of association requests. The default detection threshold is 30 requests in 10 seconds.
- Broadcasting De-authentication—This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-authenticate, then re-authenticate with their AP.
- EAPOL Packet Flooding—Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack. Several types of EAPOL packets are detected: EAPOL-FAIL, EAPOL-LOGOFF, EAPOL-START, EAPOL-SUCC.
- Invalid MAC OUI—Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
- Long Duration Attack—To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200.
- Null SSID Probe Response—When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
- Spoofed De-authentication—Spoofed de-authentication frames are a denial of service attack. They cause all clients to disconnect from the AP.
- Weak WEP IV Detection—A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
- Wireless Bridge—WiFi frames with both the fromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.

You can enable wireless IDS by selecting a WIDS Profile in your FortiAP profile.

To create a WIDS Profile

1. Go to **WiFi & Switch Controller > WIDS Profiles**.
2. Select a profile to edit or select **Create New**.
3. Select the types of intrusion to protect against.
   By default, all types are selected.
4. Select **Apply**.

You can also configure a WIDS profile in the CLI using the `config wireless-controller wids-profile` command.

Rogue AP detection

The WIDS profile includes settings for detection of unauthorized (rogue) access points in your wireless network. For more information, see Monitoring rogue APs on page 107.

WIDS client de-authentication rate for DoS attacks

As part of mitigating a Denial of Service (DoS) attack, the FortiGate sends de-authentication packets to unknown clients. In an aggressive attack, this de-authentication activity can prevent the processing of packets from valid clients. A WIDS Profile option in the CLI limits the de-authentication rate.

```
config wireless-controller wids-profile
   edit default
      set deauth-unknown-src-thresh <1-65535>
end
```

The value set is a measure of the number of de-authorizations per second. 0 means no limit. The default is 10.

WiFi data channel encryption

Optionally, you can apply DTLS encryption to the data channel between the wireless controller and FortiAP units to enhance security.

There are data channel encryption settings on both the FortiGate unit and the FortiAP units. At both ends, you can enable Clear Text, DTLS encryption, or both. The settings must agree or the FortiAP unit will not be able to join the WiFi network. By default, both Clear Text and DTLS-encrypted communication are enabled on the FortiAP unit, allowing the FortiGate setting to determine whether data channel encryption is used. If the FortiGate unit also enables both Clear Text and DTLS, Clear Text is used.

Data channel encryption settings are located in the FortiAP profile. By default, only Clear Text is supported.

Data channel encryption is software-based and can affect performance. Verify that the system meets your performance requirements with encryption enabled.

Configuring encryption on a FortiGate unit

You can use the CLI to configure data channel encryption.

To enable encryption

In the CLI, the `wireless wtp-profile` command contains a new field, `dtls-policy`, with options `clear-text` and `dtls-enabled`. To enable encryption in profile1 for example, enter:

```
config wireless-controller wtp-profile
   edit profile1
      set dtls-policy dtls-enabled
   end
```

Configuring encryption on a FortiAP unit

The FortiAP unit has its own settings for data channel encryption.

To enable CAPWAP encryption - FortiAP GUI

1. On the **System Information** page, in **WTP Configuration > AC Data Channel Security**, select one of:
   - Clear Text
   - DTLS Enabled
   - Clear Text or DTLS Enabled (default)
2. Select **Apply**.

To enable encryption - FortiAP CLI

You can set the data channel encryption using the AP_DATA_CHAN_SEC variable: 'clear', or 'ipsec', or 'dtls'.

For example, to set security to DTLS and then save the setting, enter:

```
cfg -a AP_DATA_CHAN_SEC=dtls
cfg -c
```

Protected Management Frames and Opportunistic Key Caching support

Protected Management Frames (PMF) protect some types of management frames like deauthorization, disassociation and action frames. This feature, now mandatory on WiFi certified 802.1ac devices, prevents attackers from sending plain deauthorization/disassociation frames to disrupt or tear down a connection/association. PMF is a Wi-Fi Alliance specification based on IEEE 802.11w.

To facilitate faster client roaming, you can enable Opportunistic Key Caching (OKC) on your WiFi network. When a client associates with an AP, its PMK identifier is sent to all other APs on the network. This eliminates the need for an already-authenticated client to repeat the full EAP exchange process when it roams to another AP on the same network.

Use of PMF and OKC on an SSID is configurable only in the CLI:

```
config wireless-controller vap
   edit <vap_name>
```

```
      set pmf {disable | enable | optional}
      set pmf-assoc-comeback-timeout <integer>
      set pmf-sa-query-retry-timeout <integer>
      set okc {disable | enable}
   next
end
```

When `pmf` is set to `optional`, it is considered enabled, but will allow clients that do not use PMF. When `pmf` is set to `enable`, PMF is required by all clients.

Bluetooth Low Energy scan

The FortiGate can configure FortiAP Bluetooth Low Energy (BLE) scan, incorporating Google's BLE beacon profile known as Eddystone, used to identify groups of devices and individual devices.

Only FAP-S221E, FAP-S223E, and FAP-222E models support this feature.

Use the following syntax to configure BLE profiles and BLE report intervals, and assign BLE profiles to WTP profiles.

Configure BLE profiles - CLI syntax

```
config wireless-controller ble-profile
   edit <name>
      set comment <comment>
      set advertising {ibeacon | eddystone-uid | eddystone-url}
      set ibeacon-uuid <uuid>
      set major-id <0 - 65535> - (default = 1000)
      set minor-id <0 - 65535> - (default = 1000)
      set eddystone-namespace <10-byte namespace>
      set eddystone-instance <device id>
      set eddystone-url <url>
      set txpower <0 - 12> - (default = 0)
      set beacon-interval <40 - 3500> - (default = 100)
      set ble-scanning {enable | disable} - (default = disable)
   next
end
```

Note that `txpower` determines the transmit power level on a scale of 0-12:

0: -21 dBm	**1:** -18 dBm	**2:** -15 dBm	**3:** -12 dBm	**4:** -9 dBm
5: -6 dBm	**6:** -3 dBm	**7:** 0 dBm	**8:** 1 dBm	**9:** 2 dBm
10: 3 dBm	**11:** 4 dBm	**12:** 5 dBm		

Configure BLE report intervals - CLI syntax

```
config wireless-controller timers
```

```
   set ble-scan-report-intv - (default = 30 sec)
end
```

Assign BLE profiles to WTP profiles - CLI syntax

```
config wireless-controller wtp-profile
   edit <name>
      set ble-profile <name>
   next
end
```

Preventing local bridge traffic from reaching the LAN

The following command can be enabled so that when a client connects to a VAP, and its traffic is not tunneled to the controller, the admin can control whether the client can access the local network.

Note that this entry is only available when `local-standalone-nat` is set to `enable`.

Syntax:

```
config wireless-controller vap
   edit <name>
      set local-lan {allow | deny}
   next
end
```

FortiAP-S bridge mode security profiles

If a bridge mode SSID is configured for a managed FortiAP-S (or smart FortiAP), you can add a security profile group to the wireless controller configuration that allows you to apply the following security profile features to the traffic over the bridge SSID:

- AntiVirus
- Scan Botnets
- Intrusion Prevention
- Application Control
- Web Filter

Configure Security Profile Groups - GUI

1. Go to **WiFi & Switch Controller > SSID** and select the bridge mode SSID assigned to the FortiAP Profile that you want to configure.
2. In the selected SSID, enable the **Security profile group** option.
3. From the Security profile group drop-down field, you can either edit the **wifi-default** profile or select **Create** to make a new one.

   The Security Profile Group window loads.
4. Enable or disable **Logging**.

5. Enable or disable **Scan Botnets**.
   This option is enabled by default. If you enable this option, select **Blocked** or **Monitor**.
6. Under **Security Profiles**, you can enable or disable the **AntiVirus**, **Web Filter**, **Application Control**, and **Intrusion Prevention** profiles. To view available profiles or create new ones, click the drop-down field.
7. Click **OK** to save your Security Profile Group changes.
8. Click **OK** to save your SSID changes.

Configure Security Profile Groups - CLI

You configure security profile groups on managed smart FortiAPs by using the `config wireless-controller utm-profile` command. Then, you can assign a security profile group by using the `set utm-profile` command under `config wirelesscontroller vap`, after `local-bridging` is set to `enable`.

Note that the default `utm-profile`, named `wifi-default`, has all applicable options within the command set to `wifi-default`.

To view all available profiles that you can assign, type "`?`". For example, "`set ips-sensor ?`".

```
config wireless-controller utm-profile
   edit <name>
      set comment <comment>
      set utm-log {enable | disable}
      set ips-sensor <name>
      set application-list <name>
      set antivirus-profile <name>
      set webfilter-profile <name>
      set scan-botnet-connections {disable | block | monitor}
   next
end

config wireless-controller vap
   edit <name>
      set local-bridging enable
      set utm-profile <name>
   next
end
```

To debug the wireless-controller configurations related to security profile groups, use the following diagnose command:

```
diagnose wireless-controller wlac_hlp
```

DHCP snooping and option-82 data insertion

Commands are available to enable or disable (by default) DHCP option-82 data insertion for wireless access points. DHCP snooping is used to prevent rogue DHCP servers from offering IP addresses to DHCP clients.

Syntax

```
config wireless-controll vap
   edit wifi
      set dhcp-option82-insertion {enable | disable}
```

```
      set dhcp-option82-circuit-id-insertion {style-1 | style-2 | disable}
      set dhcp-option82-remote-id-insertion {style-1 | disable}
    next
end
```

Wireless network monitoring

This section includes the following topics:

- Monitoring wireless clients on page 106
- Monitoring rogue APs on page 107
- Suppressing rogue APs on page 110
- Monitoring wireless network health on page 111
- Monitoring FortiAP with SNMP on page 112

Monitoring wireless clients

To view connected clients on a FortiGate or FortiWiFi unit

1. Go to **Monitor > WiFi Client Monitor**.
   The following information is displayed on both the FortiGate and FortiWiFi units, unless otherwise specified:

SSID	The SSID that the client is connected to.
FortiAP	The serial number of the FortiAP unit to which the client connected.
User	The user name associated with the device.
IP	The IP address assigned to the wireless client.
MAC Address	The MAC address of the device. ***Note:*** This column is available on the FortiGate only.
Device	
Channel	WiFi radio channel in use.
Bandwidth Tx/Rx	Client received and transmitted bandwidth, in Kbps.
Signal Strength / Noise	The signal-to-noise ratio in decibels calculated from signal strength and noise level.
Signal Strength	
Association Time	How long the client has been connected to this access point.

Results can be filtered. Select the filter icon on the column you want to filter. Enter the values to include. If you want to exclude values, specify them and also select NOT.

Monitoring rogue APs

The access point radio equipment can scan for other available access points, either as a dedicated monitor or in idle periods during AP operation.

Discovered access points are listed in **Monitor > Rogue AP Monitor**. You can then mark them as either Accepted or Rogue access points. This designation helps you track access points. It does not affect anyone's ability to use these access points.

It is also possible to suppress rogue APs. See Suppressing rogue APs on page 110.

On-wire rogue AP detection technique

Other APs that are available in the same area as your own APs are not necessarily rogues. A neighboring AP that has no connection to your network might cause interference, but it is not a security threat. A rogue AP is an unauthorized AP connected to your wired network. This can enable unauthorized access. When rogue AP detection is enabled, the **On-wire** column in the **Rogue AP Monitor** list shows a green up-arrow on detected rogues.

Rogue AP monitoring of WiFi client traffic builds a table of WiFi clients and the Access Points that they are communicating through. The FortiGate unit also builds a table of MAC addresses that it sees on the LAN. The FortiGate unit's on-wire correlation engine constantly compares the MAC addresses seen on the LAN to the MAC addresses seen on the WiFi network.

There are two methods of Rogue AP on-wire detection operating simultaneously: Exact MAC address match and MAC adjacency.

Exact MAC address match

If the same MAC address is seen on the LAN and on the WiFi network, this means that the wireless client is connected to the LAN. If the AP that the client is using is not authorized in the FortiGate unit configuration, that AP is deemed an 'on-wire' rogue. This scheme works for non-NAT rogue APs.

MAC adjacency

If an access point is also a router, it applies NAT to WiFi packets. This can make rogue detection more difficult. However, an AP's WiFi interface MAC address is usually in the same range as its wired MAC address. So, the MAC adjacency rogue detection method matches LAN and WiFi network MAC addresses that are within a defined numerical distance of each other. By default, the MAC adjacency value is 7. If the AP for these matching MAC addresses is not authorized in the FortiGate unit configuration, that AP is deemed an 'on-wire' rogue.

Limitations

On-wire rogue detection has some limitations. There must be at least one WiFi client connected to the suspect AP and continuously sending traffic. If the suspect AP is a router, its WiFi MAC address must be very similar to its Ethernet port MAC address.

Logging

Information about detected rogue APs is logged and uploaded to your FortiAnalyzer unit, if you have one. By default, rogue APs generate an alert level log, unknown APs generate a warning level log. This log information can help you with PCI-DSS compliance requirements.

Rogue AP scanning as a background activity

Each WiFi radio can perform monitoring of radio channels in its operating band while acting as an AP. It does this by briefly switching from AP to monitoring mode. By default, a scan period starts every 300 seconds. Each second a different channel is monitored for 20ms until all channels have been checked.

During heavy AP traffic, it is possible for Spectrum Analysis background scanning to cause lost packets when the radio switches to monitoring. To reduce the probability of lost packets, you can set the CLI `ap-bgscan-idle` field to delay the switch to monitoring until the AP has been idle for a specified period. This means that heavy AP traffic may slow background scanning.

The following CLI example configures default background rogue scanning operation except that it sets `ap-bgscan-idle` to require 100ms of AP inactivity before scanning the next channel.

```
config wireless-controller wtp-profile
   edit ourprofile
      config radio-1
         set wids-profile ourwidsprofile
         set spectrum-analysis enable
      end
   end
config wireless-controller wids-profile
   edit ourwidsprofile
      set ap-scan enable
      set rogue-scan enable
      set ap-bgscan-period 300
      set ap-bgscan-intv 1
      set ap-bgscan-duration 20
      set ap-bgscan-idle 100
   end
```

Configuring rogue scanning

All APs using the same FortiAP Profile share the same rogue scanning settings, unless override is configured.

To enable rogue AP scanning with on-wire detection - GUI

1. Go to **WiFi & Switch Controller > WIDS Profiles**.
2. Select an existing WIDS Profile and edit it, or select **Create New**.
3. Select a **Sensor mode**, you can choose either **Foreign Channels Only** or **Foreign and Home Channels**.
   On-wire detection is automatically enabled when you select both a sensor mode and enable rogue AP detection.
4. Select **Enable rogue AP detection**.
5. Optionally, enable **Auto Suppress Rogue APs in Foreground Scan**.
6. Click **OK**.

To enable the rogue AP scanning feature in a custom AP profile - CLI

```
config wireless-controller wids-profile
   edit FAP220B-default
      set ap-scan enable
      set rogue-scan enable
   end
```

Exempting an AP from rogue scanning

By default, if Rogue AP Detection is enabled, it is enabled on all managed FortiAP units. Optionally, you can exempt an AP from scanning. You should be careful about doing this if your organization must perform scanning to meet PCI-DSS requirements.

To exempt an AP from rogue scanning

1. Go to **WiFi & Switch Controller > WIDS Profiles**.
2. Create a new WIDS profile and disable **Rogue AP detection**.
3. Go to **WiFi & Switch Controller > FortiAP Profiles** and edit the profile you wish to exempt from rogue scanning.
4. Assign the WIDS profile created in step 2.

MAC adjacency

You can adjust the maximum WiFi to Ethernet MAC difference used when determining whether a suspect AP is a rogue.

To adjust MAC adjacency

For example, to change the adjacency to 8, enter

```
config wireless-controller global
   set rogue-scan-mac-adjacency 8
end
```

Using the Rogue AP Monitor

To view the list of other wireless access points that are receivable at your location, go to **Monitor > Rogue AP Monitor**.

