The bridge to possible

WPA3 Deployment Guide

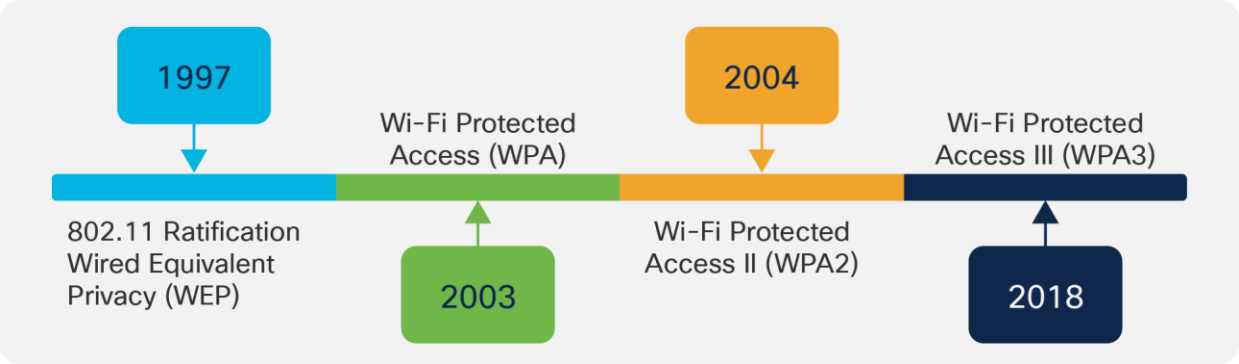
© 2024 Cisco and/or its affiliates. All rights reserved.

Introduction to WPA3

WPA3 is the third and latest iteration of the Wi-Fi Protected Access standard developed by the Wi-Fi Alliance and replaces the previous standard, WPA2. The WPA standard was created by the Wi-Fi Alliance security technical task group, chaired by Cisco's Stephen Orr, with the purpose of standardizing wireless security. WPA3 introduces new features on enterprise, personal, and open security networks through an increase in cryptographic strength, allowing for a more secure authentication process for all WPA3-supported endpoints. The WPA3 Enterprise form extends the solid foundation provided by WPA2 Enterprise by making it mandatory to use Protected Management Frames (PMF) on all connections. This security feature protects against such dangerous attacks as Denial of Service (DoS), honeypots, and eavesdropping.

Over the next few years, Cisco expects the industry to see an exponential increase in WPA3 adoption, especially in government and financial institutions. With the number of internet-connected devices forecasted to reach 41.6 billion in four years, there is an implicit need for better security, and WPA3 is the answer.

Figure 1. Wi-Fi Security Standards Timeline



Supported WPA3 Modes

- WPA3-Enterprise, for 802.1X security networks. This leverages IEEE 802.1X with SHA-256 as the Authentication and Key Management (AKM).
- WPA3-Personal, which uses the Simultaneous Authentication of Equals (SAE) method for personal security networks.
- WPA3 Transition Mode (WPA2+WPA3 security-based WLANs for both personal and enterprise). {Starting 17.12.1, this can be used with 1 SSID and 1 Profile and support 6GHz band.}
- Opportunistic Wireless Encryption (OWE) for open security networks.

Road-mapped WPA3 Features

- WPA3-Enterprise 802.1X-256 in FlexConnect Mode
- WPA3-Enterprise SuiteB192-1X in FlexConnect Mode
- WPA3-Enterprise SuiteB192-1X Fast Transition

Required Software Versions

1. For WPA3-Personal SAE hash-to-element method for password element generation - minimum software version 17.7.1 should be used.
2. For WPA3-Enterprise and WPA3-Personal Transition disabled - minimum software version 17.7.1 should be used.

© 2024 Cisco and/or its affiliates. All rights reserved.

3. For WPA3-Personal with SAE as AKM + Fast Transition (FT) - minimum software version 17.9 should be used.

Cisco Device Compatibility

Table 1. Cisco® Catalyst® 9800 Series Wireless Controller WPA3 support matrix

9800-L-F	9800-L-C	9800-L	9800-40	9800-80
Yes, starting with 16.12.1s	Yes, starting with 16.12.1s	Yes, starting with 16.12.1s	Yes, starting with 16.12.1s	Yes, starting with 16.12.1s

Table 2. Catalyst 9100 Access Points WPA3 support matrix

9105AX	9115AX	9117AX	9120AX	9130AX	9124AXE	9136AX	9166/9164/9162
Yes*	Yes*	Yes*	Yes*	Yes	Yes	Yes	Yes

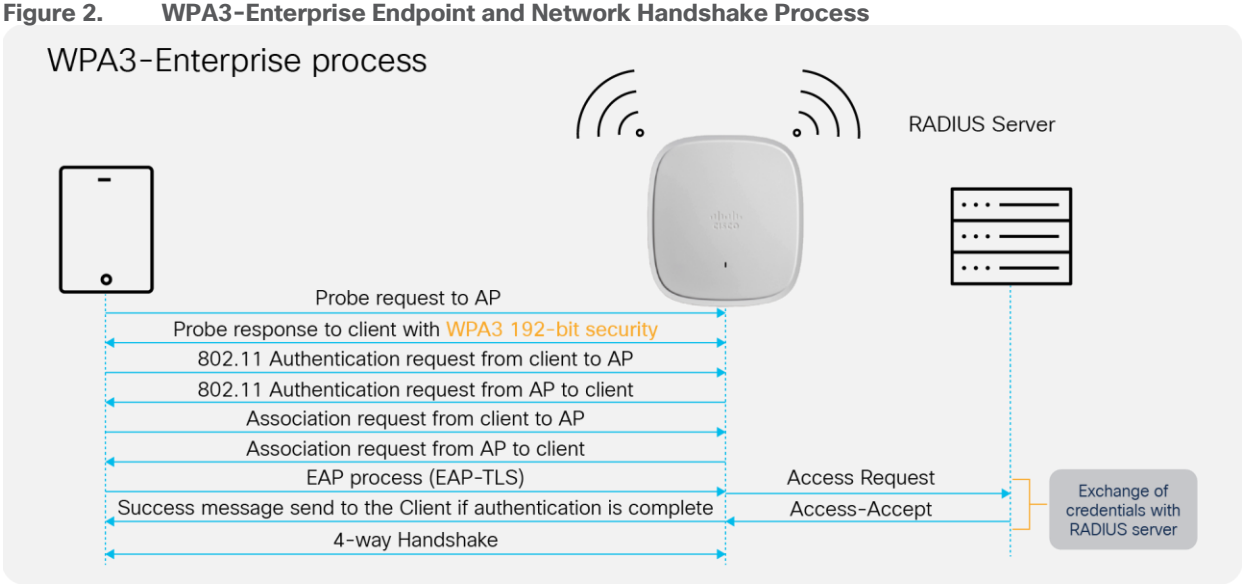
*SuiteB192-1X is not supported

The purpose of this deployment guide is to provide details of the different WPA3 modes and steps to configure them on the Cisco Catalyst 9800 Series controller, using either the GUI or the Command-Line Interface (CLI).

WPA3-Enterprise

WPA3-Enterprise builds upon the foundation of WPA2-Enterprise with the additional requirement of using Protected Management Frames on all WPA3 connections with 802.1X for user authentication with a RADIUS server. By default, WPA3 uses 128-bit encryption, but it also introduces an optionally configurable SuiteB-192 bit cryptographic strength encryption using GMCP-256, which gives additional protection to any network transmitting sensitive data. The WPA3-Enterprise is highly preferred and recommended to be used and commonly seen in enterprises, financial institutions, government, and other market sectors where network security is most critical.

Figure 2. WPA3-Enterprise Endpoint and Network Handshake Process



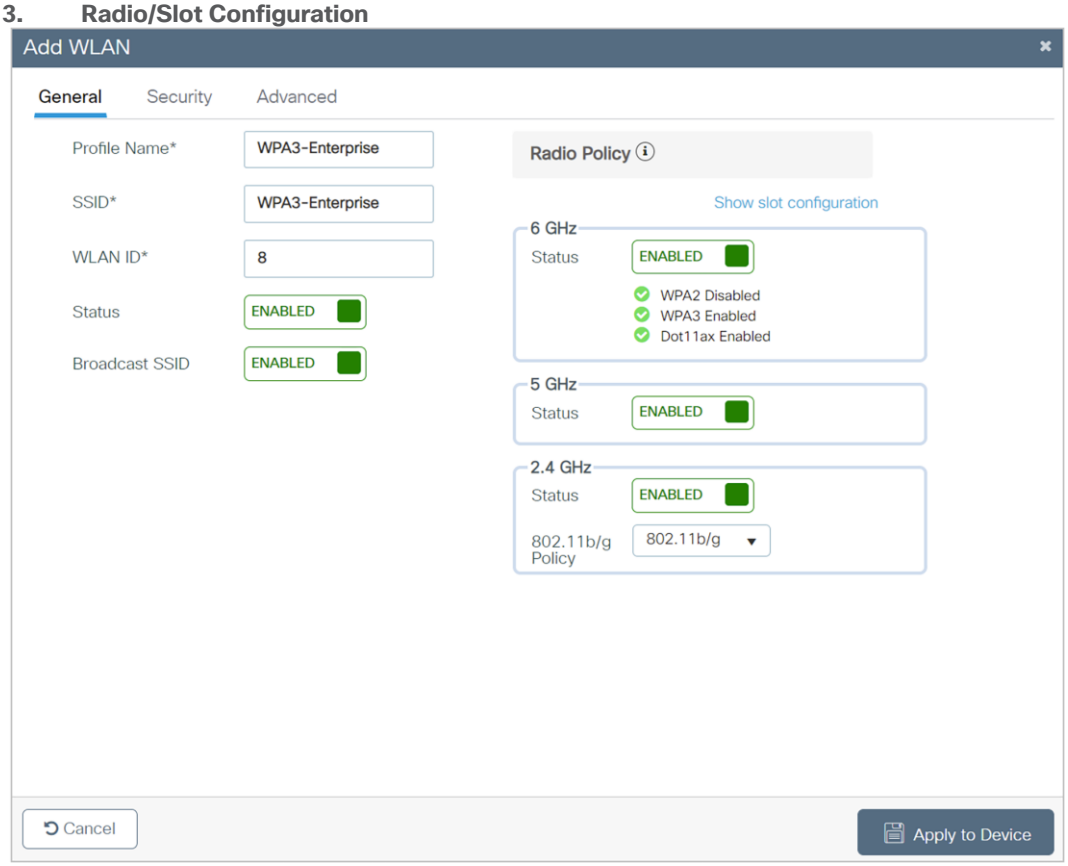
© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Enterprise GUI Configuration

The following steps create a WLAN with WPA3-Enterprise security:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). Both the SSID and WLAN ID are populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.

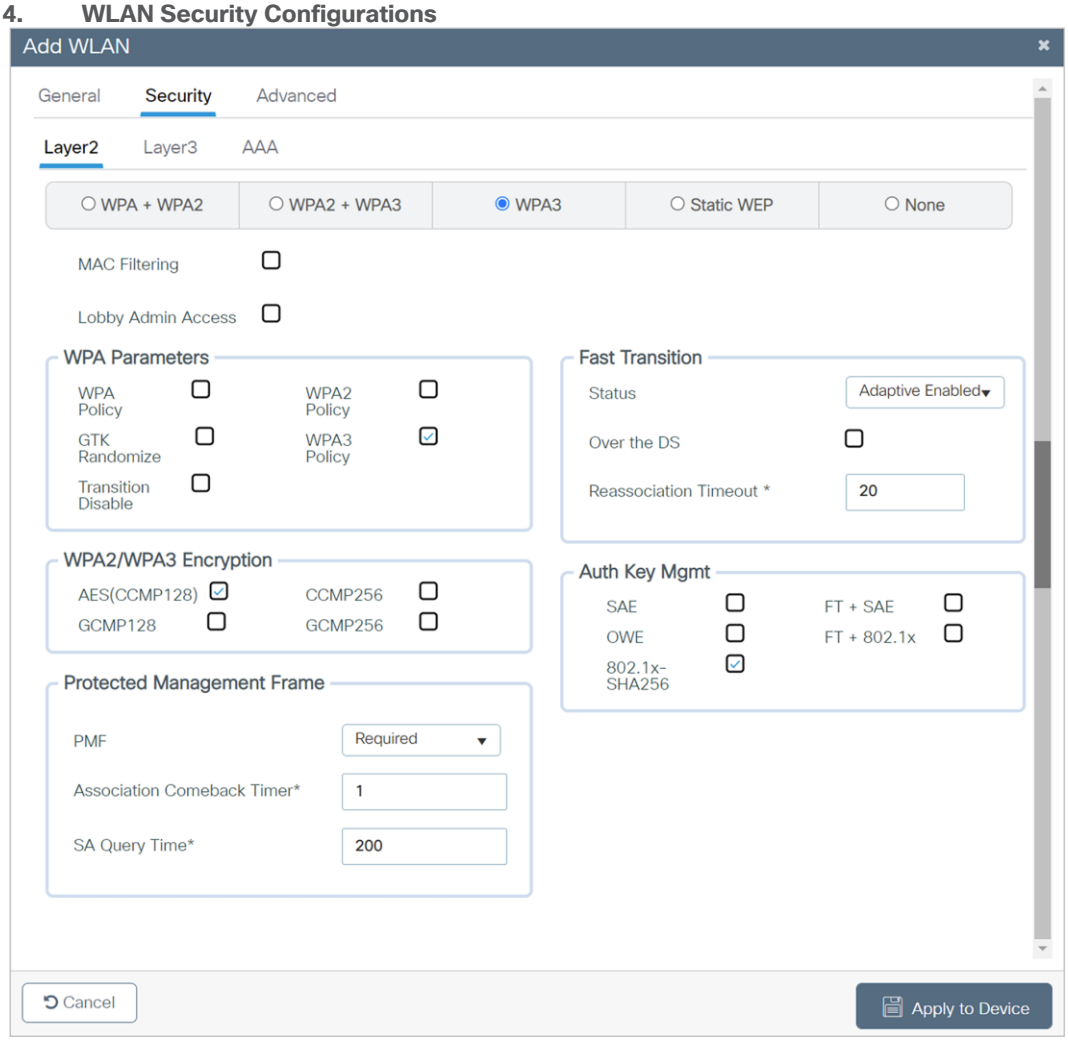
Figure 3. Radio/Slot Configuration



5. Click the **Security** tab > **Layer 2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA3**.
6. Confirm that the **PMF** is set to **Required**.

© 2024 Cisco and/or its affiliates. All rights reserved.

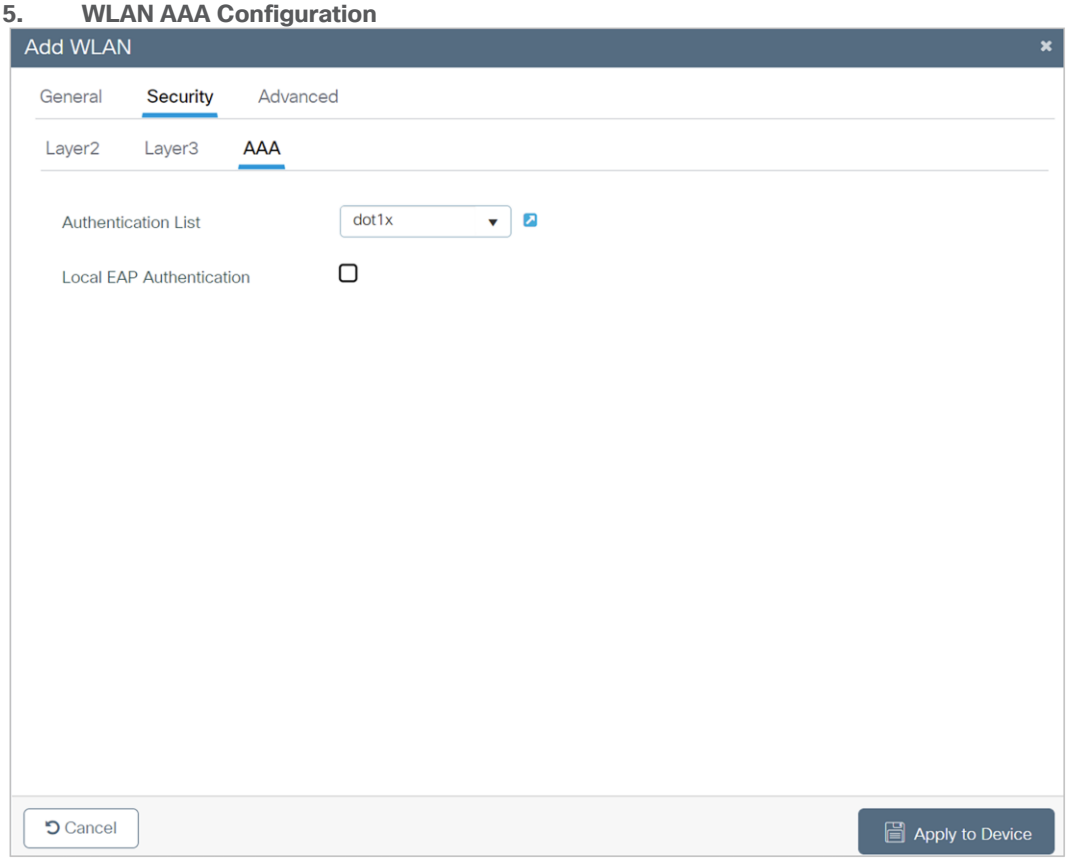
Figure 4. WLAN Security Configurations



7. Check the **WPA3 Policy, AES**, and **802.1X-SHA256** check boxes, then unselect any other selected parameters.
8. Click the **Security** tab and click the **AAA** tab and from the **Authentication List** drop-down list, choose the preconfigured RADIUS Server Authentication List.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 5. WLAN AAA Configuration



9. Click **Apply to Device** to save and finish the WLAN creation process.

WPA3-Enterprise CLI Configuration

The following steps create a WLAN with WPA3-Enterprise security:

Table 3. WPA3-Enterprise CLI Configuration

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan WPA3-Enterprise 8 WPA3-Enterprise`
		Enters the WLAN configuration sub-mode.

Step 3	`no security wpa akm dot1x`	Disables Security Auth Key Management (AKM) 802.1X-SHA1.
Step 4	`no security wpa wpa2`	Disables WPA2 security.
Step 5	`security wpa akm dot1x-sha256`	Enables Security Auth Key Management (AKM) 802.1X-SHA2.
Step 6	`security wpa wpa3`	Enables WPA3 support.

© 2024 Cisco and/or its affiliates. All rights reserved.

	Command	Purpose

Step 7	`security dot1x authentication-list list-name`
	Example:
	`Device(config-wlan)# security dot1x authentication-list dot1x`
		Configures security authentication list for 802.1X security.

Step 8	`no shutdown`	Enables the WLAN.
Step 9	`end`	Returns to the privileged EXEC mode.

