DEFINE • **DESIGN** • DEPLOY • DEMO

WPA3 + 6GHz Design Migration

Wi-Fi 6 + 7 Design and Planning Guide

Version 7.4.0

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

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

Nov 30, 2023
WPA3 + 6GHz Design Migration Planning Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-11-30	Initial release.

Introduction

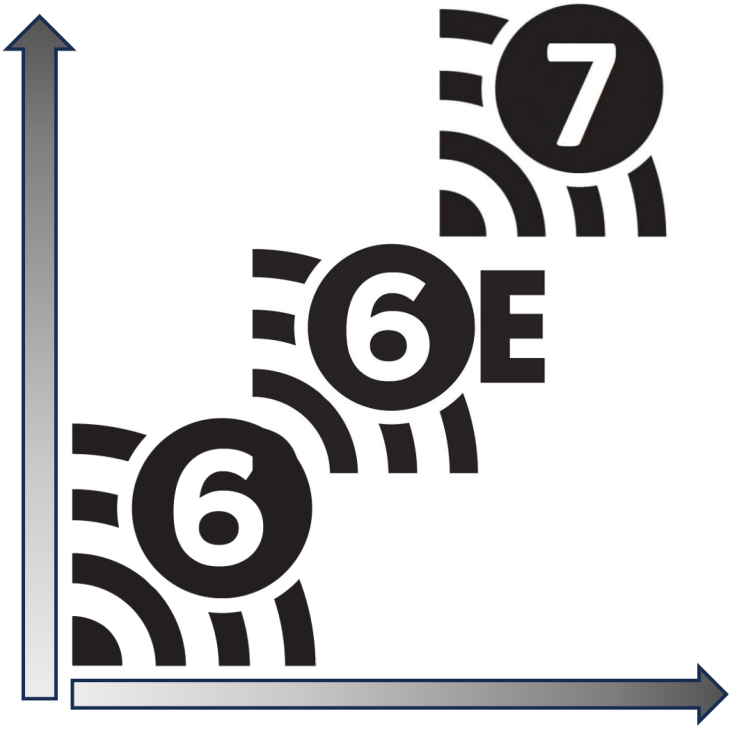
Executive Summary

Migrating a network from earlier versions of Wi-Fi to Wi-Fi 6/6E or Wi-Fi 7 involves increased complexity compared to other recent upgrades. All Wi-Fi planning must start with the question "*what are the clients that need to be supported?"* Compared to previous versions, Wi-Fi 6/6E + 7 introduces new functions at both the software and hardware level. It's essential for network administrator to understand that not all clients will be fully up to date and support the latest technology.

Wi-Fi 6 introduces significant security improvements, primarily WPA3—which is also part of Wi-Fi 7. Clients may have out-of-date software and require upgrading while older clients may not have available updates for WPA3 security. Finally, 6E and 7 utilize channels in 6 GHz, greatly expanding the capacity of Wi-Fi, but that requires new hardware and older clients will not be able to take advantage of these new channels. The new security and channel options will likely mean that SSID strategies will be more complex, with specific SSIDs for different bands and security combinations, or at least differences between 6 GHz vs 2.4 and 5 GHz.

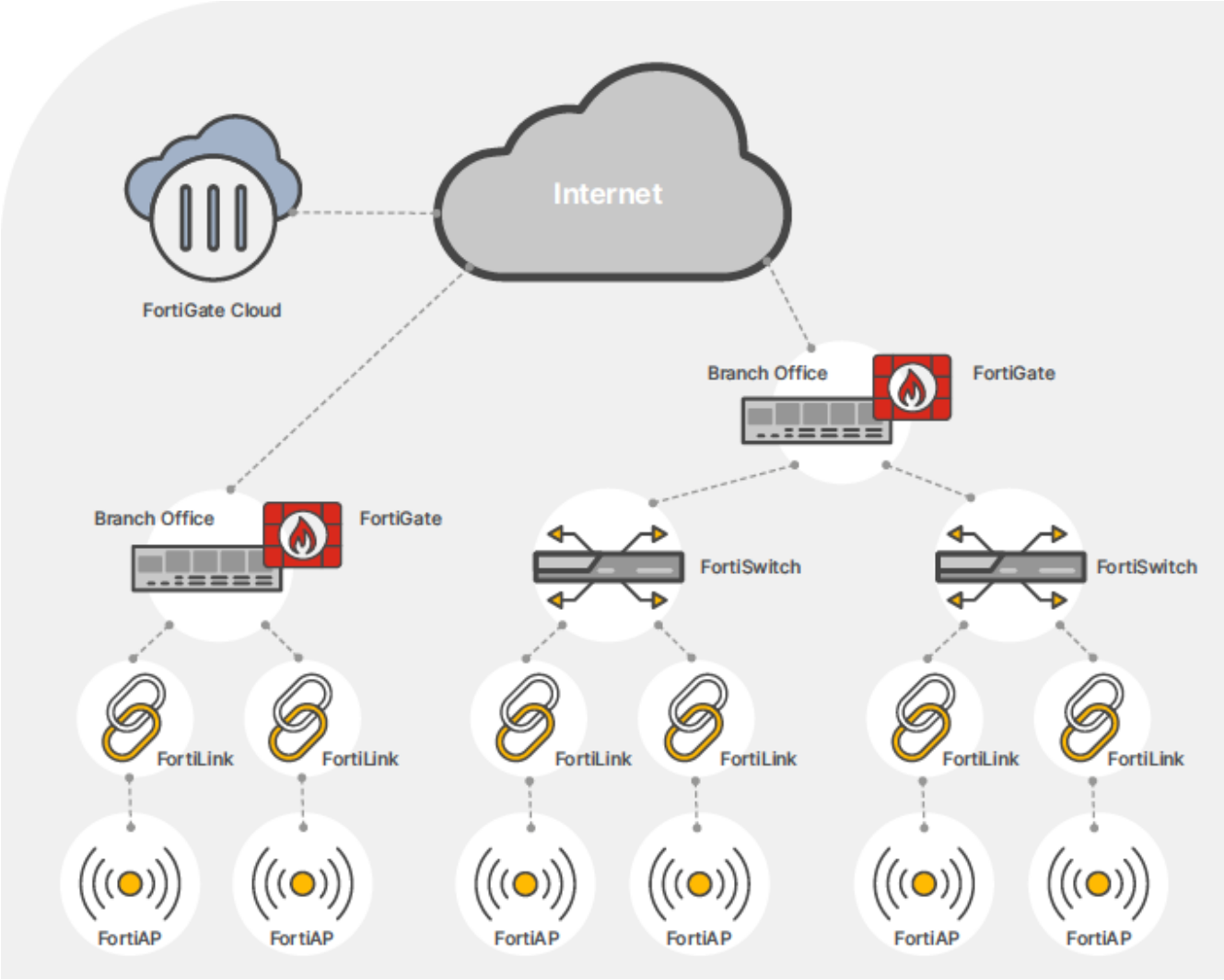
Wi-Fi 6 and 7 introduce several features aimed at improved performance, higher density, and co-channel coexistence. However, the majority of these improvements operate in the background and do not change the basic setup and administration. Two areas that significantly affect configuration in typical environments are: 1) WPA 3 + other improved security 2) 6 GHz channels available with 6E and 7.

