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.

<table>
<thead>
<tr>
<th>United States and Canada</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
</tr>
<tr>
<td>BMC Software, Inc.</td>
</tr>
<tr>
<td>2101 CityWest Blvd. Houston TX 77042-2827</td>
</tr>
</tbody>
</table>

Copyright 2006 BMC Software, Inc. or licensors, as an unpublished work.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 UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES.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.
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. To expedite your inquiry, please see "Before Contacting BMC Software."

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

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.

Before Contacting BMC Software

Before you contact BMC Software, have the following information available so that Customer Support can begin working on your problem immediately:

- Product information
- product name
- product version (release number)
- license number and password (trial or permanent)
- Operating system and environment information machine type operating system type, version, and service pack or other maintenance level such as:
  - PUT or PTF
  - system hardware configuration
  - serial numbers
  - related software (database, application, and communication) including type, version, and service
  - pack or maintenance
  - level
- Sequence of events leading to the problem
- Commands and options that you used
- Messages received (and the time and date that you received them)
- product error messages
# Table of Contents

## Requirements

Getting the BMC Software Installation utility .................................................................................. 18

## Packages

Extracting the Setup Files ............................................................................................................. 19

Installing Monitoring Studio KM for PATROL ............................................................................ 21

Uninstalling Monitoring Studio KM for PATROL ......................................................................... 34

Integrating with BMC Portal ........................................................................................................ 41

Integrating with BMC ProactiveNet Performance Management .................................................. 42

1. Creating the Application Icon ................................................................................................ 45

2. Specifying the Resources Used ............................................................................................... 49

## Monitoring Processes

1. Configuring Process Command Credentials .......................................................................... 50

2. Specifying the Process to be monitored ................................................................................ 51

   Picking the Process to Monitor from a List ............................................................................... 52

   Entering Search Criteria .......................................................................................................... 53

   Providing the PID file path ....................................................................................................... 55

3. Selecting Parameters .............................................................................................................. 56

4. Configuring the Monitoring Studio settings .......................................................................... 57

## Monitoring a Windows Service

## Monitoring a File System

## Monitoring Folders

## Monitoring Files

## Checking File Security Settings

## Monitoring Loaded KMs

## Monitoring Windows Performance

3. Specifying the Information Sources ......................................................................................... 81

## Analyzing Command Lines

## Analyzing a Database Query

   Setting connection to Microsoft SQL Server Databases ......................................................... 93

   Setting connection to MySQL Server Databases .................................................................. 96

   Setting connection to Oracle Database Server .................................................................... 100

   Setting connection to Other Databases (ODBC only) ............................................................ 104
# Table of Contents

- Setting Connection to Postgre SQL Databases ................................................................. 105
- Monitoring Web Farms ........................................................................................................ 107
- Analyzing Web Requests ................................................................................................ 112
- Analyzing WBEM Queries ............................................................................................... 115
- Analyzing WMI Queries .................................................................................................. 118
- Polling MBean Application Servers ................................................................................ 121
  - Generic JMX Client .......................................................................................................... 124
  - JBoss .............................................................................................................................. 130
  - JOnAS ............................................................................................................................. 136
  - WebLogic ....................................................................................................................... 142
  - WebSphere .................................................................................................................... 150
- Input variables for JMX polling Wizards .......................................................................... 156
- Monitoring SNMP Agents & Traps .................................................................................... 157
  - Polling SNMP Agents .................................................................................................... 158
  - Listening for SNMP Traps .............................................................................................. 162
- Monitoring Windows Events ............................................................................................ 166
- 4. Specifying the Information to be Searched ................................................................. 171
- Pre-Processing Text .......................................................................................................... 171
- Searching for a Specific String .......................................................................................... 181
- Extracting Numeric Values ............................................................................................... 185
- Monitoring Dynamic Return Outputs ............................................................................. 192
- Example: XML LOG File Parsing .................................................................................... 197
- 5. Configuring Thresholds ................................................................................................. 206
- Specifying the Threshold Mechanism Mode ..................................................................... 206
- Setting or Modifying Alert Thresholds ............................................................................. 207
- Setting Thresholds on Dynamic Numeric Value Extractions ........................................... 211
- 6. Specifying Alert Actions ............................................................................................... 211
- Alert Actions Capabilities .................................................................................................. 217
- Alert Action Macros .......................................................................................................... 227
- Alert Actions Example ...................................................................................................... 231
- 7. Configuring Advanced Settings Options ..................................................................... 236
- Configuring the Application Monitoring Start and Stop .................................................. 237
- Specifying Signature Files ............................................................................................... 238
- Configuring Application Constants .................................................................................. 239
- 8. Deploying your Configuration ...................................................................................... 241
- Exporting Configuration to a File ...................................................................................... 241
**Table of Contents**

- Importing Configuration .................................................................................................................. 245
- Displaying Entire Configuration ....................................................................................................... 250
- Displaying Object Configuration ..................................................................................................... 250
- Instant Configuration Reports .......................................................................................................... 251
- Scheduling Configuration Reports .................................................................................................... 252
- Acknowledging Alerts ....................................................................................................................... 258
- Acknowledge Alerts ............................................................................................................................ 258
- Acknowledge all and Reset ................................................................................................................. 259
- Acknowledge and Update .................................................................................................................... 259
- Configuring Java Settings ................................................................................................................... 260
- Copy, Cut and Paste ............................................................................................................................. 263
- Editing a Monitored Object ................................................................................................................ 264
- Modifying Object Name and/or ID ...................................................................................................... 264
- Pause the Monitoring of an Object .................................................................................................... 265
- Refreshing Parameters ......................................................................................................................... 265
- Rename an Object ............................................................................................................................... 266
- Restart an Application ......................................................................................................................... 268
- Restart Scan from the Beginning of the File ....................................................................................... 268
- Setting the Discovery Interval ............................................................................................................ 269
- Setting the Polling Interval ................................................................................................................. 269
- Stop an Application ............................................................................................................................. 271
- Triggering a KM Discovery ................................................................................................................ 271
- Visualizing Currently Running Processes .......................................................................................... 272
- Visualizing SNMP Traps ..................................................................................................................... 273
- Visualizing Windows EventLogs ....................................................................................................... 274
- Visualizing Monitored File Content ................................................................................................. 275
- Visualizing SNMP Agent Variables .................................................................................................. 276
- Deleting Monitored Object(s) .......................................................................................................... 276
- Enabling the Debug Mode .................................................................................................................. 278
- Frequently Asked Questions and Problems ..................................................................................... 279
- Although SNMP Trap listening seems to work, no trap matches my criteria .................................. 279
- Can I monitor the processor time usage made by a Windows service? ............................................ 279
- Can I search for Windows Events whose description match a regular expression ......................... 279
- Difference between a flat file and a LOG file ................................................................................... 280
- How do I know which version of Monitoring Studio I am running? .............................................. 282
- I’m unable to connect to WebLogic application server ................................................................. 283
<table>
<thead>
<tr>
<th>Issue</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I'm unable to connect to WebSphere application server</td>
<td>283</td>
</tr>
<tr>
<td>I'm unable to poll an SNMP agent (getting a Warning)</td>
<td>283</td>
</tr>
<tr>
<td>I'm unable to see the Monitoring Studio icons in PATROL Central</td>
<td>284</td>
</tr>
<tr>
<td>Infinite loop reported in the PATROL Agent log</td>
<td>284</td>
</tr>
<tr>
<td>Is it possible to monitor the CPU/memory usage of a process tree?</td>
<td>285</td>
</tr>
<tr>
<td>Monitoring Studio does not read the content of my file</td>
<td>285</td>
</tr>
<tr>
<td>Monitoring Studio does not update all of my folder monitoring parameters</td>
<td>285</td>
</tr>
<tr>
<td>Monitoring Studio fails to connect to my Oracle Database server</td>
<td>286</td>
</tr>
<tr>
<td>Monitoring Studio fails to connect to my remote Microsoft SQL Server</td>
<td>286</td>
</tr>
<tr>
<td>Monitoring Studio fails to connect to a secured Web server (SSL) on my UNIX/Linux server</td>
<td>286</td>
</tr>
<tr>
<td>Monitoring Studio fails to authenticate on my Web server</td>
<td>286</td>
</tr>
<tr>
<td>Monitoring Studio does not follow an HTTP redirection (Web)</td>
<td>287</td>
</tr>
<tr>
<td>Monitoring Studio is unable to listen to SNMP traps</td>
<td>287</td>
</tr>
<tr>
<td>Monitoring Studio reads my LOG file entirely</td>
<td>287</td>
</tr>
<tr>
<td>What is the meaning of the &quot;Argument1, 2...&quot; fields in the Windows Event monitoring wizard?</td>
<td>288</td>
</tr>
<tr>
<td>Not able to post a Web form to my Web server</td>
<td>288</td>
</tr>
<tr>
<td>Format Symbols for %{ASCTIME:...} Macros</td>
<td>290</td>
</tr>
<tr>
<td>Regular Expressions</td>
<td>292</td>
</tr>
<tr>
<td>Application Classes</td>
<td>293</td>
</tr>
<tr>
<td>List of Application Classes</td>
<td>294</td>
</tr>
<tr>
<td>SW_APPLICATIONS</td>
<td>295</td>
</tr>
<tr>
<td>SW_DB_QUERIES</td>
<td>297</td>
</tr>
<tr>
<td>SW_DYNAMIC</td>
<td>299</td>
</tr>
<tr>
<td>SW_DYNAMIC_CONTAINER</td>
<td>299</td>
</tr>
<tr>
<td>SW_DYNAMIC_DISCOVERY</td>
<td>300</td>
</tr>
<tr>
<td>SW_DYNAMIC NUMBERS</td>
<td>301</td>
</tr>
<tr>
<td>SW_DYNAMIC_STRINGS</td>
<td>302</td>
</tr>
<tr>
<td>SW_FILES</td>
<td>302</td>
</tr>
<tr>
<td>SW_FILESYSTEMS</td>
<td>304</td>
</tr>
<tr>
<td>SW_FILE_SECURITY</td>
<td>305</td>
</tr>
<tr>
<td>SW_FOLDERS</td>
<td>306</td>
</tr>
<tr>
<td>SW_HTTP_REQUESTS</td>
<td>308</td>
</tr>
<tr>
<td>SW_HTTP_WEBFARM</td>
<td>309</td>
</tr>
<tr>
<td>SW_JMX</td>
<td>310</td>
</tr>
<tr>
<td>SW_KMWATCH</td>
<td>312</td>
</tr>
<tr>
<td>SW_NTEVENTS</td>
<td>313</td>
</tr>
<tr>
<td>Category</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------</td>
<td>------</td>
</tr>
<tr>
<td>SW_NTPERFORMANCE</td>
<td>314</td>
</tr>
<tr>
<td>SW_NTSERVICES</td>
<td>315</td>
</tr>
<tr>
<td>SW_NT_WMI</td>
<td>316</td>
</tr>
<tr>
<td>SW_NUMBERS</td>
<td>318</td>
</tr>
<tr>
<td>SW_OSCOMMANDS</td>
<td>319</td>
</tr>
<tr>
<td>SW_PROCESSES</td>
<td>321</td>
</tr>
<tr>
<td>SW_SENTRY</td>
<td>322</td>
</tr>
<tr>
<td>SW_SNMP_POLLING</td>
<td>324</td>
</tr>
<tr>
<td>SW_SNMP_TRAPS</td>
<td>326</td>
</tr>
<tr>
<td>SW_STRINGS</td>
<td>327</td>
</tr>
<tr>
<td>SW_TRANSFORM</td>
<td>328</td>
</tr>
<tr>
<td>SW_WBEM</td>
<td>329</td>
</tr>
</tbody>
</table>
Release Notes for v8.6.54
What's New

- Full support of PATROL Agent v9.0.00 and higher.
- Database queries can now be performed natively on PostgreSQL databases with the Database Query Analysis tool. The connection method to be used is either the command line utility or the Java Database Connectivity.
- **JMX Monitoring**: The JMX Monitoring tool now supports the following MBean application servers:
  - JBoss 5.x, 6.x, and 7.x (EAP 6.x).
  - JOnAS 5.x.
  - Websphere 8.x.
  - WebLogic 11 and 12c.
- The following new macros can be used in Alert Actions:
  - `% {SW_USERNAME}`: Username configured for the instance that triggered the alert.
  - `% {SW_PASSWORD}`: Password associated to the username configured for the instance that triggered the alarm.
  - `% {BORDER_TYPE}`: Border alert type of the parameter triggering the alert (OK, WARN, ALARM).
  - `% {BORDER_MIN}`: Border minimum range of the parameter triggering the alert.
  - `% {BORDER_MAX}`: Border maximum range of the parameter triggering the alert.
  - `% {BORDER_NTIMES}`: Number of consecutive times the parameter triggering the alert must have a value outside the border range before the alert occurs.
  - `% {ALARM1_TYPE}`: Alarm1 alert type of the parameter triggering the alert (OK, WARN, ALARM).
  - `% {ALARM1_MIN}`: Alarm1 minimum range of the parameter triggering the alert.
  - `% {ALARM1_MAX}`: Alarm1 maximum range of the parameter triggering the alert.
  - `% {ALARM1_NTIMES}`: Number of consecutive times the parameter triggering the alert must have a value within the alarm1 range before the alert occurs.
  - `% {ALARM2_TYPE}`: Alarm2 alert type of the parameter triggering the alert (OK, WARN, ALARM).
  - `% {ALARM2_MIN}`: Alarm2 minimum range of the parameter triggering the alert.
  - `% {ALARM2_MAX}`: Alarm2 maximum range of the parameter triggering the alert.
  - `% {ALARM2_NTIMES}`: Number of consecutive times the parameter triggering the alert must have a value within the alarm2 range before the alert occurs.
- **BPPM Integration**: It is now possible to indicate the device the instances will be attached to in the BMC ProactiveNet console.
- **I2D Device Mapping** can now be disabled by setting the `/MASAI/SENTRY8/disableI2D` configuration variable to 1.

### Changes and Improvements

- **Alerts**: Both encrypted and unencrypted application constants can be used in Alert Actions.
- **File Monitoring**: A username and password can now be specified to monitor a file instead of using the PATROL default account.
- **Process Monitoring**: The characters '-', '_', '.' can now be used when specifying a process username.
- **String Search**: Date and time information can now be inserted in the regular expression(s) to be searched. Values are interpreted at run time.
- **Database Queries**: Encrypted connections (SSL) with MS-SQL Servers are now supported by the Java connection method.

### Fixed Issues

#### Alerts

- **SWSY-310** - No Alert Action was triggered when border thresholds were breached.
- **P1355** - The acknowledge alerts function did not work for file security monitoring. Attempting to acknowledge a file security monitoring alert triggered for the "Integrity" parameter instead caused the following popup message to appear "No file matches the entered mask. Cannot Acknowledge and update the security settings."

#### Database Queries

- **SWSY-189** - Authentication errors occurred when performing a SQL query on a MySQL database running on Windows. The password was not properly formatted when using the command line method to perform a SQL query on a MySQL database. Therefore most database queries did not work due to authentication failure.
- **P1230** - Instances were created but remained OFFLINE and no collect was performed when running a Database Query using the ODBC method.
- **P1354** - Errors related to updateable cursors were returned when performing queries against PostgreSQL databases when using the ODBC method.

#### File Monitoring

- **SWSY-358** - Monitoring Studio does not read the monitored file from the beginning anymore if this file was temporarily inaccessible. It will instead carry on from the position it was at the last polling once the file is accessible again. This has been modified to prevent false alerts when a network is temporally unaccessible.

#### File System Monitoring

- **SWSY-115** - The file system monitoring feature did not work on UNIX if the file system name contained a special character.
- **SWSY-115** - On UNIX / Linux systems, an incorrect file system name was displayed in the interface if a mount device name was more than 20 characters long. Selecting this file system would lead to false alerts.
HTTP Request

- **SWSY-402** - An error was returned when the execution time was in a scientific format; a format which cannot be interpreted by PATROL. The response time is now reformatted to an actual number to allow the PATROL Agent to properly interpret them.

- **SWSY-300** - HTTP Request did not work on UNIX and Linux because of an issue in the sopen() PSL function executed by the PATROL Agent. A workaround has been implemented.

Java MBean Polling (JMX)

- **P1320** - JMX polling failed to reconnect to the WebLogic server when a regular expression was used in the key property and the server was restarted.

- **SWSY-159** - Attributes containing more than one line are now supported.

Numeric Value Extraction

- **SWSY-229** - The Numeric Value Extraction tool removed the [ and ] characters from the list of possible column separators.

OS Commands

- **SWSY-48** - The Command Line Analysis tool ignored the last line of a text file if it was empty or if no Exit Status was configured.
Text Pre-Processing

- **SWSY-154** - The end of a multi-line record could not be found if a regular expression was used to mark the start of this record and if the regular expression marking its end was empty line ("^[^$]").

WBEM Queries

- **SWSY-407** - WBEM queries were not supported on Windows Systems.
- **SWSY-514** - An alert is triggered on the QueryStatus parameter and an appropriate message is displayed if Java is unavailable on the server.

Windows Events Monitoring

- **SWSY-40** - Some instances stayed offline when monitoring Windows events from multiple event logs. Only the first event log was taken into account by Monitoring Studio. The other event logs were ignored which lead the KM to fail collecting events notified by the other event logs.
- **SWSY-391** - Windows events were not correctly collected when a monitored event source name contained special characters in a regular expression.
- **SWSY-487** - A detection delay could sometimes been observed for Windows Events.

WMI Queries

- **SWSY-100** - When using specific user-defined credentials to perform a WMI query, the username was not stored in PATROL configuration preventing the query to be executed.
- **P1270** - It is now possible to query 64 bit VMI classes.

Miscellaneous

- **SWSY-17** - The Numeric Value Extraction KM Command triggered invalid alerts when a regular expression had no matching value.
- **SWSY-19** - The Debug feature fully supports OpenVMS.
- **SWSY-45** - “Invalid username/password” error messages were displayed in the System Output Windows of the PATROL Console when using PATROL Agent v9.0.00 and higher on Windows systems and when the default account was configured with a domain account.
- **SWSY-49** - The %{HTTP_RETURN_OUTPUT} macro is now returning the output of the HTTP request.
- **P1355** - No default PATROL ID was provided in the "File monitoring and analysis" and "File Security Check" dialog boxes.
Overview
Introduction

Monitoring Studio KM for PATROL allows you to set up the monitoring, without any coding, of almost any application, device or IT component for which there is no out-of-the-box monitoring solution. In a few clicks, and thanks to intelligent wizards, you can cover up to 100% of your critical applications in your BMC monitoring environment.

The KM more especially allows you to:

- **Monitor processes**
- **Monitor and analyze files**
- **Parse complex log files** (xml, multi-line or large files)
- Run **string searches**
- **Extract numeric values**
- **Monitor file systems** used by the application
- **Launch commands or scripts**
- Send requests to a web front-end of the application
- Send queries to the database back-end of the application
- Poll SNMP agents and listen for **SNMP traps**
- **Poll JMX-enabled application servers**
- Execute and analyze **WMI queries**
- Monitor **Windows Performance**
- Monitor **Windows Events**
- Monitor **Windows Services**
- Monitor **other KM's**

Once Monitoring Studio is properly configured, the application/device or IT component appears in your BMC monitoring environment and operators are alerted when a failure or anomaly occurs (depending on the settings).
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**

**Operating Systems**
- Windows
- UNIX or Linux-based; including Solaris, HP-UX, IBM AIX, HP Tru64, RedHat Linux, SUSE Linux, VMWare ESX Host
- OpenVMS

**Console Systems**
- PATROL Consoles
- BMC ProactiveNet Performance Management 8.6.50

**PATROL Agent**

Monitoring Studio KM for PATROL supports PATROL Agent v3.8.50 and higher.

**JAVA**

Monitoring Studio KM for PATROL requires Java 1.5 or greater and a Java Runtime Environment (JRE) to be installed on the same system that runs the PATROL Agent. A Java Runtime Environment package is provided with Monitoring Studio KM for PATROL.

The Java Settings wizard lets you define the path of the Java environment to be used by the KM.
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 BMC Software EPD (Electronic Product download) from:

- the BMC Software Website
- the Sentry Software Website.

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

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

The packages are valid for installation on Agents, Consoles and Console Servers.

Packages

The Monitoring Studio packages are available on the Sentry Software Website.

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: swsy_ALL_<version>.zip
- For UNIX and Linux systems: swsy_ALL_<version>.tar
- For OpenVMS systems: swsy_VMS_<version>.tar

A package of a suitable Java Runtime Environment, designed for use with the BMC Software Installation Utility, is also made available. 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.
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 Console Server
- PATROL Central – Web Edition

**On Windows**

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

1. First, unzip the BMC Installation Utility: `ins_Windows_<version>.zip`
2. Next, unzip the Monitoring Studio KM package in the same folder: `swsy_ALL_<version_number>.zip`
3. Then, 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:

1. First, untar the BMC Installation Utility: `tar xvf ins_ALL_<version>.tar`
2. Next, untar the Monitoring Studio KM package named: `tar xvf swsy_ALL_<version>.tar`

The files are extracted into a sub-directory named `bmc_products`. 
Installing the KM
Introduction

This chapter describes the installation procedure for Monitoring Studio 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.

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.
To install Monitoring Studio KM for PATROL

1. Allow the perl.exe program to listen on this port: Click **Allow access**.

![Windows Security Alert]

*Installation Wizard - Step 1: Windows Security Alert*
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.

*Installation Wizard - Step 5: Selecting the Installation Directory*
6. Select **Default**. Installing Monitoring Studio does not require any customization. Click **Next** to continue.
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 Console Server or on PATROL Central – Web Edition.
   Click **Next** to continue.

*Installation Wizard - Step 7: Selecting Roles*
8. Select:
   - Monitoring Sentry KM for PATROL to install the KM (it should be selected by default).
   - 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.

![Installation Wizard - Step 9: Reviewing Installation Options](image-url)
10. The setup program displays the actions performed and indicates the percentage of completion. Once the installation complete, click **Next** to 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 prompted 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

![Uninstall Wizard — Welcome Step](image)
4. Specify the BMC Software products folder. See the BMC Software documentation for more information.
5. Select **Monitoring Studio KM for PATROL**.

*Uninstall Wizard — Selecting Products and Components Directory*
6. Review the summary and click **Start Uninstall**.

*Uninstall Wizard — Reviewing Selected Products & components and start uninstalling*
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 the KM
Monitoring Studio KM for PATROL can be integrated into BMC Portal and BMC ProactiveNet Performance Management to proactively monitor your environments. The same information will be available in both consoles.

## 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 KM properly discovered your hardware and is collecting data.
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 ProactiveNet Performance Management

Depending on the version of BMC ProactiveNet Performance Management used, integration steps may need to be performed.

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.x

No specific integration steps need to be performed.
Monitoring your Applications
The configuration will mostly depend on the application to be monitored. It is however recommended to follow these guidelines:

1. Create the Application icon
2. Specify the resources used by your application
3. Specify the information sources, i.e. where or how you can get information about the application
4. Specify what should be searched for in the information sources
5. Configure Thresholds.
6. Specify what Monitoring Studio should do when an application failure has been detected.
7. Configure advanced settings.

Once configured, the application or IT component is displayed in the PATROL Console. This IT component 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 /MASAI/SENTRY8).
1. Creating the Application Icon

It is recommended to create an Application icon that will group all the objects that are related to a same application, a same IT component or device.

If you setup monitoring objects under the main Monitoring Studio icon without creating an application or container icon, you cannot set global Alert Actions on them. Global Alert Actions can only be set on an application container and will apply to the objects under it.

To create an application icon:

1. In the PATROL Console, right-click the Monitoring Studio icon and select KM Commands > New > Application icon (container)...
2. Click Next.

![Creating the Application Icon — Welcome Page](image-url)
3. Name your application icon:

- **Container name**: Enter the name of application to be monitored. This name will appear next to the container icon in the PATROL Console.
- **Description (optional)**: Describe the application or IT component to be monitored.
- **Contact (optional)**: Enter the name of the person to be alerted or who can provide support in case of an application failure.
- **Let me setup advanced options**: Check this box if you want to:
  - set command lines to start or stop the application monitoring from a KM command.
  - specify signature files
  - set application constants.

![New Application/Container Icon](image)

*Creating the Application Icon — Configuration Page*
4. Click **Next**.
5. If you checked the advanced options box, you will then have to configure the advanced options.
6. **(BPPM Users)** Provide the hostname, IP address, or FQDN of the device the instances will be attached to in the BMC ProactiveNet console and click **Next**. A device and all its related instances will be created in the BPPM console.
7. Click **Finish**.

The application icon appears in the PATROL console. You can now:

- create sub-containers by right-clicking the **application/container icon** and selecting **KM Commands > New > Sub-container...**
- create or add other objects that belong to this application. This method is recommended if you wish to apply global Alert Actions to all the monitored objects that belong to one application.
- edit your application icon by right-clicking the **application/container icon** and selecting **KM commands > Edit**.
- remove your application icon by right-clicking the **application/container icon** and selecting **KM commands > Delete**. After confirmation, the application icon and all its dependent objects will be removed from the PATROL Console and from the agent configuration.
2. Specifying the Resources Used

Once you have created the Application Icon, you can specify the resources used by the application to be monitored. You can for example choose to monitor:

- **Processes**
- **Windows services** (only available for agents running on Windows systems)
- **File systems** or logical disks used by your application
- **Directories** where your application runs, where transactional data is stored, where queries are queued, etc.
- **Files** that are critical to your application. You can for example check their presence, size, and growth, or simply check that file security is respected
- Other middleware information provided by:
  - **other KMs** if your application relies on some middleware software that can be monitored by specific KMs (Oracle, Tuxedo, MSMQ, etc.)
  - **Windows performance counters** if your application relies on middleware software under Windows and provides perfmon data.

Monitoring Processes

When you monitor an application, you typically want to check that the application's 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 (process ID)

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

⚠️ Advanced privileges may be required to collect process information. In that case, you will be prompt to enter process command credentials that will be used for running OS commands.
1. Configuring Process Command Credentials

Monitoring Studio KM for PATROL runs OS commands to collect process information. In order to gather all process information, advanced privileges are sometimes required. Monitoring Studio allows you to set or modify the process command credentials that will be used for running OS commands.

On Windows Systems

1. Right-click the Monitoring Studio icon > KM Commands > Options > Process Monitoring Credentials...

![Setting Process Command Credentials on Windows Systems]

- Enter a username and password.

2. Click OK to save your settings.

On Unix/Linux Systems

Depending on the targeted platform, Monitoring Studio may use some external system utilities to gather information. Sometimes the PATROL Agent default account does not have sufficient privileges to execute these commands and it is not possible in your environment to give super-user rights to the PATROL Agent. In such case Monitoring Studio can use the "sudo" utility to execute external commands as "root". The "sudo" utility helps UNIX system administrators secure their environment by authorizing some users to execute only certain commands specified as another user account (typically root). If this applies to you, the "sudo" options feature could be a good workaround.
1. Ensure that the sudo utility is installed on the system, and that the "/etc/sudoers" file is configured to allow the PATROL Agent to execute the selected commands as root.
2. Right-click the Monitoring Studio icon > KM Commands > Options > Process Monitoring Credentials...

3. Enter the user credentials to execute external "ps" command
4. Enter the command line to execute the sudo utility
5. Click OK to save your settings.

2. Specifying the Process to be monitored

The Process Monitoring tool, which can be accessed by right-clicking the Application icon and selecting KM Commands > New > Process monitoring..., allows you to identify the process to be monitored by either:

- picking the process from a list
- entering search criteria
- providing the PID file path.
Picking the Process to Monitor from a List

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

1. In the PATROL Console, right-click the Application icon and select KM Commands > New > Process monitoring...
2. Select Pick the process to monitor from a list and click Next. It may take a few seconds for the panel to be displayed since Monitoring Studio retrieves the list of all the currently running processes.
3. Click the process you wish to monitor and click Next.
4. The process criteria panel is displayed with all information already filled. Remove or modify any information you do not wish to monitor and click Next.
5. Select the parameters to be monitored for this process and click Next.
6. Configure the Monitoring Studio settings.
7. Click Finish.

If you proceed to the next panel and go back to this one, the process will not be pre-selected anymore. This is due to some PSL limitation. You will then have to re-select the process before clicking Next. You may, of course, select any other process.
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 **Application** icon and select **KM Commands > New > Process monitoring**...
2. Select **Enter criteria to identify and monitor processes** and click **Next**. The following dialog box is displayed:

![Process Monitoring Wizard](image)

**Process Monitoring Wizard — Enter criteria to identify and monitor processes**
3. (Optional) Click the View Processes button to list the currently running processes.

4. Specify your search criteria:
   - In the section **The name of the process...**, select a condition option and enter the string to be searched.
   - In the section **AND the command line that launched the process...**, 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.
   - In the field **AND the process must be running as this user**, enter the user name the monitored process is running as.
   - Click **Next**.

Examples:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Processes that match the criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example 1</strong></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 Identity = &lt;nothing&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PatrolAgent.exe</td>
</tr>
<tr>
<td></td>
<td>C:\Patrol\PatrolAgent.exe -p 3181</td>
</tr>
<tr>
<td></td>
<td>C:\Patrol\PatrolAgent.exe</td>
</tr>
<tr>
<td><strong>Example 2</strong></td>
<td></td>
</tr>
<tr>
<td>• Process name MUST BE EXACTLY patrolagent.exe</td>
<td></td>
</tr>
<tr>
<td>• Command-line MUST MATCH THE REGULAR EXPRESSION -[pP] 3181</td>
<td></td>
</tr>
<tr>
<td>• User Identity = &lt;nothing&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C:\Patrol\PatrolAgent.exe -p 13181</td>
</tr>
<tr>
<td><strong>Example 3</strong></td>
<td></td>
</tr>
<tr>
<td>• Process name MUST CONTAIN Pat</td>
<td></td>
</tr>
<tr>
<td>• Command-line = &lt;nothing&gt;</td>
<td></td>
</tr>
<tr>
<td>• User Identity = &lt;nothing&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PatrolAgent.exe</td>
</tr>
<tr>
<td></td>
<td>PatProcess.exe</td>
</tr>
<tr>
<td></td>
<td>PatrolPerf.exe</td>
</tr>
</tbody>
</table>

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

4. Select the parameters to be monitored for this process and click **Next**.

5. Configure the **Monitoring Studio settings**

6. Click **Finish**.
Providing the PID file path

Some applications indicate that they are running by writing the PID of their process into a given file. To make sure these applications are properly functioning, Monitoring Studio can read this file and check whether the PID written in the file corresponds to a running process.

Most Windows applications do not provide PIDs.

1. In the PATROL Console, right-click the Application icon and select KM Commands > New > Process monitoring...
2. Select Provide a PID file path and click Next.
3. Enter the path to the file containing the Process PID 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.

4. Select the parameters to be monitored for this process and click Next.
5. Configure the Monitoring Studio settings
6. Click Finish.

All processes that match the entered criteria will be monitored and identified as one icon in the PATROL Console.
3. 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>HandleCount (Windows only)</td>
<td>Displays the number of handles opened by the matching process(es).</td>
<td>Handles</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>PageFileBytes (Windows only)</td>
<td>Displays the page file 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 this process and that cannot be shared with others.</td>
<td>Megabytes</td>
</tr>
<tr>
<td>ThreadCount (Windows only)</td>
<td>Displays the number of threads of the matching process(es).</td>
<td>Threads</td>
</tr>
<tr>
<td>VirtualBytes</td>
<td>Displays the virtual memory used by the matching process(es).</td>
<td>Megabytes</td>
</tr>
<tr>
<td>WorkingSet (Windows only)</td>
<td>Displays the working set size of the matching process(es).</td>
<td>Megabytes</td>
</tr>
</tbody>
</table>

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.
4. Configuring the Monitoring Studio 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:
   - **Object display name**: Label that will be displayed in the PATROL Console for this monitoring object.
   - **Object internal identifier (ID)**: PATROL internal identifier of this monitored object.
   - **What thresholds do you want to set for the newly created object?**: Mode to be used to set alert thresholds:
     - **Use default thresholds**: Uses the default thresholds set by Monitoring Studio
     - **Set custom thresholds**: Allows you to customize the thresholds for all parameters of the instance
     - **Use 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.
     - **Do not 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.
2. Specifying the Resources Used

Monitoring a Windows Service

To monitor a Windows service:

1. In the PATROL Console, right-click the **Monitored Application icon** and select **KM Commands > New > Windows Service Monitoring...**

![Windows Service Monitoring Wizard — Welcome Page](image)

---

If you select Use 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 > Set Thresholds.

2. Click **Finish**.
2. To display the list of currently installed services:

- Select **Select a service from the existing list of services** and click **Next**.
- Select the service to be monitored and click **Next**.

![Windows Service Monitoring Wizard — Service Selection Page](image)
3. To manually enter the short name of a Windows service that is not currently installed on the managed system:

- Select **Enter manually the short name of a service** and click **Next**.
- Manually enter the name of the Windows service to be monitored and click **Next**.

