Architecture Guide

Campus Wireless LAN

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change Log

Date	Change Description
2022-02-11	Initial release.
2022-05-03	Updated Introduction on page 5.
2022-06-08	Updated FortiAP Placement Guidelines and Channel Planning on page 13.
2023-07-05	Updated Solution and technologies on page 7

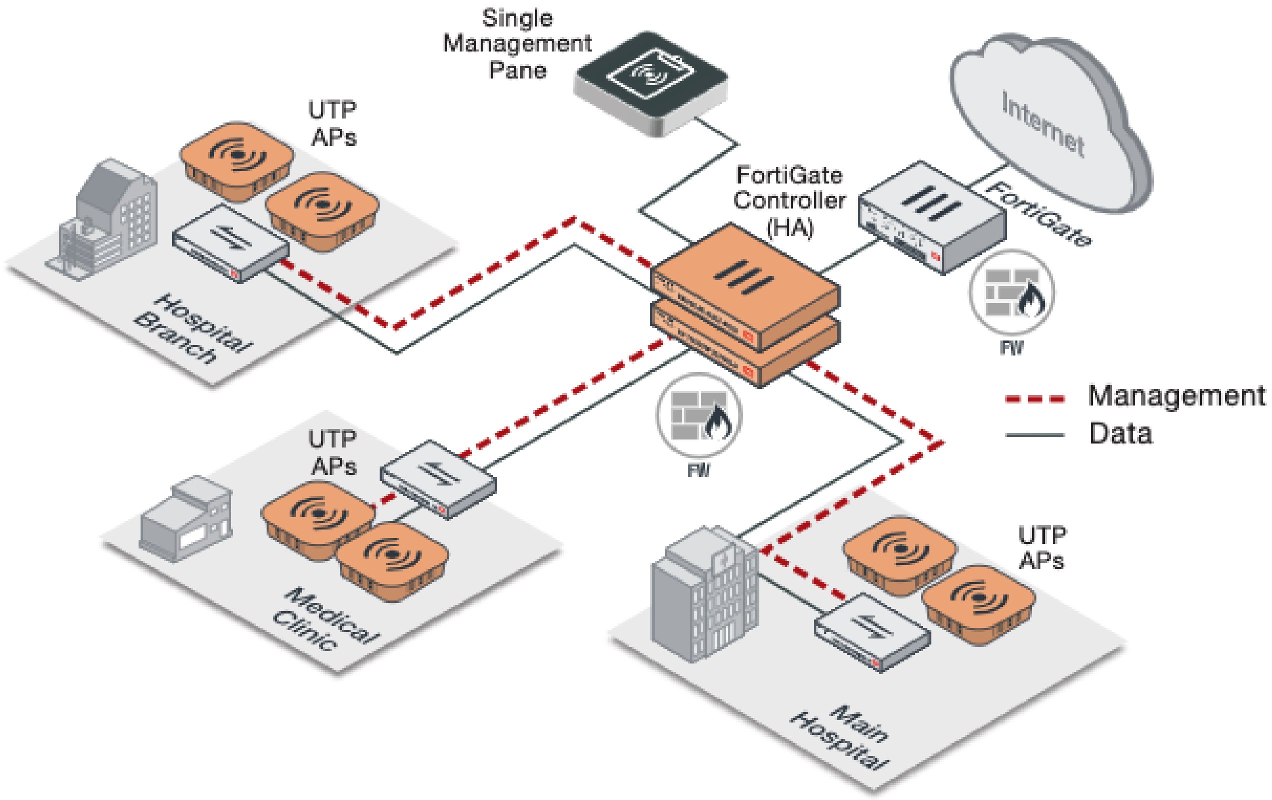
Introduction

Executive Summary

This document is intended to provide an architectural overview for campus WLANs using Fortinet Wi-Fi gear. Specifically, FortiAPs that are centrally managed on-site by a pair of FortiGate Integrated WLAN Controllers in High Availability (HA) with most, if not all, Wi-Fi traffic tunneled into the FortiGate HA pair. As one would expect from Fortinet, this architecture lends itself to maximize security of the WLAN, but is nevertheless simple and highly adaptable.

"Campus" covers a wide range of networks and locations, from multiple floors in an office tower to a university campus of a couple hundred acres. However, our recommended architecture remains the same for this wide range. In general, a single location that needs anything from dozens to about 4000 APs, with 100 to 100,000 devices will fit this campus model.

The Fortinet Campus WLAN architecture



- Main Internet NGFW Gateway
- FortiGate Integrated WLAN Controllers in HA mode
- Campus switch network

    - Campus Access/AP switches with PoE
- FortiAP controller discovery and authorization
- Possible Mesh AP backhaul
- Security isolation oriented SSIDs for
    - Corp users
    - Guest users
    - IoT devices
    - FortiLink NAC/onboarding
- Inspection policies at the controller(s)

Intended Audience

This guide is intended for an audience who is interested in learning about Fortinet's Campus 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

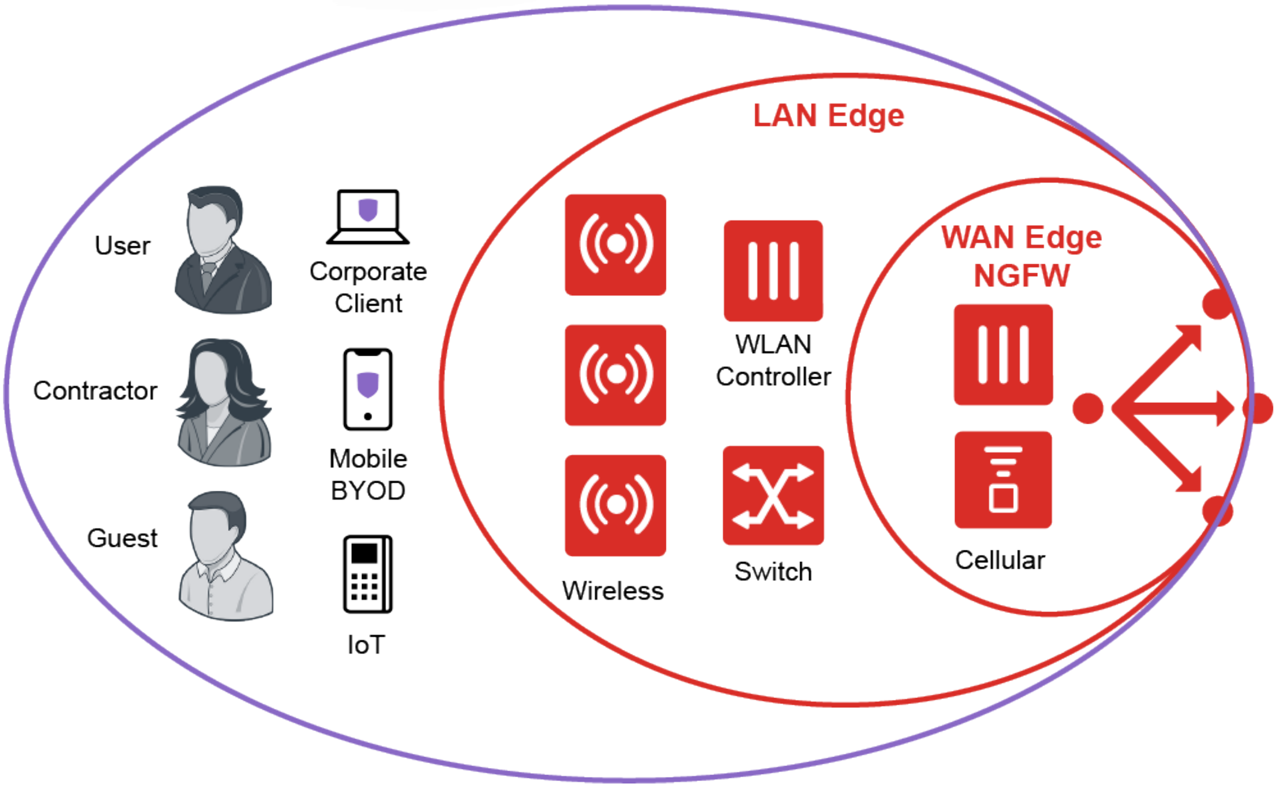
After reading the Fortinet Secure Wireless LANs Concept Guide, readers should have a basic understanding of the concepts and terminologies behind the Fortinet Wireless infrastructure. This guide explores further the design of a Wireless LAN within the scope of a Campus network. Learn about the role of 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.

You should use this guide to gather ideas for designing your wireless solution. After completing this Architecture guide, you may move on to the Fortinet Campus 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 Wi-Fi networks exist to service Wi-Fi devices, but Wi-Fi devices fall into a wide range of who they belong to and how they should be secured. The nature of a campus deployment is not just the large physical size of the network, but the greater complexity of who and what is using that network. As the network grows in size, security needs usually become more complex with more categories of end devices. At Fortinet we call this the *LAN Edge*.



