DEFINE • DESIGN • **DEPLOY**

FortiLAN Cloud

Wireless LAN Deployment

Version 1.0.0

TABLE OF CONTENTS

Change Log

Version	Change	Date
1.0.0	Release Draft	2022-10-12
1.0.0	Modified the document format.	2022-10-27
1.0.0	Corrected a spell error.	2023-04-20

Introduction

This section aims to Introduce the purpose of this guide.

Executive Summary

This deployment guide is intended to cover the key configuration needs of Fortinet Wi-Fi deployments at single or multiple locations of FortiAPs using FortiLAN Cloud management. As a Cloud Management Service hosted by Fortinet in Fortinet datacenters, FortiLAN cloud has an enormous scalability range, and is well suited to everything from a single FortiAP at a single site to tens of thousands of FortiAPs over thousands of locations.

Fortinet has a large portfolio of products and corresponding Cloud Services to manage those products. Some clarifications are warranted. The FortiLAN Cloud Service is also a management system for FortiSwitches. It is a complete LAN solution, both wired and wireless. However, this document is specifically focused on Wi-Fi deployment of FortiAPs. Although Fortinet Switches are an excellent choice and there are advantages to an all-Fortinet network, this guide is written with the assumption of generic switches from any vendor.

Another important clarification is that 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 they are typically described as stand alone.

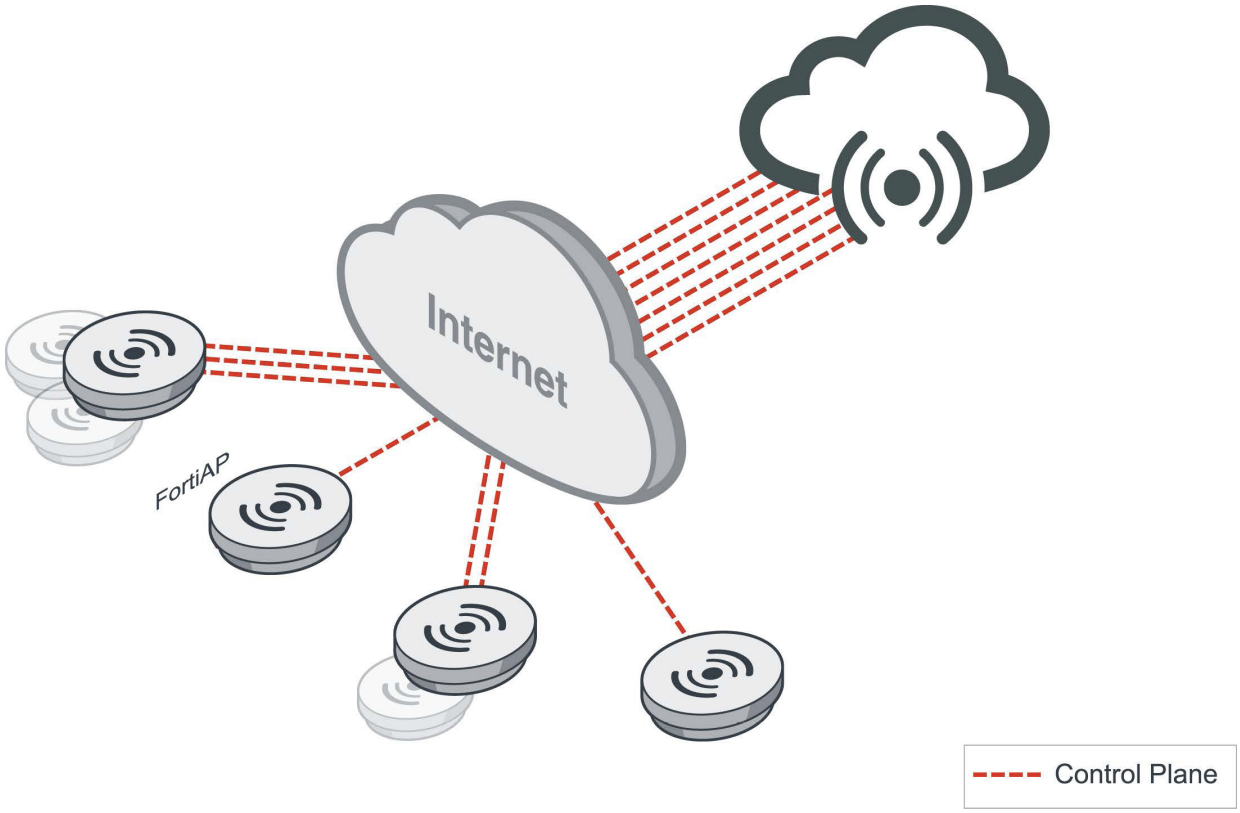
This guide is specifically focused on deployment of FortiAPs in standalone mode as managed by the FortiLAN Cloud Service.

FortiLAN Cloud Licensing Tiers

FortiLAN cloud supports 3 licensing tiers for customers of various sizes and needs.

- Free Tier – Management of up to 30 FortiAPs, 3 FortiSwitches, 3 sites and 7 days of log storage. If you have a small organization or want to pilot FortiLAN Cloud, you can simply start using the service immediately.
- Licensed Tiers - Scale with number of sites, hold one year of logs, and introduce advanced wireless and switch features. For larger organizations with greater IT needs.
- Multi-Tenancy License - Designed for managed security service providers (MSSPs). A multi-tenancy account allows creation and management of multiple sub-accounts. Devices can be added or moved between sub-accounts and each account can have its own administrators and users.

See FortiGate Cloud WLAN Architecture Guide for planning details



Intended Audience

This guide is intended for an audience who is interested in deploying a FortiAP wireless solution that will be managed via the FortiLAN Cloud Service. Readers should have a basic understanding of networking, wireless and security concepts before they begin. Interested audience may include the following.

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

About this Guide

After reading the FortiGate Cloud WLAN Architecture Guide, you should have an understanding of the components, features and design that are offered by Fortinet's Wireless FortiLAN Cloud solution. It is advisable for readers to evaluate their environment to determine whether this architecture and design is suitable for them before proceeding.

This deployment guide presents one of many possible ways to deploy the Fortinet solutions. It may also omit specific steps where readers must make design decisions to further configure their devices. It is recommended that readers also review supplementary material found in product admin guides, example guides, cookbooks, release notes and other documents where appropriate.

