Monitoring Studio KM for PATROL

Version 9.0.00

June 2015
Contacting BMC Software

You can access the BMC Software Web site at http://www.bmc.com. From this Web site, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

| United States and Canada |
|---------------------------|-----------------|-------------------|
| **Address**               | **Telephone**   |
| BMC Software, Inc.        | 1 (713) 918 8800 or 1 (800) 841 2031 (Toll Free) |
| 2101 CityWest Blvd. Houston TX 77042-2827 | |

Copyright 2006 BMC Software, Inc. or licensors, as an unpublished work. All rights reserved.

BMC Software, the BMC Software logos, and all other BMC Software product or service names are registered trademarks or trademarks of BMC Software, Inc.

All other trademarks belong to their respective companies.

BMC Software considers information included in this documentation to be proprietary and confidential. Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation.

Restricted Rights Legend

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC Software, Inc., 2101 CityWest Blvd., Houston, TX 77042-2827, USA. Any contract notices should be sent to this address.
Customer Support

You can obtain technical support by using the Support page on the BMC Software Web site or by contacting Customer Support by telephone or e-mail.

Support Web Site

You can obtain technical support from BMC Software 24 hours a day, 7 days a week at http://www.bmc.com/support_home. From this Web site, you can:

- Read overviews about support services and programs that BMC Software offers
- Find the most current information about BMC Software products
- Search a database for problems similar to yours and possible solutions
- Order or download product documentation
- Report a problem or ask a question
- Subscribe to receive e-mail notices when new product versions are released
- Find worldwide BMC Software support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

You can also access product documents and search the Knowledge Base for help with an issue at http://www.sentrysoftware.com

Support by Telephone or E-mail

In the United States and Canada, if you need technical support and do not have access to the Web, call 800 537 1813. Outside the United States and Canada, please contact your local support center for assistance. To find telephone and email contact information for the BMC Software support center that services your location, refer to the Contact Customer Support section of the Support page on the BMC Software Web site at http://www.bmc.com/support_home.
Table of Contents

Product Hierarchy ........................................................................................................................................................................19
Credentials Management ........................................................................................................................................................................21
String Searches and Numeric Value Extraction .................................................................................................................................23
Thresholds and Alerts Actions .................................................................................................................................................................24
Requirements ..........................................................................................................................................................................................27
Getting the BMC Software Installation utility ....................................................................................................................................28
Packages ...............................................................................................................................................................................................28
Extracting the Setup Files .........................................................................................................................................................................29
Installing Monitoring Studio KM for PATROL ....................................................................................................................................32
Uninstalling Monitoring Studio KM for PATROL ...................................................................................................................................45
Integrating with BMC Portal .......................................................................................................................................................................53
Integrating with BMC TrueSight OM ......................................................................................................................................................54
1. Creating a Group ................................................................................................................................................................................59
2. Adding the Hosts to be Monitored .........................................................................................................................................................62
   (Optional) Adding a Monitor Group ..................................................................................................................................................67
3. Specifying the Monitors Used .............................................................................................................................................................68
   Monitoring Processes ................................................................................................................................................................................69
      1. Specifying the Process to be Monitored ...........................................................................................................................................70
         Selecting the Process to Monitor from a List ......................................................................................................................................71
         Entering Search Criteria ....................................................................................................................................................................74
         Providing the PID file path ..............................................................................................................................................................76
      2. Selecting Parameters .......................................................................................................................................................................77
      3. Configuring the Monitor Settings ................................................................................................................................................79
      4. Configuring the Process Cache Refreshing Frequency ..................................................................................................................80
   Analyzing Command Lines ..................................................................................................................................................................81
   Analyzing a Database Query .................................................................................................................................................................86
      Performing a Query on a Microsoft SQL Server Database ................................................................................................................87
      Performing a Query on a MySQL Server Database ..........................................................................................................................90
      Performing a Query on an Oracle Database Server .........................................................................................................................92
      Performing a Query on a PostgreSQL Database ..................................................................................................................................94
      Performing a Query on an Other Database ....................................................................................................................................96
   Monitoring Files .....................................................................................................................................................................................98
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring a File System</td>
<td>101</td>
</tr>
<tr>
<td>Monitoring Folders</td>
<td>103</td>
</tr>
<tr>
<td>Monitoring a Loaded KM</td>
<td>106</td>
</tr>
<tr>
<td>Monitoring SNMP Agents &amp; Traps</td>
<td>109</td>
</tr>
<tr>
<td>Polling SNMP Agents</td>
<td>109</td>
</tr>
<tr>
<td>Listening for SNMP Traps</td>
<td>114</td>
</tr>
<tr>
<td>Acknowledging Alerts</td>
<td>117</td>
</tr>
<tr>
<td>Importing Configuration</td>
<td>123</td>
</tr>
<tr>
<td>Exporting Configuration to a File</td>
<td>127</td>
</tr>
<tr>
<td>Monitoring Windows Event Logs</td>
<td>130</td>
</tr>
<tr>
<td>Monitoring Windows Performance Counters</td>
<td>134</td>
</tr>
<tr>
<td>Monitoring a Windows Service</td>
<td>136</td>
</tr>
<tr>
<td>Analyzing WMI Queries</td>
<td>148</td>
</tr>
<tr>
<td>Monitoring SNMP Agents &amp; Traps</td>
<td>152</td>
</tr>
<tr>
<td>Extracting Numeric Values</td>
<td>157</td>
</tr>
<tr>
<td>Example: XML LOG File Parsing</td>
<td>162</td>
</tr>
<tr>
<td>Acknowledging Alerts</td>
<td>170</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>171</td>
</tr>
<tr>
<td>Acknowledge all and Reset</td>
<td>172</td>
</tr>
<tr>
<td>Reset CollectionErrorCount</td>
<td>173</td>
</tr>
<tr>
<td>Configuring Java Settings</td>
<td>174</td>
</tr>
<tr>
<td>Configuring Thresholds</td>
<td>178</td>
</tr>
<tr>
<td>Specifying the Threshold Mechanism Mode</td>
<td>179</td>
</tr>
<tr>
<td>Setting or Modifying Alert Thresholds</td>
<td>180</td>
</tr>
<tr>
<td>Copy, Cut and Paste</td>
<td>184</td>
</tr>
<tr>
<td>Deploying your Configuration</td>
<td>185</td>
</tr>
<tr>
<td>Exporting Configuration to a File</td>
<td>186</td>
</tr>
<tr>
<td>Importing Configuration</td>
<td>190</td>
</tr>
<tr>
<td>Deleting a Monitored Object</td>
<td>195</td>
</tr>
<tr>
<td>Editing a Monitored Object</td>
<td>196</td>
</tr>
<tr>
<td>Forcing the Classic Mode</td>
<td>197</td>
</tr>
<tr>
<td>Modifying a Monitor Display Name and/or ID</td>
<td>199</td>
</tr>
<tr>
<td>Modifying a Group Display Name and/or ID</td>
<td>201</td>
</tr>
</tbody>
</table>
Modifying Group Constants .................................................................................................................. 203
Temporarily Suspending the Monitoring of an Object ........................................................................ 204
Refreshing Parameters .......................................................................................................................... 205
Specifying Alert Actions ...................................................................................................................... 206

  Alert Actions Capabilities .................................................................................................................. 212
  Alert Action Macros ........................................................................................................................... 221
    Format Symbols for %{SEN_TIME:...} Macros .................................................................................. 228
  Alert Actions Example ......................................................................................................................... 230

Setting Credentials .............................................................................................................................. 234
Setting the Discovery Interval ............................................................................................................. 238
Setting the Polling Interval .................................................................................................................. 239
Visualizing Currently Running Processes .......................................................................................... 241
Visualizing SNMP Traps ...................................................................................................................... 242
Visualizing a Host Windows Event Log .............................................................................................. 243
Visualizing a Monitored File Content .............................................................................................. 244
Visualizing Properties ......................................................................................................................... 245
Visualizing SNMP Agent Variables .................................................................................................... 246
Enabling the Debug Mode ................................................................................................................... 248

Frequently Asked Questions and Problems .......................................................................................... 250

  How Do I Know Which Version of Monitoring Studio I Am Running? .............................................. 250
  Although SNMP Trap Listening Seems to Work, No Trap Matches My Criteria ............................. 250
  Monitoring Studio Is Unable to Listen to SNMP Traps .................................................................... 250
  Can I Monitor the Processor Time Usage Made by a Windows Service? ....................................... 251
  Monitoring Studio Reads My Log File Entirely ............................................................................... 251
  Monitoring Studio Does Not Update All of My Folder Monitoring Parameters ............................ 251
  I'm Unable to Poll an SNMP Agent (Getting a Warning) .............................................................. 252
  I'm Unable to See the Monitoring Studio Icons in PATROL Central ............................................ 252
  Infinite Loop Reported in the PATROL Agent Log ........................................................................... 252
  Is It Possible to Monitor the CPU/Memory Usage of a Process Tree? ............................................ 253
  Monitoring Studio Fails to Connect to a Secured Web Server (SSL) from My UNIX/Linux Server ................................................................................................................................. 253
  Monitoring Studio Fails to Authenticate to My Web Server ......................................................... 253
  Monitoring Studio Does Not Follow an HTTP Redirection (Web) ................................................ 254
  Monitoring Studio Is Not Able to Post a Web Form to My Web Server ........................................ 254

Application Classes and Parameters .................................................................................................. 257

  SEN_MS_COMMANDLINE ...................................................................................................................... 259
  SEN_MS_DBQUERY .............................................................................................................................. 261
About WMI

Managing Baselines and Key Performance Indicators

About WMI
Release Notes for v.9.0.00
What you Absolutely Need to Know

- All the application classes and macros have been renamed to SEN_MS_* . No automatic migration will therefore be performed when installing Monitoring Studio 9.0.00. Version 9.0.00 will co-exist with Monitoring Studio 8.6.5x.
- Credentials management is now easier thanks to a centralized interface.
- When the KM is installed on a PATROL Agent, which is managed by Central Monitoring Administration, all the KM configuration menus are disabled in the PATROL Console. To be able to configure Monitoring Studio from a PATROL Console in such a situation, the KM Command **Force Classic Configuration Mode** was added to the **SEN_MS_MAIN** application class.
- Open VMS is no longer supported.
- **Java v1.6 or higher is required.**
- File Security and JMX monitoring are not implemented in this version.

What you Really Need to Know

- **Improved hierarchy** to better reflect what is monitored.
- Extended support for **remote monitoring**.
- **Host availability checks**: Ping, Hostname Resolution, SNMP, SSH, WMI, or TCP Port checks can be performed to make sure hosts are available. It will automatically turn off the monitoring of the elements attached to the host, if necessary.
- The interface has been greatly improved to be more user-friendly.

What’s Interesting to Know

**Collection Errors**

- It is now possible to report collection errors at the Group level.
- Monitoring Studio now checks that Java is available on the server and triggers an alert on the **CollectionErrorCount** parameter of the **SEN_MS_MAIN** application class.

**New Parameters**

<table>
<thead>
<tr>
<th>Application Class</th>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEN_MS_FILESYSTEM</td>
<td>AvailableInodesPercentage</td>
<td>Percentage of available inodes on UNIX and Linux platforms.</td>
</tr>
<tr>
<td>SEN_MS_FOLDER</td>
<td>Exists</td>
<td>Indicates whether the folder exists or not.</td>
</tr>
<tr>
<td>SEN_MS_MAIN</td>
<td>CollectionErrorCount</td>
<td>Provide further information about Monitoring Studio.</td>
</tr>
<tr>
<td></td>
<td>DebugStatus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HostCount</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MonitorCount</td>
<td></td>
</tr>
<tr>
<td>SEN_MS_PROCESS</td>
<td>Status</td>
<td>Status of Processes running on UNIX &amp; Linux platforms.</td>
</tr>
<tr>
<td>SEN_MS_PROCESS</td>
<td>MatchingProcesses</td>
<td>Displays the list of all matching processes.</td>
</tr>
</tbody>
</table>
### Application Class Parameters Description

<table>
<thead>
<tr>
<th>Application Class</th>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEN_MS_SNMPPolling</td>
<td>ExecutionTime</td>
<td>Time taken by the SNMP polling to execute.</td>
</tr>
<tr>
<td>SEN_MS_WBEMQuery</td>
<td>ExecutionTime</td>
<td>Time taken by the WBEM query to run.</td>
</tr>
<tr>
<td>SEN_MS_Winevent</td>
<td>MatchingEvents</td>
<td>Lists all matching Windows Events which contribute to MatchingEventCount as well as their related event message.</td>
</tr>
<tr>
<td>SEN_MS_Winservice</td>
<td>ServiceDetails</td>
<td>Additional information regarding the current status of the Windows Service</td>
</tr>
<tr>
<td>SEN_MS_Wmiquery</td>
<td>ExecutionTime</td>
<td>Time taken by the WMI query to run.</td>
</tr>
</tbody>
</table>

### Command Line Analysis

- The following command line parameters have been renamed:

<table>
<thead>
<tr>
<th>Previous Parameter Name</th>
<th>New Parameter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueryStatus</td>
<td>Status</td>
</tr>
<tr>
<td>ReturnOutput</td>
<td>Result</td>
</tr>
</tbody>
</table>

### Database Query Analysis

- The Command Line tool method has been removed from Database Queries. Only JDBC and ODBC are now supported.
- SSL Encryption can now be disabled when performing SQL queries to a Microsoft SQL Server.
- Performing a query on a Microsoft SQL Server 2000 is not possible with Java 1.8 and the SSL encryption enabled.
- The `ConnectionStatus` parameter was removed (this information is now available through the `Status` parameter).
- **Microsoft SQL Server:** The instance name was ignored if the dynamic port was not set.
- When using the JDBC or ODBC connection method, the `ExecutionTime` parameter was not reported if local settings did not follow the English format.
- The following database query parameters have been renamed:

<table>
<thead>
<tr>
<th>Previous Parameter Name</th>
<th>New Parameter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueryStatus</td>
<td>Status</td>
</tr>
<tr>
<td>ReturnOutput</td>
<td>Result</td>
</tr>
</tbody>
</table>

### File System Monitoring

- The following file system parameters have been renamed:

<table>
<thead>
<tr>
<th>Previous Parameter Name</th>
<th>New Parameter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FreeMegabytes</td>
<td>AvailableCapacity</td>
</tr>
<tr>
<td>FreeSpacePercent</td>
<td>AvailableCapacityPercentage</td>
</tr>
</tbody>
</table>
Folder Monitoring

- Specific credentials can now be specified while configuring folder monitoring.
- The following folder parameters have been renamed:

<table>
<thead>
<tr>
<th>Previous Parameter Name</th>
<th>New Parameter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>UsedSpaceGrowthPercentage</td>
<td>ConsumedCapacityGrowthPercent</td>
</tr>
<tr>
<td>UsedSpaceGrowthSpeed</td>
<td>ConsumedCapacityGrowthSpeed</td>
</tr>
</tbody>
</table>

Numeric Value Extraction

- The Delta and DeltaPerSecond parameters have been removed.

Process Monitoring

- Child processes associated to a monitored process can now be included when calculating the process performance statistics.

SNMP Agents & Traps Monitoring

- When adding the SNMP Polling or SNMP Trap Monitors, Monitoring Studio now verifies if SNMP is activated on the PATROL Agent. If not, a warning message is displayed.
- The Delta and DeltaPerSecond parameters have been removed from the SEN_MS_SNMP_POLLING application class.

String Search Monitoring

- When performing a String Search on a log file, it is now possible to report matching lines in the current collect only. Previously, Monitoring Studio would always report matching lines since the last acknowledgment (incremental).

WBEM Query Analysis

- This feature has been greatly optimized and uses less resources than the previous version. The WBEM Query Analysis tool now uses the WBEM collection hub.
- It is now possible to specify a timeout after which the query will be stopped.
- The following WBEM query parameters have been renamed:

<table>
<thead>
<tr>
<th>Previous Parameter Name</th>
<th>New Parameter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueryStatus</td>
<td>Status</td>
</tr>
</tbody>
</table>
Web Request Analysis

- Web Service requests (SOAP, REST, etc.) can now be performed through the Web Request Analysis tool.
- The following Web request parameters have been renamed:

<table>
<thead>
<tr>
<th>Previous Parameter Name</th>
<th>New Parameter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReturnOutput</td>
<td>Result</td>
</tr>
<tr>
<td>ServerConnectionState</td>
<td>Status</td>
</tr>
<tr>
<td>Status</td>
<td>HTTPStatus</td>
</tr>
</tbody>
</table>

Windows Event Monitoring

- Support for all event logs, including Crimson event logs.
- It is now possible to exclude unwanted event IDs from alerting.
- The 'Critical' event level is now available when defining the event settings.
- The AUDIT_FAILURE and AUDIT_SUCCESS event types are no longer supported and argument1 & argument2 cannot be used.
- The event description was not correct when a timeout was set for automatic alert acknowledgement.

WMI Query Analysis

- WQL queries (WMI) support dot characters in the WHERE statement.
- It is now possible to specify a timeout after which the query will be stopped.
- The following WMI query parameters have been renamed:

<table>
<thead>
<tr>
<th>Previous Parameter Name</th>
<th>New Parameter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueryStatus</td>
<td>Status</td>
</tr>
<tr>
<td>ReturnOutput</td>
<td>Result</td>
</tr>
</tbody>
</table>

Miscellaneous

- Macro syntax has been improved to support white spaces.
- **Debug Mode**: The KM debugging performance has been improved.
- **Duplicate object IDs**: Monitors could share the same ID which led to incorrect configuration. A unique object ID is now assigned to each Monitor.
- Setting large text parameters could cause the PATROL Agent or Console Server to crash. The size of all text parameters is checked and truncated to 1MB to avoid such crash.
What is Monitoring Studio?

Monitoring Studio KM for PATROL is the essential tool for all administrators who want to fulfill their custom monitoring needs. This toolbox enables to monitor almost any technology (application, server, device, etc.) for which there is no out-of-the-box monitoring solution. In a few clicks, 100% of technologies can be covered in the BMC monitoring environment. Compatible with Linux/UNIX and Windows, Monitoring Studio offers a simple and effective way to rapidly deploy the monitoring of custom technologies without any coding and with all the benefits of a “standard” solution maintenance, updates and patches etc. to further respond to growing technological needs for specific business-critical technologies.

With Monitoring Studio, it is possible to set up the monitoring of any technology, customize the way a notification is performed for an alert, or specify a recovery action to run when a problem occurs.

How it Works?

Monitoring Studio KM for PATROL is a Knowledge Module (KM) for BMC PATROL. Therefore, it must be installed on the following components of the PATROL framework:

- the PATROL Agents
- the PATROL Consoles
- the PATROL Console Servers (PATROL 7 framework only)

Version 9.0.00 of the KM can be configured to monitor any technology locally and remotely.
What to Monitor with Monitoring Studio?

Depending on the nature of the technology you wish to monitor, Monitoring Studio offers a large choice of tools that you can easily configure. The KM more especially allows to:

- Monitor processes
- Launch and analyze commands or scripts
- Send queries to a database back-end
- Monitor and analyze files
- Monitor file systems
- Monitor folders
- Monitor other KMs
- Monitor Windows performance
- Poll SNMP agents and listen for SNMP traps
- Execute and analyze WBEM queries
- Send requests to a web front-end
- Monitor Windows events
- Monitor Windows services
- Execute and analyze WMI queries

With Monitoring Studio, you will also be able to process the multi-line content, perform string searches, extract numeric values and monitor dynamic return outputs.
Architecture Diagram of Monitoring Studio

The diagram below shows how Monitoring Studio integrates within your BMC framework and shows interaction between all the components that compose your monitored environment.
General Concepts
Introduction

This section provides general information about the following important concepts of Monitoring Studio KM for PATROL:

- Product Hierarchy
- Credentials Management
- String Searches and Numeric Value Extraction
- Thresholds and Alerts Actions
Product Hierarchy

The architecture of Monitoring Studio KM for PATROL has been designed in a logical manner to help you easily and intuitively manage all your technologies (application, server, device, etc.) and to reflect as accurately as possible the genuine hierarchy of the environment you want to monitor. The Monitoring Studio hierarchy has been established as follows:

1. **Monitoring Studio**
   - The Monitoring Studio instance (SEN_MS_MAIN) is at the highest level of the hierarchy. It appears once the KM has been installed on a PATROL agent and is loaded in a BMC PATROL Console. It is the starting point of the Monitoring Studio configuration. Groups are created from this instance.

2. **Group**
   - A Group instance (SEN_MS_GROUP) is the main container which corresponds to the technology you need to monitor (application, server, device, etc.). Groups are displayed at the same level as the Monitoring Studio instance and contain one or several Hosts.

3. **Host**
   - A Host instance (SEN_MS_HOST) includes information about the target server where the technology is running (hostname, system type, credentials list, SNMP community information and host availability check information, etc.). Hosts are arranged under the Group instance and contain either Monitor Groups or Monitors.
Monitor Group

A Monitor Group instance (SEN_MS_MONITORGROUP) is an optional container that you can use to group monitors. Monitor Groups are created under a Host and contain Monitors.

Monitor

Monitor instances are at the lowest level of the hierarchy and corresponds to the diverse monitoring tools available in Monitoring Studio. Monitors are either grouped directly under a Host or under a Monitor Group. They can also be referred to as "monitored objects".

Here is the complete list of Monitors:

- Command Line (SEN_MS_COMMANDLINE)
- Database Query (SEN_MS_DBQUERY)
- File (SEN_MS_FILE)
- File System (SEN_MS_FILESYSTEM)
- Folder (SEN_MS_FOLDER)
- Multi-Parameter Formula (SEN_MS_FORMULA)
- Performance Counter (SEN_MS_WINPERF)
- Process (SEN_MS_PROCESS)
- SNMP Polling (SEN_MS_SNMP POLLING)
- SNMP Trap (SEN_MS_SNMPTRAP)
- WBEM Query (SEN_MS_WBEMQUERY)
- Web Request (SEN_MS_WEBREQUEST)
- Windows Event (SEN_MS_WINEVENT)
- Windows Service (SEN_MS_WINSERVICE)
- WMI Query (SEN_MS_WMQUERY)
- Text Pre-Processing (SEN_MS_TRANSFORM)
- String Search (SEN_MS_STRING)
- Numeric Value Extraction (SEN_MSNUMBER)
- Dynamic Instances (SEN_MS_DYNAMIC)
Credentials Management

In order to avoid security integrity breach, administrators are asked to authenticate to access almost every component in a standard IT environment (host servers, databases, files, etc.).

Monitoring Studio KM for PATROL requires these credentials to connect to the host you wish to access and collect data from technologies.

Since technologies may or may not require specific username and password to grant access to their data, Monitoring Studio offers two different levels of credentials.

System Credentials

System Credentials are provided at the Host level and can be shared by several monitors. When the system credentials are changed, users only need to modify the credentials once for all the monitors to inherit the changes.

The following monitors can only use system credentials:

- File System ([SEN_MS_FILESISTEM])
- Process ([SEN_MS_PROCESS])
- Windows Event ([SEN_MS_WINEVENT])
- Windows Performance Counter ([SEN_MS_WINPERF])
- Windows Service ([SEN_MS_WINSERVICE])
- WMI Query ([SEN_MS_WMİQUERY])

If the system credentials are not specified when monitoring a localhost, Monitoring Studio will use the PATROL Agent's default account information. For remote monitoring, System Credentials are mandatory for the monitors listed above; failing to provide this authentication information will prevent the monitors from collecting any data.
Specific Credentials

For security purpose, some technologies may require additional privileges to allow access to their data. In this case, Monitoring Studio enables users to provide specific credentials that will only apply to the monitor instance they relate to.

The following monitors may require specific credentials. If specific credentials are not provided, the solution will automatically use the system credentials provided at the Host level:

- Command Line (SEN_MS_COMMANDLINE)
- Database Query (SEN_MS_DBQUERY)
- File (SEN_MS_FILE)
- Folder (SEN_MS_FOLDER)
- WBEM Query (SEN_MS_WBEMQUERY)
String Searches and Numeric Value Extraction

Some technologies report their bad health through repeated error messages or critical numbers which are hidden deep in log files, output of commands, database, Web page, etc. Monitoring Studio KM for PATROL is capable of parsing all this data by means of String Search and Numeric Value Extraction features to detect the source of potential problems and alert you when they occur.

String Search and Numeric Value Extraction features are available for the following monitors:

- Command Line (SEN_MS_COMMANDLINE)
- Database Query (SEN_MS_DBQUERY)
- Dynamic Instances (SEN_MS_DYNAMIC)
- File (SEN_MS_FILE)
- SNMP Polling (SEN_MS_SNMPOLLING)
- Text Pre-Processing (SEN_MS_TRANSFORM)
- WBEM Query (SEN_MS_WBEMQUERY)
- Web Request (SEN_MS_WEBREQUEST)
- WMI Query (SEN_MS_WMIQUERY)

Searching for a Specific String

The String Search feature (SEN_MS_STRING instance) enables you to run fast and powerful searches for strings on some of the monitored objects that you previously configured (flat or log files, the output of a Web request or a database query, OID content, etc). You can then decide to trigger an alert and send a notification to your hypervision system when the string specified is found or not found in the return output of monitored instances.

Extracting Numeric Values

The Numeric Value Extraction feature (SEN_MS_NUMBER instance) enables you to extract numeric values from a text input (the output of a command, a Web page, the result of a SQL query, or WBEM query, etc). All you need to do is indicate how to find the numeric values within the monitored object and Monitoring Studio will extract and report them as graphs in the Console.
Thresholds and Alerts Actions

What Are Thresholds?

Thresholds are used to define acceptable values for the parameters collected. You can set thresholds for each parameter of any monitor. Breaching these thresholds will trigger an alert.

Monitoring Studio KM for PATROL offers default thresholds that can be very easily tailored to your needs through wizards. Monitoring Studio accepts up to two alert thresholds in addition to defining the acceptable range values.

What Are Alert Actions?

When a threshold is breached, an alert is raised. Alert Actions enable you to configure specific actions to be executed when an alert is raised by a parameter. With Alert Actions, it is possible to customize the way a problem notification is performed, or specify a recovery action to be run when a problem occurs.
Preparing for Installation
This chapter provides information about the tasks that must be performed before you start installing Monitoring Studio KM for PATROL. Make sure to carefully read the following sections requirements:

- Requirements
- Getting the BMC Software Installation Utility
- Packages
- Extracting the Setup Files
Requirements

BMC Framework

Console Systems
- PATROL Consoles

Optional
- BMC ProactiveNet
- BMC TrueSight Operations Management

PATROL Agent
- Monitoring Studio KM for PATROL supports any version of the PATROL Agent.

JAVA

Monitoring Studio KM for PATROL requires Java 1.6 or higher and a Java Runtime Environment (JRE) to be installed on the same system that runs the PATROL Agent.

You can download the Java Runtime Environment along with the KM on the Sentry Software Web site.

UNIX/Linux Systems

Password authentication must be enabled on all UNIX/Linux systems that are monitored remotely.

To enable password authentication:

1. Edit `/etc/ssh/sshd_config` configuration file.
2. Set `PasswordAuthentication` to `yes` in `/etc/ssh/sshd_config`

   ```
   # vi /etc/ssh/sshd_config
   PasswordAuthentication yes
   ```

3. Save your modifications.
4. Run the following command to restart the SSH daemon:

   ```
   # /etc/init.d/ssh restart
   ```
Getting the BMC Software Installation Utility

In order to install Monitoring Studio KM for PATROL, you need the latest version of the BMC Software Installation Utility. You can download the latest Installation Utility from the Monitoring Studio KM for PATROL page on the Sentry Software Website.

Choose the appropriate package depending on the platform on which you plan to install Monitoring Studio KM for PATROL:

- For UNIX/Linux systems: `ins_ALL_<version>.tar`
- For Windows systems: `ins_WINDOWS_<version>.zip`

The packages are valid for all the PATROL components: Agent, Console, Console Server, etc.

Place the Installation Utility package in the same folder as the Monitoring Studio KM for PATROL packages.

Packages

The Monitoring Studio KM for PATROL packages are available on the Sentry Software Web site.

There are three packages, each of which can be used to install the KM on every PATROL component (Agent, Console, etc.) according to the platform you are using:

- For Windows systems: `senms_ALL_<version>.zip`
- For UNIX and Linux systems: `senms_ALL_<version>.tar`

Java Runtime Environment Package

Java Runtime Environment version 1.6.00 or higher is required for the KM to operate properly. A package with a suitable Java Runtime Environment, designed for use with the BMC Software Installation Utility, is made available to download on the Sentry Software Web site. It can be installed along with the Monitoring Studio package. The KM will be able to leverage either this instance of the Java Runtime Environment or another installed separately on the system.

⚠️ The Monitoring Studio KM for PATROL packages are designed for use with the BMC Software Installation Utility (formerly known as Thorium). They need to be merged with the latest available version of the BMC Software Installation Utility. Please see instructions.
Extracting the Setup Files

Like most Knowledge Modules for PATROL, you need to install Monitoring Studio on the following components of your PATROL architecture:

- Every managed system with a PATROL Agent
- Every PATROL Console (Classic)
- The PATROL Console Server
- PATROL Central – Web Edition

On Windows

The packages for Windows are to be extracted in the following order:

1. Unzip the BMC Installation Utility: ins_Windows_<version>.zip
2. Unzip the Monitoring Studio KM package in the same folder: senms_ALL_<version_number>.zip
3. Unzip the senjre_<version>_WINDOWS.zip package if you need to install a Java Runtime Environment program

The content of the packages merges into a subfolder named bmc_products.

⚠️ Windows may ask for your confirmation to overwrite files and folders. This is normal behavior and you can accept all overwrite confirmation requests.

On UNIX/Linux

The packages for UNIX/Linux are to be extracted with the tar utility in the following order:

1. Untar the BMC Installation Utility: tar xvf ins_ALL_<version>.tar
2. Untar the Monitoring Studio KM package named: tar xvf senms_ALL_<version>.tar

The files are extracted into a sub-directory named bmc_products.
Installing Monitoring Studio KM for PATROL
Introduction

This section describes the installation procedure for Monitoring Studio KM for PATROL on any PATROL component (Agents, Consoles, Console Server, etc.). As the setup is based on the BMC Software Installation Utility, this procedure applies to all operating systems supported by Monitoring Studio KM for PATROL. Although not covered by this section, the installation through the Distribution Server is fully supported. Please refer to the Distribution Server documentation for a detailed description of the deployment procedure.
Installing Monitoring Studio KM for PATROL

Installing Monitoring Studio KM for PATROL is an automated process managed by a wizard. The wizard goes through the necessary steps to properly install Monitoring Studio and all files associated with it. You are simply prompted for the product's folder location and the product/components to install. Browse to the `bmc_products` folder where the files have been extracted (both Monitoring Studio and the Common Installer).

- On Windows: Launch the `setup.exe` program.
- On UNIX: Launch the `setup.sh` script

On the more recent versions of Windows, you may get this security alert dialog: Windows detected that the BMC Software Installation Utility is listening on the 50001 port.

⚠️ No automatic migration will be performed when installing Monitoring Studio 9.0.00. Version 9.0.00 will co-exist with Monitoring Studio 8.6.5x.
To install Monitoring Studio KM for PATROL

1. Allow the perl.exe program to listen on this port: Click **Allow access**.
2. The welcome screen of the installer appears. Click **Next** to continue.
3. Read the license agreement, click the **Accept** option and then click **Next** to continue.
4. Select **Install products on this computer now** and click **Next** to continue.
5. Specify the BMC Software products folder. See the BMC Software documentation for more information about the BMC Software products folder. Click **Next** to continue.
6. Select **Default**. Installing Monitoring Studio does not require any customization. Click **Next** to continue.

**Installation Wizard - Step 6: Selecting an Installation Type**

- **Default**
  - You want to select pre-packaged solutions with pre-defined configurations.
  - You are new to the product set you want to install.
  - You are performing a first-time install (you are not upgrading).

- **Custom**
  - You want the ability to select or deselect components and customize configurations.
  - You are an advanced user of the product set you want to install.
  - You are upgrading or performing a first-time install.
7. Select:
   - **Managed System** to install Monitoring Studio on a PATROL Agent.
   - **Console Systems** to install Monitoring Studio on a PATROL Classic Console.
   - **Common services** to install Monitoring Studio on the PATROL Console Server or on PATROL Central – Web Edition.
   Click **Next** to continue.
8. Select:
   - **Monitoring Sentry KM for PATROL** to install the KM.
   - **Java Runtime Environment** program if you want to install it along with the KM (this option is only provided when you have previously [downloaded the package](#)).
   
   Click **Next** to continue.
9. Review the installation parameters and click **Start Install** to launch the installation procedure.
10. The setup program displays the actions performed and indicates the percentage of completion. Once the installation complete, click Next the view the installation results.
11. The wizard displays the installation results. Click View Log to display a detailed log of the installation procedure. Click Next and then Finish to exit the setup program.
12. Click the **Finish** button to quit the installation wizard.
Uninstalling Monitoring Studio KM for PATROL

Uninstalling Monitoring Studio is an automated process managed by a wizard. The wizard goes through the necessary steps to remove Monitoring Studio and all files associated with it. You are simply prompt for the product's folder location and the product/components to uninstall.

1. Locate the **Uninstall** folder under the BMC products directory (typically under C:\Program Files\BMC Software, or /opt/bmc)
2. Make sure the uninstall program is up-to-date. You may need to use the installation program from a fresh Installation Utility package.
3. Launch the uninstall program:
   - On Windows systems, run `uninstall.exe`
   - On UNIX, run `uninstall.sh`
4. Specify the BMC Software products folder. See the BMC Software documentation for more information.

Uninstall Wizard — Specifying folder
5. Select **Monitoring Studio KM for PATROL**.
6. Review the summary and click **Start Uninstall**.

![Uninstall Wizard — Reviewing Selected Products & components and start uninstalling](image)
7. A page displays the list of products/components processed and the percentage of completion. Click **Next** to continue.
8. A page displaying SUCCESS indicates that Monitoring Studio KM for PATROL is now uninstalled. Click Finish to quit the wizard.
Integrating Monitoring Studio KM for PATROL
Introduction

This section provides detailed information about the integration of Monitoring Studio KM for PATROL into the BMC framework.

- Integrating with BMC Portal
- Integrating with BMC TrueSight OM
Integrating with BMC Portal

An integration component for BMC Portal is released along with the Knowledge Module (KM) in the form of a PAR file: `BMC-PM-PATROL-Monitoring-Studio-<version>.par`. It enables visualization of parameter data of all objects monitored by the KM, in the BMC Portal environment.

⚠️ This integration component is valid on BMC portal v2.5 upwards.

To integrate Monitoring Studio with BMC Portal:

1. Install the KM on top of a PATROL Agent as detailed in the Installation Guide. A PATROL Console will be required to configure the KM.
2. In the PATROL Console, make sure the discovery is properly performed and data is collected.
3. Upload the PAR file in BMC Portal:
   - Place the `BMC-PM-PATROL-Monitoring-Studio-<version>.par` file in a known location on your file system.
   - Log in to BMC Portal with the superadmin credentials.
   - Click on Portal, then under Tasks click Performance Managers.
   - Click Upload and then click Browse to open a file selection dialog box.
   - Select `BMC-PM-PATROL-Monitoring-Studio-<version>.par` and click Upload.
4. Create a new managed element:
   - Log in to BMC Portal with administrator credentials.
   - Click the Configure tab > Elements > Add.
   - Select Infrastructure Element and click Next.
   - Select an RSM to collect data about the infrastructure element and click Next.
   - Enter the name of the machine on which the PATROL agent is running, the Host Name and click Next.
   - Select the group to which your PM will belong and click Next.
   - Select the PATROL category, the Application Classes to add and click Next.
   - Set the Properties and Credentials that the RSM must have to access the specified elements and click Next. The list of thresholds is displayed. You can update these settings without impacting the values set in PATROL.
5. Click Finish.

⚠️ Thresholds are set in the PATROL Console. To get the last configurations made, click the Refresh PATROL Integration button available in the Elements page.
Integrating with BMC TrueSight Operations Management

BMC ProactiveNet Performance Management 8.5 or 8.6
To integrate Monitoring Studio KM for PATROL into BMC ProactiveNet Performance Management 8.5 and 8.6, you need create a specific adapter. For more information, please refer to Integrating the Sentry Software’s KMs into BMC ProactiveNet Performance Management (BPPM).

BMC ProactiveNet Performance Management 9.0 and higher
No specific integration steps need to be performed.
Loading Monitoring Studio KM for PATROL
In order to start monitoring any technology (application, server, device, etc.) within your PATROL Console, Monitoring Studio KM for PATROL must be loaded on the appropriate managed system. Loading a Knowledge Module in PATROL Central Operator both loads the Knowledge Module on the managed system and adds the name of the Knowledge Module to your management profile.

⚠️ Before you can load a Knowledge Module, it must be installed on a managed system. Loading a Knowledge Module loads it on the managed system, if it was not already loaded, and adds it to your management profile.

Loading Monitoring Studio KM for PATROL on PATROL Classic
1. In the Console menu bar, click File > Load KM.
2. In the Files of Type list, select KM List Files (*.kml).
3. Select SEN_MS.kml.
4. Click Open.

Loading Monitoring Studio KM for PATROL on PATROL Central
1. In the Common Tasks tab of the PATROL Central Operator Taskpad, click the Load Knowledge Modules icon.
2. To start the wizard, click Next.
3. Select the check boxes for the managed systems that you want to load Monitoring Studio KM for PATROL on. Click Next.
4. Select the SEN_MS.kml check box in the Knowledge Module Lists tab.
5. Click Finish.
Configuring Groups, Hosts and Monitors
The configuration of Monitoring Studio KM for PATROL will mostly depend on the type of technology to be monitored. It is however recommended to follow these guidelines:
1. **Create a Group**
2. **Add the Hosts to be monitored**
3. **Specify objects to be monitored**
4. **Specify the information to be searched**

Once configured, the technology (application, server, device, etc.) is displayed in the PATROL Console. This technology is then monitored just like any other standard component of the system (hardware, OS, middleware, etc.).

