Architecture Guide

FortiGate Cloud WLAN

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change Log

Date	Change Description
2022-06-03	Initial release.
2022-06-08	Updated FortiAP Placement Guidelines and Channel Planning on page 14.
2023-07-05	Updated Introduction on page 5 and Solution and technologies on page 8.

Introduction

Executive Summary

This document is intended to provide an architectural overview for both single location and distributed enterprises using Fortinet Wi-Fi gear managed via the FortiGate Cloud portal. The FortiGate Cloud service provides a simple, secure and robust cloud management option for FortiGates, Fortinet's flagship product. Every FortiGate includes, at no additional cost or licensing, a full-featured *WiFi & Switch Controller* which directly controls the on-site FortiAPs (Fortinet wireless Access Points) at the FortiGate location.

Each FortiGate at a site typically serves as the site's main Internet Gateway (GW). Wireless traffic is tunneled to the controller FortiGate and security inspected before being routed internally or to the Internet. This is often referred to as a *branch* or *SD-Branch* architecture.

This guide will focus on using FortiGate Cloud as the management platform, with the site FortiGate serving as the Internet GW. The FortiGate is assumed to be a low to mid-range FortiGate model—generally up to 200/300 series. Up to dozens of FortiAPs will tunnel Wi-Fi traffic to the GW FortiGate. Adding a second FortiGate with the pair configured for High Availability (HA) is recommended, but not required.

FortiGate Cloud provides additional functionality over a standalone FortiGate, not only for distributed enterprises, but also for single sites. FortiGate Cloud adds:

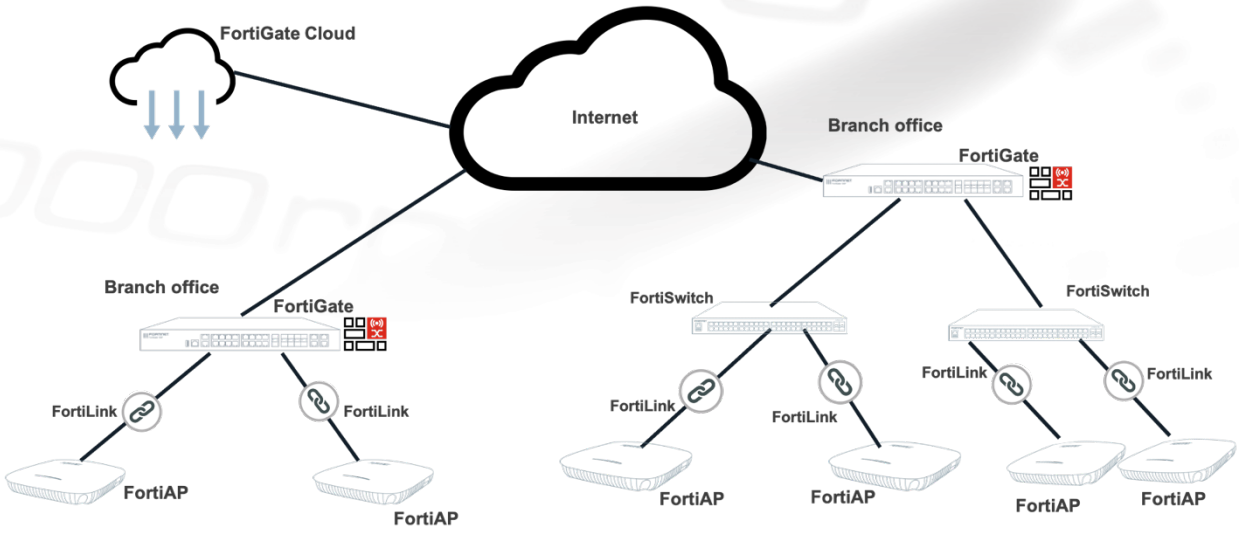
- Simplified remote management – easier, more secure and manageable than other options
- One year log retention
- Analytics – up to one year of data
- Automated backups and backup storage
- Sandboxing
- CLI Scripting and RESTFul API

Licensed features include

- Multi-tenancy – ideal for MSSPs
- Indicator of Compromise (IOC) services

The division between a branch architecture and a campus architecture is very vague, but if any of your sites exceeds around 100 APs, consider separating the WiFi & Switch controller function from the main Internet GW, as described in the Campus WLAN Architecture Guide.

The FortiGate Cloud WLAN Architecture Outline



FortiGate Cloud architecture with two branch offices

- FortiGate Cloud Management Portal (all sites)
- For each site:
  - FortiGate NGFW as Internet Gateway + WLAN controller
    - Recommended HA FortiGate
  - Campus switch network
    - Recommended PoE access switch ports for FortiAPs
  - FortiAP controller discovery and authorization
  - Possible Mesh AP backhaul
  - Security isolation oriented SSIDs for
    - Corp users
    - Guest users
    - IoT devices
    - FortiLink NAC/onboarding
  - Wi-Fi traffic Inspection policies at the controller(s)

Intended Audience

This guide is intended for an audience interested in learning about FortiGate Cloud managed wireless LAN architectures. Readers should have a basic understanding of networking, wireless and security concepts before they begin. Interested audience may include:

- *Network, Wireless and Security architects*
- *Network, Wireless and Security engineers*

About this guide

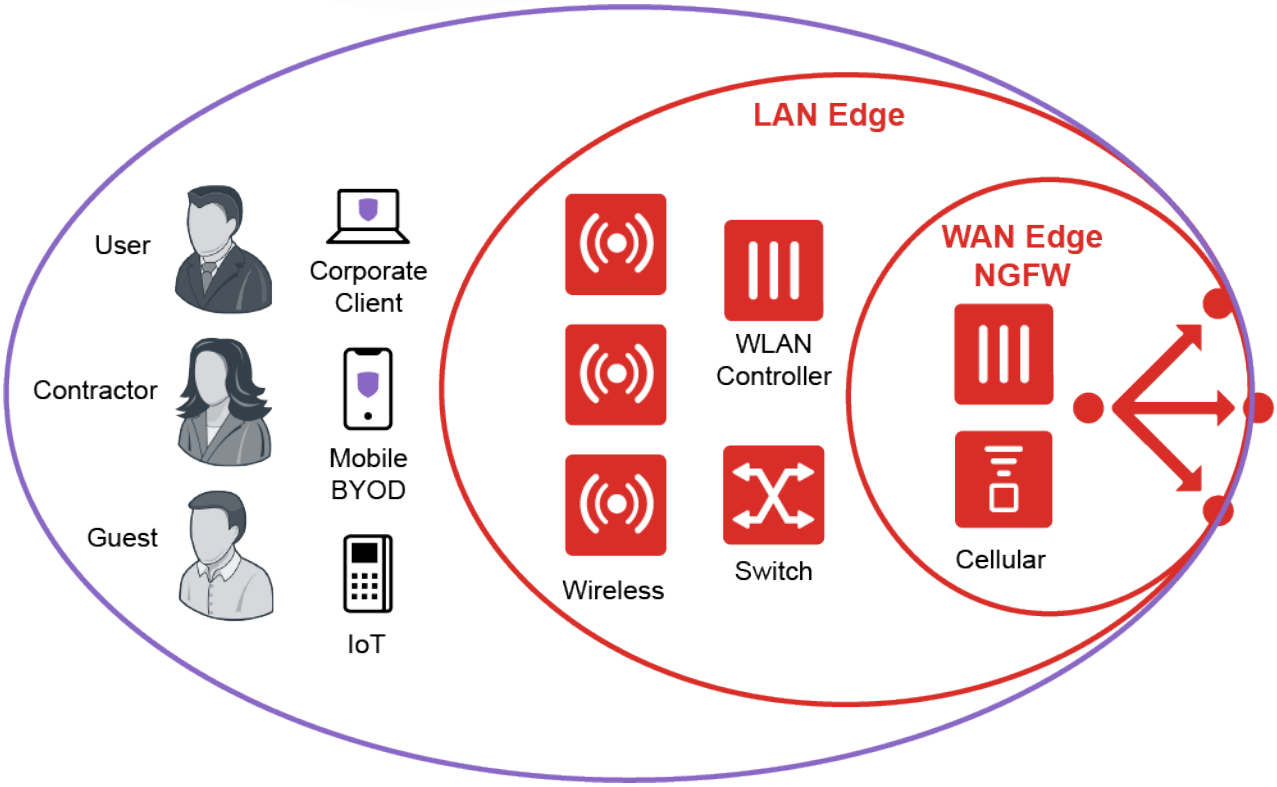
After reading the Fortinet Secure Wireless LANs Concept Guide, readers should have a basic understanding of the concepts and terminologies behind the Fortinet Wireless infrastructure. This guide further explores the design of a Wireless LAN for a branch or small campus network managed via the FortiGate Cloud service portal for a single or multiple locations. Learn about the role of the FortiGate integrated Wi-Fi controller, and the logical and physical placement of the controller. Furthermore, learn about AP placement and channel planning to achieve optimal performance. Also take a deeper dive into the details of the control plane, and how to launch and secure your SSIDs with proper user management and security.

Readers should use this guide to gather ideas for designing their wireless solution. After completing this Architecture guide, you may move on to the FortiGate Cloud WLAN Deployment Guide for actual steps in deploying a specific design scenario.

Solution and technologies

LAN Edge and Security Driven Networking

It is important to remember that while Wi-Fi networks exist to service Wi-Fi devices, Wi-Fi devices fall into a wide range of who they belong to and how they should be secured. The nature of a WLAN deployment is not just the physical considerations of network access, but the potential complexity of who and what is using that network. The greater the number of branches or locations, the more complex the security needs may become with more categories of end devices. At Fortinet, we call this the *LAN Edge*.



Physically, the LAN Edge is just the access layer, but with the evolution of networking, securing the access layer has to account for a bewildering mix of devices: enterprise owned, end user owned, guest users, known users, IoT devices with no associated users, and etc. Unlike other vendors, Fortinet takes a security first approach to WLANs (and wired LANs with our FortiSwitch line), or *Security Driven Networking*.

Fortinet's Security-driven Networking strategy tightly integrates an organization's network infrastructure and security architecture, enabling the network to scale and change without compromising security. This next generation approach is essential for effectively defending today's highly dynamic environments—not only by providing consistent enforcement across today's highly flexible perimeters, but by also weaving security deep into the network itself in a Security Fabric.

FortiGate Integrated Wi-Fi controller

A FortiGate is not only an industry leading Next Generation Firewall, but also a multipurpose Security and Networking Appliance (also available as a Virtual Machine) that includes a fully capable Wi-Fi controller. The unification of Wi-Fi controller and cybersecurity in a single appliance improve and simplifies cybersecurity for the entire network.