Physically, the LAN Edge is just the access layer, but securing the access layer now has to account for a bewildering mix of devices: enterprise owned, end user owned, guest users, known users, IoT devices with no associated users, 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 a multi-purpose 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 cyber security in a single appliance increases and simplifies cyber security for the entire network.

A FortiGate Secure Wireless Controller serves as the central Wi-Fi management system for Campus WLANs and deployed FortiAPs. All WLAN functions can be configured, managed and secured from the same FortiGate browser-based management interface. The FortiGate Wireless Controller supports multiple architectural options, but the default, and recommended in the majority of cases, is that all WLAN traffic is tunneled to the controller and then forwarded/routed from the controller onto the campus 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, such that all traffic is VLAN/subnet isolated without the need to actually deploy those VLANs or even map to existing VLANs. 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. The essence of Security Driven Networking

FortiGate Integrated Wi-Fi Controller Key Features

Integration with FortiOS/FortiGate Operating System and 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. Maximized end-to-end security, via a true single-pane-of-glass for wireless and security configuration.

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
- UTM series FortiAPs support dual 5 GHz settings for advanced channel plans

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 controllers that support more than 4000 APs, all tunneled traffic goes to a single state machine, avoiding complex tunneling through multiple intermediary controllers.

Integrated Guest Access Management - Local 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 attack identification.

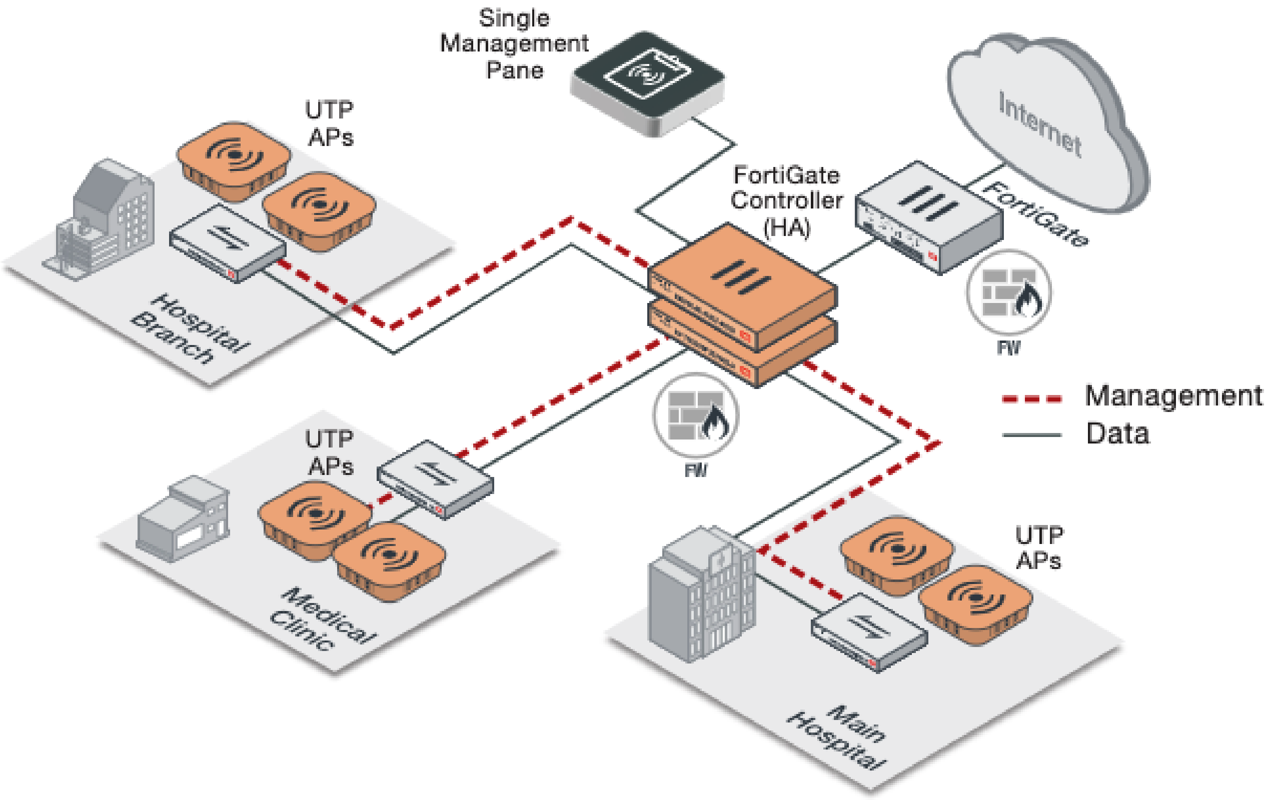
Device fingerprinting and FortiLink NAC - device fingerprinting identifies all client devices by type, operating system, and other factors. FortiLink NAC can then use that information to assign devices to designated VLANs, whether company owned or BYOD or IoT.

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.

The Fortinet Campus WLAN architecture



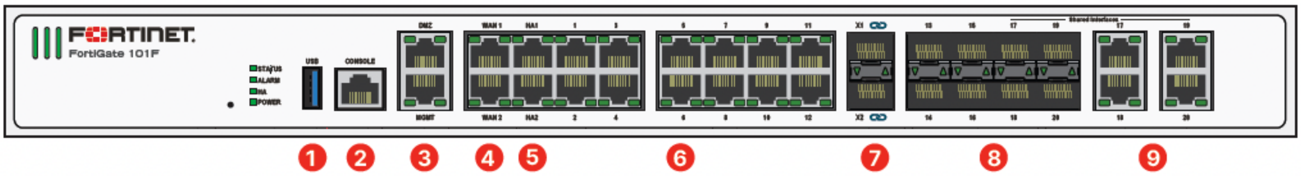
- Main Internet NGFW Gateway
- FortiGate Integrated WLAN Controllers in HA mode
- Campus switch network

  - Campus Access/AP switches with PoE
- FortiAP controller discovery and authorization
- Possible Mesh AP backhaul
- Security isolation oriented SSIDs for
  - Corp users
  - Guest users
  - IoT devices
  - FortiLink NAC/onboarding
- Inspection policies at the controller(s)

Design Overview

This section contains the following topics:

FortiGate Secure WLAN Controller Logical and Physical Placement



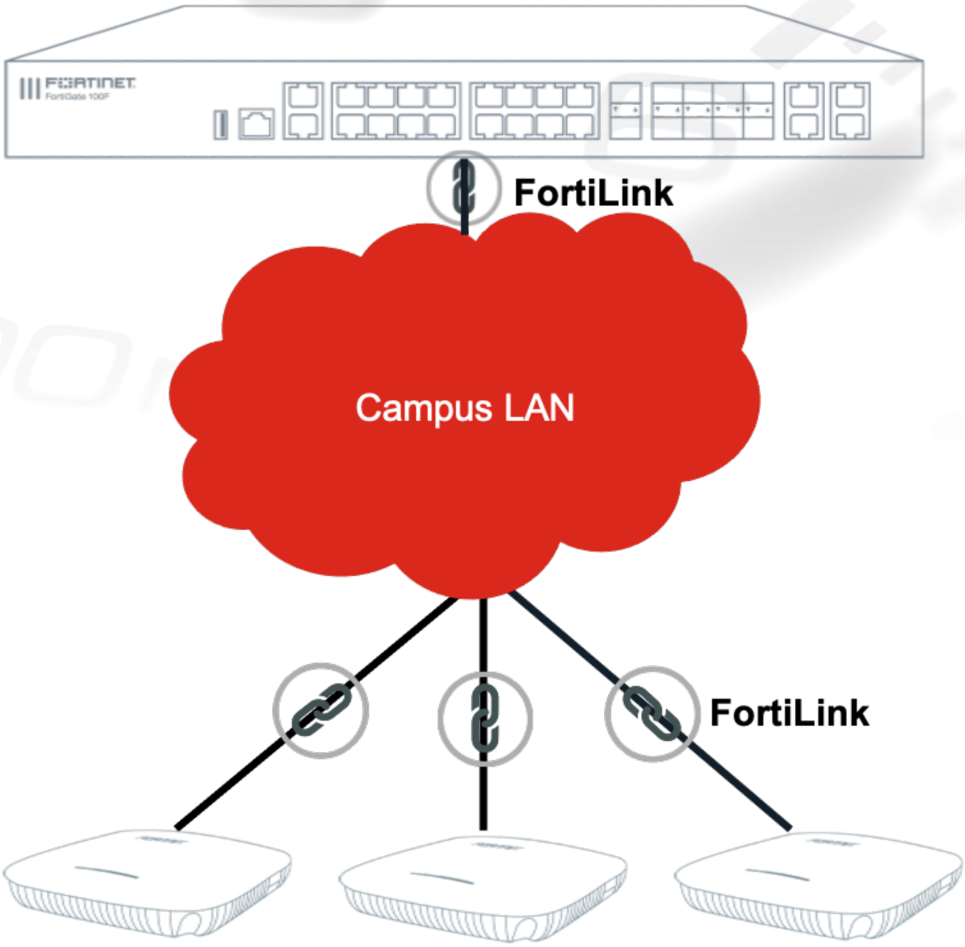
For Campus deployments with substantial numbers of APs, the Secure WLAN Controller FortiGates should generally NOT be the main WAN/Internet firewall, for a number of reasons.