⚠️ *The entire configuration of Monitoring Studio is stored in the agent configuration tree (under /SENTRY/STUDIO).*
1. Creating a Group

A Group is designed to facilitate the management of the monitored technologies (application, server, device, etc.). Typically, the Group display name is the name of the technology you wish to monitor, for example 'My Company's Web Site'. A Group is displayed at the same level as the Monitoring Studio instance and contains one or several Hosts.

To create a Group:

1. In the PATROL Console, right-click the Monitoring Studio icon and select KM Commands > New Group...

2. Name your Group:
   - **Group name**: Enter the name of the group to be created.
   - **(optional) Description**: Describe the group to be monitored.
   - **(optional) Owner contact details**: Enter the name, E-mail, phone number, etc. of the person to be alerted or who can provide support if an alerts occurs.

3. Click Next.
Group Constants

4. Define the **Group Constants** for the Monitor Group. Constants are very useful for monitoring a technology whose properties may change from one system to another. Constants are defined at the Monitor Group level and can be reused in the Monitors related to the group. They facilitate the monitoring across various systems of a technology whose properties may change from one system to another. Here is an example of use:

   **Example:** You want to specify the monitoring of a remote device using SNMP polling and SNMP trap listening objects in Monitoring Studio. Instead of specifying the IP address of the remote device directly in these SNMP monitor instances, you can define a DEVICE_IPADDRESS constant at the level of the Monitor Group and use `%{DEVICE_IPADDRESS}` in the SNMP polling and SNMP listening objects. If the IP address changes later, you will only need to modify the value of the DEVICE_IPADDRESS constant, instead of editing every SNMP polling and trap listening object.

   Fill in the following fields:
   - **Constant name**: Enter the name of the constant. Example: TECHNOLOGY_PATH
   - **Value**: Set a value for the constant. Example: /opt/MyTechnology. If you enter the word "PASSWORD" in a Constant name, the corresponding value will be automatically encrypted once you click the Finish button at the last step of the wizard.
   - **Required**: Check the box to activate this newly-set group constant. The monitoring of the Group and all its dependent objects will be offline if the value of the group constant is not set. This ensures that no monitoring operation is performed until the required group constants are properly set. This feature is particularly useful if you create a group monitoring template where all the defined group constants are empty – in this case, you first import the configuration template, then enter values to all required group constants before the monitoring actually starts.
5. Click **Next**.

![New Group dialog box](image)

6. The new group is defined by an **Internal ID** and a **Display name**. These values, set by default by Monitoring Studio, can however be modified while configuring the group. Modify the fields of your choice:

- **Internal ID**: PATROL internal identifier of this **Group**.
- **Display name**: Label that will appear next to the **Group** in the PATROL Console.

**What thresholds do you want to set for the newly created instance?**

- **I want to use the default thresholds**: Uses the default thresholds set by Monitoring Studio. (see [SEN_MS_GROUP](#))
- **I want to set custom thresholds**: Allows you to customize the thresholds for all parameters of the instance
- **I want to use the default thresholds and customize them**: Sets the default Monitoring Studio thresholds on all parameters and then allows you to customize any/all of them. This is mainly intended to help save time if you wish to customize the thresholds of just one of many parameters for the instance, and leave the default settings for the others.
- **I do not want to set any thresholds for now**: No thresholds will be set on any parameter of the instance, and as a result no alerts will be triggered. Monitoring Studio will poll the object and return the output of the polling – but will not raise any alerts until you set thresholds.
7. Click Finish.

The Group instance appears in the PATROL Console. You can now:

- Add Hosts by right-clicking the Group instance and selecting KM Commands > New > Host...
- Edit your Group by right-clicking the Group instance and selecting KM commands > Edit.
- Remove your Group by right-clicking the Group instance and selecting KM commands > Delete.

After confirmation, the Group icon and all its dependent objects will be removed from the PATROL Console and from the agent configuration.

2. Adding the Hosts to be Monitored

Once you have created the Group associated to your targeted technology, the second action you need to perform is to provide Monitoring Studio with the information related to the Host on which the technology you want to monitor is running. A Host instance contains all the information about the server where the technology to monitor is running (hostname, system type, connection credentials list, SNMP community information, host availability check information, etc.). Hosts are grouped under the Group instance and contain Monitor Groups as well as Monitors.

To create a Host:

1. In the PATROL Console, right-click the Group icon and select KM Commands > New > Hosts...

2. Name your Host icon:
   - Hostname/IP address/FQDN: Enter the Hostname, IP address or Fully Qualified Domain
Name of the host on which the technology you wish to monitor is running.

- (optional) **Display Name**: Enter the name that will be displayed in the console for this Host.
- **System type**: Select the operating system running on the host you wish to connect to (Windows, UNIX/Linux or Other).

3. **Create a separate device in TrueSight**: Check this box if you want the remote monitored host to appear as a separate device in TrueSight OM.

4. **Click Next**.
2. Adding the Hosts to be Monitored

5. **(optional) System Credentials**: Enter the **Username** and **Password** to connect to the targeted host. These credentials will be used for all **system related monitoring tasks** to gather data.

6. **(optional) SNMP Credentials**: Enter the name of the **Community** to be used when performing SNMP monitoring and/or an SNMP availability check.

7. Click **Next**.
2. Adding the Hosts to be Monitored

8. (Optional) Select the method Monitoring Studio should use to test the availability of the monitored host:
   - **Ping check**: Select this option to have Monitoring Studio ping the monitored host. To be successful, the targeted host must respond to at least one ping command out of four, during each collection cycle.
   - **Hostname Resolution Check**: Select this option to check that Monitoring Studio can resolve the hostname of the monitored host to an IP address.
   - **SNMP check**: Select this option to have Monitoring Studio check the monitored host availability via an SNMP session. For the SNMP availability check to be successful, an SNMP session is opened with the targeted host and a `snmp_get_next()` is performed on the OID "1.3.6.1". If it fails, a second `snmp_get_next()` is tried on the OID "1.3.6.1.4.1". If something is returned, the SNMP availability checked is successful.
   - **SSH check**: Select this option to have Monitoring Studio check the targeted host availability via the SSH protocol. For the SSH availability check to be successful, Monitoring Studio must be able to connect to the host using the provided System Credentials.
   - **TCP Port check**: Select this option to have Monitoring Studio check the targeted host availability via a TCP connection. You must provide the port number the protocol must use to access the host.
9. (Optional) **Signature Files Check**: Click to open the **Signature Files Check** dialog box. If at least one of the signature files is present, the check is considered successful:

![Signature Files dialog box]

- **Paths to the signature files:**

  - Provide the name and full path of the signature file on the targeted host.
  - Click **Accept**.

- **Wildcards are not supported in signature files**

10. **Disable related monitors when the host is unreachable**: Select this option if you wish Monitoring Studio to disable the monitoring of all Monitors attached to the Host.

- **The monitoring will automatically resume when the host is once again available.**

11. Click **Finish**.

The **Host** icon appears in the PATROL Console. You can now **specify the Monitors to use** or first **create a Monitor Group**.
(Optional) Adding a Monitor Group

Once you have added the Hosts to be monitored, you can decide to add an optional container under the Hosts: the Monitor Group.

The Monitor Group offers you a higher level of classification. Thanks to this additional container, you can bring Monitors together, organize, and arrange them.

To add a Monitor Group:

1. In the PATROL Console, right-click the Host icon and select KM Commands > New > Monitor Group...

2. Indicate the:
   - PATROL internal identifier (Internal ID field)
   - label to be displayed in the PATROL console (Display name field)

3. Click OK.

Your Monitor Group has been successfully created. You can now specify the Monitors to use.
3. Specifying the Monitors Used

Once you have created the **Group Icon**, the **Host(s)** and the **Monitor Group(s)** (optional) related to your technology, you need to specify what must be monitored for this technology.

You can choose among a large choice of tools that can be easily configured to monitor:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Windows to Windows</th>
<th>UNIX to Windows</th>
<th>Windows to UNIX</th>
<th>UNIX to UNIX</th>
<th>Windows To Other</th>
<th>UNIX to Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Lines</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Database Queries</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Files</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>File Systems</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Folders</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Multi-Parameter Formulas</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Processes</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SNMP Agents</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WBEM Queries</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Web Requests</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Windows Events</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Windows Performance Counters</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Windows Services</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WMI Queries</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Monitoring Processes

When monitoring a technology, you typically want to check that its processes are running properly but recognizing them amongst all the running processes can sometimes be challenging.

The Process Monitoring tool provided by Monitoring Studio allows you to easily check the presence of Windows, UNIX, or Linux processes by specifying one or more of the following criteria:

- The Process Name (as it appears in ps or in the Windows Task Manager)
- The Command Line that was used to spawn the process
- The Username the process is run as
- The PID file path that contains the process ID

⚠️ These criteria will be automatically pre-filled when selecting the process to monitor from the currently running processes list.

Once you have specified the process to be monitored, you just have to indicate which parameters should be monitored.
1. Specifying the Process to be Monitored

The **Process Monitoring** tool allows you to identify the process to be monitored by either:

- Selecting the process from a list
- Entering search criteria
- Providing the PID file path.

![Specifying the Process to Be Monitored - Three Methods](Image)
Selecting the Process to Monitor from a List

If you wish to select the process to be monitored from a list:

1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select Process from the drop-down list and click Next.
3. Check Select the process from current process list and click Next. It may take a few seconds for Monitoring Studio to retrieve the list of all the currently running processes.
4. Click Current processes to display the list of all running processes.
5. Click the process you wish to monitor and click **Accept**.

6. Click **Next**. The process criteria panel is displayed with all information already filled.

7. Remove or modify any information you do not wish to monitor and click **Next**.

   **All fields are optional but at least one field must be completed. The process to monitor must match all the criteria if more than one is entered.**
Examples:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Processes that match the criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example 1</strong>&lt;br&gt;• Process name MUST BE EXACTLY patrolagent.exe&lt;br&gt;• Command-line = &lt;nothing&gt;&lt;br&gt;• User = &lt;nothing&gt;</td>
<td>PatrolAgent.Exe&lt;br&gt;C:\Patrol\PatrolAgent.exe&lt;br&gt;-p 3181&lt;br&gt;C:\Patrol\PatrolAgent.exe</td>
</tr>
<tr>
<td><strong>Example 2</strong>&lt;br&gt;• Process name MUST BE EXACTLY patrolagent.exe&lt;br&gt;• Command-line MUST MATCH THE REGULAR EXPRESSION -[pP] 3181&lt;br&gt;• User = &lt;nothing&gt;</td>
<td>C:\Patrol\PatrolAgent.exe&lt;br&gt;-p 3181</td>
</tr>
<tr>
<td><strong>Example 3</strong>&lt;br&gt;• Process name MUST CONTAIN Pat&lt;br&gt;• Command-line = &lt;nothing&gt;&lt;br&gt;• User = &lt;nothing&gt;</td>
<td>PatrolAgent.exe&lt;br&gt;PatProcess.exe&lt;br&gt;PatrolPerf.exe</td>
</tr>
</tbody>
</table>

⚠️ To monitor all processes of a selected user, fill out the "User" field and leave "Process name" and "Command-line" empty.

8. **Select the parameters to be monitored** for this process and click **Next**.
9. **Configure the Monitoring Studio settings**
10. Click **Finish**.
Entering Search Criteria

The **Process Monitoring** tool also allows you to enter search criteria to identify the process to be monitored:

1. In the PATROL Console, right-click the **Host icon** and select **KM Commands > New > Monitor...**
2. Select **Process** from the drop-down list and click **Next**.
3. Check **Enter the criteria to select processes** and click **Next**. The following dialog box is displayed:

   ![New Process Configuration Dialog](image)

   **Entering Search Criteria** - Enter criteria to identify and monitor processes

4. Specify your search criteria:
   - (Optional) In the **Process name** section, select a condition option and enter the name of the process you wish to monitor.
   - (Optional) In the **Command line that launched the process** section, select a condition option and enter a regular expression. Only processes that have been launched by a command-line that matches this regular expression will be monitored.
   - (Optional) In the field **Process runs as this user**, enter the user name the monitored process is running as.
   - Click **Next**.

   *All fields are optional but at least one field must be completed. The process to monitor must match all the criteria if more than one is entered.*
Examples:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Processes that match the criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example 1</td>
<td></td>
</tr>
<tr>
<td>• Process name MUST BE EXACTLY patrolagent.exe</td>
<td></td>
</tr>
<tr>
<td>• Command-line = &lt;nothing&gt;</td>
<td></td>
</tr>
<tr>
<td>• User = &lt;nothing&gt;</td>
<td></td>
</tr>
<tr>
<td>PatrolAgent.Exe</td>
<td></td>
</tr>
<tr>
<td>C:\Patrol\PatrolAgent.exe</td>
<td></td>
</tr>
<tr>
<td>-p 3181</td>
<td></td>
</tr>
<tr>
<td>C:\Patrol\PatrolAgent.exe</td>
<td></td>
</tr>
</tbody>
</table>

| Example 2 |
| • Process name MUST BE EXACTLY patrolagent.exe |
| • Command-line MUST MATCH THE REGULAR EXPRESSION -[pP] 3181 |
| • User = <nothing> |
| C:\Patrol\PatrolAgent.exe |
| -p 3181 |

| Example 3 |
| • Process name MUST CONTAIN Pat |
| • Command-line = <nothing> |
| • User = <nothing> |
| PatrolAgent.exe |
| PatProcess.exe |
| PatrolPerf.exe |

⚠️ To monitor all processes of a selected user, fill out the "User" field and leave "Process name" and "Command-line" empty.

⚠️ Search criteria are case-sensitive on UNIX and Linux.

5. Select the parameters to be monitored for this process and click Next.
6. Configure the Monitoring Studio settings
7. Click Finish.
Providing the PID file path

Some technologies record their PID (process ID) in a pre-defined file. Monitoring Studio can read the PID from this file and monitor the corresponding process.

1. In the PATROL Console, right-click the Host icon and select KM Commands > New > Monitor...

2. Select Process from the drop-down list and click Next.

3. Check Provide a PID file path and click Next.

4. Enter the PID file path and click Next. At each polling, Monitoring Studio reads this file, retrieves the PID number and checks whether this process PID exists or not. Normally, the process PID is dynamically allocated. The process PID number should be at the very beginning of the file’s content.

5. Select the parameters to be monitored for this process and whether you want to include all child processes. Click Next.

6. Configure the Monitoring Studio settings

7. Click Finish.

All processes that match the entered criteria will be monitored and identified as one icon in the PATROL Console.
2. Selecting Parameters

Once you have specified a process, you will have to select the parameters to be monitored among the following ones:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>Displays the number of processes that match the criteria.</td>
<td>Processes</td>
</tr>
<tr>
<td>ChildCount</td>
<td>Displays the number of children of the matching process(es).</td>
<td>Processes</td>
</tr>
<tr>
<td>ProcessorTime</td>
<td>Displays the processor time percent used by the matching process(es).</td>
<td>Percentage (%)</td>
</tr>
<tr>
<td>WorkingSet (Windows only)</td>
<td>Displays the working set size of the matching process(es).</td>
<td>Megabytes</td>
</tr>
<tr>
<td>PageFileBytes (Windows only)</td>
<td>Displays the page file size used by the matching process(es).</td>
<td>Megabytes</td>
</tr>
<tr>
<td>PrivateBytes (Windows only)</td>
<td>Displays the amount of memory that has been allocated by matching processes and that cannot be shared with others.</td>
<td>Megabytes</td>
</tr>
<tr>
<td>VirtualBytes</td>
<td>Displays the virtual memory used by the matching process(es).</td>
<td>Megabytes</td>
</tr>
<tr>
<td>Status (UNIX/Linux only)</td>
<td>Status of the process as per selected Status Interpretation.</td>
<td>{0 = OK ; 1 = Suspicious ; 2 = Failed}</td>
</tr>
<tr>
<td>PageFaultsPerSec (Windows only)</td>
<td>Displays the number of page faults per second caused by the matching process(es).</td>
<td>Page fault/sec</td>
</tr>
<tr>
<td>HandleCount (Windows only)</td>
<td>Displays the number of handles opened by the matching process(es).</td>
<td>Handles</td>
</tr>
<tr>
<td>ThreadCount (Windows only)</td>
<td>Displays the number of threads of the matching process(es).</td>
<td>Threads</td>
</tr>
</tbody>
</table>

Check the **Include child processes** box if you want to include all child processes associated to the defined main process.

When several processes match the entered criteria, the selected parameters will be valued in the PATROL Console (under the single process icon) by summing up the value of the parameters for each matching process.

**Status Interpretation (UNIX/Linux)**

If you have previously selected the **Status** parameter, the below wizard appears to let you define the status interpretation.
3. Specifying the Monitors Used

For each of the process status, select the value of the **Status** parameter: **OK**, **Suspicious** or **Failed**. By default, the overall process status will be interpreted as shown in the table below:

<table>
<thead>
<tr>
<th>Process Status</th>
<th>Interpreted Parameter Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running</td>
<td>OK</td>
</tr>
<tr>
<td>Sleeping</td>
<td>OK</td>
</tr>
<tr>
<td>Queued</td>
<td>OK</td>
</tr>
<tr>
<td>Waiting</td>
<td>OK</td>
</tr>
<tr>
<td>Intermediate</td>
<td>OK</td>
</tr>
<tr>
<td>Stopped</td>
<td>Suspicious</td>
</tr>
<tr>
<td>Growing</td>
<td>Suspicious</td>
</tr>
<tr>
<td>Unknown</td>
<td>Suspicious</td>
</tr>
<tr>
<td>Terminated</td>
<td>Failed</td>
</tr>
<tr>
<td>Not Running</td>
<td>Failed</td>
</tr>
</tbody>
</table>

⚠️ The ultimate status reflects the worst status of all selected processes. If the child processes are selected for inclusion, they will also influence the ultimate process status.
3. Configuring the Monitor Settings

An object is created in the PATROL Console for each configured element. This object is defined by a name and an internal identifier. These values, set by default by Monitoring Studio, can however be modified while configuring the element:

1. Modify the fields of your choice:
   - **Internal ID**: PATROL internal identifier of this monitored object.
   - **Display name**: Label that will be displayed in the PATROL Console for this monitoring object.
   - **What thresholds should be set on the newly created object?** Mode to be used to set alert thresholds:
     - **I want to use the default thresholds**: Uses the default thresholds set by Monitoring Studio
     - **I want to set custom thresholds**: Allows you to customize the thresholds for all parameters of the instance
     - **I want to use the default thresholds and customize them**: Sets the default Monitoring Studio thresholds on certain parameters and then allows you to customize any/all of them. This is mainly intended to help save time if you wish to customize the thresholds of just one of many parameters for the instance, and leave the default settings for the others.
     - **I do not want to set any thresholds for now**: No thresholds will be set on any parameter of the instance, and as a result no alerts will be triggered. Monitoring Studio will poll the object and return the output of the polling – but will not raise any alerts until you set thresholds.
3. Specifying the Monitors Used

If you select I want to use the default thresholds and customize them; on clicking Finish, the Set Thresholds panel will appear, certain parameters for the instance may appear with an asterisk symbol indicating that they already have thresholds. Thresholds can be set or modified at anytime by right-clicking on the instance > KM commands > Thresholds.

2. Click Finish.

4. Configuring the Process Cache Refreshing Frequency

Monitoring Studio relies on a cache mechanism to share the information among the Monitors in order to use as little resources as possible on the target Host and over the network. The cache will be refreshed if one of the Monitors needs to collect data (polling interval reached) and the cache is older than the selected minimum cache refresh.

All Process data on the selected Host are cached and shared by all Process Monitors defined on this Host. By default, the Process cache is refreshed minimum every 15 seconds. It is however possible to change this minimum cache refresh interval as described in the Setting the Polling Interval section.
Analyzing Command Lines

Even though Monitoring Studio KM for PATROL offers a variety of monitoring methods (Monitors), there might be an in-house script or command that you need to run and analyze on a regular basis to monitor a specific technology.

The Command Lines Monitor allows you to search for strings and numeric values in the returned output of the command and trigger alerts when the string/value is found or not found.

In addition, the Command Lines Monitor allows you to stop the command execution when it times out, to verify the status of the command execution by searching for a specific string.

Command line analysis objects are instances of the SEN_MS_COMMANDLINE application class.

To create a Command Line analysis:

1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select Command Line from the drop-down list and click Next.

3. **Credentials:** Select from the drop-down list the type of credentials that you want to use for the command line execution:
   - Agent’s Default Account: Uses the PATROL Agent credentials for localhost monitoring.
   - System Credentials (default): Uses the credentials previously specified when creating the Host.
3. Specifying the Monitors Used

- **Add new credentials...:** Lets you set new credentials for this specific monitoring.

4. Enter the command line to execute:
   - **Command line:** Enter the command line or the path to the script that Monitoring Studio will execute. You can use the following macros in the command line that will be executed:
     - `%{SEN_TIME:<date-time-format>}`
     - `%{SEN_LASTTIME:<date-time-format>}`
     - `%{SEN_SCRIPTPATH:<local-script-file-path>}`

   **Warning:** The `%{SEN_SCRIPTPATH}` macro should point to the script file path on the local Agent system.

   **Warning:** The `%{SEN_SCRIPTPATH}` macro does not support local environment variables (e.g., `%PATROL_HOME` %).

- **(local monitoring) Command launched once and runs continuously:** check this box if you want the command to only be launched once.
- **Click Next.**

5. If you chose to only launch the command once, the following dialog box will be displayed:

![Analyzing Command Lines - Confirmation Message](image-url)
Click Yes. The following dialog box is displayed:

- **(local monitoring|optional) Termination command line**: Enter a specific command to execute in order to stop the execution of the previously launched never-ending Command. This command runs when the command analysis is deleted from the PATROL configuration. It is required to properly end the execution of the command.
- **(local monitoring) Terminate at Agent restart**: Select this option if you wish the system to automatically stop the execution of the previous launched never-ending Command upon the next PATROL Agent restart.
- Click Next.
6. If you did not choose to only launch the command once, the following dialog box will be displayed:

![Command Execution Validation dialog box](image)

7. Set the following **Command Execution Validation** options:
   - **Timeout**: Enter the time in seconds after which the command will be stopped. The default is set to 30 seconds. If the timeout is reached, the value of the **Status** parameter will be set to 2 (Failed), indicating that the command failed to execute properly. No further analysis will be performed (String and Numeric Value searches).
   - **(local monitoring) optional** **Recovery Command**: Click this button to type a command similar to a recovery/cleaning action that will be executed when the timeout is reached. The {%SEN_PID} macro can be used to indicate the PID of command line process being interrupted.
- (optional) **Execution is validated when output contains**: The regular expression entered here will be searched in the output of the command. If it is not found, the value of the **Status** parameter will be set to 2 (Failed), indicating that the command failed to execute properly. No further analysis will be performed (String and Numeric Value searches).

- **Exit codes below mean the command execution**: Select an execution option (succeeded/failed), to state if the command line was properly executed or not, depending on the option selected. When one of the exit codes is or not found depending on the execution option selected, the **ExitStatus** parameter of the **Command Line** monitor is automatically set to 1 (Failed) indicating that the command failed to execute properly.

- (optional) **Exit codes separated by commas**: Enter one or several exit codes separated by commas. When one of the exit codes is found or not depending on the execution option selected above, the **ExitStatus** parameter will be set to 1.

- **Report execution errors in Group's CollectionErrorCount**: Select this option to have the **CollectionErrorCount** parameter of the Group reflect possible alerts triggered upon the Command Line execution. The **CollectionErrorCount** parameter of the Group reports on the collection errors of any Monitors, associated to the Group, for which this option is available and selected, providing a global view of the collection errors for the whole Group.

8. Click **Next**.
9. **Configure the Monitor settings**.
10. Click **Finish**.
Analyzing a Database Query

The **Database Query Analysis** tool executes SQL queries on the most popular database servers currently available on the market (Microsoft SQL, MySQL, Oracle and PostgreSQL) and monitors their return output within your PATROL environment. You can then run string or numeric value searches on the return output to monitor the result in myriad ways.

If the technology you wish to monitor uses a database server, you can test this database by sending applicative queries to the database server, or by testing the content of some critical data tables. As query results are stored by Monitoring Studio in a pipe-separated table format, it is easy to specify strings to be searched or numeric values to be extracted from a database query. Please refer to the **string search** and **numeric value extraction** sections for more information.

Database query analysis objects are instances of the **SEN_MS_DBQUERY** application class.

You can perform queries on the following databases:

- [Microsoft SQL Server](#)
- [MySQL Server](#)
- [Oracle Database Server](#)
- [Other Database](#)
- [PostgreSQL](#)
Performing a Query on a Microsoft SQL Server Database

This section details the various connection settings available for performing queries on Microsoft SQL database server.

To configure a connection to a Microsoft SQL database server:
1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select Database Query: Microsoft SQL Server from the drop-down list and click Next.

3. Define the Connection Information to the Microsoft SQL database server:
   - **Instance name**: Specify the SQL server instance name if there are several SQL Server instances installed. Leave “default” if there is a single instance.
   - **Port number**: Enter the port to be used to access the Microsoft SQL database. By default, the port 1433 is used.
   - **SSL Encryption**: Check this box to enable the encryption based on the SSL (Secure Sockets Layer) protocol. SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely.

⚠ These settings apply to all Microsoft SQL Server connections defined for the host.
4. Click **Next**.
5. Define the **Query Information** to the Microsoft SQL database server:

   - **Credentials**: Select from the drop-down list the type of credentials that you want to use:
     - **System Credentials (default)**: Uses the credentials previously specified when creating the Host.
     - **Add new credentials...**: Lets you set new specific credentials.
   - **Authentication**: Select from the drop-down list the Authentication mode that you want to use:
     - **Windows Authentication**: if you wish to connect to the database through a Windows user account. In that case, SQL Server validates the account name and password using the Windows identity validation (trusted connection).
     - **SQL Server Authentication**: if you wish to connect to the database with a specified login name and password from a non-trusted connection. In that case, SQL Server performs the authentication itself by checking if a SQL Server login account has been set up and if the specified password matches the one previously recorded. If SQL Server does not have a login account set, authentication fails and you get an error message.
   - **Database name**: Enter the name of the database. (Default: master)
   - **SQL Query**: Enter the SQL query you wish to perform.
   - **Timeout**: Specify the time in seconds after which the query will be stopped. Default is 30 seconds. If the query times out, the **Status** parameter will be set to 2 (Failed) and an alarm will be triggered.
   - **Report execution errors in Group's CollectionErrorCount**: Select this option to have the **CollectionErrorCount** parameter of the Group reflect possible alerts triggered upon the query execution. The **CollectionErrorCount** parameter of the Group reports on the collection errors of any monitors, associated to the group, for which this option is available and selected, providing a global view of the collection errors for the whole Group.

6. Click **Next**.
7. **Configure the Monitor settings**.
8. Click **Finish**. The corresponding object is created in the PATROL interface.
Performing a Query on a MySQL Server Database

This section details the various connection settings available for performing queries on MySQL database server.

To configure a connection to a MySQL server database:
1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select Database Query: MySQL Server from the drop-down list and click Next.

3. Define the Connection Information to the MySQL database server:
   - **Database name**: Enter the name of the database.
   - **Port number**: Enter the port to be used to access the MySQL database. By default, the port 3306 is used.

   !> These settings apply to all MySQL Server connections defined on the host.
4. Click **Next**.

![New Database Query for Host 1](image)

5. Define the **Query Information** to the MySQL database server:
   - **Credentials**: Select from the drop-down list the type of credentials that you want to use:
     - **System Credentials (default)**: Uses the credentials previously specified when creating the Host.
     - **Add new credentials...**: Lets you set new specific credentials.
   - **SQL Query**: Enter the SQL query you wish to perform.
   - **Timeout**: Specify the time in seconds after which the query will be stopped. Default is 30 seconds. If the query times out, the **Status** parameter will be set to 2 (Failed) and an alarm will be triggered.
   - **Report execution errors in Group’s CollectionErrorCount**: Select this option to have the **CollectionErrorCount** parameter of the Group reflect possible alerts triggered upon the query execution. The **CollectionErrorCount** parameter of the Group reports on the collection errors of any monitors, associated to the group, for which this option is available and selected, providing a global view of the collection errors for the whole Group.

6. Click **Next**.

7. **Configure the Monitor settings**.

8. Click **Finish**. The corresponding object is created in the PATROL interface.
Performing a Query on an Oracle Database Server

This section details the various connection settings available for performing queries on Oracle database server.

To configure a connection to a Oracle database server:
1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select Database Query: Oracle Database Server from the drop-down list and click Next.

3. Define the Connection Information to the Oracle database server:
   - **Database name**: Enter the name of the database.
   - **Port number**: Enter the port to be used to access the Oracle database. By default, the port 1521 is used.

   *These settings apply to all Oracle Database Server connections defined for the host.*
4. Click **Next**.

5. Define the **Query Information** to the Oracle database server:
   - **Credentials**: Select from the drop-down list the type of credentials that you want to use:
     - **System Credentials (default)**: Uses the credentials previously specified when creating the Host.
     - **Add new credentials...**: Lets you set new specific credentials.
   - **SQL Query**: Enter the SQL query you wish to perform.
   - **Timeout**: Specify the time in seconds after which the query will be stopped. Default is 30 seconds. If the query times out, the **Status** parameter will be set to 2 (Failed) and an alarm will be triggered.
   - **Report execution errors in Group’s CollectionErrorCount**: Select this option to have the CollectionErrorCount parameter of the Group reflect possible alerts triggered upon the query execution. The CollectionErrorCount parameter of the Group reports on the collection errors of any monitors, associated to the group, for which this option is available and selected, providing a global view of the collection errors for the whole Group.

6. Click **Next**.
7. **Configure the Monitor settings**.
8. Click **Finish**. The corresponding object is created in the PATROL interface.
Performing a Query on a PostgreSQL Database

This section details the various connection settings available for performing queries on PostgreSQL database server.

To configure a connection to a PostgreSQL database server:
1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select Database Query: PostgreSQL from the drop-down list and click Next.

3. Define the Connection Information to the PostgreSQL database server:
   - Database name: Enter the name of the database.
   - Port number: Enter the port to be used to access the PostgreSQL database. By default, the port 5432 is used.

   These settings apply to all PostgreSQL connections defined on pc-cpwin7.
4. Click **Next**.

5. Define the **Query Information** to the PostgreSQL database server:
   - **Credentials**: Select from the drop-down list the type of credentials that you want to use:
     - **System Credentials (default)**: Uses the credentials previously specified when creating the Host.
     - **Add new credentials...**: Lets you set new specific credentials.
   - **SQL Query**: Enter the SQL query you wish to perform.
   - **Timeout**: Specify the time in seconds after which the query will be stopped. Default is 30 seconds. If the query times out, the **Status** parameter will be set to 2 (Failed) and an alarm will be triggered.
   - **Report execution errors in Group’s CollectionErrorCount**: Select this option to have the `CollectionErrorCount` parameter of the Group reflect possible alerts triggered upon the query execution. The `CollectionErrorCount` parameter of the Group reports on the collection errors of any monitors, associated to the group, for which this option is available and selected, providing a global view of the collection errors for the whole Group.

6. Click **Next**.
7. **Configure the Monitor settings**.
8. Click **Finish**. The corresponding object is created in the PATROL interface.
Performing a Query on any Other Database

This section details the various connection settings available for performing queries on database servers other than MS SQL, MySQL, Oracle or PostgreSQL.

To configure a connection to any other database server:
1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select Database Query: Other (ODBC only) from the drop-down list and click Next.

3. **Connection String specifying the way to the database**: Enter the connection string that includes attributes such as the name of the driver, server, database and security information (username and password). In computing, a connection string is a string that specifies information about a data source and the means of connecting to it. It is passed in code to an underlying driver or provider in order to initiate the connection.

   ! These settings apply to all Other (ODBC only) connections defined on the host.
Example

String = Driver={MySQL ODBC 3.51 Driver};Server=myserver;Database=mydatabase;User=user;Password=%{SEN_PASSWORD};Option=3;
Password = *********

4. Click Next.

5. Define the Query Information to the Other (ODBC only) database server:
   - Credentials: Select from the drop-down list the type of credentials that you want to use:
     - System Credentials (default): Uses the credentials previously specified when creating the Host.
     - Add new credentials...: Lets you set new specific credentials.
   - SQL Query: Enter the SQL query you wish to perform.
   - Timeout: Specify the time in seconds after which the query will be stopped. Default is 30 seconds. If the query times out, the Status parameter will be set to 2 (Failed) and an alarm will be triggered.
   - Report execution errors in Group's CollectionErrorCount: Select this option to have the CollectionErrorCount parameter of the Group reflect possible alerts triggered upon the query execution. The CollectionErrorCount parameter of the Group reports on the collection errors of any monitors, associated to the group, for which this option is available and selected, providing a global view of the collection errors for the whole Group.

6. Click Next.
7. Configure the Monitor settings.
8. Click Finish. The corresponding object is created in the PATROL interface.
Monitoring Files

The File Monitoring tool is designed to monitor the presence, content, growth and change of a specific file. Therefore, the solution is able to instantly detect and alert when a critical file goes missing, if the file size is growing too fast, for example. It is one of the most important monitoring tools offered by Monitoring Studio KM for PATROL as a lot of technologies deal with files and many of them are critical. The most typical usage of file monitoring is parsing a log file. Most technologies use log files to trace their operations and notify operators when failures occur.

Selecting the right file type to monitor (flat or log) is essential to allow Monitoring Studio to read the monitored file correctly. Note that searching strings in flat or log files is also performed slightly differently, depending on the file type. Flat files are entirely updated and therefore need to be parsed entirely, as opposed to log files where new lines are appended at the end of the file - and hence only these new lines need to be analyzed.

To monitor a File:
1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select File from the drop-down list and click Next.
3. Specify the type of file that you wish to monitor:
   - Log file: if you only want the new lines to be parsed when searching for strings or numeric values.
   - Flat file: If you want the entire file to be parsed when searching for strings or numeric values.
4. Click **Next**. The following dialog box is displayed:

![Image of the dialog box](image.png)

5. **Credentials**: Select from the drop-down list the type of credentials that you want to use for file monitoring:
   - **Agent's Default Account**: Uses the PATROL Agent credentials for localhost monitoring.
   - **System Credentials (default)**: Uses the credentials previously specified when creating the Host.
   - **Add new credentials...**: Lets you set new credentials for this specific monitoring.

6. Identify the file to monitor:
   - **Filename**: Indicate the path and name of the file to be monitored. You can use:
     - the * wildcard to replace one character; the ? wildcard to replace one or more characters.
     - Example: C:\Program Files\MyTechnology\*.log

     *In case, multiple files match the file mask, Monitoring Studio will monitor the most recent file matching this mask.*

     - a date/time format to dynamically assign the current date or time in the file name. Simply insert the following string in the "Filename" field, where the date/time format appears, replacing the three dots by date format symbols: %SEN_TIME:...). For the complete list of format symbols, meaning and some examples, please see [Format Symbols]. Example: %SEN_TIME:%Y-%m-%d %H:%M:%S*
7. Select the parameters you want to monitor. See `SEN_MS_FILE` for parameter details.

![Parameters to Monitor](image)

8. Click **Next**.
9. **Configure the Monitor settings**.
10. Click **Finish**. The most recent file found by Monitoring Studio is now monitored. You can now:
    - **Perform a string search**
    - **Extract numeric values**.

**To Restart the Scan of Log Files:**

When looking for strings or numbers in a log file, the file content is scanned as new content is added. This means that the information that is in the file is only scanned once and then skipped over by the next polling. This option offers the possibility to restart the scanning from the beginning of the file. To do so:

1. Right-click the **Log File > KM commands > Restart Scan**
2. A message asks for confirmation.
3. Click the **Yes** button to proceed. At the next polling, the entire file will be scanned.

⚠️ Once this option has been selected and confirmed, it cannot be canceled.
Monitoring a File System

Because file systems (or Windows logical disks) are often a critical resource for technologies, Monitoring Studio provides a File System Monitoring tool to rapidly identify which technologies are impacted when a file system is full.

To monitor a File System:
1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select File System from the drop-down list and click Next.
3. Specify how you want to select the file system to monitor:
   - Select the file system from current file system list
   - Enter the file system path
4. Select the file system you wish to monitor or enter the file system path and click **Next**.

![File System Selection](image)

5. **Configure the Monitor settings**.
6. Click **Finish**. The corresponding object is created in the PATROL interface.

### Configuring the File System Cache Refreshing Frequency

Monitoring Studio relies on a **cache mechanism** to share the information among the Monitors in order to use as little resources as possible on the target Host and over the network. The cache will be refreshed if one of the Monitors needs to collect data (polling interval reached) and the cache is older than the selected minimum cache refresh.

All File System usage data on the selected Host are cached and shared by all File System Monitors defined on this Host. By default, the File System cache is refreshed minimum every 15 seconds. It is however possible to change this **minimum cache refresh interval** as described in the [Setting the Polling Interval](#) section.
Monitoring Folders

Since folders/directories are critical elements for a technology, checking their content is a good way to monitor the technology’s health. The **Folder Monitoring** tool monitors folders (directories) that store files processed by the technology. It measures their size, growth and flow (including how many files moved in, how many moved out, etc.).

This feature allows you to:

- Ensure that your technology is not overloaded (number of files to be processed, e.g.)
- Measure the technology activity (how many removed files, that is, how many have been processed)
- Check the age of the newest file (whether the data is coming in properly...)
- Check the age of the oldest file (whether the technology is running late in processing queued files).

*Folder monitoring may be time-consuming for large size folders. Therefore, Monitoring Studio will automatically reduce its monitoring features when the monitored folder contains more than 1000 files. To change this limit, set the configuration variable `/SENTRY/STUDIO/<hostID>/folderLimit` to a suitable value.*

Folder monitoring objects are instances of the **SEN_MS_FOLDER** application class.