A FortiGate Secure Wireless Controller serves as the central Wi-Fi management system for the local WLAN and deployed FortiAPs. One or more FortiGates can be fully managed via the FortiGate Cloud portal, where all WLAN functions can be configured, managed and secured from the same interface. Multiple architectural options are supported, but the default and general recommendation is that all WLAN traffic is tunneled to the controller and then forwarded/routed from the controller to the Internet or the local network.

With WLAN traffic tunneled to a FortiGate, the instant an SSID (WLAN) is created, it is automatically security isolated from other network traffic without any need to configure and deploy VLANs on the intervening campus switch network. All SSIDs are created as interfaces on the FortiGate, so all traffic is VLAN/subnet isolated without the need to actually deploy those VLANs or even map to existing VLANs; they exist in the context of the controller. A single existing subnet serves to carry all management and data traffic to the FortiGate WiFi Controller.

Tunneled data traffic—also known as the Data Plane—can then have all desired and necessary security policies applied before any communication with the rest of the network. Firewall policies, content inspection, anti-virus, role assignments, device identification, traffic shaping are applied and all WLAN traffic is inspected. This is the essence of Security Driven Networking.

FortiGate Integrated Wi-Fi Controller Key Features

Integration with FortiOS (FortiGate Operating System) and the Security Fabric – Fortinet's Security Fabric, via the FortiLink tunneling protocol, extends coordinated security policies to the very edge of the wireless network where there are the most vulnerabilities. This creates maximized end-to-end security, via a true single-pane-of-glass for wireless and security configuration. That single-pane-of-glass design holds true for both local configuration directly on the FortiGate, or cloud configuration of the FortiGate via FortiGate Cloud. The two options are functionally identical.

Support for Wi-Fi 6 FortiAPs and the latest Wi-Fi standards – In addition to Wi-Fi 6 technology, FortiAPs are equipped with three Wi-Fi radios to enable continuous RF monitoring, including:

- Integrated Bluetooth
- Support for presence analytics
- Band (radio) balancing
- AP Balancing
- Support for dual 5 GHz settings for advanced channel plans on UTM series FortiAPs

High scalability and reliability – Due to Security and Network Processing Units (SPU and NPU) hardware, FortiGates have unmatched scalability and reliability, as well as High Availability support.

Seamless roaming – With branch office models that support up to 128 fully tunneled FortiAPs, all tunneled traffic goes to a single state machine, avoiding complex tunneling through multiple intermediary controllers.

Integrated Guest Access Management – FortiGate hosted guest portals, or integration with 3rd party portals, guest/lobby administrator support, and guest email self-registration.

Integrated WIDs – Rogue AP identification and management and Over-the-Air (OTA) attack identification.

Device fingerprinting and FortiLink NAC – Device fingerprinting identifies all client devices by type, operating system, and other factors. FortiLink NAC can then use that information to assign devices to designated VLANs, whether company owned or BYOD or IoT.

Remote troubleshooting – From the management console, easily run Spectrum analysis or packet captures from associated APs regardless of location.

Layer 7 application visibility and control – FortiOS Application Control is part of FortiOS, and therefore fully integrated and built-in to the Wireless LAN controller. Layer-7 deep inspection with over 4,000 application signatures to provide bandwidth guarantees and prioritization of critical applications is fully available.

Automated Channel and power selection - FortiOS DARRP (Distributed Automatic Radio Resource Provisioning) technology optimizes channel selection and AP Tx power. FortiAPs continuously monitor the RF environment for interference, noise, and signals from neighboring APs, and the FortiGate WLAN Controller optimizes the entire campus network.

FortiGate Cloud Key Features

Simplified Cloud Management - FortiGate Cloud is an ideal way for a wide range of customers to easily add simple cloud management to FortiGate based sites, whether a single campus or SD-Branch, or a highly distributed business with many sites. It is specifically aimed at sites utilizing SMB to mid-size FortiGate models, typically a FortiGate 40-200. It is the easiest way to set up remote administrative access to one or more FortiGate sites.

Multi-tenancy support – The multi-tenant option enables full data isolation over multiple sub-accounts. It is favored by MSSPs servicing multiple customers and also used by large highly distributed single enterprises for administrative division.

Simple remote administration of Fortinet LAN Edge network equipment – The entire network at a branch site can be easily administered, including FortiAPs, FortiSwitches, and FortiExtenders.

Automation and Cloud storage – FortiGate Cloud comes with:

- Automatic backups, stored in the cloud
- One year of hosted log storage
- Run and schedule CLI scripts, reuse across FortiGates
- Cloud REST API

Analytics included - Both on-demand and scheduled reporting with preconfigured and custom reports are included.

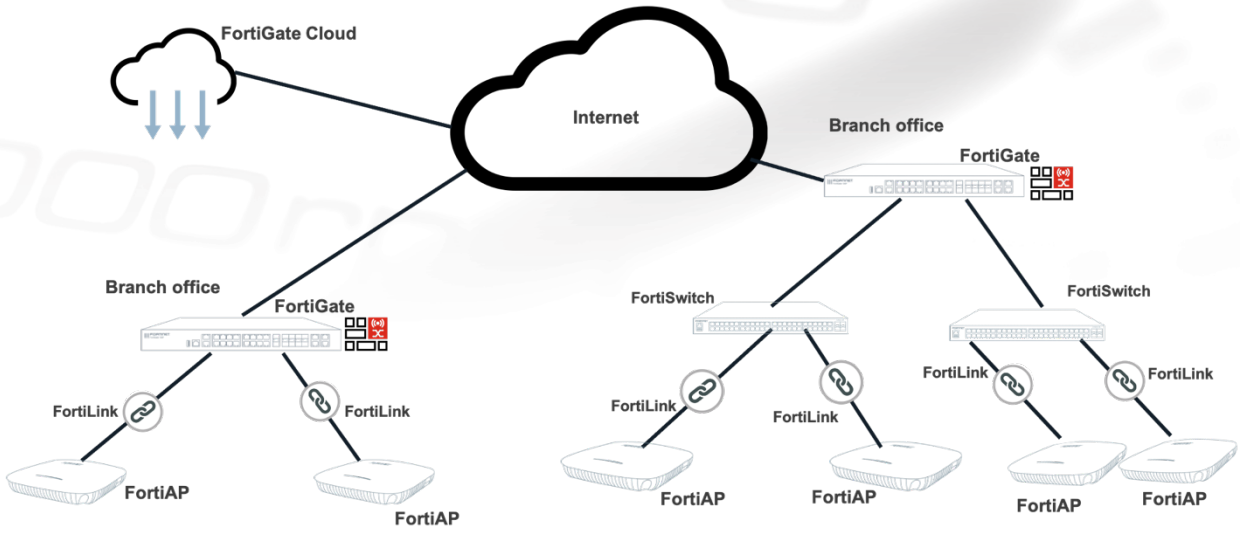
Zero-touch provisioning using FortiDeploy – Bring new branches up and running as soon as they are plugged in. No need to fly in.

Integration with other FortiCloud Services – FortiGate Cloud is part of Fortinet's suite of cloud services and fully integrated with all of them, and the FortiGate Cloud login is the single sign on for all of them.

- Integrated with FortiCare support.
- Integrated with FortiDeploy mechanisms.
- Integrated with Fortinet Asset Management – track all licenses and Fortinet devices.
- Fortinet identity and Access Management – centrally administer all your cloud services administrators and their rights, by groups or individuals.
- FortiSandbox Cloud services for the FortiGates are included with FortiGate Cloud.
- Optionally, integrated Indicator of Compromise (IOC) service can be added to FortiGate Cloud managed FortiGates.

FortiGate Cloud is the 'easy button' for adding cloud advantages to FortiGate and Fortinet Security Driven Networking for small and midsize enterprises.

The Fortinet Branch WLAN architecture

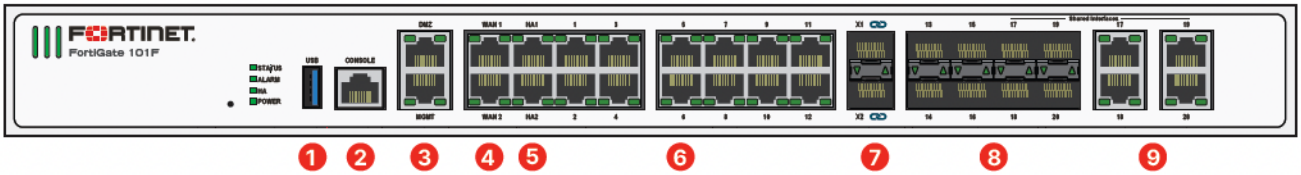


FortiGate Cloud architecture with two branch offices

- FortiGate Cloud Management Portal (all sites)
- For each site:
  - FortiGate NGFW as Internet Gateway + WLAN controller
    - Recommended HA FortiGate
  - Campus switch network
    - Recommended PoE access switch ports for FortiAPs
  - FortiAP controller discovery and authorization
  - Possible Mesh AP backhaul
  - Security isolation oriented SSIDs for
    - Corp users
    - Guest users
    - IoT devices
    - FortiLink NAC/onboarding
  - Wi-Fi traffic Inspection policies at the controller(s)

Design Overview

FortiGate Secure WLAN Controller Logical and Physical Placement

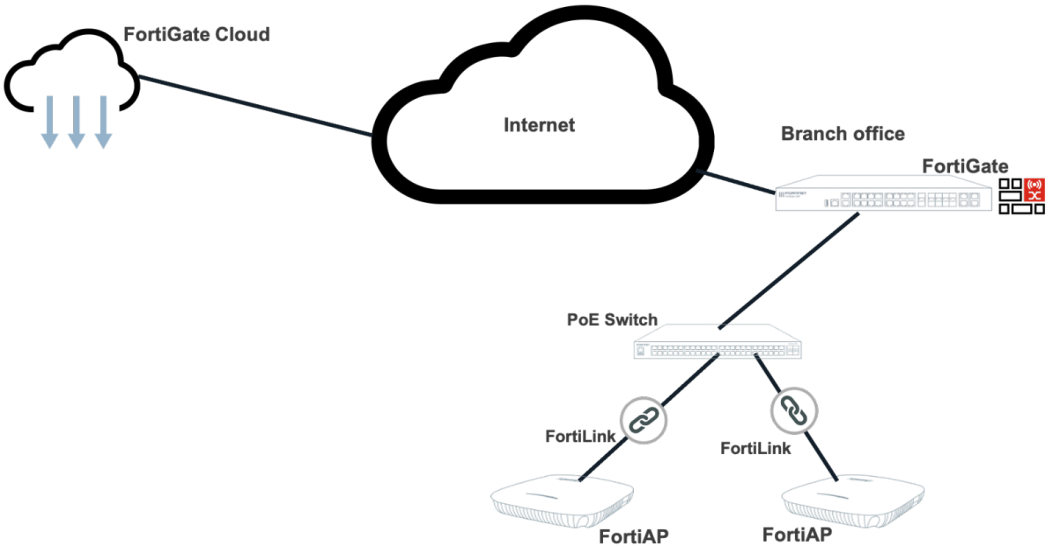


For branch deployments ranging form one to several dozen FortiAPs, the Secure WLAN Controller FortiGates will normally be the primary Internet Gateway.