For maximum flexibility, Fortinet WLAN equipment is fully compliant with network standards and will work with any vendor's network equipment. While we think our customers would be well served by having a FortiGate as their primary Internet firewall and SD-WAN solution, most networks are multi-vendor.

Even when the main Internet Firewall is a FortiGate, experience has shown that best practice is to separate the WLAN administration from the Internet Firewall/SD-WAN. This way administration of WLANs and WLAN security is simplified and appropriately divided. Performance can be 'right-sized' for the differing jobs, troubleshooting simplified, and etc. The Controller FortiGate(s) can be thought of as Internal Segmentation Firewalls for WLAN traffic.

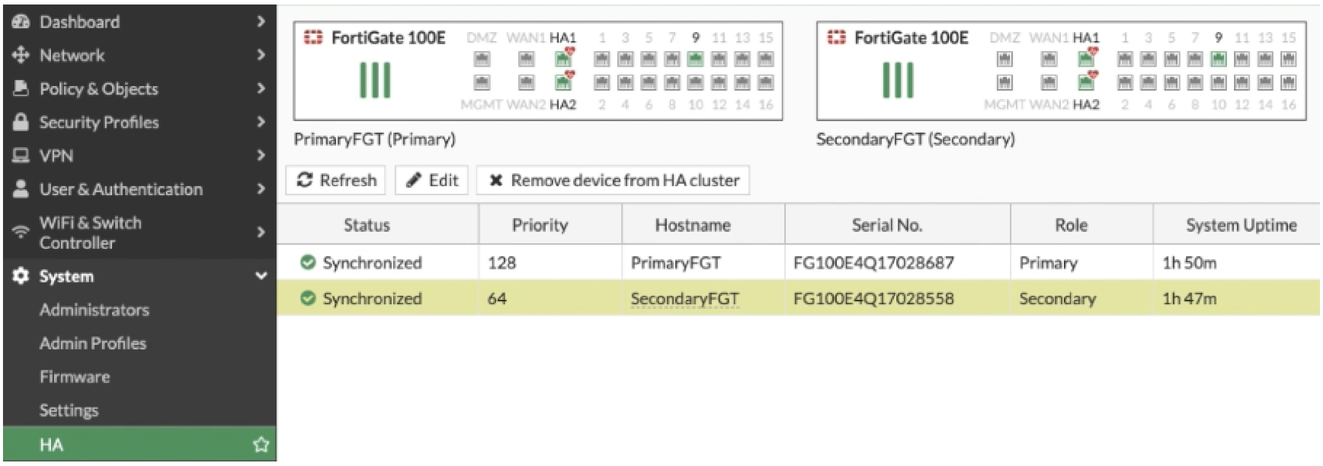
Controller and FortiAP communication

FortiAPs will 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 will work over L2 or L3. So any logical placement that allows routing from the APs to the FortGate 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.

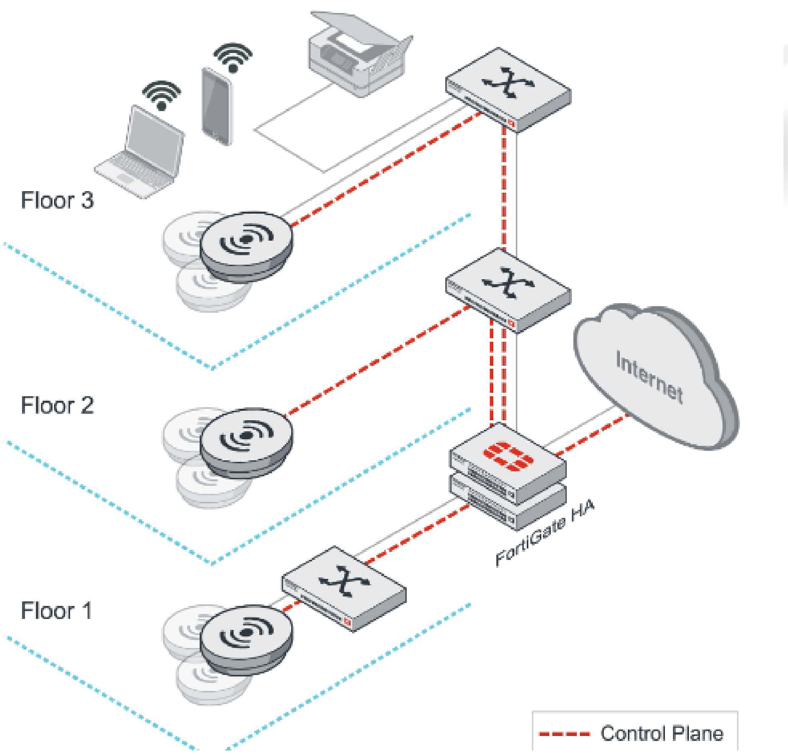


No WLAN VLAN will need to be defined going to the controller. VLANs will essentially exist in the tunnel and within the FortiGate but usually nowhere else.

FortiGate WLAN controllers should be deployed in Active/Passive High Availability mode to provide redundancy for this critical portion of the network.



Status	Priority	Hostname	Serial No.	Role	System Uptime
✓ Synchronized	128	PrimaryFGT	FG100E4Q17028687	Primary	1h 50m
✓ Synchronized	64	SecondaryFGT	FG100E4Q17028558	Secondary	1h 47m



Central pair of FortiGates managing a large site

Access Layer and Power consumption

Although the FortiGate WLAN controllers for a given network might be placed at any network level—access, distribution, or core layers of the typical switch network—FortiAPs are Wireless Access Points which are part of the access layer of the campus network and are on the LAN Edge boundary. As a general rule, the indoor Wi-Fi FortiAPs require 802.3bt High Power over Ethernet and support 2.5 Gigabit Ethernet speeds. The underlying switch network should be ready to support that for maximum value. Confirm capabilities of switch ports are matched to the FortiAPs, whether new or existing.

Wi-Fi 6 FortiAPs will work with Gigabit Ethernet, and will operate on basic 802.3af PoE, but capabilities will be reduced. There are also special case FortiAPs, such as the FAP831, an ultra-High-Density model with two 5 GE ports for uplink. There are also outdoor models with a PoE output to another device, and will require higher input power to support that output. Refer to the datasheet 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 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. This encourages a tendency to just swap out the old access points for new FortiAPs. 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. In generally, 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

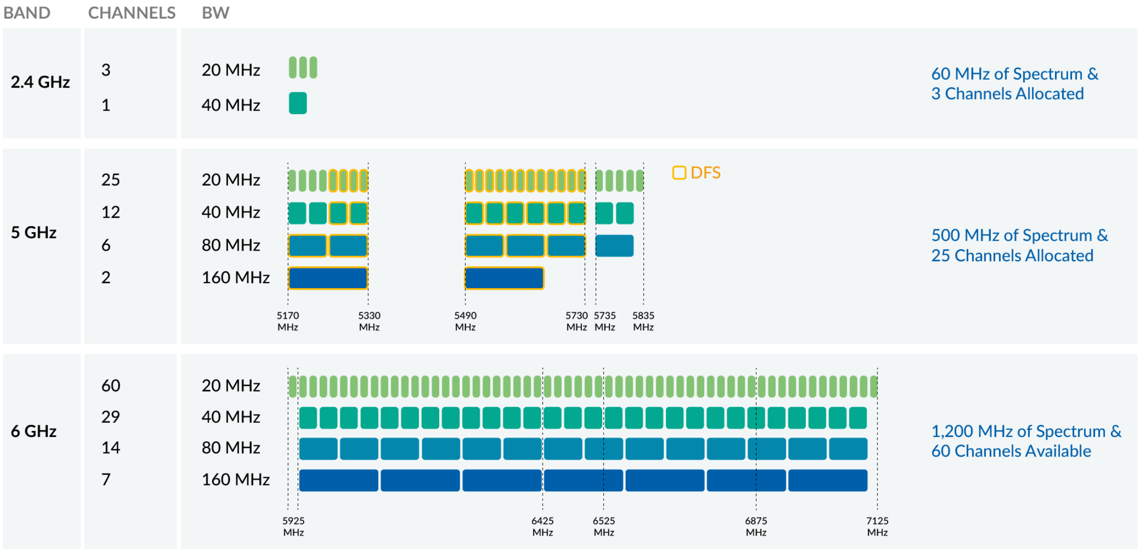
As a rule of thumb, for a pre-survey estimate, an indoor area probably requires about 1 FortiAP per 2000 Sq-Ft, with around 30 devices per AP radio. All the Wi-Fi 6 FortiAPs have 1 radio for monitoring and 2 service radios. Users are usually assumed to have 3 devices each, so 20 users and 60 devices 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 estimates, 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.

