WPA3™ and Wi-Fi Enhanced™ Open Deployment and Implementation Guide

Version 1.0

WI-FI ALLIANCE PROPRIETARY – SUBJECT TO CHANGE WITHOUT NOTICE

Document Revision History

Version	Date YYYY-MM-DD	Remarks
1.0	2024-06-10	First public release.

Table of contents

List of tables

List of figures

1 Introduction

This document provides guidelines and recommended best practices for deployment of Wi-Fi CERTIFIED WPA3™ and Wi-Fi Enhanced Open™ devices. The guidelines in this document are not mandatory for equipment certification unless specified in the WPA3 Specification [1] and Opportunistic Wireless Encryption Specification [3]; however, their use will contribute toward realizing maximum benefit from certified equipment.

1.1 Reference documents

Knowledge of the documents listed in this section is required for understanding this document. If a reference includes a date or a version identifier, only that specific version of the document is required. If the listing includes neither a date nor a version identifier, then the latest version of the document is required. In the event of a conflict between this deployment guidelines document and the following referenced specifications, the contents of the respective specification take precedence.

[1] WPA3 Specification, https://www.wi-fi.org/file/wpa3-specification

[2] IEEE 802.11-REVme/D5.0 "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", February 2024

[3] Opportunistic Wireless Encryption Specification, https://www.wi-fi.org/file/opportunistic-wireless-encryption-specification

[4] IEEE 802.11be/D5.0 "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Enhancements for extremely high throughput (EHT)", November 2023

[5] National Institute of Standards and Technology (NIST) Special Publication SP 800-56A, Revision 3, April 2018

1.2 Definitions

The definitions in Table 1, as well as the definitions in the WPA3 Specification [1], are applicable to this document.

Table 1. Definitions

Term	Definition
Dual-SSID	A configuration that uses two distinct SSIDs, each operated by a distinct BSS

1.2.1 Abbreviations and acronyms

This section defines the acronyms used throughout this document. Some acronyms are commonly used in publications and standards defining the operation of wireless local area networks, while others have been generated by Wi-Fi Alliance®.

Table 2. Abbreviations and acronyms

Acronyms	Definition
AKM	Authentication Key Management
A-MSDU	Aggregate MAC Service Data Unit
BP	Beacon Protection
CCMP	Counter Mode CBC-MAC Protocol
EHT	Extremely High Throughput (PHY/MAC defined in [4])

Acronyms	Definition
EOS	End-of-Support
FT	Fast BSS Transition
GCMP	Galois Counter Mode Protocol
GDH	Group Dependent Hash
H2E	Hash-to-element (SAE PWE method)
IE	Information element
MME	Management MIC element
OCV	Operating Channel Validation
OWE	Opportunistic Wireless Encryption
PMF	Protected Management Frame
PSK	Preshared key
RSN	Robust Security Network
RSNE	RSN Element
RSNXE	RSN eXtension Element
SAE	Simultaneous Authentication of Equals
SAE-PK	SAE Public Key
SCV	Server Certificate Validation
SHA	Secure Hash Algorithm
TKIP	Temporary Pairwise Transient Key
WEP	Wired Equivalent Privacy
WPA3™-Enterprise	Wi-Fi Protected Access® 3-Enterprise
WPA3™-Personal	Wi-Fi Protected Access® 3-Personal

2 Security mode requirements and recommendations

2.1 Introduction

2.1.1 Overview

This section summarizes the security configuration requirements for APs and STAs operating in the WPA3 and Wi-Fi Enhanced Open modes defined in the WPA3 [1] and Wi-Fi Enhanced Open [3] specifications, and also provides additional recommendations for the security configuration in those modes.

For APs, the WPA3 and Wi-Fi Enhanced Open security modes are BSS specific, and the requirements and recommendations apply to the security parameters of the BSS Configuration when a BSS is operating in a given mode. The BSSs within a network (using the same SSID) do not, in general, all operate in the same mode. The security parameters of a given BSS are advertised in the RSN element (RSNE), RSN Extension element (RSNXE) and certain other fields and elements in Beacon and Probe Response frames.

For STAs, the WPA3 and Wi-Fi Enhanced Open security modes are Network Profile specific, and the requirements and recommendations apply to the security parameters of a given Network Profile in a given mode that is configured on the STA. When the STA associates to any AP with an SSID that matches a given Network Profile, the STA uses that Network Profile (together with the security parameters advertised for the BSS) to select the security parameters used for authentication and association to that AP. When an EHT STA connects to an MLD of an EHT AP, the selected security parameters apply to all links of the association with the AP MLD.

Table 3 describes the security configuration parameters referred to in this section, and how they determine the AP and STA's behavior. In subsequent subsections, the required and recommended values for each of these parameters in each security mode are specified.

Table 3. Security configuration parameters

Parameter	Reference	AP BSS Configuration	STA Network Profile
Legacy Security Parameters		When WEP is disallowed in a BSS configuration, the AP does not advertise or use WEP cipher suites (as pairwise or group cipher suite), and does not perform WEP Shared Key authentication, in the BSS. When TKIP is disallowed in a BSS configuration, the AP does not advertise or use TKIP cipher suites (as pairwise or group cipher suite) in the BSS. When WPA v1 is disallowed in a BSS configuration, the BSS does not advertise the WPA IE in Beacon and Probe Response frames.	When WEP is disallowed in a network profile on the STA, the STA does not select a WEP cipher suite (as pairwise or group cipher suite), and does not perform WEP Shared Key authentication, with APs or AP MLDs in the network. When TKIP is disallowed in a network profile on the STA, the STA does not select a TKIP cipher suite (as pairwise or group cipher suite) when associating to an AP or AP MLD in the network. When WPA v1 is disallowed in a network profile on the STA, the STA does not send WPA IE when associating to an AP or AP MLD in the network.
Privacy	[2] 9.4.1.4 "Capability Information field"	Privacy (Data frame confidentiality) configuration for the BSS. When Privacy is required in the BSS, the AP sets the Privacy subfield to 1.	N/A
Beacon Protection	[2] Table 9-192 "Extended Capabilities field" and 11.52 "Beacon Protection Procedures"	Beacon Protection configuration for the BSS. Applicable only if PMF is enabled on the BSS. When "Disabled", the capability bit in Extended Capabilities element is not set, and Beacon Protection is disabled in the BSS. When "Enabled", Beacon Protection is enabled in the BSS, the capability bit in Extended Capabilities element is set, and Beacon frames include an MME.	Beacon Protection configuration in a network profile on the STA for use in the network (SSID). Applicable only if PMF is enabled in the network profile. When "Disabled", Beacon Protection validation is not performed when connected to an AP or AP MLD in the network. When "Enabled", the STA validates the integrity of Beacon frames using the MME when connected to an AP in the network that enables PMF and Beacon Protection and validates the integrity of Beacon frames on all links when

Parameter	Reference	AP BSS Configuration	STA Network Profile
			connected to an AP MLD that enables Beacon Protection; otherwise, it does not perform such validation. NOTE: An AP MLD always enables PMF. NOTE: A STA does not advertise its Beacon Protection configuration.
Operating Channel Validation	[2] 9.4.2.23.4 "RSN capabilities" and 12.2.9 "Operating Channel Validation"	Operating Channel Validation configuration for the BSS. Applicable only if PMF is enabled on the BSS. When "Disabled", the capability bit is not set in RSNE, and Operating Channel Validation is disabled in the BSS. When "Enabled", Operating Channel Validation is enabled in the BSS, the capability bit in RSNE is set, and the AP validates its operating channel with STAs that also support Operating Channel Validation and associate to the AP.	Operating Channel Validation configuration in a network profile on the STA for use in the network (SSID). Applicable only if PMF is enabled in the network profile. When "Disabled", the capability bit is not set in RSNE, and Operating Channel Validation is not performed when connecting to an AP or AP MLD in the network. When "Enabled", the STA validates its operating channel when connecting to an AP or AP MLD in the network that also has PMF and Operating Channel Validation enabled; otherwise, it does not perform such validation. The capability bit in RSNE is set when connecting to an AP or AP MLD in the network regardless of whether validation is actually performed.
Transition Disable	[1] 8 "Transition Disable"	Transition Disable configuration for the BSS. When "Disabled", Transition Disable KDE is not sent in the BSS. When "Enabled", Transition Disable KDE (with specific configured contents) is sent to STAs that associate to the AP using a WPA3 AKM. NOTE: An AP does not advertise its Transition Disable configuration in Beacon and Probe Response frames.	N/A NOTE: If a STA supports Transition Disable feature, it is required to process all received Transition Disable KDEs per WPA3 Specification. Transition Disable is not configured on a Network Profile basis. A STA does not advertise its support for Transition Disable.
Group Data Cipher Suite	[2] Table 9-188 "Cipher suite selectors"	A single Group Data Cipher Suite enabled for use for all protected group data communications in the BSS, advertised in RSNE. The AP rejects association requests for the BSS from STAs that specify a different Group Data Cipher Suite.	List of one or more Group Data Cipher Suites enabled in a network profile on the STA for use in the network (SSID). The STA does not attempt to associate with an AP in the network if the BSS is using a Group Data Cipher Suite that is not in this list. The STA does not attempt to associate with an AP MLD in the network if the Group Data Cipher Suite advertised by all affiliated links of the AP MLD is not in this list.
Pairwise Cipher Suite	[2] Table 9-188 "Cipher suite selectors"	List of one or more Pairwise Cipher Suites, enabled for use for protected pairwise communications in the BSS, advertised in RSNE. The AP rejects association requests for the BSS from STAs that specify a Pairwise Cipher Suite not in this list.	List of one or more Pairwise Cipher Suites enabled in a network profile on the STA for use in the network (SSID). When a STA associates with an AP in the network, it selects one of the Pairwise Cipher Suites in this list which is also enabled by the AP. When an AP associates with an AP MLD in the network, it selects one of the Pairwise Cipher Suites in this list which is enabled by the BSSs of all affiliated links. The STA indicates the selected Pairwise Cipher Suite in RSNE. If no such suite exists, the STA does not attempt to associate with the AP or AP MLD.
Group Management Cipher Suite	[2] Table 9-188 "Cipher suite selectors"	A single Group Management Cipher Suite, advertised in RSNE, and enabled for use for integrity protected group management frame communications in the BSS. Applicable only when PMF is enabled on the BSS. The AP rejects association requests for the BSS from STAs that indicate PMF "Capable" or "Required" but specify a different Group Management Cipher Suite.	List of one or more Group Management Cipher Suites enabled in a network profile on the STA for use in the network (SSID). The STA does not attempt to associate with an AP in the network if the BSS advertises a Group Management Cipher Suite that is not in this list and PMF is used. The STA does not attempt to associate with an AP MLD in the network if the Group Management Cipher Suite advertised by all affiliated links of the AP MLD is not in this list. NOTE: An AP MLD always enables PMF.

