DEFINE • **DESIGN** • DEPLOY

FortiLAN Cloud

Wireless LAN Design

Version 1.0.0

July 21, 2023
FortiLAN Cloud 1.0.0 Wireless LAN Design
66-100-836393-20230721

TABLE OF CONTENTS

Change Log

Version	Change	Date
1.0.0	Release draft	2022-10-12
	Modified the document format.	2022-10-27
	Corrected a spell error.	2023-04-20
	Format changes	2023-07-21

Introduction

This document is intended to provide an architectural overview for both single location and distributed enterprises using Fortinet Wi-Fi gear managed via the FortiLAN Cloud portal.

Executive Summary

FortiLAN Cloud is a unified management platform for standalone FortiAP and FortiSwitch deployments. FortiLAN Cloud provides configuration management and monitoring control from a handful of devices an scaling up to thousands of devices across multiple sites. FortiLAN Cloud offers a simple, intuitive, easy-to-use interface for managing your LAN that is available from anywhere at any time.

To ensure there is no confusion, FortiLAN Cloud is typically for sites that do NOT use a FortiGate. A FortiGate includes a Wifi & Switch Controller that manages local FortiSwitches and FortiAPs, and the FortiGate can be cloud-managed via the FortiGate Cloud portal. FortiLAN Cloud is specifically for FortiSwtiches and FortiAPs that are not under FortiGate management, thus the are typically referred to as stand alone. The following are the strengths of FortiLAN Cloud.

Zero Touch Deployment

Initial configuration of network equipment can be a difficult proposition, often requiring expert staff on site to configure each device individually. FortiLAN Cloud with FortiZTP greatly simplifies initial configuration and onboarding by providing one-touch provisioning when devices are deployed.

Highly Scalable

Cloud-based model can manage deployments from single digits up to multiple thousands of devices, and can easily grow with your deployment along the way.

Multi-Tenancy

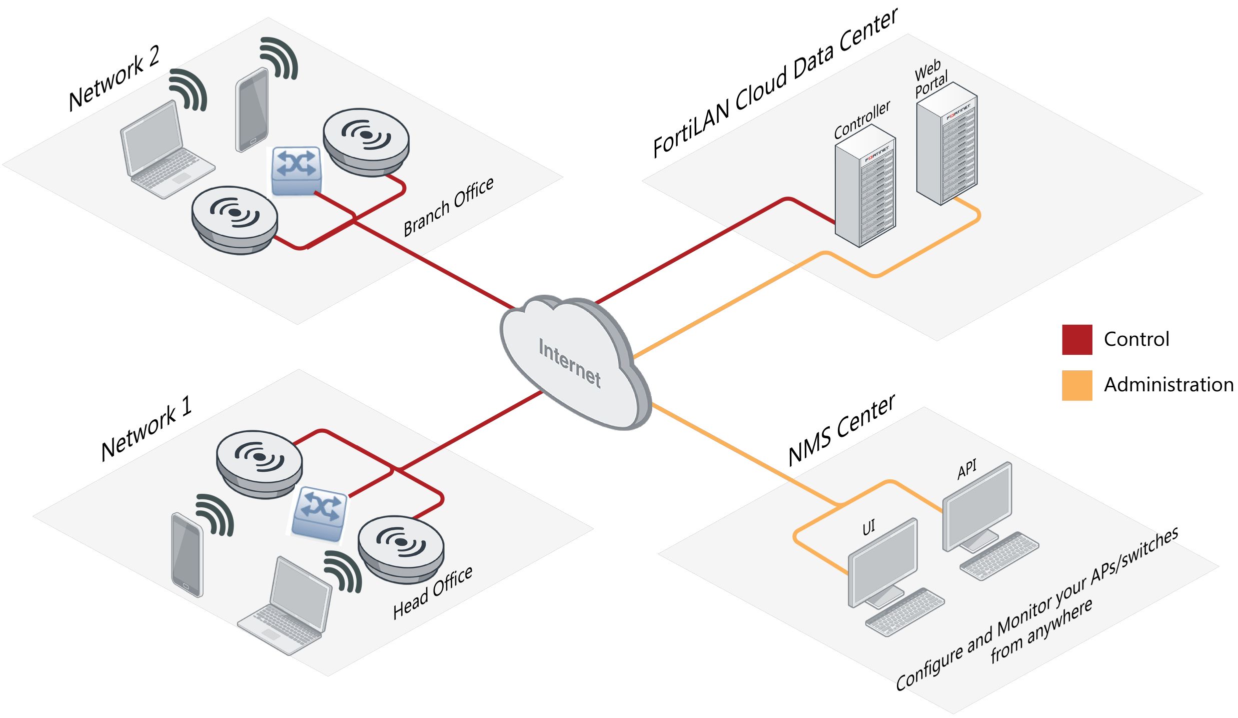
Maintain multi-tenancy for many customers within a single license. Simple Central visibility and access across all tenants. Enable Read-Only customer accounts with unique customer logos on reports.

Free and Licensed Tiers

FortiLAN Cloud has a free tier, allowing management of up to 30 FortiAPs, 3 FortiSwitches, 3 sites and 7 days of log storage. Licensed tiers scale with number of sites, hold one year of logs, and introduce advanced wireless and switch features, such as spectrum analysis, advanced roaming, Wireless Intrusion Detection, Airtime Fairness and more.

The FortiLAN Cloud WLAN Architecture Outline

This example depicts a FortiLAN Cloud architecture with branch offices.



- FortiLAN Cloud Portal and FortiCare account (all sites)
- Internet access for each site
- Ethernet switch network with PoE access switch ports for FortiAPs
- SSIDs for classes of users
- Authorized users
- Guest users
- IoT devices

Intended Audience

This guide is intended for an audience which is interested in learning about FortiLAN 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 Fortinet Standalone Wireless infrastructure. This guide explores further the design of a Wireless LAN for a branch or small campus network managed via the FortiLAN Cloud service portal for one or multiple locations. Learn about the role of the FortiLAN Cloud Portal, 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.

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

Solution and Technologies

Fortinet is possibly the world’s premier network and cyber security business. This section describes the following.

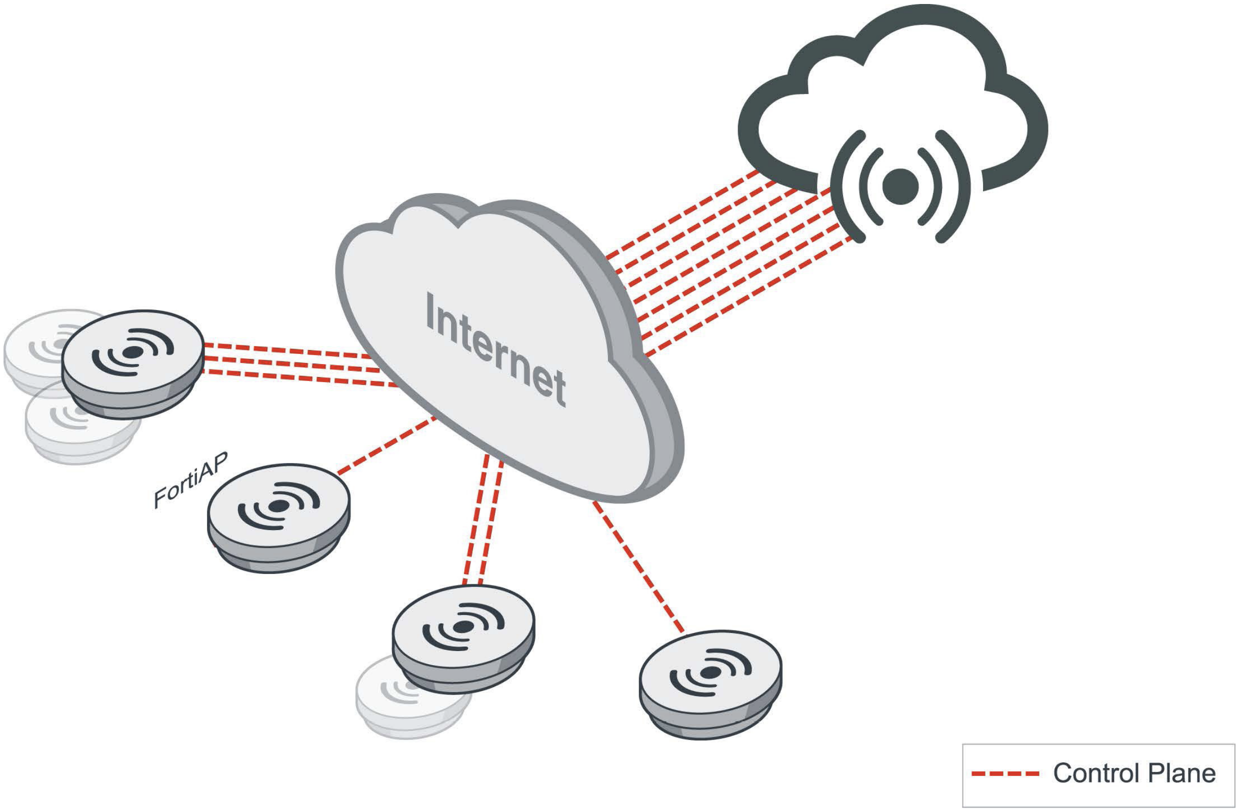
- Fortinet LAN Edge
- FortiLAN Cloud Network Management
- FortiLAN Cloud WLAN Key Features
- The Fortinet Branch WLAN Architecture

Fortinet LAN Edge

A lesser-known portion of Fortinet’s business is our pure networking portfolio, the LAN Edge product line of wireless and wired access device. Consisting of multiple models of wireless access FortiAPs and wired access FortiSwtiches, the LAN Edge product line comprises outstanding high performance network equipment for campus and branch deployments for enterprises of all sizes and profiles.

Networking needs of customers can vary a tremendously, not only from customer to customer, but from year to year for the same customer, depending on business cycle, technology cycle, growth, etc. In order to support our customers whatever their needs, Fortinet LAN Edge products can operate in Security Fabric mode or in Stand-Alone mode.

A Security Fabric centers around a FortiGate, and any FortiAPs and FortiSwtiches that are part of that fabric become extensions of the FortiGate, and are managed by that FortiGate as a unified whole. When no FortiGate is part of the LAN architecture, there is a need for an alternative management paradigm that can scale from one to 1000s of sites – enter FortiLAN Cloud. This image depicts a FortiLAN Cloud solution managing standalone FortiAPs.