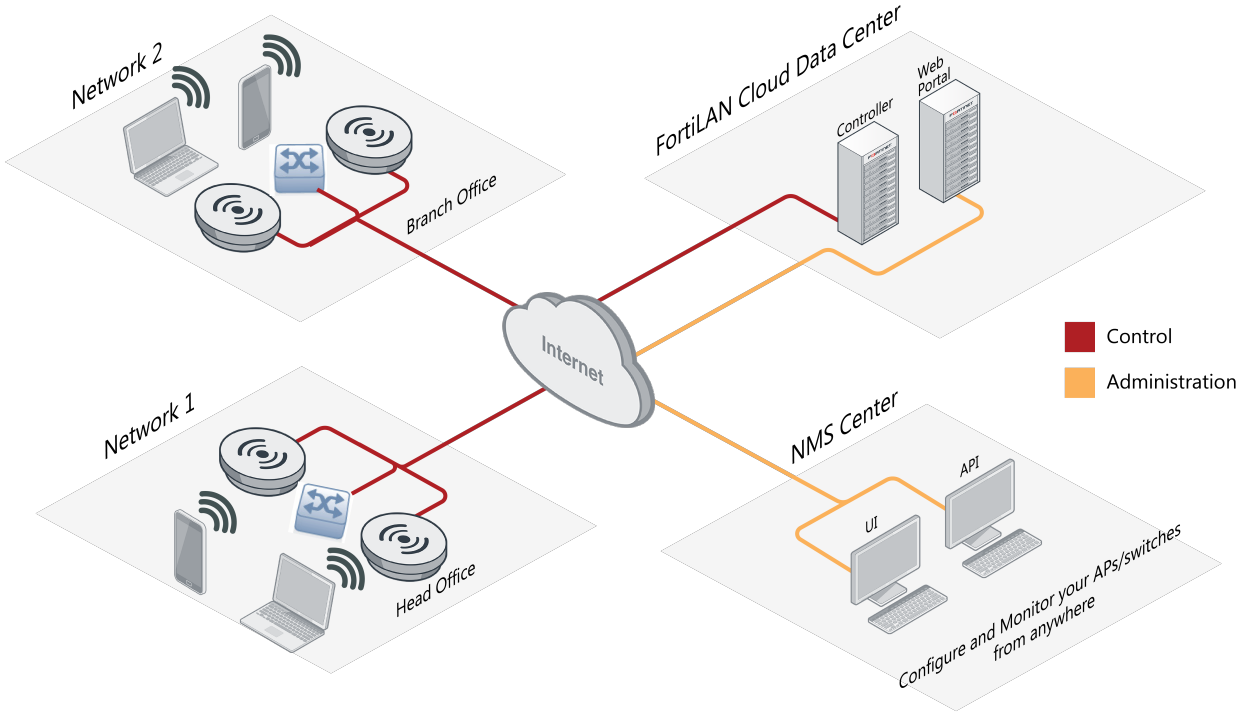
Deployment Overview

FortiAPs, and FortiSwitches, when connected to a network with Internet access will contact FortiCloud automatically as art of their startup process. When they are registered to an account and deployed to FortiLAN Cloud, they will follow the configuration assigned to them and maintain continuous connection with FortiCloud. Only management traffic, sometimes called control plane, will be routed to the FortiLAN Cloud Service, while client device, or data plane traffic, will route locally in accordance with your network configuration.

Standalone FortiAP client traffic is not typically tunneled to a central device or location, as is typical in a Wi-Fi controller-based network architecture. In the standalone AP architecture, a FortiAP is logically a network layer 2 device, like an Ethernet switch, and traffic will be switched/routed directly through the network. Of course, the details of possible network configurations are infinite, but when in doubt, remember that a standalone FortiAP is a logical switch. The Ethernet ports are uplink ports, the wireless clients are each getting a virtual port/connection.

FortiAP coverage area will depend on local conditions. Walls degrade Wi-Fi radio signals, and how much they degrade them is material dependent. A FortiAP can cover a larger open space area than an area with many small offices. As a preplanning rule of thumb, the average coverage area is likely around 2000 Sq Ft per FortiAP.

FortiLAN Cloud is built around Networks. Networks are logical groups of devices that share configuration, and usually represent locations. That is, if you have three locations, specific FortiAPs will be assigned to each location and share configurations. This image depicts a FortiLAN Cloud architecture with branch offices.



Deployment Assumptions

The following guidelines are assumed for this deployment.

- For a site, there is a working Internet connection and basic network.
- FortiAPs plugged into the network will get DHCP addresses and be able to reach the Internet; and therefore the FortiLAN Cloud service.
- Any necessary switch network already exists, of no specific vendor.
- FortiAPs will be powered either via the switches or power injectors using the correct level of Power over Ethernet (PoE) for the AP model.
- Details of physical AP deployment and hanging are not discussed here.

Steps to Follow

Perform the following steps to get started with FortiLAN Cloud deployment.

- Register a FortiCloud administrative account which will be used for asset management and configuration.
- Register the FortiGate in FortiCloud Asset Management.
- Deploy the FortiGate to FortiGate Cloud for management.
- Connect the FortiGate to the Internet.
- Examine basic ForitGate Cloud Navigation and default settings – adjust if needed.
- Authorize FortiAPs.
- Configure a secure SSID (RADIUS based) and supporting firewall policies.
- Configure a guest access and supporting firewall policies.
- Configure a pre-shared key SSID for IoT devices and supporting firewall policies.

Deployment Procedures

This section describes the following topics.

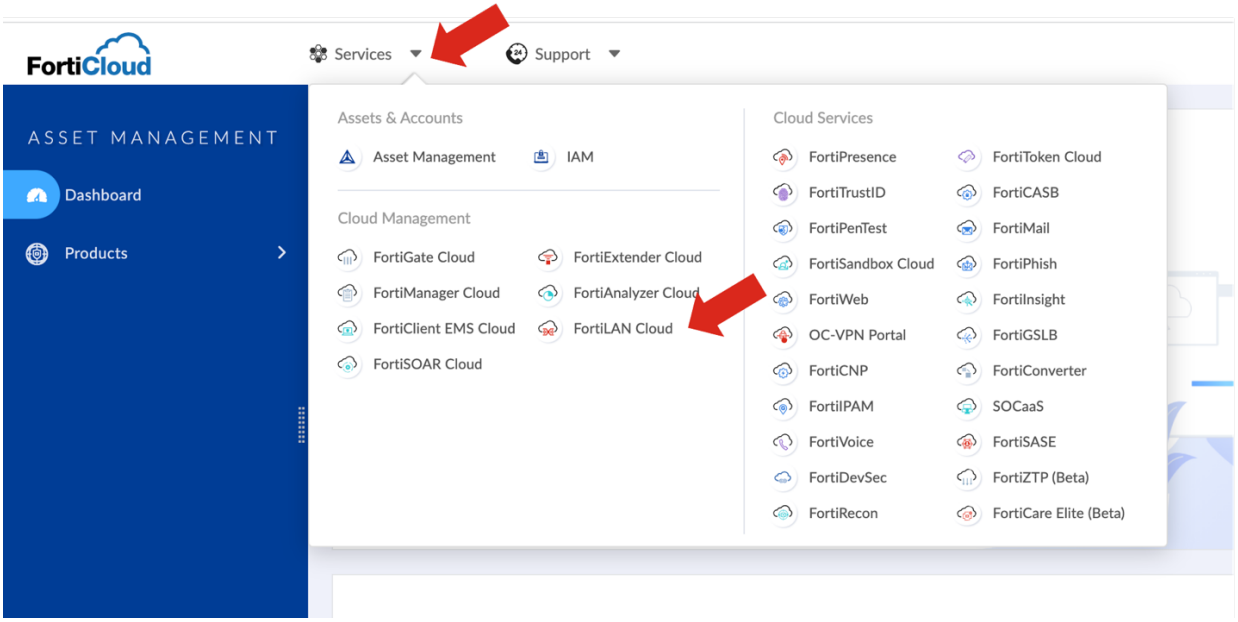
Deployment Procedures

This section describes the following topics.

Two Login paths – Support vs FortiLAN Cloud

There are actually two login paths to FortiLAN Cloud. Using support.fortinet.com takes you to the Asset Management portal, a clearing house for all of your Fortinet assets across all of your Fortinet products. From here you can navigate to all of your FortiCloud portals, including FortiLAN Cloud. Any other portal, you can navigate to FortiLAN cloud via the Services drop down menu.

- Click on the **Services** drop down.
- Under **Cloud Management**, click on **FortiLAN Cloud**.

