

Guía del usuario

Punto de acceso

© 2024 TP-Link 1910013169 REV4.9.0

Nota: Las funciones disponibles en el Programa de Asistencia al Usuario (EAP) pueden variar según el modelo y la versión del software. Todas las imágenes, pasos y descripciones de esta guía son solo ejemplos y pueden no reflejar su experiencia real con el producto.

CONTENIDO

Acerca de esta guía del usuario.....	1
Resumen	3
1 Inicio rápido.....	4
1.1 Determinar el método de gestión.....	5
1.2 Conectar dispositivos de red.....	6
1.3 Inicie sesión en el EAP y cambie el SSID.....	8
1.4 Configurar y administrar el EAP.....	23
2 Configurar la red.....	24
2.1 Configurar los parámetros inalámbricos.....	25
2.1.1 Configurar SSIDs	26
2.1.2 Configurar ajustes avanzados inalámbricos	33
Configuración de radio.....	33
Balance de carga.....	35
Equidad en el tiempo de emisión	35
Más ajustes	36
2.1.3 Configurar la red MLO (solo para dispositivos Wi-Fi 7)	38
2.2 Configurar la autenticación del portal	40
Configurar portal.....	41
Configurar la política de autenticación gratuita	47
2.3 Configurar VLAN.....	50
2.4 Configurar el filtrado MAC.....	51
2.5 Configurar el programador.....	54
2.6 Configurar la dirección de banda.....	57
2.7 Configurar QoS.....	58
2.8 Configurar la detección de puntos de acceso no autorizados.....	62
Detectar puntos de acceso no autorizados y moverlos a la lista de puntos de acceso de confianza.....	63

Administrar la lista de AP de confianza.....	64
2.9 Configurar la antena inteligente (solo para ciertos dispositivos).....	66
3. Monitorear la red	67
3.1 Monitorear el EAP.....	68
3.2 Monitorear los parámetros inalámbricos.....	70
Monitorear los SSID.....	71
Supervise la configuración de la radio.....	72
Monitorear el tráfico de radio	72
Monitorear el tráfico de la LAN.....	73
3.3 Monitorear a los clientes.....	75
Ver información del cliente.....	75
Ver información del cliente del bloque	77
4 Gestionar el EAP.....	78
4.1 Administrar los AP de puente (solo para un AP principal de puente).....	79
4.2 Gestionar la dirección IP del EAP.....	80
4.3 Administrar los registros del sistema.....	83
Ver registros del sistema	83
Configurar la forma de recibir registros.....	84
4.4 Configurar el servidor web.....	86
4.5 Configurar el acceso de administración.....	87
Configurar la administración de MAC de acceso.....	87
Configurar VLAN de administración	88
4.6 Configurar el enlace troncal (solo para ciertos dispositivos).....	89
4.7 Configurar LED.....	90
4.8 Configurar el control Wi-Fi (solo para ciertos dispositivos).....	91
4.9 Configurar PoE Out (solo para ciertos dispositivos)	92
4.10 Configurar SSH.....	93
4.11 Configurar SNMP.....	94
4.12 Configurar el ahorro de energía (solo para ciertos dispositivos)	96

5 Configurar el sistema.....	97
5.1 Configurar la cuenta de usuario.....	98
5.2 Configuración del controlador.....	99
Habilitar la administración del controlador basada en la nube.....	99
Configurar la URL de información del controlador	101
5.3 Configurar la hora del sistema.....	102
Configurar la hora del sistema	103
Configurar el horario de verano.....	105
5.4 Reiniciar y restablecer el EAP.....	107
5.5 Copia de seguridad y restauración de la configuración.....	108
5.6 Actualizar el firmware	109
 6 Ejemplo de aplicación	 110
6.1 Determinar los requisitos de la red	111
6.2 Construir la topología de red.....	112
6.3 Iniciar sesión en el EAP.....	113
6.4 Configurar el EAP	114
Configurar SSIDs	114
Configurar la autenticación del portal.....	115
Configurar el programador.....	117
6.5 Prueba la red.....	119

Acerca de esta guía del usuario

Al usar esta guía, tenga en cuenta que las funciones disponibles en el Programa de Asistencia al Usuario (EAP) pueden variar según el modelo y la versión del software. La disponibilidad del EAP también puede variar según la región o el proveedor de servicios de Internet (ISP). Todas las imágenes, pasos y descripciones de esta guía son solo ejemplos y pueden no reflejar su experiencia real.

Es posible que algunos modelos que aparecen en esta guía no estén disponibles en su país o región. Para ventas locales, consulte la información disponible.

Para obtener información, visite <https://www.tp-link.com>.

La información contenida en este documento está sujeta a cambios sin previo aviso. Se ha hecho todo lo posible para garantizar la exactitud de su contenido, pero las declaraciones, la información y las recomendaciones aquí presentadas no constituyen garantía alguna, ni expresa ni implícita. Los usuarios son totalmente responsables del uso que hagan de cualquier producto.

Descargo de responsabilidad sobre la velocidad y el alcance inalámbricos

Las velocidades máximas de transmisión inalámbrica son las velocidades físicas derivadas de las especificaciones del estándar IEEE 802.11. Las especificaciones de alcance y cobertura se definieron según los resultados de las pruebas realizadas en condiciones normales de uso. La velocidad de transmisión inalámbrica y la cobertura inalámbrica reales no están garantizadas y variarán en función de: 1) factores ambientales, como los materiales de construcción, los objetos físicos y los obstáculos; 2) las condiciones de la red, como la interferencia local, el volumen y la densidad del tráfico, la ubicación del producto, la complejidad de la red y la sobrecarga de la red; y 3) las limitaciones del cliente, como el rendimiento nominal, la ubicación, la calidad de la conexión y el estado del cliente.

Descargo de responsabilidad sobre las limitaciones del puerto Ethernet

La velocidad real de la red puede verse limitada por la velocidad del puerto Ethernet WAN o LAN del producto, la velocidad admitida por el cable de red, factores del proveedor de servicios de Internet y otros factores ambientales.
condiciones.

Descargo de responsabilidad sobre la capacidad del cliente inalámbrico

Las especificaciones de capacidad del cliente inalámbrico se definieron según los resultados de las pruebas realizadas en condiciones normales de uso. La capacidad real del cliente inalámbrico no está garantizada y variará en función de: 1) factores ambientales, como los materiales de construcción, los objetos físicos y los obstáculos; 2) las condiciones de la red, como las interferencias locales, el volumen y la densidad del tráfico, la ubicación del producto, la complejidad de la red y la sobrecarga de la misma; y 3) las limitaciones del cliente, como el rendimiento nominal, la ubicación, la calidad de la conexión y el estado del cliente.

Descargo de responsabilidad de MU-MIMO (para EAP que admiten MU-MIMO)

La compatibilidad con MU-MIMO requiere dispositivos cliente que también sean compatibles con MU-MIMO.

Aviso legal sobre la itinerancia sin interrupciones (para los EAP que admiten la itinerancia sin interrupciones)

Para que la itinerancia sea fluida, tanto el punto de acceso como los dispositivos cliente deben ser compatibles con los protocolos 802.11k y 802.11v.

Descargo de responsabilidad sobre protección contra rayos y descargas electrostáticas (para sistemas de protección contra rayos en exteriores)

La protección contra rayos y descargas electrostáticas se logra mediante una configuración adecuada del producto, la conexión a tierra y el apantallamiento de los cables. Consulte el manual de instrucciones y a un técnico informático para obtener ayuda con la configuración.

Más información

Es posible que algunos modelos que aparecen en esta guía no estén disponibles en su país o región. Para obtener información sobre ventas locales, visite <https://www.tp-link.com>

Para obtener asistencia técnica, el software más reciente y la aplicación de gestión, visite <https://www.tp-link.com/support>

La Guía de instalación rápida se puede encontrar donde se encuentra esta guía o dentro del paquete del producto.

La información de autenticación se encuentra en el mismo lugar donde se encuentra esta guía.

Las especificaciones se pueden encontrar en la página del producto en <https://www.tp-link.com>

Para hacer preguntas, encontrar respuestas y comunicarse con usuarios o ingenieros de TP-Link, visite <https://community.tp-link.com> para unirte a la comunidad TP-Link.

Descripción general

Los productos de la serie Omada proporcionan soluciones de cobertura inalámbrica para pequeñas y medianas empresas y hogares. Pueden funcionar de forma independiente como puntos de acceso autónomos o gestionarse centralmente mediante el controlador de software Omada, el controlador de hardware Omada o el controlador basado en la nube Omada, proporcionando una red inalámbrica flexible, con muchas funciones pero fácil de configurar para pequeñas y medianas empresas, empresas y hogares.

1

Comenzar

Este capítulo presenta cómo construir una red inalámbrica utilizando los EAP y cómo completar la configuración básica. Sigue los pasos a continuación:

1.1 Determinar el método de gestión

Conectar dispositivos de red 1.2

1.3 Inicie sesión en el EAP y cambie el SSID.

1.4 Configurar y Gestionar el _____

1.1 Determinar el método de gestión

Antes de construir su red, elija un método adecuado para administrar sus EAP.

Las dos opciones siguientes:

■ Modo de control

Si desea administrar una red a gran escala de forma centralizada, seleccione el Modo Controlador. En el Modo Controlador, puede configurar y supervisar múltiples EAP, conmutadores y gateways a través de Omada SDN Controller. Para obtener instrucciones detalladas, visite la [página de soporte de Omada Controlador](#) y descarga la Guía del Usuario.

■ Modo independiente

Si desea administrar solo unos pocos EAP, elija el modo independiente. En el modo independiente, puede configurar y monitorear individualmente sus EAP a través de la aplicación Omada o un navegador web, y

Cada programa de asistencia al empleado (PAE) tiene su propia página de administración.

Este capítulo explica cómo empezar a configurar el EAP en modo independiente.

Nota:

- El modo independiente es inaccesible mientras el EAP está siendo administrado por un controlador. Para volver a poner el EAP en modo independiente, En el modo independiente, puede eliminar el EAP del controlador o restablecer el EAP.
- Para que el controlador detecte sus EAP, debe configurar en ciertos escenarios. [5.2 Configuración del controlador](#)

Introducción

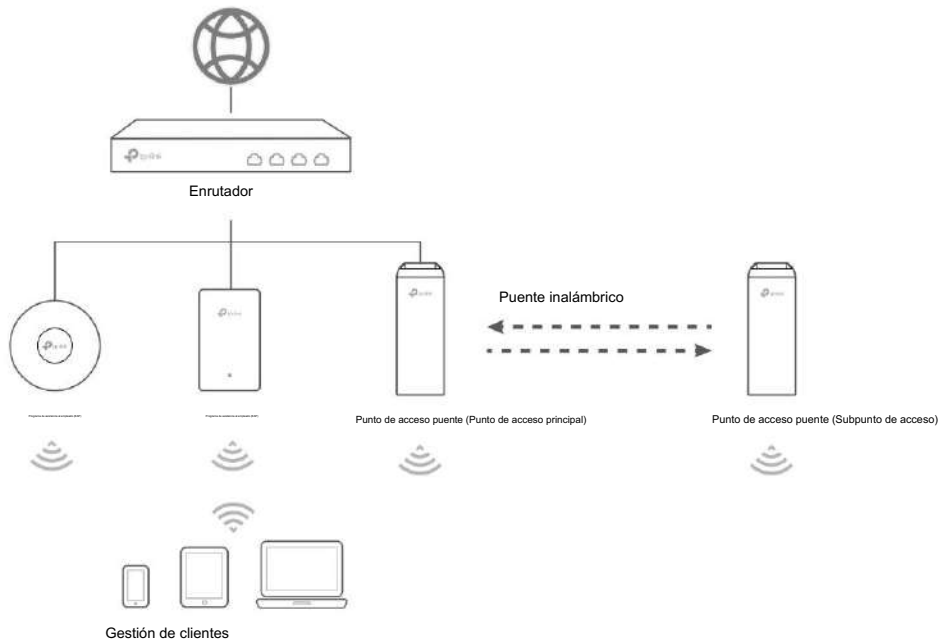
En escenarios como las conexiones inalámbricas entre edificios distribuidos y la transmisión de video de seguridad, los puentes inalámbricos PtP (punto a punto) y PtMP (punto a multipunto) son necesarios para facilitar el backend de datos desde el front-end.

Los puntos de acceso de puente inalámbrico de Omada admiten el emparejamiento automático, lo que brinda m red de puente.

Como se muestra en el diagrama de topología, puede usar EAP-Bridge para transmitir flujos de datos a larga distancia mediante la configuración de una conexión PtP.

1.2 Conectar dispositivos de red

Para conectar sus puntos de acceso EAP a la red local, consulte la siguiente topología.



1. Conecta tu router a internet.

2. Conecte sus puntos de acceso EAP a los puertos LAN de su enrutador.

Para un kit Bridge, conecte un EAP a su router. Este EAP funcionará como el AP principal. Los demás EAP del kit se conectarán automáticamente al AP principal de forma inalámbrica.

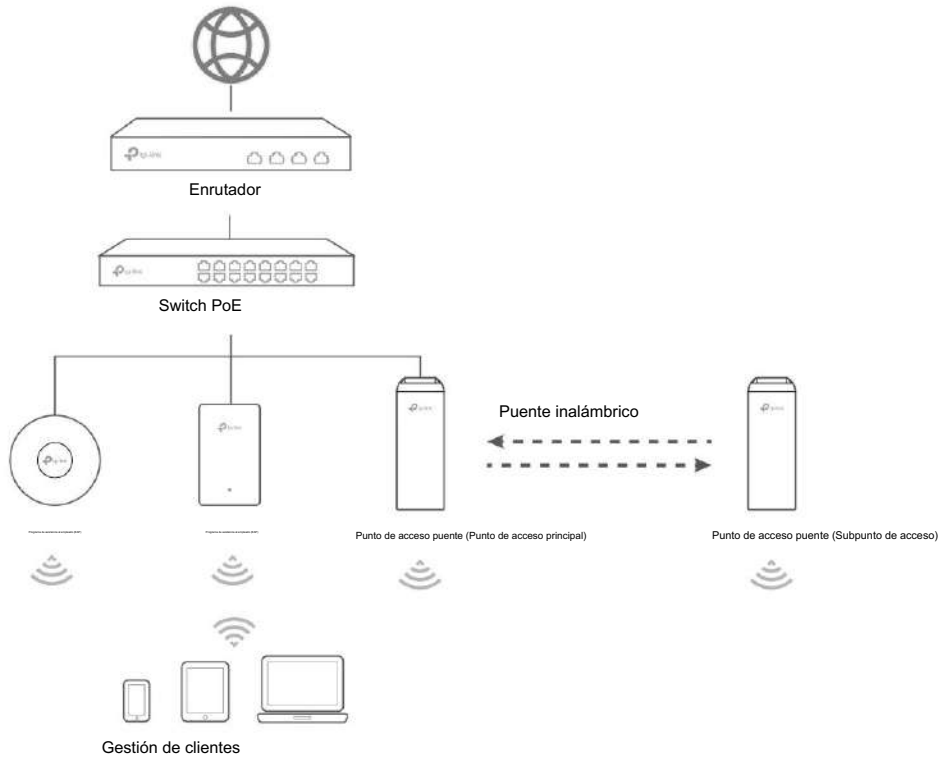
servir de enlace y trabajar como Sub-AP(s).

3. Conecte sus clientes inalámbricos, como teléfonos, tabletas y computadoras portátiles, al WiFi de un EAP. Los SSID predeterminados se imprimen en el EAP.

Ahora puedes navegar por Internet en tus teléfonos, tabletas y portátiles. Si no puedes acceder Internet, consulte las [preguntas frecuentes](#). para solucionar el problema.

Consejos:

- Si desea alimentar sus EAP mediante un conmutador PoE, consulte la siguiente topología.



- El router es la puerta de enlace de la red, y los dispositivos de la LAN navegan por Internet a través del router. Al mismo tiempo, el router actúa como servidor DHCP para asignar direcciones IP dinámicas a los puntos de acceso EAP y a los clientes.

1.3 Inicie sesión en el EAP y cambie el SSID.

Por defecto, cualquiera puede conectarse a la red WiFi de EAP sin autenticación, ya que el SSID predeterminado no tiene contraseña.

Por motivos de seguridad, recomendamos cambiar la contraseña predeterminada.

SSID.

Inicie sesión en el EAP antes de cambiar el SSID predeterminado. Puede usar la aplicación Omada en su dispositivo móvil o el navegador web en su PC. Elija un método de los siguientes:

secciones y siga las instrucciones.

Consejos:

- Solo un usuario puede iniciar sesión en el EAP a la vez.
- La aplicación Omada está diseñada para ayudarte a configurar rápidamente algunos ajustes básicos. Para configurar funciones avanzadas, utiliza el navegador web de tu ordenador.
- La aplicación Omada solo es compatible con ciertas versiones de firmware de la EAP. Para comprobar las versiones de firmware de las EAP compatibles, consulte https://www.tp-link.com/omada_compatibility_lista.

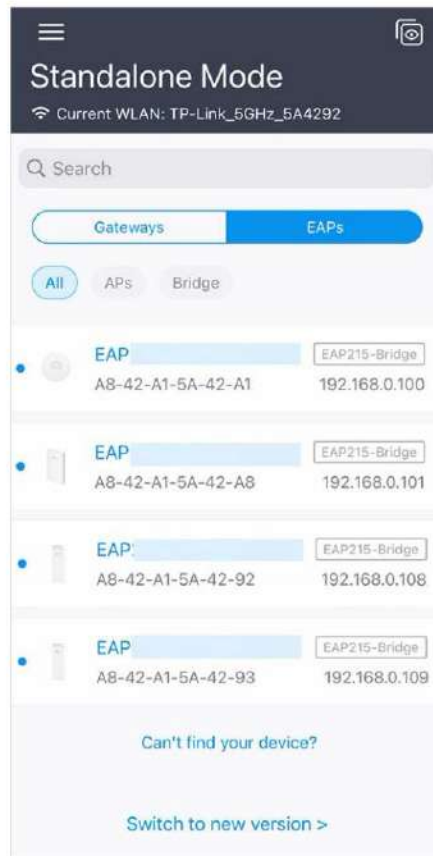
■ Uso de la aplicación Omada en su dispositivo móvil

1. Descarga e instala la aplicación TP-Link Omada desde App Store o Google Play.

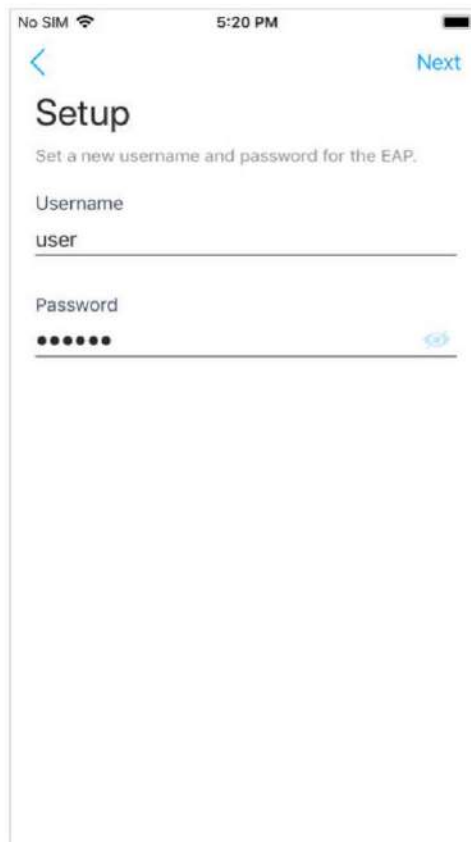


2. Conecte su dispositivo móvil a la red WiFi de un EAP. Los SSID predeterminados están impresos en el dispositivo.

3. Inicie la aplicación Omada y vaya a Dispositivos independientes > EAP. La aplicación Omada le mostrará Descubre y lista todos los EAP en la subred actual.



4. Toca cada EAP y sigue las instrucciones de la aplicación para configurarlo. Establece un nuevo nombre de usuario y la contraseña para acceder a su cuenta del EAP.



No SIM 5:20 PM

< Next

Setup

Set a new username and password for the EAP.

Username
user

Password
••••••

5. Cambia el SSID y la contraseña para mantener segura tu red inalámbrica. Pulsa Siguiete.



No SIM 3:04 PM 41%

< Next

Wireless Settings

2.4GHz Network

SSID
TP-Link_test

Password
tplink123
Password should contain at least 8 characters.

5GHz Network

Copy 2.4GHz Network

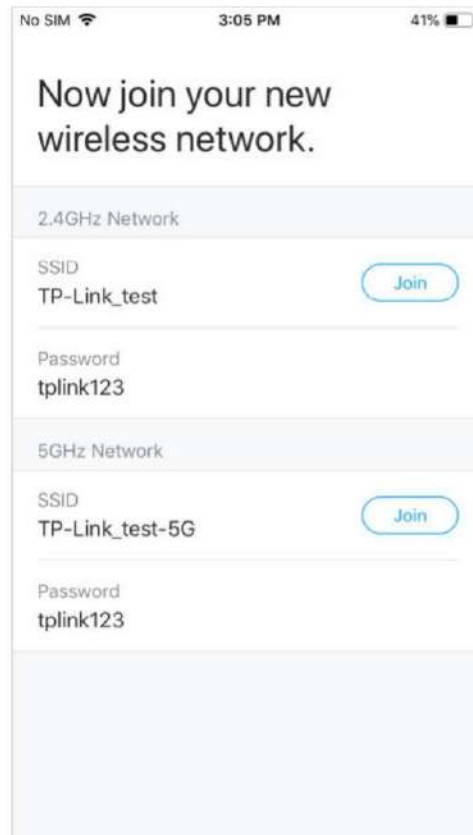
SSID
TP-Link_test-5G

Password
tplink123

6. Confirme la configuración en la página de resumen. Pulse Siguiente y la configuración se aplicará en varios minutos.



7. Para unirse a tu nueva red inalámbrica, selecciona el SSID y pulsa Unirse.



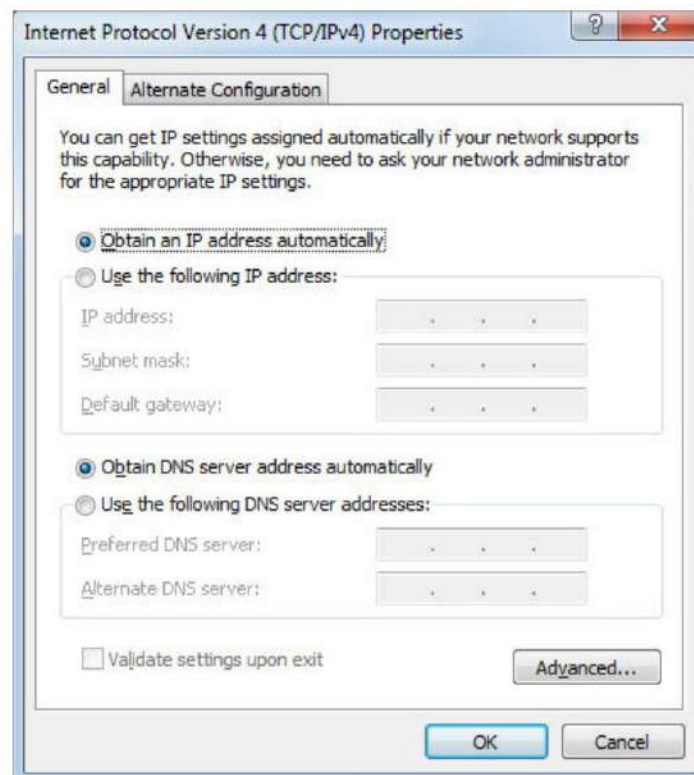
8. Pulsa Continuar para ir a la página de administración. En esta página, puedes ver la información y la configuración del EAP. Si quieres cambiar la configuración, incluyendo la radio, el SSID y la cuenta del dispositivo, pulsa .



Ahora puedes conectar tus teléfonos, tabletas y portátiles a la nueva red WiFi. Si no puedes Acceda a Internet y consulte las [preguntas frecuentes](#). para solucionar el problema.

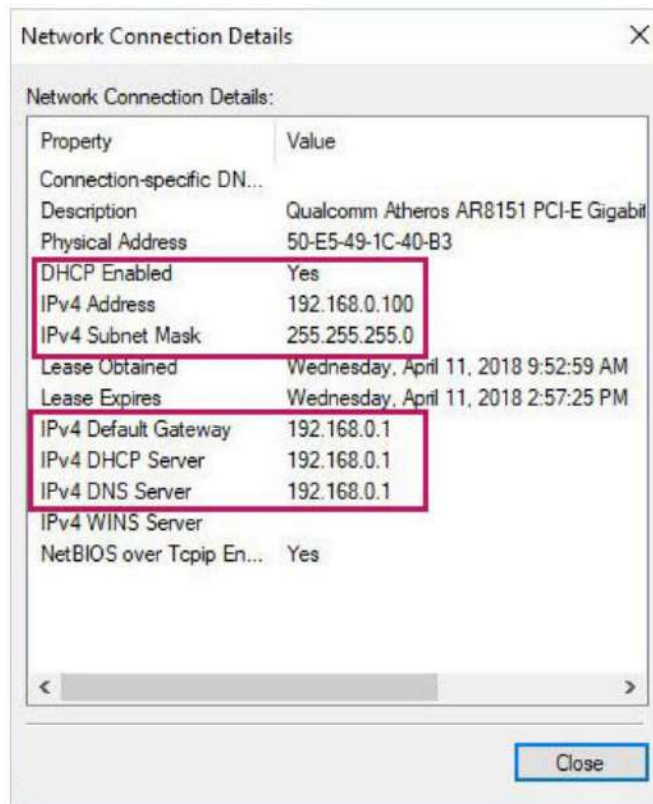
■ Usar el navegador web en su PC y conectarse a la red WiFi

1. Configura tu PC para que obtenga una dirección IP automáticamente.



2. Conecte su PC a la red WiFi de un EAP. Los SSID predeterminados están impresos en el EAP.

3. Asegúrese de que su PC tenga la dirección IP, la puerta de enlace predeterminada y el servidor DNS de el servidor DHCP.

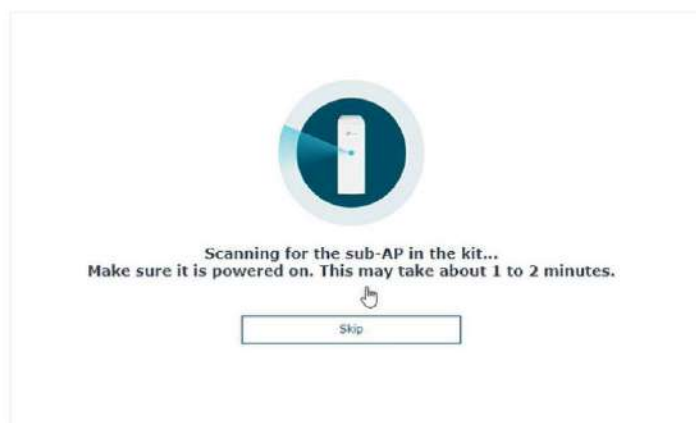


4. Para iniciar sesión en el EAP, abra un navegador web e ingrese <http://tplinkeap.net> en la dirección. barra. Aparecerá la página de inicio de sesión. Por defecto, tanto el nombre de usuario como la contraseña son admin.

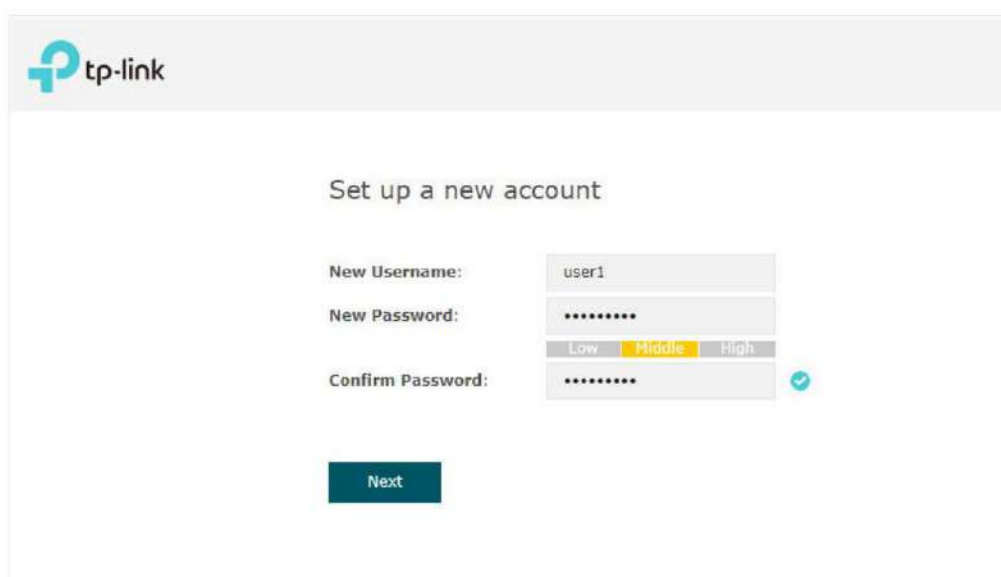


5. Después de iniciar sesión en el EAP, siga las instrucciones paso a paso para completar el proceso básico. configuraciones.

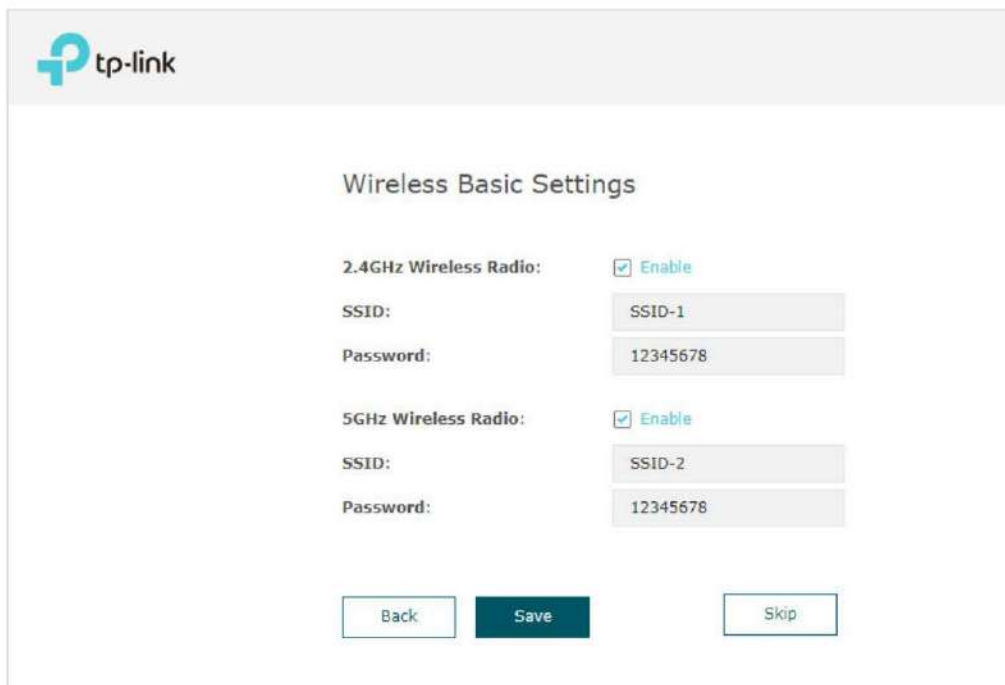
Si se conecta al AP principal (el que está conectado a su enrutador) de un producto de kit Bridge, el sistema escaneará automáticamente los Sub-AP del kit y los conectará a la red.



6. En la ventana emergente, configure un nuevo nombre de usuario y una nueva contraseña para su usuario. cuenta, luego haga clic en Siguiente.

A screenshot of the TP-Link web interface for setting up a new account. The TP-Link logo is in the top left corner. The main heading is "Set up a new account". Below this, there are three input fields: "New Username:" with the value "user1", "New Password:" with a masked password "*****" and a strength indicator below it showing "Low", "Middle" (highlighted in yellow), and "High", and "Confirm Password:" with a masked password "*****" and a blue checkmark icon to its right. At the bottom, there is a dark blue button labeled "Next".

7. Configure el SSID y la contraseña. Haga clic en Guardar.



tp-link

Wireless Basic Settings

2.4GHz Wireless Radio: Enable

SSID:

Password:

5GHz Wireless Radio: Enable

SSID:

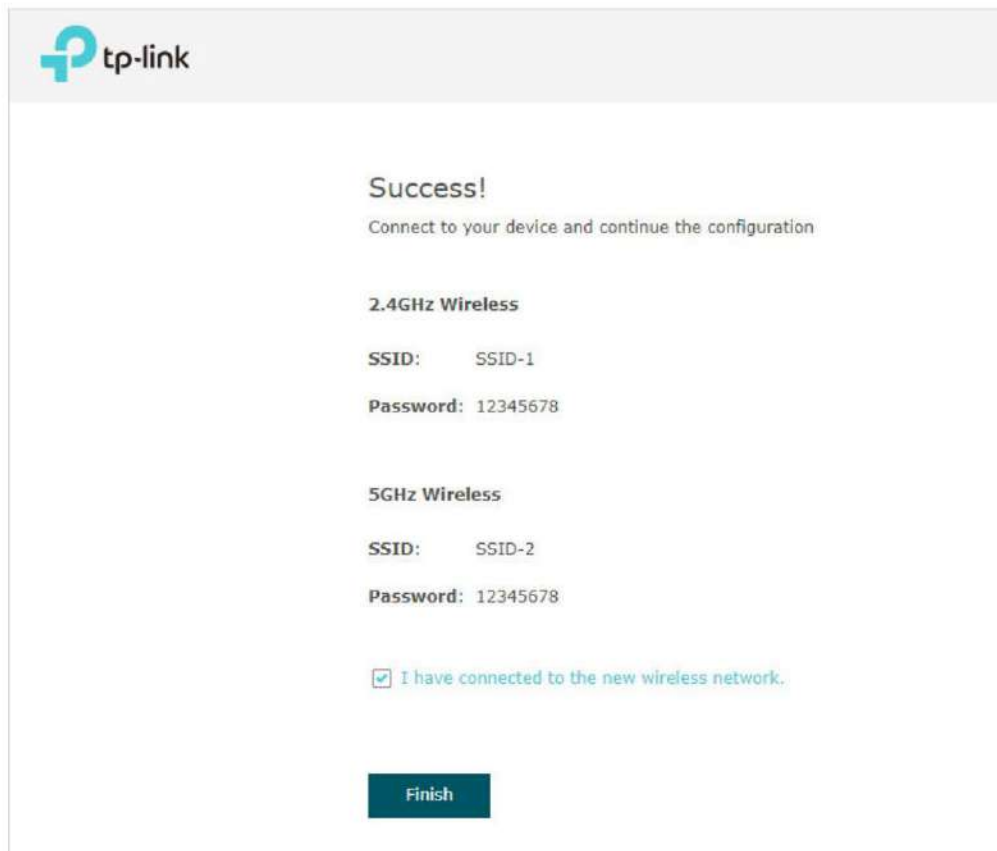
Password:

Consejos:

Puede omitir este paso y configurar los ajustes inalámbricos más adelante en la página de administración. Si es necesario, también puede crear más SSID. Para obtener instrucciones detalladas, consulte [Configurar la conexión inalámbrica](#).