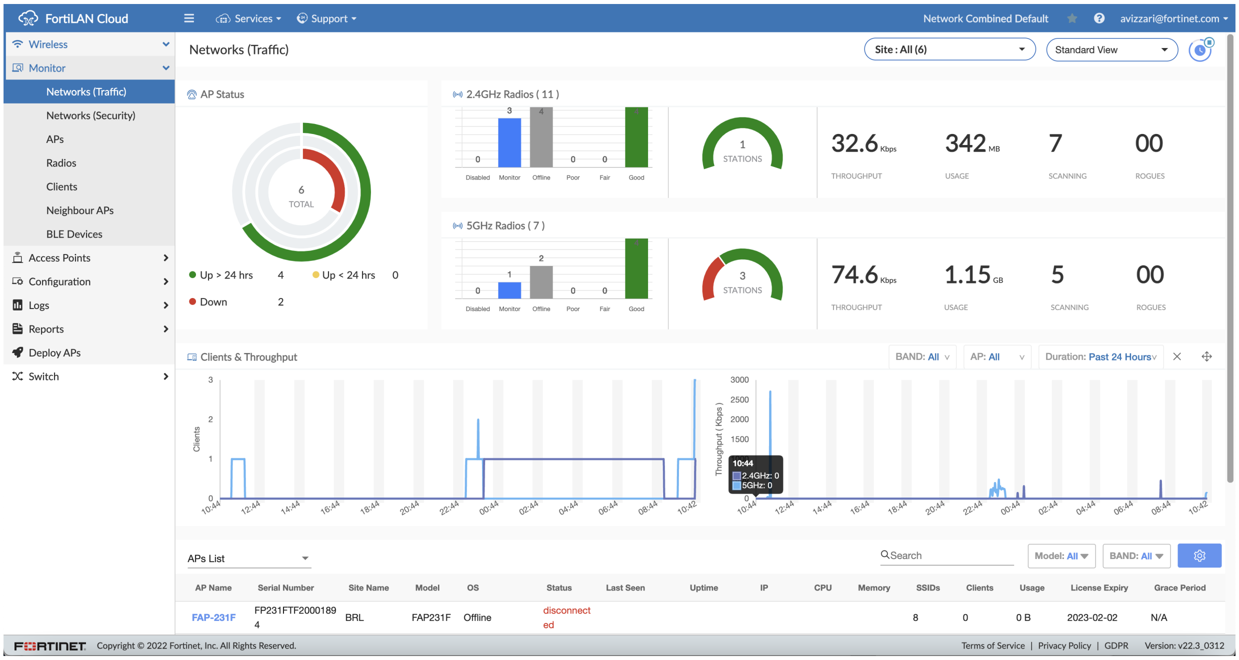


FortiLAN Cloud Network Management

Cloud management systems of Local Area Networks are here to stay. With so many enterprises geographically distributed and Internet access so reliable, it just makes sense for so many operations of any size. A hosted service in a reliable data center that is already setup to handle your network administrative needs is more and more often the best solution for many networking needs, especially smaller and more distributed operations.

FortiLAN Cloud is a hosted cloud-based management platform for Fortinet’s LAN Edge portfolio (FortiSwitch and FortiAP), offering zero touch deployment, configuration management, reporting and analytics for standalone deployments. FortiLAN Cloud offers a simple, intuitive, easy-to-use interface for managing your LAN that is available from anywhere at any time. FortiLAN Cloud can scale from a small handful of devices all the way up to thousands across multiple sites.

FortiLAN Cloud centralizes the life-cycle management of your standalone FortiAP deployment with a simple, intuitive, and easy-to-use cloud interface that is accessible from anywhere at any time. With FortiLAN Cloud, you can deploy, configure, and manage your FortiAP devices. FortiLAN Cloud also offers enhanced visibility, monitoring, reporting, and analytics features for your FortiAP devices. FortiLAN Cloud supports the FortiAP-U series which include Universal Threat Protection (UTP) security at the network edge.



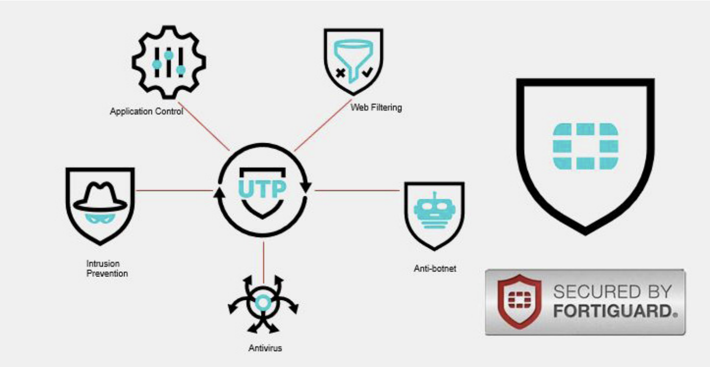
AP Name	Serial Number	Site Name	Model	OS	Status	Last Seen	Uptime	IP	CPU	Memory	SSIDs	Clients	Usage	License Expiry	Grace Period
FAP-231F	FP231FTF20001894	BRL	FAP231F	Offline	disconnected						8	0	0 B	2023-02-02	N/A

FortiLAN Cloud WLAN Key Features

Dashboards for Ease of Management and Provisioning — FortiAP and FortiSwitch network settings are configured through an easy-to-understand browser-based user interface. Multiple monitor dashboards offer a view of key statistics for all managed switches, ports, APs, radios, clients, and neighboring networks in your environment. Click to drill down on a particular item to see details on specific devices in a category. There is no need to change screens or hunt through the UI to find information.

- FortiLAN Cloud Licensing Tiers
  - Free Tier – Management of up to 30 FortiAPs, 3 FortiSwitches, 3 sites and 7 days of log storage.
  - Licensed Tiers - Scale with number of sites, hold one year of logs, and introduce advanced wireless and switch feature
- 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 the following.
  - Integrated Bluetooth
  - support for presence analytics,
  - Band (radio) balancing,
  - AP Balancing
  - UTM series FortiAPs support dual 5 GHz settings for advanced channel plans
- Robust Monitoring and Remote Troubleshooting - FortiLAN Cloud provides a host of self-healing capabilities to lessen the day-to-day management requirements for your wired and wireless network. When issues do arise a full suite of troubleshooting tools are provided.
  - Spectrum Analysis gives visibility into the RF at your locations
  - Use the included iPerf tool to test wired or wireless throughput
  - Test VLAN availability with the VLAN Probe.
  - Multiple views including Topology, Port level, and Status monitoring

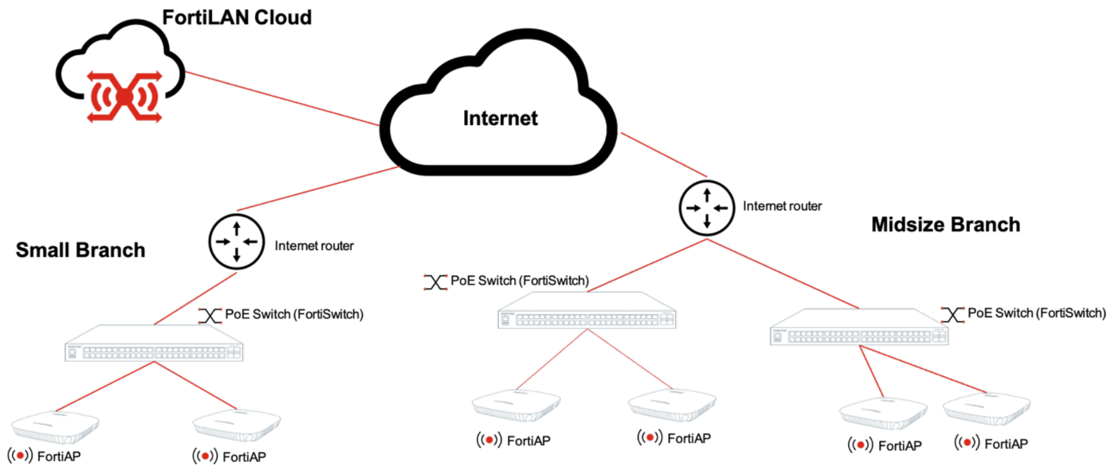
- Automated Channel and power selection - DARRP (Distributed Automatic Radio Resource Provisioning) technology optimizes channel selection and AP Tx power. FortiAPs continuously monitor the RF environment for interference, noise, and signals from neighboring APs, in order to optimize the WLAN.
- Support for the following most advanced Wi-Fi standards.
  - Fast, seemless roaming – 802.11r
  - Enterprise Voice – 802.11k and 802.11v
  - Protected Management Frames
  - Broadcast suppression
  - Bonjour Relay
  - Airtime Fairness
  - Customer MCS Rate Setting
- Two-factor Authentication - Supports FortiToken for two-factor authentication of user login.
- International Privacy Compliance - Isolated instances for Europe, Americas, and Asia to meet local privacy laws.
- Integrated Guest Access Management – 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.
- Security at the Edge - When used with the Fortinet UTP access points (FortiAP-U models) FortiLAN Cloud have the flexibility to enable security services wherever needed in the network.



- Zero-touch provisioning using FortiDeploy – Bring new branches up and running as soon as they are plugged in. No need to fly in.
- Multi-tenancy support – The available multi-tenant option enables full data isolation over multiple sub-accounts. It is favored by MSSPs servicing multiple customers, but also used by large highly distributed single enterprises for administrative division.

The Fortinet Branch WLAN Architecture

This image depicts the FortiLAN Cloud architecture with two branch offices and lists the architectural highlights.



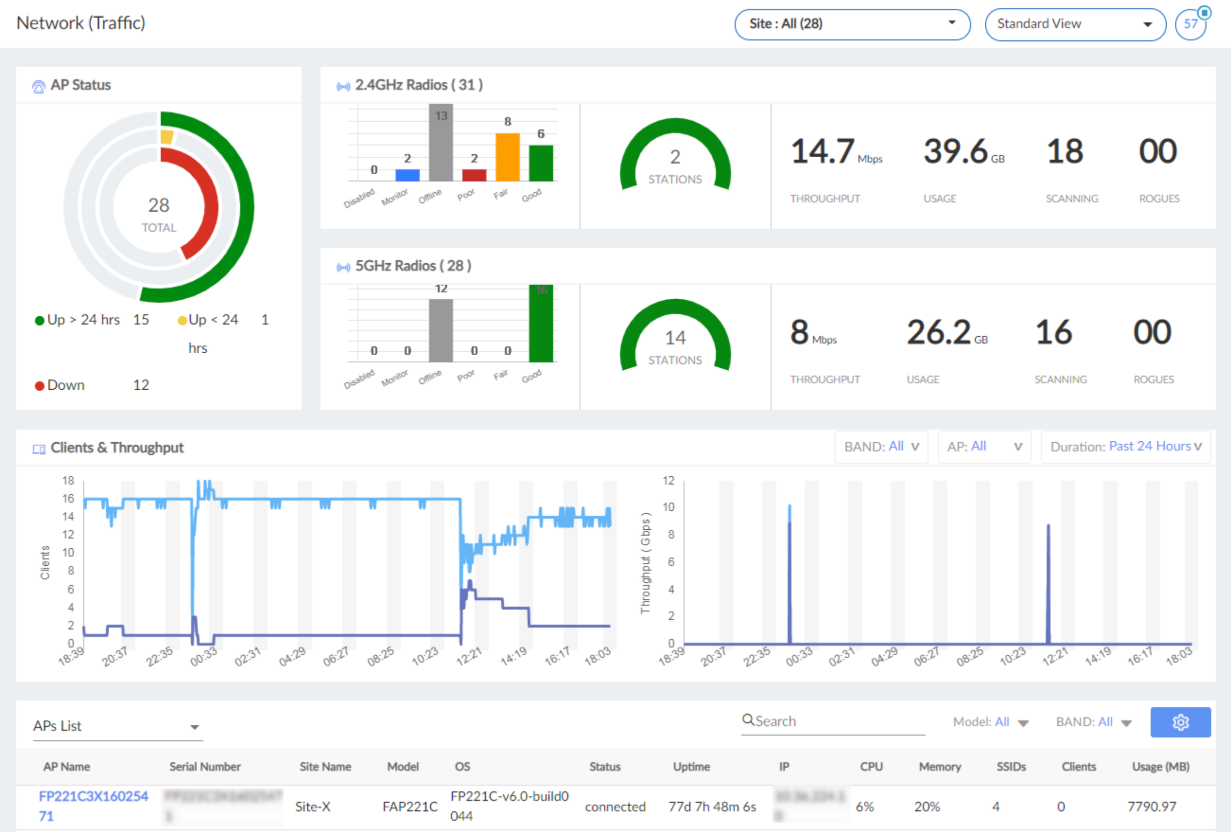
- FortiLAN Cloud Management Portal (all sites)
- Internet access – at each site
- Switch network
- Recommended PoE access switch ports for FortiAPs
- A very small site may have FortiAP directly into dual purpose router/switch
- FortiAP Registration and Deployment to FortiLAN Cloud
- Define networks (for each site)
- SSIDs for network- typically 3 types
- Authorized users – WPA2/3 Enterprise
- Guest users – likely Captive portal authentication
- ‘Headless’ devices – WPA2/3 Pre-shared key (or SAE)

Design Overview

FortiLAN Cloud centralizes the life-cycle management of your standalone FortiAP deployment with a simple, intuitive, and easy-to-use cloud interface that is accessible from anywhere at any time. With FortiLAN Cloud, you can deploy, configure, and manage your FortiAP devices. FortiLAN Cloud also offers enhanced visibility, monitoring, reporting, and analytics features for your FortiAP devices. FortiLAN Cloud also supports the FortiAP-S and FortiAP-U series which combine the elements of universal threat protection (UTP) protection at the network edge.