To monitor a Folder:

1. In the PATROL Console, right-click the **Host** or **Monitor Group** icons and select **KM Commands > New > Monitor...**
2. Select **Folder** from the drop-down list and click **Next**.
3. **Credentials:** Select from the drop-down list the type of credentials that you want to use for folder monitoring:
   - **Agent’s Default Account:** Uses the PATROL Agent credentials for localhost monitoring.
   - **System Credentials (default):** Uses the credentials previously specified when creating the Host.
   - **Add new credentials...:** Lets you set new credentials for this specific monitoring.
4. Identify the folder to be monitored:
   - **Folder name and path:** Enter the name and path of the folder (directory) to be monitored. You can use a a date/time format to dynamically assign the current date or time in the file name. Simply insert the following string in the “Filename” field, where the date/time format appears, replacing the three dots by date format symbols: `%{SEN_TIME:...}`. For the complete list of format symbols, meaning and some examples, please see [Format Symbols](#).
   - **Include sub-folders:** Check this box to monitor all the sub-folders of the above-specified folder.
   - **(optional) Monitor only files matching the mask below:** Specify the file types or enter...
masks, and only these files will be monitored (e.g.: .txt; myFiles?.log; file.* ). You can use wildcards such as "*" to replace any number of characters, or "?" to replace just one character. You may also use several masks separated by ";". Monitoring Studio will only take into account the files matching the masks entered.

- Click **Next**.
5. Select the parameters to be monitored for this folder. See the $SEN_MS_FOLDER$ application class for parameter details.

![Parameters to Monitor](image)

6. Click **Next**.
7. **Configure the Monitor settings**.
8. Click **Finish**. The corresponding object is created in the PATROL interface.
Monitoring a Loaded KM

Monitoring Studio can monitor all the KMs that are loaded in your PATROL Console, extract their parameters' values, compute them with a mathematical formula and use the value returned to perform additional operations, such as converting units, perform correlation, etc.

The objects created are instances of the `SEN_MS_FORMULA` class.

To create a Multi-Parameter Formula:
1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select Multi-Parameter Formula from the drop-down list and click Next.
3. Specify the parameters to be monitored:
   - In the list of parameters currently available on the Agent, select the parameters required. The maximum number supported by Monitoring Studio KM is 26.

   - **Off-line parameters and parameters with no values (like collectors) are displayed as "OFFLINE" in the list. It is recommended not to select these parameters as they will not have any value.**

   - (Optional) Check the Use the objects display name to build the PATROL IDs box to allow the use of label instances instead of PATROL IDs to determine a parameter’s path. This option may be particularly useful when an object ID is unknown.

   - Click Next.
4. Define the formula to apply to the monitored parameter(s):
   - **Formula**: Enter the formula you wish to apply to the parameter(s). The parameters are identified by a letter listed in the dialog box. Use the letter preceding the parameter name and the standard mathematical symbols to do so, such as: + - / * ( ).
   - **Do not collect if one or more parameter has no value**: Select this option if you wish to skip the collect when one or more parameters is not populated yet (usually after a PATROL Agent restart).
   - Click **Next**.
5. **Configure the Monitor settings.**
6. Click **Finish** to start monitoring the selected parameters. A new object is automatically created under the Group icon in the PATROL Console.
Monitoring SNMP Agents & Traps

Because many technologies rely on middleware instrumented with SNMP agents and use SNMP traps to provide information about their state, polling SNMP agents and listening for SNMP traps are a good method to ensure that your technologies are running properly.

Polling SNMP Agents

The SNMP Polling Monitor is designed to poll the SNMP agent and retrieve the values of a given OID (object identifier), or the values of an SNMP table, thereby enabling administrators to easily identify the source of the problem or just be informed of the status of the monitored device/attribute.

Many technologies rely on middleware instrumented with SNMP (Simple Network Management Protocol) agents, which contain managed objects that provide information related to the current state of its operation. These objects are arranged in a Management Information Base (MIB). SNMP is an Application Layer protocol that allows external tools to communicate with the agent and read the values of the objects.

To create an SNMP polling:

1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select SNMP Polling from the drop-down list and click Next.

⚠️ If SNMP is deactivated on the PATROL Agent, a warning message is displayed, inviting you to activate it using the following configuration variable: /snmp/support. Besides, Monitoring Studio will trigger an alert on the CollectionErrorCount parameter under the Monitoring Studio icon if SNMP is disabled in the configuration and one or several SNMP monitors have been created.
3. Specifying the Monitors Used

3. Specifying the Monitors Used

3. Specifying the Monitors Used

3. Specifying the Monitors Used

3. Specifying the Monitors Used

Polling SNMP Agents - Welcome Page

3. Select the type of value you want to poll:
   - **A single value from one OID**: Select this option to poll a value from one OID.
   - **Multiple values from rows of an SNMP table**: Select this option to poll several values from an SNMP table.
   - Click Next.

4. If you selected **A single value from one OID**, the following dialog box is displayed:
A reminder of the Community and Port number configured at the host level is displayed at the top of the dialog box.

- **OID to poll**: Enter the OID (object identifier) to poll, as given by the Management Information Base (MIB).
- **Report execution errors in Group’s CollectionErrorCount**: Select this option to have the CollectionErrorCount parameter of the Group reflect possible alerts triggered upon the SNMP monitoring execution. The CollectionErrorCount parameter of the Group reports on the collection errors of any monitors, associated to the group, for which this option is available and selected, providing a global view of the collection errors for the whole Group.
- **Click Next**.

Monitoring Studio will try to poll the OID to identify its type. This will determine which parameters are activated: "Content" for strings, "Value" for numbers. If, for some reason, the OID cannot be polled, a warning message is displayed and invites you to select an OID type, either “string” or “number,” to let Monitoring Studio know what kind of value is expected. If you are not sure about:

- the OID type, it is recommended to select “The OID content is a string.”
- the exact OID to poll, you should use a SNMP MIB Browser tool to identify which OID corresponds to which variable. You can also use the Monitoring Studio built-in SNMP Browser tool to list the available OID variables and their values. To do so, right-click the main Monitoring Studio icon > KM Commands > Tools > **SNMP Browser**.

If the OID returns a number, select the parameters you wish to collect:
- **Delta**: Calculates the difference between values collected during two consecutive polling.
- **Delta per second/minute/hour**: Reports the value resulting of the division of the Delta.
by the number of seconds/minutes/hours elapsed between the collection times.

- **Raw Value**: Reports the actual value collected upon data polling.
- **Discard negative Delta values**: Select this option if you do not want negative values to be reported on the graph.
- **Rescaling**: Use this option to configure Monitoring Studio to rescale the value that is being extracted in order to have a more readable graph in the PATROL Console. The available rescaling options are:
  - **No rescaling**
  - **Divide the value by** a value that then gives you the reading in terms best suited to you
  - **Multiply the extracted value by** a constant factor

This can be useful if you extract numeric values in bytes but prefer to show a graph in megabytes. In such a case, you would divide the values by 1048576 (1024*1024).

- Click **Next**.

5. If you selected **Multiple values from rows of an SNMP table**, the following dialog box is displayed:

![SNMP Polling Dialog Box](image)

A reminder of the Community and Port number configured at the host level is displayed at the top of the dialog box.

- **SNMP Table OID**: Enter the Table OID (object identifier) to poll, as given by the Management Information Base (MIB).
- **Columns to retrieve, separated by commas**: Enter the column numbers whose values should be retrieved. Enter "ID" to retrieve the row identifier. Leave the field blank to retrieve values from the entire row. Enter "ID" to retrieve the row identifier.

- Click **Next**.
If for some reason, the OID cannot be polled, a message is displayed stating that the table seems to be empty. In such a case, verify that you have entered the right OID and/or that the table really exists and has values.

6. **Configure the Monitor settings.**
7. Click **Finish**.

Monitoring Studio will get the value and allow you to store it in a graph, or search for strings in the OID content. For more details about the parameters discovered, please refer to the **Reference Guide**. SNMP Polling objects are instances of the **SEN_MS_SNMPPolling** class.
Listening for SNMP Traps

The SNMP Trap Listening tool monitors and listens for SNMP traps and enables rapid recovery actions depending on the traps received, thereby ensuring optimal functioning of applications or devices that send SNMP traps.

SNMP Trap listening objects are instances of the SEN_MS_SNMPTRAP application class.

⚠️ The SNMP Agent emitting the traps should be configured to send them to the PATROL Agent where Monitoring Studio is installed and running, otherwise, Monitoring Studio will not be able to receive the SNMP trap and will only listen for the SNMP traps on the localhost. No other Trap Listener should be running at the same time.

To listen to SNMP Traps:
1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select SNMP Trap from the drop-down list and click Next.

⚠️ If SNMP is deactivated on the PATROL Agent, a warning message is displayed, inviting you to activate it using the following configuration variable: /snmp/support. Besides, Monitoring Studio will trigger an alert on the CollectionErrorCount parameter under the Monitoring Studio icon if SNMP is disabled in the configuration and one or several SNMP monitors have been created.

3. Identify the traps to listen to:
   - **Enterprise OID**: Enterprise OID of the SNMP Trap. You can use regular expressions. Example: 1.3.6.1.4.44.141.32.*
- **(optional) Trap numbers**: Enter the number identifying the SNMP Trap.
- **Optional Varbinds**: Click this button to configure the Varbinds settings. A Varbind or Variable Binding is a sequence of two specific fields. The first field is an OID, which addresses a specific parameter. The second field contains the Value of the specified parameter.

![Listening for SNMP Traps - Varbinds settings](image)

- **OID 1 & 2**: First and second attached variables OID that should be contained within the SNMP trap. You can also enter the text that should be found (or not) within the OID content.
- **Case sensitive**: Indicates whether or not the search will be case sensitive.
- **Click Accept**.

All these pieces of information define the SNMP Trap that is expected. Monitoring Studio will react to the SNMP Trap received only if this information is found within the SNMP Trap. All other SNMP Traps will be ignored.

⚠️ **If you are unsure about the characteristics of the SNMP trap you want to detect, you will need to use a SNMP MIB Browser tool to understand the exact meaning of each trap. You can also use the Monitoring Studio built-in SNMP trap listener tool to view in real-time the SNMP traps and their characteristics that are received by the PATROL Agent. Right-click on the main Monitoring Studio icon > KM commands > Tools > Real-time SNMP Trap Listener.**

⚠️ **The SNMP trap listening port is actually a PATROL Agent configuration variable: /snmp/trap_port=162. You can set this variable to whatever port you want Monitoring Studio to listen on.**

⚠️ **Make sure that only one device is listening for traps on the localhost or Monitoring Studio will not be able to run the SNMP Trap listener.**
4. Click **Next**.

5. Set the automatic acknowledgment:
   - **Acknowledge alert if the following SNMP Trap is received**: Check this box if you wish to acknowledge an alert when the SNMP trap received matches the criteria set.
   - **Trap number**: Enter the trap number that will acknowledge the alerts triggered by the specified trap.
   - **Varbinds**: Click this button to configure the first and second attached variables OID that should be contained within the SNMP trap to acknowledge a matching trap received.
   - **Acknowledge alert after**: Check this box if you wish to automatically acknowledge a matching SNMP trap and then specify the time in seconds after which the matching SNMP Trap received will be acknowledged. Default is 120 minutes.
   - Choose the action to be taken when acknowledging: **Reset MatchingTrapCount**, i.e. clear all previous alerts or **Decrease MatchingTrapCount by one**; i.e. clear the previous alert.

6. Click **Next**.
7. **Configure the Monitor settings**.
8. Click **Finish**.
Analyzing Web Requests

The **Web Request Analysis** tool monitors your web-based technologies, sends Web requests, posts forms, parse the HTML page that is returned, etc. to ensure that end-users actually see what they should see on their browser.

**Web Request** analysis objects are instances of the **SEN_MS_WEBREQUEST** application class.

**To create a Web Request analysis:**
1. In the PATROL Console, right-click the **Host or Monitor Group icons** and select **KM Commands > New > Monitor...**
2. Select **Web Request** from the drop-down list and click **Next**.
3. Enter the URL of the web site that needs to be monitored.

⚠️ From a Windows agent, it is possible to poll a secure web site by using the "https" method. From a UNIX agent, this action is not possible.

4. Check the Webform HTML source to known which method needs to be used (GET, POST, or POST Web Service).
5. **HTTP request type:** Select the method to be used:
   - The "GET" mode (HTTP GET method) is the standard way to query a Web page from a Web server.
   - The "POST" mode (HTTP POST method) is classically used to post a form to a Web server and obtain the result of the processing of the form data. If you choose this mode you need
3. Specifying the Monitors Used

Monitoring Studio KM for PATROL 9.0.00

to specify which variables with what values must be passed to the Web server.

- The "POST (Web Service)" mode is used to query a web service (SOAP, REST, etc.). If you choose this mode you need to specify the content-type, header and body that must be passed to the Web server.

You must check the Web form HTML source to know which method needs to be used (GET, POST or POST Web Service).

⚠️ Some Web forms can be passed to the server with the HTTP GET method. In this case, the form data goes through the URL (http://server/form.php?varA=valueA&varB=valueB&...)

⚠️ To post a form to a Web server, you need to enter the URL of the script/CGI/page that will actually process the data, which may be different from the Web page URL that shows the form itself. Again, you need to check the Web form HTML source to identify the URL to query.

⚠️ A Web form HTML source should contain a statement like the following one: <FORM METHOD="POST" ACTION="/urlToQuery.php">
6. **Timeout**: Specify the time in seconds after which the query will be stopped. Default is 30 seconds. If the request times out, the **Status** parameter will be set to 2 (Failed) and an alarm will be triggered.

7. Select what you would like to retrieve from the Web page returned by the Web server: the entire HTTP response; only the Web page (with HTML tags) or only the content text (no HTML tags).

8. **(Optional) Advanced Options**: Click this button to enter the Proxy settings and HTTP Authentication information.

   - **Proxy settings**: Enter the **Proxy Hostname** and **Port number** required to execute the web request if your environment uses a proxy server.
   - **HTTP Authentication**: Select how you want to enter the credentials required by the HTTP server:
     - No authentication
     - System Credentials
     - Add new credentials...

   You can refer to the section on [HTTP authentication](#) for more details.
3. Specifying the Monitors Used

- Click **Accept**.
- **9.** Click **Next**.

If you previously selected the "POST" request type

![Image of POST variables definition page](image-url)
10. Enter the variable(s) name and value and click **Next**.

**If you previously selected the "POST (Web Service)" request type**

![Post to a Web Service](image)

11. Provide the following information:
   - **Content-Type**: defines the MIME type for the message and the character encoding used for the XML body of the request.
   - **Header (optional)**: contains application-specific information (like authentication, payment, etc) about the Web Service message.
   - The body of the Web Service request, or the path to the file containing the body of the request. If a file is provided, the Monitoring Studio discovery will read the file on the localhost and use its content as the Web service body.

**Example:**

```xml
<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">
  <soap:Body xmlns:m="http://www.example.org/stock">
    <m:GetStockPrice>
      <m:StockName>IBM</m:StockName>
    </m:GetStockPrice>
  </soap:Body>
</soap:Envelope>
```
- Click **Next**.
12. **Configure the Monitor settings.**
13. Click **Finish**.
Monitoring Windows Event Logs

The Windows Event Monitoring tool monitors events posted by your technology to consolidate the monitoring under a single icon. You will therefore not have to additionally look up in the Windows Event Log. It also enables you to define automatic acknowledgment of previously triggered alerts by specifying the Windows event that will acknowledge the alert.

Windows Event monitoring objects are instances of the `SEN_MS_WINEVENT` application class.

*Windows Events on Windows 2003 systems can only be monitored locally.*

To monitor a Windows Event:

1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select Windows Event from the drop-down list and click Next to retrieve all the available Windows event logs from your local or remote system.
3. Select the Windows Event log that you want to monitor from the Event log drop-down menu and click Next.

Monitoring Windows Events — Provider Selection

4. All available providers are listed in the Provider drop-down menu. Select one and click Next.

Monitoring Windows Events — Event Settings

Note: IDs must be comma delimited. Range of IDs must be hyphen delimited. Example: 4372,4375,4380-4385
5. (Optional) Define the **Event Settings**:
   - **Event level**: Select the event level(s) to monitor (Critical, Error, Warning, Information)
   - **Count events with these events IDs**: Enter the ID(s) of the event(s) to be considered for alerting.
   - **But exclude these event IDs**: Enter the ID(s) of the event(s) to be excluded from alerting.

   *Use a comma (,) to separate several IDs or a hyphen (-) between start and end values to indicate a range. Example: 4372,4375,4380-4385*

   *If you are unsure about the characteristics of the Windows event you want to detect, you will need to use the Monitoring Studio built-in Windows Event Log Reader tool to view content of the Event Logs and the characteristics of the events. Right-click a Host icon > KM commands > Tools > **Windows Event Log Reader**.*

6. Click **Next**.

7. (Optional) Define the **Acknowledgment Rule**:
   - **Acknowledge alert after**: Check this box and then specify the time in seconds after which the alerts will be acknowledged. Default is 120 minutes.
   - **Acknowledge on these event IDs**: Enter the ID(s) of the event(s) that you wish to acknowledge on. Use a comma (,) to separate several IDs or a hyphen (-) between start and end values to indicate a range.
   - **When acknowledging**: Choose between **resetting the MatchingEventCount** parameter, i.e. clear all previous alerts or simply **decreasing it by one**; i.e. clear the previous alert.
8. Click **Next**.
9. **Configure the Monitor settings**.
10. Click **Finish**.

**Configuring the Windows Event Cache Refreshing Frequency**

Monitoring Studio relies on a **cache mechanism** to share the information among the Monitors in order to use as little resources as possible on the target Host and over the network. The cache will be refreshed if one of the Monitors needs to collect data (polling interval reached) and the cache is older than the selected minimum cache refresh.

All Windows Event data on the selected Host are cached and shared by all Windows Event Monitors defined on this host. By default, the Windows Event cache is refreshed minimum every 15 seconds. It is however possible to change this **minimum cache refresh interval** as described in the **Setting the Polling Interval** section.
Monitoring Windows Performance Counters

The Windows Performance Monitoring tool is designed to monitor any commercial Windows-based technology or any custom technology relying on a Windows-based middleware which is instrumented through Windows Performance Counters.

The Performance Counter Monitor collects information about objects on your Windows systems and measures them. These objects can be processors, threads, processes, memory, etc., with each one having an associate set of counters and possibly instances. The data gathered by the Windows performance about specific components can be used to identify problems and bottlenecks within your technology and plan ahead for your future needs.

The Windows Performance Monitoring tool brings Windows performance data, important to the proper functioning of your technology, within your BMC framework and automatically notifies administrators when a value breaches a specific threshold.

A Windows performance is defined by a performance object name and a counter name, as well as anything from none to several instances. Furthermore, each performance counter contains a unique set of counters and instances. Some objects are built into the system, typically corresponding to the major hardware components, but others will only be accessible if the associated software has been installed.

Here are some definitions of the items as described by Microsoft:

- **Performance object**: A logical collection of counters that is associated with a resource or service that can be monitored. The objects that are typically installed on a system are: cache, memory, paging file, physical disk, process, processor, server, system and thread.
- **Counter**: A value corresponding to a particular aspect of the performance defined for the performance object.
- **Instance**: A term used to distinguish between multiple performance objects of the same type on a computer.

Windows Performance counter monitoring objects are instances of the `SEN_MS_WINPERF` application class.
To monitor a Performance Counter:
1. In the PATROL Console, right-click the **Host** or **Monitor Group** icons and select **KM Commands > New > Monitor...**
2. Select **Performance Counter** from the drop-down list and click **Next**.

3. Select the **Windows Performance Object** that contains the counter and click **Next**.
4. Select the counter and instances:
   - **Instance name**: Select the **Windows Performance object** to be monitored.
   - **Performance counter**: Select the **counter** to be monitored.
   - (optional) **Rescaling**: A scale can be used to divide or multiply the Windows performance value by this number. To do so, enter the number you wish the value to be divided/multiplied by (Example: the committed memory is expressed in bytes, so, to obtain the value in mega-bytes (MB), type "1024" in the field for scale. By default, the scale value is 1 (no scale).

5. Click **Next**.
6. **Configure the Monitor settings**.
7. Click **Finish**.
Monitoring a Windows Service

Many software technologies that run on any Windows operating systems run as Windows services, running as background processes with no direct user interface and no logged-on user. Typically, they start automatically and are expected to stay running without any human intervention. When one of these critical services fails, many users and external services can immediately be affected. Therefore, making sure that these services are seamlessly running is a key requirement for most system administrators.

Windows Services objects are instances of the SEN_MS_WINSERVICE application class.

To monitor a Windows Service:

1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select Windows Service from the drop-down list and click Next.

Please note that the System Credentials entered at the host level will be used to retrieve Windows Service information.

You can:

- either select a service from the list
- or manually enter the service short name
To display the list of currently installed services:

3. Select **Select a service from the list of installed services** and click **Next**.
4. Select the service to be monitored and click **Next**.

![Windows Service Selection](image-url)

*Monitoring a Windows Service - Windows Service Selection*
To manually enter the short name of a service:

3. Select **Enter manually the short name of a service** and click **Next**.
4. Enter the Windows **service short name** to be monitored and click **Next**.
5. For each possible service state, you can select the value of the Status parameter: **OK**, **Suspicious** or **Failed**. By default, the Service will be interpreted as listed in the table below:

<table>
<thead>
<tr>
<th>Service State</th>
<th>Default Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running</td>
<td>0 (OK)</td>
</tr>
<tr>
<td>Paused</td>
<td>1 (Suspicious)</td>
</tr>
<tr>
<td>Stopped</td>
<td>2 (Failed)</td>
</tr>
<tr>
<td>Start Pending</td>
<td>1 (Suspicious)</td>
</tr>
<tr>
<td>Continue Pending</td>
<td>1 (Suspicious)</td>
</tr>
<tr>
<td>Pause Pending</td>
<td>1 (Suspicious)</td>
</tr>
<tr>
<td>Stop Pending</td>
<td>1 (Suspicious)</td>
</tr>
<tr>
<td>Not Installed</td>
<td>2 (Failed)</td>
</tr>
<tr>
<td>Unknown</td>
<td>1 (Suspicious)</td>
</tr>
</tbody>
</table>

6. **Configure the Monitor settings.**

7. Click Finish.
Analyzing WBEM Queries

WBEM (Web-Based Enterprise Management) is a set of systems management technologies developed to unify the management of distributed computing environments that provides users with information about the status of local or remote computer systems.

Monitoring Studio can execute WBEM queries on your system and consolidate them under a single icon within your PATROL environment along with the other Monitors of your technology. It can also query the WBEM repository for class and instance information.

WBEM query analysis objects are instances of the `SEN_MS_WBEMQUERY` application class.

To create a WBEM Query analysis:
1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select WBEM Query from the drop-down list and click Next.

![New WBEM Query for Host 1](image)

Managed System: PC-CPUIN7_3181

Credentials: System Credentials

Common WBEM Settings - pc-cpuin7

Port: 5989

Encrypt data using HTTPS

Namespace: root/cimv2

Timeout: 30 seconds

WBEM query:

Report execution errors in Group.i's CollectionEventStream

< Back  Next >  Help >>
3. Select from the drop-down list the type of **Credentials** that you want to use for the WBEM query:
   - **Agent's Default Account**: Uses the PATROL Agent credentials for localhost monitoring.
   - **System Credentials (default)**: Uses the credentials previously specified when creating the Host.
   - **Add new credentials...**: Lets you set new credentials for this specific monitoring.
4. Set the **Common WBEM Settings**:
   - **Port**: Enter the port number you wish to use for the connection. By default, in standard environments, the port 5988 is used for non-encrypted data, while port 5989 is used for encrypted data.
   - **Encrypt data using the HTTPS protocol**: Select this option to encrypt the query with the HTTPS protocol.
5. Provide the following WBEM Query Information:
   - **Namespace**: Enter the WBEM namespace. A namespace is a logical group of related classes representing a specific technology or area of management (Example: root/cimv2)
   - **Timeout**: Specify the time in seconds after which the query will be stopped. Default is 30 seconds. If the query times out, the **Status** parameter will be set to 2 (Failed) and an alarm will be triggered.
   - **WBEM query**: Enter your WBEM query (Example: SELECT DeviceID, Speed, Description, PermanentAddress, OperationalStatus FROM HPUX_EthernetPort).
   - **Report execution errors in Group’s CollectionErrorCount**: Select this option to have the **CollectionErrorCount** parameter of the Group reflect possible alerts triggered upon the query execution. The **CollectionErrorCount** parameter of the Group reports on the collection errors of any monitors, associated to the group, for which this option is available and selected, providing a global view of the collection errors for the whole Group.
6. Click **Next**.
7. **Configure the Monitor settings**.
8. Click **Finish**.

An icon representing the WBEM query appears in the console with three parameters: **ExecutionTime**, **Result**, and **Status**. You can now run **String Searches** and **Extract Numeric Values** from this output.
Analyzing WMI Queries

WMI (Windows Management Instrumentation) is the Microsoft implementation of WBEM (Web Based Enterprise Management) that provides users with information about the status of local or remote computer systems.

Monitoring Studio can execute WMI queries on your system and consolidate them within your PATROL environment along with the technology monitoring under a single icon. It can also query the WMI repository for class and instance information. You can for example query the WMI that returns all the objects representing shut-down events from your desktop system.

WMI query analysis objects are instances of the SEN_MS_WMIQUERY application class.

ℹ️ This function is only available to Windows hosts. It can be remotely used from PATROL Agents running on Windows only.

To create a WMI Query Analysis:

1. In the PATROL Console, right-click the Host or Monitor Group icons and select KM Commands > New > Monitor...
2. Select WMI Query from the drop-down list and click Next.

ℹ️ Please note that the System Credentials entered at the host level will be used to retrieve WMI Queries information.
3. Identify the host:
   - **Namespace**: Enter the WMI namespace. A namespace is a logical group of related classes representing a specific technology or area of management. Example: root\cimv2
   - **WQL Query**: Enter your query. (Example: SELECT DeviceID, Speed, Description, PermanentAddress, OperationalStatus FROM HPUX_EthernetPort). In case you need help to build your WMI query, you could download **WMI CIM Studio**, which is one of the WMI Administrative tools on the Microsoft site.

4. Provide the following WMI Query Information:
   - **Timeout**: Specify the time in seconds after which the query will be stopped. Default is 30 seconds. If the query times out, the **Status** parameter will be set to 2 (Failed) and an alarm will be triggered.
   - **Report execution errors in Group's CollectionErrorCount**: Select this option to have the **CollectionErrorCount** parameter of the Group reflect possible alerts triggered upon the query execution. The **CollectionErrorCount** parameter of the Group reports on the collection errors of any monitors, associated to the group, for which this option is available and selected, providing a global view of the collection errors for the whole Group.

5. Click **Next**.
6. **Configure the Monitor settings**.
7. Click **Finish**. An icon representing the WMI query appears in the console. You can now run **String Searches** and **Extract Numeric Values** from this output.
4. Specifying the Information to be Searched

Once you have specified and configured the Monitors to use, you need to define what should be searched for in the output information returned by the Monitors: strings and numeric values that should or not be present. Here is the usual procedure to be followed:

- **Pre-processing the Monitor Output**
- **Split the Monitor Output**
- **Analyze the Monitor Output:**
  - **Perform string searches**
  - **Extract numeric values**

The features described in this section are exclusively available for the following Monitors:

- [ ] Command Line (**SEN_MS_COMMANDLINE**)
- [ ] Database Query (**SEN_MS_DBQUERY**)
- [ ] Dynamic Instance (**SEN_MS_DYNAMIC**)
- [ ] File (**SEN_MS_FILE**)
- [ ] SNMP Polling (**SEN_MS_SNMPPOLLING**)
- [ ] Text Pre-Processing (**SEN_MS_TRANSFORM**)
- [ ] WBEM Query (**SEN_MS_WBEMQUERY**)
- [ ] Web Request (**SEN_MS_WEBREQUEST**)
- [ ] WMI Query (**SEN_MS_WMIQUERY**)
4.1 (Optional) Pre-processing the Monitor Output

Because **String** and **Numeric Value Extractions** cannot be run in paragraphs, you may need to first process the multi-line, XML, or HTML content by using the **Text Pre-Processing** tool. This tool transforms paragraphs into single lines for easy parsing with the **String Search** and **Numeric Values Extraction** tools.

All text pre-processing objects are instances of the **SEN_MS_TRANSFORM** application class.

**Example of converting multi-line records to single lines**

The "ipconfig /all" command under Windows reports various information about each network card, and each "paragraph" is about one network card:

The aim here is to detect any disconnected cards. So we add a monitoring instance for the command `ipconfig /all`. But as the text is in paragraphs, a direct string search will not get the desired result in this case – which is why we run the Text pre-processing tool to convert the multi-line text to single lines.

In the screenshot below, the "ipconfig /all" command is executed and its output is pre-processed to transform its paragraphs into single lines, which in turn enables an efficient parsing with a String search that looks for "disconnected" network cards.
To convert Multi-Line Records into single line:

1. In the PATROL Console, right-click the File Monitoring icon and select KM Commands > New > Text Pre-processing...
2. Select Convert multi-line records into single line and click Next.

3. Define the first and/or last lines of the paragraphs:
   - **This RegExp marks the beginning of a new record**: Enter the regular expression or string that marks the beginning of a new record. Please note that the regular expression can match with any part of the first line of each paragraph. If needed, include the first line in the result.
   - **This RegExp marks the end of a record**: Enter the regular expression or string that marks the end of a new record. Please note that the regular expression can match with any part of the first line of each paragraph. If needed, include the last line in the result.

⚠️ The regular expression `^$` can be used to match an empty line.

⚠️ You can specify a regular expression that only identifies the beginning of a new paragraph (record). In this case, Monitoring Studio skips the content until it finds a line matching with the specified criteria. The text that follows this line (and optionally including this first line) is concatenated in a single line by using the specified separator, until Monitoring Studio finds another line that matches with the specified regular expression. Each line in the original content that matches with this regular expression produces a new line in the result content. The same is true for the regular expression that marks the end of a paragraph (or record).
If you specify both regular expressions to identify the beginning and the end of a record, Monitoring Studio will only take into account the text content that is in between lines that matches these regular expressions (i.e. between the start line and the end line). Lines in the original text between a line matching the end marker and the next line matching the beginning marker will be skipped and not integrated in the text result.

- Specify the character to be used as a separator.

4. Click **Next**.
5. **Configure the Monitor settings**.
6. Click **Finish**. The output will be displayed at the next discovery by the **TransformResult** parameter.

You can now [perform a string search](#) or [extract numeric values](#) from this "transformed" output.

### To convert XML to CSV

1. In the PATROL Console, right-click the **File Monitoring** icon and select **KM Commands > New > Text Preprocessing...**
2. Select **Convert XML to CSV (Comma-Separated Values)** and click **Next**.
3. Define the XML tag that defines the record, sub-objects, and properties, the character to be used as a separator and click **Next**.

4. **Configure the Monitor settings.**

5. Click **Finish**. The output will be displayed at the next discovery by the **TransformResult** parameter.

You can now **perform a string search** or **extract numeric values** from this "transformed" output.
To extract Text from HTML

1. In the PATROL Console, right-click the File Monitoring icon and select KM Commands > New > Text Preprocessing...

2. Select Extract text from HTML (Comma-Separated Values) and click Next.
3. Click **Next**.

4. **Configure the Monitor settings.**

5. Click **Finish**. The output will be displayed at the next discovery by the **TransformResult** parameter.

You can now **perform a string search** or **extract numeric values** from this "transformed" output.

**To process Text through an External Command**

This option should be selected if text inputs (files, output of commands, Web requests, etc.) need to be transformed in a special way in order to be parsed with Monitoring Studio’s String Searches and Numeric Value Extractions. If the built-in text transformation features of Monitoring Studio cannot handle such "specially formatted" text, you will have to process the content through a custom script or utility that performs the required transformation. The main advantage of processing the text through an external command feature is that it enables you to customize the processing of almost any source of information important to your technology.
1. In the PATROL Console, right-click the File Monitoring icon and select KM Commands > New > Text Preprocessing...
2. Select Text processing through an external command and click Next.

   ![Text Pre-Processing Wizard](image)

3. Specify the command to be executed to transform the text:
   - **Command to be executed:** Enter the command to be executed on the localhost where your PATROL Agent is installed. The principle is very similar to the "pipe" mechanism of the UNIX shell except that the content is not passed directly but is stored in a temporary file and then the result needs to be stored in another temporary file. Hence the command line you specify needs to take the `%{INPUTFILE}` macro as an argument (the `%{INPUTFILE}` macro is replaced by the real temporary input file location at run time) as well as `%{OUTPUTFILE}`.

   - **This command is executed on the host where the PATROL Agent is installed, not on the target Host.**
   - **The output of the command must match this RegExp to be considered as successful:** Enter a RegExp to avoid typical path problems such as getting "... not found" error messages instead of the properly transformed text

   - **If your command line redirects its output to `%{OUTPUTFILE}`, the validation regular expression is likely to fail because the standard output is empty and thus matches with nothing. Use a validation regular expression only if your command line is able to produce both the `%{OUTPUTFILE}` and some text to its standard output.**

   - **Command lines are executed locally, therefore it is not possible to use the awk command when monitoring a UNIX/Linux system from Windows.**

   - **Click Next.**
4. **Configure the Monitor settings**.

5. Click **Finish**. The output will be displayed at the next discovery by the **TransformResult** parameter.

You can now perform a string search or extract numeric values from this "transformed" output.
4.2 Splitting the Monitor Output

The **Dynamic Object Builder** tool splits the return output of objects and applies a set of user-defined rules on this return output data.

Once the PATROL administrator has created a **Dynamic Object Builder** instance, Monitoring Studio:

- Applies the user-defined set of rules to the output data
- Extracts each matching line and creates a dynamic object for each of them in the PATROL Console according to the user-defined naming
- Groups all dynamic objects under a dynamic container to facilitate the management of all the dynamic objects.

Dynamic objects can be analyzed with **String Search** and **Numeric Value Extraction**. They are instances of the **SEN_MS_DYNAMIC** application class.

**To create a Dynamic Object:**

1. In the PATROL Console, right-click one of the following monitoring features:
   - Command Line Analysis
   - Database Query Analysis
   - File Monitoring and Analysis
   - SNMP Polling
   - Text Pre-Processing
   - WBEM Query Analysis
   - Web Request Analysis
   - WMI Query Analysis
2. Select KM Commands > New > Dynamic Object Builder...

![Dynamic Object Builder](image)

3. Define the rules to apply to the output data:

- **Keep only lines matching the regular expression below**: Specify the regular expression to be searched for by the Dynamic Object Builder. Each matching line is displayed in a separated Dynamic Item automatically added in the PATROL Console under the Dynamic Container icon. Non-matching lines are discarded. If nothing is specified, all lines are kept.

- **Exclude lines matching the regular expression below**: Specify the regular expression to be searched for by the Dynamic Object Builder. Each matching line will be ignored.

- Define if and how Monitoring Studio must trigger an alert when the Dynamic Item, containing the extracted line, is missing from one collect to another:
  - **Do not trigger any alert**: Select this option if you do not wish Monitoring Studio to trigger any alert when objects are missing
  - **Trigger an INFORMATION**: Select this option if you wish Monitoring Studio to trigger an Information alert when objects are missing
  - **Trigger a WARNING**: Select this option if you wish Monitoring Studio to trigger a Warning alert when objects are missing
  - **Trigger an ALARM**: Select this option if you wish Monitoring Studio to trigger an Alarm alert when objects are missing

If you have chosen to trigger an alert, a **Status** parameter will automatically be activated and displayed under the Dynamic Item in the PATROL Console to indicate that the Dynamic Item is missing. Click the **Status** parameter to open a graph pane displaying the status history of the Dynamic Item.

- **Delete missing objects**: Set this option according to how you want Monitoring Studio to delete missing objects in the console. The available options are:
  - **Never**: Monitoring Studio never deletes missing objects in the console. They will always
4. Specifying the Information to be Searched

- **As soon as they are missing**: Monitoring Studio deletes missing objects from the console as soon as their absence is discovered. If an alarm is configured, Monitoring Studio will trigger the alarm before deleting the object.
- **When they are missing... in a row**: Monitoring Studio deletes missing objects after they have been missing a specific number of times in a row.

4. Click **Next**.

5. Configure the **Dynamic Instances Monitor** settings templates:
   - **Internal ID Template**: PATROL internal identifier of the template.
   - **Display Name Template**: Label that will be displayed in the PATROL Console for this template. Indicate the column number in which the name of the object will be found by Monitoring Studio (e.g.: %{1} for the first column).

6. Since each object dynamically created by Monitoring Studio during the collect must have a different ID, you need to specify a column number in the returned line whose content will uniquely identify the instance:
   - **Col. Separators**: Click this button to define the way the **Dynamic Object Builder** detects columns of output data.
4. Specifying the Information to be Searched

- Select or de-select applicable separators. For custom separators, enter the character in the Other field.

- **Consecutive separators must be treated as a single one** (useful for data separated by blanks): Typically, it indicates that consecutive separators must be treated as a single separator.

- **Consecutive separators mean empty columns** (useful for data separated by blanks): Each separator is treated as an individual column separator and the column is considered empty.

- Click Accept.

7. Click Next.
8. Configure the Monitor settings.
9. Click Finish. The corresponding object is created in the PATROL interface.

String Search and Numeric Value Extraction can help you analyze the Dynamic Items output (the output of a command, a web page, the result of a SQL query, or WBEM query, etc.). In order to apply this feature to all the Dynamic Items in a single operation, the Dynamic Object Builder creates **Templates instances** of the feature. While the standard **Numeric Value Extraction** feature apply to a single return output, Templates apply to all the Dynamic Items' output within the Dynamic Container.
4.3 Analyzing the Monitor Output
Searching for a Specific String

The **String Search** tool allows you to run fast and powerful searches for strings on the Monitors that you previously configured (flat, or log files, output of a Web request, or a database query, OID content, etc).

Please note that the **String Search** Monitor works a bit differently on "running sources" (Log files and never-ending command lines) than on flat sources (flat files, command lines, Web requests, etc.):

- **On "running sources"** (Log files and never ending command lines):
  - the strings are searched only in new lines since the last polling. For a string search in a running source, two graphs are built: **Number of matches since the last acknowledgment** and **Number of matches per minute since the last polling**.
  - you can specify auto-acknowledging strings that will automatically reset the graph to the "number of matches".

