

# Configuración de los parámetros generales de SNMP en WAP361 y WAP150

## Objetivo

El protocolo simple de administración de red (SNMP) es un protocolo que se utiliza para la gestión, resolución de problemas y mantenimiento de la red. SNMP registra, almacena y comparte información con la ayuda de un software de dos claves: un sistema de administración de red (NMS) que se ejecuta en dispositivos de administrador y un agente que se ejecuta en dispositivos administrados. Los dispositivos WAP361 y WAP150 admiten SNMPv2c y SNMPv3.

SNMPv2c es similar al SNMP original a través de la seguridad mejorada y el soporte de manejo de errores. Esta mejora incluye códigos de error ampliados que distinguen diferentes tipos de errores; todos los tipos de errores se informan a través de un solo código de error en SNMPv1.

SNMPv3 mejoró la segunda versión publicada al proporcionar nuevas funciones de seguridad como autenticación, privacidad, autorización y control de acceso.

Este artículo explica cómo configurar los parámetros generales de SNMP en WAP361 y WAP150.

## Dispositivos aplicables

- Serie WAP300: WAP361
- Serie WAP100: WAP150

## Versión del software

- 1.0.0.16

## Configuración general de SNMP

Paso 1. Inicie sesión en la utilidad basada en web del punto de acceso y elija **SNMP > General**.



Paso 2. En el área Global Settings , marque la casilla de verificación **Enable** para habilitar SNMP.

The screenshot shows the 'General' settings page. Under 'Global Settings', the 'SNMP' checkbox is checked and circled in red. Below it, the 'UDP Port' is set to '161' in a text box, which is also circled in red. A note next to the text box indicates '(Range:1025-65535, Default: 161)'.

Paso 3. Ingrese el número de puerto UDP en el campo *UDP Port*. El agente SNMP verifica este puerto en busca de solicitudes de acceso. El puerto predeterminado es 161.

This screenshot is identical to the previous one, but the 'UDP Port' text box containing '161' is highlighted with a red rectangle.

**Timesaver:** Si no necesita la configuración de SNMPv2, omita este paso y pase al [Paso 11](#).

Paso 4. Introduzca un nombre de comunidad de sólo lectura en el campo *Comunidad de sólo lectura* con caracteres alfanuméricos que van del 1 al 256. El nombre de comunidad es un nombre definido por el usuario que actúa como un simple mecanismo de autenticación o contraseña para restringir los dispositivos en la red que pueden solicitar datos del agente SNMP. La cadena de comunidad enviada por el remitente en el paquete de solicitud debe coincidir con la cadena de comunidad en el dispositivo agente. La cadena predeterminada para sólo lectura es `cisco_public`.

**Nota:** La contraseña de sólo lectura otorga autoridad para recuperar sólo información.

The screenshot shows the 'SNMPv2c Settings' page. The 'Read-only Community' text box contains 'public' and is circled in red. The 'Read-write Community' text box contains 'private'.

Paso 5. Ingrese un nombre de comunidad de lectura y escritura en el campo *Comunidad de lectura y escritura* con caracteres alfanuméricos que van del 1 al 256 para las operaciones permitidas del conjunto SNMP. Solo se aceptan las solicitudes de los dispositivos que se identifican con este nombre de comunidad. El valor predeterminado es `cisco_private`. Se trata de una contraseña que permite recuperar información del agente y modificar la configuración de ese dispositivo agente.

**Nota:** Se recomienda cambiar ambas contraseñas a una contraseña definida por el usuario para evitar amenazas de seguridad.

This screenshot is identical to the previous one, but the 'Read-write Community' text box containing 'private' is highlighted with a red rectangle.

Paso 6. Elija entre All (Todos) o User Defined (Definido por el usuario) en el botón de opción Management Station (Estación de administración) para elegir una preferencia de estación de administración. La estación de administración supervisa y actualiza los valores de la

Base de información de administración (MIB).

**Nota:** La opción seleccionada como ejemplo en la siguiente imagen es Definida por el usuario.

Todos: permite que todas las estaciones de la red accedan al punto de acceso inalámbrico (WAP) a través de SNMP como estación de administración. Si elige esto, continúe con el [Paso 8](#).

