Configure the SNMPv3 on the WAP125 and WAP581

Objective

Simple Network Management Protocol Version 3 (SNMPv3) is a security model in which an authentication strategy is set up for a user and the group in which the user resides. Security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used when handling an SNMP packet.

In SNMP, the Management Information Base (MIB) is a hierarchical information database containing Object Identifiers (OID) which acts as a variable that can be read or set via SNMP. MIB is organized in a tree-like structure. A subtree within the managed object naming tree is a view subtree. An MIB view is a combination of a set of view subtrees or a family of view subtrees. MIB views are created to control the OID range that SNMPv3 users can access. SNMPv3 Views configuration is essential to restrict a user to view only the limited MIB. A WAP can have up to 16 views including the two default views.

The objective of this document is to show you how to gather, view, and download the CPU/RAM activity on the WAP125 and WAP581.

Applicable Devices

- WAP125
- WAP581

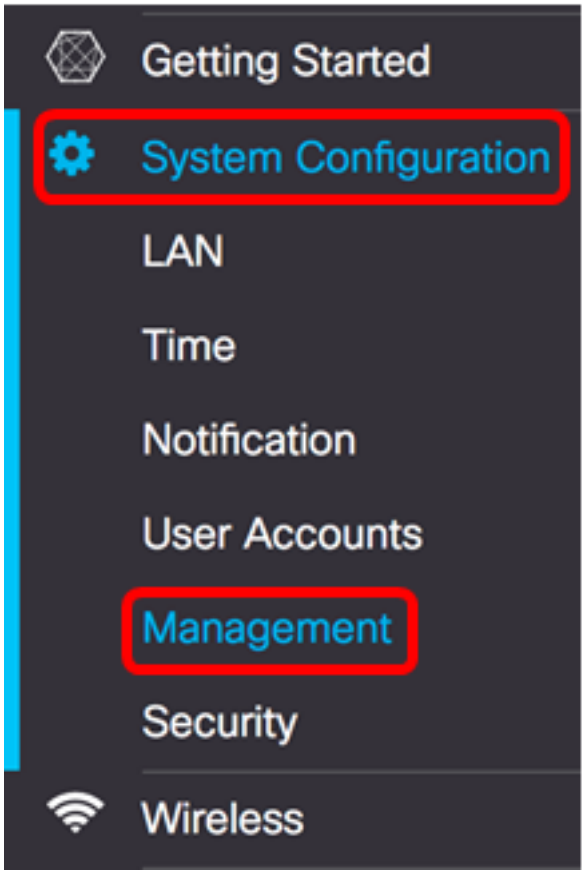
Software Version

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

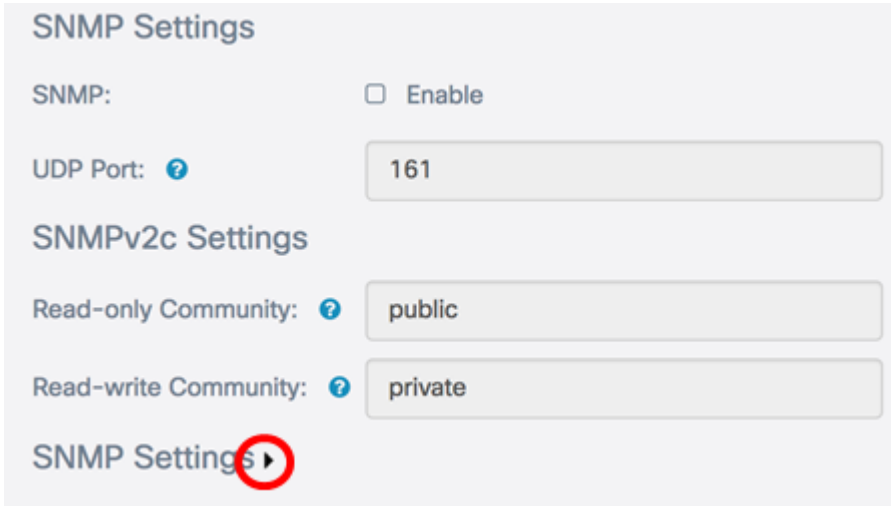
Configure the SNMPv3 Settings

Configure SNMPv3 Views

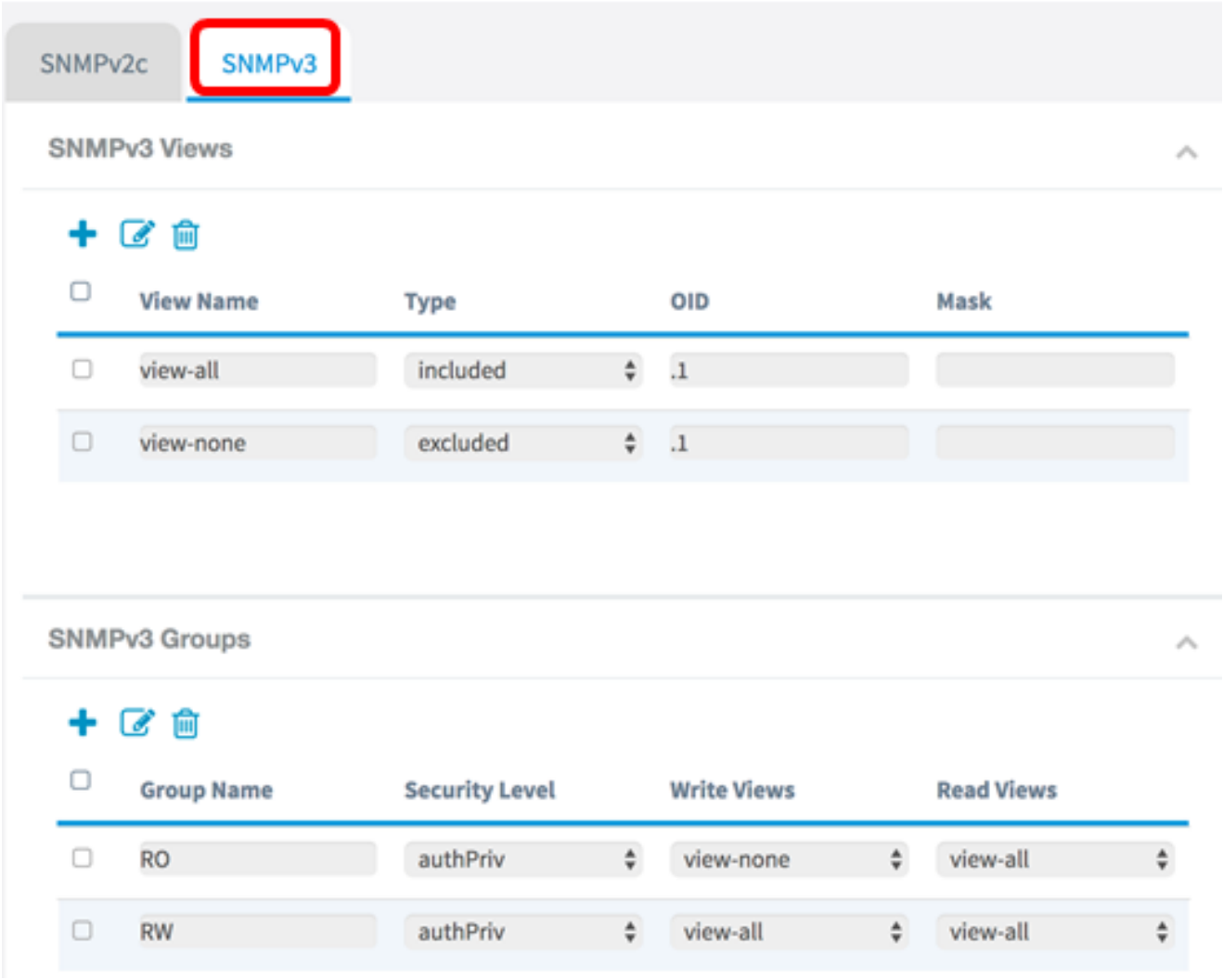
Step 1. Log in to the web-based utility and choose **System Configuration > Management**.



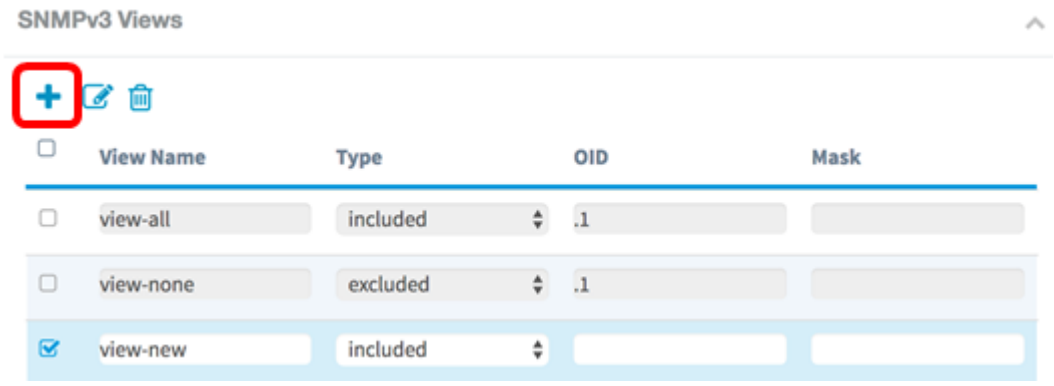
Step 2. Click the **SNMP Settings** right arrow.



