WLAN Security

Information About WPA1 and WPA2

Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

By default, WPA1 uses Temporal Key Integrity Protocol (TKIP) and Message Integrity Check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). By default, both WPA1 and WPA2 use the 802.1X for authenticated key management. However, the following options are also available:

- PSK—When you choose PSK (also known as WPA preshared key or WPA passphrase), you need to configure a preshared key (or a passphrase). This key is used as the Pairwise Master Key (PMK) between clients and authentication server.
- Cisco Centralized Key Management uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller , typically in under 150 milliseconds (ms). Cisco Centralized Key Management reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. Cisco Centralized Key Management fast secure roaming ensures that there is no perceptible delay in time-sensitive applications, such as wireless Voice over IP (VoIP), Enterprise Resource Planning (ERP), or Citrix-based solutions. Cisco Centralized Key Management is a CCXv4-compliant feature. If Cisco Centralized Key Management is selected, only Cisco Centralized Key Management clients are supported.

When Cisco Centralized Key Management is enabled, the behavior of access points differs from the controller 's for fast roaming in the following ways:

- If an association request sent by a client has Cisco Centralized Key Management enabled in a Robust Secure Network Information Element (RSN IE) but Cisco Centralized Key Management IE is not encoded and only PMKID is encoded in RSN IE, then the controller does not do a full authentication. Instead, the controller validates the PMKID and does a four-way handshake.
- If an association request sent by a client has Cisco Centralized Key Management enabled in RSN IE and Cisco Centralized Key Management IE is encoded and only PMKID is present in the RSN IE, then the AP does a full authentication. The access point does not use PMKID sent with the association request when Cisco Centralized Key Management is enabled in RSN IE.

- 802.1X+Cisco Centralized Key Management—During normal operation, 802.1X-enabled clients mutually authenticate with a new access point by performing a complete 802.1X authentication, including communication with the main RADIUS server. However, when you configure your WLAN for 802.1X and Cisco Centralized Key Management fast secure roaming, Cisco Centralized Key Management-enabled clients securely roam from one access point to another without the need to reauthenticate to the RADIUS server. 802.1X+Cisco Centralized Key Management is considered as an optional Cisco Centralized Key Management because both Cisco Centralized Key Management and non-Cisco Centralized Key Management clients are supported when this option is selected.

On a single WLAN, you can allow WPA1, WPA2, and 802.1X/PSK/Cisco Centralized Key Management/802.1X+Cisco Centralized Key Management clients to join. All of the access points on such a WLAN advertise WPA1, WPA2, and 802.1X/PSK/Cisco Centralized Key Management/ 802.1X+Cisco Centralized Key Management information elements in their beacons and probe responses. When you enable WPA1 and/or WPA2, you can also enable one or two ciphers, or cryptographic algorithms, designed to protect data traffic. Specifically, you can enable AES and/or TKIP data encryption for WPA1 and/or WPA2. TKIP is the default value for WPA1, and AES is the default value for WPA2.

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.

Configuring AAA Override

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:**	Configures WLAN policy profile and enters the wireless policy configuration mode.

	Command or Action	Purpose
	`Device(config)# wireless profile policy test-wgb`	
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA policy override. **Note** If VLAN is not pushed from the RADIUS server, the VLAN Override feature can be disabled from the RADIUS server.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Information About VLAN Override

The VLAN override requires the AAA Override to be enabled under the Policy Profile.

You can assign VLAN from the RADIUS server in two ways:

- Using IEFT RADIUS attributes 64, 65, and 81—The attribute 81 can be a VLAN ID, VLAN name, or VLAN group name. Both VLAN name and VLAN group are supported. Therefore, VLAN ID does not need to be predetermined on RADIUS.

  The RADIUS user attributes used for the VLAN ID assignment are:

  - 64 (Tunnel-Type)—Must be set to VLAN (Integer = 13).
  - 65 (Tunnel-Medium-Type)—Must be set to 802 (Integer = 6).
  - 81 (Tunnel-Private-Group-ID)—Must be set to the corresponding VLAN ID, VLAN name, or VLAN group name.

- Using Aire-Interface-Name attribute—Use this attribute to assign a successfully authenticated user to a VLAN interface name (or VLAN ID) as per the user configuration. When you use this attribute, the VLAN name is returned as a string.

The VLAN ID is 12-bits, and takes a value between 1 and 4094, inclusive. Because the Tunnel-Private-Group-ID is of type string, as defined in RFC2868 for use with IEEE 802.1X, the VLAN ID integer value is encoded as a string. When these tunnel attributes are sent, it is necessary to fill in the Tag field.

