

# Wireless LAN Controller Layer 2 – Layer 3 Security Compatibility Matrix

[TAC Notice: What's Changing on TAC Web](#)

## Contents

- [Introduction](#)
- [Prerequisites](#)
  - [Requirements](#)
  - [Components Used](#)
  - [Conventions](#)
- [Cisco Unified Wireless Network Security Solutions](#)
- [Wireless LAN Controller Layer 2 – Layer 3 Security Compatibility Matrix](#)
- [NetPro Discussion Forums - Featured Conversations](#)
- [Related Information](#)

## Introduction

This document provides the compatibility matrix for the Layer 2 and Layer 3 security mechanisms supported on the Wireless LAN Controller.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of the configuration of lightweight APs and Cisco WLCs
- Basic knowledge of Lightweight AP Protocol (LWAPP)
- Basic Knowledge of Wireless Security Solutions

### Components Used

The information in this document is based on a Cisco 4400/2100 Series WLC that runs firmware version 5.0.

### Help us help you.

Please rate this document.

Excellent  
 Good  
 Average  
 Fair  
 Poor

This document solved my problem.

Yes  
 No  
 Just browsing

Suggestions for improvement:

(256 character limit)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

## Cisco Unified Wireless Network Security Solutions

The Cisco Unified Wireless Network supports Layer 2 and Layer 3 security methods.

- Layer 2 security
- Layer 3 security (for WLAN) or Layer 3 security (for Guest LAN)

Layer 2 security is not supported on Guest LANs.

This table lists the various Layer 2 and Layer 3 security methods supported on the Wireless LAN Controller. These security methods can be enabled from the **Security** tab on the **WLANs > Edit** page of the WLAN.

Layer 2 Security Mechanism		
Parameter	Description	
Layer 2 Security	None	No Layer 2 security selected.
	WPA+WPA2	Use this setting in order to enable Wi-Fi Protected Access.
	802.1X	Use this setting in order to enable 802.1x authentication.
	Cranite	Use this setting in order to enable the WLAN to use the FIPS140-2 compliant Cranite Wireless Wall Software Suite, which uses AES encryption and VPN tunnels to encrypt and verify all data frames carried by the Cisco WLAN Solution.  <b>Note:</b> When Cranite is selected as the Layer 2 security policy, no Layer

		3 security policies are allowed.
	Static WEP + 802.1x	Use this setting in order to enable both Static WEP and 802.1x parameters.
	CKIP	Use this setting in order to enable Cisco Key Integrity Protocol (CKIP). Functional on AP Models 1100, 1130, and 1200, but not AP 1000. Aironet IE needs to be enabled for this feature to work. CKIP expands the encryption keys to 16 bytes.
MAC Filtering	Select to filter clients by MAC address. Locally configure clients by MAC address in the MAC Filters > New page. Otherwise, configure the clients on a RADIUS server.	
<b>Layer 3 Security Mechanism (for WLAN)</b>		
	<b>Parameter</b>	<b>Description</b>
Layer 3 Security	None	No Layer 3 security selected.
	IPSec	Use this setting in order to enable IPSec. You need to check software availability and client hardware compatibility before you implement IPSec.  <b>Note:</b> You must have the optional VPN/Enhanced Security Module (crypto processor card) installed to enable IPSec. Verify it is installed on your controller on the Inventory page.
	VPN Pass-Through	Use this setting in order to enable VPN Pass-Through.
	Select this check box to enable Web Policy.	

Web Policy	<p><b>Note:</b> Web Policy cannot be used in combination with IPsec or VPN Pass-Through options.</p> <p>These parameters are displayed:</p> <ul style="list-style-type: none"> <li>• Authentication—If you select this option, the user is prompted for username and password while connecting the client to the wireless network.</li> <li>• Passthrough—If you select this option, the user can access the network directly without the username and password authentication.</li> <li>• Conditional Web Redirect—If you select this option, the user can be conditionally redirected to a particular web page after 802.1X authentication successfully completes. You can specify the redirect page and the conditions under which the redirect occurs on your RADIUS server.</li> <li>• Splash Page Web Redirect—If you select this option, the user is redirected to a particular web page after 802.1X authentication successfully completes. After the redirect, the user has full access to the network. You can specify the splash web page on your RADIUS server.</li> </ul>
Preauthentication ACL	Select the ACL to be used for traffic between the client and the controller.
Over-ride Global Config	<p>Displays if you select Authentication.</p> <p>Check this box in order to override the global authentication configuration set on the Web Login Page.</p>
	<p>Displays if you select Over-ride Global Config.</p> <p>Select a type of Web authentication:</p>