Step 3. Click the **SNMPv3** tab.

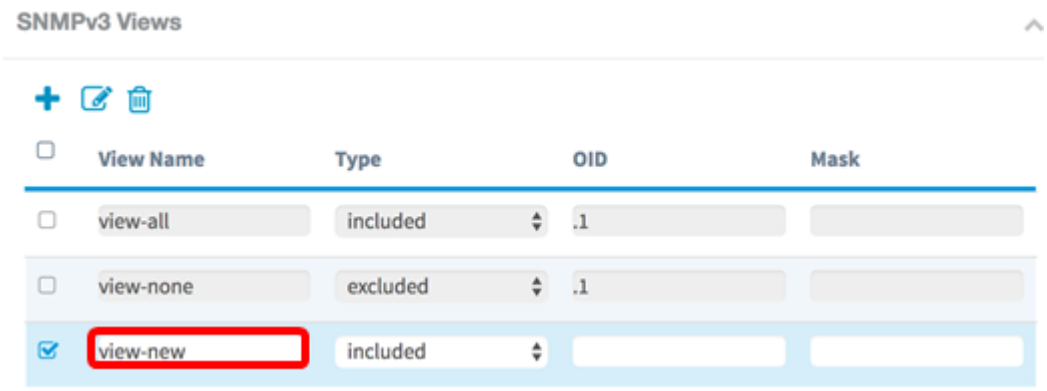


Step 4. Click the **+** button to create a new entry under SNMPv3 Views.



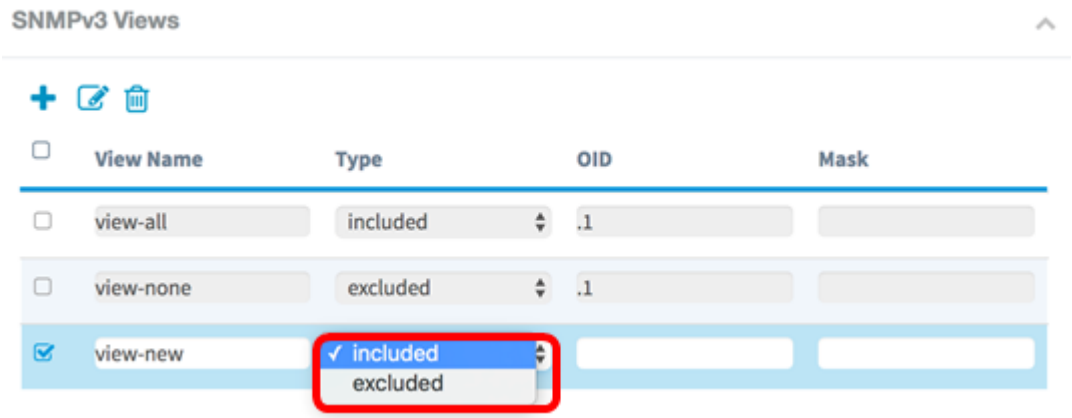
Step 5. In the *View Name* field, enter a name that identifies the MIB view.

Note: In this example, view-new is created as the View Name. View-all and view-none are created by default and contains all management objects supported by the system. These cannot be modified nor deleted.



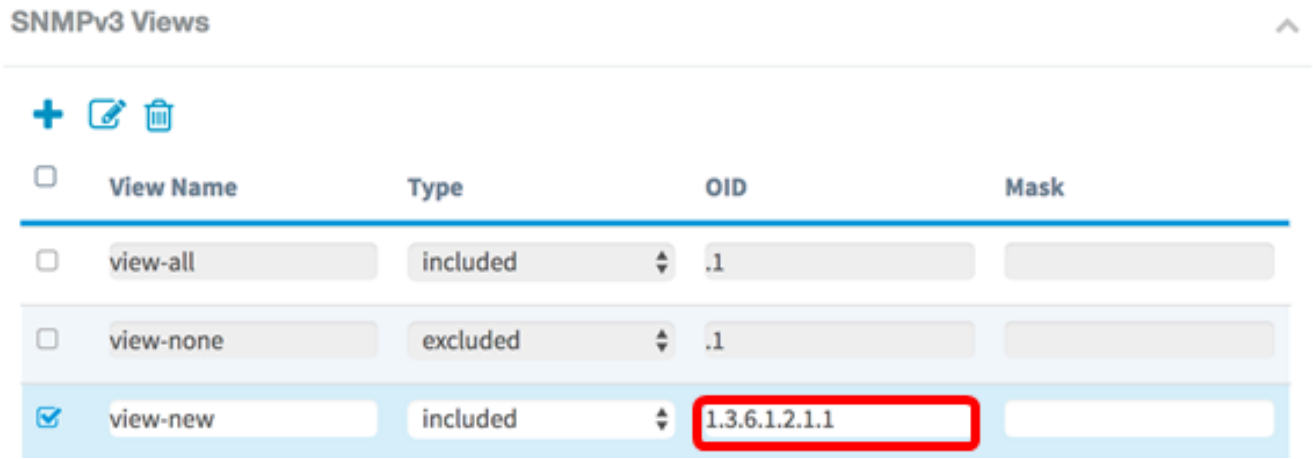
Step 6. From the Type drop-down list, choose an option whether to exclude or include the view.