Parámetros

8. Aparecerá la siguiente página. Asegúrese de que su dispositivo esté conectado a la nueva red.
Seleccione la red inalámbrica y marque la casilla. A continuación, haga clic en Finalizar.



Ahora puedes conectar tus teléfonos, tabletas y portátiles a la nueva red WiFi. Si no puedes acceder a internet, consulta las [preguntas frecuentes](#) para [solucionar](#) el problema.

■ Uso del navegador web en su PC y conexión a la red Ethernet

1. Obtenga la dirección IP del EAP. Hay dos métodos.

- Utilizar la lista de clientes DHCP del router

Inicie sesión en el router que actúa como servidor DHCP. En la lista de clientes DHCP, busque la dirección IP de su EAP según su dirección MAC. La dirección MAC se puede encontrar en

la parte inferior del EAP. En la siguiente figura, por ejemplo, la dirección IP del EAP es 192.168.0.118.

The screenshot displays the TP-Link web interface in the 'Advanced' settings section. The 'DHCP Server' is enabled, and the 'IP Address Pool' is set to 192.168.0.100 - 192.168.0.199. The 'Address Lease Time' is 120 minutes. The 'Default Gateway', 'Primary DNS', and 'Secondary DNS' are all set to 192.168.0.1. Below the settings is an 'Address Reservation' table and a 'DHCP Client List' table. The 'DHCP Client List' shows one client named 'EAP' with MAC address B0-4E-26-B4-A7-42 and assigned IP address 192.168.0.118.

ID	Client Name	MAC Address	Assigned IP Address	Lease Time
1	EAP	B0-4E-26-B4-A7-42	192.168.0.118	01:59:30

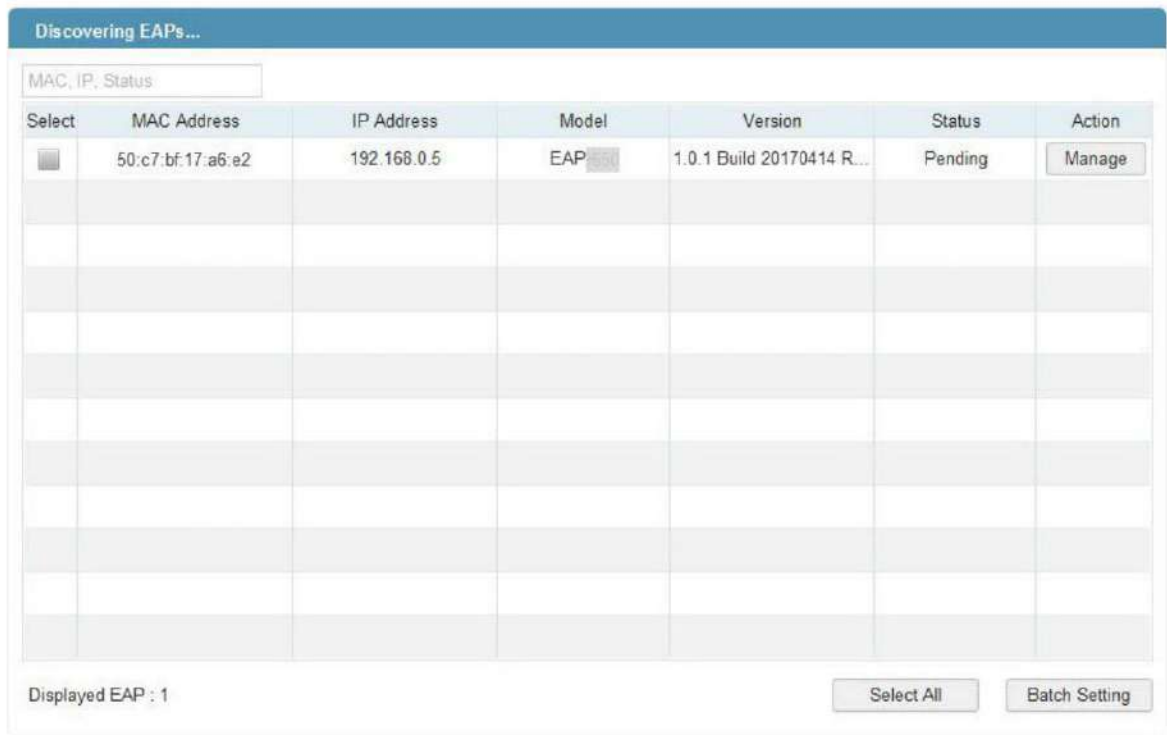
Consejos:

Cuando el servidor DHCP no está disponible en su red, el EAP tiene la dirección IP de reserva DHCP, que por defecto es 192.168.0.254 .

- Uso de la utilidad de detección de EAP

Visite https://www.tp-link.com/download/EAP-Controller.html#EAP_Discovery_Tool para descargar, instalar y ejecutar la utilidad de detección de EAP en su PC. La utilidad de detección de EAP puede

Escanee todos los EAP en el mismo segmento de red y encuentre la dirección IP del EAP. En la siguiente figura, por ejemplo, la dirección IP del EAP es 192.168.0.5.



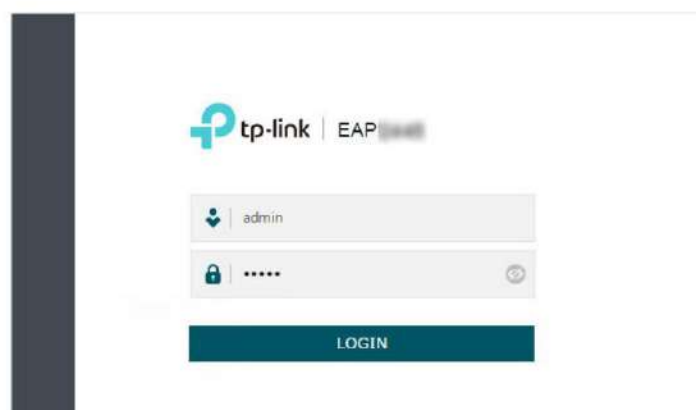
The screenshot shows a web interface titled "Discovering EAPs...". It features a search bar with the text "MAC, IP, Status". Below the search bar is a table with the following columns: "Select", "MAC Address", "IP Address", "Model", "Version", "Status", and "Action". The table contains one row with the following data: "Select" (checkbox), "MAC Address" (50:c7:bf:17:a6:e2), "IP Address" (192.168.0.5), "Model" (EAP), "Version" (1.0.1 Build 20170414 R...), "Status" (Pending), and "Action" (Manage button). At the bottom of the interface, there is a label "Displayed EAP : 1" and two buttons: "Select All" and "Batch Setting".

Select	MAC Address	IP Address	Model	Version	Status	Action
<input type="checkbox"/>	50:c7:bf:17:a6:e2	192.168.0.5	EAP	1.0.1 Build 20170414 R...	Pending	Manage

Consejos:

Algunos modelos EAP solo funcionan con ciertas versiones del software Discovery Utility. Si Discovery Utility no puede detectar su EAP, pruebe con una versión diferente del software.

2. Para iniciar sesión en el EAP, abra un navegador web e introduzca la dirección IP del EAP en la barra de direcciones. Aparecerá la página de inicio de sesión. Por defecto, tanto el nombre de usuario como la contraseña son administradores.



Consejos:

Para facilitar el acceso al EAP, puede configurar una dirección IP estática y recordarla o anotarla. Asegúrese de que esta dirección IP no esté siendo utilizada por otros dispositivos en la misma LAN.

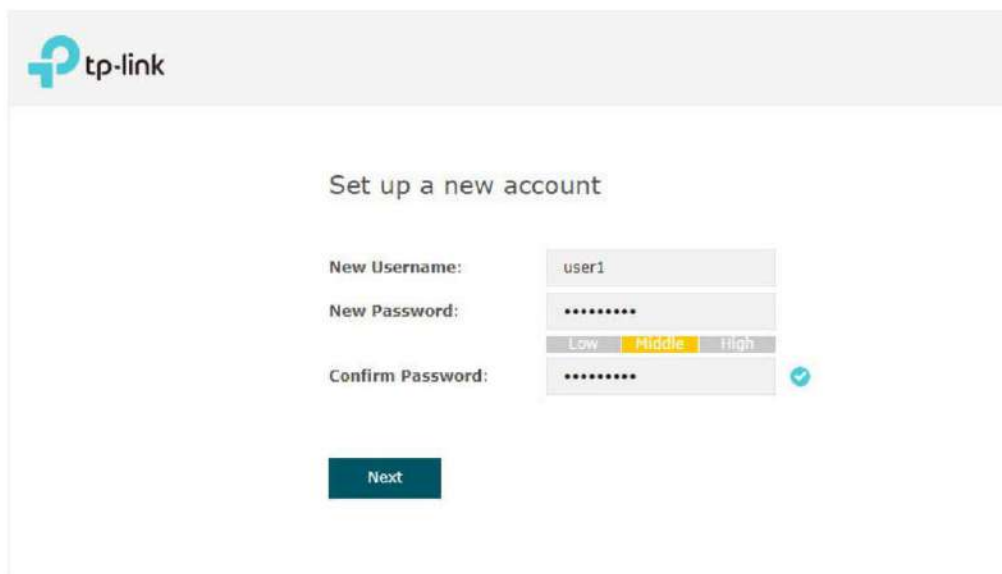
Para obtener instrucciones detalladas sobre cómo configurar una dirección IP estática para el EAP, consulte [4.2 Gestionar el IP Dirección de la](#)

3. Después de iniciar sesión en el EAP, siga las instrucciones paso a paso para completar el proceso básico de configuraciones.

Si se conecta al AP principal (el que está conectado a su enrutador) de un kit Bridge, el sistema buscará automáticamente los Sub-AP del kit y los conectará a la red.



4. En la ventana emergente, configure un nuevo nombre de usuario y una nueva contraseña para su usuario. cuenta, luego haga clic en Siguiente.

A screenshot of the TP-Link web interface for setting up a new account. The TP-Link logo is in the top left corner. The main heading is "Set up a new account". Below this are three input fields: "New Username:" with the value "user1", "New Password:" with a masked password and a strength indicator showing "Low", "Middle", and "High" (with "Middle" highlighted in yellow), and "Confirm Password:" with a masked password and a blue checkmark icon to its right. A dark blue "Next" button is located at the bottom center.

5. Configure el SSID y la contraseña. Haga clic en Guardar.

tp-link

Wireless Basic Settings

2.4GHz Wireless Radio: Enable

SSID: SSID-1

Password: 12345678

5GHz Wireless Radio: Enable

SSID: SSID-2

Password: 12345678

Back Save Skip

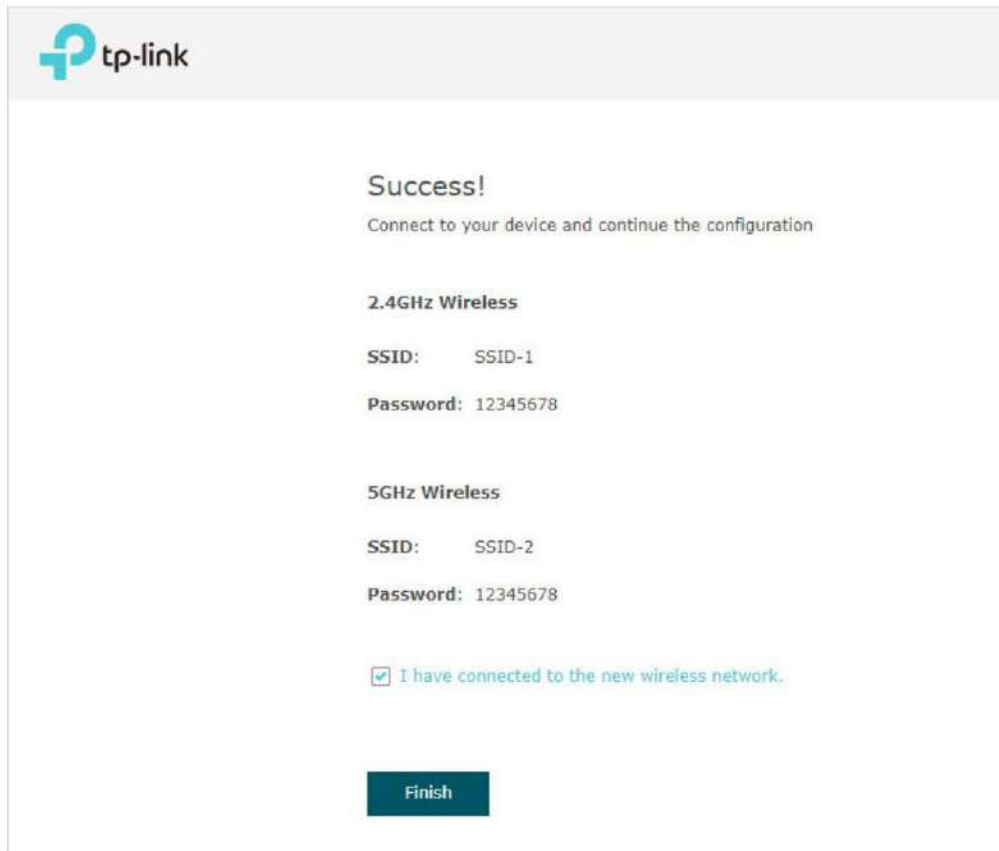
Consejos:

Puede omitir este paso y configurar los ajustes inalámbricos más adelante en la página de administración. Si es necesario, también puede crear más SSID. Para obtener instrucciones detalladas, consulte [Configurar la conexión inalámbrica](#).

Parámetros

6. Aparecerá la siguiente página. Asegúrese de que su dispositivo esté conectado a la nueva red.

Seleccione la red inalámbrica y marque la casilla. A continuación, haga clic en Finalizar.



The screenshot shows the TP-Link configuration interface. At the top left is the TP-Link logo. The main heading is "Success!" followed by the instruction "Connect to your device and continue the configuration". Below this, there are two sections for wireless networks:

- 2.4GHz Wireless**
 - SSID: SSID-1
 - Password: 12345678
- 5GHz Wireless**
 - SSID: SSID-2
 - Password: 12345678

At the bottom, there is a checked checkbox with the text "I have connected to the new wireless network." and a dark blue "Finish" button.

Ahora puedes conectar tus teléfonos, tabletas y portátiles a la nueva red WiFi. Si no puedes acceder a internet, consulta las [preguntas frecuentes](#) para solucionar el problema.

1.4 Configurar y administrar el EAP

Si utiliza el navegador web para configurar su EAP, podrá configurar opciones más avanzadas.

Funciona según tus necesidades y puedes gestionarlo cómodamente desde la página web.

En la parte superior de la página, puede hacer clic en  para cerrar sesión y hacer clic  para abrir el técnico "Sitio web de soporte".

Hay cuatro pestañas: Estado, Inalámbrico, Administración y Sistema. La siguiente tabla muestra lo que puede configurar en cada pestaña, y los siguientes capítulos tratan sobre ello.

Estos temas en detalle.

Estado	Puede consultar la información del EAP, el tráfico inalámbrico y los clientes.
Inalámbrico	Puedes configurar los parámetros inalámbricos y las funciones avanzadas, como Portal, VLAN, filtrado MAC, programador, dirección de banda, QoS y detección de puntos de acceso no autorizados.
Gestión	Puede administrar el EAP utilizando las funciones de administración, como Registros del sistema, Servidor web, Acceso de administración, Control de LED, SSH y SNMP.
Sistema	Puede configurar los parámetros del sistema, incluyendo la cuenta de inicio de sesión y la hora. Además, puede reiniciar y restablecer el EAP, realizar copias de seguridad y restaurar la configuración, y actualizar el EAP con el nuevo archivo de firmware.

2

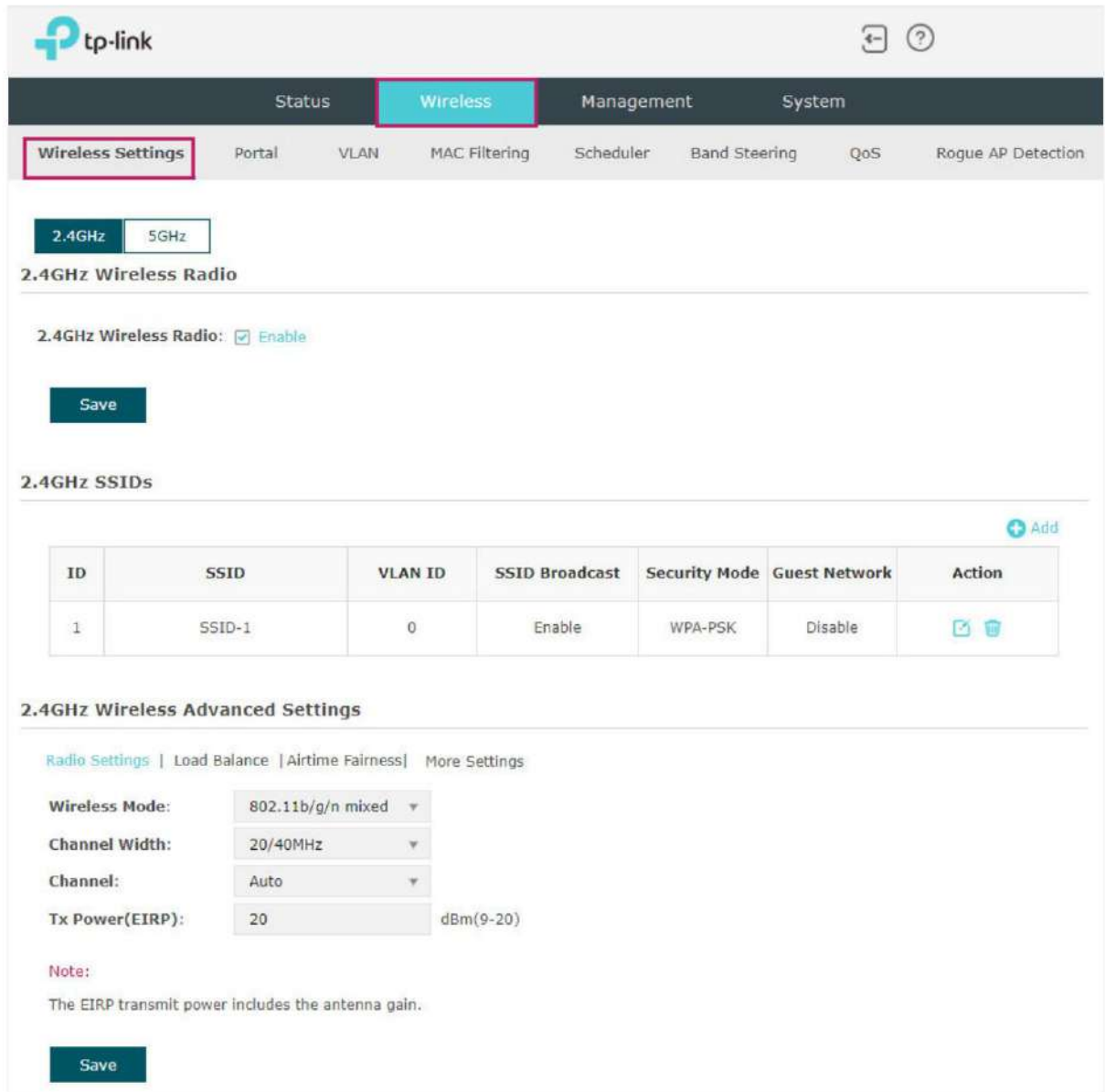
Configurar el Red

Este capítulo presenta cómo configurar los parámetros de red y las funciones avanzadas del EAP, que incluyen:

- 2.1 Configurar los parámetros inalámbricos
- 2.2 Configurar la autenticación del portal
- 2.3 Configurar VLAN
- 2.4 Configurar el filtrado MAC
- 2.5 Configurar el programador
- 2.6 Configurar la dirección
- 2.7 Configurar QoS
- 2.8 Configurar la detección de puntos de acceso no autorizados
- 2.9 Configurar modo inteligente (solo para ciertos dispositivos)

2.1 Configurar los parámetros inalámbricos

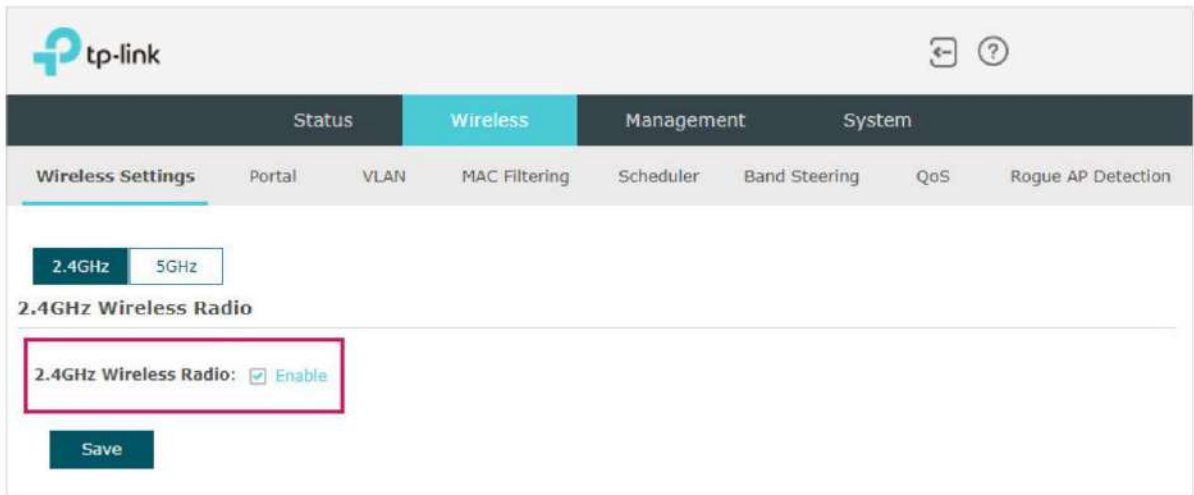
Para configurar los parámetros inalámbricos, vaya a la página Inalámbrico > Configuración inalámbrica.



The screenshot shows the TP-Link web interface with the 'Wireless' tab selected. The 'Wireless Settings' sub-tab is also highlighted. The interface is divided into three main sections:

- 2.4GHz Wireless Radio:** The '2.4GHz Wireless Radio' checkbox is checked and labeled 'Enable'. A 'Save' button is located below.
- 2.4GHz SSIDs:** A table lists the configured SSIDs. An 'Add' button is visible in the top right corner of this section.
- 2.4GHz Wireless Advanced Settings:** This section includes sub-tabs for 'Radio Settings', 'Load Balance', 'Airtime Fairness', and 'More Settings'. The 'Radio Settings' sub-tab is active, showing the following configuration:
 - Wireless Mode: 802.11b/g/n mixed
 - Channel Width: 20/40MHz
 - Channel: Auto
 - Tx Power(EIRP): 20 dBm(9-20)A 'Note' states: 'The EIRP transmit power includes the antenna gain.' A 'Save' button is located at the bottom.

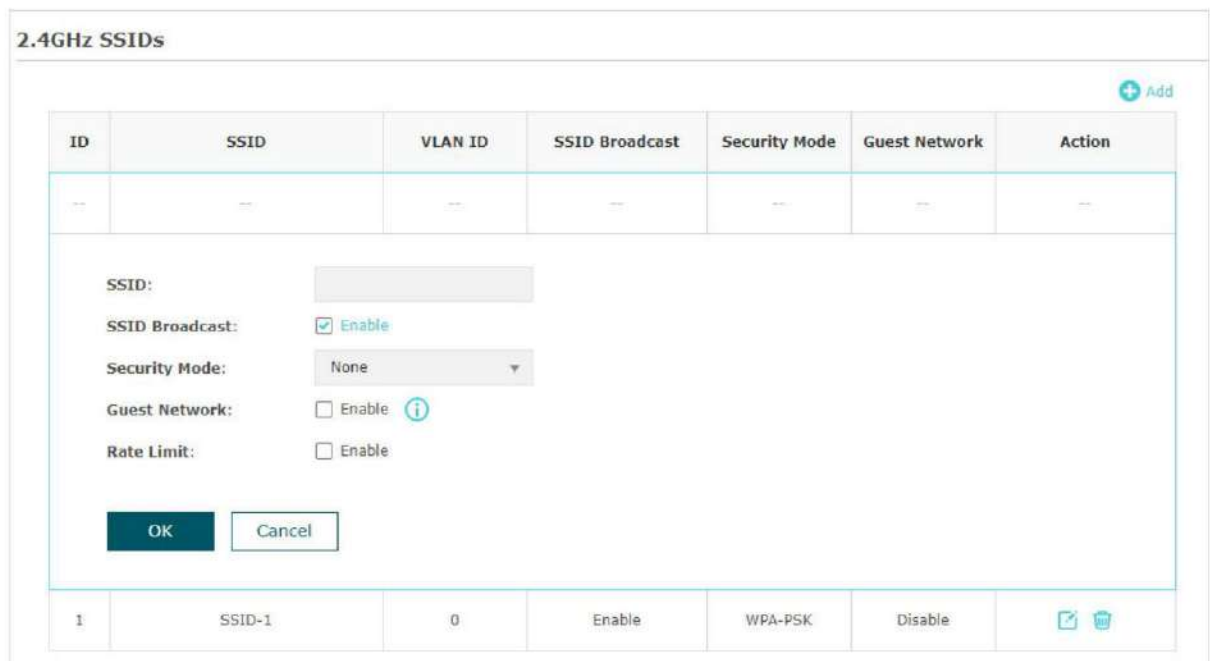
Para un EAP multibanda, puede hacer clic en cada banda para habilitar la radio inalámbrica y configurarla. parámetros inalámbricos.



Demostrado con 2,4 GHz, las siguientes secciones presentan estos contenidos: 2.1.1
 Configurar SSID y 2.1.2 Configurar ajustes avanzados inalámbricos


2.1.1 Configurar SSID

El SSID (Identificador de Conjunto de Servicios) se utiliza como identificador de una red LAN inalámbrica y se conoce comúnmente como el "nombre de la red". Los clientes pueden encontrar y acceder a la red inalámbrica mediante el SSID. Para un EAP, se pueden configurar hasta ocho SSID por banda de frecuencia.




Siga los pasos que se indican a continuación para crear un SSID en el EAP:

1. Si su EAP es un dispositivo de doble banda, haga clic en 2.4GHz 5GHz para elegir una banda de frecuencia en clic donde se creará el nuevo SSID.

2. Haga clic  **Add** para agregar un nuevo SSID en la banda elegida.

Consejos:

También puedes hacer  para editar el SSID específico que ya existe en la lista. Y puede hacer clic  clic para eliminar el SSID de la lista.

3. Configure los siguientes parámetros obligatorios para este SSID:

SSID	Especifique un nombre para la red inalámbrica.
Difusión de SSID:	Con esta opción activada, el EAP difundirá el SSID a los dispositivos cercanos para que puedan encontrar la red inalámbrica identificada por dicho SSID. Si esta opción está desactivada, los usuarios deberán introducir el SSID manualmente para conectarse al EAP.
Modo de seguridad	<p>Seleccione el modo de seguridad de la red inalámbrica. Hay cuatro opciones:</p> <p>Ninguno Los clientes pueden acceder a la red inalámbrica sin autenticación.</p> <p>WEP / WPA-Enterprise / WAP-Personal : Los clientes deben pasar la Autenticación antes de acceder a la red inalámbrica.</p> <p>Para 6 GHz:</p> <p>Mejorado Abierto Enhanced Open es una certificación de la Wi-Fi Alliance que preserva la comodidad que ofrecen las redes abiertas al tiempo que reduce algunos de los riesgos asociados con el acceso a una red no segura.</p> <p>WPA3-Enterprise / WAP3-Personal : Los clientes deben pasar la Autenticación antes de acceder a la red inalámbrica.</p> <p>Para mayor seguridad de la red, recomendamos cifrar su red inalámbrica. En las siguientes secciones se explica cómo configurar estos modos de seguridad.</p>
Red de invitados	Con esta opción habilitada, la red de invitados impedirá que los clientes accedan a cualquier subred IP privada.
Límite de tasa	<p>Con esta opción activada, la velocidad de descarga y subida de cada cliente que se conecte a la red Wi-Fi (SSID) se limitará para equilibrar el uso del ancho de banda.</p> <p>Puede limitar la velocidad de descarga y carga para algunos clientes específicos configurando el límite de velocidad en la lista de clientes; consulte Vista Cliente Información a para obtener más detalles.</p> <p>Tenga en cuenta que la velocidad de descarga y carga se limitará al valor menor si establece el valor límite tanto en la configuración del SSID como en la del cliente.</p>

4. Haga clic en **Aceptar** para crear el SSID.

A continuación se detallan las instrucciones sobre cómo configurar **WEP** , **WPA-Enterprise** , **WPA-Personal** , **WPA3-Enterprise** , y **WAP3-Personal**

• WEP (para ciertos modelos)

WEP (Wired Equivalent Privacy) es un método de cifrado tradicional. Se ha demostrado que WEP tiene fallos de seguridad y puede ser descifrado fácilmente, por lo que no puede proporcionar una protección eficaz para las redes inalámbricas. Dado que WPA-Personal y WPA-Enterprise son mucho más seguros que WEP, le recomendamos que elija WPA-Personal o WPA-Enterprise si su cliente también los apoya.

Nota:

WEP no es compatible con los modos 802.11n ni 802.11ac. Si se aplica WEP en los modos 802.11n, 802.11ac o mixto 802.11n/ac, es posible que los clientes no puedan acceder a la red inalámbrica. Si se aplica WEP en los modos 802.11b/g/n (2,4 GHz) o 802.11a/n (5 GHz), el EAP podría funcionar a una velocidad de transmisión baja.

Security Mode:	WEP
Type:	<input checked="" type="radio"/> Auto <input type="radio"/> Open System <input type="radio"/> Shared Key
Key Selected:	Key1
Wep Key Format:	<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal
Key Type:	<input checked="" type="radio"/> 64-bit <input type="radio"/> 128-bit <input type="radio"/> 152-bit
Key Value:	weppw

La siguiente tabla describe detalladamente cómo configurar cada elemento:

Tipo	Seleccione el tipo de autenticación para WEP. Automático: El EAP puede seleccionar automáticamente Sistema abierto o Clave compartida en función de la capacidad inalámbrica y la solicitud de los clientes. Sistema abierto: Los clientes pueden autenticarse y conectarse a la red inalámbrica sin contraseña. Sin embargo, se requiere la contraseña correcta para la transmisión de datos. Clave compartida: Los clientes deben introducir la contraseña correcta para autenticarse; de lo contrario, no podrán conectarse a la red inalámbrica. red o transmitir datos.
Clave seleccionada	Seleccione una tecla para especificar. Puede configurar un máximo de cuatro teclas.
Formato de clave WEP	Seleccione ASCII o Hexadecimal como formato de clave WEP. ASCII: Con este formato seleccionado, la clave WEP puede ser cualquier combinación de caracteres del teclado de la longitud especificada. Hexadecimal: Con este formato seleccionado, la clave WEP puede ser cualquier combinación de dígitos hexadecimales (0-9, af, AF) con la longitud especificada.

Tipo de clave	<p>Seleccione la longitud de la clave WEP para el cifrado.</p> <p>64 bits: Introduzca 10 dígitos hexadecimales o 5 caracteres ASCII.</p> <p>128 bits: Introduzca 26 dígitos hexadecimales o 13 caracteres ASCII.</p> <p>152 bits: Introduzca 32 dígitos hexadecimales o 16 caracteres ASCII.</p>
Valor clave	<p>Introduzca las claves WEP. La longitud y los caracteres válidos vienen determinados por el formato y el tipo de clave.</p>

• WPA-Enterprise (para ciertos modelos)

WPA-Enterprise (Wi-Fi Protected Access-Enterprise) es un método de cifrado más seguro que WEP y WPA-Personal. Requiere un servidor RADIUS para autenticar a los clientes mediante 802.1X y EAP (Extensible Authentication Protocol). WPA-Enterprise puede generar contraseñas diferentes para cada cliente, lo que garantiza una mayor seguridad de la red.

Pero también resulta más caro mantener la red, por lo que es más adecuada para redes empresariales.

The screenshot shows a configuration window for WPA-Enterprise. The 'Security Mode' dropdown is set to 'WPA-Enterprise'. The 'Version' dropdown is set to 'WPA/WPA2 - Enterpris'. Under 'Encryption', the 'Auto' radio button is selected, with 'TKIP' and 'AES' also available. The 'RADIUS Server IP' field contains '0.0.0.0' and the 'RADIUS Port' field contains '0', with a note '(1-65535. 0 means the default port, which is 1812.)'. The 'RADIUS Accounting' checkbox is checked and labeled 'Enable'. The 'Accounting Server IP' field contains '0.0.0.0' and the 'Accounting Server Port' field contains '0', with a note '(1-65535. 0 means the default port, which is 1813.)'. The 'Interim Update' checkbox is unchecked. The 'Group Key Update Period' field contains '0' with a note 'seconds (30-8640000. 0 means no update.)'. The 'Guest Network' checkbox is unchecked and has an information icon. The 'Rate Limit' checkbox is unchecked. At the bottom, there are 'OK' and 'Cancel' buttons.