The Wi-Fi 6E and 7 channels in 6 GHz add an enormous amount of capacity, more than double 5 GHz and 2.4 GHz combined. However, they only support updated WPA3 and SAE, which can complicate SSID planning. Distributing the various iterations of security and band accessibility is where the additional complexity comes from.



WPA3 and 6 GHz Design and Migration Checklist

- The FortiAP G series have three Wi-Fi service radio APs, providing 2.4, 5, and 6 GHz coverage.
- 6 GHz channels of Wi-Fi 6E and 7 add a massive amount of new capacity, but requires new 6 GHz capable radios.
- Wi-Fi 6 introduces WPA3, which is the biggest security difference for planning and administration.
- The 6 GHz coverage area is only a slightly less than that of the 5 GHz band.
- More and faster radios typically require more power, while faster speeds require Multi-gig Ethernet.
- SSID strategies often need to change from using the same SSID and security across all bands, to band/WPAx specific configurations.



Intended Audience

This guide is intended for an audience interested in learning about and administering Fortinet Wireless LAN networks. 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 factors of concern when moving from a Wi-Fi 5 (or earlier) network to Wi-Fi 6, 6E and 7. It assumes a familiarity with Wi-Fi basics and existing Wi-Fi networks in general, and Fortinet Secure Wireless Networking in particular. Additional Fortinet Wi-Fi design and deployment information can be found on the Fortinet Documents site under *Best Practices* > *Wireless* or at https://docs.fortinet.com/4d-resources/Wireless.

Wi-Fi Clients Analysis and Planning

It's important to note that Wi-Fi devices and most network devices are not all the same. Meaning that they often differ in capabilities from one Wi-Fi generation to another, and need to be classified in security groups based on who uses them and what their functions are.

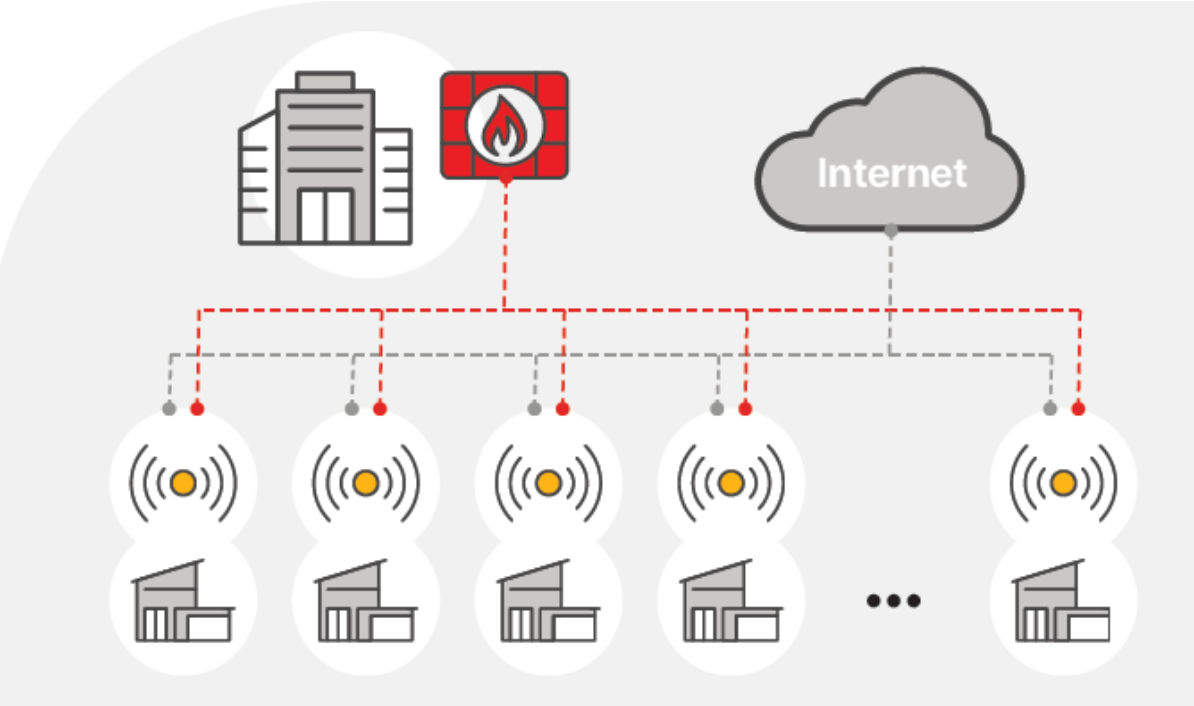
Devices issued by IT, such as laptops, can be tied to specific users with specific access control roles and to known Wi-Fi generations/capabilities.

End user owned BYOD (Bring Your Own Device) are a necessity in nearly all modern WLANs, but are inherently less secure and more uncertain as to what they can be expected to do. Guest access may have to account for a wider range of Wi-Fi generations, depending on how accommodating the network needs to be.