![Service Monitoring Wizard — Service Selection Page]

6. **Configure the Monitoring Studio settings.**
7. Click **Finish**.
Monitoring a File System

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

To monitor a file system:

1. In the PATROL Console, right-click the **Monitored Application icon** and select **KM Commands > New > File System monitoring...**

![File System Monitoring Wizard on Windows — Welcome Page](image)

2. Select the file system you wish to monitor and click **Next**.

On UNIX/Linux servers with more than 30 file systems, PSL limitations render the correct functioning of a long drop-down list difficult, hence these systems will display a dialog box. By clicking **Existing File Systems**, a small box showing current file systems will appear. Again, owing to PSL limitation, selection of the drive/file system with the cursor is not possible – you are required to enter the drive manually. The dialog box that shows all the drives is for display/information purpose only. Click **Accept/Cancel**.
3. **Configure the Monitoring Studio settings.**
4. Click **Finish**. The corresponding object is created in the PATROL interface with the following parameters:
   - **FreeMegabytes**: Free space left in megabytes. It is possible to trigger an alert when the free space in MB is lower than a given value.
   - **FreeSpacePercent**: Free space in percentage. You can configure Monitoring Studio to trigger an alert when the percentage of free space on the file system is lower than a given threshold.
   - **UsedSpaceGrowthPercentage**: Shows how fast the file system is filled up, in percentage of its size (in percentage per hour - %/hour). Note that the **UsedSpaceGrowthPercent** parameter may have negative values.
   - **UsedSpaceGrowthSpeed**: Shows how fast the file system is filled-up (in megabytes per hour – MB/hour). Note that the **UsedSpaceGrowthSpeed** parameter may have negative values.

### Monitoring Folders

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

This feature allows you to:

- Ensure that your application is not overloaded (number of files to be processed, e.g.)
- Measure the application 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 application 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 "/MASAI/SENTRY8/folderLimit" to a value greater than 1000.*

Folder monitoring objects are instances of the **SW_FOLDERS** class.
To monitor folders:

1. In the PATROL Console, right-click the **Monitored Application icon** and select **KM Commands > New > Folder monitoring**...

2. Click **Next**.

3. Identify the folder to be monitored:
   - **Folder name and path**: Enter the name and path of the folder (directory) to be monitored.
   - **Include sub-folders**: Check this box to monitor all the sub-folders of the above-specified folder.
   - **Monitor only files matching the mask below (optional)**: Specify the file types or enter masks, and only these files will be monitored (e.g.:*.txt;myFiles?.log;file.*).

   ![Folder Monitoring Wizard — Welcome Page](image)

   *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.*
2. Specifying the Resources Used

4. Select the parameters to be monitored for this folder:

- **Folder Disk Usage:**
  - **FolderSize:** Total size of all files in the folder (and sub-folders if asked). Unit: Megabytes
  - **GrowthPercentage:** Growth of the folder since the last polling. This is the last recorded size divided by the polling interval. Unit: percent per minute. This parameter can also be negative. Unit: Percentage per minute.
  - **GrowthSpeed:** Growth speed of the folder since the last polling, divided by the polling interval. Unit: kilobytes per minute.

- **Folders File Flow:**
  - **FileCount:** Current number of files in the folder. Unit: files
  - **DeletedFileCount:** Number of files deleted from this folder since the last polling, divided by the polling interval. Unit: files per minute
  - **NewFileCount:** Number of new files added to this folder since the last polling, divided by the polling interval. Unit: files per minute
  - **LongestTimeFileRemainsInFolder:** Longest time an existing file has been placed in the folder. Unit: minutes.

- **Files Modified:**
  - **ModifiedFileCount:** Number of files modified since the last polling, divided by the polling interval. Unit: files per minute
  - **LastModifiedFileElapsedTime:** Time elapsed since the last modification/creation of a file in this folder. Unit: minutes
  - **OldestModifiedFileElapsedTime:** Time elapsed since the last modification/creation of the oldest file in this folder. Unit: minutes
5. Click **Next**.
6. **Configure the Monitoring Studio settings**.
7. Click **Finish**.

### Monitoring Files

The **File Monitoring Tool** provided by Monitoring Studio can instantly detect and alert for example when a critical file goes missing, if the file size is growing too fast, if its security settings have changed, etc. It is one of the most important monitoring tools offered by Monitoring Studio as most applications deal with files and many of them are critical. The most typical usage of file monitoring is parsing a LOG file. Most applications use LOG files to trace their operations and notify operators when failures occur.
Monitoring Studio allows you to:

- monitor the main characteristics of these files such as: presence, size, growth & security
- parse the file content to retrieve useful data (including strings that should be present or not and numeric values to build graphs).

**To create a file monitoring:**

1. In the PATROL Console, right-click the **Monitored Application icon > KM Commands > New > File monitoring and analysis...**
2. Specify the type of file that you wish to monitor:
   - **LOG file**: if you only want the new lines to be scanned when searching for strings or numeric values.
   - **FLAT file**: If you want the entire file to parsed when searching for strings or numeric values.
2. Click **Next**. The following dialog box is displayed:

![New LOG file monitoring and analysis dialog box]

3. Identify the file to monitor:
   - **File name and path**: 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
     - a format Command to dynamically assign the current date or time in the file name or path. Simply insert the following string in the "File name and path" field, replacing the three dots by date format symbols: %{ASCTIME:...}. For the complete list of format symbols, meaning and some examples, please see [Format Symbols](#) in the Reference section.

### Example

- **Monitor**: /opt/myApplication/log/myApp*.log
- **Behavior**: Monitoring Studio will look for the most recent file that matches the mask (e.g. /opt/myApplication/log/myApp) and start the monitoring of this file.

When the application stops writing in this LOG file and creates a new one (e.g. /opt/myApplication/log/myApp), Monitoring Studio analyses the current file for changes and searches for strings and numbers, and then switch to this new file. This way, no information is lost when switching from the previous file to the new one.
4. **(Optional)** Fill the **Username** and **Password** fields if you want to use a specific account to monitor the file instead of the PATROL Agent default account.
5. Select the parameters you want to monitor. See [SW FILES](#) for parameter details.
6. Click **Next**.

![File Monitoring and Analysis Wizard — Settings Page](image)

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

### Checking File Security Settings

The **File Security Check** tool offers a complete file monitoring by ensuring that file security is respected. With a few clicks, you can monitor the access and rights of groups and users and define who should be alerted if the file content is changed or if security is breached.

File Security Check objects are instances of the [SW_FILE_SECURITY](#) class.
Step 1: Creating a File Security Monitoring

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

![File Security Check Wizard - Welcome Page]

2. Select the security options that you want to monitor:
   - Granted file access rights
   - User that owns the file
   - Group that may have access to the file
   - File integrity

3. Click Next.

   *By default, Monitoring Studio will use the current file attributes and owners in the next steps. If the current file configuration is the correct one, simply click on Next until the end of the wizard.*
Step 2: File’s access rights

The following dialog box will only be displayed if you previously selected the security option **The granted file access rights**. It will let you select the type of alert to be triggered if the file’s access rights do not match the criteria entered. Depending on the operating system the PATROL agent is running on, you may get different options.

### On UNIX and Linux systems

![Image of dialog box](image)

1. In the first drop-down list, choose the type of alert to be triggered if the current file mode does not match the "expected" one.
2. Specify the file's access rights. They can be looked up by executing an "ls -l" command. The mode consists of 10 characters, for example, -rwxr-xr-x. The first character indicates the entry type:
   - b: block special file
   - c: character special file
   - d: directory
   - l: symbolic link
   - n: network special file
   - p: fifo (also called a "named pipe") special file
   - s: socket
   - t: ordinary file

The next 9 characters are interpreted as three sets of three characters, each of which identifies access and execution permissions for the owner, group, and others categories. The “-” indicates that permission is not granted. Various permission combinations are possible, except that the x, s, S, t, and T characters are mutually exclusive.

The access right characters are interpreted as follows:
- : Deny all permissions in the corresponding position.
  r: Grant read permission to the corresponding user class.
  w: Grant write permission to the corresponding user class.
  x: Grant execute (or search in directory) permission to the corresponding user class.
  s: Grant execute (search) permission to the corresponding user class. Execute the file as if by the owner (set user ID, SUID) or group (set group ID, SGID), as indicated by position.
  S: Deny execute (search) permission to the corresponding user class. Execute the file as if by the owner (set user ID, SUID) or group (set group ID, SGID), as indicated by position.
  t: Grant execute (search) permission to others. The "sticky" (save text image) bit is set.
  T: Deny execute (search directory) permission to others. The "sticky" (save text image) bit is set.

On Windows systems

The file access rights depend on the Access Control List (ACL) on Windows systems. An ACL is a table that tells a computer operating system the access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to:

- Read a file (or all the files in a directory)
- Write to the file or files
- Execute the file (if it is an executable file, or program).

In Windows, an access control list is associated with each system object.

- Each ACL has one or more access control entries (ACEs) consisting of the name of a user or group of users.
- The user can also be a role name, such as "programmer," or "tester."
- For each of these users, groups, or roles, the access privileges are stated in a string of bits called an access mask.

Generally, the system administrator or the object owner creates the access control list for an object.

In the above dialog box, you can:

- Enter up to 8 users or groups
- Indicate the access criteria: read, write or execute
- Specify the type of alert to be triggered if the file’s access rights differ from the specified criteria.
Step 3: Ownership

The following dialog box will be displayed if you previously selected the security option The user that owns the file.

- **Select the type of alert**: Do not trigger any alert; Trigger an ALARM; Trigger a WARNING; Trigger an INFORMATION
- **The file owner is or is not**: Specify whether or not the file’s owner should or should not match the specified names.

Once this option is configured, Monitoring Studio checks if the file’s owner is approved.
Step 4: File’s group

The following dialog box will only be displayed if you previously selected the security option **The group that may have access to the file.**

![New File Security monitoring for 'LOG File:log.txt'](image)

**Windows Service Monitoring Wizard — File Group Page**

- **Select the type of alert**: Do not trigger any alert; Trigger an ALARM; Trigger a WARNING; Trigger an INFORMATION
- **The file’s group is or is not**: Specify whether or not the file’s group matches the specified criteria.

Once this option is configured, Monitoring Studio checks if a group differs from the specified criteria.
Step 5: File’s integrity

The following dialog box will only be displayed if you previously selected the security option **The file integrity**. It lets you select the type of alert to be triggered when the file’s content is modified. The file integrity is verified using a checksum algorithm: MD5 on Windows, cksum on UNIX.

![File Integrity Dialog Box]

*Windows Service Monitoring Wizard — File Integrity Page*
Step 6: Monitoring Studio settings

Finally, you will have to configure the Monitoring Studio settings:

![Monitoring Studio settings](image)

- **PATROL Object Label**: Enter the Label displayed in the PATROL Console.
- **PATROL Object ID**: PATROL internal identifier of this File security monitoring. It is strongly recommended not to change the default ID.
- **Poll every "x" minutes**: Set the polling interval for this monitored object. The default polling interval is 2 minutes.

### Monitoring Loaded KMs

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 `SW_KMWATCH` class.
To create a mathematical formula:
1. In the PATROL Console, right-click the Monitored Application icon and select KM Commands > New > Multi-Parameter Formula...

2. 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 currently supported by Monitoring Studio KM is 26.

   ![Multi-Parameter Formula Wizard — Welcome Page](image)

   - (Optional) Check the Use the objects display name to dynamically determine 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). 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 Monitoring Studio settings.
6. Click Finish to start monitoring the selected parameters. A new object is automatically created under the application/container icon in the PATROL console.

Monitoring Windows Performance

The **Windows Performance Monitoring** tool incorporates Windows performance data, important to the proper functioning of your applications, within your PATROL environment. Alerts can be set to provide immediate notification in case one of the parameters you are monitoring is above or below a given range.

Performance monitor collects information about objects on your Windows computer 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 performances about specific components can be used to identify problems and bottlenecks within your application and plan ahead for your future needs.

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, objects, 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.

If an object has several instances, it is possible to monitor them either individually or all at once. In the latter case, you can choose to monitor the minimum, maximum, average or total value of the instances.

Windows Performance counter monitoring objects are instances of the `SW_NTPERFORMANCE` class.

### Creating a Windows Performance monitoring

1. In the PATROL Console, right-click the **Monitored Application icon** and select **KM Commands > New > Windows Performance monitoring...**

![Windows Performance Monitoring Wizard — Welcome Page](image-url)
2. Select the Windows Performance Object that contains the counter and click **Next**.

This panel is displayed if one or more instances of the selected Windows Performance is found. Otherwise, a much simpler panel is shown displaying only the list of counters and the scale.

3. Select the counter and instances:
   - **Select one or more instances**: This list displays the selected Windows Performance object instances. Select the one(s) you wish to monitor from the list.
   - **Select a counter**: The counters available for the selected Windows Performance object are listed here. Select the one you wish to monitor.
   - **Scale**: A scale can be used to divide the Windows performance value by this number. To do so, enter the number you wish the value to be divided by (e.g.: 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).
4. If more than one instance is selected, create the PATROL object. The radio buttons at the bottom of the panel can be used to select the creation mode of the Windows performance PATROL object instance:

- **Create one PATROL object per instance**: All selected instances will have their own PATROL object and will be monitored separately.
- **Group all selected instances into one PATROL object**: All selected instances are grouped into one PATROL object and are monitored all together. If you select this option, you must choose one of the following:
  - **Calculate average of all selected instances for selected counter**: Each value will be added then divided by the number of instances. So the average value of all the selected instances will be monitored.
  - **Use minimum value of all selected instances for selected counter**: The minimum value of the different selected instances will be monitored.
  - **Use maximum value of all selected instances for selected counter**: The maximum value of the different selected instances will be monitored.
  - **Calculate total value of all selected instances for selected counter**: The value of each selected instance is added so the total value of all selected instances will be monitored.

5. **Configure the Monitoring Studio settings**.
6. Click **Finish**.

### 3. Specifying the Information Sources

Once you have specified the resources used, you can indicate to Monitoring Studio the information sources to be monitored. You can for example choose to monitor:

- **Flat files** that contain useful information about your application
- **LOG files** in which your application writes data (traces of the operations)
- **Web pages** if your application provides a web front-end that should be tested
- **Database queries** if your application relies on a database server and some tables contain useful data or procedures that should be tested
- **SNMP agents** if your application provides information through an SNMP agent that can be polled or that sends **SNMP traps**
- **Commands or scripts** that test the application, giving its status or other useful information
- **JMX**-enabled servers that you want to poll and monitor
Analyzing Command Lines

Monitoring Studio provides the **Command Line Analysis tool** to execute any operating system command, command-line or in-house script and parse the output of the command to detect any error or performance issues.

It also allows you to:

- Stop the command execution once a given timeout is reached
- Check the exit status
- Run a background command that never ends

⚠️ The program or script being executed should not need any user interaction and should not create any window. Monitoring Studio will analyze its output, i.e. what has been written to the stdout and stderr streams.

Command line analysis objects are instances of the **SW_OSCOMMANDS** class.

To create a command line analysis:

1. In the PATROL Console, right-click the **Application** icon and select **KM Commands > New > Command Line analysis**...
2. Click **Next**
3. Enter the command line to execute:

![New command line execution](image)

- **Command line to execute**: Enter the OS command line or the path to the script that Monitoring Studio will execute. You can use the %\{TIME:...\} and %\{LASTTIME:...\} macros in the command line that will be executed. They will be replaced respectively by the current time and by the last execution time. See **Format symbols** for more details on the macros.

**Examples**
The following command line runs the diagnose.sh shell script: `/opt/myApp/bin/diag/diagnose.sh`

The following command executes a VBS script: `CSCRIPT.EXE //NoLogo C:\MyApplication\bin\diag\diagnose.vbs`

The following command dumps the errpt log on IBM AIX and only takes into account the new lines that have been logged since the last polling: `errpt –a –s %\{LASTTIME:%m%d%H%M%S\}`

- **Execute this command line as Username/Password**: Enter a username and password if the command line needs to be run with a user account different from the default PATROL Agent account.
- **This command needs to be launched only once and runs continuously**: check this box if you want the command to only be launched once.
- **Click Next**.
4. If you chose to only launch the command once, the following dialog box will be displayed:

```
Command line execution

Managed System: PC11_3181

A "never ending" command has no time out and will be continuously running.
Are you sure you want to select this execution mode?

Yes  No
```

**Never-ending Command Execution — Confirmation Message**

- Click **Yes**. The following dialog box is displayed:

```
New Command line execution

Managed System: PC11_3181

Execute: ping

This command line will be executed only once and will run continuously. Monitoring Studio will check its output for new lines to be analyzed regularly.

In some cases, Monitoring Studio may need to abort the execution of this command. A standard operating system signal is then sent to the command asking it to stop.

Additional command to execute in such a case:

Abort any previous execution of this command upon a PATROL Agent restart
```

**Never-ending Command Execution — Command Execution**

- **Additional command to execute in such a case**: 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.

- **Abort any previous execution of this command upon a PATROL 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**.
5. If you did not choose to only launch the command once, the following dialog box will be displayed:

![New command line execution](image)

6. Set the execution period and execution time:
   - **Stop the command if it takes longer than ... seconds**: Enter the time in seconds after which the command will be stopped. If the timeout is reached, the value of the `ExecutionStatus` parameter will be set to 1, indicating that the command failed to execute properly. No further analysis will be performed (String and Numeric Value searches).
   - **Command to execute if the timeout above is reached (Optional)**: Type a command similar to a recovery/cleaning action that will be executed when the timeout is reached. The `{%PID}` macro can be used to indicate the PID of command line process being interrupted.
7. Click **Next**

![New command line execution](image)

8. Set the command execution validation (optional):
   - **Command Exit Status**: States if the command line has been properly executed:
     - Select an execution option (succeeded/failed). This option specifies the exit code returned at the end of the command line execution.
     - 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, Monitoring Studio triggers an alarm on the `ExitStatus` parameter to indicate that the execution failed.
   - **Command execution validation**: The regular expression entered here will be searched in the output of the command. If it is not found, the value of the `ExecutionStatus` parameter will be set to 1, indicating that the command failed to execute properly.

⚠️ This option is useful to avoid basic execution errors like "File not found" because the command line was mistyped.
9. Click **Next**.
10. Configure the **Monitoring Studio settings**.

```
Managed System: PC11_3181

Monitoring Studio will create an object in the console to represent
the monitoring of this OS Command.

You may use the default values or enter a display name as well as an
ID to identify the object in the PATROL environment.

Object display name:
OS Command: diagnose.sh

Object internal identifier (ID):
diagnose.sh

What thresholds do you want to set for the newly created object?
I want to use the default thresholds
I want to use the default thresholds and customize them
I want to set custom thresholds
I do not want to set any thresholds for now

< Back  Finish  Help >>
```

*New Application/Container Icon Wizard — Settings Page*

11. 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. You do not need to run separate SQL queries any longer.

If the application 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 application tables. Once you specify an SQL query, you can search for strings in the result set and build graphs using the numerical values returned. Queries can be set up to perform complex tasks with just the click of a button, and they can be saved for future use.

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.

**Example**

How the database query result is formatted and then searched for strings and numeric values:

<table>
<thead>
<tr>
<th>QUEUE0001</th>
<th>343</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUEUE0002</td>
<td>0</td>
<td>Pending</td>
</tr>
<tr>
<td>QUEUE0003</td>
<td>17</td>
<td>Output</td>
</tr>
<tr>
<td>QUEUE0004</td>
<td>1</td>
<td>Input</td>
</tr>
<tr>
<td>QUEUE0005</td>
<td>0</td>
<td>Testing</td>
</tr>
<tr>
<td>QUEUE0006</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Database query analysis objects are instances of the **SW_DB_QUERIES** class.
Creating a Database Query Analysis

1. In the PATROL Console, right-click the Monitored Application icon and select KM Commands > New > Database Query analysis...

2. Select the Database type:
   - Select the database used by your application among the options available (Microsoft SQL Server, MySQL Server, Oracle Database Server, Other, or PostgreSQL).
   - Check the box Let me setup the database connection method if you want to manually select the connection method to be used to access the database. A list of available connection methods will be displayed in the next dialog box.
3. Click **Next**.

4. Select the connection method:
   - **Command line utility**: Select this option to use the command line tool developed by the database provider to manage access to a database. This method is by far the fastest but requires the command line tools to be installed on the local server and properly set. These command line tools are:
     - Microsoft SQL Server: OSQL
     - MySQL Server: MySQL
     - Oracle Database Server: Oracle SQL*Plus
     - PostgreSQL: psql
   - **Java Database Connectivity (JDBC)**: Select this option to use JDBC to perform the query to the database. This method is the slowest and requires Java to be installed on your local server.
   - **Open Database Connectivity (ODBC)**: Select this option to use ODBC to perform the query to the database. This method is known as the most flexible. However, it requires the proper driver to be installed on the local server as well as Java for UNIX/Linux servers.

   ![Database Query Analysis Wizard — Database Connection Method Selection](image)

5. If JDBC is selected and Java is not detected on the server, Monitoring Studio will ask you to provide the Java path.

   ![Database Query Analysis Wizard](image)
6. Click **Next**. The next steps will depend on the database server and the connection method selected:
   - MS SQL Server:
     - 5.1a: Setting Command line connection to Microsoft SQL database servers
     - 5.2a: Setting JDBC connection to Microsoft SQL database servers
     - 5.3a: Setting ODBC connection to Microsoft SQL database servers
   - MySQL Server:
     - 5.1b: Setting Command line connection to MySQL database servers
     - 5.2b: Setting JDBC connection to MySQL database servers
     - 5.3b: Setting ODBC connection to MySQL database servers
   - Oracle Database Server:
     - 5.1c: Setting Command line connection to Oracle database servers
     - 5.2c: Setting JDBC connection to Oracle database servers
     - 5.3c: Setting ODBC connection to Oracle database servers
   - Other (ODBC only):
     - 5.1d: Setting ODBC connection to Other database servers
   - PostgreSQL:
     - 5.1e: Setting Command line connection to PostgreSQL database servers
     - 5.2e: Setting JDBC connection to PostgreSQL database servers

7. Click **Next**.

8. Define the query to be executed.
   - **SQL Query to execute**: Single line SQL statement to be executed by the server. This also can be the path to an existing SQL script file. Use the following syntax if you want to execute the SQL query from a file: "@@ <file name>" (only supported by the Command Line
connection method).
- **Query timeout**: Time in seconds after which the **ConnectionStatus** parameter goes into alert.

### Example

- **Oracle service name**: BACKENDDB
- **Username**: sysApp
- **Password**: ******
- **SQL query**: SELECT COUNT(*) FROM PendingCustomers
- **Behavior**: Will connect to the BACKENDDB Oracle server instance using the sysApp database account and ask the server to return the number of rows in the Pending Customers table. This query should give a number representing the number of waiting customers for the application.

9. Click **Next**.

![New Database Query](image)

**Managed System: PC11_3181**

Monitoring Studio will create an object in the console to represent the monitoring of this Database Query.

You may use the default values or enter a display name as well as an ID to identify the object in the PATROL environment.

**Object display name:**

Database Query: SELECT COUNT(*) FROM PendingCustomers

**Object internal identifier (ID):**

SELECT COUNT(*) FROM

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

I want to use the default thresholds

9. **Configure the Monitoring Studio settings.**

10. Click **Finish**.
Setting connection to Microsoft SQL Server Databases

This section details the various connection settings available for performing queries on Microsoft SQL database server. First steps are common to all database queries and connection methods. They are documented in the Database Query Analysis section.

Step 5.1a - Setting Command line connection to Microsoft SQL database servers

If you have selected Command Line Utility as the connection method, the following panel is displayed:

![Database Query Analysis Wizard — Microsoft SQL Server Command Line Connection Settings](image-url)
3. Specifying the Information Sources

- **Hostname**: Name of the server where SQL Server is running (hostname or IP address)
- **SQL 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
- **Database name**: Name of the database
- **Authentication mode (SQL Server/Windows)**: Select Windows if you wish to connect to the database through a Windows user account. Select SQL Server 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. Please note that since version 8.6.54, SSL encryption is supported
- **Username**: Account used to connect to the database
- **Password**: Password associated with the specified username

Click **Next** to access the query definition panel.

### Step 5.2a - Setting JDBC connection to Microsoft SQL database servers

If you have selected **Java Database Connectivity (JDBC)** as the connection method, the following panel is displayed:

![Database Query Analysis Wizard — MS SQL Server JDBC Connection Settings](image)

- **Hostname**: Name of the server where SQL Server is running (hostname or IP address)
3. Specifying the Information Sources

- **SQL 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.
- **Database name**: Name of the database.
- **Authentication mode (SQL Server/Windows)**: Select *Windows* if you wish to connect to the database through your Windows user account. Select *SQL Server* 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.
- **Port**: Specify the Microsoft SQL port number.
- **Username**: Account used to connect to the database.
- **Password**: Password associated with the specified username.

Click **Next** to access the query definition panel.

**Step 5.3a - Setting ODBC connection to Microsoft SQL database servers**

If you have selected *Open Database Connectivity (ODBC)* as the connection method, the following panel is displayed:

![Database Query Analysis Wizard — MS SQL Server ODBC Connection Settings](image)
3. Specifying the Information Sources

3. Specifying the Information Sources

- **ODBC Driver**: Select the appropriate ODBC driver. The ODBC driver must be installed on the PATROL Agent.
- **Hostname**: Name of the server where SQL Server is running (hostname or IP address).
- **Database name**: Name of the database.
- **Username**: SQL Server account used to connect to the database.
- **Password**: Password associated with the specified username.

*Monitoring Studio supports two drivers for Windows: SQL Server and SQL Server 2005; and one driver for UNIX: Easysoft ODBC-SQL*

Click **Next** to access the query definition panel.

### Setting connection to MySQL Server Databases

This section details the various connection settings available for performing queries on MySQL database server. First steps are common to all database queries and connection methods. They are documented in the [Database Query Analysis](#) section.

**Step 5.1b - Setting Command line connection for MySQL database servers**

If you have selected **Command Line Utility** as the connection method, the following panel is displayed:
3. Specifying the Information Sources

Monitoring Studio KM for PATROL
Version 8.6.54

3. Specifying the Information Sources

- **Hostname**: Name of the server where MySQL Server is running (hostname or IP address)
- **Database name**: Name of the database
- **Port**: Specify the MySQL port number
- **Path to mysql command-line tool**: Enter the path to the mysql tool
- **Username**: MySQL Server account used to connect to the database
- **Password**: Password associated with the specified username

Click **Next** to access the query definition panel.

Monitoring Studio connects to MySQL databases using the mysql command-line tool. This client can be downloaded from the MySQL website and is installed by default when installing a MySQL database. This command-line tool, called mysql on Linux/UNIX and mysql.exe on Windows needs to be installed on the system that will perform the SQL queries. Monitoring Studio uses the following optional mysql parameters to connect to the database and execute the SQL query:

- `connect_timeout`: The number of seconds before connection timeout (as entered in the Monitoring Studio interface).

- `quick`: Do not cache each query result; print each row as it is received. This may slow down the server if the output is suspended. With this option, mysql does not use the history file. It forces mysql to retrieve results from the server a row at a time rather than retrieving the entire result set and buffering it in memory before displaying it. This is done to avoid problems due to insufficient memory for large result sets.

- `safe_updates`: Allow only those UPDATE and DELETE statements that specify which rows to modify by using key values.

- `silent`: Silent mode. Produce less output.
Step 5.2b - Setting JDBC connection to MySQL database servers

If you have selected **Java Database Connectivity (JDBC)** as the connection method, the following panel is displayed:

- **Hostname**: Name of the server where MySQL Server is running (hostname or IP address)
- **Database name**: Name of the database
- **Port**: Specify the MySQL port number
- **Username**: Account used to connect to the database
- **Password**: Password associated with the specified username

Click **Next** to access the query definition panel.
Step 5.3b - Setting ODBC connection to MySQL database servers

If you have selected **Open Database Connectivity (ODBC)** as the connection method, the following panel is displayed:

![New Database Query](image)

**Managed System: PC11_3181**

**MySQL connection settings**

As several ODBC drivers can exist to connect to the same database, you need to specify which ODBC driver has been installed on PC11.

- **ODBC driver**: MySQL Connector 5.1
- **Hostname**: 
- **Database name**: 
- **Username**: 
- **Password**: 

Connect to the database server as:

- **Username**: 
- **Password**: 

Click **Next** to access the query definition panel.

- **ODBC Driver (for ODBC Connection only)**: Select the appropriate ODBC driver. The ODBC driver must be installed on the PATROL Agent
- **Hostname**: Name of the server where MySQL Server is running (hostname or IP address)
- **Database name**: Name of the database
- **Username**: Account used to connect to the database
- **Password**: Password associated with the specified username

Monitoring Studio provides two drivers (Windows and UNIX): MySQL Connector 3.5 and MySQL Connector 3.51.
Setting connection to Oracle Database Server

This section details the various connection settings available for performing queries on Oracle database server. First steps are common to all database queries and connection methods. They are documented in the Database Query Analysis section.

Step 5.1c: Setting Command line connection to Oracle database servers

If you have selected Command Line Utility as the connection method, the following panel is displayed:
- **System identifier (Oracle SID) or connection string**: Specify the Oracle SID of the database server you want to connect to. If the Oracle Instant Client is installed, you can use the syntax://hostname:1521/oracleSID. Otherwise, this must match one of the tsnames.ora entries.

- **Oracle location**: Path to the Oracle client. This can be either ORACLE_HOME if the Oracle Database Server or Full Client is installed (example: c:\Oracle\ora92, or the path to Oracle Instant Client (example: /opt/oracle_instant_client).

- **Optional alternate TNS_ADMIN path**: If the Oracle Database Server or Full Client is installed and the tsnames.ora file is not located in the default directory, you can specify the path to the directory which contains tsnames.ora that will allow SQL*Plus to resolve the Oracle SID that you entered in the first field.

- **Username**: Database account to use to connect to the server

- **Password**: Password associated with the specified username.

Tips:

- Note that space characters are not supported for passwords in Windows, thus you need to enter a space-free password if you are working with this operating system.

- SQL*Plus:
  - Monitoring Studio uses Oracle SQL*Plus to connect to an Oracle Database Server. Therefore, SQL*Plus needs to be installed on the computer where Monitoring Studio and the PATROL Agent are running.
  - SQL*Plus is installed by default with Oracle Database Server. If you are configuring local queries, you need to enter the current ORACLE_HOME as the Oracle location.
  - SQL*Plus is also installed by default with the Oracle Database Client. If the Oracle Database Client has been installed on the computer where the PATROL Agent is running, you need to enter the current ORACLE_HOME as the Oracle location.
  - Starting with version 10g, Oracle now provides a new lightweight client: Oracle Instant Client. This new client is made of several packages. In order to make Oracle queries with Monitoring Studio, you need to install the "Instant Client Basic" (or "Instant Client Basic Lite") as well as "Instant Client SQL*Plus". Specify the directory where you unzipped the Oracle packages as the Oracle location.
  - On Windows, Monitoring Studio will try to detect by itself the SQL*Plus settings. On Linux and UNIX, Monitoring Studio will detect the proper SQL*Plus settings only if the PATH environment variable contains the directory of the SQL*Plus binary.

- Oracle system identifier (Oracle SID):
  - If Oracle Database Server of the full Oracle Database Client is installed on the computer where the PATROL Agent and Monitoring Studio are running, SQL*Plus will be using the classic name resolution system. In this case, the Oracle system identifier (Oracle SID) that you enter in the first field will be resolved by using the tsnames.ora file.
  - In most cases, the tsnames.ora file is located in the $ORACLE_HOME/network/admin directory. If it is located in another specific directory, you must specify the optional alternate TNS_ADMIN path (only enter the path to the directory).
  - The tsnames.ora needs to be maintained by an Oracle administrator. Please consult your database administrator if the Oracle system identifier of the database you want to connect to is not registered in the tsnames.ora file.
  - If the Oracle Instant Client is installed on the computer where the PATROL Agent and Monitoring Studio are running, you do not need the tsnames.ora file. Instead, you can use the following syntax for the Oracle system identifier: //server_hostname:1521/database_sid

Click **Next** to access the query definition panel.
Step 5.2c - Setting JDBC connection to Oracle database servers

If you have selected **Java Database Connectivity (JDBC)** as the connection method, the following panel is displayed:

```
Hostname: Name of the server where Oracle Server is running (hostname or IP address)
Database name: Name of the database
Port: Specify the Oracle port number
Username: Database account to use to connect to the server
Password: Password associated with the specified username
```

Click **Next** to access the query definition panel.
Step 5.3c - Setting ODBC connection to Oracle database servers

If you have selected **Open Database Connectivity (ODBC)** as the connection method, the following panel is displayed:

![ODBC Connection Panel](image)

- **ODBC Driver**: Select the appropriate ODBC driver. The ODBC driver must be installed on the PATROL Agent
- **Hostname**: Name of the server where Oracle Server is running (hostname or IP address)
- **Database name**: Name of the database
- **Username**: Database account to use to connect to the server
- **Password**: Password associated with the specified username

**Monitoring Studio provides an Oracle driver for Windows and the Easysoft Oracle ODBC driver for UNIX servers. On Windows, only queries to a local Oracle database are supported.**

Click **Next** to access the query definition panel.
Setting connection to Other Databases (ODBC only)

This section details the various connection settings available for performing queries on database servers other than MS SQL, MySQL, Oracle, or PostgreSQL. First steps are common to all database queries and connection methods. They are documented in the Database Query Analysis section.