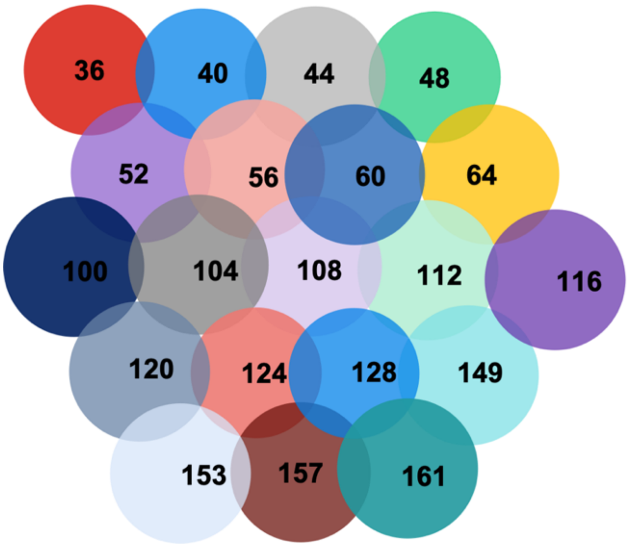
It is best to avoid requiring client-to-FortiAP radio connections to pass through more than one wall. Although one cannot see Wi-Fi signals, line of site connectivity to client devices is best, so a designer can visualize coverage by thinking about how they would deploy light fixtures. Placing APs in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

Channel Planning - Design for 5 GHz

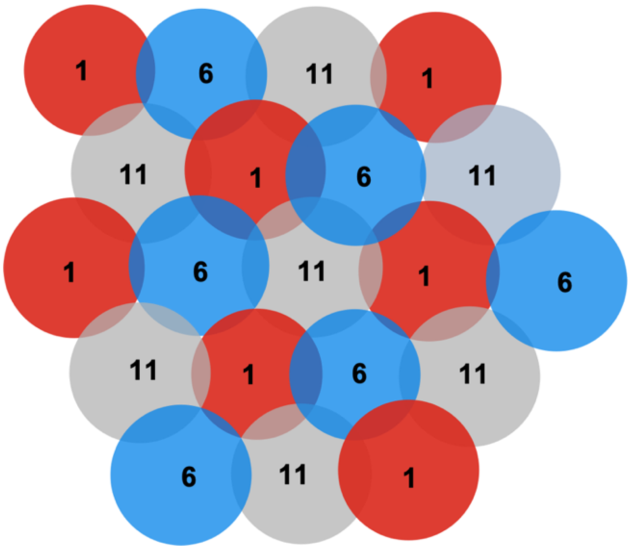
Wi-Fi in general has evolved quite a bit in a relatively short time, and so have other wireless technologies such as Bluetooth and its variations. The default assumption for Wi-Fi in the past was to design for 2.4 GHz and treat 5 GHz as secondary. Now that Wi-Fi 6 is available, Fortinet recommends designing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



5 GHz channel plan (20MHz wide)

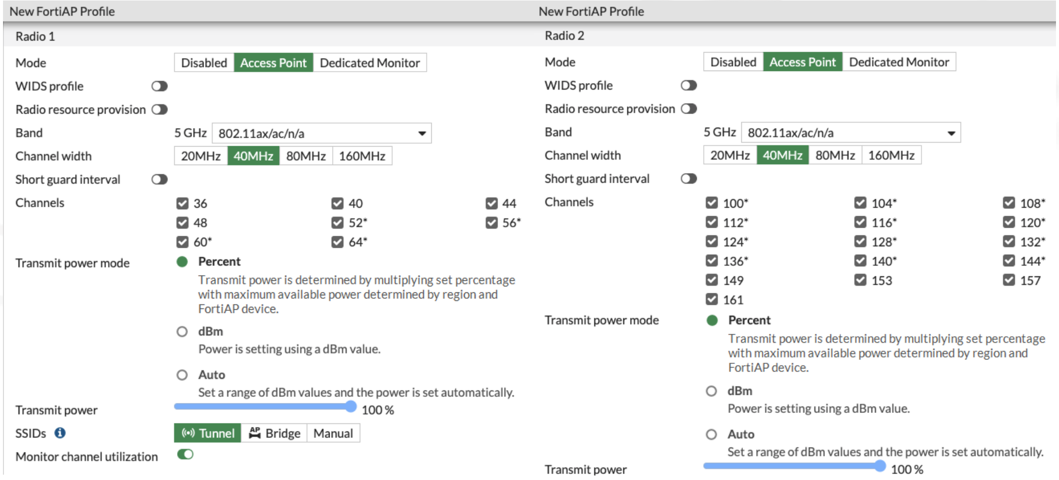


2.4 GHz channel plan

Very few client devices are so old 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.

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 to alternate the selectable radio between 5 GHz and 2.4 in the FortiAP Profiles. FortiAP profiles are per AP model, but APs can also be grouped if there is a need for different profiles on the same model on different parts of the campus.



New FortiAP Profile

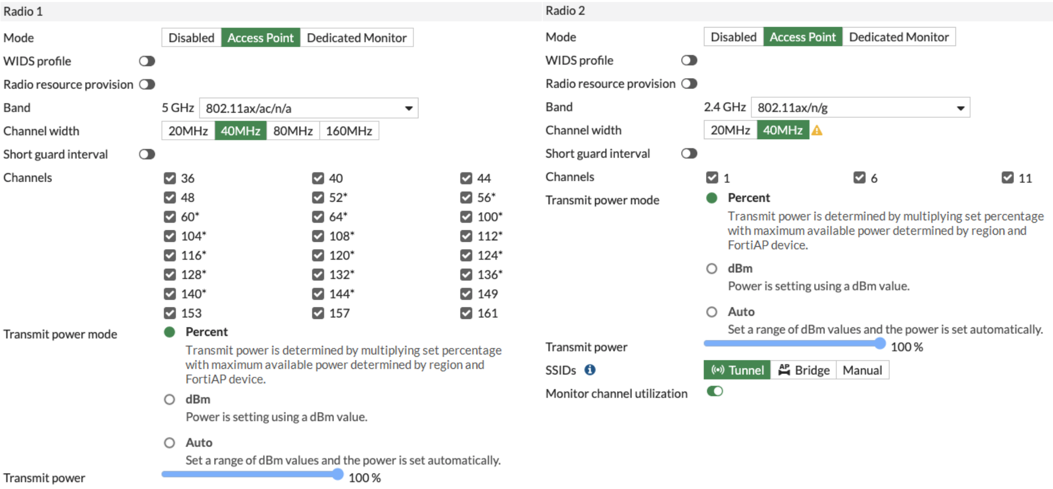
Radio 1

Mode: Disabled | **Access Point** | Dedicated Monitor
WIDS profile: ○
Radio resource provision: ○
Band: 5 GHz 802.11ax/ac/n/a
Channel width: 20MHz | **40MHz** | 80MHz | 160MHz
Short guard interval: ○
Channels:
☑ 36 ☑ 40 ☑ 44
☑ 48 ☑ 52* ☑ 56*
☑ 60* ☑ 64*
Transmit power mode:
● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.
○ dBm
Power is setting using a dBm value.
○ Auto
Set a range of dBm values and the power is set automatically.
Transmit power: 100 %
SSIDs: **Tunnel** | Bridge | Manual
Monitor channel utilization: ●

New FortiAP Profile

Radio 2

Mode: Disabled | **Access Point** | Dedicated Monitor
WIDS profile: ○
Radio resource provision: ○
Band: 5 GHz 802.11ax/ac/n/a
Channel width: 20MHz | **40MHz** | 80MHz | 160MHz
Short guard interval: ○
Channels:
☑ 100* ☑ 104* ☑ 108*
☑ 112* ☑ 116* ☑ 120*
☑ 124* ☑ 128* ☑ 132*
☑ 136* ☑ 140* ☑ 144*
☑ 149 ☑ 153 ☑ 157
☑ 161
Transmit power mode:
● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.
○ dBm
Power is setting using a dBm value.
○ Auto
Set a range of dBm values and the power is set automatically.
Transmit power: 100 %



Radio 1

Mode: Disabled | **Access Point** | Dedicated Monitor
WIDS profile: ○
Radio resource provision: ○
Band: 5 GHz 802.11ax/ac/n/a
Channel width: 20MHz | **40MHz** | 80MHz | 160MHz
Short guard interval: ○
Channels:
☑ 36 ☑ 40 ☑ 44
☑ 48 ☑ 52* ☑ 56*
☑ 60* ☑ 64* ☑ 100*
☑ 104* ☑ 108* ☑ 112*
☑ 116* ☑ 120* ☑ 124*
☑ 128* ☑ 132* ☑ 136*
☑ 140* ☑ 144* ☑ 149
☑ 153 ☑ 157 ☑ 161
Transmit power mode:
● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.
○ dBm
Power is setting using a dBm value.
○ Auto
Set a range of dBm values and the power is set automatically.
Transmit power: 100 %

Radio 2

Mode: Disabled | **Access Point** | Dedicated Monitor
WIDS profile: ○
Radio resource provision: ○
Band: 2.4 GHz 802.11ax/n/g
Channel width: 20MHz | **40MHz** ⚠
Short guard interval: ○
Channels: ☑ 1 ☑ 6 ☑ 11
Transmit power mode:
● Percent
Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.
○ dBm
Power is setting using a dBm value.
○ Auto
Set a range of dBm values and the power is set automatically.
Transmit power: 100 %
SSIDs: **Tunnel** | Bridge | Manual
Monitor channel utilization: ●

Radio Resource Provision should be enabled in FortiAP profiles and transmit power set to automatic in order for the campus network to take full advantage of FortiOS DARRP (Distributed Automatic Radio Resource Provisioning). DARRP will optimizes 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. Meanwhile, 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 WiFi concepts document 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.