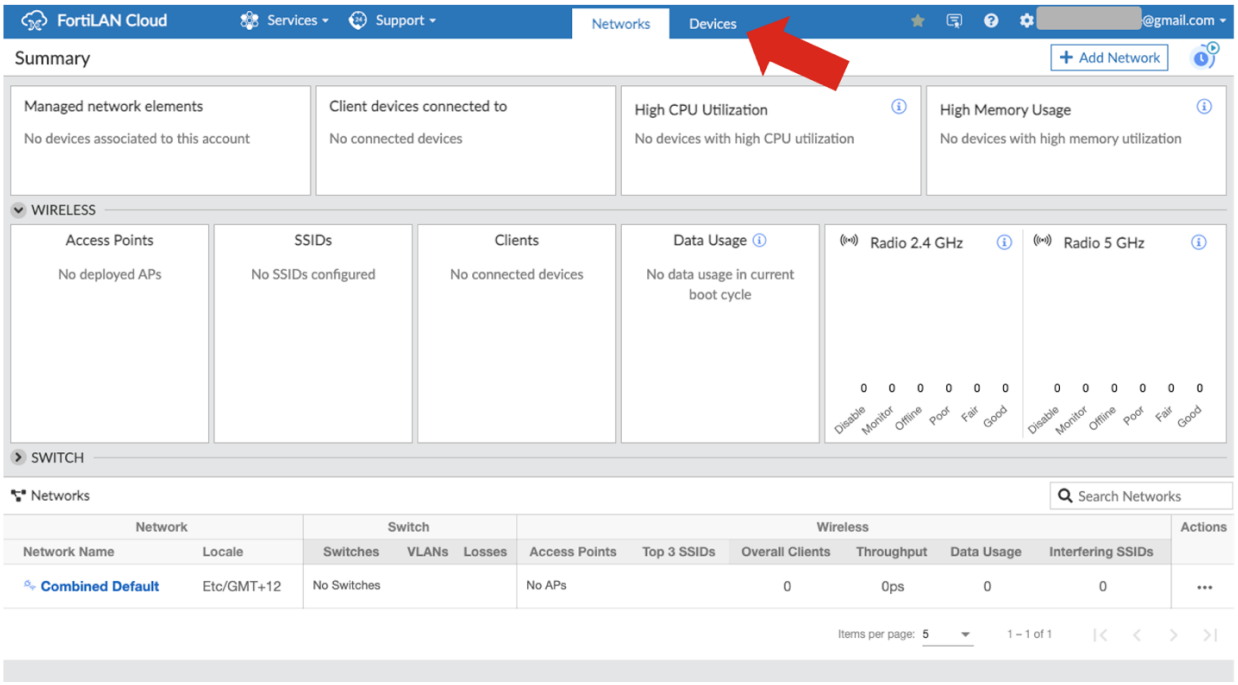


Alternatively, you can login directly to FortiLAN Cloud via fortilan-login.forticloud.com

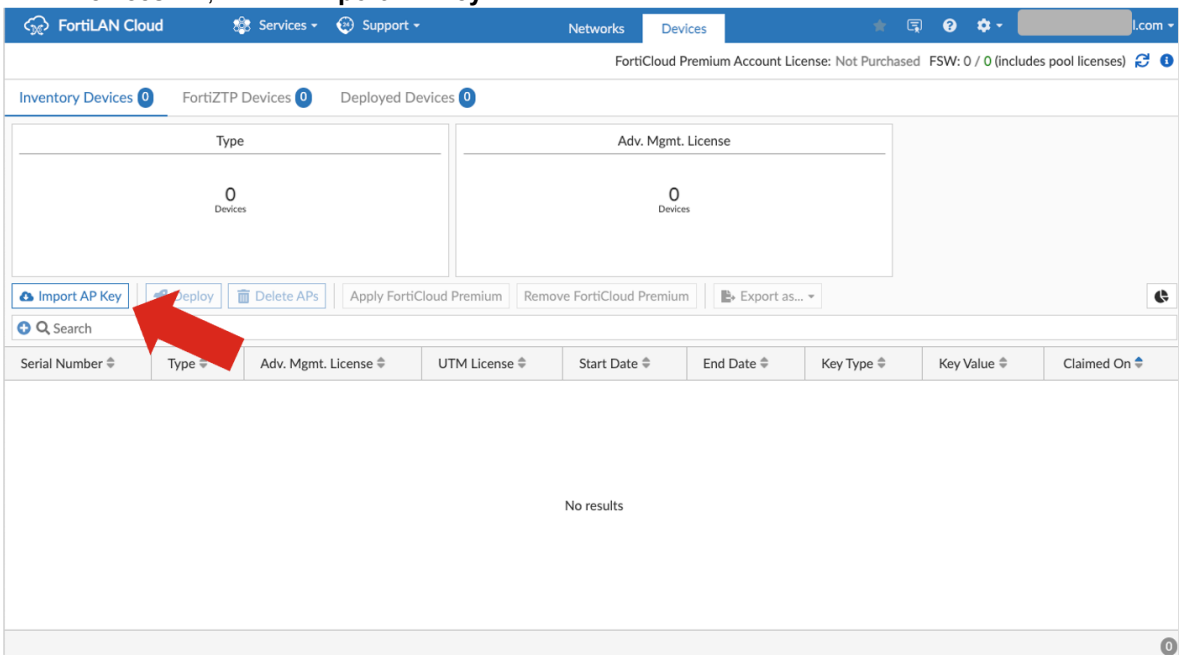
Adding FortiAPs to FortiLAN Cloud Using FortiCloud Key

Every FortiAP has a FortiCloud key associated with it. The FortiCloud Key can be found on a sticker of the back of the FortiAP. Bulk keys that cover multiple FortiAPs are also available when ordering FortiAPs as a zero coast line item. Once you have located the FortiCloud Key(s) that you will use, to add the FortiAP to FortiLAN Cloud.

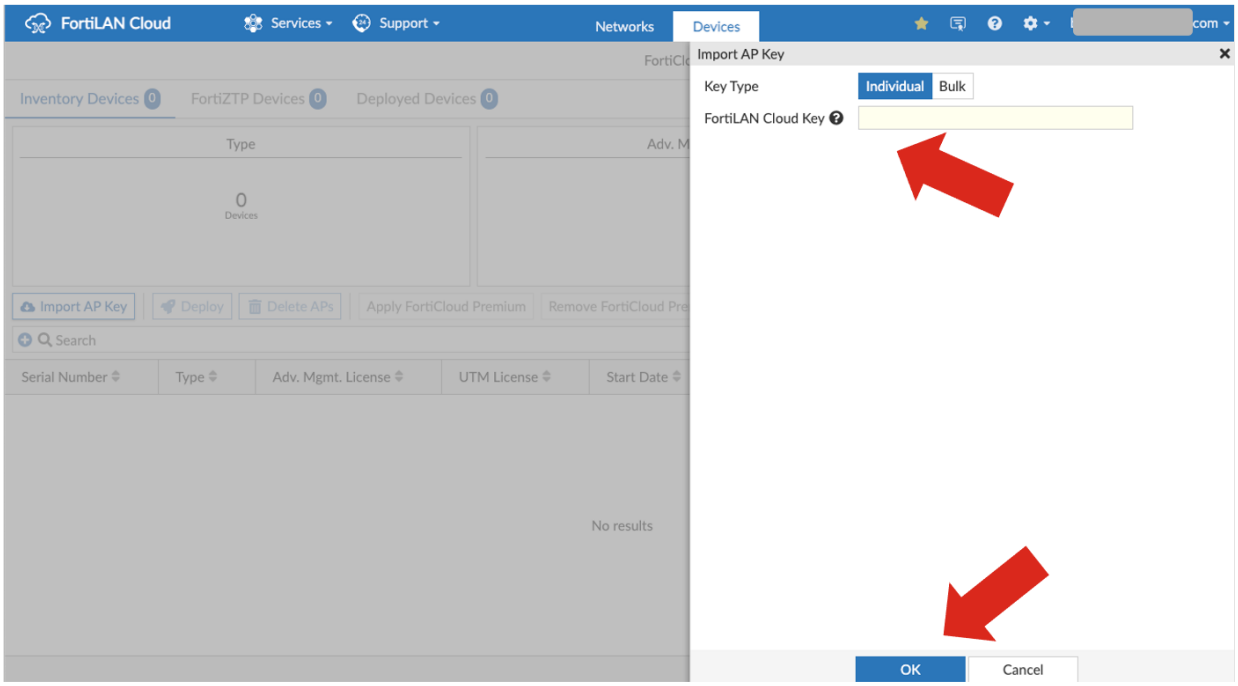
- Login to FortiLAN Cloud and go to the **Devices** tab.