Step 5.1d - Setting Command line connection to Other database servers (ODBC only)

Connection settings for databases other than MS SQL, MySQL or Oracle is only supported through ODBC connection. You can set the connection parameters with the following panel:

- **Connection String**: Enter the connection string that includes attributes such as the name of the driver, server, database and security information (user name 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.

- **Password**: Passwords are sensitive information that should not be displayed without being encrypted. When a password is included in the string you need to execute, you must use the `%{PASSWORD}` macro in the string and enter the corresponding password in the Password field (encrypted display).

**Example**

```
String = Driver={MySQL ODBC 3.51}
```
Click Next to open the query definition panel.

Setting Connection to PostgreSQL Databases

This section details the various connection settings available for performing queries on PostgreSQL database server. First steps are common to all database queries and connection methods. They are documented in the Database Query Analysis section.

Step 5.1e - Setting Command line connection to PostgreSQL database servers

If you have selected Command Line Utility as the connection method, the following panel is displayed:

```
Driver);Server=myserver;Database=mydatabase;User=user;Password=%{SW_PASSWORD};Option=3;
Password = ********
```

Click Next to open the query definition panel.
3. Specifying the Information Sources

Step 5.2e - Setting JDBC connection to Postgre SQL database servers

If you have selected **Java Database Connectivity (JDBC)** as the connection method, the following panel is displayed:

- **Hostname**: Name of the server where PostgreSQL is running (hostname or IP address)
- **Database name**: Name of the database
- **Port**: PostgreSQL port number
- **Path to psql command-line tool**: Path to the psql command-line tool
- **Username**: Account used to connect to the database
- **Password**: Password associated with the specified username

Click **Next** to access the query definition panel.
Monitoring Web Farms

Successfully measuring and monitoring the Web farms overall availability can be challenging if not relying on the Web-farm monitoring tool provided by Monitoring Studio. This tool helps you ensure the availability of your Web farms by indicating how many servers are responding with the correct Web content. It essentially groups HTTP requests all together, allowing you to use all the tools of the SW_HTTP_REQUESTS class to monitor your Web-farms.

Creating a Web Farm Monitoring

1. In the PATROL Console, right-click the Monitored Application icon and select KM Commands > New > Web-farm monitoring...

![Web-Farm Monitoring Wizard — Welcome Page](image-url)
2. Click **Next**.

3. Configure your Web-farm monitoring:
   - **URL to query**: 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.
   - **HTTP Request type**: Enter the HTTP request. There are two different modes: "GET" and "POST".
     - 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 must specify the variables and values to be transmitted to the Web server. Please note that:
       - Some Web forms can be passed to the server with the HTTP GET method. In such case, the form data is passed through the URL (http://server/form.php?varA=valueA&varB=valueB&...). You must check the Web form HTML source to know which method needs to be used (GET or POST).
       - When posting a form to a Web server, you have 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.
   - **Timeout after**: Enter the connection timeout period (By default: 30 seconds). When this timeout is reached, Monitoring Studio considers the host to be unreachable and triggers an
alert on the **ServerConnectionState** parameter.

- **Proxy settings (optional):** If your environment uses a proxy server, click to enter the proxy settings required to execute the HTTP request.
- **Web Server Authentication (optional):** See section below on [HTTP authentication](#) for details.
  - **Authenticate as:** Enter the user name as required by the HTTP server
  - **Password:** Enter the password.
- **Specify what should be shown in the ReturnOutput parameter:** 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).
- **Click Next.**

4. If you previously selected the "GET" method, enter the host information. Since a web-farm is composed of several servers, you can enter up to 10 hosts that make-up the web-farm:

![Web Request Analysis Wizard — GET Method Information Page](image)

- **Click Next.**
- **Go to Step 6.**
5. If you previously selected the "POST" method, the following dialog box is displayed:

![Web Request Analysis Wizard — POST Variables Definition Page](image_url)

- Enter the variable(s) name and value.
- Click Next.
- Enter the host information.
- Click Next.
3. Specifying the Information Sources

6. **Configure the Monitoring Studio settings.**
7. **Click Finish.**

⚠️ You cannot edit the webfarm instance but you can edit individual hosts (web-requests) under this web farm. You can add, edit and delete the hosts grouped under the webfarm icon at any time. To add a host, right-click the web farm icon > KM commands > Add host. To edit or delete a host, right-click the host icon > KM commands > Edit host or Delete as the case may be.
Analyzing Web Requests

The **Web Request Analysis** tool monitors your web-based applications, sends HTTP 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 **SW_HTTP_REQUESTS** class.

Creating a Web Request analysis

1. In the PATROL Console, right-click the **Application** icon and select **KM Commands > New > Web Request analysis**...
2. Click **Next**.

![Web Request Analysis Wizard — Definition Page](image)

3. Enter the URL to query and the method to be used:
   - **URL to query**: 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.
   - **HTTP Request type**: Select either the "GET" or "POST" mode. 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 to specify which variables with what values must be passed to the Web server. You must check the Web form HTML source to know which method needs to be used (GET or POST).

   ![Some Web forms can be passed to the server with the HTTP GET method. In this case, the form data goes through the URL](image)

   ![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.](image)

   ![A Web form HTML source should contain a statement like the following one: `<FORM METHOD="POST" ACTION="/urlToQuery.php">`](image)

   - **Timeout after**: Enter the timeout period. The default is set to 30 seconds. When this timeout
is reached, Monitor Studio considers the host to be unreachable and triggers an alert on the ServerConnectionState parameter.

- **Proxy settings (optional):** If your environment uses a proxy server, click to enter the proxy settings required to execute the HTTP request.

- **Web Server Authentication:** (optional) See section on HTTP authentication for details.
  - **Authenticate as:** enter the user name as required by the HTTP server
  - **Password:** Enter the password.
  - 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).

- Click **Next**.

4. If you previously selected the "POST" method, enter the variables to post:

![Web Request Analysis Wizard — Variables Definition Page](image)

- Enter the variable(s) name and value
3. Specifying the Information Sources

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 within your PATROL environment along with the application monitoring under a single icon. It can also query the WBEM repository for class and instance information.

WBEM query analysis objects are instances of the SW_WBEM class.

The variable used to specify the path to the jar file used to perform WBEM queries is: /MASAI/SENTRY8/wbemJarPath
Creating a WBEM query analysis

1. In the PATROL Console, right-click the **Monitored Application icon** > **KM Commands** > **New** > **WBEM Query analysis**
2. Click **Next**.

![WBEM Query](image)

### WBEM Query Analysis Wizard — Host Identification Page

3. Identify the host:
   - **Hostname**: Enter the hostname or IP address
   - **Connect through 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.
   - **Namespace**: Enter the WBEM namespace. A namespace is a logical group of related classes representing a specific technology or area of management (Ex: root\cimv2)
   - **Encrypt data using the HTTPS protocol**: Select this option to encrypt the query with the HTTPS protocol. Hyper Text Transfer Protocol Secure (HTTPS) is a secure version of the Hyper Text Transfer Protocol (http) 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.
   - **WBEM Query**: Enter your WBEM query
   - **Username and Password**: Enter your credentials. Leave these fields blank if you want the WBEM query to be executed with the PATROL Agent default account (patrol).
   - Click **Next**.


5. Click **Finish**.

An icon representing the WBEM query appears in the console with two parameters: **ReturnOutput** and **QueryStatus**. 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 application monitoring under a single icon. It can also query the WMI repository for class and instance information. You can for example request the WMI that returns all the objects representing shut-down events from your desktop system.

WMI query analysis objects are instances of the SW_NT_WMI class.

Creating a WMI Query Analysis

1. In the PATROL Console, right-click the main Monitored Application icon > KM Commands > New > WMI Query analysis
2. Click **Next**.

![WMI Query Analysis Wizard](image)

3. Identify the host:
   - **Hostname**: Enter the hostname or IP address.
   - **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`
   - **WMI Query**: Enter your query. Example: `SELECT * FROM Win32 process`. 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.
   - **Username and Password**: Enter your credentials. Leave these fields blank if you want the WMI query to be executed with the PATROL Agent default account (patrol).
4. Click **Next**.

5. **Configure the Monitoring Studio settings.**

6. Click **Finish**. An icon representing the WMI query appears in the console with two parameters: **ReturnOutput** and **QueryStatus** under it. You can now run **String Searches** and **Extract Numeric Values** from this output.
Polling MBean Application Servers

Objective

The aim of the Java MBean Polling (JMX) tool is to enable JMX polling to access and monitor the following MBean application servers:

- JBoss
- JOnAS
- BEA WebLogic
- IBM WebSphere
- Generic JMX client

Java Management Extensions (JMX) a trademark of Sun Microsystems, is a Java technology that supplies tools for managing and monitoring applications, system objects, devices (e.g. printers), and service oriented networks. Those resources are represented by objects called MBeans (for Managed Bean).

JMX Architecture

Java Management Extensions (JMX) technology provides the tools for building distributed, Web-based, modular and dynamic solutions for managing and monitoring devices, applications, and service-driven networks. Starting with J2SE 5.0, JMX technology is included in Java SE.

JMX is based on 3-level architecture:

- **The Probe level**: contains the probes (called MBeans) instrumenting the resources. It is also known as the instrumentation level.
- **The Agent level**: the MBeanServer is the core of JMX. It is an intermediary between the MBean and the applications.
- **The Remote Management level**: enables remote applications to access the MBeanServer through Connectors and Adaptors. A connector provides full remote access to the MBeanServer API using various communication frameworks such as RMI, IIOP, JMS, WS-*; while an adaptor adapts the API to another protocol (SNMP) or to Web-based GUI (HTML/HTTP, WML/HTTP...)

Applications can be generic consoles (such as JConsole and MC4J), or domain-specific (monitoring) applications.
MBeans and Platform MBean Servers

An MBean server is a repository of MBeans that provides management applications access to MBeans. An MBean is nothing but a java object that represents a manageable resource, such as an application, a service, a component, or a device. For example you could represent your laptop as an MBean and then “monitor” it.

Applications do not access MBeans directly, but instead access them through the MBean server with their unique ObjectName. An MBean server implements the interface `javax.management.MBeanServer`.

Monitoring Studio and MBeans

With the JMX polling feature of Monitoring Studio, you can easily monitor the above-mentioned application servers and consolidate the monitoring of these MBeanServers along with the application monitoring under a single icon. You need no longer to interrogate the various application servers through their respective interfaces just to view the status of the MBeans.

A management application can access platform MBeans in different ways:

- Using `ManagementFactory`
- Using an MXBean Proxy
- Using `MBeanServerConnection`

Monitoring Studio uses the `MBeanServerConnection` method to connect to the `MBeanServer` platform of a running JVM. In this method, you use the `getAttribute()` method of `MBeanServerConnection` to get an attribute of a platform MBean, providing the MBean's ObjectName and the attribute name as parameters.

Monitoring Studio can only poll the application servers and display the MBeans attributes and values. To create and register new MBeans or modify existing ones, you are required to do so using the specific application server interface.
Method (summary)

To setup the monitoring and consolidate the querying of resources represented by MBeans within your PATROL environment, all you need to do is go through the JMX wizard of Monitoring Studio. The wizard panels differ for each type of JMX application server, the following is just a summary of the overall method.

1. Right-click the main **Monitored Application icon > KM Commands > New > Java MBean polling (JMX)**
2. From the drop-down list, select the environment and its appropriate version number: JBoss/WebLogic/WebSphere/generic JMX client.
3. Enter the server connection information: hostname and the port number
4. Enter the additional information: initial context factory and JNDI name
5. Enter the connection account credentials: principle (username) and credentials (password)
6. Click Next; ensure that all the settings are accurate.
7. If the credentials entered are correct, Monitoring Studio connects to the application server and presents a list of domains for you to select from.
8. Select the domain to monitor and click Next.
9. Specify the key property to monitor from this domain and click Next.
10. Select the attribute from the list and click Next. You can only select one attribute at a time. To monitor several attributes of the same key property, you are required to go through the wizard each time.
11. Click Finish. You can add a string or numeric value search if you wish.

Once a JMX polling is configured, Monitoring Studio uses that JMX Polling configuration by default whenever you add a new Java MBean Polling. This way, you do not have to re-enter the configuration settings each time.

The above-mentioned instructions give an overview of the procedure to poll a JMX server. Please refer to the section on a specific application server for exact details and procedure. You can also consult the Input variables for JMX polling wizards section to know what input is required for which type of application server.
Generic JMX client using RMI or IIOP Protocols

To set-up the monitoring of a generic JMX client, right-click the **Monitored Application icon > KM Commands > New > Java MBean polling (JMX)** and select the **Generic** environment from the drop-down list:

![Java MBean Polling Wizard (Generic Environment) — Welcome Page](image)

- The application server should be started with the option: `-Dcom.sun.management.jmxremote.port=portNumber`
- Using the above option starts a dedicated JMX agent for this particular application. The Monitoring Studio generic JMX client needs to use this port number to establish a connection.
Step 1: Enter the generic environment connection information

- **Host**: Name of host server where the generic JMX application server is installed.
- **Port**: Enter the port number.
- **Server name**: Enter the server name
- **Protocol**: Select the relevant protocol: RMI / IIOP
Step 2: Enter the **connection account credentials**:

![New JMX Polling](image)

- **Principle**: Enter the username
- **Credentials**: Enter the password
- **Path to Java on the local server**: Enter your java bin path and ensure that all the settings are correct.
- **Connection timeout period**: Default is set to 120 seconds; you can change this if you wish. When this timeout is reached, Monitor Studio considers the host to be unreachable and triggers an alert on the **ExecutionStatus** parameter.

Click **Next**.
Step 3: Select domain

If the credentials entered are correct, Monitoring Studio connects to the application server and presents a list of domains for you to select from:

1. Select the domain to monitor
2. Choose the key property selection mode. You can either choose to select a key property among a list of existing ones or type a regular expression for the key property name.
3. Click Next.

Step 4: Specify the key property

Depending on the option selected at the previous step, you will either have to select a key property among a list of existing ones or type a key property name (regular expression).
Step 5: Select the attribute

Select the attribute to monitor and click **Next**.

You can only select one attribute at a time. To monitor several attributes of the same key property, you are required to go through the wizard each time.

Step 5a: Select parameters to collect

When you select a numeric attribute (boolean, integer, number) at the previous step, an additional panel is displayed to allow you to select the parameters to collect.

- **Value**: Reports the actual value collected upon data polling
- **Delta**: Calculates the difference between values collected during two consecutive polling.
- **DeltaPerSecond**: Reports the value resulting of the division of the Delta by the number of seconds 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).

**Step 6: Monitoring Studio settings**

You arrive at the final step of the wizard that displays the object display name, ID and threshold options. For more information, refer to the section [Configuring the Monitoring Studio Settings](#). Click **Finish**. An icon for the monitored instance will appear under the main Monitoring Studio icon bearing the name entered/displayed in the PATROL Label field; and at the next collect you will see values for the newly monitored object. You can add a string or numeric value search if you wish.

Generic JMX application objects are instances of the **SW_JMX** class.
JBoss

JBoss is an open source Java EE-based application server implemented in Java. As the JBoss Application Server is 100% pure Java, it is interoperable with most operating systems that are capable of running a Java Virtual Machine (JVM); including Red Hat Enterprise Linux, SUSE Linux, Microsoft Windows, Sun Solaris, HP-UX, and others.

To monitor your JBoss AS within your PATROL environment, right-click the **Monitored Application icon** > **KM Commands** > **New** > **Java MBean polling (JMX)** and from the drop-down list, select the environment.

![Java MBean Polling Wizard (JBoss Environment) — Welcome Page](image)
Step 1: Enter the **server connection information and the additional information**

![Java MBean Polling Wizard (JBoss Environment) — Connection Information Page](image)

**JBoss connection information:**

- Host: Name of host server where the JBoss application server is installed
- Port: JBoss port number. (1099 by default for JBoss 3.2.x, 4.x, 5.x, and 6.x, 9999 for JBoss 7.x). Can be modified

**Additional information for JBoss 3.2.x, 4.x, and 5.x:**

- Initial context factory: `org.jnp.interfaces.NamingContextFactory` (by default). Can be modified
- URL package prefixes: `org.jboss.naming.org.jnp.interfaces` (by default). Can be modified
Step 2: Enter the **connection account credentials**

- **Connection account**:  
  - **Principle**: Enter the username  
  - **Credentials**: Enter the password  
- **Path to Java on the local server**: Enter your java bin path and ensure that all the settings are correct. You can choose to execute additional JAR files by clicking the External JAR files button and enter the JAR files names and locations.  
- **Connection timeout period**: Default is set to 120 seconds; you can change this if you wish. When this timeout is reached, Monitor Studio considers the host to be unreachable and triggers an alert on the **ExecutionStatus** parameter.

Click **Next**. If the credentials entered are correct, Monitoring Studio connects to the application server and presents a list of domains for you to select from.
Step 3: Select the domain

1. Select the domain to monitor
2. Choose the key property selection mode. You can either choose to select a key property among a list of existing ones or type a regular expression for the key property name.
3. Click Next.

Step 4: Specify the key property

Depending on the option selected at the previous step, you will either have to select a key property among a list of existing ones or type a key property name (regular expression).
Step 5: Select the attribute

Select the attribute from the list and click Next.

You can only select one attribute at a time. To monitor several attributes of the same key property, you are required to go through the wizard for each attribute.

Step 5a: Select parameters to collect

When you select a numeric attribute (boolean, integer, number) at the previous step, an additional panel is displayed to allow you to select the parameters to collect.

- **Value**: Reports the actual value collected upon data polling
- **Delta**: Calculates the difference between values collected during two consecutive polling.
- **DeltaPerSecond**: Reports the value resulting of the division of the Delta by the number of seconds 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).

**Step 6: Monitoring Studio settings**

You arrive at the final step of the wizard that displays the object display name, ID and threshold options. For more information, refer to the section [Configuring the Monitoring Studio Settings](#).

Click **Finish**. An icon for the monitored instance will appear in the Console bearing the name entered/displayed in the PATROL Label field; and at the next collect you will see values for the newly monitored object.

You can add a string or numeric value search if you wish.

JBoss objects are instances of the **SW_JMX** class.
JOnAs

JOnAS is a leading edge Open Source implementation by OW2 of the Java EE specification.

⚠️ **Monitoring Studio KM for PATROL** requires application classes available only with JVM 1.5. Previous versions of JVM are not supported.

To monitor your JOnAs application server within your PATROL environment, right-click the **Monitored Application icon > KM Commands > New > Java MBean polling (JMX)**. From the drop-down list, select the environment.

![Java MBean Polling Wizard (JOnAs Environment) — Welcome Page](image-url)
Step 1: Enter the server connection information and the additional information

Java MBean Polling Wizard (JOnAs Environment) — Connection Information Page
3. Specifying the Information Sources

- **Host**: Name of host server where the JOnAS application server is installed
- **Port**: Port number. (By default: 1091). This is linked to the protocol used. Can be modified
- **Server name**: Name given to Jonas application server
- **Protocol**: JRMP or IIOP. The protocol & the port number to be used is defined in the "carol.properties" file that can be found in %jonas_home%/conf
- **Initial context factory**: com.sun.jndi.rmi.registry.RegistryContextFactory (by default). Can be modified
- **URL package prefixes**: org.objectweb.jonas.naming (by default). Can be modified.

**Step 2: Enter the connection account credentials**

**New JMX Polling**

**Managed System**: P011_0181

**Connection account**
- **Principle**: Enter the username
- **Credentials**: Enter the password

**Path to Java on the local server**: Enter your java bin path and ensure that all the settings are correct.

**Connection timeout period**: Default is set to 120 seconds; you can change this if you wish. When this timeout is reached, Monitor Studio considers the host to be unreachable and triggers an alert on the **ExecutionStatus** parameter.

Click **Next**. If the credentials entered are correct, Monitoring Studio connects to the application server and presents a list of domains for you to select from.
Step 3: Select the domain

1. Select the domain to monitor
2. Choose the key property selection mode. You can either choose to select a key property among a list of existing ones or type a regular expression for the key property name.
3. Click Next.

Step 4: Specify the key property

Depending on the option selected at the previous step, you will either have to select a key property among a list of existing ones or type a key property name (regular expression).
Step 5: Select the attribute

Select the attribute from the list and click **Next**.

You can only select one attribute at a time. To monitor several attributes of the same key property, you are required to go through the wizard each time.

Step 5a: Select parameters to collect

When you select a numeric attribute (boolean, integer, number) at the previous step, an additional panel is displayed to allow you to select the parameters to collect.
- **Value**: Reports the actual value collected upon data polling
- **Delta**: Calculates the difference between values collected during two consecutive polling.
- **DeltaPerSecond**: Reports the value resulting of the division of the Delta by the number of seconds 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).

**Step 6: Monitoring Studio settings**

You arrive at the final step of the wizard that displays the object display name, ID and threshold options. For more information, refer to the section [Configuring the Monitoring Studio Settings](#).

Click **Finish**. An icon for the monitored instance will appear under the main Monitoring Studio icon bearing the name entered/displayed in the Object display name field; and at the next collect you will see values for the newly monitored object.

You can add a string or numeric value search if you wish.

JOnAS client objects are instances of the **SW_JMX class**.
WebLogic

BEA WebLogic is a J2EE Platform product family that includes a J2EE application server: WebLogic Server, an Enterprise Portal - WebLogic Portal, an Enterprise Application Integration platform, a Transaction Server and Infrastructure - WebLogic Tuxedo, a Telecommunication Platform - WebLogic Communication Platform and also an HTTP web server for Unix, Linux, Microsoft Windows, and more.

To monitor your WebLogic application server within your PATROL environment, you first need to download the relevant WebLogic JAR files/zippered files from the Sentry Software download page and place them into: %PATROL_home%/bin.

To monitor your WebLogic application server within your PATROL environment:

1. Right-click the Monitored Application icon > KM Commands > New > Java MBean polling (JMX)
2. From the drop-down list, select the environment: WebLogic "x"
3. Click Next.
Step 1: Enter the **server connection information and the additional information**

- **Connection Information:**
  - **Host:** Name of host server where the WebLogic application server is installed.
  - **Port:** Port number. (By default: 7001). Can be modified.

- **Additional Information:**
  - **Initial context factory:** `weblogic.jndi.WLInitialContextFactory` (by default). Can be modified.
  - **JNDI name:**
    - **For WebLogic 9.x and higher:** `weblogic.management.mbeanservers.domainruntime` (by default). Can be modified.
    - **For WebLogic 8.x:** `weblogic.management.adminhome` (by default). Can be modified.
Step 2: Enter the connection account credentials

![New JMX Polling](image)

### Java MBean Polling Wizard (WebLogic Environment) — Connection Account Credentials Page

- **Principle**: Enter the username
- **Credentials**: Enter the password
- **Path to Java on the local server**: Enter your java bin path and ensure that all the settings are correct.
- **Connection timeout period**: Default is set to 120 seconds; you can change this if you wish. When this timeout is reached, Monitor Studio considers the host to be unreachable and triggers an alert on the ExecutionStatus parameter.

Click **Next**. If the credentials entered are correct, Monitoring Studio connects to the application server and presents a list of domains for you to select from.
Step 3: Select the domain

1. Select the domain to monitor
2. Choose the key property selection mode. You can either choose to select a key property among a list of existing ones or type a regular expression for the key property name.
3. Click Next.

Step 4: Specify the key property

Depending on the option selected at the previous step, you will either have to select a key property among a list of existing ones or type a key property name (regular expression).
Step 5: Select the attribute

![Java MBean Polling Wizard (WebLogic Environment) — Attribute Selection Page](image)

Select the attribute from the list and click **Next**.

You can only select one attribute at a time. To monitor several attributes of the same key property, you are required to go through the wizard each time.
Step 5a: Select parameters to collect

When you select a numeric attribute (boolean, integer, number) at the previous step, an additional panel is displayed to allow you to select the parameters to collect.

- **Value**: Reports the actual value collected upon data polling
- **Delta**: Calculates the difference between values collected during two consecutive polling.
- **DeltaPerSecond**: Reports the value resulting of the division of the Delta by the number of seconds 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).

Step 6: Monitoring Studio settings

**Object display name:** Label displayed in the PATROL Console for this WebLogic monitoring.

**Object internal identifier (ID):** PATROL internal identifier.

What thresholds do you want to set for the newly created instance? A drop-down list allows you to select the mode of setting alert thresholds:
- **Use default thresholds**: Uses the default thresholds set by Monitoring Studio
- **Set custom thresholds**: Allows you to customize the thresholds for all parameters of the instance
- **Use default thresholds and customize them**: Sets the default Monitoring Studio thresholds on certain parameters (see list of parameters with default thresholds) 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.

If you select Use 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. You can then customize (any/all) the thresholds of the parameters as per your specific needs.

- **Do not 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.

Thresholds can be set or modified at anytime by right-clicking on the instance > **KM commands** > **Set Thresholds**.

Click **Finish**. An icon for the monitored instance will appear under the main Monitoring Studio icon bearing the name entered/displayed in the Object display name field; and at the next collect you will see values for the newly monitored object. You can add a string or numeric value search if you wish.

WebLogic objects are instances of the **SW_JMX** class.
WebSphere

IBM® WebSphere Application Server is the foundation of the IBM WebSphere software platform, and a key building block for a Service Oriented Architecture (SOA). As the premier Java™ 2 Enterprise Edition (J2EE™) and Web services application platform, WebSphere Application Server delivers a high performance transaction engine that can help you build, run, integrate and manage dynamic On Demand Business™ applications.

Before setting-up the monitoring of a WebSphere AS, you need to download the WebSphere.jar files created to work with Monitoring Studio from the Sentry Software’s Website and store them in (%PATROL_Home%\bin). These files are essential in order to connect to your WebSphere AS through Monitoring Studio. They can be downloaded from the Sentry Software website.

To monitor a WebSphere application server within your PATROL environment:

1. After ensuring that the required files are present on the local host
2. In the PATROL Console, right-click the Monitored Application icon > KM Commands > New > Java MBean polling (JMX)
3. From the drop-down list, select the environment.
Step 1: Enter the **environment connection information and the additional information**

- **Host**: Name of host server where the WebSphere application server is installed
- **SOAP Port**: Enter port number. The first profile created on WebSphere is by default given the number 8880 and every profile created on WebSphere is allotted a new SOAP port number by increasing the count from 8880. This can be modified.

To connect to the WebSphere AS, it is essential to connect to certain credential files: ClientKeyFile.jks and ClientTrustFile.jks. These files are profile-specific and are created and stored by WebSphere under %IBM_HOME%\profile\profilename|etc. Depending on the security of your environment, you can either give the path to these files on where the WebSphere AS resides, or, just copy them from there to your local file-system.
3. Specifying the Information Sources

- **TrustStoreFile path**: Enter the path to the file ClientTrustFile.jks.
- **TrustStore password**: Enter the password created on WebSphere for your profile (default WebAS)
- **KeyStoreFile path**: Enter the path to the file ClientKeyFile.jks
- **KeyStore password**: Enter the password created on WebSphere for your profile (default WebAS)
- **Server name**: Name of the WebSphere application server.
- **Node name**: Enter the node name allotted to your profile. By default WebSphere assigns a unique node name to each profile created.

Click Next.

**Step 2: Enter the connection account credentials**

![Java MBean Polling Wizard (WebSphere Environment) — Connection Account Credentials Page](image)

- **Principle**: Enter the username
- **Credentials**: Enter the password
- **Path to Java on the local server**: Enter your java bin path and ensure that all the settings are correct.
- **Connection timeout period**: Default is set to 120 seconds; you can change this if you wish. When this timeout is reached, Monitor Studio considers the host to be unreachable and triggers an alert on the ExecutionStatus parameter.

Click Next. Ensure that all the settings are correct. If the credentials entered are correct, Monitoring
Studio connects to the application server and presents a list of domains for you to select from.

**Step 3: Select the domain**

![Image of domain selection window](image)

*Java MBean Polling Wizard (WebSphere Environment) — Domain Selection Page*

1. Select the domain to monitor
2. Choose the key property selection mode. You can either choose to select a key property among a list of existing ones or type a regular expression for the key property name.
3. Click **Next**.

**Step 4: Specify the key property**

Depending on the option selected at the previous step, you will either have to select a key property among a list of existing ones or type a key property name (regular expression).
Step 5: Select the attribute

![Java MBean Polling Wizard (WebSphere Environment) — Attribute Selection Page](image)

Select the attribute from the list and click **Next**.

You can only select one attribute at a time. To monitor several attributes of the same key property, you are required to go through the wizard each time.

**Step 5a: Select parameters to collect**

When you select a numeric attribute (boolean, integer, number) at the previous step, an additional panel is displayed to allow you to select the parameters to collect.
3. Specifying the Information Sources

Specifying Information Sources

Value: Reports the actual value collected upon data polling
Delta: Calculates the difference between values collected during two consecutive polling.
DeltaPerSecond: Reports the value resulting of the division of the Delta by the number of seconds 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).

Step 6: Monitoring Studio settings

You arrive at the final step of the wizard that displays the object display name, ID and threshold options. For more information, refer to the section Configuring the Monitoring Studio Settings.

Click Finish. An icon for the monitored instance will appear under the main Monitoring Studio icon bearing the name entered/displayed in the Object display name field; and at the next collect you will see values for the newly monitored object. You can add a string or numeric value search if you wish.

WebSphere objects are instances of the SW_JMX class.
### Input variables for JMX polling Wizards

Here is a recapitulative table with the input variables required to connect to the various JMX application servers.

<table>
<thead>
<tr>
<th>JMX Application Server</th>
<th>Input Variables</th>
</tr>
</thead>
</table>
| **JBoss** by Redhat    | **Connection Information**  
- Host: Name of host server where the JBoss application server is installed  
- Port: JBoss port number (1099 by default for JBoss 3.2.x, 4.x, 5.x, and 6.x; 9999 for JBoss 7.x). Can be modified  

**Additional Information for JBoss 3.2.x, 4.x, and 5.x**  
- Initial context factory: org.jnp.interfaces.NamingContextFactory by default. Can be modified  
- URL package prefixes: org.jboss.naming:org.jnp.interfaces (by default). Can be modified  

**Connection Account**  
- Principle: Username  
- Credentials: Password  
- Path to Java on the local server: java bin path  
- Connection timeout period: 120 seconds (by default). Can be modified. |
| **JOnAS**              | **Connection Information**  
- Host: Name of host server where the JOnAs application server is installed  
- Port: Port number. (By default: 1091). This is linked to the protocol used. Can be modified  

**Additional Information**  
- Server name: Name given to the JOnAs application server  
- Initial context factory: com.sun.jndi.rmi.registry.RegistryContextFactory (by default). Can be modified  
- Protocol: JRMP or IIOP  
- URL package prefixes: org.objectweb.jonas.naming (by default) Can be modified  

**Connection Account**  
- Principle: Username  
- Credentials: Password  
- Path to Java on the local server: java bin path  
- Connection timeout period: 120 seconds (by default). Can be modified. |
| **BEA WebLogic**       | **Connection Information**  
- Host: Name of host server where the WebLogic application server is installed  
- Port: Port number. (By default: 7001). Can be modified  

**Additional Information**  
- Initial context factory: weblogic.jndi.WLInitialContextFactory (by default) Can be modified  

For WebLogic 9.x and higher  
- JNDI: weblogic.management.mbeanservers.domainruntime (by default). Can be modified  

For WebLogic 8.x  
- JNDI name: weblogic.management.adminhome (by default). Can be modified  

**Connection Account**  
- Principle: Username  
- Credentials: Password  
- Path to Java on the local server: java bin path  
- Connection timeout period: 120 seconds (by default). Can be modified. |
| **IBM WebSphere**      | **Connection Information**  
- Host: Name of host server where the WebSphere application server is installed |
Monitoring Studio KM for PATROL
Version 8.6.54

### 3. Specifying the Information Sources

#### Monitoring SNMP Agents & Traps

Because many applications 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 applications are running properly.

<table>
<thead>
<tr>
<th>JMX Application Server</th>
<th>Input Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SOAP port: Enter port number. The first profile created on WebSphere is by default given the number 8880 and every profile created on WebSphere is allotted a new SOAP port number by increasing the count from 8880. This can be modified.</td>
<td></td>
</tr>
</tbody>
</table>

To connect to the WebSphere AS, it is essential to connect to certain credential files: ClientKeyFile.jks and ClientTrustFile.jks. These files are profile-specific and are created and stored by WebSphere under %IBM_HOME%/profile/profilename/etc. Depending on the security of your environment, either give the path to these files where the WebSphere AS resides, or, copy them from there to your local file-system.

**Additional Information**

- TrustStoreFile path: Enter the path to the file ClientTrustFile.jks.
- TrustStore password: Enter the password created on WebSphere for your profile (default WebAS)
- KeyStoreFile path: Enter the path to the file ClientKeyFile.jks
- KeyStore password: Enter the password created on WebSphere for your profile (default WebAS)
- Server name: Name of the WebSphere application server.
- Node name: Enter node name allotted to your profile. By default WebSphere assigns a unique node name to each profile created.

