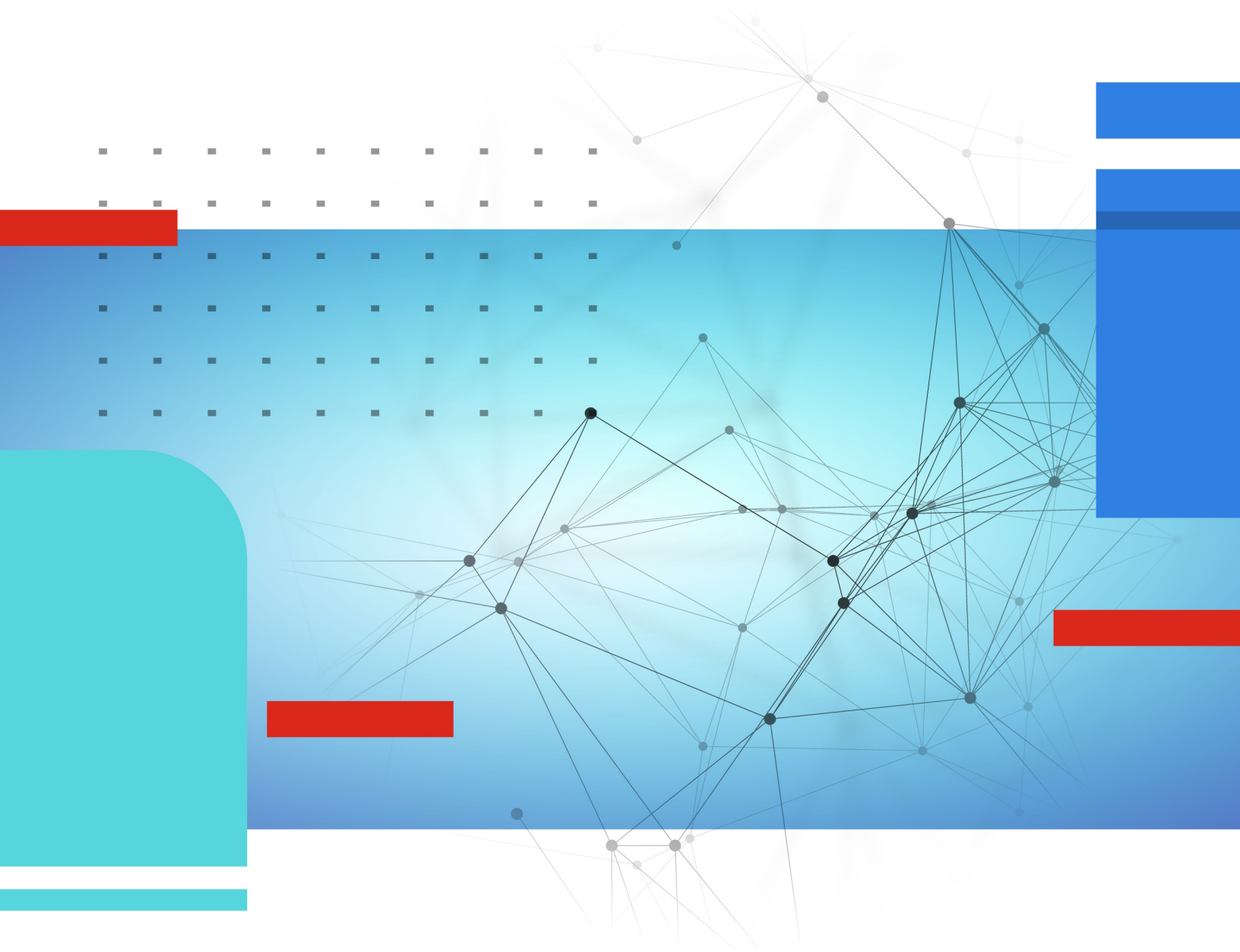
Configuration Guide

FortiWiFi and FortiAP 7.6.0



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

FORTINET VIDEO LIBRARY
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/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

Sep 12, 2024
FortiWiFi and FortiAP 7.6.0 Configuration Guide
01-760-1054323-20240912

TABLE OF CONTENTS

Change log **11**
What's new in this release **12**
Introduction **13**
Wireless network equipment 13
FortiAP units 13
FortiGate units 13
FortiWiFi units 14
Wireless management topologies 14
Integrated wireless management 14
Cloud AP management 14
Dedicated wireless controller 15
Related products for wireless networks 15
FortiManager 15
FortiAnalyzer 15
Getting started with FortiAP management **17**
Configuring the FortiGate interface to manage FortiAP units 17
Discovering, authorizing, and deauthorizing FortiAP units 18
Discovering a FortiAP unit 18
AC actions when a FortiAP attempts to get discovered 19
Authorize a discovered FortiAP 20
De-authorize a managed FortiAP 22
FortiAP diagnostics and tools 23
Setting up a mesh connection between FortiAP units 25
Data channel security: clear-text, DTLS, and IPsec VPN 30
Wireless network configuration **32**
SSIDs on FortiWiFi units 33
Reserved VLAN IDs 33
Wireless network configuration tasks 34
Setting your geographic location 35
Configuring the network interface for the AP unit 35
Understanding FortiWiFi aplink interface 37
Creating a FortiAP profile 38
Defining a wireless network interface (SSID) 43
Configuring DHCP for WiFi clients 46
Configuring DNS for local standalone NAT VAPs 47
Changing SSID to VDOM only 47
Airtime fairness 49
Configuring security 52
WPA2 Security 52
WPA3 Security 59
MPSK profiles 66
Captive Portal Security 72
Adding a MAC filter 89

Limiting the number of clients 91
Enabling multicast enhancement 92
Replacing WiFi certificate 93
Configuring WiFi with WSSO using Windows NPS and user groups 95
Enabling Beacon Protection 101
Defining SSID groups 104
Configuring dynamic user VLAN assignment 104
VLAN assignment by RADIUS 104
VLAN assignment by Name Tag 106
VLAN assignment by FortiAP group 109
VLAN assignment by VLAN pool 110
Configuring wireless NAC support 112
Example 112
Configuring user authentication 117
WPA2 and WPA3 Enterprise authentication 117
WiFi single sign-on (WSSO) authentication 122
Assigning WiFi users to VLANs dynamically 122
MAC-based authentication 123
User self-registration of MPSKs through FortiGuest 128
Authenticating guest WiFi users 130
Configuring 802.1X supplicant on LAN 130
Configure NAS-Filter-Rule attribute to set up dACL 135
Configuring firewall policies for the SSID 136
Configuring the built-in access point on a FortiWiFi unit 137
Enforcing UTM policies on a local bridge SSID 138
Configuring a Syslog profile 139
Understanding Distributed Radio Resource Provisioning 141
Channel Planning 142
Channel Quality Monitoring 142
Configuring Distributed Radio Resource Provisioning 143
Translating WiFi QoS WMM marking to DSCP values 146
Configuring Layer 3 roaming 149
Configuring L3 Roaming for Tunnel Mode SSIDs 152
Configuring L3 Roaming for Bridge Mode SSIDs 157
Advanced Wireless Features 165
Operations Profiles Entry 166
Connectivity Profiles Entry 171
Protection Profiles Entry 178
Advanced SSID options 180
Advanced WiFi Settings options 182
Configuring UNII-4 5GHz radio bands 185
Configuring Agile Multiband Operation 187
Access point configuration 192
Network topology of managed APs 193
Discovery and authorization of APs 195
Pre-authorizing a FortiAP unit 195
Enabling and configuring a discovered AP 198

Disabling the automatic discovery of unknown FortiAPs ... 199
Enabling the automatic authorization of extension devices ... 199
Assigning the same FortiAP profile to multiple FortiAP units ... 199
Overriding the FortiAP profile ... 200
Register a FortiAP to FortiCloud ... 200
FortiAP CLI access ... 201
Accessing the FortiAP CLI through the FortiAP Ethernet port ... 201
Accessing the FortiAP CLI through the FortiGate ... 202
FortiAP Configuration mode ... 202
Resetting FortiAP to enter the Configuration mode ... 203
Accessing the GUI of the FortiAP Configuration mode ... 203
Accessing the CLI of the FortiAP Configuration mode ... 205
FortiAP unit firmware upgrade ... 206
Checking the FortiAP unit firmware version ... 206
Enabling automatic FortiAP upgrade after authorization ... 206
Enabling automatic firmware updates ... 207
Upgrading FortiAP firmware from the FortiGate unit ... 207
Upgrading FortiAP firmware from the FortiAP unit ... 208
Enabling Hitless Rolling AP upgrade ... 208
Advanced WiFi controller discovery ... 212
Controller discovery methods ... 213
Configure automatic AP reboot ... 215
Wireless client load balancing for high-density deployments ... 218
Access point handoff ... 218
Frequency handoff or band-steering ... 218
Handoff configuration ... 218
FortiAP groups ... 219
LAN port options ... 220
Configuring a port to WAN-LAN operation mode ... 221
Bridging a LAN port with the WAN port ... 221
Bridging a LAN port with an SSID ... 222
Configuring FortiAP LAN ports ... 223
Verifying wired clients connected to FortiAP LAN ports ... 225
MAC Authentication for LAN port hosts ... 225
LAN port aggregation and redundancy ... 227
Enabling LACP ... 228
LAN port uplink redundancy without LACP ... 228
CAPWAP ... 229
IP fragmentation of packets in CAPWAP tunnels ... 230
CAPWAP bandwidth formula ... 231
CAPWAP Offloading ... 232
Improve CAPWAP stability over NAT ... 234
LED options ... 235
Configure FortiAP MIMO values ... 236
Configure Fortinet external antenna parameters for specific FortiAPs ... 237
Configure third-party antennas in select FortiAP models ... 239
Configure FortiAP USB port status ... 241

Wireless mesh configuration ... **243**
Wireless mesh deployment modes ... 244
Firmware requirements ... 244
Types of wireless mesh ... 244
Fast-roaming for mesh backhaul link ... 246
Configuring a meshed WiFi network ... 246
Creating the mesh root SSID ... 246
Creating the FortiAP profile ... 247
Configuring the mesh root AP ... 247
Configuring the mesh leaf FortiAPs ... 248
Authorizing leaf APs ... 249
Creating security policies ... 249
Viewing the status of the mesh network ... 250
Configuring a point-to-point bridge ... 250
Hotspot 2.0 ANQP configuration ... **251**
Configure hotspot profile ... 251
Configure 3GPP public land mobile network (PLMN) ... 253
Configure IP address type availability ... 253
Configure network access identifier (NAI) realm ... 253
Configure network authentication type ... 254
Configure roaming consortium ... 254
Configure venue name duple ... 254
Configure venue URL ... 255
Configure advice of charge (AOC) ... 255
Configure connection capability ... 256
Configure operator friendly name ... 256
Configure online sign up (OSU) provider Network Access Identifier (NAI) list ... 256
Configure online sign up (OSU) provider list ... 257
Configure terms and conditions ... 257
Configure WAN metrics ... 258
Configure Online Sign Up (OSU) provider icon ... 258
Configure Quality of Service (QoS) map set ... 258
Configuring OpenRoaming on FortiAP ... 259
Wireless network with wired LAN configuration ... **262**
How to combine a wireless network and wired LAN with a software switch ... 262
VLAN configuration ... 264
Additional configuration ... 264
How to configure a FortiAP local bridge (private cloud-managed AP) ... 264
Continued FortiAP operation when WiFi controller connection is down ... 266
How to increase the number of supported FortiAPs ... 267
How to implement multi-processing for large-scale FortiAP management ... 268
Configuring multiple cw_acd processes ... 269
Configuring multiple wpad_ac processes ... 271
Remote WLAN FortiAPs ... **274**
Configuring the FortiGate for remote FortiAPs ... 274

Enable split tunneling options ... 274
Apply split tunneling ... 274
Configure split tunneling behavior ... 275
Enable split tunneling on SSIDs ... 276
Configure a FortiAP unit to connect to FortiGate ... 276
Preauthorize a FortiAP unit for automatic authorization ... 278
Features for high-density deployments ... 279
Upgrading the firmware for multiple FortiAPs ... 279
Controlling the power save feature ... 279
11n radio powersave optimization ... 280
Configuring the broadcast packet suppression ... 280
Converting multicast streams to unicast ... 281
Ignoring weak or distant clients ... 282
Turning off the 802.11b protocol ... 282
Configuring data rates ... 282
Enabling the automatic TX power control ... 284
Enabling the frequency band load-balancing ... 284
Setting the handoff RSSI threshold ... 285
Enabling the AP load balancing ... 285
Setting the AP load balance threshold ... 285
Setting the Application Control feature ... 286
Managing the FortiAP group and assigning a dynamic VLAN ... 286
Sharing tunnel SSIDs within a single managed FortiAP ... 287
Enabling the manual quarantine of devices on FortiAP (tunnel mode) ... 287
Locating a FortiAP with LED blinking ... 289
Uploading a FortiAP image on the wireless controller ... 289
Configuring control message off-loading ... 290
Enabling Dynamic Radio Mode Assignment (DRMA) ... 290
RADIUS Change of Authorization (CoA) support ... 291
Wireless network protection ... 293
Wireless Intrusion Detection System ... 293
Rogue AP detection ... 294
WIDS client de-authentication rate for DoS attacks ... 295
WiFi data channel encryption ... 295
Configuring encryption on a FortiGate unit ... 295
Configuring encryption on a FortiAP unit ... 296
Protected Management Frames and Opportunistic Key Caching support ... 296
Preventing local bridge traffic from reaching the LAN ... 297
FortiAP-S and FortiAP-U bridge mode security profiles ... 297
DHCP snooping and option-82 data insertion ... 298
DHCP address enforcement ... 299
Disabling FortiAP port access ... 299
Suppressing phishing SSID ... 300
Wireless network monitoring ... 303
Monitoring wireless health and clients ... 303

Monitoring rogue APs ... 304
On-wire rogue AP detection technique ... 305
Rogue AP scanning as a background activity ... 306
Configuring rogue scanning ... 307
Suppressing rogue APs ... 308
Monitoring wireless clients ... 309
Understanding client health ... 310
Monitoring wireless clients over IPv6 traffic ... 311
Tunnel mode SSID IPv6 traffic ... 311
Local bridge mode SSID IPv6 traffic ... 313
CLI commands for IPv6 rules ... 316
Monitoring application usage for clients connected to bridge mode SSIDs ... 317
Monitoring FortiAP with SNMP ... 322
FortiAP SNMP implementation ... 323
Downloading the FortiAP MIB and Fortinet Core MIB files ... 323
FortiAP SNMP trap messages ... 323
FortiAP SNMP queries ... 325
Monitoring FortiAP temperatures ... 325
Enabling spectrum analysis ... 326
Disable dedicated scanning on FortiAP F-Series profiles ... 332
Enabling AP scan channel lists to optimize foreground scanning ... 335
Optimizing memory storage by limiting monitoring data ... 338
CLI commands ... 338
Wireless network examples ... 342
Basic wireless network example ... 342
Configuring authentication for wireless users ... 342
Configuring the SSID ... 343
Adding the SSID to the FortiAP Profile ... 344
Configuring security policies ... 344
Connecting the FortiAP units ... 345
Wireless network example with FortiSwitch ... 347
Configuring FortiLink ... 348
Connecting the FortiSwitch ... 349
Configuring a wireless VLAN ... 349
Connecting the FortiAP units ... 350
Complex wireless network example ... 350
Scenario example ... 350
Configuration example ... 351
Configuring authentication for employee wireless users ... 351
Configuring authentication for guest wireless users ... 352
Configuring the SSIDs ... 353
Configuring the FortiAP profile ... 355
Configuring firewall policies ... 356
Connecting the FortiAP units ... 358
FortiGate WiFi controller 1+1 fast failover example ... 360
CAPWAP hitless failover using FGCP ... 362
Diagnose commands ... 364

Wireless network with segregated WLAN traffic ... 366
Example configuration ... 367
FortiWiFi unit as a wireless client ... 370
Configuring a FortiWiFi unit as a wireless client ... 371
Controlled AP selection support in FortiWiFi client mode ... 374
Configuring a FortiWiFi unit to run in concurrent AP and wireless client mode ... 374
Enabling EAP/TLS authentication on a FortiWiFi unit in client mode ... 376
Configuring WPA3 security modes on FortiWiFi units operating in client mode ... 379
WiFi maps ... 381
Bluetooth Low Energy scan ... 384
Override BLE profiles from WTP profiles and group ... 385
Pole Star NAO Cloud service integration ... 385
Eddystone BLE beacon profile integration ... 389
Location-based services ... 390
Pole Star location-based services ... 390
Configuring location tracking ... 390
Automatic deletion of outdated presence data ... 392
Viewing device location data on a FortiGate unit ... 392
Example output ... 392
Configuring FortiPresence ... 393
FortiPresence push REST API ... 393
Configuring FortiPresence server IP ... 394
Support for Electronic Shelf Label systems ... 396
Hanshow integration ... 396
SES-Imagotag ... 397
Troubleshooting ... 399
FortiAP shell command ... 399
Signal strength issues ... 399
Asymmetric power issue ... 400
Frequency interference ... 402
Throughput issues ... 403
Link testing ... 403
Performance testing ... 403
IP packet fragmentation prevention in CAPWAP tunnels ... 404
Slow DTLS response ... 404
Client connection issues ... 404
Debugging client connection issues ... 405
Checking the WiFi password ... 406
FortiAP connection issues ... 406
Debugging FortiAP connection issues ... 406
Testing wireless network health with SAM ... 409
Captive portal authentication in service assurance management (SAM) mode ... 413
Determining the coverage area of a FortiAP ... 415
Best practices for OSI common sources of wireless issues ... 417
Best practices for Layer 1 ... 418

Best practices for Layer 2 ... 418
Best practices for Layer 3 and above ... 419
Extended logging ... 420
Packet sniffer ... 430
CAPWAP packet sniffer ... 430
Wireless traffic packet sniffer ... 431
Debug commands ... 434
Sample outputs ... 434
Extension information support ... 435
Disabling 802.11d for client backward compatibility ... 435
FortiAP CLI configuration and diagnostics commands ... 439
Configuration commands ... 439
Diagnostics commands ... 444
FortiAP API ... 447
API Schema and documentation ... 447
Enable API for Location Based Services station info ... 448

Change log

Date	Change description
2024-07-25	Initial release. See What's new in this release on page 12.
2024-08-01	Updated What's new in this release on page 12.
2024-08-08	Updated Monitoring FortiAP temperatures on page 325 and FortiAP CLI configuration and diagnostics commands on page 439.
2024-09-12	Renamed FortiLAN Cloud to FortiEdge Cloud.

What's new in this release

FortiOS 7.6.0 wireless includes the following changes:

- Support the 802.11mc protocol on FortiAP.
- Support isolating mDNS traffic on the Bonjour profile.
- Support OpenRoaming Standards on FortiAP.
- Support local LAN segregation for FortiAP.
- Improve FortiAP sniffer to capture all frame types across specified channel bandwidths.
- Support RADSEC on WPA2/WPA3-Enterprise SSID.
- Add GUI support for configuring data rate controls and sticky client thresholds.
- Support self-registration of MPSKs through FortiGuest.
- Support RADIUS NAS-ID on FortiAPs in standalone mode.
- Support WPA3-SAE and WPA3-SAE Transition security modes in MPSK profiles.
- Support IKEv2 for FortiAP IPsec data channel management.

For more information about the FortiOS 7.6.0 wireless features, see the FortiOS Release Notes and New Features Guide.

For more information about new FortiAP, FortiAP-S, and FortiAP-W2 features, see their respective release notes in the FortiAP Documentation Library.

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 13
- FortiGate units on page 13
- FortiWiFi units on page 14

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, 802.11AX, 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 FortiAP 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 14
- Cloud AP management on page 14
- Dedicated wireless controller on page 15

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 or a FortiGate.
- Connect external FortiAP units to a FortiSwitch, and then to a FortiWiFi or 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 units.

Cloud AP management

FortiEdge Cloud offers management capabilities for standalone FortiAPs that scale from individual organizations managing a handful of APs, to large enterprises managing several thousand APs. FortiEdge 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, FortiEdge Cloud eliminates the need for costly on-site technical expertise.

With the FortiEdge Cloud provisioning and management portal, you can manage and configure FortiAP units.

For more details about FortiEdge Cloud, see the FortiEdge 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.

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.

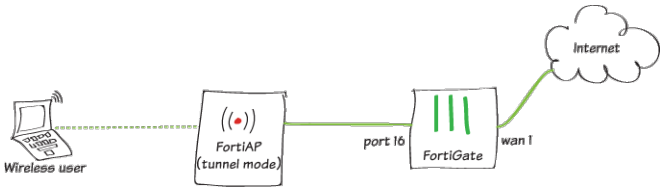
Getting started with FortiAP management

This section contains topics to get you started with using FortiGate's Wireless Controller to manage FortiAP units.

- Configuring the FortiGate interface to manage FortiAP units on page 17
- Discovering, authorizing, and deauthorizing FortiAP units on page 18
- FortiAP diagnostics and tools on page 23
- Setting up a mesh connection between FortiAP units on page 25
- Data channel security: clear-text, DTLS, and IPsec VPN on page 30

Configuring the FortiGate interface to manage FortiAP units

This guide describes how to configure a FortiGate interface to manage FortiAPs.



Based on the above topology, this example uses port16 as the interface used to manage connection to FortiAPs.

1. Enable a DHCP server on port16:
   a. From FortiGate, go to *Network* > *Interfaces*.
   b. Edit port16.
   c. In the *IP/Network Mask* field, enter an IP address for port16.
   d. Enable *DHCP Server*, keeping the default settings.
2. As it is a minimum management requirement that FortiAP establish a CAPWAP tunnel with the FortiGate, you must enable CAPWAP access on port16 to allow it to manage FortiAPs:
   a. Go to *Network* > *Interfaces*.
   b. Double-click *port16*.
   c. Under *Administrative Access*, select *Security Fabric Connection*.
   d. Click *OK*.
3. If required, you can enable the VCI-match feature using the CLI. When VCI-match is enabled, only devices with a VCI name that matches the preconfigured string can acquire an IP address from the DHCP server. To configure VCI-match, run the following commands:

```
config system dhcp server
   edit 1
      set interface port16
      set vci-match enable
      set vci-string "FortiAP"
   next
end
```

4. To create a new FortiAP entry automatically when a new FortiAP unit is discovered, run the following command. By default, this option is enabled.

```
config system interface
```

```
    edit port16
      set allow-access fabric
      set ap-discover enable
    next
end
```

5. To allow FortiGate to authorize a newly discovered FortiAP to be controlled by the FortiGate, run the following command. By default, this option is disabled.

```
config system interface
    edit port16
      set allow-access fabric
      set auto-auth-extension-device enable
    next
end
```

For more information, see Configuring the network interface for the AP unit on page 35.

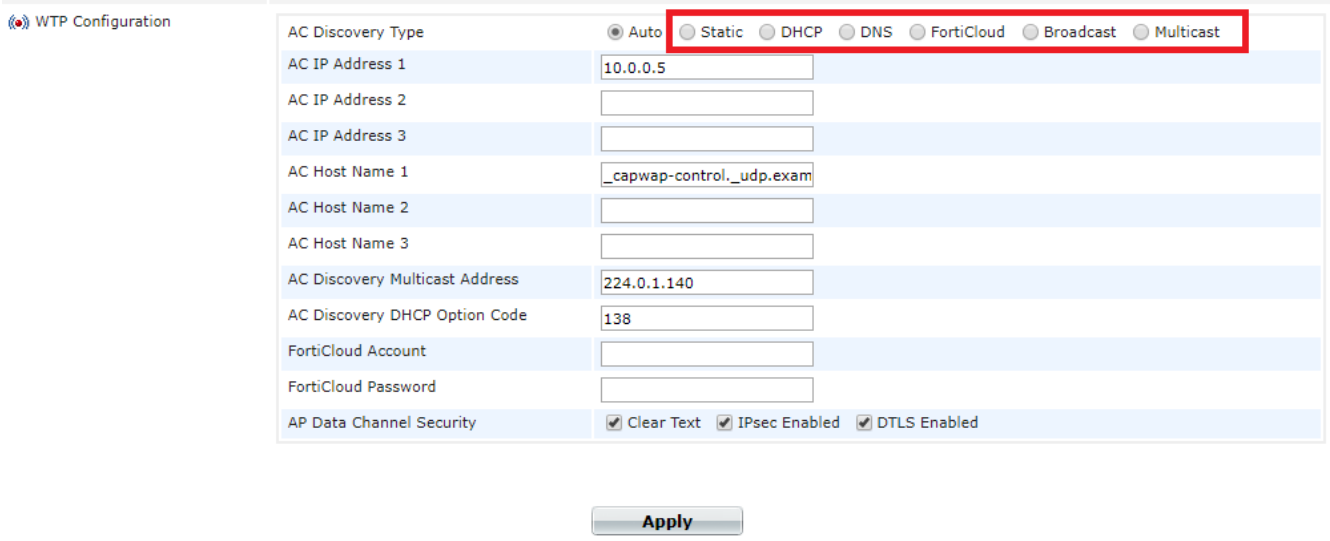
Discovering, authorizing, and deauthorizing FortiAP units

In order for FortiGate to manage a FortiAP unit, it must first discover the FortiAP and then authorize it.

For more information about discovery, authorization, and ways to pre-authorize FortiAPs, see Discovery and authorization of APs on page 195

Discovering a FortiAP unit

For a FortiGate acting as an AP controller (AC) to discover a FortiAP unit, the FortiAP must be able to reach the AC. A FortiAP with the factory default configuration has various ways of acquiring an AC's IP address to reach it.



AC discovery type	Description
Auto	The FortiAP attempts to be discovered in the below ways sequentially within an endless loop.
Static	The FortiAP sends discover requests to a preconfigured IP address that an AC owns.
DHCP	The FortiAP acquires the IP address of an AC in DHCP option 138 (the factory default) of a DHCP offer, which the FortiAP acquires its own IP address from.
DNS	The FortiAP acquires the AC's IP address by resolving a preconfigured FQDN.
FortiCloud	FortiGate Cloud discovers the FortiAP.
Broadcast	FortiAP is discovered by sending broadcasts in its local subnet.
Multicast	FortiAP is discovered by sending discovery requests to a multicast address of 224.0.1.140, which is the factory default.

See Advanced WiFi controller discovery on page 212 for more information on WiFi controller discovery methods.

AC actions when a FortiAP attempts to get discovered

Enable `ap-discover` on the AC for the interface designed to manage FortiAPs:

```
config system interface
   edit "lan"
      set ap-discover enable
   next
end
```

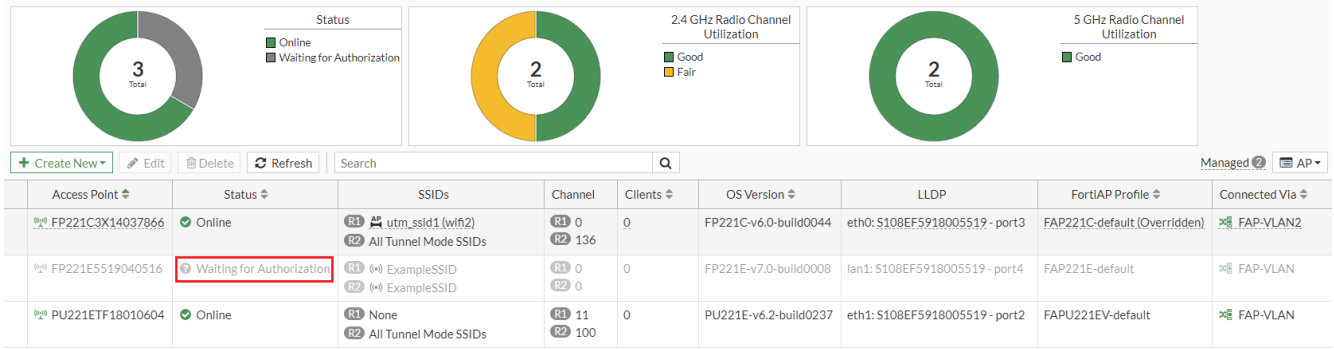
The `ap-discover` command allows the AC to create an entry in the managed FortiAPs table when it receives the FortiAP's discovery request. The `ap-discover` command is enabled by default. When the FortiAP entry is created automatically, it is marked as *discovered* status, and is pending for an administrator's authorization, unless the following setting is present:

```
config system interface
    edit "lan"
        set auto-auth-extension-device enable
    next
end
```

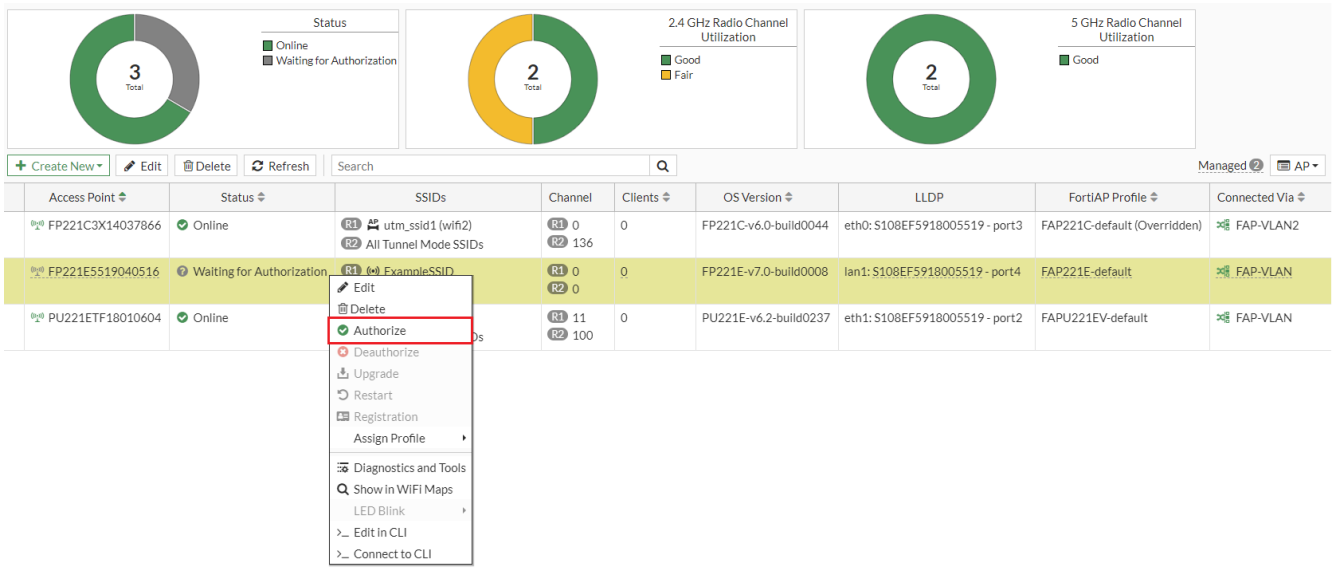
The `auto-auth-extension-device` command will allow AC authorize an new discovered FortiAP automatically without an administrator's manual authorization operation. The `auto-auth-extension-device` command is disabled by default.

Authorize a discovered FortiAP

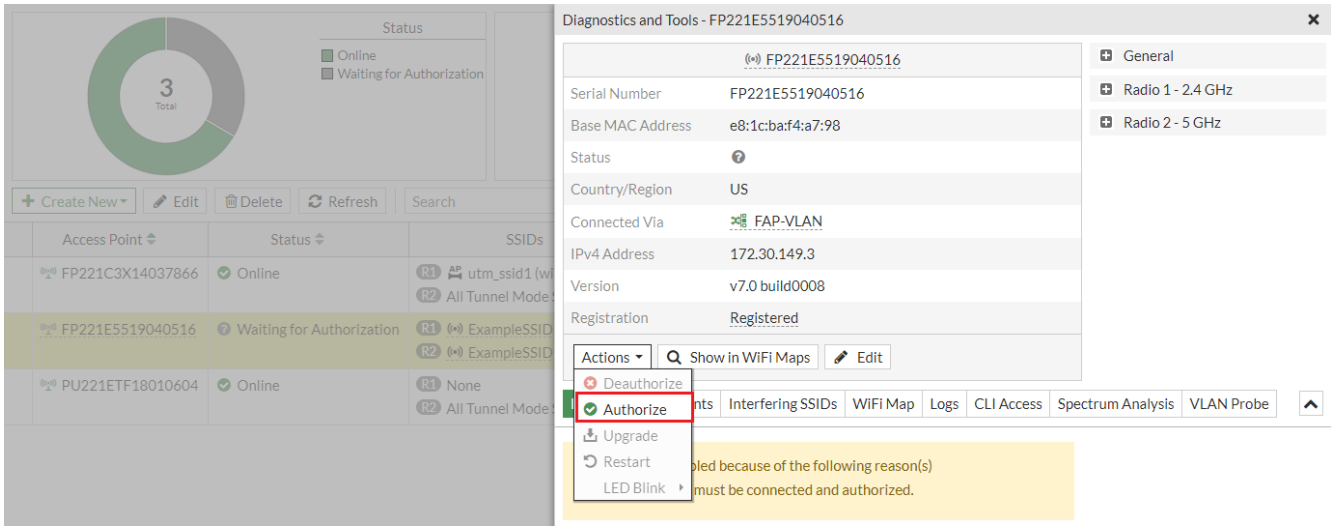
Once the FortiAP discovery request is received by AC, a FortiAP entry will be added to the managed FortiAP table and shown in *WiFi and Switch Controller > Managed FortiAPs*.



To authorize the specific AP, select the FortiAP entry, and then right-click and select *Authorize* from the context menu.



Authorization can also be granted from the FortiAP details panel under the *Actions* menu.



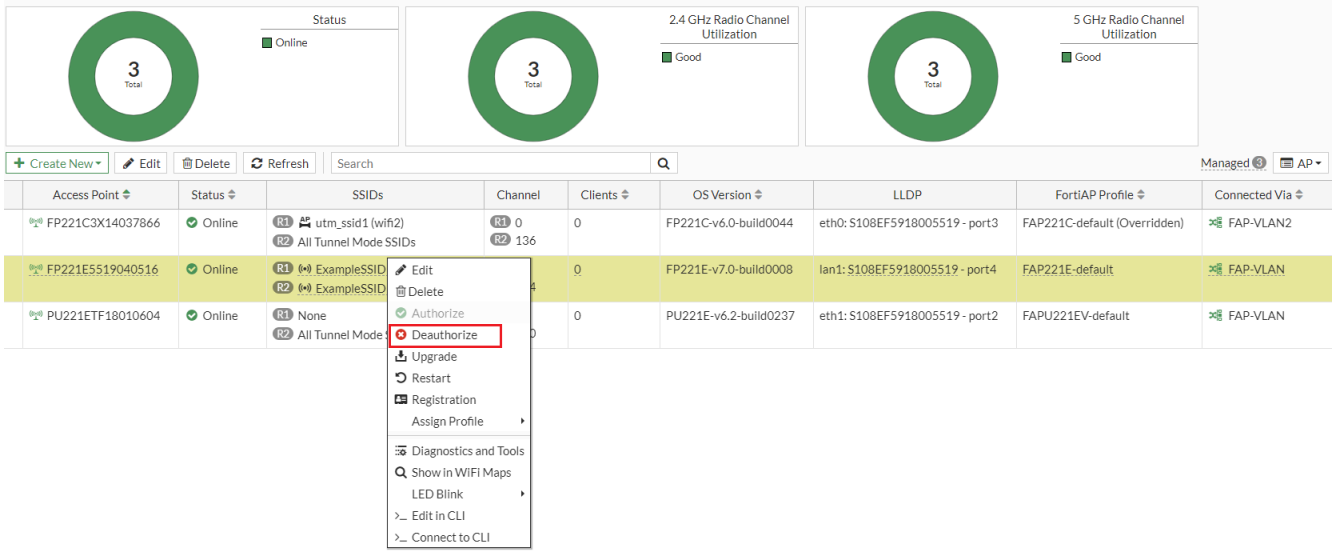
Authorization can also be granted through the following CLI commands:

```
config wireless-controller wtp
    edit "FP423E3X16000320"
        set admin enable
    next
end
```

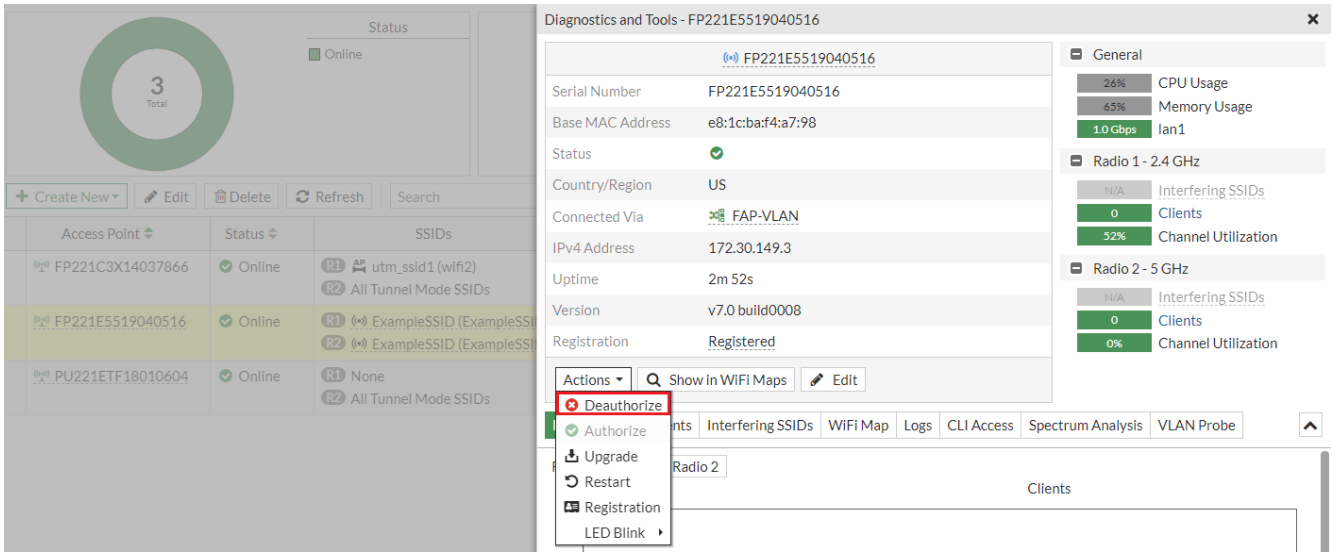
When you authorize a FortiAP unit, it is configured by default to use the default FortiAP profile (determined by model). The FortiAP profile defines the entire configuration for the AP (see Creating a FortiAP profile on page 38). You can assign a different profile, if needed, by right-clicking the authorized FortiAP and selecting *Assign Profile*.

De-authorize a managed FortiAP

To de-authorize a managed FortiAP, select the FortiAP entry, and then click *Deauthorize* on the top of the table or right-click and select *Deauthorize* from the context menu.



You can also de-authorize from the FortiAP details panel under the *Action* menu.



You can also de-authorize with the following CLI commands:

```
config wireless-controller wtp
    edit "FP423E3X16000320"
        set admin discovered
    next
end
```

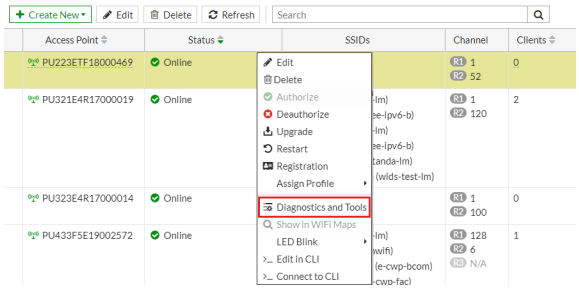
FortiAP diagnostics and tools

On the *Managed FortiAPs* page, you can use the Diagnostics and Tools option to view all available details of a FortiAP, including:

- FortiAP system information.
- Dynamic health and performance information.
- Dynamic radio and client details.
- Relevant links such as location of the FortiAP in the location map.

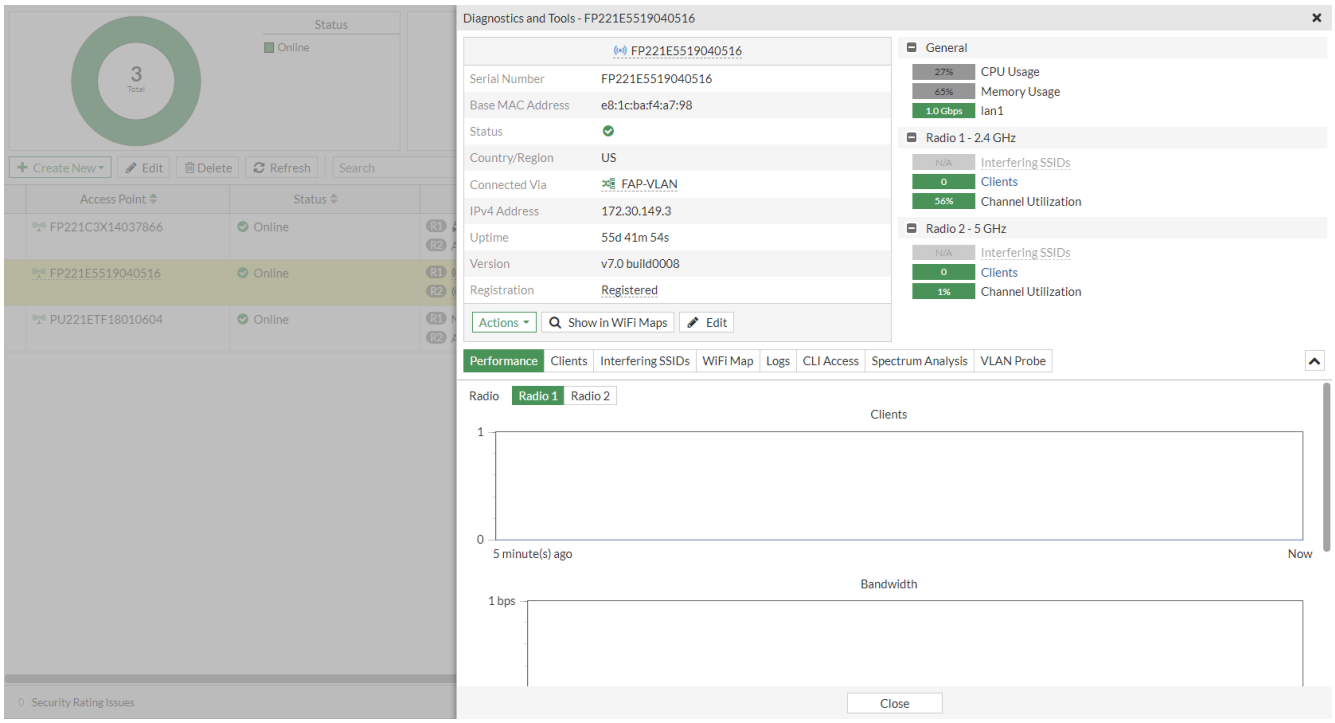
Sample configuration

In *WiFi and Switch Controller* > *Managed FortiAPs*, right-click a FortiAP and select *Diagnostics and Tools*.

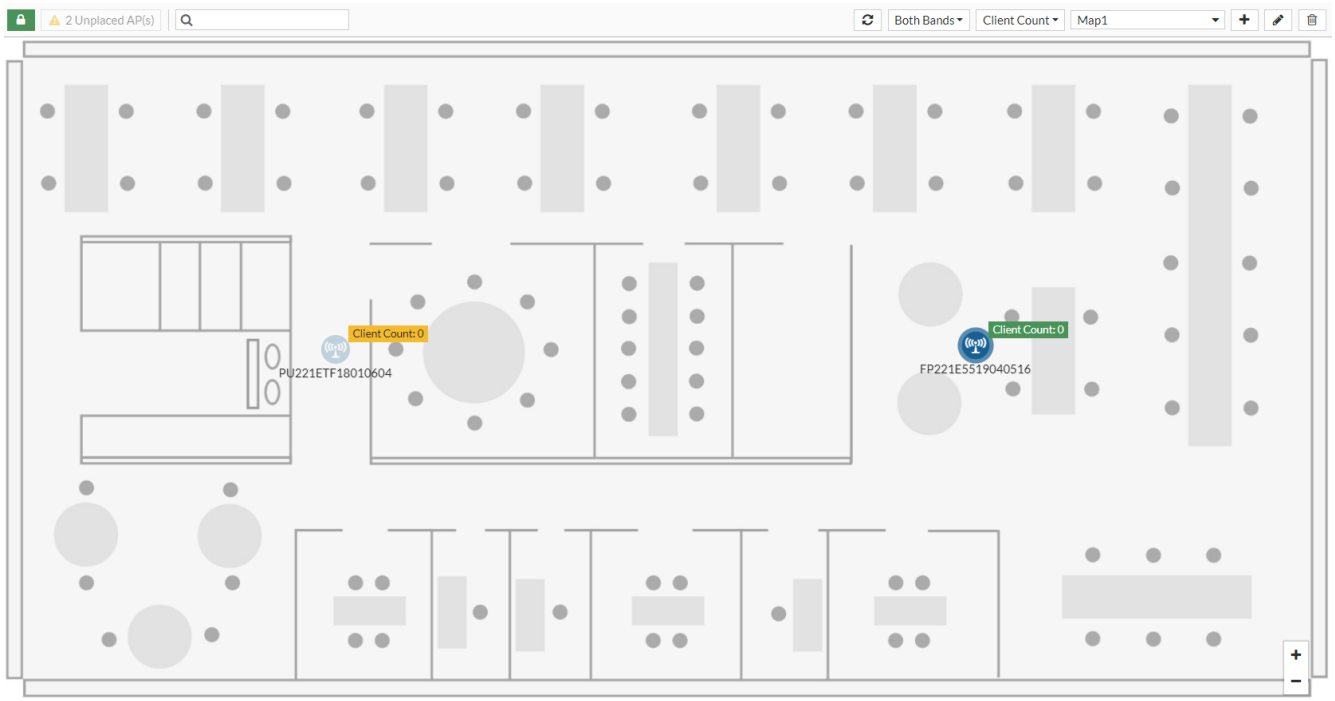


The Diagnostics and Tools pane show the following information:

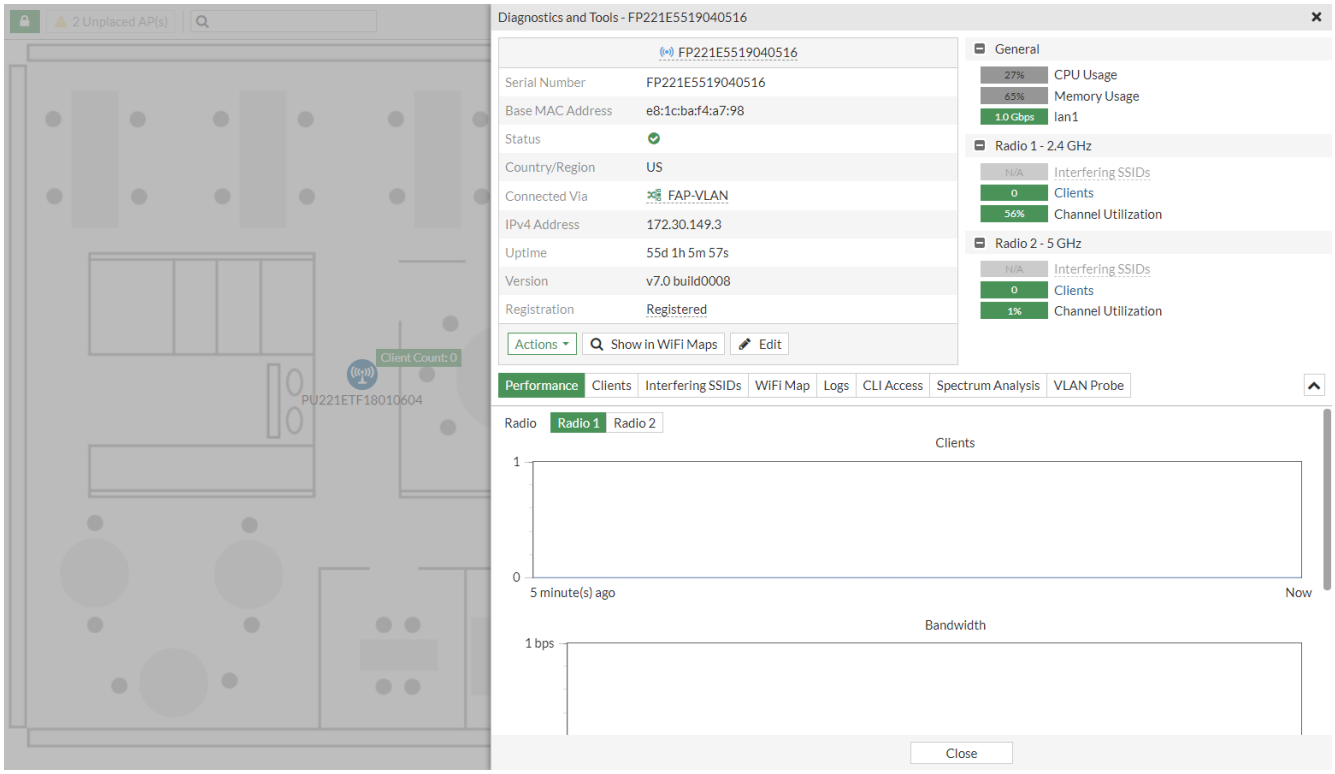
- The top left shows a summary of configuration and connection status for the AP. The *Actions* button enables you to Authorize/Deauthorize, Upgrade, Restart, and flash the LED lights on the FortiAP. The *Edit* button opens the *Edit Managed AP* pane. The *Show in WiFi Maps* button is shown if the FortiAP is on a WiFi Map.
- The top right shows the general health assessment of the AP and the health assessment based on radio band.
- The bottom section includes tabs to show the *Radios* summary, *Clients* list, and a filtered *Logs* view of all logs of the FortiAP.



If a FortiAP is on a WiFi Map, click the *Show in WiFi Maps* button and that FortiAP is highlighted with a flashing blue circle on the WiFi Map.



On the WiFi Map, click a FortiAP icon to open it's Diagnostics and Tools pane.

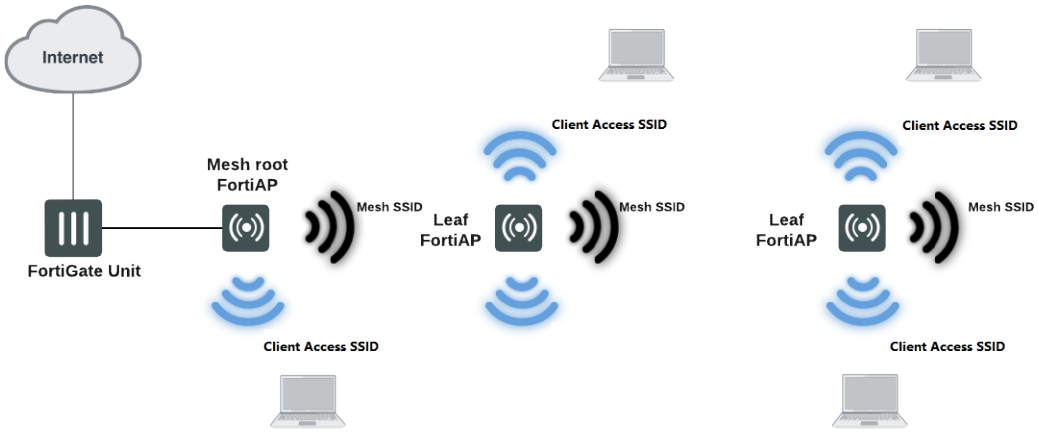


Setting up a mesh connection between FortiAP units

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. For more information about wireless mess configurations, see Wireless mesh configuration on page 243.

To set up a WiFi mesh connection, a minimum of three devices are required:

1. A FortiGate as the AP Controller (AC)
2. A FortiAP as the Mesh Root AP (MRAP)
3. A FortiAP as a Mesh Leaf AP (MLAP).

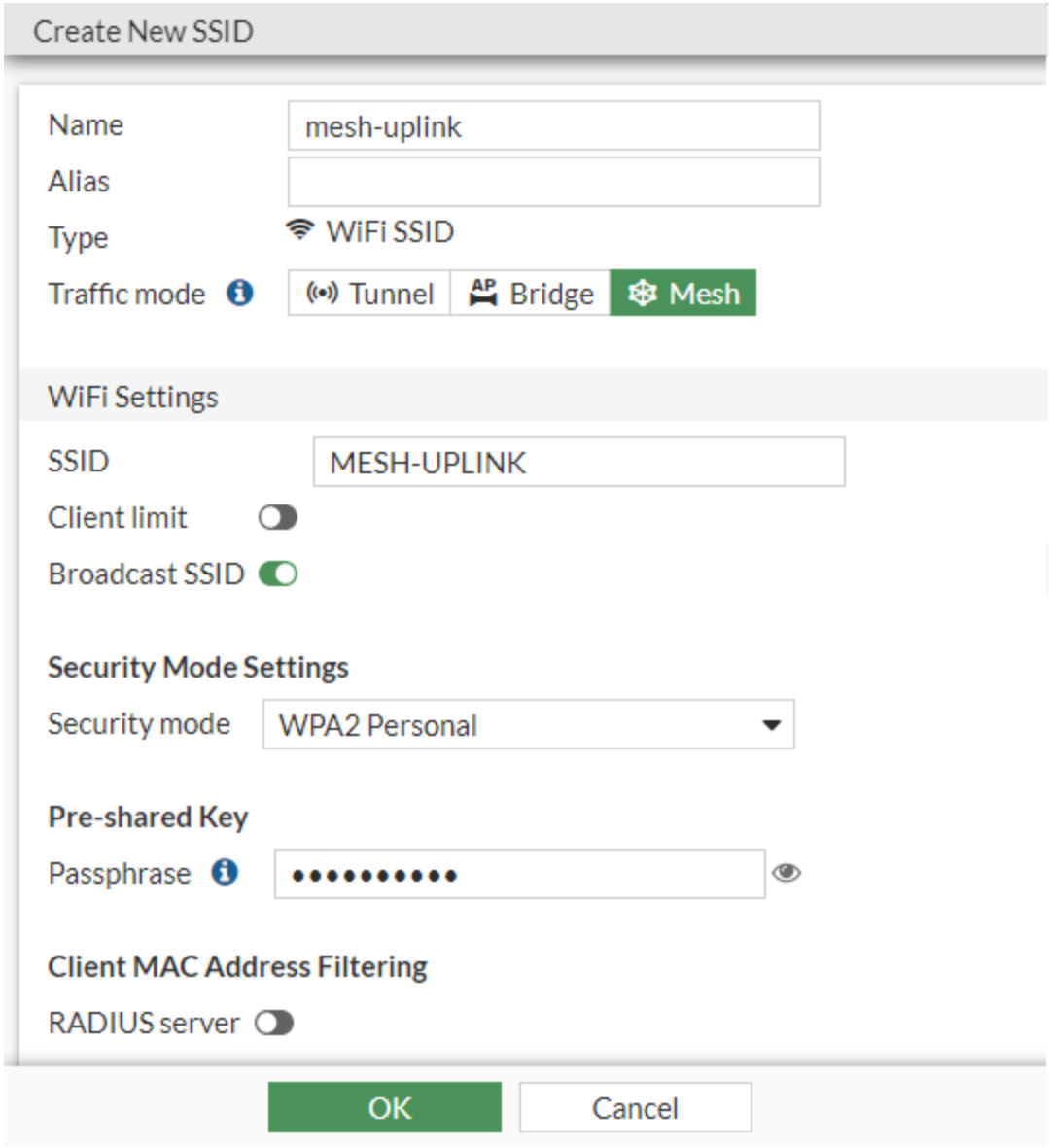


Configuring the AC

These instructions assume that the Mesh Root AP (MRAP) is already being managed by the AC (see Configuring the FortiGate interface to manage FortiAP units on page 17 and Discovering, authorizing, and deauthorizing FortiAP units on page 18).

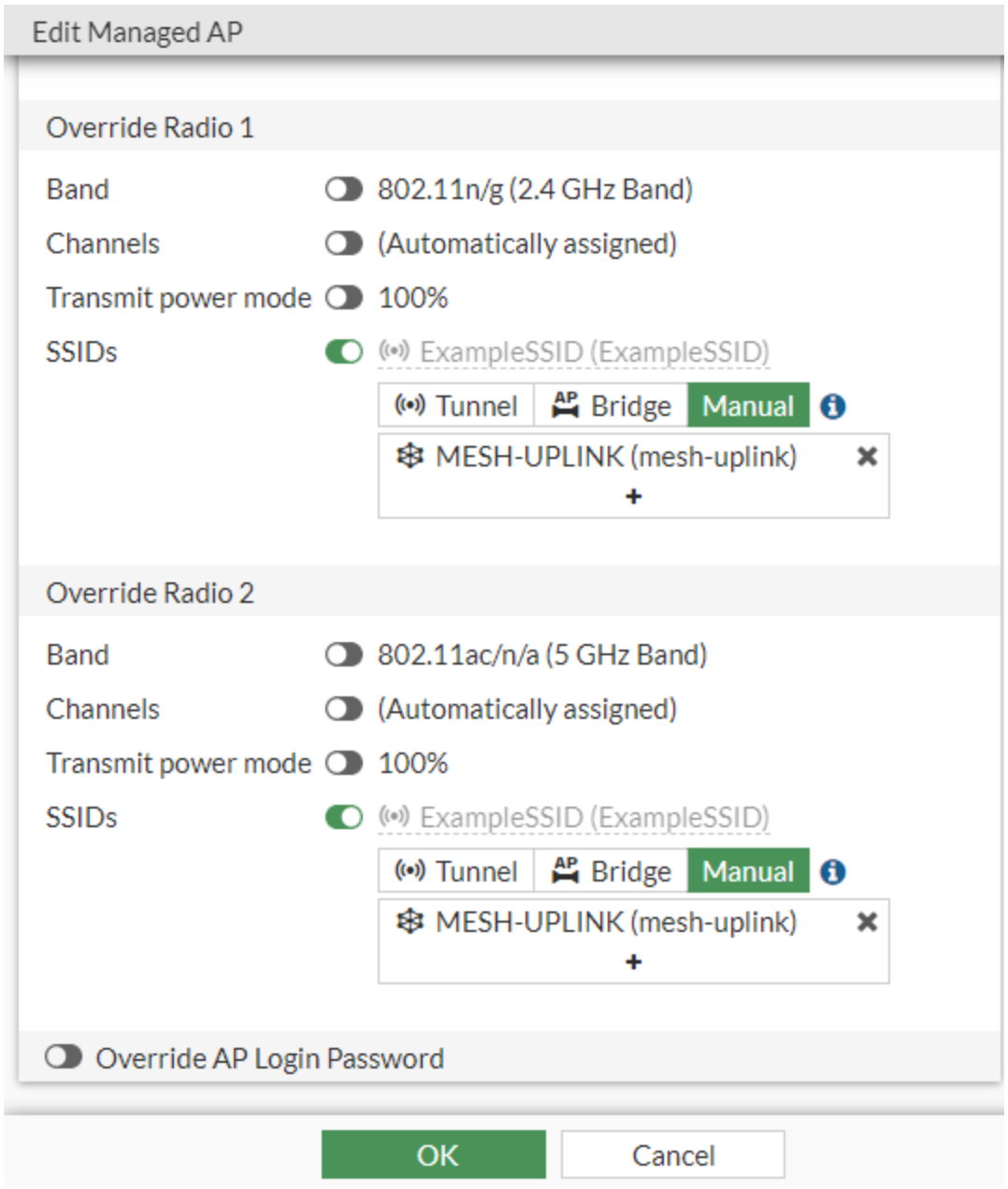
To configure the AC:

1. Go to *WiFi and Switch Controller* > *SSIDs* and create a mesh SSID.



2. Go to *WiFi and Switch Controller* > *Managed FortiAPs*, edit the MRAP, and assign the mesh SSID to the MRAP, and

wait for a connection.



Configuring the MLAP

The Mesh Leaf AP (MLAP) can be configured to use the mesh link as its Main uplink or a Backup link for Ethernet connections.

To configure the MLAP:

1. On the FortiAP, go to *Connectivity*.

2. Set *Uplink* to *Mesh* or *Ethernet with mesh backup support*.
3. Enter a mesh SSID and password.
4. Optionally, select *Ethernet Bridge* (see Main uplink on page 29).

   This option is not available if *Uplink* is set to *Ethernet with mesh backup support*.

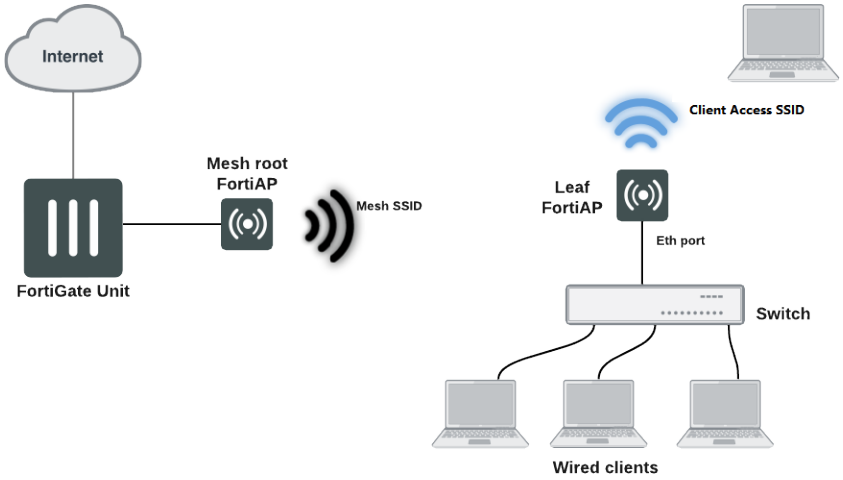
Once the MLAP has joined the AC, it can be managed in the same way as a wired AP.

A mesh SSID can also be assigned to an MLAP for other downstream MLAPs, creating a multi-hop WiFi mesh network. The maximum hop count has a default value of 4, and can be configured in the FAP console with the following commands:

```
cfg -a MESH_MAX_HOPS=n
cfg -c
```

Main uplink

When a mesh link is set as the main uplink of the MLAP, the Ethernet port on the MLAP can be set up as a bridge to the mesh link. This allows downstream wired devices to use the mesh link to connect to the network.



To enable a mesh Ethernet bridge, select *Ethernet Bridge* in the FortiAP *Connectivity* section in the GUI, or use the following console commands:

```
cfg -a MESH_ETH_BRIDGE=1
cfg -c
```

Backup link for Ethernet connections

When a mesh link is set to be the backup link for an Ethernet connection, the mesh link will not be established unless the Ethernet connection goes offline. When a mesh link is in this mode, the Ethernet port cannot be used as a bridge to the mesh link.

Data channel security: clear-text, DTLS, and IPsec VPN

After the FortiAP joins a FortiGate, a CAPWAP tunnel is established between the FortiGate and FortiAP.

There are two channels inside the CAPWAP tunnel:

- The control channel for managing traffic, which is always encrypted by DTLS.
- The data channel for carrying client data packets, which can be configured to be encrypted or not.

The default setting for `dtls-policy` is `clear-text`, meaning it is non-encrypted. The following settings are available to encrypt the data channel:

- `dtls-enabled`
- `ipsec-vpn`
- `ipsec-vpn-sn`

```
config wireless-controller wtp-profile
  edit "FortiAP-profile-name"
    set dtls-policy clear-text|dtls-enabled|ipsec-vpn|ipsec-vpn-sn
  next
end
```

Of these settings, `clear-text` has the highest possible data throughput. Furthermore, FortiGates with hardware acceleration chips can offload CAPWAP data traffic in `clear-text` and achieve much higher throughput performance (see CAPWAP Offloading on page 232).

You can only configure the data channel using the CLI.

When data security is not a major concern, we recommend that you set the data channel to non-encrypted. For example, when the FortiGate and FortiAP are operating in an internal network.

To set the data channel to non-encrypted using the CLI:

```
config wireless-controller wtp-profile
  edit "FortiAP-profile-name"
    set dtls-policy clear-text
  next
end
```

Encrypting the data channel

There are data channel encryption settings on both the FortiGate unit and the FortiAP units. The settings must agree or the FortiAP unit will not be able to join the WiFi network. For more instructions on how to configure encryption on a FortiAP unit, see WiFi data channel encryption on page 295

When the FortiGate and FortiAP are in different networks, and the data channel might transit through a public network, we recommend that you encrypt the data channel to protect your data with either DTLS or IPsec VPN.

DTLS

To encrypt the data channel with DTLS using the CLI:

```
config wireless-controller wtp-profile
  edit "FortiAP-profile-name"
    set dtls-policy dtls-enabled
    set dtls-in-kernel disable|enable
  next
end
```

`set dtls-in-kernel` is only available after `dtls-policy` is set to `dtls-enabled`. When you enable `dtls-in-kernel`, the FortiAP OS kernel processes the traffic encryption and decryption, which could provide better throughput performance. DTLS encryption cannot be hardware-accelerated on the FortiGate so when DTLS is enabled, data throughput performance is significantly lower than with `clear-text`.

IPsec VPN

To encrypt the data channel with IPsec VPN using the CLI:

```
config wireless-controller wtp-profile
  edit "FortiAP-profile-name"
    set dtls-policy ipsec-vpn|ipsec-vpn-sn
  next
end
```

This automatically establishes an IPsec VPN tunnel between the FortiGate and FortiAP that carries CAPWAP data packets. FortiGates with NP6 chips can offload CAPWAP data traffic in IPsec, so this encryption option has better throughput performance than DTLS. Because there is no built-in hardware acceleration chip, the FortiAP is considered the performance bottleneck in this scenario.

Optionally, you can use the `ipsec-vpn-sn` policy instead. It also establishes an IPsec VPN tunnel between the FortiGate and FortiAP that carries CAPWAP data packets, but it includes the FortiAP serial number within this tunnel.

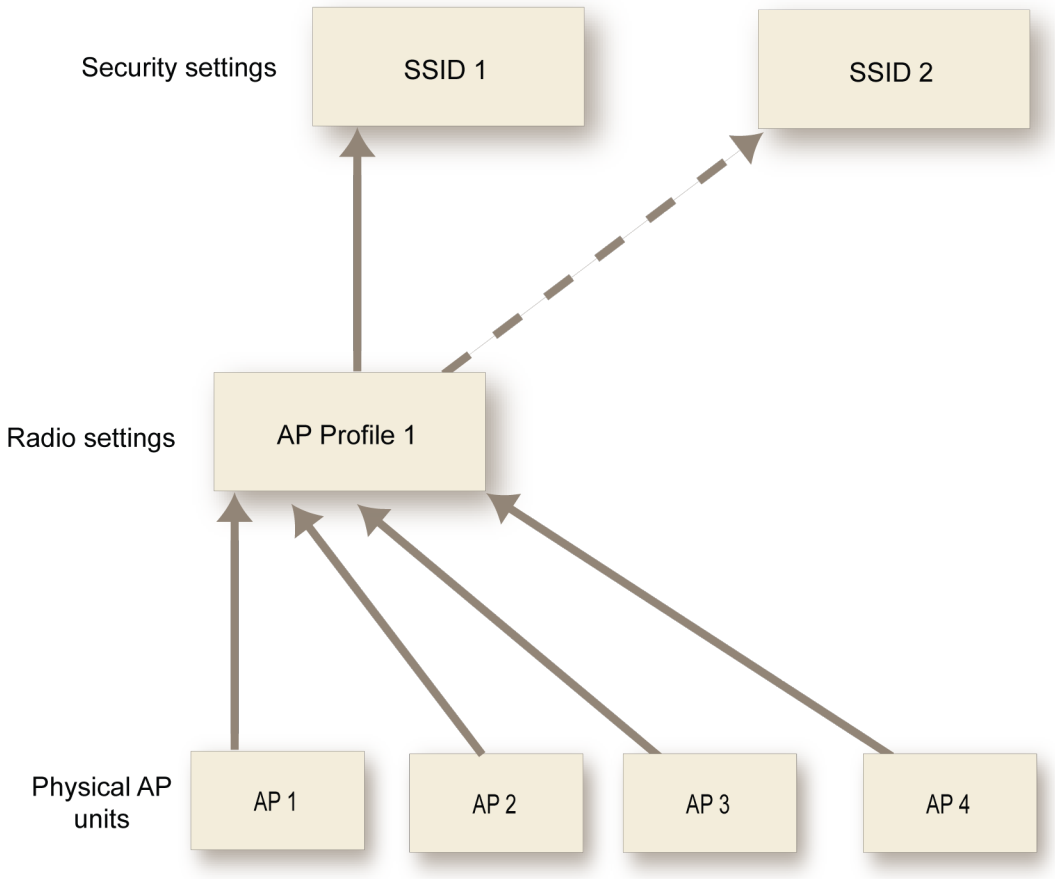
Wireless network configuration

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 Controller* > *Local WiFi Radio*. The available operational settings are the same as those for external access points which are configured at *WiFi 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, FAP-224E, and FAP-231E	97 and 98

Wireless network configuration tasks

To configure a wireless network, perform the following tasks:

1. Setting your geographic location on page 35
2. Configuring the network interface for the AP unit on page 35
3. Creating a FortiAP profile on page 38
4. Defining a wireless network interface (SSID) on page 43
5. Configuring security on page 52
6. Defining SSID groups on page 104
7. Configuring dynamic user VLAN assignment on page 104
8. Configuring user authentication on page 117
9. Configuring firewall policies for the SSID on page 136
10. Configuring the built-in access point on a FortiWiFi unit on page 137
11. Enforcing UTM policies on a local bridge SSID on page 138

For AP configuration details, see Access point configuration on page 192.

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 and 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
...	**...**	**...**	**...**	**...**

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.

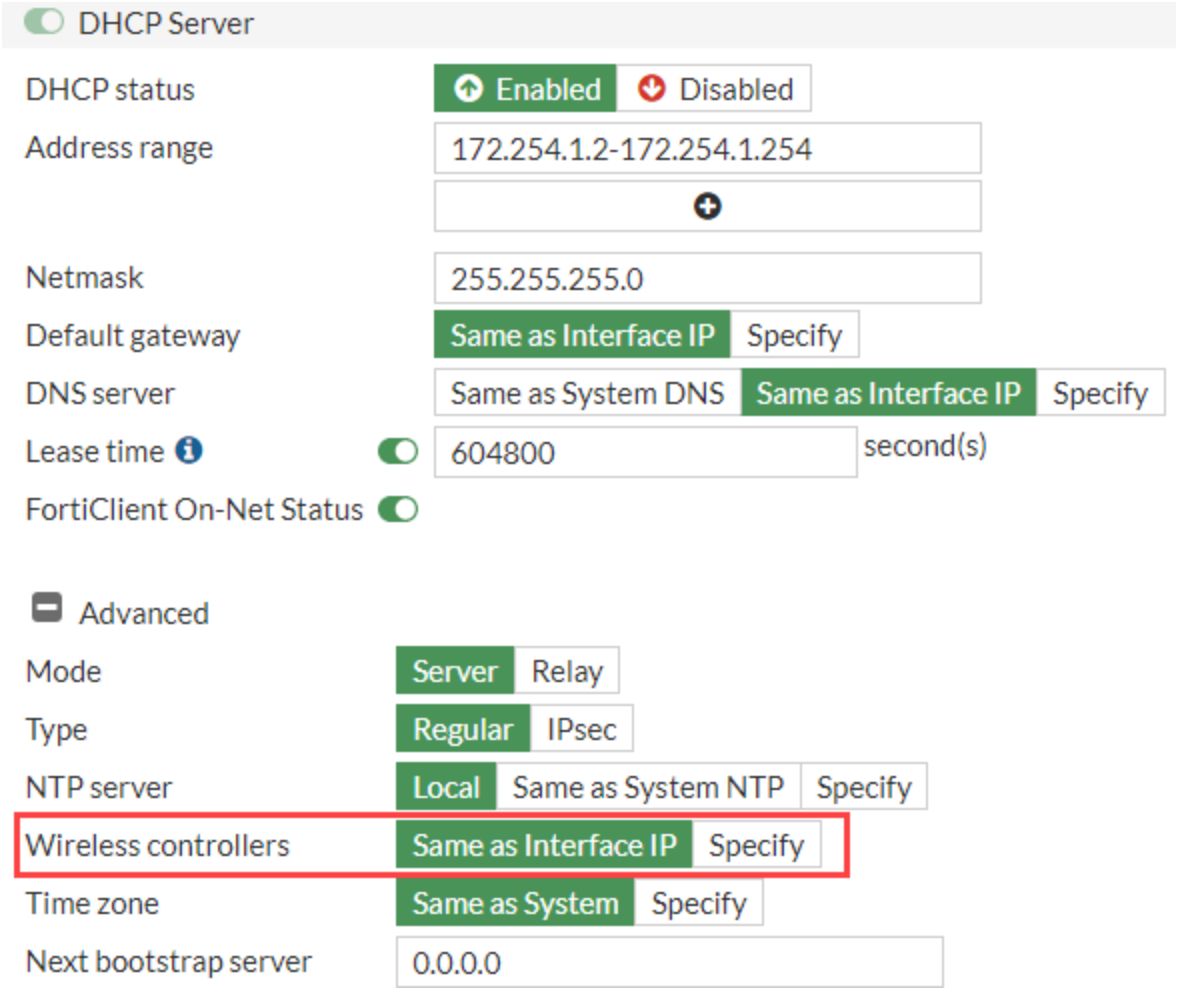
In this example, the FortiAP units connect to port3 and are controlled through IP addresses on the 10.10.70.0/24 network.

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 *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*.

If you enable DHCP Server, you can also specify the Wireless controller IP address from under the *Advanced* section.



To configure the interface for the AP unit - CLI:

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

```
config system interface
  edit "port3"
    set mode static
    set ip 10.10.70.1 255.255.255.0
```

```
        set allowaccess fabric
      next
    end
    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.

Understanding FortiWiFi aplink interface

The aplink link interface is an interface unique to certain FortiWiFi models, including, but not limited to, FWF-80F-2R and FWF-81F-2R. It acts as an internal trunk interface between the FortiAP and FortiGate. The aplink1 and aplink2 members are physical interfaces between the FortiAP and the FortiGate.

Name	Type	Members
802.3ad Aggregate 10		
aplink	802.3ad Aggregate	aplink1 aplink2
fortilink	802.3ad Aggregate	internal1

You can edit the aplink interface to change the subnet IP, however, the DHCP server should *not* be edited as it can cause the internal AP to stop working and lead to loss of WiFi capability on the AP.

To configure the aplink interface - CLI:

```
config system interface
  edit "aplink"
    set vdom "root"
    set ip 192.168.80.1 255.255.255.0
    set allowaccess ping fabric
    set type aggregate
    set member "aplink1" "aplink2"
    set device-identification enable
```

```
  next
end
```

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. Depending on the model, FortiAP units contain two or more radio transceivers, making it possible to provide 2.4 GHz 802.11b/g/n/ax, 5 GHz 802.11a/n/ac/ax/be, or 6 GHz 802.11ax/be service from the same access point. The radios can also be used for monitoring accepted or rogue APs through 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 and Switch Controller* > *FortiAP Profiles* and select *Create New*.
2. Enter a *Name* for the FortiAP Profile.

3. Configure the following options:

Platform	Select the FortiWiFi or FortiAP model to which this profile applies. If you selected a WiFi 6E capable model, select a *Platform mode*: • *Single 5G* - Only one radio operates on the 5GHz 802.11ax/ac/n/a band. • *Dual 5G* - Two radios operate on the 5GHz 802.11ax/ac/n/a band and dedicated scanning is always disabled.
Indoor/Outdoor	Select where the FortiAP is being installed. You can override the default designation of the FortiAP to change the available channels based on your region.
Country/Region	Select the country or region to apply the Country Code for where the FortiAP will be used.
Split Tunneling Subnets	If split tunneling is used, enter a comma-separated list all of the destination IP address ranges that should *not* be routed through the FortiGate WiFi controller.
AP login password	Select if you want set a new AP login password or leave the password unchanged.
Administrative access	Select which types of administrative access you want to allow for the FortiAP: • HTTPS • SSH • SNMP
Client load balancing	Select a handoff type as needed (see Wireless client load balancing for high-density deployments on page 218).
802.1X authentication	Enable if you want to configure the FortiAP to act as a 802.1x supplicant to authenticate against the server using EAP-FAST, EAP-TLS or EAP-PEAP (see Configuring 802.1X supplicant on LAN on page 130).
UNII-4 5GHz band channels	Only available on G-series models. Enable if you want to use UNII-4 5GHz band channels (see Configuring UNII-4 5GHz radio bands on page 185).

4. 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 303.
WIDS profile	Optionally, select a Wireless Intrusion Detection (WIDS) profile. See Wireless Intrusion Detection System on page 293.
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. See Understanding Distributed Radio Resource Provisioning on page 141.

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 802.11n/ac/ax/be on 5 and 6 GHz radios.
Channel plan	Select if you want to automatically configure a Channel plan or if want to select custom channels. • *Three Channels* – Automatically selects channel 1, 6, and 11. • *Four Channels* – Automatically selects channels 1, 4, 8, and 11. • *Custom* – Select custom channels.
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. For 5 and 6 GHz radios, clicking *Set Channels* loads a channel selector panel where you can select individual channels. • *Toggle DFS Channels* – Select DFS channels. • *Toggle Weather Radar Channels* – Select Weather Radar channels. The channel chart also shows channel availability for 40MHz or 80MHz channel-bonding. On 6 GHz radio with 802.11be on a 320MHz channel width, you can select a channel extension.
Short guard interval	Select to enable the short guard interval for 802.11ac or 802.11n on 5 GHz.
Transmit power mode	Select how you want to determine transmit power: • *Percent* – Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device. • *dBm* – Transmit power is set using a dBm value. • *Auto* – Specify a range of dBm values and the power is set automatically.
Transmit power	Specify either the minimum and maximum Transmit power levels in dBm or as a percentage.
SSIDs	Select a traffic mode for SSIDs. • *Tunnel* – Available tunnel-mode SSIDs are automatically assigned to this radio. • *Bridge* – Available bridge-mode SSIDs are automatically assigned to this radio. This option is not available for FortiWiFi local radio platforms. • *Manual* – Manually select which available SSIDs and SSID groups to assign to this radio.
Monitor channel utilization	Select to enable monitoring channel utilization.

Radio 2 and 3 settings are available for FortiAP models with multiple radios.

5. In *Syslog profile*, enable if you want your FortiAPs to send logs to a syslog server (see Configuring a Syslog profile on page 139).
6. Click *OK*.

To configure a FortiAP profile - CLI:

Some FortiAP profile configuration options are only available in the CLI. For a full list of available CLI options, refer to the FortiOS CLI Reference Guide.

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 configure a FortiAP profile with Wi-Fi 7 - CLI:

This example configures a FAP-441K to broadcast 802.11be on Radios 2 and 3. Radio 2 and 3 have manual VAPs selected with the "sae-trans-akm" and "sae-akm24" VAPs applied respectively. Radio 3 also has a channel-bonding extension of 320MHz selected.

1. Create a WPA3-SAE security VAP with `akm24-only` enabled.

```
config wireless-controller vap
  edit "sae-akm24"
    set ssid "sae-akm24"
    set security wpa3-sae
    set pmf enable
    set beacon-protection enable
    set sae-h2e-only enable
    set akm24-only enable
    set local-bridging enable
    set schedule "always"
    set sae-password ENC
  next
end
```

`akm24-only`	WPA3 SAE using group-dependent hash only (default = disable). • *disable*: Disable WPA3 SAE using group-dependent hash only. • *enable*: Enable WPA3 SAE using group-dependent hash only. `akm24-only` is only supported for Wi-Fi7 clients and there is **no** backward compatibility. If you know that all the clients are Wi-Fi7 capable, then the VAPs can be configured with `akm24-only` enabled.

Note: WPA3-SAE SSID allows configuring either of the `akm24-only` and `additional-akms` features.

2. Create a WPA3-SAE-Transition security VAP with `additional-akms` enabled.

```
config wireless-controller vap
  edit "sae-trans-akm"
    set ssid "sae-trans-akm"
    set security wpa3-sae-transition
    set pmf optional
    set beacon-protection enable
    set additional-akms akm24
    set passphrase ENC
    set sae-h2e-only enable
    set local-bridging enable
    set schedule "always"
    set sae-password ENC
  next
end
```

`additional-akms`	Additional AKMs. • *akm6*: Use AKM suite employing PSK_SHA256. • *akm24*: Use AKM suite employing SAE_EXT. When `additional-akms` is enabled in the VAP, clients are given a choice to pick the highest akm they support. WPA3-SAE-Transition SSID allows backward compatibility and supports clients with mixed mode, so `additional-akms` has akm6 and akm24 options.

3. Create a FortiAP profile for a FortiAP K-series model with Wi-Fi 7 enabled on the radio. This example uses FAP441K.

```
config wireless-controller wtp-profile
  edit "FAP441K-profile"
    config platform
      set type 441K
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess ssh
    config radio-1
      set band 802.11ax-2G
      set vap-all manual
    end
    config radio-2
      set band 802.11be-5G
      set channel-bonding 40MHz
      set vap-all manual
      set vaps "sae-trans-akm"
      set channel "44" "48"
    end
    config radio-3
      set band 802.11be-6G
      set channel-bonding 320MHz
      set channel-bonding-ext 320MHz-1
      set vap-all manual
      set vaps "sae-akm24"
```

```
      set channel "45" "49" "65" "69" "73" "77" "81" "85" "89" "93" "97" "101" "105"
"109" "113" "117" "121" "125"
    end
    config radio-4
      set mode monitor
    end
  next
end
```

`channel-bonding-ext`	Channel bandwidth extension: 320 MHz-1 and 320 MHz-2 (default = 320 MHz-2). • *320MHz-1*: 320 MHz channel with channel center frequency numbered 31, 95, and 159. • *320MHz-2*: 320 MHz channel with channel center frequency numbered 63, 127, and 191.

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 and Switch Controller* > *SSIDs* and select *Create New* > *SSID*.
2. Fill in the following SSID fields as needed:

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.
Address	
IP/Network Mask	Enter the IP address and netmask for the SSID.
IPv6 Address/Prefix	Enter the IPv6 address. This is available only when IPv6 has been enabled on the unit.
Secondary IP Address	Optionally, enable and define secondary IP addresses. Administrative access can be enabled on secondary interfaces.
Administrative Access	

IPv4	If you have IPv4 addresses, select the permitted IPv4 administrative access types for this SSID.
IPv6	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. **Note:** 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 46.
Network	
Device Detection	Detect connected device type. Enabled by default.
WiFi Settings	
SSID	Enter a name for SSID. This is the name that is shown when the SSID is broadcast. By default, this field contains `fortinet`.
Client limit	Limit the number of clients allowed in the SSID.
Broadcast SSID	Enable or disable broadcast of SSID. By default, the SSID is broadcast.
Beacon advertising	Enable to advertise specified vendor specific elements over beacon frames containing information about the FortiAP name, model and serial number. This can be used to determine the coverage area of a FortiAP. • *Name* – The FortiAP name. • *Model* – The FortiAP model. • *Serial Number* – The FortiAP serial number. For more information, see Determining the coverage area of a FortiAP on page 415.
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 52.
Captive Portal	Select if you want to configure a Captive Portal to authenticate users through a customizable web page. For more information, see Captive Portal Security on page 72 Captive Portal is not supported for WPA/WPA2-Enterprise or WPA3-Enterprise Security modes.
Authentication	Available only when *Security Mode* is *WPA2-Enterprise* or *WPA3 Enterprise Only*. 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.
Pre-shared Key	Available only when *Security Mode* is *WPA2-Personal*.

	Select between *Single* or *Multiple* encryption key modes that clients must use. Setting multiple pre-shared keys will enable dynamic VLAN assignment.
Additional Settings	
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.
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 33.
Broadcast suppression	Enable and add broadcasts you want to suppress.
Quarantine host	Enable so you can quarantine clients connected to the SSID.
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 274.
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).
Comments	Enter a description or comment for the SSID.

3. Click *OK* to save.

To edit the settings of an existing SSID:

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

To configure a virtual access point (VAP)/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 and Switch Controller* > *SSIDs* 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 89.
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 DNS for local standalone NAT VAPs

For SSIDs in local standalone NAT mode, up to three DNS servers can be defined and assigned to wireless endpoints through DHCP. Wireless endpoints can then receive these DNS server IPs through DHCP when connecting to the SSID.

To configure the DNS servers:

In this example, an SSID (wifi.fap.01) is configured in local standalone mode with local standalone NAT enabled. Two DNS servers, 8.8.8.8 and 8.8.4.4, are specified.

```
config wireless-controller vap
   edit "wifi.fap.01"
      set ssid "wifi-ssid.fap.01"
      set passphrase **********
      set local-standalone enable
      set local-standalone-nat enable
      set local-standalone-dns enable
      set local-standalone-dns-ip 8.8.8.8 8.8.4.4
      set local-bridging enable
      set local-authentication enable
   next
end
```

You can check the configured DNS server with the following commands:

- On FortiGate:

  ```
  # diagnose wireless-controller wlac -c wlan wifi.fap.01
  ```

- On the managed FortiAP:

  ```
  FortiAP-431F # vcfg
  FortiAP-431F # dhcpconf
  ```

Changing SSID to VDOM only

You can change the wireless-controller VAP (for SSID configuration) from a global object to a VDOM object, simplifying tracking the object reference count. It also removes the `vdom` setting from VAP configuration. When multi-vdom is enabled on a FortiGate, the wireless-controller VAP can be added, edited, or deleted only inside of a VDOM.

To create a VAP entry:

- When `vdom-mode` is `no-vdom`:

```
# config wireless-controller vap
(vap) # edit new
    new entry 'new' added
(new) # set ssid new
(new) # set passphrase 12345678
(new) # set vdom
    command parse error before 'vdom'
(new) # end
# show wireless-controller vap new
    config wireless-controller vap
        edit "new"
            set ssid "new"
```

```
            set passphrase ENC ******
        next
    end
```

- When `vdom-mode` is `multi-vdom`:
  - A VAP cannot be created in global:

```
# config global
(global) # config wireless-controller vap
command parse error before 'vap'
Command fail. Return code 1
```

  - A VAP can be created in a VDOM:

```
# config vdom
(vdom) # edit vdom2
    current vf=vdom2:1
(vdom2) # config wireless-controller vap
(vap) # edit new
    new entry 'new' added
(new) # set ssid new
(new) # set passphrase 12345678
(new) # set vdom
    command parse error before 'vdom'
(new) # end
(vdom2) # sh wireless-controller vap new
    config wireless-controller vap
        edit "new"
            set ssid "new"
            set passphrase ENC ******
        next
    end
```

To check multi-vdom VAP entry authentication:

- When `vdom-mode` is `multi-vdom`, references to `user-group` and `radius` can be checked correctly when they are used by a VAP interface:
  - A VAP interface with security-mode set to WPA2-Enterprise and RADIUS authentication:

```
(vdom2) # show wireless-controller vap new
    config wireless-controller vap
        edit "new"
            set ssid "new"
            set security wpa2-only-enterprise
            set auth radius
            set radius-server "peap"
        next
    end
(vdom2) # diagnose sys cmdb refcnt show user.radius.name peap
    entry used by table wireless-controller.vap:name 'new'
```

  - A VAP interface with security-mode set to WPA2-Enterprise and User-group authentication:

```
(vdom2) # show wireless-controller vap new
    config wireless-controller vap
        edit "new"
            set ssid "new"
            set security wpa2-only-enterprise
```

```
            set auth usergroup
            set usergroup "group-radius"
        next
    end
(vdom2) # diagnose sys cmdb refcnt show user.group.name group-radius
    entry used by child table usergroup:name 'group-radius' of table wireless-
controller.vap:name 'new'
```

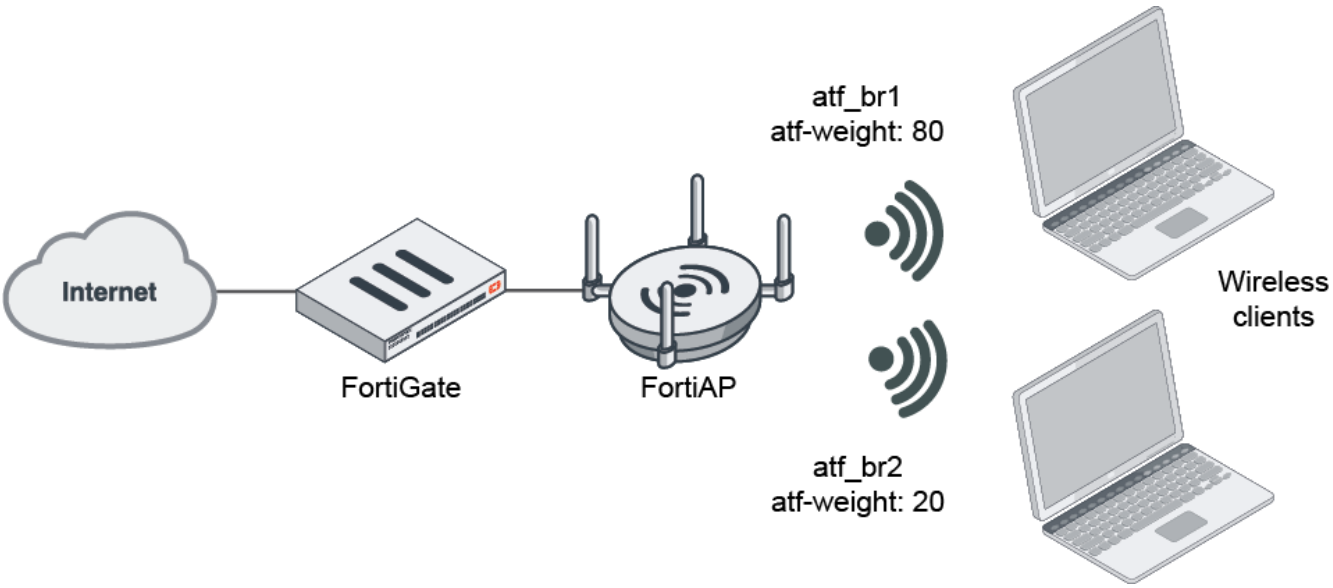
Airtime fairness

WiFi has a natural tendency for clients farther away or clients at lower data rates to monopolize the airtime and slow down overall performance. Airtime fairness helps to improve the overall network performance in these conditions.

Airtime fairness has the following characteristics:

- Only applies to downlink traffic.
- Can be set on both 2.4 GHz and 5 GHz radio bands.
- Can be set per-SSID. Each VAP is granted airtime according to the percentage assigned to the VAP.
- Can apply to all kinds of VAP (Bridge, Tunnel, or Mesh) and all kinds of authentication (Open, PSK, or Enterprise).
- Only applies to data and is not for control or management.

Airtime fairness is balanced from the TX side of the AP to the client since that's the only direction under the control of AP.



For example, there are two Bridge mode SSIDs with a wireless client and an airtime fairness weight of 80% and 20%. When traffic travels from the Ethernet to the wireless client, the traffic for each SSID matches the airtime fairness weight assigned to them.

Airtime fairness is not related to SSID type or authentication type. The following example uses Bridge mode SSID and Open Authentication security.

To set the airtime fairness weight in SSID - GUI:

To set airtime fairness weight from the GUI, you must enable Advanced Wireless Features viability (see Advanced Wireless Features on page 165).

1. Ensure Advanced Wireless Features is enabled.
2. Go to *WiFi and Switch Controller* > *SSIDs* and select the SSID you want to apply airtime fairness weight to.
3. Scroll down to *Advanced Settings*.
4. In *Airtime weight*, enter the weight you want.
5. When you are finished, click *OK*.

To set the airtime fairness weight in SSID - CLI:

The default `atf-weight` is 20 so there is no need to set this option for `atf_br2`.

```
config wireless-controller vap
    edit "atf_br1"
        set atf-weight 80
        set ssid "atf_br1"
        set security open
        set local-bridging enable
        set schedule "always"
    next
end

config wireless-controller vap
    edit "atf_br2"
        set ssid "atf_br2"
        set security open
        set local-bridging enable
        set schedule "always"
    next
end
```

To enable airtime fairness in radio:

This example uses one FAP-S423E unit with airtime fairness enabled on the 5 GHz radio band.

