Manuals+ — User Manuals Simplified.

ZEBRA WPA3 Integrator for Aruba WLAN Infrastructure User Guide

ZEBRA WPA3 Integrator for Aruba WLAN Infrastructure User Guide 📄

Contents

⋛ ZEBRA

ZEBRA WPA3 Integrator for Aruba WLAN Infrastructure

Specifications

- **Product**: Zebra WPA3 Integrator Guide for Aruba WLAN Infrastructure
- **Model Number**: MN-004378-03EN Rev A

Product Information

Zebra WPA3 is a wireless network security solution designed for integration with Aruba WLAN infrastructure. It supports WPA3-Personal and WPA3-Enterprise modes, offering enhanced security features for various network deployments.

Product Usage Instructions

Create a WPA3-Enterprise 256-Bit GCM Profile for Aruba Deployment:

Follow the detailed steps provided in section 3 of the manual to create a secure WPA3-Enterprise profile suitable for deployment in an Aruba WLAN infrastructure.

About WPA3:

WPA3 offers advanced security features compared to its predecessors, providing improved protection for wireless networks. It includes WPA3-Personal (SAE) and WPA3-Enterprise modes.

Supported Devices, Features, and Infrastructure Combinations:

Zebra WPA3 is compatible with various Zebra devices and has been validated on multiple Aruba infrastructure configurations. It offers different modes and suites to cater to different network security needs.

FAQ

- **Q:** What are the different modes supported by Zebra WPA3?
- **A:** Zebra devices with WPA3 support various modes including WPA3-Personal (SAE), WPA3-Enterprise, and Enhanced Open (OWE).
- **Q:** How can I transition to WPA3 from previous security protocols?
- **A**: For a seamless transition to WPA3, refer to the specific transition modes available for both WPA3-Personal and WPA3-Enterprise in the manual.

About WPA3

WPA3 is the next generation of Wi-Fi security, enabling robust authentication and increased cryptographic strength. WPA3 offers the following features:

- Does not allow outdated protocols.
- Requires use of Protected Management Frames (PMF).
- Backwards compatible with WPA2.
- Supports the following authentication modes:
- WPA3-Personal – Uses simultaneous authentication of equals (SAE)
- WPA3-Enterprise
- Enhanced Open – Based on opportunistic wireless encryption (OWE). Note that this is a separate Wi-Fi Alliance certification program and not WPA3.

WPA3-Personal (SAE)

WPA3-Personal uses the Simultaneous Authentication of Equals (SAE) protocol, replacing WPA2-Personal with Pre-shared Key (PSK). SAE is a variant of the Dragonfly protocol which uses a password-authenticated key exchange based on zero-knowledge proof. In SAE, passwords are used to determine a secret element in the negotiated group, called a password element (PWE). SAE is resistant to offline dictionary attacks. WPA3-Personal (SAE) has the following modes:

- WPA3-SAE Mode – Devices can only use WPA3-SAE mode and PMF is always required. Information is secured using discrete logarithm cryptography.
- WPA3-SAE Transition Mode – Provides backward compatibility for devices using WPA2. The access point (AP) uses WPA3-SAE Transition Mode to enable both WPA2-PSK and WPA3-SAE at the same time on a single basic service set (BSS). WPA (version 1)
- cannot be used and is not supported on the same BSS as WPA3-SAE. WEP and TKIP cannot be used and are not supported by WPA2-PSK when used on the same BSS as WPA3-SAE.

WPA3-Enterprise

WPA3-Enterprise is based on WPA2-Enterprise but requires Protected Management Frames (PMF) and does not allow outdated WEP and TKIP protocols. WPA3-Enterprise 192-bit Mode requires support for GCMP-256 and SHA384 ciphers.
WPA3-Enterprise has the following modes:

- WPA3-Enterprise only Mode – PMF is always required. WPA3-Enterprise devices negotiate PMF when connecting to an AP using WPA3-Enterprise only mode.
- WPA3-Enterprise Transition Mode – Provides backward combability for devices using WPA2-Enterprise. The

access point uses WPA3-Enterprise Transition Mode to enable both WPA2-Enterprise and WPA3-Enterprise at the same time on a single basic service set (BSS). WPA3-Enterprise devices negotiate PMF when connecting to an AP using WPA3-Enterprise transition mode.

- WPA3-Enterprise 192-bit Mode – PMF is set to required when WPA3-Enterprise 192-bit Mode is used by a client station (STA). The only 802.1X Authentication allowed is EAP-TLS.

Enhanced Open (OWE)

Opportunistic Wireless Encryption (OWE) is defined in the IETF document RFC 8110. OWE has the following modes:

- Enhanced Open OWE Mode – PMF is always required. To ensure interoperability, all STAs support group nineteen (19).
- Enhanced Open OWE Transition Mode – Allows both OWE STAs and non-OWE STAs to connect to the same distribution system at the same time.

Supported Devices, Features, and Infrastructure Combinations

WPA3 is supported on many Zebra devices and has been validated on several Aruba infrastructure combinations.

