



Configuring WLAN Security

- [Configuring WLAN Security \(CLI\), on page 1](#)
- [Configuring WLAN Security \(GUI\), on page 3](#)

Configuring WLAN Security (CLI)

Configuring Static WEP Layer 2 Security Parameters (CLI)

Before you begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan profile-name**
3. **security static-wep-key [authentication {open | shared} | encryption {104 | 40} {ascii | hex} [0 | 8]]**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wlan profile-name Example: # wlan test4	Enters WLAN configuration submenu. The <i>profile-name</i> is the profile name of the configured WLAN.
Step 3	security static-wep-key [authentication {open shared} encryption {104 40} {ascii hex} [0 8]]	The keywords are as follows:

	Command or Action	Purpose
	Example: <pre>(config-wlan) # security static-wep-key authentication open</pre>	• static-wep-key—Configures Static WEP Key authentication. • authentication—Specifies the authentication type you can set. The values are open and shared. • 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 4	end Example: <pre>Device(config) # end</pre>	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)



Note

The default security policy is WPA2.

Before you begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan profile-name**
3. **security wpa**
4. **security wpa wpa1**
5. **security wpa wpa1 ciphers [aes | tkip]**
6. **security wpa wpa2**
7. **security wpa wpa2 ciphers [aes | tkip]**
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Device# configure terminal	
Step 2	wlan <i>profile-name</i> Example: # wlan test4	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
Step 3	security wpa Example: (config-wlan)# security wpa	Enables WPA.
Step 4	security wpa wpa1 Example: (config-wlan)# security wpa wpa1	Enables WPA1.
Step 5	security wpa wpa1 ciphers [aes tkip] Example: (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.
Step 6	security wpa wpa2 Example: (config-wlan)# security wpa	Enables WPA2.
Step 7	security wpa wpa2 ciphers [aes tkip] Example: (config-wlan)# security wpa wpa2 ciphers tkip	Configure WPA2 cipher. Choose one of the following encryption types: • aes—Specifies WPA/AES support. • tkip—Specifies WPA/TKIP support.
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 WLAN Security (GUI)

Configuring Static WEP Layer 2 Security Parameters (GUI)

- 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 WPA + WPA2 Layer 2 Security Parameters (GUI)

- 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**.
-