

Configure los parámetros SNMPv2c en WAP125 y WAP581

Objetivo

El protocolo simple de administración de red (SNMP) se utiliza para la gestión de redes, la resolución de problemas y el mantenimiento. SNMP registra, almacena y comparte información con la ayuda de dos software clave: un sistema de administración de redes (NMS) que se ejecuta en dispositivos de administrador y un agente que se ejecuta en dispositivos administrados.

SNMP v1 es la versión original de SNMP que carece de cierta funcionalidad y sólo funciona en redes TCP/IP, mientras que SNMP v2 es una iteración mejorada de v1. SNMP v1 y v2c sólo deben elegirse para redes que utilizan SNMPv1 o SNMPv2c. SNMP v3 es el estándar más reciente de SNMP y aborda muchos de los problemas de SNMP v1 y v2c. En particular, aborda muchas de las vulnerabilidades de seguridad de v1 y v2c. SNMP v3 también permite a los administradores pasar a un estándar SNMP común.

Las trampas son mensajes que alertan al administrador SNMP de una condición de la red. Las solicitudes de información (informes) son trampas que incluyen una solicitud de confirmación de recepción del administrador SNMP. Las notificaciones pueden indicar una autenticación de usuario incorrecta, reinicios, el cierre de una conexión, la pérdida de conexión a un router vecino, un punto de acceso inalámbrico u otros eventos significativos.

En este artículo se explica cómo configurar los parámetros SNMPv2c en el WAP125.

Nota: Para aprender a configurar los parámetros de SNMPv3, haga clic [aquí](#).

Dispositivos aplicables

- WAP125
- WAP581

Versión del software

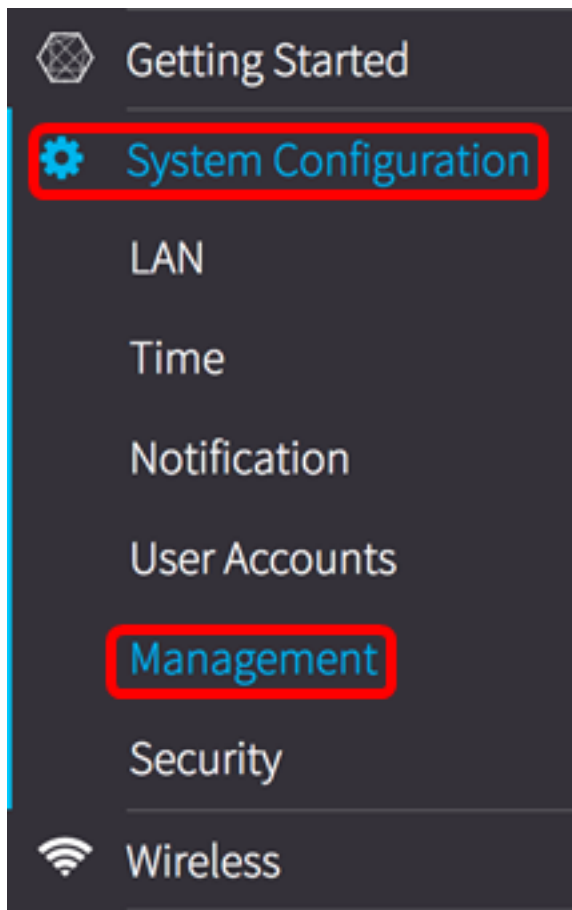
- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

Configuración de los parámetros SNMPv2c

Configuración de los parámetros de SNMP

Nota: Las opciones de menú pueden variar dependiendo del modelo exacto del WAP que esté utilizando. Las imágenes siguientes se han tomado del dispositivo WAP125.

Paso 1. Inicie sesión en la utilidad basada en web del punto de acceso inalámbrico y elija **Configuración del sistema > Administración**.