Supported Products

WPA3-Personal and WPA3-Enterprise are supported on the following Zebra devices running Android 10 or later.

- PS20
- TC52/TC52HC
- TC57
- TC72
- TC77
- MC93
- TC8300
- VC8300
- EC30
- ET51
- ET56
- L10
- CC600/CC6000
- MC3300x
- MC330x
- TC52x
- TC57x
- EC50 (LAN)
- EC55 (WAN)
- WT6300
- TC21

- TC26
- MC22
- MC27
- TC21 -HC
- TC26 -HC
- MC20
- RZ-H271
- TC52ax
- MC33AX
- TC52L

Supported WPA3 Capabilities

Zebra devices with WPA3 support many modes or suites.

Modes or Suites	Supported Capabilities
WPA3-Personal Modes	WPA3-Personal (SAE) WPA3-Personal Transition Mode WPA3-Personal Fast Transition
AKM Suites for Personal Modes	FT Authentication using SAE: 00-0F-AC:9 SAE Authentication: 00-0F-AC:8 FT Authentication using PSK: 00-0F-AC:4 PSK using SHA-256: 00-0F-AC:6 PSK: 00-0F-AC:2
WPA3-Enterprise Modes	WPA3-Enterprise WPA3-Enterprise Fast Transition WPA3-Enterprise 192-bit Mode WPA3-Enterprise 192-bit Mode Fast Transition
AKM Suites for Enterprise Modes	FT Authentication using IEEE Std 802.1X (SHA 256): 00-0F-AC:3 Authentication using IEEE Std 802.1X (SHA256): 00-0F-AC:5 Authentication using IEEE Std 802.1X: 00-0F-AC:1
AKM Suites for Enterprise 192-bit Modes	FT Authentication using IEEE Std 802.1X (SHA 384) 00-0F-AC:13 Authentication using IEEE Std 802.1X using a Suite B EAP method supporting SHA-384: 00-0F-AC:12
Cipher Suites	AES-CCMP 128: 00-0F-AC:4

Modes or Suites	Supported Capabilities
	GCMP-256: 00-0F-AC:9
Group Management Cipher Suites	BIP-CMAC-128: 00-0F-AC:6 BIP-GMAC-256: 00-0F-AC:12

WPA3 Features Validated on Aruba

The following features are validated on an Aruba infrastructure using a supported Zebra device.

- Enhanced open
- Enhanced open transition
- SAE-personal
- SAE-personal-transition
- Enterprise-128ccm
- Enterprise-256gcm
- WPA3-casa-192bit

Validation was performed using the following Aruba infrastructure:

- Controller Model – 7010 & 72xx Controller series
- AP Model – 3xx & 5xx AP series
- Software Version – ArubaOS_70xx_8.8.0.1_80393
- Software Version – ArubaOS_72xx_8.8.0.1_80393

AKM and suite-type combinations

This section describes each security combination configured on the infrastructure and device and the corresponding AKM type or Suite type over the air.

Security Combination on the Device/Infrastructure	AKM Type/Suite Type over the Air
Enhanced open	Group Cipher Suite type: AES (CCM) (4) Pairwise Cipher Suite type: AES (CCM) (4) Auth Key Management (AKM) type: Opportunistic Wireless Encryption (18) Group Management Cipher Suite type: BIP (128) (6)
Enhanced open-transition	Group Cipher Suite type: AES (CCM) (4) Pairwise Cipher Suite type: AES (CCM) (4) Auth Key Management (AKM) type: Opportunistic Wireless Encryption (18) Group Management Cipher Suite type: BIP (128) (6) Vendor Specific: Wi-Fi Alliance: OWE Transition Mode

Security Combination on the Device/Infrastructure	AKM Type/Suite Type over the Air
SAE -personal	AKM Type : SAE (SHA256) (8) Group Cipher Suite type: AES (CCM) (4) Pairwise Cipher Suite type: AES (CCM) (4) Group Management Cipher Suite type: BIP (128) (6) FT CONNECTION: Auth Key Management (AKM) type : SAE (SHA256) (8) Auth Key Management (AKM) type: FT using SAE (SHA256) (9) Group Cipher Suite type: AES (CCM) (4) Pairwise Cipher Suite type: AES (CCM) (4) Group Management Cipher Suite type: BIP (128) (6)
SAE -personal-transition	AKM Type : PSK (2) AKM Type : SAE (SHA256) (8) Group Cipher Suite type: AES (CCM) (4) Pairwise Cipher Suite type: AES (CCM) (4) Group Management Cipher Suite type: BIP (128) (6)
Enterprise-128ccm	Auth Key Management (AKM) type: WPA (1) Group Cipher Suite type: AES (CCM) (4) Pairwise Cipher Suite type: AES (CCM) (4) Group Management Cipher Suite type: BIP (128) (6)
Enterprise-256gcm	Group Cipher Suite type: GCMP (256) (9) Pairwise Cipher Suite type: GCMP (256) (9) Auth Key Management (AKM) type: WPA (SHA256) (5) Group Management Cipher Suite type: BIP (GMAC-256) (12) FT CONNECTION: Group Cipher Suite type: GCMP (256) (9) Pairwise Cipher Suite type: GCMP (256) (9) Auth Key Management (AKM) type: WPA (SHA256) (5) Auth Key Management (AKM) type: FT over IEEE 802.1X (3) Group Management Cipher Suite type: BIP (GMAC-256) (12)
WPA3-192bit	Group Cipher Suite type: GCMP (256) (9) Pairwise Cipher Suite type: GCMP (256) (9) Auth Key Management (AKM) type: WPA (SHA384-SuiteB) (12) Group Management Cipher Suite type: BIP (GMAC-256) (12)

