Configuring WLAN Security

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

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 information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:

- None (open WLAN)
- Static WEP or 802.1X

Note Because static WEP and 802.1X are both advertised by the same bit in beacon and probe responses, they cannot be differentiated by clients. Therefore, they cannot both be used by multiple WLANs with the same SSID.

- 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 that is configured with TKIP support will not be enabled on an RM3000AC module.

Related Topics

Configuring Static WEP + 802.1X Layer 2 Security Parameters (CLI), on page 2
Configuring Layer 2 Parameters (GUI), on page 7
Configuring Static WEP Layer 2 Security Parameters (CLI), on page 3
Configuring WPA + WPA2 Layer 2 Security Parameters (CLI), on page 4
Configuring 802.1X Layer 2 Security Parameters (CLI), on page 6
Configuring Advanced WLAN Properties (CLI)
Information About AAA Override, on page 2

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.

Related Topics

Configuring Advanced WLAN Properties (CLI)
Prerequisites for Layer 2 Security, on page 1

How to Configure WLAN Security

Configuring Static WEP + 802.1X 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** | **sharedkey**} | **encryption** {**104** | **40**} [**ascii** | **hex**] {**0** | **8**} } *wep-key wep-key-index1-4*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security static-wep-key** {**authentication** {**open** | **sharedkey**} | **encryption** {**104** | **40**} [**ascii** | **hex**] {**0** | **8**} } *wep-key wep-key-index1-4* **Example:** `Switch(config-wlan)# security static-wep-key encryption 40 hex 0 test 2`	Configures static WEP security on a WLAN. The keywords and arguments are as follows: • **authentication**—Configures 802.11 authentication. • **encryption**—Sets the static WEP keys and indices. • **open**—Configures open system authentication. • **sharedkey**—Configures shared key authentication. • **104, 40**—Specifies the WEP key size. • **hex, ascii**—Specifies the input format of the key. • *wep-key-index* , *wep-key-index1-4*—Type of password that follows. A value of 0 indicates that an unencrypted password follows. A value of 8 indicates that an AES encrypted follows.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 1

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:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security static-wep-key** [**authentication** {**open** | **shared**} | **encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]] **Example:** `Switch(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. • **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:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 1

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:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security wpa** **Example:** `Switch(config-wlan)# security wpa`	Enables WPA.
Step 4	**security wpa wpa1** **Example:** `Switch(config-wlan)# security wpa wpa1`	Enables WPA1.
Step 5	**security wpa wpa1 ciphers** [**aes**	**tkip**] **Example:** `Switch(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:** `Switch(config-wlan)# security wpa`	Enables WPA 2.
Step 7	**security wpa wpa2 ciphers** [**aes**	**tkip**] **Example:** `Switch(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.

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

Related Topics

Prerequisites for Layer 2 Security, on page 1

Configuring 802.1X Layer 2 Security Parameters (CLI)

Before you begin

You must have administrator privileges.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security dot1x**
4. **security** [**authentication-list** *auth-list-name* | **encryption** {**0** | **104** | **40**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Switch# wlan test4`	Enters the WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**security dot1x** **Example:** `Switch(config-wlan)# security dot1x`	Specifies 802.1X security.
Step 4	**security** [**authentication-list** *auth-list-name*	**encryption** {**0**	**104**	**40**} **Example:** `Switch(config-wlan)# security encryption 104`	The keywords and arguments are as follows: • **authentication-list**—Specifies the authentication list for IEEE 802.1X. • **encryption**—Specifies the length of the CKIP encryption key. The valid values are 0, 40, and 104. Zero (0) signifies no encryption. This is the default.

	Command or Action	Purpose
		Note All keys within a WLAN must be of the same size.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for Layer 2 Security, on page 1

Configuring Layer 2 Parameters (GUI)

Before you begin

- You must have administrator privileges.

Step 1 Click **Configuration** > **WLAN** > .

The **WLANs** page appears.

Step 2 Click the WLANs profile of the WLAN you want to configure.

The **WLANs** > **Edit** > page appears.

Step 3 Click the **Security** > **Layer 2** > tab.