Information Columns
Actual columns displayed depends on **Column Settings.**

State	 Rogue AP — Use this status for unauthorized APs that **On-wire** status indicates are attached to your wired networks.  Accepted AP — Use this status for APs that are an authorized part of your network or are neighboring APs that are not a security threat. To see accepted APs in the list, select **Show Accepted**.  Unclassified — This is the initial status of a discovered AP. You can change an AP back to unclassified if you have mistakenly marked it as Rogue or Accepted.
Online Status	 Active AP  Inactive AP  Active ad-hoc WiFi device  Inactive ad-hoc WiFi device
SSID	The wireless service set identifier (SSID) or network name for the wireless interface.
Security Type	The type of security currently being used.
Channel	The wireless radio channel that the access point uses.
MAC Address	The MAC address of the Wireless interface.
Vendor Info	The name of the vendor.
Signal Strength	The relative signal strength of the AP. Mouse over the symbol to view the signal-to-noise ratio.
Detected By	The name or serial number of the AP unit that detected the signal.
On-wire	A green up-arrow indicates a suspected rogue, based on the on-wire detection technique. A red down-arrow indicates AP is not a suspected rogue.
First Seen	How long ago this AP was first detected.
Last Seen	How long ago this AP was last detected.
Rate	Data rate in bps.

To change the Online Status of an AP, right-click that AP and select Mark Accepted or Mark Rogue.

Suppressing rogue APs

In addition to monitoring rogue APs, you can actively prevent your users from connecting to them. When suppression is activated against an AP, the FortiGate WiFi controller sends deauthentication messages to the rogue AP's clients, posing as the rogue AP, and also sends deauthentication messages to the rogue AP, posing as its clients. This is done using the monitoring radio.

Before enabling this feature, verify that operation of Rogue Suppression is compliant with the applicable laws and regulations of your region.

To enable rogue AP suppression, you must enable monitoring of rogue APs with the on-wire detection technique (see Configuring rogue scanning on page 108). The monitoring radio must be in the Dedicated Monitor mode.

To activate AP suppression against a rogue AP

1. Go to **Monitor > Rogue AP Monitor**.
2. When you see an AP listed that is a rogue detected “on-wire”, select it and then select **Mark > Mark Rogue**.
3. To suppress an AP that is marked as a rogue, select it and then select **Suppress AP**.

To deactivate AP suppression

1. Go to **Monitor > Rogue AP Monitor**.
2. Select the suppressed rogue AP and then select **Suppress AP > Unsuppress AP**.

Monitoring wireless network health

To view the wireless health dashboard, go to **Monitor > WiFi Health Monitor**.

The wireless health dashboard provides a comprehensive view of the health of your network’s wireless infrastructure. The dashboard includes widgets to display:

- **AP Status**
  Active, Down or missing, up for over 24 hours, rebooted in past 24 hours
- **Client Count Over Time**
  Viewable for past hour, day, or 30 days
- **Top Client Count Per-AP**
  Separate widgets for 2.4 GHz and 5 GHz bands
- **Top Wireless Interference**
  Separate widgets for 2.4 GHz and 5 GHz bands, requires spectrum analysis to be enabled on the radios
- **Login Failures**
  The time, SSID, host name, and username for failed login attempts. The widget also displays the AP name and AP group of FortiAP units with failed login attempts.
- **WiFi Channel Utilization**
  Three views allowing users to view top 10-20 most and least utilized channels for each AP radio and a third histogram view showing counts for utilization

The list of active clients also shows MAC address entries (similar to the **WiFi Client Monitor** page), making client information easy to view when opening the **Active Client** widget.

Monitoring FortiAP with SNMP

FortiAP-S and FortiAP-W2 version 6.2.0 and later support Simple Network Management Protocol (SNMP) queries and trap messages based on wireless-controller SNMP settings configured on FortiGate.

FortiAP-S and FortiAP-W2 support all SNMP versions (v1, v2, and v3).

The local standalone mode does not support FortiAP direct SNMP.

The SNMP manager requires the following management information base (MIB) files:

- FortiAP MIB
- Fortinet Core MIB

Downloading the FortiAP MIB and Fortinet Core MIB files

To download the FortiAP SNMP MIB and Fortinet Core MIB files, perform the following steps:

1. Go to the Fortinet Support website.
2. Log in to your account. If you do not have an account, create one and then log in.
3. From the top banner, select **Download > Firmware images**.
4. From the Select Product list, select **FortiAP-S** or **FortiAP-W2**, as applicable.
5. Click the **Download** tab.
6. Locate the v6.00 folder (or later) and then the 6.2 (or later) folder to match the firmware release running on your FortiAP-S or FortiAP-W2 device.
7. Navigate through the folders to find and then download the FORTINET-FORTIAP-MIB-buildxxxx.mib file.
8. From the Select Product list, select **FortiGate**.
9. Locate the v6.00 folder (or later) and then 6.2 (or later) folder to match the firmware release running on your FortiGate device.
10. Navigate through the folders to find and then download the FORTINET-CORE-MIB-buildxxxx.mib file.
11. You can load the MIB files into your SNMP manager.

FortiAP SNMP trap messages

FortiAP-S and FortiAP-W2 can send the following trap messages to an SNMP manager or trap receiver:

Trap message	Description
fapDevUp	The specified FortiAP device is up.
fapCpuOverload	The CPU usage of the specified FortiAP has exceeded the configured threshold.
fapMemOverload	The memory usage of the specified FortiAP has exceeded the configured threshold.
fapDevDown	The specified FortiAP device is down.
fapAcConnected	FortiAP has connected to the specified AP controller (AC).

FortiAP SNMP queries

From your SNMP manager, you can use the SNMP GET and SNMP WALK commands to query FortiAP for status information, variables values, SSID configuration, radio configuration, and so on. You can also use the SNMP SET command to configure local FortiAP variables.

Here is an example of polling FortiAP data using the *snmpwalk* command from a Linux OS computer:

$ snmpwalk -v2c -c public 10.0.28.2 .1

SNMPv2-MIB::sysDescr.0 = STRING: FortiAP-S223E

SNMPv2-MIB::sysObjectID.0 = OID: FORTINET-FORTIAP-MIB::fapHostName

DISMAN-EXPRESSION-MIB::sysUpTimeInstance = Timeticks: (27486) 0:04:34.86

SNMPv2-MIB::sysContact.0 = STRING: avizzari@fortinet.com

SNMPv2-MIB::sysName.0 = STRING: FortiAP-S223E

SNMPv2-MIB::sysLocation.0 = STRING: N/A

IF-MIB::ifNumber.0 = INTEGER: 25

...

FORTINET-FORTIAP-MIB::fapVersion.0 = STRING: PS223E-v6.2-build0229

FORTINET-FORTIAP-MIB::fapSerialNum.0 = STRING: PS223E3X170000001

FORTINET-FORTIAP-MIB::fapHostName.0 = STRING: FortiAP-S223E

FORTINET-FORTIAP-MIB::fapRegionCode.0 = STRING: E

FORTINET-FORTIAP-MIB::fapBaseMacAddr.0 = STRING: 70:4c:a5:43:7b:8

FORTINET-FORTIAP-MIB::fapBiosVer.0 = STRING: 04000002

FORTINET-FORTIAP-MIB::fapBiosDataVer.0 = INTEGER: 3

FORTINET-FORTIAP-MIB::fapSysPartNum.0 = STRING: 20155-03

FORTINET-FORTIAP-MIB::fapWtpWanMode.0 = INTEGER: wanOnly(0)

FORTINET-FORTIAP-MIB::fapWtpApAddrMode.0 = INTEGER: dhcp(0)

FORTINET-FORTIAP-MIB::fapWtpApIpAddr.0 = STRING: "192.168.1.2"

FORTINET-FORTIAP-MIB::fapWtpApIpNetmask.0 = STRING: "255.255.255.0"

FORTINET-FORTIAP-MIB::fapWtpApIpGateway.0 = STRING: "192.168.1.1"

FORTINET-FORTIAP-MIB::fapWtpApMode.0 = INTEGER: thinAp(0)

...

Wireless network examples

This section includes the following topics:

- Basic wireless network example on page 114
- Wireless network example with FortiSwitch on page 119
- Complex wireless network example on page 122

Basic wireless network example

This example uses automatic configuration to set up a basic wireless network.

To configure this wireless network, perform the following tasks:

- Configuring authentication for wireless users on page 114
- Configuring the SSID on page 115
- Adding the SSID to the FortiAP Profile on page 116
- Configuring security policies on page 116
- Connecting the FortiAP units on page 117

Configuring authentication for wireless users

You need to configure user accounts and add the users to a user group. This example shows only one account, but multiple accounts can be added as user group members.

To configure a WiFi user - GUI

1. Go to **User & Device > User Definition** and select **Create New**.
2. Select **Local User** and then click **Next**.
3. Enter a **User Name** and **Password** and then click **Next**.
4. Click **Next.**
5. Make sure that **Enable** is selected and then click **Create**.

To configure the WiFi user group - GUI

1. Go to **User & Device > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

Name	wlan_users
Type	**Firewall**
Members	Add users.

To configure a WiFi user and the WiFi user group - CLI

```
config user user
   edit "user01"
      set type password
      set passwd "asdf12ghjk"
   end
config user group
   edit "wlan_users"
      set member "user01"
   end
```

Configuring the SSID

First, establish the SSID (network interface) for the network. This is independent of the number of physical access points that will be deployed. The network assigns IP addresses using DHCP.

To configure the SSID - GUI

1. Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID**.
2. Enter the following information and select **OK**:

Interface Name		example_wifi_if
Traffic Mode		Tunnel to Wireless Controller
IP/Network Mask		10.10.110.1/24
Administrative Access		Ping (to assist with testing)
DHCP Server		Enable
	Address Range	10.10.110.2 - 10.10.110.199
	Netmask	255.255.255.0
	Default Gateway	Same As Interface IP
	DNS Server	Same as System DNS
SSID		example_wifi
Security Mode		WPA2 Enterprise
Authentication		Local, select **wlan_users** user group.
Leave other settings at their default values.		

To configure the SSID - CLI

```
config wireless-controller vap
   edit example_wifi_if
      set ssid "example_wifi"
      set broadcast-ssid enable
      set security wpa-enterprise
      set auth usergroup
      set usergroup wlan_users
```

```
      set schedule always
   end
config system interface
   edit example_wifi_if
      set ip 10.10.110.1 255.255.255.0
   end
config system dhcp server
   edit 0
        set default-gateway 10.10.110.1
      set dns-service default
      set interface "example_wifi_if"
      config ip-range
         edit 1
            set end-ip 10.10.110.199
            set start-ip 10.10.110.2
         end
      set netmask 255.255.255.0
   end
```

Adding the SSID to the FortiAP Profile

The radio portion of the FortiAP configuration is contained in the FortiAP Profile. By default, there is a profile for each platform (FortiAP model). You can create additional profiles if needed. The SSID needs to be specified in the profile.

To add the SSID to the FortiAP Profile - GUI

1. Go to **WiFi & Switch Controller > FortiAP Profiles** and edit the profile for your model of FortiAP unit.
2. In **Radio 1** and **Radio 2**, add example_wifi in **SSID**.
3. Select **OK**.

Configuring security policies

A security policy is needed to enable WiFi users to access the Internet on port1. First you create firewall address for the WiFi network, then you create the example_wifi to port1 policy.

To create a firewall address for WiFi users - GUI

1. Go to **Policy & Objects > Addresses**.
2. Select **Create New > Address**, enter the following information and select **OK**.

Name	wlan_user_net
Type	IP/Netmask
Subnet / IP Range	10.10.110.0/24
Interface	example_wifi_if
Show in Address List	Enabled

To create a firewall address for WiFi users - CLI

```
config firewall address
   edit "wlan_user_net"
      set associated-interface "example_wifi_if"
      set subnet 10.10.110.0 255.255.255.0
   end
```

To create a security policy for WiFi users - GUI

1. Go to **Policy & Objects > IPv4 Policy**and select **Create New**.
2. Enter the following information and select **OK**:

Incoming Interface	example_wifi_if
Source Address	wlan_user_net
Outgoing Interface	port1
Destination Address	All
Schedule	always
Service	ALL
Action	ACCEPT
NAT	ON. Select **Use Destination Interface Address** (default).
Leave other settings at their default values.	

To create a firewall policy for WiFi users - CLI

```
config firewall policy
   edit 0
      set srcintf "example_wifi"
      set dstintf "port1"
      set srcaddr "wlan_user_net"
      set dstaddr "all"
      set schedule always
      set service ALL
      set action accept
      set nat enable
   end
```

Connecting the FortiAP units

You need to connect each FortiAP unit to the FortiGate unit, wait for it to be recognized, and then assign it to the AP Profile. But first, you must configure the interface to which the FortiAP units connect and the DHCP server that assigns their IP addresses.

In this example, the FortiAP units connect to port3 and are controlled through IP addresses on the 10.10.70.0/24 network.

To configure the interface for the AP unit - GUI

1. Go to **Network > Interfaces**, and edit the interface to which the AP unit connects (in this example, port3).
2. In **Addressing mode**, select **Manual.**
3. In **IP/Network Mask**, enter an IP address and netmask for the interface (in this example, 10.10.70.1/255.255.255.0).
4. In the Administrative Access section, go to **IPv4** and select the **CAPWAP** checkbox.

   Note: In FortiOS 6.2.3 and later, select the **Security Fabric Connection** checkbox.
5. When FortiAP units are connected to the interface on FortiGate (directly or through a switch), you can go to the Edit Interface section and set the **Role** to **LAN**.

   Selecting the LAN role loads the DHCP Server toggle. If you enable **DHCP Server**, the GUI can automatically set the DHCP IP range based on the interface IP address.
6. Click **OK**.

To configure the interface for the AP unit - CLI

Configure the interface for FortiOS 6.2.2 and earlier:

```
config system interface
   edit "port3"
      set mode static
      set ip 10.10.70.1 255.255.255.0
      set allowaccess capwap
   next
end
```

Configure the interface for FortiOS 6.2.3 and later:

```
config system interface
   edit "port3"
      set mode static
      set ip 10.10.70.1 255.255.255.0
      set allowaccess fabric
   next
end
```

To configure the DHCP server for AP units - CLI

```
config system dhcp server
   edit 3
      set interface "port3"
      config exclude-range
         edit 1
            set start-ip 10.10.70.1
            set end-ip 10.10.70.1
         next
      end
      config ip-range
         edit 1
            set start-ip 10.10.70.2
            set end-ip 10.10.70.254
         next
      end
      set default-gateway 10.10.70.1
      set netmask 255.255.255.0
```

```
        set vci-match enable
        set vci-string "FortiAP"
    next
end
```

To connect a FortiAP unit - GUI

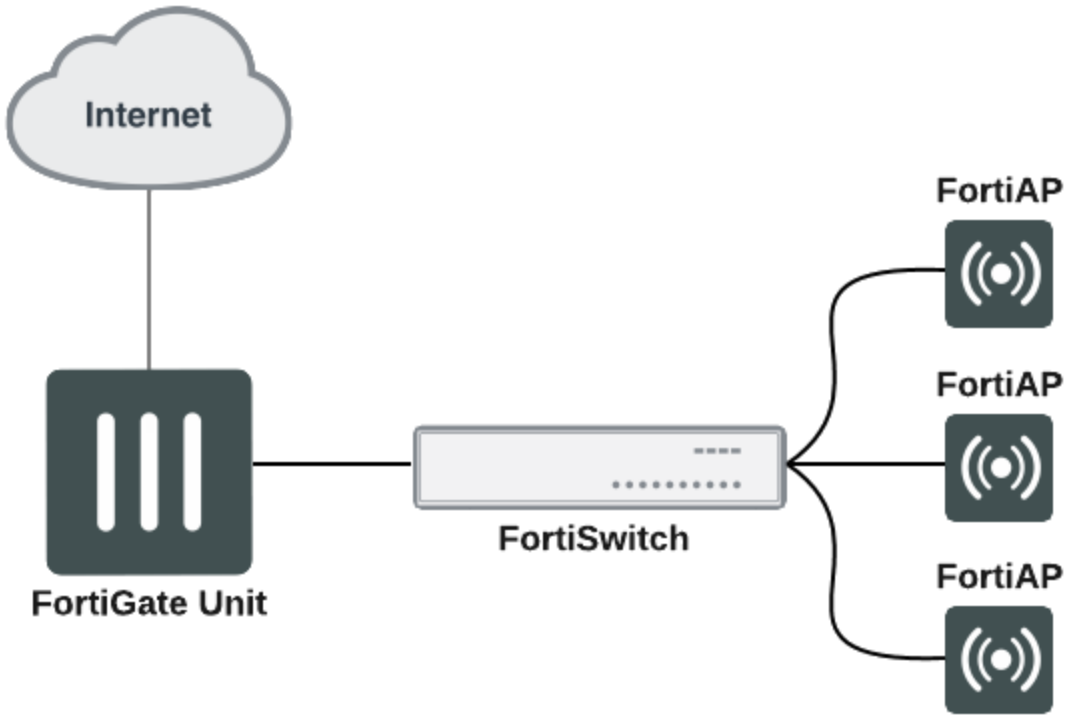
1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Connect the FortiAP unit to port 3.
3. Periodically select **Refresh** while waiting for the FortiAP unit to be listed.
   Recognition of the FortiAP unit can take up to two minutes.
   If FortiAP units are connected but cannot be recognized, try disabling VCI-Match in the DHCP server settings.
4. When the FortiAP unit is listed, select the entry to edit it.
   The **Edit Managed Access Point** window opens.
5. In **State**, select **Authorize.**
6. In **FortiAP Profile**, select the default profile for the FortiAP model.
7. Select **OK**.
8. Repeat Steps 2 through 7 for each FortiAP unit.

