WPA3

The Next Generation of Wi-Fi Security

Wireless connectivity is a business continuity requirement for most customers. As such, security of networks is a top priority, and with wireless networking celebrating its 20th anniversary, it is clear that the wireless industry recognizes that authentication and encryption protocols must evolve to guarantee the security of wireless communication moving forward. In June of 2018, nearly 14 years since the last update, the Wi-Fi Alliance announced a major security improvement to Wi-Fi: WPA3 (Wi-Fi Protected Access Three). WPA3 is the next generation Wi-Fi security standard that tackles WPA2 shortcomings to better secure personal, enterprise, and IoT wireless networks.

So, what is WPA3?

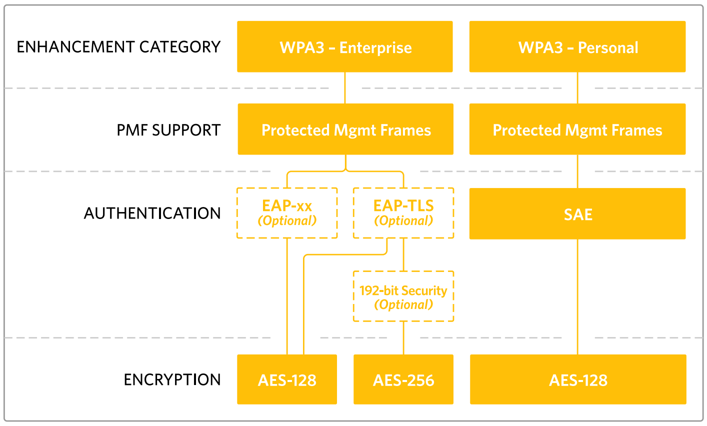
Wireless security is about being one step ahead of the bad guys. WPA3 builds on WPA2 to deliver a suite of features to simplify Wi-Fi security configuration and enhance Wi-Fi network security protections, making Wi-Fi connections safer and helping to save enterprise and home deployments from security shortcomings. It delivers more resilient password-based authentication, providing stronger security protection against password guessing attempts by third parties, and delivers greater cryptographic strength for government, defense, and other security-sensitive environments.

When it was announced in 2018, the Wi-Fi Alliance press release touted two main categories of enhancement:

- **WPA3-Personal:** The most significant changes are being realized within WPA3-Personal, which focuses on more resilient, password-based authentication even when users choose passwords that fall short of typical complexity recommendations. WPA3 replaces PSK with Simultaneous Authentication of Equals (SAE) from IEEE 802.11 specification, a secure key establishment protocol between devices, to provide stronger protections for users against password guessing attempts by third parties.

- **WPA3-Enterprise:** Provides superior security for sensitive data networks with the equivalent of 192-bit cryptographic strength, helpful in industries such as government, healthcare, or finance. The 192-bit security suite ensures a consistent combination of cryptographic tools are deployed across WPA3 networks.

Here is a more visual look at WPA3 announced in this latest update:



This exciting enhancement to the Wi-Fi Alliance standards, while remaining backwards compatible with WPA2, makes many previously-optional components (such as Protected Management Frames) mandatory. Collectively, these aid in securing against eavesdropping and man-in-the-middle type attacks, and provide resistance against both offline dictionary attacks and key recovery. Because WPA3 is resistant to offline dictionary attacks, users can choose (or administrators can assign) passwords that are simpler, easier to remember, and easier to enter, while retaining high security.

WPA3 – Personal Versus Enterprise

WPA3 – PERSONAL

Robust, password-protected authentication

- Resistant to offline dictionary attacks; stronger protections for users against password guessing attempts by third parties
- Protection even when users choose passwords that fall short of complexity recommendations
- Provides forward secrecy; protects data traffic even if a password is later compromised
- No change to the way users connect to a network

WPA3 – ENTERPRISE

Enterprise-grade security for sensitive networks

- Available 192-bit cryptographic strength for networks transmitting sensitive data
- 192-bit security suite provides additional security for networks like government and finance
- Greater consistency in application of security protocols
- Better network resiliency

WPA2 versus WPA3

The big question: is WPA3 really more secure than its predecessor? The answer: Yes, absolutely. The third edition of WPA is a long-awaited and much-welcomed update that improves on WPA2, with more robust authentication and encryption features, and a solution to the built-in flaw in WPA2 that the KRACK attack exploits.

The key WPA2 enhancements:

- Mandates support of Protected Management Frames (PMF), which prevents de-authentication attacks where an adversary can forcibly disconnect clients from a Wi-Fi network and monitor a reconnect.
- Addition of digital certificate test cases to ensure that proper certificate validation checking is performed by station devices.
- RSN Element (RSNE) multiple – AKM suite selector testing validates that client devices can successfully receive an RSNE that includes more than one AKM suite selector.
- Patched against the KRACK attack against WPA2.

Adoption of WPA3

The entire ecosystem of wireless vendors and device manufactures need to embrace WPA3 to make the many enhancements in this release a reality. It will happen in time, just as it did for WPA2. The Wi-Fi Alliance doesn't expect widespread implementation until the latter half of 2019, however with that, the Wi-Fi Alliance believes the backward interoperability with WPA2 will ensure that some added security benefits will be available as soon as the devices themselves are.

In many cases, no changes will be needed in customer configurations to take advantage of WPA3 features. As wireless vendors release software updates with WPA3 capability to existing products, coupled with purchases of new WPA3 certified wireless clients, the miracles of modern networking will just happen. And with the 802.11ax wireless standard beginning to be deployed in networking hardware and software, it only makes sense that those vendors would provide WPA3 compatibility at the same time.

Aerohive WPA3 compatibility has already been deployed

Back in June 2018, Aerohive announced plans for WPA3, and in November, delivered the first part of that promise with SAE support in our HiveManager cloud management platform, along with the release of multiple WPA3 supported devices. Aerohive APs can support and offer the highest level of security available on the client devices. This allows Aerohive to provide the latest levels of security, yet still support legacy technologies while providing isolation between the two groups. Aerohive is fully committed to access network security outside the WPA3 realm, with capabilities including Private Pre-Shared Key (PPSK), full-line rate encryption, integrated TPM chips, fully stateful layer 2-7 firewalls, Private Client Groups, Cloud-Managed NAC (A3), flexible identity-based security, and policy enforcement at the edge of the network.

WPA3 – Device & Product Support

WPA3 CERTIFIED OR SUPPORTED DEVICES

There are WPA3 supported or certified devices available on the market today, with many more being announced weekly. Here are a few examples of devices available:

Enterprise Access Points

- Aerohive
- Aruba
- Dell
- Fortinet
- Netgear
- Ruckus

Wireless Adapters:

- Broadcom
- Intel

Phones:

- LG ThinQ
- Samsung Galaxy S10

AEROHIVE WPA3 PRODUCT SUPPORT

Management

- HiveOS 8.4r7

(this version adds support for SAE)

802.11ax Access Points

- AP630
- AP650
- AP650X

802.11ac Access Points
(Wave 1 and Wave 2)

- Atom AP30
- AP122
- AP122X
- AP130
- AP150W
- AP230
- AP245X
- AP250
- AP550
- AP1130