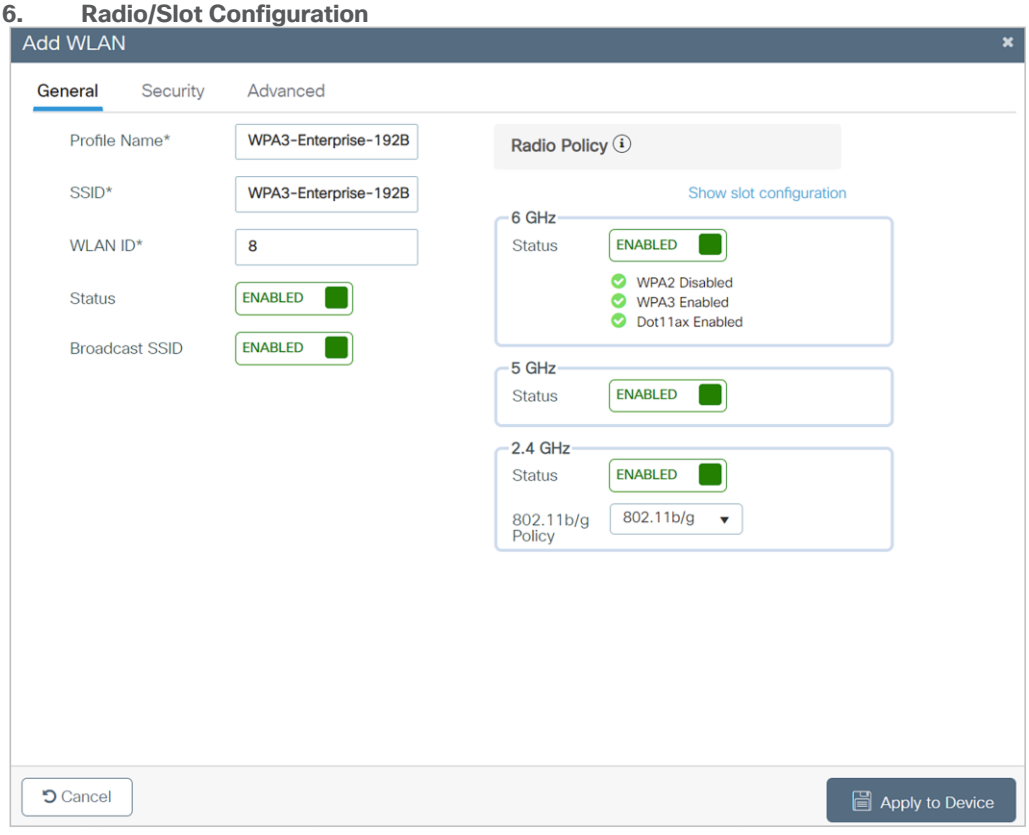
WPA3-Enterprise 192-bit GUI Configuration (optional)

For endpoints that support SuiteB192-1X encryption, refer to the client interoperability matrix section below, or reach out to the device vendor.

The following steps create a WLAN with 192-bit WPA3-Enterprise security:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). Both the SSID and WLAN ID are populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.

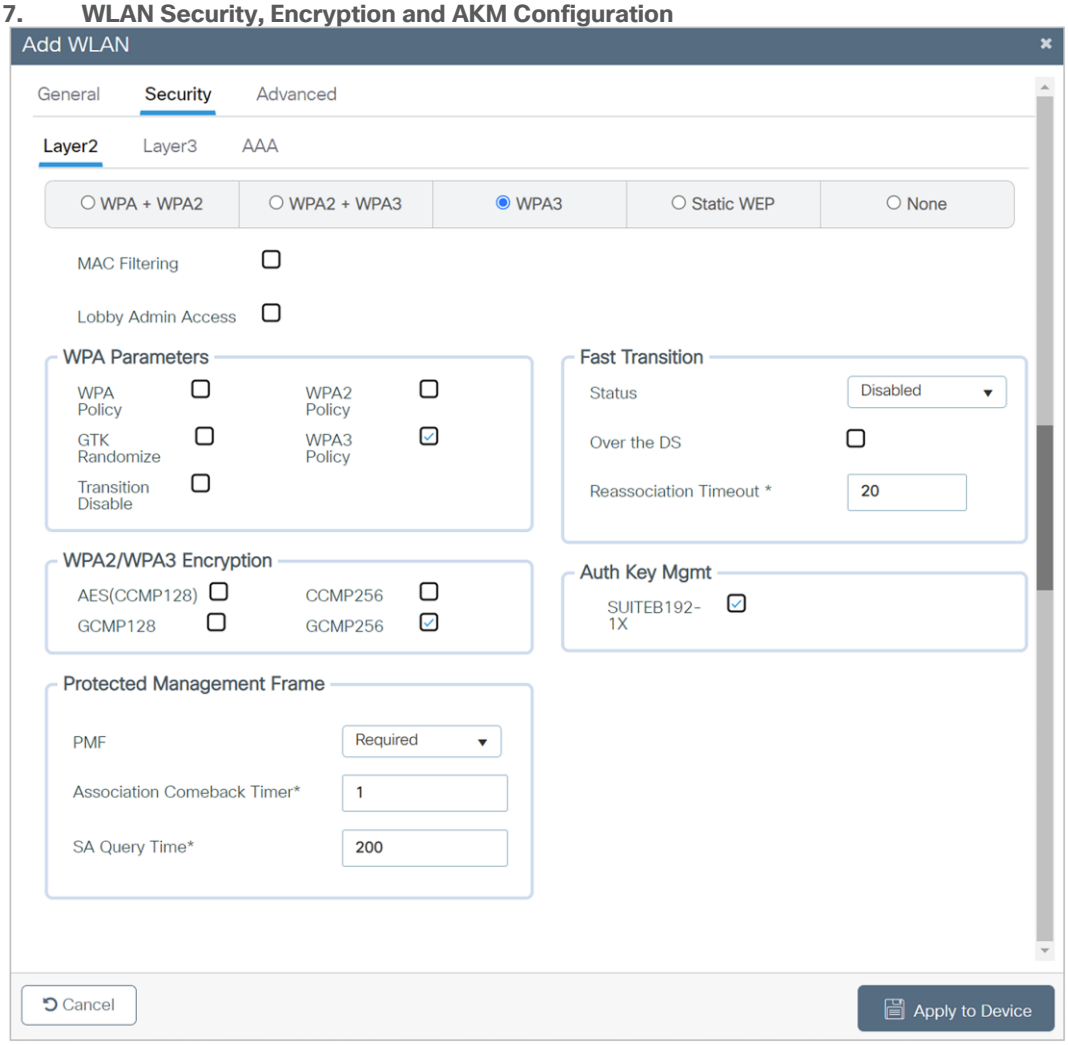
Figure 6. Radio/Slot Configuration



© 2024 Cisco and/or its affiliates. All rights reserved.

5. Click the **Security > Layer 2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA3.**
6. Confirm that the **PMF** is set to **Required**.
7. Disable Fast Transition.
8. Check the **WPA3 Policy, GCMP256**, and **SUITEB192-1X** check boxes, then unselect any other selected parameters.

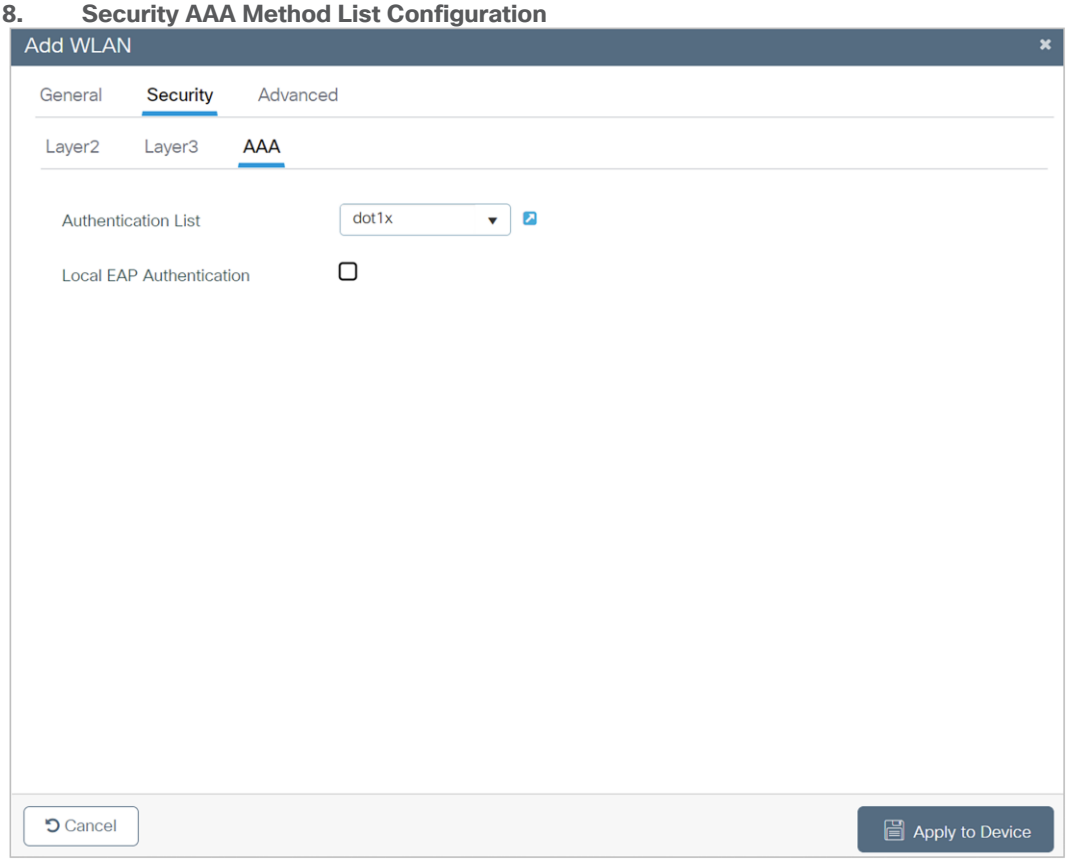
Figure 7. WLAN Security, Encryption and AKM Configuration



9. Click the **Security** tab and click the **AAA** tab and from the **Authentication List** drop-down list, choose the preconfigured RADIUS Server Authentication List.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 8. Security AAA Method List Configuration



10. Click **Apply to Device** to save and finish the WLAN creation process.

Note: SuiteB192-1X is not supported in C9120/C9105/C9115 APs and in FlexConnect Mode.

WPA3-Enterprise 192-bit CLI Configuration (optional)

The following steps create a WLAN with 192-bit WPA3-Enterprise security:

Table 4. WPA3-Enterprise 192-bit encryption CLI configuration

	Command or action	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan <wlan-name> wlan-id <SSID-name>`
	Example:
	`Device(config)# wlan WPA3-Enterprise-192B 8 WPA3-Enterprise-192B`
		Enters the WLAN configuration sub-mode.

Step 3	`no security ft adaptive`	Disables Fast Transition Adaptive support.
Step 4	`no security wpa wpa2`	Disables WPA2 security.
Step 5	`no security wpa wpa2 ciphers aes`	Disables WPA2/CCMP128 support.
Step 6	`security wpa wpa2 ciphers gcmp256`	Enables GCMP256 support.
Step 7	`no security wpa akm dot1x`	Disables security AKM 802.1X-SHA1 support.

© 2024 Cisco and/or its affiliates. All rights reserved.

	Command or action	Purpose
Step 8	`security wpa wpa3`	Enables WPA3 support.

Step 9	`security dot1x authentication-list list-name`
	Example:
	`Device(config-wlan)# security dot1x authentication-list dot1x`
		Configures security authentication list for 802.1X security.

Step 10	`no shutdown`	Enables the WLAN.
Step 11	`end`	Returns to the privileged EXEC mode.

WPA3-Enterprise Transition Mode

The WPA3-Enterprise Transition Mode, also known as WPA3+WPA2-Enterprise mixed-mode configuration, is used when some clients can support only up to WPA2 and some clients can support up to WPA3. The WPA3-capable clients will use WPA3-Enterprise's 802.1X-SHA256 AKM, while the WPA2-capable clients can use WPA2-Enterprise's 802.1X SHA1 or 802.1X-SHA256. This mode applies to both the bands 2.4 GHz and 5 GHz.

Note: This mode should be used only when necessary. For maximum security, the recommended mode is to use only WPA3 and not a mix of WPA3 and WPA2.

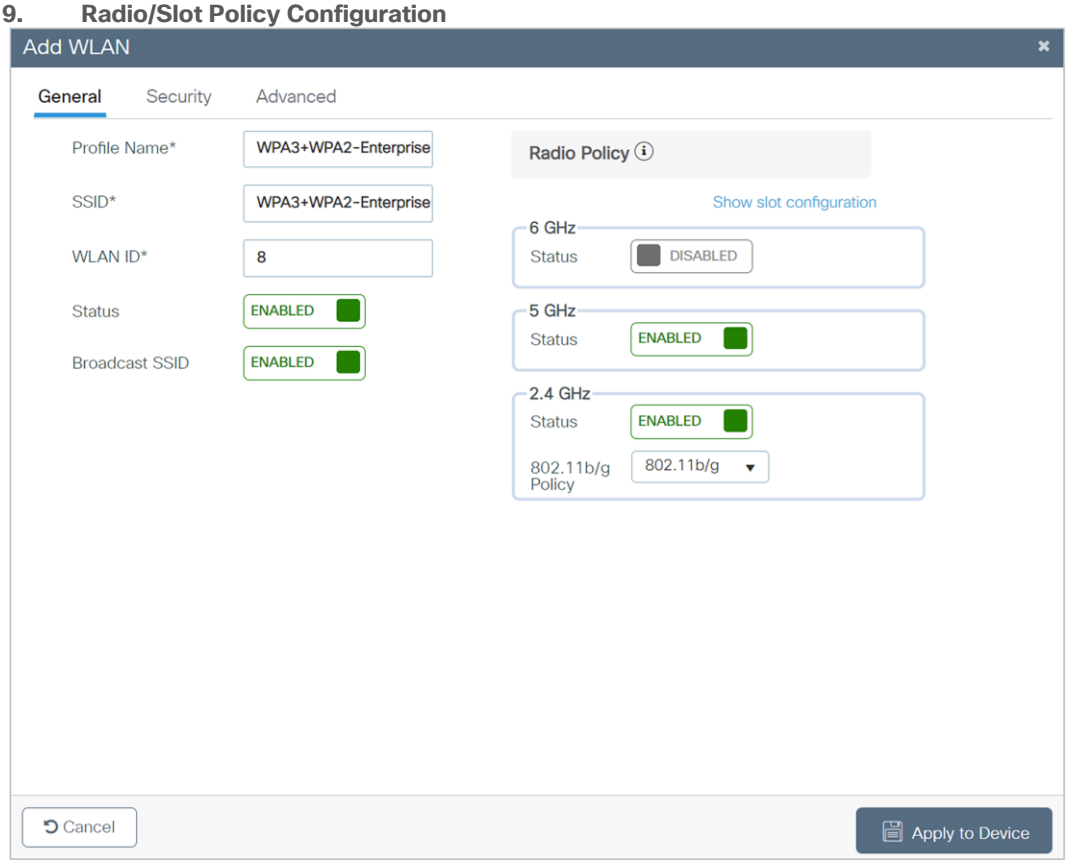
WPA3-Enterprise Transition Mode GUI Configuration

The following steps create a WLAN with WPA3+WPA2-Enterprise mixed-mode-level security:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID are populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.
5. Disable the **6-GHz Radio Policy**, as it is not supported.

© 2024 Cisco and/or its affiliates. All rights reserved.

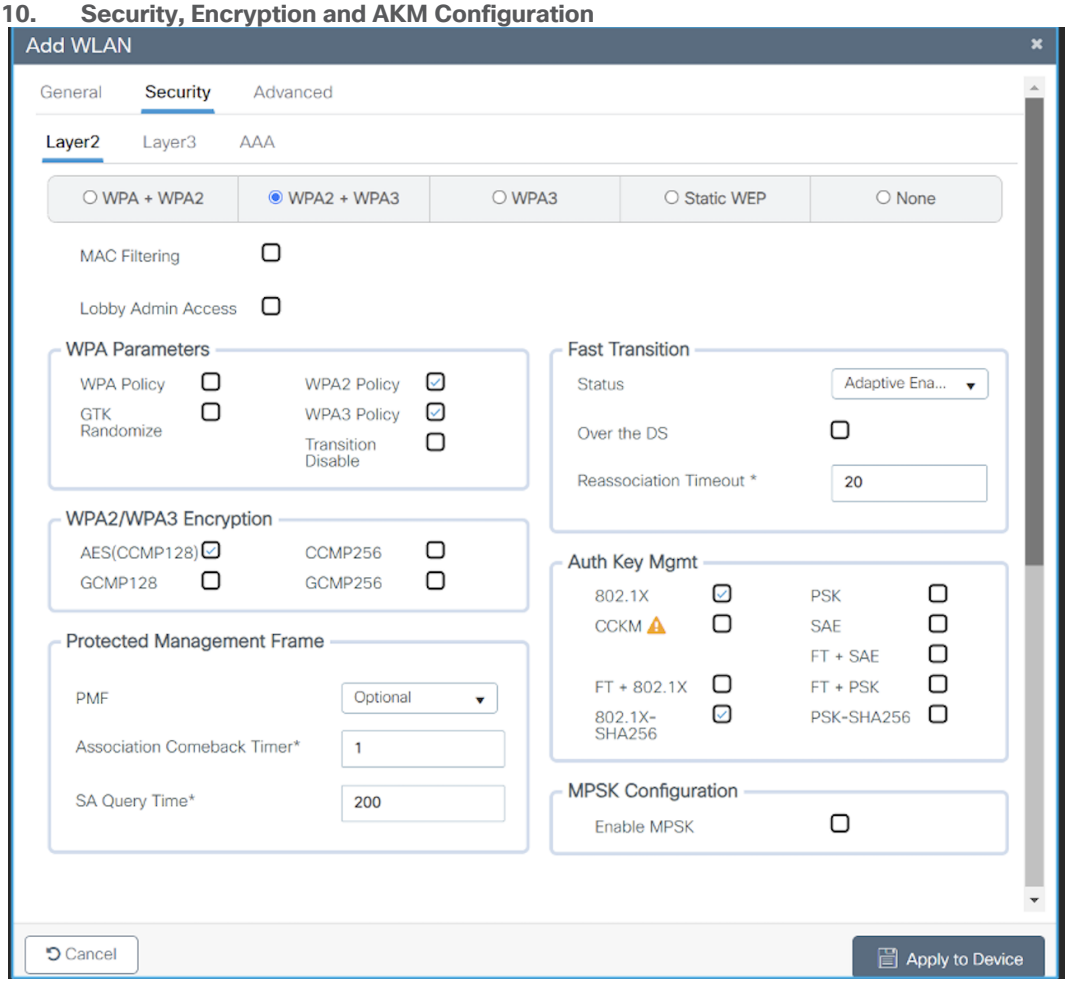
Figure 9. Radio/Slot Policy Configuration



6. Click the **Security > Layer 2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA3**.
7. Confirm that the **PMF** is set to **Optional**.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 10. Security, Encryption and AKM Configuration



8. Scroll down to the WPA Parameters. Check the **WPA2 Policy**, **WPA3 Policy**, and **Encryption AES**, and check the **802.1X and 802.1X-SHA256** check boxes.
9. Click **Apply to Device** to save and finish the WLAN creation process.

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Enterprise Transition Mode CLI Configuration

The following steps create a WLAN with WPA3+WPA2-Enterprise mixed-mode-level security:

Table 5. WPA3-Enterprise Transition Mode CLI Configuration

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device (config)# wlan WPA3+WPA2-Enterprise 8 WPA3+WPA2-Enterprise`
		Enters the WLAN configuration submode.