```
config wireless-controller wtp-profile
    edit "S423E_atf"
        config platform
            set type S423E
        end
        config radio-1
            set mode disabled
        end
        config radio-2
            set band 802.11ac
            set airtime-fairness enable
            set vap-all disable
            set vaps "atf_br1" "atf_br2"
            set channel "149"
        end
        set ext-info-enable enable
    next
end

config wireless-controller wtp
    edit "PS423E3X16000029"
        set admin enable
```

```
        set wtp-profile "S423E_atf"
        config radio-2
        end
    next
end
```

To verify the airtime fairness weight from FortiAP:

```
PS423E3X16000029 # cw_diag -c atf
Airtime Fairness Info:
 interface                              ssid  configured-atf     applied-atf
    Radio 0 ATF disabled
    Radio 1 ATF enabled
    wlan10                          atf_ssid1              80              80
    wlan11                          atf_ssid2              20              20

PS423E3X16000029 # wlanconfig wlan10 showatfinfo
                    SHOW  RADIO  ATF  TABLE
WLAN:SSID/Client(MAC Address)      Air time(%)    Config ATF(%%)   Assoc
 wlan10:atf_ssid1                       80.0            80.0
 wlan11:atf_ssid2                       20.0            20.0
 ------:Unallocated Airtime              0.0
```

Verify the airtime fairness weight from real traffic

When two similar clients connect with two SSIDs, downlink traffic is passed from Ethernet to the wireless client with the same bit rate.

This example shows that `tx_bytes` from `atf_br1` is almost four times higher than `atf_br2`.

To view traffic statistics from SSID1:

```
PS423E3X16000029 # cw_diag -d vap 90:6C:AC:8A:66:10
  VAP extension info
Radio 1 VAP 0:
    tx_packets                  : 60543
    tx_bytes                    : 70608777
    tx_data_packets             : 60543
    tx_data_bytes               : 70608777
    tx_datapyld_bytes           : 68308143
    tx_ucast_data_packets       : 57462
    tx_mbcast_data_packets      : 3081
    tx_discard                  : 94193
```

To view traffic statistics from SSID2:

```
PS423E3X16000029 # cw_diag -d vap 90:6C:AC:8A:66:11
  VAP extension info
Radio 1 VAP 1:
    tx_packets                  : 18839
    tx_bytes                    : 19731946
    tx_data_packets             : 18839
    tx_data_bytes               : 19731946
    tx_datapyld_bytes           : 19016064
    tx_ucast_data_packets       : 15760
```

```
tx_mbcast_data_packets       : 3079
tx_discard                   : 84924
```

Configuring security

You can secure access to your wireless network by configuring the following security modes on an SSID:

- Open — Unsecured.
- Wi-Fi Protected Access version 2 (WPA2), WPA2-Personal and WPA2-Enterprise
  - *WPA2-Personal* – WPA2 is WiFi Protected Access version 2. Users use a pre-shared key (password) to obtain access.
  - *WPA2-Enterprise* – similar to WPA2-Personal, but is best used for enterprise networks. Each user is separately authenticated by user name and password.
- WPA3 Security on page 59
  - 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)
- MPSK profiles on page 66 — Multiple pre-shared keys profile.
- Captive portal — Users connect 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.

You can also secure your network by:

- Adding a MAC filter
- Limiting the number of clients that can connect to an SSID
- Enabling multicast enhancement and IGMP Snooping
- Configuring WiFi with WSSO using Windows NPS and user groups on page 95
- Enabling Beacon Protection on page 101

WPA2 Security

WPA2 security with pre-shared keys (PSK) for authentication is called WPA2-Personal. This can work well for one person or a 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 Role-Based Access Control (RBAC) possible.

This section contains the following topics:

- Configuring WPA2-Personal security on page 53
- Configuring WPA2-Enterprise SSID on page 55

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:

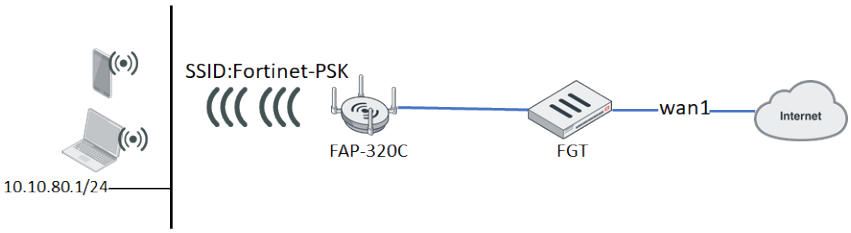
```
config wireless-controller vap
   edit example_wlan
      set security wpa-personal
      set passphrase "hardtoguess"
      set encrypt TKIP-AES
   end
```

Configuring WPA2-Personal security

WPA2-Personal security setup requires a pre-shared key (PSK) that you provide to clients. You can select between creating a single PSK or batch generating multiple pre-shared keys (MPSK). This section provides configuration instructions for deploying WPA2-Personal SSID with FortiAP. The steps include creating an SSID with a PSK, selecting the SSID for the FortiAP, and creating a policy from the SSID to the Internet.

For information on generating MPSKs, see MPSK profiles on page 66

The following shows a simple network topology:



To deploy WPA2-Personal SSID to FortiAP units - GUI:

1. Create a WPA2-Personal SSID:
   a. Go to *WiFi and Switch Controller* > *SSIDs*, select *SSID*, then click *Create New*.
   b. Enter the desired interface name. For *Traffic mode*, select *Tunnel*.
   c. In the *Address* > *IP/Network Mask* field, enter the IP address. *DHCP Server* is enabled by default. You can modify the DHCP IP address range manually.
   d. In the *SSID* field, enter the desired SSID name. For *Security*, select *WPA2 Personal*.
   e. In the *Pre-Shared Key* field, select *Single* as the pre-shared key mode.
   f. Enter the password. The password must be 8 to 63 characters long.
   g. Click *OK*.
2. Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C. Do one of the following:
   a. Select the SSID by editing the FortiAP:
      i. Go to *WiFi and Switch Controller* > *Managed FortiAPs*. Select the FortiAP-320C and click *Edit*.
      ii. Ensure that *Managed AP Status* is *Connected*.
      iii. Under *WiFi Setting*, ensure that the configured FortiAP profile is the desired profile, in this case FAP320C-default. Click *Edit entry*.
      iv. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1* > *SSIDs*. Select *Manual*, then click + to select the Fortinet-PSK SSID.

v. To broadcast the SSID from 5 G radio, scroll to *Radio 2* > *SSIDs*. Select *Manual*, then click + to select the Fortinet-PSK SSID.
vi. Click *OK*.

b. Select the SSID by editing the FortiAP profile:
i. Go to *WiFi and Switch Controller* > *FortiAP Profiles*. Select the FAP320C-default profile, then click *Edit*.
ii. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1* > *SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.
iii. To broadcast the SSID from 5 G radio, scroll to *Radio 2* > *SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.
iv. Click *OK*.

3. Create the SSID-to-Internet firewall policy:
a. Go to *Policy & Objects* > *Firewall Policy*, then click *Create New*.
b. Enter the desired policy name.
c. From the *Incoming Interface* dropdown list, select the source interface, such as wifi-vap.
d. From the *Outgoing Interface* dropdown list, select the destination interface, such as wan1.
e. In the *Source* and *Destination* fields, select all. In the *Service* field, select *ALL*. If desired, you can configure different values for these fields.
f. Click *OK*.

To deploy WPA2-Personal SSID to FortiAP units - CLI:

1. Create a WPA2-Personal SSID:
a. Create a VAP interface named "wifi-vap":

```
config wireless-controller vap
   edit "wifi-vap"
      set ssid "Fortinet-psk"
      set security wpa2-only-personal
      set passphrase "fortinet"
   next
end
```

b. Configure an IP address and enable DHCP:

```
config system interface
   edit "wifi-vap"
      set ip 10.10.80.1 255.255.255.0
   next
end
config system dhcp server
   edit 1
      set dns-service default
      set default-gateway 10.10.80.1
      set netmask 255.255.255.0
      set interface "wifi-vap"
      config ip-range
         edit 1
            set start-ip 10.10.80.2
            set end-ip 10.10.80.254
         next
      end
      set timezone-option default
   next
end
```

2. Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C:

```
config wireless-controller wtp
   edit "FP320C3X14000640"
      set admin enable
      set wtp-profile "FAP320C-default"
   next
end
config wireless-controller wtp-profile
   edit "FAP320C-default"
      config radio-1
         set vap-all disable
         set vaps "wifi-vap"
      end
      config radio-2
         set vap-all disable
         set vaps "wifi-vap"
      end
   next
end
```

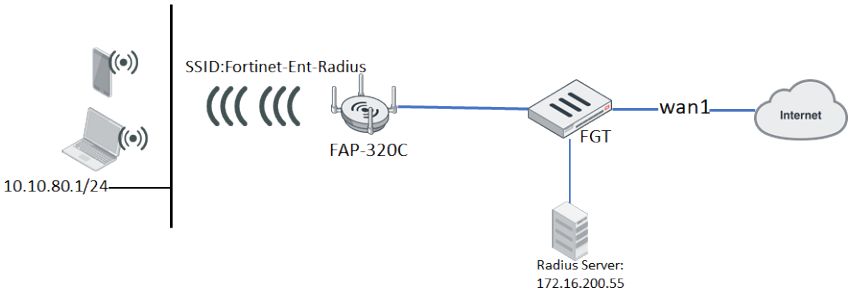
3. Create the SSID-to-Internet firewall policy:

```
config firewall policy
   edit 1
      set name "WiFi to Internet"
      set srcintf "wifi-vap"
      set dstintf "wan1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set fsso disable
      set nat enable
   next
end
```

Configuring WPA2-Enterprise SSID

This section provides configuration instructions for deploying WPA2-Enterprise SSID with FortiAP using either FortiOS user groups or a RADIUS server for authentication. Once you configure your authentication method, the remaining steps include creating an SSID, selecting the SSID for the FortiAP, and creating a policy from the SSID to the Internet.

The following shows the network topology using RADIUS server authentication:



For instructions on how to configure user authentication with locally stored FortiOS user groups, see Basic wireless network example on page 342. Note that authentication with local groups only supports PEAP, not EAP-TLS.

To configure WPA2-Enterprise SSID to FortiAP units with RADIUS server authentication - GUI:

1. Create a RADIUS server:
   a. Go to *User & Authentication* > *RADIUS Servers* and click *Create New*.
   b. Enter a *Name* for the server.
   c. Under *Primary Server*, enter the IP address or server name.
   d. In the *Secret* field, enter the secret key used to access the server.
   e. Click *Test Connectivity* to verify the connection with the RADIUS server.
   f. Click *Test User Credentials* to verify that the user account can be authenticated with the RADIUS server.
   g. Optionally, enter the information for a secondary or backup RADIUS server.
   h. Click *OK*.
2. Create a WPA2-Enterprise SSID:
   a. Go to *WiFi and Switch Controller* > *SSIDs* and click *Create New* > *SSID*.
   b. Enter the desired interface name. For *Traffic mode*, select *Tunnel*.
   c. In the *Address* > *IP/Network Mask* field, enter the IP address. *DHCP Server* is enabled by default. You can modify the DHCP IP address range manually.
   d. In the *SSID* field, enter the desired SSID name. For *Security*, select *WPA2 Enterprise*.
   e. In the *Authentication* field, select *RADIUS Server*. From the dropdown list, select the RADIUS server created in step 1.
   f. Click *OK*.

To configure WPA2-Enterprise SSID to FortiAP units with user group authentication - GUI:

1. Create a user group:
   a. Go to *User & Authentication* > *User Groups* and click *Create New*.
   b. Enter a group name.
   c. For *Type*, select *Firewall*.
   d. For *Remote Groups*, click the + button. In the dropdown list, select the desired RADIUS server. Click *OK*.
   e. Click *OK*.
2. Create a WPA2-Enterprise SSID:
   a. Go to *WiFi and Switch Controller* > *SSIDs* and click *Create New* > *SSID*..
   b. Enter an interface name. For *Traffic mode*, select *Tunnel*.
   c. In the *Address* > *IP/Network Mask* field, enter the IP address. *DHCP Server* is enabled by default. You can modify the DHCP IP address range manually.
   d. In the *SSID* field, enter the desired SSID name. For *Security*, select *WPA2 Enterprise*.
   e. In the *Authentication* field, select *Local*. From the dropdown list, select the user group(s) permitted to use the wireless network.
   f. Click *OK*.

To deploy WPA2-Enterprise SSID to FortiAP units - GUI:

Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C. Do one of the following:

1. Select the SSID by editing the FortiAP:
   a. Go to *WiFi & Switch Controller* > *Managed FortiAPs*. Select the FortiAP-320C and click *Edit*.
   b. Ensure that *Managed AP Status* is *Connected*.
   c. Under *WiFi Setting*, ensure that the configured FortiAP profile is the desired profile, in this case FAP320C-default. Click *Edit entry*.
   d. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1* > *SSIDs*. Select *Manual*, then click + to select the Fortinet-PSK SSID.
   e. To broadcast the SSID from 5 G radio, scroll to *Radio 2* > *SSIDs*. Select *Manual*, then click + to select the Fortinet-PSK SSID.
   f. Click *OK*.
2. Select the SSID by editing the FortiAP profile:
   a. Go to *WiFi & Switch Controller* > *FortiAP Profile*. Select the FAP320C-default profile, then click *Edit*.
   b. To broadcast the SSID from 2.4 G radio, scroll to *Radio 1* > *SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.
   c. To broadcast the SSID from 5 G radio, scroll to *Radio 2* > *SSIDs*. Select *Manual*, then click + to create the Fortinet-PSK SSID.
   d. Click *OK*.
3. Create the SSID-to-Internet firewall policy:
   a. Go to *Policy & Objects* > *Firewall Policy*, then click *Create New*.
   b. Enter the desired policy name.
   c. From the *Incoming Interface* dropdown list, select the source interface, such as wifi-vap.
   d. From the *Outgoing Interface* dropdown list, select the destination interface, such as wan1.
   e. In the *Source* and *Destination* fields, select all. In the *Service* field, select *ALL*. If desired, you can configure different values for these fields.
   f. Click *OK*.

To deploy WPA2-Enterprise SSID to FortiAP units - CLI:

1. Configure an authentication method (RADIUS server or user group):
   - Create a RADIUS server:
   ```
   config user radius
      edit "wifi-radius"
         set server "172.16.200.55"
         set secret fortinet
      next
   end
   ```
   - Create a user group:
   ```
   config user group
      edit "group-radius"
         set member "wifi-radius"
      next
   end
   ```
2. Create a WPA2-Enterprise SSID:
   - Create an SSID with authentication from the RADIUS server:
   ```
   config wireless-controller vap
      edit "wifi-vap"
         set ssid "Fortinet-Ent-Radius"
         set security wpa2-only-enterprise
         set auth radius
         set radius-server "wifi-radius"
   ```

```
      next
    end
```

- Create an SSID with authentication from the user group:

```
config wireless-controller vap
   edit "wifi-vap"
      set ssid "Fortinet-Ent-Radius"
      set security wpa2-only-enterprise
      set auth usergroup
      set usergroup "group-radius"
   next
end
```

a. Configure an IP address and enable DHCP:

```
config system interface
   edit "wifi-vap"
      set ip 10.10.80.1 255.255.255.0
   next
end
config system dhcp server
   edit 1
      set dns-service default
      set default-gateway 10.10.80.1
      set netmask 255.255.255.0
      set interface "wifi-vap"
      config ip-range
         edit 1
            set start-ip 10.10.80.2
            set end-ip 10.10.80.254
         next
      end
      set timezone-option default
   next
end
```

3. Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-320C and a "FAP320C-default" profile that is applied to the FortiAP-320C:

```
config wireless-controller wtp
   edit "FP320C3X14000640"
      set admin enable
      set wtp-profile "FAP320C-default"
   next
end
config wireless-controller wtp-profile
   edit "FAP320C-default"
      config radio-1
         set vap-all disable
         set vaps "wifi-vap"
      end
      config radio-2
         set vap-all disable
         set vaps "wifi-vap"
      end
   next
end
```

4. Create the SSID-to-Internet firewall policy:

```
config firewall policy
   edit 1
      set name "WiFi to Internet"
```

```
        set srcintf "wifi-vap"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set fsso disable
        set nat enable
    next
end
```

WPA3 Security

For full WPA3 support, we recommend you update your FortiGate and FortiAP devices to the latest supported firmware version.

- FortiGate devices running FortiOS 7.0.0 and later.
- FortiAP devices running 6.4.3 and later.
- FortiAP-S and FortiAP-W2 devices running 6.4.3 and later.
- FortiAP-U devices running 6.2.2 and later.

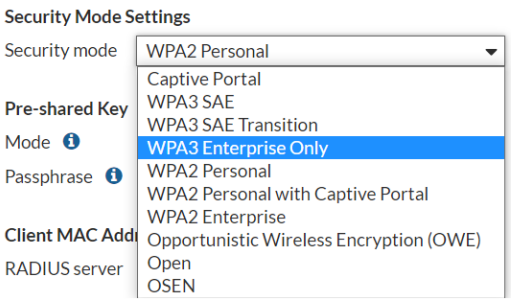
For more precise support information between FortiGate and FortiAP firmware versions, see each model's release notes.

You can configure the following WPA3 security modes:

- WPA3 Enterprise 192-bit
- WPA3 Enterprise Only
- WPA3 Enterprise Transition
- WPA3 Simultaneous Authentication of Equals (SAE)
- WPA3 SAE Transition
- Opportunistic Wireless Encryption (OWE)
- OWE Transition

To configure WPA3 on an SSID - GUI:

1. Go to *WiFi Controller* > *SSID*.
2. Create a new SSID, or edit a current one.
3. In the *WiFi Settings* section, set the *Security Mode* to a WPA3 option.



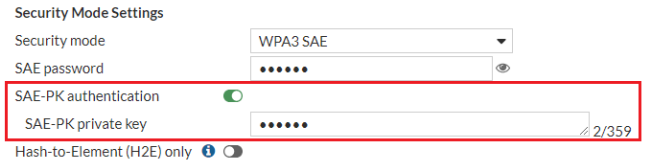
4. Configure the relevant security settings as needed.

If you set the security mode to either *WPA3-SAE* or *WPA3-SAE-Transition*, you can enable Hash-to-Element (H2E) only or Simultaneous Authentication of Equals Public Key (SAE-PK).

- *H2E only*: Use hash-to-element-only mechanism for PWE derivation.

- *SAE-PK*: Enable or disable WPA3 SAE-PK.

  When SAE-PK authentication option is enabled, the SAE-PK private key is mandatory. The private key can be generated by FortiOS (for information on how to generate the SAE-PK password and private key, see Generating SAE-PK private key and password on page 64) or through a third-party tool. FortiOS will verify the private key and reject invalid input.



5. Click *OK*.

Configuring WPA3 OWE - CLI

To configure WPA3 OWE only:

Clients that support WPA3 can connect with this SSID.

```
config wireless-controller vap
    edit "80e_owe"
        set ssid "80e_owe"
        set security owe
        set pmf enable
        set schedule "always"
    next
end
```

To configure WPA3 OWE Transition:

Clients connect with normal OPEN or OWE depending on its capability. Clients which support WPA3 connect with OWS standard. Clients which cannot support WPA3 connect with Open SSID.

```
config wireless-controller vap
    edit "80e_open"
        set ssid "80e_open"
        set security open
        set owe-transition enable
        set owe-transition-ssid "wpa3_open"
        set schedule "always"
    next
    edit "wpa3_owe_tr"
        set ssid "wpa3_open"
        set broadcast-ssid disable
```

```
        set security owe
        set pmf enable
        set owe-transition enable
        set owe-transition-ssid "80e_open"
        set schedule "always"
    next
end
```

Configuring WPA3 SAE - CLI

To configure WPA3 SAE:

Clients that support WPA3 can connect with this SSID.

```
config wireless-controller vap
    edit "80e_sae"
        set ssid "80e_sae"
        set security wpa3-sae
        set pmf enable
        set schedule "always"
        set sae-password ********
    next
end
```

To configure WPA3 SAE Transition:

There are two passwords in the SSID. If *passphrase* is used, the client connects with WPA2 PSK. If *sae-password* is used, the client connects with WPA3 SAE.

```
config wireless-controller vap
    edit "80e_sae-tr"
        set ssid "80e_sae-transition"
        set security wpa3-sae-transition
        set pmf optional
        set passphrase ********
        set schedule "always"
        set sae-password ********
    next
end
```

To configure WPA3 SAE and enable H2E only:

```
config wireless-controller vap
  edit "wifi"
    set ssid "Example_SSID"
    set security wpa3-sae
    set pmf enable
    set sae-h2e-only enable
    set schedule "always"
    set sae-password ENC *
  next
end
```

To configure WPA3 SAE and enable SAE-PK:

```
config wireless-controller vap
  edit "wifi"
    set ssid "Example_SSID"
    set security wpa3-sae
    set pmf enable
    set sae-pk enable
    set sae-private-key "*******"
    set sae-password ENC *
    set schedule "always"
  next
end
```

Note: The private key can be generated by FortiOS (see Generating SAE-PK private key and password on page 64) or through a third-party tool. FortiOS will verify the private key and reject invalid input.

Configuring WPA3 Enterprise - CLI

When using the following WPA3 Enterprise options, you can select the `auth` type to use either RADIUS authentication or local user authentication. When using RADIUS authentication, you can enable accounting interim updates to integrate with Cisco's Identity Services Engine (ISE).

To configure WPA3 Enterprise 192-bit:

By default, this option is not show in the GUI. When you configure this SSID from the CLI, the GUI will list the security option as *WPA3 Enterprise 192-bit*.

Using this option, you can set the security mode to `wpa3-enterprise` to use 192-bit encryption with PMF mandatory.

```
config wireless-controller vap
    edit "80e_wpa3"
        set ssid "80e_wpa3"
        set security wpa3-enterprise
        set pmf enable
        set auth radius
        set radius-server "wifi-radius"
        set schedule "always"
    next
    edit "80e_wpa3_user"
        set ssid "80e_wpa3_user"
        set security wpa3-enterprise
        set pmf enable
        set auth usergroup
        set usergroup "usergroup"
        set schedule "always"
    next
end
```

To configure WPA3 Enterprise Only:

Using this option, you can set the security mode to `wpa3-only-enterprise` to use WPA3 Enterprise with PMF mandatory.

```
config wireless-controller vap
  edit "wpa3"
    set ssid "wpa3"
    set security wpa3-only-enterprise
    set pmf enable
    set auth radius
    set radius-server "FAC"
    set schedule "always"
  next
end
```

To configure WPA3 Enterprise Transition:

Using this option, you can set the security mode to `wpa3-enterprise-transition` to use WPA3 Enterprise with PMF optional. A WPA3-Enterprise STA shall negotiate PMF when associating with an AP using WPA3-Enterprise transition mode.

```
config wireless-controller vap
  edit "wpa3"
    set ssid "wpa3"
    set security wpa3-enterprise-transition
    set pmf optional
    set auth radius
    set radius-server "FAC"
    set schedule "always"
  next
end
```

To configure WPA3 Enterprise SSID to integrate with Cisco ISE:

Enable accounting interim updates to integrate with Cisco's ISE session stitching feature. When a wireless client roams between FortiAPs, the FortiGate creates an "Interim-Update" accounting message with the same "Acct-Session-Id" value to avoid interrupting the ISE session.

1. Create a RADIUS server with an accounting server:

```
config user radius
  edit "peap"
    set server "172.18.56.104"
      set secret ENC
      set nas-ip 192.168.1.10
      set nas-id-type custom
      set nas-id "FWF-61F-AUTH"
      set acct-interim-interval 300
      set radius-coa enable
      set password-renewal disable
      config accounting-server
        edit 1
          set status enable
          set server "172.18.56.104"
          set secret ENC
```

```
      next
    end
  next
end
```

2. Create a WPA3 Enterprise SSID with the authentication method set to `radius` and the radius server set to the example you previously configured (`peap`).

```
config wireless-controller vap
  edit "wifi4"
    set ssid "FOS_61F_ENT"
    set security wpa3-only-enterprise
    set auth radius
    set radius-server "peap"
    set schedule "always"
  next
end
```

3. Enable `roaming-acct-interim-update`.

```
config wireless-controller vap
  edit "wifi4"
    set ssid "FOS_61F_ENT"
    set security wpa3-only-enterprise
    set auth radius
    set radius-server "peap"
    set schedule "always"
    set roaming-acct-interim-update enable
  next
end
```

4. Apply this SSID to the FortiAPs you want to roam between.

`roaming-acct-interim-update` can only be enabled when the security mode is set to a WPA2 or WPA3 Enterprise type.

Generating SAE-PK private key and password

You can use FortiOS to generate an SAE-PK private key and password in for SAE-PK authentication and WPA3 Security configuration with the following CLI command:

```
execute wireless-controller create-sae-pk [SSID] [curve:prime256v1|secp384r1|secp521r1]
```

Once the private key and password are generated, you can then apply them to an SSID with the security mode set to a WPA3-SAE option and SAE-PK authentication enabled.

To generate a SAE private key and password - CLI:

1. Use the SAE-PK generation command to create a SAE-PK Private Key and password. In this example, the SSID is "*Example_wpa3_sae_pk*" with the curve set to *prime256v1*.

```
execute wireless-controller create-sae-pk Example_wpa3_sae_pk prime256v1
```

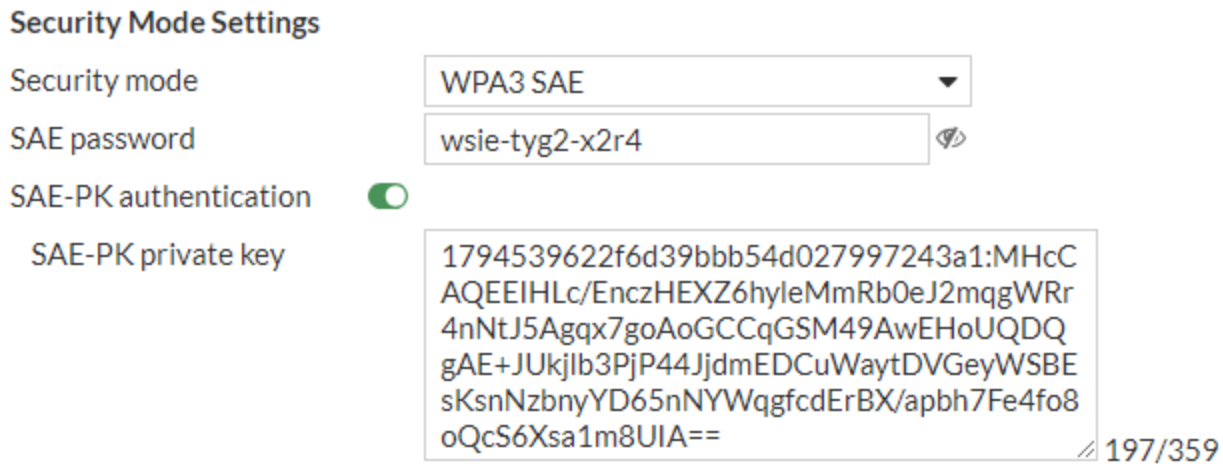
2. The command runs and displays the following:

```
sae_pk_gen ssid Example_wpa3_sae_pk sec 3 curve prime256v1:

Searching for a suitable Modifier M value
12.98%Found a valid hash in 2178339 iterations:
000000692087836 9f515848ab8d3047dc106a231c7ddd19e86ea1f2435d31f26
PasswordBase binary data for base32:
b49049e0dabea2b848abc69829f7048d4469c7dde8cf49ba87e486bd31# SAE-PK password/M/private
key for Sec=3.
sae_password=wsie-tyg2-x2r4
pk
=1794539622f6d39bbb54d027997243a1:MHcCAQEEIHLc/EnczHEXZ6hyleMmRb0eJ2mqgWRr4nNtJ5Agqx7goA
oGCCqGSM49AwEHoUQDQgAE+JUkjlb3PjP44JjdmEDCuWaytDVGeyWSBEsKsnNzbnyYD65nNYWqgfcdErBX/apbh7
Fe4fo8oQcS6Xsa1m8UIA==
# Longer passwords can be used for improved security at the cost of usability:
# wsie-tyg2-x2rl-qsfs
# wsie-tyg2-x2rl-qsfl-y2mr
# wsie-tyg2-x2rl-qsfl-y2mc-t5yi
# wsie-tyg2-x2rl-qsfl-y2mc-t5ye-rvc6
# wsie-tyg2-x2rl-qsfl-y2mc-t5ye-rvcg-tr6e
# wsie-tyg2-x2rl-qsfl-y2mc-t5ye-rvcg-tr65-5dhj
# wsie-tyg2-x2rl-qsfl-y2mc-t5ye-rvcg-tr65-5dhu-touh
# wsie-tyg2-x2rl-qsfl-y2mc-t5ye-rvcg-tr65-5dhu-touh-4sdz
# wsie-tyg2-x2rl-qsfl-y2mc-t5ye-rvcg-tr65-5dhu-touh-4sdl-2mpz
```

3. Copy the *sae-password* and *pk* values.
   - *sae-password* is the SAE Password. You can also copy one of the longer passwords instead for improved security.
   - *pk* is the SAE Private Key.

To apply the generated SAE private key and password to an SSID - GUI:

1. Go to *WiFi Controller* > *SSID* and select the SSID you want to apply the SAE-PK to.
2. In the *WiFi Settings* section, set the *Security Mode* to a WPA3 option.
3. In *SAE password*, paste the *sae_password* value you previously generated.
4. Enable *SAE-PK authentication*.
5. In *SAE-PK private key*, paste the *pk* value you previously generated.



6. When you are finished, click *OK*.

To apply the generated SAE private key and password to an SSID - CLI:

1. From the FortiOS CLI, go to the SSID you want to configure and enter the SAE-PK Private Key and Password values you copied:

```
config wireless-controller vap
  edit "wpa3-test"
    set ssid "Example_wpa3_sae_pk"
    set security wpa3-sae
    set sae-pk enable
    set sae-private-key
"1794539622f6d39bbb54d027997243a1:MHcCAQEEIHLc/EnczHEXZ6hyleMmRb0eJ2mqgWRr4nNtJ5Agqx7goA
oGCCqGSM49AwEHoUQDQgAE+JUkjlb3PjP44JjdmEDCuWaytDVGeyWSBEsKsnNzbnyYD65nNYWqgfcdErBX/apbh7
Fe4fo8oQcS6Xsa1m8UIA=="
    set sae-password wsie-tyg2-x2r4
  next
end
```

2. After applying the SSID to a FortiAP, confirm the WiFi station can connect.

```
diagnose wireless-controller wlac -d sta online
   vf=0 mpId=0 wtp=3 rId=2 wlan=wpa3-test vlan_id=0 ip=0.0.0.0 ip6=::
mac=f8:e4:e3:d8:5e:af vci= host= user= group= signal=-9 noise=-89 idle=1 bw=0 use=3
chan=161 radio_type=11AC(wave2) security=wpa3_sae mpsk= encrypt=aes cp_authed=no l3r=1,0
G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

MPSK profiles

You can batch generate or import multiple pre-shared keys (MPSK), export MPSK keys to a CSV file, dynamically assign VLANs based on used MPSK, and apply an MPSK schedule in the GUI. MPSK related configurations are managed from the MPSK profile, which is available when you enable Advanced Wireless Features (see Advanced Wireless Features on page 165). MPSK profiles support WPA2-Personal, WPA3-SAE and WPA3-SAE Transition security modes.

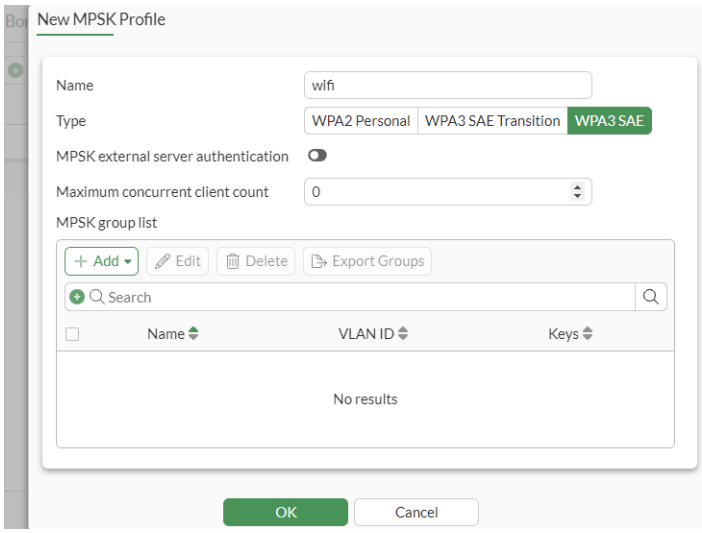
In the GUI, MPSK key entries are organized in different MPSK groups. An MPSK group can be created manually or imported. When MPSK is enabled, the previous single passphrase is dropped and a dynamic VLAN is automatically enabled.

In the CLI, an `mpsk-profile` is assigned in the VAP settings and MPSK is enabled. The dynamic VLAN is automatically enabled. Only one MPSK profile can be assigned to one VAP at a time.

To configure an MPSK profile - GUI:

1. Go to *System* > *Feature Visibility* and enable *Advanced Wireless Features*.
2. Click *Apply*.
3. Go to *WiFi & Switch Controller* > *Connectivity Profiles* > *MPSK Profiles* and click *Create new* to create an MPSK profile.

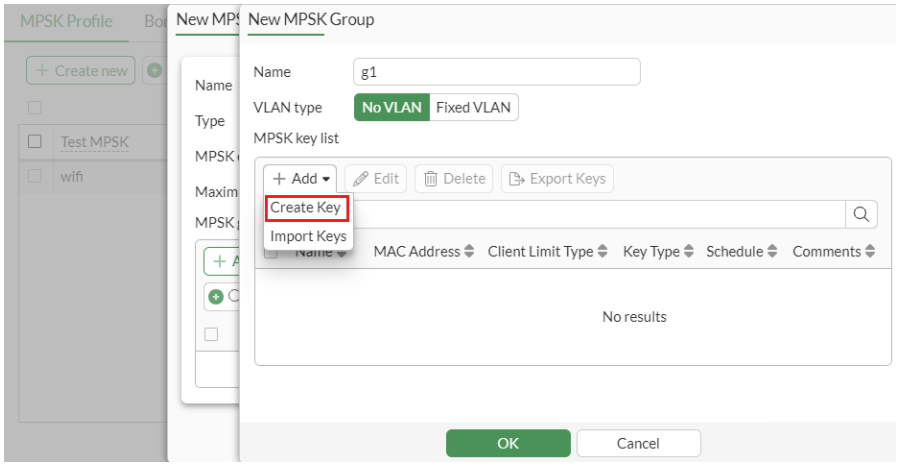
   The New MPSK Profile window loads.
4. Enter an MPSK profile *Name* and select a security *Type*.



5. Under *MPSK group list*, click *Add* > *Create Group* to create a new MPSK Group.

   The New MPSK Group window loads.

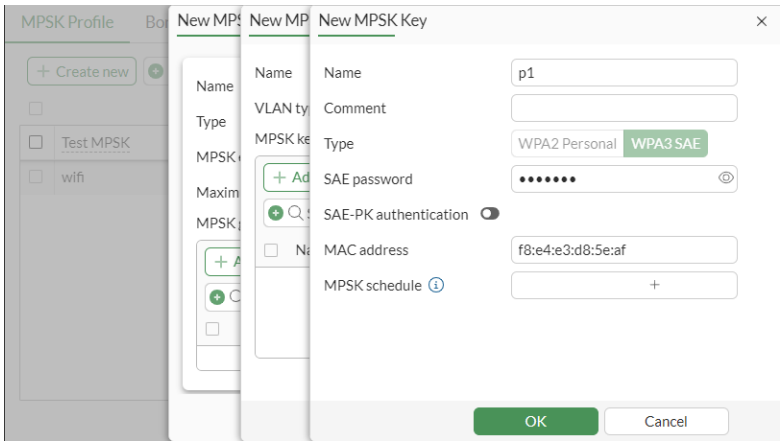
6. In the New MPSK Group window, enter an MPSK Group *Name* and click *Add* > *Create Key* to add a new key.



   The New MPSK Key window loads.

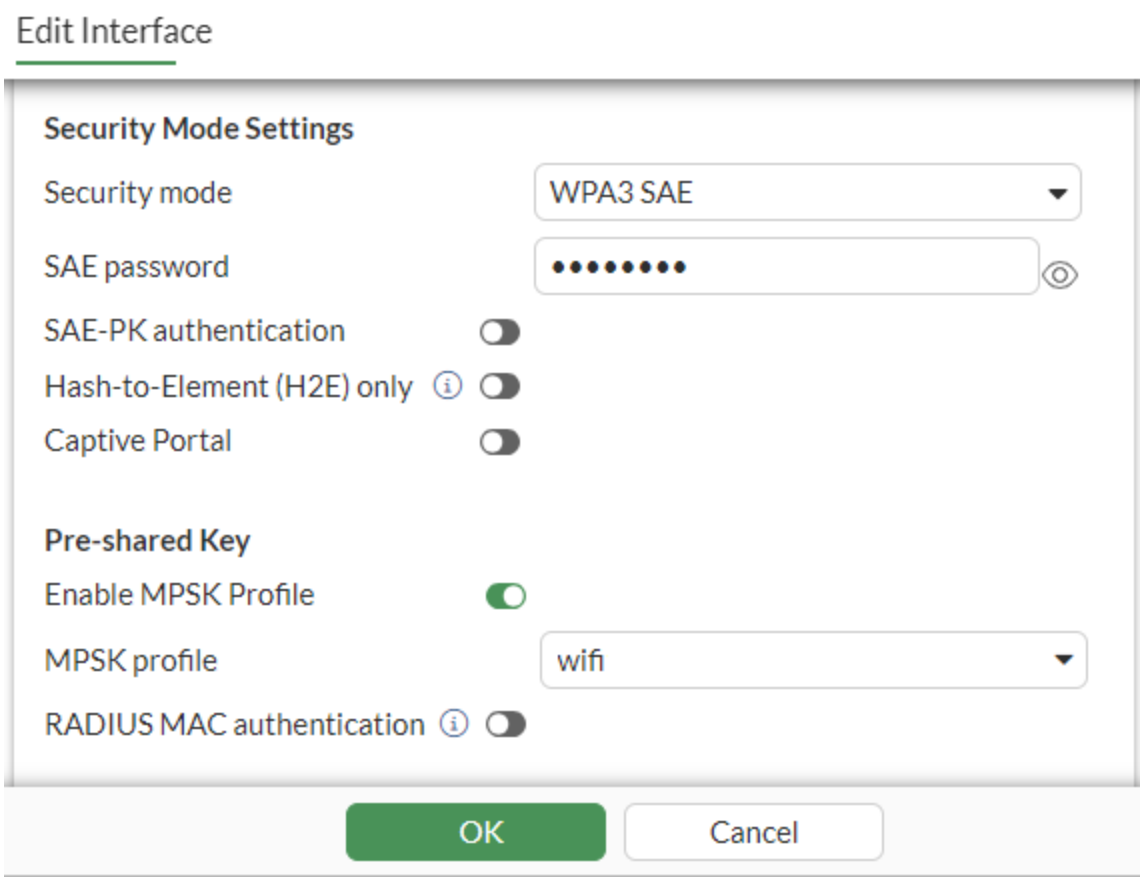
   - If you selected WPA3 SAE or WPA2 Personal as your MPSK Profile security type, the *Type* is automatically set.
   - If you selected WPA3 SAE Transition, you can choose between *WPA2 Personal* or *WPA3 SAE* as the MPSK Key security type.

7. In the New MPSK Key window, enter an MPSK Key *Name, SAE password* or *Pre-shared key*, and *MAC address*.



Note: If you selected WPA3-SAE Transition, you can create multiple MPSK keys with WPA2 Personal and WPA3 SAE security types.

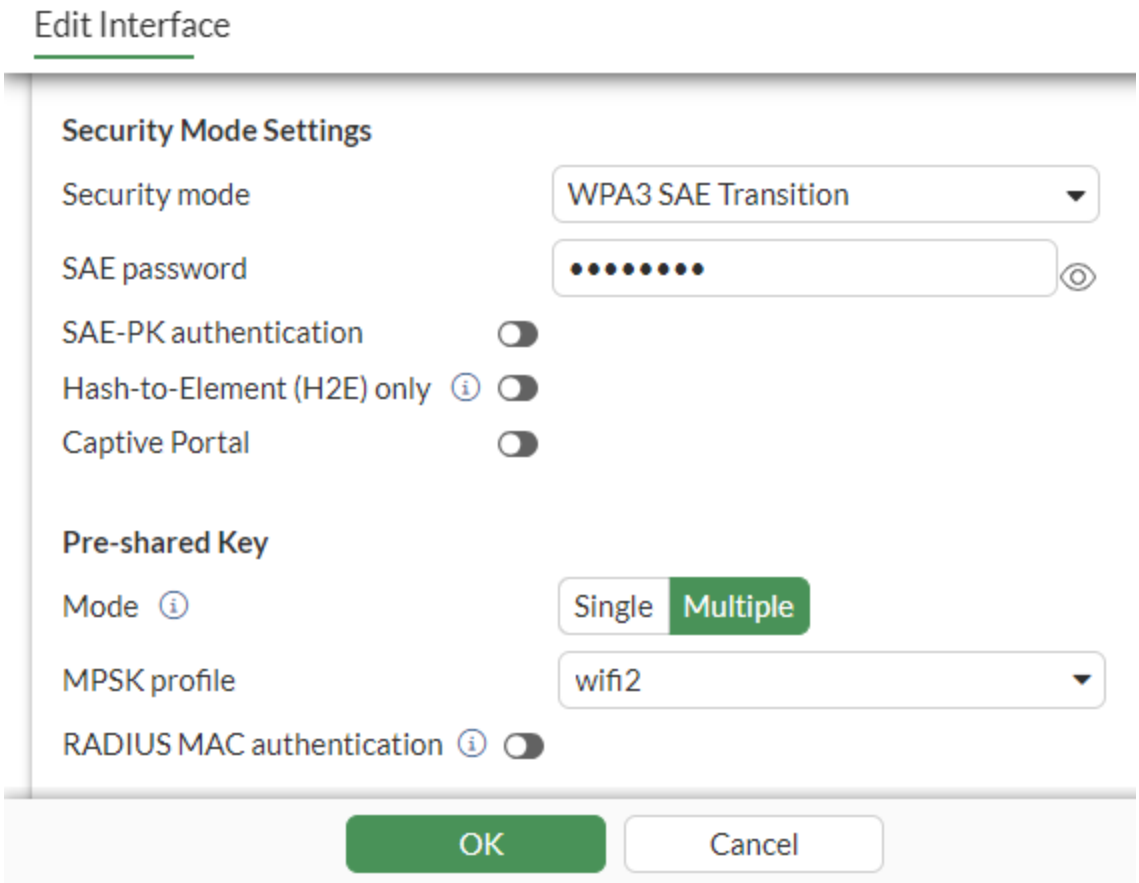
8. When you are finished, click *OK* to save your MPSK profile configurations.
9. Go to *WiFi & Switch Controller* > *SSIDs* and select or create a new SSID.
10. Under *Security Mode Settings*, select the *Security mode* and *SAE password* that matches your MPSK profile.
    a. If your security mode is WPA3 SAE:
        i. Under *Pre-shared Key*, enable *MPSK Profile* and then select the WPA3 SAE MPSK profile you configured.



b. If your security mode is WPA3 SAE Transition or or WPA2 Personal:

i. In *Mode*, select *Multiple*.

ii. the *MPSK profile*, select the WPA3 SAE Transition or WPA2 Personal MPSK profile you configured.



11. When you are finished, click *OK*.

To configure an MPSK profile with WPA3 SAE security mode - CLI:

1. Create an MPSK profile with WPA3 SAE security mode:

```
config wireless-controller mpsk-profile
  edit "wifi"
    set mpsk-type wpa3-sae
    config mpsk-group
      edit "g1"
        config mpsk-key
          edit "p1"
            set key-type wpa3-sae
            set mac f8:e4:e3:d8:5e:af
            set sae-password ENC
          next
        end
      next
    end
```

```
  next
end
```

2. Apply the MPSK profile to a VAP with the security mode also set to WPA3 SAE:

```
config wireless-controller vap
  edit "wifi"
    set ssid "FOS_81F_WPA3_MPSK"
    set security wpa3-sae
    set pmf enable
    set schedule "always"
    set mpsk-profile "wifi"
    set dynamic-vlan enable
    set sae-password ENC
  next
end
```

To configure an MPSK profile with WPA3 SAE Transition security mode - CLI:

1. Create an MPSK profile with WPA3 SAE Transition security mode:

```
config wireless-controller mpsk-profile
  edit "wifi2"
    set mpsk-type wpa3-sae-transition
    config mpsk-group
      edit "g1"
        config mpsk-key
          edit "p1"
            set key-type wpa2-personal
            set passphrase  *
          next
          edit "p2"
            set key-type wpa3-sae
            set mac f8:e4:e3:d8:5e:af
            set sae-password *
          next
        end
      next
    end
  next
end
```

2. Apply the MPSK profile to a VAP with the security mode also set to WPA3 SAE:

```
config wireless-controller vap
  edit "wifi2"
    set ssid "FOS_81F_WPA3_Transition"
    set security wpa3-sae-transition
    set pmf optional
    set schedule "always"
    set mpsk-profile "wifi2"
    set dynamic-vlan enable
    set sae-password ENC
  next
end
```

To configure an MPSK profile with WPA2 Personal security mode - CLI:

1. Configure the MPSK profile from the GUI or CLI.

```
config wireless-controller mpsk-profile
  edit "wifi-mpsk"
    config mpsk-group
      edit "group-a"
        set vlan-type fixed-vlan
        set vlan-id 10
        config mpsk-key
          edit "key-a-1"
            set passphrase ENC
            set mpsk-schedules "always"
          next
        end
      next
      edit "group-b"
        set vlan-type fixed-vlan
        set vlan-id 20
        config mpsk-key
          edit "key-b-1"
            set passphrase ENC
            set concurrent-client-limit-type unlimited
            set mpsk-schedules "always"
          next
        end
      next
    end
  next
end
```

2. Apply the MPSK profile to a VAP with the security mode also set to WPA2 Personal:

```
config wireless-controller vap
   edit "wifi-mpsk"
      set ssid "wifi-mpsk"
      set local-bridging enable
      set schedule "always"
      set mpsk-profile "wifi-mpsk"
      set dynamic-vlan enable
   next
end
```

3. Verify the event log after the WiFi client is connected:

```
1: date=2020-07-10 time=16:57:20 logid="0104043573" type="event" subtype="wireless"
level="notice" vd="root" eventtime=1594425440439070726 tz="-0700" logdesc="Wireless
client authenticated" sn="FP423E3X16000320" ap="FP423E3X16000320" vap="wifi-mpsk"
ssid="wifi-mpsk" radioid=2 user="N/A" group="N/A" stamac="3c:2e:ff:83:91:33"
srcip=10.0.10.2 channel=144 radioband="802.11ac" signal=-52 snr=50 security="WPA2
Personal" encryption="AES" action="client-authentication" reason="Reserved 0"
mpsk="key-a-1" msg="Client 3c:2e:ff:83:91:33 authenticated."
```

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 on an external authentication server.

This section includes the following topics:

- Captive portal types on page 72
- Configuring a FortiGate captive portal on page 73
- Configuring an external captive portal on page 76
- Configuring MAC Bypass for captive portal on page 78

Captive portal types

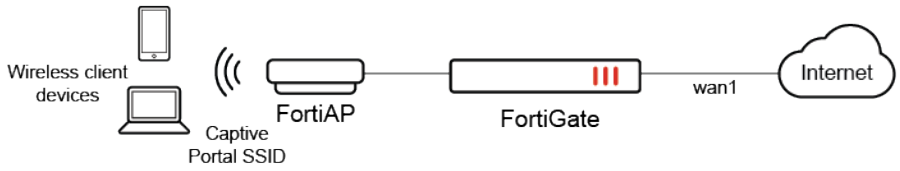
The WiFi captive portal types are available depending on your SSID traffic mode:

Name	Description	Traffic Mode
Available in the GUI and CLI		
Authentication	Until the user enters valid credentials, no communication beyond the AP is permitted.	Tunnel Bridge
Disclaimer + Authentication	Immediately after successful authentication, the portal presents the disclaimer page—an acceptable use policy or other legal statement—to which the user must agree before proceeding.	Tunnel
Disclaimer Only	The portal presents the disclaimer page—an acceptable use policy or other legal statement—to which the user must agree before proceeding. The authentication page is not presented.	Tunnel
Email Collection	The portal presents a page requesting the user's email address, for the purpose of contacting the person in future. This is often used by businesses who provide free WiFi access to their customers. The authentication page is not presented. To enable Email Collection, go to *System* > *Feature Visibility*, and enable *Email Collection*, then select *Email Collection* for *Portal Type*.	Tunnel
Available in CLI only		
`cmcc`	Set the portal type to CMCC.	Bridge
`cmcc-macauth`	Set the portal type to CMCC and MAC authentication.	Bridge
`auth-mac`	When clients are authenticated and their MAC addresses are known, they are redirected to the external captive portal.	Tunnel
`external-auth`	Clients are directed to an external captive portal for authentication.	Bridge
`external-macauth`	Clients are directed to an external portal for MAC authentication.	Bridge

Configuring a FortiGate captive portal

The built-in FortiGate captive portal is simpler than an external portal. To configure a captive portal, you need to create an SSID, apply the SSID to the FortiAP, and create a policy from the SSID to the Internet.

The following shows a simple network topology for this recipe:



To configure a WiFi Captive Portal - GUI:

1. Create a local user:
   a. Go to *User & Authentication* > *User Definition*, then click *Create New*.
   b. In the *Users/Groups Creation Wizard,* select *Local User*, then click *Next*.
   c. Enter the desired values in the *Username* and *Password* fields, then click *Next*.
   d. On the *Contact Info* tab, fill in any information as desired, then click *Next.* You do not need to configure any contact information for the user.
   e. On the *Extra Info* tab, set the *User Account Status* to *Enabled*.
   f. If the desired user group already exists, enable *User Group*, then select the desired user group.
   g. Click *Submit*.
2. Create a user group:
   a. Go to *User & Authentication* > *User Definition*, then click *Create New*.
   b. Enter the desired group name.
   c. For *Type*, select *Firewall*.
   d. For *Members*, click the + button. In the dropdown list, select the local user you created in step 1 and click *OK*.
   e. Click *OK*.
3. Create a captive portal SSID:
   a. Go to *WiFi and Switch Controller* > *SSIDs*, click *Create New* and select *SSID*.
   b. Enter the desired interface name. For *Traffic mode*, select *Tunnel*.
   c. In the *Address* > *IP/Network Mask* field, enter the IP address. *DHCP Server* is enabled by default. You can modify the DHCP IP address range manually.
   d. In the *SSID* field, enter the desired SSID name.
   e. For *Security mode*, select a Security mode.

Captive Portal is not supported for WPA/WPA2-Enterprise or WPA3-Enterprise Security modes.

f. Enable *Captive Portal* and configure the following:

Portal type	Configure a captive portal type: • *Authentication* • *Disclaimer + Authentication* • *Disclaimer Only* • *Email Collection* To enable Email Collection, go to *System* > *Feature Visibility*, and enable *Email Collection*, then select *Email Collection* for *Portal Type*. For information about each portal type, see Captive portal types on page 72.
Authentication portal	Configure the location of the portal: • *Local* - the portal is hosted on the FortiGate unit. • *External* - enter FQDN or IP address of an external portal.
User groups	Select permitted user groups or select *Use Groups from Policies*, which permits the groups specified in the security policy.
Exempt sources	Select exempt lists whose members will not be subject to captive portal authentication.
Exempt destinations/services	Select destinations and services lists whose members will not be subject to captive portal authentication.
Redirect after Captive Portal	Select whether to have authenticated users navigate to their originally requested URL or be redirected to a specific URL.

g. Click *OK*.

4. Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-221E and a "FAP221E-default" profile that is applied to the FortiAP-221E. Do one of the following:
   a. Select the SSID by editing the FortiAP:
      i. Go to *WiFi and Switch Controller* > *Managed FortiAPs*. Select the FortiAP-221E and click *Edit*.
      ii. Ensure that *Managed AP Status* is *Connected*.
      iii. Under *Wireless Settings*, ensure that the configured FortiAP profile is the desired profile, in this case FAP221E-default. Click *Edit entry*.
      iv. To broadcast the SSID from the 2.4 G radio, scroll to *Radio 1* > *SSIDs*. Select *Manual*, then click + to select the captive portal SSID you created.
      v. To broadcast the SSID from the 5 G radio, scroll to *Radio 2* > *SSIDs*. Select *Manual*, then click + to select the captive portal SSID you created.
      vi. Click *OK*.
   b. Select the SSID by editing the FortiAP profile:
      i. Go to *WiFi and Switch Controller* > *FortiAP Profiles*. Select the FAP221E-default profile, then click *Edit*.
      ii. To broadcast the SSID from the 2.4 G radio, scroll to *Radio 1* > *SSIDs*. Select *Manual*, then click + to select the captive portal SSID you created.
      iii. To broadcast the SSID from the 5 G radio, scroll to *Radio 2* > *SSIDs*. Select *Manual*, then click + to select the captive portal SSID you created.
      iv. Click *OK*.

5. Create the SSID-to-Internet firewall policy:
   a. Go to *Policy & Objects* > *Firewall Policy*, then click *Create New*.
   b. Enter the desired policy name.
   c. From the *Incoming Interface* dropdown list, select the source interface, such as wifi-vap.
   d. From the *Outgoing Interface* dropdown list, select the destination interface, such as wan1.
   e. In the *Source* and *Destination* fields, select all. In the *Service* field, select *ALL*. If desired, you can configure different values for these fields.
   f. Click *OK*.

To deploy captive portal SSID to FortiAP units - CLI:

1. Create a local user:
```
config user local
   edit "local"
      set type password
      set passwd ***
   next
end
```
2. Create a user group:
```
config user group
   edit "group-local"
      set member "local"
   next
end
```
3. Create a captive portal SSID. You can assign the following `portal-type`:
```
config wireless-controller vap
  edit "wifi-vap"
    set ssid "Fortinet-Captive"
    set security wpa3-sae
    set captive-portal enable
    set portal-type {auth | auth+disclaimer | disclaimer | email-collect}
    set selected-usergroups "group-local"
  next
end
```
4. Configure an IP address and enable DHCP:
```
config system interface
   edit "wifi-vap"
      set ip 10.10.80.1 255.255.255.0
   next
end
config system dhcp server
   edit 1
      set dns-service default
      set default-gateway 10.10.80.1
      set netmask 255.255.255.0
      set interface "wifi-vap"
      config ip-range
         edit 1
            set start-ip 10.10.80.2
            set end-ip 10.10.80.254
         next
      end
      set timezone-option default
```

```
    next
  end
```

5. Select the SSID on a managed FortiAP. The following configuration is based on a example using a managed FortiAP-221E and a "FAP221E-default" profile that is applied to the FortiAP-221E:

```
config wireless-controller wtp
  edit "FP221E3X14000640"
    set admin enable
    set wtp-profile "FAP221E-default"
  next
end
config wireless-controller wtp-profile
  edit "FAP221E-default"
    config radio-1
      set vap-all manual
      set vaps "wifi-vap"
    end
    config radio-2
      set vap-all manual
      set vaps "wifi-vap"
    end
  next
end
```

6. Create the SSID-to-Internet firewall policy:

```
config firewall policy
  edit 1
    set name "WiFi to Internet"
    set srcintf "wifi-vap"
    set dstintf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set fsso disable
    set nat enable
  next
end
```

Configuring an external captive portal

An external captive portal is a web page on a web server as opposed to the built-in captive portal on FortiGate. 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 an external WiFi Captive Portal in tunnel mode - GUI:

1. Go to *WiFi and Switch Controller* > *SSIDs.*
   If the SSID already exists, you can edit the SSID or you can edit the WiFi interface in *Network* > *Interfaces*.
2. Set the *Traffic mode* to *Tunnel*.
3. In *Security Mode*, select a Security mode.
4. Enable *Captive Portal*.
5. Select the *Portal type* you want.
6. In *Authentication portal*, select *External* and 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.
7. Configure the other settings as needed.
8. When you are finished, select *OK*.

To configure an external WiFi Captive Portal in tunnel mode - CLI:

```
config wireless-controller vap
  edit "wifi-vap"
    set ssid "Fortinet-Captive"
    set security wpa3-sae
    set captive-portal enable
    set external-web "example.com"
    set selected-usergroups "Guest-group"
    set schedule "always"
  next
end
```

To configure an auth-mac portal in tunnel mode - CLI:

To support a MAC authentication portal (such as Cisco ISE authentication) in tunnel mode, you must set `portal-type` to `auth-mac`.

```
config wireless-controller vap
  edit wifi-cap
    set ssid "fortinet-guest"
    set security wpa3-sae
    set captive-portal enable
    set portal-type auth-mac
    set radius-mac-auth enable
    set radius-mac-auth-server "CISCO_ISE"
    set radius-mac-auth-usergroups "registered"
    set external-web "https://<ISE_Portal>:8443/portal/g?p=123456789"
  next
end
```

To configure an external WiFi Captive Portal in local bridge mode - CLI:

```
config wireless-controller vap
  edit "cap"
    set ssid "fortinet-guest"
    set security wpa3-sae
    set captive-portal enable
    set external-web "example.com/portal"
    set radius-server "peap"
```

```
    set local-bridging enable
    set portal-type external-auth
  next
end
```

To configure an external-macauth portal in bridge mode - CLI:

To support an external MAC authentication portal (such as Cisco ISE authentication) in bridge mode, you must set `portal-type` to `external-macauth`.

```
config wireless-controller vap
  edit wifi-cap
    set ssid "fortinet-guest"
    set security wpa3-sae
    set captive-portal enable
    set external-web "https://<ISE_Portal>:8443/portal/g?p=jN9z47goOJg75HpaXxV8WZPQgd"
    set radius-mac-auth enable
    set radius-mac-auth-server "ISE"
    set radius-mac-auth-usergroups "AuthorizedGuest"
    set local-bridging enable
    set portal-type external-macauth
    set schedule "always"
  next
end
```

Configuring MAC Bypass for captive portal

Captive portal security supports `MAC-auth-bypass`. If a client's MAC can be authenticated from local-user or a RADIUS server, then the client can bypass firewall authentication directly.

To configure MAC bypass for the captive portal SSID - CLI:

```
config wireless-controller vap
  edit "cap"
    set ssid "fortinet-guest"
    set security wpa3-sae
    set captive-portal enable
    set mac-auth-bypass enable
    set selected-usergroups "group-radius"
  next
end
```

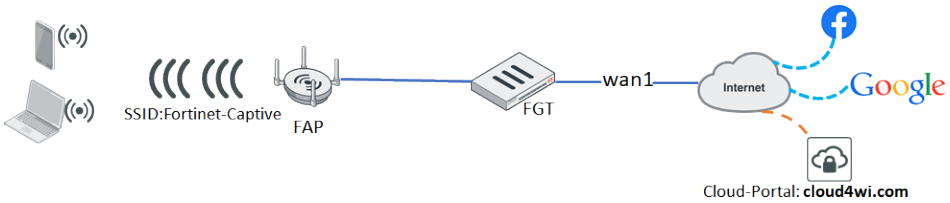
Configuring wildcard address in captive portal walled garden

This topic describes how to add and apply wildcard domain names to the walled garden of captive-portal SSID.

Captive portal SSID supports the walled garden function where WiFi clients can access preconfigured hostnames and addresses that are exempted from portal authentication.

You can configure FQDN entries using wildcard domain names, for example, `*.google.*`, `*.facebook.com`, and so on, so that one entry can have multiple matches.

Sample topology



This example uses the wildcard address feature in the following ways:

- A tunnel mode captive portal works with the third-party cloud based portal server *cloud4wi.com*.
- Connected wireless clients can access Facebook and Google websites directly even before firewall authentication via FortiGate.
- Connected wireless clients opens the portal page of cloud4wi.com and can access other Internet resources as soon as they pass authentication by FortiGate.

Sample configuration

To create the wildcard FQDN address - GUI:

1. Go to *Policy & Objects* > *Addresses* and click *Create New* > *Address*.
2. In the *New Address* page, enter the address *Name*, for example, `facebook` and `google`.
3. For *Type*, select *FQDN*.
4. For *FQDN*, enter a wildcard FQDN name, for example `*.facebook.com` and `*.google.*`.
5. Click *OK*.

This wildcard FQDN type firewall address is different from entries in *Policy & Objects* > *Wildcard FQDN Addresses* that cannot be used directly in firewall policy source or destination addresses.

To create a third-party cloud portal server address - GUI:

1. Go to *Policy & Objects* > *Addresses* and click *Create New* > *Address*.
2. In the *New Address* page, enter the address *Name*, for example, `cloud-portal`.
3. For *Type*, select *FQDN*.
4. For *FQDN*, enter the FQDN name, for example, `cloud4wi.com`.
5. Click *OK*.

To create a captive portal VAP with the third-party cloud portal server - GUI:

1. Go to *WiFi Controller* > *SSID* and select *Create New* > *SSID*.
2. For *Traffic Mode*, select *Tunnel*.
3. In the *Address* section, enter the *IP/Network Mask*, for example, `10.10.80.1/24`.
4. Optionally, you can change the DHCP *Address Range* in the *DHCP Server* section.
5. In the *WiFi Settings* section:
   a. Enter the *SSID* name, for example, `Fortinet-Captive`.
   b. For *Security Mode*, select a Security mode.
      Note: Captive Portal is not supported for WPA/WPA2-Enterprise or WPA3-Enterprise Security modes.

   c. Enable *Captive Portal*.
   d. For *Portal Type*, select *Authentication*.
   e. For *Authentication Portal*, select *External* and enter `cloud4wi.com`.
   f. Click *User Groups* and select the created user group, for example, `group-local`; or click *Create* to create a new user group.
6. Click *OK*.

To support a third-party cloud portal, use one of the following methods.

To support a third-party cloud portal using Exempt Destinations/Services - GUI:

1. Go to *WiFi Controller* > *SSID*.
2. Select the SSID you created, for example, `Fortinet-Captive` and click *Edit*.
3. In the *WiFi Settings* section, click *Exempt Destinations/Services*.
4. In the *Select Entries* pane *Address* list, select the wildcard FQDN addresses, for example, `facebook` and `google`, and the cloud portal address, for example, `cloud-portal`.
5. Still in the *Select Entries* pane, click *Service* and select *HTTP*, *HTTPS*, and *DNS*.
6. Click *OK*.

To support a third-party cloud portal using firewall policy - GUI:

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. Enter the *Name*, for example, *Exempt Service*.
3. Click *Incoming Interface* and select *wifi-vap*.
4. Click *Outgoing Interface* and select *wan1*.
5. Click *Source* and select *all*.
6. Click *Destination* and select the wildcard FQDN addresses, for example, `facebook` and `google`, and the cloud portal address, for example, `cloud-portal`.
7. Click *Service* and select *HTTP*, *HTTPS*, and *DNS*.
8. Click *OK*.
9. Use CLI commands to enable `captive-portal-exempt`. In this example, the `policy_id` is `2`.

```
config firewall policy
  edit 2
      set captive-portal-exempt enable
  next
end
```

To create the wildcard FQDN address - CLI:

```
config firewall address
   edit "facebook"
     set type fqdn
     set fqdn "*.facebook.com"  <-- New support for "*" in fqdn address
   next
   edit "google"
     set type fqdn
     set fqdn "*.google.*"      <-- New support for "*" in fqdn address
   next
end
```

To create a third-party cloud portal server address - CLI:

```
config firewall address
   edit "cloud-portal"
     set type fqdn
     set fqdn "cloud4wi.com"
   next
end
```

To create a tunnel mode captive portal VAP with the third-party cloud portal server - CLI:

```
config wireless-controller vap
    edit "wifi-vap"
        set ssid "Fortinet-Captive"
        set security wpa3-sae
        set captive-portal enable
        set external-web "cloud4wi.com"
        set selected-usergroups "group-local"
        set intra-vap-privacy enable
    next
end
```

To create security-exempt-list and select it in vap - CLI:

```
config user security-exempt-list
    edit "wifi-vap-exempt-list"
        config rule
            edit 1
                set dstaddr "facebook" "google" "cloud-portal"
                set service "HTTP" "HTTPS" "DNS"
            next
        end
end
config wireless-controller vap
    edit "wifi-vap"
        set security-exempt-list "wifi-vap-exempt-list"
    next
end
```

To create a captive-portal-exempt firewall policy and move it before the regular outgoing policy - CLI:

```
config firewall policy
    edit 2
        set name "Exempt Service"
        set srcintf "wifi-vap"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "cloud-portal" "facebook" "google"
        set action accept
        set schedule "always"
        set service "DNS" "HTTP" "HTTPS"
        set captive-portal-exempt enable
        set nat enable
    next
    edit 1
```

```
        set name "outgoing"
        set srcintf "wifi-vap"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
    move 2 before 1
end
```

Although `destination-hostname-visibility` is enabled by default, ensure this setting is enabled so that FQDN addresses can be resolved.

To enable destination-hostname-visibility

```
config system network-visibility
    set destination-hostname-visibility enable
end
```

Captive portal authentication when bridged via software switch

When a tunnel mode SSID or a VLAN sub-interface of an SSID is bridged with other interfaces via a software switch, you must set the `intra-switch-policy` to `explicit` when the switch interface is created in order to enable captive portal authentication.

To configure captive portal authentication on an SSID or VLAN sub-interface:

1. Configure the local user:

```
config user local
    edit "user1"
        set passwd *********
    next
end
```

2. Configure the user group:

```
config user group
    edit "wifi-group"
        set member "user1"
    next
end
```

3. Configure the VAP:

```
config wireless-controller vap
    edit "test-captive"
        set ssid "test-captive"
        set security wpa3-sae
        set captive-portal enable
        set portal-type auth+disclaimer
        set selected-usergroups "wifi-group"
        set schedule "always"
```

```
    next
end
```

4. Create a software switch interface consisting of a tunnel VAP with captive portal security and a physical interface (port7):

```
config system switch-interface
    edit "test-ssw"
        set vdom "vdom1"
        set member "port7" "test-captive"
        set intra-switch-policy explicit
    next
end
```

5. Create the firewall policy:

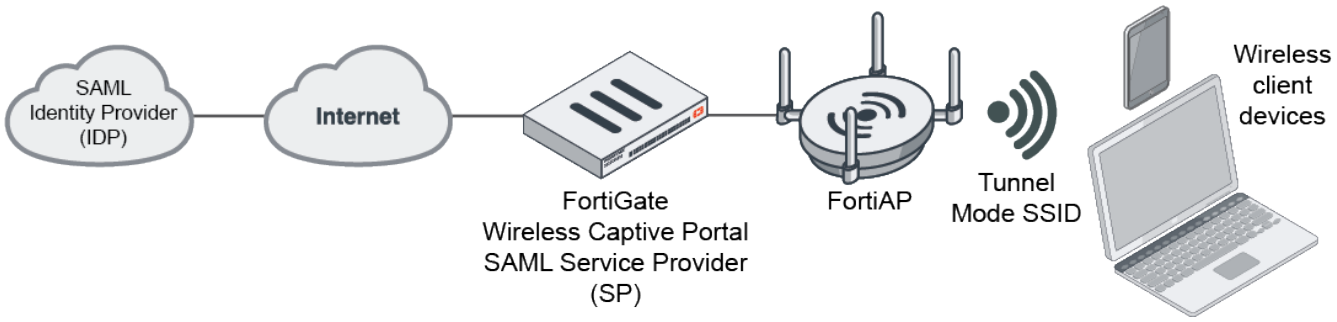
```
config firewall policy
    edit 1
        set srcintf "test-captive" "port7"
        set dstintf "port7" "test-captive"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat disable
    next
end
```

6. Connect the external DHCP server to the physical interface.
7. Connect a WiFi client to the tunnel VAP. The client will get an IP assignment from the DHCP server and pass the captive portal authentication.
8. Verify the authenticated firewall users list:

```
# diagnose firewall auth list
10.100.250.250, u1
    src_mac: fc:d8:d0:9a:8b:85
    type: fw, id: 0, duration: 29, idled: 12
    expire: 288, allow-idle: 300
    flag(100): wsso
    packets: in 229 out 162, bytes: in 192440 out 22887
    user_id: 16777218
    group_id: 2
    group_name: wifi
----- 1 listed, 0 filtered ------
```

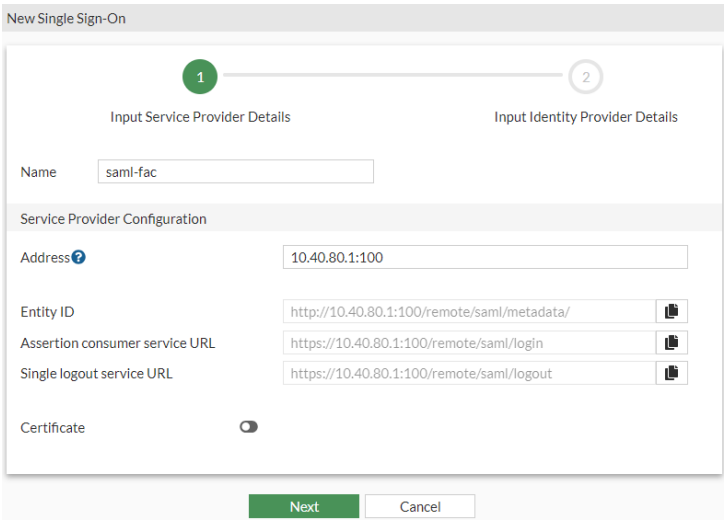
Captive portal authentication using SAML credentials

When a SAML user has been configured on the FortiGate, a user group containing this SAML user can be applied to a captive portal in a wireless tunnel mode SSID. You can configure both a captive portal exempt firewall policy to allow wireless clients to contact the SAML IDP and a firewall policy with the SAML user group applied to allow authenticated traffic. When wireless clients connect to the SSID, they will be redirected to a login page for wireless authentication using SAML.



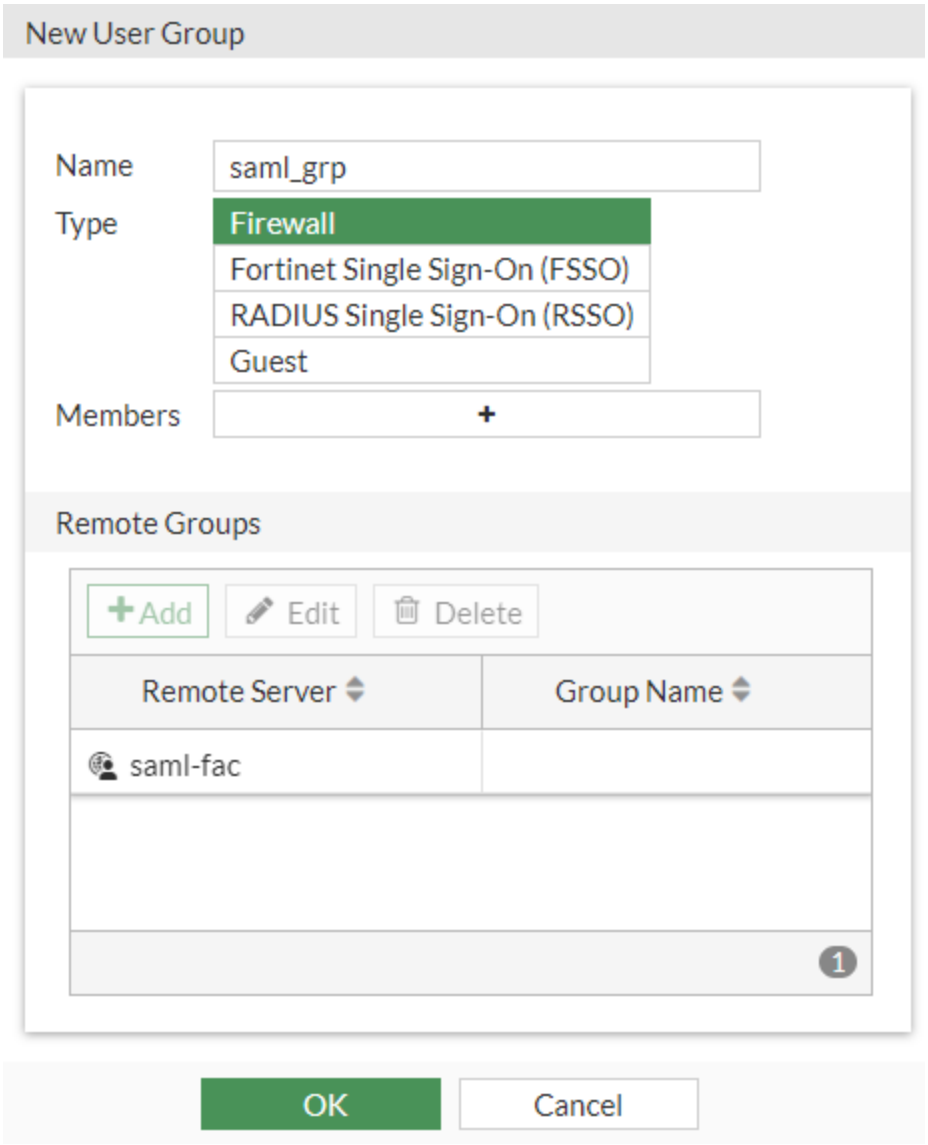
To configure SAML Authentication - GUI:

1. Create a SAML server on a FortiGate:
   a. Go to *User & Authentication* > *Single Sign-On* and click *Create new*.
   b. Enter a *Name* for the SAML server (saml-fac) and configure the Service Provider details.

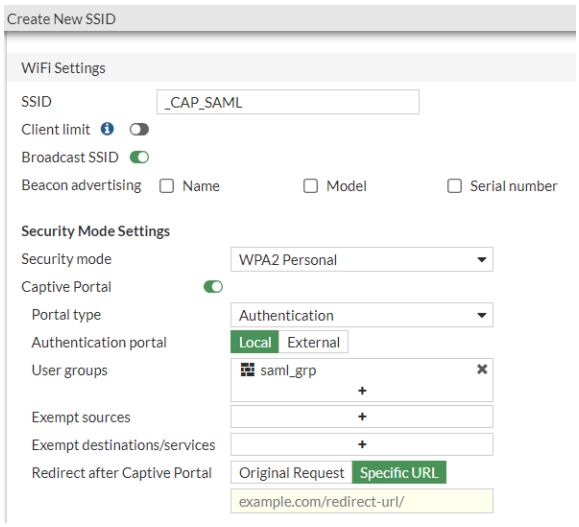


   c. Click *Next*.
   d. Input the Identity Provider information.
   e. When you are finished, click *Submit*.
2. Create a user group with members as the SAML server you created:
   a. Go to *User & Authentication* > *User Groups* and click *Create New*.
   b. Enter a *Name* for the group (saml_grp).
   c. In the *Remote Groups* table, click *Add*.

d. In the *Remove Server* dropdown, select the SAML server you created (saml-fac) and click *OK*.



3. Select the user group in a Captive portal VAP:
   a. Go to *WiFi & Switch Controller* > *SSIDs* and click *Create New* > *SSID*.
   b. Enter an *SSID* name (_CAP_SAML).
   c. Ensure that *Traffic mode* is set to *Tunnel*.
   d. Under *Security Mode Settings*, enable the *Captive Portal*.
   e. In *User groups*, select the group you created (saml_grp).



f. Configure other settings as needed.

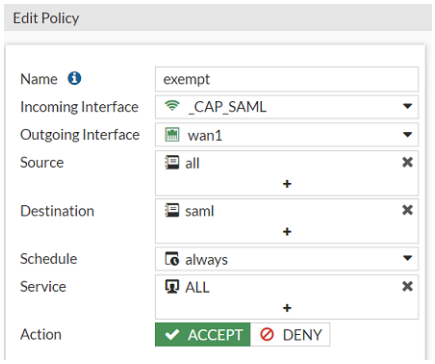
g. When you are finished, click *OK*.

4. Create a firewall policy with `captive-portal-exempt` enabled to ensure wireless clients can access the SAML server without authentication:

   a. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.

   b. Configure the following:

Incoming Interface	Select the captive portal VAP (_CAL_SAML).
Source	*all*
Destination	Select the saml server.
Action	*ACCEPT*



   c. Configure other settings as needed.

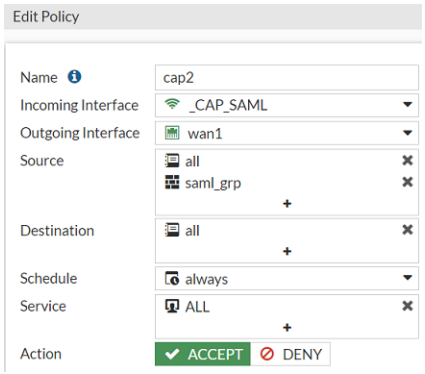
   d. When you are finished, click *OK*.

   e. You can only configure `captive-portal-exempt` from the CLI:

```
config firewall policy
 edit 8
   set captive-portal-exempt enable
 end
```

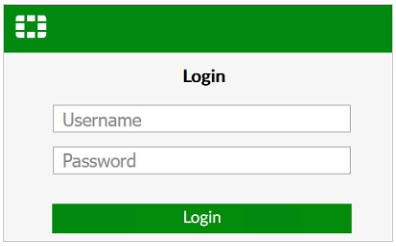
5. Create a policy to let wireless clients access the outbound after passing authentication:
   a. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
   b. Configure the following:

Incoming Interface	Select the captive portal VAP (_CAL_ SAML).
Source	*all* Select the SAML user group (*saml_grp*)
Destination	*all*
Action	*ACCEPT*



   c. Configure other settings as needed.
   d. When you are finished, click *OK*.

When a wireless client connects to the SSID, it is redirected to the SAML login portal page. After the client submits the correct credentials, it can access the internet.



To configure SAML Authentication - CLI:

1. Create a SAML server on a FortiGate:

```
config user saml
 edit "saml-fac"
   set entity-id "http://10.40.80.1:1000/saml/metadata/"
   set single-sign-on-url "https://10.40.80.1:1003/saml/login/"
   set single-logout-url "https://10.40.80.1:1003/saml/logout/"
   set idp-entity-id "http://172.18.58.93:443/saml-idp/wifiqa1234/metadata/"
   set idp-single-sign-on-url "https://172.18.58.93:443/saml-idp/wifiqa1234/login/"
   set idp-single-logout-url "https://172.18.58.93:443/saml-idp/wifiqa1234/logout/"
   set idp-cert "REMOTE_Cert_2"
   set user-name "username"
```

```
    set group-name "group"
    set digest-method sha1
  next
end
```

2. Create a user group with members as the SAML server you created:

```
config user group
  edit "saml_grp"
    set member "saml-fac"
  next
end
```

3. Select the user group in a Captive portal VAP:

```
config wireless-controller vap
  edit "wifi4"
    set ssid "_CAP_SAML"
    set security wpa3-sae
    set captive-portal enable
    set selected-usergroups "saml_grp"
    set security-exempt-list "wifi4-exempt-list"
    set security-redirect-url "http://www.example.com"
    set schedule "always"
  next
```

4. Create two policies from VAP to outbound:
   - One policy with `captive-portal-exempt` enabled to ensure wireless clients can access the SAML server without authentication (firewall policy ID 8, name "exempt").
   - One policy is a regular policy that lets wireless clients access the outbound after passing authentication (firewall policy ID 6, name "cap2").

   The firewall policy ID is 8, the name is "exempt"

```
config firewall policy
  edit 8
    set name "exempt"
    set uuid d8f2b572-b2fa-51ec-d3ad-3110a44be109
    set srcintf "wifi4"
    set dstintf "wan1"
    set action accept
    set srcaddr "all"
    set dstaddr "saml"
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set nat enable
    set comments "Exempt policy"
    set captive-portal-exempt enable
  next
  edit 6
    set name "cap2"
    set uuid 3a4f1518-7b57-55dc-f5kf-21748a5ch415
    set srcintf "wifi4"
    set dstintf "wan1"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
```

```
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
        set groups "saml_grp"
      next
    end
```

When a wireless client connects to the SSID, it is redirected to the SAML login portal page. After the client submits the correct credentials, it can access the internet.

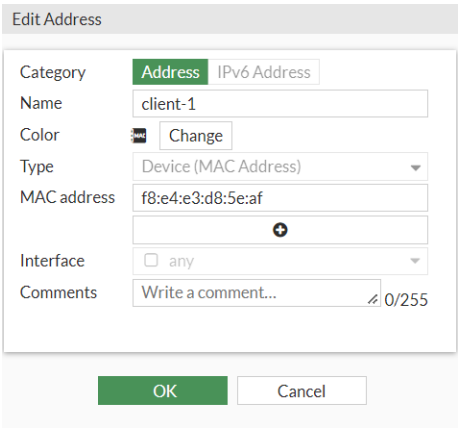
Adding a MAC filter

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.

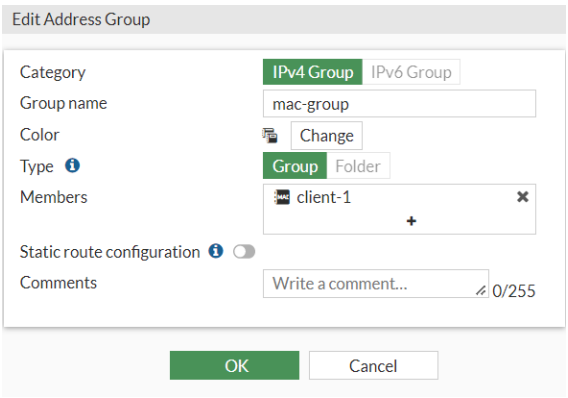
This is not the most secure method as someone seeking unauthorized access to your network can obtain MAC addresses from wireless traffic and use them to impersonate legitimate users. A MAC filter list should only be used in conjunction with other security measures such as encryption.

To create and apply a MAC address filter - GUI:

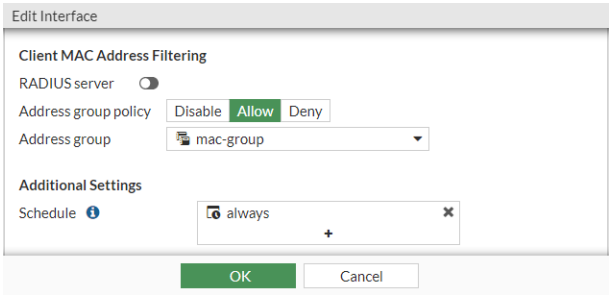
1. Go to *Policy & Objects* > *Addresses* and select *Create New* > *Address*.
2. Name the address and set the *Type* as *Device (MAC Address)*.
3. Enter the *MAC address(es)* you want to filter.



4. When you are finished, click *OK*.
5. Go to *Policy & Objects* > *Addresses* and select *Create New* > *Address Group*.
6. Name the address group
7. Click *Members* and select the address you created earlier.



8. When you are finished, click *OK*.
9. Go to *WiFi & Switch Controller* > *SSIDs* and select the SSID you want to apply the filter to.
10. Locate *Client MAC Address Filtering* and select an *Address group policy*:
    - *Disable*: Disable MAC address filtering policy for MAC addresses that are in the address group. This is the default.
    - *Allow*: Permit clients with MAC addresses that are in the address group.
    - *Deny*: Deny clients with MAC addresses that are in the address group.
11. Select the *Address group* you created.



12. When you are finished, click *OK*.
    The SSID now accepts or denies the address group you configured.

To create and apply a MAC address filter - CLI:

1. Create the firewall address entry and set the `type` to `mac`:

```
config firewall address
 edit "client-1"
   set uuid f35b2080-a199-51ec-7d97-00495859217e
   set type mac
   set macaddr "f8:e4:e3:d8:5e:af"
 next
end
```

2. Create a firewall address group and select the address entry you just created.

```
config firewall addrgrp
 edit "mac-group"
   set uuid 26260750-a19a-51ec-b054-b385dab00c07
   set member "client-1"
```

```
  next
end
```

3. Under a wireless vap interface, there is a new `address-group-policy` option to help control the mac filter function.
   - To allow the connection, select the created `address-group` and set the `address-group-policy` to `allow`:

```
config wireless-controller vap
  edit "wifi.fap.01"
    set ssid "ExampleSSID"
    set passphrase ENC *
    set schedule "always"
    set address-group "mac-group"
    set address-group-policy allow
  next
end
```

   - To deny the connection, select the created `address-group` and set the `address-group-policy` to `deny`:

```
config wireless-controller vap
    edit "wifi.fap.02"
        set ssid "ExampleSSID"
        set passphrase ENC *
        set schedule "always"
        set address-group "mac-group"
        set address-group-policy deny
    next
end
```

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 and Switch Controller* > *SSIDs* 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- GUI:

To access this setting from the GUI, you must enable Advanced Wireless Features (see Advanced Wireless Features on page 165).

1. Once you enable Advanced Wireless Features, navigate to *WiFi & Switch Controller* > *Operation Profiles* > *FortiAP Profiles*.
2. Select the profile you want to limit clients on.
3. Under *Advanced Settings* > *Maximum client count*, enter the maximum number of clients you want to allow.
4. When you are finished, click *OK*.

To limit the number of clients per AP- CLI:

Edit the wtp-profile (FortiAP profile):

```
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 Internet Group Management Protocol (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.

Enabling IGMP Snooping

IGMP snooping on SSID can prevent WiFi clients and hosts from receiving traffic for a multicast group they have not explicitly joined. Upon detecting clients' multicast group IDs, FortiAPs join the corresponding multicast groups and the controller sends multicast packets to only CAPWAP multicast groups. Thus, the controller can prune multicast traffic from managed APs that do not contain a multicast listener (an IGMP client).

To configure IGMP snooping- GUI:

To enable IGMP snooping from the GUI, you must enable Advanced Wireless Features (see Advanced Wireless Features on page 165).

1. Once you enable Advanced Wireless Features, navigate to *WiFi & Switch Controller* > *SSIDs* and select the SSID you want to enable IGMP snooping on.
2. Under *Advanced Settings*, locate *IGMP Snooping* and select if you want to enable or disable it.
3. When you are finished, click *OK*.

To configure IGMP snooping- CLI:

```
config wireless-controller vap
   edit example_wlan
      set igmp-snooping {enable | disable}
   next
end
```

To debug IGMP snooping:

```
diagnose wireless-controller wlac -c vap-mcgrp
```

Replacing WiFi certificate

You can replace the built-in WiFi certificate with one you upload.

These instruction apply to FortiWiFi devices using internal WiFi radios and FortiGate/FortiWiFi devices configured as WiFi Controllers that are managing FortiAP devices, and have WiFi clients that are connected to WPA2-Enterprise SSID and authenticated with local user groups.

On FortiOS, the built-in *Fortinet_Wifi* certificate is a publicly signed certificate that is only used in WPA2-Enterprise SSIDs with local user-group authentication. The default WiFi certificate configuration is:

```
config system global
    set wifi-ca-certificate "Fortinet_Wifi_CA"
    set wifi-certificate "Fortinet_Wifi"
end
```

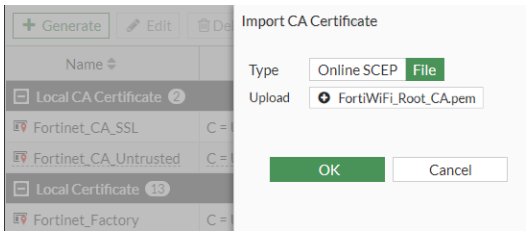
Consider the following factors:

- The *Fortinet_Wifi* certificate is issued to *Fortinet Inc.* with common name (CN) *auth-cert.fortinet.com*. If a company or organization requires their own CN in their WiFi deployment, they must replace it with their own certificate.
- The *Fortinet_Wifi* certificate has an expiry date. When it expires, it must be renewed or replaced with a new certificate.

To replace a WiFi certificate:

1. Get new certificate files, including a root CA certificate, a certificate signed by the CA, and the corresponding private key file.
   You can purchase a publicly signed certificate from a commercial certificate service provider or generate a self-signed certificate.
2. Import the new certificate files into FortiOS:
   a. In FortiGate, go to *System* > *Certificates*.
      You may need to enable *Certificates* from *System* > *Feature Visibility*.
      If VDOMs are enabled, go to *Global* > *System* > *Certificates*.
   b. Click *Import* > *CA Certificate*.

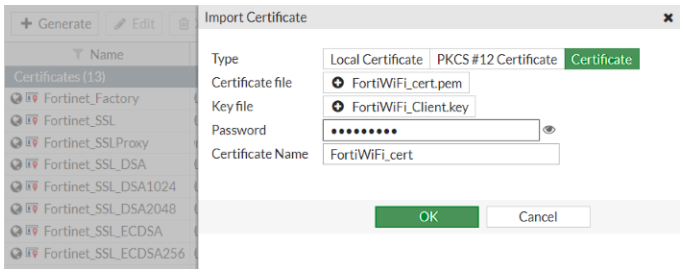
c. Set the *Type* to *File* and upload the CA certificate file from the management computer.



d. Click *OK*.
The imported CA certificate is named *CA_Cert_N* or *G_CA_Cert_N* when VDOMs are enabled, where *N* starts from *1* and increments for each imported certificate, and *G* stands for global range.

e. Click *Import* > *Local Certificate*.

f. Set the *Type* to *Certificate*, upload the certificate file and key file, enter the password, and enter the certificate name.



g. Click *OK*.
The imported certificates are listed on the *Certificates* page.

3. Change the WiFi certificate settings:
   a. Go to *WiFi & Switch Controller* > *WiFi Settings*.
   b. In *WiFi certificate*, select the imported local certificate.
   c. In the *WiFi CA certificate*, select the imported CA certificate.
   d. Click *Apply*.

To replace a WiFi certificate using the CLI:

```
config system global
    set wifi-ca-certificate <name of the imported CA certificate>
    set wifi-certificate <name of the imported certificate signed by the CA>
end
```

To restore the factory default WiFi certificates using the CLI:

```
config system global
    set wifi-ca-certificate "Fortinet_CA"
    set wifi-certificate "Fortinet_Factory"
end
```

As the factory default certificates are self-signed, WiFi clients need to accept it at the connection prompt or import the *Fortinet_CA* certificate to validate it.

Additional Information

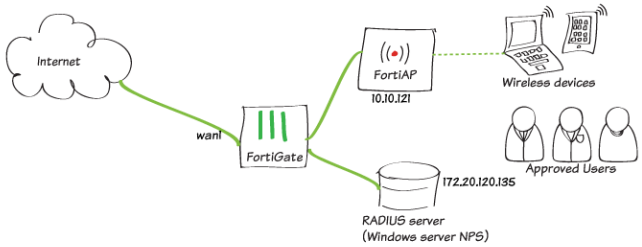
The *Fortinet_Wifi* certificate can be updated automatically through the FortiGuard service certificate bundle update.

If the built-in *Fortinet_Wifi* certificate has expired and not been renewed or replaced, WiFi clients can still connect to the WPA2-Enterprise SSID with local user-group authentication by ignoring any warning messages or bypassing *Validate server certificate* (or similar) options.

Configuring WiFi with WSSO using Windows NPS and user groups

You can configure Wireless Single Sign-On (WSSO) using a Network Policy Server (NPS) and FortiGate user groups.

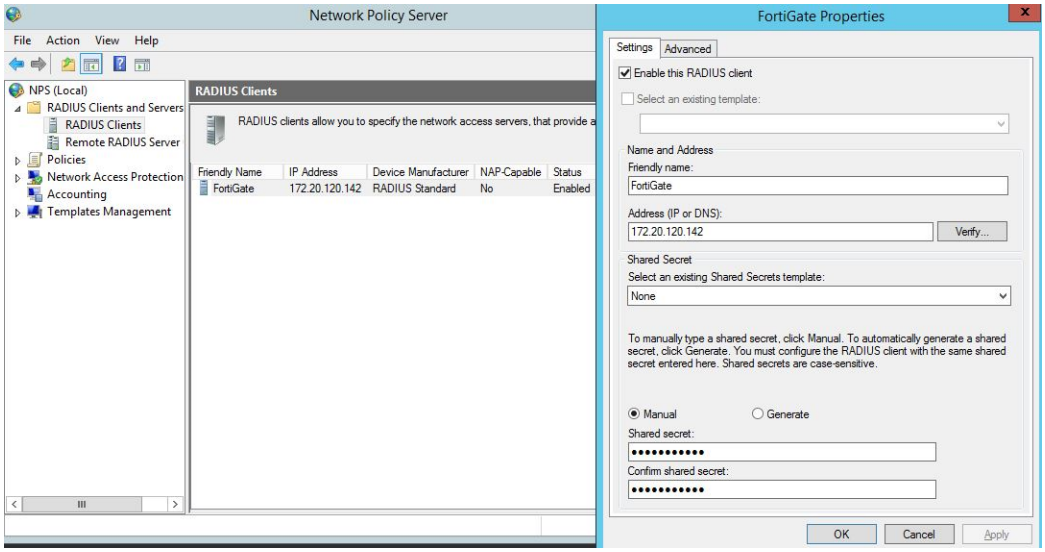
In the following example, the WiFi users are students at a school. The user group belongs to a Windows Active Directory (AD) group called *WiFiAccess*. When the users enter their WiFi user names and passwords, the FortiGate checks the local group *WiFi*. Since this user group has been set up on a remote authentication dial-in user service (RADIUS) server, the FortiGate performs user authentication against the NPS or RADIUS server. If the user is successfully authenticated, the FortiGate checks for a policy that allows the *WiFi* group access.



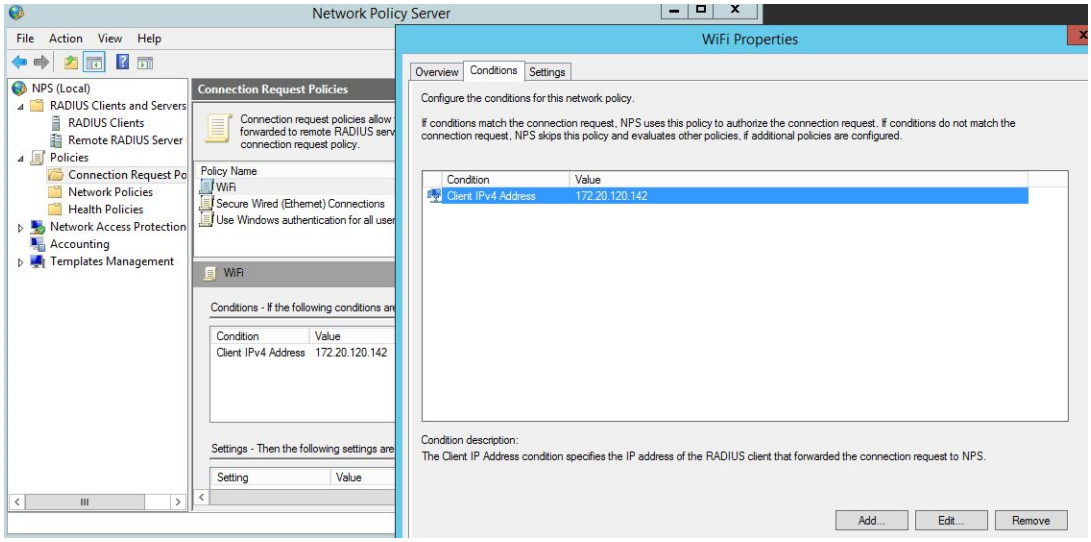
To configure WSSO using Windows NPS and user groups:

1. Register the FortiGate as a RADIUS client on the NPS:
   a. In the NPS, go to *RADIUS Clients and Servers* > *RADIUS Clients*.
   b. Right-click *RADIUS Clients* and select *New*.
   c. Enter the FortiGate information:
      - Name
      - IP address (`172.20.120.142`)
      - Shared secret (password)
   d. Click *OK*.

The FortiGate properties view:

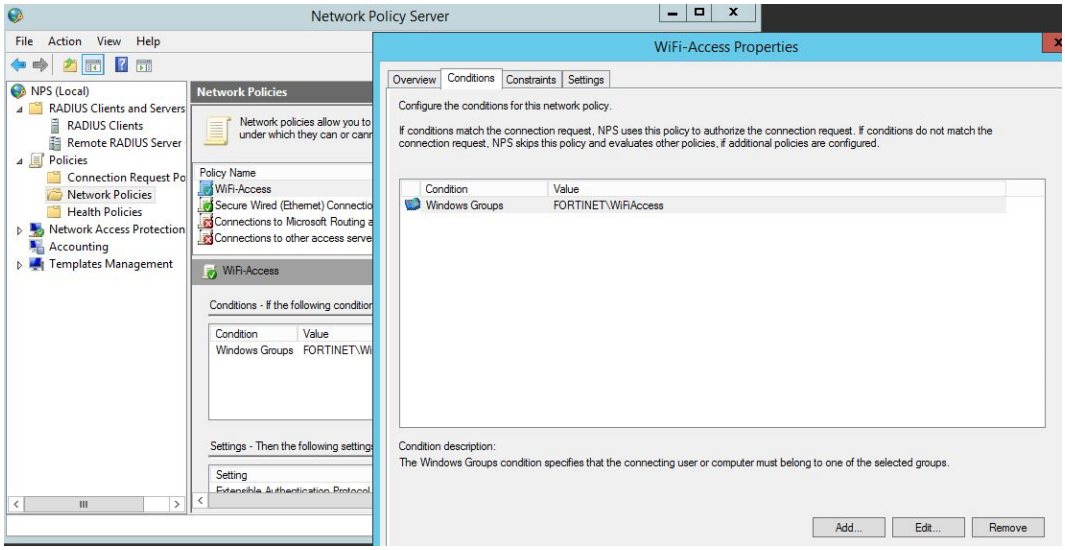


2. Create a connection request policy:
   a. Go to *Policies* > *Connection Request Policies*.
   b. Right-click *Connection Request Policies* and select *New*.
   c. Enter the policy name (`WiFi`) and select the type of network access server.
   d. Click *Next*. The *Specify Conditions* window opens.
   e. Click *Add* and under *Connection Properties*, select *Client IPv4 Address*.
   f. Configure the *Client IPv4 Address* as the FortiGate IP address.
   g. Keep clicking *Next* and leave the default settings until you can click *Finish*.

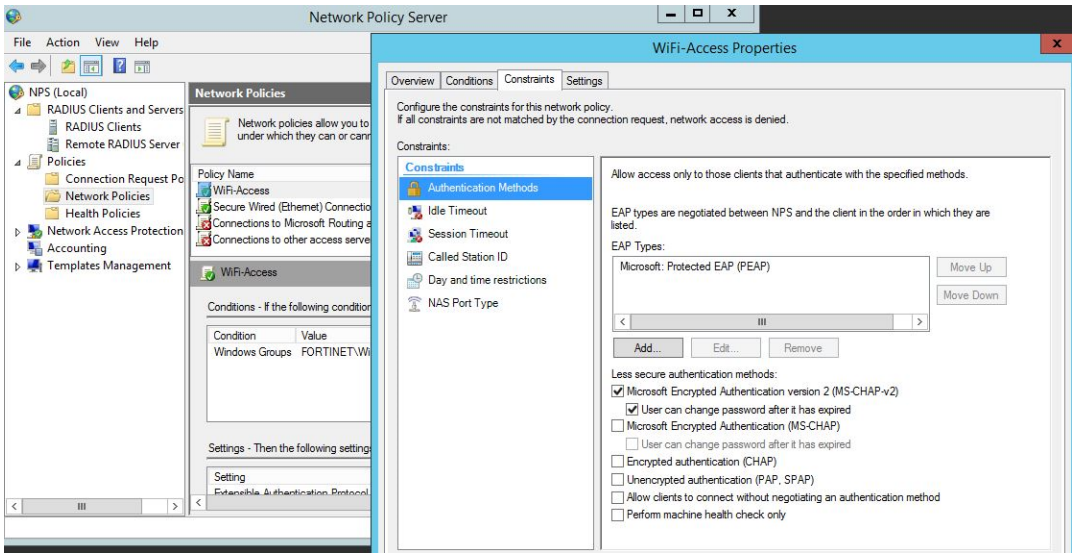


3. Create a network policy:
   a. Go to *Policies* > *Network Policies*.
   b. Right-click *Network Policies* and select *New*.
   c. Enter the policy name (`WiFi-Access`) and select the type of network access server.
   d. Click *Next*. The *Specify Conditions* window opens.
   e. Click *Add* and under *Groups*, select *Windows Groups*.

f. Click *Add Groups* and enter the Windows AD group, *WiFiAccess*, as the *object name to select*.
g. Click *OK*, then *Next* twice to advance to the *Configure Authentication Methods* window.
h. For *EAP Types*, click *Add* and select *Microsoft: Protected EAP (PEAP)*.
i. Click *OK*.
j. For *Less secure authentication methods*, make sure only the *Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)* and *User can change password after it has expired* checkboxes are selected.
k. Keep clicking *Next* and leave the default settings until you can click *Finish*.
The WiFi-Access network policy conditions properties view:

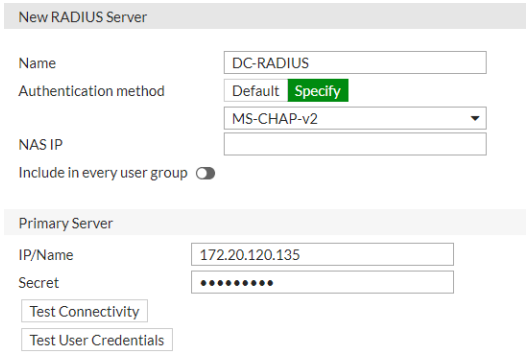


The WiFi-Access network policy constraints properties view:



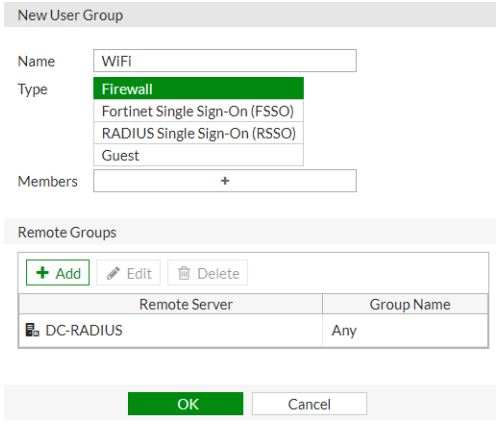
4. Configure the FortiGate to use the RADIUS server:
   a. In FortiOS, go to *User & Authentication* > *RADIUS Servers*.
   b. Click *Create New*.

c. Enter the server information:
   - Name (`DC-RADIUS`)
   - Authentication method (click *Specify* and select *MS-CHAP-v2*)
   - Domain controller IP address
   - Server secret



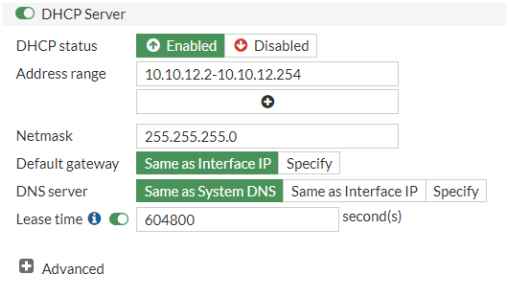
d. Optionally, you can click *Test Connectivity*. After you enter the user ID and password, the result should be successful.
e. Click *OK*.

5. Configure the WiFi user group:
   a. Go to *User & Authentication* > *User Groups*.
   b. Click *Create New*.
   c. Enter the user group information:
      - Name
      - Type (select *Firewall*)
   d. Under *Remote Groups*, click *Add*. The *Add Group Match* pane opens.
   e. In the *Remote Server* dropdown, select the RADIUS server you just configured (*DC-RADIUS*).
   f. For *Groups*, click *Any*.
   g. Click *OK* to add the server.
   h. Click *OK* to save the user group.



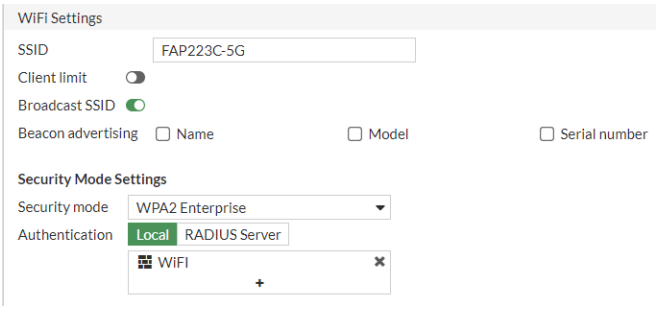
6. Create an SSID with RADIUS authentication:
   a. Go to *WiFi & Switch Controller* > *SSIDs*.
   b. Click *Create New* > *SSID*.
   c. Configure the interface and enable *DHCP Server*.

d. Enter the Address range.



e. Configure the *WiFi Settings* section:

- For *Security Mode*, select *WPA2 Enterprise*.
- For *Authentication*, click *Local* and add the *WiFi* user group.



Local vs RADIUS Server Authentication:

- Local: PEAP terminates on the FortiGate, and FortiGate uses the built-in Fortinet_WiFi certificate for the connection by default. To select a different certificate, see Replacing WiFi certificate on page 93 for details.
- RADIUS Server: PEAP is forwarded to the RADIUS Server.

f. Click *OK*.

7. Create a security policy:

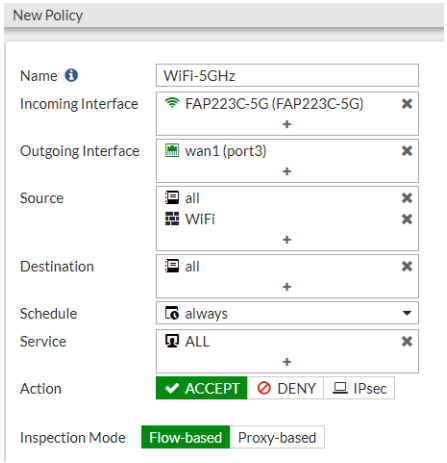
a. Go to *Policy & Objects* > *Firewall Policy*.

b. Click *Create New*.

c. Configure the policy to have the SSID you created in step 6 as the *Incoming Interface* and the WiFi user group you created in step 5 as the *Source*.

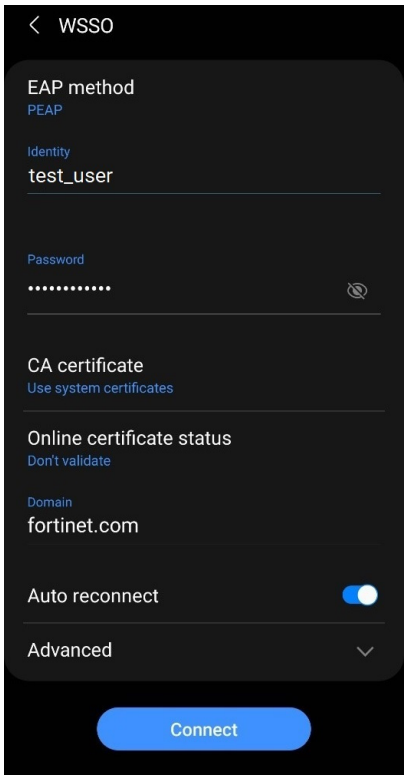
d. Configure other settings as needed.

e. Click *OK*.



To verify the WSSO authentication:

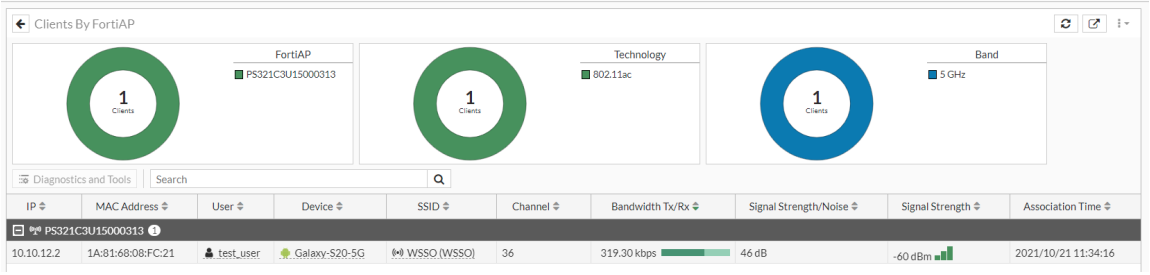
1. From the wireless client, the wireless settings may ask for the CA certificate for the PEAP connection.
   - On Android devices, you can select *Use system certificate* since the default FortiGate_WiFi certificate is signed by a public CA. If asked to specify the domain, enter `fortinet.com`. See the example Android WiFi client settings:



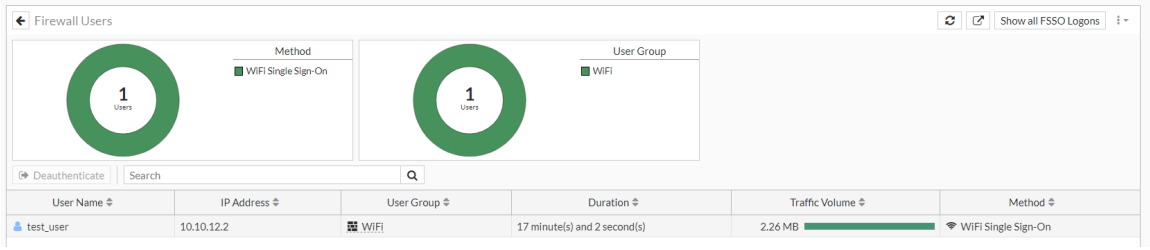
   - Alternatively, select *Don't Validate* to bypass validating the certificate used in the PEAP connection.
2. Use the credentials of a user that belongs to the Windows AD WiFiAccess group to verify that you have been successful authenticated.

a. Try connecting to the WiFi network.
b. Get authenticated.
c. Browse the internet.

3. Go to *Dashboard* > *WiFi* > *Clients By FortiAP* to see a list of logged on WiFi users.



4. Go to *Dashboard* > *User & Devices* > *Firewall Users*. The logged on user will be authenticated by Firewall Authentication and listed here.



Enabling Beacon Protection

You can enable Beacon Protection on WPA3 SSIDs which improves Wi-Fi security by protecting beacon frames. Beacon Protection was introduced in WPA3 and is designed to enhance security in Wi-Fi networks by protecting the integrity of the beacon frames, which are essential for network discovery and connection establishment. This helps devices discover and connect to legitimate networks, reducing attack risks.

Beacon Protection is supported on FortiAP K series running the "wifi7" special builds (branched out of FortiAP 7.4.x).

FortiAP F and G series running 7.4.x builds do NOT support Beacon Protection.

CLI Changes:

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

Beacon Protection is disabled by default.

To enable Beacon Protection from the FortiGate:

```
config wireless-controller vap
    edit "wpa3-sae-beacon"
        set ssid "wpa3-sae-beacon"
```

```
        set security wpa3-only-enterprise
        set pmf enable
        set beacon-protection enable
        set auth radius
        set radius-server "peap"
        set local-bridging enable
        set schedule "always"
    next
end
```

To assign Beacon Protection to a FortiAP profile:

```
conf wireless-controller wtp-profile
  edit FAP441K-default
    conf radio-2
      set vaps wpa3-sae-beacon
    end
  next
end
```

To verify that Beacon Protection is assigned and enabled on a FortiAP:

```
FortiAP-441K # vcfg
-------------------------------VAP Configuration    1-----------------------------
Radio Id  1 WLAN Id  0 wpa3-sae-beacon ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown
(-1)
           vlanid=0, intf=wlan10, vap=0x28a9202c, bssid=38:c0:ea:f1:51:70
           11ax high-efficiency=enabled target-wake-time=enabled
           bss-color-partial=enabled
           mesh backhaul=disabled
           local_auth=disabled standalone=disabled nat_mode=disabled
           local_bridging=enabled split_tunnel=disabled layer3_roaming=disabled
           intra_ssid_priv=disabled
           mcast_enhance=disabled igmp_snooping=disabled
           mac_auth=disabled fail_through_mode=disabled sta_info=0/0
           mac=local, tunnel=8023, cap=8ce0, qos=disabled
           prob_resp_suppress=disabled
           rx sop=disabled
           sticky client remove=disabled
           mu mimo=enabled           ldpc_config=rxtx
           dhcp_option43_insertion=enabled           dhcp_option82_insertion=disabled
           dhcp_enforcement=disabled
           access_control_list=disabled
           bc_suppression=dhcp dhcp-ucast arp
           auth=WPA3 Enterprise Only, RADIUS, AES WPA keyIdx=6, keyLen=16, keyStatus=1,
gTsc=000000000000
           key=92c6ab16 9239a724 bd20eaad e677d35c
           pmf=required
           beacon_prot=enabled
```

The following Beacon frame capture shows the FortiAP adds a message integrity check (MIC) element to the Beacon frames of SSID with Beacon Protection enabled:

```
IEEE 802.11 Wireless Management
    Fixed parameters (12 bytes)
    Tagged parameters (509 bytes)
```

```
        Tag: SSID parameter set: wpa3-sae-beacon
        Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
        Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
        Tag: Country Information: Country Code US, Environment Indoor
        Tag: Power Constraint: 0
        Tag: TPC Report Transmit Power: 24, Link Margin: 0
        Tag: Extended Supported Rates Unknown Rate, [Mbit/sec]
        Tag: RSN Information
        Tag: QBSS Load Element 802.11e CCA Version
        Tag: RM Enabled Capabilities (5 octets)
        Tag: HT Capabilities (802.11n D1.10)
        Tag: HT Information (802.11n D1.10)
        Tag: Extended Capabilities (13 octets)
        Tag: VHT Capabilities
        Tag: VHT Operation
        Tag: VHT Tx Power Envelope
        Tag: Reserved (201): Undecoded
        Tag: Reserved (244): Undecoded
        Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
        Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)
        Ext Tag: Spatial Reuse Parameter Set
        Ext Tag: MU EDCA Parameter Set
        Tag: Vendor Specific: Qualcomm Inc.
        Tag: Vendor Specific: Fortinet Inc.
        Tag: Vendor Specific: Fortinet Inc.
        Tag: Vendor Specific: Fortinet Inc.
        Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
        Tag: Vendor Specific: Qualcomm Inc.
        Tag: Vendor Specific: Qualcomm Inc.
        Tag: Management MIC
            Tag Number: Management MIC (76)
            Tag length: 16
            KeyID: 6
            IPN: a00300000000
            MIC: 0cc6d9f2580036f1
```

The 11th octet in "Extended Capabilities" has the Beacon Protection Flag enabled.