- included — Includes the view in the subtree or family of subtrees from the MIB view.
- excluded — Excludes the view in the subtree or family of subtrees from the MIB view.



Step 7. In the *OID* field, enter an OID string for the subtree to include or exclude from the view. Each number is used to locate information and each number corresponds to a specific branch of the OID tree. OIDs are unique identifiers of managed objects in the MIB hierarchy. The top-level MIB object IDs belong to different standards organizations, while lower-level object IDs are allocated by associated organizations. Private branches can be defined by vendors to include managed objects for their own products. MIB files map OID numbers to human readable format. To translate the OID number to the object name, click here.

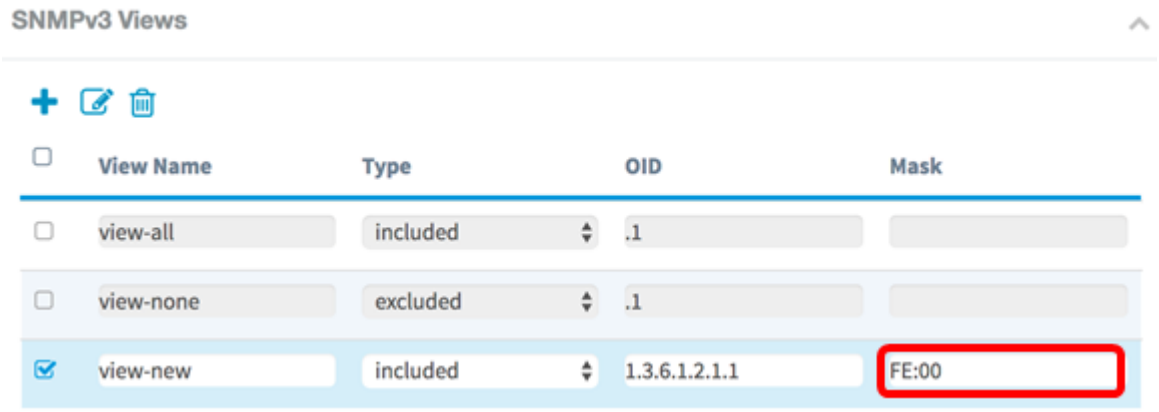
Note: In this example, 1.3.6.1.2.1.1 is used.



Step 8. Enter an OID mask in the *Mask* field. The *Mask* field is used to control the elements of the OID subtree that should be considered as relevant when you determine the view in

which an OID is, and the maximum is 47 characters in length. The format is 16 octets in length and each octet contains two hexadecimal characters separated by a period or colon. To determine the mask, count the number of OID elements and set that many bits to one. Only hexadecimal formats are accepted in this field. Consider the example OID 1.3.6.1.2.1.1, it has seven elements, so if you set seven consecutive 1s followed by one 0 in the first octet and all zeros in the second one, you get FE:00 as the mask.

Note: In this example, FE:00 is used.

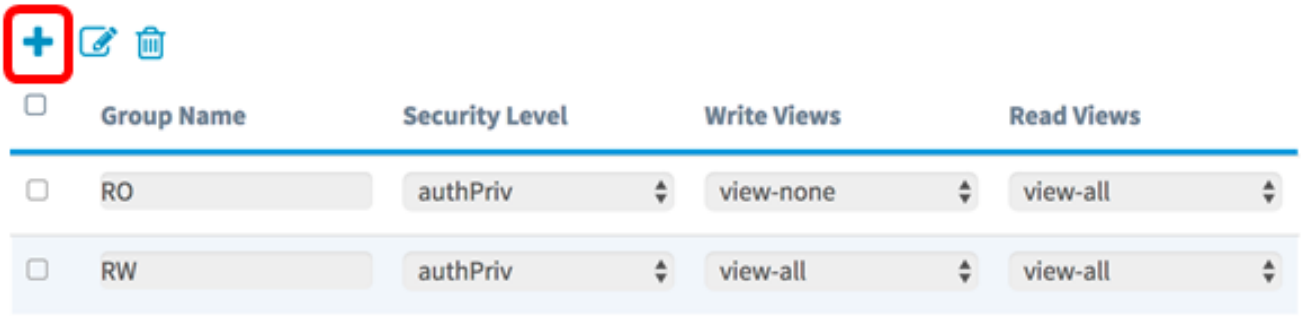


Step 9. Click Save.