Parameter	Reference	AP BSS Configuration	STA Network Profile
AKM Suite	[2] Table 9-190 "AKM suite selectors"	List of one or more AKM Suites, enabled for use for authentication and key management in the BSS, advertised in RSNE. The AP rejects association requests for the BSS from STAs that specify an AKM Suite not in this list. NOTE: The AP enables FT AKMs only when its BSS is part of an FT mobility domain. The AP enables FILS AKMs only when it supports a FILS authentication method for the BSS.	List of one or more AKM Suites enabled in a network profile on the STA for use in the network (SSID). When a STA associates with an AP in the network, it selects **one of** the AKM Suites in this list which is also enabled by the AP. When a STA associates with an AP MLD in the network, it selects one of the AKM Suites in this list which is also enabled by the BSSs of all affiliated links. The STA indicates the selected AKM Suite in RSNE. When multiple such suites exist, selection preference orders are defined (see [1]). If no such suite exists, the STA does not attempt to associate with the AP or AP MLD.
PMF	[2] Table 12-5 "Robust management frame selection in an infrastructure BSS" and 9.4.2.23.4 "RSN capabilities"	PMF configuration for the BSS. When "Disabled", the capability bits in RSNE are not set (MFPC=0; MFPR=0), and PMF is disabled in the BSS. When "Capable", PMF is enabled but not enforced in the BSS, the corresponding capability bits in RSNE are set (MFPC=1; MFPR=0), and PMF is used when a STA indicates PMF "Capable" or "Required"; otherwise, PMF is not used with the STA. When "Required", PMF is enabled and enforced in the BSS, the corresponding capability bits in RSNE are set (MFPC=1; MFPR=1), and PMF is used with all STAs; the AP rejects association requests for the BSS from STAs that have PMF disabled.	PMF configuration in a network profile on the STA for use in the network (SSID). When "Disabled", the capability bits in RSNE are not set (MFPC=0; MFPR=0) and PMF is not used when associating to an AP or AP MLD in the network; the STA does not attempt to associate with an AP that advertises PMF "Required", or with an AP MLD in the network if any of the affiliated links advertise PMF "Required". When "Capable", PMF is used when associating to an AP or AP MLD in the network that advertises PMF "Capable" or "Required"; otherwise PMF is not used. The corresponding capability bits in RSNE are set (MFPC=1; MFPR=0) when associating to an AP or AP MLD in the network regardless of whether PMF is actually used. When "Required", PMF is always used when associating to an AP or AP MLD in the network; the STA does not attempt to associate with an AP in the network that advertises PMF "Disabled", or with an AP MLD that advertises PMF "Disabled" on any of its affiliated links. The corresponding capability bits in RSNE are always set (MFPC=1; MFPR=1) when associating to an AP or AP MLD in the network.
SAE Groups		List of one or more SAE groups, enabled for use in SAE authentication. The AP rejects SAE authentication attempts using a group that is not on this list. NOTE: An AP does not advertise its enabled SAE Groups in Beacon and Probe Response frames.	Ordered list of one or more SAE groups enabled in a network profile on the STA for use in the network (SSID). When a STA attempts SAE authentication with an AP in the network, it selects the first SAE group in this list. If the AP rejects an SAE authentication attempt because it does not support the selected SAE group, the STA re-attempts SAE authentication using the next SAE group in the list (if any).
SAE Hash-to-Element	[2] Table 9-371 "Extended RSN Capabilities field" and Table 9-131 "BSS membership selector value encoding"	SAE Hash-to-Element configuration for the BSS. Applicable only if an SAE AKM suite is used. When "Disabled", SAE Hash-to-Element method is not enabled or used, and the capability bit in RSNXE is not set; the SAE Hunting-and-Pecking method is used with an SAE AKM. When "Enabled", SAE Hash-to-Element method is enabled, the capability bit in RSNXE is set, and Hash-to-Element is used with an SAE AKM when a STA indicates SAE Hash-to-Element "Enabled"; otherwise, the SAE Hunting-and-Pecking method is used with the STA. When "H2E Only", SAE Hash-to-Element method is enabled, the capability bit in RSNXE is set, the Hash-to-Element Only bit in Supported Rates and	SAE Hash-to-Element configuration in a network profile on the STA for use in the network (SSID). Applicable only if an SAE AKM suite is used. When "Disabled", the capability bit in RSNXE is not set and SAE Hash-to-Element method is not used when connecting to an AP or AP MLD in the network; the SAE Hunting-and-Pecking method is used with an SAE AKM; the STA does not attempt to connect to an AP using an SAE AKM if that AP advertises "Hash to Element Only" or if the AP MLD advertises "Hash to Element Only" on any of its affiliated links. When "Enabled", SAE Hash-to-Element method is used with an SAE AKM when connecting to an AP or AP MLD in the network that advertises SAE Hash-to-Element "Enabled" or "H2E Only"; otherwise, the SAE Hunting-and-Pecking method is used. The capability bit in RSNXE is set

Parameter	Reference	AP BSS Configuration	STA Network Profile
		BSS Membership Selectors element is set, and Hash-to-Element is always used with an SAE AKM; the SAE Hunting-and-Pecking method is not used.	when connecting to an AP or AP MLD in the network regardless of whether SAE Hash-to-Element method is actually used. When "H2E Only", SAE Hash-to-Element method is enabled and always used when connecting to an AP or AP MLD in the network; the STA does not attempt to associate to an AP if that AP does not advertise SAE Hash-to-Element "Enabled" or "H2E Only", or if the AP MLD does not advertise SAE Hash-to-Element "Enabled" or "H2E Only" on all of its affiliated links. The capability bit in RSNXE is set when connecting to an AP or AP MLD in the network.
SAE-PK	[1] 6.4 "Authentication using SAE-PK"	SAE-PK configuration for the BSS. Applicable only if an SAE AKM suite is used. When "Disabled", SAE-PK is not used and the capability bit in RSNXE is not set; SAE without SAE-PK is used with an SAE AKM. When "Enabled", the capability bit in RSNXE is set, SAE-PK is used with an SAE AKM when a STA indicates SAE-PK "Enabled"; otherwise, SAE without SAE-PK is used with the STA. NOTE: "Enabled" is only set when SAE-PK credentials are configured on the AP (and, therefore, the password is in the correct format for SAE-PK)	SAE-PK configuration in a network profile on the STA for use in the network (SSID). Applicable only if an SAE AKM suite is used. When "Disabled", SAE-PK is not used when connecting to an AP or AP MLD in the network; SAE without SAE-PK is used with an SAE AKM. When "Enabled", SAE-PK is used with an SAE AKM when connecting to an AP or AP MLD in the network that advertises SAE-PK "Enabled"; otherwise, SAE without SAE-PK is used with an SAE AKM. The capability bit in RSNXE is set when connecting to an AP or AP MLD in the network regardless of whether SAE-PK is actually used. When "SAE-PK Only", SAE-PK is always used with an SAE AKM when connecting to an AP or AP MLD in the network; the STA does not attempt to associate with an AP that advertises SAE-PK "Disabled". The capability bit in RSNXE is set when connecting to an AP or AP MLD in the network. NOTE: "Enabled" and "SAE-PK Only" are only set when the password is in the correct format for SAE-PK
Server Certificate Validation	[1] 5 "Server Certificate Validation"	N/A	Server Certificate Validation configuration in a network profile on the STA or use in the network (SSID). Applicable only when authentication uses an 802.1X EAP method that uses server certificates (e.g., WPA2-Enterprise or WPA3-Enterprise with EAP-TLS, EAP-TTLS, EAP-PEAPv0 or EAP-PEAPv1). When "Disabled", Server Certificate Validation is not performed by the STA when connecting to an AP or AP MLD in the network. When "Enabled", Server Certificate Validation is performed by the STA when authenticating using an 802.1X EAP method that uses server certificates. NOTE: A STA does not advertise its Server Certificate Validation configuration.
OWE Transition Mode element	[3] Table 3 "OWE Transition Mode element format"	OWE Transition Mode element configuration for the BSS. Applicable only if an OWE AKM suite is used. When "Disabled", OWE Transition Mode element is not sent in Beacon and Probe Response frames. When "Enabled", OWE Transition Mode element is sent in Beacon and Probe Response frames, on both the OWE BSS and the Open BSS. In addition, the SSID used by the OWE BSS is hidden.	N/A

2.1.2 Role of transition modes

Some of the WPA3 and Wi-Fi Enhanced Open modes defined in [1] and [3] are transition modes, which are intended to support interoperability between devices that only support, or are configured in, certain other legacy modes.

A transition mode configured on a BSS of an AP is a transitional solution until all STAs in the network support the higher security mode. For example, a BSS configured in WPA3-Personal Transition Mode will support connections from STAs that have Network Profiles configured in WPA3-Personal Only Mode, WPA3-Personal Transition Mode, or a WPA2-Personal mode.

Similarly, a transition mode configured on a STA is a transitional solution until all BSSs in the network support the higher security mode. For example, a STA configured with a Network Profile in WPA3-Personal Transition Mode will connect to BSSs in the network that are operating in WPA3-Personal Only Mode, WPA3-Personal Transition Mode, or a WPA2-Personal mode. On the other hand, a STA configured with a Network Profile in WPA3-Personal Only Mode will connect to APs in the network that are operating in WPA3-Personal Only Mode or WPA3-Personal Transition Mode, but not to APs operating in a WPA2-Personal mode.

NOTE: The Transition Disable feature (see [1] and Section 3.3.2) might cause a STA to modify the mode of a Network Profile configured on that STA, e.g., from a transition mode to an "only" mode.

2.1.3 Interpretation of requirements and recommendations

In the remainder of this section, the values of security parameters for each of the defined WPA3 and Wi-Fi Enhanced Open modes are specified.

For a given mode, the values are specified separately for each of four device types:

- AP: EHT enabled on BSS
- AP: EHT not enabled on BSS
- STA: EHT supported
- STA: EHT not supported

NOTE: "AP: EHT not enabled on BSS" includes all BSSs operated by APs that do not support EHT, and also BSSs operated by APs that do support EHT but where the BSS is configured with EHT and MLO disabled. "STA: EHT supported" includes all STAs that support EHT, even if EHT or MLO is not used in a given association.

For a given mode, device type and parameter, the values are annotated as follows:

- "MAND": Setting the parameter to this value is mandatory
- "RECOM": Setting the parameter to this value is not mandatory but is recommended
- "DISALLOW": Setting the parameter to this value is disallowed

The mandatory and disallowed values are derived from the WPA3 [1] and Wi-Fi Enhanced Open [3] specifications.
If a given annotation only applies under certain conditions, those conditions are shown in square brackets. For example, "[6 GHz or sub-1 GHz] MAND" for an AP means that the mandatory requirement to set the parameter to that value only applies for BSSs operating in 6 GHz and sub-1 GHz bands.

In cases where no mandatory value is specified for a parameter, or where the parameter can comprise a list of values, other unspecified values might be (additionally) configured, provided they are not annotated as disallowed.

NOTE: Some parameters, such as AKM Suite for APs and STAs, or Group Data Cipher Suite for STAs, can comprise a list of values. Therefore, it is not necessarily the case that a given mandatory value will actually be used in a given association. For example, a BSS in WPA3-Personal Transition Mode has both SAE and PSK AKM Suites enabled (as mandatory values) and might also enable other recommended AKM Suites such as FT; which of those AKM Suites is actually selected in a given association depends on the AKM Suites supported by the peer device and the AKM preference order defined in [1].

Implementers should refer to Table 3 for a description of AP and STA behavior with respect to the requirements and recommendations for each parameter.

Cipher Suites and AKM Suites are annotated with their Suite Type, where the OUI is 00-0F-AC. For example, "SAE (:8)" refers to the SAE AKM Suite 00-0F-AC:8.

Unless otherwise stated in this document or the underlying specifications (see [1], [2], [3] and [4]), no additional constraints exist regarding allowed combinations of security parameters. For example, use of AKM Suite SAE-GDH (:24) with Cipher Suite CCMP-128 (:4) is also permitted, as is use of AKM Suite SAE (:8) with Cipher Suite GCMP-256 (:9). Similarly, while the use of SAE Groups with higher strength estimates (e.g., SAE groups 20 and 21) with Cipher Suite GCMP-256 is preferable from the perspective of security strength consistency (see Section 3.3.8), use of SAE Group 19 with Cipher Suite GCMP-256 and/or AKM Suite SAE-GDH is also permitted.

2.2 Common security configuration for all WPA3 and Wi-Fi Enhanced Open modes

The security configuration that applies to **all** WPA3 and Wi-Fi Enhanced Open modes specified in this section are defined in Table 4.

Table 4. Common security configuration for all WPA3 and Wi-Fi Enhanced Open modes

Parameter	Device	Values		
		WEP	**TKIP**	**WPA v1 (WPA IE)**
Legacy Security Parameters	AP: EHT enabled on BSS	DISALLOW	DISALLOW	DISALLOW
	AP: EHT not enabled on BSS	DISALLOW	DISALLOW	DISALLOW
	STA: EHT supported	DISALLOW	DISALLOW	DISALLOW
	STA: EHT not supported	DISALLOW	DISALLOW	DISALLOW
		Required (1)	**Not required (0)**	
Privacy	AP: EHT enabled on BSS	MAND	DISALLOW	
	AP: EHT not enabled on BSS	MAND	DISALLOW	
	STA: EHT supported	N/A	N/A	
	STA: EHT not supported	N/A	N/A	
		Enabled	**Disabled**	
Beacon Protection	AP: EHT enabled on BSS	MAND	DISALLOW	
	AP: EHT not enabled on BSS	[except sub-1 GHz band *] RECOM		
	STA: EHT supported	MAND	DISALLOW	
	STA: EHT not supported	[except sub-1 GHz band *] RECOM		
Operating Channel Validation	AP: EHT enabled on BSS		RECOM (**)	
	AP: EHT not enabled on BSS		RECOM (**)	
	STA: EHT supported		RECOM (**)	
	STA: EHT not supported		RECOM (**)	
Transition Disable	AP: EHT enabled on BSS	RECOM (when applicable ***)	MAND (by default)	
	AP: EHT not enabled on BSS	RECOM (when applicable ***)	MAND (by default)	
	STA: EHT supported	N/A	N/A	
	STA: EHT not supported	N/A	N/A	
		Group 19	**Group 20**	**Group 21**
SAE Groups (****)	AP: EHT enabled on BSS	RECOM	RECOM	RECOM
	AP: EHT not enabled on BSS	RECOM	RECOM	RECOM
	STA: EHT supported	RECOM	RECOM	RECOM
	STA: EHT not supported	RECOM	RECOM	RECOM

(*) N/A for operation in sub-1 GHz band, since Beacon Protection is not supported.