To connect a FortiAP unit - CLI

1. Connect the FortiAP unit to port 3.
2. Enter
   `config wireless-controller wtp`
3. Wait 30 seconds, then enter `get`.
4. Retry the `get` command every 15 seconds or so until the unit is listed, like this:
   == [FAP22B3U10600118]
   wtp-id: FAP22B3U10600118
5. Edit the discovered FortiAP unit like this:
   ```
   edit FAP22B3U10600118
   set admin enable
   end
   ```
6. Repeat Steps 2 through 5 for each FortiAP unit.

Wireless network example with FortiSwitch

This example uses automatic configuration to set up a basic network using a FortiGate <-> FortiSwitch <-> FortiAP topology.



To configure this network, perform the following tasks:

1. Configure FortiLink on your FortiGate unit.
2. Physically connect your FortiSwitch to the FortiGate.
3. Configure a wireless VLAN for your APs.
4. Connect your FortiAPs to the FortiSwitch and authorize your FortiAPs from the FortiGate.

Configuring FortiLink

FortiLink is a management protocol that enables FortiGates to manage any FortiSwitches connected to the FortiGate. Before connecting the FortiSwitch to the FortiGate unit, ensure the switch controller feature is enabled on the FortiGate. Once the feature is enabled, you can configure the FortiLink interface by assigning FortiGate interfaces as the designated FortiLink port.

Enable the switch controller feature

1. Go to **System > Feature Visibility**.
2. From the Core Features list, enable the **Switch Controller** toggle.
3. Click **Apply**.
   The WiFi & Switch Controller menu option now shows in the FortiGate navigation menu.

Configure the FortiLink interface

1. Go to **[[[Undefined variable FortiOSGUIVariables.WiFi Controller > FortiLink Interface]]]**.
2. In the **Interface members** field, click + and select the interface(s) you want to designate as FortiLink interface members.

   Note: If you do not see any interfaces listed in the Select Entries pane, it means there are no available unused or unreferenced physical interfaces and you must free up an interface from other configurations.
3. Configure the IP/Network Mask for your network.
4. Click **Apply**.

For more detailed instructions, refer to the FortiSwitch Managed Switch guide.

Connecting the FortiSwitch

Some FortiSwitch models provide designated ports for the FortiLink connection, check the hardware manual to see which port is the designated FortiLink port.

Connect the FortiSwitch

1. Connect the FortiSwitch to the FortiGate unit via the FortiLink interface you assigned earlier.
2. Go to **[[[Undefined variable FortiOSGUIVariables.WiFi Controller > Managed FortiSwitch]]]** and locate your switch.

   Note: It may take a few minutes for the switch to show up.
3. Once the FortiSwitch shows up, right-click the switch and select **Authorize**.

Configuring a wireless VLAN

Once the FortiSwitch is connected to the FortiGate and authorized, you can use a default VLAN or create a FortiSwitch VLAN to place your FortiAPs in. A new VLAN sub-interface is created under the FortiLink interface, and it will manage the IP address assignment of your FortiAPs.

Create a FortiSwitch VLAN

1. Go to **[[[Undefined variable FortiOSGUIVariables.WiFi Controller > FortiSwitch VLANs]]]** and click **Create New**.
2. Configure the following fields:
   - **Interface Name:** Create a name for the VLAN.
   - **VLAN ID:** Enter a number (1-4094).
   - **Role:** Select LAN.
3. Select the Manual Address mode and input an IP/Netmask.
4. Under Administrative Access, enable **Security Fabric Connection** and any other access options you want.
5. Enable **DHCP Server**. Edit the default address range if needed.
6. When you finished, click **OK**.

For more detailed instructions on creating a FortiSwitch VLAN, refer to the FortiSwitch Managed Switch guide.

Once you create a FortiSwitch VLAN, assign the VLAN to the FortiSwitch ports you want to connect a FortiAP to.

Assign a VLAN to a FortiSwitch port

1. Go to **[[[Undefined variable FortiOSGUIVariables.WiFi Controller > FortiSwitch Ports]]]** and locate the port you want to connect a FortiAP to.
2. Click to select the port and click the edit icon in the Native VLAN column to change the VLAN.
   The Select Entries menu loads.
3. From the Select Entries menu, select the FortiSwitch VLAN you created and click **Apply**.

Connecting the FortiAP units

After you apply the FortiAP VLAN to a FortiSwitch port, you can connect a FortiAP unit to that FortiSwitch Port. Wait a few minutes for the FortiAP to be recognized, and then authorize the FortiAP.

Connect a FortiAP unit

1. Connect the FortiAP to the FortiSwitch port you've assigned the FortiAP VLAN.
2. Go to **WiFi & Switch Controller > Managed FortiAPs** and wait for the FortiAP unit to be listed.
   Note: Recognition of the FortiAP unit can take up to two minutes, you can periodically click the **Refresh** button.
3. When the FortiAP unit is listed, right-click and select **Authorize** to authorize the unit.
   The FortiAP can now be managed by FortiGate through a FortiSwitch.

Once the FortiAP is connected and authorized by the FortiGate, you can configure SSIDs and attach profiles to allow wireless access to the AP. For instructions on setting up your wireless network, see Wireless network configuration tasks on page 16.

Complex wireless network example

This example creates multiple networks and uses custom AP profiles.

Scenario example

In this example, Example Co. provides two wireless networks, one for its employees and the other for customers or other guests of its business. Guest users have access only to the Internet, not to the company's private network. The equipment for these WiFi networks consists of FortiAP-220B units controlled by a FortiGate unit.

The employee network operates in 802.11n mode on both the 2.4 GHz and 5 GHz bands. Client IP addresses are in the 10.10.120.0/24 subnet, with 10.10.120.1 the IP address of the WAP. The guest network also operates in 802.11n mode, but only on the 2.4 GHz band. Client IP addresses are on the 10.10.115.0/24 subnet, with 10.10.115.1 the IP address of the WAP.

On FortiAP-220B units, the 802.11n mode also supports 802.11g and 802.11b clients on the 2.4 GHz band and 802.11a clients on the 5 GHz band.

The guest network WAP broadcasts its SSID, the employee network WAP does not.

The employee network uses WPA-Enterprise authentication through a FortiGate user group. The guest network features a captive portal. When a guest first tries to connect to the Internet, a login page requests logon credentials. Guests use numbered guest accounts authenticated by RADIUS. The captive portal for the guests includes a disclaimer page.

In this example, the FortiAP units connect to port 3 and are assigned addresses on the 192.168.8.0/24 subnet.

Configuration example

To configure these wireless networks, perform the following tasks:

- Configuring authentication for employee wireless users on page 123
- Configuring authentication for guest wireless users on page 124
- Configuring the SSIDs on page 125
- Configuring the FortiAP profile on page 127
- Configuring firewall policies on page 128
- Connecting the FortiAP units on page 130

Configuring authentication for employee wireless users

Employees have user accounts on the FortiGate unit. This example shows creation of one user account, but you can create multiple accounts and add them as members to the user group.

To configure a WiFi user - GUI

1. Go to **User & Device > User Definition** and select **Create New**.
2. Select **Local User** and then click **Next**.
3. Enter a **User Name** and **Password** and then click **Next**.
4. Click **Next**.
5. Make sure that **Enable** is selected and then click **Create**.

To configure the user group for employee access - GUI

1. Go to **User & Device > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

Name	employee-group
Type	**Firewall**
Members	Add users.

To configure a WiFi user and the user group for employee access - CLI

```
config user user
   edit "user01"
      set type password
      set passwd "asdf12ghjk"
   end
config user group
   edit "employee-group"
```

```
    set member "user01"
  end
```

The user authentication setup will be complete when you select the employee-group in the SSID configuration.

Configuring authentication for guest wireless users

Guests are assigned temporary user accounts created on a RADIUS server. The RADIUS server stores each user's group name in the Fortinet-Group-Name attribute. Wireless users are in the group named "wireless".

The FortiGate unit must be configured to access the RADIUS server.

To configure the FortiGate unit to access the guest RADIUS server - GUI

1. Go to **User & Device > RADIUS Servers** and select **Create New**.
2. Enter the following information and select OK:

Name	guestRADIUS
Primary Server IP/Name	10.11.102.100
Primary Server Secret	grikfwpfdfg
Secondary Server IP/Name	Optional
Secondary Server Secret	Optional
Authentication Scheme	Use default, unless server requires otherwise.
Leave other settings at their default values.	

To configure the FortiGate unit to access the guest RADIUS server - CLI

```
config user radius
  edit guestRADIUS
    set auth-type auto
    set server 10.11.102.100
    set secret grikfwpfdfg
  end
```

To configure the user group for guest access - GUI

1. Go to **User & Device > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

Name	guest-group
Type	**Firewall**
Members	Leave empty.

3. Select **Create new**.

4. Enter:

Remote Server	Select **guestRADIUS**.
Groups	Select `wireless`.

5. Select **OK**.

To configure the user group for guest access - CLI

```
config user group
   edit "guest-group"
      set member "guestRADIUS"
      config match
         edit 0
            set server-name "guestRADIUS"
            set group-name "wireless"
         end
   end
```

The user authentication setup will be complete when you select the guest-group user group in the SSID configuration.

Configuring the SSIDs

First, establish the SSIDs (network interfaces) for the employee and guest networks. This is independent of the number of physical access points that will be deployed. Both networks assign IP addresses using DHCP.

To configure the employee SSID - GUI

1. Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID**.
2. Enter the following information and select **OK**:

Interface Name	example_inc
Traffic Mode	Tunnel to Wireless Controller
IP/Netmask	10.10.120.1/24
Administrative Access	Ping (to assist with testing)
Enable DHCP	Enable
Address Range	10.10.120.2 - 10.10.120.199
Netmask	255.255.255.0
Default Gateway	Same As Interface IP
DNS Server	Same as System DNS
SSID	example_inc
Security Mode	WPA/WPA2-Enterprise
Authentication	Select **Local**, then select **employee-group**.
Leave other settings at their default values.	

To configure the employee SSID - CLI

```
config wireless-controller vap
   edit example_inc
      set ssid "example_inc"
      set security wpa-enterprise
      set auth usergroup
      set usergroup employee-group
      set schedule always
   end
config system interface
   edit example_inc
      set ip 10.10.120.1 255.255.255.0
   end
config system dhcp server
   edit 0
      set default-gateway 10.10.120.1
      set dns-service default
      set interface example_inc
      config ip-range
         edit 1
            set end-ip 10.10.120.199
            set start-ip 10.10.120.2
         end
      set lease-time 7200
      set netmask 255.255.255.0
   end
```

To configure the example_guest SSID - GUI

1. Go to **WiFi & Switch Controller > SSID** and select **Create New**.
2. Enter the following information and select **OK**:

Name	example_guest
IP/Netmask	10.10.115.1/24
Administrative Access	Ping (to assist with testing)
Enable DHCP	Enable
Address Range	10.10.115.2 - 10.10.115.50
Netmask	255.255.255.0
Default Gateway	Same as Interface IP
DNS Server	Same as System DNS
SSID	example_guest
Security Mode	Captive Portal
Portal Type	Authentication
Authentication Portal	Local
User Groups	Select **guest-group**.

Leave other settings at their default values.

To configure the example_guest SSID - CLI

```
config wireless-controller vap
   edit example_guest
      set ssid "example_guest"
      set security captive-portal
      set selected-usergroups guest-group
      set schedule always
   end
config system interface
   edit example_guest
      set ip 10.10.115.1 255.255.255.0
   end
config system dhcp server
   edit 0
      set default-gateway 10.10.115.1
      set dns-service default
      set interface "example_guest"
      config ip-range
         edit 1
            set end-ip 10.10.115.50
            set start-ip 10.10.115.2
         end
      set lease-time 7200
      set netmask 255.255.255.0
   end
```

Configuring the FortiAP profile

The FortiAP Profile defines the radio settings for the networks. The profile provides access to both Radio 1 (2.4 GHz) and Radio 2 (5 GHz) for the employee virtual AP, but provides access only to Radio 1 for the guest virtual AP.

To configure the FortiAP Profile - GUI

1. Go to **WiFi & Switch Controller > FortiAP Profiles** and select **Create New**.
2. Enter the following information and select **OK**:

Name	example_AP
Platform	FAP220B
Radio 1	
Mode	Access Point
Band	802.11n
Channel	Select 1, 6, and 11.
Tx Power	100%
SSID	**Select SSIDs** and select **example_inc** and **example_guest**.

Radio 2	
Mode	Access Point
Band	802.11n_5G
Channel	Select all.
Tx Power	100%
SSID	**Select SSIDs** and select **example_inc**.

To configure the AP Profile - CLI

```
config wireless-controller wtp-profile
   edit "example_AP"
      config platform
         set type 220B
      end
      config radio-1
         set ap-bgscan enable
         set band 802.11n
         set channel "1" "6" "11"
         set vaps "example_inc" "example_guest"
      end
      config radio-2
         set ap-bgscan enable
         set band 802.11n-5G
         set channel "36" "40" "44" "48" "149" "153" "157" "161" "165"
         set vaps "example_inc"
      end
```

Configuring firewall policies

Identity-based firewall policies are needed to enable the WLAN users to access the Internet on Port1. First you create firewall addresses for employee and guest users, then you create the firewall policies.

To create firewall addresses for employee and guest WiFi users

1. Go to **Policy & Objects > Addresses**.
2. Select **Create New**, enter the following information and select **OK**.

Address Name	employee-wifi-net
Type	Subnet / IP Range
Subnet / IP Range	10.10.120.0/24
Interface	example_inc

3. Select **Create New**, enter the following information and select **OK**.

Address Name	guest-wifi-net

Type	Subnet / IP Range
Subnet / IP Range	10.10.115.0/24
Interface	example_guest

To create firewall policies for employee WiFi users - GUI

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Enter the following information and select **OK**:

Incoming Interface	example_inc
Source Address	employee-wifi-net
Outgoing Interface	port1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enable NAT

3. Optionally, select security profile for wireless users.
4. Select **OK**.
5. Repeat steps 1 through 4 but select Internal as the Destination Interface/Zone to provide access to the ExampleCo private network.

To create firewall policies for employee WiFi users - CLI

```
config firewall policy
   edit 0
      set srcintf "employee_inc"
      set dstintf "port1"
      set srcaddr "employee-wifi-net"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ANY"
      set nat enable
      set schedule "always"
      set service "ANY"
   next
   edit 0
      set srcintf "employee_inc"
      set dstintf "internal"
      set srcaddr "employee-wifi-net"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ANY"
      set nat enable
      set schedule "always"
```

```
    set service "ANY"
  end
```

To create a firewall policy for guest WiFi users - GUI

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Enter the following information and select **OK**:

Incoming Interface	example_guest
Source Address	guest-wifi-net
Outgoing Interface	port1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enable NAT

3. Optionally, select **UTM** and set up UTM features for wireless users.
4. Select **OK**.

To create a firewall policy for guest WiFi users - CLI

```
config firewall policy
  edit 0
    set srcintf "example_guest"
    set dstintf "port1"
    set srcaddr "guest-wifi-net"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
    set nat enable
  end
```

Connecting the FortiAP units

You need to connect each FortiAP-220B unit to the FortiGate unit, wait for it to be recognized, and then assign it to the AP Profile. But first, you must configure the interface to which the FortiAP units connect and the DHCP server that assigns their IP addresses.

In this example, the FortiAP units connect to port 3 and are controlled through IP addresses on the 10.10.70.0/24 network.

To configure the interface for the AP unit - GUI

1. Go to **Network > Interfaces**, and edit the interface to which the AP unit connects (in this example, port3).
2. In **Addressing mode**, select **Manual.**

3. In **IP/Network Mask**, enter an IP address and netmask for the interface (in this example, 10.10.70.1/255.255.255.0).
4. In the Administrative Access section, go to **IPv4** and select the **CAPWAP** checkbox.

