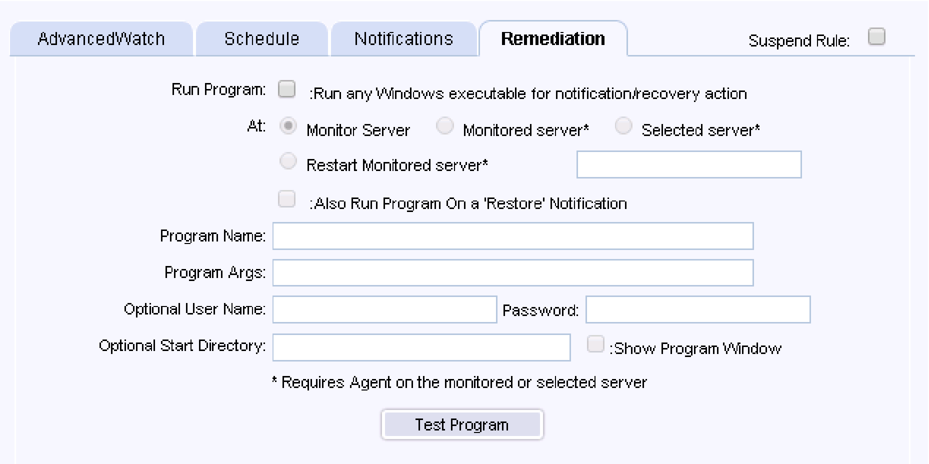
GOLIATH
TECHNOLOGIES

Configure Custom Remediation for Goliath Performance Monitor

With all alerts, remediation actions can be executed to restart service, application, or execute a custom program, batch, or command file. **PLEASE NOTE:** A Goliath Agent must be installed on the server/endpoint where the remediation will take place.



Run Program: □ :Run any Windows executable for notification/recovery action

At: ● Monitor Server ○ Monitored server* ○ Selected server*

○ Restart Monitored server*

□ :Also Run Program On a 'Restore' Notification

Program Name:

Program Args:

Optional User Name: Password:

Optional Start Directory: □ :Show Program Window

* Requires Agent on the monitored or selected server

Instructions on how to configure custom remediation actions:

1. Check the box for “run a program”. When checked **and** alert conditions have been met, the program, Powershell script, batch, or command file name specified in the *Program Name* field is executed either on the MonitorIT Server, the monitored server or a different server.

2. Select the appropriate radio button in the “At” field to choose to run the remediation action at the MonitorIT Server, at the monitored server, a different server, or to Restart the Monitored computer.

3. In the “Program Name” field, define the name of the program, Powershell, command line, batch file, etc to be opened when the alert triggers. This must be a fully qualified program name path. In order to access the network share, the agent must have rights to the share. Additional Examples:
   a. Powershell: C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe
   b. Command of Bath file: C:\Windows\system32\cmd.exe
   c. Executable: \\10.2.1.1\c$\scripts\alerts.exe

4. In the “Program Args” field, define an 'Argument' string passed to the program, batch, or command file named in the *Program Name* field when executed. The 'Argument' string text supports "macro substitution" based on macro parameters listed below. The parameters are case sensitive and must be upper case. <u>You can find these macros in the Appendix. Examples:</u>
   a. Powershell: -ExecutionPolicy Bypass -File "C:\Program Files\MonitorIT\Scritps\TestPS.ps1"
   b. Command: net stop Spooler
   c. Batch File: reboot.bat

5. The optional username and password is where you would, if necessary, define a user that the Goliath Agent will use to run the remediation. This username must be in the form of domain\user

6. Set the “Show Program Window” check box to have the remediation actions appear on the screen or uncheck to run the remediations in the background; hidden.

7. Press the “Test Program” button to test the remediation execution. The test will only process the Program Args macros, if any, and will return a message.

Appendix

Macros for Program Arguments:

&D for Date
&T for Time
&N for Name of the Server/Device causing the alert condition
&P for the Server/Device Description
&O for the Server/Device Notes
&G for the Name of the Group that the Server/Device belongs
&C for the Group Description
&A for IP Address of the Server/Device causing the alert condition
&W for the Monitoring Rule ‘Name’ responsible for the alert
&R for the Monitoring Rule ‘Description’ text
&L for the Monitoring Rule ‘Severity’ level
&E for the Monitoring Rule Notes
&S for Status message or code associated with the alert
&V for the CounterWatch value that exceeded a threshold in this type alert.