(**) It is currently recommended that Operating Channel Validation is disabled due to potential interoperability issues, particularly when EHT or MLO is enabled and/or when the BSS operating bandwidth is greater than or equal to 160 MHz. This recommendation is expected to be revised at a future date.

(***) Transition Disable must be disabled by default on APs, except where otherwise specified. It is recommended to enable Transition Disable on APs if specific network deployment conditions apply. See Sections 6.5.1 and 8.2 of [1], and Section 3.3.2.

(****) SAE Groups parameter applies to all WPA3-Personal modes. There is no requirement on the order of the enabled SAE Groups in a STA's network profile (see Table 3). Note that, if the list is ordered with the SAE Groups that have highest strength estimate (see Appendix B of [1]) first, multiple authentication attempts (and, therefore, some additional delay) might be incurred when connecting to APs that do not enable those stronger groups. On the other hand, if the list is ordered with the SAE Groups that have the highest strength estimate last, those stronger groups might not actually be used except when connecting to APs that have the weaker groups disabled.

2.3 WPA3-Personal Transition Mode

Table 5 lists the security configuration for WPA3 devices in WPA3-Personal Transition Mode [1].

Table 5. WPA3-Personal Transition Mode security configuration

Parameter	**Device**	**Values**						
Common parameters		See Common security configuration in Table 4						
		GCMP-256 (:9)		**CCMP-128 (:4)**		**WEP-40/104 (:1/:5) TKIP (:2)**		
Group Data Cipher Suite	AP: EHT enabled on BSS			MAND		DISALLOW		
	AP: EHT not enabled on BSS			MAND		DISALLOW		
	STA: EHT supported	MAND		MAND		DISALLOW		
	STA: EHT not supported	RECOM		MAND		DISALLOW		
Pairwise Cipher Suite	AP: EHT enabled on BSS	MAND		MAND		DISALLOW		
	AP: EHT not enabled on BSS	RECOM		MAND		DISALLOW		
	STA: EHT supported	MAND		MAND		DISALLOW		
	STA: EHT not supported	RECOM		MAND		DISALLOW		
		BIP-GMAC-256 (:12)				**BIP-CMAC-128 (:6)**		
Group Mgmt Cipher Suite	AP: EHT enabled on BSS					MAND		
	AP: EHT not enabled on BSS					MAND		
	STA: EHT supported	MAND				MAND		
	STA: EHT not supported	RECOM				MAND		
		SAE-GDH (:24)	**SAE (:8)**	**PSK (:6)**	**PSK (:2)**	**FT-SAE-GDH (:25)**	**FT-SAE (:9)**	**FT-PSK (:4)**
AKM Suite	AP: EHT enabled on BSS	MAND	MAND	RECOM	MAND	RECOM	RECOM	RECOM
	AP: EHT not enabled on BSS	RECOM	MAND	RECOM	MAND	RECOM	RECOM	RECOM
	STA: EHT supported	MAND	MAND	RECOM	MAND	RECOM	RECOM	RECOM
	STA: EHT not supported	RECOM	MAND	RECOM	MAND	RECOM	RECOM	RECOM
		Required (MFPR=1)		**Capable (MFPC=1; MFPR=0)**		**Disabled (MFPC=0)**		
PMF	AP: EHT enabled on BSS	DISALLOW		MAND		DISALLOW		
	AP: EHT not enabled on BSS	DISALLOW		MAND		DISALLOW		
	STA: EHT supported	DISALLOW		MAND		DISALLOW		
	STA: EHT not supported	DISALLOW		MAND		DISALLOW		

Parameter	Device	Values		
		H2E Only	**Enabled**	**Disabled**
SAE Hash-to-Element	AP: EHT enabled on BSS		MAND	DISALLOW
	AP: EHT not enabled on BSS		RECOM (if supported *)	
	STA: EHT supported	DISALLOW	MAND	DISALLOW
	STA: EHT not supported	DISALLOW	MAND (if supported *)	DISALLOW (if supported)

(*) SAE Hash-to-Element support is necessary in the following cases:

- Using SAE-GDH and FT-SAE-GDH AKM Suites
- Connecting to a BSS using any SAE AKM Suite in 6 GHz or sub-1 GHz bands
- Connecting to a BSS using any SAE AKM Suite when EHT is enabled for the association

An AP does not operate a BSS in this transition mode in the 6 GHz or sub-1 GHz bands; the mode defined in Section 2.4 can be used instead.

A STA that is configured with a hexadecimal WPA2 PSK but is not configured with a passphrase does not operate in this mode; the hexadecimal PSK can be used in WPA2-Personal mode with PSK AKM.

2.4 WPA3-Personal Only Mode

Table 6 lists the security configuration for WPA3 devices in WPA3-Personal Only Mode.

Table 6. WPA3-Personal Only Mode security configuration

Parameter	Device	Values					
Common parameters		See Common security configuration in Table 4					
		GCMP-256 (:9)		**CCMP-128 (:4)**		**WEP-40/104 (:1/:5) TKIP (:2)**	
Group Data Cipher Suite	AP: EHT enabled on BSS			RECOM (**)		DISALLOW	
	AP: EHT not enabled on BSS			RECOM (***)		DISALLOW	
	STA: EHT supported	MAND		MAND		DISALLOW	
	STA: EHT not supported	RECOM		MAND		DISALLOW	
Pairwise Cipher Suite	AP: EHT enabled on BSS	MAND		MAND (**)		DISALLOW	
	AP: EHT not enabled on BSS	RECOM		MAND		DISALLOW	
	STA: EHT supported	MAND		MAND		DISALLOW	
	STA: EHT not supported	RECOM		MAND		DISALLOW	
		BIP-GMAC-256 (:12)			**BIP-CMAC-128 (:6)**		
Group Mgmt Cipher Suite	AP: EHT enabled on BSS				RECOM (**)		
	AP: EHT not enabled on BSS				RECOM (***)		
	STA: EHT supported	MAND			MAND		
	STA: EHT not supported	RECOM			MAND		
		SAE-GDH (:24)	**SAE (:8)**	**PSK (:6) PSK (:2)**	**FT-SAE-GDH (:25)**	**FT-SAE (:9)**	**FT-PSK (:4)**
AKM Suite	AP: EHT enabled on BSS	MAND	MAND (**)	DISALLOW	RECOM	RECOM	DISALLOW
	AP: EHT not enabled on BSS	RECOM	MAND	DISALLOW	RECOM	RECOM	DISALLOW
	STA: EHT supported	MAND	MAND (**)	DISALLOW	RECOM	RECOM	DISALLOW
	STA: EHT not supported	RECOM	MAND	DISALLOW	RECOM	RECOM	DISALLOW

Parameter	Device	Values		
		Required (MFPR=1)	**Capable (MFPC=1; MFPR=0)**	**Disabled (MFPC=0)**
PMF	AP: EHT enabled on BSS	MAND	DISALLOW	DISALLOW
	AP: EHT not enabled on BSS	MAND	DISALLOW	DISALLOW
	STA: EHT supported	MAND	DISALLOW	DISALLOW
	STA: EHT not supported	MAND	DISALLOW	DISALLOW
		H2E Only	**Enabled**	**Disabled**
SAE Hash-to-Element	AP: EHT enabled on BSS	[6 GHz or sub-1 GHz] MAND	[other] MAND	DISALLOW
	AP: EHT not enabled on BSS	[6 GHz or sub-1 GHz] MAND	[other] RECOM (if supported *)	[6 GHz or sub-1 GHz] DISALLOW
	STA: EHT supported	DISALLOW (**)	MAND (**)	DISALLOW
	STA: EHT not supported	DISALLOW	MAND (if supported *)	DISALLOW (if supported)

(*) SAE Hash-to-Element support is necessary to use SAE-GDH and FT-SAE-GDH AKM Suites, and to connect to a BSS using any SAE AKM Suite in 6 GHz or sub-1 GHz bands.

(**) If this mode is used in a network where all APs and STAs are known to support EHT, GCMP-256 (00-0F-AC:9) can be used as the only Group Data Cipher Suite, BIP-GMAC-256 (00-0F-AC:12) can be used as the only Group Management Cipher Suite, CCMP-128 (00-0F-AC:4) does not need to be enabled as a Pairwise Cipher Suite, SAE (00-0F-AC:8) does not need to be enabled as an AKM Suite, and H2E Only can be used.

(***) Although not strictly required, it is strongly recommended in these cases that the AP uses CCMP-128 as the Group Data Cipher Suite, and BIP-CMAC-128 as the Group Management Cipher Suite, for compatibility with all non-EHT STAs.

2.5 WPA3-Personal SAE-PK Transition Mode

Table 7 lists the security configuration for WPA3 devices in WPA3-Personal SAE-PK Transition Mode.

Table 7. WPA3-Personal SAE-PK Transition Mode security configuration

Parameter	Device	Values		
Common parameters		See Common security configuration in Table 4		
Group Data Cipher Suite		Same as WPA3-Personal Transition Mode (Table 5)		
Pairwise Cipher Suite		Same as WPA3-Personal Transition Mode (Table 5)		
Group Mgmt Cipher Suite		Same as WPA3-Personal Transition Mode (Table 5)		
AKM Suite		Same as WPA3-Personal Transition Mode (Table 5)		
PMF		Same as WPA3-Personal Transition Mode (Table 5)		
		H2E Only	**Enabled**	**Disabled**
SAE Hash-to-Element	AP: EHT enabled on BSS		MAND	DISALLOW
	AP: EHT not enabled on BSS		MAND	DISALLOW
	STA: EHT supported	DISALLOW	MAND	DISALLOW
	STA: EHT not supported	DISALLOW	MAND	DISALLOW
		SAE-PK Only	**Enabled**	**Disabled**
SAE-PK	AP: EHT enabled on BSS		MAND	DISALLOW
	AP: EHT not enabled on BSS		MAND	DISALLOW
	STA: EHT supported		MAND	DISALLOW
	STA: EHT not supported		MAND	DISALLOW

An AP does not operate a BSS in this transition mode in the 6 GHz or sub-1 GHz bands; the mode defined in Section 2.6 can be used instead.

BSS selection rules based on SAE-PK support are defined for the STA; see [1].

2.6 WPA3-Personal SAE-PK Only Mode

Table 8 lists the security configuration for WPA3 devices in WPA3-Personal SAE-PK Only Mode.

Table 8. WPA3-Personal SAE-PK Only Mode security configuration

Parameter	Device	Values		
Common parameters		See Common security configuration in Table 4		
Group Data Cipher Suite		Same as WPA3-Personal Only Mode (Table 6)		
Pairwise Cipher Suite		Same as WPA3-Personal Only Mode (Table 6)		
Group Mgmt Cipher Suite		Same as WPA3-Personal Only Mode (Table 6)		
AKM Suite		Same as WPA3-Personal Only Mode (Table 6)		
PMF		Same as WPA3-Personal Only Mode (Table 6)		
		H2E Only	**Enabled**	**Disabled**
SAE Hash-to-Element	AP: EHT enabled on BSS	MAND	DISALLOW	DISALLOW
	AP: EHT not enabled on BSS	MAND	DISALLOW	DISALLOW
	STA: EHT supported	MAND	DISALLOW	DISALLOW
	STA: EHT not supported	MAND	DISALLOW	DISALLOW
		SAE-PK Only	**Enabled**	**Disabled**
SAE-PK	AP: EHT enabled on BSS	N/A	MAND	DISALLOW
	AP: EHT not enabled on BSS	N/A	MAND	DISALLOW
	STA: EHT supported	MAND	DISALLOW	DISALLOW
	STA: EHT not supported	MAND	DISALLOW	DISALLOW

BSS selection rules based on SAE-PK support are defined for the STA; see [1].

