

Configure Simple Network Management Protocol (SNMP) Settings on an RV34x Series Router

Objective

Simple Network Management Protocol (SNMP) is used for network management, troubleshooting, and maintenance. SNMP records, stores, and shares information with the help of two key software: a network management system (NMS) that runs on manager devices and an agent that runs on managed devices. The RV34x Series Router supports SNMP versions 1, 2, and 3.

SNMP v1 is the original version of SNMP which lacks certain functionality and only works on TCP/IP networks, while SNMP v2 is an improved iteration of v1. SNMP v1 and v2c should only be chosen for networks that utilize either SNMPv1 or SNMPv2c. SNMP v3 is the newest standard of SNMP and addresses many of the issues of SNMP v1 and v2c. In particular, it addresses many of the security vulnerabilities from v1 and v2c. SNMP v3 also allows administrators to move to one common SNMP standard.

This article explains how to configure SNMP settings on the RV34x Series Router.

Applicable Devices

- RV34x Series

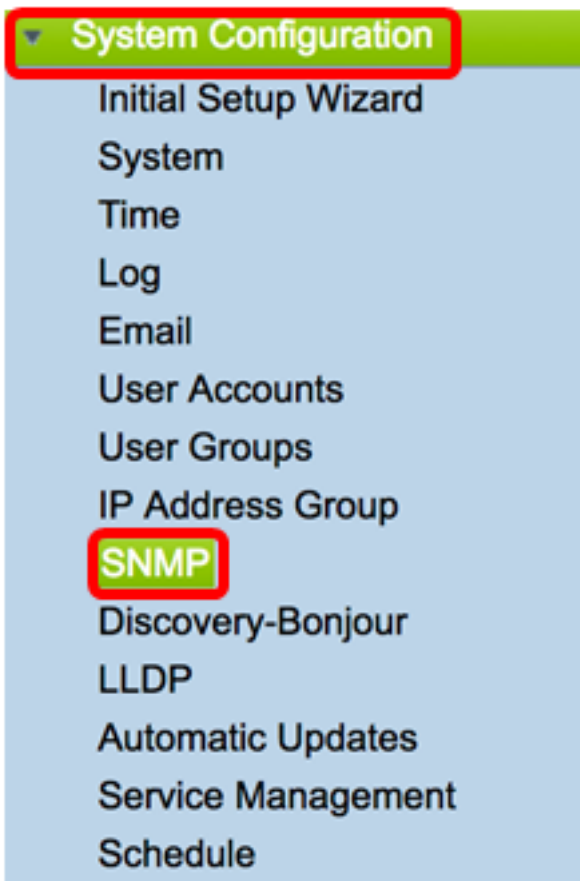
Software Version

- 1.0.1.16

Configure SNMP Settings on RV34x Series Router

Configure SNMP Settings

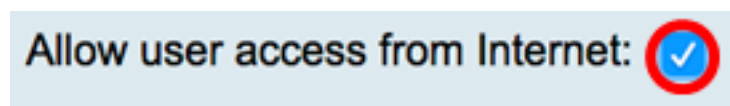
Step 1. Log in to the web-based utility of the router and choose **System Configuration > SNMP**.



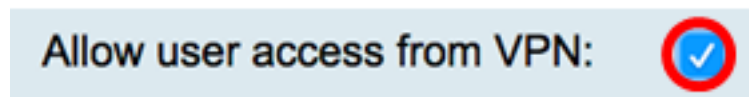
Step 2. Check the **SNMP Enable** check box to enable SNMP.



Step 3. (Optional) Check the **Enable Allow user access from Internet** check box to allow authorized user access outside the network through management applications such as the Cisco FindIT Network Management.



Step 4. (Optional) Check the **Allow user access from VPN** check box to allow authorized access from a VPN.

