



## WLAN Security

---

- [WPA1 and WPA2 security protocols, on page 1](#)
- [AAA override, on page 2](#)
- [Prerequisites for Layer 2 Security, on page 6](#)
- [How to Configure WLAN Security, on page 7](#)

## WPA1 and WPA2 security protocols

WPA1 and WPA2 are standards-based security solutions from the Wi-Fi Alliance that

- provide data protection and access control for wireless LAN systems
- offer different encryption methods, with WPA1 using TKIP and WPA2 using AES-CCMP, and
- support multiple authentication options including 802.1X, PSK, and Cisco Centralized Key Management.

### WPA1 and WPA2 implementation details

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.

## AAA override

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

## Configure AAA override (CLI)

Enable AAA override functionality to allow authentication servers to dynamically override wireless policy configurations on a per-client basis.

AAA override allows RADIUS servers to push policy attributes that supersede the locally configured wireless policy settings. This is useful for implementing dynamic policies based on user authentication results.

### Procedure

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure WLAN policy profile and enter the wireless policy configuration mode.

**Example:**

```
Device(config)# wireless profile policy profile-policy
```

**Example:**

```
Device(config)# wireless profile policy test-wgb
```

**Step 3** Configure AAA policy override.

**Example:**

```
Device(config-wireless-policy) # aaa-override
```

**Note**

If VLAN is not pushed from the RADIUS server, the VLAN Override feature can be disabled from the RADIUS server.

**Step 4** Return to privileged EXEC mode.

**Example:**

```
Device(config-wireless-policy) # end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

---

AAA override is now enabled for the wireless policy profile, allowing RADIUS server attributes to override local policy settings for authenticated clients.

## VLAN override

VLAN override is an authentication feature that

- requires AAA Override to be enabled under the Policy Profile
- enables VLAN assignment from the RADIUS server using IETF RADIUS attributes or Aire-Interface-Name attribute, and
- supports VLAN ID, VLAN name, or VLAN group name assignment.

### VLAN assignment methods

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

- Using IETF 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.



**Note** If additional 802.1x authentication is executed after VLAN override in MAB authentication, the RADIUS server must be configured to return the same value in VLAN attribute even with 802.1x authentication. VLAN overridden by MAB authentication and the VLAN assigned by 802.1x authentication should have the same value.

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.

## Configure override VLAN for central switching (CLI)

Enable dynamic VLAN assignment from a RADIUS server for centrally switched wireless clients.

Override VLAN configuration allows the RADIUS server to dynamically assign VLANs to wireless clients during authentication, providing flexible network segmentation based on user credentials or policies.

### Procedure

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Define VLANs that can be pushed from the RADIUS server.

**Example:**

```
Device(config)# vlan vlan-id
```

**Example:**

```
Device(config)# vlan 20
```

The valid VLAN ID range is 1 to 4094.

**Step 3** (Optional) Change the default name of the VLAN.

**Example:**

```
Device(config-vlan)# name vlan-name
```

**Example:**

```
Device(config-vlan)# name vlan_ascii
```

**Step 4** Return to privileged EXEC mode.

**Example:**

```
Device(config-vlan)# end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

---

The override VLAN is configured and ready to accept dynamic VLAN assignments from the RADIUS server for centrally switched clients.

## Configure override VLAN for local switching (CLI)

Configure VLAN name to ID mapping under flex profile for local switching scenarios.

### Procedure

---

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure a Flex profile.

**Example:**

```
Device(config)# wireless profile flex flex-profile-name
```

**Example:**

```
Device(config)# wireless profile flex rr-xyz-flex-profile
```

**Step 3** Define VLANs that can be pushed from the RADIUS server.

**Example:**

```
Device(config-wireless-flex-profile)# vlan-name vlan-name
```

**Example:**

```
Device(config-wireless-flex-profile)# vlan-name vlan_123
```

**Step 4** Configure VLAN ID.

**Example:**

```
Device(config-wireless-flex-profile-vlan)# vlan-id vlan-id
```

**Example:**

```
Device(config-wireless-flex-profile-vlan)# vlan-id 23
```

The valid VLAN ID range is 1 to 4096.

**Step 5** Return to privileged EXEC mode.

**Example:**

```
Device(config-wireless-flex-profile-vlan)# end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

---

The override VLAN is now configured for local switching with the specified flex profile, enabling VLAN name to ID mapping for wireless clients.

## VLAN override on Layer 3 web authentication

VLAN override on Layer 3 web authentication is a network authentication feature that

- enables the RADIUS server to push a new VLAN assignment during Layer 3 authentication
- triggers client re-association and DHCP renewal when VLAN changes occur, and
- maintains client state during the transition process.

### Authentication process and client transition

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:

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

## VLAN override verification on Layer 3 web authentication

Verify VLAN override on layer 3 web authentication using specific show commands to display override status and statistics.

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