```
Tag: Extended Capabilities (13 octets)
            Tag Number: Extended Capabilities (127)
            Tag length: 13
            Extended Capabilities: 0x04 (octet 1)
            Extended Capabilities: 0x00 (octet 2)
            Extended Capabilities: 0x0f (octet 3)
            Extended Capabilities: 0x02 (octet 4)
            Extended Capabilities: 0x00 (octet 5)
            Extended Capabilities: 0x00 (octet 6)
            Extended Capabilities: 0x00 (octet 7)
            Extended Capabilities: 0x0040 (octets 8 & 9)
            Extended Capabilities: 0x40 (octet 10)
            Extended Capabilities: 0x10 (octet 11)
                .... ...0 = Complete List of NonTxBSSID Profiles: False
                .... ..0. = SAE Password Identifiers In Use: False
                .... .0.. = SAE Passwords Used Exclusively: False
                .... 0... = Enhanced Multi-BSSID Advertisement Support: False
                ...1 .... = Beacon Protection Enabled: True
                ..0. .... = Mirrored SCS: False
```

```
                .0.. .... = OCT: False
                0... .... = Local MAC Address Policy: False
            Extended Capabilities: 0x00 (octet 12)
            Extended Capabilities: 0x00 (octet 13)
```

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 and Switch Controller* > *SSIDs* 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 methods:

- VLAN assignment by RADIUS on page 104
- VLAN assignment by Name Tag on page 106
- VLAN assignment by FortiAP group on page 109
- VLAN assignment by VLAN pool on page 110

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

Attribute type	Attributes value	Note
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 33. You can assign via name tag. See VLAN assignment by Name Tag on page 106.

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 & Authentication* > *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 and Switch Controller* > *SSIDs*, 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 33.

To create the FortiAP profile for the dynamic VLAN SSID:

1. Go to *WiFi and 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 and 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 Name Tag

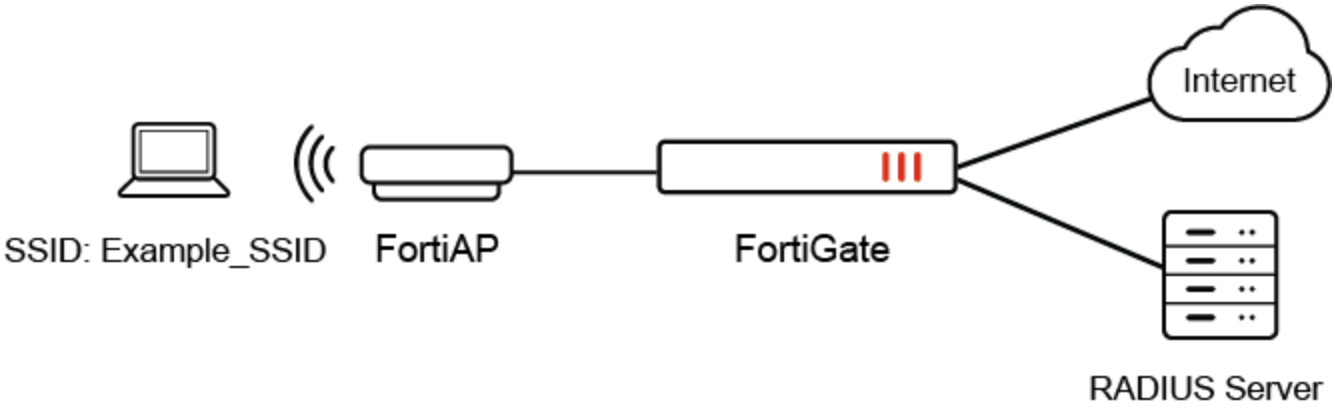
Typically, users can be assigned to VLANs dynamically according to the Tunnel-Private-Group-Id RADIUS attribute returned from the Access-Accept message. The value can either match a particular VLAN-ID on a VLAN interface, or a text string that matches a VLAN interface name.

However, there is a another option to match based on a `vlan-name` table defined under the virtual AP. You can assign either a single VLAN ID per name, or assign multiple VLAN IDs per name, up to a maximum of 8 VLAN IDs. When assigning multiple VLAN IDs, the ID is determined by a Round-robin method to ensure optimal utilization of VLAN resources.

Example use case

In the following example scenario, the customer site has set up the following topology:

- FortiAP broadcasts a bridge mode SSID with `dynamc-vlan` enabled;
- FortiGate needs to assign VLAN-ID=100 to the client if vlan-name is "voip", and assign multiple VLAN-IDs to the client if vlan-name is "data".



VLAN Name	VLAN ID
`data`	100, 200, 300 You can assign up to 8 VLAN IDs.
`voip`	100

Instead of creating VLAN interfaces on the FortiGate and naming them "data" and "voip" respectively, you can add the `vlan-name` table in the SSID:

To configure assigning VLAN IDs by VLAN name tag:

1. Set up an SSID with `dynamic-vlan` enabled, and configure `vlan-name` with the IDs you want to assign under `vlan-id`.

```
config wireless-controller vap
  edit "wifi.fap.02"
    set ssid "Example_SSID"
    set security wpa2-only-enterprise
    set voice-enterprise disable
    set auth radius
    set radius-server "peap"
    set schedule "always"
    set dynamic-vlan enable
    config vlan-name
```

```
      edit "data"
        set vlan-id 100 200 300
      next
      edit "voip"
        set vlan-id 100
      next
    end
  next
end
```

2. Create user accounts in the Radius server with the `Tunnel-Private-Group-Id` matching the previously configured `vlan-name`.

```
data      Cleartext-Password := "123456"
          Tunnel-Type = "VLAN",
          Tunnel-Medium-Type = "IEEE-802",
          Tunnel-Private-Group-Id = data

voip      Cleartext-Password := "123456"
          Tunnel-Type = "VLAN",
          Tunnel-Medium-Type = "IEEE-802",
          Tunnel-Private-Group-Id = voip
```

Once wireless clients connect to the SSID, the FortiGate wireless controller assigns VLAN ID based on its `Tunnel-Private-Group-Id`. If the `Tunnel-Private-Group-Id` is "voip", it will be assigned to VLAN ID 100. If the `Tunnel-Private-Group-Id` is "data", it will be assigned to either VLAN ID 100, 200, 300.

To verify the clients connect and are assigned to the correct VLAN ID:

1. Connect four WiFi clients with `user=data` to verify that they can be assigned to the VLAN IDs from the VLAN Pool 100, 200, and 300 using a Round-robin method:
   a. Connect the first client and verify that it is assigned VLAN ID 100.

```
vf=2 mpId=6 wtp=2 rId=2 wlan=wifi.fap.02 vlan_id=100 ip=100.1.10.2 ip6=::
mac=00:0e:c9:9f:77:04 vci= host= user=data group= signal=-40 noise=-95 idle=25 bw=0
use=5 chan=48 radio_type=11N_5G security=wpa2_only_enterprise mpsk= encrypt=aes cp_
authed=no l3r=1,0 G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

   b. Connect the second client and verify that it is assigned VLAN ID 200.

```
vf=2 mpId=6 wtp=2 rId=2 wlan=wifi.fap.02 vlan_id=200 ip=100.2.10.2 ip6=::
mac=00:0e:ce:2d:e0:dd vci= host= user=data group= signal=-40 noise=-95 idle=0 bw=0
use=5 chan=48 radio_type=11N_5G security=wpa2_only_enterprise mpsk= encrypt=aes cp_
authed=no l3r=1,0 G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

   c. Connect the third client and verify that it is assigned VLAN ID 300.

```
vf=2 mpId=6 wtp=2 rId=2 wlan=wifi.fap.02 vlan_id=300 ip=100.3.10.2
ip6=fe80::20e:95ff:fef3:f124 mac=00:0e:95:f3:f1:24 vci= host= user=data group=peap
signal=-41 noise=-95 idle=0 bw=0 use=5 chan=48 radio_type=11N_5G security=wpa2_only_
enterprise mpsk= encrypt=aes cp_authed=no l3r=1,0 G=0.0.0.0:0,1.149.24.1:39198-0-0 --
0.0.0.0:0 0,0 online=yes mimo=2
```

   d. Connect the fourth client and verify that it is assigned VLAN ID 100 again.

```
vf=2 mpId=6 wtp=2 rId=2 wlan=wifi.fap.02 vlan_id=100 ip=100.1.10.3 ip6=::
mac=00:0e:44:9e:71:e5 vci= host= user=data group= signal=-40 noise=-95 idle=29 bw=0
```

```
use=5 chan=48 radio_type=11N_5G security=wpa2_only_enterprise mpsk= encrypt=aes cp_
authed=no l3r=1,0 G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

2. As a comparison, connect two WiFi clients stations with `user=voip`. They are assigned VLAN ID 100 as it matches the VLAN name "voip".

```
vf=2 mpId=6 wtp=2 rId=2 wlan=wifi.fap.02 vlan_id=100 ip=100.1.10.5
ip6=fe80::20e:5cff:fe03:e411 mac=00:0e:5c:03:e4:11 vci= host= user=voip group=peap
signal=-43 noise=-95 idle=14 bw=0 use=5 chan=48 radio_type=11N_5G security=wpa2_only_
enterprise mpsk= encrypt=aes cp_authed=no l3r=1,0 G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0
0,0 online=yes mimo=2

vf=2 mpId=6 wtp=2 rId=2 wlan=wifi.fap.02 vlan_id=100 ip=100.1.10.4 ip6=::
mac=f8:e4:e3:d8:5e:af vci= host=WiFi-Client-2 user=voip group=peap signal=-39 noise=-95
idle=4 bw=0 use=5 chan=48 radio_type=11AX_5G security=wpa2_only_enterprise mpsk=
encrypt=aes cp_authed=no l3r=1,0 G=0.0.0.0:0,2.3.81.76:29193-0-0 -- 0.0.0.0:0 0,0
online=yes mimo=2
```

3. Check the VLAN assignment count using the following diagnostic command: `Diagnose wpa wpd vlan-name <SSID_NAME>`.

```
# diagnose wpa wpad vlan-name Example_SSID
No SSID is configured in hostapd.
No SSID is configured in hostapd.
SSID config: SSID(Example_SSID) VAP(wifi.fap.02) refcnt(2)
        Vlan info (1): v100.wifi => 100
        Vlan info (2): v200.wifi => 200
        Vlan info (3): v300.wifi => 300
        Vlan info (4): wqtn.50.wifi.fa => 4093
        Vlan info (5): data => 100(2) 200(1) 300(1)
        Vlan info (6): voip => 100(2)
```

VLAN assignment by FortiAP group

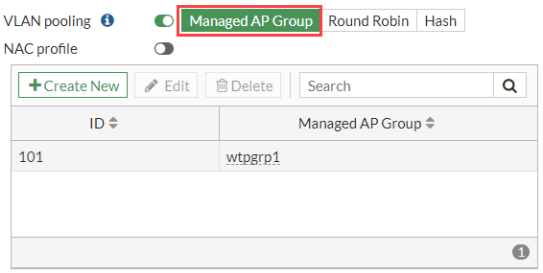
VLANs can be assigned dynamically based on FortiAP groups. Dynamic VLAN assignment allows the same SSID to be deployed to many APs, avoiding the need to produce multiple SSIDs.

You can create FortiAP groups to manage multiple APs at once. Grouping an AP enables you to apply assign VLANs to all the APs in that group, simplifying the administrative workload. For example, you can group APs based on the floor or section of the office they are installed on. Each AP can belong to one group only. This feature is useful in large deployments as you can break down the broadcast domain, rather than putting all wireless clients into a single subnet. You can also apply security inspections and firewall rules based on the location of the wireless clients, providing you with more granular control over wireless traffic.

To create a FortiAP group, navigate to *WiFi and Switch Controller* > *Managed FortiAPs* and click *Create New* > *Managed AP Group*.

To assign a VLAN by FortiAP group - GUI:

1. Navigate to *WiFi and Switch Controller* > *SSIDs* to define an SSID.
2. Enable *VLAN Pooling* and select *Managed AP Group* to assign a VLAN ID to a specified group.
   You can also choose other methods of assigning VLAN IDs (see Load balancing on page 110).
3. Click *Create New* to enter the VLAN ID you want to assign and the AP group you want to apply the ID to.



4. Click *OK* to save.

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
```

VLAN assignment by VLAN pool

You can define VLAN pooling and load balancing VLANs on the SSID configuration page. FortiGate automatically adds all load balancing VLANs to a zone based on the SSID they were defined in. VLANs are tied to the SSID interface, the zone name includes the SSID interface name followed by `.zone`. You must configure the network and DHCP options for each VLAN ID.

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 33.

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

Load balancing

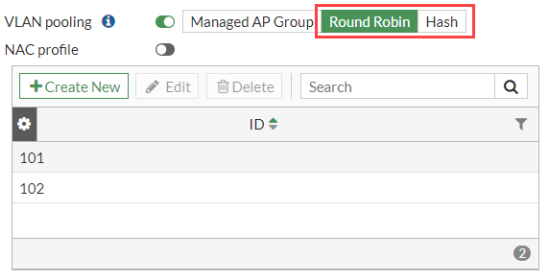
VLAN pooling load balancing is available only for SSIDs operating in tunnel mode. There are two VLAN pooling methods available to provide load balancing options for wireless clients:

- **Round robin** - Assigns the least busy VLAN (the VLAN with the smallest number of clients) to new clients from the VLAN pool.

- **Hash** - Identifies which VLAN to use based on the hash value of the current number of clients connected to the SSID and the number of VLANs available in the pool.

To assign a VLAN load balancing method - GUI:

1. Navigate to *WiFi and Switch Controller* > *SSIDs* to define an SSID.
2. Enable *VLAN Pooling* and select a load balancing method.
   - *Round Robin*: Assigns the next VLAN ID to each device as it is detected.
   - *Hash*: Always assigns the same VLAN ID to a specific device.



3. Click *Create New* to enter the VLAN ID you want to assign.
4. Click *OK* to save.

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 wireless NAC support

The wireless controller can support Network Access Control (NAC) profiles to onboard wireless clients into default VLANs. It can also apply NAC policies to match clients based on device properties, user groups, or EMS tags, and then assign the clients to specific VLANs. VLAN subinterfaces based on VAP interfaces are used for the VLAN assignments.

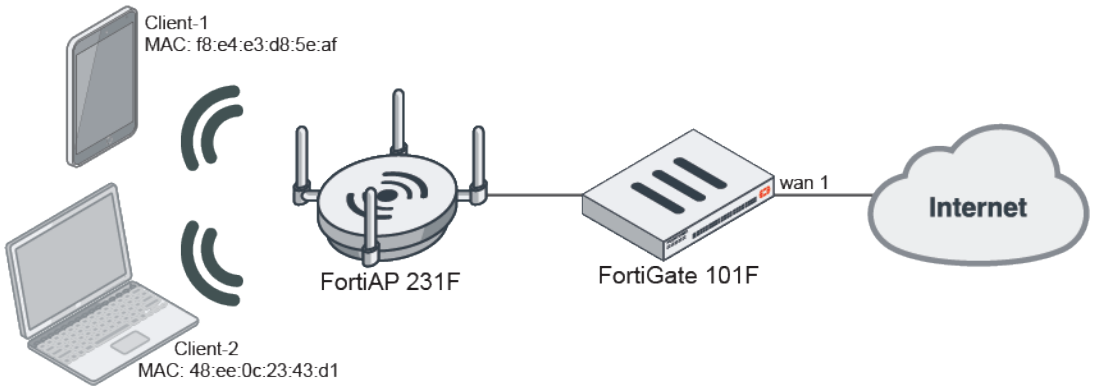
When a wireless client first connects, it is assigned to the default VLAN per the NAC profile. After the client information is captured, if it matches a NAC policy, the client is disconnected and, when it reconnects, assigned to the VLAN that is specified by the SSID policy.

The device properties that can be matched include: MAC address, hardware vendor, type, family, operating system, hardware version, software version, host, user, and source.

Example

When both clients first connect, they are onboarded into the `vap_v100` VLAN. The client information is captured after up to two minutes and, if it matches the NAC policy, the wireless controller disconnects the client. When the client reconnects, it is assigned to the VLAN specified by the policy.

In this example, NAC profiles are configured to onboard wireless Client-1 into default VLANs based on the device's MAC address, user group, or EMS tag.



To configure the VAP, interfaces, profiles, and SSID policy in the GUI:

1. Go to *WiFi & and Switch Controller* > *NAC Policies* and click *Create New* to create a NAC policy.
2. Enter a *Name* for the NAC policy and select what Category you want to base the NAC policy on (Device, User, EMS Tag).
3. Configure the policy device patterns based on the Category you selected.
4. In the Wireless Controller Action section, enable *Assign VLAN* and select which VLAN you want to apply to the policy.
5. When you are finished, click *OK*.
6. Go to *WiFi and Switch Controller* > *SSIDs* and select the SSID you want to apply the NAC policy to.
7. Enable *NAC profile* and select the NAC policy you want to apply.
8. Click *OK* to apply the changes.

To configure the VAP, interfaces, profiles, and SSID policy in the CLI:

1. Create the VAP SSID:

```
config wireless-controller vap
    edit "wifi.fap.01"
        set ssid "wifi-ssid.fap.01"
        set passphrase **********
        set schedule "always"
    next
end
```

2. Create two VLAN interfaces under the VAP:

```
config system interface
    edit "vap_v100"
        set vdom "vdom1"
        set ip 10.100.1.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 37
        set interface "wifi.fap.01"
        set vlanid 100
    next
    edit "vap_v200"
        set vdom "vdom1"
        set ip 10.101.1.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 40
        set interface "wifi.fap.01"
        set vlanid 200
    next
end
```

3. Create the wireless NAC profile:

```
config wireless-controller nac-profile
    edit "wifi-nac-profile-1"
        set onboarding-vlan "vap_v100"
    next
end
```

4. Select the wireless NAC profile in the VAP:

```
config wireless-controller vap
    edit "wifi.fap.01"
        set nac enable
        set nac-profile "wifi-nac-profile-1"
    next
end
```

5. Create the SSID policy:

```
config wireless-controller ssid-policy
    edit "wifi-ssid-policy-1"
        set vlan "vap_v200"
```

```
    next
end
```

6. Create NAC policies to match clients based on Device properties, User groups, or EMS tags.

Device properties

This policy matches clients with the MAC address `f8:e4:e3:d8:5e:af`.

To match a wireless client based on its MAC address:

1. Create a NAC policy that matches wireless clients with a specific MAC address:

```
config user nac-policy
    edit "wifi-nac-policy-1"
        set category device
        set mac "f8:e4:e3:d8:5e:af"
        set ssid-policy "wifi-ssid-policy-1"
    next
end
```

When both clients first connect, they are onboarded into the `vap_v100` VLAN:

```
# diagnose wireless-controller wlac -d sta online
   vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.10 ip6=::
mac=f8:e4:e3:d8:5e:af vci= host=fosqa-PowerEdge-R210 user= group= signal=-45 noise=-95
idle=1 bw=2 use=6 chan=157 radio_type=11AX_5G security=wpa2_only_personal mpsk=
encrypt=aes cp_authed=no online=yes mimo=2
   vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.11 ip6=::
mac=48:ee:0c:23:43:d1 vci= host=wifi-qa-01 user= group= signal=-25 noise=-95 idle=14
bw=0 use=6 chan=157 radio_type=11AC security=wpa2_only_personal mpsk= encrypt=aes cp_
authed=no online=yes mimo=2
```

After the client information is collected, Client-1 matches the policy. It is disconnected, then reconnects and is assigned to the `vap_v200` VLAN in accordance with the NAC policy:

```
# diagnose wireless-controller wlac -d sta online
   vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=200 ip=10.101.1.10 ip6=::
mac=f8:e4:e3:d8:5e:af vci= host=fosqa-PowerEdge-R210 user= group= signal=-24 noise=-95
idle=0 bw=7 use=6 chan=157 radio_type=11AX_5G security=wpa2_only_personal mpsk=
encrypt=aes cp_authed=no online=yes mimo=2
   vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.11 ip6=::
mac=48:ee:0c:23:43:d1 vci= host=wifi-qa-01 user= group= signal=-25 noise=-95 idle=0 bw=4
use=6 chan=157 radio_type=11AC security=wpa2_only_personal mpsk= encrypt=aes cp_
authed=no online=yes mimo=2
```

2. Verify that Client-1 matched the policy, and Client-2 did not:

```
# diagnose wireless-controller wlac_hlp -c sta-nac

STA (001/002) vfid,mac: 1, 48:ee:0c:23:43:d1
    ip                    : 10.100.1.11
    wlan                  : wifi.fap.01(tunnel)
    vlan-id(oper/dflt)    : 100/100
    matched nac-policy    : N/A
STA (002/002) vfid,mac: 1, f8:e4:e3:d8:5e:af
    ip                    : 10.101.1.10
```

```
    wlan                  : wifi.fap.01(tunnel)
    vlan-id(oper/dflt)    : 200/100
    matched nac-policy    : wifi-nac-policy-1
```

User groups

This policy matches clients that are authenticated in the `group_local` user group.

To match a wireless client based on its user group:

1. Change the security mode to WPA2 enterprise only and add a user group in the VAP:

```
config wireless-controller vap
    edit "wifi.fap.01"
        set security wpa2-only-enterprise
        set auth usergroup
        set usergroup "group_local" "group_radius"
        set schedule "always"
    next
end
```

2. Create a NAC policy that matches wireless clients that are authenticated in a specific user group:

```
config user nac-policy
    edit "wifi-nac-policy-2"
        set category firewall-user
        set user-group "group_local"
        set ssid-policy "wifi-ssid-policy-1"
    next
end
```

When both clients first connect, they are onboarded into the `vap_v100` VLAN:

```
# diagnose wireless-controller wlac -d sta online
   vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.10 ip6=::
mac=f8:e4:e3:d8:5e:af vci= host=fosqa-PowerEdge-R210 user=local group=group_local
signal=-45 noise=-95 idle=1 bw=2 use=6 chan=157 radio_type=11AX_5G security=wpa2_only_
enterprise mpsk= encrypt=aes cp_authed=no online=yes mimo=2
   vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.11 ip6=::
mac=48:ee:0c:23:43:d1 vci= host=wifi-qa-01 user=tester group=group_radius signal=-24
noise=-95 idle=27 bw=0 use=6 chan=157 radio_type=11AC security=wpa2_only_enterprise
mpsk= encrypt=aes cp_authed=no online=yes mimo=2
```

After the client information is collected, Client-1 matches the policy. It is disconnected, then reconnects and is assigned to the `vap_v200` VLAN in accordance with the NAC policy:

```
# diagnose wireless-controller wlac -d sta online
   vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=200 ip=10.101.1.10 ip6=::
mac=f8:e4:e3:d8:5e:af vci= host=fosqa-PowerEdge-R210 user=local group=group_local
signal=-20 noise=-95 idle=1 bw=9 use=6 chan=157 radio_type=11AX_5G security=wpa2_only_
enterprise mpsk= encrypt=aes cp_authed=no online=yes mimo=2
   vf=1 wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=100 ip=10.100.1.11 ip6=::
mac=48:ee:0c:23:43:d1 vci= host=wifi-qa-01 user=tester group=group_radius signal=-24
noise=-95 idle=35 bw=0 use=6 chan=157 radio_type=11AC security=wpa2_only_enterprise
mpsk= encrypt=aes cp_authed=no online=yes mimo=2
```

3. Verify that Client-1 matched the policy, and Client-2 did not:

```
# diagnose wireless-controller wlac_hlp -c sta-nac

STA (001/002) vfid,mac: 1, 48:ee:0c:23:43:d1
    ip                    : 10.100.1.11
    wlan                  : wifi.fap.01(tunnel)
    vlan-id(oper/dflt)    : 100/100
    matched nac-policy    : N/A
STA (002/002) vfid,mac: 1, f8:e4:e3:d8:5e:af
    ip                    : 10.101.1.10
    wlan                  : wifi.fap.01(tunnel)
    vlan-id(oper/dflt)    : 200/100
    matched nac-policy    : wifi-nac-policy-2
```

EMS tags

This policy matches clients that have the specified EMS tag. EMS control must already be configured, refer to Synchronizing FortiClient EMS tags and configurations for details.

To match a wireless client based on its EMS tag:

1. Find the EMS tag:

```
# diagnose firewall dynamic list
MAC_FCTEMSTA20002318_ems135_winOS_tag(total-addr: 2): ID(62)
        MAC(F0:B4:D2:AB:E0:09)
        MAC(10:C3:7B:9C:46:AA)
```

2. Create a NAC policy that matches a wireless client with that tag:

```
config user nac-policy
    edit "wifi-nac-policy-3"
        set category ems-tag
        set ems-tag "MAC_FCTEMSTA20002318_ems135_winOS_tag"
        set ssid-policy "wifi-ssid-policy-1"
    next
end
```

When both clients first connect, they are onboarded into the `vap_v100` VLAN. After the client information is collected, Client-1 matches the policy. It is disconnected, then reconnects and is assigned to the `vap_v200` VLAN in accordance with the NAC policy:

```
# diagnose wireless-controller wlac -d sta online
  wtp=1 rId=2 wlan=wifi.fap.01 vlan_id=200 ip=10.101.1.11 ip6=fe80::add7:9b4a:cd39:e65c
mac=f0:b4:d2:ab:e0:09 vci=MSFT 5.0 host=DESKTOP-05HBKE1 user= group= signal=-52 noise=-
95 idle=6 bw=0 use=6 chan=40 radio_type=11AC(wave2) security=wpa2_only_personal mpsk=
encrypt=aes cp_authed=no online=yes mimo=2
                ip6=*fe80::add7:9b4a:cd39:e65c,256,
```

3. Verify that Client-1 matched the policy, and Client-2 did not:

```
# diagnose wireless-controller wlac_hlp -c sta-nac

STA (001/002) vfid,mac: 1, 48:ee:0c:23:43:d1
    ip                    : 10.100.1.11
    wlan                  : wifi.fap.01(tunnel)
    vlan-id(oper/dflt)    : 100/100
```

```
    matched nac-policy    : N/A
STA (002/002) vfid,mac: 1, f8:e4:e3:d8:5e:af
    ip                    : 10.101.1.10
    wlan                  : wifi.fap.01(tunnel)
    vlan-id(oper/dflt)    : 200/100
    matched nac-policy    : wifi-nac-policy-3
```

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.

You can use the following methods to authenticate connecting clients:

- WPA2 and WPA3 Enterprise authentication on page 117
  - Custom RADIUS NAS-ID on page 119
- WiFi single sign-on (WSSO) authentication on page 122
- Assigning WiFi users to VLANs dynamically on page 122
- MAC-based authentication on page 123
- User self-registration of MPSKs through FortiGuest on page 128
- Authenticating guest WiFi users on page 130
- Authenticating wireless clients with SAML credentials
  - You can configure SAML user groups and apply it to a captive portal through a tunnel mode SSID. Then you can configure both a captive portal exempt firewall policy to allow wireless clients to contact the SAML IDP and a firewall policy with the SAML user group applied to allow authenticated traffic. When wireless clients connect to the SSID, they will be redirected to a login page for wireless authentication using SAML.

    For configuration information, see Captive portal authentication using SAML credentials on page 83.
- 802.1X authentication
  - Configuring 802.1X supplicant on LAN on page 130
  - Configure NAS-Filter-Rule attribute to set up dACL on page 135

WPA2 and WPA3 Enterprise authentication

WEP and WPA-Personal security rely on legitimate users knowing the correct key or passphrase for the wireless network. However, 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.

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.

WPA3 improves on WPA2 and offers some transition modes where a single SSID supports corresponding WPA3 and WPA2 devices. WPA3 is required by the Wi-Fi Alliance for Wi-Fi 6 and 7 certifications, so all Wi-Fi 6 and 7 certified

devices support it. From the administrative and the end-user experiences, WPA3 Enterprise is identical to WPA2-Enterprise.

If your WiFi network uses WPA2 or WPA3 Enterprise authentication verified by a RADIUS server, you need to configure the FortiGate unit to connect to that RADIUS server.

To configure a RADIUS server - GUI:

1. Go to *User & Authentication* > *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. Select an *Authentication method*.
4. In *Primary Server* area:
   a. *IP/Name:* Enter the IP address or resolvable FQDN of the RADIUS server.
   b. *Secret*: Enter the password used to connect to the RADIUS server.
5. Optionally, enter the information for a secondary or backup RADIUS server.
6. Select *OK*.

To configure a RADIUS server - CLI:

Advanced settings for RADIUS servers can be configured in the CLI.

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

You can configure RADSEC over TLS and TCP for 802.1X authentication of wireless clients. For more information, refer to Configuring a RADSEC client in the *FortiOS Administration Guide*.

To implement WPA2 or WPA3 Enterprise security:

1. Apply the RADIUS server you configured to a WPA2 or WPA3 Enterprise SSID.
   a. To configure from the GUI, seeDefining a wireless network interface (SSID) on page 43.
   b. To configure from the CLI:

```
config wireless-controller vap
  edit "wifi.fap.01"
    set ssid "FOS_101F_Enterprise"
    set security wpa2-only-enterprise
    set auth radius
    set radius-server "exampleRADIUS"
    set schedule "always"
  next
end
```

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. For instructions on how to configure locally stored user groups, see Basic wireless network example on page 342.
- 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.

Custom RADIUS NAS-ID

You can configure the RADIUS NAS-ID as a custom ID or the hostname. When deploying a wireless network with WPA-Enterprise and RADIUS authentication, or using the RADIUS MAC authentication feature, FortiGate can use the custom NAS-ID in its Access-Request.

The FortiGate can also push the RADIUS NAS-ID to a managed FortiAP in standalone mode. The FortiAP can then forward the NAS-Identifier value in an Access-Request packet when authenticating a wireless client with a remote RADIUS server.

The FortiAP must run on firmware 7.6.0 or later to receive the NAS-Identifier value from the FortiGate.

Configuring RADIUS NAS-ID CLI:

```
config user radius
  edit < server >
    set nas-id-type { legacy | custom | hostname }
    set nas-id < custom ID >
  next
end
```

You can configure `nas-id-type` with the following three options:

`legacy`	NAS-ID value is the value previously used by each daemon. This is the default setting.
`custom`	NAS-ID value is customized. Set `nas-id` to enter the custom ID.
`hostname`	NAS-ID value is the FortiGate hostname or HA group name if applicable.

To create an SSID with WPA2-Enterprise security mode using RADIUS authentication:

1. Configure the SSID:

```
config wireless-controller vap
 edit "wifi7"
   set ssid "80F_ent_radius"
   set security wpa2-only-enterprise
   set voice-enterprise disable
   set auth radius
   set radius-server "server-55"
   set schedule "always"
 next
end
```

2. Configure the RADIUS server:

```
config user radius
 edit "server-55"
   set server "172.18.56.104"
   set secret ENC *
   set acct-interim-interval 60
   set radius-coa enable
   config accounting-server
     edit 1
       set status enable
       set server "172.18.56.104"
       set secret ENC *
     next
   end
 next
end
```

3. Set the `nas-id-type`:

```
config user radius
  edit server-55
    set nas-id-type hostname
 next
end

config system global
  set hostname "FortiWiFi-80F-2R"
end
```

4. After the station connects to the SSID, check the radius packets to confirm the NAS-Identifier value matches the hostname FortiWiFi-80F-2R:

```
(64) Received Access-Request Id 35 from 172.16.200.254:63111 to 172.16.200.55:1812
length 367
(64)   User-Name = "tester"
(64)   NAS-IP-Address = 0.0.0.0
(64)   NAS-Identifier = "FortiWiFi-80F-2R"
```

To create a WPA2-Personal SSID using RADIUS MAC authentication:

1. Configure the SSID:

```
config wireless-controller vap
  edit "wifi2"
    set ssid "80F_psk"
    set voice-enterprise disable
    set radius-mac-auth enable
    set radius-mac-auth-server "server-55"
    set passphrase ENC *
    set schedule "always"
  next
end
```

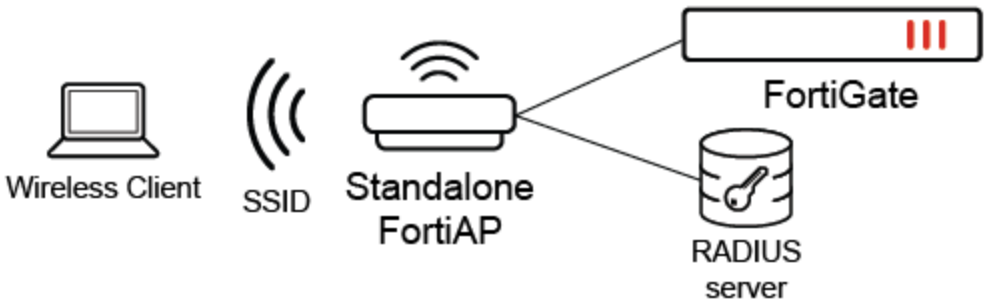
2. Set the `nas-id-type`:

```
config user radius
  edit server-55
    set nas-id-type custom
    set nas-id FWF-80F-LR
  next
end
```

3. After the station connects to the SSID, check the radius packets to confirm the NAS-Identifier value matches the custom value you configured, "FWF-80F-LR":

```
(87) Received Access-Request Id 3 from 172.16.200.254:62884 to 172.16.200.55:1812 length
228
(87)   User-Name = "F1-A4-23-75-9F-B1"
(87)   User-Password = "F1-A4-23-75-9F-B1"
(87)   Calling-Station-Id = "F1-A4-23-75-9F-B1"
(87)   NAS-IP-Address = 0.0.0.0
(87)   NAS-Identifier = "FWF-80F-LR"
```

To configure and push a NAS-ID to a FortiAP in standalone mode:



1. From FortiOS, configure the RADIUS server with a NAS-ID. You can use custom or hostname NAS-IDs.

```
config user radius
  edit "wifi-radius"
    set server "172.16.200.55"
    set secret ENC
    set nas-ip 172.16.200.9
    set nas-id-type custom
```

```
    set nas-id "AP-431F"
  next
end
```

2. Apply the RADIUS server to an SSID.

```
config wireless-controller vap
  edit "stand-vap"
    set ssid "FOS_101F_Stand_Ent_Radius"
    set security wpa2-only-enterprise
    set auth radius
    set radius-server "wifi-radius"
    set local-standalone enable
    set local-bridging enable
    set schedule "always"
  next
end
```

3. When the client connects to the SSID, the NAS-Identifier attribute you configured, *AP-431F*, will be sent in an Access-Request packet.

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 and WPA3 Enterprise authentication on page 117.
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.

For configuration information see, Configuring WiFi with WSSO using Windows NPS and user groups on page 95.

When a user authenticates by WSSO, the Firewall Users widget (*Dashboard* > *Users & Device*) 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

You can authenticate wireless clients 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
```

See also Adding a MAC filter on page 89

Combined MAC and MPSK based authentication

You can also use a combined MAC and MPSK based authentication to authenticate wireless clients against a RADIUS server. Instead of statically storing the MPSK passphrase(s) on the FortiGate, it can be passed from the RADIUS server dynamically when the client MAC is authenticated by the RADIUS server. The resulting passphrase will be cached on the FortiGate for future authentication, with a timeout configured for each VAP.

When a WiFi client attempts to connect to a SSID and inputs a password, the user is "registered" to the RADIUS server which stores the client's MAC and generates a passphrase for the user device or group. When the user connects to the FortiAP SSID using WPA2-Personal, the FortiGate wireless controller will dynamically authenticate the device's MAC address using RADIUS-based MAC authentication.

If authentication is successful, the RADIUS server will return a tunnel-password for that user device or group. If the client-provided passphrase matches this password, it can successfully connect to the SSID and be placed in a VLAN (if specified).

To implement MAC and MPSK based authentication, you must first configure the RADIUS server and MPSK profile. Then you can configure authentication based on how the client connects to the SSID.

To configure the RADIUS server and MPSK profile:

1. Configure a RADIUS server:

```
config user radius
  edit "peap"
    set server "172.16.200.55"
    set secret ********
  next
end
```

2. Configure the MPSK profiles from the GUI or CLI.
   - From the GUI:
     i. Go to *System* > *Feature Visibility* and enable *Advanced Wireless Features*.
     ii. Click *Apply*.
     iii. Go to *WiFi & Switch Controller* > *Connectivity Profiles* > *MPSK Profiles* and click *Create new* to create an MPSK profile.
     iv. Enter an MPSK profile *Name* and select a security *Type*.
     v. Under *MPSK group list*, click *Add* > *Create Group* to create a new MPSK Group.
     vi. Enter your MPSK group and key configurations as needed.
     vii. Click *OK* to save your MPSK profile configurations.
     viii. Go to *WiFi & Switch Controller* > *SSIDs* and select or create a new SSID.
     ix. Under *Security Mode Settings*, select the *Security mode* and *SAE password* that matches your MPSK profile.
     x. Select the *MPSK profile* you created.
     xi. When you are finished, click *OK*.
   - From the CLI:

```
i. config wireless-controller mpsk-profile
     edit "wifi.fap.01"
       set ssid "wifi-ssid.fap.01"
       config mpsk-group
         edit "g1"
           config mpsk-key
             edit "p1"
               set passphrase ********
               set mpsk-schedules "always"
             next
           end
         next
       end
     next
     edit "wifi.fap.02"
       set ssid "wifi-ssid.fap.02"
       config mpsk-group
         edit "g1"
           config mpsk-key
             edit "p1"
               set passphrase ********
               set mpsk-schedules "always"
             next
           end
```

```
            next
          end
        next
      end
```

3. Check that the PMK values from the RADIUS server are cached on the FortiGate:

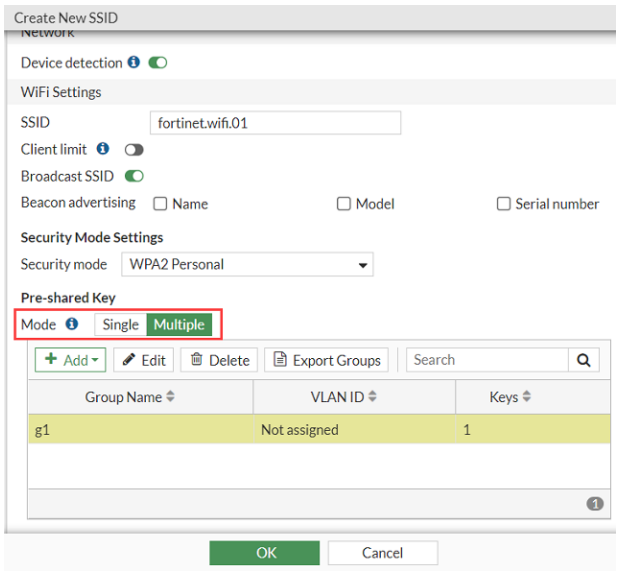
```
show wireless-controller mpsk-profile
  edit "wifi.fap.01"
    set ssid "wifi-ssid.fap.01"
    config mpsk-group
      edit "g1"
        config mpsk-key
          edit "p1"
            set passphrase *****
            set pmk ENC ***
            set mpsk-schedules "always"
          next
        end
      next
    end
  next
  edit "wifi.fap.02"
    set ssid "wifi-ssid.fap.02"
    config mpsk-group
      edit "g1"
        config mpsk-key
          edit "p1"
            set passphrase ****
            set pmk ENC ***
            set mpsk-schedules "always"
          next
        end
      next
    end
  next
end
```

After you've configured the RADIUS server and MPSK profile, you can configure MAC and MPSK based authentication based on how the client connects to the SSID:

- If the client connects to the SSID in tunnel mode, the MPSK key is cached on the FortiGate.
- If the client connects to the SSID in bridging mode, the MPSK key is cached on the FortiAP.

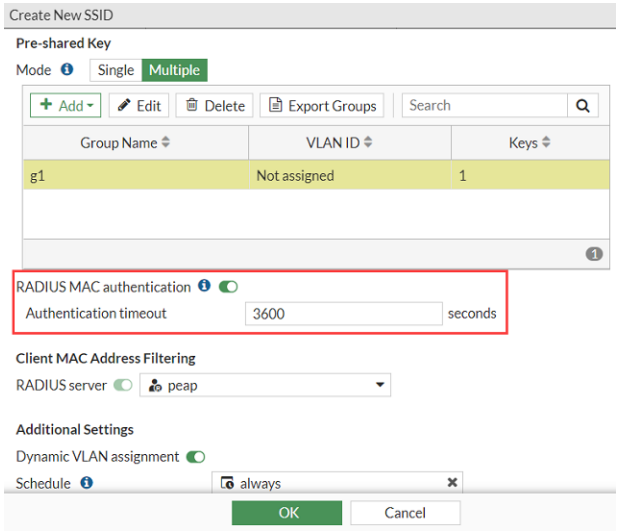
To enable the RADIUS MAC Authentication - GUI:

1. Go to *WiFi & Switch Controller* > *SSIDs*, and click *Create New* > *SSID* or edit an existing SSID.
2. In *Security mode*, select *WPA2 Personal*.
3. Under *Pre-shared Key Mode*, select *Multiple*.



4. Enable *RADIUS MAC authentication*.

   The Authentication timeout field loads. You can change the timer from 1800 to 86400 seconds.



5. Enable *RADIUS server* and select a server.
6. When you are finished, click *OK*.

To configure MAC and MPSK authentication in tunnel mode:

1. Configure the wireless controller VAP, enable `radius-mac-auth`, and select a profile for `mpsk-profile`:

```
config wireless-controller vap
   edit "wifi.fap.01"
      set ssid "wifi-ssid.fap.01"
      set radius-mac-auth enable
      set radius-mac-auth-server "peap"
      set radius-mac-mpsk-auth enable
      set radius-mac-mpsk-timeout 1800
      set schedule "always"
      set mpsk-profile "wifi.fap.01"
```

```
    next
end
```

2. On the RADIUS server, set a `Tunnel-Password` attribute in the example MAC account "`F8-E4-E3-D8-5E-AF`".

```
F8-E4-E3-D8-5E-AF Cleartext-Password := "F8-E4-E3-D8-5E-AF"
   Tunnel-Type = "VLAN",
   Tunnel-Medium-Type = "IEEE-802",
   Tunnel-Private-Group-Id = 100,
   Tunnel-Password = "111111111111",
   Fortinet-Group-Name = group_mac
```

3. Confirm the example client (`MAC:f8:e4:e3:d8:5e:af`) can connect to the SSID using the same `Tunnel-Password` passphrase "`111111111111`".

```
# dia wireless-controller wlac -d sta online
   vf=1 wtp=7 rId=2 wlan=wifi.fap.01 vlan_id=0 ip=10.10.80.2 ip6=:: mac=f8:e4:e3:d8:5e:af
        vci= host=fosqa-PowerEdge-R210 user=F8-E4-E3-D8-5E-AF group=group_mac signal=-33
        noise=-95 idle=3 bw=1 use=6 chan=149 radio_type=11AX_5G security=wpa2_only_
        personal mpsk= encrypt=aes cp_authed=no online=yes mimo=2
rad_mac_auth=allow  age=12
```

4. Verify that the RADIUS MPSK can be cached in the FortiGate:

```
# diagnose wpa wpad radius-mac-mpsk wifi-ssid.fap.01
SSID config: SSID(wifi-ssid.fap.01) VAP(wifi.fap.01) refcnt(1)
Total RADIUS MPSK cache count: (1)
   mac-binding: f8:e4:e3:d8:5e:af
   vlan-id: 100
   expiration: 1785 seconds
```

5. MAC and MPSK based authentication is successfully implemented.

To configure MAC and MPSK authentication in bridge mode:

1. Configure the wireless controller VAP, enable `radius-mac-mpsk`, and select a profile for`mpsk-profile`:

```
config wireless-controller vap
   edit "wifi.fap.02"
      set ssid "wifi-ssid.fap.02"
      set radius-mac-auth enable
      set radius-mac-auth-server "peap"
      set radius-mac-mpsk-auth enable
      set radius-mac-mpsk-timeout 1800
      set local-standalone enable
      set local-bridging enable
      set local-authentication enable
      set schedule "always"
      set mpsk-profile "wifi.fap.02"
   next
end
```

2. Confirm the example client (MAC:f8:e4:e3:d8:5e:af) can now connect to the above local-standalone SSID using the same `Tunnel-Password` passphrase "`111111111111`".

```
FortiAP-231F # sta
wlan11 (wifi-ssid.fap.02) client count 1
   MAC:f8:e4:e3:d8:5e:af ip:10.100.100.231 ip_proto:dhcp ip_age:74 host:fosqa-PowerEdge-
        R210 vci:
   vlanid:0 Auth:Yes channel:149 rate:48Mbps rssi:65dB idle:11s
   Rx bytes:6095 Tx bytes:1719 Rx rate:87Mbps Tx rate:48Mbps Rx last:11s Tx last:68s
   AssocID:1 Mode:  Normal Flags:1000000b PauseCnt:0
```

3. Verify that the RADIUS MPSK can be cached on FortiAP:

```
FortiAP-231F # h_diag radius-mac-mpsk wifi-ssid.fap.02
```

```
SSID config: SSID(wifi-ssid.fap.02) VAP(wlan11) refcnt(1)
Total RADIUS MPSK cache count: (1)
   mac-binding: f8:e4:e3:d8:5e:af
   vlan-id: 100
   expiration: 1660 seconds
```

4. MAC and MPSK based authentication is successfully implemented.

Because Dynamic VLAN is not configured on each of the VAPs, the cache returned by the RADIUS server and the station statistics show different VLAN IDs. FortiGate does not use the VLAN passed by the RADIUS server, but still caches it.

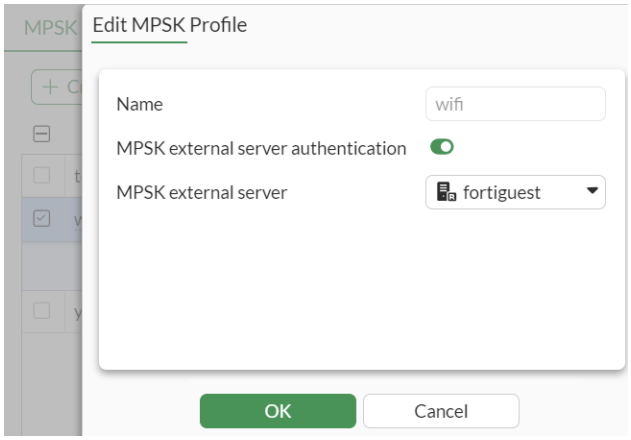
User self-registration of MPSKs through FortiGuest

You can enable users to generate Multi Pre-Shared Keys (MPSK) through the FortiGuest self-registration portal. Users can self-register their devices through the portal, receiving a unique pre-shared key (MPSK) bound to their device's MAC address. When they connect to the SSID, FortiGate sends the client's passphrase and MAC address to FortiGuest during the 4-way handshake. Based the FortiGuest response, FortiGate authenticates or de-authenticates the client.

Example Topology

To configure a FortiGuest external MPSK server - GUI:

1. Go to *System* > *Feature Visibility* and enable *Advanced Wireless Features*.
2. Click *Apply*.
3. Go to *WiFi & Switch Controller* > *Connectivity Profiles* > *MPSK Profiles* and click *Create new* to create an MPSK profile.
4. Enter an MPSK profile *Name* and select a security *Type*.
5. Enable *MPSK external server authentication* and select an *MPSK external server*.



6. When you are finished, click *OK*.

To configure a FortiGuest external MPSK server - GUI:

1. Create an external FortiGuest server.

```
config user radius
  edit "fortiguest"
    set server "172.16.200.117"
    set secret ENC *
  next
end
```

2. Create an MPSK profile, enable MPSK external server authentication, and apply the external server you created.

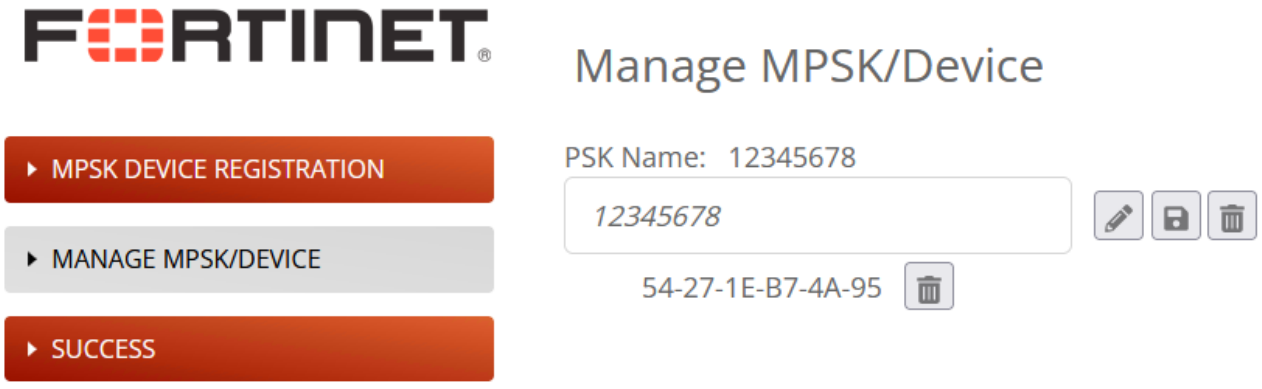
```
config wireless-controller mpsk-profile
  edit "wifi"
    set mpsk-external-server-auth enable
    set mpsk-external-server "fortiguest"
  next
end
```

3. Apply the MPSK profile to a VAP.

```
config wireless-controller vap
  edit "wifi"
    set ssid "FOS_81F_POE_MPSK"
    set schedule "always"
    set mpsk-profile "wifi"
    set dynamic-vlan enable
    set quarantine disable
  next
end
```

To verify external MPSK authentication:

1. Using a wireless client, create a key in the FortiGuest self-registration portal.



   - The MAC address of the device is *54:27:1E:B7:4A:95*.
   - The PSK key is *12345678*.
2. Verify that you can connect the wireless client to the SSID using the configured PSK key of *12345678*.

```
# dia wireless-controller wlac -d sta online
   vf=0 mpId=0 wtp=4 rId=1 wlan=wifi vlan_id=0 ip=192.168.1.110
```

```
ip6=fe80::dc46:a41f:5546:f07f mac=54:27:1e:b7:4a:95 vci=MSFT 5.0 host=DESKTOP-05HBKE1
user= group= signal=-70 noise=-95 idle=1 bw=0 use=5 chan=11 radio_type=11N
security=wpa2_only_personal mpsk= encrypt=aes cp_authed=no l3r=1,0
G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=1
                ip6=*fe80::dc46:a41f:5546:f07f,26,
```

3. Check the WiFi event log and verify there is a log with the action as *EXT-MPSK-auth-success*, indicating that the 4-way handshake is successful.

```
# exe log display
date=2024-03-13 time=09:02:06 eventtime=1710345725686198360 tz="-0700"
logid="0104043657" type="event" subtype="wireless" level="notice" vd="root"
logdesc="Wireless station association failed" sn="FP433GTY22001147"
ap="FP433GTY22001147" vap="wifi" ssid="FOS_QA_Starr_81F_3G_psk" radioid=1 user="N/A"
stamac="54:27:1e:b7:4a:95" signal=-45 snr=50 authserver="N/A" channel=11 security="WPA2
Personal" encryption="AES" action="EXT-MPSK-auth-success" reason="Reserved 0"
msg="External MPSK authentication was successful for client 54:27:1e:b7:4a:95"
```

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

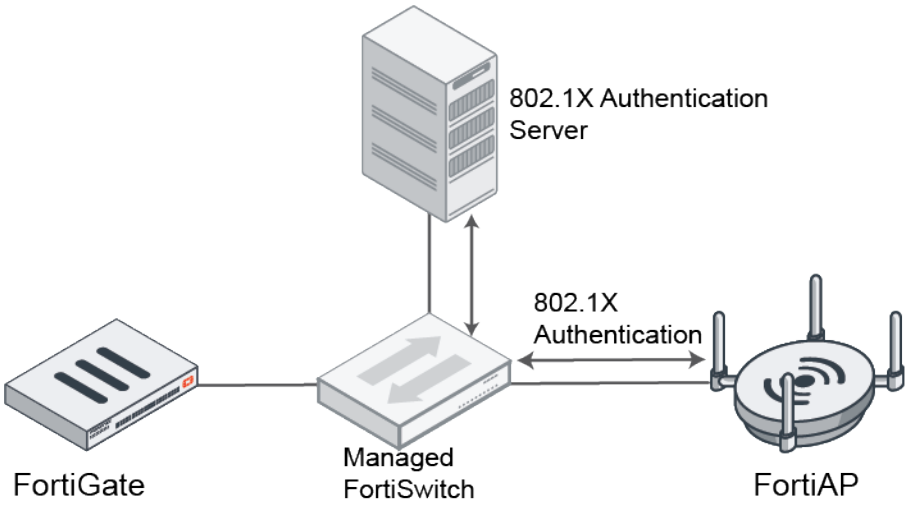
1. Go to *User & Authentication* > *User Groups* and create one or more guest user groups.
2. Go to *User & Authentication* > *Guest Management* to create guest accounts. You can print the guest account credentials or send them to the user as an email or SMS message.
3. Go to *WiFi and Switch Controller* > *SSIDs* 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 802.1X supplicant on LAN

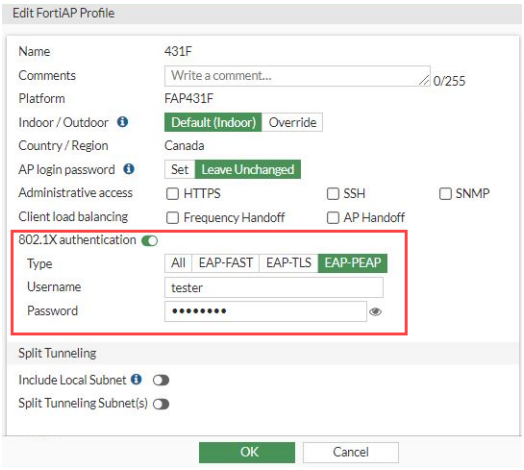
When the FortiAP is connected to a switch port with 802.1x authentication enabled, the FortiAP can be configured to act as a 802.1x supplicant to authenticate against the server using EAP-FAST, EAP-TLS or EAP-PEAP.

When the port is configured for 802.1x authentication, the switch does not allow any traffic other than 802.1x traffic to pass through the port until the device connected to the port authenticates successfully. Once the authentication is successful, FortiAP packets can pass through the switch port and join the FortiGate.



To enable 802.1X authentication - GUI:

1. Go to *WiFi & Switch Controller* > *FortiAP Profiles* and select the profile you want to enable 802.1X authentication on.
2. Enable *802.1X authentication* and select the authentication method:
   - *All*
   - *EAP-FAST*
   - *EAP-TLS*
   - *EAP-PEAP*



3. Enter a *Username* and *Password* for authentication.
4. Click *OK* to save.

To enable 802.1X authentication on a FortiGate managed FortiAP - CLI:

```
config wireless-controller wtp-profile
  edit "431F"
    config platform
      set type 431F
      set ddscan enable
    end
    set handoff-sta-thresh 55
```

```
    set ap-country CA
    config radio-1
      set band 802.11ax,n,g-only
    end
    config radio-2
      set band 802.11ax-5G
    end
    config radio-3
      set mode monitor
    end
    set wan-port-auth 802.1x
    set wan-port-auth-usrname "tester"
    set wan-port-auth-password ENC ***********
    set wan-port-auth-methods EAP-PEAP
  next
end
```

The default setting for `wan-port-auth` is "`none`" and the default setting for `wan-port-auth-methods` is "`all`"

To enable 802.1X authentication on a FortiAP not managed by FortiGate - CLI:

```
FortiAP-431F # cfg -a WAN_1X_ENABLE=1
cfg -a WAN_1X_USERID=tester
cfg -a WAN_1X_PASSWD=12345678
cfg -a WAN_1X_METHOD=3
```

`WAN_1X_ENABLE`	Enable or Disable WAN port 802.1x supplicant: • 0: Disabled • 1: Enabled The default setting is 0.
`WAN_1X_USERID`	WAN port 802.1x supplicant user.
`WAN_1X_PASSWD`	WAN port 802.1x supplicant password.
`WAN_1X_METHOD`	Select an EAP method for the WAN port 802.1x supplicant: • 0: EAP-ALL • 1: EAP-FAST • 2: EAP-TLS • 3: EAP-PEAP The default setting is 0.

To upload certificates via the FortiAP CLI:

```
cw_diag -c wan1x [<get-ca-cert|get-client-cert|get-private-key> <tftp server IP> <file
name>]
FortiAP-431F # cw_diag -c wan1x get-ca-cert 172.16.200.100 ca.cert.pem
Get "ca.cert.pem" from tftp server OK.
```

To verify a FortiAP is successfully authenticated from 802.1x radius:

```
FortiAP-431F # cw_diag -c wan1x
WAN port 802.1x supplicant:
EAP methods : EAP-PEAP
Username : tester
PasswordENC : ************
CA CERT : users
Client CERT : default
Private Key : default
Port Status : Authorized
```

Media Access Control Security

Media Access Control Security (MACsec) is a network protocol that provides authenticity and integrity for the entire Ethernet frame as well as encryption of the Layer 2 data payload. Enabling MACsec on a FortiAP improves communication security of Layer 2 frames passing through wired networks.

Since MACsec is an extension to 802.1X, which provides secure key exchange and mutual authentication for MACsec nodes, FortiAPs must first be configured to pass 802.1X authentication as a supplicant. MACsec can be enabled from the FortiGate or locally on a FortiAP.

- MACsec is only supported on FortiAP G-series models.
- Only the MACsec dynamic-CAK model is supported; PSK mode is not supported,
- Due to technical limitations, FortiAP G -series models only support the MACsec policy Confidentiality Offset value of 0 (default for most implementations) or 30. It does not support 50.

Enabling MACsec on FortiAP

In deployments where all FortiAPs are managed by a FortiGate, you can configure 802.1x and MACsec on the FortiAP profile and the configurations will be pushed to assigned FortiAPs. Then, depending on the switch used in your deployment, configure and apply 802.1x and MACsec on the switch ports to which the FortiAPs connect. The FortiAPs continue to communicate with their managing FortiGate and function as usual.

In deployments where you need to connect a new FortiAP to your network before it is managed by FortiGate, you can pre-configure the FortiAP profiles while also configuring MACsec locally on the FortiAP device. Then, ensure that the switch ports to which the FortiAPs will connect have 802.1x and MACsec configured before connecting the FortiAPs.

If MACsec is enabled on a FortiAP, but the switch port that the FortiAP connects to does not have 802.1x and MACsec enabled, then authentication will fail and the FortiAP will lose network connection.

To enable MACsec from a FortiAP profile - CLI:

```
config wireless-controller wtp-profile
  edit <name>
    set wan-port-auth 802.1x
    set wan-port-auth-usrname "tester"
    set wan-port-auth-password ENC *
```

```
    set wan-port-auth-methods EAP-PEAP
    set wan-port-auth-macsec enable
  next
end
```

To enable MACsec locally from a FortiAP - CLI:

```
FortiAP-233G # cfg -a WAN_1X_ENABLE:=1
cfg -a WAN_1X_USERID:=tester
cfg -a WAN_1X_PASSWD:=*
cfg -a WAN_1X_METHOD:=3
cfg -a WAN_1X_MACSEC_POLICY:=1
```

To verify a FortiAP successfully passes MACsec authentication:

```
FP233G # cw_diag -c wan1x macsec
participant_idx=0
ckn=972149b46b1ff31c11d3c1d864b0bad9
mi=94a9763a40b2905ba3ec2be9
mn=78974
active=Yes
participant=No
retain=No
live_peers=1
potential_peers=0
is_key_server=No
is_elected=Yes
TX SCI : 74:78:a6:98:dc:28@1
RX SCI : 70:35:09:21:cb:84@2
Cipher : GCM-AES-256
Tx Next PN: 298329
Distributed SAK Received : 1
  Distributed_an : 0
  AN : 0
      tx : InUse
      rx : InUse
  Confidentiality_offset : 30
  replay_protect : 0
  replay_window : 0
```

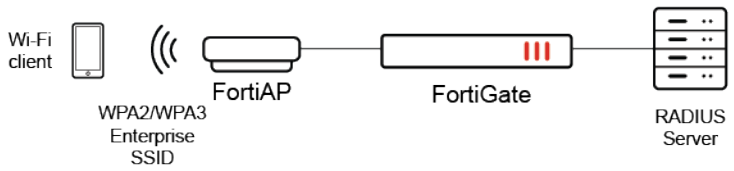
To verify a FortiAP is registered in FortiGate with 802.1X and MACsec authentication:

```
FortiGate-301E (vdom1) # diagnose  wireless-controller  wlac -c wtp

WTP vd               : vdom1, 3-FP233GTF23000132    MP00
    uuid                 : 0d96e930-1aaf-51ef-0a3a-315f022a18d7
    mgmt_vlanid      : 0
    region code        : E  invalid
    refcnt                 : 3 own(1) wtpprof(1) ws(1)   deleted(no)
    apcfg status       : N/A,N/A cfg_ac=0.0.0.0:0 val_ac=0.0.0.0:0 cmds T 0 P 0 U 0 I 0 M 0
    apcfg cmd details:
    plain_ctl           : disabled
    image-dl(wtp,rst): yes,no
    admin                : enable
    wtp-profile       : cfg(233G) override(disabled) oper(233G)
…….
```

```
SNMP                : disabled
WAN port authentication: 802.1X
WAN port 802.1x EAP method: EAP-PEAP
WAN port 802.1x Macsec: enabled
```

Configure NAS-Filter-Rule attribute to set up dACL

You can enable receiving the NAS-Filter-Rule attribute after successful WiFi 802.1X authentication. When a wireless client connects to a WPA2/WPA3 Enterprise SSID and gets authenticated by a RADIUS server, the server sends attributes—including the NAS-Filter-Rule attribute—with an "Access-Accept" message to the FortiGate. The FortiGate then forwards these rules to the FortiAP associated with the wireless client. The FortiAP can set up a dynamic Access Control List (dACL) using these rules, which regulates the wireless client's access to the network.



The NAS-Filter-Rule attribute is only supported by Tunnel and Local Bridging mode SSIDs. It is not supported on Local Standalone mode.

The NAS-Filter-Rule attribute is only supported when the security mode is set to WPA2/WPA3 Enterprise with a RADIUS server as the Authentication protocol.

To enable NAS-Filter-Rule on a VAP - CLI:

1. Create a VAP with `nas-filter-rule` enabled.

```
config wireless-controller vap
  edit "wifi3"
    set ssid "FOS_81F"
    set security wpa2-only-enterprise
    set fast-bss-transition enable
    set auth radius
    set radius-server "peap"
    set nas-filter-rule enable
    set schedule "always"
  next
end
```

2. Set up an example user account in the RADIUS server with NAS-Filter-Rules configuring access control.

```
test3           Cleartext-Password := "123456"
                Tunnel-Type = "VLAN",
                Tunnel-Medium-Type = "IEEE-802",
                Fortinet-Group-Name = "group1",
                Session-Timeout=300,
                Tunnel-Private-Group-Id = 100,
                Termination-Action=1,
                NAS-Filter-Rule = "permit in icmp from assigned to
```

```
172.16.200.44/32\000",
                NAS-Filter-Rule += "deny in tcp from assigned to 172.16.200.44/32"
```

3. Connect a wireless client with the authenticated example user account "test3" to the SSID and verify the NAS-Filter-Rules are sent to the FortiAP.
4. Verify the wireless client follows the NAS-Filter-Rules.
   a. The wireless client can ping the server 172.16.200.44.

```
root@WiFi-Client-2:/home/wpa-test# ping 172.16.200.44
PING 172.16.200.44 (172.16.200.44) 56(84) bytes of data.
64 bytes from 172.16.200.44: icmp_seq=1 ttl=63 time=57.0 ms
--- 172.16.200.44 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 57.013/57.013/57.013/0.000 ms
```

   b. The wireless client is denied access to the server 172.16.200.44 over HTTP.

```
root@WiFi-Client-2:/home/wpa-test# curl http://172.16.200.44
root@WiFi-Client-2:/home/wpa-test#
```

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 enable IPv6 addresses, go to *System* > *Feature Visibility* and enable *IPv6*.

To create a firewall address for WiFi users - GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Select *Create New* > *Address* and enter the following information:

Category	Select *Address* to create an IPv4 address.
Name	Enter a name for the address. For example, wifi_net.
Type	Select *Subnet.*
IP/Netmask	Enter the subnet address. For example, 10.10.110.0/24.
Interface	Select the interface where this address is used. For example, example_wifi.

3. When you are finished, click *OK*

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* > *Firewall 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
```

To configure IPv6 addresses, use `set srcaddr6` and `set dstaddr6`.

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 & and Switch Controller* > *Local WiFi Radio*.
2. Select a FortiAP profile to apply to the FortiWiFi access point (see Creating a FortiAP profile on page 38 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 192.

Enforcing UTM policies on a local bridge SSID

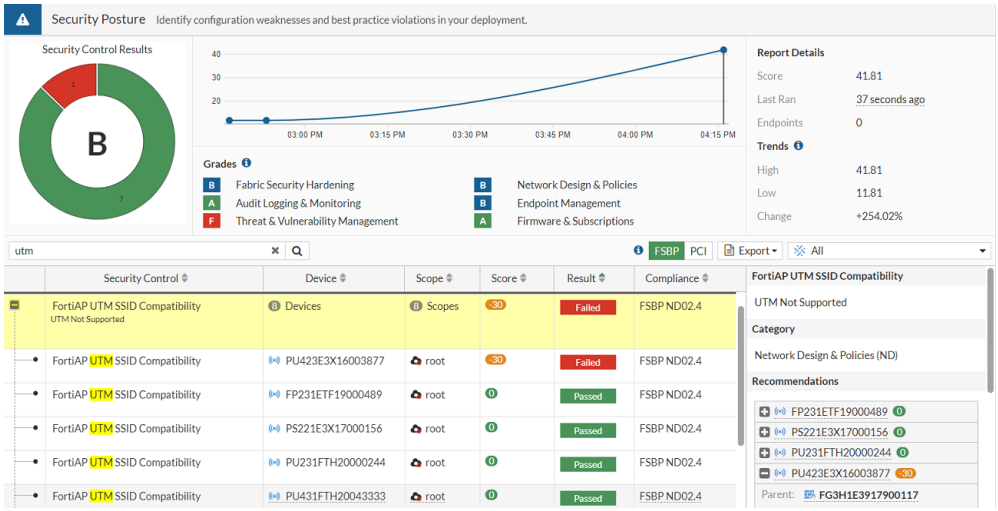
If a bridge mode SSID is configured for a UTM capable FortiAP, you can add security profiles to the wireless controller configuration that enables you to apply security profile features to the traffic over the bridge SSID.

For information on how to configure security profiles, see FortiAP-S and FortiAP-U bridge mode security profiles on page 297

However, not all FortiAPs are UTM capable. You can use the Security Rating check to review your managed FortiAPs and check if any UTM incapable FortiAPs are broadcasting SSIDs that contain security profiles.

To run the Security Rating:

1. Go to *Security Fabric* > *Security Rating* and click *Run Now* to run the security rating check.
2. Select the *Security Posture* scorecard and search for *FortiAP UTM SSID Compatibility* to find the result.
   If there are any UTM incapable FortiAPs broadcasting SSIDs with security profiles, the result will show as *Failed*.

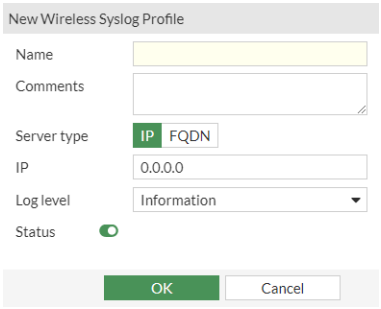


Configuring a Syslog profile

When FortiAPs are managed by FortiGate, you can configure your FortiAPs to send logs (Event, UTM, and etc) to the syslog server. Syslog server information can be configured in a Syslog profile that is then assigned to a FortiAP profile.

To configure a Syslog profile - GUI:

1. Go to *WiFi & Switch Controller* > *FortiAP Profiles* and select the profile you want to assign a syslog profile to.
2. Locate *System Log* and enable *Syslog profile*.
3. Click the *Syslog profile* field and click *Create* to create a new syslog profile.
   The New Wireless Syslog Profile window loads.



4. Enter a *Name* for the Syslog profile.
5. Select the *Server type* you want to use.
   - If you select *IP*, enter the IP address of the syslog server.
   - If you select *FQDN*, enter the FQDN address of the syslog server.
6. Select a *Log level* to determine the lowest level of log messages that the FortiAP sends to the server:
7. Ensure that the *Status* is enabled.
8. Click *OK* to save the Syslog profile.
9. From the FortiAP profile, select the Syslog profile you created.
10. Click *OK* to save the FortiAP profile.

To configure a Syslog profile - CLI:

1. Configure a syslog profile on FortiGate:

```
config wireless-controller syslog-profile
  edit "syslog-demo-1"
    set comment ''
    set server-status enable
    set server-addr-type ip
    set server-ip 192.16.9.12
    set server-port 514
    set log-level debugging
  next
end
```

2. Assign the syslog profile to a FortiAP profile:

```
config wireless-controller wtp-profile
  edit "FAP231F-default"
```

```
    config platform
      set type 231F
      set ddscan enable
    end
    set syslog-profile "syslog-demo-1"
    ...
  next
end
```

3. Assign the FortiAP profile to a managed FortiAP unit:

```
config wireless-controller wtp
  edit "FP231FTF20026472"
    set uuid 183ae8c6-09de-81ec-d12e-02a3c8eb88d6
    set admin enable
    set wtp-profile "FAP231F-default"
    config radio-1
    end
    config radio-2
    end
  next
end
```

4. From the FortiGate console, verify that the syslog profile has been successfully adopted:

```
FortiGate-80E-POE # diagnose wireless-controller wlac -c wtpprof FAP231F-default
WTPPROF (001/005) vdom,name: root, FAP231F-default
    platform         : FAP231F.
    refcnt           : 5 own(1) wlan(2) wtp(1)
    deleted          : no
    apcfg-profile    :
    ddscan           : enabled
    ble-profile      :
    syslog-profile   : syslog-demo-1(enabled server=192.16.9.12:514 log-level=7)
    led-state        : enabled
    lldp             : enabled
    poe-mode         : auto
...
FortiGate-80E-POE # diagnose wireless-controller wlac -c syslogprof
SYSLOG (001/001) vdom,name : root, syslog-demo-1
    refcnt                 : 2 own(1) wtpprof(1)
    deleted                : no
    server status          : enabled
    server address         : 192.16.9.12
    server port            : 514
    server log level       : 7
    wtpprof cnt            : 1
       wtpprof 001         : FAP231F-default
```

5. From the FortiAP console, verify that the configurations have been successful pushed to the FortiAP unit:

```
FortiAP-231F # cw_diag -c syslog config
Syslog configuration: en=1 addr=192.16.9.12 port=514 log_level=7
```

To configure a Syslog profile using a FQDN server address - CLI:

1. Configure a syslog profile on FortiGate:

```
config wireless-controller syslog-profile
  edit "syslog-demo-2"
    set comment ''
    set server-status enable
    set server-addr-type fqdn
    set server-fqdn "syslog.test.env"
    set server-port 5140
    set log-level critical
  next
end
```

2. Assign the FortiAP profile to a managed FortiAP unit:

```
config wireless-controller wtp-profile
  edit "FAP231F-default"
    config platform
      set type 231F
      set ddscan enable
    end
    set syslog-profile "syslog-demo-2"
    ...
  next
end
```

3. Assign the FortiAP profile to a managed FortiAP unit:

```
config wireless-controller wtp
  edit "FP231FTF20026472"
    set uuid 183ae8c6-09de-81ec-d12e-02a3c8eb88d6
    set admin enable
    set wtp-profile "FAP231F-default"
    config radio-1
    end
    config radio-2
    end
  next
end
```

4. From the FortiAP console, verify that the configurations have been successful pushed to the FortiAP unit:

```
FortiAP-231F # cw_diag -c syslog config
Syslog configuration: en=1 addr=syslog.test.env(192.16.9.12) port=5140 log_level=2
```

Understanding Distributed Radio Resource Provisioning

To prevent interference between APs, the FortiOS WiFi Controller features Distributed Automatic Radio Resource Provisioning (DARRP). 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. Channel selection is optimized by monitoring neighboring AP channels and by performing periodic background scans to collect signal strength.

DARRP has two phases:

- **Channel Planing Phase**
  - Sub-phase 1: Find channels to be excluded from consideration.
  - Sub-phase 2: If all channels are excluded during sub-phase 1, select a channel to use based on an assigned channel score.
- **Channel Quality Monitoring Phase**: The AP monitors the channel quality using `monitor-period` to check for TX and RX retries and errors. If the threshold is crossed, the AP changes channels as needed.

Channel Planning

Sub-phase 1

The AP first identifies channels with AP scanning and spectral scanning. The AP then excludes channels that exceed the following configured threshold values:

- `threshold-ap 250`
- `threshold-noise-floor "-85"`
- `threshold-channel-load 60`
- `threshold-spectral-rssi "-65"`

DARRP will also exclude the DFS channel and weather channel if they are disabled.

After excluding channels, channels are selected based on the following criteria:

- If there is only one channel left, that channel is picked.
- If there are multiple channels left, a random channel is picked.
- It there are no channels left, the AP Controller proceeds to sub-phase 2.

Sub-phase 2

If all channels are excluded after sub-phase 1, the AP Controller calculates a channel score and selects the channel with the lowest score. The channel score is based on a combination of the following factors:

```
channel_score = weight-managed-ap * rssi_score_managed_ap +
                weight-rogue-ap * rssi_score_rogue_ap +
                weight-noise-floor * noise_floor +
                weight-channel-load * channel load +
                weight-spectral-rssi * spectral RSSI +
```

The channel with the lowest score is then selected. If no channel is available, the AP disables the radio.

Channel Quality Monitoring

Once a channel is picked, the AP performance on that channel is periodically monitored by the AP and switched if required. If a channel switch occurs, the AP reports the new channel to the controller.

Channel quality is calculated with the following:

If (`current tx-retries` > `threshold-tx-retries`) or (`current rx-errors` > `threshold-rx-errors`), then the AP will select a new channel to use. This is similar to how channels are selected in Channel Planning sub-phase 2.

The `current tx-retries` and `current rx-errors` is averaged over the configured time under `monitor-period`.

Configuring Distributed Radio Resource Provisioning

Channels are selected based on parameters including total RSSI, Noise Floor, Channel Load, Spectral RSSI, and more. Each of those parameters are multiplied by a weight value assigned by default under the `arrp-profile`. You can adjust the weights of each individual parameter based on the priority and importance of the parameter.

Once you enable DARRP under a radio, the default `arrp-profile` takes effect. You can create multiple ARRP profiles and apply them to radios under FortiAP profiles.

To configure ARRP profiles - CLI:

```
config wireless-controller arrp-profile
   edit "arrp-default"
      set comment ''
      set selection-period 3600
      set monitor-period 300
      set weight-managed-ap 50
      set weight-rogue-ap 10
      set weight-noise-floor 40
      set weight-channel-load 20
      set weight-spectral-rssi 40
      set weight-weather-channel 1000
      set weight-dfs-channel 500
      set threshold-ap 250
      set threshold-noise-floor "-85"
      set threshold-channel-load 60
      set threshold-spectral-rssi "-65"
      set threshold-tx-retries 300
      set threshold-rx-errors 50
      set include-weather-channel no
      set include-dfs-channel no
   next
end
```

The AP Controller uses historical data in `selection-period` to calculate scores based on channel load, noise floor, and spectral RSSI values.

Parameter definitions

selection-period	Period in seconds to measure average channel load, noise floor, spectral RSSI (default = 3600).
monitor-period	Period in seconds to measure average transmit retries and receive errors (default = 300)
weight-managed-ap	Weight in DARRP channel score calculation for managed APs (0 - 2000, default = 50).
weight-rogue-ap	Weight in DARRP channel score calculation for rogue APs (0 - 2000, default = 10).

weight-noise-floor	Weight in DARRP channel score calculation for noise floor (0 - 2000, default = 40).
weight-channel-load	Weight in DARRP channel score calculation for channel load (0 - 2000, default = 20).
weight-spectral-rssi	Weight in DARRP channel score calculation for spectral RSSI (0 - 2000, default = 40).
weight-weather-channel	Weight in DARRP channel score calculation for weather channel (0 - 2000, default = 1000).
weight-dfs-channel	Weight in DARRP channel score calculation for DFS channel (0 - 2000, default = 500).
threshold-ap	Threshold to reject channel in DARRP channel selection phase 1 due to surrounding APs (0 - 500, default = 250).
threshold-noise-floor	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to noise floor (-95 to -20, default = -85).
threshold-channel-load	Threshold in percentage to reject channel in DARRP channel selection phase 1 due to channel load (0 - 100, default = 60).
threshold-spectral-rssi	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to spectral RSSI (-95 to -20, default = -65).
threshold-tx-retries	Threshold in percentage for transmit retries to trigger channel reselection in DARRP monitor stage (0 - 1000, default = 300).
threshold-rx-errors	Threshold in percentage for receive errors to trigger channel reselection in DARRP monitor stage (0 - 100, default = 50)
include-weather-channel	Enable/disable use of weather channel in DARRP channel selection phase 1 (default = disable).
include-dfs-channel	Enable/disable use of DFS channel in DARRP channel selection phase 1 (default = disable).
override-darrp-optimize	Enable to override setting darrp-optimize and darrp-optimize-schedules (default = disable).

To enable DARRP and apply ARRP profiles to FortiAP profiles:

The DARRP feature is disabled by default. To enable DARRP, edit the FortiAP profile and set `darrp enable` under each radio. The default ARRP profile, `arrp-default`, will then be automatically applied. Alternatively, you can customize ARRP profiles and apply them to FortiAP radios respectively. For example:

```
config wireless-controller arrp-profile
    edit "arrp-default"
    next
    edit "arrp-example"
        set selection-period 1800
    next
end
config wireless-controller wtp-profile
    edit "FAP433F-DARRP"
        config platform
            set type 433F
            set ddscan enable
        end
        set handoff-sta-thresh 55
        config radio-1
```

```
            set band 802.11ax,n,g-only
            set darrp enable
            set arrp-profile "arrp-default"
        end
        config radio-2
            set band 802.11ax-5G
            set channel-bonding 40MHz
            set darrp enable
            set arrp-profile "arrp-example"
        end
        config radio-3
            set mode monitor
        end
    next
end
```

When `channel-bonding` is set to 20MHz (default value), 40MHz, or larger, the DARRP algorithm will consider the channel bandwidth during channel selection.

To set DARRP timing:

DARRP optimization is repeatedly run at an interval defined by the `darrp-optimize` setting. The date and time at which DARRP optimization is run is scheduled according to the `darrp-optimize-schedules` setting.

`darrp-optimize`	Set the time interval in seconds for running Distributed Automatic Radio Resource Provisioning within your configured DARRP schedule (`darrp-optimize-schedules`). If the time interval exceeds the time window in the firewall schedule, DARRP optimization will only run once within the scheduled time slot. The default value is 86400 seconds (24 hours).
`darrp-optimize-schedules <name>`	Select the firewall schedules for when to run DARRP. DARRP will run at intervals defined in `darrp-optimize` within the schedules. Separate multiple schedule names with a space. The default schedule is `default-darrp-optimize`.

By default, ARRP profiles use the same settings per VDOM, as shown in the following:

```
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
```

During DARRP optimization, the FortiGate may change the operating channels of managed FortiAP units and cause connected Wi-Fi clients to experience intermittent service disruption. Therefore, we do not recommend running DARRP

optimization too frequently to avoid disrupting clients with unnecessary channel changes. The default value of `darrp-optimize` is 86400 seconds (24 hours), which means DARRP optimization is run only once per day.

Additionally, we recommend scheduling DARRP optimization to avoid peak periods of heavy wireless traffic. The default schedule, `default-darrp-optimize`, runs DARRP optimization during a low-traffic period of 1:00am to 1:30am every day.

DARRP scheduling example:

The following example shows how to configure an ARRP profile to use a custom `darrp-optimize` and `darrp-optimize-schedules`:

```
config firewall schedule recurring
    edit "darrp-optimize1"
        set start 07:00
        set end 07:30
        set day monday tuesday wednesday thursday friday
    next
    edit "darrp-optimize2"
        set start 19:00
        set end 19:30
        set day monday tuesday wednesday thursday friday
    next
end
config wireless-controller arrp-profile
    edit "arrp-profile1"
        set override-darrp-optimize enable
        set darrp-optimize 43200
        set darrp-optimize-schedules "darrp-optimize1" "darrp-optimize2"
    next
end
```

In this example, DARRP optimization runs twice a day at between 07:00-07:30 and 19:00-19:30. Since the configured time interval in `darrp-optimize` is 43200 (12 hours), DARRP optimization will only run once at 07:00 and 19:00.

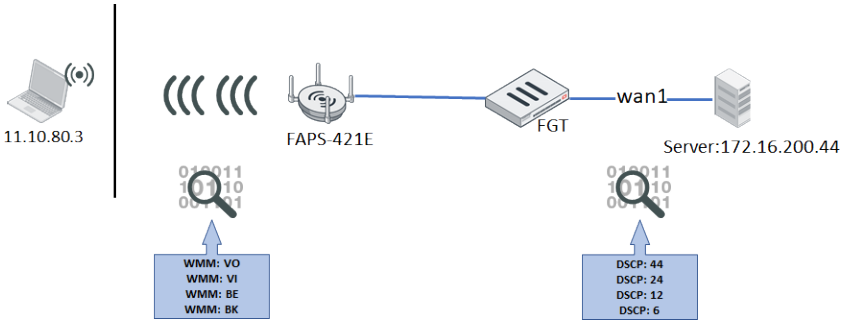
Translating WiFi QoS WMM marking to DSCP values

FortiGates can preserve the WiFi Multi-Media (WMM) QoS marking of packets by translating them to Differentiated Services Code Point (DSCP) values when forwarding upstream. When wireless client sends QOS type packets with WMM priority categories such as AC_VO, AC_VI, AC_BE, AC_BK, FortiAP can forward these packets by translating WMM to DSCP marking and transmit the packets from the Ethernet to their destination.

Use the following QoS profile CLI commands to implement this function:

```
config wireless-controller qos-profile
  edit qos-wifi
    set wmm-dscp-marking [enable/disable]
    enable     Enable WMM Differentiated Services Code Point (DSCP) marking.
    disable    Disable WMM Differentiated Services Code Point (DSCP) marking.
end
```

`wmm-dscp-marking`	Enable/disable WMM Differentiated Services Code Point (DSCP) marking (default = disable).
`wmm-vo-dscp`	DSCP marking for voice access (default = 48).
`wmm-vi-dscp`	DSCP marking for video access (default = 32).
`wmm-be-dscp`	DSCP marking for best effort access (default = 0).
`wmm-bk-dscp`	DSCP marking for background access (default = 8).



To configure WMM QoS marking of packets - GUI:

1. To create a QoS profile from the GUI, you must first enable Advanced Wireless Features (see Advanced Wireless Features on page 165).
2. Once you enable Advanced Wireless Features, navigate to *WiFi & Switch Controller* > *Operation Profiles* > *QoS Profiles* and click *Create new*.
3. Enable *DSCP marking* and configure the following:

Voice access	44
Video access	24
Best effort access	12
Background access	6

4. When you are finished, click OK.
5. Go to *WiFi & Switch Controller* > *SSIDs* and select the SSID you want to apply the QoS profile to.
6. Under *Advanced Settings*, enable *QoS profile* and select the QoS profile you configured.
7. When you are finished, click *OK*.

To configure WMM QoS marking of packets - CLI:

1. Create a QoS profile with `wmm-dscp-marking` enabled, and modify the `wmm-dscp` settings.

```
config wireless-controller qos-profile
  edit qos-wifi
    set wmm-dscp-marking enable
    set wmm-vo-dscp 44
    set wmm-vi-dscp 24
    set wmm-be-dscp 12
```

```
    set wmm-bk-dscp 6
end
```

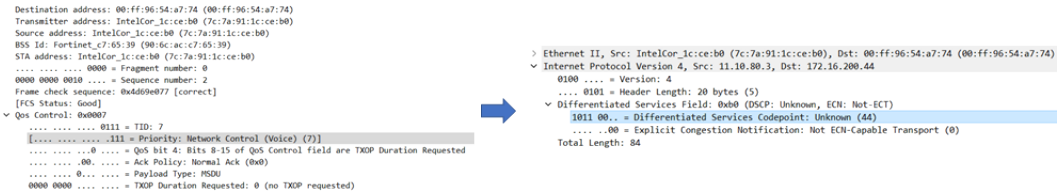
2. Select the QoS profile on a VAP interface.

