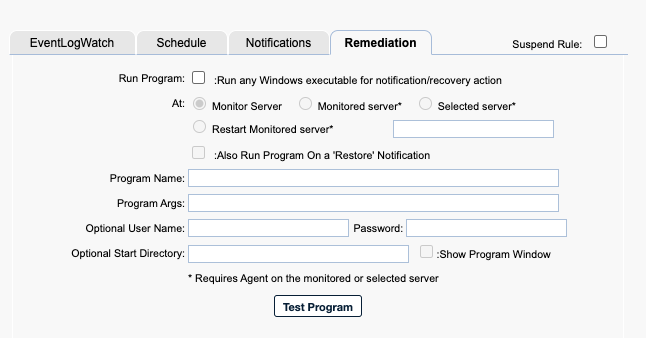
**Configure Custom Remediation**

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

With all rules/alerts, custom remediation actions can 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.



**Configure Custom Remediation Actions**

1. Check the box for **Run Program**
   1. When checked and the 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 Goliath Server, the monitored server or a designated server.
2. Select the appropriate radio button in the **At** field to choose to run the remediation action at the **Monitor Server** (Goliath Server), **Monitored Server** (machine where alert triggered), **Selected Server** (a different designated server), or to **Restart the Monitored Server**.
   1. If choosing **Selected Server**, use the text field below the option to enter the name of the machine as it is displayed on the **Configure - Inventory** page. Note, this machine must have a connected Goliath Agent in order for the remediation to take place
3. In the **Program Name** field, define the name of the program, Powershell, command line, batch file, etc to be executed 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:
   1. Powershell: C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe or powershell.exe
   2. Command line: C:\Windows\system32\cmd.exe or cmd.exe
   3. Bat File: C:\Temp\Test.bat
   4. 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. You can find these macros in the  Examples:
   1. Powershell: -ExecutionPolicy Bypass -File "C:\Program Files\MonitorIT\Scripts\test.ps1"
   2. Command: net stop Spooler
5. The **optional username and password** field 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 remediation 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.

**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.