

# Configuración de WPA/WPA2 con clave precompartida: IOS 15.2JB y posteriores

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración con GUI](#)

[Configuración con CLI](#)

[Verificación](#)

[Troubleshoot](#)

## Introducción

Este documento describe una configuración de ejemplo de acceso inalámbrico protegido (WPA) y WPA2 con una clave previamente compartida (PSK).

## Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Familiaridad con la GUI o la interfaz de línea de comandos (CLI) para el software Cisco IOS®
- Familiaridad con los conceptos de PSK, WPA y WPA2

## Componentes Utilizados

La información de este documento se basa en el punto de acceso Cisco Aironet 1260 (AP) que ejecuta la versión 15.2JB del software Cisco IOS.

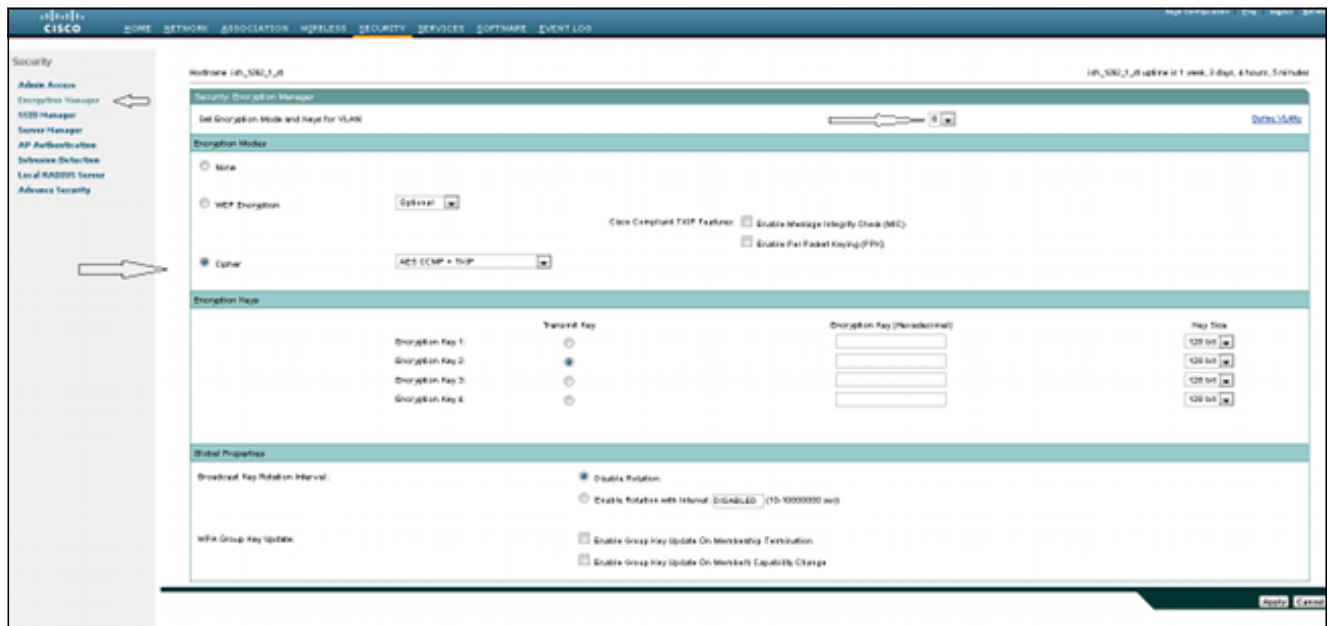
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Configurar

## Configuración con GUI

Este procedimiento describe cómo configurar WPA y WPA2 con un PSK en la GUI del software Cisco IOS:

