

RUT900 SNMP

[Main Page](#) > [RUT Routers](#) > [RUT900](#) > [RUT900 Manual](#) > [RUT900 WebUI](#) > [RUT900 Services section](#) > **RUT900 SNMP**

The information in this page is updated in accordance with firmware version .

Note: [click here](#) for the old style WebUI (FW version RUT9XX_R_00.06.09.5 and earlier) user manual page.

□

Contents

- [1 Summary](#)
- [2 SNMP settings](#)
 - [2.1 SNMP agent settings](#)
 - [2.2 SNMP System Summary](#)
- [3 SNMP v3 users](#)
- [4 Communities](#)
- [5 Trap Settings](#)
 - [5.1 Trap Service Settings](#)
 - [5.2 Trap Rules](#)
 - [5.2.1 Signal strength](#)
 - [5.2.2 Connection type](#)
 - [5.2.3 Events log](#)
- [6 SNMP variables list](#)

Summary

Simple Network Management Protocol (SNMP) is a network management protocol used for collecting information and configuring network devices. This page is an overview of the SNMP function in RUT900 devices.

Note: SNMP is additional software that can be installed from the **System** → **Package Manager** page.

If you're having trouble finding this page or some of the parameters described here on your device's WebUI, you should **turn on "Advanced WebUI" mode**. You can do that by clicking the "Advanced" button, located at the top of the WebUI.

✖

SNMP settings

The **SNMP settings** page is used to configure SNMP accessibility and general SNMP information for your device.

SNMP agent settings



| Field | Value | Description |
|----------------------|--|---|
| Enable SNMP service | off on; default: off | Run SNMP service on system's startup. |
| Enable remote access | off on; default: off | Open port in firewall so that SNMP service may be reached from WAN. |
| IP type | IPv4 IPv6 IPv4v6; default: IPv4 | IP type used by SNMP. |
| Port | integer [0..65535]; default: 161 | SNMP service's port. |
| SNMP v1 Mode | off on; default: on | Enable/disable SNMP v1 Mode. |
| SNMP v2c Mode | off on; default: on | Enable/disable SNMP v2c Mode. |
| SNMP v3 Mode | off on; default: off | Enable/disable SNMP v3 Mode. |

SNMP System Summary

The **SNMP System Summary** section contains general information about SNMP on this device. You can also download this device's **MIB file** from this section.



| Field | Value | Description |
|------------|---|--|
| MIB file | -(interactive button) | Downloads the device's MIB file. |
| System OID | 1.3.6.1.4.1.48690 | OID or Object Identifier, is an identifier used to name and point to an object in the MIB hierarchy. |
| Location | string; default: location | Trap named sysLocation. |
| Contact | string; default: email@example.com | Trap named sysContact. |
| Name | string; default: name | Trap named sysName. |

SNMP v3 users

The **SNMP v3 users** page is used to create and manage users, who can be authenticated using SNMP v3. To configure an SNMP user, you must first create it:

1. Enter a custom name for the new user in the 'Name' field.
2. Click the 'Add' button.
3. Click the 'Edit' button next to the newly created user.



The SNMP user configuration window should look similar to this:



Note: this table has coloring scheme to indicate which fields can be seen with different configuration.

| Field | Value | Description |
|---------------------------|---|--|
| Enable | off on; default: off | Turns this SNMP user on or off. |
| Username | string; default: none | Set username to access SNMP. |
| Security level | No authentication, no privacy Authentication, no privacy Authentication and privacy ; default: No authentication, no privacy | A security level is an authentication strategy that is set up for the user. No authentication, no privacy - authenticates with a username. Authentication - provides MD5 or SHA algorithms for authentication. Privacy - Provides DES or AES encryption. |
| Authentication type | Authentication, no privacy Authentication and privacy : SHA MD5; default: SHA | Set authentication type to use with SNMP v3. |
| Authentication passphrase | Authentication, no privacy Authentication and privacy : string; default: none | Set authentication passphrase to generate key for SNMP v3. |
| Privacy type | Authentication and privacy : DES AES; default: DES | Set privacy type to use with SNMP v3. |
| Privacy passphrase | Authentication and privacy : string; default: none | Set privacy passphrase to generate key for SNMP v3. |
| Access Mode | Read-Only Read-Write; default: Read-Only | The access mode specifies the access the hosts in the community are allowed with respect to retrieving and modifying the MIB variables from a specific SNMP agent. |
| MIB subtree | string; default: none | Leave empty to access full MIB tree. |

