

## How to Configure SNMP Monitoring

<https://campus.barracuda.com/doc/41107638/>

The Barracuda NextGen Firewall X-Series offers the ability to supply information to Network Management Systems via SNMP. Both SNMP v2c and v3 are supported. Barracuda Networks recommends using SNMP v3 because it is more secure. Use the [Barracuda Firewall MIB file](#) to use the reference objects included for your SNMP monitor software appliance or script.

### SNMP v2

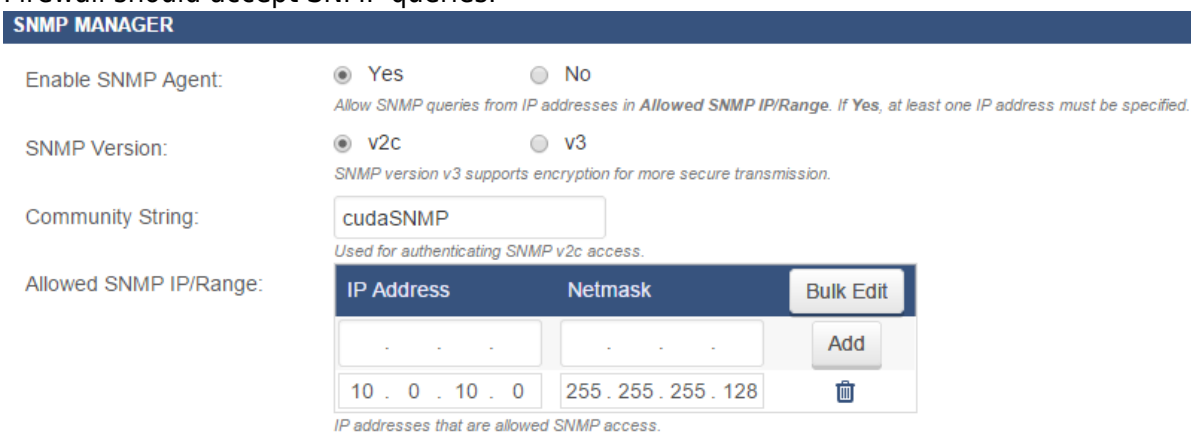
- IP address (range) from which the Network Management System will contact the X-Series Firewall SNMP service.
- SNMP community string.

### SNMP v3

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

## Configure SNMP v2

1. Open the **BASIC > Administration** page.
2. In the **SNMP Manager** section, configure the following settings:
  - **Enable SNMP Agent** – Select Yes.
  - **SNMP Version** – Select **v2c**.
  - **Community String** – Enter a password to authenticate the SNMP server.
  - **Allowed SNMP IP/Range** – Add the IP addresses or range from which the X-Series Firewall should accept SNMP queries.



**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: ☒ 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	
<input type="text" value="."/>	<input type="text" value="."/>	<input type="button" value="Add"/>
10 . 0 . 10 . 0	255 . 255 . 255 . 128	<input type="button" value=""/>

IP addresses that are allowed SNMP access.

3. In the **Administrator IP/Range** section, add the **Allowed SNMP IP/Range** to the **IP/Network Address** list.

Verify that the computer used to administer the X-Series Firewall is in one of the networks included in the **Administrator IP/Range**. 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 X-Series Firewall.

## ADMINISTRATOR IP/RANGE

IP/Network Address	Netmask	Bulk Edit
0 . 0 . 0 . 0	0 . 0 . 0 . 0	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**.

## 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.
  - **Authentication Method** – Select the authentication method supported by your network management software. E.g., SHA
  - **Encryption Method** – Select the encryption method supported by your network management software. E.g., AES
  - **Allowed SNMP IP/Range** – Add the IP addresses or range from which the X-Series Firewall should accept SNMP queries.

SNMP MANAGER

Enable SNMP Agent:

☒ Yes
 ☐ No

SNMP Version:

☐ v2c
 ☒ v3

User:

admin

Password:

●●●●●●●●●●

Authentication Method:

☒ MD5
 ☐ SHA

Encryption Method:

☐ DES
 ☒ AES

Allowed SNMP IP/Range:

IP ADDRESS	NETMASK	Bulk Edit
<input type="text" value=" . . ."/>	<input type="text" value=" . . ."/>	<input type="button" value="Add"/>
10 . 0 . 10 . 0	255 . 255 . 255 . 128	

Allow SNMP queries from IP addresses in Allowed SNMP IP/Range. If Yes, at least one IP address must be specified.

SNMP version v3 supports encryption for more secure transmission.

SNMP username, required only for SNMP version v3.

SNMP password, required only for SNMP version v3.

SHA is the more secure authentication method.



AES is the more secure encryption method.

IP addresses that are allowed SNMP access.

3. In the **Administrator IP/Range** section, add the **Allowed SNMP IP/Range** to the **IP/Network Address** list.

Verify that the computer used to administer the X-Series Firewall is in one of the networks included in the **Administrator IP/Range**. 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 X-Series Firewall.

#### ADMINISTRATOR IP/RANGE

IP/Network Address	Netmask	Bulk Edit
0 . 0 . 0 . 0	0 . 0 . 0 . 0	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\_67.png
3. snmp\_03.png
4. snmp\_01\_67.png

© Barracuda Networks Inc., 2024 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.