Step 3	`security wpa wpa3`	Enables WPA3.
Step 4	`Security wpa wpa2`	Enables WPA2.
Step 5	`security wpa akm dot1x-sha256`	Enables the 802.1X SHA2 AKM.
Step 6	`radio policy dot11 24ghz`	Enables the 2.4-GHz band.
Step 7	`radio policy dot11 5ghz`	Enables the 5-GHz band.
Step 8	`no shutdown`	
Step 9	`end`	

Note: This security combination can be used with FT-enabled mode as well.

WPA3-Enterprise Transition Disable Mode

Ease of network upgrade: WPA2 devices have been there for many years in Wi-Fi networks, so it was important to have a mode of deployment where both WPA2 and WPA3 devices can co-exist. This certainly helps Wi-Fi networks migrate gradually from WPA2 to WPA3-based networks. Wi-Fi Alliance has introduced the WPA3 Transition modes for both personal and enterprise networks. With transition mode enabled on SSID, both WPA2 and WPA3 supporting devices can connect simultaneously, thus paving the path for the gradual migration of the device eco-system from WPA2 to WPA3.

Transition Disable: With the above ease of network upgrade using transition mode comes the security challenge of WPA3 STAs (stations) undergoing downgrade attacks. The attackers can force WPA3 STAs to downgrade to use WPA2 and legacy security-vulnerable technologies. To circumvent this problem, the Wi-Fi alliance has introduced the “Transition Disable” indication, using which APs and network operators can update WPA3 STAs that the network is fully upgraded to support the most secured algorithm defined in a transition mode. The Transition Disable indication is used (in a 4-way handshake during association) to disable transition modes for that network on a STA, and therefore provide protection against downgrade attacks. STAs upon receiving this indication, shall disable certain transition modes for subsequent connections and will disallow association without negotiation of PMF.

An STA implementation might enable certain transition modes (and possibly other legacy security algorithms) in a network profile.

© 2024 Cisco and/or its affiliates. All rights reserved.

For example, a WPA3-Personal STA might by default enable WPA3-Personal transition mode in a network profile, which enables a pre-shared key (PSK) algorithm. However, when a network (fully) supports the most secure algorithm defined in a transition mode, it can use the Transition Disable indication to disable transition modes for that network on an STA, and therefore protect against downgrade attacks.

On one side, this is good for security, as it will migrate all client devices to WPA3 only as they join the transition mode WLAN, but if the network is composed of multiple physical locations, for example, some are set to WPA2, others to WPA3/WPA2 transition mode, this will cause the migrated clients to fail when moved to a location with WPA2 only.

This is a possible scenario for some large networks, with the same SSID covering different controllers/AP setups and with configurations not matching 100%. The largest example would be Edu Roam, which shares the same SSID name worldwide. Setting this could have serious issues for clients moving across different network providers, so please use this with care, and only if you can ensure the same security setting is set properly across all network locations.

This method is not generally recommended and should be enabled only when it is absolutely necessary.

The section below explains how to enable Transition Disable in the WLAN.

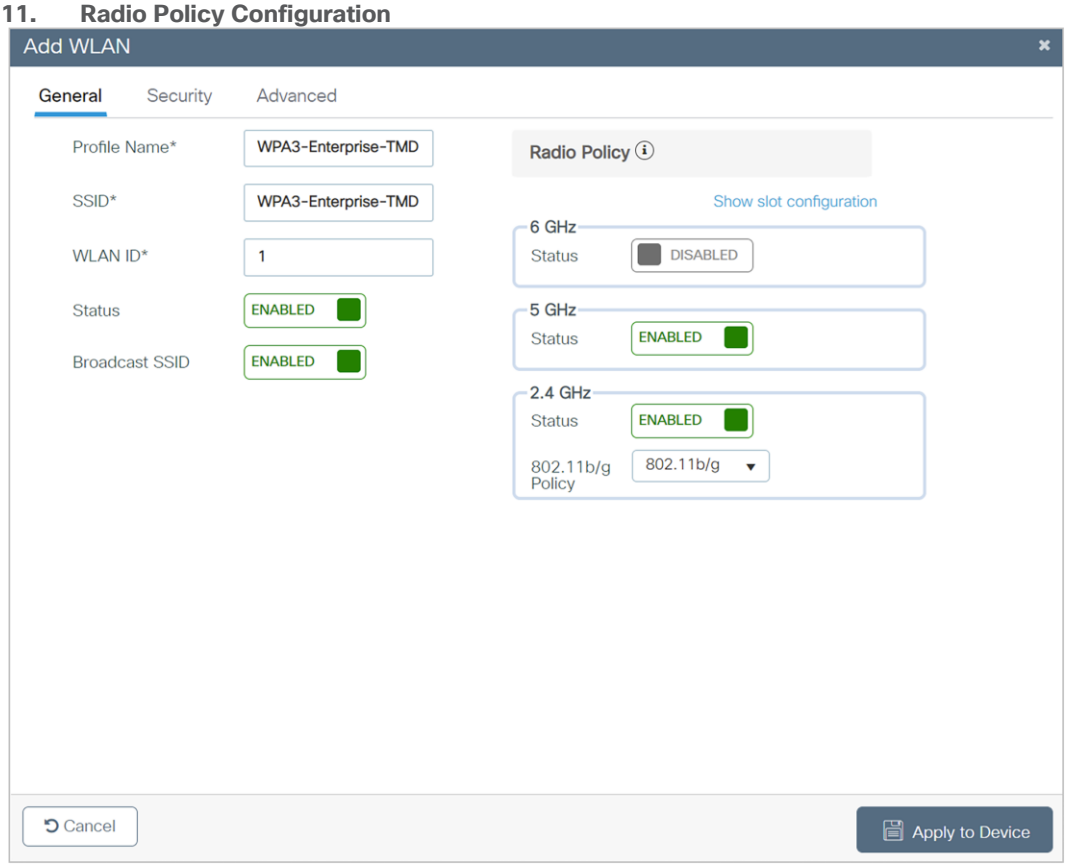
WPA3-Enterprise Transition Mode Disable GUI Configuration

The following steps create a WLAN with WPA3-Enterprise security with Transition Disable:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID are populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.

© 2024 Cisco and/or its affiliates. All rights reserved.

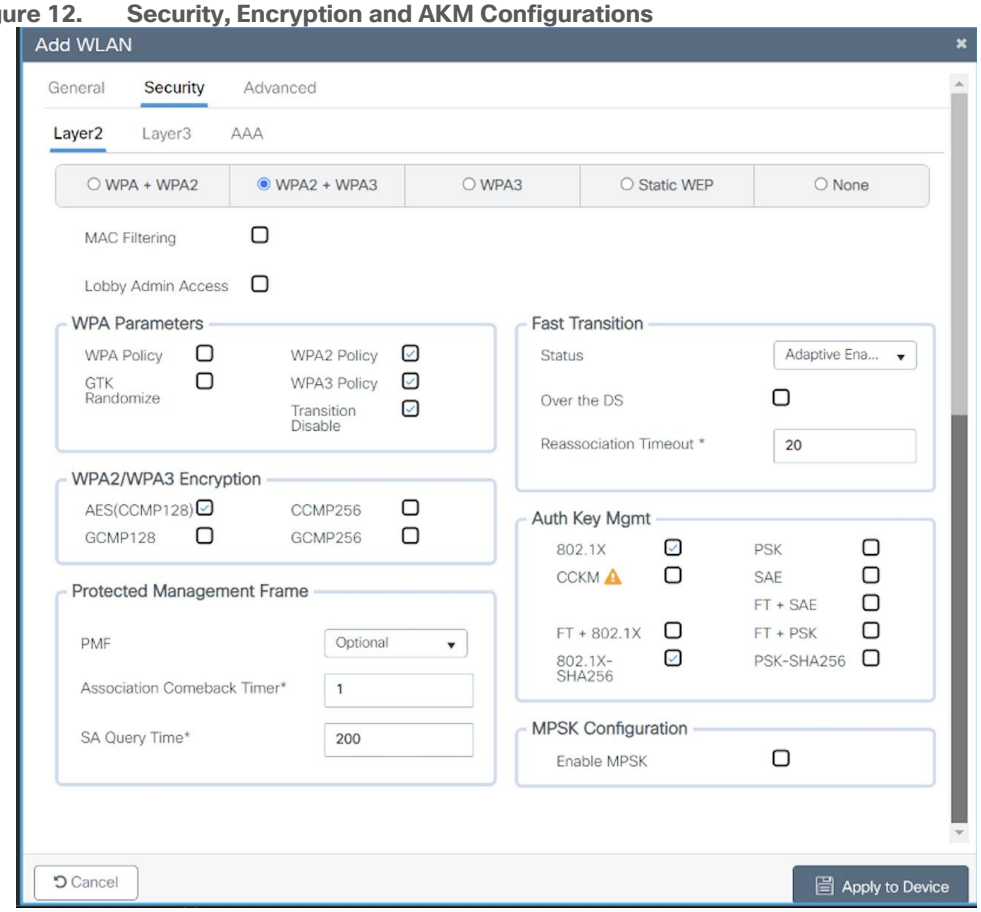
Figure 11. Radio Policy Configuration



5. Disable the **6-GHz policy**, as it is not supported.
6. Check the **Security** tab and enable the **WPA2 + WPA3** option.
7. Scroll down to the WPA Parameters. Check the **WPA2** and **WPA3 Policy**, **AES**, and **802.1X** and **802.1X-SHA256** check boxes as AKM.
8. Confirm that the PMF is set to be **Optional**.
9. Enable **Transition Disable** under WPA Parameters.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 12. Security, Encryption and AKM Configurations



WPA3-Enterprise Transition Mode Disable CLI Configuration

Table 6. WPA3-Enterprise Transition Mode Disable CLI Configuration

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan WPA3-Enterprise-TMD 1 WPA3-Enterprise-TMD`
		Enters the WLAN configuration submode.

Step 3	`security wpa wpa3`	Enables WPA3.
Step 4	`security wpa wpa2`	Enables WPA2 security. PMF is optional now.
Step 5	`security wpa wpa2 ciphers aes`	Enables Advanced Encryption Standard (AES)/CCMP128 ciphers.
Step 6	`security wpa akm dot1x-sha256`	Enables AKM 802.1x-SHA256.

© 2024 Cisco and/or its affiliates. All rights reserved.

	Command	Purpose
Step 7	`transition-disable`	Enables Transition Disable.
Step 8	`radio policy dot11 5ghz`	Enables the 5-GHz band.
Step 9	`radio policy dot11 24ghz`	Enables the 2.4-GHz band.
Step 10	`no shutdown`	Enables the WLAN.
Step 11	`end`	Returns to the privileged EXEC mode.

Note: This security combination can be used with FT enabled mode as well.

WPA2+WPA3-Enterprise Transition Mode with 6 GHz

Per 6 GHz standard, broadcasting a WLAN in the 6-GHz band is not allowed when configured with WPA2 security (applies to both WPA2 only and WPA2+WPA3 WLAN), so this essentially leads to the behavior that we don't support 6-GHz radio when WLAN is configured with WPA2.

This poses limitations in certain use cases when legacy clients want to support 802.1X-SHA1 along with PMF optional in 5-GHz on the same SSID, whereas 6-GHz clients support 802.1X-SHA256 AKM with PMF mandatory.

To support these deployments, the recommendation in pre-17.12.1 SW versions was to use WPA2+WPA3 transition mode with the same WLAN with different profiles to support both legacy and the latest 6-GHz clients. The challenge with this design is roaming. The roaming between bands in this configuration is not supported, and it is always full roam, which is not preferred.

Starting from 17.12.1, we support transition mode with pure WPA3 for the 6-GHz band, which allows users to enable WPA2+WPA3 in the same WLAN with 6 GHz. This mode eliminates the need to create two different profiles to accommodate legacy and the latest 6-GHz devices. In this mode, the WPA2+WPA3 transition mode can be used in 2.4-GHz/5-GHz, and only WPA3 relevant configurations will be pushed on the 6-GHz band when WLAN has both WPA2 & WPA3 configurations.

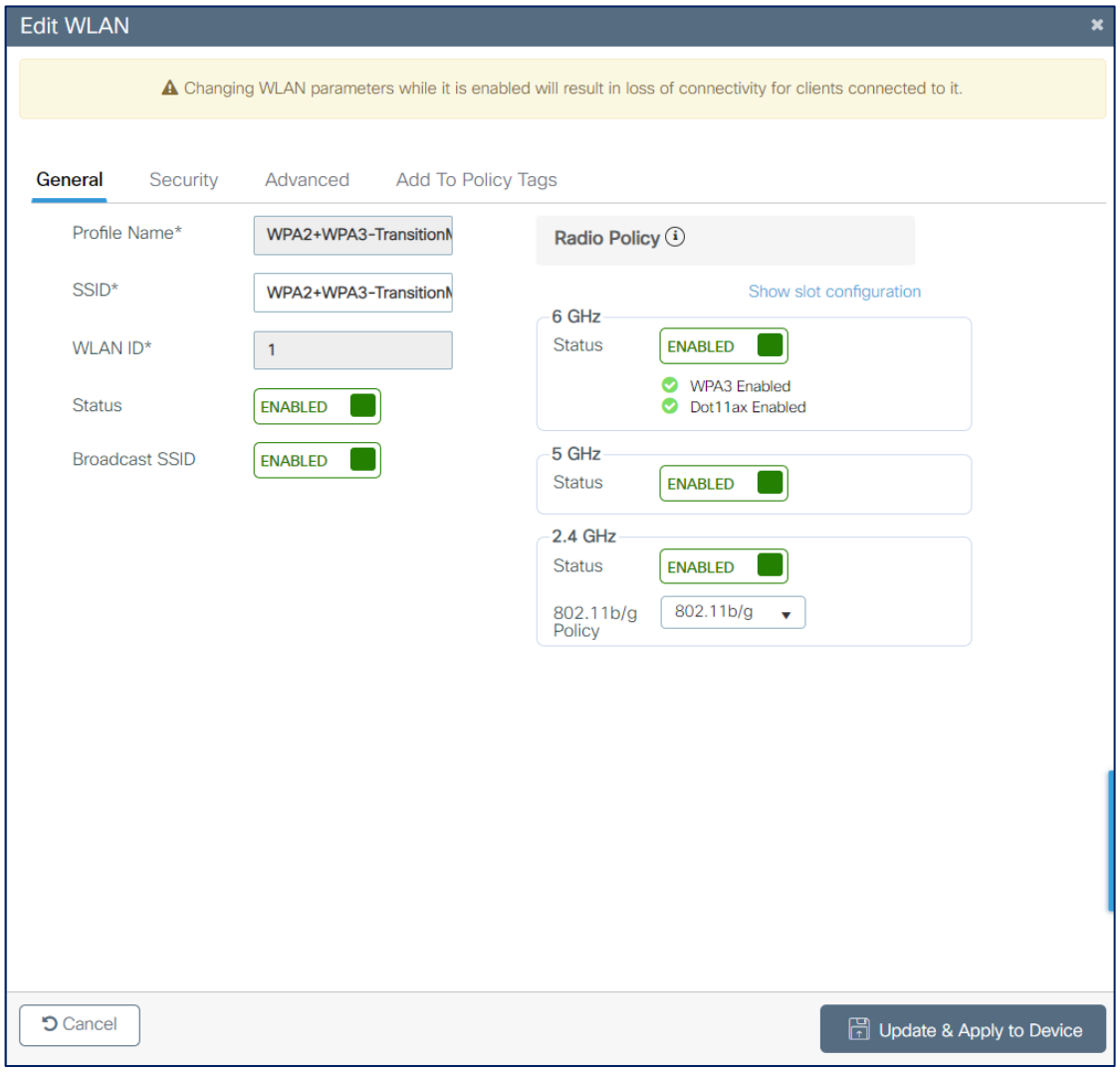
WPA2+WPA3-Enterprise Transition Mode with 6GHz – GUI Configuration

The following steps create a WLAN with WPA2+WPA3-Enterprise transition mode with 6 GHz:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). Both the SSID and WLAN ID are populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 13. Radio/Slot Configuration

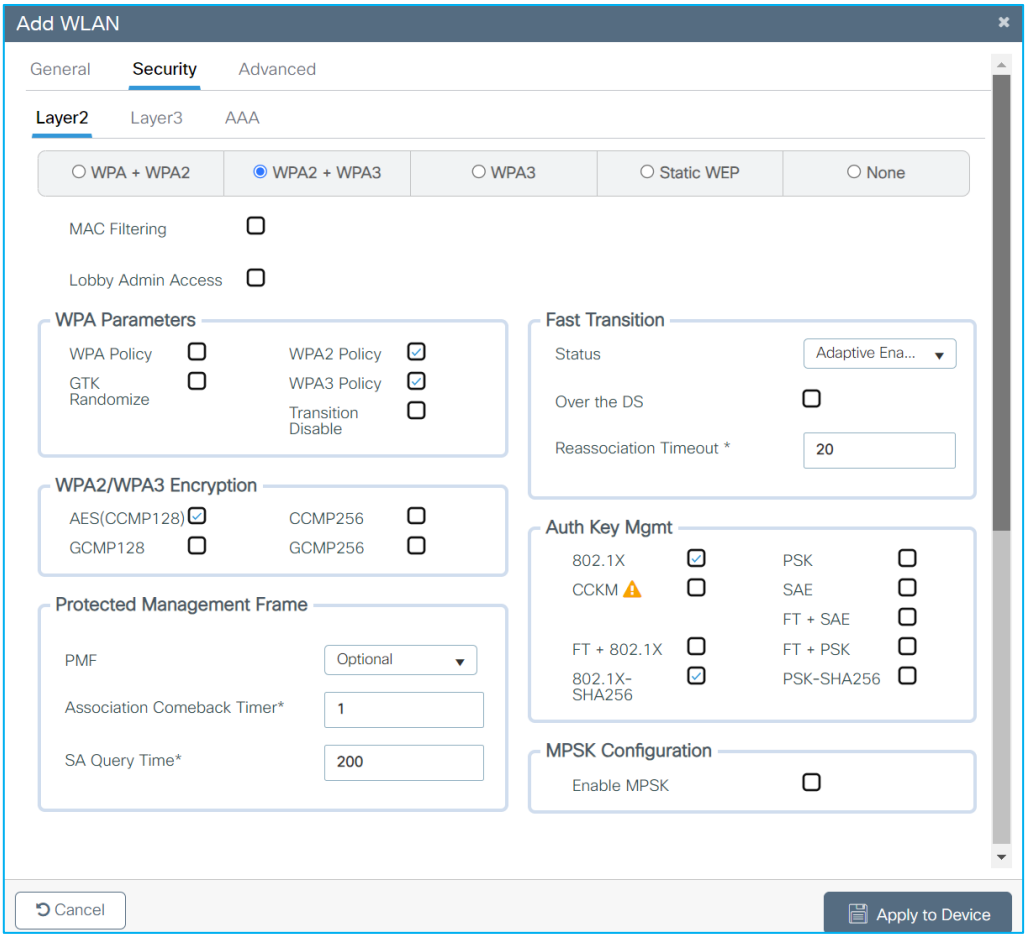


5. Click the **Security > Layer 2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA3.**
6. Confirm that the PMF is set to **Optional**.