<table>
<thead>
<tr>
<th>Connection Account</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Principle: Username</td>
<td></td>
</tr>
<tr>
<td>• Credentials: Password</td>
<td></td>
</tr>
<tr>
<td>• Path to Java on the local server: java bin path</td>
<td></td>
</tr>
<tr>
<td>• Connection timeout period: 120 seconds (by default). Can be modified.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Generic JMX applications</th>
<th>Connection Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Host: Name of host server where the generic JMX application server is installed</td>
<td></td>
</tr>
<tr>
<td>• Port: Enter port number</td>
<td></td>
</tr>
</tbody>
</table>

**Generic environment additional information**

- Server name: Name of generic server
- Protocol: RMI or IIOP

**Connection Account**

- Principle: Username
- Credentials: Password
- Path to Java on the local server: java bin path
- Connection timeout period: 120 seconds (by default). Can be modified.

**The application server should be started with the option:**

- Dcom.sun.management.jmxremote.port=portNumber

*Using this option starts a dedicated JMX agent for this particular application. The Monitoring Studio generic JMX client needs to use this port number to establish a connection.*
Polling SNMP Agents

Monitoring Studio can directly poll SNMP agents to collect critical information about the middleware.

The basic steps to follow to poll the SNMP agent are:

- Launch the SNMP polling wizard
- Identify the host (SNMP agent), port and community string
- Specify the OID to be polled or values from an SNMP Table

Creating an SNMP polling

1. In the PATROL Console, right-click the Application icon and select KM Commands > New > SNMP polling.

2. 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.
3. If you selected **A single value from one OID**, the following dialog box is displayed:

![SNMP Polling Wizard](image)

**SNMP Polling Wizard — SNMP agent and OID selection Page**

- Identify the SNMP agent and the OID to poll:
  - **Host**: Enter the IP of the computer running the SNMP agent that will be polled. If it is the same server as the one the PATROL agent runs on, it is possible to use the following IP: 127.0.0.1
  - **Port**: Enter the port used by the SNMP agent to communicate.
  - **Community**: Enter the name of the community used by the SNMP agent.
  - **OID to poll**: Enter the OID (object identifier) to poll, as given by the Management Information Base (MIB).

- Click **Next**. The wizard will try to poll the OID to identify its type. If, for some reason, the OID cannot be polled, a warning message is displayed. The user must select an OID type, either "String" or "Integer," 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 returns 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:

- **Value**: Reports the actual value collected upon data polling.
- **Delta**: Calculates the difference between values collected during two consecutive polling.
- **DeltaPerSecond**: Reports the value resulting of the division of the Delta by the number of seconds 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).

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

![SNMP Polling Wizard](image)

**SNMP Polling Wizard — SNMP agent identification Page**

- Identify the SNMP agent and the list of columns from the SNMP table to poll:
  - **Host**: Enter the IP of the computer running the SNMP agent that will be polled. If it is the same server as the one the PATROL agent runs on, it is possible to use the following IP: 127.0.0.1
  - **Port**: Enter the port used by the SNMP agent to communicate.
  - **Community**: Enter the name of the community string used by the SNMP agent.
  - **SNMP Table OID**: Enter the Table OID (object identifier) to poll, as given by the Management Information Base (MIB).
  - **List of table columns to poll**: Enter the column numbers whose values should be retrieved. Enter “ID” to retrieve the row identifier. Leave the field blank to retrieve all values; or enter the column numbers separated by commas. Example: 4,8,9.

⚠️ *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.*
3. Specifying the Information Sources

Monitoring Studio KM for PATROL
Version 8.6.54

5. **Configure the Monitoring Studio settings.**
6. 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 `SW_SNMP_POLLING` 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 `SW_SNMP_TRAPS` class.

⚠️ The SNMP Agent emitting the traps should be configured to send them to the PATROL Agent where Monitoring Studio is installed and running. If the SNMP agent is not properly configured, Monitoring Studio will not receive any SNMP trap.
Creating an SNMP Trap Listening

1. In the PATROL Console, right-click the Monitored Application icon and select KM Commands > New > SNMP Trap listening...

SNMP Trap Listening Wizard — Welcome Page
2. Click **Next**.

SNMP Trap Listening Wizard — Agent Identification Page

3. Identify the agent and traps to listen to:
   - **IP address (optional)**: IP address of the computer or device where the SNMP agent is running and that will send the SNMP traps. Leave this field empty to listen to SNMP traps from any computer or device.
   - **Community**: Enter the name of the community string used by the SNMP agent.
   - **Enterprise OID**: Enter the OID of the SNMP Trap. You may use wildcards.
   - **Trap number (optional)**: Trap number contained in the SNMP Trap.
   - **OID 1 & 2 (optional)**: First and second attached variables OID that should be contained within the SNMP trap.
     - **Case sensitive**: Indicates whether or not the search will be case sensitive.

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.
4. Click **Next**.

5. Set the automatic acknowledgement:
   - **Acknowledge alert(s) 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.
   - **OID1 & 2**: First and second attached variables OID that should be contained within the SNMP trap to acknowledge a matching trap received.
   - **Acknowledge alert(s) if the following timeout is reached**: Check this box if you wish to acknowledge a matching SNMP trap after a certain period of time.
   - **Timeout value**: Time, in minutes, after which the matching SNMP Trap received, will be acknowledged. This value is only applicable if you have checked the "Acknowledge alert(s) if the following timeout is reached" box.
   - Choose the action to be taken when the condition above is reached: **Reset the MatchingTrapCount parameter to zero**, i.e. clear all previous alerts or **Decrease the MatchingTrapCount by one**, i.e. clear the previous alert.
6. Click **Next**.

![SNMP Trap Listening Wizard — Settings Page](image)

7. **Configure the Monitoring Studio settings.**
8. Click **Finish**.

### Monitoring Windows Events

The **Windows Events** tool monitors events posted by your application to consolidate the application monitoring under a unique icon. You will therefore not have to additionally look up Windows EventLog. 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 **SW_NTEVENTS** class.
Creating a Windows Event Monitoring

1. In the PATROL Console, right-click the Application icon and select KM Commands > New > Windows Event Monitoring...

![Windows Event Monitoring Wizard — Welcome Page]

2. Select the Windows Event log to monitor:
   - **Application**: Any event related to an application.
   - **Security**: Security events that are specified in the audit policy.
   - **System**: Any event related to the operating system.
   - Any other event available on your system.

   and click Next.

3. Identify the Windows Event to monitor:
   - **Source**: The software that logged the event, which can be either a program name such as "SQL Server," or a component of the system or of a large program such as a driver name. For example, "Elkii" indicates an EtherLink II driver.
   - **NT Event Types to monitor**: A classification of the event severity: Error, Information, or Warning in the system and application logs; Success Audit or Failure Audit in the security log. In the Event Viewer normal list view, these are represented by a symbol.
   - **Enter the searched NT Event ID**: A number identifying the particular event type. The first line of the description usually contains the name of the event type.
Example

6005 is the ID of the event that occurs when the Event log service is started. The first line of the description of such an event is "The Event log service was started." The Event ID and the Source can be used by product support representatives to troubleshoot system problems.

- **Optional information**: Arguments (insertion strings) that create a description of the NT Event. See the documentation of the NT Event you are monitoring for more information about these arguments. The argument number specifies where in the description the information should be found. Up to two arguments can be chosen and it is possible to indicate whether the information entered in the text bound is to be found within the argument ("must contain") or actually indicates the entire argument ("must exactly be").
- **Case sensitive**: Indicates whether or not the search for the Argument that is to be found within the Windows Event description will be case sensitive.

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 EventLog Reader tool to view content of the EventLogs and the characteristics of the events, including their arguments (insertion strings). Right-click on the main Monitoring Studio icon > KM commands > Tools > Windows EventLog Reader.

Click **Next**.
4. Configure the automatic acknowledgement feature. This feature allows you to reset the `MatchingEventCount` parameter to zero and its status to 'normal' — thereby, acknowledging the alert. This can be done in the following two cases:

- **Acknowledge alert(s) if the following timeout is reached**: A timeout since the last found matching Event
- **Acknowledge alert(s) if the following NT Event is found**: Specify the Windows Event

When this occurs, you can specify whether to:

- **Acknowledge all alerts, previously triggered by this Windows Event monitoring**: All the previous alerts are acknowledged in one action and the `MatchingEventCount` parameter is reset.
- **Acknowledge only one alert triggered by this NT Event search**: Just one alert should be acknowledged (the `MatchingEventCount` parameter is thus decreased by one).

Click **Next**.
5. **Configure the Monitoring Studio settings.**

![New Windows (NT) Event monitoring window]

- **Managed System:** PC11_3181
- **Monitoring Studio will create an object in the console to represent the monitoring of this Windows Event.**
- **You may use the default values or enter a display name as well as an ID to identify the object in the PATROL environment.**

**Object display name:**
- **Windows Event:** .NET Runtime

**Object internal identifier (ID):**
- **NETRuntime**

**What thresholds do you want to set for the newly created object?**
- **I want to use the default thresholds**

![Windows Event Monitoring Wizard — Settings Page]

6. Click **Finish**.

An icon representing the Windows event appears in the console under which are displayed the parameters **MatchingEventRate** and **MatchingEventCount**. You can set alert thresholds and automatic acknowledgements for the events found.
4. Specifying the Information to be Searched

Once the monitoring of the information sources is set up, you will have to specify the information to be searched in these sources. Because problems can be reported in files as a string or numeric values, Monitoring Studio allows you to:

- perform string searches
- extract numeric values
- monitor dynamic return outputs.

Please note that string or numeric value searches cannot be run in multi-line XML or HTML content and will require a pre-processing to be performed first.

Monitoring Studio also allows you to monitor dynamic return outputs.

Pre-processing Text

Because string and numeric value searches cannot be run in paragraphs, you will have 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 SW_Transform class.
Converting Multi-Line Records into single line

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

   - Specify the character to be used as a separator.

   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.
4. Click **Next**.
5. **Configure the Monitoring Studio 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.

### Converting XML to CVS

1. In the PATROL Console, right-click the **File Monitoring** icon and select **KM Commands > New > Text Preprocessing...**
2. Select **Convert XML to CVS (Comma-Separated Values)** and click **Next**.

![Text Pre-Processing Wizard — Welcome Page](image-url)
3. Define the XML tag that defines the record, the sub-objects and properties, the character to be used as a separator and click **Next**.

7. **Configure the Monitoring Studio settings.**
8. 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.

*An example of the XML LOG File Parsing, is available [here](#).*
Extracting 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. There are no options to select since Monitoring Studio will simply transform the HTML source by removing the HTML tags and display the output in the parameter TransformResult. Click **Next**.

4. **Configure the Monitoring Studio 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.

### Processing Text through an External Command

This option should be selected if text inputs (files, output of commands, Web requests, etc.) may 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 application.
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.

3. Specify the OS command to be executed to transform the text:
   - Command to be executed: Enter the command. 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.
   - 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.
   - Click Next.
4. **Configure the Monitoring Studio 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.
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 OS 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.
Searching for a Specific String

The **String Search** tool allows you to run fast and powerful searches for strings on the information sources 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 tool 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 OS commands):
  - 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 acknowledgement 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"** (flat files, OS commands, Web requests, database queries):
  - 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 **SW_STRINGS** 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 **information source** icon (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).
     - **Case sensitive**: Check the box or leave it unchecked as per your need
     - **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:

- **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. 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 the String(s) in all lines**: The string(s) will be searched for in all the lines of the specified source.
- **Search for the String(s) 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
- **Click Next**.
6. For string searches on a "running source" (LOG file and never-ending OS commands, 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
  - Indicate whether or not it is case-sensitive
  - Select where to search: specify the location of the string, enter the column separators if any
- **Acknowledge alert(s) if a timeout of "x" minutes is reached**: Check the box to enable alert acknowledgement. A timeout expires since the last matching line found; enter the value (default is set to 120 minutes).
  - Select the action to be performed when the condition is reached.
  - Click **Next**.

7. **Configure the Monitoring Studio settings**.
8. **Click Finish**
Extracting Numeric Values

Problems with an application are not always as simple as a sentence explaining that an "error has occurred." Sometimes, an application 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 application 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 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 information source. The basic mechanism is:

1. Specify an information source
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 these values.

Numeric value search objects are instances of the **SW NUMBERS** 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 information source icon (file, Web request, etc.) and select **KM Commands > New > Numeric Value Extraction**...
2. Click **Next**.

![Image of numeric value extraction wizard]

**Numeric Value Extraction Wizard — Lines Identification Page**

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 enter anything.

- **Line numbers (fill in 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

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 lines matching the **regular expression** specified in the field.

Click **Next**.
4. Indicate the position of the numeric value to be found:
   - **The numeric value is located**: There are four different modes to choose from and the information to enter depends on this choice.
   - **After/before the string**: Indicate if the numeric value is located after or before the string to be entered in the text field.
   - **At the character offset**: 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**: 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.
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. 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.

6. Check the box The value can be negative if the numeric values that you are looking for can be negative.

7. Click Next.

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 value found
   - Keep the last value found (default)
   - Calculate the average
   - Keep the lowest value
   - Keep the greatest value
   - Add up all values

Numeric Value Extraction Wizard — Additional Options Page
9. Click **Next**.

```
Managed System:PC11_3181

Select the parameters you wish to collect:

- **Value**: Actual value collected upon data polling
- **Delta**: Difference between values collected during two consecutive polling
- **DeltaPerSecond**: Delta divided by the elapsed time in seconds between the collection times

**Discard negative Delta values**

**Rescaling**: [No rescaling]
```

10. Select the parameters you wish to collect:
- **Value**: Reports the actual value collected upon data polling
- **Delta**: Calculates the difference between values collected during two consecutive polling.
- **DeltaPerSecond**: Reports the value resulting of the division of the Delta by the number of seconds 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**.

![Image of Numeric Value Extraction Wizard](image)

12. **Configure the Monitoring Studio 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).

## Monitoring Dynamic Return Outputs

The **Dynamic Object Builder** tool monitors objects whose return output is dynamic by applying 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 **SW_DYNAMIC** class.
Creating 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
   - Java MBean Polling
   - SNMP Polling
   - Text Pre-Processing
   - WBEM Query Analysis
   - Web Request Analysis
   - WMI Query Analysis

2. Select **KM Commands > New > Dynamic Object Builder...**
2. Click **Next**.

3. Define the rules to apply to the output data:
   
   - **View File Content**: Displays the current output data to which the Dynamic Object Builder rules will be applied.
   
   - **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.
   
   - **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.
   
   - **Trigger an alarm when objects are missing**: This option allows you to 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 display missing objects in the console. The available options are:
  - **Never**: Monitoring Studio never deletes missing objects in the console. They will always be present.
  - **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
  - **Column separators**: Define the way the Dynamic Object Builder detects columns of output data. Column contents are used to generate the Dynamic Items display name and ID in the PATROL Console.

- Click the **Column Separators** button to define how the Dynamic Object Builder will detect columns in the output data. Column contents are used to generate the Dynamic Items display name and ID in the PATROL Console

4. Click **Next**.

5. Define the dynamic objects, instance names and internal identifier:
   - **Object Display Name**: Name of the Dynamic Object Builder as it will appear in the PATROL Console
   - **Object Internal Identifier (ID)**: Name used by the PATROL Console to internally identify the Dynamic Object Builder
   - **%{Column Number}**: Indicate the column number in which the name of the object will be found by Monitoring Studio (e.g., %{1} for the first column)
   - **More Information**: Provides information about the objects creation and labeling
6. Click **Finish** to apply the Dynamic Object Builder rules to the KM command output file.

**Using String Search and Numeric Value Extraction Templates**

Features such as **String Search** and **Numeric Value Extraction** can help you analyze the Dynamic Items output. In order to apply these features to all the Dynamic Items in a single operation, the Dynamic Object Builder creates Templates instances of these features. While standard String Search and Numeric Value Extraction features apply to a single return output, Templates apply to all the Dynamic Items' output within the Dynamic Container (see step 5 in the example below).

When you modify a Template, the changes will apply to all the Dynamic Items upon the next data collection.

---

**Example**

How a Dynamic Object Builder elements are managed and displayed in the PATROL Console
Example: XML LOG File Parsing

Monitoring the content of an XML LOG file with Monitoring Studio

Specifying the file to monitor

1. Right-click the main Monitoring Studio icon or your previously-created application icon > KM Commands > New > File monitoring and analysis...
2. 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.
3. Specify the path to the file. You can use wildcards (*) 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.
4. Enter a label and ID for the icon which is going to be created in the PATROL Console.

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)

Right-click the File object which has been created > KM Commands > New > Text Pre-Processing... Select the Convert XML to CSV option.
Selecting a Type of Conversion to Apply to a Log File

In this example, the records in this XML LOG file are in the following format:

```
<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>
    <cthid>User_3_0.getDefaultUserRole</cthid>
    <reqid>2</reqid>
    <sesid>1uEPHTdRG2mM6GCFhV1EkwcBrCi68ffGizgIetGHWFm5Hc7lwE7!-1625978434!-1455528670!7502!1064223951289</sesid>
    <thrid>ExecuteThread: '68' for queue: 'default'-f7c8b25c01</thrid>
    <cthid>ExecuteThread: '68' for queue: 'default'-f7c8b1696c</cthid>
  </ctx>
  <msg>
    <![CDATA[FNNotAuthorizedException;FIA002002;No authorization to execute service operation]]>
  </msg>
  <ex>
    <ts>2003-09-22 11:47:35.509 CEST</ts>
    <sev>ERROR</sev>
    <ctx>
      <pid>A141607</pid>
      <appid>frontnet</appid>
      <cthid>User_3_0.getDefaultUserRole</cthid>
      <reqid>2</reqid>
      <sesid>1uEPHTdRG2mM6GCFhV1EkwcBrCi68ffGizgIetGHWFm5Hc7lwE7!-1625978434!-1455528670!7502!1064223951289</sesid>
      <thrid>ExecuteThread: '68' for queue: 'default'-f7c8b25c01</thrid>
      <cthid>ExecuteThread: '68' for queue: 'default'-f7c8b1696c</cthid>
    </ctx>
    <stack>
```

4. Specifying the Information to be Searched
<![CDATA[com.csg.pb.frontnet.exec_arch.calx.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_EOImpl.getDefaultUserRole(UserBean_3_0_3c05dc_EOImpl.java:145)
  at com.csg.pb.frontnet.services.user_3_0.bean.UserBean_3_0_3c05dc_EOImpl_WLSkel.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)]]>
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:

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;FNDBDataAccessFailureException;RDS001003;Code not Found - TableName: Landcode_1_RefTableObject, BusinessUnit: 0012, Language: 891, Code: 001];

2003-09-22 12:10:39.566 CEST;ERROR;KycBeneficialOwnerProfiles;FNDBDataAccessFailureException;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;FNDBDataAccessFailureException;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;FNDBDataAccessFailureException;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](image)

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

5. This brings us to the last panel, where we select the option **I want to use the default thresholds** and click **Finish**.

![String search object](image)

**String Search Confirmation**

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

![String search tree](image)

**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.
5. 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 sub-sections:

- **Specifying the Threshold Mechanism Mode**
- **Setting or Modifying Alert Thresholds**
- **Setting Thresholds on Dynamic Numeric Value Extractions**.

### 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 > Options > Thresholds Mechanism Selection...

![Threshold Mechanism Selection — Default option](image-url)
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 the **Application/Container icon > KM commands > Set 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

BMC Performance Manager 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 the user has to do is to enter actual "limits" as per the specific requirement, and the frequency of occurrence. This type of threshold can raise a maximum of two alerts.
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 alerts:

- **Border Alert**: An alert can be triggered when 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. This 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.
Setting Thresholds on Dynamic Numeric Value Extractions

Monitoring Studio enables you to set thresholds on Dynamic Numeric Value Extractions, that is Numeric Value Extractions performed on instances of a Dynamic Object.

Extracting numeric values 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.

To know how to set or modify alert thresholds on Dynamic Numeric Value Extractions, please refer to the section Setting or Modifying Alert Thresholds.

6. Specifying Alert Actions

Alert Actions enables the PATROL administrator to choose/configure the execution of certain actions when an application 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 for the overall application/root container. They specify the way in which the notification of a problem is done for all instances under the application/root container. This means that any parameter within this application/root container that trigger an alert will perform the Alert Actions set at the global level.
- Specific Alert Actions are set 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 root container already set to trigger Global Alert Actions, both settings will be taken into account for that particular parameter instance.

⚠️ If you setup monitoring objects under the main Monitoring Studio icon without creating an application or container icon, you cannot set global Alert Actions on them. Global Alert Actions can only be set on an application container and will apply to all objects under it.
Set Global Alert Actions

1. Right-click on a monitored application icon > **KM commands** > **Set Global Actions**.
2. Select the Alert Actions you want to trigger each time the parameter(s) enter(s) a state of alert and click **Next**.
3. Enter the relevant text with the help of Alert Action macros, as in the example shown below and click Next.

![Set Alert Actions for the application “Files”](image)

**Managed System:PC11_3181**

**Alert Action: Trigger a PATROL Event**

**Enter the text to be sent with the PATROL Event:**

Application `%{APPLICATION_LABEL}: %{ALARM_TYPE} on %{PARAMETER_NAME};`

**Note:** You can use macro variables in the fields above. See the documentation to have the complete list of available macros.

![Global Alert Action Wizard — Input Definition Page](image)

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

![Set Alert Actions for the application “Files”](image)

**Managed System:PC11_3181**

**The Alert Actions you selected will be executed for all the monitored parameters of the application.**

Click [Finish] to apply your settings.

**Note:** You will be able to set additional Alert Actions by using the "Specific Alert Actions" on the monitored parameters of the application.

![Global Alert Action Wizard — Alert Execution Confirmation Page](image)

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

1. Right-click on a **Monitored Instance > KM commands > Set Alert Actions**.
2. Select the parameters for which you wish to set specific Alert Actions. Click **Next**.

![Specific Alert Action Wizard — Parameter Selection Page](image-url)
3. The panel lists all the available specific Alert Actions. Make your selection and click **Next**.

```
Managed System:PC11_3181

Select the Specific Alert Actions to be executed when an alert is triggered for the DeletedFileCount parameter of "Folder: c:\Windows".

- Trigger a PATROL Event
- Annotate the parameter's graph
- Execute a command line
- Execute a PSL statement (advanced)
- Send a pop-up to the PATROL Consoles
- Write a line to a LOG file
- Send a basic SNMP trap
- Send a custom SNMP trap (advanced)
- Send an E-mail

Note: the Specific Alert Actions you select above will be executed when the chosen parameter triggers an alert, in addition to the overall Alert Actions.
```

4. Enter the required input. Click **Next**.

```
Managed System:PC11_3181

Alert Action: Trigger a PATROL Event

Enter the text to be sent with the PATROL Event:

```
Application %{APPLICATION_LABEL}: %{ALARM_TYPE} on %{PARAMETER_NAME};
```

Note: You can use macro variables in the fields above. See the documentation to have the complete list of available macros.
```
5. Click **Finish**.

![Specific Alert Action Wizard — Alert Execution Confirmation Page](image)

When the selected parameter goes into alert, it will trigger the specific Alert Action as configured.
Alert Actions Capabilities

Alert Actions offers a large choice of actions in order to notify the administrator of a problem with the application 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.
The following types of Alert Actions can be performed by Monitoring Studio:

**Trigger a PATROL event**

If you select the **Trigger a PATROL Event** action, you need to enter the string that will be displayed with the event:

```
Managed System: PC11_3181

Alert Action: Trigger a PATROL Event

Enter the text to be sent with the PATROL Event:
Application %{APPLICATION_LABEL}: %{ALARM_TYPE} on %{PARAMETER_NAME};

Note: You can use macro variables in the fields above. See the documentation to have the complete list of available macros.
```

**Alert Actions: Trigger a PATROL 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
- Other third-party products that interface with PATROL.
Annotate the parameter's graph

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

![Image of Annotate the parameter's graph interface]

**Note:** You can use macro variables in the fields above. See the documentation to have the complete list of available macros.
Execute an OS command

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

![Alert Actions: Execute an OS command panel]

**Enter the OS command to be executed:**

**Execute this command as (leave empty to use the PATROL default account):**

- Username:
- Password:

*Note: You can use macro variables in the fields above. See the documentation to have the complete list of available macros.*

- Enter a command line to be executed
- Enter the username and password used to run the command.

The command can be a program utility or a script shell, and can have arguments.

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

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

![PSL command interface]

**Alert Actions: Execute a PSL statement**

⚠️ The PSL command is recommended for advanced user of PATROL.
Send a pop-up to the PATROL consoles

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

---

**Alert Actions: Send a pop-up to the PATROL Consoles**

- **Enter the pop-up window title:**
  
  `%(ALARM_TYPE): Application %(APPLICATION_LABEL)`

- **Enter the text of the pop-up that will be sent to the PATROL Consoles:**
  
  `Application %(APPLICATION_LABEL): %(ALARM_TYPE) on %(PARAMETER_NAME)`

- **Warning:** heavy use of pop-ups is not recommended.

---

**Note:** You can use macro variables in the fields above. See the documentation to have the complete list of available macros.
Write a line to a LOG file

If you select the **Write a line to a LOG file** action, you need to enter the LOG file path and the content of the line.

![Alert Action: Write a line to a LOG file](image)

**Enter the LOG file path:**

C:\%{APPLICATION_ID}\LOG

**Enter the line that should be written in the LOG file:**

%{ASCTIME:%Y-%m-%d %H:%M:%S} %{APPLICATION_ID}: %{ALARM_TYPE} on %

**Note:** You can use macro variables in the fields above. See the documentation to have the complete list of available macros.
Send a basic SNMP trap (using the PATROL MIB)

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

![Send a basic SNMP trap panel](image)

**Alert Actions: Send a basic SNMP trap**

- IP address or hostname of the SNMP trap destination
- SNMP port and community string
- Text that will be sent in the SNMP trap
Send a custom SNMP trap

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

- IP address or hostname of the SNMP trap destination
- SNMP port and community string
- All the characteristics of the trap: Enterprise ID, 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:

---

**Alert Actions: Send an E-mail**

- 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
- 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 or JMX applications etc.

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><code>${PARAMETER_NAME}</code></td>
<td>Name of the parameter triggering the alert.</td>
</tr>
<tr>
<td><code>${VALUE}</code></td>
<td>Value of the parameter triggering the alert.</td>
</tr>
<tr>
<td><code>${ALARM_TYPE}</code></td>
<td>Type of the alert triggered (ALARM, WARN or INFORMATION).</td>
</tr>
<tr>
<td><code>${OBJECT_ID}</code></td>
<td>PATROL ID of the object triggering the alert.</td>
</tr>
<tr>
<td><code>${OBJECT_LABEL}</code></td>
<td>Display name of the object triggering the alert.</td>
</tr>
<tr>
<td><code>${OBJECT_CLASS}</code></td>
<td>Class (&quot;.KM&quot;) of the object triggering the alert.</td>
</tr>
<tr>
<td><code>${OBJECT_TYPE}</code></td>
<td>Type of the object triggering the alert (&quot;Process&quot;, &quot;String&quot;, etc.).</td>
</tr>
<tr>
<td><code>${PARENT_&lt;PARENT_MACRO&gt;}</code></td>
<td>Gets the parent's object of a macro. Example: In the case of String Search performed in Command Line, use the following macro to get complete command line return output: <code>${PARENT_OSCOMMAND_RETURN_OUTPUT}</code></td>
</tr>
<tr>
<td><code>${PARENT_ID}</code></td>
<td>ID of the object's parent triggering the alert (the parent of a String object could be a LOG file, e.g.).</td>
</tr>
<tr>
<td><code>${PARENT_LABEL}</code></td>
<td>Display name of the object's parent triggering the alert.</td>
</tr>
<tr>
<td><code>${PARENT_CLASS}</code></td>
<td>Class (&quot;.KM&quot;) of the object's parent triggering the alert.</td>
</tr>
<tr>
<td><code>${PARENT_TYPE}</code></td>
<td>Type of the object's parent triggering the alert (&quot;File&quot;, &quot;OSCommand&quot;, etc.).</td>
</tr>
<tr>
<td><code>${APPLICATION_ID}</code></td>
<td>PATROL ID of the application triggering the alert.</td>
</tr>
<tr>
<td><code>${APPLICATION_LABEL}</code></td>
<td>Display name of the application triggering the alert.</td>
</tr>
<tr>
<td><code>${APPLICATION_CLASS}</code></td>
<td>Class (&quot;.KM&quot;) of the application triggering the alert.</td>
</tr>
<tr>
<td><code>${APPLICATION_TYPE}</code></td>
<td>Type of the application triggering the alert (&quot;Application&quot;).</td>
</tr>
<tr>
<td><code>${APPLICATION_CONTACT}</code></td>
<td>Contact information in case of an application failure.</td>
</tr>
<tr>
<td><code>${APPLICATION_DESCRIPTION}</code></td>
<td>Description of the application.</td>
</tr>
<tr>
<td><code>${APPLICATION_EXISTENCEFILES}</code></td>
<td>List of files that identify the application as present.</td>
</tr>
</tbody>
</table>
### General Macros

<table>
<thead>
<tr>
<th>Description</th>
<th>General Macros</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current time when the Alert Action is performed. Specify a formatting as described under Format Symbols in the Reference section. Example: <code>%{TIME:%H:%M:%S}</code> will be replaced by 09:45:17 at run time. Note: <code>%{TIME:...}</code> is also accepted.</td>
<td>%{ASCTIME:...}</td>
</tr>
<tr>
<td>Inserts carriage return.</td>
<td>%{NEWLINE}</td>
</tr>
<tr>
<td>Recommended for advanced users only. Provides an internal instance variable name to be inserted. The path is relative to the object triggering the alert. Example: <code>%{/worstParam}</code> 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>
<td>%{/...}</td>
</tr>
<tr>
<td>Border alert type of the parameter triggering the alert (OK, WARN, ALARM).</td>
<td>%{BORDER_TYPE}</td>
</tr>
<tr>
<td>Border minimum range of the parameter triggering the alert.</td>
<td>%{BORDER_MIN}</td>
</tr>
<tr>
<td>Border maximum range of the parameter triggering the alert.</td>
<td>%{BORDER_MAX}</td>
</tr>
<tr>
<td>Number of consecutive times the parameter triggering the alert must have a value outside the border range before the alert occurs.</td>
<td>%{BORDER_NTIMES}</td>
</tr>
<tr>
<td>Alarm alert type of the parameter triggering the alert (OK, WARN, ALARM).</td>
<td>%{ALARM1_TYPE}</td>
</tr>
<tr>
<td>Alarm1 minimum range of the parameter triggering the alert.</td>
<td>%{ALARM1_MIN}</td>
</tr>
<tr>
<td>Alarm1 maximum range of the parameter triggering the alert.</td>
<td>%{ALARM1_MAX}</td>
</tr>
<tr>
<td>Number of consecutive times the parameter triggering the alert must have a value within the alarm1 range before the alert occurs.</td>
<td>%{ALARM1_NTIMES}</td>
</tr>
<tr>
<td>Alarm2 alert type of the parameter triggering the alert (OK, WARN, ALARM).</td>
<td>%{ALARM2_TYPE}</td>
</tr>
<tr>
<td>Alarm2 minimum range of the parameter triggering the alert.</td>
<td>%{ALARM2_MIN}</td>
</tr>
<tr>
<td>Alarm2 maximum range of the parameter triggering the alert.</td>
<td>%{ALARM2_MAX}</td>
</tr>
<tr>
<td>Number of consecutive times the parameter triggering the alert must have a value within the alarm2 range before the alert occurs.</td>
<td>%{ALARM2_NTIMES}</td>
</tr>
</tbody>
</table>

### Object Specific Macros

<table>
<thead>
<tr>
<th>Description</th>
<th>Database Macros</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of the database.</td>
<td>%{DATABASE_TYPE}</td>
</tr>
<tr>
<td>SQL statement sent for execution.</td>
<td>%{DATABASE_QUERY}</td>
</tr>
<tr>
<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>
<td>%{DATABASE_NAME}</td>
</tr>
<tr>
<td>Output returned by the SQL statement.</td>
<td>%{DATABASE_RETURN_OUTPUT}</td>
</tr>
<tr>
<td>Username configured to connect to the database and execute the SQL statement.</td>
<td>%{SW_USERNAME}</td>
</tr>
<tr>
<td>Password associated with the configured username.</td>
<td>%{SW_PASSWORD}</td>
</tr>
</tbody>
</table>

### Dynamic Object Macros

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

### File Macros

<table>
<thead>
<tr>
<th>Description</th>
<th>File Macros</th>
</tr>
</thead>
</table>

6. Specifying Alert Actions
### File System Macro

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%FILESYSTEM_NAME</td>
<td>Name of the monitored file system</td>
</tr>
</tbody>
</table>

### Folder Macro

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%FOLDER_PATH</td>
<td>Folder being monitored</td>
</tr>
<tr>
<td>%FOLDER_OLEST_REMAINING_FILE</td>
<td>Folder with the oldest remaining file</td>
</tr>
</tbody>
</table>