- **On "flat sources"** (any other source):
  - the strings are searched in the entire source every time (the whole file, the whole standard output, the whole HTTP response, the whole dataset). For a string search in a flat source, one graph is built: **Number of matches at the current polling**.
  - you cannot specify auto-acknowledging strings since the parameter is recalculated from "0" at each polling.
  - you can specify where information should be searched in the file (n lines, pre-filter, etc.).

String search objects are instances of the **SEN_MS_STRING** application class.
To search for a specific String:

1. If the file to be parsed is a multi-line, XML, or HTML content, pre-process its content.
2. In the PATROL Console, right-click the Monitor instance (file, Web request, etc.) and select KM Commands > New > String Search...

3. Specify the information to search for:
   - **Search for lines that:**
     - **Contain/do not contain:** You can enter up to two strings (regular expressions) to look for, and decide whether or not those strings should be contained in the line. It is also possible to specify if the two strings should be found together (AND), or if only one of the two strings is sufficient (OR).
     - **Select where to search:** For each entered string, you can specify where in the line to search for the string:
       - **Anywhere in the line** (default)
       - **At the following character offset:** if you choose to search for the string from a character offset in the line, you must specify the offset in this field. Character offset is nothing but the character number. For example, to search for a string that starts from the seventh character in the line, you enter the digit 7 as the character offset.
       - **In the following column number:** Enter the column number
4. If the option **In the following column number** was previously selected, click the **Column separators** button to specify how to identify the relevant column by entering the column number and specifying the separator:

![Column separators](image)

**Searching for a Specific String — Column separator definition**

- Select or de-select applicable separators. For custom separators, enter the character in the **Other** field.
- **Consecutive separators must be treated as a single one** (useful for data separated by blanks): Typically, it indicates that consecutive separators must be treated as a single separator.
- **Consecutive separators mean empty columns** (useful for data separated by blanks): Each separator is treated as an individual column separator and the column is considered empty.
- Click **Accept**.

5. (Log File Monitoring) **Report Matching Lines**:

- **since last acknowledge (incremental)**: Select this option to count the lines matching the string search since the last time the **MatchingLineCount** parameter was reset or the PATROL Agent started.
- **in the current collect only**: Select this option to count the lines matching the string search during the current collect.
6. Click **Next**.

a) For string searches on a flat source (flat file, command line, Web request, etc.), the following dialog box is displayed:

- **Select which lines of the source should be scanned**
- **Search for Strings in all lines**: The string(s) will be searched for in all the lines of the specified source.
- **Search for Strings only in the following line numbers**: Enter the list of line numbers you wish to scan separated by ‘;’. Lines are specified as follows:
  - x, y: line x and line y
  - x-y: all lines from x to y inclusive
  - x: Only line x
  - x-: all lines from x to the end of the file inclusive

**Example**
Here are some examples of formats that can be used when specifying line numbers: "4;6;8", or "3-", or "-5", or "1;3-5;7-9"

- Click **Next**.
b) For string searches on a running source (log file and never-ending command lines) the following dialog box is displayed:

- Set the automatic acknowledgment of alerts:
  - **Acknowledge alert(s) if the string below is found**: Check the box to acknowledge the alert.
    - Specify the string
    - Select where to search: specify the location of the string
  - **Acknowledge alert(s) after**: Check this box and then specify the time in seconds after which the alerts will be acknowledged. Default is 120 minutes.
  - **When Acknowledging**: Specify the action you wish Monitoring Studio to perform when acknowledging an alert:
    - Select the **Reset MatchingLineCount parameter to zero** option to have Monitoring Studio automatically reset the counter of the **MatchingLineCount** parameter to zero.
    - Select the **Reset MatchingLineCount parameter by one** option to have Monitoring Studio automatically decrease by one the value of the counter of the **MatchingLineCount** parameter. Use this option if you need the solution to acknowledge each event counter and get a close follow-up on the log activity.
- Click Next.
7. Configure the Monitor settings.
8. Click Finish
Extracting Numeric Values

Problems with a technology (application, server, device, etc.) are not always as simple as a sentence explaining that an "error has occurred." Sometimes, a technology reports its health by providing critical numbers, like a queue length, a processing time, a utilization percentage, etc. These numbers may be reported by the technology through its files, in the output of commands, in a database, in a Web page, etc. Monitoring Studio extracts these values and reports them as graphs in the PATROL Console. This feature is called **Numeric Value Extraction** as its purpose is to extract numeric values from a text input (the output of a command, a Web page, the result of a SQL query, or WBEM query etc.).

All you need to do is indicate how to find the numeric value(s) within the Monitor. The basic mechanism is:

1. **Specify a Monitor**
2. Specify with a regular expression the location of the numeric value within the searched lines
3. Indicate the numeric value’s position in these lines i.e. before/after the string; column number etc.
4. Indicate which numbers are to be considered if several lines contain the searched numeric value: first value, last value, calculate average; highest value; lowest value.

The numeric value searching function works a bit differently on "running sources" (Log files and never-ending command lines) than on flat sources (flat files, command lines, Web requests, etc.):

- On "running sources" (Log files and never-ending command lines); the numeric values are searched only in new lines since the last polling.
- On "flat sources" (flat files, command lines, Web requests, database queries), the numeric values are searched in the entire source (the whole file, the whole standard output, the whole HTTP response, the whole data-set).

If several values are found, it is possible to select which value should be kept: the last value found, the average of all values, the minimum or maximum or a total of all values. A graph is then built with this value.

Numeric value search objects are instances of the `SEN_MS_NUMBER` application class.
To extract a Numeric Value:

1. If the file to be parsed is a multi-line, XML, or HTML content, **pre-process its content**.
2. In the PATROL Console, right-click the Monitor instance (file, Web request, etc.) and select **KM Commands > New > Numeric Value Extraction**...

   ![Image of Numeric Value Extraction dialog]

3. Specify which lines are to be searched for the numeric value. The information to enter subsequently depends on this first choice. There are three modes to choose from:
   - **All lines**: All lines of the text will be scanned for the Numeric value search. There is no need to provide further information.
   - **The Line numbers below**: Only specific line numbers will be scanned. If this mode is selected, the line numbers must be specified in the text field below. Line numbers are specified as follows:
     - \(x, y\): line \(x\) and line \(y\)
     - \(x-y\): all lines from \(x\) to \(y\) inclusive
     - \(x\): only line \(x\)
     - \(x-\): all lines from \(x\) to the end of the file inclusive

   **Example**
   Here are some examples of formats that can be used when specifying line numbers: "4;6;8", or "3-", or "-5", or "1;3-5;7-9"

   If the **Skip blank lines** option is selected, empty lines will be ignored in the line-count.
   - **Lines matching the regular expression below**: The lines scanned will be the lines matching the **regular expression** specified in the field.

Click **Next**.
4. Indicate the position of the numeric values to be found:

- **The numeric value are located**: There are four different modes to choose from and the information to enter depends on this choice.

- **After the string specified below**: If the numeric value is located after the string to be entered in the text field.

- **Before the string specified below**: If the numeric value is located before the string to be entered in the text field.

- **At the character offset specified below**: The value should be at a specific character offset in the line. Enter the offset number in the box. Monitoring Studio will look for the numeric value at that exact character offset in the line. If no numeric data is found, no value will be collected.

- **In the column number specified below**: The previously selected lines contain several columns identified by a separator character. Enter the column number that should contain the value and click the **Column separators** button to specify how columns are separated.
4. Specifying the Information to be Searched

Extracting Numeric Values - Column Separator Definition

- **Check or uncheck separators as you need.** You can also add a list of custom separators in the Other field. Simply type the separators one after the other.
- **Consecutive separators must be treated as a single one:** Typically, it indicates that consecutive separators must be treated as a single separator.
- **Consecutive separators mean empty columns:** Each separator is treated as an individual column separator and the column is considered empty.

The above two options are especially useful for data separated by blanks.

- Click Accept.

5. Click Next.
6. From the **Expected format** drop-down list, select how the numeric values are formatted. This option allows you to extract numeric values that use blank, comma, or points as decimal and thousand separators. Monitoring Studio will look for a number in the location specified previously. When a character that does not match the expected format is found, the parsing will stop. So if the expected format is 1,000 and Monitoring Studio finds 1.000, the returned value will be 1.

7. Check the box **Support negative values** if the numeric values that you are looking for can be negative. The '-' sign will be considered as an acceptable character when looking for the number.

8. Indicate which value should be used to set the parameter value and build the graph in the PATROL Console if several values are found in the searched text. The possible values are:
   - **Keep the first**: Only the first value found will be kept.
   - **Keep the last (default)**: Only the latest value found will be kept.
   - **Calculate the average**: The values found will be averaged and only the result will be kept.
   - **Keep the lowest value**: Only the lowest value found will be kept.
   - **Keep the greatest**: Only the greatest value found will be kept.
   - **Calculate the sum**: The values found will be summed and only the result will be kept.

9. Click **Next**.

<table>
<thead>
<tr>
<th>Monitored Value</th>
<th>Raw Value</th>
<th>Monitored Value:</th>
<th>Raw Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw Value:</td>
<td>Delta:</td>
<td>Post-processing performed on the extracted value:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delta:</td>
<td>- Raw Value: no post processing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delta:</td>
<td>- Delta: difference between two polling.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delta:</td>
<td>- Delta per....: difference between two polling on a time scale.</td>
<td></td>
</tr>
<tr>
<td>Discard negative Delta values</td>
<td>Rescaling:</td>
<td>No rescaling</td>
<td></td>
</tr>
</tbody>
</table>

10. **Monitored Value**: Select the option corresponding to the post-processing action you wish the solution to perform.
   - **Raw Value**: The values are reported as collected. No post-processing is performed.
   - **Delta**: The value reported corresponds to the difference between values collected during two consecutive polling.
   - **Delta per second/minute/hour**: The value reported corresponds to the result of the division of the Delta by the number of seconds/minutes/hour elapsed between the collection times.
- Select the option **Discard negative Delta values** if you do not want negative values to be reported on the graph.
- Use the **Rescaling** option to configure Monitoring Studio to rescale the value that is being extracted in order to have a more readable graph in the PATROL Console. The available rescaling options are:
  - No rescaling
  - Divide the value by a value that then gives you the reading in terms best suited to you
  - Multiply the extracted value by a constant factor
This can be useful if you extract numeric values in bytes but prefer to show a graph in megabytes. In such a case, you would divide the values by 1048576 (1024*1024).

11. Click **Next**.
12. **Configure the Monitor settings**.
13. Click **Finish**.

⚠️ If Monitoring Studio does not find a number at the specified location, no numeric value will be extracted and the PATROL graph will not be refreshed (space characters are ignored).

### Example: XML LOG File Parsing

**Monitoring the content of an XML LOG file with Monitoring Studio**

**Specifying the file to monitor**

1. In the PATROL Console, right-click the **Host** or **Monitor Group** icons and select **KM Commands > New > Monitor...**
2. Select **File** from the drop-down list and click **Next**.
3. Specify that file is a LOG file, i.e. that Monitoring Studio needs to monitor only the new lines that are being added to the file.
4. Specify the path to the file. You can use wildcards (* and ?) if the name of the file changes over time (like a time-stamped LOG file). In such case, Monitoring Studio monitors the most recently updated file which matches with the specified path.
5. Select the parameters you want to monitor. See **SEN_MS_FILE** for parameter details.
6. **Configure the Monitor settings**.

You have successfully setup the monitoring of an XML log file. Now to parse this file, you first need to preprocess the XML text in order to then run string searches or perform numeric value extraction on the result.

**Pre-processing the content of the file (converting XML to CSV)**

In the PATROL Console, right-click the **File Monitoring** icon and select **KM Commands > New > Text Pre-processing...**. Select the **Convert XML to CSV** option.
In this example, the records in this XML LOG file are in the following format:

```xml
<rec>
<vm>su37sr72</vm>
<ts>2003-09-22 11:47:35.511 CEST</ts>
<level>ERROR</level>
<class></class>
<method></method>
<ctx>
<pid>A141607</pid>
<appid>frontnet</appid>
<cname>User_3_0.getDefaultUserRole</cname>
<reqid>2</reqid>
<sesid>1uEPHTdRG2mM6GCfhv1EkwcBrCi68ffGlzgIEtGWHFMs5Hd71wE7!-1625978434!-1455528670!7501!7502!1064223951289</sesid>
<thrid>ExecuteThread: '68' for queue: 'default'-f7c8b25c01</thrid>
</ctx>
<msg><![CDATA[FNNotAuthorizedException;FEA002002;No authorization to execute service operation]]></msg>
<exc>
<ts>2003-09-22 11:47:35.509 CEST</ts>
<sev>ERROR</sev>
<context></context>
<pid>A141607</pid>
<appid>frontnet</appid>
<cname>User_3_0.getDefaultUserRole</cname>
<reqid>2</reqid>
<sesid>1uEPHTdRG2mM6GCfhv1EkwcBrCi68ffGlzgIEtGWHFMs5Hd71wE7!-1625978434!-1455528670!7501!7502!1064223951289</sesid>
<thrid>ExecuteThread: '68' for queue: 'default'-f7c8b25c01</thrid>
</exc>
</rec>
```
4. Specifying the Information to be Searched

<cthid>ExecuteThread: '68' for queue: 'default'=-f7c8b1696c</cthid>
</ctx>

<![CDATA[com.csg.pb.frontnet.exec_arch.ca1x.FNNotAuthorizedException: No authorization to execute service operation
at com.csg.pb.frontnet.services.user_3_0.bean.UserBean_3_0.getDefaultUserRole(UserBean_3_0.java:345)
at com.csg.pb.frontnet.services.user_3_0.bean.UserBean_3_0_3c05dc_MOImpl.getDefaultUserRole(UserBean_3_0_3c05dc_MOImpl.java:145)
at com.csg.pb.frontnet.services.user_3_0.bean.UserBean_3_0_3c05dc_MOImpl_WLSkeln.invoke(Unknown Source)
at weblogic.rmi.internal.BasicServerRef.invoke(BasicServerRef.java:360)
at weblogic.rmi.cluster.ReplicaAwareServerRef.invoke(ReplicaAwareServerRef.java:93)
at weblogic.rmi.internal.BasicServerRef.handleRequest(BasicServerRef.java:329)
at weblogic.rmi.internal.BasicServerRef.dispatch(BasicServerRef.java:178)
at weblogic.rmi.internal.ServerRequest.sendOneWayRaw(ServerRequest.java:92)
at weblogic.rmi.internal.ServerRequest.sendReceive(ServerRequest.java:112)
at weblogic.rmi.cluster.ReplicaAwareRemoteRef.invoke(ReplicaAwareRemoteRef.java:263)
at weblogic.rmi.cluster.ReplicaAwareRemoteRef.invoke(ReplicaAwareRemoteRef.java:230)
at weblogic.rmi.internal.ProxyStub.invoke(ProxyStub.java:35)
at $Proxy1401.getDefaultUserRole(Unknown Source)
at com.csg.pb.frontnet.services.user_3_0.bean.UserCA_3_0.getDefaultUserRole(UserCA_3_0.java:244)
at com.csg.pb.frontnet.apps.common.brokers.FnUserBroker.getDefaultPortalUserSettings(FnUserBroker.java:56)
at com.csg.pb.frontnet.apps.common.brokers.FnUserBroker.getDefaultMandant(FnUserBroker.java:280)
at com.csg.cs.servlet.CSServlet.doGet(CSServlet.java:82)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:740)
at com.csg.cs.servlet.CSServlet.service(CSServlet.java:459)
at com.csg.pb.frontnet.apps.common.base.CommonServlet.service(CommonServlet.java:66)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:853)
at weblogic.servlet.internal.ServletStubImpl.invokeServlet(ServletStubImpl.java:262)
at weblogic.servlet.internal.TailFilter.doFilter(TailFilter.java:21)
at weblogic.servlet.internal.FilterChainImpl.doFilter(FilterChainImpl.java:27)
at com.csg.cs.security.wis.enforce.IntranetPLEnfflter.doFilter(IntranetPLEnfflter.java:27)
at weblogic.servlet.internal.FilterChainImpl.doFilter(FilterChainImpl.java:27)
at weblogic.servlet.internal.RequestDispatcherImpl.forward(RequestDispatcherImpl.java:27)
at com.csg.pb.frontnet.apps.common.util.RequestForwarder.forward(RequestForwarder.java:27)
at com.csg.pb.frontnet.apps.portals.base.PortalSelectionController.doGetManaged(PortalSelectionController.java:49)]]>
So, <REC> is the XML tag for each new record. Let’s say that we would like to retrieve the <TS> value, the <LEVEL> value, the <CNAME> value under <CTX> and the <MSG> value.

Therefore, we are specifying that REC is the XML tag for a new record and that we would like to include the value for the following properties and sub-tags: TS LEVEL CTX.CNAME MSG. Please note the syntax "CTX.CNAME" which means the value of CNAME under the CTX tag.
Then, specify a label and ID for the text pre-processing object that will be created under the file icon.

As a result, we get a new icon in the PATROL Console, corresponding to the XML to CSV pre-processing:

![XML to CSV Pre-processing Icon](image)

Accessing the Result File

This object has a single **TransformResult** text parameter as a result of the XML to CSV pre-processing:

```
2003-09-22 11:47:35.511 CEST;ERROR;User_3_0.getDefaultUserRole;FNNotAuthorizedException;FEA002002;No authorization to execute service operation]] >;
2003-09-22 11:52:05.984 CEST;ERROR;User_3_0.getDefaultUserRole;FNNotAuthorizedException;FEA002002;No authorization to execute service operation]] >;
2003-09-22 12:06:18.272 CEST;ERROR;User_3_0.getDefaultUserRole;FNNotAuthorizedException;FEA002002;No authorization to execute service operation]] >;
2003-09-22 12:09:53.920 CEST;ERROR;User_3_0.getDefaultUserRole;FNNotAuthorizedException;FEA002002;No authorization to execute service operation]] >;
2003-09-22 12:10:39.557 CEST;ERROR;KycBeneficialOwnerProfiles;FNDataServiceFailureException;RDS001003;Code not found - TableName:Landcode_1_RefTableObject, BusinessUnit: 0012, Language: 891, Code: 001]] >;
2003-09-22 12:10:39.566 CEST;ERROR;KycBeneficialOwnerProfiles;FNDataServiceFailureException;RDS001003;Code not found - TableName:Landcode_1_RefTableObject, BusinessUnit: 0012, Language: 891, Code: 001]] >;
2003-09-22 12:10:56.637 CEST;ERROR;CIFS_Customer_1.getCustomer;FNDataServiceFailureException;RDS001002;Code not found - TableName:Service_Status_InfoRefTableObject, BusinessUnit: 0000, Code: CIFS_Customer_1_0]] >;
2003-09-22 12:10:56.643 CEST;SEVERE;CIFS_Customer_1.getCustomer;FNServiceNotAvailableException;FEA000001;Service not available - Service FNServiceState.getState]] >;
2003-09-22 12:10:56.945 CEST;ERROR;BPST_UserProfile_3.getUsers;FNDataServiceFailureException;RDS001002;Code not found - TableName:Service_Status_InfoRefTableObject, BusinessUnit: 0000, Code: BPST_UserProfile_3_0]] >;
2003-09-22 12:10:56.950 CEST;SEVERE;BPST_UserProfile_3.getUsers;FNServiceNotAvailableException;FEA000001;Service not available - Service FNServiceState.getState]] >;
2003-09-22 12:21:30.004 CEST;ERROR;User_3_0.getDefaultUserRole;FNNotAuthorizedException;FEA002002;No authorization to execute service operation]] >;
```
Searching for strings in the result of the XML-to-CSV pre-processing

1. Right-click the **Text-Pre-Processing icon > KM Commands > New > String Search...**
2. Search for lines that contain the string "SEVERE" in the second column, corresponding to XML records whose <LEVEL> is "SEVERE"

### Performing a String Search Command on a Converted File

- From the first pull-down list, select **contain**.
- Type **SEVERE**
- From the second pull-down list, select **in the following column number:**
- Type **2**.
3. Click the **Column Separators** button, uncheck all the separators except the semicolon and click **Accept**.
4. Click **Next** and follow the wizard steps as for any normal string search on a LOG file, keeping the default values shown.
5. **Configure the Monitor settings.**
6. Click **Finish**

As a result, we get the following String search object: SEVERE under the XML-to-CSV pre-processing object.

![Diagram showing the string search object]

**Accessing the String Search Results**

⚠️ You can create as many string searches as you want on a file and on a text-processing object, and you can create several different text-processing objects on the same file object.
Administrative Tasks
This section deals with information on basic configuration and administrative tasks.

Acknowledging Alerts

Monitoring Studio KM for PATROL allows you to acknowledge alerts through the following KM Commands:

- Acknowledge Alerts
- Acknowledge all and Reset
- Reset CollectionErrorCount
Acknowledging Alerts

PATROL Administrators can use the **Acknowledge Alerts** menu command to acknowledge any alert.

This option is applicable to all Monitors except for **String Search**, **SNMP Trap** and **Windows Event** instances for which a specific command **Acknowledge all and Reset** can be used to acknowledge all alerts and reset the count parameters.

To acknowledge all alerts for a specific Monitor:

1. Right-click the **object icon > KM Commands > Acknowledge Alerts**...

   ![Acknowledging Alerts](image)

   **Acknowledging Alerts**

   2. Monitoring Studio displays the name of the parameters for which an alert can be acknowledged. Click a parameter to select it and click **OK**. The selected parameter(s) will be deactivated and then reactivated. An acknowledging event will automatically be triggered.
Acknowledge all and Reset

Some technologies are unable to inform a 'back to normal situation' when performing the monitoring with String Searches, SNMP Traps, and Windows Events. PATROL administrators may at times want to manually acknowledge the alerts and reset the MatchingLineCount, MatchingTrapCount, or MatchingEventCount parameters to zero.

To manually acknowledge alerts, right-click the object icon > KM commands > Acknowledge all and Reset.
Reset CollectionErrorCount

The CollectionErrorcount parameter reports all data collection related errors that occurred during the collection process. Because this parameter is cumulative, a PATROL administrator might want to acknowledge it manually.

The Reset CollectionErrorCount menu command allows you to reset the CollectionErrorCount parameter of a Group or the Monitoring Studio instance to zero.

To perform the Reset CollectionErrorCount menu command, right-click the object icon > KM commands > Reset CollectionErrorCount.

⚠️ By default, the CollectionErrorCount parameter will be reset after 15 minutes (Group instance) or after 135 minutes (Monitoring Studio instance) if no new errors are found. These default settings can be respectively customized with the configuration variables /SENTRY/STUDIO/<groupID>/collectionErrorCountAutoAcknowledgeTime and /SENTRY/STUDIO/collectionErrorCountAutoAcknowledgeTime.
Configuring Java Settings

The Java Settings wizard enables you to define which Java instance is to be used by Monitoring Studio. You can either use the automatic detection, select a pre-detected java path or enter manually the path leading to the Java executable directory to be used.

⚠️ Java v1.6 and higher is needed for Monitoring Studio to run properly.

To access the Java Settings wizard, right-click the main Monitoring Studio icon > KM commands > KM Settings > Java Settings.

Select the Java executable detection method: Select one of the three following options:

- **Automatic**: Select this option if you wish Monitoring Studio to detect the Java executable directory by itself upon each discovery.
- **User Selection**: Select this option if you wish to select a Java executable directory within a list of pre-detected executables.
- **Manual**: Select this option if you wish to manually enter the Java executable directory path. Click Next to continue.
Automatic Detection

If you have selected the automatic detection at the previous step of the wizard and if Monitoring Studio detects Java on the managed system, the path of the Java executable directory that will be used when performing commands requiring Java features is displayed.

1. (optional) Enter a **Username** and **Password** if you want to use a specific account to run Java on your system.
2. Click **Finish** to save your settings.

⚠️ The PATROL Agent needs to be restarted for the new setting to be taken into account.
User Selection

If you have selected the user selection option at the previous step of the wizard, Monitoring Studio displays a list of all the Java executable directory found on your machine.

1. Select the Java executable directory you wish Monitoring Studio to use when performing commands involving Java features.
2. (optional) Enter a **Username** and **Password** if you want to use a specific account to run Java on your system.
3. Click **Finish** to save your settings.

⚠️ The PATROL Agent needs to be restarted for the new setting to be taken into account.
If you have selected the Manual option at the previous step of the wizard, Monitoring Studio lets you enter the path to the Java executable directory you wish Monitoring Studio to use when performing commands requiring Java features.

1. Enter the path to the Java executable.
2. (optional) Enter a Username and Password if you want to use a specific account to run Java on your system.
3. Click Finish to save your settings.

⚠️ The PATROL Agent needs to be restarted for these changes to take effect.
Configuring Thresholds

Alert thresholds are dynamically set by Monitoring Studio KM for PATROL. However, it is possible to change threshold mechanism as well as the alert settings, as described in the following subsections:

- Specifying the Threshold Mechanism Mode
- Setting or Modifying Alert Thresholds
Specifying the Threshold Mechanism Mode

By default, Monitoring Studio KM for PATROL automatically determines which mechanism (Tuning or Event Management) is best suited to the managed system when it first runs. This threshold mechanism selection can however be modified later on through the **Thresholds Mechanism Selection** KM Command:

1. Right-click the main **Monitoring Studio icon > KM Commands > KM Settings > Thresholds Mechanism Selection**...

2. Select one of the following options:
   - **Automatic (Recommended)**: Monitoring Studio automatically detects the way thresholds are managed by the PATROL Agent and uses the most relevant mode (Tuning or Event Management).
   - **Tuning**: Monitoring Studio manages its thresholds through the standard internal PATROL mechanism (Override parameters). Thresholds are stored in the PATROL Agent configuration under the `/___tuning___` tree.
   - **Event Management**: Monitoring Studio manages its thresholds through the Event Management mechanism. Thresholds are stored in the PATROL Agent configuration under the `/AS` tree. This option requires that you set up the PATROL for Event Management KM on your PATROL Agent. PATROL for Event Management has to be enabled and preloaded.

⚠️ In order to avoid side effects and unpredictable behavior, if you change the thresholds management option, Monitoring Studio will automatically migrate the thresholds set through the previous method to the new method (only for its monitored objects).
Setting or Modifying Alert Thresholds

Monitoring Studio enables you to set alert thresholds for each parameter through the command menu. To set or modify alert thresholds, right-click any Monitor icon > KM commands > Thresholds... and the threshold management wizard appears.

⚠️ The Threshold Management wizard can also be prompted immediately following the setup of a new monitoring object. The last panel of the wizard offers you the option of either accepting default thresholds, modifying them right away, or setting them later.

A drop-down list displays the parameters available for the instance.

⚠️ An asterisk symbol “*” displayed next to the parameter name signifies that the parameter already has thresholds. You can then choose to either keep the same thresholds or just view them or modify them… as per the requirement.

The Reference Guide lists all the classes with details on the menu commands and the parameters available for each class.

Threshold Type and Alert actions

Monitoring Studio has two "types" of thresholds: Simple (2 alerts maximum) and Advanced (3...
alerts maximum). Depending on the user’s selection, both types of thresholds can raise the following alerts:

- Do not trigger any alert
- Trigger an INFORMATION
- Trigger a WARNING
- Trigger an ALARM

In addition, you can set Alert Actions to be triggered when an alert is raised on a parameter. Please see the section: Alert Actions capabilities for more details on the same.

**Simple Thresholds**

This type of threshold is easy and very user-friendly: the threshold values are expressed in terms of "greater than/lower than". All that you need to do is to enter actual "limits" as per the specific requirement, and the frequency of occurrence. This type of threshold has a maximum of two alert types.

Certain parameters have "pre-defined" values. Basically these parameters are the ones with boolean values, so the choice you can make can only be one or the other – depending on the parameter itself.
Advanced thresholds

To access the advanced threshold options, check the box for **Use advanced thresholds...** when you select the parameter > click **Next**.

The advanced thresholds mode allows you to set up to a maximum of 3 alerts.
This type of threshold setting is a little more complex as it requires the user to enter specific ranges of values as thresholds. This setting is like that of PATROL thresholds, where you have the possibility of raising three alert types:

- **Border Alert:** An alert will be triggered if the value polled is not between "x" and "x" and occurs "x" times in a row.
- **Alert 1:** An alert will be triggered if the value is between "x" and "x" and occurs "x" times in a row.
- **Alert 2:** An alert will be triggered if the value is between "x" and "x" and occurs "x" times in a row.

⚠️ Note applicable to both Simple and Advanced Thresholds: In general, Alert Actions are triggered only when a parameter breaches its thresholds. However for certain parameters, such as MatchingTrapCount, MatchingLineCount, and MatchingEventCount, it is possible to trigger Alert Actions not just when thresholds are breached, but also each time an SNMP trap is received or a matching line/event is found. The option Execute the Alert Actions appears in the thresholds wizard for the parameters to which this feature is applicable under the section for Alarms.

**Example**

Let’s say you are setting thresholds on a string search. In this wizard you will find the option Execute the Alert Action as string search has the parameter MatchingLineCount. If you select Execute the Alert Actions every time a matching line is found on the MatchingLineCount parameter, Monitoring Studio will run the Alert Actions every time a line matching the string search is found.
Copy, Cut, and Paste

Once you have configured one or several monitoring tools, you may need to copy or move them under a new container. You may for example need to duplicate a String Search that you have setup to one Command Line execution to another one. This can be done easily with the Copy, Cut, and Paste feature of Monitoring Studio.

To access the Copy, Cut, and Paste features, right-click the object icon > KM commands > and select either Copy, Cut, or Paste, depending on the action that you wish to perform.

⚠️ Some objects cannot be pasted<other objects. For example, you cannot paste a String Search object under a Process monitoring object. Basically, you can paste everything everywhere that you would have been able to do with the regular wizards.

⚠️ The Paste menu command also pastes the children of the copied/cut object.
Deploying your Configuration

Monitoring Studio allows you to export your configuration and deploy it on all the machines where the technology to be monitored is installed. The deployment consists in:

- Exporting your configuration
- Importing it on the relevant machines.
Exporting Configuration to a File

This feature provides a simple way to save the configuration of a PATROL Agent by exporting it to a file for reuse later. The configuration saved in a file can then be loaded onto a different PATROL Agent through the PATROL interface. The main benefits are that it:

- Eliminates the trouble of manually configuring Monitoring Studio on another PATROL Agent all over again
- Ensures both configurations are identical

Monitoring Studio offers you two options:

- To export the entire Monitoring Studio configuration
- To export a Group configuration
Exporting the Entire Monitoring Studio Configuration

1. Right-click the main Monitoring Studio icon > KM commands > Configuration > Export Configuration.

![Image of Monitoring Studio Configuration Export]

Managed System: PC-CPW7_3181

**Configuration Export**

Export Monitoring Studio configuration to a .cfg file. This configuration can then be imported from a PATROL Agent or used in BMC TrueSight CMA policies.

**Export:**
- The entire Monitoring Studio configuration
- My Group
- The entire Monitoring Studio configuration
- INCLUDE Monitoring Studio global settings

[Cancel] [Next] [Help]
2. Select **The Entire Monitoring Studio configuration**.
3. (Optional) Check **Include Monitoring Studio global settings** if you want the global settings to be included in the export file:

- Select the global variables to be included. Please note that global variables will only be displayed if they have previously been configured.
- Click **Next**.
4. Enter the path and name of the file on the PATROL Agent system to export the configuration. By default, the file will be saved on the localhost. It will be written to SEN_MS_<hostname>-<port>.cfg under %PATROL_HOME%\config on Windows and $PATROL_HOME/config on UNIX systems.

5. Click **Finish**. A successful export of the configuration will bring-up this panel:

![Exporting Configuration to a File - Export Confirmation Message](image)

### Exporting a Group configuration

Exporting one or several Group configurations works exactly the same way as exporting the entire configuration. The main difference is that only the information relevant to the Group will be saved.

To export a Group configuration, you can either:

- Right-click the main **Monitoring Studio** icon > **KM commands** > **Configuration** > **Export Configuration** and select the Group to export from the drop-down list
- Or right-click a Group > **KM commands** > **Export Configuration**...

You will then have to specify the path and name of the file that will contain the Group configuration.

![If there are any Global Constants defined for the Group, a dialog appears allowing you to clear the values in the exported file.](image)

A confirmation message will pop-up once the configuration has been successfully exported.
Importing Configuration

This feature allows you to configure Monitoring Studio by importing a configuration already in use on another PATROL Agent. It:

- Eliminates the trouble of manually configuring Monitoring Studio on another PATROL Agent all over again
- Ensures both configurations are identical

Basically, you import a configuration file that has been exported from another PATROL Agent. All information found in the exported file will be imported and merged into the current installation.

⚠️ You may import a PATROL agent configuration (".cfg") with any type of thresholds. If necessary, Monitoring Studio will convert the thresholds to the type of thresholds currently used at the next discovery (within an hour).

To import an existing configuration:

1. Right-click the Monitoring Studio icon > KM commands > Configuration > Import Configuration.

![Importing Configuration - Welcome Page](image_url)
2. Enter the path to the folder containing the configuration file(s) and click **Next**. By default, all .cfg files found under %PATROL_HOME%\config on Windows and $PATROL_HOME/config on UNIX systems will be listed.

3. Select the configuration file to import and click **Next**.
4. Choose whether global settings will be imported.

> Importing global settings will overwrite the current global settings of your existing objects.

Importing Configuration - Group Constant(s) Import

**Managed System:** PC-CPWIN7_3181

SEM_MS_MyGroup.cfg has 3 Group Constant(s) defined that may not have accurate value(s) for the proper operation of Monitoring Studio on pc-cpwin7.

Do you wish to clear the value(s) of these Group Constant(s)?

MyGroup: %{SYSTEM_USERNAME} = patrol
MyGroup: %{SYSTEM_PASSWORD} = B6244248EBEED94F63E2B9
MyGroup: %{LYNC_PATH} = C:\Program Files\Microsoft Office 15\root\office15

Once they are imported, use the “Edit” menu from the Group icon to update the Group Constant(s).

[Clear values] [Keep values]

Importing Configuration - Existing Objects

Some objects defined in SEM_MS_MyGroup.cfg already exist.

Do you wish to overwrite the existing objects or rename the imported Group ID(s)?

Existing Group ID(s):

MyGroup

[Overwrite] [Rename]
6. Click:
   - **Overwrite** to overwrite existing objects.
   - **Rename** if you do not want to overwrite existing objects.

   ![Monitoring Studio]

   _Managed System: PC-CPWIN7_3181_

   _Prefix all object IDs with: _

   ![Importing Configuration - Prefix Definition]

   If you click **Rename**, you will have to specify the prefix to be assigned to these copied objects. The prefix will be applied to the ID of all the Groups, Hosts and Monitors found in the configuration. Example: you enter "NEW_" in the prefix box and you have a Group called "Lync". The new ID will be "NEW_Lync" thus avoiding overwriting the existing "Lync" configuration. Click **OK**.

   ![Importing Configuration - Summary]

   _Summary_

   28 object(s) to be imported from SEM_Hi_HyGroup.cfg in 1 Group(s):
   - HyGroup
   
   Keep the values of Group Constants
   
   Click [Finish] to start the import.
7. Before importing the configuration, the number of objects to be imported and the previously chosen options are listed. Click **Finish**.

![Importing Configuration - Completed Import Confirmation](image)

8. A panel confirming the import appears. Click **OK**.

On completion of the discovery process, you will see all the objects of the imported configuration in your console.
Deleting a Monitored Object

Monitoring Studio allows you to delete:

- any monitored object by right-clicking object icon > KM commands > Delete. This object and all its children will be removed and no longer monitored.
- all objects and children under a Group, Host, or Monitor Group instance by right-clicking it and selecting KM commands > Delete All.
Editing a Monitored Object

To edit a Host, Group or Monitor:

1. Right-click the instance of the monitored object > KM Commands > Edit...
2. Modify the information related to the selected object, just as you wish. Click Next.

3. The final step of the wizard displays the Monitor Settings of the monitored object. The wizard:
   - Displays a reminder of the object's Internal ID.
   - Lets you edit the object's Display name.

   Please note that you can also edit the Display Name using the Rename KM command.

4. Click Finish to validate your changes.
Forcing the Classic Mode

Monitoring Studio KM for PATROL can either be configured from BMC PATROL Console (Classic Mode) or BMC TrueSight Operations Management. When the KM is installed on a PATROL Agent, which is managed by Central Monitoring Administration (CMA), all the KM configuration menus are disabled in the PATROL Console. These configuration menus will display an error when selected, asking to use CMA instead. To configure Monitoring Studio from a PATROL Console, you need to force the KM to run in Classic Mode.

This will disconnect Monitoring Studio from receiving configuration from BMC ProactiveNet Central Monitoring Administration. Any monitoring that was configured in CMA and used by the PATROL Agent will be removed and replaced by Monitors created from the PATROL Console. However, this will not delete the policies created in CMA from the configuration.

⚠️ Any configuration for Monitoring Studio received from BMC ProactiveNet Central Monitoring Administration will be ignored.

To force the KM to run in Classic Mode:

1. In the PATROL Console, right-click the Monitoring Studio icon > KM commands > KM Settings > Force Classic Configuration Mode...
2. Check **Force the KM to run in Classic mode** and click **OK**.

Monitoring Studio will now start running in Classic Mode, enabling you to use the KM Configuration menus.
Modifying a Monitor Display Name and/or ID

Once you have configured one or several Monitors, you may need to rename/modify some display names or IDs. The Rename feature allows you to:

- Enter a new Monitor display name
- Modify the Monitor internal identifier (ID)

![Screenshot of Rename feature](image_url)
To modify the Monitor display name:
1. Right-click the **object icon > KM commands > Rename**...
2. In the **Monitor display name** text field, enter a new display name.
3. Click **OK** to validate changes.