   Note: Though PMF is optional, with WPA3 configuration, it is considered required for the 6-GHz band.
7. Scroll down to the WPA parameters. Select the **WPA2** and **WPA3 Policy**, **AES(CCMP128)** in **WPA2/WPA3 encryption**, and **802.1X** and **802.1X-SHA256** check boxes, then unselect any other selected parameters.

© 2024 Cisco and/or its affiliates. All rights reserved.

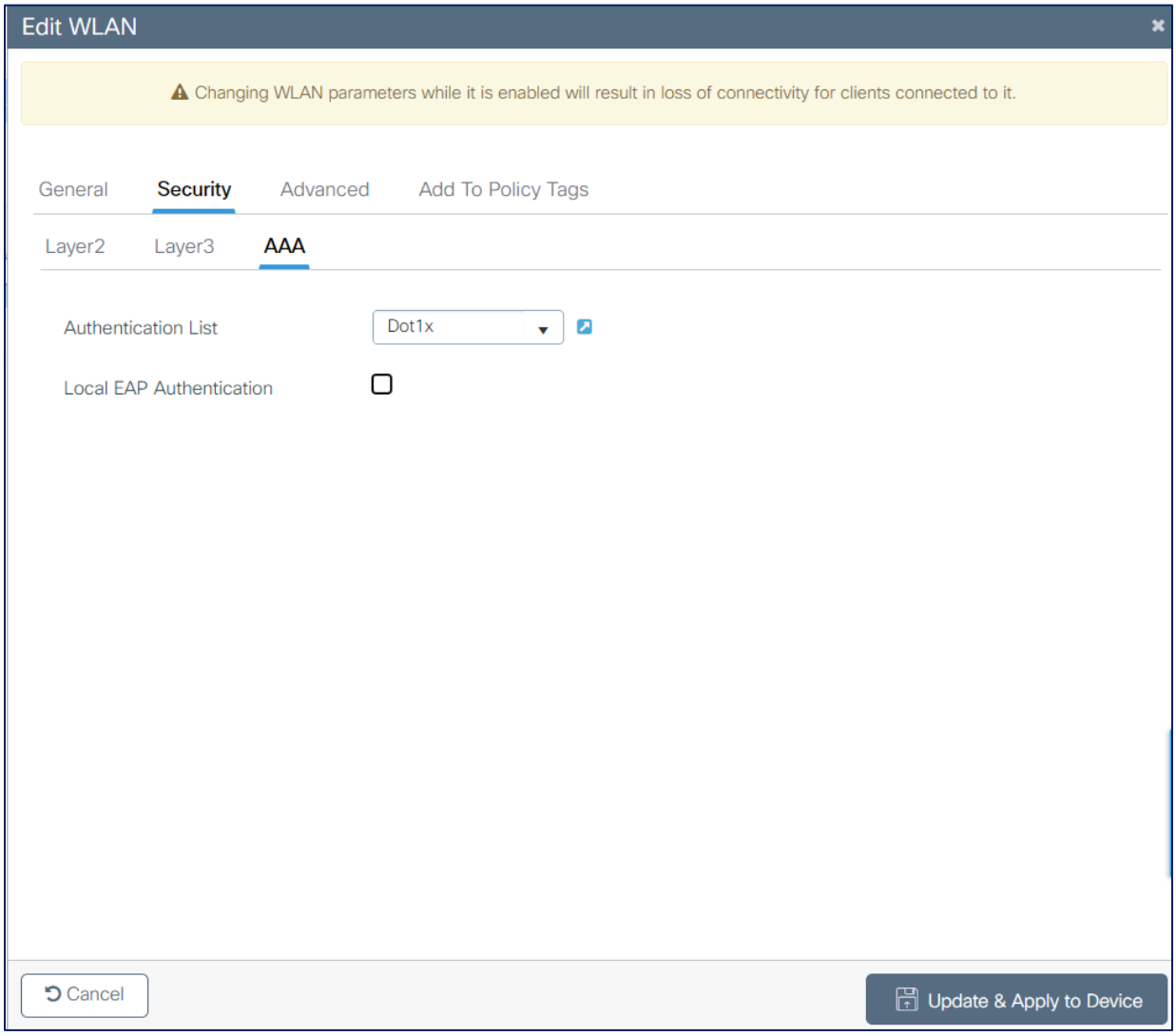
Figure 14. Radio/Slot Configuration



8. Click the **Security** tab and click the **AAA** tab and from the **Authentication List** drop-down list, choose the preconfigured RADIUS Server Authentication List.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 15. Radio/Slot Configuration



9. Click **Apply to Device** to save and finish the WLAN creation process.

WPA2+WPA3-Enterprise Transition Mode with 6 GHz CLI Configuration

The following steps create a WLAN with WPA2+WPA3-Enterprise transition mode with 6 GHz:

Table 7. WPA2+WPA3-Enterprise Transition Mode CLI configuration

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	wlan wlan-name wlan-id SSID-name Example: Device (config)# wlan WPA2+WPA3-TransitionMode 1 WPA2+WPA3-TransitionMode	Enters the WLAN configuration submode.
Step 3	security wpa wpa3	Enables WPA3.

© 2024 Cisco and/or its affiliates. All rights reserved.

	Command	Purpose
Step 4	security wpa wpa2	Enables WPA2.
Step 5	security wpa akm dot1x-sha256	Enables the SHA2 AKM.
Step 6	security wpa akm dot1x	Enables the SHA1 AKM.
Step 7	radio policy dot11 6ghz	Enables the 6-GHz band
Step 8	radio policy dot11 24ghz	Enables the 2.4-GHz band.
Step 9	radio policy dot11 5ghz	Enables the 5-GHz band
Step 10	no shutdown	
Step 11	end	

WPA2+WPA3-Enterprise transition mode with 6 GHz CLI Output

```
#show wlan summary
           Number of WLANs: 1
           ID    Profile Name                    SSID                            Status
           2.4GHz/5GHz Security
           6GHz Security
           ------------------------------------------------------------------------------------
           ------------------------------------------------------------------------------------
           ------------------------------------------------------------------------------------
           ----------------------------------
           1     WPA2+WPA3-TransitionMode        WPA2+WPA3-TransitionMode        UP
           [WPA2 + WPA3][802.1x][AES][PMF 802.1X]
           [WPA3][AES][PMF 802.1X]
```

Note: This configuration is supported in GCM256 encryption SuiteB192-1X too. When WPA2+WPA3 transition mode with pure WPA3 is enabled along with 192-bit encryption, the bands operate as below:

- 2.4 GHz & 5 GHz: WPA2 + WPA3-SUITEB-192-1X-GCMP256
- 6 GHz: WPA3-SUITEB-192-1X-CCMP256

WPA3-Personal

WPA3-Personal uses 128-bit cryptographic-strength encryption with a password-based authentication method through SAE for user authentication purposes. In addition, unlike WPA2-Personal, WPA3-Personal heightens network security against offline dictionary attacks by limiting password guesses and requiring users to interact with a live network every time they do so. This requirement makes hacking into a network much more time-consuming and dissuades attempts at a brute force attack.

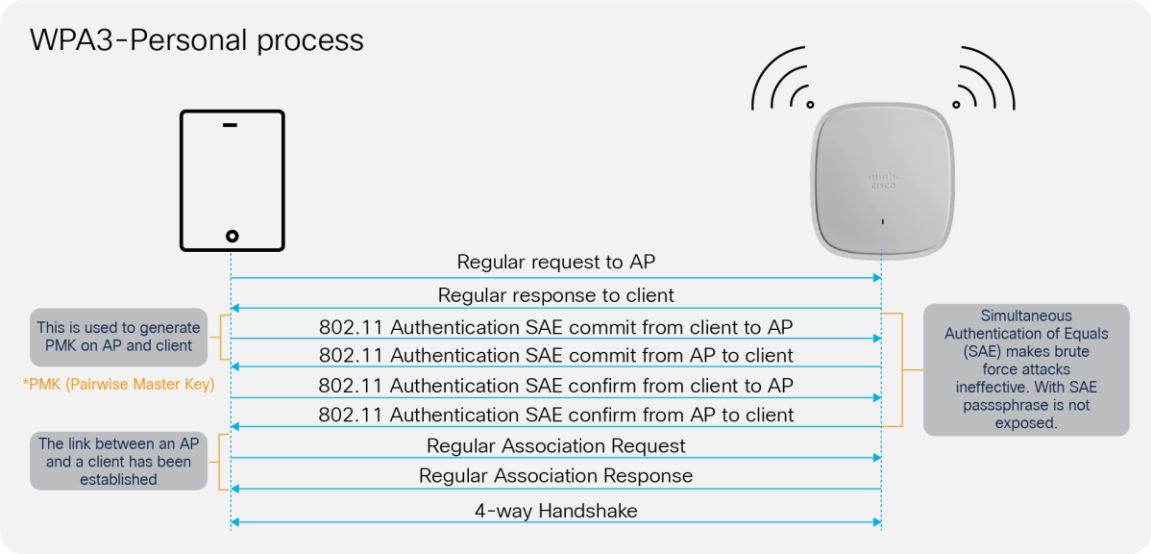
WPA3-Personal provides the following key advantages:

- Creates a shared secret that is different for each SAE authentication
- Protects against brute force “dictionary” attacks and passive attacks

© 2024 Cisco and/or its affiliates. All rights reserved.

- Provides forward secrecy

Figure 16. WPA3-Personal Endpoint and Network Handshake Process



WPA3-Personal GUI Configuration

The following steps create a WLAN with WPA3-Personal-level security:

1. Choose **Configuration > Tags and Profiles > WLANs**.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID are populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.

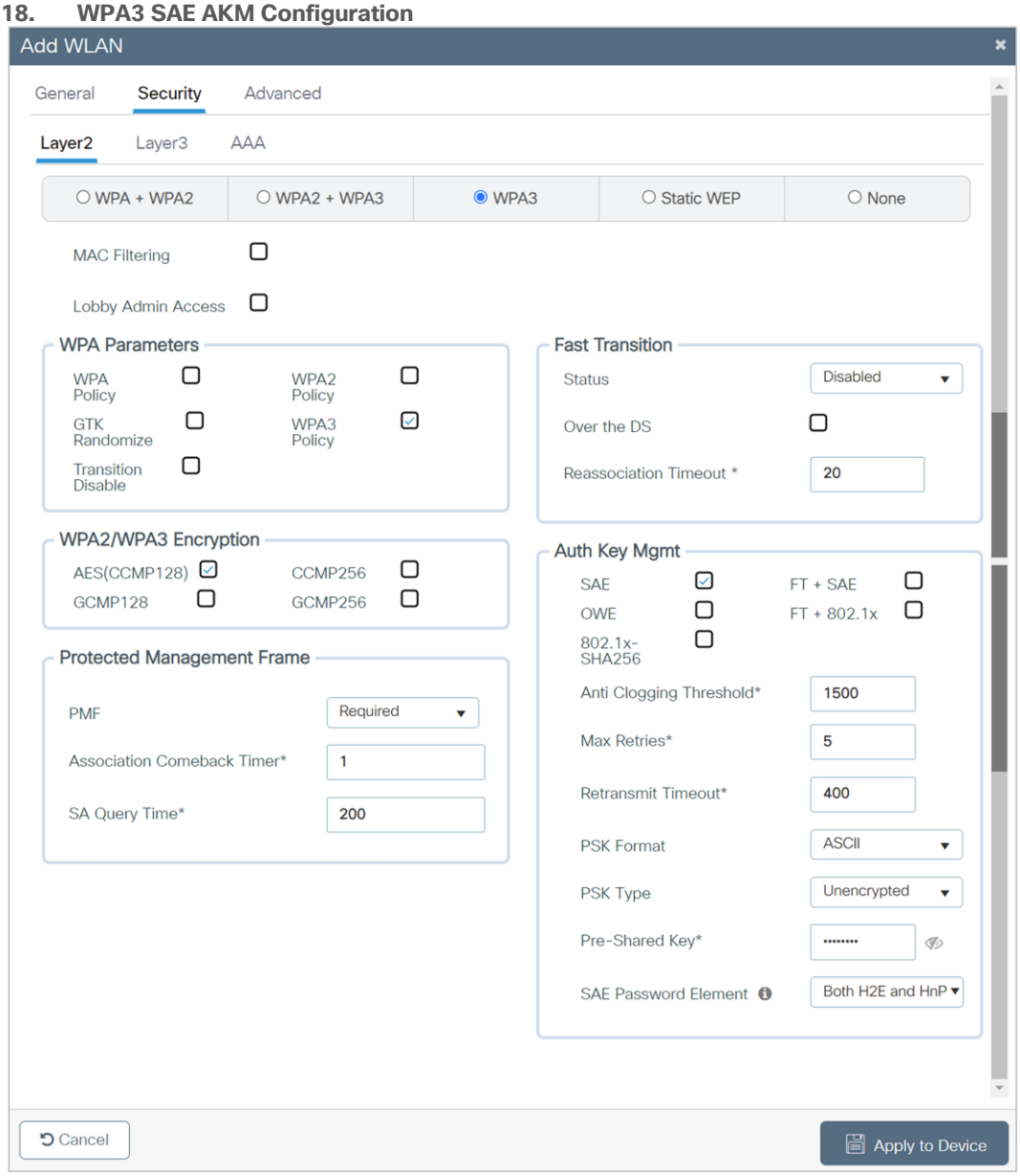
© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 17. WPA3 Personal Radio/Slot Configuration

5. Click the **Security > Layer 2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA3.**
6. Confirm that the **PMF** is set to **Required**.
7. Disable Fast Transition.
8. Scroll down to the WPA Parameters. Check the **WPA3 Policy, AES**, and **SAE** check boxes.
9. Enter the **Pre-Shared Key** and from the **PSK Format** drop-down list, choose the **PSK format** and from the **PSK Type** drop-down list, choose the **PSK type**.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 18. WPA3 SAE AKM Configuration



10. Click **Apply to Device** to save and finish the WLAN creation process.

Note: If only the 6-GHz band is used, the SAE Password Element supported is Hash to Element (H2E). Hunting and Pecking (HnP) cannot be used in a 6 GHz-only network. If both 5 GHz and 2.4 GHz are used, H2E and HnP can be used as the SAE Password Element.

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Personal CLI Configuration

The following steps create a WLAN with WPA3-Personal-level security:

Table 8. WPA3-Personal CLI configuration

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan WPA3-Personal 8 WPA3-Personal`
		Enters the WLAN configuration sub-mode.

Step 3	`no security wpa akm dot1x`	Disables security AKM 802.1X.
Step 4	`no security ft over-the-ds`	Disables Fast Transition over the data source on the WLAN.
Step 5	`no security ft`	Disables 802.11r Fast Transition on the WLAN.
Step 6	`no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	`security wpa wpa2 ciphers aes`	Enables Advanced Encryption Standard (AES)/CCMP128 ciphers.

Step 8	`security wpa psk set-key ascii value preshared-key`
	`Example:`
	`Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`
		Specifies a preshared key.

Step 9	`security wpa wpa3`	Enables WPA3 support. **Note:** If both WPA2 and WPA3 are supported (SAE and PSK together), it is optional to configure PMF. However, you cannot disable PMF. For WPA3, PMF is mandatory.
Step 10	`security wpa akm sae`	Enables AKM SAE support.
Step 11	`security wpa akm sae pwe h2e/hnp/both`	Chooses the Password Element.
Step 12	`no shutdown`	Enables the WLAN.
Step 13	`End`	Returns to the privileged EXEC mode.

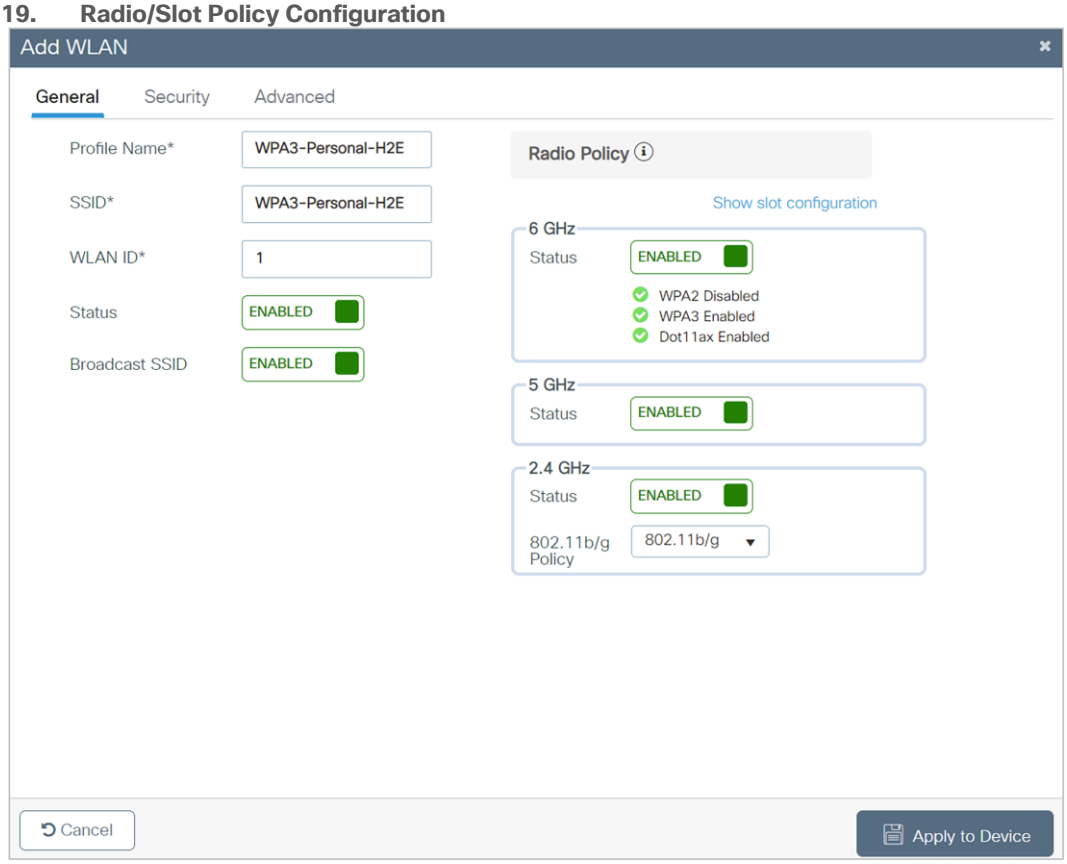
© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Personal SAE Hash-to-Element Method for Password Element Generation

The following steps will create a WLAN with WPA3-Personal-level security with H2E for password element generation:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID are populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.
5. Click the **Security > Layer 2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA3**.

