Certified products, news, etc. SEARCH

Discover Wi-Fi

Security

Wi-Fi® is an integral part of daily life. Billions of people the world over depend on Wi-Fi in their homes and businesses, to shop, bank, coordinate life, and stay connected. Securing Wi-Fi connections is an important element of securing personal data, and Wi-Fi Alliance® has been on the forefront of evolving Wi-Fi security as the number of Wi-Fi devices in use worldwide has grown.

Since 2003, Wi-Fi Alliance has enabled individuals and businesses to increase the protection of information moving across Wi-Fi networks through the Wi-Fi Protected Access® family of technologies. Security features of Wi-Fi Protected Access constantly evolve to include stronger protections and new security practices as the security landscape changes.

The Wi-Fi Protected Access security family includes solutions for personal and enterprise networks.

Wi-Fi CERTIFIED WPA3™

WPA3™ is the next generation of Wi-Fi security and provides cutting-edge security protocols to the market. Building on the widespread success and adoption of Wi-Fi CERTIFIED WPA2™, WPA3 adds new features to simplify Wi-Fi security, enable more robust authentication, deliver increased cryptographic strength for highly sensitive data markets, and maintain resiliency of mission critical networks. All WPA3 networks:

- Require use of Protected Management Frames (PMF)

Since Wi-Fi networks differ in usage purpose and security needs, WPA3 includes additional capabilities specifically for personal and enterprise networks. Users of WPA3-Personal receive increased protections from password guessing attempts, while WPA3-Enterprise users can now take advantage of higher grade security protocols for sensitive data networks.

WPA3, which retains interoperability with WPA2™ devices, is currently an optional certification for Wi-Fi CERTIFIED devices. It will become required over time as market adoption grows.

WPA3-Personal

WPA3-Personal brings better protections to individual users by providing more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE), which replaces Pre-shared Key (PSK) in WPA2-Personal. The technology is resistant to offline dictionary attacks where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

- **Natural password selection:** Allows users to choose passwords that are easier to remember
- **Ease of use:** Delivers enhanced protections with no change to the way users connect to a network
- **Forward secrecy:** Protects data traffic even if a password is compromised after the data was transmitted

WPA3-Enterprise

Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocols across the network.

WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data:

- **Authenticated encryption:** 256-bit Galois/Counter Mode Protocol (GCMP-256)
- **Key derivation and confirmation**: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- **Key establishment and authentication:** Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
- **Robust management frame protection:** 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

The 192-bit security mode offered by WPA3-Enterprise ensures the right combination of cryptographic tools are used and sets a consistent baseline of security within a WPA3 network.

Wi-Fi CERTIFIED WPA2

The WPA2 certification program has continually evolved to meet security needs as the security environment changes. In 2018, Wi-Fi Alliance augmented existing security protections for networks through configuration, authentication, and encryption enhancements. Enhanced validation of vendor security implementations reduces the potential for vulnerabilities due to network misconfiguration and further safeguard managed networks with centralized authentication services.

Since 2006, all Wi-Fi CERTIFIED™ devices implement WPA2.

WPA2 will continue to evolve to meet standards for interoperability and security in all Wi-Fi CERTIFIED devices. WPA2 will be available in Wi-Fi CERTIFIED devices for the foreseeable future, and all devices supporting WPA3 will continue to work with WPA2 devices.

Open Wi-Fi networks

Users access Wi-Fi networks everywhere: at home, in the office, in hotels, shopping malls, transportation hubs, and municipal locations. Accessing unsecured networks in these locations presents a risk that someone could acquire personal data, which is why Wi-Fi Alliance highly recommends users ensure they access secure, authenticated networks whenever possible. However, there are situations where an open Wi-Fi network is the only feasible option. While many consumers worldwide utilize open networks with no issue, it is important to be aware of the risk an open network presents, and to be diligent in protecting user data. To address these risks, Wi-Fi Alliance has developed a solution to benefit users of open Wi-Fi networks.

Wi-Fi CERTIFIED Enhanced Open™ is a Wi-Fi Alliance certification that preserves the convenience open networks offer while reducing some of the risks associated with accessing an unsecured network. Wi-Fi Enhanced Open™ networks provide unauthenticated data encryption to users, an improvement over traditional open networks with no protections at all. These protections are transparent to the user. Based on Opportunistic Wireless Encryption (OWE) defined in the Internet Engineering Task Force (IETF) RFC8110 specification and the **Wi-Fi Alliance Opportunistic Wireless Encryption Specification**, Wi-Fi Enhanced Open benefits users by providing data encryption that maintains the ease of use of open networks, and benefits network providers because there are no public passphrases to maintain, share, or manage.

Because Wi-Fi Enhanced Open is a Wi-Fi CERTIFIED™ program, the technology is interoperable with legacy networks, even those using a captive portal. Network operators wishing to deploy a fully-featured authentication and device-provisioning solution should consider approaches such as **Wi-Fi CERTIFIED Passpoint**®.

Wi-Fi Alliance News **See All**

Let’s talk about new wireless security certifications

Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security

Wi-Fi CERTIFIED Enhanced Open™: Transparent Wi-Fi® protections without complexity

Media Coverage **See All**

Wi-Fi Alliance introduces WPA3 and Wi-Fi Easy Connect

Product Finder

WPA2-Personal-certified products

WPA2-Enterprise-certified products

Download Additional Resources

Wi-Fi CERTIFIED WPA3™ Technology Overview

Wi-Fi CERTIFIED Enhanced Open™ Technology Overview

Opportunistic Wireless Encryption Specification v1.0

WPA3 Specification v1.0

Security Highlights

Technical Note: Removal of TKIP from Wi-Fi® Devices

Frequently Asked Questions

What does “security” mean in the context of Wi-Fi?

What is the KRACK attack?

What are Protected Management Frames?

What security measures should I take when working away from my home?

Are Wi-Fi CERTIFIED products protected by security?

What are “legacy protocols”?

Browse All Topics

- **Connect Your Life**
- **Enterprise**
- **Healthcare**
- **Miracast**
- **Operators**
- **Passpoint**
- **Security**

- **Wi-Fi Aware**
- **Wi-Fi CERTIFIED ac**
- **Wi-Fi CERTIFIED n**
- **Wi-Fi CERTIFIED Voice Programs**
- **Wi-Fi CERTIFIED WiGig**
- **Wi-Fi CERTIFIED WMM Programs**
- **Wi-Fi Direct**
- **Wi-Fi Easy Connect**
- **Wi-Fi EasyMesh**
- **Wi-Fi HaLow**
- **Wi-Fi Home Design**
- **Wi-Fi Location**
- **Wi-Fi Protected Setup**
- **Wi-Fi TimeSync**
- **Wi-Fi Vantage**