

# Configuración de la Contraseña o de la Complejidad WPA-PSK en un Punto de Acceso WAP125 o WAP581

## Objetivo

La seguridad de las contraseñas aumenta con el aumento de la complejidad de las contraseñas. Es vital que utilice contraseñas largas con una combinación de letras, números y símbolos en mayúsculas y minúsculas para mantener una seguridad sólida. La complejidad de la contraseña se utiliza para establecer los requisitos de las contraseñas con el fin de reducir el riesgo de una violación de la seguridad.

El acceso Wi-Fi protegido (WPA) es uno de los protocolos de seguridad utilizados para las redes inalámbricas. En comparación con el protocolo de seguridad de privacidad equivalente a conexión con cables (WEP), WPA ha mejorado las funciones de autenticación y cifrado. Si se configura WPA en el AP, se elige una clave precompartida WPA (PSK) para autenticar los clientes de forma segura. Cuando se habilita la complejidad WPA-PSK, se pueden configurar los requisitos de complejidad para la clave utilizada en el proceso de autenticación. Las claves más complejas proporcionan una mayor seguridad.

El objetivo de este documento es mostrarle cómo configurar la Complejidad de la Contraseña y los Parámetros de Complejidad WPA-PSK en su punto de acceso WAP125 o WAP581.

## Dispositivos aplicables

- WAP125
- WAP581

## Versión del software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

## Configuración de la seguridad de contraseña

### Configurar la complejidad de la contraseña

Paso 1. Inicie sesión en la utilidad basada en Web de su WAP. El nombre de usuario y la contraseña predeterminados son cisco/cisco.



## Wireless Access Point

A login form for a Cisco Wireless Access Point. The form is enclosed in a red rounded rectangle. It contains a text input field with "cisco" entered, a password input field with ".....|" entered, a language dropdown menu currently set to "English", and a blue "Login" button at the bottom.

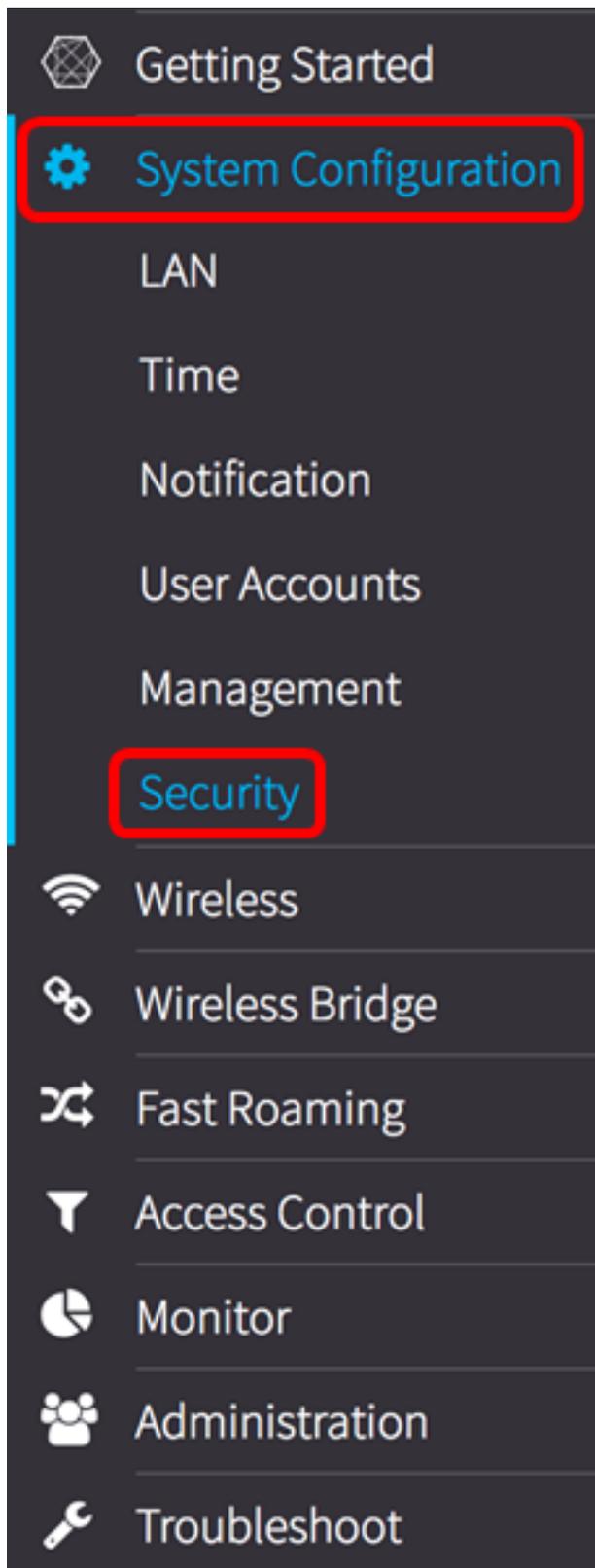
©2017 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

