How to Configure the SNMP Service

https://campus.barracuda.com/doc/73007753/

SNMP allows a Network Management System (NMS) to remotely monitor the network and system state of the firewall. The CloudGen Firewall supports both SNMP v2c and v3. Barracuda Networks recommends using SNMP v3 because it is more secure.

SNMP v2

- IP address (range) from which the Network Management System will contact the CloudGen Firewall SNMP service.
- SNMP community string.

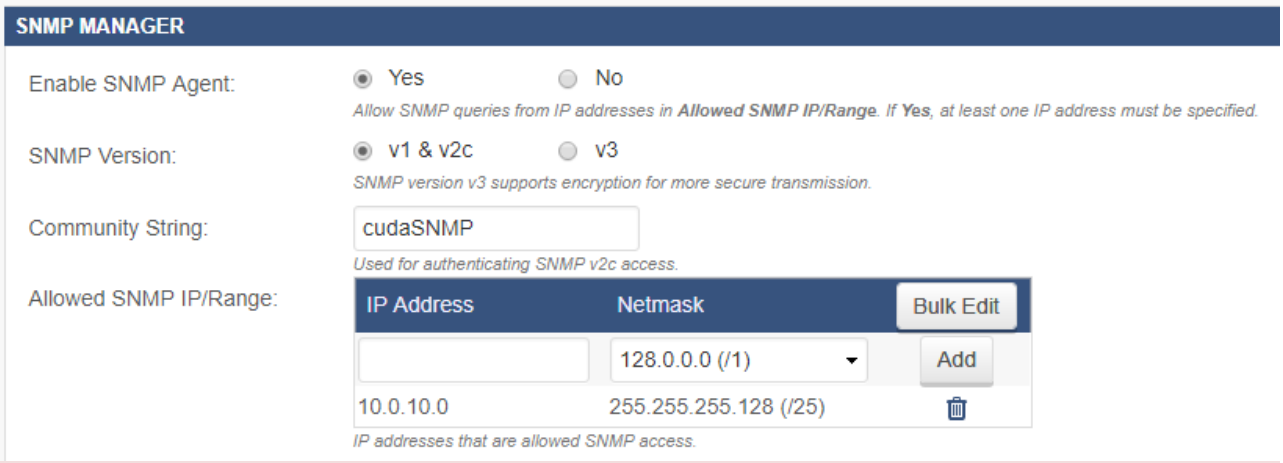
SNMP v3

- User and password to authenticate the NMS.
- Authentication Method (supported encryption methods).
- Allowed IP address or range for the Network Management System.

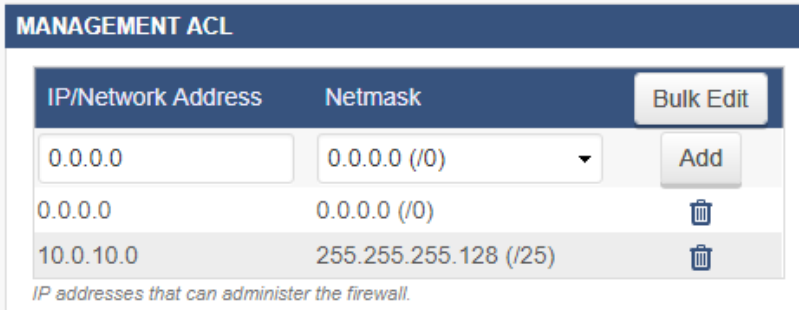
Use the Barracuda NextGen Firewall MIB file to use the reference objects included for your SNMP monitor software appliance or script.

Configure SNMP v2

1. Go to **BASIC > Administration**.
2. In the **SNMP Manager** section, configure the following settings:
   - **Enable SNMP Agent** – Select **Yes**.
   - **SNMP Version** – Select **v1 & v2c**.
   - **Community String** – Enter a password to authenticate the SNMP server.
   - **Allowed SNMP IP/Range** – Add the IP addresses or range from which the CloudGen Firewall should accept SNMP queries.
3. In the **Management ACL** section, add the **Allowed SNMP IP/Range** to the **IP/Network Address** list.



Verify that the computer used to administer the CloudGen Firewall is in one of the networks included in the **Management ACL**. You will be locked out of the firewall otherwise. The default value of 0.0.0.0/0.0.0.0 allows all networks and IP addresses to administer the CloudGen Firewall.



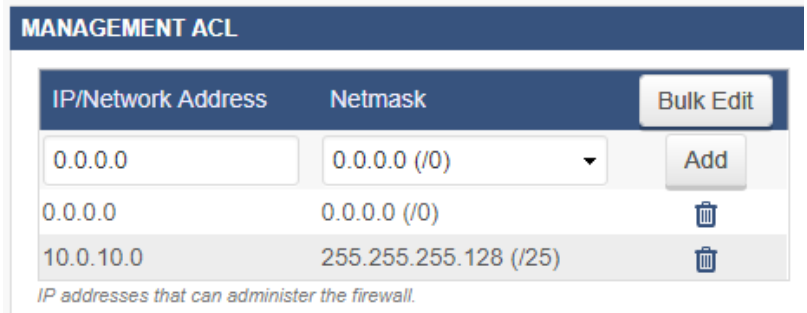
4. Click **Save**.

Configure SNMP v3

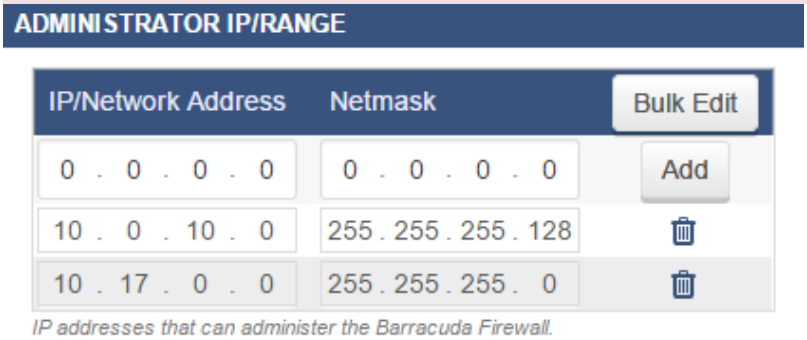
1. Open the **BASIC > Administration** page.
2. In the **SNMP Manager** section configure the following settings:
   - **Enable SNMP Agent** – Select *Yes*.
   - **SNMP Version** – Select **v3**.
   - **User** – Enter a username.
   - **Password** – Enter a password.

3. In the **Management ACL** section, add the **Allowed SNMP IP/Range** to the **IP/Network**

Address list.



Verify that the computer used to administer the CloudGen Firewall is in one of the networks included in the **Management ACL.** You will be locked out of the firewall otherwise. The default value of 0.0.0.0/0.0.0.0 allows all networks and IP addresses to administer the CloudGen Firewall.



4. Click **Save**.

Figures

1. snmp_02_67.png
2. snmp_01_67a.png
3. snmp_v3.png
4. snmp_01_67a.png
5. snmp_01_67.png