For maximum flexibility, Fortinet WLAN equipment is fully compliant with network standards and works with any vendor's switches. There are advantages to using FortiSwitches as the wired backbone, but FortiAPs can tunnel through any local switch network, and this guide concerns itself with only WLAN design.

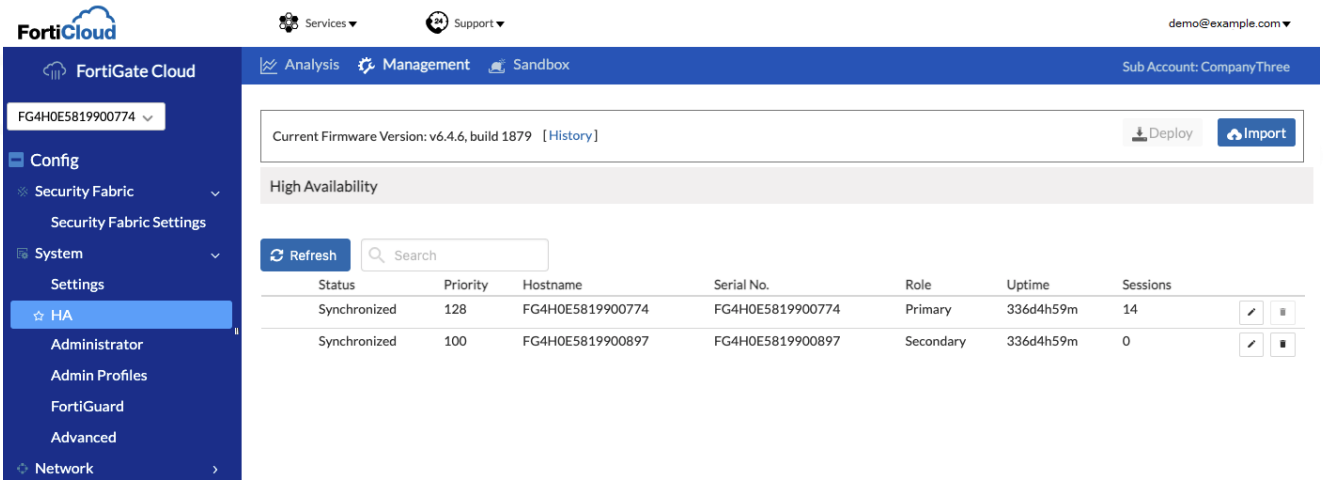
Controller and FortiAP communication

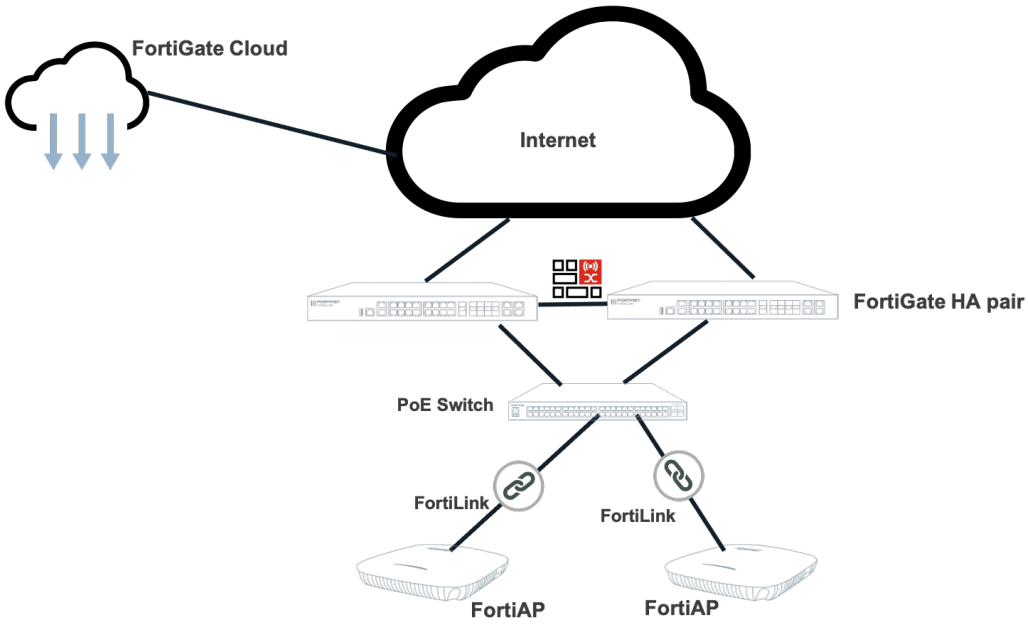
FortiAPs communicate with their controllers via the FortiLink protocol, which provides both *control plane traffic,* or management of the APs, and *data plane tunneling,* securely bringing all data traffic to a central management and inspection point. Data plane traffic is the control and administration traffic between the FortiAPs and the FortiGate WLAN controller, and works over L2 or L3. Any logical placement that allows routing from the APs to the FortiGate Controller will work, but should be analyzed for expected traffic and how it fits into the network. The FortiGate WLAN Controller will be the central router for all WLAN traffic to the rest of the network while providing security inspection services.



No WLAN VLAN needs to be defined going to the controller. VLANs exist in the tunnel and within the FortiGate but usually nowhere else.

When redundancy is needed, dual FortiGates can be deployed as a High Availability (HA) pair. FortiGates are highly reliable, and redundant deployments are recommended, but branch deployments come in all sizes and budgets, so network admins have more flexibility. When an HA pair of FortiGates are deployed, they should be deployed in Active/Passive mode.





Redundant HA FortiGate Controllers

Access Layer and Power consumption

Power over Ethernet (PoE) switches should be used to power the FortiAPs for maximum flexibility of AP placement, although power injectors can be used instead. It is common in a branch deployment for a single switch to power all APs, but it is also not unusual to see multiple access switches. Any switch that FortiAPs will connect to should be checked for its per-port and total power capabilities to ensure it will deliver enough power. If the switch does not

support the needed power budget, options include new switches, single port and multi-port (midspan) power injectors.

In general, the indoor Wi-Fi 6 FortiAPs require 802.3bt High Power over Ethernet and support 2.5 Gigabit Ethernet speeds. Wi-Fi 6 FortiAPs will work with Gigabit Ethernet, and will operate on basic 802.3af PoE, but capabilities will be reduced. In Wi-Fi, there tends to be a tug-of-war between *capacity* and *coverage.* Lightly populated branch offices may not need the full capacity of a FortiAP, or may not need it right away if existing switches are not up to the latest. Check the datasheets for both the switches and APs and ensure capacities match expectations.

There are also special case FortiAPs, such as the FAP831, an ultra-High-Density model with two 5 GE ports for uplink. Similarly, outdoor models with a PoE output to another device will require higher input power to support both the FortiAP and the corresponding PoE out.

Again, in all cases, check the datasheets of the particular models you wish to deploy and make sure the underlying switch network supports the capabilities you are seeking. Power injectors are available and can increase flexibility when dealing with an underlying switch network that is not ready for a refresh.

FortiAP Placement Guidelines and Channel Planning

Fortinet recommends performing a site survey for all Wi-Fi deployments. Wi-Fi is well established as the primary access technology, and most Wi-Fi deployments are a network refresh, which encourages a tendency to just swap out the old access points for newer ones. That tendency should be resisted, because environments change, and AP capabilities also change with Wi-Fi generations. Environmental changes can come from surprising places. With wide adoption of Bluetooth, the 2.4 GHz band is nosier than ever while new paint on the walls can have surprising RF effects. Chrome flecked paint looks stylish, until the reflectivity interferes with the Wi-Fi. Generally speaking, coverage areas will be less for a 5 GHz radio, let alone a 6 GHz (6E) radio vs a 2.4 GHz radio due to reduced wall penetration of signal.

A walk-through examination of the site with *a spot-check of representative areas* may be a good idea on a refresh. New sites always benefit from getting a clear idea of wall properties and corresponding dB loss. Glass walls in office can range from very transparent to Wi-Fi, to very opaque—wire supported and leaded glass have surprised more than a few Wi-Fi designers.

Capacity and coverage estimations

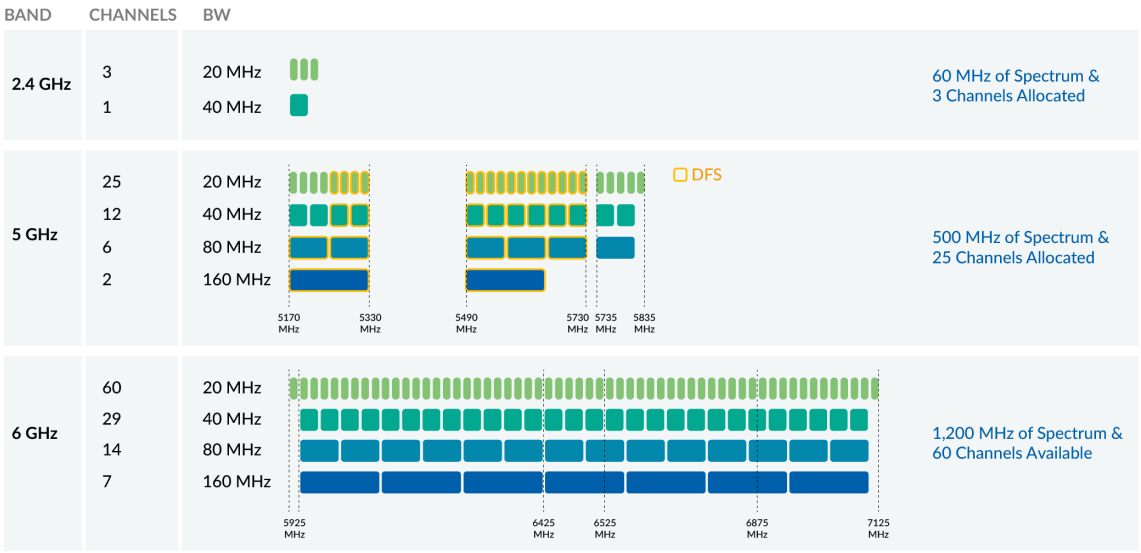
For a general pre-survey estimate, an indoor area probably requires about 1 FortiAP per 2000 Sq-Ft, with around 30 devices per AP radio. All the Wi-Fi 6 FortiAPs have 1 radio for monitoring and 2 service radios. Users are usually assumed to have 3 devices each, so 20 users and 60 devices can be serviced per physical AP. UTP series FortiAPs can have both radios on 5 GHz, so set both radios to 40 MHz wide channels for increased bandwidth and capacity.