La siguiente tabla muestra cómo configurar cada elemento:

Versión	<p>Seleccione la versión de WPA-Enterprise según sus necesidades. Si selecciona WPA/WPA2-Enterprise, el EAP decidirá automáticamente si usar WPA-Enterprise o WPA2-Enterprise durante la autenticación proceso.</p>
---------	---

Cifrado	<p>Seleccione el tipo de cifrado. Tenga en cuenta que algunos tipos de cifrado solo están disponibles en determinadas circunstancias.</p> <p>Automático: La configuración predeterminada es Automático y el EAP seleccionará TKIP o AES automáticamente según la solicitud del dispositivo cliente.</p> <p>TKIP: Protocolo de integridad de clave temporal. TKIP no es compatible con los modos 802.11n, 802.11ac ni con el modo mixto 802.11n/ac. Si se aplica TKIP en estos modos, los clientes podrían no tener acceso a la red inalámbrica. Si se aplica TKIP en los modos 11b/g/n (2,4 GHz) o 11a/n (5 GHz), el dispositivo podría funcionar a una velocidad de transmisión baja.</p> <p>AES: Estándar de cifrado avanzado. Es más seguro que TKIP.</p>
Dirección IP del servidor RADIUS	Introduzca la dirección IP del servidor RADIUS.
Puerto RADIUS	Introduzca el número de puerto del servidor RADIUS.
Contraseña RADIUS	Introduzca la clave secreta compartida del servidor RADIUS.
Contabilidad RADIUS	Habilitar o deshabilitar la función de contabilidad RADIUS.
Dirección IP del servidor de contabilidad	Introduzca la dirección IP del servidor de contabilidad.
Servidor de contabilidad Puerto	Introduzca el número de puerto del servidor de contabilidad.
Servidor de contabilidad Contraseña	Introduzca la clave secreta compartida del servidor de contabilidad.
Actualización provisional	<p>Con esta opción activada, puede especificar el intervalo entre las actualizaciones de la información contable. Por defecto, la función está desactivada.</p> <p>Introduzca la duración adecuada entre actualizaciones para los EAP en Intervalo de actualización intermedio.</p>
Actualización provisional Intervalo	Con la opción de Actualización Interina habilitada, especifique la duración adecuada entre actualizaciones para las EAP. La duración predeterminada es de 600 segundos.
Actualización de clave de grupo Período	Especifique un período de actualización para la clave de cifrado. El período de actualización indica con qué frecuencia el EAP debe cambiar la clave de cifrado. Un valor de 0 significa que la clave de cifrado no cambia en ningún momento.

- WPA-Personal (para ciertos modelos)

WPA-Personal se basa en una clave precompartida. Se caracteriza por su alta seguridad y configuración sencilla, por lo que es utilizado principalmente por hogares y pequeñas empresas.

The screenshot shows a configuration window for WPA-Personal. The fields are as follows:

- Security Mode:** WPA-Personal (dropdown)
- Version:** WPA/WPA2-PSK (dropdown)
- Encryption:** Auto (selected), TKIP, AES (radio buttons)
- Wireless Password:** 12345678 (text input)
- Group Key Update Period:** 0 (text input) seconds (30-8640000. 0 means no update.)
- Guest Network:** Enable (checkbox with info icon)
- Rate Limit:** Enable (checkbox)

Buttons: OK, Cancel

La siguiente tabla muestra cómo configurar cada elemento:

Versión	Seleccione la versión de WPA-Personal que mejor se adapte a sus necesidades. Si selecciona WPA/WPA2-PSK, el EAP decidirá automáticamente si utilizar WPA-PSK o WPA2-PSK durante el proceso de autenticación.
Cifrado	<p>Seleccione el tipo de cifrado. Tenga en cuenta que algunos tipos de cifrado solo están disponibles en determinadas circunstancias.</p> <p>Automático: La configuración predeterminada es Automático y el EAP seleccionará TKIP o AES automáticamente según la solicitud del dispositivo cliente.</p> <p>TKIP: Protocolo de integridad de clave temporal. TKIP no es compatible con los modos 802.11n, 802.11ac ni con el modo mixto 802.11n/ac. Si se aplica TKIP en estos modos, los clientes podrían no tener acceso a la red inalámbrica. Si se aplica TKIP en los modos 11b/g/n (2,4 GHz) o 11a/n (5 GHz), el dispositivo podría funcionar a una velocidad de transmisión baja.</p> <p>AES: Estándar de cifrado avanzado. Es más seguro que TKIP.</p>
Inalámbrico Contraseña	<p>Configure la contraseña inalámbrica con caracteres ASCII.</p> <ul style="list-style-type: none"> • Para ASCII, la longitud debe estar entre 8 y 63 caracteres, y los caracteres válidos incluyen números, letras (distinguiendo mayúsculas y minúsculas) y signos de puntuación comunes.
Clave de grupo Período de actualización	Especifique un período de actualización para la clave de cifrado. El período de actualización indica con qué frecuencia el EAP debe cambiar la clave de cifrado. Un valor de 0 significa que la clave de cifrado no cambia en ningún momento.

- WPA3-Enterprise (para ciertos modelos)

WPA3-Enterprise es un método de cifrado más seguro en comparación con WPA3-Personal. Requiere un servidor RADIUS para autenticar a los clientes a través de 802.1X y AP (Autenticación Extensible)

Protocolo). WPA3-Enterprise puede generar diferentes contraseñas para diferentes clientes, lo que garantiza una mayor seguridad de la red. Pero también cuesta más mantener la red, por lo que es más adecuado para redes empresariales.

Security Mode:	WPA3-Enterprise ▼
Encryption:	<input checked="" type="radio"/> AES-GCM 256 <input type="radio"/> AES-CNSA
RADIUS Server IP:	0.0.0.0
RADIUS Port:	0 (1-65535. 0 means the default port, which is 1812.)
RADIUS Password:	
RADIUS Accounting:	<input type="checkbox"/> Enable
Group Key Update Period:	0 seconds (30-8640000. 0 means no update.)

La siguiente tabla muestra cómo configurar cada elemento:

Cifrado	Seleccione el tipo de cifrado: AES-GCM 256 o AES-CNSA.
Dirección IP del servidor RADIUS	Introduzca la dirección IP del servidor RADIUS.
Puerto RADIUS	Introduzca el número de puerto del servidor RADIUS.
Contraseña RADIUS	Introduzca la clave secreta compartida del servidor RADIUS.
Contabilidad RADIUS	Habilitar o deshabilitar la función de contabilidad RADIUS.
Dirección IP del servidor de contabilidad	Introduzca la dirección IP del servidor de contabilidad.
Servidor de contabilidad Puerto	Introduzca el número de puerto del servidor de contabilidad.
Servidor de contabilidad Contraseña	Introduzca la clave secreta compartida del servidor de contabilidad.
Actualización provisional	Con esta opción activada, puede especificar el intervalo entre las actualizaciones de la información contable. Por defecto, la función está desactivada. Introduzca la duración adecuada entre actualizaciones para los AP en Intervalo de actualización intermedio.
Actualización provisional Intervalo	Con la función de actualización intermedia habilitada, especifique la duración adecuada entre actualizaciones para los puntos de acceso. La duración predeterminada es de 600 segundos.
Actualización de clave de grupo Período	Especifique un período de actualización para la clave de cifrado. El período de actualización indica con qué frecuencia el punto de acceso debe cambiar la clave de cifrado. Un valor de 0 significa que la clave de cifrado no cambia en ningún momento.

- WPA3-Personal (para ciertos modelos)

WPA-Personal se basa en una clave precompartida. Se caracteriza por su alta seguridad y configuración sencilla, por lo que es utilizado principalmente por hogares y pequeñas empresas.

Security Mode:	WPA3-Personal	▼
Wireless Password:	wpapass1	
Group Key Update Period:	0	seconds (30-8640000. 0 means no update.)

La siguiente tabla muestra cómo configurar cada elemento:

Inalámbrico Contraseña	Configure la contraseña inalámbrica con caracteres ASCII. • Para ASCII, la longitud debe estar entre 8 y 63 caracteres, y los caracteres válidos incluyen números, letras (distinguiendo mayúsculas y minúsculas) y signos de puntuación comunes.
Clave de grupo Período de actualización	Especifique un período de actualización para la clave de cifrado. El período de actualización indica con qué frecuencia el punto de acceso debe cambiar la clave de cifrado. Un valor de 0 significa que la clave de cifrado no cambia en ningún momento.

2.1.2 Configurar ajustes avanzados inalámbricos

Unos parámetros inalámbricos adecuados pueden mejorar el rendimiento de su red inalámbrica.

Esta sección presenta cómo configurar los parámetros inalámbricos avanzados del EAP, incluido [Radio Configuración](#), [Carga Balance](#), [Tiempo en antena Justicia](#) y [Más Ajustes](#).

Configuración de radio

La configuración de la radio controla directamente el comportamiento de la radio en el EAP y su interacción con el medio físico; es decir, cómo y qué tipo de señal emite el EAP.

Nota: Para los Sub-AP, el Modo inalámbrico, el Ancho de canal y el Canal seguirán la configuración de su AP principal y no se puede editar.

2.4GHz Wireless Advanced Settings

[Radio Settings](#) | [Load Balance](#) | [Airtime Fairness](#) | [More Settings](#)

Wireless Mode:	802.11b/g/n mixed	▼
Channel Width:	20/40MHz	▼
Channel:	Auto	▼
Tx Power(EIRP):	20	dBm(5-20)

Note:
The EIRP transmit power includes the antenna gain.

[Save](#)

Seleccione la banda de frecuencia y configure los siguientes parámetros.

Modo inalámbrico Seleccione el modo IEEE 802.11 que utiliza la radio.

- Para 2,4 GHz:

Se recomienda la configuración mixta de 802.11b/g/n/ax/be para que todos los clientes 802.11b, 802.11g, 802.11n, 802.11ax y 802.11be que operan en la frecuencia de 2.4 GHz puedan conectarse al punto de acceso. Tenga en cuenta que algunos dispositivos podrían no ser compatibles con 802.11ax y 802.11be; en ese caso, seleccione el que tenga la mayor cantidad de tipos combinados.

- Para 5 GHz:

Se recomienda la configuración mixta 802.11a/n/ac/ax/be para que todos los clientes 802.11a, 802.11n, 802.11ac, 802.11ax y 802.11be que operen en la frecuencia de 5 GHz puedan conectarse al punto de acceso. Tenga en cuenta que algunos dispositivos podrían no ser compatibles con 802.11ax y 802.11be; en ese caso, seleccione el que tenga la mayor cantidad de tipos combinados.

- Para 6 GHz:

Se recomienda la configuración mixta 802.11ax/be para que todos los clientes 802.11ax y 802.11be que operen en la frecuencia de 6 GHz puedan conectarse al punto de acceso. Tenga en cuenta que los dispositivos Wi-Fi 6E solo son compatibles con 802.11ax.

Ancho del canal

Seleccione el ancho de canal del punto de acceso. Las opciones disponibles varían según el modelo de punto de acceso.

Le recomendamos configurar el ancho de banda del canal en Automático para mejorar la velocidad de transmisión. Sin embargo, puede optar por un ancho de banda menor por los siguientes motivos:

- Para aumentar el número de canales disponibles dentro del total limitado ancho de banda.
 - Para evitar interferencias de canales superpuestos ocupados por otros dispositivos en el entorno.
 - Un menor ancho de banda puede concentrar una mayor potencia de transmisión, aumentando Estabilidad de los enlaces inalámbricos a largas distancias.
-

Límite de canales

Marque la casilla para habilitar la función Límite de canal. Con esta función

Si se habilita, la frecuencia inalámbrica de 5150 MHz a 5350 MHz se desactivará. Esta función puede influir en las opciones disponibles en Canal.

Esta función solo está disponible en determinados dispositivos. Para comprobar si su dispositivo es compatible con esta función, consulte la interfaz web.

Canal

Seleccione el canal utilizado por el EAP. Por ejemplo, 1/2412MHz significa que el canal es 1 y la frecuencia es 2412MHz.

Por defecto, el canal se selecciona automáticamente, y le recomendamos que mantenga la configuración predeterminada.

Potencia de transmisión (PIRE)

Especifique el valor de la potencia de transmisión.

Si este valor se establece en un valor superior a la potencia de transmisión máxima permitida por la normativa local, se aplicará la potencia de transmisión máxima regulada en la situación real.

Nota: En la mayoría de los casos, no es necesario utilizar la máxima potencia de transmisión.

Especificar una potencia de transmisión mayor de la necesaria puede causar interferencias en el vecindario.

Además, consume más energía y reduce la vida útil del dispositivo.

Balance de carga

Con la función de balanceo de carga, puede limitar el número máximo de clientes que pueden acceder al EAP. De esta forma, se logra un uso racional de los recursos de la red.



2.4GHz Wireless Advanced Settings


Radio Settings | **Load Balance** | Airtime Fairness | More Settings

Load Balance: Enable

Maximum Associated Clients: 0 (1-99)

Save

Siga los pasos que se indican a continuación para configurar el balanceo de carga:

1. Haga clic  para elegir una banda de frecuencia en la que se aplicará la función de equilibrio de carga. tener un efecto.
2. Marque la casilla para habilitar el equilibrio de carga.
3. Especifique el número máximo de clientes que pueden conectarse al EAP al mismo tiempo.
Mientras que el número de clientes conectados ha alcanzado el límite y hay más clientes
Al solicitar acceso a la red, el EAP desconectará a aquellos usuarios con señales más débiles.
4. Haga clic en Guardar.

Equidad en el tiempo de emisión

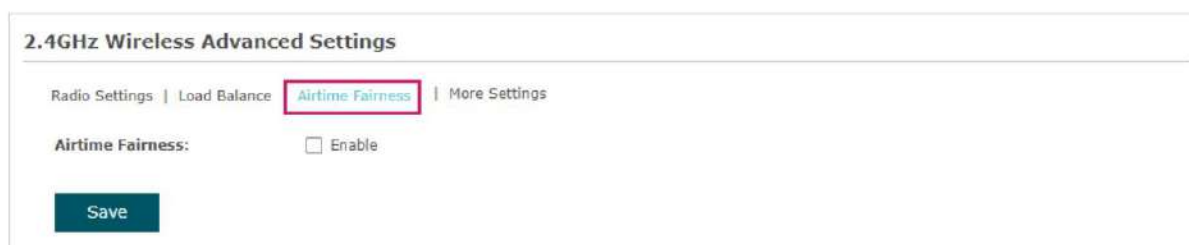
Nota:

La función Airtime Fairness solo está disponible en ciertos dispositivos. Para comprobar si tu dispositivo es compatible con esta función, consulta la interfaz web.

Con Airtime Fairness habilitado, cada cliente conectado al EAP puede obtener la misma cantidad de tiempo para transmitir datos, evitando que los clientes con baja velocidad de datos ocupen demasiado espacio en la red.
ancho de banda.

En comparación con los dispositivos cliente relativamente nuevos, algunos dispositivos cliente heredados admiten Menor velocidad de conexión inalámbrica. Si se comunican con el mismo punto de acceso (EAP), los clientes con menor velocidad de conexión tardan más en transmitir y recibir datos que los clientes con mayor velocidad. Como resultado, el rendimiento general de la red inalámbrica disminuye.

Por lo tanto, le recomendamos marcar la casilla para habilitar esta función en redes inalámbricas multivelocidad. De esta manera, los clientes más rápidos dispondrán de más tiempo para la transmisión de datos y se mejorará el rendimiento general de la red.

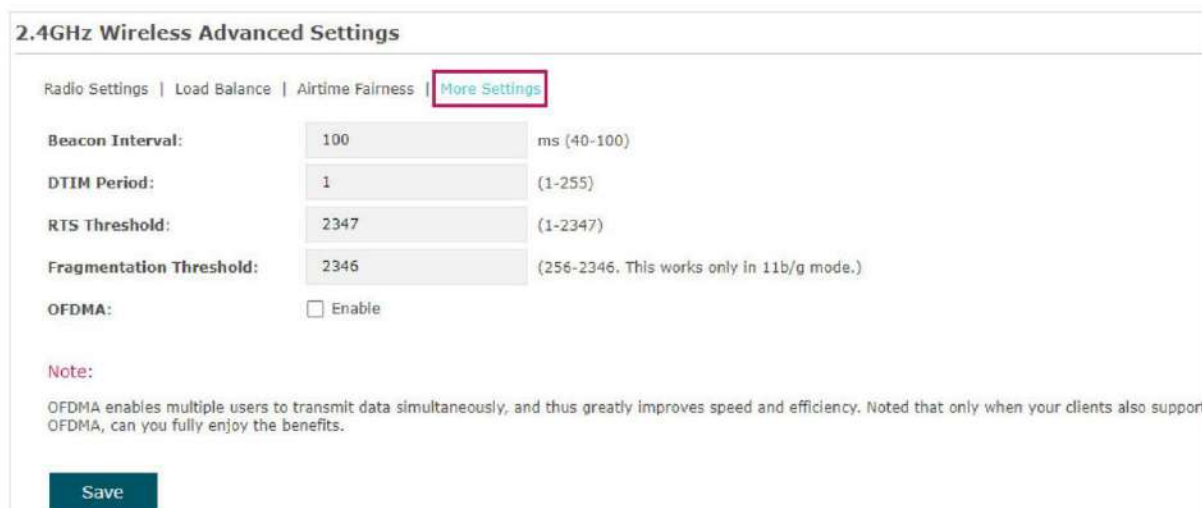


Nota:

Con la función Airtime Fairness activada, un máximo de 50 clientes inalámbricos pueden conectarse al EAP en la banda de 2,4 GHz.

Más configuraciones

Unos parámetros inalámbricos adecuados pueden mejorar la estabilidad, la fiabilidad y la eficiencia de la comunicación de la red.



La siguiente tabla muestra cómo configurar cada elemento:

Intervalo de baliza	El EAP transmite balizas periódicamente para anunciar la presencia de una red inalámbrica a los clientes. El intervalo de balizas determina el intervalo de tiempo entre las balizas enviadas por el EAP. Puedes especificar un valor entre 40 y 100 ms. El valor predeterminado es 100 ms.
-------------------------------------	--

Período DTIM	<p>El DTIM (Mensaje de Indicación de Tráfico de Entrega) está contenido en algunas tramas Beacon. Indica si el EAP ha almacenado datos en búfer para el cliente.</p> <p>dispositivos. El período DTIM indica con qué frecuencia los clientes atendidos por este EAP deben comprobar si hay datos almacenados en búfer en el EAP pendientes de recogida.</p> <p>Puede especificar un valor entre 1 y 255 intervalos de baliza. El valor predeterminado es 1, lo que indica que los clientes comprueban si hay datos almacenados en búfer en cada baliza. Un intervalo DTIM excesivo puede reducir el rendimiento de las aplicaciones de multidifusión, por lo que recomendamos mantener el valor predeterminado.</p>
Umbral RTS	<p>El sistema RTS/CTS (Solicitud de envío/Autorización de envío) se utiliza para mejorar la eficiencia de la transmisión de datos en redes con nodos ocultos, especialmente cuando hay muchos paquetes grandes que transmitir.</p> <p>Cuando el tamaño de un paquete de datos es mayor que el umbral RTS, el RTS/CTS se activará el mecanismo CTS. Con este mecanismo activado, antes de enviar un paquete de datos, el cliente enviará un paquete RTS al EAP para solicitar la transmisión de datos. Posteriormente, el EAP enviará un paquete CTS para informar a los demás clientes que retrasen la transmisión de sus datos. De esta forma, se evitan las colisiones de paquetes.</p> <p>En una red con mucho tráfico y nodos ocultos, un umbral bajo ayuda a reducir las interferencias y las colisiones de paquetes. Sin embargo, en una red con poco tráfico, un umbral demasiado bajo provoca un desperdicio de ancho de banda y reduce el rendimiento de datos. El valor recomendado y predeterminado es de 2347 bytes.</p>
Fragmentación Límite	<p>La función de fragmentación permite limitar el tamaño de los paquetes transmitidos por la red. Si el tamaño de un paquete supera el umbral de fragmentación, se activa dicha función y el paquete se divide en varios subpaquetes.</p> <p>La fragmentación ayuda a mejorar el rendimiento de la red si se configura correctamente. Sin embargo, un umbral de fragmentación demasiado bajo puede provocar un rendimiento deficiente de la conexión inalámbrica debido al trabajo adicional que supone dividir y reensamblar las tramas, así como al aumento del tráfico de mensajes. El valor recomendado y predeterminado es de 2346 bytes.</p>
OFDMA	<p>OFDMA permite que varios usuarios transmitan datos simultáneamente, lo que mejora considerablemente la velocidad y la eficiencia. Solo si sus clientes también son compatibles con OFDMA, podrá disfrutar plenamente de sus ventajas.</p> <p>Esta función solo está disponible en determinados dispositivos. Para comprobar si su dispositivo es compatible con esta función, consulte la interfaz web.</p>
No PSC Canal	<p>Los canales de escaneo preferidos (PSC, por sus siglas en inglés) son canales priorizados dentro de la banda Wi-Fi de 6 GHz para una conectividad eficiente. Algunos clientes podrían no detectar redes de 6 GHz utilizando canales que no sean PSC.</p> <p>Esta función solo está disponible en determinados dispositivos. Para comprobar si su dispositivo es compatible con esta función, consulte la interfaz web.</p>

2.1.3 Configurar la red MLO (solo para dispositivos Wi-Fi 7)

MLO (Multi-Link Operation) permite que los dispositivos Wi-Fi 7 envíen y reciban simultáneamente datos en diferentes bandas y canales. Esto garantiza conexiones rápidas y fiables incluso en entornos de red densa.

Para configurar una red MLO, vaya a Inalámbrico > Configuración inalámbrica > MLO y haga clic en Agregar.

MLO SSIDs

ID	SSID	Band	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
...

SSID:

Band: 2.4GHz 5GHz 6GHz ⓘ

SSID Broadcast: Enable

Security Mode: WPA-Personal ▾

Version: WPA/WPA2-PSK ▾

Encryption: Auto AES

Wireless Password:

Group Key Update Period: seconds (30-8640000. 0 means no update.)

Guest Network: Enable ⓘ

Rate Limit: Enable

OK **Cancel**

Configure los parámetros y guarde la configuración.

SSID	Especifique un nombre para la red MLO.
Banda	Seleccione las bandas para formar la red MLO. Las opciones de bandas disponibles pueden variar según el modelo.
Difusión de SSID:	Con esta opción habilitada, el punto de acceso (AP) difundirá el SSID a los hosts cercanos, de modo que estos puedan encontrar la red inalámbrica identificada por dicho SSID. Si esta opción está desactivada, los usuarios deberán introducir el SSID manualmente para conectarse al punto de acceso.
Modo de seguridad/ Versión/ Cifrado	Configure los ajustes de seguridad de la red inalámbrica. Para obtener instrucciones detalladas, consulte 2.1.1 Configurar SSID .
Red de invitados	Con esta opción habilitada, la red de invitados impedirá que los clientes accedan a cualquier subred IP privada.

Límite de tasa

Con esta opción activada, la velocidad de descarga y subida de cada cliente que se conecte a la red Wi-Fi (SSID) se limitará para equilibrar el uso del ancho de banda.

Puede limitar la velocidad de descarga y carga para algunos clientes específicos configurando el límite de velocidad en la lista de clientes; consulte [Vista Cliente Información](#) ^a para obtener más detalles.

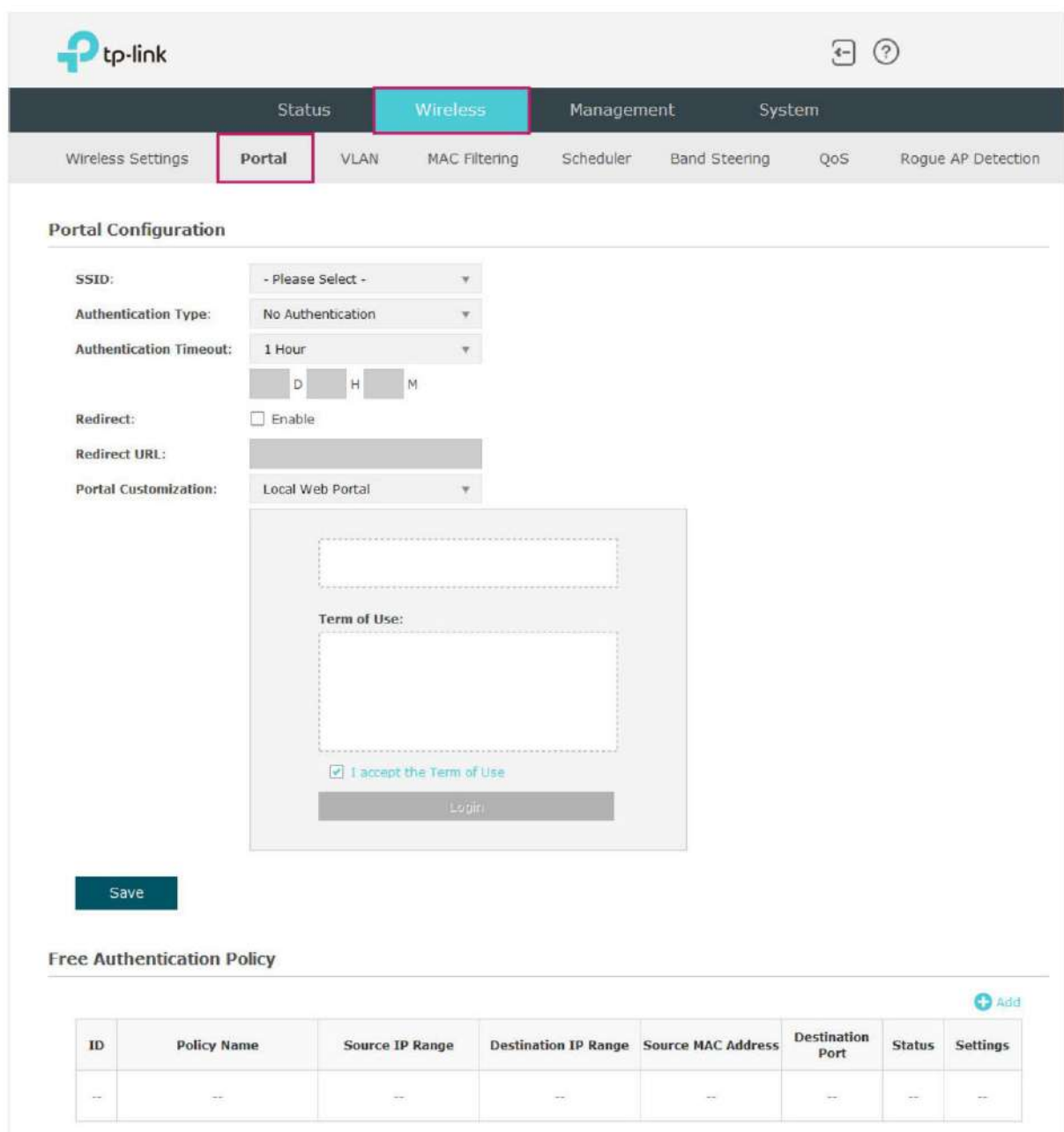
Tenga en cuenta que la velocidad de descarga y carga se limitará al valor menor si establece el valor límite tanto en la configuración del SSID como en la del cliente.

2.2 Configurar la autenticación del portal

La autenticación del portal proporciona un servicio de autenticación a los clientes que solo necesitan acceso temporal a la red inalámbrica, como los clientes de un restaurante o un supermercado. Para acceder a la red, estos clientes deben ingresar a la página de inicio de sesión de autenticación y usar la información de inicio de sesión correcta para completar la autenticación. Además, puede personalizar la página de inicio de sesión de autenticación y especificar una URL a la que los clientes autenticados puedan acceder. será redirigido a.

En este módulo, también puede configurar la Política de Autenticación Libre, que permite a los clientes específicos acceder a los recursos de red específicos sin autenticación.

Para configurar la autenticación del portal, vaya a la página Inalámbrico > Portal.



Portal Configuration

SSID: - Please Select -

Authentication Type: No Authentication

Authentication Timeout: 1 Hour

Redirect: Enable

Redirect URL:

Portal Customization: Local Web Portal

Term of Use:

I accept the Term of Use

Login

Save

Free Authentication Policy

ID	Policy Name	Source IP Range	Destination IP Range	Source MAC Address	Destination Port	Status	Settings
--	--	--	--	--	--	--	--

Configurar portal

Existen tres tipos de autenticación de portal disponibles: **No Autenticación** , **Local Contraseña** y **Externo RADIO Servidor**. Las siguientes secciones presentan cómo configurar cada una tipo de autenticación.

• Sin autenticación

Con este tipo de autenticación configurado, los clientes pueden pasar la autenticación y acceder a la red sin proporcionar ninguna información de inicio de sesión. Solo necesitan aceptar el término de usar en la página de autenticación.

The screenshot displays the 'Portal Configuration' settings. The 'Authentication Type' is set to 'No Authentication'. The 'Authentication Timeout' is set to '1 Hour'. The 'Redirect' option is disabled. The 'Portal Customization' is set to 'Local Web Portal'. A preview of the login page is shown, featuring a 'Term of Use' section with a checkbox for 'I accept the Term of Use' and a 'Login' button.

SSID:	- Please Select -
Authentication Type:	No Authentication
Authentication Timeout:	1 Hour
Redirect:	<input type="checkbox"/> Enable
Redirect URL:	
Portal Customization:	Local Web Portal

Term of Use:

I accept the Term of Use

Login

Save

Siga los pasos que se indican a continuación para configurar "Sin autenticación" como tipo de autenticación del portal:

1. Seleccione el SSID en el que el portal tendrá efecto.
2. Seleccione Sin autenticación como tipo de autenticación.
3. Configure los parámetros correspondientes como se muestra en la siguiente tabla:

Autenticación <small>Se acabó el tiempo</small>	<p>Especifique el valor del tiempo de espera de autenticación.</p> <p>La autenticación de un cliente caducará tras el tiempo de espera de autenticación y el cliente deberá iniciar sesión de nuevo en la página de autenticación para acceder a la red.</p> <p>Las opciones disponibles son: 1 hora, 8 horas, 24 horas, 7 días y Personalizado. Al seleccionar Personalizado, puede configurar el tiempo en días, horas y minutos.</p>
Redireccionar	<p>Una vez configurada esta función, el cliente recién autenticado será redirigido a la URL especificada.</p>
<small>URL de redireccionamiento</small>	<p>Con la redirección habilitada, también debe ingresar la URL en este campo. El cliente recién autenticado será redirigido a esta URL.</p>
Portal Personalización	<p>Configure la página de autenticación. El portal web local es la única opción disponible para este tipo de autenticación. Introduzca el título y el plazo de uso en las dos casillas.</p> <p>El EAP utiliza su servidor web integrado para proporcionar esta página de autenticación a los clientes. Para autenticarse, los clientes solo tienen que marcar la casilla "Acepto los Términos de uso" y hacer clic en el botón "Iniciar sesión".</p>

4. Haga clic en Guardar.

• Contraseña local

Con este tipo de autenticación configurado, los clientes deben proporcionar la información correcta. contraseña para pasar la autenticación.

The screenshot displays the 'Portal Configuration' interface. It includes the following fields and options:

- SSID:** A dropdown menu currently set to '- Please Select -'.
- Authentication Type:** A dropdown menu set to 'Local Password'.
- Password:** An empty text input field.
- Authentication Timeout:** A dropdown menu set to '1 Hour', with sub-fields for 'D' (Days), 'H' (Hours), and 'M' (Minutes).
- Redirect:** A checkbox labeled 'Enable' which is currently unchecked.
- Redirect URL:** An empty text input field.
- Portal Customization:** A dropdown menu set to 'Local Web Portal'.

Below these settings is a preview of the web portal login page. The preview shows a dashed box for a header, a 'Password:' label next to a password input field, a 'Term of Use:' label next to a larger text area, a checked checkbox labeled 'I accept the Term of Use', and a 'Login' button.

A 'Save' button is located at the bottom left of the configuration panel.

Siga los pasos que se indican a continuación para configurar la contraseña local como tipo de autenticación del portal:

1. Seleccione el SSID en el que el portal tendrá efecto.
2. Seleccione Contraseña local como tipo de autenticación.
3. Configure los parámetros correspondientes como se muestra en la siguiente tabla:

Contraseña	Especifique una contraseña para la autenticación.
------------	---

Autenticación <small>Se acabó el tiempo</small>	<p>Especifique el valor del tiempo de espera de autenticación.</p> <p>La autenticación de un cliente caducará tras el tiempo de espera de autenticación y el cliente deberá iniciar sesión de nuevo en la página de autenticación para acceder a la red.</p> <p>Las opciones disponibles son: 1 hora, 8 horas, 24 horas, 7 días y Personalizado. Al seleccionar Personalizado, puede configurar el tiempo en días, horas y minutos.</p>
Redireccionar	<p>Una vez configurada esta función, el cliente recién autenticado será redirigido a la URL especificada.</p>
URL de redireccionamiento	<p>Con la redirección habilitada, también debe ingresar la URL en este campo. El cliente recién autenticado será redirigido a esta URL.</p>
Portal Personalización	<p>Configure la página de autenticación. El portal web local es la única opción disponible para este tipo de autenticación. Introduzca el título y el plazo de uso en las dos casillas.</p> <p>El EAP utiliza su servidor web integrado para proporcionar esta página de autenticación a los clientes. Para completar la autenticación, los clientes deben proporcionar la contraseña correcta en el campo Contraseña y marcar la casilla Acepto los Términos de uso.</p> <p>y haga clic en el botón Iniciar sesión.</p>

4. Haga clic en Guardar.

- Servidor RADIUS externo

Si tiene un servidor RADIUS en la red para autenticar a los clientes, puede seleccionar Servidor Radius externo. Los clientes deben proporcionar la información de inicio de sesión correcta para pasar el servidor. autenticación.

Portal Configuration

SSID:	<input type="text" value="- Please Select -"/>
Authentication Type:	<input type="text" value="External Radius Server"/>
RADIUS Server IP:	<input type="text"/>
RADIUS Port:	<input type="text" value="1812"/> (1-65535)
RADIUS Password:	<input type="text"/>
NAS ID:	<input type="text"/>
RADIUS Accounting:	<input checked="" type="checkbox"/> Enable
Accounting Server IP:	<input type="text"/>
Accounting Server Port:	<input type="text" value="1813"/> (1-65535)
Accounting Server Password:	<input type="text"/>
Interim Update:	<input type="checkbox"/> Enable
Interim Interval:	<input type="text" value="600"/> seconds (60-86400)
Authentication Timeout:	<input type="text" value="1 Hour"/>
	<input type="text"/> D <input type="text"/> H <input type="text"/> M
Redirect:	<input type="checkbox"/> Enable
Redirect URL:	<input type="text"/>
Portal Customization:	<input type="text" value="Local Web Portal"/>

Username:

Password:

Term of Use:

I accept the Term of Use

Login

Save

Siga los pasos a continuación para configurar el servidor Radius externo como autenticación del portal.

tipo:

1. Seleccione el SSID en el que el portal tendrá efecto.
2. Configure un servidor RADIUS en la red y asegúrese de que el EAP pueda acceder a él.
3. Vaya a la página de configuración del portal en el EAP. Seleccione Servidor Radius externo como tipo de autenticación.
3. Configure los parámetros correspondientes como se muestra en la siguiente tabla:

Dirección IP del servidor RADIUS	Introduzca la dirección IP del servidor RADIUS.
Puerto RADIUS	Introduzca el puerto del servidor RADIUS.
Contraseña RADIUS	Introduzca la contraseña del servidor RADIUS.
ID de NAS	Configure un identificador de servidor de acceso a la red (NAS ID) de 1 a 64 caracteres en el portal. El EAP envía el NAS ID al servidor RADIUS mediante un paquete de solicitud de autenticación. Con el NAS ID, que clasifica a los usuarios en diferentes grupos, el servidor RADIUS puede enviar una respuesta de autenticación personalizada.
Contabilidad RADIUS	Habilitar o deshabilitar la función de contabilidad RADIUS.
Dirección IP del servidor de contabilidad	Introduzca la dirección IP del servidor de contabilidad.
Puerto del servidor de contabilidad	Introduzca el número de puerto del servidor de contabilidad.
Servidor de contabilidad Contraseña	Introduzca la clave secreta compartida del servidor de contabilidad.
Actualización provisional	Con esta opción activada, puede especificar el intervalo entre las actualizaciones de la información contable. Por defecto, la función está desactivada. Introduzca la duración adecuada entre actualizaciones para los EAP en Intervalo de actualización intermedio.
Intervalo provisional	Con la opción de Actualización Interina habilitada, especifique la duración adecuada entre actualizaciones para las EAP. La duración predeterminada es de 600 segundos.
Tiempo de espera de autenticación	Especifique el valor del tiempo de espera de autenticación. La autenticación de un cliente caducará tras el tiempo de espera de autenticación y el cliente deberá iniciar sesión de nuevo en la página de autenticación para acceder a la red. Las opciones incluyen 1 hora, 8 horas, 24 horas, 7 días y opciones personalizadas. Con la opción Personalizado seleccionada, puede personalizar el tiempo en días, horas y minutos.