To modify the Monitor internal identifier (ID):
1. Right-click the **object icon > KM commands > Rename**...
2. In the **Monitor internal identifier (ID)** text field, enter a new ID. If the Monitors attache
3. Click **OK** to validate changes. The following pop-up appears:

![Modification of a Monitor Name and/or ID - Warning]

4. If you are certain that the new ID will not cause any problem, click **Yes**.

The PATROL Console will display the new label and will update the ID of the Monitor as well as all its dependent items.
Modifying a Group Display Name and/or ID

Once you have added Groups, you may need to rename/modify some display names or IDs. The Rename feature allows you to:

- Enter a new Group display name
- Modify the Group internal identifier (ID)
To modify the Group display name:
1. Right-click the object icon > KM commands > Rename...
2. In the Group display name text field, enter a new display name.
3. Click OK to validate changes.

To modify the Group internal identifier (ID):
1. Right-click the object icon > KM commands > Rename...
2. In the Group internal identifier (ID) text field, enter a new short ID.
3. Click OK to validate changes. The following pop-up appears:

![Modification of a Group Name and/or ID - Warning]

4. If you are certain that the new ID will not cause any problem, click Yes.

The PATROL Console will display the new label and will update the ID of the Group as well as all its dependent items.
Modifying Group Constants

Group constants are defined at the **Group** level and can be reused in the various objects underneath. They facilitate the monitoring across various systems of a technology whose properties may change from one system to another. If you have previously specified **Group constants when creating a Group**, you will be able to modify them later on.

**To modify group constants:**

1. **Right-click a Group icon** and select **KM Commands > Group Constants...**

2. For each of the predefined group constants, enter a new value.

3. **Click OK** to validate changes.

The new group constants will now be taken into consideration by Monitoring Studio.

*Modifying Group Constants is also possible by right-clicking a Group > KM Commands > Edit.*
Temporarily Suspending the monitoring of an Object

In order to perform certain tasks, such as maintenance for example, it is often useful to pause the monitoring of an object or a group of objects. To pause the monitoring of a specific object or group of objects, right-click the object (or object container) icon > KM Commands > Pause Monitoring.

When in paused state, the object/group of objects is displayed with an OFFLINE status in the PATROL Console. Additionally, the mention '(Suspended)' may appear beside each related parameter.
To resume the monitoring of the object/group of objects, click Resume Monitoring in the menu.
Refreshing Parameters

To manually refresh parameters, without waiting for an automatic polling cycle, right-click the object icon > KM Commands > Refresh Parameters. This will reset the time to wait for the next polling interval. This will not affect "Once a day" or "Once a week" type collects. They will be collected at the scheduled day and time.
Specifying Alert Actions

Alert Actions enable the PATROL administrator to choose/configure the execution of certain actions when a monitored technology goes into a state of alert. With the Alert Actions functionality, it is possible to do one of the following:

- Customize notifications
- Specify recovery actions

Global vs Specific Alert Actions

Alert Actions can be set at two different levels:

- **Global Alert Actions** are set at the **Group level** for the overall technology. They specify the way in which the notification of a problem is done for all instances under this Group. This means that any parameter within this Group that triggers an alert will perform the Alert Actions set at the global level, in addition to any specific alert action that might have been set.

- **Specific Alert Actions** are set at the **Host level and Monitor level** for individual parameters and generally indicate the actions to perform in order to recover from a particular problem (e.g.: when this parameter goes into alarm - execute this recovery script). Therefore, specific Alert Actions need to be set for each parameter as the need may be.

If a specific Alert Action is set on a parameter belonging to a Group already set to trigger Global Alert Actions, both settings will be taken into account for that particular parameter instance.
Set Global Alert Actions

1. In the PATROL Console, right-click the **Group icon** and select **KM Commands > Alert Actions...**

   ![Specifying Global Alert Actions - Alert Actions Selection Page](image)

   **Alert Actions**

   Select the alert actions to be executed when the parameters of any monitor under My Group go into alarm:

   - Trigger an event
   - Annotate the graph
   - Execute a command
   - Execute a PSL statement (advanced)
   - Display a pop-up on the consoles
   - Log to a file
   - Send a basic SNMP trap
   - Send a custom SNMP trap (advanced)
   - Send an e-mail

   ![Specify Global Alert Actions](image)

   ![Specifying Global Alert Actions - Event Configuration](image)

2. Select the **Alert Action(s)** that you want to trigger each time the parameters enter a state of alert and click **Next**.
3. Configure the selected **Alert Action** and click **Next**.

⚠️ The `%{SEN_ALERT_DEFAULTCONTENT}` alert macro is the default alert content suitable for events and annotations. It resolves to the following macro syntax: `%{SEN_GROUP_NAME} %{SEN_HOST_NAME} %{SEN_PARAMETER_STATUS} on %{SEN_PARAMETER_NAME} of %{SEN_OBJECT_LABEL}`.

![Alert Actions for My Group](image)

- The alert actions you selected will be executed for all monitored parameters under each monitor of the group.
- **Click [Finish]** to apply your settings.
- **Note:** You will be able to set additional alert actions on each parameter by using the "Alert Actions" menu from the monitor.

4. Global Alert Actions have been set. Click **Finish**.

⚠️ You can set additional Alert Actions on any/all of the monitored parameters by using the "Alert Actions" menu from the monitor.
Set Specific Alert Actions

1. In the PATROL Console, right-click any Host or Monitor instance and select KM Commands > Alert Actions...

![Alert Actions Parameter Selection Page]

**Alert Action Parameter**

Select the parameter to set specific alert actions:

- `GrowthSpeed`

**Note:** Alert actions set for the group will automatically apply to all its related parameters.

- `Group Alert Actions`

---

Specifying Specific Alert Actions - Parameter Selection Page
2. Select the parameter for which you wish to set specific Alert Actions and click **Next**.

You can see the list of previously set Global Alert Actions by clicking the **Group Alert Actions** button.

3. The panel lists all available Alert Actions. Make your selection and click **Next**.
4. Configure the selected Alert Action and click Next.

![Specifying Specific Alert Actions - Alert Execution Confirmation Page]

4. Click Finish. When the selected parameter goes into alert, it will trigger the specific Alert Action as configured.

⚠️ You can set Global Alert Actions on all parameters by using the "Alert Actions" menu from the Group icon.
Alert Actions Capabilities

The Alert Actions feature offers a large choice of actions in order to notify the administrator of a problem with the technology or to recover from a particular problem. Monitoring Studio can be configured to run one or several types of actions when an alert is triggered by PATROL. You can use Alert Action macros to construct Alert Actions.

The following types of Alert Actions can be performed by Monitoring Studio:

**Trigger an event**

If you select the Trigger an Event action, you need to enter the string that will be displayed with the event.

A PATROL Event can be viewed from:

- Standard PATROL Consoles (Classic Console, PATROL Central)
- PATROL Enterprise Manager
- BMC Impact Manager
- BMC ProactiveNet Performance Management/BMC TrueSight Operations Management
- Other third-party products that interface with PATROL.
Annotate the graph

If you select the **Annotate the graph** action, you need to enter the string that will be displayed within the annotation point.

To view an annotation, when a threshold is breached, open the graph associated to the parameter in alert and double-click on the black annotation mark on top of the first data point.
**Execute a command**

If you select the **Execute a command** action, you need to complete the following panel:

1. Enter a command line to be executed on the target host.
2. (Optional) Enter the username and password used to run the command. By default, the command is executed using the default credentials for the monitor.

The command line can be a program utility or a script call with arguments.

⚠️ The command must be non-interactive (no window, no user input)
Execute a PSL statement

If you select the **Execute a PSL statement (advanced)** action, you need to enter the PSL statement to be executed by the PATROL Agent on the localhost. Although only a single line is permitted, it can have several PSL instructions.

![PSL Command Configuration](image)

Enter the PSL command to be executed on pc-cpwin7:

Note: You can use macro variables in the fields above. See the documentation for details about supported macros.

⚠️ The PSL command is recommended for advanced users of PATROL.
Display a pop-up on the consoles

If you select the **Display a pop-up on the consoles** action, you need to enter the message that will be displayed in the pop-up as well as in the title of the pop-up window.

**Console Pop-up Configuration**

Enter the pop-up window title:

```
%(SEN_PARAMETER_STATUS): %(SEN_GROUP_LABEL)
```

Enter the message for the pop-up displayed on the consoles:

```
%(SEN_ALERT_DEFAULTCONTENT)
```

Note: You can use macro variables in the fields above. See the documentation for details about supported macros.
Log to a file

If you select the **Log to a file** action, you need to enter the log file path on the localhost and the content of the line.

```
Log Configuration

Enter the log file path:
C:\Program Files\Patriot\log\%{SEN_GROUP_ID}.log

Enter the line to be written to the log file:
$SEN_ALERT_DEFAULTLOGMESSAGE

Note: You can use macro variables in the fields above. See the documentation for details about supported macros.
```
Send a basic SNMP trap

If you select the **Send a basic SNMP trap** action, you need to complete the following panel:

- IP address or hostname of the SNMP trap destination (Host field)
- SNMP port and community string
- Text that will be sent with the SNMP trap
Send a custom SNMP trap

If you select the **Send a custom SNMP trap (advanced)** action, you need to complete the following panel:

- IP address or hostname of the SNMP trap destination (**Host** field)
- SNMP port and community string
- All the characteristics of the trap: Enterprise OID, trap number and up to 4 varbinds.
Send an e-mail

If you select the **Send an e-mail** action, you need to complete the following panel:

- Enter the sender and the recipient email address in the **From** and **To** field. To send the email to multiple recipients, use the comma (,) or the semi-column (;) to separate the recipients' email addresses (ex: RecipientAddress1;RecipientAddress2;RecipientAddress2 OR RecipientAddress1,RecipientAddress2,RecipientAddress2)
- Enter the **SMTP server** name
- With the help of **Alert Action macros**, type the email subject and the message you wish to send.
Alert Action Macros

A macro is a variable whose value is replaced when an Alert Action is triggered. Macros can be used to customize the content of each Alert Action. For example: %{VALUE} is replaced by the actual current value of the parameter that triggered the alert.

Each macro listed in the tables below contains information about what triggered the PATROL alert. Some macros are "general" or "common" - these can be used for any object, and some are "object-specific" macros that are specific to the object, such as databases or files, etc.

Macro syntax supports white spaces.

General Macros

The macros given in the table below can be used on any object:

<table>
<thead>
<tr>
<th>General Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>% (SEN_ALERT_DEFAULTCONTENT)</td>
<td>Default alert content suitable for events and annotations, which resolves to the following macro syntax: % (SEN_GROUP_NAME) % (SEN_HOST_NAME) % (SEN_PARAMETER_STATUS) on % (SEN_PARAMETER_NAME) of % (SEN_OBJECT_LABEL)</td>
</tr>
<tr>
<td>% (SEN_ALERT_DEFAULTLOGMESSAGE)</td>
<td>Default alert content suitable for log files, which resolves to the following macro syntax: % (SEN_TIME:%Y-%m-%d %H:%M:%S) % (SEN_GROUP_ID) % (SEN_PARAMETER_STATUS) on % (SEN_PARAMETER_NAME) of % (SEN_OBJECT_LABEL).</td>
</tr>
<tr>
<td>% (SEN_CREDENTIALS)</td>
<td>System Credentials.</td>
</tr>
<tr>
<td>% (SEN_HOST_DOMAIN)</td>
<td>Domain of the targeted host.</td>
</tr>
<tr>
<td>% (SEN_HOST_FQDN)</td>
<td>Fully qualified domain name of the targeted host.</td>
</tr>
<tr>
<td>% (SEN_HOST_IPADDRESS)</td>
<td>IP address of the targeted host.</td>
</tr>
<tr>
<td>% (SEN_HOST_NAME)</td>
<td>Name of the targeted host.</td>
</tr>
<tr>
<td>% (SEN_HOST_SNMP_COMMUNITY)</td>
<td>SNMP community set for the SNMP Agent on the targeted host.</td>
</tr>
<tr>
<td>% (SEN_HOST_SYSTEMTYPE)</td>
<td>Operating system type of the targeted host.</td>
</tr>
<tr>
<td>% (SEN_HOSTNAME)</td>
<td>Name of the monitored host as provided in the GUI.</td>
</tr>
<tr>
<td>% (SEN_INFORMATION)</td>
<td>Provides additional information about the problem/alert.</td>
</tr>
<tr>
<td>% (SEN_INFORMATIONONELINE)</td>
<td>Provides additional information about the problem/alert in a single line.</td>
</tr>
<tr>
<td>% (SEN_NEWLINE)</td>
<td>Inserts carriage return.</td>
</tr>
<tr>
<td>% (SEN_OBJECT_CLASS)</td>
<td>Class name of the object to which the alert action belongs.</td>
</tr>
<tr>
<td>% (SEN_OBJECT_ID)</td>
<td>PATROL ID of the object triggering the alert.</td>
</tr>
<tr>
<td>General Macros</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>%{SEN_OBJECT_LABEL}</td>
<td>Display name of the object triggering the alert.</td>
</tr>
<tr>
<td>%{SEN_OBJECT_TYPE}</td>
<td>Type of the object triggering the alert (&quot;Process&quot;, &quot;String&quot;, etc.).</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_ALARM1MAX}</td>
<td>Alarm1 maximum range of the parameter triggering the alert.</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_ALARM1MIN}</td>
<td>Alarm1 minimum range of the parameter triggering the alert.</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_ALARM1NTIMES}</td>
<td>Number of consecutive times the parameter triggering the alert must have a value within the alarm1 range before the alert occurs.</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_ALARM1TYPE}</td>
<td>Alarm alert type of the parameter triggering the alert (OK, WARN, ALARM).</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_ALARM2MAX}</td>
<td>Alarm2 maximum range of the parameter triggering the alert.</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_ALARM2MIN}</td>
<td>Alarm2 minimum range of the parameter triggering the alert.</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_ALARM2NTIMES}</td>
<td>Number of consecutive times the parameter triggering the alert must have a value within the alarm2 range before the alert occurs.</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_ALARM2TYPE}</td>
<td>Alarm2 alert type of the parameter triggering the alert (OK, WARN, ALARM).</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_BORDERMAX}</td>
<td>Border maximum range of the parameter triggering the alert.</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_BORDERMIN}</td>
<td>Border minimum range of the parameter triggering the alert.</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_BORDERNTIMES}</td>
<td>Number of consecutive times the parameter triggering the alert must have a value outside the border range before the alert occurs.</td>
</tr>
<tr>
<td>% {SEN_PARAMETER_BORDERTYPE}</td>
<td>Border alert type of the parameter triggering the alert (OK, WARN, ALARM).</td>
</tr>
<tr>
<td>%{SEN_PARAMETER_NAME}</td>
<td>Name of the parameter triggering the alert.</td>
</tr>
<tr>
<td>%{SEN_PARAMETER_STATUS}</td>
<td>Status of the parameter.</td>
</tr>
<tr>
<td>%{SEN_PARAMETER_VALUE}</td>
<td>Value of the parameter triggering the alert.</td>
</tr>
<tr>
<td>%{SEN_PARENT_&lt;macro-name-without-SEN_&gt;}</td>
<td>Gets the parent object's macro. The name of the parent's macro is copied in the syntax without the SEN_.</td>
</tr>
<tr>
<td>General Macros</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Example: In the case of String Search performed on a Command Line (parent) output, to read the full output from the alert action in LastMatchingLines, we need to read parent's %{SEN_RESULT}, which can be accessed using %{SEN_PARENT_RESULT}.</td>
</tr>
<tr>
<td>%{SEN_PARENT_CLASS}</td>
<td>Class name of the parent object to which the alert action belongs.</td>
</tr>
<tr>
<td>%{SEN_PARENT_ID}</td>
<td>PATROL identifier of the object's parent.</td>
</tr>
<tr>
<td>%{SEN_PARENT_LABEL}</td>
<td>Display name of the object's parent.</td>
</tr>
<tr>
<td>%{SEN_PARENT_TYPE}</td>
<td>Type of the object's parent. (&quot;File&quot;, &quot;CommandLine&quot;, etc.).</td>
</tr>
<tr>
<td>%{SEN_PASSWORD}</td>
<td>Encrypted password of the targeted host.</td>
</tr>
<tr>
<td>%{SEN_RESULT}</td>
<td>Query result received for the monitored object during data collection, when available.</td>
</tr>
<tr>
<td>% (SEN_STATUSINFORMATION)</td>
<td>Provides further explanation for the Status parameter.</td>
</tr>
<tr>
<td>%{SEN_TIME:&lt;date-time-format&gt;}</td>
<td>Time of the alert action with a configurable time format as described in the Format Symbols chapter. Example: %{SEN_TIME:%H%M%S} may read 094517 at run time.</td>
</tr>
<tr>
<td>%{SEN_USERNAME}</td>
<td>Username to use to connect to the targeted host.</td>
</tr>
<tr>
<td>%{/...}</td>
<td>FOR ADVANCED USERS ONLY</td>
</tr>
<tr>
<td></td>
<td>Provides an internal instance variable name to be inserted. The path is relative to the object triggering the alert. Example: %{/worstParam} will contain the name of the worst parameter on this instance, which is an application instance built-in variable (see the &quot;PATROL Script Language Reference&quot; document).</td>
</tr>
</tbody>
</table>
Object Specific Macros

The macros listed in the tables below can be used with alert actions specifically for their respective object type.

Command Line Macros

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{SEN_COMMANDLINE}</td>
<td>Command line being executed and analyzed.</td>
</tr>
<tr>
<td>%{SEN_EXITSTATUSCODE}</td>
<td>Exit status returned by the system after executing the command.</td>
</tr>
</tbody>
</table>

Database Macros

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{SEN_DATABASENAME}</td>
<td>Name of the database the SQL query is sent to. May be the database name for SQL Server, or the Oracle SID for Oracle.</td>
</tr>
<tr>
<td>%{SEN_DATABASETYPE}</td>
<td>Type of the database.</td>
</tr>
<tr>
<td>%{SEN_QUERY}</td>
<td>SQL statement sent for execution.</td>
</tr>
</tbody>
</table>

Dynamic Objects Macro

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{SEN_EXTRACTEDLINE}</td>
<td>Returns the output of the dynamic object.</td>
</tr>
</tbody>
</table>

File Macros

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{SEN_FILENAME}</td>
<td>Name of the monitored file as entered in the GUI.</td>
</tr>
<tr>
<td>%{SEN_MONITOREDFILE}</td>
<td>Current file being monitored.</td>
</tr>
</tbody>
</table>

File System Macro

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{SEN_FILESYSTEM}</td>
<td>Name of the monitored file system.</td>
</tr>
</tbody>
</table>

Folder Macros
### Specifying Alert Actions

#### Monitoring Studio KM for PATROL 9.0.00

**Macro** | **Description**
--- | ---
`%{SEN_FOLDER}` | Folder being monitored.
`%{SEN_OLEDESTFILESNDFOLDER}` | Name of the oldest file in the folder.

**Group Macros**

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%{SEN_GROUP_CLASS}</code></td>
<td>Class name of the Monitor Group.</td>
</tr>
<tr>
<td><code>%{SEN_GROUP_COLLECTIONERRORS}</code></td>
<td>List of collection errors that occurred between the current collect and the previous one.</td>
</tr>
<tr>
<td><code>%{SEN_GROUP_CONTACT}</code></td>
<td>Contact information in case of a Group failure.</td>
</tr>
<tr>
<td><code>%{SEN_GROUP_DESCRIPTION}</code></td>
<td>Description of the Group.</td>
</tr>
<tr>
<td><code>%{SEN_GROUP_ID}</code></td>
<td>PATROL ID of the Group triggering the alert.</td>
</tr>
<tr>
<td><code>%{SEN_GROUP_LABEL}</code></td>
<td>Display name of the Group triggering the alert action.</td>
</tr>
<tr>
<td><code>%{SEN_GROUP_TYPE}</code></td>
<td>Type of the Group triggering the alert (&quot;Group&quot;).</td>
</tr>
</tbody>
</table>

**Host Macros**

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%{SEN_AVAILABILITYCHECKS}</code></td>
<td>List of availability checks, separated by commas.</td>
</tr>
<tr>
<td><code>%{SEN_CREDENTIALS_LIST}</code></td>
<td>List of credentials, separated by commas.</td>
</tr>
<tr>
<td><code>%{SEN_SIGNATUREFILES}</code></td>
<td>List of signatures files, separated by commas.</td>
</tr>
<tr>
<td><code>%{SEN_TCP_PORT}</code></td>
<td>Port number used for the TCP availability check.</td>
</tr>
</tbody>
</table>

**Multi-Parameter Formula Macro**

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%{SEN_FORMULA}</code></td>
<td>User-defined formula used to calculate the parameter value.</td>
</tr>
</tbody>
</table>

**Process Macros**

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%{SEN_COMMANDLINE}</code></td>
<td>Process command line being searched for, as entered in the GUI.</td>
</tr>
<tr>
<td><code>%{SEN_MATCHINGPROCESSES}</code></td>
<td>List of all matching processes.</td>
</tr>
<tr>
<td><code>%{SEN_PID_FILE}</code></td>
<td>Path to the PID file whose corresponding process is being monitored.</td>
</tr>
<tr>
<td><code>%{SEN_PROCESSNAME}</code></td>
<td>Process name being searched for, as entered in the GUI.</td>
</tr>
</tbody>
</table>
### Specifying Alert Actions

#### Monitoring Studio KM for PATROL 9.0.00

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%{SEN_USERID}</code></td>
<td>Process user ID being searched for, as entered in the GUI.</td>
</tr>
<tr>
<td><code>%{SEN_WORSTPROCESS_COMMANDLINE}</code></td>
<td>Command line of the first worst process.</td>
</tr>
<tr>
<td><code>%{SEN_WORSTPROCESS_NAME}</code></td>
<td>Name of the first worst process.</td>
</tr>
<tr>
<td><code>%{SEN_WORSTPROCESS_PID}</code></td>
<td>PID of the first worst process.</td>
</tr>
<tr>
<td><code>%{SEN_WORSTPROCESS_PPID}</code></td>
<td>PPID of the first worst process.</td>
</tr>
<tr>
<td><code>%{SEN_WORSTPROCESS_STATE}</code></td>
<td>State of the first worst process.</td>
</tr>
<tr>
<td><code>%{SEN_WORSTPROCESS_USERNAME}</code></td>
<td>Username of the first worst process.</td>
</tr>
<tr>
<td><code>%{SEN_WORSTPROCESSES}</code></td>
<td>List of worst processes, semicolon delimited, containing PID, process name, username, PPID, state and command line.</td>
</tr>
</tbody>
</table>

#### SNMP Polling Macros

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%{SEN_CONTENT}</code></td>
<td>Value of the OID being polled.</td>
</tr>
<tr>
<td><code>%{SEN_OID}</code></td>
<td>SNMP OID being polled.</td>
</tr>
</tbody>
</table>

#### SNMP Trap Macros

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%{SEN_CONTENT}</code></td>
<td>Content of the found trap.</td>
</tr>
<tr>
<td><code>%{SEN_ENTERPRISEID}</code></td>
<td>Enterprise ID (OID) of the SNMP traps being looked for.</td>
</tr>
<tr>
<td><code>%{SEN_FOUNDIP}</code></td>
<td>Actual originating IP address of the trap that has been received.</td>
</tr>
<tr>
<td><code>%{SEN_FOUNDTRAPNUMBER}</code></td>
<td>Actual SNMP trap number that has been received and matches the entered criteria.</td>
</tr>
<tr>
<td><code>%{SEN_TRAPNUMBER}</code></td>
<td>SNMP Trap numbers (specific numbers) being looked for.</td>
</tr>
</tbody>
</table>

#### String Search Macros

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%{SEN_LASTMATCHINGLINE}</code></td>
<td>Last line that matches with the String search criteria.</td>
</tr>
<tr>
<td><code>%{SEN_LASTMATCHINGLINES}</code></td>
<td>Last 10 lines that match with the String search criteria.</td>
</tr>
<tr>
<td><code>%{SEN_STRING1}</code></td>
<td>First regular expression being searched for.</td>
</tr>
<tr>
<td><code>%{SEN_STRING2}</code></td>
<td>Second regular expressions being searched for.</td>
</tr>
</tbody>
</table>

#### WBEM Query Macros

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%{SEN_NAMESPACE}</code></td>
<td>Namespace of the WBEM query.</td>
</tr>
<tr>
<td>Macros</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>%{SE N_QUERY}</td>
<td>WBEM statement sent for execution.</td>
</tr>
</tbody>
</table>

**Web Request Macros**

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{SE N_HTTPMETHOD}</td>
<td>GET or POST depending on what was selected in the GUI.</td>
</tr>
<tr>
<td>%{SE N_URL}</td>
<td>URL being tested.</td>
</tr>
</tbody>
</table>

**WMI Macros**

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{SE N_NAMESPACE}</td>
<td>Namespace of the WMI query.</td>
</tr>
<tr>
<td>%{SE N_QUERY}</td>
<td>WMI statement sent for execution.</td>
</tr>
</tbody>
</table>

**Windows Event Macros**

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{SE N_CONTENT}</td>
<td>Message content of the last matching event.</td>
</tr>
<tr>
<td>%{SE N_EVENTID}</td>
<td>ID of the Windows events being searched for.</td>
</tr>
<tr>
<td>%{SE N_EVENTLOG}</td>
<td>Name of the Windows event log being monitored.</td>
</tr>
<tr>
<td>%{SE N_MATCHINGEVENTS}</td>
<td>List of matching events.</td>
</tr>
<tr>
<td>%{SE N_PROVIDER}</td>
<td>Windows Event source whose new entries are monitored.</td>
</tr>
<tr>
<td>%{SE N_RECORDNUMBER}</td>
<td>Last matching event record number</td>
</tr>
</tbody>
</table>

**Windows Performance Macros**

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{SE N_PERFORMANCECOUNTER}</td>
<td>Windows performance counter being monitored.</td>
</tr>
<tr>
<td>%{SE N_PERFORMANCEINSTANCE}</td>
<td>Windows performance object instances being monitored.</td>
</tr>
<tr>
<td>%{SE N_PERFORMANCEOBJECT}</td>
<td>Windows performance object name being monitored.</td>
</tr>
</tbody>
</table>

**Windows Service Macro**

<table>
<thead>
<tr>
<th>Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%{SE N_SERVICENAME}</td>
<td>Name of the service of an Windows service class.</td>
</tr>
</tbody>
</table>
Format Symbols for %{SEN_TIME:...} Macros

The following table recapitulates all of the time formats available in the %{SEN_TIME:...} and %{SEN_LASTTIME:...} macros in the Command Line execution wizard, the File monitoring and analysis wizard, and the Alert Actions wizard.

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%%</td>
<td>This symbol allows you to use a percent sign (%) in the format of a date string</td>
</tr>
<tr>
<td>%a</td>
<td>Locale's abbreviated name of the day of week</td>
</tr>
<tr>
<td>%A</td>
<td>Locale's full name of the day of week</td>
</tr>
<tr>
<td>%b</td>
<td>Locale's abbreviated name of the month</td>
</tr>
<tr>
<td>%B</td>
<td>Locale's full name of the month</td>
</tr>
<tr>
<td>%c</td>
<td>Locale's appropriate date and time representation</td>
</tr>
<tr>
<td>%C</td>
<td>Data and time as %c</td>
</tr>
<tr>
<td>%d</td>
<td>Day of month [1,31]; single digits are preceded by 0</td>
</tr>
<tr>
<td>%D</td>
<td>Date as %m/%d/%y</td>
</tr>
<tr>
<td>%e</td>
<td>Day of month [1,31]; single digits are preceded by a space</td>
</tr>
<tr>
<td>%h</td>
<td>Locale's abbreviated name of the month</td>
</tr>
<tr>
<td>%H</td>
<td>Hour (24-hour clock) [0,23]; single digits are preceded by 0</td>
</tr>
<tr>
<td>%I</td>
<td>Hour (12-hour clock) [1,12]; single digits are preceded by 0</td>
</tr>
<tr>
<td>%j</td>
<td>Day of year [1,366]; single digits are preceded by 0</td>
</tr>
<tr>
<td>%k</td>
<td>Hour (24-hour clock) [0,23]; single digits are preceded by a space</td>
</tr>
<tr>
<td>%l</td>
<td>Hour (12-hour clock) [1,12]; single digits are preceded by a space</td>
</tr>
<tr>
<td>%m</td>
<td>Month as a decimal number [1,12]; single digits are preceded by 0</td>
</tr>
<tr>
<td>%M</td>
<td>Minute [0,59]; leading zero is permitted but not required</td>
</tr>
<tr>
<td>%n</td>
<td>Insert a new line</td>
</tr>
<tr>
<td>%p</td>
<td>Locale's equivalent of either a.m. Or p.m.</td>
</tr>
<tr>
<td>%r</td>
<td>Appropriate time representation in 12-hour clock format with %p</td>
</tr>
<tr>
<td>%R</td>
<td>Time as %H:%M</td>
</tr>
<tr>
<td>%S</td>
<td>Seconds [0,61]</td>
</tr>
<tr>
<td>%t</td>
<td>Insert a tab</td>
</tr>
<tr>
<td>%T</td>
<td>Time as %H:%M:%S</td>
</tr>
<tr>
<td>%u</td>
<td>Day of week as a decimal number [1,7], with 1 representing Monday</td>
</tr>
<tr>
<td>%U</td>
<td>Week of the year as a decimal number [0,53], with Sunday as the first day of week 1</td>
</tr>
<tr>
<td>%V</td>
<td>Week of the year as a decimal number [01,53], with Monday as the first day of the week</td>
</tr>
</tbody>
</table>

If the week containing 1 January has four or more days in the new year, then it is considered week 1; otherwise, it is week 53 of the previous year, and the next week is, week 1.
<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%w</td>
<td>Day of week as a decimal number [0,6], with 0 representing Sunday</td>
</tr>
<tr>
<td>%W</td>
<td>Week of the year as a decimal number [0,53], with Monday as the first day of week 1</td>
</tr>
<tr>
<td>%x</td>
<td>Locale's appropriate date representation</td>
</tr>
<tr>
<td>%X</td>
<td>Locale's appropriate time representation</td>
</tr>
<tr>
<td>%y</td>
<td>Year within century [0,99]</td>
</tr>
<tr>
<td>%Y</td>
<td>Year, including the century (for example 1993)</td>
</tr>
<tr>
<td>%z</td>
<td>Abbreviated or full name of time zone, or no bytes if no information of the time zone exists</td>
</tr>
<tr>
<td>%E</td>
<td>Locale's alternative appropriate date and time representation</td>
</tr>
<tr>
<td>%EC</td>
<td>Name of the base year (period) in the locale's alternative representation</td>
</tr>
<tr>
<td>%EX</td>
<td>Locale's alternative date representation</td>
</tr>
<tr>
<td>%Ey</td>
<td>Locale's alternative time representation</td>
</tr>
<tr>
<td>%Ey</td>
<td>Offset from %EC (year only) in the locale's alternative representation</td>
</tr>
<tr>
<td>%EY</td>
<td>Alternative representation of the year in full</td>
</tr>
<tr>
<td>%Od</td>
<td>Day of the month using the locale's alternative numeric symbols</td>
</tr>
<tr>
<td>%Oe</td>
<td>Same as %Od</td>
</tr>
<tr>
<td>%OH</td>
<td>Hour (24-hour clock) using the locale's alternative numeric symbols</td>
</tr>
<tr>
<td>%OI</td>
<td>Hour (12-hour clock) using the locale's alternative numeric symbols</td>
</tr>
<tr>
<td>%OM</td>
<td>Month using the locale's alternative numeric symbols</td>
</tr>
<tr>
<td>%OM</td>
<td>Minutes using the locale's alternative numeric symbols</td>
</tr>
<tr>
<td>%OS</td>
<td>Seconds using the locale's alternative numeric symbols</td>
</tr>
<tr>
<td>%OU</td>
<td>Week of the year (Sunday as the first day of the week) using the locale's alternative numeric symbols</td>
</tr>
<tr>
<td>%OW</td>
<td>Day of week (Sunday=0) using the locale's alternative numeric symbols</td>
</tr>
<tr>
<td>%OW</td>
<td>Week of the year (Monday as the first day of the week) using the locale's alternative numeric symbols</td>
</tr>
<tr>
<td>%Oy</td>
<td>Year (offset from %C) in the locale's alternative representation and using the locale's alternative numeric symbols</td>
</tr>
</tbody>
</table>
Alert Actions Example

In this example, we monitor a log file and look for the string "error" in the lines. Every time an "error" is found, we want to trigger a standard PATROL event containing the name of the parameter, the name of the log file, the content of the line that triggered the alert and the name of the technology.

Before setting the alert action, you will first have to make sure that the thresholds for the MatchingLineCount Parameter is set to 1. To do so:
1. Right-click the String Search icon and select Thresholds...

2. Select the MatchingLineCount parameter and click Next.
3. Verify that an alarm is triggered if the value is greater than 1 and execute the Alert Actions "every time a matching line is found".
4. Click Set thresholds.

To Set the Alert Action
1. Right-click the String Search icon and select the Alert Actions... command from the menu to run the Alert Actions wizard:

   ![Alert Actions wizard](image)

   Selecting the MatchingLineCount Parameter

3. Select the MatchingLineCount parameter and click Next.
4. Select the type of action to be executed when the MatchingLineCount parameter goes into alert state:
   - Check the Trigger an event box and click Next.
   - Enter the message of the event: Name of the Group ; Name of the log file ; The error message (i.e. the line in the log file that triggered the alert)
   - Enter the text below in the box called Enter the text to be sent with the event:

   ```
   %{SEN_GROUP_LABEL}: error found in %{SEN_PARENT_LABEL}.%{SEN_NEWLINE}Error message: %{SEN_LASTMATCHINGLINE}%{SEN_GROUP_LABEL} contains the Group display name in the PATROL Console.
   %{SEN_PARENT_LABEL} contains the log file display name (it is the parent of the String search in the PATROL Console).
   %{SEN_NEWLINE} will create a new line in the message.
   %{SEN_LASTMATCHINGLINE} contains the entire line in the log file that triggered the alert.
   ```
Specifying Alert Actions

Setting the Alert Parameters

The text sent with the event will look like this:

```
Group: Lync: error found in Log File: C:\Program Files\Lync\Lync_Error.log
Error message: server connection error - main server is down.
```

5. Click the **Next** button to get to the final panel of the Alert Actions wizard that summarizes the Alert Actions set for the **MatchingLineCount** parameter.

In this example you just set one Alert Action, **Trigger an event**, but it would have been possible to set several Alert Actions, such as a command line that runs a recovery action for the monitored application or writes an annotation to the graph built by the **MatchingLineCount** parameter with the content of the matching line.
Setting Credentials

For security purpose, some technologies may require additional privileges to allow access to their data. In this case, Monitoring Studio enables users to:

- Set new Specific Credentials
- Modify existing Specific Credentials
- Delete existing Specific Credentials

⚠️ System Credentials cannot be edited or deleted using the below menu commands. Use the "Edit" menu command from the Host icon to edit System Credentials.

To add new credentials:

1. Right-click the Host icon > KM Commands > Credentials > New Credentials...

2. Current Credentials: Click this button to display the list of previously configured credentials.

3. Provide the following information:
   - **Username**: Enter the username on the target host.
   - **Password**: Enter the corresponding password for the user.
   - **(Optional) Label**: Enter the label for the new credentials.

⚠️ If no label is provided, the username will be used as the label and set by the credentials wizard.
4. Click **OK**. The new credentials are successfully added and ready to use.

To edit credentials:

1. Right-click the **Host icon > KM Commands > Credentials > Edit Credentials...**

2. Select the Credentials to edit from the drop-down list and click **Next**.
3. **Monitors using these credentials:** Click this button to see which Monitor(s) is/are currently using these Credentials.

4. Modify the following information:
   - **Username:** Edit the username on the target host.
   - **Password:** Edit the corresponding password for the user.
   - **(Optional) Label:** Edit the label for the new credentials.

5. Click **Finish** to validate your changes.

**To delete credentials:**

1. Right-click the **Host icon > KM Commands > Credentials > Delete Credentials...**

![Delete Credentials](image)

2. Select the Credentials to delete from the drop-down list and click **Next**.

   ![](image)  
   *Credentials that are currently being used by any Monitor cannot be deleted.*
3. Click Finish to confirm and permanently delete the selected Credentials.
Setting the Discovery Interval

By default, Monitoring Studio performs a discovery every hour to create, modify, and update monitored objects, if necessary. However, you can easily change the default discovery interval to meet your specific needs.

1. Right-click the Monitoring Studio icon > KM commands > KM Settings > Discovery Interval...

2. Use the spin button to customize the discovery interval from once every 5 minutes to once every 24 hours.

3. Click OK to save your settings.

You can also force a discovery manually by right-clicking on the Monitoring Studio icon > KM Commands > Trigger a KM Discovery.
Setting the Polling Interval

A polling interval defines how often new data is collected. A new collect can be performed from once every second, to once in a week. Polling intervals can be set for objects created by Monitoring Studio that collect data (files, processes, command lines, SNMP polling, etc.). By default, the polling interval is set to 2 minutes on all objects, which can be modified at any time.

⚠️ The option to set polling intervals is not available for String Searches, Numeric Values, Text Pre-Processing, Monitor Groups, and SNMP Trap instances, since either they do not have collectors, or as in the case of SNMP Traps – have collectors that react to events.

To set the polling interval:

1. In the PATROL Console, right-click the object icon > KM commands > Polling Interval...
2. Configure the polling interval options:
   - **Collect every: x hours x minutes x seconds**: Set the polling interval in hours, minutes, and seconds.
   - **Collect once a day at: x hours (24 hours) x minutes x seconds**: Here the values selected indicate the time of day. Example: 14 hours 30 minutes 0 seconds would mean that the polling is done only once a day at 2:30pm (14:30 hrs)
   - **Collect once a week on <weekday> at: x hour x minutes x seconds**: Here the values selected indicate the time of the selected weekday. Example: Monday at 14 hours 30 minutes 0 seconds would mean that the polling is done only once a week on Mondays at 2:30pm (1430 hrs)
3. (For File Systems/Processes/Windows Events only) Monitoring Studio relies on a cache mechanism to share the information among the Monitors in order to use as little resources as possible on the target Host and over the network. The cache will be refreshed if one of the Monitors needs to collect data (polling interval reached) and the cache is older than the selected minimum cache refresh. Configure the cache refreshing frequency:
   - **Minimum File System/Process/Windows Event cache refresh interval**: Use the spin button to set the minimum number of seconds Monitoring Studio must wait before refreshing the cache. Default is 15 seconds.
4. Click **OK** to validate your changes.
Visualizing Currently Running Processes

The Process Viewer tool displays all the processes that are currently running on a host as well as their characteristics to help you monitor them in the most efficient way.