2.7 WPA3-Enterprise Transition Mode

Table 9 lists the security configuration for WPA3 devices in WPA3-Enterprise Transition Mode.

Table 9. WPA3-Enterprise Transition Mode security configuration

Parameter	Device	Values		
Common parameters		See Common security configuration in Table 4		
		GCMP-256 (:9)	**CCMP-128 (:4)**	**WEP-40/104 (:1/:5) TKIP (:2)**
Group Data Cipher Suite	AP: EHT enabled on BSS		MAND	DISALLOW
	AP: EHT not enabled on BSS		MAND	DISALLOW
	STA: EHT supported	MAND	MAND	DISALLOW
	STA: EHT not supported	RECOM	MAND	DISALLOW
Pairwise Cipher Suite	AP: EHT enabled on BSS	MAND	MAND	DISALLOW
	AP: EHT not enabled on BSS	RECOM	MAND	DISALLOW
	STA: EHT supported	MAND	MAND	DISALLOW

Parameter	Device	Values		
	STA: EHT not supported	RECOM	MAND	DISALLOW
		BIP-GMAC-256 (:12)	**BIP-CMAC-128 (:6)**	
Group Mgmt Cipher Suite	AP: EHT enabled on BSS		MAND	
	AP: EHT not enabled on BSS		MAND	
	STA: EHT supported	MAND	MAND	
	STA: EHT not supported	RECOM	MAND	
		802.1X SHA-256 (:5)	**802.1X SHA-1 (:1)**	**FT-802.1X SHA-256 (:3)** **FILS SHA-256 (:14)** **FILS-FT SHA-256 (:16)**
AKM Suite	AP: EHT enabled on BSS	MAND	MAND	RECOM
	AP: EHT not enabled on BSS	MAND	MAND	RECOM
	STA: EHT supported	MAND	MAND	RECOM
	STA: EHT not supported	MAND	MAND	RECOM
		Required (MFPR=1)	**Capable (MFPC=1; MFPR=0)**	**Disabled (MFPC=0)**
PMF	AP: EHT enabled on BSS	DISALLOW	MAND	DISALLOW
	AP: EHT not enabled on BSS	DISALLOW	MAND	DISALLOW
	STA: EHT supported	DISALLOW	MAND	DISALLOW
	STA: EHT not supported	DISALLOW	MAND	DISALLOW
		Enabled	**Disabled**	
Server Certificate Validation	AP: EHT enabled on BSS	N/A	N/A	
	AP: EHT not enabled on BSS	N/A	N/A	
	STA: EHT supported	MAND (if supported)	DISALLOW (if supported)	
	STA: EHT not supported	MAND (if supported)	DISALLOW (if supported)	

An AP does not operate a BSS in this transition mode in the 6 GHz band; the mode defined in Section 2.8 can be used instead.

NOTE: WPA3-Enterprise transition mode is similar to WPA2-Enterprise, except that TKIP is disallowed, PMF is enabled ("Capable"), and support for SHA-256 AKM (in addition to SHA-1 AKM) is required.

2.8 WPA3-Enterprise Only Mode

Table 10 lists the security configuration for WPA3 devices in WPA3-Enterprise Only Mode.

Table 10. WPA3-Enterprise Only Mode security configuration

Parameter	Device	Values		
Common parameters		See Common security configuration in Table 4		
		GCMP-256 (:9)	**CCMP-128 (:4)**	**WEP-40/104 (:1/:5)** **TKIP (:2)**
Group Data Cipher Suite	AP: EHT enabled on BSS		RECOM (**)	DISALLOW
	AP: EHT not enabled on BSS		RECOM (***)	DISALLOW
	STA: EHT supported	MAND	MAND	DISALLOW
	STA: EHT not supported	RECOM	MAND	DISALLOW
	AP: EHT enabled on BSS	MAND	MAND (**)	DISALLOW

Parameter	Device	Values		
Pairwise Cipher Suite	AP: EHT not enabled on BSS	RECOM	MAND	DISALLOW
	STA: EHT supported	MAND	MAND	DISALLOW
	STA: EHT not supported	RECOM	MAND	DISALLOW
		BIP-GMAC-256 (:12)	**BIP-CMAC-128 (:6)**	
Group Mgmt Cipher Suite	AP: EHT enabled on BSS		RECOM (**)	
	AP: EHT not enabled on BSS		RECOM (***)	
	STA: EHT supported	MAND	MAND	
	STA: EHT not supported	RECOM	MAND	
		802.1X SHA-256 (:5)	**802.1X SHA-1 (:1)**	**FT-802.1X SHA-256 (:3) FILS SHA-256 (:14) FILS-FT SHA-256 (:16)**
AKM Suite	AP: EHT enabled on BSS	MAND	DISALLOW	RECOM
	AP: EHT not enabled on BSS	MAND	DISALLOW	RECOM
	STA: EHT supported	MAND	DISALLOW	RECOM
	STA: EHT not supported	MAND	DISALLOW	RECOM
		Required (MFPR=1)	**Capable (MFPC=1; MFPR=0)**	**Disabled (MFPC=0)**
PMF	AP: EHT enabled on BSS	MAND	DISALLOW	DISALLOW
	AP: EHT not enabled on BSS	MAND	DISALLOW	DISALLOW
	STA: EHT supported	MAND	DISALLOW	DISALLOW
	STA: EHT not supported	MAND	DISALLOW	DISALLOW
		Enabled	**Disabled**	
Server Certificate Validation	AP: EHT enabled on BSS	N/A	N/A	
	AP: EHT not enabled on BSS	N/A	N/A	
	STA: EHT supported	MAND (if supported)	DISALLOW (if supported)	
	STA: EHT not supported	MAND (if supported)	DISALLOW (if supported)	

(**) If this mode is used in a network where all APs and STAs are known to support EHT, GCMP-256 (00-0F-AC:9) can be used as the only Group Data Cipher Suite, BIP-GMAC-256 (00-0F-AC:12) can be used as the only Group Management Cipher Suite, and CCMP-128 (00-0F-AC:4) does not need to be enabled as a Pairwise Cipher Suite.

(***) Although not strictly required, it is strongly recommended in these cases that the AP uses CCMP-128 as the Group Data Cipher Suite, and BIP-CMAC-128 as the Group Management Cipher Suite, for compatibility with all non-EHT STAs.

NOTE: WPA3-Enterprise Only Mode is separate and distinct from WPA3-Enterprise 192-bit Mode. For example, although WPA3-Enterprise Only Mode requires PMF and disallows SHA-1 based AKMs, it allows FT and FILS AKMs to be used and does not mandate use of CNSA Suite compliant EAP methods or GCMP-256 cipher suites.

2.9 WPA3-Enterprise 192-bit Mode

Table 11 lists the security configuration for WPA3 devices in WPA3-Enterprise 192-bit Mode.

Table 11. WPA3-Enterprise 192-bit Mode security configuration

Parameter	Device	Values	
Common parameters		See Common security configuration in Table 4	
		GCMP-256 (:9)	**All other cipher suites**

Parameter	Device	Values		
Group Data Cipher Suite	AP: EHT enabled on BSS	MAND	DISALLOW	
	AP: EHT not enabled on BSS	MAND	DISALLOW	
	STA: EHT supported	MAND	DISALLOW	
	STA: EHT not supported	MAND	DISALLOW	
Pairwise Cipher Suite	AP: EHT enabled on BSS	MAND	DISALLOW	
	AP: EHT not enabled on BSS	MAND	DISALLOW	
	STA: EHT supported	MAND	DISALLOW	
	STA: EHT not supported	MAND	DISALLOW	
		BIP-GMAC-256 (:12)	**All other cipher suites**	
Group Mgmt Cipher Suite	AP: EHT enabled on BSS	MAND	DISALLOW	
	AP: EHT not enabled on BSS	MAND	DISALLOW	
	STA: EHT supported	MAND	DISALLOW	
	STA: EHT not supported	MAND	DISALLOW	
		802.1X CNSA Suite compliant EAP method SHA-256 (:12)	**All other AKM Suites**	
AKM Suite	AP: EHT enabled on BSS	MAND	DISALLOW	
	AP: EHT not enabled on BSS	MAND	DISALLOW	
	STA: EHT supported	MAND	DISALLOW	
	STA: EHT not supported	MAND	DISALLOW	
		Required (MFPR=1)	**Capable (MFPC=1; MFPR=0)**	**Disabled (MFPC=0)**
PMF	AP: EHT enabled on BSS	MAND	DISALLOW	DISALLOW
	AP: EHT not enabled on BSS	MAND	DISALLOW	DISALLOW
	STA: EHT supported	MAND	DISALLOW	DISALLOW
	STA: EHT not supported	MAND	DISALLOW	DISALLOW
		Enabled	**Disabled**	
Server Certificate Validation	AP: EHT enabled on BSS	N/A	N/A	
	AP: EHT not enabled on BSS	N/A	N/A	
	STA: EHT supported	MAND (if supported)	DISALLOW (if supported)	
	STA: EHT not supported	MAND (if supported)	DISALLOW (if supported)	

In WPA3-Enterprise 192-bit Mode, EAP-TLS is the only permitted EAP method, using one of the following EAP cipher suites [1]:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 using P-384 curve for ECDHE and ECDSA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 using P-384 curve for ECDHE and at least 3072-bit RSA modulus
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 using at least 3072-bit DHE and RSA modulus

2.10 Wi-Fi Enhanced Open Transition Mode

Table 12 lists the security configuration for devices in Wi-Fi Enhanced Open Transition Mode.

Table 12. Wi-Fi Enhanced Open Transition Mode security configuration

Parameter	Device	Values		
Common parameters		See Common security configuration in Table 4		
		GCMP-256 (:9)	**CCMP-128 (:4)**	**WEP-40/104 (:1/:5) TKIP (:2)**
Group Data Cipher Suite	AP: EHT enabled on BSS		MAND	DISALLOW
	AP: EHT not enabled on BSS		MAND	DISALLOW
	STA: EHT supported	MAND	MAND	DISALLOW
	STA: EHT not supported	RECOM	MAND	DISALLOW
Pairwise Cipher Suite	AP: EHT enabled on BSS	MAND	MAND	DISALLOW
	AP: EHT not enabled on BSS	RECOM	MAND	DISALLOW
	STA: EHT supported	MAND	MAND	DISALLOW
	STA: EHT not supported	RECOM	MAND	DISALLOW
		BIP-GMAC-256 (:12)	**BIP-CMAC-128 (:6)**	
Group Mgmt Cipher Suite	AP: EHT enabled on BSS		MAND	
	AP: EHT not enabled on BSS		MAND	
	STA: EHT supported	MAND	MAND	
	STA: EHT not supported	RECOM	MAND	
		OWE (:18)		
AKM Suite	AP: EHT enabled on BSS	MAND		
	AP: EHT not enabled on BSS	MAND		
	STA: EHT supported	MAND		
	STA: EHT not supported	MAND		
		Required (MFPR=1)	**Capable (MFPC=1; MFPR=0)**	**Disabled (MFPC=0)**
PMF	AP: EHT enabled on BSS	MAND	DISALLOW	DISALLOW
	AP: EHT not enabled on BSS	MAND	DISALLOW	DISALLOW
	STA: EHT supported	MAND	DISALLOW	DISALLOW
	STA: EHT not supported	MAND	DISALLOW	DISALLOW
		Enabled	**Disabled**	
OWE Transition Mode element	AP: EHT enabled on BSS	MAND	DISALLOW	
	AP: EHT not enabled on BSS	MAND	DISALLOW	
	STA: EHT supported	N/A	N/A	
	STA: EHT not supported	N/A	N/A	

An AP in this mode operates a pair of BSSs - a legacy Open BSS and an OWE BSS. The Open BSS uses the network SSID. The OWE BSS uses a different, hidden, SSID. Both BSSs in the pair send an OWE Transition Mode element (see Section 2.2 of [3]).

The Network Profile of a STA in this mode matches both SSIDs. It allows connection to both OWE BSSs and Open BSSs using the network SSID, and also allows connection to OWE BSSs in Wi-Fi Enhanced Open Transition Mode using the hidden SSID (discovered by receiving the OWE Transition Mode element).

An AP does not operate a BSS in this transition mode in the 6 GHz or sub-1 GHz bands, or if EHT or MLO is enabled on the BSS in any band (see deployment considerations in Section 3.1.3); the mode defined in Section 2.11 can be used instead.