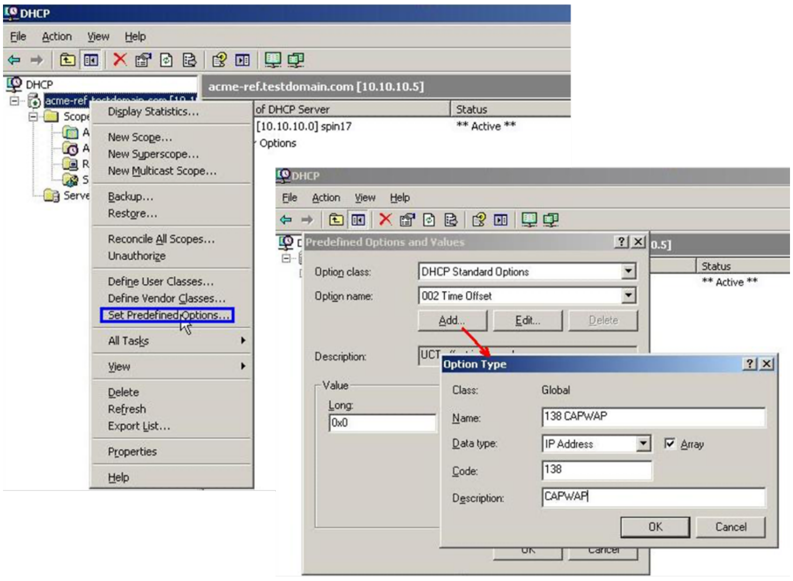
FortiAP Discovery, Authorization and Control Plane

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 will usually require some preparation of the underlying network.

Best practice is for the FortiAPs to be on an AP specific subnet. It does not have to be a FortiAP only subnet, but it is the *Control Plane* subnet for the FortiAPs and FortiLink communication with the FortiGate Controller. FortiAPs will use DHCP to get an IP address. The subnet's DHCP server, or its DNS server, can be configured to tell the FortiAP the IP address of the controllers. Of course, 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 networks. For example, on a Windows DHCP Server:

1. Go to *Set Predefined Options* and click *Add*.
2. *Name* the option.
3. Set *Code* to `138`.
4. In *Type* enter the IP address, and click *OK.*
5. Go to the option name and enter the controller IP address as a value.
6. Go to the scope the FortiAPs will use and click *Configure options.*
7. Check *option 138*, and then click *OK*.



acme-ref.testdomain.com [10.10.10.5]

[10.10.10.0] spin17 ** Active **

Predefined Options and Values

Option class: DHCP Standard Options

Option name: 002 Time Offset

Value Long: 0x0

Option Type

Class: Global

Name: 138 CAPWAP

Data type: IP Address ☑ Array

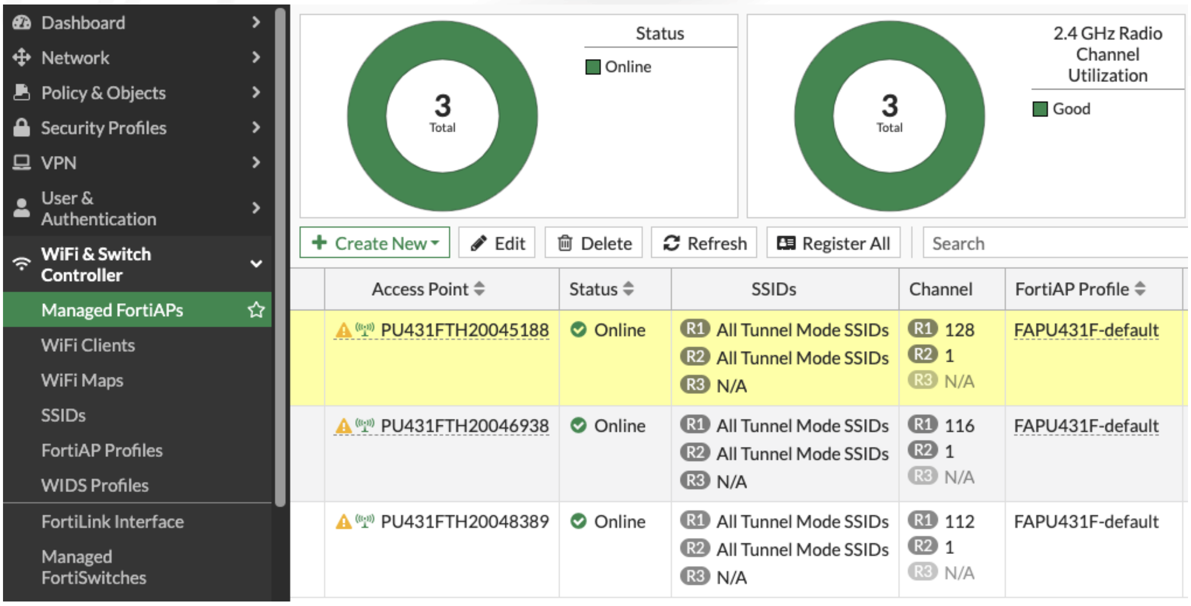
Code: 138

Description: CAPWAP

For DNS resolution, configure the DNS server to respond to `_capwap-control._udp.example.com` with the Wi-fi controller IP address.

When the controller and the FortiAP are in the same broadcast domain, the FortiAP will easily locate the FortiGate via broadcast, but a Campus deployment can be assumed to have L3 separation between the FortiAPs and the FortiGate. Multi-cast is also supported, and APs can be preconfigured via CLI with the controller address, but DHCP and DNS are usually the simplest in campus networks. See the FortiAP documentation for details on these discovery methods

Once FortiAPs have established FortiLink communications with the FortiGate, it must be authorized in *Managed FortiAPs* by right-clicking on the FortiAP entry and selecting *Authorize*.



Access Point	Status	SSIDs	Channel	FortiAP Profile
PU431FTH20045188	Online	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs R3 N/A	R1 128 R2 1 R3 N/A	FAPU431F-default
PU431FTH20046938	Online	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs R3 N/A	R1 116 R2 1 R3 N/A	FAPU431F-default
PU431FTH20048389	Online	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs R3 N/A	R1 112 R2 1 R3 N/A	FAPU431F-default

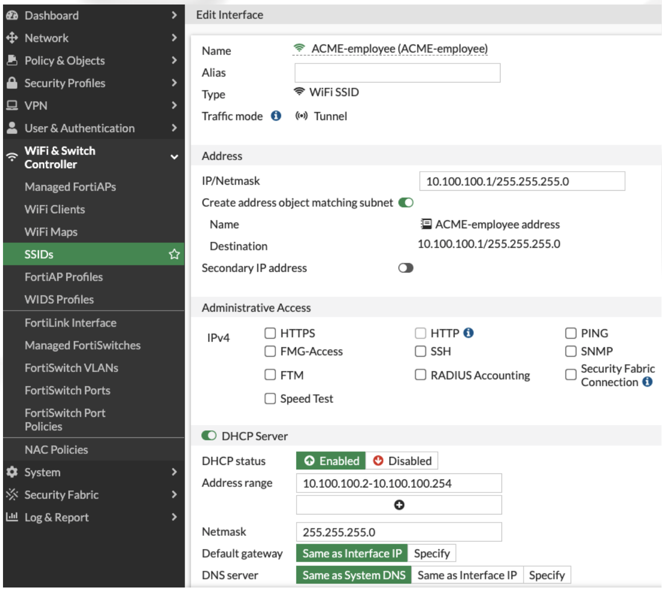
SSID Configuration and Traffic mode

SSIDs and Secure Interface Integration

SSID (or WLAN) setup on a FortiOS Wi-Fi controller 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 then 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.