FortiLAN Cloud can manage FortiAPs and their WLANs (SSIDs) across multiple sites over the Internet. So long as the FortiAPs can access the Internet, they can receive their configurations, get updates and send logs to the FortiLAN Cloud portal. FortiLAN Cloud is appropriate for networks of a single site with a single FortiAP to highly distributed organizations national organizations with 100s of sites or more.

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



AP Name	Serial Number	Site Name	Model	OS	Status	Uptime	IP	CPU	Memory	SSIDs	Clients	Usage (MB)
FP221C3X16025471	[redacted]	Site-X	FAP221C	FP221C-v6.0-build0044	connected	77d 7h 48m 6s	[redacted]	6%	20%	4	0	7790.97

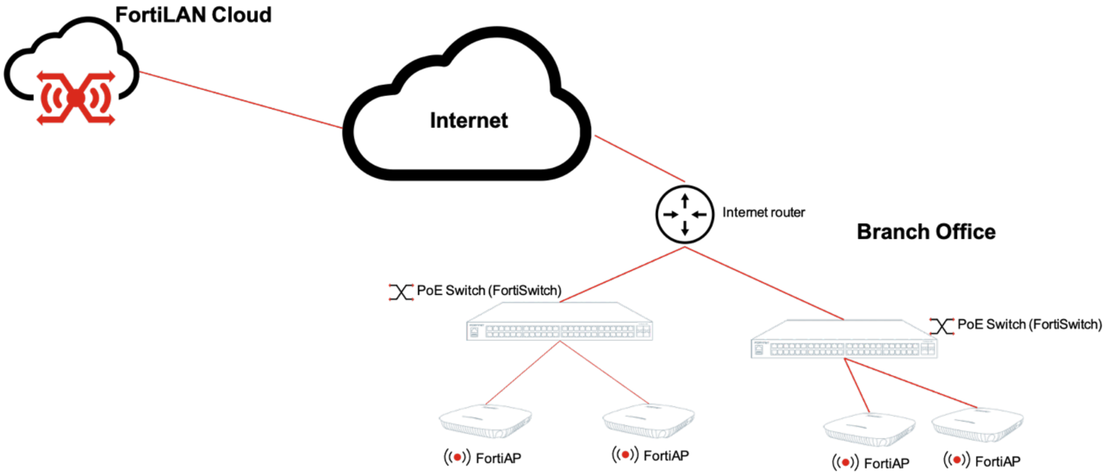
This section describes the following topics.

- FortiLAN Cloud and FortiAP Communication
- FortiAPs and Electrical Power
- FortiAP Placement Guidelines and Channel Planning
- FortiCloud Accounts and Services

- Define Networks and Deploy FortiAPs
- SSID Configuration
- Guest User Management
- Ownerless devices – PSK + MPSK
- FortiLAN Cloud Wi-Fi Design Conclusion

FortiLAN Cloud and FortiAP Communication

FortiAPs communicate with FortiLAN Cloud for management or control plane traffic. Client Traffic from devices using the WLAN/SSID is sometimes called data plane traffic. Wireless client traffic is locally bridged/switched from the FortiAP and is not tunneled or otherwise sent to FortiLAN Cloud. That is, FortiAPs that are managed via FortiLAN Cloud are layer 2 networking devices similar to switches. FortiAP control plane traffic is similarly locally bridged/switched, but the destination is the FortiLAN Cloud service. The FortiAPs initiate the connection, so there is no need to allow incoming traffic; The FortiAPs *dial home* pretty much like any client device accessing the Internet.



Many sites have an Internet access policy that allows any internally initiated traffic. For sites that need to be more locked down, the following protocols must be allowed.

Purpose	Protocol	Port
Customer UI and API access	HTTPS	TCP/443
FortiAP initial discovery	HTTPS	TCP/443
FortiAP CAPWAP (Configuration, event logs, statistics)	CAPWAP	UDP/5246 UDP/5247
FortiAP UTP logs		TCP/514
FortiAP firmware download	HTTPS	TCP/443
FortiGuard Services		UDP/53 UDP/8888

Purpose	Protocol	Port
FortiAP to FortiPresence		UDP/4013
FortiSwitch		TCP/443 TCP/8443

FortiAPs and Electrical Power

Power over Ethernet (PoE) switches should be used to power the FortiAPs for maximum flexibility of FortiAP placement, although power injectors or AC power supplies can certainly be used. With PoE switch ports, both network connectivity and power are delivered over the same Ethernet cable, up to 100 meters of cable from the switch port. This is much simpler and more flexible than cabling power separately.

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, and the larger the site, the more likely multiple switches will come into play. Any switch that FortiAPs will directly connect to should be checked for both 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 upgrading to new switches or adding single port or multi-port (midspan) power injectors. AC power supplies do not come with FortiAPs by default but can be ordered from Fortinet. Nevertheless, power over Ethernet is so much more convenient it is highly recommended.

As a rule of thumb, 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, see 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 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 new FortiAPs. That tendency should be resisted, because environments really do change, and AP capabilities also change with Wi-Fi generations. Environmental changes can come from surprising places. We have seen countless Wi-Fi networks that performed worse over time not because of any change to the network, but because of poorly designed neighbor WLANs moved in and interfered with the original network. Sort of like new housing putting more cars on the road and ruining your once pleasant commute.

There are other factors that might affect an originally well-planned WLAN. With the 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 mucks 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, but interference will be less on the higher channels as few other devices use them.

On the other hand, rather than a full site survey, a walk-through examination of the site with a spot-check of representative areas may be a reasonable risk on a refresh. New sites always warrant getting a clear idea of wall properties and corresponding dB loss. Glass walls in an 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
- Channel Planning – Design for 5 GHz
- FortiAP Profiles
- Designing for High Density Environments

Capacity and Coverage Estimations

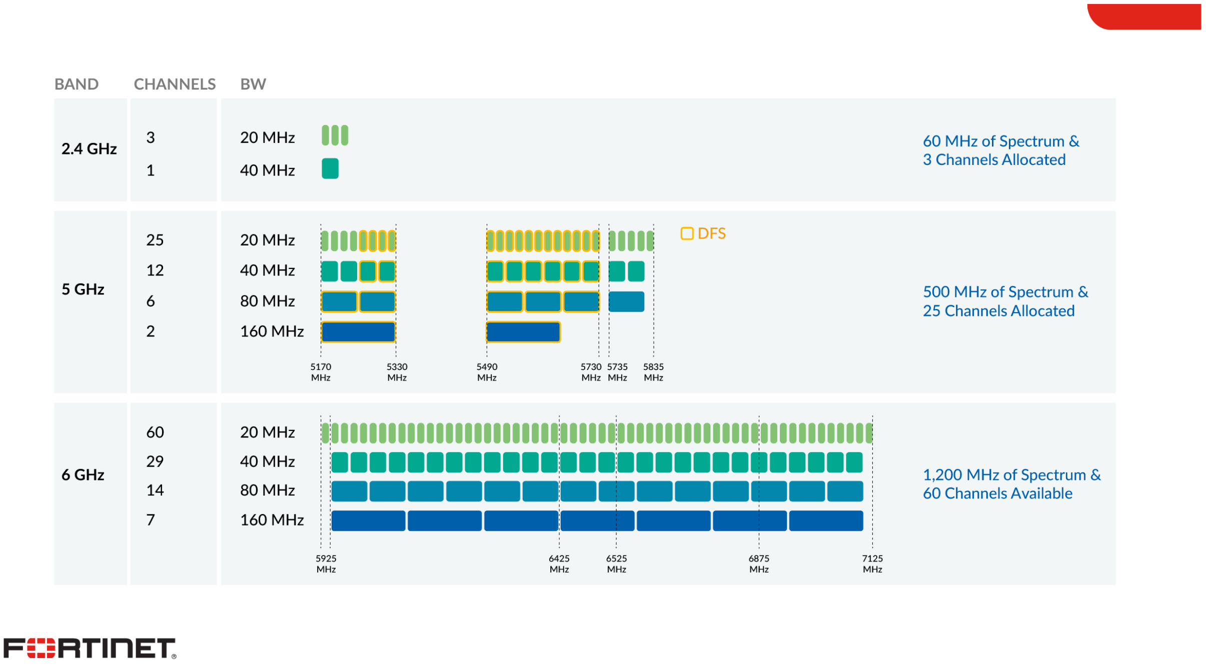
As a rule of thumb, for a pre-survey estimate, an indoor area probably requires about 1 FortiAP per 2000 Sq-Ft, with around 30 devices per AP radio. All the Wi-Fi 6 FortiAPs have 1 radio for monitoring and 2 service radios, so 60 devices typically. Users are usually assumed to have 3 devices each, so 20 users and 60 devices can be serviced per physical AP. UTP series FortiAPs can have both radios on 5 GHz, and there are enough channels in 5GHz to 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; that is, capacity more than coverage is generally the design driver these days. Designing for capacity rather than coverage is helped by designing for 5 GHz bands.