2.11 Wi-Fi Enhanced Open Only Mode

Table 13 lists the security configuration for devices in Wi-Fi Enhanced Open Only Mode.

Table 13. Wi-Fi Enhanced Open Only Mode security configuration

Parameter	Device	Values		
Common parameters		See Common security configuration in Table 4		
		GCMP-256 (:9)	**CCMP-128 (:4)**	**WEP-40/104 (:1/:5) TKIP (:2)**
Group Data Cipher Suite	AP: EHT enabled on BSS		MAND (**)	DISALLOW
	AP: EHT not enabled on BSS		MAND	DISALLOW
	STA: EHT supported	MAND	MAND	DISALLOW
	STA: EHT not supported	RECOM	MAND	DISALLOW
Pairwise Cipher Suite	AP: EHT enabled on BSS	MAND	MAND (**)	DISALLOW
	AP: EHT not enabled on BSS	RECOM	MAND	DISALLOW
	STA: EHT supported	MAND	MAND	DISALLOW
	STA: EHT not supported	RECOM	MAND	DISALLOW
		BIP-GMAC-256 (:12)	**BIP-CMAC-128 (:6)**	
Group Mgmt Cipher Suite	AP: EHT enabled on BSS		MAND (**)	
	AP: EHT not enabled on BSS		MAND	
	STA: EHT supported	MAND	MAND	
	STA: EHT not supported	RECOM	MAND	
		OWE (:18)		
AKM Suite	AP: EHT enabled on BSS	MAND		
	AP: EHT not enabled on BSS	MAND		
	STA: EHT supported	MAND		
	STA: EHT not supported	MAND		
		Required (MFPR=1)	**Capable (MFPC=1; MFPR=0)**	**Disabled (MFPC=0)**
PMF	AP: EHT enabled on BSS	MAND	DISALLOW	DISALLOW
	AP: EHT not enabled on BSS	MAND	DISALLOW	DISALLOW
	STA: EHT supported	MAND	DISALLOW	DISALLOW
	STA: EHT not supported	MAND	DISALLOW	DISALLOW
		Enabled	**Disabled**	
OWE Transition Mode element	AP: EHT enabled on BSS	DISALLOW	MAND	
	AP: EHT not enabled on BSS	DISALLOW	MAND	
	STA: EHT supported	N/A	N/A	
	STA: EHT not supported	N/A	N/A	

(**) If this mode is used in a network where all APs and STAs are known to support EHT, GCMP-256 (00-0F-AC:9) can be used as the only Group Data Cipher Suite, BIP-GMAC-256 (00-0F-AC:12) can be used as the only Group Management Cipher Suite, and CCMP-128 (00-0F-AC:4) does not need to be enabled as a Pairwise Cipher Suite.

3 Deployment and implementation recommendations

3.1 Default requirements and recommendations

3.1.1 WPA3-Personal

3.1.1.1 APs

When a new network is configured on APs that use a PSK or SAE passphrase for authentication, the AP should use one of the following modes as the default security configuration for each BSS:

- For BSSs in 2.4 and 5 GHz band:
  - WPA3-Personal Transition Mode as defined in Section 2.3, or
  - WPA3-Personal Only Mode as defined in Section 2.4, with provisions for the end-user to reconfigure the BSS to WPA3-Personal Transition Mode
- For BSSs in 6 GHz and sub-1 GHz bands:
  - WPA3-Personal Only Mode

An example of such configuration is shown in Appendix A.1.

For new networks deployed after December 31st, 2027, the recommended default security configuration will be WPA3-Personal Only Mode for BSSs in all bands.

For SAE-PK networks, the SAE-PK versions of the above modes should be used instead.

If the network also comprises non-WPA3 APs, the BSSs on those APs should be configured in a WPA2-Personal mode.

The same password should be configured on all BSSs of the network. This allows a STA, when provisioned with a single password for the network, to authenticate in all BSSs of that network.

If the network enables a PSK AKM on any BSS (e.g., in a WPA2-Personal mode, or WPA3-Personal Transition Mode), it is recommended that the deployment does not use WPA3-Personal Only Mode on any 2.4 or 5 GHz BSS of that network. This is because some STA implementations might use the discovery of WPA3-Personal Only APs in 2.4 or 5 GHz bands as a basis for configuring their Network Profile in WPA3-Personal Only mode, or with a policy that that will not connect to BSSs that have a PSK AKM enabled.

If the default security configuration uses a non-unique or easily guessable password, the AP should include a label or UI indication that recommends the user reconfigures the network with a stronger password, and the UI should enforce password complexity requirements for user configured passwords (see Section 3.3.6).

3.1.1.2 STAs

If a STA auto-generates a network profile for an SSID (e.g., when the STA displays a list of discovered SSIDs and the user selects one of the SSIDs for the first time), and one or more discovered BSSs with the selected SSID advertise a PSK or SAE AKM, by default it should configure the network profile in WPA3-Personal Transition Mode (Section 2.3).

NOTE: WPA3-Personal Transition Mode does not permit use of WEP or TKIP. If the STA might need to enable WEP or TKIP in the network (e.g., if any of the BSSs in the network are configured in WPA/WPA2-Personal Mixed Mode, which uses TKIP group cipher), the network profile might need to be modified to additionally enable WEP and/or TKIP.

If the STA supports SAE-PK and the password is in the correct form, by default the network profile should be configured in WPA3-Personal SAE-PK Transition Mode (Section 2.5).

3.1.2 WPA3-Enterprise

3.1.2.1 APs

When a new network is configured on APs that use IEEE 802.1X for authentication, and the network is not intended for WPA3-Enterprise 192-bit mode security, the AP should use one of the following modes as the default security configuration for each BSS:

- For BSSs in 2.4 and 5 GHz band:
  - WPA3-Enterprise Transition Mode as defined in Section 2.7, or
  - WPA3-Enterprise Only Mode as defined in Section 2.8, with provisions for the end-user to reconfigure the BSS to WPA3-Enterprise Transition Mode
- For BSSs in 6 GHz and sub-1 GHz bands:
  - WPA3-Enterprise Only Mode.

An example of such configuration is shown in Appendix A.2.

If the network also comprises non-WPA3 APs, the BSSs on those APs should be configured in a WPA2-Enterprise mode.

All BSSs in a WPA3-Enterprise network should allow authentication using the same EAP server, so that a STA can use the same EAP credentials to authenticate in all BSSs of that network.

3.1.2.2 STAs

If a STA auto-generates a network profile for an SSID, and one or more discovered BSSs with the selected SSID advertise an 802.1X AKM, by default it should configure the network profile in WPA3-Enterprise Transition Mode (Section 2.7).

NOTE: WPA3-Enterprise Transition Mode does not permit use of WEP or TKIP. If the STA might need to enable WEP or TKIP in the network (e.g., if any of the BSSs in the network are configured in WPA/WPA2-Enterprise Mixed Mode, which uses TKIP group cipher), the network profile might need to be modified to additionally enable WEP and/or TKIP.

NOTE: It is expected that STAs connecting to a WPA3-Enterprise 192-bit Mode network will be explicitly configured with a network profile for WPA3-Enterprise 192-bit Mode.

3.1.3 Wi-Fi Enhanced Open

3.1.3.1 APs

When a new network is configured on APs that does not enable authentication, the AP should use one of the following modes as the default security configuration for each BSS:

- For BSSs in 2.4 and 5 GHz band:
  - Non-EHT AP in a network that does not include EHT APs:
    - Wi-Fi Enhanced Open Transition Mode (using a pair of BSSs) as defined in Section 2.10 and [3], or
    - Wi-Fi Enhanced Open Only Mode as defined in Section 2.11
  - Other APs:
    - Wi-Fi Enhanced Open Only Mode
- For BSSs in 6 GHz and sub-1 GHz bands:
  - Wi-Fi Enhanced Open Only Mode

Examples of such configuration are shown in Appendix A.3 (transition mode for non-EHT AP) and Appendix A.4 (Dual-SSID for EHT APs).If Wi-Fi Enhanced Open Transition Mode is configured, and other BSSs (in 6 GHz or sub-1 GHz band) are configured in the same network using Wi-Fi Enhanced Open Only mode, those other BSSs should use the network SSID (i.e., the same SSID that is used by the Open BSSs that are in transition mode).

If the network also comprises APs that do not support Wi-Fi Enhanced Open, the BSSs on those APs should be configured in legacy Open mode and use the network SSID (i.e., the same SSID that is used by the Open BSSs that are in transition mode).

If Wi-Fi Enhanced Open Transition Mode is configured, it is recommended that Wi-Fi Enhanced Open Only Mode is not configured on any other BSS in the same network, except for operation in the 6 GHz or sub-1 GHz bands. In other words, in 2.4 and 5 GHz bands, other BSSs in the network should be configured in Wi-Fi Enhanced Open Transition Mode (if supported) or legacy Open mode. This avoids interoperability issues between legacy STAs and BSSs in Wi-Fi Enhanced Open Only mode (which do not use hidden SSID with OWE BSS).

If the network includes EHT or MLO APs and needs to support legacy STAs (that do not support Wi-Fi Enhanced Open) then the network should be configured with Dual SSIDs, per the example given in Appendix A.4. In this configuration, the BSSs using the legacy Open SSID have EHT and MLO disabled and operate in 2.4 and/or 5 GHz band only. The BSSs using the OWE SSID can operate with EHT and MLO enabled and in any band. The OWE Transition Mode element is not sent by any of the BSSs.

NOTE: Wi-Fi Enhanced Open Transition Mode is disallowed on BSSs with EHT or MLO enabled.

3.1.3.2 STAs

If a STA auto-generates a network profile for an SSID, and one or more discovered BSSs with the selected SSID advertise legacy Open or OWE AKM, by default it should configure the network profile in Wi-Fi Enhanced Open Transition Mode (Section 2.10).

When a STA "roams" between the OWE BSS of Wi-Fi Enhanced Open Transition Mode (in 2.4 or 5 GHz) and a BSS in Wi-Fi Enhanced Open Only Mode (e.g., in 6 or sub-1 GHz GHz) or a BSS in legacy Open mode (e.g., operated by a non-OWE AP in the same network), the SSID that the STA is associated with will change. The OWE Transition Mode element provides the indication that both SSIDs provide access to the same DS. A STA implementation should handle this change of SSID transparently to the upper layers, so that it does not cause unexpected user impact.

In the case of a Dual-SSID Wi-Fi Enhanced Open configuration, STAs that support Wi-Fi Enhanced Open should be configured with a network profile for the OWE SSID only, while STAs that do not support Wi-Fi Enhanced Open should be configured with a network profile for the Open SSID only.

3.1.4 General

The following recommendations apply to all modes of operation.

3.1.4.1 APs

Where possible, it is recommended that the WPA3 AKMs (including, when appropriate, FT and FILS AKMs) supported by a network are advertised by all BSSs of that network. This can help maximize interoperability when STAs roam between BSSs because a consistent AKM can be used for all roams.

When FT is enabled on a network, where possible it is recommended that the same set of pairwise cipher suites is enabled by all BSSs of a given FT mobility domain. This allows STAs to roam between all BSSs of the mobility domain using FT protocol, which requires the pairwise cipher suite of target BSS (or target MLD APs) to be the same as that used in the initial FT association (see 12.7.1.6.1 of [2]).

While in principle it is permitted for a given BSS, or different BSSs in the same network, to advertise a mixture of WPA3-Personal, WPA3-Enterprise and/or OWE AKMs, it should be noted such deployments might cause unexpected interoperability issues with STAs, e.g., related to auto-join, roaming or UI behavior.

NOTE: The RSNE and RSNXE advertised by all links of an AP MLD must be identical, except for the AKM Suite List field and MFPR subfield of the RSN Capabilities field [4]. The (subset of) AKM Suites that is advertised on all links of an AP MLD can be used in ML associations; AKM Suites that are not advertised on all links can only be used for non-ML associations to the BSS that is advertising that AKM Suite.

3.1.4.2 STAs

A STA should not auto-configure a network profile in an "only" mode, rather than a transition mode, based purely on the absence of BSS operating with legacy security in scan results, since BSSs in the network may be operating in different modes and not all BSSs in the network might be detected in a given scan.

NOTE: The security mode of an auto-generated network profile might subsequently change after the STA's first connection to the network if Transition Disable indication is enabled, e.g., from WPA3-Personal Transition Mode to WPA3-Personal Only Mode.