IoT (Internet of Things) devices are characterized by *not* being associated with a particular user. User-owned devices tend to migrate to the latest and technology much faster than connected thermostats, wireless door locks, or conference room video systems. Even when IoT devices support the newest Wi-Fi, they often only support WPAx-Personal, and not WPAx-Enterprise. If the goal is to move end-users to WPA3-Enterprise security (as it should be) IoT devices will frequently need their own SSIDs with additional security isolation via FortiLink NAC, VLAN isolation, etc.

Note that this document will not go into depth on Layer-3 and above security isolation as it is focused on Wi-Fi, a Layer-1 + 2 technology, but higher layer security should be part of the planning process—refer to other Fortinet documentation as appropriate.

When planning a Wi-Fi migration, the devices to support must be categorized not only by device capabilities and user needs that affect security, but also by the likely upgrade path of those users. Laptops and smartphones are probably going to cycle faster than the Wi-Fi infrastructure; generally, 2 years for laptops and phones, but commonly 3-5 years for APs.



Example scenarios

- Employee company issued laptops: IT has full control over security software such as Antivirus and FortiClient. All the laptops support WPA3, some already support 6 GHz channels, and they are likely the highest priority devices.
- Employee smartphones: Mostly leaning into the newest technology, but with less security control and perhaps lower priority.
- IoT devices: Perhaps operations has just rolled out connected door locks that support 5 GHz Wi-Fi but do not support 6 GHz channels, so the foreseeable network will have to support 5 GHz. Or, quite frequently, they only support 2.4 GHz.

Finally, you need to consider how density will be affected when evaluating clients. A university lecture hall may have to support many simultaneous devices that tends to use the newest technology, while a K-12 school district may have Chromebook carts that use Wi-Fi 5 and requires support for several more years. A great part of migrating to Wi-Fi 6 or 7 in these cases is that much of the improvements are aimed specifically at higher Wi-Fi densities, so any high-density areas of an existing network should not need to be fundamentally redesigned. Channel planning for 6 GHz will be discussed later.

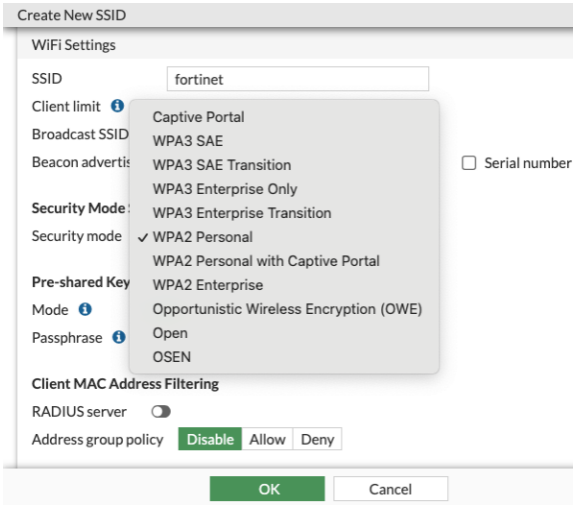
In conclusion, whether migrating to a new Wi-Fi generation or deploying a green field in a new building, you must be very clear about your network needs. Next, this document will delve into the options available in Wi-Fi 6/6E/7 and return to client analysis after.

WPA3 and Other Wi-Fi 6/6E/7 Security Improvements

WPA3 is required by the Wi-Fi Alliance for Wi-Fi 6 and 7 certifications, so all Wi-Fi 6 and 7 certified devices support it. WPA3 improves on WPA2 and offers some transition modes where a single SSID supports corresponding WPA3 and WPA2 devices. These security improvements should not be noticed by end-users and their experience should remain the same in WPA2 and WPA3.

From an end-user point of view, there are three ways to connect to a Wi-Fi network:

- **WPA3-Enterprise or WPA2-Enterprise:** The user connects using *username/password* (or a certificate). This is usually the answer to "What's my network logon?"
- **WPA3-SAE or WPA2-Personal:** The user enters a Pre-Shared Key (SAE is subtly different from PSK, but that doesn't matter for our purposes). Usually, everyone uses the same key (MPSK is discussed later). This is usually the answer to "What's the Wi-Fi password?"
- **Open Network:** The user just joins the network. Traffic is unencrypted at Layer-2 over the air. Wi-Fi 6 and 7 introduce *Enhanced Open* so that OTA traffic is encrypted from the client to the Access Point even though users are not authenticated. Note that Fortinet is focused on *security*, so by default, open SSIDs are not an option unless you specifically enabled that option from *System > Feature Visibility > Wireless Open Security.*



WPA-3 Enterprise is what all known users should be using. "Known users" are regular network users and there is a database of those users such that their security identity can be individualized. From the administrative and the end-user experiences, this is identical to WPA2-Enterprise. It is 802.1X based security, and a large organization should have the infrastructure for this. Even a small organization with a FortiGate managing the Wi-Fi can have the FortiGate serve as the user database, or they can use FortiAuthenticator. This is hopefully how the Wi-Fi has been secured all along, by using WPA2-Enterprise and taking advantage of all the additional cybersecurity and network isolation that a FortiGate offers. Detailed discussion of that subject can be found in other Fortinet documents.

Advantages of WPA3 Enterprise

So why migrate to WPA3-Enterprise if it is the same as WPA2-Enterprise? While WPA2-Enterprise remains quite secure, cyber-security is not static, and known and zero-day threats are constantly evolving. WPA3 introduces *Management Frame Protection* (MFP) which encrypts the management frames the same way data frames have always been encrypted. MFP allows the wireless network to resist De-authenticate and Disassociate attacks. In a WPA2 protected network, an attacker can potentially spoof the AP (or the client) and inject de-authentication or disassociation frames. This could simply be a Denial of Service (DoS) attack, or it could be part of a honeypot attack—knock the client off the network and use a common public hotspot SSID to lure the client to the wrong network. With MFP encryption, this attack is no longer possible. In the case of WPA3-SAE, MFP provides resistance to offline dictionary attacks on the passphrase via unique encryption for each client.

