
WPA3 DEPLOYMENT MODEL FOR THE ENTERPRISE NETWORK

How to achieve upgradeable Secure Access

Monday, July 24, 2023



Contents

Security Enhancement Explained	6
Opportunistic Wireless Encryption (OWE) replacing the “guest” WLAN.....	6
WPA3-Personal is the replacement for WPA2-Personal “PSK” networks	7
WPA3-Enterprise 128 bit Encryption Mode.....	9
WPA3-Enterprise with 192-bit Encryption Mode	9
WPA3 Transition Mode Connectivity Chart	11
Challenges to Migration.....	11
Inclusion of Internal Security	13
Wi-Fi 6 Validation Testing	13
Lab Validation is Complicated and less expensive than a Severity One Incident causing BU Shut Down..	14
Cost Drivers for WPA3 Conversion	15
Lowering the cost of “Network Distribution”	15
A New Generation of “Assistant”	16
Implementation Plan	16
Limiting the number of WLANs.....	16
Separate your access rights.	17
Client Support Matrix.....	19
Jumbo Frames.....	20
Orthogonal Frequency Division Multiplexing - OFDMA.....	20
Summary	22
Enabling WPA3 Step by Step.....	22
Enterprise WLAN.....	22
OWE Compatibility WLAN.....	23
Machine Authentication Establishes Perimeter Security	24
Federated Authenticators.....	25
How do Federated Authenticators Onboard Devices?	27

Introduction

This document will help you plan your organization migration to WPA3 and 6GHz operations. Subjects are delivered in additional detail to highlight various options. Developing a secure network is an ongoing journey, we are here to assist you on your journey.

Enterprise networks are required to move from WPA2 to WPA3 encryption for their Wi-Fi networks. The primary drivers behind the need to migrate is that WPA2 has been around for almost 15 years, and during this time, it has become vulnerable to various attacks. Advancements in “Hacker” tools have found ways to exploit the weaknesses in WPA2. The weaker key length of preshare key technology makes it easier for unauthorized access to your enterprise network. Domain based authentication systems expose your organizations security architecture to “Social Media” leakage and exploits.

In contrast, WPA3 is a newer and more secure encryption protocol including a feature called Dragonfly; which provides better protection against these attacks. Dragonfly also provides a path to even higher initial encryption key lengths; further guarding against AI enabled hacking tools. Dragonfly uses a cryptographic technique called elliptic curve cryptography (ECC), which makes it much harder for attackers to guess the “root” passphrase.

One of the main advantages of WPA3 is that it provides stronger encryption than WPA2. WPA3 can use a 192-bit encryption key, which is much more difficult to crack than the 128-bit key used by WPA2 and WPA3 compatibility mode. This means that even if a hacker manages to decrypt the Group-Keyed Wi-Fi traffic, they will not be able to decipher the data frames. This is especially important for enterprise networks that deal with sensitive information such as:

- Financial Data
- Customer Information
- Intellectual Property

Another advantage of WPA3 is the protection against brute-force attacks. In a brute-force attack, a hacker tries to guess the Wi-Fi password by trying out different combinations of characters normally based on common phrases such as “helloDolly” = “he1l0D0lly”.

WPA3 has a feature called "Simultaneous Authentication of Equals" (SAE), which makes it much harder for hackers to guess the password. SAE uses the Dragonfly technique to generate a unique key for each authentication attempt, which makes it exponentially more difficult for hackers to guess the root password. WPA3 authentication method first creates a new security key based on the “Pre Shared Key” but does not expose the “Pre Share Key” itself by only sending “A” key generated transaction using the “base Passkey” that has been shared between devices. The initial sharing of passwords can be encrypted within a QR code that could be decrypted by the customers device WLAN “Management Agent” (Optional).


Man-in-the-middle attacks are also protected against when not using WPA3 “Open while Encrypted” (OWE). In a man-in-the-middle attack, a hacker intercepts the Wi-Fi traffic and then relays it to the intended

recipient. The recipient thinks that they are communicating directly with the sender, but in reality, the hacker is eavesdropping on the conversation. WPA3 has a feature called "Protected Management Frames" (PMF), which provides advanced protection against these types of attacks. Open with EAP is required to support management frame encryption. Once encryption is enabled existing 3rd party network monitoring tools will lose insights into the 802.11 counter validations of the Wi-Fi physical RF layer.

