

# Configure Simple Network Management Protocol (SNMP) Settings on SPA100 Series

## Objective

Simple Network Management Protocol (SNMP) is a tool used to monitor and regulate devices on a network as well as maintain configurations. Its statistics collection, performance, and security enable you to solve network issues quickly. A SNMP managed network consists of managed devices, agents, and a network manager. Managed devices are devices that are capable of the SNMP feature. An agent is SNMP software on a managed device. A network manager is an entity that receives data from the SNMP agents. You must install a SNMP v3 manager program to view SNMP notifications. On the device, a user can adjust trap configuration settings. Traps are error messages that are sent to a specific IP address when an error occurs in the network.

The objective of this document is to show you how to configure the SNMP settings on the SPA100 Series Analog Telephone Adapter (ATA).

## Applicable Devices

- SPA100 Series Analog Telephone Adapter

## Software Version

- v1.1.0

## SNMP Configuration

Step 1. Log in to the web configuration utility and choose **Administration > Management > SNMP**. The *SNMP* page opens:

# SNMP

## SNMP Setting

SNMP:  Enabled  Disabled

Trusted IP:  Any

Address:  .  .  .

Netmask:  .  .  .

Get / Trap Community:

Set Community:

SNMPV3:  Enabled  Disabled

R/W User:

Auth- Protocol:  ▾

Auth- Password :

PrivProtocol:  ▾

Privacy Password:

## Trap Configuration

IP Address:  .  .  .  (Hint:192.168.15.100)

Port:  (Range: 162 or 1025-65535,Default:162)

SNMP Version:  ▾

Submit

Cancel

Step 2. To the right of the *SNMP* field, click the **Enabled** radio button to enable SNMP, or click the **Disabled** radio button to disable SNMP on the device.

**SNMP Setting**

SNMP:  Enabled  Disabled

Trusted IP:  Any

Address: 192 . 168 . 10 . 1

Netmask: 255 . 255 . 255 . 0

Get / Trap Community: public

Set Community: private

Step 3. In the *Trusted IP* field, click **Any** to allow access to the ATA from any IP address through SNMP, or click **Address** to allow a range of IP addresses to access the ATA through SNMP.

Step 4. In the *Get Community* field, enter a phrase that acts as a password for GET commands in the SNMP community.

Step 5. In the *Set Community* field, enter a phrase that acts as a password for SET commands in the SNMP community.

SNMPV3:  Enabled  Disabled

R/W User: v3rwuser

Auth- Protocol: HMAC-SHA

Auth- Password : .....

PrivProtocol: CBC-DES

Privacy Password: .....

Step 6. SNMPV3 is a more secure implementation of SNMP. It enables the use of more advanced authentication and encryption mechanisms to ensure that only authorized devices are able to read and write to your network devices over SNMP. Click the **Enabled** radio button to use SNMPv3 or click the **Disabled** radio button to disable it.

Step 7. In the *R/W User* field, enter a username for the SNMPv3 authentication.

Step 8. From the *Auth-Protocol* drop-down list, choose an authentication protocol for SNMPv3. The available options are defined as follows:

- MD5 — Message-Digest 5 (MD5) is an algorithm that takes an input and produces a 128 bit message digest of the input.
- SHA — Secure Hash Algorithm (SHA) is an algorithm that takes an input and produces a 160 bit message digest of the input.

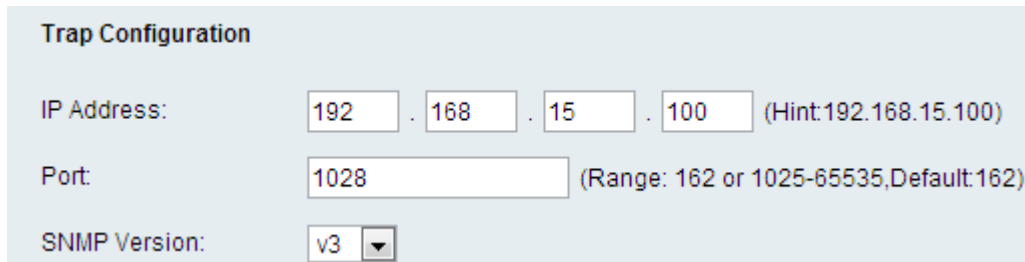
**Note:** HMAC-SHA is considered more secure than HMAC-MD5 and is recommended.

Step 9. In the *Auth-Password* field, enter a password for authentication.

Step 10. From the *PrivProtocol* drop-down list, choose a privacy authentication protocol. It is recommended that the user must have a privacy feature so that data is secured. The available options are defined as follows:

- None — No privacy algorithm is used. The data of a message will be sent unencrypted.
- CBC-DES — This option encrypts the data of a message using DES encryption.

Step 11. In the *Privacy Password* field, enter a password for the privacy authentication protocol.



The screenshot shows a 'Trap Configuration' form with three fields: 'IP Address' with four input boxes containing '192', '168', '15', and '100' and a hint '(Hint:192.168.15.100)'; 'Port' with an input box containing '1028' and a range '(Range: 162 or 1025-65535,Default:162)'; and 'SNMP Version' with a dropdown menu showing 'v3'.

Step 12. In the *IP Address* field, enter an IP address that will receive trap messages.

Step 13. In the *Port* field, enter the port number that will receive trap messages. The default port is 162.

Step 14. From the *SNMP Version* drop-down list, choose a version of SNMP to use to find trap messages. The available options are as follows:

- v1 — Uses SNMPv1 traps. SNMPv1 traps use a community string to authenticate trap messages, and does not encrypt data.
- v2 — Uses SNMPv2 traps. SNMPv2 traps use a community string to authenticate trap messages, and does not encrypt data.
- v3 — Uses SNMPv3 traps. SNMPv3 traps can be set to use a username and password to authenticate the source of a trap, and can encrypt the data of a trap. SNMPv3 must be enabled and configured as described in Step 6 in order to use this option.

Step 15. Click **Submit** to apply changes, or **Cancel** to discard them.