```
Device# show wireless client mac <mac> detail
[...]
```

```
Vlan Override after L3 Auth: True
```

To display the statistics about client, use this 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)

## How to Configure WLAN Security

### Configure static WEP Layer 2 security parameters (GUI)

Configure static WEP layer 2 security parameters to secure wireless network communication using WEP encryption keys.

Use this procedure when you need to configure WEP layer 2 security for a WLAN. Static WEP provides basic encryption for wireless communications using either 40-bit or 104-bit encryption keys.

#### 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**.

---

The WLAN is configured with static WEP layer 2 security parameters. The settings are applied to the device and WEP encryption is enabled for the wireless network.

## Configure static WEP layer 2 security parameters (CLI)

Set up static WEP encryption and authentication for WLAN security.

Static WEP provides basic wireless security through shared encryption keys. This configuration is used when legacy devices require WEP compatibility, though WPA/WPA2 is recommended for better security.

### Before you begin

You must have administrator privileges.

### Procedure

---

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Enter WLAN configuration submenu.

**Example:**

```
Device# wlan profile-name wlan-id SSID-Name
```

**Example:**

```
Device# wlan test4 1 test4
```

*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** Disable fast transition.

**Example:**

```
Device(config-wlan)# disable ft
```

**Step 4** Disable fast transition over the data source on the WLAN.

**Example:**

```
Device(config-wlan)# no security ft over-the-ds
```

**Step 5** Disable 802.11r Fast Transition on the WLAN.

**Example:**

```
Device(config-wlan)# no security ft
```

**Step 6** Disable the WPA/WPA2 support for a WLAN.

**Example:**

```
Device(config-wlan)# no security wpa wpa1 ciphers tkip
```

**Step 7** Configure Static WEP Key authentication with authentication type.

**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 8** Configure Static WEP Key encryption parameters.

**Example:**

```
Device(config-wlan)# security static-wep-key encryption 104 ascii 0 encryption-key key-index
```

**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.
- **hex**: Specifies the key format as HEX.

**Step 9** Exit configuration mode and return to privileged EXEC mode.

**Example:**

```
Device(config-wlan)# end
```

---

Static WEP layer 2 security is now configured on the WLAN with the specified authentication and encryption parameters.

## Configure WPA + WPA2 Layer 2 security parameters (GUI)

This task configures WPA + WPA2 layer 2 security parameters to secure wireless network communications using the graphical user interface.

Use this procedure when you need to set up wireless network security using both WPA and WPA2 protocols through the GUI interface. This configuration provides enhanced security for your wireless network by supporting both protocols simultaneously.

### 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**.
- 

The WPA + WPA2 layer 2 security parameters are configured and applied to the device. The WLAN profile now uses both WPA and WPA2 security protocols to protect wireless network communications.

## Configure WPA + WPA2 layer 2 security parameters (CLI)

This task configures WPA and WPA2 layer 2 security settings to secure wireless networks using command-line interface commands.



- 
- 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.

Follow these steps to configure WPA + WPA2 layer 2 security parameters using commands:

### Procedure

- 
- Step 1** Enter global configuration mode.  
**Example:**  
Device# `configure terminal`
  - Step 2** Enter the WLAN configuration submode.**wlan**  
**Example:**  
Device(config)# `wlan profile-name wlan-id SSID_name`  
**Example:**  
Device(config)# `wlan test4 1 test4`

- *profile-name* is the profile name of the configured WLAN.
- *wlan-id* is the wireless LAN identifier. The range is from 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** Enables WPA or WPA2 support for WLAN.

**Example:**

```
Device(config-wlan)# security wpa {akm | wpa1 | wpa2}
Device(config-wlan)# security wpa
```

**Step 4** Enables WPA.

**Example:**

```
Device(config-wlan)# security wpa wpa1
```

**Step 5** Specify the WPA1 cipher.

**Example:**

```
Device(config-wlan)# security wpa wpa1 ciphers [aes | tkip]
Device(config-wlan)# security wpa wpa1 ciphers aes
```

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** 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. **security WPA AKM {CCKM| dot1x | dot1x-sha256 | ft | PSK |PSK-sha256}**

**Example:**

```
Device(config-wlan)# security wpa akm {cckm | dot1x | dot1x-sha256 | ft | psk | psk-sha256}
Device(config-wlan)# security wpa akm psk-sha256
```

**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** Enter this command to specify a preshared key, if you have enabled PSK.

**Example:**

```
Device(config-wlan)# security wpa psk set-key {ascii | hex} {0 | 8} password
Device(config-wlan)# security wpa psk set-key ascii 0 test
```

WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

**Step 8** Enable or disable authentication key management suite for fast transition.

**Example:**

```
Device(config-wlan)# security wpa akm ft {dot1x | psk | sae}
Device(config-wlan)# security wpa akm ft psk
```

**Note**

You can now choose between PSK and fast transition PSK as the AKM suite.

**Step 9** Enable WPA2.

**Example:**

```
Device(config-wlan)# security wpa wpa2
```

**Step 10** Configure WPA2 cipher. **security wpa wpa2 ciphers aes**

**Example:**

```
Device(config-wlan)# security wpa wpa2
```

**Example:**

- **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 value received from the AAA server or the WLAN session timeout setting.

**Note**

- The command will show VLAN ID with VLAN pooling feature in VLAN-Override field.
- Sticky key caching (SKC) is not supported.

---

WPA and WPA2 layer 2 security parameters are configured for the WLAN. The wireless network is secured with the specified authentication and encryption settings.