```
config wireless-controller vap
  edit "stability3"
    set qos-profile "qos-wifi"
  next
end
```

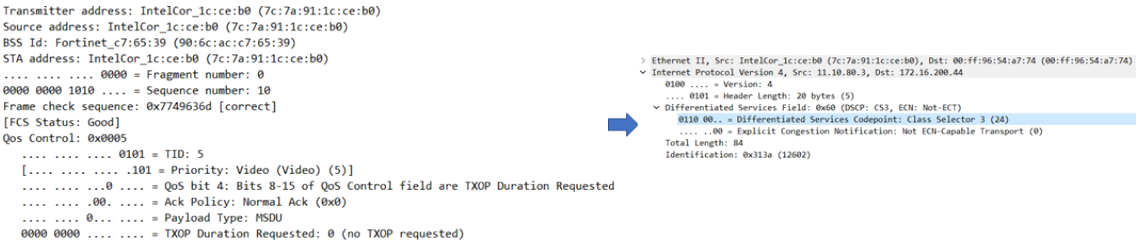
3. Verify that the `wmm-dscp-marking` values are pushed on FortiAP.

```
cw_diag -c k-qos wlan00
WLAN Kernel QoS Settings
..
....
WLAN wlan00 :
     wmm                          : 1
     wmm uapsd                    : 1
     call admission control       : 0
     call capacity                : 0
     bandwidth admission control  : 0
     bandwidth capacity           : 0
     dscp mapping                 : 0
     dscp marking                 : 1
          vo dscp                 : 44
          vi dscp                 : 24
          be dscp                 : 12
          bk dscp                 : 6
```

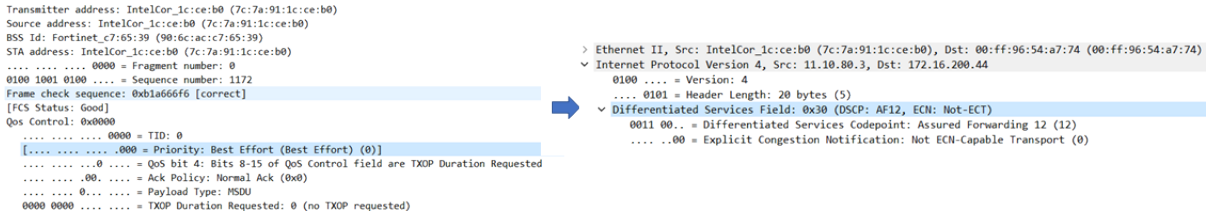
4. Verify that, when sending traffic from a client with a WMM setting of VO, the FortiGate receives the packets with a DSCP TID value or 44.



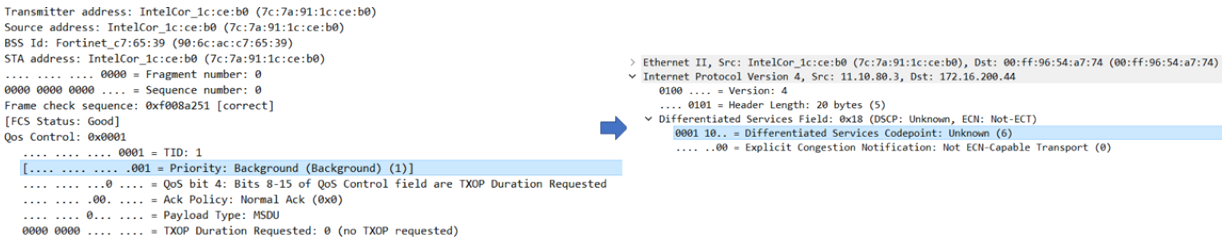
5. Verify that, when sending traffic from a client with a WMM setting of VI, the FortiGate receives the packets with a DSCP TID value or 24.



6. Verify that, when sending traffic from a client with a WMM setting of BE, the FortiGate receives the packets with a DSCP TID value or 12.



7. Verify that, when sending traffic from a client with a WMM setting of BK, the FortiGate receives the packets with a DSCP TID value or 6.



Configuring Layer 3 roaming

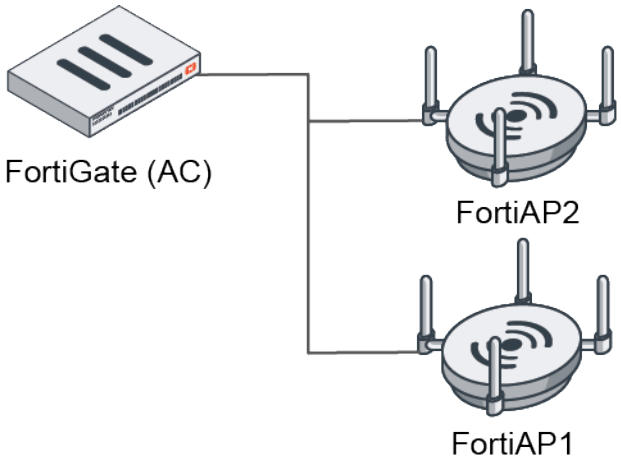
Roaming is client's ability to maintain its association while it roams from one AP to another with as little latency as possible. When a wireless client connects to an access point, the managed wireless controller maintains client's database or information like MAC and IP addresses, security context and associations, quality of service (QoS) , the WLAN. The controller uses this information to forward frames and manage traffic to and from the wireless client.

As a wireless client roams from one department or floor to another, the design could mean that they cross an L3 boundary and experience latency. This is especially noticeable when running VoIp, Video or streaming services. To support this, you can configure a wireless network to enable Layer 3 roaming between different VLANs and subnets on the same or different Wireless Controller. A client connected to the SSID on one FortiAP can roam to the same SSID on another FortiAP managed by the same or different FortiGate Wireless Controller, and continue to use the same IP. When the client idles longer than a configurable amount of time (`client-idle-rehome-timeout`), the client will rehome, receive an address on the new subnet from the new FortiAP, and move to its new L3 segement.

This feature supports two topologies:

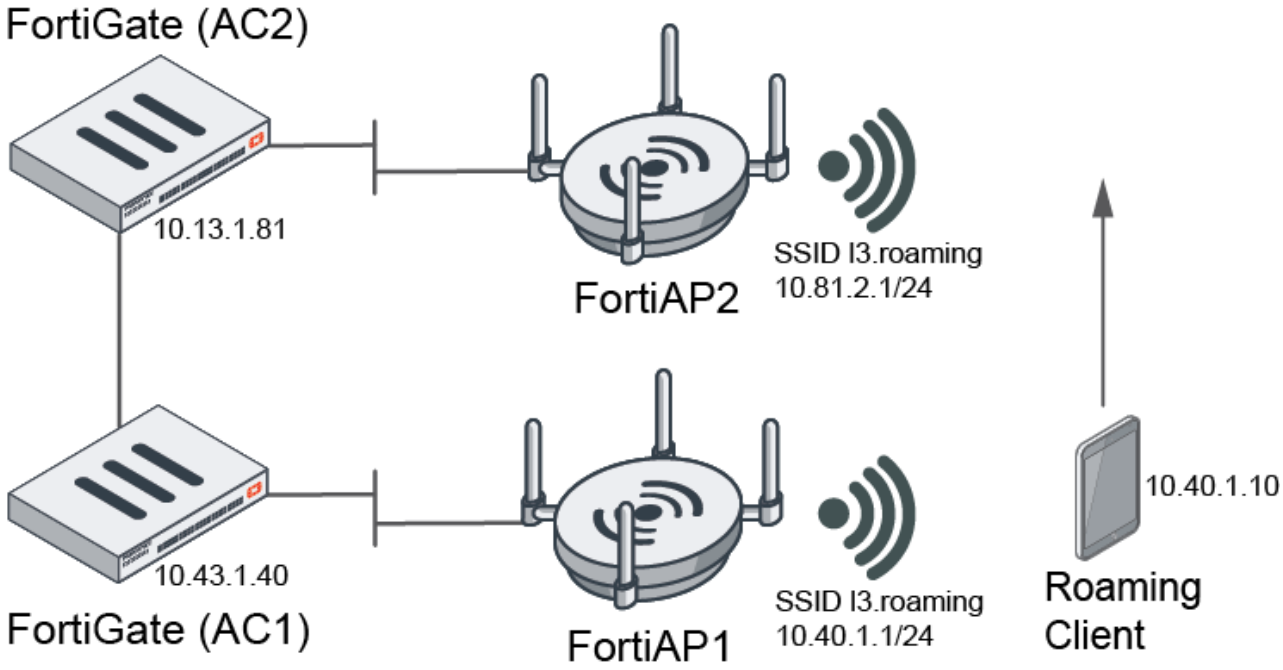
- **L3 roaming intra-controller**

  In this example, there are two FortiAPs (FAP1 and FAP2) being managed by a controller. The FortiAPs are located on different floors of the same building. Each FortiAP is mapped to a different VLAN, but are on the same SSID. The client roams from FAP1 to FAP 2 and the L3 handoff is handled by the controller. The client maintains the same IP address.



- **L3 roaming inter-controller**

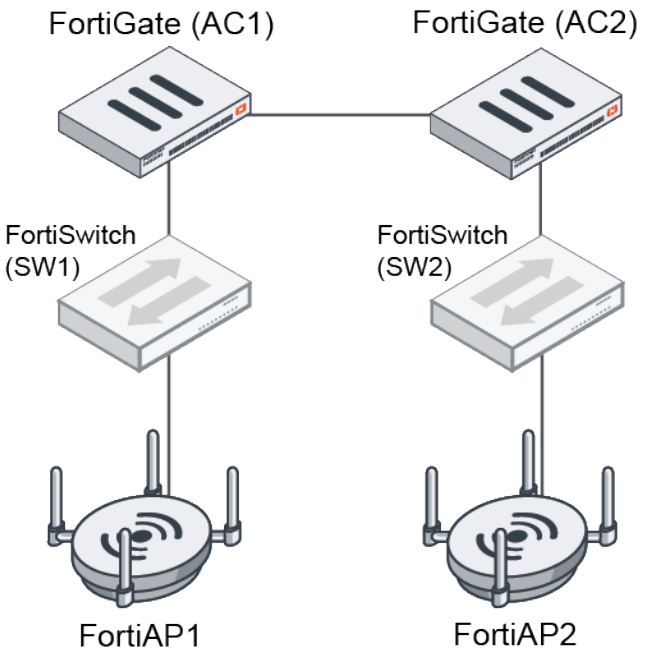
  In this example, there are two controllers (Controller1 and Controller2) each managing a FortiAP (FAP1 and FAP2) respectively. The L3 client roams from Controller1's FAP1 to Controller 2's FAP2. Both FortiAPs have the same SSID, and each FAP has the SSID tied to a different VLAN. The client roams between the two FAPs and the L3 handoff is handled by Controller1 and Controller2's mobility tunnel. The client maintains the same IP address.



  In addition, for the L3 roaming inter-controller topology, bridge mode SSIDs support two roaming modes:

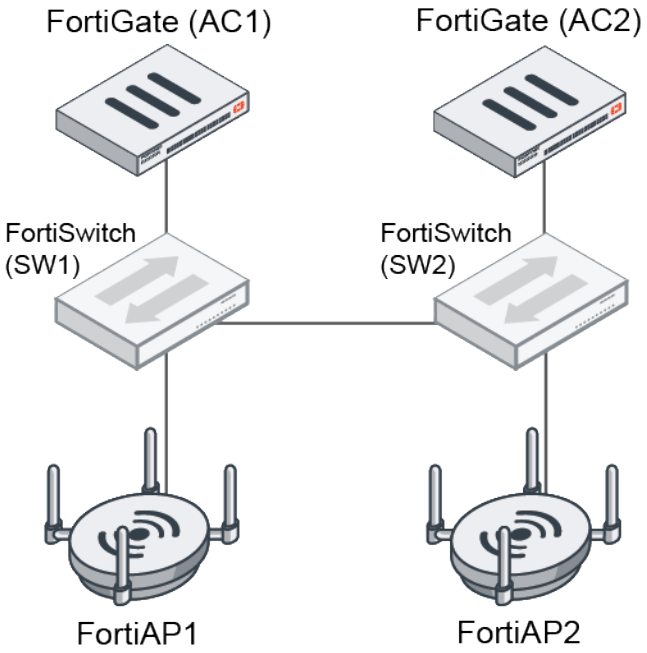
  - **Indirect Mode**

    In indirect mode, the L3 handoff is handled by the mobility tunnel between the FortiGate Wireless Controllers.



- **Direct Mode**

  In direct mode, the two FortiAPs must be able to reach each other with no NAT in the path and the L3 handoff occurs between the FortiAPs directly.



Note: Direct mode is preferred when feasible.

Configuring L3 Roaming for Tunnel Mode SSIDs

To configure Intra-Controller L3 roaming - CLI:

1. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
config wireless-controller timers
  set client-idle-rehome-timeout 20
end
```

2. configure the L3 roaming support SSID:

```
config wireless-controller vap
  edit "l3_rm1"
    set ssid "l3.roaming"
    set passphrase ENC
    set schedule "always"
    set l3-roaming enable
  next
end
config system interface
  edit "l3_rm1"
    set vdom "root"
    set ip 10.40.1.1 255.255.255.0
    set allowaccess ping
    set type vap-switch
    set role lan
    set snmp-index 18
  next
end
```

3. Assign L3 roaming VAP to FAP433F:

```
config wireless-controller wtp-profile
  edit "433F"
    config platform
      set type 433F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess ssh
    config radio-1
      set mode disabled
    end
    config radio-2
      set band 802.11ax-5G
      set power-mode dBm
      set power-value 1
      set channel "36"
      set vap-all manual
      set vaps "l3_rm1"
    end
    config radio-3
      set mode monitor
    end
  next
end
```

```
config wireless-controller wtp
  edit "FP433FXX00000000"
    set uuid b04f1cca-8528-51ec-2dc0-c744cbef4179
    set admin enable
    set wtp-profile "433F"
    config radio-2
    end
  next
end
```

4. Assign L3 roaming VAP to FAP831F:

```
config wireless-controller wtp-profile
  edit "831F"
    config platform
      set type 831F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess ssh
    config radio-1
      set mode disabled
    end
    config radio-2
      set band 802.11ax-5G
      set channel "36" "40"
      set vap-all manual
      set vaps "13_rm1"
    end
    config radio-3
      set mode disabled
    end
  next
end
config wireless-controller wtp
  edit "FP831FXX00000000"
    set uuid 23ed4966-af92-51ec-44e8-3c1318698661
    set admin enable
    set wtp-profile "831F"
    config radio-2
    end
  next
end
```

To configure Inter-Controller L3 roaming - CLI:

This configuration requires two FortiGate units. In order to enable L3 roaming supported VAP, both FortiGate units must have the same SSID, security, and passphrase.

The following example uses:

- AC1 as FGT40F
  - FAP1 as FAP433E
- AC2 as FGT81EP
  - FAP2 as FAP831F

1. Configure the L3 roaming peer IP for AC1 (FGT-40F):

```
config system interface
  edit "wan"
    set vdom "root"
    set ip 10.43.1.40 255.255.255.0
    set allowaccess ping https ssh http fabric
    set type physical
    set role wan
    set snmp-index 1
  next
end
config wireless-controller inter-controller
  set l3-roaming enable
  config inter-controller-peer
    edit 1
      set peer-ip 10.43.1.81
    next
  end
end
```

   a. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
config wireless-controller timers
  set client-idle-rehome-timeout 20
end
```

   b. configure the L3 roaming support SSID:

```
config wireless-controller vap
  edit "l3_rm1"
    set ssid "l3.roaming"
    set passphrase ENC
    set schedule "always"
    set l3-roaming enable
  next
end
config system interface
  edit "l3_rm1"
    set vdom "root"
    set ip 10.40.1.1 255.255.255.0
    set allowaccess ping
    set type vap-switch
    set role lan
    set snmp-index 18
  next
end
```

   c. Assign L3 roaming VAP to FAP433F:

```
config wireless-controller wtp-profile
  edit "433F"
    config platform
      set type 433F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess ssh
```

```
        config radio-1
          set mode disabled
        end
        config radio-2
          set band 802.11ax-5G
          set power-mode dBm
          set power-value 1
          set channel "36"
          set vap-all manual
          set vaps "13_rm1"
        end
        config radio-3
          set mode monitor
        end
      next
    end
    config wireless-controller wtp
      edit "FP433FXX00000000"
        set uuid b04f1cca-8528-51ec-2dc0-c744cbef4179
        set admin enable
        set wtp-profile "433F"
        config radio-2
        end
      next
    end
```

2. Configure the L3 roaming peer IP for AC2 (FGT-81EP):

```
config system interface
  edit "wan"
    set vdom "root"
    set ip 10.43.1.81 255.255.255.0
    set allowaccess ping https ssh http fabric
    set type physical
    set role wan
    set snmp-index 1
  next
end
config wireless-controller inter-controller
  set l3-roaming enable
  config inter-controller-peer
    edit 1
      set peer-ip 10.43.1.40
    next
  end
end
```

   a. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
    config wireless-controller timers
      set client-idle-rehome-timeout 20
    end
```

   b. configure the L3 roaming support SSID:

```
    config wireless-controller vap
      edit "l3_rm1"
        set ssid "l3.roaming"
```

```
    set passphrase ENC
    set schedule "always"
    set l3-roaming enable
  next
end
config system interface
  edit "l3_rm1"
    set vdom "root"
    set 10.81.2.1 255.255.255.0
    set allowaccess ping speed-test
    set type vap-switch
    set role lan
    set snmp-index 23
  next
end
```

c. Assign L3 roaming VAP to FAP831F:

```
config wireless-controller wtp-profile
  edit "831F"
    config platform
      set type 831F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess ssh
    config radio-1
      set mode disabled
    end
    config radio-2
      set band 802.11ax-5G
      set channel "36" "40"
      set vap-all manual
      set vaps "l3_rm1"
    end
    config radio-3
      set mode disabled
    end
  next
end
config wireless-controller wtp
  edit "FP831FXX00000000"
    set uuid 23ed4966-af92-51ec-44e8-3c1318698661
    set admin enable
    set wtp-profile "831F"
    config radio-2
    end
  next
end
```

3. Check the peer status from AC1 (FGT-40F):

```
FortiGate-40F  # diagnose wireless-controller wlac -c ha
WC fast failover info
    mode    : disabled
    l3r     : enabled
```

```
    peer cnt: 1
              FG81EPXX00000000 10.43.1.81:5246       UP 2
```

4. Check the peer status from AC2 (FGT-81EP):

```
FortiGate-81E-POE # diagnose wireless-controller wlac -c ha
WC fast failover info
    mode    : disabled
    l3r     : enabled
    peer cnt: 1
              FGT40FXX00000000 10.43.1.40:5246       UP 3
```

Understanding L3 roaming events for inter-controller L3 roaming for a tunnel mode SSID

When the wireless client is connected with "l3.roaming" on AP1 in AC1, the client receives IP 10.40.1.10 from AP1 in AC1:

```
FortiGate-40F # diagnose wireless-controller wlac -d sta online
   vf=0 wtp=2 rId=2 wlan=l3_rm1 vlan_id=0 ip=10.40.1.10 ip6=fe80::7766:7ffe:ee4d:c396
mac=a4:c3:f0:6d:69:33 vci= host=test-wifi user= group= signal=-65 noise=-95 idle=1 bw=3
use=7 chan=36 radio_type=11AC(wave2) security=wpa2_only_personal mpsk= encrypt=aes cp_
authed=no l3r=1,1 10.43.1.81:5247 -- 10.43.1.40:5247 33,0 online=yes mimo=2
```

When the client leaves AP1 and roams towards AP2, it connects with the same SSID "l3.roaming" on AP2. Wireless traffic passed from AP2 and is sent to AC2. Eventually the wireless traffic is transferred from AC2 to AC1 and traffic is maintained from AC1. The wireless client maintains the original IP of 10.40.1.10:

```
FortiGate-81E-POE # diagnose wireless-controller wlac -d sta online
   vf=0 wtp=3 rId=2 wlan=l3_rm1 vlan_id=0 ip=10.40.1.10 ip6=:: mac=a4:c3:f0:6d:69:33 vci=
host= user= group= signal=-66 noise=-95 idle=0 bw=2 use=7 chan=36 radio_type=11AC(wave2)
security=wpa2_only_personal mpsk= encrypt=aes cp_authed=no l3r=0,1 0.0.0.0:0 -- 0.0.0.0:0
0,0 online=yes mimo=2
```

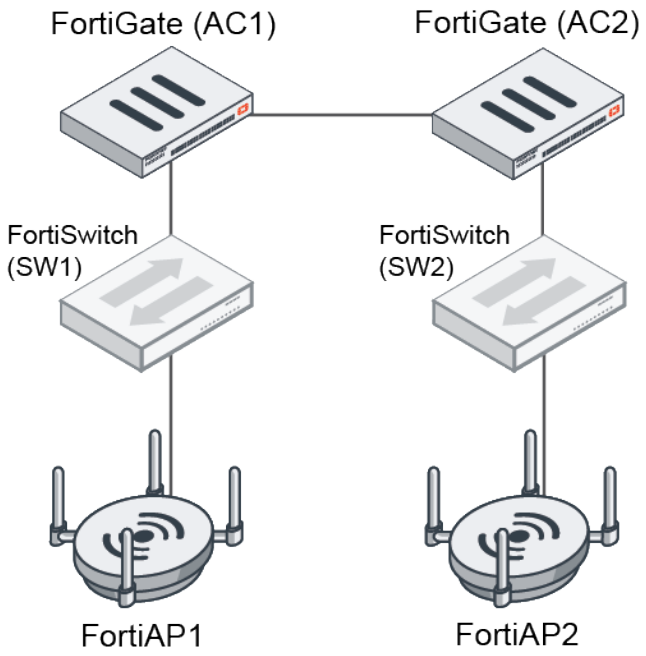
If the wireless client idle time exceeds `client-idle-rehome-timeout`, it triggers the rehome event. The wireless client will send a DHCP request and obtain a new IP address from AC2 (10.81.2.20). Now the wireless client traffic is maintained from AC2:

```
FortiGate-81E-POE # diagnose wireless-controller wlac -d sta online
   vf=0 wtp=3 rId=2 wlan=l3_rm1 vlan_id=0 ip=10.81.2.20 ip6=:: mac=a4:c3:f0:6d:69:33 vci=
host=test-wifi user= group= signal=-65 noise=-95 idle=0 bw=0 use=6 chan=36 radio_type=11AC
(wave2) security=wpa2_only_personal mpsk= encrypt=aes cp_authed=no l3r=1,0 0.0.0.0:0 --
0.0.0.0:0 0,0 online=yes mimo=2
```

Configuring L3 Roaming for Bridge Mode SSIDs

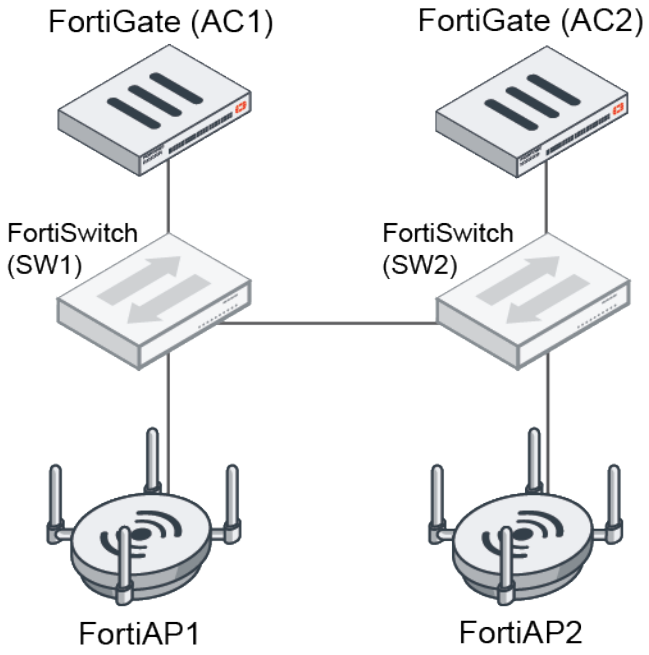
L3 roaming inter-controller topology using bridge mode SSIDs supports two roaming modes:

- **Indirect Mode**
  In indirect mode, the L3 handoff is handled by the mobility tunnel between the FortiGate Wireless Controllers.



- **Direct Mode**

  In direct mode, the two FortiAPs must be able to reach each other with no NAT in the path and the L3 handoff occurs between the FortiAPs directly.



Direct mode is preferred if it is feasible in the topology.

The following configurations require dynamic user VLAN assignment by RADIUS to be configured for RADIUS users per the steps in VLAN assignment by RADIUS on page 104, specifically, configuring RADIUS user attributes that are used for the VLAN ID assignment.

To configure Intra-Controller L3 roaming for a bridge mode SSID - CLI:

1. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
config wireless-controller timers
  set client-idle-rehome-timeout 20
end
```

2. configure the L3 roaming support bridge mode SSID and related VLAN interface:

```
 config wireless-controller vap
    edit "l3_br1"
        set ssid "L3Roaming_br1"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "wifi-radius"
        set local-bridging enable
        set schedule "always"
        set dynamic-vlan enable
        set l3-roaming enable
    next
end
config system interface
    edit "lan"
        set vdom "root"
        set ip 10.40.0.1 255.255.255.0
        set allowaccess ping https ssh http fabric
        set type hard-switch
        set stp enable
        set role lan
        set snmp-index 4
    next
end
config system interface
    edit "lan_100"
        set vdom "root"
        set ip 10.43.100.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 10
        set interface "lan"
        set vlanid 100
    next
end
```

3. Assign L3 roaming VAP to FAP433F:

```
config wireless-controller wtp-profile
    edit "433F"
        config platform
            set type 433F
            set ddscan enable
        end
        set handoff-sta-thresh 55
        config radio-1
            set mode disabled
        end
```

```
        config radio-2
            set band 802.11ax-5G
            set vap-all manual
            set vaps "l3_br1"
            set channel "36"
        end
        config radio-3
            set mode disabled
        end
    next
end
config wireless-controller wtp
    edit "FP433FXX00000000"
        set uuid b04f1cca-8528-51ec-2dc0-c744cbef4179
        set admin enable
        set wtp-profile "433F"
        config radio-2
        end
    next
end
```

4. Assign L3 roaming VAP to FAP831F:

```
config wireless-controller wtp-profile
    edit "831F.1"
        config platform
            set type 831F
            set ddscan enable
        end
        set handoff-sta-thresh 55
        set allowaccess https ssh
        config radio-1
            set mode disabled
        end
        config radio-2
            set band 802.11ax-5G
            set power-level 99
            set vap-all manual
            set vaps "l3_br1"
            set channel "36" "40"
        end
        config radio-3
            set mode disabled
        end
    next
end
config wireless-controller wtp
    edit "FP831FXX00000000"
        set uuid b867ca7c-cbc5-51ec-d5ac-4a395282be68
        set admin enable
        set wtp-profile "831F.1"
        config radio-2
        end
    next
end
```

To configure Inter-Controller L3 roaming for a bridge mode SSID - CLI:

This configuration requires two FortiGate units. In order to enable L3 roaming supported VAP, both FortiGate units must have the same SSID, security, and passphrase.

The following example uses:

- AC1 as FGT40F
  - FAP1 as FAP433E
- AC2 as FGT81EP
  - FAP2 as FAP831F

1. Configure the L3 roaming peer IP for AC1 (FGT-40F):

```
config system interface
  edit "wan"
    set vdom "root"
    set ip 10.43.1.40 255.255.255.0
    set allowaccess ping https ssh http fabric
    set type physical
    set role wan
    set snmp-index 1
  next
end
config wireless-controller inter-controller
  set l3-roaming enable
  config inter-controller-peer
    edit 1
      set peer-ip 10.43.1.81
    next
  end
end
```

   a. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
config wireless-controller timers
  set client-idle-rehome-timeout 20
end
```

   b. Configure the L3 roaming support bridge mode SSID and related VLAN interface:

```
config wireless-controller vap
    edit "l3_br1"
        set ssid "L3Roaming_br1"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "wifi-radius"
        set local-bridging enable
        set schedule "always"
        set dynamic-vlan enable
        set l3-roaming enable
        set l3-roaming-mode indirect
    next
end
config system interface
    edit "lan"
        set vdom "root"
        set ip 10.40.0.1 255.255.255.0
```

```
            set allowaccess ping https ssh http fabric
            set type hard-switch
            set stp enable
            set role lan
            set snmp-index 4
        next
    end
    config system interface
        edit "lan_100"
            set vdom "root"
            set ip 10.43.100.1 255.255.255.0
            set allowaccess ping
            set device-identification enable
            set role lan
            set snmp-index 10
            set interface "lan"
            set vlanid 100
        next
    end
```

c. Assign L3 roaming VAP to FAP433F:

```
config wireless-controller wtp-profile
    edit "433F"
        config platform
            set type 433F
            set ddscan enable
        end
        set handoff-sta-thresh 55
        config radio-1
            set mode disabled
        end
        config radio-2
            set band 802.11ax-5G
            set vap-all manual
            set vaps "l3_br1"
            set channel "36"
        end
        config radio-3
            set mode disabled
        end
    next
end
config wireless-controller wtp
    edit "FP433FXX00000000"
        set uuid b04f1cca-8528-51ec-2dc0-c744cbef4179
        set admin enable
        set wtp-profile "433F"
        config radio-2
        end
    next
end
```

2. Configure the L3 roaming peer IP for AC2 (FGT-81EP):

```
config system interface
  edit "wan1"
```

```
    set vdom "root"
    set ip 10.43.1.81 255.255.255.0
    set allowaccess ping https ssh http fabric
    set type physical
    set role wan
    set snmp-index 1
  next
end
config wireless-controller inter-controller
  set l3-roaming enable
  config inter-controller-peer
    edit 1
      set peer-ip 10.43.1.40
    next
  end
end
```

a. Configure the `client-idle-rehome-timeout` (default is 20 seconds):

```
config wireless-controller timers
  set client-idle-rehome-timeout 20
end
```

b. Configure the L3 roaming support bridge mode SSID and related VLAN interface:

```
config wireless-controller vap
    edit "l3_br1"
        set ssid "L3Roaming_br1"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "wifi-radius"
        set local-bridging enable
        set schedule "always"
        set dynamic-vlan enable
        set l3-roaming enable
        set l3-roaming-mode indirect
    next
end
config system interface
    edit "lan_hw"
        set vdom "root"
        set ip 10.81.0.129 255.255.255.0
        set allowaccess ping https ssh http fabric
        set type hard-switch
        set stp enable
        set role lan
        set snmp-index 52
    next
end
config system interface
    edit "lan_100"
        set vdom "root"
        set ip 10.81.100.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 34
```

```
            set interface "lan_hw"
            set vlanid 100
        next
    end
```

c. Assign L3 roaming VAP to FAP831F:

```
config wireless-controller wtp-profile
    edit "831F.1"
        config platform
            set type 831F
            set ddscan enable
        end
        set handoff-sta-thresh 55
        set allowaccess https ssh
        config radio-1
            set mode disabled
        end
        config radio-2
            set band 802.11ax-5G
            set power-level 99
            set vap-all manual
            set vaps "l3_br1"
            set channel "36" "40"
        end
        config radio-3
            set mode disabled
        end
    next
end
config wireless-controller wtp
    edit "FP831FXX00000000"
        set uuid b867ca7c-cbc5-51ec-d5ac-4a395282be68
        set admin enable
        set wtp-profile "831F.1"
        config radio-2
        end
    next
end
```

3. Check the peer status from AC1 (FGT-40F):

```
FortiGate-40F  # diagnose wireless-controller wlac -c ha
WC fast failover info
    mode    : disabled
    l3r     : enabled
    peer cnt: 1
              FG81EPXX00000000 10.43.1.81:5246       UP 0
```

4. Check the peer status from AC2 (FGT-81EP):

```
FortiGate-81E-POE # diagnose wireless-controller wlac -c ha
WC fast failover info
    mode    : disabled
    l3r     : enabled
    peer cnt: 1
              FGT40FXX00000000 10.43.1.40:5246       UP 0
```

Understanding L3 roaming events for inter-controller L3 roaming for a bridge mode SSID

When the wireless client is connected with "L3Roaming_br1" on AP1 in AC1, the client receives IP 10.43.100.2 from AP1 in AC1, bridged to "lan_100" VLAN interface:

```
FortiGate-40F # diagnose wireless-controller wlac -d sta online
   vf=0 wtp=2 rId=2 wlan=l3_br1 vlan_id=100 ip=10.43.100.2 ip6=fe80::c84:737e:2ba0:7ae2
mac=22:cf:0e:1a:7f:d2 vci= host= user=vlan0100 group=wifi-radius signal=-67 noise=-95 idle=6
bw=0 use=6 chan=36 radio_type=11AC security=wpa2_only_enterprise mpsk= encrypt=aes cp_
authed=no l3r=1,0 G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

When the client leaves AP1 and roams towards AP2, it connects with the same SSID "L3Roaming_br1" on AP2. Wireless traffic passes from AP2 and is sent to AC2. Eventually the wireless traffic is transferred from AC2 to AC1 and traffic is maintained from AC1. The wireless client maintains the original IP of 10.43.100.2:

```
FortiGate-81E-POE # diagnose wireless-controller wlac -d sta online
   vf=0 wtp=10 rId=2 wlan=l3_br1 vlan_id=0 ip=10.43.100.2 ip6=:: mac=22:cf:0e:1a:7f:d2 vci=
host= user=vlan0100 group=wifi-radius signal=-58 noise=-95 idle=1 bw=5 use=7 chan=36 radio_
type=11AC security=wpa2_only_enterprise mpsk= encrypt=aes cp_authed=no l3r=0,1
G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

If the wireless client idle time exceeds `client-idle-rehome-timeout`, it triggers the rehome event. The wireless client will send a DHCP request and obtain a new IP address from AC2 (10.81.100.2). Now the wireless client traffic is maintained from AC2:

```
FortiGate-81E-POE # diagnose wireless-controller wlac -d sta online
   L vf=0 wtp=10 rId=2 wlan=l3_br1 vlan_id=100 ip=10.81.100.2 ip6=fe80::c84:737e:2ba0:7ae2
mac=22:cf:0e:1a:7f:d2 vci= host= user=vlan0100 group=wifi-radius signal=-55 noise=-95 idle=3
bw=0 use=6 chan=36 radio_type=11AC security=wpa2_only_enterprise mpsk= encrypt=aes cp_
authed=no l3r=1,0 G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

Advanced Wireless Features

By default, the FortiGate GUI hides advanced features to simplify the site layout. You can go to *System* > *Feature Visibility* to enable different types advanced features, including Advanced Wireless Features.

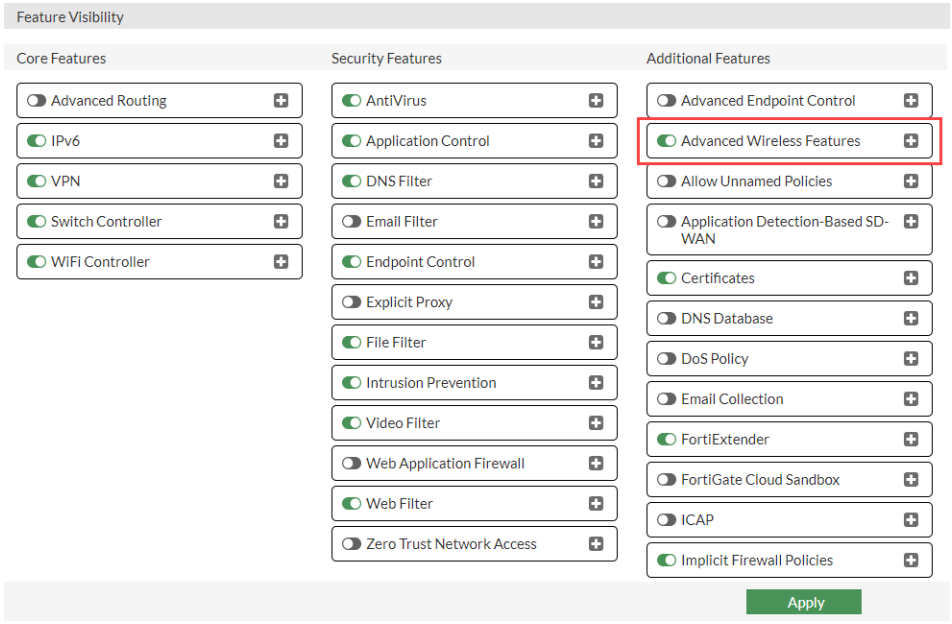
After enabling Advanced Wireless Features, several entries in the Navigation bar will change names.

- Operations Profiles Entry on page 166: FortiAP, QoS, and FortiAP Configuration.
- Connectivity Profiles Entry on page 171: MPSK and Bonjour.
- Protection Profiles Entry on page 178: WIDS and L3 Firewall (also known as L3 Access Control List configurations for FortiAPs).
- The following additional advanced wireless features under the Advanced SSID options on page 180 and Advanced WiFi Settings options on page 182 become available.
  - *SSIDs* > *Edit Interface.*
  - *WiFi Settings.*

Note that this guide is intended to be used when Advanced Wireless Features is disabled, and therefore uses the default entry names. If a topic covers a feature that requires Advanced Wireless Features to be enabled, it will specify users must first enable Advanced Wireless Features.

To enable Advanced Wireless Features - GUI:

1. From the FortiOS GUI, go to *System* > *Feature Visibility*.
2. Under the *Additional Features* column, locate and enable *Advanced Wireless Features*.



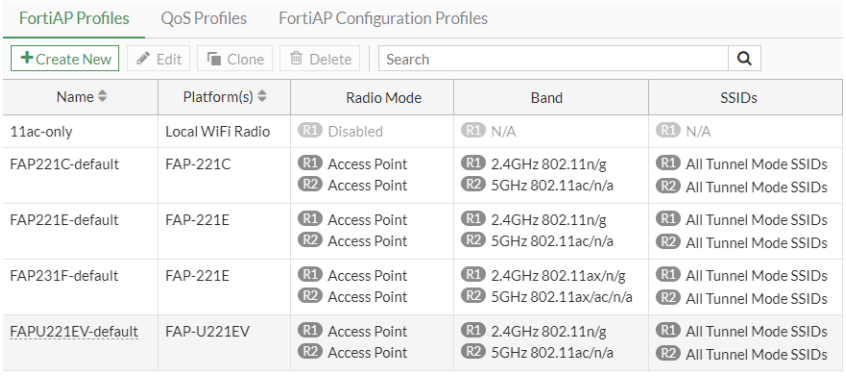
3. Click *Apply*.
   The Navigation bar reloads with the new features visible.

To enable Advanced Wireless Features - CLI:

```
config system settings
    set gui-advanced-wireless-features enable
end
```

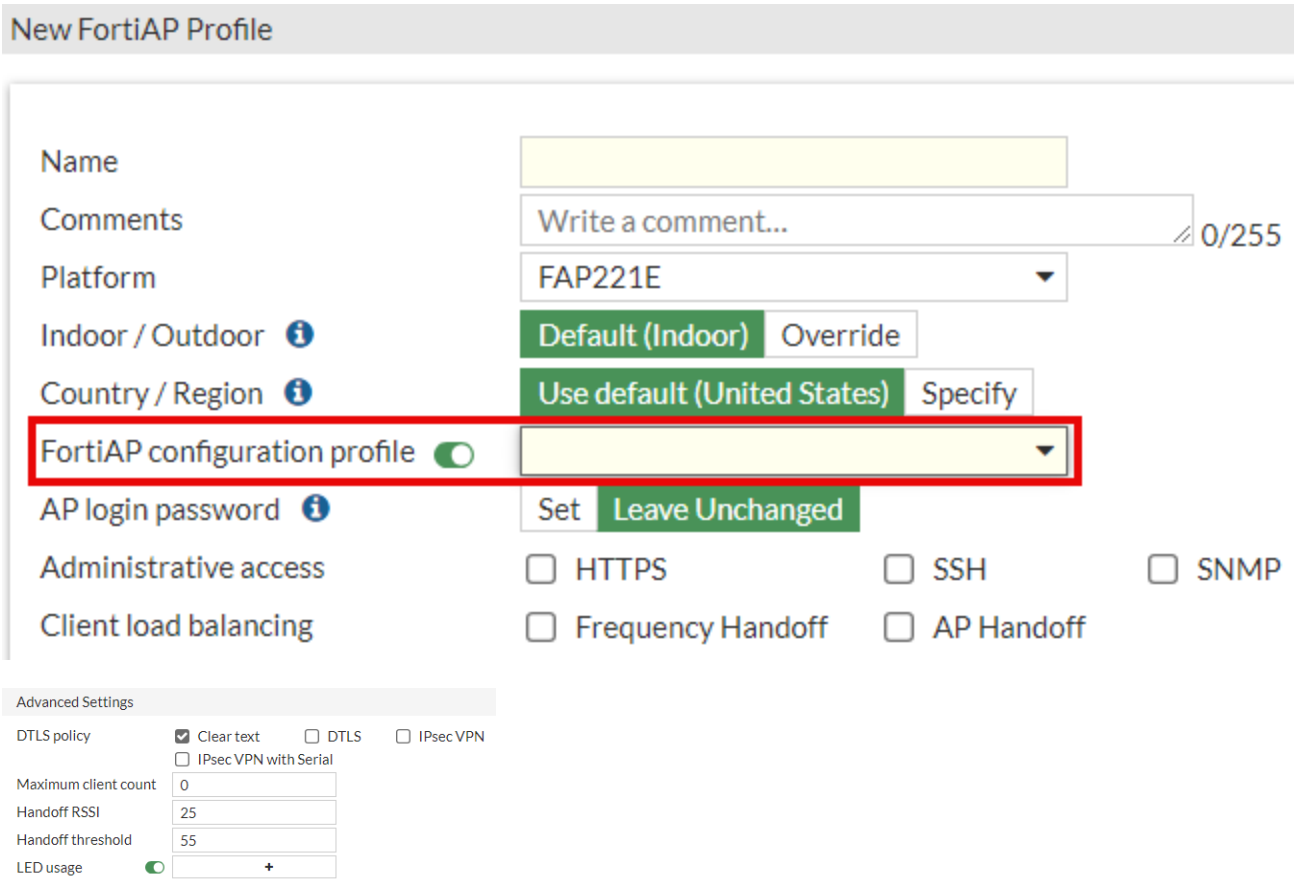
Operations Profiles Entry

When you enable Advanced Wireless Features, FortiAP Profiles is renamed to Operation Profiles and contains additional tabs that enable you to manage QoS and FortiAP Configuration profiles.



FortiAP Profiles

When you create or edit a FortiAP profile, you can apply a FortiAP Configuration Profile (see FortiAP Configuration Profiles on page 170) and configure additional advanced settings:



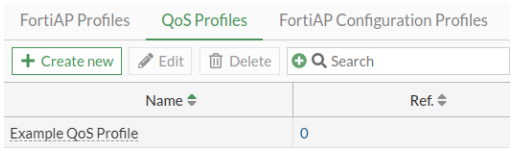
These fields correspond to the following CLI settings under `config wireless-controller wtp-profile`:

DTLS Policy	Select which DTLS policy you want to apply to the profile. See WiFi data channel encryption on page 295.	`set dtls-policy {option1}, {option2}, …`
Maximum client count	Limit the number of clients. See Limiting the number of clients on page 91.	`set max-clients {integer}`
Handoff RSSI	Set the minimum handoff RSSI threshold for when FortiAP applies load balancing to a client. See Setting the handoff RSSI threshold on page 285.	`set handoff-rssi {integer}`
Handoff threshold	Set the number of clients at which AP load balancing begins. See Setting the AP load balance threshold on page 285.	`set handoff-sta-thresh {integer}`
LED usage	Enable or disable LEDs.	`set led-state [enable|disable]` `set led-schedules <name1>,`

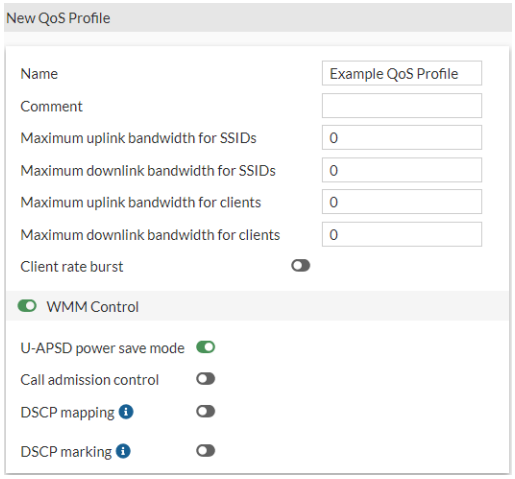
	When you enable LED usage, you can also assign recurring firewall schedules for illuminating the LEDs. See LED options on page 235.	`<name2>, ...`

QoS Profiles

In the *QoS Profiles* tab, you can create or edit Quality of Service (QoS) profiles.



Click *Create new* to create a QoS profile.



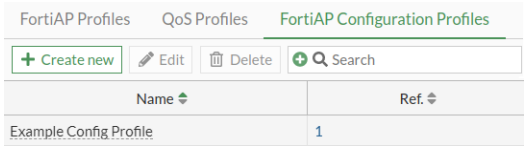
These fields correspond to the following CLI settings under `config wireless-controller qos-profile`:

Name	Enter a name for the profile.	`edit <name>`
Comment	Optionally, enter comments.	`set comment {string}`
Maximum uplink bandwidth for SSIDs	The maximum uplink speed (VAPs), in Kbps.	`set uplink {integer}`
Maximum downlink bandwidth for SSIDs	The maximum downlink speed (VAPs), in Kbps.	`set downlink {integer}`
Maximum uplink bandwidth for clients	The maximum uplink speed (Clients), in Kbps.	`set uplink-sta {integer}`
Maximum downlink bandwidth for clients	The maximum downlink speed (Clients), in Kbps.	`set downlink-sta {integer}`
Client rate burst	Enable/disable client rate burst.	`set burst [enable|disable]`
WMM Control	Enable/disable WiFi Multimedia (WMM) control.	`set wmm [enable|disable]`

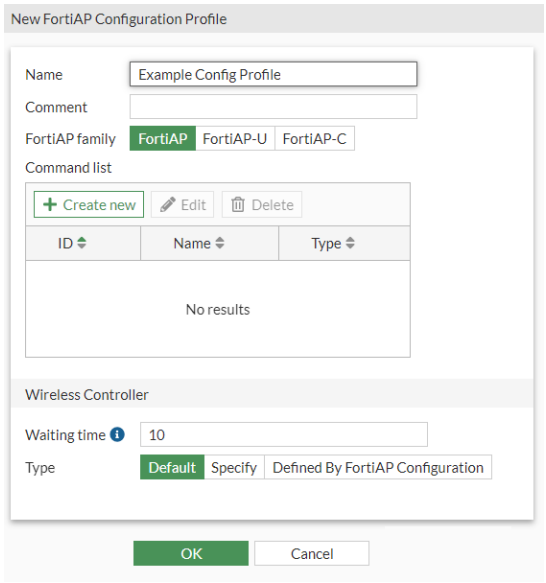
U-APSD power save mode	Enable/disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode. This option is only available if *WMM Control* is enabled.	`set wmm-uapsd [enable|disable]`
Call admission control	Enable/disable WMM call admission control. This option is only available if *WMM Control* is enabled.	`set call-admission-control [enable|disable]`
Maximum VoWLAN phones count	Maximum number of Voice over WLAN. Shown when *Call admission control* is enabled.	`set call-capacity {integer}`
Bandwidth admission control	Enable/disable WMM bandwidth admission control. This option is only available if *Call admission control* is enabled.	`set bandwidth-admission-control [enable|disable]`
Maximum bandwidth capacity (Kbps)	Maximum bandwidth capacity allowed. Shown when Bandwidth admission control is enabled	`set bandwidth-capacity {integer}`
DSCP mapping	Enable/disable differentiated Services Code Point (DSCP) mapping.	`set dscp-wmm-mapping [enable|disable]`
Voice access	DSCP mapping for voice access. Shown when *DSCP mapping* is enabled.	`set dscp-wmm-vo <id1>, <id2>, …`
Video access	DSCP mapping for video access Shown when *DSCP mapping* is enabled.	`set dscp-wmm-vi <id1>, <id2>, …`
Best effort access	DSCP mapping for best effort access. Shown when *DSCP mapping* is enabled.	`set dscp-wmm-be <id1>, <id2>, …`
Background access	DSCP mapping for background access Shown when *DSCP mapping* is enabled.	`set dscp-wmm-bk <id1>, <id2>, …`
DSCP marking	Enable/disable differentiated Services Code Point (DSCP) marking..	`set wmm-dscp-marking [enable|disable]`
Voice access	DSCP marking for voice access. Shown when *DSCP marking* is enabled.	`set wmm-vo-dscp {integer}`
Video access	DSCP marking for video access. Shown when *DSCP marking* is enabled.	`set wmm-vi-dscp {integer}`
Best effort access	DSCP marking for best effort access. Shown when *DSCP marking* is enabled.	`set wmm-be-dscp {integer}`
Background access	DSCP marking for background access. Shown when *DSCP marking* is enabled.	`set wmm-bk-dscp {integer}`

FortiAP Configuration Profiles

In the *FortiAP Configuration Profiles* tab, you can create or edit FortiAP Configuration Profiles for managing local FortiAP configurations.



Click *Create new* to create a FortiAP Configuration profile. You can select which FortiAP family you want to apply local configurations to.



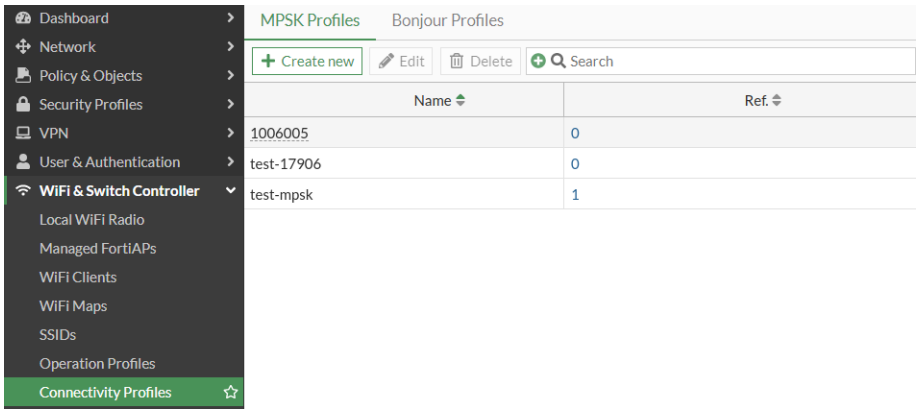
In *Command list*, you can create a list of commands you want to apply to a local FortiAP. Enter the name of the command you want to apply and the value you want to take effect. These fields correspond to the following CLI settings under `config wireless-controller apcfg-profile`:

Name	Enter a name for the profile.	`edit <name>`
Comment	Optionally, enter comments.	`set comment {var-string}`
FortiAP family	FortiAP family type.	`set ap-family [fap|fap-u|...]`
Command list > New / Edit Command	Configure FortiAP local configuration commands. For the command names and possible values, see FortiAP CLI configuration and diagnostics commands on page 439	`config command-list`
ID	Enter a command ID.	`edit <id>`
Name	Enter the name of the FortiAP local configuration command name. For example, AC_DISCOVERY_TYPE.	`set name {string}`

Type	Select the command type.	`set type [non-password|password]`
Value/Password	Set the AP local configuration command value or password depending on the command *Type* you selected. For example, if you entered AC_DISCOVERY_TYPE, enter 6 for Multicast.	`set value {string} / set passwd-value {password}`
Waiting time	Maximum waiting time in minutes for the AP to join the wireless controller after applying AP local configuration.	`set ac-timer {integer}`
Type	Validation controller type: • *Default*: This controller is the one and only controller that the AP could join after applying AP local configuration. • *Specify*: Specified controller is the one and only controller that the AP could join after applying AP local configuration. • *Defined by FortiAP Configuration*: Any controller defined by AP local configuration after applying AP local configuration.	`set ac-type [default|specify|...]`
IP	IP address of the validation controller that AP must be able to join after applying AP local configuration. Shown when *Type* is set to *Specify*.	`set ac-ip {ipv4-address}`
Port	Port of the validation controller that AP must be able to join after applying AP local configuration. Shown when *Type* is set to *Specify*.	`set ac-port {integer}`

Connectivity Profiles Entry

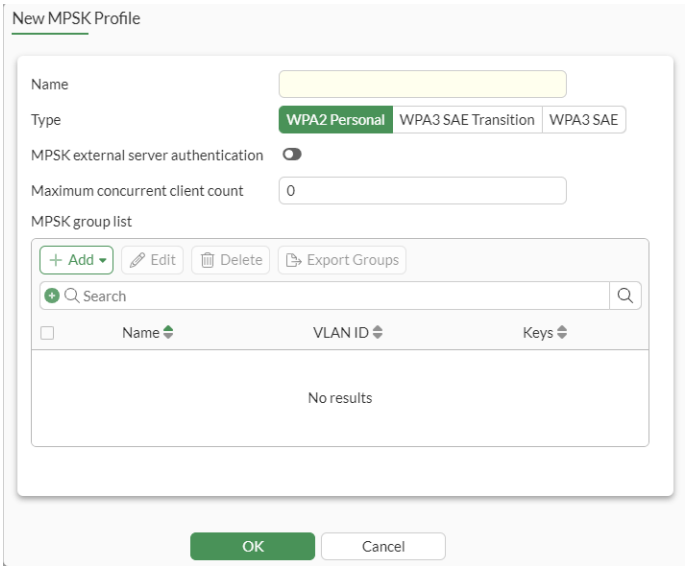
You can access Connectivity Profiles to manage your MPSK and Bonjour profiles.



MPSK Profiles

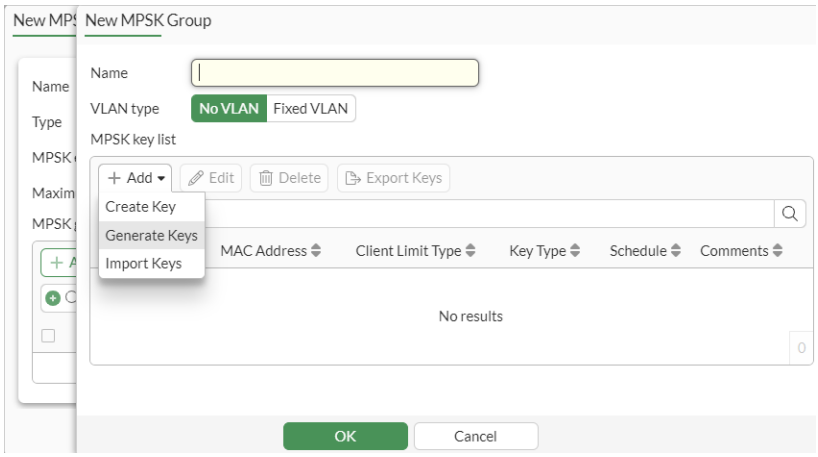
After you click *Connectivity Profile*, the *MPSK Profiles* tab loads by default. From there you can create or edit MPSK profiles to manage multiple pre-shared keys.

Click *Create new* to create an MPSK profile.



From there you can make the following configurations:

- Select a security *Type*.
- Select if you want to enable *MPSK external server authentication*.
- Enter the *Maximum concurrent client count*.
- Click *Add* to create or import MPSK groups and determine how you want to *Create*, *Generate*, or *Import* MPSK keys.



These fields correspond to the following CLI settings under `config wireless-controller mpsk-profile`:

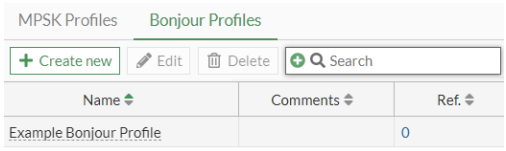
Name	MPSK profile name.	`edit <name>`
Type	Select the security type of keys for this profile.	`set mpsk-type [wpa2-`

		`personal|wpa3-sae|...]`
MPSK external server authentication	Enable/Disable MPSK external server authentication.	`set mpsk-external-server-auth [enable|disable`
MPSK external server	RADIUS server to be used to authenticate MPSK users.	`set mpsk-external-server {string}`
Maximum concurrent client count	Maximum number of concurrent clients that connect using the same passphrase in multiple PSK authentication.	`set mpsk-concurrent-clients {integer}`
MPSK Group List > New/Edit MPSK Group	List of multiple PSK groups.	`config mpsk-group`
Name	MPSK group name.	`edit <name>`
VLAN type	MPSK group VLAN options.	`set vlan-type [no-vlan|fixed-vlan]`
VLAN ID	Optional VLAN ID. Shown when *VLAN type* is set to *Fixed VLAN*.	`set vlan-id {integer}`
MPSK key list > New / Edit MPSK Key	List of multiple PSK entries.	`config mpsk-key`
Name	Pre-shared key name.	`edit <name>`
Comment	Enter optional comment.	`set comment {var-string}`
Type	Select the security type of the key.	`set key-type [wpa2-personal|wpa3-sae]`
SAE password	WPA3 SAE password.	`set sae-password {password}`
SAE-PK authentication	Enable/disable WPA3 SAE-PK.	`set sae-pk [enable|disable]`
SAE-PK private key	Private key used for WPA3 SAE-PK authentication.	`set sae-private-key {string}`
Pre-shared key	WPA Pre-shared key.	`set passphrase {password}`
MAC address	MAC address.	`set mac {mac-address}`
Client limit type	MPSK client limit type options. • *Default*: Use the value in profile configuration. • *Unlimited*: Unlimited number of clients. • *Specified*: Specify the *Client limit*.	`set concurrent-client-limit-type [default|unlimited|...]`
Client limit	Number of clients that can connect using this pre-shared key. Shown when *Client limit type* is set to *Specified*.	`set concurrent-clients {integer}`

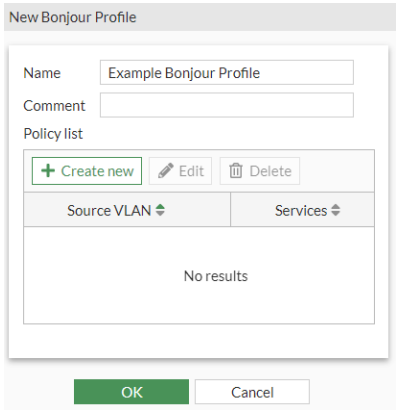
MPSK schedule	Firewall schedule for MPSK passphrase. The passphrase will be effective only when at least one schedule is valid.	`set mpsk-schedules <name1>, <name2>, …`

Bonjour Profiles

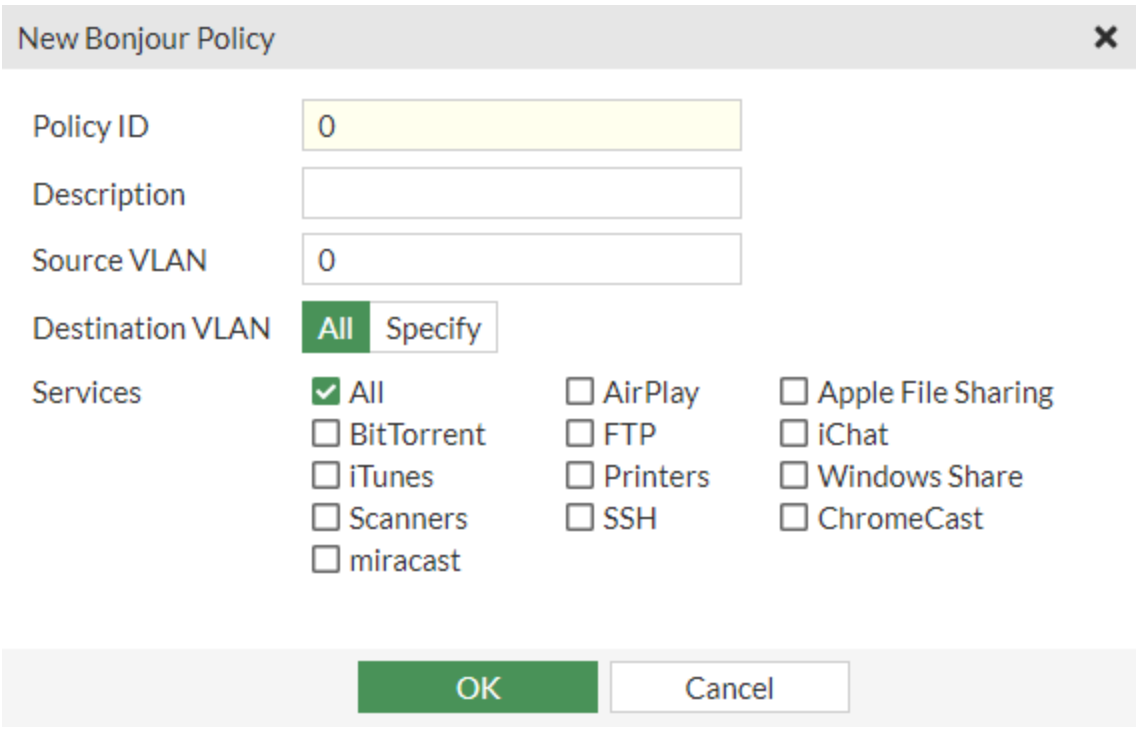
Bonjour is Apple's zero configuration networking protocol. Bonjour profiles allow FortiAPs to connect to networks using Bonjour. You can create or edit Bonjour profiles by clicking the *Bonjour Profiles* tab.



Click *Create new* to create a Bonjour profile.



From there you can create and add policies that determine which services you want to advertise across the network.



These fields correspond to the following CLI settings under `config wireless-controller bonjour-profile`:

Name	Enter a name for the profile.	`edit <name>`
Comment	Optionally, enter comments.	`set comment {string}`
Policy list > New/Edit Bonjour Policy	Configure the policy list.	`config policy-list`
Policy ID	Enter the Policy ID.	`edit <policy-id>`
Description	Description of the Bonjour profile policy.	`set description {string}`
Source VLAN	The VLAN ID that the Bonjour service will be advertised from.	`set from-vlan {string}`
Destination VLAN	The VLAN ID that the Bonjour service will be made available to.	`set to-vlan {string}`
Services	Select services for the VLAN.	`set services {option1}, {option2}, …`

To apply a Bonjour profile at the FortiAP profile level - CLI:

Once you create a Bonjour profile, you can apply it at the FortiAP profile and device level.

```
config wireless-controller wtp-profile
  edit FAP234F-default
    set bonjour-profile "Example-Bonjour-Profile"
  next
end
```

If a Bonjour profile is applied at both the device and profile level, the configuration made at the device level takes precedence. If a Bonjour profile is applied to multiple APs, the APs execute an algorithm to determine the Bonjour Default Gateway. The AP with the highest base MAC address is selected as the primary default gateway while the other APs are designated as backup default gateways in case the primary default gateway becomes unavailable.

To verify that the Bonjour profile is successfully applied to a FortiAP:

1. From the FortiAP CLI, enter `cw_diag -c bonjour`:

```
cw_diag -c bonjour
Bonjour Gateway: Controlled by AC
Configured Bonjour Vlans:
    10    ==> 20    services 00000001  all
    101   ==> 202   services 00000001  all
Total 2 Bonjour Vlans
Bonjour Gateway Election Info:
1/2 e8:ed:d6:a5:2e:e8 state=cap,8825 live=16605 age=1
2/2 e8:ed:d6:a5:31:08 state=oper,8807 live=8825 age=1
---- e0:23:ff:b2:18:68 state=cap,16609
```

The diagnoses output also provides details of the last election process under "Bonjour Gateway Election Info". The AP with the MAC address of `8:ed:d6:a5:31:08` is in the `oper` state, meaning it serves as the default gateway. The other APs are in the `cap` state, meaning they act as back-up gateways in case the primary gateway becomes unavailable. If there are any more APs in the same setup, they will go into a `hold` state.

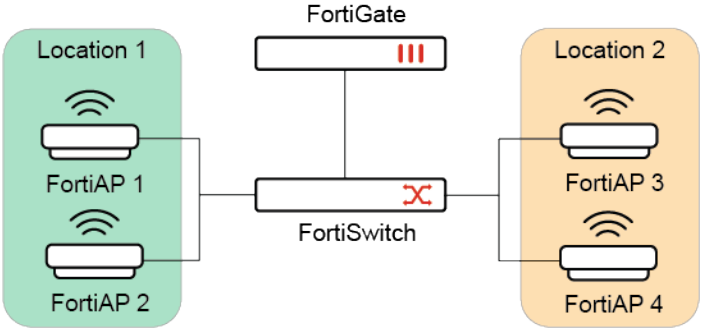
Isolate mDNS traffic on the Bonjour profile

Bonjour profiles can isolate multicast Domain Name System (mDNS) traffic using the Micro-Location feature. Micro-Location confines mDNS traffic originating from one location so that it remains isolated from other locations. In this scenario, "location" is defined by the FortiAP group configured on the FortiGate.

This enables you to confine mDNS traffic within designated areas of the network, specifically targeting the same SSID and VLAN, on a per-AP or AP group level. For example, you can segregate your FortiAPs by zones such as floor1 or floor2.

To isolate mDNS traffic with Micro-Location:

In this example, there are four FortiAP devices located in two separate locations.



1. Configure a Bonjour profile with a policy list and enable `micro-location`.

```
config wireless-controller bonjour-profile
  edit "micro-loc"
    set micro-location enable
    config policy-list
      edit 1
        set from-vlan "100"
        set to-vlan "200"
        set services airplay printers chromecast
      next
    end
  next
end
```

2. Apply the Bonjour profile to a FortiAP profile.

```
config wireless-controller wtp-profile
  edit "FAP231G-default"
    config platform
      set type 231G
    end
    set bonjour-profile "micro-loc"
    set handoff-sta-thresh 55
    config radio-1
      set mode disabled
    end
    config radio-2
      set band 802.11a 802.11n-5G 802.11ac-5G 802.11ax-5G
      set channel-bonding 40MHz
      set vap-all manual
      set vaps "wifi.fap.01" "wifi.fap.02"
    end
    config radio-3
      set mode disabled
    end
  next
end
```

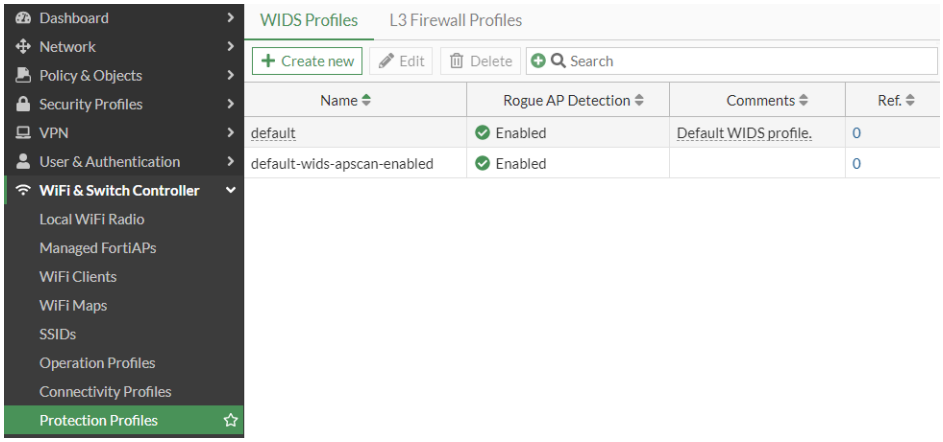
3. Once the Bonjour profile is added to the FortiAP profile, the Bonjour function determines each FortiAP's location based on the FortiAP group the device belongs to. Since this example has four FortiAP units located in two places, you will need to create two FortiAP group to define each location.

```
config wireless-controller wtp-group
  edit "Loc-1"
    set wtps "FP231GTF23042734" "FP231GTF23045868"
  next
  edit "Loc-2"
    set wtps "FP231GTF23046245" "FP231GTF23041369"
  next
end
```

4. From the FortiGate, verify the configurations have been successful made with `diagnose wireless-controller wlac -c bjprof`.
5. From the FortiAPs in each location, verify the configurations have been successful made with `cw_diag -c bonjour` and `bjallow`.

Protection Profiles Entry

When you enable Advanced Wireless Features, WIDS Profiles is renamed to Protection Profiles and contains additional tabs that enable you to manage L3 Firewall Profiles.

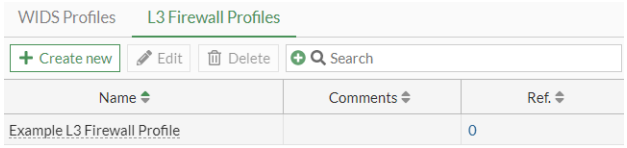


WIDS Profiles

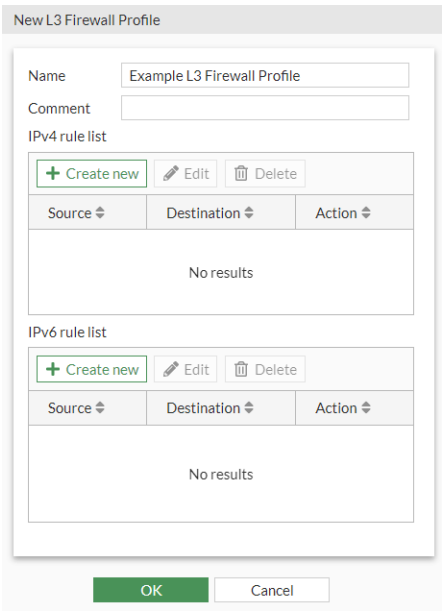
After you click *Protection Profiles*, the *WIDS Profiles* tab loads by default. From there you can create or edit WIDS profiles to configure the type of security threats you want to monitor.

L3 Firewall Profile

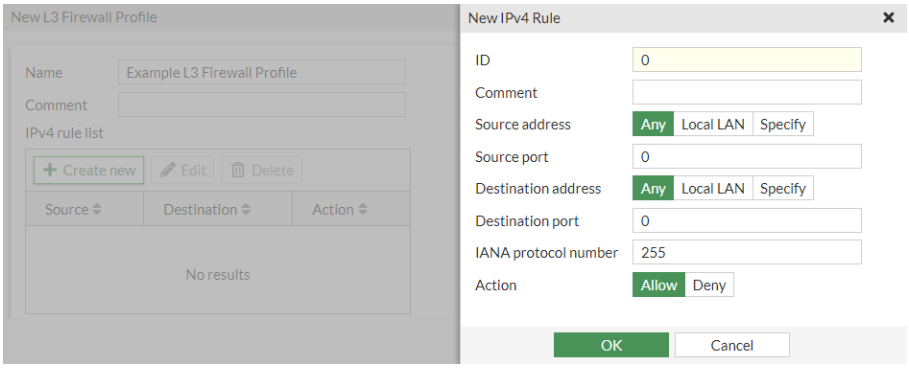
In the *L3 Firewall Profiles* tab, you can create or edit L3 Firewall Profiles to configure the WiFi bridge access control list.



Click *Create new* to create a L3 Firewall profile.



From there, you can create IPv4 or IPv6 rule lists to allow or deny traffic that matches the configured policy.



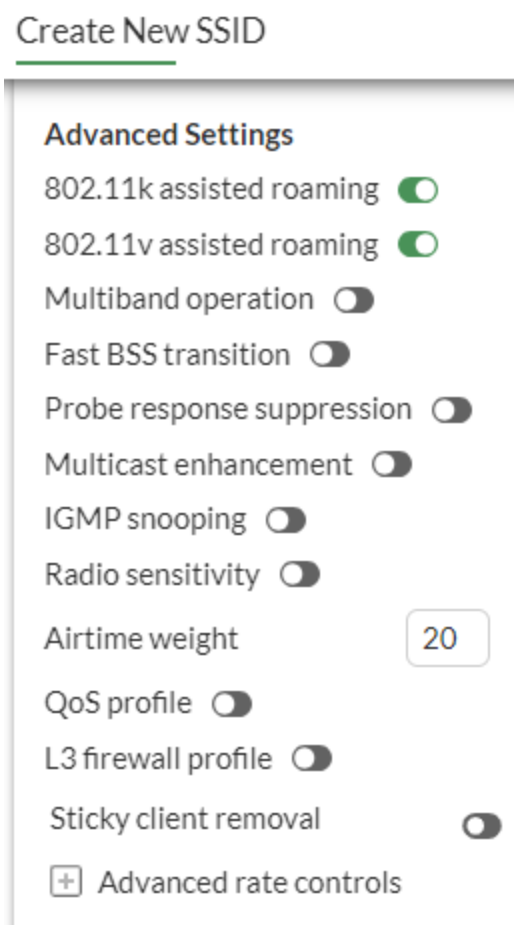
These fields correspond to the following CLI settings:

L3 Firewall Profiles > New/Edit L3 Firewall Profile	`config wireless-controller access-control-list`
Name	`edit <name>`
Comment	`set comment {string}`
IPv4 rule list > New/Edit IPv4 Rule	`config layer3-ipv4-rules`
ID	`edit <rule-id>`
Comment	`set comment {string}`
Source address	`set srcaddr {user}`
Source port	`set srcport {integer}`
Destination address	`set dstaddr {user}`

Destination port	set dstport {integer}
IANA protocol number	set protocol {integer}
Action	set action [allow|deny]
IPv6 rule list > New/Edit IPv6 Rule	config layer3-ipv6-rules
ID	edit <rule-id>
Comment	set comment {string}
Source address	set srcaddr {user}
Source port	set srcport {integer}
Destination address	set dstaddr {user}
Destination port	set dstport {integer}
IANA protocol number	set protocol {integer}
Action	set action [allow|deny]

Advanced SSID options

When you create or edit an SSID, you can configure additional advanced settings.



These fields correspond to the following CLI settings:

802.11k assisted roaming	When 802.11k is enabled, APs provide clients with a list of other neighboring APs and a site report, passively assisting roaming clients in deciding which APs to connect to.	`set 80211k`
802.11v assisted roaming	When 802.11v is enabled, APs help clients choose the least congested AP by actively sending deauthentication frames to clients that try to connect to congested APs when other APs have better RSSI.	`set 80211v`
Multiband operation	Enable/disable Multiband Operation (see Configuring Agile Multiband Operation on page 187	`set mbo`
Fast BSS transition	Enable/disable 802.11r Fast BSS Transition.	`set fast-bss-transition`
Probe response suppression	Enable/disable probe response suppression.	`set probe-resp-suppression`
Multicast enhancement	Enable/disable converting multicast to unicast to improve performance (see Enabling multicast enhancement on page 92).	`set multicast-enhance`

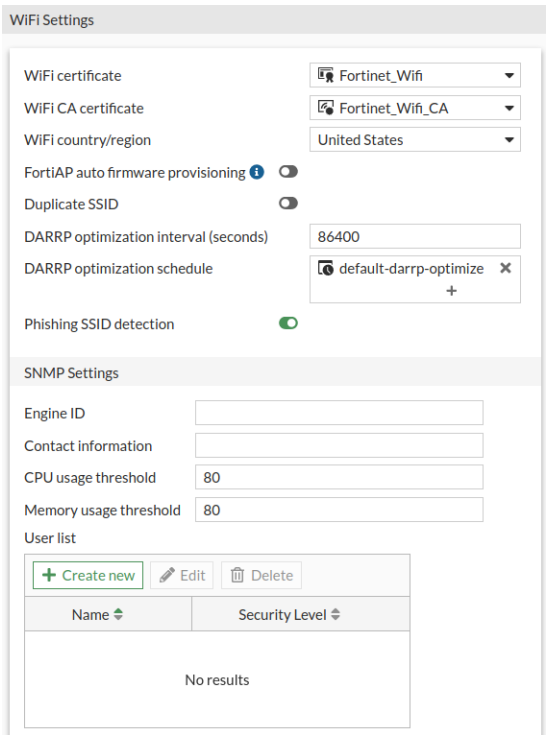
IGMP snooping	Enable/disable IGMP snooping to allow the wireless controller to detect which FortiAP(s) have IGMP clients. The wireless controller will only forward a multicast stream to the FortiAP where there is a listener for the multicast group. For more information, see Enabling IGMP Snooping on page 92.	`set igmp-snooping`
Radio sensitivity	Enable/disable software radio sensitivity.	`set radio-sensitivity`
Airtime weight	Set Airtime weight in percentage (see Airtime fairness on page 49).	`set atf-weight`
QoS profile	Enable to select a Quality of service profile. The QoS profile helps to set up different QoS parameters for voice, video, data wireless networks, or guest/employee wireless networks.	`set qos-profile`
L3 firewall profile	Enable to select a Layer 3 firewall profile. L3 firewall profile provides granular access control of client traffic in your wireless network. An L3 firewall profile allows or denies traffic between wireless clients based on the configured source and destination IP addresses/ports and specific protocols.	`set access-control-list`

Sticky client removal	Enable/disable sticky client removal and configure the minimum threshold in dBM required for clients to be serviced by the AP.	`set sticky-client-remove`
		`set sticky-client-threshold-2g`
		`sticky-client-threshold-5g`
		`sticky-client-threshold-6g`

Advanced rate controls	Set allowed data rates for *802.11a* and *802.11bg*: • *Mandatory*: Clients must support this data rate in order to associate with an access point on the controller. • *Supported*: Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate. • *Disabled*: The clients specify the data rates used for communication.	`set rates-11a` `set rates-11bg`
	Set allowed data rates for each *802.11n MCS* spatial stream.	`set rates-11n-ss12` `set rates-11n-ss34`

Advanced WiFi Settings options

More options are exposed on WiFi Settings page, including Duplicate SSID, DARRP related settings, Phishing SSID detection setting, and SNMP settings.



These fields correspond to the following WiFi CLI settings under `config wireless-controller setting`:

Duplicate SSID	Enable/disable allowing VAPs to use the same SSID name in the same VDOM.	`set duplicate-ssid [enable|disable]`
DARRP optimization interval (seconds)	Time for running Distributed Automatic Radio Resource Provisioning.	`set darrp-optimize {integer}`
DARRP optimization schedule	Firewall schedules for DARRP running time. DARRP will run periodically based on darrp-optimize within the schedules. Separate multiple schedule names with a space.	`set darrp-optimize-schedules <name1>, <name2>, …`
Phishing SSID detection setting	Enable/disable phishing SSID detection. For more information, see Suppressing phishing SSID on page 300	`set phishing-ssid-detect [enable|disable]`

These fields correspond to the following SNMP CLI settings under `config wireless-controller snmp`:

Engine ID	AC SNMP engineID string.	`set engine-id {string}`
Contact information	Contact Information.	`set contact-info {string}`
CPU usage threshold	CPU usage when trap is sent.	`set trap-high-cpu-threshold {integer}`
Memory usage threshold	Memory usage when trap is sent.	`set trap-high-mem-threshold {integer}`

User list > New/Edit SNMP User	**SNMP User Configuration.**	`config user`
Name	SNMP user name.	`edit <name>`
Current SNMP user	Enable/Disable SNMP user.	`set status [enable|disable]`
Queries	Enable/disable SNMP queries for this user.	`set queries [enable|disable]`
Traps	Enable/disable traps for this SNMP user.	`set trap-status [enable|disable]`
Authentication	Security level for message authentication and encryption: • *No privacy*: Message with authentication but no privacy (encryption). • *Privacy*: Message with authentication and privacy (encryption).	`set security-level [no-auth-no-priv|auth-no-priv|...]`
Authentication protocol	Select an authentication procol. Shown when *Authentication* is enabled	`set auth-proto [md5|sha]`
Authentication password	Password for authentication protocol. Shown when *Authentication* is enabled	`set auth-pwd {password}`
Privacy	Privacy (encryption) protocol. Shown when *Authentication* is enabled	`set priv-proto [aes|des|...]`
Privacy password	Password for privacy (encryption) protocol. Shown when *Authentication* is enabled	`set priv-pwd {password}`
Notify host IP	Configure SNMP User Notify Hosts.	`set notify-hosts {ipv4-address}`
Community list > New/Edit SNMP Community	**SNMP Community Configuration**	`config community`
ID	Community ID.	`edit <id>`
Name	Community name.	`set name {string}`
Current SNMP community	Enable/disable this SNMP community.	`set status [enable|disable]`
V1 queries	Enable/disable SNMP v1 queries.	`set query-v1-status [enable|disable]`
V2c queries	Enable/disable SNMP v2c queries.	`set query-v2c-status [enable|disable]`
V1 traps	Enable/disable SNMP v1 traps.	`set trap-v1-status [enable|disable]`
V2c traps	Enable/disable SNMP v2c traps.	`set trap-v2c-status [enable|disable]`

Host list > New/Edit Host List	Configure IPv4 SNMP managers (hosts).	`config hosts`
ID	Host entry ID.	`edit <id>`
IP	IPv4 address of the SNMP manager (host).	`set ip {user}`

Configuring UNII-4 5GHz radio bands

FortiAP G-series models operating in Single 5G mode can make use of the UNII-4 frequency band. The 5.85 GHz-5.925 GHz channels of "169", "173", and "177" become available when configuring the 5GHz radio.

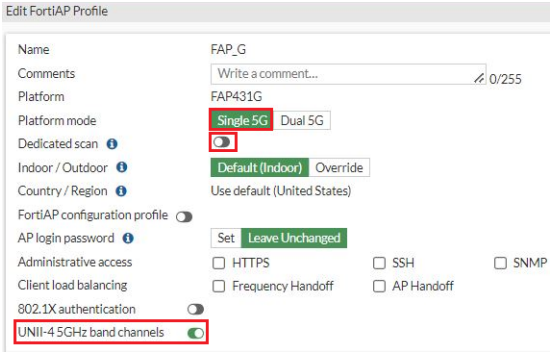
There are a few important points to note about UNII-4 band usage:

1. UNII-4 5GHz channels are not available when operating in Dual 5G platform mode.
2. Not all countries allow UNII-4 band usage.
3. For APs operating in Single 5G platform mode, note the following behavior changes based on Dedicated scan:
   - When Dedicated scan is enabled, UNII-4 5 GHz channels are available by default. Radio 3 does not work in AP mode and Radio 2 can utilize all UNII-4 5GHz channels.
   - When Dedicated scan is disabled, you are given an option to enable or disable UNII-4 5GHz.

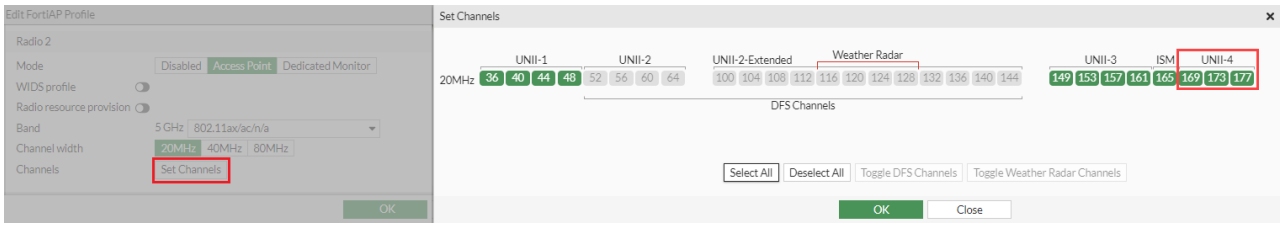
By default, FortiAP G-series models support UNII-4 5GHz channels when operating in Single 5G mode with Dedicated scan enabled; there is no need to configure anything. You can immediately select channels "169", "173", and "177" when configuring the 5GHz radio.

To configure UNII-4 5GHz band channels when the FortiAP is running in Single 5G mode with Dedicated scan disabled - GUI:

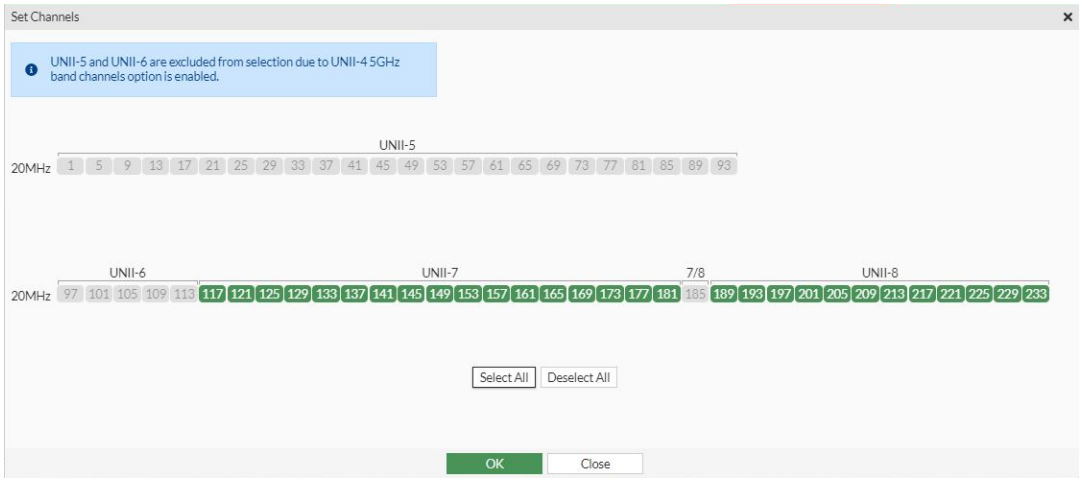
1. From the FortiGate GUI, navigate to *WiFi & Switch Controller* > *FortiAP Profiles*.
2. Select if you want to create a new profile or edit an existing FAP-43xG profile.
3. Set the *Platform mode* to *Single 5G*.
4. Disable *Dedicated scan*.
5. Enable *UNII-4 5GHz band channels*.



6. Go to Radio 2 and click *Set Channels* and select which channels you want to use.
   In the *Set Channels* window, you can see new channels "169", "173", and "177" under the UNII-4 category.



Note: Enabling UNII-4 5GHz band channels will cause the UNII-5 and UNII-6 Channels to be disabled on Radio 3.



To configure UNII-4 5GHz band channels when the FortiAP is running in Single 5G mode with Dedicated scan disabled - CLI:

1. When `DDSCAN` is disabled, you can configure the new `set unii-4-5ghz-band` command in FAP-431G or FAP-433G wtp-profiles.

```
config wireless-controller wtp-profile
  edit FAP_G
    config platform
      set  431G
    end
    set unii-4-5ghz-band ?
      enable     Enable UNII-4 5Ghz band channels.
      disable    Disable UNII-4 5Ghz band channels.
```

2. When you select enable, the following notification shows:

```
set unii-4-5ghz-band enable
  Enabling UNII-4 will reset radio-3 channel lists, UNII-5 and UNII-6 channels will be
unavailable
  Do you want to continue? (y/n)
```

3. Enter `y` to continue. The UNII-4 5Ghz channels become available under `radio-2`.

```
config  radio-2
  set channel
  *wireless_channel    <36,40,44,48,149,153,157,161,165,169,173,177>
```

Note: Enabling UNII-4 5GHz band channels will cause the UNII-5 and UNII-6 Channels to be disabled on radio-3.

Configuring Agile Multiband Operation

The Wi-Fi Alliance Agile Multiband Operation (MBO) feature enables better use of Wi-Fi network resources in roaming decisions and improves overall performance. This allows the FortiGate to push the MBO configuration to managed APs, which adds the MBO information element to the beacon and probe response for 802.11ax.

```
config wireless-controller vap
    edit <name>
        set mbo {enable | disable}
        set gas-comeback-delay <integer>
        set gas-fragmentation-limit <integer>
        set mbo-cell-data-conn-pref {excluded | prefer-not | prefer-use}
    next
end
```

`mbo {enable | disable}`	Enable/disable Multiband Operation (default = disable).
`gas-comeback-delay <integer>`	GAS comeback delay in milliseconds (100 - 10000, default = 500, 0 = special).
`gas-fragmentation-limit <integer>`	GAS fragmentation limit (512 - 4096, default = 1024).
`mbo-cell-data-conn-pref {excluded | prefer-not | prefer-use}`	MBO cell data connection preference: • excluded: Wi-Fi Agile Multiband AP does not want the Wi-Fi Agile Multiband STA to use the cellular data connection. • prefer-not: Wi-Fi Agile Multiband AP prefers that the Wi-Fi Agile Multiband STA should not use cellular data connection. • prefer-use: Wi-Fi Agile Multiband AP prefers that the Wi-Fi Agile Multiband STA should use cellular data connection.

To configure MBO for an 802.11ax FortiAP:

1. Configure MBO on the VAP:

```
config wireless-controller vap
    edit "MBO-Test"
        set max-clients 15
        set ssid "MBO-Test-01"
        set pmf enable
        set pmf-assoc-comeback-timeout 8
        set mbo enable
        set gas-comeback-delay 0
        set gas-fragmentation-limit 2048
        set mbo-cell-data-conn-pref prefer-use
        set passphrase <somepassword>
        set schedule "always"
        set target-wake-time disable
        set igmp-snooping enable
        unset broadcast-suppression
        set mu-mimo disable
        set quarantine disable
        set dhcp-option82-insertion enable
        set qos-profile "test"
```

```
    next
end
```

2. Enable the VAP on a WTP profile:

```
config wireless-controller wtp-profile
    edit "FAP234F-default"
        set ble-profile "new"
        set wan-port-mode wan-lan
        config lan
            set port-mode bridge-to-ssid
            set port-ssid "16sep"
        end
        set handoff-sta-thresh 55
        set ip-fragment-preventing tcp-mss-adjust icmp-unreachable
        set allowaccess https ssh snmp
        set poe-mode high
        set frequency-handoff enable
        set ap-handoff enable
        config radio-1
            set band 802.11ax
            set short-guard-interval enable
            set auto-power-level enable
            set auto-power-high 21
            set auto-power-low 1
            set darrp enable
            set vap-all manual
            set vaps "MBO-Test"
            set channel "1" "6" "11"
        end
        config radio-2
            set band 802.11ax-5G
            set short-guard-interval enable
            set auto-power-level enable
            set auto-power-low 1
            set darrp enable
            set vap-all manual
            set vaps "MBO-Test"
            set channel "36" "40" "44" "48" "149" "153" "157" "161" "165"
        end
        config radio-3
            set mode monitor
            set wids-profile "default"
        end
        config lbs
            set station-locate enable
        end
    next
end
```

3. Verify the MBO settings are pushed to the FortiAP:

```
# diagnose debug application wpad 255
21176.239 Received data - hexdump(len=153):
    13 02 00 00 00 00 00 00 00 00 00 B0 01 A5 C0   ................
    7E 14 01 00 04 D5 90 E9 F4 E0 46 50 34 33 31 46   ~.........FP431F
    54 46 32 30 30 30 30 30 31 35 00 00 00 00 00 00   TF20000015......
```

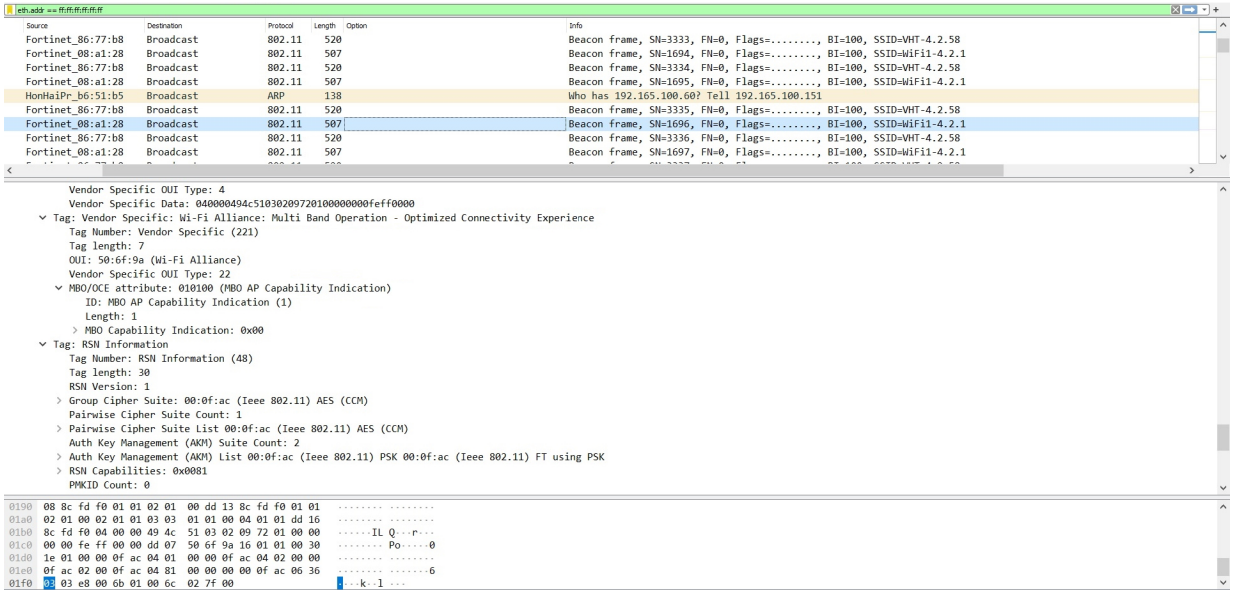
```
    80 18 39 91 FF 7F 00 00 00 E2 C2 90 07 E0 32 AC   ..9...........2.
    FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00   ................
    00 00 00 00 00 00 00 00 78 BF E1 15 00 00 00 00   ........x.......
    00 00 01 00 31 00 00 00 D0 00 3C 00 04 D5 90 E9   ....1.....<.....
    F4 E0 A0 51 0B 4A 84 F4 FF FF FF FF FF FF A0 03   ...Q.J..........
    04 0A 00 6C 02 00 00 10 00 00 01 02 00 10 01 DD   ...l............
    DD 06 00 50 6F 9A 12 01 02                        ...Po....
21176.239 HOSTAPD: <0>192.165.1.176:5246<1-0>  entering state RUN
mgmt::action
: GAS: GAS Initial Request from a0:51:0b:4a:84:f4 (dialog token 0)
ANQP: 1 Info IDs requested in Query list
ANQP: Unsupported WFA vendor type 18
ANQP: Locally generated ANQP responses - hexdump(len=0):
ANQP: Initial response (no comeback)
21176.239 Sending data - hexdump(len=141):
    0C 03 00 00 00 00 00 00 00 00 00 B0 01 A5 C0   ................
    7E 14 01 00 04 D5 90 E9 F4 D0 00 00 00 00 00 00   ~...............
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

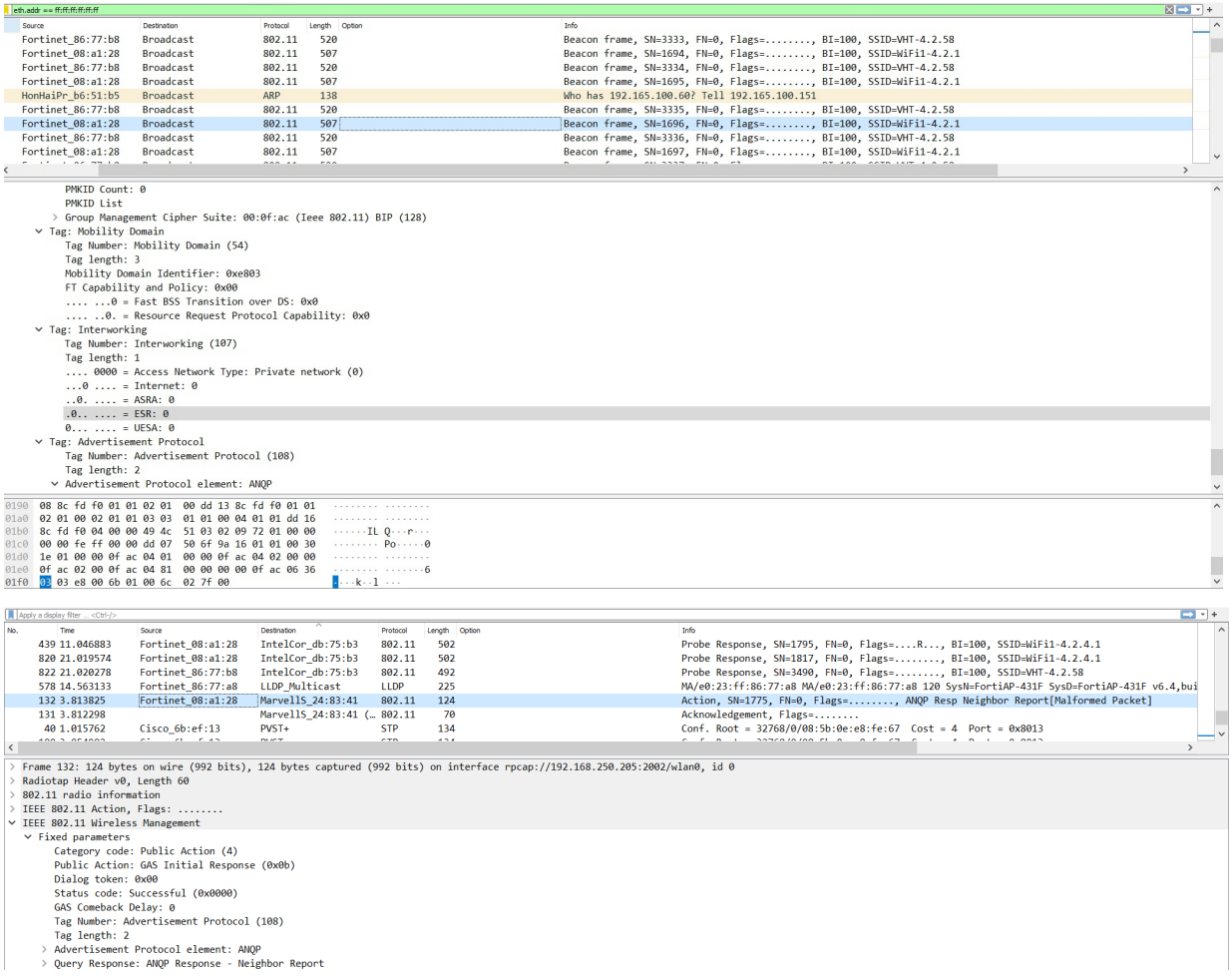
4. On the FortiAP, verify the MBO settings are pushed from the FortiGate:

```
# vcfg
-------------------------------VAP Configuration    1-----------------------------
Radio Id  0 WLAN Id  0 MBO-Test-01 ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown
(-1)
           vlanid=0, intf=wlan00, vap=0x12b8018, bssid=e0:23:ff:b2:18:70
           11ax high-efficiency=enabled target-wake-time=disabled bss-color=0
partial=enabled
           mesh backhaul=disabled
           local_auth=disabled standalone=disabled nat_mode=disabled
           local_bridging=disabled split_tunnel=disabled
           intra_ssid_priv=disabled
           mcast_enhance=disabled igmp_snooping=enabled
           mac_auth=disabled fail_through_mode=disabled sta_info=0/0
           mac=local, tunnel=8023, cap=8ce0, qos=disabled
           prob_resp_suppress=disabled
           rx sop=disabled
           sticky client remove=disabled
           mu mimo=disabled           ldpc_config=rxtx
           dhcp_option43_insertion=enabled           dhcp_option82_insertion=enabled,
dhcp_option82_circuit_id=disable, dhcp_option82_remote_id=disable
           access_control_list=disabled
           bc_suppression=
           auth=WPA2, PSK, AES WPA keyIdx=4, keyLen=16, keyStatus=1, gTsc=000000000000
           key=dee8be7d 3675eda2 7123f695 1d740319
           pmf=required
           okc=disabled, dynamic_vlan=disabled, extern_roaming=disabled
           voice_ent(802.11kv)=disabled, fast_bss_trans(802.11r)=disabled mbo=enabled
           airfairness weight: 20%
           schedules=SMTWTFS 00:00->00:00,
           ratelimit(Kbps): ul=100 dl=0 ul_user=0 dl_user=0 burst=disabled

-------------------------------VAP Configuration    2-----------------------------
Radio Id  1 WLAN Id  0 MBO-Test-01 ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown
(-1)
```

```
            vlanid=0, intf=wlan10, vap=0x12b8860, bssid=e0:23:ff:b2:18:78
            11ax high-efficiency=enabled target-wake-time=disabled bss-color=0
partial=enabled
            mesh backhaul=disabled
            local_auth=disabled standalone=disabled nat_mode=disabled
            local_bridging=disabled split_tunnel=disabled
            intra_ssid_priv=disabled
            mcast_enhance=disabled igmp_snooping=enabled
            mac_auth=disabled fail_through_mode=disabled sta_info=0/0
            mac=local, tunnel=8023, cap=8ce0, qos=disabled
            prob_resp_suppress=disabled
            rx sop=disabled
            sticky client remove=disabled
            mu mimo=disabled           ldpc_config=rxtx
            dhcp_option43_insertion=enabled           dhcp_option82_insertion=enabled,
dhcp_option82_circuit_id=disable, dhcp_option82_remote_id=disable
            access_control_list=disabled
            bc_suppression=
            auth=WPA2, PSK, AES WPA keyIdx=4, keyLen=16, keyStatus=1, gTsc=000000000000
            key=6042ccb8 66c18743 18cdb5d0 12f9c0fc
            pmf=required
            okc=disabled, dynamic_vlan=disabled, extern_roaming=disabled
            voice_ent(802.11kv)=disabled, fast_bss_trans(802.11r)=disabled mbo=enabled
            airfairness weight: 20%
            schedules=SMTWTFS 00:00->00:00,
            ratelimit(Kbps): ul=100 dl=0 ul_user=0 dl_user=0 burst=disabled

--------------------------------Total    2 VAP Configurations-----------------------------
```

5. Verify the beacon frames in the packet captures:




eth.addr == ff:ff:ff:ff:ff:ff
Source Destination Protocol Length Option Info
Fortinet_86:77:b8 Broadcast 802.11 520 Beacon frame, SN=3333, FN=0, Flags=........, BI=100, SSID=VHT-4.2.58
Fortinet_08:a1:28 Broadcast 802.11 507 Beacon frame, SN=1694, FN=0, Flags=........, BI=100, SSID=WiFi1-4.2.1
Fortinet_86:77:b8 Broadcast 802.11 520 Beacon frame, SN=3334, FN=0, Flags=........, BI=100, SSID=VHT-4.2.58
Fortinet_08:a1:28 Broadcast 802.11 507 Beacon frame, SN=1695, FN=0, Flags=........, BI=100, SSID=WiFi1-4.2.1
HonHaiPr_b6:51:b5 Broadcast ARP 138 Who has 192.165.100.60? Tell 192.165.100.151
Fortinet_86:77:b8 Broadcast 802.11 520 Beacon frame, SN=3335, FN=0, Flags=........, BI=100, SSID=VHT-4.2.58
Fortinet_08:a1:28 Broadcast 802.11 507 Beacon frame, SN=1696, FN=0, Flags=........, BI=100, SSID=WiFi1-4.2.1
Fortinet_86:77:b8 Broadcast 802.11 520 Beacon frame, SN=3336, FN=0, Flags=........, BI=100, SSID=VHT-4.2.58
Fortinet_08:a1:28 Broadcast 802.11 507 Beacon frame, SN=1697, FN=0, Flags=........, BI=100, SSID=WiFi1-4.2.1
PMKID Count: 0
PMKID List
Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
Tag: Mobility Domain
Tag Number: Mobility Domain (54)
Tag length: 3
Mobility Domain Identifier: 0xe803
FT Capability and Policy: 0x00
....0 = Fast BSS Transition over DS: 0x0
.... ..0. = Resource Request Protocol Capability: 0x0
Tag: Interworking
Tag Number: Interworking (107)
Tag length: 1
.... 0000 = Access Network Type: Private network (0)
...0 .... = Internet: 0
..0. .... = ASRA: 0
.0.. .... = ESR: 0
0... .... = UESA: 0
Tag: Advertisement Protocol
Tag Number: Advertisement Protocol (108)
Tag length: 2
Advertisement Protocol element: ANQP
0190 08 8c fd f0 01 01 02 01 00 dd 13 8c fd f0 01 01
01a0 02 01 00 02 01 01 03 03 01 01 00 04 01 01 dd 16
01b0 8c fd f0 04 00 00 49 4c 51 03 02 09 72 01 00 00
01c0 00 00 fe ff 00 00 dd 07 50 6f 9a 16 01 01 00 30
01d0 1e 01 00 00 0f ac 04 01 00 00 0f ac 04 02 00 00
01e0 0f ac 02 00 0f ac 04 81 00 00 00 00 0f ac 06 36
01f0 03 e8 00 6b 01 00 6c 02 7f 00

Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Option Info
439 11.046883 Fortinet_08:a1:28 IntelCor_db:75:b3 802.11 502 Probe Response, SN=1795, FN=0, Flags=....R..., BI=100, SSID=WiFi1-4.2.4.1
820 21.019574 Fortinet_08:a1:28 IntelCor_db:75:b3 802.11 502 Probe Response, SN=1817, FN=0, Flags=........, BI=100, SSID=WiFi1-4.2.4.1
822 21.020278 Fortinet_86:77:b8 IntelCor_db:75:b3 802.11 492 Probe Response, SN=3490, FN=0, Flags=........, BI=100, SSID=VHT-4.2.58
578 14.563133 Fortinet_86:77:a8 LLDP_Multicast LLDP 225 MA/e0:23:ff:86:77:a8 MA/e0:23:ff:86:77:a8 120 SysN=FortiAP-431F SysD=FortiAP-431F v6.4,bui
132 3.813825 Fortinet_08:a1:28 Marvell$_24:83:41 802.11 124 Action, SN=1775, FN=0, Flags=........, ANQP Resp Neighbor Report[Malformed Packet]
131 3.812298 Marvell$_24:83:41 (… 802.11 70 Acknowledgement, Flags=........
40 1.015762 Cisco_6b:ef:13 PVST+ STP 134 Conf. Root = 32768/0/08:5b:0e:e8:fe:67 Cost = 4 Port = 0x8013
Frame 132: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface rpcap://192.168.250.205:2002/wlan0, id 0
Radiotap Header v0, Length 60
802.11 radio information
IEEE 802.11 Action, Flags: ....
IEEE 802.11 Wireless Management
Fixed parameters
Category code: Public Action (4)
Public Action: GAS Initial Response (0x0b)
Dialog token: 0x00
Status code: Successful (0x0000)
GAS Comeback Delay: 0
Tag Number: Advertisement Protocol (108)
Tag length: 2
Advertisement Protocol element: ANQP
Query Response: ANQP Response - Neighbor Report

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 193 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 195.