Flow Charts for WPA3 Authentication

This section contains flow charts describing WPA3-based authentication.

WPA3-SAE Authentication Flow Chart

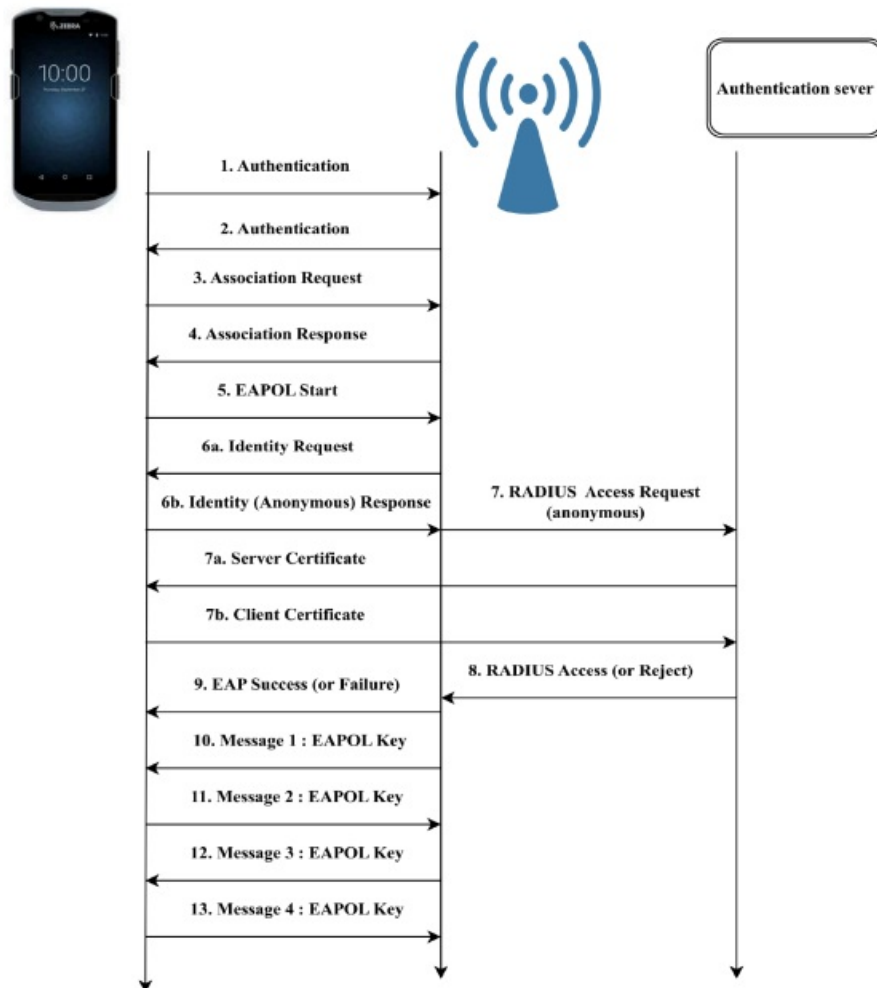Flow chart demonstrating the WPA3-SAE authentication workflow.