   Note: In FortiOS 6.2.3 and later, select the **Security Fabric Connection** checkbox.
5. When FortiAP units are connected to the interface on FortiGate (directly or through a switch), you can go to the Edit Interface section and set the **Role** to **LAN**.

   Selecting the LAN role loads the DHCP Server toggle. If you enable **DHCP Server**, the GUI can automatically set the DHCP IP range based on the interface IP address.
6. Click **OK**.

To configure the interface for the AP unit - CLI

To configure the interface for the AP unit - CLI

In the CLI, you must configure the interface IP address and DHCP server separately.

Configure the interface for FortiOS 6.2.2 and earlier:

```
config system interface
   edit "port3"
      set mode static
      set ip 10.10.70.1 255.255.255.0
      set allowaccess capwap
   next
end
```

Configure the interface for FortiOS 6.2.3 and later:

```
config system interface
   edit "port3"
      set mode static
      set ip 10.10.70.1 255.255.255.0
      set allowaccess fabric
   next
end
```

To configure the DHCP server for AP units - CLI

```
config system dhcp server
   edit 3
      set interface "port3"
      config ip-range
         edit 1
            set start-ip 10.10.70.2
            set end-ip 10.10.70.254
         next
      end
      set default-gateway 10.10.70.1
      set netmask 255.255.255.0
      set vci-match enable
      set vci-string "FortiAP"
   next
end
```

The optional `vci-match` and `vci-string` fields ensure that the DHCP server will provide IP addresses only to FortiAP units.

To connect a FortiAP-220B unit - GUI

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Connect the FortiAP unit to port 3.
3. Periodically select **Refresh** while waiting for the FortiAP unit to be listed.
   Recognition of the FortiAP unit can take up to two minutes.
   If there is persistent difficulty recognizing FortiAP units, try disabling VCI-Match in the DHCP server settings.
4. When the FortiAP unit is listed, select the entry to edit it.
   The **Edit Managed Access Point** window opens.
5. In **State**, select **Authorize.**
6. In the **AP Profile,** select **[Change]** and then select the **example_AP** profile.
7. Select **OK**.
8. Repeat Steps 2 through 7 for each FortiAP unit.

To connect a FortiAP-220B unit - CLI

1. Connect the FortiAP unit to port 3.
2. Enter:
   ```
   config wireless-controller wtp
   ```
3. Wait 30 seconds, then enter `get`.
4. Retry the `get` command every 15 seconds or so until the unit is listed, like this:
   == [FAP22B3U10600118]

   wtp-id: FAP22B3U10600118
5. Edit the discovered FortiAP unit like this:
   ```
   edit FAP22B3U10600118
      set admin enable
      set wtp-profile example_AP
   end
   ```
6. Repeat Steps 2 through 5 for each FortiAP unit.

FortiWiFi unit as a wireless client

A FortiWiFi unit operates by default as a wireless access point. But a FortiWiFi unit can also operate as a wireless client, connecting the FortiGate to another wireless network.

This section includes the following topics:

- FortiWiFi unit in client mode
- Configuring a FortiWiFi unit as a wireless client

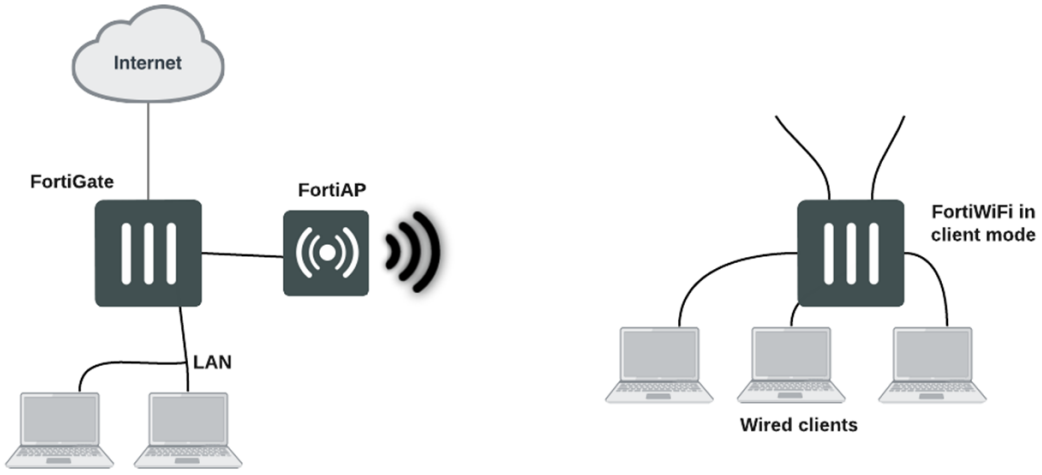
FortiWiFi unit in client mode

In client mode, the FortiWiFi unit connects to a remote WiFi access point to access other networks or the Internet. This is most useful when the FortiWiFi unit is in a location that does not have a wired infrastructure.

For example, in a warehouse where shipping and receiving are on opposite sides of the building, running cables might not be an option due to the warehouse environment. The FortiWiFi unit can support wired users using its Ethernet ports and can connect to another wireless access point as a client. This connects the wired users to the network using the 802.11 WiFi standard as a backbone.

In client mode, the FortiWiFi unit cannot operate as an AP. WiFi clients cannot see or connect to the FortiWiFi unit in client mode.

FortiWiFi unit in client mode



Configuring a FortiWiFi unit as a wireless client

To set up the FortiWiFi unit as a wireless client, you must use the CLI. Before you do this, make sure to remove any AP WiFi configurations such as SSIDs, DHCP servers, and policies.

To configure wireless client mode

1. Change the wireless mode to client. In the CLI, enter the following commands:
```
config system global
   set wireless-mode client
end
```
2. Respond “y” when asked if you want to continue. The FortiWiFi unit reboots.
3. Configure the WiFi interface settings.
   For example, to configure the client for WPA-Personal authentication on the **our_wifi** SSID with passphrase **justforus**, enter the following in the CLI:
```
config system interface
   edit wifi
      set mode dhcp
      config wifi-networks
         edit 0
            set wifi-ssid our_wifi
               set wifi-security wpa-personal
               set wifi-passphrase "justforus"
            end
      end
```
   The WiFi interface client_wifi receives an IP address using DHCP.
4. Configure a WiFi to port1 policy.
   You can use either CLI or GUI to do this. The important settings are:

Incoming Interface (srcintf)	wifi
Source Address (srcaddr)	all
Outgoing Interface (dstintf)	port1
Destination Address (dstaddr)	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Selected

Controlled AP selection support in FortiWiFi client mode

Use the following CLI commands to provide a more controlled AP selection method (supported in FortiWiFi client mode).

Syntax

```
config system interface
   edit {name}
      set wifi-ap-band {any | 5g-preferred | 5g-only}
   next
end
```

Support for location-based services

FortiOS supports location-based services by collecting information about WiFi devices near FortiGate-managed access points, even if the devices do not associate with the network.

WiFi devices broadcast packets as they search for available networks. The FortiGate WiFi controller can collect information about the interval, duration, and signal strength of these packets. The Euclid Analytics service uses this information to track the movements of the device owner. A typical application of this technology is to analyze shopper behavior in a shopping center. Which stores do people walk past? Which window displays do they stop to look at? Which stores do they enter and how long do they spend there? The shoppers are not personally identified, each is known only by the MAC address of their WiFi device.

After enabling location tracking on the FortiGate unit, you can confirm that the feature is working by using a specialized diagnostic command to view the raw tracking data. The Euclid Analytics service obtains the same data in its proprietary format using a JSON inquiry through the FortiGate GUI interface.

Configuring location tracking

You can enable location tracking in any FortiAP profile, using the CLI. Location tracking is part of location-based services. Set the `station-locate` field to `enable`. For example:

```
config wireless-controller wtp-profile
   edit "FAP220B-locate"
      set ap-country US
      config platform
         set type 220B
      end
      config lbs
         set station-locate enable
      end
   end
```

Automatic deletion of outdated presence data

The FortiGate generates a log entry only the first time that station-locate detects a mobile client. No log is generated for clients that have been detected before. To log repeat client visits, previous station presence data must be deleted (flushed). The sta-locate-timer can flush this data periodically. The default period is 1800 seconds (30 minutes). The timer can be set to any value between 1 and 86400 seconds (24 hours). A setting of 0 disables the flush, meaning a client is logged only on the very first visit.

The timer is one of the wireless controller timers and it can be set in the CLI. For example:

```
config wireless-controller timers
   set sta-locate-timer 1800
end
```

To avoid the duplication of logs, set the sta-locate-timer value to be more that the sta-capability-timer value (default 30 seconds).

FortiPresence push REST API

When the FortiGate is located on a private IP network, the FortiPresence server cannot poll the FortiGate for information. Instead, the FortiGate must be configured to push the information to the FortiPresence server.

Enter the following command:

```
config wireless-controller wtp-profile
   edit "FP223B-GuestWiFi"
      config lbs
         set fortipresence {enable | disable}
         set fortipresence-server <ip-address> Default is 3000.
         set fortipresence-port <port>
         set fortipresence-secret <password>
         set fortipresence-project <name>
         set fortipresence-frequency <5-65535> Default is 30.
         set fortipresence-rogue {enable | disable} Enable/disable reporting of Rogue APs.
         set fortipresence-unassoc {enable | disable} Enable/disable reporting of
              unassociated devices.
      end
end
```

Viewing device location data on a FortiGate unit

You can use the FortiGate CLI to list located devices. This is mainly useful to confirm that the location data feature is working, You can also reset device location data.

To list located devices

```
diag wireless-controller wlac -c sta-locate
```

To reset device location data

```
diag wireless-controller wlac -c sta-locate-reset
```

Example output

The following output shows data for three WiFi devices.

```
FWF60C3G11004319 # diagnose wireless-controller wlac -c sta-locate
   sta_mac vfid rid base_mac freq_lst frm_cnt frm_fst frm_last intv_sum intv2_sum intv3_sum
        intv_min intv_max signal_sum signal2_sum signal3_sum sig_min sig_max sig_fst sig_
        last ap

   00:0b:6b:22:82:61 0
   FAP22B3U11005354 0 0 00:09:0f:f1:bb:e4 5745 257 708 56 651 1836 6441 0 12 -21832 1855438
        -157758796 -88 -81 -84 -88 0

   00:db:df:24:1a:67 0
   FAP22B3U11005354 0 0 00:09:0f:f1:bb:e4 5745 42 1666 41 1625 97210 5831613 0 60 -3608
        310072 -26658680 -90 -83 -85 -89 0
```

```
10:68:3f:50:22:29 0
FAP22B3U11005354 0 0 00:09:0f:f1:bb:e4 5745 102 1623 58 1565 94136 5664566 0 60 -8025
     631703 -49751433 -84 -75 -78 -79 0
```

The output for each device appears on two lines. The first line contains only the device MAC address and the VLAN ID. The second line begins with the ID (serial number) of the FortiWiFi or FortiAP unit that detected the device, the AP MAC address, and then the fields that the Euclid service uses. Because of its length, this line wraps around and displays as multiple lines.

Troubleshooting

To troubleshoot the FortiOS wireless controller and FortiAP units, this section includes the following topics:

- FortiAP shell command on page 139
- Signal strength issues on page 139
- Throughput issues on page 143
- Client connection issues on page 145
- FortiAP connection issues on page 147
- Best practices for OSI common sources of wireless issues on page 150
- Packet sniffer on page 153
- Debug commands on page 157

FortiAP shell command

The FortiAP is often behind a NAT device and access to the FortiAP through SSH is not available. The FortiGate WiFi controller can send a FortiAP shell command (up to 127 bytes) to the FortiAP. The FortiAP runs this command and then returns the results to the controller using the Control and Provisioning of Wireless Access Points Protocol (CAPWAP) tunnel.

The maximum output from a FortiAP shell command is limited to 4 MB. The default output size is set to 32 KB.

The FortiAP reports the running results to the controller after the command is finished. If the controller sends a new command to the FortiAP before the previous command is finished, the previous command is canceled.

Enter the following command:

```
diag w-c wlac wtpcmd wtp_ip wtp_port cmd [cmd-to-ap] cmd: run,show,showhex,clr,r&h,r&sh
```

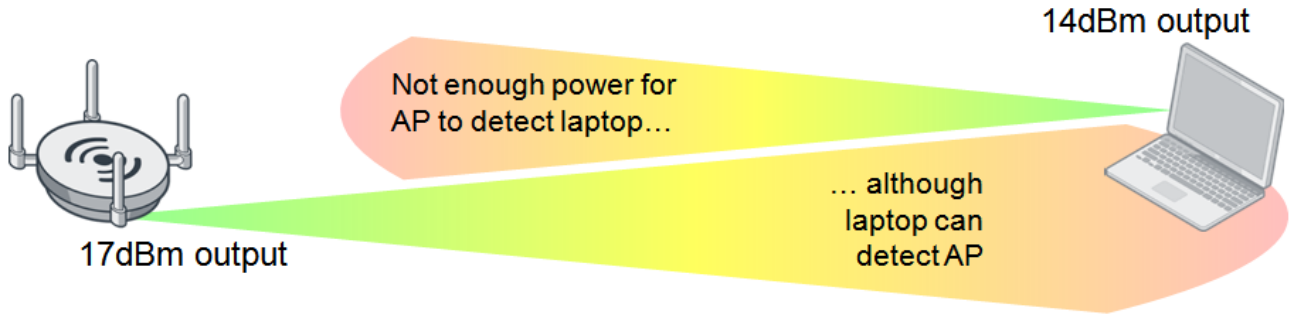
- **cmd-to-ap:** any shell commands, but FortiAP does not report results until the command is finished on the FortiAP
- **run:** controller sends the ap-cmd to the FortiAP to run
- **show:** show current results reported by the FortiAP in text
- **showhex:** show current results reported by the FortiAP in hexadecimal format.
- **clr:** clear reported results
- **r&s:** run and show
- **r&sh:** run and show in hexadecimal format

Signal strength issues

This section includes information to help you identify and troubleshoot poor signal strength issues.

Asymmetric power issue

Asymmetric power issues are a typical problem in wireless communications. Access points (AP) can have a high transmit power which means that a signal can travel a long distance. However, clients may not have a transmit power strong enough for the APs to detect their signal.



Measuring signal strength in both directions

To solve an asymmetric power issue, measure the signal strength in both directions. APs usually have enough power to transmit long distances, but sometimes battery-powered clients have a reply signal that has less power, and therefore the AP cannot detect their signal.

It is recommended that you match the transmission power of the AP to the least powerful wireless client—around 10 decibels per milliwatt (dBm) for iPhones and 14 dBm for most laptops.

Even if the signal is strong enough, other devices may also emit radiation and cause interference. To identify the difference, read the client Rx strength from the FortiGate GUI (under **Monitor > WiFi Client Monitor**) or CLI.

The **Signal Strength/Noise** value provides the received signal strength indicator (RSSI) of the wireless client. For example, a value of -85 dBm to -95 dBm is equal to about 10 dB levels; this is not a desirable signal strength. In the following screenshot, one of the clients is at 18 dB, which is getting close to the perimeter of its range.

SSID	FortiAP	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal
MavisF	FAP28C3X13000119 (1)	10.0.2.8	e8:91:20:90:6e:23	6	1 kbps	29 dB	
MavisF	FP320C3X14000668 (1)	192.168.255.112	1c:69:a5:c8:e8:3e	11	80 bps	35 dB	
MavisF	FP320C3X14000668 (2)	192.168.255.101	58:55:ca:36:28:7d	44	12 kbps	51 dB	
MavisF	FAP28C3X13000119 (1)	10.0.2.9	Acer A1-830 Tablet	6	543 bps	18 dB	
MavisF	FAP28C3X13000119 (1)	10.0.2.13	08:ed:b9:4f:98:ad	6	16 kbps	31 dB	
MavisF	FP320C3X14000668 (1)	192.168.255.115	Ellas_Tablet	11	0 bps	35 dB	

The recommended Signal Strength/Noise value from and to the FortiAP by clients is in the range of -20 dBm to -65 dBm.

You can also confirm the transmission (Tx) power of the controller on the AP profile (`wtp-profile`) and the FortiAP (`iwconfig`), and check the power management (auto-Tx) options.