WPA3-Enterprise has three supported modes on an SSID/WLAN:

- **WPA3-Enterprise Only**, which requires all clients to be WPA3 capable. Often even older clients can connect over WPA3 with a driver update, so client testing is recommended. Use this if the clients support it.
- **WPA3-Enterprise Transition** allows both WPA2-Enterprise and WPA3-Enterprise on the same SSID. The WPA3 capable clients use MFP, but the WPA2 clients receive unencrypted management frames. If this mode is necessary, do not forget to revisit it in the future. Client updates continue to move the client base to WPA3 capable, so we suggest setting a calendar reminder to re-evaluate it every six months.
- **WPA3-Enterprise 192-Bit** is an optional mode for particularly sensitive environments. Data encryption is increased from 128-bit to 256-bit and EAP-TLS is used for authentication. As it is optional, client support may be less common, and it may be excessive in most enterprise environments. It is only available on FortiOS via CLI.

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

Advantages of WPA3-SAE

WPA3 SAE (Simultaneous Authentication of Equals) is the update for WPA2-Personal. While it was originally intended for home use and should be avoided in a FortiGate secured network for the primary users, it can still be useful for a variety of devices that the WLAN may have to support. IoT or consumer-oriented devices, like streaming TVs, often lack support for WPAx-Enterprise. Even if they do, adding username/password combinations for possibly many IoT devices may prove impractical due to overhead, internal procedures, or RADIUS database management.

WPA3-SAE improves both authentication and encryption compared to WPA2-Personal while maintaining the same user experience.

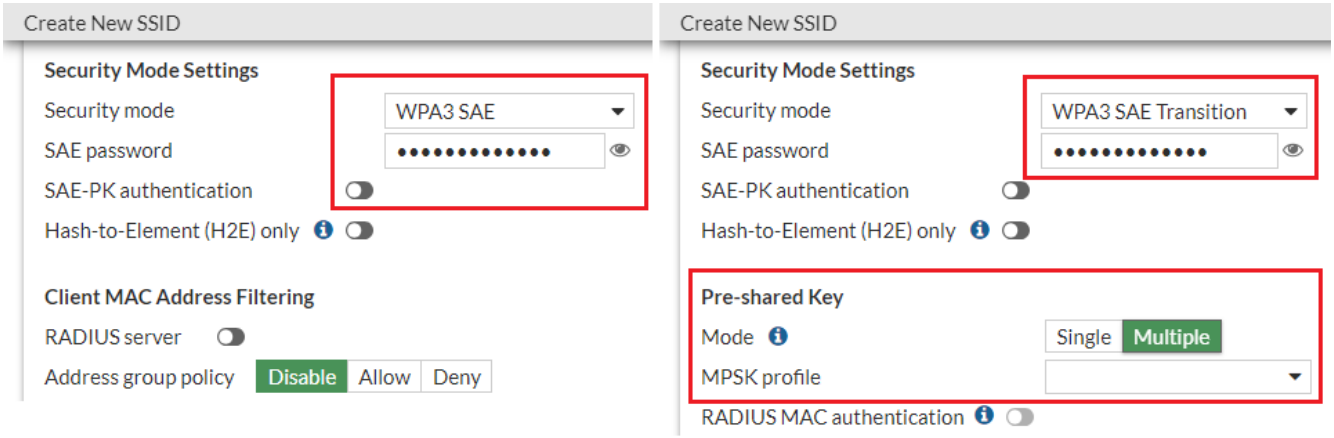
The WPA2-Personal mechanism uses a Pre-Shared Key (PSK) both as the authentication mechanism (requiring the client device to 'know' the key) and the encryption key (requiring every device to use the same encryption key).

The WPA3-Personal mechanism uses the passphrase to generate unique keys for each session. The passphrase itself is never sent, even encrypted, over the air. This mechanism is known as *Simultaneous Authentication of Equals* (SAE), based on the Dragonfly key exchange. MFP is enabled, every client has a unique key, and the keys are periodically updated. SAE is a significant improvement over PSK.

WPA3-SAE has two supported modes on an SSID/WLAN:

- **WPA3 SAE**, which requires all clients to be WPA3 capable. Often, even older clients can connect over WPA3 with a driver update, so we recommend client testing. Use this mode if your clients can support it.
- **WPA3 SAE Transition** allows both WPA2-Personal (PSK) and WPA3-SAE on the same SSID. The WPA3 capable clients use MFP, while the WPA2 clients receive unencrypted management frames. If this mode is necessary, do not forget to revisit it in the future. Client updates continue to move the client base to WPA3 capable devices, so we suggest setting a calendar reminder every six months to re-evaluate your needs .

One downside to WPA3-SAE is if your network already uses *Multiple Pre-Shared Key* (MPSK) since the SAE mechanism breaks what enables MPSK. Although multiple vendors have enabled something like Fortinet's MPSK, it has never been part of the Wi-Fi standard. MPSK and similar technologies are something of a loophole in WPA2-personal PSK, although a very useful loophole. However, Fortinet also supports *WPA3 SAE Transition.* Transition supports both WPA3 SAE clients and WPA2-PSK (including MPSK) clients. You can continue to support MPSK clients, while allowing clients that use the SAE password on the same SSID for the improved encryption and MFP features.



MPSK reduces the over-the-air threat by providing multiple encryption keys on a single SSID, so it is more secure than WPA2-Personal. An MPSK utilizing WPA2 SSID can remain a good strategy for such devices as long as you are using additional upper-layer mechanisms such as FortiLink-NAC, a good VLAN isolation strategy, and well-defined firewall policies.

Even though the general recommendation is to move to WPA3 whenever possible, the strategies outlined above make it a wise choice to continue using WPA2-Personal with MPSK (or WPA3-SAE transition) for IoT devices in order to take advantage of MPSK.

Again, this document is not meant to cover higher layer security mechanisms in depth. One of the most common and best uses of MPSK is with IoT devices that are placed in a specific VLAN via SSID or FortiLink NAC, secured using a firewall policy, and only allowed to communicate with their reporting server, whether local or on the Internet.