Redireccionar	Una vez configurada esta función, el cliente recién autenticado será redirigido a la URL especificada.
URL de redireccionamiento	Con la redirección habilitada, también debe ingresar la URL en este campo. El cliente recién autenticado será redirigido a esta URL.
Personalización del portal	<p>Configure la página de autenticación. Hay dos opciones: Portal web local y Portal web externo.</p> <ul style="list-style-type: none"> • Portal web local <p>Introduzca el título y el plazo de uso en las dos casillas. El EAP utiliza su servidor web integrado para proporcionar esta página de autenticación a los clientes. Para completar la autenticación, los clientes deben proporcionar el nombre de usuario y la contraseña correctos en los campos "Nombre de usuario" y "Contraseña", marcar la casilla "Acepto los Términos de uso" y hacer clic en el botón "Iniciar sesión".</p> • Portal web externo <p>Una vez configurado el portal web externo, la página de autenticación será proporcionada por el servidor del portal web construido en la red. Para configurar el portal web externo, debe completar las siguientes configuraciones:</p> <ol style="list-style-type: none"> 1. Cree un servidor de portal web externo en su red y haga Asegúrese de que sea accesible mediante el EAP. 2. En esta página de configuración, introduzca la URL de autenticación. <p>Página proporcionada por el servidor del portal externo.</p> <div data-bbox="683 1220 1385 1332"> <p>Portal Customization: External Web Portal ▼</p> <p>External Web Portal URL: <input style="width: 100%; height: 20px;" type="text"/></p> </div> 3. Agregue el servidor del portal web externo a la lista de Política de autenticación gratuita. De esta manera, los clientes pueden acceder al servidor del portal web antes de autenticarse. Para obtener más información sobre cómo configurar la Política de autenticación gratuita, consulte Configurar Política de autenticación gratuita.

4. Haga clic en Guardar.


Configurar la política de autenticación gratuita

La política de autenticación libre permite que algunos clientes específicos accedan a recursos de red específicos sin autenticación. Por ejemplo, puede configurar una política de autenticación libre para permitir que los clientes visiten el servidor del portal web externo antes de autenticarse. De esta manera,

Los clientes pueden acceder a la página de inicio de sesión proporcionada por el servidor del portal web y, a continuación, completar el proceso de autenticación.

Free Authentication Policy							
ID	Policy Name	Source IP Range	Destination IP Range	Source MAC Address	Destination Port	Status	Settings
--	--	--	--	--	--	--	--

Siga los pasos que se indican a continuación para agregar una política de autenticación gratuita.

1. En la sección Política de autenticación gratuita, haga clic en  para cargar la siguiente página.

ID	Policy Name	Source IP Range	Destination IP Range	Source MAC Address	Destination Port	Status	Settings
--	--	--	--	--	--	--	--

Policy Name:

Source IP Range: / (Optional)

Destination IP Range: / (Optional)

Source MAC Address: (Optional)

Destination Port: (Optional)

Status: Enable

2. Configure los siguientes parámetros. Cuando se cumplan todas las condiciones configuradas, El cliente puede acceder a la red sin autenticación.

Nombre de la póliza	Especifique un nombre para la política.
Rango de IP de origen	Especifique un rango de IP con la longitud de la máscara y la subred. Los clientes en este rango de direcciones IP pueden acceder a la red sin autenticación. Si se deja el campo vacío, los clientes con cualquier dirección IP podrán acceder a los recursos específicos.
Dirección IP de destino Rango	Especifique un rango de direcciones IP con la subred y la longitud de la máscara. Los dispositivos dentro de este rango de direcciones IP pueden ser accedidos por los clientes sin autenticación. Si se deja el campo vacío, significa que los clientes específicos podrán acceder a todos los dispositivos de la LAN.
Fuente MAC DIRECCIÓN	Especifique la dirección MAC del cliente, que puede acceder a los recursos específicos sin autenticación. Dejar el campo vacío significa que los clientes con cualquier dirección MAC pueden acceder a los recursos específicos.

Puerto de destino	<p>Especifique el número de puerto del servicio. Al utilizar este servicio, los clientes pueden acceder a los recursos específicos sin autenticación.</p> <p>Dejar el campo vacío significa que los clientes pueden acceder a los recursos específicos independientemente del servicio que estén utilizando.</p>
--------------------------	--

Estado	<p>Marque la casilla para habilitar la política.</p>
---------------	--

Consejos:

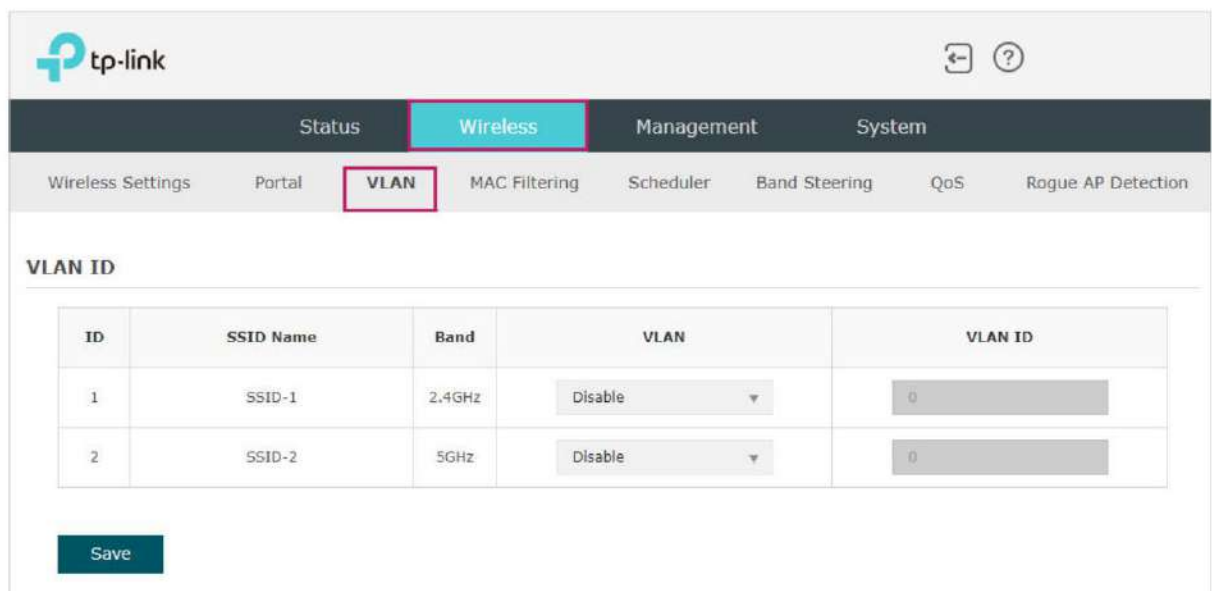
Cuando se configura el portal web externo, debe establecer la dirección IP y la máscara de subred del servidor web externo como rango de direcciones IP de destino. En cuanto al rango de direcciones IP de origen, la dirección MAC de origen y el puerto de destino, puede dejarlos en blanco o configurarlos según sus necesidades.

3. Haga clic en Aceptar para agregar la política.

2.3 Configurar VLAN

La VLAN inalámbrica se utiliza para configurar VLANs para las redes inalámbricas. Con esta función, el EAP puede funcionar con conmutadores compatibles con VLAN 802.1Q. El tráfico de los clientes en distintas redes inalámbricas se etiqueta con diferentes VLAN según la configuración de VLAN de dichas redes. De esta forma, los clientes inalámbricos en distintas VLAN no pueden comunicarse directamente entre sí. Cabe destacar que el tráfico de los clientes cableados no se etiqueta con VLAN.

Para configurar la VLAN para la red inalámbrica, vaya a la página Inalámbrico > VLAN.



The screenshot shows the TP-Link web interface for configuring wireless VLANs. The 'Wireless' tab is selected, and the 'VLAN' sub-tab is highlighted. Below the navigation bar, there is a table with the following columns: ID, SSID Name, Band, VLAN, and VLAN ID. The table contains two rows of data:

ID	SSID Name	Band	VLAN	VLAN ID
1	SSID-1	2.4GHz	Disable	0
2	SSID-2	5GHz	Disable	0

Below the table, there is a 'Save' button.

Siga los pasos que se indican a continuación para configurar la VLAN en esta página.

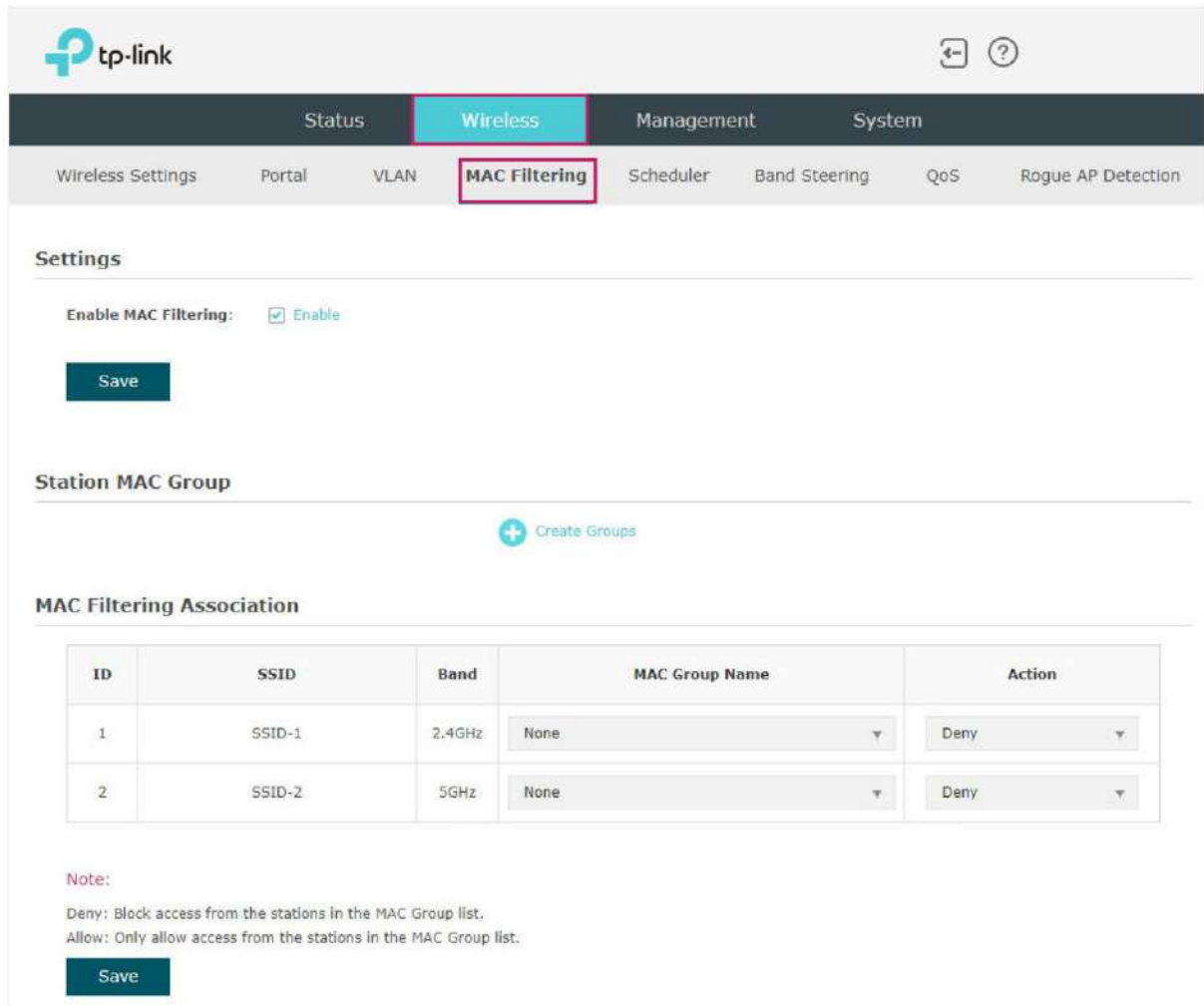
1. Seleccione el SSID específico en la lista para configurar la VLAN.
2. En la columna VLAN, seleccione Habilitar para activar la función VLAN en el SSID.
3. Especifique el ID de VLAN para la red inalámbrica en la columna ID de VLAN. Cada ID de VLAN representa una VLAN diferente. Admite un máximo de 8 VLAN por banda de frecuencia. El rango de ID de VLAN es de 0 a 4094. El valor 0 se utiliza para deshabilitar el etiquetado de VLAN.
4. Haga clic en Guardar.

2.4 Configurar el filtrado MAC

El filtrado MAC se utiliza para permitir o bloquear el acceso a la red a clientes con direcciones MAC específicas. Con esta función, puede controlar eficazmente el acceso de los clientes a la red inalámbrica.

Conéctate según tus necesidades.

Para configurar el filtrado MAC, vaya a la página Inalámbrico > Filtrado MAC.



Settings

Enable MAC Filtering: Enable

Save

Station MAC Group

+ Create Groups

MAC Filtering Association

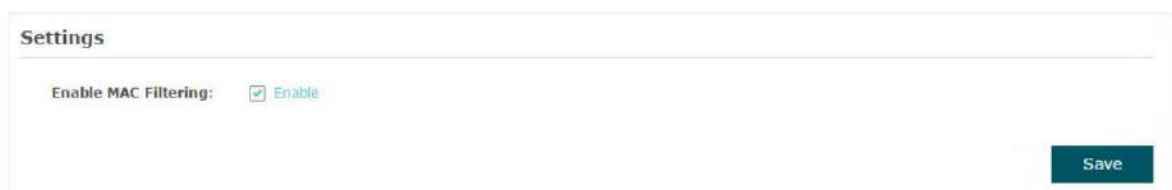
ID	SSID	Band	MAC Group Name	Action
1	SSID-1	2.4GHz	None	Deny
2	SSID-2	5GHz	None	Deny

Note:
Deny: Block access from the stations in the MAC Group list.
Allow: Only allow access from the stations in the MAC Group list.

Save

Siga los pasos que se indican a continuación para configurar el filtrado MAC en esta página:


1. En la sección Configuración, marque la casilla para habilitar el filtrado MAC y haga clic en Guardar.



Settings

Enable MAC Filtering: Enable

Save

2. En la sección Grupo MAC de la estación, haga clic en  **Create Groups** y la página siguiente será aparecer.




The screenshot shows the 'Station MAC Group' interface. On the left, there is a table with the following structure:

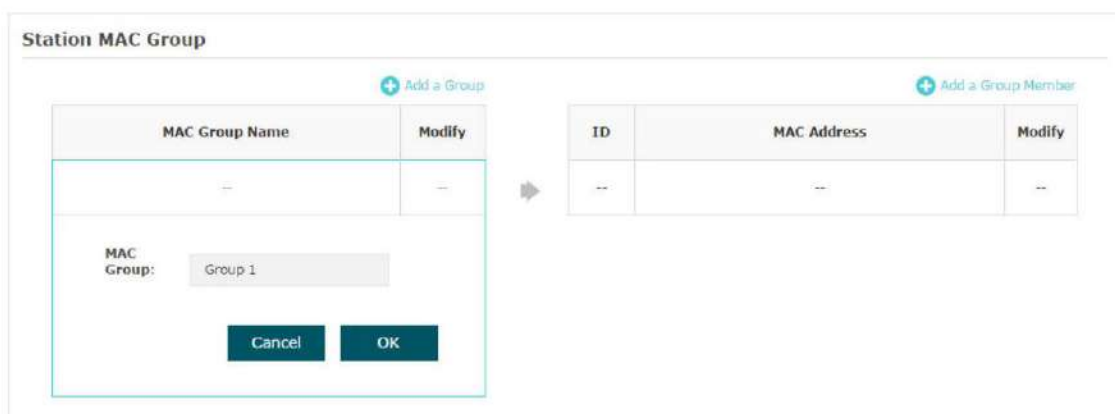
MAC Group Name	Modify
--	--

On the right, there is another table with the following structure:


ID	MAC Address	Modify
--	--	--

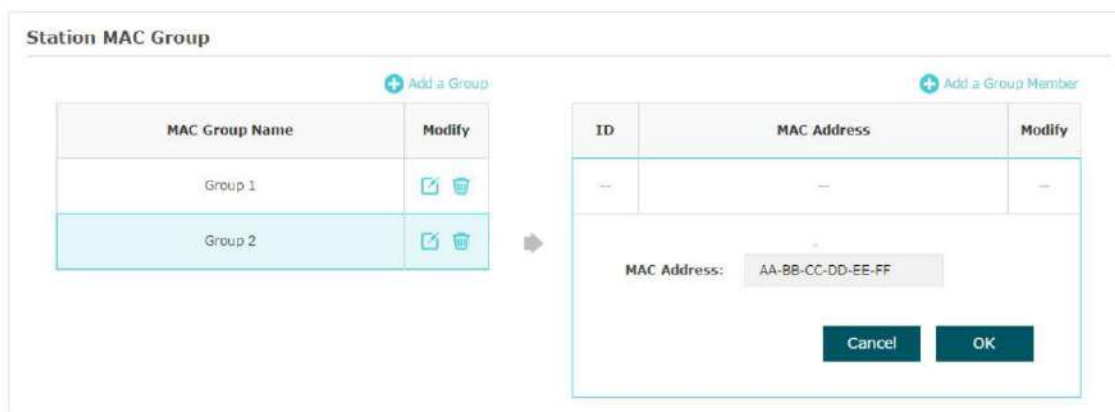
Both tables have a '+' icon and the text 'Add a Group' or 'Add a Group Member' above them. An arrow points from the first table to the second.

- 1) Haga clic  **Add a Group** y especifique un nombre para el grupo MAC que se va a crear. Haga clic en Aceptar. Puedes crear hasta ocho grupos MAC.



The screenshot shows the 'Station MAC Group' interface. The 'MAC Group Name' table has one row with 'Group 1' and a 'Modify' button. A modal dialog is open, showing a text input field with 'Group 1' and 'Cancel' and 'OK' buttons. The 'MAC Address' table is empty.

- 2) Seleccione un grupo MAC en la lista de grupos (el color del seleccionado cambiará a azul). Haga clic  para agregar miembros al grupo MAC. Especifique la dirección MAC del host y haga clic en Aceptar. De la misma manera, puede agregar más direcciones MAC. direcciones al grupo MAC seleccionado.



The screenshot shows the 'Station MAC Group' interface. The 'MAC Group Name' table has two rows: 'Group 1' and 'Group 2'. 'Group 2' is highlighted in blue. A modal dialog is open, showing a text input field with 'AA-BB-CC-DD-EE-FF' and 'Cancel' and 'OK' buttons. The 'MAC Address' table is empty.

3. En la sección Asociación de filtrado MAC, configure la regla de filtrado. Para cada SSID, puede seleccionar un grupo MAC en la columna Nombre del grupo MAC y seleccionar la regla de filtrado (Permitir/Denegar) en la columna Acción. Haga clic en Guardar.

Por ejemplo, la siguiente configuración significa que a los hosts del Grupo 2 se les deniega el acceso. acceder al SSID SSID-1 en la banda de 2.4GHz y se permite el acceso al SSID SSID-2 en la banda de 5 GHz.

MAC Filtering Association

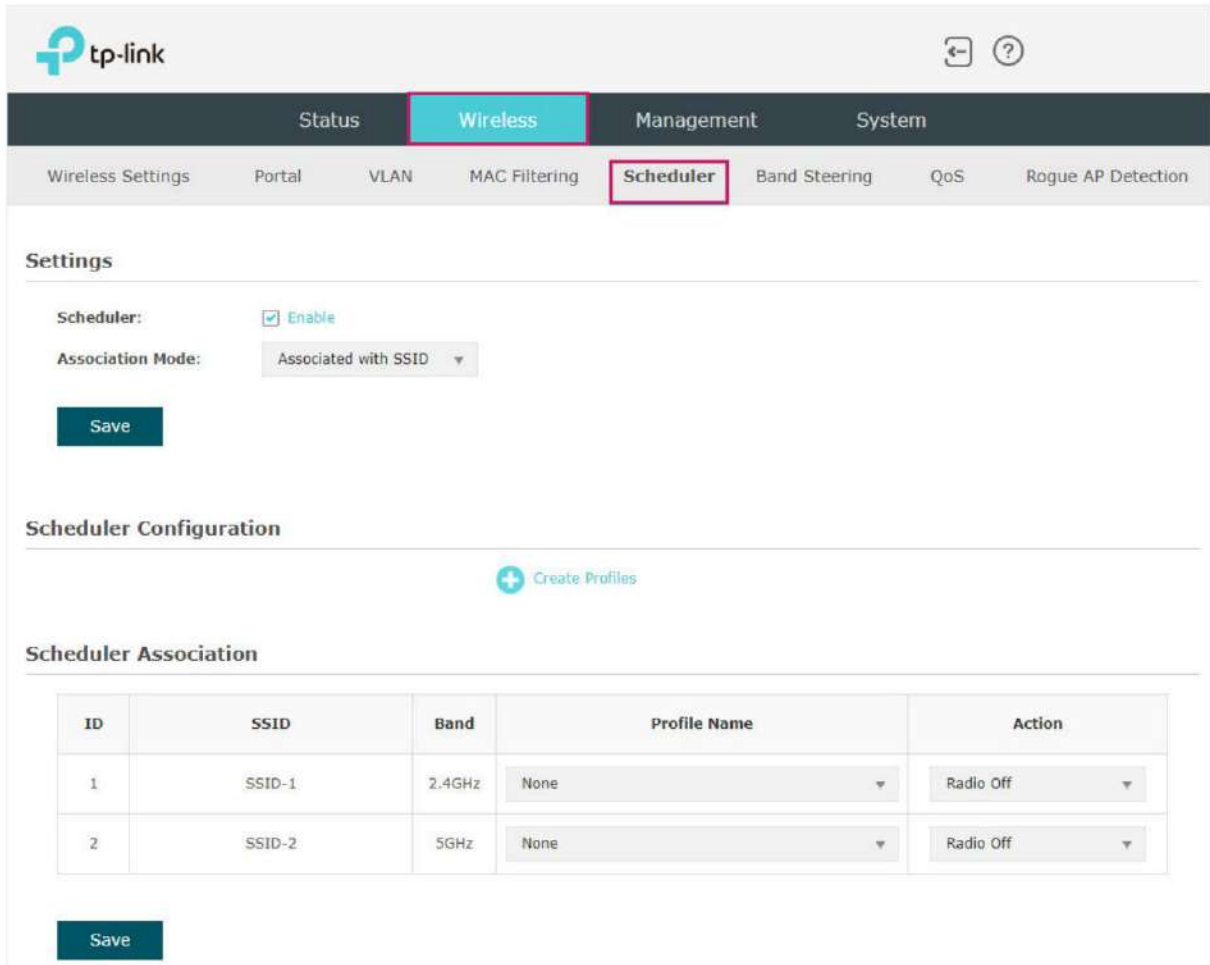
ID	SSID	Band	MAC Group Name	Action
1	SSID-1	2.4GHz	Group2 ▼	Deny ▼
2	SSID-2	5GHz	Group2 ▼	Allow ▼

Note:
Deny: Block access from the stations in the MAC Group list.
Allow: Only allow access from the stations in the MAC Group list.

2.5 Configurar el programador

Con la función de Programador, el EAP o su red inalámbrica se pueden encender o apagar automáticamente a la hora que usted configure. Por ejemplo, puede programar la radio para que funcione solo durante el horario laboral y así reducir el consumo de energía.

Para configurar el programador, vaya a la página Inalámbrico > Programador.



Settings

Scheduler: Enable

Association Mode: Associated with SSID ▼

Save

Scheduler Configuration

+ Create Profiles

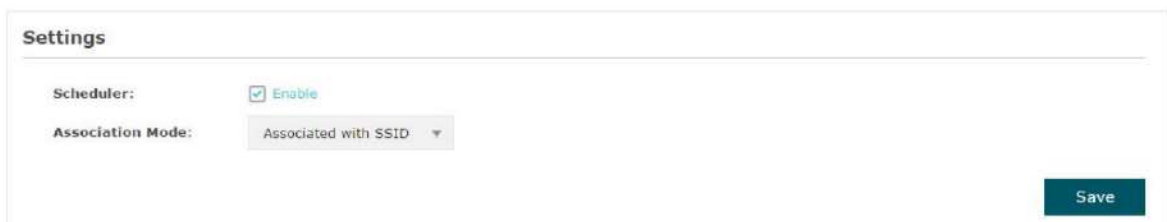
Scheduler Association

ID	SSID	Band	Profile Name	Action
1	SSID-1	2.4GHz	None ▼	Radio Off ▼
2	SSID-2	5GHz	None ▼	Radio Off ▼

Save

Siga los pasos que se indican a continuación para configurar el programador en esta página:

1. En la sección Configuración, marque la casilla para habilitar el programador y seleccione el modo de asociación. Hay dos modos: Asociado con SSID (el perfil del programador se aplicará al SSID específico) y Asociado con AP (el perfil se aplicará a todos los SSID del EAP). A continuación, haga clic en Guardar.




Settings

Scheduler: Enable

Association Mode: Associated with SSID ▼

Save

2. En la sección Configuración del perfil del programador, aparecerá  **Create Profiles** y lo siguiente la página de clic.

Scheduler Profile Configuration

 Add a Profile

Profile Name	Modify
--	--


→

 Add an item

ID	Profile Name	Days	Start Time	End Time	Modify
--	--	--	--	--	--


- 1) Haga clic y especifique un nombre para el perfil que se va a crear. Haga clic en Aceptar. Puede crear hasta ocho perfiles.

Scheduler Profile Configuration

 Add a Profile

Profile Name	Modify
--	--


→

 Add an item


ID	Profile Name	Days	Start Time	End Time	Modify
--	--	--	--	--	--





Profile:

- 2) Seleccione un perfil en la lista (el color del seleccionado cambiará a azul). Haga clic.


 **Add an item** Para agregar elementos de rango de tiempo al perfil, especifique el día, la hora de inicio y la hora de finalización del rango de tiempo y haga clic en Aceptar.

Scheduler Profile Configuration

 Add a Profile

Profile Name	Modify
Profile 1	 
Profile 2	 

→

 Add an item

ID	Profile Name	Days	Start Time	End Time	Modify
--	--	--	--	--	--

Day: Weekday Weekend Every Day Custom

Mon Tue Wed Thu Fri Sat

Sun

Time: 24 hours

Start Time: 09 : 00

End Time: 18 : 00

Consejos:

Puedes añadir hasta ocho intervalos de tiempo a un perfil. Si un perfil contiene varios intervalos de tiempo, el intervalo total será la suma de todos ellos.

3. En la sección Asociación de planificador, configure la regla del planificador. Hay dos. Las siguientes modos de asociación: [Asociación con SSID](#) y [Asociación con AP](#)
- Estas secciones explican cómo configurar cada modo.

■ Asociación con SSID

Si selecciona Asociación con SSID en el paso 1, la tabla de Asociación del programador mostrará todos los SSID en el EAP. Para cada SSID, puede seleccionar un perfil en la columna Nombre del perfil y seleccionar la regla del programador (Radio encendida/Radio apagada) en la columna Acción.

Luego haga clic en Guardar.

Por ejemplo, la siguiente configuración significa que durante el intervalo de tiempo definido en el perfil 2, la radio del SSID SSID-1 está encendida y la radio del SSID SSID-2 está apagada.

Scheduler Association				
ID	SSID	Band	Profile Name	Action
1	SSID-1	2.4GHz	profile2	Radio On
2	SSID-2	5GHz	profile2	Radio Off

[Save](#)

■ Asociación con AP

Si selecciona Asociación con AP en el paso 1, se mostrará la tabla de Asociación del programador. el nombre y la dirección MAC del EAP. Seleccione un perfil en la columna Nombre del perfil y Seleccione la regla del programador (Radio encendida/Radio apagada) en la columna Acción. A continuación, haga clic en Guardar.

Por ejemplo, la siguiente configuración significa que durante el intervalo de tiempo definido en Perfil 2: la radio de todos los SSID en el EAP está encendida.

Scheduler Association				
ID	AP	AP MAC	Profile Name	Action
1	EAP245-50-c7-bf-17-a6-e2	50-C7-BF-17-A6-E2	Profile 2	Radio On

[Save](#)

2.6 Configurar la dirección de banda

Un dispositivo cliente capaz de comunicarse en múltiples bandas de frecuencia normalmente se conectará a la banda de 2,4 GHz.

Sin embargo, si hay demasiados dispositivos cliente conectados a un punto de acceso en la misma banda, la eficiencia de la comunicación disminuirá. La dirección de banda puede

Dirija los clientes multibanda a diferentes bandas para mejorar considerablemente la calidad de la red.

Para configurar la función de dirección de banda, vaya a la página Inalámbrico > Dirección de banda.

Band Steering

Band Steering: Disable ▾

Note:
To run the Band Steering function on an SSID, please create the SSID with the same wireless password on the 2GHz, 5GHz, and 6GHz bands.

Save

Dirección de banda

Configure la función de dirección de banda.

Deshabilitar: El punto de acceso no dirigirá a los clientes.

Preferir 5GHz/6GHz: El punto de acceso dirigirá a los clientes a las bandas de 5GHz y 6GHz en prioridad.

Balance: El punto de acceso equilibrará las conexiones de los clientes entre las diferentes bandas.

2.7 Configurar QoS

La calidad de servicio (QoS) se utiliza para optimizar el rendimiento y la transmisión de datos del EAP al gestionar tráfico inalámbrico diferenciado, como la voz sobre IP (VoIP), otros tipos de audio, vídeo, transmisión de contenido multimedia y datos IP tradicionales.

En la configuración de QoS, debe establecer parámetros en las colas de transmisión para diferentes tipos de tráfico inalámbrico y especificar el tiempo de espera mínimo y máximo para los datos.

transmisión. En condiciones normales de uso, recomendamos mantener los valores predeterminados.

Para configurar la calidad de servicio (QoS), vaya a la página Inalámbrico > QoS.

The screenshot shows the TP-Link web interface for configuring QoS. The 'Wireless' tab is selected, and the 'QoS' sub-tab is highlighted. The interface includes frequency selection (2.4GHz and 5GHz), a checked 'Wi-Fi Multimedia (WMM): Enable' option, and two tables for EDCA parameters. The 'AP EDCA Parameters' table has columns for Queue, Arbitration Inter-Frame Spacing, Minimum Contention Window, Maximum Contention Window, and Maximum Burst. The 'Station EDCA Parameters' table has columns for Queue, Arbitration Inter-Frame Spacing, Minimum Contention Window, Maximum Contention Window, and TXOP Limit. At the bottom, there are checkboxes for 'No Acknowledgement' (disabled) and 'Unscheduled Automatic Power Save Delivery' (enabled), and a 'Save' button.

Queue	Arbitration Inter-Frame Spacing	Minimum Contention Window	Maximum Contention Window	Maximum Burst
Data 0 (Voice)	1	3	7	1504
Data 1 (Video)	1	7	15	3008
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Queue	Arbitration Inter-Frame Spacing	Minimum Contention Window	Maximum Contention Window	TXOP Limit
Data 0 (Voice)	2	3	7	1504
Data 1 (Video)	2	7	15	3008
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

Siga los pasos que se indican a continuación para configurar la calidad de servicio (QoS) en esta página:

1. Haga clic  para elegir una banda de frecuencia que se vaya a configurar.

2. Marque la casilla para habilitar Wi-Fi Multimedia (WMM). Con WMM habilitado, el EAP utiliza La función QoS garantiza la alta prioridad de la transmisión de audio y vídeo. paquetes.

Wi-Fi Multimedia (WMM): Enable

Nota:

Si se selecciona el modo 802.11n únicamente en la banda de 2,4 GHz (o el modo mixto 802.11n/ac o 802.11n/ac en la banda de 5 GHz), se debe habilitar el WMM. Si el WMM está deshabilitado, no se podrá seleccionar el modo 802.11n únicamente en la banda de 2,4 GHz (ni el modo mixto 802.11n/ac o 802.11n/ac en la banda de 5 GHz).

3. En la sección Parámetros de AP EDCA, configure los parámetros de AP EDCA (Acceso de canal distribuido mejorado). Los parámetros de AP EDCA afectan el tráfico que fluye desde el EAP hacia la estación cliente. La siguiente tabla explica detalladamente estos parámetros.