You should now have successfully configured the SNMPv3 views on the WAP125.

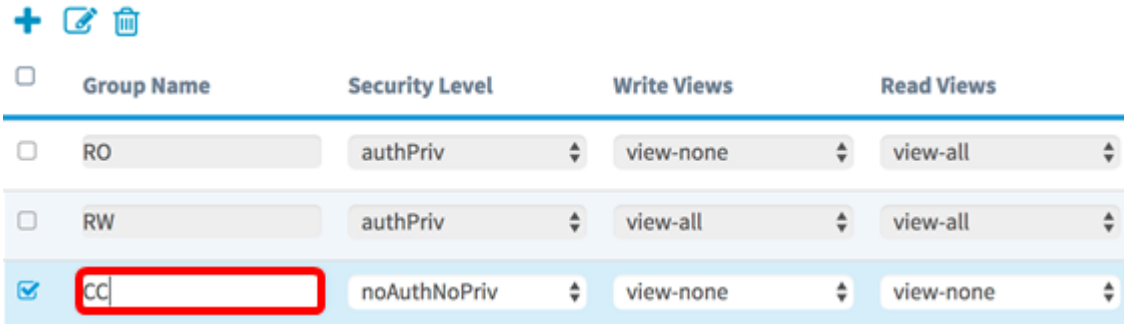
Configure SNMPv3 Groups

Step 1. Click the **+** button to create a new entry under SNMPv3 Groups.



Step 2. 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.

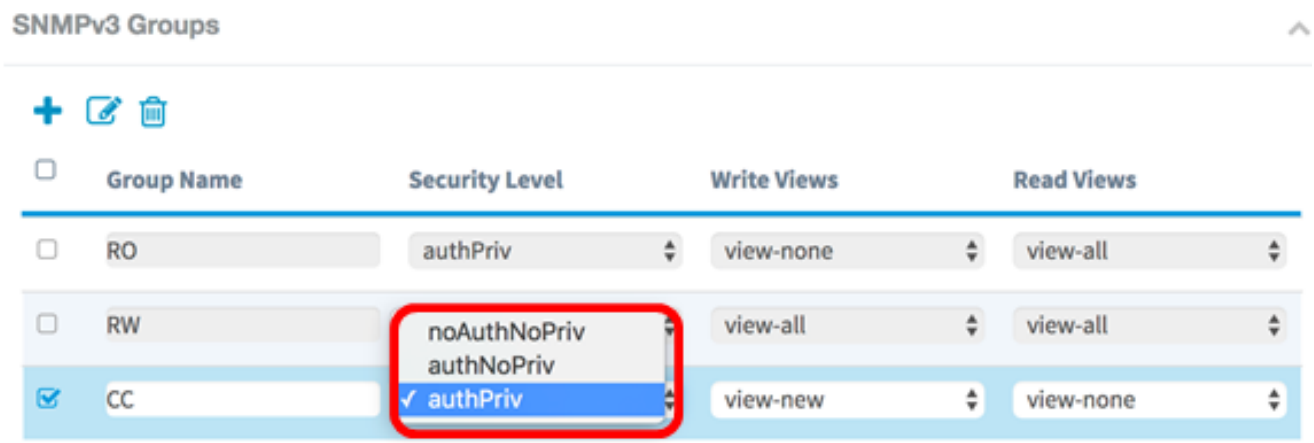
Note: In this example, CC is used.



Step 3. From the Security Level drop-down list, choose an appropriate level of authentication.