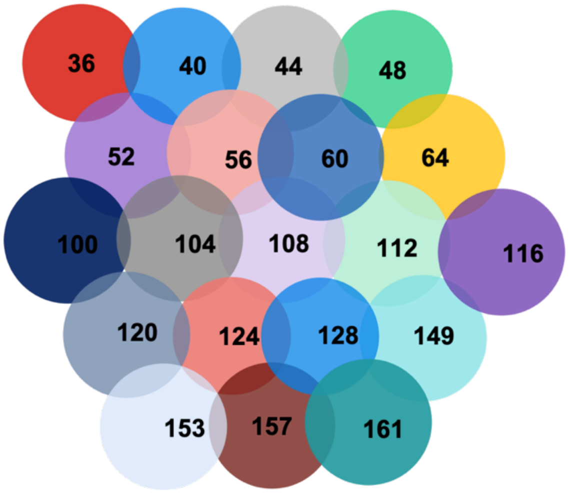
It is best to avoid requiring client-to-FortiAP radio connections to pass through more than one wall. Although one cannot see Wi-Fi signals, line of site connectivity to client devices is best, so a designer can visualize coverage by thinking about how they would deploy light fixtures. Placing APs in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

Channel Planning – Design for 5 GHz

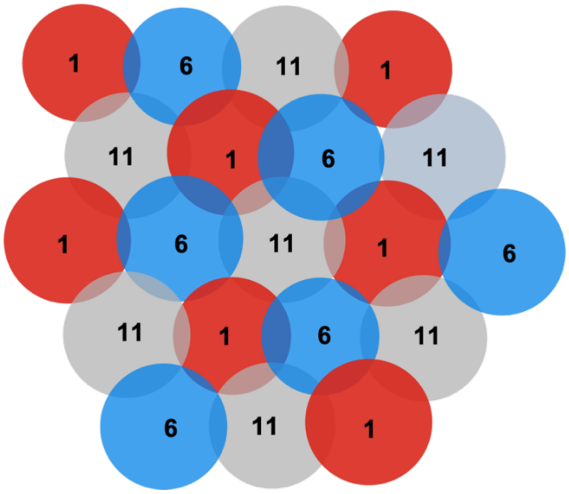
Wi-Fi in general has evolved quite a bit in a relatively short time, and so have other wireless technologies such as Bluetooth and its variations. The default assumption for Wi-Fi in the past was to design for 2.4 GHz and treat 5 GHz as secondary. Now that we are at Wi-Fi 6, Fortinet recommends designing 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 an ever-increasing number of Bluetooth devices. The following is a 5GHz channel plan (20MHz wide), no self-interference.



The following is a 2.4 GHz channel plan, much potential self-interference.

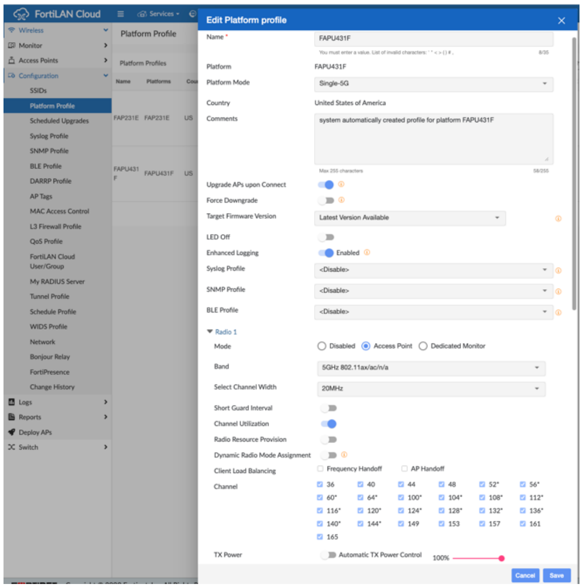


Very few client devices are so old or so “inexpensive” that they do not fully support 5 GHz. In addition, DFS (Dynamic Frequency Selection) regulations apply to the APs, not the clients. A good reference for client 5 GHz support can be found here: http://clients.mikealbano.com/

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 is to alternate the selectable radio between 5 GHz and 2.4 GHz 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

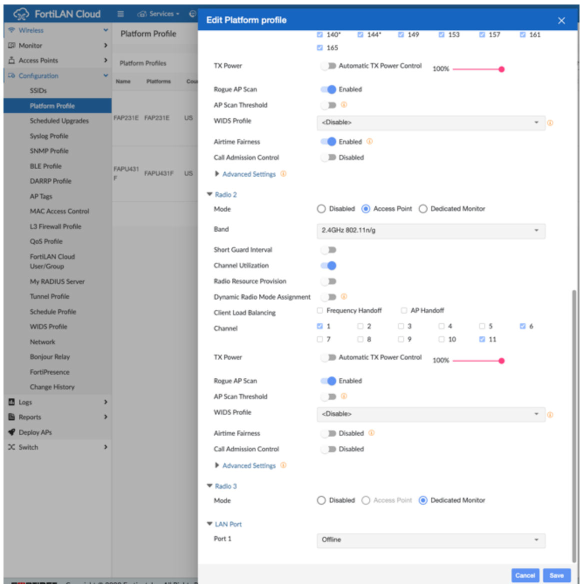


Name	Platforms	Cou
FAP231E	FAP231E	US
FAPU431F	FAPU431F	US

Edit Platform profile

Name *: FAPU431F
You must enter a value. List of invalid characters: ' " < > ( ) # . 8/35
Platform: FAPU431F
Platform Mode: Single-5G
Country: United States of America
Comments: system automatically created profile for platform FAPU431F
Max 255 characters 58/255
Upgrade APs upon Connect: on
Force Downgrade: off
Target Firmware Version: Latest Version Available
LED Off: off
Enhanced Logging: Enabled
Syslog Profile: <Disable>
SNMP Profile: <Disable>
BLE Profile: <Disable>

Radio 1
Mode: ○ Disabled ● Access Point ○ Dedicated Monitor
Band: 5GHz 802.11ax/ac/n/a
Select Channel Width: 20MHz
Short Guard Interval: off
Channel Utilization: on
Radio Resource Provision: off
Dynamic Radio Mode Assignment: off
Client Load Balancing: □ Frequency Handoff □ AP Handoff
Channel:
☑ 36 ☑ 40 ☑ 44 ☑ 48 ☑ 52* ☑ 56*
☑ 60* ☑ 64* ☑ 100* ☑ 104* ☑ 108* ☑ 112*
☑ 116* ☑ 120* ☑ 124* ☑ 128* ☑ 132* ☑ 136*
☑ 140* ☑ 144* ☑ 149 ☑ 153 ☑ 157 ☑ 161
☑ 165
TX Power: Automatic TX Power Control off 100%



Name	Platforms	
FAP231E	FAP231E	US
FAPU431F	FAPU431F	US

Edit Platform profile

☑ 140* ☑ 144* ☑ 149 ☑ 153 ☑ 157 ☑ 161
☑ 165

TX Power: Automatic TX Power Control 100%
Rogue AP Scan: Enabled
AP Scan Threshold
WIDS Profile: <Disable>
Airtime Fairness: Enabled
Call Admission Control: Disabled
Advanced Settings

Radio 2
Mode: ○ Disabled ● Access Point ○ Dedicated Monitor
Band: 2.4GHz 802.11n/g
Short Guard Interval
Channel Utilization
Radio Resource Provision
Dynamic Radio Mode Assignment
Client Load Balancing: □ Frequency Handoff □ AP Handoff
Channel: ☑ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6
□ 7 □ 8 □ 9 □ 10 ☑ 11
TX Power: Automatic TX Power Control 100%
Rogue AP Scan: Enabled
AP Scan Threshold
WIDS Profile: <Disable>
Airtime Fairness: Disabled
Call Admission Control: Disabled
Advanced Settings

Radio 3
Mode: ○ Disabled ○ Access Point ● Dedicated Monitor

LAN Port
Port 1: Offline

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. But 5 GHz can potentially have 600 devices when using 20 MHz wide channels with no FortiAPs needing to contend with each other - which is exactly the 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

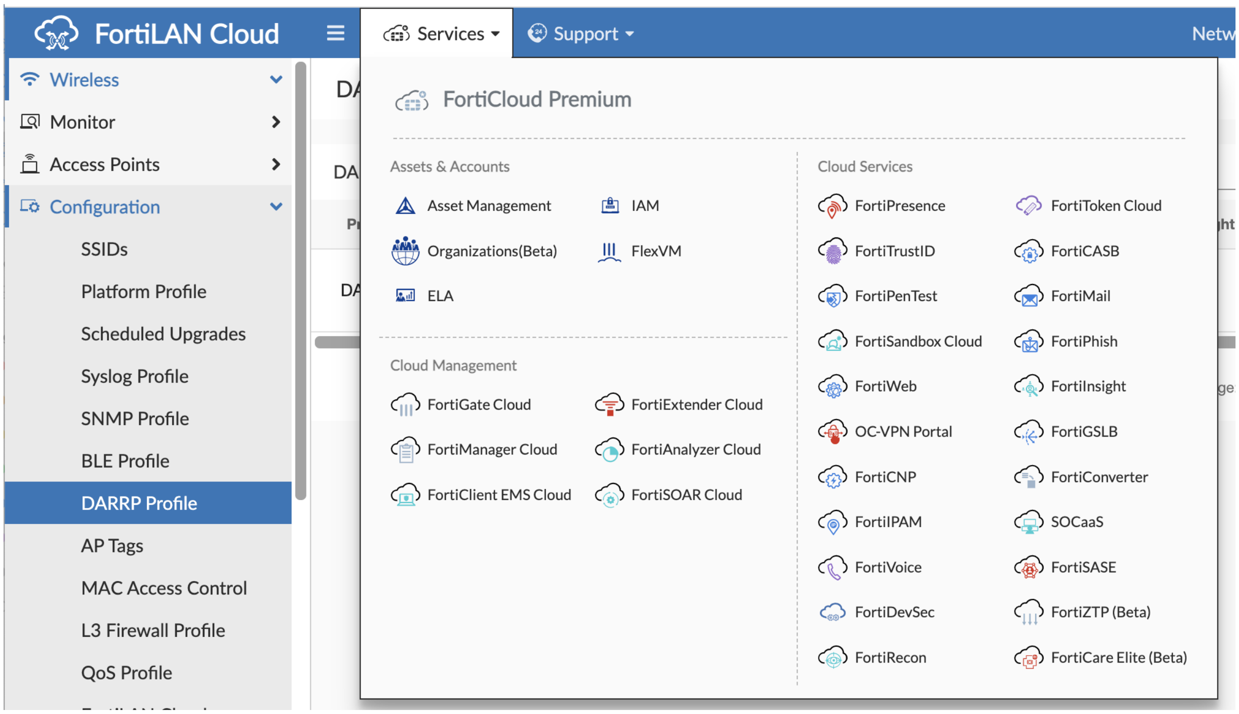
This high throughput enterprise class 802.11ax indoor AP provides three radios and 8 spatial streams. This top-of-the line access point supports OFDMA, a 5.0 Gigabit Ethernet port, plus an additional 1 Gbps Ethernet port for PoE diversity. The AP can provide 24/7 scanning across both bands while still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

FortiCloud Accounts and Services

FortiCloud is an umbrella for multiple Fortinet Cloud services; FortiLAN cloud is only part of the FortiCloud suite. The FortiCloud Portal unifies all of Fortinet's Cloud offerings and support under one FortiCare Account. Prior to using FortiLAN Cloud, you are required to register on the FortiCloud portal. Use the https://support.fortinet.com access link to register on the FortiCloud portal. A security code is emailed to the address specified during registration; use the code to complete registration and activate your account.

If multiple users will have access to the FortiLAN Cloud portal, then Identity and Access Management (IAM) is a service to help you control access to FortiCloud portals and assets. You can use the IAM portal to manage users, authentication credentials, and asset permissions. For more information, see FortiCloud documentation. Access the IAM service from the FortiCloud portal using the master FortiLAN Cloud account.