Communities

The **SNMP Community** section is used to manage access rights. You can edit an SNMP community by clicking the 'Edit' button next to it:



This will redirect you to the community's configuration page.



| Field | Value | Description |
|----------------|------------------------------|----------------------------------|
| Community name | string; default: none | Name of the community. |
| IP Address | ip; default: none | IP address of the community. |
| IP Mask | ip; default: none | Netmask for IP of the community. |

Access Mode Read-Only | Read-Write; default: **Read-Only** Access mode for current community.

SNMPv6 community configuration page:



| Field | Value | Description |
|---|---|------------------------------------|
| Community name string; default: public | | Name of the community. |
| Source | ip6 domain name; default: default | Source of the community. |
| Access Mode | Read-Only Read-Write; default: Read-Only | Access mode for current community. |

Trap Settings

SNMP Traps are used to send alert messages to a central collector, the “SNMP manager” when an important event happens. A benefit of using Traps for reporting alarms is that they trigger instantaneously, rather than waiting for a status request from the manager.

Trap settings page is divided in two sections - **Trap service settings** and **Trap rules**. Trap service settings lets you manage hosts which will get configured alert messages, Trap rules lets you manage rules which when triggered will send alerts.

Trap Service Settings

The **Trap Service Settings** is used to manage **hosts** which will be alerted when an SNMP trap is triggered. The host list is empty by default thus, to begin configuration you must first create at least one host.

Click the 'Add' button at the bottom-right side of the table to create a new host.



The newly added Host configuration should look similar to this:



| Field | Value | Description |
|---------------|---|---|
| Host/IP | url ip; default: none | Hostname or IP address to transfer SNMP traffic to. |
| Port | integer [0..65535]; default: 162 | Trap host's port number. |
| Community | string; default: Public | Name of the community to which the trap belongs. |
| Delete | - (interactive button) | Deletes the host next to the button. |
| off/on slider | off on; default: off | Turns the host on or off. SNMP traffic is only sent to enabled hosts. |

Trap Rules

SNMP Trap Rules are alerts that trigger when certain user-specified events occur. When the trigger event happens, the trap will notify known SNMP hosts.

You can create a new trap rule by clicking the 'Add' button.



You should be redirected to the rule's configuration page which should look something like this:



Above is an example of what rule configuration window looks like. Below is a table with detailed explanations on how to configure the rule and what each of the fields mean.

To avoid redundancy, screenshots for the other rules will not be provided, since the structures, syntax and the overall look of the configuration windows for each rule are very similar. Instead, only tables containing information on how to edit each rule will be provided.

Signal strength

| Field | Value | Description |
|-----------------|---|---|
| Enable | off on; default: off | Enable or disable this rule. |
| Action | Signal strength trap | Rule will be triggered if signal strength falls below specified number. |
| Signal strength | integer [-130..0]; default: none | GSM signal's strength value in dBm, e.g. -85 |

Connection type

| Field | Value | Description |
|--------|-------------------------------|--|
| Enable | off on; default: off | Enable or disable this rule. |
| Action | Connection type trap | Rule will be triggered when connection type will change. |