### HTTP Macros

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%HTTP_RETURN_OUTPUT</td>
<td>Result of the HTTP request</td>
</tr>
<tr>
<td>%HTTP_METHOD</td>
<td>GET or POST depending on what was selected in the GUI</td>
</tr>
<tr>
<td>%HTTP_URL</td>
<td>URL being tested</td>
</tr>
<tr>
<td>%SW_USERNAME</td>
<td>Web authentication username</td>
</tr>
<tr>
<td>%SW_PASSWORD</td>
<td>Password associated with the configured username</td>
</tr>
</tbody>
</table>

### JMX Macros

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%JMXPOLLING_SERVER_TYPE</td>
<td>Type of JMX server being polled</td>
</tr>
<tr>
<td>%JMXPOLLING_HOST</td>
<td>Hostname of JMX server polled</td>
</tr>
<tr>
<td>%JMXPOLLING_PORT</td>
<td>Port number of the JMX server polled</td>
</tr>
<tr>
<td>%JMXPOLLING_DOMAIN</td>
<td>Domain of the JMX server polled</td>
</tr>
<tr>
<td>%JMXPOLLING_KEY_PROPERTY</td>
<td>Key property of the JMX server polled</td>
</tr>
<tr>
<td>%JMXPOLLING_ATTRIBUTE</td>
<td>Attribute of the JMX server polled</td>
</tr>
<tr>
<td>%JMXPOLLING_CONTENT</td>
<td>Content of the result output of the JMX server polled</td>
</tr>
<tr>
<td>%SW_USERNAME</td>
<td>Username configured to connect to the JMX server</td>
</tr>
<tr>
<td>%SW_PASSWORD</td>
<td>Password associated with the configured username</td>
</tr>
</tbody>
</table>

### MPF Macros

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%MPF_FORMULA</td>
<td>User-defined formula used to rescale the parameter value</td>
</tr>
</tbody>
</table>

### OS Command Macro

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%OSCOMMAND_OSCOMMAND</td>
<td>Command line being executed and analyzed</td>
</tr>
<tr>
<td>%OSCOMMAND_RETURN_OUTPUT</td>
<td>Return output of the OS command</td>
</tr>
<tr>
<td>%OSCOMMAND_EXIT_STATUS_CODE</td>
<td>Exit status returned by the system after executing the command</td>
</tr>
<tr>
<td>%SW_USERNAME</td>
<td>Username configured to execute the OS command</td>
</tr>
<tr>
<td>Macros Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Process Macros</td>
<td>%SW_PASSWORD: Password associated with the configured username</td>
</tr>
<tr>
<td></td>
<td>%{PROCESS_NAME}: Process name being searched for, as entered in the GUI</td>
</tr>
<tr>
<td></td>
<td>%{PROCESS_COMMAND_LINE}: Process command line being searched for, as entered in the GUI</td>
</tr>
<tr>
<td></td>
<td>%{PROCESS_USER_ID}: Process user ID being searched for, as entered in the GUI</td>
</tr>
<tr>
<td></td>
<td>%{PROCESS_PID_FILE}: Path to the PID file whose corresponding process is being monitored</td>
</tr>
<tr>
<td>SNMP Polling Macros</td>
<td>%SNMPOLLING_OID: SNMP OID being polled</td>
</tr>
<tr>
<td></td>
<td>%SNMPOLLING_HOST: SNMP Agent’s hostname being polled</td>
</tr>
<tr>
<td></td>
<td>%SNMPOLLING_COMMUNITY: SNMP community string being used to query the SNMP agent</td>
</tr>
<tr>
<td></td>
<td>%SNMPOLLING_PORT: UDP port being used to poll the SNMP agent. 161 by default</td>
</tr>
<tr>
<td></td>
<td>%SNMPOLLING_CONTENT: Value of the OID being polled</td>
</tr>
<tr>
<td>SNMP Trap Macros</td>
<td>%SNMPTRAP_IP: Originating IP Address of the SNMP traps being looked for</td>
</tr>
<tr>
<td></td>
<td>%SNMPTRAP_FOUNDIP: Actual originating IP address of the trap that has been received</td>
</tr>
<tr>
<td></td>
<td>%SNMPTRAP_COMMUNITY: SNMP community string of the SNMP traps being looked for</td>
</tr>
<tr>
<td></td>
<td>%SNMPTRAP_ENTERPRISEID: Enterprise ID (OID) of the SNMP traps being looked for</td>
</tr>
<tr>
<td></td>
<td>%SNMPTRAP_TRAPNUMBER: SNMP Trap numbers (specific numbers) being looked for</td>
</tr>
<tr>
<td></td>
<td>%SNMPTRAP_FOUNDTRAPNUMBER: Actual SNMP trap number that has been received and matches the entered criteria</td>
</tr>
<tr>
<td></td>
<td>%SNMPTRAP_CONTENT: Content of the found trap</td>
</tr>
<tr>
<td>String Search Macros</td>
<td>%STRING_SEARCHED_1: First regular expression being searched for</td>
</tr>
<tr>
<td></td>
<td>%STRING_SEARCHED_2: Second regular expressions being searched for</td>
</tr>
<tr>
<td></td>
<td>%STRING_LAST_MATCHING_LINE: Last line that match with the String search criteria</td>
</tr>
<tr>
<td></td>
<td>%STRING_LAST_MATCHING_LINES: Last 10 lines that match with the String search criteria</td>
</tr>
<tr>
<td>WBEM Macros</td>
<td>%WBEM_HOST: Name of host where the WBEM query is being run</td>
</tr>
<tr>
<td></td>
<td>%WBEM_NAME_SPACE: Namespace of the WBEM query</td>
</tr>
<tr>
<td></td>
<td>%WBEM_QUERY: WBEM statement sent for execution</td>
</tr>
<tr>
<td></td>
<td>%WBEM_USERNAME: WBEM execution username</td>
</tr>
<tr>
<td></td>
<td>%WBEM_RETURN_OUTPUT: Content of the result output of the WBEM query</td>
</tr>
<tr>
<td></td>
<td>%SW_USERNAME: WBEM execution username</td>
</tr>
<tr>
<td></td>
<td>%SW_PASSWORD: Password associated with the configured username</td>
</tr>
</tbody>
</table>
### WMI Macros

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of host where the WMI query is being run</td>
</tr>
<tr>
<td>Namespace of the WMI query</td>
</tr>
<tr>
<td>WMI statement sent for execution</td>
</tr>
<tr>
<td>WMI execution username</td>
</tr>
<tr>
<td>Content of the result output of the WMI query</td>
</tr>
<tr>
<td>WMI execution username</td>
</tr>
<tr>
<td>Password associated with the configured username</td>
</tr>
</tbody>
</table>

### Windows Event Macros

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the Windows event log being monitored</td>
</tr>
<tr>
<td>Windows Event source whose new entries are monitored</td>
</tr>
<tr>
<td>ID of the Windows events being searched for</td>
</tr>
<tr>
<td>Last matching event found</td>
</tr>
<tr>
<td>Content of the NT event</td>
</tr>
</tbody>
</table>

### Windows Performance Macros

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows performance object instances being monitored</td>
</tr>
<tr>
<td>Windows performance counter being monitored</td>
</tr>
<tr>
<td>Windows performance object name being monitored</td>
</tr>
</tbody>
</table>

### Windows Service Macros

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the service of an NT service class</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 application.

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 **Set Thresholds**.

![Set Thresholds](image1.png)

2. Select the **MatchingLineCount** parameter and click **Next**.

![Set Thresholds](image2.png)
3. Verify that an alarm is triggered if the value is greater than 1 and click Set thresholds.
4. Click OK.

To Set the Alert Action

1. Select the Set Alert Actions... command from the menu to run the Alert Actions wizard:

![Set Specific Alert Actions](image)

Selecting the MatchingLineCount Parameter
3. Select the **MatchingLineCount** parameter and click **Next**.

![Set Specific Alert Actions for 'String Search: test' - MatchingLineCount](image)

**Managed System:** PC11\_0181

Select the Specific Alert Actions to be executed when an alert is triggered for the MatchingLineCount parameter of "String Search: test".

- **Trigger a PATROL Event:**
  - Annotate the parameter’s graph
  - Execute a command line
  - Execute a PSL statement (advanced)
  - Send a pop-up to the PATROL Consoles
  - Write a line to a LOG file
  - Send a basic SNMP trap
  - Send a custom SNMP trap (advanced)
  - Send an E-Mail

*Note: the Specific Alert Actions you select above will be executed when the chosen parameter triggers an alert, in addition to the overall Alert Actions.*

![Selecting an Alert](image)

4. Select the type of action to be executed when the **MatchingLineCount** parameter goes into alert state:
   - Check the **Trigger a PATROL event** box and click **Next**.
   - Enter the message of the PATROL event: Name of the application ; 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 PATROL Event:

   ```plaintext
   Application %{APPLICATION_LABEL}: error found in %{PARENT_LABEL}.%{NEWLINE}Error message: %{MORE_INFORMATION}
   
   %{APPLICATION_LABEL} contains the application display name in the PATROL Console.  
   %{PARENT_LABEL} contains the LOG file display name (it is the parent of the String search in the PATROL Console).  
   %{NEWLINE} will create a new line in the message.  
   %{MORE_INFORMATION} contains the entire line in the LOG file that triggered the alert.
   ```
6. Specifying Alert Actions

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 set just one Alert Action, Trigger a PATROL Event, but it would have been possible to set several Alert Actions, such as an OS command 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.

7. Configuring Advanced Settings Options

Advanced settings are configured at the application level. They can either be set:

- at the time of **creating the Application icon** by checking **Let me setup advanced options** box
- by editing an existing application icon. You will then have to:
  - right-click the **Application icon > KM Commands > Edit**
  - make sure the **Let me setup advanced options** box is checked
  - click **Next**. The following dialog box will appear:

![New Application/Container Icon](image)

**New Application/Container Icon Wizard — Advanced Options Page**

You can now:

- set command lines to **start or stop** the application monitoring from a KM command.
- specify **signature files**. The presence of signatures files indicates that the managed application is currently present on the system and should be monitored
- set **application constants**. This feature is useful to monitor applications whose properties may change from one system to another.
Configuring the Application Monitoring Start and Stop

Monitoring Studio allows you to set command lines to start and/or stop the application monitoring:

1. In the Advanced Options page, click Start -- Stop.
2. Set the following start and stop options:

   - **<Application name> can be started with the following command line**: Set a command line to start the application.
   - **<Application name> can be stopped with the following command line**: Set a command line to stop the application.
   - **Run these commands as this user with password**: Enter a login and password to execute the start and stop command lines. Please note that password will be encrypted once you complete all the configuration steps.

![Start and stop options for "MySQL"](image)

3. Click Accept.

   You will now be able to start/stop the application monitoring by right-clicking the Monitored Application icon > KM commands > Manage > Start the application/Stop the application.
Specifying Signature Files

This feature is used to monitor clustered applications. It specifies all the signature files to be searched. If the signature files are:

- present, Monitoring Studio starts monitoring the managed application
- missing, Monitoring Studio disable the monitoring of the entire application. This can be extremely useful when the application is hosted by a “fail-over” cluster.

To set signature files:

1. In the Advanced Options page, click Signature files.
2. Enter the paths to the signature files.

⚠️ Wildcards are not accepted.

3. Click Accept.

The application monitoring will only be performed if at least one of the four signature file paths is found. If none of the required files can be found, the application monitoring will be turned offline.
Configuring Application Constants

Application constants are defined at the application level and can be reused in the various objects underneath. They facilitate the monitoring across various systems of an application whose properties may change from one system to another. Here are some examples of use:

**Example 1**
When creating the application/container icon for "MyApplication", you define the APP_PATH constant with the /opt/MyApp value. Then, when creating a "LOG File Analysis" object in Monitoring Studio, you can specify %{APP_PATH}/log/MyApp.log as the path to the LOG file. If you plan to monitor the same application on another system, and this application is located under another directory (/usr/local/MyApp for example), you will be able to use the same configuration of Monitoring Studio (export and import) and just modify the APP_PATH constant on the new system.

**Example 2**
You 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 objects, you can define a DEVICE_IPADDRESS Application Constant at the level of the application/container 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.
To set application constants:

1. In the **Advanced Options** page, click **Application Constants**.
2. Fill in the following fields:
   - **Constant name**: Enter the name of the constant. Example: APPLICATION_PATH
   - **Value**: Set a value for the constant. Example: /opt/MyApp. If you enter the word "PASSWORD" as a Constant name, the corresponding value will be automatically encrypted once you click the **Finish** button at the last step of the wizard. The **Value** field will then show **** instead of the actual password characters.
   - **Required**: Check the box to activate this newly-set application constant. The monitoring of the application container and all its dependent objects will be offline if the value of the application constant is not set. This ensures that no monitoring operation is performed until the required application constants are properly set. This feature is particularly useful if you create an application monitoring template where all the defined application constants are empty — in this case, you first import the configuration template, then enter values to all required application constants before the monitoring actually starts.

3. Click **Accept**. The application constants will now be taken into consideration by Monitoring Studio.
8. Deploying your Configuration

Monitoring Studio allows you to export your configuration and deploy it on all the machines where the application 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 an [application monitoring configuration](#)
Exporting the entire Monitoring Studio configuration

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

![Configuration Export Wizard — Application/Container Selection Page](image)

This wizard helps you export the monitoring configuration you created in Monitoring Studio to a .CFG file that you can later import with pconfig (xconfig or VPCONF.EXE) and PCM (PATROL Configuration Manager).

Select an application or container:
- The entire Monitoring Studio configuration
- My Application
- The entire Monitoring Studio configuration — Include Monitoring Studio global settings
2. Select **The Entire Monitoring Studio configuration**.
3. (Option) Check **Include Monitoring Studio global settings** if you want the global settings to be included in the export file:

```
< Back   Next >   Help >>
```

**Configuration Export Wizard — Application/Container Selection Page**

- Select the global variables to be included. Please note that global variables will only be displayed if they have previously been enabled. In the example above, the Debug variables are listed because the Debug mode is enabled.
- Click **Next**.

4. Enter the path and file name of the file that will contain the PATROL Agent’s configuration:

```
< Back   Finish   Help >>
```

**Configuration Export Wizard — Configuration File Location Page**
- **Export configuration to**: Enter the path and file name for the configuration file.
- **Split the file in smaller parts if necessary**: Select this option if you feel that your pconfig version may not support large files.

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

   ![Configuration Export Wizard — Export Confirmation Message](image)

   **Configuration Export Wizard — Export Confirmation Message**

   - By default, the configuration file is created in the "%PATROL_HOME%\config" directory and named "Export_SW_Sentry.cfg".

### Exporting an application monitoring configuration

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

To export an application monitoring configuration, you can either:

- Right-click the main Monitoring Studio icon > KM commands > Configuration > Export Configuration and select the application-monitoring to export from the drop down list
- Or right-click an application or sub-application container > KM commands > Export Configuration.

You will then have to specify the path and name of the file that will contain the PATROL Agent’s configuration.

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

This feature allows you to configure a PATROL Agent 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 Agent and saved. Monitoring Studio offers you two options:

- To import the entire Monitoring Studio configuration
- To import an application monitoring configuration

The options displayed by the import configuration wizard will depend on the file type exported and saved (entire Monitoring Studio configuration and/or application monitoring).

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.
2. Enter the path to the configuration file and click **Next**.

![Importing Configuration Wizard — File Selection Page]

3. Select the configuration file to import and click **Next**.

![Importing Configuration Wizard — Global Setting Import Page]

4. Choose whether global settings will be imported.

   ![Warning: Importing global settings will overwrite the current global settings of your existing objects.]

8. Deploying your Configuration
5. Click:
   - **Overwrite** to overwrite existing objects.
   - **Make a new copy** if you do not want to overwrite existing objects. In that case, you will have to specify the prefix to be assigned to these copied objects:

   ![Importing Configuration Wizard — Prefix Definition Page]

   and click **OK**.
6. Click **Finish**. A panel confirming the import appears:

![Importing Configuration Wizard — Completed Import Confirmation Page](image)

7. Click **OK**.

On completion of the discovery process, you will see all the objects of the imported configuration in your console.
Generating Configuration Reports
Displaying Entire Configuration

To display the entire configuration, right-click the Monitoring Studio icon > KM Commands > Configuration > Display Entire Configuration.

Displaying Object Configuration

To display an object configuration:

1. Right-click the Object icon for which you wish to get an instant report
2. Select KM Commands > Display Object configuration.
   The report is generated and displayed instantly.
Instant Configuration Reports

Monitoring Studio enables you to generate an instant report on the configuration of all monitored objects:

To generate an instant configuration report:

1. Right-click the Monitoring Studio icon > KM Commands > Configuration > Report > Now...

2. Configure the report settings:
   - Select the report output format (CSV, Plain English, or XML)
   - Indicate where the report will be saved
   - Indicate the filename template to be used

3. Click OK. The report is generated in the selected format and saved in the defined location.
Scheduling Configuration Reports

To schedule a report:

1. Right-click the Monitoring Studio icon > KM Commands > Configuration > Report > Schedule Report. The scheduling wizard is displayed:

![Scheduling Wizard Image]

This wizard enables you to schedule configuration reports of monitored objects on PC11. Reports are automatically generated on an hourly, daily, weekly or monthly basis at precise times as per options selected.

You can schedule reports using the CSV or XML format.

2. Click Next.
3. Select the report output format and configure the scheduling options:
   - **Report Output formats**: Select one of the three available formats in the list:
     - CSV (Comma Separated Values) to create delimited text files reports which use a comma to separate values. Monitoring Studio will create a report per class
     - Plain English to create a report where data is displayed in an unformatted style.
     - XML (Extensible Markup Language) to create a report formatted as a standard XML file
   - **Scheduling options**: Select the frequency:
     - **Never**: to cancel a previously set schedule.
     - **Every hour**
     - **Every day at a specific time**
     - **Every week at a specific time and day**
     - **Every month at a specific time and day**
4. Click **Next**. The following panels depend on the option selected:

**Every hour**

![Report Scheduler Wizard — Every Hour Option](image-url)

**Report Scheduler Wizard — Every Hour Option**
- **Save the report in the following folder:** Enter the path and name of the folder.
- **Use this filename template:** Indicate the path and folder where the report is to be saved and its filename. Available macros are listed under Macros of the Reference section. Using the given macros will enable you to have reports that are properly named with the hostname and time the reports are generated.

Click **Next** to continue.

The last step of the Configuration Report Scheduling Wizard confirms the specified settings. Click **Finish** to close the wizard.

### Every day at a specific time

Indicate the time at which the report is to be generated.

![Monitoring Studio Configuration Report Scheduling Wizard](image)

The configuration report will be produced at the specified time.

Click **Next**.

The **Settings Panel** is displayed to allow you to define the folder in which the file must be saved, the filename template you wish to use.

Proceed with the appropriate settings and click **Next** to continue.

The last step of the Configuration Report Scheduling Wizard confirms the specified settings. Click **Finish** to close the wizard.
Every week at a specific time and day

Select the time and the day(s) of the week on which the report is to be generated.

Click **Next**.

The **Settings Panel** is displayed to allow you to define the folder in which the file must be saved, the filename template you wish to use.

Proceed with the appropriate settings and click **Next** to continue.

The last step of the Configuration Report Scheduling Wizard confirms the specified settings. Click **Finish** to close the wizard.
Every month at a specific time and day

Indicate the day of each month and the time at which the report is to be generated.

Click **Next**.

The **Settings Panel** is displayed to allow you to define the folder in which the file must be saved, the filename template you wish to use.

Proceed with the appropriate settings and click **Next** to continue.

The last step of the Report Scheduler Wizard confirms the specified settings. Click **Finish** to quit the wizard.
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
- Acknowledge and Update.

Acknowledge Alerts

This option is applicable to all application classes except for String searches, SNMP traps, Windows events, and File Security instances for which a specific command Acknowledge Alerts and Reset can be used to acknowledge all alerts and reset parameters to zero.

To acknowledge all alerts for a specific instance:

1. Right-click the **Object icon > KM Commands > Acknowledge 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 deactivate and then reactivate. An acknowledging event will automatically be triggered.

*No new data can be collected upon an alert acknowledgment.*

**Acknowledging all and Reset**

This is applicable to **String searches**, **SNMP traps** and **Windows events** instances. Right-click the **object icon > KM commands > Acknowledge all and reset**.

This menu command allows you to acknowledge all alerts and reset the MatchingTrapCount or MatchingEventCount parameter to zero.

**Acknowledge and Update**

This is applicable to File Security instances. Right-click **File Security icon > KM commands > Acknowledge alerts and update**.

This menu command allows you to acknowledge all alerts triggered on a File security monitoring object, and update the settings to conform with the recently made changes to the security settings (user access rights etc).
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.

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

Click Finish to save your settings.
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.

Select the Java executable directory you wish Monitoring Studio to use when performing commands requiring Java features and click **Finish** to save your settings.
Manual

If you have selected the Manual option at the previous step of the wizard, Monitoring Studio let you enter the path to the Java executable directory you wish Monitoring Studio to use when performing commands requiring Java features.

Click **Finish** to save your settings.

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 the String searches that you have setup on one command line execution on another one. This can be done easily with the Copy, Cut and Paste feature of Monitoring Studio: Copy or Cut any Monitoring Studio object and then Paste it in a new container.

To access the Copy, Cut and Paste features, right-click the desired **object** > **KM commands** > **Copy** or **Cut** or **Paste**, depending on what you want to do.

Some objects cannot be pasted in other objects. For example, you cannot paste a String search object in/under a Process monitoring object. Basically, you can paste everything everywhere that you would have been able to do with the regular wizards.
Editing a Monitored Object

To edit a monitored object, right-click the instance of the monitored object > **KM Commands** > **Edit**.

Modifying Object Name and/or ID

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

- Rename the Object display name
- Modify the Object internal identifier (ID)

To rename an object:

1. Right-click the desired object > **KM commands** > **Rename**.

![Modifying an Object Name and/or ID](image)
2. Make the changes and click **OK**. If you modified the object ID, the following pop-up appears:

![Modification of an Object Name and/or ID Warning](image)

3. If you are certain that the new ID will not cause any problems, click **Yes**, and the PATROL console will display the new label and will update the ID as well.

**Temporarily suspend 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 element or a group of elements. To pause the monitoring of a specific element or group of elements, right-click the **element (or element container) icon > KM Commands > Pause Monitoring**.

When in paused state, the element/group of elements 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 element/group of elements click **Resume Monitoring** in the menu.

**Refreshing Parameters**

To manually refresh parameters, without waiting for an automatic polling cycle, right-click the **instance icon > KM Commands > Refresh Parameters**.
Rename an Object

Monitoring Studio provides two ways for renaming objects:

- through the Edit KM command. Please note that the object ID cannot be changed with this method.
- through the Rename KM Command. Both the object display name and the object ID can be changed with this method.

Using the Edit KM Command

1. Right-click on the **object icon > KM commands > Edit**.
2. Follow the wizard steps until you arrive at the last panel shown below:

![Renaming an object](image)

*Renaming an object*
1. Change the object label/display name, and click **Finish**.
2. The object icon will now display the new label in the PATROL console.

### Using the Rename KM Command

1. Right-click on the **object icon > KM commands > Rename**.

   ![Rename KM Command](image)

   **Modifying an object ID**

2. Modify the **Object display name** and/or the **Object internal Identifier (ID)** and click **OK**.
3. If you modified the object ID, a pop-up asks you to confirm your modification. If you are certain that the new ID will not cause any problems, click **Yes**. The PATROL console will display the new label and will update the ID as well.
Restart an Application

If Monitoring Studio warns you that the application you are monitoring is down, it is possible to re-launch the application by using the Application/Container icon > KM commands > Manage > Start the application command menu.

This runs the command line entered in the "Start--Stop" option of New/Edit Application icon (container) wizard. If no starting command line is provided, the following message pops-up:

![Cannot Start the Application Message]

If the execution of the Start application command is confirmed, a window comes up with the output of the command being executed.

⚠️ This option should be used by advanced users only.

Restart Scan from the Beginning of the File

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 icon > KM commands > Restart scan from the Beginning of file.
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.
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 > Options > 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.

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 day. Polling intervals can be set for objects created by Monitoring Studio that collect data (files, processes, OS commands, SNMP polling etc.). By default, the polling interval is set to 2 minutes on all objects, which can be modified at any time.
To set the polling interval:

1. In the PATROL Console, right-click the Monitored Application icon or the object icon > KM commands > Set Polling Interval.

- The option to set polling intervals is not available for string searches, numeric values, text pre-processing, application/containers 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.

2. Configure the polling interval options:
   - **Collect every: x hours; x minutes; x seconds**: Set the polling interval in hours/minutes/seconds.
   - **Collect once a day at: x hour (24 hours); x minutes; x seconds**: Here the values selected indicate the time of day. Example: 14; 30; 0 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: 14; 30; 0 would mean that the polling is done only once a week on <selected weekday> at 2:30pm (14:30 hrs)

3. Click OK.
Stop an Application

It is possible to stop an application that you are monitoring by using the Application/Container icon > KM commands > Manage > Stop the application command menu.

This runs the command line entered in the Start--Stop option of the New/Edit Application icons (container) wizard. If no stopping command line is provided, the following message pops-up:

*If the execution of the Stop application command is confirmed, a window comes up with the output of the command being executed.*

This option should be used by advanced users only.

Triggering a KM Discovery

Monitoring Studio automatically executes a discovery every hour of all objects for the monitored system. This enables discovering and then monitoring any new objects added or removed etc.

You can also force a discovery manually by right-clicking on the Monitoring Studio icon > KM Commands > Trigger a KM Discovery.
Visualizing Currently Running Processes

The **Process Viewer** tool displays all the processes that are currently seen by Monitoring Studio 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 main Monitoring Studio icon > **KM commands** > **Tools** > **Process Viewer**.

   ![Process Viewer](image)

   **Process Viewer**

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

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 real time 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" (attached variables). 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 to 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 Windows EventLogs

The **Windows EventLog Reader** tool shows how each event is actually registered in a specific Windows EventLog by providing its source, its ID and its arguments (or "insertion strings"). All these criteria are required for monitoring EventLogs.

To access the Windows EventLog Reader tool:

1. Right-click the main Monitoring Studio icon > KM commands > Tools > Windows EventLog Reader.

2. Select the EventLog you wish to view and click the **Update** button to refresh the window. This may take a few seconds to complete. The latest event is shown first in this list.

3. Refer to the **Arguments** column to know the arguments registered in each event. There is one line per argument: the first argument line corresponds to the "Argument 1" field in the Windows Event monitoring wizard, the second argument line corresponds to the "Argument 2" field, etc.

4. Click:
   - **Update** to refresh the information displayed.
   - **Close** to quit the Windows EventLog Reader tool.
Visualizing Monitored File Content

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

1. Right-click on the main Monitoring Studio icon > **KM commands > Tools > File Viewer**.
2. Specify the visualization options:
   - **File path**: path of the file that you wish to visualize.
   - **Show me**: The first/last: X KB: Indicate the part of the file that you wish to visualize
   - **Only lines matching with (RegExp)**: Enter a [regular expression](https://en.wikipedia.org/wiki/Regular_expression) and only the lines matching this regular expression are displayed in the File content field.
3. Click **Update**. The file content is now displayed.
4. Click **Close**.
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.

To set the SNMP Browser tool:

1. Right-click the main **Monitoring Studio icon > KM commands > Tools > SNMP Browser**
2. Enter the hostname or IP address of the computer where the SNMP agent is running
3. Enter its port (by default: 161) and its community
4. Specify the root OID from which you want to perform a "SNMP walk" (sort of SNMP dump)
5. 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 some details 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 thousands of variables may take a long time._

6. Click **Close** to quit the SNMP Browser tool.

Deleting Monitored Object(s)

Monitoring Studio allows you to delete:

- any monitored object by right-clicking **object icon > KM commands > Delete**. The object icon and dependencies are then removed and no longer monitored.
- all objects under the main Monitoring Studio icon by right-clicking **Monitoring Studio icon > KM commands > Delete All**.
Troubleshooting
This section deals with troubleshooting. It tells you how to enable the debug mode 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 > Options > Debug...
2. Check the **Enable debug box**.
3. By default, the debug output is displayed in the System Output Window. 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 specify a debug output file path if you want 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 for a few minutes since information may also be lost by the PATROL Console if its buffer is full.
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 the debug mode off once the required information has been collected.

5. Click OK.

Frequently Asked Questions and Problems

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.

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)

Can I search for Windows Events whose description match a regular expression

Monitoring Studio does not parse the description string of the events in the Windows EventLog because this operation is very resource-intensive because each possible description string corresponds to a unique event ID. If you know the event ID, you do not need to identify the description string.

You only need to check the value of the insertion strings in the description. More information about insertion strings ...

Use the built-in Windows EventLog Reader utility of Monitoring Studio: right-click the main Monitoring Studio icon > KM commands > Tools > Windows EventLog Reader.
Difference between a flat file and a LOG file

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.

**String Searches of Flat vs LOG files**

The string searching function works differently on "running sources" i.e. LOG files and never-ending OS commands; than on flat sources (flat files, OS commands, Web requests, etc.):

**Running sources: LOG files**

On "running sources" (LOG files and never ending OS commands), 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 acknowledgement
- Number of matches per minute since the last polling

In addition, for LOG files and never-ending OS commands, you can specify auto-acknowledging strings that will automatically reset the graph to the "number of matches".

**Automatic acknowledgement of string search alerts (LOG files and "never-ending" command lines only)**

Each time the specified strings have been found, the **MatchingLineCount** parameter will increase and will trigger an alert. The automatic acknowledgement feature allows you to make the MatchingLineCount graph go back to zero and reset its status to 'normal'.
Automatic Acknowledgment of String Search Alerts

- **Acknowledge alert(s) if the string below is found**: Specify the string; indicate whether, or not, it is case-sensitive.
  
  Select where to search: specify the location of the string, enter the column separators if any

- **Acknowledge alert(s) if a timeout of "x" minutes is reached**: A timeout expires since the last matching line is found; enter the value (default is set to 120 minutes).
  
  When this occurs, you can either specify if all alerts previously triggered by this string search should be acknowledged at one time (the MatchingLineCount parameter goes back to zero), or if only one alert should be acknowledged (the MatchingLineCount parameter is decreased by one):

- **When the above condition is reached**:  
  - Reset the MatchingLineCount parameter to zero (clear all previous alerts)
  - Decrease the MatchingLineCount by one (clear the previous alert)

Flat sources

On "flat sources" (flat files, OS commands, Web requests, database queries), the strings are searched within the entire source (the whole file, the whole standard output, the whole HTTP response, the whole dataset) every time.

String search in a flat source: Line selection.

In flat sources, you have the option to select the lines in which to search for the specified string(s):
How do I know which version of Monitoring Studio I am running?

To find out which version of BMC Performance Manager Monitoring Studio you are running, right-click the **KM main 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](http://www.bmc.com) or the Sentry Software Web site at [www.sentrysoftware.com](http://www.sentrysoftware.com) for the latest information and product versions.
I'm unable to connect to the WebLogic application server

There could be several reasons for this:

- Ensure that the input variables are correct.
- Ensure you have downloaded the essential external files corresponding to your WebSphere application server version from the Sentry Software Website.

Before setting-up the monitoring of a WebLogic AS, you need to download certain WebLogic files created to work with Monitoring Studio from the Sentry Software website and store them in %PATROL_Home%\bin. These files are essential in order to connect to your WebLogic AS through Monitoring Studio.

Please ensure you have the right java virtual machine depending on the version of your WebLogic application servers.

I'm unable to connect to the WebSphere application server

There could be several reasons for this:

- Ensure that the input variables are correct (connection credentials, SOAP port number etc.)
- Ensure you have downloaded the essential external files corresponding to your WebSphere application server version from the Sentry Software website.

Before setting-up the monitoring of a WebSphere AS, you need to download certain WebSphere files created to work with Monitoring Studio from the Sentry Software website and store them in %PATROL_Home%\Patrol3\bin. These files are essential in order to connect to your WebSphere AS through Monitoring Studio.

Please ensure you have the right java virtual machine depending on the version of your WebSphere application servers.

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 is listening on the UDP/161 port (by default)

Use an 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 the main Monitoring Studio 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.

By default, when a PSL script executes 500,000 instructions within 2 hours (7200 seconds), the PATROL Agent issues a warning, assuming that the PSL script has entered into an infinite loop. However, nowadays, it is very common for computers to execute as many instructions as this, and the more powerful the computer is, the more likely this is to occur.

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 recommends that users set these upper thresholds. This can be achieved by modifying the following configuration variables with WPCONFIG or xpconfig:

- /AgentSetup/AgentTuning/psInstructionMax = 1,000,000
- /AgentSetup/AgentTuning/psInstructionPeriod = 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 not able to measure the processor time usage and memory usage of a group of processes like a tree (a main process, its children, children of children, etc.).

Monitoring Studio can 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 does not read the content of my file

You could encounter such a problem if you incorrectly selected the LOG file option although you wanted to monitor a FLAT file. You have to then redo the whole configuration:

1. Create a new file monitoring
2. Choose the LOG file option
3. Copy and paste the string search and numeric value extraction objects 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 gets updated entirely and so must be read entirely at each polling.

In LOG files, new lines are appended at the end of the file. Only these new lines need to be analyzed.

