SNMP Configuration on the RV315W VPN Router

Objective

Simple Network Management Protocol (SNMP) is a TCP/IP protocol for network management. SNMP allows for administrators to oversee network performance, error rates. SNMP can also map network availability. The SNMP framework consists of three elements; an SNMP manager, an SNMP agent, and a MIB. The function of the SNMP manager is to control and monitor the activities of the network hosts that utilize SNMP. The SNMP agent is within the software of the device and it aids in the maintenance of data in order to manage the system. Lastly, the Management Information Base (MIB) is a virtual storage area for network management information. These three combine to monitor and manage the devices in a network.

This article helps explain how to configure SNMP on the RV315W VPN Router.

Applicable Device

- RV315W

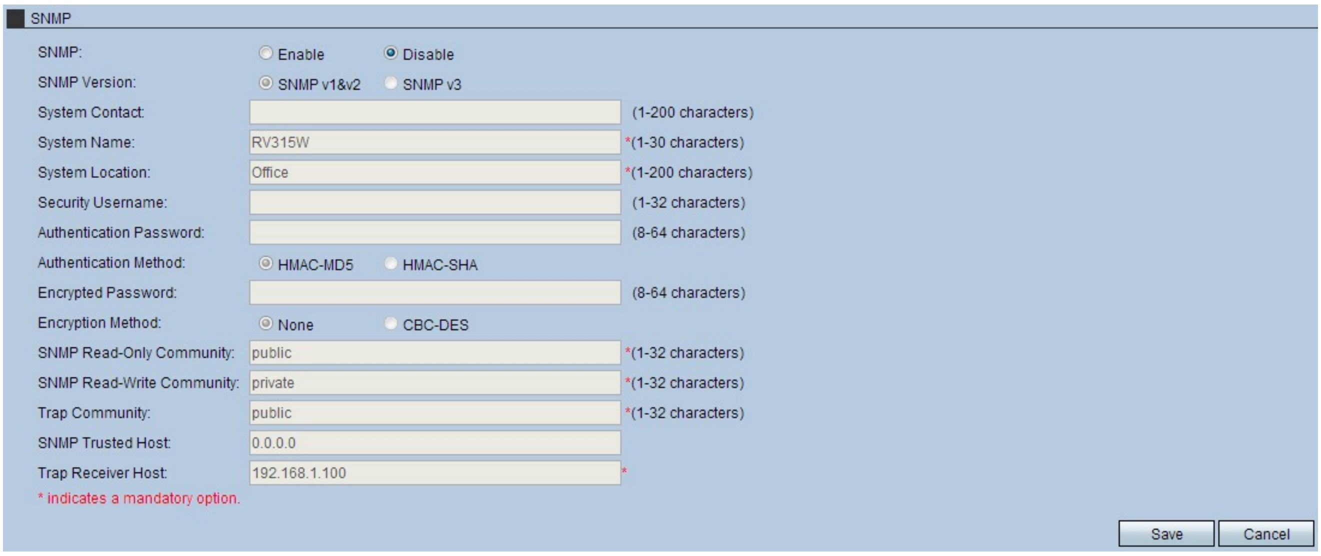
Software Version

- 1.01.03

Configure SNMP

SNMP v1 is the original version of SNMP, which lacks certain functionality and only works on TCP/IP networks, SNMP v2 is an improved iteration of v1. SNMP v1&v2 should only be chosen for networks that utilize either SNMPv1 or SNMPv2. SNMP v3 is the newest standard of SNMP and addresses many of the issues of SNMP v1 and v2. In particular, it addresses many of the security vulnerabilities from v1 and v2. SNMP v3 also allows administrators to move to one common SNMP standard.

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



SNMP

SNMP:	○ Enable ● Disable	
SNMP Version:	● SNMP v1&v2 ○ SNMP v3	
System Contact:		(1-200 characters)
System Name:	RV315W	*(1-30 characters)
System Location:	Office	*(1-200 characters)
Security Username:		(1-32 characters)
Authentication Password:		(8-64 characters)
Authentication Method:	● HMAC-MD5 ○ HMAC-SHA	
Encrypted Password:		(8-64 characters)
Encryption Method:	● None ○ CBC-DES	
SNMP Read-Only Community:	public	*(1-32 characters)
SNMP Read-Write Community:	private	*(1-32 characters)
Trap Community:	public	*(1-32 characters)
SNMP Trusted Host:	0.0.0.0	
Trap Receiver Host:	192.168.1.100	*

* indicates a mandatory option.