Advantages of OWE

OWE (Opportunistic Wireless Encryption) or ***Enhanced Open*** is not actually part of WPA3, but it is an optional part of Wi-Fi 6 for public access networks. From an end-user point of view, it behaves exactly like any open Wi-Fi SSID. However, 'open' previously meant both no authentication (any device can connect) and no privacy, or no over-the-air encryption of the data. Of course, encryption can take place at a higher network layer, such as IPSec VPN or an https web page, so the local coffee shop has been a reasonably secure place to do some work.

OWE lacks authentication by design as it is meant for public networks. However, it does add over-the-air encryption so that client to FortiAP traffic is private, and management frames are also be encrypted (MFP). Unique encryption keys are generated for each session in a similar fashion as SAE, mitigating any possible eavesdropping. This is an improvement to public Wi-Fi but should only be used in public networks. While Enhanced Open is more secure for users in retail operations or in public spaces, it should not be used for a private network.

Although OWE Enhanced Open vs Open is completely transparent to an end user, only Wi-Fi 6 + 7 devices will support it and client support may be spotty because it is optional. Also public access spaces will find it necessary to support the oldest devices the longest. A fast-food chain with no onsite IT staff may find it excessive to try to move to Enhanced Open for some time.

Enhanced Open has two supported modes on an SSID/WLAN:

- **OWE (Enhanced Open)** has no authentication mechanism but encrypts both data and management frames. Again, supporting clients are required.
- **OWE (Enhanced Open) Transition** provides backwards compatibility, although the mechanism is surprisingly complex. When a transition SSID is created, an additional hidden SSID is also created. OWE capable clients learn of the hidden SSID from information elements in the broadcast SSID and steer to it while the OWE incapable clients simply connect to the open broadcast SSID. The second SSID is hidden to avoid confusing legacy drivers and end users.

  Note that on FortiGate, OWE Transition must be configured via CLI.

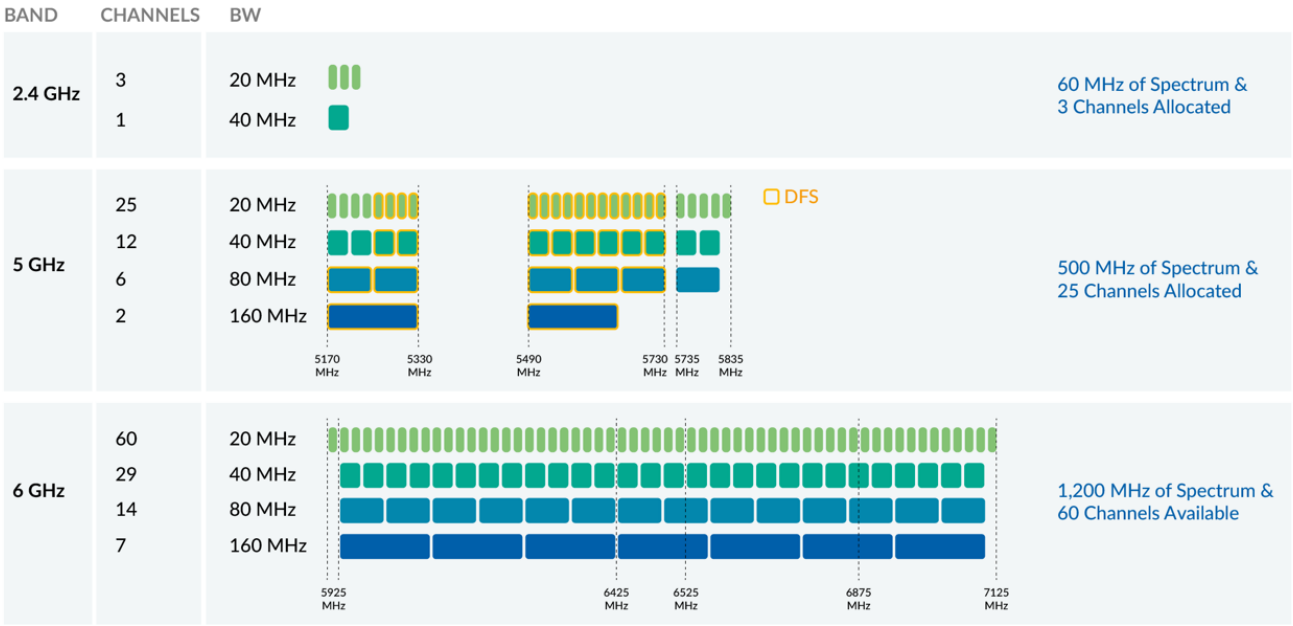
Wi-Fi 6 + 7 security enhancements can be summarized as improvements to encryption and denial of service attack resistance via MFP. Management Frame Protection is added to the three existing security levels: Enterprise class (802.1X), Personal/SAE, and open networks (OWE). There are also privacy (encryption) improvements for all levels as well.

One additional issue to be aware of is that 6 GHz channels are *not* backwards compatible because no previous devices supported those channels. There are no Wi-Fi 5 and lower devices that can connect to any of the 6 GHz extended channels. However, the SSID scheme for a given location may get more complex moving across 2.4, 5, and 6 GHz channels if, as is likely, a mix of security settings is needed. At the least, IT cannot deploy the same WPA2 SSID across all three bands.

6 GHz Channel Planning

Wi-Fi 6E adds only one thing to Wi-Fi 6: additional channels in the 6 GHz spectrum. These additional channels are also part of Wi-Fi 7 and provide an excellent long term improvement. The 6 GHz band adds 1200 MHz of spectrum (sixty 20-MHz wide channels) to Wi-Fi, more than doubling the potential capacity of a Wi-Fi network. Having more channels solves lots of problems, and this is the future. However, because the 6 GHz channels use new radio frequencies they are not backwards compatible with previous Wi-Fi technologies.