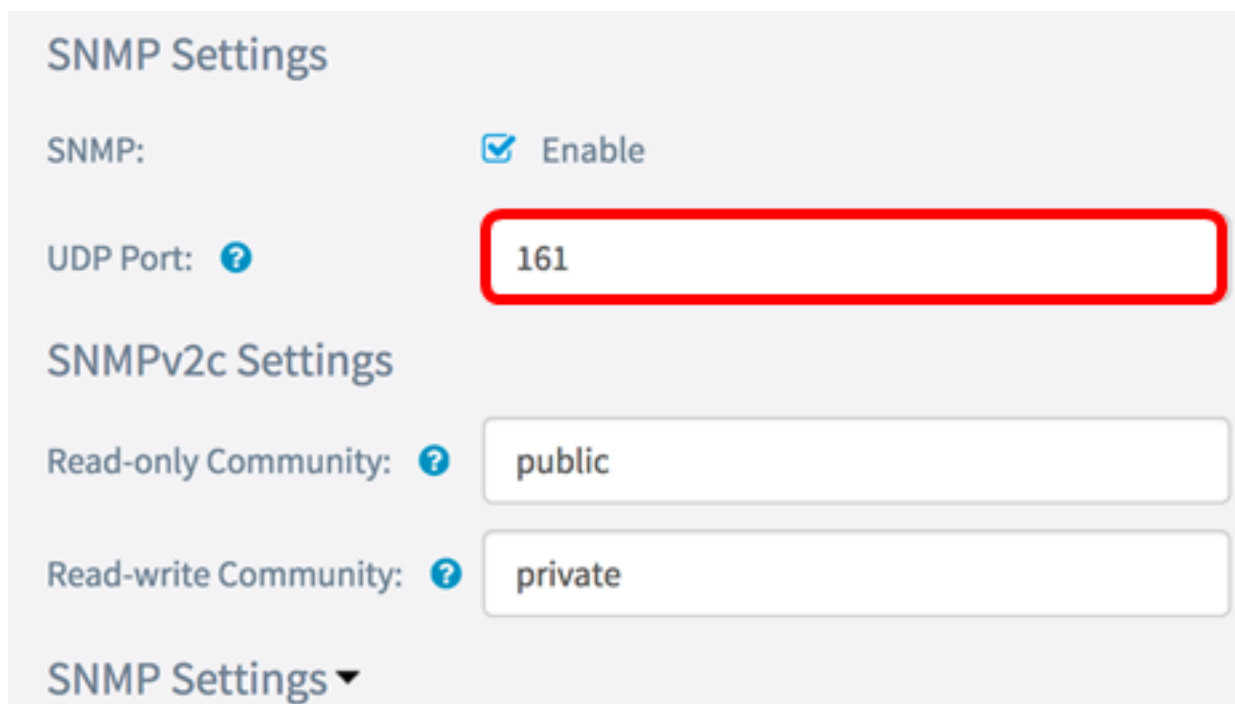


Paso 2. En SNMP Settings, marque la casilla de verificación SNMP **Enable**.

A screenshot of the 'SNMP Settings' configuration page. The title 'SNMP Settings' is at the top. Below it, the 'SNMP:' label is followed by a checked checkbox icon (circled in red) and the word 'Enable'. Underneath is the 'UDP Port:' label with a help icon and a text input field containing '161'. The section 'SNMPv2c Settings' follows, with 'Read-only Community:' and 'Read-write Community:' labels, each with a help icon and a text input field containing 'public' and 'private' respectively. At the bottom is a dropdown menu labeled 'SNMP Settings' with a downward arrow.

Paso 3. Introduzca un número de puerto de protocolo de datagramas de usuario (UDP) en el campo *UDP Port*. El agente SNMP verifica este puerto en busca de solicitudes de acceso. El valor predeterminado es 161. El rango válido es de 1025 a 65535.

Nota: Para este ejemplo, se utiliza 161.