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 Controllers 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 configure any VLANs for Wi-Fi traffic. As part of the configuration flow, a DHCP server can also be configured, again, 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.



Edit Interface

Name: ACME-employee (ACME-employee)
Alias:
Type: WiFi SSID
Traffic mode: Tunnel

Address
IP/Netmask: 10.100.100.1/255.255.255.0
Create address object matching subnet: ●
Name: ACME-employee address
Destination: 10.100.100.1/255.255.255.0
Secondary IP address: ○

Administrative Access
IPv4: □ HTTPS □ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection □ Speed Test

DHCP Server ●
DHCP status: [✓ Enabled] Disabled
Address range: 10.100.100.2-10.100.100.254
Netmask: 255.255.255.0
Default gateway: [✓ Same as Interface IP] Specify
DNS server: [✓ Same as System DNS] Same as Interface IP Specify

Bridge Mode, on the other hand keeps the SSID operation at Layer-2, with traffic being directly bridged to 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 campus deployment—the tight integration with FortiGate's security and inspection capabilities.

Mesh mode is for 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, the two latest generations of Wi-Fi security, WPA2 and WPA3 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), but client support is still not 100%. When possible, use WPA3, and if not possible develop a plan for transitioning to it, depending on your clients.

With WPA2 and WPA3, there are three basic security modes, covering 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 normally used for guest users.

- **Firewall policies and other inspection options.** One of the benefits of using FortiOS Integrated WLAN Controllers is that 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 '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 here 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 classes can share a single SSID while using RADIUS attributes to assign them different VLANs.

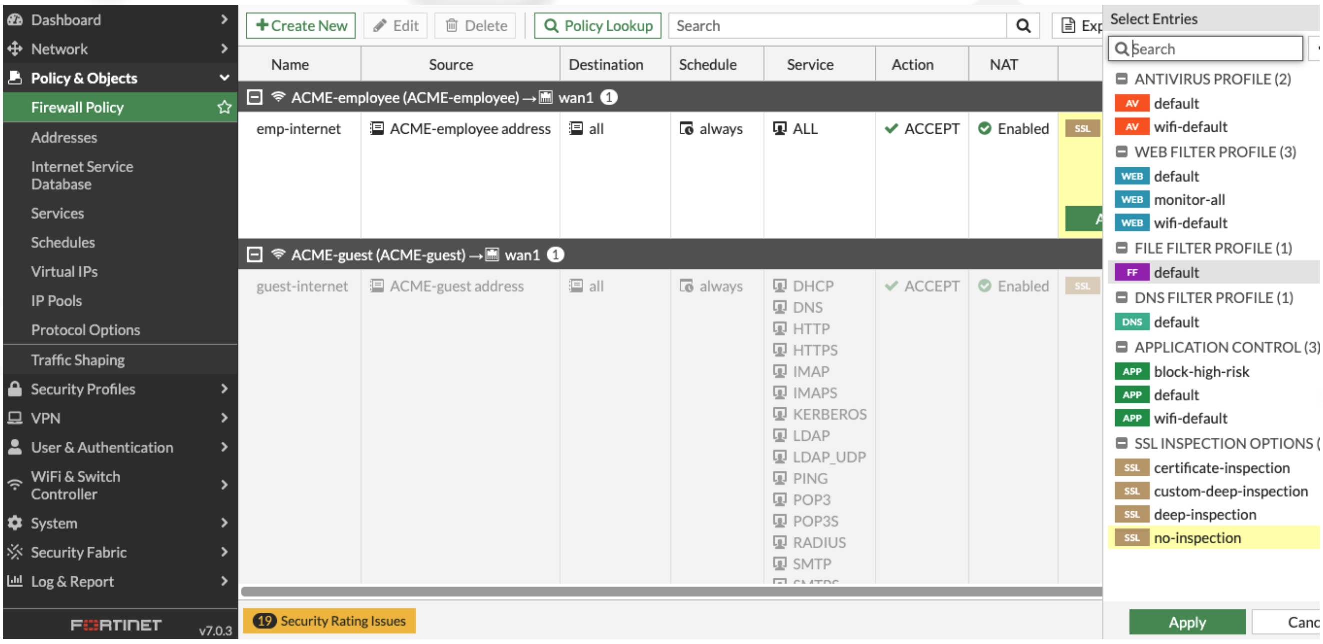
Fully authenticated users using Enterprise class WPA2 or WPA3.

Fully authenticated or Known users are campus 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 Wi-Fi.

A campus deployment might 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 be included, such as Anti-virus, Web Filter, Application Control, and etc.



Name	Source	Destination	Schedule	Service	Action	NAT
ACME-employee (ACME-employee) → wan1 1						
emp-internet	ACME-employee address	all	always	ALL	✓ ACCEPT	Enabled
ACME-guest (ACME-guest) → wan1 1						
guest-internet	ACME-guest address	all	always	DHCP DNS HTTP HTTPS IMAP IMAPS KERBEROS LDAP LDAP_UDP PING POP3 POP3S RADIUS SMTP	✓ ACCEPT	Enabled

Select Entries

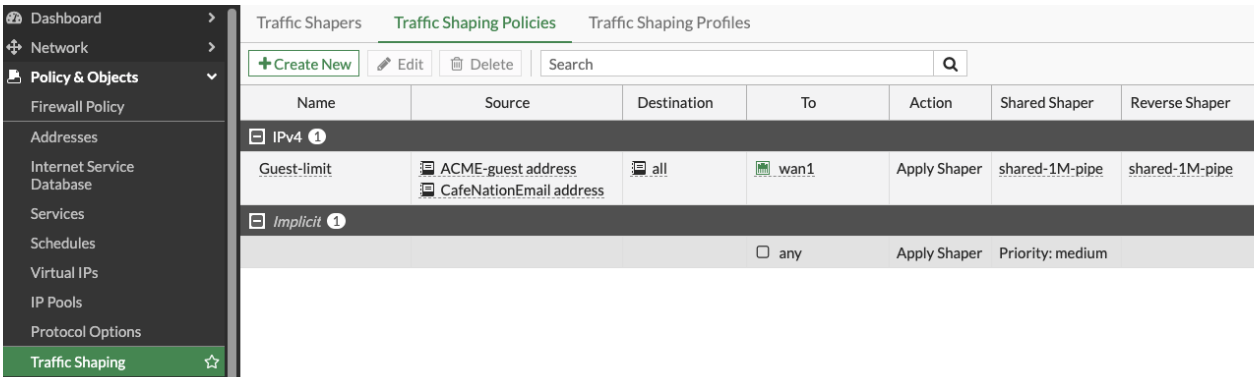
- ANTIVIRUS PROFILE (2)
  - AV default
  - AV wifi-default
- WEB FILTER PROFILE (3)
  - WEB default
  - WEB monitor-all
  - WEB wifi-default
- FILE FILTER PROFILE (1)
  - FF default
- DNS FILTER PROFILE (1)
  - DNS default
- APPLICATION CONTROL (3)
  - APP block-high-risk
  - APP default
  - APP wifi-default
- SSL INSPECTION OPTIONS (
  - SSL certificate-inspection
  - SSL custom-deep-inspection
  - SSL deep-inspection
  - SSL no-inspection

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 should be added. Traffic shaping policies are very similar to firewall policies and are found in their own table under policy and objects.



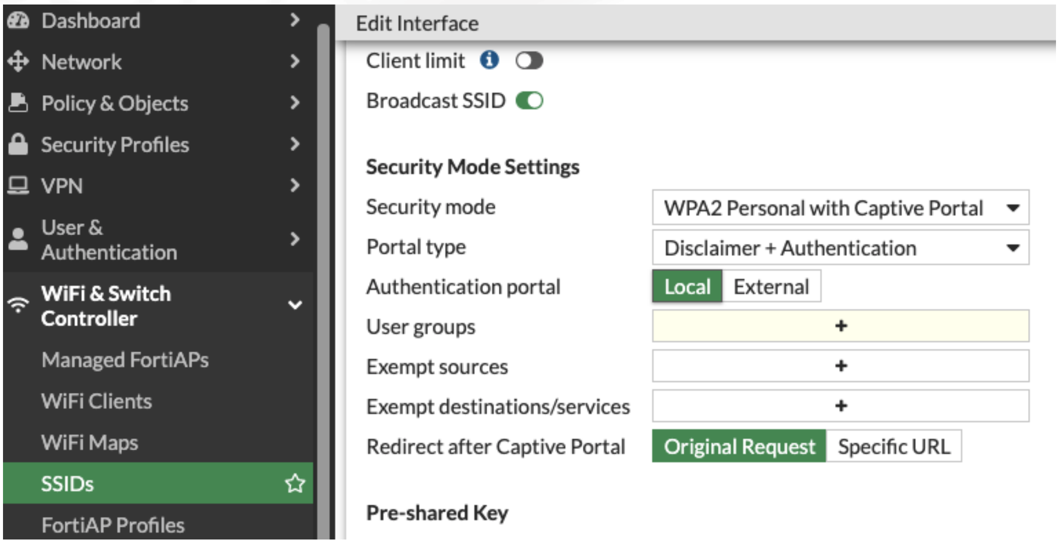
Name	Source	Destination	To	Action	Shared Shaper	Reverse Shaper
IPv4 1						
Guest-limit	ACME-guest address CafeNationEmail address	all	wan1	Apply Shaper	shared-1M-pipe	shared-1M-pipe
Implicit 1						
			any	Apply Shaper	Priority: medium	

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. This option is useful for reducing casual use of the network by neighbors when the portal is a disclaimer only.