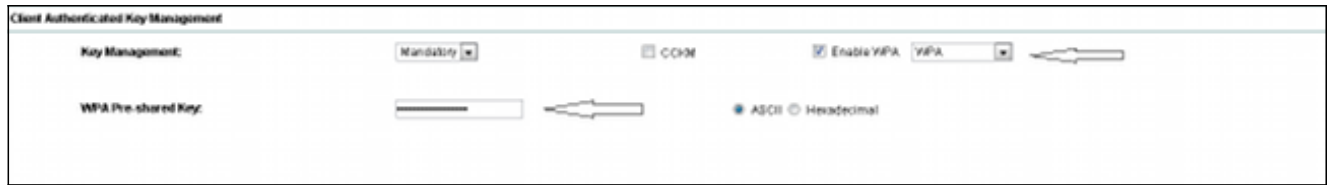
1. Configure el Administrador de cifrado para la VLAN definida para el identificador del conjunto de servicios (SSID). Navegue hasta **Seguridad > Administrador de cifrado**, asegúrese de que Cipher esté habilitado y seleccione **AES CCMP + TKIP** como el cifrado que se utilizará para ambos SSID.



2. Habilite la VLAN correcta con los parámetros de cifrado definidos en el Paso 1. Navegue hasta **Seguridad > Administrador SSID** y seleccione el SSID de la Lista SSID actual. Este paso es común para la configuración WPA y WPA2.



3. En la página SSID, establezca Key Management en **Obligatorio** y marque la casilla **Enable WPA**. Seleccione **WPA** en la lista desplegable para habilitar WPA. Introduzca la clave precompartida WPA.



4. Seleccione **WPA2** en la lista desplegable para habilitar WPA2.



## Configuración con CLI

### Notas:

Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver un análisis de información de salida del comando show.

Esta es la misma configuración que se realiza dentro de la CLI:

```
sh run
Building configuration...Current configuration : 5284 bytes
!
! Last configuration change at 04:40:45 UTC Thu Mar 11 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ish_1262_1_st
!
!
logging rate-limit console 9
enable secret 5 $1$Iykv$1tUkNYeB6omK4lS18lTbQ1
!
no aaa new-model
ip cef
ip domain name cisco.com
!
!
!
dot11 syslog
!
dot11 ssid wpa
vlan 6
authentication open
authentication key-management wpa
mbssid guest-mode
```