To make the advantages clear, we'll briefly cover Wi-Fi history and channel planning:



There is no technical reason for Wi-Fi to use the channels it uses. The channels used are because of government regulations, particularly the FCC in the United States, although there are differences in other regulatory domains. Wi-Fi uses unlicensed, but not unregulated, radio frequencies. Licensed frequencies are used by entities such as radio, TV stations, and mobile phone operators, who have exclusive rights (license) in an area to use those frequencies.

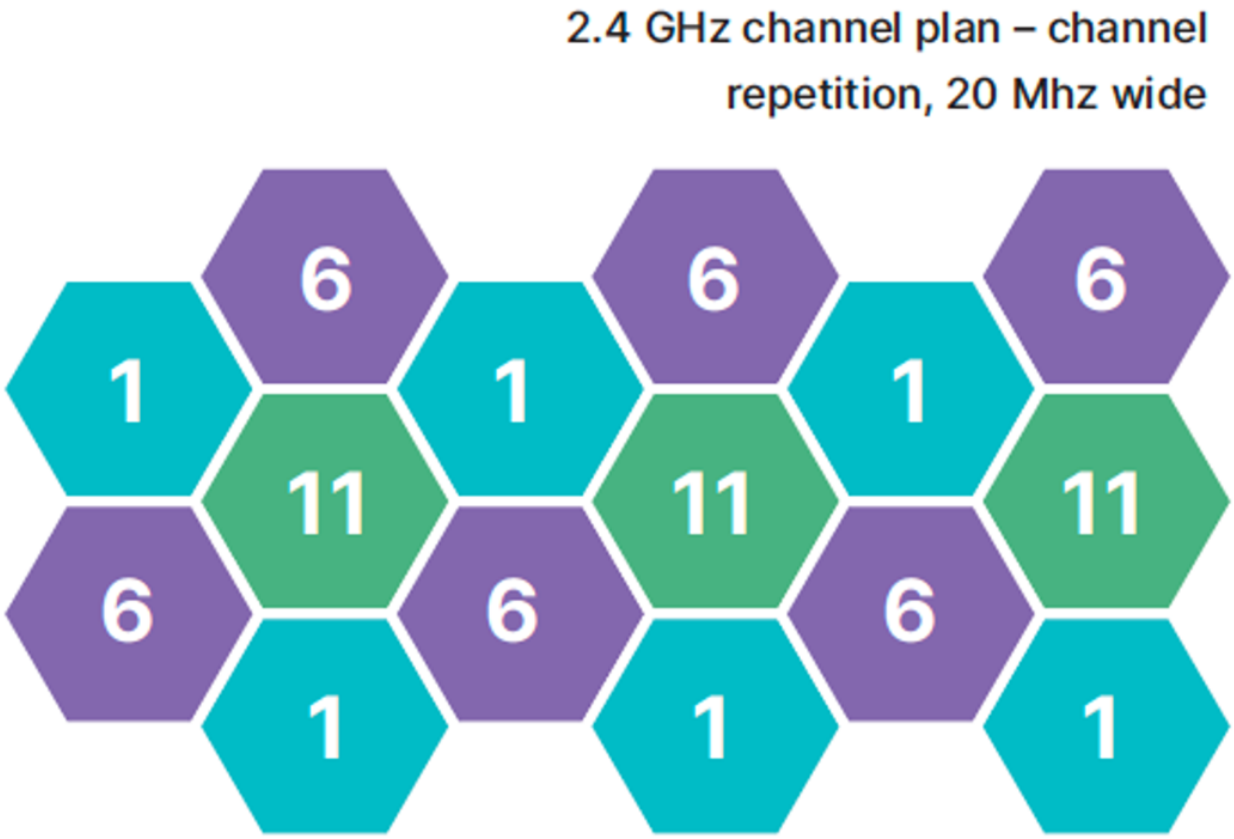
Unlicensed frequencies can be used by anyone and any emerging technology, although they are still regulated, mostly as to their maximum signal strength. Compare a 50,000-Watt (W) radio station to a 200 milliWatt (mW) Wi-Fi access point. The radio station may cover many square miles of area, meanwhile an AP typically covers around 1000-2000 sq ft. The same AP channel can be used by another AP and, if they are far enough apart, there will be no signal interference between the two.

Wi-Fi users do not have to license their spectrum and can trust that equipment from vendors such as Fortinet to operate within all applicable regulations.

By default, FortiGates are set to the US regulatory domain by default, so it is important for users outside of the US to set the country code correctly on the FortiGate that operates as a WiFi & Switch Controller.

Differences between Bands + Wi-Fi Evolution

The biggest limitation on Wi-Fi performance is the number of channels available. Each generation adds signal processing improvements, improved overhead management, and related technologies. However, Wi-Fi fundamentally works like walkie-talkies—only one radio can use the channel at a time, whether an AP or a client. The 2.4 GHz band has three Wi-Fi channels (which must be 20 MHz wide), which is the bare minimum for a 'cell' plan—where no adjacent cells use the same channel.



2.4 GHz band

The design problem with an entirely 2.4 GHz WLAN and only three channels is that APs on the same channel must be far enough apart that they can 'talk' at the same time. Worse, even if the APs themselves have enough separation, the clients at the edges of those cells may be too close together and interfere. The greatest interference source for modern Wi-Fi networks is self-interference by the WLAN itself. 2.4 GHz also suffers from interference from other technologies. Microwave ovens, baby monitors, old cordless land-line phones are all problems, but the biggest current external problem now is Bluetooth, which also uses 2.4 GHz.