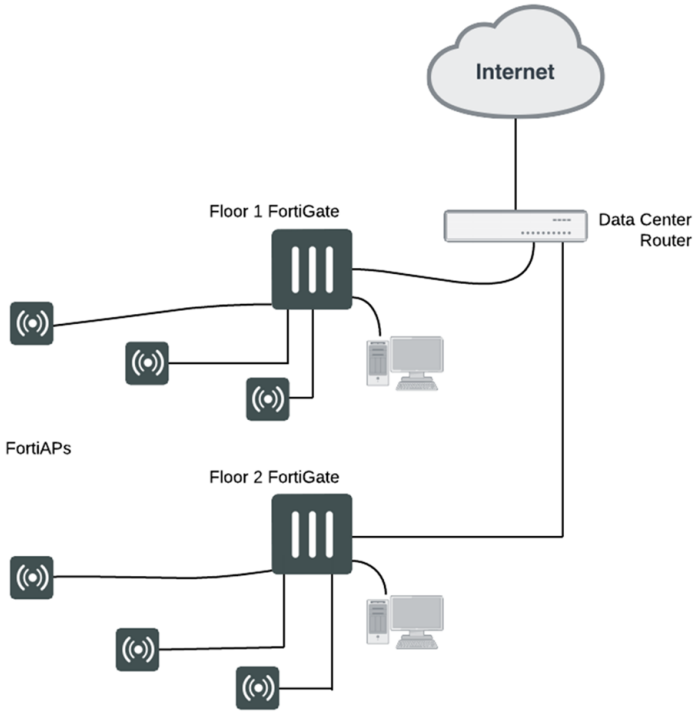
If your FortiAP units are unable to find the WiFi controller, refer to Advanced WiFi controller discovery on page 212 for detailed information about the FortiAP unit controller discovery methods and how you can configure them.

Network topology of managed APs

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

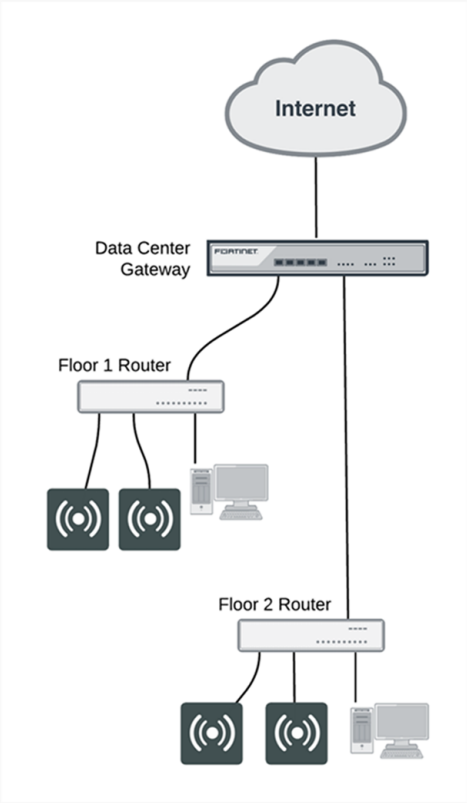
- **Direct connection**: The FortiAP unit is directly connected to the FortiGate unit with no switches between them. This configuration is common for locations where the number of FortiAPs matches the number of internal ports available on the FortiGate. In this configuration, the FortiAP unit requests 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



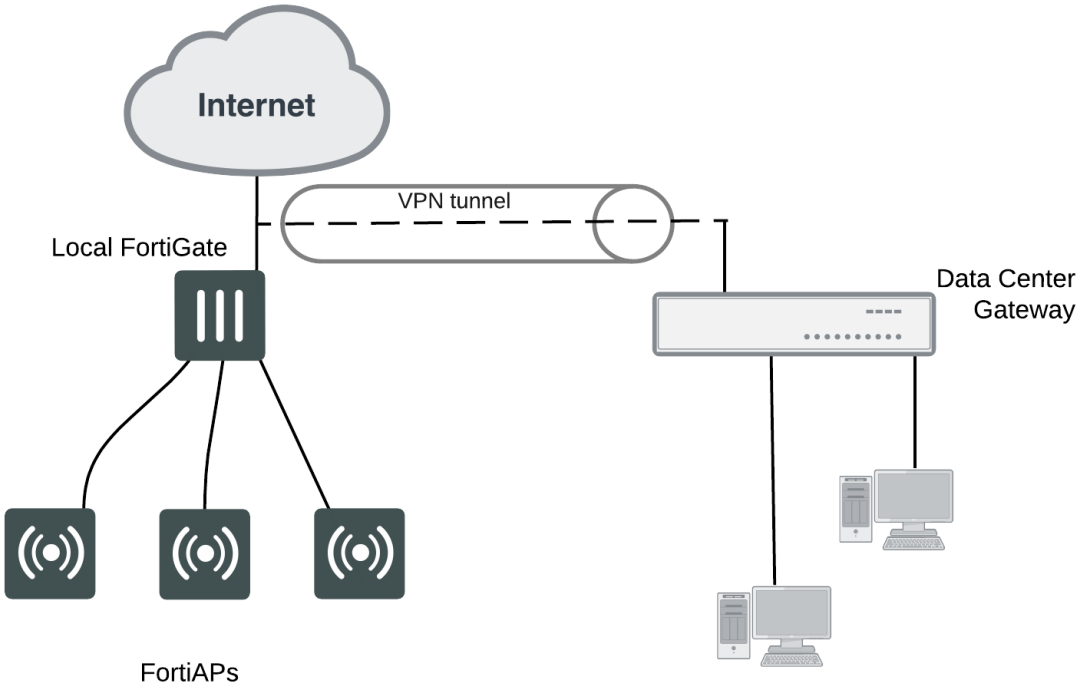
- **Switched connection**: The FortiAP unit is connected to the FortiGate WiFi controller by an Ethernet switch operating in L2 switching mode or L3 routing mode. There must be a routable path between the FortiAP unit and the FortiGate unit and ports 5246 and 5247 must be open. This configuration is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

- Pre-authorizing a FortiAP unit on page 195
- Enabling and configuring a discovered AP on page 198
- Disabling the automatic discovery of unknown FortiAPs on page 199
- Enabling the automatic authorization of extension devices on page 199
- Assigning the same FortiAP profile to multiple FortiAP units on page 199
- Overriding the FortiAP profile on page 200

Pre-authorizing a FortiAP unit

There are two ways of pre-authorizing a FortiAP unit:

- Enter an individual FortiAP unit information in advance; the unit is authorized and begins to function when it is connected.
- Specify a Wildcard Serial Number to represent the model of the FortiAPs you want to authorize; the pre-configured SN is replaced by the actual SN of the FortiAP, and the FortiAP is authorized when it is connected.

Pre-authorizing an individual FortiAP unit

To pre-authorize an individual FortiAP unit:

1. Go to *WiFi and 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*.

Pre-authorizing a FortiAP by specifying a Wildcard Serial Number

You can pre-configure and pre-authorize a template FortiAP SN to represent the SN of specific FortiAP models. When a physical FortiAP connects, the pre-configured SN is replaced by the actual SN of the FortiAP, and the FortiAP can be automatically authorized.

For example, a Wildcard Serial Number of FP231F****000001 will allow the first FortiAP-231F to register to the Wireless Controller to be authorized automatically and adopt profile configurations.

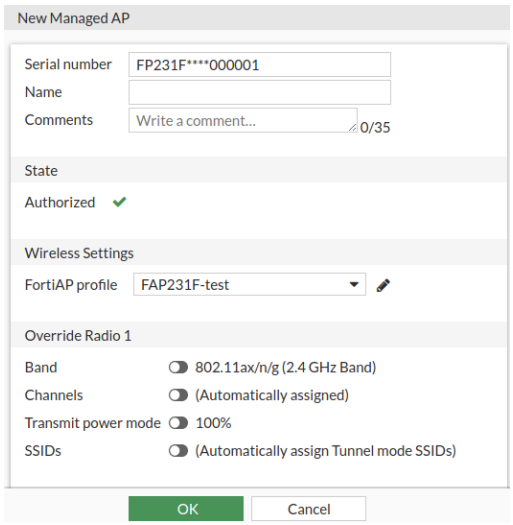
A Wildcard Serial Number consists of three parts:

- A six digit valid prefix for a FortiAP model, like "FP231F".
- Four "*" (asterisks) to indicate that the Serial Number is a Wildcard Serial Number.
- Six digits containing any valid characters. The characters do not need the match the actual Serial Number of the FortiAP you are registering.

  The last six digits enable you to create multiple profiles where each new FortiAP that registers adopt one of the wildcard SN profiles in order.

To pre-authorize a FortiAP by specifying a Wildcard Serial Number - GUI:

1. Go to *WiFI & Switch Controller* > *Managed FortiAPs* and click *Create New* > *Managed AP*.
2. In *Serial number*, enter a Wildcard Serial Number (example "FP231F****000001").
3. Select a *FortiAP profile* you want to apply to the FortiAP.



4. Click *OK* to save.
5. Connect the FortiAP unit to your topology.

   Once the FortiAP is discovered by FortiGate, FortiGate will try to find a matching Wildcard SN. When FortiGate finds a matching Wildcard SN, the template Serial Number is renamed to match the newly discovered physical FortiAP SN.

To configure a Wildcard Serial Number and pre-authorize a FortiAP- CLI:

1. Pre-configure a Wildcard FortiAP SN (example "FP231F****000001").

```
config wireless-controller wtp
 edit "FP231F****000001"
   set uuid 47ab50f8-5f7c-51ec-0a60-4ff00a3eba2e
   set admin enable
   set wtp-profile "FAP231F-test"
   config radio-1
   end
   config radio-2
   end
 next
end
```

2. Connect the FortiAP unit to your topology.

   Once the FortiAP is discovered by FortiGate, FortiGate will try to find a matching Wildcard SN. When FortiGate finds a matching Wildcard SN, the template Serial Number is renamed to match the newly discovered physical FortiAP SN.

```
FortiGate-80E-POE # diag debug enable
FortiGate-80E-POE # diag debug cli 7
Debug messages will be on for unlimited time.
FortiGate-80E-POE # 0: config wireless-controller wtp
0: rename "FP231F****000001" to "FP231FTF20026472"
0: end
```

   The pre-configured template FortiAP SN is successfully renamed to match the FortiAP SN "FP231FTF20026472".
3. The new FortiAP is now pre-authorized and can be managed from the FortiGate without manual authorization. Note that the UUID does not change.

```
config wireless-controller wtp
 edit "FP231FTF20026472"
   set uuid 47ab50f8-5f7c-51ec-0a60-4ff00a3eba2e
   set admin enable
   set wtp-profile "FAP231F-test"
   config radio-1
   end
   config radio-2
   end
  next
end
```

Enabling and configuring a discovered AP

1. Connect the FortiAP unit to the FortiGate unit. Within two minutes, the *WiFi 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 a FortiAP unit, it is configured by default to use the default FortiAP profile (determined by model). The FortiAP profile defines the entire configuration for the AP (see Creating a FortiAP profile on page 38). You can assign a different profile, if needed, by right-clicking the authorized FortiAP and selecting *Assign Profile*.

To add and configure the discovered AP unit - GUI:

1. Go to *WiFi and 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 and 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 and 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 *Channels*. Make appropriate settings in *Channels*.
Channels	Choose channels. The available channels depend on the Band.
Transmit power mode	Select how you want to determine transmit power. The 100% setting is the maximum power permitted in your region. See Setting your geographic location on page 35.
SSIDs	Select a traffic mode for SSIDs. • *Tunnel* – available tunnel-mode SSIDs are automatically assigned to this radio. • *Bridge* – available bridge-mode SSIDs are automatically assigned to this radio. • *Manual* – manually select which available SSIDs and SSID groups to assign to this radio.

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
```

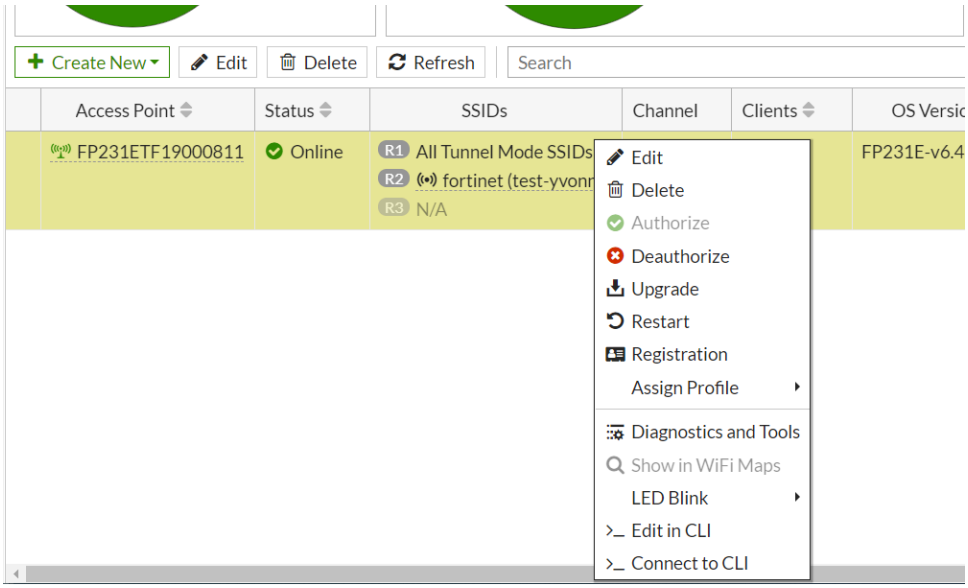
You can override settings for band, channel, vaps (SSIDs), and Transmit power mode.

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.

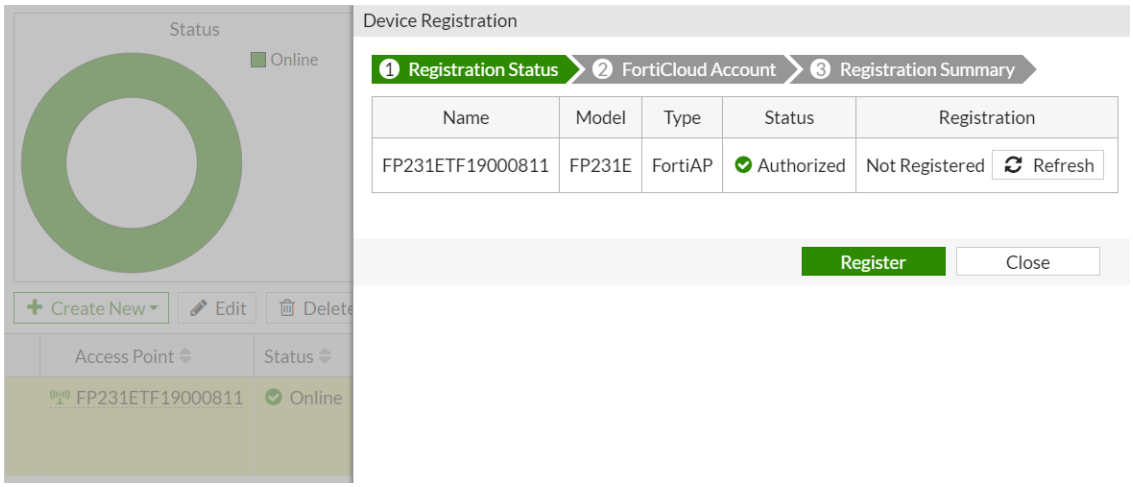
Register a FortiAP to FortiCloud

After authorizing a FortiAP, you can resister that FortiAP to FortiCloud directly from the FortiGate GUI.

1. Go to *WiFi and Switch Controller* > *Managed FortiAPs*.
2. Select the FortiAP unit you want to register.
3. Right-click and select *Registration*.



The Device Registration window opens.



4. Click *Register* to proceed to the next step.
5. Enter your FortiCloud account information and click *Submit*.
   It can take up to 30 minutes to register the device.
6. Once the device is registered, you can view the registration status from the FortiAP Diagnostic and Tools page.

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 and 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

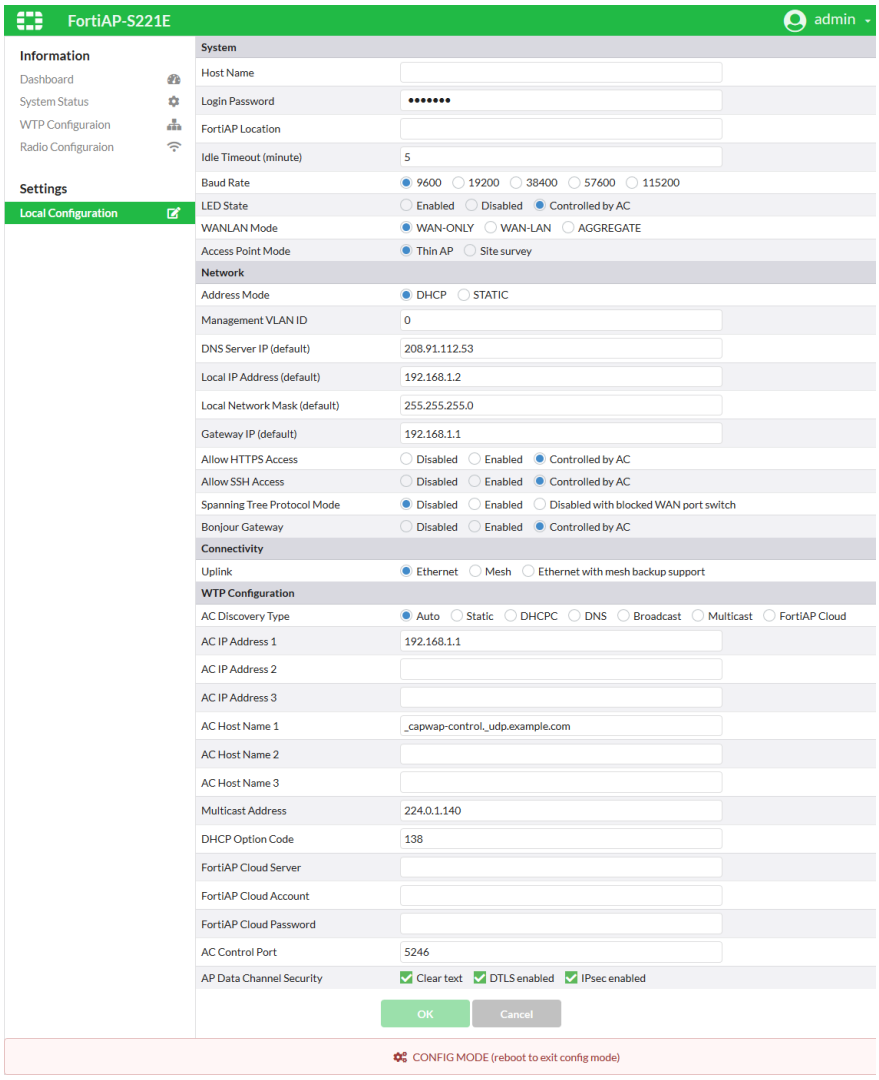
1. Make sure FortiAP is booted up.
2. Use a pin to push and hold the reset button for 5 to 10 seconds.
   FortiAP reboots and then enters the Configuration mode.
   FortiAP starts to broadcast an open security SSID `FAP-config-<serial-number>`, for example `FAP-config-FP421E3X16000715`.
3. You can now 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 203
   - or Accessing the CLI of the FortiAP Configuration mode on page 205

Accessing the GUI of the FortiAP Configuration mode

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*.

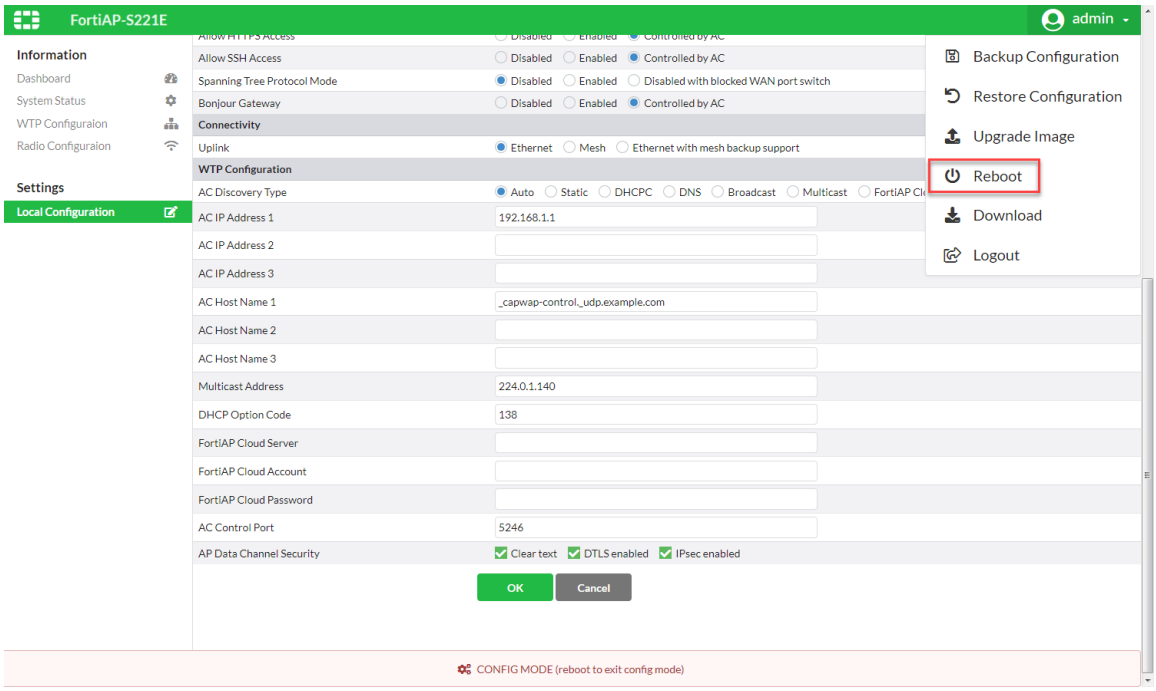
FortiAP Config Mode - Local Configuration



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 439.
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

There are multiple ways you can upgrade the FortiAP unit firmware:

- You can enable newly discovered FortiAPs to be automatically upgraded to the latest compatible firmware. This happens once after the FortiAP is authorized by the WiFi controller.
- You can enable automatic firmware updates on your FortiGate which checks for patch upgrades for your FortiGates, FortiSwitches, and FortiAPs. If a compatible upgrade is available, FortiGate automatically downloads and installs them at a scheduled time.
- You can manually view and upgrade the FortiAP firmware from the FortiGate unit.

When upgrading multiple APs, you can enable Hitless Rolling upgrade where FortiAPs are upgraded in a staggered process so that they can continue to provide Wi-Fi service.

Checking the FortiAP unit firmware version

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

Enabling automatic FortiAP upgrade after authorization

You can enable the automatic federated upgrade of a FortiAP unit upon discovery and authorization by the WiFi controller. When you enable this feature, newly discovered FortiAPs are automatically upgraded to the latest compatible firmware from FortiGuard Distribution Service (FDS).

To enable automatic FortiAP upgrade - GUI:

1. Go to *WiFI & Switch Controller* > *WiFi Settings* and enable *FortiAP auto firmware provisioning*.
2. Click *Apply*.
3. Connect and authorize a FortiAP.

   The FortiAP will be upgraded to the latest compatible firmware from FDS.

To enable automatic FortiAP upgrade - CLI:

1. Enable `firmware-provision-on-authorization` via the CLI:

```
config wireless-controller setting
  set firmware-provision-on-authorization enable
  set darrp-optimize-schedules "default-darrp-optimize"
end
```

2. Connect and authorize a FortiAP.

   The FortiAP will be upgraded to the latest compatible firmware from FDS.

When `firmware-provision-on-authorization` is enabled, any new FortiAPs that are authorized will automatically have `firmware-provision-latest` set to `once`.

Enabling automatic firmware updates

Automatic firmware updates will upgrade your FortiGates, FortiSwitches, and FortiAPs at a scheduled time.

When you enable automatic firmware updates, it upgrades the FortiAP directly to the target version and does not follow an upgrade path. Refer to the Supported Upgrade Path documentation to ensure you follow the proper upgrade path.

To enable automatic firmware updates - GUI:

1. Go to *System* > *Firmware & Registration* and click *Automatic patch upgrades disabled*.
2. Select *Enable automatic patch upgrades for vX.X*.
3. Select a date and time for when you want to schedule your upgrade.
4. Click OK.

To enable automatic firmware updates - CLI:

Enable automatic firmware upgrade and schedule a day and time to upgrade.

```
config system fortiguard
  set auto-firmware-upgrade enable
  set auto-firmware-upgrade-day sunday monday tuesday wednesday thursday friday saturday
  set auto-firmware-upgrade-delay 0
  set auto-firmware-upgrade-start-hour 17
  set auto-firmware-upgrade-end-hour 19
end
```

The auto-upgrade time is scheduled daily, between 5:00 p.m. and 7:00 p.m.

Upgrading FortiAP firmware from the FortiGate unit

You can manually 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 and 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. You can 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
   ```

Enabling Hitless Rolling AP upgrade

When upgrading FortiAPs using the Hitless Rolling upgrade method, an algorithm considers the reach of neighboring APs and their locations. The APs are then upgraded in staggered process with some APs being immediately upgraded while others continue to provide Wi-Fi service to clients and are placed in a standby queue. Once the SSIDs on the initial upgraded APs are able to serve clients, the APs in the standby queue begin upgrading.

The following CLI commands for configuring Hitless Rolling AP upgrades are available at both global settings and per-VDOM settings:

Enabling Hitless Rolling Upgrade at the global level

```
config wireless-controller global
  set rolling-wtp-upgrade {Enable | disable}
  set rolling-wtp-upgrade-threshold <integer>
end
```

`rolling-wtp-upgrade`	Enable/disable rolling WTP upgrade (default = disable). **Note:** Enabling this at the global-level will enforce all managed FortiAPs in all VDOMs to implement the rolling upgrade, regardless of the VDOM-level settings.

`rolling-wtp-upgrade-threshold`	Minimum signal level/threshold in dBm required for the managed WTP to be included in rolling WTP upgrade (-95 to -20, default = -80).

Enabling Hitless Rolling Upgrade at the per-VDOM level

```
config wireless-controller setting
  set rolling-wtp-upgrade {Enable | disable}
end
```

`rolling-wtp-upgrade`	Enable/disable rolling WTP upgrade (default = disable). **Note:** Enabling this at the VDOM-level will let managed FortiAPs in the current VDOM to implement the rolling upgrade, regardless of the global-level setting.

Executing Hitless Rolling Upgrade

```
exec wireless-controller rolling-wtp-upgrade <all>|<SN>|<wtp-group>
```

`rolling-wtp-upgrade`	Select which APs you want to upgrade with the Hitless Rolling upgrade. You can select all APs, by their WTP serial number, or WTP group.

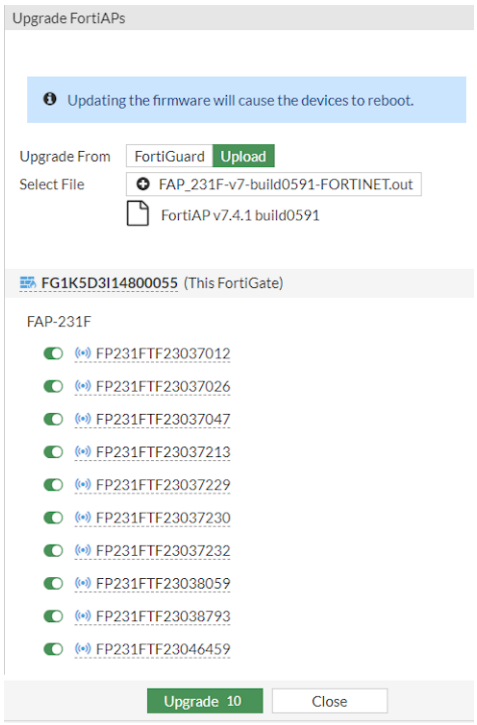
To configure Hitless Rolling AP upgrade - GUI

1. Before you can run Hitless Rolling AP upgrade from the GUI, you must first enable `rolling-wtp-upgrade` and configure the `rolling-wtp-upgrade-threshold` level in the CLI.

   ```
   config wireless-controller global
     set rolling-wtp-upgrade enable
     set rolling-wtp-upgrade-threshold -70
   end
   ```

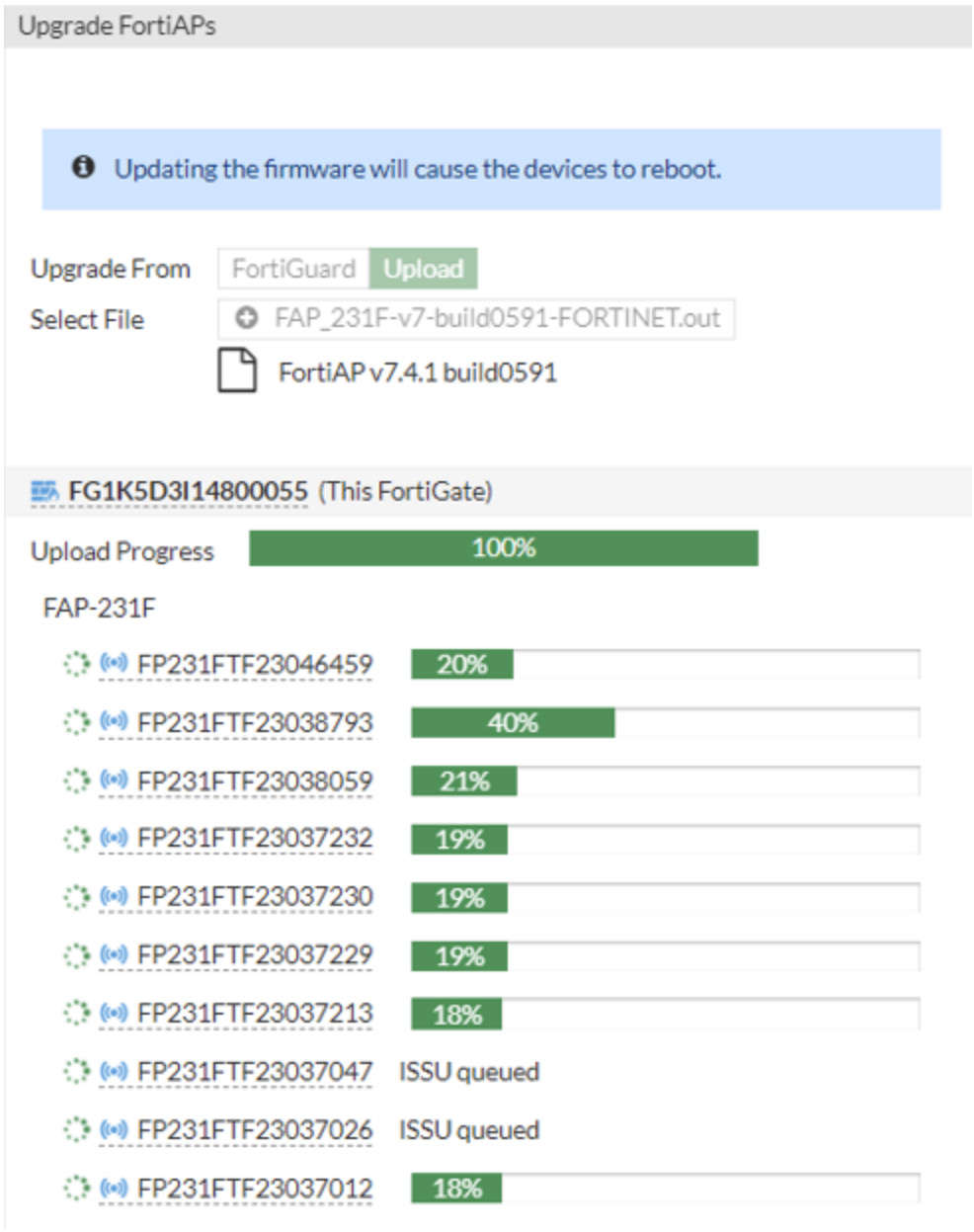
   ```
   config wireless-controller setting
     set rolling-wtp-upgrade enable
   end
   ```

2. From the FortiGate GUI, go to *WiFi & Switch Controller > Managed FortiAPs*.
3. Select multiple FortiAPs of the same model, and then right-click and select *Upgrade*.
   The *Upgrade FortiAPs* window loads.
4. Upload the FortiAP image file and click *Upgrade*.



The FortiAPs are automatically upgraded using the Hitless Rolling upgrade method.

5. Some FortiAPs immediately begin upgrading while others are marked with "ISSU queued". In-Service Software Upgrade (ISSU) indicates that these are the standby APs that continue to provide Wi-Fi service to clients and are queued to be upgraded later.



6. Once the first batch of FortiAPs are upgraded and can provide service, the ISSU queued FortiAPs will begin upgrading.

To configure Hitless Rolling AP upgrade - CLI

1. Enable `rolling-wtp-upgrade` at either the global or VDOM level and configure the `rolling-wtp-upgrade-threshold` level.

```
config wireless-controller global
  set rolling-wtp-upgrade enable
  set rolling-wtp-upgrade-threshold -70
end
```

```
config wireless-controller setting
  set rolling-wtp-upgrade enable
end
```

2. Upload FortiAP images to FortiGate and check the image list. In this example, FAP231F is uploaded:

```
execute wireless-controller upload-wtp-image tftp /FortiAP/v7.00/images/build0626/FAP_
231F-v7-build0626-FORTINET.out 172.18.52.254
```

3. Verify the uploaded FortiAP images:

```
execute wireless-controller list-wtp-image
WTP Images on AC:
ImageName                              ImageSize(B)    ImageInfo              ImageMTime
…
FP231F-v7.4.2-build0626-IMG.wtp        37605058        FP231F-v7.4-build0626  Mon Nov 27
10:39:53 2023
```

4. Run the Rolling WTP Upgrade and prepare to check the FortiAP upgrade status.

```
exec wireless-controller rolling-wtp-upgrade all
```

5. The FortiAPs begin upgrading on a rolling basis. You can use `diagnose wireless-controller wlac -c ap-upd` to check the upgrade process.

```
diagnose wireless-controller wlac -c ap-upd

1,50,66 0-FP231FTF23037012 FP231F-v7.4-build0591 ==> FP231F-v7.4-build0626 ws (0-
10.233.10.7:5246) upd-download,3 5%           <- The image download has started (may
still be blocked by concurrent AP image downloading limit)
2,50,66 0-FP231FTF23037026 FP231F-v7.4-build0591 ==> FP231F-v7.4-build0626 ws (0-
10.233.10.3:5246) upd-download,3 6%
3,50,66 0-FP231FTF23037047 FP231F-v7.4-build0591 ==> FP231F-v7.4-build0626 ws (0-
10.233.10.24:5246) upd-download,3 6%
…
15,50,66 0-FP431FTF23000559 FP431F-v7.4-build0591 ==> FP431F-v7.4-build0626 ws (0-
10.233.30.40:5246) upd-enqueue-issu,4 0%      <- In queue for rolling AP upgrade to
avoid Wi-Fi service drop
16,50,66 0-FP431FTF23021146 FP431F-v7.4-build0591 ==> FP431F-v7.4-build0626 ws (0-
10.233.30.42:5246) upd-enqueue-issu,4 0%
…
19,50,66 0-FP433FTF21001215 FP433F-v7.4-build0591 ==> FP433F-v7.4-build0626 ws (0-
10.233.30.41:5246) upd-enqueue-issu,4 0%
…
```

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 and 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. When the FortiAP discovery type is set to auto, the AP Controller (AC) uses the following discovery methods in sequence:

1(static) → 2(dhcp) → 3(dns) → 7(fortiedgecloud) → 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.

If FortiAP gets stuck in a discovery loop due to changes in the network, you might need to reboot the AP to detect the new changes. You can set up automatic AP reboot to reduce the need for manual intervention (see Configure automatic AP reboot on page 215).

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 201.

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 201.

DNS

FortiAP can discover controllers through your domain name server (DNS) from DHCP option 15 (e.g. "example.com"), which can be configured on a 3rd-party DHCP server.

By default, FortiAP has the default AC hostname of "`fortinet-capwap-controller`" and combines it with the AC domain suffix to form one FQDN (e.g. "`fortinet-capwap-controller.example.com`").

If necessary, you can customize the default AC hostname without the "`.`" character on FortiAP.

To customize the default AC hostname:

1. From the FortiAP CLI, enter the following commands to customize the `AC_HOSTNAME_1/2/3`:

```
cfg -a AC_HOSTNAME_1=<yourcompany>
cfg -a AC_HOSTNAME_2=<yourcompany2>
cfg -a AC_HOSTNAME_3=<yourcompany3>
cfg -c
```

The new example DNS hostname would become "`yourcompany.example.com`".

FortiEdge Cloud

FortiAP can discover FortiEdge Cloud by doing a DNS lookup of the hardcoded FortEdge Cloud AP controller hostname "apctrl1.forticloud.com". The FortiAP discovers the FortiEdge Cloud AP controller via HTTPS to get the AC address.

FortiEdge Cloud - APController: `apctrl1.forticloud.com`

Broadcast request

The FortiAP 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 FortiAP 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 201.

Configure automatic AP reboot

You can configure FortiAPs to automatically reboot when they are stuck in an AP Controller (AC) discovery dead loop, eliminating the need to manually reboot or power cycle those FortiAP units to recover. FortiAPs have a configurable timeout period during AC discovery and can automatically reboot if they do not detect an active AC within the set time interval. Once the FortiAPs reboot, they can detect any changes made to the LAN/WAN and discover the AC.

The following CLI commands have been added to configure automatic AP reboot:

```
config wireless-controller timers
  set ap-reboot-wait-interval < integer >
  set ap-reboot-wait-time < hh:mm >
  set ap-reboot-wait-interval2  < integer >
end
```

`ap-reboot-wait-interval1`	Time in minutes to wait before the AP reboots when there is no controller detected (5 - 65535, default = 0, 0 for no reboot). Applies only to FortiAP units that have no local-standalone SSID assigned.
`ap-reboot-wait-time`	Time to reboot the AP when there is no controller detected and standalone SSIDs are pushed to the AP in the previous session, format hh:mm.

	This command apples to FortiAPs with at least one local-standalone SSID and ones with no local-standalone SSIDs. If both "`ap-reboot-wait-interval1`" and "`ap-reboot-wait-time`" are set, FortiAPs *with* standalone SSIDs will reboot at the configured "`ap-reboot-wait-time`" every day. However, FortiAPs *without* standalone SSIDs will reboot after waiting for "`ap-reboot-wait-interval1`" or "`ap-reboot-wait-time`", whichever come first.
`ap-reboot-wait-interval2`	Time in minutes to wait before the AP reboots when there is no controller detected and standalone SSIDs are pushed to the AP in the previous session (5 - 65535, default = 0, 0 for no reboot). Applies only to FortiAP units that have at least one local-standalone SSID assigned.

For automatic reboot to be enabled, the FortiAPs need to be managed by a FortiGate once and have an interval and wait-time set from the FortiGate side. Only then will the APs auto-reboot if they cannot detect an active AC.

To configure FortiAP automatic reboot intervals - CLI:

1. Configure the FortiAP reboot interval:

```
config wireless-controller timers
  set ap-reboot-wait-interval1 5
  set ap-reboot-wait-interval2 10
end
```

2. Assign a non-standalone SSID to FAP1:

```
config wireless-controller vap
  edit "test_bridge"
    set ssid "test_bridge"
    set passphrase ENC
    set local-bridging enable
    set schedule "always"
  next
end
```

3. Assign a standalone SSID to FAP2:

```
config wireless-controller vap
  edit "test_standalone"
    set ssid "test_standalone"
    set passphrase ENC
    set local-standalone enable
    set local-bridging enable
    set schedule "always"
  next
end
```

4. When the FortiAPs are disconnected from the FortiGate, they will reboot at the configured time.
   - The FortiAP with no standalone SSID (FAP1) reboots at the time interval configured in interval1 (5 minutes or 300 seconds).

```
FortiAP-432FR # 03901.181 *****cwFwctlReboot:*****
03901.181     SSID_CNT 1,0. No AC is found in 309 sec (> 300) Rebooting...
[ 4134.665936] reboot: Restarting system
```

- The FortiAP with standalone SSID (FAP2) reboots at the time interval configured in interval2 (10 minutes or 600 seconds).

```
FortiAP-831F login: 01548.738 *****cwFwctlReboot:*****
01548.738     SSID_CNT 1,1. No AC is found in 625 sec (> 600) Rebooting...
[ 1603.673046] reboot: Restarting system
```

To configure FortiAP automatic reboot intervals and wait time - CLI:

When `ap-reboot-wait-interval1` and `ap-reboot-wait-time` is configured, FortiAPs *without* standalone SSIDs wait for `ap-reboot-wait-interval1` or `ap-reboot-wait-time` (whichever comes first). Meanwhile FortiAPs *with* standalone SSIDs wait for the set time in `ap-reboot-wait-time` before automatically rebooting.

1. Configure the FortiAP reboot interval and wait time:

```
config wireless-controller timers
  set ap-reboot-wait-interval1 5
  set ap-reboot-wait-time "15:50"
end
```

2. Verify that FAP1 is managed by FortiGate and has an SSID assigned with local-standalone disabled:

```
FortiAP-432FR # wcfg | grep fsm
fsm-state            : RUN 463
FortiAP-432FR # vcfg
-------------------------------VAP Configuration    1----------------------------
Radio Id  1 WLAN Id  0 test_bridge ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown
(-1)
           vlanid=0, intf=wlan10, vap=0x3915502c, bssid=74:78:a6:e3:63:48
           11ax high-efficiency=enabled target-wake-time=enabled
           bss-color-partial=enabled
           mesh backhaul=disabled
           local_auth=disabled standalone=disabled nat_mode=disabled

FortiAP-432FR # cw_diag -c acs | grep "last seen"
AC last seen time:  0 SSID cnt 0,0 ap reboot wait time 300,0 16:51
```

The `cw_diag -c acs` command output shows the AP reboot wait time as hh+1:mm+1. The 00:00 value is used to indicate that the reboot time is not configured, not that the reboot time is set to 00:00.

3. When the FortiAPs are disconnected from the FortiGate, they will reboot at the configured time.
   - The FortiAP with no standalone SSID (FAP1) reboots at the time interval configured in interval1 (5 minutes or 300 seconds).

```
FortiAP-432FR # 03901.181 *****cwFwctlReboot:*****
03901.181     SSID_CNT 1,0. No AC is found in 309 sec (> 300) Rebooting...
[ 4134.665936] reboot: Restarting system
```

   - The FortiAP with standalone SSID (FAP2) reboots at the time configured in wait-time (15:50).

```
FortiAP-831F # date
Fri Nov 17 15:50:10 GMT 2023
```

```
FortiAP-831F # 01140.026 *****cwFwctlReboot:*****
01140.026     SSID_CNT 1,1. No AC is found in 177 sec (15:50) Rebooting...
[ 1195.218481] reboot: Restarting system
```

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 in the Client load balancing field, select *Frequency Handoff* and *AP Handoff* as required for the AP profile.

From the CLI, you configure wireless client load balancing thresholds for each custom AP profile.

```
config wireless-controller wtp-profile
   edit new-ap-profile
      set handoff-rssi <rssi_int>
      set handoff-sta-thresh <clients_int>
      set frequency-handoff {disable | enable}
      set ap-handoff {disable | enable}
      config radio-1
      end
      config radio-2
      end
   end
```

Configuration options	Description
handoff-rssi	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	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 55, range is 5-60.
frequency-handoff	Enable or disable frequency handoff load balancing. Disabled by default.
ap-handoff	Enable or disable access point handoff load balancing. Disabled by default.

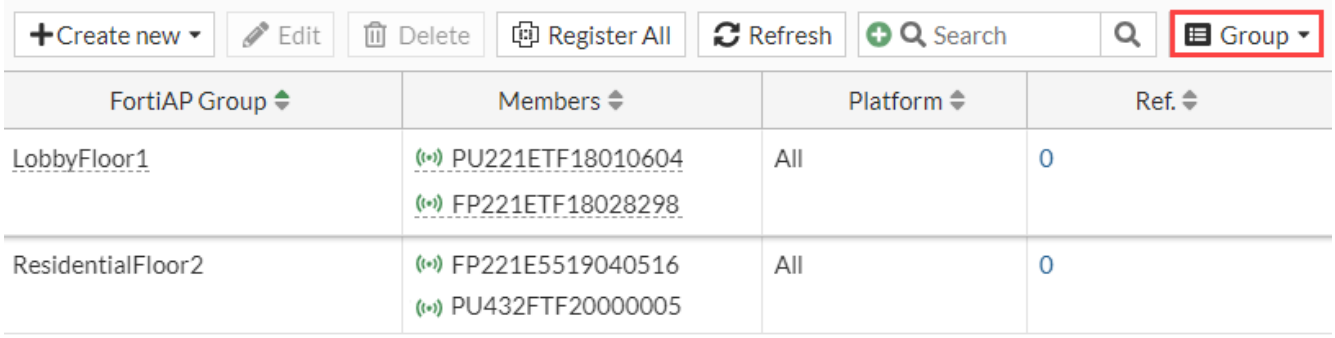
Frequency handoff must be enabled on the 5 GHz radio to learn client capability.

FortiAP groups

FortiAP groups facilitate the management of a large numbers of FortiAPs. For example, you can group APs based on the floor or section of the office they are installed on. Each AP can belong to one group only. Grouping an AP enables you to assign VLANs to all the APs in that group, simplifying the administrative workload. This feature is useful in large deployments as you can break down the broadcast domain, rather than putting all wireless clients into a single subnet. You can also apply security inspections and firewall rules based on the location of the wireless clients, providing you with more granular control over wireless traffic.

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 FortiAP group on page 109.

Once you create a FortiAP group and add FortiAPs to it, you can filter your Managed FortiAPs view by group and easily identify which AP belongs to which areas.



To create a FortiAP group - GUI:

1. Go to *WiFi and 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 FortiEdge Cloud. Some FortiAP models have multiple LAN ports that can provide wired network access.

There are some differences in LAN configuration among FortiAP models:

- Some FortiAP models 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`).
- Other FortiAP models 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.

For information on which FortiAP models have configurable WAN/LAN ports, refer to the FortiAP product data sheet.

This section covers the following topics:

- Configuring a port to WAN-LAN operation mode on page 221
- Bridging a LAN port with the WAN port on page 221

- Bridging a LAN port with an SSID on page 222
- Configuring FortiAP LAN ports on page 223
- Verifying wired clients connected to FortiAP LAN ports on page 225

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 201).
4. Enable the WAN-LAN mode. The method varies depending on the FortiAP model type.
   - Enabling WAN-LAN mode on FortiAP 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 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 LAN port and the WAN port work together as a layer-2 bridge.
- Wired clients are allowed to access the LAN port directly and send/receive data throughout the WAN port without authentication.
- Wired client traffic has the same VLAN ID as that of the WAN port, that is, it has no VLAN tag when `AP_MGMT_VLAN_ID` is `0` (by default), or it is tagged with the same VLAN ID as the current `AP_MGMT_VLAN_ID` value (range 1 to 4094).
- Wired LAN clients are in the same subnet as the FortiAP itself. If wired clients use DHCP address mode, they can get IP addresses assigned by a DHCP server behind the WAN port.

Example configuration:

```
config wireless-controller wtp-profile
  edit "FAP231G-LAN"
    config platform
      set type 231G
    end
    set wan-port-mode wan-lan
      config lan
        set port-mode bridge-to-wan
    end
  next
end
```

For configuration instructions, see Configuring FortiAP LAN ports on page 223.

Bridging a LAN port with an SSID

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

In this configuration:

- The LAN port and the SSID interface work together as a layer-2 bridge.
- The SSID security mode or wireless authentication does not apply to wired clients accessing the LAN port. Wired clients are allowed by default, or undergo MAC-address based authentication configured per LAN port. For information on configuring MAC address authentication, see MAC Authentication for LAN port hosts on page 225
- Wired client traffic follows the VLAN ID assignment of the SSID interface. For static VLANs, wired client traffic has no VLAN tag when the SSID VLAN ID is 0 (by default), or it is tagged with the SSID VLAN ID (range 1 to 4094).
- When the SSID traffic mode is Tunnel, wired LAN clients are in the same subnet of the SSID (or its subordinate VLAN) interface on the FortiGate. If wired clients use DHCP address mode, they can get IP addresses from the DHCP server as configured under the SSID (or sub VLAN) interface in the FortiGate.
- When the SSID traffic mode is Bridge, wired client traffic (with or without a VLAN tag) is bridged locally to the FortiAP WAN port, while the WAN port works as a trunk port. If wired clients use DHCP address mode, they can get IP addresses assigned by a DHCP server behind the WAN port (no VLAN tag) or the corresponding VLAN segment (VLAN tagged).

Example configuration:

```
config wireless-controller vap
  edit "ssid-tunnel"
    set ssid "ssid-tunnel"
    set security wpa3-sae
    set sae-password ********
  next
  edit "ssid-bridge"
    set ssid "ssid-bridge"
    set security wpa3-sae
    set sae-password ********
    set local-bridging enable
    set vlanid 100
  next
end
config wireless-controller wtp-profile
```

```
  edit "FAP23JF-LAN"
    config platform
      set type 23JF
    end
    config lan
      set port1-mode bridge-to-ssid
      set port1-ssid "ssid-tunnel"
      set port2-mode bridge-to-ssid
      set port2-ssid "ssid-bridge"
    end
  next
end
```

The "port1" LAN traffic has no VLAN tag and is sent to the FortiGate through a CAPWAP-data tunnel the same way as the "ssid-tunnel" SSID traffic.

The "port2" LAN traffic is bridged to the local network out of the FortiAP WAN port and has VLAN ID 100 tagged. From the perspective of wired clients, the `vlanid` setting carried by a local-bridging SSID is the most useful information for their local traffic bridging and VLAN ID tagging purposes, especially when the required VLAN is different from the FortiAP's own `AP_MGMT_VLAN_ID`.

For configuration instructions, see Configuring FortiAP LAN ports on page 223.

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 221.
2. Go to *WiFi and 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-23JF 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 "FAP23JF-default"
    config platform
      set type 23JF
    end
      config lan
        set port1-mode bridge-to-ssid
        set port1-ssid "office"
        set port2-mode bridge-to-wan
        set port3-mode bridge-to-wan
    end
  next
end
```

In this example, the default FortiAP-231G profile is configured to bridge the LAN port to the office SSID.

```
config wireless-controller wtp-profile
  edit "FAP231G-default"
    config platform
      set type 231G
    end
    set wan-port-mode wan-lan
    config lan
      set port-mode bridge-to-ssid
      set port-ssid "office"
    end
  next
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 and 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* 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 "FP231GTF22000022"
    set admin enable
    set wtp-profile "FAP231G-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
  next
end
```

Verifying wired clients connected to FortiAP LAN ports

Once the FortiGate and FortiAP have WAN-LAN operation and LAN Port Mode options configured, you can verify and collect data about connected wired clients such as their mode of connection, Tx/Rx rate, authentication status, and OS details. The information is displayed in the FortiGate CLI using `diagnose wireless-controller wlac -c lan-sta`.

The FortiAP LAN1 port must be connected to the FortiGate.

The FortiAP LAN2 port must be connected to the wired clients, either directly to the LAN2 port or through a switch connected to LAN2.

```
# diagnose wireless-controller wlac -c lan-sta
------------------------------LAN STA    1----------------------------
LAN STA mac     : 00:24:9b:79:df:48 (0-1.1.1.2:5246)
    pId         : 0  BR-TO-TUN-SSID Example_SSID
    vlan        : 0
    macauth     : No
    ip          : 95.1.1.2  ARP  48 seconds
    ip6         : fe80::ddaa:41b0:4633:30dd  ARP  4945 seconds  666 pkts
    host info   : VAN-301127-PC1
    vci info    : MSFT 5.0
    os info     : Windows
    uplink      : 226.00bps 33637 pkts 7221244 bytes 9 seconds
    downlink    : 31.00bps 29085 pkts 15442358 bytes 9 seconds
------------------------------Total    1 LAN STAs----------------------------
```

MAC Authentication for LAN port hosts

The following models and versions support the MAC authentication on LAN port:

- FAP-U 6.2.0 and later, managed by FGT running FOS 6.4.3+, without RADIUS accounting and dynamic VLAN assignment.
- FAP 7.0.0 and later, FAP-W2 7.0.0 and later, FAP-C 5.4.3, managed by FGT running FOS 7.0.0+, with RADIUS accounting and dynamic VLAN assignment.

There are two methods for authenticating hosts connected to a LAN port:

- RADIUS-based MAC authentication; and
- MAC address group based from FortiGate.

To configure RADIUS-based MAC authentication:

1. On a RADIUS server, add user entries that have the same username and password as the MAC addresses of the hosts connecting through the LAN port (see Configuring user authentication on page 117).

   The MAC-address user entries can have additional RADIUS attributes added for dynamic VLAN ID assignment (see Configuring dynamic user VLAN assignment on page 104).
2. Prepare a VAP with the "`radius-mac-auth`" feature enabled, and then set the MAC authentication of the LAN port to the RADIUS method.

```
config wireless-controller vap
   edit "port-mac"
      set ssid "lan-bridge-port-mac"
      set security open
      set radius-mac-auth enable
      set radius-mac-auth-server "peap"
      set schedule "always"
      set port-macauth radius
      set port-macauth-timeout 300
      set port-macauth-reauth-timeout 180
      set dynamic-vlan enable
   next
end
```

3. Assign the VAP to a LAN port with the "`bridge-to-ssid`" mode in an AP profile.

   Note: In order for the LAN authentication to take effect, the same VAP must be set under an AP radio at the same time.

```
config wireless-controller wtp-profile
   edit "AP profile"
      config platform
         set type 23JF
      end
      config lan
         set port1-mode bridge-to-ssid
         set port1-ssid "port-mac"
      end
      config radio-1
         set band 802.11ax,n,g-only
         set vap-all manual
         set vaps "port-mac"
      end
      ... ...
      ... ...
   next
end
```

To configure address group based MAC authentication:

1. On FortiGate WiFi controller, add an address group containing MAC addresses with either an allow or deny policy (see Adding a MAC filter on page 89).

```
config wireless-controller address
   edit "001"
      set mac 01:02:03:0a:0b:0c
```

```
      set policy allow
    next
    edit "002"
      set mac 01:02:03:0a:0b:0d
      set policy deny
    next
  end
  config wireless-controller addrgrp
    edit "mac-group"
      set default-policy deny
      set addresses "001" "002"
    next
  end
```

2. In a VAP, first select the address group for the "MAC filter" feature, and then set the MAC authentication of the LAN port to `address-group`.

```
config wireless-controller vap
  edit "port-mac"
    set ssid "lan-bridge-port-mac"
    set security open
    set address-group "mac-group"
    set port-macauth address-group
  next
end
```

3. Assign the VAP to a LAN port with the "`bridge-to-ssid`" mode in an AP profile.

   Note: In order for the LAN authentication to take effect, the same VAP must be set under an AP radio at the same time.

```
config wireless-controller wtp-profile
  edit "AP profile"
    config platform
      set type 23JF
    end
    config lan
      set port1-mode bridge-to-ssid
      set port1-ssid "port-mac"
    end
    config radio-1
      set band 802.11ax,n,g-only
      set vap-all manual
      set vaps "port-mac"
    end
    ... ...
    ... ...
  next
end
```

LAN port aggregation and redundancy

Some FortiAP models have dual Ethernet ports, labeled LAN1 and LAN2. These ports can be reconfigured to support Link Aggregation Control Protocol (LACP) and uplink/POE redundancy.

For information on which FortiAP models have ports that support being reconfigured, refer to the FortiAP product data sheet.

Enabling LACP

Such FortiAP LAN1 and LAN2 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.

LACP enables you to bind two or more physical interfaces together to form an aggregated (combined) link. This new link has the bandwidth of all the links combined. If a link in the group fails, traffic is transferred automatically to the remaining interfaces. The only noticeable effect is reduced bandwidth.

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 201).
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:

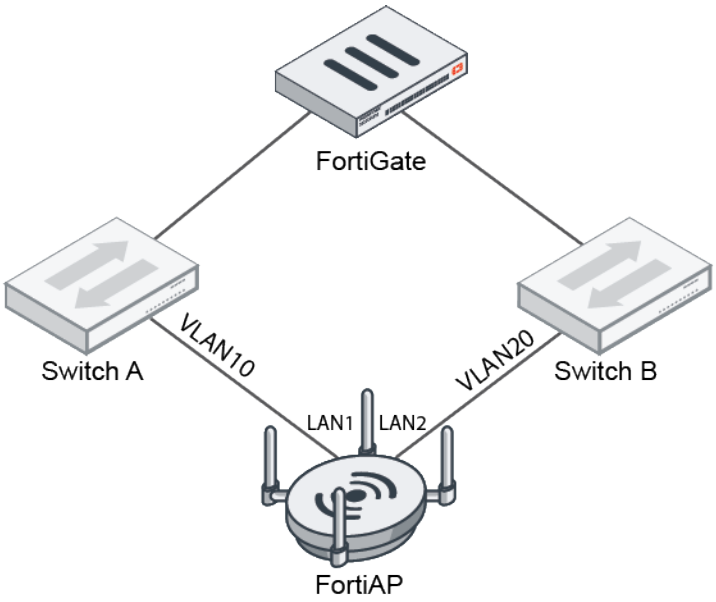
1. Access the CLI of your FortiAP (see FortiAP CLI access on page 201).
2. In the FortiAP CLI, set the `FAP_ETHER_TRUNK` parameter to `2` by entering the following command:
   ```
   cfg -a FAP_ETHER_TRUNK=2
   ```
   Note: By default, `FAP_ETHER_TRUNK` is set to `0`.
3. Save the changes to the device flash with the following command:
   ```
   cfg -c
   ```

LAN port uplink redundancy without LACP

In a redundant interface, traffic only travels over one interface at any time. This differs from an aggregated interface where traffic travels over all interfaces for increased bandwidth.

FortiAP models with dual LAN1 and LAN2 ports can support Layer 2 redundant uplink *without* configuring LACP. One way to achieve redundancy is to isolate both ports with two different management VLANs.

Example Layer 2 uplink redundancy configuration



The preceding figure shows an example uplink configuration:

- On Switch A, VLAN10 is configured as the untagged management VLAN and connects from the FortiAP LAN 1 port to Switch A. On Switch B, VLAN20 has been configured as the untagged management VLAN and connects from the FortiAP LAN 2 port to Switch B.
- Having different management VLANs prevent L2 loops. There are no routing or policies between these VLANs/subnets so the FortiAP cannot discover a management interface outside of its subnet. This prevents routing loops if multicast policies or Bonjour are configured later.
- On the FortiAP, AC1 is set to the VLAN10 management IP and AC2 to the VLAN20 management IP.
- If the uplink on VLAN10 and Switch A fails, the FortiAP will reboot and come online using VLAN20 on Switch B.
  Note that even if VLAN10 becomes reachable again, the FortiAP will not switch back to VLAN 10.
- The FortiAP does not check for AC reachability and only checks to see if the DHCP is available. It gets the IP from either VLAN10 or VLAN20 depending on which DHCP server replies first. It may take a few minutes for the FortiAP to give up on the old AC and rediscover the new one.

For FortiAP models where both LAN ports support POE, this configuration can also achieve POE redundancy. Due to POE sharing, the AP will not reboot when it experiences an uplink failure.

CAPWAP

This section contains topics related to CAPWAP management and configuration.

- IP fragmentation of packets in CAPWAP tunnels on page 230
- CAPWAP bandwidth formula on page 231

- CAPWAP Offloading on page 232
- Improve CAPWAP stability over NAT on page 234

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
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
```

CAPWAP Offloading

Offloading over CAPWAP traffic is supported on mid-range to high-end FortiGates with traffic from tunnel mode virtual APs. The WTP data channel DTLS policy (`dtls-policy`) must be set to `clear-text` or `ipsec-vpn` in the WTP profile (**wireless-controller wtp-profile**). Traffic is not offloaded if it is fragmented.

Session fast path requirements:

1. Enable offloading managed FortiAP and FortiLink CAPWAP sessions:

   ```
   config system npu
       set capwap-offload enable
   end
   ```

2. Enable offloading security profile processing to CP processors in the policy:

   ```
   config firewall policy
       edit 1
           set auto-asic-offload enable
       next
   end
   ```

Verify the system session for offloading:

- Check the system session, when dtls-policy=clear-text to verify npu info: **flag=0x81/0x89, offload=8/8**

```
FG1K2D3I16800192 (vdom1) # diagnose sys session list
    session info: proto=6 proto_state=01 duration=21 expire=3591 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=5
    origin-shaper=
    reply-shaper=
    per_ip_shaper=
    class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
    state=log may_dirty npu f00
    statistic(bytes/packets/allow_err): org=16761744/11708/1 reply=52/1/1 tuples=2
    tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
    orgin->sink: org pre->post, reply pre->post dev=57->37/37->57
gwy=172.16.200.44/10.65.1.2
    hook=post dir=org act=snat 10.65.1.2:50452->172.16.200.44:5001(172.16.200.65:50452)
    hook=pre dir=reply act=dnat 172.16.200.44:5001->172.16.200.65:50452(10.65.1.2:50452)
    pos/(before,after) 0/(0,0), 0/(0,0)
    misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=1
    serial=00009a97 tos=ff/ff app_list=0 app=0 url_cat=0
    rpdb_link_id = 00000000
    dd_type=0 dd_mode=0
    npu_state=0x000c00
    npu info: flag=0x81/0x89, offload=8/8, ips_offload=0/0, epid=158/216, ipid=216/158,
vlan=0x0000/0x0000
    vlifid=216/158, vtag_in=0x0000/0x0000 in_npu=2/2, out_npu=2/2, fwd_en=0/0, qid=4/2
total session 1
```

- Check the system session, when dtls-policy=ipsec-vpn to verify npu info: **flag=0x81/0x82, offload=8/8**

```
FG1K2D3I16800192 (vdom1) # diagnose sys session list
    session info: proto=6 proto_state=01 duration=7 expire=3592 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=5
    origin-shaper=
    reply-shaper=
    per_ip_shaper=
    class_id=0 ha_id=0 policy_dir=0 tunnel=/wlc-004100_0 vlan_cos=0/255
    state=log may_dirty npu f00
    statistic(bytes/packets/allow_err): org=92/2/1 reply=92/2/1 tuples=2
    tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
    orgin->sink: org pre->post, reply pre->post dev=57->37/37->57
gwy=172.16.200.44/10.65.1.2
    hook=post dir=org act=snat 10.65.1.2:50575->172.16.200.44:5001(172.16.200.65:50575)
    hook=pre dir=reply act=dnat 172.16.200.44:5001->172.16.200.65:50575(10.65.1.2:50575)
    pos/(before,after) 0/(0,0), 0/(0,0)
    misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=1
    serial=0000a393 tos=ff/ff app_list=0 app=0 url_cat=0
    rpdb_link_id = 00000000
    dd_type=0 dd_mode=0
    npu_state=0x000c00
    npu info: flag=0x81/0x82, offload=8/8, ips_offload=0/0, epid=158/216, ipid=216/158,
vlan=0x0000/0x0000
    vlifid=216/158, vtag_in=0x0000/0x0000 in_npu=2/2, out_npu=2/2, fwd_en=0/0, qid=0/0
total session 1
```

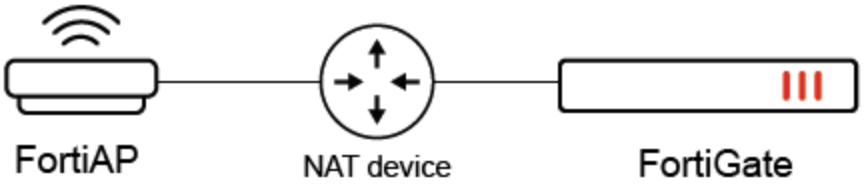
Improve CAPWAP stability over NAT

To minimize downtime caused by unstable Network Address Translation (NAT) device networks, you can customize an interval at which keep-alive messages are sent from FortiAPs to their managing FortiGate. Once the keep-alive message is sent, FortiAPs will not disconnect from the FortiGate even if there is a session timeout configured on the NAT device. This improves CAPWAP stability for FortiAPs that are managed by a FortiGate behind a NAT device.

CLI syntax

```
config wireless-controller timers
  set nat-session-keep-alive <integer>
end
```

`set nat-session-keep-alive`	Maximal time in seconds between control requests sent by the managed WTP, AP, or FortiAP (0 - 255 seconds, default = 0).



To configure NAT session keep-alive message - CLI

1. Configure the interval at which NAT session keep-alive messages are sent in seconds.

```
config wireless-controller timers
  set nat-session-keep-alive 10
end
```

2. Verify the configurations on the FortiAP.

```
FortiAP-231F # cw_diag -c acs
WTP Configuration
    name                 : FortiAP-231F
    loc                  : N/A
    ap mode              : thin AP
    led state            : enable
    PWR LED state        : GREEN     REASON: ACS 0 changed in DATA_CHECK state.
    poe mode cal         : full
    poe mode oper        : full
    allowaccess          :
    lldp enable          : enable
    extension info enable: enable
    radio cnt            : 3
    sta info             : 0/0
    echo-interval        : 30
    nat-sess-keep-alive  : 10
    keep-alive-interval  : 30
...
```

From the cwWtpd deamon output, you can see that a `FTNT_WTP_NOTIF` message is sent every 10 seconds to keep the connection alive if there is no `ECHO_REQ` sent. The timer of `FTNT_WTP_NOTIF` is 10 seconds while the timer of `ECHO_REQ` is 30 seconds.

```
[12/5/2023 7:17:46 PM] 15290.608 AC0     msgType       : 3163149 FTNT_WTP_NOTIF      0
    10.40.29.57:5246
[12/5/2023 7:17:56 PM] 15300.609 AC0     msgType       : 3163149 FTNT_WTP_NOTIF      0
    10.40.29.57:5246
[12/5/2023 7:18:02 PM] 15306.680 AC0     msgType       : 13 ECHO_REQ                 163
    10.40.29.57:5246
[12/5/2023 7:18:12 PM] 15316.608 AC0     msgType       : 3163149 FTNT_WTP_NOTIF      0
    10.40.29.57:5246
[12/5/2023 7:18:22 PM] 15326.609 AC0     msgType       : 3163149 FTNT_WTP_NOTIF      0
    10.40.29.57:5246
[12/5/2023 7:18:32 PM] 15336.608 AC0     msgType       : 3163149 FTNT_WTP_NOTIF      0
    10.40.29.57:5246
[12/5/2023 7:18:32 PM] 15336.677 AC0     msgType       : 13 ECHO_REQ                 164
    10.40.29.57:5246
[12/5/2023 7:18:46 PM] 15350.609 AC0     msgType       : 3163149 FTNT_WTP_NOTIF      0
    10.40.29.57:5246
```

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 can be configured from the CLI and GUI.

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
```

To disable the LEDs from the GUI you must enable Advanced Wireless Features (see Advanced Wireless Features on page 165).

1. Once you enable Advanced Wireless Features, navigate to *WiFi & Switch Controller* > *Operation Profiles* > *FortiAP Profiles*.
2. Select the profile you want.
3. Under *Advanced Settings*, locate *LED usage* and disable the setting.
4. When you are finished, click *OK*.

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`.

To configure LED schedules - GUI:

1. Once you enable Advanced Wireless Features, navigate to *WiFi & Switch Controller* > *Operation Profiles* > *FortiAP Profiles*.
2. Select the profile you want.
3. Under *Advanced Settings*, locate *LED usage* and enable the setting.
4. Click the LED usage field and select the schedules you want to associate LED illumination with.
5. When you are finished, click *OK*.

Syntax

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

Configure FortiAP MIMO values

You can configure Multiple-Input Multiple-Output (MIMO) values on select FortiAP and FortiAP-U models, offering more flexibility when using a third-party antenna connected to a limited number of AP ports.

MIMO mode configuration is supported on the following:

Family	Series
FortiAP	F and G series models
FortiAP-U	EV and F series models

MIMO values can be set under radio configuration when creating or editing a FortiAP profile. The value range available is confined within each AP platform and radio's MIMO specifications (default, 1x1, 2x2, 3x3, 4x4, 8x8).

```
config wireless-controller wtp-profile
  edit < profile_name >
    config radio-< number >
      set mimo-mode [ actual modes supported depend on AP platform ]
    end
  next
end
```

For example, FAP-231G radios support a maximum of 2x2 MIMO, so you can select between 1x1 or 2x2. Meanwhile FAP-831F radios support a maximum of 8x8 MIMO, so you can select between 1x1, 2x2, 3x3, 4x4 or 8x8.

To configure MIMO mode values:

```
config wireless-controller wtp-profile
  edit FAP431G-default
    config radio-1
      set mimo-mode 3x3
    end
    config radio-2
      set mimo-mode 3x3
    end
    config radio-3
      set mimo-mode 2x2
    end
  end
```

To verify that the MIMO mode settings have been applied:

```
FortiAP-431G # rcfg | grep mimo
   mimo,chainmask : 3, 0x7 (mimo) 0xf (power) 0x7/0x7 (oper)
   mimo,chainmask : 3, 0x70 (mimo) 0xf0 (power) 0x70/0x70 (oper)
   mimo,chainmask : 2, 0x3 (mimo) 0xf (power) 0x3/0x3 (oper)
```

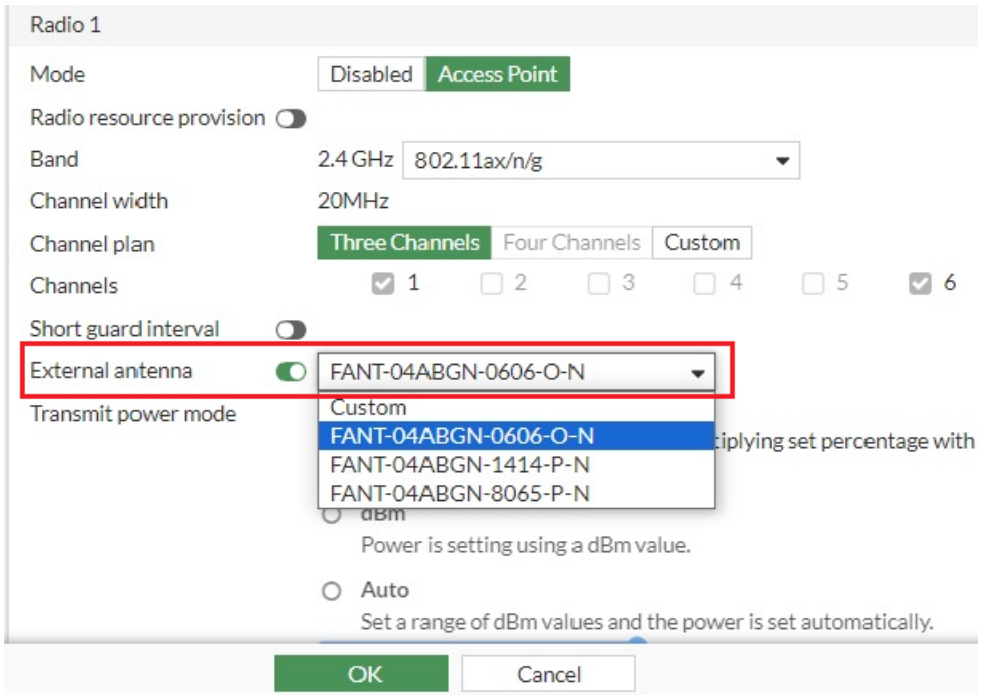
Configure Fortinet external antenna parameters for specific FortiAPs

You can install Fortinet external antennas on FAP-432F, FAP-433F, FAP-U432F, and FAP-U433F models. Fortinet external antennas can help optimize coverage and overall wireless performance in various installation settings. On supported FortiAP models, you can configure a new FortiAP profile setting and choose from a list of supported Fortinet external antenna models. This setting allows antenna gains specific to the Fortinet external antenna model and the Wi-Fi band (2.4 GHz or 5 GHz) to be taken into consideration by the FortiGate Wireless controller when setting transmit power for a managed FortiAP device.

To see which external antenna and predefined types correspond to which SKU, refer to the Fortinet Antenna Portfolio Data Sheet.

To configure supported external antenna - GUI

1. Go to *WiFi and Switch Controller* > *FortiAP Profiles* and select *Create New*.
2. From *Platform*, select a FortiAP model that supports external antennas.
3. Under the *Radio* section, enable *External antenna* and select the antenna that you want to install.



4. When you are finished, click *OK*.

To configure supported external antenna - CLI

1. Create a FortiAP profile and select a platform that supports external antennas. In `set optional-antenna`, enter the antenna model.

```
config wireless-controller wtp-profile
  edit "FP432F"
    config platform
      set type 432F
    end
    config radio-2
      set optional-antenna FANT-04ABGN-1414-P-N
    end
  next
end
```

2. Verify the settings have been applied:

```
# diagnose wireless-controller wlac -c wtpprof FP432F | grep antenna
    ..
    opt antenna      : FANT_04ABGN_1414_P_N
```

3. From the FortiAP CLI, check that antenna configurations have been applied:

```
FortiAP-432F # rcfg
… …
Radio 1: AP
   country         : cfg=US oper=US
   countryID       : cfg=841 oper=841
   802.11d enable  : enabled
   sta info        : 0/0
   radio type      : 11AX_5G
```

```
      mimo,chainmask : 4, 0xf0 (mimo) 0xf0 (power) 0xf0/0xf0 (oper)
      airtime fairness   : disabled
      ps optimize    : 0
      tx optimize    : f
      11g prot mode  : 0
      HT20/40 coext  : 1
      beacon intv    : 100
      opt antenna    : FANT_04ABGN_1414_P_N
      txpwr mode     : set by percentage (100%)
   … …
```

Configure third-party antennas in select FortiAP models

You can install third-party antennas on select FortiAP models and customize their antenna gain. On FortiAP models that support third-party antennas, you can enable a FortiAP profile external antenna setting and customize the antenna gain in dB. Third-party antennas can help optimize coverage and overall wireless performance in various installation settings.

The following table shows which FortiAP models support third-party antennas:

FortiAP F models	FAP-432F
	FAP-432FR
	FAP-433F
FortiAP G models	FAP-233G
	FAP-432G
	FAP-433G
FortiAP-U F models	FAP-U432F
	FAP-U433F

The following CLI commands are used to configure third-party antenna parameters:

```
config wireless-controller wtp-profile
  edit <name>
    config platform
      set type [432F|432FR|...]
    end
    config radio-2
      set optional-antenna [none|custom|FANT-04ABGN-0606-O-R|...]
      set optional-antenna-gain {integer}
    end
   next
end
```

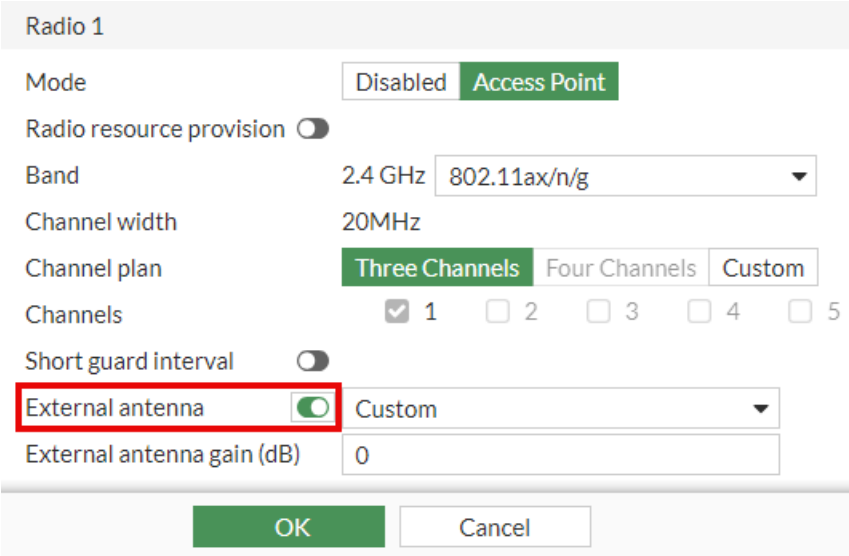
`set optional-antenna`	Set which optional antenna you want to use on the FAP (default = none).
`set optional-antenna-gain`	Set the optional antenna gain in dBi (0 to 20, default = 0).

When configuring your antenna, the antenna gain values (in dBi) must remain within regulatory EIRP limits.

Consult your external antenna documentation and regulatory authority standards for details.

To configure FortiAP to use third-party antennas - GUI

1. Go to *WiFi and Switch Controller* > *FortiAP Profiles* and select *Create New*.
2. In *Platform*, select a FortiAP model that supports external antennas.
3. Under the *Radio* section, enable *External antenna* and select *Custom*.



4. In *External antenna gain (dB)*, configure a value between 0 to 20.
5. When you are finished, click *OK*.

To configure FortiAP to use third-party antennas - CLI

1. Create a FortiAP profile and select a platform that supports third-party antennas.

   Set `optional-antenna` to `custom` and configure an `optional-antenna-gain` value between 0 to 20.

```
config wireless-controller wtp-profile
  edit "FP433G"
    config platform
      set type 433G
    end
    config radio-2
      set optional-antenna custom
      set optional-antenna-gain "10"
    end
   next
end
```

2. Verify the settings have been applied:

```
# diagnose wireless-controller wlac -c wtpprof FP433G | grep antenna
    opt antenna      : Custom
    opt antenna gain : 10
```

3. From the FortiAP CLI, check that antenna configurations have been applied:

```
FortiAP-433G # rcfg
… …
Radio 1: AP
   country         : cfg=US oper=US
   countryID       : cfg=841 oper=841
   802.11d enable  : enabled
   sta info        : 0/0
   radio type      : 11AX_5G
   mimo,chainmask : 4, 0xf0 (mimo) 0xf0 (power) 0xf0/0xf0 (oper)
   airtime fairness   : disabled
   ps optimize     : 0
   tx optimize     : f
   11g prot mode   : 0
   HT20/40 coext   : 1
   beacon intv     : 100
   opt antenna     : Custom
   opt ant gain    : 10
… …
```

Configure FortiAP USB port status

You can enable or disable the USB port on applicable FortiAP models provided the FortiAP is operating in Full Power mode. If the FortiAP lacks sufficient power supply to operate in Full Power mode, the USB is enforced to turn off.

CLI commands:

```
conf wireless-controller wtp-profile
  edit <name>
    set usb-port {enable | disable}
  next
end
```

By default, `usb-port` is set to `enable`.

To configure the FortiAP USB port status:

1. From the FortiGate, set the USB port status on a FortiAP profile:

```
config wireless-controller wtp-profile
  edit FAP231G-default
    set usb-port enable
  next
end
```

2. Apply the FortiAP profile to a FortiAP:

```
config wireless-controller wtp
  edit "FP231GTF23046245"
    set wtp-profile FAP231G-default
  next
end
```

To verify the FortiAP USB port status:

1. Check that the USB port status matches the configurations you applied.

```
diag wireless-controller wlac -c wtp FP231GTF23046245 | grep usb
    usb port         : enabled(enabled from AC)
    usb port oper    : enabled
```

2. From the FortiAP, check the profile is successfully applied and that the AP is operating in full power mode.

```
FortiAP-231G # cw_diag power
Power Detection Data: dc=0 ps1=1 af1=0 at1=1 psv1=0 bt1=0 ps2=0 af2=0 at2=0 psv2=0 bt2=0
                      Budget lldp 0,0 poe 25,0 (dc=99 af=13 at=25 psv=60 bt=50 full=24.9
low=24.9)
Current   Power Mode: full (2)  Oper Power Mode: full (2)
    Radio 1: MaxTxpower 50 TxChainMask 0x03 RxChainMask 0x03
    Radio 2: MaxTxpower 50 TxChainMask 0x03 RxChainMask 0x03
    Radio 3: MaxTxpower 50 TxChainMask 0x03 RxChainMask 0x03
        USB: enabled
full:usb,txpower full; low:txpower 17,disable radio-3
```

3. Use the `wcfg` command to show the USB port status.

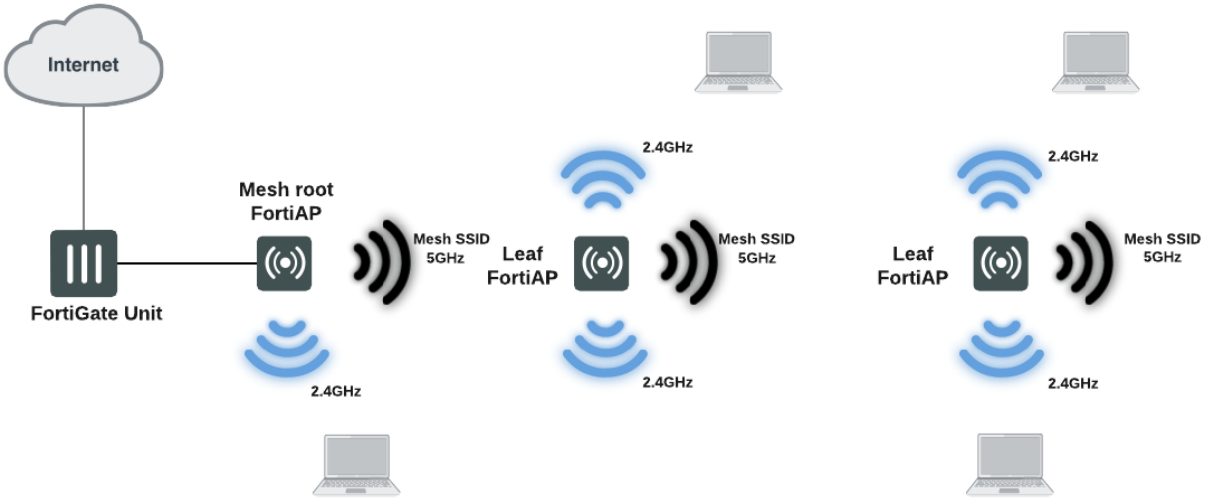
```
FortiAP-231G # wcfg | grep usb
    usb port             : enabled(enabled from AC)
    usb port oper        : enabled
```

4. Verify that you can successfully plug in a USB device to the FortiAP.

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.

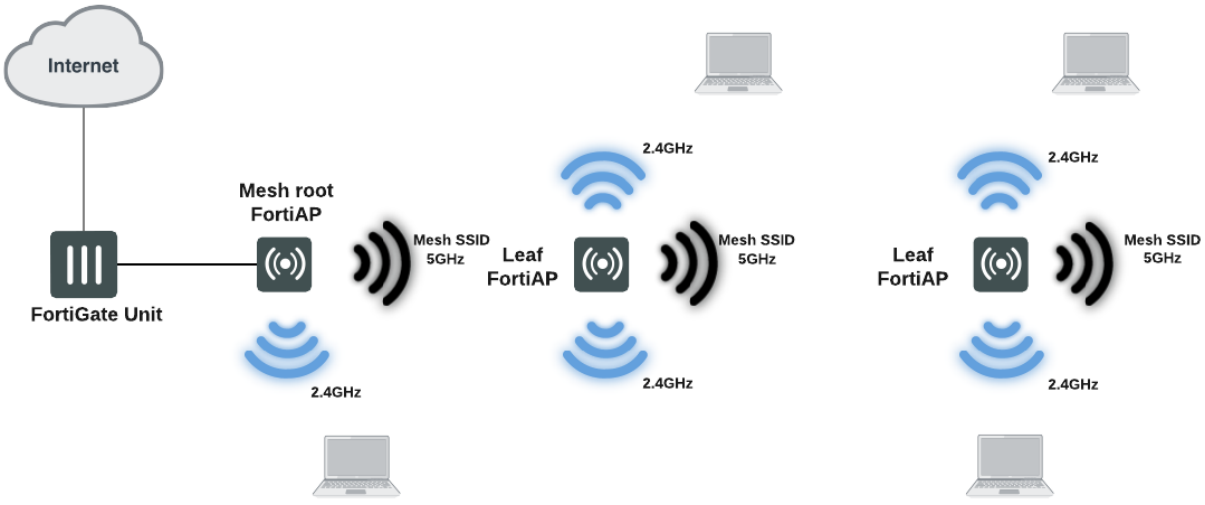
Firmware requirements

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.

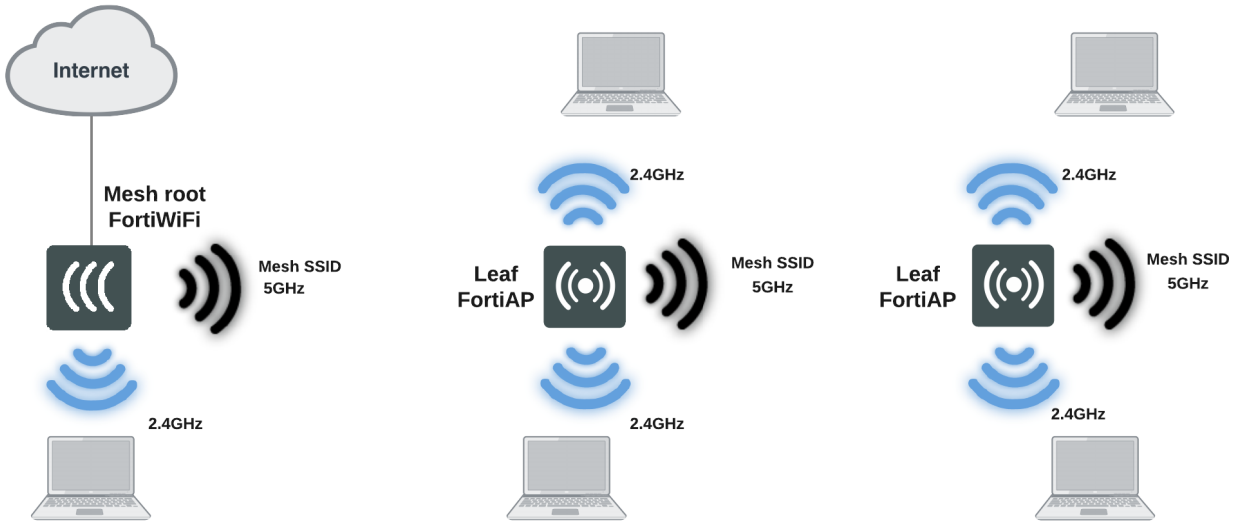
Types of wireless mesh

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

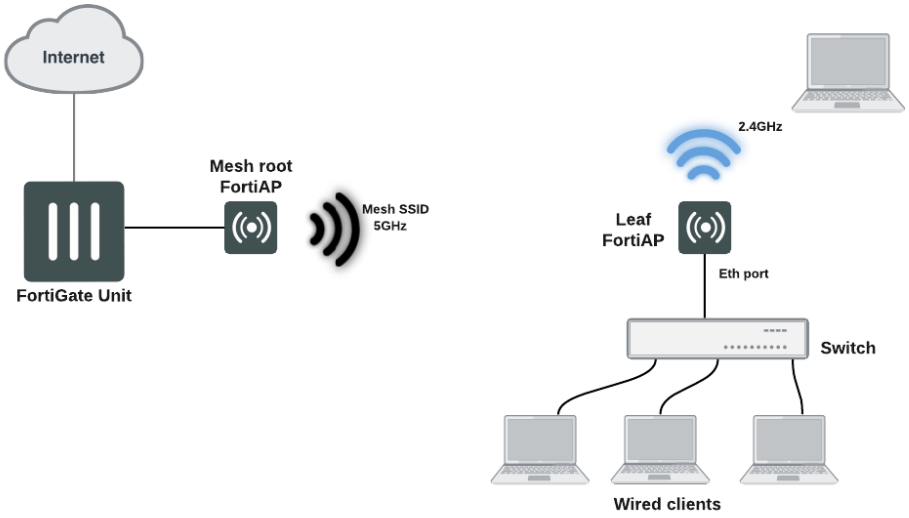


FortiWiFi unit as mesh root AP with FortiAP units as leaf APs



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 442

Configuring a meshed WiFi network

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

- Creating the mesh root SSID on page 246
- Creating the FortiAP profile on page 247
- Configuring the mesh root AP on page 247
- Configuring the mesh leaf FortiAPs on page 248
- Authorizing leaf APs on page 249
- Creating security policies on page 249
- Viewing the status of the mesh network on page 250

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 - GUI:

1. Go to *WiFi and Switch Controller* > *SSIDs* and select *Create New* > *SSID*.
2. Enter a *Name* for the WiFi interface.
3. In *Traffic Mode*, select *Mesh*.
4. Enter the *SSID*.
5. Select a *Security Mode*. You can choose between the following:
   - *WPA2 Personal*.

     If you select WPA2 Personal, you must enter a *Pre-shared key*. Remember the key because you need to enter it for the leaf FortiAP configuration.
   - *WPA3 SAE*.

     If you select WPA3 SAE, you must enter an SAE password. Hash-to-Element (H2E) only is enabled by default and cannot be disabled as it is mandatory for WiFi 6E technology.
6. When you are finished, click *OK*.

To configure the mesh root SSID - CLI:

```
config wireless-controller vap
  edit "MESHROOT"
    set mesh-backhaul enable
    set ssid "fortinet.mesh.root"
```

```
    set security wpa3-sae
    set pmf enable
    set sae-h2e-only enable
    set schedule "always"
    set sae-password ENC *
  next
end
```

You can set the security mode to WPA3-SAE when using the CLI. WPA3-SAE (with Hash-to-Element only enabled) is mandatory in Wi-Fi 6E technology, so you must select it if you want to use Wi-Fi 6E FortiAPs to set up mesh connections over the 6GHz band.

By default, `sae-h2e-only` is enabled when you set the security mode to `wpa3-sae`.

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 38.

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 & and 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 *Transmit power* amount or select *Auto*.
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 and Switch Controller* > *SSIDs* 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 *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 248), 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 and 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, password (pre-shared key), and security mode:

```
cfg -a MESH_AP_TYPE=1
cfg -a MESH_AP_SSID=fortinet.mesh.root
cfg -a MESH_AP_PASSWD=hardtoguess
cfg -a MESH_AP_SECURITY=2
cfg -c
```

```
exit
```

Note: By default, `MESH_AP_SECURITY` is set to `0` (Open network). Depending on the security mode of your mesh backhaul SSID, you must explicitly set it to either `1` (WPA/WPA2-Personal) or `2` (WPA3-SAE).

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 and 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, password (pre-shared key), and security mode:

```
cfg -a MESH_AP_TYPE=1
cfg -a MESH_AP_SSID=fortinet.mesh.root
cfg -a MESH_AP_PASSWD=hardtoguess
cfg -a MESH_AP_SECURITY=2
cfg -c
exit
```

   Note: By default, `MESH_AP_SECURITY` is set to `0` (Open network). Depending on the security mode of your mesh backhaul SSID, you must explicitly set it to either `1` (WPA/WPA2-Personal) or `2` (WPA3-SAE).
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 and 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.

See Configuring firewall policies for the SSID on page 136.

Viewing the status of the mesh network

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

Access Point	SSIDs	Channel	Clients	OS Version
Online 2				
FP221E5519040516	R1 DocuTest (wifi) R2 MeshRoot (mesh.root)	R1 11 R2 36	0	v7.2.0 build0317
PU221ETF18010604	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs	R1 1 R2 112	0	v6.2.0 build0323

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, hover 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 247.
  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 248 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. FortiGate configurations are available up Hotspot 2.0 Release 3.

To configure Hotspot 2.0 ANQP, use the CLI commands available under `config wireless-controller hostspot20`.

A hotspot profile needs to be attached to 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
```

Configure hotspot profile

```
config wireless-controller hotspot20 hs-profile
```

`edit <name>`	Hotspot profile name.
`set 3gpp-plmn {string}`	3GPP PLMN name.
`set access-network-asra [enable|disable]`	Enable/disable additional step required for access (ASRA).
`set access-network-esr [enable|disable]`	Enable/disable emergency services reachable (ESR).
`set access-network-internet [enable|disable]`	Enable/disable connectivity to the Internet.
`set access-network-type {option}`	Access network type.
`set access-network-uesa [enable|disable]`	Enable/disable unauthenticated emergency service accessible (UESA).
`set advice-of-charge {string}`	Advice of charge.
`set anqp-domain-id {integer}`	ANQP Domain ID.
`set bss-transition [enable|disable]`	Enable/disable basic service set (BSS) transition Support.
`set conn-cap {string}`	Connection capability name.
`set deauth-request-timeout {integer}`	Deauthentication request timeout (in seconds).

