

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

Objective

Simple Network Management Protocol (SNMP) is used to manage network devices. It helps to keep a record of the activities of various devices in the network, which helps you to find the point of issue in the network when needed. The user based security model in SNMPv3 allows you to separate devices into user groups, assign them various security credentials, and thus control the authorization of management operation. This article explains how to configure Simple Network Management Protocol (SNMP) user configuration on WAP121 and WAP321 Access Points.

Applicable Devices

- WAP121
- WAP321

Software Version

- 1.0.3.4

SNMP User Configuration

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

	User Name	Group	Authentication Type	Authentication Pass Phrase	Encryption Type	Encryption Pass Phrase
<input type="checkbox"/>	New	RW	MD5	*****	DES	*****
<input type="checkbox"/>	User	RO	None		None	

Step 2. Click **Add** to add a new user.

Note: The user configuration page on WAP121 and WAP321 access points allows you to create up to eight new users.

Users

SNMPv3 Users						
	User Name	Group	Authentication Type	Authentication Pass Phrase	Encryption Type	Encryption Pass Phrase
<input type="checkbox"/>	New	RW	MD5	*****	DES	*****
<input type="checkbox"/>	User	RO	None		None	
<input checked="" type="checkbox"/>	User2	RW	MD5	*****	DES	*****
		RO	MD5		DES	
		RW	None		None	

Add Edit Delete

Save

Step 3. Check the check box that corresponds to the new user based on which you can provide the authentication and encryption to each individual.

Step 4. Click **Edit** to enter the required information.

Step 5. Enter the user name of the new SNMP user in the User Name field. It can contain up to 32 alphanumeric characters.

Step 6. Choose a group for the user from the Group drop-down list. The available options are:

- Read Only (RO) — This group allows a user to only view the configuration.
- Read and Write (RW) — This group allows a user to view the configuration and also make the necessary changes to the configuration.

Note: To create more groups, refer to the article *SNMP Group Configuration on the WAP121 and WAP321 Access Points*.

Step 7. Choose the authentication type for the user from the Authentication Type drop-down list. If you want to use a password to strengthen authentication, choose **MD5**. MD5 is a hash function that produces a 128 bit hash value for the password; otherwise choose **None**. Skip Step 8 if you have chosen None.

Step 8. Enter the associated authentication pass phrase for the user in the Authentication Pass Phrase field if you chose MD5 in Step 7. This is the SNMP password that has to be configured to authenticate the devices in order for them to connect with each other. The pass phrase has to match on both the devices. The pass phrase can range from 8 to 32 characters in length.

Step 9. The access point provides the encryption of data with the DES encryption algorithm. Choose **DES** from the Encryption Type drop-down list to provide encryption in the network if you wish to use DES authentication on SNMPv3 requests; otherwise, choose **None**. Skip Step 10 if you have chosen None.

Step 10. If you have chosen DES in the previous step, enter the associated encryption pass phrase for the user in the Encryption Pass Phrase field. This is used to encrypt the data sent to the other devices in the network. This password is also used to decrypt the data on the other end. The pass phrase has to match in the communicating devices. The pass phrase can range from 8 to 32 characters in length.

Step 11. Click **Save** to save this user.

Users

SNMPv3 Users

	User Name	Group	Authentication Type	Authentication Pass Phrase	Encryption Type	Encryption Pass Phrase
<input type="checkbox"/>	New	RW	MD5	*****	DES	*****
<input type="checkbox"/>	User	RO	None		None	
<input type="checkbox"/>	User2	RW	MD5	*****	None	

Add Edit Delete

Save

Step 12. (Optional) The SNMPv3 Users table displays the current users configured on the Access Point. To remove a user from the list, check the check box of the user to be removed, click **Delete**, and click **Save**.