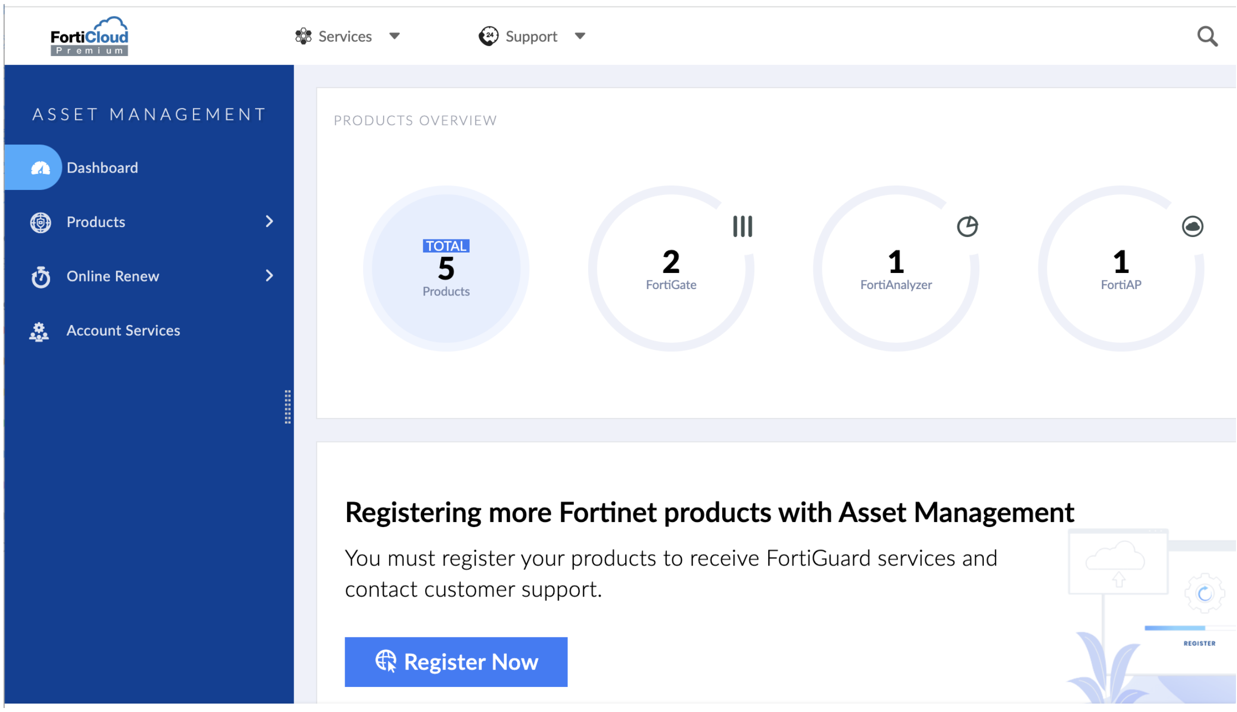
The suite of FortiCloud portals and services can be access from the **Services** drop down menu available from all FortiCloud Screens. Complete documentation of all available services including the Asset & Accounts can be found at https://docs.fortinet.com/forticloud-landing



- Adding FortiAPs and Licenses in Asset Management
- Multi-Tenancy Account

Adding FortiAPs and Licenses in Asset Management

Both devices (FortiAPs) and licenses must be registered in the Asset Management portal. The **Register Now** button will launch a registration wizard. The wizard steps will vary slightly depending on the type of product.



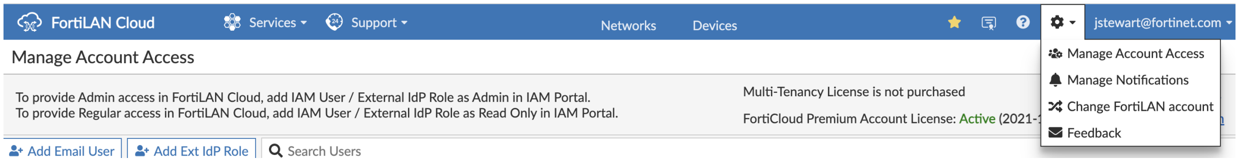
Registering more Fortinet products with Asset Management

You must register your products to receive FortiGuard services and contact customer support.

Once your devices and licenses are registered in Asset Management, you can go directly to FortiLAN Cloud via https://fortilan-login.forticloud.com/samlsplash, or you can use the services menu from FortiCloud at https://support.fortinet.com/welcome/#/. The services menu is available from all FortiCloud portals.

Multi-Tenancy Account

The multi-tenancy account is designed for Managed Security Service Providers (MSSPs). A multi-tenancy account allows an organization to create and manage multiple sub-accounts. Devices can be added and moved between these sub-accounts, while each account can have its own administrators and users, allowing more control over a managed service's provisioning. The multi-Tenancy license can be installed undere the Managed Account access, available under the upper left account services menu in FortiLAN cloud.



Manage Account Access

To provide Admin access in FortiLAN Cloud, add IAM User / External IdP Role as Admin in IAM Portal.
To provide Regular access in FortiLAN Cloud, add IAM User / External IdP Role as Read Only in IAM Portal.

Multi-Tenancy License is not purchased

FortiCloud Premium Account License: Active (2021-1

Define Networks and Deploy FortiAPs

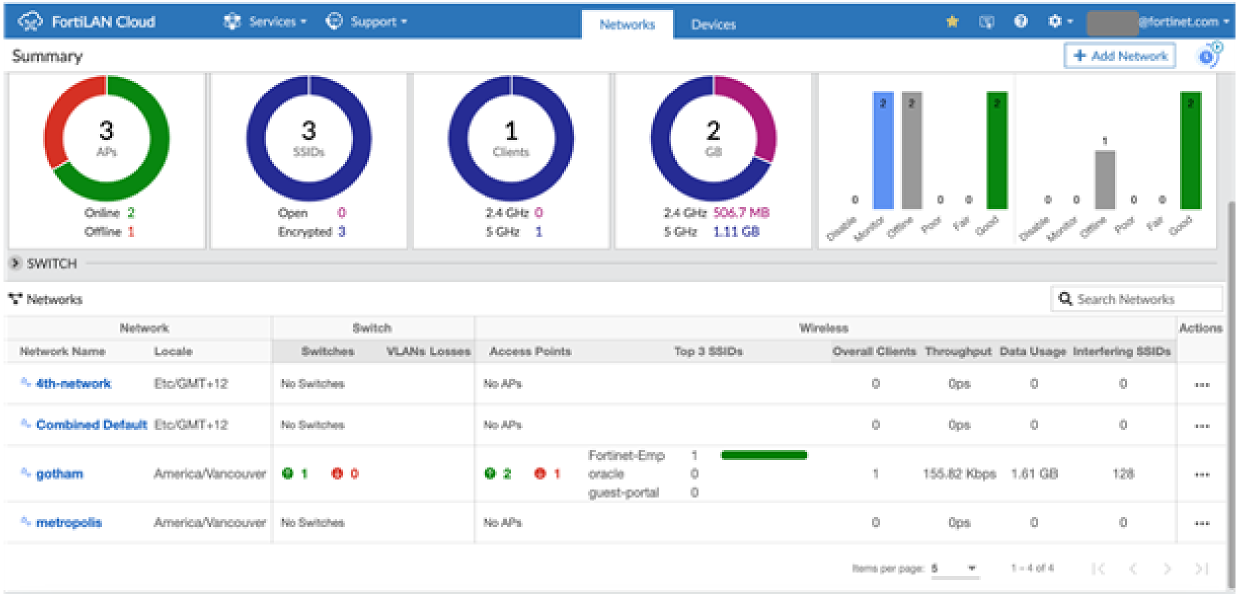
This section describes the following topics.

- FortiLAN Cloud Networks
- FortiLAN Cloud Key Import and FortiAP Deployment

FortiLAN Cloud Networks

In FortiLAN Cloud terms, a *Network* is a logical grouping of FortiAP and FortiSwitch devices for common configuration and management. A FortiLAN Cloud account can have multiple networks. For instance, if you have 20 devices and you plan to use 10 devices in the head office and the other 10 devices in a branch office, then you would create two networks.

Typically, a Network aligns with a site or location, but you can also group devices into subsets (sites) and then apply configurations to those subsets. For example, in an office building, you can have a device subset for each floor of the building. Though it is possible and valid to have a single network containing all devices, and apply configurations to subsets of devices, the recommendation is that you create multiple independent networks.



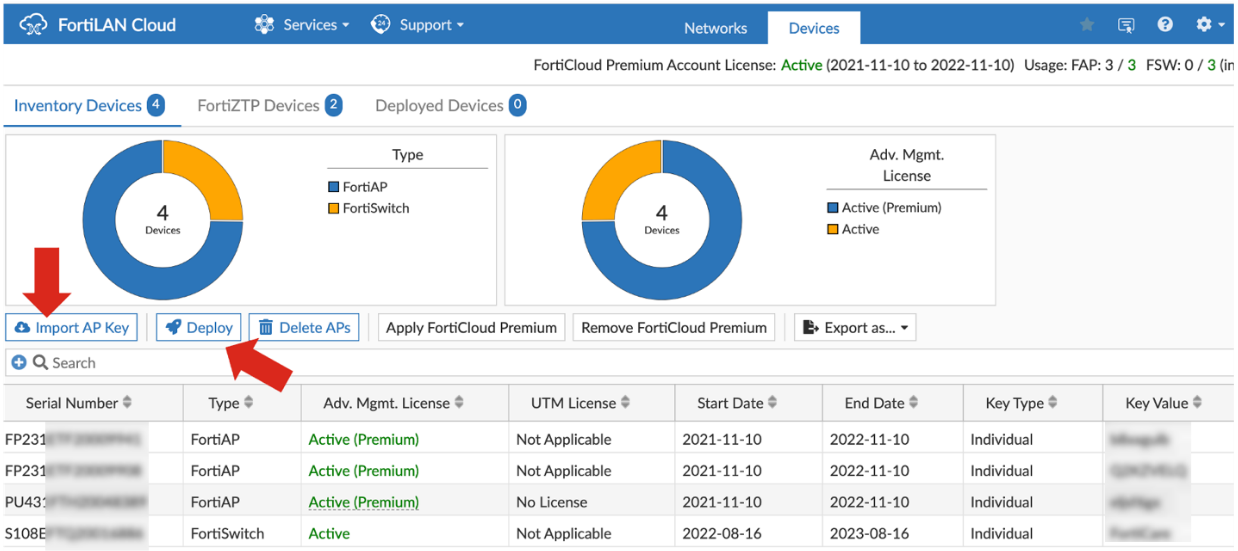
Network		Switch		Wireless						Actions
Network Name	Locale	Switches	VLANs Losses	Access Points	Top 3 SSIDs	Overall Clients	Throughput	Data Usage	Interfering SSIDs	
4th-network	Etc/GMT+12	No Switches		No APs		0	0ps	0	0	•••
Combined Default	Etc/GMT+12	No Switches		No APs		0	0ps	0	0	•••
gotham	America/Vancouver	● 1 ● 0		● 2 ● 1	Fortinet-Emp 1 oracle 0 guest-portal 0	1	155.82 Kbps	1.61 GB	128	•••
metropolis	America/Vancouver	No Switches		No APs		0	0ps	0	0	•••

Items per page: 5 1 - 4 of 4

FortiLAN Cloud Key Import and FortiAP Deployment

Because FortiAPs can be managed by a FortiGate or by FortiLAN Cloud, they have to be *informed* that they belong in the FortiLAN Cloud portal. Every FortiAP has a FortiLAN Cloud Key. For convenience, there is also the option to 'purchase' a no cost bulk key on a multiple FortiAP order. The individual cloud key can be found on the FortiAP, and the bulk key, if there is one, can be found on the purchase order.