Queue	Arbitration Inter-Frame Spacing	Minimum Contention Window	Maximum Contention Window	Maximum Burst
Data 0 (Voice)	1	3	7	1504
Data 1 (Video)	1	7	15	3008
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

La siguiente tabla explica detalladamente estos parámetros:

Cola	<p>Muestra la cola de transmisión. Por defecto, la prioridad, de mayor a menor, es Datos 0, Datos 1, Datos 2 y Datos 3. La prioridad puede modificarse si se restablecen los parámetros EDCA.</p> <p>Datos 0 (Voz): Cola de máxima prioridad, mínima demora. Los datos sensibles al tiempo, como VoIP y medios de transmisión, se envían automáticamente a esta cola.</p> <p>Datos 1 (Vídeo): Cola de alta prioridad, mínima demora. Los datos de vídeo sensibles al tiempo se envían automáticamente a esta cola.</p> <p>Datos 2 (Mejor esfuerzo): Cola de prioridad media, rendimiento y retardo medios. La mayoría de los datos IP tradicionales se envían a esta cola.</p> <p>Cola de datos 3 (fondo): Cola de menor prioridad, alto rendimiento. Los datos masivos que requieren el máximo rendimiento y no son sensibles al tiempo se envían a esta cola (datos FTP, por ejemplo).</p>
Arbitraje Inter-Espacio del marco	<p>Tiempo de espera para los marcos de datos. El tiempo de espera se mide en ranuras. Válido Los valores van de 0 a 15.</p>

Mínimo
Contención
Ventana

Una lista del algoritmo que determina el tiempo de espera (ventana) de retroceso aleatorio inicial para reintentar una transmisión.

Este valor no puede ser superior al valor de la Ventana de Contención Máxima.

Máximo
Contención
Ventana

El límite superior (en milisegundos) para la duplicación del valor de retroceso aleatorio. Esta duplicación continúa hasta que se envía el marco de datos o se alcanza el tamaño máximo de la ventana de contención.

Este valor debe ser superior al valor de la Ventana de Contención Mínima.

Ráfaga máxima

La opción "Ráfaga máxima" especifica la longitud máxima permitida para las ráfagas de paquetes en la red inalámbrica. Una ráfaga de paquetes es un conjunto de múltiples tramas transmitidas sin información de encabezado. La reducción de la sobrecarga se traduce en un mayor rendimiento y una mejor transmisión de datos.

4. En la sección Parámetros EDCA de la estación, configure los parámetros EDCA (Enhanced Distributed Channel Access) de la estación. Los parámetros EDCA de la estación afectan al tráfico fluyendo desde la estación del cliente hacia el EAP.

Queue	Arbitration Inter-Frame Spacing	Minimum Contention Window	Maximum Contention Window	TXOP Limit
Data 0 (Voice)	2	3	7	1504
Data 1 (Video)	2	7	15	3008
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

La siguiente tabla explica detalladamente estos parámetros:

Cola

Muestra la cola de transmisión. Por defecto, la prioridad, de mayor a menor, es Datos 0, Datos 1, Datos 2 y Datos 3. La prioridad puede modificarse si se restablecen los parámetros EDCA.

Datos 0 (Voz): Cola de máxima prioridad, mínima latencia. Los datos sensibles al tiempo, como VoIP y la transmisión de contenido multimedia, se envían automáticamente a esta cola.

Datos 1 (Vídeo): Cola de alta prioridad, mínima demora. Los datos de vídeo sensibles al tiempo se envían automáticamente a esta cola.

Datos 2 (Mejor esfuerzo): Cola de prioridad media, rendimiento y retardo medios. La mayoría de los datos IP tradicionales se envían a esta cola.

Cola de datos 3 (fondo): Cola de menor prioridad, alto rendimiento. Los datos masivos que requieren el máximo rendimiento y no son sensibles al tiempo se envían a esta cola (datos FTP, por ejemplo).

Arbitraje Inter-Espacio del marco	Tiempo de espera para los marcos de datos. El tiempo de espera se mide en ranuras. Válido Los valores van de 0 a 15.
Mínimo Contención Ventana	Una lista del algoritmo que determina el tiempo de espera (ventana) de retroceso aleatorio inicial para reintentar una transmisión. Este valor no puede ser superior al valor de la Ventana de Contención Máxima.
Máximo Contención Ventana	El límite superior (en milisegundos) para la duplicación del valor de retroceso aleatorio. Esta duplicación continúa hasta que se envía el marco de datos o se alcanza el tamaño máximo de la ventana de contención. Este valor debe ser superior al valor de la Ventana de Contención Mínima.
Límite de TXOP	El límite TXOP es un parámetro EDCA de la estación y solo se aplica al tráfico que fluye desde la estación cliente hacia el EAP. La Oportunidad de Transmisión (TXOP) es un intervalo de tiempo, en milisegundos, durante el cual una estación cliente WME (Wireless Multimedia Extensions) tiene derecho a iniciar transmisiones en el medio inalámbrico (WM) hacia el EAP. Los valores válidos son múltiplos de 32, entre 0 y 8192.

5. Elija si desea habilitar las siguientes dos opciones según sus necesidades.

No Acknowledgement: Enable

Unscheduled Automatic Power Save Delivery: Enable

La siguiente tabla explica detalladamente estas opciones:

Sin acuse de recibo	Con esta opción habilitada, el EAP no confirmará la recepción de tramas con QoSNoAck. No se recomienda la confirmación de recepción si los teléfonos VoIP acceden a la red a través del EAP.
No programado Ahorro de energía automático Entrega	Como método de gestión de energía, puede mejorar considerablemente la capacidad de ahorro energético de los clientes.

6. Haga clic en Guardar.

2.8 Configurar la detección de puntos de acceso no autorizados

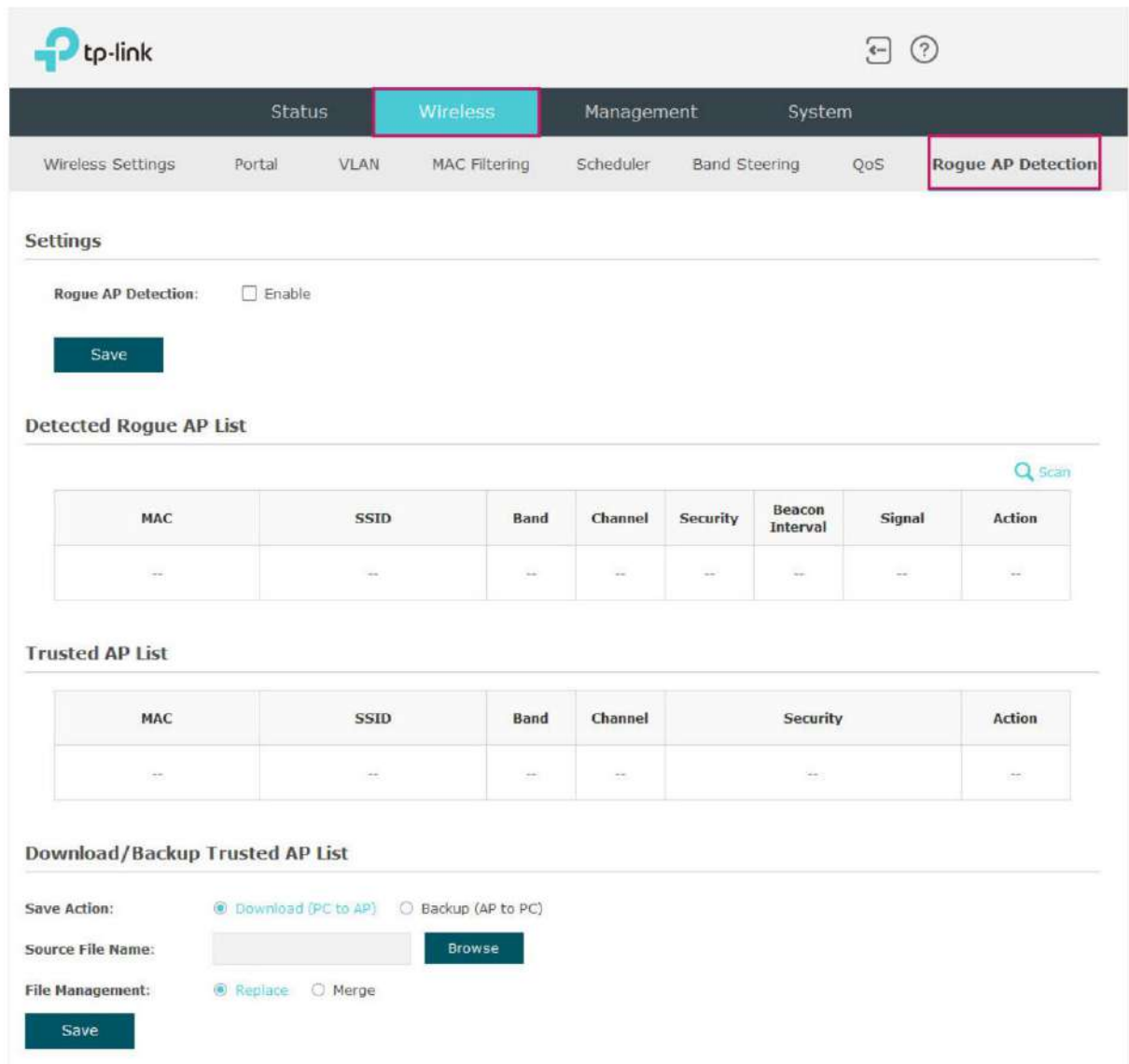
Un AP no autorizado es un punto de acceso instalado en una red segura sin autorización explícita del administrador de la red. Con la detección de AP no autorizados, el EAP puede escanear todos los canales para detectar los AP cercanos y mostrarlos en la lista de AP no autorizados detectados. Si se sabe que el AP específico es seguro, puede moverlo a la lista de AP de confianza. Además,

Puede realizar copias de seguridad e importar la lista de puntos de acceso de confianza según sea necesario.

Nota:

La función de detección de puntos de acceso no autorizados solo se utiliza para recopilar información de la red inalámbrica cercana y no afecta a los puntos de acceso detectados, independientemente de las operaciones que haya realizado en esta función.

Para configurar la detección de puntos de acceso no autorizados, vaya a la página Inalámbrico > Detección de puntos de acceso no autorizados.



The screenshot shows the TP-Link web interface for configuring Rogue AP Detection. The 'Wireless' tab is selected, and 'Rogue AP Detection' is highlighted in the sub-menu. The 'Settings' section has 'Rogue AP Detection' disabled. Below are empty tables for 'Detected Rogue AP List' and 'Trusted AP List'. The 'Download/Backup Trusted AP List' section offers options to download or backup the list.

Settings

Rogue AP Detection: Enable

Save

Detected Rogue AP List

MAC	SSID	Band	Channel	Security	Beacon Interval	Signal	Action
--	--	--	--	--	--	--	--

Trusted AP List

MAC	SSID	Band	Channel	Security	Action
--	--	--	--	--	--

Download/Backup Trusted AP List

Save Action: Download (PC to AP) Backup (AP to PC)

Source File Name: Browse

File Management: Replace Merge

Save

Detectar puntos de acceso no autorizados y moverlos a la lista de puntos de acceso de confianza.

Siga los pasos a continuación para detectar los AP cercanos y mover los de confianza a la sección de Confianza.


Lista AP.

1. En la sección Configuración, marque la casilla para habilitar la detección de AP no autorizados. Haga clic en Guardar.

Settings

Rogue AP Detection: Enable











Save

2. En la sección Lista de AP no autorizados detectados, haga clic en .

3. Espere unos segundos sin realizar ninguna operación. Una vez finalizada la detección, el objeto detectado...

Los puntos de acceso se mostrarán en la lista.

Detected Rogue AP List

MAC	SSID	Band	Channel	Security	Beacon Interval	Signal	Action
00:0A:EB:13:09:17	C7v3_5G	5.0	36	ON	100		Known
00:0A:EB:13:09:18	C7v3	2.4	11	ON	100		Known
00:0A:EB:13:7A:FD	TP-Link_7B00_5G_1	5.0	36	ON	100		Known
00:0A:EB:13:7A:FE	TP-Link_7B00_5G_2	5.0	36	ON	100		Known
00:0A:EB:13:7A:FF	TP-Link_7B00	2.4	1	ON	100		Known
00:0A:EB:13:7B:01	RvR5	5.0	48	OFF	100		Known
00:1D:0F:E3:33:B1	Camera	2.4	4	ON	100		Known
00:20:02:16:38:22	TP-LINK_2.4G_3822	2.4	1	ON	100		Known
02:71:CC:4C:16:B8	DIRECT-na-BRAVIA	2.4	11	ON	100		Known
06:18:D6:C1:92:23	qwer	2.4	6	OFF	100		Known

1 2 3 4 5 ... 8

La siguiente tabla presenta la información mostrada de los AP:

IMPERMEABLE	Muestra la dirección MAC del punto de acceso.
SSID	Muestra el SSID del punto de acceso.
Banda	Muestra la banda de frecuencia en la que está funcionando el punto de acceso.
Canal	Muestra el canal que está utilizando el punto de acceso.
Seguridad	Indica si el modo de seguridad está habilitado en el punto de acceso.

Intervalo de baliza

Muestra el valor del intervalo de baliza del EAP.

El punto de acceso (AP) envía periódicamente tramas de baliza para informar a las estaciones de la presencia de una red inalámbrica. El intervalo de baliza determina el intervalo de tiempo entre los envíos de tramas de baliza por parte del AP.

Señal

Muestra la intensidad de la señal del punto de acceso.

4. Para mover el AP específico a la lista de AP de confianza, haga clic aquí. [Known](#) en la columna de Acción. Para por ejemplo, movemos los dos primeros AP de la lista anterior de AP no autorizados detectados a la lista de confianza.

Lista AP.

5. Vea los AP de confianza en la sección Lista de AP de confianza. Para mover el AP específico de vuelta a

La lista de AP de Rogue, puedes hacer clic [Unknown](#) en la columna de Acción.

Trusted AP List					
MAC	SSID	Band	Channel	Security	Action
00:0A:EB:13:7A:FD	TP-Link_7B00_5G_1	5.0	36	ON	Unknown
00:0A:EB:13:7A:FE	TP-Link_7B00_5G_2	5.0	36	ON	Unknown

Administrar la lista de AP de confianza

Puede descargar la lista de puntos de acceso de confianza desde su equipo local al EAP o realizar una copia de seguridad de la lista actual de puntos de acceso de confianza en su equipo local.

- Descargue la lista de puntos de acceso de confianza desde el servidor.

Puedes importar una lista de puntos de acceso (AP) de confianza que registre las direcciones MAC de dichos puntos. Los AP cuya dirección MAC figure en la lista no serán detectados como puntos de acceso no autorizados.

Download/Backup Trusted AP List

Save Action: Download (PC to AP) Backup (AP to PC)

Source File Name:

File Management: Replace Merge


Siga los pasos que se indican a continuación para importar una lista de puntos de acceso de confianza al EAP:

1. Adquiera la lista de AP de confianza. Hay dos maneras:

- Realice una copia de seguridad de la lista desde un EAP. Para obtener más detalles, consulte [Copia de seguridad Confiable AP Lista para el Anfitrión](#).

- Cree manualmente una lista de AP de confianza. Cree un archivo .txt, introduzca las direcciones MAC de los AP de confianza en el formato XX:XX:XX:XX:XX:XX y utilice la tecla Espacio para separar cada dirección MAC. Guarde el archivo como un archivo .cfg.

2. En esta página, marque la casilla para elegir Descargar (PC a AP).

3. Haga clic  y seleccione la lista de puntos de acceso de confianza de su host local.

4. Seleccione el modo de gestión de archivos. Hay dos modos disponibles: Reemplazar y Combinar.

Reemplazar significa que la lista actual de puntos de acceso de confianza será reemplazada por la que importe.

La opción "Fusionar" significa que los puntos de acceso (AP) de la lista importada se añadirán a la lista actual, manteniendo los puntos de acceso originales.

5. Haga clic en Guardar para importar la lista de AP de confianza.

- Realice una copia de seguridad de la lista de puntos de acceso de confianza en el host.

Puede realizar una copia de seguridad de la lista actual de puntos de acceso de confianza y guardar el archivo de copia de seguridad en el host local.

Download/Backup Trusted AP List

Save Action: Download (PC to AP) Backup (AP to PC)

Save

Siga los pasos que se indican a continuación para realizar una copia de seguridad de la lista actual de puntos de acceso de confianza:

1. En esta página, marque la casilla para elegir Copia de seguridad (AP a PC).

2. Haga clic en Guardar y la lista actual de AP de confianza se descargará en su host local como un archivo .cfg.

archivo.

2.9 Configurar la antena inteligente (solo para ciertos dispositivos)

La tecnología Smart Antenna mejora el rendimiento de Wi-Fi en entornos con gran cantidad de usuarios gracias a su conjunto de antenas y a un algoritmo inteligente, y ayuda a superar obstáculos e interferencias de señal.

Para activar o desactivar la antena inteligente, vaya a la página Inalámbrico > Antena inteligente.

Smart Antenna

Smart Antenna: Enable

Note:

Smart Antenna improves Wi-Fi performance for user-heavy scenarios through antenna array and intelligent algorithm, and it helps overcome obstacles and signal interference.

[Save](#)

3

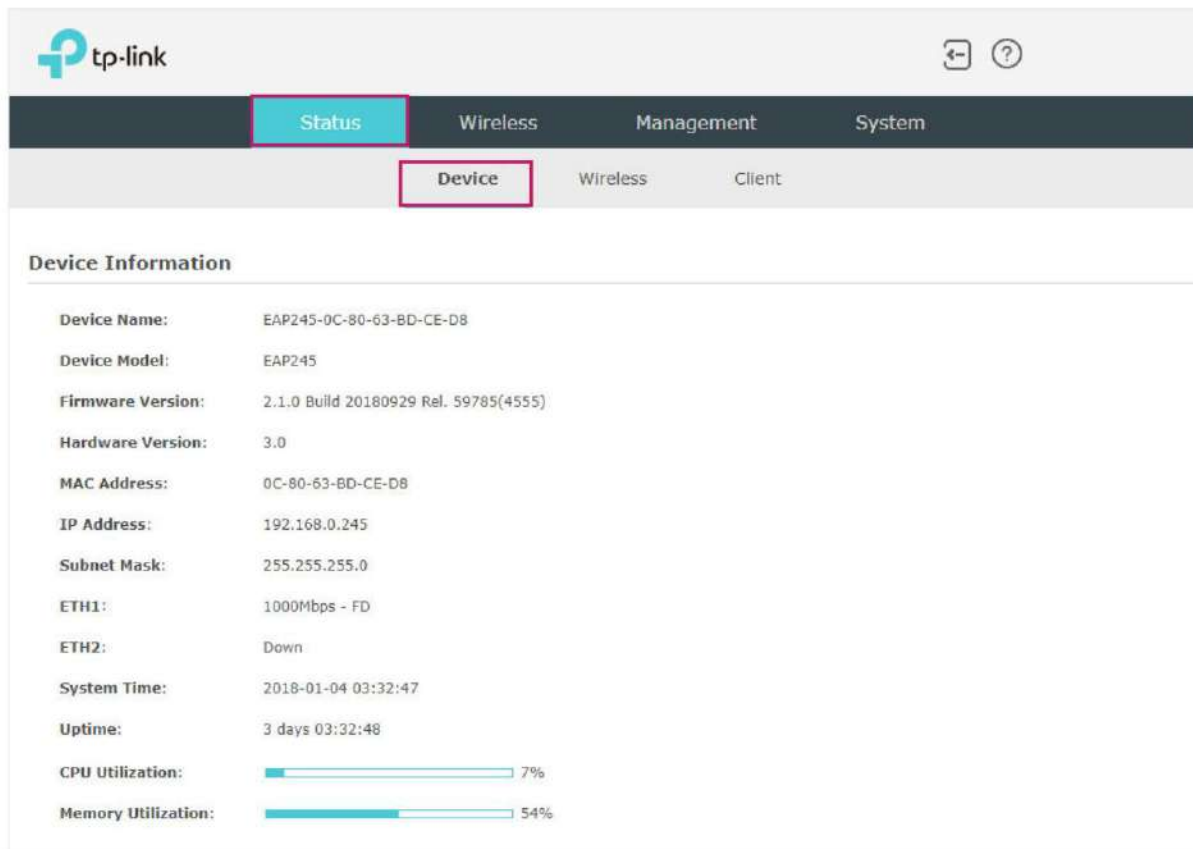
Monitorear el Red

Este capítulo presenta cómo supervisar el estado de funcionamiento y las estadísticas de la conexión inalámbrica. red, que incluye:



- 3.1 Supervisar el EAP
- 3.2 Monitorizar los parámetros inalámbricos
- 3.3 Monitorear el Clientela

3.1 Supervisar el EAP

Para supervisar la información de EAP, vaya a la página Estado > Dispositivo.



The screenshot shows the TP-Link web interface. At the top, there is a navigation bar with tabs for 'Status', 'Wireless', 'Management', and 'System'. The 'Status' tab is active. Below this, there is a sub-navigation bar with 'Device', 'Wireless', and 'Client' options. The 'Device' option is highlighted. The main content area is titled 'Device Information' and contains the following details:

Device Name:	EAP245-0C-80-63-BD-CE-D8
Device Model:	EAP245
Firmware Version:	2.1.0 Build 20180929 Rel. 59785(4555)
Hardware Version:	3.0
MAC Address:	0C-80-63-BD-CE-D8
IP Address:	192.168.0.245
Subnet Mask:	255.255.255.0
ETH1:	1000Mbps - FD
ETH2:	Down
System Time:	2018-01-04 03:32:47
Uptime:	3 days 03:32:48
CPU Utilization:	 7%
Memory Utilization:	 54%


Se muestra la siguiente información del dispositivo:

Nombre del dispositivo	Muestra el nombre del EAP. Por defecto, el nombre consta del modelo del producto seguido de la dirección MAC del EAP.
Modelo de dispositivo	Muestra el modelo de producto del EAP.
Versión del firmware	Muestra la versión actual del firmware del EAP. Para actualizar el firmware, puede consultar 5.6 Actualizar el firmware .
Versión de hardware	Muestra la versión de hardware del EAP.
Dirección MAC	Muestra la dirección MAC del EAP.
Dirección IP	Muestra la dirección IP del EAP.
Máscara de subred	Muestra la máscara de subred del EAP.
Hora del sistema	Muestra la hora actual del sistema. Para configurar la hora del sistema, puede consultar 5.3 Configurar la hora del sistema .
Tiempo de actividad	Muestra cuánto tiempo lleva funcionando el EAP desde que se inició.

Utilización de la CPU	Muestra la ocupación de la CPU. Si este valor es demasiado alto, el EAP podría funcionar de forma anómala.
Utilización de la memoria	Muestra la ocupación de la memoria.

Si su producto es un kit Bridge:

En la página de dispositivos del AP principal, puede ver la lista de sub-AP. Para una entrada de sub-AP, puede

hacer clic  para lanzar su página web.

Sub-APs				
ID	MAC Address	IP Address	Signal Strength	Action
1	A8-42-A1-5A-42-93	192.168.0.105	 -51dbm	

En la página de dispositivos del Sub-AP, puede ver su AP principal.

Main AP	
MAC Address:	A8-42-A1-5A-42-92

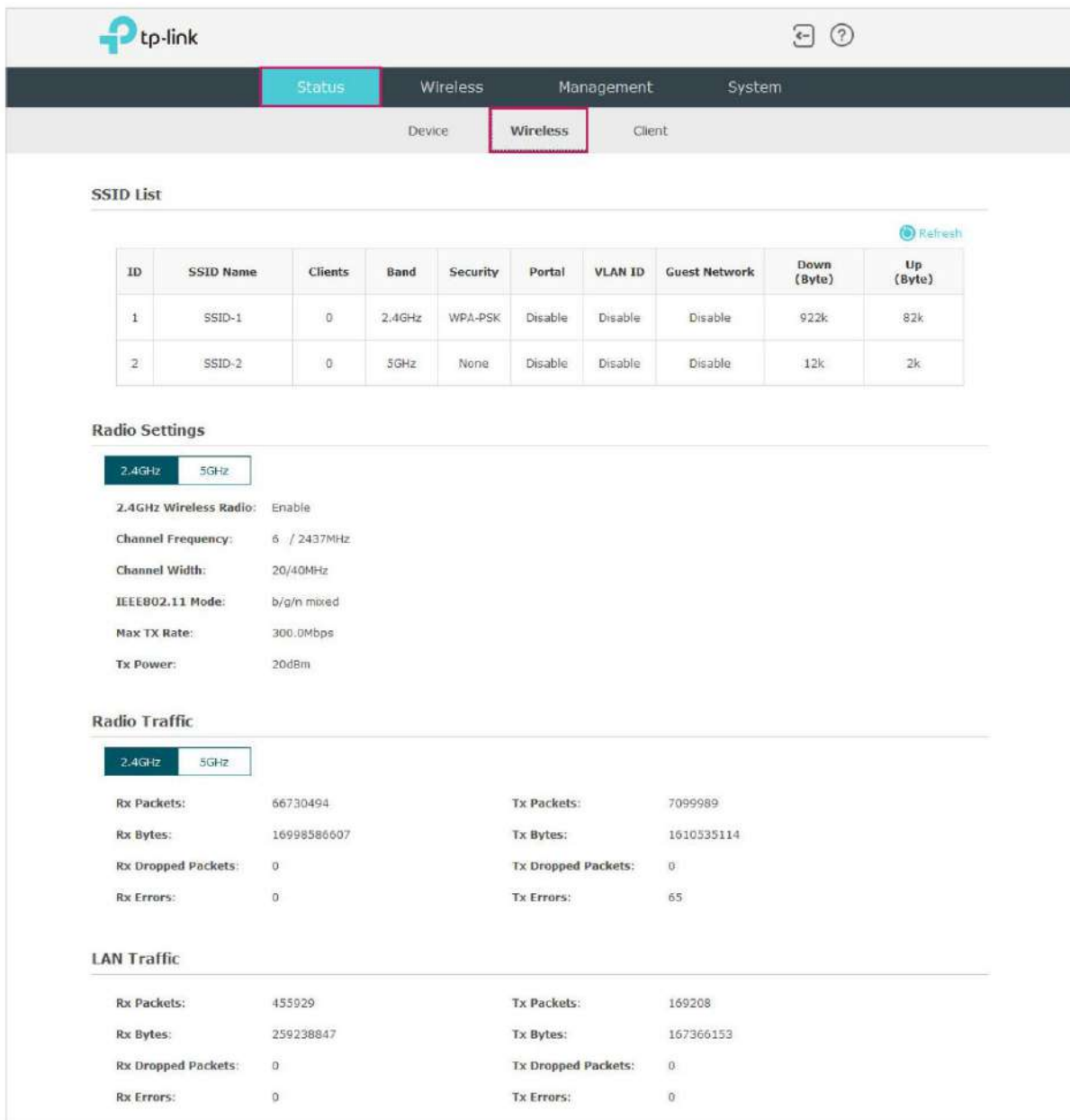
3.2 Monitorizar los parámetros inalámbricos

Puede ver los parámetros inalámbricos del EAP, incluidas las listas de SSID, la configuración de radio, la radio tráfico y tráfico LAN.

Consejos:

Para cambiar los parámetros inalámbricos, puede consultar: [2.1 Configurar los parámetros inalámbricos](#)

Para supervisar los parámetros inalámbricos, vaya a la página Estado > Inalámbrico.



The screenshot displays the TP-Link web interface for monitoring wireless parameters. The top navigation bar includes 'Status', 'Wireless', 'Management', and 'System'. The 'Wireless' section is active, showing a sub-menu with 'Device', 'Wireless', and 'Client'. The main content area is divided into four sections: SSID List, Radio Settings, Radio Traffic, and LAN Traffic.

SSID List

ID	SSID Name	Clients	Band	Security	Portal	VLAN ID	Guest Network	Down (Byte)	Up (Byte)
1	SSID-1	0	2.4GHz	WPA-PSK	Disable	Disable	Disable	922k	82k
2	SSID-2	0	5GHz	None	Disable	Disable	Disable	12k	2k

Radio Settings

2.4GHz | 5GHz

2.4GHz Wireless Radio: Enable

Channel Frequency: 6 / 2437MHz

Channel Width: 20/40MHz

IEEE802.11 Mode: b/g/n mixed

Max TX Rate: 300.0Mbps

Tx Power: 20dBm

Radio Traffic

2.4GHz | 5GHz

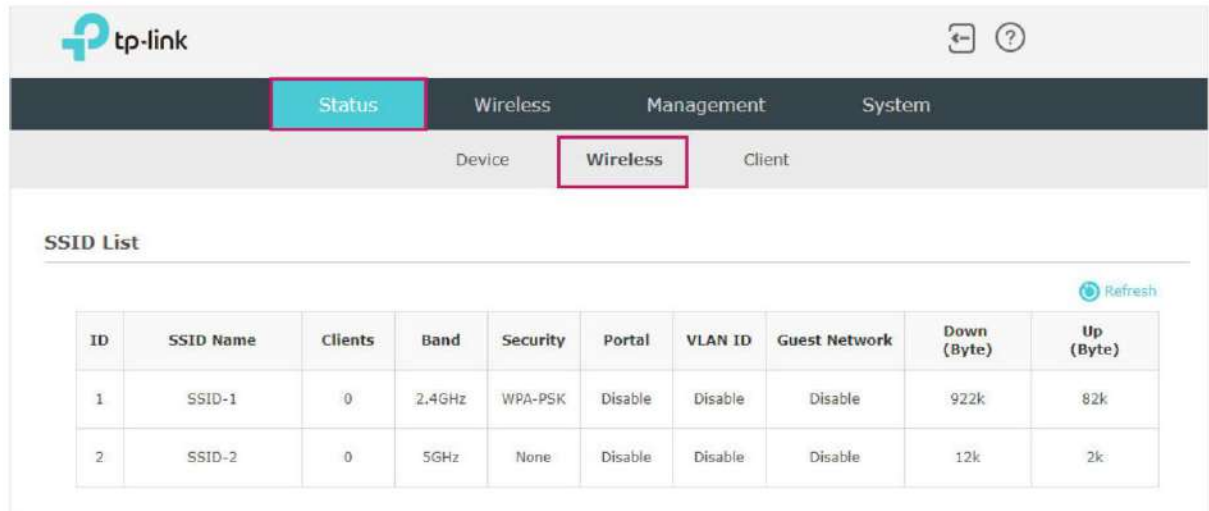
Rx Packets:	66730494	Tx Packets:	7099989
Rx Bytes:	16998586607	Tx Bytes:	1610535114
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	65

LAN Traffic

Rx Packets:	455929	Tx Packets:	169208
Rx Bytes:	259238847	Tx Bytes:	167366153
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	0

Monitorea los SSID

Puedes monitorizar la información SSID del EAP.



The screenshot shows the TP-Link web interface. At the top, there is a navigation bar with 'Status' highlighted. Below it, there are tabs for 'Device', 'Wireless', and 'Client', with 'Wireless' selected. The main content area is titled 'SSID List' and contains a table with the following data:

ID	SSID Name	Clients	Band	Security	Portal	VLAN ID	Guest Network	Down (Byte)	Up (Byte)
1	SSID-1	0	2.4GHz	WPA-PSK	Disable	Disable	Disable	922k	82k
2	SSID-2	0	5GHz	None	Disable	Disable	Disable	12k	2k

La siguiente tabla presenta la información mostrada del SSID:

Nombre del SSID	Muestra el nombre del SSID.
Cientela	Muestra el número de clientes conectados actualmente a la red Wi-Fi (SSID).
Banda	Muestra la banda de frecuencia que está utilizando actualmente el SSID.
Seguridad	Muestra el modo de seguridad del SSID.
Portal	Muestra si la función de portal está habilitada en el SSID.
ID de VLAN	Muestra el ID de VLAN del SSID.
Red de invitados	La visualización de la red de invitados está habilitada en el SSID.
Abajo (Byte)	Muestra el tráfico total de descarga desde que la red Wi-Fi (SSID) comenzó a funcionar.
Arriba (Byte)	Muestra el tráfico total de subida desde que la red Wi-Fi (SSID) comenzó a funcionar.

Supervise la configuración de la radio.

Puede monitorear la configuración de radio del EAP. La siguiente figura publicada en el

En esta introducción se toma como ejemplo la frecuencia de 2,4 GHz.

Radio Settings	
2.4GHz 5GHz	
2.4GHz Wireless Radio:	Enable
Channel Frequency:	6 / 2437MHz
Channel Width:	20/40MHz
IEEE802.11 Mode:	b/g/n mixed
Max TX Rate:	300.0Mbps
Tx Power:	20dBm

La siguiente tabla presenta la información que se muestra en el EAP.

radio inalámbrica	Indica si la función inalámbrica está habilitada en la banda de radio.
Frecuencia del canal	Muestra el canal y la frecuencia que está utilizando actualmente el EAP.
Ancho del canal	Muestra el ancho de canal que está utilizando actualmente el EAP.
Modo IEEE802.11	Muestra el protocolo IEEE802.11 que utiliza actualmente el EAP.
Tasa máxima de transmisión	Muestra la velocidad física máxima del EAP.
Potencia de transmisión	Muestra la potencia de transmisión del EAP.

Monitorear el tráfico de radio

Puede monitorizar el tráfico de radio del EAP. La siguiente figura, que aparece en la introducción, toma como ejemplo la frecuencia de 2,4 GHz de un dispositivo de doble banda.

Radio Traffic			
2.4GHz 5GHz			
Rx Packets:	82874437	Tx Packets:	8800930
Rx Bytes:	20906526476	Tx Bytes:	1990845129
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	65

Se muestra la siguiente información de tráfico de la radio:

Paquetes Rx	Muestra el número total de paquetes recibidos en la banda actual desde que se inició el EAP.
-------------	--

Paquetes de transmisión	Muestra el número total de paquetes enviados en la banda actual desde que se inició el EAP.
Bytes Rx	Muestra el tráfico total recibido en la banda actual desde que se inició el EAP. arriba.
Bytes de transmisión	Muestra el tráfico total enviado en la banda actual desde que se inició el EAP.
Rx eliminado Paquetes	Muestra el número total de paquetes descartados que se reciben en la banda actual desde que se inicia el EAP.
Tx caído Paquetes	Muestra el número total de paquetes descartados que se envían en la banda actual desde que se inicia el EAP.
Errores de Rx	Muestra el número total de paquetes de error recibidos en la banda actual desde que se inició el EAP.
Errores de transmisión	Muestra el número total de paquetes de error que se envían en la banda actual desde que se inicia el EAP.

Monitorear el tráfico de la LAN

Puedes ver el tráfico LAN de EAP.

LAN Traffic			
Rx Packets:	559223	Tx Packets:	206607
Rx Bytes:	320073875	Tx Bytes:	204207153
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	0

A continuación se muestra la información de tráfico de la LAN:

Paquetes Rx	Muestra el número total de paquetes recibidos en la LAN desde que se inició el EAP.
Paquetes de transmisión	Muestra el número total de paquetes enviados en la LAN desde que se inició el EAP. arriba.
Bytes Rx	Muestra el tráfico total recibido en la LAN desde que se inició el EAP.
Bytes de transmisión	Muestra el tráfico total enviado en la LAN desde que se inició el EAP.
Rx eliminado Paquetes	Muestra el número total de paquetes descartados que recibe el EAP desde su inicio.
Tx caído Paquetes	Muestra el número total de paquetes descartados que envía el EAP desde su inicio.