Web Auth type	<ul style="list-style-type: none"> <li>• Internal</li> <li>• Customized (Downloaded) <ul style="list-style-type: none"> <li>○ Login Page—Select a login page from the drop-down list.</li> <li>○ Login Failure page—Select a login page that displays to the client if Web authentication fails.</li> <li>○ Logout page—Select a login page that displays to the client when the user logs out of the system.</li> </ul> </li> <li>• External (Re-direct to external server) <ul style="list-style-type: none"> <li>○ URL—Enter the URL of the external server.</li> </ul> </li> </ul>
---------------	--

Email Input	<p>Displays if you select Passthrough.</p> <p>If you select this option, you are prompted for your email address while connecting to the network.</p>
-------------	---

**Layer 3 Security Mechanism (for Guest LAN)**

Parameter		Description
Layer 3 Security	None	No Layer 3 security selected.
	Web Authentication	If you select this option, you are prompted for username and password while connecting the client to the network.
	Web Passthrough	If you select this option, you can access the network directly without the username and password authentication.

Preauthentication ACL	Select the ACL to be used for traffic between the client and the controller.
-----------------------	--

	Check this box in order to override the global
--	--

Over-ride Global Config	authentication configuration set on the Web Login Page.
Web Auth type	<p>Displays if you select Over-ride Global Config. Select a type of Web authentication:</p> <ul style="list-style-type: none"> <li>• Internal</li> <li>• Customized (Downloaded) <ul style="list-style-type: none"> <li>○ Login Page—Select a login page from the drop-down list.</li> <li>○ Login Failure page—Select a login page that displays to the client if Web authentication fails.</li> <li>○ Logout page—Select a login page that displays to the client when the user logs out of the system.</li> </ul> </li> <li>• External (Re-direct to external server) <ul style="list-style-type: none"> <li>○ URL—Enter the URL of the external server.</li> </ul> </li> </ul>
Email Input	<p>Displays if you select Web Passthrough.</p> <p>If you select this option, you are prompted for your</p>

email address while connecting to the network.
--

**Note:** In controller software release 4.1.185.0 or later, CKIP is supported for use only with static WEP. It is not supported for use with dynamic WEP. Therefore, a wireless client that is configured to use CKIP with dynamic WEP is unable to associate to a wireless LAN that is configured for CKIP. Cisco recommends that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

## Wireless LAN Controller Layer 2 – Layer 3 Security Compatibility Matrix

When you configure security on a Wireless LAN, both Layer 2 and Layer 3 security methods can be used in conjunction. However, not all the Layer 2 security methods can be used with all Layer 3 security methods. This table shows the compatibility matrix for the Layer 2 and Layer 3 security methods supported on the Wireless LAN Controller.

Layer 2 Security Mechanism	Layer 3 Security Mechanism	Compatibility
None	None	Valid
WPA+WPA2	None	Valid
WPA+WPA2	Web Authentication	Invalid
WPA-PSK/WPA2-PSK	Web Authentication	Valid
WPA+WPA2	Web Passthrough	Invalid
WPA-PSK/WPA2-PSK	Web Passthrough	Valid
WPA+WPA2	Conditional Web Redirect	Valid
WPA+WPA2	Splash Page Web Redirect	Valid
WPA+WPA2	VPN-PassThrough	Valid
802.1x	None	Valid
802.1x	Web Authentication	Invalid
802.1x	Web Passthrough	Invalid
802.1x	Conditional Web Redirect	Valid
802.1x	Splash Page Web Redirect	Valid
802.1x	VPN-PassThrough	Valid