Figure 1   WPA3-SAE Authentication Flow Chart
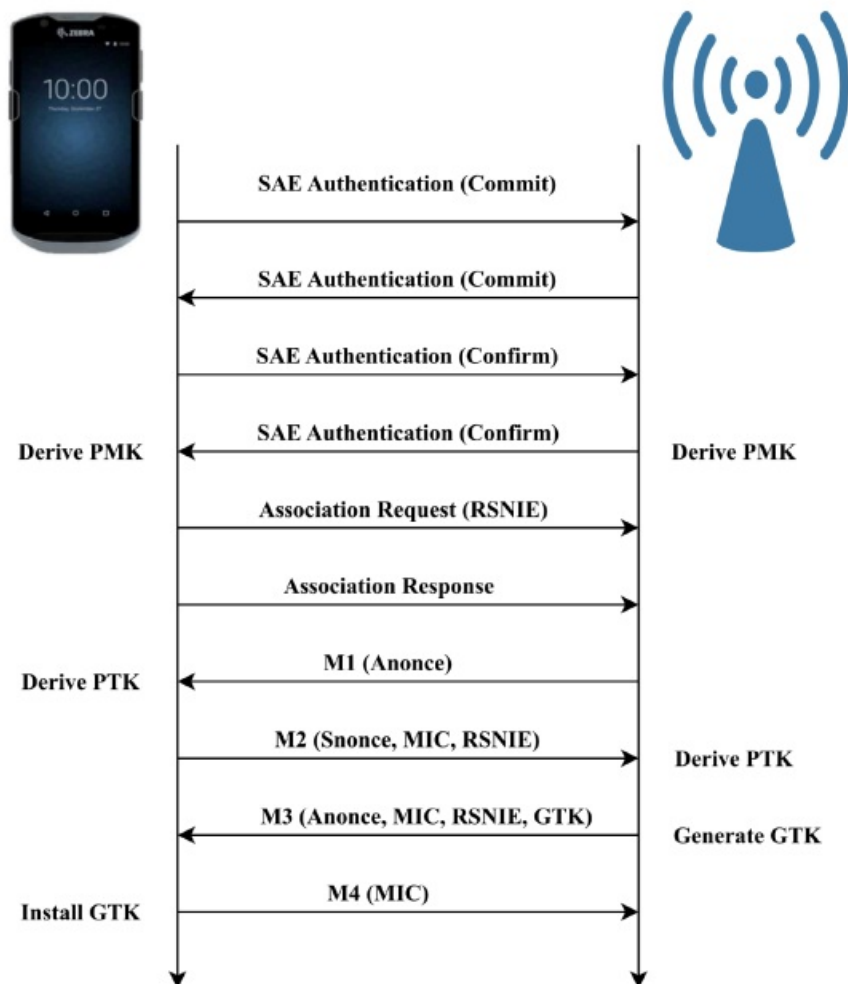
WPA3-Enterprise EAP-TLS Flow Chart

Flow chart demonstrating the WPA3-Enterprise EAP-TLS authentication workflow.

Figure 2 WPA3-Enterprise EAP-TLS Flow Chart

1. Authentication

2. Authentication

3. Association Request

4. Association Response

5. EAPOL Start

6a. Identity Request

6b. Identity (Anonymous) Response

7. RADIUS Access Request (anonymous)

7a. Server Certificate

7b. Client Certificate

8. RADIUS Access (or Reject)

9. EAP Success (or Failure)

10. Message 1 : EAPOL Key

11. Message 2 : EAPOL Key

12. Message 3 : EAPOL Key

13. Message 4 : EAPOL Key

Authentication sever

Enhanced Open OWE Flow Chart

Flow chart demonstrating the Enhanced Open OWE authentication workflow.

Figure 3 Enhanced Open OWE Flow Chart
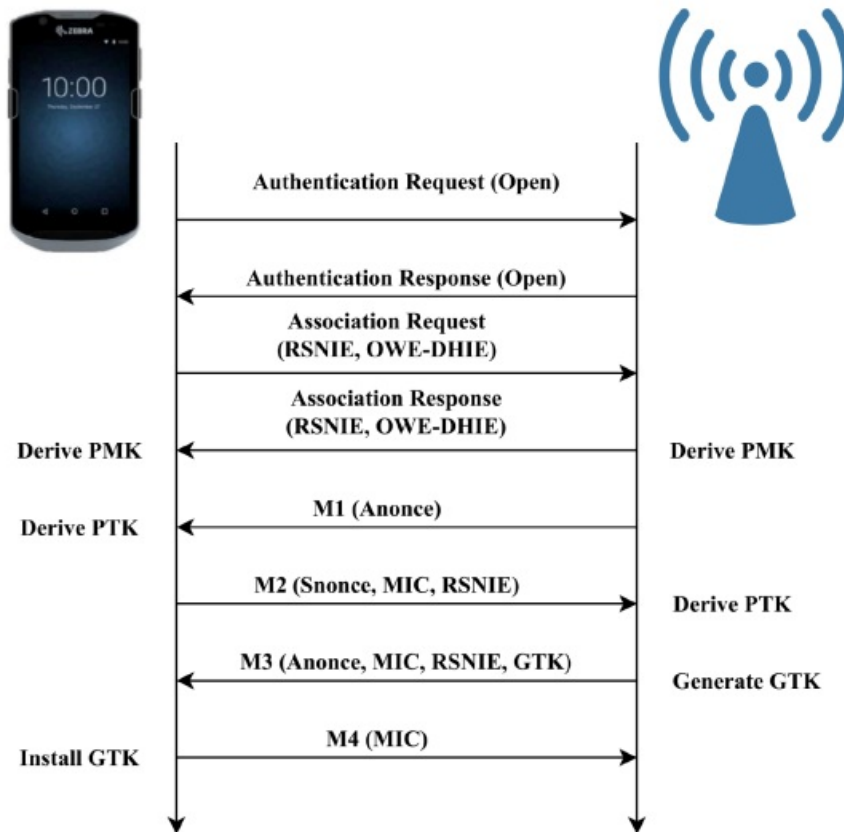
WPA3 Profiles for Aruba Deployment

Create WPA3 profiles on an Aruba infrastructure.

