


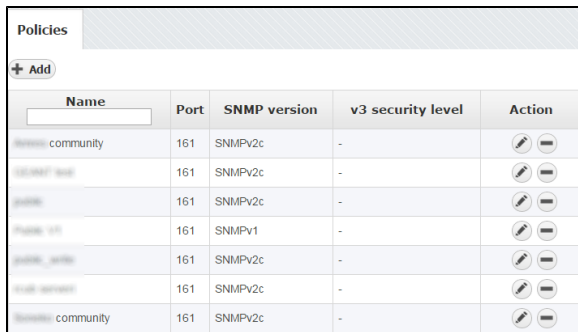
Configuring SNMP Policies















Policies are used for discovery of devices in Traffic Statistics (exporters and interfaces) for NetFlow Analyzer module and sending SNMP requests to devices in MIB Browser module etc.

 Policy for a certain device in NetVizura has to match that actual SNMP configuration of that device in order for to get SNMP reports for particular MIB or OID for that device.

Administrator can view, add, edit or delete SNMP policies.

To access Policies, go to **Settings > Control Panel > SNMP Policies**.



Name	Port	SNMP version	v3 security level	Action
x community	161	SNMPv2c	-	 
x community	161	SNMPv2c	-	 
x community	161	SNMPv2c	-	 
x community	161	SNMPv1	-	 
x community	161	SNMPv2c	-	 
x community	161	SNMPv2c	-	 
x community	161	SNMPv2c	-	 

On the screenshot to the left we can see Policy table together with some policy examples. As you can see, table shows basic policy parameters:

1. Name
2. Port
3. SNMP version
4. v3 security level

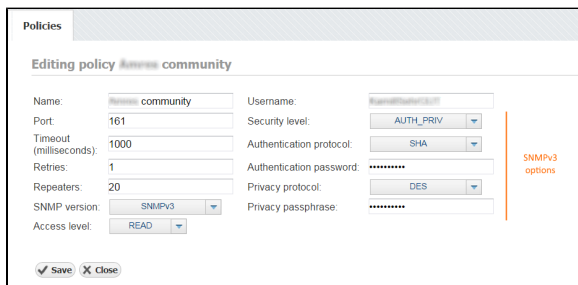
Looking at the first policy “x community” we can see that the port used for SNMP is 161, and that SNMP version is v2c. Naturally, since it is v2c there are no associated v3 security levels.

Adding a SNMP Policy

To Add a new policy, click the **+ Add** button at the top of the Policy table.

Editing a SNMP Policy

To edit a policy, click on the pen (edit icon) or double click on the policy table row.



Editing policy **x community**

Name: Username:

Port: Security level:

Timeout (milliseconds): Authentication protocol:


Retries: Authentication password:

Repeaters: Privacy protocol:

SNMP version: Privacy passphrase:

Access level:

Available policy parameters are: Name, Port, Timeout, Retries, Repeaters, SNMP version, Access level, Username and SNMPv3 security level options (authentication protocol and password, privacy protocol and password).

 SNMPv3 security level options are only visible if SNMP version is set to SNMPv3.

When an SNMP request is sent to a device associated with a protocol the request will be sent to the policy UDP port using the policy username as SNMP community and version. In order for request to be successful the policy has to match the SNMP configuration of the target device.

Successful request will result in a number of packets each containing a number of OIDs set by the Repeaters parameter (this is a number of SNMP request repeats in one SNMP Query). If the request is unsuccessful, there will be a number of retries (Retries parameter) with a certain timeout between each request based on the Timeout parameter (timeout incrementally grows after each request).

In the example shown in the screenshot above the SNMP request in view mode will result in a SNMPv3 request to a device on UDP port 161 with the above set security parameters. If the device doesn't reply, there will be one more retry after 1000ms.

Removing a SNMP Policy

To remove a policy, click - (remove icon) in the Action column.