**Nota:** Si ya ha cambiado la contraseña o ha creado una nueva cuenta, introduzca sus nuevas credenciales.

Paso 2. Elija **System Configuration > Security**.

**Nota:** Las opciones disponibles pueden variar en función del modelo exacto del dispositivo. En este ejemplo, se utiliza WAP125.



Paso 3. Debajo del área Rogue AP Detection, haga clic en el botón **Configure Password Complexity...**

# Security

## Rogue AP Detection

AP Detection for Radio 1 (2.4 GHz) :  Enable

AP Detection for Radio 2 (5 GHz):  Enable

[View Rogue AP List...](#)

[Configure Password Complexity...](#)

[Configure WPA-PSK Complexity...](#)

Paso 4. Marque la casilla de verificación **Enable Password Complexity** (Habilitar complejidad de contraseña) para activar los pasos para establecer la complejidad de la contraseña. Si no se marca, vaya directamente al [Paso 8](#).

## Password

Password Complexity:



Paso 5. Elija un valor de la lista desplegable Clase de caracteres mínimos de contraseña. El número introducido representa el número de caracteres mínimo o máximo de las diferentes clases:

- La contraseña consta de caracteres en mayúsculas (ABCD).
- La contraseña consta de caracteres en minúsculas (abcd).
- La contraseña consta de caracteres numéricos (1234).
- La contraseña consta de caracteres especiales (!@#%).

**Nota:** En este ejemplo, se elige 3.

## Password

Password Complexity:

0

1

2

Password Minimum Character Class:

✓ 3

4

Paso 6. Marque la casilla de verificación **Enable** Password Different from Current para permitir a los usuarios actualizar su contraseña cuando caduque. Si no se marca, los usuarios pueden volver a introducir la misma contraseña cuando caduque.

## Password

Password Complexity:

Enable

Password Minimum Character Class:

3

Password Different from Current:

Enable

Paso 7. En el campo *Maximum Password Length*, introduzca un valor entre 64 y 127 para definir el número de caracteres y la longitud de la contraseña. El valor predeterminado es 64.

**Nota:** En este ejemplo, se utiliza 65.

## Password

Password Complexity:

Enable

Password Minimum Character Class:

3

Password Different from Current:

Enable

Maximum Password Length: 

65

[Paso 8.](#) En el campo *Longitud mínima de contraseña*, introduzca un valor entre 0 y 32 para establecer el número mínimo de caracteres necesario para la contraseña. El valor predeterminado es 8.

**Nota:** En este ejemplo, la longitud mínima de la contraseña es 9.

## Password

---

Password Complexity:  Enable

Password Minimum Character Class: 3

Password Different from Current:  Enable

Maximum Password Length:

Minimum Password Length:

Paso 9. Marque la casilla de verificación **Habilitar** soporte de caducidad de contraseñas para permitir que las contraseñas caduquen. Si está activado, continúe con el siguiente paso; de lo contrario, vaya directamente a .

## Password

---

Password Complexity:  Enable

Password Minimum Character Class: 3

Password Different from Current:  Enable

Maximum Password Length:

Minimum Password Length:

Password Aging Support:  Enable

[Paso 10.](#) En el campo *Password Ageing Time*, ingrese un valor entre 1 y 365 para establecer el número de días antes de que venza una contraseña recién creada. El valor predeterminado es 180 días.

**Nota:** En este ejemplo, se utiliza 180.

## Password

---

Password Complexity:  Enable

Password Minimum Character Class:

Password Different from Current:  Enable

Maximum Password Length:

Minimum Password Length:

Password Aging Support:  Enable

Password Aging Time:

Paso 11. Click OK. Volverá a la página principal de configuración de seguridad.

