

# Configure Simple Network Management Protocol (SNMP) Groups on the WAP551 and WAP561 Access Points

## Objective

Simple Network Management Protocol (SNMP) groups are useful when sorting SNMP clients into separate groups, and then setting 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.

This article explains how to configure Simple Network Management Protocol (SNMP) groups on the Cisco WAP551 and WAP561 access points.

## Applicable Devices

- WAP551
- WAP561

## Software Version

- v1.2.0.2 - WAP551
- v1.2.0.2 - WAP561

## SNMP Group Configuration

Step 1. Log in to the Web Configuration Utility of the Access Point and choose **SNMP > Groups**. The *SNMP Groups* page opens:

SNMPv3 Groups				
	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all

Buttons: Add, Edit, Delete, Save

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

### Groups

#### SNMPv3 Groups

	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all

Step 3. Check the check box of the newly created group.

### Groups

#### SNMPv3 Groups

	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all
<input type="checkbox"/>		noAuthNoPriv	view-all	view-all

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

### Groups

#### SNMPv3 Groups

	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/>		noAuthNoPriv	view-all	view-all

Step 5. Enter a name for the new 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. The name chosen has no impact on the operation of the SNMP group.

## Groups

### SNMPv3 Groups

	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/>	GN	noAuthNoPriv	view-all	view-all

Add
Edit
Delete

Save

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

## Groups

### SNMPv3 Groups

	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/>	GN	noAuthNoPriv	view-all	view-all

Add
Edit

Save

The available options are described as follows:

- 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 key/password.
- AuthPriv — Provides both authentication and data encryption.

**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. For user configuration, refer to the article [SNMP User Configuration on the WAP551 and WAP561 Access Points](#).

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 actions a group may perform on MIBs. This list will also include any new SNMP Views that have been created on the WAP.

## Groups

### SNMPv3 Groups

	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/>	GN	noAuthNoPriv	view-all view-none	view-all

Add
Edit
Delete

Save

The available options are described as follows:

- View-all — Allows groups to create, alter, and delete all MIBs.
- View-none — Restricts group to create, alter, or delete any MIBs

**Note:** For configuration of new view, refer to the article [Simple Network Management Protocol \(SNMP\) Views Configuration on the WAP551 and WAP561 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 appear along with any other views created on the WAP.

## Groups

### SNMPv3 Groups

	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/>	GN	noAuthNoPriv	view-all	view-all view-none