Controller configured transmitting power - CLI:

```
config wireless-controller wtp-profile
```

```
config <radio>
   show
```

(the following output is limited to power levels)

```
        auto-power-level : enable
        auto-power-high : 17
        auto-power-low : 10
```

Actual FortiAP transmitting power - CLI:

```
iwconfig wlan00
```

Result:

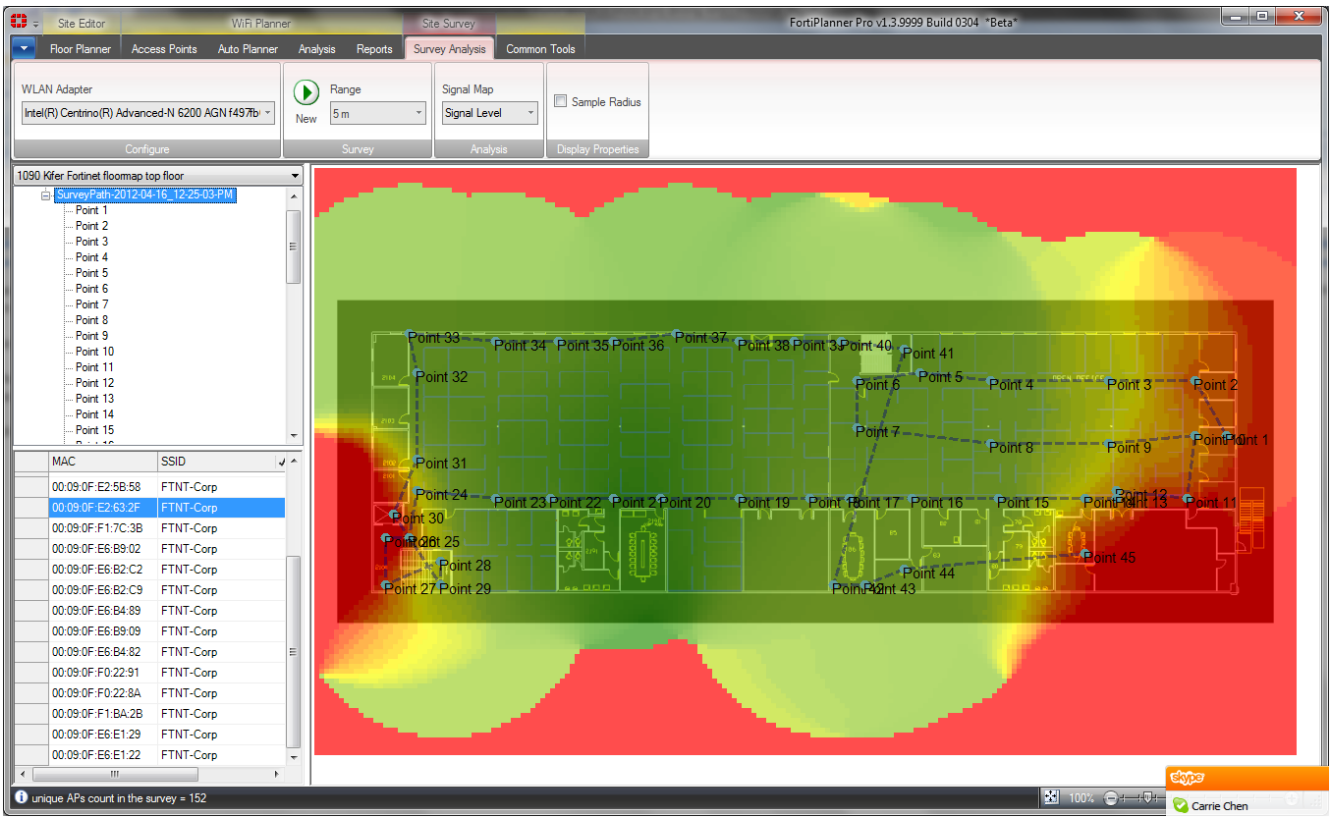
```
wlan00 IEEE 802.11ng ESSID:"signal-check"
Mode:Master Frequency:2.412 GHz   Access Point:<MAC add>
Bit Rate:130 Mb/s Tx-Power=28 dBm
```

Using FortiPlanner

The most thorough method to solve signal strength issues is to perform a site survey using FortiPlanner.

For details about FortiPlanner, visit the FortiPlanner website. You can download FortiPlanner here.

Sample depiction of a site survey using FortiPlanner



The site survey helps with the optimal placement for your APs based on the variables in your environment. You must provide the site survey detailed information such as a floor plan (to scale) and structural materials. FortiPlanner allows you to place the APs on the map and adjust the radio bands and power levels while providing you with visual wireless coverage.

The following list includes mechanisms for gathering further information on the client for Rx strength. The goal is to see how well the client is receiving the signal from the AP. You can also verify FortiAP signal strength on the client using WiFi client utilities, or third-party utilities such as InSSIDer or MetaGeek Chanalyzer.

- Professional Site Survey software (Ekahau, AirMagnet survey Pro, FortiPlanner)
- InSSIDer
- On Windows: "*netsh wlan show networks mode=bssid*" (look for the BSSID, it's in % not in dBm)
- On MacOS: Use the "*airport*" command:

"/System/Library/PrivateFrameworks/Apple80211.framework/Versions/A/Resources/airport" airport –s | grep <the_bssid> (live scan each time)

- On Android: WiFiFoFum

Frequency interference

If the wireless signal seems to be strong but then periodically drops, this may be a symptom of frequency interference. Frequency interference is when another device also emits radio frequency using the same channel, co-channel, or adjacent channel, thereby overpowering or corrupting your signal. This is a common problem on a 2.4 GHz network.

There are two types of interference: coherent and non-coherent.

- **Coherent interference** is a result of another device using the same channel as your AP, or poor planning of a wireless infrastructure. Perhaps the other nearby APs are using the same channel or the signal strength is too high.
- **Non-coherent interference** is a result of other radio signals such as Bluetooth, microwave, cordless phone, or x-ray machines (as in medical environments).

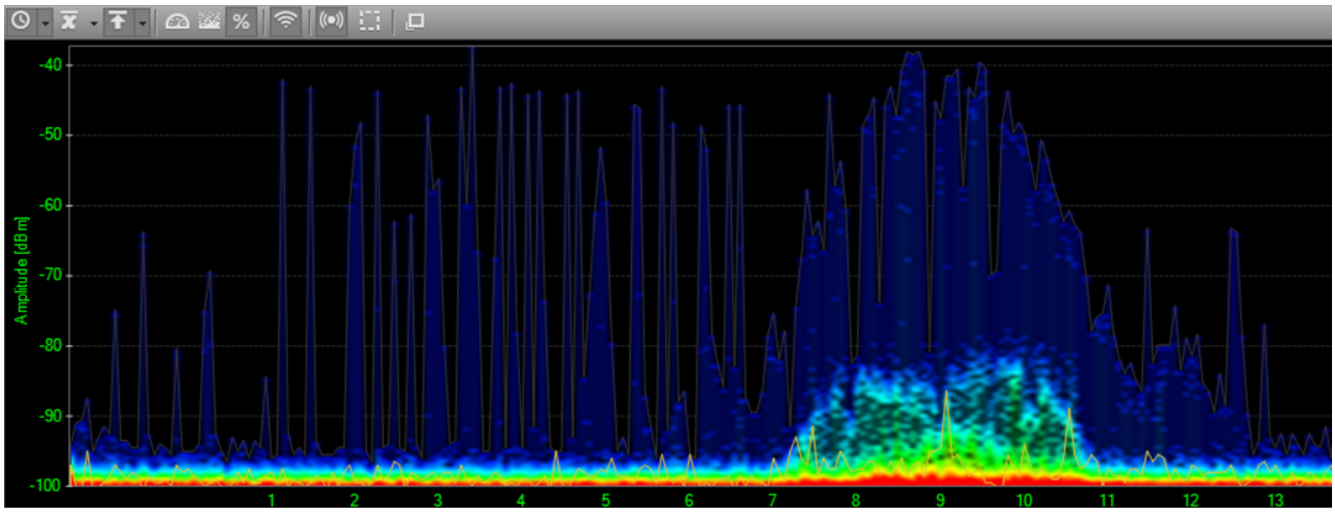
The most common and simple solution for frequency interference is to change your operation channel. Typically, the channel can be set from 1 to 11 for the broadcast frequency, although it is recommended to use channels 1, 6, and 11 on the 2.4 GHz band.

Another solution, if it is appropriate for your location, is to use the 5 GHz band instead.

MetaGeek Chanalyzer

You can perform a site survey using spectrum analysis at various points in your environment to locate sources of interference. MetaGeek Chanalyzer is an example of a third-party utility used for spectrum analysis of complex WiFi networks.

Fortinet wireless adapters ignore signals of -95 dBm or less.



Throughput issues

This section helps you identify throughput issues and suggests actions to address them.

Link testing

You can identify delays or lost packets by sending ping packets from your wireless client. If there is more than 10 ms of delay, there may be a problem with your wireless deployment, such as:

- The client transmits a week signal. The host does not reach the AP.
- The AP utilization is too high. Your AP is saturated with connected clients.
- There is interference in the wireless network. Third-party signal can degrade your AP or the client's ability to detect signals between them.
- The AP has a weak transmit power. The AP does not reach the host. This problem is not common in a properly deployed network, unless the client is too far away.

Performance testing

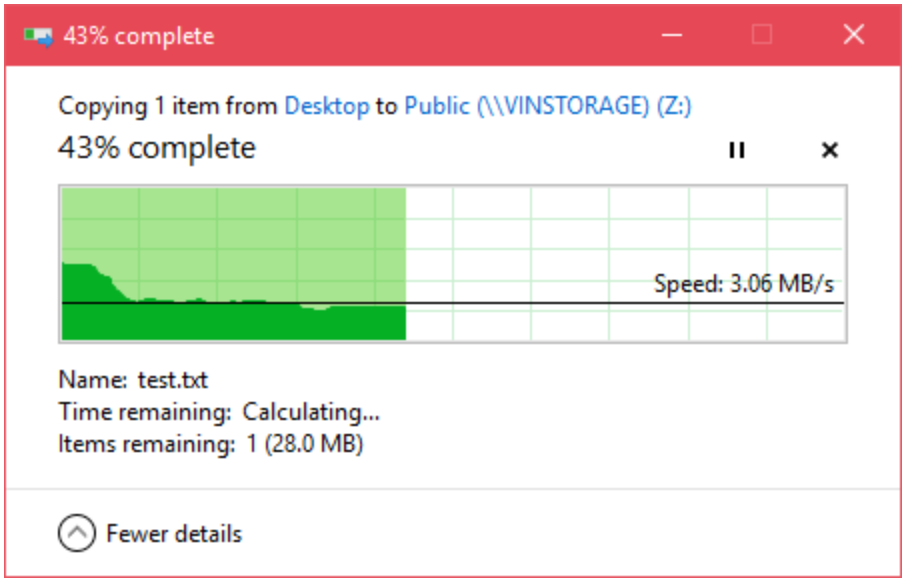
If the FortiAP gives poor throughput to the client, the link can drop. You can measure the link throughput or performance between two devices by using third-party application tools such as iPerf and jPerf.

Measuring the file transfer speed

Another way to get a sense of your throughput issues is to measure the speed of a file transfer on your network. Create a test file at a specific size and measure the speed at which Windows measures the transfer. The command below creates a 50 MB file. The file name is test.txt.

- `fsutil file createnew test.txt 52428800`

The following image shows a network transfer speed of just over 24 Mbps. The theoretical speed of 802.11g is 54 Mbps, which is what this client is using. A wireless client is never likely to see the theoretical speed.



TKIP limitation

If you find that throughput is a problem, avoid WPA security encrypted with Temporal Key Integrity Protocol (TKIP) as it supports communications only at 54 Mbps. Use WPA-2 AES instead.

Speeds are very much based on what the client computer can handle as well. The maximum client connection rate of 130 Mbps is for 2.4 GHz on a 2x2, or 300 Mbps for 5 GHz on a 2x2 (using shortguard and channel bonding enabled).

If you want to get more than 54 Mbps with 802.11n, do not use legacy TKIP, use CCMP instead. This is standard for legacy compatibility.

IP packet fragmentation prevention in CAPWAP tunnels

TKIP is not the only possible source of decreased throughput. When a wireless client sends jumbo frames using a CAPWAP tunnel, it can result in data loss, jitter, and decreased throughput. For more details, see IP fragmentation of packets in CAPWAP tunnels on page 63.

Slow DTLS response

The following elements are involved in the CAPWAP association:

- request
- response
- full of DTLS (Datagram Transport Layer Security) tunnel establishment
- join
- configuration

All of these element are bidirectional. If the DTLS response is slow, there could be a configuration error or an issue with a certificate during the discovery response. For details about the CAPWAP Protocol Specification, see RFC 5415 and RFC 5416.

Client connection issues

1. If the client is unable to connect to FortiAP:
   - Make sure the client security and authentication settings match with FortiAP and also check the certificates.
   - Try upgrading the Wi-Fi adapter driver, FortiGate and FortiAP firmware.
   - If other clients can connect, the issue can be with device interoperability. Run debug commands and sniffer packets.
   - Look for rogue suppression by sniffing the wireless traffic and looking for the connection issue in the output (using the AP or wireless packet sniffer).
   - Try changing the IEEE protocol from 802.11n to 802.11bg or 802.11a only.
2. If the client drops and reconnects:
   - The client might be de-authenticating periodically. Check the sleep mode on the client.
   - The issue could be related to power-saver settings. The client may need to update the drivers.
   - The issue could also be caused by flapping between APs. Check the roaming sensitivity settings on the client or the preferred wireless network settings on the client. If another WiFi network is available, the client may connect to it if it is a preferred network. Also, check the DHCP configuration as this configuration may be an IP conflict.
3. If the client drops and never connects:
   - The client could have roamed to another SSID. Check the standby and sleep modes.
   - You may need to bring the interface up and down.
4. If the client connects, but no IP address is acquired by the client:
   - Check the DHCP configuration and the network.
   - There could be a broadcast issue. Check the WEP encryption key and set a static IP address and VLANs.

Debugging client connection issues

To see the stage at which the client fails to connect, enable the client debug on the controller for problematic clients. Try to connect from the problematic client and run the following debug command, which allows you to see the four-way handshake of the client association:

```
diagnose wireless-controller wlac sta_filter <client MAC address> 2
```

Example of a successful client connection:

The following example debug output is for the above command. This example shows the successful association phase, DHCP phase, and the PSK key exchange (identified in color):

```
FG600B3909600253 #
91155.197 <ih> IEEE 802.11 mgmt::assoc_req <== 30:46:9a:f9:fa:34 vap signal-check rId 0 wId
     0 00:09:0f:f3:20:45
91155.197 <ih> IEEE 802.11 mgmt::assoc_resp ==> 30:46:9a:f9:fa:34 vap signal-check rId 0 wId
     0 00:09:0f:f3:20:45 resp 0
91155.197 <cc> STA_CFG_REQ(15) sta 30:46:9a:f9:fa:34 add ==> ws (0-192.168.35.1:5246) rId 0
     wId 0
```

```
91155.197 <dc> STA add 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rId 0 wId
     0 bssid 00:09:0f:f3:20:45 NON-AUTH
91155.197 <cc> STA add 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rId 0 wId
     0 00:09:0f:f3:20:45 sec WPA2 AUTO auth 0
91155.199 <cc> STA_CFG_RESP(15) 30:46:9a:f9:fa:34 <== ws (0-192.168.35.1:5246) rc 0
     (Success)
91155.199 <eh> send 1/4 msg of 4-Way Handshake
91155.199 <eh>send IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=95 replay cnt 1
91155.199 <eh> IEEE 802.1X (EAPOL 99B) ==> 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rId 0
     wId 0 00:09:0f:f3:20:45
91155.217 <eh> IEEE 802.1X (EAPOL 121B) <== 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rId 0
     wId 0 00:09:0f:f3:20:45
91155.217 <eh> recv IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=117
91155.217 <eh> recv EAPOL-Key 2/4 Pairwise replay cnt 1
91155.218 <eh> send 3/4 msg of 4-Way Handshake
91155.218 <eh> send IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=175 replay cnt 2
91155.218 <eh> IEEE 802.1X (EAPOL 179B) ==> 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rId 0
     wId 0 00:09:0f:f3:20:45
91155.223 <eh> IEEE 802.1X (EAPOL 99B) <== 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rId 0
     wId 0 00:09:0f:f3:20:45
91155.223 <eh> recv IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=95
91155.223 <eh> recv EAPOL-Key 4/4 Pairwise replay cnt 2
91155.223 <dc> STA chg 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rId 0 wId
     0 bssid 00:09:0f:f3:20:45 AUTH
91155.224 <cc> STA chg 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rId 0 wId
     0 00:09:0f:f3:20:45 sec WPA2 AUTO auth 1
91155.224 <cc> STA_CFG_REQ(16) sta 30:46:9a:f9:fa:34 add key (len=16) ==> ws (0-
     192.168.35.1:5246) rId 0 wId 0
91155.226 <cc> STA_CFG_RESP(16) 30:46:9a:f9:fa:34 <== ws (0-192.168.35.1:5246) rc 0
     (Success)
91155.226 <eh> ***pairwise key handshake completed*** (RSN)
91155.257 <dc> DHCP Request server 0.0.0.0 <== host ADMINFO-FD4I2HK mac 30:46:9a:f9:fa:34 ip
     172.16.1.16
91155.258 <dc> DHCP Ack server 172.16.1.1 ==> host mac 30:46:9a:f9:fa:34 ip 172.16.1.16 mask
     255.255.255.0 gw 172.16.1.1
```

where:

- Orange represents the association phase.
- Blue represents the PSK exchange.
- Green represents the DHCP phase.