Please also ensure that the PATROL Agent default account has sufficient access rights to access and read this file.

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 /MASAI/SENTRY8/folderLimit variable in the PATROL agent configuration (if not manually changed, the default is 1000).
Monitoring Studio fails to connect to my Oracle Database server

1. Check that SQL*Plus is properly installed on the same computer where Monitoring Studio is running (with the PATROL Agent).
2. SQL*Plus is installed with the Oracle Database Server, Oracle Database Client and Oracle Instant Client.
3. Ensure that you have provided Monitoring Studio with the path to SQL*Plus (either ORACLE_HOME or path to the SQL*Plus binary).
4. Check that SQL*Plus is able to resolve the Oracle system identifier (Oracle SID).
   - When SQL*Plus is installed with Oracle Database Server or Oracle Database Client, the Oracle SID needs to be properly registered in the tnsnames.ora file, usually located in the $ORACLE_HOME/network/admin directory.
   - If the tnsnames.ora file is not located in this default directory, specify its location in the optional alternate TNS_ADMIN path field (enter the directory that contains tnsnames.ora).
   - If the Oracle Instant Client is installed, you do not need the tnsnames.ora file. You can use the following syntax to specify the Oracle Database Server you want to connect to: // server_hostname:1521/oracle_sid

Monitoring Studio fails to connect to my remote Microsoft SQL Server

Check that the Microsoft SQL Server client has been properly installed on the same computer where Monitoring Studio is running (with the PATROL Agent).

Verify that the PATH variable has been properly set in the PATROL environment.

Monitoring Studio fails to connect to a secured Web server (SSL) on my UNIX/Linux server

Monitoring Studio only supports HTTPS queries on Windows.

Monitoring Studio fails to authenticate on 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 PATROL Agent default account 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 Studio.
Monitoring Studio does not follow an HTTP redirection (Web)

Some HTTP redirection is 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 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).

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.
What is the meaning of the "Argument1, 2..." fields in the Windows Event monitoring wizard?

Windows Events are identified by their source and an event ID. Each event ID corresponds to a description string in the event source. This description string contains "insertion strings", or arguments, that are replaced at problem time.

To identify the arguments or insertion strings of an event:

1. Launch the Windows EventLog Reader built-in tool of Monitoring Studio
2. Right-click on the main Monitoring Studio icon > KM commands > Tools > Windows EventLog Reader.

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.
Introduction

This chapter gives you some additional information on Processes, WMI, Regular expression and Format symbols for macros.

Format Symbols for \%{ASCTIME:...} Macros

The following table recapitulates all of the time formats available in the \%{TIME:...}, \%{ASCTIME:...} and \%{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>Format Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</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. 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.</td>
</tr>
<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>%Ec</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>%EX</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>
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
- Retrieve numbers, etc.

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[0-9A-F] 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 |
| ^         | Match the beginning of the line  
Example: ^Err will match all lines that begin with Err |
| $         | Match the end of the line |
Application Classes

This section lists the application classes of Monitoring Studio KM for PATROL with details on the parameters discovered and the menu commands available for each application class.

Baselines and Key Performance Indicators

Some parameters are identified by default as Key Performance Indicators (KPIs) and therefore automatically included in the base lining calculation. To learn more about auto baselining and KPIs, please refer to the Managing Baselines and Key Performance Indicators chapter.

In this guide, parameters flagged as KPIs and included by default in the baseline calculation process are respectively identified by the following icons:

- Baselining
- KPI

Regular Expressions

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]\application\> will match all lines that contain the word Application or application but not ApplicationAA

\{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:

\(firewall\)|\(antivirus\) 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
List of Application Classes

If the KM is properly loaded, the following 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>SW_APPLICATIONS</td>
<td>Monitors application/container icons</td>
</tr>
<tr>
<td>SW_DB_QUERIES</td>
<td>Executes and monitors database queries</td>
</tr>
<tr>
<td>SW_DYNAMIC</td>
<td>Executes Dynamic Items</td>
</tr>
<tr>
<td>SW_DYNAMIC_CONTAINER</td>
<td>Creates a Dynamic Object Container</td>
</tr>
<tr>
<td>SW_DYNAMIC_DISCOVERY</td>
<td>Creates a Dynamic Object Builder</td>
</tr>
<tr>
<td>SW_DYNAMIC_NUMBERS</td>
<td>Performs dynamic numeric value extractions</td>
</tr>
<tr>
<td>SW_DYNAMIC_STRING</td>
<td>Executes dynamic string searches</td>
</tr>
<tr>
<td>SW_FILES</td>
<td>Monitors files and file content</td>
</tr>
<tr>
<td>SW_FILE_SECURITY</td>
<td>Monitors file security</td>
</tr>
<tr>
<td>SW_FILESYSTEMS</td>
<td>Monitors file-systems</td>
</tr>
<tr>
<td>SW_FOLDERS</td>
<td>Monitors folders</td>
</tr>
<tr>
<td>SW_HTTP_REQUESTS</td>
<td>Monitors web-based applications and executes HTTP requests</td>
</tr>
<tr>
<td>SW_HTTP_WEBFARM</td>
<td>Monitors web farms</td>
</tr>
<tr>
<td>SW_JMX</td>
<td>Polls and monitors JMX-enabled application servers</td>
</tr>
<tr>
<td>SW_KMWATCH</td>
<td>Monitors parameters of other KMs</td>
</tr>
<tr>
<td>SW_NTEVENTS</td>
<td>Monitors Windows Event Logs</td>
</tr>
<tr>
<td>SW_NT_PERFORMANCE</td>
<td>Monitors Windows Performance counters</td>
</tr>
<tr>
<td>SW_NTSERVICES</td>
<td>Monitors Windows Services</td>
</tr>
<tr>
<td>SW_NT_WMI</td>
<td>Executes and monitors WMI queries</td>
</tr>
<tr>
<td>SW_NUMBERS</td>
<td>Performs numeric value extractions</td>
</tr>
<tr>
<td>SW_OSCOMMANDS</td>
<td>Executes, monitors and parses command lines and scripts</td>
</tr>
<tr>
<td>SW_PROCESSES</td>
<td>Monitors processes</td>
</tr>
<tr>
<td>SW_SENTRY</td>
<td>Main application class</td>
</tr>
<tr>
<td>SW_SNMP_POLLING</td>
<td>Polls and monitors SNMP devices</td>
</tr>
<tr>
<td>SW_SNMP_TRAPS</td>
<td>Monitors and listens for SNMP traps</td>
</tr>
<tr>
<td>SW_STRINGS</td>
<td>Executes string searches</td>
</tr>
<tr>
<td>SW_TRANSFORM</td>
<td>Transforms complex (multi-line, HTML, XML) text to enable string/numeric value searches</td>
</tr>
<tr>
<td>SW_WBEM</td>
<td>Executes and monitors WBEM queries</td>
</tr>
</tbody>
</table>
SW_APPLICATIONS

You can create SW_APPLICATIONS instances (application/container icons) through the New > Application icon (container)... Menu Command of the Monitoring Studio icon.

- SW_APPLICATIONS instances are used to group different monitoring tools configured to monitor a given application, device, or any other IT component.
- SW_APPLICATIONS instances may contain other SW_APPLICATIONS instances (containers and sub-containers).

Parameters

None.

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the application/container icon</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the parent icon</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the root parent icon</td>
</tr>
<tr>
<td>First required file</td>
<td>File whose presence is required to activate the monitoring of this application/container</td>
</tr>
<tr>
<td>Second required file</td>
<td>File whose presence is required to activate the monitoring of this application/container</td>
</tr>
<tr>
<td>Third required file</td>
<td>File whose presence is required to activate the monitoring of this application/container</td>
</tr>
<tr>
<td>Fourth required file</td>
<td>File whose presence is required to activate the monitoring of this application/container</td>
</tr>
<tr>
<td>Constant 1</td>
<td>Name of the first application constant</td>
</tr>
<tr>
<td>Constant 2</td>
<td>Name of the second application constant</td>
</tr>
<tr>
<td>Constant 3</td>
<td>Name of the third application constant</td>
</tr>
<tr>
<td>Constant 4</td>
<td>Name of the fourth application constant</td>
</tr>
<tr>
<td>Constant 5</td>
<td>Name of the fifth application constant</td>
</tr>
<tr>
<td>Contact</td>
<td>Name or contact information of the person in charge of the application</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the application</td>
</tr>
<tr>
<td>Start command line</td>
<td>Displays the command line that will be used to start the application by the &quot;Manage &gt; Start the application&quot; Menu Command</td>
</tr>
<tr>
<td>Stop command line</td>
<td>Displays the command line that will be used to stop the application by the &quot;Manage &gt; Stop the application&quot; Menu Command</td>
</tr>
</tbody>
</table>
### Menu Commands

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &gt; Process monitoring</td>
<td>Adds a Process monitoring using the New Process wizard</td>
</tr>
<tr>
<td>New &gt; Windows Service monitoring</td>
<td>Adds a Windows Service monitoring using the New Windows Service wizard (only available on Windows servers)</td>
</tr>
<tr>
<td>New &gt; File monitoring and analysis</td>
<td>Adds a File monitoring using the New File wizard</td>
</tr>
<tr>
<td>New &gt; Folder monitoring</td>
<td>Adds a Folder monitoring using the New Folder wizard</td>
</tr>
<tr>
<td>New &gt; File System monitoring</td>
<td>Adds a File System monitoring using the New File System wizard</td>
</tr>
<tr>
<td>New &gt; Command line analysis</td>
<td>Adds an OS Command monitoring using the New OS Command wizard</td>
</tr>
<tr>
<td>New &gt; Database Query analysis</td>
<td>Adds a Database Query analysis using the New Database Request wizard.</td>
</tr>
<tr>
<td>New &gt; Java MBean Polling (JMX)</td>
<td>Adds a JMX polling using the Java MBean polling wizard</td>
</tr>
<tr>
<td>New &gt; Web Request analysis</td>
<td>Adds an HTTP Request analysis using the New HTTP Request wizard</td>
</tr>
<tr>
<td>New &gt; Web-farm monitoring</td>
<td>Adds a Web-farm monitoring using the New web-farm wizard</td>
</tr>
<tr>
<td>New &gt; SNMP polling</td>
<td>Adds an SNMP polling monitoring using the New SNMP polling wizard</td>
</tr>
<tr>
<td>New &gt; SNMP Trap listening</td>
<td>Adds an SNMP polling monitoring using the New SNMP Trap wizard</td>
</tr>
<tr>
<td>New &gt; WMI Query analysis</td>
<td>Adds a WMI Query analysis using the new WMI query wizard.</td>
</tr>
<tr>
<td>New &gt; WBEM Query analysis</td>
<td>Adds a WBEM Query analysis using the new WBEM query wizard.</td>
</tr>
<tr>
<td>New &gt; Windows Event monitoring</td>
<td>Adds a Windows Event monitoring using the New Windows Event wizard (only available on Windows servers)</td>
</tr>
<tr>
<td>New &gt; Windows Performance monitoring</td>
<td>Adds a Windows Performance counter monitoring using the New Windows Performance wizard (only available on Windows servers)</td>
</tr>
<tr>
<td>New &gt; Multi-Parameter Formula</td>
<td>Allows to monitor any KM that is loaded in the PATROL Console by applying mathematical formulas to the collected values.</td>
</tr>
<tr>
<td>New &gt; Sub-container</td>
<td>Starts the new sub-container icon wizard</td>
</tr>
<tr>
<td>Edit</td>
<td>Allows you to edit the Application monitoring</td>
</tr>
<tr>
<td>Modify Application constants</td>
<td>Modifies the application constants</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval</td>
</tr>
<tr>
<td>Set Global Alert Actions</td>
<td>Allows you to add Alert Actions that will be used for the application as well as its dependent objects</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this Database Query instances and all dependent instances</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts the application/container object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies the application/container object</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes a previously copied or cut object into this application/container</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the application monitoring and all its dependent object</td>
</tr>
<tr>
<td>Rename</td>
<td>Allows you to rename this application monitoring</td>
</tr>
<tr>
<td>Manage &gt; Start Application</td>
<td>Allows you to start the application using the Start command line.</td>
</tr>
<tr>
<td>Manage &gt; Stop Application</td>
<td>Allows you to stop the application using the Stop command line.</td>
</tr>
</tbody>
</table>
### SW_DB_QUESTIES

**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>ConnectionStatus*</td>
<td>State of the server connection. Value set by DbQueryColl every 2 minutes</td>
<td>{0 = Successful; 1 = Connection failed}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<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>QueryStatus</td>
<td>Displays whether or not the query was successfully executed; Value set by DbQueryColl every 2 minutes</td>
<td>{0 = Successful; 1 = Execution failed}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>ReturnOutput</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>
</tbody>
</table>

* This parameter is used by default when visualizing the corresponding monitor instance in BPPM.

For detailed information about Baselining and KPI, see Managing Baselines and Key Performance Indicators.

<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 parent application</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the Database query’s root application</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>Hostname</td>
<td>Display the name of the host machine</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>
</tbody>
</table>
### Application Classes

**Monitoring Studio KM for PATROL**  
Version 8.6.54

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>New &gt; Numeric Value Extraction</td>
<td>Creates a new Numeric Value extraction for this Database Query analysis</td>
</tr>
<tr>
<td>New &gt; Text Pre-Processing</td>
<td>Creates a new Text pre-processing for this Database Query analysis</td>
</tr>
<tr>
<td>New &gt; Dynamic Object Builder</td>
<td>Creates a new Dynamic Object Builder for this Database Query analysis</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the Database Query monitoring settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this Database Query analysis monitoring</td>
</tr>
<tr>
<td>Set Alert actions</td>
<td>Adds specific Alert Actions to the Database Query analysis monitoring</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this Database Query object and all dependent objects</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 Database Query analysis object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the Database Query analysis monitoring and all its dependent objects</td>
</tr>
<tr>
<td>Rename</td>
<td>Allows you to rename this Database Query analysis 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 monitoring of this Database Query analysis object</td>
</tr>
<tr>
<td>Resume monitoring</td>
<td>Resumes the monitoring of this Database Query analysis object</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the Database Query analysis monitoring</td>
</tr>
</tbody>
</table>
**SW_DYNAMIC**

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 = Instance is present; 1 = Instance is missing}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
</tbody>
</table>

* This parameter is used by default when visualizing the corresponding monitor instance in BPPM.

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Dynamic object ID</td>
</tr>
</tbody>
</table>

**SW_DYNAMIC_CONTAINER**

Parameters

None.
SW_DYNAMIC_DISCOVERY

Parameters

None.

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Dynamic discovery ID</td>
</tr>
<tr>
<td>Type</td>
<td>Dynamic object type</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the parent application</td>
</tr>
<tr>
<td>Dynamic Object Display Name</td>
<td>Defines how dynamic object labels are generated</td>
</tr>
<tr>
<td>Dynamic Object ID</td>
<td>Defines how dynamic object IDs are generated</td>
</tr>
<tr>
<td>Column Separators</td>
<td>Defines symbols used to separate columns in the dynamic parent output file</td>
</tr>
<tr>
<td>Consecutive Separators</td>
<td>Indicates whether consecutive separators are treated as a single separator</td>
</tr>
<tr>
<td>Include Object Matching</td>
<td>Keeps only lines matching a user-defined regular expression from the dynamic parent output file</td>
</tr>
<tr>
<td>Exclude Object Matching</td>
<td>Discard lines matching a user-defined regular expression from the dynamic parent output file</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 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>Set 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>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this File monitoring object and all dependent objects</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>
</tbody>
</table>
# SW_DYNAMIC_NUMBERS

## 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 polling</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 BPPM

## Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the numeric extraction</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the numeric extraction’s parent</td>
</tr>
<tr>
<td>Type</td>
<td>Dynamic object type</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 extraction the number 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 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</td>
</tr>
<tr>
<td>After/Before</td>
<td>Searches for the numeric either after or before the specified string</td>
</tr>
<tr>
<td>Specified String</td>
<td>Searches for the number before or after this specified string</td>
</tr>
<tr>
<td>Character Offset</td>
<td>Character offset where the number is searched for</td>
</tr>
<tr>
<td>Field Number</td>
<td>Numeric of the field in which the numeric 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>
SW_DYNAMIC_STRINGS

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 BPPM

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>

SW_FILES

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>%/min</td>
<td>None</td>
<td>Availability</td>
</tr>
<tr>
<td>GrowthPercentage</td>
<td>File growth percentage. Value set by fileColl</td>
<td></td>
<td></td>
<td>Statistics</td>
</tr>
<tr>
<td>GrowthSpeed</td>
<td>File growth speed. Value set by fileColl</td>
<td>KB/min</td>
<td></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>
</tbody>
</table>
### Application Classes

#### Monitoring Studio KM for PATROL

**Version 8.6.54**

<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>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 BPPM

### 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>Application ID</td>
<td>PATROL internal identifier of the File’s root application.</td>
</tr>
<tr>
<td>File Name &amp; Path</td>
<td>File name and path (with wildcards)</td>
</tr>
<tr>
<td>Monitored Parameters</td>
<td>List of parameters that are currently being used for the File monitoring</td>
</tr>
<tr>
<td>Monitored File</td>
<td>File name path of the file currently being monitored</td>
</tr>
<tr>
<td>File Type</td>
<td></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 File</td>
</tr>
<tr>
<td>New &gt; Numeric Value Extraction</td>
<td>Creates a new Numeric Value extraction for this File</td>
</tr>
<tr>
<td>New &gt; Text Pre-Processing</td>
<td>Creates a new Text pre-processing for this File</td>
</tr>
<tr>
<td>New &gt; File Security Check</td>
<td>Creates a new File security monitoring for the current File</td>
</tr>
<tr>
<td>New &gt; Dynamic Object Builder</td>
<td>Creates a new Dynamic Object Builder for the current file</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the File monitoring settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this File monitoring</td>
</tr>
<tr>
<td>Set Alert actions</td>
<td>Adds specific Alert Actions to the File monitoring</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this File 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 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</td>
</tr>
<tr>
<td>View file content</td>
<td>Displays the File content</td>
</tr>
</tbody>
</table>
**Restart scan from start of file**
If a String, Numeric value search is performed for this File, restart the File scan from the Beginning of the File (only relevant to "LOG" Files)

**Acknowledge Alerts**
Acknowledges all alerts and reset parameters to zero.

**Pause monitoring**
Pauses the File monitoring

**Resume monitoring**
Resumes the File monitoring as well as all its dependent objects

**Refresh parameters**
 refreshes all instance parameters of the SW_FILES class

---

### SW_FILESYSTEMS

**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>FreeMegabytes*</td>
<td>File system free space left in megabytes. Value set by FileSystemColl every 2 minutes</td>
<td>Megabytes (MB)</td>
<td>Alarm ≤ 10</td>
<td>Statistics</td>
</tr>
<tr>
<td>FreeSpacePercentage*</td>
<td>File system free space left in percentage. Value set by FileSystemColl every 2 minutes</td>
<td>Percent</td>
<td>Warning ≤ 10 Alarm ≤ 1</td>
<td>Statistics</td>
</tr>
<tr>
<td>UsedSpaceGrowthPercentage</td>
<td>How fast the file system is getting filled in, in percentage of its size. Value set by FileSystemColl every 2 minutes</td>
<td>%/h</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>UsedSpaceGrowthSpeed</td>
<td>How fast the file system is getting filled in. Value set by FileSystemColl every 2 minutes</td>
<td>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 BPPM

### 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>Application ID</td>
<td>PATROL internal identifier of the File systems’ root application</td>
</tr>
<tr>
<td>File System Object</td>
<td>File System object monitored</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>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this File systems monitoring</td>
</tr>
<tr>
<td>Set Alert Actions</td>
<td>Adds specific Alert Actions to the File systems monitoring</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the configuration report of this File system object and all dependent objects</td>
</tr>
</tbody>
</table>

---

Application Classes
<table>
<thead>
<tr>
<th>Cut</th>
<th>Cuts this File system monitoring object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td>Copies this File system monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the File systems monitoring and all its dependent objects</td>
</tr>
<tr>
<td>Rename</td>
<td>Allows you to rename this File systems 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 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 SW_FILESYSTEMS application class</td>
</tr>
</tbody>
</table>

**SW_FILE_SECURITY**

**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>AccessRightsCheck</td>
<td>File's access right status. Value set by fileSecurityColl every 2 minutes</td>
<td>{0 = OK ; 1 = Invalid Access Rights}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>GroupCheck</td>
<td>File's group status. Value set by fileSecurityColl every 2 minutes</td>
<td>{0 = OK ; 1 = Invalid group}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>Integrity*</td>
<td>File's integrity status (i.e. no changes made to the content). Value set by fileSecurityColl every 2 minutes</td>
<td>{0 = OK ; 1 = File has been modified}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>OwnerCheck</td>
<td>File's owner status. Value set by fileSecurityColl every 2 minutes</td>
<td>{0 = OK ; 1 = Invalid owner}</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 BPPM*

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the File security check</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the File security check's parent</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the File security check's root application</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 File security monitoring settings</td>
</tr>
<tr>
<td><strong>Set Polling Interval</strong></td>
<td>Sets the polling interval for this File monitoring</td>
</tr>
<tr>
<td><strong>Set Alert Actions</strong></td>
<td>Adds specific Alert Actions to the File security monitoring</td>
</tr>
<tr>
<td><strong>Display Object Configuration</strong></td>
<td>Displays the Monitoring Studio configuration report of this File security monitoring object and all dependent objects</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this File security monitoring object.</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this File security monitoring object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the File security monitoring and all its dependent objects</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Renames this File security monitoring</td>
</tr>
<tr>
<td><strong>Acknowledge and Update</strong></td>
<td>Acknowledges all the alerts on this File security object and updates its settings to reflect any security changes made</td>
</tr>
<tr>
<td><strong>Pause monitoring</strong></td>
<td>Pauses the File security monitoring</td>
</tr>
<tr>
<td><strong>Resume monitoring</strong></td>
<td>Resumes the File security monitoring</td>
</tr>
<tr>
<td><strong>Refresh parameters</strong></td>
<td>Refreshes all instance parameters of the SW_FILE_SECURITY application class</td>
</tr>
</tbody>
</table>

SW_FOLDERS

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>DeletedFileCount</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>FileCount*</td>
<td>Displays the number of files in a folder. If the option &quot;Include sub-folders&quot; is selected, the number of files is the sum of the number of files of every sub-folders and the main folder. Value set by FolderColl</td>
<td>file(s)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>FolderSize*</td>
<td>Displays the folder size (include sub-folders) in MB. Value set by FolderColl</td>
<td>Megabytes (MB)</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>%/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>KB/min</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>LastModifiedFileElapsedTime</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.</td>
<td>minutes</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>
### Application Classes

**Monitoring Studio KM for PATROL**

**Version 8.6.54**

<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>ModifiedFileCount</td>
<td>Displays the number of modified files per minute. Value set by FolderColl</td>
<td>files/min</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>NewFileCount</td>
<td>Displays the number of new files per minute. Value set by FolderColl</td>
<td>files/min</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>OldestModifiedFileElapsedTime</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>
</tbody>
</table>

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BPPM

### 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>Application ID</td>
<td>PATROL internal identifier of the Folder’s root application</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>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling interval</td>
<td>Sets the polling interval for this Folder monitoring</td>
</tr>
<tr>
<td>Set Alert Actions</td>
<td>Adds specific Alert Actions to the Folder monitoring</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this Folder monitoring object and all dependent objects</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 SW_FOLDERS class</td>
</tr>
</tbody>
</table>
SW_HTTP_REQUESTS

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 HTTP request to execute. Value set by httpRequestColl</td>
<td>seconds</td>
<td>Warning ≥ 15 Alarm ≥ 30</td>
<td>Response Time</td>
</tr>
<tr>
<td>HTTPStatusCode</td>
<td>HTTP Response Status code. Value set by httpRequestColl</td>
<td>--</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>ReturnOutput</td>
<td>Displays the returned output of the HTTP Request execution.</td>
<td>--</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>ServerConnectionState</td>
<td>State of the connection to the server. Value set by httpRequestColl</td>
<td>{0 = OK ; 1 = Server could not be reached}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>Status</td>
<td>HTTP Request status. Value set by httpRequestColl</td>
<td>{0 = OK ; 1 = Degraded ; 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 BPPM

Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the HTTP Request analysis</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the HTTP Request’s parent</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the HTTP Request’s root application</td>
</tr>
<tr>
<td>Used HTTP method</td>
<td>HTTP method that is used for this HTTP Request analysis</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>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>
</tbody>
</table>
### Menu Command

<table>
<thead>
<tr>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td>Edits the Web Request analysis settings.</td>
</tr>
<tr>
<td><strong>Set Thresholds</strong></td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Set Polling Interval</strong></td>
<td>Sets the polling interval for this Web Request monitoring object</td>
</tr>
<tr>
<td><strong>Set Alert Actions</strong></td>
<td>Adds specific Alert Actions to the Web Request analysis</td>
</tr>
<tr>
<td><strong>Display Object Configuration</strong></td>
<td>Displays the Monitoring Studio configuration report of this Web request object and all dependent objects</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
<td>Cuts this Web request object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
<td>Copies this Web request object</td>
</tr>
<tr>
<td><strong>Paste</strong></td>
<td>Pastes a previously copied or cut String search or Numeric Value search object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Deletes the Web Request analysis and all its dependent objects</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>Renames the Web Request 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 Web Request analysis as well as all its dependent objects</td>
</tr>
<tr>
<td><strong>Resume monitoring</strong></td>
<td>Resumes the Web Request analysis as well as all its dependent objects</td>
</tr>
<tr>
<td><strong>Refresh Parameters</strong></td>
<td>Refreshes all parameters of this Web request object</td>
</tr>
</tbody>
</table>

### SW_HTTP_WEBFARM

**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>OperationServerCount*</td>
<td>Percentage of operational servers. Value set by httpWebFarmColl</td>
<td>server</td>
<td>Alarm = 0</td>
<td>Statistics</td>
</tr>
<tr>
<td>OperationalServerPercent</td>
<td>Number of servers that are operational. Value set by httpWebFarmColl</td>
<td>%</td>
<td>Warning ≤ 80 Alarm ≤ 50</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BPPM

### Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the Web-farm monitoring</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Web-farm monitoring’s parent</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the Web-farm monitoring’s root application</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-farm monitoring</td>
</tr>
<tr>
<td>New &gt; Numeric Value Extraction</td>
<td>Creates a new Numeric Value extraction for this Web-farm monitoring</td>
</tr>
<tr>
<td>New &gt; Text Pre-Processing</td>
<td>Creates a new Text pre-processing for this Web-farm monitoring</td>
</tr>
<tr>
<td>Add hosts</td>
<td>Adds new hosts to the Web-farm monitoring. A new Web request monitoring will be created for each host added</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this object monitoring</td>
</tr>
<tr>
<td>Set Alert actions</td>
<td>Adds specific Alert Actions to the Web-farm monitoring</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this Web-farm monitoring object and all dependent objects</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this Web farm monitoring object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this Web farm monitoring object</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes a previously copied or cut Web request monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the Web-farm monitoring and all its dependent objects</td>
</tr>
<tr>
<td>Acknowledge Alerts</td>
<td>Acknowledges all alerts and reset parameters to zero.</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the Web-farm monitoring object</td>
</tr>
<tr>
<td>Pause monitoring</td>
<td>Pauses the Web-farm monitoring as well as all its dependent objects</td>
</tr>
<tr>
<td>Resume monitoring</td>
<td>Resumes the Web-farm monitoring as well as all its dependent objects</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the Web-farm monitoring</td>
</tr>
</tbody>
</table>

SW_JMX

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 polling</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>ExecutionStatus</td>
<td>Displays the output of the JMX poll execution. Value set by JMXPoll every 2 minutes</td>
<td>{0 = Successful ; 1 = Execution failed}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
</tbody>
</table>
**Application Classes**

**Monitoring Studio KM for PATROL**

**Version 8.6.54**

<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>Text</td>
<td>Displays the value of an attribute in text. Value set by JMXColl every 2 minutes</td>
<td>n/a</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>Value*</td>
<td>Displays the value of an attribute in integers. Value set by JMXColl every 2 minutes</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 BPPM

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the JMX polling object</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the JMX polling object’s parent</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the JMX polling object’s root application</td>
</tr>
<tr>
<td>Server type</td>
<td>Type of JMX server (JBoss/WebLogic/generic etc.)</td>
</tr>
<tr>
<td>Host</td>
<td>Displays name of host machine</td>
</tr>
<tr>
<td>Port</td>
<td>Displays port number of JMX server</td>
</tr>
<tr>
<td>Username</td>
<td>Displays the user name</td>
</tr>
<tr>
<td>Path to java</td>
<td>Displays the path of the java virtual machine on the local server e.g.,%JAVA_HOME%(bin)</td>
</tr>
<tr>
<td>Timeout</td>
<td>Displays the execution timeout</td>
</tr>
<tr>
<td>Domain</td>
<td>Displays the domain monitored</td>
</tr>
<tr>
<td>Key Property</td>
<td>Displays the key property monitored</td>
</tr>
<tr>
<td>Attribute</td>
<td>Displays the attribute monitored</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 JMX polling object</td>
</tr>
<tr>
<td>New &gt; Numeric Value Extraction</td>
<td>Creates a new Numeric value extraction for this JMX polling object</td>
</tr>
<tr>
<td>New &gt; Text Pre-Processing</td>
<td>Creates a new Text pre-processing for this JMX polling object</td>
</tr>
<tr>
<td>New &gt; Dynamic Object Builder</td>
<td>Creates a new Dynamic Object Builder for this JMX polling object</td>
</tr>
<tr>
<td>Edit</td>
<td>Allows you to edit the JMX polling settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this JMX polling object monitoring</td>
</tr>
<tr>
<td>Set Alert actions</td>
<td>Adds specific Alert Actions to the JMX polling monitoring</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this JMX polling object and all dependent objects</td>
</tr>
</tbody>
</table>
### SW_KMWATCH

#### 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 KMWatchColl</td>
<td>Depends on the parameter</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 BPPM

#### Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the KM Watch monitoring</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the KM Watch’s parent</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the KM Watch’s root application</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 KM Watch monitoring settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Intervals</td>
<td>Sets the polling interval for this KM Watch monitoring</td>
</tr>
<tr>
<td>Set Alert Actions</td>
<td>Adds specific Alert Actions to the KM Watch monitoring</td>
</tr>
</tbody>
</table>
Menu Command | Description
---|---
Display Object Configuration | Displays the Monitoring Studio configuration report of this KM Watch object and all dependent objects
Cut | Cuts this KM Watch monitoring object
Copy | Copies this KM Watch monitoring object
Delete | Deletes the KM Watch monitoring object
Rename | Renames the KM Watch monitoring object
Acknowledge Alerts | Acknowledges all alerts and reset parameters to zero
Pause monitoring | Pauses the KM Watch monitoring
Resume monitoring | Resumes the KM Watch monitoring
Refresh Parameters | Refreshes all instance parameters of the SW_KMWATCH class

SW_NTEVENTS

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>MatchingEvent Count*</td>
<td>Number of Matching Windows Events. Value set by NTEventColl</td>
<td>events</td>
<td>Alarm = 1</td>
<td>Statistics</td>
</tr>
<tr>
<td>MatchingEvent Rate*</td>
<td>Rate of matching Windows Events. Value set by NTEventColl</td>
<td>events/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 BPPM

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>Application ID</td>
<td>PATROL internal identifier of the Windows Event's root application</td>
</tr>
<tr>
<td>Event log</td>
<td>Indicates which EventLog is searched</td>
</tr>
<tr>
<td>Event Source</td>
<td>Source of the event to be searched for</td>
</tr>
<tr>
<td>Event ID</td>
<td>ID of the event to be searched for</td>
</tr>
<tr>
<td>Acknowledging NT Event</td>
<td>Is the auto-acknowledgment activated</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>Alert Actions trigger</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 Event monitoring settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this Windows Event monitoring</td>
</tr>
<tr>
<td>Set Alert Actions</td>
<td>Adds specific Alert Actions to the Windows Event monitoring</td>
</tr>
<tr>
<td>Display Object</td>
<td>Displays the Monitoring Studio configuration report of this Windows Event object and all dependent objects</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this Windows Event monitoring object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this Windows Event monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the Windows Event monitoring</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the Windows Event monitoring</td>
</tr>
<tr>
<td>Acknowledge all and reset</td>
<td>Acknowledges all alerts and resets the &quot;MatchingEventCount&quot; parameter to '0'</td>
</tr>
<tr>
<td>Pause Monitoring</td>
<td>Pauses the Windows Event monitoring</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the Windows Event monitoring</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the SW_NTEVENTS class</td>
</tr>
</tbody>
</table>

SW_NTPERFORMANCE

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 NTPerformanceColl</td>
<td></td>
<td>Depends on the parameter</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

* Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BPPM

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>Application ID</td>
<td>PATROL internal identifier of the Windows Performance’s root application</td>
</tr>
<tr>
<td>Performance object</td>
<td>Name of the Windows Performance object that is read</td>
</tr>
<tr>
<td>Counter</td>
<td>Name of the Windows Performance counter that is read</td>
</tr>
</tbody>
</table>
### Application Classes