Errores de Rx

Muestra el número total de paquetes de error recibidos desde que se inició el EAP.

Errores de transmisión

Muestra el número total de paquetes de error enviados desde que se inició el EAP.

3.3 Monitorear a los clientes

Puede supervisar la información de los clientes conectados al EAP.

Para consultar la información del cliente, vaya a la página Estado > Cliente.

The screenshot shows the TP-Link web interface. At the top, there are navigation tabs: Status (highlighted), Wireless, Management, and System. Below these, there are sub-tabs: Device, Wireless, and Client (highlighted). The main content area is titled 'Client List' and has two tabs: 'User' (selected) and 'Guest'. A table lists client information with columns: ID, Hostname, IP Address, MAC Address, Band, SSID, Active Time, Up (Byte), Down (Byte), RSSI (dBm), Rate (Mbps), and Action. One client is listed with ID 1, Hostname 'iPhone', IP 192.168.1.100, and MAC D0-A6-37-83-DA-99. Below this is the 'Block Client List' section, which has a table with columns: ID, Hostname, MAC Address, Up (Byte), Down (Byte), and Action. One blocked client is listed with ID 1, Hostname 'android-6532c20e9aa005cc', and MAC 1C-77-F6-91-C7-B8.

Ver información del cliente

Hay dos tipos de clientes: usuarios e invitados autenticados por portal. Los usuarios son los clientes que se conectan al SSID con la autenticación por portal deshabilitada. Los invitados son los clientes que Conéctese a la red Wi-Fi (SSID) con la autenticación de portal habilitada.

Haga clic para seleccionar los tipos de clientes para ver la información del EAP. en la siguiente figura publicada en la introducción, que toma al usuario como ejemplo.

This screenshot shows a detailed view of the 'Client List' table. The 'User' tab is selected. The table has the following data for the first row:

ID	Hostname	IP Address	MAC Address	Band	SSID	Active Time	Up (Byte)	Down (Byte)	RSSI (dBm)	Rate (Mbps)	Action
1	iPhone	192.168.1.100	D0-A6-37-83-DA-99	5GHz	SSID-2	0 days 00:00:07	4k	1k	-80	175.0	[Refresh] [Close]

Se muestra la siguiente información del cliente:

nombre de host	Muestra el nombre de host del usuario.
Dirección IP	Muestra la dirección IP del usuario.

Dirección MAC	Muestra la dirección MAC del usuario.
Banda	Muestra la banda de frecuencia en la que está trabajando el usuario.
SSID	Muestra el SSID al que se está conectando el usuario.
Tiempo activo	Muestra cuánto tiempo ha estado conectado el usuario a la red Wi-Fi (SSID).
Arriba (Byte)	Muestra el tráfico total subido por el usuario al EAP desde la última conexión.
Abajo (Byte)	Muestra el tráfico total descargado por el usuario desde el EAP desde la última conexión.
RSSI (dBm)	Muestra el RSSI (Indicador de Intensidad de Señal Recibida) del usuario.
Velocidad (Mbps)	Muestra la velocidad de transmisión inalámbrica del usuario.

Puede ejecutar la operación correspondiente en el EAP haciendo clic en un icono de la columna Acción.



Haz clic en el icono para configurar el límite de velocidad del cliente y así equilibrar el uso del ancho de banda. Introduce el límite de descarga y el límite de subida y haz clic en Aceptar.

Al configurar los SSID, puede limitar la velocidad de descarga y carga para cada cliente que se conecte a SSID específicos; consulte la documentación para obtener más detalles. **2.1.1**

Configurar SSID

Tenga en cuenta que la velocidad de descarga y carga se limitará al valor menor si establece el valor límite tanto en la configuración del SSID como en la del cliente.

Rate Limit: Enable i

Download Limit: Kbps (1-10240000)

Upload Limit: Kbps (1-10240000)

OK




Haz clic en el icono para bloquear el acceso del cliente a la red.

Ver información del cliente de Block

Puede ver la información de los clientes que han sido bloqueados y reanudar el cliente acceso.

Block Client List					
ID	Hostname	MAC Address	Up (Byte)	Down (Byte)	Action
1	android-6532c20e9aa005cc	1C-77-F6-91-C7-B8	3k	1k	 Refresh 

Se muestra la siguiente información del cliente bloqueado:

nombre de host	Muestra el nombre de host del usuario.
Dirección MAC	Muestra la dirección MAC del usuario.
Arriba (Byte)	Muestra el tráfico total subido por el usuario al EAP desde la última conexión.
Abajo (Byte)	Muestra el tráfico total descargado por el usuario desde el EAP desde la última conexión.
Acción	Puedes hacer clic en el  para restablecer el acceso del cliente a Internet.

4

Gestionar el

Programa de asistencia al empleado (EAP)

El EAP proporciona potentes funciones de gestión y mantenimiento de dispositivos.

Este capítulo presenta cómo gestionar el programa de asistencia al empleado (PAE), incluyendo:

- 4.1 Administrar los AP puente (solo para un AP principal puente)
- 4.2 Gestionar la dirección IP del EAP
- 4.3 Administrar registros
- 4.4 Configurar el servidor web
- 4.5 Configurar el acceso de administración
- 4.6 Mantener el sistema (solo para ciertos dispositivos)
- 4.7 Configurar LED
- 4.8 Configurar el control Wi-Fi (solo para ciertos dispositivos)
- 4.9 Configurar salida PoE (solo para ciertos dispositivos)
- 4.10 Configurar SSH
- 4.11 Configurar SNMP
- 4.12 Configurar el guardado (solo para ciertos dispositivos)

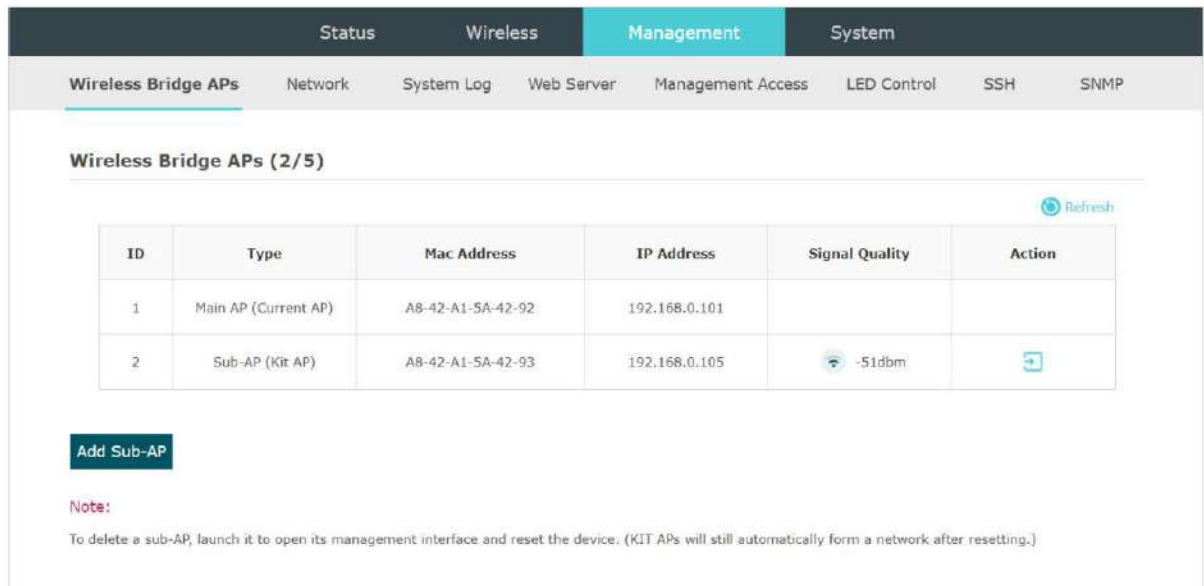
4.1 Administrar los AP puente (solo para un AP principal puente)

Si su producto es un kit Bridge, puede ver y administrar los AP Bridge de forma centralizada en la página principal.

Página web de AP.

Vaya a la página Administración > Puntos de acceso de puente inalámbrico. El sistema muestra automáticamente


El AP principal y los AP secundarios incluidos en el kit.



The screenshot shows a web interface with a navigation bar at the top containing 'Status', 'Wireless', 'Management' (highlighted), and 'System'. Below the navigation bar is a sub-menu with 'Wireless Bridge APs' (highlighted), 'Network', 'System Log', 'Web Server', 'Management Access', 'LED Control', 'SSH', and 'SNMP'. The main content area is titled 'Wireless Bridge APs (2/5)' and features a table with the following data:

ID	Type	Mac Address	IP Address	Signal Quality	Action
1	Main AP (Current AP)	A8-42-A1-5A-42-92	192.168.0.101		
2	Sub-AP (Kit AP)	A8-42-A1-5A-42-93	192.168.0.105	-51dbm	

Below the table is a button labeled 'Add Sub-AP'. A 'Note:' section follows, stating: 'To delete a sub-AP, launch it to open its management interface and reset the device. (KIT APs will still automatically form a network after resetting.)' There is also a 'Refresh' button in the top right corner of the table area.

Para una entrada Sub-AP, puede hacer clic aquí.  para lanzar su página web.

Si desea agregar otros puntos de acceso, haga clic en el botón Agregar sub-AP y siga las instrucciones web para agregarlos.

4.2 Gestionar la dirección IP del EAP

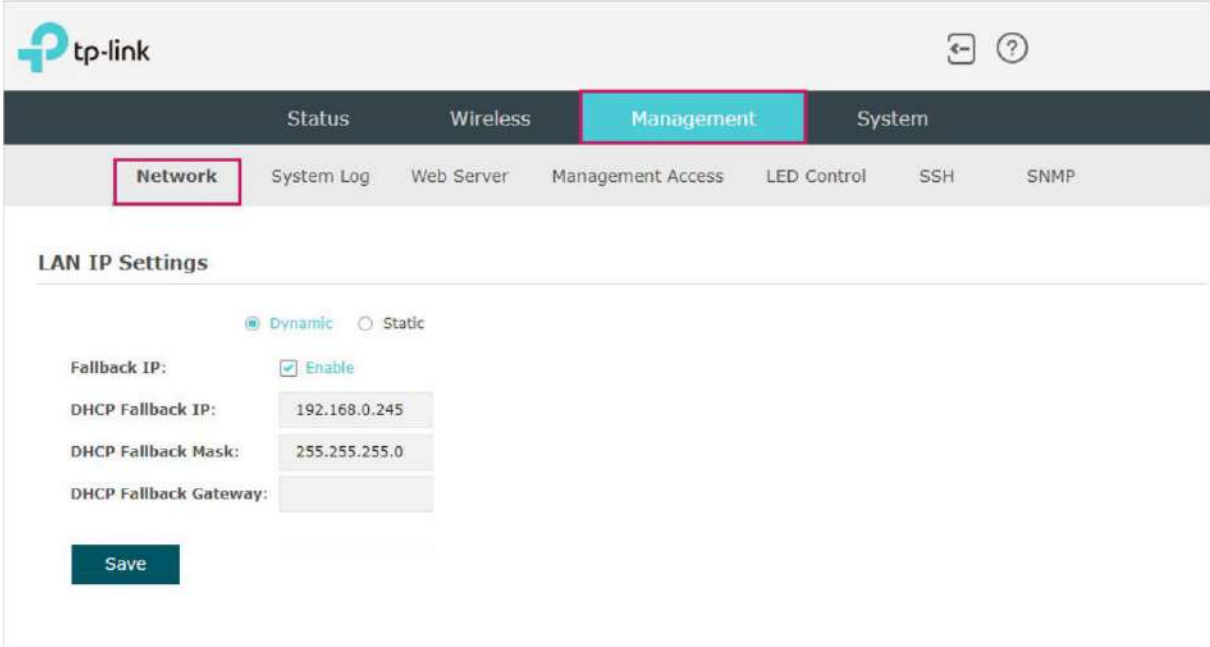
La dirección IP del EAP puede ser una dirección IP dinámica asignada por el servidor DHCP o una dirección IP estática especificada manualmente por usted. Por defecto, el EAP obtiene una dirección IP dinámica del servidor DHCP. También puede especificar una dirección IP estática según sus preferencias.

necesidades.

Consejos:

Para obtener una introducción detallada sobre cómo encontrar la dirección IP dinámica del EAP, consulte [Usando Web Navegador Su PC y Conectando con el Ethernet](#) .

Para configurar la dirección IP del EAP, vaya a la página Administración > Red.



The screenshot shows the TP-Link web management interface. At the top, there is a navigation bar with tabs for Status, Wireless, Management (highlighted in red), and System. Below this, a sub-menu includes Network (highlighted in red), System Log, Web Server, Management Access, LED Control, SSH, and SNMP. The main content area is titled 'LAN IP Settings'. It features two radio buttons: 'Dynamic' (selected) and 'Static'. Below these are several input fields: 'Fallback IP' with a checked 'Enable' checkbox, 'DHCP Fallback IP' with the value '192.168.0.245', 'DHCP Fallback Mask' with the value '255.255.255.0', and 'DHCP Fallback Gateway' which is currently empty. A 'Save' button is located at the bottom left of the settings area.

Siga los pasos que se indican a continuación para configurar la dirección IP del EAP:

1. Elija el modo de dirección IP que desee: Dinámico o Estático.
2. Configure los parámetros correspondientes según su selección.

- Dinámico

Si selecciona Dinámico como modo de dirección IP, asegúrese de que haya un servidor DHCP accesible en su red y que dicho servidor esté configurado correctamente para asignar la dirección IP y los demás parámetros de red al EAP.

The screenshot shows a configuration window for Dynamic IP mode. At the top, there are two radio buttons: 'Dynamic' (selected) and 'Static'. Below this, there are four fields: 'Fallback IP:' with a checked 'Enable' checkbox; 'DHCP Fallback IP:' with the value '192.168.0.245'; 'DHCP Fallback Mask:' with the value '255.255.255.0'; and 'DHCP Fallback Gateway:' which is currently empty.

Para garantizar la estabilidad de la red, también puede configurar los parámetros de IP de reserva para el EAP:

IP de respaldo	Con la IP de reserva configurada, si el EAP no logra obtener una dirección IP de un servidor DHCP en 10 segundos, la IP de reserva funcionará como la dirección IP del EAP. Sin embargo, después de eso, el EAP seguirá intentando obtener una dirección IP del servidor DHCP hasta que lo consiga.
IP de reserva DHCP	Especifique una dirección IP de reserva para el EAP. Asegúrese de que esta dirección IP no esté siendo utilizada por ningún otro dispositivo en la misma LAN. La dirección IP de reserva DHCP predeterminada es 192.168.0.254.
Máscara de IP de reserva DHCP	Especifique la máscara de red de la IP de reserva. DHCP predeterminado La máscara de IP de reserva es 255.255.255.0.
Puerta de enlace de reserva DHCP	Especifique la puerta de enlace de red.

- Estático

Si selecciona Estática como modo de dirección IP, deberá especificar manualmente una dirección IP y los parámetros de red correspondientes para el EAP. Asegúrese de que la dirección IP especificada no esté siendo utilizada por ningún otro dispositivo en la misma LAN.

The screenshot shows a configuration window for Static IP mode. At the top, there are two radio buttons: 'Dynamic' and 'Static' (selected). Below this, there are five fields: 'IP Address:' with the value '192.168.0.245'; 'IP Mask:' with the value '255.255.255.0'; 'Gateway:' with the value '0.0.0.0'; 'Primary DNS:' with the value '192.168.0.1'; and 'Secondary DNS:' with the value '0.0.0.0' and '(Optional)' next to it.

Configure la dirección IP y los parámetros de red como se muestra en la siguiente tabla:

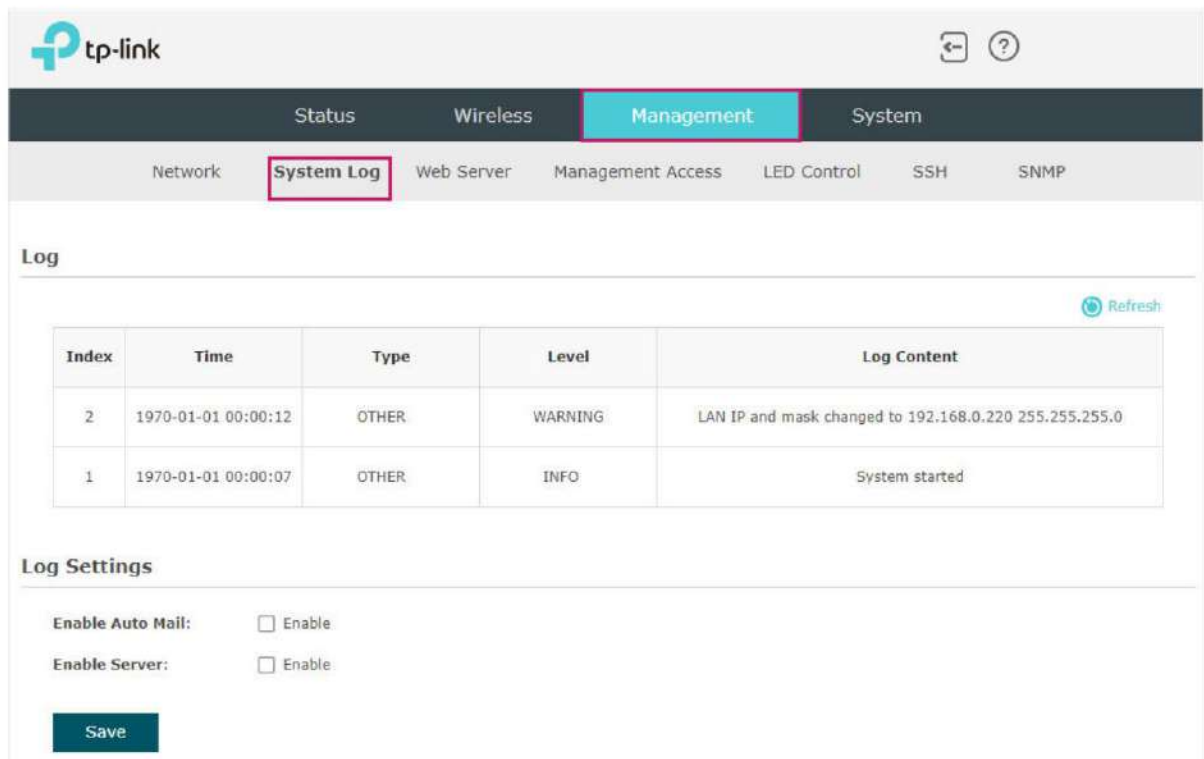
Dirección IP	Especifique una dirección IP estática para el EAP.
Máscara IP	Especifique la máscara de red.
Puerta	Especifique la puerta de enlace de red.
DNS principal	Especifique el servidor DNS principal.
DNS secundario:	Especifique el servidor DNS secundario. (Opcional)

3. Haga clic en Guardar.

4.3 Administrar los registros del sistema

Los registros del sistema almacenan información sobre el hardware, el software y los problemas del sistema, además de supervisar los eventos del mismo. Gracias a los registros del sistema, puede conocer el estado de funcionamiento del sistema y detectar las causas de los fallos.

Para administrar los registros del sistema, vaya a la página Administración > Registro del sistema.



The screenshot shows the TP-Link web interface. The top navigation bar includes 'Status', 'Wireless', 'Management' (highlighted), and 'System'. Below this, a secondary navigation bar contains 'Network', 'System Log' (highlighted with a red box), 'Web Server', 'Management Access', 'LED Control', 'SSH', and 'SNMP'. The main content area is titled 'Log' and features a 'Refresh' button. A table displays the following log entries:

Index	Time	Type	Level	Log Content
2	1970-01-01 00:00:12	OTHER	WARNING	LAN IP and mask changed to 192.168.0.220 255.255.255.0
1	1970-01-01 00:00:07	OTHER	INFO	System started

Below the table is the 'Log Settings' section, which includes two checkboxes: 'Enable Auto Mail' and 'Enable Server', both currently unchecked. A 'Save' button is located at the bottom of this section.

En esta página, puede ver los registros del sistema y configurar la forma en que los recibe.

Ver registros del sistema

En la sección Registro, puede hacer clic  Refresh para actualizar los registros y verlos en la tabla.

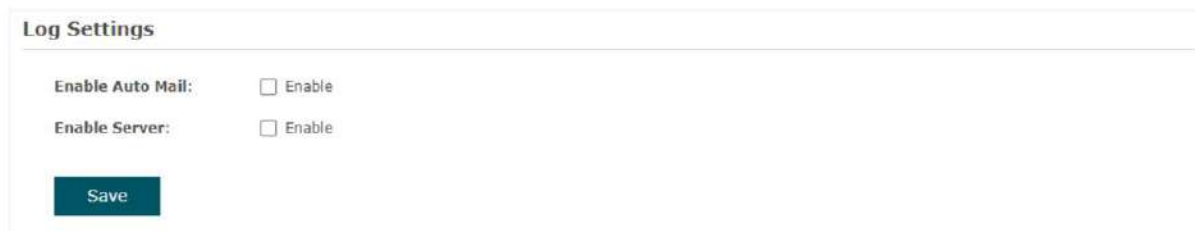


The screenshot shows the 'Log' section of the TP-Link web interface. It features a 'Refresh' button and a table with the following data:

Index	Time	Type	Level	Log Content
2	1970-01-01 00:00:12	OTHER	WARNING	LAN IP and mask changed to 192.168.0.220 255.255.255.0
1	1970-01-01 00:00:07	OTHER	INFO	System started

Configurar la forma de recibir los registros

En la sección Configuración de registros, puede configurar las formas en que se reciben los registros del sistema.



Log Settings

Enable Auto Mail: Enable

Enable Server: Enable

Save

Siga los pasos que se indican a continuación para configurar esta función:

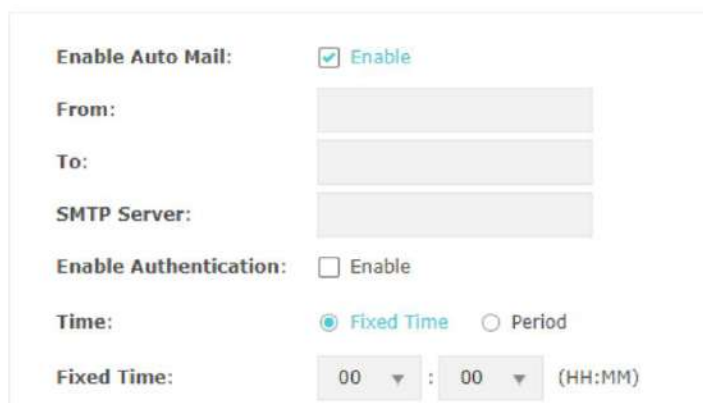
1. Marque la casilla correspondiente para habilitar una o más formas de recibir registros del sistema, y configurar los parámetros relacionados. Hay dos maneras disponibles: [Auto](#) [Correo y Servidor](#).

■ Correo automático

Si la opción Correo automático está configurada, los registros del sistema se enviarán a un buzón de correo específico. Marque la casilla para habilitar la función y configurar los parámetros relacionados.

Nota:

Actualmente, el cifrado SSL no es compatible.



Enable Auto Mail: Enable

From:

To:

SMTP Server:

Enable Authentication: Enable

Time: Fixed Time Period

Fixed Time: : (HH:MM)

La siguiente tabla muestra cómo configurar estos parámetros:

De	Introduzca la dirección de correo electrónico del remitente.
A	Introduzca la dirección de correo electrónico del destinatario.
Servidor SMTP	Introduzca la dirección IP del servidor SMTP del remitente. Nota: Actualmente, el nombre de dominio del servidor SMTP no es compatible con este campo.
Permitir Autenticación	Si el buzón del remitente está configurado con Puede marcar la casilla para habilitar la autenticación del servidor de correo. Ingrese el nombre de usuario y la contraseña del remitente.

Modo de tiempo	<p>Seleccione el modo de hora: Hora fija o Hora periódica.</p> <p>Hora fija significa que los registros del sistema se enviarán a una hora específica todos los días. Hora periódica significa que los registros del sistema se enviarán a intervalos de tiempo específicos.</p>
Tiempo fijo	<p>Si selecciona Hora fija, especifique una hora fija para el envío de los correos electrónicos de registro del sistema. Por ejemplo, 08:30 indica que el correo se enviará a las 8:30 de la mañana todos los días.</p>
Período de tiempo	<p>Si selecciona Período de tiempo, especifique un intervalo de tiempo para enviar periódicamente el correo electrónico de registro del sistema. Por ejemplo, 6 indica que el correo se enviará cada seis horas.</p>

■ Servidor

Si el servidor está configurado, los registros del sistema se enviarán al servidor de registros del sistema especificado, y podrá utilizar el software syslog para ver los registros en el servidor.

Habilite esta función e introduzca la dirección IP y el puerto del servidor de registro del sistema.

Enable Server: **Enable**

System Log Server IP:

System Log Server Port:

More Client Detail Log: **Enable**

Dirección IP del servidor de registro del sistema	Introduzca la dirección IP del servidor.
Puerto del servidor de registro del sistema	Introduzca el puerto del servidor.
Registro de detalles del cliente	Con la opción habilitada, los registros de los clientes se enviarán a la servidor.


2. Haz clic en Guardar.

4.4 Configurar el servidor web

Con el servidor web, puede iniciar sesión en la página web de administración del EAP. Puede configurar los parámetros del servidor web de EAP según sus necesidades.

Para configurar el servidor web, vaya a la página Administración > Servidor web.

Web Server

Secure Server Port:	<input type="text" value="443"/>
Server Port:	<input type="text" value="80"/>
Session Timeout:	<input type="text" value="15"/> minutes
Layer-3 Accessibility:	<input type="checkbox"/> Enable
TLS Version 1.0/1.1:	<input type="checkbox"/> Enable 

Note:
Please enter the EAP's IP address to access the web-based configuration utility via an HTTPS connection.

Siga los pasos que se indican a continuación para configurar el servidor web:

1. Consulte la siguiente tabla para configurar los parámetros:

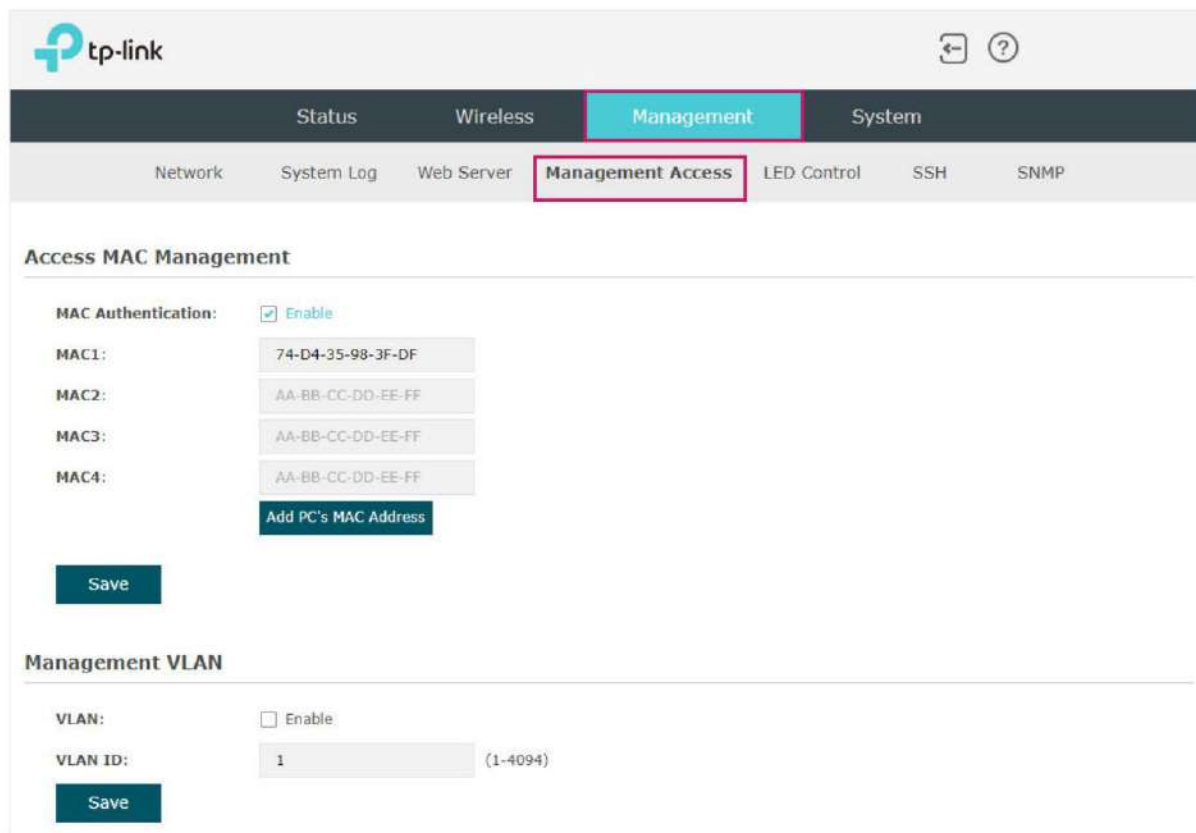
Puerto de servidor seguro	Designe un puerto de servidor seguro para el servidor web en modo HTTPS. Por defecto, el puerto es el 443.
Puerto del servidor	Especifique un puerto de servidor para el servidor web en modo HTTP. Por defecto, el puerto es el 80.
Tiempo de espera de la sesión	Establezca el tiempo de espera de la sesión. Si no realiza ninguna acción en la página web dentro de ese plazo, el sistema cerrará la sesión automáticamente. Puede volver a iniciar sesión si desea regresar a la página web.
Capa 3 Accesibilidad	Con esta función activada, los dispositivos de una subred diferente pueden acceder a los dispositivos gestionados por Omada a través de la página web de administración. Con esta función desactivada, solo los dispositivos de la misma subred pueden acceder a los dispositivos gestionados por Omada a través de la página web de administración.
Versión TLS 1.0/1.1	La página de administración de EAP utiliza TLS v1.2 de forma predeterminada. Puede habilitar esta función si prefiere TLS v1.0/1.1. Esta función solo está disponible en determinados dispositivos. Para comprobar si su dispositivo es compatible con esta función, consulte la interfaz web.

2. Haz clic en Guardar.

4.5 Configurar el acceso de administración

De forma predeterminada, todos los hosts de la LAN pueden iniciar sesión en la página web de administración del EAP con el nombre de usuario y la contraseña correctos. Para controlar el acceso de los hosts a la página web del EAP, puede especificar las direcciones MAC y la VLAN de administración de los hosts autorizados a acceder a ella.

Para configurar el acceso de administración, vaya a la página Administración > Acceso de administración.

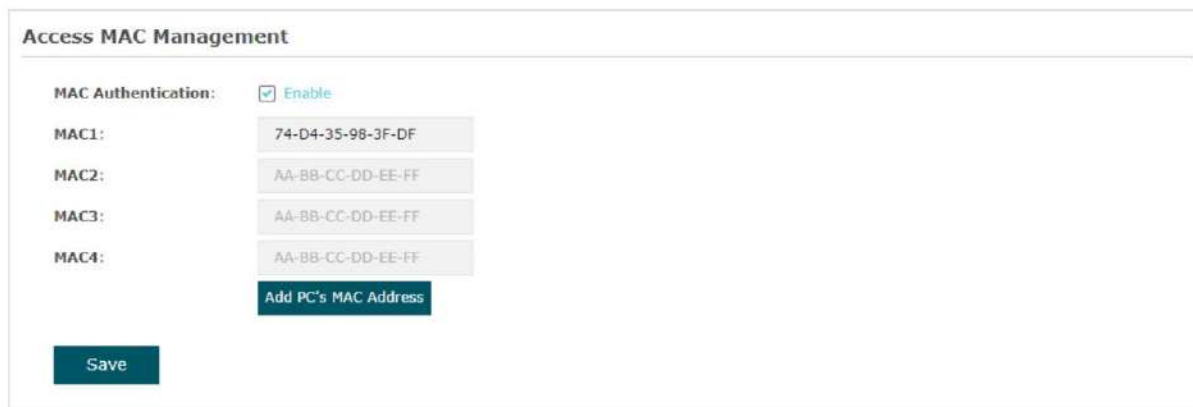


The screenshot shows the TP-Link web management interface. The top navigation bar includes 'Status', 'Wireless', 'Management' (highlighted in blue), and 'System'. Below this, a sub-menu contains 'Network', 'System Log', 'Web Server', 'Management Access' (highlighted in red), 'LED Control', 'SSH', and 'SNMP'. The main content area is titled 'Access MAC Management' and contains two sections:

- Access MAC Management:** This section has a 'MAC Authentication' checkbox checked and labeled 'Enable'. Below it are four input fields for MAC addresses: 'MAC1:' (74-D4-35-98-3F-DF), 'MAC2:' (AA-BB-CC-DD-EE-FF), 'MAC3:' (AA-BB-CC-DD-EE-FF), and 'MAC4:' (AA-BB-CC-DD-EE-FF). A button labeled 'Add PC's MAC Address' is located below these fields. A 'Save' button is at the bottom of this section.
- Management VLAN:** This section has a 'VLAN' checkbox unchecked and labeled 'Enable'. Below it is a 'VLAN ID' input field containing the number '1' and a range '(1-4094)'. A 'Save' button is at the bottom of this section.

Configurar la administración de MAC de acceso

Solo los hosts con las direcciones MAC específicas tienen permitido acceder a la página web, y otros hosts sin direcciones MAC especificadas no tienen permitido acceder a la página web.



This screenshot shows a close-up of the 'Access MAC Management' configuration page. It displays the 'MAC Authentication' checkbox checked and labeled 'Enable'. Below it are four input fields for MAC addresses: 'MAC1:' (74-D4-35-98-3F-DF), 'MAC2:' (AA-BB-CC-DD-EE-FF), 'MAC3:' (AA-BB-CC-DD-EE-FF), and 'MAC4:' (AA-BB-CC-DD-EE-FF). A button labeled 'Add PC's MAC Address' is located below these fields. A 'Save' button is at the bottom of this section.

Siga los pasos que se indican a continuación para configurar el acceso de administración en esta página:

1. Marque la casilla para habilitar la autenticación MAC.
2. Especifique una o más direcciones MAC en los campos MAC1/MAC2/MAC3/MAC4. Hasta Se pueden añadir cuatro direcciones MAC.
3. Haga clic en Guardar.

Consejos:

- Puedes hacer clic **Add PC's MAC Address** Para agregar rápidamente la dirección MAC del host en el que ha iniciado sesión actualmente, .
- Verifique cuidadosamente las direcciones MAC. Una vez guardada la configuración, solo los hosts incluidos en la lista de direcciones MAC podrán acceder a la página web del EAP.
- Si no puede iniciar sesión en la página web después de guardar la configuración incorrecta, puede restablecer el EAP a los valores predeterminados de fábrica y usar el nombre de usuario y la contraseña predeterminados (ambos admin) para iniciar sesión.