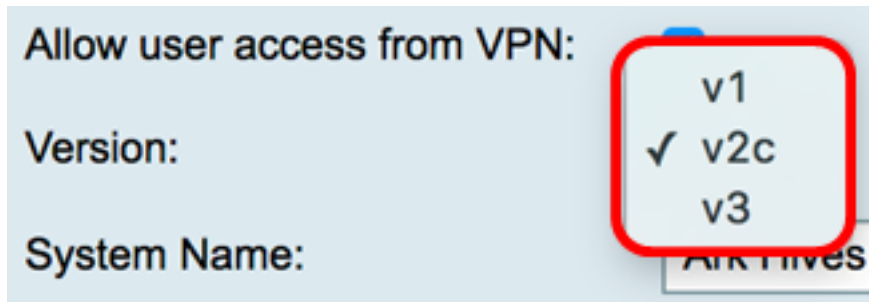


Step 5. From the Version drop-down menu, choose an SNMP version to use on the network. The options are:

- v1 — Least secured option. Uses plaintext for community strings.
- v2c — The improved error handling support provided by SNMPv2c includes expanded error codes that distinguish different types of errors; all types of errors are reported through a single error code in SNMPv1.
- v3 — SNMPv3 is a security model in which an authentication strategy is set up for a user and the group in which the user resides. Security level is the permitted level of security within a

security model. A combination of a security model and a security level determines which security mechanism is used when handling an SNMP packet.

Note: In this example, v2c is chosen.



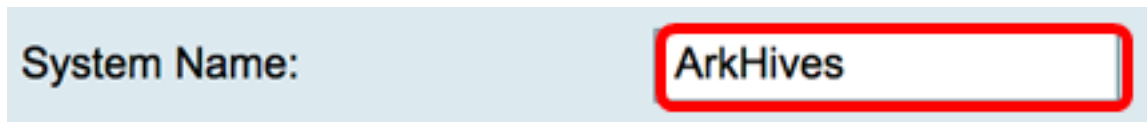
Allow user access from VPN:

Version: v1
✓ v2c
v3

System Name: ArkHives

Step 6. In the *System Name* field, enter a name for the router for easier identification in network management applications.

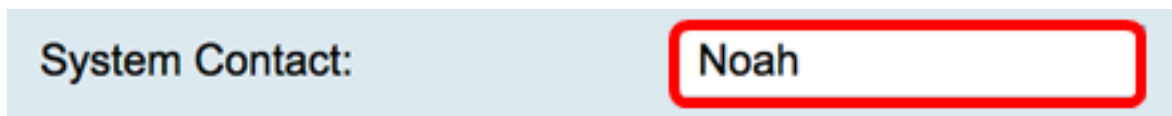
Note: In this example, ArkHives is used as the System Name.



System Name: ArkHives

Step 7. In the *System Contact* field, enter a name of an individual or administrator to identify with the router in case of emergency.

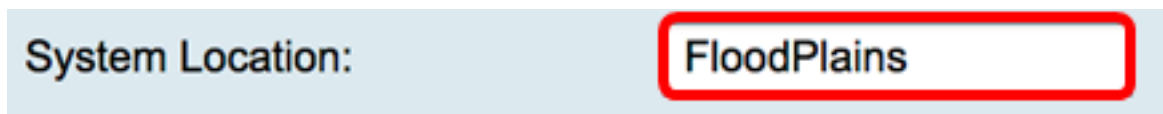
Note: For this example, Noah is used as the System Contact.



System Contact: Noah

Step 8. In the *System Location* field, enter a location of the router. This makes locating a problem much easier for an administrator.

Note: For this example, FloodPlains is used as the System Location.



System Location: FloodPlains

To proceed with the configuration, click on the SNMP version that was chosen in Step 5.

- [Configure SNMP 1 or v2c](#)
- [Configure SNMP v3](#)

[Configure SNMP 1 or v2c](#)

Step 1. If SNMP v2c was chosen in Step 5, enter the SNMP community name in the *Get Community* field. It creates read-only community which is used to access the information for SNMP agent. The community string sent in the request packet sent by sender has to match the community string on the agent device. The default string for read-only is public.

Note: The read-only password gives authority to retrieve information only. In this example, pblick is used.

Get Community:

pblick

Step 2. In the *Set Community* field, enter an SNMP community name. It creates read-write community which is used to access the information for SNMP agent. Only requests from the devices that identify themselves with this community name are accepted. This is a user-created name. The default is private.