If a STA's UI displays a list of discovered networks, a given SSID should be displayed only once, even when the BSSs advertising that SSID are operating in different security modes.

A STA should not reject a BSS as a candidate for selection (either on initial network join, or on roam using the reassociation procedure) on the basis of security if the BSS configuration and the STA's security configuration (for the corresponding network profile) have a mutually compatible set of security parameters. Roaming between BSSs with the same SSID (and in addition, in the case of Wi-Fi Enhanced Open Transition Mode, between an OWE BSS and Open BSS) should be performed without user intervention or disconnection.

NOTE: This means that a STA configured in a transition mode might need to roam to a target BSS using a different AKM and/or cipher suites than was used with the source BSS. Similarly, the STA might need to roam to a target BSS without negotiating PMF even when PMF was negotiated with the source BSS (and vice versa).

NOTE: Specific rules for security-based BSS selection prioritization are defined for SAE-PK, see [1].

NOTE: Due to the AKM preference order requirements in [1], a STA that associated to a BSS using a WPA2 FT AKM (e.g., FT-PSK) might need to perform non-FT reassociation or FT initial mobility domain reassociation (instead of FT authentication) when roaming to a BSS that supports a WPA3 AKM (e.g., SAE or FT-SAE). Network deployments can maximize the use of FT authentication by ensuring the same FT AKMs are enabled across all BSSs of a network.

3.2 Troubleshooting and resolving issues with legacy client connectivity to WPA3-Personal networks

It is expected that a large majority of legacy WPA2 STAs will correctly interoperate with APs operating BSSs in WPA3-Personal Transition Mode. However, it is possible that connection issues might be found with certain legacy STAs, e.g., due to incorrect parsing of RSN element sent by the AP when it indicates multiple AKM Suites or interoperability issues with other WPA3 mechanisms. These issues might manifest to end users as unexpected UI messages (e.g., incorrect password error, unexpected prompts for network credentials, etc.,).

Therefore, the AP vendor should include a label or UI indication that describes how the end user can reconfigure the BSSs, if necessary, to support non-interoperable legacy STAs.

Legacy STAs are more likely to have interoperability issues with WPA3-Personal Transition Mode if they meet one or more of the following criteria:

- The STA has been designated as EOS by the device manufacturer, and so is no longer receiving software updates, or
- The STA was manufactured prior to December 31st, 2015

In the event that such issues are found with legacy STAs, it is recommended that a workaround configuration defined in this section is used instead:

- Dual-SSID WPA3-Personal configuration for legacy STA interoperability (section 3.2.1)

Unless the workaround configurations described in this section result in an unacceptable user experience, it is not recommended to disable WPA3 on the network, since to do so would reduce security for WPA3 STAs. In addition, it should be noted that EHT or MLO associations using password-based authentication require WPA3 to be enabled on the network.

3.2.1 Dual-SSID WPA3-Personal configuration for legacy STA interoperability

The Dual-SSID configuration for legacy STA interoperability is defined in Table 14.

An example of this configuration is shown in Appendix A.5.

The main benefits of this configuration are:

- It ensures legacy STAs with interoperability issues do not attempt to connect to any BSS in the network with WPA3 enabled (since they are not configured with a Network Profile for the Main SSID)
- All WPA3 STAs will connect to the more secure SSID using WPA3

However, this configuration comes at the expense of deployment complexity and/or usability. For example, it may result in a poor user experience for users who have difficulty determining which SSID a given STA should be configured to use (based on whether it is a legacy STA with WPA3 interoperability issues), or who have difficulty manually reconfiguring legacy STAs with the Legacy SSID.

Table 14. Dual-SSID WPA3-Personal configuration for legacy STA interoperability

	Configuration
AP and radio deployment	Main BSS: Deployed on all radios of all APs. Legacy BSS: Deployed on all radios of all APs other than 6 GHz and sub-1 GHz radios.
SSID	Distinct SSIDs, e.g. Main BSS: "HomeNet" Legacy BSS: "HomeNet-legacy"
Security mode	Main BSS (6 GHz and sub-1 GHz): WPA3-Personal Only Mode (Section 2.4) Main BSS (2.4 GHz and 5 GHz on WPA3 APs): WPA3-Personal Transition Mode (Section 2.3) Main BSS (2.4 GHz and 5 GHz on WPA2-only APs): WPA2-Personal mode Legacy BSS: WPA2-Personal mode
EHT	Main BSS: EHT and MLO enabled if supported (WPA3 is also enabled) Legacy BSS: EHT and MLO disabled
Password	The same password can be used for Main SSID and Legacy SSID for convenience (see footnote 1)
Layer-2 forwarding	The BSSs are bridged
STA configuration	Legacy STAs that have WPA3 interoperability issues are configured with a Network Profile for the Legacy SSID (but not the Main SSID) All other STAs are configured with a Network Profile for the Main SSID (but not the Legacy SSID)

In the event that interoperability issues continue to be experienced even when this workaround is configured, the following changes to the Legacy BSS configuration might be considered:

- Try disabling PMF (MFPC=0) on the Legacy BSS, to avoid issues with legacy STAs that advertise support for PMF but fail to properly negotiate or sustain a PMF-enabled connection (see footnote 2)
- If there is a need for legacy pre-WPA2 STAs to connect, configure the Legacy BSS in Mixed Mode with WEP/TKIP enabled

3.3 Considerations to maximize Wi-Fi network security

The deployment and implementation recommendations in this section are intended, along with the mandatory requirements defined in the WPA3 Specification [1], to maximize Wi-Fi network security with WPA3.

Failure to implement these recommendations correctly may expose the vendor implementation to attack and/or compromise the network.

[1] When additional security protection is required, the configuration described in Section 3.3.3 is recommended.
[2] Unless interoperability issues are found, it is recommended that PMF is enabled on the Legacy BSS since it protects against deauthentication attacks that can be used to facilitate offline dictionary attacks on the WPA2 passphrase.

3.3.1 WPA3-Enterprise Server Certificate Validation policies

When a WPA3-Enterprise network uses a TLS-based EAP method (EAP-TTLS, EAP-TLS, EAP-PEAPv0 or EAP-PEAPv1), a Trust Override Disable (TOD) policy can be included in the TLS server certificate to provide STAs that support Server Certificate Validation (SCV) with protection against inadvertent acceptance of trust in malicious networks (see Section 5 of [1]).

When the network deployment is such that all STAs are configured with TLS-based EAP credentials (including the trust basis for SCV) via a secure out-of-band mechanism (e.g., using third-party device management technologies), the TOD-STRICT policy should be included in the server certificate.

In other network deployments using TLS-based EAP credentials, the TOD-TOFU policy should be included in the server certificate unless it is expected the server certificate will be renewed in the future and a mechanism to update the SCV trust basis on STAs is not available.

3.3.2 Transition Disable indication

As specified in [1], Transition Disable is an indication from an AP to a STA, which causes the STA to disable transition mode in the network profile corresponding to the AP (i.e., modify the network profile to an "only" mode) and/or change the values of parameters permitted within a given mode. The network administrator should ensure that, when Transition Disable is enabled on a given BSS, it is also enabled on all other BSSs that have the same SSID. The configured Transition Disable KDE should be identical across those APs. Since some multi-site network deployments might be independently managed at each site, the Transition Disable configuration at one site needs to take into account the potential impact on STAs that might subsequently attempt to connect to BSSs with the same SSID at other sites if the Transition Disable configuration is not fully synchronized across all sites. Since the SSID is not guaranteed to be a globally unique identifier of a network, caution should be applied if enabling Transition Disable on a network that uses an SSID that is likely to also be used by other independent networks.

In general, Transition Disable should be used to disable a given transition mode only if all BSSs in the network have enabled the most secure algorithm defined for that mode. However, in certain cases, a network administrator might enable a Transition Disable configuration even when only a subset of BSSs in the network enable the most secure algorithm. In such cases, STAs would subsequently only connect to that subset of BSSs, but would be protected against downgrade attacks. The network administrator should evaluate the impact on network coverage and performance when considering such configuration.

When an AP enables Transition Disable indication, the Transition Disable Bitmap field should be set as follows:

- If the APs in the network have WPA3-Personal enabled, bit 0 (WPA3-Personal) should be set to 1. This causes a STA that supports WPA3-Personal to configure the network profile in WPA3-Personal Only Mode:
  - If the APs also have SAE-PK enabled, bit 1 (SAE-PK) should also be set to 1. This causes a STA that supports SAE-PK to configure the network profile in WPA3-Personal SAE-PK Only Mode
- If the APs in the network have WPA3-Enterprise enabled, bit 2 (WPA3-Enterprise) should be set to 1. This causes a STA that supports WPA3-Enterprise to configure the network profile in WPA3-Enterprise Only Mode

3.3.3 Dual-SSID alternative to WPA3-Personal transition mode for additional security protection

When a WPA3-Personal network needs to support both WPA3-Personal and WPA2-Personal STAs, BSSs in 2.4 and 5 GHz bands are typically configured in WPA3-Personal Transition Mode as discussed in Section 3.1.1. This provides the convenience of a single SSID and password that can be used by all WPA3 and WPA2 devices. When a WPA3 STA connects to an AP that is configured in WPA3-Personal Transition Mode, it is protected against passive link decryption attacks and is also protected against (unicast) management frame spoofing attacks.

However, a trade-off of this convenience is that the common password of a WPA3-Personal Transition Mode network can be determined by attacking a WPA2-Personal device using a simple offline dictionary attack. The WPA2-Personal attack could be performed passively on a legacy client device that only supports WPA2-Personal, or a more complex active downgrade attack could be performed on a client that supports WPA3-Personal.

The passive attack on legacy WPA2-Personal only client devices is the same as exists with legacy WPA2-Personal only networks. The active attack on an WPA3-Personal client device is complex and gains the attacker little because of the possibility to run the simpler passive attack on legacy clients. An attacker who determines the password can access the network simply by using WPA2-Personal, irrespective of WPA3-Personal. In addition, even after this attack is successful and the attacker determines the password, the clients that connect with WPA3-Personal will still benefit from the forward-secrecy that SAE affords—that is, the traffic encryption keys will still remain unknown even if the password is known.

Nevertheless, in some deployments, enhanced security is required to protect against the above attack. For these scenarios, the Dual-SSID network configuration in Table 15 is recommended.

In this Dual-SSID configuration, since the WPA3 password is not used for WPA2 authentication exchanges, offline dictionary attacks on the WPA2 passphrase (which, in transition mode, could lead to attacks on WPA3 STAs) are not possible. In addition, since layer-2 forwarding between WPA2 and WPA3 BSSs is disabled or minimized, the risk of insider attacks on WPA3 STAs via the network infrastructure, by an attacker that manages to obtain the WPA2 passphrase, is mitigated.

The benefits of this Dual-SSID configuration may come at the expense of deployment complexity and/or usability. For example, it may result in a poor user experience for users who have difficulty determining which SSID a given STA should connect to (based on its support for WPA3), or who have difficulty manually reconfiguring the SSID and password on STAs that previously only supported WPA2 but were subsequently updated to support WPA3.

Table 15. Dual-SSID WPA3-Personal network configuration for enhanced security

	Configuration
AP and radio deployment (see footnote 3)	WPA3 BSS: Deployed on all radios of all APs that support WPA3 (see footnote 4) WPA2 BSS: Deployed on all radios of all APs other than 6 GHz and sub-1 GHz radios (see footnote 5).
SSID	Distinct SSIDs, e.g., (see footnote 6) WPA3 BSS: "HomeNet" WPA2 BSS: "HomeNet-legacy"
Security mode	WPA3 BSS: WPA3-Personal Only Mode (Section 2.4) WPA2 BSS: WPA2-Personal mode
EHT	WPA3 BSS: EHT and MLO enabled if supported WPA2 BSS: EHT and MLO disabled
Password	Distinct passwords are used for WPA3 SSID and WPA2 SSID. It is necessary for the WPA3 password to be unguessable – either directly, or from knowledge of the WPA2 passphrase, see Section 3.3.6. The WPA2 passphrase should be a non-dictionary, high entropy password to improve resistance to dictionary attack, and have length between 8 and 63 characters.
Layer-2 forwarding	Layer-2 forwarding between WPA2 and WPA3 BSSs is disabled or (at least) limited to minimal forwarding rules (see footnote 7)
Transition Disable	WPA3 BSS: Enabled (if network deployment conditions apply) WPA2 BSS: Disabled
STA configuration	WPA3 STAs are configured with network profile for WPA3 SSID and password WPA2 STAs are configured with network profile for WPA2 SSID and passphrase

[3] An AP that supports "virtual APs" (aka "co-hosted BSSs" or "multiple BSSID set") can typically be configured with both a WPA2 BSS and a WPA3 BSS on the same band/radio.
[4] If an AP does not support WPA3, it is not configured with the WPA3 SSID or password.
[5] Configuration of a WPA2-Personal BSS in the 6 GHz or Sub 1GHz bands is not permitted. All STAs that support the 6 GHz band or sub-1 GHz band also support WPA3-Personal.
[6] The SSIDs should be chosen to encourage an end user (who might not know whether a STA supports WPA3) to first try configuring a STA with the WPA3 SSID and password.
[7] See Section 3.3.4. It is not necessary to disable forwarding between STAs in the same BSS (aka intra-BSS STA isolation) unless in a public network deployment.