Configuring Override VLAN for Central Switching

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**vlan** *vlan-id* **Example:** `Device(config)# vlan 20`	Defines VLANs that can be pushed from the RADIUS server. **Note** The valid VLAN ID ranges from 1 to 4094.
Step 3	**name** *vlan-name* **Example:** `Device(config-vlan)# name vlan_ascii`	(Optional) Changes the default name of the VLAN.
Step 4	**end** **Example:** `Device(config-vlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Override VLAN for Local Switching

If the VLAN name ID mapping under flex profile is newly added or updated, then the WLAN policy profiles having a matching VLAN name configured, must be shut and unshut. This is to ensure that the updated WLAN-VLAN mapping is pushed to the APs and the client receives the IP address from the intended VLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex_profile_name* **Example:** `Device(config)# wireless profile flex rr-xyz-flex-profile`	Configures a Flex profile.
Step 3	**vlan-name** *vlan_name* **Example:** `Device(config-wireless-flex-profile)# vlan-name vlan_123`	Defines VLANs that can be pushed from the RADIUS server.
Step 4	**vlan-id** *vlan_id* **Example:** `Device(config-wireless-flex-profile-vlan)# vlan-id 23`	Configures VLAN ID. The valid VLAN ID ranges from 1 to 4096.
Step 5	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-wireless-flex-profile-vlan)# end`	Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

VLAN Override on Layer 3 Web Authentication

The VLAN override can be pushed from the RADIUS server during Layer 3 authentication.

When a client gets connected to the controller and authenticated using the RADIUS server for Local Web Authentication (LWA) and Central Web Authentication (CWA), the RADIUS server pushes back in access-accept the new VLAN. If the RADIUS server pushes back a new VLAN in the access-accept, the client goes back to IP learn state on the controller. The controller de-associates the client while maintaining the client state for 30 seconds. Once the client re-associates, the client lands immediately to the new VLAN and re-triggers a new DHCP request. The client then learns a new IP and moves to the RUN state on the controller.

The VLAN Override on Layer 3 Web authentication supports the following:

- Local clients
- Anchored clients
- FlexConnect central authentication, central or local switching

Verifying VLAN Override on Layer 3 Web Authentication

To display the VLAN override after L3 authentication, use the following command:

```
Device# show wireless client mac <mac> detail
[…]
        Vlan Override after L3 Auth: True
```

To display the statistics about client, use the following command:

```
Device# show wireless stats client detail
[…]
      Total L3 VLAN Override vlan change received      : 1
      Total L3 VLAN Override disassociations sent      : 1
      Total L3 VLAN Override re-associations received  : 1
      Total L3 VLAN Override successful VLAN change    : 1
      […]
      L3 VLAN Override connection timeout                          : 0
```

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)

Restrictions for WPA2 and WP3

- You cannot enable security ft or ft-adaptive without enabling WPA2 or WPA3.
- You cannot enable ft-dot1x or ft-psk without enabling WPA2 or WPA3.
- You cannot enable 802.1x or PSK simultaneously with SHA256 key derivation type without enabling WPA2 or WPA3 on a WLAN.
- You cannot configure PMF on WPA1 WLAN without WPA2 security.
- IOS APs do not support WPA3.

Feature History for Fallback for AAA-Overridden VLAN

This table provides release and related information for the feature explained in this module.

This feature is available in all the releases subsequent to the one in which it is introduced in, unless noted otherwise.

Table 1: Feature History for Fallback for AAA-Overridden VLAN

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.6.1	Fallback for AAA-Overridden VLAN	In Cisco IOS XE Bengaluru 17.5.1 and earlier releases, if there is a network with a single AAA server dictating policies that need to be applied to a client; and this client moves across different sites that have different policy definitions. If these policy definitions are not defined on the site to which the client needs to connect, the client does not get access to the network. For example, if a client is to be given access in VLAN 1, and VLAN 1 is not defined on the site to which the client connects, the client is excluded and does not get any access to the network. The Fallback for AAA-Overridden VLAN feature is introduced to allow fallback to policy profile VLAN when the overridden VLAN is not available.

Information About Fallback for AAA- Overridden VLAN

From Cisco IOS XE Bengaluru 17.6.1, fallback for AAA-overridden VLAN or VLAN groups is supported on the wireless policy profile.

A new command is introduced in the wireless policy profile to configure the Fallback for AAA-Overridden VLAN feature. In Cisco IOS XE Bengaluru 17.6.1, you cannot configure the Fallback for AAA Overridden VLAN feature using the GUI.