The above estimates are conservative, and there are some factors that can move the average up or down. For coverage, walls are the key concern. A FortiAP can cover a very large space with an open floor plan, while floor plans with many small offices will require more APs. At the same time, the client count per AP may be a more important factor; capacity more than coverage is also a major design consideration. Designing for capacity rather than coverage is helped by designing for 5 GHz bands.

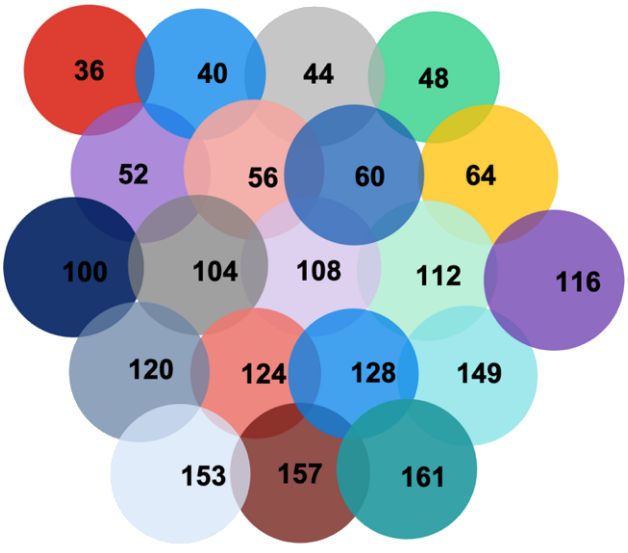
It is best to avoid requiring client-to-FortiAP radio connections to pass through more than one wall. Although one cannot see Wi-Fi signals, line of site connectivity to client devices is best, so a designer can visualize coverage by thinking about how they would deploy light fixtures. Placing APs in closets, behind ductwork and other obstructions will not maximize performance.

Channel Planning – Design for 5 GHz

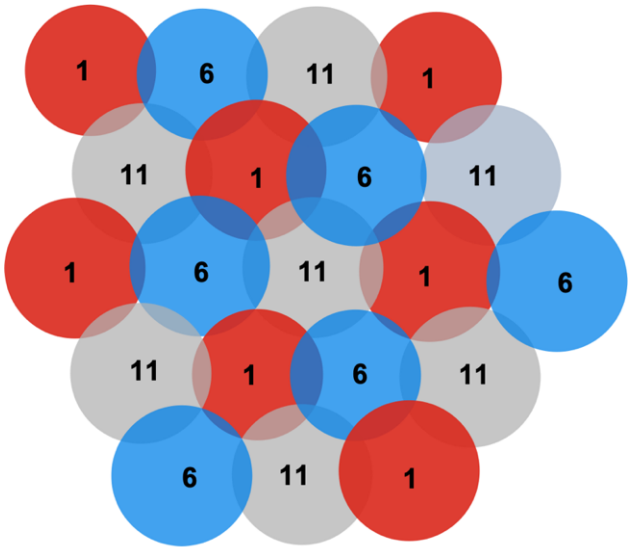
Wi-Fi in general has evolved quite a bit in a relatively short time, and so have other wireless technologies such as Bluetooth and its variations. The default assumption for Wi-Fi in the past was to design for 2.4 GHz and treat 5 GHz as secondary. Now that Wi-Fi 6 is available, Fortinet recommends designing for 5 GHz as the primary band.



The large number of 5 GHz channels make for much more forgiving channel plans. WLAN self-interference is massively reduced. Furthermore, 2.4 GHz continues to become increasingly crowded with wider adoption of Bluetooth.



5 GHz channel plan (20MHz wide)
No self-interference



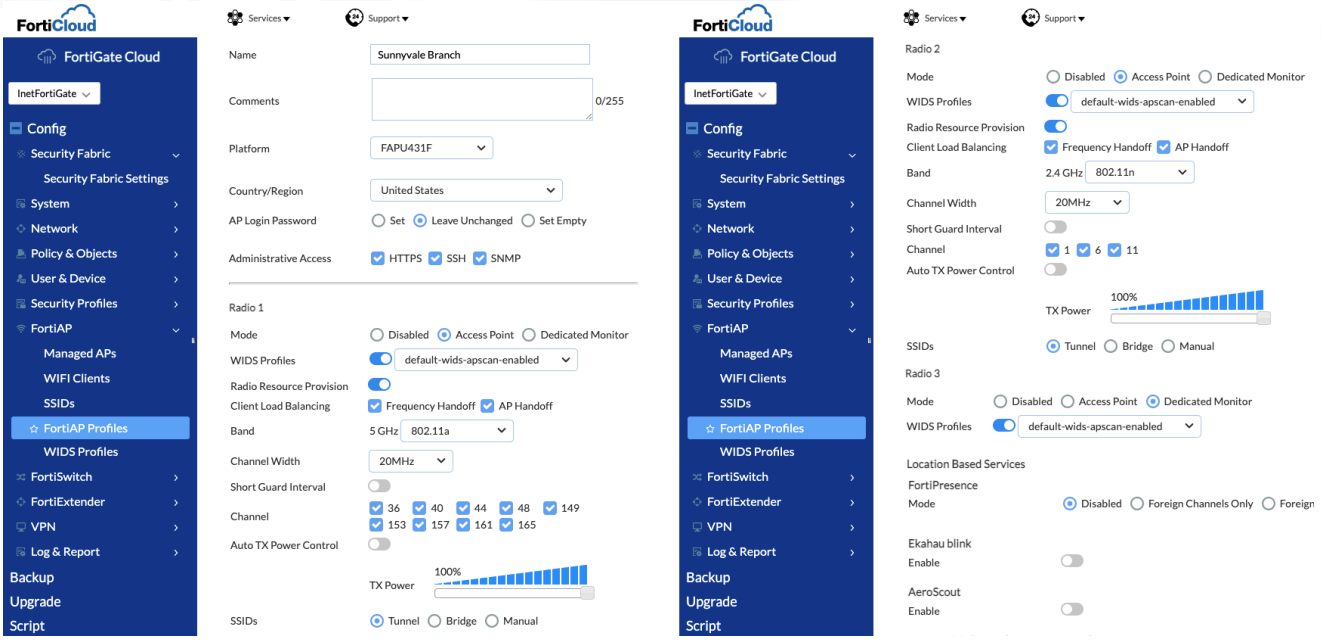
2.4 GHz channel plan
Potential self-interference

Very few client devices are so old or so “inexpensive” that they do not fully support 5 GHz. In addition, DFS (Dynamic Frequency Selection) regulations apply to the APs, not the clients. A good reference for client 5 GHz support can be found here: http://clients.mikealbano.com.

Even when designing for a branch location with only a few APs, pay attention to the neighbor networks on a site survey. The smaller the location's foot print, the more of it may border someone else's WLAN.

FortiAP Profiles

UTM series FortiAPs include a band selectable radio and a good channel plan that prioritizes 5 GHz but provides high support for 2.4 GHz. This allows for the FortiAP profile to alternate the selectable radio between 5 GHz and 2.4 GHz. FortiAP profiles are per AP model, but APs can also be grouped if there is a need for different profiles on the same model.



Radio Resource Provision should be enabled in FortiAP profiles and transmit power set to automatic in order for the WLAN network to take full advantage of FortiOS DARRP (Distributed Automatic Radio Resource Provisioning). DARRP will optimize channel selection and AP Tx power periodically. The default is to adjust every 24 hours at 2 am. The timing can be adjusted in the FortiGate CLI.

Designing for High Density environments

High density areas such as auditoriums and cafeterias are a good illustration of the power of multiple 5 GHz channels over only three 2.4 GHz channels. In a single large room, the maximum number of devices, at 30 per radio, that can be on the 3 channels in 2.4 GHz is 90. More client devices can be accommodated with more FortiAPs, but then all FortiAPs on the same channel will have to contend for airtime. However, 5 GHz can potentially have 600 devices when using 20 MHz wide channels with no FortiAPs needing to contend with each other—which is the best way to design for such a high-density deployment.

Wi-Fi 6 is specifically designed to maximize performance in high density situations. The FAP-831F supports 8x8 MIMO and is an excellent choice for such a situation.

See the Fortinet Secure Wireless Concept Guide for details on Wi-Fi 6 for high density.

FortiAP 831F – 8x8:8 MU-MIMO Indoor/High Density

This high throughput enterprise class 802.11ax indoor AP provides three radios and 8 spatial streams. This top-of-the line access point supports OFDMA, a 5.0 Gigabit Ethernet port, plus an additional 1 Gbps Ethernet port for PoE diversity. The AP can provide 24/7 scanning across both bands while still providing access on both the 2.4 GHz and 5 GHz bands. The integrated BLE radio can be used for beacons and locationing applications.

FortiAP Discovery, Authorization, and Control Plane

Communication must be established between the FortiGate and the FortiAPs it will manage. The FortiAP must then be authorized on the WLAN controller for security purposes. FortiAPs use a protocol called FortiLink to communicate with the WLAN Controller. FortiLink is also the tunneling protocol that encapsulates the client traffic, but initial discovery may require some preparation of the underlying network.

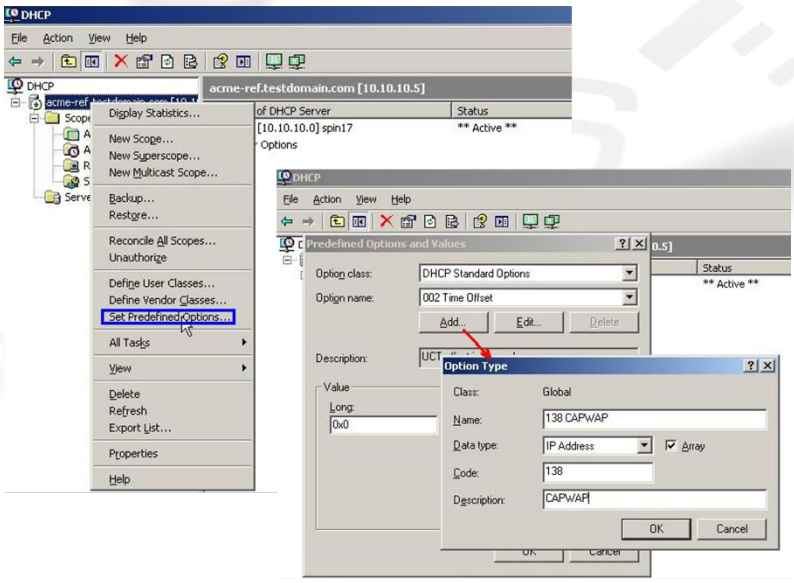
The simplest method for a FortiAP to locate its controlling FortiGate is for both to be in the same *broadcast domain.* When the FortiGate and FortiAPs are on the same L2 network, they will discover each other with no need to adjust anything else on the network. Branch and smaller location can often work this way.