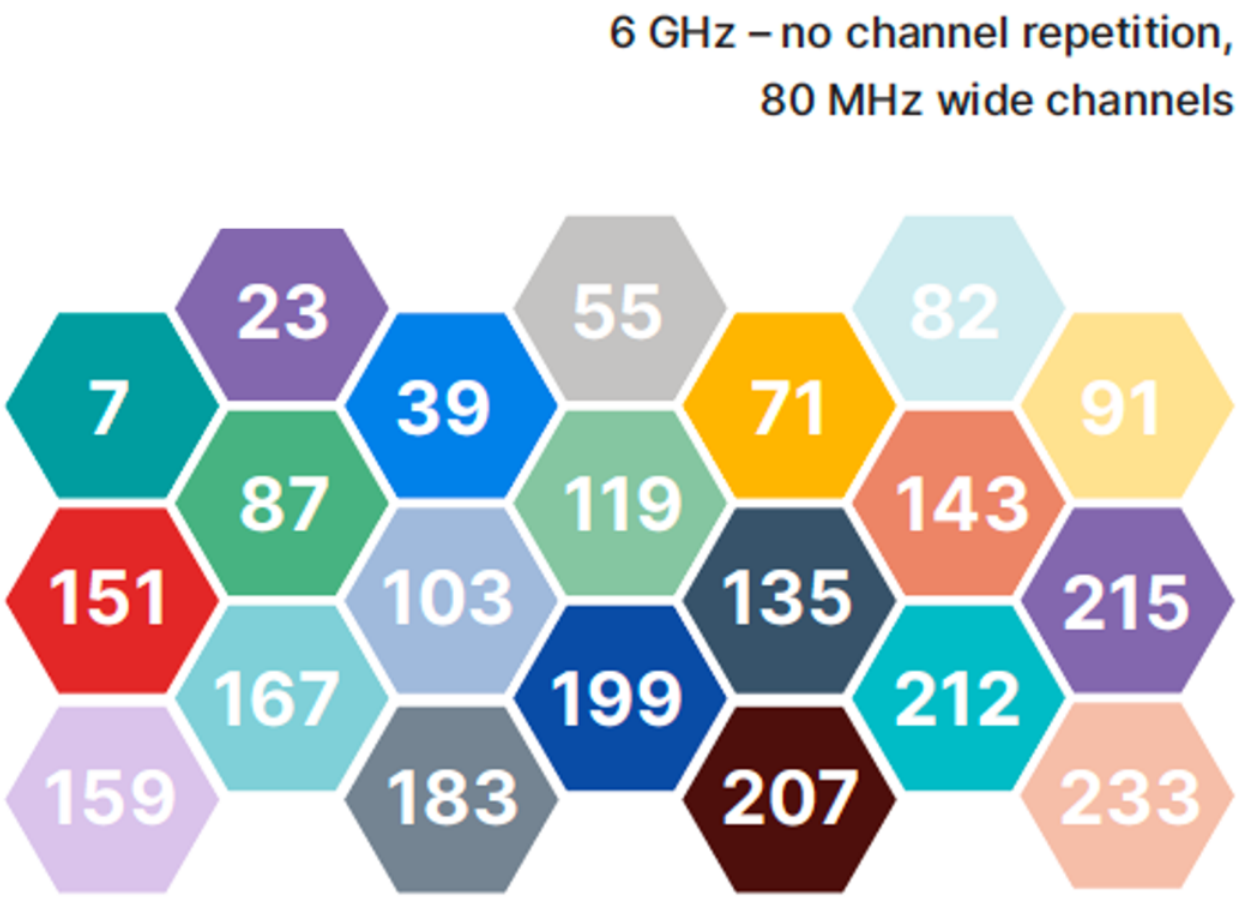
5 GHz band

5 GHz added nine channels initially, then a total of 25 with *Dynamic Frequency Selection,* which enables an AP to recognize and avoid channels that may also have airport radar. With those extra channels, *channel bonding* becomes

useful. Channel bonding enables a single radio to use more spectrum for more throughput. 5 GHz is almost always deployed as a 40 MHz wide channel, which doubles the possible throughput, and can reasonably be 80 MHz wide (4X throughput) when making full use of the DFS channels. Six 80 MHz wide channels enable both high throughput networks and a much more flexible channel re-use pattern for reduced self-interference. There is also considerably less non-Wi-Fi interference in 5 GHz. 5 GHz does not penetrate walls as much as 2.4 GHz, but as Wi-Fi moved from a convenience to a daily necessity, that helped with reducing self-interference. APs are rarely used to cover as large an area as in the past, with emphasis typically on higher performance, rather than maximum coverage area. Non-Wi-Fi interference is very rare in 5 GHz, with no major competing technologies.

6 GHz band

6 GHz channels are allowed because of new regulations from governing agencies. For example, the FCC in the US allows sixty 20 MHz wide channels. Other jurisdictions may have fewer channels, but the full set is more than double the capacity of 2.4 and 5 GHz together. There are seven 160 MHz channels, and there will be the option of three 320 MHz channels with Wi-Fi 7. The more non-repeating channels available, the more forgiving channel planning is. In a Fortinet system, such planning can largely be left to Fortinet's Distributed Automatic Radio Resource Provisioning (DARRP). This is a substantial increase in Wi-Fi capacity and a direct, government supported acknowledgment of how important Wi-Fi has become.



However, the problem with migrating to 6 GHz is the same one that follows every Wi-Fi generation: client catchup. To reiterate, you must know what devices make up your clients. The client capabilities you must support will affect your planning. The great news is that the current FortiAP Wi-Fi 6 are ideal for this transition. They have three client servicing

radios so that they can support clients across all three bands. This is excellent future proofing—even if there are few 6 GHz clients to support today, there will be more in the future. Channel planning is always simpler with more channels.

Coverage Areas (Cell Sizes)

5 GHz is famous for having smaller coverage area than 2.4 GHz. However, 6 GHz frequencies are much closer to 5 GHz than 5 GHz is to 2.4 GHz—20% greater instead of 200% greater. Generally, a higher frequency results in reduced coverage area, mostly because of reduced wall penetration, but 5 and 6 GHz frequencies are close enough that a conservative 5 GHz design should also work for 6 GHz.

Old habits from a 2.4 GHz only network are difficult to break, but the greater number of channels available in 5 and 6 GHz, among other design considerations, also mean cells can be smaller and designed for performance and density because it will take so many more FortiAPs until a channel needs to repeat. 6 GHz is also nearly empty of non-Wi-Fi interference, even more than 5 GHz, which does have to concern itself with radar/DFS channels.

