

Simple Network Management Protocol (SNMP) Configuration on RV215W

Objective

Simple Network Management Protocol (SNMP) is an application layer protocol that is used to manage and monitor a network. SNMP is used by network administrators to manage network performance, detect and correct network problems, and collect network statistics. 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. The user must install a SNMP v3 manager program to view SNMP notifications.

This article explains how to configure SNMP on the RV215W.

Applicable Devices

- RV215W

Software Version

- 1.1.0.5

SNMP Configuration

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

SNMP

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

SNMPv3 User Configuration

UserName: guest admin

Access Privilege: Read Write User

Security level:

Authentication Algorithm Server: MD5 SHA

Authentication Password:

Privacy Algorithm: DES AES

Privacy Password:

Trap Configuration

IP Address: (Hint: 192.168.1.100 or fec0::64)

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

Community:

SNMP Version:

Save

Cancel

SNMP System Information

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

Step 1. Check **Enable** in the SNMP field to allow SNMP configuration on the RV215W.

Note: The engine ID for the agent of the RV215W is displayed in the Engine ID field. Engine IDs are used to uniquely identify agents on managed devices.

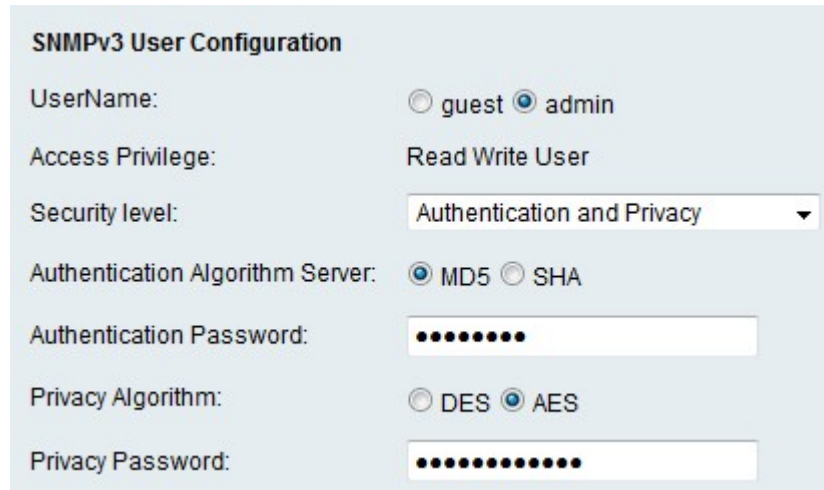
Step 2. Enter a name for the system contact in the SysContact field. It is common practice to include contact information for the system contact.

Step 3. Enter the physical location of the RV215W in the SysLocation field.

Step 4. Enter a name for identification of the RV215W in the SysName field.

Step 5. Click **Save**.

SNMPv3 User Configuration



SNMPv3 User Configuration

UserName: guest admin

Access Privilege: Read Write User

Security level: Authentication and Privacy

Authentication Algorithm Server: MD5 SHA

Authentication Password:

Privacy Algorithm: DES AES

Privacy Password:

Step 1. Click the radio button that corresponds to the desired account to configure in the UserName field. The access privilege of the user is displayed in the Access Privilege field.

- Guest — A guest user only has read privileges.
- Admin — An admin user has read and write privileges.

Step 2. From the Security level drop-down list choose the desired security. Authentication is used to authenticate and allow users to view or manage the SNMP features. Privacy is another key that can be used to increase security on the SNMP feature.

- No Authentication and No Privacy — No authentication or privacy password is required by the user.
- Authentication and No Privacy — Only authentication is required by the user.
- Authentication and Privacy — Both authentication and a privacy password is required by the user.

Step 3. If the security level includes authentication, click the radio button that corresponds to the desired server in the Authentication Algorithm Server field. This algorithm is a hash function. Hash functions are used to convert keys into a designated bit message.

- 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.

Step 4. Enter a password for the users in the Authentication Password field.

Step 5. If the security level includes privacy, click the radio button that corresponds to the desired algorithm in the Privacy Algorithm field.

- DES — Data Encryption Standard (DES) is an encryption algorithm that uses the same method to encrypt and decrypt a message. The DES algorithm processes faster than AES.
- AES — Advanced Encryption Standard (AES) is an encryption algorithm that uses different methods to encrypt and decrypt a message. This makes AES a more secure encryption algorithm than DES.

Step 6. Enter a privacy password for the users in the Privacy Password field.

Step 7. Click **Save**.

Trap Configuration

Traps are generated SNMP messages used to report system events. A trap will force a managed device to send a SNMP message to the network manager which notifies the network manager of a system event.



The screenshot shows a 'Trap Configuration' form with the following fields and values:

Field	Value	Hint/Range
IP Address:	192.168.1.100	(Hint: 192.168.1.100 or fec0::64)
Port:	162	(Range: 162 or 1025 - 65535, Default: 162)
Community:	community1	
SNMP Version:	v1	

Step 1. Enter the IP address to which the trap notifications will be sent in the IP address field.

Step 2. Enter the port number of the IP address to which the trap notifications will be sent in the Port field.

Step 3. Enter the community string to which the trap manager belongs to in the Community field. A community string is a text string that acts as a password. It is used by SNMP to authenticate messages sent between an agent and a network manager.

Note: This field is only applicable if the SNMP trap version is not version 3.

Step 4. From the SNMP Version drop-down list choose the SNMP manager version for the SNMP trap messages.

- v1 — Uses a community string to authenticate trap messages.
- v2c — Uses a community string to authenticate trap messages.
- v3 — Uses encrypted passwords to authenticate trap messages.

Step 5. Click **Save**.