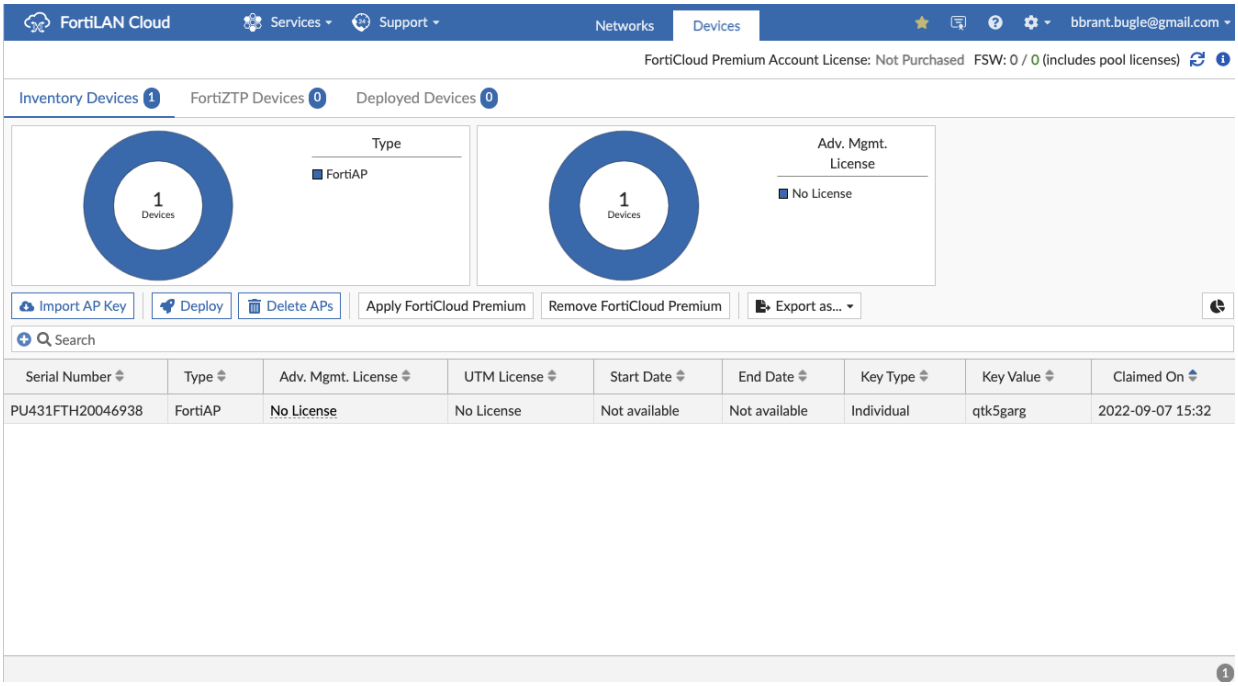
- In the **Devices** tab, click on **Import AP Key**.



- Choose **Individual** (the default) or **Bulk** for the **Key Type**.
- Enter the **FortiLAN Cloud Key**.
- Click **OK**



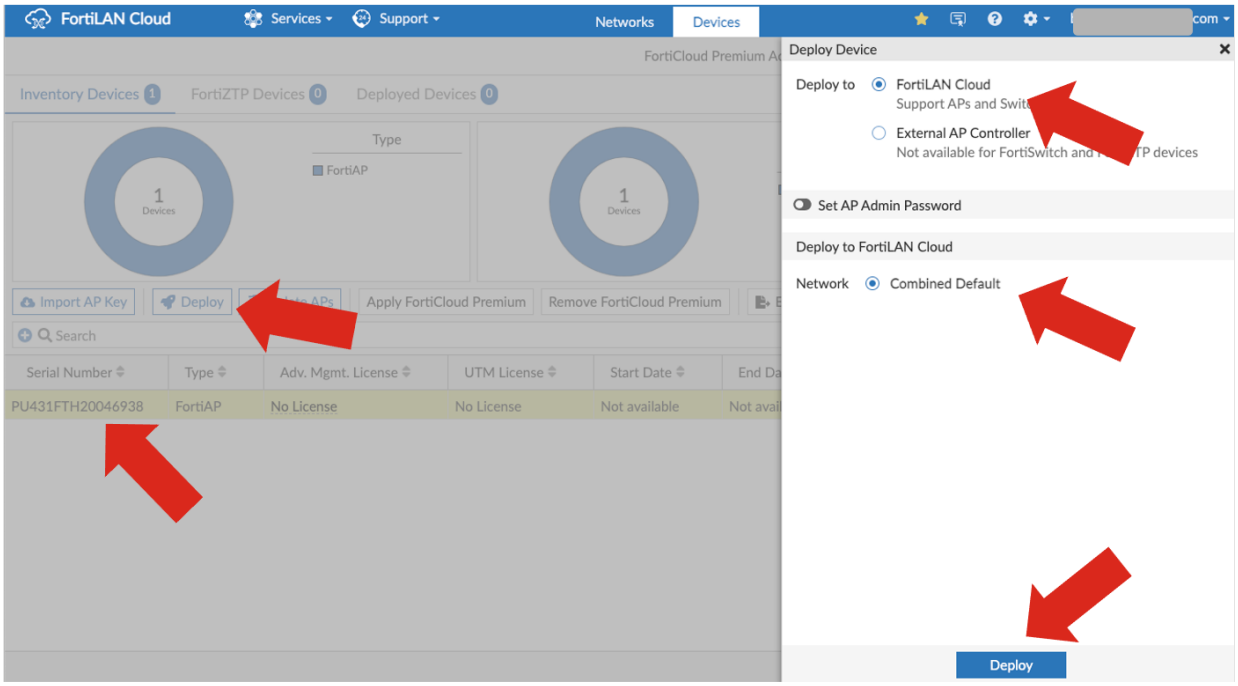
- The FortiAP is added to the **Inventory Devices**.