Edit Interface

Client limit ○

Broadcast SSID ●

Security Mode Settings

Security mode	WPA2 Personal with Captive Portal
Portal type	Disclaimer + Authentication
Authentication portal	[✓ Local] External
User groups	+
Exempt sources	+
Exempt destinations/services	+
Redirect after Captive Portal	[✓ Original Request] Specific URL

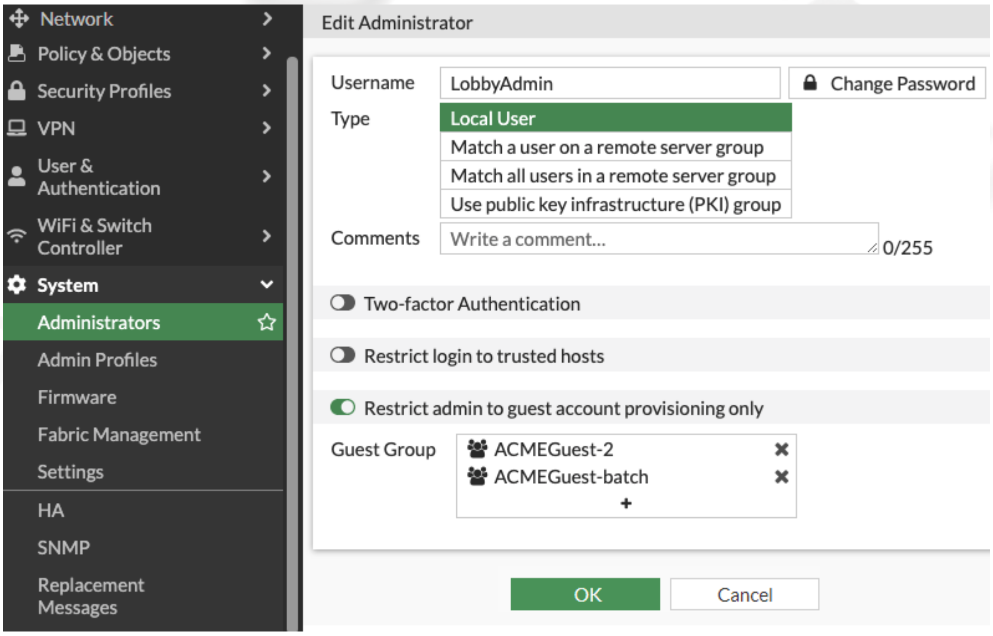
Pre-shared Key

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, 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 example is a FortiGate administrator that is restricted to only managing and provisioning guest user accounts.



Edit Administrator

Username: LobbyAdmin 🔒 Change Password

Type: Local User (selected) | Match a user on a remote server group | Match all users in a remote server group | Use public key infrastructure (PKI) group

Comments: Write a comment... 0/255

○ Two-factor Authentication

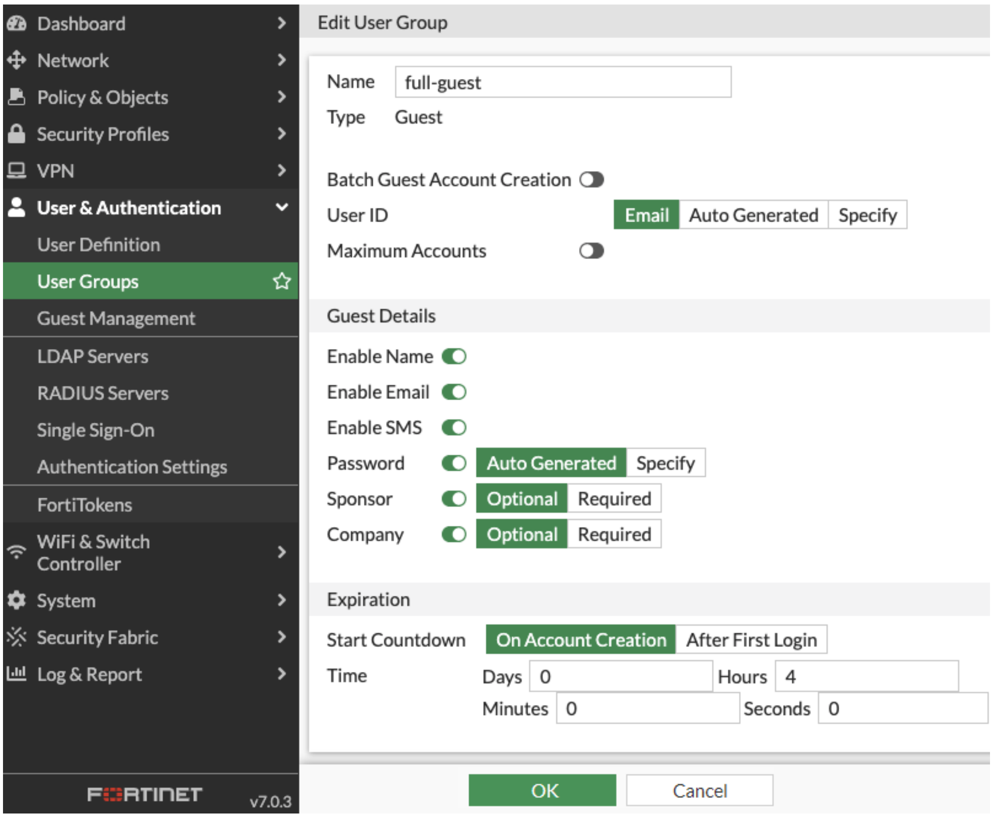
○ Restrict login to trusted hosts

● Restrict admin to guest account provisioning only

Guest Group: ACMEGuest-2 ✖
ACMEGuest-batch ✖
+

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 example is a Guest User group setup page showing options that can be configured for the group.



Edit User Group

Name: full-guest

Type: Guest

Batch Guest Account Creation ○

User ID: Email (selected) | Auto Generated | Specify

Maximum Accounts ○

Guest Details

Enable Name ●

Enable Email ●

Enable SMS ●

Password ● Auto Generated (selected) | Specify

Sponsor ● Optional (selected) | Required

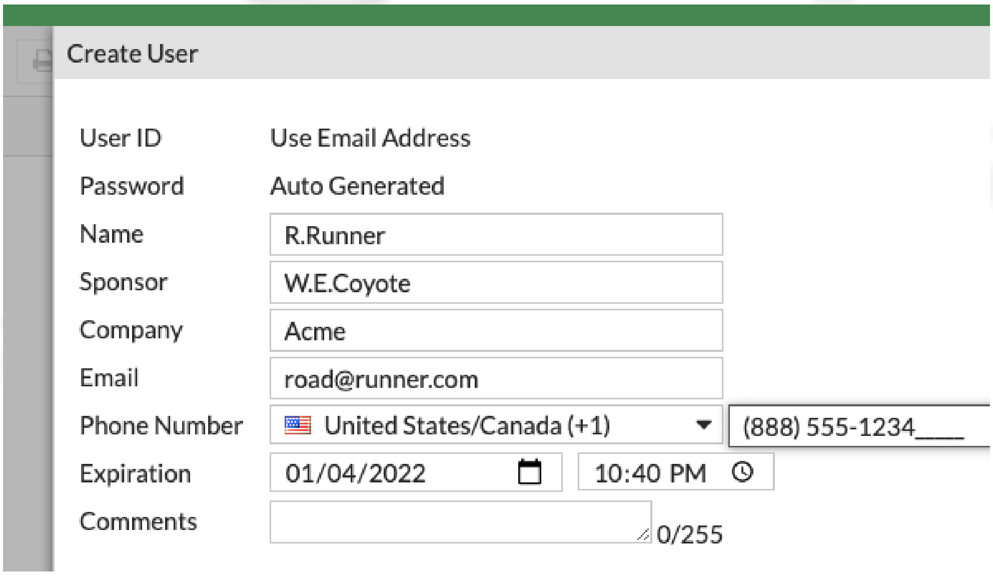
Company ● Optional (selected) | Required

Expiration

Start Countdown: On Account Creation (selected) | After First Login

Time: Days 0 Hours 4 Minutes 0 Seconds 0

The following example from *User & Authentication > Guest Management* is another location where a new Guest user can be manually added.



