

Configure General SNMP Settings on the WAP361 and WAP150

Objective

Simple Network Management Protocol (SNMP) is a protocol used for network management, troubleshooting, and maintenance. SNMP records, stores, and shares information with the help of a two-key software: a Network Management System (NMS) that runs on manager devices and an agent that runs on managed devices. The WAP361 and WAP150 support SNMPv2c and SNMPv3.

SNMPv2c is similar to the original SNMP through improved security and error handling support. This improvement includes expanded error codes that distinguish different types of errors; all types of errors are reported through a single error code in SNMPv1.

SNMPv3 improved the second released version by providing new security features such as Authentication, Privacy, Authorization, and Access control.

This article explains how to configure the general SNMP settings on the WAP361 and WAP150.

Applicable Devices

- WAP300 Series — WAP361
- WAP100 Series — WAP150

Software Version

- 1.0.0.16

SNMP General Settings

Step 1. Log in to the access point web-based utility and choose **SNMP > General**.



Step 2. In the Global Settings area, check the **Enable** checkbox to enable SNMP.

General

Global Settings

SNMP: Enable

UDP Port: (Range:1025-65535, Default: 161)

Step 3. Enter the UDP port number in the *UDP Port* field. The SNMP agent checks this port for access requests. The default port is 161.

General

Global Settings

SNMP: Enable

UDP Port: (Range:1025-65535, Default: 161)

Timesaver: If you do not need SNMPv2 configuration, skip this step, and jump to [Step 11](#).

Step 4. Enter a read-only community name in the *Read-only Community* field with alphanumeric characters ranging from 1 to 256. The community name is a user-defined name that acts as a simple authentication mechanism or password to restrict the devices on the network that can request data from the SNMP agent. The community string sent by the sender in the request packet has to match the community string on the agent device. The default string for read-only is `cisco_public`.

Note: The read-only password gives authority to retrieve information only.

SNMPv2c Settings

Read-only Community:

Read-write Community:

Step 5. Enter a read-write community name in the *Read-write Community* field with alphanumeric characters ranging from 1 to 256 for permitted SNMP set operations. Only requests from the devices that identify themselves with this community name are accepted. The default is `cisco_private`. This is a password that allows both to retrieve information from the agent and to modify settings on that agent device.

Note: It is recommended to change both the passwords to a user-defined password in order to avoid security threats.

SNMPv2c Settings

Read-only Community:

Read-write Community:

Step 6. Choose between All or User Defined in the Management Station radio button to choose a management station preference. The management station monitors and updates the values in the Management Information Base (MIB).

Note: The option selected as an example in the image below is User Defined.

All — Allows all the stations in the network to access the Wireless Access Point (WAP) through SNMP as a management station. If you choose this, proceed to [Step 8](#).

User Defined — Limits the access to a specific station or group of stations.



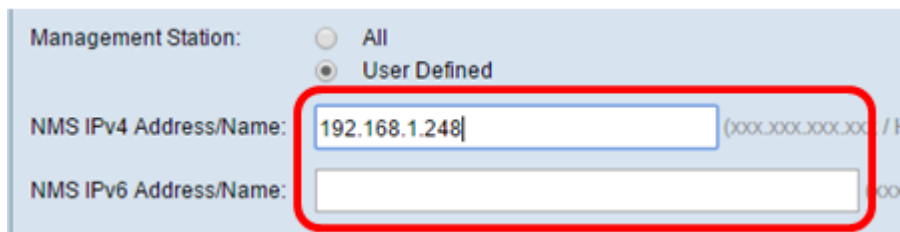
Management Station: All User Defined

NMS IPv4 Address/Name: (xxx.xxx.xxx.xxx / Hostname)

NMS IPv6 Address/Name: (xxxx:xxxx:xxxx:xxxx)

Step 7. Enter the IPv4 or IPv6 addresses, DNS hostname, or subnet of the NMS that can execute, get, and set the requests to the managed devices in the *NMSIPv4 Address/Name* and *NMS IPv6 Address/Name* fields, respectively. An NMS refers to the management stations that execute applications that monitor and control managed devices.

Note: The NMS IPv4 address 192.168.1.241 is used as an example in the image below.



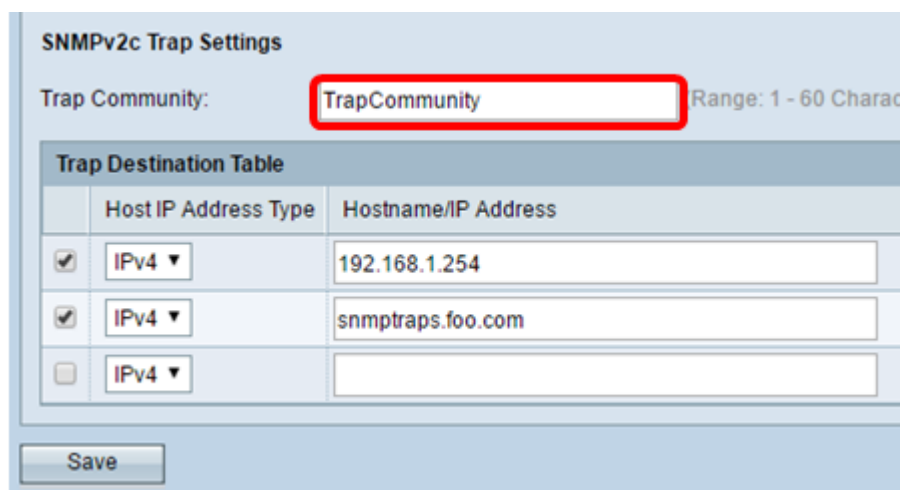
Management Station: All User Defined

NMS IPv4 Address/Name: (xxx.xxx.xxx.xxx / Hostname)

NMS IPv6 Address/Name: (xxxx:xxxx:xxxx:xxxx)

Step 8. Enter the global community name associated with SNMP traps in the *Trap Community* field. The valid range is from 1 to 60 alphanumeric and special characters. In the image below, TrapCommunity is used as an example.

Note: Traps are notifications from agent to manager containing agent information. Traps sent from the device use the string entered as a community name.



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"/>

Save

Step 9. In the Trap Destination Table area, check the box and choose between IPv4 and IPv6 in the Host IP Address Type drop-down list.

Note: In the example below, the first two boxes were checked with both IPv4 set as the Host IP Address Type.

SNMPv2c Trap Settings

Trap Community: (Range: 1 - 60 Characters)

Trap Destination Table		
<input type="checkbox"/>	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"/>

Step 10. In the *Hostname/IP Address* field, enter the host names or IP addresses of up to three hosts to receive SNMP traps.

Note: In the image below, an IP address and a hostname were entered as examples.

SNMPv2c Trap Settings

Trap Community: (Range: 1 - 60 Characters)

Trap Destination Table		
<input type="checkbox"/>	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"/>

Step 11. Click **Save**.

SNMPv2c Trap Settings

Trap Community: (Range: 1 - 60 Characters)

Trap Destination Table		
<input type="checkbox"/>	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"/>

You have successfully configured the SNMP General Settings on your WAP.

For more information on General Settings Simple Network Management Protocol, click on the following links:

- [Simple Network Management Protocol \(SNMP\) General Settings on the WAP121 and](#)

WAP321 Access Points

- Simple Network Management Protocol (SNMP) General Settings Configuration on the WAP551 and WAP561 Access Points