- WPA3-SAE
- WPA3-SAE Transition
- WPA3-Enterprise 128-Bit CCM
- WPA3-Enterprise 256 Bit GCM
- WPA3-Enterprise 192 Bit
- Enhanced Open
- Enhanced Open Transition.

NOTE: To enable 802.11r/FT, ensure the Advertise 802.11r Capability is enabled for the SSID. It is then automatically applicable as a WPA3 FT profile if the selection from the above-mentioned options is WPA3.

Create a WPA3-SAE Profile for Aruba Deployment

Create a WPA3-SAE WLAN profile in Aruba and configure the network on the device.

Creating a WPA3-SAE Profile in Aruba

1. In Aruba, create a WLAN profile.
2. Set Key Management to WPA3-Personal.
3. Ensure that Enable backward Compatibility is unchecked.

Configuring a WPA3-SAE Network on the Device

1. On the device, enter the SSID Name in the Network name field.
2. In the Security field, select WPA3-Personal.
3. In the Password field, enter the password.

Figure 4 Android 10/11
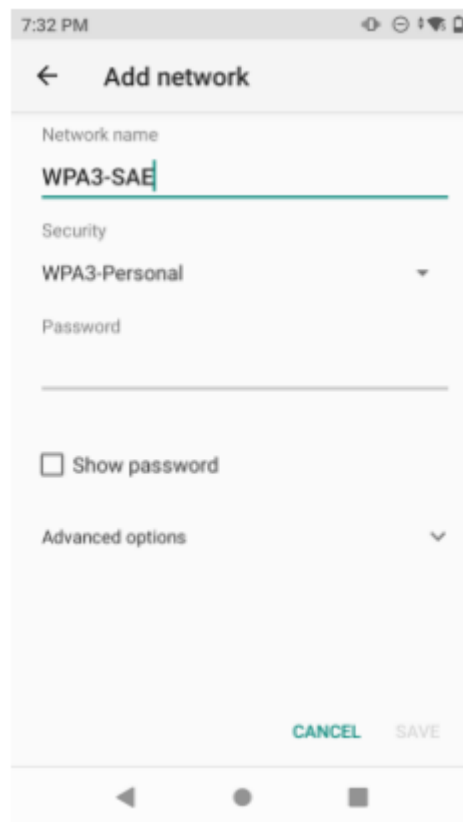
Create a WPA3-SAE Transition Profile for Aruba Deployment

Create a WPA3-SAE Transition WLAN profile in Aruba and configure the network on the device.

Creating a WPA3-SAE Transition Profile in Aruba

1. In Aruba, create a WLAN profile.
2. Set Key Management to WPA3-Personal.
3. Ensure that Enable backward Compatibility is checked.

Configuring a WPA3-SAE Transition Network on the Device

1. On the device, enter the SSID Name in the Network name field.
2. In the Security field, select WPA3-Personal.
3. In the Password field, enter the password.

Figure 5 Android 10/11
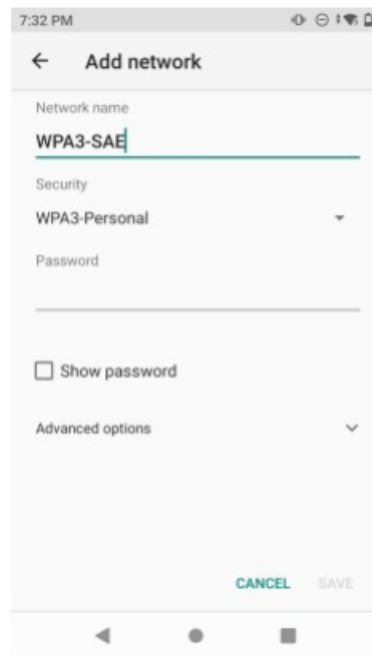
Create a WPA3-Enterprise 128-Bit CCM Profile for Aruba Deployment

Create a WPA3-Enterprise 128-bit CCM profile in Aruba and configure the network on the device.

Creating a WPA3-Enterprise 128-Bit CCM Profile in Aruba

1. In Aruba, create a WLAN profile.
2. Set Key Management to WPA3-Enterprise.
3. Set Key Size to 128 Bits.

Configuring a WPA3-Enterprise 128 Bit CCM Network on the Device

1. On the device, enter the SSID Name in the Network name field.
2. In the Security field, select WPA/WPA2/WPA3-Enterprise.
3. Select the desired EAP method.
4. Set the remaining fields as required.