Create User

User ID	Use Email Address
Password	Auto Generated
Name	R.Runner
Sponsor	W.E.Coyote
Company	Acme
Email	road@runner.com
Phone Number	United States/Canada (+1) ▾ (888) 555-1234____
Expiration	01/04/2022 10:40 PM
Comments	0/255

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.

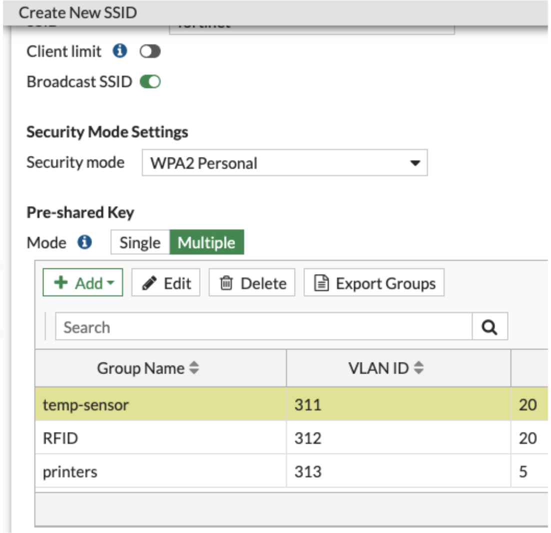
To learn more about Guest Management:

- Captive Portal Security
- Deploying captive portal SSID to FortiAP units
- Guest Management

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 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



Client limit
Broadcast SSID

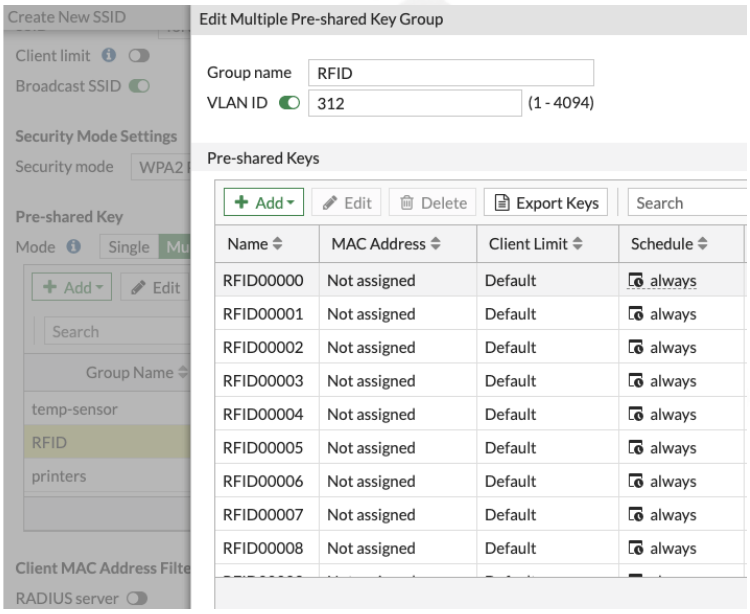
Security Mode Settings

Security mode: WPA2 Personal

Pre-shared Key

Mode: Single [✓ Multiple]

Group Name	VLAN ID	
temp-sensor	311	20
RFID	312	20
printers	313	5



Group name: RFID

VLAN ID: 312 (1 - 4094)

Pre-shared Keys

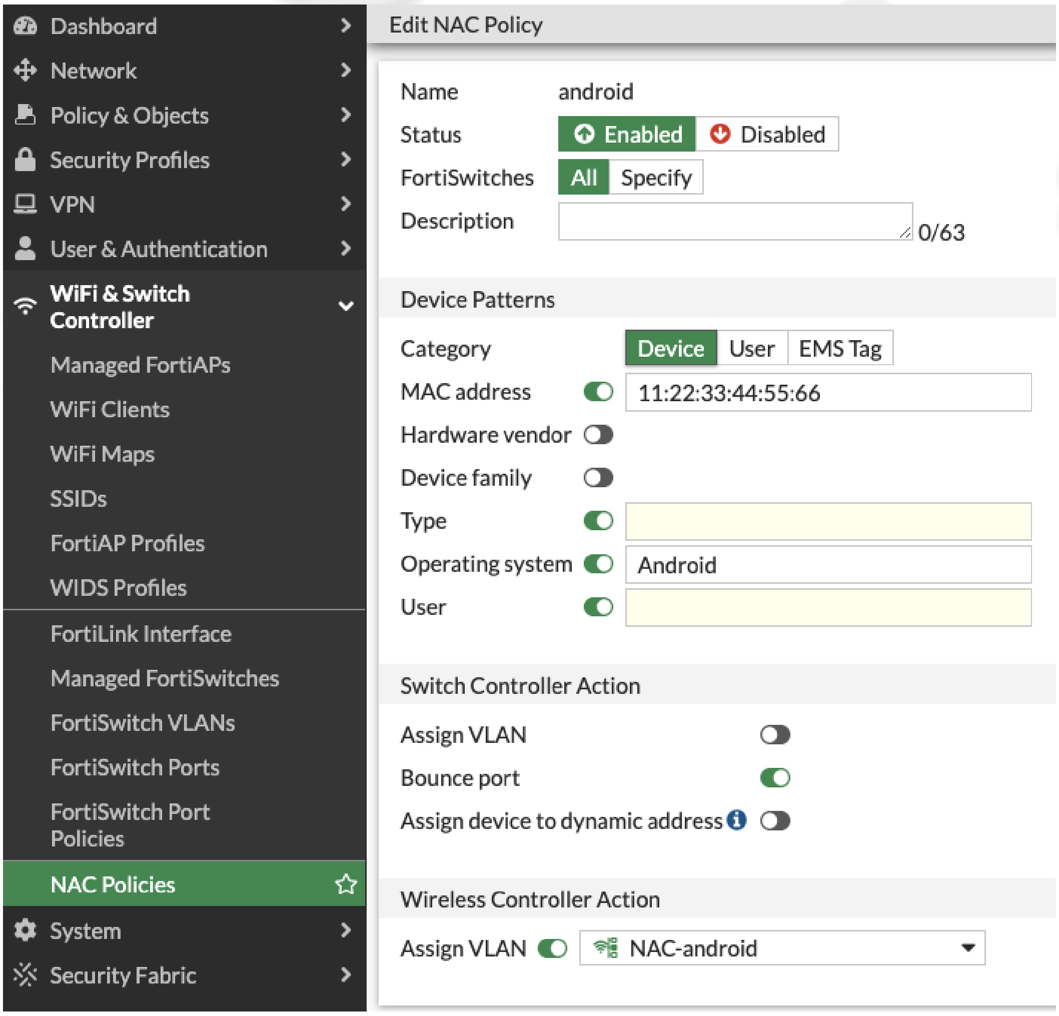
Name	MAC Address	Client Limit	Schedule
RFID00000	Not assigned	Default	always
RFID00001	Not assigned	Default	always
RFID00002	Not assigned	Default	always
RFID00003	Not assigned	Default	always
RFID00004	Not assigned	Default	always
RFID00005	Not assigned	Default	always
RFID00006	Not assigned	Default	always
RFID00007	Not assigned	Default	always
RFID00008	Not assigned	Default	always

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.

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 often 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 base 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.



Edit NAC Policy

Name: android
Status: Enabled | Disabled
FortiSwitches: All | Specify
Description: 0/63

Device Patterns

Category: Device | User | EMS Tag
MAC address: 11:22:33:44:55:66
Hardware vendor
Device family
Type
Operating system: Android
User

Switch Controller Action

Assign VLAN
Bounce port
Assign device to dynamic address

Wireless Controller Action

Assign VLAN: NAC-android

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 campus 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

Fortinet Campus Wi-Fi Design Conclusion

The Fortinet Campus Wireless LAN architecture is highly adaptable. It scales both up and down from a dozen Access Points to thousands of Access Points. It is architected to easily overlay an existing campus wired network from any vendor, or to serve in a completely new network deployment. Following these guidelines, it can even be rolled out gradually, as an area-by-area upgrade to an existing campus WLAN. All while simultaneously truly integrating network security.

Fortinet's *Security Driven Networking* ensures no area of the Campus WLAN is overlooked or unsecured. Every SSID created in the FortiOS 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 singe-pane-of-glass, the Campus Network administrator's job is simplified. Campus complexity comes as much from the variety of end users and client devices as from the large coverage areas. The Campus architecture is designed to accommodate as much, or as little, differentiation of user classes as needed while without having to make any changes to the 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

- 7.0 FortiWiFi and FortiAP Configuration Guide

Solution Hub

- Secure Access Solution Hub

Related 4-D Documentation

- Secure Wireless Concept Guide

www.fortinet.com

20-700-772114-20230705