Note: It is advisable to change both the passwords to something more customized in order to avoid security attack from outsiders. In this example, pribado is used.

Set Community:

pribado

You should now have successfully configured the SNMP v1 or v2 settings. Proceed to the [Trap Configuration](#) area.

[Configure SNMP v3](#)

Step 1. If SNMP v3 was chosen, click a radio button in the Username area to choose an access privilege. The options are:

- guest — Read-only privileges
- admin — Read & write privileges

Note: For this example, guest is chosen.

The Access Privilege area shows the type of privilege depending on the radio button clicked.

Username:

guest admin

Access Privilege:

Read

Step 2. Click a radio button in the Authentication Algorithm area to choose a method which the SNMP agent will use to authenticate. The options are:

- None — No user authentication is used.
- MD5 — Message-Digest Algorithm 5 uses a 128-bit hash value for authentication. Requires Username and Password.
- SHA1 — Secure Hash Algorithm (SHA-1) is a one-way hashing algorithm that produces a 160-bit digest. SHA-1 computes slower than MD5, but is more secure than MD5.

Note: For this example, MD5 is chosen.

Authentication Algorithm:

None MD5 SHA1

Authentication Password:

Note: If you chose None, Skip to the [Trap Configuration](#) area.

Step 3. In the *Authentication Password* field, enter a password.

Authentication Algorithm: None MD5 SHA1

Authentication Password:

Step 4. (Optional) In the Encryption Algorithm area, click on a radio button to choose how SNMP information will be encrypted. The options are:

- None — No encryption is used. If this step is chosen, skip to the [Trap Configuration](#) area.
- DES — Data Encryption Standard (DES) is a 56-bit encryption method which is not very secure, but may be required for backwards compatibility.
- AES — Advanced Encryption Standard (AES). If this is chosen, an encryption password is required.

Note: For this example, DES is chosen.

Encryption Algorithm: None DES AES

Encryption Password:

Step 5. (Optional) If DES or AES was chosen, enter an encryption password in the *Encryption Password* field.

Encryption Algorithm: None DES AES

Encryption Password:

You should now have successfully configure the SNMP v3 settings. Proceed now to the [Trap Configuration](#) area.

Trap Configuration

Step 1. In the *Trap Receiver IP Address* field, enter an IPv4 or an IPv6 IP address that will receive the SNMP traps.

Note: For this example, 192.168.2.202 is used.

Trap Configuration

Trap Receiver IP Address (Hint: 1.2.3.4 or fc02::0)

Step 2. Enter a User Datagram Protocol (UDP) port number in the *Trap Receiver Port* field. The SNMP agent checks this port for access requests.

Note: For this example, 161 is used.

Trap Receiver Port

161

Step 3. Click **Apply**.

Trap Configuration

Trap Receiver IP Address

192.168.2.100

Trap Receiver Port

161

Apply

Cancel

SNMP



Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.


SNMP Enable:	<input checked="" type="checkbox"/>
Allow user access from Internet:	<input checked="" type="checkbox"/>
Allow user access from VPN:	<input checked="" type="checkbox"/>
Version:	v3
System Name:	Ark Hives
System Contact:	Noah
System Location:	FloodPlains
Username:	<input checked="" type="radio"/> guest <input type="radio"/> admin
Access Privilege:	Read
Authentication Algorithm:	<input type="radio"/> None <input checked="" type="radio"/> MD5 <input type="radio"/> SHA1
Authentication Password:
Encryption Algorithm:	<input type="radio"/> None <input checked="" type="radio"/> DES <input type="radio"/> AES
Encryption Password:

Trap Configuration

Trap Receiver IP Address	192.168.2.100	(Hint: 1.2.3.4 or fc02::0)
Trap Receiver Port	161	

Apply

Cancel

Step 4. (Optional) To save the configuration permanently, go to the Copy/Save Configuration page or click the  icon at the upper portion of the page.

You should now have successfully configured the SNMP settings on an RV34x Series Router.