It is important to note the messages for a correct association phase, four-way handshake, and DHCP phase.

Checking the WiFi password

An Administrator can view plain text passwords (`captive-portal-radius-secret` and `passphrase`) under `config wireless-controller vap`.

Note that `security` must be set as a WPA-personal setting.

FortiAP connection issues

A communication problem can arise from the FortiAP.

Some examples include:

- The FortiAP is not connecting to the wireless controller.
- One FortiAP intermittently disconnects and re-connects.
- All FortiAPs intermittently disconnect and re-connect.

In the above cases:

- Check networking on the distribution system for all related FortiAPs.
- Check the authorization status of managed APs from the wireless controller.
- Restart the *cw_acd* process.
  Note: A restart of the *cw_acd* process drops all APs.
- For any wireless controller daemon crashes, check the controller crash log using the following command:
  ```
  diagnose debug crashlog read
  ```

Debugging FortiAP connection issues

For a quick assessment of the association communication between the controller and the FortiAP, run the following sniffer command to see if you can verify that the AP is communicating to the controller by identifying the CAPWAP communication:

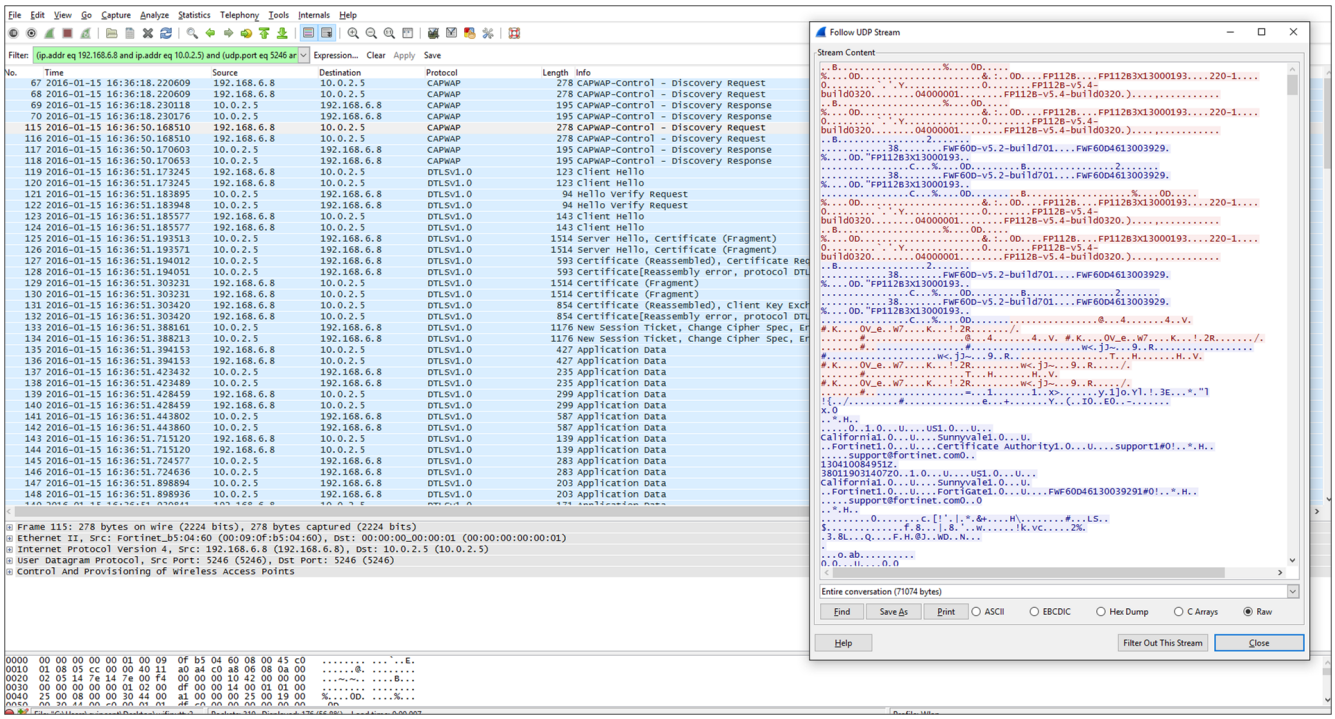
```
diagnose sniff packet <interface_name> "port 5246" 4
```

If you do not see this communication, then you can investigate the network or the settings on the AP to see why it is not reaching the controller.

To collect verbose output from the sniff that can be converted to a PCAP and viewed in Wireshark, use the following command:

```
diagnose sniff packet <interface_name> "port 5246" 6 0 1
```

The image below shows the beginning of the AP association to the controller. You can see the discovery Request and Response at the top.



Throughout debugging it is recommended to:

- Enable SSH login to the FortiAP device so that you can log in and issue local debugging commands:

```
config wireless-controller wtp
   edit "<FortiAP_serial_number>"
      set override-allowaccess {disable|enable}
      set allowaccess {https | ssh}
   end
```

- Try to connect to the wireless controller from the problematic FortiAP to verify routes exist.
- Enable wtp (FortiAP) debugging on the wireless controller for problematic FortiAPs to determine the point at which the FortiAP fails to connect:

```
diag wireless-controller wlac wtp_filter FP112B3X13000193 0-192.168.6.8:5246 2
```

(replace the serial number and IP address of the FortiAP)

```
di de console timestamp en
di de application cw_acd 0x7ff
di de en
```

Example of a successful AP and controller association:

Here is another example of a successful association between the FortiAP and the wireless controller. This example includes elements of the CAPWAP protocol; Request, Response, DTLS, Join, and Configuration (identified in color). All of these elements are bi-directional. So, if the DTLS response is slow, there could be a configuration error.

```
56704.575 <msg> DISCOVERY_REQ (12) <== ws (0-192.168.35.1:5246)
56704.575 <msg> DISCOVERY_RESP (12) ==> ws (0-192.168.35.1:5246)
56707.575 <msg> DISCOVERY_REQ (13) <== ws (0-192.168.35.1:5246)
56707.575 <msg> DISCOVERY_RESP (13) ==> ws (0-192.168.35.1:5246)
56709.577 <aev> - CWAE_INIT_COMPLETE ws (0-192.168.35.1:5246)
56709.577 <aev> - CWAE_LISTENER_THREAD_READY ws (0-192.168.35.1:5246)
56709.577 <fsm> old CWAS_START(0) ev CWAE_INIT_COMPLETE(0) new CWAS_IDLE(1)
```

```
56709.577 <fsm> old CWAS_IDLE(1) ev CWAE_LISTENER_THREAD_READY(1) new CWAS_DTLS_SETUP(4)
56709.623 <aev> - CWAE_DTLS_PEER_ID_RECV ws (0-192.168.35.1:5246)
56709.623 <aev> - CWAE_DTLS_AUTH_PASS ws (0-192.168.35.1:5246)
56709.623 <aev> - CWAE_DTLS_ESTABLISHED ws (0-192.168.35.1:5246)
56709.623 <fsm> old CWAS_DTLS_SETUP(4) ev CWAE_DTLS_PEER_ID_RECV(7) new CWAS_DTLS_AUTHORIZE
     (2)
56709.623 <fsm> old CWAS_DTLS_AUTHORIZE(2) ev CWAE_DTLS_AUTH_PASS(3) new CWAS_DTLS_CONN(5)
56709.623 <fsm> old CWAS_DTLS_CONN(5) ev CWAE_DTLS_ESTABLISHED(8) new CWAS_JOIN(7)
56709.625 <msg> JOIN_REQ (14) <== ws (0-192.168.35.1:5246)
56709.625 <aev> - CWAE_JOIN_REQ_RECV ws (0-192.168.35.1:5246)
56709.626 <fsm> old CWAS_JOIN(7) ev CWAE_JOIN_REQ_RECV(12) new CWAS_JOIN(7)
56709.629 <msg> CFG_STATUS (15) <== ws (0-192.168.35.1:5246)
56709.629 <aev> - CWAE_CFG_STATUS_REQ ws (0-192.168.35.1:5246)
56709.629 <fsm> old CWAS_JOIN(7) ev CWAE_CFG_STATUS_REQ(13) new CWAS_CONFIG(8)
56710.178 <msg> CHG_STATE_EVENT_REQ (16) <== ws (0-192.168.35.1:5246)
56710.178 <aev> - CWAE_CHG_STATE_EVENT_REQ_RECV ws (0-192.168.35.1:5246)
56710.178 <fsm> old CWAS_CONFIG(8) ev CWAE_CHG_STATE_EVENT_REQ_RECV(23) new CWAS_DATA_CHAN_
     SETUP(10)
56710.220 <aev> - CWAE_DATA_CHAN_CONNECTED ws (0-192.168.35.1:5246)
56710.220 <msg> DATA_CHAN_KEEP_ALIVE <== ws (0-192.168.35.1:5246)
56710.220 <aev> - CWAE_DATA_CHAN_KEEP_ALIVE_RECV ws (0-192.168.35.1:5246)
56710.220 <msg> DATA_CHAN_KEEP_ALIVE ==> ws (0-192.168.35.1:5246)
56710.220 <fsm> old CWAS_DATA_CHAN_SETUP(10) ev CWAE_DATA_CHAN_CONNECTED(32) new CWAS_DATA_
     CHECK(11)
56710.220 <aev> - CWAE_DATA_CHAN_VERIFIED ws (0-192.168.35.1:5246)
56710.220 <fsm> old CWAS_DATA_CHECK(11) ev CWAE_DATA_CHAN_KEEP_ALIVE_RECV(35) new CWAS_DATA_
     CHECK(11)
56710.220 <fsm> old CWAS_DATA_CHECK(11) ev CWAE_DATA_CHAN_VERIFIED(36) new CWAS_RUN(12)
56710.228 <msg> WTP_EVENT_REQ (17) <== ws (0-192.168.35.1:5246)
56710.228 <aev> - CWAE_WTP_EVENT_REQ_RECV ws (0-192.168.35.1:5246)
56710.228 <fsm> old CWAS_RUN(12) ev CWAE_WTP_EVENT_REQ_RECV(42) new CWAS_RUN(12)
56710.230 <msg> CFG_UPDATE_RESP (1) <== ws (0-192.168.35.1:5246) rc 0 (Success)
56710.230 <aev> - CWAE_CFG_UPDATE_RESP_RECV ws (0-192.168.35.1:5246)
56710.230 <msg> WTP_EVENT_REQ (18) <== ws (0-192.168.35.1:5246)
56710.230 <aev> - CWAE_WTP_EVENT_REQ_RECV ws (0-192.168.35.1:5246)
56710.230 <fsm> old CWAS_RUN(12) ev CWAE_CFG_UPDATE_RESP_RECV(37) new CWAS_RUN(12)
56710.230 <fsm> old CWAS_RUN(12) ev CWAE_WTP_EVENT_REQ_RECV(42) new CWAS_RUN(12)
56710.231 <msg> WTP_EVENT_REQ (19) <== ws (0-192.168.35.1:5246)
56710.231 <aev> - CWAE_WTP_EVENT_REQ_RECV ws (0-192.168.35.1:5246)
56710.231 <fsm> old CWAS_RUN(12) ev CWAE_WTP_EVENT_REQ_RECV(42) new CWAS_RUN(12)
56710.232 <msg> CFG_UPDATE_RESP (2) <== ws (0-192.168.35.1:5246) rc 0 (Success)
56710.232 <aev> - CWAE_CFG_UPDATE_RESP_RECV ws (0-192.168.35.1:5246)
56710.232 <fsm> old CWAS_RUN(12) ev CWAE_CFG_UPDATE_RESP_RECV(37) new CWAS_RUN(12)
56710.233 <msg> WTP_EVENT_REQ (20) <== ws (0-192.168.35.1:5246)
56710.233 <aev> - CWAE_WTP_EVENT_REQ_RECV ws (0-192.168.35.1:5246)
56710.233 <fsm> old CWAS_RUN(12) ev CWAE_WTP_EVENT_REQ_RECV(42) new CWAS_RUN(12)
56712.253 < . > AC (2) -> WTP (0-192.168.35.1:5246) State: CWAS_RUN (12) accept 3 live 3 dbg
     00000000 pkts 12493 0
56715.253 < . > AC (2) -> WTP (0-192.168.35.1:5246) State: CWAS_RUN (12) accept 3 live 6 dbg
     00000000 pkts 12493 0
56718.253 < . > AC (2) -> WTP (0-192.168.35.1:5246) State: CWAS_RUN (12) accept 3 live 9 dbg
     00000000 pkts 12493 0
56719.253 <aev> - CWAE_AC_ECHO_INTV_TMR_EXPIRE ws (0-192.168.35.1:5246)
56719.253 <fsm> old CWAS_RUN(12) ev CWAE_AC_ECHO_INTV_TMR_EXPIRE(39) new CWAS_RUN(12)
56719.576 <msg> ECHO_REQ (21) <== ws (0-192.168.35.1:5246)
56719.576 <aev> - CWAE_ECHO_REQ_RECV ws (0-192.168.35.1:5246)
56719.577 <fsm> old CWAS_RUN(12) ev CWAE_ECHO_REQ_RECV(27) new CWAS_RUN(12)
```

where:

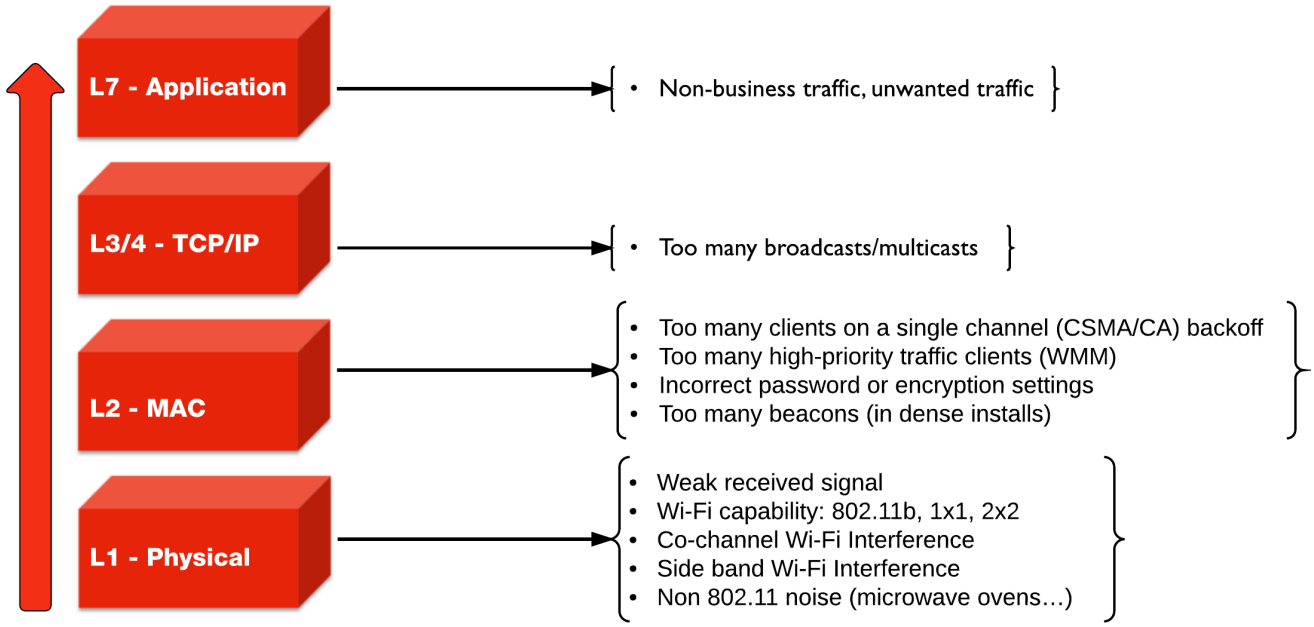
- **Orange** represents the Discovery phase.
- **Blue** indicates that the control channels have been established using DTLS.
- **Green** represents the access point Discovery and Join phase.
- **Purple** represents the Clear Text channel.
- **Pink** indicates that the FortiAP is successfully connected to the wireless controller.