In principle, a single-SSID solution is also possible, whereby the AP is configured with a different password for SAE AKM and PSK AKM on the same BSS. However, this requires an AP configuration that might not be supported in typical implementations (as well as the ability to apply per-STA filtering rules based on AKM), so is not discussed further.

3.3.4 STA isolation and filtering

Some network services (for example, some network printing, content sharing and display services) rely on STAs being able to communicate with each other across the network. However, if a network enables such communication and an attacker is able to gain access to the network, other STAs are potentially vulnerable to insider attacks.

In network deployments where STA-to-STA communication is not required – which in general includes all public Wi-Fi networks – forwarding of packets between STAs in the same BSS should be disabled (aka STA isolation), and forwarding of packets between STAs associated to different BSSs in the same network (aka BSS bridging) should be disabled; only packet forwarding rules to/from a gateway should be configured. In addition, if broadcast data communications is not required (e.g., if Proxy ARP is enabled and the AP converts group-addressed IP packets such as DHCP and Router Advertisement packets to individually addressed 802.11 frames), the AP should provide a random GTK to each STA or (if supported by all STAs) set the group data cipher suite to 00-07-AC:7 (group addressed traffic not allowed).

If STA-to-STA communication is required but there is risk of unauthorized network access, it is recommended that filtering rules are configured to minimize the scope of forwarded packets to the needed communications.

3.3.5 Wireless Protected Setup and Wi-Fi Easy Connect with WPA3 modes

An AP can enable Wireless Protected Setup (WPS) or Wi-Fi Easy Connect when operating in any WPA3-Personal mode.

However, it is recommended that WPS is not enabled on a BSS if the BSSs in that network are configured in WPA3-Personal Only Mode.

An AP can enable Wi-Fi Easy Connect when operating in any WPA3-Enterprise mode, except for WPA3-Enterprise 192-bit mode.

A STA can use a password for a given network, that was obtained using WPS (with Authentication Type = WPA2-Personal) or Wi-Fi Easy Connect (using DPP Configuration), to authenticate with any AP in that network using any PSK or SAE AKM.

A STA can use an enterprise credential (X.509 certificate) for a given network, that was obtained using Wi-Fi Easy Connect (using DPP Configuration), to authenticate with any AP in that network using any 802.1X AKM.

NOTE: The use of DPP AKM is defined in the Wi-Fi Easy Connect specification.

NOTE: In general, the overall security of network devices depends on the security of the bootstrapping and provisioning mechanisms supported.

3.3.6 WPA3-Personal password selection considerations

Passwords used with WPA3-Personal should be complex enough to not be easily guessable, and WPA3-Personal implementations should limit authentication attempts when an implementation identifies an active attack.

WPA3-Personal replaces the WPA2-Personal Pre-Shared Key (PSK) authentication with SAE. Unlike PSK, SAE is resistant to offline dictionary attacks. The only way for an attacker to learn a password is through repeated active attacks, each of which tests whether a single guess of the password is correct or not. Repeated authentication failures may indicate that an active attack is underway, allowing implementations to respond appropriately, including throttling authentication attempts and/or issuing alerts such as Simple Network Management Protocol (SNMP) trap, log message, or others.

The requirement for exceedingly long, random passwords with mixed-case characters and special characters is no longer necessary with WPA3-Personal. Passwords used with WPA3-Personal should be extremely difficult to guess due to the possibility of an active attack; however, the difficulty in guessing a password directly correlates to the security that SAE offers.

NOTE: This does not apply to SAE-PK passwords, which are cryptographically generated.

To illustrate the benefits that WPA3-Personal affords, consider a password selected randomly from 5,000 possible passwords. The attacker knows this but does not know which password was randomly chosen. With WPA2-Personal an attacker could determine the password through an off-line dictionary attack with a probability of success of 1. With WPA3-Personal, the attacker must launch repeated active attacks, guessing a different password each time. The probability of success of the WPA3-Personal attack would only reach 0.5 after 2,500 active attacks. It should be possible to detect such an attack on WPA3-Personal long before the probability of success becomes high.

Implementations of WPA3-Personal should limit authentication attempts for a particular password—identified with an SAE Password Identifier or not—when an active attack is identified. Determination of whether an attack is underway is implementation dependent and left up to the vendor. One possible mitigation strategy may be that the AP temporarily disable a password after a series of unsuccessful authentication attempts. Note that the source medium access control (MAC) address used with failed authentication attempts is irrelevant and should not factor into the decision to disable or limit authentication for a particular password because an attacker can easily change the MAC address between attempts.

3.3.7 WPA3-Personal AP denial-of-service protection

WPA3-Personal implementations should handle SAE operations on non-privileged processing queues which, even if overwhelmed, will not result in a failure of the entire BSS through CPU resource consumption.

An AP performs a significant amount of cryptographic work upon receipt of the first message in an SAE handshake. A denial of service attack can be initiated by flooding the AP with fraudulent messages from fake MAC addresses resulting in the failure of the entire BSS through CPU resource consumption.

SAE defines an anti-clogging cookie response in which the AP statelessly generates a string that is bound to the sender of the message when the AP detects it is under a denial of service attack. An AP may consider itself under a denial of service attack when the number of nascent connections, those in which the first message has been received but not the third message, reaches a threshold. The AP, when in a “cookie demanding” state, will not process the first SAE message unless that message contains a valid cookie bound to the MAC address of the sender.

This technique works against rudimentary and simple packet spraying attacks because the attacker is simply sending random packets and not processing responses. However, this technique does not work if the attacker chooses to receive the AP cookie request and respond with the cookie from the same MAC address. Therefore, SAE does not afford adequate protection against more sophisticated denial of service attacks. WPA3-Personal implementations should handle SAE operations on non-privileged processing queues which, even if overwhelmed, will not result in a failure of the entire BSS through CPU resource consumption.

3.3.8 SAE Group downgrade protection

In SAE, the initiator chooses the group to use and includes the group number in the first message. The responder accepts the group or responds with a message containing an error code indicating group rejection if the responder does not want to use the group. If the group is rejected, the initiator chooses another group and tries again.

When SAE is used with the Hunting-and-Pecking method, it is vulnerable to a downgrade attack where an attacker impersonates the AP and responds with a rejection of a stronger group until the client device offers a weak group and then lets the protocol proceed with the real AP. This can be mitigated by not allowing weak groups and only allowing rejections to offer “upgraded” groups.

When SAE is used with the Hash-to-Element method, explicit protection against SAE Group Downgrade attacks is provided because identifiers of the rejected groups are included in the KDF for subsequent SAE exchanges using other groups.

Suitable Diffie-Hellman groups for use with SAE (aka suitable SAE Groups) all generate a key whose strength is appropriate for the cipher CCMP-128. Stronger ciphers such as CCMP-256 and GCMP-256 can also be used with SAE. When those stronger ciphers are used, it is recommended that SAE groups with higher strength estimates (e.g., SAE group 20 or 21) are used, together with SAE AKMs that use a group-dependent hash function (e.g., SAE-GDH (00-0F-AC:24) or FT-SAE-GDH (00-0F-AC:25)), in order that the security level is consistent.

When a STA uses SAE to connect to an AP using a given pairwise cipher suite, it is recommended that it first offers an SAE group whose strength estimate (see Appendix B of [1]) is greater than or equal to the strength estimate of that pairwise cipher suite. See Appendix D Table 24 and Table 25 of [5] for more information.

3.3.9 Protections against A-MSDU flag manipulation attacks

A receiving device should discard all subframes in an A-MSDU if its first subframe exhibits any of the following behaviors:

- DA does not map to 802.11 MAC header RA in a frame exiting DS (i.e., From DS subfield is 1 and To DS subfield is 0 in MAC header, DA is neither the device's RA address nor a group/multicast address)
- SA does not match 802.11 MAC header TA in a frame destined to DS (i.e., To DS subfield is 1 and From DS subfield is 0 in MAC header)
- DA is AA:AA:03:00:00:00 (any DS bits including 4-addr)

NOTE: This does not apply to some cases when operating as a GLK STA or S1G STA.

By flipping the A-MSDU Present subfield in the QoS Control field of the 802.11 MAC header in a non-A-MSDU frame, one can make a vulnerable receiving device accept it as an A-MSDU frame. The first subframe will exhibit the pattern as shown in the recommendation above and is usually discarded given its invalid construct. However, if a vulnerable device retains the subsequent subframes, an adversary can inject specially formulated data to solicit sensitive user information. Thus, a device should implement the mitigation mechanism to detect an abnormal first A-MSDU subframe behavior and then discard the subsequent subframes. Such a mechanism can be accomplished on the receiving device side.

A more comprehensive solution may be to protect the A-MSDU Present subfield in the QoS Control field of the 802.11 MAC header using a mechanism such as Signaling and Payload Protection (SPP), and to offer a transition means to bridge the gap between legacy and enhanced devices. The purpose of SPP is to protect an A-MSDU against attacks that manipulate the unauthenticated A-MSDU Present subfield in its plaintext QoS Control field. SPP includes this flag as part of the AAD calculation, which can effectively detect such manipulation.

Appendix A Example AP configurations

A.1 Example tri-band AP configuration using WPA3-Personal Transition Mode

Figure 1 shows an example configuration using WPA3-Personal Transition Mode on a 2.4+5+6 GHz tri-band AP, when support for legacy STAs is required. The AP is configured to operate BSSs in WPA3-Personal Transition Mode in 2.4 and 5 GHz bands and operate a BSS in WPA3-Personal Only Mode in 6 GHz band. All three BSSs use the same SSID. When the AP supports EHT, all three BSSs can be affiliated with the same MLD.

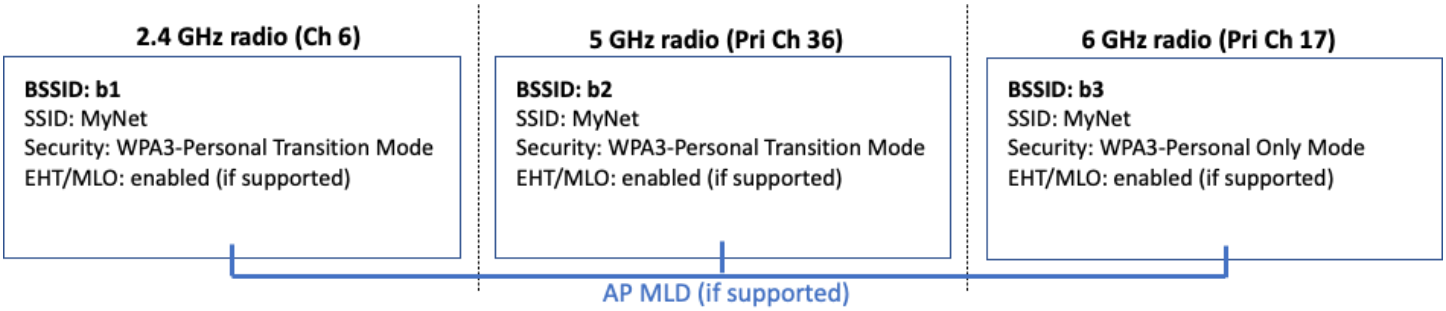

Figure 1. Example tri-band AP configuration using WPA3-Personal Transition Mode

A.2 Example tri-band AP configuration using WPA3-Enterprise Transition Mode

Figure 2 shows an example configuration using WPA3-Enterprise Transition Mode on a 2.4+5+6 GHz tri-band AP, when support for legacy STAs is required. The AP is configured to operate BSSs in WPA3-Enterprise Transition Mode in 2.4 and 5 GHz bands, and operate a BSS in WPA3-Enterprise Only Mode in 6 GHz band. All three BSSs use the same SSID. When the AP supports EHT, all three BSSs can be affiliated with the same MLD.