Central Switching and FlexConnect Mode Scenarios

If fallback is enabled for AAA-overridden VLAN or VLAN groups, you might encounter the following scenarios in Central Switching and FlexConnect modes.

Central Switching:

If the AAA server gives a VLAN policy to a client, and the VLAN ID or the VLAN name is defined in the controller, the client is assigned to the VLAN specified by the AAA server. If the VLAN is not defined in the controller, the client is assigned to a VLAN that is configured on the wireless policy profile.

If a VLAN group is configured on a wireless policy profile, the VLAN, as computed by the existing VLAN group logic, is assigned to the client. In the VLAN group case, fallback to policy profile VLAN occurs only when all the VLANs in the group are not configured in the controller, or, if the VLAN group is not defined in the controller.

If both, AAA-overridden VLAN and the VLAN configured on the wireless policy profile are not defined in the controller, the configuration is termed as invalid, and the client is excluded.

If a VLAN policy is not configured, or, if the default wireless policy profile is configured, the client is assigned a VLAN from the management VLAN.

FlexConnect Mode:

If the AAA server assigns a VLAN policy to a client configured in the FlexConnect profile, the VLAN is resolved by the controller. If the VLAN is not configured on the FlexConnect profile, the behavior of the

VLAN name and the VLAN ID is made consistent, with the help of the fallback feature, and the client receives the IP address from the wireless policy profile configuration.

The following points summarize the FlexConnect mode behavior:

- If AAA VLAN is defined in FlexConnect profile, the client is assigned the AAA VLAN.
- If AAA VLAN is not defined in the FlexConnect profile, FlexConnect VLAN Central Switching is configured, and VLAN is defined in the controller, and the client is assigned AAA VLAN and is centrally switched.
- If AAA VLAN is not defined in the FlexConnect profile, FlexConnect VLAN Central Switching is configured, the VLAN is not defined in the controller, and the client is assigned a VLAN from the wireless policy profile.
- If AAA VLAN is not defined in the FlexConnect profile, and FlexConnect VLAN Central Switching is not configured, the client is assigned a VLAN from the wireless policy profile.

Configuring Fallback for AAA-Overridden VLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)# wireless profile policy wlan-policy-profile-name`	Configures the WLAN policy profile. Enters the wireless policy profile configuration mode.
Step 3	**aaa-override vlan fallback** **Example:** `Device(config-wireless-policy)# aaa-override vlan fallback`	Allows fallback to the policy profile VLAN when the overridden VLAN is not available.

Verifying Fallback for AAA-Overridden VLAN

To verify if the fallback for AAA-overridden VLAN is enabled, use the following command:

```
Device# show wireless profile policy detailed default-policy-profile | sec AAA Policy Params
AAA Policy Params
  AAA Override                  : DISABLED
  NAC                           : DISABLED
  AAA Policy name               : default-aaa-policy
  AAA Vlan Fallback             : ENABLED
```

How to Configure WLAN Security

Configuring Static WEP Layer 2 Security Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the name of the WLAN.

Step 3 In the **Edit WLAN** window, click the **Security** tab.

Step 4 From the **Layer 2 Security Mode** drop-down list, select the **Static WEP** option.

Step 5 (Optional) Check the **Shared Key Authentication** check box to set the authentication type as shared. By leaving the check box unchecked, the authentication type is set to open.

Step 6 Set the **Key Size** as either **40 bits** or **104 bits**.

- 40 bits: The keys with 40-bit encryption must contain 5 ASCII text characters or 10 hexadecimal characters.
- 104 bits: The keys with 104-bit encryption must contain 13 ASCII text characters or 26 hexadecimal characters.

Step 7 Set the appropriate **Key Index**; you can choose between 1 to 4.

Step 8 Set the **Key Format** as either **ASCII** or **Hex**.

Step 9 Enter a valid **Encryption Key**.

- 40 bits: The keys with 40-bit encryption must contain 5 ASCII text characters or 10 hexadecimal characters.
- 104 bits: The keys with 104-bit encryption must contain 13 ASCII text characters or 26 hexadecimal characters.

Step 10 Click **Update & Apply to Device**.

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.