**Monitoring Studio KM for PATROL**

**Version 8.6.54**

#### Name

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instances</td>
<td>Selected Windows performance instances</td>
</tr>
<tr>
<td>Value Type</td>
<td>How the value is calculated (average, maximum, etc.) when more than one instance was selected</td>
</tr>
<tr>
<td>Scale</td>
<td>Scale used (the original performance value is divided by this number)</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>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this Windows Performance monitoring</td>
</tr>
<tr>
<td>Set Alert Actions</td>
<td>Adds specific Alert Actions to the Windows Performance monitoring</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this Windows Performance object and all dependent objects</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>Delete</td>
<td>Deletes the Windows Performance monitoring</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the Windows Performance 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 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 SW_NTPERFORMANCE class</td>
</tr>
</tbody>
</table>

#### SW_NTPERFOMANCE

**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 NTServicell</td>
<td>{0 = Started ; 1 = Intermediate state ; 2 = Stopped}</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 BPPM*
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>Application ID</td>
<td>PATROL internal identifier of the Windows Service’s root application</td>
</tr>
<tr>
<td>Service name</td>
<td>Name of the Service that is monitored</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 Service monitoring settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this Windows Service monitoring</td>
</tr>
<tr>
<td>Set Alert Actions</td>
<td>Adds specific Alert Actions to the Windows Service monitoring</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this Windows Service object and all dependent objects</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</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the Windows Service 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 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 SW_NTSERVICES class</td>
</tr>
</tbody>
</table>

SW_NT_WMI

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>QueryStatus*</td>
<td>Displays whether or not the query was successfully executed. Value set by WMIQueryColl every 2 minutes</td>
<td>{0 = Successful; 1 = Execution failed}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>ReturnOutput</td>
<td>Displays the output of the WMI query execution. Value set by WMIQueryColl every 2 minutes</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 BPPM

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>Application ID</td>
<td>PATROL internal identifier of the T WMI query object’s root application</td>
</tr>
<tr>
<td>Host</td>
<td>Displays name of host machine</td>
</tr>
<tr>
<td>Name Space</td>
<td>Displays WMI namespace (e.g.: root\cimv2)</td>
</tr>
<tr>
<td>WMI Query</td>
<td>Displays the 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>New &gt; Text Pre-Processing</td>
<td>Creates a new Text pre-processing for this WMI query</td>
</tr>
<tr>
<td>New &gt; Dynamic Object Builder</td>
<td>Creates a new Dynamic Object Builder for this WMI query</td>
</tr>
<tr>
<td>Edit</td>
<td>Allows you to edit the WMI query monitoring settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this WMI query monitoring</td>
</tr>
<tr>
<td>Set Alert actions</td>
<td>Adds specific Alert Actions to the WMI query monitoring</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this WMI query object and all dependent objects</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>Pasters 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 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 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 WMI query monitoring</td>
</tr>
</tbody>
</table>
**SW_NUMBERS**

**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 polling</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 valued has been found</td>
<td>{0 = Value found ; 1 = Value not found}</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 BPPM

**Infobox**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the numeric extraction</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the numeric extraction's parent</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the numeric extraction's root application</td>
</tr>
<tr>
<td>Parent Type</td>
<td>Type of the parent (File, OS Command, 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 extraction the number 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 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</td>
</tr>
<tr>
<td>After/Before</td>
<td>Searches for the numeric either after or before the specified string</td>
</tr>
<tr>
<td>Specified String</td>
<td>Searches for the number before or after this specified string</td>
</tr>
<tr>
<td>Character Offset</td>
<td>Character offset where the number is searched for</td>
</tr>
<tr>
<td>Field Number</td>
<td>Numeric of the field in which the numeric 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>Edit</td>
<td>Edits the numeric extraction settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Alert Actions</td>
<td>Adds specific Alert Actions to the Numeric Value extraction object</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this object and all dependent objects</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this Numeric Value extraction object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this Numeric Value extraction object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the Numeric Value extraction</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the Numeric Value extraction 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 Numeric Value extraction</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the Numeric Value extraction</td>
</tr>
</tbody>
</table>

SW_OSCOMMANDS

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>ExecutionStatus*</td>
<td>Status of the execution. Value set by OSCommandColl</td>
<td>{0 = Successful ; 1 = Execution Failed}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>ExecutionTime*</td>
<td>Time taken by the OS Command to run. Value set by OSCommandColl</td>
<td>seconds</td>
<td>Warning ≤ 30</td>
<td>Response Time</td>
</tr>
<tr>
<td>ExitStatus</td>
<td>Status of the OS command exit code. Value set by OSCommandColl</td>
<td>{0 = Successful ; 1 = Execution Failed}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>ReturnOutput</td>
<td>Displays the return output of the OS command. Value set by OSCommandColl</td>
<td>n/a</td>
<td>None</td>
<td>--</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 BPPM.
Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>PATROL internal identifier of the OS Command analysis.</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the OS Command’s parent.</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the OS Command’s root application.</td>
</tr>
<tr>
<td>OS Command</td>
<td>Command line that is given to the OS to execute.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Maximum execution time before timeout.</td>
</tr>
<tr>
<td>Username</td>
<td>The command line is executed with this username.</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>
<tr>
<td>New &gt; Numeric Value Extraction</td>
<td>Creates a new Numeric value extraction for this command line execution</td>
</tr>
<tr>
<td>New &gt; Text Pre-Processing</td>
<td>Creates a new Text pre-processing for this command line execution</td>
</tr>
<tr>
<td>New &gt; Dynamic Object Builder</td>
<td>Creates a new Dynamic Object Builder for this command line execution</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the command line execution settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this command line execution monitoring</td>
</tr>
<tr>
<td>Set Alert Actions</td>
<td>Adds specific Alert Actions to the command line execution</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this command line object and all dependent objects</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this command line execution object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this command line execution 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 command line execution and all its dependent objects</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the command line execution monitoring 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 command line execution as well as all its dependent objects</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the command line execution as well as all its dependent objects</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Re-execute the command line (if needed) and refresh all parameters. All dependent objects will be refreshed as well (SW_STRINGS and SW_NUMBERS instances)</td>
</tr>
</tbody>
</table>
# SW_PROCESSES

## 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 children of the matching process(es). Value set by proColl</td>
<td>processes</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Count*</td>
<td>Displays the number of processes that match the criteria. Value set by proColl</td>
<td>processes</td>
<td>Alarm = 0</td>
<td>Statistics</td>
</tr>
<tr>
<td>HandleCount (Windows only)</td>
<td>Displays the number of handles opened by the matching process(es). Value set by proColl</td>
<td>handles</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>PageFaultsPerSec (Windows only)</td>
<td>Displays the number of page faults per second caused by the matching process(es). Value set by proColl</td>
<td>faults/s</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>PageFileBytes (Windows only)</td>
<td>Displays the page file used by the matching process(es). Value set by proColl</td>
<td>Megabytes</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>PrivateBytes (Windows only)</td>
<td>Displays the amount of memory that has been allocated by this process and that cannot be shared with others. Value set by proColl</td>
<td>Megabytes</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>ProcessorTime* + Displays the processor time percent used by the matching process(es). Value set by proColl</td>
<td>Percent (%)</td>
<td>Warning ≥ 100</td>
<td>Statistics</td>
<td></td>
</tr>
<tr>
<td>ThreadCount (Windows only)</td>
<td>Displays the number of threads of the matching process(es). Value set by proColl</td>
<td>threads</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>VirtualBytes Displays the virtual memory used by the matching process(es). Value set by proColl</td>
<td>Megabytes</td>
<td>None</td>
<td>Statistics</td>
<td></td>
</tr>
<tr>
<td>WorkingSet (Windows only)</td>
<td>Displays the working set size of the matching process(es). Value set by proColl</td>
<td>Megabytes</td>
<td>None</td>
<td>Statistics</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 BPPM

## Infobox

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object ID</td>
<td>PATROL internal identifier of the Process monitoring</td>
</tr>
<tr>
<td>Object Type</td>
<td>Type of the object (Process)</td>
</tr>
<tr>
<td>Object Class</td>
<td>Class of the object (SW_PROCESSES)</td>
</tr>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Process’ parent</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the Process’ root application</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 Process monitoring settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Polling Interval</td>
<td>Sets the polling interval for this instance</td>
</tr>
<tr>
<td>Set Alert Actions</td>
<td>Adds specific Alert Actions to the Process monitoring</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this Process monitoring object and all dependent objects</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this Process monitoring object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this Process monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the Process monitoring</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the Process monitoring 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 Process monitoring</td>
</tr>
<tr>
<td>Resume Monitoring</td>
<td>Resumes the Process monitoring</td>
</tr>
<tr>
<td>Refresh Parameters</td>
<td>Refreshes all instance parameters of the SW_PROCESSES class</td>
</tr>
</tbody>
</table>

SW_SENTRY

One single instance of the SW_SENTRY class is created and labeled Monitoring Studio. Once installed, it is the only visible icon under host icon in the PATROL Console. This icon gives you access to the various monitoring tools available in Monitoring Studio.

Monitoring objects will be placed under this Monitoring Studio icon by default. You can also use this icon to create new application/container icons in the PATROL Console tree.

Parameters

None.

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>
<tr>
<td>Website</td>
<td>Web site 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 &gt; Process Monitoring</strong></td>
<td>Starts the process monitoring wizard.</td>
</tr>
<tr>
<td><strong>New &gt; Windows Service Monitoring</strong></td>
<td>Starts the Windows service monitoring wizard.</td>
</tr>
<tr>
<td><strong>New &gt; File Monitoring and Analysis</strong></td>
<td>Starts the file monitoring and analysis wizard.</td>
</tr>
<tr>
<td><strong>New &gt; Folder Monitoring</strong></td>
<td>Starts the folder monitoring wizard</td>
</tr>
<tr>
<td><strong>New &gt; File System Monitoring</strong></td>
<td>Starts the file system monitoring wizard</td>
</tr>
<tr>
<td><strong>New &gt; Command Line Analysis</strong></td>
<td>Starts the command line execution and analysis wizard.</td>
</tr>
<tr>
<td><strong>New &gt; Database Query Analysis</strong></td>
<td>Starts the database query analysis wizard</td>
</tr>
<tr>
<td><strong>New &gt; Java MBean Polling (JMX)</strong></td>
<td>Starts the Java MBean polling wizard</td>
</tr>
<tr>
<td><strong>New &gt; Web Request Analysis</strong></td>
<td>Starts the Web request analysis wizard</td>
</tr>
<tr>
<td><strong>New &gt; Web-farm Monitoring</strong></td>
<td>Starts the Web-farm monitoring wizard</td>
</tr>
<tr>
<td><strong>New &gt; SNMP Polling</strong></td>
<td>Starts the SNMP polling wizard</td>
</tr>
<tr>
<td><strong>New &gt; SNMP Trap Listening</strong></td>
<td>Starts the SNMP trap listening wizard</td>
</tr>
<tr>
<td><strong>New &gt; WMI Query Analysis</strong></td>
<td>Starts the WMI query wizard</td>
</tr>
<tr>
<td><strong>New &gt; WBEMQuery Analysis</strong></td>
<td>Starts the WBEM query wizard</td>
</tr>
<tr>
<td><strong>New &gt; Windows Event Monitoring</strong></td>
<td>Starts the Windows EventLog monitoring wizard (On Windows Agents only)</td>
</tr>
<tr>
<td><strong>New &gt; Windows Performance Monitoring</strong></td>
<td>Starts the Windows Performance counter monitoring wizard (On Windows Agents only)</td>
</tr>
<tr>
<td><strong>New &gt; Multi-Parameter Formula</strong></td>
<td>Allows you to monitor any KM that is loaded in your PATROL Console by applying mathematical formulas to the collected values.</td>
</tr>
<tr>
<td><strong>New &gt; Application icon (container)</strong></td>
<td>Starts the new application/container icon wizard</td>
</tr>
<tr>
<td><strong>Trigger a KM Discovery</strong></td>
<td>Allows you to manually force a discovery</td>
</tr>
<tr>
<td><strong>Cut All</strong></td>
<td>Cuts all monitoring objects under this icon</td>
</tr>
<tr>
<td><strong>Copy All</strong></td>
<td>Copies all monitoring objects under this icon</td>
</tr>
<tr>
<td><strong>Paste</strong></td>
<td>Pastes the previously copied object under the Monitoring Studio icon</td>
</tr>
<tr>
<td><strong>Delete All</strong></td>
<td>Deletes all monitoring objects under this icon</td>
</tr>
<tr>
<td><strong>Tools &gt; Process Viewer</strong></td>
<td>Starts the process viewer tool</td>
</tr>
<tr>
<td><strong>Tools &gt; File Viewer</strong></td>
<td>Starts the file viewer tool</td>
</tr>
<tr>
<td><strong>Tools &gt; Windows EventLog Reader</strong></td>
<td>Starts the Windows EventLog Reader tool (On Windows Agents only)</td>
</tr>
<tr>
<td><strong>Tools &gt; SNMP Browser</strong></td>
<td>Starts the SNMP browser tool</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>Options &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>Options &gt; Thresholds Mechanism</strong></td>
<td>Shows the thresholds management options</td>
</tr>
</tbody>
</table>
**Options > Process Monitoring Credentials**
Allows you to specify the credentials to be used to run OS commands to collect process information.

**Options > Java Settings**
Enables you to define which Java instance is to be used by the KM.

**Options > Debug**
Shows the debug options

**Configuration > Export configuration**
Starts the Export configuration wizard

**Configuration > Import configuration**
Starts the Import configuration wizard

**Configuration > Report > Now**
Allows you to generate an instant report on the configuration of all monitored objects

**Configuration > Report > Schedule Report**
Allows you to schedule configuration reports for the monitored objects

**Configuration > Display Object Configuration**
Generates a report containing the object configuration

**Configuration > Display Entire Configuration**
Generates a report containing the entire object configuration

**About...**
Shows the version and general information about Monitoring Studio

---

**SW_SNMP_POLLING**

**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 Note: Only applicable to SNMP of String type.</td>
<td>--</td>
<td>None</td>
<td>--</td>
</tr>
<tr>
<td>Delta</td>
<td>Displays the difference between values collected during two consecutive polling</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>Status*</td>
<td>Status of the SNMP Polling. Value set by SNMPPollingColl {0 = OK ; 1 = Failed}</td>
<td></td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>Value*</td>
<td>Value of the SNMP received. Value set by SNMPPollingColl Note: Only applicable to SNMPs of integer type.</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 BPPM

**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>Parent ID</td>
<td>PATROL internal identifier of the SNMP Polling’s parent.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
Application ID | PATROL internal identifier of the SNMP Polling’s root application.
OID | OID that is polled.
OID type | Type of the value of the selected OID (number or string).
Host | Hostname where the SNMP agent is running.
Port | Port used to connect to the SNMP agent.
Community | Community used to connect to the SNMP agent.

### Menu Commands

| Menu Command | Description |
--- | ---
New > String Search | Creates a new String search for this SNMP Polling
New > Numeric Value Extraction | Creates a new Numeric Value search for this SNMP Polling
New > Dynamic Object Builder | Creates a new Dynamic Object Builder for this SNMP Polling
Edit | Edits the SNMP Polling settings
Set Thresholds | Allows you to set or edit the thresholds
Set Polling Interval | Sets the polling interval for this SNMP Polling
Set Alert Actions | Adds specific Alert Actions to the SNMP Polling
Display Object Configuration | Displays the Monitoring Studio configuration report of this SNMP Polling object and all dependent objects
Cut | Cuts this SNMP Polling object
Copy | Copies this SNMP Polling object
Paste | Pastes a previously copied or cut String search or Numeric Value search
Delete | Deletes the SNMP Polling and all its dependent objects
Rename | Renames the SNMP Polling object
Acknowledge Alerts | Acknowledges all alerts and reset parameters to zero
Pause Monitoring | Pauses the SNMP Polling as well as all its dependent objects
Resume Monitoring | Resumes the SNMP Polling as well as all its dependent objects
Refresh Parameters | Re-poll the OID and refresh all parameters. All dependent objects will be refreshed as well (SW_STRINGS and SW_NUMBERS instances)
SW_SNMP_TRAPS

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>MatchingTrap Count**</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>MatchingTrap Rate*</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 BPPM

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>Application ID</td>
<td>PATROL internal identifier of the SNMP Trap listening root application</td>
</tr>
<tr>
<td>Source IP</td>
<td>IP address of the SNMP agent that raises the traps</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>Number of the trap 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>
<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>Edit</td>
<td>Edits the SNMP Trap listening settings</td>
</tr>
</tbody>
</table>
### Menu Command |
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Set Thresholds</strong></td>
</tr>
<tr>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td><strong>Set Alert Actions</strong></td>
</tr>
<tr>
<td>Adds specific Alert Actions to the SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Display Object Configuration</strong></td>
</tr>
<tr>
<td>Displays the Monitoring Studio configuration report of this SNMP Trap object and all dependent objects</td>
</tr>
<tr>
<td><strong>Cut</strong></td>
</tr>
<tr>
<td>Cuts this SNMP Trap listening object</td>
</tr>
<tr>
<td><strong>Copy</strong></td>
</tr>
<tr>
<td>Copies this SNMP Trap listening object</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
</tr>
<tr>
<td>Deletes the SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
</tr>
<tr>
<td>Renames the SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Acknowledge all and reset</strong></td>
</tr>
<tr>
<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>
</tr>
<tr>
<td>Pauses the SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Resume Monitoring</strong></td>
</tr>
<tr>
<td>Resumes the SNMP Trap listening</td>
</tr>
<tr>
<td><strong>Refresh Parameters</strong></td>
</tr>
<tr>
<td>Refreshes all parameters of the SW_SNMP_TRAPS class</td>
</tr>
</tbody>
</table>

### SW_STRINGS

#### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</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;\MASAI\SENTRYB\LastMatchingLinesNumber&quot; with the proper line number to the PATROL Agent configuration. Default: the 10 last matching lines are displayed.</td>
</tr>
<tr>
<td>MatchingLineCount*</td>
<td>Number of lines matching the String search. Value set by the collector of the parent object</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</td>
</tr>
</tbody>
</table>

Parameters marked with an asterisk are used by default when visualizing the corresponding monitor instance in BPPM.

#### 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>Application ID</td>
<td>PATROL internal identifier of the String search's root application</td>
</tr>
</tbody>
</table>
### Application Classes

#### Monitoring Studio KM for PATROL

**Version 8.6.54**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent type</td>
<td>Type of the parent (File, OSCommand, 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>When Alert Actions have to be executed</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 String search settings</td>
</tr>
<tr>
<td>Set Thresholds</td>
<td>Allows you to set or edit the thresholds</td>
</tr>
<tr>
<td>Set Alert Actions</td>
<td>Adds specific Alert Actions to the String search</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this String search object and all dependent objects</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this String search object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this String search object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the String search</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the String search object</td>
</tr>
<tr>
<td>Acknowledge all and reset</td>
<td>Acknowledge all alerts for this object. The MatchingLineCount parameter is set to zero</td>
</tr>
<tr>
<td>Pause monitoring</td>
<td>Pauses the String search</td>
</tr>
<tr>
<td>Resume monitoring</td>
<td>Resumes the String search</td>
</tr>
</tbody>
</table>

### SW_Transform

#### 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>
</tbody>
</table>
### Application Classes

#### Monitoring Studio KM for PATROL

**Version 8.6.54**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent ID</td>
<td>PATROL internal identifier of the Text Pre-processing object’s parent</td>
</tr>
<tr>
<td>Application ID</td>
<td>PATROL internal identifier of the Text Pre-processing object’s root application</td>
</tr>
<tr>
<td>Parent type</td>
<td>Type of the parent (File, OS Command, etc.)</td>
</tr>
</tbody>
</table>

### Menu Commands

#### SW_WBEM

#### 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>QueryStatus *</td>
<td>Displays whether or not the query was successfully executed. Value set by WBEMQueryColl every 2 minutes</td>
<td>{0 = Successful ; 1 = Execution failed}</td>
<td>Alarm = 1</td>
<td>Availability</td>
</tr>
<tr>
<td>ReturnOutput</td>
<td>Displays the output of the WBEM query execution. Value set by WBEMQueryColl every 2 minutes</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 BPPM
### 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>Application ID</td>
<td>PATROL internal identifier of the WBEM query object’s root application</td>
</tr>
<tr>
<td>Host</td>
<td>Displays name of host machine</td>
</tr>
<tr>
<td>Name Space</td>
<td>Displays WBEM namespace</td>
</tr>
<tr>
<td>WBEM Query</td>
<td>Displays the 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 File</td>
</tr>
<tr>
<td>New &gt; Numeric value extraction</td>
<td>Creates a new Numeric Value extraction for this File</td>
</tr>
<tr>
<td>New &gt; Dynamic Object Builder</td>
<td>Creates a new Dynamic Object Builder for this File</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the WBEM monitoring settings</td>
</tr>
<tr>
<td>Display Object Configuration</td>
<td>Displays the Monitoring Studio configuration report of this monitoring object and all dependent objects</td>
</tr>
<tr>
<td>Cut</td>
<td>Cuts this WBEM monitoring object</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies this WBEM monitoring object</td>
</tr>
<tr>
<td>Paste</td>
<td>Pastes this WBEM monitoring object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the WBEM monitoring</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the WBEM monitoring object</td>
</tr>
<tr>
<td>Pause monitoring</td>
<td>Pauses the WBEM monitoring</td>
</tr>
<tr>
<td>Resume monitoring</td>
<td>Resumes the WBEM monitoring</td>
</tr>
</tbody>
</table>
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).

Tip: The naming of processes is highly platform dependant. 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 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>
</table>

336
<table>
<thead>
<tr>
<th>Name</th>
<th>Unique name of the service.</th>
</tr>
</thead>
<tbody>
<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.
HTTP Authentication
Starting with version 8.5.00, Monitoring Studio supports 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 on Hotmail or Yahoo mail or any public webmail service.

There are 3 different HTTP authentication schemes, depending on the machine where Monitoring Studio 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 on a Windows system and set up the Web requests from this machine (Web requests can be sent to remote systems)
Managing Baselines and KPI
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 baseline 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](image)
- ![KPI](image)
Index

- A -

Abnormalities 342
About
  Process 332
  WMI 335
AccessRights
  File 68
Acknowledge
  Alerts 258, 259
  All 259
Acknowledgement
  Automatic 162, 166, 181, 280
  Configuration 166
Administration
  Features 258
Advanced Options 239
Advanced Settings
  Configure 236
Alarm
  Trigger 192
Alert
  Actions 211
Alert Actions
  Annotate the parameter's graph 217
  Capabilities 217
  Customize 217
  Do not trigger any alert 207
  Example 231
  Execute an OS command 217
  Macros 227
  Send a basic SNMP trap 217
  Send a custom SNMP trap 217
  Send a pop-up to the PATROL consoles 217
  Send an E-mail 217
  Trigger a PATROL event 217
  Trigger a WARNING 207
  Trigger an ALARM 207
  Trigger an INFORMATION 207
  Write a line to a LOG file 217
Alert Thresholds
  Modify 207
Set 206, 207
Alerts
  Acknowledge 258, 259
  Do not trigger any alert 211
  Trigger a WARNING 211
  Trigger an ALARM 211
  Trigger an INFORMATION 211
  Update 259
Analysis
  Command Line 82
  Database Query 88
  LOG file 181
  WBEM Query 115
  WMI Query 118
Application 45
  Constants 45
  Create 45
  Edit 45
  Restart 268
  Stop 271
Application Classes 107, 293
  List 294
  SW_APPLICATIONS 295
  SW_DB_QUERIES 297
  SW_DYNAMIC 299
  SW_DYNAMIC_CONTAINER 299
  SW_DYNAMIC_DISCOVERY 300
  SW_DYNAMIC_NUMBERS 301
  SW_DYNAMIC_STRINGS 302
  SW_FILE_SECURITY 305
  SW_FILES 302
  SW_FILESYSTEMS 304
  SW_FOLDERS 62, 306
  SW_HTTP_REQUESTS 107, 112, 308
  SW_HTTP_WEBFARM 107, 309
  SW_JMX 124, 130, 136, 142, 150, 310
  SW_KMWATCH 75, 312
  SW_NT_WMI 118, 316
  SW_NT_EVENTS 166, 313
  SW_NT_PERFORMANCE 78, 314
  SW_NT_SERVICES 315
  SW_NUMBERS 185, 318
  SW_OSCOMMANDS 319
  SW_PROCESSES 49, 269, 321
  SW_SENTRY 269, 322
  SW_SNMP_POLLING 158, 324
  SW_SNMP_TRAPS 326
  SW_STRINGS 327
  SW_Transform 328
Application Classes 107, 293
  SW_WBEM 115, 329
Authentication
  HTTP 340
Automatic
  Acknowledgement 162, 166, 181, 280

- B -
Baselines 293
  BMC ProactiveNet Performance Management 342
  Generation 342
  Manage 342
  Requirements 342
BEA WebLogic 121
BMC
  BMC Installation Utility 18
  BMC Performance Manager 41
  BMC Performance Manager Monitoring Studio 34
  BMC Portal 41
  BMC Software Installation utility 18
BMC ProactiveNet Performance Management
  Abnormalities 342
  Baselines 342
  Key Performance Indicators 342
  KPI 342
Builder
  Dynamic Object 192

- C -
Changes 10
Check
  File Security 68
CIM 115, 118
  CIM contains 335
  CIM Repository 335
  CIM stands 335
  CIM_DataFile 335
Class
  CIM_DataFile 335
  Win32_ComputerSystem 335
  Win32_Process 335
Collectors
  Common 269
  Column Separator
  Blank 181, 185
  Comma 181, 185
  Point 181, 185
  Command 316
  Acknowledge Alerts 297
  Copy 297
  Cut 297
  Delete 297
  Display Object Configuration 297
  Dynamic Object Builder 297
  Edit 297
  External 171
  Numeric Value Extraction 297
  Paste 297
  Pause monitoring 297
  Refresh Parameters 297
  Rename 297
  Resume monitoring 297
  Set Alert actions 297
  Set Polling Interval 297
  Set Thresholds 297
  String search 297
  Text Pre-Processing 297
Command Execution
  Never ending 82
Command Line 88, 93, 96, 100, 104, 105, 332
  Analysis 82
Commands
  About 322
  Acknowledge all and reset 313, 326, 327
  Acknowledge and Update 305
  Add hosts 309
  Application icon (container) 322
  awk 292
  Command Line Analysis 295, 322
Configuration 322
  Copy 295, 300, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327, 328, 329
  Copy All 322
  Cut 295, 300, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327, 328, 329
  Cut All 322
  Database Query Analysis 295, 322
  Debug 322
Index

Monitoring Studio KM for PATROL
Version 8.6.54

Commands
Delete 295, 300, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327, 328, 329
Delete All 322
Discovery Interval 322
Display Entire Configuration 322
Display Object Configuration 295, 300, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 322, 324, 326, 327, 328, 329
Dynamic Object Builder 302, 308, 310, 316, 319, 324, 328, 329
Edit 295, 300, 302, 304, 305, 306, 308, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327, 328, 329
Export configuration 295, 322
File Monitoring and Analysis 295, 322
File Security Check 302
File System Monitoring 295, 322
File Viewer 322
Folder Monitoring 295, 322
grep 292
Import configuration 322
Java MBean Polling (JMX) 295, 322
Java Settings 322
Manage 295
Modify Application constants 295
Multi-Parameter Formula 295, 322
New 295, 300, 302, 308, 309, 310, 316, 319, 322, 324, 328, 329
Now 322
Numeric value extraction 302, 308, 309, 310, 316, 319, 324, 328, 329
Numeric Value Extraction Template 300
Options 322
Paste 295, 300, 302, 308, 309, 310, 316, 319, 322, 324, 328, 329
Pause monitoring 295, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327, 328, 329
Process Monitoring 295, 322
Process Monitoring Credentials 322
Process Viewer 322
Real-time SNMP Trap listener 322
Refresh Parameters 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 319, 321, 324, 326
Remove Missing Items 300
Rename 295, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327, 328, 329
Report 322
Restart scan from start of file 302
Resume monitoring 295, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327, 328, 329
Schedule Report 322
sed 292
Set Alert Actions 300, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327
Set Global Alert Actions 295
Set Polling Intervals 312
Set Thresholds 302, 304, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327
SNMP Browser 322
SNMP Polling 295, 322
SNMP Trap Listening 295, 322
Start Application 295
Stop Application 295
String search 302, 308, 309, 310, 316, 319, 324, 328, 329
String Search Template 300
Sub-container 295
Text Pre-Processing 302, 308, 309, 310, 316, 319, 324, 328, 329
Thresholds Mechanism Selection 322
Tools 322
Trigger a KM Discovery 322
View file content 302
WBEM Query analysis 295
WBEMquery Analysis 322
Web Request Analysis 295, 322
Web-farm Monitoring 295, 322
Windows Event Monitoring 295, 322
Windows EventLog Reader 322
Windows Performance Monitoring 295, 322
Windows Service Monitoring 295, 322
WMI Query Analysis 295, 322
Community 158
Configuration
Automatic Acknowledgement 166
Export 241
Configuration
  Import 245
  Monitoring Studio 241
Configuration Report
  Schedule 251, 252
Configure
  Advanced Settings 236
Connection 104
  Database 93, 96, 100, 104, 105
  Information 88
  JDBC 93, 96, 100, 104, 105
  Method 88
  ODBC 93, 96, 100, 104
  Settings 93, 96, 100, 104, 105
  String 104
Connection Information
  Host 130, 136, 142, 150
  Initial context factory 130, 136, 142
  JNDI 142
  KeyStore password 150
  KeyStoreFile path 150
  Node name 150
  org.jboss.naming:org.jnp.interfaces 130
  org.jnp.interfaces.NamingContextFactory 130
  Port 130, 136, 142
  Protocol 136
  Server name 136, 142, 150
  SOAP Port 150
  TrustStore password 150
  TrustStoreFile path 150
  URL package prefixes 130, 136
  weblogic.jndi.WLInitialContextFactory 142
  weblogic.management.mbeanservers.domai
  nruntime 142
Console system
  Requirements 17
Content
  View 275
Copy
  Monitoring Tools 263
Create
  Application 45
  Command Line 82
  Database Query Analysis 88
  Dynamic Object 192
  File security monitoring 68
  File System Monitoring 61
  Folder Monitoring 62
  Multi-Parameter Formula 75
  Numeric Value Search 185
  Process Monitoring 49
  SNMP polling 158
  String Search 181
  Text Preprocessing object 171
  WBEM Query Analysis 115
  Web Request Analysis 112
  Web-farm Monitoring 107
  Windows event monitoring 166
  Windows Performance Monitoring 78
  Windows Service Monitoring 58
  WMI Query Analysis 118
Credential Files
  ClientKeyFile.jks 150
  ClientTrustFile.jks 150
Credentials 124
  Connection timeout period 130, 136, 142
  Path to Java on the local server 130, 136, 142
  Principle 130, 136, 142
  Process Command 50
Criteria 49
Cut
  Monitoring Tools 263

- D -

Database
  Connection 104
  Microsoft SQL 88
  Microsoft SQL Server 93
  MySQL 88
  MySQL Server 96
  Oracle 88, 100
  Other 104
  Postgre SQL 88
  PostgreSQL 105
  Settings 104
Database Macros
  %{DATABASE_NAME} 227
  %{DATABASE_QUERY} 227
  %{DATABASE_RETURN_OUTPUT} 227
  %{DATABASE_TYPE} 227
  %{SW_PASSWORD} 227
  %{SW_USERNAME} 227
Database Query
  Analysis 88
Debug Mode
  Enable 278
Delete
  Monitored Object 276
Discovery
  Trigger 271
Discovery Interval
  Set 269
Display
  Entire Configuration 250
  Object Configuration 250
DMTF 115
Download 283
Dynamic Numeric Value Extractions 211
Dynamic Object 211
  Builder 192
Dynamic Object Builder 192
Dynamic Objects Macros
  %{DYNAMIC_RETURN_OUTPUT} 227

- E -

Edit
  Application 45
  Command Line 82
  Database Query Analysis 88
  Dynamic Object 192
  File security monitoring 68
  File System Monitoring 61
  Folder Monitoring 62
  Instance 264
  Monitored Object 264
  Multi-Parameter Formula 75
  Numeric Value Search 185
  Process Monitoring 49
  SNMP polling 158
  String Search 181
  Text Preprocessing object 171
  WBEM Query Analysis 115
  Web Request Analysis 112
  Windows event monitoring 166
  Windows Performance Monitoring 78
  Windows Service Monitoring 58
  WMI Query Analysis 118
Enable
  Debug Mode 278
Entire Configuration
  Display 250
Event ID 288
Example 49, 82, 166, 171, 207
  Alert Actions 231
Execute
  OS Command 217
  PSL command 217
Execution
  Period 82
  Timeout 82
Export
  Configuration 241
Extract
  Numeric Values 211
  Setup Files 19
  Text from HTML 171
Extraction
  Numeric Value 185