Once the FortiAPs (and any FortiSwitches) are added to the device inventory via the cloud key(s), they can be deployed to the appropriate network.



FortiCloud Premium Account License: Active (2021-11-10 to 2022-11-10) Usage: FAP: 3 / 3 FSW: 0 / 3 (in

Serial Number	Type	Adv. Mgmt. License	UTM License	Start Date	End Date	Key Type	Key Value
FP231[redacted]	FortiAP	Active (Premium)	Not Applicable	2021-11-10	2022-11-10	Individual	[redacted]
FP231[redacted]	FortiAP	Active (Premium)	Not Applicable	2021-11-10	2022-11-10	Individual	[redacted]
PU431[redacted]	FortiAP	Active (Premium)	No License	2021-11-10	2022-11-10	Individual	[redacted]
S108E[redacted]	FortiSwitch	Active	Not Applicable	2022-08-16	2023-08-16	Individual	[redacted]

SSID Configuration

This section describes the following topics.

- Wi-Fi Security Modes
- WPAx Modes and Users and Device Classes
- Fully Authenticated Users using Enterprise Class WPA2 or WPA3.

Wi-Fi Security Modes

As part of the Wi-Fi standards, the two latest generations of Wi-Fi security, WPA2 and WPA3 are supported and recommended with any 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, in the future.

It is important to remember that Wi-Fi is an OSI Layer 2 technology, and Wi-Fi security is, in and of itself, concerned with over-the-air (OTA) encryption and authorization/authentication to network access. Encryption ends when the packet goes onto the Ethernet cable unless a higher layer protocol is involved, such as https or SSL.

With WPA2 and WPA3, there are 3 security modes, covering authentication and encryption.

- WPAx Enterprise class – using 802.1X/RADIUS, usually username/password based.
- Every device has a unique encryption key.
- Requires a database of users with a RADIUS front end.
- WPAx Personal – all users use the same Pre-Shared Key (PSK) for authentication and encryption

- Also called “SAE” in WPA3, which improves the encryption key generation
- Can be combined with a Captive Portal with the following.
  - WPAx Open – No security at the Wi-Fi level
  - Open networks are typically used in public access venues and often as a Captive Portal, where the user has to interact with an initial web page before being granted additional network access.
  - A Captive Portal can provide various levels of authentication, but no OTA encryption

WPAx Modes and Users and Device Classes

The way to think about when to use what version of WPAx Security is to consider there are 3 broad categories of Wi-Fi users in most organizations.

- Known and authenticated users
- Guest users
- Ownerless devices that do not support RADIUS

The known and authenticated users are members of your organization known to you who are granted a high degree of access to your network via your FortiAPs. Ideally, you have a database of such users, with individual passwords in order to take advantage of WPAx Enterprise. It is certainly possible to simply use a Pre-Shared Key, the answer to *what’s the Wi-Fi password?*, but there is a reason that is called *WPAx Personal*. It is essentially a single shared user account and only appropriate to a VERY small organization with limited security needs. The *password* will get shared inappropriately. Ben Franklin allegedly said *Three can keep a secret, if two of them are dead.* What if you do not have a DB of users? You can easily create a user group in FortiLAN Cloud that can fill that role!

Guest Users are temporary users of the network. There are a number of ways to handle guest users, depending on your organization’s needs, but the most common approach is to combine an Open SSID with a Captive Portal. The open SSID has no Over-The-Air encryption and any Wi-Fi device can access the network, but traffic is then blocked at a higher network layer. The Captive Portal is a web page served up to the user, who must interact with it in some way. The interaction could simply be a *click though* warning page as is common in public venues such as coffee shops, or it could require a temporary username/password issued by a Guest Admin.

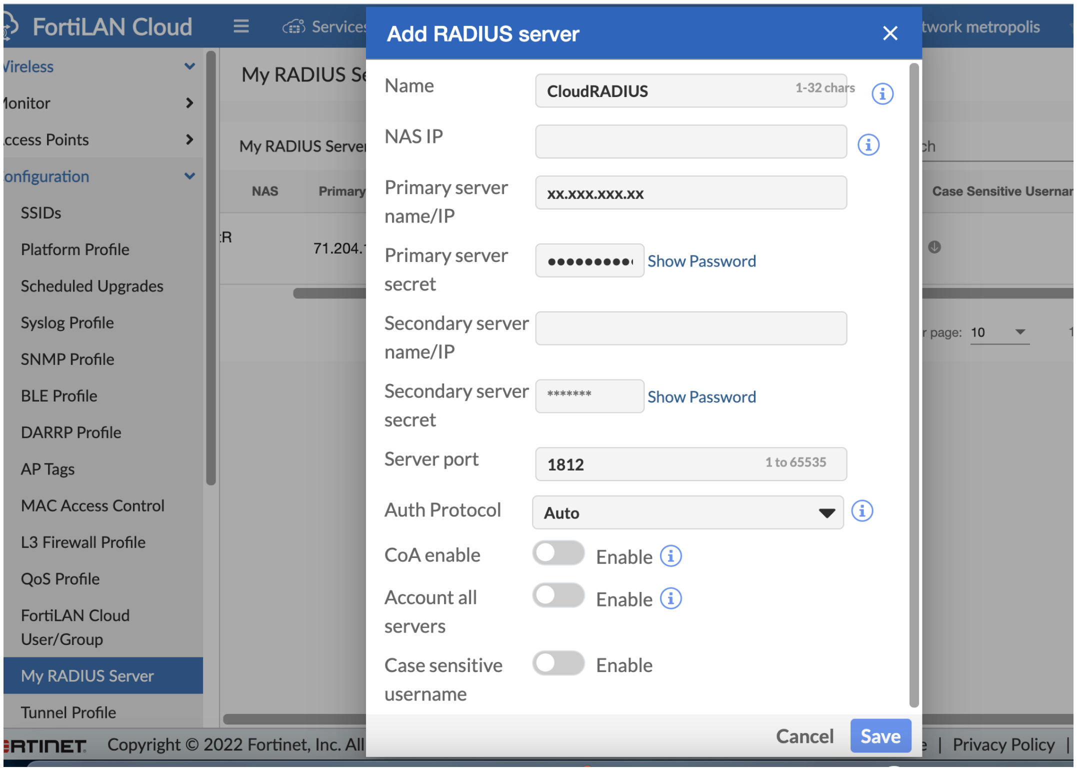
Ownerless Devices are common with consumer grade devices such as streaming TV or Internet of Things (IoT) such as temperature of light sensors. Such devices almost never support a RADIUS username/password combo and usually support only PSK SSIDs. One great advantage of using FortiLAN Cloud is the option of using Multiple-PSK or MPSK. With MPSK, a unique key can be generated and locked to each device, or a group of devices.

Generally speaking, the above are the recommended uses of Wi-Fi security, but if it is right for your environment, variations are possible. Captive Portal can be combined with PSK. MPSK can be used for known users, etc. This is one of those subjects where the first answer to most questions is, *it depends*.

An 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 types of users can share a single SSID but use RADIUS attributes to assign them different VLANs. See below.

Fully Authenticated Users using Enterprise Class WPA2 or WPA3.

These are the network users that are fully part of the organization. There should be a database that they can be authenticated against via RADIUS. Active Directory is a common choice, but most user DBs have a RADIUS connection option. Cloud based services have also become increasingly common. FortilLAN Cloud itself can be the RADIUS server. In this case, all user and user groups can be defined in FortiLAN Cloud.



Add RADIUS server

Name: CloudRADIUS (1-32 chars)

NAS IP:

Primary server name/IP: xx.xxx.xxx.xx

Primary server secret: ●●●●●●●●●● Show Password

Secondary server name/IP:

Secondary server secret: ******* Show Password

Server port: 1812 (1 to 65535)

Auth Protocol: Auto

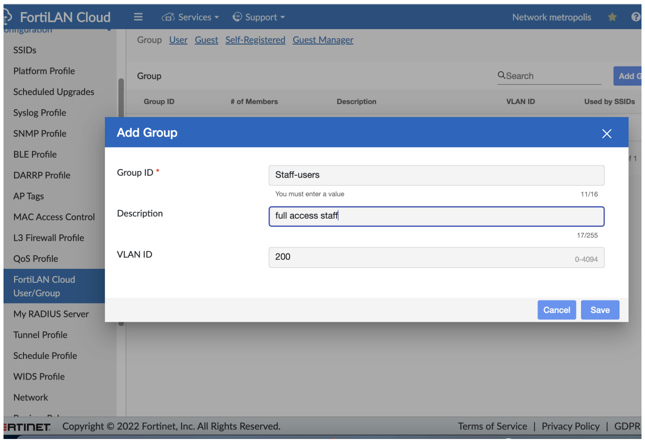
CoA enable: Enable

Account all servers: Enable

Case sensitive username: Enable

Cancel Save

Alternatively, you can use the FortiLAN Cloud as the RADIUS Server. If you do not already have a RADIUS database of users, this is a very convenient option.



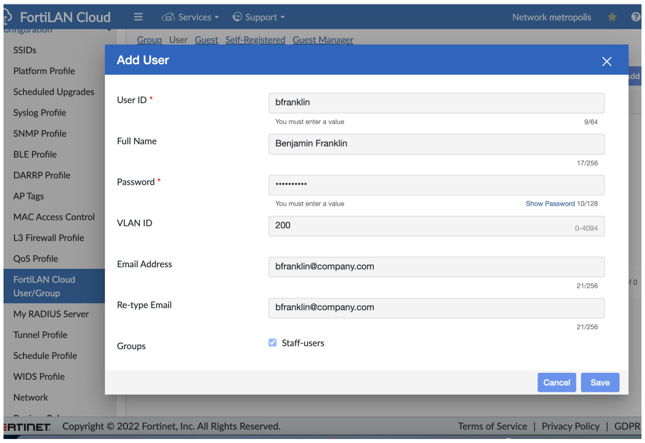
Add Group

Group ID *: Staff-users (You must enter a value, 11/16)

Description: full access staff (17/255)

VLAN ID: 200 (0-4094)