Static WEP	None	Valid
Static WEP	Web Authentication	Valid
Static WEP	Web Passthrough	Valid
Static WEP	Conditional Web Redirect	Invalid
Static WEP	Splash Page Web Redirect	Invalid
Static WEP	VPN-PassThrough	Valid
Cranite	None	Valid
Cranite	Web Authentication	Invalid
Cranite	Web Passthrough	Invalid
Cranite	Conditional Web Redirect	Invalid
Cranite	Splash Page Web Redirect	Invalid
Cranite	VPN-PassThrough	Invalid
Static-WEP+ 802.1x	None	Valid
Static-WEP+ 802.1x	Web Authentication	Invalid
Static-WEP+ 802.1x	Web Passthrough	Invalid
Static-WEP+ 802.1x	Conditional Web Redirect	Invalid
Static-WEP+ 802.1x	Splash Page Web Redirect	Invalid
Static-WEP+ 802.1x	VPN-PassThrough	Invalid
CKIP	None	Valid
CKIP	Web Authentication	Valid
CKIP	Web Passthrough	Valid
CKIP	Conditional Web Redirect	Invalid
CKIP	Splash Page Web Redirect	Invalid
CKIP	VPN-PassThrough	Valid

## NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

---

NetPro Discussion Forums - Featured Conversations for Wireless
Wireless - Mobility: WLAN Radio Standards
<a href="#">Increase power output to 17 or 20 dBm not possible on AP 1131 AG</a> - Oct 1, 2008 <a href="#">Where to see signal Strength on wireless BR 350</a> - Sep 25, 2008 <a href="#">3G-WIC and SIM-card</a> - Sep 23, 2008 <a href="#">Which IOS command allows me to check APs current working mode?</a> - Sep 22, 2008 <a href="#">1200 Series Access points</a> - Sep 18, 2008
Wireless - Mobility: Security and Network Management
<a href="#">Securing Wireless Access using ACS</a> - Oct 3, 2008 <a href="#">No encryption No security</a> - Oct 2, 2008 <a href="#">Authenticate users by Windows group using ACS</a> - Oct 2, 2008 <a href="#">Authentication Failure WLC ACS 3.3</a> - Oct 1, 2008 <a href="#">WLSE</a> - Oct 1, 2008
Wireless - Mobility: Wireless IP Voice and Video
<a href="#">Vlan Config 1242ag/ vlan config HP 2848 Procurve switch</a> - Sep 30, 2008 <a href="#">7921g and wlc 4404 oneway voice problem</a> - Sep 29, 2008 <a href="#">7920 Call manager registration</a> - Sep 29, 2008 <a href="#">voice muted between wireless phone and IP phone</a> - Sep 29, 2008 <a href="#">7921s are "locating network services"</a> - Sep 29, 2008
Wireless - Mobility: Getting Started with Wireless
<a href="#">MAC addressing across the DS</a> - Oct 2, 2008 <a href="#">WCS cannot add WLC over slow link</a> - Oct 2, 2008 <a href="#">4402 CSR generation?</a> - Oct 2, 2008 <a href="#">Extending wireless to AP in order to extend network</a> - Oct 1, 2008 <a href="#">Multiple Aironet 1310 APs / One Wireless Network / How To???</a> - Oct 1, 2008
Wireless - Mobility: General
<a href="#">Wireless Mesh</a> - Oct 3, 2008 <a href="#">WLC4400 controller and AP power level</a> - Oct 2, 2008 <a href="#">Point to point wireless using 1310 and 1231 on each site</a> - Oct 2, 2008 <a href="#">Wireless Lan Controller</a> - Oct 2, 2008 <a href="#">Radio going down on 1310AP</a> - Oct 2, 2008

## Related Information

- [Wireless LAN Controller and Lightweight Access Point Basic Configuration Example](#)
- [Lightweight AP \(LAP\) Registration to a Wireless LAN Controller \(WLC\)](#)
- [Configuring Security Solutions](#)
- [Wireless LAN Controller \(WLC\) FAQ](#)
- [Technical Support & Documentation - Cisco Systems](#)