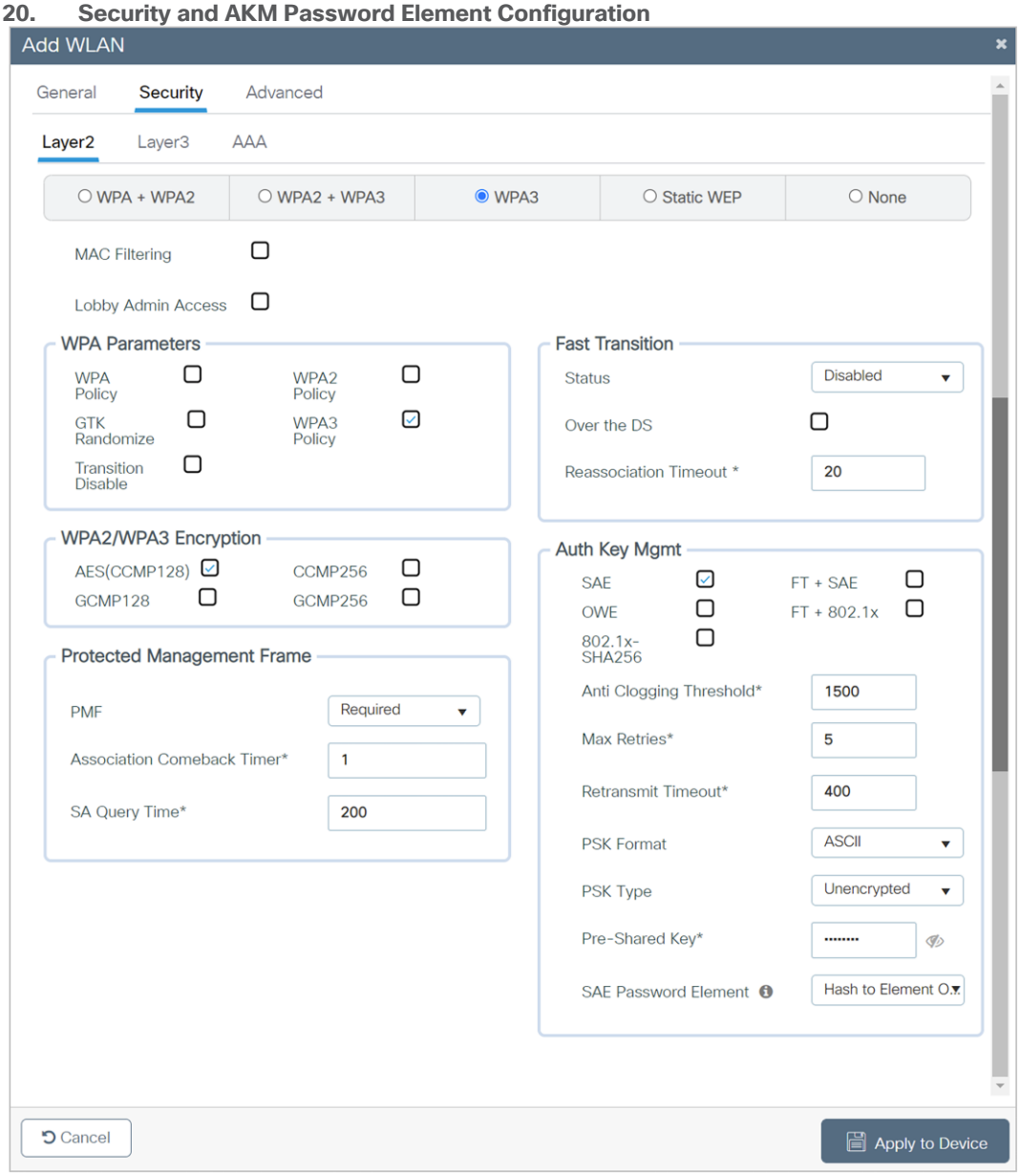
Figure 19. Radio/Slot Policy Configuration



6. Confirm that the **PMF** is set to **Required**.
7. Disable Fast Transition.
8. Scroll down to the **WPA Parameters**. Check the **WPA3 Policy**, **AES**, and **SAE** check boxes.
9. Enter the **Pre-Shared Key** and then from the **PSK Format** drop-down list, choose the PSK format, and from the **PSK Type** drop-down list, choose the PSK type.
10. From the **SAE Password Element** drop-down list, enable **Hash to Element Only**.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 20. Security and AKM Password Element Configuration



Note: If only the 6-GHz band is used, the SAE Password Element supported is H2E. HnP cannot be used in a 6-GHz-only network. If both 5 GHz and 2.4 GHz are used, H2E and HnP can be used as the SAE Password Element.

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Personal SAE Hash-to-Element Method for Password Element Generation CLI configuration

The following steps create a WLAN with WPA3-Personal-level security with H2E for password element generation:

Table 9. WPA3-Personal SAE hash-to-element CLI configuration

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan WPA3-Personal-H2E 1 WPA3-Personal-H2E`
		Enters the WLAN configuration submode.

Step 3	`no security wpa akm dot1x`	Disables security AKM 802.1X.
Step 4	`security wpa wpa3`	Enables WPA3.
Step 5	`no security ft`	Disables 802.11r Fast Transition on the WLAN.
Step 6	`no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	`security wpa wpa2 ciphers aes`	Enables AES/CCMP128 ciphers.

Step 8	`security wpa psk set-key ascii value preshared-key`
	`Example:`
	`Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`
		Specifies a preshared key.

Step 9	`security wpa akm sae`	Enables AKM SAE support.
Step 10	`security wpa akm sae pwe h2e`	Enables H2E for password element generation.
Step 11	`no shutdown`	Enables the WLAN.
Step 12	`End`	Returns to the privileged EXEC mode.

© 2024 Cisco and/or its affiliates. All rights reserved.

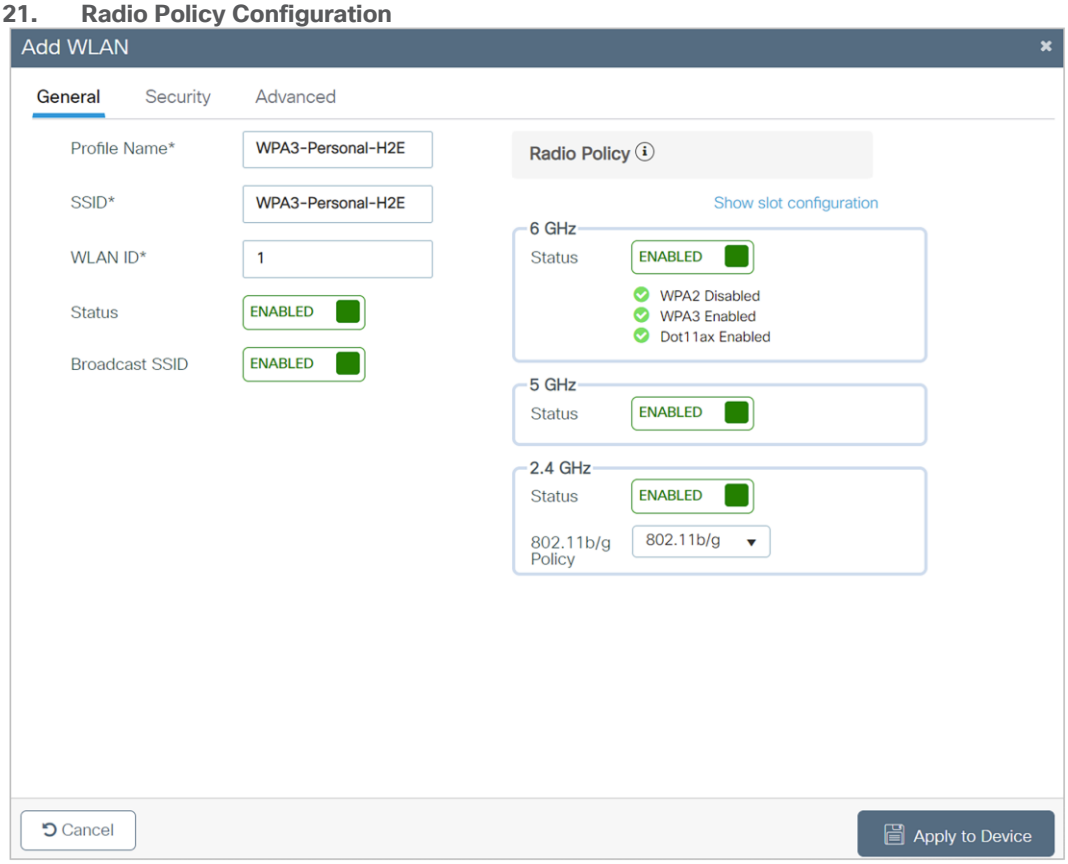
WPA3-Personal SAE with Fast Transition Enabled

Starting from Cisco IOS® XE version 17.9.1, WPA3-Personal SAE with Fast Transition (SAE-FT) is supported. Follow the instructions below to configure the WLAN for WPA3 SAE-FT.

The following steps create a WLAN with WPA3-Personal-level SAE security with Fast Transition enabled:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add.**
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID are populated automatically.
4. Enable the Status and Broadcast SSID toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.
5. Click the **Security > Layer 2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA3**

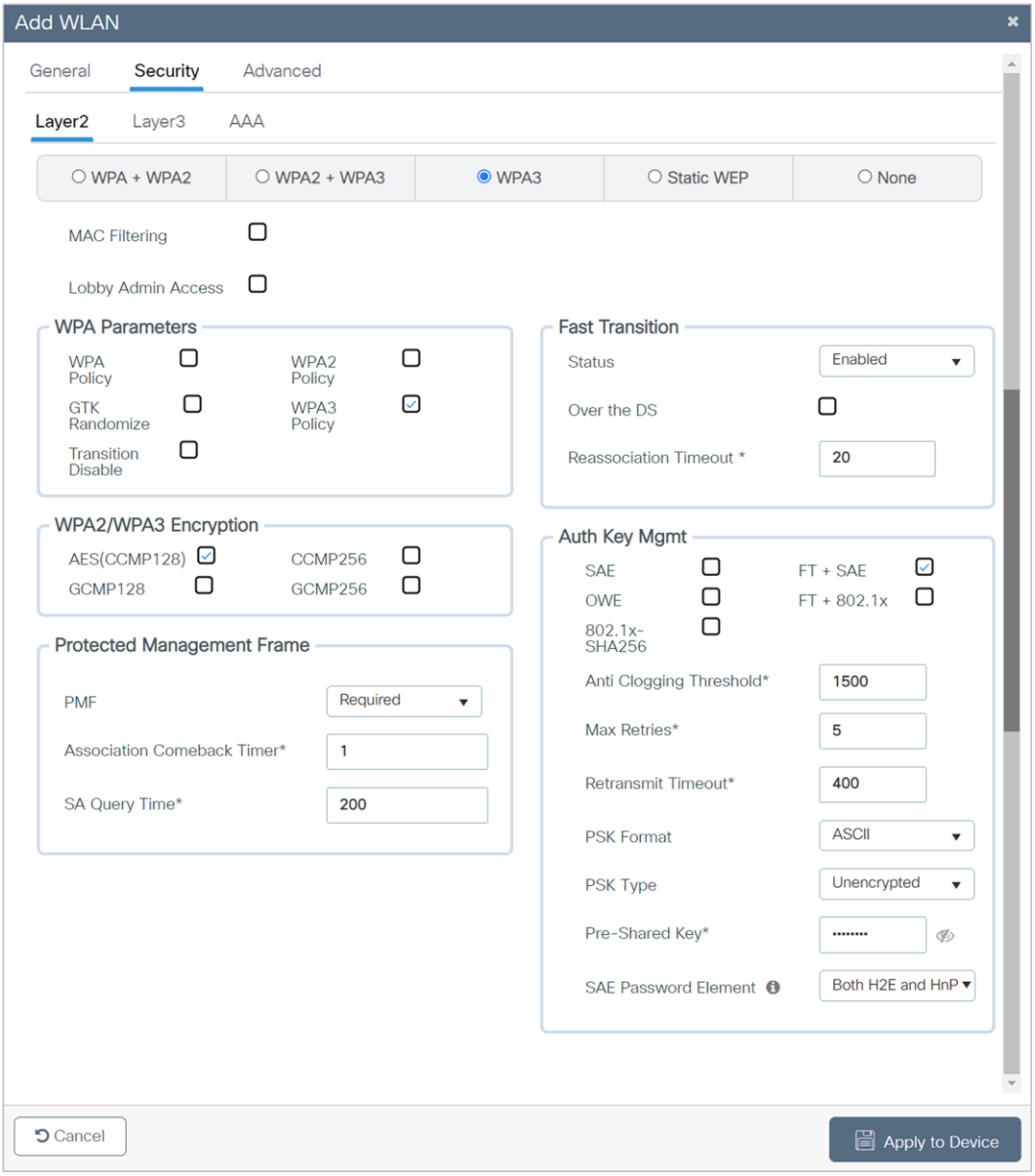
Figure 21. Radio Policy Configuration



6. Confirm that the **PMF** is set to **Required**.
7. Enable Fast Transition.
8. Scroll down to the **WPA Parameters**. Check the **WPA3 Policy, AES,** and **SAE** check boxes.
9. Enter the **Pre-Shared Key** and from the **PSK Format** drop-down list, choose the **PSK format** and from the **PSK Type** drop-down list, choose the **PSK type**.
10. Enable **Hash to Element Only** or **HnP** or **both** from the SAE Password Element drop-down.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 22. WPA3 SAE with FT Enabled



WPA3-Personal SAE with Fast Transition Enabled CLI Configuration

The following steps create a WLAN with WPA3-Personal-level security with Fast Transition enabled:

Table 10. WPA3-Personal SAE FT CLI configuration

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan WPA3-Personal-H2E 1 WPA3-Personal-H2E`
		Enters the WLAN configuration sub-mode.

Step 3	`no security wpa akm dot1x`	Disables security AKM 802.1X.

© 2024 Cisco and/or its affiliates. All rights reserved.

	Command	Purpose
Step 4	`security wpa wpa3`	Enables WPA3.
Step 5	**`security ft`**	Enables 802.11r Fast Transition on the WLAN.
Step 6	`no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	`security wpa wpa2 ciphers aes`	Enables AES/CCMP128 ciphers.

Step 8	`security wpa psk set-key ascii value preshared-key`
	`Example:`
	`Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`
		Specifies a preshared key.

Step 9	`security wpa akm sae`	Enables AKM SAE support.
Step 10	`Security wpa akm ft sae`	Enables FT SAE.
Step 11	**`security wpa akm sae pwe h2e`**	Enables H2E for password element generation.
Step 12	`no shutdown`	Enables the WLAN.
Step 13	`End`	Returns to the privileged EXEC mode.

WPA3-Personal Transition Mode

The WPA3-Personal Transition Mode, also known as WPA2+WPA3-Personal mixed-mode configuration, is used when some clients are capable of supporting only WPA2 and some clients are capable of supporting up to WPA3. The WPA3-capable clients will use WPA3-Personal's SAE, while the WPA2-capable clients will use WPA2-Personal's PSK. This mode applies to both the bands of 2.4-GHz and 5-GHz.

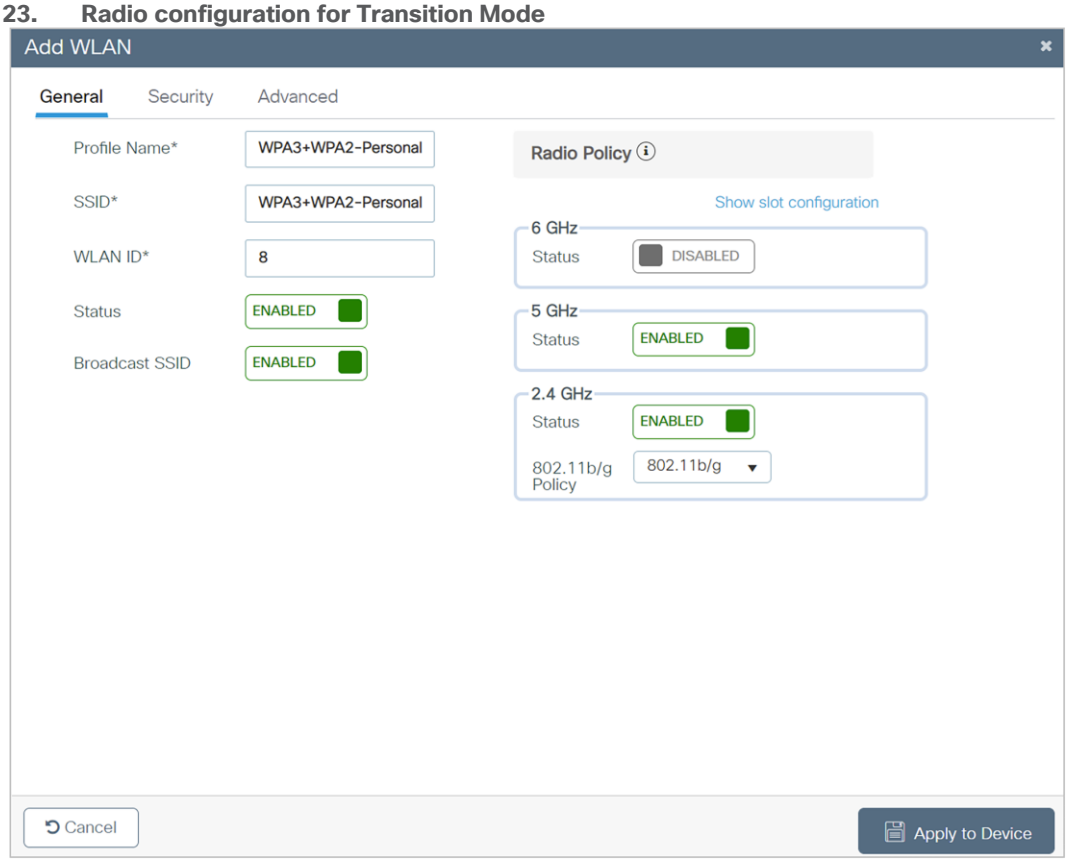
> **Note:** This mode should be used only when necessary. For maximum security, the recommended mode is to use only WPA3 and not a mix of WPA3 and WPA2.

The following steps create a WLAN with WPA3+WPA2-Personal mixed-mode-level security:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID are populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.
5. Disable the **6-GHz** band.

© 2024 Cisco and/or its affiliates. All rights reserved.

