

# Introducción a la configuración WPA

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Teoría Precedente](#)

[Convenciones](#)

[Configurar](#)

[Red EAP \(Protocolo de autenticación extensible\) o autenticación abierta con EAP.](#)

[Configuración de CLI](#)

[Configuración de la interfaz gráfica para el usuario](#)

[Verificación](#)

[Troubleshooting](#)

[Procedimiento de resolución de problemas](#)

[Comandos para Troubleshooting](#)

[Información Relacionada](#)

## Introducción

Este documento proporciona una configuración de ejemplo de WPA (Wi-Fi Protected Access), el estándar de seguridad interina que utilizan los miembros de Wi-Fi Alliance.

## prerrequisitos

### Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento completo de las redes inalámbricas y de los problemas de seguridad inalámbrica
- Conocimiento de los métodos de seguridad del Protocolo de Autenticación Extensible (EAP)

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- (APS) basado en software de los Puntos de acceso de Cisco IOS®
- Cisco IOS Software Release 12.2(15)JA o Posterior **Nota:** Preferiblemente, utilice la última

versión de Cisco IOS Software, aunque el WPA se soporta en el Cisco IOS Software Release 12.2(11)JA y Posterior. Para obtener la última versión de Cisco IOS Software, refiera a las [descargas \(clientes registrados solamente\)](#).

- Un Network Interface Cards WPA-obediente (NIC) y su software de cliente WPA-obediente

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## [Teoría Precedente](#)

Las funciones de seguridad en una red inalámbrica, como WEP, son vulnerables. El grupo industrial del Wi-Fi Alliance (o WECA) ideó una última generación, estándar de seguridad interino para las redes inalámbricas. El estándar proporciona la defensa contra las debilidades hasta que la organización IEEE ratifique el estándar 802.11i.

Este nuevo esquema se basa en la autenticación actual EAP/802.1x y la administración de claves dinámicas y agrega un encriptación de cifras más fuerte. Después del dispositivo del cliente y del servidor de autenticación haga una asociación del EAP/802.1x, negocian a la administración de claves WPA entre el AP y el dispositivo del cliente WPA-obediente.

Los Productos de Cisco AP también prevén una Configuración de Híbrido en la cual ambos clientes EAP basados en WEP de la herencia (con la herencia o ninguna administración de claves) trabajen conjuntamente con los clientes WPA. Esta configuración se refiere como modo de migración. El modo de migración tiene en cuenta un acercamiento organizado emigrar al WPA. Este documento no cubre al modo de migración. Este documento proporciona un delinear para una red WPA-asegurada pura.

Además de los problemas de seguridad de la empresa o del nivel corporativo, el WPA también proporciona una versión de la clave previamente compartida (WPA-PSK) que se piense para el uso en el oficina pequeña, oficina en el hogar (SOHO) o las redes inalámbricas caseras. La utilidad de cliente del Cisco Aironet (ACU) no soporta el WPA-PSK. La utilidad de configuración de la Tecnología inalámbrica cero de Microsoft Windows soporta el WPA-PSK para la mayoría de las placas de red inalámbrica, al igual que estas utilidades:

- AEGIS Client de las comunicaciones de Meetinghouse **Nota:** Refiera al [EOS y al anuncio EOL para la línea de producto de la TUTELA de Meetinghouse](#).
- Cliente Odyssey del software Funk **Nota:** Refiera al [Customer Support Center de las redes Juniper](#).
- Utilidades de cliente del Original Equipment Manufacturer (OEM) de algunos fabricantes

Usted puede configurar el WPA-PSK cuando:

- Usted define al modo de encriptación como Temporal Key Integrity Protocol (TKIP) de la cifra en la ficha Manager del cifrado.
- Usted define el tipo de autenticación, el uso de la administración de claves autenticada, y la clave previamente compartida en la ficha Manager del Service Set Identifier (SSID) del GUI.
- No se necesita configuración en la ficha Server Manager (Administrador de servidor).

Para habilitar el WPA-PSK a través del comando line interface(cli), ingrese estos comandos. Salga del modo de configuración:

```
AP(config)#interface dot11Radio 0 AP(config-if)#encryption mode ciphers tkip AP(config-if)#ssid
```

```
ssid_name AP(config-if-ssid)#authentication open AP(config-if-ssid)#authentication key-  
management wpa AP(config-if-ssid)#wpa-psk ascii pre-shared_key
```

**Nota:** Esta sección proporciona solamente la configuración que es relevante al WPA-PSK. La configuración en esta sección es solamente darle una comprensión en cómo habilitar el WPA-PSK y no es el foco de este documento. Este documento explica cómo configurar el WPA.

## Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

## Configurar

WPA se basa en los métodos de EAP/802.1x. Este documento asume que usted tiene una luz EAP (SALTO), EAP, o la configuración protegida EAP (PEAP) que trabaja antes de que usted agregue la configuración para dedicar el WPA.

Esta sección presenta los datos para configurar las características descritas en este documento.

**Nota:** Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

## Red EAP (Protocolo de autenticación extensible) o autenticación abierta con EAP.

En cualquier método de autenticación EAP/802.1x-based, usted puede preguntar cuáles están las diferencias entre el Network EAP y la autenticación abierta con el EAP. Estos ítems se refieren a valores en el campo de autenticación de algoritmos en los encabezados de paquetes de administración y asociación. La mayoría de los fabricantes de conjunto de los clientes de red inalámbrica este campo en el valor 0 (autenticación abierta), y entonces señalan su deseo de hacer la autenticación EAP más adelante en el proceso de asociación. Cisco establece un valor distinto, desde el comienzo de la asociación con el indicador de red EAP.

Utilice el método de autenticación que esta lista indica si su red tiene los clientes que son:

- Clientes de Cisco — Utilice el Network EAP.
- Clientes de tercera persona (que incluyen los Ciscos Compatibles Extension que el [CCX] - los Productos obedientes) — utiliza la autenticación abierta con el EAP.
- Una combinación de ambo Cisco y clientes de tercera persona — elija el Network EAP y la autenticación abierta con el EAP.

## Configuración de CLI

En este documento, se utilizan estas configuraciones:

- Una configuración LEAP que existe y trabaja
- Cisco IOS Software Release 12.2(15)JA para el Cisco IOS AP basados en software

<b>AP</b>
<pre>ap1#show running-config Building configuration... . . . aaa new-model ! aaa group server radius rad_eap server 192.168.2.100 auth-port 1645 acct-port 1646 . . aaa</pre>

```

authentication login eap_methods group rad_eap . . . !
bridge irb ! interface Dot11Radio0 no ip address no ip
route-cache ! encryption mode ciphers tkip !--- This
defines the cipher method that WPA uses. The TKIP !---
method is the most secure, with use of the Wi-Fi-defined
version of TKIP. ! ssid WPAlabap1200 authentication open
eap eap_methods !--- This defines the method for the
underlying EAP when third-party clients !--- are in use.
authentication network-eap eap_methods !--- This defines
the method for the underlying EAP when Cisco clients are
in use. authentication key-management wpa !--- This
engages WPA key management. ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 192.168.2.108 255.255.255.0
!--- This is the address of this unit. no ip route-cache
! ip default-gateway 192.168.2.1 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server host 192.168.2.100 auth-port 1645 acct-
port 1646 key shared_secret !--- This defines where the
RADIUS server is and the key between the AP and server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip !! line con 0
line vty 5 15 ! end ! end

```

## Configuración de la interfaz gráfica para el usuario

Complete estos pasos para configurar el AP para el WPA:

1. Complete estos pasos para configurar al administrador del cifrado: Active el encriptación para TKIP. Borre el valor en la clave de encriptación 1. Fije la clave de encriptación 2 como la clave de transmitir. Haga clic la Aplicar-radio

#.

The screenshot displays the configuration interface for a Cisco 1200 Access Point, specifically the 'Security: Encryption Manager' for radio interface Radio0 802.11B. The left sidebar contains navigation menus for various system settings. The main content area is divided into several sections:

- Encryption Modes:** Includes radio buttons for 'None', 'WEP Encryption' (with a 'Mandatory' dropdown), and 'Cipher' (which is selected and circled in red). A dropdown menu next to 'Cipher' shows 'TKIP' selected.
- Encryption Keys:** A table with columns for 'Transmit Key', 'Encryption Key (Hexadecimal)', and 'Key Size'. 'Encryption Key 2' is selected with a radio button and circled in red.
- Global Properties:** Contains options for 'Broadcast Key Rotation Interval' (with 'Disable Rotation' selected) and 'WPA Group Key Update' (with two unchecked checkboxes).