	Command or Action	Purpose
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device# wlan test4 1 test4`	Enters the WLAN configuration submode. *profile-name* is the profile name of the configured WLAN. *wlan-id* is the wireless LAN identifier. The range is 1 to 512. *SSID_Name* is the SSID which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.
Step 3	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 4	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r Fast Transition on the WLAN.
Step 5	**no security wpa**{**akm** | **wpa1** | **wpa2**} **Example:** `Device(config-wlan)# no security wpa wpa1 ciphers tkip`	Disables the WPA/WPA2 support for a WLAN.
Step 6	**security static-wep-key** [**authentication** {**open** | **shared**}] **Example:** `Device(config-wlan)# security static-wep-key authentication open`	The keywords are as follows: • **static-wep-key**—Configures Static WEP Key authentication. • **authentication**—Specifies the authentication type you can set. The values are open and shared.
Step 7	**security static-wep-key** [**encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]] **Example:** `Device(config-wlan)# security static-wep-key encryption 104 ascii 0 1234567890123 1`	The keywords are as follows: • **static-wep-key**—Configures Static WEP Key authentication. • **encryption**—Specifies the encryption type that you can set. The valid values are 104 and 40. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters. • **ascii**—Specifies the key format as ASCII.

	Command or Action	Purpose
		• **hex**—Specifies the key format as HEX.
Step 8	**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 (GUI)

Procedure

Step 1 Click **Configuration** > **Tags and Profiles** > **WLANs**.

Step 2 Click **Add** to add a new WLAN Profile or click the one you want to edit.

Step 3 In the **Edit WLAN** window, click **Security** > **Layer2**.

Step 4 From **Layer 2 Security Mode** drop-down menu, select **WPA + WPA2**.

Step 5 Configure the security parameters and then click **Save and Apply to Device**.

Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

Note The default values for security policy WPA2 are:

- Encryption is AES.
- Authentication Key Management (AKM) is dot1x.

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	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device# wlan test4 1 test4`	Enters the WLAN configuration submode. • *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
		• *wlan-id* is the wireless LAN identifier. The range is 1 to 512. • *SSID_Name* is the SSID that contains 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.
Step 3	**security wpa {akm | wpa1 | wpa2}** **Example:** `Device(config-wlan)# security wpa`	Enables WPA or WPA2 support for WLAN.
Step 4	**security wpa wpa1** **Example:** `Device(config-wlan)# security wpa wpa1`	Enables WPA.
Step 5	**security wpa wpa1 ciphers** [**aes** | **tkip**] **Example:** `Device(config-wlan)# security wpa wpa1 ciphers aes`	Specifies the WPA1 cipher. Choose one of the following encryption types: • **aes**—Specifies WPA/AES support. • **tkip**—Specifies WPA/TKIP support. The default values are TKIP for WPA1 and AES for WPA2. **Note** You can enable or disable TKIP encryption only using the CLI. Configuring TKIP encryption is not supported in GUI. When you have VLAN configuration on WGB, you need to configure the encryption cipher mode and keys for a particular VLAN, for example, **encryption vlan 80 mode ciphers tkip**. Then, you need to configure the encryption cipher mode globally on the multicast interface by entering the following command: **encryption mode ciphers tkip**.
Step 6	**security wpa akm** {**cckm**| **dot1x** | **dot1x-sha256** | **ft** | **psk** |**psk-sha256**} **Example:** `Device(config-wlan)# security wpa akm 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.

	Command or Action	Purpose
		Note • You cannot enable 802.1x and PSK with SHA256 key derivation type simultaneously. • When you configure Cisco Centralized Key Management SSID, you must enable the **ccx aironet-iesupport** for Cisco Centralized Key Management to work. • WPA3 Enterprise dot1x-sha256 is supported only in local mode.
Step 7	**security wpa psk set-key** {**ascii** | **hex**} {**0** | **8**} *password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 test`	Enter this command to specify a preshared key, if you have enabled PSK. WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
Step 8	**security wpa akm ft** {**dot1x** | **psk**| **sae**} **Example:** `Device(config-wlan)# security wpa akm ft psk`	Enable or disable authentication key management suite for fast transition. **Note** You can now choose between PSK and fast transition PSK as the AKM suite.
Step 9	**security wpa wpa2** **Example:** `Device(config-wlan)# security wpa wpa2`	Enables WPA2.
Step 10	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2` **Example:**	Configure WPA2 cipher. • **aes**—Specifies WPA/AES support.
Step 11	**show wireless pmk-cache**	Displays the remaining time before the PMK cache lifetime timer expires. If you have enabled WPA2 with 802.1X authenticated key management or WPA1 or WPA2 with Cisco Centralized Key Management authenticated key management, the PMK cache lifetime timer is used to trigger reauthentication with the client when necessary. The timer is based on the timeout

	Command or Action	Purpose
		value received from the AAA server or the WLAN session timeout setting. If you configure 802.1x with session timeout between 0 and 299, Pairwise Master Key (PMK) cache is created with a timer of 1 day 84600 seconds. **Note** • The command will show VLAN ID with VLAN pooling feature in VLAN-Override field. • Sticky key caching (SKC) is not supported.