Definido por el usuario: limita el acceso a una estación o grupo de estaciones específico.

Management Station:  All  User Defined

NMS IPv4 Address/Name:  (xxx.xxx.xxx.xxx / Hostn

NMS IPv6 Address/Name:  (xxxx:xxxx

Paso 7. Ingrese las direcciones IPv4 o IPv6, el nombre de host DNS o la subred del NMS que pueden ejecutar, obtener y establecer las solicitudes en los dispositivos administrados en los campos *NMSIPv4 Address/Name* y *NMS IPv6 Address/Name*, respectivamente. Un NMS se refiere a las estaciones de administración que ejecutan aplicaciones que supervisan y controlan los dispositivos administrados.

**Nota:** La dirección IPv4 de NMS 192.168.1.241 se utiliza como ejemplo en la siguiente imagen.

Management Station:  All  User Defined

NMS IPv4 Address/Name:  (xxx.xxx.xxx.xxx / H

NMS IPv6 Address/Name:  xxx

Paso 8. Ingrese el nombre de comunidad global asociado con trampas SNMP en el campo *Trap Community*. El intervalo válido es de 1 a 60 caracteres alfanuméricos y especiales. En la siguiente imagen, TrapCommunity se utiliza como ejemplo.

**Nota:** Las trampas son notificaciones de agente a administrador que contienen información del agente. Las trampas enviadas desde el dispositivo utilizan la cadena ingresada como nombre de comunidad.

SNMPv2c Trap Settings

Trap Community:  Range: 1 - 60 Charact

Trap Destination Table	
Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/> IPv4	192.168.1.254
<input checked="" type="checkbox"/> IPv4	snmptraps.foo.com
<input type="checkbox"/> IPv4	

Save

Paso 9. En el área Tabla de destino de trampa, active la casilla y elija entre IPv4 e IPv6 en la lista desplegable Tipo de dirección IP de host.

**Nota:** En el siguiente ejemplo, las dos primeras casillas se activaron con IPv4 configurado como Host IP Address Type (Tipo de dirección IP de host).

SNMPv2c Trap Settings

Trap Community:  (Range: 1 - 60 Charac

Trap Destination Table	
Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/> IPv4 ▾	<input type="text" value="192.168.1.254"/>
<input checked="" type="checkbox"/> IPv4 ▾	<input type="text" value="snmptraps.foo.com"/>
<input type="checkbox"/> IPv4 ▾	<input type="text"/>

Paso 10. En el campo *Nombre de host/Dirección IP*, ingrese los nombres de host o direcciones IP de hasta tres hosts para recibir trampas SNMP.

**Nota:** En la siguiente imagen, se escribieron como ejemplos una dirección IP y un nombre de host.

SNMPv2c Trap Settings

Trap Community:  (Range: 1 - 60 Charact

Trap Destination Table	
Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/> IPv4 ▾	<input type="text" value="192.168.1.254"/>
<input checked="" type="checkbox"/> IPv4 ▾	<input type="text" value="snmptraps.foo.com"/>
<input type="checkbox"/> IPv4 ▾	<input type="text"/>

Paso 11. Click **Save**.

**SNMPv2c Trap Settings**

Trap Community:  (Range: 1 - 60 Characters)

Trap Destination Table		
	Host IP Address Type	Hostname/IP Address
<input checked="" type="checkbox"/>	IPv4 ▾	<input type="text" value="192.168.1.254"/>
<input checked="" type="checkbox"/>	IPv4 ▾	<input type="text" value="snmptraps.foo.com"/>
<input type="checkbox"/>	IPv4 ▾	<input type="text"/>

Ha configurado correctamente los parámetros generales de SNMP en su WAP.

Para obtener más información sobre General Settings Simple Network Management Protocol, haga clic en los siguientes enlaces:

- [Parámetros generales del protocolo simple de administración de red \(SNMP\) en los puntos de acceso WAP121 y WAP321](#)
- [Configuración general del protocolo simple de administración de red \(SNMP\) en los puntos de acceso WAP551 y WAP561](#)