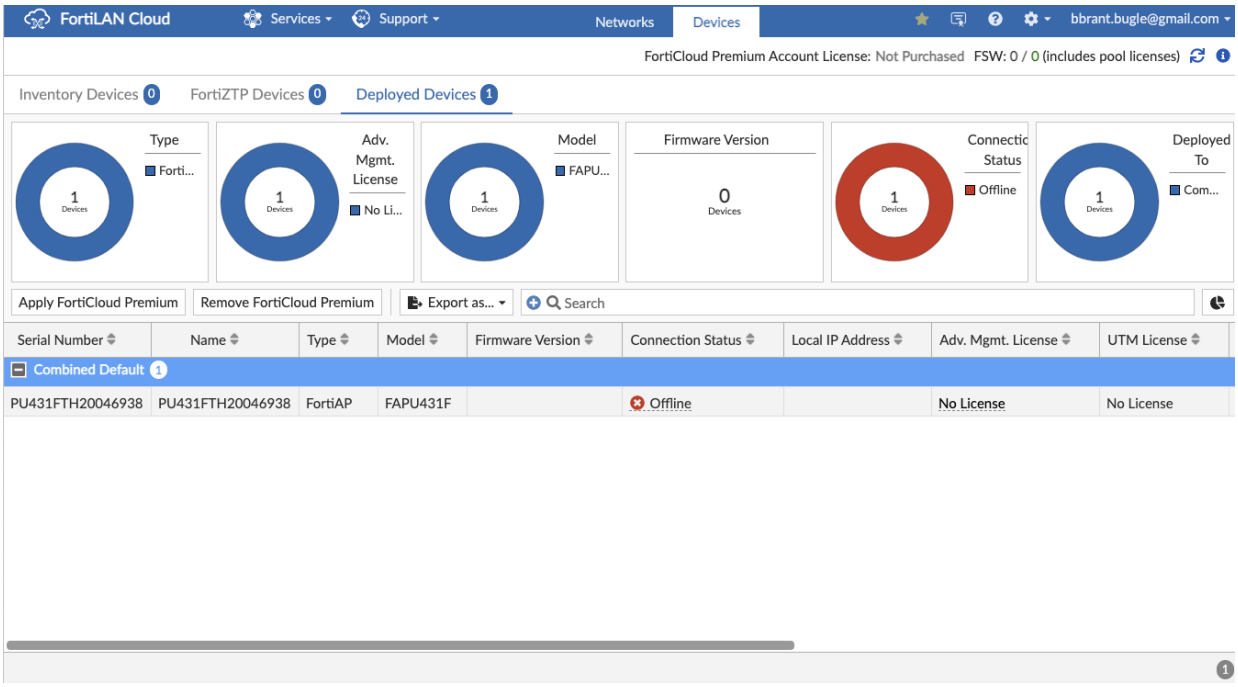
Deploy a FortiAP to a Network

In FortiLAN Cloud, a network is a group of devices that share configuration. Usually this means they are on the same physical site. A default network exists, and for a single location deployment can be used to deplly the first FortiAPs. A later section will describe adding networks. The only change to deploying a FortiAP is that there will be more networks to choose from. To deploy an inventory FortiAP to a network

- Select the FortiAP(s) to deploy
- Click **Deploy** and in the **Deploy Device** page, select **FortiLAN Cloud**.
- Choose the **Network**, if there is more than one.
- Click **Deploy**.



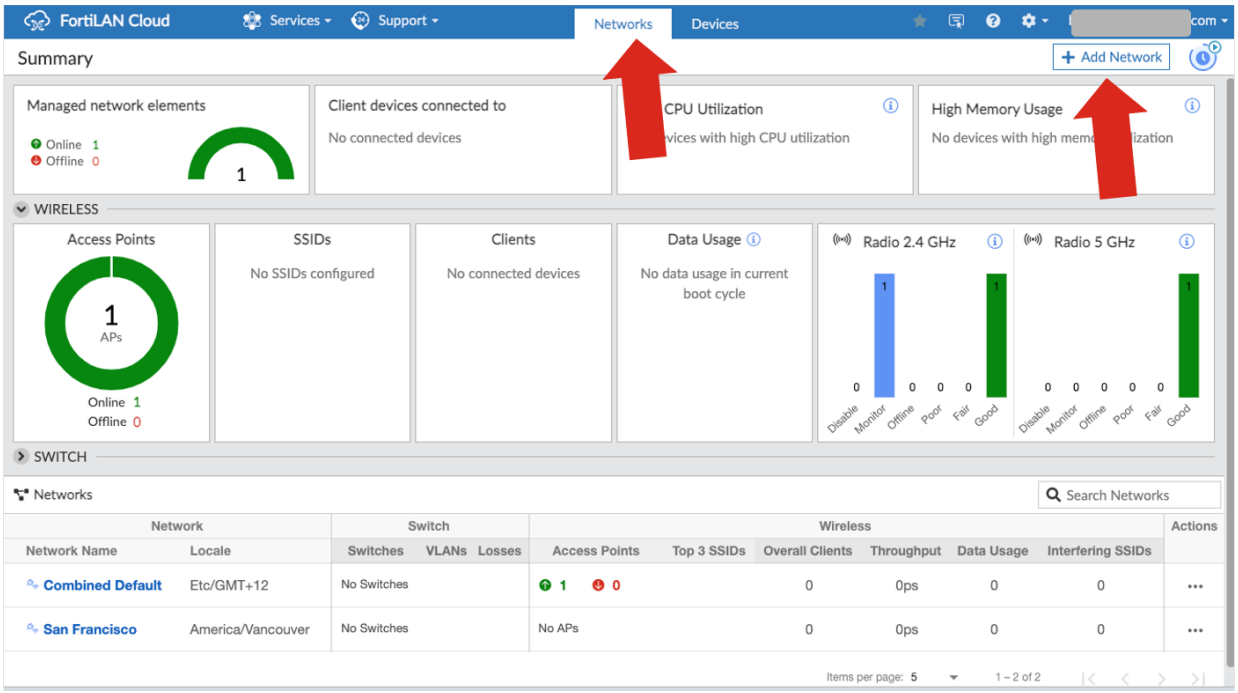
The FortiAP is now deployed to the network.


FortiLAN Cloud
Services
Support
Networks
Devices
bbrant.bugle@gmail.com
FortiCloud Premium Account License: Not Purchased FSW: 0 / 0 (includes pool licenses)
Inventory Devices 0
FortiZTP Devices 0
Deployed Devices 1
Type
Forti...
Adv. Mgmt. License
No Li...
Model
FAPU...
Firmware Version
Connectic Status
Offline
Deployed To
Com...
1 Devices
0 Devices
Apply FortiCloud Premium
Remove FortiCloud Premium
Export as...
Search
Serial Number
Name
Type
Model
Firmware Version
Connection Status
Local IP Address
Adv. Mgmt. License
UTM License
Combined Default 1
PU431FTH20046938
PU431FTH20046938
FortiAP
FAPU431F
Offline
No License
No License