When network architecture requires FortiAPs to have layer 3 separation (routing) from their FortiGate controller, the DHCP or DNS server of the network can tell the FortiAPs the IP address of the FortiGate controller.

With L3 separation of the APs and FortiGate, the best practice is for the FortiAPs to be on a specific subnet. It does not have to be a FortiAP only subnet, but it should be a *Control Plane* subnet for the FortiAPs and FortiLink to communicate with the FortiGate Controller. The subnet's DHCP server, or its DNS server, can be configured to tell the FortiAP the IP address of the controllers. That IP address must be an existing interface on the FortiGate controllers and routable to and from the FortiAPs

With DHCP, Option 138 can be set for controller discovery. This is probably the easiest choice for most L3 networks. As an example, on a Windows DHCP Server:

1. Go to *Set Predefined Options* and click *Add*.
   a. *Name* the option.
   b. Set *Code* to *138*.
   c. Set *Data type* to *IP Address*.
   d. Click *OK*.



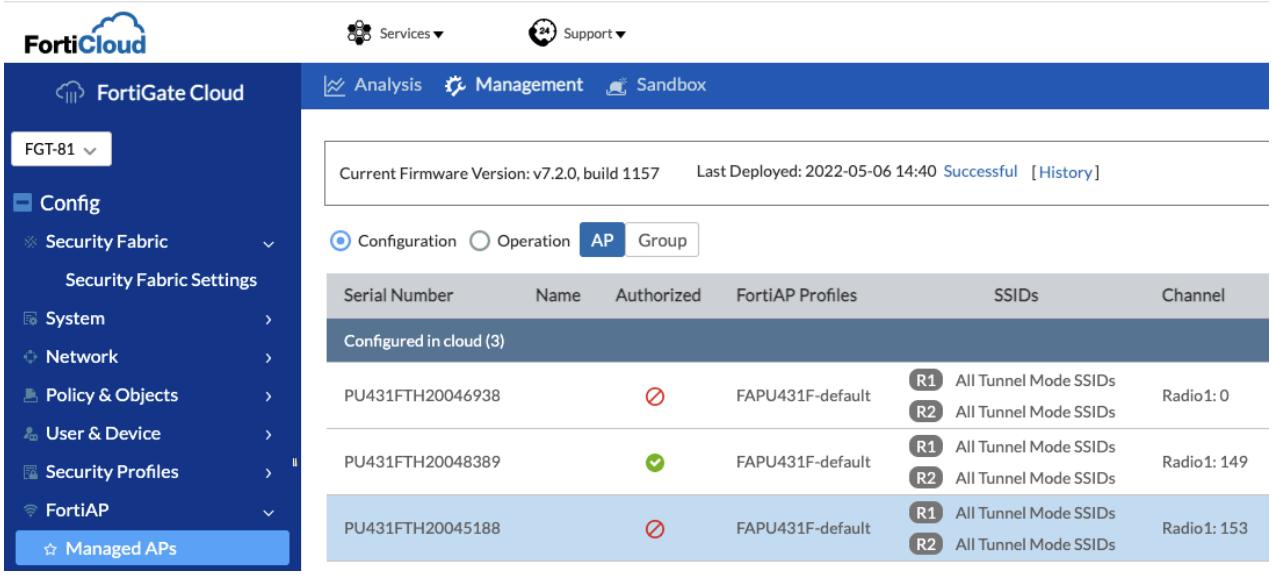
2. Go to the option name and then enter the controller IP address as a value.
3. Go to the scope the FortiAPs will use and then choose *Configure options*
4. Check *option 138*, and then click *OK*.

For DNS resolution option, the network DNS server can be configured to respond to *_capwap-control._udp.example.com* with the Wi-Fi controller IP address.

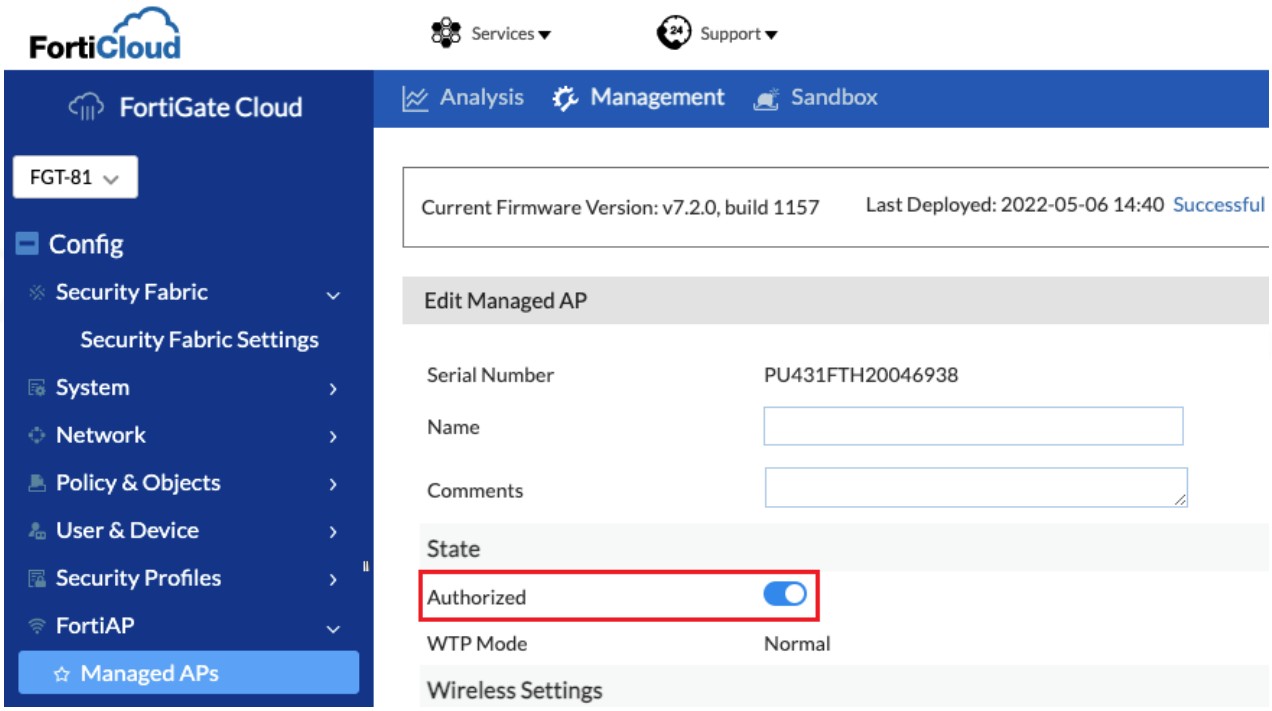
If L2 broadcast, DHCP, or DNS options are not desirable, more options are supported. FortiAPs can use multi-cast discovery, or FortiAPs can be preconfigured via CLI with the controller address. See the Advanced WiFi controller discovery in the *FortiWiFi and FortiAP Configuration Guide* for details on these discovery methods.

Once FortiAPs have established FortiLink communications with the FortiGate, it must be authorized:

1. Go to *Managed FortiAPs* and click the edit button on the FortiAP entry.



2. Change the State to *Authorized,* and then deploy the change.



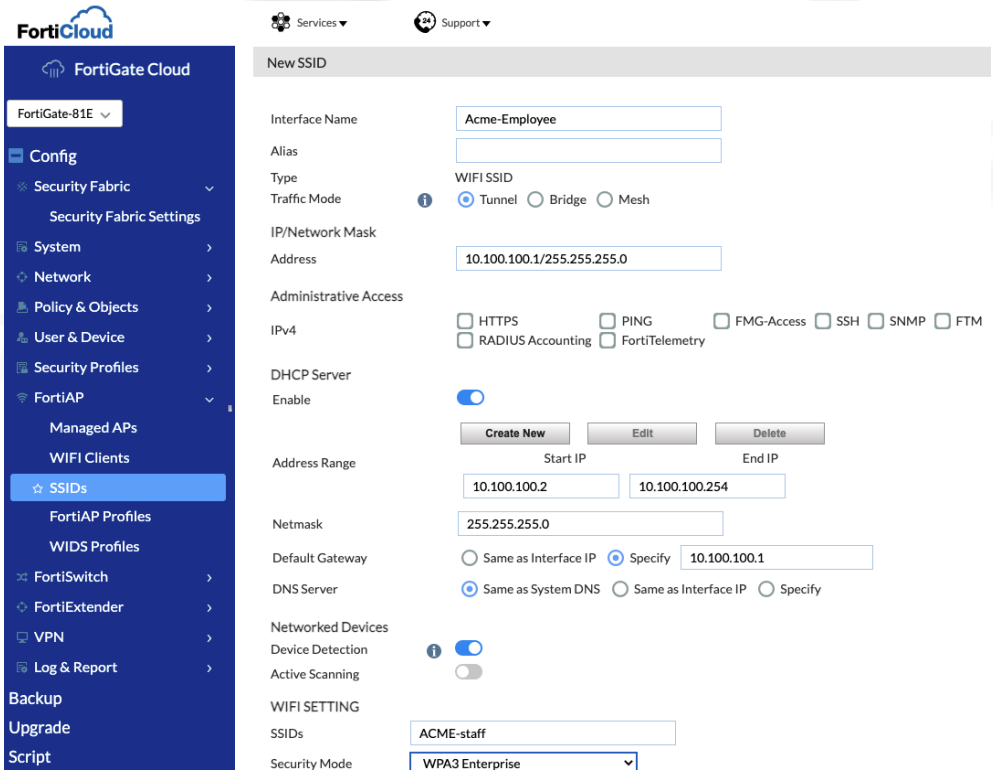
SSID Configuration and Traffic mode

SSIDs and Secure Interface Integration

SSID (or WLAN) setup in FortiGate Cloud is where the power of FortiGate integration and the advantages of Security Driven Networking truly become clear. Unlike other systems where SSID setup is strictly a network Layer-2 process that must be mapped to the Layer-3 overlay and then to a security overlay, the FortiGate integrated Wi-Fi controller simplifies and integrates all of this into a unified flow under a true single pane of glass. By default, an SSID is also a network interface on the firewall router, with a DHCP server available, and an address object on the firewall is automatically created for policy definition. When setting up multiple branches, the configuration of the first one can be captured and turned into a CLI script that can be run on all other locations singly or together.

