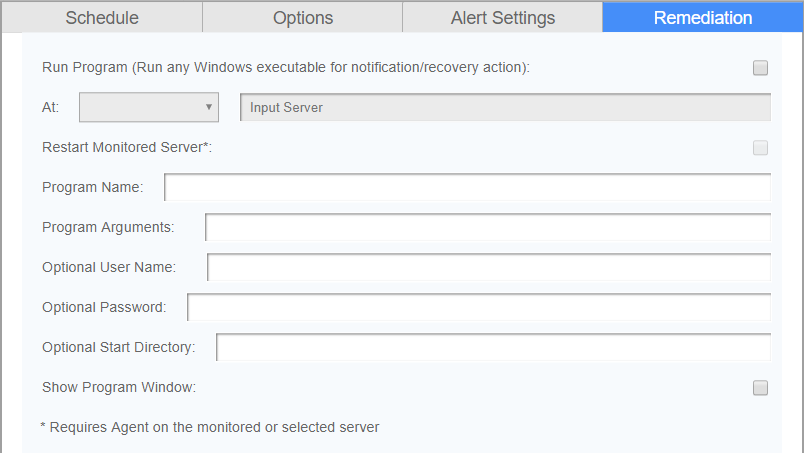
**Configure GAAM Custom Remediation**

This article was updated to support v11.7.8 of Goliath Performance Monitor.

When launches fail, remediation actions can be executed which will run 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.



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** (GAAM launch endpoint), **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.

**Appendix**

**Macros for Program Arguments**

 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:
    - GAAM: The full launch 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 launch ‘Description’ text
* &L: which is replaced by the for the launch ‘Severity’ level
* &E: which is replaced by the for the launch Rule Notes
* &V: (only for CounterWatch)