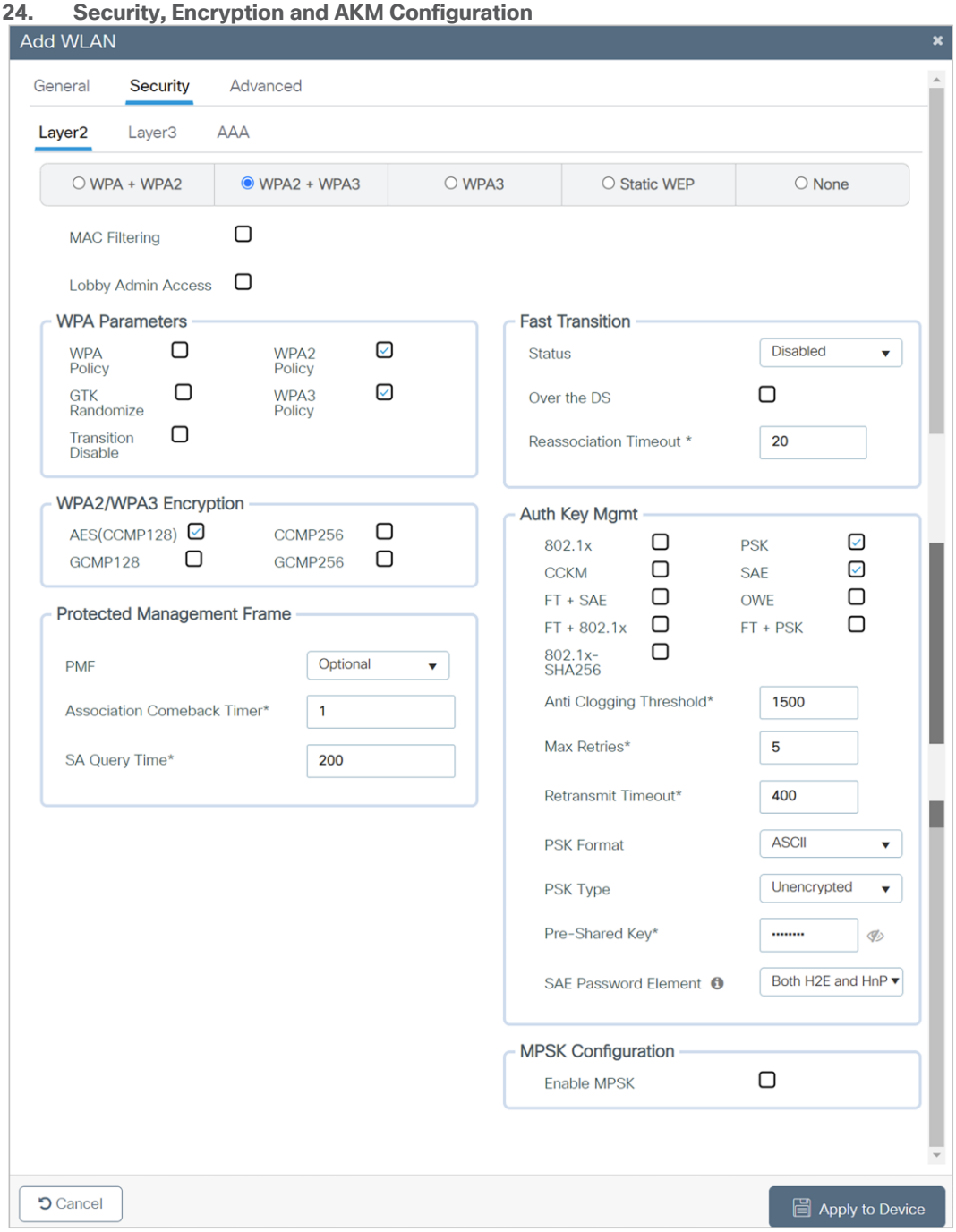
Figure 23. Radio configuration for Transition Mode



6. Click the **Security** > **Layer 2 tab**. From the **Layer 2 Security Mode** drop-down list, choose **WPA3.**
7. Confirm that the **PMF** is set to **Optional**.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 24. Security, Encryption and AKM Configuration



8. Scroll down to the WPA Parameters. Check the **WPA2 Policy**, **WPA3 Policy**, **AES**, **PSK**, and **SAE** check boxes.
9. Enter the **Pre-Shared Key** and from the **PSK Format** drop-down list, choose the **PSK format** and from the **PSK Type** drop-down list, choose the **PSK type**.
10. Click **Apply to Device** to save and finish the WLAN creation process.

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3 Personal Transition Mode CLI Configuration

The following steps create a WLAN with WPA3+WPA2-Personal mixed-mode-level security:

Table 11. WPA3 Personal transition mode CLI configuration

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan WPA3+WPA2-Personal 1 WPA3+WPA2-Personal`
		Enters the WLAN configuration submode.

Step 3	`no security wpa akm dot1x`	Disables security AKM 802.1X.
Step 4	`no security ft`	Disables 802.11r Fast Transition on the WLAN.
Step 5	`security wpa wpa2 ciphers aes`	Configures the WPA2 cipher. **Note:** You can check whether the cipher is configured by using the **no security wpa wpa2 ciphers aes** command. If the cipher is not reset, configure the cipher.
Step 6	`security wpa psk set-key ascii 0 Cisco123`	Specifies a preshared key.
Step 7	`security wpa wpa3`	Enables WPA3 support. **Note:** If both WPA2 and WPA3 are supported (SAE and PSK together), it is optional to configure PMF. However, you cannot disable PMF. For WPA3, PMF is mandatory.
Step 8	`security wpa akm sae`	Enables AKM SAE support.
Step 9	`security wpa akm psk`	Enables AKM PSK support.
Step 10	`radio policy dot11 24ghz`	Enables the 2.4-GHz band.
Step 11	`radio policy dot11 5ghz`	Enables the 5-GHz band.
Step 12	`no shutdown`	Enables the WLAN.
Step 13	`end`	Returns to the privileged EXEC mode.

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Personal Transition Mode Disable

Transition Disable is an indication from an AP to a STA, that the STA is to disable certain transition modes for subsequent connections to the AP's network.

A STA implementation might enable certain transition modes (and possibly other legacy security algorithms) in a network profile. For example, a WPA3-Personal STA might by default enable WPA3-Personal transition mode in a network profile, which enables a PSK algorithm. However, when a network (fully) supports the most secure algorithm defined in a transition mode, it can use the Transition Disable indication to disable transition modes for that network on a STA, and therefore provide protection against downgrade attacks.

Note: An AP that uses Transition Disable indication is not required to disable the corresponding transition mode(s) on its own BSS. For example, the APs in a WPA3-Personal network might use Transition Disable indication to ensure that all STAs that support WPA3-Personal are protected against downgrade attacks while still enabling WPA3-Personal transition mode on their BSS so that legacy STAs can connect.

On one side, this is good for security, as it will migrate all client devices to WPA3 only, as they join the transition mode WLAN, but if the network is composed of multiple physical locations, for example, some are set to WPA2, others to WPA3/WPA2 transition mode, this will cause the migrated clients to fail when moved to a location with WPA2 only.

This is a possible scenario for some large networks, with the same SSID covering different controllers/AP setups and with configurations not matching 100%. The largest example would be Edu Roam, which shares the same SSID name worldwide. Setting this could have serious issues for clients moving across different network providers, so please use this with care, and only if you can ensure the same security setting is set properly across all network locations.

Note: This method is not generally recommended and should be enabled only when it is absolutely necessary.

The below section explains how to enable Transition Disable in the WLAN.

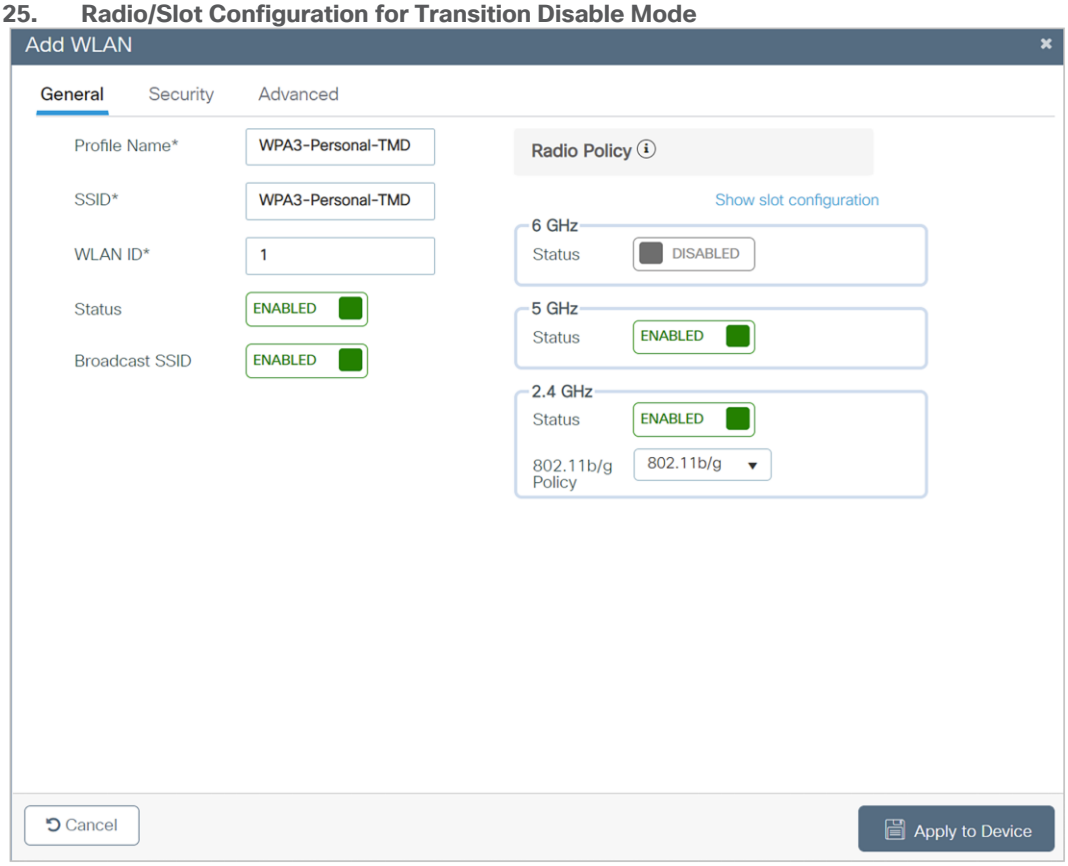
WPA3-Personal Transition Mode Disable GUI Configuration

The following steps create a WLAN with WPA3-Personal-level security with Transition Disable:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID are populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.

© 2024 Cisco and/or its affiliates. All rights reserved.

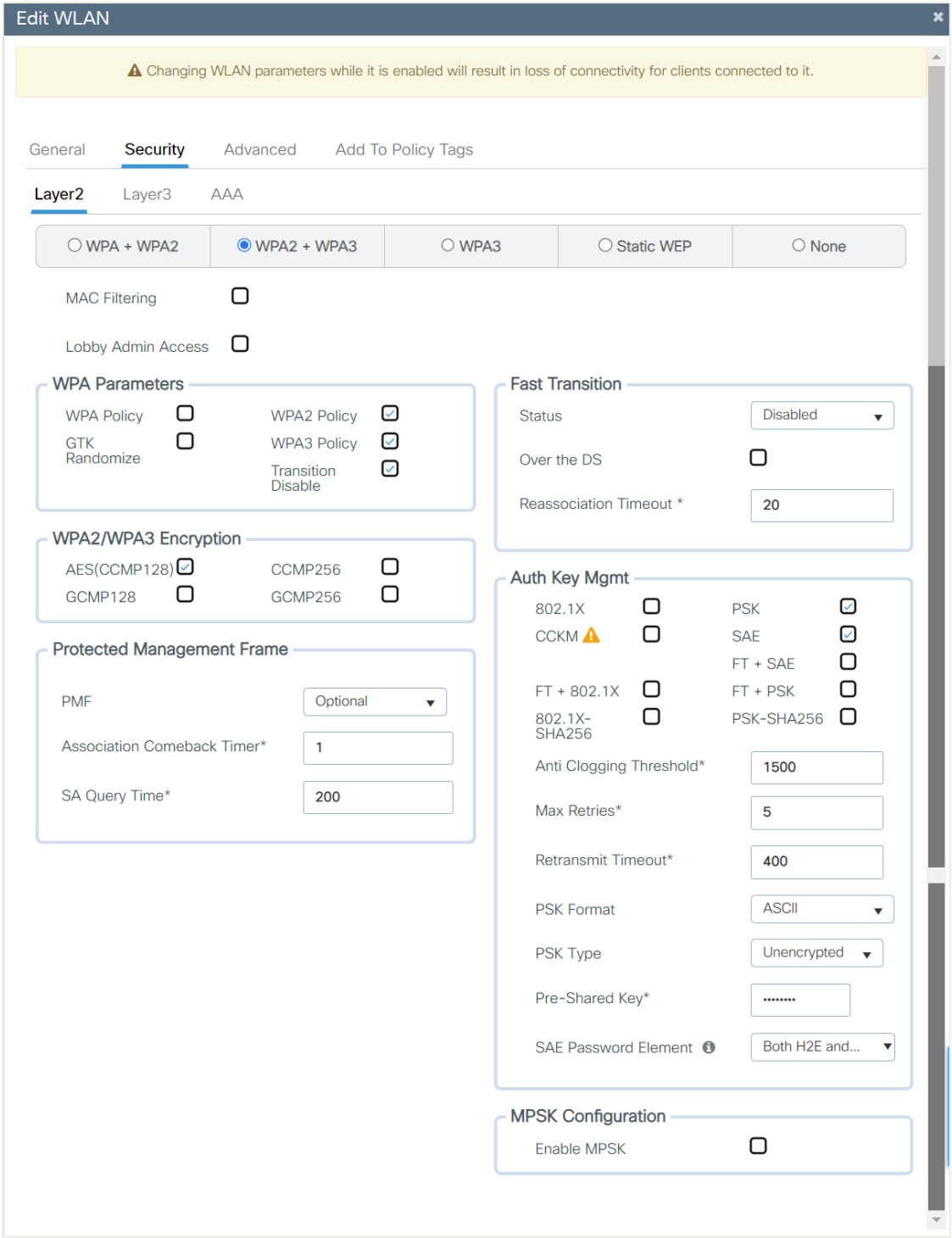
Figure 25. Radio/Slot Configuration for Transition Disable Mode



5. Disable the **6 GHz** band.
6. Under the **Security tab**, enable the **WPA2+WPA3** option.
7. Disable Fast Transition.
8. Scroll down to the **WPA Parameters**. Check the **WPA2** and **WPA3 Policy**, **AES**, and **SAE** and **PSK** check boxes as AKM.
9. Enter the **Pre-Shared Key** and from the **PSK Format** drop-down list, choose the **PSK format** and from the **PSK Type** drop-down list, choose the **PSK type**.
10. Confirm that the **PMF** be Optional.
11. Enable the **Transition Disable** option in WPA Parameters.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 26. Security and AKM configuration for Transition Disable Mode



© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Personal Transition Mode Disable CLI Configuration

Table 12. WPA3-Personal transition mode disable CLI configuration

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan WPA3-Personal-TMD 1 WPA3-Personal-TMD`
		Enters the WLAN configuration sub-mode.

Step 3	`no security wpa akm dot1x`	Disables security AKM 802.1X.
Step 4	`security wpa wpa3`	Enables WPA3.
Step 5	`no security ft`	Disables 802.11r Fast Transition on the WLAN.
Step 6	`security wpa wpa2`	Enables WPA2 security. PMF is optional now.
Step 7	`security wpa wpa2 ciphers aes`	Enables AES/CCMP128 ciphers.

Step 8	`security wpa psk set-key ascii value preshared-key`
	`Example:`
	`Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`
		Specifies a preshared key.

Step 9	`security wpa akm sae`	Enables AKM SAE support.
Step 10	`security wpa akm psk`	Enables AKM PSK.
Step 11	**`transition-disable`**	Enables Transition Disable.
Step 11	`radio policy dot11 24ghz`	Enables 2.4-GHz.
Step 12	`radio policy dot11 5ghz`	Enables 5-GHz.
Step 13	`no shutdown`	Enables the WLAN.
Step 14	`End`	Returns to the privileged EXEC mode.

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA2+WPA3-Personal Transition Mode with 6 GHz

Per 6-GHz standard, broadcasting a WLAN in the 6-GHz band is not allowed when configured with WPA2 security (applies to both WPA2 only and WPA2+WPA3 WLAN), so this essentially leads to behavior that we don't support 6-GHz radio when WLAN is configured with WPA2.

We do have use cases like 2.4-GHz/5-GHz that can be on PSK/SAE AKM with PMF optional and 6-GHz with SAE AKM for WPA3 on the same SSID, which is not a valid configuration pre-17.12.1.

To support these deployments, the recommendation in pre-17.12.1 SW versions were to use WPA2+WPA3 transition mode with the same WLAN with different profiles to support both legacy and the latest 6-GHz clients. The challenge with this design is roaming. The roaming b/w bands in this configuration are not supported and it is always full roam, which is not preferred.

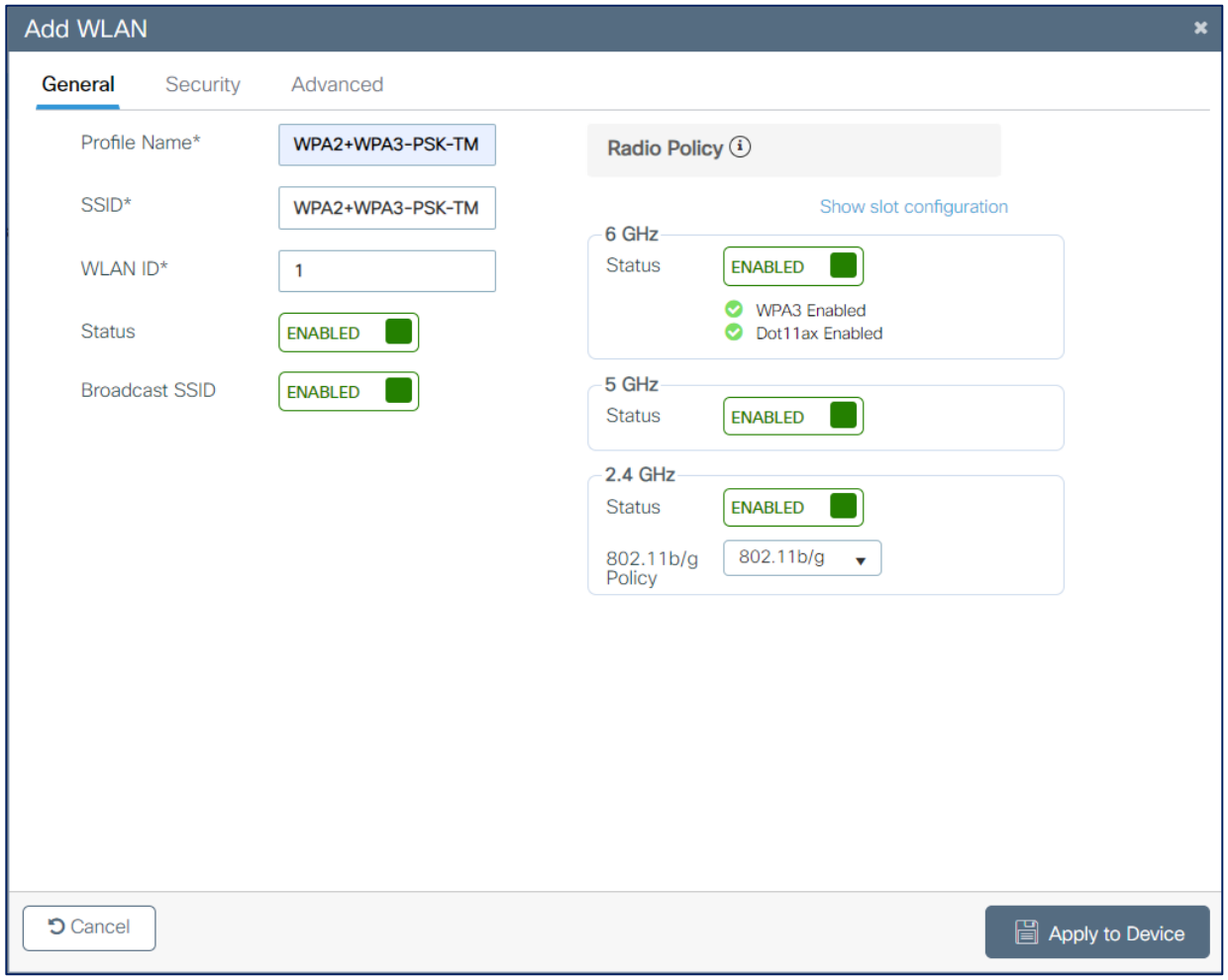
Starting from 17.12.1, we are supporting transition mode with pure WPA3 for 6 GHz band, which allows users to enable WPA2+WPA3 in the same WLAN with 6-GHz. This mode eliminates the need to create two different profiles to accommodate legacy and the latest 6-GHz devices. In this mode, WPA2+WPA3 transition mode can be used in 2.4-GHz/5-GHz and only WPA3 relevant configs will be pushed on the 6-GHz band when WLAN has both WPA2 and WPA3 configurations.