Figure 6 Android 10
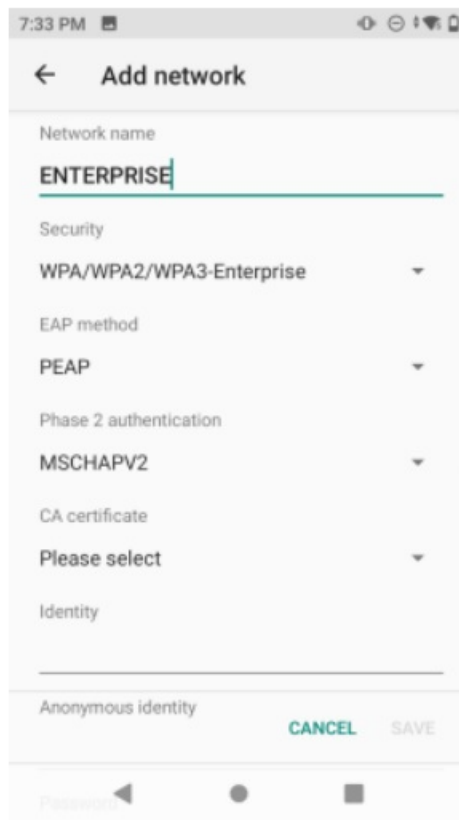
Figure 7 Android 11
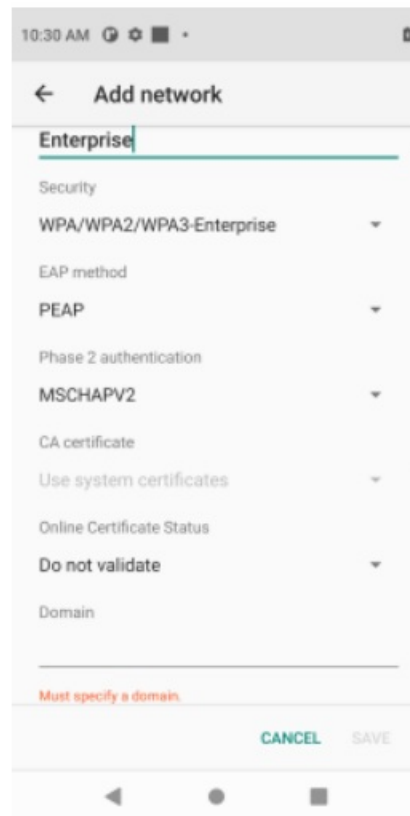
NOTE: Domain Name should be the same as the Common Name in server Certificate.

Create a WPA3-Enterprise 256-Bit GCM Profile for Aruba Deployment

Create a WPA3-Enterprise 256 Bit GCM profile in Aruba and configure the network on the device.

Creating a WPA3-Enterprise 256-Bit GCM Profile in Aruba

1. In Aruba, create a WLAN profile.
2. Set Key Management to WPA3-Enterprise.
3. Set Key Size to 256 Bits.

Configuring a WPA3 Enterprise 256-Bit Network on the Device

1. On the device, enter the SSID Name in the Network name field.
2. In the Security field, select WPA/WPA2/WPA3-Enterprise.
3. Select the desired EAP method.
4. Set the remaining fields as required.

Figure 8 Android 10
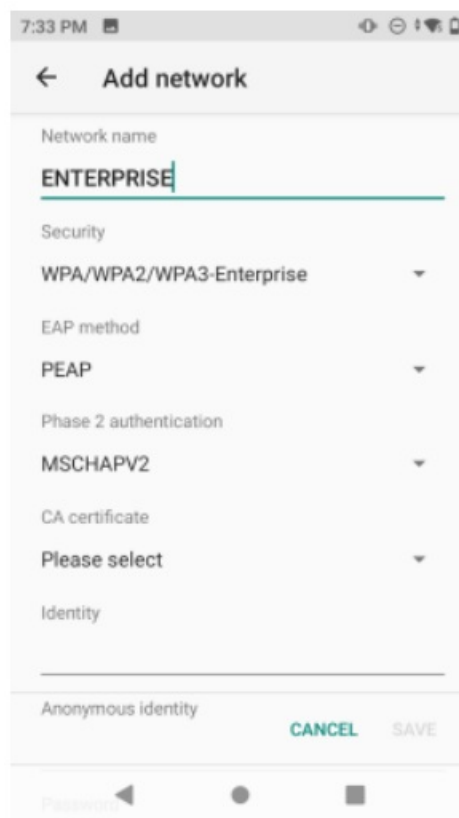
Figure 9 Android 11
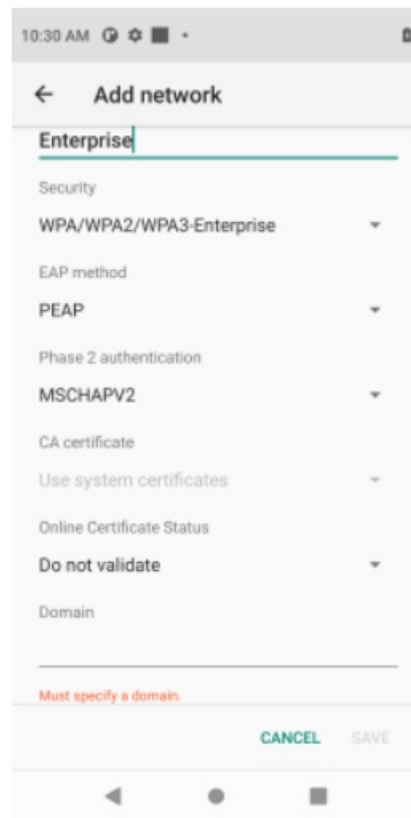
NOTE: Domain Name should be the same as the Common Name in server Certificate.