To access the Process Viewer tool:

1. Right-click the desired Host instance > KM commands > Tools > Process Viewer...

2. Click:
   - **Update** to refresh the process list
   - **Close** to close the Process Viewer tool.

The Process Viewer tool uses the system credentials provided during Host configuration.
Visualizing SNMP Traps

For localhost monitoring, the **Real-time SNMP Trap Listener** tool allows you to visualize all of the SNMP traps and their characteristics received by the PATROL Agent and Monitoring Studio. This tool is particularly helpful when you want to setup a SNMP Trap listening object in Monitoring Studio but you ignore the characteristics of the traps you want to detect.

To access the **SNMP Trap Listener** tool:

1. Right-click the main **Monitoring Studio icon > KM commands > Tools > Real-time SNMP Trap Listener**.
   - The incoming SNMP traps are shown in this window as soon as they arrive.
   - You can view their main characteristics (originating IP address, community, Enterprise OID, and trap specific number) as well as their attached varbinds (variable bindings). This will help you specify the search criteria in the **SNMP Trap Listening** wizard.
   - The newest (or latest arrived) trap is shown first in the list.
2. **Pause** if you wish to stop the reception of traps and have more time to analyze the characteristics of the previously arrived traps.
3. **Resume** to resume the listening.
4. **Close** to quit the tool window.

⚠️ Due to an SNMP protocol limitation, it is not possible to have more than one program on one computer listening to SNMP traps (handling the UDP/162 port). If another program is listening to SNMP traps, Monitoring Studio is not able to listen for SNMP traps and an error message is shown. For the same reason, it is not possible to use this tool and listen for SNMP traps from a Monitoring Studio object in the PATROL Console. It may just be one or the other.
Visualizing a Host Windows Event Log

The **Windows Event Log Reader** tool displays all Windows Events registered in a specific event log during the last selected period. It helps to identify the provider, event ID and event level for configuring **Windows Event Log** Monitors.

To access the **Windows Event Log Reader** tool:

1. Right-click the desired **Host icon** > **KM commands** > **Tools** > **Windows Event Log Reader**...

2. Select the Event log and the time span you wish to view, and click the **Update** button to refresh the window. This may take a few seconds to retrieve the events from the host. They are displayed in the order they are registered.

3. Click:
   - **Update** to refresh the information displayed.
   - **Close** to quit the **Windows Event log Reader** tool.

*The Windows Event Log Reader tool uses the system credentials provided during Host configuration.*
Visualizing a Monitored File Content

Administrators can use the File Viewer tool to check the content of a file that is being monitored:

1. Right-click the Host icon > KM commands > Tools > File Viewer... or the File icon > KM commands > View File Content
2. Specify the visualization options:
   - **File path**: Path of the file that you wish to view
   - **Show me**: The first/last: x KB: Indicate the size and part of the file that you wish to view
   - **Only the lines matching with**: (optional regular expression) Enter a regular expression and only the lines matching this regular expression are displayed in the File content field.

![File Viewer](image)

3. Click **Update**. The file content is now displayed.
4. Click **Close**.

   If the tool is accessed from File object, the File Viewer tool uses the credentials assigned to the File Monitor; if this tool is accessed from the Host icon, the System Credentials configured for the Host are used.
Visualizing Properties

Administrators can use the **Properties** KM command to display a Configuration Report for the monitored object of their choice at a given instant. This tool can be used to verify the configuration of a monitored object and all its children objects.

To visualize properties:

1. In the PATROL Console, right-click the **object** icon > **KM commands** > **Properties** or the Monitoring Studio icon > **KM Commands** > **Configuration** > **Show Configuration**...

![Monitoring Studio Configuration Report]

A new task window opens and displays the Monitoring Studio Configuration Report.
Visualizing SNMP Agent Variables

The SNMP Browser tool allows you to easily visualize the variables (OID and values) available in an SNMP agent. This tool is very useful to identify which OID you need to poll in the SNMP Polling wizard.

🌟 It is recommended to turn off the debug mode when using this KM Command.

To set the SNMP Browser tool:

1. Right-click a Host icon > KM commands > Tools > SNMP Browser
2. **Start SNMP walking from this root OID**: Specify the root OID from which you want to perform a SNMP walk
3. Click the **Update** button. If the information entered is correct, the result of the SNMP walk is shown a few seconds later. If not, an error message is displayed with additional information about the failure. You can use the same settings when you setup a new SNMP Polling object in Monitoring Studio

⚠️ Performing an SNMP walk on a remote SNMP agent that has a large amount of variables may take a long time.

6. Click **Close** to quit the SNMP Browser tool.
Troubleshooting
This section provides some troubleshooting guidelines for Monitoring Studio. It describes how the KM debugging can be enabled to diagnose any issues and then states the most frequently asked questions based on issues encountered by customers.

### Enabling the Debug Mode

If you encounter an issue, and want to report it to Sentry Software, you will be asked to enable the **Debug Mode** and provide the debug output to the Sentry Software support team.

To enable the debug mode:

1. Right-click the main Monitoring Studio icon > KM Commands > KM Settings > Debug...

![Debug Mode dialog box]

2. Check the **Enable debug mode** box.

3. By default, the debug output is displayed in the PATROL Console System Output Window (SOW). If you want the debug information to be saved in a file on the computer where the PATROL Agent is running, specify the debug output file path. It is recommended to use a debug output file, if you are intending to send it to the Sentry Support team. The debug output file will allow you to:
   - have debug information about the discovery process since debug information about the discovery process may be lost by the PATROL Console during the PATROL Agent startup.
   - trace the activity of Monitoring Studio for a few minutes since information may also be lost by the PATROL Console if its buffer is full.
The debug capturing in SOW can be affected if the Console connection is lost while debugging. If the debug data exceeds the SOW buffer size, it will be trimmed and debug data will not be complete.

4. Specify the maximum file size.

Please note that the debug output file size may quickly become very large if you selected the "Unlimited" option. It is therefore recommended to turn off the debug mode once the required information has been collected.

5. Click OK.
Frequently Asked Questions and Problems

How Do I Know Which Version of Monitoring Studio I Am Running?

To find out which version of Monitoring Studio KM for PATROL you are running, right-click the main Monitoring Studio icon > KM Commands > About... The Monitoring Studio version and release date are displayed in the dialog box that pops up.

To know if your version of Monitoring Studio is up-to-date, please check the BMC Software Web site at www.bmc.com or the Sentry Software Web site at www.sentrysoftware.com for the latest information and product versions if the "Unlimited" option has been selected.

Although SNMP Trap Listening Seems to Work, No Trap Matches My Criteria

Use the built-in SNMP Trap Listener tool of Monitoring Studio to visualize the incoming traps and their characteristics. Verify the originating IP address and the community used to generate the trap.

Check that the SNMP agent that generates the traps is properly configured to send them to the computer, where Monitoring Studio and the PATROL Agent are running.

Monitoring Studio Is Unable to Listen to SNMP Traps

Because of SNMP protocol limitations, it is not possible to have several programs listening to SNMP traps on the same computer (at least on the same network interface). Only one program can listen to the UDP/162 port for incoming SNMP traps.

If you have another program that is listening to SNMP traps, Monitoring Studio will not be able to listen to incoming SNMP traps.

Please stop any other program that listens to SNMP traps (typically the SNMP Traps Windows service).
Can I Monitor the Processor Time Usage Made by a Windows Service?

You cannot directly monitor the processor time usage of a Windows service.

1. First identify the process (its characteristics) that corresponds to this process
2. Then, simply add the monitoring of this process with the Process monitoring wizard

⚠️ It can be difficult to identify the process associated to a given Windows service because one single program can handle/host several Windows services and one program (e.g. svchost.exe)

Monitoring Studio Reads My Log File Entirely

If you erroneously selected the flat file option when you actually wanted to monitor a log file, you will have to redo the whole configuration: create a new file monitoring and choose the log file option, and then copy and paste the String and Numeric Value searches from your previous file monitoring to the new one.

It is very important to properly configure a file monitoring by first indicating the type of the file being monitored: flat or log.

- A flat file is updated entirely and so must be read entirely, at each poll.
- In log files, new lines are appended at the end of the file. Only these new lines need to be analyzed.

Monitoring Studio Does Not Update All of My Folder Monitoring Parameters

If a folder monitored by Monitoring Studio contains more than 1000 files, Monitoring Studio automatically reduces its features and stops collecting most parameters to avoid excessive resource consumption.

This limit can be changed by setting the folderLimit variable either at the global level (/SENTRY/STUDIO/folderLimit) or at the host level (/SENTRY/STUDIO/<hostID>/folderLimit), with host level taking precedence. (if not manually changed, the default is 1000).
I'm Unable to Poll an SNMP Agent (Getting a Warning)

Please check the IP address or, if you use a hostname, that the hostname can be resolved.

Check the community and ensure that the SNMP agent that is running on the target computer uses SNMP v1 and matches what has been set in Monitoring Studio.

Use a MIB Browser utility to identify the OID that matches your needs.

You can also use the built-in SNMP Browser tool of Monitoring Studio to check your settings:
Right-click on a Host icon > KM commands > Tools > SNMP Browser.

I'm Unable to See the Monitoring Studio Icons in PATROL Central

In order to have the Monitoring Studio icons in PATROL Central, you need to install Monitoring Studio on the Agents (managed systems) as well as on the Console Server.

Please read the Monitoring Studio Installation Guide for more information about how to setup Monitoring Studio.

Infinite Loop Reported in the PATROL Agent Log

In some cases, the PATROL Agent may report a possible infinite loop in its log file (*.errs) or in the System Output Window in the PATROL Console, as in the following:

Tue May 4 17:12:28 2004 PatrolAgent-W-EUSER: PSL script 'fileColl', 'File: myLogFile.LOG', 'myApp#myLogFileLOG' may be in an infinite loop - executed 500016 instructions

While this message may be worrying, it is only due to an outdated loop mechanism of the PATROL Agent, as default settings often do not suit the computing power of recent machines.

Monitoring Studio has internal mechanisms, which prevent it from consuming too much processor time (for example, it will not parse more than 8 megabytes of a file at one time, it will not process more than 1,000 files in one folder, etc.).

The loop detection settings of the PATROL Agent can be changed and Sentry Software
Frequently Asked Questions and Problems

Monitoring Studio KM for PATROL 9.0.00 recommends that users set these upper thresholds. This can be achieved by modifying the following configuration variables with WPCONFIG or xpconfig:

- `/AgentSetup/AgentTuning/pslInstructionMax = 1,000,000`
- `/AgentSetup/AgentTuning/pslInstructionPeriod = 1`
- This basically disables the loop detection mechanism of the PATROL Agent

⚠️ Disabling the loop detection mechanism of the PATROL Agent does have a drawback: you will not be able to detect infinite loops in other KMs anymore. Sentry Software recommends that you use this tip only when necessary and that you set the thresholds back to the default if your PATROL Agent does not behave properly.

Is It Possible to Monitor the CPU/Memory Usage of a Process Tree?

Monitoring Studio is able to measure the processor time usage and memory usage of a group of processes like a tree (a main process, its children, etc.).

Monitoring Studio can also count the number of children of the process that match the specified criteria. To do so: Select the **ChildCount** parameter in the Process monitoring wizard.

Monitoring Studio Fails to Connect to a Secured Web Server (SSL) from My UNIX/Linux Server

Monitoring Studio only supports HTTPS queries on Windows.

Monitoring Studio Fails to Authenticate to My Web Server

Some authentication schemes are really complex and will not be supported by Monitoring Studio. The only authentication system supported is the Windows authentication on Microsoft IIS Web server.

The provided credentials must have been given specific access rights and must be allowed to log on to this Web site.

HTML-based authentication (non-HTTP authentication) may be supported in some cases but such systems often require advanced browser features that are not implemented in Monitoring
Monitoring Studio Does Not Follow an HTTP Redirection (Web)

Some HTTP redirections are not implemented as true HTTP redirection (HTTP status codes 300, 301, 302, etc.) but are instead HTML pages with specific meta-tags, or even HTML pages with Javascript code performing the redirection from the browser.

Monitoring Studio only supports true HTTP redirection and does not support other types of redirection that require advanced browser features.

Monitoring Studio Is Not Able to Post a Web Form to My Web Server

Verify that the URL that you entered is not the URL of the page that displays the form to fill in but the URL indicated in the <FORM ACTION="<url>"> tag in the HTML source of this page.

Verify that the names of the variables to post are correct. They are identified by the <INPUT NAME="<variableName>"> and <SELECT NAME="<variableName>"> tags in the HTML source of the page that shows the form to fill in.

The <INPUT TYPE="SUBMIT" NAME="..."> variable may be required for the form to be properly processed by the Web server.
Reference Guide
Introduction

This chapter contains tables describing the parameters used in the KM, grouped by Application Classes, and provides a brief description of each parameter and its default settings. It also gives you some additional information about HTTP authentication, Processes, Regular expressions and WMI.
Application Classes and Parameters

This section lists the application classes of Monitoring Studio KM for PATROL. It gives you details on the icons that represent the class, Infobox, parameters, and the menu commands available for each application class.

If the KM is properly loaded, the following application classes should be loaded on the monitored system and console:

<table>
<thead>
<tr>
<th>Application Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEN_M S_COMMANDLINE</td>
<td>Executes, monitors, and parses command lines and scripts</td>
</tr>
<tr>
<td>SEN_M S_DBQUERY</td>
<td>Executes and monitors database queries</td>
</tr>
<tr>
<td>SEN_M S_DYNAMIC</td>
<td>Creates Dynamic Items</td>
</tr>
<tr>
<td>SEN_M S_DYNAMIC_CONT</td>
<td>Creates a dynamic object container</td>
</tr>
<tr>
<td>SEN_M S_DYNAMICDISCOVERY</td>
<td>Creates a dynamic object builder</td>
</tr>
<tr>
<td>SEN_M S_DYNAMICNUMBER</td>
<td>Performs dynamic numeric value extractions</td>
</tr>
<tr>
<td>SEN_M S_DYNAMICSTRING</td>
<td>Executes dynamic string searches</td>
</tr>
<tr>
<td>SEN_M S_FILE</td>
<td>Monitors files and file content</td>
</tr>
<tr>
<td>SEN_M S_FILESYSTEM</td>
<td>Monitors file systems</td>
</tr>
<tr>
<td>SEN_M S_FOLDER</td>
<td>Monitors directories</td>
</tr>
<tr>
<td>SEN_M S_FORMULA</td>
<td>Monitors values derived from other parameters</td>
</tr>
<tr>
<td>SEN_M S_GROUP</td>
<td>Groups all the hosts</td>
</tr>
<tr>
<td>SEN_M S_HOST</td>
<td>Monitors hosts and allows adding more monitors</td>
</tr>
<tr>
<td>SEN_M S_MAIN</td>
<td>Main application class where groups are created from</td>
</tr>
<tr>
<td>SEN_M S_MONITORGROUP</td>
<td>Monitor Group. Groups monitors within a host</td>
</tr>
<tr>
<td>SEN_M S_NUMBER</td>
<td>Extracts numeric values</td>
</tr>
<tr>
<td>SEN_M S_PROCESS</td>
<td>Monitors processes</td>
</tr>
<tr>
<td>SEN_M S_SNMPOLLING</td>
<td>Polls SNMP devices</td>
</tr>
<tr>
<td>SEN_M S_SNMPTRAP</td>
<td>Listens for SNMP traps</td>
</tr>
<tr>
<td>SEN_M S_STRING</td>
<td>Executes string searches</td>
</tr>
<tr>
<td>SEN_M S_TRANSFORM</td>
<td>Transforms complex (multi-line, HTML, XML) text to enable string/numeric value searches</td>
</tr>
<tr>
<td>SEN_M S_WBEMQUERY</td>
<td>Performs WBEM queries</td>
</tr>
<tr>
<td>SEN_M S_WEBREQUEST</td>
<td>Executes Web requests</td>
</tr>
<tr>
<td>SEN_M S_WINEVENT</td>
<td>Monitors Windows Event logs</td>
</tr>
<tr>
<td>SEN_M S_WINPERF</td>
<td>Monitors Windows Performance counters</td>
</tr>
<tr>
<td>Application Class</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>SEN_MS_WINSERVICE</td>
<td>Monitors Windows Services</td>
</tr>
<tr>
<td>SEN_MS_WMIQUERY</td>
<td>Performs WMI queries</td>
</tr>
</tbody>
</table>
## SEN_MS_COMMANDLINE

### Icon

![Icon](image)

### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Condition(s)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExecutionTime*</td>
<td>Time taken by the command to run. Value set by commandLineColl</td>
<td>seconds</td>
<td>Warning = 30</td>
<td>Response Time</td>
</tr>
<tr>
<td>ExitStatus</td>
<td>Status of the command exit code. Value set by commandLineColl</td>
<td>{0 = Successful ; 1 = Failed}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>Result</td>
<td>Displays the return output of the command. Value set by commandLineColl</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>Status*</td>
<td>Status of the execution. Value set by commandLineColl</td>
<td>{0 = OK ; 1 = Suspicious ; 2 = Failed}</td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management.*

For detailed information about Baselining and KPI, see [Managing Baselines and Key Performance Indicators](#).

### Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the object</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the parent object</td>
</tr>
<tr>
<td>Command Line</td>
<td>Command line that is given to the OS to execute</td>
</tr>
<tr>
<td>Timeout</td>
<td>Maximum time allowed for the command line execution</td>
</tr>
<tr>
<td>Username</td>
<td>Username configured for the command line execution</td>
</tr>
</tbody>
</table>

### Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &gt; String Search</td>
<td>Creates a new String search for this command line execution</td>
</tr>
</tbody>
</table>
### Menu Command | Description
--- | ---
**New > Numeric Value Extraction** | Creates a new numeric values extraction for this command line execution.
**New > Text Pre-Processing** | Creates a new text pre-processing for this command line execution.
**New > Dynamic Object Builder** | Creates a new dynamic object builder for this command line execution.
**Edit** | Edits the command line execution configuration.
**Thresholds** | Sets or edits the thresholds for parameters.
**Polling Interval** | Sets the polling interval for this command line execution.
**Alert Actions** | Adds specific Alert Actions to the command line execution.
**Properties** | Displays all available information for this command line execution.
**Cut** | Cuts this command line execution object and all children for pasting under a host or monitor group.
**Copy** | Copies this command line execution object and all children for pasting under a host or monitor group.
**Paste** | Pastes a previously copied or cut String search or Numeric Value search and all children for pasting under a host or monitor group.
**Delete** | Deletes the command line execution and all its dependent objects.
**Rename...** | Renames the command line execution monitoring object.
**Acknowledge Alerts...** | Acknowledges all alerts and reset parameters to zero.
**Pause Monitoring** | Pauses the command line execution as well as all its dependent objects.
**Resume Monitoring** | Resumes the command line execution as well as all its dependent objects.
**Refresh Parameters** | Re-execute the command line (if needed) and refresh all parameters. All dependent objects will be refreshed as well (SEN_MS_STRING and SEN_MS_NUMBER instances).
SEN_MS_DBQUERY

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExecutionTime*</td>
<td>Displays the SQL query execution time. Value set by dbQueryColl every 2 minutes</td>
<td>seconds</td>
<td>Warning ≥ 15, Alarm ≥ 60</td>
<td>Response Time</td>
</tr>
<tr>
<td>Result</td>
<td>Displays the output of the database query execution. Value set by dbQueryColl every 2 minutes</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>Status</td>
<td>Displays whether or not the query was successfully executed. Value set by dbQueryColl every 2 minutes</td>
<td>{0 = OK; 1 = Suspicious; 2 = Failed}</td>
<td>Warning = 1, Alarm = 2</td>
<td>Availability</td>
</tr>
</tbody>
</table>

For detailed information about Baselining and KPI, see Managing Baselines and Key Performance Indicators.

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management.

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Database query analysis</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Database query's parent</td>
</tr>
<tr>
<td>Database Type</td>
<td>Displays the Database type</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Displays the connection type</td>
</tr>
<tr>
<td>Database Name</td>
<td>Displays the database name</td>
</tr>
<tr>
<td>Connect as</td>
<td>Login used to connect to the database server</td>
</tr>
<tr>
<td>SQL Query</td>
<td>Displays the SQL query that will be executed</td>
</tr>
</tbody>
</table>

Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &gt; String search</td>
<td>Creates a new String search for this Database Query analysis</td>
</tr>
<tr>
<td>Menu Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>New &gt; Numeric Value Extraction</strong></td>
<td>Creates a new Numeric Value extraction for this Database Query analysis</td>
</tr>
<tr>
<td><strong>New &gt; Text Pre-Processing</strong></td>
<td>Creates a new Text pre-processing for this Database Query analysis</td>
</tr>
<tr>
<td><strong>New &gt; Dynamic Object Builder</strong></td>
<td>Creates a new Dynamic Object Builder for this Database Query analysis</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Edits the Database Query monitoring settings</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Sets the polling interval for this Database Query analysis monitoring</td>
</tr>
<tr>
<td><strong>Alert Actions</strong></td>
<td>Adds specific Alert Actions to the Database Query analysis monitoring</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for this Database Query analysis</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this object</td>
</tr>
<tr>
<td><strong>Paste</strong></td>
<td>Pastes a previously copied or cut Database Query analysis object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the Database Query analysis monitoring and all its dependent objects</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Allows you to rename this Database Query analysis monitoring</td>
</tr>
<tr>
<td><strong>Acknowledge Alerts</strong></td>
<td>Acknowledges all alerts and reset parameters to zero</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Pauses the monitoring of this Database Query analysis object</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Resumes the monitoring of this Database Query analysis object</td>
</tr>
<tr>
<td><strong>Refresh Parameters</strong></td>
<td>Refreshes all instance parameters of the SEN_MS_DBQUERY application class</td>
</tr>
</tbody>
</table>
**SEN_MS_DYNAMIC**

**Icon**

![SEN_MS_DYNAMIC Icon](image)

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExtractedLine</td>
<td>Displays the output of the dynamic object</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>Status</td>
<td>Instance missing status. Default pooling interval: 1 minute</td>
<td>{0 = present; 1 = Instance is missing}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management*

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the dynamic object</td>
</tr>
</tbody>
</table>

**Menu Commands**

None
SEN_MS_DYNAMIC_CONT

Icon

Parameters
None

Infobox
None

Menu Commands
None
SEN_MS_DYNAMICDISCOVERY

Icon

Parameters
None

Infobox
None

Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &gt; String Search Template</td>
<td>Creates a new String search template for this File</td>
</tr>
<tr>
<td>New &gt; Numeric Value Extraction Template</td>
<td>Creates a new Numeric Value extraction template for this File</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the File monitoring settings</td>
</tr>
<tr>
<td>Alert actions</td>
<td>Adds specific Alert Actions to the File monitoring</td>
</tr>
<tr>
<td>Remove Missing Items</td>
<td>Removes missing items</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays all available information for this File monitoring object</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this object</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes a previously copied or cut File monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the File monitoring and all its dependent objects</td>
</tr>
<tr>
<td>Rename</td>
<td>Allows you to rename this File monitoring object</td>
</tr>
</tbody>
</table>
SEN_MS_DYNAMICNUMBER

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delta</td>
<td>Displays the difference between values collected during two consecutive pollings</td>
<td>Delta</td>
<td>None</td>
<td>Delta</td>
</tr>
<tr>
<td>DeltaPerSecond</td>
<td>Displays the value corresponding to &quot;Delta&quot; divided by the elapsed time in seconds between the collection times</td>
<td>delta/s</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Value*</td>
<td>Value of the searched Numeric Value (no value will be given if no number is found). Value set by the collector of the parent's object</td>
<td>Value</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>ValueFound</td>
<td>States if a numeric value has been found</td>
<td>{0 = Value found ; 1 = Value not found}</td>
<td>Alarm = 1</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the numeric value extraction</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the numeric value extraction's parent</td>
</tr>
<tr>
<td>Line Mode</td>
<td>Method used to select lines to search for the numeric value</td>
</tr>
<tr>
<td>Column Mode</td>
<td>Method chosen to search and extract the numeric value in the line</td>
</tr>
<tr>
<td>Parameter Type</td>
<td>Type of the parameter</td>
</tr>
<tr>
<td>Line Numbers</td>
<td>Line numbers in which the numeric value will be extracted from</td>
</tr>
<tr>
<td>Regular Expression</td>
<td>Regular expression used to select the lines where the number will be searched for</td>
</tr>
<tr>
<td>Skip Blank Lines</td>
<td>Indicates whether or not blank lines are ignored when searching for the numeric value</td>
</tr>
<tr>
<td>After/Before</td>
<td>Searches for the numeric value either after or before the specified string</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td>Specified String</td>
<td>Searches for the numeric value before or after this specified string</td>
</tr>
<tr>
<td>Character Offset</td>
<td>Character offset where the numeric value is searched for</td>
</tr>
<tr>
<td>Field Number</td>
<td>Field number where the numeric value is extracted from</td>
</tr>
<tr>
<td>Field Separators</td>
<td>Characters that separate the fields in a text line</td>
</tr>
<tr>
<td>Unique Separator</td>
<td>Considers consecutive separators as a single separator</td>
</tr>
</tbody>
</table>
SEN_MS_DYNAMICSTRING

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MatchingLineCount*</td>
<td>Indicate if a matching string has been found. Value set by the collector of the parent object</td>
<td>{0 = No matching string; 1 = Matching string}</td>
<td>Alarm = 1</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC TrueSight Operations Management

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Dynamic String search</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Dynamic String search's parent</td>
</tr>
<tr>
<td>Type</td>
<td>Dynamic String type</td>
</tr>
<tr>
<td>Lines</td>
<td>Lines that are searched</td>
</tr>
<tr>
<td>Run Alert Actions</td>
<td>When Alert Actions have to be executed</td>
</tr>
</tbody>
</table>
SEN_MS_FILE

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exists*</td>
<td>Determines whether the file exists or not. Value set by fileColl</td>
<td>[0 = File exists; 1 = File does not exist]</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>GrowthPercentage</td>
<td>File growth percentage. Value set by fileColl</td>
<td>Percentage per minute (%/min)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>GrowthSpeed</td>
<td>File growth speed. Value set by fileColl</td>
<td>Kilobytes per minute (KB/min)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>LastChanged</td>
<td>Elapsed time since the file was modified. Value set by fileColl</td>
<td>minutes</td>
<td>Warning ≥ 7 200 Alarm ≥ 14 400</td>
<td>Statistics</td>
</tr>
<tr>
<td>Size*</td>
<td>File size. Value set by fileColl</td>
<td>Kilobytes (KB)</td>
<td>Alarm = 0</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC TrueSight Operations Management

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the File monitoring</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of File's parent</td>
</tr>
<tr>
<td>File</td>
<td>Configured file path in the monitor</td>
</tr>
<tr>
<td>Monitored File</td>
<td>Currently monitored file path</td>
</tr>
<tr>
<td>File Type</td>
<td>File type (flat/log) as configured in the monitor</td>
</tr>
</tbody>
</table>
## Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New &gt; String Search</strong></td>
<td>Creates a new String search for this File</td>
</tr>
<tr>
<td><strong>New &gt; Numeric Value Extraction</strong></td>
<td>Creates a new Numeric Value extraction for this File</td>
</tr>
<tr>
<td><strong>New &gt; Text Pre-Processing</strong></td>
<td>Creates a new Text pre-processing for this File</td>
</tr>
<tr>
<td><strong>New &gt; Dynamic Object Builder</strong></td>
<td>Creates a new Dynamic Object Builder for the current File</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Edits the File monitoring settings</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Sets the polling interval for this File monitoring</td>
</tr>
<tr>
<td><strong>Alert Actions</strong></td>
<td>Adds specific Alert Actions to the File monitoring</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for the File Monitoring</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this object</td>
</tr>
<tr>
<td><strong>Paste</strong></td>
<td>Pastes a previously copied or cut File monitoring object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the File monitoring and all its dependent objects</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Allows you to rename this File monitoring</td>
</tr>
<tr>
<td><strong>View File Content</strong></td>
<td>Displays the File content</td>
</tr>
<tr>
<td><strong>Restart Scan</strong></td>
<td>Restart the scanning of the file from the beginning at the next polling cycle, when performing string searches or numeric value extractions</td>
</tr>
<tr>
<td><strong>Acknowledge Alerts</strong></td>
<td>Acknowledges all alerts and resets parameters to zero</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Pauses the File monitoring</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Resumes monitoring of the file and all its depend objects</td>
</tr>
<tr>
<td><strong>Refresh Parameters</strong></td>
<td>Refreshes all instance parameters of the SEN_MS_FILE application class</td>
</tr>
</tbody>
</table>
SEN_MS_FILESYSTEM

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AvailableCapacity*</td>
<td>Total capacity not consumed in the file system. Value set by fileSystemColl</td>
<td>Megabytes (MB)</td>
<td>Alarm ≤ 10</td>
<td>Statistics</td>
</tr>
<tr>
<td>AvailableCapacityPercentage*</td>
<td>Percentage of capacity not consumed in the file system. Value set by fileSystemColl</td>
<td>Percent (%)</td>
<td>Warning ≤ 10 Alarm ≤ 1</td>
<td>Statistics</td>
</tr>
<tr>
<td>AvailableInodesPercentage</td>
<td>Percentage of available inodes on UNIX and Linux platforms. Value set by fileSystemColl</td>
<td>Percent (%)</td>
<td>Warning ≤ 10 Alarm ≤ 1</td>
<td>Statistics</td>
</tr>
<tr>
<td>ConsumedCapacityGrowthPercentage</td>
<td>Percentage of the capacity that is actually consumed per hour in the file system. Value set by fileSystemColl</td>
<td>Percent per hour (%/h)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>ConsumedCapacityGrowthSpeed</td>
<td>Speed at which the capacity is actually consumed in the file system. Value set by fileSystemColl</td>
<td>Megabytes per hour (MB/h)</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the File systems monitoring</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of File systems’ parent</td>
</tr>
<tr>
<td>File System</td>
<td>Drive or path of the monitored file system</td>
</tr>
</tbody>
</table>

Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Edits the File system monitoring settings</td>
</tr>
<tr>
<td>Menu Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Sets the polling interval for this File systems monitoring</td>
</tr>
<tr>
<td>Alert Actions</td>
<td>Adds specific Alert Actions to the File systems monitoring</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays all available information for the File systems Monitoring</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this File system monitoring object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this File system monitoring object</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes this File system monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the File system monitoring and all its dependent objects</td>
</tr>
<tr>
<td>Rename</td>
<td>Allows you to rename this File system monitoring instance</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>Acknowledges all alerts and reset parameters to zero</td>
</tr>
<tr>
<td>Pause Monitoring</td>
<td>Pauses the File systems monitoring</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the File systems monitoring</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the SEN_MS_FILESYSTEM application class</td>
</tr>
</tbody>
</table>
### SEN_MS_FOLDER

#### Icon

#### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeletedFileRate</td>
<td>Displays the number of deleted files per minute. Value set by folderColl</td>
<td>files/min</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Exists*</td>
<td>Indicates whether the folder exists or not. Value set by folderColl.</td>
<td>(0 = Folder exists; 1 = Folder does not exist)</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>FileCount*</td>
<td>Displays the current number of files in a folder (includes sub-folders, if any, when the option is activated). Value set by folderColl</td>
<td>file(s)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>GrowthPercentage</td>
<td>Displays the percentage of the folder size growth per minute. Value set by folderColl</td>
<td>Percentage per minute (%/min)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>GrowthSpeed</td>
<td>Displays the folder size growth per minute. Value set by folderColl</td>
<td>Kilobytes per minute (KB/min)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>LastModifiedFileSizeedTime</td>
<td>Displays the elapsed time since the last modification of any file in this folder. Value set by folderColl</td>
<td>minutes</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>LongestTimeFileRemainsInFolder</td>
<td>Displays the longest time an existing file has been placed in the folder. Value set by folderColl</td>
<td>minutes</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>ModifiedFileRate</td>
<td>Displays the rate of modified files per minute. Value set by folderColl</td>
<td>files/min</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>NewFileRate</td>
<td>Displays the rate of new files per minute. Value set by folderColl</td>
<td>files/min</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>OldestModifiedFileSizeedTime</td>
<td>Displays the elapsed time since the oldest modification of any file in this folder or sub-folder. Value set by folderColl</td>
<td>minutes</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Units</td>
<td>Default Alert Conditions</td>
<td>Type</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Size*</td>
<td>Displays the total size of all the files in the folder (include sub-folders if any) in MB. Value set by folderColl</td>
<td>Megabytes (MB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management*

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Folder monitoring</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Folder’s parent</td>
</tr>
<tr>
<td>Folder</td>
<td>Path of the monitored folder</td>
</tr>
<tr>
<td>Include subfolders</td>
<td>Displays whether subfolders are monitored or not</td>
</tr>
</tbody>
</table>

**Menu Commands**

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Edits the Folder monitoring settings</td>
</tr>
<tr>
<td>Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Polling interval</td>
<td>Sets the polling interval for this Folder monitoring</td>
</tr>
<tr>
<td>Alert Actions</td>
<td>Adds specific Alert Actions to the Folder monitoring</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays all available information for the Folder Monitoring</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this Folder monitoring object.</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this Folder monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the Folder monitoring</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the Folder monitoring</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>Acknowledges all alerts and reset parameters to zero</td>
</tr>
<tr>
<td>Pause Monitoring</td>
<td>Pauses the Folder monitoring</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the Folder monitoring</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the SEN_MS_FOLDER application class</td>
</tr>
</tbody>
</table>
SEN_MS_FORMULA

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value*</td>
<td>Value of the parameter that is being monitored. Value set by formulaColl</td>
<td>Value</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the multi-parameter formula monitoring</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the multi-parameter formula’s parent</td>
</tr>
<tr>
<td>Formula</td>
<td>Formula applied to the parameters</td>
</tr>
<tr>
<td>Variable [A to Z]</td>
<td>Parameter associated to the variable</td>
</tr>
</tbody>
</table>

Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Edits the multi-parameter formula monitoring settings</td>
</tr>
<tr>
<td>Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Polling Intervals</td>
<td>Sets the polling interval for this multi-parameter formula monitoring</td>
</tr>
<tr>
<td>Alert Actions</td>
<td>Adds specific Alert Actions to the multi-parameter formula monitoring</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays all available information for this multi-parameter formula monitoring</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this multi-parameter formula monitoring object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this multi-parameter formula monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the multi-parameter formula monitoring</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the multi-parameter formula monitoring object</td>
</tr>
<tr>
<td>Menu Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>Acknowledges all alerts and resets parameters</td>
</tr>
<tr>
<td>Pause Monitoring</td>
<td>Pauses the multi-parameter formula monitoring</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the multi-parameter formula monitoring</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the SEN_MS_FORMULA application class</td>
</tr>
</tbody>
</table>
**SEN_MS_GROUP**

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CollectionErrorCount*</td>
<td>Reports the number of collection issues that happened to the hosts and monitors that belong to the group. This parameter is cumulative, new errors increase the value of the parameter. The CollectionErrorCount value will be reset after a given time if no new errors are found. The default timeout is 15 minutes but can be configured with the: <code>/SENTRY/STUDIO/&lt;groupId&gt;/collectionErrorCountAutoAcknowledgeTime</code> variable. Value set by collectionErrorColl.</td>
<td>errors</td>
<td>Alarm ≥ 1</td>
<td>Collection Status</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management*

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Group</td>
</tr>
<tr>
<td>Contact</td>
<td>Name or contact information of the person in charge of the Group.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the Group</td>
</tr>
<tr>
<td>Constant 1</td>
<td>Name of the first Group constant</td>
</tr>
<tr>
<td>Constant 2</td>
<td>Name of the second Group constant</td>
</tr>
<tr>
<td>Constant 3</td>
<td>Name of the third Group constant</td>
</tr>
<tr>
<td>Constant 4</td>
<td>Name of the fourth Group constant</td>
</tr>
<tr>
<td>Constant 5</td>
<td>Name of the fifth Group constant</td>
</tr>
<tr>
<td>Menu Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>New &gt; Hosts</strong></td>
<td>Allows you to add a Host</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Allows you to edit the Group</td>
</tr>
<tr>
<td><strong>Group Constants</strong></td>
<td>Modifies the Group constants</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Sets the polling interval</td>
</tr>
<tr>
<td><strong>Alert Actions</strong></td>
<td>Allows you to add Alert Actions that will be used for the Group as well as its dependent objects</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for the Group</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies the Group icon</td>
</tr>
<tr>
<td><strong>Paste</strong></td>
<td>Pastes a previously copied object into this Group</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the Group icon and all its dependent objects</td>
</tr>
<tr>
<td><strong>Delete all</strong></td>
<td>Deletes all objects under the Group</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Allows you to rename this Group</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Allows you to pause the monitoring of the Group as well as all its dependent objects</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Allows you to resume the monitoring of the Group as well as all its dependent objects after it has been paused</td>
</tr>
<tr>
<td><strong>Refresh Parameters</strong></td>
<td>Refreshes all instance parameters of the SEN_MS_Group application class</td>
</tr>
</tbody>
</table>
**SEN_MS_HOST**

**Icon**

![Icon](image)

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status*</td>
<td>Status of the host availability. Value set by the availabilityCheckColl.</td>
<td>{ 0 = OK ; 1 = Signature Files Not Present ; 2 = Unreachable }</td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management*

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Host: &lt;groupID&gt;@&lt;hostname&gt;</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the host’s parent</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname or IP address of the Host</td>
</tr>
<tr>
<td>BMC TrueSight Device</td>
<td>FQDN and Token ID of the Host (separated by '/')</td>
</tr>
<tr>
<td>Credentials</td>
<td>Lists the type of credentials provided</td>
</tr>
<tr>
<td>Signature File 1</td>
<td>First signature file</td>
</tr>
<tr>
<td>Signature File 2</td>
<td>Second signature file</td>
</tr>
<tr>
<td>Signature File 3</td>
<td>Third signature file</td>
</tr>
<tr>
<td>Signature File 4</td>
<td>Fourth signature file</td>
</tr>
</tbody>
</table>

