How to Set Up Alerts and SNMP Monitoring

https://campus.barracuda.com/doc/6160422/

Alerts and Notifications

Emailed System Alerts

Use the **BASIC > Administration** page to configure the Barracuda Web Security Gateway to automatically email system alerts to the email addresses you specify. System alerts notify you when:

- Your Energize Update subscription is about to expire
- Your system is low on disk space
- Threat Alerts

When any virus downloads or spyware downloads are detected in the HTTP data path, threat alerts can be sent to the email address(es) you specify in the **Email Notifications** section of the **BASIC > Administration** page. To have alerts sent to your Slack account, see How to Send System Notifications to Slack.

Setting up SNMP Query, Alerts and Traps

While the Barracuda Web Security Gateway will send email alerts to the **System Alerts Email Address** as specified on the **BASIC > Administration** page, these alerts are limited and do not include latency, inqueue sizes, and other system health information. To monitor more specific information on a Barracuda Web Security Gateway, Barracuda Networks recommends using SNMP monitoring with an SNMP server. The Barracuda Web Security Gateway 410 and higher offers the ability to monitor various settings via SNMP alerts or traps, including system statistics such as:

- System Load Averages (1m/5m/15m)
- Memory Utilization
- System Uptime
- Raid Status
- CPU idle times

To query the Barracuda Web Security Gateway for these statistics via SNMP, you must do the following in the **SNMP Manager** section of the **BASIC > Administration** page:

1. Set **Enable SNMP** to *Yes.*
2. Enter the **SNMP Community String.**
3. Select the **SNMP Version**. The Barracuda Web Security Gateway supports both versions v2c

and v3. SNMP v2c queries and responses are NOT encrypted, so it is not as secure as SNMP v3. With SNMP v3, traffic is encrypted and you can set up access control for specified users with passwords. **Barracuda Networks strongly recommends using version v3.** Version v3 provides the following options for additional security (make sure that the settings you select are supported by your SNMP monitor):
- Authentication methods MD5 or SHA, where SHA is the more secure method.
- Encryption methods DES or AES, where AES is the more secure method.

4. Enter the IP address of the server that will be making the SNMP connection in the **Allowed SNMP and API IP/Range** section of the page. IP addresses entered in this field are allowed to access the Barracuda Web Security Gateway via SNMP queries to retrieve error information, or via the API to configure the device.

You can configure SNMP traps by listing one or more IP addresses to which the Barracuda Web Security Gateway has access for sending SNMP traps as configured by a client.

SNMP MIBs

Click to view the Barracuda Web Security Gateway SNMP MIB and the Barracuda Networks Reference MIB. You can monitor objects included in these MIBs either from custom scripts or from your SNMP monitor. See also SNMP OID's for CPU, Memory and Disk Statistics on Linux.