At the bottom right, there are buttons for 'Apply-Radio0', 'Apply-All', and 'Cancel'. The footer includes the text 'Cisco Window' and 'Copyright (c) 1997-2004 by Cisco Systems, Inc.'

- Complete estos pasos para configurar al administrador SSID: Seleccione el SSID deseado de la lista actual SSID. Elija un método de autenticación apropiado. Base esta decisión en el tipo de placas cliente que usted utilice. Vea la [red EAP o la autenticación abierta con la sección EAP](#) de este documento para más información. Si el EAP trabajó antes de la adición de WPA, un cambio no es probablemente necesario. Complete estos pasos para habilitar la administración de claves: Elija **obligatorio** del menú desplegable de la administración de claves. Marque la casilla de verificación WPA. Haga clic la Aplicar-radio #.

The screenshot displays the configuration interface for a Cisco 1200 Access Point. The main title is 'Cisco 1200 Access Point'. The page is divided into several sections:

- Security: SSID Manager - Radio0-802.11B**: This section contains the 'SSID Properties' and 'Authentication Settings'.
- SSID Properties**: Shows the 'Current SSID List' with a new entry 'WPAIabop1200'. The 'SSID' field is 'WPAIabop1200', the 'VLAN' is 'NONE', and the 'Network ID' is '(0-4095)'. There are 'Delete-Radio0' and 'Delete-All' buttons.
- Authentication Settings**:
  - Methods Accepted**:
    - Open Authentication: with EAP
    - Shared Authentication: NO ADDITION
    - Network EAP: NO ADDITION
  - Server Priorities**:
    - EAP Authentication Servers**:
      - Use Defaults (selected) / Define Defaults
      - Customize
      - Priority 1: NONE
      - Priority 2: NONE
      - Priority 3: NONE
    - MAC Authentication Servers**:
      - Use Defaults (selected) / Define Defaults
      - Customize
      - Priority 1: NONE
      - Priority 2: NONE
      - Priority 3: NONE
- Authenticated Key Management**:
  - Key Management**: Mandatory (selected)
  - CCKM
  - WPA
  - WPA Pre-shared Key**: (empty field)
  - ASCII  Hexadecimal

## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **muestre el `mac_address` de la asociación del dot11** — Este comando visualiza la información sobre un cliente asociado específicamente identificado. Verifique que el cliente negocie la administración de claves como **WPA** y el cifrado como **TKIP**.

```

Cisco - HyperTerminal
File Edit View Call Transfer Help
labap1200ip102#sho dot ass 0030.6527.f74a
Address      : 0030.6527.f74a  Name      :
IP Address   : 10.0.0.25      Interface : Dot11Radio 0
Device       : -           Software Version :
CCX Version  :
State        : EAP-Assoc    Parent     : self
SSID         : WPA1abap1200  VLAN      : 0
Hops to Infra : 1         Association Id : 4
Clients Associated: 0       Repeaters associated: 0
Tunnel Address : 0.0.0.0
Key Mgmt type : WPA          Encryption : TKIP
Current Rate  : 11.0        Capability :
Supported Rates : 1.0 2.0 5.5 11.0
Signal Strength : -61 dBm    Connected for : 797 seconds
Signal Quality : 88 %      Activity Timeout : 20 seconds
Power-save    : Off        Last Activity : 40 seconds ago

Packets Input : 57        Packets Output : 42
Bytes Input   : 10976     Bytes Output   : 6767
Duplicates Rcvd : 0      Data Retries  : 10
Decrypt Failed : 0        RTS Retries   : 0
MIC Failed    : 0
MIC Missing   : 0

labap1200ip102#

```

- La entrada de tabla de la asociación para un cliente particular debe también indicar la administración de claves como **WPA** y el cifrado como **TKIP**. En la tabla de asociación, haga clic un MAC Address determinado para un cliente para ver los detalles de la asociación para ese cliente.