SNMP Settings

SNMP: ☒ Enable

UDP Port:

SNMPv2c Settings

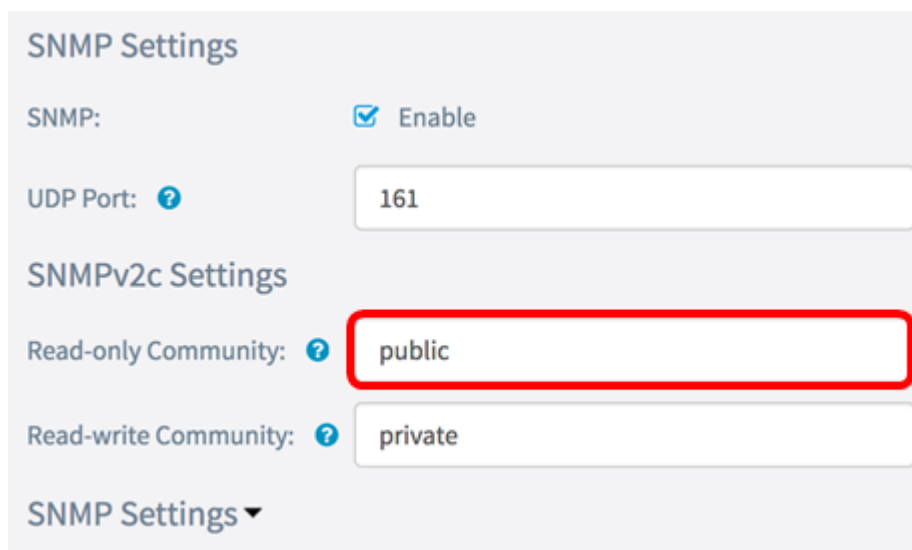
Read-only Community:

Read-write Community:

SNMP Settings ▼

Paso 4. Ingrese el nombre de comunidad SNMP en el campo *Comunidad de sólo lectura*. Crea una comunidad de sólo lectura que se utiliza para acceder a la información del agente SNMP. La cadena de comunidad enviada en el paquete de solicitud enviado por el remitente debe coincidir con la cadena de comunidad en el dispositivo agente. La cadena predeterminada para sólo lectura es pública.

Nota: En este ejemplo, se utiliza el valor predeterminado. El nombre de comunidad de sólo lectura sirve como contraseña, lo que da autoridad para recuperar sólo información.



SNMP Settings

SNMP: ☒ Enable

UDP Port:

SNMPv2c Settings

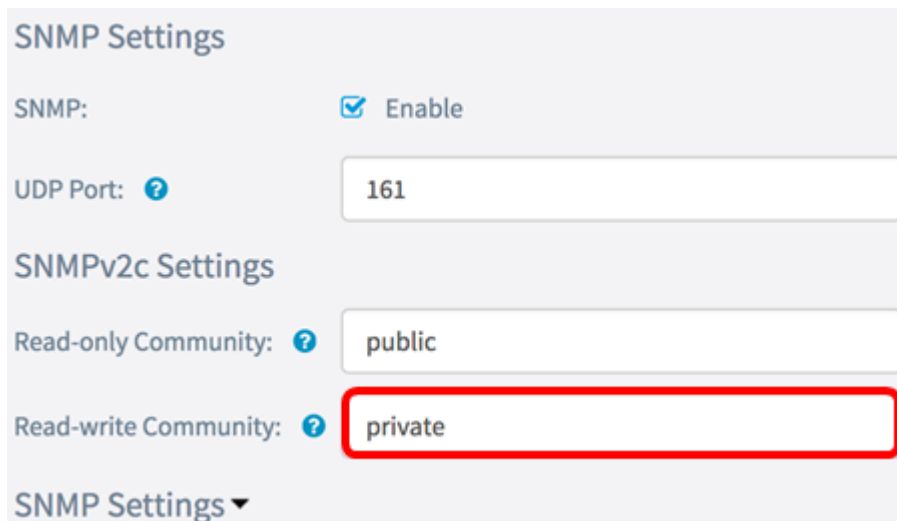
Read-only Community:

Read-write Community:

SNMP Settings ▼

Paso 5. En el campo *Comunidad de lectura y escritura*, ingrese un nombre de comunidad SNMP. Crea una comunidad de lectura y escritura que se utiliza para acceder a la información del agente SNMP. Solo se aceptan las solicitudes de los dispositivos que se identifican con este nombre de comunidad. Este es un nombre creado por el usuario. El valor predeterminado es private (privado).