Best practices for OSI common sources of wireless issues

Not all WiFi problems are related to signal strength, interference, or misconfiguration. The following Open System Interconnection (OSI) model identifies some of the more common issues per layer.

Best practices for troubleshooting vary depending on the affected layer. See the following illustration.

Common sources of wireless issues



Best practices for Layer 1

Common physical layer issues include:

- weak received signal
- WiFi capability: 802.11b, 1x1, 2x2
- co-channel WiFi interference

- side band WiFi interference
- non 802.11 noise (such as microwave ovens)

To avoid physical layer issues:

- Determine the RST (Receiver Sensitivity Threshold) for your device, or use -70 dBm as a rule of thumb.
- Match the AP TX output power to the client TX output power.
- Use DFS (Dynamic Frequency Selection) for high performance data 20/40 MHz.
- Use 5 GHz UNII-1 & 3 (Non-DFS) bands with static channel assignment for latency-sensitive applications.
- Do not use 40 MHz channels in 2.4 GHz band. (FortiOS does not allow channel bonding.)

Best practices for Layer 2

Common data link (MAC) layer issues include:

- too many clients on a single channel (CSMA/CA) backoff
- too many high-priority traffic clients (WMM)
- incorrect password or encryption settings
- too many beacons (in high-density installations)

To avoid data link layer issues:

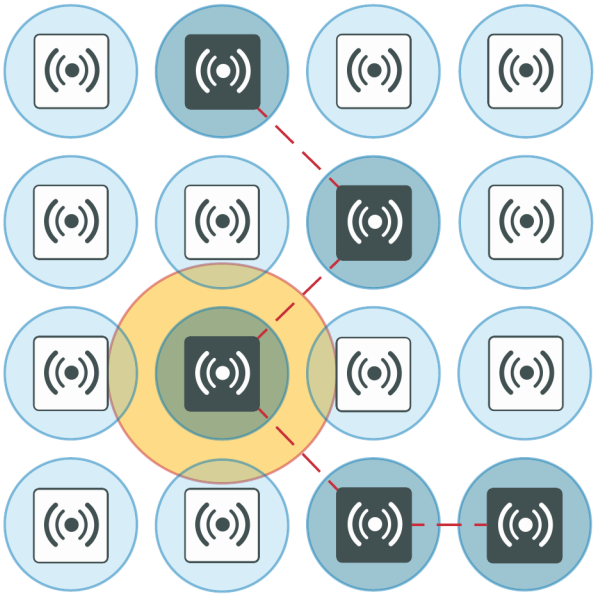
- Only use CCMP/AES (WPA2) encryption (not TKIP).
- In high-density deployments, turn off SSID broadcast or turn down SSID rates. Review and possibly reduce the beacon interval.
- Determine the best cell size for applications:
  - For few users and low bandwidth latency sensitive applications, use high-transmit power to create larger cells.
  - For high-performance and high-capacity installations, use lower transmit power to create smaller cells (set FortiPlanner at 10 dBm TX power), but bear in mind that this setting requires more roaming.

Cells and co-channel interference

In high-density deployments, multiple APs are used, and each one services an area called a cell. However, these cells can cause interference with each other. This is a common problem. The radio signal from one AP interferes with, or cancels out, the radio signal from another AP.

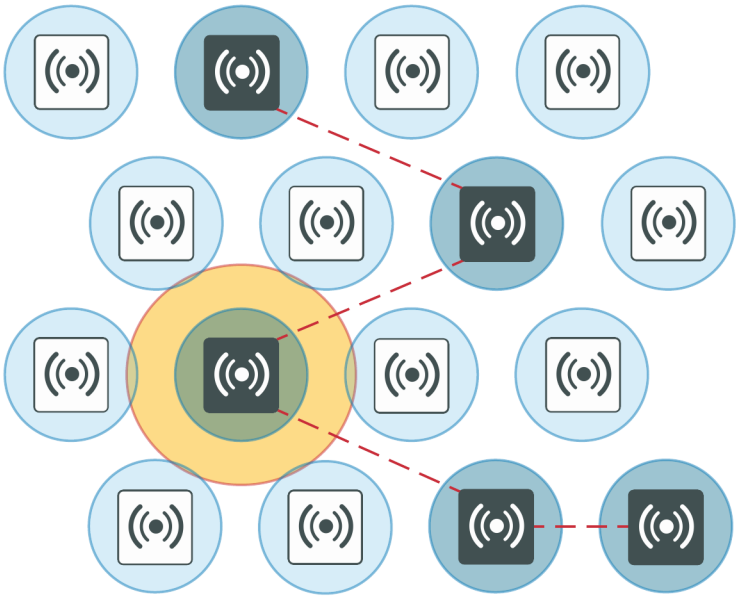
In the following diagram, note the interference zone created by one radio, causing interference on its neighboring APs.

The interference zone can be twice the radius of the signal, and the signal at its edge can be -67 dBm.



Reducing co-channel interference

For best results, use a honeycomb pattern as a deployment strategy. The idea is to *stagger* repeated channels furthest from each other to avoid interference.



Best practices for Layer 3 and above

For TCP/IP layers and above, a common source of latency, or slowness in the wireless traffic, is too many broadcasts or multicasts. These types of issues can result from non-business or unwanted traffic, or both.

To resolve issues at the TCP/IP layer and above, you can:

- identify business-critical applications
- use Application Control, Web Filtering, Traffic Shaping, and QoS to prioritize applications
  - Identify unwanted traffic, high-bandwidth web-related traffic, and use Security Profiles.
  - Use the traffic shaping on a policy to rate-limit this traffic.

  You perform these configurations directly on the FortiGate.

Packet sniffer

Capturing the traffic between the controller and the FortiAP can help you identify most FortiAP and client connection issues.

CAPWAP packet sniffer

The first recommended technique consists of sniffing the CAPWAP traffic.

- Enable plain control on the controller and on the FortiAP to capture clear control traffic on UDP port 5246.
  - On the controller:
    ```
    diagnose wireless-controller wlac plain-ctl <FortiAP_serial_number> 1
    Result:
    WTP 0-FortiAP2223X11000107 Plain Control: enabled
    ```
  - On the FortiAP:
    ```
    cw_diag plain-ctl 1
    Result:
    Current Plain Control: enabled
    ```

Note that some issues are related to the keep-alive for control and data channel.

Data traffic on UDP port 5247 is not encrypted. The data itself is encrypted by the wireless security mechanism.

Data traffic is helpful to troubleshoot most of the issues related to station association, EAP authentication, WPA key exchange, roaming, and FortiAP configuration.

You can also set up a host or server to which you can forward the CAPWAP traffic:

1. Configure the host or server to which CAPWAP traffic is forwarded:
   ```
   diagnose wireless-controller wlac sniff-cfg <Host_IP_address> 88888
   ```
   Result:

   Current Sniff Server: 192.168.25.41, 23352
2. Choose which traffic to capture, the interface to which the FortiAP is connected, and the FortiAP serial number:
   ```
   diagnose wireless-controller wlac sniff <interface_name> <FortiAP_serial_number> 2
   ```
   Result:

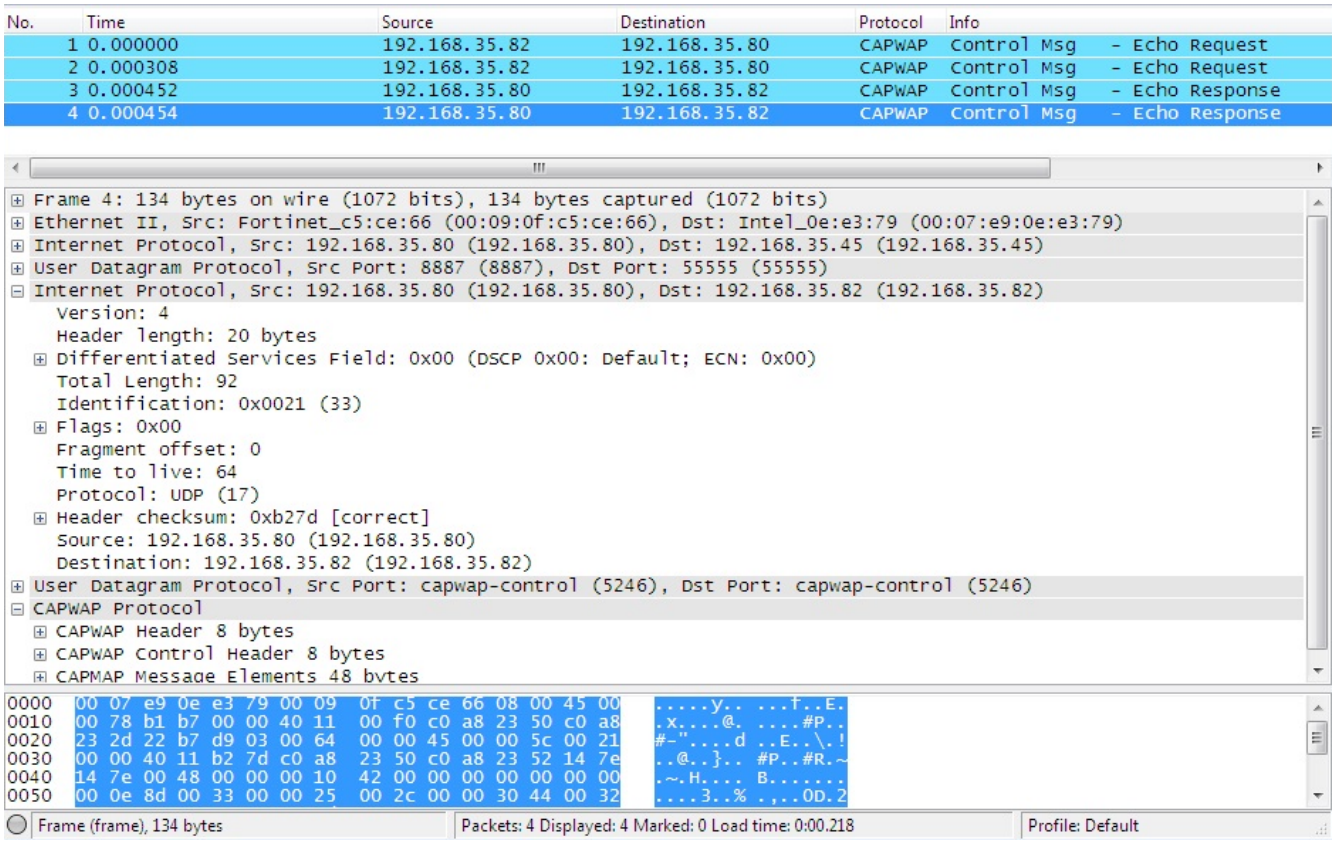
   WTP 0-FortiAP2223X11000107 Sniff: intf port2 enabled (control and data message)

   In the above syntax, the '`2`' captures the control and data message. The '`1`' would capture only the control message and '`0`' would disable it.
3. Run Wireshark on the host or server to capture CAPWAP traffic from the controller.
4. Decode the traffic as IP to check inner CAPWAP traffic.

Example CAPWAP packet capture

The following image shows an example of a CAPWAP packet capture, where you can see the following details:

- Layer 2 header
- sniffed traffic encapsulated into Internet Protocol for transport
- CAPWAP encapsulated into UDP for sniffer purpose and encapsulated into IP
- CAPWAP control traffic on UDP port 5246
- CAPWAP payload



Wireless traffic packet sniffer

The second recommended technique consists of sniffing the wireless traffic directly on the air using your FortiAP.

Wireless traffic packet capture

Packet captures are useful for troubleshooting all wireless client related issues because you can verify data rate and 802.11 parameters, such as radio capabilities, and determine issues with wireless signal strength, interference, or congestion on the network.

A radio can only capture one frequency at a time; one of the radios is set to sniffer mode depending on the traffic or channel required. You must use two FortiAPs to capture both frequencies at the same time.

- Set a radio on the FortiAP to monitor mode.
  ```
  iwconfig wlan10
  ```

  Result:
  ```
  wlan10 IEEE 802.11na    ESSID:""
  Mode:Monitor Frequency:5.18 GHz Access Point: Not-Associated
  ```

- The capture file is stored under the temp directory as *wl_sniff.pcap*
  /tmp/wl_sniff.cap

  The capture file is only stored temporarily. If you want to save it, upload it to a TFTP server before rebooting or changing the radio settings.

  - The command `cp wl_sniff.cap newname.pcap` allows you to rename the file.
  - To send the pcap file to a remote TFTP server, use the following commands depending on your AP model:
    - For FAP-U:
      ```
      tftp -l /tmp/wl_sniff.cap -r wl_sniff_remote.cap -p 192.168.50.100
      ```
    - For Standard FAP W1:
      ```
      ftftp -l /tmp/wl_sniff.cap -r wl_sniff_remote.cap -p 192.168.50.100
      ```
    - For Standard FAP W2:
      ```
      ftftp 192.168.50.100 -m binary -c put /tmp/wl_sniff.cap wl_sniff_remote.cap
      ```

    Where 192.168.50.100 is the IP address of the tftp server.

Syntax

The following syntax demonstrates how to set the radio to sniffer mode (configurable from the CLI only). Sniffer mode provides options to filter for specific traffic to capture. Notice that you can determine the buffer size, which channel to sniff, the AP MAC address, and select if you want to sniff the beacons, probes, controls, and data channels.

```
configure wireless-controller wtp-profile
   edit <profile_name>
      configure <radio>
         set mode sniffer
         set ap-sniffer-bufsize 32
         set ap-sniffer-chan 1
         set ap-sniffer-addr 00:00:00:00:00:00
         set ap-sniffer-mgmt-beacon enable
         set ap-sniffer-mgmt-probe enable
         set ap-sniffer-mgmt-other enable
         set ap-sniffer-ctl enable
         set ap-sniffer-data enable
      end
end
```

Once you have performed the previous CLI configuration, you can see the packet sniffer mode selected in the GUI dashboard under **WiFi & Switch Controller > FortiAP Profiles** and **WiFi & Switch Controller > Managed FortiAPs**. Bear in mind that if you change the mode from the GUI, you need to return to the CLI to re-enable the sniffer mode.