SSID Traffic Modes

Tunnel mode is the default setting for a new SSID. The other available modes are *Bridge* and *Mesh*, which are for special cases. A Tunnel Mode SSID sends all traffic over the FortiLink connection to the FortiGate Wi-Fi Controller for inspection and routing. Because each SSID is a unique interface, each SSID is security isolated from the rest of the network, regardless of the underlying network structure. There is no need to manually configure and deploy any VLANs for Wi-Fi traffic. As part of the configuration flow, a DHCP server can also be configured with no need to make ANY changes to the underlying wired network, or to the control plane subnet's DHCP server. Routing will be handled by the FortiGate.



Bridge Mode keeps the SSID operation at Layer-2, with traffic being directly bridged to the FortiAP management subnet. There may be specific reasons for using this mode, and the WLAN traffic could be isolated with VLAN tags, but such reasons are relatively rare and bridge mode gives up one of the great strengths of a Fortinet Wi-Fi deployment—the tight integration with FortiGate's security and inspection capabilities.

Mesh mode is used when Ethernet backhaul is not available. It bridges traffic from one SSID—the client service SSID—to a wireless backhaul SSID. Mesh mode is for cases where a FortiAP radio, rather than its Ethernet port, provides the backhaul to the controller. A Mesh SSID is meant for only connecting FortiAPs wirelessly. For instance, an outbuilding with power but no Ethernet to the main building could have a FortiAP in mesh mode connected to a root FortiAP that does have an Ethernet connection to the main network. In this remote building example, wired devices that are Ethernet connected to the mesh FortiAP could also use this uplink.

Wi-Fi Security Modes and FortiGate Security Extensions

As part of the Wi-Fi standards, WPA2 and WPA3 Wi-Fi security standards are supported and recommended with a Fortinet Wi-Fi deployment. WPA3 improves on WPA encryption and authentication security, particularly at the personal level (or Pre-Shared Key level). When possible, use WPA3. If you cannot use WPA3, develop a plan for eventually transitioning to it, depending on your clients.

With WPA2 and WPA3, there are 3 basic security modes that cover authentication and encryption:

- Open – no security
- Personal – all users use the same Pre-Shared Key (PSK)
  - also called *SAE* in WPA3
- Enterprise class – using 802.1X, usually username/password based

FortiGate Security Extensions

Other security options operate above the Layer-2 Wi-Fi level:

- **Captive portal** authenticates users at essentially layer 7 in a web page. The lower layer security could be either Open or Personal. Technically, the device is already on the network and has an IP address, but network access is limited until portal level authentication has been accepted. In public venues, this may simply be checking a Terms and Conditions screen. Captive portals are most commonly used for guest users.
- **Firewall policies and other inspection options.** One of the great strengths of using FortiOS Integrated WLAN Controllers is the fact it is also a fully functional FortiGate, with simple integration of traffic inspection. All tunneled SSIDs are interfaces that firewall policies can, and must, be applied to. The configuration flow to set up the Interface and the SSID are unified. After SSID setup, it is necessary to go to Firewall Policies and specifically enable the Wi-Fi traffic.
- **FortiLink NAC** uses device fingerprinting to identify devices or classes of devices on a Wi-Fi onboarding/default VLAN and move them to a specifically designated VLAN for that device type. This is particularly useful for IoT devices or other 'no-owner' devices such as printers.

Users and device classes – the key to a well secured network

To take full advantage of Fortinet Security Driven Networking, you need to clearly define the classes of devices and users. Then use a mix of VLANs and SSIDs to securely isolate these classes and use Firewall Policies to control access to network resources. There are three broad classes to consider:

- Fully authenticated or *Known* users
- Guest users
- Ownerless devices

One important point is that you do NOT want to have a separate SSID for every class of user/device. Excess SSIDs will eat into WLAN performance because every SSID will have to advertise with over-the-air beacons at the lowest supported data rate. Three SSIDs will probably be necessary because of the different WPAx authentication methods. However, it is a bad idea in a school, for example, to have an SSID for Teachers, an SSID for Students, and SSID for administrators. Using RADIUS, multiple types of users can share a single SSID while using RADIUS attributes to assign them different VLANs.

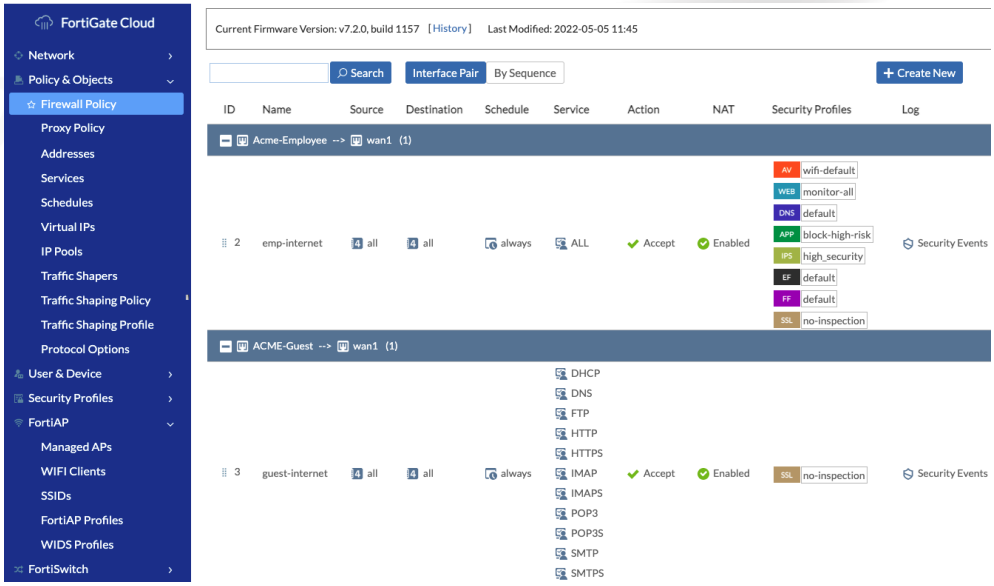
Fully authenticated users using Enterprise class WPA2 or WPA3

Fully authenticated or Known users are network users that are fully part of the organization. There should be a database that they can be authenticated against via RADIUS, most commonly in an Active Directory. Users would have their own authentication credentials, typically username and passwords, but certificate authentication is also supported with FortiGate Cloud Wi-Fi.

An enterprise branch may have multiple classes of authenticatable users like the previous school example. For example, Engineering, Sales, and HR in a technology company. FortiOS can also authenticate WPA2-Enterprise users through its built-in user group functionality. FortiGate user groups can select users from a RADIUS server by RADIUS user group. This makes it possible to apply Role-Based Access Control (RBAC) by defining the attributes in the external user database that include VLAN assignment.

Firewall Policies

Firewall Policies must be added to allow traffic. In the simplest case, a rule for outbound traffic from the SSID interface to the Internet needs to be added. In cases with multiple VLANs, each VLAN is an interface and firewall policies are needed for each interface. Additional policies can be added to control access to internal resources. Other FortiGate Security Profiles can also be included, such as Anti-virus, Web Filter, Application Control, and etc.

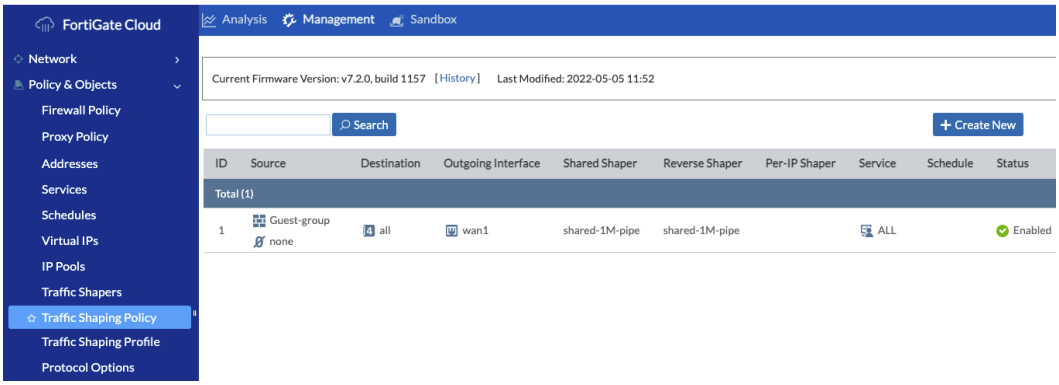


Guest User Management

Guest users are temporary users of the network, without pre-existing identities associated with a specific person. Organizations can have a wide variety of needs for guest users, with greater or lesser needs for access control. The FortiGate WiFi controller supports multiple options and many of those options can be combined.

Firewall policies and traffic shaping

Firewall policies can be used for traffic shaping as well as resource access. In most cases, guest traffic will be limited to Internet only, and possibly more restricted. Additionally, when guest access is a courtesy that is a lower priority than authorized user traffic, a traffic shaping policy could be added. Traffic shaping policies are very similar to firewall policies and are found in their own table under policy and objects:

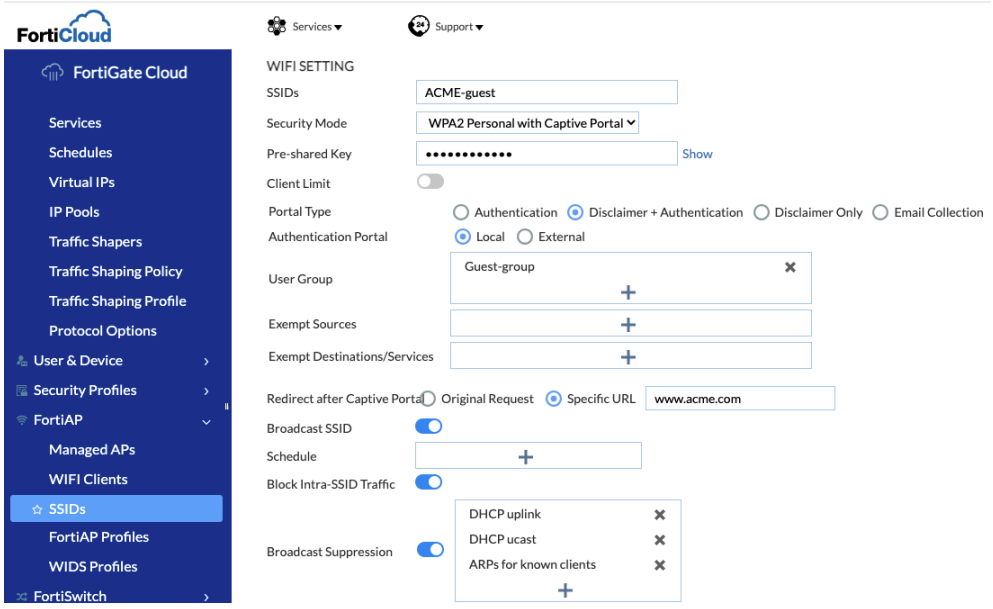


The preceding example sets traffic on the guest interfaces to a lower priority. The traffic policies can be configured as per IP/device or for SSID-wide, by priority, or by a maximum allowed bandwidth.