Cancel Save



Add User

User ID *: bfranklin
You must enter a value 9/64

Full Name: Benjamin Franklin
17/256

Password *: ••••••••••
You must enter a value Show Password 10/128

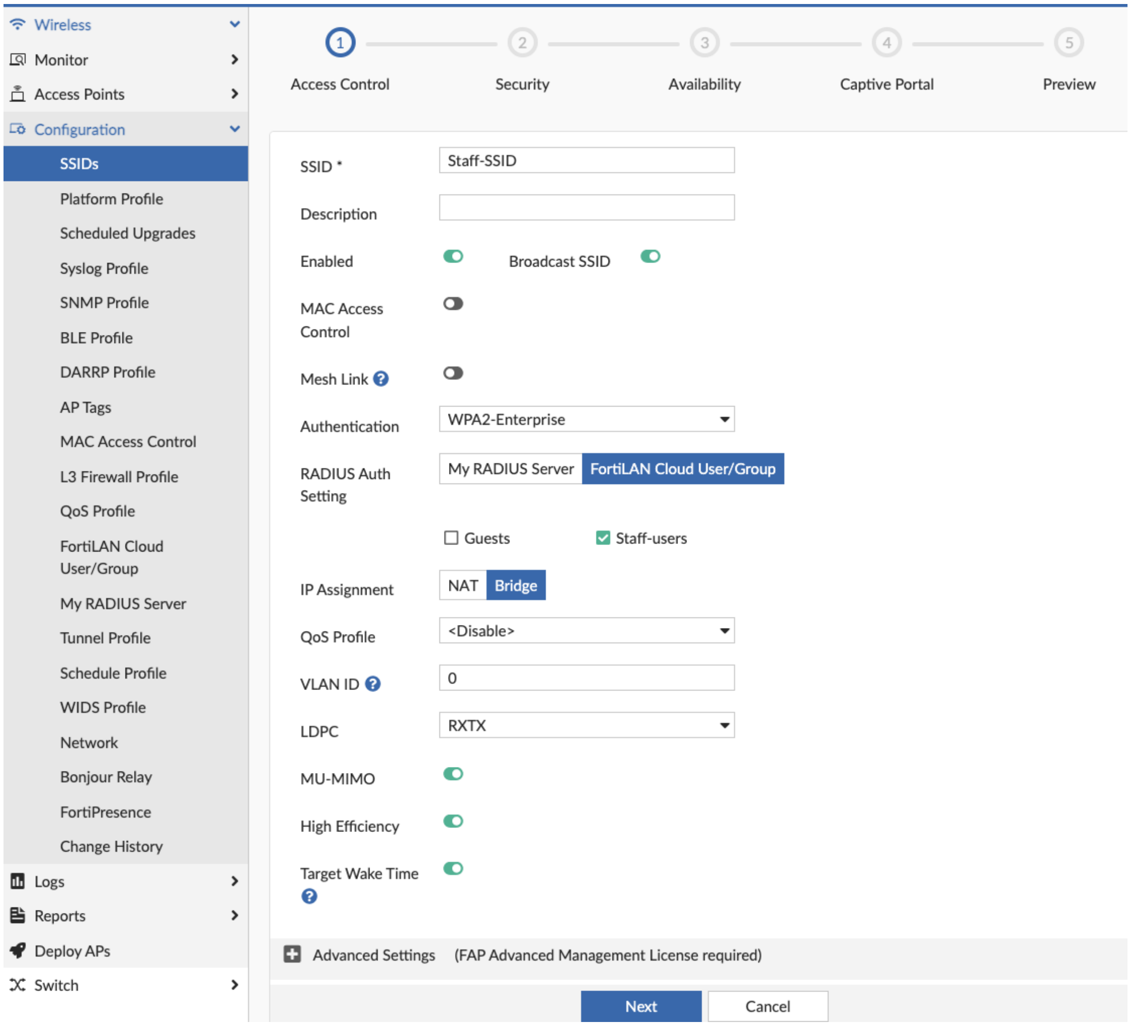
VLAN ID: 200 0-4094

Email Address: bfranklin@company.com
21/256

Re-type Email: bfranklin@company.com
21/256

Groups: ☑ Staff-users

After you have your RADIUS setup, The FortiLAN Cloud SSID creation includes a brief wizard style setup that walks you though several options.



SSID *: Staff-SSID

Description:

Enabled: ● Broadcast SSID: ●

MAC Access Control: ○

Mesh Link: ○

Authentication: WPA2-Enterprise

RADIUS Auth Setting: My RADIUS Server [✓ FortiLAN Cloud User/Group]

☐ Guests ☑ Staff-users

IP Assignment: NAT [✓ Bridge]

QoS Profile: <Disable>

VLAN ID: 0

LDPC: RXTX

MU-MIMO: ●

High Efficiency: ●

Target Wake Time: ●

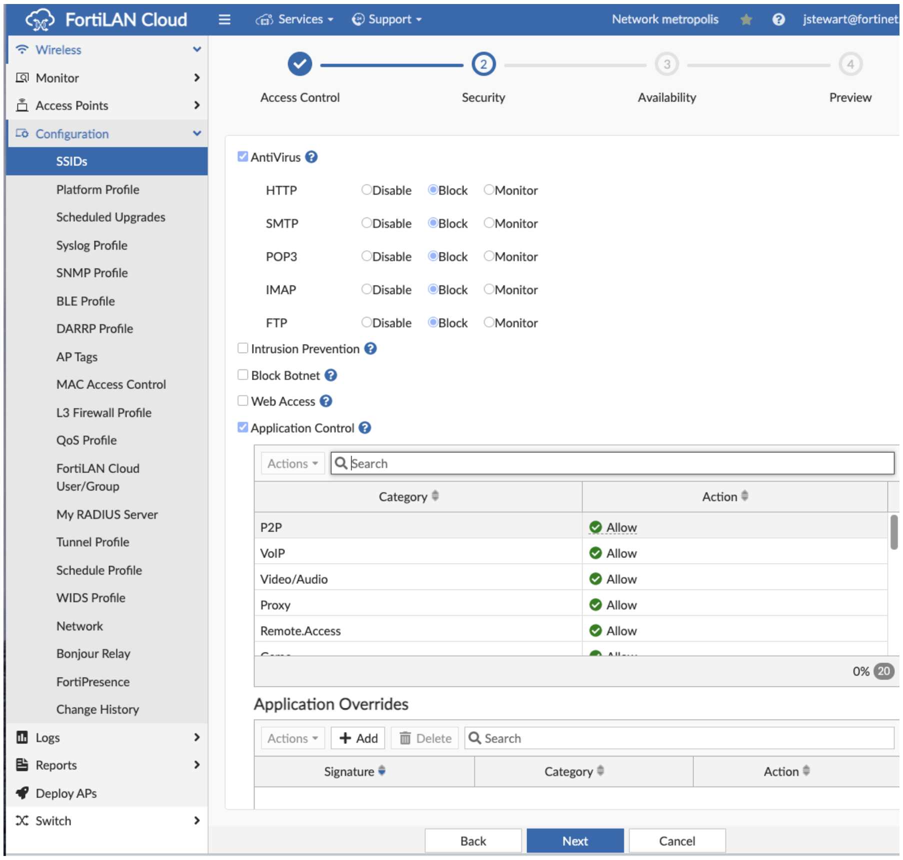
Advanced Settings (FAP Advanced Management License required)

Security Options

Multiple security options can be run on U-model FortiAPs, including:

- Antivirus
- Intrusion Prevention
- Block Botnet
- Web Access
- Application Control

These options can be configured per SSID. Note that these security checks will not run on basic FortiAPs but only the FortiAP-U models, and any necessary licensing must be enabled.



☑ AntiVirus

HTTP	○Disable	●Block	○Monitor
SMTP	○Disable	●Block	○Monitor
POP3	○Disable	●Block	○Monitor
IMAP	○Disable	●Block	○Monitor
FTP	○Disable	●Block	○Monitor

□ Intrusion Prevention

□ Block Botnet

□ Web Access

☑ Application Control

Category	Action
P2P	✓ Allow
VoIP	✓ Allow
Video/Audio	✓ Allow
Proxy	✓ Allow
Remote.Access	✓ Allow
Game	✓ Allow

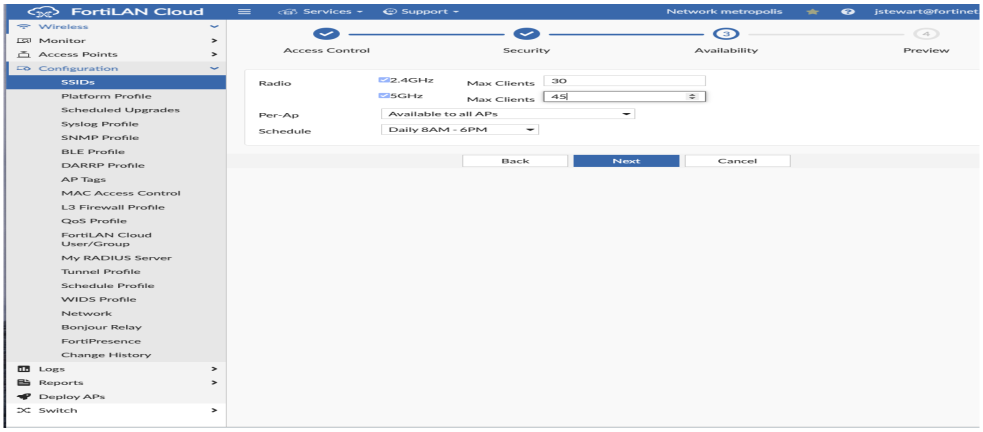
0% 20

Application Overrides

Signature	Category	Action

Availability

The Availability section allows you to configure when the SSID runs, such as business hours only, and set the radio availability and maximum number of clients on a radio.



Radio ☑ 2.4GHz Max Clients 30
☑ 5GHz Max Clients 45
Per-Ap: Available to all APs
Schedule: Daily 8AM - 6PM

This is followed by a final review screen and the SSID is configured and deployed.

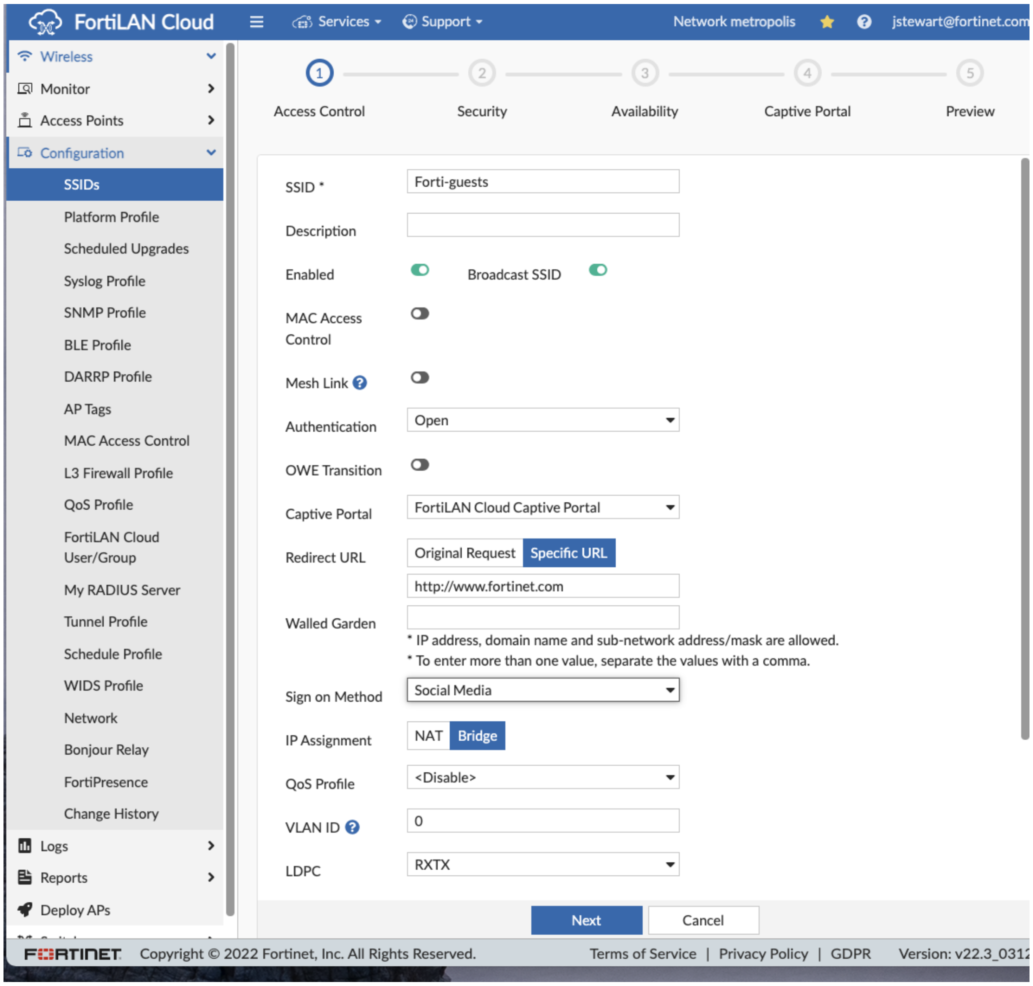
Guest User Management

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 FortiLAN Cloud supports multiple options, and many of those options can be combined.