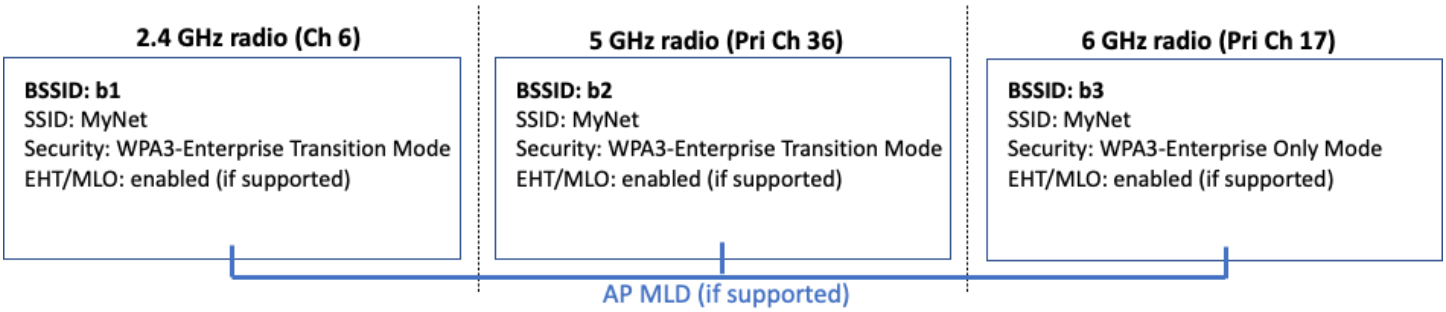

Figure 2. Example tri-band AP configuration using WPA3-Enterprise Transition Mode

A.3 Example tri-band AP configuration using Wi-Fi Enhanced Open Transition Mode

Figure 3 shows an example configuration using Wi-Fi Enhanced Open Transition Mode on a 2.4+5+6 GHz tri-band AP, when support for legacy STAs is required. The AP is configured to operate BSSs in Wi-Fi Enhanced Open Transition Mode in 2.4 and 5 GHz bands, with both OWE and legacy Open BSSs on each band, and operate an OWE BSS in Wi-Fi Enhanced Open Only Mode in 6 GHz band.

All OWE BSSs in transition mode (i.e., in 2.4 and 5 GHz) use the same hidden SSID ("MyNetOWE3257" in this example). OWE BSSs and legacy Open BSSs advertise each other by sending an OWE Transition Mode element.

The advertised SSID ("MyNet" in this example) is used by the 6 GHz OWE BSS and also by the legacy Open BSSs in 2.4 and 5 GHz. The advertised SSID is not hidden.The 6 GHz OWE BSS does not advertise an OWE Transition Mode element.

NOTE: This configuration cannot be used if any of the 2.4 or 5 GHz BSSs have EHT or MLO enabled.

If the network does not need to support legacy STAs, all BSSs in the network should be configured in Enhanced Open Only mode on all bands.

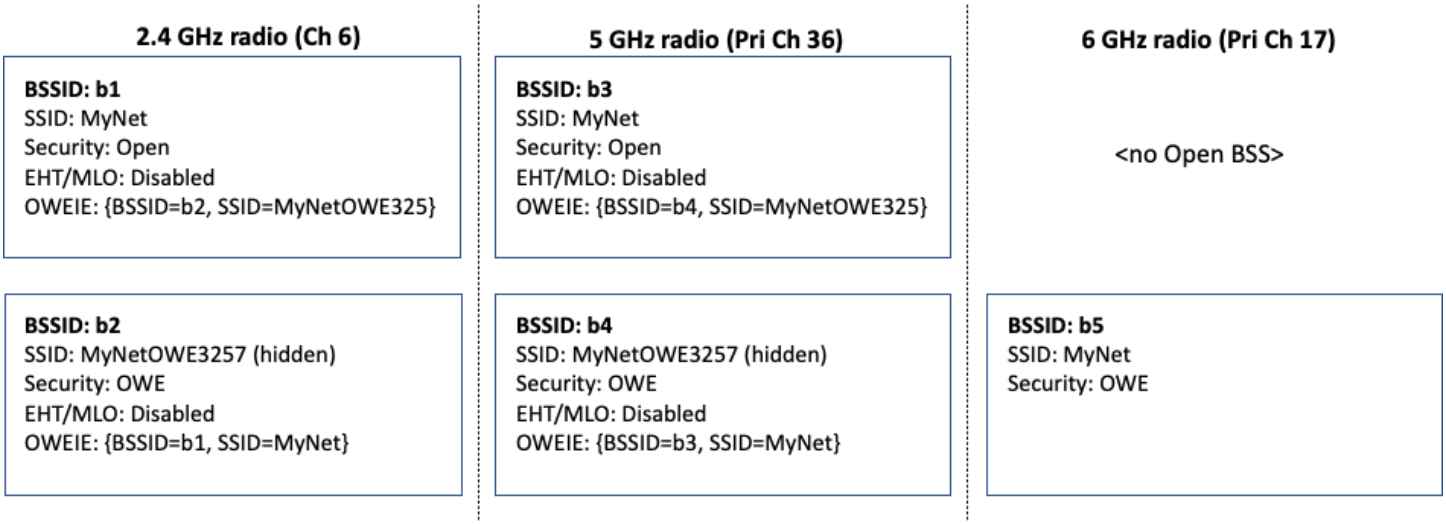

Figure 3. Example tri-band AP configuration using Wi-Fi Enhanced Open Transition Mode

A.4 Example tri-band AP configuration using Dual-SSID Wi-Fi Enhanced Open

If a Wi-Fi Enhanced Open network contains one or more AP MLDs, then Wi-Fi Enhanced Open Transition Mode cannot be used on those AP MLDs. If support for legacy STAs is required, all APs in the network should instead use the Dual-SSID configuration shown in Figure 4.

NOTE: Even for networks that do not contain AP MLDs, this Dual-SSID configuration might be preferred over Wi-Fi Enhanced Open Transition Mode, since STAs that support Wi-Fi Enhanced Open can roam across all BSSs in the network without changing SSID. On the other hand, since neither SSID is hidden, both SSIDs will appear in a STA's network picker. The end-user of a STA supporting Wi-Fi Enhanced Open should (preferably) manually select the OWE SSID. The end-user of a STA that does not support Wi-Fi Enhanced Open should manually select the Open SSID (and will not be able to connect if selecting the OWE SSID).

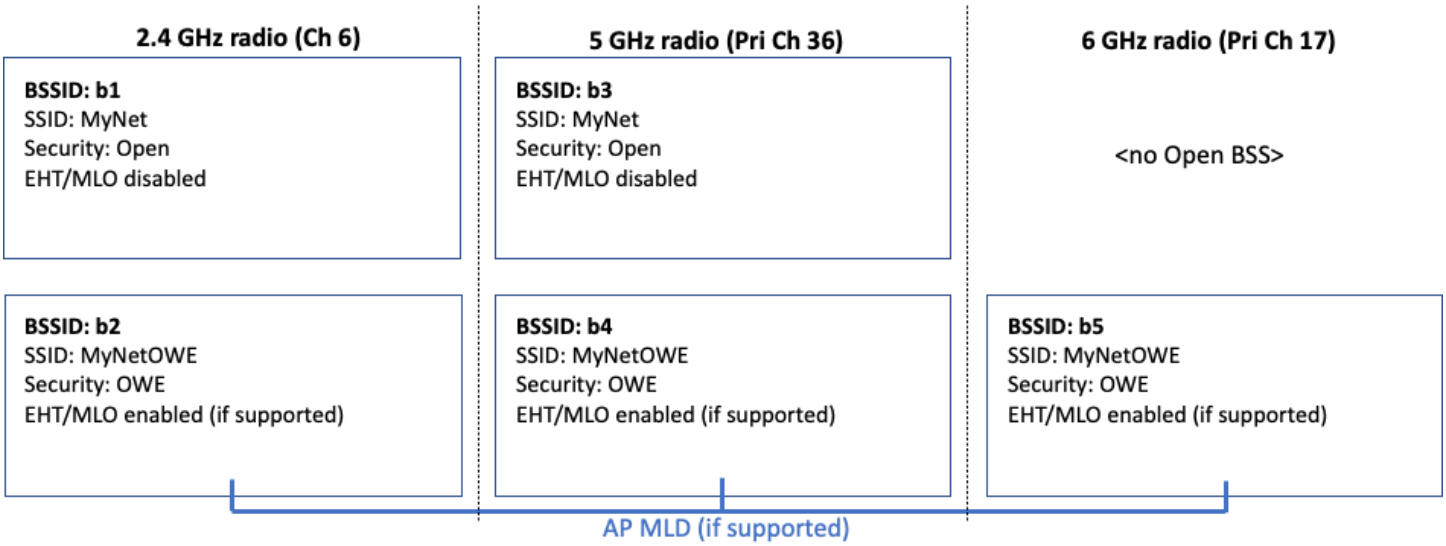

Figure 4. Example tri-band AP configuration using Dual-SSID Wi-Fi Enhanced Open

A.5 Example tri-band Dual-SSID WPA3-Personal configuration for legacy STA interoperability

Figure 5 shows an example Dual-SSID WPA3-Personal configuration for legacy STA interoperability on a 2.4+5+6 GHz tri-band AP. The configuration of BSSs b2, b4 and b5 is the same as shown in Figure 1. In addition, the AP operates BSSs b1 and b3 in 2.4 and 5 GHz bands, which have a different SSID, and are configured in WPA2-Personal mode (and therefore do not enable EHT or MLO).

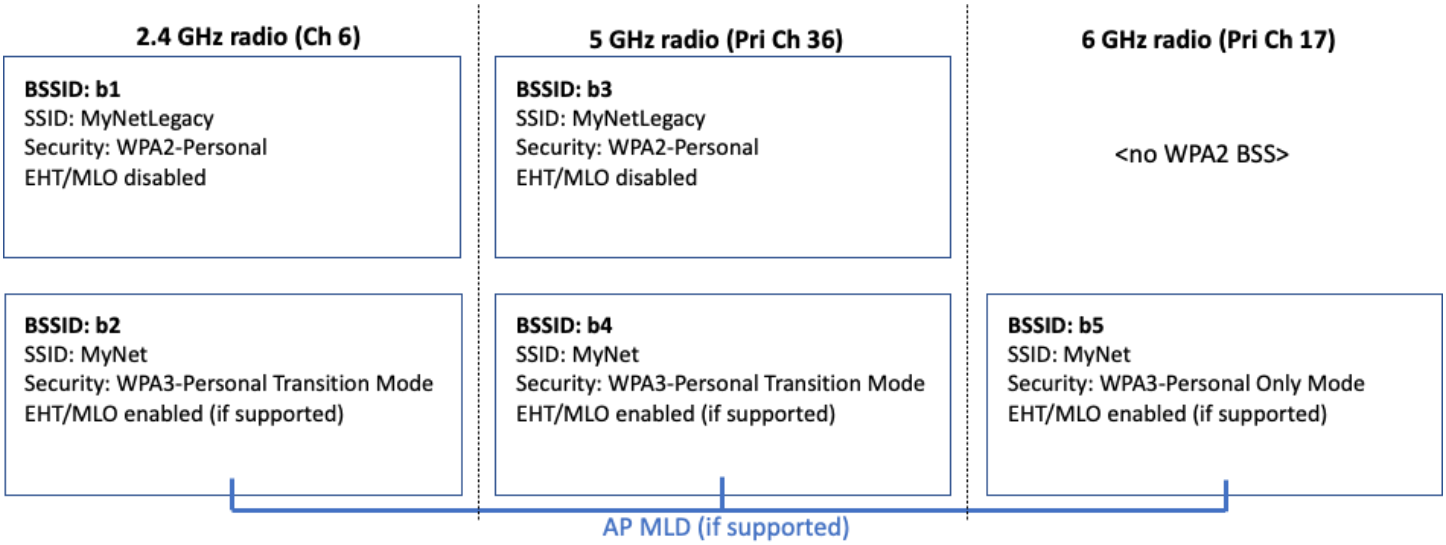

Figure 5. Example tri-band Dual-SSID WPA3-Personal configuration for legacy STA interoperability