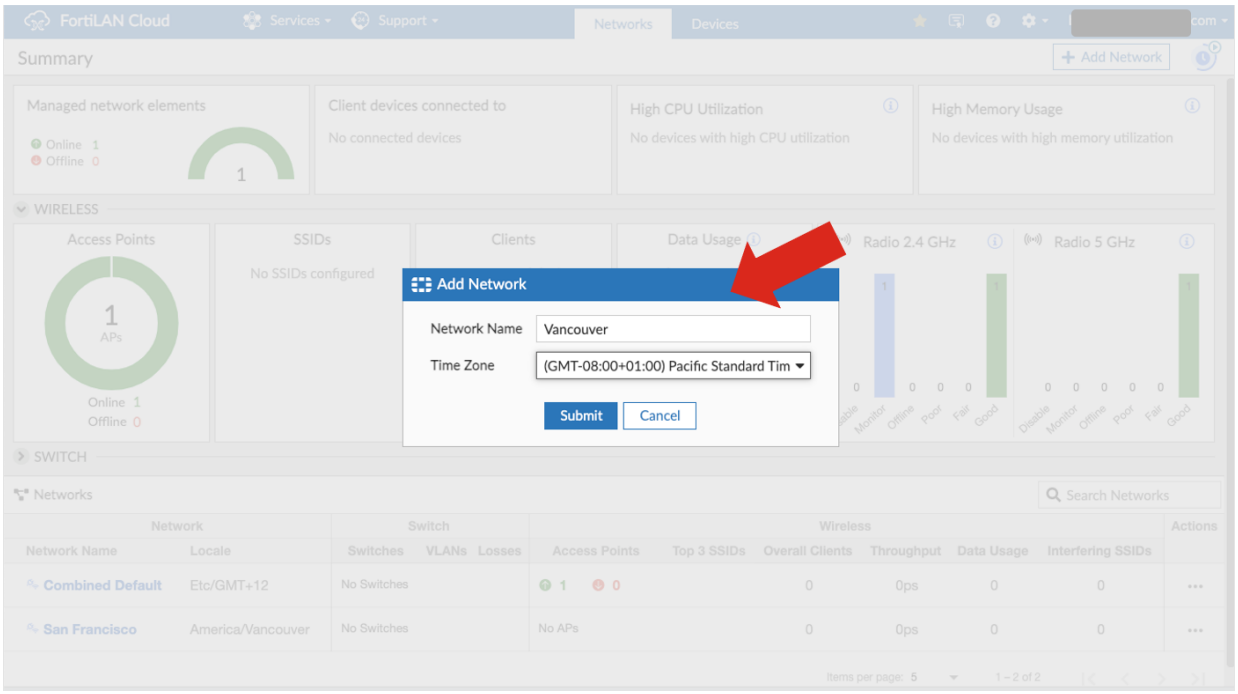
Adding a Network to FortiLAN Cloud

As stated above, Networks in FortiLAN cloud are collections of devices with will receive the same (or very similar) configurations. Usually, they correspond to locations. To add a Network…

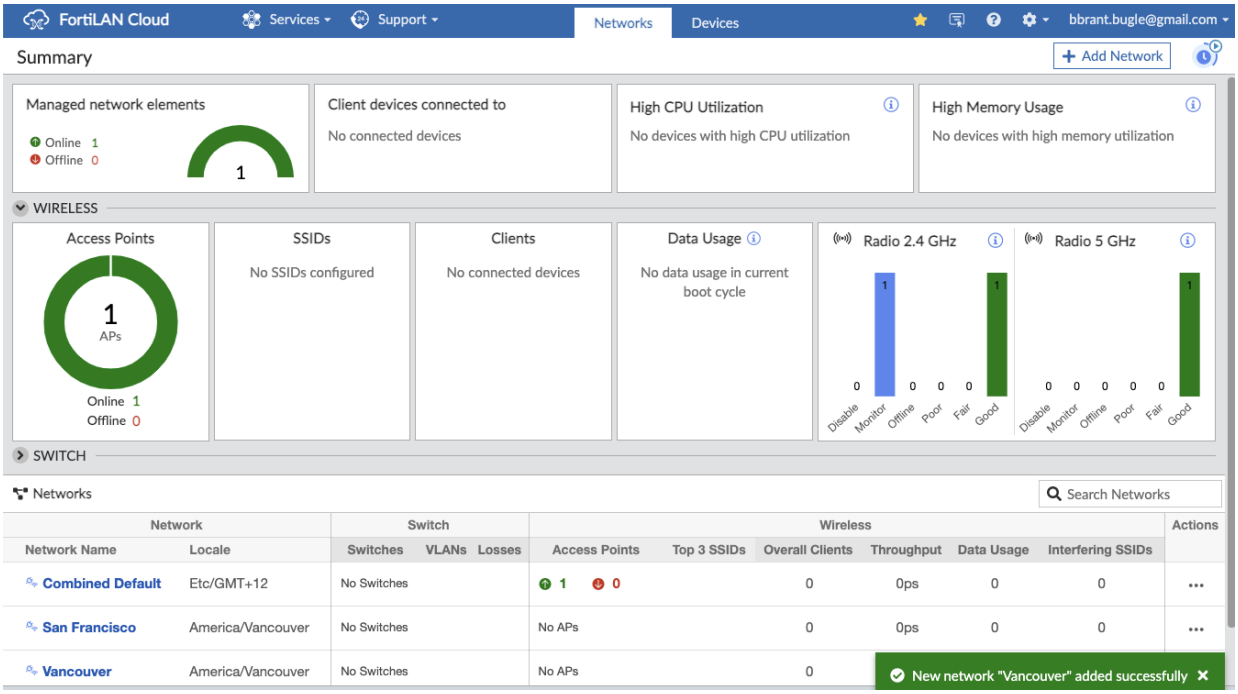
- Click on the **Networks** tab and then click **+ Add Network**.



- Enter the **Network Name** and choose the **Time Zone**.
- Click **Submit**.



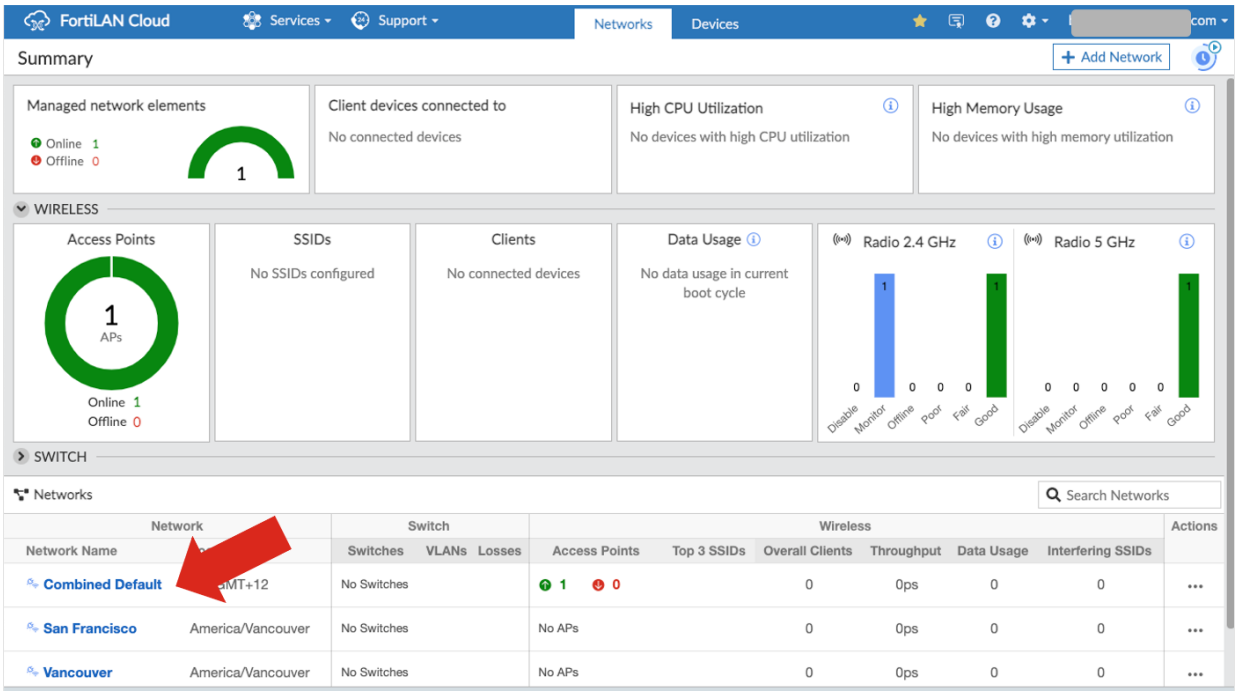
The network is added to the **Networks** List. FortiAPs can deployed (or redeployed) now.