Configurar VLAN de administración

La VLAN de administración proporciona un método más seguro para administrar el EAP. Con la VLAN de administración habilitada, solo los hosts que se encuentran dentro de la VLAN de administración pueden acceder a la página web del EAP.

Dado que la mayoría de los hosts no pueden procesar las etiquetas VLAN, puede conectar el host de administración a la red a través de un conmutador y configurar los ajustes VLAN correctos para los conmutadores de la red para garantizar la comunicación entre el host y el EAP en la VLAN de administración.

Management VLAN

VLAN: Enable

VLAN ID: (1-4094)

Save

Siga los pasos que se indican a continuación para configurar la VLAN de administración en esta página:

1. Marque la casilla para habilitar la VLAN de administración.
2. Especifique el ID de VLAN de la VLAN de administración. Solo los hosts en la Administración Los usuarios de VLAN pueden iniciar sesión en el EAP a través del puerto Ethernet.
3. Haga clic en Guardar.

4.6 Configurar el enlace troncal (solo para ciertos dispositivos)

La función de enlace troncal puede agrupar varios enlaces Ethernet en un enlace lógico para aumentar ancho de banda y mejorar la fiabilidad de la red.

Para configurar la función de enlace troncal, vaya a la página Administración > Enlace troncal.

Trunk Settings

Enable: Enable

Mode: SRC MAC+DST MAC ▼

Save

Permitir

Marque la casilla para habilitar la función.

Modo

Seleccione el modo de algoritmo troncal. Según el modo de algoritmo seleccionado, el punto de acceso determina qué puerto físico se utiliza para enviar el paquete recibido.

MAC de origen + MAC de destino: El punto de acceso determina el puerto de salida en función de las direcciones MAC de origen y destino del paquete.

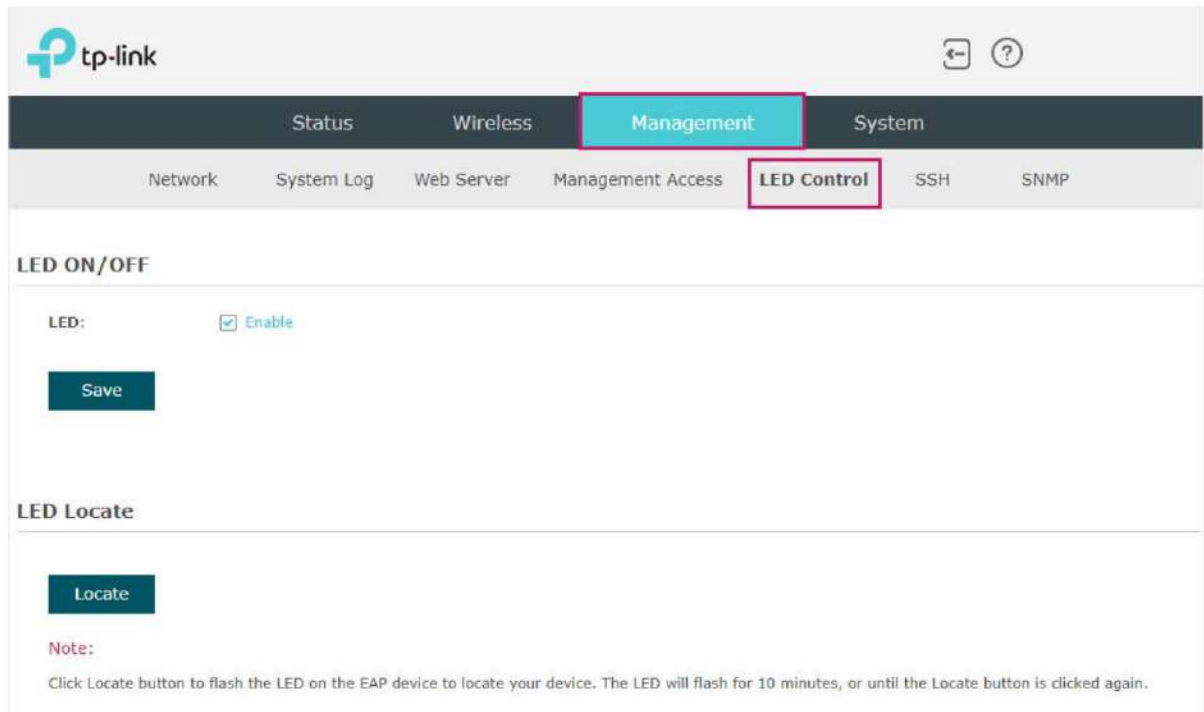
DST MAC: El punto de acceso determina el puerto de salida en función de la dirección MAC de destino del paquete.

MAC de origen: El punto de acceso determina el puerto de salida en función de la dirección MAC de origen del paquete.

4.7 Configurar LED

Puedes encender o apagar la luz LED del EAP y hacer parpadear el LED para localizar tu dispositivo.

Para configurar los LED, vaya a la página Gestión > Control de LED.



The screenshot shows the TP-Link web interface. At the top left is the TP-Link logo. The navigation menu includes 'Status', 'Wireless', 'Management' (highlighted in a red box), and 'System'. Below this, a secondary menu shows 'Network', 'System Log', 'Web Server', 'Management Access', 'LED Control' (highlighted in a red box), 'SSH', and 'SNMP'. The main content area is divided into two sections: 'LED ON/OFF' and 'LED Locate'. In the 'LED ON/OFF' section, there is a label 'LED:' followed by a checked checkbox and the text 'Enable'. Below this is a dark blue 'Save' button. The 'LED Locate' section contains a dark blue 'Locate' button. Below the 'Locate' button is a 'Note:' section with the text: 'Click Locate button to flash the LED on the EAP device to locate your device. The LED will flash for 10 minutes, or until the Locate button is clicked again.'

Marque la casilla para encender o apagar la luz LED del EAP y haga clic en Guardar. Para parpadear el LED, haga clic en Localizar. El LED parpadeará durante 10 minutos o hasta que se vuelva a pulsar el botón de localización de nuevo.

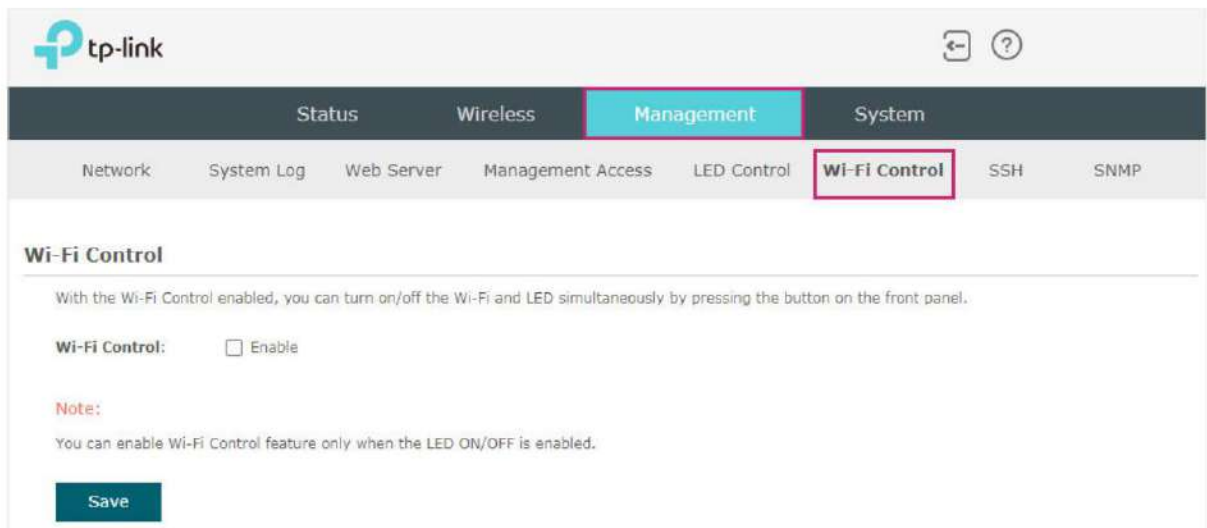
4.8 Configurar el control Wi-Fi (solo para ciertos dispositivos)

Nota:

El control Wi-Fi solo está disponible en ciertos dispositivos. Para comprobar si su dispositivo es compatible con esta función, consulte la interfaz web. Si el control Wi-Fi está disponible, encontrará la opción Administración > Control Wi-Fi en el menú.

Algunos dispositivos tienen un botón LED/Wi-Fi en el panel frontal. Con el control Wi-Fi habilitado, puedes pulsar el botón para encender o apagar tanto el Wi-Fi como el LED al mismo tiempo.

Para configurar el control de Wi-Fi, vaya a la página Administración > Control de Wi-Fi.



Marque la casilla para habilitar el control Wi-Fi y haga clic en Guardar.

Nota:

Solo puedes activar el control Wi-Fi cuando la opción LED ON/OFF esté habilitada.

4.9 Configurar la salida PoE (solo para ciertos dispositivos)

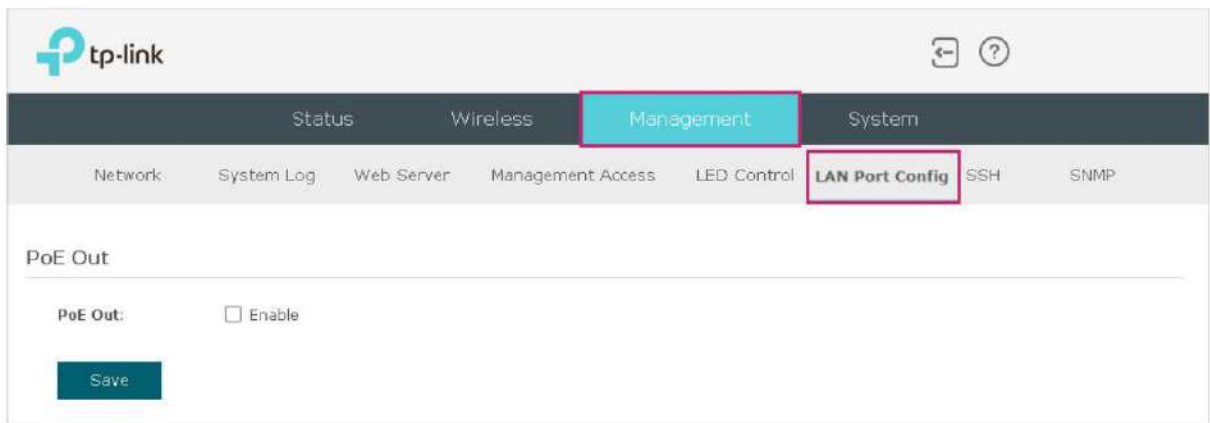
Nota:

La función PoE Out solo está disponible en ciertos dispositivos. Para comprobar si su dispositivo es compatible con esta función, consulte la interfaz web. Si PoE Out está disponible, encontrará la opción Administración > Configuración del puerto LAN en el menú.

Algunos dispositivos tienen un puerto PoE OUT que puede transmitir datos y suministrar energía al cliente.

Al mismo tiempo. También puede deshabilitar PoE Out para que el puerto solo transmita datos.

Para configurar la salida PoE, vaya a la página Administración > Configuración del puerto LAN.



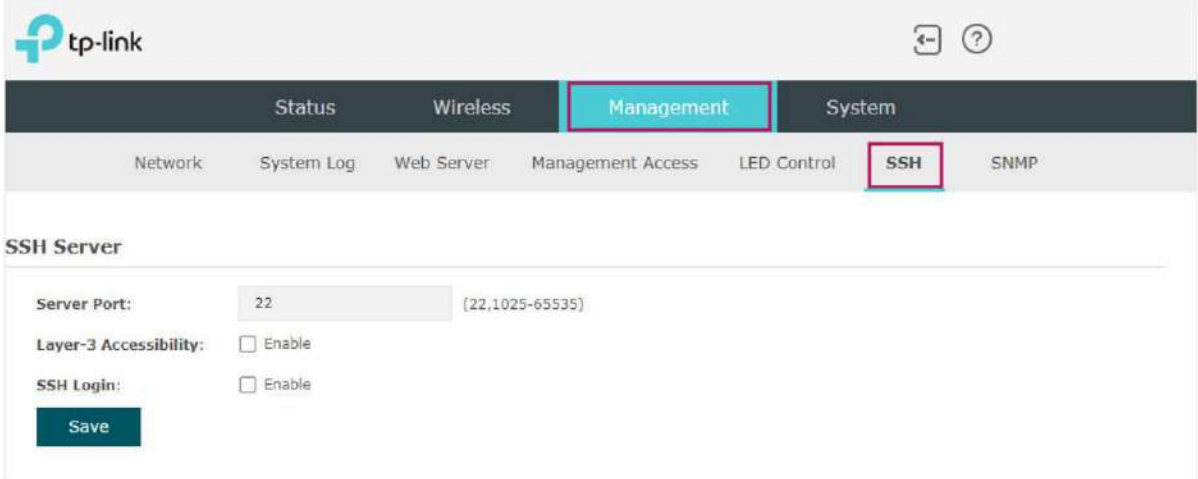
The screenshot shows the TP-Link web interface. At the top left is the TP-Link logo. The navigation menu includes Status, Wireless, Management (highlighted in blue), and System. Below this, a secondary menu shows Network, System Log, Web Server, Management Access, LED Control, LAN Port Config (highlighted with a red box), SSH, and SNMP. The main content area is titled 'PoE Out' and contains a 'PoE Out:' label followed by an unchecked checkbox labeled 'Enable'. A blue 'Save' button is located below the checkbox.

Marque la casilla para habilitar la salida PoE y haga clic en Guardar.

4.10 Configurar SSH

Si desea iniciar sesión de forma remota en el EAP a través de SSH, puede implementar un servidor SSH en su red y configurar la función SSH en el EAP.

Para configurar SSH, vaya a la página Administración > SSH.



The screenshot shows the TP-Link web interface. At the top, there is a navigation bar with tabs for 'Status', 'Wireless', 'Management', and 'System'. The 'Management' tab is active. Below this, there is a sub-navigation bar with options: 'Network', 'System Log', 'Web Server', 'Management Access', 'LED Control', 'SSH', and 'SNMP'. The 'SSH' option is highlighted with a red box. The main content area is titled 'SSH Server' and contains the following configuration options:

- Server Port:** A text input field containing '22' and a tooltip '(22,1025-65535)'.
- Layer-3 Accessibility:** A checkbox labeled 'Enable' which is currently unchecked.
- SSH Login:** A checkbox labeled 'Enable' which is currently unchecked.
- A dark blue 'Save' button.

Siga los pasos que se indican a continuación para configurar SSH en esta página:

1. Consulte la siguiente tabla para configurar los parámetros:

Puerto del servidor	Designa un puerto de servidor para SSH. Por defecto, el puerto es el 22.
Capa 3 Accesibilidad	Con esta función habilitada, los dispositivos de una subred diferente pueden acceder a los dispositivos administrados por Omada a través de SSH. Con esta función deshabilitada, solo los dispositivos de la misma subred pueden acceder a los dispositivos administrados por Omada a través de SSH.
Inicio de sesión SSH	Habilitar o deshabilitar el inicio de sesión SSH globalmente.

2. Haz clic en Guardar.

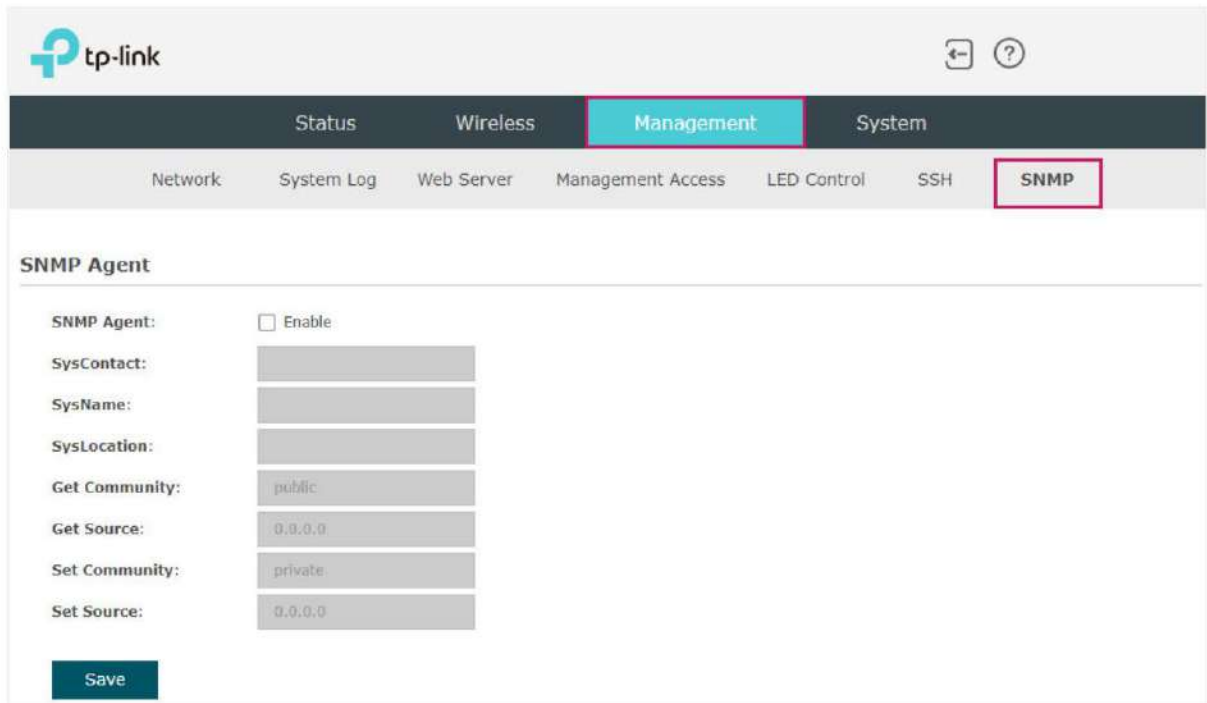
4.11 Configurar SNMP

El EAP se puede configurar como un agente SNMP y funcionar conjuntamente con el gestor SNMP.

Una vez que el EAP se convierte en un agente SNMP, puede recibir y procesar mensajes de solicitud del administrador SNMP.

Actualmente, el EAP es compatible con SNMP v1 y v2c.

Para configurar el EAP como agente SNMP, vaya a la página Administración > SNMP.



Siga los pasos que se indican a continuación para completar la configuración en esta página:

1. Marque la casilla para habilitar el agente SNMP.
2. Consulte la siguiente tabla para configurar los parámetros necesarios:

Contacto del sistema	Introduzca la identificación textual de la persona de contacto para este nodo gestionado.
Nombre del sistema	Introduzca un nombre asignado administrativamente para este nodo administrado.
Ubicación del sistema	Introduzca la ubicación física de este nodo administrado.
Obtener Comunidad.	Comunidad se refiere a un grupo anfitrión cuyo objetivo es la gestión de redes. El usuario Get Community solo tiene permisos de lectura para la información SNMP del dispositivo. El nombre de la comunidad puede considerarse una contraseña de grupo. La configuración predeterminada es pública.
Obtener fuente	Define la dirección IP (por ejemplo, 10.10.10.1) para los sistemas de administración que pueden servir como Get Community para leer la información SNMP de este dispositivo. El valor predeterminado es 0.0.0.0, lo que significa que todos los hosts pueden leer la información SNMP de este dispositivo.

La configuración de la comunidad otorga permisos de lectura y escritura a la información SNMP del dispositivo.

Introduzca el nombre de la comunidad que permite el acceso de lectura/escritura a dicha información. El nombre de la comunidad puede considerarse una contraseña de grupo. La configuración predeterminada es privada.

Establecer origen

Define la dirección IP (por ejemplo, 10.10.10.1) para los sistemas de administración que pueden servir como Set Community para leer y escribir la información SNMP de este dispositivo. El valor predeterminado es 0.0.0.0, lo que significa que todos los hosts Puede leer y escribir la información SNMP de este dispositivo.

3. Haga clic en Guardar.

Nota:

Definir una comunidad permite que los sistemas de gestión de la misma se comuniquen con el Agente SNMP. El nombre de la comunidad puede considerarse como la contraseña compartida del grupo de hosts de la red. Por lo tanto, para mayor seguridad, recomendamos modificar el nombre de la comunidad predeterminado antes de habilitar el servicio del Agente SNMP. Si el campo de comunidad está vacío, el Agente SNMP no responderá a ningún nombre de comunidad.

4.12 Configurar el ahorro de energía (solo para ciertos dispositivos)

El ahorro de energía puede reducir el consumo energético del punto de acceso.

Para configurar el ahorro de energía, vaya a la página Energía > Ahorro de energía.

Power Saving

Trigger by Time: Enable

Start Time: 00 : 00

End Time: 00 : 00

Note:
Enable Power Saving every day from 00:00 to 00:00.

Trigger by Band: Enable

Bands: - Please Select -

Idle Duration: 0

Note:
Enable Power Saving when there are no connections for 0 min on the no band(s).

Save

Activación por hora: Con esta opción habilitada, puede especificar la hora de inicio y finalización para activar el ahorro de energía todos los días dentro del período de tiempo establecido.

Desencadenado por Banda Con esta opción habilitada, puede especificar las bandas y la duración de inactividad para activar el ahorro de energía cuando no haya conexiones durante el tiempo especificado en las bandas.

5

Configurar el

Sistema

Este capítulo presenta cómo configurar el sistema EAP, incluyendo:

- 5.1 Configurar la cuenta de usuario
- 5.2 Configuración del controlador
- 5.3 Configurar el sistema
- 5.4 Reiniciar y restablecer el EAP
- 5.5 Copia de seguridad y restauración de la configuración
- 5.6 Actualizar el firmware

5.1 Configurar la cuenta de usuario

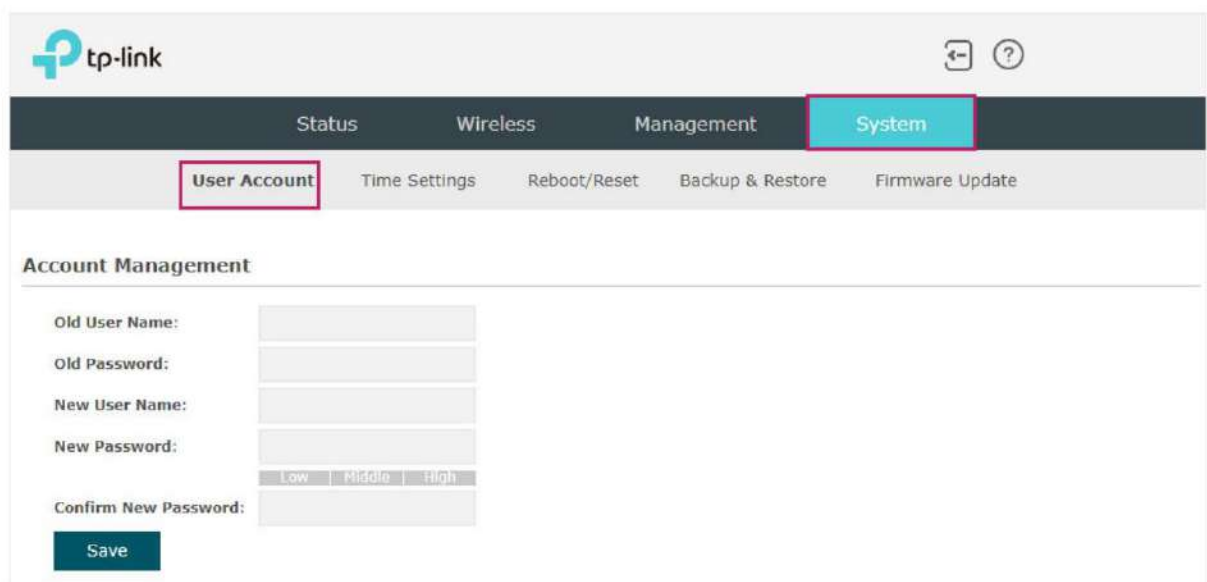
Cada EAP tiene una cuenta de usuario, que se utiliza para iniciar sesión en la página de administración del EAP.

Al iniciar sesión en el EAP por primera vez, el nombre de usuario y la contraseña de la cuenta de usuario son ambos "admin". Tras el primer inicio de sesión, el sistema le pedirá que establezca un nuevo nombre de usuario y una nueva contraseña para la cuenta. A continuación, podrá usar la nueva cuenta de usuario para iniciar sesión en el EAP. También puede cambiar su cuenta de usuario cuando lo necesite.

Consejos:

Recuerde bien su cuenta de usuario. Si la olvida, restablezca el EAP a la configuración de fábrica e inicie sesión con la cuenta de usuario predeterminada (tanto el nombre de usuario como la contraseña son "admin").

Para configurar la cuenta de usuario, vaya a Sistema > Cuenta de usuario.



The screenshot shows the TP-Link web interface. At the top left is the TP-Link logo. The navigation bar includes 'Status', 'Wireless', 'Management', and 'System' (highlighted in blue). Below this, a sub-menu contains 'User Account' (highlighted with a red box), 'Time Settings', 'Reboot/Reset', 'Backup & Restore', and 'Firmware Update'. The main content area is titled 'Account Management' and contains the following fields:

- Old User Name:
- Old Password:
- New User Name:
- New Password: with a strength indicator below it showing 'Low', 'Middle', and 'High'.
- Confirm New Password:

A 'Save' button is located at the bottom left of the form.

Sigue los pasos que se indican a continuación para cambiar tu cuenta de usuario en esta página:

1. Introduce el nombre de usuario y la contraseña antiguos de tu cuenta de usuario.
2. Especifique un nuevo nombre de usuario y una nueva contraseña para su cuenta de usuario. El sistema detectará automáticamente la seguridad de la contraseña que ingrese. Por seguridad, nosotros Le recomendamos que establezca una contraseña segura.
3. Vuelva a escribir la nueva contraseña.
4. Haga clic en Guardar.

5.2 Configuración del controlador

Para que el controlador adopte su EAP, asegúrese de que el controlador pueda detectar el EAP. La configuración del controlador permite que su EAP se detecte en cualquiera de los siguientes métodos: escenarios.

- Si está utilizando Omada Cloud-Based Controller, [Permitir Basado en la nube Controlador Gestión](#) .
- Si su EAP y controlador se encuentran en la misma red, LAN y VLAN, el controlador puede descubrir y adoptar el EAP sin ninguna configuración del controlador. De lo contrario, debe informar al EAP la URL/dirección IP del controlador, y una forma posible es: [Configurar Controlador Informar URL](#) .

Para obtener información detallada sobre todo el procedimiento, consulte la Guía del usuario del controlador Omada SDN. La guía se encuentra en el centro de descargas de nuestro sitio web oficial: <https://www.tp-link.com/support/download/>

Habilitar la gestión de controladores basada en la nube

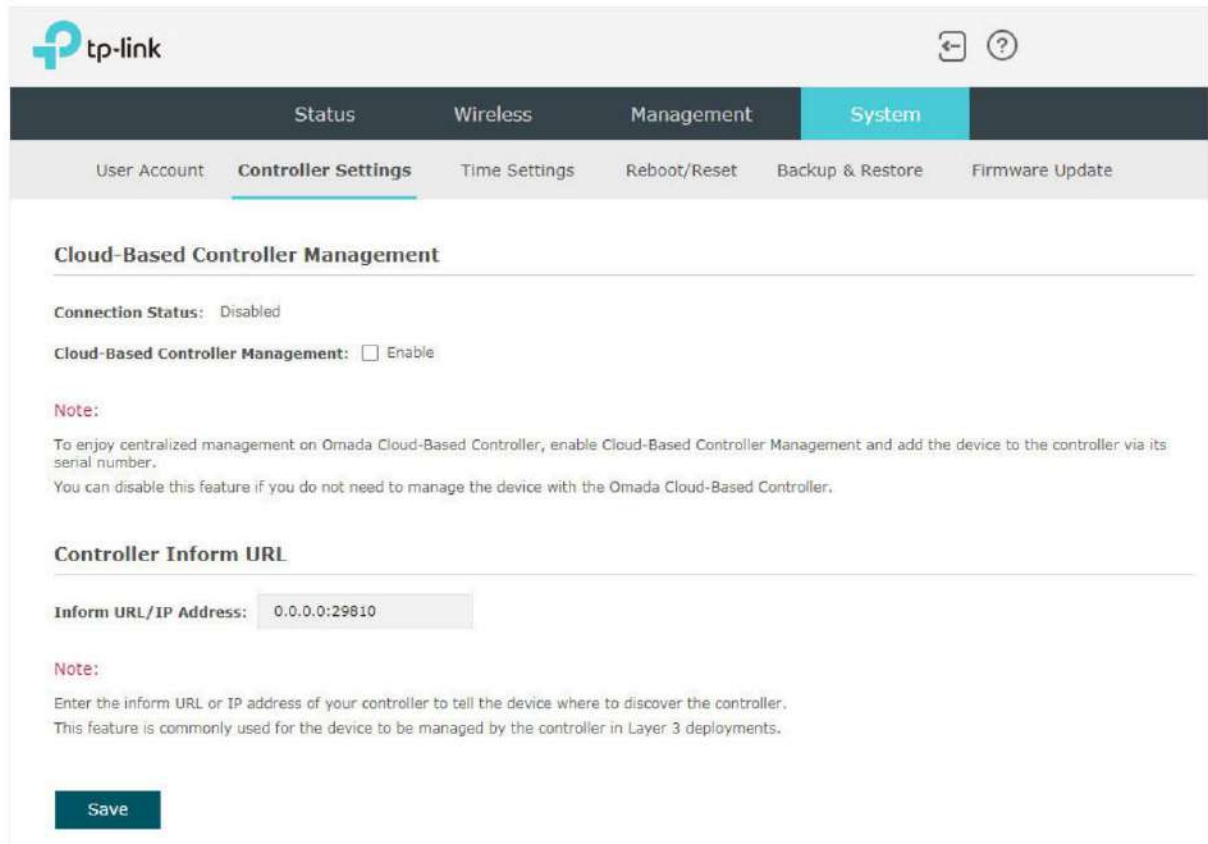
Vaya a la [página Sistema > Configuración del controlador](#) . En la administración del controlador basada en la nube sección, habilite la administración del controlador basada en la nube y haga clic en Guardar. Después de agregar el

EAP a su controlador basado en la nube de Omada, puede verificar el estado de la conexión en esta página.

The screenshot shows the TP-Link Omada controller web interface. At the top left is the TP-Link logo. The navigation bar includes 'Status', 'Wireless', 'Management', and 'System' (which is highlighted). Below this, a secondary navigation bar includes 'User Account', 'Controller Settings' (which is highlighted), 'Time Settings', 'Reboot/Reset', 'Backup & Restore', and 'Firmware Update'. The main content area is titled 'Cloud-Based Controller Management'. It shows 'Connection Status: Disabled' and 'Cloud-Based Controller Management: Enable'. A note states: 'To enjoy centralized management on Omada Cloud-Based Controller, enable Cloud-Based Controller Management and add the device to the controller via its serial number. You can disable this feature if you do not need to manage the device with the Omada Cloud-Based Controller.' Below this is the 'Controller Inform URL' section, which has a text input field for 'Inform URL/IP Address' containing '0.0.0.0:29810'. Another note says: 'Enter the inform URL or IP address of your controller to tell the device where to discover the controller. This feature is commonly used for the device to be managed by the controller in Layer 3 deployments.' At the bottom left of the main content area is a 'Save' button.

Configurar la URL de información del controlador

Vaya a la página Sistema > Configuración del controlador . En la sección URL de información del controlador, ingrese la URL/dirección IP del controlador en el EAP y haga clic en Guardar. Luego, el EAP se pondrá en contacto con el controlador para que el controlador pueda descubrir el EAP.



The screenshot shows the TP-Link Omada Controller Settings page. The top navigation bar includes the TP-Link logo and a user account icon. The main navigation tabs are Status, Wireless, Management, and System (highlighted). Below these are sub-tabs: User Account, Controller Settings (highlighted), Time Settings, Reboot/Reset, Backup & Restore, and Firmware Update.

Cloud-Based Controller Management

Connection Status: Disabled

Cloud-Based Controller Management: Enable

Note:
To enjoy centralized management on Omada Cloud-Based Controller, enable Cloud-Based Controller Management and add the device to the controller via its serial number.
You can disable this feature if you do not need to manage the device with the Omada Cloud-Based Controller.

Controller Inform URL

Inform URL/IP Address:

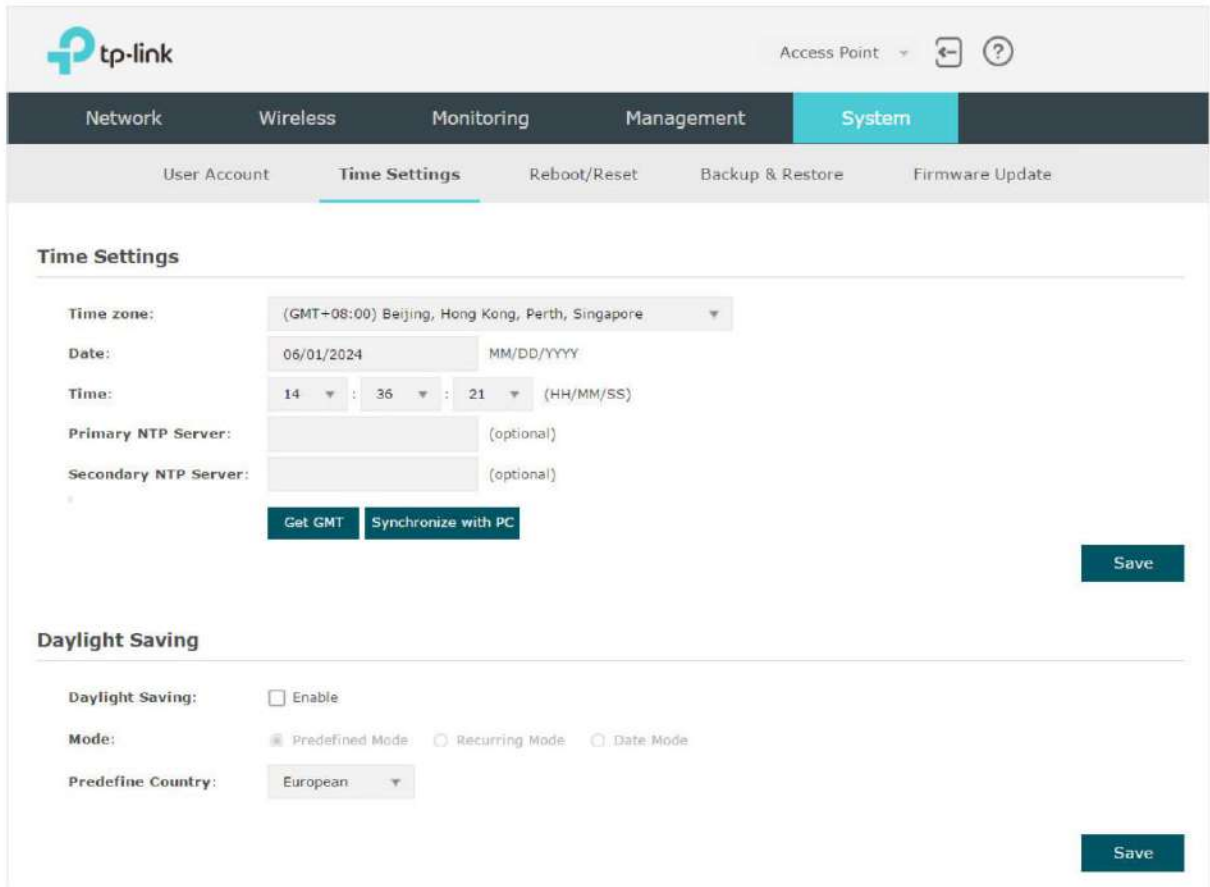
Note:
Enter the inform URL or IP address of your controller to tell the device where to discover the controller.
This feature is commonly used for the device to be managed by the controller in Layer 3 deployments.