Parameter	Description
Layer2 Security	Layer 2 security for the selected WLAN. Values are the following: • None—No Layer 2 security selected. • WPA+WPA2—Wi-Fi Protected Access. • 802.1X—WEP 802.1X data encryption type. For information on these settings, see the Layer 2 802.1X Parameters topic. • Static WEP—Static WEP encryption parameters. • Static WEP + 802.1x—Both Static WEP and 802.1X parameters.
MAC Filtering	MAC address filtering. You can locally configure clients by their MAC addresses in the **MAC Filters** > **New page** . You can add a maximum of 12000 local net users. Otherwise, configure the clients on a RADIUS server. **Note** MAC Filtering is also known as MAC Authentication By Pass (MAB).
Fast Transition	Check box to enable or disable a fast transition between access points.
Over the DS	Check box to enable or disable a fast transition over a distributed system.
Reassociation Timeout	Time in seconds after which a fast transition reassociation times out.

To configure the **WPA + WPA2** parameters, provide the following details:

Parameter	Description
WPA Policy	Check box to enable or disable WPA policy.
WPA Encryption	WPA2 encryption type: TKIP or AES. Available only if the WPA policy is enabled.
WPA2 Policy.	Check box to enable or disable WPA2 policy.
WPA2 Encryption	WPA2 encryption type: TKIP or AES. Available only if the WPA2 policy is enabled.
Authentication Key Management	The rekeying mechanism parameter.. Values are the following: • 802.1X • CCKM • PSK • 802.1x + CCKM
PSK Format	Enabled when you select the PSK value for Authentication Key Management. Choose ASCII or the HEX format and enter the preshared key.

To configure **802.1x** parameters, provide the following details:

Parameter	Description
802.11 data encryption	WEP 802.11 data encryption type.
Type	Security type.
Key size	Key size. Values are the following: • None • 40 bits • 104 bits The third-party AP WLAN (17) can only be configured with 802.1X encryption. Drop-down configurable 802.1X parameters are not available for this WLAN.

To specify **Static WEP**, configure the following parameters:

Parameter	Description
802.11 Data Encryption	Static WEP encryption type.
Current Key	Displays the current selected key details.
Type	Security type.

Parameter	Description
Key size	Key size. Values are the following: • Not set • 40 bits • 104 bits
Key Index	Key index from 1 to 4. One unique WEP key index can be applied to each WLAN. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption.
Encryption Key	Encryption key.
Key Format	Encryption key format in ASCII or HEX.
Allow Shared Key Authentication	Key authentication that you can enable or disable.

To configure Static WEP + 802.1X Parameters

Parameter	Description
Static WEP Parameters	
802.11 Data Encryption	Static WEP encryption type.
Current Key	Displays the current selected key details.
Type	Security type.
Key size	Key size. Values are the following: • Not set • 40 bits • 104 bits
Key Index	Key index from 1 to 4. The key index is unique per WLAN. You can only have one "key 1" on a given WLAN. You can define up to 4 keys per WLAN, and the switch will announce the key index, to allow clients configured the same way to know what key to use. This is per WLAN. You can configure all your WLANs (up to 512) as WEP if you want, each with up to 4 keys.
Encryption Key	Encryption key.
Key Format	Encryption key format in ASCII or HEX.
Allow Shared Key Authentication	Key authentication that you can enable or disable.

Parameter	Description
802.1x Parameters	
802.11 Data Encryption	Static WEP encryption type.
Type	Security type.
Key size	Key size. Values are the following: • Not set • 40 bits • 104 bits

Step 4 Click **Apply**.

Related Topics

Prerequisites for Layer 2 Security, on page 1

Additional References

Related Documents

Related Topic	Document Title
WLAN command reference	*WLAN Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)WLAN Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
Security configuration guide	*Security Configuration Guide (Cisco WLC 5700 Series)Security Configuration Guide (Catalyst 3650 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information about WLAN Layer 2 Security

This table lists the features in this module and provides links to specific configuration information.

Feature Name	Release	Feature Information
WLAN Security functionality	Cisco IOS XE 3.3SECisco IOS XE 3.2SECisco IOS XE 3.2SE	This feature was introduced.