Create a WPA3-Enterprise 192-Bit Profile for Aruba Development

Create a WPA3-Enterprise 192 Bit profile in Aruba and configure the network on the device.

Creating a WPA3-Enterprise 192 Bit Profile in Aruba

1. In Aruba, create a WLAN profile.
2. Set Key Management to WPA3-Enterprise.
3. Ensure that Use CNSA Suite is checked.

Configuring WPA3 Enterprise 192-Bit Network On the Device

1. On the device, enter the SSID Name in the Network name field.
2. In the Security field, select WPA3-Enterprise 192-bit.
3. Set the remaining fields as required.

Figure 10 Android 10
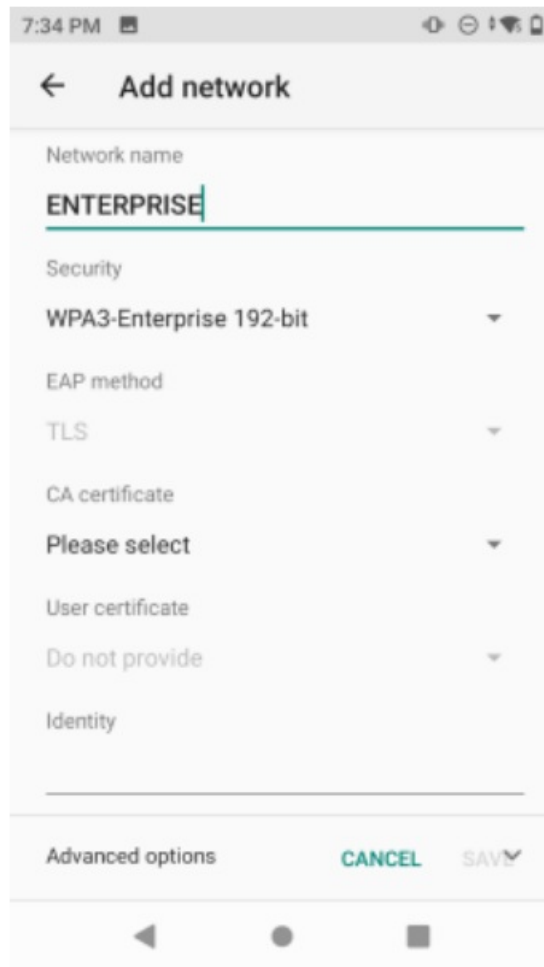
Figure 11 Android 11
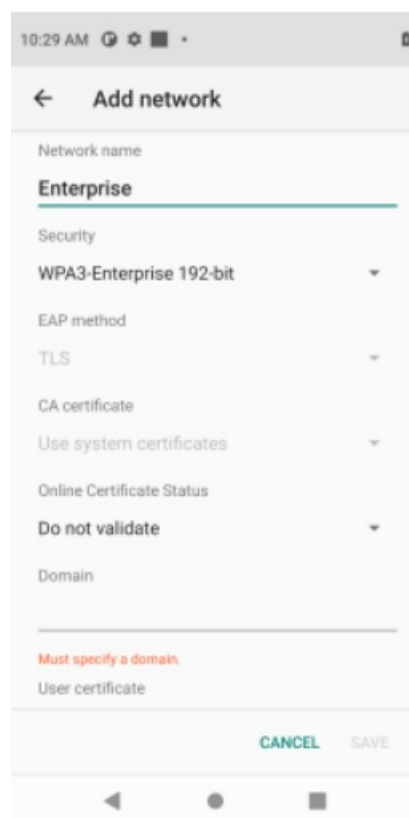
NOTE: Domain Name should be the same as the Common Name in server Certificate.

Create an Enhanced Open Profile for Aruba Deployment

Create an Enhanced Open profile in Aruba and configure the network on the device.

Creating an Enhanced Open Profile on Aruba

1. In Aruba, create a WLAN profile.
2. Set Security to Enhanced Open.
3. Ensure that Enable Backward Compatibility is unchecked.

Configuring an Enhanced Open Network on the Device.

1. On the device, enter the SSID Name in the Network name field.
2. In the Security field, select Enhanced Open.

Figure 12 Android 10/11
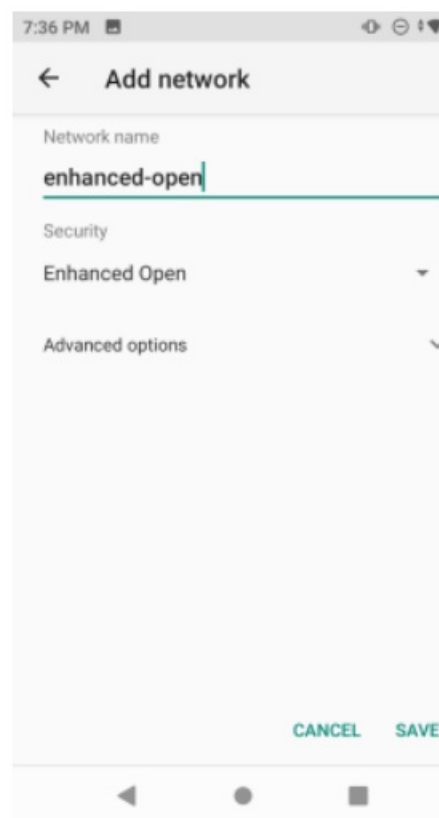
Create an Enhanced Open Transition Profile for Aruba Deployment

Create an Enhanced Open Transition profile in Aruba and configure the network on the device.

