**Configure SNMP Alert Notifications**

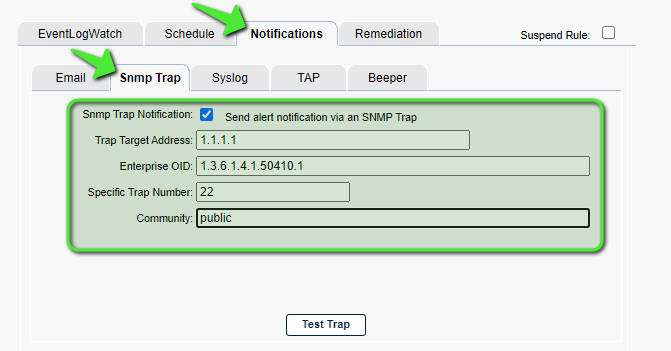
This article was updated to support v12.0 of Goliath Performance Monitor.

This document will guide you through the process of configuring SNMP notifications.

**Article Contents**

1. [Configure SNMP Notifications](https://support.goliathtechnologies.com/hc/en-us/articles/360024726913-Configure-SNMP-Alert-Notifications-#h_6f4f2503-79e2-49bd-af33-e7a8f53fd651)
2. [Appendix](https://support.goliathtechnologies.com/hc/en-us/articles/360024726913-Configure-SNMP-Alert-Notifications-#h_90cbb68b-1742-4ef9-9d1a-327da2475ce0)
   1. [Macro Substitution](https://support.goliathtechnologies.com/hc/en-us/articles/360024726913-Configure-SNMP-Alert-Notifications-#h_677bd9d2-1725-4db8-bb51-9c10207dfd4c)

**Configure SNMP Notifications**

1. Open the Goliath Console and navigate to the **Configure - Monitoring Rules** page
2. Select the alert condition(s) in which you’d like to enable SNMP Trap notifications and then click the **Edit** button at the top of the page
3. A new pane will open, click the **Notifications** tab
4. The subsection for **Email** will be selected by default, on this tab please use the **Email Subject** field to define the subject for the SNMP message.
   1. In order to edit the subject you must first check the box to enable email notifications, update the subject, and then check the box again to disable email notifications
   2. Please note, by default you will see characters like ‘&N’ in the subject, this is a part of our macro functionality. A full list of macros is provided in the Appendix at the end of this document.
5. Click the tab for **SNMP Trap** and select the checkbox at the top of the subsection to enable SNMP notifications.
6. In the **Trap Target Address** field, define the IP address or machine name where the SNMP Trap notification will be sent. To send to multiple addresses please delimit with a semi-colon.  
   
7. For the **Enterprise OID** menu, enter 1.3.6.1.4.1.50410.x where **‘x’** is the category of alert based on the table in the [Appendix](https://support.goliathtechnologies.com/hc/en-us/articles/360024726913-Configure-SNMP-Alert-Notifications-#h_01FYW2BQDXQJ9R981HTKP5B33H).
8. For the **Specific Trap Number** option, define a number representing the specific trap/alert/notification. These numbers are typically sequential and specific to each Monitoring Rule that will be sending notifications.
9. Define your SNMP Community string in the **Community.**
   1. If multiple trap addresses are defined, and the community string is the same for all addresses, it only needs to be defined once. If multiple trap addresses are defined, and the community string is different for all addresses, semi-colon delimit the strings (in the same order the trap addresses are defined).
10. When finished, you can click the **Test Trap** button to confirm that the SNMP trap is received by appropriately by the target device/service.
11. Click **Save** when ready to enable this configuration.

**Appendix**

**Goliath OID List**

|  |  |
| --- | --- |
|  | **Category** |
| 1 | Goliath Performance Monitor |
| 2 | VMware |
| 3 | XenServer |
| 4 | Citrix Role Servers |
| 5 | Citrix XenApp |
| 6 | Citrix XenDesktop |
| 7 | VMware Horizon |
| 8 | Remote Desktop Services |
| 9 | Goliath Application Availability Monitor |
| 10 | Microsoft Windows |

**Macro Substitution**

The notification **Subject** field supports fourteen Macros that are substituted with the appropriate data for a particular alert when it occurs. The parameters are **case sensitive and must be upper case.**

* &N: which is replaced by the name of the server/device causing the alert
* &A: which is replaced by the IP Address of the server/device causing the alert
* &W: which is replaced by the name of the Monitoring Rule
* &S: which is replaced by the Status message associated with this failure causing the alert status information is source dependent and differs based upon the watch type.
  + For Example:
    - ServerWatch: 429 Mb memory free; 2% available
    - ProcessWatch: Process not running no restart attempted
    - EventLogWatch: Event ID, Source, & Description
    - GAAM: The full simulation details log
* &D: which is replaced by the date of the alert
* &T: which is replaced by the time of the alert
* &P: which is replaced by the Server/Device Description
* &O: which is replaced by the Server/Device Notes
* &G: which is replaced by the name of the Group that the Server/Device belongs
* &C: which is replaced by the Group Description
* &R: which is replaced by the Monitoring Rule ‘Description’ text
* &L: which is replaced by the for the Monitoring Rule ‘Severity’ level
* &E: which is replaced by the for the Monitoring Rule Notes
* &V: (only for CounterWatch)is replaced by the Counter value that exceeded the threshold and caused an alert.