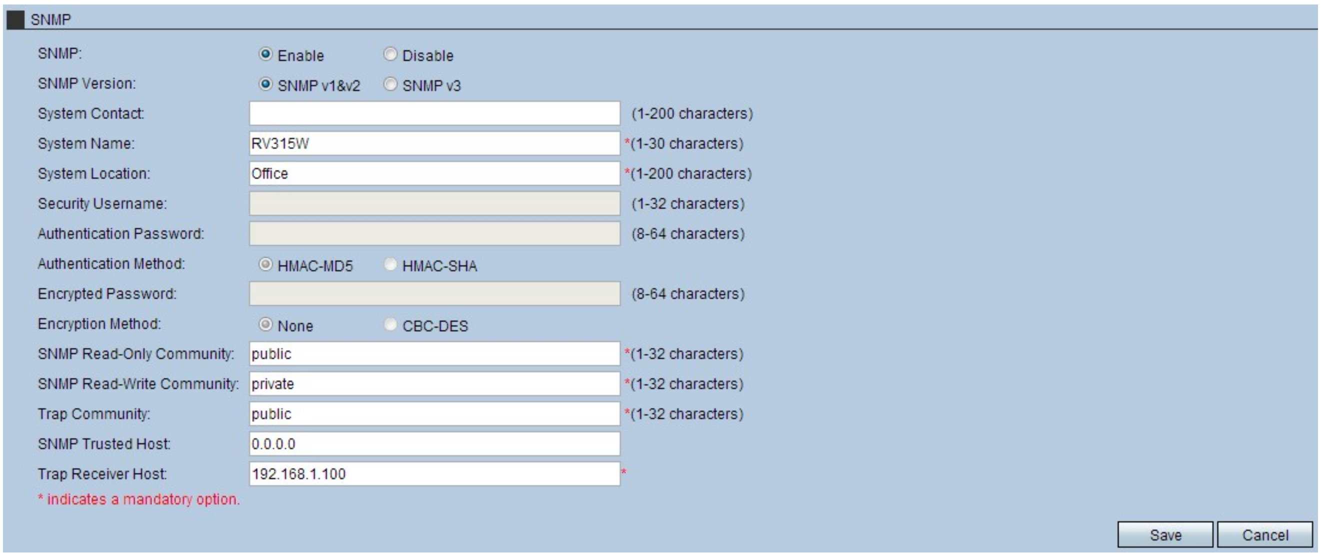
Step 2. Click the **Enable** radio button to enable SNMP.

Step 3. Click the desired SNMP version radio button.

- SNMP v1&v2 — SNMP v1 is the original iteration of SNMP and lacks certain functionality, SNMP v2 is the newer version that improves functionality, but this option should only be chosen for networks that run either SNMP v1 or SNMP v2.

- SNMP v3 — SNMP 3 is the newest version, that allows administrators to utilize one standard. This option should be chosen as it patches many security flaws within v1 and v2.

Configure SNMP for SNMP v1&v2



SNMP

SNMP:	● Enable ○ Disable	
SNMP Version:	● SNMP v1&v2 ○ SNMP v3	
System Contact:		(1-200 characters)
System Name:	RV315W	*(1-30 characters)
System Location:	Office	*(1-200 characters)
Security Username:		(1-32 characters)
Authentication Password:		(8-64 characters)
Authentication Method:	● HMAC-MD5 ○ HMAC-SHA	
Encrypted Password:		(8-64 characters)
Encryption Method:	● None ○ CBC-DES	
SNMP Read-Only Community:	public	*(1-32 characters)
SNMP Read-Write Community:	private	*(1-32 characters)
Trap Community:	public	*(1-32 characters)
SNMP Trusted Host:	0.0.0.0	
Trap Receiver Host:	192.168.1.100	*

* indicates a mandatory option.

Step 4. (Optional) Enter the contact information in the System Contact field. This is the individual to contact for network assistance.

Step 5. Enter a name in the System Name field. This is the name allocated to SNMP setup.

Step 6. Enter a location in the System Location field. This is where the system is located.

Step 7. Enter a community in the SNMP Read-Only Community field. This is the client parameter for read only access of the SNMP setup.

Step 8. Enter a community in the SNMP Read-Write Community field. This is the client parameter for read and write access of the SNMP setup.

Step 9. Enter a community in the Trap Community field. This is the community with the ability to utilize SNMP traps. Traps are directed notifications sent to the administrator. Traps allows for the administrator to manage each device by allowing their user to notify them by using a trap.

