Configure SNMP Alert Notifications in Goliath Performance Monitor and Logon Simulator

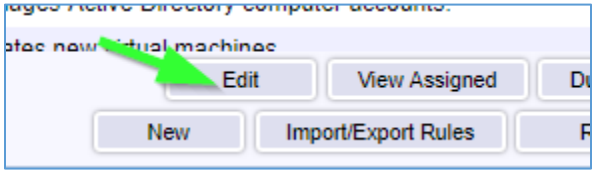
This document will guide you through the process of configuring SNMP notifications.

Contents

I. Configure SNMP Notifications

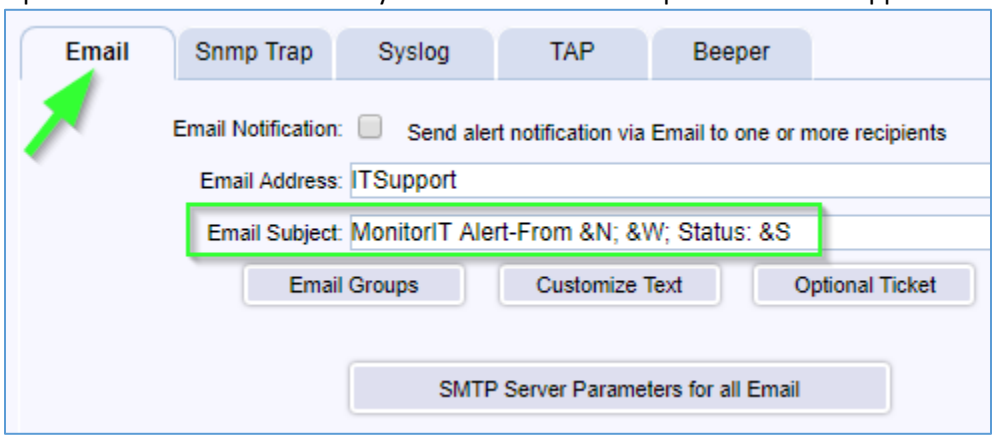
1. Open the Goliath Console
2. Select the **'Configure'** tab, and then the **'Monitoring Rules'** sub menu

3. Select the alert condition in which you'd like to enable email or text message notifications
4. Click the **'Edit'** button at the bottom of the page

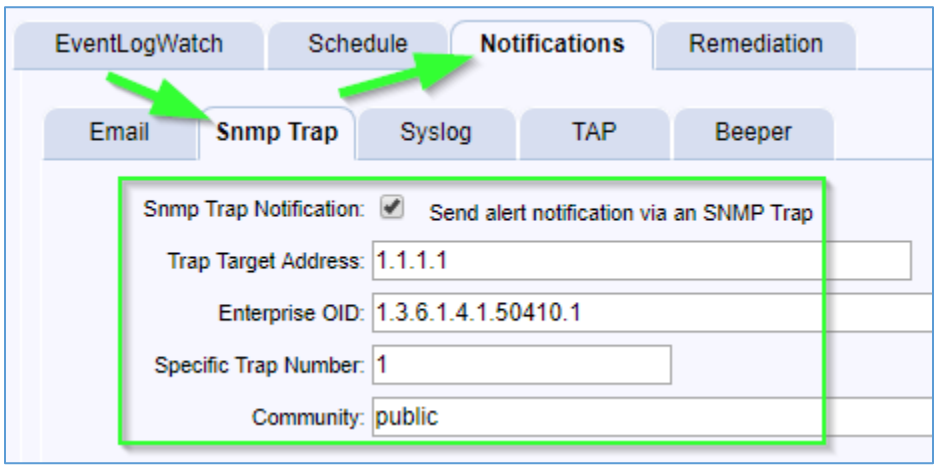


5. A new pane will open, choose the **'Notifications'** tab
6. The subsection for **'Email'** will be selected by default, on this tab please use the **'Email Subject'** field to define the subject for the SNMP message. Please note, by default you will see characters like '&N' in the subject, this is

a part of our macro functionality. A full list of macros is provided in the Appendix at the end of this document.



7. Click the tab for **'SNMP Trap** and select the checkbox at the top of the subsection to enable SNMP notifications.
8. In the **'Trap Target Address'** field, define the IP address or machine name where the SNMP Trap notification will be sent.



9. 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 below.

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

10. 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.
11. Define your SNMP Community string in the **'Community'** field.
12. When finished, you can click the **'Test Trap'** button to confirm that the SNMP trap is received by appropriately by the target device/service.

13. Click **'Save'** when ready to enable this configuration.

II. Appendix

A. Macro Substitution

Custom Email and SMS Text Notifications 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
        - Logon Simulator: 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.