WPA2+WPA3-Personal Transition Mode with 6 GHz GUI Configuration

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). Both the **SSID** and **WLAN ID** are populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have Access Points (APs) associated with this profile begin broadcasting this configured WLAN.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 27. Radio/Slot Configuration

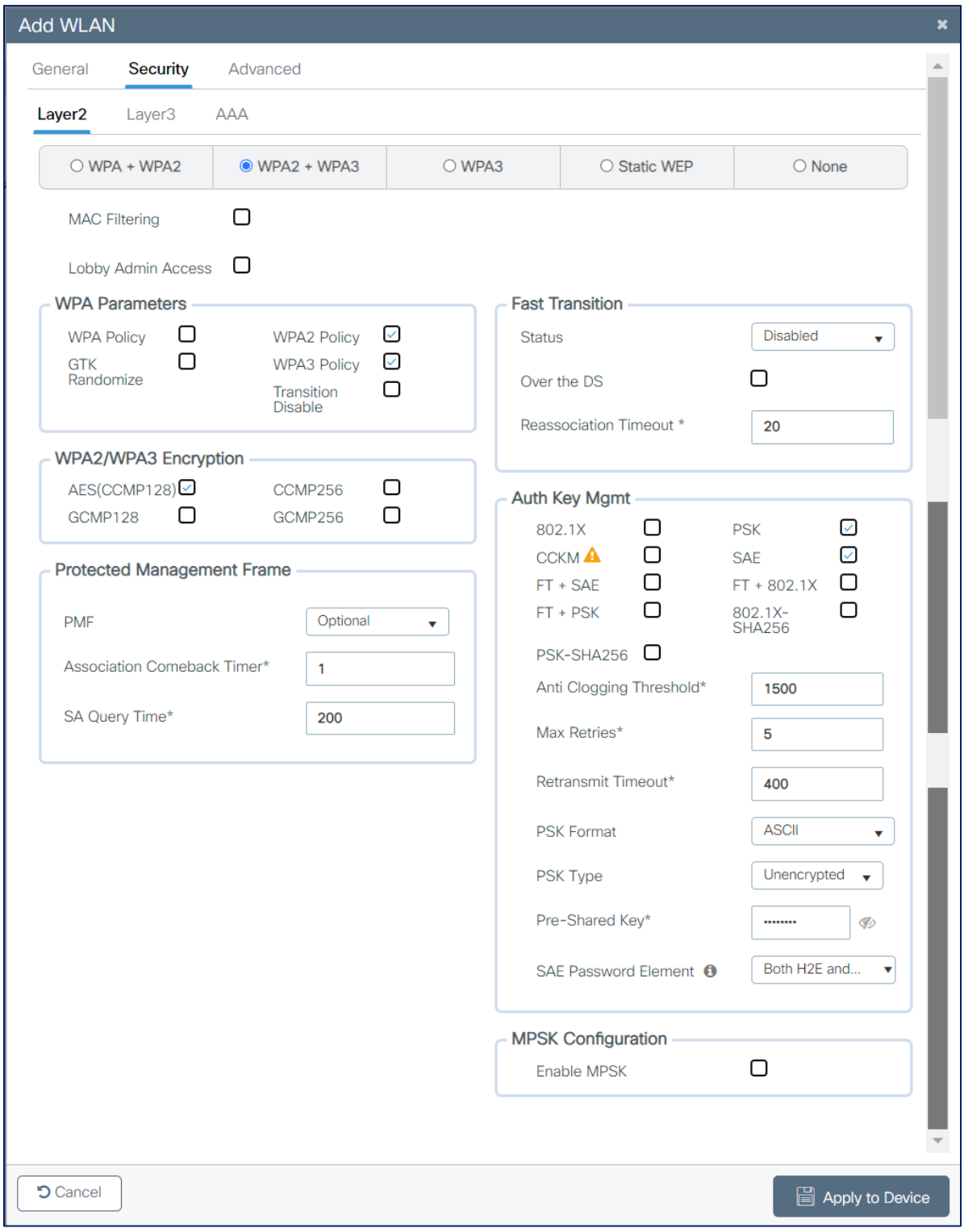


5. Click the **Security** tab > **Layer 2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA3**.
6. Confirm that the PMF is set to Optional.

   Note: Though PMF is optional, with WPA3 configuration, it will be considered required for the 6-GHz band.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 28. Configuration



7. Choose the **WPA2** & **WPA3 Policy** in **WPA Parameters**, **AES(CCMP128)** in **WPA2/WPA3** encryption, and enable **PSK** & **SAE** check boxes, then unselect any other selected parameters.
8. Input the Shared key.
9. Click **Apply to Device** to save and finish the WLAN creation process.

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA2+WPA3-Personal Transition Mode with 6 GHz CLI Configuration

The following steps create a WLAN with WPA3+WPA2-Personal transition mode with 6 GHz enabled:

Table 13. WPA2+WPA3 Transition mode with pure 6 GHz CLI configuration

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan WPA2+WPA3-PTM 1 WPA2+WPA3-PTM`
		Enters the WLAN configuration submode.

Step 3	`no security wpa akm dot1x`	Disables security AKM for 802.1X.
Step 4	`no security ft`	Disables 802.11r Fast Transition on the WLAN.
Step 5	`security wpa wpa2 ciphers aes`	Configures the WPA2 cipher. Note: You can check whether the cipher is configured by using the no security wpa wpa2 ciphers aes command. If the cipher is not reset, configure the cipher.
Step 6	`security wpa psk set-key ascii 0 Cisco123`	Specifies a preshared key.
Step 7	`security wpa wpa3`	Enables WPA3 support. Note: If both WPA2 and WPA3 are supported (SAE and PSK together), it is optional to configure PMF. However, you cannot disable PMF. For WPA3, PMF is mandatory.
Step 8	`security wpa akm sae`	Enables AKM SAE support.
Step 9	`security wpa akm psk`	Enables AKM PSK support.
Step 10	`radio policy dot11 6ghz`	Enables the 6-GHz band.
Step 11	`radio policy dot11 24ghz`	Enables the 2.4-GHz band.
Step 12	`radio policy dot11 5ghz`	Enables the 5-GHz band.
Step 13	`no shutdown`	Enables the WLAN.
Step 14	`end`	Returns to the privileged EXEC mode.

© 2024 Cisco and/or its affiliates. All rights reserved.

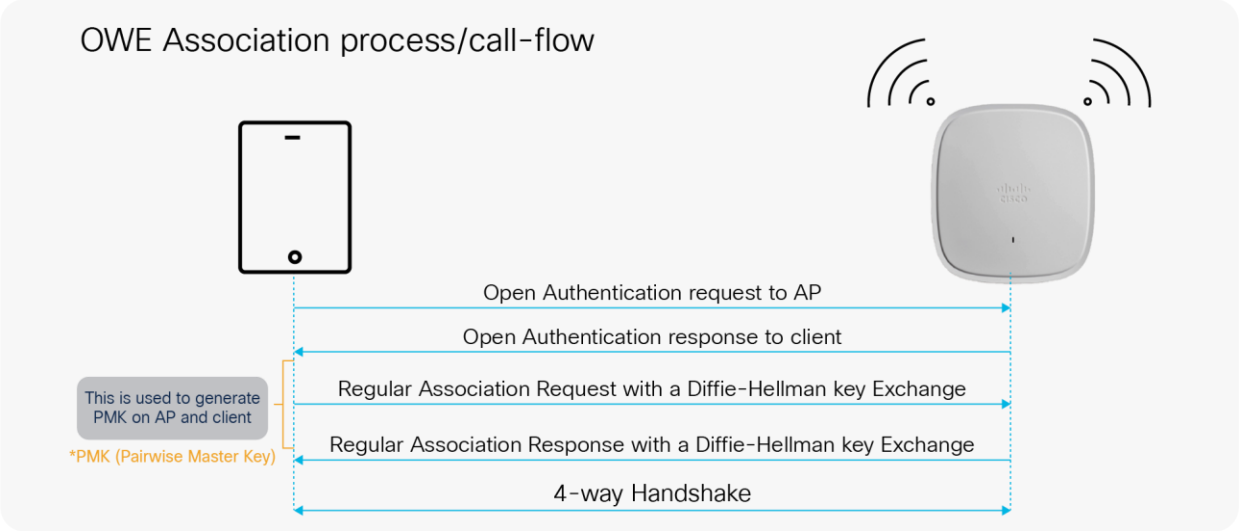
WPA2+WPA3-Personal Transition Mode with 6 GHz CLI Output

```
#show wlan summary

Number of WLANs: 1

ID   Profile Name                    SSID                            Status 2.4GHz/5GHz
Security
6GHz Security
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
---
1    WPA2+WPA3-PTM                   WPA2+WPA3-PTM                   UP     [WPA2 +
WPA3][PSK][SAE][AES]
[WPA3][SAE][AES]
```

OWE

OWE is a security method paired with an open-security wireless network to provide it with encryption to protect the network from eavesdroppers. With OWE, the client and AP perform a Diffie-Hellman key exchange during the endpoint association packet exchange and use the resulting PMK to conduct the 4-way handshake. Being associated with open-security wireless networks, OWE can be used with regular open networks as well as those associated with captive portals.

Figure 29. OWE Endpoint and Network Handshake Process



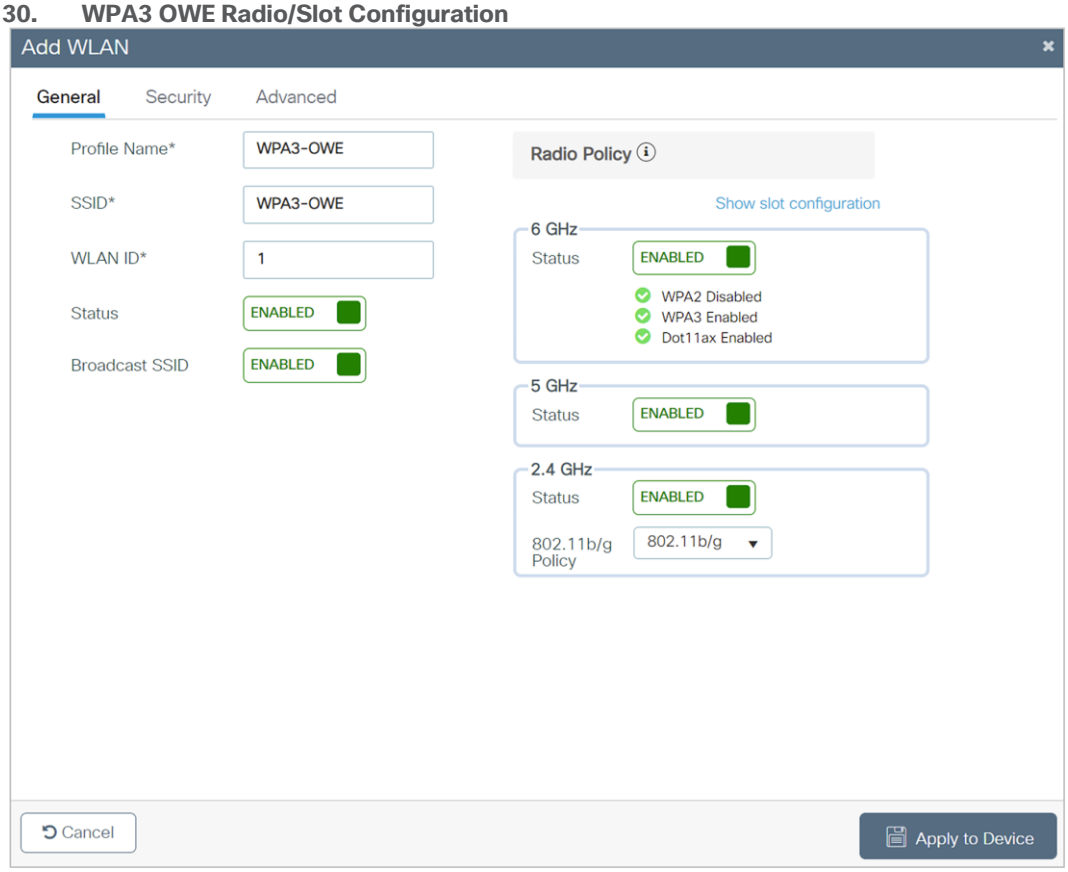
WPA3 OWE GUI Configuration

The following steps create a WLAN with WPA3 OWE security:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and the WLAN ID will be populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons.

© 2024 Cisco and/or its affiliates. All rights reserved.

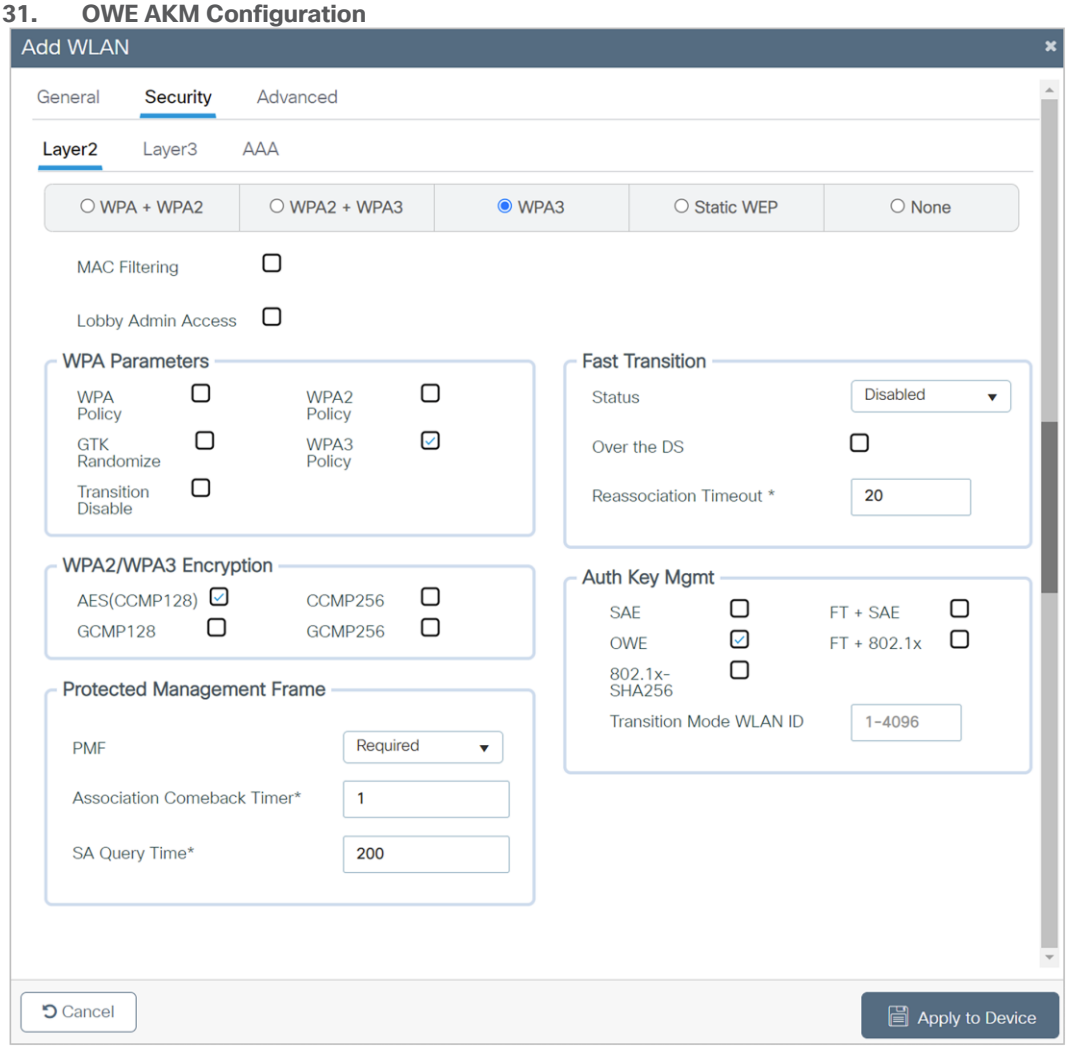
Figure 30. WPA3 OWE Radio/Slot Configuration



5. Click the **Security > Layer 2** tab. From the Layer 2 Security Mode drop-down list, choose WPA3.
6. From the **Fast Transition** drop-down list, select **Disabled**.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 31. OWE AKM Configuration



7. Check the **WPA3 Policy, AES (CCMP 128)**, and **OWE** check boxes. Uncheck any other selected parameters.
8. Click **Apply to Device** to save and finish the WLAN creation process.

WPA3 OWE CLI Configuration

The following steps create a WLAN with WPA3 OWE security:

Table 14. WPA3 OWE CLI configuration

	Command	Purpose

Step 1	`configure terminal`
	Example:
	`Device# configure terminal`
		Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan WPA3 1`
		Enters the WLAN configuration sub-mode.

© 2024 Cisco and/or its affiliates. All rights reserved.

	Command	Purpose
	WPA3	
Step 3	no security ft over-the-ds	Disables Fast Transition over the data source on the WLAN.
Step 4	no security ft	Disables 802.11r Fast Transition on the WLAN.
Step 5	no security wpa akm dot1x	Disables security AKM for 802.1X.
Step 6	no security wpa wpa2	Disables WPA2 security. PMF is disabled now.
Step 7	security wpa wpa2 ciphers aes	Enables WPA2 ciphers for AES. Note: The ciphers for WPA2 and WPA3 are common.
Step 8	security wpa wpa3	Enables WPA3 support.
Step 9	security wpa akm owe	Enables WPA3 OWE support.
Step 10	no shutdown	Enables the WLAN.
Step 11	End	Returns to the privileged EXEC mode.