Step 10. Enter a host in the SNMP Trusted Host field. This is the IP address of the trust host for the SNMP setup.

Step 11. Enter a host in the Trap Receiver Host field. This is the IP address of the administrator to receive the traps.

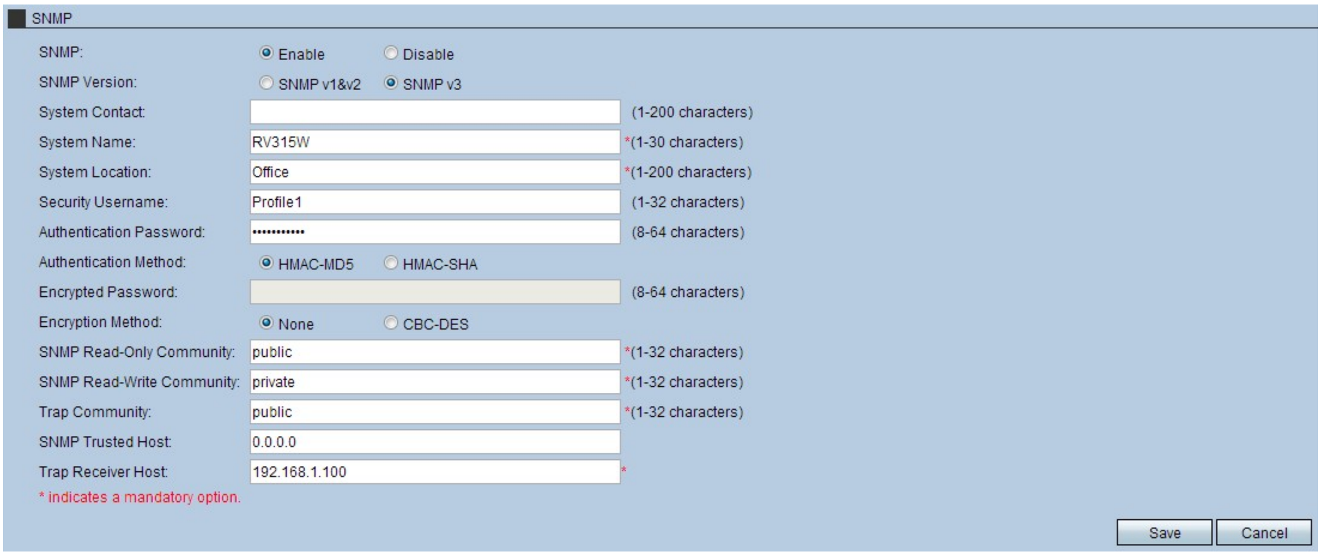
Step 12. Click **Save** to apply settings.

Configure SNMP for SNMP v3

Step 4. (Optional) Enter the contact information in the System Contact field. This is the individual to contact for network assistance.

Step 5. Enter a name in the System Name field. This is the name allocated to SNMP setup.

Step 6. Enter a location in the System Location field. This is where the system is located.



SNMP

SNMP:	● Enable ○ Disable	
SNMP Version:	○ SNMP v1&v2 ● SNMP v3	
System Contact:		(1-200 characters)
System Name:	RV315W	*(1-30 characters)
System Location:	Office	*(1-200 characters)
Security Username:	Profile1	(1-32 characters)
Authentication Password:	•••••••••••	(8-64 characters)
Authentication Method:	● HMAC-MD5 ○ HMAC-SHA	
Encrypted Password:		(8-64 characters)
Encryption Method:	● None ○ CBC-DES	
SNMP Read-Only Community:	public	*(1-32 characters)
SNMP Read-Write Community:	private	*(1-32 characters)
Trap Community:	public	*(1-32 characters)
SNMP Trusted Host:	0.0.0.0	
Trap Receiver Host:	192.168.1.100	*

* indicates a mandatory option.