Events log

| Event | Event subtype | Description |
|----------------------|---|---|
| Config change | All Specific config change; default: all | Informs on changes to the device's configuration. |
| Reboot | All From Web UI From ping reboot From reboot scheduler From button From SMS; default: All | Informs on if the device was rebooted. |
| Startup | Device startup completed | Informs on when the device is fully booted. |

| | | |
|------------------------|---|--|
| Mobile data | All Connected Disconnected; default All | Informs on changes to the state of the device's mobile connection. |
| New DHCP client | All Connected from LAN; default All | Informs on new DHCP lease give outs. |
| Reboot | All From button From Input/Output From Ping Reboot From Reboot Scheduler From WebUI From SMS; default: All | Informs after device reboot occurrences. |
| Signal strength | All - 121 dBm - 113 dBm - 113 dBm - 98 dBm - 98 dBm - 93 dBm - 93 dBm - 75 dBm - 75 dBm - 60 dBm - 60 dBm - 50 dBm; default: All | Informs on signal strength changes. |
| SMS | SMS received | Informs on received SMS messages. |
| SSH | All Successful authentication Unsuccessful authentication; default: All | Informs on successful or unsuccessful SSH login attempts. |
| WebUI | ALL Successful authentication Unsuccessful authentication; default: All | Informs on successful or unsuccessful HTTP/HTTPS login attempts. |

SNMP variables list

| Name | OID | Description |
|----------------------|-------------------------------|---|
| Device | | |
| serial | .1.3.6.1.4.1.48690.1.1.0 | Device serial number |
| routerName.0 | .1.3.6.1.4.1.48690.1.2.0 | Device name |
| productCode | .1.3.6.1.4.1.48690.1.3.0 | Device product (ordering) code |
| batchNumber | .1.3.6.1.4.1.48690.1.4.0 | Device batch number |
| hardwareRevision | .1.3.6.1.4.1.48690.1.5.0 | Device hardware revision |
| fwVersion | .1.3.6.1.4.1.48690.1.6.0 | Device RutOS firmware version |
| deviceUptime | .1.3.6.1.4.1.48690.1.7.0 | Device uptime |
| Mobile | | |
| modemNum | .1.3.6.1.4.1.48690.2.1.0 | The number of modems (regardless of their current state) present on this system |
| mIndex | .1.3.6.1.4.1.48690.2.2.1.1.1 | Available modem indexes; used to index OIDs between when the device has multiple modems |
| mDescr | .1.3.6.1.4.1.48690.2.2.1.2.1 | Modem description |
| mImei | .1.3.6.1.4.1.48690.2.2.1.3.1 | Modem IMEI |
| mModel | .1.3.6.1.4.1.48690.2.2.1.4.1 | Modem model |
| mManufacturer | .1.3.6.1.4.1.48690.2.2.1.5.1 | Modem manufacturer |
| mRevision | .1.3.6.1.4.1.48690.2.2.1.6.1 | Modem firmware version |
| mSerial | .1.3.6.1.4.1.48690.2.2.1.7.1 | Modem serial number |
| mIMSI | .1.3.6.1.4.1.48690.2.2.1.8.1 | Modem IMSI number |
| mSimState | .1.3.6.1.4.1.48690.2.2.1.9.1 | SIM card status |
| mPinState | .1.3.6.1.4.1.48690.2.2.1.10.1 | PIN status |
| mNetState | .1.3.6.1.4.1.48690.2.2.1.11.1 | Mobile network registration status |
| mSignal | .1.3.6.1.4.1.48690.2.2.1.12.1 | Signal strength level |
| mOperator | .1.3.6.1.4.1.48690.2.2.1.13.1 | Current mobile network operator |
| mOperatorNumber | .1.3.6.1.4.1.48690.2.2.1.14.1 | Mobile operator number (MCC+MNC) |
| mConnectionState | .1.3.6.1.4.1.48690.2.2.1.15.1 | Mobile data connection state |
| mConnectionType | .1.3.6.1.4.1.48690.2.2.1.16.1 | Mobile data connection type |
| mTemperature | .1.3.6.1.4.1.48690.2.2.1.17.1 | Modem's temperature in 0.1 degrees Celsius |
| mCellID | .1.3.6.1.4.1.48690.2.2.1.18.1 | Cell (Base transceiver station) ID |
| mSINR | .1.3.6.1.4.1.48690.2.2.1.19.1 | SINR value in dB |
| mRSRP | .1.3.6.1.4.1.48690.2.2.1.20.1 | RSRP value in dBm |
| mRSRQ | .1.3.6.1.4.1.48690.2.2.1.21.1 | RSRQ value in dB |
| mSent | .1.3.6.1.4.1.48690.2.2.1.22.1 | Total bytes sent |
| mReceived | .1.3.6.1.4.1.48690.2.2.1.23.1 | Total bytes received |
| mIP | .1.3.6.1.4.1.48690.2.2.1.24.1 | Modem IP address(es) |
| mSentToday | .1.3.6.1.4.1.48690.2.2.1.25.1 | Bytes sent today |
| mReceivedToday | .1.3.6.1.4.1.48690.2.2.1.26.1 | Bytes received today |
| mICCID | .1.3.6.1.4.1.48690.2.2.1.27.1 | SIM ICCID |
| mSentCurrentWeek | .1.3.6.1.4.1.48690.2.2.1.28.1 | Bytes sent this week |
| mReceivedCurrentWeek | .1.3.6.1.4.1.48690.2.2.1.29.1 | Bytes received this week |