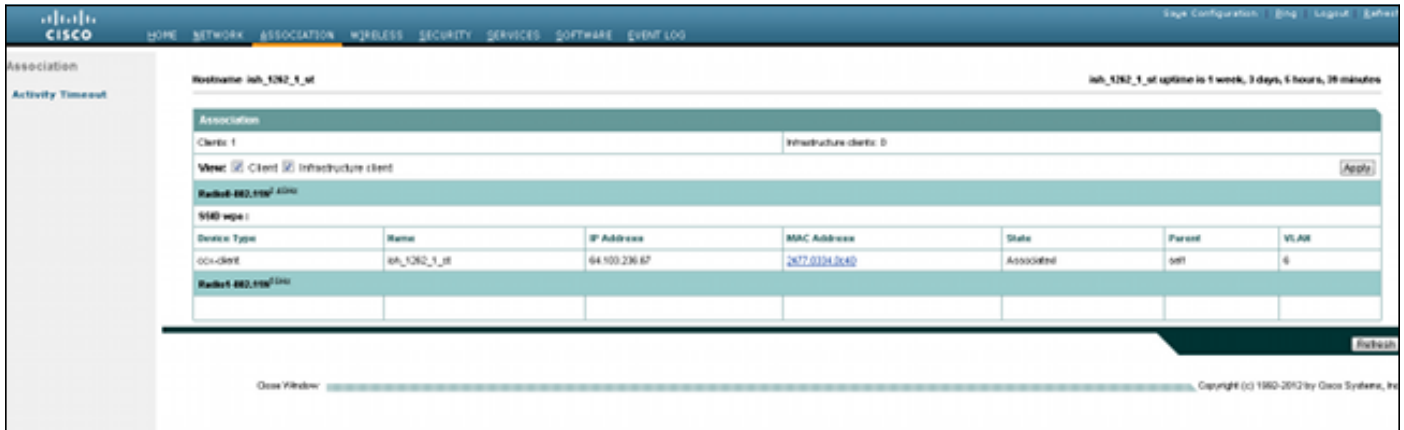
```
wpa-psk ascii 7 060506324F41584B56
!
dot11 ssid wpa2
vlan 7
authentication open
authentication key-management wpa version 2
wpa-psk ascii 7 110A1016141D5A5E57
!
bridge irb
!
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption vlan 6 mode ciphers aes-ccm tkip
!
encryption vlan 7 mode ciphers aes-ccm tkip
!
ssid wpa
!
ssid wpa2
!
antenna gain 0
mbssid
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.6
encapsulation dot1Q 6
no ip route-cache
bridge-group 6
bridge-group 6 subscriber-loop-control
bridge-group 6 spanning-disabled
bridge-group 6 block-unknown-source
no bridge-group 6 source-learning
no bridge-group 6 unicast-flooding
!
interface Dot11Radio0.7
encapsulation dot1Q 7
no ip route-cache
bridge-group 7
bridge-group 7 subscriber-loop-control
bridge-group 7 spanning-disabled
bridge-group 7 block-unknown-source
no bridge-group 7 source-learning
no bridge-group 7 unicast-flooding
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption vlan 6 mode ciphers aes-ccm tkip
!
encryption vlan 7 mode ciphers aes-ccm tkip
!
ssid wpa
!
```

```
ssid wpa2
!
antenna gain 0
no dfs band block
mbssid
channel dfs
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.6
encapsulation dot1Q 6
no ip route-cache
bridge-group 6
bridge-group 6 subscriber-loop-control
bridge-group 6 spanning-disabled
bridge-group 6 block-unknown-source
no bridge-group 6 source-learning
no bridge-group 6 unicast-flooding
!
interface Dot11Radio1.7
encapsulation dot1Q 7
no ip route-cache
bridge-group 7
bridge-group 7 subscriber-loop-control
bridge-group 7 spanning-disabled
bridge-group 7 block-unknown-source
no bridge-group 7 source-learning
no bridge-group 7 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface GigabitEthernet0.6
encapsulation dot1Q 6
no ip route-cache
bridge-group 6
bridge-group 6 spanning-disabled
no bridge-group 6 source-learning
!
interface GigabitEthernet0.7
encapsulation dot1Q 7
no ip route-cache
bridge-group 7
bridge-group 7 spanning-disabled
no bridge-group 7 source-learning
!
interface BVI1
ip address 10.105.132.172 255.255.255.128
no ip route-cache
!
ip forward-protocol nd
ip http server
```

ip http secure-server

## Verificación

Para confirmar que la configuración funciona correctamente, navegue hasta **Asociación** y verifique que el cliente esté conectado:



También puede verificar la asociación del cliente en la CLI con este mensaje de syslog:

```
*Mar 11 05:39:11.962: %DOT11-6-ASSOC: Interface Dot11Radio0, Station  
ish_1262_1_st 2477.0334.0c40 Associated KEY_MGMT[WPAv2 PSK]
```

## Troubleshoot

**Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Utilice estos comandos debug para resolver problemas de conectividad:

- **debug dot11 aaa manager keys** - Esta depuración muestra el intercambio de señales que se produce entre el AP y el cliente como negociación de clave transitoria de par (PTK) y clave transitoria de grupo (GTK).
- **debug dot11 aaa authenticator state-machine** - Esta depuración muestra los diversos estados de negociaciones que pasa un cliente mientras el cliente asocia y autentica. Los nombres de estado indican estos estados.
- **debug dot11 aaa authenticator process** - Esta depuración le ayuda a diagnosticar problemas con las comunicaciones negociadas. La información detallada muestra lo que cada participante en la negociación envía y muestra la respuesta del otro participante. También puede utilizar esta depuración junto con el comando **debug radius authentication**.
- **debug dot11 station connection failure** - Esta depuración ayuda a determinar si los clientes fallan la conexión y ayuda a determinar la razón de las fallas.