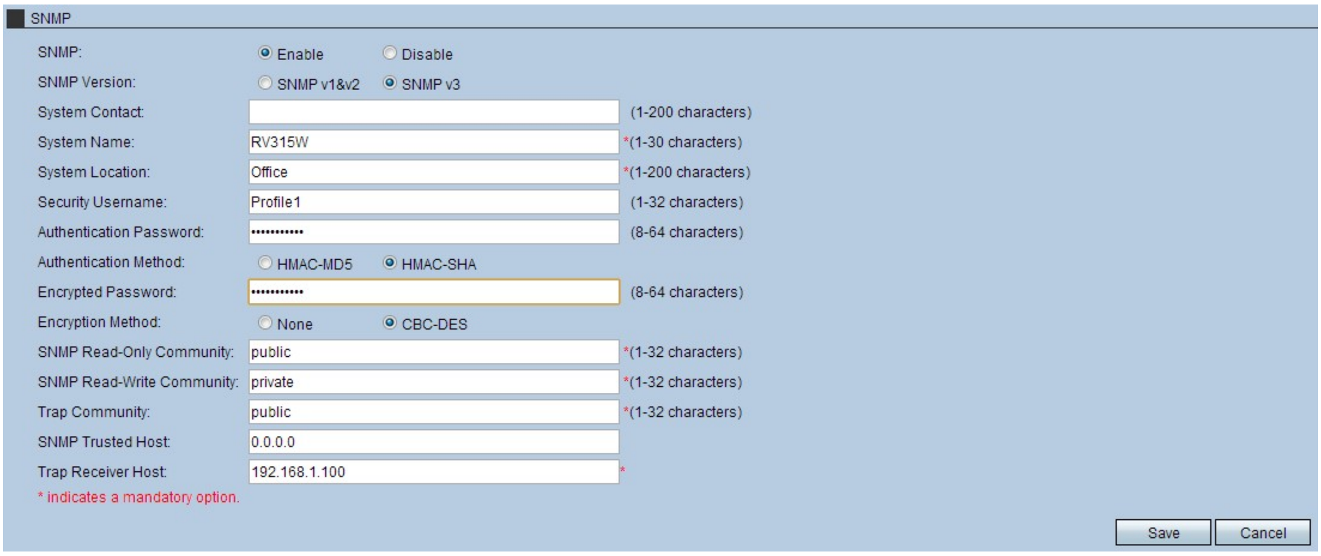
Step 7. (Optional) Enter a username in the Security Username field. This is the username that is used in order to gain access to the SNMP setup.

Step 8. (Optional) Enter a password in the Authentication Password field. This is the password that is used in order to gain access to the SNMP setup.

Step 9. Click the HMAC-MD5 or HMAC-SHA radio button in the Authentication Method field. The Hash-based message authentication code (HMAC) is an encrypted code that combines an authentication code and a secret cryptographic key. The primary purpose of HMAC is for message security. An HMAC will authenticate the data based off secret keys produced.

- HMAC MD5 — This hash algorithm has several security flaws and data can be compromised. The HMAC MD5 is a mechanism for message authentication using cryptographic hash functions. MD5 is utilized in situations where superior performance speed is vital for a system, albeit less secure.

- HMAC SHA — This hash algorithm is much more secure as the encryption method is superior. This is a more secure mechanism for message authentication using cryptographic hash functions. HMAC SHA should be used when security is of vital importance.



SNMP

SNMP:	● Enable ○ Disable	
SNMP Version:	○ SNMP v1&v2 ● SNMP v3	
System Contact:		(1-200 characters)
System Name:	RV315W	*(1-30 characters)
System Location:	Office	*(1-200 characters)
Security Username:	Profile1	(1-32 characters)
Authentication Password:	•••••••••••	(8-64 characters)
Authentication Method:	○ HMAC-MD5 ● HMAC-SHA	
Encrypted Password:	•••••••••••	(8-64 characters)
Encryption Method:	○ None ● CBC-DES	
SNMP Read-Only Community:	public	*(1-32 characters)
SNMP Read-Write Community:	private	*(1-32 characters)
Trap Community:	public	*(1-32 characters)
SNMP Trusted Host:	0.0.0.0	
Trap Receiver Host:	192.168.1.100	*

* indicates a mandatory option.

Step 10. Enter a password in the Encrypted Password field.

Step 11. Click the CBC-DES radio button in the Encryption Method field. CBC and DES are encryption standards that combine to secure data that is transferred.

Step 12. Enter a community in the SNMP Read-Only Community field. This is the client parameter for read only access of the SNMP setup.

Step 13. Enter a community in the SNMP Read-Write Community field. This is the client parameter for read and write access of the SNMP setup.

Step 14. Enter a community in the Trap Community field. This is the community with the ability to utilize SNMP traps. Traps are directed notification sent to the administrator. Traps allows for the administrator to manage each device by allowing their user to notify them by using a trap.

Step 15. Enter a host in the SNMP Trusted Host field. This is the IP address of the trust host for the SNMP setup.

Step 16. Enter a host in the Trap Receiver Host field. This is the IP address of the administrator to receive the traps.

Step 17. Click **Save** to apply settings.