`set dgaf [enable|disable]`	Enable/disable downstream group-addressed forwarding (DGAF).
`set domain-name {string}`	Domain name.
`set gas-comeback-delay {integer}`	GAS comeback delay.
`set gas-fragmentation-limit {integer}`	GAS fragmentation limit.
`set hessid {mac-address}`	Homogeneous extended service set identifier (HESSID).
`set ip-addr-type {string}`	IP address type name.
`set l2tif [enable|disable]`	Enable/disable Layer 2 traffic inspection and filtering.
`set nai-realm {string}`	NAI realm list name.
`set network-auth {string}`	Network authentication name.
`set oper-friendly-name {string}`	Operator friendly name.
`set oper-icon {string}`	Operator icon.
`set osu-provider <name1>, <name2>, ...`	Manually selected list of Online Sign Up (OSU) provider (s). OSU provider name.
`set osu-provider-nai {string}`	Online Sign Up (OSU) Provider NAI.
`set osu-ssid {string}`	Online sign up (OSU) SSID.
`set pame-bi [disable|enable]`	Enable/disable Pre-Association Message Exchange BSSID Independent (PAME-BI).
`set proxy-arp [enable|disable]`	Enable/disable Proxy ARP.
`set qos-map {string}`	QoS MAP set ID.
`set release {integer}`	Hotspot 2.0 Release number.
`set roaming-consortium {string}`	Roaming consortium list name.
`set terms-and-conditions {string}`	Terms and conditions.
`set venue-group {option}`	Venue group.
`set venue-name {string}`	Venue name.
`set venue-type {option}`	Venue type.
`set venue-url {string}`	Venue name.
`set wan-metrics {string}`	WAN metric name.
`set wnm-sleep-mode [enable|disable]`	Enable/disable wireless network management (WNM) sleep mode.
`set roaming-consortium <string>`	Enable/disable Wireless Broadband Alliance (WBA) OpenRoaming support.

set wba-open-roaming [enable|disable]	WBA ID of financial clearing provider.
set wba-financial-clearing-provider <string>	WBA ID of data clearing provider.
set wba-data-clearing-provider <string>	Three letter currency code.
set wba-charging-currency <string>	Number of currency units per kilobyte (0 to 4294967295).
set wba-charging-rate <integer>	Enable/disable Wireless Broadband Alliance (WBA) OpenRoaming support.

Configure 3GPP public land mobile network (PLMN)

```
config wireless-controller hotspot20 anqp-3gpp-cellular
```

edit <name>	3GPP PLMN name.
config mcc-mnc-list	Mobile Country Code and Mobile Network Code configuration.
edit <id>	ID.
set set id {integer}	ID.
set mcc {string}	Mobile country code.
set mnc {string}	Mobile network code.

Configure IP address type availability

```
config wireless-controller hotspot20 anqp-ip-address-type
```

edit <name>	IP type name.
set ipv6-address-type {option}	IPv6 address type.
set ipv4-address-type {option}	IPv4 address type.

Configure network access identifier (NAI) realm

```
config wireless-controller hotspot20 anqp-nai-realm
```

edit <name>	NAI realm list name.
config nai-list	NAI list.

edit <name>	NAI realm name.
set encoding {enable | disable}	Enable/disable format in accordance with IETF RFC 4282.
set nai-realm {string}	Configure NAI realms (delimited by a semi-colon character).
config eap-method	EAP Methods.
edit <index>	EAP method index.
set method {option}	EAP method type.
config auth-param	EAP auth param.
edit <index>	Param index.
set id {option}	ID of authentication parameter.
set val {option}	Value of authentication parameter.

Configure network authentication type

```
config wireless-controller hotspot20 anqp-network-auth-type
```

edit <name>	Authentication type name.
set auth-type {option}	Network authentication type.
set url {string}	Redirect URL.

Configure roaming consortium

```
config wireless-controller hotspot20 anqp-roaming-consortium
```

edit <name>	Roaming consortium name.
config oi-list	Organization identifier list.
edit <index>	OI index.
set oi {string}	Organization identifier.
set comment {string}	Comment.

Configure venue name duple

```
config wireless-controller hotspot20 anqp-venue-name
```

edit <name>	Name of venue name duple.
config value-list	Name list.
edit <index>	Value index.
set lang {string}	Language code.
set value {string}	Venue name value.

Configure venue URL

```
config wireless-controller hotspot20 anqp-venue-url
```

edit <name>	Name of venue url.
config value-list	URL list.
edit <index>	URL index.
set number {integer}	Venue number.
set value {string}	Venue URL value.

Configure advice of charge (AOC)

```
config wireless-controller hotspot20 h2qp-advice-of-charge
```

edit <name>	Plan name.
config aoc-list	AOC list.
edit <name>	Advice of charge ID.
set type {option}	Usage charge type.
set nai-realm-encoding {string}	NAI realm encoding.
set nai-realm {string}	NAI realm list name.
config plan-info	Plan info.
edit <name>	Plan name.
set lang {string}	Language code.
set currency {string}	Currency code.
set info-file {string}	Info file.

Configure connection capability

```
config wireless-controller hotspot20 h2qp-conn-capability
```

edit <name>	Connection capability name.
set icmp-port {option}	Set ICMP port service status.
set ftp-port {option}	Set FTP port service status.
set ssh-port {option}	Set SSH port service status.
set http-port {option}	Set HTTP port service status.
set tls-port {option}	Set TLS VPN (HTTPS) port service status.
set pptp-vpn-port {option}	Set Point to Point Tunneling Protocol (PPTP) VPN port service status.
set voip-tcp-port {option}	Set VoIP TCP port service status.
set voip-udp-port {option}	Set VoIP UDP port service status.
set ikev2-port {option}	Set IKEv2 port service for IPsec VPN status.
set ikev2-xx-port {option}	Set UDP port 4500 (which may be used by IKEv2 for IPsec VPN) service status.
set esp-port {option}	Set ESP port service (used by IPsec VPNs) status.

Configure operator friendly name

```
config wireless-controller hotspot20 h2qp-operator-name
```

edit <name>	Friendly name ID.
config value-list	Name list.
edit <index>	Value index.
set lang {string}	Language code.
set value {string}	Friendly name value.

Configure online sign up (OSU) provider Network Access Identifier (NAI) list

```
config wireless-controller hotspot20 h2qp-osu-provider-nai
```

edit <name>	OSU provider NAI ID.
config nai-list	Name list.
edit <name>	OSU NAI ID.
set osu-nai {string}	OSU NAI.

Configure online sign up (OSU) provider list

```
config wireless-controller hotspot20 h2qp-osu-provider
```

edit <name>	OSU provider ID.
config friendly-name	OSU provider friendly name.
edit <index>	OSU provider friendly name index.
set lang {string}	Language code.
set friendly-name {string}	OSU provider friendly name.
set server-uri {string}	Server URI.
set osu-method {option}	OSU method list.
set osu-nai {string}	OSU NAI.
config service-description	OSU service name.
edit <service-id>	OSU service ID.
set lang {string}	Language code.
set service-description {string}	Service description.
set icon {string}	OSU provider icon.

Configure terms and conditions

```
config wireless-controller hotspot20 h2qp-terms-and-conditions
```

edit <name>	Terms and Conditions ID.
set filename {string}	File name.
set timestamp {integer}	Timestamp.
set url {string}	URL.

Configure WAN metrics

```
config wireless-controller hotspot20 h2qp-wan-metric
```

edit <name>	WAN metric name.
set link-status {option}	Link status.
set symmetric-wan-link {option}	WAN link symmetry.
set link-at-capacity {enable | disable}	Link at capacity.
set uplink-speed {integer}	Uplink speed (in kilobits/s).
set downlink-speed {integer}	Downlink speed (in kilobits/s).
set uplink-load {integer}	Uplink load.
set downlink-load {integer}	Downlink load.
set load-measurement-duration {integer}	Load measurement duration (in tenths of a second).

Configure Online Sign Up (OSU) provider icon

```
config wireless-controller hotspot20 icon
```

edit <name>	Icon list ID.
config icon-list	Icon list.
edit {name}	Icon name.
set lang {string}	Language code.
set file {string}	Icon file.
set type {option}	Icon type.
set width {integer}	Icon width.
set height {integer}	Icon height.

Configure Quality of Service (QoS) map set

```
config wireless-controller hotspot20 qos-map
```

edit <name>	QOS-MAP name.
config dscp-except	Differentiated Services Code Point (DSCP) exceptions.
edit <index>	DSCP exception index.

`set dscp {integer}`	DSCP value.
`set up {integer}`	User priority.
`config dscp-range`	Differentiated Services Code Point (DSCP) ranges.
`edit <index>`	DSCP range index.
`set up {integer}`	User priority.
`set low {integer}`	DSCP low value.
`set high {integer}`	DSCP high value.

Configuring OpenRoaming on FortiAP

FortiGate supports the Wireless Broadband Alliance (WBA) OpenRoaming Standards on FortiAPs. OpenRoaming enhances Wi-Fi management and user experience by automating guest Wi-Fi onboarding, enabling seamless and secure roaming between Wi-Fi and LTE/5G networks, and providing you with insightful customer analytics. For example, when implemented in a city, tourists can roam between Wi-Fi networks throughout the city without manual authentication, enabling them to stay connected while traveling.

The following CLI configuration settings are used to configure OpenRoaming:

```
config wireless-controller hotspot20 hs-profile
    edit <name>
        set roaming-consortium <string>
        set wba-open-roaming [enable | disable]
        set wba-financial-clearing-provider <string>
        set wba-data-clearing-provider <string>
        set wba-charging-currency <string>
        set wba-charging-rate <integer>
    next
end
```

`set wba-open-roaming`	Enable/disable Wireless Broadband Alliance (WBA) OpenRoaming support.
`set wba-financial-clearing-provider`	WBA ID of financial clearing provider.
`set wba-data-clearing-provider`	WBA ID of data clearing provider.
`set wba-charging-currency`	Three letter currency code.
`set wba-charging-rate`	Number of currency units per kilobyte (0 to 4294967295).

To enable OpenRoaming on FortiAP - CLI:

1. Create a Hotspot 2.0 Access Network Query Protocol (ANQP) Roaming Consortium profile, and specify the Organization Identifier (OI) for the device's service provider.

```
config wireless-controller hotspot20 anqp-roaming-consortium
  edit "openroaming"
    config oi-list
      edit 1
        set oi "BAA2D00000"
      next
    end
  next
end
```

2. Create a Hotspot 2.0 profile and apply the ANQP Roaming Consortium profile you created, and then configure OpenRoaming options.

```
config wireless-controller hotspot20 hs-profile
  edit "openroaming"
    set roaming-consortium "openroaming"
    set wba-open-roaming enable
    set wba-financial-clearing-provider "RBC"
    set wba-data-clearing-provider "444444"
    set wba-charging-currency "CAN"
    set wba-charging-rate 135
  next
end
```

3. Apply the Hotspot 2.0 profile to a FortiAP Virtual AP.

```
config wireless-controller vap
  edit "40f.ent.radius"
    set ssid "radius.openroaming"
    set security wpa2-only-enterprise
    set auth radius
    set radius-server "radius-wifi"
    set schedule "always"
    set hotspot20-profile "openroaming"
  next
end
```

4. Apply the Virtual AP to a FortiAP profile.

```
config wireless-controller wtp-profile
  edit "831F"
    config platform
      set type 831F
    end
    config radio-2
      set vap-all manual
      set vaps "40f.ent.radius"
    end
  next
end
```

5. Apply the FortiAP profile to a FortiAP.

```
config wireless-controller wtp
  edit "FP831FTF21000074"
    set admin enable
    set wtp-profile "831F"
```

```
  next
end
```

6. Using a packet capture tool, verify that OpenRoaming configurations have been successfully applied.

   When the client connects to the SSID, the Access-Request from the FortiGate to the RADIUS server includes the following example OpenRoaming information:

```
WBA-Offered-Service (Type:26, Vendor ID:14122, Subtype:12),
WBA_FINANCIAL_CLEARING_PROVIDER (Type: 26, Vendor ID:14122, Subtype:13),
WBA_DATA_CLEARING_PROVIDER (Type:26, Vendor ID:14122, Subtype:14),
WBA-Linear-Volume-Rate (Type:26, Vendor ID:14122, Subtype:15),
```

Wireless network with wired LAN configuration

This section includes the following topics:

- How to combine a wireless network and wired LAN with a software switch on page 262
- How to configure a FortiAP local bridge (private cloud-managed AP) on page 264
- How to increase the number of supported FortiAPs on page 267
- How to implement multi-processing for large-scale FortiAP management on page 268

How to combine a wireless network and wired LAN with a software switch

A wireless network can be combined with a wired LAN so that wireless 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 wireless 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 wireless and internal network interface as members.
- Configure Captive Portal security for the software switch interface.

To configure the SSID - GUI:

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

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

3. Click *OK*.
4. Go to *WiFi and 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 wireless 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 33. 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

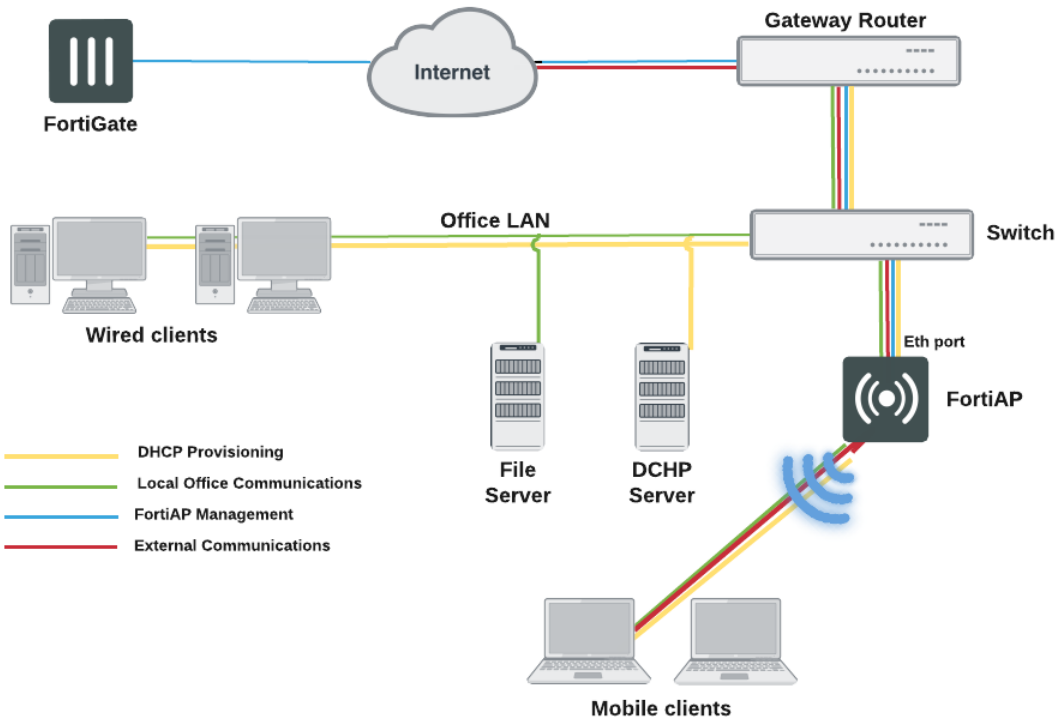
The configuration described above provides communication between wireless and wired LAN users only. To provide access to other networks, create appropriate firewall policies between the software switch and other interfaces.

How to configure 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.

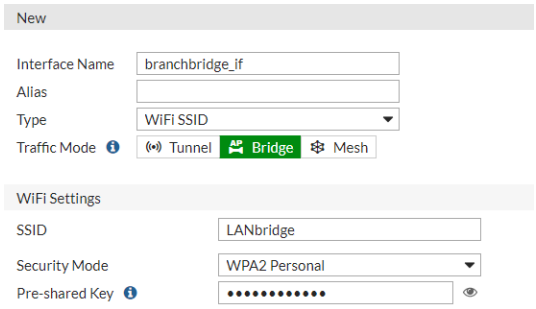
To configure a FortiAP local bridge - GUI:

1. Go to *WiFi and Switch Controller* > *SSIDs* 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 and 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 Wi-Fi and wired networks.

The FortiAP unit can continue to authenticate users if the SSID meets the following conditions:

- *Traffic mode* is set to *Bridge* with the FortiAP Interface.
  In this mode, the FortiAP unit does not send traffic back to the wireless controller.

- *Security mode* is set to one of the following modes:
  - Open
  - WPA/WPA2-Personal
  - WPA/WPA2-Enterprise
  - WPA3-Enterprise
  - WPA3-SAE
  - WPA3-SAE Transition
  - WPA3-OWE
- *Captive Portal* with external authentication portal is enabled.
- *Local standalone* mode is enabled.
  This allows new Wi-Fi client connections when the controller is down. This field is available only if the other conditions have been met. By default, this option is disabled.

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
```

How to increase the number of supported FortiAPs

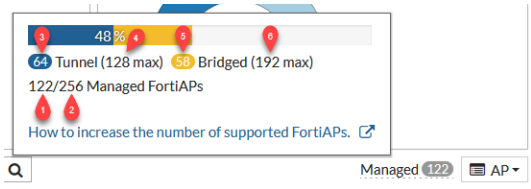
You can increase the number of FortiAP units supported by the FortiGate wireless controller if you configure the FortiAPs to run in local Bridge mode instead of in Tunnel mode.

For each FortiGate model, there are two maximum values that represent the number of FortiAP units that can be supported:

- The number of FortiAPs that can be supported while operating in Tunnel mode; and
- The number of FortiAPs that can be supported while operating in Bridged mode.

To see the maximum number of FortiAPs that can be supported, go to the Managed FortiAP page (*WiFi and Switch Controller* > *Managed FortiAPs*) and look at the top right for *Managed*. The number by *Managed* represents the number of FortiAPs currently being managed.

Hold the pointer over the number to see the maximum number of FortiAPs that can be supported.



Label	Description
1	The total number of Tunnel and Bridged FortiAPs currently being managed.
2	The maximum number of Tunnel and Bridged FortiAPs that can be supported by this FortiGate. For more detailed information, consult the Maximum Values Table.
3	The number of Tunnel FortiAPs currently being managed.
4	The maximum possible number of Tunnel FortiAPs that can be supported currently. This number may change if you add or remove Bridged FortiAPs, but has an upper limit.
5	The number of Bridged FortiAPs currently being managed.
6	The maximum possible number of Bridged FortiAPs that can be supported currently. This number changes if you add or remove Tunnel FortiAPs.

To configure FortiAP units for Bridge mode operation via the GUI:

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 the designated FortiAP unit to use the custom AP profile.

   The FortiAP unit automatically switches to Bridge mode.

To configure FortiAP units for Bridge mode operation via the CLI:

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. Use the following CLI example to manually select the custom AP profile for the FortiAP unit:

```
config wireless-controller wtp
  edit FP221E3X16000017
    set wtp-profile 221E_bridge
  end
```

How to implement multi-processing for large-scale FortiAP management

You can configure multiple processors for wireless daemons to scale large numbers of FortiAP per FortiGate Controller. For FortiGate managed APs, it splits the total number of FortiAPs into smaller groups where each daemon manages a group. The processes won't be as overloaded, and if one child daemon has an issue, it only affects that group of FortiAPs instead of all the FortiAPs managed by the FortiGate.

The number of processors you can assign varies by FortiGate model and is based on the number of FortiAPs it is allowed to manage. The maximum value you can specify in varies according to the `wireless-controller.wtp` in table size from different platforms.

wireless-controller.wtp	Maximum acd-process-count
8192	32
4096	16
512-1024	8
128-256	4
16-64	2

You can configure the following processors:

- cw_acd
- wpad_ac

Configuring multiple cw_acd processes

The `acd-process-count` option allows you to specify the number of cw_acd processes to manage FortiAPs.

To configure multiple cw_acd processes:

In this example, there are about 1300 FortiAPs managed by a FortiGate with 16 cw_acd processes to handle all the FortiAPs.

1. Set the `acd-process-count` to `0` in `wireless-controller global`:

```
config wireless-controller global
  set acd-process-count 16
end
```

2. Verify the number of FortiAPs managed per cw_acd:

```
# diagnose wireless wlac -c mpmt
acd main  process pid     : 321
acd child process count   : 16
      idx=01 pid= 321 sl=N/A                   sm=/tmp/cwAcSock_mpmt_mngr sh=

      idx=02 pid= 376 sl=/tmp/cwCwAcSocket_data sm=/tmp/cwAcSock_mpmt_data sh=

    * idx=03 pid= 377 sl=/tmp/cwCwAcSocket    sm=/tmp/cwAcSock_mpmt    sh=
                  ws_cnt=1305 1283(RUN)   86(cfg) 1189(oper)
      idx=04 pid= 401 sl=/tmp/cwCwAcSocket_1  sm=/tmp/cwAcSock_mpmt_1  sh=/tmp/hasync_
to_cw_acd_unix_sock_1  ws_cnt=80     77(RUN)    4(cfg)    70(oper)
      idx=05 pid= 402 sl=/tmp/cwCwAcSocket_2  sm=/tmp/cwAcSock_mpmt_2  sh=/tmp/hasync_
to_cw_acd_unix_sock_2  ws_cnt=78     77(RUN)    5(cfg)    72(oper)
      idx=06 pid= 403 sl=/tmp/cwCwAcSocket_3  sm=/tmp/cwAcSock_mpmt_3  sh=/tmp/hasync_
to_cw_acd_unix_sock_3  ws_cnt=91     89(RUN)    6(cfg)    83(oper)
      idx=07 pid= 404 sl=/tmp/cwCwAcSocket_4  sm=/tmp/cwAcSock_mpmt_4  sh=/tmp/hasync_
to_cw_acd_unix_sock_4  ws_cnt=93     92(RUN)    6(cfg)    84(oper)
      idx=08 pid= 405 sl=/tmp/cwCwAcSocket_5  sm=/tmp/cwAcSock_mpmt_5  sh=/tmp/hasync_
to_cw_acd_unix_sock_5  ws_cnt=92     91(RUN)    7(cfg)    84(oper)
      idx=09 pid= 406 sl=/tmp/cwCwAcSocket_6  sm=/tmp/cwAcSock_mpmt_6  sh=/tmp/hasync_
to_cw_acd_unix_sock_6  ws_cnt=92     91(RUN)   10(cfg)    81(oper)
```

```
      idx=10 pid= 407 sl=/tmp/cwCwAcSocket_7  sm=/tmp/cwAcSock_mpmt_7  sh=/tmp/hasync_
to_cw_acd_unix_sock_7  ws_cnt=78     77(RUN)    4(cfg)   73(oper)
      idx=11 pid= 408 sl=/tmp/cwCwAcSocket_8  sm=/tmp/cwAcSock_mpmt_8  sh=/tmp/hasync_
to_cw_acd_unix_sock_8  ws_cnt=76     74(RUN)    5(cfg)   69(oper)
      idx=12 pid= 409 sl=/tmp/cwCwAcSocket_9  sm=/tmp/cwAcSock_mpmt_9  sh=/tmp/hasync_
to_cw_acd_unix_sock_9  ws_cnt=82     79(RUN)    9(cfg)   70(oper)
      idx=13 pid= 410 sl=/tmp/cwCwAcSocket_10 sm=/tmp/cwAcSock_mpmt_10 sh=/tmp/hasync_
to_cw_acd_unix_sock_10 ws_cnt=76     74(RUN)    4(cfg)   70(oper)
      idx=14 pid= 411 sl=/tmp/cwCwAcSocket_11 sm=/tmp/cwAcSock_mpmt_11 sh=/tmp/hasync_
to_cw_acd_unix_sock_11 ws_cnt=80     77(RUN)    6(cfg)   70(oper)
      idx=15 pid= 412 sl=/tmp/cwCwAcSocket_12 sm=/tmp/cwAcSock_mpmt_12 sh=/tmp/hasync_
to_cw_acd_unix_sock_12 ws_cnt=78     78(RUN)    5(cfg)   72(oper)
      idx=16 pid= 413 sl=/tmp/cwCwAcSocket_13 sm=/tmp/cwAcSock_mpmt_13 sh=/tmp/hasync_
to_cw_acd_unix_sock_13 ws_cnt=76     76(RUN)    5(cfg)   71(oper)
      idx=17 pid= 414 sl=/tmp/cwCwAcSocket_14 sm=/tmp/cwAcSock_mpmt_14 sh=/tmp/hasync_
to_cw_acd_unix_sock_14 ws_cnt=78     78(RUN)    5(cfg)   73(oper)
      idx=18 pid= 415 sl=/tmp/cwCwAcSocket_15 sm=/tmp/cwAcSock_mpmt_15 sh=/tmp/hasync_
to_cw_acd_unix_sock_15 ws_cnt=76     75(RUN)    1(cfg)   74(oper)
      idx=19 pid= 416 sl=/tmp/cwCwAcSocket_16 sm=/tmp/cwAcSock_mpmt_16 sh=/tmp/hasync_
to_cw_acd_unix_sock_16 ws_cnt=79     78(RUN)    4(cfg)   73(oper)
Curr Time: 683
```

Each cw_acd process handles a small number of FortiAPs, about 90.

3. Verify the CPU used by cw_acd:

```
# diagnose system top 5 30
Run Time:  0 days, 0 hours and 11 minutes
5U, 0N, 4S, 91I, 0WA, 0HI, 0SI, 0ST; 16063T, 8236F
            csfd      340      R      87.5     1.3    8
          cw_acd      377      S      12.9     6.5    6
          flpold      336      S       1.9     0.0    1
          cu_acd      325      S       1.4     0.1    0
          cw_acd      402      S       0.9     0.9    6
          cw_acd      401      S       0.9     0.9    2
          cw_acd      412      S       0.4     1.2    8
          cw_acd      404      S       0.4     1.0    10
          cw_acd      405      S       0.4     1.0    4
          cw_acd      403      S       0.4     1.0    2
          cw_acd      409      S       0.4     0.9    4
          cw_acd      408      S       0.4     0.9    6
          cw_acd      414      S       0.4     0.9    2
          cw_acd      413      S       0.4     0.9    8
            node      275      S       0.4     0.3    4
         miglogd      295      S       0.4     0.3    10
             cid      345      S       0.4     0.2    6
         miglogd      391      S       0.4     0.2    6
         miglogd      389      S       0.4     0.2    8
       forticron      282      S       0.4     0.1    6
          flcfgd      326      S       0.4     0.1    9
      fortilinkd      324      S       0.4     0.0    0
          cw_acd      376      S       0.0     2.8    3
          cw_acd      406      S       0.0     1.0    6
          cw_acd      411      S       0.0     0.9    10
          cw_acd      416      S       0.0     0.9    8
          cw_acd      407      S       0.0     0.9    2
          cw_acd      415      S       0.0     0.9    0
```

```
          cw_acd      410      S       0.0     0.8    4
         cmdbsvr      237      S       0.0     0.7    0

# get system performance status
CPU states: 5% user 3% system 0% nice 92% idle 0% iowait 0% irq 0% softirq
CPU0 states: 6% user 4% system 0% nice 90% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 5% system 0% nice 95% idle 0% iowait 0% irq 0% softirq
CPU2 states: 2% user 2% system 0% nice 96% idle 0% iowait 0% irq 0% softirq
CPU3 states: 0% user 2% system 0% nice 98% idle 0% iowait 0% irq 0% softirq
CPU4 states: 1% user 6% system 0% nice 93% idle 0% iowait 0% irq 0% softirq
CPU5 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU6 states: 37% user 2% system 0% nice 61% idle 0% iowait 0% irq 0% softirq
CPU7 states: 1% user 0% system 0% nice 99% idle 0% iowait 0% irq 0% softirq
CPU8 states: 9% user 13% system 0% nice 78% idle 0% iowait 0% irq 0% softirq
CPU9 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU10 states: 1% user 2% system 0% nice 97% idle 0% iowait 0% irq 0% softirq
CPU11 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 16448692k total, 7867592k used (47.8%), 8208572k free (49.9%), 372528k freeable
(2.3%)
Average network usage: 1710 / 942 kbps in 1 minute, 18999 / 19647 kbps in 10 minutes,
15826 / 16285 kbps in 30 minutes
Maximal network usage: 2804 / 1473 kbps in 1 minute, 27949 / 27754 kbps in 10 minutes,
31749 / 32829 kbps in 30 minutes
Average sessions: 2864 sessions in 1 minute, 2262 sessions in 10 minutes, 1995 sessions
in 30 minutes
Maximal sessions: 2941 sessions in 1 minute, 2945 sessions in 10 minutes, 2945 sessions
in 30 minutes
Average session setup rate: 1 sessions per second in last 1 minute, 5 sessions per
second in last 10 minutes, 7 sessions per second in last 30 minutes
Maximal session setup rate: 20 sessions per second in last 1 minute, 214 sessions per
second in last 10 minutes, 278 sessions per second in last 30 minutes
Average NPU sessions: 48 sessions in last 1 minute, 45 sessions in last 10 minutes, 40
sessions in last 30 minutes
Maximal NPU sessions: 52 sessions in last 1 minute, 59 sessions in last 10 minutes, 94
sessions in last 30 minutes
Average nTurbo sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0
sessions in last 30 minutes
Maximal nTurbo sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0
sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days,  0 hours,  12 minutes
```

Each cw_acd uses about 1% of the CPU.

Configuring multiple wpad_ac processes

The `wpad-process-count` allows you to configure multiple wpad_ac processes to handle WPA authentication requests. You can set the `wpad-process-count` to a non-zero value such as 4, so the FortiGate will have four child wpad daemons where each process can handle a small group of SSIDs.

To configure multiple wpad processes:

This example uses a FGT-101F that has a maximum `wpad-process-count` of 4.

1. Set the `wpad-process-count` under `wireless-controller global`:

```
config wireless-controller global
  set wpad-process-count 4
end
```

   Note that both `wpad_ac` and `cw_acd` processes are restarted when `wpad-process-count` is configured.

2. Verify the number of child wpad daemons created:

```
# diagnose wpa wpad mp
    main process pid:      2221
    child process num:     4
            [1]:          2223
            [2]:          2225
            [3]:          2226
            [4]:          2227
```

3. Verify that VAPs with security modes of WPA-PSK, WPA-Enterprise, or radius-mac-auth are enabled and can be added to different wpad child daemons:

```
# diagnose wpa wpad vap
-------------------------   wpad[1]  -------------------------
VAP number:    2
VAP 0-10.10.24.20:35276-0-0 e0:22:ff:b2:19:30 state IDLE
    AC socket: /tmp/cwCwAcSocket_1
    Radius MAC Auth:0
    wpa version: WPA2
    preauth: 1
    ssid: FOS_101f.br1
    key_mgmt: WPA-PSK WPA-FT-PSK
    rsn_pairwise: CCMP
    rsn_group: CCMP
VAP 0-10.10.24.20:35276-1-0 e0:22:ff:b2:19:38 state IDLE
    AC socket: /tmp/cwCwAcSocket_1
    Radius MAC Auth:0
    wpa version: WPA2
    preauth: 1
    ssid: FOS_101f.br.ent
    key_mgmt: WPA-EAP WPA-FT-EAP
    rsn_pairwise: CCMP
    rsn_group: CCMP
    auth: radius, server: wifi-radius
    Radius Auth NAS-IP: 0.0.0.0
    Radius Auth NAS-ID-TYPE: legacy
    Radius Auth NAS-ID: 10.10.24.20/35276-br2
VAP number: 2              Radius VAP number: 1
-------------------------   wpad[2]  -------------------------
There is no any WPA enabled VAP!
-------------------------   wpad[3]  -------------------------
VAP number:    3
VAP 0-10.6.30.254:25246-1-0 04:d5:90:b5:d7:e7 state IDLE
    AC socket: /tmp/cwCwAcSocket_3
    Radius MAC Auth:0
    wpa version: WPA2
    preauth: 1
    ssid: FOS_101f.ssid1
    key_mgmt: WPA-PSK
```

```
    rsn_pairwise: CCMP
    rsn_group: CCMP
VAP 0-10.6.30.254:5246-0-0 00:0c:e6:de:6f:31 state IDLE
    AC socket: /tmp/cwCwAcSocket_3
    Radius MAC Auth:0
    wpa version: WPA2
    preauth: 1
    ssid: FOS_101f.br1
    key_mgmt: WPA-PSK WPA-FT-PSK
    rsn_pairwise: CCMP
    rsn_group: CCMP
VAP 0-10.6.30.254:5246-1-0 00:0c:e6:de:6f:41 state IDLE
    AC socket: /tmp/cwCwAcSocket_3
    Radius MAC Auth:0
    wpa version: WPA2
    preauth: 1
    ssid: 101f.ssid.ent
    key_mgmt: WPA-EAP
    rsn_pairwise: CCMP
    rsn_group: CCMP
    auth: radius, server: wifi-radius
    Radius Auth NAS-IP: 0.0.0.0
    Radius Auth NAS-ID-TYPE: legacy
    Radius Auth NAS-ID: 10.5.30.252/5246-101f.ssid.ent
VAP number: 3             Radius VAP number: 1
-------------------------   wpad[4]  -------------------------
There is no any WPA enabled VAP!
```

4. Connect clients to the SSIDs and verify that each wpad child daemon can handle the authentication separately.

```
# diagnose wpa wpad sta
-------------------------   wpad[1]  -------------------------
VAP number:    2
    STA=48:ee:0c:23:43:d1,   state: PTKINITDONE
-------------------------   wpad[2]  -------------------------
There is no any WPA enabled VAP!
-------------------------   wpad[3]  -------------------------
VAP number:    3
    STA=f8:e4:e3:d8:5e:af,   state: PTKINITDONE
-------------------------   wpad[4]  -------------------------
There is no any WPA enabled VAP!
```

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 directly 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 38.
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 and Switch Controller* > *SSIDs* and edit your SSID. In the *WiFi Settings* section, enable *Split Tunneling*.

Go to *WiFi 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 275), 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.

  If you want the remote wireless client to be able to communicate with internal devices at their home/remote site, clear the *Include Local Subet* checkbox in the FortiAP profile.
- **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.

  If you want the remote wireless client to be able to communicate with internal devices at their home/remote site, select the *Include Local Subnet* checkbox in the FortiAP profile.

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 and Switch Controller* > *SSIDs* 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 212.

- *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 FortiCloud 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 and 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.

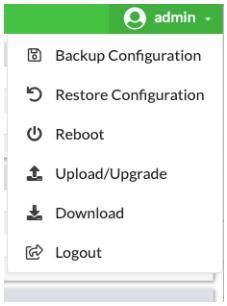
   ```
   cfg -a AC_IPADDR_1=172.20.120.142
   cfg -c
   ```
6. To log out of the FortiAP CLI, enter `exit`.

Applying configurations to multiple FortiAPs

If you have multiple FortiAPs that you need to configure, you can save a backup configuration file and use the restore function to apply these configurations to other FortiAPs. In order for this method to work, the firmware version of all your FortiAPs must match.

To apply configurations to multiple FortiAPs:

1. From your FortiAP page, in the top right corner, click to expand the *admin* menu.



2. Click *Backup Configuration* to save a configuration file.
3. Log in to the FortiAP page that you want to apply to configuration to.
4. Click to expand the *admin* menu.
5. Click *Restore Configuration* and select the configuration file you created.

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 and 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 when deploying in high-density environments.

- Upgrading the firmware for multiple FortiAPs
- Controlling the power save feature
- Configuring the broadcast packet suppression
- Converting multicast streams to unicast
- Ignoring weak or distant clients
- Turning off the 802.11b protocol
- Configuring data rates
- Enabling the automatic TX power control
- Enabling the frequency band load-balancing
- Enabling the AP load balancing
- Setting the Application Control feature
- Managing the FortiAP group and assigning a dynamic VLAN
- Sharing tunnel SSIDs within a single managed FortiAP
- Enabling the manual quarantine of devices on FortiAP (tunnel mode)
- Locating a FortiAP with LED blinking
- Uploading a FortiAP image on the wireless controller
- Configuring control message off-loading
- Enabling Dynamic Radio Mode Assignment (DRMA)
- Setting the Application Control feature
- RADIUS Change of Authorization (CoA) support on page 291

Upgrading the firmware for multiple FortiAPs

Administrators can upgrade the firmware for multiple FortiAPs; they don't need to upgrade each AP individually.

From *WiFi and Switch Controller* > *Managed FortiAPs*, you can select a FortiAP Group and right-click to select *Upgrade.* This will upgrade all the APs in that group.

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}
```

Transmit optimization options	Description
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
```

Broadcast suppression options	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.

Broadcast suppression options	Description
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.
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
```

Configuring 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 rate control on the VAP level based on the number of spatial streams. You can configure data rates on up to 8 spatial streams under the VHT (802.11ac) and HE (802.11ax) standards.

The 802.11n and ac protocols are specified by the Modulation and Coding Scheme (MCS) Index and the number of spatial streams. Enabling MCS data rate with MCS index 9 will automatically enable data rate with MCS index 8.

Data rate commands	Example
`set rates-11ac-mcs-map`	For example, mcs5/1 is converted to 7 to represent VHT-MCS 0-7 for n spatial streams:

Data rate commands	Example

`Comma separated list of max supported VHT MCS for spatial streams 1 through 8, max supported mcs option:`
`- spatial streams not supported.`
`7 support for VHT-MCS 0-7 for n spatial streams.`
`8 support for VHT-MCS 0-8 for n spatial streams.`
`9 support for VHT-MCS 0-9 for n spatial streams.`
`11 support for VHT-MCS 0-11 for n spatial streams.`
	`set rates-11ac-mcs-map "7"`

`set rates-11ax-mcs-map`
`Comma separated list of max supported HE MCS for spatial streams 1 through 8, max supported mcs option:`
`- spatial streams not supported.`
`7 support for HE-MCS 0-7 for n spatial streams.`
`9 support for HE-MCS 0-9 for n spatial streams.`
`11 support for HE-MCS 0-11 for n spatial streams.`
	For example, mcs8/2 is converted to 9 to represent HE-MCS 0-9 for n spatial streams:
	`set rates-11ax-mcs-map "9"`

To set data rates in VAP - GUI:

1. Enable Advanced Wireless Features on page 165.
2. Navigate to *WiFi & Switch Controller* > *SSIDs* and create or edit an SSID.
3. Under *Advanced Settings*, make you configurations in *Advanced rate controls* (see Advanced SSID options on page 180).

   Note that you can only configure the following data rates from the GUI:
   - 802.11a.
   - 802.11b/g.
   - 802.11n with 1 or 2 spatial streams.
   - 802.11n with 3 or 4 spatial streams.

To set data rates in VAP - CLI:

The following example configuration on a 4x4 AP shows how to set data rates for four streams where stream 5-8 are not supported. The numbers used in this example are separated by commas that correspond to MCS values in the 802.11ax and 802.11ac WiFi standards.

1. Set data rates in the wireless controller VAP.

```
config wireless-controller vap
  edit "new_rate_test"
    set ssid "newratetest"
```

```
    set security wpa-personal
    set passphrase ENC ******
    set rates-11ac-mcs-map "7,8,9,8"
    set rates-11ax-mcs-map "7,9,11,7"
  next
end
```

2. Apply the SSID to the wtp-profile.

```
config wireless-controller wtp-profile
  edit "431F_rate"
    config platform
      set type 431F
      set ddscan enable
    end
    set handoff-sta-thresh 55
    set allowaccess https ssh snmp
    config radio-1
      set band 802.11ax,n,g-only
      set vap-all manual
      set vaps "new_rate_test"
    end
    config radio-2
      set band 802.11ax-5G
      set vap-all manual
      set vaps "new_rate_test"
      set channel "108"
    end
    config radio-3
      set mode monitor
    end
  next
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 which can be set from the FortiAP profile.

1. Go to *WiFi and Switch Controller* > *FortiAP Profiles* and edit the profile for your AP model.
2. For each radio, set *Transmit power mode* to *Auto* and set the minimum and maximum range for *Transmit power* 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 and 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
      set frequency-handoff enable
   end
```

The FortiGate WiFi controller continuously scans 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.

```
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 degrades 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 and 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
      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, and is accessible only through the GUI and CLI:

To configure Handoff RSSI and threshold from the GUI, you must enable Advanced Wireless Features (see Advanced Wireless Features on page 165).

1. Once you enable Advanced Wireless Features, navigate to *WiFi & Switch Controller* > *Operation Profiles* > *FortiAP Profiles*.
2. Select the profile you want.
3. Under *Advanced Settings*, locate *Handoff RSSI* and enter the signal strength threshold.
4. In *Handoff threshold*, enter the number of clients at which AP load balancing begins.
5. When you are finished, click *OK*.

```
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* > *Firewall Policy* and edit your Firewall policy.
5. In the *Security Profiles* section, enable *Application Control* and select the security profile that you edited.
6. Click *OK*.

Managing the FortiAP group and assigning a dynamic VLAN

You can create FortiAP groups to manage multiple APs at once. Grouping an AP enables you to apply specific profile settings and assign VLANs to all the APs in that group, simplifying the administrative workload. Each AP can belong to one group only.

To create a FortiAP group, navigate to *WiFi and Switch Controller* > *Managed FortiAPs* and click *Create New* > *Managed AP Group*.

In addition, VLANs can be assigned dynamically based on FortiAP groups. Dynamic VLAN assignment allows the same SSID to be deployed to many APs, avoiding the need to produce multiple SSIDs.

1. Navigate to *WiFi and Switch Controller* > *SSIDs* to define an SSID.
2. Enable *VLAN Pooling* and select *Managed AP Group* to assign a VLAN ID to a specified group.
   You can also choose other methods of assigning VLAN IDs:

- *Round Robin*: Assigns the next VLAN ID to each device as it is detected.
- *Hash*: Always assigns the same VLAN ID to a specific device.

3. Under VLAN pooling, click *Create New* to enter the VLAN ID you want to assign and the AP group you want to apply the ID to.
4. Click *OK* to save.

Sharing tunnel SSIDs within a single managed FortiAP

This feature enables you 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)

You can only quarantine an SSID that is in 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. 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.

To enable quarantine - GUI:

1. Go to WiFi and Switch Controller > SSIDs and select the SSID.
2. Enable *Quarantine Host*.
3. Click *OK*.

To quarantine a wireless client- GUI:

1. You can quarantine a client from multiple locations:
   - Go to *Dashboard* > *WiFi* > *Clients by FortiAP*.
   - Go to *WiFi and Switch Controller* > *WiFi Clients*.
2. Select the wireless client and then click *Quarantine*.

To enable quarantine - CLI:

1. Under global quarantine settings, enable quarantine:
```
config wireless-controller vap
   edit <name>
      set quarantine {enable | disable}
   next
end
```
2. Under virtual access point (VAP) settings, enable quarantine:
```
config wireless-controller vap
   edit wifi-vap
      set ssid "Fortinet-psk"
      set security wpa2-only-personal
      set passphrase ********
      set quarantine enable
   next
end
```
3. Quarantine a wireless client. The example client has the MAC address b4:ae:2b:cb:d1:72:
```
config user quarantine
   config targets
      edit "DESKTOP-Surface"
         config macs
            edit b4:ae:2b:cb:d1:72
               set description "Surface"
            next
         end
      next
   end
end
```

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.

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
```

Locating a FortiAP with LED blinking

If you have an environment that contains numerous APs it can be difficult to locate a specific AP that you need to monitor. To help you locate specific APs, you can configure the AP lights to blink, making it easier to find.

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

1. Go to *WiFi and 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
```

Enabling Dynamic Radio Mode Assignment (DRMA)

In deployments with a high AP density, there can be redundant coverage and strong radio interference. Dynamic Radio Mode Assignment (DRMA) allows FortiAP devices to calculate the Network Coverage Factor (NCF) based on radio interference and reassign the AP mode.

When DRMA is enabled in the WTP profile or on the specific AP, the APs run in automatic mode. The AC assigns the radio mode to the APs based on the DRMA NCF value that is calculated at each configured interval.

The NCF value is calculated based on overlapping coverage in a radio coverage area. If a radio is determined to be redundant based on the configured NCF threshold, then it switches from AP mode to monitor mode. When the NCF is next calculated, if the value is below the threshold then the radio switches back to AP mode.

To configure the DRMA interval:

```
config wireless-controller timers
```

```
   set drma-interval <integer>
end
```

drma-interval	Dynamic radio mode assignment (DRMA) schedule interval, in minutes (1 - 1440, default = 60).

To configure DRMA in a WTP profile:

```
config wireless-controller wtp-profile
   edit <profile>
      config <2.4Ghz radio>
         set drma enable
         set drma-sensitivity {low | medium | high}
      end
   next
end
```

DRMA is disabled by default. The sensitivity options are:

low	Consider a radio as redundant when its NCF is 100% (default).
medium	Consider a radio as redundant when its NCF is 95%.
high	Consider a radio as redundant when its NCF is 90%.

To manually configure DRMA on a specific AP device:

```
config wireless-controller wtp
   edit <id>
      config <2.4Ghz radio>
         set drma-manual-mode {ap | monitor | ncf | ncf-peek}
      end
   next
end
```

Manual mode options include:

ap	Set the radio to AP mode.
monitor	Set the radio to monitor mode.
ncf	Select and set the radio mode based on the NCF score (default).
ncf-peek	Select the radio mode based on the NCF score, but do not apply it.

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
```

Wireless network protection

This section includes the following topics:

- Wireless Intrusion Detection System on page 293
- WiFi data channel encryption on page 295
- Protected Management Frames and Opportunistic Key Caching support on page 296
- Preventing local bridge traffic from reaching the LAN on page 297
- FortiAP-S and FortiAP-U bridge mode security profiles on page 297
- DHCP snooping and option-82 data insertion on page 298
- DHCP address enforcement on page 299
- Disabling FortiAP port access on page 299
- Suppressing phishing SSID on page 300

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 WIDS by enabling and selecting a WIDS Profile on a designated radio from a FortiAP profile.

To create a WIDS Profile - GUI:

1. Go to *WiFi and Switch Controller* > *WIDS Profiles*.
2. Select a profile to edit or select *Create New*.
3. Under *Intrusion Detection Settings*, enable the intrusion types you want protect against.
4. When you are finished, click *OK*.

   Once you create a WIDS profile, you can enable WIDS Profile on a specified radio under a FortiAP profile.

To create a WIDS Profile - CLI:

```
config wireless-controller wids-profile
  edit "example-wids-profile"
    set ap-scan enable
    ...
  next
end
```

To apply a WIDS Profile to a FortiAP - CLI:

```
config wireless-controller wtp-profile
  edit "example-FAP-profile"
    config platform
      set type <FAP-model-number>
    end
    set handoff-sta-thresh 55
    set ap-country US
    config radio-1
      set band 802.11n
      set wids-profile "example-wids-profile"
      set vap-all disable
    end
    config radio-2
      set band 802.11ac
      set vap-all disable
    end
  next
end
```

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 304.

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 configure data channel encryption from a FortiAP profile. For more information about encryption options, see Data channel security: clear-text, DTLS, and IPsec VPN on page 30

To enable encryption - CLI:

In the CLI, the `wireless wtp-profile` command contains a `dtls-policy` field, with the following options

- `clear-text` (non-encrypted)
- `dtls-enabled`
- `ipsec-vpn`
- `ipsec-vpn-sn`

To enable encryption in profile1 for example, enter:

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

To enable encryption - GUI:

To configure encryption from the GUI, you must enable Advanced Wireless Features (see Advanced Wireless Features on page 165).

1. Once you enable Advanced Wireless Features, navigate to *WiFi & Switch Controller* > *Operation Profiles* > *FortiAP Profiles*.
2. Select the profile you want to enable encryption on.
3. Under *Advanced Settings*, select the *DTLS policy* you want to apply to the profile.
4. When you are finished, click *OK*.

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`', '`ipsec`', '`ipsec-sn`, 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.

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 and FortiAP-U bridge mode security profiles

If a bridge mode SSID is configured for a managed FortiAP-S or FortiAP-U, you can add security profiles 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 profiles - GUI:

1. Go to *System* > *Feature Visibility* to enable the Security Features you want to apply to your SSID, and then click *Apply*.

   You can enable the AntiVirus, Application Control, Intrusion Prevention, and Web Filter features.
2. Go to *WiFi and Switch Controller* > *SSIDs* and select the bridge mode SSID assigned to the FortiAP Profile that you want to configure.
3. In the selected SSID, enable *Security Profiles* option.
4. Enable the security profiles you want to apply to the SSID. You can choose from *AntiVirus*, *Web Filter*, *Application Control*, and *Intrusion Prevention*.

   You can either use or edit an existing default profile, or click *Create* to make a new one. To see what each default profile does, hover your mouse over the profile for a brief description.
5. In the *Scan Botnets* field, select if you want to *Block* or *Monitor* botnets.

Botnet scanning is enabled by default. To disable this feature, select *Disable*.

6. Enable or disable *Logging*.
7. Click *OK* to save your SSID changes.

   Once you save your changes, you can check to the SSID page to see which security profiles are attached to an SSID in the Security Profiles column.

Configure security profiles - CLI:

You can configure security profiles on managed FortiAP-S and FortiAP-U under `config wireless-controller vap`, after `local-bridging` and `utm-status` are set to `enable`.

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

```
config wireless-controller vap
   edit "utm_ssid1"
      set ssid "utm_ssid1"
      set local-bridging enable
      set utm-status enable
      set ips-sensor "wifi-default"
      set application-list "wifi-default"
      set antivirus-profile "wifi-default"
      set webfilter-profile "wifi-default"
      set scan-botnet-connections monitor
   next
end
```

Debug configurations:

To debug `wireless-controller` configurations related to security profiles, 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. This feature adds the Circuit ID and Remote ID sub-option onto the DHCP packets, which helps the user identify which FortiAP makes the request and for which SSID it requests.

Syntax

```
config wireless-controll vap
   edit wifi
      set dhcp-option82-insertion {enable | disable}
      set dhcp-option82-circuit-id-insertion {style-1 | style-2 | Style-3 | disable}
      set dhcp-option82-remote-id-insertion {style-1 | disable}
   next
end
```

The `circuit-id` option includes information specific to the cirtcuit the request came from. This option is an identifier that identifies the FortiAP.

The `remote-id` option includes information on the remote host end of the circuit. This option usually contains information that identifies the station.

Options	Description
Circuit-ID style-1	An ASCII string composed of AP-MAC;SSID;SSID-TYPE
Circuit-ID style-2	An ASCII string composed of AP-MAC
Circuit-ID Style-3	An ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC
Remote-ID Style-1	An ASCII string composed of the Station-MAC

This feature is only supported in Bridge mode, Tunnel mode, and Mesh SSIDs.

DHCP address enforcement

DHCP address enforcement ensures that clients who connect must complete the DHCP process to obtain an IP address. Otherwise they are disconnected from the SSID. This prevents access from users using static addresses which may conflict with the DHCP address scheme, or users that fail to obtain DHCP IP assignment.

To configure DHCP address enforcement:

```
config wireless-controller vap
   edit "test-tunnel"
      set ssid "test-tunnel"
      set passphrase ********
      set schedule "always"
      set dhcp-address-enforcement enable
   next
end
```

By default, `dhcp-address-enforcement` is set to `disabled`.

Disabling FortiAP port access

If your FortiAP is located in an easily accessible location, you can disable the serial console port and USB port to prevent intruders from physically accessing the FortiAP.

To disable console login:

```
config wireless-controller wtp-profile
   edit <profile>
      set console-login disable
   next
end
```

By default, console login is enabled in WTP profiles.

When the console access is changed, all managed FortiAPs using the profile are rebooted.

You can confirm console login is disabled by logging into the FortiAP with the SSH connection.

```
FortiAP-433F # wcfg | grep console-login
   console-login : disabled
```

To disable the USB port:

```
config wireless-controller wtp-profile
  edit <profile>
    set usb-port disable
  next
end
```

The USB port can be disabled when the FortiAP input power mode status is `full`.

Use `cw_diag power` to check the power mode status.

You can confirm the USB port is disabled with the following diagnostics command:

```
diag wireless-controller wlac -c wtp FP433GTY22002014 | grep usb
    usb port : disabled(enabled from AC)
    usb port oper : disabled
```

Suppressing phishing SSID

You can enable FortiAPs to log and suppress phishing SSIDs. Phishing SSIDs are defined as:

- An SSID defined on FortiGate that is broadcast from an uncontrolled AP.
- A pre-defined pattern for an offending SSID pattern. For example, you can define any SSID that contains your company name to be a phishing SSID.

To configure phishing SSID functions:

```
config wireless-controller setting
     set phishing-ssid-detect enable|disable
     set fake-ssid-action log|suppress
     config offending-ssid
        edit 1
           set ssid-pattern "OFFENDING*"
           set action log|suppress
```

```
        next
    end
end
```

`set phishing-ssid-detect enable|disable`	Enable or disable the phishing SSID detection function. The default is `enable`.
`set fake-ssid-action log|suppress`	Specify the FortiGate action after detecting a fake SSID. The default is `log` and can be set to either one or both.
`set ssid-pattern "OFFENDING*"`	Specify the criteria to match an offending SSID. This example shows all SSID names with a leading string `OFFENDING` (not case-sensitive).
`set action log|suppress`	Specify the FortiGate action after detecting the offending SSID pattern entry. The default setting is `log` and can be set to either one or both.

Log examples

WiFi event log sample for fake SSID detection

The following is a sample of the log that is generated when a fake SSID is first detected:

```
1: date=2019-03-01 time=14:53:23 logid="0104043567" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480803 logdesc="Fake AP detected" ssid="CORP_
     WIFI_ACCESS" bssid="08:5b:0e:18:1b:d0" aptype=0 rate=130 radioband="802.11n-5G"
     channel=149 action="fake-ap-detected" manuf="Fortinet, Inc." security="WPA2 Personal"
     encryption="AES" signal=-41 noise=-95 live=173397 age=0 onwire="no"
     detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="FP321C3X15001615"
     radioiddetected=1 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
     msg="Detected Fake AP CORP_WIFI_ACCESS 08:5b:0e:18:1b:d0 chan 149 live 173397 age 0"
```

The following is a sample of the log that is periodically generated when a fake SSID is continuously detected:

```
1: date=2019-03-01 time=14:58:53 logid="0104043568" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551481133 logdesc="Fake AP on air" ssid="CORP_
     WIFI_ACCESS" bssid="08:5b:0e:18:1b:d0" aptype=0 rate=130 radioband="802.11n-5G"
     channel=149 action="fake-ap-on-air" manuf="Fortinet, Inc." security="WPA2 Personal"
     encryption="AES" signal=-41 noise=-95 live=173728 age=330 onwire="no"
     detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A" radioiddetected=0
     stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0 msg="Fake AP On-
     air CORP_WIFI_ACCESS 08:5b:0e:18:1b:d0 chan 149 live 173728 age 330"
```

WiFi event log sample for fake SSID suppression

The following is a sample of the log that is generated when a fake SSID is suppressed:

```
1: date=2019-03-01 time=14:53:23 logid="0104043569" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480803 logdesc="Rogue AP suppressed"
     ssid="CORP_WIFI_ACCESS" bssid="08:5b:0e:18:1b:d0" aptype=0 rate=130
     radioband="802.11n-5G" channel=149 action="rogue-ap-suppressed" manuf="Fortinet, Inc."
     security="WPA2 Personal" encryption="AES" signal=-41 noise=-95 live=173397 age=0
     onwire="no" detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A"
     radioiddetected=0 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
     msg="AP CORP_WIFI_ACCESS 08:5b:0e:18:1b:d0 chan 149 live 173397 age 0"
```

WiFi event log sample for offending SSID detection

The following a sample of the log that is generated when an offending SSID is first detected:

```
1: date=2019-03-01 time=14:53:33 logid="0104043619" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480811 logdesc="Offending AP detected"
     ssid="OFFENDING_SSID" bssid="1a:5b:0e:b5:f3:bf" aptype=0 rate=130 radioband="802.11n-
     5G" channel=153 action="offending-ap-detected" manuf="Fortinet, Inc." security="WPA2
     Personal" encryption="AES" signal=-41 noise=-95 live=173406 age=8 onwire="no"
     detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="FP321C3X15001615"
     radioiddetected=1 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
     msg="Detected Offending AP OFFENDING_SSID 1a:5b:0e:b5:f3:bf chan 153 live 173406 age
     8"
```

The following is a sample of a log that is periodically generated when an offending SSID is continuously detected:

```
1: date=2019-03-01 time=14:55:54 logid="0104043620" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480952 logdesc="Offending AP on air"
     ssid="OFFENDING_SSID_TEST" bssid="9a:5b:0e:18:1b:d0" aptype=0 rate=130
     radioband="802.11n-5G" channel=149 action="offending-ap-on-air" manuf="N/A"
     security="WPA2 Personal" encryption="AES" signal=-41 noise=-95 live=173548 age=150
     onwire="no" detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A"
     radioiddetected=0 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
     msg="Offending AP On-air OFFENDING_SSID_TEST 9a:5b:0e:18:1b:d0 chan 149 live 173548
     age 150"
```

WiFi event log sample for offending SSID suppression

The following is a sample of the log that is generated when an offending SSID is suppressed:

```
1: date=2019-03-01 time=14:53:33 logid="0104043569" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480811 logdesc="Rogue AP suppressed"
     ssid="OFFENDING_SSID" bssid="1a:5b:0e:b5:f3:bf" aptype=0 rate=130 radioband="802.11n-
     5G" channel=153 action="rogue-ap-suppressed" manuf="Fortinet, Inc." security="WPA2
     Personal" encryption="AES" signal=-41 noise=-95 live=173406 age=8 onwire="no"
     detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A" radioiddetected=0
     stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0 msg="AP OFFENDING_
     SSID 1a:5b:0e:b5:f3:bf chan 153 live 173406 age 8"
```

Wireless network monitoring

This section includes topics related to monitoring your wireless network.

- Monitoring wireless health and clients on page 303
- Monitoring rogue APs on page 304
- Suppressing rogue APs on page 308
- Monitoring wireless clients on page 309
- Monitoring application usage for clients connected to bridge mode SSIDs on page 317
- Monitoring FortiAP with SNMP on page 322
- Monitoring FortiAP temperatures on page 325
- Enabling spectrum analysis on page 326
- Disable dedicated scanning on FortiAP F-Series profiles on page 332
- Enabling AP scan channel lists to optimize foreground scanning on page 335
- Optimizing memory storage by limiting monitoring data on page 338

Monitoring wireless health and clients

You can see an overview of your FortiGate or FortiWiFi unit by navigating to *Dashboard* > *WiFi*. The WiFi dashboard provides a comprehensive view of the health of your network's wireless infrastructure.

The following widgets are displayed on the dashboard:

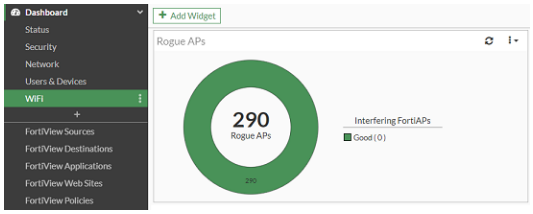
Dashboard widget	Description
Channel Utilization	Monitor FortiAPs per radio channel utilization.
Clients By FortiAP	Monitor the number of clients per FortiAP.
FortiAP Status	Monitor FortiAP status.
Historical Clients	Real-time number of WiFi clients over the selected time frame.
Interfering APs	Monitor FortiAPs that are reporting interfering APs.
Login Failures	Monitor WiFi login failures.
Rogue APs	Monitor rogue APs.
Signal Strength	Monitor the signal strength of WiFi clients.

To add a new widget, click + *Add Widget* and select from a list of predefined widget categories.

Monitoring rogue APs

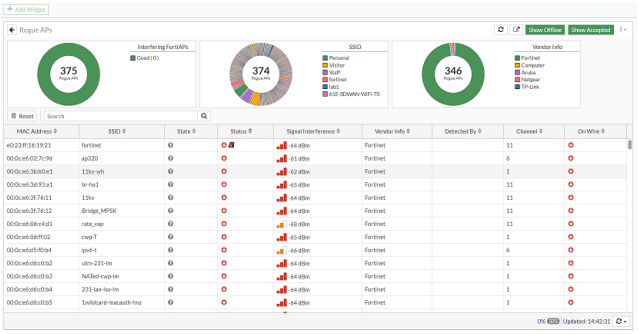
The access point radio equipment can scan for other available access points, either as a dedicated monitor or in idle periods during AP operation.

To see all the rogue APs detected by your managed FortiAP or FortiWiFi unit, go to *Dashboard* > *WiFi* > *Rogue APs*.



The Rogue AP widget shows three charts containing rogue AP statistic information in different categories.

- The Interfering FortiAPs chart shows the amount of rogue APs detected by each managed FortiAP unit or FortiWiFi local radio.
- The SSID chart shows the amount of SSID names detected as rogue APs.
- The Vendor Info chart shows the vender information of the detected rogue APs.



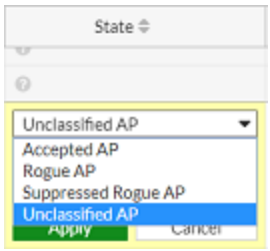
All the rogue APs are listed in a table, where you can mark each one as either Accepted or Rogue access points. You can click the *Show Offline* or *Show Accepted* button to toggle views for seeing offline rogue APs and accepted rogue APs.

Column Name	Description
MAC Address	The MAC address of the Wireless interface.
SSID	The wireless service set identifier (SSID) or network name for the wireless interface.
State	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*. Rogue AP — Use this status for unauthorized APs that the *On-wire* status indicates are attached to your wired networks. Suppressed Rogue AP — Use this status to suppress unauthorized APs. 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.

Column Name	Description
Online Status	Active AP Inactive AP Active ad-hoc WiFi device Inactive ad-hoc WiFi device
Signal Interference	The relative signal strength of the AP. Hover over the symbol to view the signal-to-noise ratio.
Vendor Info	The name of the vendor.
Detected By	The name or serial number of the AP unit that detected the signal.
Channel	The wireless radio channel that the access point uses.
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.
Security Type	The type of security currently being used.
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.

Changing a rogue AP state

1. In the table of rogue APs, select the AP you want and hover over the *State* column until an *Edit* icon appears
2. Click the *Edit* icon and select a state from the drop-down list.



3. Click *Apply*.

You can use this to suppress rogue APs, see Suppressing rogue APs on page 308.

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 APs* widget 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 and 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*.
   You can then apply the WIDS profile to a FortiAP profile.

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

1. Create a WIDS profile:
```
config wireless-controller wids-profile
   edit "example-wids-profile"
      set ap-scan enable
      set rogue-scan enable
   end
```
2. Select the WIDS profile for the managed FortiAP:
```
config wireless-controller wtp-profile
   edit "example-FAP-profile"
      config platform
         set type <FAP-model-number>
      end
      set handoff-sta-thresh 55
      set ap-country US
      config radio-1
         set band 802.11n
         set wids-profile "example-wids-profile"
         set vap-all disable
      end
      config radio-2
         set band 802.11ac
```

```
            set vap-all disable
        end
    next
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 and Switch Controller* > *WIDS Profiles*.
2. Create a new WIDS profile and disable *Rogue AP detection*.
3. Go to *WiFi and 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
```

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 307). The monitoring radio must be in the Dedicated Monitor mode.

To activate AP suppression against a rogue AP:

1. Go to *Dashboard* > *WiFi* > *Rogue APs*.
2. In the table of rogue APs, select the AP you want to suppress and hover your mouse over the *State* column.
3. Click the *Edit* icon and select *Suppressed Rogue AP*.
4. Click *Apply*.

To deactivate AP suppression:

1. Go to *Dashboard* > *WiFi* > *Rogue APs*.
2. In the table of rogue APs, select the AP you want to suppress and hover your mouse over the *State* column.
3. Click the *Edit* icon and select another state.
4. Click *Apply*.

You can change the state of multiple APs by selecting multiple rows.

To activate AP suppression against a rogue AP - CLI:

```
config wireless-controller ap-status
  edit 1
    set bssid 90:6c:ac:da:a7:f1
    set ssid "example-SSID"
    set status suppressed
  next
end
```

Monitoring wireless clients

You can view detailed information about the health of individual WiFi connections from *WiFi and Switch Controller* > *WiFi Clients*. You can also Quarantine or Disassociate a wireless client from there.

To view connected clients on a FortiGate or FortiWiFi unit:

1. Go to *WiFi and Switch Controller* > *WiFi Clients*.
   The following information is displayed by default on both the FortiGate and FortiWiFi units:

Column headers	Description
Association Time	How long the client has been connected to this access point.
Bandwidth Tx/Rx	Client received and transmitted bandwidth, in Kbps.
Channel	WiFi radio channel in use.
Device	The name of the device.
FortiAP	The serial number of the FortiAP unit to which the client connected.

Column headers	Description
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.
Signal Strength	The current signal strength and health.
Signal Strength / Noise	The signal-to-noise ratio in decibels calculated from signal strength and noise level.
SSID	The SSID that the client is connected to.
User	The user name associated with the device.

You can hover over the columns and click the Settings icon to add more columns to the table.

You can also click each row and drill down for a summary about the applications, destinations, policies, and logs on each client. From the summary page, you can also choose to Quarantine or Disassociate the host.

To quarantine the host:

You can block a specific host for your network by quarantining it.

1. From the WiFi Clients page, double-click the client you want to quarantine.
   The client summary page loads.
2. Click *Quarantine* to open the Quarantine Host dialog.
3. Click *OK* to quarantine the selected wireless client, and close the dialog.

To disassociate a host:

You can remove a specific host from your network by disassociating it.

1. From the WiFi Clients page, double-click the client you want to disassociate.
   The client summary page loads.
2. Click *Disassociate*.
   The Confirm dialog opens.
3. Click *OK* to disassociate the selected wireless client, and close the dialog.

Understanding client health

From the summary page, the Health section displays the overall health for the wireless connection. The overall health of the connection is:

- **Good** if the value range for all three conditions are Good
- **Fair** or Poor if one of the three conditions is Fair or Poor.

Condition	Value Range
Signal Strength	• **Good** > -56dBm

Condition	Value Range
	• -56dBm > **Fair** > -75dBm • **Poor** < -75dBm
Signal Strength/Noise	• **Good** > 39dBm • 20dBm < **Fair** < 39dBm • **Poor** < 20dBm
Band	• **Good** = 5G band • **Fair** = 2.4G band

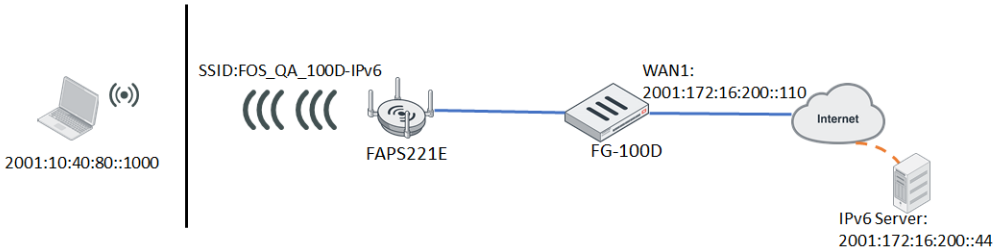
Monitoring wireless clients over IPv6 traffic

Wireless client IPv6 traffic is supported from both tunnel and local bridge mode SSID in FortiOS. To configure and monitor wireless clients on IPv6:

- Tunnel mode SSID IPv6 traffic on page 311
- Local bridge mode SSID IPv6 traffic on page 313
- CLI commands for IPv6 rules on page 316

Tunnel mode SSID IPv6 traffic

In the following example, FortiAP S221E is managed by FortiGate 100D and broadcasts tunnel mode SSID:FOS_QA_100D-IPv6.



To configure a WiFi client accessing IPv6 tunnel mode traffic:

1. In FortiOS, create a tunnel mode VAP:

```
config wireless-controller vap
    edit "wifi4"
        set ssid "FOS_QA_100D-IPv6"
        set passphrase ********
        set schedule "always"
    next
end
```

2. Create an IPv6 address for the VAP with DHCP enabled:

```
config system interface
    edit "wifi4"
        set vdom "vdom1"
        set ip 10.40.80.1 255.255.255.0
        set allowaccess ping https http
        set type vap-switch
        set alias "vdom1:"
        set device-identification enable
        set role lan
        set snmp-index 36
        config ipv6
            set ip6-address 2001:10:40:80::1/64
            set ip6-allowaccess ping https http
            set ip6-send-adv enable
            set ip6-manage-flag enable
            set ip6-other-flag enable
        end
    next
end

config system dhcp6 server
    edit 1
        set subnet 2001:10:40:80::/64
        set interface "wifi4"
        config ip-range
            edit 1
                set start-ip 2001:10:40:80::1000
                set end-ip 2001:10:40:80::1100
            next
        end
    next
end
```

3. Create an IPv6 policy from the VAP to WAN1:

```
config firewall policy6
    edit 1
        set name "ipv6"
        set srcintf "wifi4"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end
```

4. Verify the IPv6 address in the station list:
   a. In the FortiGate CLI:

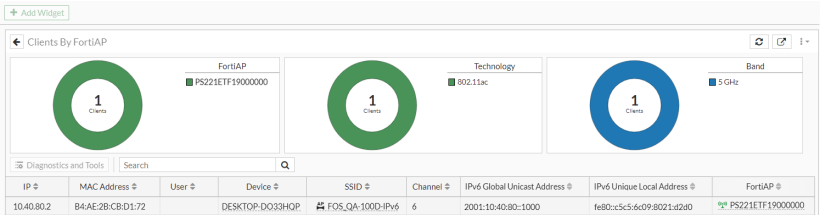
```
# diagnose wireless-controller wlac -d sta online
   vf=4 wtp=3 rId=1 wlan=wifi4 vlan_id=0 ip=10.40.80.2 ip6=2001:10:40:80::1000
mac=b4:ae:2b:cb:d1:72 vci=MSFT 5.0 host=DESKTOP-DO33HQP user= group= signal=-29
```

```
noise=-93 idle=1 bw=48 use=5 chan=6 radio_type=11N security=wpa2_only_personal
mpsk=default encrypt=aes cp_authed=no online=yes mimo=2
                ip6=fe80::c5c5:6c09:8021:d2d0,88, *2001:10:40:80::1000,8,
```

b. In the FortiAP CLI:

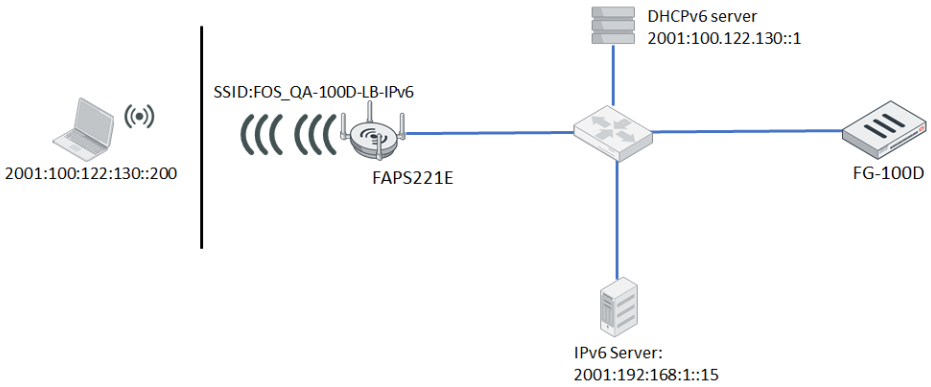
```
FortiAP-S221E # sta
wlan00 (FOS_QA_100D-IPv6) client count 1
    MAC:b4:ae:2b:cb:d1:72 ip:10.40.80.2 ip_proto:dhcp ip_age:84 host:DESKTOP-DO33HQP
vci:MSFT 5.0
                          ip6:fe80::c5c5:6c09:8021:d2d0 ip6_proto:arp ip6_age:2 ip6_
rx:101
                          ip6:2001:10:40:80::1000 ip6_proto:dhcp ip6_age:82 ip6_rx:20
        vlanid:0 Auth:Yes channel:6 rate:130Mbps rssi:65dB idle:0s
        Rx bytes:256951 Tx bytes:53947 Rx rate:130Mbps Tx rate:130Mbps Rx last:0s Tx
last:0s
        AssocID:1 Mode:  Normal Flags:f PauseCnt:0
        KEY type=aes_ccm pad=0 keyix=65535 keylen=16 flags=3(xmit recv) RSC=0 TSC=0
            e7 6f 05 ce   06 e1 4a 9b   3a d4 4f 43   1f 57 bb 49
            00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00
            00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00
        KEY type=aes_ccm pad=0 keyix=1 keylen=16 flags=83(xmit recv dflt) RSC=0 TSC=0
            01 47 6f 21   9b ac 73 4b   7c ae 07 66   7e 5a c6 7e
            00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00
            00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00
FortiAP-S221E #

FortiAP-S221E # usta

WTP daemon STA info:

  1/1   b4:ae:2b:cb:d1:72 00:00:00:00:00:00 vId=0    type=wl----sta,  vap=wlan00,FOS_
QA_100D-IPv6(0) mpsk=default  ip=10.40.80.2/1  host=DESKTOP-DO33HQP vci=MSFT 5.0
os=Windows
                          ip6=fe80::c5c5:6c09:8021:d2d0/2 rx=101
                          ip6=2001:10:40:80::1000/1 rx=21
                          replycount=0000000000000002

Total STAs: 1
```

c. In the FortiOS GUI, go to *WiFi and Switch Controller* > *WiFi Clients*. The address is displayed in the *IPv6 Global Unicast Address* and *IPv6 Unique Local Address* columns.



Local bridge mode SSID IPv6 traffic

In the following example, FortiAP S221E is managed by FortiGate 100D through a local NATed switch and broadcasts local bridge mode SSID:FOS_QA_100D-LB-IPv6.



To configure a WiFi client accessing IPv6 local bridge mode traffic:

1. In FortiOS, create a local bridge mode VAP:

```
config wireless-controller vap
    edit "test1"
        set ssid "FOS_QA-100D-LB-IPv6"
        set passphrase ********
        set local-bridging enable
        set schedule "always"
    next
end
```

2. Create an IPv6 DHCP server for the local NATed switch (FortiWiFi 60E is used in this example):

```
config system interface
    edit "internal6"
        set vdom "vdom1"
        set ip 2.2.3.1 255.255.255.0
        set allowaccess ping https http fabric
        set type physical
        set snmp-index 18
        config ipv6
            set ip6-address 2001:100:122:130::1/64
            set ip6-allowaccess ping https http fabric
            set ip6-send-adv enable
            set ip6-manage-flag enable
            set ip6-other-flag enable
        end
    next
end

config system dhcp6 server
    edit 1
        set subnet 2001:100:122:130::/64
        set interface "internal6"
        config ip-range
            edit 1
                set start-ip 2001:100:122:130::200
                set end-ip 2001:100:122:130::300
            next
        end
```

```
    next
end
```

3. Create an IPv6 policy for the local NATed switch:

```
config firewall policy6
    edit 2
        set name "ipv6"
        set uuid 56368fc6-3268-51ea-a791-91a6ab82a109
        set srcintf "internal6"
        set dstintf "internal7"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end
```

4. Verify the IPv6 address in the station list:
   a. In the FortiGate CLI:

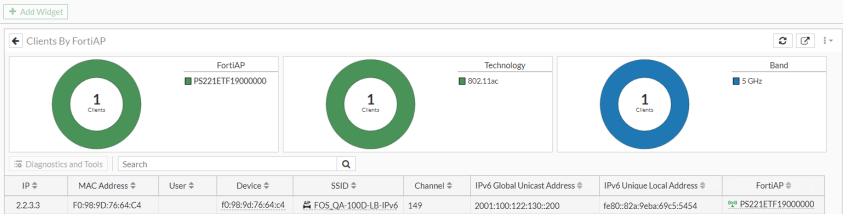
```
# diagnose wireless-controller wlac -d sta online
    vf=4 wtp=3 rId=2 wlan=test1 vlan_id=0 ip=2.2.3.3 ip6=2001:100:122:130::200
mac=f0:98:9d:76:64:c4 vci= host=iPhoneX user= group= signal=-41 noise=-105 idle=18
bw=0 use=5 chan=36 radio_type=11AC security=wpa2_only_personal mpsk=default
encrypt=aes cp_authed=no online=yes mimo=2
                ip6=fe80::82a:9eba:69c5:5454,13, *2001:100:122:130::200,2,
```

   b. In the FortiAP CLI:

```
FortiAP-S221E # sta
wlan10 (FOS_QA-100D-LB-IPv6) client count 1
    MAC:f0:98:9d:76:64:c4 ip:2.2.3.3 ip_proto:dhcp ip_age:8 host:iPhoneX vci:
                          ip6:fe80::82a:9eba:69c5:5454 ip6_proto:arp ip6_age:1 ip6_
rx:12
                          ip6:2001:100:122:130::200 ip6_proto:dhcp ip6_age:8 ip6_rx:2
        vlanid:0 Auth:Yes channel:36 rate:173Mbps rssi:64dB idle:0s
        Rx bytes:26654 Tx bytes:27949 Rx rate:78Mbps Tx rate:173Mbps Rx last:0s Tx
last:0s
        AssocID:1 Mode:  Normal Flags:1000000b PauseCnt:0
        KEY type=aes_ccm pad=0 keyix=65535 keylen=16 flags=3(xmit recv) RSC=0 TSC=0
            83 25 7e 72   d2 b1 d2 ef   30 9f 6e 9f   50 e5 6f 5a
            00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00
            00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00
        KEY type=aes_ccm pad=0 keyix=1 keylen=16 flags=83(xmit recv dflt) RSC=0 TSC=0
            1f 25 64 3e   02 4d e2 f1   2c b0 5e 03   ed 99 a4 47
            00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00
            00 00 00 00   00 00 00 00   00 00 00 00   00 00 00 00
FortiAP-S221E #

FortiAP-S221E # usta

WTP daemon STA info:

 1/1   f0:98:9d:76:64:c4 00:00:00:00:00:00 vId=0    type=wl----sta,  vap=wlan10,FOS_
```

```
QA-100D-LB-IPv6(0) mpsk=default  ip=2.2.3.3/1  host=iPhoneX vci= os=iOS
                          ip6=fe80::82a:9eba:69c5:5454/2 rx=12
                          ip6=2001:100:122:130::200/1 rx=2
                          replycount=0000000000000002

Total STAs: 1
```

c. In the FortiOS GUI, go to *WiFi and Switch Controller* > *WiFi Clients*. The address is displayed in the *IPv6 Global Unicast Address* and *IPv6 Unique Local Address* columns.



CLI commands for IPv6 rules

The following IPv6 rules can be used in VAP configurations:

Command	Description
drop-icmp6ra	Drop ICMPv6 router advertisement (RA) packets that originate from wireless clients.
drop-icmp6rs	Drop ICMPv6 router solicitation (RS) packets to be sent to wireless clients.
drop-llmnr6	Drop Link-Local Multicast Name Resolution (LLMNR) packets.
drop-icmp6mld2	Drop ICMPv6 Multicast Listener report V2 (MLD2) packets.
drop-dhcp6s	Drop DHCPv6 server generated packets that originate from wireless clients.
drop-dhcp6c	Drop DHCPv6 client generated packets to be sent to wireless clients.
ndp-proxy	Enable IPv6 NDP proxy; send back NA on behalf of the client and drop the NS.
drop-ns-dad	Drop ICMPv6 NS DAD when target address is not found in the NDP proxy cache.
drop-ns-nondad	Drop ICMPv6 NS non-DAD when target address is not found in the NDP proxy cache.

To configure IPv6 rules on a VAP in FortiOS:

```
config wireless-controller vap
    edit "wifi4"
        set ssid "FOS_QA_100D-IPv6"
        set passphrase ********
        set schedule "always"
        set ipv6-rules drop-icmp6ra drop-icmp6rs drop-llmnr6 drop-icmp6mld2 drop-dhcp6s
drop-dhcp6c ndp-proxy drop-ns-dad drop-ns-nondad
    next
end
```

The IPv6 rules settings can be pushed to a FortiAP when the VAP is broadcast.

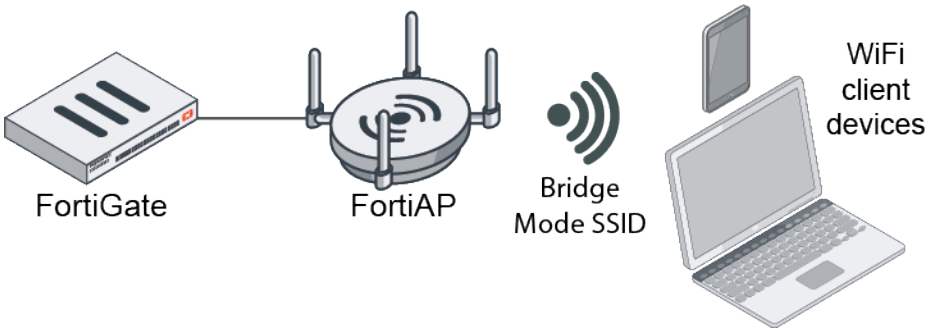
To view the pushed settings on the FortiAP:

```
FortiAP-S221E # iwpriv wlan00 get_bmcs6
wlan00    get_bmcs6:991  (0x3df)
00000001 icmp6-ra            : yes
00000002 icmp6-rs            : yes
00000004 dhcp6-server        : yes
00000008 dhcp6-client        : yes
00000010 llmnr               : yes
00000040 icmp6-mld2          : yes
00000080 ndp-proxy           : yes
00000100 ns-dad              : yes
00000200 ns-nondad           : yes
```

Monitoring application usage for clients connected to bridge mode SSIDs

FortiAPs must be running firmware version 7.2.0 and later. WiFi clients must be connected to a bridge mode SSID.

You can monitor the application usage data for clients that are connected on bridge mode IDs by using the CLI command "`diagnose wireless-controller wlac -d sta <mac-address of wireless station>`". FortiGate receives the wireless client application information from FortiAPs and analyzes the traffic information on each application.



The following CLI commands can be configured under `config wireless-controller vap`:

- `set application-detection enable | disable`: Enable or disable the reporting of wireless client application information for the bridge mode SSID that it is configured for. Application reporting is disabled by default.
- `set application-report-intv <seconds>`: Configure the time interval for the FortiAP to collect and report the application traffic information to the FortiGate. The default interval is 120 seconds.

To enable application-detection in VAP:

```
config wireless-controller vap
  edit "vap-ndpi"
    set ssid "SSID_NDPI"
    set passphrase ENC
```

```
    set local-bridging enable
    set schedule "always"
    set application-detection-engine enable
    set application-report-intv 60
  next
end
```

To check the application detection attribute from FortiAP:

```
FortiAP-231F # vcfg
-----------------------------VAP Configuration    1-----------------------------
Radio Id  1 WLAN Id  0 SSID_NDPI ADMIN_UP(INTF_UP) init_done 0.0.0.0/0.0.0.0 unknown (-1)
           vlanid=0, intf=wlan10, vap=0x3db5702c, bssid=e0:23:ff:d7:74:b0
           11ax high-efficiency=enabled target-wake-time=enabled
           bss-color-partial=enabled
           mesh backhaul=disabled
           local_auth=disabled standalone=disabled nat_mode=disabled
           local_bridging=enabled split_tunnel=disabled
           intra_ssid_priv=disabled
           mcast_enhance=disabled igmp_snooping=disabled
           mac_auth=disabled fail_through_mode=disabled sta_info=1/0
           mac=local, tunnel=8023, cap=8ce0, qos=disabled
           prob_resp_suppress=disabled
           rx sop=disabled
           sticky client remove=disabled
           mu mimo=enabled           ldpc_config=rxtx
           dhcp_option43_insertion=enabled           dhcp_option82_insertion=disabled
           dhcp_enforcement=disabled
           access_control_list=disabled
           bc_suppression=dhcp dhcp-ucast arp
           auth=WPA2, PSK, AES WPA keyIdx=1, keyLen=16, keyStatus=1, gTsc=000000000000
           key=f4cf7fd6 32dbced5 6d9fb25c 8894ad9b
           pmf=disable
           okc=disabled, dynamic_vlan=disabled, extern_roaming=disabled
           voice_ent(802.11kv)=disabled, fast_bss_trans(802.11r)=disabled mbo=disabled
           port_macauth=disable
           airfairness weight: 20%
           schedules=SMTWTFS 00:00->00:00,
           ratelimit(Kbps): ul=0 dl=0 ul_user=0 dl_user=0 burst=disabled
           primary wag:
           secondary wag:
           application detection engine: enabled, report-interval=60, configured
------------------------------Total    1 VAP Configurations----------------------------
```

To check the application detection information from FortiAP:

```
FortiAP-231F # cw_diag -d ndpi sta


Station 00:c0:ca:87:07:50 flow stats list:
--------------------------------------------------------------------------------
 AID  TX total   TX new     RX total   RX new     Application/Protocol Name
----- ---------- ---------- ---------- ---------- --------------------------
    0      992 B        0 B   3.821 KB        0 B ukn
    7   2.056 KB        0 B   1.888 KB        0 B twitter
   12      342 B        0 B       62 B        0 B icloud
```

```
   28  68.553 KB   7.416 KB  11.400 KB   3.879 KB youtube
  139   6.281 KB        0 B   1.841 KB        0 B yahoo
  609   4.847 KB        0 B   1.734 KB        0 B new-relic
  632  20.167 KB        0 B   4.310 KB        0 B google-services
  664   6.080 KB        0 B  13.842 KB        0 B microsoft-services
  728  18.324 KB        0 B  12.785 KB        0 B amazon-services
  765   2.031 MB        0 B 345.697 KB        0 B service_amazon
  768  70.786 KB  70.497 KB   7.094 KB   7.031 KB service_google
  786   3.927 KB        0 B   1.992 KB        0 B service_microsoft
  866   5.842 KB        0 B   2.656 KB        0 B spotxchange
  889      359 B        0 B       63 B        0 B goodreads
 1032      480 B      480 B       58 B       58 B imdb
 1090  23.201 KB        0 B   7.608 KB        0 B adobeanalytics
 1141   7.160 KB        0 B   2.030 KB        0 B casale
 1218   5.226 KB        0 B   2.002 KB        0 B rubiconproject
 1397   5.411 KB   5.411 KB   1.938 KB   1.938 KB exelate
 1788  25.110 KB  25.110 KB   6.503 KB   6.503 KB bing
 1838  12.417 KB  12.417 KB   2.830 KB   2.830 KB delicious
 1861   6.106 KB   6.106 KB   2.008 KB   2.008 KB pubmatic
 1968      753 B        0 B      406 B        0 B http
 1974  11.720 KB  11.375 KB   1.826 KB   1.757 KB dns
 1979 475.727 KB        0 B  66.211 KB        0 B ssl
 2012      357 B        0 B        0 B        0 B dhcp
 2182   1.033 MB        0 B 152.760 KB        0 B quic
--------------------------------------------------------------------------------
```

To check the application detection information from FortiGate:

```
# diagnose wireless-controller wlac -d sta <mac-address of wireless station>
STA:
    vf : 0
    wtp id : AP-2
    wtp index : 786
    rId : 2
    wlan : !1qcadpi
    vlan_id : 0
    ssid : !!1qcadpi-kv
    essid : !!1qcadpi-kv
    bssid : 74:78:a6:98:47:f8
    assoc time : 2024-03-13 12:01:51
    ip : 192.168.250.23
    ip6 : fe80::c01:3236:b69f:b18b
    mac : 16:8c:c6:3a:3e:32
    vci :
    host :
    user :
    group :
    signal : -26
    noise : -77
    atf val : 0%
    maxrate : 1201 Mbps
    rxrate : 216 Mbps
    rxrate_mcs : 4
    rxrate_score : 18%
    txrate : 258 Mbps
    txrate_mcs : 10
```

```
    txrate_score : 21%
    idle : 1
    bw : 209
    use : 5
    chan : 149
    radio_type : 11AX_5G
    security : WPA2_PERSONAL
    mpsk :
    encrypt : aes
    cp_authed : no
    online : yes
    mimo : 2
    handoff time : 0
  STA extension data :
    rx_bytes : 5057186
    rx_data : 26952
    rx_rate : 216 Mbps
    rx_throughput : 47.03 Kbps
    rx_dup : 0
    rx_noprivacy : 0
    rx_wepfail : 0
    rx_demicfail : 0
    rx_tkipmic : 0
    rx_ccmpmic : 0
    rx_wpimic : 0
    rx_tkipicv : 0
    rx_decap : 0
    rx_defrag : 0
    rx_decryptcrc : 0
    rx_unauth : 0
    rx_unencrypted : 0
    rx_err : 0
    tx_bytes : 119997874
    tx_frames : 94270
    tx_rate : 258 Mbps
    tx_throughput : 162.43 Kbps
    tx_discard : 0
    current tx_discard_percentage: 0%
    tx_target_discard : 0
    tx_host_discard : 0
    tx_retries : 22957
    current tx_retry_percentage: 24%
    sounding_count : 0
    explicit_compbf : off
    explicit_noncompbf : off
    implicit_bf : off
    SU Beamformer support : off
    SU Beamformee support : on
    MU Beamformer support : off
    MU Beamformee support : off
    Capabilities : WMM
    RSSI : 51 dB

    rx_ucast_bytes : 5006071
    rx_mcast_bytes : 51115
    rx_ucast_pkts : 26584
```

```
  rx_mcast_pkts : 368
  rx_decrypt_succeeds : 0
  rx_ratemcs : 0x4
  rx_pkts_retried : 8056
  rx_mic_err : 0
  rx_qos_pkts[0] : 25194
  rx_qos_bytes[0] : 0
  rx_qos_pkts[1] : 1514
  rx_qos_bytes[1] : 0
  rx_qos_pkts[2] : 35
  rx_qos_bytes[2] : 0
  rx_qos_pkts[3] : 1158
  rx_qos_bytes[3] : 0
  rx_ampdu_mpdu : 0
  tx_ucast_bytes : 119997874
  tx_mcast_bytes : 0
  tx_ucast_pkts : 94270
  tx_mcast_pkts : 0
  tx_ratemcs : 0xa
  tx_pkts_retried : 22957
  tx_qos_pkts[0] : 63962
  tx_qos_bytes[0] : 0
  tx_qos_pkts[1] : 19
  tx_qos_bytes[1] : 0
  tx_qos_pkts[2] : 17846
  tx_qos_bytes[2] : 0
  tx_qos_pkts[3] : 12574
  tx_qos_bytes[3] : 0
STA Recent Top Applications : 2024-03-13 13:58:16 (7 seconds ago)
  1. Application ID : 28 - "youtube"
      Tx Bytes : 1401807
      Rx Bytes : 42790
  2. Application ID : 12 - "icloud"
      Tx Bytes : 138353
      Rx Bytes : 66468
  3. Application ID : 139 - "yahoo"
      Tx Bytes : 38742
      Rx Bytes : 19002
  4. Application ID : 1979 - "ssl"
      Tx Bytes : 20190
      Rx Bytes : 8004
  5. Application ID : 128 - "edk"
      Tx Bytes : 1228
      Rx Bytes : 6890
  6. Application ID : 1974 - "dns"
      Tx Bytes : 2281
      Rx Bytes : 1178
  7. Application ID : 20 - "amazon-cloud"
      Tx Bytes : 1957
      Rx Bytes : 878
  8. Application ID : 768 - "service_google"
      Tx Bytes : 941
      Rx Bytes : 602
  9. Application ID : 1805 - "imrworldwide"
      Tx Bytes : 630
      Rx Bytes : 216
```

```
    10. Application ID : 1218 - "rubiconproject"
        Tx Bytes : 510
        Rx Bytes : 219
```

Monitoring FortiAP with SNMP

You can enable SNMP directly on FortiAP by implementing a SNMPD daemon/subagent on the FortiAP side.

To configure SNMP operation settings per VDOM:

```
config wireless-controller snmp
    set engine-id "fap-fortinet"
    set contact-info "user@example.com"
    set trap-high-cpu-threshold 80
    set trap-high-mem-threshold 80
    config community
        edit 1
            set name "fap-comm-1"
            set status enable
            set query-v1-status enable
            set query-v2c-status enable
            set trap-v1-status enable
            set trap-v2c-status enable
            config hosts
                edit 1
                    set ip 192.168.1.168 255.255.255.0
                next
            end
        next
    end
    config user
        edit "fap"
            set status enable
            set queries enable
            set trap-status enable
            set security-level no-auth-no-priv
            set notify-hosts 192.168.1.168
        next
    end
end
```

To allow SNMP access in FortiAP profiles or per FortiAP device:

```
config wireless-controller wtp-profile
    edit FAP423E-default
        append allowaccess snmp
    next
end
```

To disallow SNMP access in FortiAP profiles or per FortiAP device:

```
config wireless-controller wtp-profile
    edit FAP423E-default
        unselect allowaccess snmp
    next
end
```

FortiAP SNMP implementation

Simple Network Management Protocol (SNMP) queries and trap messages based on wireless-controller SNMP settings configured on FortiGate is supported on the following:

- FortiAP-S and FortiAP-W2 version 6.2.0 and later.
- FortiAP 6.4.3 and later.
- FortiAP-U 6.0.4 and later.

All SNMP versions (v1, v2, and v3) are supported.

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:

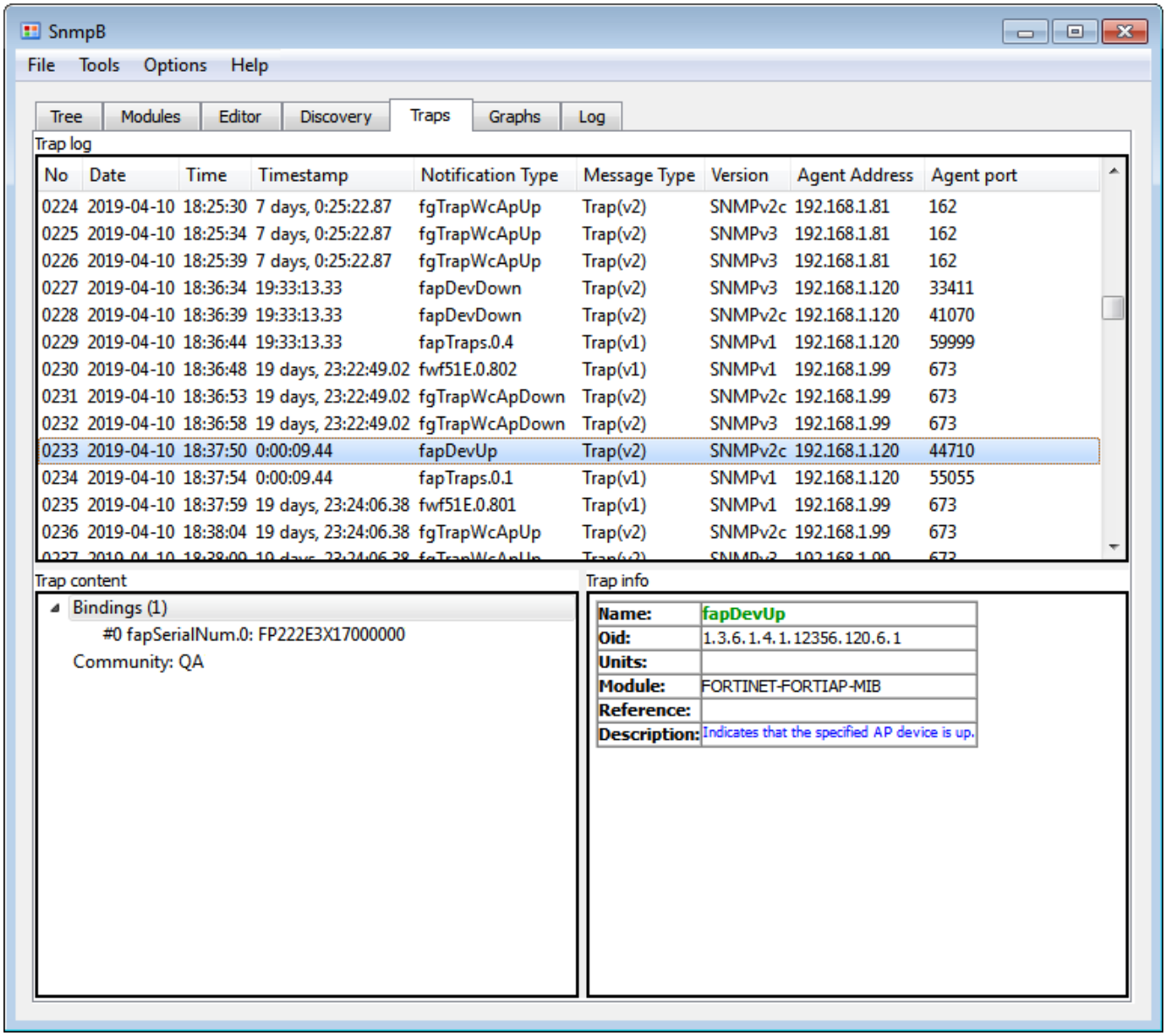
1. Go to the Fortinet Support website.
2. Log in to your account. If you do not have an account, create one and then log in.
3. From the top banner, select *Support* > *Firmware Download*.
4. From *Select Product* drop-down, select *FortiAP-S* or *FortiAP-W2*, as applicable.
5. Click the *Download* tab.
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* drop-down, select *FortiGate*.
9. Click the *Download* tab.
10. Locate the v6.00 folder (or later) and then 6.2 (or later) folder to match the firmware release running on your FortiGate device.
11. Navigate through the folders to find and then download the FORTINET-CORE-MIB-buildxxxx.mib file.
12. 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).

The following screenshot shows an SNMP trap receiver (SnmpB) that has received one `fapDevUp` trap message from a FortiAP unit (serial number: FP222E3X17000000).



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: user@example.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)
...
```

Monitoring FortiAP temperatures

You can obtain the operating temperature of FortiAP models with built-in temperature sensors.