Captive Portal

Captive portals are browser-based authentication screens and are the most common restriction used with guest access SSIDs. Wi-Fi itself is a layer 2 technology with three access control options—RADIUS, PSK/SAE, and Open (unrestricted). Captive Portals operate on a higher layer, after the Wi-Fi device has connected to the network and received a DHCP address in order to reach the web authentication screen. Until authenticated by the web page, no other traffic is allowed.

Captive Portals are most commonly used with open networks, but can optionally be used in Wi-Fi networks that apply Pre-Shared Key as layer 2 security with encryption. This option is useful for reducing casual use of the network by neighbors when the portal is a disclaimer only.



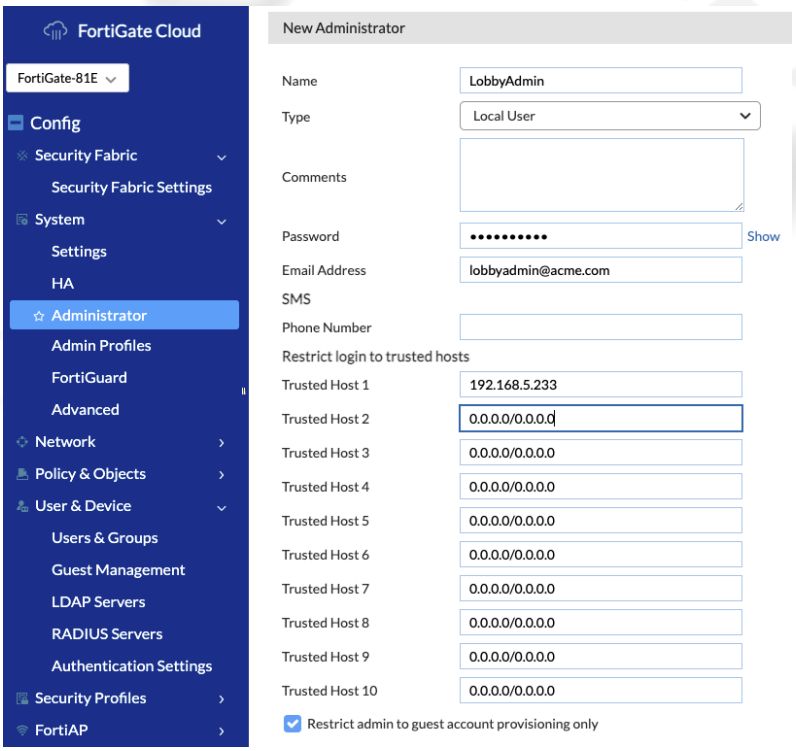
Captive portal options integrated into the FortiGate WiFi Controller include a simple disclaimer display, or a disclaimer with authentication. When authentication is enabled, a user name and password must be provided by an admin to the guest.

Guest users

A guest user group can be created in the FortiGate via FortiGate Cloud, as well as an on-site guest administrator. The Guest Admin is an account on the FortiGate with rights limited to creating guest users.

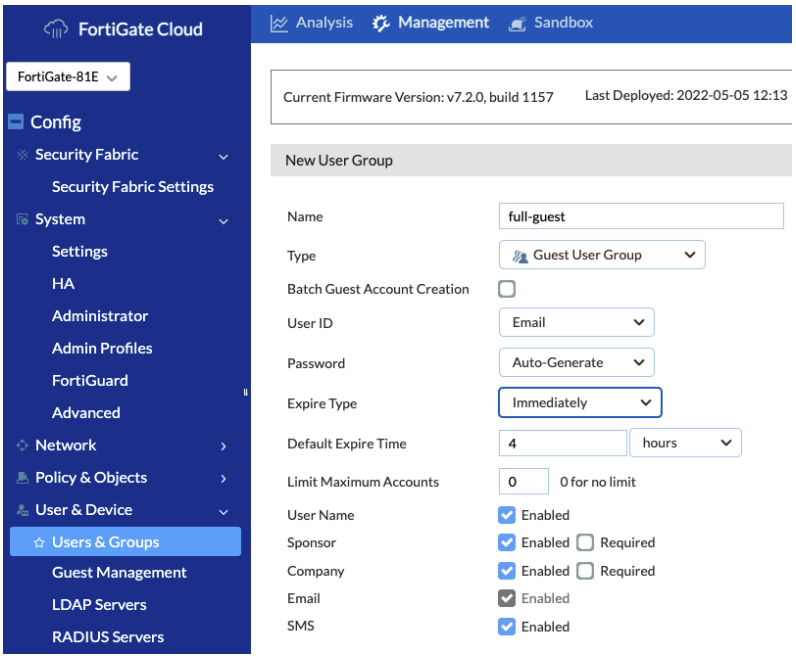
The following image shows a FortiGate administrator that is restricted to only managing and provisioning guest user accounts.

GUEST USER MANAGEMENT

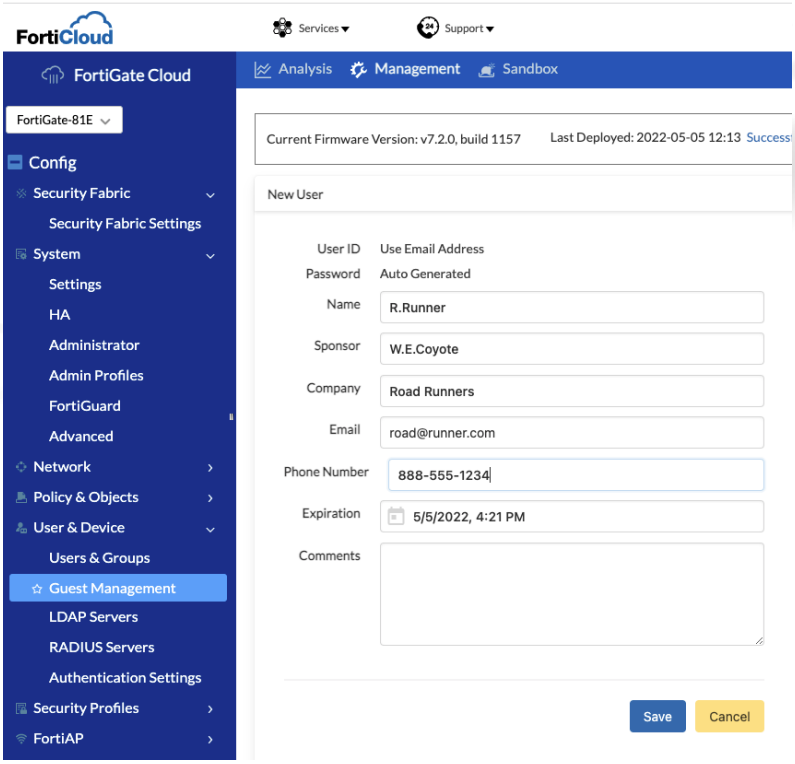


Users can be created on the fly, or batches can be made up ahead of time. With batch creation, the account can be created, printed out, and handed out as needed without access to the FortiGate. The advantage of having a Guest Admin is that they can capture additional guest info, such as email, phone number, and etc.

The following image shows a Guest User group setup page with options that can be configured for the group.



The following image shows the Guest Management page where a new Guest user can be manually added.



There are a lot of varieties in guest access, whether pre-generated and pre-printed user/password, on the fly registration with a lobby administrator, or simply open with a disclaimer. The latter may be entirely reasonable with bandwidth limitations and constraints. The method for managing guest access should be well thought out ahead of time to align with business needs.

To learn more about Guest Management:

- Captive Portal Security
- User definition and groups

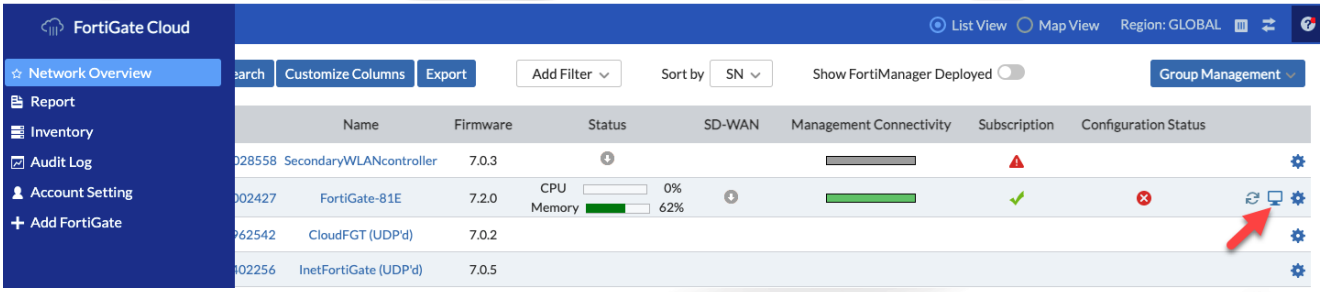
Ownerless devices – IoT, MPSK and FortiLink NAC

The final type of devices to be concerned with are ones that do not have a user associated to them and/or do not support RADIUS, but only Pre-Shared Key (PSK) associations. This category of devices, led by the increase of Internet of Things (IoT), has greatly expanded the attack surface of the network. They may be consumer-oriented devices like AppleTV, Roku, Amazon Echo, Smart TVs and others, or office appliances like printers, scanners, mobile credit card readers, etc., or operations devices like temperature sensors, door locks, and more. Using a single PSK for a large number of devices leaves many opportunities for the PSK to become known and exploited. Two FortiGate technologies are key in helping solve this problem: Multiple Pre-Shared Key (MPSK) and FortiLink NAC.