WPA3 OWE Transition Mode GUI Configuration

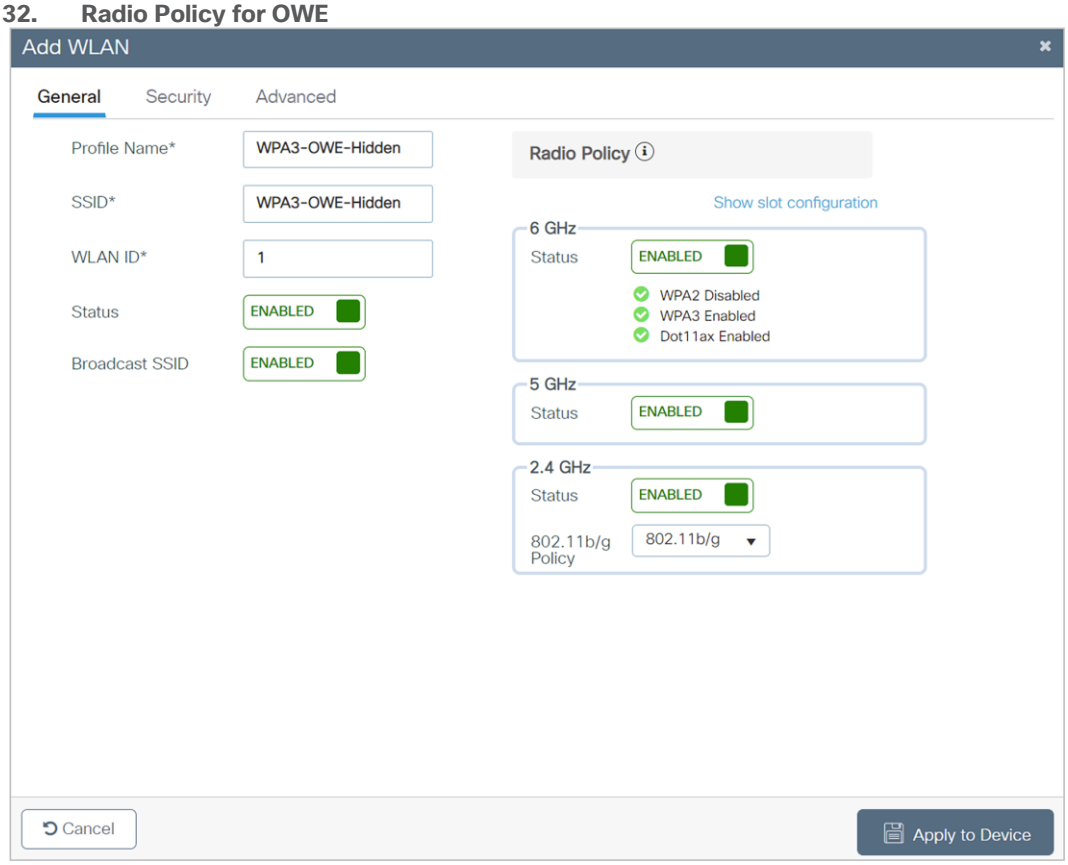
The Transition mode was introduced to the public since not all devices support enhanced open capability (refer to the device interoperability matrix). Transition mode is designed to make the enhanced open OWE mode more adaptable. The Wi-Fi Alliance recommends using this strategy to implement an enhanced open wireless network in an environment where not all devices support this mode. The OWE Transition mode requires a separate open SSID configured with properties similar to those of the enhanced open OWE SSID. Both OWE and open WLAN have a corresponding Transition mode WLAN ID, which means that the OWE WLAN has a Transition mode ID set to the open WLAN ID, and the open WLAN has a Transition mode ID set to the OWE WLAN ID.

Part 1: The following steps create a hidden WLAN with WPA3 OWE security:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID are populated automatically.
4. Disable the **Status** and **Broadcast SSID** toggle buttons.
5. Note the **WLAN ID** of the **WLAN**.

© 2024 Cisco and/or its affiliates. All rights reserved.

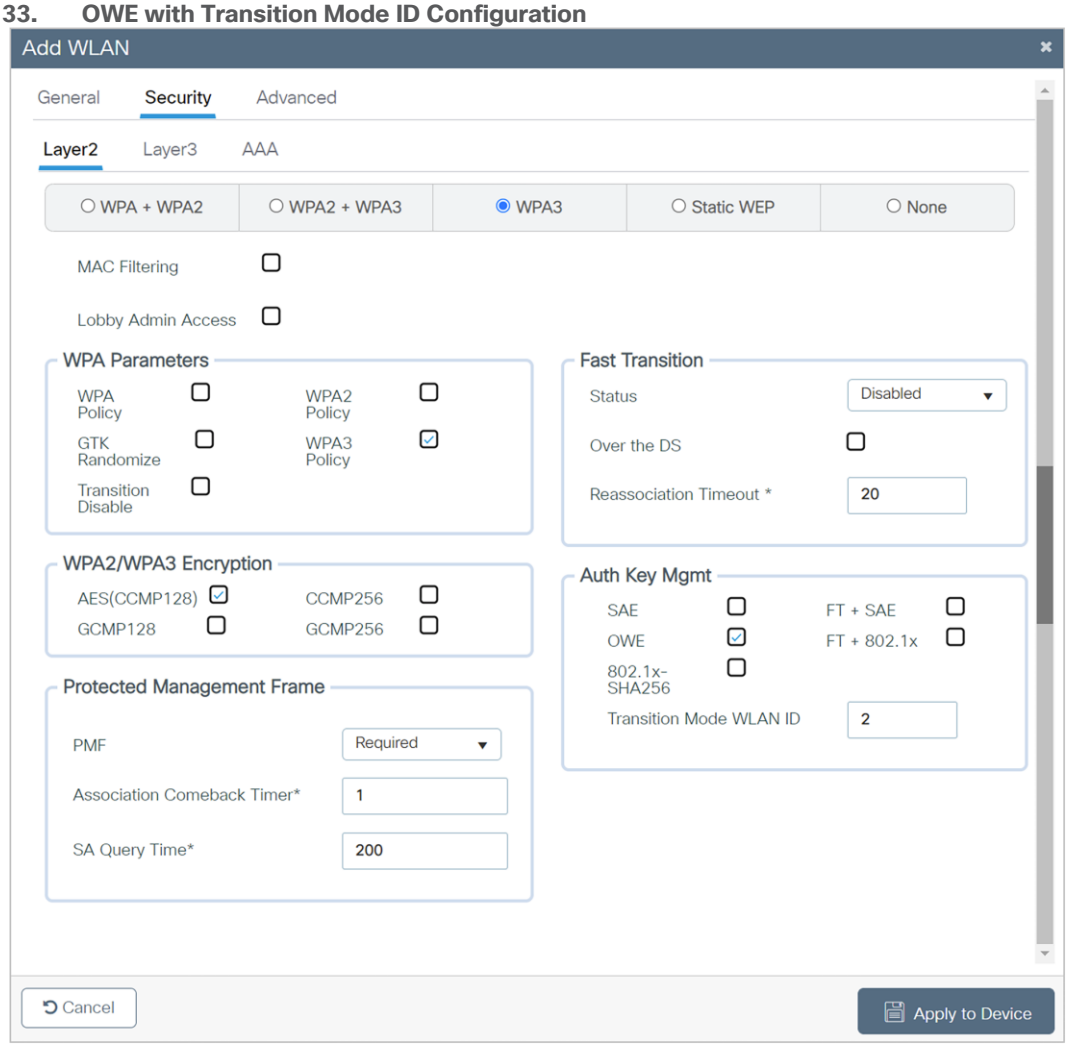
Figure 32. Radio Policy for OWE



6. Click the **Security > Layer 2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA3**.
7. Confirm that the **PMF** is set to **Required**.
8. From the **Fast Transition** drop-down list, select **Disabled**.
9. Check the **WPA3 Policy, AES (CCMP 128)**, and **OWE** check boxes. Uncheck any other selected parameters.
10. Enter the **Transition mode WLAN ID**, which will be the WLAN ID of the SSID that will be configured next.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 33. OWE with Transition Mode ID Configuration



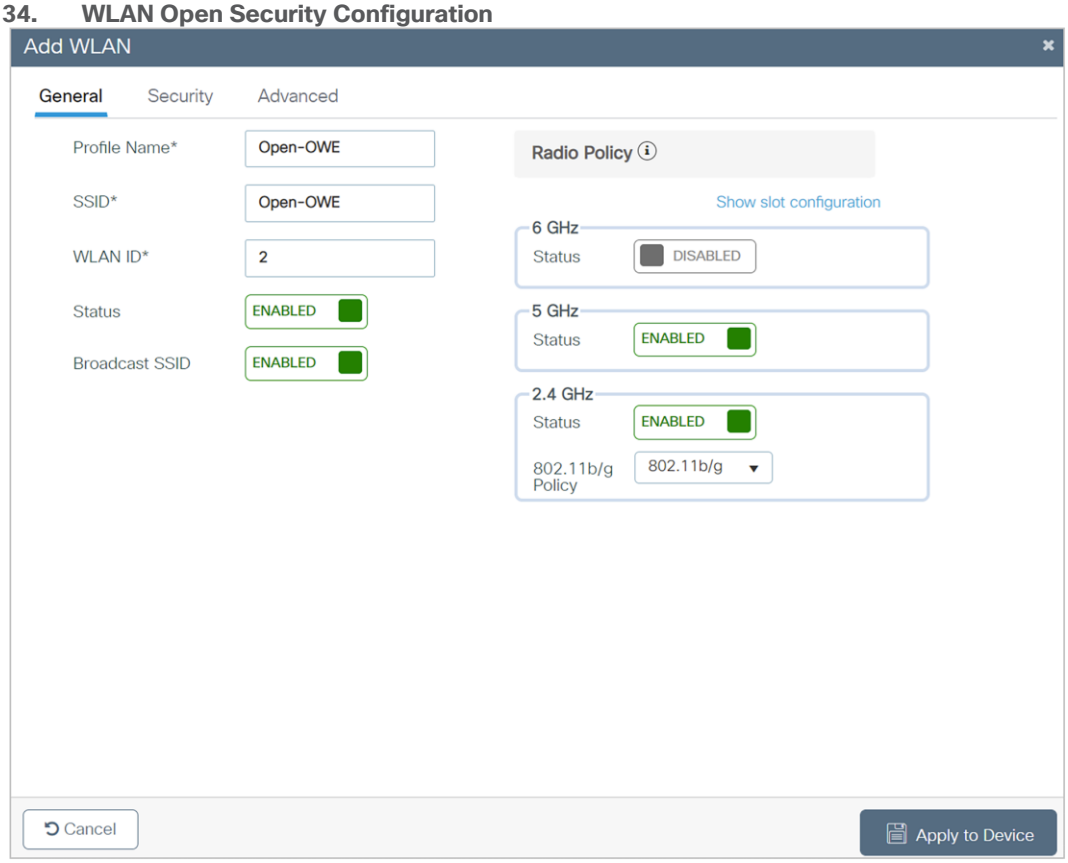
11. Click **Apply to Device** to save and finish the WLAN creation process.

Part 2: The following steps create a WLAN with open security:

1. Choose Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier).
4. The **SSID** must match the enhanced open SSID. The **WLAN ID** is populated automatically.
5. Enable the **Status** and **Broadcast SSID** toggle buttons.

© 2024 Cisco and/or its affiliates. All rights reserved.

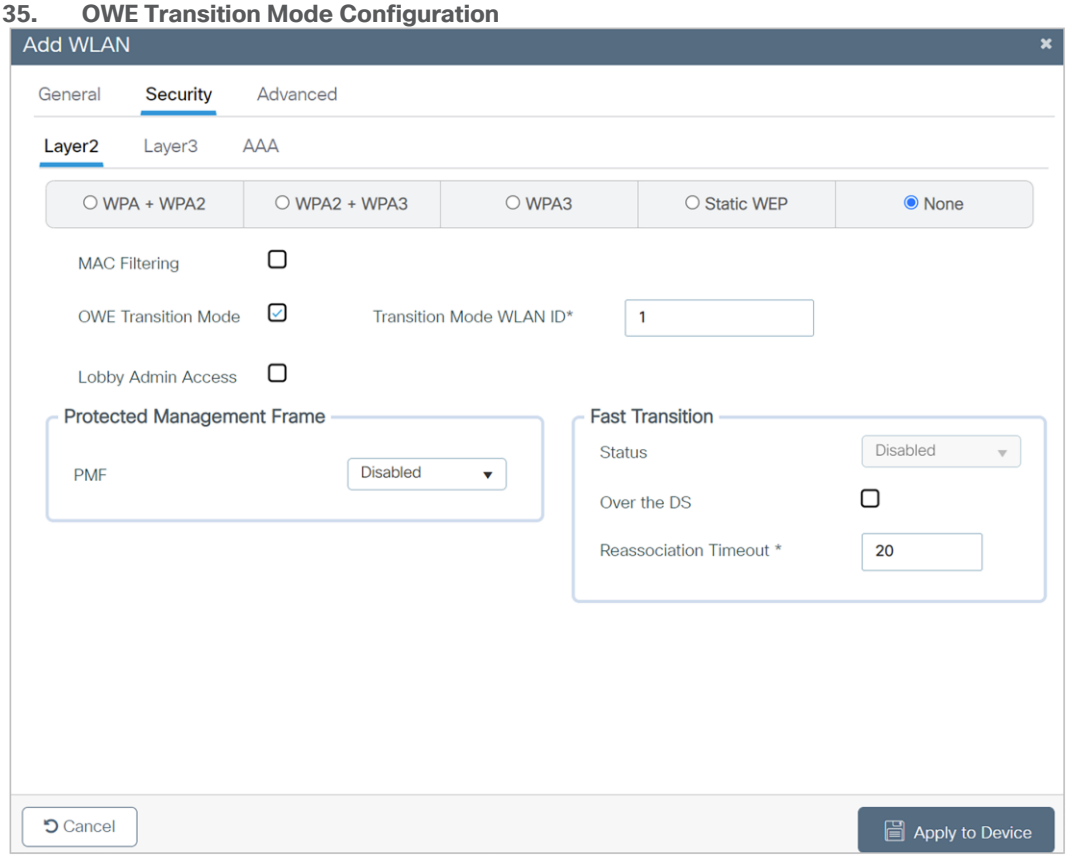
Figure 34. WLAN Open Security Configuration



6. Click the **Security > Layer 2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA3**.

© 2024 Cisco and/or its affiliates. All rights reserved.

Figure 35. OWE Transition Mode Configuration



7. For the **Transition Mode WLAN ID**, enter the **WLAN ID** that has Layer 2 security set to **Enhanced Open** to be mapped to the open WLAN.
8. Click **Apply to Device** to save and finish the WLAN creation process.

WPA3 OWE Transition Mode CLI Configuration

Part1: The following steps create a hidden WLAN with WPA3 OWE security:

Table 15. WPA3 OWE transition mode CLI configuration

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan WPA3-OWE-Hidden 1 WPA3-OWE-Hidden`
		Enters the WLAN configuration sub-mode.

Step 3	`no broadcast-ssid`	Disables SSID broadcast.
Step 4	`no security ft over-the-ds`	Disables Fast Transition over the data source on the WLAN.
Step 5	`no security ft`	Disables 802.11r Fast Transition on the WLAN.
Step 6	`no security wpa akm dot1x`	Disables security AKM for 802.1X.

© 2024 Cisco and/or its affiliates. All rights reserved.

	Command	Purpose
Step 7	`no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 8	`security wpa akm owe`	Enables WPA3 OWE support.
Step 9	`security wpa transition-mode-wlan-id 2`	Enables Transition mode.
Step 10	`security wpa wpa3`	Enables WPA3 support.
Step 11	`no shutdown`	Enables the WLAN.
Step 12	`End`	Returns to the privileged EXEC mode.

Part 2: The following steps create a WLAN with open OWE security:

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.

Step 2	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device(config)# wlan Open-OWE 2 Open-OWE`
		Enters the WLAN configuration sub-mode.
		Note: The SSID of the hidden WLAN and the open WLAN must be the same.

Step 3	`no security ft over-the-ds`	Disables Fast Transition over the data source on the WLAN.
Step 4	`no security ft`	Disables 802.11r Fast Transition on the WLAN.
Step 5	`no security wpa akm dot1x`	Disables security AKM for 802.1X.
Step 6	`no security wpa`	Disables security.
Step 7	`no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	`security wpa transition-mode-wlan-id 1`	Enables Transition mode.
Step 9	`no shutdown`	Enables the WLAN.
Step 10	`end`	Returns to the privileged EXEC mode.

Client Interoperability Matrix

WPA3-supported AP Modes and Supported Clients

Table 16. WPA3 supported AP modes and Clients

© 2024 Cisco and/or its affiliates. All rights reserved.

	WPA3 Support Matrix									
WPA3 protocol	**Cipher/AKM**	**AP mode Local**	**AP mode Flex(Central Auth)**	**AP mode Flex(Local Auth)**	**Apple (11/12/13)**	**Samsung S21/Google Android**	**Intel**	**Apple iPad(iPadOS: 16.3)**	**MacOS(M1 or above)**	**Zebra(TCS53/58/73)**
WPA3-Personal	WPA3-SAE AES CCMP128	Supported	Supported	Supported FT: Not supported	Supported FT: Not supported	Supported FT-SAE: Supported H2E: Supported in iOS16	Supported FT-SAE: Supported only in S21 Galaxy Ultra/Galaxy Z Fold	Supported: H2E only FT-SAE: Supported in Linux WPA Supplicant(AX210)	Supported FT-SAE: Supported	Supported FT-SAE: Supported Adaptive FT: Not supported
WPA3-Enterprise	WPA3-802.1x-SHA256 AES CCMP 128	Supported	Not Supported	Not Supported	Supported	Supported	Supported	Supported: SHA256 and FT-OTA Not supported: FT-ODS	Supported: SHA256, Adaptive and FT-OTA	*Supported* Adaptive FT: Not supported
	WPA3-Enterprise GCMP128 SuiteB 1x	Supported	Not Supported	Not supported	Not supported	Not supported	Not supported	Not supported: GCMP128, FT-OTA, and FT-ODS	Not supported	Not supported
	WPA3-Enterprise GCMP256 SuiteB 192 bit	Supported	Not Supported	Not supported	Not supported	Supported	Supported Not supported:FT-ODS	Supported: GCMP256 Not supported: FT (both FT-OTA and FT-ODS)	Supported	Supported: FT-ODS/ITA
OWE	WPA3-OWE AES CCMP128	Supported	Supported	Supported	Supported	Not supported	Supported	Supported: OWE Auth	Supported: OWE Auth	Supported

© 2024 Cisco and/or its affiliates. All rights reserved.

Useful Catalyst 9800 Controller Commands

To view the system-level statistics for a client that has undergone successful SAE authentication, SAE authentication failures, SAE ongoing sessions, or SAE commits, and to confirm message exchanges, use the following show command:

```
show wireless stats client detail
```

To view the WLAN summary details, use the following command:

- `show wlan summary`
- `show wlan all`
- `show wlan name <wlan-name>`
- `show wlan id {Starting 17.12.1, the security section on the WLAN is displayed individually for 2.4GHz/5GHz band and 6GHz band as below}`

```
#show wlan id 1
WLAN Profile Name     : WPA2+WPA3-TransitionMode
================================================
Identifier                                    : 1
Description                                   :
Network Name (SSID)                           : WPA2+WPA3-TransitionMode
Status                                        : Enabled
....
    Security-2.4GHz/5GHz
         ....
     Security-6GHz
....
#
```

To view the correct AKM for a client that has undergone SAE authentication, use the following command:

```
show wireless client mac-address <xxxx.xxxx.xxxx> detail
```

To view a list of the PMK cache stored locally:

```
show wireless pmk-cache
```

Useful Catalyst AP Commands

Configure debugging of WPA3 on a client by entering this command:

```
debug client client-mac-address
```

Configure debugging of SAE events and details by entering this command:

```
debug sae {events | details} {enable | disable}
```

References

- Cisco Catalyst 9800 Series Wireless Controller 17.8.1 Configuration Guide: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-8/config-guide/b_wl_17_8_cg.html

© 2024 Cisco and/or its affiliates. All rights reserved.

- Cisco Catalyst 9100 Access Points documentation: https://www.cisco.com/c/en/us/support/wireless/catalyst-9100ax-access-points/series.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

© 2024 Cisco and/or its affiliates. All rights reserved.