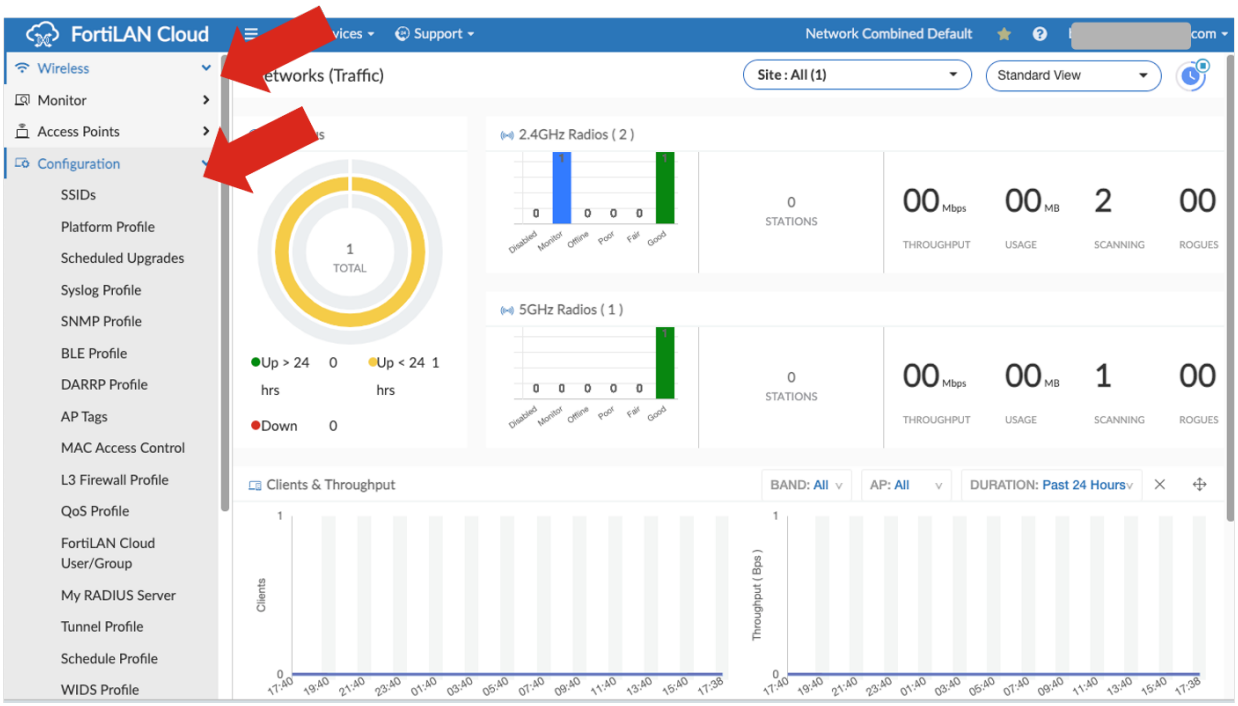
Configuring Networks in FortiLAN Cloud

Follow this procedure to configure networks in FortiLAN Cloud.

- Login to FortiLAN Cloud portal and click on the **Network Name** of the network you wish to configure.



- The screen opens in another browser tab; in the left-hand ribbon menu, select **Wireless > Configuration**.



There is a lot of power here, with many options that can be configured. The focus of this guide is to get a the most common network configurations up and running efficiently. For a full understanding of all the available options, we recommend the FortiLAN Cloud User Guide .

In this guide, we focus on 3 types of SSIDs, or WLANs:

- SSIDs using a Pre-Shared Key authentication, or WPA-Personal
- SSIDS using 802.1X/RADIUS authentication, or WPA-Enterprise
- Guest SSIDs using Captive Portal authentication
- Additional Fortinet specific options for each of the above.

Considerations on Physical Deployment of FortiAPs

All of the above can be configured without having actually installed any APs. That is, all configuration can be done before FortiAPs are actually on site and powered. So long as they connected to a network switch with sufficient PoE and which puts them on a network with DHCP and internet access, they will connect to FortiLAN Cloud and receive their configuration and any configuration changes at a later time.

Of course, you can similarly physically install the FortiAPs ahead of configuring them, the only caveat being, make sure you have the FortiCloud Key information accurately recorded ahead of time.

This document will not go into details of physically mounting FortiAPs. See the respective QuickStart Guides. However, some best practices to note:

- APs with integrated/internal antennas are intended for ceiling mounts.
- If wall mounting is necessary, an external antenna FortiAP such as the 433F should be chosen with the appropriate antenna. External dipole antennas (the usual “rubber ducks”) should normally be mounted such that they are vertically aligned.
- All antennas have a directional element. Omni-directional antennas propagate the signal in a kind of donut pattern (a torus) and have the strongest signal at the level of the antenna. Perfectly fine for 10 -20-foot

ceilings. Higher ceilings may be better off with down pointed directional antennas. High-gain omni antennas are a poor choice for high ceilings because they flatten the donut into a pancake, raising signal strength at the ceiling level and lowering it at the floor level.

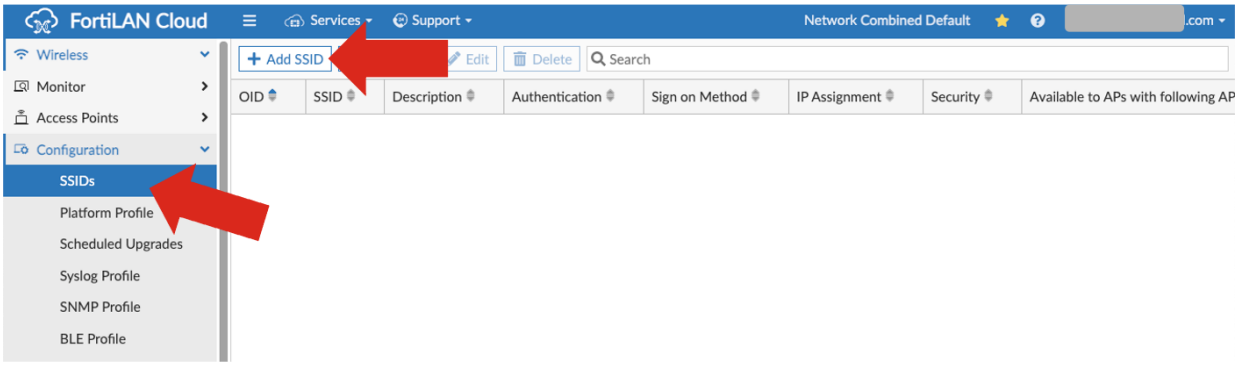
- Be sure the correct PoE level to power the FortiAPs is available from the connecting switches, and that the total PoE budget of a switch is sufficient for the total number of connected FortiAPs. If the connecting switches do not match the needed PoE requirements, power injectors can be used.
- Record the MAC address and/or a serial number of the FortiAPs and their locations. This will help with later documentation and administration.
- When running cable for APs, leave plenty of loop at the AP end to allow them to be moved to adjust coverage. Sometimes moving a FortiAP a few feet/meters can eliminate an unanticipated dead spot. Avoid mounting a FortiAP directly next to metal duct work.

Configure an SSID with Pre-Shared Key/WPA-Personal Authentication

In many ways, the pre-shared key SSID is the *basic* option. Users must authenticate to the network, but they must all use the Pre-Shared Key, usually called the *Wi-Fi password*, but this guide's author admits to being a bit pedantic when writing Wi-Fi documentation.