Operating temperature measures the junction temperature of the CPU. It is not a measurement of the ambient temperature for the FortiAP.

To obtain the temperature value of a FortiAP - FortiGate:

```
# get wireless-controller wtp-status <serial number> | grep Temp
   Temperature in Celsius: 1 (52)


# diagnose wireless-controller wlac -c wtp <serial number> | grep Temp
   Temperature in Celsius: 3 (55,57,54)
```

To obtain the temperature value of a FortiAP - FortiAP:

```
# cw_diag -c temperature
   Temperature in Celsius: 3 (52,52,52)
```

Enabling spectrum analysis

Spectrum analysis is visible in the FortiOS GUI through the *Managed FortiAPs* page for select FortiAP models. Spectrum analysis can also be performed in the FortiOS CLI.

To start or stop the spectrum analysis:

```
execute wireless-controller spectral-scan <wtp-id> <radio-id > <on | off> <duration>
<channel> <report-interval>
```

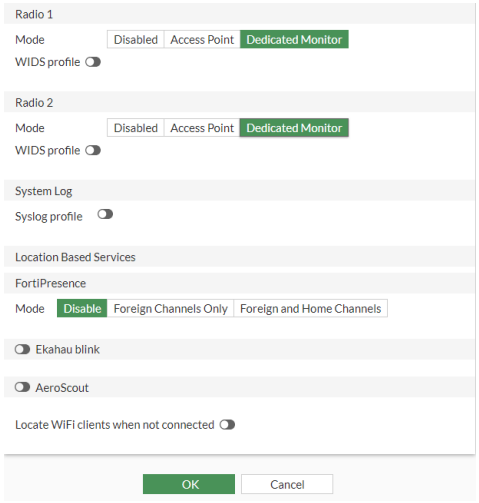
To verify the results:

```
diagnose wireless-controller wlac -c rf-sa <wtp-id> <radio-id> <channel>
```

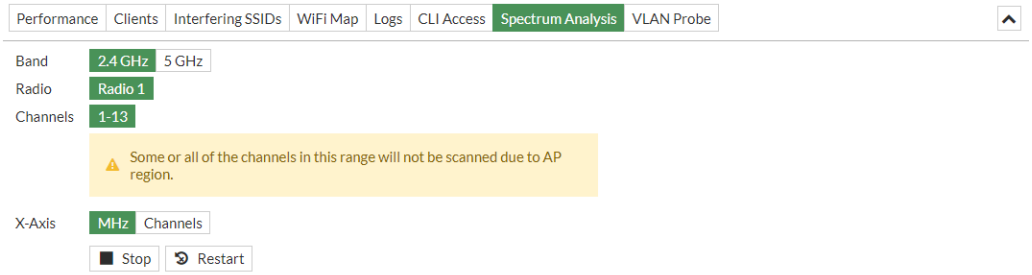
```
get wireless-controller spectral-info <wtp-id> <radio-id>
```

To view spectrum analysis in the FortiOS GUI:

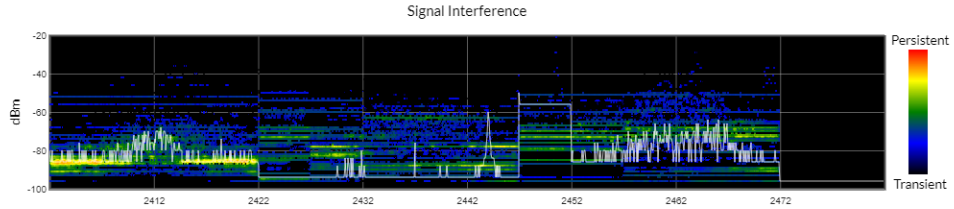
1. Change the radio mode:
   a. Go to *WiFi and Switch Controller* > *FortiAP Profiles* and double-click the FortiAP to edit the profile.
   b. In the *Radio 1* and *Radio 2* sections for *Mode*, select *Dedicated Monitor*.

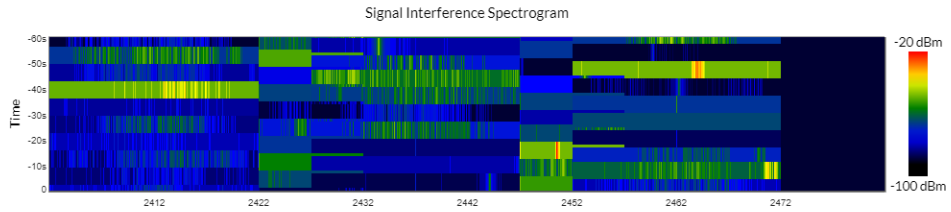


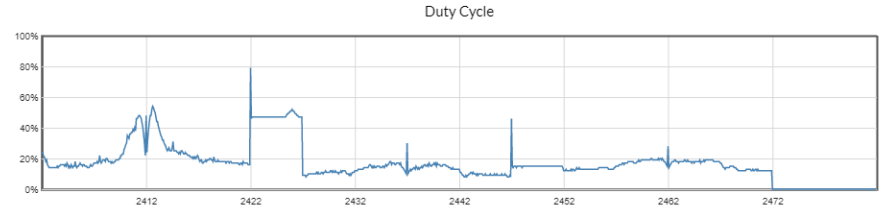
   c. Click *OK*.
2. Go to *WiFi and Switch Controller* > *Managed FortiAPs*.
3. In the table, hover over the AP so the context menu appears and click *Diagnostics and Tools*.
   The summary pane appears.
4. Click *Spectrum Analysis*.
5. Select a band frequency to view the analysis for: *Signal Interference*, *Signal Interference Spectrogram*, *Duty Cycle*, *Duty Cycle Spectrogram*, and *Detected Interference* (list).
   Analysis for 2.4 GHz:

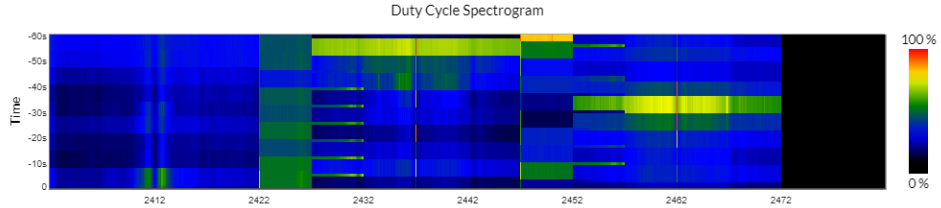


Analysis





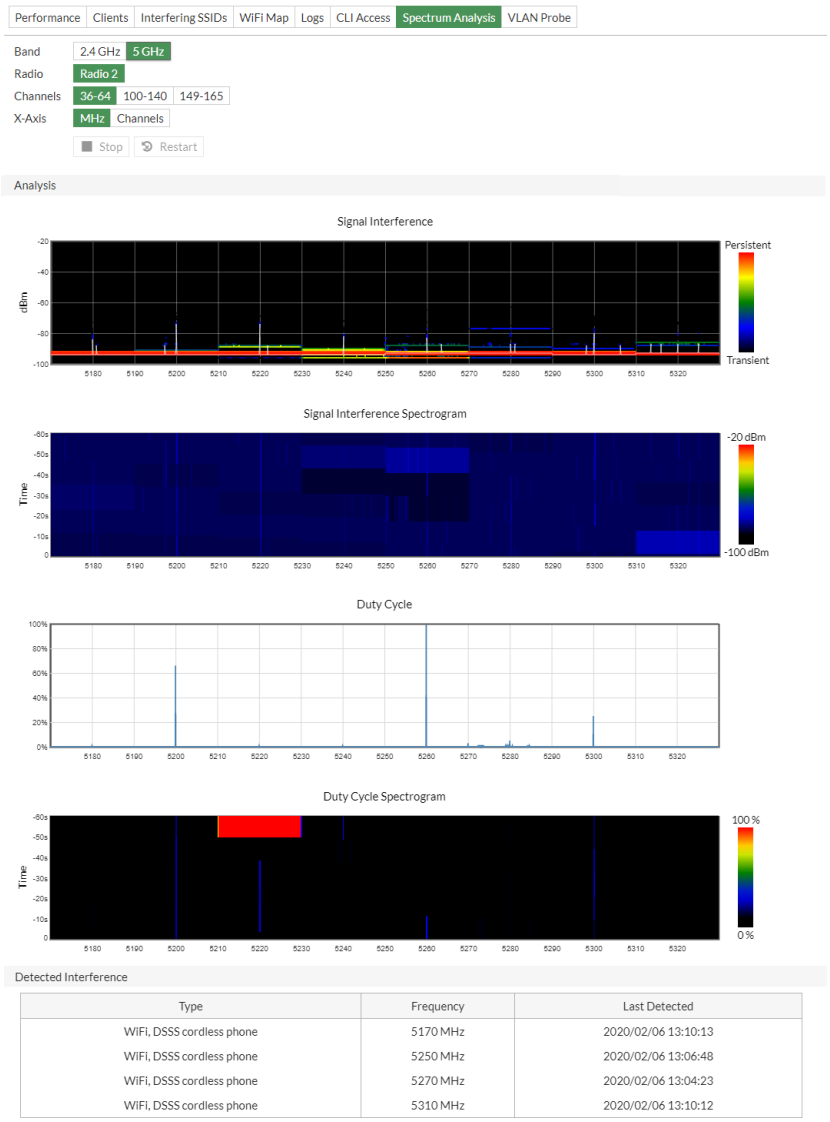




Detected Interference

Type	Frequency	Last Detected
WiFi, DSSS cordless phone	2402 MHz	2020/02/06 13:00:29
Bluetooth, FHSS cordless phone	2402 MHz	2020/02/06 12:53:43
Bluetooth, FHSS cordless phone	2412 MHz	2020/02/06 13:00:30
WiFi, DSSS cordless phone	2412 MHz	2020/02/06 13:00:30
WiFi, DSSS cordless phone	2427 MHz	2020/02/06 13:00:25
Bluetooth, FHSS cordless phone	2427 MHz	2020/02/06 12:57:26
Microwave	2437 MHz	2020/02/06 13:00:09
WiFi, DSSS cordless phone	2437 MHz	2020/02/06 13:00:27
Bluetooth, FHSS cordless phone	2437 MHz	2020/02/06 12:57:45
WiFi, DSSS cordless phone	2452 MHz	2020/02/06 13:00:28
Bluetooth, FHSS cordless phone	2452 MHz	2020/02/06 12:58:52

Analysis for 5 GHz:



Type	Frequency	Last Detected
WiFi, DSSS cordless phone	5170 MHz	2020/02/06 13:10:13
WiFi, DSSS cordless phone	5250 MHz	2020/02/06 13:06:48
WiFi, DSSS cordless phone	5270 MHz	2020/02/06 13:04:23
WiFi, DSSS cordless phone	5310 MHz	2020/02/06 13:10:12

6. Click *Close*.

To change the radio mode in the FortiOS CLI:

```
config wireless-controller wtp-profile
    edit "421E"
        config platform
            set type 421E
        end
        config radio-1
            set mode monitor
        end
        config radio-2
            set mode monitor
        end
    next
end
```

To view spectrum analysis for radio 1 in the FortiOS CLI:

1. Start the spectrum analysis on channel 1:

```
# execute wireless-controller spectral-scan FP421ETF19000000 1 on 30 1 1000
```

2. View the analysis results:

```
# diagnose wireless-controller wlac -c rf-sa FP421ETF19000000 1 1
------------------------------RF Spectrum Data    1----------------------------
rId: 1 Age: 24   gen 27     rssi: 11  nf: -96 bw: 1 Freq: 2412 Chan: 1   Cnt bin 256
Interf: 0   (idx,duty_max,duty,pwr_max,pwr)
  0  45  14   -67  -89        1  45  14   -60  -89        2  44  14   -63  -89        3
44  13   -57  -83  -
  4  44  13   -61  -89        5  43  12   -67  -89        6  43  11   -67  -89        7
42  11   -67  -89
  8  42  10   -67  -89        9  42  10   -67  -89       10  41  10   -67  -83  -    11
41  10   -67  -89
 12  41  10   -67  -89       13  42  10   -67  -89       14  41  10   -67  -83  -    15
41  10   -67  -89
 16  41  10   -61  -89       17  41  10   -67  -89       18  41  10   -67  -89       19
41  9    -67  -89
 20  41  10   -67  -89       21  41  10   -67  -89       22  41  10   -67  -89       23
42  10   -67  -79  -

# get wireless-controller spectral-info FP421ETF19000000 1
================================================================================
Spectrum info for band freq [2402, 2482] chan [1,13]: (idx,age,gen,duty_max,duty,pwr_
max,pwr)
2402      0      1      7   19   19    -21   -83    -               1      1      7   18
  18    -33   -83    -
          2      1      7   18   18    -35   -83    -               3      1      7   17
  17    -39   -83    -
          4      1      7   17   17    -43   -83    -               5      1      7   16
  16    -47   -83    -
          6      1      7   15   15    -33   -83    -               7      1      7   15
  15    -45   -83    -
          8      1      7   14   14    -59   -83    -               9      1      7   14
  14    -53   -83    -
         10      1      7   14   14    -59   -83    -              11      1      7   14
  14    -59   -83    -
```

3. Stop the spectrum analysis on radio 1:

```
# execute wireless-controller spectral-scan FP421ETF19000000 1 off
```

4. Verify the analysis has stopped:

```
# get wireless-controller spectral-info FP421ETF19000000 1
================================================================================
No spectrum info is found for band freq [2402, 2482] chan [1,13]
================================================================================
No spectrum info is found for band freq [5170, 5330] chan [36,64]
================================================================================
No spectrum info is found for band freq [5490, 5710] chan [100,140]
================================================================================
No spectrum info is found for band freq [5735, 5835] chan [149,165]
FortiGate-80E-POE # diagnose wireless-controller wlac -c rf-sa FP421ETF19000000 1 1
------------------------------Total    0 RF Spectrum Datas----------------------------
```

To view spectrum analysis for radio 2 in the FortiOS CLI:

1. Start the spectrum analysis on all channels:

```
# execute wireless-controller spectral-scan FP421ETF19000000 2 on
```

2. View the analysis results:

```
# get wireless-controller spectral-info FP421ETF19000000 2
 ================================================================================
 No spectrum info is found for band freq [2402, 2482] chan [1,13]
 ================================================================================
 Spectrum info for band freq [5170, 5330] chan [36,64]: (idx,age,gen,duty_max,duty,pwr_
max,pwr)
 5170      0     24      9   0    0     -92   -94                    1     24      9   0
   0     -92   -94
           2     24      9   0    0     -92   -94                    3     24      9   0
   0     -92   -94
           4     24      9   0    0     -92   -94                    5     24      9   0
   0     -92   -94
           6     24      9   0    0     -92   -94                    7     24      9   0
   0     -92   -94
           8     24      9   0    0     -92   -94                    9     24      9   0
   0     -92   -94
          10     24      9   0    0     -92   -94                   11     24      9   0
   0     -92   -94
          12     24      9   0    0     -92   -94                   13     24      9   0
   0     -92   -94
          14     24      9   0    0     -92   -94                   15     24      9   0
  0     -92   -94
```

3. Check the spectrum analysis results on specific channels:

```
# diagnose wireless-controller wlac -c rf-sa FP421ETF19000000 2 36
------------------------------RF Spectrum Data    1-----------------------------
rId: 2 Age: 6    gen 7      rssi: 2   nf: -96 bw: 1 Freq: 5180 Chan: 36  Cnt bin 256
Interf: 0   (idx,duty_max,duty,pwr_max,pwr)
  0  0   0    -92  -94        1  0   0    -92  -94        2  0   0    -92  -94        3
0   0    -92  -94
  4  0   0    -92  -94        5  0   0    -92  -94        6  0   0    -92  -94        7
0   0    -92  -94
  8  0   0    -92  -94        9  0   0    -92  -94       10  0   0    -92  -94       11
0   0    -92  -94
 12  0   0    -92  -94       13  0   0    -92  -94       14  0   0    -92  -94       15
0   0    -92  -94
 16  0   0    -92  -94       17  0   0    -92  -94       18  0   0    -92  -94       19
0   0    -92  -94
 20  0   0    -92  -94       21  0   0    -92  -94       22  0   0    -92  -94       23
0   0    -92  -94
 24  0   0    -92  -94       25  0   0    -92  -94       26  0   0    -92  -94       27
0   0    -92  -94
 28  0   0    -92  -94       29  0   0    -92  -94       30  0   0    -92  -94       31
0   0    -92  -94

# diagnose wireless-controller wlac -c rf-sa FP421ETF19000000 2 165
------------------------------RF Spectrum Data    1-----------------------------
rId: 2 Age: 22   gen 6      rssi: 11  nf: -96 bw: 1 Freq: 5825 Chan: 165 Cnt bin 256
Interf: 0   (idx,duty_max,duty,pwr_max,pwr)
```

```
  0  0   0    -90  -90        1  0   0    -90  -90        2  0   0    -90  -90        3
0   0    -90  -90
  4  0   0    -90  -90        5  0   0    -90  -90        6  0   0    -90  -90        7
0   0    -90  -90
  8  0   0    -90  -90        9  0   0    -90  -90       10  0   0    -90  -90       11
0   0    -90  -90
 12  0   0    -90  -90       13  0   0    -90  -90       14  0   0    -90  -90       15
0   0    -90  -90
 16  0   0    -90  -90       17  0   0    -90  -90       18  0   0    -90  -90       19
0   0    -90  -90
 20  0   0    -90  -90       21  0   0    -90  -90       22  0   0    -90  -90       23
0   0    -90  -90
 24  0   0    -90  -90       25  0   0    -90  -90       26  0   0    -90  -90       27
0   0    -90  -90
 28  0   0    -90  -90       29  0   0    -90  -90       30  0   0    -90  -90       31
0   0    -90  -90
```

4. Stop the spectrum analysis on radio 2:

```
# execute wireless-controller spectral-scan FP421ETF19000000 2 off
```

5. Verify the analysis has stopped:

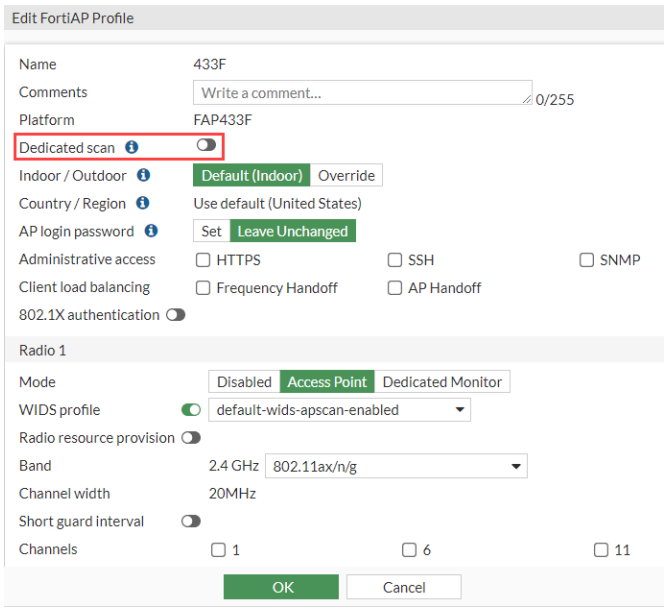
```
# get wireless-controller spectral-info FP421ETF19000000 2
================================================================================
No spectrum info is found for band freq [2402, 2482] chan [1,13]
================================================================================
No spectrum info is found for band freq [5170, 5330] chan [36,64]
================================================================================
No spectrum info is found for band freq [5490, 5710] chan [100,140]
================================================================================
No spectrum info is found for band freq [5735, 5835] chan [149,165]
```

Disable dedicated scanning on FortiAP F-Series profiles

The FortiAP F-series product family supports two radios while a third radio performs dedicated scans at all times. However, due to wireless chipset limitations on the third radio, some of the data packets cannot be scanned which may impact the detection capabilities for FortiPresence and other related solutions. You can disable dedicated scan which will allow background scanning using WIDS profile to be enabled on Radios 1 and 2.

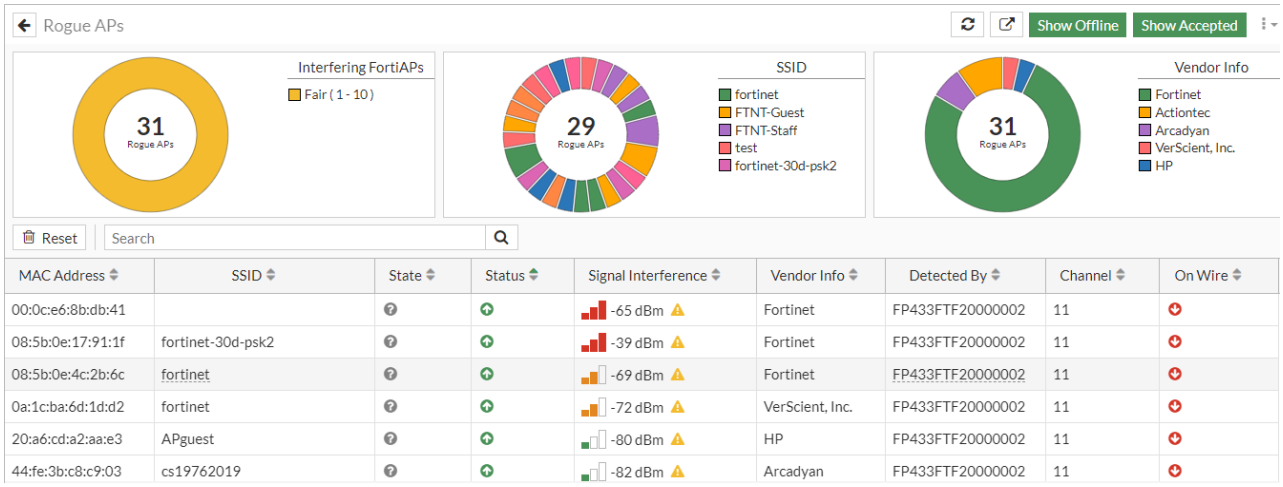
To disable dedicated scanning and enable background scanning - GUI:

1. Go to *WiFi & Switch Controller* > *FortiAP Profiles* and select the FortiAP F-series profile you want to disable dedicated scanning for.
2. Disable *Dedicated scan*.



After you disable *Dedicated scan*, the *WIDS profile* option becomes available under Radio 1 and Radio 2 configuration.

3. Set the *Mode* of the Radio to *Access Point*.
4. Enable *WIDS profile* and select a WIDS profile to perform background scanning.
5. Go to *Dashboard* > *WiFi* > *Rogue APs* to verify that the Rogue AP list is on the same channel as the Radio you configured.



To disable dedicated scanning and enable background scanning - CLI:

When you create a new FortiAP F-series profile, dedicated scanning is automatically enabled.

1. Disable dedicated scanning and assign a WIDS profile:

```
config wireless-controller wtp-profile
  edit 433F
    config platform
      set type 433F
      set ddscan disable
    end
    set handoff-sta-thresh 55
    config radio-1
      set band 802.11ax,n,g-only
      set wids-profile "default-wids-apscan-enabled"
    end
    config radio-2
      set band 802.11ax-5G
      set wids-profile "default-wids-apscan-enabled"
    end
    config radio-3
      set mode disabled
    end
  next
end
```

2. Configure the WIDS profile to enable background scan:

```
config wireless-controller wids-profile
  edit "default-wids-apscan-enabled"
    set ap-scan enable
    set ap-bgscan-period 60
    set ap-bgscan-intv 1
    set ap-bgscan-duration 20
    set ap-bgscan-idle 0
  next
end
```

3. Assign the wtp-profile to a managed FortiAP:

```
config wireless-controller wtp
  edit "FP433FTF20000002"
    set uuid e3beadf4-6fdf-51ec-d2ed-cd489ee341cb
    set admin enable
    set wtp-profile "433F"
    config radio-1
    end
    config radio-2
    end
  next
end
```

4. Check managed FortiAP Channel and background scan status:

```
FortiGate-80E-POE # diag wire wlac -c wtp FP433FTF20000002
------------------------------WTP    1----------------------------
WTP vd               : root
    vfid             : 0
    id               : FP433FTF20000002
    ...
  Radio 1            : AP
    ...
```

```
    bgscan oper    : enabled
      bgscan period  : oper 60 cfg 60
      bgscan intv    : 1
      bgscan dur     : 20
      bgscan idle    : 0
      bgscan rptintv : 30
    ...
  Radio 2            : AP
    ...
    bgscan oper    : enabled
      bgscan period  : oper 60 cfg 60
      bgscan intv    : 1
      bgscan dur     : 20
      bgscan idle    : 0
      bgscan rptintv : 30
    ...
------------------------------Total    1 WTPs-----------------------------
```

5. Check the Rogue AP list on FortiGate:

```
 FortiGate-80E-POE # diag wire wlac -c ap-rogue
CMWP AP: vf                  bssid ssid             ch  rate  sec
signal noise  age      sta mac                wtp cnt     ici    bw sgi band

UNNN AP: 0       08:5b:0e:17:91:1f fortinet-30d-... 11  130   WPA2 Personal          -
39 -95    8        00:00:00:00:00:00       1   /1    56->0    20 0  11NGHT20

 N               FP433FTF20000002 fortinet-30d-... 11  130   WPA2 Personal          -
39 -95    8        10.43.1.18:25246-0  1
UNNN AP: 0       08:5b:0e:4c:2b:6c fortinet         11  130   WPA2 Personal          -
67 -95    18       00:00:00:00:00:00       1   /1    28->0    20 0  11NGHT20

 N               FP433FTF20000002 fortinet         11  130   WPA2 Personal          -
67 -95    18       10.43.1.18:25246-0  1
...
C - Configured  (G:accept, B:rogue, S:suppress, U:unconfigured)
M - AC managed  (V:vdom, C:AC, N:unmanaged)
W - On wire     (Y:yes, N:no)
P - Phishing    (F:fake, O:offending, N:no)
Total Rogue-AP:34 Rogue-AP-WTP(displayed):34 Rogue-AP-WTP(total):34
Total Entries: 34
```

Enabling AP scan channel lists to optimize foreground scanning

You can use AP scan channel lists to optimize wireless foreground scanning by limiting the number of radio channels scanned. When DAARP, location-based services (LBS) for FortiPresence, or rogue AP monitoring are configured, you can select which channels to run a wireless foreground scan on based on frequency bands. With fewer channels to scan, the overall dwell cycle time is reduced while the frequency of the reporting interval is increased.

Under the Wireless Intrusion Detection System (WIDS) profile, use the following CLI commands to configure select channels:

```
config wireless-controller wids-profile
  edit < WIDS_profile_name >
```

```
    set ap-scan enable
    set ap-scan-channel-list-2G-5G < channel-1 > < channel-2 > ... < channel-x >
    set ap-scan-channel-list-6G < channel-1 > < channel-2 > ... < channel-y >
  next
end
```

ap-scan-channel-list-2G-5G	Add the 2.4G and 5G band AP channels you want to scan.
ap-scan-channel-list-6G	Add the 6G band AP channels you want to scan.

To create a WIDS profile to scan for specific radio channels:

1. Create a WIDS profile and add the selected channels to the appropriate AP scan channel list:

```
config wireless-controller wids-profile
  edit "wids.test"
    set sensor-mode both
    set ap-scan enable
    set ap-scan-channel-list-2G-5G "1" "6" "149" "161"
    set ap-scan-channel-list-6G "109" "201" "217"
  next
end
```

To scan specified 2.4G and 5G channels:

1. From the FortiAP profile, enable dedicated scanning and set Radio 3 to monitor mode with the WIDS profile applied.

```
config wireless-controller wtp-profile
  edit "FAP431G.ddscan"
    config platform
      set type 431G
      set ddscan enable
    end
    set handoff-sta-thresh 55
    config radio-1
      set band 802.11ax,n,g-only
    end
    config radio-2
      set band 802.11ax-5G
    end
    config radio-3
      set mode monitor
      set wids-profile "wids.test"
    end
  next
end
```

   Radio 3 will scan the 2.4G and 5G channels specified in `ap-scan-channel-list-2G-5G`.

2. Verify that the scan is only run on the specified 2.4G and 5G channels.

```
FortiGate-40F # diag wireless-controller wlac -c ap-rogue
CMWP AP: vf                 bssid ssid             ch  rate  sec
 signal noise  age      sta mac                wtp cnt     ici    bw sgi band
         freq(MHz)
UNNN AP: 0       04:d5:90:4a:19:b1 FOS_test_001_... 161 260   WPA3 OWE               -
```

```
55 -95    562      00:00:00:00:00:00       1   /1     none    20 0  11ACVHT20 (wave2)
   5805

 N                FP431GTY22003576 FOS_test_001_... 161 260   WPA3 OWE               -
55 -95    562      172.20.1.29:5246 -2  11

UNNN AP: 0       06:18:d6:67:29:42                 6   144   WPA2 Personal          -
85 -95    958      00:00:00:00:00:00       1   /1     none    20 1  11NGHT20
   2437

 N                FP431GTY22003576                  6   144   WPA2 Personal          -
85 -95    958      172.20.1.29:5246 -2  11

UNNN AP: 0       06:93:7c:65:49:f8                 1   1181  WPA2 Personal          -
87 -95    688      00:00:00:00:00:00       1   /1     none    20 1  11AXGHE20
   2412

 N                FP431GTY22003576                  1   1181  WPA2 Personal          -
87 -95    688      172.20.1.29:5246 -2  11

UNNN AP: 0       90:6c:ac:45:5b:8a Example_001_test 149 130   WPA2 Personal          -
69 -95    51438    00:00:00:00:00:00       1   /1     none    20 0  11NAHT20 (wave2)
   5745

 N                FP431GTY22003576 Example_001_test 149 130   WPA2 Personal          -
69 -95    51438    172.20.1.29:5246 -2  11
```

To scan specified 6G channels:

1. From the FortiAP profile, **do not** enable dedicated scanning. Set Radio 3 to monitor mode with the WIDS profile applied.

```
config wireless-controller wtp-profile
  edit "FAP431G.noddscan"
    config platform
      set type 431G
    end
    set handoff-sta-thresh 55
    config radio-1
      set band 802.11ax,n,g-only
    end
    config radio-2
      set band 802.11ax-5G
    end
    config radio-3
      set mode monitor
      set wids-profile "wids.test"
    end
  next
end
```

   Radio 3 will scan the 6G channels specified in `ap-scan-channel-list-6G`.

2. Verify that the scan is only run on the specified 6G channels.

```
FortiGate-40F # diag wireless-controller  wlac -c ap-rogue
```

```
CMWP AP: vf                  bssid ssid             ch  rate  sec
signal noise  age      sta mac                wtp cnt     ici    bw sgi band
              freq(MHz)

UNNN AP: 0       84:39:8f:1f:0e:c8 test01-GUI-SS... 109 1147  WPA3 SAE               -
80 -95    6        00:00:00:00:00:00       1   /1     none    20 0  11AX6HE20-6G
 6495

 N               FP431GTY22003576 test01-GUI-SS... 109 1147  WPA3 SAE               -
80 -95    6        172.20.1.29:5246 -2  17
```

Optimizing memory storage by limiting monitoring data

You can optimize memory storage in the FortiGate wireless controller and improve CAPWAP stability by limiting the data stored from rogue APs, station capabilities, rogue stations and Bluetooth devices.

CLI commands

The following CLI commands limit the amount of information stored in the FortiGate.

```
config wireless-controller global
  set max-sta-cap <integer>
  set max-sta-cap-wtp <integer>
  set max-rogue-ap <integer>
  set max-rogue-ap-wtp <integer>
  set max-rogue-sta <integer>
  set max-ble-device <integer>
end
```

max-sta-cap	Maximum number of station cap stored on the controller (default = 0).
max-sta-cap-wtp	Maximum number of station cap's wtp info stored on the controller (1 - 8, default = 8).
max-rogue-ap	Maximum number of rogue APs stored on the controller (default = 0).
max-rogue-ap-wtp	Maximum number of rogue AP's wtp info stored on the controller (1 - 16, default = 16).
max-rogue-sta	Maximum number of rogue stations stored on the controller (default = 0).
max-ble-device	Maximum number of BLE devices stored on the controller (default = 0).

The following CLI commands have been added to clean up data and reduce the amount of information stored in the FortiGate.

```
config wireless-controller timer
  set sta-cap-cleanup <integer>
  set rogue-ap-cleanup <integer>
  set rogue-sta-cleanup <integer>
  set ble-device-cleanup <integer>
end
```

sta-cap-cleanup	Time period in minutes to keep station capability data after it is gone (default = 0).

rogue-ap-cleanup	Time period in minutes to keep rogue AP after it is gone (default = 0).
rogue-sta-cleanup	Time period in minutes to keep rogue station after it is gone (default = 0).
ble-device-cleanup	Time period in minutes to keep BLE device after it is gone (default = 60).

If 0 is set, it means there is no limit placed.

Example memory optimization configuration:

1. Using the FortiGate CLI, enter `diagnose wireless-controller wlac -c stats` to check the number of rogue APs.

```
diagnose wireless-controller wlac -c stats
cw_rbtts_sta_cap_tree                    : cnt=524416     mem=(     248B,     130MB)
tmo=0      max_cnt=524416,524416
cw_sta_cap_wtp_tree                      : cnt=668740     mem=(     296B,     197MB)
cw_rbtts_ap_rogue_tree                   : cnt=8511       mem=(     560B,       4MB)
tmo=0      max_cnt=65664,65664
cw_ap_rogue_wtp_tree                     : cnt=133761     mem=(     408B,      54MB)
cw_rbtts_sta_rogue_tree                  : cnt=6177       mem=(     232B,       1MB)
tmo=0      max_cnt=528384,528384
cw_ble_dev_tree                          : cnt=1920       mem=(     232B,       0MB)
tmo=60     max_cnt=131200,131200
```

   The number of rogue APs is 8511.

2. Check the current amount of memory used in the FortiGate:

```
get system performance status
......
Memory: 49539060k total, 26111804k used (52.7%), 22613800k free (45.6%), 813456k
freeable (1.7%)
......
```

   The amount of memory used is 52.7%.

3. Configure the FortiGate CLI to set maximum limits and timers on stored data:

```
config wireless-controller global
  set max-sta-cap 10
  set max-sta-cap-wtp 1
  set max-rogue-ap 10
  set max-rogue-ap-wtp 1
  set max-rogue-sta 10
  set max-ble-device 10
end
config wireless-controller timer
  set sta-cap-cleanup 2
  set rogue-ap-cleanup 2
  set rogue-sta-cleanup 2
  set ble-device-cleanup 2
end
```

4. Verify that rogue AP limits are successful configured by using `diagnose wireless-controller wlac -c stats`.

```
diagnose wireless-controller wlac -c stats
cw_rbtts_sta_cap_tree                   : cnt=10         mem=(     248B,       0MB)
tmo=2      max_cnt=10,524416
cw_sta_cap_wtp_tree                     : cnt=10         mem=(     296B,       0MB)
cw_rbtts_ap_rogue_tree                  : cnt=10         mem=(     560B,       0MB)
tmo=2      max_cnt=10,65664
cw_ap_rogue_wtp_tree                    : cnt=10         mem=(     408B,       0MB)
cw_rbtts_sta_rogue_tree                 : cnt=3          mem=(     232B,       0MB)
tmo=2      max_cnt=10,528384
cw_ble_dev_tree                         : cnt=10         mem=(     232B,       0MB)
tmo=2      max_cnt=10,131200
```

   The number of rogue APs decreased to 10, the same as the maximum number set.

5. Check the current memory used:

```
get system performance status
......
Memory: 49539060k total, 25568512k used (51.6%), 23156900k free (46.7%), 813648k
freeable (1.7%)
......
```

   The amount of memory used decreased to 51.6%.

To verify cleanup timers:

This example verifies the cleanup timer configured for `rogue-ap-cleanup`. In this example, the rogue AP's data should be cleaned up after 2 minutes.

1. Verify that the cleanup timers are successfully configured with `diagnose wireless-controller wlac -c ap-rogue`.

```
diagnose wireless-controller wlac -c ap-rogue
CMWP AP: vf               bssid ssid       ch rate  sec            signal noise  age
 sta mac             wtp cnt   ici   b
w sgi band                freq(MHz)
UNNN AP: 1     e0:23:ff:4a:83:c0 FOS_Device 6  286   WPA2 Enterprise   -31 -95    2
  00:00:00:00:00:00    1   /1   none   2
0 0  11AXGHE20              -
 N             FP234FTF21003786 FOS_Device 6  286   WPA2 Enterprise   -31 -95    2
 10.131.0.120:5246 -2  11
```

   In this example, the FortiAP was turned off after 2 seconds when the `age` was at `2`.

2. Enter `diagnose wireless-controller wlac -c ap-rogue` again to check the rogue AP data.

```
diag wir wlac -c ap-rogue
CMWP AP: vf              bssid ssid        ch  rate  sec            signal noise  age
 sta mac             wtp cnt   ici   b
w sgi band                freq(MHz)
UNNN AP: 1    e0:23:ff:4a:83:c0 FOS_Device  6   286   WPA2 Enterprise   -31 -95    122
 00:00:00:00:00:00    1   /1   none   2
0 0  11AXGHE20              -
 N            FP234FTF21003786 FOS_Device  6   286   WPA2 Enterprise   -31 -95    122
  10.131.0.120:5246 -2  11
```

The rogue AP `age` is now `122` (or 122 seconds). The rogue AP data was held for 2 minutes, matching the value set under `rogue-ap-cleanup`. After 2 minutes have elapsed, the data will no longer be stored.

Wireless network examples

This section includes the following topics:

- Basic wireless network example on page 342
- Wireless network example with FortiSwitch on page 347
- Complex wireless network example on page 350
- FortiGate WiFi controller 1+1 fast failover example on page 360
- CAPWAP hitless failover using FGCP on page 362
- Wireless network with segregated WLAN traffic on page 366

Basic wireless network example

This example uses automatic configuration to set up a basic wireless network with locally stored FortiOS user groups. Note that authentication with local groups only supports PEAP, not EAP-TLS.

To configure this wireless network, perform the following tasks:

- Configuring authentication for wireless users on page 342
- Configuring the SSID on page 343
- Adding the SSID to the FortiAP Profile on page 344
- Configuring security policies on page 344
- Connecting the FortiAP units on page 345

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 & Authentication* > *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 and Switch Controller* > *SSIDs* 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 and 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* > *Firewall 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 *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:

```
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 and Switch Controller* > *Managed FortiAPs*.
2. Connect the FortiAP unit to port 3.

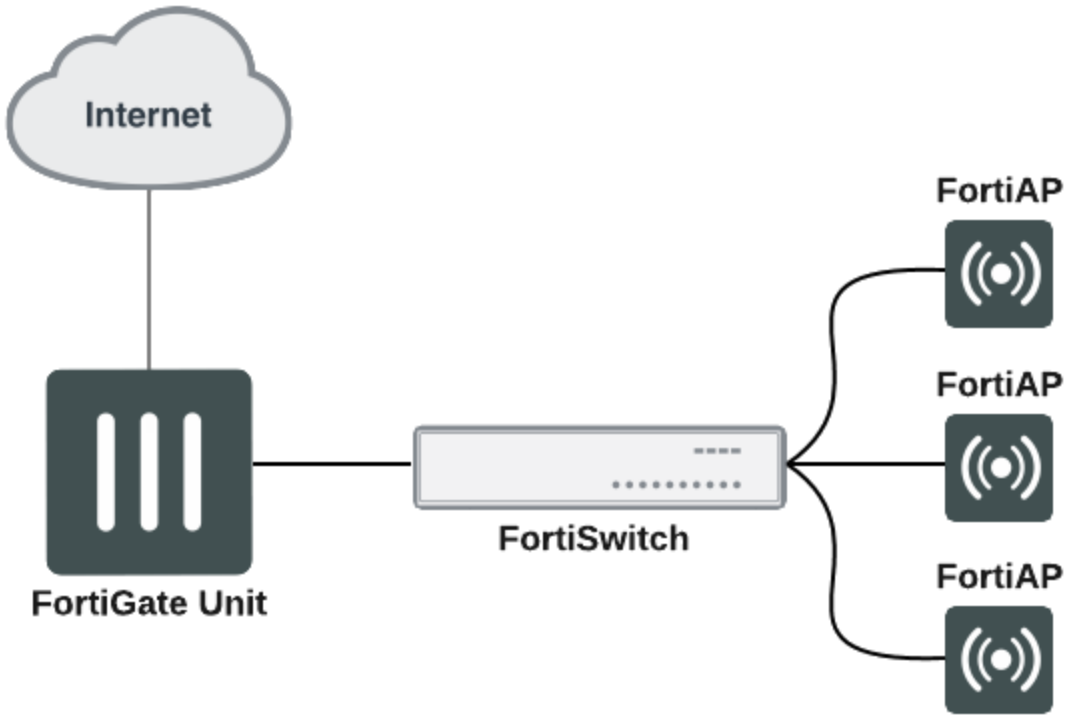
3. Periodically select *Refresh* while waiting for the FortiAP unit to be listed.
   Recognition of the FortiAP unit can take up to two minutes.
   If FortiAP units are connected but cannot be recognized, try disabling VCI-Match in the DHCP server settings.
4. When the FortiAP unit is listed, select 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 *WiFi and Switch 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 FortiLink 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 *WiFi and Switch 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 *WiFi and Switch 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 FortiLink 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 *WiFi and Switch 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 and 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 34.

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 wireless networks consists of FortiAP 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 the FortiAP 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 351
- Configuring authentication for guest wireless users on page 352
- Configuring the SSIDs on page 353
- Configuring the FortiAP profile on page 355
- Configuring firewall policies on page 356
- Connecting the FortiAP units on page 358

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 & Authentication* > *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 & Authentication* > *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 and Switch Controller* > *SSIDs* 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 and Switch Controller* > *SSIDs* 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	WPA3 SAE
Captive Portal	Enable
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 wpa3-sae
      set captive-portal enable
      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 and Switch Controller* > *FortiAP Profiles* and select *Create New*.
2. Enter the following information and select *OK*:

Name	example_AP
Platform	FAP221E
Radio 1	
Mode	Access Point
Band	802.11n
Channel plan	Select *Three Channels*.
Transmit power mode	Select *Percent*.
Transmit power	Set the bar to *100%*.
SSID	Select *Manual* and select *example_inc* and *example_guest*.
Radio 2	
Mode	Access Point
Band	802.11n_5G

Channel	*Select All*.
Transmit power mode	Select *Percent*.
Transmit power	Set the bar to *100%*.
SSID	Select *Manual* and select *example_inc*.

To configure the AP Profile - CLI:

```
config wireless-controller wtp-profile
   edit "example_AP"
      config platform
         set type 221E
      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* > *Firewall 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* > *Firewall 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 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 *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:

```
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 unit - GUI:

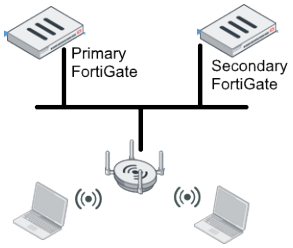
1. Go to *WiFi and Switch Controller* > *Managed FortiAPs*.
2. Connect the FortiAP unit to port 3.
3. Periodically select *Refresh* while waiting for the FortiAP unit to be listed.
   Recognition of the FortiAP unit can take up to two minutes.
   If there is persistent difficulty recognizing FortiAP 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 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.

FortiGate WiFi controller 1+1 fast failover example

This example uses a simple network topology to set up 1+1 fast failover between FortiGate WiFi controllers. The primary and secondary FortiGates must be routed into subnets and NAT must not be done on the traffic. The FortiAP must be able to reach both the primary and secondary FortiGates.



The following takes place in the event of a failover:

1. The primary FortiGate syncs the wireless configuration to the secondary FortiGate.
2. If the primary FortiGate fails, the secondary FortiGate takes over management of the FortiAP. The client can still connect with the SSID from the FortiAP and pass traffic.
3. When the primary FortiGate is back online, it returns to managing the FortiAP.

In the following CLI example, the primary FortiGate has an IP address of 10.43.1.80, and the secondary FortiGate has an IP address of 10.43.1.62.

To configure the primary FortiGate:

```
config wireless-controller inter-controller
   set inter-controller mode 1+1
   set inter-controller key 123456
   config inter-controller-peer
      edit 1
         set peer-ip 10.43.1.62
         set peer-priority secondary
      next
```

```
   end
```

To configure the secondary FortiGate:

```
config wireless-controller inter-controller
   set inter-controller mode 1+1
   set inter-controller key 123456
   set inter-controller-pri secondary
   config inter-controller-peer
      edit 1
         set peer-ip 10.43.1.80
      next
   end
```

To run diagnose commands:

1. On the primary FortiGate, run the `diagnose wireless-controller wlac -c ha` command. The output should resemble the following:
   ```
   WC fast failover info
   cfg iter: 1 (age=17995, size=220729, fp=0x5477e28)
   dhcpd_db iter: 123 (age=132, size=1163, fp=0x5435930)
   dhcpd_ipmac iter: 123 (age=132, size=2860, fp=0x587d848)
   mode: 1+1-ffo
   pri: primary
   key csum: 0x9c99
   max: 10
   wait: 10
   peer cnt: 1
      FWF60E4Q16027198: 10.43.1.62:5245 secondary UP (age=0)
   ```
2. On the secondary FortiGate, run the `diagnose wireless-controller wlac -c ha` command. The output should resemble the following:
   ```
   WC fast failover info
   mode: 1+1-ffo
   status: monitoring
   pri: secondary
   key csum: 0x43e
   max: 10
   wait: 10
   peer cnt: 1
      FG22E1T919900557: 10.43.1.80:5246 primary UP (age=0)
         dfile 0 iter 1 (age=133, size=1564731/1564731)
         dfile 1 iter 1 (age=163, size=0/0)
         dfile 2 iter 1 (age=163, size=0/0)
   ```

You cannot use FortiGate Clustering Protocol and Wireless 1+1 fast failover together. They are two different HA features and cannot be combined.

CAPWAP hitless failover using FGCP

CAPWAP hitless failover with FGCP is only available on FortiAP AX platforms and F Series models when FortiGates are running in Active-Passive mode.

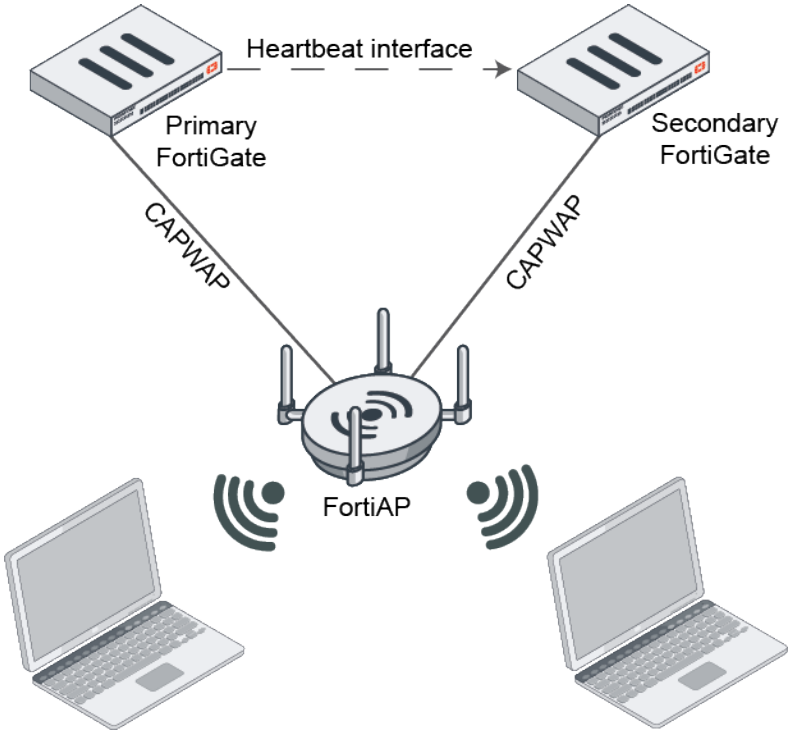
This example uses a simple network topology to set up FortiGates as WLAN controllers in HA Active-Passive by using the FortiGate Clustering Protocol (FGCP). FGCP is the most commonly used HA solution. It enables two FortiGates Wireless controllers of the same type and model to be put into a cluster in Active-Passive (A-P) mode. A-P mode provides redundancy by having one or more FortiGates in hot standby in case the primary device experiences a detectable failure. If a failure occurs, CAPWAP traffic quickly fails over to a secondary device, preventing significant AP downtime with minimal impact for the wireless clients.

For more information, refer to FGCP in the FortiGate Administration Guide.

The FortiAP establishes two CAPWAP tunnels:

- One tunnel to an Active/Primary FortiGate.
- One tunnel to a Backup/Standby FortiGate.

The CAPWAP traffic is always processed by the Active FortiGate, which relays the FortiAP information to the Backup/Standby FortiGate using heartbeat interface over FGCP.



The FortiAP forms dual CAPWAP sessions with both FortiGates:

- `fsm state RUN` with the Active FortiGate.
- `RUN_STANDBY` with the Backup FortiGate.

FortiAP uses two sets of control and data channels:

- FAP---------->5246/5247---------->Active FGT
- FAP---------->5248/5249---------->Active FGT ----------5246/5247---------->Secondary FGT

When the primary FortiGate fails, the secondary FortiGate immediately takes over as the new active FortiGate and manages the FortiAP. Wireless clients connected over tunnel/bridge SSID also maintain the connection during the failover.

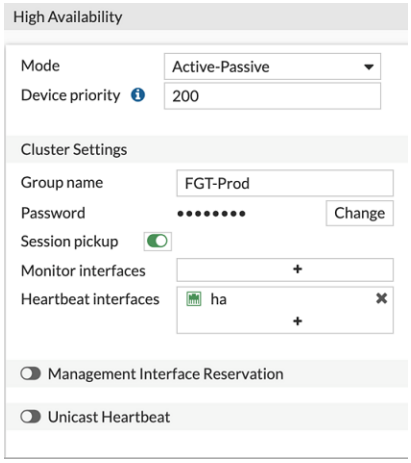
The general configuration steps are:

1. Configure the primary FortiGate for HA with higher priority.
2. Configure the secondary FortiGate for HA with a lower device priority than the primary FortiGate.
3. Connect heartbeat interface to the primary FortiGate.
4. Connect the LAN interface to the network.
5. Configure the override flag in HA configuration for preemptive failover and fallback.
6. Manually configure the override and priority configuration on both FortiGates as they don't sync as part of HA sync.
7. Enable session pickup in the Active FortiGate's HA configuration. This setting ensures that existing sessions on active firewall is synced with the backup unit and the session persists upon failover.

To configure the primary FortiGate:

For detailed instructions on setting up an HA active-passive cluster, refer to HA active-passive cluster setup in the FortiGate Administration Guide.

```
config system ha
  set group-name "FGT-Prod"
  set mode a-p
  set password <PWD>
  set hbdev "ha" 0
  set override disable
  set priority 200
  set session-pickup enable
  set override disable
end
```



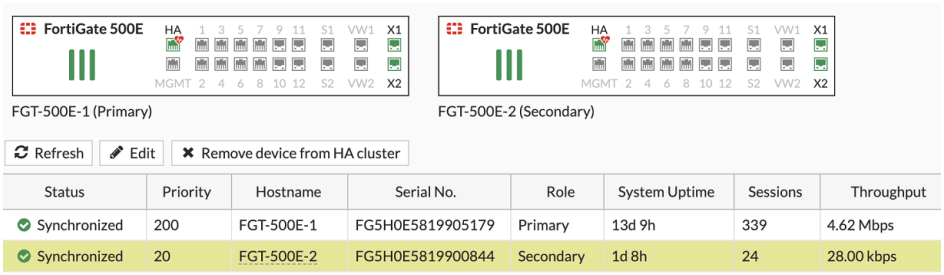
When `session-pickup` is enabled in the HA settings, existing TCP sessions are kept, and users on the network are not impacted by downtime as the traffic can be passed without re-establishing the sessions. Other sessions such as UDP, ICMP, and etc., can also be synchronized. For more information, refer to the FortiGate CLI documentation.

To configure the secondary FortiGate:

```
config system ha
  set group-name "FGT-Prod"
  set mode a-p
  set password <PWD>
  set hbdev "ha" 0
  set override disable
  set priority 20
  set session-pickup enable
  set override disable
end
```

When `override` is enabled, it ensures the FortiGate will always get the same node as the primary FortiGate.

When you are finished, confirm the cluster shows both nodes.



Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	200	FGT-500E-1	FG5H0E5819905179	Primary	13d 9h	339	4.62 Mbps
Synchronized	20	FGT-500E-2	FG5H0E5819900844	Secondary	1d 8h	24	28.00 kbps

Diagnose commands

FGCP debug commands

To check HA status:

Execute the following command:

```
diagnose sys ha status
HA information
Statistics
       traffic.local = s:0 p:694553983 b:606857125628
       traffic.total = s:0 p:694508998 b:606848291577
       activity.ha_id_changes = 3
       activity.fdb  = c:0 q:0
Model=500, Mode=2 Group=0 Debug=0
nvcluster=1, ses_pickup=1, delay=0
[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FG5H0E5819905179:      Primary, serialno_prio=0, usr_priority=200, hostname=FGT-500E-1
FG5H0E5819900844:    Secondary, serialno_prio=1, usr_priority=20, hostname=FGT-500E-2
[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.1, primary_id=0:
```

```
FG5H0E5819905179:      Primary, ha_prio/o_ha_prio=0/0
FG5H0E5819900844:      Secondary, ha_prio/o_ha_prio=1/1
```

To check HA sync:

```
get sys ha status
```

Wireless Controller HA status

To check the status of the primary FortiGate:

On the primary FortiGate, run the `diagnose wireless-controller wlac -c ha` command. The output should resemble the following:

```
FGT-500E-1 # diagnose wireless-controller wlac -c ha
HA info:
   mode: a-p (2)
   group name: FGT-Prod
   master: 1
```

To check the status of the secondary FortiGate:

On the secondary FortiGate, run the `diagnose wireless-controller wlac -c ha` command. The output should resemble the following:

```
FGT-500E-2 # diagnose wireless-controller wlac -c ha
HA info:
   mode: a-p (2)
   group name: FGT-Prod
   master: 0
```

Troubleshooting FortiAP

To check FortiAP connectivity to the primary and secondary FortiGates:

On each FortiAP, you can check their connectivity to both the primary and secondary FortiGates with the following command:

```
FAP-431F # cw_diag -c ha
wcha_mode: FGCP @2294596

ACS-0: 10.199.0.46:5246       10.199.0.46:5247       RUN(25929)            9    HA M 5248
FG5H0E5819905179 25653 FGT-500E
ACS-1: 10.199.0.46:5248       10.199.0.46:5249       RUN_STANDBY(23789)    9    HA S 5248
FG5H0E5819900844 23789 FGT-500E-2

HA SYNC status:
       vap00 1, vap01 1, vap02 1, vap03 1,
       vap10 1, vap11 1, vap12 1, vap14 1,
```

Control plane	5246 5248

DATA plane	5247 5249
Connection state	RUN RUN_STANDBY

You can verify the connection with the following command:

```
FAP-431F # cw_diag -c acs
WTP Configuration
    name                : FAP-431F
    loc                 : N/A
    ap mode             : thin AP
    ...
ACS 0 info
    ha   info           : ac=FG5H0E5819905179 master=1 ctl_port=5248
    fsm-state           : RUN 264272
    ac-ip-addr          : 10.199.0.46:5246,5247        MULTICAST
    ac-name             : FGT-500E
    ...
ACS 1 info
    ha   info           : ac=FG5H0E5819900844 master=0 ctl_port=5248
    fsm-state           : RUN_STANDBY 262132
    ac-ip-addr          : 10.199.0.46:5248,5249        MULTICAST
    ac-name             : FGT-500E-2
    ...
```

Debugging options from FortiAP:

```
cw_debug on
cw_diag debug ha 5
```

Debugging options from FortiGate:

```
diag wireless-controller wlac debug ha 4
diag debug enable
```

Wireless network with segregated WLAN traffic

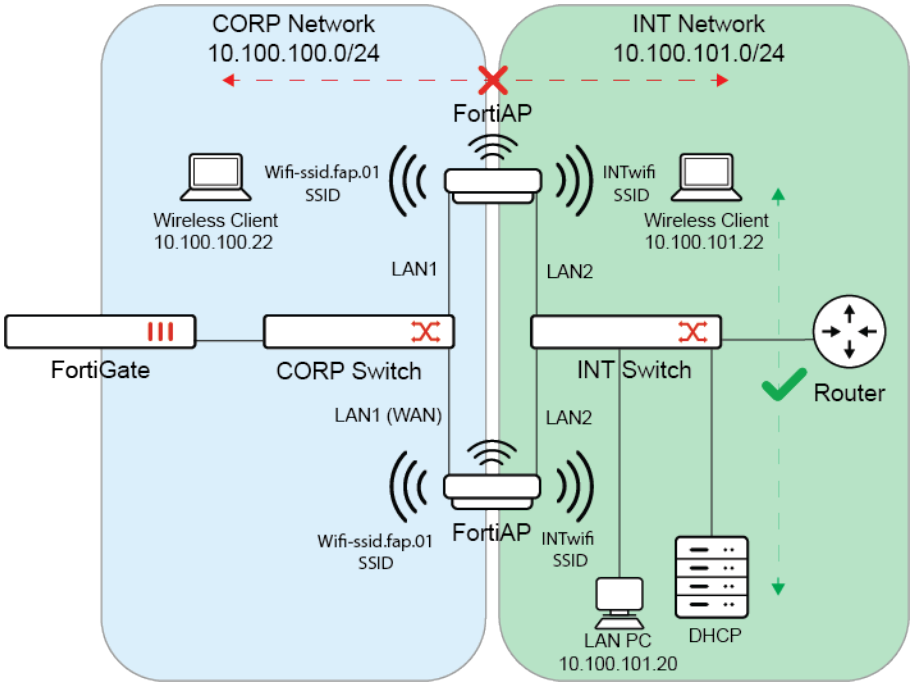
This example uses FortiAPs operating in WAN-LAN mode to segregate local LAN. When implemented, wired clients on the LAN port and wireless clients on the SSID remain within the same layer-2 bridge. Clients can continue to send and receive data traffic through the same VLAN segment of the FortiAP WAN port, however, their local traffic is segregated from the FortiAP's WAN side.

For more information on configuring a FortiAP to operate in WAN-LAN mode, see Configuring a port to WAN-LAN operation mode on page 221

Example configuration

In this example, the customer has two separate networks: CORP and INT. They want to deploy dual LAN FortiAP units and connect the LAN1 port to the CORP network and the LAN2 port to the INT network.

- Both networks have their own switches, routers, firewalls, policies, and ingress/egress to the internet.
- The FortiGate on the CORP network manages all FortiAPs, with the FortiAPs broadcasting all necessary SSIDs.
- The FortiAP LAN2 port bridges to INTwifi (Standalone mode), it connects to the INT switch and INT wired network to provide DHCP, gateway, and traffic routing.



The CORP network is a typical WLAN and LAN network. This example focuses on configuring the INT network.

To configure a network for LAN segregation:

1. Configure the bridge-mode VAP for LAN segregation:

```
config wireless-controller vap
  edit "INT"
    set ssid "INTwifi"
    set passphrase ENC *
    set local-standalone enable
    set local-lan-partition enable
    set local-bridging enable
    set local-authentication enable
    set schedule "always"
    set vlanid 100
  next
end
```

- `local-lan-partition` is only applicable when `local-bridging` and `local-standalone` mode are enabled in the VAP.
- `vlanid` is used to distinguish the VLAN segregated from the FortiAP WAN port. The SSID and LAN local bridge traffic has no VLAN tag.

2. Configure the FortiAP unit to operate in WAN-LAN mode, and then bridge the LAN port to the bridge mode VAP. For more information, see Configuring a port to WAN-LAN operation mode on page 221
   - From the FortiGate, make the following configurations to bridge the LAN port to the bridge mode VAP:

```
config wireless-controller wtp-profile
  edit "431F"
    config platform
      set type 431F
      set ddscan enable
    end
    set wan-port-mode wan-lan
    config lan
      set port-mode bridge-to-ssid
      set port-ssid "INT"
    end
    set handoff-sta-thresh 55
    config radio-1
      set mode disabled
    end
    config radio-2
      set band 802.11a 802.11n-5G 802.11ac-5G 802.11ax-5G
      set channel-bonding 40MHz
      set vap-all manual
      set vaps "INT" "wifi.fap.01"
      set channel "40"
    end
    config radio-3
      set mode monitor
    end
  next
end
```

   - From the FortiAP, configure the FortiAP to operate in WAN-LAN mode:

```
FortiAP-431F # cfg -a WANLAN_MODE=WAN-LAN
FortiAP-431F # cfg -c
```

3. Log into the FortiAP CLI to verify the changes have been successfully made.

```
FortiAP-431F # wcfg
WTP Configuration
    name                          : FortiAP-431F
    ......
    LAN mode                 : WAN LAN, ESL
    ESL ses-imagotag      : scd disabled, conn_state tcp-conn-down compliance level 2,
chan 127, power A, coex 0, apc :0, tls cert enabled fqdn disabled
    LAN port cnt             : 2
            port1-cfg        : BR-TO-SSID(3) 0 84:39:8f:88:5d:61 ssid=INTwifi
 vlan_tag=0064 flags=0000402b lsw lbr loc_auth st lan_loc
            port2-cfg        : offline   (0)
    encrypt_key[0-15]        : 16-fa-3b-ec-f7-b5-10-2e-d7-7b-a3-f5-e9-e8-a5-10
```

```
 encrypt_key[16-31]       : ca-28-cc-4f-c1-85-d9-18-0b-a8-9a-1a-cc-6e-9a-f2
 syslog conf              : disabled server=0.0.0.0():0 log-level=0
```

4. Verify the settings from the client side:
   a. Connect a Wi-Fi client (MAC 1c:87:2c:b7:bc:cc) to the INTwifi SSID. Since there is a DHCP server in the INT network, it can assign an IP address to the Wi-Fi client.
   b. Connect another client (MAC 54:27:1e:e6:43:a7) to the wifi-ssid.fap.01 SSID, the traffic of which is routed through the FortiAP WAN port.
   c. Verify the client status in FortiAP:

```
FortiAP-431F # usta

WTP daemon STA info:

  1/2   1c:87:2c:b7:bc:cc 00:00:00:00:00:00 vId=100  type=wl----sta,loc-auth
vap=wlan11,INTwifi(100) mpsk=  ip=10.100.101.22/1  mimo=3 host=wifi1-fap-robot vci=
os=Linux
                         ip6=fe80::1e87:2cff:feb7:bccc/3 rx=20
                         replycount=0000000000000002
  2/2   54:27:1e:e6:43:a7 00:00:00:00:00:00 vId=0    type=wl----sta,
 vap=wlan10,wifi-ssid.fap.01(0) mpsk=  ip=10.10.100.22/1  mimo=1 host=wifi2-fap-robot
vci= os=Linux
                         replycount=0000000000000002
```

5. Verify that the connected clients can ping the correct networks.
   a. Log into a client on the INTwifi network, and run the following command:

```
wifi1-fap-robot:~# ifconfig
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.100.101.22  netmask 255.255.255.0  broadcast 10.100.101.255
        inet6 fe80::1e87:2cff:feb7:bccc  prefixlen 64  scopeid 0x20<link>
        ether 1c:87:2c:b7:bc:cc  txqueuelen 1000  (Ethernet)
        RX packets 1421  bytes 146158 (146.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 346
        TX packets 1931  bytes 164133 (164.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 17
```

   b. Verify that the INTwifi client can ping LAN PC in the INT network (subnet 10.100.101.0/24).

```
root@wifi1-fap-robot:~# ping 10.100.101.20
PING 10.100.101.20 (10.100.101.20) 56(84) bytes of data.
64 bytes from 10.100.101.20: icmp_seq=1 ttl=64 time=5.88 ms
```

   c. Verify that the INTwifi client cannot reach CORP network (subnet 10.10.100.0/24) or the other way around.

```
root@wifi1-fap-robot:~# ping 10.10.100.22
PING 10.10.100.22 (10.10.100.22) 56(84) bytes of data.
From 10.100.101.1 icmp_seq=1 Destination Net Unreachable
```

FortiWiFi unit as a wireless client

By default, a FortiWiFi unit operates as a wireless access point. However, select FortiWiFi models can be configured to operate as a wireless client, connecting the FortiGate to another wireless network. In this 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.

For most models, the FortiWiFi unit cannot operate as an AP while also operating in client mode, so wireless clients cannot see or connect to the FortiWiFi unit. However, select models such as the FortiWiFi 80F series can support AP and client mode concurrently.

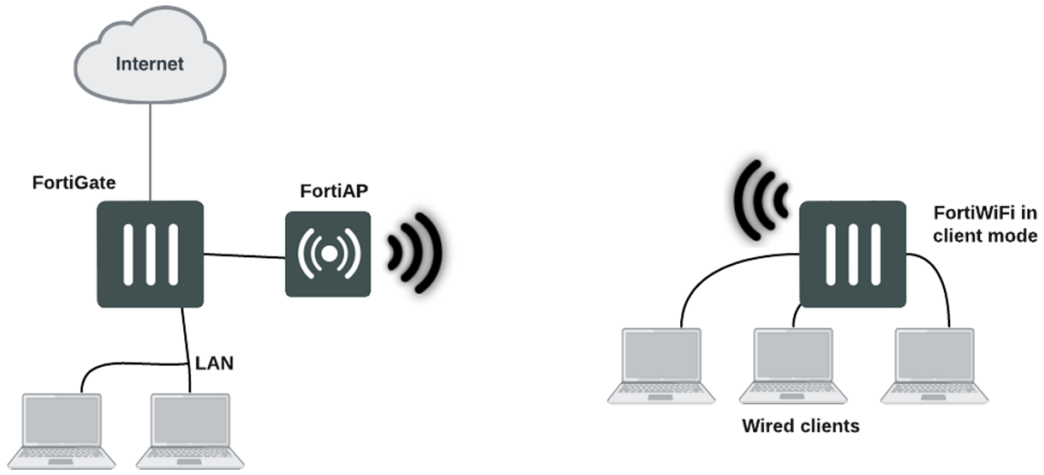
Wireless client mode is supported on the following models:

Models
FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E_DSL, FWF-60E_DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE

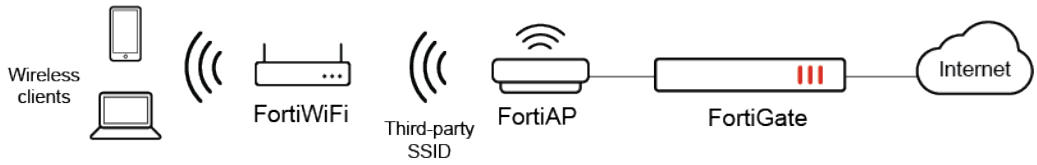
Concurrent AP and wireless client mode is supported on the following models:

Models
FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE

FortiWiFi unit in client mode



FortiWiFi unit in AP and client mode



This section includes the following topics:

- Configuring a FortiWiFi unit as a wireless client
- Enabling EAP/TLS authentication on a FortiWiFi unit in client mode
- Configuring WPA3 security modes on FortiWiFi units operating in client mode on page 379

Configuring a FortiWiFi unit as a wireless client

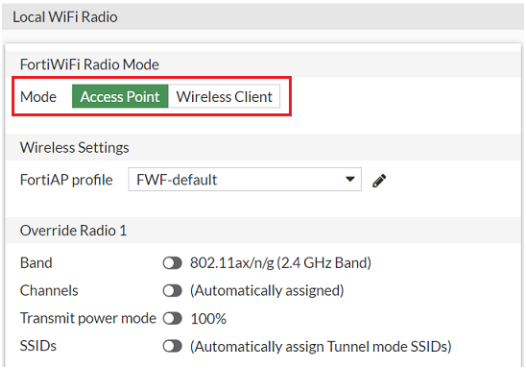
Wireless client configuration is only available on select FortiWiFi models. See FortiWiFi unit as a wireless client on page 370 for the list of supported models.

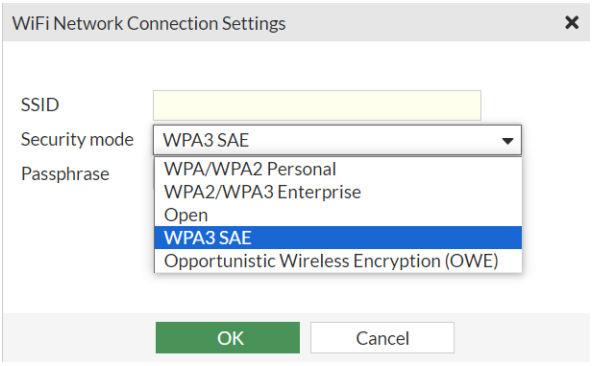
For most models, the FortiWiFi unit cannot operate as an AP while also operating in client mode. However, select models such as the FortiWiFi 80F series can support AP and client mode concurrently.

Before setting up the FortiWiFi unit as a wireless client using the steps described below, make sure to remove any AP WiFi configurations such as SSIDs, DHCP servers, policies, and software switch members using the CLI or GUI.

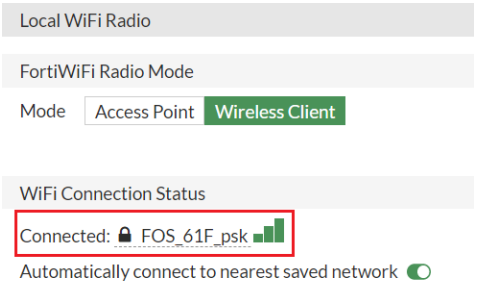
To configure wireless client mode - GUI:

1. Go to *WiFi and Switch Controller* > *Local WiFi Radio* and change the *Mode* to *Wireless Client*.



   Note: You must remove any AP WiFi configurations such as SSIDs, DHCP servers, policies, and software switch members before you can change the mode to Wireless Client. Once you select Wireless Client, the FortiWiFi unit will reboot.
2. Click *Add Network* and enter the name of the *SSID* you want to use.
3. On 8xF/6xF/40F models, you can select a *Security mode*; other models will default to WPA/WPA2 Personal.
4. 

5. Enter a *Passphrase* if needed.
6. Click *OK* to save the WiFi Network Connection Setting.
7. From the Local WiFi Radio page, verify that the WiFi network is connected.



8. Go to *Policy & Object* > *Firewall Policy* and click *Create New* to create a firewall policy.

9. Enter the following policy information:

Incoming Interface (srcintf)	wifi
Source Address (srcaddr)	all

For FortiWiFi 80F series models, you must select "aplink" as the destination interface in the firewall policy. Older FortiWiFi models must select "wifi" as the destination interface.

For more information on the aplink interface, see Understanding FortiWiFi aplink interface on page 37.

10. Configure remaining fields as needed, when you are finished, click *OK*.

To configure wireless client mode - CLI:

1. Change the wireless mode to client.

```
config system global
  set wireless-mode client
end
```

Note: You must remove any AP WiFi configurations such as SSIDs, DHCP servers, policies, and software switch members before you can change the mode to Wireless Client. Once you select Wireless Client, the FortiWiFi unit will reboot.

2. Set up a wifi-network entry under interface "wifi".

```
config system interface
  edit "wifi"
    config wifi-networks
      edit 1
        set wifi-ssid "FOS_61F_psk"
        set wifi-passphrase *
      next
    end
  next
end
```

3. Create a firewall policy from "internal" to "wifi".

For FortiWiFi 80F series models, you *must* select "aplink" as the destination interface in the firewall policy. Older FortiWiFi models must select "wifi" as the destination interface.

```
config firewall policy
  edit 1
    set name "lan"
    set srcintf "internal"
    set dstintf "wifi"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
```

```
      set nat enable
    next
  end
```

4. Connect a wired client to the internal ports of the FortiWiFi to verify that it can pass traffic to the Internet.

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
```

Configuring a FortiWiFi unit to run in concurrent AP and wireless client mode

FortiWiFi 80F/81F-2R-XX models support concurrent AP and Client mode. When the FortiWiFi is configured to run in wireless client mode and the FortiWiFi local radio connects to a third-party SSID, the local radio can concurrently operate in AP mode to provide service to wireless clients.

To configure concurrent AP and wireless client mode - CLI:

1. Configure the FortiWiFi unit to operate in client mode.

```
config system global
  set wireless-mode client
end
```

2. Connect to a third-party SSID, in this example FOS_101F_psk.

```
config system interface
  edit "wifi"
      config wifi-networks
        edit 1
          set wifi-ssid "FOS_101F_psk"
          set wifi-passphrase *
        next
      end
  next
end
```

Optionally, you can configure the wireless client to use a static IP or DHCP by modifying the addressing mode of the WiFi interface:

```
config system interface
  edit "wifi"
    set vdom "root"
    set mode static # For static IP. Use "set mode dhcp" for DHCP
    set ip 10.20.80.3 255.255.255.0 # For static IP only
    set allowaccess ping fabric
    set type wireless
    config wifi-networks
      edit 1
        set wifi-ssid "FOS_101F_psk"
        set wifi-passphrase *
      next
    end
  next
end
```

3. Verify the connection between the local radio and the third-party SSID with `diag wireless-controller wlsta cfg`.

```
FortiWiFi-81F-2R-POE # diagnose wireless-controller wlsta cfg
STA intf        name: wlan17
              status: up
                  ip: 192.168.81.2
                 mac: d4:76:a0:18:e0:8f
        auto connect: yes
           auto save: no
             ap band: any
    wifi network cnt: 1
                   1: FOS_101F_psk, 8, 1
           connected: FOS_101F_ psk
```

4. Verify the local radio status when working in AP mode with `diag wireless-controller wlac -c wtp`.

```
FortiWiFi-81F-2R-POE # diagnose wireless-controller wlac -c wtp FW81FP-WIFI0 | grep
connection
connection state : Connected
```

The FortiWiFi unit can now operate in both AP mode and client mode.

To configure VAP and SSID interfaces on the FortiWiFi local radio profile - CLI:

By default, the FortiWiFi local radio has a FWF-default profile; no other profiles can be applied to the local radio. You can modify the band, channel, and SSID selections in the FWF-default profile to apply to the local radio. Wireless clients that connect to the local radio are subject to the FortiWiFi firewall policies.

1. Create a new VAP interface and select it in the FWF-default profile.

```
config wireless-controller vap
  edit "wifi1"
    set ssid "FOS_lab_psk"
    set passphrase *
  next
```

```
end
config wireless-controller wtp-profile
  edit "FWF-default"
    config radio-1
      set vap-all manual
      set vaps "wifi1"
    end
    config radio-2
      set vap-all manual
      set vaps "wifi1"
    end
  next
end
```

The local radio applies the profile setting when broadcasting SSIDs.

2. Verify that these settings are applied with `diag wireless-controller wlac -c wtp`.
3. Create a firewall policy from "wifi1" to the "aplink" interface to allow wireless clients to pass traffic from the unit.

```
config firewall policy
  edit 1
    set name "wifi1"
    set uuid e0140546-1d0d-51ee-da6c-53fb724051ac
    set srcintf "wifi1"
    set dstintf "aplink"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set nat enable
  next
end
```

4. Connect a wireless client through the local radio of the FortiWiFi and verify that it has the correct IP and can pass traffic to the Internet with `diagnose wireless-controller wlac -d sta online`.

```
FortiWiFi-81F-2R-POE # diagnose wireless-controller wlac -d sta online
   vf=0 mpId=0 wtp=1 rId=2 wlan=wifi1 vlan_id=0 ip=10.10.80.2 ip6=::
mac=f8:e4:e3:d8:5e:af vci= host=WiFi-Client-2 user= group= signal=-45 noise=-95 idle=0
bw=0 use=5 chan=108 radio_type=11AX_5G security=wpa2_only_personal mpsk= encrypt=aes cp_
authed=no l3r=1,0 G=0.0.0.0:0,0.0.0.0:0-0-0 -- 0.0.0.0:0 0,0 online=yes mimo=2
```

Enabling EAP/TLS authentication on a FortiWiFi unit in client mode

FortiWiFi 80F/60F/40F series models operating in wireless client mode can be configured to use EAP/TLS authentication. This allows the FortiWiFi local radio to connect with a WPA2/WPA3-Enterprise SSID and support PEAP and EAP-TLS authentication methods.

EAP/TLS authentication can be configured with the `wpa-enterprise` CLI option for the `wifi-security` setting under `wifi-network` configuration.

```
config wifi-networks
  edit < ID >
    set wifi-security wpa-enterprise
```

```
    set wifi-eap-type [both | tls | peap]
    set wifi-username < username >
    set wifi-client-certificate < client_cert_name >
    set wifi-private-key < client_cert_name >
  next
end
```

When `wifi-security` is set to `wpa-enterprise`, the local radio can recognize the security mode of third-party SSIDs and automatically adapt when connecting. These security modes include WPA2-Only-Enterprise, WPA3-Only-Enterprise, WPA3-Enterprise with 192-bit encryption, and etc.

When connecting to a WPA2/WPA3-Enterprise SSID via EAP-TLS, users must also configure the WiFi username, client certificate, private key settings, and etc as applicable.

To configure FortiWiFi to run in client mode and support EAP/TLS:

1. Change the wireless mode to client. See Configuring a FortiWiFi unit as a wireless client on page 371.
2. Set the `wifi-security` mode to `wpa-enterprise`.

```
config system interface
  edit "wifi"
    config wifi-networks
      edit 1
        set wifi-ssid "FOS_101F_WPA2_ENT_PEAP"
        set wifi-security wpa-enterprise
        ...
```

3. After setting `wpa-enterprise`, configure the following as needed:

`wifi-eap-type`	Select a WPA2/WPA3-ENTERPRISE EAP method. • `PEAP` - `wifi-username` and wifi-passphrase should be set as the user account's name and password. • `TLS` - The client certificate should be specified by following settings: ◦ `wifi-client-certificate` ◦ `wifi-private-key` ◦ `wifi-private-key-password:`
`wifi-username`	Username for WPA2/WPA3-ENTERPRISE.
`wifi-client-certificate`	Client certificate for WPA2/WPA3-ENTERPRISE.
`wifi-private-key`	Private key for WPA2/WPA3-ENTERPRISE.
`wifi-private-key-password`	Password for private key file for WPA2/WPA3-ENTERPRISE.
`wifi-ca-certificate`	CA certificate for WPA2/WPA3-ENTERPRISE.

Example Use Case - WPA2-Only-Enterprise SSID using the EAP-PEAP

The following example configures the local radio to connect to a WPA2-Only-Enterprise SSID using the EAP-PEAP authentication method.

1. Upload the CA certificate to verify the server certificate from the 3rd-party SSID.

The CA certificate verification is an optional setting, users can decide whether to verify the server certificate by changing `wifi-ca-certificate` setting. To upload the CA certificate to FortiGate, log into the GUI and go to *System* > *Certificates*. Click *Create/Import* > *CA Certificate*, and follow the onscreen instructions to import the CA certificate.

2. Configure the `wifi-network` entry:

```
config system interface
  edit "wifi"
    config wifi-networks
      edit 1
        set wifi-ssid "FOS_101F_WPA2_ENT_PEAP"
        set wifi-security wpa-enterprise
        set wifi-eap-type peap
        set wifi-username "tester"
        set wifi-passphrase *
        set wifi-ca-certificate "CA_Cert_1"     <---This is an optional setting. "CA_
Cert_1" is the imported CA certificate
      next
    end
  next
end
```

3. Check the connection status:

```
FortiWiFi-81F-2R-POE # diagnose wireless-controller wlsta cfg
STA intf        name: wlan17
              status: up
                  ip: 10.4.1.2
                 mac: d4:76:a0:18:e0:8f
        auto connect: yes
           auto save: no
             ap band: any
    wifi network cnt: 1
                   1: FOS_101F_WPA2_ENT_PEAP, 16, 1
           connected: FOS_101F_WPA2_ENT_PEAP
```

Example Use Case - WPA3-Only-Enterprise SSID using EAP-TLS

The following example configures the local radio to connect to a WPA3-Only-Enterprise SSID using EAP-TLS authentication method.

1. Upload the CA certificate to verify the server certificate from the 3rd-party SSID.

The CA certificate verification is an optional setting, users can decide whether to verify the server certificate by changing `wifi-ca-certificate` setting. To upload the CA certificate to FortiGate, log into the GUI and go to *System* > *Certificates*. Click *Create/Import* > *CA Certificate*, and follow the onscreen instructions to import the CA certificate.

2. Upload the client certificate (with private key file), which will be sent to the 3rd-party SSID side for verification and authentication.

a. To upload the client certificate with private key file to FortiGate, log into the GUI and go to *System* > *Certificates*.
b. Click *Create/Import* > *Certificate*
c. Click *Import Certificate*, select *PKCS #12 Certificate* or *Certificate,* and then follow the onscreen instructions to import the client certificate with private key file.

3. Configure the `wifi-network` entry:

```
config system interface
  edit "wifi"
    config wifi-networks
      edit 2
        set wifi-ssid "FOS_101F_WPA3_ENT_TLS"
        set wifi-security wpa-enterprise
        set wifi-eap-type tls
        set wifi-username "81F-client"
        set wifi-client-certificate "client-cert"     <----"client-cert" is the name of
imported client certificate
        set wifi-private-key "client-cert"          <---It uses the same name of
imported client certificate
        set wifi-private-key-password *
        set wifi-ca-certificate "CA_Cert_1"     <---This is an optional setting. "CA_
Cert_1" is the imported CA certificate
      next
    end
  next
end
```

- `wifi-username` is the "identity" of the client-mode local radio during EAP-TLS authentication.
- `wifi-private-key-password` is the password created when importing the client certificate on the FortiWiFi.

4. Check the connection status:

```
FortiWiFi-81F-2R-POE # diagnose wireless-controller wlsta cfg
STA intf        name: wlan07
              status: up
                  ip: 10.30.80.2
                 mac: d4:76:a0:18:e0:87
        auto connect: yes
           auto save: no
             ap band: any
    wifi network cnt: 1
                   1: FOS_101F_WPA3_ENT_TLS, 16, 1
           connected: FOS_101F_WPA3_ENT_TLS
```

Configuring WPA3 security modes on FortiWiFi units operating in client mode

When the local radio of a FortiWiFi 8xF/6xF/40F model is operating in client mode, it can connect with third-party SSIDs with a WPA3-SAE or OWE security mode. You can configure the security mode from the GUI (see FortiWiFi unit as a

wireless client on page 370) or from the CLI under `config wifi-networks`.

```
config wifi-networks
  edit < ID >
    set wifi-security [open | wpa-personal | wpa3-sae | owe]
  next
end
```

To configure WPA3 security mode SSID on a FortiWiFi running in client mode - CLI:

1. Change the wireless mode to client. See Configuring a FortiWiFi unit as a wireless client on page 371.

   Note: You must remove any AP WiFi configurations such as SSIDs, DHCP servers, policies, and software switch members before you can change the mode to Wireless Client. Once you select Wireless Client, the FortiWiFi unit will reboot.
2. Create a wireless network by connect to a third-party SSID and setting the security mode. In this example, the SSID is FOS_101F_WAP3_SAE and the security mode is WPA3 SAE.

   ```
   config system interface
     edit "wifi"
       config wifi-networks
         edit 1
           set wifi-ssid "FOS_101F_WAP3_SAE"
           set wifi-security wpa3-sae
           set wifi-passphrase *
         next
       end
     next
   end
   ```

To verify the connection status:

1. Verify the connection between the local radio and the third-party SSID with `diagnose wireless-controller wlsta cfg`.

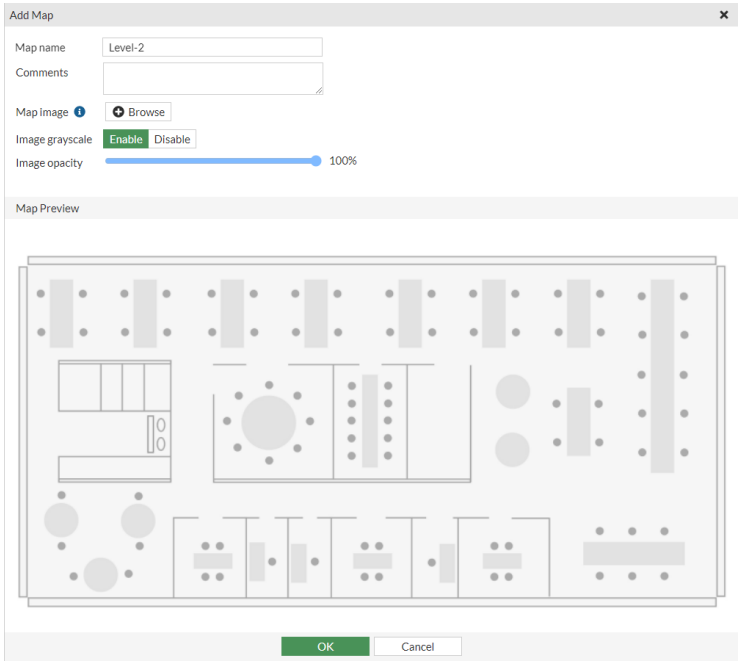
   ```
   diagnose wireless-controller wlsta cfg
   STA intf        name: wlan17
                 status: up
                     ip: 3.1.1.2
                    mac: d4:76:a0:18:e0:8f
           auto connect: yes
              auto save: no
                ap band: any
       wifi network cnt: 1
                      1: FOS_101F_WPA3_SAE, 19, 1
              connected: FOS_101F_WPA3_SAE
   ```

WiFi maps

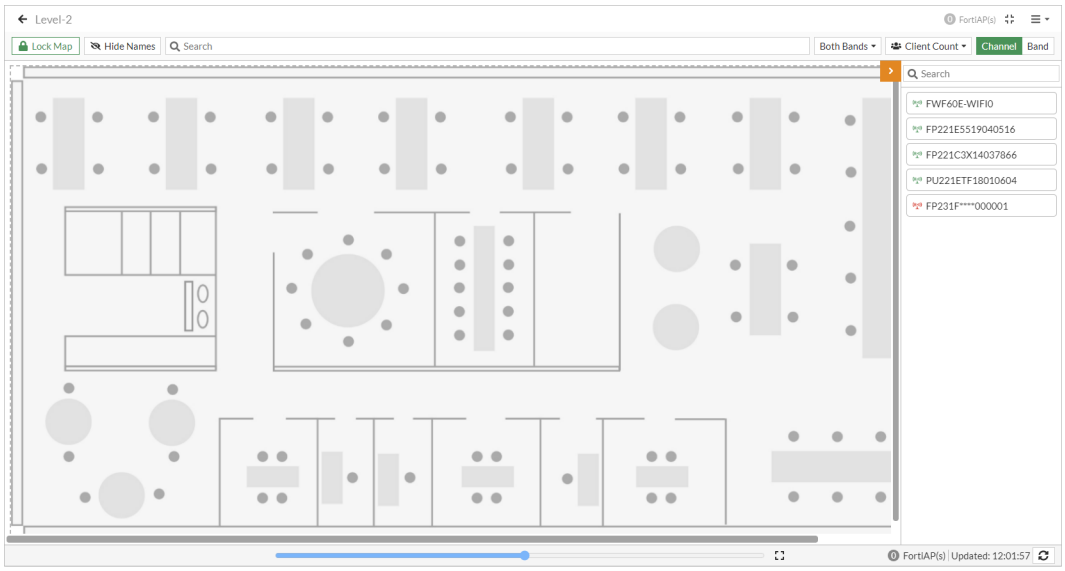
You can place FortiAP units on a custom map that you upload, such as an office floor plan. WiFi Maps show real-time status and alerts of FortiAP units so that you can quickly see the location and status of each FortiAP unit on the map.

To configure WiFi maps on the FortiWiFi and FortiAP GUI:

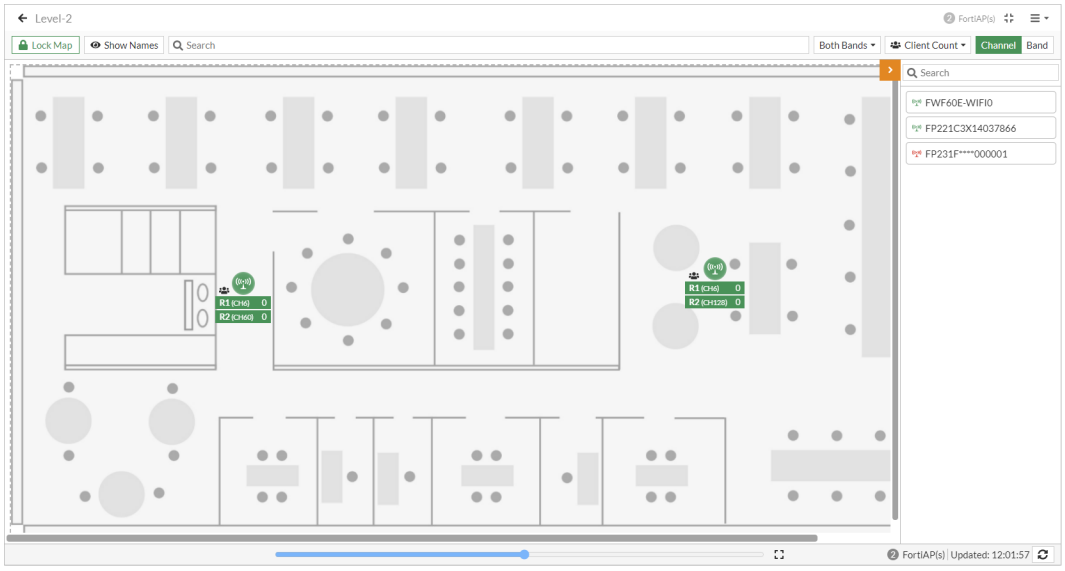
1. Obtain a floor plan or map (in PNG, JPEG, or GIF format) of where FortiAP units are located.
2. Go to *WiFi Controller* > *WiFi Maps* and click *Create New*.
   a. Enter a *Map name* for example, *Level-2*.
   a. Click *Browse* to upload the map.
   a. Optionally, enable *Image grayscale* to change a color map to grayscale.
   a. Set *Image opacity* to specify map transparency.



   a. Click *OK*.
3. Place FortiAP units on the map you uploaded.
   a. Click *Unlock Map* to enable editing.
   The list of unplaced APs loads.

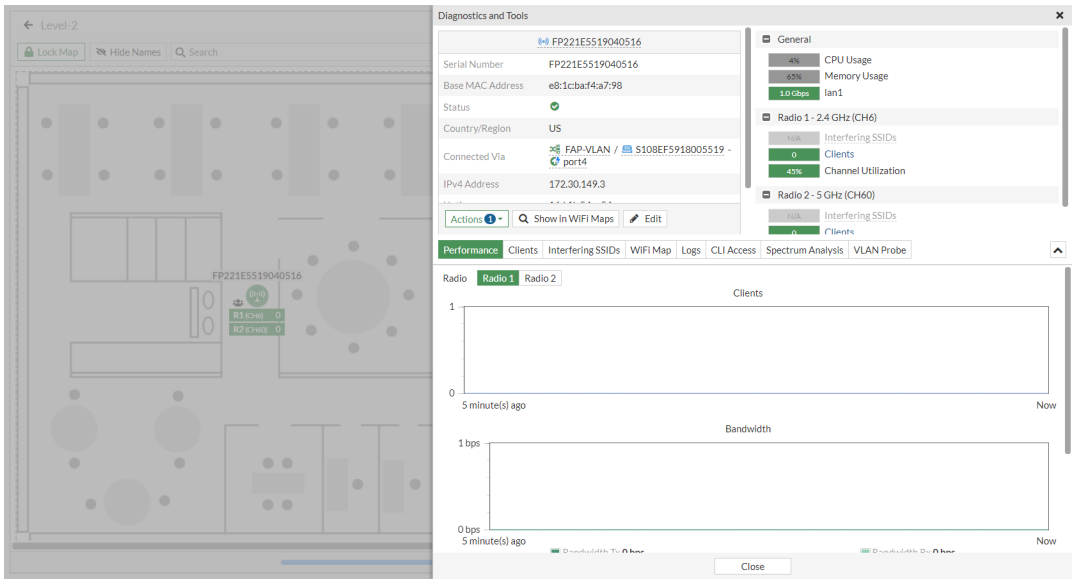


b. Drag and drop each FortiAP unit onto its location on the map.

