



Configuring and Validating SNMP

- [Configuring and Validating SNMP, on page 1](#)

Configuring and Validating SNMP

SNMP (simple network monitoring protocol) applications used in Cisco URWB software for network management functionalities.

The following illustration shows the SNMP process. SNMP agent receives a request from SNMP client, and it passes the request to the subagent. The subagent then returns a response to the SNMP agent and the agent creates an SNMP response packet and sends the response to the remote network management station that initiated the request.

Figure 1: SNMP Process



Configuring SNMP from CLI

The following CLI commands are used for SNMP (Simple Network Monitoring Protocol) configuration.



- Note**
- SNMP CLI logic modified for SNMP configuration, all parameters of SNMP are required to be configured before enable SNMP feature by CLI “configure snmp enabled”.
 - All the related configurations of SNMP will be removed automatically when disable SNMP feature.

To **enable or disable SNMP** functionality use the following CLI command.

```
Device# configure snmp [enable | disable]
```

To specify the **SNMP protocol version**, use the following CLI command.

```
Device#configure snmp version {v2c | v3}
```

To specify the **SNMP v2c community ID** number (SNMP v2c only), use the following CLI command.

```
Device#configure snmp v2c community-id <length 1-64>
```

To specify the **SNMP v3 username** (SNMP v3 only), use the following CLI command.

```
Device#configure snmp v3 username <length 32>
```

To specify the **SNMP v3 user password** (SNMP v3 only), use the following CLI command.

```
Device#configure snmp v3 password <length 8-64>
```

To specify the **SNMP v3 authentication** protocol (SNMP v3 only), use the following CLI command.

```
Device#configure snmp auth-method <md5|sha>
```

To specify the **SNMP v3 encryption protocol** (SNMP v3 only), use the following CLI command.

```
Device#configure snmp encryption {des | aes | none}
```

Possible encryption values are des or aes. Alternatively, enter none if a v3 encryption protocol is not needed.

To specify the **SNMP v3 encryption passphrase** (SNMP v3 only), use the following CLI command.

```
Device#configure snmp secret <length 8-64>
```

To specify the **SNMP periodic trap** settings, use the following CLI command.

```
Device#configure snmp periodic-trap {enable | disable}
```

To specify the **notification trap period** for periodic SNMP traps, use the following CLI command.

```
Device#configure snmp trap-period <1-2147483647>
```

Notification value trap period measured in minutes.

To **enable or disable SNMP event traps**, use the following CLI command.

```
Device#configure snmp event-trap {enable | disable}
```

To specify the **SNMP NMS hostname** or IP address, use the following CLI command.

```
Device#configure snmp nms-hostname {hostname | Ip Address}
```

To **Disable SNMP configuration**, use the following CLI command:

```
Device#configure snmp disabled
```

SNMP is disabled and all sensitive information and credentials have been cleared. Please respecify all valid values to enable SNMP again.

Example of SNMP configuration.

CLI for SNMP v2:

```
Device#configure snmp v2 community-id <length 1-64>
Device #configure snmp nms-hostname hostname/Ip Address
Device #configure snmp trap-period <1-2147483647>
Device #configure snmp periodic-trap enable/disable
Device #configure snmp event-trap enable/disable
Device #configure snmp version v2c
Device #configure snmp enabled
```

CLI for SNMP v3:

```
Device #configure snmp nms-hostname hostname/Ip Address
Device #configure snmp trap-period <1-2147483647>
Device #configure snmp v3 username <length 32>
Device #configure snmp v3 password <length 8-64>
Device #configure snmp auth-method <md5|sha>
Device #configure snmp encryption <aes|des|none>
Device #configure snmp secret <length 8-64>
Device #configure snmp periodic-trap enable/disable
Device #configure snmp event-trap enable/disable
```

```
Device #configure snmp version v3
Device #configure snmp enabled
```

Validating SNMP from CLI

To validate a SNMP, use the following show commands.

Show SNMP info:

```
Device# show snmp
SNMP: enabled
Version: v3
Username: username
Password: password
Authentication method: SHA
Encryption: AES
Encryption Passphrase: passphrase
Engine ID: 0x8000000903c0f87fe5f314
Periodic Trap: enabled
Notification Period (minutes): 5
Event Trap: enabled
NMS hostname: 192.168.116.11
Device# show snmp
SNMP: enabled
Version: v2c
Community ID: test
Periodic Trap: enabled
Notification Period (minutes): 5
Event Trap: enabled
NMS hostname: 192.168.116.11
Device# show system status snmpd
Service Status
Service Name : snmpd
Loaded : loaded
Active : active (running)
Main ProcessID : 6437
Running Since : Mon 2022-09-19 14:45:27 UTC; 3h 34min ago
Service Restart : 0
```

Configuring SNMP from GUI

The following images shows the configuration of SNMP from GUI

GUI for SNMP v2:

The screenshot shows the Cisco URWB IW9167EH Configurator interface. The main title is "Cisco URWB IW9167EH Configurator" with the version "5.21.200.136 - MESH END MODE". The left sidebar contains a navigation menu with categories like "IOTOD IW", "GENERAL SETTINGS", "NETWORK CONTROL", "ADVANCED SETTINGS", and "MANAGEMENT SETTINGS". The "SNMP" configuration page is active, showing the following settings:

- SNMP mode: v2c
- Community ID: test
- Enable SNMP periodic trap:
- Enable SNMP event trap:
- NMS hostname: 192.168.0.100
- Notification period (minutes): 1

Buttons for "Reset" and "Save" are visible at the bottom of the configuration area.

GUI for SNMP v3:

The screenshot shows the Cisco URWB IW9167EH Configurator interface for SNMP v3 configuration. The main title is "Cisco URWB IW9167EH Configurator" with the version "5.21.200.136 - MESH END MODE". The left sidebar is the same as in the previous screenshot. The "SNMP" configuration page is active, showing the following settings:

- SNMP mode: v3
- SNMP v3 username: user
- SNMP v3 password: *****
- Show SNMP v3 password:
- SNMP v3 authentication proto: SHA
- SNMP v3 encryption: AES
- SNMP v3 encryption passphrase: *****
- Show SNMP v3 encryption passphrase:
- Enable SNMP periodic trap:
- Enable SNMP event trap:
- Engine ID: Currently Unavailable
- NMS hostname: 192.168.0.100
- Notification period (minutes): 1

Buttons for "Reset" and "Save" are visible at the bottom of the configuration area.

Disable SNMP via GUI