Save

5.3 Configurar la hora del sistema

La hora del sistema es la hora estándar para el programador y otras funciones basadas en el tiempo. El EAP admite la configuración básica de la hora del sistema y la función de horario de verano (DST).

Para configurar la hora del sistema, vaya a la página Sistema > Configuración de hora.



The screenshot displays the TP-Link web interface for configuring system time. The top navigation bar includes 'tp-link' and 'Access Point'. The main menu has 'System' selected, with sub-options: 'User Account', 'Time Settings', 'Reboot/Reset', 'Backup & Restore', and 'Firmware Update'. The 'Time Settings' section includes a 'Time zone' dropdown set to '(GMT+08:00) Beijing, Hong Kong, Perth, Singapore', a 'Date' field with '06/01/2024' and 'MM/DD/YYYY' format, and a 'Time' field with '14 : 36 : 21' and '(HH/MM/SS)' format. There are also fields for 'Primary NTP Server' and 'Secondary NTP Server', both marked '(optional)'. Below these are buttons for 'Get GMT' and 'Synchronize with PC', and a 'Save' button. The 'Daylight Saving' section has a 'Daylight Saving' checkbox (unchecked) with 'Enable' text, a 'Mode' section with radio buttons for 'Predefined Mode' (selected), 'Recurring Mode', and 'Date Mode', and a 'Predefine Country' dropdown set to 'European'. A 'Save' button is also present at the bottom right of this section.

Las dos secciones siguientes explican cómo configurar los ajustes básicos de la hora del sistema y la función de horario de verano.

Configurar la hora del sistema

En la sección Configuración de hora, puede configurar la hora del sistema. Hay tres métodos.

Para configurar la hora del sistema: [Establecer el Sistema Tiempo A mano](#) , [Adquiera el Sistema Tiempo Desde un NTP Servidor](#) , y [Sincronizar el Sistema Tiempo con PC Reloj](#) .

Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore ▼

Date: 06/01/2024 MM/DD/YYYY

Time: 14 : 36 : 21 (HH/MM/SS)

Primary NTP Server: (optional)

Secondary NTP Server: (optional)

[Get GMT](#) [Synchronize with PC](#)

[Save](#)

Determine la forma de configurar la hora del sistema y siga los pasos que se indican a continuación para completar la configuración:

- **Configure la hora del sistema manualmente**

Para configurar la hora del sistema manualmente, siga los pasos que se indican a continuación:

1. Configure las siguientes tres opciones en la página: Zona horaria, Fecha y Hora.

Huso horario	Seleccione su zona horaria en la lista desplegable. Aquí, GMT significa Hora Media de Greenwich.
Fecha	Indique la fecha actual en formato MM/DD/AAAA. MM significa mes, DD significa día y AAAA significa año. Por ejemplo: 06/01/2017.
Tiempo	Indique la hora actual en el formato HH/MM/SS. HH significa hora, MM significa minuto y SS significa segundo. Utiliza el formato horario de 24 horas. Por ejemplo: 14:36:21.

2. Haz clic en Guardar.

Nota:

La hora del sistema configurada manualmente se perderá después de reiniciar el EAP.

- **Obtener la hora del sistema de un servidor NTP**

Para obtener la hora del sistema desde un servidor NTP, siga los pasos que se indican a continuación:

1. Configure un servidor NTP en su red y asegúrese de que sea accesible mediante el EAP. O Puedes simplemente encontrar un servidor NTP en Internet y obtener su dirección IP.

Nota:

Si utiliza un servidor NTP en Internet, asegúrese de que la dirección de la puerta de enlace esté configurada correctamente en el EAP. De lo contrario, el EAP no podrá obtener la hora del sistema del servidor NTP correctamente. Para configurar la dirección de la puerta de enlace, consulte [los parámetros inalámbricos](#).

2. Especifique el servidor NTP para el EAP. Si tiene dos servidores NTP, puede configurar uno de ellos. ellos como servidor NTP principal y el otro como servidor NTP secundario. Una vez que el servidor NTP principal está caído, el EAP puede obtener la hora del sistema del servidor NTP secundario. servidor.

NTP primario Servidor	Introduzca la dirección IP del servidor NTP principal. Nota: Si solo tiene un servidor NTP en su red, ingrese la IP. Dirección del servidor NTP en este campo.
NTP secundario Servidor	Introduzca la dirección IP del servidor NTP secundario.

3. Haz clic en el botón **Get GMT** y la hora del sistema adquirida se mostrará en la fecha. y campos de tiempo.

4. Haga clic en Guardar.

• Sincroniza la hora del sistema con el reloj del PC.

Para sincronizar la hora del sistema con el reloj del equipo en el que ha iniciado sesión, siga los pasos que se indican a continuación:

1. Haz clic en el botón **Synchronize with PC** y se mostrará la hora del sistema sincronizado. en los campos de Fecha y Hora.
2. Haz clic en Guardar.

Nota:

La hora del sistema sincronizada con el reloj del PC se perderá después de reiniciar el EAP.

Configurar el horario de verano

El horario de verano consiste en adelantar los relojes durante los meses estivales para que la luz del atardecer dure más, a costa de acortar la hora habitual del amanecer. El EAP ofrece la configuración del horario de verano.

Daylight Saving

Daylight Saving: Enable

Mode: Predefined Mode Recurring Mode Date Mode

Predefine Country: European ▼

[Save](#)

Siga los pasos que se indican a continuación para configurar el horario de verano:

1. Marque la casilla para activar el horario de verano.
2. Seleccione el modo de horario de verano. Hay tres modos disponibles: Modo predefinido, Modo recurrente y modo fecha.
3. Configure los parámetros correspondientes del modo seleccionado.

■ Modo predefinido

Si selecciona el modo predefinido, elija su región en la lista desplegable y el EAP.

Se utilizará el horario de verano predefinido de la región seleccionada.

Mode: Predefined Mode Recurring Mode Date Mode

Predefine Country: European ▼

Se ofrecen cuatro regiones: EE. UU., Europa, Australia y Nueva Zelanda. La siguiente tabla muestra el horario de verano predefinido para cada región.

EE.UU	Desde las 2:00 de la madrugada del segundo domingo de marzo hasta las 2:00 de la madrugada del primer domingo de noviembre.
Europeo	Desde la 1:00 de la madrugada del último domingo de marzo hasta la 1:00 de la madrugada del último domingo de octubre.
Australia	Desde las 2:00 de la madrugada del primer domingo de octubre hasta las 3:00 de la madrugada del primer domingo de abril.
Nueva Zelanda	Desde las 2:00 de la madrugada del último domingo de septiembre hasta las 3:00 de la madrugada del primer domingo de abril.

■ Modo recurrente

Si selecciona el modo recurrente, especifique manualmente un intervalo de tiempo para el horario de verano del EAP. Esta configuración se utilizará todos los años.

Mode: Predefined Mode Recurring Mode Date Mode

Time Offset: minutes (1-180)

Start: in at :

End: in at :

La siguiente tabla muestra cómo configurar el rango de tiempo del ciclo.

Desfase horario	Especifique la hora en la que se debe adelantar el reloj.
Comenzar	Especifique la hora de inicio del horario de verano. El intervalo entre la hora de inicio y la hora de finalización debe ser superior a 1 día e inferior a 1 año (365 días).
Fin	Especifique la hora de finalización del horario de verano. El intervalo entre la hora de inicio y la hora de finalización debe ser superior a 1 día e inferior a 1 año (365 días).

■ Modo de fecha

Si selecciona el modo Fecha, especifique manualmente un rango de tiempo absoluto para el horario de verano. hora del EAP. Esta configuración se utilizará solo una vez.

Mode: Predefined Mode Recurring Mode Date Mode

Time Offset: minutes (1-180)

Start: - - at :

End: - - at :

La siguiente tabla muestra cómo configurar el rango de tiempo absoluto.

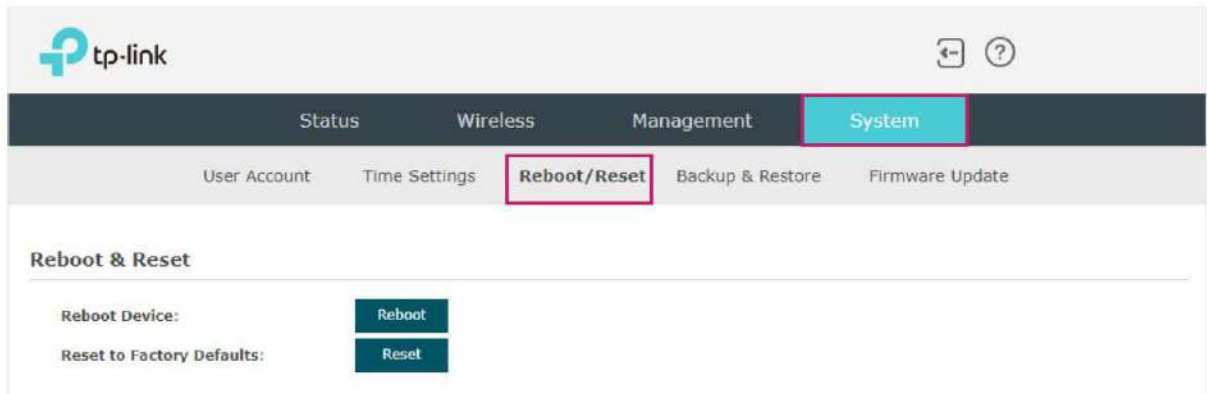
Desfase horario	Especifique la hora en la que se debe adelantar el reloj.
Comenzar	Especifique la hora de inicio del horario de verano. El intervalo entre la hora de inicio y la hora de finalización debe ser superior a 1 día e inferior a 1 año (365 días).
Fin	Especifique la hora de finalización del horario de verano. El intervalo entre la hora de inicio y la hora de finalización debe ser superior a 1 día e inferior a 1 año (365 días).

4. Haga clic en Guardar.

5.4 Reiniciar y restablecer el EAP

Puedes reiniciar y restablecer el EAP según tus necesidades.

Para reiniciar y restablecer el EAP, vaya a la página Sistema > Reiniciar y restablecer.



- Para reiniciar el EAP, haga clic en el **Reboot** botón , y el EAP se reiniciará automáticamente.

Por favor, espere sin realizar ninguna operación.

- Para restablecer el EAP, haga clic en el **Reset** botón , El EAP se restablecerá automáticamente a la configuración de fábrica. Por favor, espere sin realizar ninguna acción.

Nota:

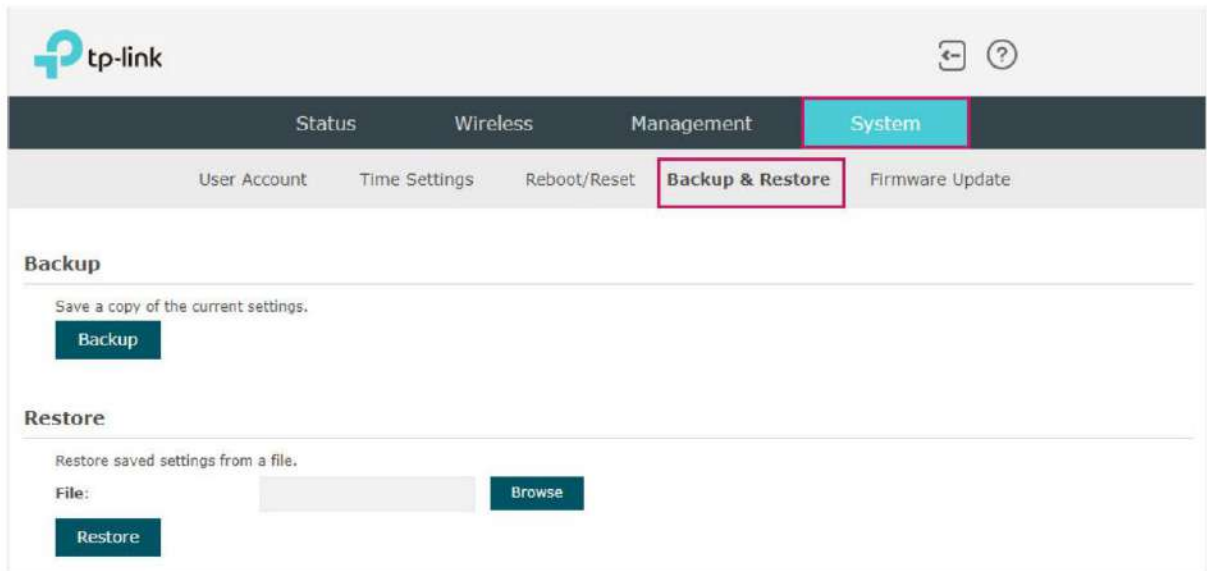
Tras el reinicio, se perderá toda la configuración actual del EAP. Le recomendamos que compruebe si tiene alguna configuración que deba respaldar antes de reiniciar el EAP.

5.5 Copia de seguridad y restauración de la configuración

Puedes guardar la configuración actual del EAP como un archivo de copia de seguridad y guardarlo en tu host. Y si es necesario, puedes usar el archivo de copia de seguridad para restaurar la configuración.

Recomendamos que realice una copia de seguridad de la configuración antes de restablecer o actualizar el EAP.

Para realizar una copia de seguridad y restaurar la configuración, vaya a la página Sistema > Copia de seguridad y restauración.



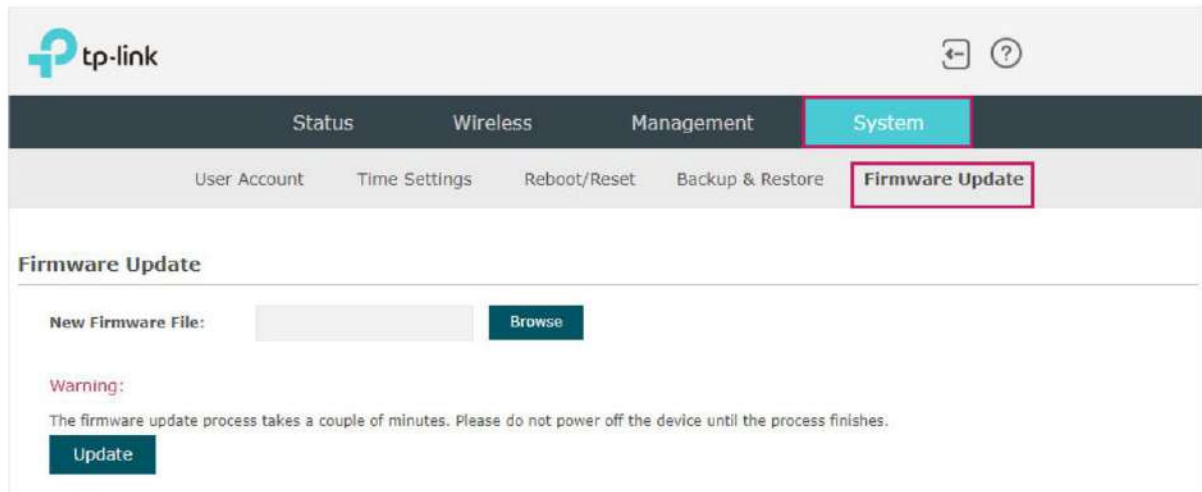
- Para realizar una copia de seguridad de la configuración, haga clic en el botón **Backup** en la sección Copia de seguridad y el El archivo de copia de seguridad se guardará automáticamente en el servidor.

- Para restaurar la configuración, haga clic en el botón **Browse** en la sección Restaurar y Seleccione el archivo de copia de seguridad del host. A continuación, haga clic en el botón de **Restore** para restaurar el configuración.



5.6 Actualizar el firmware

Ocasionalmente, publicamos los archivos de actualización de firmware para los productos EAP en nuestro sitio web oficial. Para acceder a las nuevas funciones de su EAP, visite nuestro sitio web oficial y descargue los archivos de actualización.

Para actualizar el firmware, vaya a la página Sistema > Actualización de firmware.



Siga los pasos que se indican a continuación para actualizar el firmware de su EAP:

1. Visita nuestra página web. <https://www.tp-link.com> y busque su modelo EAP. Descargue el archivo de firmware correcto se encuentra en la página de soporte de EAP.
2. Haz clic en el botón  , Localiza y selecciona el archivo de firmware correcto en tu equipo.
3. Haz clic en el botón  para actualizar el firmware del EAP. Después de la actualización, el EAP se reiniciará automáticamente.

Nota:

El proceso de actualización tarda varios minutos. Para evitar daños en la aplicación EAP, espere sin realizar ninguna operación hasta que finalice la actualización.

6

Ejemplo de aplicación

Este capítulo ofrece un ejemplo práctico sobre cómo establecer y gestionar un programa de asistencia al empleado (PAE). red inalámbrica:

Un restaurante quiere proporcionar acceso inalámbrico a internet para sus empleados y clientes.

El restaurante ahora cuenta con un enrutador, un conmutador, un punto de acceso inalámbrico de doble banda y una computadora.

Siga los pasos a continuación para establecer la red inalámbrica:

6.1 Determinar los requisitos de la red

6.2 Construir la topología de red

6.3 Inicie sesión en el EAP

6.4 Configurar el EAP

6.5 Prueba la red

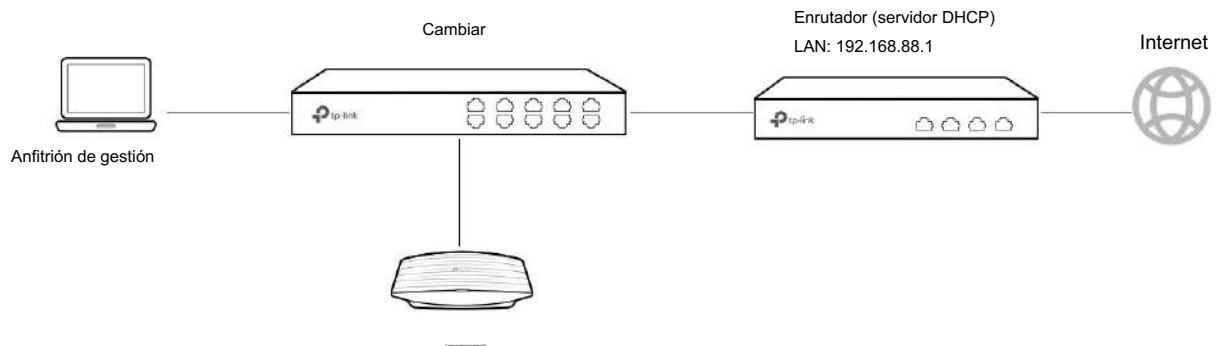
6.1 Determinar los requisitos de la red

Antes de comenzar a construir la red, primero debemos analizar y determinar los requisitos de la misma. En este ejemplo de restaurante, los requisitos de la red son los siguientes:

- En las bandas de 2,4 GHz y 5 GHz se necesitan dos SSID: uno para el restaurante.
uno para los empleados y otro para los huéspedes.
- Para promocionar el restaurante, es necesario configurar la función Portal en las redes Wi-Fi (SSID) de los clientes. De esta forma, los clientes que hayan completado la autenticación del portal podrán acceder al mismo. Se le redirigirá al sitio web oficial del restaurante: <http://www.restaurant1.com>.
- Los empleados del restaurante pueden usar la contraseña correcta para acceder a Internet.
y no necesitan pasar la autenticación del portal. Por motivos de seguridad, las redes Wi-Fi (SSID) de los empleados deben estar cifradas con WPA2-PSK.
- Para reducir el consumo de energía, es necesario configurar la función de programador. La radio Deberá operar únicamente durante el horario laboral (de 9:00 a 22:00 horas).

6.2 Construir la topología de red

Construya la topología de red como se muestra en la siguiente figura.



- El router es la puerta de enlace de la red y actúa como servidor DHCP para asignar direcciones IP dinámicas al host de administración, al EAP y a los clientes. La dirección IP LAN del router es 192.168.88.1/24.
- Conecte el conmutador al puerto LAN del enrutador.
- Conecte el host de administración y el EAP al conmutador. El modo de dirección IP de El host de administración y el EAP son dinámicos, lo que significa que obtendrán una IP dinámica. direcciones del enrutador.

Consejos:

Si el router tiene más de un puerto LAN, también podemos conectar respectivamente el host de administración y el EAP a los puertos LAN del router.

6.3 Inicie sesión en el EAP

Después de construir la topología de red, siga los pasos a continuación para iniciar sesión en la página web de la


1. En el host de administración, abra el navegador web e ingrese "192.168.88.1" en la barra de direcciones. Luego, inicie sesión en el enrutador y encuentre la dirección IP del EAP. Como

La siguiente figura muestra que la dirección IP del EAP es 192.168.88.101.

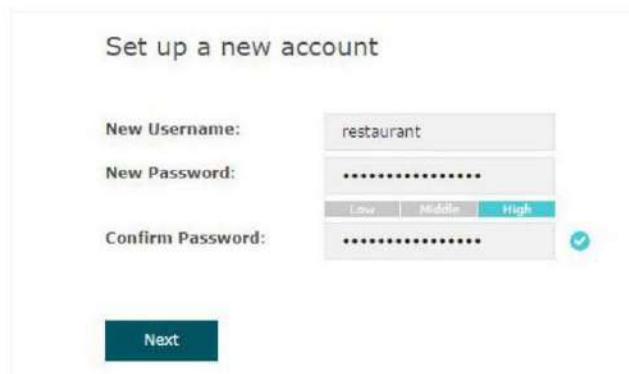
No.	Host Name	MAC Address	IP Address	Lease Time
1	EAP245-50-C7-BF	50-C7-BF-17-A6-E2	192.168.88.101	00:00:43
2	tplink2	F8-BC-12-9B-93-A4	192.168.88.100	00:00:58

Refresh Search Help

2. Introduce "192.168.88.101" en la barra de direcciones para acceder a la página de inicio de sesión del EAP. Introduce el nombre de usuario y la contraseña predeterminados (ambos "admin") en los dos campos y haz clic en INICIAR SESIÓN.



3. En la ventana emergente, especifique un nuevo nombre de usuario y una nueva contraseña para el usuario. Cuenta. Haz clic en Siguiente.

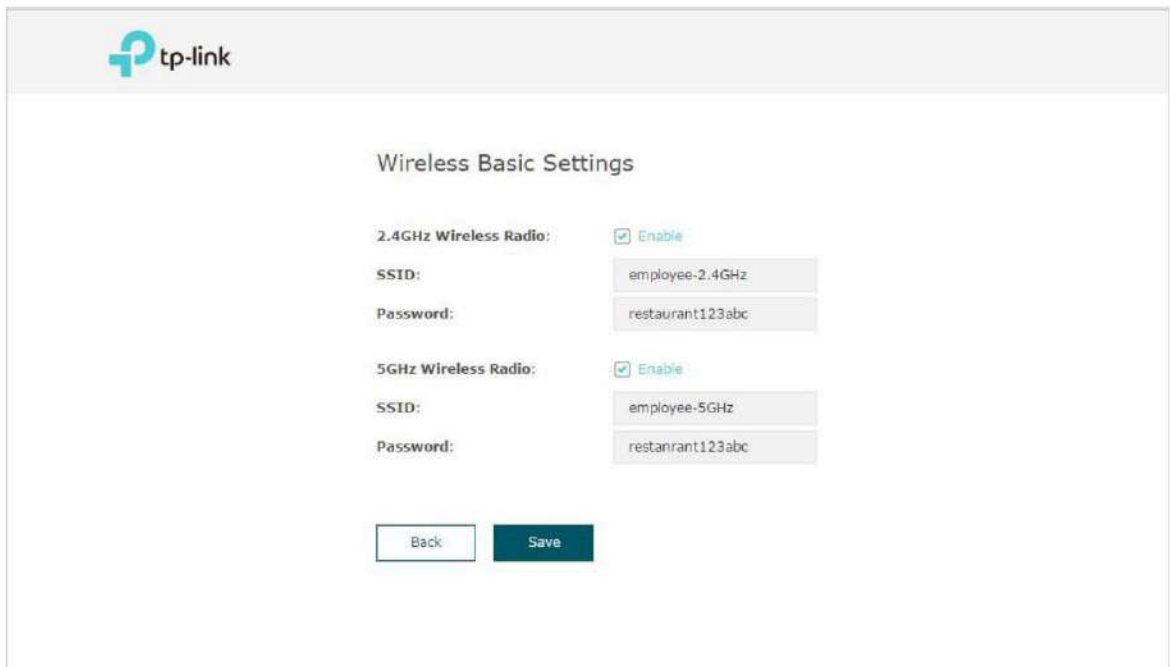


6.4 Configurar el EAP

Para cumplir con los requisitos de red en este ejemplo de aplicación, necesitamos: [Configurar SSID](#) , [Configurar Portal Autenticación](#) y [Configurar Planificador](#).

Configurar SSID

1. Tras iniciar sesión en EAP, siga las instrucciones paso a paso para completar la configuración básica de creación de SSID. Configure los SSID como “employee_2.4GHz” y “employee_5GHz”, e indique la contraseña “restaurant123abc”. Haga clic en Guardar.



tp-link

Wireless Basic Settings

2.4GHz Wireless Radio: Enable

SSID: employee-2.4GHz

Password: restaurant123abc


5GHz Wireless Radio: Enable

SSID: employee-5GHz

Password: restaurant123abc

Back Save

2. Vaya a la página Inalámbrico > Configuración inalámbrica. Cree SSID para invitados en 2.4 GHz. Haga clic

 **Add** para agregar un nuevo SSID.



2.4GHz SSIDs						
ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
1	employee-2.4GHz	0	Enable	WPA-PSK	Disable	 

3. Aparecerá la siguiente página. Configure este SSID como "guest_2.4GHz", mantenga el Modo de seguridad como "Ninguno" y marque la casilla para habilitar la función Portal para este SSID.

Haz clic en Aceptar.

2.4GHz SSIDs

[+ Add](#)

ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
1	employee-2.4GHz	0	Enable	WPA-PSK	Disable	 

SSID:

SSID Broadcast: Enable

Security Mode: ▼

Guest Network: Enable

Rate Limit: Enable

4. Haga clic para acceder a la página de configuración de la banda de 5 GHz. De forma similar a las configuraciones para la banda de 2,4 GHz, configure otro SSID para los invitados en la Banda de 5 GHz.

Configurar la autenticación del portal

Siga los pasos que se indican a continuación para configurar la autenticación del portal:

1. Vaya a la página Inalámbrico > Portal.

2. Configure la función del portal como se muestra en la siguiente figura.

The screenshot shows the TP-Link web management interface for configuring a wireless portal. The 'Wireless' tab is selected, and the 'Portal' sub-tab is active. The configuration fields are as follows:

- SSID:** guest-2.4GHz, guest-5GHz
- Authentication Type:** Local Password
- Password:** restaurant123
- Authentication Timeout:** Custom (0 D, 2 H, 0 M)
- Redirect:** Enable
- Redirect URL:** http://restaurant1.com
- Portal Customization:** Local Web Portal

A preview of the portal shows a welcome message: "Welcome to XXX restaurant." Below it is a password field labeled "Password:". Underneath is a "Term of Use" section with the text: "By using the provided internet, you agree to these terms: 1.xxxxxxxx 2.xxxxxxxxxx". There is a checkbox labeled "I accept the Term of Use" which is checked, and a "Login" button at the bottom.

A "Save" button is located at the bottom left of the configuration area.

- 1) Seleccione los SSID para los invitados en los que el portal tendrá efecto.
- 2) Seleccione el tipo de autenticación como "Contraseña local" y especifique la contraseña como "restaurant123".
- 3) Configurar el tiempo de espera de autenticación. Aquí personalizamos el tiempo de espera a 2 horas. Esto significa que los invitados cerrarán sesión después de haber sido autenticados durante 2 horas. Para continuar utilizando el servicio de internet, estos huéspedes deben introducir la contraseña para autenticarse en el portal una vez más.
- 4) Marque la casilla para habilitar la redirección e ingrese el sitio web del restaurante: http://www.restaurant1.com.

- 5) Configure la página de autenticación. Especifique el título y el período de uso. Para acceder a Internet, los invitados deben ingresar la contraseña correcta en el campo Contraseña, Acepte los Términos de uso y haga clic en el botón Iniciar sesión.

3. Haga clic en Guardar.

Configurar el programador

Siga los pasos a continuación para programar la radio para que funcione solo durante el horario laboral (9:00 de 00:00 a 22:00).

1. Vaya a la página Inalámbrico > Programador.
2. En la sección Configuración, marque la casilla para habilitar el programador y seleccione la asociación. Modo como "Asociado con AP". Haga clic en Guardar.

Settings

Scheduler: Enable

Association Mode: Associated with AP ▼

Save

3. En la sección Configuración del perfil del programador, haga clic en [+ Create Profiles](#).

Scheduler Profile Configuration

[+ Create Profiles](#)

- 1) Aparecerá la siguiente página. Haga clic en [+ Add a Profile](#) y especifique el nombre del perfil como "horario laboral". Haga clic en Aceptar.

Scheduler Profile Configuration

[+ Add a Profile](#)

Profile Name	Modify
--	--

Profile: worktime

Cancel OK

[+ Add an item](#)

ID	Profile Name	Days	Start Time	End Time	Modify
--	--	--	--	--	--



2) Elija el perfil recién agregado "worktime" y haga clic. [+ Add an item](#). Luego el artículo

Aparecerá la página de configuración. Especifique el intervalo horario como de 9:00 a 22:00 todos los días.

Haz clic en Aceptar.

Scheduler Profile Configuration

[+ Add a Profile](#)

Profile Name	Modify
worktime	 

→

[+ Add an item](#)

ID	Profile Name	Days	Start Time	End Time	Modify
--	--	--	--	--	--

Day:

Weekday Weekend Every Day Custom

Mon Tue Wed Thu Fri Sat

Sun

Time: 24 hours

Start Time: 09 : 00

End Time: 22 : 00

4. En la sección Asociación de programador, seleccione "worktime" en la columna Nombre del perfil.

y seleccione "Radio encendida" en la columna Acción. Haga clic en Guardar.

Scheduler Association

ID	AP	AP MAC	Profile Name	Action
1	EAP245-50-c7-bf-17-a6-e2	50-C7-BF-17-A6-E2	worktime	Radio On

6.5 Prueba la red

Para garantizar que los empleados y los invitados puedan navegar por Internet a través de la red inalámbrica, podemos usar un dispositivo cliente, como un teléfono, para comprobar si los SSID funcionan correctamente.

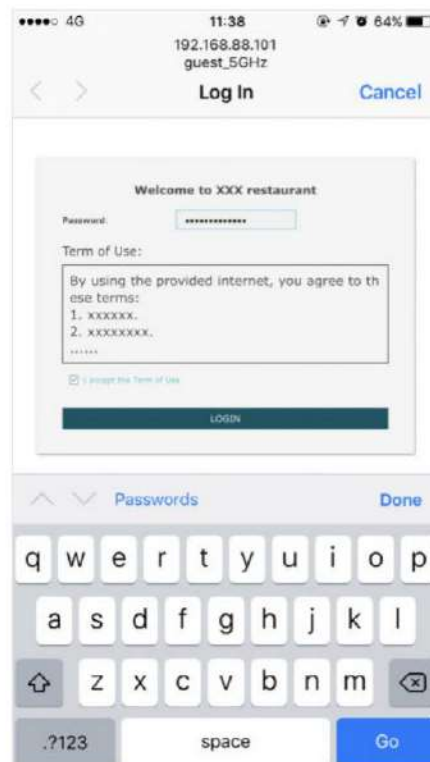
normalmente.

• Para probar los SSID de los empleados, siga los pasos que se indican a continuación:

- 1) Habilite la función Wi-Fi del dispositivo cliente.
- 2) Elija el SSID "employee_2.4GHz" o "employee_5GHz" entre los detectados. SSID.
- 3) Introduce la contraseña "restaurant123abc" para unirte a la red inalámbrica.
- 4) Compruebe si se puede acceder correctamente a los sitios web de Internet.

• Para probar los SSID para los invitados, siga los pasos que se indican a continuación:

- 1) Habilite la función Wi-Fi del dispositivo cliente.
- 2) Elija el SSID "guest_2.4GHz" o "guest_5GHz" entre los SSID detectados.
- 3) El navegador web predeterminado del dispositivo aparecerá y la página de autenticación se abrirá. Aparecerá. Introduzca la contraseña "restaurant123", marque la casilla para aceptar los términos de Utilice y haga clic en el botón INICIAR SESIÓN.



Consejos:

Por lo general, el navegador web se abre automáticamente. Pero si no se abre, podemos abrirlo manualmente y visitar cualquier sitio web HTTP. Entonces aparecerá la página de autenticación.

4) Si la red funciona normalmente, seremos redirigidos al sitio web de la Restaurante: <http://www.restaurant1.com>.



www.rosarioseguridad.com.ar

✉ ventas@rosarioseguridad.com.ar

☎ +54 9 341 6708000

☎ +54 9 341 6799822

📷 [rosarioseguridadok](#)

📺 Rosario Seguridad

📘 Rosario Seguridad

Grupo Instaladores

📘 <https://www.facebook.com/groups/591852618012744/>

☎ +54 9 341 6591429

☎ +54 9 341 4577532

Avenida Pellegrini 4820 - Presidente Perón 3998 - Rosario - Santa Fe - Argentina