**Menu Commands**

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &gt; Monitor</td>
<td>Allows you to add a new Monitor</td>
</tr>
<tr>
<td>New &gt; Monitor Group</td>
<td>Allows you to add a new Monitor Group</td>
</tr>
<tr>
<td>Menu Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Allows you to edit the Host</td>
</tr>
<tr>
<td>Credentials &gt; New Credentials</td>
<td>Creates new credentials</td>
</tr>
<tr>
<td>Credentials &gt; Edit Credentials</td>
<td>Edits existing credentials</td>
</tr>
<tr>
<td>Credentials &gt; Delete Credentials</td>
<td>Deletes existing credentials</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Sets the polling interval</td>
</tr>
<tr>
<td><strong>Alert Actions</strong></td>
<td>Allows you to add Alert Actions that will be used for the Host as well as its dependent objects</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for this Host</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts the Host</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies the Host</td>
</tr>
<tr>
<td><strong>Paste</strong></td>
<td>Pastes a previously copied object into this Host</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the Host instance and all its dependent objects</td>
</tr>
<tr>
<td>Delete all</td>
<td>Deletes all objects under the Host</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>Acknowledges all alerts and reset parameters to zero</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Allows you to pause the monitoring of the Host as well as all its dependent objects</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Allows you to resume the monitoring of the Host as well as all its dependent objects after it has been paused</td>
</tr>
<tr>
<td>Tools &gt; Process Viewer</td>
<td>Starts the process viewer tool</td>
</tr>
<tr>
<td>Tools &gt; File Viewer</td>
<td>Starts the file viewer tool</td>
</tr>
<tr>
<td>Tools &gt; Windows Event Log Reader</td>
<td>Starts the Windows Event log reader tool (On Windows Agents only)</td>
</tr>
<tr>
<td>Tools &gt; SNMP Browser</td>
<td>Starts the SNMP browser tool</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the SEN_MS_HOST application class</td>
</tr>
</tbody>
</table>
## SEN_MS_MAIN

### Icon
![Icon](image)

### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CollectionErrorCount</td>
<td>Number of errors that prevent Monitoring Studio from working properly. This parameter is cumulative, new errors increase the value of the parameter. The CollectionErrorCount value will be reset after a given time if no new errors are found. The default timeout is 135 minutes but can be configured with the: <code>/SENTRY/STUDIO/collectionErrorCountAutoAcknowledgeTime</code> variable. Value set by discoveryColl.</td>
<td>errors</td>
<td>Alarm ≥ 1</td>
<td>Statistics</td>
</tr>
<tr>
<td>DebugStatus</td>
<td>Indicates whether the debug mode has been enabled or not. Value set by studioColl.</td>
<td>{0 = Off ; 1 = On}</td>
<td>None</td>
<td>Availability</td>
</tr>
<tr>
<td>HostCount</td>
<td>Displays the total number of Hosts added to all Groups. Note: identical hosts are counted as if they were unique. Value set by studioColl.</td>
<td>Hosts</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>MonitorCount*</td>
<td>Displays the total number of Monitors added to all Groups. Value set by studioColl.</td>
<td>Monitors</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management*

### Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>Name of the product</td>
</tr>
<tr>
<td>Version</td>
<td>Current version of the product</td>
</tr>
<tr>
<td>Release Date</td>
<td>Release date of the current version of the product</td>
</tr>
<tr>
<td>Copyright</td>
<td>Copyright information</td>
</tr>
</tbody>
</table>
### Application Classes and Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>Website address</td>
</tr>
<tr>
<td>Support</td>
<td>Support contact information</td>
</tr>
</tbody>
</table>

#### Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Group</strong></td>
<td>Allows you to add a new Group</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Starts the thresholds configuration wizard</td>
</tr>
<tr>
<td><strong>Trigger a KM Discovery</strong></td>
<td>Allows you to manually force a full KM discovery</td>
</tr>
<tr>
<td><strong>Paste</strong></td>
<td>Pastes the previously copied group and its children objects as a new group</td>
</tr>
<tr>
<td><strong>Tools &gt; Real-time SNMP Trap listener</strong></td>
<td>Starts the real-time SNMP trap listener</td>
</tr>
<tr>
<td><strong>KM Settings &gt; Discovery Interval</strong></td>
<td>Allows you to customize the discovery interval. By default, discovery is performed every hour</td>
</tr>
<tr>
<td><strong>KM Settings &gt; Thresholds Mechanism Selection</strong></td>
<td>Allows you to customize the thresholds mechanism used by Monitoring Studio</td>
</tr>
<tr>
<td><strong>KM Settings &gt; Java Settings</strong></td>
<td>Enables you to change the Java installation path used by Monitoring Studio</td>
</tr>
<tr>
<td><strong>KM Settings &gt; Force Classic Configuration Mode</strong></td>
<td>Forces the KM to “Classic Mode” and allows to configure Monitoring Studio from PATROL Consoles</td>
</tr>
<tr>
<td><strong>KM Settings &gt; Debug</strong></td>
<td>Enables or disables the KM debug options</td>
</tr>
<tr>
<td><strong>Configuration &gt; Show Configuration</strong></td>
<td>Generates a report containing the entire object configuration</td>
</tr>
<tr>
<td><strong>Configuration &gt; Export Configuration</strong></td>
<td>Exports the PATROL agent configuration</td>
</tr>
<tr>
<td><strong>Configuration &gt; Import Configuration</strong></td>
<td>Imports the PATROL agent configuration</td>
</tr>
<tr>
<td><strong>ResetCollectionErrorCount</strong></td>
<td>Resets the CollectionErrorCount parameter</td>
</tr>
<tr>
<td><strong>Refresh Parameters</strong></td>
<td>Refreshes all instance parameters of the SEN_MS_MAIN application class</td>
</tr>
<tr>
<td><strong>About…</strong></td>
<td>Shows the version and general information about Monitoring Studio</td>
</tr>
</tbody>
</table>
SEN_MS_MONITORGROUP

Icon

Parameters

None

Infobox

None

Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New &gt; Monitor</strong></td>
<td>Allows you to add a new Monitor</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for this Monitor Group</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this object</td>
</tr>
<tr>
<td><strong>Paste</strong></td>
<td>Pastes a previously copied object into this Monitor Group</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the Monitor Group instance and all its dependent objects</td>
</tr>
<tr>
<td><strong>Delete all</strong></td>
<td>Deletes all objects under the Monitor Group</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Allows you to rename this Monitor Group</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Allows you to pause the monitoring of the Group as well as all its dependent objects</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Allows you to resume the monitoring of the Group as well as all its dependent objects after it has been paused</td>
</tr>
</tbody>
</table>
SEN_MS_NUMBER

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value*</td>
<td>Value of the searched Numeric Value (no value will be given if no number is found) Value set by the collector of the parent’s object</td>
<td>Value</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>ValueFound</td>
<td>States if a numeric value has been found {0 = Value found ; 1 = Value not found}</td>
<td>None</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the numeric value extraction</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the numeric value extraction’s parent</td>
</tr>
<tr>
<td>Parent Type</td>
<td>Type of the parent (File, Command Line, etc.)</td>
</tr>
<tr>
<td>Line Mode</td>
<td>Method used to select lines to search for the numeric</td>
</tr>
<tr>
<td>Column Mode</td>
<td>Method chosen to search and extract the numeric value in the line</td>
</tr>
<tr>
<td>Parameter Type</td>
<td>Type of the parameter</td>
</tr>
<tr>
<td>Line Numbers</td>
<td>Line numbers in which the numeric value will be extracted from</td>
</tr>
<tr>
<td>Regular Expression</td>
<td>Regular expression used to select the lines where the number will be searched for</td>
</tr>
<tr>
<td>Skip Blank Lines</td>
<td>Indicates whether or not blank lines are skipped when searching for the numeric value</td>
</tr>
<tr>
<td>After/Before</td>
<td>Searches for the numeric value either after or before the specified string</td>
</tr>
<tr>
<td>Specified String</td>
<td>Searches for the numeric value before or after this specified string</td>
</tr>
<tr>
<td>Character Offset</td>
<td>Character offset where the numeric value is searched for</td>
</tr>
<tr>
<td>Field Number</td>
<td>Number of the field in which the numeric value will be searched for</td>
</tr>
<tr>
<td>Field Separators</td>
<td>Characters that separates the fields in a text line</td>
</tr>
<tr>
<td>Unique Separator</td>
<td>Considers consecutive separators as a unique separator</td>
</tr>
</tbody>
</table>
## Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td>Edits the numeric value extraction settings</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Alert Actions</strong></td>
<td>Adds specific Alert Actions to the Numeric Value extraction object</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for the Numeric Value extraction</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this Numeric Value extraction object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this Numeric Value extraction object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the Numeric Value extraction object</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Renames the Numeric Value extraction object</td>
</tr>
<tr>
<td><strong>Acknowledge Alerts</strong></td>
<td>Acknowledges all alerts and resets parameters.</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Pauses the Numeric Value extraction</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Resumes the Numeric Value extraction</td>
</tr>
</tbody>
</table>
## SEN_MS_PROCESS

### Icon

#### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChildCount</td>
<td>Displays the number of child processes of the matching process(es). Value set by processColl</td>
<td>processes</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Count*</td>
<td>Displays the number of parent processes that match the criteria. Value set by processColl</td>
<td>processes</td>
<td>Alarm = 0</td>
<td>Statistics</td>
</tr>
<tr>
<td>HandleCount</td>
<td>Displays the number of handles opened by the matching process(es). Value set by processColl</td>
<td>handles</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>MatchingProcesses</td>
<td>Displays the list of all matching processes. Value set by processColl</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>PageFaultsPerSec</td>
<td>Displays the number of page faults per second caused by the matching process(es). Value set by processColl</td>
<td>faults/s</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>PageFileBytes</td>
<td>Displays the page file used by the matching process(es). Value set by processColl</td>
<td>Megabytes (MB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>PrivateBytes</td>
<td>Displays the amount of memory that has been allocated by this process and that cannot be shared with others. Value set by processColl</td>
<td>Megabytes (MB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>ProcessorTime*</td>
<td>Displays the processor time percent used by the matching process(es). Value set by processColl</td>
<td>Percentage (%)</td>
<td>Warning ≥ 100</td>
<td>Statistics</td>
</tr>
<tr>
<td>Status*</td>
<td>Status of the process monitoring execution. Value set by processColl.</td>
<td>(0 = OK ; 1 = Suspicious ; 2 = Failed)</td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
<tr>
<td>ThreadCount</td>
<td>Displays the number of threads of the matching process(es). Value set by processColl</td>
<td>threads</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>VirtualBytes</td>
<td>Displays the virtual memory used by the matching process(es). Value set by processColl</td>
<td>Megabytes (MB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>
Application Classes and Parameters

### WorkingSet

**Name:** WorkingSet (Windows only)

**Description:** Displays the working set size of the matching process(es). Value set by processColl

**Units:** Megabytes (MB)

**Default Alert Conditions:** None

**Type:** Statistics

For detailed information about Baselining and KPI, see *Managing Baselines and Key Performance Indicators.*

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management

### Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the monitor</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Process’ parent</td>
</tr>
<tr>
<td>Process IDs</td>
<td>Monitored process IDs (PIDs)</td>
</tr>
<tr>
<td>Child Process IDs</td>
<td>Detected child process IDs (PIDs)</td>
</tr>
</tbody>
</table>

### Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td>Edits the Process monitoring settings</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Sets the polling interval for this instance</td>
</tr>
<tr>
<td><strong>Alert Actions</strong></td>
<td>Adds specific Alert Actions to the Process monitoring</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for the Process monitoring</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this Process monitoring object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this Process monitoring object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the Process monitoring object</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Renames the Process monitoring object</td>
</tr>
<tr>
<td><strong>Acknowledge Alerts</strong></td>
<td>Acknowledges all alerts and reset parameters to zero</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Pauses the Process monitoring</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Resumes the Process monitoring</td>
</tr>
<tr>
<td><strong>Refresh Parameters</strong></td>
<td>Refreshes all instance parameters of the SEM_MS_PROCESS class</td>
</tr>
</tbody>
</table>
SEN_MS_SNMP POLLING

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Content of the SNMP received. Value set by snmpPollingColl</td>
<td></td>
<td></td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Note: Only applicable to SNMP of String type.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ExecutionTime*</td>
<td>Time taken by the SNMP polling to execute. Value set by snmpPollingColl</td>
<td></td>
<td>Warning ≤ 30</td>
<td>Response Time</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the SNMP polling. Value set by snmpPollingColl</td>
<td></td>
<td></td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>{0 = OK; 1 = Suspicious; 2 = Failed}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value*</td>
<td>Value of the SNMP received. Value set by snmpPollingColl</td>
<td></td>
<td></td>
<td>Statistics</td>
</tr>
<tr>
<td></td>
<td>Note: Only applicable to SNMPs of integer type.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the SNMP Polling</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname where the SNMP agent is running.</td>
</tr>
<tr>
<td>Community</td>
<td>Community used to connect to the SNMP agent.</td>
</tr>
<tr>
<td>Port</td>
<td>Port used to connect to the SNMP agent.</td>
</tr>
<tr>
<td>OID</td>
<td>OID that is polled</td>
</tr>
<tr>
<td>OID type</td>
<td>Type of the selected OID value (number or string)</td>
</tr>
</tbody>
</table>

Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &gt; String Search</td>
<td>Creates a new String search for this SNMP Polling</td>
</tr>
<tr>
<td>Menu Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>New &gt; Numeric Value Extraction</td>
<td>Creates a new Numeric Value search for this SNMP Polling</td>
</tr>
<tr>
<td>New &gt; Dynamic Object Builder</td>
<td>Creates a new Dynamic Object Builder for this SNMP Polling</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the SNMP Polling settings</td>
</tr>
<tr>
<td>Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Sets the polling interval for this SNMP Polling</td>
</tr>
<tr>
<td>Alert Actions</td>
<td>Adds specific Alert Actions to the SNMP Polling</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays all available information for this SNMP Polling</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this SNMP Polling object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this SNMP Polling object</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes a previously copied or cut String search or Numeric Value search</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the SNMP Polling and all its dependent objects</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the SNMP Polling object</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>Acknowledges all alerts and reset parameters to zero</td>
</tr>
<tr>
<td>Pause Monitoring</td>
<td>Pauses the SNMP Polling as well as all its dependent objects</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the SNMP Polling as well as all its dependent objects</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Re-polls the OID and refresh all parameters. All dependent objects will be refreshed as well (SEN_MS_STRING and SEN_MS_NUMBER instances)</td>
</tr>
</tbody>
</table>
**SEN_MS_SNMPTRAP**

**Icon**

![SNMP Trap Icon](image)

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MatchingTrapCount*</td>
<td>Number of matching SNMP traps per minute. Value set by snmpTrapColl</td>
<td>traps</td>
<td>Alarm = 1</td>
<td>Statistics</td>
</tr>
<tr>
<td>MatchingTrapRate*</td>
<td>Number of SNMP traps matching the search. Value set by snmpTrapColl</td>
<td>traps/min</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management*

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the SNMP Trap listening</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the SNMP Trap listening parent</td>
</tr>
<tr>
<td>Community</td>
<td>Community used to listen to traps</td>
</tr>
<tr>
<td>Enterprise ID</td>
<td>Enterprise ID of the SNMP agent that raises the traps</td>
</tr>
<tr>
<td>Trap number</td>
<td>Number of the searched trap</td>
</tr>
<tr>
<td>OID 1</td>
<td>OID of the first varBind of the searched traps</td>
</tr>
<tr>
<td>String 1</td>
<td>Searched string in the first varBind</td>
</tr>
<tr>
<td>OID 2</td>
<td>OID of the second varBind of the searched traps</td>
</tr>
<tr>
<td>String 2</td>
<td>Searched string in the second varBind</td>
</tr>
<tr>
<td>Acknowledging Trap Number</td>
<td>Trap number that will acknowledge this trap search</td>
</tr>
<tr>
<td>Acknowledging OID 1</td>
<td>OID of the first varBind of the trap that will acknowledge this trap search</td>
</tr>
<tr>
<td>Acknowledging String 1</td>
<td>Searched string in the first varBind of the acknowledging trap</td>
</tr>
<tr>
<td>Acknowledging OID 2</td>
<td>OID of the second varBind of the trap that will acknowledge this trap search</td>
</tr>
<tr>
<td>Acknowledging String 2</td>
<td>Searched string in the second varBind of the acknowledging trap</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout for auto-acknowledgment</td>
</tr>
</tbody>
</table>
## Application Classes and Parameters

### Monitoring Studio KM for PATROL 9.0.00

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Alert Actions</td>
<td>Indicates when Alert Actions should be executed</td>
</tr>
</tbody>
</table>

### Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td>Edits the SNMP Trap listening settings</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Alert Actions</strong></td>
<td>Adds specific Alert Actions to the SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for this SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this SNMP Trap listening object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this SNMP Trap listening object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Renames the SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Acknowledge all and reset</strong></td>
<td>Acknowledges all alerts on the SNMP Trap object and resets the &quot;MatchingTrapCount&quot; parameter to '0'</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Pauses the SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Resumes the SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Refresh Parameters</strong></td>
<td>Refreshes all parameters of the SEN_MS_SNMPTRAP application class</td>
</tr>
</tbody>
</table>
**SEN_MS_STRING**

**Icon**

![Icon](image)

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastMatchingLines</td>
<td>Lines matching the String search. Value set by the collector of the parent object. Note: The number of lines displayed can be changed to a custom value by adding the variable &quot;/SENTRY/STUDIO/LastMatchingLinesNumber&quot; with the proper line number to the PATROL Agent configuration. Default: the 10 last matching lines are displayed.</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>MatchingLineCount</td>
<td>Number of lines matching the String search. Value set by the collector of the parent object.</td>
<td>lines</td>
<td>Alarm ≥ 1</td>
<td>Statistics</td>
</tr>
<tr>
<td>MatchingLineRate</td>
<td>Number of lines matching the String search per minute. Value set by the collector of the parent object. The MatchingLineRate parameter is only activated for String searches in log files and in &quot;never-ending&quot; command lines.</td>
<td>lines/min</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management*

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the String search</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the String search’s parent</td>
</tr>
<tr>
<td>Parent type</td>
<td>Type of the parent (File, Command Line, etc.)</td>
</tr>
<tr>
<td>Search</td>
<td>Search mode</td>
</tr>
<tr>
<td>Lines</td>
<td>Lines that are searched</td>
</tr>
<tr>
<td>Acknowledging String</td>
<td>String that auto-acknowledges this string search</td>
</tr>
<tr>
<td>Acknowledge</td>
<td>Indicates whether the auto-acknowledgment is enabled</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout for the auto-acknowledging</td>
</tr>
<tr>
<td>Run Alert Actions</td>
<td>Indicates when Alert Actions should be executed</td>
</tr>
</tbody>
</table>
**Menu Commands**

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td>Edits the String search settings</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Alert Actions</strong></td>
<td>Adds specific Alert Actions to the String search</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for this String search</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this String search object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this String search object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the String search object</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Renames the String search object</td>
</tr>
<tr>
<td><strong>Acknowledge all and reset</strong></td>
<td>Acknowledges all alerts for this object. The MatchingLineCount parameter is set to zero</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Pauses the String search</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Resumes the String search</td>
</tr>
</tbody>
</table>
SEN_MS_TRANSFORM

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>TransformResult</td>
<td>Lines matching the Text pre-processing</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Text Pre-processing object</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Text Pre-processing object's parent</td>
</tr>
<tr>
<td>Parent type</td>
<td>Type of the parent (File, Command Line, etc.)</td>
</tr>
</tbody>
</table>

Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &gt; String search</td>
<td>Creates a new String search for this Text pre-processing object</td>
</tr>
<tr>
<td>New &gt; Numeric value extraction</td>
<td>Creates a new Numeric value extraction for this Text pre-processing object</td>
</tr>
<tr>
<td>New &gt; Dynamic Object Builder</td>
<td>Creates a new Dynamic Object Builder for this Text pre-processing object</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the Text-preprocessing monitoring settings</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays all available information for this Text pre-processing object</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this object</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes a previously copied or cut Text pre-processing object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the Text-preprocessing monitoring and all its dependent objects</td>
</tr>
<tr>
<td>Rename</td>
<td>Allows you to rename this Text pre-processing object</td>
</tr>
<tr>
<td>Pause Monitoring</td>
<td>Pauses the monitoring of this Text pre-processing object</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the monitoring of this Text pre-processing object</td>
</tr>
</tbody>
</table>
**SEN_MS_WBEMQUERY**

**Icon**

[Image]

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExecutionTime*</td>
<td>Time taken by the WBEM query to run. Value set by wbemQueryColl</td>
<td>seconds</td>
<td>None</td>
<td>Response Time</td>
</tr>
<tr>
<td>Result</td>
<td>Displays the return output of the WBEM query. Value set by wbemQueryColl</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>Status*</td>
<td>Status of the execution. Value set by wbemQueryColl</td>
<td>{0 = OK ; 1 = Suspicious ; 2 = Failed}</td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC TrueSight Operations Management*

---

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the WBEM query object</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the WBEM query object’s parent</td>
</tr>
<tr>
<td>Host</td>
<td>Displays the name of the host machine</td>
</tr>
<tr>
<td>Name Space</td>
<td>Displays the WBEM namespace</td>
</tr>
<tr>
<td>WBEM Query</td>
<td>Displays the WBEM query</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the port number used for the WBEM query</td>
</tr>
<tr>
<td>Protocol</td>
<td>Displays the protocol used (HTTP/HTTPS)</td>
</tr>
<tr>
<td>Username</td>
<td>username for the WBEM query</td>
</tr>
</tbody>
</table>

**Menu Commands**

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &gt; String search</td>
<td>Creates a new String search for this WBEM query object</td>
</tr>
</tbody>
</table>

---

*For detailed information about Baselining and KPI, see [Managing Baselines and Key Performance Indicators](#).*
<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New &gt; Numeric value extraction</strong></td>
<td>Creates a new Numeric Value extraction for this WBEM query object</td>
</tr>
<tr>
<td><strong>New &gt; Text Pre-Processing</strong></td>
<td>Creates a new Text pre-processing for this WBEM query object</td>
</tr>
<tr>
<td><strong>New &gt; Dynamic Object Builder</strong></td>
<td>Creates a new Dynamic Object Builder for this WBEM query object</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Edits the WBEM monitoring settings</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Sets the polling interval for this command line execution monitoring</td>
</tr>
<tr>
<td><strong>Alert Actions</strong></td>
<td>Adds specific Alert Actions to the command line execution</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for this WBEM query object</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this WBEM monitoring object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this WBEM monitoring object</td>
</tr>
<tr>
<td><strong>Paste</strong></td>
<td>Pastes this WBEM monitoring object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the WBEM monitoring object</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Renames the WBEM monitoring object</td>
</tr>
<tr>
<td><strong>Acknowledge Alerts</strong></td>
<td>Acknowledges all alerts and resets parameters</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Pauses the WBEM monitoring</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Resumes the WBEM monitoring</td>
</tr>
<tr>
<td><strong>Refresh Parameters</strong></td>
<td>Refreshes all instance parameters of the SEN_MS WBEMQUERY application class</td>
</tr>
</tbody>
</table>
SEN_MS_WEBREQUEST

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExecutionTime*</td>
<td>Time taken by the Web request to execute. Value set by webRequestColl</td>
<td>seconds</td>
<td>Warning ≥ 15 Alarm ≥ 30</td>
<td>Response Time</td>
</tr>
<tr>
<td>HTTPStatus*</td>
<td>Web request status. Value set by webRequestColl</td>
<td>{0 = OK ; 1 = Degraded ; 2 = Failed}</td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
<tr>
<td>HTTPStatusCode</td>
<td>Web response status code. Value set by webRequestColl</td>
<td>--</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Result</td>
<td>Displays the result of the Web Request execution. Value set by webRequestColl</td>
<td>--</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the connection to the Web server. Value set by webRequestColl</td>
<td>{0 = OK ; 1 = Suspicious ; 2 = Failed}</td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
</tbody>
</table>

For detailed information about Baselining and KPI, see Managing Baselines and Key Performance Indicators.

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC TrueSight Operations Management.

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Web Request analysis</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Web Request’s parent</td>
</tr>
<tr>
<td>Used HTTP method</td>
<td>HTTP method used by the Web Request</td>
</tr>
</tbody>
</table>

Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &gt; String Search</td>
<td>Creates a new String search for this Web Request</td>
</tr>
<tr>
<td>Menu Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>New &gt; Numeric Value Extraction</td>
<td>Creates a new Numeric Value extraction for this Web Request</td>
</tr>
<tr>
<td>New &gt; Text Pre-processing</td>
<td>Creates a new Text pre-processing for this Web Request</td>
</tr>
<tr>
<td>New &gt; Dynamic Object Builder</td>
<td>Creates a new Dynamic Object Builder for this Web Request</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the Web Request analysis settings.</td>
</tr>
<tr>
<td>Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Sets the polling interval for this Web Request monitoring object</td>
</tr>
<tr>
<td>Alert Actions</td>
<td>Adds specific Alert Actions to the Web Request analysis</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays all available information for this Web Request</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this Web request object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this Web request object</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes a previously copied or cut String search or Numeric Value search object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the Web Request analysis and all its dependent objects</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the Web Request monitoring object</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>Acknowledges all alerts and reset parameters.</td>
</tr>
<tr>
<td>Pause Monitoring</td>
<td>Pauses the Web Request analysis as well as all its dependent objects</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the Web Request analysis as well as all its dependent objects</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all parameters of the SEN_MS_WEBREQUEST application class</td>
</tr>
</tbody>
</table>
**SEN_MS_WINEVENT**

**Icon**

![Icon](image)

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MatchingEventCount*</td>
<td>Number of matching Windows Events. Value set by winEventColl</td>
<td>events</td>
<td>Alarm ≥ 1</td>
<td>Statistics</td>
</tr>
<tr>
<td>MatchingEventRate*</td>
<td>Rate of matching Windows Events. Value set by winEventColl</td>
<td>events/ min</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>MatchingEvents</td>
<td>Lists all matching events, which are counted in MatchingEventCount.</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Windows Event monitoring</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Windows Event’s parent</td>
</tr>
<tr>
<td>Event Log</td>
<td>Indicates which event log is searched</td>
</tr>
<tr>
<td>Provider</td>
<td>Indicates the provider selected</td>
</tr>
<tr>
<td>Event ID</td>
<td>ID of the event to be searched for</td>
</tr>
<tr>
<td>Acknowledging Event ID</td>
<td>Event IDs that will acknowledge the detected events</td>
</tr>
<tr>
<td>Acknowledge</td>
<td>What is to be acknowledged: one event or all events</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time after which a matching Windows Event is acknowledged</td>
</tr>
<tr>
<td>Run Alert Actions</td>
<td>Indicates when Alert Actions should be executed</td>
</tr>
</tbody>
</table>
### Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td>Edits the Windows Event monitoring settings</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Sets the polling interval for this Windows Event monitoring</td>
</tr>
<tr>
<td><strong>Alert Actions</strong></td>
<td>Adds specific Alert Actions to the Windows Event monitoring</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays all available information for this Windows Event monitoring</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this Windows Event monitoring object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this Windows Event monitoring object</td>
</tr>
<tr>
<td><strong>Paste</strong></td>
<td>Pastes a previously copied or cut Windows Event monitoring object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the Windows Event monitoring object</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Renames the Windows Event monitoring object</td>
</tr>
<tr>
<td><strong>Acknowledge All and Reset</strong></td>
<td>Acknowledges all alerts and resets the &quot;MatchingEventCount&quot; parameter to '0'</td>
</tr>
<tr>
<td><strong>Pause Monitoring</strong></td>
<td>Pauses the Windows Event monitoring</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
<td>Resumes the Windows Event monitoring</td>
</tr>
<tr>
<td><strong>Refresh Parameters</strong></td>
<td>Refreshes all instance parameters of the SEN_MS_WINEVENT application class</td>
</tr>
</tbody>
</table>
SEN_MS_WINPERF

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Value of the monitored Windows Performance counter. Value set by winPerfCol</td>
<td>Depends on the counter</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

*Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management*

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Windows Performance monitoring</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Windows Performance’s parent</td>
</tr>
<tr>
<td>Performance Object</td>
<td>Name of the Windows Performance object that is read</td>
</tr>
<tr>
<td>Instance Name</td>
<td>Selected Windows performance instance</td>
</tr>
<tr>
<td>Performance Counter</td>
<td>Name of the Windows Performance counter that is read</td>
</tr>
</tbody>
</table>

Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Edits the Windows Performance monitoring settings</td>
</tr>
<tr>
<td>Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Sets the polling interval for this Windows Performance monitoring</td>
</tr>
<tr>
<td>Alert Actions</td>
<td>Adds specific Alert Actions to the Windows Performance monitoring</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays all available information for the Windows Performance monitoring</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this Windows Performance monitoring object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this Windows Performance monitoring object</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes a previously copied or cut Windows Performance monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the Windows Performance monitoring object</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the Windows Performance monitoring object</td>
</tr>
<tr>
<td>Menu Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>Acknowledges all alerts and reset parameters</td>
</tr>
<tr>
<td>Pause Monitoring</td>
<td>Pauses the Windows Performance monitoring</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the Windows Performance monitoring</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the SEN_MS_WINPERF application class</td>
</tr>
</tbody>
</table>
**SEN_MS_WINSERVICE**

**Icon**

![Icon](image)

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status*</td>
<td>Status of the Windows Service. Value set by winServiceColl</td>
<td>{0 = Started ; 1 = Intermediate state ; 2 = Stopped}</td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
<tr>
<td>ServiceDetails</td>
<td>Details about the Windows Service</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Windows Service monitoring</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Windows Service’s parent</td>
</tr>
<tr>
<td>Service name</td>
<td>Name of the Service that is monitored</td>
</tr>
</tbody>
</table>

**Startup Mode**

Indicates the startup mode. Possible values are:
- **Boot**: device driver started by the operating system loader
- **System**: device driver started by the operating system initialization process
- **Auto**: service to be started automatically by the service control manager during system startup
- **Manual**: these services do not start unless a user logs on and starts them
- **Disabled**: service that cannot be started until its startup mode is changed to either Auto or Manual

**Path**

Fully qualified path to the service binary file that implements the service

**Menu Commands**

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td>Edits the Windows Service monitoring settings</td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Sets the polling interval for this Windows Service monitoring</td>
</tr>
<tr>
<td>Menu Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Alert Actions</td>
<td>Adds specific Alert Actions to the Windows Service monitoring</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays all available information for the Windows Service monitoring</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this Windows Service monitoring object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this Windows Service monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the Windows Service monitoring object</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the Windows Service monitoring object</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>Acknowledges all alerts and reset parameters</td>
</tr>
<tr>
<td>Pause Monitoring</td>
<td>Pauses the Windows Service monitoring</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the Windows Service monitoring</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the SEN_MS_WINSERVICE application class</td>
</tr>
</tbody>
</table>
SEN_MS_WMIQUERY

Icon

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExecutionTime*</td>
<td>Time taken by the WMI query to be executed. Value set by wmiQueryColl</td>
<td>Seconds</td>
<td>Warning ≤ 30</td>
<td>Response Time</td>
</tr>
<tr>
<td>Result</td>
<td>Displays the result of the WMI query execution. Value set by wmiQueryColl</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>Status*</td>
<td>Status of the WMI query. Value set by wmiQueryColl</td>
<td></td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
</tbody>
</table>

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BMC Truesight Operations Management.

For detailed information about Baselining and KPI, see Managing Baselines and Key Performance Indicators.

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the WMI query object</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the WMI query object’s parent</td>
</tr>
<tr>
<td>Namespace</td>
<td>Displays WMI namespace (e.g.: root\cimv2)</td>
</tr>
<tr>
<td>WQL Query</td>
<td>Displays the WQL query to be executed</td>
</tr>
<tr>
<td>Username</td>
<td>Displays the user name</td>
</tr>
</tbody>
</table>

Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &gt; String Search</td>
<td>Creates a new String search for this WMI query</td>
</tr>
<tr>
<td>New &gt; Numeric Value Extraction</td>
<td>Creates a new Numeric Value extraction for this WMI query</td>
</tr>
<tr>
<td>Menu Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Edit</td>
<td>Allows you to edit the WMI query monitoring settings</td>
</tr>
<tr>
<td>Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Sets the polling interval for this WMI query monitoring</td>
</tr>
<tr>
<td>Alert actions</td>
<td>Adds specific Alert Actions to the WMI query monitoring</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays all available information for this WMI query monitoring</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this object</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes a previously copied or cut WMI query object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the WMI query monitoring and all its dependent objects</td>
</tr>
<tr>
<td>Rename</td>
<td>Allows you to rename this WMI query object</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>Acknowledges all alerts and reset parameters</td>
</tr>
<tr>
<td>Pause Monitoring</td>
<td>Pauses the monitoring of this WMI query object</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the monitoring of this WMI query object</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the SEN_MS_WMIQUERY application class</td>
</tr>
</tbody>
</table>
Managing Baselines and Key Performance Indicators

In order to facilitate the detection of abnormalities on your monitored environment, BMC ProactiveNet calculates baselines per parameter (metrics or attributes) based on values collected over a specified period of time to determine a normal operating range. When the collected values for these parameters are out of range, an alert is triggered.

Some parameters are identified by default as Key Performance Indicators and therefore automatically included in the baselining calculation.

Managing baselines

The baseline is the expected normal operating range for a metric or attribute of a monitor.

The baseline is calculated by collecting the values for a monitor’s attributes and metrics over a specified time period and establishing a low baseline value (consisting of the 10th percentile of all the values for a given time period) and a high baseline value (consisting of the 90th percentile of all the values for a given time period), taking a weighted average of these values over time. A higher weight is given to the latest data being factored into the baseline average. The accuracy of the baseline improves over time.

Requirements for baseline generation

For baselines to be generated for an attribute, that abnormality threshold means that the threshold exists and is not suppressed.
Additionally, if the Key Performance Indicator (KPI) mode is active, only those attributes that have an active abnormality threshold and are also KPI attributes will have baselines generated for them.

⚠️ Absolute thresholds (with "outside baseline") or signature thresholds do not satisfy these requirements.

Managing Key Performance Indicators

The KPI attribute of a parameter can be activated or deactivated manually through the BMC ProactiveNet Administration Console. In this KM, some parameters or attributes have been designated as important indicators of performance (KPIs). We do not recommend that these default settings are modified.

However, advanced users may activate or deactivate KPIs from the BMC ProactiveNet Administration Console.
To add or remove Key Performance Indicator (KPI) attributes for a monitor type

1. In the Administration Console, from the menu bar, choose Tools > KPI Administration. The KPI Administration dialog box is displayed.

2. From the Monitor Type list, choose the monitor type for which you want to add or remove KPI attributes. A list of attributes for the selected monitor type is displayed.

3. In the KPI column for the attributes that you want to add or remove as Key Performance Indicators:
   - select the KPI check box to add the corresponding attribute as a KPI
   - deselect the KPI check box to remove the corresponding attribute from the KPIs for that monitor type

⚠️ For complete and detailed information on this procedure, please refer to the BMC ProactiveNet documentation available from BMC Web site.

Parameters for which the system by default calculates baselines as well as parameters considered as KPIs are respectively identified by the following icons:

- 📈 Baselining
- 🎉 KPI
About...

About HTTP Authentication

The HTTP authentication is a login/password-based mechanism implemented in the HTTP protocol itself. A Web server that requires an HTTP authentication will display a dialog box in Internet Explorer.

⚠️ HTTP authentication has nothing to do with an authentication system of a Web page with a form asking for user credentials like any public web mail service, for example.

There are 3 different HTTP authentication schemes, depending on the machine where Monitoring Studio KM for PATROL is running:

- Basic (Windows, UNIX, Linux)
- Digest (Windows)
- NTLM (Windows)

For Basic HTTP authentication, the password is sent in a base 64-encoded form and is therefore very easily decoded.

If you need to test a Web page or retrieve information from a Web server that requires HTTP Digest or NTLM authentication, we recommend that you install Monitoring Studio KM for PATROL on a Windows system and set up the Web requests from this machine (Web requests can be sent to remote systems).
About Internal Identifiers (IDs)

In Monitoring Studio KM for PATROL, all objects are identified with a unique ID. When configuring Monitoring Studio using a third-party tool, it is important to have a clear understanding of the ID formats.

There are four different ID formats which vary according to the type of objects:

- **Group ID**
- **Host ID**
- **Monitor ID**
- **Monitor Children ID**

**Group ID**

The Group ID is the internal identifier as entered when configuring the Group Settings. It is referred to as `<groupID>`.
Host ID

The Host ID is referred to as <hostID> and always follows this format: <groupID>@<hostname>
where:
- <groupID> is the Internal ID as entered when configuring the Group Settings
- <hostname> is the Hostname/IP address/FQDN of the host on which the technology you wish
to monitor is running

Monitor ID

For all Monitors added from the Host using KM Commands > New > Monitor... the Monitor ID
format is as follows: <groupID>@<hostID>:<monitorType>:<monitorID> where:

- <groupID> is the Internal ID as entered when configuring the Group Settings
- <hostID> is the <groupID>@<hostname> (Hostname/IP address/FQDN)
- <monitorType> is the type of Monitor (Command Line, Web Request, Folder, Process, etc.)
- <monitorID> is the internal ID as entered when configuring the Monitor Settings

Example

If you create a File Monitoring with ID "myFile" under the Host "myHost" which belongs to
Group "myGroup", the complete ID of the File Monitoring would be:
myGroup@myHost:File:myFile
Monitor Children ID

For all Monitors added from another Monitor using **KM Commands > New** > (String Search, Numeric Value Extraction, Text Pre-Processing, and Dynamic Object Builder), the Monitor Children ID format is as follows: `<parentID>:<monitorType>:<monitorID>` where:

- `<parentID>` is the `<groupID>@<hostID>:<monitorType>:<monitorID>`
- `<monitorType>` is the type of Monitor (String Search, Numeric Value Extraction, Text Pre-Processing, and Dynamic Object Builder)
- `<monitorID>` is the internal ID as entered when configuring the Monitor Settings

**Example**

If you create a **String Search Monitoring** with ID "myStringSearch" under the File "myFile" which belongs to the Host "myHost" which itself belongs to the Group "myGroup", the complete ID of the String Search Monitoring would be: **myGroup@myHost:File:myFile:Substring:myStringSearch**
Monitor Children ID - Example
About Processes

What’s a process

In practice, a process is basically a binary code being executed by processors. Processes are launched by the operating system (since the operating system controls the execution flow) and have several properties: PID (unique identifier of a process); Name; User ID; Command line that was used to launch the process (arguments passed to the binary); Environment; CPU and memory usage; Other various OS-specific properties.