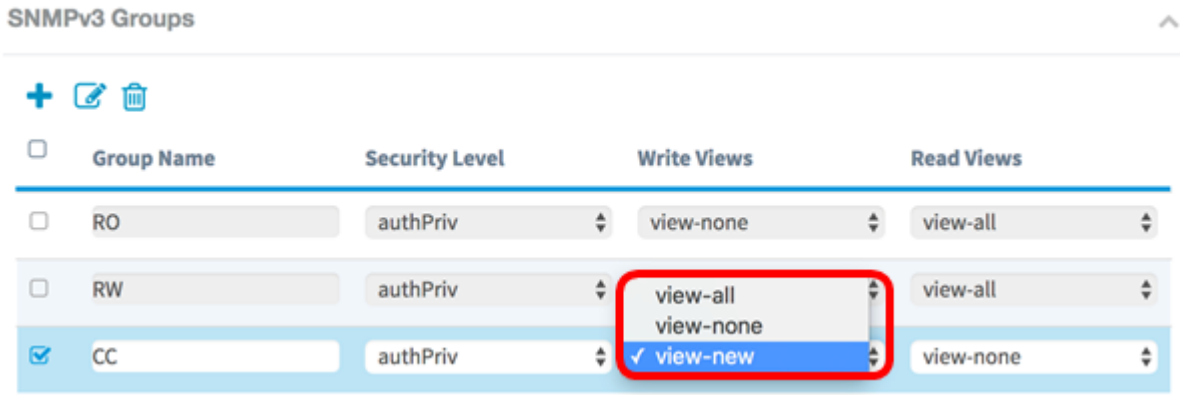
- noAuthNoPriv — Provides no authentication and no data encryption (no security).
- authNoPriv — Provides authentication but no data encryption (no security). Authentication is provided by a Secure Hash Authentication (SHA) passphrase.
- authPriv — Authentication and data encryption. Authentication is provided by an SHA passphrase. Data encryption is provided by DES passphrase.

Note: In this example, authPriv is used.



Step 4. From the Write Views drop-down list, choose the write access to all management objects (MIBs) for the new group. 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.

Note: In this example, view-new is used.



Step 5. 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.
- view-new — User created view.

Note: In this example, view-none is used.

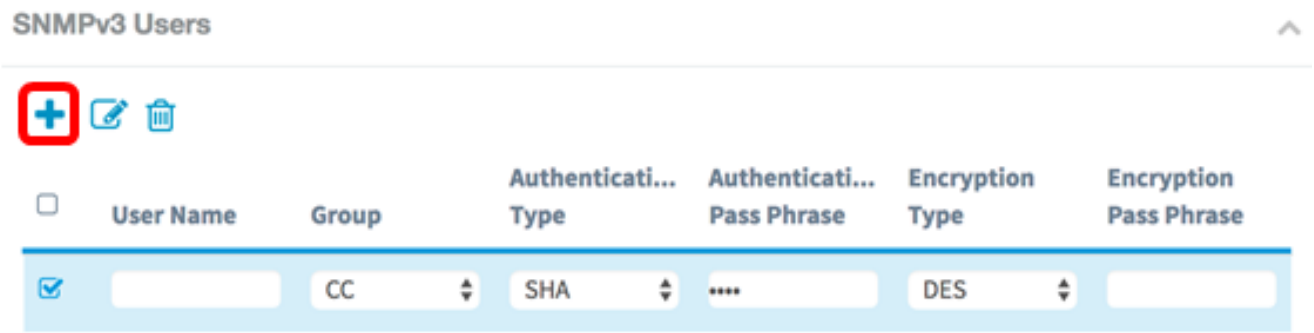
Step 6. Click Save.

You should now have successfully configured the SNMPv3 Groups.

Configure SNMPv3 Users

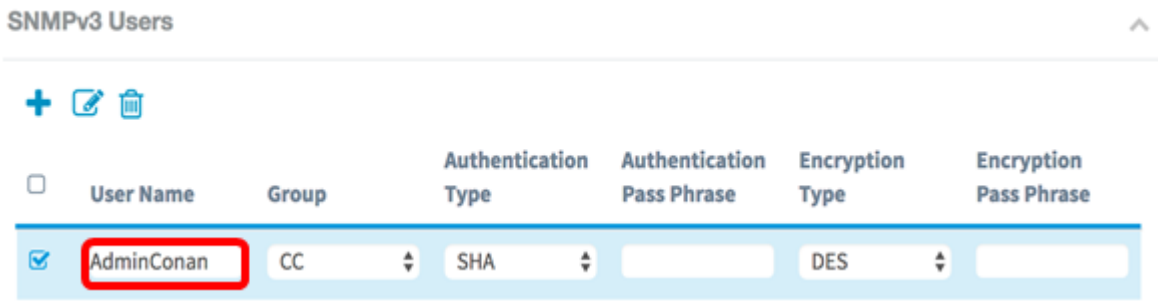
An SNMP user is defined by its login credentials (username, passwords, and authentication method) and it is operated in association with an SNMP group and engine ID. Only SNMPv3 uses SNMP users. Users with access privileges are associated with an SNMP view.

Step 1. Click the **+** button to create a new entry under SNMPv3 Users.



Step 2. In the *User Name* field, create a user name that would denote an SNMP user.

Note: In this example, AdminConan is used.