**Cisco 1200 Access Point**

Hostname: labap1200ip102 | 11:51:37 Wed Apr 7 2004

Association Station View - Client

Station Information and Status			
MAC Address	0030.6527.f74a	Name	
IP Address	0.0.0.0	Class	
Device		Software Version	
CCX Version			
State	EAP-Associated	Parent	self
SSID	WPA1abap1200	VLAN	none
Hops To Infrastructure	1	Communication Over Interface	Radio0-802.11B
Clients Associated	0	Repeaters Associated	0
Key Mgmt type	WPA	Encryption	TKIP
Current Rate (Mb/sec)	11.0	Capability	
Supported Rates(Mb/sec)	1.0, 2.0, 5.5, 11.0	Association Id	4
Signal Strength (dBm)	-54	Connected For (sec)	3
Signal Quality (%)	75	Activity TimeOut (sec)	59
Power-save	Off	Last Activity (sec)	1

# Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

## Procedimiento de resolución de problemas

Esta información es importante para esta configuración. Siga estos pasos para resolver problemas con su configuración:

1. Si este SALTO, EAP, o configuración de PEAP no se ha probado a conciencia antes de la implementación de WPA, usted debe completar estos pasos: Inhabilite temporalmente al modo de encriptación WPA. Vuelva a permitir el EAP apropiado. Confirme que la autenticación trabaja.
2. Verifique que la configuración del cliente haga juego el del AP. Por ejemplo, cuando el AP se configura para el WPA y el TKIP, confirme que las configuraciones hacen juego las configuraciones que se configuran en el cliente.

## Comandos para Troubleshooting

**Nota:** Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un **comando debug**.

La administración de claves WPA implica un apretón de manos de cuatro terminales después de que la autenticación EAP complete con éxito. Usted puede ver estos cuatro mensajes en los debugs. Si el EAP no autentica con éxito al cliente o si usted no ve los mensajes, complete estos pasos:

1. Inhabilite temporalmente el WPA.
2. Vuelva a permitir el EAP apropiado.
3. Confirme que la autenticación trabaja.

Esta lista describe los debugs:

- **claves del administrador aaa del dot11 del debug** — Este debug muestra que el apretón de manos que sucede entre el AP y el cliente WPA como la clave en parejas transitoria (PTK) y la clave transitoria del grupo (GTK) negocian. Este debug fue introducido en el Cisco IOS Software Release 12.2(15)JA. Si aparecen ningunas salidas de los debugs, verifique estos elementos: Se habilita el **término** terminal **lunes del** monitor (si usted utiliza a una sesión telnet). Se habilitan los debugs. Configuran al cliente apropiadamente para el WPA. Si el debug muestra que el PTK y/o las entradas en contacto GTK están construidos pero no verificados, marque el software del solicitante de WPA para la configuración correcta y la versión actualizada.
- **haga el debug de la estado-máquina del authenticator aaa del dot11** — Este debug muestra los diversos estados de las negociaciones a que va un cliente a través mientras que se asocian y autentican. Los nombres del estado indican estos estados. Este debug fue introducido en el Cisco IOS Software Release 12.2(15)JA. Los obsoletes del debug el **comando debug dot11 aaa dot1x state-machine** en el Cisco IOS Software Release 12.2(15)JA y Posterior.



- **estado-máquina del dot1x aaa del dot11 del debug** — Este debug muestra los diversos estados de las negociaciones a que va un cliente a través mientras que se asocian y autentican. Los nombres del estado indican estos estados. En las versiones de Cisco IOS Software que son anteriores que el Cisco IOS Software Release 12.2(15)JA, este debug también muestra la negociación de la administración de claves WPA.
- **debug dot11 aaa authenticator process**—Este comando de depuración es muy útil para diagnosticar problemas con comunicaciones negociadas. La información detallada muestra lo que envía cada participante en la negociación y muestra la respuesta del otro participante. Usted puede también utilizar este debug conjuntamente con el **comando debug radius authentication**. Este debug fue introducido en el Cisco IOS Software Release 12.2(15)JA. Los obsoletes del debug el **comando debug dot11 aaa dot1x process** en el Cisco IOS Software Release 12.2(15)JA y Posterior.
- **debug dot11 aaa dot1x process**—Este comando de depuración es útil para diagnosticar problemas con comunicaciones negociadas. La información detallada muestra lo que envía cada participante en la negociación y muestra la respuesta del otro participante. Usted puede también utilizar este debug conjuntamente con el **comando debug radius authentication**. En las versiones de Cisco IOS Software que son anteriores que el Cisco IOS Software Release 12.2(15)JA, este debug muestra la negociación de la administración de claves WPA.

## [Información Relacionada](#)

- [Configuración de conjuntos Cipher y WEP](#)
- [Configuración de los tipos de autenticación](#)
- [WPA2 - Acceso protegido Wi-Fi 2](#)
- [Acceso protegido Wi-Fi 2 \(configuración WPA 2\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)