Captive Portal

Captive portals are browser-based authentication screens and are the most common restriction used with guest access SSIDs. Recall that 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 often useful to reduce casual use of the network by neighbors when the portal is a disclaimer only.

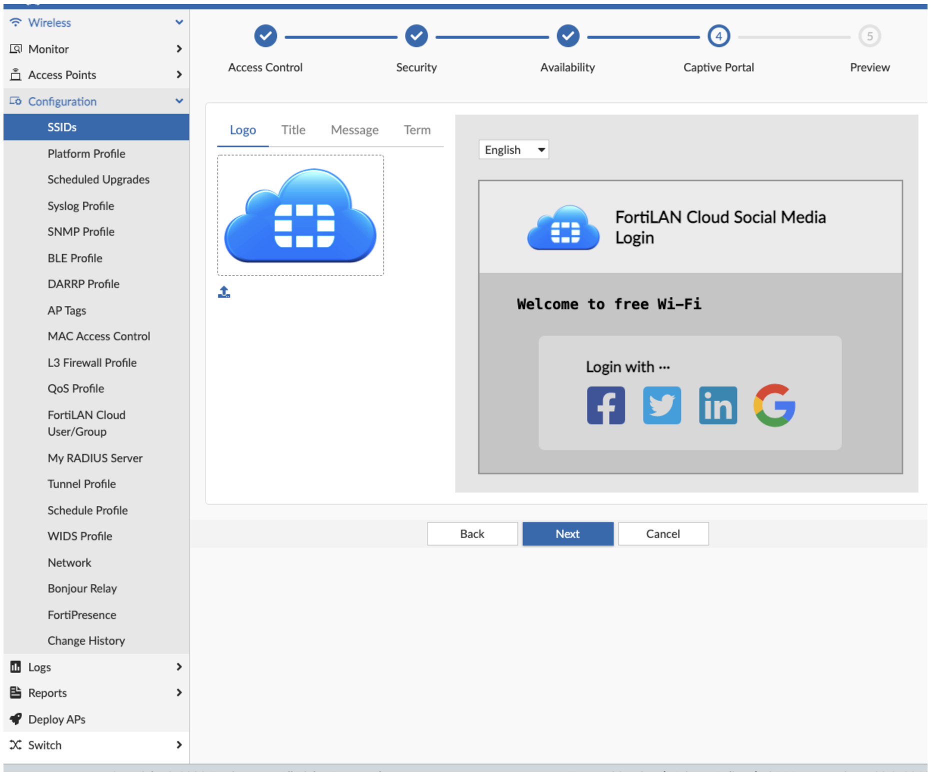


SSID *	Forti-guests
Description	
Enabled	●
Broadcast SSID	●
MAC Access Control	○
Mesh Link	○
Authentication	Open
OWE Transition	○
Captive Portal	FortiLAN Cloud Captive Portal
Redirect URL	Original Request [✓ Specific URL] http://www.fortinet.com
Walled Garden	
Sign on Method	Social Media
IP Assignment	NAT [✓ Bridge]
QoS Profile	<Disable>
VLAN ID	0
LDPC	RXTX

* IP address, domain name and sub-network address/mask are allowed.
* To enter more than one value, separate the values with a comma.

Captive portal configuration has the following options.

- My Captive Portal for the case where you have an existing or third-party captive portal that you want to direct users to. In this case, you would have to provide the URL of the captive portal
- FortiLAN Cloud Captive Portal is for the case where FortiLAN Cloud provides the portal, The wizard will provide a view of the portal and the option to adjust configuration at step 4 after the Security and Availability steps.



FortiLAN Cloud Captive Portal with Social Media Login provides the following options.

- Redirect URL determines, once the user is allowed access, if they go to the originally requested URL, or to something else, typically the company’s home page.
- The Walled Garden Sometimes a network or internet resource needs to be available before a user has authenticated. The Walled Garden is a list of web domains that users can access before completing the authentication process. You can type an IP address, domain name, and subnetwork address/mask. Separate multiple entries with a comma.
- Sign on Method is where the choices get truly interesting.
  - Click through simply provides a continue button. This is typical of a public access venue that simply wants to present a terms and conditions page.
  - My RADIUS Server allows authentication via the RADIUS server. However, this is via the captive portal and not 802.1X. Probably WPA Enterprise would be a better choice, but your network may have an unusual need.
  - FortiLAN Cloud user and group is similar, but makes sense when combined with a guest group. Note that a guest administrator can be created in IAM and then granted guest Management Access, able to create temporary users.
  - Self-registered guests access thecaptive portal page and sign up for an account.They receive their username and password detailsby SMS or email. The registration information is captured and can be found in the FortiLAN Cloud network page.
  - Social MediaUsers can sign on with a socialmedia account. FortiLAN Cloud supportsFacebook, Google+, LinkedIn, and Twitteraccounts.

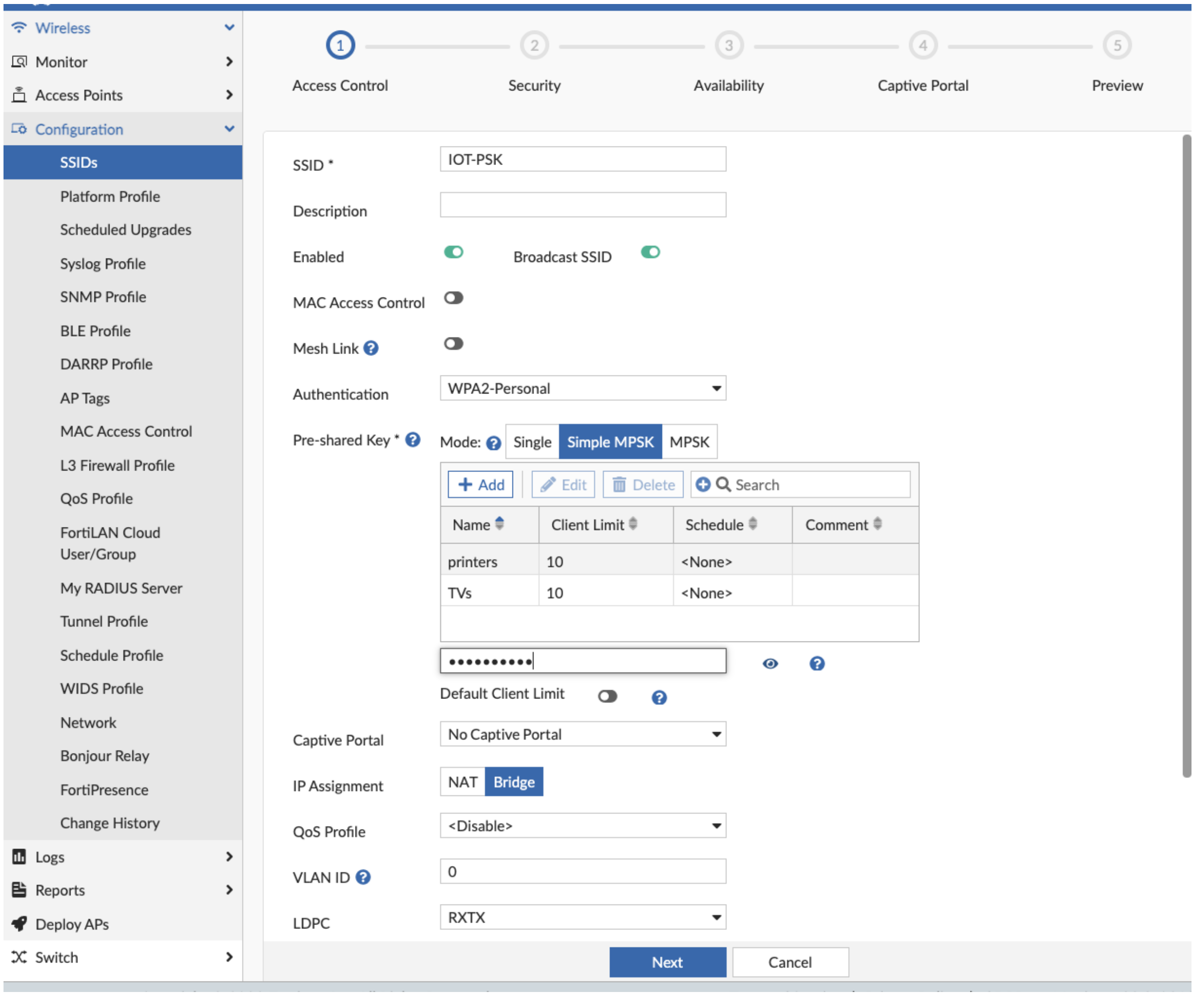
Ownerless devices – PSK + MPSK

The final type of devices to be concerned with are, broadly speaking, the 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 pre-shared key 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.

Two levels of MPSK are available in the SSID configuration. Full MPSK allows creation of MPSK groups and including VLAN assignments and automatic generation of large numbers of keys. Simple reduces the configuration overhead. At creation, an MPSK key can be set for a single or multiple devices.

MPSK is an extension of WPA2 Personal, and is not available with WPA3 SAE. Of course, there is no reason why you cannot use the single key option for a WPA2 Personal SSID, if that fits your needs



SSID * IOT-PSK

Description

Enabled ● Broadcast SSID ●

MAC Access Control ○

Mesh Link ○

Authentication WPA2-Personal

Pre-shared Key * Mode: Single [✓ Simple MPSK] MPSK

Name	Client Limit	Schedule	Comment
printers	10	<None>	
TVs	10	<None>	

••••••••••

Default Client Limit ○

Captive Portal No Captive Portal

IP Assignment NAT [✓ Bridge]

QoS Profile <Disable>

VLAN ID 0

LDPC RXTX

FortiLAN Cloud Wi-Fi Design Conclusion

FortiLAN Cloud Wireless LAN architecture is highly adaptable. It scales both up and down from one or two FortiAPs at one site to a virtually unlimited number at 1000s of sites. 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.

Appendix A: Documentation References

This appendix provides additional reference information for FortiLAN Cloud.

Solution Hub

- FortiCloud Solution Hub
- Secure Access Solution Hub

Feature Documentation

- FortiLAN Cloud User Guide
- FortiCloud Account Services

Related 4-D Documentation

- FortiCloud Overview
- 4-D resources Wireless
- FortiLAN Cloud Wireless Concept Guide

www.fortinet.com