How to identify a process

When you monitor an application, you typically want to check that the application's processes are running properly. The problem lies in how to identify the processes of this application, how to recognize them amongst all of the running processes.

The only thing that really identifies a process is its PID (Process ID). But since the PID is an integer number randomly set upon the process startup, most often we cannot use it to identify the processes of an application (unless the application gives you its PID in a so-called PID file).

In general, you recognize application processes by their name if this criterion is enough to distinguish them from other processes. If the name of the process is not sufficient, you can identify application processes by parsing the process’s command lines. This is typically useful with scripts and java processes, whose process names are the same: java, CSCRIPT.EXE, etc.

Process name

Under Windows, the name of a process is basically the file name of the binary file which is being executed: Java.exe, IisAdmin.Exe. It always includes the " .EXE" extension. Process names can easily be shown in Windows Task Manager.

Under UNIX, the process name could be either the file name of the binary being executed, including the path or not, or something completely different (e.g. Oracle processes).

⚠️ The naming of processes is highly platform dependent. Linux processes are not named in the same way as on HP-UX servers, for example. Under UNIX, process names can be shown by executing the " ps –e –o name" command line.

Process command line

Every process is launched through a command line, which consists of the file path to the binary which has to be executed, and arguments that have to be passed to the binary: <path to the binary file> <argument1> <argument2> etc.
If the directory of the binary file is in the PATH environment variable, the path may not be included in the command line: `<binary file name> <argument1> <argument2> etc.

This is the only way to distinguish Java processes and scripts from others, because their process names are all identical (Java.EXE). Unfortunately, in Windows, there is no easy way to see the command lines of the currently running processes. Under UNIX, processes command lines can be shown by executing the "ps -e -o comm" command.

**Process user ID**

On both Windows and UNIX systems, processes run "as" a user. Depending on this, the process may be allowed to access various system resources (files, network, databases, etc.). In secured environments, most applications processes have to run as a specific user to let them access the application resources. If the processes run as another user, the application is very likely to fail and not run properly. This is why it could be important to check that the processes of the application you want to monitor are running as the appropriate user.

**PID file**

A classic way for applications to indicate they are running is to write the PID of their process into a given file. In this case we only need to read this file and check whether the PID written in the file corresponds to a running process. Please note that now the PID file is not provided for all the applications and most Windows applications do not provide PIDs.
About Regular Expressions

Regular expressions are used in Monitoring Studio to define strings to be searched for. A regular expression is:

- A string formatted with a specific syntax.
- It is intended to select some lines in a text, which will match the regular expression.

Regular expressions are commonly used in pattern matching, and especially on UNIX systems with the grep, awk and sed commands. You can use regular expressions in Monitoring Studio in order to:

- Find a process
- Search for strings in a file
- Check a web page
- Parse a table in a database

The following table describes the regular expression syntax that is supported in Monitoring Studio.

<table>
<thead>
<tr>
<th>Character</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| . (dot)   | Match any single character  
Example:  
Err.. will match Err01, Err02 or ErrAB, etc. |
| [xyz]     | Match any character in the brackets  
Example:  
Err[123] will match Err1, Err2 or Err3  
[Ee]rror will match either error or Error |
| [^xyz]    | Match any character not in the brackets  
Example:  
Err[^12345] will match Err0, Err6, Err7, etc. but not Err1 |
| [a-z]     | Match any character in the range in the brackets  
Example:  
Err[0-9] will match Err0, Err1, etc. and Err9  
Err[A-Z][0-9] will match ErrA0, ErrA1, ErrS9, ErrZ0, etc. but not Err1A  
Err[A-Z0-9] will match ErrA0, ErrA1, etc. and Err1A |
| [^a-z]    | Match any character not in the range in the brackets  
Example:  
Application[^0-9] will match ApplicationA, ApplicationB, Application! but not Application1 |
| *         | Match zero or more repetitions of the preceding  
Example:  
Err[0-9A-F]* will match Err, Err0, ErrA, Err11, ErrBF0001, etc.  
Error.*ApplicationABC will match all lines that contains Error and ApplicationABC further  
(Critical Error 0x000295F0 on ApplicationABC) |
| +         | Match one or more repetitions of the preceding  
Example:  
Err[0-9A-F]+ will match Err0, ErrA, Err11, ErrBF0001, etc. but not Err |
<p>| ^         | Match the beginning of the line |</p>
<table>
<thead>
<tr>
<th>Example: ^Err will match all lines that begin with Err</th>
</tr>
</thead>
</table>
| $ | Match the end of the line  
Example: [0-9]+ connections$ will match all lines that end with xxx connections where xxx is an integer |
| < | Match the beginning of a word  
Example: <set will match any line that contains a word that begins with set. It will not match a line that only contains the word unset |
| > | Match the end of a word  
Example: [Aa]pplication> will match all lines that contain the word Application or application but not ApplicationAA |
| \(\text{expression}\) | Defines an expression which has to be processed as a unit regarding the modifier *, + and \|  
Example: \(\_\[a-zA-Z0-9\]\)+ will match only sequences like _patrol, _patrol_agent, _patrol_console, etc. |
| exprA\|exprB | Match either exprA or exprB  
Example: \(\text{firewall}\)\(\text{antivirus}\) will match all lines that contains either the word firewall or the word antivirus |
| \ | Avoid the meaning of the following character  
Example: \. will match the single character dot (.)  
C:\\Program Files will match C:\Program Files |
About WMI

Definition

Windows Management Instrumentation (WMI) is a set of specifications from Microsoft for consolidating the management of devices and applications in a network from Windows computing systems. WMI is the Microsoft implementation of Web Based Enterprise Management (WBEM), which is built on the Common Information Model (CIM), a computer industry standard for defining device and application characteristics so that system administrators and management programs can control devices and applications from multiple manufacturers or sources in the same way.

What does it do?

WMI provides users with information about the status of local or remote computer systems. It also supports such actions as the configuration of security settings, setting and changing system properties, setting and changing permissions for authorized users and user groups, assigning and changing drive labels, scheduling processes to run at specific times, backing up the object repository, and enabling or disabling error logging. You can use WMI to manage both local and remote computers.

The word "Instrumentation" in WMI refers to the fact that WMI can get information about the internal state of computer systems, much like the dashboard instruments of cars can retrieve and display information about the state of the engine. WMI "instruments" by modeling objects such as disks, processes, or other objects found in Windows systems. These computer system objects are modeled using classes such as Win32_LogicalDisk or Win32_Process; as you might expect, the Win32_LogicalDisk class models the logical disks installed on a computer, and the Win32_Process class models any processes currently running on a computer. Classes are based on the extensible schema called the Common Information Model (CIM). The CIM schema is a public standard of the Distributed Management Task Force (http://www.dmtf.org/). WMI capabilities also include eventing, remoting, querying, views, user extensions to the schema, instrumentation, and more.

WMI Concepts

CIM Repository

CIM stands for Common Information Model and the repository is the WMI schema that stores the class definitions that model WMI-managed resources. The repository holds the information required to work with live resources in the computing environment. It does not contain actual data about these resources since this data is dynamically retrieved as required. It is this schema that allows the wide variety of different resources to be uniformly managed.
Namespace

CIM classes are organized into namespaces. Each namespace in the CIM contains a logical group of related classes representing a specific technology or area of management. Anytime a connection is made to WMI, a namespace must be specified. Only the classes contained within this namespace may be accessed by the connection. The most common namespace used for Windows management is root\cimv2. This contains the classes with the Win32_ prefix representing various components of the Windows operating system and hosting computer. Examples include Win32_Process (running processes in Windows), Win32_LogicalDisk (Windows logical disk drives), and Win32_ComputerSystem (the computer hosting Windows).

The namespace also includes the CIM_DataFile class which can be used to monitor files and folders. The following table lists common namespaces.

<table>
<thead>
<tr>
<th>Namespace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>root\cimv2</td>
<td>Contains the most useful classes including all Win32_ classes</td>
</tr>
<tr>
<td>root\default</td>
<td>Contains registry events</td>
</tr>
</tbody>
</table>

Class

Every resource managed by WMI is defined by a class. A class is a template for each type of resource and defines the properties that will be collected for that resource. Examples of common WMI classes are shown in the table below:

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Win32_Process</td>
<td>Processes running on a Windows computer</td>
</tr>
<tr>
<td>Win32_ComputerSystem</td>
<td>The computer running a Windows operating system</td>
</tr>
<tr>
<td>CIM_DataFile</td>
<td>A file stored on a disk</td>
</tr>
</tbody>
</table>

Instance

An Instance is a unique occurrence of a particular class. For example, each service installed on a Windows computer is an instance of the Win32_Service class. The C: drive is an instance of the Win32_LogicalDrive class.

<table>
<thead>
<tr>
<th>Instance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Winmgmt</td>
</tr>
<tr>
<td>DisplayName</td>
<td>Windows Management Instrumentation</td>
</tr>
<tr>
<td>PathName</td>
<td>C:\WINDOWS\system32\svchost.exe -k netsvcs</td>
</tr>
<tr>
<td>StartMode</td>
<td>Auto</td>
</tr>
<tr>
<td>State</td>
<td>Running</td>
</tr>
</tbody>
</table>
Property

A property is unique piece of information about an instance. All instances of a class will have the same set of properties although the values each instance’s properties may differ. Sample Properties of the Win32_Service class are shown in the table below:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of the service.</td>
</tr>
<tr>
<td>DisplayName</td>
<td>Displayed name of the service.</td>
</tr>
<tr>
<td>PathName</td>
<td>The command line path that was executed to start the service.</td>
</tr>
<tr>
<td>StartMode</td>
<td>Startup type of the service (Auto, Manual, or Disabled)</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the service (Running, Stopping, or Stopped)</td>
</tr>
</tbody>
</table>
Basic WMI Queries

Queries may be issued against WMI resources using WMI Query Language (WQL). WQL is a subset of SQL designed to retrieve information from WMI. A simple example of a WMI query would be: `SELECT * FROM Win32_Process`. This retrieves all attributes (the * is used as a wildcard) for all processes currently running on the computer. Win32_Process is the name of the WMI class for Windows processes.

WMI queries of this type are often issued from a script using Windows Script Host or from any application or tool that can access WMI. Queries retrieve specific information from instances of WMI resources or execute methods against instances to perform such actions as stopping services, or starting processes.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Example code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELECT</td>
<td>SELECT *</td>
<td>Specifies what properties are returned. Typically * is used to simply retrieve all.</td>
</tr>
<tr>
<td>FROM</td>
<td>FROM __InstanceCreationEvent</td>
<td>Specifies the event class to query. This will be the extrinsic or intrinsic event class.</td>
</tr>
<tr>
<td>WHERE</td>
<td>WHERE TargetInstance ISA 'Win32_Process' AND TargetInstance.Name = 'notepad.exe'</td>
<td>Filters the results. For intrinsic events, will usually include the ISA keyword to specify the class of the TargetInstance.</td>
</tr>
</tbody>
</table>

In case you need help to build your WMI query, you could download [WMI CIM Studio](#) – which is one of the WMI Administrative tools on the Microsoft site.
Index

A

About
  Process 314
  WMI 318
Acknowledgment
  Alerts 171
  All 172
  CollectionErrorCount 173
Acknowledgment
  Automatic 114, 123, 152
  Configuration 123
Add
  Credentials 234
Administration
  Features 170
Alarm
  Trigger 148
Alert 24
Alert Actions 24
  Annotate the graph 212
  Capabilities 212
  Customize 212
  Display a pop-up on the consoles 212
  Do not trigger any alert 180
  Example 230
  Execute a command 212
  Global 206
  Log to a file 212
  Macros 221
  Send a basic SNMP trap 212
  Send a custom SNMP trap 212
  Send an e-mail 212
  Specific 206
  Trigger a WARNING 180
  Trigger an ALARM 180
  Trigger an event 212
  Trigger an INFORMATION 180
Alert Thresholds
  Modify 180
  Set 179, 180
Alerts

Acknowledge 171

Analysis
  Command Line 81
  Database Query 86, 87, 90, 92, 94, 96
  log file 152
  WBEM Query 134
  WMI Query 136

Application Classes
  SEN_MS_COMMANDLINE 259
  SEN_MS_DBQUERY 86, 87, 90, 92, 94, 96
  SEN_MS_DYNAMIC 148, 263
  SEN_MS_DYNAMIC_CONT 264
  SEN_MS_DYNAMICDISCOVERY 265
  SEN_MS_DYNAMICNUMBER 266
  SEN_MS_DYNAMICSTRING 268
  SEN_MS_FILE 98, 269
  SEN_MS_FILESYSTEM 101, 271
  SEN_MS_FOLDER 103, 273
  SEN_MS_FORMULA 106, 275
  SEN_MS_GROUP 277
  SEN_MS_HOST 279
  SEN_MS_MAIN 239, 281
  SEN_MS_MONITORGROUP 283
  SEN_MS_NUMBER 157, 284
  SEN_MS_PROCESS 69, 239, 286
  SEN_MS_SNMPOLLING 109, 288
  SEN_MS_SNMPTRAP 114, 290
  SEN_MS_STRING 152, 292
  SEN_MS_TRANSFORM 294
  SEN_MS_WBEMQUERY 134, 295
  SEN_MS_WEBREQUEST 117, 297
  SEN_MS_WINEVENT 123, 299
  SEN_MS_WINPERF 127, 301
  SEN_MS_WINSERVICE 130, 303
  SEN_MS_WMIQUERY 136, 305

Architecture 14

Authentication
  HTTP 309
Automatic
  Acknowledgment 114, 123, 152

B

Baselines 307
BMC
  BMC Installation Utility 28
  BMC Performance Manager 53
BMC
  BMC Performance Manager Monitoring Studio 45
  BMC Portal 53
  BMC Software Installation utility 28
Builder
  Dynamic Object 148

- C -

CA
  Mode 197
Cache
  Refresh 80, 101, 123, 239
Changes 9
CIM 134, 136
  CIM contains 318
  CIM Repository 318
  CIM stands 318
  CIM_DataFile 318
Class
  CIM_DataFile 318
  Win32_ComputerSystem 318
  Win32_Process 318
Classic
  Mode 197
Classic Mode
  Force 197
Collectors
  Common 239
Column Separator
  Blank 152, 157
  Comma 152, 157
  Point 152, 157
Command
  Execute 212
  External 139
Command Execution
  Never ending 81
Command Line 86, 96, 314
  Analysis 81
  Specify 139
Command Line Macros 221
Commands
  About... 281
  Acknowledge Alerts 269, 271, 273, 275, 279, 284, 286, 288, 295, 297, 301, 303, 305
  Acknowledge Alerts... 259
Acknowledge All and Reset 281, 290, 292, 299
Alert actions 259, 261, 269, 271, 273, 275, 277, 279, 284, 286, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
awk 316
Copy 259, 269, 271, 273, 275, 277, 279, 283, 284, 286, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
Cut 259, 269, 271, 273, 275, 279, 283, 284, 286, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
Debug 281
Delete 259, 269, 271, 273, 275, 277, 279, 283, 284, 286, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
Delete all 277, 279, 283
Discovery Interval 281
Display Entire Configuration 281
Dynamic Object Builder 259, 261, 269, 288, 294, 295, 297
Edit 259, 261, 269, 271, 273, 275, 279, 284, 286, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
Edit Credentials 279
Export Configuration 281
File Viewer 279
Force Classic Configuration Mode 281
grep 316
Group Constants 277
Hosts 277
Import Configuration 281
Java Settings 281
Monitor 279, 283
Monitor Group 279
New Credentials 279
New Group 281
Numeric Value Extraction 259, 261, 269, 288, 294, 295, 297, 305
Paste 259, 269, 271, 277, 279, 281, 283, 288, 294, 295, 297, 301, 305
Pause Monitoring 259, 269, 271, 273, 275, 277, 279, 283, 284, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
Polling Interval 259, 261, 269, 271, 273, 277, 279, 286, 288, 295, 297, 299, 301, 303, 305
Polling Intervals 275
Commands
Properties 259, 261, 269, 271, 273, 275, 277, 279, 283, 284, 286, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
Real-time SNMP Trap listener 281
Refresh Parameters 259, 269, 271, 273, 275, 277, 279, 281, 288, 290, 295, 297, 299, 301, 303, 305
Rename 269, 271, 273, 275, 277, 283, 284, 286, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
Rename... 259
Report 281
Reset CollectionErrorCount 281
Restart scan 269
Resume Monitoring 259, 269, 271, 273, 275, 277, 279, 283, 284, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
Schedule Report 281
sed 316
Show Configuration 281
SNMP Browser 279
String Search 259, 261, 269, 288, 294, 295, 297, 305
Text Pre-Processing 259, 261, 269, 295, 297
Thresholds 259, 261, 269, 271, 273, 275, 277, 279, 281, 284, 286, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
Thresholds Mechanism Selection 281
Trigger a KM Discovery 281
View file content 269
Windows Event Log Reader 279

Community 109
Configuration
Automatic Acknowledgment 123
Export 186
Import 190
Monitoring Studio 186
Report 245

Configure
Group 58
Host 58
Monitor 58

Connection 96
Database 87, 90, 92, 94, 96
Information 86
Method 86
ODBC 96
Settings 87, 90, 92, 94, 96

String 96
Console Administration 197
Console system
Requirements 27
Content
Viewer 244
Copy
Monitoring Tools 184
Create
Command Line 81
Database Query Analysis 86
Dynamic Object 148
File System Monitoring 101
Folder Monitoring 103
Group 59
Monitor Group 67
Multi-Parameter Formula 106
Numeric Value Search 157
Process Monitoring 69
SNMP polling 109
String Search 152
Text Preprocessing object 139
WBEM Query Analysis 134
Web Request Analysis 117
Windows event monitoring 123
Windows Performance Monitoring 127
Windows Service Monitoring 130
WMI Query Analysis 136

Credentials 234
Add 234
Delete 234
Edit 234
Manage 21, 234
System 62
Criteria 69
Cut
Monitoring Tools 184

-D-

Database
Connection 96
Microsoft SQL 86
Microsoft SQL Server 87
MySQL 86
MySQL Server 90
Oracle 86, 92
Other 96
- E -

D - E -

Edit
Command Line 81
Credentials 234
Database Query Analysis 86
Dynamic Object 148
File System Monitoring 101
Folder Monitoring 103
Group 59
Instance 196
Monitored Object 196
Multi-Parameter Formula 106
Numeric Value Search 157
Process Monitoring 69
SNMP polling 109
String Search 152
Text Preprocessing object 139
WBEM Query Analysis 134
Web Request Analysis 117
Windows event monitoring 123
Windows Performance Monitoring 127
Windows Service Monitoring 130
WMI Query Analysis 136
Enable
Debug Mode 248

Event 24
Example 69, 81, 123, 139, 180
Alert Actions 230
Execute
Command 212
Execution
Period 81
Timeout 81
Export
Configuration 186
Group Configuration 186
Monitoring Studio Configuration 186
Extract
Setup Files 29
Text from HTML 139
Extraction
Numeric Value 157

- F -

FAQ
Although SNMP Trap listening seems to work, no trap matches my criteria 250
Can I monitor the processor time usage made by a Windows service? 251
How do I know which version of Monitoring Studio I am running? 250
I'm unable to poll an SNMP agent (getting a Warning) 252
I'm unable to see the Monitoring Studio icons in PATROL Central 252
Infinite loop reported in the PATROL Agent log 252
Is it possible to monitor the CPU/memory usage of a process tree? 253
Monitoring Studio does not follow an HTTP redirection (Web) 254
Monitoring Studio does not update all of my folder monitoring parameters 251
Monitoring Studio fails to authenticate on my Web server 253
Monitoring Studio fails to connect to a secured Web server (SSL) on my UNIX/Linux server 253
Monitoring Studio is unable to listen to SNMP traps 250
Monitoring Studio reads my log file entirely 251
Not able to post a Web form to my Web server 254

Database
PostgreSQL 94
Settings 96
Database Macros 221
Database Query Analysis 86
Debug Mode Enable 248
Delete
Credentials 234
Monitored Object 195
Diagram 14
Discovery Interval Set 238
Display name 79
DMTF 134
Dynamic Object Builder 148
Dynamic Object Builder 148
Dynamic Objects Macros 221
Features
  Administration 170
File
  flat 98, 251
  Growth 98
  log 98, 251
  Monitor 162
  Monitoring 98
  PID 314
  Presence 98
  Size 98
File Content
  Viewer 244
File Macro 221
File System
  Monitoring 101
Files
  PID 69
  flat
  File 251
  flat File
  Monitoring 98
Folder
  Monitoring 103
Folder Monitoring
  Create 103
  Edit 103
Force
  Classic Mode 197
Format Symbols
  %%% 228
  %a 228
  %b 228
  %c 228
  %d 228
  %e 228
  %Ec 228
  %Ex 228
  %Ey 228
  %h 228
  %I 228
  %j 228
  %k 228
  %l 228
  %m 228
  %n 228
  %Od 228
  %Oe 228
  %OH 228
  %OI 228
  %Om 228
  %OS 228
  %OU 228
  %Ow 228
  %Oy 228
  %p 228
  %r 228
  %S 228
  %t 228
  %u 228
  %V 228
  %w 228
  %x 228
  %y 228
  %Z 228

Formula
  Multi-Parameter 106

-G-
General Concepts 18, 19, 21, 23, 24
Getting Started 14
Global
  Settings 190
Group
  Constants 59, 203
  Create 59
  Edit 59
Growth
  Size 98

-H-
Host 19, 62, 109
  Identify 134, 136
Host availability
  Hostname 62
  Ping 62
  SNMP 62
  SSH 62
  TCP Port 62
HTTP
  Authentication 309
HTTP authentication schemes
  Basic 117
  Digest 117
  NTLM 117
HTTP Macros 221

Icons
  Container 59
  Group 59
ID
  Monitor 310
Identify
  Host 134, 136
  Process 314
Import
  Configuration 190
  Global Settings 190
  Group Configuration 190
  Group Constants 190
  Monitoring Studio Configuration 190
Improvements 9
Infobox 250, 283
  Acknowledge 292, 299
  Acknowledge Alerts 261
  Acknowledging Event ID 299
  Acknowledging OID 1 290
  Acknowledging OID 2 290
  Acknowledging String 292
  Acknowledging String 1 290
  Acknowledging Trap Number 290
After/Before 266, 284
BMC TrueSight Device 279
Character Offset 266, 284
Child Process IDs 286
Column Mode 266, 284
Command Line 259
Community 288, 290
Connect as 261
Connection Type 261
Constant 1 277
Constant 2 277
Constant 3 277
Constant 4 277
Constant 5 277
Contact 277
Copy 261
Copyright 281
Credentials 279
Cut 261
Database name 261
Database Type 261
Delete 261
Description 277
Enterprise ID 290
Event ID 299
Event log 299
Field Number 266, 284
Field Separators 266, 284
File 269
File System 271
File Type 269
Folder 273
Formula 275
Host 295
Hostname 279, 288
ID 259, 261, 263, 266, 268, 269, 271, 273, 275, 277, 279, 284, 286, 288, 290, 292, 294, 295, 297, 299, 301, 303, 305
Include subfolders 273
Instance Name 301
Line Mode 266, 284
Line Number 266
Lines 268, 292
Monitored File 269
Name Space 295
Namespace 305
OID 288
OID 1 290
OID 2 290
OID type 288
Parameter Type 266, 284
Parent ID 259, 261, 266, 268, 269, 271, 273, 275, 279, 284, 286, 290, 292, 294, 295, 297, 299, 301, 303, 305
Parent type 284, 292, 294
Paste 261
Path 303
Pause monitoring 261
Performance Counter 301
Performance Object 301
Port 288, 295
Process IDs 286
Product 281
Protocol 295
Provider 299
Refresh Parameters 261
Regular Expression 266, 284
Method
  Get 117
  Post 117
  Post Web Service 117
MIB
  Management Information Base 109
Microsoft SQL Server Database
  Connection 87
  Settings 87
Minimum Cache Refresh Interval
  Set 80, 101, 123
Modify
  Alert Thresholds 180
  Group Constants 203
  Object ID 199, 201
  Object Name 199, 201
Monitor
  Command Lines 68
  Database Queries 68
  File 162
  File Systems 68
  Files 68
  Folders 68
  log File 230
  Multi-Parameter Formula 68
  Performance Counters 68
  Processes 68
  Settings 79
  SNMP Agents 68
  SNMP Traps 68
  Technology 59
  WBEM Queries 68
  Web Requests 68
  Windows Events 68
  Windows Services 68
  WMI Queries 68
Monitor Group 19
  Create 67
  Monitor Internal Identifier 310
  Monitor Settings 79
Monitored Object
  Delete 195
  Monitoring 204
    File 98
    File System 101
    Folder 103
    Pause 204
    Process 69, 70, 71, 74, 76, 77
    Suspend 204
    Windows Event 123
    Windows Event log 123
    Windows Performance 127
    Windows Service 130
Monitoring Features
  Command Line Analysis 148
  Database Query Analysis 148
  File Monitoring and Analysis 148
  SNMP Polling 148
  Text Pre-Processing 148
  WBEM Query Analysis 148
  Web Request Analysis 148
  WMI Query Analysis 148
Monitor Group 19
  Configuration 186
    Settings 59, 69, 81, 101, 103, 109, 114, 123, 127, 130, 134, 136, 139, 152, 157
Monitors 19, 67
Move
  Monitoring Tools 184
  MPF Macros 221
  Multi-Parameter
    Formula 106
    MySQL Server Database
    Connection 90
    Settings 90
- N -
  Namespace 318
  New 9
  Numeric Value 23
    Extraction 157
    Lines 157
    Location 157
    Search 157
  Numeric value extraction 23
- O -
  Object
    Edit 196
    Object Specific Macros 221
Monitoring Studio KM for PATROL 9.0.0

**ODBC**  86
  - Connection  96
  - Settings  96

**Operating Systems**
  - Compatibility  68

**Option**
  - Rescaling  157

**Oracle Database**
  - Connection  92
  - Settings  92

**OS**
  - Compatibility  68

**Overview**  14

- **P** -

**Packages**
  - Download  28

**Parameters**  123, 283
  - Alert actions  265
  - AvailableCapacity  271
  - AvailableCapacityPercentage  271
  - AvailableInodesPercentage  271
  - ChildCount  69, 253, 286
  - CollectionErrorCount  277, 281
  - ConnectionStatus  86
  - ConsumedCapacityGrowthPercentage  271
  - ConsumedCapacityGrowthSpeed  271
  - Content  109, 288
  - Copy  265
  - Count  69, 286
  - Cut  265
  - DebugStatus  281
  - Delete  265
  - DeletedFileCount  103
  - DeletedFileRate  273
  - Delta  266
  - DeltaPerSecond  266
  - Edit  265
  - ExecutionTime  109, 259, 261, 288, 295, 297, 305
  - Exists  269, 273
  - ExitStatus  259
  - ExtractedLine  263
  - FileCount  103, 273
  - FolderSize  103
  - FreeMegabytes  101
  - FreeSpacePercent  101
  - GrowthPercentage  103, 269, 273
  - GrowthSpeed  103, 269, 273
  - HostCount  281
  - HTTPStatus  297
  - HTTPStatusCode  297
  - LastChanged  269
  - LastMatchingLines  292
  - LastModifiedFileElapsedTime  103, 273
  - LongestTimeFileRemainsInFolder  103, 273
  - MatchingEventCount  123, 299
  - MatchingEventRate  123, 299
  - MatchingEvents  299
  - MatchingLineCount  152, 230, 268, 292
  - MatchingLineRate  292
  - MatchingProcesses  286
  - MatchingTrapCount  114, 290
  - MatchingTrapRate  290
  - ModifiedFileCount  103
  - ModifiedFileRate  273
  - MonitorCount  281
  - NewFileCount  103
  - NewFileRate  273
  - Numeric Value Extraction Template  265
  - OldestModifiedFileElapsedTime  103, 273
  - PageFaultsPerSec  69, 286
  - PageFileBytes  69, 286
  - Paste  265
  - PrivateBytes  69, 286
  - ProcessorTime  69, 286
  - Properties  265
  - Refresh  205
  - Remove Missing Items  265
  - Rename  265
  - Result  134, 136, 259, 261, 295, 297, 305
  - Select  69, 157
  - ServerConnectionState  117
  - ServiceDetails  303
  - Size  269, 273
  - Status  109, 134, 148, 259, 261, 263, 279, 288, 285, 297, 305
  - String Search Template  265
  - ThreadCount  69, 286
  - TransformResult  139, 162, 294
  - UsedSpaceGrowthPercentage  101
  - UsedSpaceGrowthSpeed  101
  - Value  109, 266, 275, 284, 288, 301
  - ValueFound  266, 284
  - VirtualBytes  69, 286
Parameters 123, 283
Working Set 69, 286
Parsing
XML LOG File 162
Paste
Monitoring Tools 184
PATROL
BMC Impact Manager 212
BMC Software PATROL Console 27
Console Server 252
Event 212
PATROL administrator 148
PATROL Agent 32, 186, 252
PATROL Agents 252
PATROL Central 32, 252
PATROL Central Operator 27
PATROL Configuration Manager 179
PATROL Console 32
PATROL Console Servers 32
PATROL Console Web-edition 27
PATROL Consoles 212
PATROL Enterprise Manager 212
PATROL for Event Management 179
PATROL interface 186
PATROL event
Trigger 230
Pause
Monitoring 204
Period
Execution 81
Pick
Process 69
PID
File 314
Files 69
Polling Interval
Set 239
Port 109
PostgreSQL Database
Connection 94
Settings 94
Pre-processing 162
Convert multi-line records to single records 139
Convert XML to CSV 139
Text 139
Text processing through an external command 139
Presence
File 98
Process
About 314
Command Line 314
Criteria 69
Identify 314
Monitoring 69, 70, 71, 74, 76, 77
Name 314
Parameters 77
Pick 69
Status interpretation 77
User ID 314
Process Macros 221
Process monitoring method
List 71
PID file path 76
Search criteria 74
Process Viewer
Tool 241
Product Aarchitecture 19
Product hierarchy 19
Properties
Command line 69, 314
Name 69, 314
PID 69, 314
Tool 245
User ID 69, 314
Property
DisplayName 318
Name 318
PathName 318
StartMode 318
State 318
Proxy
Server 117
Settings 117
- Q -
Query
Set 86
SQL 86
- R -
Reference Guide 256
Refresh
Cache 80, 101, 123, 239
Parameters 205
Regular Expressions
$  316
*  316
. (dot)  316
[^a-z]  316
[^xyz]  316
[a-z]  316
[xyz]  316
\  316
\(expression\)  316
\<  316
\>  316
^  316
+  316
exprA\|exprB  316
Release Notes  9
Remove
Group  59
Icon  59
Report
Configuration  245
Request
Web  117
Requirements
Console systems  27
Managed systems  27
Rescaling  109
Option  157
Reset
All  172
CollectionErrorCount  173
REST  117
Restart
Scan  98
Result  69

-S-
Scan
Restart  98
Search
String  152
Select
Counter  127
Instances  127
Lines  152
Parameters  69, 109, 157
Windows Performance object  127
Windows Service  130
Separator  157
Comma  152
Set
Alert Thresholds  179, 180
Discovery Interval  238
Minimum Cache Refresh Interval  80, 101, 123
Polling Interval  239
Settings
Connection  87, 90, 92, 94, 96
Global  190
Java  174
Microsoft SQL Server  87, 96
Monitoring Studio  59, 69, 81, 86, 101, 109, 114, 123, 127, 130, 134, 136, 139, 152, 157
MySQL Server  90
Oracle  92
PostgreSQL Server  94
Setup Files
Extract  29
Signature Files  62
Size
File  98
SNMP
Agent  109
Polling  109
SNMP Trap Listener  242
Table OID  109
Trap  114
SNMP Browser
Tool  246
SNMP Browser tool  252
SNMP polling
Create  109
Edit  109
SNMP Polling Macros  221
SNMP Trap
Listening  114
SNMP Trap Listener
Tool  242
SNMP Trap Listener tool  250
SNMP Trap Macros  221
SOAP
Authentication  117
Request  117
Specific Credentials  21, 234
Monitoring Studio KM for PATROL 9.0.00

Specify
  Command Line 139
Streams
  stderr 81
  stdout 81
String 23
  Search 152
String Search 23
  Create 152
  Edit 152
String Search Macros 221
Suspend
  Monitoring 204
System Credentials 21, 62
Systems
  Linux 27, 28, 29
  UNIX 27, 28, 29, 32, 314, 316
  Windows 27, 28, 29, 32, 314

-T-
Templates
  Numeric Value Extraction 148
  String Search 148
Test 103
Text
  Pre-Processing 139
Text Preprocessing object
  Create 139
  Edit 139
Threshold 24
Thresholds
  Advanced 180
  Automatic 179
  Custom 69, 79, 81, 86, 101, 103, 106, 109, 114, 117, 123, 127, 130, 134, 136, 152, 157
  Default 69, 79, 81, 86, 101, 103, 106, 109, 114, 117, 123, 127, 130, 134, 136, 152, 157
Event Management 179
  Manage 179
  Mechanism mode 179
  Simple 180
  Type 180
Update 53
Timeout
  Execution 81
Tool
  Process Viewer 241

Properties 245
SNMP Browser 246
SNMP Trap Listener 242
Windows Event log Reader 243
Traps
  Incoming 250
Trigger
  Alarm 148
  Event 230
Troubleshooting 248
  Although SNMP Trap listening seems to work, no trap matches my criteria 250
  Can I monitor the processor time usage made by a Windows service? 251
  How do I know which version of Monitoring Studio I am running? 250
  I'm unable to poll an SNMP agent (getting a Warning) 252
  I'm unable to see the Monitoring Studio icons in PATROL Central 252
  Infinite loop reported in the PATROL Agent log 252
  Is it possible to monitor the CPU/memory usage of a process tree? 253
  Monitoring Studio does not follow an HTTP redirection (Web) 254
  Monitoring Studio does not update all of my folder monitoring parameters 251
  Monitoring Studio fails to authenticate on my Web server 253
  Monitoring Studio fails to connect to a secured Web server (SSL) on my UNIX/Linux server 253
  Monitoring Studio is unable to listen to SNMP traps 250
  Monitoring Studio reads my log file entirely 251
  Not able to post a Web form to my Web server 254
Tuning 179

-U-
Uninstall
  BMC Performance Manager Monitoring Studio 45
Update
  Thresholds 53
URL 117
- V -
Variables
   folderLimit  251
View
   Content  244
   Properties  245

- W -
WBEM  136, 318
   Query  134
WBEM Macros  221
WBEM Query Analysis
   Create  134
   Edit  134
WEB  117
Web Request Analysis
   Create  117
   Edit  117
Windows Event
   Monitor  123
   Monitoring  123
   Types  123
Windows Event log
   Application  123
   Monitor  123
   Security  123
   System  123
Windows Event log Reader
   Tool  243
Windows Event Macros  221
Windows event monitoring
   Create  123
   Edit  123
Windows Performance
   Monitoring  127
Windows Performance Macros  221
Windows Performance Monitoring
   Create  127
   Edit  127
Windows Service
   Monitoring  130
Windows Service Macros  221
Windows Service Monitoring
   Create  130
   Edit  130

- X -
XML LOG File
   Parsing  162
About Sentry Software™
Sentry Software, a strategic Technology Alliance Partner of BMC Software, provides comprehensive multi-platform monitoring solutions that enable management of the hardware and software aspects of all servers and SANs and covering up to 100% of custom applications within the BMC ProactiveNet Performance Management environment. Sentry Software also develops adapters for BMC Atrium Orchestrator that enables IT administrators to automate the execution of common requests and tasks that occur in the daily course of IT operations. Combined with BMC’s servers and network automation tools, the adapters allow IT administrators to implement provisioning and decommissioning workflows that cover all layers of their IT infrastructure. Finally, Sentry Software designs connectors that bring storage capacity metrics into BMC TrueSight Capacity Optimization to ensure IT administrators that their storage infrastructure is properly sized for their current and future needs.

About BMC Software™
BMC Software helps leading companies around the world put technology at the forefront of business transformation, improving the delivery and consumption of digital services. From mainframe to cloud to mobile, BMC delivers innovative IT management solutions that have enabled more than 20,000 customers to leverage complex technology into extraordinary business performance—increasing their agility and exceeding anything they previously thought possible. For more information about BMC Software, visit www.bmc.com.

ABOUT MARKETZONE DIRECT PRODUCTS
The BMC MarketZone Direct program sells and supports third-party products that complement and/or augment BMC solutions. MarketZone Direct products are available under BMC license and support terms.

BUSINESS RUNS ON I.T.
I.T. RUNS ON BMC SOFTWARE
Business thrives when IT runs smarter, faster and stronger. That’s why the most demanding IT organizations in the world rely on BMC Software across distributed, mainframe, virtual and cloud environments. Recognized as the leader in Business Service Management, BMC offers a comprehensive approach and unified platform that helps IT organizations cut cost, reduce risk and drive business profit. For the four fiscal quarters ended September 30, 2011, BMC revenue was approximately $2.2 billion.

LEARN MORE
To learn more about our solutions, please visit: www.sentrysoftware.com/solutions

Like us on Facebook: facebook.com/sentrysoftware
Follow us on Twitter: twitter.com/sentrysoftware