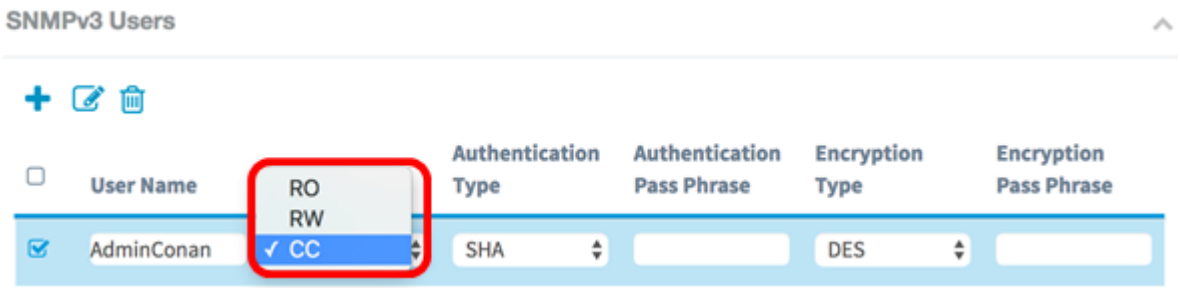


Step 3. From the Group drop-down list, choose a group to map to the user. The options are:

- RO — Read-only group, created by default. This group allows a user to only view the configuration.
- RW — Read/write group, created by default. This group allows a user to view and make necessary changes to the configuration.

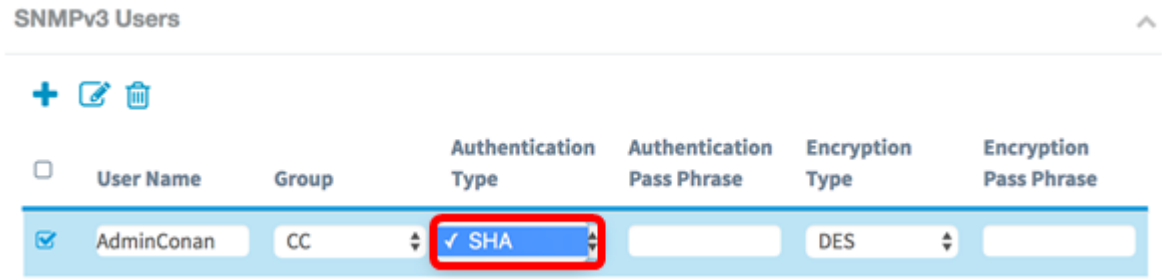
- CC — CC, a user-defined group. User-defined group only appears if a group has been defined.

Note: In this example, CC is chosen as defined in Step 2 under Configure SNMPv3 Groups.

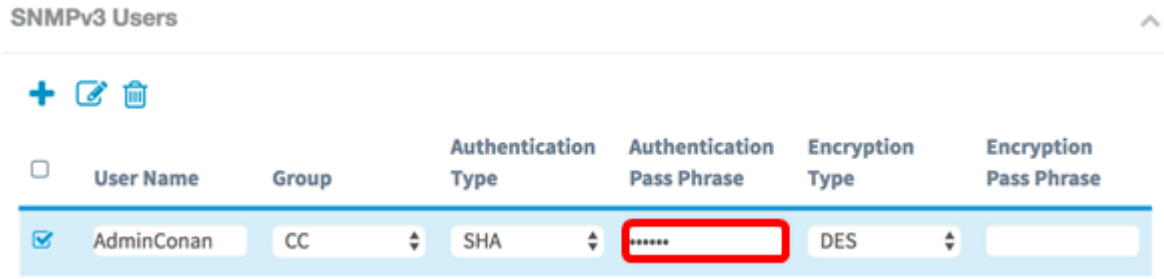


Step 4. From the Authentication drop-down list, choose **SHA**.

Note: This area is greyed out if the group security level chosen in Step 3 was set to noAuthNoPriv.



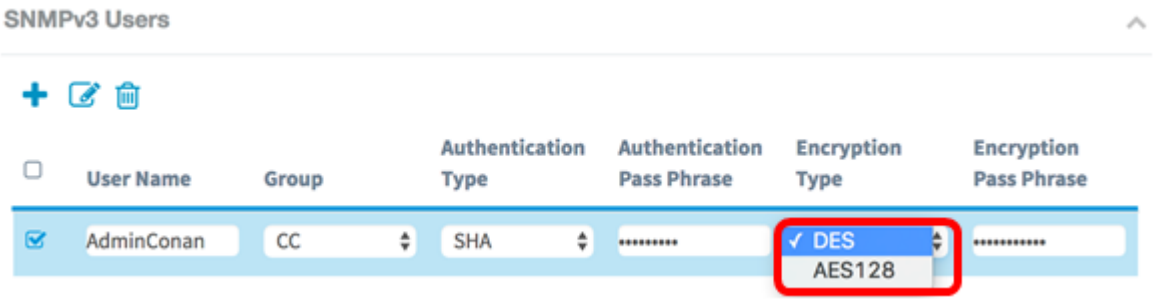
Step 5. In the *Authentication Pass Phrase* field, enter the associated passphrase for the user. This is the SNMP password that has to be configured to authenticate the devices in order for them to connect with each other.