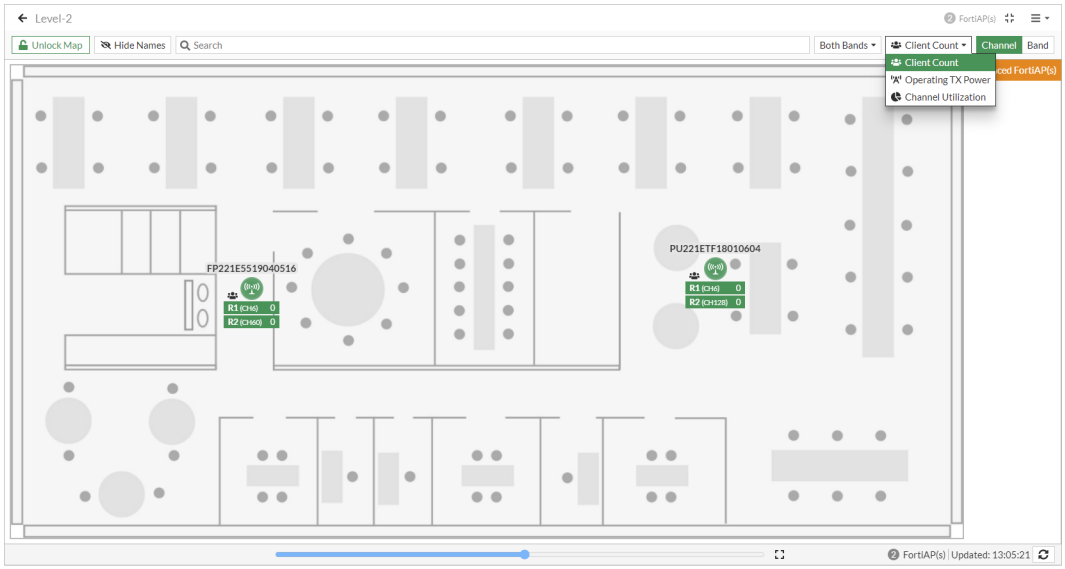


c. When all FortiAP units have been placed on the map, click *Lock Map* to save.

4. To view a FortiAP unit's detailed operating data or to configure AP settings, right-click the FortiAP icon and select *Diagnostics and Tools*.

5. 

6. Use the filters above the map to show one or both the 2.4 GHz or 5 GHz band. You can also use the dropdown lists to show numerical operating data such as client count, channel, radio TX power, and channel utilization.



To configure WiFi maps using the FortiWiFi and FortiAP CLI:

```
config wireless-controller region
   edit <MAP_NAME>
      set grayscale enable <enable|disable>
      set opacity 40 <0-100>
   next
end
config wireless-controller wtp
   edit <FAP_SN>
      set region <MAP_NAME>
      set region-x "0.419911" <0-1>
      set region-y "0.349466" <0-1>
   next
end
```

Bluetooth Low Energy scan

For FortiAPs with built-in Bluetooth radios, the FortiGate can configure FortiAP Bluetooth Low Energy (BLE) scan and integrate with several BLE Beacon profiles. To see which FortiAP models support BLE scanning, refer to the FortiAP Data Sheets.

Once a BLE profile is configured, you can then assign it to a FortiAP profile.

To assign a BLE profile to a FortiAP profile - CLI:

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

You can also configure BLE report intervals.

To configure BLE report intervals - CLI:

```
config wireless-controller timers
   set ble-scan-report-intv - (default = 30 sec)
end
```

Override BLE profiles from WTP profiles and group

For FortiOS 7.2.5 and later and 7.4.1 and later, you can override the BLE major and minor IDs set in the BLE profile by making configurations directly to the WTP profile and group settings. This simplifies Bluetooth Low Energy (BLE) iBeacon provisioning for RTLS deployments.

- The BLE major ID can be set in WTP settings and WTP group settings as well as in the BLE profile settings.
- The BLE minor ID can be set in WTP settings and in the BLE profile settings.

To set BLE major and minor IDs from the WTP settings:

The BLE major ID set in the WTP settings overrides the ID set in the WTP group and the BLE profile.

The BLE minor ID set in the WTP settings overrides the ID set in the BLE profile.

```
config wireless-controller wtp
  edit < FortiAP-serial-number >
    set ble-major-id < ID >
    set ble-minor-id < ID >
  next
end
```

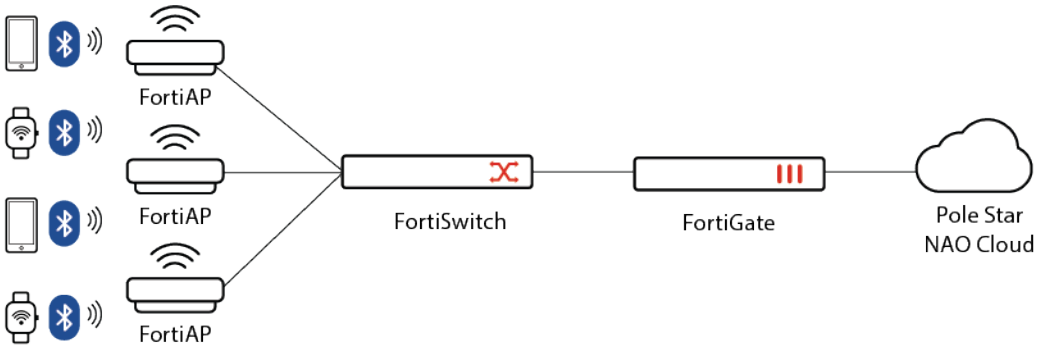
To set BLE major IDs from the WTP group settings:

The BLE major ID set in the WTP group settings overrides the ID set in the BLE profile.

```
config wireless-controller wtp-group
  edit < FortiAP-group-name >
    set ble-major-id < ID >
    set wtps < FortiAP-serial-number-1 > < FortiAP-serial-number-2 > ...
  next
end
```

Pole Star NAO Cloud service integration

Managed FortiAP units can be configured to scan Pole Star BLE asset tags and send the scanned data to the Pole Star's NAO Cloud. This enables wearable devices with BLE asset tags to communicate with FortiAPs via their built-in Bluetooth radios. The data forwarded to the cloud service is processed by Pole Star and analytics are generated to map the location of each asset.



To configure a Pole Star BLE profile - CLI:

```
config wireless-controller ble-profile
  edit "testpolestar"
    set ble-scanning enable
    set scan-type passive
    set scan-period 1000
    set scan-interval 30
    set scan-window 30
  next
end
```

`scan-type`	There are two types of scanning; active and passive. • Active BLE scanning: Send a scan request for additional information from the advertiser. • Passive BLE scanning: Only receive data from the advertising device. Scan Type (default = active).
`scan-threshold`	Enter a minimum signal level/threshold in dBm required for the AP to report detected BLE device (-95 to -20, default = -90).
`scan-period`	The scan period is the total time for each round. Enter an integer value from <1000> to <10000> (default = <4000>).
`scan-time`	The scan time is the duration in which the device stays in the scanning state. Enter an integer value from <1000> to <10000> (default = <1000>).
`scan-interval`	The scan interval is the interval between the start of two consecutive scan windows. Enter an integer value from <10> to <1000> (default = <50>).
`scan-window`	The scan window is the duration the Link layer scans on one channel. Enter an integer value from <10> to <1000> (default = <50>)

Once you configure a BLE profile, you must apply the BLE profile to a FortiAP profile and then configure Pole Star server settings under location-based services (LBS) in the wtp-profile.

To configure Pole Star location-based services - CLI:

```
config wireless-controller wtp-profile
  edit "FAP431G-default"
    config platform
      set type 431G
    end
```

```
    set ble-profile "testpolestar"
    set handoff-sta-thresh 55
    config radio-1
      set band 802.11ax,n,g-only
    end
    config radio-2
      set band 802.11ax-5G
      set channel-bonding 40MHz
    end
    config radio-3
      set band 802.11ax-6G
      set channel-bonding 160MHz
    end
    config lbs
      set polestar enable
      set polestar-server-fqdn "ws-staging.nao-cloud.com"
      set polestar-server-token "nrhxj1qlmagx7dqakfihhw"
      set polestar-asset-uuid-list1 "1234*-*-*-*-12345*12"
      set polestar-asset-uuid-list2 "1234*-1234-1234-1234-123456789012"
      set polestar-asset-uuid-list3 "*-12*-*12-*-1234*55"
      set polestar-asset-uuid-list4 "12345678-1234-1234-1234-123456789012"
      set polestar-asset-addrgrp-list "pole-grp"
    end
  next
end
```

polestar	Enable/disable Pole Star BLE NAO Track Real Time Location Service (RTLS) support (default = disable).
polestar-protocol	Select the protocol to report Measurements, Advertising Data, or Location Data to NAO Cloud (default = WSS).
polestar-server-fqdn	FQDN of Pole Star NAO Track Server (default = ws.nao-cloud.com).
polestar-server-path	Path of Pole Star NAO Track Server (default = /v1/token/<access_token>/pst-v2).
polestar-server-token	Access Token of Pole Star NAO Track Server.
polestar-server-port	Port of Pole Star NAO Track Server (default = 443).
polestar-accumulation-interval	Time that measurements should be accumulated in seconds (default = 2).
polestar-reporting-interval	Time between reporting accumulated measurements in seconds (default = 2).
polestar-asset-uuid-list1	Tags and asset UUID list 1 to be reported (string in the format of 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX').

`polestar-asset-uuid-list2`	Tags and asset UUID list 2 to be reported (string in the format of 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX').
`polestar-asset-uuid-list3`	Tags and asset UUID list 3 to be reported (string in the format of 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX').
`polestar-asset-uuid-list4`	Tags and asset UUID list 4 to be reported (string in the format of 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX').

`polestar-asset-addrgrp-list`	Tags and asset `addrgrp` list to be reported.
	The `polestar-asset-addrgrp-list` setting uses a FortiOS firewall address group to include MAC addresses of Pole Star BLE tags. Either individual MAC address or MAC address range can be supported. For example:
	`config firewall addrgrp`
	`  edit "pole-grp"`
	`  set member "addr-01" "addr-05"`
	`  next`
	`end`
	`config firewall address`
	`  edit "addr-01"`
	`  set type mac`
	`  set macaddr "ee:0f:4d:00:11:22"`
	`  next`
	`  edit "addr-05"`
	`  set type mac`
	`  set macaddr "ee:0f:4d:00:00:00-ff:ff:ff:00:00:00"`
	`  next`

To verify the configurations:

From the FortiAP CLI, enter the following diagnostic commands:

```
FortiAP-431G # cw_diag -c ble-config
WTP Bluetooth Low Energy Configuration:
        ble scan report interval  : 30
        advertising               :
        ibeacon_uuid              : 00000000-0000-0000-0000-000000000000
        major ID                  : 0
        minor ID                  : 0
        eddystone namespace ID    :
        eddystone instance ID     :
        eddystone URL             :
        txpower                   : 0
        beacon interval           : 100
        ble scanning              : enabled (mode=passive,thresh=-
90,period=1000,time=1000,intv=30,wind=30)

BLE address: c4:39:8f:ef:5b:67
BLE oper pid: 17473
BLE conf pid: 17473
```

```
FortiAP-431G # cw_diag -c ble-polestar
BLE PoleStar Config:
   ps_enable = enabled
   ps_proto = WSS
   ps_server_fqdn = ws-staging.nao-cloud.com
   ps_server_path = /v1/token/<access_token>/pst-v2
   ps_server_token = nrhxj1qlmagx7dqakfihhw
   ps_server_port = 443
   ps_acc_intv = 2
   ps_rpt_intv = 2
   ps_addrgrp_uuid_policy = allow
       B001 12340000-0000-0000-0000-123450000012 - ffff0000-0000-0000-0000-ffff00000ff
       B002 12340000-1234-1234-1234-123456789012 - ffff0000-ffff-ffff-ffff-fffffffffff
       B003 00000000-1200-0012-0000-123400000055 - 00000000-ff00-00ff-0000-ffff000000ff
       B004 12345678-1234-1234-1234-123456789012 - ffffffff-ffff-ffff-ffff-fffffffffff
   ps_addrgrp_policy = allow
       S005 ee:0f:4d:00:11:22
       B006 ee:0f:4d:00:00:00 - ff:ff:ff:00:00:00
   ps_ble_dev_max_rpt = 128
   ps_ble_dev_max_batch = 64
```

Eddystone BLE beacon profile integration

Eddystone is Google's BLE beacon profile that can be used to identify groups of devices and individual devices.

Use the following syntax to configure a BLE profile that integrates Eddystone. Once you configure the BLE profile, you must then assign it to a FortiAP profile.

To configure BLE profiles for Eddystone - CLI:

```
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		

Location-based services

FortiOS supports location-based services by collecting information about WiFi devices near FortiAPs, 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. Through FortiPresence, you can use this information to track and analyze the movements of the device owner. FortiPresence processes the data and displays it in an analytics dashboard. The device owners 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.

Pole Star location-based services

Managed FortiAP units can be configured to scan Pole Star BLE asset tags and send the scanned data to the Pole Star's NAO Cloud. This enables wearable devices with BLE asset tags to communicate with FortiAPs via their built-in Bluetooth radios. The data forwarded to the cloud service is processed by Pole Star and analytics are generated to map the location of each asset.

For more information, see Pole Star NAO Cloud service integration on page 385

Configuring location tracking

You can enable location tracking in any FortiAP profile by setting the `station-locate` field to `enable`. You can also enable enhanced location accuracy through the 802.11mc Wi-Fi protocol.

To enable location tracking - CLI:

```
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
```

To enable 802.11mc on a FortiAP - CLI:

The 802.11mc Wi-Fi protocol enables supported devices and clients to measure their distance to nearby Wi-Fi access points. APs act as a Fine Timing Measurement (FTM) responder to time measurement queries sent from a client. FortiAP radios can be configured to operate in 802.11mc responder mode, enabling connected devices and clients to use enhanced location accuracy.

The FortiAP must be running firmware version 7.6.0 or later to support this feature.

```
config wireless-controller wtp-profile
  edit "FAP23JF-default"
    config radio-1
      set 80211mc enable
    end
  next
end
```

To verify that 802.11mc is configured on a FortiAP:

1. From the FortiGate, verify that 802.11mc has been successfully enabled.

```
FortiGate-81E-POE (Interim)# diagnose wireless-controller wlac -c wtp FP23JFTF21000769 |
grep 80211mc -B 2
  Radio 1            : AP
    80211d enable:   : enabled
    80211mc enable   : enabled
--
  Radio 2            : AP
    80211d enable:   : enabled
    80211mc enable   : enabled
```

2. From the FortiAP, verify that 802.11mc has been successfully enabled.

```
FortiAP-23JF # rcfg | grep 802.11mc -B4
Radio 0: AP
   country        : cfg=US  oper=US
   countryID      : cfg=841 oper=841
   802.11d enable  : enabled
   802.11mc enable : enabled
--
Radio 1: AP
   country        : cfg=US  oper=US
   countryID      : cfg=841 oper=841
   802.11d enable  : enabled
   802.11mc enable : enabled
```

3. Using a packet capture tool, check the packet capture result for the *customer_usage* SSID configured in the FortiAP profile.

   Fine Timing Measurement Responder should be set to *True*, indicating that the FortiAP supports the 802.11mc responder mode.
4. Optionally, you can use a scanning app such as Google's WifiRttScan App to scan for nearby Wi-Fi RTT (802.11mc) capable access points.

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).

Viewing device location data on a FortiGate unit

You can use the FortiGate CLI to list located devices. This is can be used to confirm that the location data feature is working. You can also reset the 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 FortiPresence uses. Because of its length, this line wraps around and displays as multiple lines.

Configuring FortiPresence

You can configure FortiPresence to process and analyze the results of your location tracking. For comprehensive instructions on configuring FortiPresence, see the FortiPresence Administration Guide.

Once you've set up FortiPresence, you can enable it on a FortiAP profile to apply your settings to your APs.

To apply FortiPresence settings to a FortiAP:

1. From the FortiGate GUI navigate to *WiFi and Switch Controller* > *FortiAP Profiles*.
2. Select the FortiAP profile you want to configure FortiPresence for.
3. Locate the FortiPresence section and select which mode you want to use to enable the service.
   - *Foreign Channels Only:* AP will only listen to clients on foreign channels when doing background scan. It will not listen to clients associated to other APs running on its home (or operating) channel to preserve associated clients traffic.
   - *Foreign and Home Channels:* AP will also listen to connected clients associated to other APs on its home channel. This is useful for FortiPresence, but can negatively impact AP performance when AP is serving clients.
4. Enter the Project name and Password from FortiPresence (Use the Project Name and Project Secret Key from the FortiPresence GUI *Admin* > *Settings* > *Discovered APs*).
5. Enter the FortiPresence server IP and FortiPresence server port from FortiPresence (Location Server IP and Port are displayed in the FortiPresence GUI *Admin* > *Settings* > *Discovered APs*).
6. When you are finished, click *OK*.

FortiPresence push REST API

To configure FortiGate to push information to the FortiPresence server, enter the following commands:

```
config wireless-controller wtp-profile
   edit "FP223B-GuestWiFi"
      config lbs
         set fortipresence {disable | foreign | both}
         set fortipresence-server-addr-type {ipv4 | fqdn}
         set fortipresence-port <port>
         set fortipresence-secret <password> Password to be obtained from FortiPresence UI
         set fortipresence-project <name> Name to be obtained from FortiPresence UI
         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.
         set station-locate enable
      end
end
```

Configuring FortiPresence server IP

When defining the FortiPresence server for location based services, the server address can be configured as an IPV4 address or as a FQDN. Using FQDN means that the wireless controller configuration does not need to be changed when the FortiPresence server IP address changes, it can keep the same domain name.

To configure FortiPresence server as IPV4:

```
config wireless-controller wtp-profile
   edit "FAP431F-default"
      config lbs
         set fortipresence foreign
         set fortipresence-server-addr-type ipv4
         set fortipresence-server "34.245.252.61" (FortiPresence location server IP)
         set fortipresence-port 4013
      end
   next
end
```

Debug configurations:

From the FortiGate CLI:

```
diag sniffer packet <port> "host 34.245.252.61 and port 4013" 6 0 a
```

From the FortiAP CLI:

```
cw_diag -c fortipresence - show scanned fortipresence data from kernel
diag_sniffer br0 'host 34.245.252.61'
```

To configure FortiPresence server as FQDN:

```
config wireless-controller wtp-profile
   edit "FAP431F-default"
      config lbs
         set fortipresence foreign
         set fortipresence-server-addr-type fqdn
         set fortipresence-server-fqdn "test.fortipresence.com"
         set fortipresence-port 10443
      end
   next
end
```

To verify that FortiAP receives the FortiPresence server domain name and resolves the IP address:

```
FortiAP-431F # wcfg
WTP Configuration
       name                : FortiAP-431F
       ...
       fsm-state           : RUN 75
       wtp-ip-addr         : 10.19.20.20:5246 - 10.19.20.20:53582
       ac-ip-addr          : 172.18.56.42:5246 - 172.18.56.42:5247        STATIC
       ...
       fortipresence       : foreign, ble enabled, rogue disabled, unassoc_sta enabled, freq 30
                             server 0172.16.200.133(test.fortipresence.com):10443 secret csum [0xc6a7]
[fortipresence]
```

```
        LAN mode            : WAN LAN, ESL
        ...
```

Support for Electronic Shelf Label systems

Some FortiAP models equipped with a USB port can support Electronic Shelf Labels (ESL) systems. These FortiAPs can be configured to accept a ESL-Radio through a USB dongle that works on a 2.4 GHz frequency band. Once the ESL dongle is connected, you can configure the communication mode from a FortiGate. ESL traffic from the ESL-Radio is sent to ESL-Servers that are either located on-premise or in the Cloud.

Fortinet currently supports the following third-party ESL service providers:

- Hanshow
- SES-Imagotag

Hanshow integration

To configure ESL integration for Hanshow:

```
config wireless-controller wtp-profile
  edit "421E-dongle"
    config platform
      set type 421E
    end
    config lan
      set port-esl-mode bridge-to-ssid
      set port-esl-ssid "WIFI-Private"
    end
  next
end
```

The following configuration are available in `port-esl-mode`:

offline	Offline.
nat-to-wan	NAT WTP ESL port to WTP WAN port.
bridge-to-wan	Bridge WTP ESL port to WTP WAN port.
bridge-to-ssid	Bridge WTP ESL port to SSID.

Hanshow ESL is supported on select FortiAP models, including but not limited to:

- FortiAP-S/W2 models: FAP-S421E, FAP-S423E, FAP-421E and FAP-423E, running firmware 6.4.2 and later.
- FortiAP models: Wi-Fi 6/802.11ax capable, running firmware 6.4.3 and later.

SES-Imagotag

To configure ESL integration for SES-Imagotag:

```
config wireless-controller wtp-profile
  edit FAP433F-default
    config esl-ses-dongle
      set esl-channel 10
      set scd-enable enable
      set output-power b
      set apc-fqdn "example.fqdn"
      set apc-port 7354
    end
  next
end
```

The following configuration are available for `esl-ses-dongle`:

`compliance-level`	Compliance levels for the ESL solution integration: • -1: No esl-channel is set • 0: ESL channel 0 • <…> • 10: ESL channel 10 • 127: Managed channel enabled, indicates that the APC (server) is setting the esl-channel via the slot channel (default = compliance-level-2)
`scd-enable`	Enable/disable ESL SES-imagotag Serial Communication Daemon (SCD) (default = disable)
`esl-channel`	ESL SES-imagotag dongle channel (default = 127)
`output-power`	ESL SES-imagotag dongle output power: • a: About 15mW • b: About 7mW • c: About 5mW • d: About 1mW • e: About 13mW • f: About 10mW • g: About 3mW • h: About 2mW (default = A)
`apc-addr-type`	ESL SES-imagotag APC address type: • fqdn: Fully Qualified Domain Name address • ip IPv4: address (default = fqdn)
`apc-fqdn / apc-ip`	FQDN / IP of ESL SES-imagotag Access Point Controller

`apc-port`	Port of ESL SES-imagotag Access Point Controller
`coex-level`	ESL SES-imagotag dongle coexistence level (default = none). **Note:** As of today there is no coexistence, interference-free parallel operation with regular 2.4GHz servicing radios
`tls-cert-verification`	Enable/disable TLS Certificate verification (default = enable)
`tls-fqdn-verification`	Enable/disable TLS Certificate verification (default = disable)

To check the ESL dongle status:

On FortiOS:

```
diagnose wireless-controller wlac -c ws-esl [wtp-ip]
```

On FortiAP:

```
cw_diag -c esl-ses
```

To toggle ESL-SES debug level:

To see the the ESL log level on a FortiAP:

```
# cw_diag -c esl-dbg

# ----------------------ESL SCD debug conf----------------------
# (console-output: 0 - off, 1 - on)
console 0
# (debug-levels: 0 - none, 1 - fatal, 2 - error, 3 - warn, 4 - info, 5 - debug)
data_block.data_block_container 2
firmware.load_firmware 2
…
```

To enable debugs:

```
cw_diag -c esl-dbg console 1
```

To apply the level change, you need to restart the SDC daemon or reboot the FortiAP.

To set other debug object levels:

```
cw_diag -c esl-dbg firmware.load_firmware 3
```

Level "`3`" is "warn", which means "fatal", "error" and "warn" logs will be displayed for "`firmware.load_firmware`".

SES-Imagotag ESL is supported on Wi-Fi 6/802.11ax capable FortiAP models running firmware 7.0.1 and later.

Troubleshooting

This section contains topics to help troubleshoot the FortiOS wireless controller and FortiAP units.

- FortiAP shell command on page 399
- Signal strength issues on page 399
- Throughput issues on page 403
- Client connection issues on page 404
- FortiAP connection issues on page 406
- Testing wireless network health with SAM on page 409
- Determining the coverage area of a FortiAP on page 415
- Best practices for OSI common sources of wireless issues on page 417
- Extended logging on page 420
- Packet sniffer on page 430
- Debug commands on page 434
- Disabling 802.11d for client backward compatibility on page 435

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
```

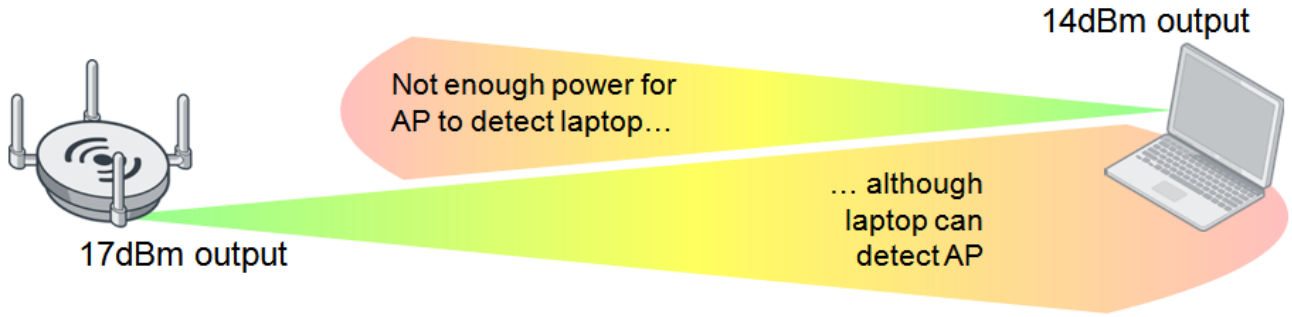
- **cmd-to-ap:** any shell commands, but FortiAP does not report results until the command is finished on the FortiAP
- **run:** controller sends the ap-cmd to the FortiAP to run
- **show:** show current results reported by the FortiAP in text
- **showhex:** show current results reported by the FortiAP 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 Signal Strength widget (under *Dashboard* > *WiFi*) 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:

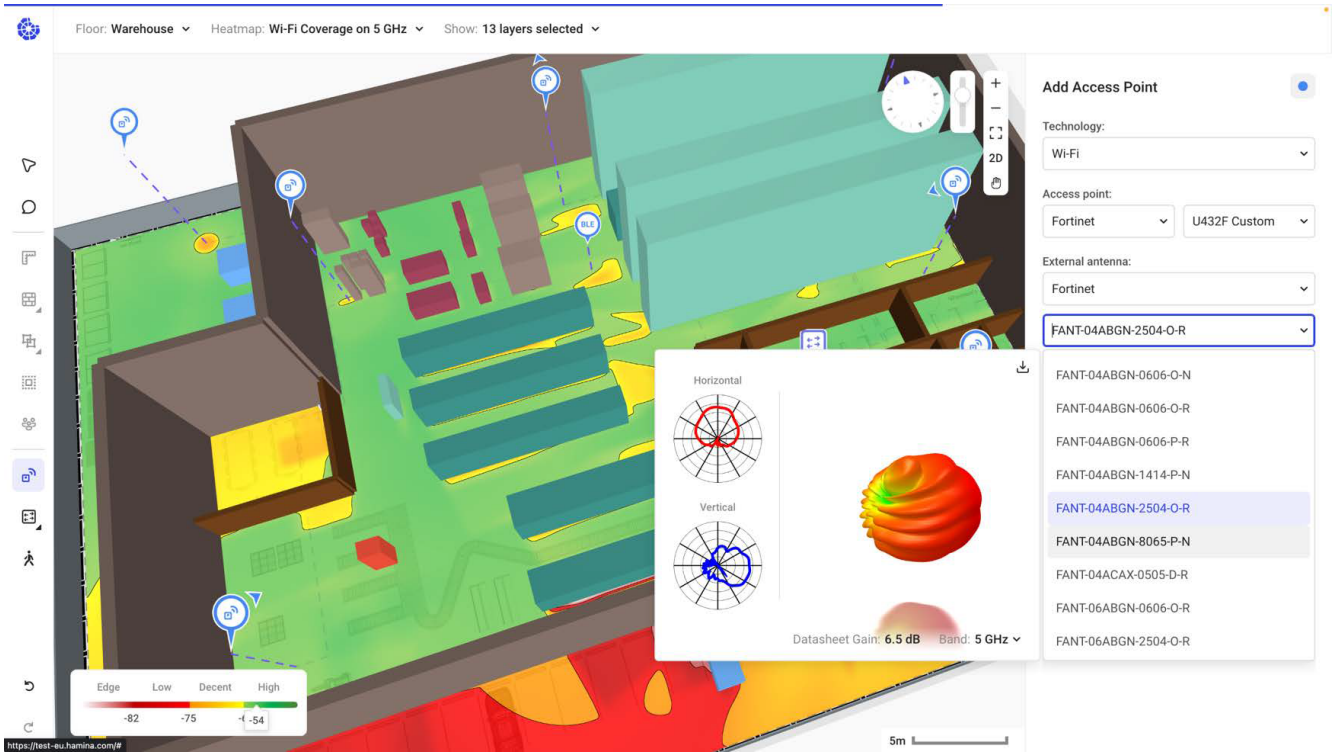
```
wlan00 IEEE 802.11ng ESSID:"signal-check"
Mode:Master Frequency:2.412 GHz   Access Point:<MAC add>
Bit Rate:130 Mb/s Tx-Power=28 dBm
```

Perform a site survey

The most thorough method to solve signal strength issues is to perform a site survey.

A 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. You can then overlay the floor plan with a Wi-Fi heat map, allowing you to map the APs and adjust the radio bands and power levels while providing you with visual wireless coverage.

Sample depiction of a site survey using Hamina Wireless Network Planner



The following 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 (Hamina Wireless Network Planner, Ekahau, AirMagnet Survey Pro, and etc.)
- 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).

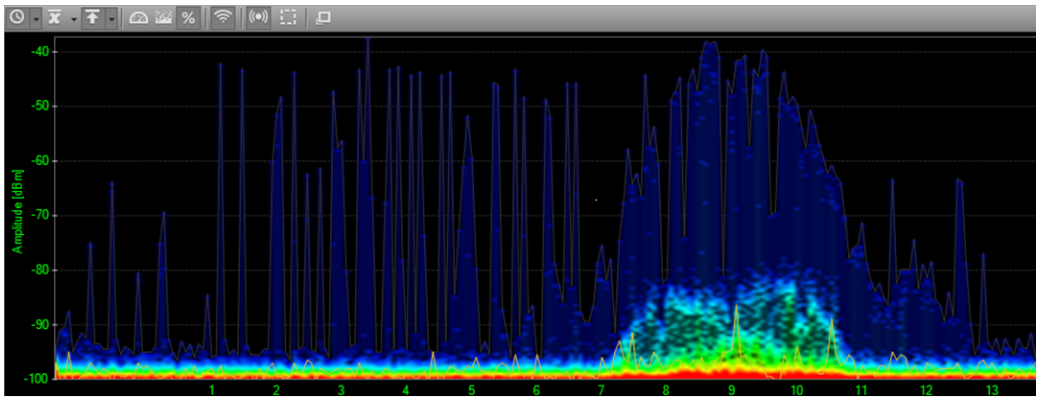
The most common and simple solution for frequency interference is to change your operation channel. Typically, the channel can be set from 1 to 11 for the broadcast frequency, although it is recommended to use channels 1, 6, and 11 on the 2.4 GHz band.

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

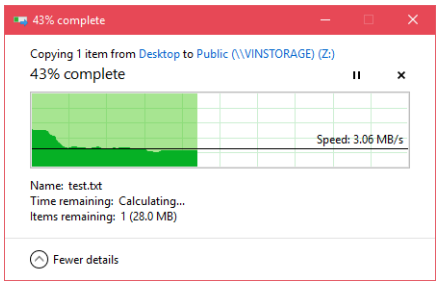
If the FortiAP gives poor throughput to the client, the link can drop. You can measure the link throughput or performance between two devices by using third-party application tools such as iPerf and jPerf.

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 230.

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:

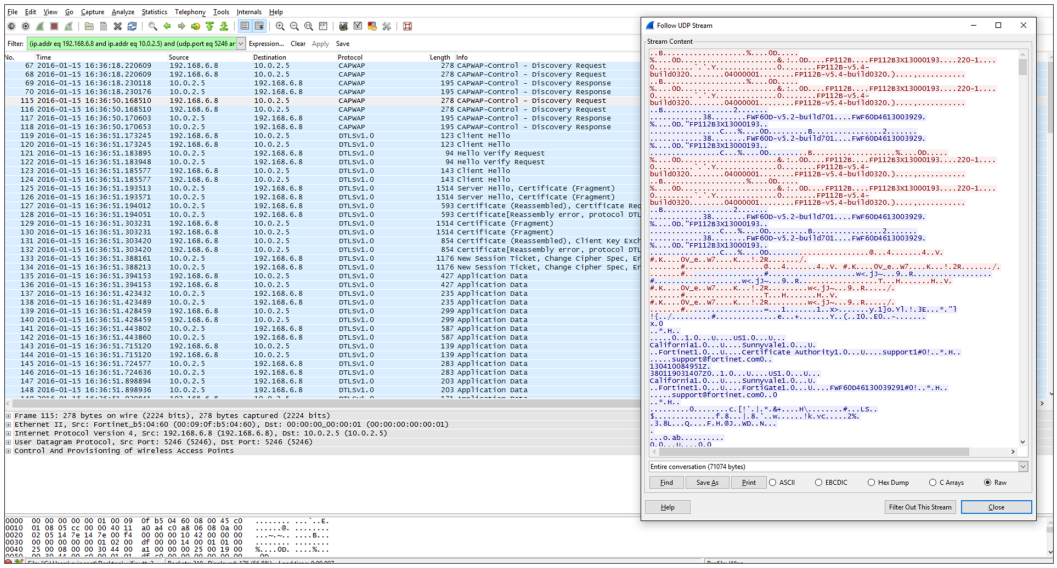
```
diagnose sniff packet <interface_name> "port 5246" 4
```

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 l
```

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.

Testing wireless network health with SAM

Fortinet's Service Assurance Manager (SAM) is a predictive diagnostic software for remotely diagnosing the health of wireless networks without requiring overlay sensors. With Service Assurance Manager, the network automatically performs predictive health checks and reports any issues before end users are impacted.

FortiAPs can be configured to run in Service Assurance Management mode, where a radio is designated to operate as a client and perform tests against another AP. Ping tests and Iperf tests can be run on interval, with results captured in the WiFi event logs. This allows the FortiGate to verify and ensure that an existing Wi-Fi network can provide acceptable services.

To configure a FortiAP profile to run in SAM mode - CLI:

In this example, a FortiGate manages two FortiAPs. One FortiAP (FAP_1) broadcasts a test SSID using WPA3 security, while the second FortiAP (FAP_2) is configured as a SAM test client with the same WPA3 security method so it can connect with the SSID on FAP_1 and perform a SAM ping or Iperf test.

1. (Optional) Upload the CA certificate to verify the server certificate.
   a. Go to System > Certificates > Create/Import > CA Certificate and complete the fields to upload the certificate.
2. (Optional) Upload the client certificate with private key file.
   a. Go to *System* > *Certificates* > *Create/Import* > *Certificate* and click *Import Certificate*.
   b. Select *Certificate* or *PKCS #12 Certificate*, then follow the onscreen instructions to import the client certificate with private key file, and set the private-key-password.
3. Create an SSID and select an authentication method:

WPA3 Enterprise authentication using EAP-TLS	WPA3-SAE authentication	OWE authentication
config wireless-controller vap edit "sam-test-ent3" set ssid "sam-test-ent3" **set security wpa3-only-enterprise** set pmf enable set auth radius	config wireless-controller vap edit "sam-test-sae" set ssid "sam-test-sae" **set security wpa3-sae** set pmf enable set schedule "always" set sae-password ENC next	config wireless-controller vap edit "sam-test-owe" set ssid "sam-test-owe" **set security owe** set pmf enable set schedule "always" next end

WPA3 Enterprise authentication using EAP-TLS	WPA3-SAE authentication	OWE authentication
set radius-server "eap_tls" set schedule "always" next end	end	

4. Broadcast the SSID on FAP_1:

WPA3 Enterprise authentication using EAP-TLS	WPA3-SAE authentication	OWE authentication
config wireless-controller wtp-profile edit "FAP433F-sam-test" config platform set type 433F set ddscan enable end config radio-2 set band 802.11ax-5G set vap-all manual **set vaps "sam-test-ent3"** end next end	config wireless-controller wtp-profile edit "FAP433F-sam-test " config platform set type 433F set ddscan enable end config radio-2 set band 802.11ax-5G set vap-all manual **set vaps "sam-test-sae"** end next end	config wireless-controller wtp-profile edit "FAP433F-sam-test" config platform set type 433F set ddscan enable end config radio-2 set band 802.11ax-5G set vap-all manual **set vaps "sam-test-owe"** end next end

5. Configure the AP profile for FAP_2 to run in SAM mode and select a SAM security type. Then enable a SAM ping or Iperf test:

SAM ping test with WPA3 Enterprise authentication using EAP-TLS	SAM Iperf test with WPA3-SAE authentication	SAM ping test with OWE authentication
If the SAM security type is set to `wpa-enterprise`, you can configure SAM EAP methods and SAM certificate settings: config wireless-controller wtp-profile edit "FAP431F-sam-ent3" config radio-2 set mode sam set sam-ssid "sam-test-ent3"	config wireless-controller wtp-profile edit "FAP431F-sam-sae" config radio-2 set mode sam set sam-ssid "sam-test-sae" **set sam-security-type wpa3-sae** set sam-password ENC **set sam-test iperf** set sam-server-ip	config wireless-controller wtp-profile edit "FAP431F-sam-owe" config radio-2 set mode sam set sam-ssid "sam-test-owe" **set sam-security-type owe** set sam-server-ip 8.8.8.8 **set sam-test ping** set sam-report-intv

SAM ping test with WPA3 Enterprise authentication using EAP-TLS	SAM Iperf test with WPA3-SAE authentication	SAM ping test with OWE authentication
set sam-security-type wpa-enterprise set sam-eap-method tls set sam-client-certificate "client2.cert" set sam-private-key "client2.cert" set sam-private-key-password ENC set sam-ca-certificate "CA_Cert_1" set sam-username "tester" set sam-password ENC **set sam-test ping** set sam-server-ip 8.8.8.8 set sam-report-intv 60 end next end	"172.18.56.99" set iperf-server-port 5201 set iperf-protocol tcp set sam-report-intv 60 end next end	60 end next end

When the "sam-eap-method" is "tls" or "both", the "sam-client-certificate", "sam-private-key", and "sam-private-key-password" settings are required.

- `sam-client-certificate`: The name of imported client certificate.
- `sam-private-key`: Uses the same name of imported client certificate.
- `sam-private-key-password`: Created when importing the client certificate.
- `sam-ca-certificate`: The name of the imported CA certificate.

6. Log in to the FAP_2 CLI to verify the configurations:

SAM ping test with WPA3 Enterprise authentication using EAP-TLS	SAM Iperf test with WPA3-SAE authentication	SAM ping test with OWE authentication
FortiAP-431F # rcfg < other output omitted > sam ssid : sam-test-ent3 sam bssid : 00:00:00:00:00:00 sam security type :	FortiAP-431F # rcfg sam ssid : sam-test-sae sam bssid : 00:00:00:00:00:00 sam security type : SAE sam captive portal :	FortiAP-431F # rcfg < other output omitted > sam ssid : sam-test-owe sam bssid : 00:00:00:00:00:00 sam security type : OWE

SAM ping test with WPA3 Enterprise authentication using EAP-TLS	SAM Iperf test with WPA3-SAE authentication	SAM ping test with OWE authentication
Enterprise sam captive portal : disabled sam test : **Ping** sam server : 8.8.8.8 sam report interval: 60 sam eap method : EAP TLS sam client cert : 1 sam ca cert : 1 < other output omitted >	disabled sam test : **Iperf** sam server : 172.18.56.99 sam report interval: 60 sam iperf port : 5201 sam iperf protocol : TCP < other output omitted >	sam captive portal : disabled sam test : **Ping** sam server : 8.8.8.8 sam report interval: 60 < other output omitted >

7. The FortiOS WiFi event log shows the corresponding event:

WPA3 Enterprise authentication using EAP-TLS	SAM Iperf test with WPA3-SAE authentication	SAM ping test with OWE authentication
1: date=2023-11-10 time=12:02:16 eventtime=1699646536236321385 tz="-0800" logid="0104043711" type="event" subtype="wireless" level="notice" vd="root" logdesc="SAM ping test result" sn="FP431FTF23031585" ap="FP431FTF23031585" vap="sam-test-ent3" ssid="sam-test-ent3" stamac="80:80:2c:0c:01:9f" radioid=2 channel=161 security="WPA3 Enterprise Only" encryption="AES" action="sam-ping-result" msg="Connected to AP FP433FTF20001556, 0.0% packet loss" remotewtptime="3012.616987"	1: date=2023-11-10 time=12:20:31 eventtime=1699647630989156870 tz="-0800" logid="0104043710" type="event" subtype="wireless" level="notice" vd="root" logdesc="SAM iperf test result" sn="FP431FTF23031585" ap="FP431FTF23031585" vap="sam-test-sae" ssid="sam-test-sae" stamac="80:80:2c:0c:01:9f" radioid=2 channel=161 security="WPA3 SAE" encryption="AES" action="sam-iperf-result" msg="Connected to AP FP433FTF20001556, TCP, max rate 0.6 MB/s" remotewtptime="11.468787"	1: date=2023-11-10 time=12:28:11 eventtime=1699648091131525936 tz="-0800" logid="0104043711" type="event" subtype="wireless" level="notice" vd="root" logdesc="SAM ping test result" sn="FP431FTF23031585" ap="FP431FTF23031585" vap="sam-test-owe" ssid="sam-test-owe" stamac="80:80:2c:0c:01:9f" radioid=2 channel=161 security="OWE" encryption="AES" action="sam-ping-result" msg="Connected to AP FP433FTF20001556, 0.0% packet loss" remotewtptime="469.609833"

Captive portal authentication in service assurance management (SAM) mode

When configuring a radio in service assurance management (SAM) mode, a client can be configured to authenticate with the captive portal. The captive portal match, success, and failure strings must be specified to automatically detect the authentication success or failure.

Example specification:

```
config wireless-controller wtp-profile
   edit <name>
      config radio-1
         set sam-cwp-username "wifi"
         set sam-cwp-password ENC
         set sam-cwp-test-url "www.fortinet.com"
         set sam-cwp-match-string "Login"
         set sam-cwp-success-string "Success"
         set sam-cwp-failure-string "again"
      end
   next
end
```

sam-cwp-username	Enter the username for captive portal authentication.
sam-cwp-password	Enter the password for captive portal authentication.
sam-cwp-test-url	Enter the website the client is trying to access.
sam-cwp-match-string	Enter the identification string from the captive portal login form.
sam-cwp-success-string	Enter the success identification text to appear on the page after a successful login.
sam-cwp-failure-string	Enter the failure identification text on the page after an incorrect login.

To perform a SAM test with captive portal authentication, create an SSID with captive portal authentication and broadcast it on a FortiAP (FAP_A). Then configure SAM with captive portal settings in the wtp-profile on a second FortiAP (FAP_B).

Configuring an SSID with captive portal authentication:

Configure the following steps on FAP_A.

1. Configure the RADIUS server:
```
config user radius
   edit "172.18.56.161"
      set server "172.18.56.161"
      set secret ENC
   next
end
```
2. Configure the VAP:
```
config wireless-controller vap
   edit "test-sam"
      set ssid "TEST-SAM"
```

```
      set security wpa3-sae
      set captive-portal enable
      set external-web "http://172.18.56.163/portal/index.php"
      set radius-server "172.18.56.161"
      set local-bridging enable
      set portal-type external-auth
      set schedule "always"
   next
end
```

3. Configure the FortiAP profile:

```
config wireless-controller wtp
   edit "FP423E3X16000020"   << A FAP423E is configured to broadcast test SSID.
      set uuid 404a75f2-c3ca-51eb-eb61-7678e900029c
      set admin enable
      set wtp-profile "FAP423E-default"
      config radio-1
         set override-vaps enable
         set vap-all manual
         set vaps "test-sam"
      end
      config radio-2
         set override-vaps enable
         set vap-all manual
      end
   next
end
```

Configuring SAM with captive portal settings:

Configure the following steps on FAP_B.

1. Configure the FortiAP profile:

```
config wireless-controller wtp-profile
   edit "FAP231E-default"
      config platform
         set type 231E
         set ddscan enable
      end
      set handoff-sta-thresh 55
      set allowaccess https ssh snmp
      config radio-1
         set mode sam
         set sam-ssid "TEST-SAM"
         set sam-captive-portal enable
         set sam-cwp-username "tester"
         set sam-cwp-password ENC
         set sam-cwp-test-url "https://www.fortinet.com"
         set sam-cwp-match-string "fgtauth"   << This string is a part of the URL of the
              Captive Portal redirect page.
         set sam-cwp-success-string "Fortinet"
         set sam-cwp-failure-string "failed"
         set sam-password ENC
         set sam-test ping
         set sam-server-type ip
         set sam-server-ip 8.8.8.8
         set sam-report-intv 60
```

```
        end
        config radio-2
           unset band
        end
        config radio-3
           set mode monitor
        end
     next
  end
```

2. Configure the managed FortiAP settings:

```
config wireless-controller wtp
   edit "FP231ETF20000449"
      set uuid 404c8e50-c3ca-51eb-f111-040b31b593a1
      set admin enable
      set wtp-profile "FAP231E-default"
      config radio-2
      end
   next
end
```

Check the managed FortiAP to verify SAM settings:

After a few minutes, check the FAP_B configuration in the managed FortiAP:

```
FortiAP-231E # rcfg
Radio 0: AP
...
   sam ssid : TEST-SAM
   sam bssid : 00:00:00:00:00:00
   sam security type : Open
   sam captive portal : enabled
   sam cwp test url : https://www.fortinet.com
   sam cwp match string : fgtauth
   sam cwp success string : Fortinet
   sam cwp failure string : failed
   sam test : Ping
   sam server : 8.8.8.8
   sam report interval: 60
   sam iperf port : 5001
   sam iperf protocol : UDP
...
```

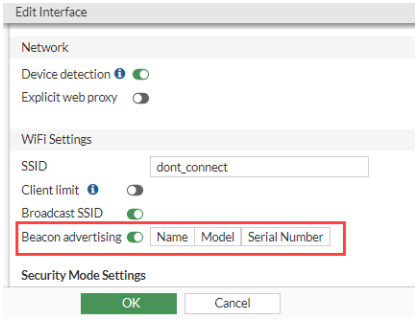
Determining the coverage area of a FortiAP

Vendor specific elements can be enabled by SSID and send out information about the FortiAP name, model and serial number. This allows wireless administrator performing site surveys to easily determine the coverage area of a FortiAP. The administrator can slowly move away from a FortiAP while continuously sniffing the beacons to determine if they can still hear from the FortiAP.

Another use case is to ensure that the FortiAP can be correctly identified during post-implementation wireless site surveys. This make troubleshooting and design improvements much easier.

To enable beacon advertising - GUI:

1. Go to *WiFi & Switch Controller* > *SSIDs* and select the SSID you want to enable Beacon advertising on.
2. Under *WiFi Settings*, enable *Beacon advertising* and select which element(s) you want to advertise:
   - *Name* - The FortiAP name.
   - *Model* - The FortiAP model.
   - *Serial Number* - The FortiAP serial number.



3. Click *OK* to save.

To enable beacon advertising - CLI:

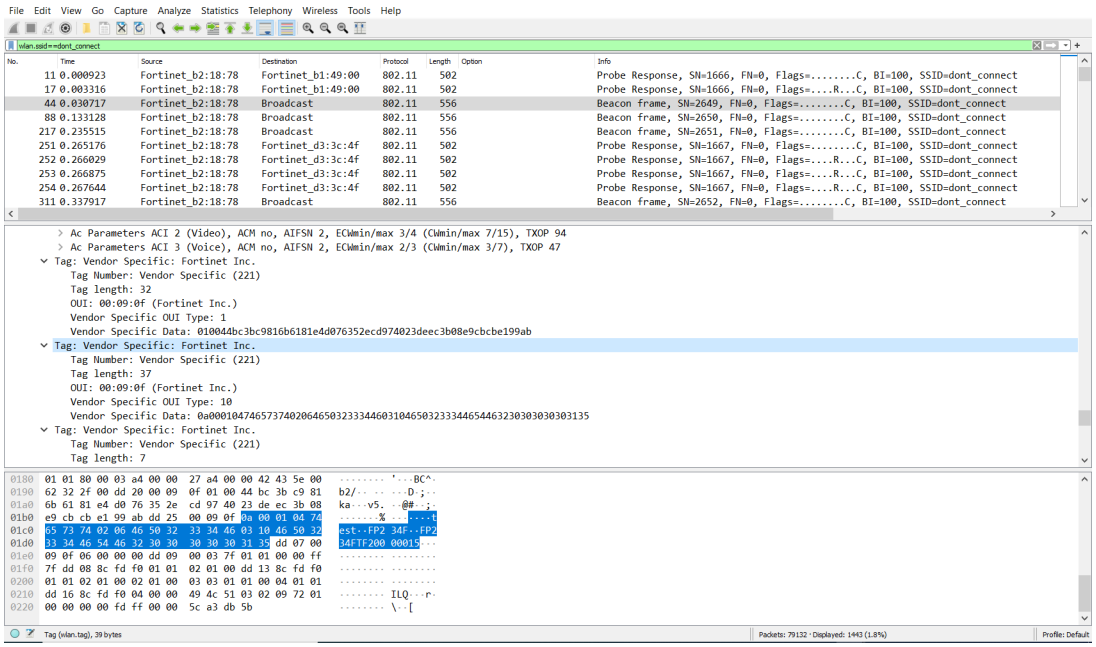
```
config wireless-controller vap
  edit "dont_connect"
    set ssid "dont_connect"
    set pmf enable
    set passphrase ENC ********
    set schedule "always"
    set quarantine disable
    set beacon-advertising name model serial-number
  next
end
```

The `beacon-advertising` setting can select up to three items (name, model and serial number).

To verify beacon advertising - CLI:

```
diag wireless wlac -c wlan dont_connect | grep "beacon advertising"
     beacon advertising        : name model sn
```

Upon sniffing the air packet, an additional field vendor specific Fortinet can be found in SSID beacon which has name of the advertising FAP (test), model 234F and serial number of 234F.

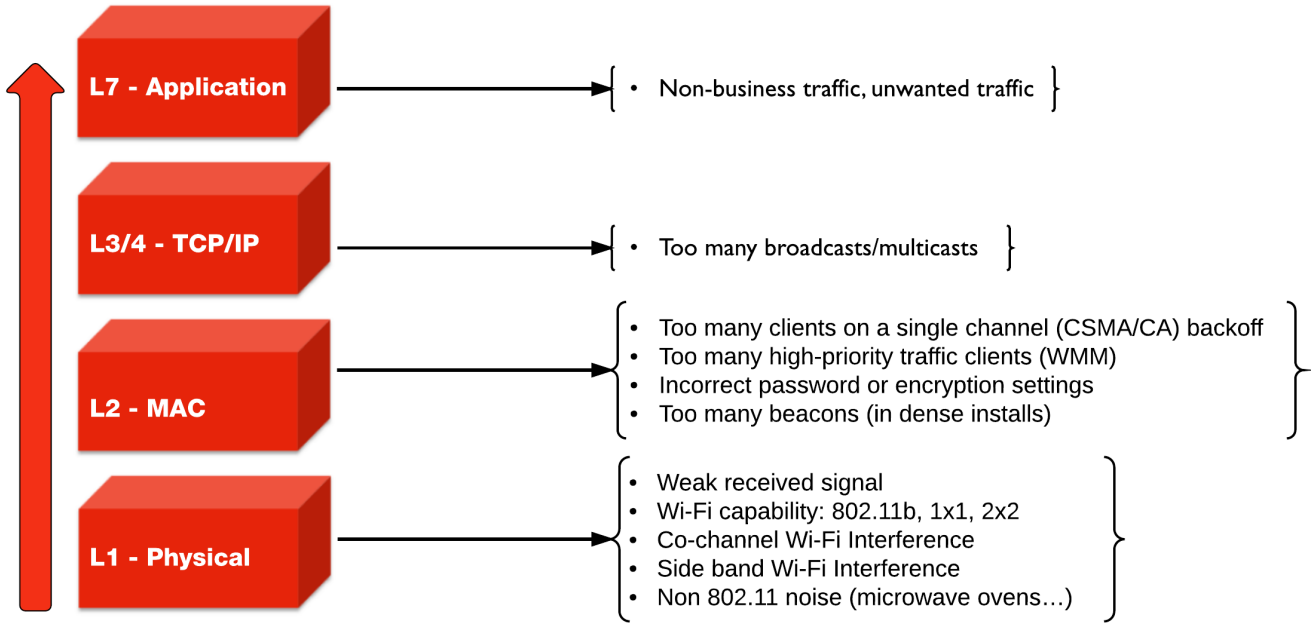


Best practices for OSI common sources of wireless issues

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:

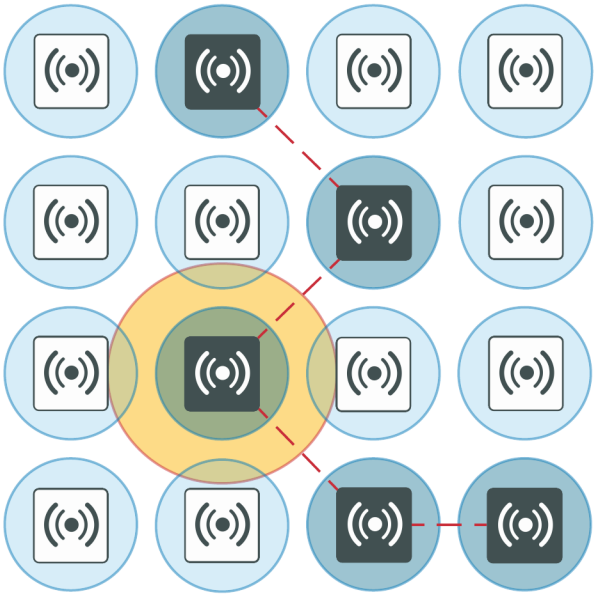
- Only use CCMP/AES (WPA2) encryption (not TKIP).
- In high-density deployments, turn off SSID broadcast or turn down SSID rates. Review and possibly reduce the beacon interval.
- Determine the best cell size for applications:
  - For few users and low bandwidth latency sensitive applications, use high-transmit power to create larger cells.
  - For high-performance and high-capacity installations, use lower transmit power to create smaller cells (set 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.

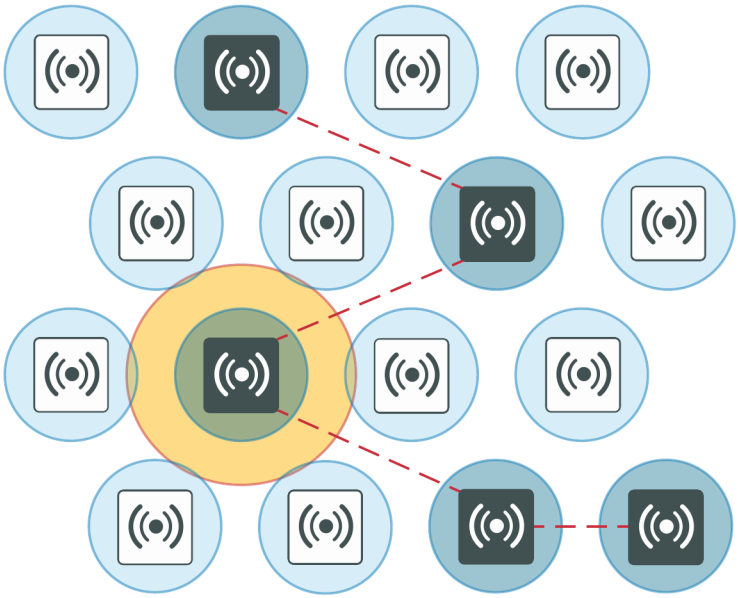
In the following diagram, note the interference zone created by one radio, causing interference on its neighboring APs.

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:

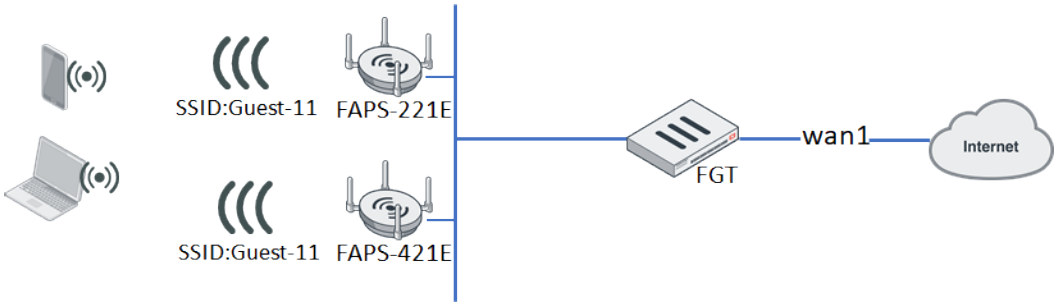
- identify business-critical applications
- use Application Control, Web Filtering, Traffic Shaping, and QoS to prioritize applications
  - Identify unwanted traffic, high-bandwidth web-related traffic, and use Security Profiles.
  - Use the traffic shaping on a policy to rate-limit this traffic.

  You perform these configurations directly on the FortiGate.

Extended logging

Extended logging information in these four key areas help WiFi troubleshooting: Association, Authentication, DHCP, and DNS.

The detailed wireless event logs show client connection procession to help IT administrators troubleshoot WiFi connection problems. The FortiAP can send more detailed events of client connections (such as probe, associate, authentication, 4-way handshake, DHCP), and FortiGate can create associated logs of these event.



New probe, authentication, and associate logs when wireless clients try to connect a broadcasted SSID with any security-mode

Probe request and response logs

Action	Description	Message	Detail
probe-req	Probe request from wireless station	AP received probe request frame from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:52 logid="0104043681" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="Probe request from wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="probe-req" reason="Reserved 0" msg="AP received probe request frame from client f0:98:9d:76:64:c4" remotewtptime="49.326391"

Action	Description	Message	Detail
probe-resp	Probe response to wireless station	AP sent probe response frame to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:52 logid="0104043682" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="Probe response to wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="probe-resp" reason="Reserved 0" msg="AP sent probe response frame to client f0:98:9d:76:64:c4" remotewtptime="49.326459"

Authentication request and response logs

Action	Description	Message	Detail
auth-req	Authentication request from wireless station	AP received authentication request frame from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043675" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Authentication request from wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="auth-req" reason="Reserved 0" msg="AP received authentication request frame from client f0:98:9d:76:64:c4" remotewtptime="44.902962"
auth-resp	Authentication response to wireless station	AP sent authentication response frame to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043676" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Authentication response to wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="auth-resp" reason="Reserved 0" msg="AP sent authentication response frame to client f0:98:9d:76:64:c4" remotewtptime="44.903038"

Associate request and response logs

Action	Description	Message	Detail
assoc-req	Association request from wireless station	AP received association request frame from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043677" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Association request from wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="assoc-req" reason="Reserved 0" msg="AP received association request frame from client f0:98:9d:76:64:c4" remotewtptime="44.915155"
assoc-resp	Association response to wireless station	AP sent association response frame to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043679" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Association response to wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="assoc-resp" reason="Reserved 0" msg="AP sent association response frame to client f0:98:9d:76:64:c4" remotewtptime="44.916829"

New WPA 4-Way handshake logs when wireless clients try to connect WPA2-Personal/WPA2-Enterprise SSID

Complete WPA 4-Way handshake logs

Action	Description	Message	Detail
WPA-1/4-key-msg	AP sent 1/4 message of 4 way handshake to wireless client	AP sent 1/4 message of 4-way handshake to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043650" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="AP sent 1/4 message of 4 way handshake to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-1/4-key-msg" reason="Reserved 0" msg="AP sent 1/4 message of 4-way handshake to client f0:98:9d:76:64:c4" remotewtptime="44.920791"

Action	Description	Message	Detail
WPA-2/4-key-msg	Wireless client sent 2/4 message of 4 way handshake	AP received 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043651" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Wireless client sent 2/4 message of 4 way handshake" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-2/4-key-msg" reason="Reserved 0" msg="AP received 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4" remotewtptime="44.926647"
WPA-3/4-key-msg	AP sent 3/4 message of 4 way handshake to wireless client	AP sent 3/4 message of 4-way handshake to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043652" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="AP sent 3/4 message of 4 way handshake to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-3/4-key-msg" reason="Reserved 0" msg="AP sent 3/4 message of 4-way handshake to client f0:98:9d:76:64:c4" remotewtptime="44.928406"
WPA-4/4-key-msg	Wireless client sent 4/4 message of 4 way handshake	AP received 4/4 message of 4-way handshake from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043653" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Wireless client sent 4/4 message of 4 way handshake" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-4/4-key-msg" reason="Reserved 0" msg="AP received 4/4 message of 4-way handshake from client f0:98:9d:76:64:c4" remotewtptime="44.933383"

Invalid 2/4 handshake logs with wrong PSK input

Action	Description	Message	Detail
WPA-invalid-2/4-key-msg	Wireless client 4 way handshake failed with invalid 2/4 message	Probably wrong password entered, invalid MIC in 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4	date=2019-01-31 time=16:41:02 logid="0104043648" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548981661 logdesc="Wireless client 4 way handshake failed with invalid 2/4 message" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=11 security="WPA2 Personal" encryption="AES" action="WPA-invalid-2/4-key-msg" reason="Reserved 0" msg="Probably wrong password entered, invalid MIC in 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4" remotewtptime="0.0"

New RADIUS authentication logs when clients connect WPA2-Enterprise with User-group or Radius-auth SSID

RADIUS authenticate success log when client pass authentication

Action	Description	Message	Detail
RADIUS-auth-success	Wireless client RADIUS authentication success	Wireless client RADIUS authentication success	date=2019-01-30 time=14:36:09 logid="0104043630" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548887768 logdesc="Wireless client RADIUS authentication success" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="RADIUS-auth-success" reason="Reserved 0" msg="Client f0:98:9d:76:64:c4 RADIUS authentication success" remotewtptime="0.0"

RADIUS authenticate failure log when client fails to pass authentication

Action	Description	Message	Detail
RADIUS-auth-failure	Wireless client RADIUS authentication failure	Client f0:98:9d:76:64:c4 RADIUS authentication failure	date=2019-01-30 time=14:35:51 logid="0104043629" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548887750 logdesc="Wireless client RADIUS authentication failure" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="RADIUS-auth-failure" reason="Reserved 0" msg="Client f0:98:9d:76:64:c4 RADIUS authentication failure" remotewtptime="0.0"

New RADIUS MAC authentication logs when clients try to connect a SSID with radius-mac-auth enabled

RADIUS MAC authenticate success log when client passes RADIUS MAC authentication

Action	Description	Message	Detail
RADIUS-MAC-auth-success	Wireless client RADIUS MAC authentication success	Client b4:ae:2b:cb:d1:72 RADIUS MAC authentication success	date=2019-01-30 time=15:54:40 logid="0104043633" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548892477 logdesc="Wireless client RADIUS MAC authentication success" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="b4:ae:2b:cb:d1:72" channel=6 security="WPA2 Personal" encryption="AES" action="RADIUS-MAC-auth-success" reason="Reserved 0" msg="Client b4:ae:2b:cb:d1:72 RADIUS MAC authentication success" remotewtptime="0.0"

RADIUS MAC authenticate failure log when client fails to pass RADIUS MAC authentication

Action	Description	Message	Detail
RADIUS-MAC-auth-success	Wireless client RADIUS MAC authentication success	Client 1c:87:2c:b6:a8:49 RADIUS MAC authentication failure	date=2019-01-30 time=15:47:42 logid="0104043632" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548892061 logdesc="Wireless client RADIUS MAC authentication failure" sn="FP320C3X17001909" ap="320C-TEST" vap="stability3" ssid="Guest-11" radioid=2 stamac="1c:87:2c:b6:a8:49" channel=40 security="WPA2 Personal" encryption="AES" action="RADIUS-MAC-auth-failure" reason="Reserved 0" msg="Client 1c:87:2c:b6:a8:49 RADIUS MAC authentication failure" remotewtptime="0.0"

New DHCP logs when clients try to acquire IP after connected

Complete DHCP Discover/Offer/Request/ACK logs

Action	Description	Message	Detail
DHCP-DISCOVER	Wireless station sent DHCP DISCOVER	DHCP DISCOVER from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043663" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Wireless station sent DHCP DISCOVER" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-DISCOVER" reason="N/A" msg="DHCP DISCOVER from client f0:98:9d:76:64:c4" remotewtptime="45.123652"
DHCP-OFFER	DHCP server sent DHCP OFFER	DHCP OFFER of IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:49 logid="0104043664" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886189 logdesc="DHCP server sent DHCP OFFER" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-OFFER" reason="N/A" msg="DHCP OFFER of IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4" remotewtptime="46.156969"

Action	Description	Message	Detail
DHCP-REQUEST	Wireless station sent DHCP REQUEST	DHCP REQUEST for IP 11.10.80.2 offered by server 11.10.80.1 from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:50 logid="0104043666" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="Wireless station sent DHCP REQUEST" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-REQUEST" reason="N/A" msg="DHCP REQUEST for IP 11.10.80.2 offered by server 11.10.80.1 from client f0:98:9d:76:64:c4" remotewtptime="47.243792"
DHCP-ACK	DHCP server sent DHCP ACK	DHCP ACK for IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:50 logid="0104043667" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="DHCP server sent DHCP ACK" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-ACK" reason="N/A" msg="DHCP ACK for IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4" remotewtptime="47.246381"

Error logs when DHCP failure happens

Action	Description	Message	Detail
DHCP-NAK	DHCP server sent DHCP NAK	IP address not assigned, DHCP NAK from server 11.10.80.1 for client b4:ae:2b:cb:d1:72	date=2019-01-30 time=15:22:08 logid="0104043661" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548890528 logdesc="DHCP server sent DHCP NAK" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-NAK" reason="requested address not available" msg="IP address not assigned, DHCP NAK from server 11.10.80.1 for client b4:ae:2b:cb:d1:72" remotewtptime="289.83561"
DHCP-no-response	Wireless station DHCP process failed with no server response	DHCP server not responding for client b4:ae:2b:cb:d1:72	date=2019-02-01 time=10:39:07 logid="0104043658" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549046347 logdesc="Wireless station DHCP process failed with no server response" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-no-response" reason="N/A" msg="DHCP server not responding for client b4:ae:2b:cb:d1:72" remotewtptime="457.629929"

Action	Description	Message	Detail
DHCP-no-ACK	No DHCP ACK from server	No DHCP ACK for IP 11.10.80.3 requested by client b4:ae:2b:cb:d1:72	date=2019-02-01 time=10:38:56 logid="0104043660" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549046336 logdesc="No DHCP ACK from server" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-no-ACK" reason="N/A" msg="No DHCP ACK for IP 11.10.80.3 requested by client b4:ae:2b:cb:d1:72" remotewtptime="448.236740"
DHCP-self-assigned-IP	Wireless station is using self-assigned IP	Detected self assigned IP 169.254.210.208 of client b4:ae:2b:cb:d1:72	date=2019-02-01 time=10:38:51 logid="0104043670" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549046330 logdesc="Wireless station is using self-assigned IP" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-self-assigned-IP" reason="N/A" msg="Detected self assigned IP 169.254.210.208 of client b4:ae:2b:cb:d1:72" remotewtptime="441.742363"

New GTK-Rekey logs when clients perform gtk-rekey

Action	Description	Message	Detail
WPA-group-1/2-key-msg	AP sent 1/2 message of group key handshake to wireless client	AP sent 1/2 message of group key handshake to client f0:98:9d:76:64:c4	date=2019-01-30 time=15:12:01 logid="0104043654" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548889920 logdesc="AP sent 1/2 message of group key handshake to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="WPA-group-1/2-key-msg" reason="Reserved 0" msg="AP sent 1/2 message of group key handshake to client f0:98:9d:76:64:c4" remotewtptime="3778.128070"
WPA-group-2/2-key-msg	Wireless client sent 2/2 message of group key handshake	AP received 2/2 message of group key handshake from client f0:98:9d:76:64:c4	date=2019-01-30 time=15:12:01 logid="0104043655" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548889920 logdesc="Wireless client sent 2/2 message of group key handshake" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="WPA-group-2/2-key-msg" reason="Reserved 0" msg="AP received 2/2 message of group key handshake from client f0:98:9d:76:64:c4" remotewtptime="3778.228253"

New Fast-BSS-Transition (FT) logs when 802.11r clients roam between 2 FAPs

FT logs when clients succeed to roaming

Action	Description	Message	Detail
FT-action-req	Wireless client sent FT action request	AP received FT action request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043642" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="Wireless client sent FT action request" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=1 security="WPA2 Personal" encryption="AES" action="FT-action-req" reason="Reserved 0" msg="AP received FT action request frame from client f0:98:9d:76:64:c4" remotewtptime="146.847041"
FT-action-resp	FT action response was sent to wireless client	AP sent FT action response frame to client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043643" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="FT action response was sent to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=1 security="WPA2 Personal" encryption="AES" action="FT-action-resp" reason="Reserved 0" msg="AP sent FT action response frame to client f0:98:9d:76:64:c4" remotewtptime="146.849137"
FT-reassoc-req	Wireless client sent FT re-association request	AP received FT re-association request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043646" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="Wireless client sent FT reassociation request" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=40 security="WPA2 Personal" encryption="AES" action="FT-reassoc-req" reason="Reserved 0" msg="AP received FT reassociation request frame from client f0:98:9d:76:64:c4" remotewtptime="146.899110"
FT-reassoc-resp	FT re-association response was sent to wireless client	AP sent FT re-association response frame to client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043647" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="FT reassociation response was sent to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=40 security="WPA2 Personal" encryption="AES" action="FT-reassoc-resp" reason="Reserved 0" msg="AP sent FT reassociation response frame to client f0:98:9d:76:64:c4" remotewtptime="146.904372"

Action	Description	Message	Detail
FT-auth-req	Wireless client sent FT auth request	AP received FT authentication request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:18 logid="0104043644" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548982158 logdesc="Wireless client sent FT auth request" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-auth-req" reason="Reserved 0" msg="AP received FT authentication request frame from client f0:98:9d:76:64:c4" remotewtptime="1805.311496"
FT-auth-resp	FT auth response was sent to wireless client	AP sent FT authentication response frame to client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:18 logid="0104043645" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548982158 logdesc="FT auth response was sent to wireless client" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-auth-resp" reason="Reserved 0" msg="AP sent FT authentication response frame to client f0:98:9d:76:64:c4" remotewtptime="1805.312777"

Error logs when FT failure

Action	Description	Message	Detail
FT-invalid-action-req	Wireless client sent invalid FT action request	Receive invalid FT request action frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:17 logid="0104043639" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548982157 logdesc="Wireless client sent invalid FT action request" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-invalid-action-req" reason="Reserved 0" msg="Receive invalid FT request action frame from client f0:98:9d:76:64:c4" remotewtptime="0.0"
FT-invalid-auth-req	Wireless client sent invalid FT auth request	Receive invalid FT authentication request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:18 logid="0104043640" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548982157 logdesc="Wireless client sent invalid FT auth request" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-invalid-auth-req" reason="Reserved 0" msg="Receive invalid FT authentication request frame from client f0:98:9d:76:64:c4" remotewtptime="0.0"

New DNS error logs in DNS service failure

Action	Description	Message	Detail
DNS-no-domain	Wireless station DNS process failed due to non-existing domain	DNS lookup of uop.umeng.com from client 3c:2e:ff:83:91:33 failed with \"non-existing domain\"	date=2019-02-01 time=09:42:03 logid="0104043673" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549042922 logdesc="Wireless station DNS process failed due to non-existing domain" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="3c:2e:ff:83:91:33" security="WPA2 Personal" encryption="AES" action="DNS-no-domain" reason="Server 100.100.16.172 replied \"non-existing domain\"" msg="DNS lookup of uop.umeng.com from client 3c:2e:ff:83:91:33 failed with \"non-existing domain\"" remotewtptime="1130.445518"

Packet sniffer

Capturing the traffic between the controller and the FortiAP can help you identify most FortiAP and client connection issues. There are two ways to sniff traffic:

- CAPWAP packet sniffer on page 430
- Wireless traffic packet sniffer on page 431

CAPWAP packet sniffer

One method consists of sniffing the CAPWAP traffic.

- Enable plain control on the wireless 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:

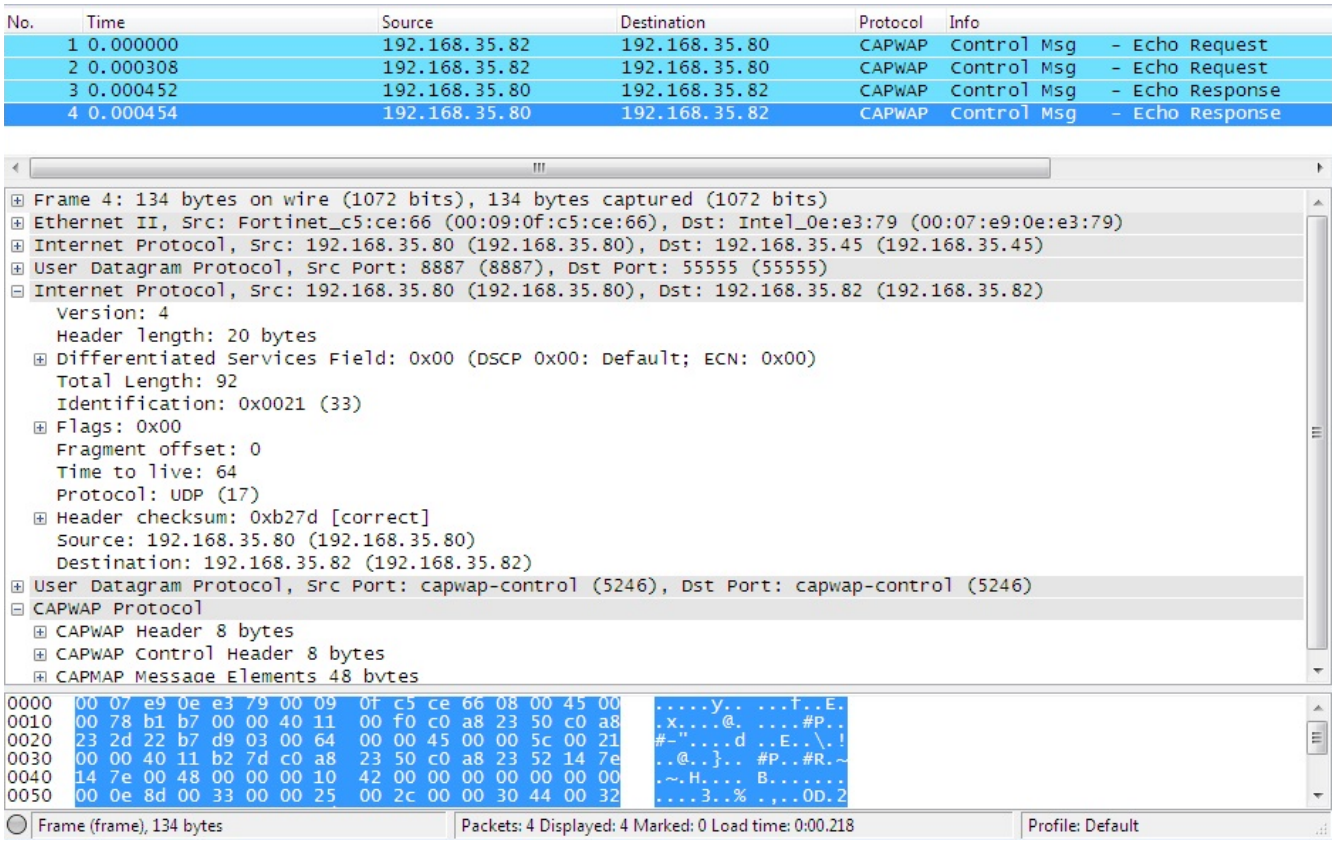
   WTP 0-FortiAP2223X11000107 Sniff: intf port2 enabled (control and data message)

   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 other method consists of sniffing the wireless traffic directly on the air using your FortiAP.

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 FortiAP radio to sniffer mode (configurable from the CLI only). Sniffer mode can capture all frame types and provides options to filter for specific traffic to capture. Notice that you can determine the buffer size, which channel to sniff, the channel width, 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 {integer}
      set ap-sniffer-chan {integer}
      set ap-sniffer-chan-width [320MHz|160MHz|80MHz|...]
      set ap-sniffer-addr {mac-address}
      set ap-sniffer-mgmt-beacon [enable|disable]
      set ap-sniffer-mgmt-probe [enable|disable]
      set ap-sniffer-mgmt-other [enable|disable]
      set ap-sniffer-ctl [enable|disable]
      set ap-sniffer-data [enable|disable]
    end
  next
end
```

Once you configure the radio and apply the profile to a FortiAP device, you can see the packet sniffer mode selected in the GUI dashboard under *WiFi and Switch Controller > FortiAP Profiles* and *WiFi and Switch Controller > Managed FortiAPs*. 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:

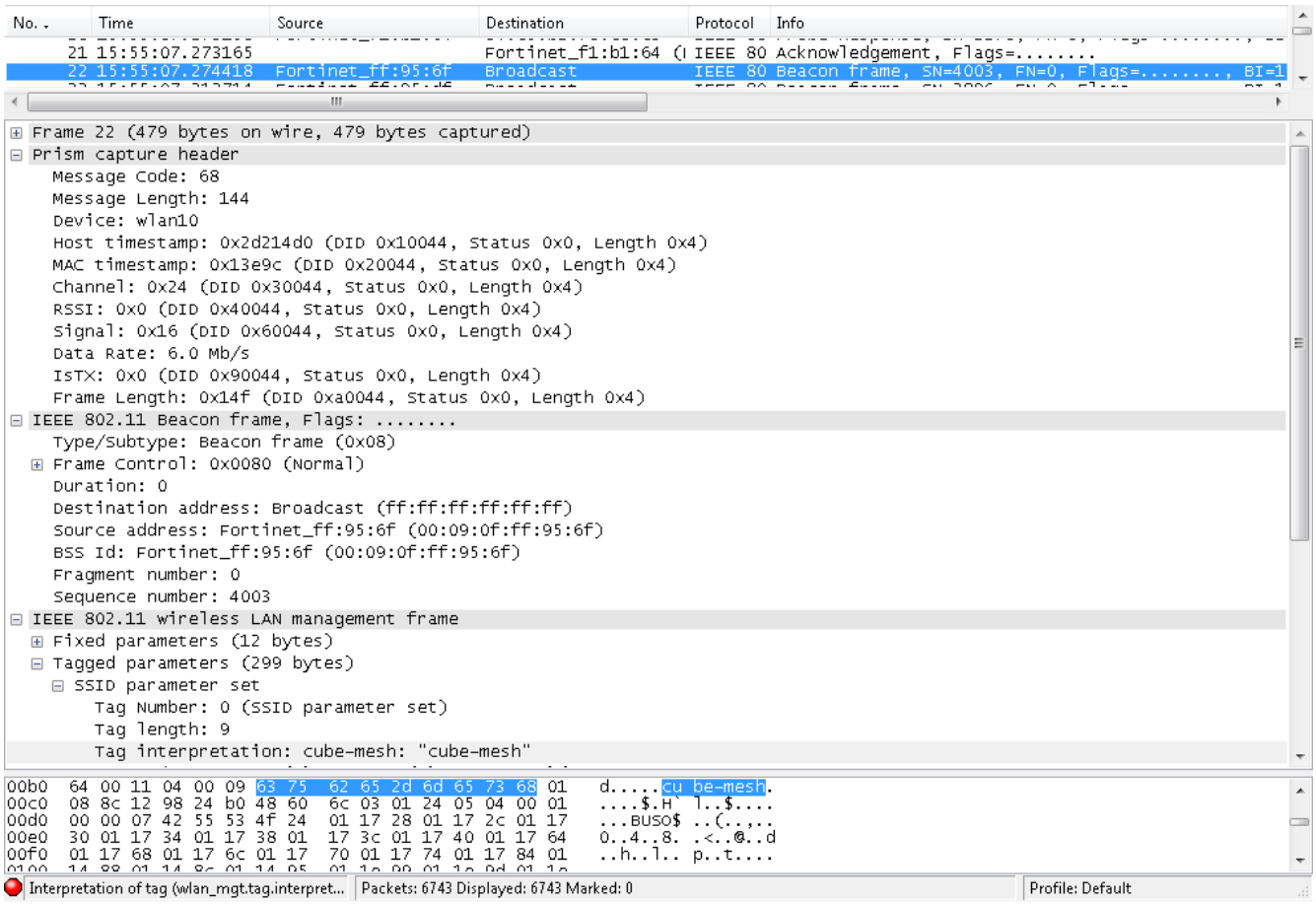
```
config wireless-controller wtp-profile
   edit <profile_name>
      config <radio>
         set ap-sniffer-mgmt-beacon disable
         set ap-sniffer-mgmt-probe disable
         set ap-sniffer-mgmt-other disable
         set ap-sniffer-ctl disable
         set ap-sniffer-data disable
      end
end
```

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).

Disabling 802.11d for client backward compatibility

By default, 802.11d is always enabled on FortiAPs. When 802.11d is enabled, FortiAPs broadcast the country code in beacons, probe responses, and probe requests. This can lead to some older legacy clients failing to associate to the FortiAP. You can disable 802.11d to prevent broadcasting country code settings and provide backwards compatibility with those clients

Since IEEE 802.11d only applies to 2.4 GHz radios operating in the 802.11g band, disabling 802.11d only applies to radios configured to operate in the 802.11g band.

To disable 802.11d:

```
config wireless-controller wtp-profile
  edit FAP231F-default
    config radio-1
    set 80211d disable
  end
end
```

To verify the configuration from FortiGate:

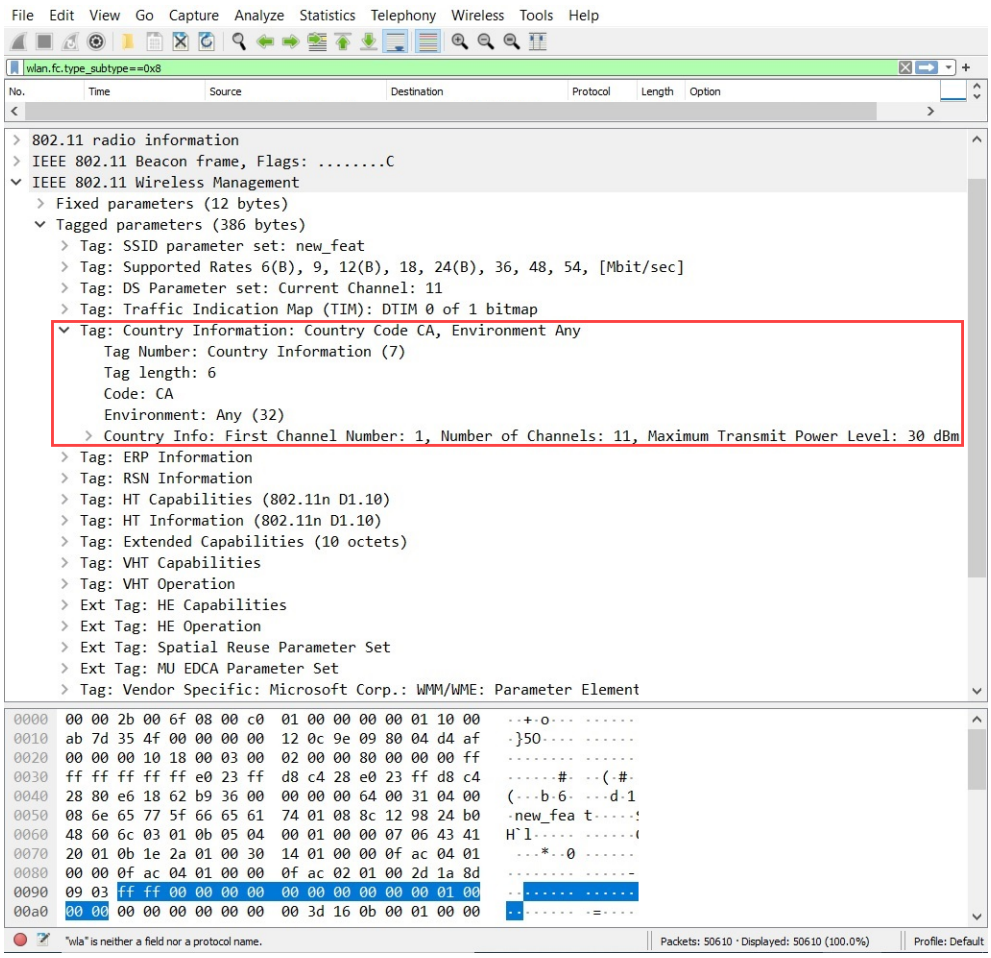
1. From the FortiGate:

```
diagnose wireless-controller wlac -c wtp FP231FTF20007509 | grep 80211d
   80211d enable : disabled
```

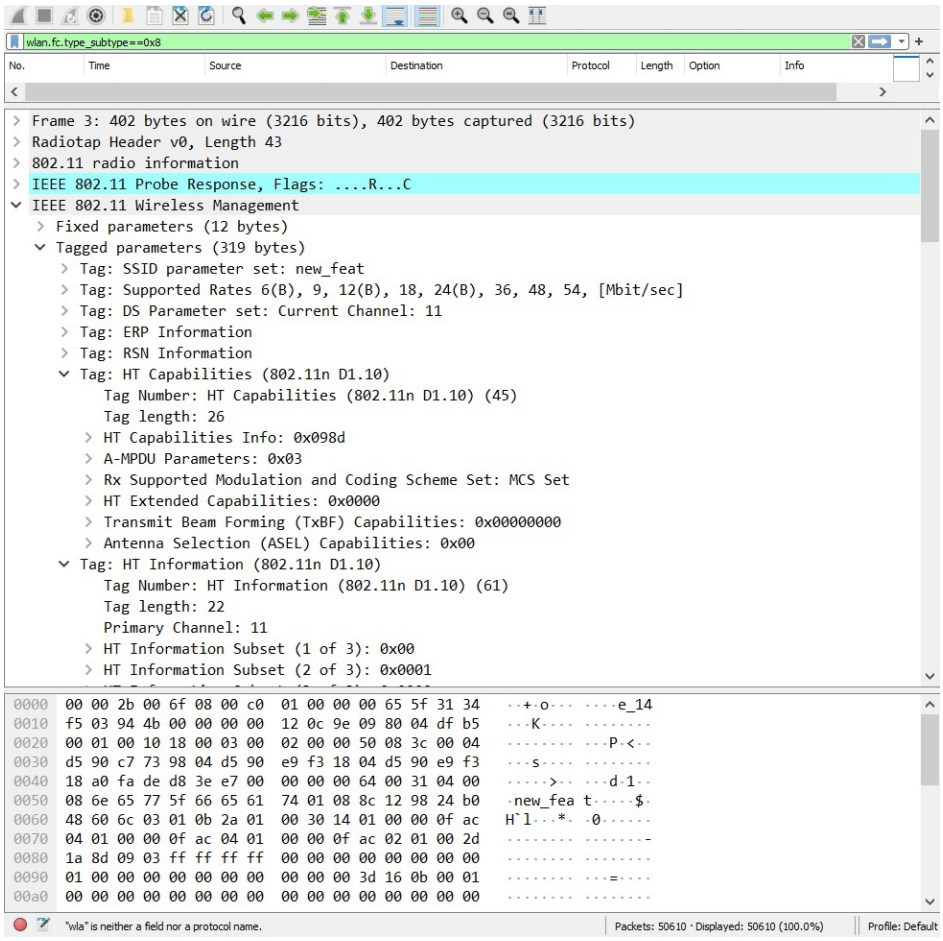
2. When the previous FortiGate setting are applied to a Managed FortiAP, the settings can be verified on the FortiAP CLI through the `rcfg` and `iwpriv` commands:

```
FortiAP-231F # rcfg | grep 802
   802.11d enable : disabled
FortiAP-231F #

Check iwpriv

FortiAP-231F # iwpriv wlan00 get_countryie
wlan00 get_countryie:0 (0x0)
FortiAP-231F #
```

3. Sniff the packets in the air before and after disabling the feature:
   a. Before enabling the feature, use a packet analyzer to check the sample beacon packet for the *Country Information* Tag in *Tagged parameters*.



b. After disabling the 802.11d on a 2.4Ghz radio, use a packet analyzer to check the beacon and verify that the *Country Information* Tag is no longer under in *Tagged Parameters.*


wlan.fc.type_subtype==0x8
No.
Time
Source
Destination
Protocol
Length
Option
Info
Frame 3: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits)
Radiotap Header v0, Length 43
802.11 radio information
IEEE 802.11 Probe Response, Flags: ....R...C
IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Tagged parameters (319 bytes)
Tag: SSID parameter set: new_feat
Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
Tag: DS Parameter set: Current Channel: 11
Tag: ERP Information
Tag: RSN Information
Tag: HT Capabilities (802.11n D1.10)
Tag Number: HT Capabilities (802.11n D1.10) (45)
Tag length: 26
HT Capabilities Info: 0x098d
A-MPDU Parameters: 0x03
Rx Supported Modulation and Coding Scheme Set: MCS Set
HT Extended Capabilities: 0x0000
Transmit Beam Forming (TxBF) Capabilities: 0x00000000
Antenna Selection (ASEL) Capabilities: 0x00
Tag: HT Information (802.11n D1.10)
Tag Number: HT Information (802.11n D1.10) (61)
Tag length: 22
Primary Channel: 11
HT Information Subset (1 of 3): 0x00
HT Information Subset (2 of 3): 0x0001
0000 00 00 2b 00 6f 08 00 c0 01 00 00 00 65 5f 31 34
0010 f5 03 94 4b 00 00 00 00 12 0c 9e 09 80 04 df b5
0020 00 01 00 10 18 00 03 00 02 00 00 50 08 3c 00 04
0030 d5 90 c7 73 98 04 d5 90 e9 f3 18 04 d5 90 e9 f3
0040 18 a0 fa de d8 3e e7 00 00 00 00 64 00 31 04 00
0050 08 6e 65 77 5f 66 65 61 74 01 08 8c 12 98 24 b0
0060 48 60 6c 03 01 0b 2a 01 00 30 14 01 00 00 0f ac
0070 04 01 00 00 0f ac 04 01 00 00 0f ac 02 01 00 2d
0080 1a 8d 09 03 ff ff ff ff 00 00 00 00 00 00 00 00
0090 01 00 00 00 00 00 00 00 00 00 00 3d 16 0b 00 01
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
"wla" is neither a field nor a protocol name.
Packets: 50610 · Displayed: 50610 (100.0%)
Profile: Default

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 201.

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`	Supported data channel security policies. clear - Clear text dtls - DTLS (encrypted) ipsec - IPsec VPN ipsec-sn - IPsec VPN that includes the FortiAP serial number.
`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

Variable	Description and value
	7- FortiCloud
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 33. Default: 0.
AP_MODE	FortiAP operating mode. 0 - Thin AP 2 - Unmanaged Site Survey mode. See SURVEY variables. Default: 0.

Variable	Description and value
BAUD_RATE	Console data rate: 9600, 19200, 38400, 57600, or 115200 baud. 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).
FIPS_CC	Enable Federal Information Processing Standards (FIPS) mode on FortiAP models. 1 - Enable FIPS mode. To disable FIPS mode, factory reset the FortiAP. **Note:** FAP-431F and FAP-433F do not support FIPS mode.
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
TPM	Wi-Fi 6E Models only: Enable Trusted Platform Module (TPM). 1 - Enable TPM 0 - Disable TPM Default : 0.
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
WAN_1X_ENABLE	Enable or Disable WAN port 802.1x supplicant: • 0: Disabled

Variable	Description and value
	• 1: Enabled The default setting is 0.
WAN_1X_USERID	WAN port 802.1x supplicant user ID.
WAN_1X_PASSWD	WAN port 802.1x supplicant password.
WAN_1X_MACSEC_POLICY	Can only be configured when WAN_1X_ENABLE = 1 Enable or Disable MACsec locally: • 0: Disabled • 1: Enabled The default setting is 0.
WAN_1X_METHOD	Select an EAP method for the WAN port 802.1x supplicant: • 0: EAP-ALL • 1: EAP-FAST • 2: EAP-TLS • 3: EAP-PEAP The default setting is 0.
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.
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_BSSID	WiFi MAC address.
MESH_AP_PASSWD	Pre-shared key for mesh backhaul.
MESH_AP_SCANCHANLIST	Specify those channels to be scanned.
MESH_AP_SECURITY	Configure the security mode of a mesh-backhaul SSID.

Variable	Description and value
	0 - Open 1 - WPA/WPA2-Personal 2 - WPA3-SAE Default: 0.
MESH_AP_SSID	SSID for mesh backhaul. Default: fortinet.mesh.root.
MESH_AP_TYPE	Type of communication for backhaul to controller: 0 - Ethernet 1 - WiFi mesh 2 - Ethernet with mesh backup support Default: 0.
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).
SURVEY_TX_POWER_24	2.4 GHz transmitter power used for site survey SSID in dBm. Default=30.
SURVEY_TX_POWER_50	5 GHz transmitter power used for site survey SSID in dBm. Default=30.
SURVEY_TX_POWER_60	6 GHz transmitter power used for site survey SSID in dBm. Default=30.
SURVEY_BEACON_INTV	Site survey beacon interval in seconds. Default: 100 ms.

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_CH_60	Site survey transmit channel for the 6 GHz band. Default: 36.
SURVEY_CW_24	2.4 GHz channel-bonding bandwidth for site survey SSID. 0 - 20MHz 1 - 40MHz Default=0
SURVEY_CW_50	5 GHz channel-bonding bandwidth for site survey SSID. 0 - 20MHz 1 - 40MHz 2 - 80MHz 3 - 160MHz Default=0
SURVEY_CW_60	6 GHz channel-bonding bandwidth for site survey SSID. 0 - 20MHz 1 - 40MHz 2 - 80MHz 3 - 160MHz Default=0

Diagnostics commands

Command	Description
fap-tech	Shows a consolidated log command output for debugging purposes.
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 debug ping_ac	Enable AC IP ping check and set the ping interval (disabled by default).
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.

Command	Description
`cw_diag wlanfw-dump <TFTP server IP>`	Upload Target Assert logs to a specified TFTP server.
`cw_diag -c acs-chan-stats`	Check the real-time status of CAPWAP connections to the AP controllers (AC).
`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 bonjour`	Show the current Bonjour gateway configuration in the control plane.
`cw_diag -c darrp`	Show the DARRP radio channel.
`cw_diag -c fortipresence`	Show FortiPresence statistics including reported BLE devices.
`cw_diag -c k-lan-host`	Display wired client information for clients connected to LAN2 of the FortiAP
`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.
`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 temperature`	Show operating temperature of the FortiAP CPU.
`cw_diag -c vap-cfg`	Show the current VAPs in the control plane.
`cw_diag -c vlan-probe-cmd <action> <interface ID> <start Vlan ID> <end Vlan ID> <retry> <timeout>`	Start the VLAN probe. "Action" value list: • `0` - start • `1` - stop

Command	Description
	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 wan1x`	Show WAN 802.1x supplicant configuration. • get-ca-cert • get-client-cert • get-private-key `cw_diag -c wan1x [show-ca-cert|show-client-cert|del-all|del-ca-cert|del-client-cert|del-private-key|[<get-ca-cert|get-client-cert|get-private-key> <TFTP server IP> <file name>]]`
`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 API

FortiAP-S and FortiAP-W2 version 6.2.0 and later support REST API calls that allow you to see device information, apply configurations, reboot your devices, and more.

You can access the host at `https://<FAP-IP>` where `<FAP-IP>` is the IP address of the FortiAP.

API Schema and documentation

To see the full FortiAP API schema, you will need a Fortinet Developer Network account.

Once you have an account, you can access the FortiAP API documentation.

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 get 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

REST API call	HTTP	Path	Description
			• 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
}
```

Enable API for Location Based Services station info

You can retrieve Location Based Services (LBS) information of associated and unassociated wireless stations through the FortiOS REST API. To enable this feature, configure the following:

1. Configure the region on a managed FortiAP:

```
config wireless-controller wtp
   edit "FP431FTF20012724"
      set uuid 882b4410-fac9-51eb-ab55-520bdbb17d52
      set admin enable
      set region "wifi"
      set region-x "0.2514256912442"
      set region-y "0.3601190476190"
      set wtp-profile "FAP431F-default"
      config radio-1
      end
      config radio-2
      end
   next
end
```

2. Enable `station-location` in an applied profile:

```
FortiGate-101F (vdom1) # config wireless-controller wtp-profile
FortiGate-101F (wtp-profile) # ed FAP431F-default
FortiGate-101F (FAP431F-default) # config lbs
```

```
FortiGate-101F (lbs) # set station-locate enable
FortiGate-101F (lbs) # end
FortiGate-101F (FAP431F-default) # end
FortiGate-101F (vdom1) #
```

3. Enable `ble-scanning` to detect BLE devices, if needed:

```
FortiGate-101F (vdom1) # config wireless-controller ble-profile
FortiGate-101F (ble-profile) # edit fortiap-discovery
FortiGate-101F (fortiap-discovery) # set ble-scanning enable
FortiGate-101F (fortiap-discovery) # en
FortiGate-101F (vdom1) #
FortiGate-101F (vdom1) # config wireless-controller wtp-profile
FortiGate-101F (wtp-profile) # ed FAP431F-default
FortiGate-101F (FAP431F-default) # set ble-profile fortiap-discovery
FortiGate-101F (FAP431F-default) # end
FortiGate-101F (vdom1) #
```

www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.