| | | |
|-----------------------------------|-------------------------------|---|
| mSentCurrentMonth | .1.3.6.1.4.1.48690.2.2.1.30.1 | Bytes sent this month |
| mReceivedCurrentMonth | .1.3.6.1.4.1.48690.2.2.1.31.1 | Bytes received this month |
| connectionUptime | .1.3.6.1.4.1.48690.2.3.0.1 | Mobile connection uptime |
| Input/Output notifications | | |
| Hotspot Notifications | | |
| clientConnectedNotification | .1.3.6.1.4.1.48690.4.3.1 | Hotspot client connected trap |
| clientDisconnectedNotification | .1.3.6.1.4.1.48690.4.3.2 | Hotspot client disconnected trap |
| Hotspot | | |
| hsState | .1.3.6.1.4.1.48690.5.1.0 | Current Hotspot state |
| hsIP | .1.3.6.1.4.1.48690.5.2.0 | Hotspot IP address |
| hsNet | .1.3.6.1.4.1.48690.5.3.0 | WiFi interface ID |
| hsAuth | .1.3.6.1.4.1.48690.5.4.0 | Hotspot authentication type |
| hsSessionCount | .1.3.6.1.4.1.48690.5.5.0 | Hotspot current active session (connected user) count |
| Hotspot Sessions | | |
| hssIndex | .1.3.6.1.4.1.48690.5.6.1.1.1 | Connected Hotspot user indexes |
| hssMAC | .1.3.6.1.4.1.48690.5.6.1.2.1 | Hotspot user MAC addresses |
| hssIP | .1.3.6.1.4.1.48690.5.6.1.3.1 | Hotspot user local IP addresses |
| hssID | .1.3.6.1.4.1.48690.5.6.1.4.1 | Hotspot user session unique IDs |
| hssUsername | .1.3.6.1.4.1.48690.5.6.1.5.1 | Hotspot connected user usernames |
| hssState | .1.3.6.1.4.1.48690.5.6.1.6.1 | Hotspot user session states |
| hssDwLimit | .1.3.6.1.4.1.48690.5.6.1.7.1 | Hotspot user download limits |
| hssUpLimit | .1.3.6.1.4.1.48690.5.6.1.8.1 | Hotspot user upload limits |
| hssTimeLimit | .1.3.6.1.4.1.48690.5.6.1.9.1 | Hotspot user session time limit |
| hssIdleTimeout | .1.3.6.1.4.1.48690.5.6.1.10.1 | Hotspot user maximum idle timeout values |
| hssDwBandwidth | .1.3.6.1.4.1.48690.5.6.1.11.1 | Hotspot user maximum download speed |
| hssUpBandwidth | .1.3.6.1.4.1.48690.5.6.1.12.1 | Hotspot user maximum upload speed |
| hssURL | .1.3.6.1.4.1.48690.5.6.1.13.1 | Hotspot URL |