

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.

SNMP MANAGER

Enable SNMP Agent: Yes No
Allow SNMP queries from IP addresses in Allowed SNMP IP/Range. If Yes, at least one IP address must be specified.

SNMP Version: v1 & v2c v3
SNMP version v3 supports encryption for more secure transmission.

Community String:
Used for authenticating SNMP v2c access.

Allowed SNMP IP/Range:

IP Address	Netmask	Bulk Edit
<input type="text"/>	128.0.0.0 (/1)	Add
10.0.10.0	255.255.255.128 (/25)	

IP addresses that are allowed SNMP access.

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.

MANAGEMENT ACL

IP/Network Address	Netmask	Bulk Edit
<input type="text" value="0.0.0.0"/>	0.0.0.0 (/0)	Add
0.0.0.0	0.0.0.0 (/0)	
10.0.10.0	255.255.255.128 (/25)	

IP addresses that can administer the 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.

SNMP MANAGER

Enable SNMP Agent: Yes No
Allow SNMP queries from IP addresses in Allowed SNMP IP/Range. If Yes, at least one IP address must be specified.

SNMP Version: v1 & v2c v3
SNMP version v3 supports encryption for more secure transmission.

User:
SNMP username, required only for SNMP version v3.

Password:
SNMP password, required only for SNMP version v3. A minimum length of 12 characters is required.

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

Address list.

MANAGEMENT ACL		
IP/Network Address	Netmask	Bulk Edit
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0 (/0)"/>	<input type="button" value="Add"/>
0.0.0.0	0.0.0.0 (/0)	
10.0.10.0	255.255.255.128 (/25)	

IP addresses that can administer the firewall.

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.

ADMINISTRATOR IP/RANGE		
IP/Network Address	Netmask	Bulk Edit
<input type="text" value="0 . 0 . 0 . 0"/>	<input type="text" value="0 . 0 . 0 . 0"/>	<input type="button" value="Add"/>
10 . 0 . 10 . 0	255 . 255 . 255 . 128	
10 . 17 . 0 . 0	255 . 255 . 255 . 0	

IP addresses that can administer the Barracuda 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

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.