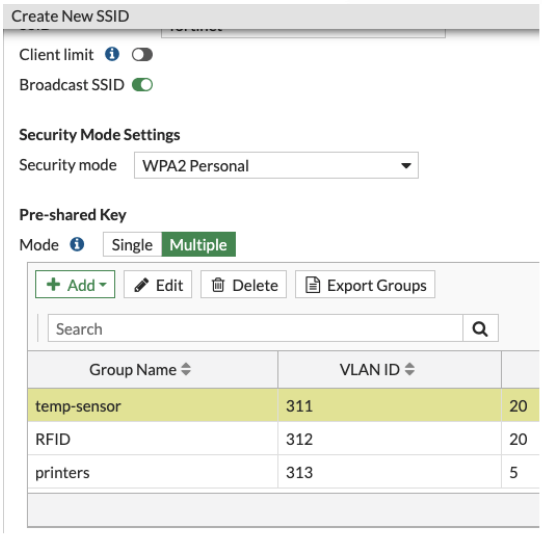
MPSK allows what is technically a Pre-Shared Key SSID to have a unique key and a specific VLAN associated with each individual client device. Keys can be pre-generated and locked to the specific device on first use so that no other device can use the same key. If a device is removed, the key can be deleted.

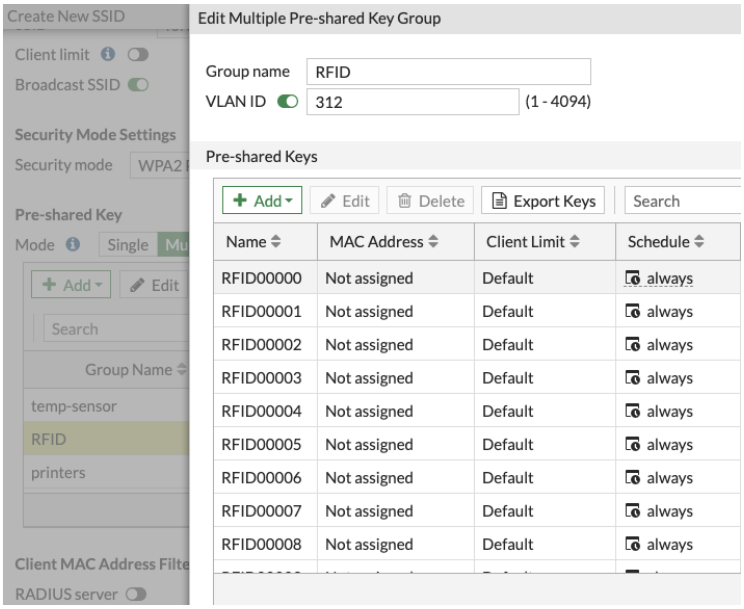
As of version FortiGate Cloud version 22.1, MPSK must be directly configured on the FortiGate UI, but FortiGate Cloud makes it simple to remotely, and directly, launch a remote session on each cloud connected FortiGate using the *Remote Access* button:

OWNERLESS DEVICES – IOT, MPSK AND FORTILINK NAC



The same SSID can have multiple MPSK groups, with each group assigned a specific VLAN. The Multiple PSKs solve the Layer 2 problem of not being able to keep the single authentication key private. However, the group VLAN assignment is central to the necessary security isolation. Note that any tunneled WLAN traffic has one layer of isolation, but grouping devices can enable further isolation within the tunnel.



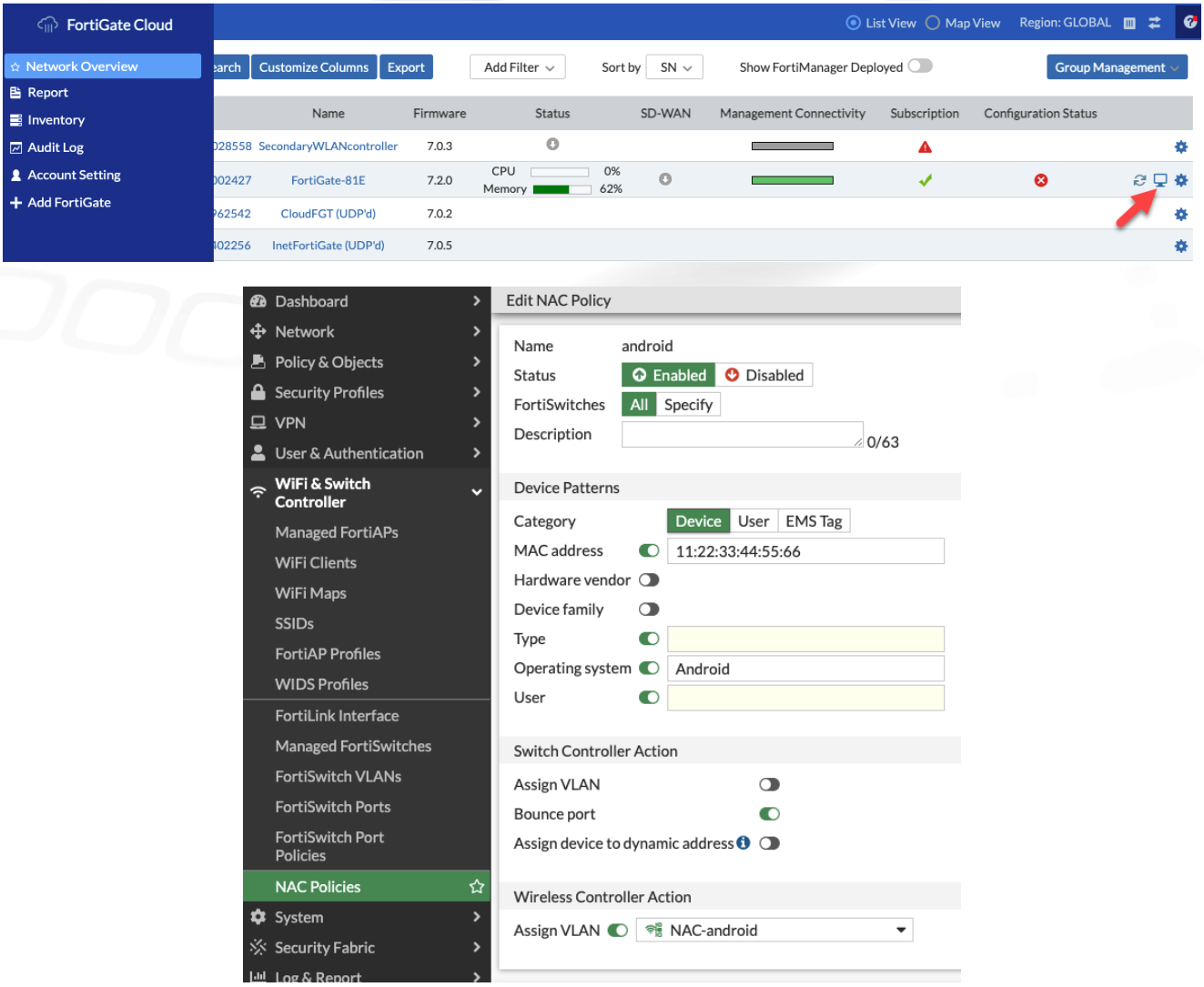


VLAN isolation, FortiGate firewall policies, and network architecture make this simple to secure. For IoT devices belonging to the same MPSK group and VLAN, create firewall policies that only allow exactly the traffic they must access. This is typically only to their management server on campus or perhaps a specific internet address.

Note that MPSK can provide an alternative to guest networking for long term users such as contractors. Contractors can be assigned to a contractor VLAN with exactly the access they require while onsite, and their MPSKs can be deleted when they leave.

FortiLink NAC is another approach available with Fortinet Security Driven Networking. FortiLink NAC dynamically assigns devices to VLANs based on selection criteria such as operating system, MAC address range, hardware vendor, and others. One advantage of FortiLink NAC is that it is not confined to PSK SSIDs and may prove useful for BYOD devices in conjunction with a RADIUS based username/password scheme. When FortiLink NAC is used with an SSID, a device connects to the SSID, authenticates, and is assigned to an initial onboarding VLAN. Once devices details are detected, the device is moved to a VLAN specifically secured to the device needs.

As of version FortiGate Cloud version 22.1, FortiLink NAC must be directly configured on the FortiGate UI, but FortiGate Cloud makes it simple to remotely, and directly, launch a remote session on each cloud connected FortiGate using the *Remote Access* button:



In many cases, it is simpler to administer NAC Policies than MPSK for IoT devices. With NAC Policies, administrators can group devices by certain device patterns and allow the FortiGate to automatically assign them to their isolated VLAN. With MPSK, administrators must have a procedure to define which users or devices belong to a MPSK group and assign keys to them. However, these decisions are dependent on the needs of individual branch network(s). The critical security concern is for devices to get assigned to an isolated VLAN, which can be accomplished by both security provisioning methods.

To learn more about MPSK and FortiLink NAC, see the following documents:

- Configuring WPA2-Personal security with MPSK
- Combined MAC and MPSK based authentication
- Configuring wireless NAC support

FortiGate Cloud Wi-Fi Design Conclusion

The FortiGate Cloud Wireless LAN architecture is highly adaptable. It scales both up and down from one or two Access Points to hundreds of Access Points, at one site to multiple branches. It is architected to easily overlay an existing wired network at any given site from any vendor, or to serve in a completely new network deployment.

FORTIGATE CLOUD WI-FI DESIGN CONCLUSION

Fortinet's *Security Driven Networking* ensures no branch's WLAN unsecured. Every SSID created in the FortiGate Cloud for the onsite WiFi Controller is also a layer 3 interface on the FortiGate Next Generation Firewall. WLAN traffic is VLAN isolated by default, without having to specifically create VLANs or deploy them throughout the wired network. All WLAN traffic is tunneled and inspected by the NGFW, and allowed only when specifically compliant with all policies.

With Wi-Fi and network security integrated under a true single-pane-of-glass, the Campus Network administrator's job is simplified. WLAN complexity comes as much from the variety of end users and client devices as from Wi-Fi design. The FortiGate Cloud branch architecture is designed to accommodate as much, or as little, differentiation of user classes as needed, all without having to make any changes to any pre-existing underlying wired network.

Fortinet's Security-driven Networking strategy tightly integrates an organization's network infrastructure and security architecture, enabling the network to scale and change without compromising security. This next generation approach is essential for effectively defending today's highly dynamic environments—not only by providing consistent enforcement across today's highly flexible perimeters, but by also weaving security deep into the network itself.

Appendix A: Documentation References

Feature Documentation

- FortiGate Cloud Administration Guide
- 7.0 FortiWiFi and FortiAP Configuration Guide
- FortiCloud Account Services

Solution Hub

- FortiGate Cloud Solution Hub
- Secure Access Solution Hub

Related 4-D Documentation

- FortiCloud Overview
- Secure Wireless Concept Guide

www.fortinet.com