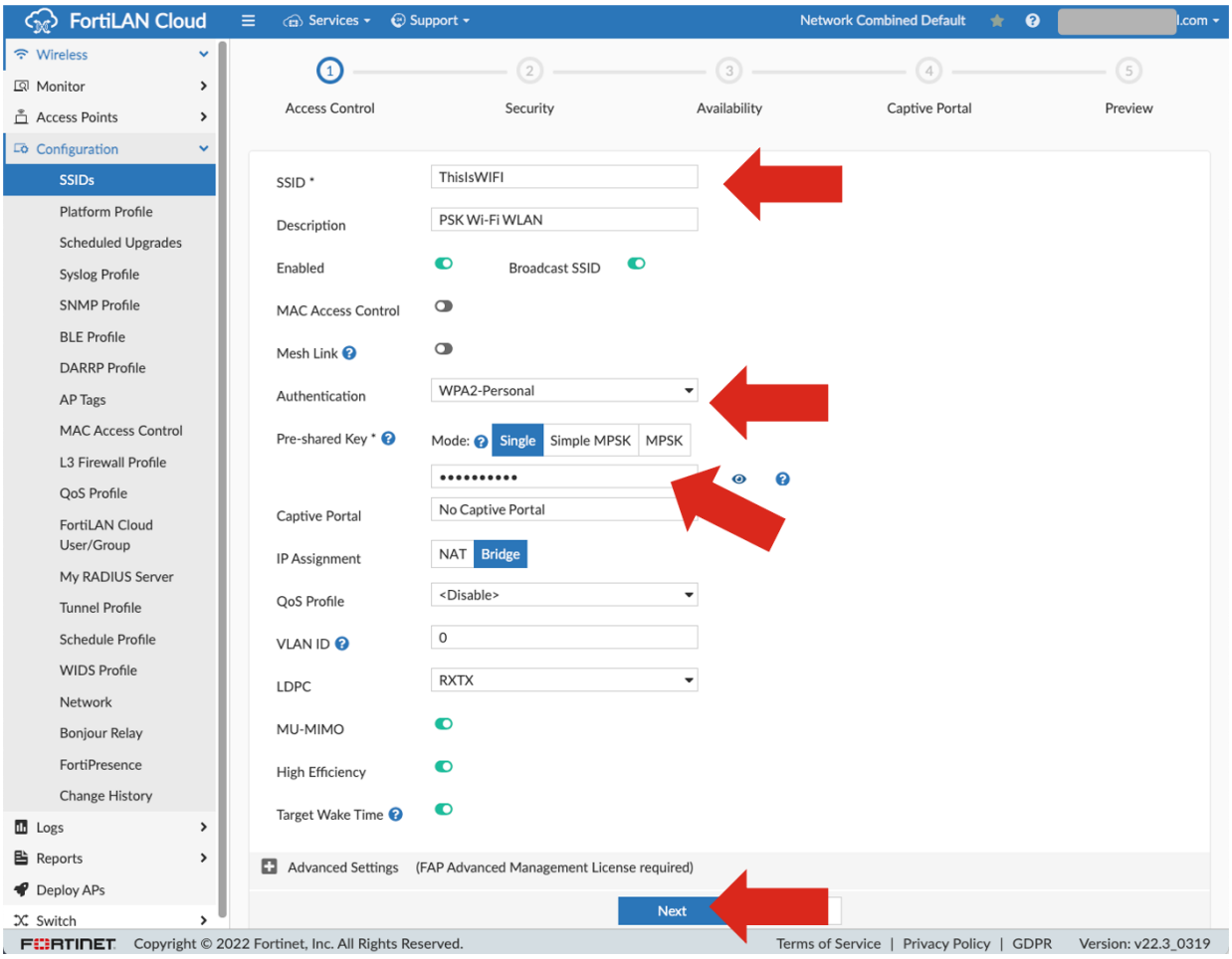
To add an PSK SSID to a network, as above.

- Login into FortiLAN Cloud and click on the **Network Name** of the network the SSID is added to.
- In the newly launched network tab, in the left-hand menu, expand **Wireless > Configuration > SSIDs**.
- In the SSIDs screen, click **+Add SSID**.



- Name the **SSID** and ensure **Authentication** is set to **WPA2-Personal**.
- Set the **Pre-shared Key** Mode as **Single**.
- Enter a value for the pre-shared key and click **Next**.

There are a number of options that will be discussed below.


FortiLAN Cloud
Services
Support
Network Combined Default
Wireless
Monitor
Access Points
Configuration
SSIDs
Platform Profile
Scheduled Upgrades
Syslog Profile
SNMP Profile
BLE Profile
DARRP Profile
AP Tags
MAC Access Control
L3 Firewall Profile
QoS Profile
FortiLAN Cloud User/Group
My RADIUS Server
Tunnel Profile
Schedule Profile
WIDS Profile
Network
Bonjour Relay
FortiPresence
Change History
Logs
Reports
Deploy APs
Switch
1 Access Control
2 Security
3 Availability
4 Captive Portal
5 Preview
SSID *
ThisIsWIFI
Description
PSK Wi-Fi WLAN
Enabled
Broadcast SSID
MAC Access Control
Mesh Link
Authentication
WPA2-Personal
Pre-shared Key *
Mode:
Single
Simple MPSK
MPSK
Captive Portal
No Captive Portal
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)
Next
Copyright © 2022 Fortinet, Inc. All Rights Reserved.
Terms of Service | Privacy Policy | GDPR
Version: v22.3_0319

Configure an SSID with 802.1X/RADIUS for Fully Authenticated Users

WPA-Personal is called ‘personal’ for a reason: it is simple, easy to implement, but really intended for home use or otherwise for environments with a few, trustworthy individuals. Although FortiLAN Clouds MPSK feature adds much needed flexibility and security, the ideal is to have a full database of user that they authenticate to, individually. This is WPA-Enterprise authentication.

There are multiple RADIUS implementations in the real world, with possibly the most common one Microsoft Active Directory with Microsoft Network Policy Server. Online RADIUS implementations have been common, and of course there are numerous non-Microsoft flavors.

If you already have such an authentication scheme, you should use it. You simply have to configure it in FortiLAN Cloud before using it in the SSID definition. If you do not already have a database of users, yoiiu can easily create one in FortiLAN Cloud and use that as the RADIUS service.

Configure a Guest SSID with FortiLAN Cloud Captive Portal

Guest networks are common, of course. With FortiLAN cloud, there ae multiple options to choose from, depending on your goals. Keep in mind, the trivial case for Guest Access is to simply have an open or PSK SSID, matching the above configurations. Beyond those options, guest network options are driven by the choice of how a captive portal operates. Captive portal options in FortiLAN Cloud include the following.

None – Simply allow guests to use an open or PSK WLAN

My Captive Portal – is for the case where you wish to create your own captive portal, beyond the customization available with FortiLAN Captive Portal. See the FortiLAN Cloud user Guide for this case.

FortiLAN Cloud Captive Portal – uses the integrated Captive Portal options included with FortiLAN Cloud. Multiple sign-in methods are supported, and are generally customizable.

- Click through
- My RADIUS Server
- FortiLAN Cloud User Group
- Self-Registered Guests
- Social Media

Each option is described in more detail below

FortiLAN Cloud WLAN Configuration is Complete

This design has been validated in real world environments and should serve well for any single office or widely distributed enterprise. Further, these configurations can be repeated and adapted across multiple customers of a Service Provider.

In many ways, this design can be considered a baseline, and only scratches the surface of Networking and Cyber Security possibilities available with Fortinet's Security Driven Networking Architecture. As your needs and design goals evolve, please see other Fortinet documentation found in the Appendix.

Appendix

This appendix describes additional reference information for FortiLAN Cloud.

Appendix A: Products used in this guide

The following product models and firmware were used in this guide

Product	Model	Firmware
FortiAP	U431F	6.2.3
FortiGate Cloud	n/a	22.

Appendix B: Documentation References

This appendix describes the following.

4-D Documents

- All 4-D Wireless Resources

Solution Hub

Refer to the following FortiLAN Cloud documents.

FortiCloud

FortiLAN Cloud User Guide

www.fortinet.com