Because the coverage areas are larger, and there are only three channels, 2.4 GHz will have more self-interference. However, good client strategy can mitigate this. End user laptops and high-performance wireless devices belong on 5 and 6 GHz. Low performance devices, such as IoT Wi-Fi devices only need to deliver small spurts of data. Using the WLAN in short bursts results in less interference as they just don't take up much airtime. If a 6 GHz dead spot creeps in, 2.4 GHz can serve as a backup in that location—perhaps a closet that the Wi-Fi site survey missed.

Of course, a site survey is always recommended, but design for 5 and 6 GHz to be used by phones, laptops, and tablets. Meanwhile low data IoT clients can be regulated to 2.4 GHz.

SSID Strategies

Initially, the introduction of 5 GHz on top of 2.4 GHz generally resulted in the strategy of deploying the same SSID/WLAN on both bands and letting a mix of client behavior and controller band-steering distribute the clients. This was possible because of identical security standards on each band—WPA2. However, that strategy will not work on three bands with 6 GHz unless *all* devices support WPA3, a very unlikely situation for a network of any complexity. More SSIDs will be needed.

2.4 GHz only devices are seeing more use in the form of IoT devices, which have similar needs—they must be cheap (favoring 2.4 GHz) and they get placed in less accessible places (also favoring 2.4 GHz). Fortunately, they tend to deliver only small amounts of data and individual devices do not use a lot of bandwidth. On a security level, they have a longer replacement cycle and often only support WPA2-Personal/PSK.

- For Wi-Fi IoT, generally use a 2.4 GHz only SSID, with WPA3-SAE transition and most likely use MPSK. Test these devices first as WPA3-SAE transition may confuse them. If they have problems, fall back to WPA2-PSK, using MPSK. Take advantage of higher layer FortiGate functions such as FortiLink NAC, VLAN isolation, and targeted firewall polices.

For laptops, phones, tablets, and other higher performance end user devices:

- If they support 6 GHz (6E or 7) they will also support WPA3-Enterprise. Create a high performance 6 GHz SSID for these devices.
- 5 GHz will likely have to support WPA2, so use WPA3-Enterprise Transition. Non-6 GHz radios will not see 6 GHz, but until you have completed a complete switchover to FortiAP G series or later, even 6 GHz users will probably utilize 5 GHz in some areas.
- Treat 2.4 GHz as a backup—so do *not* have identical SSIDs! Make it clear which band is being offered.

Examples SSIDs

- "Mycompany-6GHz" with WPA3, Enterprise or SAE.
  - Only WPA3 capable devices will be able to use 6 GHz, and other devices will not see the SSID. This makes it clear for users with 6 GHz capable devices and will help migration.
- "Mycompany-5GHz" with WPA3-transition and "Mycompany-2.4GHz" with WPA3-transition
  - Or use the traditional approach of having the same WLAN settings, "MyCompany" with WPA3-transition, on both bands. It will depend on your goals and environment.
- "Mycompany-IoT"—in 2.4 GHz, with MPSK

The examples above are merely suggestions. Details depend on the needs of the specific environment, which can be discovered by analyzing the clients involved.

Infrastructure Needs: Site Surveys, Multi-gigabit Switches + PoE

Site Survey

A wireless site survey is always necessary when making changes to a WLAN, and although 6 GHz is similar to 5 GHz, it is not identical. When deploying FortiAPs, we always recommend leaving significant slack in the Ethernet cable. Wi-Fi coverage can often be improved by moving an AP a few feet further away from an air-conditioning duct.

PoE and switching that suit your needs will also be required. Multi-gig switches with high PoE output will maximize the capacity of Wi-Fi 6 and 7 FortiAPs. However, switch upgrades and wireless upgrades often do not happen at the same time, so they are designed to run at a variety of power levels and Ethernet speeds. You can also consider using power injectors and PoE midspans.

Current Wi-Fi 6 FortiAPs

FAP-431G/433G – Two 5 GE ports, *bt* or Dual *at* Power

- Wi-Fi 6E
- Tri-Radio 2.4 + 5GHz + 5GHz / 6GHz / Scanning
- 4x4 MU-MIMO
  - Up to 1148 Mbps + 2402 Mbps + 4804 Mbps
- Ethernet:
  - x2 100/1000/2500/5000 Base-T RJ45
- Power modes
  - One 802.3bt PoE default
  - Two 802.3at PoE (Dual PoE current sharing)
  - One 802.3af : Low – All Radios Disabled ; USB – Disabled
  - One 802.3at : Low – Tx Power 17dBm ; Chain 4x4; USB – Disabled
  - One 802.3bt / DC: Full – Tx Power Full ; Chain 4x4;USB – Enabled

FAP-231G/233G – One 2.5 GE + One GE ports, *at* Power

- Wi-Fi 6E
- Tri-Radio 2.4 + 5GHz + 5GHz / 6GHz / Scanning
- 2x2 MU-MIMO
  - Up to 574 Mbps + 1201 Mbps + 2402 Mbps
- Ethernet:
  - one 100/1000/2500/5000 Base-T RJ45 +
  - one 10/100/1000 Base-T RJ45
- Power modes
  - One 802.3at PoE default

- 802.3af: Low – Tx Power limited to 17 dBm; Radio3 – Disabled ;USB – Disabled
- 802.3at / DC: High/Full – Tx Power Full; USB – Enabled

Conclusion

With Fortinet's 4x4 FAP-44xG and 2x2 FAP23xG series Wi-Fi access points, migration to Wi-Fi 6 + 6E is straightforward from a multi-band or future proofing point of view. The three services radios cover all three bands—2.4, 5 and 6 GHz—simultaneously, and 6 GHz coverage is very similar to 5 GHz. Migrating to WPA3, which is required for 6 GHz, can complicate SSID strategies and will likely require band specific SSIDs. Supporting Ethernet switching and PoE also needs to be evaluated to maximize the benefits of the G series, although there are multiple options for less than bt PoE. Always plan with your current and future client strategy in mind, grouping devices by radio and security capabilities and needs.

Appendix A: Documentation References

Feature Documentation

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

Solution Hub

- FortiGate Cloud Solution Hub
- Secure Access Solution Hub

Related 4-D Documentation

- FortiCloud Overview
- Secure Wireless Concept Guide

www.fortinet.com