To disable the sniffer profile in the CLI, use the following commands:

```
config wireless-controller wtp-profile
   edit <profile_name>
```

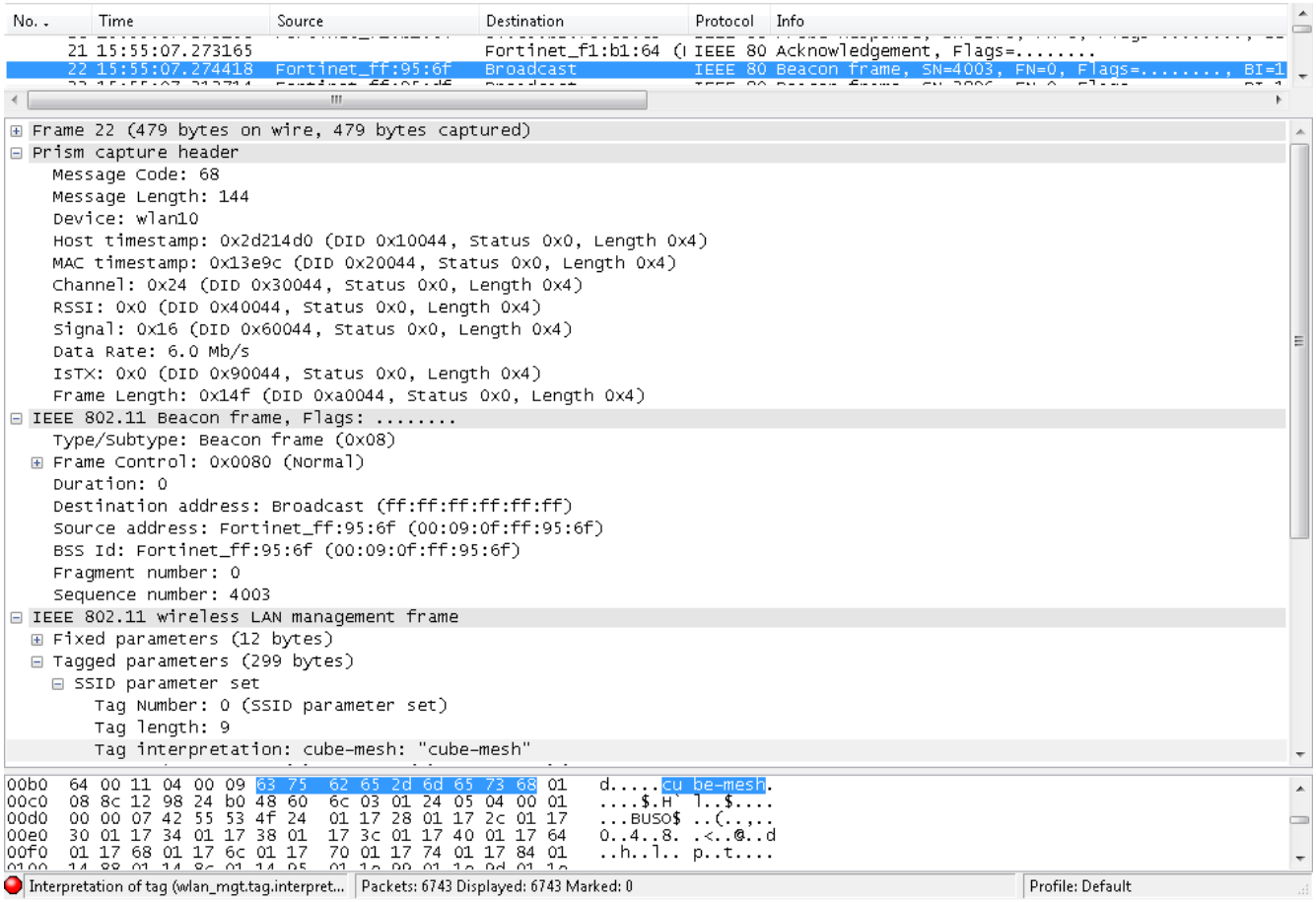
```
      config <radio>
         set ap-sniffer-mgmt-beacon disable
         set ap-sniffer-mgmt-probe disable
         set ap-sniffer-mgmt-other disable
         set ap-sniffer-ctl disable
         set ap-sniffer-data disable
      end
end
```

If you change the radio mode before sending the file *wl_sniff.cap* to an external TFTP, the file is deleted and you lose your packet capture.

Example AP packet capture

The following image shows an example of the AP packet capture with the following details:

- capture header showing channel 36
- beacon frame
- source, destination, and BSSID of the beacon frame
- SSID of the beacon frame



Debug commands

For a list of debug options available for the wireless controller, use the following command on the controller:

```
diagnose wireless-controller wlac help
```

Sample outputs

Syntax

```
diagnose wireless-controller wlac -c vap
```

(This command lists the information about the virtual access point, including its MAC address, the BSSID, its SSID, the interface name, and the IP address of the APs that are broadcasting it.)

Result:

```
bssid             ssid   intf     vfid:ip-port rId wId
00:09:0f:d6:cb:12 Office Office   ws (0-192.168.3.33:5246) 0 0
00:09:0f:e6:6b:12 Office Office   ws (0-192.168.1.61:5246) 0 0
06:0e:8e:27:dc:48 Office Office   ws (0-192.168.3.36:5246) 0 0
0a:09:0f:d6:cb:12 public publicAP ws (0-192.168.3.33:5246) 0 1
```

Syntax

```
diagnose wireless-controller wlac -c darrp
```

(This command lists the information pertaining to the radio resource provisioning statistics, including the AP serial number, the number of channels set to choose from, and the operation channel. Note that the 5 GHz band is not available on these APs listed.)

Result:

```
wtp_id           rId  base_mac          index nr_chan vfid 5G oper_chan age
FAP22A3U10600400 0    00:09:0f:d6:cb:12 0     3       0    No 1         87588
FW80CM3910601176 0    06:0e:8e:27:dc:48 1     3       0    No 6         822
```

Extension information support

You can enable or disable extension information at `wtp-profile`, and use the diagnose option below to print out the detail of extension information.

Syntax

```
config wireless-controller wtp-profile
   edit test
      set lldp [enable | disable]
      set ext-info-enable
      [enable | disable] --> Enable or disable station, VAP, and radio extension
           information.
   end
end

diagnose wireless-controller wlac -d [wtp | vap | sta]
```

where:

- `wlac -d wtp [SN|name] [reset]` --> List or reset wtp info (data).
- `wlac -d vap [bssid] [reset]` --> List or reset vap info (data). .
- `wlac -d sta [mac] [reset]` --> list or reset sta info (data).

FortiAP CLI configuration and diagnostics commands

The FortiAP CLI controls radio and network operations through the use of variables manipulated with the configuration and diagnostics commands.

For details about accessing the FortiAP CLI, see FortiAP CLI access on page 49.

Configuration commands

Command	Description
`cfg -s`	List variables for most popular settings and also the ones that are not using default values.
`cfg -a var=value`	Add or change a variable value.
`cfg -c`	Commit the change to flash.
`cfg -x`	Reset settings to factory defaults.
`cfg -r var`	Remove variable.
`cfg -e`	Export variables.
`cfg -h`	Display help for all configuration commands and a complete list of configuration variables.

Configuration variables

Variable	Description and value
`AC_CTL_PORT`	WiFi Controller control (CAPWAP) port. Default: 5246.
`AC_DATA_CHAN_SEC`	Data channel security. 0 - Clear text 1 - DTLS (encrypted) 2 - Accept either DTLS or clear text (default)
`AC_DISCOVERY_TYPE`	0 - Auto - Cycle through all of the discovery types until successful. 1 - Static. Specify WiFi Controllers 2 - DHCP 3 - DNS 5 - Broadcast 6 - Multicast 7- FortiCloud

Variable	Description and value
AC_HOSTNAME_1 AC_HOSTNAME_2 AC_HOSTNAME_3	WiFi Controller host names for static discovery.
AC_IPADDR_1 AC_IPADDR_2 AC_IPADDR_3	WiFi Controller IP addresses for static discovery.
AC_DISCOVERY_DHCP_OPTION_CODE	Option code for DHCP server. Default: 138.
AC_DISCOVERY_MC_ADDR	Multicast address for controller discovery. Default: 224.0.1.140.
ADDR_MODE	How the FortiAP unit obtains its IP address and netmask. DHCP - FortiGate interface assigns address. STATIC - Specify in AP_IPADDR and AP_NETMASK. Default: DHCP.
ADMIN_TIMEOUT	Administrative timeout in minutes. Applies to GUI sessions. Default: 5 minutes.
AP_IPADDR AP_NETMASK IPGW	These variables set the FortiAP unit IP address, netmask and default gateway when ADDR_MODE is STATIC. Default for AP_IPADDR: 192.168.1.2 . Default for AP_NETMASK: 255.255.255.0. Default for IPGW: 192.168.1.1.
ALLOW_HTTPS	0 - https disable 1 - https enable 2 - controlled by AC Default: 2.
ALLOW_SSH	0 - SSH disable 1 - SSH enable 2 - controlled by AC Default: 2.
AP_MGMT_VLAN_ID	Non-zero value applies VLAN ID for unit management. See Reserved VLAN IDs on page 15. Default: 0.
AP_MODE	FortiAP operating mode. 0 - Thin AP 2 - Unmanaged Site Survey mode. See SURVEY variables. Default: 0.
BAUD_RATE	Console data rate: 9600, 19200, 38400, 57600, or 115200 baud.

Variable	Description and value
	Default: 9600.
DNS_SERVER	DNS Server for clients. If ADDR_MODE is DHCP the DNS server is automatically assigned.
FAP_ETHER_TRUNK	Configure port behavior on FortiAP-U models. 0 - Dummy Switch. Default mode. 1 - Ether Hardware Bonding. Support Static Ethernet Channel Bonding on LAN1 and LAN2 ports. Only available on select FortiAP-U models. 2 - Ether 802.3ad Bonding. Support IEEE 802.3ad Link Aggregation Control Protocol (LACP) on LAN1 and LAN2 ports. 3 - Enable WAN-LAN. Supports configuration of a second WAN port as a LAN (WAN-LAN mode configuration).
FIRMWARE_UPGRADE	Default: 0.
LED_STATE	Enable/disable status LEDs. 0 - LEDs enabled 1 - LEDs disabled 2 - follow AC setting
LOGIN_PASSWD	Administrator login password. By default this is empty.
STP_MODE	Spanning Tree Protocol. 0 - off 1 - on
WANLAN_MODE	Configure port behavior on FortiAP, FortiAP-S, and FortiAP-W2 models. WAN-ONLY - Default mode WAN-LAN - Bridges the LAN port to the incoming WAN interface AGGREGATE - Enables link aggregation
WTP_LOCATION	Optional string describing AP location.
Mesh variables	
MESH_AP_BGSCAN	Enable or disable background mesh root AP scan. 0 - Disabled 1 - Enabled
MESH_AP_BGSCAN_RSSI	If the signal of the root AP is weak, and lower than the received signal strength indicator (RSSI) threshold, the WiFi driver immediately starts a new round scan and ignores the configured MESH_AP_BGSCAN_PERIOD delays. Set the value between 0 and 127. After the new round scan is finished, a scan done event is passed to wtp daemon to trigger roaming.

Variable	Description and value
MESH_AP_BGSCAN_PERIOD	Time in seconds that a delay period occurs between scans. Set the value between 1 and 3600.
MESH_AP_BGSCAN_IDLE	Time in milliseconds. Set the value between 0 and 1000.
MESH_AP_BGSCAN_INTV	Time in milliseconds between channel scans. Set the value between 200 and 16000.
MESH_AP_BGSCAN_DUR	Time in milliseconds that the radio will continue scanning the channel. Set the value between 10 and 200.
MESH_AP_SCANCHANLIST	Specify those channels to be scanned.
MESH_AP_TYPE	Type of communication for backhaul to controller: 0 - Ethernet 1 - WiFi mesh 2 - Ethernet with mesh backup support Default: 0.
MESH_AP_SSID	SSID for mesh backhaul. Default: fortinet.mesh.root.
MESH_AP_BSSID	WiFi MAC address.
MESH_AP_PASSWD	Pre-shared key for mesh backhaul.
MESH_ETH_BRIDGE	1 - Bridge mesh WiFi SSID to FortiAP Ethernet port. This can be used for point-to-point bridge configuration. This is available only when MESH_AP_TYPE =1. 0 - No WiFi-Ethernet bridge Default: 0.
MESH_MAX_HOPS	Maximum number of times packets can be passed from node to node on the mesh. Default: 4.
The following factors are summed and the FortiAP associates with the lowest scoring mesh AP.	
MESH_SCORE_HOP_WEIGHT	Multiplier for number of mesh hops from root. Default: 50.
MESH_SCORE_CHAN_WEIGHT	AP total RSSI multiplier. Default: 1.
MESH_SCORE_RATE_WEIGHT	Beacon data rate multiplier. Default: 1.
MESH_SCORE_BAND_WEIGHT	Band weight (0 for 2.4 GHz, 1 for 5 GHz) multiplier. Default: 100.
MESH_SCORE_RSSI_WEIGHT	AP channel RSSI multiplier. Default: 100.
Survey variables	
SURVEY_SSID	SSID to broadcast in site survey mode (AP_MODE=2).
SURVEY_TX_POWER	Transmitter power in site survey mode (AP_MODE=2).

Variable	Description and value
SURVEY_CH_24	Site survey transmit channel for the 2.4 GHz band. Default: 6.
SURVEY_CH_50	Site survey transmit channel for the 5 GHz band. Default: 36.
SURVEY_BEACON_INTV	Site survey beacon interval. Default: 100 ms.

Diagnostics commands

Command	Description
cw_diag admin-timeout [30]	Set the shell idle timeout in minutes.
cw_diag baudrate [9600 | 19200 | 38400 | 57600 | 115200]	Set the console baud rate.
cw_diag help	Display help for all diagnostics commands.
cw_diag plain-ctl [0|1]	Show or change the current plain control setting.
cw_diag sniff [0|1|2]	Enable or disable the sniff packet.
cw_diag sniff-cfg ip port	Set the sniff server IP and port.
cw_diag stats wl_intf	Show the wl_intf status.
cw_diag uptime	Show daemon uptime.
cw_diag -c ap-scan	Show scanned APs.
cw_diag -c ap-suppress	Show suppressed APs.
cw_diag -c arp-req	Show scanned arp requests.
cw_diag -c atf	Show Air Time Fairness information at the FortiAP level.
cw_diag -c ble-scan	Show scanned Bluetooth Low Energy (BLE) devices that are reported to FortiPresence.
cw_diag -c darrp	Show the DARRP radio channel.
cw_diag -c fortipresence	Show FortiPresence statistics including reported BLE devices.
cw_diag -c k-qos wlan00	Verify that the vmn-dscp-marking values are pushed to FortiAP.
cw_diag -c mesh	Show the mesh status.
cw_diag -c mesh-ap	Show the mesh ap candidates.
cw_diag -c mesh-veth-acinfo	Show the mesh veth ac info, and mesh ether type.
cw_diag -c mesh-veth-host	Show the mesh veth host.
cw_diag -c mesh-veth-vap	Show the mesh veth vap.
cw_diag -c radio-cfg	Show the current radio config parameters in the control plane.
cw_diag -c scan-clr-all	Flush all scanned AP/STA/ARPs.

Command	Description
`cw_diag -c snmp`	Show configuration details for SNMP support.
`cw_diag -c sta-cap`	Show scanned STA capabilities.
`cw_diag -c sta-deauth`	De-authenticate an STA.
`cw_diag -c sta-scan`	Show scanned STAs.
`cw_diag -c vap-cfg`	Show the current VAPs in the control plane.
`cw_diag -c vlan-probe-cmd action (0:start 1:stop 2:clear) intf [start-vlan end-vlan retries timeout]`	Start the VLAN probe. Example command: cw_diag -c vlan-probe-cmd 0 eth0 2 300 3 10 Example output: VLAN probing: start intf [eth0] vlan range[2,300] retries[3] timeout[10] ...
`cw_diag -c vlan-probe-rpt`	Show the VLAN probe report.
`cw_diag -c wids`	Show scanned WIDS detections.
`cw_diag -c wtp-cfg`	Show the current wtp config parameters in the control plane.
`cw_diag --clog <on|off>`	Turn on or off console log message.

FortiAP REST API

FortiAP-S and FortiAP-W2 version 6.2.0 and later support REST API calls.

You can access the host at https://<FAP-IP> where <FAP-IP> is the IP address of the FortiAP.

The following REST API calls are supported:

REST API call	HTTP	Path	Description
cfg-get	GET	/api/v1/cfg-get	List effective FortiAP variables. To filter for specific parameters: /api/v1/cfg-get?names=parameter-name Examples: • Get WTP_NAME: /api/v1/cfg-get?names=WTP_NAME • Get WTP_NAME and ADMIN_TIMEOUT: /api/v1/cfg-get?names=WTP_NAME,ADMIN_TIMEOUT
cfg-meta-get	GET	/api/v1/cfg-meta-get	List all variables.
cfg-set	POST	/api/v1/cfg-set	Add or change variables.
logincheck	POST	/logincheck	Log in to FortiAP with/without a password.
logout	POST	/logout	Log out from FortiAP.
radio-cfg	GET	/api/v1/radio-cfg	Get current radios configuration parameters of the control plane. To specific radio configuration parameters of the control plane: • rcfg info from radio 0: /api/v1/radio-cfg?rId=0 • rcfg info from radio 1: /api/v1/radio-cfg?rId=1
reboot	POST	/api/v1/reboot	Reboot FortiAP.
sys-perf	GET	/api/v1/sys-perf	Get system performance values (CPU, memory).
sys-status	GET	/api/v1/sys-status	Get system status (`fap-get-status`).
vap-cfg	GET	/api/v1/vap-cfg	Get current SSIDs of the control plane. To get the current SSIDs for each independent radios: • vcfg info from radio 0: /api/v1/vap-cfg?rId=0 • vcfg info from radio-1: /api/v1/vap-cfg?rId=1 To get specific SSIDs from specific radios: • wlan 0 vcfg info from radio 0: /api/v1/vap-cfg?rId=0&wId=0 • wlan 1 vcfg info from radio 0: /api/v1/vap-cfg?rId=0&wId=1
wtp-cfg	GET	/api/v1/wtp-cfg	Get current FortiAP configuration parameters of the control plane.

Example request

```
https://<FAP-IP>/api/v1/sys-perf
```

Example response

```
{
 "cpu_usage": 1,
 "memory_usage": 60
}
```