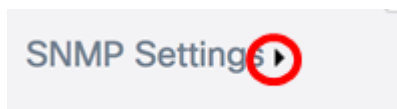
Nota: En este ejemplo, se utiliza private. El nombre de comunidad de lectura y escritura sirve como contraseña, lo que da autoridad para recuperar y cambiar información. Se recomienda cambiar el nombre de la comunidad a algo más personalizado para evitar ataques de seguridad por parte de terceros.



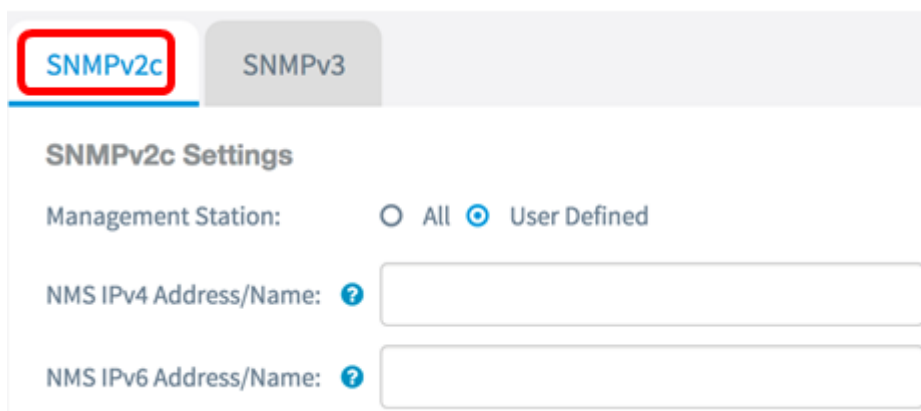
The image shows a configuration page for SNMP. At the top, under 'SNMP Settings', the 'SNMP' checkbox is checked and labeled 'Enable'. Below this, the 'UDP Port' is set to '161'. The 'SNMPv2c Settings' section contains two fields: 'Read-only Community' set to 'public' and 'Read-write Community' set to 'private'. The 'private' field is highlighted with a red rectangle. At the bottom, there is a dropdown menu labeled 'SNMP Settings'.

Configuración de los parámetros de SNMPv2c

Paso 6. Haga clic en el botón derecho SNMP Settings (Parámetros de SNMP).



Paso 7. Haga clic en la pestaña **SNMPv2c** para configurar los parámetros SNMPv2c.



The image shows the 'SNMPv2c Settings' configuration page. At the top, there are two tabs: 'SNMPv2c' (highlighted with a red rectangle) and 'SNMPv3'. Below the tabs, the 'SNMPv2c Settings' section is visible. It includes a 'Management Station' section with two radio buttons: 'All' and 'User Defined' (selected). Below this, there are two input fields: 'NMS IPv4 Address/Name' and 'NMS IPv6 Address/Name', both with question mark icons.

Paso 8. En el área Management Station, elija un método en el que las estaciones puedan acceder al WAP a través del SNMP. Las opciones son:

- Todos: Todas las estaciones tienen acceso al WAP a través de SNMP. Si selecciona esta opción, vaya directamente al [Paso 11](#).
- Definido por el usuario: conjunto de solicitudes SNMP definidas a las que se concede acceso. Si se selecciona esta opción, continúe con el paso siguiente.

Nota: En este ejemplo, se utiliza User Defined (Definido por el usuario).

The image shows the 'SNMPv2c Settings' tab in a configuration interface. The 'Management Station' is set to 'User Defined' (indicated by a red target icon). Below this are two empty input fields: 'NMS IPv4 Address/Name' and 'NMS IPv6 Address/Name', each with a help icon (question mark in a blue circle) to its left.

