Simple Network Management Protocol (SNMP) Groups Configuration on the WAP121 and WAP321 Access Points

Objective

Simple Network Management Protocol (SNMP) groups are useful to divide SNMP clients into separate groups and then set common authorization and access privileges to each group. This allows SNMP to determine which security mechanism it employs when it handles an SNMP packet from a certain group of agents. The WAP121 and WAP321 have two default groups, RO and RW, which can neither be edited nor deleted. RO is a read-only group, and RW is a read/write group, both of which use authentication and data encryption. The WAPs can have up to 8 groups configured including the default groups.

This article explains how to configure Simple Network Management Protocol (SNMP) Groups on the WAP121 and WAP321 access points.

Applicable Devices

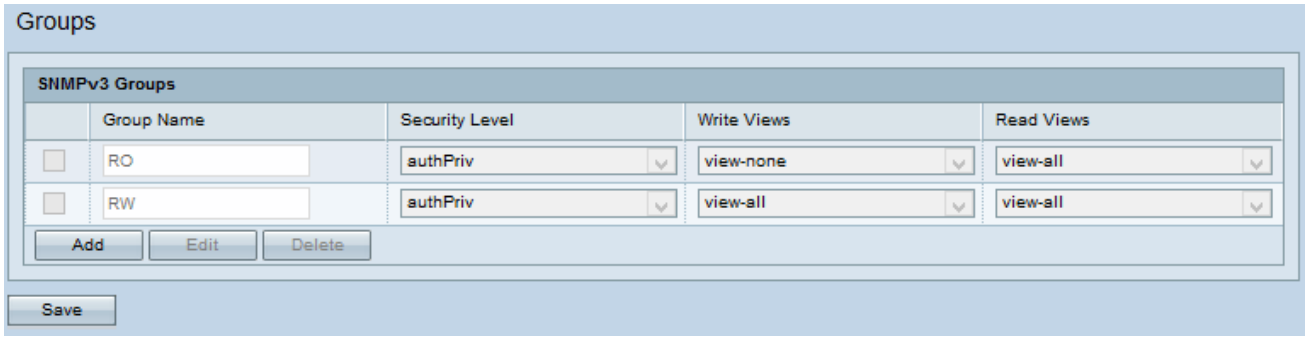
- WAP121
- WAP321

Software Version

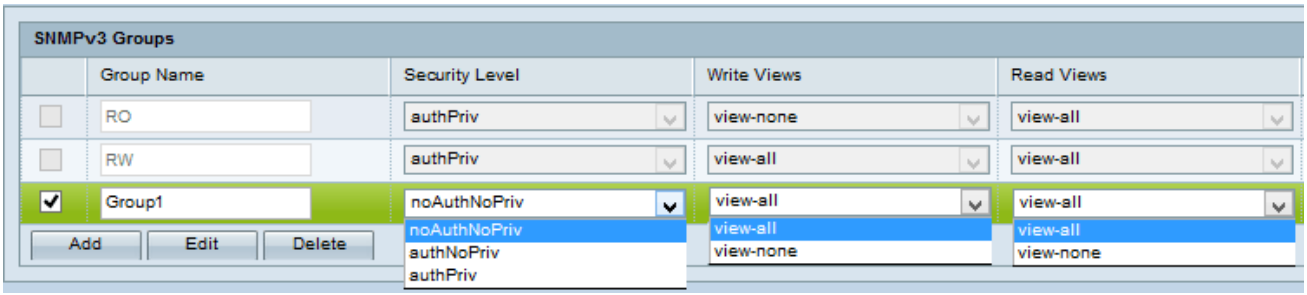
- 1.0.3.4

SNMP Group Configuration

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



Step 2. Click **Add** to add a new SNMP group.



Step 3. Check the check box that corresponds to the new group added.

Step 4. Click **Edit** to edit the new SNMP group.

Step 5. Enter a name used to identify the group in the Group Name field. The default names of RO and RW cannot be reused. Group names can contain up to 32 alphanumeric characters.

Step 6. Choose the appropriate security level from the Security Level drop-down list.

- NoAuthNoPriv — Provides no authentication and no data encryption (no security).
- AuthNoPriv — Provides authentication but no data encryption (no security). Authentication is provided by an MD5 passphrase.
- AuthPriv — Authentication and data encryption. Authentication is provided by an MD5 passphrase. Data encryption is provided by DES passphrase.

Note: For the created groups that require authentication, encryption, or both, you must define the MD5 and DES keys/passwords on the *SNMP Users* page. Refer to the article *SNMP User Configuration on the WAP121 and WAP321 Access Points* for user configuration.

Step 7. Choose the write access to all management objects (MIBs) for the new group from the Write Views drop-down list. This defines the action a group may perform on MIBs. This list will also include any new SNMP Views that have been created on the WAP.

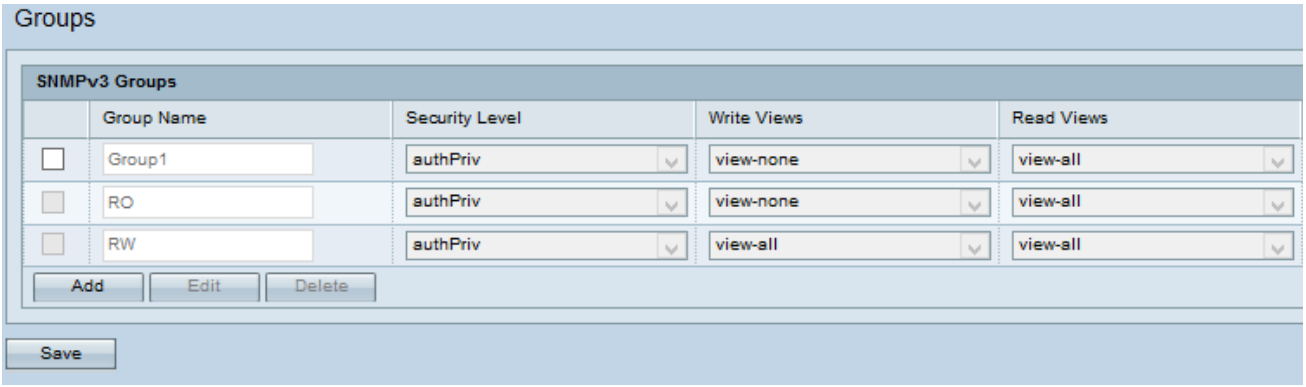
- View-all — This allows groups to create, alter, and delete all MIBs.
- View-none — This restricts the group so that no one can create or edit the MIBs.

Note: For configuration of a new view refer to the article *SNMP Views Configuration on the WAP121 and WAP321 Access Points*.

Step 8. Choose the read access for all management objects (MIBs) for the new group from the Read Views drop-down list. The default options given below appears along with any other views created on the WAP.

- View-all — This allows groups to view and read all MIBs.
- View-none — This restricts the group so that no one can view or read any MIBs.

Step 9. Click **Save** to save the configuration.



Step 10. (Optional) To edit a group from the list, check the check box for the desired group and click **Edit**.

Step 11. (Optional) The SNMPv3 Groups field displays the names of the current groups configured on the Access Point. To remove a group from the list, check the check box for the unwanted group and click **Delete**.