- F -

FAQ
  Although SNMP Trap listening seems to work, no trap matches my criteria 279
  Can I monitor the processor time usage made by a Windows service? 279
  Can I search for Windows Events whose description match a regular expression? 279
  Difference between a flat file and a LOG file 280
  How do I know which version of Monitoring Studio I am running? 282
  I'm unable to connect to the WebLogic application server 283
  I'm unable to connect to the WebSphere application server 283
  I'm unable to poll an SNMP agent (getting a Warning) 283
  I'm unable to see the Monitoring Studio icons in PATROL Central 284
  Infinite loop reported in the PATROL Agent log 284
  Is it possible to monitor the CPU/memory usage of a process tree? 285
  Monitoring Studio does not follow an HTTP redirection (Web) 287
  Monitoring Studio does not read the content of my file 285
  Monitoring Studio does not update all of my folder monitoring parameters 285
FAQ
  Monitoring Studio fails to authenticate on my Web server 286
  Monitoring Studio fails to connect to a secured Web server (SSL) on my UNIX/Linux server 286
  Monitoring Studio fails to connect to my Oracle Database server 286
  Monitoring Studio fails to connect to my remote Microsoft SQL Server 286
  Monitoring Studio is unable to listen to SNMP traps 287
  Monitoring Studio reads my LOG file entirely 287
  Not able to post a Web form to my Web server 288
  What is the meaning of the "Argument 1, 2..." fields in the Windows Event monitoring wizard? 288
Features
  Administration 258
File
  Access rights 68
  Flat 65, 280, 287
  Growth 65
  LOG 65, 280, 287
  Monitor 197
  Monitoring 65
  PID 332
  Presence 65
  Size 65
  tnsnames.ora 286
File Content
  View 275
File Macro
  %FILE_CURRENT_NAME 227
  %FILE_NAME 227
  %SW_PASSWORD 227
  %SW_USERNAME 227
File Security
  Check 68
File System
  Monitoring 61
File System Macro
  %FILESYSTEM_NAME 227
Files
  FLAT 285
  LOG 285
  PID 49
  Signature 45

Flat
  File 287
  Sources 280
FLAT File
  Monitoring 65
Folder
  Monitoring 62
Folder Macro
  %FOLDER OLDEST REMAINING_FILE 227
  %FOLDER_PATH 227
Folder Monitoring
  Create 62
  Edit 62
Format Symbols
  \% 290
  \%a 290
  \%b 290
  \%c 290
  \%d 290
  \%e 290
  \%Ec 290
  \%Ex 290
  \%Ey 290
  \%h 290
  \%I 290
  \%j 290
  \%k 290
  \%l 290
  \%m 290
  \%n 290
  \%Od 290
  \%Oe 290
  \%OH 290
  \%OI 290
  \%Om 290
  \%OS 290
  \%OU 290
  \%Ow 290
  \%Oy 290
  \%p 290
  \%r 290
  \%S 290
  \%t 290
  \%u 290
  \%V 290
  \%w 290
  \%x 290
  \%y 290
Index

Format Symbols
  %Z  290
Formula
    Multi-Parameter  75

- G -
Generate
  Baselines  342
Generic JMX client  121
Getting Started  15
Global
  Settings  245
Growth
  Size  65

- H -
Host  158
  Identify  115, 118
HTTP
  Authentication  107, 112, 340
  Request  107, 112
HTTP authentication schemes
  Basic  107, 112
  Digest  107, 112
  NTLM  107, 112
HTTP Macros
  %{HTTP_METHOD}  227
  %{HTTP_RETURN_OUTPUT}  227
  %{HTTP_URL}  227

- I -
IBM WebSphere  121
Icons
  Application  45
  Container  45
Identify
  Host  115, 118
  Process  332
Import
  Configuration  245
Improvements  10
Infobox  282
  Acknowledge  313, 327
  Acknowledging OID 1  326
Acknowledging OID 2  326
Acknowledging String  327
Acknowledging String 1  326
Acknowledging String 2  326
Acknowledging Trap Number  326
Acknowledging Windows Event  313
After/Before  301, 318
Application ID  295, 297, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327, 328, 329
Attribute  310
Character Offset  301, 318
Column Mode  301, 318
Column Separators  300
Community  324, 326
Connect as  297
Connection Type  297
Consecutive Separators  300
Constant 1  295
Constant 2  295
Constant 3  295
Constant 4  295
Constant 5  295
Contact  295
Copyright  322
Counter  314
Database name  297
Database Type  297
Description  295
Domain  310
Dynamic Object Display Name  300
Dynamic Object ID  300
Enterprise ID  326
Event ID  313
Event log  313
Event source  313
Exclude Object Matching  300
Field Number  301, 318
Field Separators  301, 318
File Name & Path  302
File System Object  304
File Type  302
First required file  295
Folder  306
Formula  312
Fourth required file  295
Host  310, 316, 324, 329
Hostname  297
**Index**

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infobox</td>
<td>282</td>
</tr>
<tr>
<td>ID</td>
<td>295, 297, 299, 300, 301, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 324, 326, 327, 328, 329</td>
</tr>
<tr>
<td>Include Object Matching</td>
<td>300</td>
</tr>
<tr>
<td>Include subfolders</td>
<td>306</td>
</tr>
<tr>
<td>Instances</td>
<td>314</td>
</tr>
<tr>
<td>Key Property</td>
<td>310</td>
</tr>
<tr>
<td>Line Mode</td>
<td>301, 318</td>
</tr>
<tr>
<td>Line Number</td>
<td>301</td>
</tr>
<tr>
<td>Line Numbers</td>
<td>318</td>
</tr>
<tr>
<td>Lines</td>
<td>302, 327</td>
</tr>
<tr>
<td>Monitored File</td>
<td>302</td>
</tr>
<tr>
<td>Monitored Parameters</td>
<td>302</td>
</tr>
<tr>
<td>Name Space</td>
<td>316, 329</td>
</tr>
<tr>
<td>Object Class</td>
<td>321</td>
</tr>
<tr>
<td>Object ID</td>
<td>321</td>
</tr>
<tr>
<td>Object Type</td>
<td>321</td>
</tr>
<tr>
<td>OID</td>
<td>324</td>
</tr>
<tr>
<td>OID 1</td>
<td>326</td>
</tr>
<tr>
<td>OID 2</td>
<td>326</td>
</tr>
<tr>
<td>OID type</td>
<td>324</td>
</tr>
<tr>
<td>OS Command</td>
<td>319</td>
</tr>
<tr>
<td>Parameter Type</td>
<td>301, 318</td>
</tr>
<tr>
<td>Parent ID</td>
<td>295, 297, 300, 301, 302, 304, 305, 306, 308, 309, 310, 312, 313, 314, 315, 316, 318, 319, 321, 324, 326, 327, 328, 329</td>
</tr>
<tr>
<td>Parent type</td>
<td>318, 327, 328</td>
</tr>
<tr>
<td>Path to java</td>
<td>310</td>
</tr>
<tr>
<td>Performance object</td>
<td>314</td>
</tr>
<tr>
<td>Port</td>
<td>310, 324</td>
</tr>
<tr>
<td>Product</td>
<td>322</td>
</tr>
<tr>
<td>Regular Expression</td>
<td>301, 318</td>
</tr>
<tr>
<td>Release Date</td>
<td>322</td>
</tr>
<tr>
<td>Run Alert Actions</td>
<td>302, 313, 326, 327</td>
</tr>
<tr>
<td>Scale</td>
<td>314</td>
</tr>
<tr>
<td>Scan mode</td>
<td>302</td>
</tr>
<tr>
<td>Search</td>
<td>327</td>
</tr>
<tr>
<td>Second required file</td>
<td>295</td>
</tr>
<tr>
<td>Server type</td>
<td>310</td>
</tr>
<tr>
<td>Service name</td>
<td>315</td>
</tr>
<tr>
<td>Skip Blank Lines</td>
<td>301, 318</td>
</tr>
<tr>
<td>Source IP</td>
<td>326</td>
</tr>
<tr>
<td>Specified String</td>
<td>301, 318</td>
</tr>
<tr>
<td>SQL Query</td>
<td>297</td>
</tr>
<tr>
<td>Start command line</td>
<td>295</td>
</tr>
<tr>
<td>Stop command line</td>
<td>295</td>
</tr>
<tr>
<td>String 1</td>
<td>326</td>
</tr>
<tr>
<td>String 2</td>
<td>326</td>
</tr>
<tr>
<td>Support</td>
<td>322</td>
</tr>
<tr>
<td>Third required file</td>
<td>295</td>
</tr>
<tr>
<td>Timeout</td>
<td>310, 313, 319, 326, 327</td>
</tr>
<tr>
<td>Trap number</td>
<td>326</td>
</tr>
<tr>
<td>Type</td>
<td>300, 302</td>
</tr>
<tr>
<td>Unique Separator</td>
<td>301, 318</td>
</tr>
<tr>
<td>Used HTTP method</td>
<td>308</td>
</tr>
<tr>
<td>Username</td>
<td>310, 316, 319, 329</td>
</tr>
<tr>
<td>Value Type</td>
<td>314</td>
</tr>
<tr>
<td>Variable</td>
<td>312</td>
</tr>
<tr>
<td>Version</td>
<td>322</td>
</tr>
<tr>
<td>WBEM Query</td>
<td>329</td>
</tr>
<tr>
<td>Website</td>
<td>322</td>
</tr>
<tr>
<td>WMI Query</td>
<td>316</td>
</tr>
<tr>
<td>Input Variables</td>
<td>283</td>
</tr>
<tr>
<td>Installation</td>
<td>21</td>
</tr>
<tr>
<td>BMC Software Installation utility</td>
<td>18</td>
</tr>
<tr>
<td>Packages</td>
<td>18</td>
</tr>
<tr>
<td>Procedure</td>
<td>21</td>
</tr>
<tr>
<td>Setup Files</td>
<td>19</td>
</tr>
<tr>
<td>Utility</td>
<td>18</td>
</tr>
<tr>
<td>Instance</td>
<td></td>
</tr>
<tr>
<td>Display Name</td>
<td>335</td>
</tr>
<tr>
<td>Edit</td>
<td>264</td>
</tr>
<tr>
<td>Name</td>
<td>335</td>
</tr>
<tr>
<td>PathName</td>
<td>335</td>
</tr>
<tr>
<td>StartMode</td>
<td>335</td>
</tr>
<tr>
<td>State</td>
<td>335</td>
</tr>
<tr>
<td>Integration</td>
<td>41</td>
</tr>
<tr>
<td>BMC Portal</td>
<td>41</td>
</tr>
<tr>
<td>Overview</td>
<td>41</td>
</tr>
<tr>
<td>Issues</td>
<td>41</td>
</tr>
<tr>
<td>Fixed</td>
<td>10</td>
</tr>
<tr>
<td>Known</td>
<td>10</td>
</tr>
<tr>
<td>Overloaded Application</td>
<td>62</td>
</tr>
<tr>
<td><strong>- J -</strong></td>
<td></td>
</tr>
<tr>
<td>Java</td>
<td>18</td>
</tr>
<tr>
<td>Automatic Detection</td>
<td>260</td>
</tr>
<tr>
<td>IBM JVM</td>
<td>283</td>
</tr>
<tr>
<td>Java MBean Polling</td>
<td>121</td>
</tr>
<tr>
<td>JDK v1.4</td>
<td>283</td>
</tr>
<tr>
<td>JDK v1.5</td>
<td>283</td>
</tr>
<tr>
<td>JMX</td>
<td>121</td>
</tr>
<tr>
<td>JVM v1.4</td>
<td>283</td>
</tr>
<tr>
<td>JVM v1.5</td>
<td>283</td>
</tr>
<tr>
<td>Manual</td>
<td>260</td>
</tr>
</tbody>
</table>
Index

Java 18
  Settings 260
  Sun JVM 1.5 283
  User Selection 260
JBoss 121
  Attribute 130
  Domain 130
  key property 130
JDBC 88
  Connection 93, 96, 100, 104, 105
  Settings 93, 96, 100, 104, 105
JMX
  Agent 121
  Architecture 121
  Generic JMX client 124
  ManagementFactory 121
  MBean ServerConnection 121
  MBeans 121
  MBeanServer 121
  MXBean Proxy 121
  Probe 121
JMX Application Server
  BEA WebLogic 156
  Generic JMX applications 156
  IBM WebSphere 156
  JBoss by Redhat 156
  JOnAS 156
JMX Macros
  %{JMXPOLLING_ATTRIBUTE} 227
  %{JMXPOLLING_CONTENT} 227
  %{JMXPOLLING_DOMAIN} 227
  %{JMXPOLLING_HOST} 227
  %{JMXPOLLING_KEY_PROPERTY} 227
  %{JMXPOLLING_PORT} 227
  %{JMXPOLLING_SERVER_TYPE} 227
  %{SW_PASSWORD} 227
  %{SW_USERNAME} 227
JOnAs 121
  Attribute 136
  Connection information 136
  Credentials 136
  Domain 136
  Key property 136
JRe 18

- K -
  Key Performance Indicators

BMC ProactiveNet Performance Management 342
  Manage 342
KM Discovery
  Trigger 271
KPI 293
  BMC ProactiveNet Performance Management 342
  Manage 342

- L -
  Lines
    Numeric Value 185
    Select 181
  Listening
    SNMP Trap 162
  Location
    Numeric Value 185
LOG
  File 231, 287
LOG File
  Analysis 181
  Monitoring 65

- M -
  Macros 82
    %{/...} 227
    %{ALARM_TYPE} 227
    %{ALARM1_MAX} 227
    %{ALARM1_MIN} 227
    %{ALARM1_NTIMES} 227
    %{ALARM1_TYPE} 227
    %{ALARM2_MAX} 227
    %{ALARM2_MIN} 227
    %{ALARM2_NTIMES} 227
    %{ALARM2_TYPE} 227
    %{APPLICATION_CLASS} 227
    %{APPLICATION_CONTACT} 227
    %{APPLICATION_DESCRIPTION} 227
    %{APPLICATIONEXISTENCEFILES} 227
    %{APPLICATION_ID} 227
    %{APPLICATION_LABEL} 227
    %{APPLICATION_TYPE} 227
    %{ASCTIME:...} 227, 290
    %{BORDER_MAX} 227
    %{BORDER_MIN} 227
Monitoring Studio KM for PATROL
Version 8.6.54

Macros 82
  {BORDER_NTIMES} 227
  {BORDER_TYPE} 227
  {NEWLINE} 227
  {OBJECT_CLASS} 227
  {OBJECT_ID} 227
  {OBJECT_LABEL} 227
  {OBJECT_TYPE} 227
  {PARAMETER_NAME} 227
  {PARENT_<_PARENT_MACRO>} 227
  {PARENT_CLASS} 227
  {PARENT_ID} 227
  {PARENT_LABEL} 227
  {PARENT_TYPE} 227
  {VALUE} 227
  Alert Actions 227

Manage
  Baselines 342
  Key Performance Indicators 342
  KPI 342
  Thresholds 206

Managed Systems
  Requirements 17

Measure 62
  Method 45
    Get 107, 112
    Post 107, 112

MIB
  Management Information Base 158

Microsoft SQL Server Database
  Connection 93
  Settings 93

Modify
  Alert Thresholds 207
  Object ID 264
  Object Name 264

Monitor
  Application 45
  File 197
  LOG File 231
  Security Parameters 68

Monitored Object
  Delete 276
  Monitoring 265
    File 65
    File System 61
    Folder 62
    Pause 265
    Process 49
    Start 237
    Stop 237
    Suspend 265
    Web-farm 107
    Windows Event 166
    Windows Event log 166
    Windows Performance 78
    Windows Service 58

Monitoring Features
  Command Line Analysis 192
  Database Query Analysis 192
  File Monitoring and Analysis 192
  Java MBean Polling 192
  SNMP Polling 192
  Text Pre-Processing 192
  WBEM Query Analysis 192
  Web Request Analysis 192
  WMI Query Analysis 192

Monitoring Studio 121
  Configuration 241
  Settings 45, 49, 58, 61, 62, 78, 82, 88, 107, 115, 118, 130, 136, 142, 150, 158, 162, 166, 171, 181, 185

Monitoring Tools
  Copy 263
  Cut 263
  Paste 263

Move
  Monitoring Tools 263

MPF Macros
  {MPF_CLASS} 227
  {MPF_FORMULA} 227
  {MPF_ID} 227

Multi-Parameter
  Formula 75

MySQL Server Database
  Connection 96
  Settings 96

- N -

Namespace 335
  New 10

Numeric Value
  Extraction 185
  Lines 185
  Location 185
  Search 185
- O -

Object
   Edit 264
   Rename 266
Object Configuration
   Display 250
Object Specific Macros
   \%{DATABASE_NAME} 227
   \%{DATABASE_QUERY} 227
   \%{DATABASE_TYPE} 227
   \%{DYNAMIC_RETURN_OUTPUT} 227
   \%{FILE_CURRENT_NAME} 227
   \%{FILE_NAME} 227
   \%{FILESYSTEM_NAME} 227
   \%{FOLDER_OLEDEST_REMAINING_FILE} 227
   \%{FOLDER_PATH} 227
   \%{HTTP_METHOD} 227
   \%{HTTP_RETURN_OUTPUT} 227
   \%{HTTP_URL} 227
   \%{JMXPOLLING_ATTRIBUTE} 227
   \%{JMXPOLLING_CONTENT} 227
   \%{JMXPOLLING_DOMAIN} 227
   \%{JMXPOLLING_HOST} 227
   \%{JMXPOLLING_KEY_PROPERTY} 227
   \%{JMXPOLLING_PORT} 227
   \%{JMXPOLLING_SERVER_TYPE} 227
   \%{KMWATCH_CLASS} 227
   \%{KMWATCH_ID} 227
   \%{KMWATCH_PARAMETER} 227
   \%{MPF_CLASS} 227
   \%{MPF_FORMULA} 227
   \%{MPF_ID} 227
   \%{NTEVENT_ID} 227
   \%{NTEVENT_LAST_MATCHING_CONTENT} 227
   \%{NTEVENT_LAST_MATCHING} 227
   \%{NTEVENT_LOG} 227
   \%{NTEVENT_SOURCE} 227
   \%{OSCOMMAND_OSCOMMAND} 227
   \%{OSCOMMAND_RETURN_OUTPUT} 227
   \%{PERFORMANCE_COUNTER} 227
   \%{PERFORMANCE_INSTANCLIST} 227
   \%{PERFORMANCE_PERFORMANCE} 227
   \%{PROCESS_COMMAND_LINE} 227
   \%{PROCESS_NAME} 227
   \%{PROCESS_PID_FILE} 227
   \%{PROCESS_USER_ID} 227
   \%{SERVICE_NAME} 227
   \%{SNMPPOLLING_COMMUNITY} 227
   \%{SNMPPOLLING_CONTENT} 227
   \%{SNMPPOLLING_HOST} 227
   \%{SNMPPOLLING_OID} 227
   \%{SNMPPOLLING_PORT} 227
   \%{SNMPTRAP_COMMUNITY} 227
   \%{SNMPTRAP_CONTENT} 227
   \%{SNMPTRAP.EnterpriseID} 227
   \%{SNMPTRAP_FOUNDTRAPNUMBER} 227
   \%{SNMPTRAP_IP} 227
   \%{SNMPTRAP_TRAPNUMBER} 227
   \%{STRING_LAST_MATCHING_LINE} 227
   \%{STRING.SEARCHED_1} 227
   \%{STRING.SEARCHED_2} 227
   \%{WBEM_HOST} 227
   \%{WBEM_NAME_SPACE} 227
   \%{WBEM_QUERY} 227
   \%{WBEM_RETURN_OUTPUT} 227
   \%{WBEM_USERNAME} 227
   \%{WMI_HOST} 227
   \%{WMI_NAME_SPACE} 227
   \%{WMI_QUERY} 227
   \%{WMI_USERNAME} 227
   ODBC 88
      Connection 93, 96, 100, 104
      Settings 93, 96, 100, 104
Option
   Rescaling 185
Options 45
      Advanced 45
      Start-Stop 45
Oracle
   Oracle SID 100
   Oracle system identifier 100
Oracle Database
   Connection 100
   Settings 100
OS Command
   Execute 217
   Specify 171
OS Command Macros
   \%{OSCOMMAND.EXIT_STATUS_CODE} 227
OS Command Macros

%{OSCOMMAND_OSCOMMAND} 227
%{OSCOMMAND_RETURN_OUTPUT} 227
%{SW_PASSWORD} 227
%{SW_USERNAME} 227

Output format

CSV 252
Plain English 252
XML 252

- P -

Packages

Download 18

Parameters 166

AccessRightsCheck 305
ChildCount 49, 285, 321
ConnectionStatus 88, 297
Content 324
Count 49, 321
DeletedFileCount 62, 306
Delta 124, 130, 136, 142, 150, 158, 301, 310, 318, 324
DeltaPerSecond 124, 130, 136, 142, 150, 158, 301, 310, 318, 324
Discard negative Delta values 158
ExecutionStatus 124, 310, 319
ExecutionTime 297, 308, 319
Exists 302
ExitStatus 319
ExtractedLine 299
FileCount 62, 306
FolderSize 62, 306
FreeMegabytes 61, 304
FreeSpacePercent 61, 304
GroupCheck 305
GrowthPercentage 62, 302, 306
GrowthSpeed 62, 302, 306
HandleCount 49, 321
HTTPStatusCode 308
Integrity 305
LastChanged 302
LastMatchingLines 327
LastModifiedFileElapsedTime 62, 306
LongestTimeFileRemainsInFolder 62, 306
MatchingEventCount 166, 313
MatchingEventRate 166, 313
MatchingLineCount 181, 231, 280, 302, 327

MatchingLineRate 327
MatchingTrapCount 162, 326
MatchingTrapRate 326
ModifiedFileCount 62, 306
Monitor 68
NewFileCount 62, 306
OldestModifiedFileElapsedTime 62, 306
OperationServerPercent 309
OperationServerCount 309
OwnerCheck 305
PageFaultsPerSec 49, 321
PageFileBytes 49, 321
PrivateBytes 49, 321
ProcessorTime 49, 321
QueryStatus 115, 118, 297, 316, 329
Refresh 265
ReturnOutput 107, 115, 118, 297, 308, 316, 319, 329
Security 68
Select 49, 158, 185
ServerConnectionState 107, 112, 308
Size 302
Status 192, 299, 308, 315, 324
Text 310
ThreadCount 49, 321
TransformResult 171, 197, 328
UsedSpaceGrowthPercentage 61, 304
UsedSpaceGrowthSpeed 61, 304
Value 124, 130, 136, 142, 150, 158, 301, 310, 312, 314, 318, 324
ValueFound 301, 318
VirtualBytes 49, 321
WorkingSet 49, 321

Parsing

XML LOG File 197

Paste

Monitoring Tools 263

PATROL

BMC Impact Manager 217
BMC Software PATROL Console 17
Console Server 284
Event 217
PATROL administrator 192
PATROL Agent 21, 241, 284
PATROL Agents 284
PATROL Central 21, 284
PATROL Central Operator 17
PATROL Configuration Manager 206
PATROL Console 21

Index
PATROL

PATROL Console Servers 21
PATROL Console Web-edition 17
PATROL Consoles 217
PATROL Enterprise Manager 217
PATROL for Event Management 206
PATROL interface 241

PATROL event

Trigger 231
Pause
Monitoring 265
Period
Execution 82
Pick
Process 49

PID
File 332
Files 49

Polling Interval
Set 269

Port 158

PostgreSQL Database
Connection 105
Settings 105

Pre-processing 197

Convert multi-line records to single records 171
Convert XML to CSV 171
Text 171
Text processing through an external command 171

Presence
File 65

Process
About 332
Command Line 332
Criteria 49
Identify 3232
Monitoring 49
Name 332
Pick 49
User ID 332

Process Command

Credentials 50
Process Macros

%{PROCESS_COMMAND_LINE} 227
%{PROCESS_NAME} 227
%{PROCESS_PID_FILE} 227
%{PROCESS_USER_ID} 227

Process Viewer

Tool 272

Properties

Command line 49, 332
Name 49, 332
PID 49, 332
User ID 49, 332

Property

DisplayName 335
Name 335
PathName 335
StartMode 335
State 335

Protocol

IIOP 136
JRFMP 136

Protocols

IIOP 124
RMI 124

Proxy

Server 107, 112
Settings 107, 112
PSL command
Execute 217

- Q -

Query
Set 88
SQL 88

- R -

Reference Guide 290
Refresh
Parameters 265

Regular Expressions

$ 292
* 292
.(dot) 292
[^a-z] 292
[^xyz] 292
[a-z] 292
[xyz] 292
\ 292
\expression\ 292
< 292
> 292
Monitoring Studio KM for PATROL
Version 8.6.54

Regular Expressions
^ 292
+ 292
exprA|exprB 292
Release Notes 10
Remove
Application Container 45
Application Icon 45
Rename
Object 266
Report 250
Configuration 252
Instant Configuration 251
Request
HTTP 107, 112
Requirements
Console systems 17
Managed systems 17
Rescaling 124, 130, 136, 142, 150, 158
Option 185
Reset
All 259
Restart
Application 268
Scan 268
Result 45, 49

- S -
Scan
Restart 268
Schedule
Configuration Report 251, 252
Search
String 181
Select
Counter 78
Instances 78
Lines 181
Parameters 49, 158, 185
Windows Performance object 78
Windows Service 58
Separator 185
Comma 181
Set
Alert Thresholds 206, 207
Discovery Interval 269
Polling Interval 269
Thresholds 211
Settings
Connection 93, 96, 100, 104, 105
Global 245
Java 260
Microsoft SQL Server 93, 104
Monitoring Studio 45, 49, 58, 61, 78, 82, 88, 107, 115, 118, 130, 136, 142, 150, 158, 162, 166, 171, 181, 185
MySQL Server 96
Oracle 100
PostgreSQL Server 105
Setup Files
Extract 19
Signature
Files 45
Size
File 65
SNMP
Agent 158
Polling 158
SNMP Trap Listener 273
Table OID 158
Trap 162
SNMP Browser
Tool 276
SNMP Browser tool 283
SNMP polling
Create 158
Edit 158
SNMP Polling Macros
%{SNMPPOLLED_COMMUNITY} 227
%{SNMP_POLLED_CONTENT} 227
%{SNMPPOLLED_HOST} 227
%{SNMP_POLLED_OID} 227
%{SNMPPOLLED_PORT} 227
SNMP Trap
Listening 162
SNMP Trap Listener
Tool 273
SNMP Trap Listener tool 279
SNMP Trap Macros
%{SNMP_TRAP_COMMUNITY} 227
%{SNMP_TRAP_CONTENT} 227
%{SNMP_TRAP_ENTERPRISEID} 227
%{SNMP_TRAP_FOUNDIP} 227
%{SNMP_TRAP_FOUNDTRAPNUMBER} 227
%{SNMP_TRAP_IP} 227
SNMP Trap Macros
  %{SNMPTRAP_TRAPNUMBER}  227
Sources
  Flat  280
Specify
  OS Command  171
SQL
    SQL*Plus  100
    SQL*Plus  286
Start
  Application Monitoring  237
Stop
  Application  271
  Application Monitoring  237
Streams
  stderr  82
  stdout  82
String
  Search  181
String Search
  Create  181
  Edit  181
String Search Macros
  %{STRING_LAST_MATCHING_LINE}  227
  %{STRING_LAST_MATCHING_LINES}  227
  %{STRING_SEARCHED_1}  227
  %{STRING_SEARCHED_2}  227
Sudo
  Utility  50
Suspend
  Monitoring  265
Systems
  HP Tru64  17
  HP-UX  17
  IBM AIX  17
  Linux  17, 18, 19, 50, 107
  Open VMS  17
  RedHat Linux  17
  Solaris  17
  SUSE Linux  17
  UNIX  17, 18, 19, 21, 50, 107, 292, 332
  VMWare ESX Host  17
  Windows  17, 18, 19, 21, 50, 107, 332

- T -

Templates

Numeric Value Extraction  192
String Search  192
Test  62
Text
  Pre-Processing  171
  Text Preprocessing object
    Create  171
    Edit  171
Thresholds
  Advanced  207
  Automatic  206
  Custom  49, 58, 61, 62, 75, 78, 82, 88, 107, 112, 115, 118, 124, 130, 136, 142, 150, 158, 162, 166, 181, 185
  Default  49, 58, 61, 62, 75, 78, 82, 88, 107, 112, 115, 118, 124, 130, 136, 142, 150, 158, 162, 166, 181, 185
  Event Management  206
  Manage  206
  Mechanism mode  206
  Simple  207
  Type  207
  Update  41
Timeout  124
Execution  82
Tool
  Process Viewer  272
  SNMP Browser  276
  SNMP Trap Listener  273
  Windows EventLog Reader  274
Traps
  Incoming  279
Tresholds
  Set  211
Trigger
  Alarm  192
  KM Discovery  271
  PATROL event  231
Troubleshooting  278
  Although SNMP Trap listening seems to work, no trap matches my criteria  279
  Can I monitor the processor time usage made by a Windows service?  279
  Can I search for Windows Events whose description match a regular expression?  279
  Difference between a flat file and a LOG file  280
  How do I know which version of Monitoring Studio I am running?  282
Troubleshooting 278
I'm unable to connect to the WebLogic application server 283
I'm unable to connect to the WebSphere application server 283
I'm unable to poll an SNMP agent (getting a Warning) 283
I'm unable to see the Monitoring Studio icons in PATROL Central 284
Infinite loop reported in the PATROL Agent log 284
Is it possible to monitor the CPU/memory usage of a process tree? 285
Monitoring Studio does not follow an HTTP redirection (Web) 287
Monitoring Studio does not read the content of my file 285
Monitoring Studio does not update all of my folder monitoring parameters 285
Monitoring Studio fails to authenticate on my Web server 286
Monitoring Studio fails to connect to a secured Web server (SSL) on my UNIX/Linux server 286
Monitoring Studio fails to connect to my Oracle Database server 286
Monitoring Studio fails to connect to my remote Microsoft SQL Server 286
Monitoring Studio is unable to listen to SNMP traps 287
Monitoring Studio reads my LOG file entirely 287
Not able to post a Web form to my Web server 288
What is the meaning of the "Argument1, 2,..." fields in the Windows Event monitoring wizard? 288

Tuning 206

- V -

Variables
Credentials 156
Dcom.sun.management.jmxremote.port 156
folderLimit 285
Host 156
Initial context factory 156
JNDI 156
KeyStore password 156
KeyStoreFile path 156
Node name 156
org.jboss.naming:org.jnp.interfaces 156
org.jnp.interfaces.NamingContextFactory 156
Path to Java on the local server 156
Port 156
Principle 156
Protocol 156
Server name 156
SOAP port 156
TrustStore password 156
TrustStoreFile path 156
URL package prefixes 156
View
Content 275

- W -

WBEM 118, 335
Query 115
WBEM Macros
{%SW_PASSWORD%} 227
{%SW_USERNAME%} 227
{%WBEM_HOST%} 227
{%WBEM_NAME_SPACE%} 227
{%WBEM_QUERY%} 227
{%WBEM_RETURN_OUTPUT%} 227
{%WBEM_USERNAME%} 227
WBEM Query Analysis
Create 115
Edit 115
Web Request Analysis
Create 112
Edit 112
Web-farm
Web-farm
  Monitoring 107
Web-farm Monitoring
  Create 107
WebLogic
  Attribute 142
  Connection information 142
  Credentials 142
  Domain 142
  Key property 142
WebSphere
  Attribute 150
  Credentials 150
  Domain 150
  Key property 150
Windows Event 166
  Monitor 166
  Monitoring 166
  Types 166
Windows Event log
  Application 166
  Monitor 166
  Security 166
  System 166
Windows Event Macros
  \%{EVENT_ID} 227
  \%{EVENT_LAST_MATCHING_CONTENT} 227
  \%{EVENT_LAST_MATCHING} 227
  \%{EVENT_LOG} 227
  \%{EVENT_SOURCE} 227
Windows event monitoring
  Create 166
  Edit 166
Windows EventLog Reader 288
  Tool 274
  Windows Events 288
Windows Performance
  Monitoring 78
Windows Performance Macros
  \%{PERFORMANCE_COUNTER} 227
  \%{PERFORMANCE_INSTANCELIST} 227
  \%{PERFORMANCE_PERFORMANCE} 227
Windows Performance Monitoring
  Create 78
  Edit 78
Windows Service
  Monitoring 58
Windows Service Macros
  \%{SERVICE_NAME} 227
Windows Service Monitoring
  Create 58
  Edit 58
WMI
  About 335
  Query 118
WMI Macros
  \%{SW_PASSWORD} 227
  \%{SW_USERNAME} 227
  \%{WMI_HOST} 227
  \%{WMI_NAME_SPACE} 227
  \%{WMI_QUERY} 227
  \%{WMI_RETURN_OUTPUT} 227
  \%{WMI_USERNAME} 227
WMI Query
  FROM 335
  SELECT 335
  WHERE 335
WMI Query Analysis
  Create 118
  Edit 118
  Workaround 41

- X -

XML LOG File
  Parsing 197
About BMC® Software

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 Capacity Optimization to ensure IT administrators that their storage infrastructure is properly sized for their current and future needs. The combination of its monitoring, automation, and capacity optimization capabilities for IT infrastructures, makes Sentry Software a key-partner in the storage management marketplace. For more information about Sentry Software, please visit www.sentrysoftware.com.