Paso 9. En el campo *NMS IPv4 Address/Name*, introduzca una dirección del sistema de administración de red (NMS) o una dirección del servidor del sistema de nombres de dominio (DNS) con el formato IPv4 (xxx.xxx.xxx.xxx). Esta es la dirección que ejecutará, obtendrá y establecerá las solicitudes en los dispositivos administrados.

Un DNS es una base de datos distribuida en la que puede asignar nombres de host a direcciones IP a través del protocolo DNS desde un servidor DNS. Cada dirección IP única puede tener un nombre de host asociado. Un nombre de host DNS puede constar de varias etiquetas y cada etiqueta está separada por un punto.

Un NMS es una herramienta o programa que utiliza un administrador para recibir mensajes SNMP.

Nota: En este ejemplo, se utiliza un NMS de 192.168.2.126.

This image shows the 'SNMPv2c Settings' form with the 'NMS IPv4 Address/Name' field populated with '192.168.2.126'. The field is highlighted with a red rectangular border. The 'Management Station' remains 'User Defined', and the 'NMS IPv6 Address/Name' field is still empty.

Paso 10. En el campo *NMS IPv6 Address/Name*, ingrese una dirección NMS o una dirección de servidor DNS que tenga el formato IPv6 (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx). Esta es la dirección que ejecutará, obtendrá y establecerá las solicitudes en los dispositivos administrados.

Nota: En este ejemplo, se utiliza fdce:223e:c00d:d00d:afaf:0000:0000:0000.

This image shows the 'SNMPv2c Settings' form with both fields populated. The 'NMS IPv4 Address/Name' is '192.168.2.126' and the 'NMS IPv6 Address/Name' is 'fdce:223e:c00d:d00d:afaf:0000:0000:0000'. The IPv6 field is highlighted with a red rectangular border. The 'Management Station' is still 'User Defined'.

[Paso 11.](#) En el campo *Trap Community* bajo SNMPv2c Trap Settings, ingrese el nombre de comunidad para la trampa.

Nota: En este ejemplo, snmptraps.foo.com se utiliza como nombre de comunidad de trampa.

SNMPv2c Settings

Management Station: ☐ All ☒ User Defined

NMS IPv4 Address/Name:

NMS IPv6 Address/Name:

SNMPv2c Trap Settings

Trap Community:

Paso 12. Marque la casilla de verificación de una entrada de nombre de host en la Tabla de destino de trampa para habilitar la edición.

Nota: Puede configurar hasta tres direcciones IP/nombre de host.

Trap Destination Table

	Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/>	IPv4	<input type="text"/>
<input type="checkbox"/>	IPv4	<input type="text"/>
<input type="checkbox"/>	IPv4	<input type="text"/>

Paso 13. En la lista desplegable Host IP Address Type (Tipo de dirección IP de host), elija una versión IP. Las opciones son:

- IPv4: cuarta generación o versión del esquema de direcciones del protocolo de Internet (IP) que sigue el formato xxx.xxx.xxx.xxx.
- IPv6: sexta generación o versión del esquema de direcciones IP que sigue el formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

Trap Destination Table

	Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/>	IPv4	<input type="text"/>
<input type="checkbox"/>	IPv4	<input type="text"/>
<input type="checkbox"/>	IPv4	<input type="text"/>

Paso 14. En el campo *Nombre de host/Dirección IP*, ingrese una dirección IPv4 o IPv6 que recibirá las trampas SNMP.

Nota: Para este ejemplo, se utiliza 192.168.2.202.

Trap Destination Table

	Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/>	IPv4 ⓘ	192.168.2.202
<input type="checkbox"/>	IPv4 ⓘ	
<input type="checkbox"/>	IPv4 ⓘ	

Paso 15. Haga clic [Save](#).

Ahora debería haber configurado correctamente los parámetros SNMPv2c en WAP125 y WAP581.