WLAN Security

Information About AAA Override

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

Prerequisites for Layer 2 Security

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on the information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:

- None (open WLAN)
- WPA+WPA2

Note

- Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and Wi-Fi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP) with 802.1X, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X.
- A WLAN configured with TKIP support will not be enabled on an RM3000AC module.

- Static WEP (not supported on Wave 2 APs)

How to Configure WLAN Security

Configuring Static WEP Layer 2 Security Parameters (CLI)

Before you begin

You must have administrator privileges.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

Before you begin

You must have administrator privileges.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**security wpa** **Example:** `Device(config-wlan)# security wpa`	
Step 3	**security wpa wpa1** **Example:** `Device(config-wlan)# security wpa wpa1`	Enables .
Step 4	**security wpa wpa1 ciphers** [**aes** | **tkip**] **Example:**	Specifies the WPA1 cipher. Choose one of the following encryption types: • **aes**—Specifies WPA/AES support.

	Command or Action	Purpose
	`Device(config-wlan)#` **`security wpa wpa1 ciphers aes`**	• **tkip**—Specifies WPA/TKIP support.
Step 5	**security wpa akm** {**cckm**| **dot1x** | **dot1x-sha256** | **ft** | **psk** |**psk-sha256**}	Enable or disable Cisco Centralized Key Management, 802.1x, 802.1x with SHA256 key derivation type, Fast Transition, PSK or PSK with SHA256 key derivation type. **Note** You cannot enable 802.1x and PSK with SHA256 key derivation type simultaneously. **Note** When you configure Cisco Centralized Key Management SSID, you must enable the **ccx aironet-iesupport** for Cisco Centralized Key Management to work.
Step 6	**security wpa wpa2** **Example:** `Device(config-wlan)#` **`security wpa`**	Enables WPA2.
Step 7	**security wpa wpa2 ciphers aes** **Example:**	Configure WPA2 cipher.

Step 8	**end**
	Example:
	`Device(config)#` **`end`**
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.