Creating an Enhanced Open Transition Profile on Aruba

1. In Aruba, create a WLAN profile.

2. Set Security to Enhanced Open.

3. Ensure that Enable Backward Compatibility is checked.

Configuring an Enhanced Open Transition Network on the Device

1. On the device, enter the SSID Name in the Network name field.

2. In the Security field, select Enhanced Open

Figure 13 Android 10/11
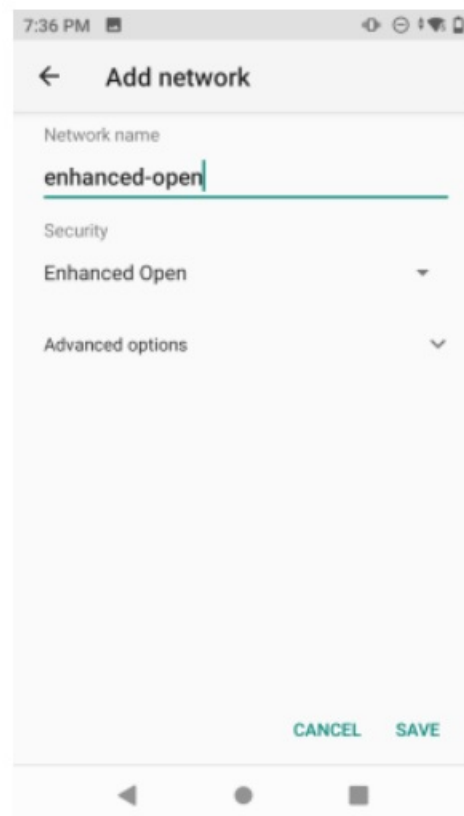
Client Certificate Requirements for WPA3 Profiles

Make sure to follow the client certificate requirements for WPA3 profiles and use the correct digital signature algorithm.v WPA3-Enterprise 192-bit uses EAP-TLS authentication with the following TLS ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- ECDHE and ECDSA using the 384-bit prime modulus curve P-384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ECDHE using the 384-bit prime modulus curve P-384
- RSA ≥ 3072-bit modulus

To comply with the above requirements, the client certificate should use one of the following digital signature algorithms:

- ECDSA: Elliptic curve digital signature algorithm
- RSA encryption with a minimum key size of 3072 bits

Our Zebra devices support

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384: This is mandatory
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384: This is optional
- There is no fallback mechanism from one cipher to another.

For the mandatory TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher, the certificates must be:

- Key: elliptic curve with P-384 curve i.e., ASN1 OID: secp384r1, NIST CURVE: P-384
- Signature algorithm: ecdsa-with-SHA384

For the optional TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 cipher, the certificates must be:

- Key: use RSA with 3072 bits or more
- Signature algorithm: sha384WithRSAEncryption

The cipher rules apply to all certificates starting from the CA certificate, any intermediate certificates (if used) and up to the client and server certificates. This means that 192-bit mode does not allow weaker CA certificates to sign stronger server/client certificates or mix RSA CA certificates to sign EC certificates.

WPA3 Abbreviations

The following abbreviations are used in this guide.

- **AES**

  Advanced Encryption Standard
- **AKM**

  Authentication and Key Management
- **AP**

  Access Point
- **BIP**

  Broadcast Integrity Protocol
- **BSS**

  Basic Service Set
- **CCMP**

  Counter Mode Cipher Block Chaining Message Authentication Code Protocol
- **FT**

  Fast Transition
- **GMAC**

  Galois Message Authentication Code
- **OWE**

  Opportunistic Wireless Encryption
- **PMF**

  Protected Management Frames
- **PWE**

Password Element

- **PSK**

  Pre-Shared Key

- **SAE**

  Simultaneous Authentication of Equals

- **SHA**

  Secure Hash Algorithms

- **STA**

  Client Station

- **WPA**

  Wi-Fi Protected Access

business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Documents / Resources

Zebra WPA3 WPA3 Integrator Guide for Aruba WLAN Infrastructure	**[ZEBRA WPA3 Integrator for Aruba WLAN Infrastructure](#)** [pdf] User Guide WPA3, WPA3 Integrator for Aruba WLAN Infrastructure, Integrator for Aruba WLAN Infrastructure, Aruba WLAN Infrastructure, WLAN Infrastructure, Infrastructure

References

- **[User Manual](#)**