WPA3 is the latest and most secure wireless network security protocol and is designed to protect against various types of attacks. One of the key features of WPA3 is the Protected Management Frames (PMF) that provides an additional layer of security to the wireless network. PMF is designed to protect against attacks that exploit vulnerabilities in the management frames of the Wi-Fi protocol. Security groups require enterprise networks to adopt WPA3 security postures and retire WPA2 WLANs as soon as possible and one of the primary drivers to moving forward with the technology suite.

Wireless security cheat sheet

ENCRYPTION STANDARD	FAST FACTS	HOW IT WORKS	SHOULD YOU USE IT?
Wired Equivalent Privacy (WEP)	First 802.11 security standard. Easily hacked due to its 24-bit initialization vector (IV) and weak authentication.	Uses RC4 stream cipher and 64- or 128-bit keys. Static master key must be manually entered into each device.	No
Wi-Fi Protected Access (WPA)	An interim standard to address major WEP flaws. Backward-compatible with WEP devices.	Retains use of RC4 but adds longer IVs and 256-bit keys. Each client gets new keys with TKIP. Enterprise mode: Stronger authentication via 802.1x and EAP.	No
WPA2	Upgraded hardware ensured advanced encryption didn't affect performance.	Replaces RC4 and TKIP with CCMP and AES algorithm for stronger authentication and encryption.	If WPA3 is not available
WPA3	Current standard. New authentication method helps thwart KRACK and offline dictionary attacks.	Replaces PSK four-way handshake with SAE. Enterprise mode has optional 192-bit encryption and a 48-bit IV.	Yes

©2020 TECHTARGET. ALL RIGHTS RESERVED 

Security Enhancement Explained

Opportunistic Wireless Encryption (OWE) replacing the “guest” WLAN

OWE provides the replacement for the “Open” Guest WLAN we are all accustomed to for “no login” guest access. The issue with Wi-Fi 6 is the requirement for all management frames to be encrypted between the client and radio. When you add 6Ghz radios into the mix, you are now required to have management frame encryption for all 6Ghz SSID’s and WPA3 enabled on all RF Bands. To solve the need for both encrypted and non-encrypted (legacy) user access of SSID’s providing multi-band guest internet access. It is recommended to use the transitional mode OWE. In this configuration, the legacy Guest WLAN is modified to advertise a hidden SSID that is OWE enabled. Because the advertisement of the “hidden” WLAN is not really Hidden, it only serves as a mechanism to try and lesson the user complications involved with explaining to each user when to use which WLANs. Multi WLANs is the primary cause of poor user experience in the campus networking model. The following manual section provides a Cisco approach for each enterprise IT group to customize.

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217737-configure-enhanced-open-ssid-with-transi.html>

Next is three legal articles that deal with operating a Guest network. The articles indicate that the only “Legal” parallels in offering free internet is 1st the retention of user identifiable information, 2nd the legal requirements of notification for tracking and reporting purposes.

<https://www.findlaw.com/legalblogs/small-business/5-legal-tips-if-youre-offering-free-wi-fi/>

<https://www.findlaw.com/legalblogs/small-business/legal-to-track-customers-via-in-store-wifi/>

<https://arstechnica.com/information-technology/2016/08/public-wi-fi-forget-the-scare-stories-read-this/>

If the customer wishes to not use a two SSID solution than the use of WPA3 Personal or the use of a 3rd party authenticator like the Open Roaming Project could be a valid alternative.

The use of the "Open Roaming Organization" of federated authenticators, as described on the “WB” Alliance website <https://wballiance.com/openroaming/how-it-works/>. Allows for seamless and secure roaming across different providers Wi-Fi networks. The use of SaaS type services removes the need for users to constantly re-enter login credentials as they move between companies and locations. The federated authenticators work together to verify the user's identity and grant access to your guest or visitor network. The extent that the user is verified is not fully understood, nor the methods of auditing and remediation also needs research with evaluation on a per service provider basis.

One of the strengths of this technology is that it can greatly improve the user experience by eliminating the need for users to constantly re-enter login credentials as they move between different Wi-Fi service providers networks. This can be especially beneficial for organizations with large campuses or multiple locations and competitors, where users may need to frequently switch between different networks.