## Password

---

Password Complexity:  Enable

Password Minimum Character Class:

Password Different from Current:  Enable

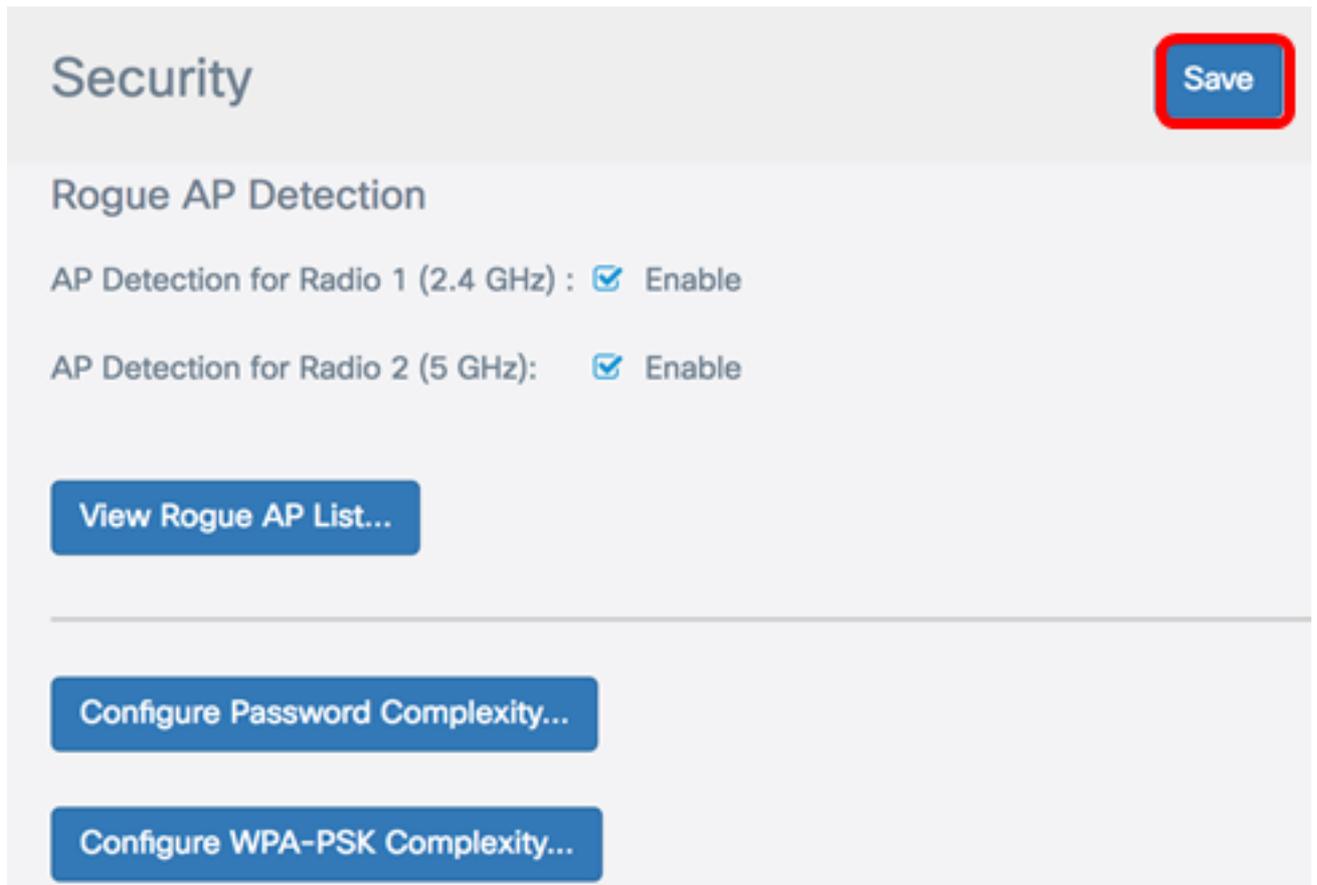
Maximum Password Length:

Minimum Password Length:

Password Aging Support:  Enable

Password Aging Time:

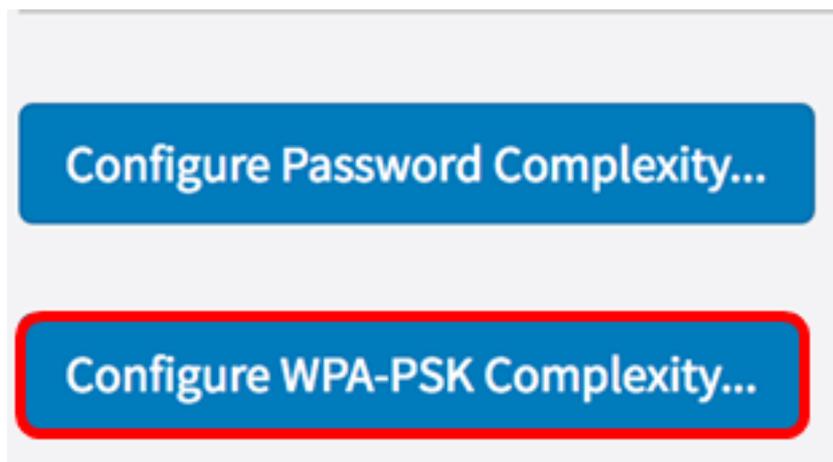
Paso 12. Haga clic en el botón **Guardar** para guardar los parámetros configurados.



Ahora debería haber configurado correctamente los parámetros de seguridad de complejidad de contraseña en su WAP.

## Configuración de la complejidad WPA-PSK

Paso 1. Haga clic en el botón **Configurar complejidad WPA-PSK**.



Paso 2. Marque la casilla de verificación **Enable** WPA-PSK Complexity (Habilitar complejidad WPA-PSK) para activar los pasos para establecer la complejidad de la contraseña.

## WPA-PSK

WPA-PSK Complexity:



Paso 3. Elija un valor de la lista desplegable Clase de caracteres mínimos WPA-PSK. El número introducido representa el número de caracteres mínimo o máximo de las diferentes clases:

- La contraseña consta de caracteres en mayúsculas (ABCD).
- La contraseña consta de caracteres en minúsculas (abcd).
- La contraseña consta de caracteres numéricos (1234).
- La contraseña consta de caracteres especiales (!@#%).

**Nota:** En este ejemplo, se elige 3.

## WPA-PSK

WPA-PSK Complexity:

WPA-PSK Minimum Character Class:

A dropdown menu with a light gray background and a blue highlight on the selected option. The options are 0, 1, 2, 3, and 4. The option 3 is selected and highlighted with a red border. A blue arrow on the right side indicates the dropdown is open.

Paso 4. Marque la casilla de verificación **Enable** WPA-PSK Different from Current para permitir que los usuarios actualicen su contraseña cuando caduque. Si no se marca, los usuarios pueden volver a introducir la misma contraseña cuando caduque.

## WPA-PSK

WPA-PSK Complexity:



WPA-PSK Minimum Character Class:

3

WPA-PSK Different from Current:



Paso 5. En el campo *Longitud máxima WPA-PSK*, introduzca un valor de 32 a 63 para definir el número de caracteres y la longitud de la contraseña. El valor predeterminado es 63.

**Nota:** En este ejemplo, se utiliza 63.

## WPA-PSK

---

WPA-PSK Complexity:  Enable

WPA-PSK Minimum Character Class:

3

WPA-PSK Different from Current:  Enable

Maximum WPA-PSK Length: 

63

Paso 6. En el campo Longitud *mínima* WPA-PSK, introduzca un valor entre 0 y 32 para establecer el número *mínimo* requerido de caracteres para la contraseña. El valor predeterminado es 8.

**Nota:** En este ejemplo, la longitud mínima de la contraseña es 9.

## WPA-PSK

---

WPA-PSK Complexity:  Enable

WPA-PSK Minimum Character Class:

3

WPA-PSK Different from Current:  Enable

Maximum WPA-PSK Length: 

63

Minimum WPA-PSK Length: 

9

Paso 7. Click OK. Volverá a la página principal de configuración de seguridad.

## WPA-PSK

WPA-PSK Complexity:  Enable

WPA-PSK Minimum Character Class:

WPA-PSK Different from Current:  Enable

Maximum WPA-PSK Length:

Minimum WPA-PSK Length:

OK

cancel

Paso 8. Haga clic en el botón **Guardar** para guardar los parámetros configurados.

## Security

Save

### Rogue AP Detection

AP Detection for Radio 1 (2.4 GHz) :  Enable

AP Detection for Radio 2 (5 GHz):  Enable

View Rogue AP List...

Configure Password Complexity...

Configure WPA-PSK Complexity...

Ahora debería haber configurado correctamente los parámetros de seguridad de complejidad WPA-PSK en su WAP.