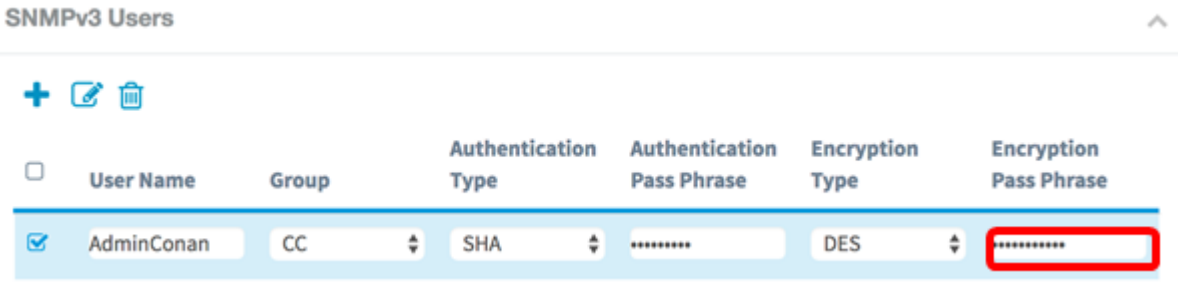
Step 6. From the Encryption Type drop-down menu, choose an encryption method to encrypt the SNMPv3 requests. The options are:

- DES — Data Encryption Standard (DES) is a symmetric block cipher that uses a 64-bit shared secret key.
- AES128 — Advanced Encryption Standard that uses a 128-bit key.

Note: In this example, DES is chosen.



Step 7. In the *Encryption Pass Phrase* field, enter the associated passphrase for the user. 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 passphrase has to match in the communicating devices. The passphrase can range from eight to 32 characters in length.



Step 8. Click Save.

You should now have successfully configured the SNMPv3 Users on the WAP125.

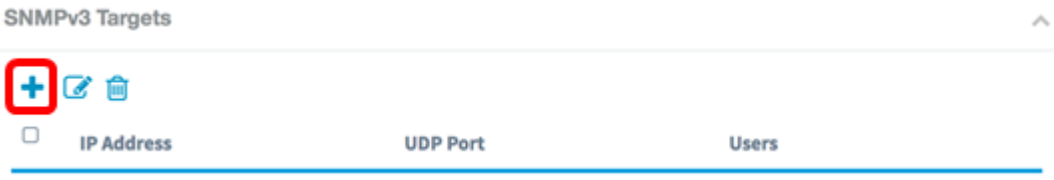
Configure SNMPv3 Targets

An SNMP Target refers to both the message sent and the management device to which agent notifications are sent. Each target is identified by target name, IP address, UDP port, and user name.

SNMPv3 send SNMP target notifications as Inform messages to the SNMP Manager rather than traps. This ensures target delivery since traps do not use acknowledge but informs do.

Step 1. Click the **+** button to create a new entry under SNMPv3 Targets.

Note: A total of up to 16 targets can be configured.



Step 2. In the *IP Address* field, enter the target IP address where all SNMP traps will be sent. This is typically the Network Management System address. This can either be an IPv4 or IPv6 address.

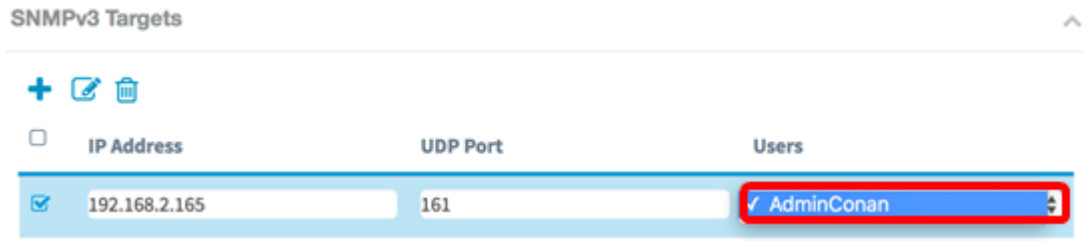
Note: In this example, 192.168.2.165 is used.

Step 3. Enter a User Datagram Protocol (UDP) port number in the *UDP Port* field. The SNMP agent checks this port for access requests. The default is 161. The valid range is from 1025 to 65535.

Note: For this example, 161 is used.

Step 4. Choose the user to associate with the target from the Users drop-down list. This list shows a list of all the users created on the Users page.

Note: AdminConan is chosen as the User.



Step 5. Click 

.

You should now have successfully configured the SNMPv3 Targets on the WAP125 and WAP581.