Add
Edit
Delete

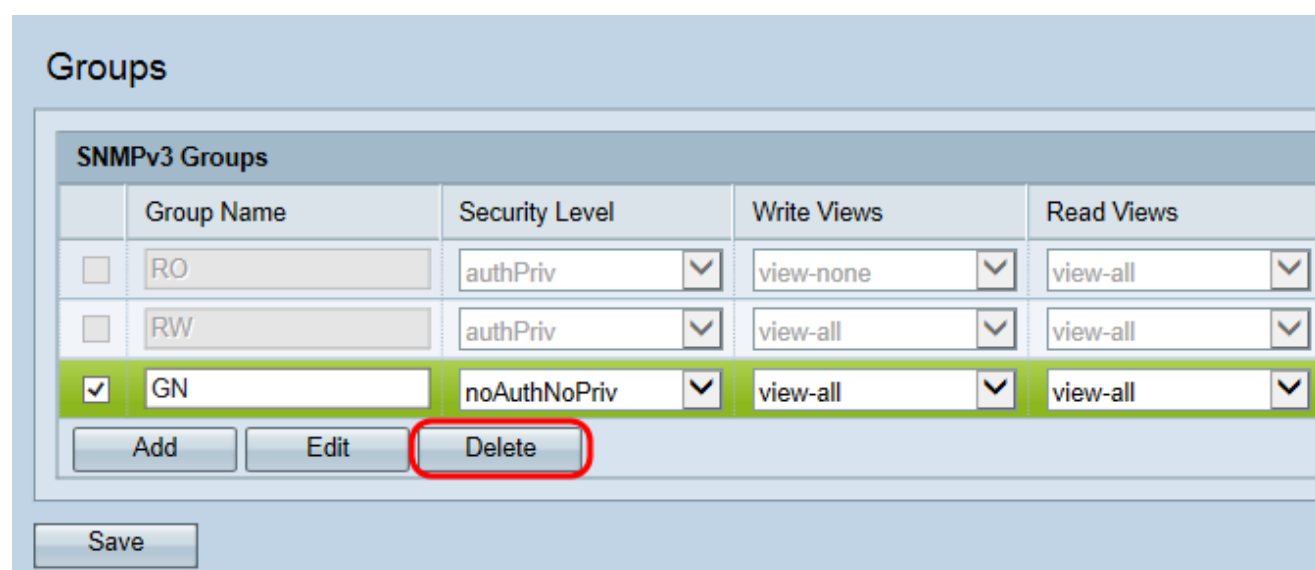
Save

The available options are described as follows:

- View-all — Allows groups to view and read all MIBs.
- View-none — Restricts group to view or read any MIBs.

Step 9. (Optional) For each additional SNMP group you need, click **Add** and repeat Steps 2 through 8.

Step 10. (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**.

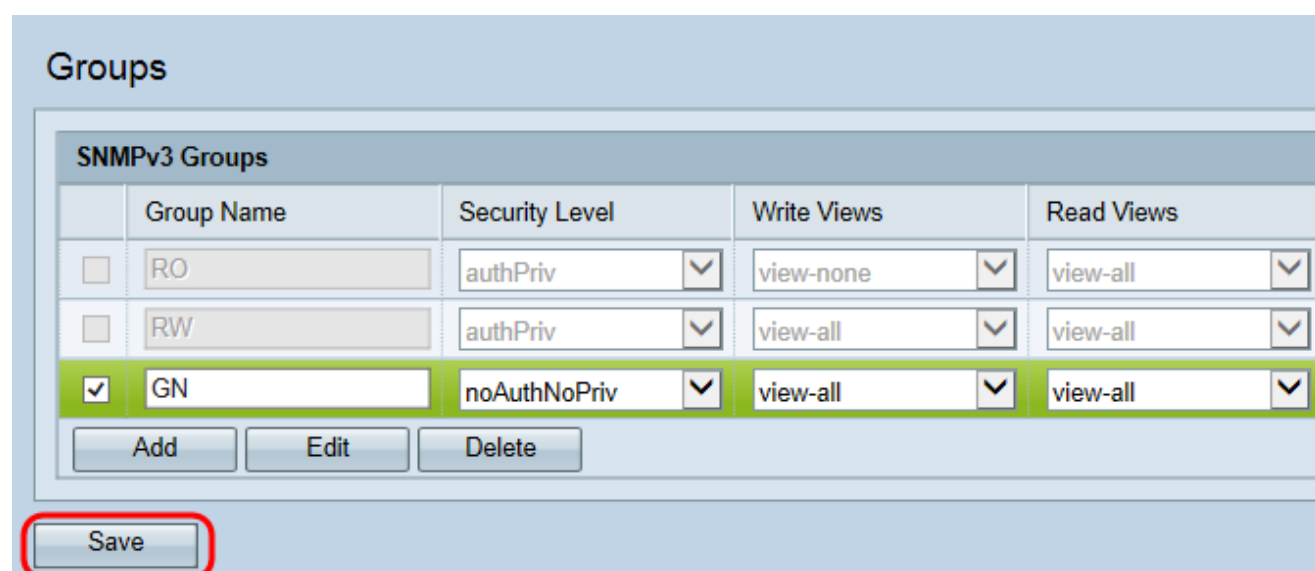


The screenshot shows the 'Groups' configuration page. Under the 'SNMPv3 Groups' section, there is a table with the following data:

	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/>	GN	noAuthNoPriv	view-all	view-all

Below the table are three buttons: 'Add', 'Edit', and 'Delete'. The 'Delete' button is circled in red. At the bottom of the page is a 'Save' button.

Step 11. Click **Save** to save the configuration.



This screenshot shows the same 'Groups' configuration page as the previous one. In this step, the 'Save' button at the bottom left is circled in red, indicating the final action to be taken.